

The 2011 “Tour of Cyber Crimes”

Joe St Sauver, Ph.D. (joe@uoregon.edu)

Room 142, Knight Law School

University of Oregon

6:00-7:50PM, January 18th, 2011

<http://pages.uoregon.edu/joe/cybercrime2011/>

Disclaimer: All opinions strictly my own.

Format and Disclaimer

- Sean told me to plan on having about an hour to talk, which for me generally means building roughly 120 slides. If that sounds like a lot, relax! When Sean tells me I'm out of time, I **will** stop. I won't run us late!
- Even though my slides may appear visually dense, I also promise I'm not going to read from them – they're really just meant to:
 - keep me on track,
 - free you from the need to take notes as we cover this material,
 - give you links to items for further study (if you're interested),
 - help any of your classmates who may not be able to be here with us tonight,
 - improve the accessibility of this material for those of you who may be hearing impaired (I know I sometimes talk too fast, or some of you may think I have a funny accent)
- While I'd prefer to have this be a seminar-style dialog, since I don't know your backgrounds I've built this session as a lecture, but you should feel free to jump in and ask any questions you have as they come up.
- As mentioned on the title slide, all opinions expressed are solely my own.
- Before we dive in, though, **is cybercrime really a national LE priority?** 2

FBI 2011 Budgetary Priorities

- “To address current and emerging national security threats, the FY 2011 budget proposes additional funding for:

Counterterrorism and Counterintelligence Investigations and Operations: 90 new positions (27 special agents, 32 IAs [IA==Intelligence Analysts], and 31 professional staff) and \$25.2 million to enhance surveillance and investigative capabilities, improve intelligence collection and analysis capabilities, and enhance the Bureau’s legal attaché presence in Pakistan and Ethiopia.

Computer Intrusions: 163 new positions (63 special agents, 46 IAs, and 54 professional staff) and \$45.9 million for the Comprehensive National Cybersecurity Initiative to continue the enhancement of the FBI’s capacities for combating cyber attacks against the U.S. information infrastructure.

Weapons of Mass Destruction: 35 positions (15 special agents and 20 professional staff) and \$9.1 million to develop further the FBI’s capacity to implement countermeasures aimed at detecting and preventing a WMD incident, improve the capacity to provide a rapid response to incidents, and enhance capacities to collect and analyze WMD materials, technology, and information.

Render Safe: 13 new positions (six special agents and seven professional staff) and \$40 million to acquire necessary replacement aircraft critical to the timely deployment and response of specialized render safe assets.”

- “To address current and emerging crime problems and threats, the FY 2011 budget requests additional funding for:

White Collar Crime: 367 new positions (143 special agents, 39 IAs, and 185 professional staff) and \$75.3 million to address increasing mortgage, corporate, and securities and commodities fraud schemes, including a backlog of over 800 mortgage fraud cases with over \$1 million in losses per case.

Child Exploitation: 20 new positions (four special agents, one IA, and 15 professional staff) and \$10.8 million to enhance ongoing Innocence Lost, child sex tourism, and Innocent Images initiatives.

Organized Crime: four new positions (three special agents and one professional staff) and \$952,000 to establish, in partnership with the Criminal Division of the Justice Department, a new integrated international organized crime mobile investigative team to focus on combating illicit money networks and professional money laundering.

Violent Crime/Gangs and Indian Country: two new positions and \$328,000 to provide enhanced forensic services for Indian Country investigations. Additionally, \$19 million is requested as a reimbursable program through the Department of the Interior to hire an additional 45 special agents and 36 professional staff to investigate violent crimes in Indian Country.”

See: “Statement Before the House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies Washington, DC March 17, 2010,
<http://www.fbi.gov/news/testimony/the-fbi-budget-for-fiscal-year-2011>

A Cyber Crime Taxonomy: Sorting Through a Big Pile of Badness

- When it comes to looking at a topic as broad as cyber crime, it's helpful to have some structure. For me, the organization that makes the most sense is:
 1. "Classic" Cybercrimes: Focus Is On the Hardware/Network Itself
 2. Internet Fraud: Crimes of Deception
 3. Content/Substance-Oriented Online Crimes
- That list should catch most of the major cyber crimes that folks are worried about, EXCEPT for cyber war, cyber terrorism, and cyber espionage (all of which I'm defining as being out of scope for this talk except as those areas may incidentally come up in connection with other cyber crimes).

If you're interested in those other areas, feel free to see my October 2008 talk covering those areas at <http://pages.uoregon.edu/joe/cyberwar/cyberwar.pdf>

I'd be happy to stay for a while after tonight's class to informally discuss the content of that presentation if there's interest.

“Why Do You Have So Many Examples of Arrests and Prosecutions and Convictions?”

- As we go through the rest of tonight’s talk together, you may notice many examples of arrests and prosecutions and convictions, and you may wonder why I included them.
- There are several reasons, including:
 - sometimes people believe that cybercrimes just aren’t getting prosecuted; these examples are proof by example to the contrary
 - sometimes people may wonder what *sort* of cybercrimes are getting prosecuted; these examples show you some of the cases which are getting worked by law enforcement
 - it can also be helpful to see how many different agencies are prosecuting cyber crimes, and how long it can take for a case to work it’s way through the system, etc., etc., etc.

**1. "Classic" Cybercrimes:
Focus Is On the Hardware/Network Itself**

1. (a) Theft of Services

- Theft of services is, in many ways, the first "cyber" or "network-oriented" crime (albeit one which was originally committed against a phone network or a cable TV network rather than a modern packet-switched computer network)
- Phone phreaking involved things such as toll fraud, the "creative routing" of calls in non-optimal ways (e.g., call next door, but do so over long distance circuits nailed up literally around the world), and other illegal things that folks weren't supposed to be doing
- Cable TV theft of service typically involved unauthorized reception of basic or premium channel traffic, or the interception of microwave TV signals, w/o payment to the TV company
- Some of these crimes, or their Internet analogs, continue today, although the world is a vastly different place now, and most theft-of-service crimes have evolved over time...

Folks Know What This Is/What It Was Used For? Or Who (Allegedly) Used to Own It?



Source: [http://en.wikipedia.org/wiki/Blue_box_\(phreaking\)](http://en.wikipedia.org/wiki/Blue_box_(phreaking))

“Colored Boxes” and Other Phone Tech

- **Blue box:** emitted a 2600Hz in-band signal that the call had ended, after which additional in-band signals could be sent to make calls which wouldn't be charged
- **Red box:** faked the sound of coins being deposited in a payphone
- **Green box:** generated coin collect, coin return and ringback tones for payphones
- **Black box:** prevents call-has-been-answered detection
- **Silver box:** this device generates “flash,” “flash override priority,” “priority communication” and “priority override (top military)” signaling tones, although those tones were not officially used.
- **War dialers:** these would systematically call all lines in a given telephone prefix, typically looking for lines with dial in modems

Source: “Steal This Computer Book 4.0,” Wally Wang, 2006.
See also http://en.wikipedia.org/wiki/Phreaking_Boxes

Satellite TV

http://www.usdoj.gov/criminal/cybercrime/OPdecrypt_walterPlea.htm

BBC News

Operation Decrypt Leads to Charges Against 17 For Developing Technology Used to Steal Millions of Dollars Worth of Satellite TV Six Defendants Charged Under Digital Millennium Copyright Act

In an FBI undercover investigation that targeted the software writers and manufacturers behind equipment that allows the theft of satellite television signals, 17 people have been charged in Los Angeles with causing millions of dollars of losses to companies that have spent tens of millions of dollars creating some of the world's most sophisticated conditional access technology.

Six of the charged defendants are accused of violating the criminal anti-decryption provisions of the Digital Millennium Copyright Act. These charges represent the first time the DMCA has been used in this district and only the second time in the nation that a grand jury has issued an indictment under this statute.

After five of the defendants were taken into custody this morning, federal authorities announced that the year-long investigation dubbed Operation Decrypt has led to charges against high-level computer hackers who work together in underground, online communities to develop technology to steal satellite programming. The announcement was made at a press conference this morning by United States Attorney Debra W. Yang and FBI Assistant Director Ronald Iden.

This case demonstrates our commitment to identifying and prosecuting sophisticated computer hackers who steal the intellectual property of others for their own economic benefit, said United States Attorney Yang. No matter how sophisticated the criminals are, we will uncover the devices they create and the strategies they use to steal the lifeblood of the business community.

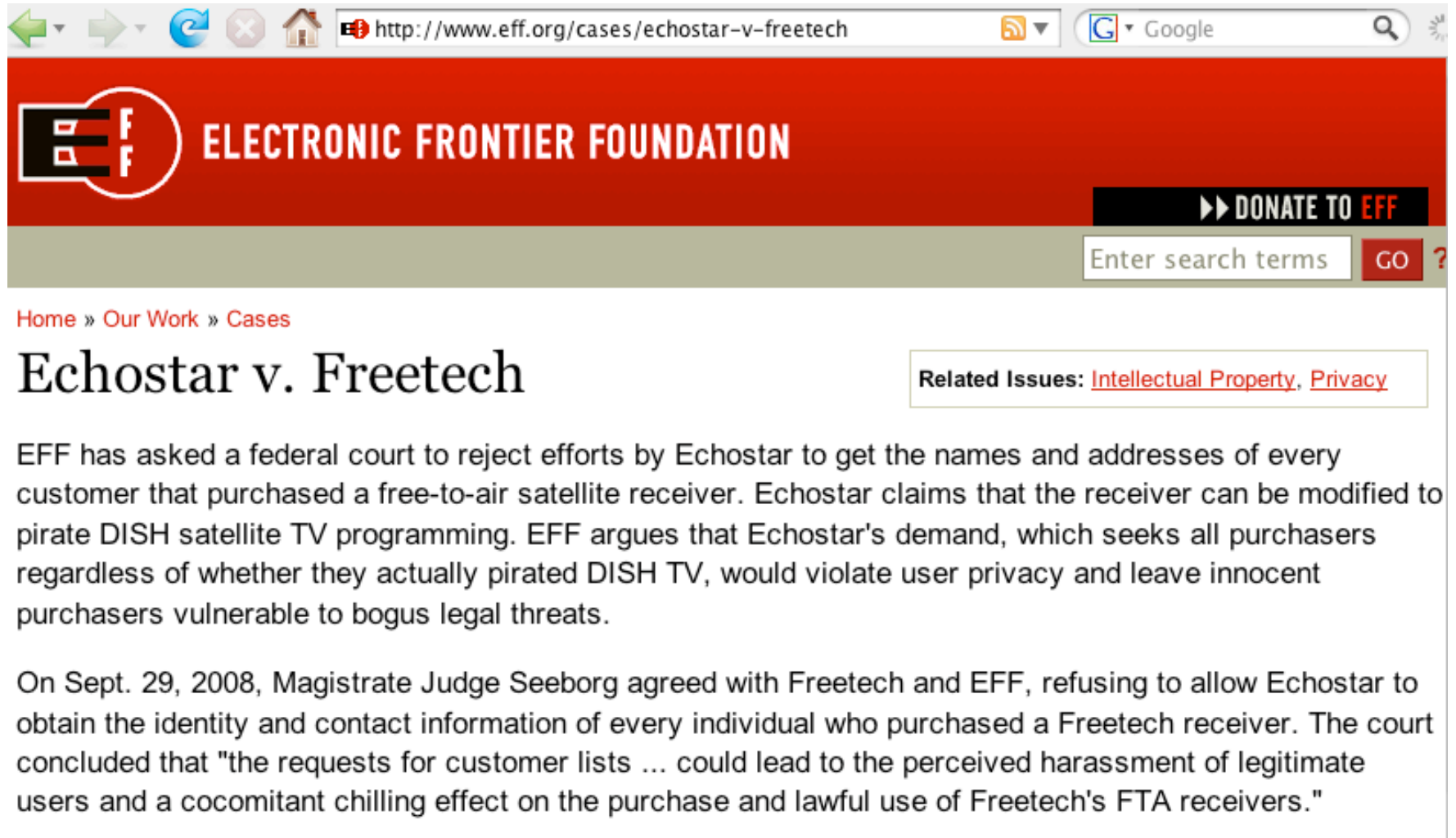
FBI Assistant Director Iden stated: Cybercrime is one of the top priorities of the FBI. We will continue to devote considerable resources to remain a potent deterrent in this changing world.

The victims of the hackers and hardware distributors are satellite programming providers such as DirecTV and DISH Network, companies that lose millions of dollars every year from satellite signal piracy. Additionally, members of the Motion Picture Association of America lose millions of dollars every year in unpaid royalties when satellite programming is stolen.

In an illustration of the scope of the problem, one defendant already has pleaded guilty and admitted that he was responsible for losses of nearly \$15 million. Another nine defendants have agreed to plead guilty to charges based on conduct that also caused significant losses. Six of the remaining defendants have been named in four indictments that were returned by a federal grand jury in Los Angeles last month and unsealed this morning. One additional defendant has been charged in a criminal complaint.

Operation Decrypt shed light on the normally hidden world of computer hackers who use secret online chat rooms to exchange data and techniques to

Free-To-Air Satellite Receivers



The screenshot shows a web browser window with the address bar displaying <http://www.eff.org/cases/echostar-v-freetech>. The browser's toolbar includes navigation buttons (back, forward, home, stop, reload) and a search bar with the Google logo. The website header is red with the EFF logo (a stylized 'E' and 'F' inside a circle) and the text "ELECTRONIC FRONTIER FOUNDATION". To the right of the header is a black button with white text that says "DONATE TO EFF". Below the header is a search bar with the placeholder text "Enter search terms" and a red "GO" button. The main content area has a breadcrumb trail: "Home » Our Work » Cases". The title of the page is "Echostar v. Freetech". To the right of the title is a box labeled "Related Issues:" containing links to "Intellectual Property" and "Privacy". The main text of the page describes the legal case: "EFF has asked a federal court to reject efforts by Echostar to get the names and addresses of every customer that purchased a free-to-air satellite receiver. Echostar claims that the receiver can be modified to pirate DISH satellite TV programming. EFF argues that Echostar's demand, which seeks all purchasers regardless of whether they actually pirated DISH TV, would violate user privacy and leave innocent purchasers vulnerable to bogus legal threats." Below this is a paragraph about the court's decision: "On Sept. 29, 2008, Magistrate Judge Seeborg agreed with Freetech and EFF, refusing to allow Echostar to obtain the identity and contact information of every individual who purchased a Freetech receiver. The court concluded that 'the requests for customer lists ... could lead to the perceived harassment of legitimate users and a concomitant chilling effect on the purchase and lawful use of Freetech's FTA receivers.'"

Home » Our Work » Cases

Echostar v. Freetech

Related Issues: [Intellectual Property](#), [Privacy](#)

EFF has asked a federal court to reject efforts by Echostar to get the names and addresses of every customer that purchased a free-to-air satellite receiver. Echostar claims that the receiver can be modified to pirate DISH satellite TV programming. EFF argues that Echostar's demand, which seeks all purchasers regardless of whether they actually pirated DISH TV, would violate user privacy and leave innocent purchasers vulnerable to bogus legal threats.

On Sept. 29, 2008, Magistrate Judge Seeborg agreed with Freetech and EFF, refusing to allow Echostar to obtain the identity and contact information of every individual who purchased a Freetech receiver. The court concluded that "the requests for customer lists ... could lead to the perceived harassment of legitimate users and a concomitant chilling effect on the purchase and lawful use of Freetech's FTA receivers."

An Extreme Example of “FTA Video” Reception

http://www.wired.com/dangerroom/tag/dyi

Insurgents Intercept Drone Video in King-Size Security Breach (Updated, with Video)

By Noah Shachtman December 17, 2009 | 10:15 am | Categories: Drones



In Iraq and Afghanistan, the U.S. military depends on an array of drones to snoop on and stalk insurgents. Now it looks as if insurgents are tapping into those same drones' broadcasts, to see what the flying robot spies see. If true — and widespread — it's potentially one of the most serious military security breaches in years.

"U.S. military personnel in Iraq discovered the problem late last year when they [apprehended a Shiite militant whose laptop contained files of intercepted drone video feeds](#)," *Wall Street Journal* reports. "In July, the U.S. military found pirated drone video feeds on other militant laptops, leading some officials to conclude that militant groups trained and funded by Iran were regularly intercepting feeds."

How'd the militants manage to get access to such secret data? Basically by [pointing satellite dishes up](#), and waiting for the drone feeds to pour in. According to the *Journal*, militants have exploited a weakness: The data links

A Particular Type of "Theft of Services:" Computer Intrusions

- You don't tend to hear much about "theft of services" anymore when it comes to computer and network cybercrime, in part because there are now specific statutes relating to:
 - access device fraud (covering things such as unlawful possession and use of computer passwords, credit and debit cards, ATM cards and PINs, long-distance access codes, cell phone SIMs, satellite TV encryption devices, etc.), as well as
 - specific computer intrusion laws which tend to dominate more general "theft of service" laws.
- In any event, let's briefly consider computer intrusions next.

1. (b) Oregon's Computer Intrusion Law

O.R.S. 164.377 (see also 18 USC 1030 for the Federal computer crime statute):

(2) Any person commits computer crime who knowingly accesses, attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof for the purpose of:

(a) Devising or executing any scheme or artifice to defraud;

(b) Obtaining money, property or services by means of false or fraudulent pretenses, representations or promises; or

(c) Committing theft, including, but not limited to, theft of proprietary information. [* * *]

(4) Any person who knowingly and without authorization uses, accesses or attempts to access any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime.

(5)(a) A violation of the provisions of subsection (2) or (3) of this section shall be a Class C felony. Except as provided in paragraph (b) of this subsection, a violation of the provisions of subsection (4) of this section shall be a Class A misdemeanor.

Sample “Old School” Intrusion With Defacement

Tumwater, Washington Man Indicted in Connection with Comcast Hacking Defendant and Two Others Accused of Disrupting Comcast Service in May 2008

JAMES ROBERT BLACK, JR., a.k.a. ‘Defiant’, 20, of Tumwater, Washington will make his initial appearance in U.S. District Court in Tacoma tomorrow, November 24, 2009, on an indictment from the Eastern District of Pennsylvania.

BLACK is charged with conspiring to disrupt service at Comcast Corporation’s www.comcast.net website on May 28 and 29, 2008. BLACK will appear before U.S. Magistrate Judge J. Richard Creatura at 2:30 tomorrow. BLACK is charged in the conspiracy along with CHRISTOPHER ALLEN LEWIS, a.k.a. EBK, 19, of Newark, Delaware, and MICHAEL PAUL NEBEL, a.k.a. Slacker, 27, of Kalamazoo, Michigan. The three were associated with the hacker group Kryogeniks. The indictment charges that on May 28, 2008, LEWIS, BLACK, and NEBEL used their hacking skills to redirect all traffic destined for the www.comcast.net website to websites that they had established. As a result, Comcast customers trying to read their e-mail or listen to their voice mail were sent to a website on which the only thing that they could find was a message that read “KRYOGENIKS Defiant and EBK RoXed COMCAST sHouTz to VIRUS Warlock elul21 coll1er seven.” [...]

If convicted each defendant faces a maximum possible sentence of 5 years imprisonment, a \$250,000 fine, a \$100 special assessment, and up to 3 years of supervised release following any imprisonment. In addition, the court could order the defendants to pay restitution.

Who Commits Cyber Intrusions?

- Traditional journalism-speak answer: "hackers"
- Note: journalists really should be saying *crackers*, not *hackers*, but we both understand the casual/popular misuse of the "hacker" term instead of the more strictly correct "cracker" nomenclature.
- Some more specific possible answers to the question of "Who commits cyber intrusions?" might be...
 - The financially motivated
 - Disgruntled/untrustworthy (former) insiders
 - Juveniles
 - Ideologically motivated individuals
 - Sophisticated professionals
- Examples of what I mean by those sort of perpetrators...



Department of Justice

FOR IMMEDIATE RELEASE
TUESDAY, DECEMBER 29, 2009
WWW.JUSTICE.GOV

CRM
(202) 514-2008
TDD (202) 514-1888

MAJOR INTERNATIONAL HACKER PLEADS GUILTY FOR MASSIVE ATTACK ON U.S. RETAIL AND BANKING NETWORKS

WASHINGTON- Albert Gonzalez, 28, of Miami, pleaded guilty today to conspiring to hack into computer networks supporting major American retail and financial organizations, and to steal data relating to tens of millions of credit and debit cards, announced Assistant Attorney General of the Criminal Division Lanny A. Breuer, U.S. Attorney for the District of New Jersey Paul J. Fishman, U.S. Attorney for the District of Massachusetts Carmen Milagros Ortiz and Director of the U.S. Secret Service Mark Sullivan.

Gonzalez, aka "segvec," "soupnazi" and "j4guar17," pleaded guilty to two counts of conspiracy to gain unauthorized access to the payment card networks operated by, among others, Heartland Payment Systems, a New Jersey-based card processor; 7-Eleven, a Texas-based nationwide convenience store chain; and Hannaford Brothers Co. Inc., a Maine-based supermarket chain. The plea was entered in federal court in Boston before U.S. District Court Judge Douglas P. Woodlock. The case is one of the largest data breaches ever investigated and prosecuted in the United States.

According to information contained in the plea agreement, Gonzalez leased or otherwise controlled several servers, or "hacking platforms," and gave access to these servers to other hackers, knowing that they would use them to store malicious software, or "malware," and launch attacks against corporate victims. Malware used against several of the corporate victims was also found on a server controlled by Gonzalez. Gonzalez tested malware by running multiple anti-virus programs in an attempt to ascertain if the programs detected the malware. According to information in the plea agreement, it was foreseeable to Gonzalez that his co-conspirators would use malware to steal tens of millions of credit and debit card numbers, affecting more than 250 financial institutions. Gonzalez was indicted in New Jersey in August 2009 for this criminal conduct.

Based on the terms of the plea agreement, Gonzalez will not seek a prison term under 17 years and the government will not seek a prison term of more than 25 years. Gonzalez pleaded guilty in September 2009 in Boston to 19 counts of conspiracy, computer fraud, wire fraud, access device fraud and aggravated identity theft relating to hacks into numerous major U.S. retailers including TJX

Former Insider



NEWS RELEASE

For Immediate Distribution

December 18, 2007

Thomas P. O'Brien

United States Attorney
Central District of California

Thom Mrozek, Public Affairs Officer
(213) 894-6947

thom.mrozek@usdoj.gov
www.usdoj.gov/usao/cac

L.A. COUNTY MAN PLEADS GUILTY TO HACKING INTO HOTEL BUSINESS KIOSKS AND STEALING CREDIT CARD INFORMATION

A Lomita man pleaded guilty this afternoon to federal charges stemming from his hacking into business kiosks at hotels and stealing credit card information.

Hario Tandiwidjojo, 28, pleaded guilty to one count of unauthorized access to a protected computer to conduct fraud.

In a plea agreement filed in United States District Court, Tandiwidjojo admitted that he hacked into approximately 60 computers inside business kiosks operated by Showcase Business Centers, Inc. Tandiwidjojo bypassed four password checks that Showcase Business Centers had in place on their computers, using passwords he obtained while employed by a company that serviced the business

Juvenile

Juvenile Computer Hacker Sentenced to Six Months in Detention Facility

Case marks first time a juvenile hacker sentenced to serve time

WASHINGTON, D.C. - The Justice Department announced today that a 16-year-old from Miami has pleaded guilty and been sentenced to six months in a detention facility for two acts of juvenile delinquency. Under adult statutes, those acts would have been violations of federal wiretap and computer abuse laws for intercepting electronic communications on military computer networks and for illegally obtaining information from NASA computer networks.

"Breaking into someone else's property, whether it is a robbery or a computer intrusion, is a serious crime," said Attorney General Janet Reno. "This case, which marks the first time a juvenile hacker will serve time in a detention facility, shows that we take computer intrusion seriously and are working with our law enforcement partners to aggressively fight this problem."

The juvenile, whose is known on the Internet as "c0mrade," admitted today in U.S. District Court in Miami that he was responsible for computer intrusions from August 23, 1999, to October 27, 1999, into a military computer network used by the Defense Threat Reduction Agency (DTRA). DTRA is an agency of the Department of Defense charged with reducing the threat to the U.S. and its allies from nuclear, biological, chemical, conventional and special weapons.

In pleading guilty, "c0mrade" also admitted that he gained unauthorized access to a computer server, known as a "router," located in Dulles, Va., and installed a concealed means of access or "backdoor" on the server. The program intercepted more than 3,300 electronic messages to and from DTRA staff. It also intercepted at least 19 user names and passwords of computer accounts of DTRA employees, including at least 10 user names and passwords on military computers.

"The Department of Defense takes seriously any threats against its information infrastructure," said Joseph A. McMillan, Special Agent in Charge of the DOD Mid Atlantic Field Office. "Any segments of society, be them adults or juveniles, which are intent on threatening DOD's information infrastructure, should be aware that steps will be taken to identify and thoroughly investigate their activities and seek the necessary judicial actions."

In addition to the computer intrusions at DOD, on June 29 and 30, 1999, "c0mrade" illegally accessed a total of 13 NASA computers located at the Marshall Space Flight Center, Huntsville, Ala., using two different ISPs to originate the attacks. As part of his unauthorized access, he obtained and downloaded proprietary software from NASA valued at approximately \$1.7 million. The software supported the International Space Station's (ISS) physical environment, including control of the temperature and humidity within the living space.

As a result of the intrusions and data theft, the NASA computer systems were shut down for 21 days in July 1999. This shutdown resulted in a delivery delay of program software costing NASA approximately \$41,000 in contractor labor and computer equipment replacement costs.

And An Ideologically Motivated Example



<http://www.israelnationalnews.com/News/News.aspx/124768>

Published: 01/01/08, 10:09 AM

Arab Israeli Arrested for Cyber-Sabotage of Israeli Websites

by Nissan Ratzlav-Katz

(IsraelINN.com) Police have arrested a 17-year-old Israeli Arab for involvement in an international group of hackers that targeted Israeli websites for cyber-vandalism. In 2006, the hackers managed to shut down about 750 Israeli websites and their attacks have caused millions of shekels in damage.

The group, calling itself "Team-Evil", apparently includes hackers in Saudi Arabia, Lebanon, Turkey, and other Muslim countries.

Three main networks from which the virtual terrorism originated were found to have been located in Saudi Arabia, and police suspect that other Arabs with Israeli citizenship are involved, as well.

The Israeli youth arrested in recent days was apprehended after an 18-month investigation. The young man's mother attempted to hide his personal computer when police arrived at the house, but the computer was found, and investigators found additional evidence of the teen's criminal activity. He will be charged with several serious computer-related crimes.

In June of 2006, around 750 Israeli websites were hacked in one day in a coordinated campaign. The sites were taken down and replaced with a screen displaying the message: "Hacked by Team-Evil Arab hackers u KILL palestin people we KILL Israeli servers." Among the targeted sites were those of Bank Hapoalim, a Haifa-area hospital, the Israeli representatives of international car manufacturers BMW, Subaru and Citroen, and of the Kadima party. Most of the



The hackers managed to shut down about 750 Israeli websites.



Example of Sophisticated Professionals

October 20, 2005 (Computerworld) -- At the moment, there's a dirty little secret that only a few people in the information security world seem to be privileged to know about, or at least take seriously. Computers around the world are systematically being victimized by rampant hacking. This hacking is not only widespread, but is being executed so flawlessly that the attackers compromise a system, steal everything of value and completely erase their tracks within 20 minutes.

When you read this, it almost sounds like the plot of a cheesy science fiction novel, where some evil uberhacker is seeking world domination, while a good uberhacker applies all his super brain power to save the world. Sadly, this isn't science fiction, and we don't typically have uberhackers on our side.

Talk of these hacks is going on within the intelligence and defense communities in the U.S. and around the world. The attacks were even given a code name, **Titan Rain**, within the U.S. government. The attackers appear to be targeting systems with military and secret information of any type. [* * *]

<http://www.computerworld.com/securitytopics/security/story/0,10801,105585,00.html> [emphasis added]

RELATED KEYWORDS

- Internet (computer Network)
- Business
- Security
- China
- Computer Crime

RELATED ARTICLES

Google may leave China in wake of hacker attacks
January 13, 2010

Cyber-Crime Loss at Firms Doubles to \$10 Billion
March 22, 2000

Scaling the heights
November 17, 2006

Chinese hackers pose a growing threat to U.S. firms

Escalating cyber attacks on Google and other companies alarm government officials who say the U.S. may be powerless to stop the online industrial espionage.

January 15, 2010 | By Jessica Guynn

The scale and sophistication of the cyber attacks on Google Inc. and other large U.S. corporations by hackers in China is raising national security concerns that the Asian superpower is escalating its industrial espionage efforts on the Internet.

While the U.S. focus has been primarily on protecting military and state secrets from cyber spying, a new battle is being waged in which corporate computers and the valuable intellectual property they hold have become as much a target of foreign governments as those run by the Pentagon and the CIA.

Advertisement

"This is a watershed moment in the cyber war," James Mulvenon, director of the Center for Intelligence Research and Analysis at Defense Group Inc., a national-security firm, said Thursday. "Before, the Chinese were going after defense targets to modernize the country's military machine. But these intrusions strike at the heart of the American innovation community."

The attacks on Google and several dozen other companies have alarmed government officials and lawmakers who warned that the U.S. may already be losing the battle to protect the nation's besieged cyber infrastructure.

"The recent cyber intrusion that Google attributes to China is troubling and the U.S. government is looking into it," White House spokesman Nick Shapiro said Thursday.

Cyber Intrusions and Weak Passwords

  <http://www.news.com/2009-1001-916719.html>

Passwords: the weakest link?

NEWS.COM SPECIAL REPORT

Hackers can crack most in less than a minute

By [Rob Lemos](#)

Staff Writer, CNET News.com

May 22, 2002, 4:00 a.m. PT

When a regional health care company called in network protection firm Neohapsis to find the vulnerabilities in its systems, the Chicago-based security company knew a sure place to look.

Retrieving the password file from one of the health care company's servers, the consulting firm put "John the Ripper," a well-known cracking program, on the case. While well-chosen passwords could take years--if not decades--of computer time to crack, it took the program only an hour to decipher 30 percent of the passwords for the nearly 10,000 accounts listed in the file.


But Heck, You Don't Even Need to Try Technical Approaches in Many Cases

"[...] some managers and employees are still susceptible to social engineering techniques. Similar to our tests in 2001, we placed telephone calls to **100 IRS employees**, including managers. We posed as Information Technology (IT) helpdesk personnel who were seeking assistance to correct a network problem. Under this scenario, we asked employees to provide their network logon name and temporarily change their password to one we suggested. **We were able to convince 35 managers and employees to provide us their username and to change their password.** While our results represented about a 50 percent improvement over the previous test conducted in 2001 (see Figure 1), the noncompliance rate suggests additional emphasis or awareness is needed."

<http://treas.gov/tigta/auditreports/2005reports/200520042fr.pdf>

What about two factor authentication, combining something you know (like a conventional password), with something you have (like a hardware cryptographic token)? Surely THAT would eliminate password-based cyber intrusions -- wouldn't it?

Sample Two Factor Hardware Crypto Fob



Secured by **RSA**

E*TRADE FINANCIAL already maintains the highest levels of security available, including 128-bit encryption on our Web site.

Now, with the addition of our new **E*TRADE Complete™ Digital Security ID¹**, you can get an extra level of security that makes unauthorized log-on virtually impossible.²

- Receive a keychain-sized device that generates a personal 6-digit access code every 60 seconds
- Use the unique code with your regular User ID and Password to log on to your account(s)
- Keeps out hackers even in the unlikely event that your User ID and Password are compromised

| How to Qualify | Device Cost |
|---|------------------------------|
| 10 or more stock or options trades/month | FREE ³ |
| \$50,000 or more in combined assets | FREE ³ |
| All other brokerage, bank or lending accounts | \$25 one-time fee per device |

To Get Your FREE³ Digital Security ID

ORDER NOW

You will be prompted to log on. Please have your User ID and Password ready.

Forgot your password? [Click here.](#)

This can indeed be an improvement over just passwords. But, what if every online account you have has to be protected by it's own two factor encryption fob? Better buy a good belt or some suspenders! There has also been discussion of some remaining vulnerabilities...



Here are two new active attacks we're starting to see:

- **Man-in-the-Middle attack.** An attacker puts up a fake bank website and entices user to that website. User types in his password, and the attacker in turn uses it to access the bank's real website. Done right, the user will never realize that he isn't at the bank's website. Then the attacker either disconnects the user and makes any fraudulent transactions he wants, or passes along the user's banking transactions while making his own transactions at the same time.
- **Trojan attack.** Attacker gets Trojan installed on user's computer. When user logs into his bank's website, the attacker piggybacks on that session via the Trojan to make any fraudulent transaction he wants.

See how two-factor authentication doesn't solve anything? In the first case, the attacker can pass the ever-changing part of the password to the bank along with the never-changing part. And in the second case, the attacker is relying on the user to log in.

The real threat is fraud due to impersonation, and the tactics of impersonation will change in response to the defenses. Two-factor authentication will force criminals to modify their tactics, that's all.

Recently I've seen examples of two-factor authentication using two different communications paths: call it "two-channel authentication." One bank sends a challenge to the user's cell phone via SMS and expects a reply via SMS. If you assume that all your customers have cell phones, then this results in a two-factor authentication process without extra hardware. And even better, the second authentication piece goes over a different communications channel than the first; eavesdropping is much, much harder.

1. (c) Computer Viruses, Worms, Trojan Horses, Spyware & Other Malware

- **Computer virus:** program which can copy itself and surreptitiously infect another computer, often via shared media such as a floppy disk, CD, thumb drive, shared directory, etc. Viruses are always embedded within another file or program.
- **Worm:** self-reproducing program which propagates via the network.
- **Trojan horse:** program which purports to do one thing, but secretly does something else; example: free screen saver which installs a backdoor
- **Root kit:** set of programs designed to allow an adversary to surreptitiously gain full control of a targeted system while avoiding detection and resisting removal, with the emphasis being on evading detection and removal
- **Botnet:** set of compromised computers ("bots" or "zombies") under the unified command and control of a "botmaster;" commands are sent to bots via a command and control channel (bot commands are often transmitted via IRC, Internet Relay Chat).
- **Spyware:** assorted privacy-invading/browser-perverting programs
- **Malware:** an inclusive term for all of the above -- "malicious software"

Example: David Smith & The Melissa Virus

Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison

The New Jersey man accused of unleashing the “Melissa” computer virus in 1999, causing millions of dollars in damage and infecting untold numbers of computers and computer networks, was sentenced today to 20 months in federal prison, U.S. Attorney Christopher J. Christie and state Attorney General David Samson announced. David L. Smith, 34, of Aberdeen Township in Monmouth County, was ordered to serve three years of supervised release after completion of his prison sentence and was fined \$5,000. U.S. District Judge Joseph A. Greenaway Jr. further ordered that, upon release, Smith not be involved with computer networks, the Internet or Internet bulletin boards unless authorized by the Court. Finally, Judge Greenaway said Smith must serve 100 hours of community service upon release. [* * *] In a cooperating federal plea agreement Smith acknowledged that **the Melissa virus caused more than \$80 million in damage** by disrupting personal computers and computer networks in business and government. [emphasis added]

For Release: October 1, 2007

FTC Permanently Halts Media Motor Spyware Scam

Trojan Program Downloaded Spyware, Adware, Porno Pop-Ups to Consumers' Computers

Operators who infected more than 15 million computers with destructive, intrusive spyware will give up \$330,000 in ill-gotten gains from their venture to settle FTC charges that their scam violated federal law. The settlement will bar the defendants from downloading software onto consumers' computers without disclosing its function and obtaining consumers' consent prior to installation, bars them from downloading software that interferes with consumers' computer use, and bars false or misleading claims.

In November 2006, the FTC charged ERG Ventures, LLC and its principals with tricking consumers into downloading malevolent software by hiding the Media Motor program within seemingly innocuous free software, including screensavers and video files. Once downloaded, the Media Motor program silently activated itself and downloaded "malware" that was intrusive, disruptive, and made it difficult for consumers to use their computers. The software changed consumers' home pages, tracked their Internet activity, altered browser settings, degraded computer performance, and disabled anti-spyware and anti-virus software. Many of the malware programs installed by the Media Motor program were extremely difficult or impossible for consumers to remove from their computers.

The FTC charged that ERG Ventures and its principals violated the FTC Act, which bars unfair and deceptive practices. Specifically, the FTC alleged that the defendants failed to disclose to consumers that the free software they offered was bundled with malware. The agency also charged the defendants with using a deceptive End User License Agreement, which gave consumers the option to

Sale of A Million Pieces of “Scareware”

For Release: December 10, 2008

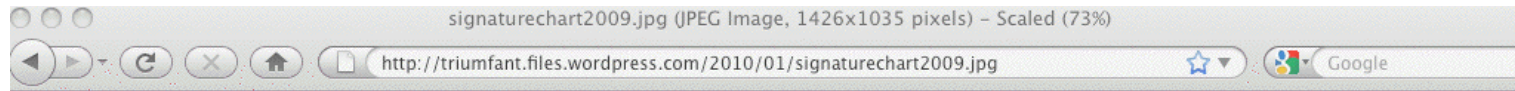
Court Halts Bogus Computer Scans

At the request of the Federal Trade Commission, a U.S. district court has issued a temporary halt to a massive “scareware” scheme, which falsely claimed that scans had detected viruses, spyware, and illegal pornography on consumers’ computers. According to the FTC, the scheme has tricked more than one million consumers into buying computer security products such as WinFixer, WinAntivirus, DriveCleaner, ErrorSafe, and XP Antivirus. The court also froze the assets of those responsible for the scheme, to preserve the possibility of providing consumers with monetary redress.

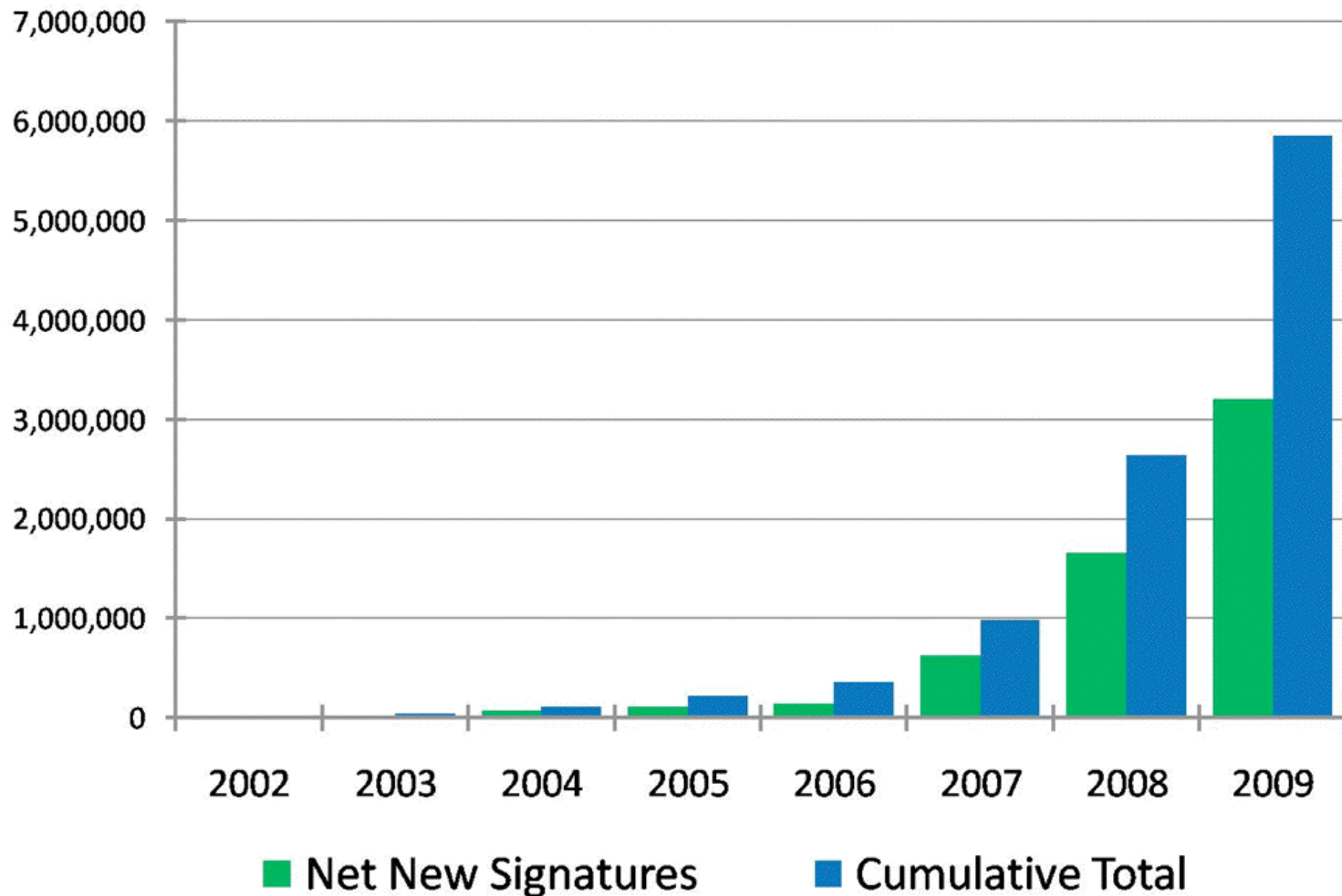
According to the FTC’s complaint, the defendants used an elaborate ruse that duped Internet advertising networks and popular Web sites into carrying their advertisements. The defendants falsely claimed that they were placing Internet advertisements on behalf of legitimate companies and organizations. But due to hidden programming code that the defendants inserted into the advertisements, consumers who visited Web sites where these ads were placed did not receive them. Instead, consumers received exploitive advertisements that took them to one of the defendants’ Web sites. These sites would then claim to scan the consumers’ computers for security and privacy issues. The “scans” would find a host of purported problems with the consumers’ computers and urge them to buy the defendants’ computer security products for \$39.95 or more. However, the scans were entirely false.

<http://www.ftc.gov/opa/2008/12/winsoftware.shtm>

The Pace of Malware Release is Accelerating



Signature Counts By Year



Signature-Based Antivirus Software Is "Struggling" <cough, cough>

- Assume updated antivirus signatures are being released once or maybe twice a day; similarly, let's assume some miscreants are releasing new malware variants every hour (because they are)
- Also assume it takes antivirus companies at least a few hours to collect a sample of any new malware and generate a signature which can detect the new malware variant
- Combining those facts means that there will ALWAYS be a window of time during which at least some new malware will NOT be detected even if you are running the absolute latest antivirus definitions from the best antivirus companies in the business.

Example: "Video Codec" Malware

- If you Google for a sex-related term and limit the returned results to the cn domain (although I wouldn't recommend that you actually do this), it is virtually assured that one or more of the top search results will likely be a web page which will attempt to trick you into downloading a "new video codec" that's "required" for you to view free sex-related videos.
- If you do intentionally (or accidentally) end up downloading and running that "new codec" you will actually be infecting your system with rather poorly detected malware (checking an example of this malware at Virustotal, only 5 of 32 antivirus products detected this malware, and the two antivirus products with the largest market share, Symantec and McAfee, don't catch it at all at the time I tested the malware).
- See the report on the next two slides...

File **setup.exe** received on **01.01.2008 03:01:21 (CET)**

Current status: **finished**

Result: **5/32 (15.63%)**

 [Compact](#)

[Print results](#) 

| Antivirus | Version | Last Update | Result |
|---------------|--------------|-------------|-----------------------|
| AhnLab-V3 | 2008.1.1.10 | 2007.12.31 | - |
| AntiVir | 7.6.0.46 | 2007.12.31 | - |
| Authentium | 4.93.8 | 2007.12.31 | - |
| Avast | 4.7.1098.0 | 2007.12.31 | Win32:Zlob-AHS |
| AVG | 7.5.0.516 | 2007.12.31 | - |
| BitDefender | 7.2 | 2008.01.01 | - |
| CAT-QuickHeal | 9.00 | 2007.12.31 | - |
| ClamAV | 0.91.2 | 2008.01.01 | Trojan.Dropper-2529 |
| DrWeb | 4.44.0.09170 | 2007.12.31 | Trojan.Popuper.origin |
| eSafe | 7.0.15.0 | 2007.12.31 | - |
| eTrust-Vet | 31.3.5421 | 2008.01.01 | - |
| Ewido | 4.0 | 2007.12.31 | - |
| FileAdvisor | 1 | 2008.01.01 | - |
| Fortinet | 3.14.0.0 | 2007.12.31 | - |
| F-Prot | 4.4.2.54 | 2007.12.31 | - |
| F-Secure | 6.70.13030.0 | 2007.12.31 | - |

| | | | |
|-------------------|-------------|------------|------------------------------------|
| Ikarus | T3.1.1.15 | 2008.01.01 | - |
| Kaspersky | 7.0.0.125 | 2008.01.01 | Trojan-Downloader.Win32.Zlob.fpi |
| McAfee | 5196 | 2007.12.31 | - |
| Microsoft | 1.3109 | 2008.01.01 | TrojanDownloader:Win32/Zlob.gen!AL |
| NOD32v2 | 2758 | 2007.12.31 | - |
| Norman | 5.80.02 | 2007.12.31 | - |
| Panda | 9.0.0.4 | 2007.12.31 | - |
| Prevx1 | V2 | 2008.01.01 | - |
| Rising | 20.24.52.00 | 2007.12.29 | - |
| Sophos | 4.24.0 | 2008.01.01 | - |
| Sunbelt | 2.2.907.0 | 2007.12.30 | - |
| Symantec | 10 | 2008.01.01 | - |
| TheHacker | 6.2.9.176 | 2008.01.01 | - |
| VBA32 | 3.12.2.5 | 2007.12.31 | - |
| VirusBuster | 4.3.26:9 | 2008.01.01 | - |
| Webwasher-Gateway | 6.6.2 | 2007.12.31 | - |

Additional information

File size: 80139 bytes

MD5: cf46a1a8b4e94711ed779eba26d17eae

SHA1: e76b73e902184cdfd900bc3b355efc877bc66464

PEiD: -

An Example From 2009 of Why The World Gets Confused About Computer Security

[MALWARE -- DO NOT VISIT THIS SITE!]

My computer Online Scan

The page at <http://www.securitytoolstoday.com> says:

Your computer remains infected by viruses! They can cause data loss and file damages and need to be cured as soon as possible. Return to System Security and download it secure to your PC

Cancel OK

System Tasks

- View system information
- Add or remove programs
- Change a settings

Other Places

- My Network Places
- My Documents
- Shared Documents
- Control Panel

Details

My Computer
System Folder

System security

Hard drive

Local Disk (C:) 358 trojans

Local Disk (D:) 153 trojans

DVD

DVD-RAM Drive(E:)

100%

Now scanning: drwtsn32.msc

Your Computer is Infected!

fileinfos and actions:

| Name | Risk level | Date | Files infected | State |
|----------------------|------------|------------|----------------|-----------------|
| Email-Worm.Win32.Net | Critical | 07.13.2009 | 15 | Waiting removal |
| Email-Worm.Win32.Myd | Critical | 05.13.2009 | 23 | Waiting removal |
| Trj-Dwnldr.Win | Critical | 09.17.2009 | 37 | Waiting removal |

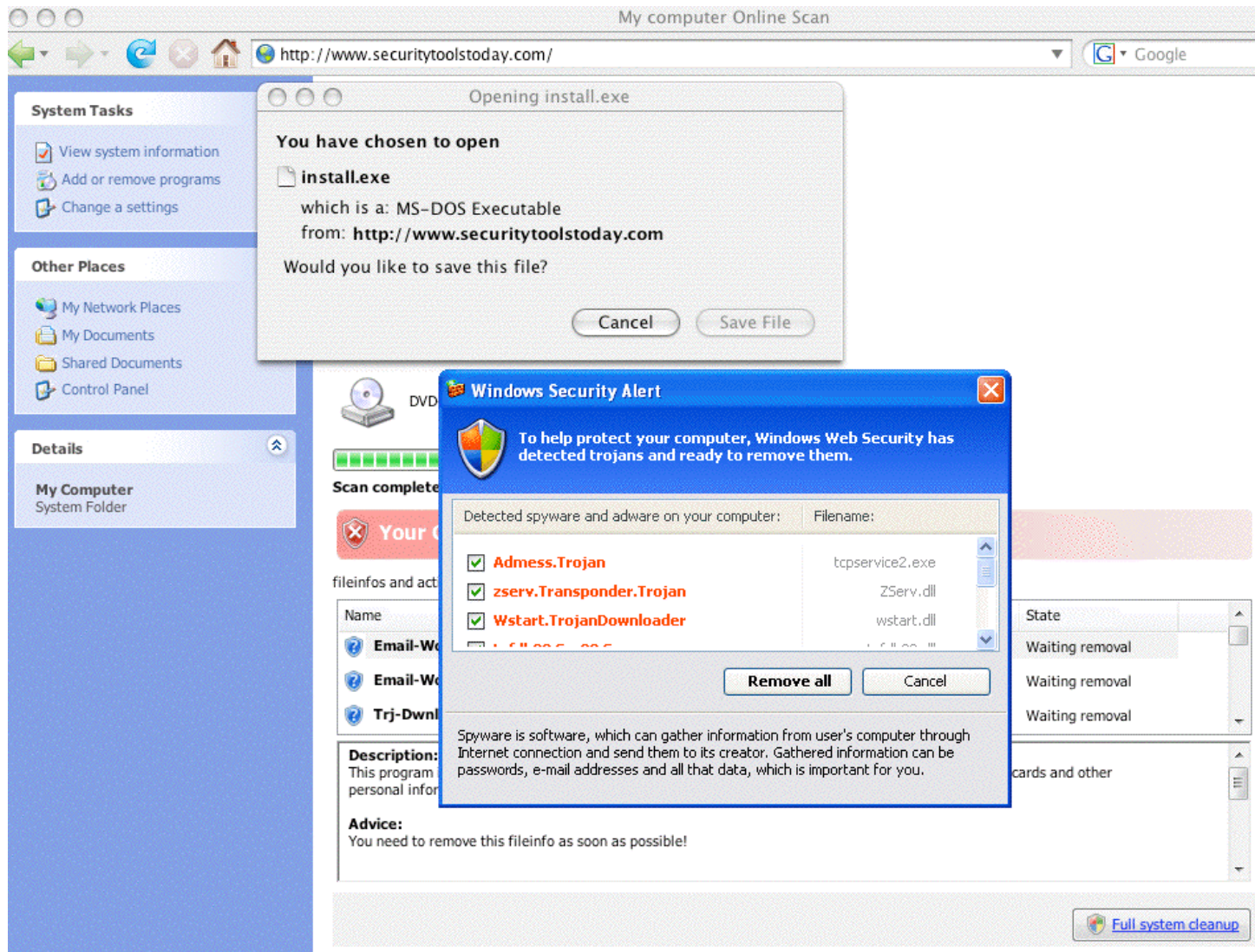
Description:
This program is potentially dangerous for your system. **Trojan-Downloader** stealing passwords, credit cards and other personal information from your computer.

Advice:
You need to remove this fileinfo as soon as possible!

Full system cleanup

Why The World Gets Confused (2)

[MALWARE -- DO NOT VISIT THIS SITE!]



Why The World Gets Confused (3)

- Note that that report came from a “scan” of my Mac, which doesn’t run Windows nor does it have a C:\ drive nor is it infected

:-)

- If you were to download the recommended installer from that site while it was live, it contained malware, although only one antivirus product in five detected it at the time the site was live.
- See the Virustotal report on the next slide...

The Widespread Failure of Antivirus

| VirusTotal – Free Online Virus and Malware Scan – Result | | | |
|---|-------------|-------------|--------------------------------|
| http://www.virustotal.com/analysis/7c3d09edf81cb030ad4bf64cde06419243dc58a1289e8e0z | | | |
| File install_5_.exe received on 2009.12.01 22:53:59 (UTC) | | | |
| Current status: finished | | | |
| Result: 8/40 (20%) | | | |
| Compact Print results | | | |
| Antivirus | Version | Last Update | Result |
| a-squared | 4.5.0.43 | 2009.12.01 | - |
| AhnLab-V3 | 5.0.0.2 | 2009.12.01 | - |
| AntiVir | 7.9.1.88 | 2009.12.01 | - |
| Antiy-AVL | 2.0.3.7 | 2009.12.01 | - |
| Authentium | 5.2.0.5 | 2009.12.01 | W32/FakeAlert.DX3.gen!Eldorado |
| Avast | 4.8.1351.0 | 2009.12.01 | - |
| AVG | 8.5.0.426 | 2009.12.01 | FakeAlert.NV |
| BitDefender | 7.2 | 2009.12.01 | - |
| CAT-QuickHeal | 10.00 | 2009.12.01 | - |
| ClamAV | 0.94.1 | 2009.12.01 | - |
| Comodo | 3103 | 2009.12.01 | - |
| DrWeb | 5.0.0.12182 | 2009.12.01 | - |
| eSafe | 7.0.17.0 | 2009.12.01 | - |
| eTrust-Vet | 35.1.7151 | 2009.12.01 | - |
| F-Prot | 4.5.1.85 | 2009.12.01 | W32/FakeAlert.DX3.gen!Eldorado |
| F-Secure | 9.0.15370.0 | 2009.11.29 | - |
| Fortinet | 4.0.14.0 | 2009.12.01 | - |
| GData | 19 | 2009.12.01 | - |
| Ikarus | T3.1.1.74.0 | 2009.12.01 | - |
| Jiangmin | 11.0.800 | 2009.12.01 | - |
| K7AntiVirus | 7.10.906 | 2009.11.27 | - |
| Kaspersky | 7.0.0.125 | 2009.12.01 | - |

The Widespread Failure of Antivirus (2)

| VirusTotal – Free Online Virus and Malware Scan – Result | | | |
|---|----------------|------------|---------------------------------------|
| http://www.virustotal.com/analysis/7c3d09edf81cb030ad4bf64cde06419243dc58a1289e8e0a2d4d1afc4895e708 | | | |
| K7AntiVirus | 7.10.906 | 2009.11.27 | - |
| Kaspersky | 7.0.0.125 | 2009.12.01 | - |
| McAfee | 5819 | 2009.12.01 | - |
| McAfee+Artemis | 5819 | 2009.12.01 | - |
| McAfee-GW-Edition | 6.8.5 | 2009.12.01 | Heuristic.LooksLike.Trojan.PCK.Krap.H |
| Microsoft | 1.5302 | 2009.12.01 | - |
| NOD32 | 4652 | 2009.12.01 | - |
| Norman | 6.03.02 | 2009.12.01 | - |
| nProtect | 2009.1.8.0 | 2009.11.28 | - |
| Panda | 10.0.2.2 | 2009.12.01 | Suspicious file |
| PCTools | 7.0.3.5 | 2009.12.01 | RogueAntiSpyware.SecurityToolFraud |
| Rising | 22.24.01.09 | 2009.12.01 | - |
| Sophos | 4.48.0 | 2009.12.01 | Mal/FakeAV-AD |
| Sunbelt | 3.2.1858.2 | 2009.12.01 | FraudTool.Win32.RogueSecurity (v) |
| Symantec | 1.4.4.12 | 2009.12.01 | - |
| TheHacker | 6.5.0.2.083 | 2009.12.01 | - |
| TrendMicro | 9.100.0.1001 | 2009.12.01 | - |
| VBA32 | 3.12.12.0 | 2009.11.30 | - |
| ViRobot | 2009.12.1.2065 | 2009.12.01 | - |
| VirusBuster | 5.0.21.0 | 2009.12.01 | - |
| Additional information | | | |
| File size: 1256004 bytes | | | |
| MD5...: 544059650c3a2be8061bcc65eabc98a6 | | | |
| SHA1...: 1120ad8355211cdf2d33a6bc4c4b3eb44e6f2c1a | | | |
| SHA256: 7c3d09edf81cb030ad4bf64cde06419243dc58a1289e8e0a2d4d1afc4895e708 | | | |

Looking At That Infested Site Just A Little

- `% dig www.securitytoolstoday.com +short`
94.102.63.245
- `% whois -h whois.ripe.net 94.102.63.245`
inetnum: 94.102.63.128 - 94.102.63.255
netname: KINGH-NET
descr: The King Host
country: NL
admin-c: AW137-RIPE
tech-c: AW137-RIPE
status: ASSIGNED PA
mnt-by: ECATEL-MNT
mnt-lower: ECATEL-MNT
mnt-routes: ECATEL-MNT
source: RIPE # Filtered

person: Andrew Willson
address: Honderdland 112F, 2677LT Maasdijk
phone: +31174712185
abuse-mailbox: ipadmin@thekinghost.biz
nic-hdl: AW137-RIPE [...]

Looking At That Infested Site A Little (2)

- % whois securitytoolstoday.com
Domain name: securitytoolstoday.com

Name servers:

ns1.securitytoolstoday.com
ns2.securitytoolstoday.com

Registrar: Regtime Ltd.

Creation date: 2009-11-25

Expiration date: 2010-11-25

Status: active

Registrant:

Kevin Neely

Email: kevinrneely@trashymail.com

Organization: Private person

Address: 3809 Hillview Drive

City: Oakland

State: CA

ZIP: 94612

Country: US

Phone: +1.7072310192

[etc]

Looking At That Infested Site A Little (3)

Anonymous Email and Free Spam Blocker

http://www.mytrashmail.com/myTrashMail_inbox.aspx?email=kevinrneely

Google

myTrashMail.com
smart email services





[Login](#)
[Register](#)
[About](#)
[FAQ](#)

News!!!

@trashymail.com domain is not active anymore.
Use our new anonymous email domain **@trash2009.com**

Email Account
kevinrneely

☐ Remember Me


| <input type="checkbox"/> | Sender | Subject | Date | Size | Delete |
|--------------------------|--------|---------|------|------|--------|
| No messages found! | | | | | |

[Delete Selected](#)


Looking At That Infested Site A Little (4)

USPS - ZIP Code Lookup - Search By Address

http://zip4.usps.com/zip4/zcl_0_results.jsp

 [USPS Home](#) | [FAQs](#)

ZIP Code Lookup

 **ZIP Code Lookup**

[Search By Address >>](#) [Search By City >>](#) [Search By Company >>](#) [Find All Cities in a ZIP Code™ >>](#)

Find a ZIP Code by entering an address.
(You can also search for a partial address, such as "Main Street, Fairfax, VA.")

We're sorry! We were unable to process your request.

The address was not found. Please check the address below.
You may want to utilize the Yellow Pages and/or White Pages below.

* Required Fields

* Address 1

Address 2 Apt, floor, suite, etc.

* City

* State [Find state abbreviation](#)

ZIP Code

[Submit >](#)

If You're So Inspired...

- The domain from this example no longer exists, but you may run into other domains with bad whois information. When you do, you can report them to Internic using the form at:

<http://wdprs.internic.net>

- Note that the WDPRS process isn't particularly rapid, and by the time you make progress on this one, the bad guys will usually have moved on and will be using another domain.
- Dot cn domains have been particularly popular because there is no WDPRS system for them, and they can cost as little as one yuan (USD ~\$0.15-\$0.20) to buy. Dot ru (Russian) domains have recently taken over from dot cn (Chinese) domains in popularity (and unfortunately ccTLD domains can't be reported via WDPRS)

Are There Potentially-Related Sites?

BFK edv-consulting GmbH – Sicherheit

http://www.bfk.de/bfk_dnslogger.html?query=94.102.63.245#result ▼

The server returned the following data:

| | | |
|------------------------------|---|---------------|
| onlineworldclub.com | A | 94.102.63.245 |
| ns1.onlineworldclub.com | A | 94.102.63.245 |
| antispywaresoftworld.com | A | 94.102.63.245 |
| ns1.antispywaresoftworld.com | A | 94.102.63.245 |
| securitytoolcode.com | A | 94.102.63.245 |
| ns1.securitytoolcode.com | A | 94.102.63.245 |
| scanonlinesite.com | A | 94.102.63.245 |
| ns1.scanonlinesite.com | A | 94.102.63.245 |
| antyspywaressite.com | A | 94.102.63.245 |
| ns1.antyspywaressite.com | A | 94.102.63.245 |
| securitytoolblog.com | A | 94.102.63.245 |
| ns1.securitytoolblog.com | A | 94.102.63.245 |
| bestfreecheck.com | A | 94.102.63.245 |
| ns1.bestfreecheck.com | A | 94.102.63.245 |
| webbillcheck.com | A | 94.102.63.245 |
| ns1.webbillcheck.com | A | 94.102.63.245 |
| thetoolsdiscount.com | A | 94.102.63.245 |
| ns1.thetoolsdiscount.com | A | 94.102.63.245 |
| securitytooltoday.com | A | 94.102.63.245 |
| ns1.securitytooltoday.com | A | 94.102.63.245 |
| securitytoolsimage.net | A | 94.102.63.245 |
| ns1.securitytoolsimage.net | A | 94.102.63.245 |
| securityutilitystore.net | A | 94.102.63.245 |
| ns1.securityutilitystore.net | A | 94.102.63.245 |

So Why Do People Drop Malware on Systems?

- It's usually to **make money**.
- Sometimes criminal organizations will pay people to install malware, anything from a dime per install to over a dollar per install. That's a pretty tempting opportunity for someone in Eastern Europe or the third world where a “good” regular job might pay a thousand bucks a month, if you can get one at all.
- What do the criminal organizations who've paid a dime or a dollar per machine do with malware infested machines once they've got them? We'll talk about that more later in this talk, but some common reasons include:
 - stealing valuable information (credit card #'s, passwords, etc.)
 - sending spam (e.g., your PC gets turned into a “spam cannon”)
 - hosting illegal content (typically known as “fast flux” hosting)
 - engaging in click fraud against pay-per-click advertisers
 - etc., etc., etc.

GDP Purchasing Power Parity Per Capita (Selected States)

| | | | |
|-----|----------------------------|-----------|-----------|
| 1 | Liechtenstein | \$118,000 | 2007 est. |
| 2 | Qatar | \$111,000 | 2008 est. |
| 3 | Luxembourg | \$81,200 | 2008 est. |
| ... | | | |
| 9 | Brunei | \$51,300 | 2008 est. |
| 10 | United States | \$47,500 | 2008 est. |
| 11 | Ireland | \$45,500 | 2008 est. |
| ... | | | |
| 73 | Russia | \$16,100 | 2008 est. |
| ... | | | |
| 90 | Romania | \$12,200 | 2008 est. |
| ... | | | |
| 92 | Turkey | \$11,900 | 2008 est. |
| 133 | China | \$6,000 | 2008 est. |
| ... | | | |
| 227 | Burundi | \$300 | 2008 est. |
| 228 | Congo, Democratic Republic | \$300 | 2008 est. |
| 229 | Zimbabwe | \$200 | 2008 est. |

Doing It For \$\$\$:

This Is A Big Change From The Old Days

- In the old days, at least some cyber crimes might have been committed as a result of an misplaced sense of curiosity, or because hacking a system was a challenge (sort of like “matching wits” with the creator of a puzzle), or for “bragging rights” among one’s peers.
- Now many of the people who committing cyber crimes are economically motivated. Committing cyber crimes has become their full time job (or at least a part time one).
- An underground economy has developed as a result, complete with specialization and the ability to buy (rather than build) what’s needed to get started. No longer do you need to be a “computer genius,” you just need to know where to go/who to talk to.
- This obviously greatly expands the pool of potential participants, and even leads to what amounts to the “franchising of cyber crime” through things like criminal affiliate programs.

1. (d) Distributed Denial of Service (DDoS) Attacks

Using a distributed denial of service (“DDoS”) attack, miscreants can flood servers or wide area network connection with traffic from thousands of hosts, thereby taking virtually any networked site “off the Internet” for as long as they want -- or at least they can make you work very hard in order to stay on. How/why do miscreants use DDoS attacks? There are a variety of reasons:

At one point, it was common for cyber gangs to targeting online gambling sites for extortion ("Pay, or we'll DDoS your web site and shut you down!") [remember, these days cybercrime is often all about making money]

On the other hand, multi gigabit/second DDoS attacks have been observed (see www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf) targeting critical Internet infrastructure, and distributed denial of service attacks have even been used to attack entire countries (such as Estonia).

Sometimes a DDoS is just something done by a disgruntled competitor. 51

"Why Couldn't I Just Block That DDoS With My Firewall???"

- **Answer:** because by the time the firewall sees the traffic, it's too late, and firewalls, because they track connect “state” in relatively small finite tables, may even make you **MORE** vulnerable to DDoS attacks.
- Consider a denial of service attack which is attempting to flood your network connection with unsolicited traffic. Your firewall is located at your company or institution, interposed between you and the world. That firewall is connected to your Internet Service Provider (ISP) by a comparatively small (and comparatively expensive) network connection. A DoS attack will **FILL** that network connection **BEFORE** it encounters and is blocked by your firewall. If you attempt to offset the attack traffic by increasing the size of your network connection, the bad guys or bad gals will just send you more traffic to compensate (they can scale up their operations cheaper/quicker than you can)
- Thus, even though your firewall may protect your **hosts** from seeing DoS traffic, your firewall will **NOT** protect your **network connection** from being filled to the brim (and beyond) with huge volumes of unwanted traffic which will effectively squeeze out all the good traffic you do want to receive.

2. Internet Fraud: Crimes of Deception

For Release: October 29, 2007

FTC Releases Consumer Fraud Survey

30.2 Million Americans - 13.5 Percent of U.S. Adults - Fell Victim to Fraud

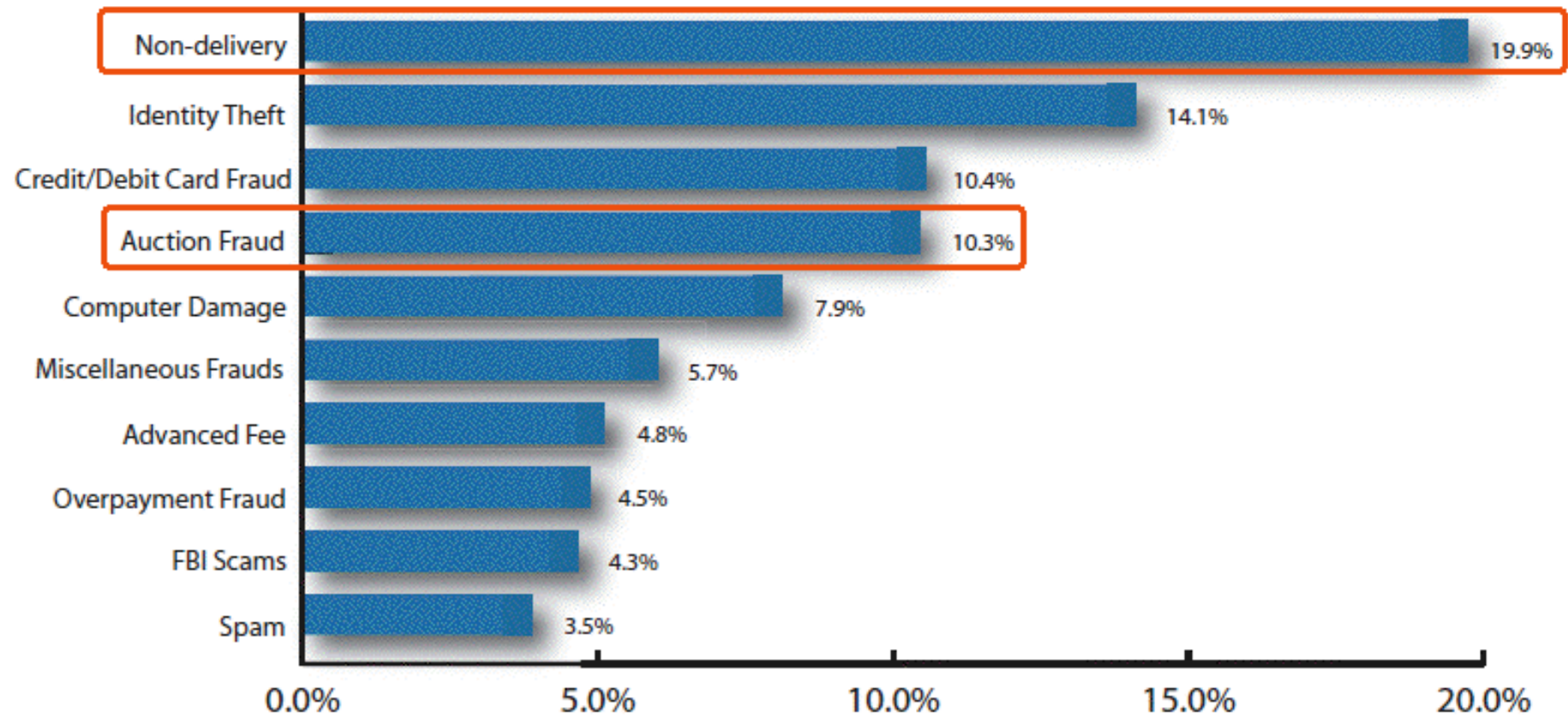
The Federal Trade Commission today released a statistical survey of fraud in the United States that shows that 30.2 million adults – 13.5 percent of the adult population – were victims of fraud during the year studied. More people – an estimated 4.8 million U.S. consumers – were victims of fraudulent weight-loss products than any of the other frauds covered by the survey.

Fraudulent foreign lottery offers and buyers club memberships tied for second place in the survey. Lottery scams occur when consumers are told they have won a foreign lottery that they had not entered. Victims supplied either personal information such as their bank account numbers or paid money to receive their "winnings." In the case of buyers clubs, victims are billed for a "membership" they had not agreed to buy. An estimated 3.2 million people were victims of these frauds during the period studied.

<http://www.ftc.gov/opa/2007/10/fraud.shtm>

2. (a) Internet Auction Fraud

Figure 5: 2009 Top 10 Most Referred IC3 Complaint Categories (Percent of Total Complaints Referred)



Source: http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

2. (b) Pay-Per-Click Click Fraud

- Many leading Internet companies earn a majority of their revenue by selling pay-per-click advertisements. In pay-per-click (PPC) advertising models, true to the model's name, an advertiser agrees to pay whenever someone clicks on one of their ads.
- PPC ads are placed both on things like search engine results, and on relevant syndicated web pages authored by 3rd parties. To compensate 3rd parties for inserting ads on their web pages, the advertising company shares part of what they've been paid with the 3rd parties.
- Priority for ad placement is determined by what advertisers are willing to pay -- the highest bids get the best placement on a given page which contains the term of interest
- An example of pay-per-click rates for one advertising program for some terms related to fishing boats can be seen on the next page...










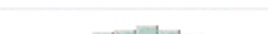












Calculate estimates using a different maximum CPC bid:

US Dollars (USD \$)

Recalculate

Choose columns to display: ?

Show/hide columns

| Keywords | Estimated Avg. CPC | Advertiser Competition | Local Search Volume: December | Global Monthly Search Volume | Search Volume Trends (Jan - Dec 2009) | Highest Volume Occurred In | Match Type: Broad |
|---|-----------------------|---|--|---------------------------------------|---|-------------------------------------|-----------------------|
| Keywords related to term(s) entered - sort by relevance | | | | | | | |
| flats fishing boats | \$3.53 |  | 1,900 | 1,900 |  | Sep | Add ▾ |
| fishing boat dealers | \$3.37 |  | 720 | 1,300 |  | Jul | Add ▾ |
| fishing boat sales | \$2.52 |  | 1,600 | 2,900 |  | May | Add ▾ |
| charter fishing boat | \$1.81 |  | 22,200 | 22,200 |  | Jul | Add ▾ |
| salt water fishing boats | \$1.49 |  | 1,000 | 1,300 |  | Jul | Add ▾ |
| boston whaler fishing boats | \$1.46 |  | 3,600 | 1,900 |  | Sep | Add ▾ |
| fly fishing boats | \$1.35 |  | 2,400 | 2,900 |  | Jul | Add ▾ |
| fishing boat charters | \$1.34 |  | 2,400 | 2,900 |  | Jul | Add ▾ |
| charter fishing boats | \$1.32 |  | 8,100 | 9,900 |  | Jul | Add ▾ |
| fishing deck boats | \$1.21 |  | 880 | 590 |  | Nov | Add ▾ |
| fishing boating | \$1.20 |  | 450,000 | 550,000 |  | Jun | Add ▾ |

PPC Gone Awry

- Thus, every time you click on a top-rated PPC ad for a boat, it may cost someone as much as \$3.53 or more depending on the keywords you searched for). Of course, if a visitor ends up buying a boat from you after clicking on your ad, that's \$3.53 that's very well invested.
- But now, imagine what happens if people who have no interest in a product start clicking on PPC ads -- the advertiser pays for clicks which don't, won't, and never will, result in a sale!
- Clicking on PPC ads can be manual, or via automated programs.
- When the advertiser gets a huge PPC advertising bill, but no associated sales, they become disgruntled and complain to the advertising company, or stop advertising online altogether...
- While antifraud measures have been deployed (IP addresses associated with at least some weird PPC traffic patterns can be readily identified), this is still a HUGE deal to many leading Internet businesses.

India's secret army of online ad 'clickers'

3 May 2004, 0820 hrs IST, N Vidyasagar, TNN

SMS NEWS to 58888 for latest updates

NEW DELHI: With her baby on her lap, Maya Sharma (name changed) gets down to work every evening from her eighth-floor flat at Vasant Vihar. Maya's job is to click on online advertisements. She doesn't care about the ads, but diligently keeps count — it's \$0.18 to \$0.25 per click.



"It's boring, but it is extra money for a couple of hours of clicking weblinks every day," says a resident of Delhi's Patparganj, who has kept a \$300-target for the summer.

Traffic to click overseas Internet ads - from home loans to insurance - is spreading fast in India. "I have no interest in what appears when clicking an ad. I care only whether to pause 60 seconds or 90 seconds, as money is credited if you stay online for a fixed time," says another user.

Here's how it works: online advertisers in developed markets agree to pay hosting website each time an ad is clicked. With performance-based deals becoming dominant on the Internet, intermediaries have sprung up to "do the needful". Why, type in 'earn rupees clicking ads' in Google — you get 25,000 results.

"I'm not surprised. As competition intensifies, people are using every trick to increase their revenues," says Sam Balsara, CMD, Madison.

The trend is catching up in India. Says Goutam Rakshit, chairman, Advertising Council of India: "It's a numbers game as far as media buying is concerned. And anybody who can manipulate numbers gets the edge. This is unethical, and needs to be curbed."

Take Click2freemoney.com. Calling itself an Internet advertising company that shares profits with members, it gives three options to earn money — by clicking on website links via e-mails that they send, by clicking on banners and text ads in their paid-to-click section, and by referring others to the website.

No wonder Internet ad firms have been floated in neighbourhood colonies, promising to share "secrets" to earning in dollars by clicking online ads for an upfront fee of Rs 250 to Rs 1,500.

Typically, online ad clickers get their money remitted by opening accounts through PayPal or StormPay — which enables money transaction if you have an e-mail address.

Most clickers, however, opt to pay commission to middle men and encash earnings in rupees. Clickers say they pay \$7 commission for every \$50 earned.

Google CFO: Fraud a big threat

Google exec calls click fraud the "biggest threat" to the Internet economy, urges quick action.

December 2, 2004: 6:30 PM EST

By Krysten Crawford, CNN/Money staff writer

NEW YORK (CNN/Money) - A top Google official said that growing abuse of the company's lucrative sponsored ad-search model jeopardizes the popular Internet search engine's business.

"I think something has to be done about this really, really quickly, because I think, potentially, it threatens our business model," Google Chief Financial Officer George Reyes said Wednesday.

Reyes, speaking at an investor conference sponsored by Credit Suisse First Boston, was referring to an illegal practice known as "click fraud" that occurs when individuals click on ad links that appear next to search results in order to force advertisers to pay for the clicks.

In cost-per-click advertising, marketers pay a search engine, like Google, Yahoo! or FindWhat.com, when users click on links to the advertisers' Web sites. Google and others also generate revenue by posting sponsored ad links on other Web sites and splitting the fees generated by user clicks.

The paid-search model is now the fastest-growing form of Internet advertising, according to the Interactive Advertising Bureau.

But analysts, fraud experts and now [Google](#) (down \$0.56 to \$179.40, [Research](#)) are openly fretting about the rise of click fraud.

The main perpetrators appear to be competitors of advertisers and also scam sites set up for the sole purpose of hosting ad links provided by Google, through its AdSense unit, or Yahoo!, through its Overture service. Humans or specially designed software then click on those ad links in order to "steal" revenue from advertisers.

Estimates of how prevalent click fraud has become since it appeared four years ago are all over the map. Jessie Stricchiola, the president of Alchemist Media, estimated that as much as 20 percent of all clicks on paid search ads are shams.



The advertisement features the 'PLAN b' logo in the top left corner. The main headline reads 'Color Laser Printers and All-In Ones that give you more.' Below the headline, three Brother printers are displayed: a compact desktop model, a larger floor-standing model, and a multifunction all-in-one model. The text 'Starting around \$399' is positioned below the printers. At the bottom left is a blue oval button with the text 'Learn more'. At the bottom right is the 'brother' logo with the tagline 'At your side.' in a smaller font. A rainbow-colored horizontal bar runs along the very bottom of the advertisement.

The Vanishing Click-Fraud Case

Why was a seemingly slam-dunk case against an alleged click-fraudster who attempted to extort Google quietly dismissed?

by [Ben Elgin](#)

A detective novelist might call it *The Mystery of the Vanishing Click-Fraud Case*.

It began on Mar. 10, 2004, when a computer programmer from Oak Park, Calif., named Michael Anthony Bradley arrived at Google's ([GOOG](#)) offices for a prearranged meeting with the company's engineers, according to a criminal indictment filed two years ago in the U.S. District Court in San Jose. Bradley, then 32, proceeded to demonstrate new software, dubbed "Google Clique," designed to generate false clicks on Google ads. Bradley claimed his program could force Google to pay millions of dollars on false clicks and threatened to release it to others unless Google paid him approximately \$150,000, according to the indictment.

Law enforcement, tipped off earlier, taped the meeting from the room next door and soon arrested Bradley. It appeared Bradley would become the first person criminally prosecuted for charges related to click fraud, the Achilles heel of the Internet-advertising industry, which costs marketers as much as \$1 billion a year (see BusinessWeek, 10/2/06, "[Click Fraud](#)").

GOOGLE BACKS DOWN

But on Nov. 22, the U.S. Attorney's Office quietly dismissed charges against Bradley. The prosecutors, who had announced the arrest and indictment of Bradley in press releases, refused to discuss why they dropped the case. Defense attorney Jay Rorty declined to comment or make his client available. Attempts to reach Bradley weren't successful. A Google spokesman issued a vague statement: "We continue to work closely with law enforcement in many areas, including click fraud. Individual cases may or may not be pursued by law enforcement at their discretion."

www.businessweek.com/print/technology/content/dec2006/tc20061204_923336.htm

Arguably, Google Is Still “Limping Along” Notwithstanding the Click Fraud Problem: Google (upper line) vs. NASDAQ, 2004-2011



2. (c) Nigerian Advance Fee Fraud (4-1-9)

From: "Mr. Don Peter"

To: undisclosed-recipients::

Subject: Dear Friend

Date: Thu, 18 Oct 2007 08:39:10 -0400

Reply-to: hellen_doris1@yahoo.fr

Dear Friend

It has been long we communicate last, am so sorry for the delay, I want to Inform you that your cheque of (\$850.000.00) Which my boss asked me to mail to you as soon as you requested it, is still with me.

But due to some minure issue you fails to respond at the Approprete time, and presently the cheque is with me here in LAGOS-NIGERIA Though i had a new contact from a friend of mine who works with one security company here in NIGETIA that will deliver you your cheque at your door step with a cheeper rate, which the company said that it will cost you the sum of \$198.00 usd, So you have to Contact them and register with them now.

Considering That Sample...

- The actual 419 scam sample you've just seen is so full of spelling and usage errors that it may be hard to believe that anyone would take it seriously.
- Yet we know that people do fall for these sort of 4-1-9 scams...

In Some Cases, Losses Can Be *Very* High

ABUJA, Nigeria (AP) --Nigerian prosecutors leveled 86 counts of fraud and conspiracy against five people Thursday for allegedly swindling a Brazilian bank of \$242 million, in the biggest crackdown yet on the West African nation's advance-fee fraud or "419" scams.

The five are accused of luring an employee of Sao Paulo's Banco Noroeste into siphoning off the funds from his employer, persuading him he could land a share in a lucrative Nigerian construction contract if he just paid enough handling fees up front.

The five appeared in court in Nigeria's capital, Abuja, in handcuffs to hear the charges Thursday. All the suspects, including housewife Amaka Anajemba, lawyer Obum Osakwe, and businessman Emmanuel Nwude -- described by prosecutors as "a major shareholder" in a leading Nigerian bank -- pleaded innocent.

Penalties for each of the counts range between seven and 10 years.

Four Nigerian companies -- Ocean Marketing, Fynbaz, Emrus, and the African Shelter Bureau -- also accused of involvement in the alleged crime were not represented in court.

Presiding Judge Lawal Gumi entered innocent pleas on behalf of the companies and postponed proceedings until Wednesday, when he will consider requests for bond.

There was mild drama in court when suspect Nzeribe Okoli, while making his plea, declared he would make "shocking revelations" during the trial.

"There are so many hidden things which Nigerians should know," Okoli said before he was interrupted by the judge, who told him to restrict his answers to the questions he was asked.

Nigeria's anti-fraud body, the Economic and Financial Crimes Commission, alleges in court papers the suspects told the Brazilian bank worker he would receive \$13.4 million from an \$187 million Nigerian airport contract -- if he invested money up front.

The bank worker allegedly dug illegally into his bank's funds, transferring the \$242 million -- in segments as high as \$4.75 million at a time -- to accounts around the world designated by the suspects, the papers showed.

Nigeria has gained global notoriety as a base for such advance-fee fraud, known as '419' schemes after the section of the country's criminal code that prohibits fraud.

<http://www.cnn.com/2004/WORLD/africa/02/05/nigeria.419.trial.ap/index.html>

SA cops, Interpol probe murder

31/12/2004 12:31 - (SA)

Philip de Bruin , Beeld

Interpol and the police forces of South Africa, America and Greece have joined forces to investigate the brutal murder of a wealthy Greek national whose badly mutilated body was found in Durban shortly before Christmas.

George Makronalli, 29, was a victim of a notorious 419 fraud scheme.

He was apparently lured to the country under the pretence that he could earn hundreds of thousands of rands. He was then kidnapped and summarily killed when his family refused to pay the ransom.

A spokesperson for the Durban police confirmed on Thursday that Makronalli was a victim of a 419 syndicate.

Caught in a trap

The syndicate issued a statement on the internet in which they claimed that they had stolen about R150m from the South African government by submitting false claims for "contracts" and that they needed help from overseas to get the money out of the country.

Whoever was willing to help them, would receive a large part of the "profit". Makronalli was caught with this ruse. He reacted to the "invitation" and was convinced to come to South Africa in November.

He returned to Greece, but re-entered South Africa through Johannesburg International Airport at the request of syndicate members on December 18. He then disappeared.

When his brother, Sotirus Makronelli, from Los Angeles, could not establish contact with him for two days, he contacted Interpol and the American police. The police spokesperson said Sotirus allegedly also invested money in the 419 scheme.

Shortly after, Sotirus received an e-mail from the syndicate in which they informed him that they had kidnapped his brother and demanded that \$160 000 (about R1m) be deposited in an American bank account within 24 hours. They threatened to kill George if their demands were not met.

The ransom was not paid. A day later, police found George's body in Durban. Both his legs and arms were broken and he had been set alight - probably while he was still alive.

"I Go Chop Your Dollar"

- **'I Go Chop Your Dollar' star arrested: 419 spoof turns real**

http://www.theregister.co.uk/2007/07/02/419_singer_caught/

Nigerian comedian and actor Nkem Owoh was one of the 111 suspected 419 scammers arrested in Amsterdam recently as part of a seven month investigation, dubbed Operation Apollo.

Owoh became a well known star within the Nigerian film industry, sometimes colloquially known as Nollywood because of its trite plots, poor dialogue, terrible sound, and low production standards.

Owoh starred in the 2003 film *Osuofia*, and a year later was one of several actors temporarily banned from appearing in movies by Nigeria's Association of Movie Marketers and Producers because he demanded excessive fees and unreasonable contract demands.

Owoh became internationally known for his song "I Go Chop Your Dollar", the anthem for 419 scammers ("Oyinbo man I go chop your dollar, I go take your money and disappear 419 is just a game, you are the loser I am the winner" [...]), which was banned in Nigeria after many complaints.

[The video's at: http://www.tlcafrica.com/I_go_chop_your_dollar1.mov]

Enforcement Can Be Difficult

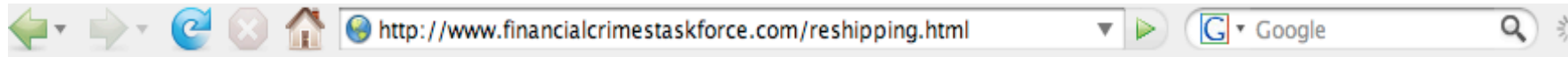
- For an example of what a raid on a Nigerian Cyber Café looks like, you may want to see the video at:
“EFCC Busts Some Nigerian Scammers”
<http://www.youtube.com/watch?v=ISMgGdaGOJM>
- Or see the account of a raid by an Irish cyber café owner:
“I fought the scammer... and I won” <http://www.antonline.com/archive/index.php/t-254170.html>
- Corruption at high levels can hinder efforts at cleaning this all up...
“Nigerian courts last year recorded high profile cases, many of which made newspapers and magazines headlines because of their nature and personalities involved. The list includes cases involving the President, former Head of States, former Vice-President, sitting and past governors, serving and former ministers, members of the National Assembly, heads of government agencies and notable party leaders, among others.”
<http://allafrica.com/stories/200901080331.html>

Corruption Perceptions Index (selected states)

- www.transparency.org/policy_research/surveys_indices/cpi/2010/results

| Country rank | country | 2009 CPI Score |
|--------------------|-------------|----------------|
| 1 (least corrupt) | Denmark | 9.3 |
| 1 | New Zealand | 9.3 |
| 1 | Singapore | 9.3 |
| ... | | |
| 22 | USA | 7.1 |
| ... | | |
| 78 | China | 3.5 |
| ... | | |
| 134 | Nigeria | 2.4 |
| ... | | |
| 154 | Russia | 2.1 |
| ... | | |
| 175 | Iraq | 1.5 |
| 176 | Afghanistan | 1.4 |
| 176 | Myanmar | 1.4 |
| 178 (most corrupt) | Somalia | 1.1 |

2. (d) Reshipping Fraud



RESHIPPING SCAM

Reshipping scams involve the receiving and reshipping of merchandise ordered online, to locations usually overseas. The shipper is an unwilling participant and the merchandise has been paid for with stolen or fraudulent credit cards.

Two methods are used frequently to entice victims to unwillingly take part in this scam. The first is through the use of help wanted advertisements posted on popular Internet job search sites, such as Monster.com. As part of the process, the prospective employee is required to provide all of his/her personal information, including social security number and date of birth. Once this employee is "hired," they immediately begin receiving packages at their residence and are then responsible for repackaging and shipping the merchandise abroad.

Payment to these employees usually arrive in the form of a third party cashier's check instead of a regular paycheck. Additionally, the check is usually for an amount in excess of what had previously been agreed upon. The employee is instructed to cash the check and electronically forward the excess amount to an overseas bank account. After the transaction is complete but before the check has had a chance to "clear," the financial institution realizes that the cashier's check is not valid. The employee is then responsible for the total amount of the fraudulent check.

By this point, the employee realizes that they have not only fallen victim to a scam but that the operators of the scam are now in possession of their personal information.

The second method used to facilitate reshipping scams involves the use of Internet. Unknown subjects participate in chat rooms pretending to look for a special friend or romance. After carefully forging a good relationship, the subject explains that his/her country will not accept direct business shipments from the United States. The subject asks if the victim will permit him/her to use the victim's U.S. residential address to receive and reship recent online purchases. As soon as the victim agrees, packages begin to arrive for reshipment. Several weeks pass with the victim dutifully sending on the merchandise. Eventually, victim merchants contact the U.S. "friend" and explain that the recently shipped merchandise was purchased with fraudulent credit card.

"Reshippers" Economic Impact

- In preparation for Operation Cyber Sweep, the Internet Crime Complaint Center (IC3), through its established public/private alliance with the Merchants Risk Council (MRC), requested suspected on-line fraudulent “Reshipper” transaction[s] for the 120 days preceding November 1, 2003.
- Numerous Reshipper investigations have been initiated nationwide and abroad, coordinated via the IC3. USPIS, FBI, USSS and a myriad of state and local agencies have participated in these investigations.
- Members of the MRC reported 7,812 fraudulent transactions with an aggregated potential economic loss of \$1.7 million. **Analysis of the transactional data identified 5,053 addresses in the United States that were utilized in the furtherance of the “Reshipper” scheme.**
- As a result of the continual real time sharing of information between law enforcement and private industry, over \$350,000 in merchandise was recovered and returned to the respective victim companies.
- **According to the MRC, e-commerce in the United States has experienced losses related to the “Reshipper” scheme in excess of 500 million dollars.**

A Site That Tracks Reshipper/Mule Scams

The screenshot shows a web browser window with the title 'Money Laundering and Reshipping Fraud' and the URL 'http://www.bobbear.com/'. The page features a search bar with the Google logo and a list of 'Active Frauds' under a green-bordered header. The list is organized into two columns. The left column contains links to various companies, including 1K Management, 1M Diversified Financial, 1st Class Recruitment, 1st Edition Process Service, 1st Quest Technology, 2 Affordable, 20th Century Financial, 2Consumer Ltd., 21st Century Advanced Technologies, 24 Hour Express Service, 24 Spanish Realty, Abcat Finance, ABC Web Design Inc, Abela Financial Group, ABP Group, AccessUSA (Stolen Identity), Active Solutions Inc., Adamas Jewellery LLC, Adam Diaz International, Adecco, AdexComp, AD Machinery, Adriatic Finance Services (**Rockphish**), Advanced Finance Inc., Advance Finance Group LLC, Advance Finance LLC, Advanta TN, ADVERTISING AGENCY LLC, Advertising Enterprises, LLC, Advertising International Company, Affina Group Inc, AFG Financial Group, and AFS Financial Group. The right column contains links to Milet Business, Inc., Minara Company, Mirax Cargo, ML-Group, MMM Reselling, Moonbeam Logistics, Inc., Moranna (**Rockphish**), Morgan Trading Co., Movement Ltd., MTK, Multiconcept Group Inc., Multi Group Inc., My Health Direct Inc., MyUs (Stolen Identity), Navitex, Navy Finance and Payroll Inc., NBIV, Co., N Design Studio, Inc, NEO INVESTMENT MANAGEMENT, Neweca Payments Inc., Nexins Inc., Neztro Corporation, NG Logistics, Nixon Consult, LLC., Norsten Logistics, NTT Pty Ltd, Nvidia Group Inc, Offshore Loans Ltd., OG Express, Oka Overseas Agencies, OnaOdn Company, One Box Advertising, Onicks Group Inc., OnlineCompanySite Inc, and OnlineOfficeSource.

Active Frauds

[1K Management](#)
[1M Diversified Financial](#)
[1st Class Recruitment](#)
[1st Edition Process Service](#)
[1st Quest Technology](#)
[2 Affordable](#)
[20th Century Financial](#)
[2Consumer Ltd.](#)
[21st Century Advanced Technologies](#)
[24 Hour Express Service](#)
[24 Spanish Realty](#)
[Abcat Finance](#)
[ABC Web Design Inc](#)
[Abela Financial Group](#)
[ABP Group](#)
[AccessUSA \(Stolen Identity\)](#)
[Active Solutions Inc.](#)
[Adamas Jewellery LLC](#)
[Adam Diaz International](#)
[Adecco](#)
[AdexComp](#)
[AD Machinery](#)
[Adriatic Finance Services \(**Rockphish**\)](#)
[Advanced Finance Inc.](#)
[Advance Finance Group LLC](#)
[Advance Finance LLC](#)
[Advanta TN](#)
[ADVERTISING AGENCY LLC](#)
[Advertising Enterprises, LLC](#)
[Advertising International Company](#)
[Affina Group Inc](#)
[AFG Financial Group](#)
[AFS Financial Group](#)

[Milet Business, Inc.](#)
[Minara Company](#)
[Mirax Cargo](#)
[ML-Group](#)
[MMM Reselling](#)
[Moonbeam Logistics, Inc.](#)
[Moranna \(**Rockphish**\)](#)
[Morgan Trading Co.](#)
[Movement Ltd.](#)
[MTK](#)
[Multiconcept Group Inc.](#)
[Multi Group Inc.](#)
[My Health Direct Inc.](#)
[MyUs \(Stolen Identity\)](#)
[Navitex](#)
[Navy Finance and Payroll Inc.](#)
[NBIV, Co.](#)
[N Design Studio, Inc](#)
[NEO INVESTMENT MANAGEMENT](#)
[Neweca Payments Inc.](#)
[Nexins Inc.](#)
[Neztro Corporation](#)
[NG Logistics](#)
[Nixon Consult, LLC.](#)
[Norsten Logistics](#)
[NTT Pty Ltd](#)
[Nvidia Group Inc](#)
[Offshore Loans Ltd.](#)
[OG Express](#)
[Oka Overseas Agencies](#)
[OnaOdn Company](#)
[One Box Advertising](#)
[Onicks Group Inc.](#)
[OnlineCompanySite Inc](#)
[OnlineOfficeSource](#)

2. (e) "High Yield Investment Programs"

- Well-known banks and credit unions in the Eugene-Springfield area are currently paying 0.10% to 0.25% (one tenth to one quarter of one percent) per year on savings accounts. <cough>
- So imagine what a surprise it would be if someone offered to pay you two to three percent PER DAY!!! Wow! Gee!
- Oh yeah, naturally, this is a complete and total scam/ripoff!
- How HYIP/"Prime Bank" fraud schemes often work:
 - a web site promises you an outrageously great rate of return, often for a convoluted but allegedly "riskless" investment
 - "investments" are sent in online, usually via an irrevocable online e-currency
 - the investment program prohibits withdrawal of your "investment" for a period of time, perhaps 90 or 180 days
 - when it **IS** finally time to withdraw your money (and receive your lucrative interest payment), surprise!, the program you "invested" in has vanished
 - in other cases, the HYIP may have a Ponzi-scam like component, with funds from later investors used to pay (some) early investors (for a while) until the HYIP program operator disappears with all the rest of the loot 73

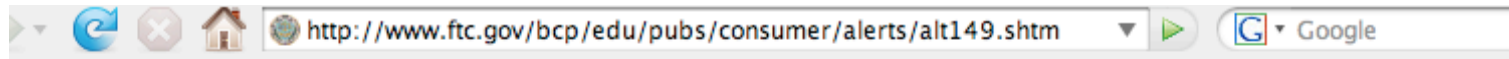
SEC v. Zahra Ghods and RUSA Cap., Inc., Defendants, & Unisource Cap., LLC, Relief Defendant, Civ. Act No. 1:07-CV-1047 (NDGA May 8, 2007)

On May 8, 2007, the Securities and Exchange Commission (Commission) filed a Complaint for Injunctive Relief (Complaint) in the United States District Court for the Northern District of Georgia against Zahra Ghods, a U. S. citizen who currently resides in Hong Kong, and RUSA Cap., Inc. (RUSA), an entity located in Newport Beach, California that Ghods owns and controls.

The Complaint alleges that from as early as February 2004 through May 2006, Ghods and RUSA actively participated in a fraudulent **prime bank scheme** perpetrated by Geoffrey Gish (Gish) and several entities that he controlled. That prime bank scheme involved the sale of approximately **\$29.6 million of securities to more than 300 investors located throughout the United States**. The Commission previously filed an emergency action against Gish and his affiliated companies on May 17, 2006. [citation omitted]

The Complaint alleges that Ghods and RUSA participated in one of the three fraudulent prime bank schemes that Gish offered, Zamindari Capital, LLC, and **received approximately \$9 million of investor funds**. Zamindari was represented to be a **high yield investment program** that generated lucrative profits by purchasing debt instruments from major international banks at a discount and quickly reselling them at face value. [continues]

2. (f) Diploma Scams



Diploma Mills: Degrees of Deception

Are you ever tempted by an email or an ad claiming you can "earn a college degree based...on life experience"? Don't be, say attorneys for the Federal Trade Commission (FTC), America's consumer protection agency. Chances are good that the ad is for a "diploma mill," a company that offers "degrees" or certificates for a flat fee, requires little course work, if any, and awards degrees based solely on life experience.

Most employers and educational institutions consider it lying if you claim academic credentials that you didn't earn through actual course work. Federal officials say it's risky behavior: If you use a so-called "degree" from a diploma mill to apply for a job or promotion, you risk not getting hired, getting fired, and in some cases, prosecution.

Diploma mills may claim to be "accredited." Colleges and universities accredited by legitimate organizations undergo a rigorous review of the quality of their educational programs. Although many diploma mills claim to be "accredited," their accreditation is from a bogus, but official-sounding agency that they created. You can use the Internet to check if a school is accredited by a legitimate organization at the database of accredited academic institutions posted by the U.S. Department of Education at www.ope.ed.gov/accreditation or at the Council for Higher Education Accreditation database at www.chea.org/search. (There are a few legitimate institutions that have not pursued accreditation.)

Look out for sound-alikes. Some diploma mills take on names that are very similar to well-known colleges or universities; a ".edu" Web address is no guarantee of legitimacy, either. Keep in mind that some diploma mills use credible-sounding foreign names. Researching the legitimacy of a foreign school can be a challenge, but is clearly worth the time. If you're having a tough time checking out a particular school, call the registrar of a local college or university and ask if it would accept transfer credits from the school you are considering.

So how can you tell if the institution you're thinking about is legitimate? Here are some tell-tale signs of a diploma mill:

- **No Studies, No Exams — Get a Degree for Your Experience.** Diploma mills grant degrees for "work or life experience" alone. Accredited colleges may give a few credits for specific experience pertinent to a degree program, but not an entire degree.
- **No Attendance.** Legitimate colleges or universities, including online schools, require substantial course work.
- **Flat Fee.** Many diploma mills charge on a per-degree basis. Legitimate colleges charge by the credit, course, or semester, not a flat fee for an entire degree.
- **No Waiting.** Operations that guarantee a degree in a few days, weeks, or even months aren't legitimate. If an ad promises that you can earn a degree very quickly, it's probably a diploma mill.
- **Click Here To Order Now!** Some diploma mills push themselves through aggressive sales tactics. Accredited colleges don't use spam or high-pressure telemarketing to market themselves. Some diploma mills also advertise in newspapers, magazines, and on the Web.

Oregon Office of Degree Authorization

- Oregon is somewhat unusual in that it has an Office of Degree Authorization (see <http://www.osac.state.or.us/oda/>) which works to combat the non-disclosed use of unaccredited degrees. It is thus not uncommon to see items such as:

State likely to pull Burright's police certifications

CORVALLIS — Jack Burright, a former sheriff candidate who was fired from the Benton County Sheriff's Office last year for providing false information in his personnel file, now is likely to lose his police certifications.
[* * *]

During a routine check of candidates' credentials in May 2006, the Gazette-Times discovered discrepancies in Burright's personnel file, which included statements by Burright that he was a graduate of Corvallis High School, and had a college degree from Farington University. In truth, Burright dropped out of CHS and later earned a GED.

Farington University is not an accredited institution of higher learning but a degree mill, where people can purchase diplomas. Using this kind of degree as a credential is illegal in Oregon. [article continues]

[www.dhonline.com/articles/2007/11/21/news/local/4loc05_burright.txt]⁶

Example Diploma Mill Criminal Conviction

Spokane – United States Attorney James A. McDevitt announced that Dixie Ellen Randock, age 58, Heidi Kae Lorhan, age 41, and Roberta Markishtum, age 40, all residents of the greater Spokane area, were sentenced yesterday for their roles in conducting a diploma mill with sales worldwide.

Dixie Ellen Randock was sentenced to a 36 month term of imprisonment, followed by 3 years of court supervision; her daughter, Heidi Kae Lorhan was sentenced to 12 months and one day imprisonment, followed by 2 years of court supervision; and Roberta Markishtum was sentenced to a 4 month term of imprisonment followed by 1 year of court supervision.

Steven Karl Randock, Sr., Blake Allan Carlson, Kenneth Wade Pearson, Richard John Novak, and Amy Leann Hensley will be sentenced at a later date.

According to the plea agreements, from August 1999, until August 2005, Dixie Ellen Randock, Steven Karl Randock, Sr., Heidi Kae Lorhan, Roberta Lynn Markishtum, Kenneth Wade Pearson, Richard John Novak, Blake Alan Carlson, and Amy Leann Hensley operated an internet-based diploma business selling false and fraudulent academic products. These products included high school degrees, college and graduate-level degrees (e.g., Bachelor of Arts, Bachelor of Sciences, Master of Arts, Master of Sciences, and Doctor of Philosophy), fabricated academic transcripts, and “Professorships.” During this period, the diploma business sold approximately \$6,282,679 of fraudulent academic products to over nine thousand individuals located in the United States and elsewhere.

They created numerous fictitious institutions such as: Saint Regis University; James Monroe University; Robertstown University; Holy Acclaim University; Ameritech University; Fort Young University; Pan America University; All Saints American University; American Capital University;

Fake degrees help terrorists skirt immigration, lawmakers say

By Wilson P. Dizard III

Published on December 10, 2007

Worthless university degrees "conferred" by criminal rings that help dupes and wrongdoers obtain fraudulent credentials have played a part in foreign terrorists' plots to skirt federal immigration and visa laws, say backers of a bill pending in Congress that would crack down on the practice.

Earlier exposes of the wide extent of degree mill abuses committed by federal technologists, first reported in [Government Computer News](#), led to the exposure of credential misrepresentation by one senior Homeland Security Department official, who lost the No. 2 job in the department's Chief Information Officer's Office, in addition to credential fakery by dozens of other government information technology employees.

That award-winning, yearlong series of stories prompted two federal investigations, a Senate hearing and changes in the government's methods of evaluating higher-education credentials. Attention now has been focused on the prosecution of a fake degree ring centered in Spokane, Wash.

Rep. Betty McCollum (D-Minn.) and eight other Democrats in the House have sponsored the Diploma Integrity Protection Act as the first federal legislation since the creation of the Internet to directly confront the problem of fraud related to diploma mills.

The House Education and Labor Committee unanimously approved a major higher-education bill that includes McCollum's language Nov. 15. The bill, H.R. 4137 or the College Opportunity and Affordability Act of 2007, serves as a catchall vehicle for

2. (g) "Free" Product and Service Offers

Major Online Advertiser Settles FTC Charges. "Free" Gifts Weren't Free; Settlement Calls for \$650,000 Civil Penalty

A large online advertiser that drove traffic to its Web sites using spam e-mails with misleading subject lines has agreed to settle Federal Trade Commission charges that it failed to disclose that consumers have to spend money to receive the so-called "free" gifts it offers. The settlement, filed by the Department of Justice on behalf of the FTC, requires the defendant to disclose the costs and obligations to qualify for the advertised "gifts," and bars it from sending e-mail that violates the CAN-SPAM Act. The settlement also requires that the company pay \$650,000 in civil penalties.

According to the FTC, Adteractive, Inc., doing business as FreeGiftWorld.com and SamplePromotionsGroup.com, used deceptive spam and online advertising to lure consumers to its Web sites. For example, Adteractive used e-mail subject lines such as, "Test and keep this Flat-Screen TV," "Test it – Keep it – Microsoft Xbox 360," and "Congratulations! Claim Your Choice of Sony, HP or Gateway Laptop." Similarly, Adteractive's banner ads and pop-up ads contained claims such as, "Participate Now and You'll Receive a FREE SONY PLAYSTATION."

When consumers arrive at Adteractive's promotional Web pages, they are led through a series of ads for goods and services from third parties. To "qualify" for their "free gifts," consumers must first wade through pages of "optional" offers. If they clear this hurdle, they discover that they must "participate in" a series of third-party promotions. Participation in these promotions requires consumers to do such things as purchase products, take out a car loan, subscribe to satellite television service, or apply for multiple credit cards.

<http://www.ftc.gov/opa/2007/11/free.shtm>

Homework/In-Class-work

- Bearing in mind the description from the preceding slide, Google for

"free laptop" or

"free wii" or

"free plasma tv"

and see what you discover.

- **Note:** I would **NOT** recommend actually visiting any sites offering any "free" major prize of this sort nor should you provide **any** personal information to any site offering "free" prizes of this sort. Why? Well...
 - visiting such a site may result in your computer being infected with malware
 - and if you provide your email address, you may end up inundated with spam
 - you will be pressured to sign up for economically crazy “offers”
 - the likelihood that you will ever get your “free” prize is nil

Another “Free Product” Scam Variant

- Another example of a common “free product” scam involves a two week “free trial” of a product (such as an “herbal weight loss aid”):
 - Users sign up for a “fourteen day” “free trial” of a product, paying only a nominal shipping and handling fee via their credit card (note that the cost of the product is typically only pennies, so even just the shipping and handling fee still yields a profit for the scammer)
 - The “free trial period” commences at the time the product is ordered; shipping time may consume a week or even more of that “trial period”
 - If the “trial” isn’t cancelled within the trial period, the customer is automatically charged for the cost of the “free trial” product
 - Making matters worse, the customer then begins to receive additional shipments of the product at absurd prices via “negative option rebilling”
 - The seller insures that it is difficult or impossible to cancel
 - If shipments are refused, they aren’t credited to the “member’s” account
 - The product itself doesn’t deliver whatever magic was claimed for it
 - This continues until the victim cancels their credit card
 - The victim’s email address and phone number is also sold to other scammers

2. (h) Bogus Diet Patches and Other Dubious Health-Related Products

FTC Case Against Phoenix Avatar

The FTC charged Phoenix Avatar and its Detroit-based principals with sending illegal spam to sell bogus diet patches. Consumers who wanted to purchase the products clicked on a hyperlink in the message and were connected to one of the defendants' many Web sites. The agency alleges the defendants were earning nearly \$100,000 per month from product sales. The FTC alleges that the claims made for these diet patches are false and that the patches, which sell for \$59.95, will have no effect at all.

The spammers hoped to obscure their identities by using innocent third party e-mail addresses in the "reply-to" or "from" fields of their spam – a practice known as spoofing. When spam was undeliverable and bounced back, tens of thousands of undelivered e-mails bounced to unwitting third parties, sometimes getting the third parties mislabeled as spammers, themselves. The spam did not offer consumers the ability to opt-out of receiving future e-mail.

The agency charged that the deceptive claims violate the FTC Act and that the spoofing and failure to provide an opt-out capability violate provisions of the recently enacted CAN-SPAM Act. At the FTC's request, U.S. District Court Judge James F. Holderman entered a Temporary Restraining Order requiring an end to illegal spamming and deceptive product claims and freezing the defendants' assets.

<http://www.ftc.gov/opa/2004/04/040429canspam.shtm>

FDA and Johnson & Johnson Warn Public About Counterfeit Contraceptive Patches Sold Through Foreign Internet Site

FDA and Johnson & Johnson of Raritan, NJ are warning the public about an overseas internet site selling counterfeit contraceptive patches that contain no active ingredients. These counterfeit patches provide no protection against pregnancy.

This internet site's domain name, www.rxpharmacy.ws apparently is operated by American Style Products of New Delhi, India. The site also sells other products that purport to be versions of FDA-approved drugs. FDA is investigating these other products as well, and urges consumers to treat any drugs purchased from this firm as being suspect. None of these products should be considered safe or effective. Consumers who have any of these products should not use them, but instead contact their healthcare providers immediately.

"FDA will continue to do all it can to protect Americans from unsafe and counterfeit drugs purchased from illegal foreign sites," said FDA Commissioner Mark B. McClellan, M.D., Ph.D. "This case highlights the serious risks posed by foreign drug operations that bypass FDA safeguards. People are risking their health, in some cases their very lives, by buying illegal internet drugs."

To protect the public health FDA has obtained the cooperation of the U.S.-based internet service provider in shutting down service to this site.

The counterfeit contraceptive patches were promoted as Ortho Evra transdermal patches, which are FDA approved, and made by Johnson & Johnson's Ortho-McNeil Pharmaceutical, Inc. subsidiary.

Instead customers receive packages of patches without the active ingredient necessary to make the patches effective. Moreover, the counterfeits are sent in simple plastic zip-lock bags without identifying materials, lot numbers, expiration dating or any other labeling information needed to safely and effectively use this prescription product.

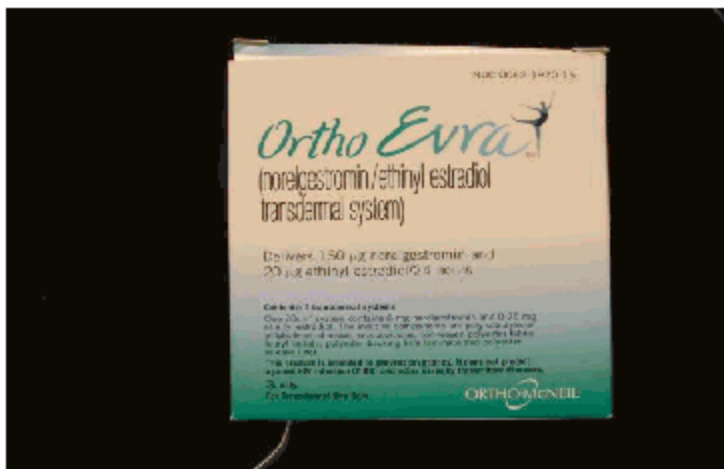
<http://www.fda.gov/bbs/topics/NEWS/2004/NEW01017.html>



Authentic Ortho Evra Transdermal Patch



Counterfeit Contraceptive Patches



Packaging for Authentic Ortho Evra Transdermal Patch



Counterfeit Contraceptive Patch

Super scam me

Some see them as a joke, a few even take them at their word, but to most of us spam e-mails that promise to "enlarge your manhood" have become an everyday pest. Simon Cox, of Radio 4's the Investigation, set out to discover who is behind them.

Would you like your penis enlarged? It is a question I get asked a lot.

Not by women, thankfully, but in the e-mails I receive every morning. For just \$70, I could open up "new exciting horizons of sensual pleasure" and put an end to "being shy of [my] manhood in the showers".

If it was only me, I might develop a complex. But billions of these junk e-mails are being sent out advertising the wonders of Manster, herbal pills that guarantee to add "intimate inches".

A similar strain of spam extols the virtues of "herbal Viagra" or "miracle breast improvement" products.

They are probably one of the most intense spam operations on the internet today

Richard Cox, Spamhaus

It would be tempting to think no-one responded to such offers. Quite the opposite, says Brian McWilliams, who managed to access the file directory of a spammers' website.

"There were orders from veterinarians and doctors," says Mr McWilliams, author of Spam Kings, "... people who I think would be sophisticated and unlikely to want to give out their credit card number to a website that had no contact information".

In a bid to track down the elusive figures sending me these spam e-mails, I had to try to buy the product. I clicked on a link in one of the e-mails, which led to an Elite Herbal website.

Elite Herbal is the biggest spammer of them all, says Richard Cox of the internet monitoring organisation Spamhaus.

"They are probably one of the most intense spam operations on the internet today," says Mr Cox, who calls them an "absolute pest".

Trail to India

<http://news.bbc.co.uk/1/hi/magazine/7140449.stm> (13 December 2007)

Alleged spam man exposed

A Christchurch businessman alleged to be the source of millions of emails offering sexual enhancement pills has become the first person in New Zealand to be raided under tough new anti-spam laws.

The man had been identified by a Danish spambuster.

Department of Internal Affairs (DIA) spokesman Trevor Henry said the department had been investigating the international spam operation but was forced into action when the BBC in Britain identified the New Zealand connection in a news report on Friday.

On Monday, DIA inspectors obtained search warrants and made four simultaneous raids on Christchurch properties, seizing 22 computers and boxes of documents.

On Tuesday, they spoke to two men who they described as "businessmen" but declined to identify.

They were now assessing the evidence before deciding what action to take. The raids were the first since New Zealand's anti-spam law took effect in September, bringing in fines of up to \$500,000 for an organisation or \$200,000 for an individual.

In August 2003, the Christchurch businessman named by the Danish spambuster told The Press the spamming business paid well, and claimed to have had sales of \$300,000 in the previous eight months.

"When you look at it, most men are willing to spend a couple of hundred bucks if they think it will give them a few more inches down there," he said, referring to penis-enlargement products.

"What man doesn't want that? So, yes, it is a good business."

The alleged spammer, then described as a father of two and former hospitality worker, said he had 15 different types of American-made penis-enlargement pills, with the spam emails being channelled through servers in Poland and Pakistan.

He said he had had "plenty of death threats", but was unapologetic about the impact on recipients, adding: "If you don't want to receive spam, don't connect to the internet, or don't have an email address."

<http://www.stuff.co.nz/stuff/4330134a28.html> (20 Dec 2007)

2. (i) Bogus Charity Sites Soliciting Donations

BROTHERS WHO OPERATED FRAUDULENT SALVATION ARMY WEBSITE AFTER KATRINA SENTENCED TO PRISON

(HOUSTON, TX) - Two brothers convicted of multiple counts of wire fraud and aggravated identify theft as the result of fraudulently operating a website that purported to raise money on behalf of the Salvation Army for Hurricane Katrina victims have been sentenced to prison, United States Attorney Don. DeGabrielle announced today.

Steven Stephens, 24, and Bartholomew Stephens, 27, were sentenced today by U. S. District Judge David Hittner. At this morning's hearing, the Court found that the Stephens brothers used sophisticated means to promote and conceal their internet fraud <mailto:www.salvationarmyonline@yahoo.com>, and that more than 250 persons were victims of the scheme. Judge Hittner sentenced Steven Stephens to a 63 month prison term on each of his six convictions for wire fraud, with each of those sentences to be served concurrently. Bartholomew Stephens was sentenced to concurrent 57 month prison terms on each six wire fraud convictions. In addition, both Stephens brothers were sentenced to mandatory two-year sentences for each of their two aggravated identity theft convictions. Each of these two mandatory sentences are to be served consecutive to each other and to the sentences imposed for their wire fraud convictions. Steven Stephens will thus serve a total of 111 months in federal prison. Bartholomew Stephens will serve a total of 105 months in federal prison. All federal prison terms are served without the benefit of parole.

Judge Hittner reserved the issue of restitution for a possible hearing within the next ninety days. Upon completion of their prison terms, each brother must also serve a three-year term of supervised release. Steven and Bartholomew Stephens have been in federal custody since their convictions in June 2007.

A jury convicted Steven and Bartholomew Stephens after a four-day trial in June. The evidence during the trial proved that the brothers registered www.salvationarmyonline.org on September 3, 2005, less than a week after Hurricane Katrina struck New Orleans. The website stated that it was "The Salvation Army International Home Page" and falsely purported to solicit charitable donations for Hurricane Katrina (and later Hurricane Rita) relief. A link on the website directed those wishing to donate to PayPal, a service that allows for online money transfers. The defendants created numerous accounts with PayPal, such as

2. (j) Phishing, Carding and Money Laundering

- "Phishing is a form of online identity theft that employs both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e- mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as account usernames and passwords. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. **Technical subterfuge** schemes plant **crimeware** onto PCs to steal credentials directly, often using key logging systems to intercept consumers online account user names and passwords, and to corrupt local and remote navigational infrastructures to misdirect consumers to counterfeit websites and to authentic websites through phisher-controlled proxies that can be used to monitor and intercept consumers' keystrokes."

http://www.antiphishing.org/reports/apwg_report_sept_2007.pdf at pdf page 1



Members of the theft ring managed to steal \$70 million. **View:** Wanted poster of suspects.

Cyber Banking Fraud

Global Partnerships Lead to Major Arrests

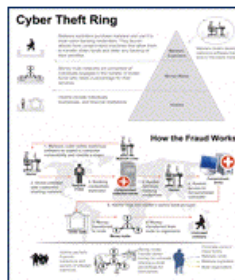
10/01/10

The cyber thieves were smart. Instead of targeting corporations and large banks that had state-of-the-art online security, they went after the accounts of medium-sized companies, towns, and even churches. Before they were caught, members of the theft ring managed to steal \$70 million.

Today, with our law enforcement partners in the United States, the United Kingdom, Ukraine, and the Netherlands, we announced the execution of numerous arrests and search warrants in multiple countries in one of the largest cyber criminal cases we have ever investigated.

"This was a major theft ring," said Gordon Snow, assistant director of the FBI's Cyber Division. "Global criminal activity on this scale is a threat to our financial infrastructure, and it can only be effectively countered through the kind of international cooperation we have seen in this case."

Using a Trojan horse virus known as Zeus, hackers in Eastern Europe infected computers around the world. The virus was carried in an e-mail, and when targeted individuals at businesses and municipalities opened the e-mail, the malicious software installed itself on the victimized computer, secretly capturing passwords, account numbers, and other data used to log into online banking accounts.



Red-slashed individuals are believed to have been captured or surrendered per <http://www.fbi.gov/wanted/alert/federal-cyber-crime-charges/view>

Carding and Money Laundering

“The corporate defendant WESTERN EXPRESS INTERNATIONAL, INC., through its managerial agents VADIM VASSILENKO, YELENA BARYSHEVA, and TETYANA GOLOBORODKO, provided financial services designed to conceal the source and destination of funds earned through the trafficking of stolen credit card numbers and other personal identifying information, as well as the identity of individuals engaged in such transactions. They used conventional banks and money transmitters to move large sums of money for their clients, thus permitting their clients to remain anonymous and insulated from reporting requirements. They also provided information and assistance to other members of the group through the WESTERN EXPRESS websites Dengiforum.com and Paycard2000.com.

“The investigation revealed that, in a four year period, over \$35 million flowed through numerous bank accounts set up by WESTERN EXPRESS.

[* * *]

“The Western Express Cybercrime Group is responsible for over \$4 million worth of identified credit card fraud, and trafficked in well over 95,000 stolen credit card numbers.”

The “Dark Market” Carding Forum

For Immediate Release
October 16, 2008

Washington D.C.
FBI National Press Office
(202) 324-3691

FBI Coordinates Global Effort to Nab ‘Dark Market’ Cyber Criminals

***Joint Two-Year Undercover Operation Results in 56 arrests; \$70 million
in Economic Loss Prevention***

The FBI, in conjunction with many partners in international law enforcement, today announced the conclusion of a two-year undercover operation targeting members of the online “carding” forum known as Dark Market.

Cyber criminals using this forum represented a virtual transnational criminal network spanning numerous countries who were involved with the buying and selling of stolen financial information including credit card data, login credentials (user names and passwords), as well as equipment used in carrying out certain financial crimes. At its peak the Dark Market website had over 2,500 registered members.

A primary objective of this operation was to infiltrate the forum, develop intelligence on its leading members, and in coordination with our U.S. and international law enforcement partners, systematically identify, locate, and arrest them over a sustained period. This operation resulted in 56 arrests worldwide. Additionally, \$70 million in economic loss was prevented from the seizure of compromised victim accounts. Separate from these successes, this operation created new leads and more investigative information to pursue. These efforts are being followed up by the FBI and international law enforcement partners.

<http://www.fbi.gov/pressrel/pressrel08/darkmarket101608.htm>

Some Additional Documents Well Worth Reading

- For a nice analysis of the carding economy, see: “An Inquiry Into the Nature And Causes of the Wealth of Internet Miscreants,” <http://www.icir.org/vern/papers/miscreant-wealth.ccs07.pdf>
- For an excellent discussion of how cyber criminals move their ill gotten gains around, see the “U.S. Money Laundering Threat Assessment,” www.ustreas.gov/offices/enforcement/pdf/mlta.pdf
- And for an extended book length treatment of phishing, carding and identity theft, see Byron Acohido and Jon Swartz’s “Zero Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity,” Union Square Press, April 2008. (Byron and Jon are USA Today reporters)

“But How Do Miscreants Collect Debit Card Numbers and PINs?” Many Ways, Including...

- The University of Texas has an excellent series of photos showing how a low profile skimmer (surreptitious card reader) plus digital camera are concealed on a genuine ATM machine. For example:



See: http://www.utexas.edu/police/alerts/atm_scam/

2. (k) Pump-and-Dump Stock Fraud

"Pump and dump" schemes, also known as "hype and dump manipulation," involve the touting of a company's stock (typically microcap companies) through false and misleading statements to the marketplace. After pumping the stock, fraudsters make huge profits by selling their cheap stock into the market.

Pump and dump schemes often occur on the Internet where it is common to see messages posted that urge readers to buy a stock quickly or to sell before the price goes down, or a telemarketer will call using the same sort of pitch. Often the promoters will claim to have "inside" information about an impending development or to use an "infallible" combination of economic and stock market data to pick stocks. In reality, they may be company insiders or paid promoters who stand to gain by selling their shares after the stock price is "pumped" up by the buying frenzy they create. Once these fraudsters "dump" their shares and stop hyping the stock, the price typically falls, and investors lose their money.

<http://www.sec.gov/answers/pumpdump.htm>

SEC Suspends Trading Of 35 Companies Touted In Spam Email Campaigns -- Investor Protection Agency Unveils "Operation Spamalot"

Washington, D.C., March 8, 2007 - The Securities and Exchange Commission this morning suspended trading in the securities of 35 companies that have been the subject of recent and repeated spam email campaigns (see examples). The trading suspensions - the most ever aimed at spammed companies - were ordered because of questions regarding the adequacy and accuracy of information about the companies.

The trading suspensions are part of a stepped-up SEC effort - code named "Operation Spamalot" - to protect investors from potentially fraudulent spam email hyping small company stocks with phrases like, "Ready to Explode," "Ride the Bull," and "Fast Money." It's estimated that 100 million of these spam messages are sent every week, triggering dramatic spikes in share price and trading volume before the spamming stops and investors lose their money.

[* * *]

The trading suspensions will last for ten business days.

<http://www.sec.gov/news/press/2007/2007-34.htm>

SEC Charges Two Texas Swindlers In Penny Stock Spam Scam Involving Computer Botnets

Washington, D.C., July 9, 2007 - The Securities and Exchange Commission has filed securities fraud charges against two Texas individuals in a high-tech scam that hijacked personal computers nationwide to disseminate millions of spam emails and cheat investors out of more than \$4.6 million. The scheme involved the use of so-called computer "botnets" or "proxy bot networks," which are networks comprised of personal computers that, unbeknownst to their owners, are infected with malicious viruses that forward spam or viruses to other computers on the Internet. The scheme began to unravel, however, when a Commission enforcement attorney received one of the spam emails at work.

The Commission alleges that Darrel Uselton and his uncle, Jack Uselton, both recidivist securities law violators, illegally profited during a 20-month "scalping" scam by obtaining shares from at least 13 penny stock companies and selling those shares into an artificially active market they created through manipulative trading, spam email campaigns, direct mailers, and Internet-based promotional activities. Scalping refers to recommending that others purchase a security while secretly selling the same security in the market.

[<http://www.sec.gov/news/press/2007/2007-130.htm>]

Alan Ralsky, Ten Others, Indicted In International Illegal Spamming And Stock Fraud Scheme

WASHINGTON - A federal grand jury indictment was unsealed today in Detroit charging 11 persons, including Alan M. Ralsky, his son-in-law Scott K. Bradley, and Judy M. Devenow, of Michigan, and eight others, including a dual national of Canada and Hong Kong and individuals from Russia, California, and Arizona, in a wide-ranging international fraud scheme involving the illegal use of bulk commercial e-mailing, or "spamming."

Charged in the 41-count indictment are:

Alan M. Ralsky, 52, of West Bloomfield, Michigan

Scott K. Bradley, 46, of West Bloomfield, Michigan

Judy M. Devenow, 55, of Lansing, Michigan

John S. Bown, 47, of Poway, California

William C. Neil, 45, of Fresno, California

Anki K. Neil, 36, of Fresno, California

James E. Bragg, 39, of Queen Creek, Arizona

James E. Fite, 34, of Whittier, California

Peter Severa, age unknown, of Russia

How Wai John Hui, 49, of Vancouver, Canada and Hong Kong

Francis A. Tribble, of Los Angeles, California

Appearing in court for arraignment today were defendants Scott Bradley and Judy Devenow, who were arrested today. Defendant How Wai John Hui was arrested in the Eastern District of New York on Jan. 2, 2008. The remaining defendants are being sought.

Assistant Attorney General Alice S. Fisher of the Criminal Division said, "The flood of illegal spam continues to wreak havoc on the online marketplace and has become a global criminal enterprise. It clogs consumers' email boxes with scams and unwanted messages and imposes



Department of Justice

FOR IMMEDIATE RELEASE
MONDAY, NOVEMBER 23, 2009
WWW.JUSTICE.GOV

CRM
(202) 514-2007
TDD (202) 514-1888

DETROIT SPAMMER AND THREE CO-CONSPIRATORS SENTENCED FOR MULTI-MILLION DOLLAR E-MAIL STOCK FRAUD SCHEME

WASHINGTON – Four individuals were sentenced today by U.S. District Judge Marianne O. Battani in federal court in Detroit for their roles in a wide-ranging international stock fraud scheme involving the illegal use of bulk commercial e-mails, or “spamming,” announced Assistant Attorney General of the Criminal Division Lanny A. Breuer and U.S. Attorney for the Eastern District of Michigan Terrence Berg.

Alan M. Ralsky, 64, of West Bloomfield, Mich., and Scott Bradley, 48, also of West Bloomfield, were sentenced to 51 months and 40 months in prison, respectively, for conspiring to commit wire fraud, mail fraud, and to violate the CAN-SPAM Act, and also for committing wire fraud, engaging in money laundering and violating the CAN-SPAM Act. Ralsky and Bradley were also each sentenced to five years of supervised release following their respective prison terms, and were each ordered to forfeit \$250,000 that the United States seized in December 2007.

How Wai John Hui, 51, a resident of Hong Kong and Canada, was sentenced to 51 months in prison for conspiring to commit wire fraud, mail fraud and to violate the CAN-SPAM Act, and also for committing wire fraud and engaging in money laundering. Hui was sentenced to three years of supervised release following his prison term, and agreed to forfeit \$500,000 to

3. Content/Substance-Oriented Online Crimes

This Next Set of Online Crimes All Are "Content Sensitive"

- Unlike the preceding category of crimes, where fraud was an inherent element, the crimes in this category are all "content sensitive" – to land in this category, the product or service must exist/be real, unlike the previous category, where the product/service/scam is inherently deceptive or fraudulent.
- So if the product or service isn't fraudulent, why does it show up here? Answer: **at least in some (if not all) jurisdictions, the product or service itself must be illegal.**

3. (a) Spam

- You've seen spam (unsolicited commercial email) show up as a component of some cybercrimes we've already discussed, but I think that ultimately it also deserves its own listing here, because at least in some cases bulk mail may be legal or illegal based solely on what's being sent and how it is being delivered.
- In some jurisdictions, any or all commercial email is permissible, but in other jurisdictions, such as the United States, unsolicited commercial email is regulated.
- In the US, spam is regulated by the CAN-SPAM Act (15 USC 7701) and 18 USC 1037, "Fraud and related activity in connection with electronic mail"

A Historical Artifact: The First Spam

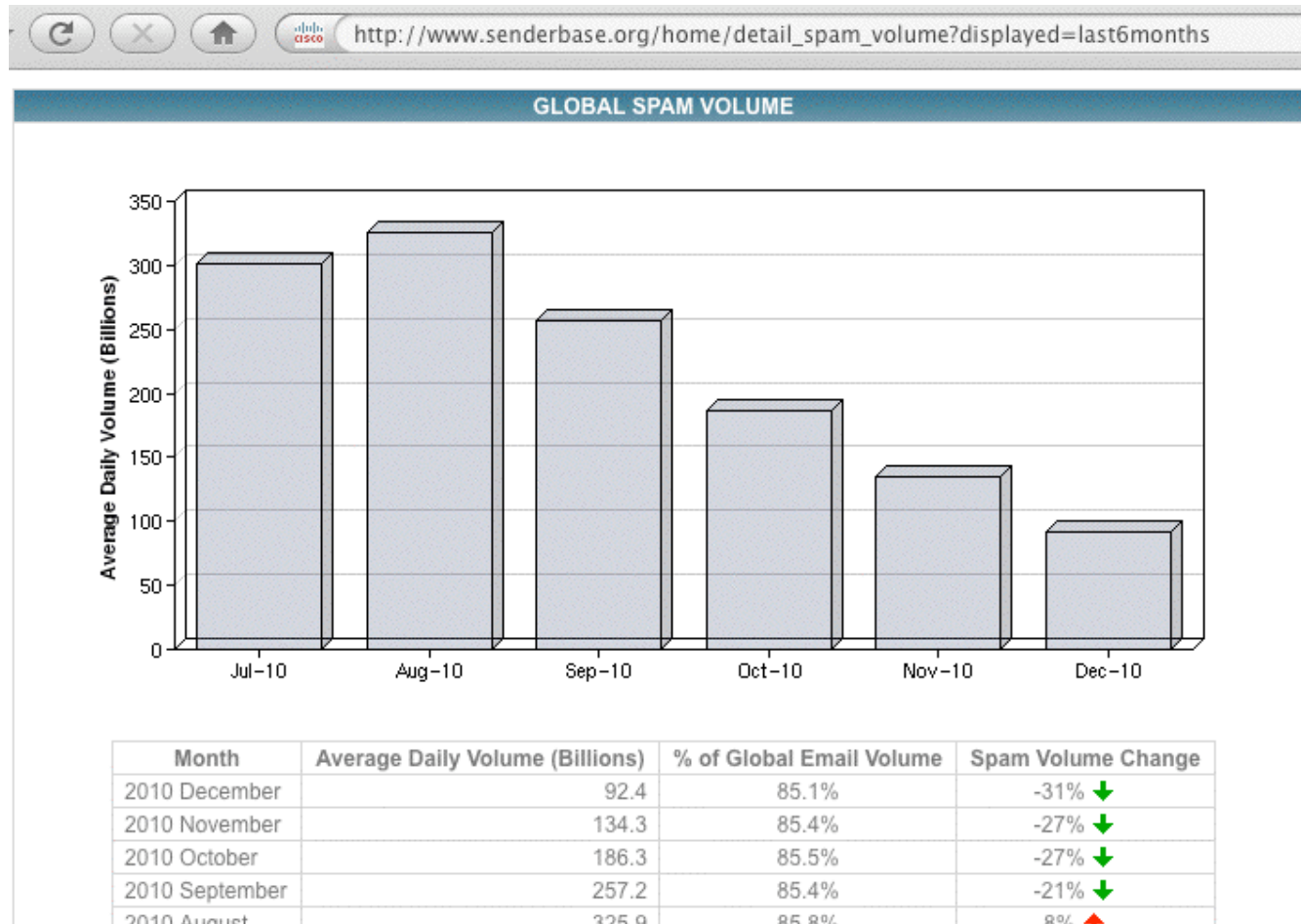
The first spam, (sent to Usenet News groups, not to email accounts, BTW).
It was sent by lawyers... Grr!

From: Laurence Canter (nike@indirect.com)
Subject: Green Card Lottery- Final One?
Newsgroups: alt.brother-jed, alt.pub.coffeehouse.amethyst
View: Complete Thread (4 articles) | Original Format
Date: 1994-04-12 00:40:42 PST

Green Card Lottery 1994 May Be The Last One!
THE DEADLINE HAS BEEN ANNOUNCED.

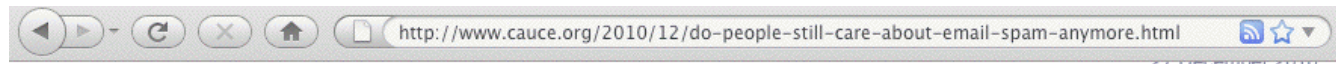
The Green Card Lottery is a completely legal program giving away a certain annual allotment of Green Cards to persons born in certain countries. The lottery program was scheduled to continue on a permanent basis. However, recently, Senator Alan J Simpson introduced a bill into the U. S. Congress which could end any future lotteries. THE 1994 LOTTERY IS SCHEDULED TO TAKE PLACE SOON, BUT IT MAY BE THE VERY LAST ONE. [continues]

Global Spam Volumes, Last Six Months



http://www.senderbase.org/home/detail_spam_volume?displayed=last6months

One Assessment of The Future of Spamming



Do People Still Care About Email Spam Anymore?

This may seem like a strange question for an anti-spam organization to ask.

CAUCE obviously still cares about email spam, and always will, but does anyone else?

If you talked to your friends or relatives over the holidays and asked them about the amount of spam they get in their inboxes, most of them may tell you that they rarely see it (even basic spam filtering on free email accounts has gotten pretty good).

When you talk to some younger people about email spam, be prepared for them to laugh.

They'll tell you that when *they* need to communicate, they'll usually use some sort of instant messaging, or maybe send text messages from their Blackberry or their iPhone. Email just isn't relevant to them any more. ("Sheesh! What will you ask about next? Faxes? Telegrams? Papyrus? Stone tablets? Get with the modern era! Who cares about stupid email?")

For all those sort of users, email is about as relevant as horse-drawn buggies. Email is archaic. They don't care about email, much less email *spam*.

Other users may tell you that they *do* care about unsolicited email, but if you probe a little, you'll find that they *really* only care about certain *types* of "spam." Everyone hates spam that might infect their computer with a virus or other malware, and many may find it creepy to get personalized phishing messages, but we empirically know that most spam *doesn't* contain malware or phishing-related content.

In fact, we even find ourselves wondering about email spammers themselves.

Do any *smart* spammers still care about email spamming? When's the last time you saw anything even relatively creative when it came to spam? I remember being impressed the first time I saw randomized image spam, and fast flux web hosting, but since then I haven't seen a whole lot in the way of spam-related developments that are very technically impressive. (I think this may be evidence that the smart spammers have already moved on to greener and more lucrative cyber crime fields.)



Sending email spam has acquired an increasingly last-decade (or last-century!) sort of feeling, sort of like being a person from the Eastern Bloc still proudly driving a rattle trap [Trabant](#). The world's moved on, even if a few Communist-era fossils haven't.

True, there are some back-of-the-pack guys who are still sending cliché spam for illegal pharmaceuticals and quick-to-break knock-off watches or untrustworthy casinos.

I'm sure it's partially a matter of inertia. If sending email spam using someone else's seldom-updated and easily detected spamware is all you really know how to do, well, I suppose that's what you're going to keep doing, even if it doesn't pay

3. (b) Scheduled Controlled Substances Sold Online Without A Bona Fide Prescription

- In the United States, the Controlled Substances Act (CSA) regulates the manufacture and distribution of narcotics, stimulants, depressants, hallucinogens, anabolic steroids, and chemicals used in the illicit production of controlled substances. See 21 USC 811.
- Substances are categorized by the CSA into five tiers, I through V:
 - Schedule I: heroin, LSD, marijuana, MDMA, peyote, psilocybin, etc.
 - Schedule II: cocaine, methamphetamine, methylphenidate, morphine, PCP, etc.
 - Schedule III: anabolic steroids, codeine/acetaminophen combinations, etc.
 - Schedule IV: alprazolam, diazepam, phentermine, zolpidem, etc.
 - Schedule V: codeine-based cough syrups, etc.See the summary table at <http://www.usdoj.gov/dea/pubs/scheduling.html>
- States can also schedule controlled substances beyond federal levels; for example, while carisoprodol ("Soma") is not a federally controlled substance at the time this was written, it **IS** scheduled by Oregon and other individual states (see http://www.deadiversion.usdoj.gov/drugs_concern/carisoprodol.htm)
- Other drugs (such as antibiotics, insulin, birth control pills, ED pills) require a bona fide prescription, but they're regulated by the FDA rather than the DEA.¹⁰⁵

Notorious Spammer And 'Drug Kingpin' Sentenced To 30 Years

A man who made about \$24 million illegally selling pharmaceuticals online and then fled the country to avoid prosecution faces 30 years in prison.

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

August 3, 2007 01:32 PM

- » [E-Mail](#)
- » [Print](#)
- » [Discuss](#)
- » [Write To Editor](#)
- » [Digg](#)
- » [Slashdot](#)
- » [News Stories](#)

A notorious spammer who made millions of dollars illegally selling medications online was hit with a 30-year prison sentence this week.

Christopher William Smith, 27, who ran Xpress Pharmacy, was sentenced in U.S. District Court in Minnesota, according to a court clerk in an interview. Assistant U.S. Attorney James Alexander told *InformationWeek* that prosecutors asked for a higher sentence because Smith made a death threat against a witness' children.

Smith was convicted last November on nine charges of conspiracy, illegal distribution of drugs, money laundering, and operating a "continuing criminal enterprise."

Going by the nickname "Rizler," Smith made about \$24 million selling medications to customers without proper prescriptions and selling drugs without a license. During his sentencing, U.S. District Judge Michael Davis called Smith a "drug kingpin," according to a [report in the Minneapolis Star Tribune](#).

Court records show that in 2005, Smith fled the country and hid out in the Dominican Republic. He went on the lam just days after federal authorities executed a search warrant on his home, seizing his passport and \$4.2 million in assets, including a \$1.1 million house and luxury vehicles worth \$1.8 million. The FBI also closed down his online operation, which employed 85 people. Soon after the search, Smith was forced to appear in federal court to face charges. He fled the country, using a false passport, a few days later.

He was eventually arrested, when he flew back into the country and touched down in the Minneapolis-St. Paul International airport.

Speaking of the sale of controlled substances...

Anabolic Steroids: Operation Raw Deal

SEP 24 [2007] WASHINGTON – DEA and federal law enforcement officials from the FDA’s Office of Criminal Investigations and the U.S. Postal Inspection Service today announced the culmination of *Operation Raw Deal*, an international case targeting the global underground trade of anabolic steroids, human growth hormone (HGH) and insulin growth factor (IGF). In addition, the investigation includes significant enforcement of illicit underground trafficking of ancillary and counterfeit medications. The investigation represents the largest steroid enforcement action in U.S. history and took place in conjunction with enforcement operations in nine countries worldwide. The Internal Revenue Service (IRS), Immigration and Customs Enforcement (ICE), Federal Bureau of Investigation (FBI), and the National Drug Intelligence Center (NDIC) also played key roles in the investigation.

143 federal search warrants were executed on targets nationwide, resulting in 124 arrests and the seizure of 56 steroid labs across the United States. In total, 11.4 million steroid dosage units were seized, as well as 242 kilograms of raw steroid powder of Chinese origin. As part of Operation Raw Deal, \$6.5 million was also seized, as well as 25 vehicles, 3 boats, 27 pill presses, and 71 weapons.

These law enforcement operations were the result of *Operation Raw Deal*, the largest steroid enforcement action in U.S. history. [continues]

[<http://www.usdoj.gov/dea/pubs/pressrel/pr092407.html>]

Forfeited: \$11.8 Million In Illegal Drug Proceeds

News Release

FOR IMMEDIATE RELEASE

November 14, 2008

Erin Mulvey

Public Information Officer

212 337-2906

Father and Son Convicted of Running Illegal Internet Pharmacy

Defendants to Forfeit a Total of \$11.8 Million in Illegal Drug Proceeds

NOV 14 -- (BROOKLYN, NY) Following four weeks of trial, a federal jury in Brooklyn today returned a verdict convicting ANTONIO QUINONES, the owner and operator of illegal internet pharmacies, of illegal distribution of prescription medication, conspiracy, and money laundering. The jury also returned a verdict convicting HERMAN QUINONES, ANTONIO's son and the owner of an illegal internet pharmacy, of illegal distribution of prescription medication. In addition, the jury ordered that ANTONIO QUINONES forfeit \$10 million in illegal proceeds that he obtained through the scheme. HERMAN QUINONES' agreed to forfeit \$1.8 million in illegal proceeds based on his conviction.

<http://www.usdoj.gov/dea/pubs/states/newsrel/2008/nyc111408p.html>

News & Events

[Home](#) > [News & Events](#) > [Newsroom](#) > [Press Announcements](#)

[Share](#) [Email this Page](#)  [Print this page](#)  [Change Font Size](#)

FDA NEWS RELEASE

For Immediate Release: Nov. 19, 2009

Media Inquiries: Karen Riley, 301-796-4674; karen.riley@fda.hhs.gov

Consumer Inquiries: 888-INFO-FDA

FDA Issues 22 Warning Letters to Web site Operators *Part of International Internet Week of Action*

The U.S. Food and Drug Administration today completed a coordinated, weeklong, international effort, called the International Internet Week of Action (IIWA), intended to curb illegal actions involving medical products.

During the effort, the FDA's Office of Criminal Investigations (OCI), in conjunction with the Center for Drug Evaluation and Research and the Office of Regulatory Affairs, Office of Enforcement, targeted 136 Web sites that appeared to be engaged in the illegal sale of unapproved or misbranded drugs to U.S. consumers. None of the Web sites are for pharmacies in the United States or Canada.

The agency issued 22 warning letters to the operators of these Web sites and notified Internet service providers and domain name registrars that the Web sites were selling products in violation of U.S. law. In many cases, because of these violations, Internet service providers and domain name registrars may have grounds to terminate the Web sites and suspend the use of domain names.

"The FDA works in close collaboration with our regulatory and law enforcement counterparts in the United States and throughout the world to protect the public," said FDA Commissioner Margaret A. Hamburg, M.D. "Many U.S. consumers are being misled in the hopes of saving money by purchasing prescription drugs over the Internet from illegal pharmacies. Unfortunately, these drugs are often counterfeit, contaminated, or unapproved products, or contain an inconsistent amount of the active ingredient. Taking these drugs can pose a danger to consumers."

The IIWA is an initiative sponsored by the International Criminal Police Organization, the World Health Organization's International Medical Products Anti-Counterfeiting Task Force, the Permanent Forum on International Pharmaceutical Crime, and national health and law enforcement agencies from 24 participating countries.

The goal of the IIWA is to protect public health by:

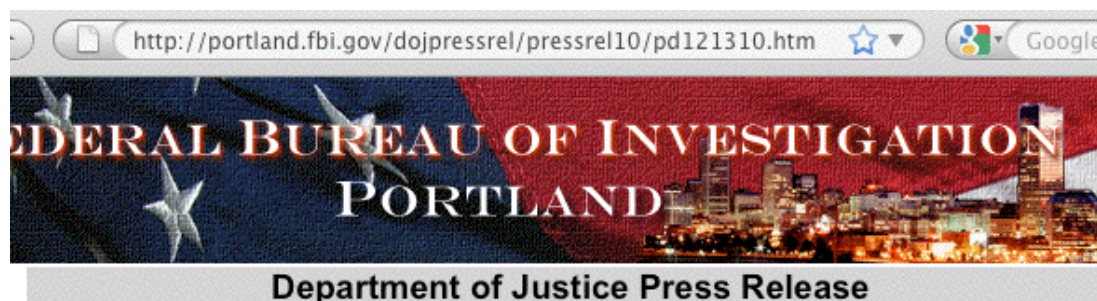
- increasing the public's awareness about the dangers and risks associated with purchasing drugs and medical devices from Web sites
- identifying producers and distributors of counterfeit and illegal pharmaceutical products and medical devices
- targeting these individuals and businesses with civil or criminal action
- seizing counterfeit and illegal products and removing them from the supply chain.

Code named Operation Pangea II, the IIWA provided an opportunity to enhance cooperation among international and domestic regulatory and law enforcement agencies to effectively combat those involved in the manufacture and distribution of illegal products.

3. (c) Child Exploitation/Child Pornography and Illegal Obscenity

- Internet porn is a multi-billion dollar-per-year industry with content ranging from the risqué to the hardcore; thus, it is hardly surprising that there is a variety of content-related cyber crimes associated with this online content area.
- In the United States, sexually explicit content is subject to federal regulation:
 - 18 USC 1466A and 18 USC 2252 prohibit child pornography
 - 18 USC 2257 levies specific record keeping requirements on the adult industry, meant to insure that all individuals appearing in sexually explicit pictures or movies are of legal age at the time the material was made
 - 42 USC 13032 requires electronic communication service providers (e.g., ISPs), to report child pornography they may discover to the National Center for Missing and Exploited Children (NCMEC)
 - plus there are additional federal, state and local laws and regulations.
- **WARNING:** Perhaps more than any other online crime related area, child porn is one area where any and **all** investigation of potentially illegal content **MUST** be left to law enforcement. If you run into a child porn site do **NOT** attempt to investigate it yourself! Instead, report it immediately to the NCMEC or the FBI's Innocent Images program (see <http://www.fbi.gov/innocent.htm>) 110

Example Child Pornography Sentence: 25 Years



For Immediate Release
December 13, 2010

United States Attorney's Office
District of Oregon
Contact: (503) 727-1000

Washington Man Sentenced to 25 Years in Prison for Producing Child Pornography

PORTLAND, OR—An Oroville, Washington man was sentenced in federal court this morning after pleading guilty to one count of producing child pornography involving a 4-year-old girl. U.S. District Judge Michael Mosman sentenced Donald Wayne George, 64, to 25 years in prison followed by a 10-year term of supervised release. George will be subject to a number of conditions of supervision, including limitations on his association with minors and his use of computers. George will also be required to participate in sex offender treatment, and will be required to register as a sex offender. George's federal sentence was imposed to run concurrently with a similar Oregon state sentence George received in Washington County following his pleas of guilty there to a variety of sex offenses involving the same minor victim.

George came to the attention of law enforcement authorities after the victim's father discovered more than 100 digital photographs depicting the victim engaging in sexually explicit conduct, many with George, who is her step-grandfather. George sexually abused the victim and created photographs of the abuse while visiting the victim's family over the course of more than one year. After discovering the photographs, the victim's father called the police and detained George until they arrived. Investigating officers seized two digital cameras, computer equipment, and sex toys, some of which were used on the victim. The victim was only 3 or 4 years old when the abuse occurred and the photographs were made.

Judge Mosman imposed the 25-year sentence after considering the federal sentencing guidelines, the nature, circumstances, and seriousness of the offense, and the need for the sentence to provide just punishment, to act as a deterrent, to promote respect for the law, and to prevent George from committing additional crimes in the future. George said nothing during the sentencing hearing.

"A Siege On the Child-Porn Market"

NEW YORK – Some of America's most powerful financial institutions have a new target - and it doesn't involve making money. For the first time, titans such as American Express, Bank of America, and Citigroup will join forces to try to thwart the use of credit cards and other financial tools to buy child pornography. A group of 18 corporate giants intends to share information, issue cease-and-desist orders to offenders, and try to expand its reach to almost every financial institution that matters. The aim: to snuff out the commercial spread of the smut by 2008.

"People say it's crazy, but I don't think it is," says Ernie Allen, president of the National Center for Missing and Exploited Children, which will act as clearinghouse for the effort. "If we can eliminate the credit-card use, the third-party payments, or any of the illegal mechanisms, we can make it a whole lot harder."

By many estimates, child pornography has mushroomed into a giant business, attracting organized crime. At least **200,000 websites sell such images**, according to Mr. Allen, and rake in from \$20 billion to \$30 billion a year. "Its use is absolutely exploding," says Allen, whose organization each week fields as many as 1,500 tips on illicit sites. [continues]

[<http://www.csmonitor.com/2006/0316/p01s03-ussc.html> ; emphasis added]¹¹²

"Operation Ore: Can the UK cope?"

The UK's largest ever police hunt against internet paedophiles - Operation Ore - has resulted in about 1,300 arrests out of a list of 6,000 suspects, but could be putting a strain on the criminal justice system. The arrest of a computer consultant in Texas led to an international criminal investigation which is putting pressure on police forces in three continents.

Thomas Reedy was jailed last year for 1,335 years for running an internet child internet porn ring which was far bigger than police had imagined.

Credit card details used to access material gave police direct leads on 250,000 people worldwide [* * *].

Last year, police in the UK complained they lack the resources to investigate all the names passed to them by the United States Postal Inspection Service (USPIS), a federal agency that investigates online paedophile activity.
[article continues]

[<http://news.bbc.co.uk/1/hi/uk/2652465.stm> emphasis added]

"Child Porn Suspects Blame Fraud"

A BBC investigation has raised concerns about the way the UK's biggest internet child porn inquiry was conducted.

Operation Ore focused on over 7,000 people whose credit cards were used to buy illegal porn from a US website.

Lawyers and computer experts have told BBC Radio 4's The Investigation that many of those arrested may have been innocent victims of credit card fraud.

Police say some on the list may have been fraud victims, but deny that any of them were subsequently prosecuted.

Lawyers and computer experts said some forces did not carry out proper checks to see if suspects arrested as part of the investigation were fraud victims.

Operation Ore was launched in May 2002 when police received the list with the names of people whose credit cards had been used to buy child pornography from a US website called Landslide Inc.

So far, 2,300 people on the list have been found guilty of offences.

But another 2,000 people spent many months under investigation before charges were dropped. [article continues]

3. (d) Warez

- "Warez" (pronounced "wearzz," NOT "wahr-ez") are pirated copies of proprietary commercial software, typically distributed over the Internet after the program's copyright protection mechanisms (if any) have been disabled. Pirated music, pirated movies and pirated games may also be distributed.
- Individuals in the warez scene may amass and freely share huge collections of programs (even if they have no personal use for particular programs) as a competitive matter or to increase their status with their peers; others may avoid an emphasis on sheer volume, focusing instead on how quickly they can get and distribute newly developed programs or particularly obscure or expensive ones.
- Others may accumulate titles to build an inventory of programs which can be sold to retail customers online. These pirates typically attempt to explain their unusually low prices (and unorthodox distribution mechanisms) by falsely claiming that the downloadable software they're selling is an "original equipment manufacturer" ("OEM") version which is inexpensive because it is being distributed without physical media, manuals or or fancy packaging. In reality, of course, that software is sold cheaply because it's been stolen.
- Stolen intellectual property may also be distributed in the form of authentic-looking physical CD or DVD copies, again typically sold at large discounts.

SOFTWARES

Intuit Quicken
Maxon Cinema for MAC
McAfee Anti-virus
Microsoft for MAC
Native Instruments
Office software
Other
Photo and Graphic Editors
Quark XPress
Rogue Amoeba
Roxio
Utilites and Programming
Video and Audio Editors
VMware

Browse by Category

NEWLY ADDED SOFTWARE

Digital Photo Maker 9 
onOne Plug-In Suite 5 
Roxio Popcorn 4 for MAC 
Roxio Toast 10 Titanium for MAC 
Snow Leopard Server 10.6 
Wing FTP Server 3 Corporate Edition 
AVG Internet Security 9 
Windows Server 2008 
Datacenter 32bit 

AutoCAD Inventor Professional Suite 2010 32 and 64 bit



Available languages versions:




Retail Price: \$7599.95

Our Price: \$249.95

You Save: \$7350

ZIP Archive - 9Mb

info / add 

AutoCAD Inventor Suite 2010 32 and 64 bit



Available languages versions:



Retail Price: \$5999.95

Our Price: \$199.95

You Save: \$5800

ZIP Archive - 9Mb

info / add 

AutoCAD Inventor Routed Systems Suite 2010 32 and 64 bit



Available languages versions:




Retail Price: \$6999.95

Our Price: \$199.95

You Save: \$6800

ZIP Archive - 9Mb

info / add 

AutoCAD Inventor Simulation Suite 2010 32 and 64 bit



Available languages versions:



Retail Price: \$6999.95

Our Price: \$199.95

You Save: \$6800

ZIP Archive - 9Mb

info / add 

3ds Max 2010 32 and 64 bit



Available languages versions:



Retail Price: \$3999.95

Our Price: \$199.95

You Save: \$3800

ZIP Archive - 6247MB

3ds Max Design 2010 32 and 64 bit



Available languages versions:



Retail Price: \$3999.95

Our Price: \$199.95

You Save: \$3800

"Justice Department Announces Seventh Guilty Plea in P2P Piracy Crackdown"

November 14, 2007 [* * *] An Duc Do, 25, of Orlando, Fla., pleaded guilty to a two-count felony information charging him with conspiracy to commit criminal copyright infringement and criminal copyright infringement in violation of the Family Entertainment Copyright Act.

Do's conviction is the seventh in a series of convictions arising from Operation D-Elite, an ongoing federal crackdown against the illegal distribution of copyrighted movies, software, games and music over P2P networks employing the BitTorrent file sharing technology. Operation D-Elite targeted leading members of a technologically sophisticated P2P network known as Elite Torrents. **In its prime, the Elite Torrents network attracted more than 133,000 members and facilitated the illegal distribution of more than 17,800 titles—including movies, software, music and games—that were downloaded over 2 million times.** The large unlimited content selection available on the Elite Torrents network often included illegal copies of copyrighted works before they were available in retail stores or movie theaters. [* * *] Do faces a maximum of 10 years in prison and a fine of \$500,000. [<http://www.cybercrime.gov/doPlea.htm>]

"First Two Defendants Plead Guilty in Largest CD Manufacturing Piracy Scheme Uncovered in U.S. to Date"

[...] the first two defendants today pleaded guilty and admitted in open court to their involvement in what the recording industry is calling the largest music manufacturing piracy seizure in the United States to date. On October 6, 2005, law enforcement conducted searches of 13 locations in California and Texas in the undercover investigation called Operation Remaster. **The FBI estimates that approximately 494,000 pirated music, software, and movie CDs, and DVDs, and more than 5,500 stampers were seized during those raids.**

The defendants, YE TENG WEN, a.k.a. Michael Wen, 30, and HAO HE, a.k.a. Kevin He, 30, both of Union City, California, today admitted to participating in a conspiracy to mass-produce pirated music and software CDs. Nearly 200,000 pirated CDs were seized at locations associated with these two individuals. Many of the pirated CDs contained counterfeit FBI AntiPiracy Seals and silk screened artwork to make them appear legitimate. [...] The copyright and trademark violations largely involved Latin music titles and Norton anti-virus software.
[press release continues]

[<http://www.usdoj.gov/criminal/cybercrime/wenPlea.htm> ; emphasis added]

3. (e) Online Sale of "Replica" (Counterfeit) Trademarked Products

- Some stats from Union des Fabricants' "Counterfeiting and Organized Crime"
<http://www.interpol.int/Public/FinancialCrime/IntellectualProperty/Publications/UDFCounterfeiting.pdf> (2003):
 - "According to European customs statistics, nearly 100 million products were seized in 2001, i.e. 39% more than in 2000. Globally, an OECD report published in 1998 estimated that counterfeiting was generating €250 billion in illegal earnings annually and represented 5 to 7% of world trade, while a press release issued by the World Customs Organisation on 27th January 2003 valued unlawful trade at €450 billion."
 - "On 9th July 2002, a consignment of 2.6 tonnes of counterfeit watches originating from Hong Kong and bound for Spain was seized at Roissy."
 - "On 24th November 2002, an attempt was made to murder Konstantin Zemenchov, head of the RAPO (Russian Anti-Piracy Organisation). Everything points to this attack being related to raids carried out a few days previously, which had led to the seizure of 117,000 pirate DVDs and 1,060,000 high-quality jackets. Shortly after the attack on Mr Zemenchov, a factory manufacturing optical disks was discovered near Moscow and 500,000 CDs were seized."

"[...] electrical cords, batteries, handbags, wallets, suitcases, shoes, hats, sunglasses, watches, key holders, umbrellas, and different items of clothing and accessories [...]"

Five Individuals Indicted for Trafficking in Counterfeit Goods


[* * *] on December 22, 2005, a federal grand jury in Miami, Florida, returned two (2) separate Indictments against five (5) individual defendants, Lizhou Shao, Changbiao Fu, Li Fen Fu, Ji Wu Chen, and Meihua Li. The grand jury Indicted the defendants on three (3) separate charges: (1) conspiring to traffic in counterfeit goods, in violation of Title 18, United States Code, Section 371; (2) trafficking in counterfeit goods, in violation of Title 18, United States Code, Section 2320(a); and (3) concealing and selling imported counterfeit goods, in violation of Title 18, United States Code, Section 545. The defendants were arraigned before U.S. Magistrate Judge Stephen T. Brown in Miami at 10:00 A.M.

The maximum statutory sentences for each count in the Indictments are: five (5) years in prison and a \$2 million fine for conspiracy to traffic in counterfeit goods; ten (10) years in prison and a \$2 million fine for trafficking in counterfeit goods; and five (5) years in prison and a \$250,000 fine for illegally concealing and selling counterfeit goods. [continues]

[<http://www.usdoj.gov/criminal/cybercrime/shaoIndict.htm>]

3(f). Sale of Untaxed Cigarettes

http://www.fbi.gov/news/stories/2011/january/cigarette_011411/cigarette_011411



Boxes of seized contraband cigarettes in a Mississippi warehouse.

Operation Secondhand Smoke Cigarette Case Yields Unexpected Results

01/14/11

When the smoke cleared from Major Case 253, a network of schemers trafficking in contraband cigarettes was dismantled, a Mississippi police department earned a new headquarters, and the FBI gained one more partner in the fight against terrorism.


Those three things might not seem related, but then again, Operation Secondhand Smoke is no ordinary case. It began—as many investigations do—when a person of interest in a criminal matter offered information about a larger criminal enterprise, a massive fraud in the cigarette industry.

Working with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the Tupelo Police Department, and the Marshall County Sheriff's Office in Mississippi, we began an undercover investigation into a nationwide network of retailers, wholesalers, distributors, importers, and manufacturers who were avoiding cigarette taxes to make millions of dollars in profits.

"The amount of criminal activity in this case to avoid taxes was just phenomenal," said Special Agent Carl Cuneo, one of the case supervisors based in our Oxford, Mississippi Resident Agency.

In the tobacco industry, the crime is known as "diverting," and it applies to those who scheme to avoid the various federal and state taxes levied on cigarette sales. Operation Secondhand Smoke involved the so-called fourth-tier market—not well-known cigarette brands, but off-labels such as those manufactured in Armenia.

Taxes represent the majority of the total retail cost of a pack or carton of cigarettes. By illegally avoiding those taxes—through schemes including hiding shipments from auditors and regulators



Asset Forfeiture Program

The asset forfeiture program is a nationwide federal law enforcement initiative administered by the Department of Justice and made possible by a 1984 congressional act designed to take the profit out of crime.

The use of asset forfeiture in federal criminal investigations aims to undermine

Thanks For the Chance To Talk Tonight!

- Are there any questions?