

A Succinct Cyber Crime Tour Meant To Illustrate By Way of Assorted Examples The Sort of Online Crimes Which Are Occurring -- And Why We Need More Cyber Crime-Trained Attorneys

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

Room 142, Knight Law School

University of Oregon

6:00-7:50PM, January 8th, 2007

<http://www.uoregon.edu/~joe/tour/>

Disclaimer: All opinions strictly my own.

Cyber Crime As An Area of Legal Specialization

- Somewhere along the line, unless you're planning on having a general law practice, **you'll need to decide on an area of specialization.** What should you choose?
- While each area of law has its own appeal and all are important, I'd like to spend a little time with you tonight explaining why **I believe you should specialize in prosecuting cyber crimes.**
- The fact that you're in Sean's class leads me to believe you already have at least a passing interest in cyber crime, but by go-home time tonight, I hope you'll decide that prosecuting cyber crime should be the center of your legal career.
- Perhaps the easiest way for me to do this is by **giving you a tour** of some online crimes, so you can see:
 - the magnitude of the cyber crime problem we face as a society,
 - the diversity of cyber crime topics involved,
 - some of the challenges which make prosecuting these cases difficult, and
 - some of the cases currently being brought against some online miscreants.
- But you may wonder, "Why did Sean ask this guy to talk with us? What's his background?"

My Background and A Disclaimer

- My Ph.D. is in Production and Operations Management from the University of Oregon School of Business, and I've been at the UO Computing Center (now Information Services) for over twenty year. I'm currently on contract with Internet2 through Information Services as a Security Programs Manager.
- I'm active in the higher education cyber security community, including serving on the Research and Education Network Information Sharing and Analysis Center (REN-ISAC) Technical Advisory Group, participating in the Educause/Internet2 Security Task Force, and this past summer I was invited to co-lead one of four breakout sessions for the Department of Energy Cyber Security Research Needs for Open Science Meeting. I routinely present at national and international events, and many of my talks are available in the form of detailed slide sets (like this one) from <http://www.uoregon.edu/~joe/>
- I also serve as one of half a dozen Senior Technical Advisors for MAAWG (the Messaging Anti-Abuse Working Group). MAAWG's an anti-spam group which represents carriers with over 600 million consumer mailboxes worldwide (as well as leading legitimate senders, anti-spam technology vendors, etc.)
- I don't have a J.D., I'm not member of the Oregon Bar, I'm not a prosecutor and I'm not a cop, so nothing I say tonight should be taken as legal advice.
- Finally, no one is responsible for any of my statements except me.

Format

- 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),
 - memorialize this session for those of your classmates who may not be able to be here with us tonight, and
 - 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 and haven't had the chance to give you any preparatory readings, 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.
- Before we dive in, though, **is cybercrime really a national LE priority?**

Federal Law Enforcement Priorities

- **"After counterterrorism and counterintelligence, cyber crime is our next priority.** Cyber investigations used to be done on an ad hoc basis in many different divisions and programs. Last year, we created a Cyber Division which consolidated responsibility for investigations involving cyber viruses, privacy invasions, child pornography on the Internet and fraudulent e-commerce. From February to May of this year alone, we have opened over 90 cybercrime investigations involving 84 thousand victims worldwide and losses exceeding \$162 million. These cases have resulted in 97 arrests and 64 separate indictments for cybercrime offenses."

Robert S. Mueller, III, Director, FBI, June 20, 2003

<http://www.fbi.gov/pressrel/speeches/npc062003.htm>

- More recently, see also Robert Mueller's November 2007 speech, "The FBI: Stopping Real Enemies at the Virtual Gates"

<http://www.fbi.gov/pressrel/speeches/mueller110607.htm>

- Based on everything I can see, cyber crime is DEFINITELY a LE priority.⁵

I. An Arbitrary Taxonomy of Cybercrimes

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
 4. Cyber Incidents Gone Awry – Why We Need Cyber Savvy Defense Attorneys, Too
- That list should catch most of the major cyber crimes that folks are worried about, EXCEPT for cyber terrorism (which I'm defining as being out of scope for this talk except as it may come up incidentally in connection with other cyber crimes)

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 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 today, and most theft-of-service crimes have evolved over time...

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



http://en.wikipedia.org/wiki/Image:Blue_Box_in_museum.jpg 10

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

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) Computer Intrusions

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.

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...
 - Disgruntled/untrustworthy (former) insiders
 - Juveniles
 - Ideologically motivated individuals
 - Sophisticated professionals

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

 [7 http://www.israelnationalnews.com/News/News.aspx/124768](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]

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.

So Much for "Two Channel" Security...

[* * *] The Star newspaper reported yesterday that an online fraud syndicate had hacked into the bank account of a Cape Town non-profit and stole R90 460 from orphans and other vulnerable children.

The Novalis Ubuntu Institute had its account hacked in mid-November, after criminals stole the identity of its CFO, Anne-Lise Bure-Shepherd. **They cancelled her SIM card and had MTN issue a replacement card, which allowed the criminals to receive a one-time password (OTP) to access the account and transfer its funds to other accounts.** [* * *]

“The breakdown in the security procedure lies with the mobile operator. The customer's cellphone SIM card gets falsely declared stolen by the fraudster at the service provider. A replacement SIM card is issued, rendering the customer's original SIM card void.

“What this means is that all security messages and codes sent to the customer by Standard Bank are sent to the fraudsters who utilise the customer's replacement SIM card. Using Standard Bank's secure OTP, the criminals were able to change and add beneficiaries and transfer money out of the customer's account using the original information obtained through the phishing compromise.”

[<http://www.itweb.co.za/sections/business/2007/0712071100.asp>]

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

The Pace of Malware Release is Accelerating

- "At the start of 2007, computer security firm F-Secure had about 250,000 malware signatures in its database, the result of almost 20 years of antivirus research. Now, near the end of 2007, the company has about 500,000 malware signatures.

"We added as many detections this year as for the previous 20 years combined," said Patrik Runald, security response manager at F-Secure.

http://news.yahoo.com/s/cmp/20071206/tc_cmp/204701370

December 5th, 2007

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: -

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!")

Multi gigabit/second DDoS attacks have been observed (see <http://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. 32

"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.
- 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. 33

Gambling Site DDoS Extortion Threats



DK Matai of MI2G, which monitors unauthorised computer hacking says criminal syndicates operating from Russia have targeted large online payment systems belong to gambling sites.

A typical criminal syndicate extortion to online gambling and payment companies would range from 'You have to pay us \$50,000 or we will start Dos attacks' to 'If you don't pay us what we want, then we'll make sure you don't have any customers'.

Several companies, with high stakes in terms of revenues or large customer base are giving in as they have revenues of over \$50,000 per week, and the damage would be more, from the Dos attacks.



Report of 31.05.2007 17:36

[<< previous](#) [next >>](#)

Estonian DDoS - a final analysis

In the aftermath of the recent distributed denial of service (DDoS) targeting Estonia, information has emerged that suggests this was not a concerted attack orchestrated by some single agency, but rather the spontaneous product of a loose federation of separate attackers. It appears to have been a statement of disapproval at the relocation of the Bronze Soldier, a memorial to the WW2 Russian Unknown Soldier, from the centre of Tallinn to a suburban cemetery. The social significance of this should not be underestimated - to the indigenous Russians the statue represents the wartime sacrifice, whereas to the native Estonians it represents Russian occupation of their country.

Data gathered by [Arbor Networks](#) showed that sources of attack were worldwide rather than concentrated in a few locations. Attack bandwidths ranged from under 10 Mbps to 95Mbps, with the majority in the range 10-30 Mbps. 75 per cent of attacks lasted no longer than one hour and only 5.5 percent, over 10 hours. However the peak global effect was of a botnet with up to 100Mbps capacity. Bearing in mind the level of IT power available in Estonia, this had a crippling effect on those services that were targeted.

Michigan Man Gets 30 Months for Conspiracy to Order Destructive Computer Attacks on Business Competitors

NEWARK, N.J. -- A Michigan man was sentenced today to 30 months in prison for conspiring to conduct highly destructive computer attacks on competitors of his online sportswear business, including a web-based New Jersey company, U.S. Attorney Christopher J. Christie announced.

U.S. District Judge Joseph E. Irenas also ordered Jason Salah Arabo, 19, of Southfield, Michigan, to make restitution of \$504,495 to his victims -- the websites he targeted as well as an Internet hosting company.

Arabo pleaded guilty today before Judge Irenas on April 12, to a one-count Information charging him with conspiracy to cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer.

In pleading guilty, Arabo acknowledged that in 2004, he ran two web-based companies, www.customleader.com and www.jerseydomain.com, that sold sports apparel, including reproductions of sports uniforms, popularly known as "retro" or "throwback" jerseys.

"Arabo's 30-month prison sentence reflects the very serious and damaging nature of the computer attacks he orchestrated," said Christie. "This case went far beyond a teenager using his computer for online pranks. We will continue to investigate and aggressively prosecute the misuse of computers to commit crime."

According to Assistant U.S. Attorney Eric H. Jaso, who prosecuted the case, Arabo admitted that in online "instant message" conversations he met a New Jersey resident, Jasmine Singh, who communicated using the online name "Pherk." Arabo learned that Singh had covertly infected some two thousand personal computers with programs that enabled him to remotely control them. Singh demonstrated to Arabo online that he could command these computers to conduct attacks, known as distributed denial of service, or "DDOS" attacks, on computer servers and disable websites supported by those servers. Arabo admitted that he asked Singh to take down the websites and online sales operations of certain of his competitors. Arabo promised to



Denial-of-Rockies-Tickets Attack

Ticket-sales system unable to thwart DDOS attack, leaving many Colorado Rockies fans empty-handed

OCTOBER 24, 2007 | Nasty hackers or just greedy ticket brokers? Either way, it's a moot point now: The Colorado Rockies sold out its World Series tickets yesterday when the team's online ticket-sales system was restored after a [distributed denial-of-service attack \(DDOS\)](#) caused a server outage on its Website on Monday.

The outage occurred as a result of some 8.5 million visits to the Rockies' Website within 90 minutes, which was more than enough to bring down servers at Rockies' ticket-sales system provider Paciolan. Bob Bowman, CEO of MLB.com, said yesterday in published reports that the attacking computers were blocked from purchasing tickets, but they continued to try to connect to the site, which eventually knocked it offline. His guess is it could have been ticket brokers.

Whether the DDOS was malicious or inadvertent, the outcome was the same. "Most DDOS attacks appear to be just customers" coming to the site, says Richard Stiennon, chief marketing officer at Fortinet. "They were unprepared for the onslaught... of getting all of those transactions at once."

The Rockies, which will face the Boston Red Sox tonight in Game 1 of the Colorado club's first-ever World Series, had decided to open up ticket sales worldwide with online sales. The club sold over [50,000 tickets](#) in about two and a half hours after the site went back online yesterday, according to published reports. About 80 percent of the transactions were made by buyers with Colorado zip codes.

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>

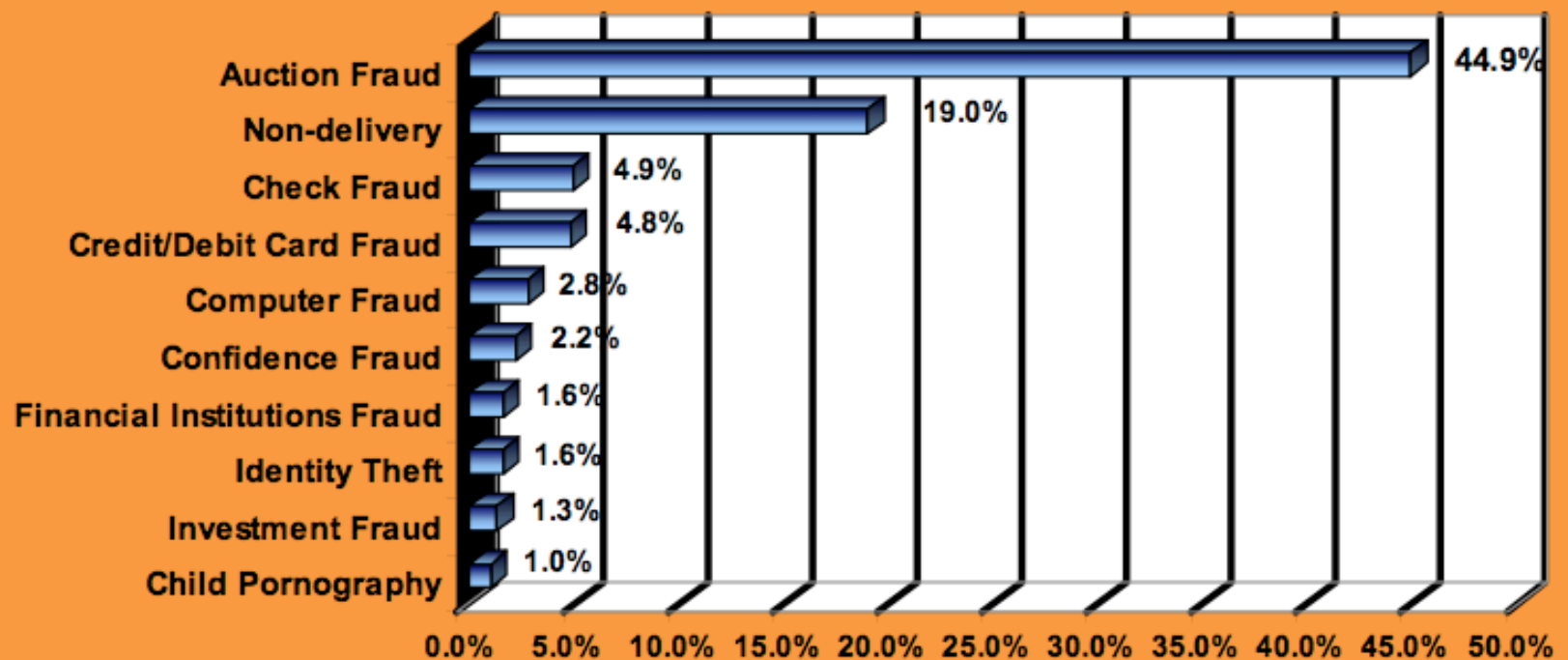
2. (a) Internet Auction Fraud

- "In 2006, IC3 [the FBI's Internet Crime Complaint Center] processed more than 200,481 complaints that support Internet crime investigations by law enforcement and regulatory agencies nationwide. [* * *] **Internet auction fraud was by far the most reported offense**, comprising 44.9% of referred complaints. [* * *]

"Statistics contained within the complaint category must be viewed as a snapshot which may produce a misleading picture due to the perception of consumers and how they characterize their particular victimization within a broad range of complaint categories. It is also important to realize IC3 has actively sought support from many key Internet E-Commerce stake holders. **As part of these efforts, many of these companies, such as eBay, have provided their customers links to the IC3 website. As a direct result, an increase in referrals depicted as auction fraud has emerged.**"

2006 Internet Crime Report, [FBI] Internet Crime Complaint Center,
http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf
at pdf pages 3 and 7, emphasis added.

**Chart 5 -- 2006 Top 10 IC3 Complaint Categories
(Percent of Total Complaints Received)**



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 terms related to fishing boats can be seen on the next page...

<u>Keywords</u>	<u>Estimated Ad Position</u> <small>?</small>	<u>Estimated Avg. CPC</u> <small>?</small>	Match Type: <small>?</small> Broad <small>▼</small>
fishing boats	1 - 3	\$0.37	Add <small>↕</small>
small fishing boats	1 - 3	\$0.46	Add <small>↕</small>
fishing boats for sale	1 - 3	\$0.41	Add <small>↕</small>
used fishing boats	1 - 3	\$0.39	Add <small>↕</small>
aluminum fishing boats	1 - 3	\$0.38	Add <small>↕</small>
sport fishing boats	1 - 3	\$0.39	Add <small>↕</small>
bass fishing boats	1 - 3	\$0.40	Add <small>↕</small>
fishing boat	1 - 3	\$0.37	Add <small>↕</small>
charter fishing boats	1 - 3	\$0.42	Add <small>↕</small>
aluminum fishing boat	1 - 3	\$0.40	Add <small>↕</small>
commercial fishing boats	1 - 3	\$0.37	Add <small>↕</small>
fishing boat for sale	1 - 3	\$0.38	Add <small>↕</small>
charter boat fishing	1 - 3	\$0.42	Add <small>↕</small>
fishing boat rentals	1 - 3	\$0.34	Add <small>↕</small>
small fishing boat	1 - 3	\$0.43	Add <small>↕</small>
party boat fishing	1 - 3	\$0.35	Add <small>↕</small>
lund fishing boats	1 - 3	\$0.36	Add <small>↕</small>

PPC Gone Awry

- Thus, every time you click on a top-rated PPC ad for a boat, it costs someone just under half a buck. Of course, if a visitor ends up buying a boat from you after clicking on your ad, that's fifty cents 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.



PLAN b

Color Laser Printers and All-In Ones that give you more.



Starting around \$399

Learn more

brother At your side.

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

2. (c) Nigerian Advanced 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...

- **Attorney General Hardy Myers announced how to respond to Nigerian advance fee scheme** [August 8, 2002]

Attorney General Hardy Myers today announced how best to respond to increasing occurrences of "advance fee fraud." The most common of these schemes is the "Nigerian advance fee fraud" which is circulated through electronic mail, ground mail and facsimile. There is, however, a wide range of similar scams that have victimized Oregonians.

These schemes, which are also known as 4-1-9 frauds (based on the section of the Nigerian penal code that addresses fraudulent activity) [...]

Profits for Nigerian swindlers have increased over the past several years, despite significant efforts by federal, state and local authorities to alert citizens to the fraudulent activities. The U.S. Secret Service indicates that the scam is targeted towards middle and upper income individuals, and those with access to business or work-related bank accounts. **In the past three years, U.S. citizens have been victimized for over \$100 million.**

<http://www.doj.state.or.us/releases/2002/rel080902.shtml>

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.

Even Harder to Believe...

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>

"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.

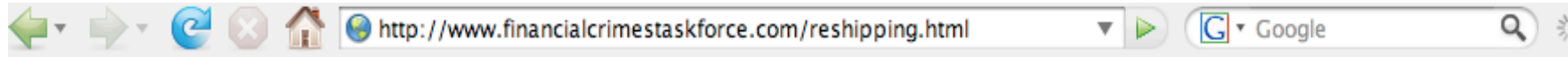
Owoh became a well known star within the Nigerian film industry, sometimes colloquially known as Nollywood because of its trite plots, poor dialogue, terrible sound, and low production standards.

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]

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.**

2. (e) "High Yield Investment Programs"

- Well-known banks and credit unions in the Eugene-Springfield area are currently paying 0.10%-0.50% (one tenth of one percent to half of one percent) per year on regular 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

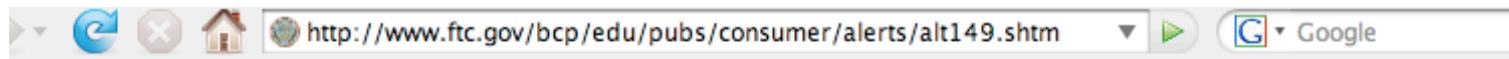
SEC v. Zahra Ghods and RUSA Cap., Inc., Defendants, & Unisource Cap., LLC, Relief Defendant, Civ. Act No. 1:07-CV-1047 (NDGA May 8, 2007)

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 Scam



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 Burrigh's police certifications

CORVALLIS — Jack Burrigh, 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 Burrigh's personnel file, which included statements by Burrigh that he was a graduate of Corvallis High School, and had a college degree from Farington University. In truth, Burrigh 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_burrigh.txt]⁹

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

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.

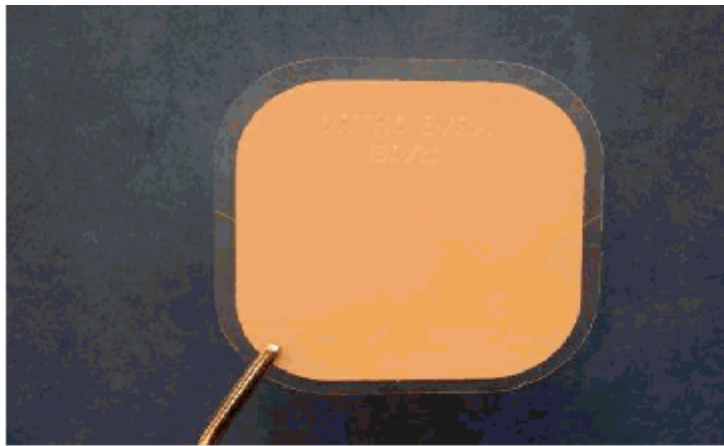
"FDA will continue to do all it can to protect Americans from unsafe and counterfeit drugs purchased from illegal foreign sites," said FDA Commissioner Mark B. McClellan, M.D., Ph.D. "This case highlights the serious risks posed by foreign drug operations that bypass FDA safeguards. People are risking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

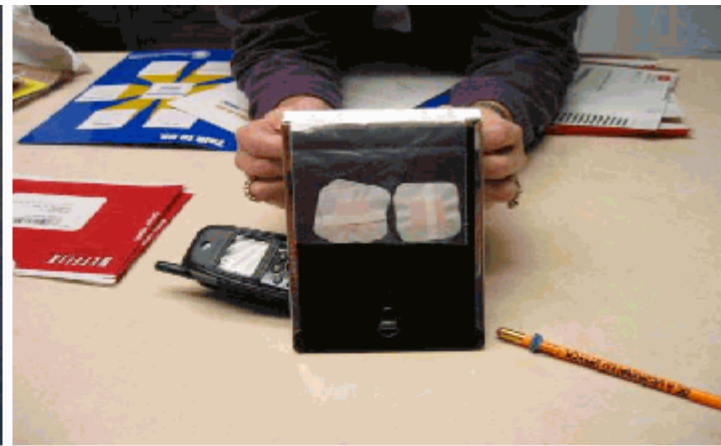
The counterfeit contraceptive patches were promoted as Ortho Evra transdermal patches, which are FDA approved, and made by Johnson & Johnson's Ortho-McNeil Pharmaceutical, Inc. subsidiary.

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.

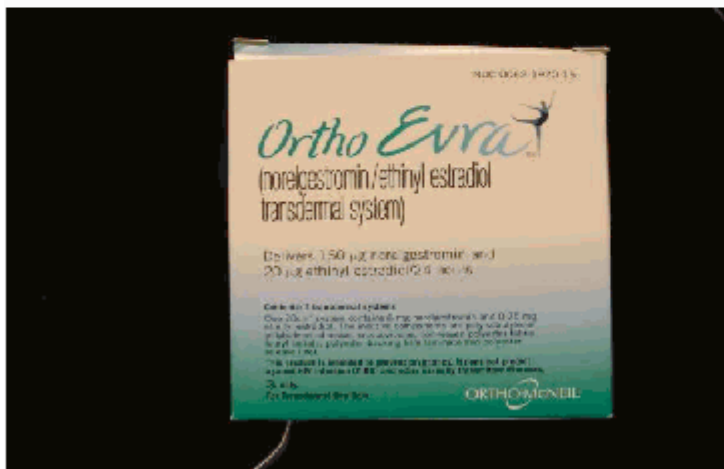
<http://www.fda.gov/bbs/topics/NEWS/2004/NEW01017.html>



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.

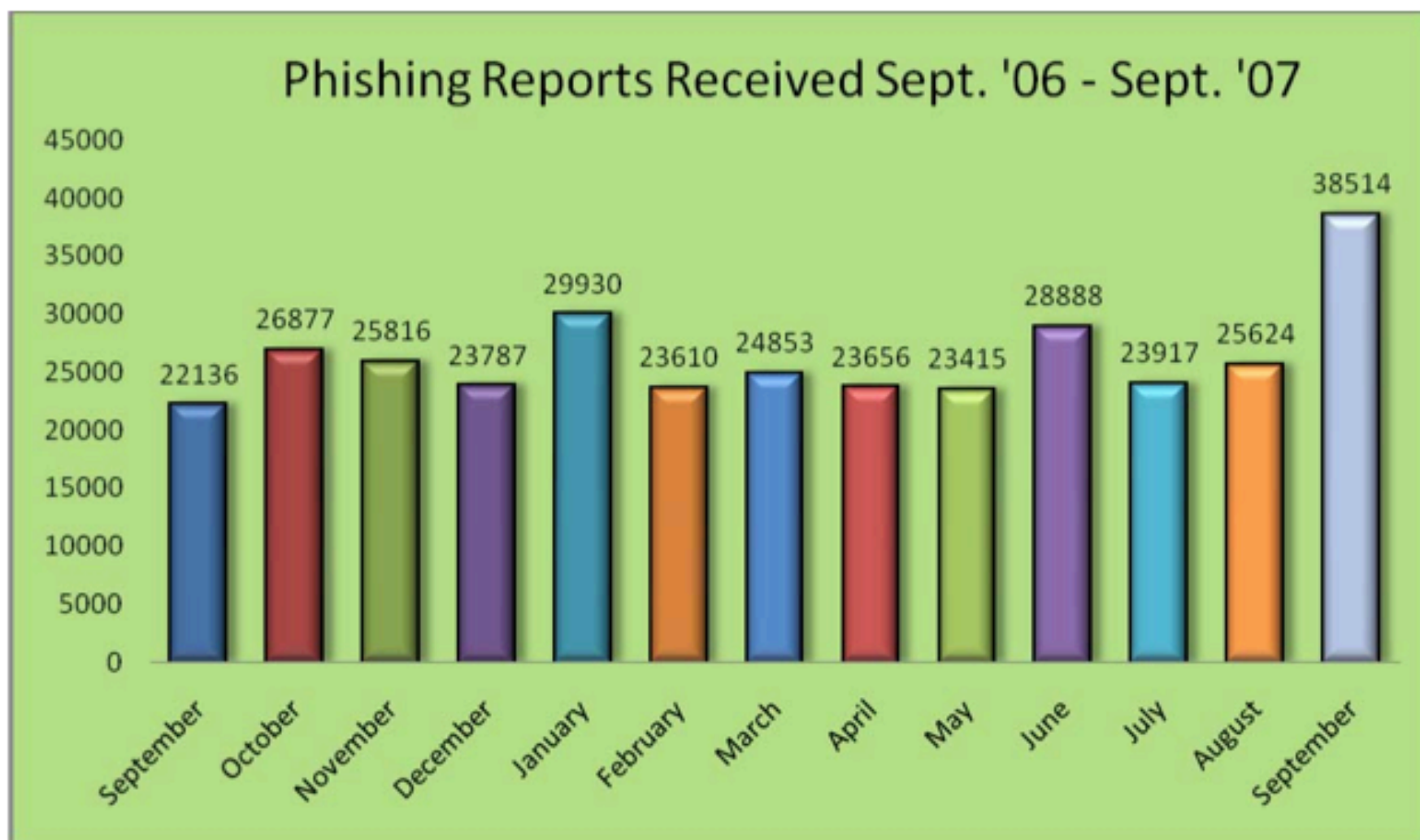
Judge Hittner reserved the issue of restitution for a possible hearing within the next ninety days. Upon completion of their prison terms, each brother must also serve a three-year term of supervised release. Steven and Bartholomew Stephens have been in federal custody since their convictions in June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



[Total phishing reports made to APWG 10/06-9/07: **318,887**]

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.

And If You'd REALLY Like To Understand The Money Laundering Issue...

- See the interagency "U.S. Money Laundering Threat Assessment,"
<http://www.ustreas.gov/offices/enforcement/pdf/mlta.pdf>

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

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

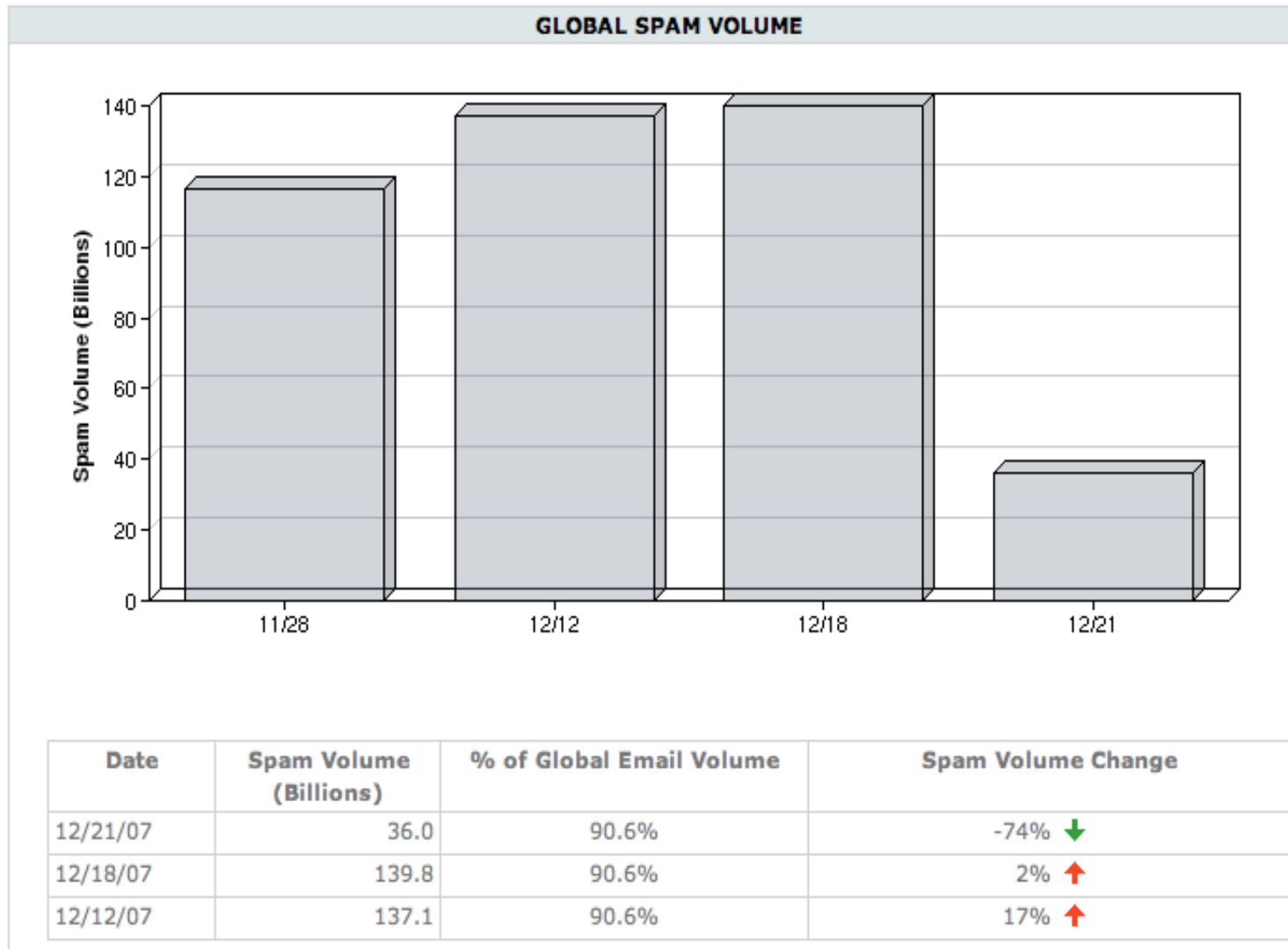
Date: 1994-04-12 00:40:42 PST

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]

Spam Volumes Today



http://www.senderbase.org/home/detail_spam_volume?action=&screen=&order=&displayed=lastmonth

Network Reputation - Estimated Spam Volume by ISP

Jump to: [\[Page 1\]](#)[\[Page 2\]](#)[\[Page 3\]](#)[\[Page 4\]](#)

Rank data last updated: December 31 2007, 12:20 PST

Rank This Week	Rank Last Week		ASN	ISP Name	Est. Spam Volume(24hrs)	Botnet Activity
001	001	→	9121	TTNET Ttnet Autonomous System	4.62B	12.8
002	003	↑	19262	VZGNI-TRANSIT - Verizon Internet Services Inc.	2.51B	-1.1
003	002	↓	3269	ASN-IBSNAZ TELECOM ITALIA	2.25B	34.6
004	004	→	5617	TPNET Polish Telecom's commercial IP network	1.63B	21.9
005	005	→	6147	Telefonica del Peru S.A.A.	1.07B	4.8
006	010	↑	4766	KIXS-AS-KR Korea Telecom	673.8M	20.3
007	007	→	7738	Telecomunicacoes da Bahia S.A.	783.9M	1.6
008	017	↑	4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	448.1M	5.3
009	012	↑	3352	TELEFONICA-DATA-ESPANA Internet Access Network of TDE	444.8M	13.1
010	011	↑	15557	LDCOMNET NEUF CEGETEL (formerly LDCOM NETWORKS)	704.1M	21.6

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.⁸³

Unfortunately, That Law Does Not Keep People From Attempting to Sell Even Bulk Schedule II Controlled Substances Online...

2) RITALIN BRAND NAME (Methylphenidate) 10mg

By Novartis ,Blister of 10 pills
normal price is \$1.80 each tablet
60 pills x \$1.80 plus Postage
90 pills x \$1.80 plus Postage
120 pills x \$1.80 plus Postage

Ritalin is on sale Right now
200 Pills are for \$300 dollars or \$1.5 each
400 Pills are for \$ 550 or \$1.375 Each

This sale price is for VIPs



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>]

Seeds/Spores for the Production of Street Drugs

- A prime example of how the Internet allows miscreants to exploit non-uniform national laws can be seen in the availability of things such as seeds for the production of marijuana, or spores for the production of hallucinogenic mushrooms. At least in some jurisdictions, possession and/or sale of those seeds or spores is lawful, while in others it is not.
- The Internet thus makes it feasible for those living in some restrictive jurisdictions to obtain prohibited products from sources in less restrictive jurisdictions.
- International delivery of the prohibited product frequently goes undetected and un-interdicted among the crush of of huge numbers of international letters and parcels. For an excellent discussion of issues associated with border inspection of immense volumes of mail, albeit soley in the context of prescription drug importation, see the GAO's "PRESCRIPTION DRUGS: Preliminary Observations on Efforts to Enforce the Prohibitions on Personal Importation," July 22nd, 2004, <http://www.gao.gov/cgi-bin/getrpt?GAO-04-839T>

"Prince of Pot" Arrested by US-Canadian Task Force

Major Distributor of Marijuana Federally Indicted in Seattle, Washington

JUL 29--(Seattle, WA) The Royal Canadian Mounted Police (RCMP) and the Halifax Police Department arrested MARC EMERY, 47, of Vancouver, BC, today on a warrant issued from the Western District of Washington in Seattle. EMERY is accused of selling millions of dollars of marijuana seeds over the internet, though the mail, and in person to individuals in the United States and across the globe. The DEA, in an investigation of EMERY has traced his seeds to illegal marijuana crops in Indiana, Florida, California, Tennessee, Montana, Virginia, Michigan, New Jersey and North Dakota. An estimated 75% of the seeds EMERY sells are transported to the United States.

"The tentacles of the Mark Emery criminal enterprise reached out across North America to include all 50 United States and Canada," said Special Agent in Charge Rodney G. Benson of the Drug Enforcement Administration (DEA). "Mr. Emery utilized the internet to sell his marijuana seeds throughout this country to customers no matter their age. He directed his business with efficiency, was motivated by greed, and will now be prosecuted for this illegal activity."

MARC EMERY has operated Marc Emery Direct since 1994, taking orders for marijuana seeds over the internet and is a well known figure in Canada as publisher of *Cannabis Culture magazine*, and leader of the BC Marijuana Party. According to the web site run by EMERY, he has made more than \$3 million annually, illegally selling marijuana seeds. EMERY claims to stock the largest supply of marijuana seeds in the world and is considered the largest distributor of marijuana seeds. According to court filings, Emery seeds are associated with multiple illegal grow operations across the U.S.



BBC <http://news.bbc.co.uk/2/hi/europe/7041961.stm>



One-Minute World News



Last Updated: Friday, 12 October 2007, 16:10 GMT 17:10 UK

[E-mail this to a friend](#)

[Printable version](#)

Netherlands bans magic mushrooms

The Dutch government is banning the sale of all magic mushrooms after a series of high-profile incidents involving tourists who had taken them.

The decision will take effect within several months, said a spokesman for the Dutch justice ministry.



Magic mushrooms are big business in the Netherlands

A major Dutch producer of the psychedelic mushrooms said he stood to lose millions of euros as a result.

The Netherlands is famed for its liberal drugs policy, with marijuana openly sold in licensed cafes.

Magic mushrooms, more properly known as psilocybe, contain the psychedelic chemicals psilocybin and psilocin.

"We intend to forbid the sale of magic mushrooms," said justice ministry spokesman Wim van der Weegen.

"That means shops caught doing so will be closed."

Currently in the Netherlands the sale of dried magic mushrooms - in which the psychoactive chemicals psilocybin and psilocin are stronger - is banned but fresh mushrooms are allowed.

This is because it is more difficult to ascertain how much of the chemicals fresh mushrooms contain. But Mr Van der Weegen said this was exactly the issue.

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>) 90

Example Child Porn Sentence: 8 Years

Portland Resident Receives 96 Months Prison Sentence for Distribution of Child Pornography

Portland, Ore. - Ronald Vandel Thoreson, 62, of Portland, was sentenced on December 10, 2007 to 96 months in prison by U.S. District Court Judge Garr M. King. On July 12, 2007, Thoreson pled guilty to an indictment charging him with distribution of child pornography during the months of July through October, 2005. Thoreson became the subject of an investigation by Immigration and Customs Enforcement (ICE) following reports by the German National Police that an Internet access account, associated with defendant's account, was used to download a number of images containing child pornography using the file sharing program Limewire. [continues]

http://www.usdoj.gov/usao/or/PressReleases/2007/20071211_Thoreson.html

Not Only Child Porn: Rape/Sexual Torture

TWO MEN SENTENCED TO FEDERAL PRISON ON OBSCENITY CONVICTION

Clarence Thomas Gartman, age 35, and his brother-in-law, former Houston Police Officer, Brent Alan McDowell, age 37, were sentenced today in Dallas, announced Assistant Attorney General Alice S. Fisher for the Criminal Division and United States Attorney Richard B. Roper. The Honorable Barefoot Sanders, United States Senior District Judge, sentenced Gartman to 34 months in prison and McDowell to 30 months in prison. [* * *]

The case was initially investigated by the Dallas Police Department after they received a tip from a German citizen who told them that a website selling rape videos was registered to a Garry Ragsdale. At that time, Garry Ragsdale was a Dallas Police Department officer. [* * *]

The government provided evidence at trial that beginning in 1998, Gartman and McDowell maintained a web site on the Internet, “forbiddenvideos.com.” The web site was used to advertise and distribute obscene videos by VHS cassettes, CDs, and streaming video, depicting rape scenes, sexual torture and other explicit sex acts. [continues]

"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]p³

FY 2012 Outcome Goal: Shut down a cumulative total of 6,000 websites or web hosts (FY 2007-2012)
FY 2007 Progress: The Department is on target to achieve this long-term goal.

Background/Program Objectives: Facilitation of crimes against children through the use of a computer and the Internet is a national crime problem that is growing dramatically. The Innocent Images National Initiative (IINI), a component of the FBI's Cyber Crimes Program, is an intelligence-driven, proactive, multi-agency investigative initiative to combat the proliferation of child pornography and/or child sexual exploitation facilitated by online computers. The mission of the IINI is to: Identify, investigate, and prosecute sexual predators who use the Internet and other online services to sexually exploit children; identify and rescue witting and unwitting child victims; and establish a law enforcement presence on the Internet as a deterrent to subjects who seek to exploit children.

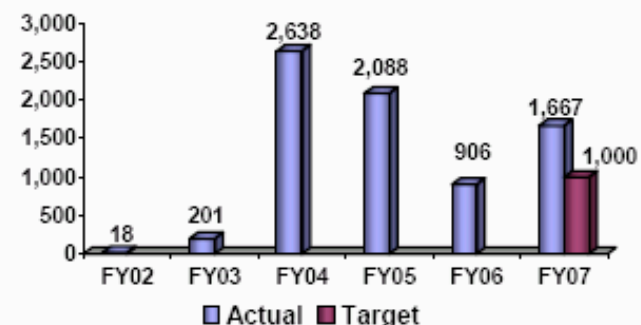
Performance Measure: Number of Child Pornography Websites or Web Hosts Shut Down

FY 2007 Target: 1,000

FY 2007 Actual: 1,667

Discussion of FY 2007 Results: A website/web host gets shut down at the request of the FBI once a subpoena is served to obtain information on who is responsible for the illicit content. Often the subpoena would be the factor that alerted the Internet Service Provider (ISP) of the illegal

Number of Child Pornography Websites or Web Hosts Shut Down



Data Collection and Storage: The data source is a database maintained by FBI personnel detailed to the National Center for Missing and Exploited Children, as well as statistics derived by the FBI's Cyber Division's program personnel.

Data Validation and Verification: Data are reviewed and approved by FBI Headquarters program personnel.

Data Limitations: Data for this report are compiled less than 30 days after the end of the fiscal year, and thus may not fully represent the accomplishments during the reporting period. Information based upon reporting of locates and convictions are necessary for compilation of some of these statistics.

"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.

"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>]

Let's Look at A Sample "Replica" Spam...

Return-Path: <bnvv3evvg@urscorp.com>
Received: from uibtrgga ([89.20.8.37])
by smtp.uoregon.edu (8.13.8/8.13.8) with SMTP id 1A7JKj0x005302;
Wed, 7 Nov 2007 11:20:46 -0800
To: <[redacted]@darkwing.uoregon.edu>
From: "Brandee Britni" <bnvv3evvg@urscorp.com>
Subject: CheapestRolexReplica! Exclusive ReplicaWATCHES Online, buy
fake designerWatches fi
Message-ID: <7575w32151.58183b30285153@urscorp.com>
Date: Wed, 07 Nov 2007 22:18:05 +0300
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

New Arrival 2007 models

RolexMens
RolexLadies
RolexSports
RolexDateJusts
A.Lange & Sohne
[* * *]

Order Your Brand New Watches Now!

<http://rnxft.qhference.com>
<http://rxzz.qhference.com>

What Do We Know About **qhference.com**?

Domain Name: QHREFERENCE.COM

Registrar: XIN NET TECHNOLOGY CORPORATION

Whois Server: whois.paycenter.com.cn

Referral URL: <http://www.xinnet.com>

Name Server: NS1.MYMUSICROCKZZ.COM [70.162.220.41]

Name Server: NS2.MYMUSICROCKZZ.COM [67.64.157.179]

Name Server: NS3.MYMUSICROCKZZ.COM [69.233.105.149]

Name Server: NS4.MYMUSICROCKZZ.COM [125.128.3.171]

Status: ok

Updated Date: 18-dec-2007

Creation Date: 30-oct-2007

Expiration Date: 30-oct-2008

70.162.220.41	==>	ip70-162-220-41.ph.ph.cox.net	}	
67.64.157.179	==>	adsl-67-64-157-179.dsl.rcsntx.swbell.net	}	Note
69.233.105.149	==>	ppp-69-233-105-149.dsl.irvnca.pacbell.net	}	these...
125.128.3.171	==>	NXDOMAIN; Korean Telecom netblock	}	

[The referral whois server did not supply any registrant name/address data]¹⁰³

"Fastflux" Web Hosting

Rather than using a regular web hosting provider, some individuals host their websites on hijacked broadband connected consumer PCs, potentially changing hosts every few minutes (in this case, the TTL is set to be just 180 seconds):

```
% dig rxzz.qhference.com
```

```
[ * * * ]
```

```
rxzz.qhference.com.      180      IN      CNAME   qhference.com.
qhference.com.           180      IN      A        65.96.100.205
                        [c-65-96-100-205.hsd1.ma.comcast.net]
qhference.com.           180      IN      A        67.9.38.205
                        [205-38.9-67.se.res.rr.com]
qhference.com.           180      IN      A        68.75.173.252
                        [adsl-68-75-173-252.dsl.emhril.ameritech.net]
qhference.com.           180      IN      A        68.78.33.64
                        [adsl-68-78-33-64.dsl.emhril.ameritech.net]
qhference.com.           180      IN      A        69.138.15.252
                        [c-69-138-15-252.hsd1.md.comcast.net]
qhference.com.           180      IN      A        75.118.148.205
                        [d118-75-205-148.try.wideopenwest.com]
qhference.com.           180      IN      A        208.22.14.76
                        [NXDOMAIN; Sprint Government Systems netblock]
qhference.com.           180      IN      A        221.156.79.48
                        [NXDOMAIN; Korean Telecom netblock]
```


If We Visit The Spamvertised URL, It Immediately Sends Us Elsewhere...

```
% wget "http://rxzz.qhference.com"
--22:54:58--  http://rxzz.qhference.com/
               => `index.html'
Resolving rxzz.qhference.com... 124.104.214.215, 24.122.220.47, 67.64.157.179,
...
Connecting to rxzz.qhference.com[124.104.214.215]:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://keogbw.net [following]
--22:54:59--  http://keogbw.net/
               => `index.html'
Resolving keogbw.net...
Connecting to keogbw.net[219.251.217.166]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]

[          <=>          ] 43,351          12.80K/s
22:55:07 (12.79 KB/s) - `index.html' saved [43351]
```

219.251.217.166 is an IP address which belongs to Hanaro Telecom (KR)

219.251.217.166 Is Listed On The SBL



Ref: SBL61719

219.251.217.166/32 is listed on the Spamhaus Block List (SBL)

15-Dec-2007 21:35 GMT | SR22

Spam webhosting - azfuek.net

The spamvertized URL is on Googlepages, which has a redirect to:

<http://rdj.pjuseof.com>

<http://rdj.pjuseof.com> is fast-flux hosted, and gives this redirection target:

Location: <http://azfuek.net>

azfuek.net has address 219.251.217.166

azfuek.net. 2D IN NS ns1.fat357.com.

azfuek.net. 2D IN NS ns2.fat357.com.

Some Web Sites Known to Be Hosted on 219.251.217.166

www.qwe4321.com	A	219.251.217.166
www.streetnstrut02.com	A	219.251.217.166
www.streetnstrut32.com	A	219.251.217.166
watchwildworld.com	A	219.251.217.166
bonuscasinogame.com	A	219.251.217.166
www.goldgamesite.com	A	219.251.217.166
watchezsite.com	A	219.251.217.166
luxclubgaming.com	A	219.251.217.166
richluxcasino.com	A	219.251.217.166
wildreplicas.com	A	219.251.217.166
www.101watches.com	A	219.251.217.166
leisuretimewatches.com	A	219.251.217.166
thebigwatches.com	A	219.251.217.166
flywatches.com	A	219.251.217.166
flowfakes.com	A	219.251.217.166
goldwatchdirect.com	A	219.251.217.166
gamblingplacelux.com	A	219.251.217.166
bulkwatchz.com	A	219.251.217.166
justwatchz.com	A	219.251.217.166
gamingfirstplace.net	A	219.251.217.166
luxcasinoonline.net	A	219.251.217.166
onlineplusgambling.net	A	219.251.217.166
topluxgambling.net	A	219.251.217.166
greatluxgambling.net	A	219.251.217.166
toproyalgaming.net	A	219.251.217.166
topdestgaming.net	A	219.251.217.166
clubluxgaming.net	A	219.251.217.166
topplacecasino.net	A	219.251.217.166
greatgamecasino.net	A	219.251.217.166
stylevipcasino.net	A	219.251.217.166
luxtopcasino.net	A	219.251.217.166
baidens.net	A	219.251.217.166
keogbw.net	A	219.251.217.166



Currencies: US Dollars

Search

Support Tickets

MAIN PAGE

NEW PRODUCTS

MY ACCOUNT

SHOPPING CART

CHECKOUT

FEATURED PRODUCTS

- A.Lange & Sohne
- Alain Silberstein
- Audemars Piguet
- Bell & Ross
- Breguet
- Breitling
- Bvlgari
- Cartier
- Chanel
- Chopard

FEATURED PRODUCTS



Rolex

Submariner Silver Band
Harley Davidson, Brown
Face

\$299.00

[Detail](#) [Add to cart](#)



Rolex

SWISS Rolex Yachtmaster
SS/18K band Blue Face

\$599.00

[Detail](#) [Add to cart](#)



Rolex

SWISS Rolex Daytona SS
Band Black with Red Dial
2005 Edition

\$799.00

[Detail](#) [Add to cart](#)



Rolex

Cosmograph Silver Band,
White Face, Double
Diamond Bezel Roman #

\$239.00

[Detail](#) [Add to cart](#)

Do you have a physical store and address as well?

No, currently we have no other retail location other than our online store.

[back](#) [top](#) [top](#)

Why would I want to buy a replica watch instead of a real one?

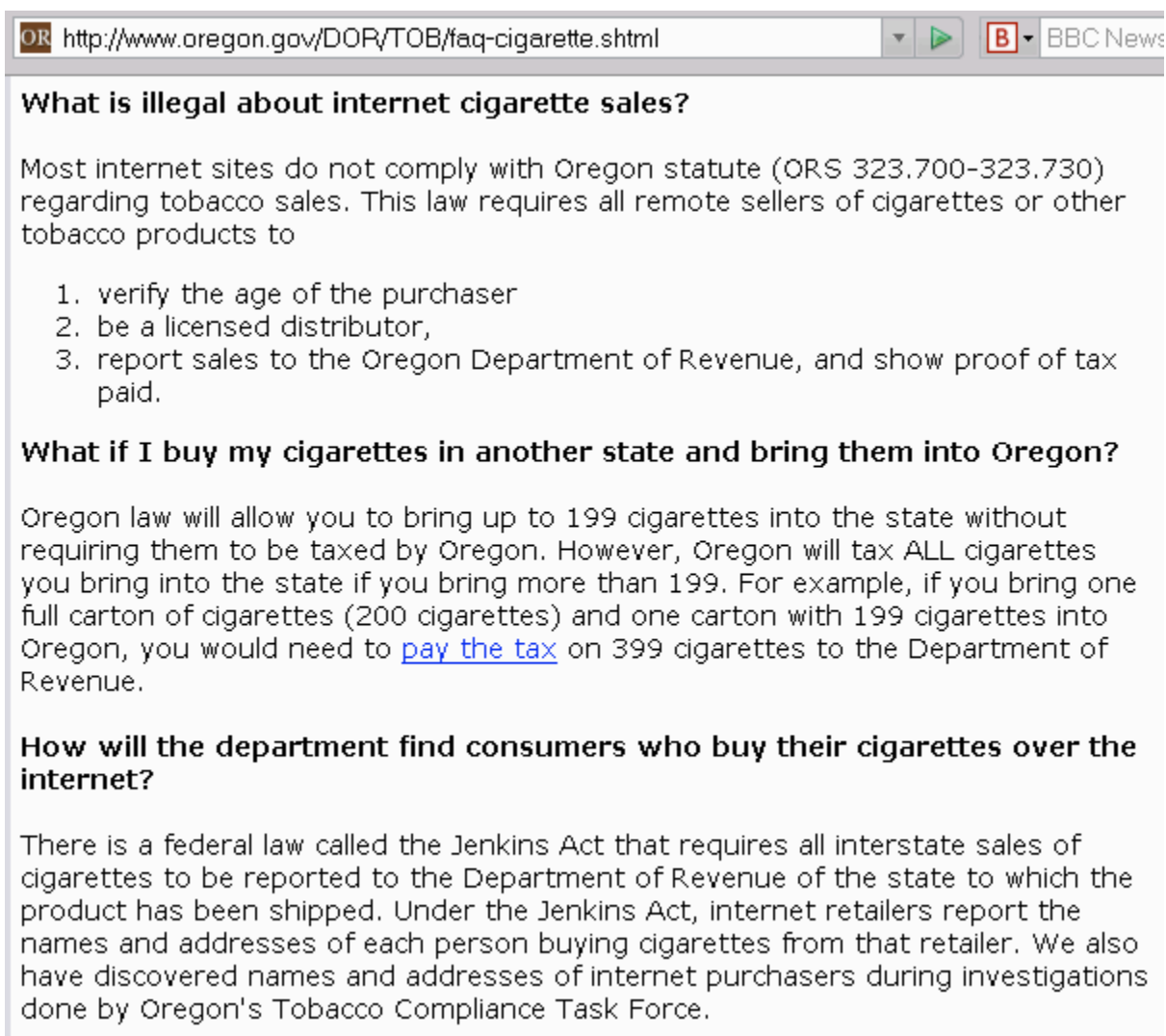
The reason why replica watches are so popular is because you can look classy and professional, yet not have to spend tens of thousands of dollars doing it. These watches look identical to the ones you will find at the jewellery store selling for prices most people would not be able to afford. There is no reason why these beautiful watches should only be limited to the rich, but to everyone who wants to add a touch of class to their life style.

[back](#) [top](#) [top](#)

Are these watches of high quality or will they break after I open the box?

It depends on how you wear it. If you wear it regularly, it will last a few years without any problems. The watches we offer are of a very high quality. These are not the cheap quality watches you will find on the streets that will break after a few days, these will last for years! We are so confident in our watches, we offer an exchange or refund for any watches if they are ever defective. View our **Warranty** section to see types of warranties and details.

3. (f) Untaxed Cigarettes Sold Over The Internet



OR <http://www.oregon.gov/DOR/TOB/faq-cigarette.shtml> BBC News

What is illegal about internet cigarette sales?

Most internet sites do not comply with Oregon statute (ORS 323.700-323.730) regarding tobacco sales. This law requires all remote sellers of cigarettes or other tobacco products to

1. verify the age of the purchaser
2. be a licensed distributor,
3. report sales to the Oregon Department of Revenue, and show proof of tax paid.

What if I buy my cigarettes in another state and bring them into Oregon?

Oregon law will allow you to bring up to 199 cigarettes into the state without requiring them to be taxed by Oregon. However, Oregon will tax ALL cigarettes you bring into the state if you bring more than 199. For example, if you bring one full carton of cigarettes (200 cigarettes) and one carton with 199 cigarettes into Oregon, you would need to [pay the tax](#) on 399 cigarettes to the Department of Revenue.

How will the department find consumers who buy their cigarettes over the internet?

There is a federal law called the Jenkins Act that requires all interstate sales of cigarettes to be reported to the Department of Revenue of the state to which the product has been shipped. Under the Jenkins Act, internet retailers report the names and addresses of each person buying cigarettes from that retailer. We also have discovered names and addresses of internet purchasers during investigations done by Oregon's Tobacco Compliance Task Force.

Unpaid Taxes Associated With Online Cigarette Purchases Can Be Substantial



http://www.nyc.gov/html/dof/html/services/services_fraud_ciga

Whenever Finance obtains purchase, payment, or shipping information from a vendor of untaxed cigarettes, the purchasers must pay the New York City Cigarette Tax. Recently, this occurred when Finance obtained the purchase and shipping records of various Internet cigarette dealers as part of a legal settlement with the companies. To date, Finance has billed and collected the following amounts:

	COLLECTED	BILLED	# NYC CUSTOMERS BILLED
Affordablecigs.com	\$574,854	\$956,340	2,313
Cigoutlet.com	\$35,355	\$120,845	136
Smokes4less.com	\$177,068	\$277,695	1,331
Dirtcheap.com *	\$1,427,868	\$3,300,585	2,000
eSmokes.com *	\$1,064,340	\$2,504,789	2,000
other	\$2,195		
TOTAL	\$3,281,679	\$7,160,254	

* Still ongoing. Numbers reflect efforts from from September 1, 2006 through September 1, 2007.

Cigarette Smuggling Also Has a History of Ties to Terrorism

Reports of tobacco smuggling by individuals with ties to terrorist organizations include:

- **June 21, 2002:** A federal jury in North Carolina finds Mohamad Hammoud guilty of cigarette smuggling, racketeering, and money laundering. Hammoud and his brother smuggled \$7.9 million worth of cigarettes from North Carolina to Michigan. Together they steered profits from their multimillion dollar cigarette smuggling operation to Hezbollah.
- **May 1, 2003:** 10 men of Middle Eastern descent are arrested in New York and Virginia for possession of 71, 467 cartons valued over \$2.2 million, wire fraud and money laundering. Federal government opens investigation into suspected ties with Hezbollah, a man linked to the case reportedly was found with wire transfer receipts linking him to the terror organization.
- **May 29, 2005:** 19 men in Dearborn, Michigan are arrested and federally indicted for a smuggling operation that evaded "tens of millions in state cigarette taxes" and funneled illegal proceeds to Hezbollah. Most of the smuggled cigarettes were sold in Michigan and New York.
- **September 20, 2006:** Karim H. Nassar from Windsor, Canada pleads guilty to tobacco smuggling and trafficking \$500,000 of cigarettes from Cattaraugus Indian Reservation in New York State to North Carolina, Kentucky and Michigan. Some of the profits were sent to Hezbollah guerillas.
- **October 5, 2007:** ATF agent Patrick Awe tells a Senate committee that "the link to terrorism has been established" and proceeds from some of the counterfeiting schemes had ended up going to groups like Hezbollah or organized crime groups that have the financial resources to run sophisticated operations.

3. (g) Online Gambling

- Internet gambling, like Internet porn, is big business – a USA Today article (http://www.usatoday.com/sports/2007-04-27-internet-gambling-bill_N.htm) puts its value at \$12 billion dollars per year, and Calvin Ayre (of the Bodog Internet gambling empire) even made Forbes list of billionaires, see <http://www.forbes.com/forbes/2006/0327/112.html> and <http://www.forbes.com/lists/2006/10/GCUD.html>
- While Internet gambling is legal in some jurisdictions, in the United States, with only narrow exceptions, Internet gambling is NOT legal as a result of statutes including:
 - 18 USC 1084: "The Wire Act,"
 - 18 USC 1952: "The Travel Act,"
 - 18 USC 1955: "The Illegal Gambling Business Act,"
 - 31 USC 5361 et. seq., The Unlawful Internet Gambling Enforcement Act of 2006, Title VIII of HR 4954, the SAFE Port Act, available online at <http://thomas.loc.gov/cgi-bin/query/z?c109:h4954>:
- The FBI has been pursuing a variety of online gambling-related cases, including...

Financial Transactions Associated with Internet Gambling



In 2005, Neteller processed over \$7.3 billion in financial transactions. According to reports issued by Neteller, 95% of its revenue was derived from money transfers involving internet gambling companies. On September 11, 2006, the President and Chief Executive Officer of Neteller described the "online gaming market" as Neteller's "main market," and stated that, in the first half of 2006, Neteller processed \$5.1 billion in financial transactions. As charged in the complaint, approximately 85% of Neteller's revenue during that period derived from individuals in North America, and 75% of its North American revenue was generated in the United States. Both the operation of an internet gambling operation and the transferring of the proceeds from these businesses overseas are illegal under United States law.

LAWRENCE and LEFEBVRE are both charged with conspiring to transfer funds with the intent to promote illegal gambling. If convicted, both defendants face a maximum sentence of 20 years' imprisonment.

Internet Gambling and Online Advertising

MICROSOFT, GOOGLE, & YAHOO! PAY MILLIONS TO U.S. FOR THEIR PAST PROMOTION OF ILLEGAL GAMBLING

ST. LOUIS, Missouri - Microsoft Corporation, Google, Inc., and Yahoo! have entered into settlements with the U.S. to resolve claims that they promoted illegal gambling, United States Attorney Catherine L. Hanaway, of the Eastern District of Missouri announced today. The total amount of the three settlements is \$31.5 million in value to the United States.

<http://stlouis.fbi.gov/dojpressrel/pressrel07/illegalgambling121907.htm>

4. Cyber Incidents Gone Awry – Why We Need Cyber Savvy Defense Attorneys, Too

WiFi Theft of Services

- **Using free wireless at library described as theft**

Anchorage Daily News (Published: February 24, 2007)

WASILLA -- Brian Tanner was sitting in his Acura Integra recently outside the Palmer Library playing online games when a Palmer police pulled up behind him.

The officer asked him what he was doing.

Tanner, 21, was using the library's wireless Internet connection. He was told that his activity constituted theft of services and was told to leave. The next day, Sunday, police spotted him there again.

"It was kind of like, 'Well gee whiz, come on,' " police Lt. Tom Remaley said.

The police officer confiscated Tanner's laptop in order to inspect what he may have been downloading, Remaley said. Remaley on Friday said he hasn't looked inside the computer yet; he's putting together a search warrant application. [continues]

<http://dwb.adn.com/news/alaska/story/8667098p-8559268c.html>

[some cyber incidents, like this one, frankly strike me as rather pointless]¹¹⁷

Julie Amero: Part I

- **Substitute Teacher Faces Jail Time Over Spyware**

A 40-year-old former substitute teacher from Connecticut is facing prison time following her conviction for endangering students by exposing them to pornographic material displayed on a classroom computer.

Local prosecutors charged that the teacher was caught red-handed surfing for porn in the presence of seventh graders. The defense claimed the graphic images were pop-up ads generated by spyware already present on the computer prior to the teacher's arrival. The jury sided with the prosecution and convicted her of four counts of endangering a child, a crime that brings a punishment of up to 10 years per count. She is due to be sentenced on March 2.

I had a chance this week to speak with the accused, Windham, Conn., resident Julie Amero. Amero described herself as the kind of person who can hardly find the power button on a computer, saying she often relies on written instructions from her husband explaining how to access e-mail, sign into instant messaging accounts and other relatively simple tasks.

On the morning of Oct 19, 2004, Amero said she reported for duty at a seventh grade classroom at Kelly Middle School in Norwich, Conn. After stepping out into the hall for a moment, Amero returned to find two students

hovering over the computer at the teacher's desk. As supported by an analysis of her computer during the court proceedings, the site the children were looking at was a seemingly innocuous hairstyling site called "new-hair-styles.com." Amero said that shortly thereafter, she noticed a series of new Web browser windows opening up displaying pornographic images, and that no matter how quickly she closed each one out, another would pop up in its place.

"I went back to computer and found a bunch of pop-ups," Amero said. "They wouldn't go away. I mean, some of the sites stayed on there no matter how many times I clicked the red X, and others would just pop back up."

Amero said she panicked and ran down the hall to the teacher's lounge to ask for help. "I dared not turn the the computer off. The teacher had asked me not to sign him out" of the computer, she recalled. Amero said none of the teachers in the lounge moved to help her, and that another teacher later told her to ignore the ads, that they were a common annoyance. Later on, prosecutors would ask why she hadn't just thrown a coat or a sweater over monitor. On that day Amero hadn't worn either.

Several children told their parents about the incident, who in turn demanded answers from the school's principal. Three days later, school administrators told Amero she was not welcome back. Not long after that, local police arrested her on charges of risking injury to several students. [continues]
blog.washingtonpost.com/securityfix/2007/01/substitute_teacher_faces_jail.html

Julie Amero: Part II

Substitute Teacher Granted New Trial in Porn Case

A former Connecticut middle-school teacher was granted a new trial today at her sentencing hearing, where she had faced up to 40 years in prison for exposing her students to pornographic material on a classroom computer.

Judge Hillary Strackbein said 40-year-old Julie Amero was entitled to a new trial "because a witness the state presented as a computer expert, a Norwich police detective, provided 'erroneous' testimony about the classroom computer," according to the Hartford Courant. [* * *]

The defense's key witness, a forensics expert who had examined the PC Amero was using in the Norwich middle-school classroom, was barred from presenting his technical evidence during the trial. There also was the prosecution's admission that it had failed to conduct any scan of the computer's hard drive with anti-spyware software. [article continues]

[blog.washingtonpost.com/securityfix/2007/06/
substitute_teacher_granted_new.html](http://blog.washingtonpost.com/securityfix/2007/06/substitute_teacher_granted_new.html)

Some Other Interesting Cyber Cases

e360Insight vs. The Spamhaus Project (jurisdiction and pleading issues)

<http://www.spamsuite.com/node/5>

James S. Gordon et al. v. Virtumundo (with respect to his standing & costs)

<http://news.justia.com/cases/featured/washington/wawdce/2:2006cv00204/133422/>

Bennett Haselton's Experience with Filings in WA Small Claims Courts

<http://yro.slashdot.org/article.pl?sid=07/04/18/1247229>

State of Oregon v. Randal Schwartz

http://w2.eff.org/legal/cases/Intel_v_Schwartz/schwartz_case.intro

http://www.lightlink.com/spacenka/fors/order_to_set_aside.pdf

Shawn Carpenter (termination of government employment)

"Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)"

<http://www.time.com/time/magazine/article/0,9171,1098961,00.html>

Thanks For the Chance To Talk Tonight!

- Are there any questions?