Project on Cybercrime
www.coe.int/cybercrime

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, France

Version 13 March 2008

Discussion paper

Cybercrime:
current threats and trends

prepared by
Laurence Ifrah, France

This report has been prepared within the framework of the Project on Cybercrime of the Council of Europe.

Contact

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
E-mail: alexander.seger@coe.int

Contents

1 Introduction

The US Internet Crime Complaint Center (IC3), created in May 2000, logged its one millionth consumer complaint about alleged online fraud or cyber crime on 11 June 2007 at 01:26 p.m. The evolution of cybercrime in the past seven years is tremendous and this paper aims to report all current threats and what has to be expected in the matter of computer crime.

New emerging threats overflowing the Internet have been seen in 2007, a consequence of the high professionalism of criminal organisations. Professional hackers are being paid to develop new malwares. The evolution of the threats is much more sophisticated than it used to be: they are patching their codes in real time, as soon as antivirus editors are publishing updates in order to avoid computers getting compromised. There are changes in the ways used to infect computers, as before users had to download and open an infected file; now they directly receive infected e-mail attachments. Spyware or other malware are included in web pages and users are invited to visit compromised websites via spammed e-mail invitations, or are redirected to infected web pages by search engines. Any site can be infected, from cooking to gambling or from gardening to pornography.[1]

The top threats are[2]:

- Botnets
- Targeted attacks to governments, firms, end-users
- Financial fraud to banks, firms, end-users
- ID fraud
- Spam, phishing
- Espionage – firms and governments
- Web attacks
- Social networks
- Internal misuse of network resources
- Viruses – Worms – Rootkits (customised-written codes)

According to a Netcraft survey in December 2007, they received responses from 155,230,051 sites. This is an increase of 5.4 million sites since November 2007, continuing the very strong growth seen during this same year; the web has grown by nearly 50 million sites since December 2006.

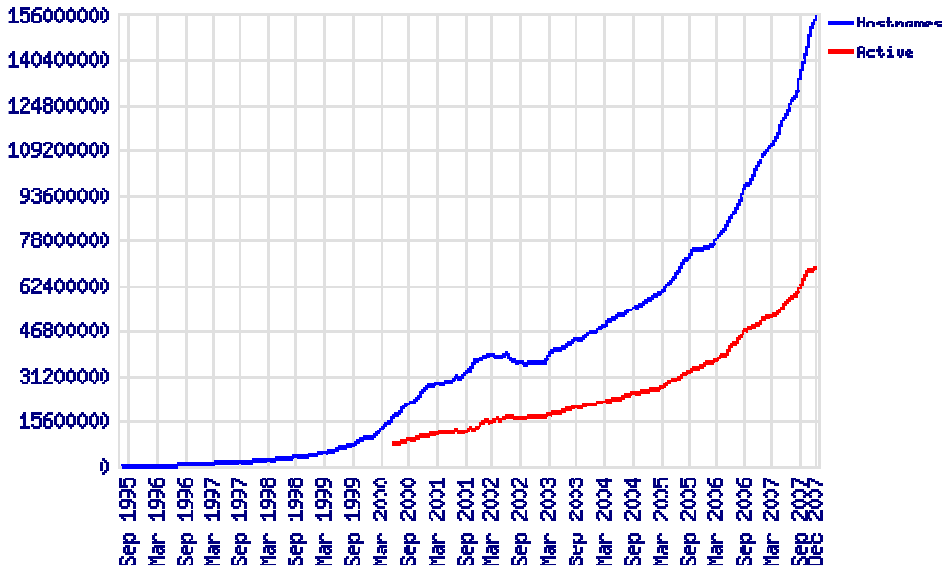
This once again breaks the record for growth of the web in one year; the previous highest growth was 30 million sites in 2006. The growth is also impressive in percentage terms, with the web growing by 48% since last December — although this remains far less than the runaway growth of 160% seen back in 2000.

The most dramatic growth this year has been the inclusion of ever larger numbers of sites at blogging service providers. The three largest alone — MySpace, Live Spaces and Blogger — now account for around 25 million sites in the survey. Both Microsoft and Google are attracting large numbers of users by integrating a range of services — search, online collaboration, blogging and electronic mail.

The growth in the number of active sites – an alternative measure that excludes parked domains and other templated sites – has also been impressive, with nearly 19 million new active sites since last December, an annual growth of 38%.[3]

[1] http://www.sophos.com
[2] When not specified, threats are concerning all resources.
[3] http://www.netcraft.com

Total Sites Across All Domains August 1995 - December 2007[4]



2 Malware

According to the computer security firm F-Secure, in December 2007 the Internet counted over 500,000 malware signatures in the wild, being 250,000 twelve months earlier. Underground forums or websites are publishing a large range of warez tools like worms, viruses or Trojan DIY programs, a sort of construction tool kit that allow hackers to develop and release their own version of the code. In doing so, criminals can provide a new version of a malware a few hours after the previous one has been blocked by an antivirus program. Programmers who write malicious codes are also working on the presentation of their malware. Being aware that users are more informed about worm and virus attacks, they are designing them in order to lure their victims.

The tremendous success of Apple products like the iPod and the iPhone, the latest Mac OS X operating system Leopard, plus very popular applications like iTunes, QuickTime and the web browser Safari has been contributing to the increase of attacks against the company. Malware authors are now seriously targeting Apple's products.

International events are used to spread viruses in the wild, hackers take advantage of the latest news that might enable a new attack vector.

More than 24 hours after the assassination of the former Prime Minister of Pakistan, Mrs Benazir Bhutto, a new malicious JavaScript was embedded in a website containing information about the event. Web surfers wanting additional details about Mrs Bhutto's death were directed to the compromised websites. Windows users were told that they needed to install a new high-definition video codec (program that decodes the digital data stream), to view the clip. Instead it would download a variant of the Zlob Trojan horse, opening a back door that would infect the victim's computer with other malware.[5]

[4] Netcraft.
[5] Gregg Keizer, Computerworld, December 2007.

Compromised hardware: in August 2007, Seagate Technology LLC, a firm specialised in digital storage informed customers on its website that the August 2007 production of their hard drive Maxtor manufactured in China had been infected with two password stealing Trojan horses. Kapersky Labs, an editor of antivirus software, alerted Seagate and said that the Trojan was sending the stolen data to a server located in China. 1,800 hard drives were reported malware-equipped.

2.1 Vulnerabilities

There is a significant growth in the number of client-side vulnerabilities, including vulnerabilities in browsers, software, media players and other desktop applications. These vulnerabilities are being discovered on multiple operating systems and are being massively exploited in the wild, often to drive recruitment for botnets.

Attackers are finding more creative ways of obtaining sensitive data from organisations. Succeeding in compromising a machine requires a system penetration which can only be achieved by the exploitation of a vulnerability. Some administrators tools have been developed for them to check their application before publishing; these tools are called "Fuzzers" and is also been used by criminals and criminal organisations so they can create botnets easier and faster. "Fuzz Testing" or "fuzzing" is a Black Box software testing technique which consists in finding implementation bugs in codes using malformed data injection in an automated style. If the program fails, by crashing or by failing built-in code assertions, then there are defects to correct. The most famous "fuzzer" is Metasploit Framework, a great application dedicated to exploit development and security tests.

Wfuzz is a tool designed for bruteforcing web applications; it can be used for finding resources not linked (directories, servlets, scripts, etc.), bruteforce GET and POST parameters for checking different kinds of injections (SQL, XSS, LDAP,etc), bruteforce Forms parameters (User/Password), "fuzzing", etc.

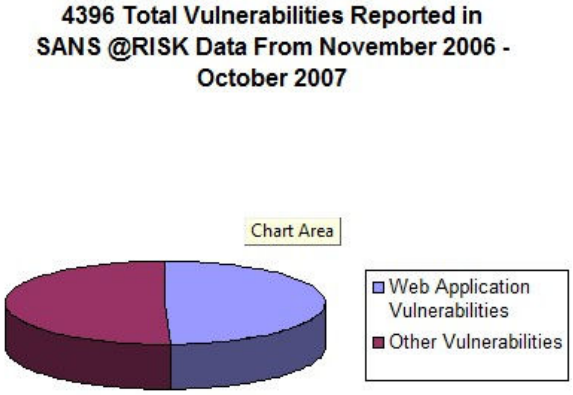
"Fuzzing" is meant to check any possible vulnerability about a system or an application; once found, the bug is exploited for further tests and IT experts will analyse the results before publishing them. The increase in vulnerabilities has reached 38% in 2005, due to "Fuzzers". Secure Computing, a security firm, has mentioned that hackers are sharing results of their tests on IRC channels or forum, in order to develop new hacking tools[6].

> PDF files: Russian hackers are using vulnerability in the Adobe software Acrobat and Reader for PDF files. Criminals were sending malformed pdf files to their target and when files were opened they released a rootkit Trojan; Pidief.a which would disable the Firewall to update itself and send the user personal data to a remote server belonging to RBN[7] (Russian Business Network). Once these action done, the Trojan would then download two new rootkits. According to Symantec, compromised files were named BILL.pdf, YOUR_BILL.pdf, INVOICE.pdf and STATEMENT.pdf

Finding vulnerability has a price, when security firms are paying between $4,000 to $12,000; criminals are offering up to $75,000 for Windows XP and $50,000 for Windows Vista vulnerabilities.[8] Security firms will report any bugs to the software editor so it can be quickly patched, as criminals will use them for launching attacks to make more malware profits.

[6] Christophe Auffray, JDN Solutions.
[7] See page 3.
[8] Raimund Genes, Trend Micro's chief researcher.

Browsing the Internet today has become a major security risk for users as their computers are compromised by malicious web pages. This happens mainly because patches are not applied to the browser or protection systems like IDS, or firewalls are misconfigured. Old versions of browsers are being exploited and lead to remote code execution without any action from the user other than loading the Internet page on their screen. Internet Explorer and Mozilla Firefox are the most popular web browsers; both applications have released several patches in 2007 after disclosing vulnerabilities. Similarly to Internet Explorer, unpatched or older versions of Firefox contain multiple vulnerabilities that can lead to memory corruption, spoofing and execution of arbitrary scripts or code. The websites exploiting the browser vulnerabilities typically host a several exploits, and even launch the appropriate exploit(s) based on which browser the potential victim is using.[9] Web applications are also targeted; their weaknesses are offer a wild range of possible attacks, such as Cross-site scripting, SQL injection, Ajax injection or PHP scripts. These attacks will allow remote control of the computer to launch code execution or rootkit installation.



Targeted attacks are focused on office software vulnerabilities; they include e-mail clients, word (Microsoft Word), spreadsheet (Microsoft Excel), presentation (Microsoft PowerPoint) and document viewer (Adobe Reader and Acrobat) applications.

In December 2007, two Russians were arrested for creating and distributing the Pinch Trojan. Ermishkin and Farhutdinov are believed to be behind a highly successful series of Trojans sometimes known as LdPinch and PdPinch. Pinch production was being done in a highly professional manner, with the authors creating 'point and click' tools to quickly get stolen information from infected computers. It has been estimated that the Pinch Trojans infected over 10 million PCs worldwide and the actual financial loss could be huge.

January 2008, a very convincing phishing attack using a cross-site scripting vulnerability on an Italian bank's own website to attempt to steal customers' bank account details was discovered.

Fraudsters are currently sending phishing mails which use a specially-crafted URL to inject a modified login form onto the bank's login page. The vulnerable page is served over SSL with an SSL certificate issued to Banca Fideuram S.p.A. in Italy. Nonetheless, the fraudsters have been able to inject an IFRAME onto the login page which loads a modified login form from a web server hosted in Taiwan.

[9] SANS Institut, Information Security Research Center, November 2007.

In 2006, users would receive an e-mail from actual BBC News stories which offered a link to 'Read More...'. Those who followed that link were directed to a fake BBC website which would exploit the unpatched vulnerability createTextRange on Internet Eplorer browser. The exploit would install a keylogger, monitoring all activities in order to capture data when the user connected for financial transactions. Captured information would be sent to the server's attacker.

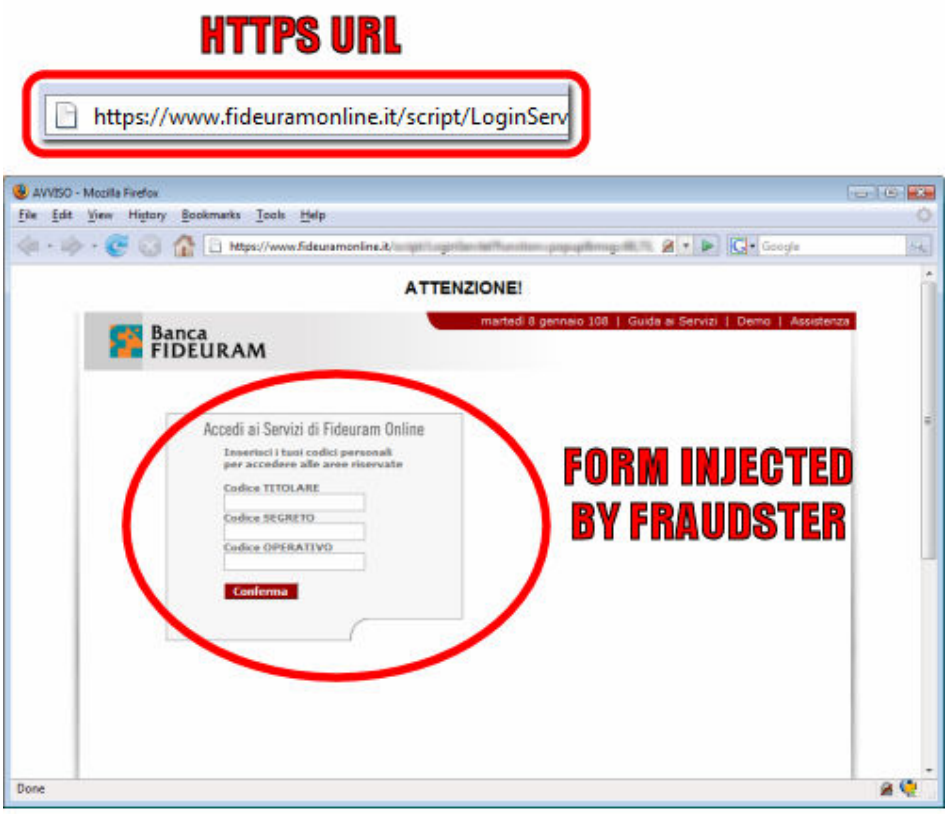


Figure 1 – Fraudsters login form presented on the bank's SSL page (F-Secure)

Cross-site scripting vulnerabilities on banking websites have to be taken seriously as there is no guarantee assured by an SSL site showing an "https" on the Url; nor is it enough to control the name of the domain on the browser.

> Cross-site scripting vulnerabilities on SSL sites also undermine the purpose of SSL certificates - while the attack detailed here injects external content via an IFRAME, it is important to note that a malicious payload could also be delivered solely via the vulnerable GET parameter. In the latter case, any SSL certificate associated with the site - including Extended Validation certificates - would display a padlock icon and apparently assure the user that the injected login form is genuine.
>
> This particular attack is made all the more convincing by the vector used by the fraudsters: the URL employed by the attack injects a series of numbers directly into a JavaScript function call that already exists on the bank's LoginServlet page. This makes it difficult even for an experienced user to identify this as a cross-site scripting attack, as the URL does not look readily suspicious, with the injected content consisting only of numbers and commas.
>
> In a possible attempt to bypass automated security filters, the injected content from Taiwan also contains encoded JavaScript which is used to display the text "Inserisci i tuoi codici personali" ("Insert your personal codes") and "per accedere alle aree riservate" ("To access all reserved

areas"). When the modified form is submitted, the contents are transmitted to the Taiwanese server before the user is redirected to the bank's genuine, unaltered homepage.[10]

2.2 Botnets

Botnets are actually the most pressing problem for any network operator in the world. To create a Botnet, one needs to have a remote control program loaded on computers that go unnoticed by their owner, which leaves the backdoors open for communication with the C&C (Command and Control), which is most often an IRC (Internet Relay Chat) server installed illegally on a high-bandwidth network. Botnets run silently until they strike with increasing speed and power. Millions of infected computers are turned into digital armies controlled by criminals or criminal organisations who use them for only one purpose, making more money. This lucrative business is growing faster and bigger every year, hijacked computers can be used for extortion, spam, "DDoS", phishing, malware installation (rootkits), spyware for identity theft (keyloggers that grab keystroke and bank account information) or other fraudulent activities.

The botnet owner, known as Botherd, has complete control over the zombied machines and he will use the virus/worm/Trojan combined work to keep his army growing. A system enabling check-in for further instructions will be implemented, allowing owners to lead massive distributed denial of service (DDoS) attacks.

Computer infection can be made through various means: infected web pages, e-mail attachments, social engineering and application or operating system exploits. There is no frontier nor barrier to this malware, therefore they are difficult to track as one botnet counts an average of 20,000 hijacked computers from all over the world. There are between 40 to 50 million infected computers worldwide connected to a botnet, with China, USA, Germany, Spain and France being the top five countries for the number of compromised machines.[11]

In 2007, botnets have become extremely aggressive and are using sophisticated techniques which make it nearly impossible for law enforcement to track them down and stop criminal organisation activities. One of them, the fast-flux networks, (made of compromised computer systems with public DNS records that are constantly changing, in some cases every few minutes)[12] has been used by RBN (Russian Business Network), one of the most creative cybercriminal organisations. They were heavily involved in the massive DDoS attacks that struck Estonia in April and May 2007 where they sold a rootkit called Mpack for $700. This Trojan horse has a graphic user interface with a configuration that can be totally customised depending on the owner's choices. The source of attacks can be selected and stolen data, mainly passwords and bank details are encrypted when returning to the user who will log to the back office with his login and password. After the success of Mpack during the Estonian attacks, its price has raised to $1,000, proving that demand for malware tools has increased.[13]

The latest victim of this attack was among the largest financial institutions in India. In late August, the website of the Bank of India was compromised by an Mpack-created virus, which forwarded purloined financial data to drop sites at RBN's network.

[10] Netcraft, Newsletter, January 2008.
[11] http://www.viruslist.com
[12] ITU, International Telecommunication Union, September 2007.
[13] Laurence Ifrah, Robert Schuman Newsletter, September 2007.

2.2.1 Market prices of malwares tools

- **Keylogger Teller 2.0:** typical keylogger; it uses stealth techniques and is quite complete: US$40.

- **Webmoney Trojan:** it captures Webmoney accounts: US$500, but the first 100 will obtain it for US$400!

- **WMT-spy:** Another Trojan to obtain WebMoney accounts but quite cheaper than the previous one (its creator publishes the results it has obtained in virustotal): an executable US$5, updates US$5, the builder costs US$10.

- **Polaris**: Polymorphic encryption for your executables: US$20.

- **Freejoiner**: hides executables joining them with other files for US$30 + US$5 for update.

- **My joiner**: Other joiner belonging to the creator of Pinch: US$10.

- **MPACK**: an application that is installed in a server and allows Trojans to be installed on remote systems using several exploits.

- **Snatch Trojan**: steals passwords and has rootkit functionalities: US$600.

- **Dream Bot Builder**: floods servers for only US$500 + US$25 for update.

- **Pinch**: a make-to-order Trojan creator, very complete. US$30. Update: US$5

2.2.2 The RBN case

RBN (Russian Business Network) is the most notorious player in global cybercrime. The range of their criminal activities is certainly one of the largest possible. The company is offering bulletproof hosting to any website regardless, of the content: child pornography or gambling, phishing, scam, spam, rent of DDoS attacks through their botnet, sale of malware, piracy and ID theft. RBN is a world hub for anything related to cybercrime. Some security experts deduced that RBN was behind most identity theft in the UK.[14] According to Symantec, the gang's online hosting company is blamed for 60% of all criminal activities on the Internet. RBN got famous with their fake antivirus and antispyware software website with infected pages. They used web exploits on Google web search sites to redirect users to a bad website where would get a Trojan infection which would lead to data theft and a zombie PC. The computer would advise the user that it got infected and suggested running an antispyware which would report that some malicious programs were installed and that they should be removed with a simple click on the software. Thousands of users clicked and executed the spysheriff malware causing their machine to crash.

Yet suddenly, on 7 November 2007, they vanished from the Internet. Trend Micro's researchers said they had seen sign of RBN activities in China, Turkey and Taiwan. They believed that the gang was trying to move to places where the law is poorly established. Spamhaus published a note on its website confirming that RBN had set its servers in China late November, then they disappeared again until early January 2008, when they were traced in Panama.

[14] http://rbnexploit.blogspot.com/

November 2007, New Zealand police arrested an 18-year-old-boy who owned a huge network of one million compromised computers. The teenager was suspected of leading a gang who used infected PCs to raid online bank accounts through various phishing scams and ran spams or DDoS attacks on demand.

2.2.3 The Storm Worm

The Storm Worm botnet has been defined as the biggest botnet ever running on the Internet and is suspected to own around five million zombies.[15] It shows a spectacular growth rate, an ability to distribute large volumes of spam and a capacity to avoid detection and eradication.

On January 2007 anti-spam sites and anti-rootkit software developers were targeted by multiple DDoS attacks sent by Storm, which succeeded in shutting down some victim's servers. Spammers have decided to attack anyone's servers or website which could be a threat to their profitable business.

Storm's effectiveness could be attributed to its creativity constantly renewed for sending infected links. E-mails sent kept changing in appearance and subject lines: worm alert spam, e-card, Christmas, weather disaster, holidays or football games. The main fear created by Storm is its potential capability of taking out government facilities and causing much mayhem on the Internet.[16]

From mid-July to mid-September, Storm has sent 1.2 billion emails. A record was set on 22 August 2007, when out of 57 million virus-infected messages tracked across the Internet, 99% of them were from the Storm Worm.[17]

Despite the wide ranging estimates as to the size of the botnet, researchers tend to agree that it's one of the largest zombie grids ever seen – one capable of doing great damage. Matt Sergeant, chief anti-spam technologist with MessageLab, in an interview:

> In terms of power, the botnet utterly blows the supercomputers away. If you add up all 500 of the top supercomputers, it blows them all away with just 2 million of its machines. It's very frightening that criminals have access to that much computing power, but there's not much we can do about it.

Sergeant said researchers see about two million different computers in the botnet sending out spam on any given day, and he adds that he estimates the botnet is generally operating at about 10% of capacity.

"We've seen spikes where the owner is experimenting with something and those spikes are usually five to 10 times what we normally see", he said, noting he suspects the botnet could be as large as 50 million computers. "That means they can turn on the taps whenever they want to."

No one could provide detailed and specific comparisons between the strength of the botnet and the top supercomputers, mainly because it is hard to know for sure the size of the botnet or the power of each computer that is part of the botnet.[18]

In December 2007, Storm released new messages attempting to dupe users into installing its Trojan using links like happycards2008.com and newyearcards2008.com, then a second wave attack began on Christmas Day (an offer to download a free tool to

[15] http://blog.wired.com
[16] http://www.spamhaus.org
[17] Postini.
[18] Sharon Gaudin, InformationWeek, September 2007.

watch Christmas-themed strippers) adding a new malware on its hosting servers; a rootkit to cloak the bot code from anti-virus software. The upgrade is pretty sophisticated, so now Storm has better hiding skills and no visible running processes.[19]

2.2.4 Peer-to-peer

Peer-to-peer networks consist of collections of computers or "hubs" that simultaneously function as both "clients" and "servers" to achieve a common purpose. The hubs may exchange data, share resources, provide directory services, support communications and provide real time collaboration tools. There are around 25,000 computers per hub.

Many legitimate applications use P2P. Software tool vendors, including Microsoft and Sun, provide a variety of tools and encourage the development of P2P applications. However, like any data transfer tool, P2P applications can be misused or exploited to illegally share copyrighted material; obtain confidential data; expose users to unwanted pornography, violence or propaganda; distribute and execute malware (viruses, spyware, bots, etc.); overload the network; mine usage and behaviour patterns; and control bots, all of which can create a legal liability. The liability and legal prosecution may not be limited to the perpetrator and may be extended to the network sponsor, supporters or members.

The P2P networks themselves may be attacked by modifying legitimate files with malware, seeding malware files into shared directories, exploiting vulnerabilities in the protocol or errors in coding, blocking (filtering) the protocol, denial of service by making the network function slowly, spamming and identity attacks that identify network users and harass them. Legal action has been successfully used to shut down some popular networks that were culprits of copyright infringement.

Storm Worm uses eDonkey/Overnet Peer to Peer protocol to communicate with infected hosts. It is estimated to run on as many as 1,000,000 to 50,000,000 infected and compromised computer systems as of September 2007.[20]

One such example is a wave of peer-to-peer attacks that occurred in April and May 2007, where the security firm Prolexic mitigated several extremely large peer-to-peer attacks with over 200,000 attacking computers. Each computer on its own sent a small amount of data, but at any given moment over 80,000 connections was being opened on the victim. Analysis of the attack showed that the attacking computers were not a normal botnet. Instead, the attacking computers were simply running a popular peer-to-peer file sharing client that had been told by the P2P hub server to also connect to a victim. A weakness (now corrected) in the hub software protocol gave attackers the ability to instruct the clients connected to the hub to also connect to a victim's web server. Users of the P2P software would see nothing pop up, and notice little or no degradation to their own connections, so the likelihood of them stopping their contribution to the attack is low. With the attacker doing this to several hubs, each hub managing 20 to 25k clients, suddenly a victim may find hundreds of thousands of IP addresses 'attacking' at maddening speed.

> In September 2007 a former employee of Citi's ABN Amro Mortgage group leaked the personal information, including social security numbers, of more than 5,000 customers via a peer-to-peer (p2p) file-sharing network.[21]

[19] Gregg Keizer, NetworkWorld, December 2007.
[20] SANS security Top 20, 2007.
[21] Channelregister, December 2007.

As stated in January's Zombie Report, 'slow and sneaky' attacks that try to bypass threshold-based DdoS mitigation was a major attack trend in 2007, and the peer-to-peer attacks seen in April and May have a number of characteristics that defeat many types of automated DdoS mitigation systems:

- Each IP sends a small amount of data (no thresholds exceeded);
- Each IP connects at a low-enough rate that normal IP's may connect faster (hard to tell from regular traffic);
- The sheer number of IP's (hundreds of thousands) that add power to the attack;
- While the attacks have a definite signature, blocking hundreds of thousands of IP's fast enough brings problems of its own;
- The real danger is when we start seeing more browser malware attacks, for they can gain all the benefits of this P2P attack vector, but will be slower, sneakier, and look more like legitimate traffic.[22]

On 7 Sept 2007, the U.S. Secret Service, U.S. Postal Inspection Service, and the Seattle Police indicted Gregory Thomas Kopiloff of Seattle for allegedly using information on tax returns, bank statements and credit reports to obtain identity information to defraud consumers, banks and retailers. According to their investigation, thousands of potential criminals each day use P2P networks to steal consumer information necessary to commit identity theft and fraud. According to a four-count indictment unsealed in U.S. District Court, Thomas Kopiloff used LimeWire, Soulseek and other "peer-to-peer" file-sharing programs to troll other computers for financial information, which he used to open credit cards for an online shopping spree. The report said, he bought more than US$73,000 worth of goods online, then resold those items at steep discounts and kept the proceeds.

Chris Boyd, director of malware research for FaceTime Security Lab believes the biggest danger is copyright; but not in the way that one might think. Above having personal data such as credit card details of other information, the risk for a user to have his computer hacked and that the attacker will steal the music he has bought online and upload it to a peer-to-peer network. The victim will potentially be sued for music piracy and face a fine of hundreds of thousands of dollars.[23]

2.2.5 Spam

Unsolicited e-mails represented 94% of all e-mail traffic at the end of 2006, therefore using a large part of bandwidth. Spammers are hosting their databases and websites in offshore locations to providers known as bulletproof hosts or bulk-friendly hosts. Their term of services allow their customers to upload any material or programs or services, such as pornography or online gambling. Spammers are then able to rent their database to anyone, as they guaranty anonymity and they provide tools to create predefined spams.

It takes about 10 minutes to create a spam, one can choose between an e-card, e-mail in HTML or text only. A service called "E-mail Campaign Management" is offering a choice of predesigned layout where the only thing to do is to choose the text colour, add a logo or images. When this is done, the message is then sent to a sample of 25 e-mail addresses coming from the provider's database and an access to the Backoffice gives a detail report of the campaign success. If the beginner is lost he can still go to the online virtual university where a tour of all service and a video showing the 'how-to' are provided for free.

[22] Prolexic 2007 report.
[23] Stephanie Jordan, October 2007, http://www.messagingnews.com

Of course this service is promoted using their actual spamming tools; below is an example of a bulk e-mail hosting company:

> We are the marketing specialists that provide cheap bullet proof bulk e-mail friendly hosting for your website ($400 for one month of bullet proof hosting) and cheap bulk e-mail campaigns ($200 for 1 million emails sent).
>
> As you may already know, many web hosting companies have Terms of Service (TOS) or Acceptable Use Policies (AUP) against the delivery of emails advertising or promoting your web site. If your web site host receives complaints or discovers that your web site has been advertised in e-mail broadcasts, they may disconnect your account and shut down your web site.
>
> Adult and gambling sites welcomed. No set up fee.
>
> We only ask $200 us dollars for 1 million emails sent with your ad.
> We don't use duplicate emails.
> Our e-mail base is up to date and it is updated weekly.
> Our current e-mail data base contains over 50,000,000 emails sorted by various parameters to meet your specific needs.
> No competitors may offer this price.
> The lowest price you can find on the net is well over $500 for 1 million.
> Don't make the mistake of bulk emailing directly to your website without bulletproof web hosting.
> Your web host will close your account and shut your site down in no time!
> No matter how long you have been with them, how much you are paying them, or how beautiful your site is.
> There are companies charging thousands for bulletproof web hosting and they can't keep you up and running like we can.
> If you host with us, your site will NOT BE SHUT DOWN due to complaints! Bulk e-mail campaign together with bullet proof hosting will bring your business to success.
> Just imagine how many people will learn about your business or product at a really low price. Bulk e-mail is considered to be the most effective way to advertise on the net. It is hundreds times effective than banner, solo ad and other campaigns.
> Once people use our service they always come back for more.
> E-mail us, targetemailrequest@xxx.net.cn for more information and to order your bulk e-mail hosting or/and e-mail campaign.

Antivirus software firm; BitDefender's 2007 Top 10 spam list includes:

1. Penny stocks spam
2. Drug spam
3. Pornography
4. Replica watches
5. Loans
6. Phishing spam
7. Pirated software
8. Fake job ads
9. Dating site spam
10. Fake diplomas

According to Spamhaus, the anti-spam organisation, 200 professional spam gangs are responsible for 80& of the high volume of junk mail pumped onto the Internet every day.

Public enemy number one is a Ukrainian known variously as Alex or Alexey, a prolific user of botnets, networks of PCs compromised with malware, to send out junk mail in association with a Russian spam gang called Pavka/Artofit. Alexey is involved in distributing child porn spam, among many other types of unsolicited junk mail.

The world's second worst spammer, is allegedly Leo Kuvayev, also in relation with Pavka/Artofit. Kuvayev was fined US$37 million for his anti-social activities by a Massachusetts court in October 2005.

Spamhaus's number three offender, Michael Lindsay of iMedia Networks, runs a spam-hosting operation in the US that is used by numerous other junk mail firms. Down at number eight on the list, but well-known to law enforcement agencies is Western Europe, is Alexey Panov, an author of software used to send spam from compromised computers.

Four of the world's most prolific spammers in Spamhaus's Register Of Known Spam Operations (ROKSO) database are from Russia and two are from the US. The other four members of the rogue's gallery are from Canada, Hong Kong, Israel and the Ukraine. Between them they push out a huge volume of junk mails about porn, penis pills, loans, stock scams and other assorted illicit matters.[24]

Spam technique that uses subliminal messages

Madrid, 5 September 2006 – Panda Labs has detected a spam message that uses subliminal advertising techniques. At first glance, it is an advertisement that gives the user the opportunity to but certain stocks online. However, the user not only sees a static image, but also a sequence of images that are displayed extremely rapidly. To be more specific, there are four images, three of which show the word "buy" in different positions.

> Subliminal advertising techniques have been used for a long time and are based on composing images that users perceive, even though they are not aware of it. In the case of this e-mail message, the word "buy" appears on screen for a maximum of 40 milliseconds, and in some cases, for only 10 milliseconds. By doing this, although the recipient is not consciously aware of the "buy" message, the subconscious levels of perception receive it and store it, influencing the recipient.[25]

Panda Labs also reported the existence of emails with a link to YouTube that invite recipients to watch a video. Recipients who click the link are redirected to a page with an online casino video.

2.2.6 Pump and Dump

Pump and Dump is a highly illegal stock market practice where a small group of informed people buy a stock of a company shares before they recommend it to thousands of investors. The result is a quick spike in the stock price, followed by an equally fast downfall. The perpetrators who bought the stock early sell off when the price peaks at a huge profit. Most pump and dump schemes recommend companies that are over-the-counter bulletin board (OTCBB) and have a small float. Small companies are more volatile and it is easier to manipulate a stock when there is little or no information available about the company. There is also a variation of this scam called the "short and distort". Instead of spreading positive news, fraudsters use a smear

[24] John Leyden, The Register, November 2006.
[25] Oxygen3, Panda Software.

campaign and attempt to drive the stock price down. Profit is then made by short selling.

Example of Pump and Dump spam e-mail:

> Company Name: P E R M A N E N T T E C H (Other OTC:PERT.PK)
> Symbol: P E R T . P K
> Current Price: 0.46
>
> WEDNESDAY Target: 1.00
>
> The first Big Release for 2008 from Investors Alert!!!
>
> Investors are starting to move on *PERT* as news concerning recent
> expansions begins circulate.
> Get ahead of a climb and reap the highest returns.
>
> Watch for more news and get on *PERT* first thing on Wed *Jan 02, 2008*.
>
> What a GREAT way to start the New Year with a 200-300% profit on your investment.

These e-mails always come with capitalised letters and many exclamation marks, besides promising huge results with no risk; the spammers use free e-mail providers such as hotmail, yahoo or gmail to hide where the original message comes from. Obviously, no legal firm would use this scheme, so the only wise thing to do is to delete the e-mail.[26]

In August 2007, the security software vendor Sophos detected one of the biggest online stock manipulation campaigns, increasing global spam levels by 30% in 24 hours. About 500 million e-mails containing advice to invest into a company named Prime Time Stores in Puerto Rico and goes on to say:

> Imagine if you had the chance to buy a Wal-Mart franchise in Mexico right when it first opened its doors there and all you needed was a small stake to get in.

The stock rose 2.35% in morning trade in the United States on Wednesday to 0.087 dollars, but gained 30% on Monday and 14.8% on Tuesday, in the days running up to the detection of the campaign. Sophos estimates that "pump-and-dump" stock campaigns account for about 25% of all spam nowadays, up from less than 1.0% in January 2005. The e-mails promoting Prime Time Stores stock, which are being propagated by thousands of virus-infected home computers whose owners are unaware, has a PDF attachment that contains the investment advice. The use of a PDF file, a special document-friendly format, makes it easier for the e-mail to slip through spam filters.

[26] http://www.investopedia.com

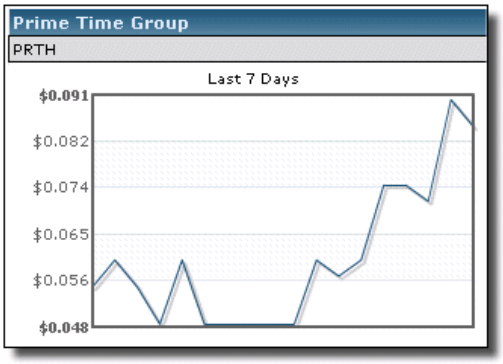


Figure 2 – Price share evolution of Prime Time Stores company[27]

The US Securities and Exchange Commission (SEC) suspended trading in 35 firms as a punishment after the companies were frequently referenced in pump-and-dump stock e-mail campaigns.

> Aleksey Kamardin reaped $13,158 in just 104 minutes by buying and selling penny stocks. The 21-year-old bought 43,000 shares in a small Wisconsin equipment company that makes, among other things, potato harvesters. He sold the shares less than two hours later at nearly double the investment.
>
> But Kamardin's is no success story. Instead, federal authorities say, his methods place him at the front of a wave of techno-criminals who meld computer hacking with identity theft to create nightmares for legitimate investors. Kamardin and his accomplices allegedly hacked into four online trading accounts of unsuspecting investors, selling off their holdings in higher-valued companies to purchase shares in Thomas Equipment, a firm whose stock that day soared from 26 cents to 80 cents a share, authorities said. The trading volume of Thomas increased tenfold. Kamardin, allegedly part of an East European ring, repeated this scheme on 13 other occasions in July and August, defrauding investors of $82,960, according to a civil complaint filed yesterday by the Securities and Exchange Commission.[28]
>
> ***
>
> Two Texas men, Darrel and Jack Usleton, were accused of running a massive stock spam scheme using botnets. The Texas attorney general has also filed charges against the Useltons, alleging organised criminal activity and money laundering. The Texas AG has seized more than $4.2 million from bank accounts belonging to the two men and the SEC alleges that the Useltons may have defrauded investors of more than $4.6 million in all. Those numbers show just how much money is involved in stock spam.[29]

By October 2007, virtual stock spammers had abandoned pdf files and image spam for a new campaign featuring MP3 files. These audio files were widely spammed in e-mails mostly without any subject line or message body. Some of the filenames used included hurricanechris.mp3, allforone.mp3, carrieunderwood.mp3, elvis.mp3, baby.mp3, fergie.mp3, and bbrown.mp3. The female (apparently British) voice on the MP3 file, recorded at low bit-rate and randomly altered to avoid detection by anti-spam filters, seeks to attract interest in Exit Only, a Canadian firm that runs a website marketplace for new and used motors.[30] Anti-virus firms advise users to block MP3 files in e-mail.

[27] Image from Sophos PLC.
[28] Ellen Nakashima, Washington Post, January 2007.
[29] http://www.sec.gov, July 2007.
[30] Sophos PLC.

2.2.7 DDoS

Distributed Denial of Services is the commonest form of attack to date and it enables the perpetrator to saturate the targeted servers with false requests, to the extent of rendering them unavailable for a length of time, varying from a few minutes to several days. Servers configured to cope with a certain number of requests are unable to transmit the required data if the volume of connections becomes excessive. It is very difficult, even impossible in some cases, to counter this type of attack; hence its success. Offered as an online service in the underground Internet forums or newsgroups by criminals or criminal organisations, prices are subject to the length and strength of attack requested by the client. It can cost between $US 10 to 20 for one hour strike, up to $40 for 2 hours and about $US 100 for one day. Being very professional, the criminal's offer includes a 10 minute test to evaluate quality of the service. Promotional sales can give up to 20% reduction for the first 100 clients.[31]

Extortion Dos attacks seem to have declined since mid-2006 as they are no longer profitable to attackers.[32] More victims refuse to pay, therefore the criminal has to perform an attack for which he won't get paid; he is losing time and putting himself at risk for nothing. One point that is making extortion difficult to organise is the antispam filter in companies, rules for fighting spam are automatically deleting threat messages so no one can answer to the attacker. He has no other solution than to send the attack. A more cost effective approach is the DDoS on demand where the attacker receives a prepaid order to launch an attack to a specific target. Criminals are paid to just provide the service and this kind of offer is rising dangerously as legitimate businesses are willing to turn to cybercriminals to help them cripple rival websites.[33] DDoS offers a tremendous amount of destructive power at criminals' fingertips.

However whilst extortion is declining, it is still present; at the beginning of November 2006, Russian authorities jailed three criminals who used DDoS attacks to blackmail online businesses. Ian Maksakov, Alexander Petrov and Denis Stepanov were each sentenced to eight years for extorting more than £2m from UK online casinos after threatening to hit their websites. Apparently, they made more than 50 similar attacks in 30 countries in six months. Canbet Sport Bookmakers refused to pay a £5,000 ransom and lost £100,000 when its business was taken down for days.[34]

End of April 2007, Estonia was heavily struck by massive DDoS attacks, after the government had decided to remove from the centre of its capital, Tallinn, a statue representing the victory of the Red Army troops over the Nazis at the end of WWII. 128 DDoS attacks were recorded by Arbor Networks. Most of them did not exceed one hour; the most aggressive of over 90 Mbps, lasted ten hours. This corresponds to downloading the whole of Microsoft's Windows XP operating system every six seconds. As a result, the Parliament, Finance and Agriculture Ministries, banks and insurance websites were immediately unavailable, a particularly difficult situation since 97% of bank services are only provided online.[35]

[31] Laurence Ifrah, *Défense nationale et sécurité collective*, Publication of August/September 2007.
[32] Yazan Gable, Symantec Weblog, April 2007.
[33] Dancho Danchev's blog related to BBC News website.
[34] Tom Young, Computing, November 2006.
[35] Laurence Ifrah, *Défense National et sécurité collective*, August/September 2007.

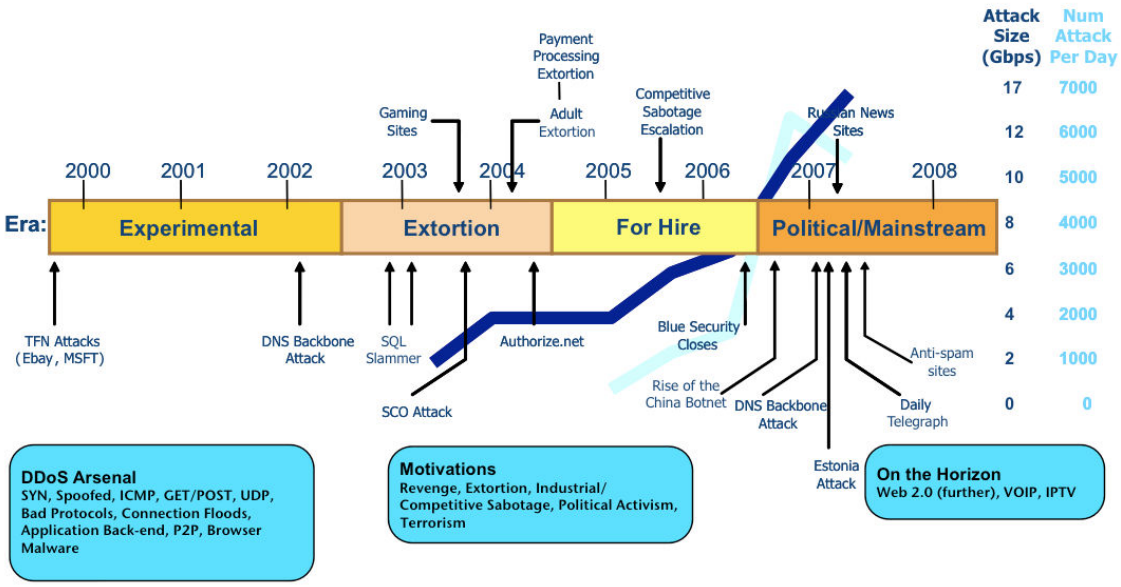


Figure 3 – New motivations for DDoS attacks – Prolexic's zombie weather 2007 report

3 Fraud on the Internet

3.1 Phishing

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal data, such as ID and/or financial account credentials. Although lure e-mails and counterfeit websites are the most prominent phishing techniques, there is a rise in alternative methods to co-opt consumers' online credential or gain control of their accounts without using direct deception. The APWG[36] saw that in Brazil, the population was attracted to generic entertainment sites in order to plant keyloggers.[37] Phishers hacking a server's database offers many advantages, being one hack for thousands of data, plus it allows attackers to prepare for the victims credible phishing mail that plants malware on their machines. Phishing attacks are, according to Websense and the APWG, classified in the following types:

Phishing-based Trojan – Keyloggers

This kind of attack is designed in order to collect information on the end-user for stealing his credentials. Their tracking components are created to start the malware program when the user is connecting to his bank website or any other financial establishment, ecommerce sites and web-based mail sites.

Phishing-based Trojan Redirectors

Malware code in this situation is trying to redirect end-users network traffic to a location where they did not intend to go to. This is happening by changing hosts files or using DNS redirection by modifying bookmarks of infected computers. Browsers are then opening counterfeited sites opening PCs to reveal personal data and get criminals to record them for ID fraud or other illicit means.

Man-Int-the-Middle Phishing or Pharming

This attack intercepts information in between two parties' communications in order to redirect users to a fraudulent location.

Others

- Typo-attacks: mistyping a popular domain to redirect users to infected websites.

[36] Anti-Phishing Working Group.
[37] Keyloggers are programs used to record keystroke and screen shots and send them in a stealth way to the attacker.

- Search-engine poisoning: being directed to a fraudulent website, through a simple research on a search engine.

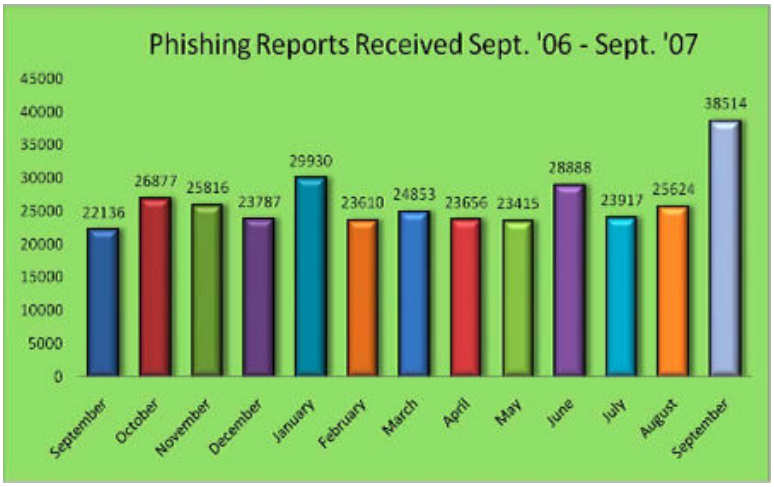


Figure 4 - September saw a substantial increase in phishing attack reports, amounting to a more than 28% rise from the previous high in January 2007[38]

In May 2007, a powerful phishing technique able to spoof eBay, Paypal and other top web destinations without triggering antiphishing filters in IE 7 or Norton 360, was revealed by a reader from TheRegister, Matty Hall. Having updated and patched both applications, he tried to log onto the Paypal website and realised he was asked for his date of birth, social security number, mother's maiden name and credit card details. Poor grammar and awkward syntax showed it was a counterfeited website:

> We have noticed an increasing fraudulent activity recently. In order to provide your security and protect you from fraudsters we have introduced a new system of identification that will help us to avoid any kind of fraud or unauthorised access. Please enter as more information as possible to provide your complete identification and to activate all the features of the new system.

Roger Thompson, who tracks web exploits for Exploit Prevention Labs, guesses those experiencing this attack have inadvertently installed an html injector. That means the victims' browsers are, in fact, visiting the PayPal website or other intended URL, but that a dll file that attaches itself to IE is managing to read and modify the html while in transit.[39]

November 2006, more than 20 FBI offices are said to be involved in the investigation into the global identity theft ring, which is claimed to have carried out a phishing attack against a major financial institution. The criminal gang was established in Poland (where the alleged leader was living), USA and Romania. They were selling stolen identities, credit cards and bank accounts details using machines to encode data on blank credit cards.

Another interesting case was discovered in October 2007, when the SVP National Police Academy in India was found to host on one of their server a Bank of America phishing site.[40]

[38] Graphic from Websense Inc.
[39] Dan Goodin, TheRegister, May 2007.
[40] F-Secure.

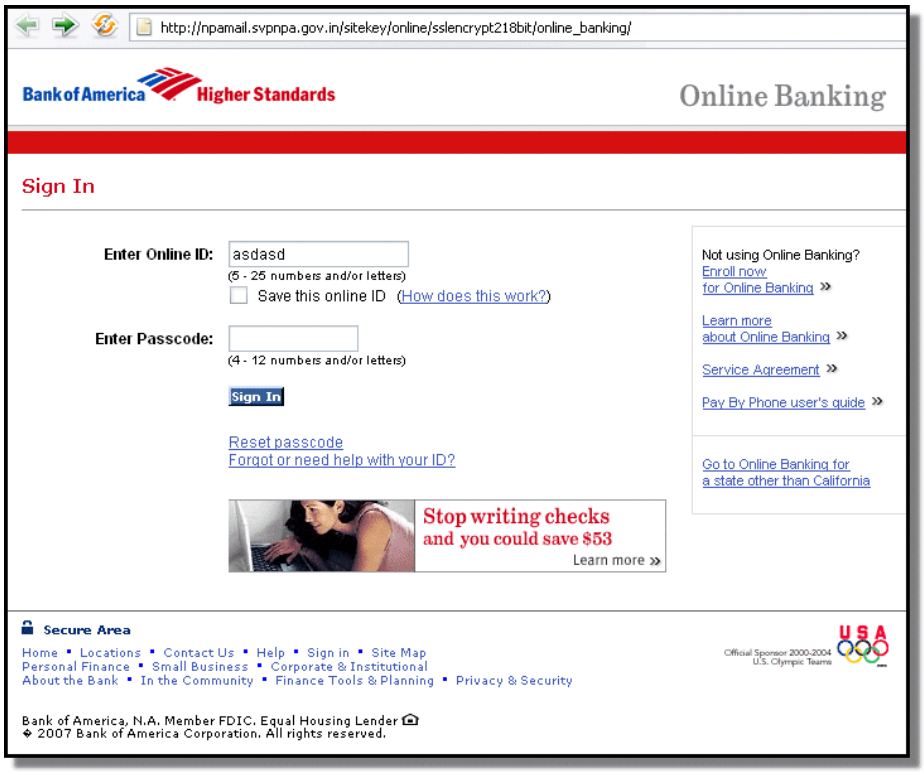


Figure 5 – Screen shot of a fake site of Bank of America hosted on a compromised server from the Police Academy in India.

End of 2007, a website selling cannabis appeared to be a phishing site, proving that selling drugs online was a success. Criminals concluded that if drug addicts were able to find money to provide themselves with herbs, they could then be a target for phishing.

3.2 Banks

Online services such as banking are suffering from the emergence of a complex and highly technical market for malware. Criminal organisations are developing sophisticated keyloggers which will only get a screen shot of the end-user's computer if he is connecting to his online bank. Security experts estimate that one in three computers worldwide is infected with some version of software that steals personal identification numbers (PINs), passwords and personal data — and delivers it all to online crooks.

In January 2008, a virus has been released to target any end-user trying to access his bank online. "Silentbanker", is a Trojan horse virus that computer users can unknowingly download onto their computers by simply browsing websites. It operates undetected, between the computer's user and his bank website, giving the criminal full access to his credential and therefore freedom to drain his account.

As a 'more conventional' type of cyber banking fraud, phishing is redirecting customers towards fake bank's websites. This is done either by sending false e-mails or by using a malicious program that will modify the user's cache DNS (high volume of attacks can be attributed to automated bot-controlled phishing attack kits utilising "fast flux" network infrastructure) or his bookmarks.

Customers of ABN Amro were lured to bogus websites in Hong Kong which were set up to gather security details. Money stolen from their accounts was then transferred to Russia and other countries.[41]

3.3 Emules

A "money mule" or "money transfer agent" launders funds obtained as a result of phishing and Trojan scams. After being recruited by the fraudsters, money mules receive funds into their accounts and they then withdraw the money and send it overseas using a wire transfer service, minus a certain commission payment. Fraudsters recruit 'money mules' through spam e-mails, newsletters, advertisements in newspapers, online job websites and chat rooms. They pose as 'financial managers' or other top level functionaries for international money transfer companies and clearly mention that no specific skills are required.

So mules are lured into working as some sort of Financial Manager. Next, they are required to open an account, or eventually use their own bank account where the criminals will deposit funds stolen from their phishy victims. Mules will be asked to transfer money to overseas' banks minus a small percentage.

Money mules end up getting burned as soon as the phish-site victims realise that their credit cards or identities have been compromised. In addition to possible trouble with the police, the money mule gets to pay back the banks and institutions that were involved in the fraud while the crooks disappear into anonymity.

Dutch police have arrested 14 suspects who allegedly lent their bank accounts at ABN Amro to cybercriminals in Russia and Ukraine. After being recruited by the fraudsters, the mules received funds taken from phishing scams, which they transferred overseas. In April the bank compensated at least four customers for undisclosed amounts taken from their bank accounts.[42]

Law enforcement authorities in Prague charged a man with assisting in fraud, after arresting him at a bank where he allegedly attempted to pick up cash wired to him by phishing victims.

The man - thought to be a middleman, or "mule," used by a phishing gang to pick up proceeds of the scam - is the first to be arrested for such crimes in the Czech Republic, according to newspaper accounts and a statement released by antivirus firm Sophos. The man had allegedly tried to withdraw tens of thousands of Czech Crowns (Koruna), equivalent to thousands of U.S. dollars at the current exchange rate.

An online banking scam has arrived in India in December 2007, where unsuspecting people are made to transfer stolen money for fraudsters, in what is being called a money mule operation. Banks have gotten cautious, after such an incident was recently noticed at an Indian bank.[43]

3.4 Counterfeit products - Medication

If botnets are used to send billions of spam e-mails, mostly concerning the sale of drugs without a prescription, end-users are also actively searching pharmacies online to buy products, which are not allowed in their countries. In France, nearly all forums display requests from users looking for diet pills and websites that provide them. Because of

[41] Jan Libbenga, Channelregister, December 2007.
[42] Jan Libbenga, Channelregister, December 2007.
[43] Indiainfo.com, December 2007.

the prohibition of these kinds of products, people are ready to pay very high prices as they strongly believe that it would be the only way to lose weight. Other products are on the top list, all of them require a prescription. Criminals quickly understood the huge profits they could make from selling counterfeited medicines; they offer a large range of products from anti-depressants to pain-control and provide 20% revenue out of any order placed for those who are interested in the affiliate program. The most desired brands are among others: Viagra, Cialis, Xenical, Tamiflu, Zocor, Prozac.

Top ten countries in December 2006, ranked by counterfeit seized/discovered medicines[44]:

1 – Russian Federation
2 – China
3 – Korea
4 – Peru
5 – Colombia
6 – USA
7 – UK
8 – Ukraine
9 – Germany
10 – Israel

Counterfeit medication is a massive health disaster: 70% of anti-paludism pills are fake in Africa and about 10% of the total drugs in the world. When sold online, these numbers raised dangerously, reaching nearly all of offshore pharmacies with no physical address or official contact. It is a silent disease and thousands of people are dying of counterfeited medication each year.

In March 2007, a 57-year-old man died of poisoning after purchasing medicine on the Internet. The medication was laced with dangerous mineral traces of uranium, strontium, selenium, aluminium, arsenic, barium and boron.[45]

Christopher Smith, a notorious spammer was sentenced to 30 years in prison by a US federal judge in July 2007 for sending more than one billion spam e-mails promoting penis pills, Viagra and for selling prescription drugs without licence. On May 2005, authorities raided Xpress Pharmacy and Smith's home, seized his false passport and $4.2m in assets. The 25-year-old man was making about $18m that year from his business. The following month, Smith was back to work running new websites under false names, selling drugs online without prescriptions through a Dominican call centre.

A former doctor from New York state has pleaded guilty to a charge related to a multistate ring that allegedly used the Internet to sell $US 40m worth of steroids to professional athletes.

Ryan Wheele, 31, from Ohio, US, was charged in September 2007 with one count of conspiracy and one count of trafficking in counterfeit prescription drugs, namely Viagra, Cialis and Levitra. Wheele had met a co-conspirator on the Internet who was acting as an Internet pharmacy, and agreed to receive prescription drugs in bulk and distribute these drugs by mailing them to individuals.

The man had set up a post office box address and received packages which were sent by the co-conspirator. These shipments came from such countries as Pakistan, India, and Great Britain. They contained large quantities of pills in bulk of counterfeit Viagra,

[44] Valerio Reggi, IMPACT: International Medical Products Anti-counterfeiting Taskforce, March 2007.
[45] Ian Austin, Canada.com, March 2007.

Cialis, and Levitra tablets. In many cases these counterfeit pills were not uniformly the same. He would then spread out the bulk order of pills, sort through them, and fill these vials by hand in unsanitary conditions such as the sink area of his basement where his pet cats live.[46]

3.5 Counterfeit products – Diplomas

Criminals have expanded selling fake university degrees online into a veritable industry. The state of the art academic fraud includes not only diplomas, but fake transcripts and recommendation letters, bogus "verification services", even fake accrediting organisations - all apparently designed to make the degree look real. The practice appears to be on the increase across the world, bringing a costly threat to societies and therefore becoming a matter of extreme concern, as the pressure for professional qualification grows.

Prices are from $70 to $700; the gap depends on how sophisticated the diploma needs to be (simple degree to full range of degrees with complete transcripts); delivery takes only few days. Counterfeited diplomas bear the names of real universities; they also provide an unlimited hotline service so if anyone calls the phone number to check if the degree is real they will get a positive answer. Any additive mark such as a hologram or choice of quality papers will be included to fool the unwary person.

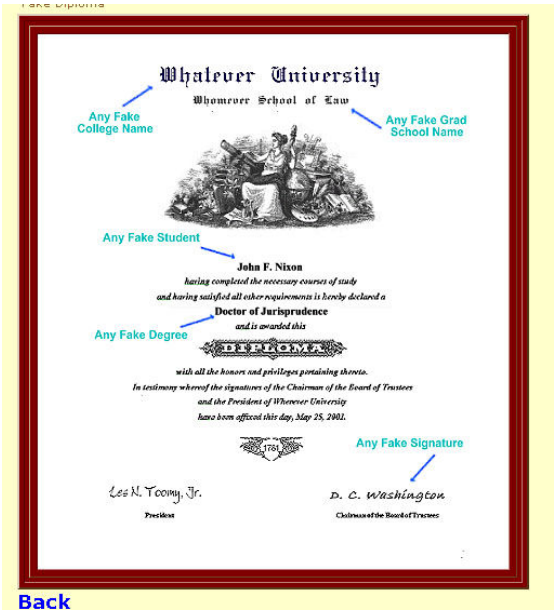


Figure 6 – Fake diploma allowing buyer to choose all information from name of the University to the grade desired.

> Two former college students avoided jail when they pleaded guilty Thursday to a charge related to paying school officials to falsify their grades and transcripts.
>
> Uzi Azizov, 22, and Boris Yakubov, 25, pleaded guilty to a misdemeanour state charge of falsifying business records. Each was sentenced to seven days of community service and fined $1,000.[47]

[46] United States Department of Justice, September 2007.
[47] The Associated Press, December 2007.

3.6 Counterfeit products – ID Fraud

ID fraud is mostly used for financial reason, but other means are making this lucrative business explode online:

Professional ID cards; criminals are offering simple do-it-yourself kits where the only thing to do is to type in personal information, add a picture and laminate with the material provided. Holograms are also available with pocket clip for official high grade ID cards.

- Company ID's/Badges
- Security Badges
- Name Badges
- Special Event ID's/Badges
- Special Occasion ID's/Badges
- Child ID Cards
- Custom ID's/Badges
- Badges for Police Units or grade for military officers
- Driving licence
- Visa Card
- International / national ID card
- Social Security Card
- Student Card

Figure 7 – Sample of a fake ID card available online.

ID profiles are worth a lot more than credit card details, as mentioned by Gunter Ollman, a security researcher for IBM. He discovered in November 2007 that a list of 2,000 credit card complete details is worth about the same as 40 standard identities (i.e. name, address, phone number, social security number, and date of birth).

Complete banking identities - including full contact information, mother's maiden name, bank account number, and account password – can be worth eight times as much as standard identity details, depending on the bank. Although stolen credit card details rapidly go out of date, the same is not true for identities which are, of course, much harder to cancel.

"Identity" itself is now a form of currency, according to Ollmann, who reports that it is more common for identity information to be traded rather than sold.[48]

> Twenty people have been charged in a Southern California identity theft ring that allegedly committed millions of dollars in fraud. The suspects, whose names were not immediately available, face charges of conspiracy, identity theft, making false financial statements and receiving stolen property, the police said. The group committed $2 million in fraud last year

[48] http://blogs.iss.net

alone. Investigators seized computer equipment, victims' identity profiles, counterfeit checks and records of wire and real estate fraud, as well as firearms and drugs.[49]

***

The 46,000 people reportedly infected by ads on job sites may be only a fraction of the victims of an ambitious, multi-stage attack that has stolen data belonging to several hundred thousand people who posted resumes on Monster.com, a researcher said this weekend.

According to Symantec Security Analyst Amado Hidalgo, a new Trojan horse the company calls Infostealer.Monstres has stolen more than 1.6 million records belonging to several hundred thousand people from the job search service Monster.com. That data is then used to target the Monster.com users with credible phishing mail that plants more malware on their machines. The personal information from Monster.com includes names, e-mail addresses, home address, phone numbers, and resume ID number who traced the data to a remote server used by the attackers to store the stolen information.

Infostealer.Monstres ripped off Monster.com by using legitimate log-ons, likely stolen from recruiters and human resource personnel who have access to the "Monster for employers" areas of the site. Once inside, the Trojan ran automated searches for resumes of candidates located in certain countries or working in certain fields. The results were then uploaded to the attackers' remote server.[50]

The US Secret Service has worked with local authorities to arrest ID thieves in Canada and France.[51]

The U.S. Secret Service has cracked down on an international ID theft ring that is responsible for more than US$14 million in fraud losses. On June 2007, French National Police arrested four on online fraud charges, acting on information provided by the Secret Service. The arrests were part of an undercover investigation into the activities of an online criminal known by the alias, "Lord Kaisersose", who is "associated with Internet sites known for identity theft and financial fraud activities".

Investigators found more than 28,000 stolen credit- and bank-card numbers as a result of this operation, the Secret Service said. "Fraud losses associated with this investigation have exceeded US$14 million".

In the UK, at the end of 2007, detectives who were asked to investigate on important purchases (holidays, mobile phones, iPods and other expensive items) made by a very young user, faced a horrific ID fraud business. The actual big spender identity belonged to a baby who had died at the age of seven months old. The detectives discovered that the identities of hundreds of babies were stolen, used to make purchases and finally sold on the Internet for an average price of £30. Experts believe that about four million Britons have been victims of ID theft.

November 2007, 25 million Britons had their sensitive personal details exposed to the risk of ID fraud. Names, addresses, birth dates, national insurance number and bank account details of every child benefit claimant in the country were engraved on two CDs; the CDs were then posted by a junior employee; both disks never reached their destination. If the data were to fall into the hands of organised crime, the risk of ID fraud is extremely high. Thieves could plunder bank accounts, obtain credit cards or loans.[52]

[49] http://www.sfgate.com
[50] Computerworld, August 2007.
[51] Robert McMillan, IDG, June 2007.
[52] http://timesonline.co.uk

3.7 Counterfeit products – others

Nearly everything is counterfeited and available online: branded watches, jewels, clothes, commercial software, music, movies, IT devices (phones, PDAs, computers), etc. You name it, you can find it on the Internet. According to a UNICRI report, "Counterfeiting: a global spread, a global threat", organised crime has developed a massive industrial counterfeiting production which is using the same routes as drug, human or weapons trafficking. Financial loss for European countries is as high as €3.7 billion just for toys and sports item sectors. It also represents the loss of more than 100,000 jobs each year.[53]

3.8 Ebay fraud

The auction website is so successful that criminals have created specific frauds for it among all the usual ones which have also being customised just for Ebay. ID theft is one of them.

The online auction site eBay has been targeted by identity thieves, who have a botnet that uses brute force to uncover valid account log-in information. According to Elzam, the product manager of Aladdin's eSafe threat-protection line, the brute-force attacks are launched by a large botnet that the identity thieves have built using a sophisticated, multistage campaign that begins with compromised legitimate websites. The resulting botnet is used to call an eBay application programming interface (API) with pairs of possible usernames and passwords allowing the Trojan horse-infected PC – the bot – to communicate directly with the eBay database using XML-formatted code. If the database contains the username-password pair, it responds, which the Trojan horse notes, then later transmits to a hacker controlled server. With enough username-password combinations – the brute-force part of the attack – the criminals can uncover a limited number of real credentials.[54]

Hacking legitimate Ebay seller accounts is providing criminals with a highly positive customer satisfaction rating, so they can use it to list fraudulent auctions. To make it work quickly and efficiently, hackers will try to sell cars or other costly items and will require a money transfer payment with a favour for Western Union services. Of course, nothing will be delivered to the buyer who has lost the total amount wired.

> A Canadian man was scammed out of $20,000 when he tried to buy a car through eBay to seller with 98% positive rating. Six weeks after he wired the money, he still hadn't received the vehicle; he then realized he had been scammed like 1,000 other Canadians since 2000.[55]
>
> Two Convicted of selling $6 Million Worth of Counterfeit Software on eBay. Robert Koster of Jonesboro, Arkansas; pleaded guilty to selling counterfeit Rockwell Automation computer software over the Internet. The software sold by the two defendants had a combined retail value of almost $6 million. Each defendant faces up to five years in prison, a fine of $250,000, and three years of supervised release. The defendants will be sentenced before Judge Stadtmueller in November 2007 along with four additional defendants who previously pleaded guilty in Milwaukee on April 26, 2007.[56]
>
> ***

[53] AFP, December 2007.
[54] ComputerWorld, September 2007.
[55] CBC, November 2007.
[56] Department of Justice, June 2007.

> Two eBay traders agreed this week to pay a total of $100,000 in damages after they were caught selling illegal copies of Norton security software. Liu and Tian completed well over 8,000 auctions on eBay over the past two years. They sold software having a retail price of more than $750,000, for approximately $123,000. Kevin Liu said: "If I had known that SIIA was checking eBay for software piracy, and if I had known the software was pirated and that I'd have to pay such a high fine, I would have never sold the pirated software to begin with."[57]
>
> ***
>
> A Madison man who sold coins on eBay for several years until he suffered losses in commodity trading and gambling pleaded guilty in federal court in connection with defrauding customers of $171,000. Between May 1 and Dec. 29, 2006, John E. Paul took payment from 24 customers for collectible coins he auctioned on eBay's Web site without sending them their merchandise.[58]

Auction sites are also used to sell illicit items, all kind of counterfeited products from software to clothing brand. It is also possible to find the field manual for sniper training from the Headquarters of the Department of the American Army to the Anarchy cookbook where one can find all recipes to make a bomb at home. Websites like Ebay are the ideal place for selling stolen items such as art, computer, cell phone, etc. Criminals who buy goods with a stolen credit card sell them on an auction website in order to get cash. A mule account receives the payment from the buyer and the mule will withdraw it in cash to forward it to the criminal via Western Union.

3.9 Illegal Drugs

Drug traffickers are increasingly using the Internet to sell illegal narcotics ranging from ecstasy to heroin to consumers around the world, according to a senior Interpol official. "There is a risk of massive distribution, it is quite easy to purchase drugs on the Internet", Interpol's sub director for the fight against organised crime and drugs, Emmanuel Leclaire, told a news conference in Marrakech in November 2007.

Narcotics are being sold on e-commerce websites, materiel to grow marijuana plants inside or outside the house are available on legal websites. Help and know-how can easily be found on forums, blogs and demonstrations are even published on youtube or dailymotion. Criminals are even selling guaranteed drug-free substitution urine kits in order to pass any drug test, available for men and women; these kits are delivered in 24 hours to the end-user. This shows how criminals handle every step of illicit activities, helping illegal consumers to hide from authorities as the websites inform about which kind of drugs are looked for in a drug test; alcohol, amphetamine, barbiturates, benzodiazepines, cannabinoids, cocaine, opiates, phencyclidine. Each substance is detailed with its medical use if any, route of administration and detection times. Tests for Ecstasy, cocaine or marijuana are available for $5.95 each.

> The Narcotics Control Bureau arrested the CEO and president of an ISO 9001:2000 company based in Salt Lake's Sector V on the charge of trading in illicit drugs online.
>
> Sanjay Kedia, an alumnus of IIT-Delhi, was charged under the Narcotic Drugs and Psychotropic Substances Act and remanded in judicial custody for two weeks by a Barasat court, India. The arrest, which sources said was the first for such a crime, came after NCB sleuths stumbled upon a syndicate operating an online drug pharmacy that offered to sell narcotics and other

[57] http://www.out-law.com
[58] CoinLink.com, September 2007.

psychotropic substances. After taking orders from customers across the globe, they were sending the drug consignments through post with misleading names as labels.[59]

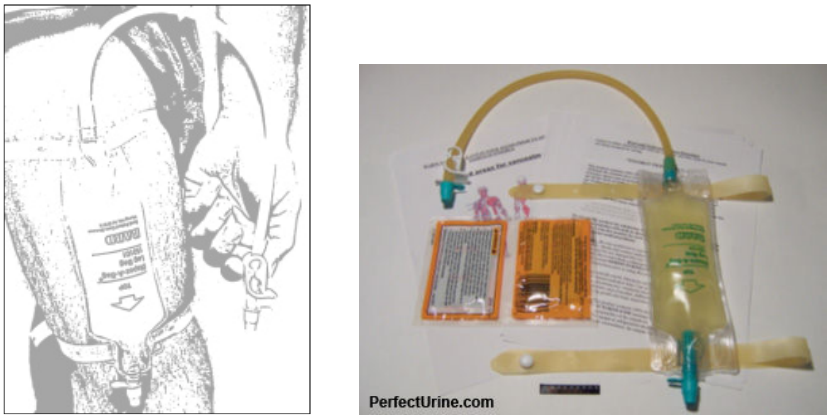


Figure 8 – Drug free urine kits

In Geneva, Switzerland, the Police arrested a gang of eight who were selling marijuana online. The leader, a 30-year-old woman, was living of of this business with her brother, five deliverymen and the Webmaster. The website began the operation at the end of 2006, they had registered over 6500 orders for nearly €1m. 60 kilos of illicit drugs were seized by the Police.[60]

***

France, January 2007, a teenager asked in forum-hachich.com the recipe in order to manufacture methamphetamine and crystal drugs.[61]

***

UK - Three members of a drug dealing ring who used the internet to sell cannabis to addresses across the UK were sent to prison in April 2005.

The hi-tech dealers plied their illicit trade from a website known as budmonkey that was set up by Sean Jackson, a former heroin addict. Regular customers used the site to order their drugs online. The dealers - the UK's first online drug ring - then shipped the cannabis to their clients using hermetically-sealed bags to hide the smell of the drugs.

The scam was so successful that the gang was netting more than £500,000 a year and Jackson, its inventor, later sold the idea of his computer database as a franchise to other dealers.[62]

3.10 Organ traffic

Hospitals in Asia are openly advertising their organ transplant services on the Internet.[63] Sale of kidneys is a lucrative business. In some villages in Pakistan, most adults have sold one and transplant specialists estimate that between 4,000 to 5,000 kidneys are sold every year. Clients are international and coming from Jordan, Saudi

[59] Times of India, February 2007.
[60] ATS, December 2007.
[61] Laurence Ifrah, research for DRMCC (Department of Research for Contemporary Menaces), Paris University II, Pantheon-Assas.
[62] Pete Warren, TheRegister, May 2005.
[63] http://daledamos.blogspot.com/2007/12/chesed-announcement-kidney-needed.html

Arabia, the US or UK. Market places are operating on forums or newsgroups where young adults are trying to sell their organ for a few thousand dollars.

> *I AM VERY POOR AND I HAVE TO PAY BACK A HUGE AMOUNT (debt) THEREFORE I HAVE DECIDED TO SELL MY KIDNEY, I AM HEALTHY 22 YEARS MALE FROM PAKISTAN*
> *I WILL SELL KIDNEY JUST FOR US$ 5000/-*
> *PLEASE CONTACT ME FOR FURTHER DETAILS,*
>
> *KHURRAM KHAN*
> *LAHORE, PAKISTAN*
> *KHURRAM23FEB@YAHOO.COM*
>
> ---
>
> *I M 26 YR OLD GUY FROM INDIA I M IN GR88 FINANCIAL NEED SO WANA SELL MY KIDNEY FOR $50000 I M VERY FIT I M A SPORTS MAN DONT DRINK & DONT SMOKE & JUNK FOOD WAITING FOR REPLY RESPOND ME AT SANJU6778@HOTMAIL.COM*

4 Pornography, crime and games in the virtual world

4.1 Pornography and sexual violence

Pornography has played a significantly larger role in people's lives since the rise of the Internet. With the push of a button, explicit sexual images are accessible 24 hours a day for all eyes to see. Alarmingly, youth from 12 to 17 years old are the largest consumers of Internet pornography, exceeding the number of all adult viewers, according to HealthyMind.com.

Under new laws announced by UK Home Office Minister Vernon Coaker in August 2006, it will be illegal to possess pornographic images depicting scenes of extreme sexual violence. This would include, for example, material featuring violence that appears to be life threatening.

The proposals are part of the government's response to its consultation on the possession of violent and extreme pornographic material launched a year ago.

It is already illegal in the UK to publish or distribute the material covered by the ban, but violent pornography has become increasingly accessible from abroad via the Internet. The new law will ensure possession of violent and extreme pornography is illegal both on and offline.

> The bereaved mother whose two-year campaign inspired the forthcoming ban on viewing violent pornography said yesterday that the measure would be a memorial to her daughter. Liz Longhurst began her battle to change the law after her daughter Jane was killed in 2003 by a man said to be obsessed with violent internet pornography. More than 50,000 people signed a petition supporting her.
>
> "My daughter Sue and I are very pleased that after 30 months of intensive campaigning we have persuaded the government to take action against these horrific internet sites which can have such a corrupting influence and glorify extreme sexual violence," she said.[64]

[64] Tania Branigan, The Guardian, August 2006.

Legal pornographic websites are attacked by criminals for ID theft or financial fraud in using users' credentials to withdraw from their bank accounts; they are easy target as victims are too embarrassed to report the fraud. Illegal porn websites are infecting end-users with compromised pages which upload malicious codes on victim's computers.

4.2 Child pornography

More than seven websites showing child abuse are reported to the police every day, an online charity has said. The Internet Watch Foundation (IWF) also said new research showed the images, which included rape, sadism and bestiality, had become more severe.

It also said more than a third of all child sexual abuse sites contained images of the most severe kinds of abuse. Nearly one in three children appearing on the sites were under six years old, while one in 20 were under the age of two. The foundation said so far this year it had passed on details of 2,092 child sexual abuse websites to police and child protection agencies.[65]

> German prosecutors are investigating 12,000 suspected members of a child sex abuse network on the internet - the biggest in the country's history. A senior public prosecutor said the suspects were accused of downloading or possessing illegal images of children. The investigation, which has been going on for several months, also points to suspects in about 70 other countries.
>
> An internet provider in Berlin is said to have helped by alerting the inquiry to a huge amount of internet traffic. "The material was analysed. Then we called for search warrants", said Peter Vogt, head of the central office tackling child internet sex abuse. He was speaking to German radio station Mitteldeutscher Rundfunk (MDR). The suspects include 300 under investigation in the eastern German state of Sachsen-Anhalt.[66]
>
> ***
>
> A former NSW police officer is among 31 men arrested for child sex pornography offences in two Australia-wide police operations. The ex-policeman had been previously arrested in a 2004 pornography sting and had just completed a good behaviour bond, police said.
>
> Police are sifting through more than one million photographs and videos of child exploitation that were seized in the arrests.
>
> "The images that our officers view and that we seize are not images of children in sexual poses. These are images of children getting raped and abused and tortured", the acting national manager of high tech crime operations, Kevin Zuccato, said.
>
> He said the victims, ranging from infants to teenagers, were Caucasian and Asian in appearance and their nationalities were yet to be determined. The men arrested for downloading the images were aged between 30 and 70 and were from various sectors and no direct links have been found between them.
>
> He said a forensic psychologist, a television station worker, teachers, an RSPCA worker and a 70-year-old retiree were among the arrested. Some were known to police for child sex exploitation offences.[67]

[65] BBC News, October 2007.
[66] BBC News – December 2007
[67] Yuko Narushima, The Sydney Morning Herald, December 2007.

***

> Nine Canadians have been arrested as part of an ongoing international child abuse and internet child pornography investigation. The probe code-named "Operation Koala" involved videos of children being abused that were filmed mainly in a Ukraine studio and purchased by customers around the world.
>
> "They sought it out, they previewed the samples, they paid in advance and they waited for a password to download the videos", said McColl, head of the National Child Exploitation Co-ordination Centre, who was accompanied by representatives from other law enforcement agencies including Europe's Europol, the Ontario Provincial Police, the Vancouver Police and the Winnipeg Police Service. More than 92 people have been arrested in Europe as part of the investigation.[68]

4.3 Virtual world

Internet based virtual worlds are the latest fashionable online places where people meet. Second Life, launched in 2003 by Linden Research Inc (Linden Lab), became famous in 2006. A downloadable client program called the Second Life Viewer enables users to create a customisable avatar and interact with other characters. Residents can explore, meet other avatars, participate in different events and activities, create and trade virtual items or services. The virtual currency is the Linden Dollar and has to be acquired with real money.[69] By the end of 2007, 20 million accounts had been created but most of them were inactive, there are no reliable figures for actual long term usage.[70] Firms, embassies, political groups, NGOs, religious organisations have created places where they hold virtual meeting places. There is also a place for crime; paedophilia, gambling, narcotics, violence:

> An area called Wonderland in Second Life, was used by child abusers. A reporter from Sky News, Jason Farell, created his own character to carry out his investigation for months. He found out that online paedophiles are cruising on a virtual world to act out their sexual fantasies with young children. Farell said that Wonderland at first glance looks like a children's playground but in fact it is a place where child avatars from all ages (even toddlers) are offering sex. The reporter, after talking to one child, was offered a range of sordid and sick sexual acts including violent rapes and tortures.[71]

Virtual crimes have in fact real victims, avatars attracted to child pornography are then able to meet online and exchange real pictures of abused children.

Figure 9 – Virtual land for pedophiles Wonderland in Second Life[72]

[68] CBC News, January 2008.
[69] Currency by end of December 2007 was one $US for 276 Linden$.
[70] Wikipedia.
[71] Sky News, October 2007.
[72] http://news.sky.com

> RedLightCenter.com is a virtual world only focusing on sexual activities, since early 2007 they are offering their users virtual drugs like ecstasy or simulated hallucinogenic mushrooms. The owner of the website is convinced that users can enjoy both the social benefits of virtual drugs as well as the entertainment associated with their use without actual drug consumption.[73]

The sex industry is huge in virtual worlds because there is actually no police or law regulation which can control it. But there is more than that, Islamic militants are suspected of using Second Life to hunt for recruits and mimic real-life terrorism. Police and the intelligence services are concerned that it may have been infiltrated by extremists to proselytise, communicate and transfer money to one another. Kevin Zuccato, head of the Australian government's High Tech Crime Centre, said jihadists may also be using the virtual reality world to master skills such as reconnaissance and surveillance. "We need to start thinking about living, working and protecting two worlds and two realities", he told a security industry conference in Sydney.

Europol also believes that Second Life provides a means to transfer money across borders in a way that is more difficult for the authorities to monitor. Linden Lab said that about $1m a day was exchanged in Second Life. Europol and the British Serious Organised Crime Agency (Soca) are concerned that Second Life provides an ideal facility for criminals to launder money through in-world enterprises such as casinos. There are fears that terrorists could also take advantage of difficulties in policing Linden dollar movements to transfer funds between operatives around the world.

Mid-2007, an attack took place at the Australian Broadcasting Corporation's Second Life base. A number of these attacks, known as "griefings", have been launched by what industry insiders say are "geeky teenagers" giving themselves names such as the Second Life Liberation Army. Some experts, however, believe that the "virtual atrocities" may have been committed by real Islamic radicals. Rohan Gunaratna, a terrorism expert at the International Centre for Political Violence and Terrorism Research in Singapore, said that for the past three months he had monitored about 12 jihadists who have assumed identities in Second Life. He said they were mostly based in America and Europe. Some radicals had given themselves provocative jihadist names such as Irhabi007 (Arabic for "Terrorist007").[74]

Anonymous communication is easy to get in virtual worlds and numerous websites are selling different accessories to users in order to enhance their avatar; from skins to hair, clothes, houses, cars, jewels, anything is available. So are virtual phones, on slexchange.com, one of the popular marketplaces for selling HUD objects;[75] users are able to buy usual accessories, as above mentioned, and more specific ones like weapons, wheelchairs, Vietnam veteran look. Slexchange.com is offering cell phones to buy, which allow avatars to have telephone conversation over a private channel or open chat. Because avatars can only be traced by their IP which can easily be spoofed, it does not take much time to imagine the benefit this can bring to criminal or terrorist organisations. They can communicate without any risk of getting caught; this is more serious than virtual terror bombing, meetings to proselytise or recruit hunting. What's more, Linden Lab are going to release a new feature in early 2008 which will enable avatars to receive phone calls from the real world. "In the first quarter of 2008, users in Second Life will be able to get real-world phone numbers assigned to their avatars, and receive calls from real-world phones", said Joe Miller, vice president, platform & technology development for Linden Lab. "Users will be able to get voicemail, which can be e-mailed to the user or listened to when in-world."

[73] Technology Review, April 2007.
[74] Chris Gourlay and Abul Taher, The Sunday Times, August 2007.
[75] HUD objects are designed items which are attached to the screen instead of being attached to the avatar.

Figure 10 – Disable Vet Veteran avatar and cell phone for Second Life virtual world

This situation is offering criminals the possibility to organise their real life crimes over the phone from any part of the world; all they need is an Internet connection.

Spy tools can be found in any website selling virtual items. They allow a victim to be targeted and give the user all the information about the avatar he is spying on. He will get all the public chat around the target; his exact position every five minutes; who the victim is seeing and what they are talking about, in a totally undetectable way.

4.4 Online games – MMORPGs (Massively multiplayer online role-playing game

MMORPGs are extremely popular throughout the world. In 2006, 15 million players spent hours online bringing a revenue of over one billion $US, just on the Western side of the world. Users assume the role of a virtual character (mainly in a fantasy world) which commits actions with other online partners. The interesting point is that characters continue to exist and evolve while the player is not at his computer.[76] During the game, users have to achieve actions so they can get to a higher level and it can takes months or years to obtain the accumulation of wealth and combat-useful items necessary. Criminals have created an easy way for making money while playing.

- Use of bots in order to assist players in accumulating wealth to the disadvantage of other players;
- Use of auction sites to sell stolen 34rojan34d characters;
- Execution of malware codes for password and account stealing;
- Extortion;
- Threats (online and physical).

Online gamers are becoming a major target for cyber criminals as they know that players are so passionate they would be inclined to pay ransom to get their character back or even buy stolen virtual items to level it. Auction websites such as Ebay are the market place to find those virtual items for an average price of 200 euros. In the UK Ebay has stopped this kind of auctioning due to the legal complexity of virtual goods, but this decision is only local and items can be found in any other country; the French Ebay for example is still selling levelled characters. Everyday new 34rojan password-

[76] Wikipedia.

stealers appear, each of them is designed for a specific game. Virtual theft is real because the furniture is paid for with real money.

> Habbo Hotel is a virtual community where six million teenagers from 30 countries play each month. In November 2007, a 17-years-old was accused of stealing 4,000 euros worth of virtual furniture bought with real money by players. With five friends, the teenager has lured his victim into handling over their Habbo passwords by creating fake Habbo websites. There is actually an increasing of fake online game websites to get players credentials.

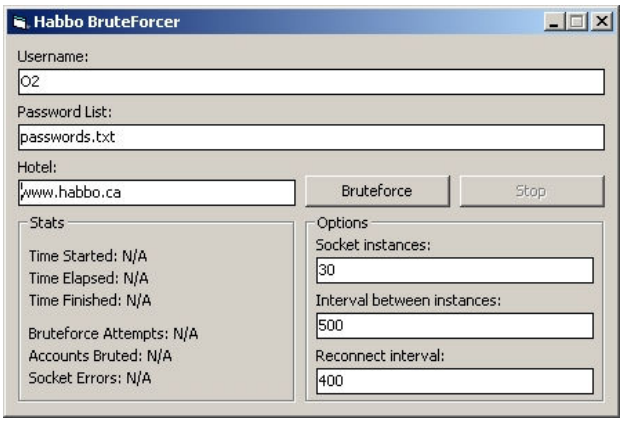


Figure 11 – Hack tool for Habbo Hotel online game

> A Chinese gamer was stabbed to death in a row over a sword game in 2005. Shangai gamer Qiu Chengwei killed player Zhu Caoyuan when he discovered he had sold a "Dragon Sabre" he had been loaned.[77]

> In September 2006, Word of Warcraft players were locked out of the game. A malware designed to steal user names and passwords has been planted on maliciously constructed websites pretending to be a resource for gaming advice.[78]

More than 40% of all online game Trojans are created in China and 90% of the passwords stolen by these malware belong to players on South Korean sites. More than 40% of all Trojan target Lineage 2 and 20% are written for Word of Warcraft, both are the most popular games.

4.5 Social Networks

The incredible success of social networks has attracted millions of people from all over the world. Facebook has amassed an audience of 33 million web users since its creation in 2004. This social hub has become the place to see and be seen. Lots of companies have created their own private space in Facebook for their employees to extend their professional network, exchange ideas, or get advices from colleagues. 150,000 new users are joining Facebook each day. Whilst Web 2.0 and social networking technologies hold potential for increased collaboration for companies and lead to exponential productivity gains, they also represent a target for malware enabling security risk for office networks. In November 2007, security vendor McAfee identified them as one of the top 10 security threats for 2008.[79] 48% of social networking users are connecting to these websites at work, almost 24% log in every day with half of them several times a day. Up to 45% log in at least once a week. A Sophos online survey on 500 respondents in September and October 2007 revealed that more than one fifth of these Facebook

[77] BBC News.
[78] John Leyden, TheRegister, September 2006.
[79] Linn Tan, ZDNet Asia, November 2007.

users are actually abusers. It is estimated that in UK alone, 233 million hours are lost every month.[80]

The most popular social network websites are:

- MySpace
- YouTube
- Facebook
- LinkedIn
- Friends Reunited
- Bebo

Having a page on a social network website offers the advantage to find friends and family with whom one had lost track of for years. People are getting so enthusiastic that they are spending an inordinate amount of time on them. As they get more and more visiting friends, users are giving personal information out to anybody, publishing their employment history and mobile numbers, forgetting that anyone can access their page.

Security firm Sophos has made a study about irresponsible behaviour in social network websites and found out that 72% of respondents publicised one or more e-mail address and 84% divulged their full date of birth. Sophos researchers created a profile on Facebook and tested 200 users randomly selected from across the world. When contacted, 41% unveiled personal information while 78% published their current address or location. At the end, Sophos managed to get 82 users out of 200 to hand over their personal details on a place. This information gathering was sufficient to create phishing e-mail or malware that specifically target individual users or businesses. Criminals can use data to spoof identities and gain access to the online user or infiltrate their employer's network.

Key findings from the Sophos study[81]:

- 87 of the 200 Facebook users responded to "friend requests" from Sophos' fake profile
- 72% revealed their e-mail address
- 84% published their full date of birth
- 87% provide details about education and work places
- 78% unveiled their current address or location
- 23% listed their current phone number
- 26% gave their IM screen name

> In October 2007, British troops were asked not to post personal details on web sites because of the elevated risk of being targeted by al-Qaeda terrorists. The security service, MI5 has released a note warning soldiers that the terrorist organization was increasingly using the Internet to track down potential targets (early 2007 they uncovered an alleged plot to kidnap a British Muslim soldier recently returned from abroad and behead him on the Internet). Army users connecting to Facebook, MySpace and Friends Reunited may potentially be at most risk. The Sunday Telegraph found at least 888 names on the Royal Marine network on Facebook and 72 members from the Royal Anglian Regiment. Thousands of servicemen and women have already published their full names, dates of birth, home towns, names of family members, partners and location where they had served including pictures posing with colleagues and weapons.[82]

[80] Sophos News, October 2007.
[81] Sophos for ZDNet Asia.
[82] http://www.telegraph.co.uk

The main problem is that it is not possible to delete an account on Facebook; it can be deactivated but the profile will always remain on its server. After investigation from UK data protection watchdogs, Facebook stated that its terms and conditions are clearly mentioning that subscribers are giving up any rights to anything posted on their website. There is therefore a real concern about the security of personal details if Facebook servers were hacked.

> Fortinet researchers have discovered the first of January 2008 a new malicious widget hosted through a popular Facebooks' feature "Secret Crush" which invites users to find out who from their friends could be a real admirer. Before being able to know the answer, users were asked to recommend five of their friends, a good combination of social engineering and spyware techniques. As soon as they clicked, users downloaded the worm and were forced to view unsolicited advertisements from the Zango adware web site. Over 3 percent of Facebook accounts were affected by the widget.[83]
>
> ***
>
> In November 2007, the MySpace page of pop singer Alicia Keys appeared to be compromised with an image of 8,000 pixels by 1,000 pixels, like a blank image overlapping the page. If a user clicked on it, he would be redirected to a server based in China, which would attempt to perform exploits into his computer system.[84]
>
> ***
>
> In January 2008, criminals spoofed a Microsoft Update window in which they inserted malicious code. The update was appearing on top of a profile (named Rita) page on MySpace website. If any user clicked and accepted to download the update, he would get a whole bunch of malwares installed such as downloader, Trojan and backdoors related to multiple servers in Malaysia and Ukraine.

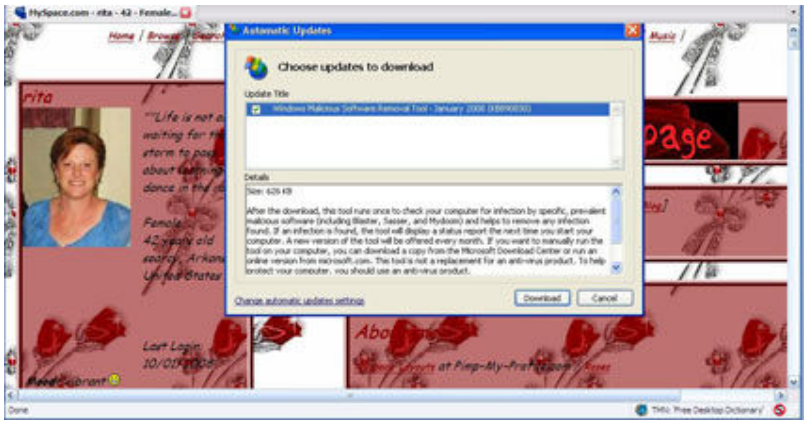


Figure 12 – Microsoft spoofed Automatic Update window over a MySpace user profile

As for launching a targeted attack, social networks are the best source of information one can find. For example, imagine a hacker wants to get inside a company's network; he will need to find enough information on the Internet to prepare a malware which won't be detected by the firm's protection's system. Then the easiest way to get the malicious program inside will be to send an e-mail to an executive who has higher access into the information system. Thanks to Facebook, hackers will get the complete profile of a potential victim, his career, his friends, his family, and the best part will be

[83] Stefanie Hoffman, CMP Channel, January 2008.
[84] Roger Thompson, Researcher at Exploit Prevention Labs, November 2007.

that he will get to see who from his contact is sending him videos or funny images or who is the closest friend or family member. The last step will be for the hacker to spoof the contact's ID and send the target an e-mail with a compromised attachment.

4.6 YouTube – DailyMotion

Threats, bullying, An end to privacy: cell phones are used to record violent or intimate scenes of people unaware that they will soon be online seen by millions of surfers. Online video sites have a great influence towards surfers, therefore people can use this media to attempt to damage someone's reputation. In England, students are publishing video clips where they show teachers being verbally and physically, as a warning against authority. Violence, beatings, beheadings, rapes, murders, cruelty in any kind of ways, everything is published online.

> In December 2007, a video showing a French swimmer naked was posted on Internet, privacy is no longer guaranteed today, once on Internet data are lost forever. One month after the first release of this video, around 2 million websites were mentioning the event, showing pictures or publishing a copy of the clip. Fake videos were also created and published with humiliating images for the victim.
>
> In France a 6 min video clip was posted on YouTube in January 2007, showing a gang of hundred youngster driving cars with guns. This cyber-bullying was a message to the opposite gang in Paris' suburbs.

5 Groups of offenders

5.1 Criminal organisations

For years hackers were known to be precocious teenagers who spent hours on their computers committing digital offences, such as defacing websites; today, they are hardly noticeable, as they have been replaced by talented computer programmers using their skill to make money by stealing instead of working. Computer crime has turned into huge business and is highly organised by gangs to steal millions of dollars from their fraudulent but very profitable activities. Most of them are located in Eastern Europe (Ukraine), Brazil, Russia and Asia (South Korea, China, India). They recruit from universities or IT schools, offering the best students wages they cannot refuse. Those IT geniuses are many, but they are surrounded by groups of young hackers hanging around, hoping to be part of the 'Elite' and ready to perform any small task, like cracking passwords to supplement their meagre incomes. To cover their crimes, gangs have taken root in countries that do not have the technical response, laws and investigate support to respond to the threat.

In Brazil, criminal gangs operate on a large scale, sharing the underground market between them. In a 2005 case, over 50 Brazilians were arrested for using a Trojan horse allowing them to steal online-banking passwords. They stole $33 million out of this targeted attack. Later another ring of 100 criminals was found; they had gained access to 10,000 Brazilian bank accounts.

Organised gangs are recruiting the next generation of Internet criminals by approaching undergraduates on university campuses. They even go as far as financing their studies and use them as moles inside businesses they have targeted.

5.2 Terrorist organisations

A Saudi researcher announced in December 2007 at a security conference that there are about 5,600 websites promoting al-Qaeda's ideology worldwide, and 900 more are appearing each year. Extremist websites are constantly on the rise and are difficult to track as they often change addresses to avoid detection or start up again elsewhere once infiltrated.

Terrorists are developing marketing and communication like never before; they now use Al-Sahab, the group's media arm on an Islamic militant website which shows the latest in al-Qaida's increasingly sophisticated efforts to get out its message. Al-Sahab has dramatically increased the number of messages it has issued this year, and its videos have shown more complex production. Al-Sahab has issued more than 90 videos in 2007, more than the total number for all three previous years, according to IntelCenter, a U.S. counter-terrorism centre that monitors militant message trafficking. They are always subtitled in English, and messages this year from bin Laden and al-Zawahri focusing on Pakistan and Afghanistan have been dubbed into the local languages, Urdu and Pashtun.

In December 2007, Al-Qaida invited journalists to send questions to its No. 2 figure, Ayman al-Zawahri, the first time the terror network has offered an "interview" with one of its top leaders since the 11 September 2001 attacks in the United States.

Al-Zawahri invited individuals, agencies and all media to submit written questions by sending them to the Islamic Web forums where Al-Sahab traditionally posts its messages.

The cyber jihadist community is sharing hacking tools and tutorials to launch attacks against Western countries.

Figure 13 – Islamist hackers website

> Until late 2005, the Internet hacker who called himself "Irhabi 007" - "irhabi" is Arabic for "terrorist" - was a key enabler of Abu Musab Zarqawi's Internet recruiting and propaganda efforts outside Iraq. He is now in custody in the United Kingdom. It turns out "Irhabi" is a 22-year-old West Londoner fluent in Arabic and English whose rather unremarkable combination of Islamist sympathies and technological aptitude ended up making him indispensable to the world's most dangerous terror network.
>
> The story of how and why he was apprehended, just now trickling out thanks to researchers at the Washington-based SITE Institute, suggests a mix of technological savvy and old-fashioned gumshoeing to fight the Internet jihad.

"Irhabi 007" made his mark in al Qaeda message forums helping insurgents and propagandists spread videos and multimedia, tighten Internet security and hack websites.

But his role as teacher and Web expert was extolled by his cohorts; he offered a "Seminar on Hacking Websites" and is said to have demonstrated it on sites run by the state of Arkansas and George Washington University. "You are one of the top people who care about serving your brothers," one admirer wrote on a message forum. "Carry on serving jihad and its supporters."[85]

Terrorists who for years have used the Internet and its various tools to organise and communicate are paying more attention to addressing security and privacy concerns similar to those of other web users. They have posted the following guide to advise readers about the risk of Internet surveillance.

Security Advice to Forum Attendees

In the name of God, the Merciful, the Compassionate.

It is well-known that the discussion forums on the Internet have become of an eminent importance and influence in the media, and through which renowned newspapers and satellite channels extract and follow the news of the mujahideen. The mujahideen have positively profited from the Internet as well and from the forums specifically because they helped eliminate the blackout and the Zionist-Christian media restrictions that contained the jihadist movement for many years.

A wide variety of intelligence agencies understand the danger of the use of the Internet by the mujahideen. They also understand the considerable opportunity offered by the discussion forums which allow them to capture as many 'terrorists' as they can, and those who oppose one regime or another. So they anxiously set out to infiltrate those forums by:

Inserting their members into the forums so they can catch whoever they can catch; and pressuring the owners of the forum so they work with them.

CNN has reported that an American intelligence agency has announced that it has plans to open an Arabic discussion forum to capture terrorists.

Based on what we mentioned above, it is the duty of every person who visits the forums, either the mujahideen who are responsible for posting the statements, communiques, and publications, their supporters, or even the people who follow the mujahideen's news through the forums to be very cautious because the mere fact of entering or visiting such forums is a criminal act to be punished by the apostate regimes in our Islamic world.

We say it has become necessary to observe a few preventive procedures and take precautions when dealing with the forums. Dear reader, here are a few things to which you pay attention to when you participate in forums, whether they are forums that follow a jihadist point of view or just forums you visit to share your opinion on specific topics.

First, remember that the people with whom you discuss issues in the forums are not always what they seem to be. You might meet a young man who is yearning for jihad, asking other forum users about the ways that would lead him to the lands of jihad, but really he may be a secret agent writing from an intelligence agency' s building!

As for that writer who is always writing those radical articles that defend the mujahideen and their honour, he might be the same, an agent trying to lure forum users until they trust him

[85] http://jimstroud.com April 2006

and then he would ask them to get acquainted in order to help each other spread the 'call for jihad' and finally get them arrested.

What is important is to always remember that it is easy to pass for somebody else while on the Internet, so you should not trust anyone in the forums. Yes some people are true and thank God there are many of them, but unfortunately it is hard to distinguish the good from the bad, so it suffices to only take what might benefit you from the forums and remember that 'everything that shines is not gold.'

Second, it is a fact that just registering or visiting a forum would allow the forum's owner to trace your 'IP' address and in many cases locate with a great accuracy the computer you are using when visiting the forum. Thus it has become very easy to establish your location after they find out your Internet address. In fact, there are many sites on the Internet that offer this service free of charge.

Yes the forum's owner can disable the Internet registration feature, therefore when joining a forum and posting materials, the IP address won't be registered, and that is what we advise our brothers who run and own forums to do. But it is possible to obtain an IP address through the e-mail address that is being used when joining a forum. Of course the servers won't object to supplying security agencies with your IP address since it is part of the 'fight against terror.' The same applies when using the proxy.

The best thing to do when dealing with this problem if you are responsible for posting news and statements or if you are wanted by the apostate intelligence agencies is to use 'internet cafes.' There are other safer ways but we cannot mention them or we will attract the enemy's attention to them. 'Necessity is the mother of invention'!

We have to mention that many Internet cafes are being used to spy on their customers, especially those customers with an Islamic appearance, so attention needs to be given to this particular point.

Advice and Warnings

The Internet address is registered every time you put up a post and not only when you become a member. This means that even if you register in an Internet cafe and then you put up a post from your home computer, your IP address is registered.

Finding out your personal IP address is not necessarily done through the forum's administration; it is easily done through the server that hosts the forum, and the server also acquires all the information regarding the participants.

Most Internet sites are equipped with statistics programs that register every move made by a visitor along with his personal IP address.

Third, when becoming a member in any forum, you are requested to provide personal and general information like your name, your country, and your date of birth. Do not enter any accurate personal information; instead give false information. If a forum moderator or somebody else emails you to get personal information from you to confirm the validity of an account, do not supply them with your personal information.

Fourth, if you are a participant in a forum and join discussions from an Internet cafe, you should use different Internet cafes and preferably the ones that are the furthest from your house.

The person responsible for publishing news should not spend more time than needed to finish his work, for the Internet cafes are the easiest to get to since the apostate security systems know the personal IP address of each one of them.

After each session, erase all temporary Internet files the dates and history and the 'cookies' and then close the browser to end all sessions. If you do not do this the the next person who uses the same computer will be able to enter the forum through your account. Do not forget to restart the computer before you leave.

Remark: in many instances, after erasing all the information, it will all come back when you open the browser; in this case you have to manually erase all entries.

Fifth, be careful of the files in the forums because some might contain spying files that would enable the person who is disseminating them to spy on your computer and know all the contents of your hard disk.

Sixth, if you are asked to install any program while browsing the forum, do not accept whatever the reason might be. There are programs that would enable the other side (intelligence agencies) to spy on your computer like certain Java mini-applications or 'Java applets.' As a matter of a fact, one of the intelligence agencies has set up an alleged jihadist forum, and after people started visiting the forum, they were requested to install little programs and other applications on their computer with the pretext that it would allow them to browse the forum. After a short while, personal pictures of people with their complete names and addresses were released after they were stolen from their personal computers.

It is important to point to a very important idea when dealing with computers: never enter or keep correct personal information in the computer like names, countries, etc. whether during an installation or otherwise.

Seventh, if you are asked to give your e-mail address in order to receive mail, refrain from doing so. Instead ask to be sent mail to your forum's e-mail account if provided.

Eighth, when registering in more than one forum, do not use the same password. If one forum is infiltrated, your membership in other forums will still be kept secret. We strongly advise that you avoid using the same name in registering in more than one forum so your movements are not tagged along on the Internet. If you would like to publish the same material in more than one forum, tail it with words like 'copied from such and such forum' or other words that do not implicate you as being an originator of a publication but only a forwarder.

Ninth, do not give any specific information about yourself that would disclose your identity, not even the town in which you live. Do not give specific names of places or say you were at a certain place at a certain time or that you attended a sermon of such and such shaykh or things like that.

Tenth, if you would like to get acquainted with people and make friends, consider that the jihadist forums are not the right place for you.

These are a few things that we wanted to bring to the attention of the people that visit the discussion forums on the Internet. 'But Allah is the best to take care (of him), and He is the Most Merciful of those who show mercy' (Yusuf 12:64).

Terrorists are using the Internet to focus on children and attract young people to the ideology, and then later to the way of terrorism. They promote their ideology with comic books, fan fiction, graphics, videos and contests. There are also websites for women that show pink manuals explaining the why’s and how’s of female suicide bombing. Islamists are mainly producing websites that show pictures of war, dead babies, killed

soldiers, torture, bombing; first they publish pictures of their own people wounded, arrested or dead, then they demonstrate how the strength of fate is giving them the power to defeat the enemy with other pictures of mostly American soldiers caught in a trap and killed.

> Technically, terrorists are heading towards more security regarding their communication, therefore the USB keys that include a program's portability as an application (not requiring installation on a personal computer) will become an increasingly desirable feature, especially considering the high use of Internet cafés.[86] "Mujahedin Secrets", which can be downloaded for free, offers "the five best encryption algorithms, with symmetrical encryption keys (256 bit), asymmetrical encryption keys (2048 bit) and data compression", according to a translation of a Global Islamic Media Front's announcement about the software on January 2007, provided by Middle East Media Research Institute.[87]

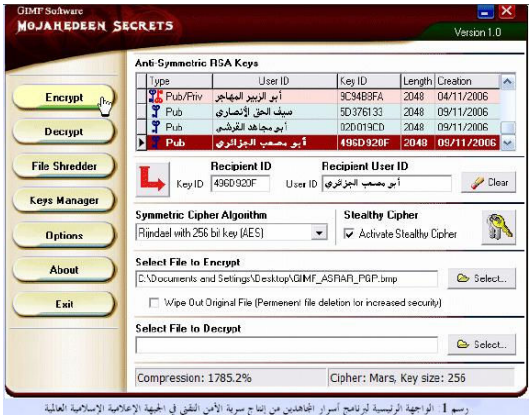


Figure 14 – Mujahedeen secrets encryption tool

DdoS evolution appears in cyberterror

As DdoS enters more mainstream audiences, new motivations for DdoS will appear. According to the security firm Prolexic, the massive increase in activity from Middle-Eastern countries suggests that the 2007/2008 timeframe will hold a large increase in cyber-terrorism.

Hactivism

Groups with political motivations have entered the crime scene too. They perform website defacement and virtual sit-ins, but are also very active in virtual worlds like SecondLife, where they demonstrate against nuclear power, by showing the potential impact created by explosion of irradiated containers. Finally they hack government and large petroleum, chemical or nuclear international firms, in order to insert their political messages on web pages. Hactivists are publishing messages on blogs, websites, forums and newsgroups that include almost unbearable images or video clips of people wounded after being contaminated by chemicals, malformed-born babies, animals killed for the fur industry. Video clips relayed on YouTube on the animal section violently hurt end-users, especially younger ones.

[86] iDefense Middle East analyst Andretta Summerville.
[87] Dancho Danchez, February 2007.

5.3 Espionage

There is a growing threat of electronic espionage from agents acting for foreign governments. Security experts are warning about hackers' gangs targeting sensitive government systems in order to gain access to classified information and transfer it to their country. NATO analysts believe that this kind of attacks may have been directed by competing nation-state governments. A cyber cold war waged over the world's computers threatens to become one of the biggest threats to security in the next decade. About 120 countries are developing ways to use the Internet as a weapon to target financial markets, government computer systems and utilities, Internet security company McAfee said in an annual report. Intelligence agencies already routinely test other states' networks looking for weaknesses and their techniques are growing more sophisticated every year, it said. Governments must urgently shore up their defenses against industrial espionage and attacks on infrastructure.[88]

In December 2007, the head of MI5, Jonathan Evans, warned that a "number of countries continue to devote significant time and energy" to stealing sensitive government information using increasingly sophisticated technical methods. MI5 has had to divert "significant amounts of equipment, money and staff" from major counter-terrorism operations in order to defend against these Internet-based attacks, a predicament Evans described as disappointing. He mentioned that Russia and China increasingly use Internet-enabled intrusion techniques "to penetrate computer networks". The startling scale and ambition of the Chinese military's cyber strategy was unveiled in September, when the Times newspaper obtained a Pentagon report outlining China's alleged 'blueprint' for cyberwar.

The revelation followed a series of recent incidents in which the Chinese government has been accused of sponsoring military-led cyber assaults against Western government networks, including Germany, UK, France, Australia and New Zealand. As today, the Chinese government firmly denies being involved in these attacks.

All the governments received the same attack. A Trojan horse was embedded in a Microsoft Word or a PowerPoint file to addressees selected by the attackers. The offending servers receiving the stolen information were mainly located in the provinces of Lanzhou and Beijing in China.

"The Chinese were first to use cyber-attacks for political and military goals", James Mulvenon, director of the Center for Intelligence and Research in Washington, was quoted as saying in the McAfee's report. According to Johannes Ullrich, a SANS Technology Institute expert, everybody is hacking everybody, recalling Israeli hacks against the United State and the French against European Union Partners.

Corporate espionage costs the world's 1,000 largest companies in excess of $45bn (£22.8bn) every year, according to research from consulting firm PricewaterhouseCoopers. Because information is stored on servers, it becomes easier to reach and some unscrupulous companies hire hackers' services to get it from competitors. PricewaterhouseCoopers, for example, reported that losses from corporate espionage doubled between 1990 and 2000. The theft of commercial and financial information, secret formulations of products, or a new marketing campaign is highly valuable for competitors.

Michael and Ruth Haephrati, an Israeli couple, had developed and sold customised spyware or Trojan horse packages designed to evade detection by security tools to three private investigation companies in Israel - Modi'in Ezrahi, Zvi Krochmal, and

[88] McAfee, Criminology report 2007.

Philosof-Balali, The Jerusalem Post reports. This spyware code was allegedly installed on victims' PCs by private detectives from a diskette or via e-mail, as part of a spying scam that ran for up to two years. The malware sent stolen documents to an FTP site, allowing unscrupulous firms to swipe confidential documents from rivals. Each software installation allegedly netted the Haephratis £2,000.

> Firms suspected of using the malware include Mayer Motors (an importer of Volvo and Honda cars) against Champion Motors (an Audi and Volkswagen dealership), satellite television company Yes is accused of spying on rival cable TV outfit HOT, while Israeli mobile phone firms Pelephone and Cellcom are accused of spying Haaretz reports.[89]
>
> ***
>
> Hackers are not using only direct attack to acquire information. According to a source close to the situation, the chief information security officer of the US Department of Commerce learned in summer 2006 that his home computer was being used to send data to computers in China. He found his family had been the victim of a spear-phishing attack, in which his child had been encouraged by an e-mail to unwittingly download malware onto the family's home computer. Once it was compromised, the attackers used the security officer's personal computer as a tunnel into the Department of Commerce's systems.[90]

5.4 Insider threats

Unauthorised access to information resources by trusted insiders poses an even greater threat to corporate and government security than external attacks, as insiders have legitimate reasons to access sensitive data. Despite the continuous growth of malware and other threats, more than 80% of unauthorised access to data is committed by an organisation's own employees. Most of the time, they have already showed signs of concerning behaviour such as tardiness, truancy, arguing with colleagues, and poor job performance. Insider activity might involve such incidents as manipulating, exceeding authorised access to, tampering with and even disabling company's information resources, workstation, or network.

Consequences include financial losses, negative publicity, and clients' loss; they can severely damage the organisation's critical assets by deleting data, destroying the information system or compromising the back up. They can even lead a company to lay off employees or close down. Many organisations underestimate the risk of potential insider threats, mostly focusing on protecting their information system from external attacks.

> "By default you trust insiders", said Ron Ben-Natan, chief technology officer of Waltham, Mass.-based data security firm Guardium, Inc. "The challenge is always in how you balance the trust you give them with the right amount of security so a few bad apples can't get away with this sort of thing."
>
> Gary Min, also known as Yonggang Min, is a former senior chemist for DuPont who faces up to a decade in prison and a $250,000 fine after pleading guilty to stealing trade secrets in November. The case was unsealed by federal prosecutors in Wilmington, Del., Thursday. Min, 43, was accused of stealing approximately $400 million worth of information from DuPont and attempting to leak it to a third party. He is scheduled to be sentenced March 29.

[89] John Leyden, The Register, January 2006.
[90] ZdNet, November 2007.

> According to local news reports, a naturalized U.S. citizen from China surrendered his passport and is cooperating with federal authorities. Min's attorney, Michael Mustokoff, said his client accepts responsibility for what he did.
>
> Investigators say Min joined DuPont in 1995 but began exploring a new job opportunity in Asia in 2005 with Victrex PLC, a DuPont competitor. Shortly after opening the dialog with Victrex, Min reportedly proceeded to download approximately 22,000 abstracts from DuPont's data library and accessed about 16,700 documents. After Min gave his notice, DuPont discovered what he was up to and brought in the FBI.[91]

A considerable amount of insider abuse is performed offsite via remote access. They are less likely to be caught stealing sensitive information when they can do it offsite. Also, inadequately protected remote computers may turn up in the hands of a third-party if the computer is left unattended, lost or stolen.

Perhaps the most unintentional insider threat is that of unsecure wireless network usage. Whether it's at a coffee shop, airport or hotel, unsecured airwaves can easily put sensitive information in jeopardy.

According to a study from the CERT and the US Secret Service, revenge is the main motive of insiders due to disputes with other employees. The most frequently reported goals of attacks are financial gain, theft of information/property and sabotage to the organisation's data, systems, networks, business operations or reputations.

The study reported some keys information that could help preventing potential damages:

- The majority of insiders planned their activities in advance;
- The majority of insiders came to the attention of someone in the workplace for problematic or unusual behaviour prior to the incident;
- Others had information about the insider's intentions, plans and/or ongoing activities.[92]

> In December 2006 a former system administrator at UBS Paine Webber was sentenced to 97 months for launching a logic bomb attack on the company's network causing $3m damage early 2002. Roger Duronio had been working two years at the bank for $125,000 salary; he expected a bonus of $50,000 but he only got $32,000. Enraged, the man resigned and took revenge, so he planted the logic bomb with the goal of deleting all the files in the host server in the central data server and then every server in branch.[93]

Behaviours and information known by other individuals prior to the attack have proved to be highly suspicious. Insiders told co-workers, friends or family members about their project to perpetrate illicit activities against the company and/or they showed or told them how easy it could be done. What should really be taken as a sign is when insiders are leaving the office later than usual, or when they are frequently observed in unusual places or areas.

[91] SearchSecurity, February 2007.
[92] CERT.
[93] US Department of Justice, December 2006.

5.5 Laptop theft

It is clear that private companies suffer from twice as many data leaks, cases of sabotage and other breaches than government structures. There are several reasons. First, the number of private companies greatly exceeds the number of government organisations. Second, it is easier for government organisations to conceal a leak when one occurs. It often happens that the controlling body is responsible for a breach of internal information system. Thus, there is the problem of lack of control over the controller. Meanwhile, some cases of information theft from government structures become public. This happens when it is simply impossible to hide the incident, or when it becomes necessary to make a public example of the offender. For instance, for many years the US government kept quiet about breaches of internal IS. But today, news about information leaks and gaps in security systems is commonplace. One of the latest cases reached the news when the US Tax Inspectorate announced in November 2006 that almost 500 laptops had been stolen over the preceding four years.

Millions of people run the risk of ID fraud each year by data leakage due to stolen laptops from corporate or organisation's employees.

Commercial organisations do not just experience a lot of data leaks, but also suffer from the huge losses they cause. The company's reputation and brand image are significantly damaged by such leaks. The effect of laptop loss and theft on a business is potentially devastating.

Organisational Information – internal information about a company may be stored on an employee's laptop, for example, passwords, banking or financial information or confidential employee data.

Customer Information – loss of confidential customer data such as account details, telephone numbers and e-mail addresses could cause corporate embarrassment, loss of business and legal penalties.

Personal Information – bank information, Internet shopping accounts and credit cards create a loss of productivity and time at work while the situation is resolved.

Remote Access – an intruder could potentially gain widespread access to a company's central network through a stolen laptop, including accounts and financial data, confidential personal files and customer details, causing untold amounts of damage.

Amazingly, firms are not taking the proper actions to protect their data. According to William Malik, vice president and information-security research director for market researcher Gartner Group, informal surveys indicate that about 10% to 15% of those laptops are stolen by criminals' intent on selling the data.[94]

> On May 3, 2006 criminals stole a hard drive from the house of an employee of the US Department of Veteran Affairs. As a result, personal details of 26.5 million veterans and 2.2 million active-duty servicemen fell into the hands of fraudsters.
>
> The biggest leak in Great Britain happened in August 2006. Burglars got into the house of an employee of the Nationwide Building Society and stole a laptop with the company's clients' personal information in unencrypted form. 11 million people face the risk of ID theft as a result. Nationwide notified the police at once, but the investigation was fruitless. Three months later the company started sending notifications to the victims.[95]

[94] Sec-1.
[95] www.infowatch.com February 2007 – Global Data Leakage Survey 2006

6 New types of threats

6.1 Cell phones

Mobile phone crimes have become a widespread problem; viruses, worms, Trojan programs started to appear in Japan and Europe by the end of 2004. Denial of service attacks, infection of devices via an ActiveSync connection to Windows PCs, application that offers free texts, but is in fact charging user around $5 per message – new malware are released every day. Wireless and Bluetooth connections make this easier to operate. But hackers are now looking to programs that target companies' executives to launch larger attacks on corporate networks with the intent of accessing business-critical information.

The increasing processing power and growing features available on mobile phones make the devices one of the best tools for spying on someone. Some websites are offering spying services to end-users. For a price starting at $20 per month, mobile spy software allows anyone to get full access to their target. The user is asked to enter the IMEI of the target phone and a number of his personal mobile. After subscribing and paying his fee, the user will receive software which has to be executed on the victim's phone. He will then have access to the following features:

- GSM localisation sent by sms;
- SMS-MMS copies of any sent or received message;
- Sound Recorder that will transfer any phone or "in the air" conversation;
- Interception allowing user to listen to ongoing conversation in real time;
- Copy of the target's address book.

Untraceable GSM Phone is available online and gives users guarantee that nobody can intercept their conversation. The IMEI number is unique to each device, by changing it randomly with each new SIM card inserted, interception becomes impossible to perform. IMEI changer applications are available on the Internet with tutorial explaining how to clone SIM cards.

370 mobile phone viruses have been created so far; Cabir and Commwarrior are still in the wild since 2004 and are reported in more than 30 countries. The future threats are rootkits and mobile botnets.[96]

> Spanish police arrested in June 2007 a 28-year-old man on suspicion of creating and spreading a virus that affected more than 115,000 mobile phones. The virus struck Bluetooth enabled phones that run on Symbian operating system was presented as messages claiming to contain erotic images, sports information or virus protection software. It caused millions of Euros in damages to the phone owners and the service providers.[97]

[96] F-Secure.
[97] AFP, June 2007.

6.2 Digital devices

Removable media devices are now seen as the biggest security threat to corporate security, and yet 80% of firms do not have safeguards in place. Centennial's annual Security Attitudes Survey 2007, which surveyed more than 370 mid and senior level IT managers attending the Infosecurity Europe expo in London, indicates that 38.4% of respondents rank removable media devices such as USB memory sticks and MP3 Players, as the number one security issue facing their organisation. Most information leaks (50%) are perpetrated via mobile devices (laptops, PDAs, USB flash, CD, DVD, etc.). Whereas the small size of mobile devices makes them convenient, they can easily be lost or stolen. In the case of accidental loss of media, the confidential information ends up in the hands of a stranger to be used at the finder's discretion.[98]

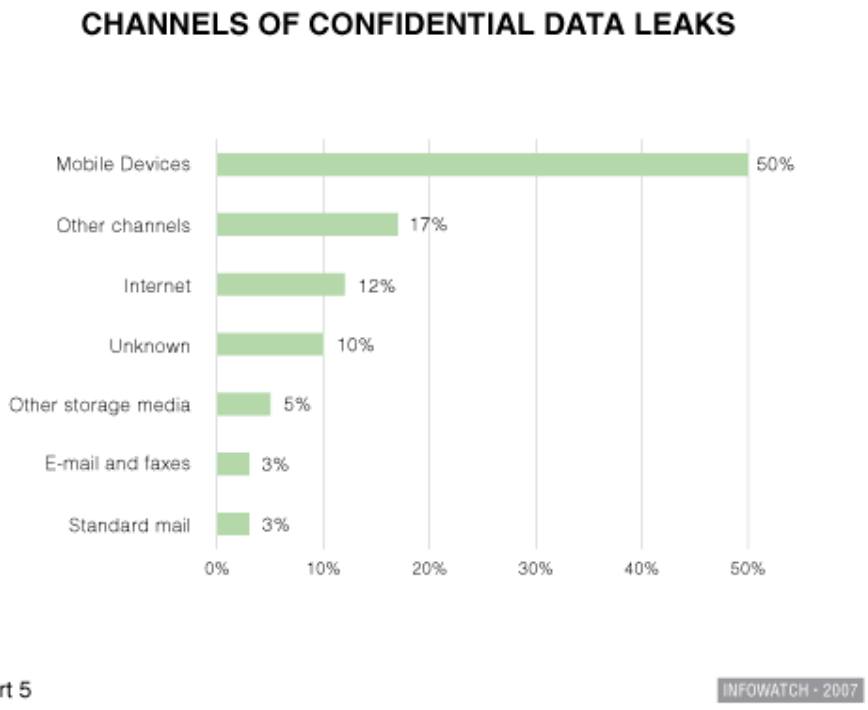


Chart 5

Despite a raft of recent media stories surrounding insider data theft using removable media, 43% of those questioned have no controls whatsoever in place to manage removable media devices, while 27.4% leave it to individual manager's discretion. Just 8.6% of respondents have taken the drastic step of introducing a company-wide ban on the use of removable media devices.

A similar study carried out by business advisory firm Deloitte last July which indicated a 50% rise in security breaches, found that almost half of all incidents originated internally, which the firm said was unsurprising given the increased popularity of portable media devices.[99]

> A USB memory stick containing classified NATO information was found in January 2008 in a library in Stockholm.
>
> According to Swedish daily Aftonbladet, the stick contained material on NATO's ISAF peace-keeping force in Afghanistan, as well as an intelligence report on the attempted assassination of

[98] InfoWatch.
[99] http://www.enn.ie

Lebanon's defense minister and the murder of Sri Lanka's foreign minister. Colonel Bengt Sandström of the Swedish Military Intelligence and Security Service says this kind of carelessness is intolerable and could result in up to six months in prison. It is unclear how the USB stick ended up in the library.

***

In 2006, a memory stick containing files on the Dutch military mission to Afghanistan was lost in a rented car. The documents also included information about the rules of engagement for Dutch troops in Afghanistan and the personal protection of Dutch Defense Minister Henk Kamp.

Also in 2006, the Dutch Defense Ministry reported the loss of another memory stick containing sensitive information about military intelligence agency MIVD[100].

6.3 Wireless

The global wireless market continues to grow rapidly with continuous technology innovation. As the WiFi deployment becomes more and more pervasive, the larger the risk that massive attacks exploiting the WiFi security weaknesses could affect large numbers of users. Hackers have financial motivations, corresponding to the ever increasing sophistication needed to bypass newly developed security technologies in the wireless environment. They can now launch fraudulent attacks that were reasonably assumed unlikely to be performed.

A large percentage of users do not change their password from the default established by the router manufacturer, and these passwords can easily be found on the Internet.

For all the other routers, it is assumed that 25% of them can have the password guessed with 65,000 login attempts, based on the evidence provided by security studies19 which showed that 25% of all users' passwords are contained in a dictionary of 65,000 words. Another 11% of passwords are contained in a larger library of approximately a million words. No back off mechanism exists on the routers that prevent systematic dictionary attacks. In the case where the password is not found in either dictionary, the attack cannot proceed. Alternatively, if the password has been overcome, the attacker can upload a worm's code into the router's firmware, a process that typically takes just a few minutes.

Airports, hotels, convention centres, and other public WiFi hotspots are known for being insecure. However that does not make users more cautious, as 24%, who have their laptop connected in a public place, never disconnect after they are done with surfing. Victims of an automatic wireless connection from a laptop are countless. By default, a laptop wireless device will connect to the first available hotspot around, which is how users get their computer hacked and their personal information stolen. This technique is known as the "Evil Twin". "The Evil Twin waits for a user to mistakenly sign into the wrong access point and captures the user's network data or attacks the computer", says Mike Klein, chief executive of Interlink Networks, Inc. It does not require technical expertise. Anyone armed with a wireless laptop and software widely available on the Internet can broadcast a radio signal that overpowers the hot spot.

"War Driving" is normally done by hackers cruising around in their cars and trying to find unsecured wireless network. Today, unsatisfied employees or paid hackers are spending time down a firm's building trying to break the WEP keys to get inside its network. Numerous tools are provided for free on the Internet, allowing any user to perform attacks in order to break into a wireless router.

[100] The Register, January 2008.

The last outbreak of any note was in July 2007, when another Trojan horse, dubbed "GpCode", demanded $300 to unlocked frozen files.[101]

6.4 VoIP

Use of Voice over Internet Protocol (VoIP) technologies has continued to expand during the past year. Rapid adoption to garner the economic advantages of VoIP has led many to overlook, or even set aside, security concerns. Vulnerabilities can exist throughout a VoIP network, from mismanaged and unpatched call proxy and media servers to the VoIP phones themselves. Vulnerabilities have been found in products such as Cisco Unified Call Manager and Asterisk, along with VoIP phones from multiple vendors. By leveraging those vulnerabilities, attackers can carry out VoIP phishing scams, eavesdropping, toll fraud, or denial-of-service attacks. Poorly designed implementations can provide inroads to data networks and researchers are continuing to uncover additional areas for potential attack, such as cross-site scripting through VoIP clients.

The vulnerability allows an attacker to initiate VoIP calls on the user's machine. From the end-user's perspective, it would appear that the victim is receiving the call from a falsified number that is specified by the attacker. Attackers on the other end could then coax account credentials or other sensitive information from the victim by impersonating a person from a bank, a stock brokerage or some other trusted organisation where the call appears to be originating.

VoIP is also another messaging medium ripe for spam. During the next few years, VoIP spam – also known as Spam over Internet Telephony (SPIT) – could raise the telemarketing industry at a high threat level to users. Unlike traditional phone lines, VoIP allows spammers to place a large volume of calls virtually free. Worse still, calls can be forged to fool more victims. Spoofed VoIP phishing attacks called Vishing will likely be more successful than their e-mail counterparts because anti-SPIT technology is far behind that of antispam, and many VoIP users will not expect attacks to come from names and numbers that match those of their banks. The growth of VoIP also provides criminals with easy access to disposable phone numbers, which they use, along with social engineering, to entice people to hand over their credit card details.

Vishing operates like phishing, by persuading consumers to divulge their Personally Identifiable Information (PII), claiming their account was suspended, deactivated, or terminated. Recipients are directed to contact their bank via a telephone number provided in the e-mail or by an automated recording. Upon calling the telephone number, the recipient is greeted with "Welcome to the bank of …" and then requested to enter their card number in order to resolve a pending security issue.

For authenticity, some fraudulent e-mails claim the bank would never contact customers to obtain their PII by any means, including e-mail, mail, or instant messenger. These e-mails further warn recipients not to provide sensitive information when requested in an e-mail and not to click on embedded links, claiming they could contain "malicious software aimed at capturing login credentials".

A new version recently reported involves the sending of text messages to cell phones claiming the recipient's on-line bank account has expired. The message instructs the recipient to renew their on-line bank account by using the link provided.[102]

[101] Computerworld, January 2008.
[102] http://www.fbi.gov, January 2008.

VoIP threats are:

- Worms and virus attacks causing service disruption that could have significant consequences
- Attacks on VoIP equipment could result in multi hour or day outages, call centres shut down, quality of customer service impacted or no access to critical services
- Leakage of sensitive corporate information through eavesdropping, resulting in loss of revenue, identity theft, scams, etc.
- Intercept or masquerading resulting in third parties gaining access to information related to national security, citizen's private information, etc.

6.5 Ransomware

Ransomware is a term used to describe malware that tries to extort money from users after an infection, usually to return access to suddenly-encrypted files. At the beginning of January 2008, a new one that locks up a person's PC and demands $35 to return control to its user appeared. It looks like this means of extortion is getting end-users to pay if they ever want to get their hands back on their data.

> The extortionists tell victims of the Delf.ctk Trojan horse to dial a 900 number, said Alex Eckelberry, CEO of Sunbelt Software Distribution Inc., a Clearwater, Fla.-based security developer. That number can be traced to "passwordtwoenter.com," a payment processor also used by hardcore pornography Web sites to charge for access to their content, added Eckelberry.
>
> Users infected with the Trojan horse see a full-screen message posing as an error generated by Windows.
>
> The bogus update window includes a "Click to activate new license" button that in turn brings up another screen, this one telling U.S. users to dial a 900 telephone number and enter a personal identification number (PIN). If the 900 number doesn't work, the page instructs users to dial alternate numbers - one in the West African nation of Cameroon, the other a satellite telephone number. The only way to regain control is to pay up by dialling. [103]

6.6 Anti-forensic

Forensic is gathering and analysing data without any possible distortion and reconstruct data or past activities from a system. When a miscreant perpetrates a malicious activity on a computer or a network, he leaves traces behind him which could lead to his identity, so in order to enable anonymity, hackers are using anti-forensic tools which are easy to find on the Internet. These tools allow their users to erase or replace data on a system, making computer crime investigators' lives difficult.

A hacking process will go through reconnaissance, scanning, gaining access, maintaining access and finally covering the tracks before leaving the attacked system. Today forensics faces anti-forensics who are subverting justice with exploitation. Since major forensics programs have started to attract unwanted attention from security researchers of a type that have plagued mainstream software developers for years.

List of common anti-forensic methods:

- Modifying files attributes like changing last date accessed
- Overwriting with data which provides misleading information to investigators
- Removing/wiping files; overwriting content with useless data

[103] http://indrakurniawan.blogspot.com – January 2008

- Deleting files (overwriting pointer to content)
- Data encapsulation – hiding by placing files inside other files
- Account hijacking – evidence is created to make it appear as if another person did the ''bad act''
- Archive/image bombs – evidence is created to attempt to compromise the analysis of an image
- Disabling logs - information about activities is never recorded

The Internet is full of specific tools like Timestomp, Slacker, Sam Juicer, Data Mule and others whose sole goal in life is to disrupt the work of forensic analysers and law enforcement.

6.7 Google's hacking

Since 2006, Google has been associated with malware. Fake Google search bar infected by a Trojan and all sort of vulnerabilities have taken the website to a high level of attacks.

In July 2006, users received an e-mail with a link to a fake Google page offering to download a file called 'GoogleToolbarFirefox.exe' which instead was installing a malware turning the computer into a zombie machine.

Google bombing refers to the attempt to influence the ranking rate of a website in results returned by a search engine. Google's algorithm will rank a page according to the number of external links referring to it. So the more sites publish links to a page the higher rank its gets. This technique was specially used by politics in the US when a group of Democrats attacked 50 Republicans during the 2006 campaign.

> Hackers have created, in 2007, tens of thousands of individual pages that have been created to obtain high search engine ranking. The anti-spyware firm Sunbelt Software discovered that surfers who click onto the malicious sites with vulnerable systems are infected with a strain of malware using the iFrame exploit. Computers compromised transmit false clicks to the hacker's URLs in a stealth way. The goal is to generate income through a pay-per-click affiliate program.[104]

But overall Google is definitely the most powerful search engine for hackers who can routinely find information on projects and personnel and the file names of confidential documents, even if they cannot access the documents themselves. Searches can be automated and results are received by e-mail. Hackers are using this huge source of information to perform spear phishing attacks which are one of the hardest for governments and companies to counter. Hackers will send an e-mail to a corporate executive that appears to be from someone inside the company (like the system administrator), a business partner or a supplier and related to a common project. Once the employee clicks on the attached document, the company's network will be infected by custom-written Trojan horse to bypass signature detection and will give potential access to confidential data.

6.8 Diallers

A German gang was jailed in December 2006 for having infected more than 100,000 computers with a Trojan horse that generated profits exceeding 12 million euros. The malware was dialling a premium rate 0190 phone number to contact an adult website.[105]

[104] Sunbelt Software.
[105] Net-security, December 2006.

6.9 Anti-theft keyless ignition system

State of the art high tech vehicles equipped with remote keyless entry systems use a circuit board, a coded Radio-Frequency Identification (RFID) technology chip, a battery, and a small antenna. The RFID chip in the key fob contains a select set of codes designed to work with a given car. Given that the car is broadcasting its code and is looking for a response, it is possible if sitting next to someone holding a keyless ignition device, to capture challenge-and-response pairs to crack the encryption using brute-force attack.[106]

In 2006, a 32-year-old car thief from the Czech Republic is alleged to have stolen several expensive cars in Prague only using a laptop and a reader.

The same year, soccer player David Beckham had two custom-designed BMW X5 SUVs stolen, the most recent theft occurred in Madrid, Spain. Police believed that it was done by an auto theft gang using software.

7 Conclusion

This report is a brief statement of criminal activities happening on the Internet. It shows how vulnerable systems are, but the weakest point still remains the end-user. The end-user is the one who clicks on the links, or shows a naive attitude when faced with social engineering techniques. Training users is only efficient for a short period of around three to six months, then the routine which sets in will erase all alarms which have been set up.

Cybercrime suffers from under-reporting and victims should be encouraged to file a complaint. The lack of reliable figures when it comes to work on statistics is due to end-users or firms who do not want to be known as victims. That is mostly because they do not want their story published as it could hurt their reputation and serves their competitors' purposes. The economic consequences of cybercrime are enormous. Billions of dollars are lost every year. As access to the Internet has grown, the opportunities for cybercrime have increased and bring a broader range of potential victims within reach. Information weapons have become a real threat for countries and firms, which should make information protection their most important concern.

Most difficulties experienced in cybercrime investigations and prosecutions are due to insufficient specialised training for law enforcement personnel. IT police should get a high level of technical, legal and international training. Reinforced and efficient international co-operation is one of the most needed solutions against cybercrime. But most of all it will require analyses by security experts, computer crime experts, criminologists, police and army forces whose knowledge and professional experience will provide the most refined response to cyber threats.

The next key problem that law enforcement will face is hard drive encryption. While it is essential that data are protected and secure, this causes major problems for investigations. Measures need to be identified to permit law enforcement access to encrypted data.

With technologies, ICT use and related cyber-threats quickly evolving, organisations such as the Council of Europe need to be kept up-to-date and remain alert so that counter-measures can be developed.

[106] Security Watch – May 2006