THE STATE OF CYBERCRIMES

Your computer may be “pwned.”(1) While you’re reading this article a miscreant might be virtually peering over your shoulder, or worse. Then again, perhaps you follow best practices for securing your computer: you patch your operating system, you maintain a current anti-virus software subscription, and your Web surfing habits are fastidiously cautious. Unfortunately your computer may still be pwned.

Depending on whom you ask, approximately 1.8 billion people are connected to the Internet.(2) Team Cymru(3) conservatively estimates that over 5 million unique computers are compromised at any given time. In dispensing with the FUD (Fear, Uncertainty, and Doubt) that often plagues the cyber security industry, the realistic global compromise rate is approximately 0.003%. An issue that plagues less than 1%(4) of the world’s computers may not appear to be an issue at all, but context is everything. When a new worm begins spreading, the cost of repairing millions of computers and interruptions to business can be staggering. When bank accounts are drained and e-mail accounts compromised, the victim is often left feeling helpless. When mothers are social engineered out of their life savings by a faceless criminal thousands of miles away, all of a sudden the impact of technology used for malevolent purposes becomes important. When a network responsible for processing 100 million debit/credit cards daily is breached, or the control systems for a city’s electric grid are disabled the fallout is beyond unpleasant.

Over the past decade cybercrime has continuously evolved, motivated by profit, ideology, and nationalism.(5) The Internet has enabled criminals to ply their trade in new and innovative ways. The physical elements of crime have been replaced by digital trails that are becoming increasingly difficult for law enforcement to follow. Attribution for cybercrime is rare, and prosecution is even rarer. Yet, the fight continues as investigators work harder toward criminal attribution. In this article, Team Cymru explores the nuances of today's most insidious cybercrimes.

The Underground Economy

The term "Underground Economy" has historically been used to denote business that occurs outside of regulatory channels. Around the turn of the 21st century, Team Cymru adapted the term to the cyber locations and individuals who buy, sell, and trade criminal goods and services. Today the Underground Economy can be found in IRC(6) networks, HTTP forums (web boards), various Instant Messaging services, and any other communications platform that lends itself to anonymous collaboration.
Today, the publicly available Underground Economy is a shell of its former self. The undercover operations targeting and subsequently arresting criminals involved in web forums like Shadow Crew,(7) Carders Market,(8) and Dark Market(9) have pushed the fraud trade further underground.

The Underground Economy is comprised of criminals who typically specialize in a specific criminal commodity. A few of the more common commodities include credit/debit cards, personal identities, hacked servers, hacked network equipment, malware (malicious code), Internet vulnerability scanners, e-mail spam lists, fictitious identification documents, and fraudulent money movement services.
Like any economy, this one involves various strata of criminal proficiency and experience. Participation in the Underground Economy requires only minimal technical ability, and many criminals' strategy is to defraud other criminals. The higher levels of the Underground Economy involve technically talented actors who work with other criminals through private communication methods often involving encryption. The public criminal market place is contracting, but the criminal activity itself is increasing in both volume and sophistication.

Scareware/“Fake Anti-Virus”

One of the latest trends in cybercrime profiteering involves “scareware,” also known as fake anti-virus software. The scam is maximized during a global event, such as the recent earthquake in Haiti. Criminals understand that a large event such as Haiti creates millions of queries on popular search engines like Google. Savvy criminals research key words linked to the event in question and then use those terms to create a new website that is pushed to Google for indexing. Often within hours of an event occurring (Michael Jackson’s death was another of these large global events), the newly created website appears in Google’s top 10 page rankings. Now millions of people may be visiting this newly created website in search of information related to the global event in question. Once the public accesses the website, a message is displayed informing the user that his/her computer is infected with malicious code. The webpage encourages the user to download an application that will clean the current infection and also locate additional malicious code that may be residing on the victim’s computer. Before this theoretical activity occurs, the program solicits credit card information. Typically the price for this scareware is twice what legitimate anti-virus companies charge for their product. The victim’s credit card is then charged and the user is left with a piece of software that is deliberately spurious at worst, and marginally legitimate at best. Either way, the victim is scared into believing a threat exists and the fraudster’s software package is the only way to resolve the issue.

Phishing

Phishing is the digital representation of social engineering tactics. The ploy involves tricking Internet users into providing confidential information, believing that the website requesting the information is legitimate. In fact, these Phishing sites are cleverly designed forgeries. The sophistication of these attacks continues to increase and the line between malware and phishing is blurring.

One of the largest criminal platforms for phishing and spam has been labelled by anti-virus software companies as “Avalanche.” It is believed that Avalanche is operated by a group of miscreants who run their criminal enterprise like any legitimate software company. Avalanche uses a technology that is specifically known in the security community as a “fast flux botnet.” The botnet is large and compromised of geographically diverse “zombies” (infected computers). The botnet also possesses powerful functionality (known as “fast flux”) that allows phishing websites to avoid take down efforts much longer by constantly migrating the website’s address to a different zombie in the botnet. The Avalanche owners generate revenue by leasing their expansive botnet platform to criminal customers for a wide array of wickedness. The flexibility of this particular botnet ensures owner attribution efforts are especially difficult.
Phishing has given birth to Pharming and Smishing.

Pharming typically involves changing the internal settings on a victim’s computer thereby bypassing a victim’s legitimate address query functionality. For example, a victim may open a web browser and request hsbc.com. The website loads and while the page appears to be hsbc.com, it is in fact a Phishing site. The user is seamlessly delivered to a spurious website because the victim computer’s internal settings were changed to redirect specific website requests to malicious websites that appear legitimate.

Smishing is Phishing across mobile phones. Smishing involves spamming SMS (mobile phone text messages) messages to a large pool of mobile phone numbers with a social engineering message and a corresponding website link to visit. Fortunately consumers appear to be much more wary of unknown mobile phone message senders vs. unknown e-mail senders. If mobile phone identity becomes a future challenge, then Smishing will become more interesting to criminals.
Banks protect their customers by campaigning to have phishing sites disconnected from the Internet as soon as the site is detected. Typically a bank will petition a website hosting provider to take down a phishing site within four hours of detection.

Cybercrime and Fraud

Recently the author of this article was on a trip to Chicago when he was notified that his credit card was used in Philadelphia. The spurious credit card was presented in person to purchase physical goods. The thieves had managed to capture the data contained on the credit card’s magnetic stripe before replicating the data to the magnetic stripe of a blank “white plastic” card. The swiftness between card compromise and physical exploitation was amazing. Unfortunately this scene occurs daily all over the world.(10) A credit card compromised in Britain, may be used within 24 hours in India. Criminals involved in physical world fraud are constantly leveraging technology to increase their profits.

Victim debit/credit cards can be used or sold as “cvv” or “dumps.” The criminal colloquial “cvv” represents the data embossed on the front of a card such as name, card number, expiration date, and the 3-digit security code printed on the rear of the card. “Dumps” describe the track1 and/or track 2 data encoded to the card’s magnetic stripe. A criminal is able to monetize “cvv” through online or phone purchases of legitimate goods. “Dumps” are monetized through duplication of the physical card and subsequent purchases of goods in person. Typically criminals resell the fraudulently obtained merchandise on auction type websites for competitive prices.

Stolen credit/debit card details remain especially lucrative for criminals. When PIN numbers can be tangentially obtained with a victim’s card details, criminals will monetize cash very quickly at ATM locations.

Team Cymru has observed groups of criminals operating in disparate geographic locations to maximize profit. Attacks on ATMs have been well coordinated, as have groups buying physical goods. Criminal groups can compromise and monetize their own credit cards, but typically criminals seek to purchase credit cards details from quality suppliers. The lure of easy profits creates a constant demand for quality dumps.

The source of stolen cards continues to originate through two primary methods: skimmers and network breaches. A hardware skimmer is a device placed over a card port on an ATM or gas pump. The skimmer is designed to capture the data on the card’s magnetic strip as it is inserted for payment or to withdraw cash.

This physical attack on the card previously required a criminal to retrieve the skimmer in order to download the captured data. Today, most skimmers sold in the Underground Economy are equipped with GSM or Bluetooth functionality thereby allowing criminals to remotely retrieve the stolen data and reduce the risk of capture. Generally these skimmers are equipped with enough memory to store a few hundred credit card numbers. Additionally, skimmers are sold to specifically match the manufacturer and model of ATM being targeted. Since ATM manufacturers publicly release new bank contracts, criminals are able to plan skimmer placement before new ATMs are even installed.

A soft skimmer is a device placed on a POTS (Plain Old Telephone Service) circuit in order to intercept the data in transit. Stand-alone ATMs in convenience stores or hotel lobbies may rely on modems for communication with a merchant network. After recording the tones on these phone lines, criminals use widely available software to convert the tones to digital data, specifically credit card numbers. Skimmers continue to be a threat to consumers in countries that rely on magnetic stripe cards.

Unauthorized access to computers and networks containing credit card track data has proven especially disastrous for merchants and banks. The breaches of Heartland Payment Systems,(11) RBS WorldPay,(12) and TJX(13) illustrate the determination of criminals to find and secure large databases of credit card track data. In the past, Point of Sale (POS) terminals used in retail outlets were exploited through vulnerabilities in the underlying operating system that these terminals use. Failure to patch the operating system has led to remote exploitation via freely available hacker tools. Data exfiltration has occurred for months before the merchant discovered or was alerted to the tainted POS terminal. Criminals continue to aggressively hunt for large amounts of card track data either in storage or in transit. Once a target is identified, the compromise is only a matter of time and resources. Today, financial databases and networks continue to fall victim to the most motivated and talented hackers. Previously, compromises have existed for over a year before the breach was discovered. The purveyors of this data will quickly become rich, as will the end users who purchase the data for coordinated exploitation.

The payment card industry (PCI) is in the final stages of implementing an updated version of the Data Security Standard (DSS).(14) DSS is a collection of policies and procedures designed to establish a best practices document for organizations involved in transferring or storing payment card details. While DSS is absolutely necessary and obligatory for merchants, it merely acts as a stopgap for an outdated magnetic stripe card technology. Multiple European countries have fully implemented EMV (also known as “Chip + PIN”), which has significantly reduced the criminal demand for “chipped cards” in these respective countries.

In this framework, debit/credit cards store data on an encrypted chip embedded in the card. While the implementation of the technical EMV specification may be different at various banks, overall the adoption has been very successful from a fraud perspective. Unfortunately this evolution has increased demand for monetization schemes in countries that do not use EMV. A global bank movement to the EMV standard would significantly raise the bar on criminals specializing in this trade. In the realm of “Card Not Present” fraud (telephone and Internet purchases), Visa and MasterCard implemented “Verified by Visa” and “SecureCode” respectively, which require an additional password before a transaction is successfully completed. Unfortunately, a substantial number of “cvv” sold in the Underground Economy today are accompanied by the corresponding Verified by Visa or SecureCode password. This is the result of criminals slightly modifying Phishing and malware attacks.

Malware

EMV also acts as a specification for secure online banking. Securing online banking access via a username and password in concert with security questions is a failed model. The financial services sector obviously defines failure on an annual rolling metric basis, but consumers and businesses feel the failure effects daily. Multi-factor authentication is a security term used to describe authentication procedures that require additional criteria be validated before access is granted. This usually means producing something you have in your possession in concert with something you know like a password or PIN.

Multi-factor authentication certainly increases the difficultly of bank account compromise, but in its current

form it is far from a solution for preventing fraud. Most two-factor deployments involve a hardware “token” issued by a bank to a customer. The digits displayed on the token change at regular time intervals. These digits are required in tandem with a customer’s password in order to successfully authenticate online.
The criminal response to two-factor authentication has been a continual stream of malicious code (also known as “malware”). Some of the more malevolent malware families are labelled by anti-virus software companies as “Sinowal,” Zeus,” “Silent Banker Trojan,” etc. The malware itself is programmed to execute clever functions while remaining as undetectable on the victim’s computer as possible. The malware typically turns off any anti-virus software present on the computer and then silently waits. It waits for the victim to open a web browser and login into their bank or other financial account(s). The malware then typically conducts a “Man in the Middle”(15) or “Man in the Browser”(16) attack. Skipping the technical minutiae, the malware is capable of initiating an account transfer that looks legitimate to the victim’s financial institution as well as manipulating returning data in the webpage to hide the fraudulent activity from the user. Both sides of the transaction are unaware of the digital thievery occurring in real time. Additionally, different malware families are able to extend the authenticated online banking session even after the victim believes they logged off or closed their browser. Regardless of the two-factor authentication banks are currently employing, malware authors continue to devise clever countermeasures. The technical arms race has no apparent end in sight.
The current situation is particularly harmful to small businesses and financial accounts that are not rigorously checked(17) by their owner(s). Criminals are performing online reconnaissance about specific businesses that appear to lack sufficient information security safeguards. Once a target is identified, malware placement is strategized, and then unauthorized bank account transfers or international wires begin occurring daily.
Of course online banking interception is only one small facet of modern malware. Today, the functionality embedded in malicious code is as diverse as the criminal population who utilizes it. Victim computers may be participating in spamming, DDoS(18) (Distributed Denial of Service) attacks, proxy points for cyber criminals, data theft, extortion (via encrypting the victim’s hard drive), key logging, advertising, and more. As Internet users’ habits evolve, malware authors take notice and develop new malicious features both for infection and monetization.

Then again, malware’s objective is not always revenue. Consider “Operation Aurora”(19) and the intended purpose of an apparent attack on Google’s network for the purpose of collecting data about human rights activists. On the surface it certainly appears the attack was not motivated by greed. Therein lies the differentiator between malware: purpose. Custom malware is typically only written when the surfeit of available malware or hacking tools will not suffice. Often, this is the case where stealth is paramount, such as in the case of “GhostNet,”20 which appeared to be exfiltrating data from the Dalai Lama’s network for over a year before anyone discovered the breach.

Malware is a scourge upon the Internet, and a particularly nasty subset of that malware is botnets. A botnet is a collection of infected computers (also known as “zombies”) that are typically centrally controlled by a remote entity. Ten years ago a bot was a piece of code that automated some activity, typically in Internet Relay Chat (IRC). Today, the term bot usually implies a malicious persistent connection from an infected computer to a Command & Control (CnC) interface.(21) This has created the problem of exporting real criminal tools to the criminal masses for a small fee. A handful of malware authors create botnet code that is then sold to the criminal public, typically for a few hundred dollars. These “crimeware” kits are delivered with meticulous instructions for use and a scale of fees for updated functionality and/or upgrades that prevent anti-virus detection. In fact the escalating game of cat and mouse between malware authors and anti-virus companies has become so extreme that over the past five years Team Cymru has observed 30 million unique malware samples(22) and a very small percentage of those samples are actually new pieces of computer code. The difference represents the by-product of polymorphism, encryption, and other obfuscation techniques (known in the security industry as “stubs”). Since anti-virus companies largely depend on exact signatures to identify malicious code and malware authors create malware that mutates (or is “packed” differently) every time it runs, thus producing a completely different signature for detection. Other obfuscation techniques attempt to hide the malicious code in a virtual shell (a stub) and anti-virus software only scans the benign shell.

Botnets are particularly sinister because they exponentially increase a criminal’s capabilities and malicious

schemes. Instead of infecting and controlling one victim's computer, a bot herder (an individual who controls a botnet) is capable of centrally controlling thousands, sometimes even hundreds of thousands, of victim computers at once. Presently, criminals who have no technical ability can purchase a botnet and further their criminality online. Regrettably, the purveyors of these botnets are now publicly advertising and marketing in order to differentiate their product in the market place. In Underground web forums and Twitter feeds,(23) botnet authors are actively attempting to increase revenue despite raising their risk profile with law enforcement.
Given the geographic disparities between victim's computers, CnC nodes, and the bot herder(s), law enforcement's attribution efforts are increasingly protracted and frustrating affairs. Until national cybercrime legislation enjoys global reciprocity,(24) law enforcement's efforts will continually be stymied. The picture, however, is not completely bleak. Law enforcement continues to pursue malware/botnet cases across international boundaries with occasional success.(25)
Presently, the problem is in scope. The current number of cyber-trained investigators is a pittance in relation to the number of criminals currently writing or using malware. The other impediment to quick criminal case disposition is the nature of the Internet itself. Technologies like TOR(26) and VPN networks allow criminals to move about the Internet anonymously. Internet privacy is certainly a noble value to support and uphold, but when law enforcement is unable to acquire required data in a timely fashion, cybercrime will continue to increase because the risk/reward equation is fundamentally skewed in their favour.

The World Wide Web

A confluence of malevolence is affecting the Web today. While "Web 2.0" represents an exciting new structure for ideas and opportunity, criminals are mirroring the optimism. Websites like Twitter and Facebook have become de facto communication tools, and criminals are leveraging the communication streams with innovative schemes. The trust models built into social media networks allow criminals to commandeer a victim's account and subsequently communicate with all of the victim's friends and associates. This equates to a new infection vector for bot herders. Additionally, groups specializing in criminal money movement used to create fictitious businesses online and then post reshipping and bank funds forwarding employment advertisements on employment search websites. Now these operations are migrating to social networking sites to recruit those desperate for work to participate in their ever-expanding criminal operations.(27)

Additionally, new web application vulnerabilities are announced almost daily with corresponding "point and click" exploit code(28) and accompanied by informative tutorial videos. Vulnerable websites are easily found via Google or other search engines by searching for specific text combinations (also known as "strings"). Once a vulnerable website is identified, typically it then becomes a race to steal sensitive data first.(29) Hackers understand that websites are increasingly powered by databases containing valuable data that could include customer lists, e-mail addresses, personal identifiers, credit/debit card data, etc. If a hacker is able to establish unauthorized communications with a database through a web browser, then the entire integrity of the website may be in jeopardy. Technical labels for these attacks include SQL Injection, Cross Site Scripting, Buffer Overflows, Remote File Include, etc. Many of the current web applications in development use new frameworks such as Rails and Django to simplify the development process, and history has shown that is it

only a matter of time before vulnerabilities are discovered in even the newest frameworks. Miscreants use freely available “friendly use” tools to exploit vulnerable websites. Black-hat hackers may hunt for new vulnerabilities in web application source code to keep for themselves, but eventually the new information will trickle down to the malicious masses.

Small business owners realize the need for a web presence and e-commerce solutions, but unfortunately security is often an afterthought, if it is considered at all. Web security also suffers because of cost. Knowledgeable web penetration testers are in demand and their services are typically out of reach for a small business. These professionals think like hackers and hunt for insecure code and configurations.

Speaking of infection vectors, do you ever wonder how all of this malware actually infects a victim’s computer in the first place? Malicious e-mail attachments were once the main threat that required wariness, along with self propagating worms that exploited unpatched operating systems; and while those threats still remain, by and large the favourite infection vectors include “drive by downloads,” Peer-to-Peer network file distribution, and social network social engineering.

Criminals discovered that it was becoming increasing difficult to push malware to victims so they decided to post the malware in locations where victims would naturally infect themselves on the Web. By hacking popular websites or incentivating visits to a lesser known website that hosts malicious code, criminals entice victims to download a “component” or “control” that is required for content functionality. Since many Internet users are conditioned to click through the successive dialogue boxes on these types of prompts, the malware installation occurs effortlessly.

When direct e-mails are the infection vector of choice (known as “Spear Phishing”), sophisticated actors will use vulnerabilities in prolific applications such as Adobe Acrobat.(30) A PDF attachment appears much more innocuous to the end user than a zip or executable file. Past attacks of this nature against US government contractors(31) have started with the receipt of an e-mail from a free web e-mail account like Gmail or Hotmail where the sender’s name is that of a co-worker or superior within the company. This social engineering coupled with the latest software vulnerability is effective and difficult to prevent from a human behaviour perspective.

Currently, social networks are being used to spam malicious web links that purport to originate from “friends,” when in fact the link originates with the “friends account.” Who is controlling that account is the rub. A decade of cyber security incidents has taught a level of mistrust for content received from unknown entities. When the content originates within an established trust model, often times the miscreants win.

Lastly, Peer-to-Peer networks can quickly become hazardous if they are used to locate and download pirated media/software. Criminals routinely insert malware into various Peer-to-Peer networks mislabelled as frequently requested content. Peer-to-Peer networks can be especially disastrous for business computers not only because of the malicious files they are exposed to, but also because of the information shared on the computer with the rest of the network.

The good news is that ISPs (Internet Service Providers) are implementing “walled gardens” in an effort to help protect their customers. Working with cyber security researchers, ISPs integrate daily lists of known CnC servers across the Internet. When a customer’s computer is observed communicating with a known CnC server, the computer is “quarantined” from the larger network and the customer is alerted. Once the customer’s computer has been cleaned of the malicious infection then the computer is reconnected to the Internet. This approach has proven effective to minimize a customer’s potential vulnerability after becoming infected.

The future

While it is difficult to accurately predict the future cyber threat landscape, Team Cymru believes the

continued adoption of smart phones represents an increasingly lucrative target for criminals. Mobile malware that creates a “backdoor”(32) or is able to perform “man in the application” functions will be able to compromise(33) victims’ mobile banking activities. Additionally, maintaining secure code in mobile phone applications will remain a challenge(34) for the companies providing the application storefronts such as Google, RIM, and Apple. Since thousands of applications are submitted for approval on different mobile phone platforms, storeowners must continue to rigorously check each application’s code for maliciousness and ensure the company in question authorizes the application being represented.

Conclusion

At one end of the spectrum, cybercrime appears to be increasing in scope and complexity, but the vexing concern is that decade old attacks still enjoy success. Well known vulnerabilities continue to exist on the Internet and information security best practices are continually ignored. Information assurance is still regarded as a niche field of study for students and professionals who labour in back rooms. Fortunately, large cybercrime events are garnering additional publicity, and government policy makers are beginning to appreciate the constant threat to governments, businesses, and individuals constantly at risk of being victimized.
The issue is crime. Fundamentally we are discussing people and their behaviours. Cybercrime is not a technical problem and technology will never solve crime regardless of whether it occurs in the cyber realm or not. The incentives must be removed. The risk of attribution for cybercrime must increase through global legislative reciprocity and a substantial increase in technical law enforcement staffing and training.
The good news is that law enforcement is forging partnerships with the cyber security industry, researchers, and academics that are on the front lines in the cybercrime war. Often these individuals provide the keenest insights into particular cybercrime groups and criminal cases. The proactive partnerships are leading to noticeable arrests and that is good for the world’s 1.8 billion Internet users who hope their computer is not pwned.

* Levi Gundert is a Southern California native with a background in business, technology, and security. Mr. Gundert is a former Secret Service Agent who specialized in economic and cyber crimes. He led multiple proactive cybercrime initiatives within the Electronic Crimes Task Force which resulted in world-wide arrests in cybercrimes. Mr. Gundert currently supports Team Cymru’s business intelligence group. He is a Certified Ethical Hacker (CEH), Systems Security Certified Professional (SSCP), and Certified Information Systems Security Professional (CISSP).

---

(1) “Pwned” is criminal parlance for the act of compromising a computer or network device and gaining unauthorized access to the resources within. The term is a derivation of “owned”.

(2) http://www.internetworldstats.com/stats.htm

(3) Team Cymru Research NFP is a specialized Internet security research firm and 501(c)3 non-profit dedicated to making the Internet more secure. By researching the ‘who’ and ‘why’ of malicious Internet activity worldwide, Team Cymru helps organizations identify and eradicate problems in their networks. Much of Team Cymru’s time is spent identifying emerging trends within the Underground related to the monetization of compromised information. Team Cymru works with various organizations and industries affected by the Underground Economy. Many of Team Cymru’s efforts are for the benefit of Internet users, and at no cost to their partners. Team Cymru also works with Law Enforcement, where appropriate, from over 60 countries around the world.

(4) On a rolling basis, over 25% of the world’s computers have probably been infected at some point.

(5) http://www.paltelegraph.com/latest/6288-1000-israeli-websites-hacked-since-flotilla-attack

(6) Internet Relay Chat was an early Internet protocol that allows multiple clients to connect to a server or network of servers. Channels are created within an IRC server that are akin to.

(7) http://www.consumeraffairs.com/news04/2005/shadowcrew.html

(8) http://news.softpedia.com/news/Former-CardersMarket-Admin-Sentenced-to-13-Years-in-Prison-134900.shtml

(9) http://www.fbi.gov/page2/oct08/darkmarket_102008.html

(10) http://www.msnbc.msn.com/id/37701078/ns/world_news-europe/

(11) http://datalossdb.org/incidents/1518-malicious-software-hack-compromises-unknown-number-of-credit-cards-at-fifth-largest-credit-card-processor

(12) http://www.wired.com/threatlevel/2010/03/alleged-rbs-hacker-arrested/

(13) http://www.computerworld.com/s/article/9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever

(14) https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

(15) http://www.owasp.org/index.php/Man-in-the-middle_attack.

(16) http://www.owasp.org/index.php/Man-in-the-browser_attack

(17) http://www.theregister.co.uk/2010/06/07/electronic_account_raided/

(18) http://en.wikipedia.org/wiki/Denial-of-service_attack

(19) http://www.wired.com/threatlevel/2010/01/operation-aurora/

(20) http://en.wikipedia.org/wiki/GhostNet

(21) A bot may poll a CnC server at different time intervals, but the bot herder maintains control of the infected computer.

(22) This number includes code embedded in HTML (webpages) which tends to contain a high level of similarity to other malicious web samples.

(23) http://www.infoworld.com/t/hacking/your-favorite-malware-authors-now-twitter-651

(24) http://www.hurriyetdailynews.com/n.php?n=turkey-to-ink-cybercrime-treaty-2010-06-03

(25) http://www.silicon.com/technology/security/2007/02/01/toxbot-hackers-sentenced-by-dutch-court-39165572/

(26) http://www.torproject.org/

(27) http://www.thenewnewinternet.com/2010/06/01/facebook-used-to-find-money-mules/

(28) http://www.theregister.co.uk/2010/06/08/padding_oracle_attack_tool/

(29) http://www.physorg.com/news194849560.html

(30) http://www.adobe.com/support/security/advisories/apsa10-01.html

(31) http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

(32) http://www.net-security.org/secworld.php?id=9371 -
http://marienfeldt.wordpress.com/2010/03/22/iphone-business-security-framework/

(33) http://www.itpro.co.uk/624025/hackers-target-windows-based-phones

(34) http://online.wsj.com/article/SB10001424052748703340904575284532 1ttoWhatsNewsFifth