Cyber Criminality

Is Your Worst Nightmare Coming True?

Cyber Criminality
– Is Your Worst Nightmare Coming True?

It is early Saturday morning. You are still lying in bed next to your peacefully sleeping wife. From the ground floor you hear the familiar sound of your two young children already awake and playing with their toys. You are in a great mood and it feels like everything is going your way right now. After several tough years the furniture manufacturing company you are heading is definitely on the right track, and just a few weeks ago you won a lengthy legal process against a foreign company. Their CEO seemed quite bitter and disappointed. On a personal level you could definitely feel compassion for him, but he did not deliver as promised and you eventually had no other choice than to terminate the co-operation with his company. It most likely put him in a terrible situation, but he had himself to blame and at the end of the day business is business.

Suddenly the doorbell rings. A few hours later you find yourself sitting at the police station right in the middle of the worst nightmare of your life. The policemen had escorted you out of your home in front of your family and neighbors, at the same time confiscating your private computer. When they showed you some of the pictures and videos that were found on your hard drive, you thought they were playing a bad joke on you. It was the most disgusting material you had ever seen - illustrating young children being sexually abused. As the interrogator kept on pushing you about these awful media files, you started to realize that your life had just been completely ruined. Your computer contained log files proving that it had been used as a tool to search for, download, and distribute child pornography materials. You were facing an extensive prison penalty and were about to lose your family, career, and entire life for a crime you did not commit.

This story could have been taken out of a science fiction novel. But the scary truth is that we live in a world where an attack like this would not be harder to accomplish for a skillful cyber criminal than breaking into your house would be for an experienced burglar.

Weapons, Criminals, and Stolen Goods for Sale

In the early eighties people started to realize the frightening implications of cyber-crime, it also became a popular theme for movies. Who doesn't remember the movie WarGames, where a high school student via his home computer and modem hacks into what he thinks is a new thrilling computer game. When in reality, the system he has hacked into is controlling U.S. nuclear weapons and a third world war is avoided at the very last minute.

Cyber-crime today is not carried out by "innocent" hackers just for the fun of it. It has turned into organized economical crime and at an estimated value of $100 billion annually it represents a higher value than illegal drug sales worldwide.

Information Technology has become business critical to organizations of all sizes and the sensitive information that is stored in any organization's network represents significant monetary values. Risk managers worldwide try to estimate the potential damages of competitors getting their hands on their intellectual property and it is a scaring exercise. According to PricewaterhouseCoopers, corporate espionage costs only the world's 1.000 largest companies more than $45 billion every year and cyber espionage is ranked number three on the SANS Institute's list of "Top Ten Cyber Menaces for 2008".

All evidence points in one direction; cyber espionage poses a substantial threat for businesses of all sizes. The reason that cyber espionage attacks get relatively little attention in the media is that the affected companies do not always discover the intrusions. And if they do, then they are very reluctant to go public with such announcements. For example, Citibank learnt this lesson back in 1995. After announcing that they had been hacked, millions of dollars were withdrawn by people who feared that their funds were at risk.

In closed communities on the Internet, information that has been stolen during cyber-crime attacks are bought and sold literally every day. And as if that wasn't enough, tools for carrying out attacks are traded on these well-developed underground markets. The availability of these tools has made it much easier to become a cyber criminal. It is surprising how little technical knowledge is required today. According to a report from Symantec, the following items are the most commonly traded on the underground market:

RANK FOR SALE	GOODS AND SERVICES	PERCENTAGE FOR SALE	RANGE OF PRICES
1	Bank account credentials	18%	$10-$1,000
2	Credit cards with CVV2 numbers	16%	$0.50-$12
3	Credit cards	13%	$0.10-$25
4	Email addresses	6%	$0.30-0.40/MB
5	Email passwords	6%	$4-$30
6	Full identities	5%	$0.90-$25
7	Cash-out services	5%	8%-50% of total value
8	Proxies	4%	$0.30-$20
9	Scams	3%	$2.50-$100/week for hosting $5-$20 for design
10	Mailers	3%	$1-$25

Table 1. Goods and services available for sale along with advertised prices.

As shown above, bank account credentials are found at the top of the list. Financial account information is attractive as it provides the opportunity to withdraw large amounts of currency without the need for PIN codes or similar. The average advertised bank account balance was much higher than the average advertised credit card limit – nearly $40,000 for the former compared to about $4,000 for the latter. This is also reflected in the price for corresponding information. Bank account details are priced considerably higher, ranging from $10 - $1,000, while credit card information goes for $0.50-$25.

Combined, credit card details are the single largest group of information traded in the underground communities. If you are a frequent buyer on e-commerce sites, you are probably familiar with the CVV2 code that is printed on the back of your credit card. This code, that is not stored on the magnetic stripe, is requested when paying online with a credit card. Not surprisingly, credit card details with corresponding CVV2 numbers have a much higher market value than credit card details without CVV2 numbers.

Stolen information is very often sold in bulk, with prices depending on the geographical location and the issuing bank in the case of credit cards. It is also interesting to notice that EU accounts are advertised at a considerably higher price than their US counterparts.

To withdraw from a bank account, the criminal can assume the identity of the account owner or accept the proposal of a professional cashier that is prepared to do the dirty work. Acquired credit card details can easily be used to buy goods or services over the Internet. To disguise the criminal's physical location, advertisers offer drop locations to which bought goods can be delivered and picked up. Stolen credit card details can also be sent to production facilities which return physical cards ready to be used for cash withdrawals in ATMs and of course, purchases in traditional stores.

Other frequently traded items are email addresses and email passwords. Email addresses are sold in bulk and they constitute a substantial value as they can be used in spamming and phishing attacks. A phishing attack means that the victim is cheated to hand out sensitive information such as username, password, or credit card details, by masquerading as a trustworthy entity. Making a fake website whose look and feel is very similar to a well known bank is a typical example. Stolen email passwords can be used to "borrow" the email account for spam attacks and for collecting email addresses.

Personal identity information is also hard currency in the underground economy. A stolen identity can be used in many different ways. The criminal can use the fake identity to obtain credit cards, apply for loans, get access to confidential information, etc.

Methods used by Cyber Criminals

You may ask yourself how is it possible for a cyber criminal to store child pornography on your computer without leaving any traces, how someone can get inside your corporate network to get their hands on your intellectual property and how such massive quantities of stolen financial account details, credit card numbers and personal identity information can be available for sale on the Internet? To straighten it out let's start with dividing attacks into two main groups; opportunistic and targeted attacks.

An opportunistic attack is when a cyber criminal targets potential victims randomly in the hope that some of them will be vulnerable to an attack. It is not important for the criminal who the victim is, but rather how many victims there are. For example, a cyber criminal stealing and trading stolen credit card information is likely to take an opportunistic approach as his income is in direct proportion to the number of credit card details he can offer on the underground market. Mass mailing attacks are a typical opportunistic approach where the criminal only expects a low percentage of the targets to be affected.

In a targeted attack, the victim is a specific organization or person. Some possible scenarios could be cyber espionage, hijacking of a website due to political reasons, blackmailing or personal attacks for reasons of revenge. In general it is much harder to protect against a targeted attack, as the attack is tailored to make use of the specific security weaknesses you are exposed to rather than being a generic way of attacking the easiest targets, i.e. the least protected networks.

The traditional way of committing cyber attacks has been to send different types of malware, e.g. computer viruses or Trojan horses, in mass-mailing attacks to potential victims. Because commonly used anti-malware solutions today handle these kinds of opportunistic attack attempts quite well, the "effectiveness" of these kinds of attacks has definitely decreased.

But don't make the mistake of letting this give you a false sense of security. The cyber criminal community is very creative and dynamic in its nature. The methods for exploring the growing number of security weaknesses are constantly evolving. At the same time our network infrastructures are becoming increasingly complex, integrated, and open - which expands the attack surface for cyber criminals.

A very insidious way of committing cybercrime is to turn a legitimate website into a weapon to compromise and control computers that visit the website. This is achieved by injecting malicious code into the website by exploring vulnerabilities in the website architecture. Once the malicious code has been executed on your computer it is under complete control of the criminals, most likely without your knowledge. If your computer is connected to a network, you have now also provided the cyber criminals with an entry point to that entire network. Even worse, you computer can be used for criminal activities such as botnet attacks, where a large number of compromised computers are used as "weapons" by cyber criminals.

For targeted attacks, a very common approach is to hack into an organization's network by making use of security vulnerabilities that the infrastructure is exposed to. Vulnerabilities can be known security weaknesses or misconfigurations of any software or hardware component in the network. In fact, there are tens of thousands of publicly known vulnerabilities, with numerous new vulnerabilities being discovered every day.

Hacking into networks may sound like something only a small community of very skilled technical people is involved in. However, that is no longer true since several different hacking tools are available for free or for sale in the underground communities.

The most popular hacking tools include:

- **Exploits** – A small piece of code that explores specific vulnerabilities. This can be everything from exploits making use of general vulnerabilities in web browsers to exploits targeting site specific vulnerabilities on financial sites.

- **Autorooters** – A tool that scans any specified network range for vulnerabilities. Found vulnerabilities are automatically explored by executing an exploit on the compromised computer providing the attacker with complete control of the computer. The autorooters then remove all traces of the intrusion by cleaning log files. According to Symantec, autorooters are available from $40 with an average price of $70.

The characteristics of a hacker have changed quite dramatically over the last few decades. The nice high school student in WarGames is no longer a good representative of today's heavy cyber criminals that are the brains behind the organized and economically devastating crimes being carried out today. The availability of easy-to-use tools for performing cyber-crime activities has definitely contributed to this development, luring in potential attackers all over the world and bringing cyber-crime to a completely new level.

Conclusions

To summarize, cyber-crime has turned into a well-developed underground market of massive magnitudes. Attack methods are getting more sophisticated every day and organizations of all sizes are potential targets. So what can be done to protect your valuable assets?

First of all, it is important to take an overall approach to IT security. The chain is not stronger than the weakest link so it is crucial not to lose sight of the big picture. At the same time, we can conclude that most organizations have already implemented anti-malware software, firewalls and other reactive measures. Unfortunately, that is no longer enough. With today's complex and open network infrastructures combined with a true explosion in security vulnerabilities in commonly used operating systems, applications, and hardware components a more proactive approach is needed.

In order to compromise a website or a network, cyber criminals, or the tools they are using, search for vulnerabilities to exploit. When visiting a website on which malicious code has been implanted, you are at greater risk of infection if your web browser has unknown vulnerabilities that can be exploited. Today, actively managing and eliminating vulnerabilities in order to reduce your risk exposure to an acceptable level is absolutely key. As new vulnerabilities are discovered at such a rapid pace, an automated approach that provides the ability to assess the network on a regular basis is the natural starting point.

In order to learn more about Vulnerability Management, please feel warmly welcome to visit **www.outpost24.com**