ESET

Cybersecurity Review

Background, threatscape, best-practices and resources

Jeff Debrosse
Research Director, ESET, North America

Table of Contents

Background

Cybercrime is pervasive, pandemic and increasingly connected with other parts of the criminal ecosystem. It ranges from the theft of an individual's identity to the complete disruption of a country's Internet connectivity due to a massive attack against its networking and computing resources.

There was clearly vision (or luck) when the following statements were made in the 1992 movie "Sneakers":

> *"The world isn't run by weapons anymore, or energy or money. It's run by ones and zeroes, little bits of data. It's all just electrons."*
>
> *"There's a war out there, old friend, a world war. And it's not about who's got the most bullets. It's about who controls the information: ...what we see and hear, how we work, what we think. It's all about the information."*
>
> *— Universal City Studios, Inc.*

The target of cybercrime centers on information – the data that is electronically stored for retrieval and subsequent use. To get an idea of the scale of the threat of cybercrime, let's take a look at the overall use of the Internet, theft or exposure of personal data through data breaches and the amount of money lost to a cybercrime called "phishing" – one of the most common online attacks where a person is socially engineered to provide personally identifiable information by someone posing to be a trusted source.

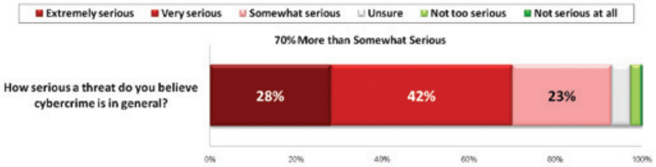
By the numbers

- 6.7B – Global population (census.gov)
- 60% - Global mobile phone subscriber penetration rate by end of 2008 (itu.org)
- 4B – Global number of mobile phones subscribers by end of 2008 (itu.org)
- 23.8% - Global Internet penetration rate (internetworldstats.com)
- 1.6B – Global Internet users (internetworldstats.com)
- 306M – Domestic population (census.gov)
- 74% - Domestic Internet penetration rate (internetworldstats.com)
- 251M – Domestic Internet users (internetworldstats.com)
- 251M – Number of data records exposed through domestic data breaches from Jan '05 – Jan '09 (Privacy Rights Clearing House)
- 3.2B – Total dollars lost to phishing scams against U.S. residents in 2007 (Gartner)
- 3.6M – Number of U.S. residents that lost $3.2B in 2007 (Gartner)
- 275,284 – Number of complaints filed with the IC3 (Internet Crime Complaint Center) in 2008– a 33% increase from 2007

Cybercrimes, like phishing and data breaches, are a scalable threat to the United States. These threats are so severe they are detailed as national security threats in the 2009 Annual Threat Assessment Intelligence Briefing to the Senate Intelligence Committee.

What exactly is cybercrime? Definition: Cybercrime encompasses any criminal act dealing with computers and networks. Additionally, cybercrime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, wire fraud, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet. Criminals will follow the money trail.

According to a Q1 2009 survey of 1000 adults by Competitive Edge Research and Communication (CERC) the public is aware of, and takes, cybercrime seriously.



— *Results of CERC survey Jan 27th – February 4th 2009*

Crime is a sociological problem that hasn't been solved in 4000 years of recorded history. Cybercrime is just the most recent vehicle and like the bank robber, Willie Sutton Jr. stated when asked why he robbed banks — his response was, "it's where the money is".

Consider for a moment the impact of 3.2 billion dollars, the amount lost just to phishing, invested in any country's real estate, its restaurants and corner shop coffeehouses, etc. Total spam-based fraud netted 43 billion dollars in 2008. Now imagine 43 billion dollars as venture capital, political clout for cybercrime syndicates or funding for terrorist organizations.

> *"This year, GTISC researchers estimatet hat botnet-affected machines may comprise 15 percent of online computers".*

Emerging Cyber Threats Report for 2009 — Georgia Tech Information Security Center.

Threatscape

The threatscape, as with any landscape, can be viewed as endless vistas of changing complexities and unfathomable permutations of technologies, network topologies, risk scenarios and user requirements. It is the white noise of this dizzying array of technologies – built upon an operating system monoculture, which makes for a healthy breeding ground for cybercrime.

Below are several negative elements of the threatscape:

1. Botnets
2. Malware
3. Phishing
4. End users
5. Cybercriminals
6. Data Breaches

Botnets

A botnet is a network of infected computers (bots, also known as drones or zombies) that is under the management of a central controller (bot herder) through the use of one or more command and control servers. The goal of the botnet is to use the infected computers for criminal activity such as generating spam, attacking a target (company, country, network, etc.). Regardless of the crime committed with the botnet, it can be used to generate revenue for the owner(s) of the particular botnet, political purposes, or simply to wreak mayhem.

"Botnets are the most dangerous species of network-based attack today because they involve the use of very large, coordinated groups of hosts for both brute-force and subtle attacks. "[1]According to Professor Randy Vaughn (Baylor University), "there are as few as six or seven major bot gangs and as few as 1,000 criminals controlling all infected computers."

The Nuwar, or Storm Worm created a botnet that consisted of over 2 million infected zombies or bots. Most recently, Conficker created a botnet that (depending on the source) is estimated to range from 5 million infected PCs to over 10 million.

Malware

The term malware is short for "malicious software." One of the most popular types of malware is bots. Bots are malware that cause the infected system to be part of a botnet, but not all malware is designed to turn an infected host into a bot or zombie (although that is a popular use for malware since it is a profitable business model for cybercriminals). Other types of malware are keyloggers, trojans, spyware and adware – to name a few.

E-mail Phishing & Spam

Phishing is a direct marketing scam targeting a recipient's bank account information or other private data, such as account credentials, social security numbers and so forth, by appearing as a trusted source to the victim. Phishing is just one form of cybercrime made unique in that its vehicle – spam – was originally used successfully for Business to Consumer (or B2C) sales before it was outlawed. It may come as a surprise to some people that cybercrime syndicates are very similar in some ways to startup businesses. They are even using the same business development tools that legitimate business use.

End Users

Hard facts disclosed in a February 2009 study detail how six out of ten people will leave with a company's contact lists (or other proprietary information) and either use them against their former company or leverage that data to increase their overall value to their new employer. This can become the worst nightmare any business owner or executive can imagine – a trusted employee with access to intellectual property, customer information or other sensitive data taking that information with them to work for a competitor.

Fact: in a recent survey of approximately 1,000 adult-age white-collar employees, 59% of the respondents stated that they would leave with sensitive corporate data upon layoff or departure.

Without adequate deterrence, this study shows that, similar to various reality television shows, as people get "voted off the island" — betrayal of trust becomes inevitable.

Directly quoting the February 2009 Ponemon study:

- 79% of these respondents admit that their former employer did not permit them to leave with company data.
- Approximately 68% are planning to use such information as email lists, customer contact lists and employee records that they stole from their employer.
- Not only is this putting customer and other confidential information at risk for a data breach but it could affect companies' competitiveness and future revenues.

-Presented by Dr. Larry Ponemon, February 2009

Cybercriminals

"Not everyone on the Internet is a bad guy, but every bad guy is on the Internet."

- Karen Hewitt, U.S. Attorney for the Southern District of California.

Cybercrime can best be thought of as the ultimate business plan. The compelling numbers behind cybercrime drive the criminals to go where the money is. Aside from the risk factor of it being the federal offense form of illegal, it's very compelling.

What motivates cybercriminals?

- Distribution model. Do it from anywhere with no required storefront.
- A large number of competing vendors. Some syndicates, under protection of their home country's government, offer license agreements for their malware similar to the legitimate approaches used by companies such as Microsoft and Adobe.
- Very low startup capital. While you can't approach a bank for this kind of startup, it doesn't take a lot of money to get started in the cybercrime business.
- Lack of law enforcement/regulation. Difficulty in prosecuting (expensive, difficulties in evidence gathering, jurisdictional squabbles, etc.)
- Downside: the cybercriminal can be quickly betrayed by their business partners or rolled up in a criminal investigation, and end up spending 3 – 10 years in prison earning $450 a year or less (a lot less than the criminal is used to earning).

ARMED ROBBERY:

Avg. "take" = $1,200
Arrested 8/10 Time
90% Conviction Rate

WHITE COLLAR CRIME:

Avg. "take" = $100,000
40% Conviction Rate
10% Serve Jail Time

For the criminally-minded, cybercrime is less risky and the end result is the potential to steal a significant amount of money versus a traditional crime such as armed robbery.

Generating revenue is the primary goal of cybercriminals. Getting past security is the challenge they face to reach this goal. The top two ways cybercriminals accomplish this are:

1. Betrayal of human trust (spam, phishing, social engineering)
2. Betrayal by automated software designed for illegal intent (malware, botnets).

To clearly illustrate the scale and impact a single crime organization can have, when the McColo hosting service was finally taken down mid-November 2008, according to Joe Stewart (Director of Malware research, SecureWorks), it was estimated that over 500,000 bots were disabled. Various reports from across the globe indicated that spam levels dropped 50% - 75% globally for the next 4-6 weeks.

Data Breaches

A data breach is the theft or leakage of information. This can range from the loss of a USB memory device to subverting a large organization's network security and stealing customer information.

Let us take some time to dissect a data breach that occurred in 2008 which involved the exposure/release of 4.2 million records. In the aviation world, when there is an accident it is referred to as a "chain of events" or the "error chain." These terms simply mean that multiple factors, rather than a single one, lead to an accident. The same can be said for security incidents such as data leakage. Take, for instance, the case of the Maine-based Hannaford Bros. grocery stores. Let's look at this chain of events:

1. The supermarket chain reported to Mass. Regulators that the scope of the malware infections appears to be larger than anything that is remotely possible. It is Hannaford's belief that a "trusted" source had physical access to the servers.
2. A trusted source with administrative remote or physical access to one or more servers installed malicious software (malware) onto those servers.
3. The malware intercepts customer card data and transmits that data outside of the network to remote servers.

These are just a few points, but if you add them up you will see the chain of events that added up to a data breach that revealed up to 4.2 million customer records. Keep in mind, that at the time of the breach, Hannaford Brothers was, in fact, PCI compliant. This reinforces the fact that companies must stay vigilant and look for anomalous behavior as well as correlate

HEALTH INSURANCE PORTABILITY and ACCOUNTABILITY ACT
HIPAA
ADMINISTRATIVE SIMPLIFICATION:
PRIVACY, SECURITY, TRANSACTIONS

Sarbanes-Oxley
COMPLIANCE JOURNAL

disparate pieces of information to draw larger pictures and determine the probability of attacks from various vectors.

According to the ITRC (Identity Theft Resource Center) data loss associated with insider-theft doubled from 2007 to 2008. The economic climate, and resultant desperation, doesn't help things either — recent figures show a 7.2% domestic unemployment rate in December of 2008. According to the Bureau of Labor Statistics we haven't seen unemployment rates this high since 1993. What's alarming is the rate at which this number grew - from 4.9% in January to 7.2% in December. With these numbers, there's a good chance that we'll be seeing more people engaging in insider-theft tactics as the jobless rates continue to climb.

While most would directly attribute penalties and fines per record involved in data breaches, there are additional consequences, some of which are:

- Loss of sales
- Investigation and notification costs
- Fines and litigation
- The cost of credit monitoring services for each customer
- Interruption of operations
- Last – but definitely not least: brand erosion (reputation, customer trust, etc.)

According to the ITRC "The number of records involved in data breaches are either under-reported or, in some cases, not reported at all". One trend is that corporations are facing greater financial risk from insufficient controls and unclear policies. Problems also arise when controls are put in place before the policies are written or completed — the controls are designed to be put in place to enforce policies.

With respect to data loss, increasing penalties as well as increased transparency, or at least opaqueness (limited transparency), are two paths that have been cited time and again in regard to increasing corporate responsibility.

Preventing breaches is a hot topic. Even in corporations that have well-written policies and effective controls, the percentage of data breaches that occur due to human error is still above 80%. There are two excellent paths to reducing data loss (or the value of the lost data):

1. Behavior modification – via employee training
2. Data encryption - which renders lost or stolen data useless to any unauthorized person that comes in contact with that data (and doesn't have the appropriate key).

The top three ways that data breaches occur:

- Weak passwords. A password works just like a key in a lock. With the right key, a cybercriminal can open the lock just as well as the intended party. Poor password protection is easier to crack and actually aids cybercrime. According to research the more people who have root access, defined as total control access, the higher the probability of a rotten password.
- Unprotected transmission. The most common form of data leak comes via unsecured email. Users perform their most basic duties or requesting a new password get a reply with the new password in their email. When retrieved by the user through an insecure email connection, say over an unsecured Wi-Fi at an Internet café, that email may be retrieved by someone other than, or including, the intended recipient.

- Under protected internal networks. For example, any business that refuses to do periodic security upgrades because they don't see the value in them. This action could cause their customers to be in the highest risk group for data breaches involving their credit or debit card information. For manufacturing facilities this translates to a large risk factor since a breach may also allow the introduction of malware into their products at some point in the manufacturing process.

A final thought on data breaches: with the retention of great amounts of personal information, comes great responsibility — and risk.

Cybersecurity Best Concepts and Practices

While there are seemingly limitless best-practices when it comes to cybersecurity, below are a several that should help reduce the likelihood of becoming a victim of cybercrime.

The OODA Loop

Cybercriminals have typically been on the inside edge when it comes to the race between cybercrime and cybersecurity. One of the strategies that has the potential to change this losing streak is called OODA – Observe, Orient, Decide and Act. This acronym was a revolutionary concept created by USAF Colonel John Boyd in the early 1960s.

Colonel Boyd observed that when two adversarial forces are maneuvering there is a tendency for one side to be constantly outmaneuvered. One side is deciding and acting before the other side can make a move. When one party gets locked into only Observe/Orient and is unable to Decide and Act, they are at the complete and utter mercy of the other party.

The challenge was that too many American pilots were becoming casualties of poor air to air tactics against the smaller, more agile Russian MiG aircraft. When the US Navy instituted TOPGUN to combat the MiG exchange ratio, its educational effort showed dramatic results. The exchange ratio increased nearly three times from just under 4:1 to 13:1.: (source: Benjamin Lambeth's *The Transformation of American Airpower*).

The cybercrime OODA loop:

- Cybercriminals are inside corporate OODA loops every time they steal data. They are inside consumer's OODA loop every time an online scam or phishing attempt works.
- Cybercriminals are global and often well organized.
- Cybercrime organizations are smaller and more maneuverable than most corporations.
- Some criminals are sheltered by certain countries' policies and laws, or lack thereof. Their thefts fuel their home country's economy and they aren't prosecuted if the crime is beyond the border.
- Cybercriminals collaborate in the design and use of malware as their tools.
- Malware, quickly explained, is literally 'bad software.' It's a tool used for criminal purposes just like a pry bar and lock picks would be used for a burglary.

Like TOPGUN education provided better decision making for Navy pilots, you increase your resistance by becoming more aware of the real world threats we face. Successful businesses OODA loop their competition. They are quicker off the start and constantly crushing the market. With cybercrime, that's where we all want to be, and hopefully some of you are there right now.

Antivirus

If you look at where antivirus was versus where antivirus is today, one can see that the industry has grown and changed tremendously. In the past there were static signatures which were somewhat easy to defeat over time – and opened a "window of vulnerability" – which was the time from when an exploit was discovered to when a signature was created and globally distributed. Following static signatures was the heuristic analysis of applications. This has often been plagued with a high number of false positives (which can be as time-consuming and disruptive as having real malware on a system).

Fast-forward to today; leveraging active/passive heuristics and static signatures for exceedingly high performance and detection with very low false-positive rates has proven to be a very successful combination. This is the best of both worlds and is able to scale with the ever-increasing prevalence of malware creation and distribution. Even with a technology such as whitelisting, there are pros and cons and the implementation of whitelisting will have to be evaluated for a particular organization's model. Whitelisting, while requiring fewer updates than traditional antivirus signatures, requires constant maintenance and querying of an ever-growing database of "allowed" applications, as well as their patches, updates and hotfixes, transferring the burden of analysis from antivirus companies' malware researchers to system administrators. Once an application is determined to be legitimate, it is allowed to run on the host system. If the application in question is, instead, malicious, effective (active) heuristic analysis will be able to determine the application's intentions and flag it as malicious.

The future of Antivirus: What we are seeing today is the convergence of several solutions into comprehensive security packages that address multiple security issues – including malware. Security/antivirus has historically been an after-thought in the development of applications and operating systems. Today, application and operating system vendors are taking a more active role in securing their products – but we still have quite a distance to travel. With the amount of mergers and acquisitions over the last few years regarding antivirus vendors, one can clearly watch the antivirus landscape morph into different models and meta-solutions. I see antivirus not as dead or dying, but changing to meet the threat from vectors that were not viable at the beginning of the antivirus industry.

Best Practices

CONSUMER:

- Use strong passwords.
- Keep systems updated and patched – this pertains to applications as well as operating systems and security software.
- Become aware that risk from Internet connected machines will never be 0%. The realistic goal is to reduce the risk to an acceptable level.
- If you are sent a link or attachment (via email, instant message and so forth) verify with the sending party. It takes a moment to check – but it may take hours or days to clean an infected system.
- Use a residential broadband gateway router between your computer and your broadband provider's modem to break the direct link the Internet has to your home computer.
- Periodically test your backups by restoring them.

BUSINESS:

- Simplify security for the end users – the more complex it is, the less inclined users are to using it.
- Keep systems updated (patched) – this includes applications as well as operating systems.
- Partner with the government and academia.
- Educate end users and make this an on-going process.
- Inventory assets – know what's on your network.
- Use business assets for business only. By doing this in conjunction with an effective policy (and enforcement), the risk level can be reduced dramatically.
- Run network audits regularly (log files, anomalous traffic, etc.)
- Hire a security firm to help secure your business.

Resources

The following is a comprehensive (although not exhaustive) list of resources:

- Securing Our eCity: www.securingourecity.org
- Internet Crimes Complaint Center: www.ic3.org
- National Cyber Security Alliance (NCSA): www.staysafeonline.org
- United States Computer Emergency Readiness Team (US-CERT): www.us-cert.gov
- Multi-state Information Sharing and Analysis Center: www.msisac.org
- Federal Trade Commission (FTC) *Protecting Personal Information: A Guide for Small Businesses*: www.ftc.gov/bcp/conline/edcams/infosecurity
- National Security Agency (NSA) Security configuration Guidelines: www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml
- Anti-phishing Working Group: www.antiphishing.org
- Anti-Spyware Coalition: www.antispywarecoalition.org

Conclusion

While it can be argued that the scaling cybercrime threat is an unsolvable problem, the fact of the matter is that the problem has not been solved – yet. Technological innovation has consistently leap-frogged security innovation primarily because security was not part of the initial design of the Internet.

As Internet usage matures, the advances in cybersecurity continue to move forward in leaps and bounds. The question is not if cybersecurity innovation will catch up to cybercrime innovation, but when the two shall meet.

Regardless of the agreements or disagreements on how individuals, companies and governments are to combat cybercrime, one fact stands true: Doing nothing is the worst posture to assume. Cyber risk is as limitless as human determination, ingenuity and ignorance.

www.eset.com

ESETSECWP20090508