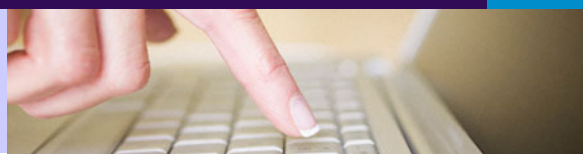
# Security Awareness News

February 2008



# Hacking for Profit

**Hacking 1960s:** It all started off as a game, a challenge among first generation computer scientists. A handful got the bright idea to siphon off rounding errors, amounts less than one penny, to another bank account in one of the first criminal endeavors.

**Hacking 1970s:** The only networks to speak of were the telephones, owned and operated by the monopoly, AT&T. Telephone hackers, also known as Phreaks (some say phreakers) took advantage of early network security weaknesses. The magic tone, 2600Hz, was exploited and an array of 'hacks' allowed unlimited free long distance calls. Blue boxes, red boxes and a rainbow assortment of hardware made it easy for newbies to 'hack' the then-much-maligned telcos. In retrospect, these hacks seem almost juvenile.

**Hacking 1980s:** The Internet grew up, a little, and almost 1 million people were its early occupants. A few million PCs were attached to very slow dial-up lines, but the hackers had fun anyway, breaking into corporate mainframes (for educational purposes, of course). In those days, remote access for updates and maintenance was done over a modem, with a phone number, all too often, with zero security. Hackers loved that. By today's standards the damage was very low. Viruses made their first appearance in the wild, many even appearing in the master software floppy disks from Novel, Intel and other companies.

**Hacking 1990s:** The web made a strong appearance in 1994, and hackers had a ball modifying home pages with graffiti. Viruses turned into a small epidemic, and the first major computer crimes appeared. The Citibank hack made headlines and the FBI, Secret Service and Department of Defense got into the game as Information Warfare and Cyberterrorism loomed on the horizon.

**Hacking 2000-2005:** Massive malware distribution world-wide caused hundreds of millions of dollars in damage; viruses, worms and Trojan horses infected computers with near impunity as the security experts attempted to keep up. Identity theft grew rapidly, affecting millions, and despite all warnings, it continued to grow almost exponentially. A global study in 2001 says the losses to cyber-crime exceeded $1 Trillion in the prior year.

**Hacking today:** The days of playful hackers are clearly gone. Today, hacking and its associated hostile code distribution are operating on a mass production line with profit as the goal. Hacking is now a global criminal enterprise. Losses are almost incalculable, but estimated to certainly be beyond the study we mentioned above.

The distribution of hostile code – malware – is clearly focused on scams, fraud and similar types of computer crimes. They generally work due to poor security awareness and ignorance of the basics of safe computer behavior. Tens of millions of users practice next to no security even though

*Continued on p. 2*

## Who Ya Gonna Call?

**Need to Report Something?**

**Contact Security, your IT manager, or Help Desk immediately.**

**Good security comes from timely response!**

Continued from p. 1

their computers are connected via high-speed connections 24/7 to the Internet. Criminal hackers discover new unprotected computers within 15 minutes of them being connected to the Internet. They can be compromised within an hour.

However, there are many other goals of the on-line criminal element. We, as a company, are the ultimate target of these sorts of attacks. The methods are the same, but the risk is much, much higher. Some of the most valuable goals would be:

- Our intellectual property.
- Employee privacy, which leads to costly identity theft.
- Our customer's privacy, which is also known as data leakage, and can cost us our reputation, business, bad press and deep financial losses.
- Massive identity theft.

In short, we are all targets. But, the security awareness techniques we cover monthly, if practiced every day, in all environments, are the simplest, most effective methods of security and crime prevention, here and at home.

## Did You Know?

The term 'hacker' is often used when the term 'cracker' would be more appropriate. 'Hacker' is really just slang for someone who enjoys learning about computers, programming, taking things apart and rebuilding them to do something that they weren't originally intended to do. The pejorative sense of the word 'hacker' usually refers to 'crackers', people who do criminal hacking, gaining unauthorized access to systems with the purpose of stealing, corrupting data or gaining profit. Within the hacking community, these crackers are not tolerated.

- www.hackinglinuxexposed.com

# Espionage at the Global Level

In its 2007 Report to Congress, the U.S.- China Economic and Security Review Commission (USCC) calls Chinese espionage the top threat to U.S. technology. www.uscc.gov.

"Chinese espionage activities in the United States are so extensive that they comprise the single greatest risk to the security of American technologies," states a USCC summary of the report.

As was written in the book "Information Warfare" in 1993, espionage will save nation-states the time and cost of researching and developing advanced technologies. Simply stated, it is faster and cheaper to steal than it is to develop.

The Commission also expressed concern about China's increasingly capable ability to destroy satellites and to wage cyber attacks against U.S. computer networks. Organized attacks on U.S. networks have been widely reported since 2005, following a coordinated assault that started in 2003, dubbed "Titan Rain." American security experts blame the campaign on hackers backed by the Chinese military.

In 1999, China actually declared cyberwar against the U.S., with concerted goals of taking over our critical infrastructures: finance, communications, transportation, power, emergency services and so on. By early 2008, according to some experts in the defense arena, they are succeeding due to our lack of awareness and appropriate precautions.

It's not just China, though, that has interest in stealing intellectual property and taking advantage of security vulnerabilities. Since the 1980s, France, Israel, Germany, Taiwan, Korea lead a pack of 122 countries practicing varying degrees of aggressive on-line espionage.

So, the next time you see an e-mail promising vast instant wealth (or any other suspicious claims), it is most likely not coming from your neighborhood hacker. It's coming from an organized criminal organization or, very possibly, from a nation-state sponsored attack, aimed at the company.

Defense requires little or no technical skills: just a level of awareness that will guide your behavior. Be sure to also become familiar with internal corporate policies, which are aimed at protecting us from these kinds of attacks.

# The Perfect Storm

Imagine if a million+ computers decided to attack the company, all at the same time. What would happen?

That is exactly what is happening on the Internet today. No, all million+ machines are not specifically targeting our company, but certainly we are seeing many of the attacks coming our way.

On January 19, 2007, a criminal endeavor, allegedly from Eastern Europe, launched a highly sophisticated suite of malware. Within 3 days, the Storm Worm accounted for 8% of global computer infections, an astounding growth rate.

The hostile code is so sophisticated, its internal defenses repel the majority of attempts to defuse it. Using a peer-to-peer model, the Storm Botnet is estimated to today infect between 1 and 50 millions computers world-wide. Capturing the attention of law enforcement and cyber-defense organizations, three highly disturbing trends are emerging:

*1. The Storm's creators and human controllers are seemingly selling pieces of the Botnet's power and capabilities to criminals who have their own agendas. It is alleged that the Denial of Service attack against Estonia in April 2007 may have been a politically motivated attack, and the Storm Botnet a 'hired gun'; a hostile network for hire.*

*2. The Storm can be apparently used to target specific organizations, IP addresses, persons, or perhaps even entire countries. In addition to the Estonian DOS attack, reports of highly targeted spam and scams, aimed at specific companies are emerging.*

*3. Much of the Storm's power is used for vast spam generation, allegedly able to send billions of e-mails daily. As the Storm grows, the spam-power will only increase. Some companies say that 96% of Internet traffic is spam.*

The Storm is going through continual upgrades, keeping security researchers several steps behind in analysis of the code as they attempt to learn how to create defenses.

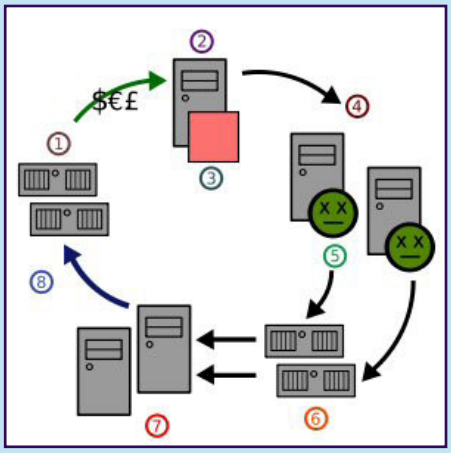
While the Storm is perhaps the world's greatest spam generation engine, one of the hidden goals of much of that spam is to infect the targeted machines and make them part of the Storm Botnet.

In protecting our corporate information, we have to continually keep in mind that criminal elements are active, highly sophisticated and powerful in the cyber realm. These are not eager teenage hackers out for a joy ride. Given the incredible value of company information, the Storm can become, at any time, an even greater threat if we become targeted.

All the more reason to practice safe computing. Wherever you happen to be, do not open those e-mails that smell of spam. Delete them immediately. Be smart. Be alert. The Storm Botnet has grown to the size it has due to the unintentional, yet still dangerous, poor security habits of consumers and users at companies of all sizes.

And, if you suspect for any reason that your personal or work computers might have become infected with Storm or any other type of hostile code, contact your administrator. We do not want the Perfect Storm reaching our corporate shores.

## How the Storm Botnet Works




*The typical lifecycle of spam that originates from a Storm botnet:*
***(1)** Spammer's web site **(2)** Spammer*
***(3)** Spamware **(4)** Infected computers*
***(5)** Virus or trojan **(6)** Mail servers*
***(7)** Users **(8)** Web traffic*

# COMING NEXT MONTH!

## Backing Up Mission Critical PCs & Other Devices

1. Corporate data no longer resides in a single location, making backup all the more difficult.

2. Do you know how your desktop is backed up? Maybe it's time to find out – for sure.

3. When on the road, how is your laptop backed up?

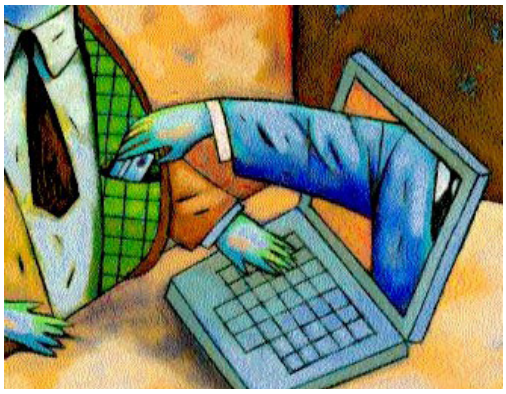
4. What about your cell phone, PDA, Blackberry and other smaller intelligent devices? Do they need backup? What about electronic meltdowns or if you lose one? Have a plan?

# Scamming for $$$$$$$$$$

According to the Internet Crime Complaint Center (www.ic3.gov) the top-ranking scams that become major multi-million dollar crimes are indicative of the kinds of mass marketing used to victimize unsuspecting users, at work and at home. The exact extent of this kind of computer crime is unknown. Estimates, though, range from a few hundred million to several billion dollars annually; but those are low guesses at best. Keep in mind that these scams are not run by some kid down the street. These are operated by professional criminal organizations, often overseas, who hire people with the technical skills necessary to run a large-scale operation.

In most cases, the criminal(s) will send a convincing e-mail. Get Rich Quick and Greed are the most often cited reasons for people to respond. Unaware users get sucked in by professionals who know how to work the greed psychology of the respondent. By the time a victim recognizes he has become scammed, his money is gone and there is little, if any, chance of recovery.

The criminals who have perfected this system send out vast quantities of e-mails (yes, spam) and only need a small response



to make their operation profitable. We are talking about a billion plus e-mails every day. You may only lose $25, $100 or so, but many of the more gullible victims lose $5,000 and more. In a few cases, certain individuals have lost $100,000 and worse. Even so, law enforcement will more than likely do no more than just take your name. You become another statistic.

To avoid becoming a victim, being security aware is #1 on the list. That means being sensitive to a few key points:

1. If it's too good to be true, then it probably is.
2. Know who you are dealing with. Precisely.
3. Deal with reputable firms that offer other means of contact than just e-mail.
4. Don't believe that every URL you see is legit. Learn how to read what is 'behind' the link.
5. Be suspicious, not paranoid.
6. Trust, but verify.

For an in-depth list of recommendations on behavior for each of these scams, visit www.ic3.gov/preventiontips.aspx.

Lastly, and exceedingly important for the company, is, never respond to these kinds of offers or scams from work, especially using your company e-mail address.

Any sort of response endangers company security. Your response…

*…legitimizes company e-mail and company domains.*

*…only encourages further spam and solicitation.*

*…could infect company computers with hostile software.*

*…could affect our overall security posture and the privacy of customers and employees.*

Please be certain you are aware of corporate policies if such e-mails do reach your desk.

## Yet Another, But Effective Cyber-Crime: Scamming with Gas

According to police, potentially tens of thousands of people could become the victims of the Gas Station Scam. It's occurring all across the country, in cities large and small, and no one is immune. Debit card users, beware!

The crooks hijack your account information by planting an electronic device called a ***skimmer*** inside the gas pumps. They merely leave it there for a period of time, come back and remove the device. Later, they download that information to a card that has a magnetic strip, and then they are able to use the fake card, just like they would if they had ***your*** debit card. You don't even have to lose possession of your card for someone to be using it!

Police say skimmers of this type are one of the hottest trends in crime right now. Debit cards are especially vulnerable because the skimmers record pin numbers as well. Installing them, police say, is relatively quick and easy. They just block the worker's view by parking a large vehicle (SUV) in front of the pump. This gives the person who is doing this crime, time to get in there and plant the skimmer – it takes just a few seconds - and then come back later to remove it.

Potentially hundreds of thousands of victims don't even know they have become victims yet, and the scam is likely to expand to more retail outlets that accept debit cards, and even ATM machines themselves.

So how do you defend against skimming? Here are some options:

- **Pay cash.**
- **Use a credit cards and check statements thoroughly.**
- **Get a monthly credit monitoring service for about $20 year.**

This is not meant to create paranoia, only to alert you to another scamming technique and to remind you to stay ever aware of how your own personal information is handled and exposed in every day living!