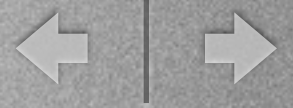




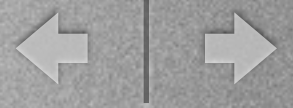
Threat, Vulnerabilities and Solutions: Protecting You and Your Members

National Pension Education
Association
October 28, 2008



Who Am I?

- Mark McChesney, Information Security Officer, Kentucky Retirement Systems
- Former Senior Manager responsible for the architecture, management and operation of enterprise voice, video and data infrastructures, as well as security at the Commonwealth Data Center.
- Past Regional President and Board of Directors member of the National Association of State Technology Directors (NASTD)
- Chair of the NASTD Security Special Interest Group (SIG) 2003-2008
- Member Multi-State Information Sharing & Analysis Center (MS-ISAC)
- Member NASCIO Security and Privacy Committee



- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- Certified in the Governance of Enterprise IT (CGEIT)
- GIAC HIPAA Security Implementation (GHSC)



Disclaimer

The information and opinions expressed in this presentation are solely mine and may not be those of my employer. Additionally, These stunts are performed by professional “security researchers” and should not be tried at home. You could be injured or even worse, Go to Jail!



SANS Top 10 Menaces (2008)

(www.sans.org)

- Increasingly Sophisticated **Web Site Attacks** That Exploit Browser Vulnerabilities - Especially On **Trusted** Web Sites
- Increasing Sophistication And **Effectiveness In Botnets**
- Cyber Espionage Efforts By Well Resourced Organizations Looking To **Extract Large Amounts Of Data** - Particularly Using Targeted Phishing
- **Mobile** Phone Threats, Especially Against iPhones And Android-Based Phones; Plus VOIP
- **Insider Attacks**
- Advanced Identity Theft from Persistent Bots
- **Increasingly Malicious Spyware**
- **Web Application Security Exploits**
- Increasingly **Sophisticated Social Engineering** Including Blending Phishing with VOIP and Event Phishing
- Supply Chain Attacks Infecting Consumer Devices (USB Thumb Drives, GPS Systems, **Photo Frames**, etc.) Distributed by Trusted Organizations

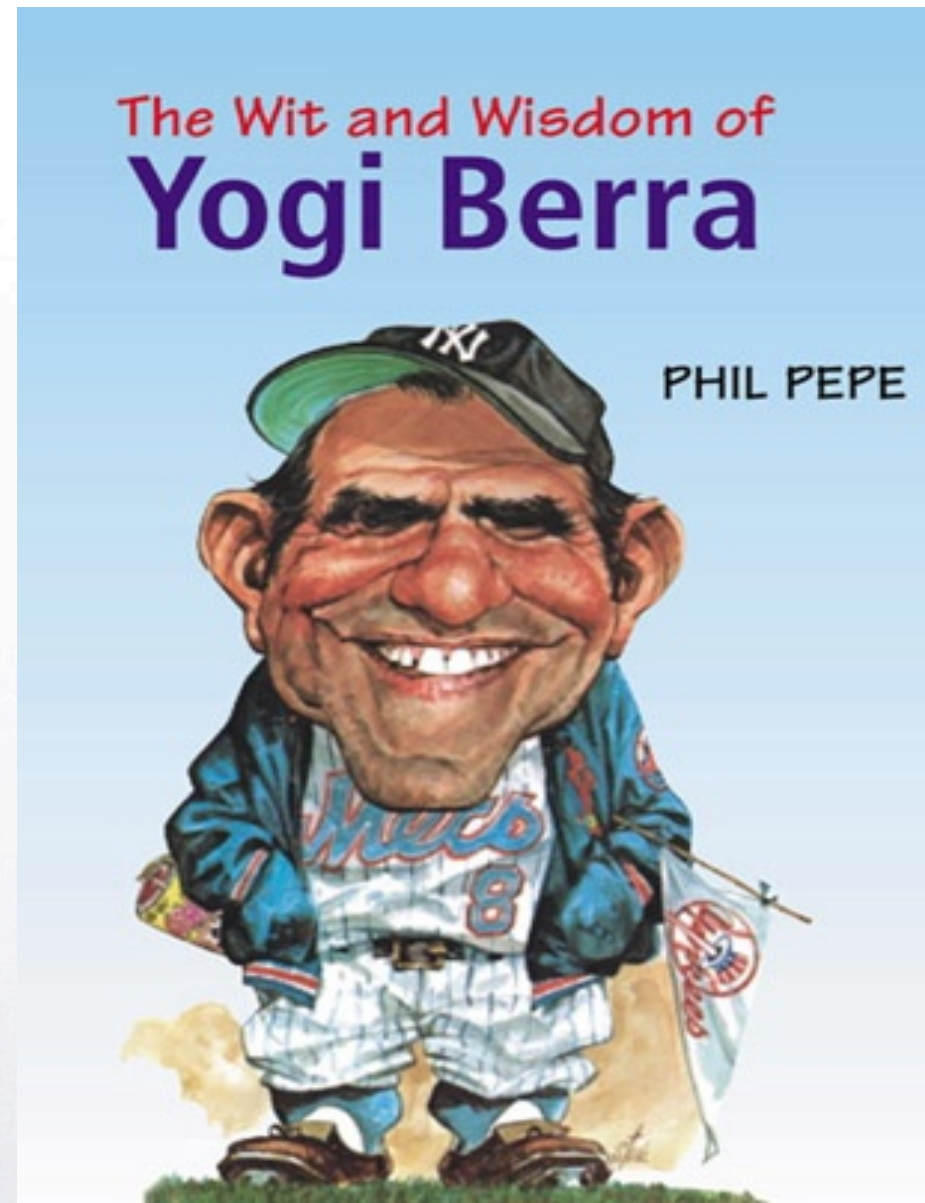


Risk - It's Everywhere

- Web Mobs and Organized Crime
- Powerful Hacker Tools: Useable by Anyone
- Disgruntled or Fired Employees
- Social Engineering
- Passwords on Post-It Notes
- Instant Messaging and Peer-to-Peer Applications
- Social Networks: Facebook, MySpace, Linked-In, Plaxo, Twitter, Yahoo!360, etc.



“The future ain’t what it used to



The Motivation Today





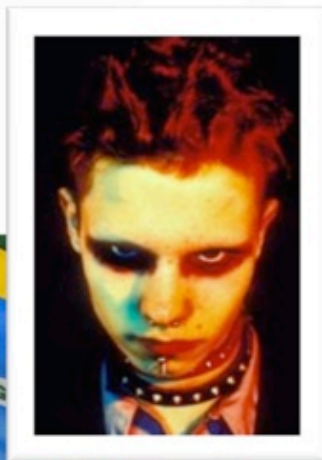
The Bad Guys



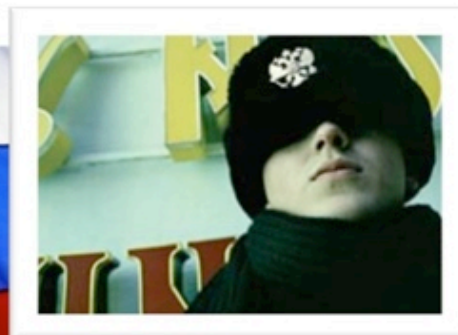
USA



Brazil



Russia



China





SCAM CZARS

What's Russian for 'Hacker'?

By CLIFFORD J. LEVY

Published: October 21, 2007

MOSCOW



PERHAPS the most famous con artist of the Soviet era was a fast-talking, eye-winking, nimble-fingered, double-dealing journeyman named Ostap Bender. He was fictional, the antihero of a satirical novel about a quest for lost jewels called "The 12 Chairs," but his casual disdain for the law reflected a widely held cynicism here.

"This misdeed, though it does come under the penal code, is as innocent as a children's game," Bender says of a scheme to use a purloined document to steal another man's identity.

SIGN IN TO E-MAIL
OR SAVE THIS

PRINT

SINGLE PAGE

REPRINTS

SHARE

The hackers go by names like ZOMBiE and the Hell Knights Crew, and they inhabit such a robust netherworld that Internet-security firms in places like Silicon Valley have had to acquire an expertise in Russian hacking culture half a world away. The security firms have not received much assistance from the Russian government, which seems to show little interest in a crackdown, as if officials privately take some pleasure in knowing that their compatriots are tormenting millions of people in the West.

In fact, Russian hackers became something akin to national heroes last spring when a wave of Internet attacks was launched from Russia against Web sites in Estonia, the former Soviet republic. The incidents began after the Estonians angered the Kremlin by moving a Soviet-era war monument.



Random Search Stops \$600 Million In Trade Secrets Bound For China

The feds have indicated a software engineer who was flying to China with confidential technical documents, a thumb drive, four external hard drives, 29 recordable compact discs, and a videotape.

By Thomas Claburn, [InformationWeek](#)

April 3, 2008

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=207001607>

A former software engineer for a telecommunications company based near Chicago was indicted for allegedly stealing trade secrets worth an estimated \$600 million and trying to take the documents to China.

The FBI [said](#) Wednesday that Hanjuan Jin of Schaumburg, Ill., a naturalized U.S. citizen who was born in China, was stopped at Chicago's O'Hare International Airport on Feb. 28, 2007, in a random search.

According to an affidavit filed by FBI special agent Michael R. Diekmann, Jin was traveling on a one-way ticket to Beijing at the time. She declared that she had \$10,000 in U.S. currency in her carry-on luggage. Customs and Border Protection officers found about \$30,000 in cash.

According to Diekmann, this prompted officers to further inspect Jin's luggage, whereupon they found several technical documents labeled "[Company A] Confidential Property," Chinese documents, a European company's product catalog of military technology written in English, a personal laptop computer, a thumb drive, four external hard drives, 29 recordable compact discs, and one videotape.

A search of the thumb drive and hard drives, conducted with Jin's consent, revealed numerous documents marked "[Company A] Confidential Property." Initially, Jin told customs officers she worked for Company A. In a subsequent interview with law enforcement agents, Jin said she was on medical leave from Company A. She later said she worked for Company A and Company B at the same time. Company B is a Chicago-area company that competes with Company A.



Answers? What was the question?


- Owns Nearly \$500 Billion in US Treasury Securities
- Over 200 Million Internet Users



The Soprano's?

TECH BIZ : MEDIA 

Cybercrime Is Getting Organized

Reuters  09.15.06 | 8:15 AM

Cyberscams are increasingly being committed by organized crime syndicates out to profit from sophisticated ruses rather than hackers keen to make an online name for themselves, according to a top U.S. official.

Christopher Painter, deputy chief of the computer crimes and intellectual property section at the Department of Justice, said there had been a distinct shift in recent years in the type of cybercriminals that online detectives now encounter.

"There has been a change in the people who attack computer networks, away from the 'bragging hacker' toward those driven by monetary motives," Painter told Reuters in an interview this week.

Although media reports often focus on stories about teenage hackers tracked down in their bedroom, the greater danger lies in the more anonymous virtual interlopers.

"There are still instances of these 'lone-gunman' hackers but more and more we are seeing organized criminal groups, groups that are often organized online targeting victims via the internet," said Painter, in London for a cybercrime conference.



The Soprano's?



Current Rank	Previous Rank	Goods and Services	Current Percentage	Previous Percentage	Range of Prices
1	2	Bank accounts	22%	21%	\$10-\$1000
2	1	Credit cards	13%	22%	\$0.40-\$20
3	7	Full identities	9%	6%	\$1-\$15
4	N/A	eBay accounts	7%	N/A	\$1-\$8
5	8	Scams	7%	6%	\$2.50/week-\$50/week for hosting, \$25 for design
6	4	Mailers	6%	8%	\$1-\$10
7	5	Email addresses	5%	6%	\$0.83/MB-\$10/MB
8	3	Email passwords	5%	8%	\$4-\$30
9	N/A	Drop (request or offer)	5%	N/A	10%-50% of total drop amount
10	6	Proxies	5%	6%	\$1.50-\$30

Table 1. Breakdown of goods and services available for sale on underground economy servers

Source: Symantec Corporation



Malware

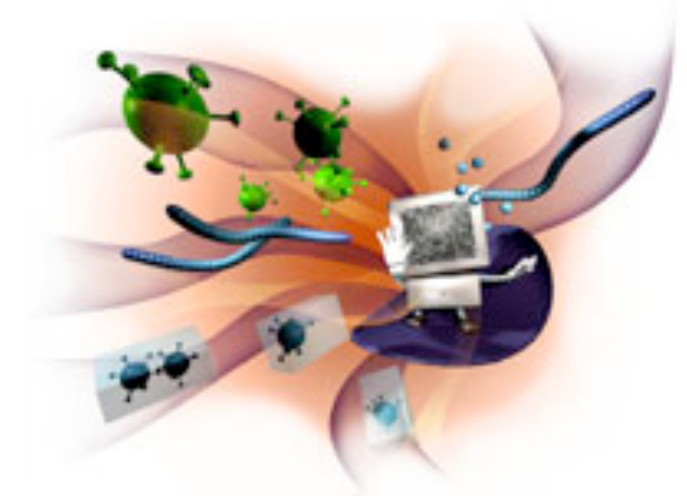


Malware

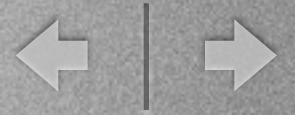
- Historically, malware has plagued e-mail, hidden in malicious attachments
- While that's still happening, more malware writers are putting their efforts into malicious Web sites
- 70% of porn is downloaded between 9 and 5



Malware



- There are now more than 200,000 known examples of malware
- Almost all those are for Windows or Internet Explorer on Windows
- About 50 new instances are reported each day



Botnets/Zombies

- These Botnets are used as tools by Hackers for:
 - Distributed Denial-of-Service Attacks
 - Spamming
 - Sniffing Traffic
 - Keylogging
 - Spreading new malware
 - Installing Advertisement Add-ons



Super Bowl stadium site packed Trojan horse

By Joris Evers

Staff Writer, CNET News.com

Published: February 2, 2007, 11:59 AM PST

Last modified: February 2, 2007, 2:36 PM PST

[TalkBack](#) [E-mail](#) [Print](#) [del.icio.us](#) [Digg this](#)

Cybercrooks broke in to the Dolphin Stadium Web site and rigged it to load malicious software onto unpatched Windows PCs, security experts warned Friday.

Hackers reprogrammed the Web site for the Super Bowl stadium so it would automatically load a malicious script, Web security firm Websense said. This script would attempt to exploit a [pair of known Windows security holes](#) and install programs that would put the PC under the attacker's control.



"Assuming you're not patched, a Trojan downloader with a backdoor and a password stealer gets installed on your computer without you knowing it," said Dan Hubbard, vice president of security research at San Diego, Calif.-based Websense.

The initial breach of the Dolphin Stadium Web site appears to have occurred on January 25, Hubbard said. The site was cleaned up around 11 a.m. PST on Friday, he said.

A Dolphin Stadium representative confirmed the hack. "The stadium Web site was compromised and the problem was resolved," said the representative, who asked not to be named. She could not give an indication as to how many people were exposed to the attack, but did say the site is getting more visits "just because of the Super Bowl."

The attack exploited two known security holes in the way Windows handles Vector Markup Language, or VML, documents, Websense

[Ad Feedback](#)

Introducing Schwab Bank High Yield Investor Checking.™

- ▶ Zero ATM fees
- ▶ 4.25% APY (9x the National Average)
- ▶ No catches

TALK TO CHUCK

[Learn more](#)

charles SCHWAB BANK



Featured gallery

Photos: Happy developers in da ho

A German timber technology student turned to material--beech wood--for his two-wheeled cr this gallery...

RELATED STORIES

WHAT'S HOT

LATEST HEADLINES

Related news

- [Attack code out for 'critical' Windows flaw](#)
January 16, 2007
- [Microsoft leaves Word zero-day holes unpatched](#)
January 9, 2007
- [Microsoft rushes out 'critical' fix](#)
September 26, 2006



Region : [US](#) [UK](#) [Asia](#) [Aus/NZ](#)

Awards: [US](#) [Europe](#)

Google™ Custom Search

Search

[Home](#) [News](#) [Alerts](#) [Products](#) [Vendors](#) [Blogs](#) [White Papers](#) [Jobs](#) [Subscribe](#) [Events](#)

[IT Security Training](#) [Mobile/Endpoint Security](#) [Patch Management](#) [Compliance](#) [Email Security](#)

You are here: [SC Magazine US](#) > [News](#) > March Madness could lead to malware infection, experts warn

NEWS

[Email this article](#) [Print this page](#) [Digg this article](#) [Order Reprint](#)

March Madness could lead to malware infection, experts warn

Dan Kaplan Mar 15 2007 16:48

Assuming they have not called in "sick," employees at companies of all sizes could spend today and Friday bringing the network to a screeching halt or opening it up to malware infection, security experts warn.

Welcome to March Madness, when dozens of men's college basketball games air Thursday and Friday as teams compete in the opening round of the 64-team tournament. For many workers, that means a serious drop in productivity as they neurotically watch the games, hoping to improve their standing in the company office pool.

But for IT administrators, this annual tradition means clogged network connections – as users stream video of the games at their desks – or the risk of [malware](#) infiltration, as those same users visit malicious websites to place bets, manage brackets or get scores.

"It's the last major sporting event that occurs during the business day," Eric Lundbohm, vice president of marketing at [8e6 Technologies](#), a web filtering firm, told SCMagazine.com. "It's not just interest; these games are actually happening."

Paul Henry, vice president of technology at [Secure Computing](#), said cyberthieves are increasingly targeting popular websites with [script malware](#), often undetectable by anti-[virus](#) signatures. He cited [the example](#) of Dolphin Stadium's website, which crooks embedded with [JavaScript](#) malware that took advantage of two patched Microsoft [vulnerabilities](#), in the days leading up to this year's Super Bowl.

"The popularity of the sites is going to drive hackers (there) to see if they can be compromised," Henry said. "The malware would traditionally be [keyloggers](#) and [trojans](#)."



IN OTHER NEWS

Related News Stories

[Kaspersky: Keylogger use up 500 percent in three-plus years](#)

[PadaLabs: Trojan targets corporate data](#)

[Mozilla releases updates for Firefox, SeaMonkey flaws](#)

[Watchfire spots Google Desktop vulnerability that can allow access to sensitive files](#)

[JavaScript malware infecting various websites](#)

[Just two days before Super Bowl XLI, hackers use Dolphin Stadium website to exploit PCs](#)

Latest Headlines



Compromised Halloween websites passing along rogue software

Angela Moscaritolo October 22 2008

An internet search using the keywords "halloween costumes" may turn up a number of legitimate sites that have been compromised, and users might end up with [rogue anti-virus software](#) on their machine.

The Halloween attack uses search engine optimization manipulation to distribute the campaigns, according to a Wednesday TrendLabs [blog](#) post.

Attackers prey on the vulnerabilities in legitimate websites to embed malicious code, according to Trend. Once determining a website is vulnerable, a pointer to a specially crafted rogue page -- containing many mentions of the words "halloween costumes" -- is injected into the legitimate website.

That way, when an unsuspecting web user searches those terms, the legitimate but compromised website will return a high ranking and he or she will be more likely to visit there.

The infected site contains malicious JavaScript that will redirect users to another site without their knowing. When, for example, a user clicks an online store to browse Halloween costumes, they will be redirected to a page with a pop-up claiming their computer is running slower than normal. The pop-up says the user's PC might be infected with some type of malware.

"When users click on the resulting pages, there will be software directions and the final payload will be the fake or rogue anti-virus software," Ivan Macalintal, research manager at Trend Micro, told SCMagazineUS.com Wednesday.

The pop-up asks users if they want to download Antivirus 2009, claiming the software will scan their machine for malware -- but Antivirus 2009 is really a fake program.



From the News Desk

Compromised web sites serve more malware than malicious ones

By [Joel Hruska](#) | Published: January 22, 2008 - 09:40PM CT

The fact that legitimate web sites can be compromised and used to distribute malware under an admin's nose is something Ars has [touched on](#) of late. In that particular case, the culprit has been a particular type of JavaScript exploit, but the general issue of legitimate web sites serving malware is a growing problem.

According to security firm WebSense, the number of legitimate web sites that have been hacked and are distributing or enabling various types of malware attacks is greater than the number of malicious sites created specifically for that purpose. The company's latest [report](#) (PDF) discusses this trend, along with the tremendous impact the Storm Worm had on the 'Net through all of 2007. As WebSense states, there's a clear advantage to infecting a legitimate site that comes with its own built-in traffic and a user base.

The type of theft varies depending on the site. Personal data and credit card information are the most obvious acquisition targets, but online gaming account theft and click-fraud are apparently common as well. It's well known that there are forums, discussion groups, and IRC channels devoted to the topics of which web sites are known to be vulnerable. The problem also runs deeper than simply educating administrators about security vulnerabilities in the software that they use—locating the correct host provider for any particular web space can be difficult, and many sites don't fall off WebSense's malicious site blacklist quickly, sometimes remaining there for weeks or even months after being notified of a problem.



October 21, 2008

A Robot Network Seeks to Enlist Your Computer

By [JOHN MARKOFF](#)

REDMOND, Wash. — In a windowless room on [Microsoft's](#) campus here, T. J. Campana, a cybercrime investigator, connects an unprotected computer running an early version of Windows XP to the Internet. In about 30 seconds the computer is “owned.”

An automated program lurking on the Internet has remotely taken over the PC and turned it into a “zombie.” That computer and other zombie machines are then assembled into systems called “botnets” — home and business PCs that are hooked together into a vast chain of cyber-robots that do the bidding of automated programs to send the majority of e-mail [spam](#), to illegally seek financial information and to install malicious software on still more PCs.

Botnets remain an Internet scourge. Active zombie networks created by a growing criminal underground peaked last month at more than half a million computers, according to [shadowserver.org](#), an organization that tracks botnets. Even though security experts have diminished the botnets to about 300,000 computers, that is still twice the number detected a year ago.

The actual numbers may be far larger; Microsoft investigators, who say they are tracking about 1,000 botnets at any given time, say the largest network still controls several million PCs.

“The mean time to infection is less than five minutes,” said Richie Lai, who is part of Microsoft’s Internet Safety Enforcement Team, a group of about 20 researchers and investigators. The team is tackling a menace that in the last five years has grown from a computer hacker pastime to a dark business that is threatening the commercial viability of the Internet.



MONDAY, JANUARY 14, 2008

Computer data more valuable than coins and equipment

An [office breakin story](#) (highlit by [InfoSec News](#)) appears to indicate a targeted theft of computers for the valuable data they contained, rather than the hardware itself.

"PICKY thieves have led one private education centre to believe that industrial espionage might be the motive for a recent break-in. Early this week, three of the CES group's computers - containing the personal details and contacts of its 30,000 students - were stolen from its Eu Tong Sen Street office. Surprisingly, 10 other computers in the same location, some of them newer than the stolen items, and other expensive equipment like scanners were left untouched. The thieves' specific choices have led CES group chairman Desmond Lim, 35, to suspect that they could have been looking for the information stored in these computers for business reasons. ... And while the computer stolen from the administration room might have been the oldest, it was also the only one with all the students' data, said Camford Business School principal Indra Padmakumara, 30, whose school is part of the CES group. The other three computers in that room were not taken, she said. Nor were they tampered with. The door to Mr Lim's room was forced open, although a brand new projector, a digital camera and a box full of coins, all lying within plain view, were not taken."



Laptops and Wireless Networks

- How Many of You Have a Laptop?
- How Many of You Use Wireless Networks at Work, Home or While You Travel?



Compromised

- Compromised laptop computers are the target of choice
- Laptops by their nature are "promiscuous" and could be attached to any number of unsafe networks
- Once a laptop is compromised and a good Trojan installed that bypasses firewall security; then the whole network, including any VPN is possibly and hopelessly compromised





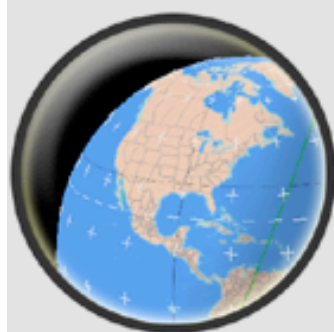
Why Are They Hacking Wireless Networks?

- To get direct access to your internal network
 - This gets them “inside the door”
 - Allows them to by-pass normal security barriers
- Complete anonymity
 - No risk of being traced
 - Not being watched
 - Difficult to find the trespasser
- Easy to use tools that are cheap or FREE
- Very large attack surface



Wireless Signal Leakage





[Home](#) | [Download](#) | [Forums](#) | [Post File](#) | [Query](#) | [Screenshots](#) | [Stats](#) | [Uploads](#) | [Web Maps](#) | [MapPacks/T](#)

WIGLE.NETTM

Wireless Geographic Logging Engine: Making maps of wireless networks since 2001

15,234,822 points from 918,844,664 unique observations.

login user: password: ☐ Don't expire auth cookie [non-ssl](#) or [make a new account](#)

news:

the seven year itch

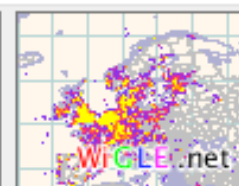
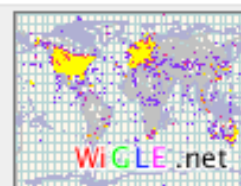
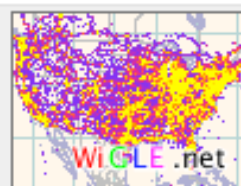
Tue Sep 9 10:39:40 2008

seven years and 15+ million networks later and WiGLE.net keeps on putting a lot of little dots on maps. thank you all for keeping us company on this long strange stumble. truly amazing!
-uhtu

an 'F' of a lot of points.

Thu Aug 28 21:27:11 2008

well, 0xF-million points. Once again, Dutch crested the WiGLE upload tsunami as it broke upon the shore of 15 millions. Congratulations, and thanks to EVERYONE who has helped us reach this milestone! I knew we shouldn't have used a single hex digit to represent our millions of access points... time to rewrite everything.
-arkasha



The wireless world this morning (GMT-6:00).



Find a wireless network by [\[searching\]](#) (must be registered) or [\[browsing the interactive map\]](#)



Add a wireless network to WiGLE [\[from a stumble file\]](#) or [\[by hand\]](#)



Add [\[remarks\]](#) to an existing network(must be registered)

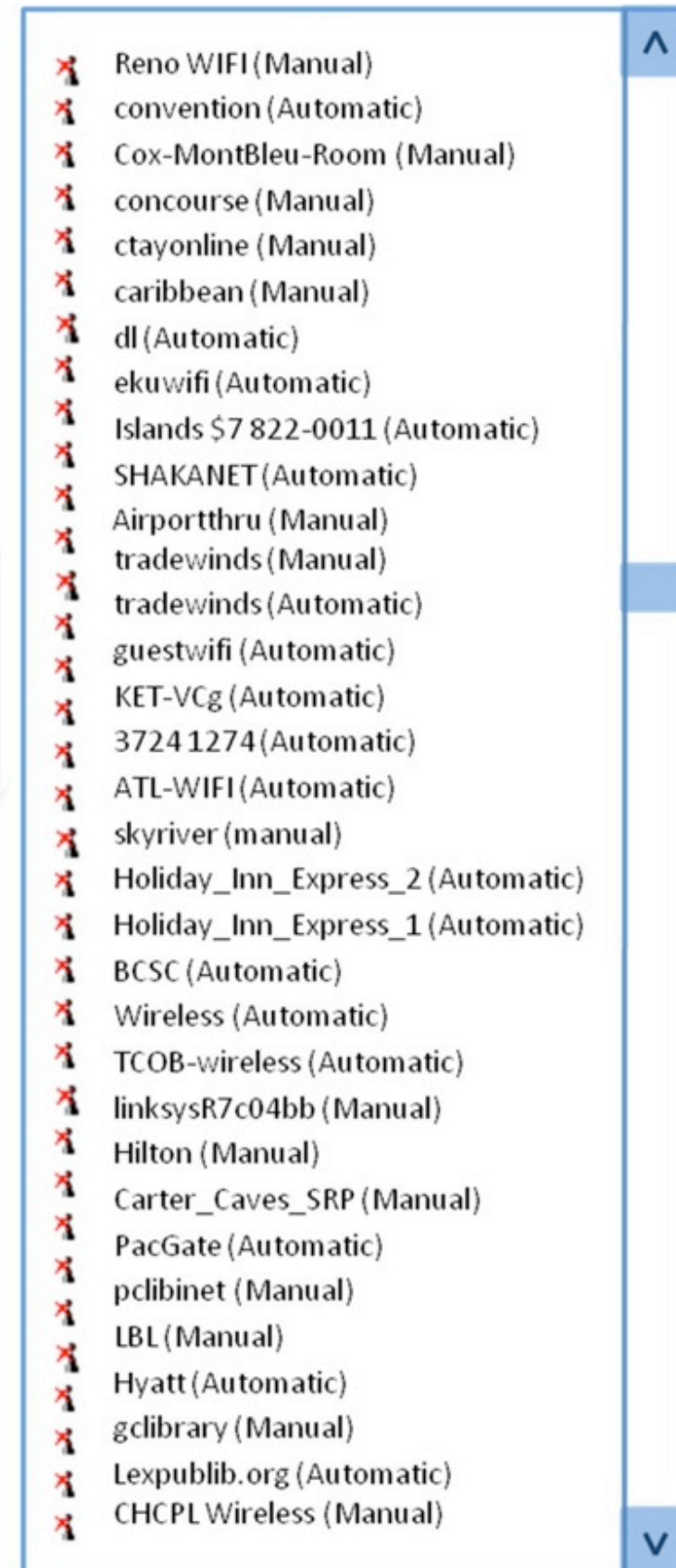
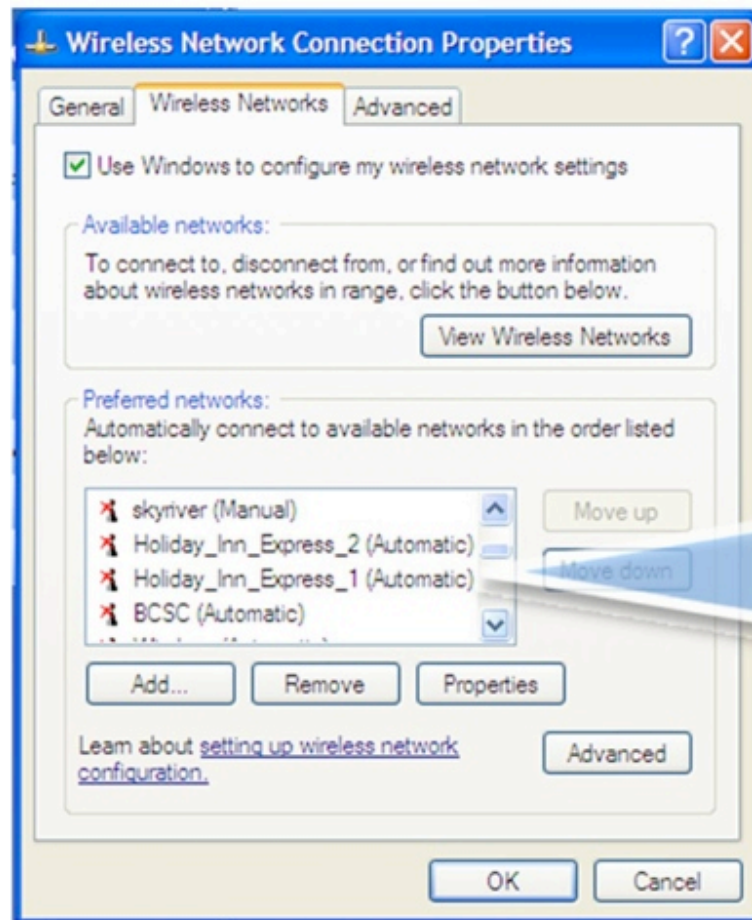


See statistics: [\[general\]](#), [\[personal\]](#) (must be registered), or [\[group\]](#) (must be registered)



Download [\[interactive clients\]](#), [\[location data for clients\]](#), (must be registered) [\[screenshots\]](#), or [\[random pictures\]](#)




Do NOT Let your computer cache wireless networks!



And Remember: There is no such thing
as a free lunch or **Free Public WiFi**



Do You Use Bluetooth?

	Device Type	Device Name	MAC Address	Vendor	Paired	Linked	Fa
	computer	Mike Knezevich's Com	00-1b-63-5c-a4-c6	00-1B-63	No	No	N
	computer	BHS000FB06EA3FC	00-10-c6-84-b9-b2	00-10-C6	No	No	N
	phone		00-0f-86-ae-44-36	00-0F-86			



Do You Use Bluetooth?



Bluetooth Threats

- If Your Device/Phone is “Discoverable” with the Default PIN, ANYONE can Connect
- Paired Devices Get Access to the Entire Device
- Read/Write SMS, Phonebook, Notes, Photos, etc.
- Most Devices Use Default PINS
- Listen to Conversations
- Inject Audio?
- Track You? Many Phones Now Include GPS



Some Things You Can Do

- Turn Off Bluetooth When Not In Use
- At Least, Turn Off “Discoverable” Mode
- Change the Default PIN
- Limit Access to Specific Paired Devices
- Turn Off Headsets and Other Devices When Not in Use



Your Blackberry, iPhone and Smartphone IS a Computer

The Insider is hard to Identify





FOXNEWS.COM HOME > SCITECH

Angry Employee Deletes All of Company's Data

Thursday, January 24, 2008

FOX NEWS

[E-Mail](#) | [Print](#)

Share: Digg | Facebook | StumbleUpon



Jacksonville Sheriff's Office

A mug shot of Marie Lupe Cooley released by the Jacksonville Sheriff's Office.

going to get axed."

It didn't take Steven Hutchins, owner of the architectural firm that bears his name, much time to figure out who'd done it — Cooley was the only other person who had full access to the files.

Call it a tale of revenge gone wrong.

When Marie Lupe Cooley, 41, of Jacksonville, Fla., saw a help-wanted ad in the newspaper for a position that looked suspiciously like her current job — and with her boss's phone number listed — she assumed she was about to be fired.

So, police say, she went to the architectural office where she works late Sunday night and erased 7 years' worth of drawings and blueprints, estimated to be worth \$2.5 million.

"She decided to mess up everything for everybody," Jacksonville Sheriff's Office spokesman Ken Jefferson told reporters. "She just sabotaged the entire business, thinking she was

Boeing Employee Charged With Stealing 320,000 Sensitive Files

A quality assurance inspector faces 16 charges of computer trespass for allegedly loading sensitive data on his thumb drive and walking out with it over the course of more than two years.

By [Sharon Gaudin](#)
[InformationWeek](#)

July 11, 2007 03:50 PM



Two accused of thefts from church, business

Josh Sullivan

March 20, 2008



Tonya Blackburn

Tonya Blackburn, a Frankfort woman with a criminal record, was accused by a grand jury Thursday of stealing more than \$30,000 from her company.

Melissa Dean, also of Frankfort, was charged by the same jury of stealing \$10,000 from local high school football boosters and a church.

The \$30,000 theft was among 34 felony and six misdemeanor theft by unlawful taking between June of 2007 and the indictment of Blackburn, 34, a secretary at Me

The indictments were handed out in Franklin County Attorney Larry Cleveland said Blackburn wrote checks that pretended they were being issued to a vendor.

"She was attempting to masquerade them as legitimate business expenses,"

The largest forged check was written for \$7,250 in January.

Blackburn was convicted of theft by unlawful taking in a separate incident in 2006, found guilty to stealing \$13,569.04 from the Frankfort Younger Women's Club and diverting the money. The charges were expected to be dropped.

[Email To A Friend](#)
[Printer Friendly](#)
[Comments](#)



State employee charged with stealing \$2,000 from non-profits

BY CHARLIE PEARL

March 13, 2008

Leela Flowers, a state employee involved in charitable work, was indicted Wednesday on three counts of theft.

A Franklin County grand jury accused Flowers, 47, of 200 Smoot Lane, of unlawfully taking monies belonging to the Kentucky Employees Charitable Contributions Fund of the Kentucky Office of Insurance in November 2007.

"She converted money collected in her office, \$2,068, to her own personal use and did not pay back the money," said Commonwealth's Attorney Larry Cleveland.

Flowers is an administrative assistant for the Kentucky Office of Insurance in the Environmental and Public Protection Cabinet, Cleveland said.

In addition to facing one felony count of theft by unlawful taking over \$300, Flowers was charged with one count each of theft by deception of property over \$300, a felony, and theft by deception of property under \$300, a misdemeanor.

Cleveland said Flowers wrote two checks "in the amounts of \$1,829 and \$239 to pay back the money" "but the checks bounced," he said.

[Email To A Friend](#)
[Printer Friendly](#)
[Comments](#)





Feds Charge California Woman With Stealing IDs From the Dead

By Kevin Poulsen April 17, 2008 | 3:14:12 PM Categories: [Crime](#)

Federal prosecutors this week charged a Southern California woman with aggravated identity theft and other crimes for allegedly using a popular genealogy research website to locate people who had recently died, and then taking over their credit cards.

Tracy June Kirkland, 42, allegedly used [Rootsweb.com](#) to find the names, Social Security numbers and birth dates of people who, shall we say, had no further need for their consumer credit lines. She then "would randomly call various credit card companies to determine if the deceased individual had an ... account," according to the [15-count indictment](#) (.pdf) filed in federal court in Los Angeles Tuesday.

She'd then persuade the issuer to change the mailing address for the dead victim to one of her many rented mail drops in Orange and Riverside counties, and in some cases she'd add her own name as an authorized user of the card, prosecutors say. The lenders included Nordstrom Federal Savings Bank, Macy's and GE Money Bank.



UCLA workers snooped in Spears' medical records



Dan Steinberg / Associated Press

Security guards stand outside of the ambulance entrance to the at the UCLA Medical Center emergency room in Los Angeles on Thursday, Jan. 31, 2008, after Britney Spears was admitted. At least 13 employees of the hospital are to be fired for peeking at Spears' medical records without authorization.

The Medical Center is taking steps to fire at least 13 employees and is disciplining others, including doctors, for looking at the pop star's confidential files.

By Charles Ornstein, Los Angeles Times Staff Writer
March 15, 2008

UCLA Medical Center is taking steps to fire at least 13 employees and has suspended at least six others for snooping in the confidential medical records of pop star Britney Spears during her recent hospitalization in its psychiatric unit, a person familiar with the matter said Friday.

In addition, six physicians face discipline for peeking at her computerized records, the person said.



Identity thieves prey on patients' medical records

Updated 2h 16m ago | [Comments 41](#) | [Recommend 19](#)

[E-mail](#) | [Save](#) | [Print](#) | [Reprints & Permissions](#) | [RSS](#)

■ BASIC SAFEGUARDS

To guard against and deal with medical record theft:

- Check medical records or statements from your insurer for benefits paid under your name but not received.
- Monitor your credit report for collection notices from medical providers.
- File a police report if your information is stolen.
- Amend your records to correct misinformation.

Source: USA TODAY research

By [Julie Appleby](#), USA TODAY

Doctors' offices, clinics and hospitals are a fruitful hunting ground for identity thieves, who are using increasingly sophisticated methods to steal patient information, lawyers and privacy experts say.

Recent disclosures that hospital workers snooped into the medical files of Maria Shriver, Britney Spears and George Clooney highlight the vulnerability of patients to the merely curious and the criminal.

Legal experts say lawbreakers use medical information to get credit card numbers, drain bank accounts or falsely bill Medicare and other insurers.

RECORDS: [It's often hard for patients to get even their own files](#)

Marc Rotenberg, executive director of the Electronic Privacy Information Center, says attention on identity theft has focused

on how easily criminals can get financial records. "Now we're moving into an era where many of those same problems occur with medical records," he says.



Other ways to share:



[What's this?](#)

The State Journal

50 CENTS DAILY

FRANKFORT, KENTUCKY

\$1.25 SUNDAY

Cheak pleads guilty to

Former Revenue Cabinet employee David Cheak pleaded guilty to embezzling \$4.2 million from the Kentucky State Treasury.

- By DAVE BAKER
- State Journal Staff Writer

Former Revenue Cabinet employee David Cheak pleaded guilty to embezzling \$4.2 million from the state.

Cheak, 41, told Frankfort Judge William Graham he was on medication for a bi-polar disorder, but said the drugs did not impair his decision to enter a guilty plea.

Cheak pleaded guilty to 10 counts of unlawful access to a computer and three counts of theft. Assistant Commonwealth's Attorney Larry Cleveland recommended a 14-year sentence.

The former Revenue Cabinet employee, a graduate of the University of Kentucky, had contended the thefts were the result of a mental illness.

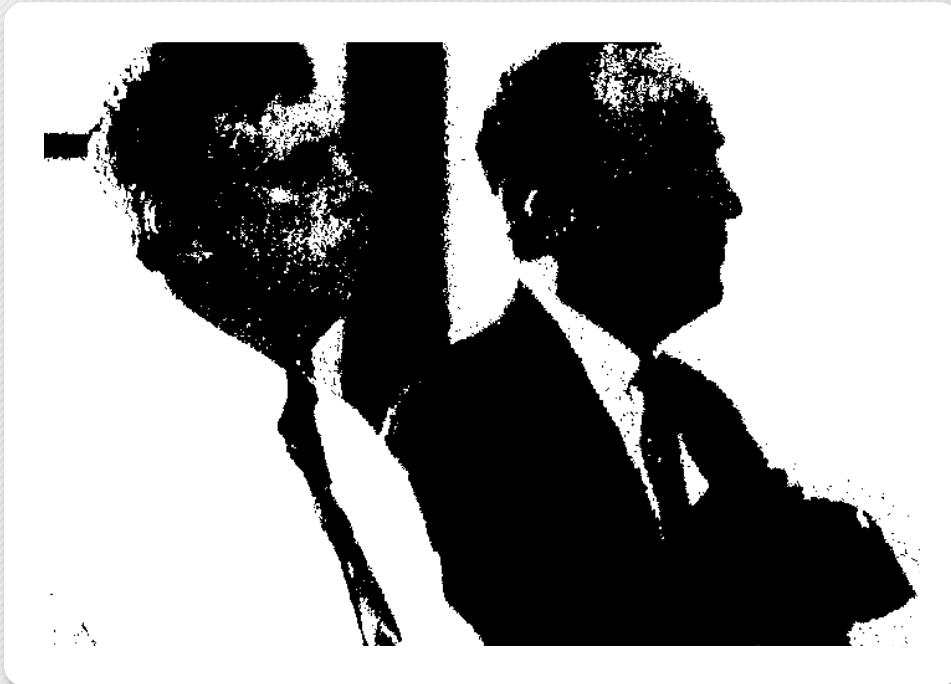
Cheak, who appeared clean-shaven for his court appearance, was to stand trial today. Cheak pleaded guilty to all his counts instead. "He felt it wasn't in his best interest to go to trial," said.

later time.

As part of his plea bargain agreement, Cheak will reveal to Cleveland and Kentucky State Police Det. Mark Stapleton how he stole the money.

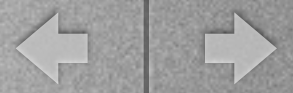
Cheak also will surrender \$184,000 he maintained in three Indiana bank accounts, give up rights to \$453,000 from the sale of various farms and other items purchased with the stolen money, and turn over personal computer equipment, according to his plea bargain.

Cleveland said he had a solid case against Cheak. "We could show to the second when each theft was done."



State Journal/John Sommers II

DAVID Cheak, left, pleaded guilty today to the embezzlement of \$4.2 million in state money. He appeared with attorney Paul Harnice.



FRONT

**SOCIAL ENGINEERING
SPECIALIST**

BACK

**Because there is no patch
for human stupidity**

FRONT



BACK





Sometimes the Insider Issue is Not Even a Malicious Act



Oops: Cable company deletes 14K customers' e-mail accounts

Charter Communications is blaming a software error for the deletion of all the messages in e-mail accounts belonging to 14,000 customers across the USA.

The [St. Louis Post-Dispatch](#) says when customers logged into their accounts Monday many were shocked to discover that everything was gone — for good. That's because, a spokeswoman says, the company set out to delete inactive e-mail accounts, but ended up destroying thousands of active ones, too.

"It's never happened before. They are taking steps to make sure it never happens again," spokeswoman Anita Lamont tells the Associated Press.

[PC World](#) says the company is offering each of the customers a \$50 credit.

State employee fired after security breach

Advertisement

Mailing errors taken seriously, official tells privacy committee

By Keegan Kyle

Press-Gazette Madison bureau kkyle@greenbaypressgazette.com January 25, 2008

MADISON — A state contractor has fired an employee in connection with a breach of Social Security numbers in a statewide mailing earlier this month, officials said Thursday.

Department of Health and Family Services Secretary Kevin Hayden appeared before a state Assembly committee on privacy to discuss the Jan. 8 incident involving 260,000 disclosed Social Security numbers in mailings to BadgerCare and SeniorCare recipients in southern Wisconsin.

Hayden told the committee he was informed by Electronic Data Systems — the company that manages the state's Medicaid system — that the "individual who failed to follow the (company's) policies was terminated."

The firing is the latest development in a series of confidentiality breaches of private information involving state agency mailings in the past year.

More than a week ago, the Department of Administration and the Department of Revenue admitted that a mechanical error resulted in some Northeastern Wisconsin taxpayers receiving a 1099G form with their Social Security numbers visible through the envelope window.

In December 2006, another vendor mailed about 171,000 tax forms from the Department of Revenue with Social Security numbers on the label.

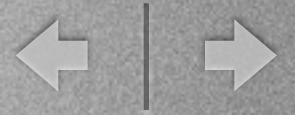
What Were They Thinking?



AFP Published This Untouched Photograph of a Hurricane Katrina Evacuee and Her Debit Card; What Happened Next Was No Surprise

Insider Threat

- **Insider Threat Studies**
 - ✦ Illicit Cyber Activity in the Banking and Finance Sectors
 - ✦ Illicit Cyber Activity in the IT and Telecommunications Sectors
 - ✦ Illicit Cyber Activity in the Government Sector
 - ✦ Computer System Sabotage in Critical Infrastructure Sectors
- **Combating the Insider Cyber Threat**
- **Protecting Against Insider Threat**
- **Common Sense Guide to Prevention & Detection of Insider Threats**
- **Risk Mitigation Strategies: Lessons Learned from Actual Attacks**
http://www.cert.org/insider_threat/
- **Insider Security Threats: State CIOs Take Action Now!**
<http://www.nascio.org/publications/documents/NASCIO-InsiderSecurityThreats.pdf>



Who Else is Interested?

- The Media
- CPA and Consulting Firms
- The Auditor of Public Accounts (APA)
- The Attorney General





Office of the Attorney General

Attorney General Stumbo Announces Results Of Identity Theft Prevention Initiative

Press Release Date: Tuesday, October 30, 2007

Revision Date: Wednesday, October 31, 2007

(Added links to our new brochure and other online resources.)

Contact Information: Corey Bellamy, 502-696-5643 Office

Attorney General Greg Stumbo today announced the Office of Consumer Protection's records disposal investigation to determine if Kentucky businesses are complying with state law by properly disposing of personal information contained in business records.

During July and August the Office of Consumer Protection examined publicly accessible trash receptacles of 121 businesses in Florence, Frankfort, Lexington and Louisville. Of those examined, 33 threw away over 500 records containing the personal information of over 1,250 people. Of these, 14 businesses threw away more sensitive information, like Social Security numbers, bank and credit card account numbers, birth dates, driver's license or personal ID card numbers, loan numbers, customer account numbers, insurance policy numbers, medical insurance policy and group numbers, and personal medical information, of almost 1,000 people.

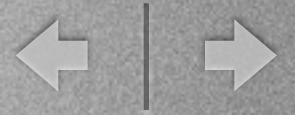


Social Networks and Peer-to-Peer Networks



Look what's happening – Collaboration!

- MySpace – close to 190 million profiles
- Flickr – again, in the millions
- Facebook - 40 Billion Page Views each Month; 150,000 new subscribers every day
- Twitter, Pownce, etc.
- Second Life – 3.7 million ‘residents’; 62,000 online this past weekend at the same time
- YouTube – more than 13 million unique users; 2/1/08: 69 Million videos.
- Bittorent
- Other Peer-to-Peer Applications



- This adds a whole new specter of threats and vulnerabilities into the network
- Multiple threats in the past 6 months with many of these applications.
- Four out of 10 users of Web site Facebook unwittingly expose themselves to the risk of identity theft and virus attacks
- 41 percent divulged personal information, such as phone numbers, birthdates and e-mail addresses, that could be viewed by strangers

Accusation of ID theft by file-sharing

AP Associated Press

TECHNOLOGY VIDEO

**Wi-fi bridges
digital divide**
BBC**Sony Upgrades
PSP**
ABC News[» All news video](#)

\$ RELATED QUOTES

^IXIC	2559.11	0.00
^IXK	1147.24	0.00
^DJUSS	511.79	-4.39

Delayed Data
[Providers - Disclaimer](#)

ELSEWHERE ON THE WEB

CNN.com: [Moonwalker: Nowak
should be admired](#)**ABC News:** [Insurgents Fight Iraq
War in Cyberspace](#)**CNN.com:** [Fossett searchers
returning to skies](#)

By GENE JOHNSON, AP Legal Affairs Writer

Thu Sep 6, 8:08 PM ET

SEATTLE - A Seattle man has been arrested in what the Justice Department described as its first case against someone accused of using file-sharing digital data to commit identity theft.

Gregory Thomas Kopiloff primarily used Limewire's file-sharing program to troll other people's computers for financial information, which he used to open credit cards for an online shopping spree, federal prosecutors said Thursday.

Kopiloff was arrested Wednesday at his government-subsidized apartment a few blocks from the federal courthouse here. According to a four-count indictment, he bought at least \$73,000 worth of goods online — including iPods and laptop computers — then resold those items at half-price and kept the proceeds. Investigators said he blew through most of the money supporting a gambling habit.

Authorities said they have identified least 83 victims — most of whom have teenage children and did not know the file-sharing software was on their computer. But investigators also said they believe the number of people affected was in the hundreds — and that in all they lost hundreds of thousands of dollars.

REPLAY

THE NEW
YAHOO.COM

DO YOU YAHOO!?

MAKE IT YOUR
HOME PAGE



PCWorld

Personal Data on 17,000 Pfizer Employees Exposed

A Pfizer employee has exposed Social Security numbers and other personal data belonging to about 17,000 employees.

Jaikumar Vijayan, Computerworld

Tuesday, June 12, 2007 03:00 PM PDT

A Pfizer Inc. employee who installed unauthorized file-sharing software on a company laptop provided for use at her home has exposed the Social Security numbers and other personal data belonging to about 17,000 current and former employees at the drug maker.

Of that group, about 15,700 individuals actually had their data accessed and copied by an unknown number of persons on a peer-to-peer network, the company said in letters sent to affected employees and to state attorneys general alerting them of the breach.

Pfizer officials could not be immediately reached for comment. But copies of the letters were posted on several sites, including Pharnalot, a blog covering the pharmaceutical industry.



What Can You Do To Protect Yourself?

- Be VERY careful on social networking sites
 - Facebook
 - MySpace
 - Linked-In
 - Plaxo
- Block Access





Tips on Becoming a Hacker



The Tools

Top 100 Network Security Tools

Nmap Security Scanner

- [Intro](#)
- [Ref Guide](#)
- [Install Guide](#)
- [Download](#)
- [Changelog](#)
- [Docs](#)

Security Lists

- [Nmap Hackers](#)
- [Nmap Dev](#)
- [Bugtraq](#)
- [Full Disclosure](#)
- [Pen Test](#)
- [Basics](#)
- [More](#)

Security Tools

- [Pass crackers](#)
- [Sniffers](#)
- [Vuln Scanners](#)
- [Web scanners](#)
- [Wireless](#)
- [Exploitation](#)
- [Packet crafters](#)
- [More](#)

Site News

Exploit World

Advertising

About/Contact

Credits

Sponsors:


After the tremendously successful [2000](#) and [2003](#) security tools surveys, [Insecure.Org](#) is delighted to release this 2006 survey. I ([Fyodor](#)) asked users from the [nmap-hackers](#) mailing list to share their favorite tools, and 3,243 people responded. This allowed me to expand the list to 100 tools, and even subdivide them into categories. Anyone in the security field would be well advised to go over the list and investigate tools they are unfamiliar with. I discovered several powerful new tools this way. I also point newbies to this site whenever they write me saying "I don't know where to start".


Respondents were allowed to list open source or commercial tools on any platform. Commercial tools are noted as such in the list below. No votes for the [Nmap Security Scanner](#) were counted because the survey was taken on a Nmap mailing list. This audience also biases the list slightly toward "attack" hacking tools rather than defensive ones.


Each tool is described by one ore more attributes:


NEW! Did not appear on the [2003 list](#)


↑/↓ Popularity ranking **↑rose** / **↓fell** the given number since the [2003 survey](#)

 Generally costs money. A free limited/demo/trial version may be available.


 Works natively on Linux

 Works natively on OpenBSD, FreeBSD, Solaris, and/or other UNIX variants

 Works natively on Apple Mac OS X

 Works natively on Microsoft Windows

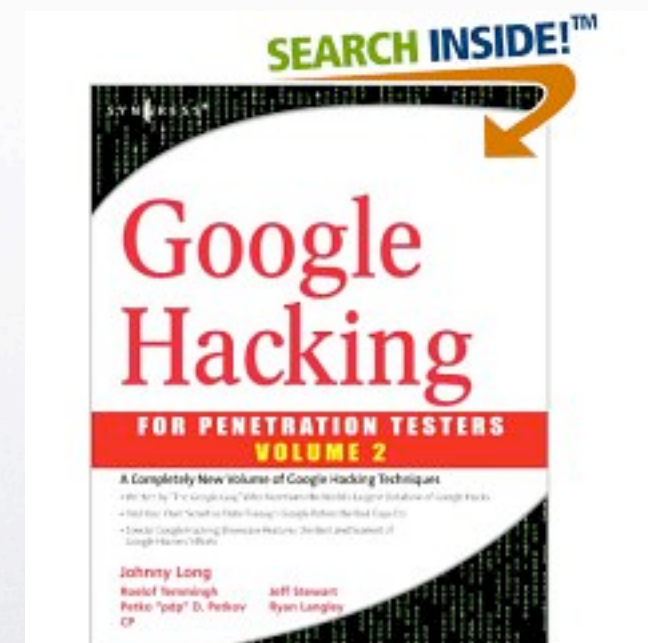
 Features a command-line interface

 Offers a GUI (point and click) interface



Where to Get the Tools

- sectools.org (The Top 100 Tools)
- www.wardrive.net/wardriving/tools (14 Printed Pages of Software....Mostly Free)
- www.google.com





[About](#) | [Location](#) | [Call For Papers](#) | [Registration](#) | [Contests](#) | [Hacker Arcade](#) | [Labs](#) | [Sponsors](#) | [Past Events](#)

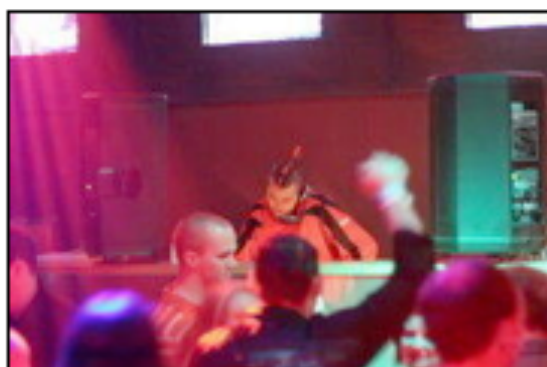
Latest News

2007-11-01 20:36:36 : Ticket Sales Continued...

Tickets were pretty much gone in the first 2-3 hours. At the time of this post, there are only 6 "I Love Shmooscon" tickets left. Thanks to everyone who purchased. The next round of ticket sales will be Noon on December 1st. Yes. Noon.

Watch this space for updates on speaker selection, shmooscon labs and more.

Thanks again!



If our entertainment isn't enough, the 100+ .gov or Beltway Bandit wireless networks within 5 miles could make for some ... fun.







(hack at your own risk... :P)



Hacker Resources on iTunes (For FREE!!)

PODCASTS

1-9 of 9

	DEFCON 14: [Video] Speeches ... The Dark Tangent Category: Training Free SUBSCRIBE		DEFCON 13: [Video] Speakers f... The Dark Tangent Category: Software How-To Free SUBSCRIBE
	DEFCON 13: [Audio] Speakers f... The Dark Tangent Category: Software How-To Free SUBSCRIBE		Defcon 12: [Video] Speakers fr... The Dark Tangent Category: Software How-To Free SUBSCRIBE
	DEFCON 13: [Music Videos] DJ... The Dark Tangent Category: Music Free SUBSCRIBE		DEFCON 12: [Music] DJs and B... The Dark Tangent Category: Music Free SUBSCRIBE



Hacker Resources on iTunes (For FREE!!)

PODCAST DESCRIPTION

Name	Time
Jon Callas and Panel: Traffic Analysis	53:56
Broward Horne: MEME Hacking	48:38
Robert Clark: Legal Aspects of Internet & Computer Network Defense	1:15:51
Dark Tangent: Award Ceremonies	1:50:24
Joe Grand: Hardware Hacking	39:29
Thomas X. Grasso: Fighting Organized Cyber Crime: War Stories an...	51:29
Atlas: The Making of atlas: Kiddie to Hacker in 5 Sleepless Nights	47:43
Greg Conti: Googling: I'm Feeling (un)Lucky	42:01
Paul Simmonds: The Jericho Forum and Challenge	40:55
Matt Hargett: Remote Pair Programming and Test-driven Developm...	47:50
Renderman: New Wireless Fun From the Church Of WiFi	42:58
Richard Thieme: Beyond Social Engineering: Tools for Reinventing ...	53:24
Panel: Panel: Internet Wars 2006	1:42:02
Rick Hill: WarRocketing :Network Stumbling 50 sq. miles in <60 sec.	37:19
Bruce Potter: Trusted Computing: Could it be... SATAN?	51:15
Valsmith: Hacking Malware: Offense Is the New Defense	44:07
Collin Mulliner: Advanced Attacks Against PocketPC Phones	43:43



Hacker Resources on iTunes (For FREE!!)

PODCAST DESCRIPTION

Name	Time
Scott Moulton: Rebuilding HARD DRIVES for Data Recovery; Anatom...	41:54
Major Malfunction: Old Skewl Hacking: Magstripe Madness	48:59
Thomas Holt: Exploring the Changing Nature of DEFCON over the P...	50:24
Johnny Long: Death By 1000 cuts	53:29
Strom Carlson: Hacking FedEx Kinko's: How Not To Implement Stor...	47:15
Robert Clark: Legal Aspects of Internet & Computer Network Defen...	52:34
Amber Schroader: Cyber-crime Foiled Once Again? Help prove the i...	47:26
EFF: Panel: Ask EFF: The Year in Digital Civil Liberties	52:40
Chris Paget: US-VISIT: Raping Personal Privacy Since 2004	50:40
Scott Miller: A New Bioinformatics-Inspired and Binary Analysis: Co...	41:13
Teli Brown: Phishing, it starts with "Ph" for a reason."Some best pra...	26:55
Timothy M O'Neill: 'What has the NSA done for me lately?'	23:31
Charles Edge: 10 Ways To Not Get Caught Hacking On Your Mac	20:57
Melanie Rieback: A Hacker's Guide to RFID Spoofing and Jamming	50:07
James Christy: PANEL: Meet the Feds: 'OODA Loop and the Science ...	51:55
Jay Beale: Discovering Mac OS X Weaknesses and Fixing Them with ...	57:23
Lukas Grunwald: First We Break Your Tag, Then We Break Your Syst...	42:09



What Can I Do to Protect My Infrastructure?



We need to start plugging the leaks!





Disclosure Events

- It's NOT if, but When you have a disclosure event
- You have already had a breach/disclosure event
- Kentucky Retirement Systems adopted a policy in 2006
- 42 States plus DC have legislation
- Federal breach legislation pending



www.privacyrights.org

Privacy Rights CLEARINGHOUSE

Nonprofit Consumer Information
and Advocacy Organization

Consumers | Reporters & Media | Legislators & Policymakers

Home
Alerts & New Info
Fact Sheets -- English
-- En Español
FAQ & Index
Identity Theft
Background Checks &
Workplace
Financial Privacy
Internet Privacy
Medical Records

Privacy Compilations on Our Web Site

- [Privacy Today](#) — A summary of the top privacy issues of our time.
- [A Chronology of Data Breaches](#) — Over 226 million data records of U.S. residents have been exposed due to security breaches since Jan 05.
- [Online Data Brokers](#) — Our greatly expanded listing is now available. Learn which information brokers do -- and do not -- allow you to opt-out.

DONATE NOW
SECURE DONATIONS
BY GROUNDSPRING.org

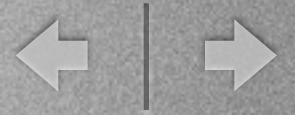


Search



Things You Need to Know

- The threats are constantly changing
- That something bad is going to happen to your technology infrastructure
- That **you** are a **target**
- Today's hackers are smart; Most have significantly more time to spend attacking than your system administrator has to protect your systems



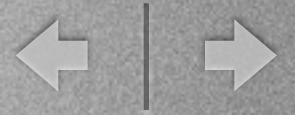
Prepare

- Plan for the best – prepare for the worst
- When it happens, don't be caught saying, "What do we do now?" In the end,
 - You will have a data disclosure,
 - A worm or virus will affect you,
 - A hacker will find you or,
 - A trusted **Insider** will take advantage of you



Educate

- Education starts at the top and works its way down the food chain throughout your organization
- Security is a business practice, NOT an IT responsibility
- Before any employee puts fingers on the keyboard they must understand that it is not their computer
- Have regular training and awareness (Presentation, posters, emails, security alerts, newsletters, etc.)



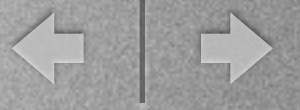
Communicate

- Inform your employees and management team about enterprise policies
- Facilitate your own policies based on best practices
- Make sure you have a disclosure policy and/or incident reporting policy
- Make sure your Executive and Legal staff are involved at every step
- Be timely; Be honest: A forensic review will betray you



Maybe Most Important: Share and Collaborate

- United States Secret Service/Kentucky Electronic Crimes Task Force
- National Association of State Technology Directors (NASTD)
- National Association of State Chief Information Officers (NASCIO)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)



Questions?