"Highest Performance
Lowest Price"

Microsoft GOLD CERTIFIED Partner

GFI WHITE PAPER

Targeted cyber attacks

The dangers faced by your corporate network

Sign up to GFI's FREE SMB-Zone Newsletter

Receive FREE invites to SMB focused content such as IT Advice, Topical White Papers, MVP Tips and Tricks, Webcasts and much more!

Introduction

This paper helps you identify key features needed to effectively deal with spam.

Abstract

Cyber attack is the name given by (usually sensationalist) articles and documents describing crimes that occur in a virtual world as opposed to tangible attacks such as war. A targeted cyber attack is when the attacker specifically targets someone or a company. A successful attack will typically allow the attacker to gain access to the victim's assets, allowing stealing of sensitive internal data and possibly cause disruption and denial of service in some cases. One example of a targeted cyber attack is an attack in an industrial espionage case where documents were stolen by penetrating a victim's database server. Another example can be the actions of a jealous boyfriend spying on his girlfriend's online activities by hacking into her instant messenger or email account. Increasingly, the results of cyber attacks can be felt in a tangible world – victims of such attacks typically suffer financial losses and might also lose credibility.

Cyber attacks: A real threat for every organization

Most organizations wrongly assume that cyber attacks will never reach them because an attacker will not find value in targeting them. In general, most organizations feel that they cannot become a victim to an Internet (or network-based) attack and might hide under one or more of the following:

- "That will never happen to me"
- "I have nothing to hide"
- "We're too small to be a target"
- "Why me, when they could hit some bigger company? "

It will never happen to me

It is very easy to distance yourself or your organization from any kind of online threat, because a good majority of the victims of targeted attacks never reveal any information about when they were attacked. Unless one

looks hard, it is relatively difficult to find people or organizations that admit that were victim to an online attack. Organizations are especially cautious before they inform their customers (and effectively the public), that their data got stolen because this usually triggers a security concern in customers and they might even look for another "more secure" vendor or service provider. For example, in 1995, when Citibank announced to the general public that it got hacked by a Russian hacker, millions of dollars were withdrawn by people who believed that their funds were at risk. After this incident, Citibank learnt one valuable lesson: "Don't make it public" (Scheiner).

Luckily, companies under the jurisdiction of the California law (Civil Code 1798.82) now required any person or business that maintains computerized data such as personal information that the person or business does not own to notify the customers immediately of (possible) intrusions which involve data theft.

All organizations have something to hide

As more organizations are incorporating email and Internet into their workflow, it is safe to assume that most organizations send or receive confidential emails including emails with attachments of documents which are not intended to be public. Modern-day organizations also resort to corporate online shopping or other forms of online transactions. Therefore, an email address that initially doesn't seem to have any value suddenly becomes the email address used to buy products from online retailers.

People say, "I have nothing to hide", but then are aware that the password for an online retailer might mean that their account will be used for forfeit purchases. They might choose a more secure password than the one they use for their email account but some online retailers offer to send your password to your email address if you forget it and the password of the email address might be much simpler than the one used to purchase from the online retailer. Even worse, most people use the same password everywhere for different services, so cracking one password means that the attacker can access the victim's other accounts. Some online services might not be as trustworthy as others – they might be vulnerable to attack, or else the operator himself is corrupt. As the saying goes, security is a problem of the weakest link.

While targeted attacks are generally a corporate problem rather than a personal one, some attackers do take their actions to a personal level. The reasons behind these actions may be various: Spying on a partner, revenge on a previous employer or even identity theft.

Industrial espionage

Business is a bit like war, except that there are legal restrictions that govern what can be done and what cannot be done. Competitors in the same industry aim to conquer similar territories through different ways and means. Research is a valuable asset and some organizations might resort to foul play and fund industrial espionage to catch up with a competitive firm. Normally, stealing research only costs a fraction of the millions of dollars that were put into research and development for a given product or service.

In an ever-changing world, most organizations are exposed to worldwide competition. Laws and ethics belonging to one country do not apply to another country. Strong concerns have been raised over Chinese organizations making use of industrial espionage to catch up with the US and European counterparts (The Guardian). For example, in January 2003, Cisco filed a lawsuit against Huawei accusing the Chinese rival of copying the IOS source code, Cisco's technical documentation, command line interface and patent infringement (Cisco). However, China is of course not the only country to be involved; France, Russia, Israel, Japan, the United States and others are known to have stolen technology secrets from other countries. In 2001,

US consumer goods giant Proctor & Gamble agreed to settle out of court with Anglo-Dutch rival Unilever over allegations of corporate spying (Center for Management Research).

In May 2005, the news broke out about an Israeli industrial espionage ring making use of trojan horse software to conduct these operations. Haaretz newspaper described how a large number of businesses, including TV, mobile phone, car import and utility organizations, used a trojan horse written purposely to target rivals and gain financial and industrial advantage (PCWorld, 2006). This particular case came to light when an Israeli author, Amnon Jacont, complained that parts of an unpublished book that he was working on appeared on the Internet without his consent. Further investigations pointed towards the trojan horse used in the industrial espionage ring and proved that the case was much more complex than originally assumed.

Extent of the problem

Effectiveness of a targeted attack

Most attacks on the Internet consist of opportunistic attacks rather than attacks targeted for some specific entity. An opportunistic attack is when an attacker targets various different parties by using one or various generic ways to attack such parties, in the hope that some of them will be vulnerable to attack. In an opportunistic attack, an attacker will have a large number of targets and will not care that much on who the victim is, but rather on how many victims there are.

Examples of opportunistic attacks:

- 419 Scams
- Mass Mailing Worms
- Trojans emailed to various people
- Scams involving well-known services such as PayPal or Ebay
- Mass scanning for vulnerable services (SSH, UPnP, IIS servers etc)

An attacker will generally find it much easier to make use of an opportunistic attack then a targeted one, simply because a broad scope will probably have a better chance of success in gaining access to sensitive information. There is simply more money (and possibly less risk) in computers that are vulnerable to common attacks and not well guarded, than attacking a specific company or person which might be better protected against such attacks. In a test, which lasted two weeks (TechWeb, 2006), AvanteGarde concluded that on average, it takes four minutes for a new Windows machine exposed to the Internet to get hacked.

On the other hand, various individual organizations are still potential victims to targeted attacks. The motivations behind such attacks can be various:

- Industrial espionage
- Publicity attacks
- Malicious insider

- Personal attacks (such as revenge or spying)

A targeted attack is much more effective and damaging for the victim since the actions performed by the malicious hacker are tailored. This means that it is much more difficult to stop a targeted attack than an opportunistic one simply because the attacks themselves are not general.

Email is of course a medium that is used to carry out both opportunistic and targeted attacks. The fact that there is no specific point and click product that protects against targeted attacks is what makes them so effective and hard to avoid. Most security solutions handle general attacks quite well, because the security solutions themselves are for the general public. An email content filtering solution that catches email worms by identifying them through a signature aimed towards known worms will most likely let through malicious executable code, which is targeted for a specific company running. In fact, most content filtering solutions handle opportunistic attacks quite well since that is what customers will face on a daily basis and therefore software companies working on such solutions cannot afford to let in a single mass-mailing worm.

Common attack vectors

Email

People generally expect that someone who is authorized to do so will contact them. On the other hand, they do not want to choose who is authorized. This assumption creates a loophole because email allows anyone to contact anyone else (and vice-versa) regardless of who “they“ are. The basic email protocols (RFC) do not provide any authentication of the “From“ address. Additional tools such as Pretty Good Privacy (PGP) and Sender Policy Framework (SPF) attempt to fix this, but they are not generally accepted by most of the end users. This essentially means that when a user receives a notice from their service provider to inform them that their account is about to be terminated, verifying the authenticity of such an email is not so straightforward. There is no alert that says, "This email is not from the person in the sender field" or “This email is from the person in the sender field”.

Such an email will probably ask the end user to perform an action, such as visiting a website. But should one trust such a request, based on which criteria, is it worth the risk and what's the risk? The level of risk depends on the request. The email might also ask you to:

- Visit the service provider's offices to update your account
- Visit the service provider's website to update your account
- Open an attached file which contains more information
- Reply to the email with your details

If one cannot easily verify the service provider's website against the one provided in the email, then it is generally very risky to click on the link in the email. Attackers will use various methods to fool victims into visiting their malicious website while pretending to be a trusted sender. These are some of the methods used:

- Similar domain names, where an attacker will try to mimic the domain name by altering one letter, for example instead of www.yahoo.com an attacker would register yaho0.com. The last "o" is actually a

zero, which would point to the attacker's website. Similarly, attackers have previously used Unicode characters in URLs Unicode URL Hack (Schneier, 2006)

- Various well-known methods to obscure URL's (PCHelp, 2006).
- An email might point towards a URL which exploits Cross Site Scripting vulnerability on the service provider's website. Citizen Bank and several others have suffered such an attack (CNet, 2006).
- Exploit vulnerabilities in web browsers.

Given the growing number of web browser security vulnerabilities (Secunia), some of which do not have any official remedy from the vendor, it is very easy to be duped into browsing a malicious website which may execute code remotely on the victim's computer.

In the case of the Cross Site scripting attacks, it is the case that the Service Provider (unknowingly) becomes an accomplice to the attacker. The website location is authentic in the sense that it does belong to the legitimate owner, but the content of the website has been modified by an attacker gain and profit, for example to harvest information such as usernames and passwords.

The most straightforward and effective way for an attacker to launch his own code on his victim's computer is to actually attach his executable to an email message. The most common of this kind of attack is known as "Mass Mailing Worms", like the Nimda worm which made rounds back in 2001, or the more recent variants of Bagle and Netsky worms which made up a substantial part of the email traffic during 2005.

While these worm attacks may actually get a lot of press, email is a very useful tool for **targeted** cyber attacks. The fact that email:

- Allows an attacker to contact his victim directly
- Can act as a file transfer medium
- Does not provide sender identification.

All of the above are good reasons for this useful tool to also get useful for the aspiring intruder.

June 2005 saw the arrest of a London-based computer specialist Michael Haephrati and his wife Ruth accused of supplying Trojan horse software to third parties bent on committing crime (Washington Post). Related to this, in July 2005 the US Computer Emergency Readiness Team issued an advisory which suggested that attackers were sending out email attachments with Trojan files which when launched, are able to perform the following functions:

- Collection of usernames and passwords for email accounts
- Collection of critical system information and scanning of network drives
- Use of infected machine to compromise other machines and networks
- Downloading of further programs (e.g., worms, more advanced Trojans)

- Uploading of documents and data to a remote computer

September 2005, Taipei Times reported an “attempted e-mail attack”. According to the article, an unknown attacker had sent Trojan attachments via email to the National Security Council's (NSC) secretary computers. The email subjects read "freedom" and "arms procurement”, which was a way to try enticing the end user in running the attached Trojans by making the email content sound relevant.

According to a Message Labs July Report, one or two targeted attack incidents are seen each week. The report also details how in July 2005, an exploit in Microsoft Word was used by attackers to target a particular international organization. The emails were destined to just a few “highly targeted list of recipients” and contained a Microsoft Word attachment, which in turn would exploit a buffer overflow and typically (though not necessarily) give remote access to attackers.

Network attack

When an attacker decides to target a specific corporation, they can either get personal with the employees by making use of email and other similar technology, or go through the gateway. Finding the location (IP address) of the company network is usually quite straightforward, since a lot of organizations host the email server on the company network. Even if it is not the case, email headers of mail sent out by employees, usually contain enough information to point towards the internal and external IP address of the network.

From there, the attacker will enumerate the IP address pool belonging to (or hired by) the victim, and enumerate the services exposed to the Internet, such as SMTP, HTTP or VPN. Version information (for example, gathered through HTTP headers or SMTP banner) will usually help the hacker determine if the service is running up-to-date software with all the security fixes. Even if the software running on the server is not known to be vulnerable, a determined attacker will likely audit the software for new unknown security flaws – provided that the software is available publicly. For example, if the target is known to be running IIS 6 with a specific commercial or OpenSource Web Application, the attacker is likely to download that web application and test it out on IIS 6, learn all about its default settings, how the web application implements security, where sensitive files are stored and so on.

Misconfiguration is often another flaw that a lot of administrators overlook. For example, it is very easy to set incorrect permissions which allow anyone to view sensitive files. Some Windows administrators make use of software written or packaged for Unix/Linux operating systems. When the software is installed on a Unix/Linux OS, it would set the right permissions so that sensitive files and directories are not accessible by unauthorized personnel. However, when installed on Windows, these permissions are not set and therefore a service exposing those directories will allow attackers to read sensitive files that should have otherwise been inaccessible.

Common examples include:

- PHP scripts packaged in tarballs (.tar files) for Unix/Linux servers and installed on a Windows Web server. All directories end up “world readable”.

- Web Applications written for Apache (and making use of .htaccess files), but installed on IIS. By default, IIS does not know about .htaccess files, and will expose these files to anyone with a web browser (or less).

- Traditional misconfigurations such as default passwords and open proxies are still often found in large networks.

In an article by SecurityFocus, back in 2002, Kevin Poulsen wrote about Adrian Lamo who found "no less than seven misconfigured proxy servers" belonging to the New York Times exposed on the Internet. This particular security hole allowed Lamo to get on the internal network and further access more important documents such as "a database of 3,000 contributors to the Times op-ed page, the August soap box of the cultural elite and politically powerful."

The compromise of one of the servers belonging to CardSystems, which was reported publicly on June 2005, affected directly VISA, MasterCard, American Express and Discover and obviously their customers (The New York Times). Although the full intrusion details did not emerge, a MasterCard International spokesman was quoted (SoftPedia, 2006) saying that the data security breach at the CardSystems could have happened because of software security vulnerabilities that were "cleverly exploited by the intruders who had manage to install a rogue program to capture credit data on its network". The same article goes on to suggest that old Microsoft software (such as Windows 2000 and IIS 5) was to blame. John M. Perry, President and CEO of CardSystems Solutions INC., testified (Financial Services, 2006) in front of the United States House of Representatives, that the attackers (somehow) dropped a script on a server belonging to CardSystems, which was exposed on the Internet. The job of the script was specifically to search for a particular file type, extract information from that file type and send it to a remote server through the FTP protocol.

Instant Messenger Attacks

Instant messenger attacks are very similar to email. With instant messenger, the attacker is able to more easily and instantly communicate with her victim. However most instant messengers have the following security differences from email:

- It initially requires more effort to get the victim to trust because (with MSN and Yahoo Messenger), one is required to sign up.

- The victim can choose whom to communicate with and therefore (unlike email), can choose to "not talk to strangers".

However, when those steps are followed, it becomes easier for the attacker to get his own custom code on the victim's computer, or gain access to sensitive information. People are generally trusting, especially when they think that they know the person already. What makes instant messaging easier is that unlike email, IM is not constantly targeted by opportunistic attacks and therefore most people will trust content coming from their instant messenger when they wouldn't give the same content coming from email a second thought.

Targeted attacks via Instant Messenger generally require further information gathering for the attacker, but is more likely to give 'return on investment' than email – especially since a lot of businesses are moving towards IM from email for quick messages that would take much longer to arrive through email.

Distributed denial of service attacks

DDoS (Distributed Denial of service) allows attackers to knock off its victim rather than steal information. Although this attack is less technically challenging when compared to others, its effectiveness should not be underestimated. Some of the attackers making use of DDoS are hired by competitors – such as the case of Jay Echouafni, who was CEO of TV retailer Orbit Communications (SecurityFocus, 2006). Echouafni is accused of

financially backing up (and effectively recruiting) hackers to cripple three competitor online stores. This created long periods of downtime for the victims with estimated $2 million in losses to the victims and their service providers.

Distributed denial of service attacks typically consist of flooding the network with packets, reaching its limits. As a result, legitimate requests are lost or at least the service becomes too slow to work with. The attackers gather a large botnet, as described earlier, by making use of opportunistic attacks. Then they use these botnets to direct thousands of systems to attack a single server or network. Even when a service, such as eBay, has much larger bandwidth than any of the bots, it is no match against all of them at the same time.

Increasingly, it is becoming popular for attackers to attempt to extort money out of the victims. This is very similar to the traditional Mafia, when the attacker asks for a ransom and in turn promises to stop harassing people for a while. One particularly well-known case (Prolexic Technologies) is when online-casino BetCRIS.com was hit by an attacker who demanded $500 in protection money. When the owner paid up, the attacker hit again and this time she demanded $40,000. Rather than paying up just like others had done before, this particular casino decided to fight back. This resulted in the discovery of a ring of students who were later arrested and charged.

In another similar story, three Dutch attackers were arrested and accused of used botnets as large as 1.5 million computers to target organizations such as 180Solutions (CNet, 2006) – which eventually helped gather evidence against the suspects. While some of these stories might sound impressive, they only come out as a result of action being taken. It is assumed that the majority of cases are not disclosed with the general public.

Bypassing security mechanisms

Most modern corporate environments nowadays make use of various security solutions such as:

- Firewalls
- Content filtering for email and web
- Intrusion Detection/Prevention Systems (IDS/IPS)
- Virtual Private Network (VPN)
- Patch management
- Anti-virus

While these security solutions do help a lot with the majority of attacks, none of them provide a single solution against the problem of security as a whole. Each of these solutions addresses specific security issues. The following are examples of well-known ways that clever attackers use to bypass specific security mechanisms:

- **Bypassing the traditional anti-virus**

  To bypass anti-virus software, the most straightforward attack is to avoid making use of a known malware that will be caught. Instead, an attacker usually creates a custom made backdoor and delivers that to the victim. The anti-virus software will try to match the attacker's program against a list of

known signatures belonging to malware in the wild (ITW) and will probably be bypassed. Anti-virus heuristics try to catch unknown malware by passing it through various 'advanced' technologies such as a sandbox. Therefore a stealthy adversary would test his piece of software against various commercial or popular anti-virus software and makes sure that it is not caught. This is not a difficult task.

- **Bypassing email content filtering**

  Email content filtering solutions usually make use of anti-virus solutions, so methods which use anti-virus signatures are likely to bypass the content filtering. Apart from the attacks outlined in the previous paragraph, attackers are simply making use of a link to a website (URL) which contains malware. Therefore the email content filtering solution will only see a plain email with a URL as no actual malware is attached to the email. Instead the victim is expected to follow (with the help of a little bit of social engineering) the link that leads to a compromise of her machine.

- **Bypassing the firewall**

  To bypass firewalls, attackers can attack servers that are not fully protected by the firewall and hop from server to server. Some administrators might bounce from server to server themselves; so all the attacker has to do in this case is to follow the administrator's steps.

  Since traditional firewalls do not look at the content of the network packets (except for a few exceptions such as FTP), attackers can piggyback allowed traffic such as instant messaging and email.

- **Bypassing IDS/IPS**

  Intrusion Detection/Prevention Systems inherit similar problems that affect the anti-virus vendors. Since there are various ways of representing (possibly malicious) information, bypassing patterns is a matter of changing an original attack to achieve the same effect (for example, exploiting a buffer overflow in Sendmail) in a slightly different way. For example, if a signature searches for "../" in an HTTP request, the attacker can encode the URL or parts of it to look like "..%2f". While the web server will decode the request back to "../", our theoretical IDS signature will not match the exploit attempt and therefore be bypassed.

Apart from the fact that security mechanisms can be bypassed one way or another, these same security solutions can also be vulnerable to various attacks that they're supposed to be protecting other software from! For example, Snort has previously had vulnerabilities (Secunia, 2006) that could be exploited by malicious attackers remotely controlling the security application. Various anti-virus software packages were vulnerable to similar attacks (remote, 2006).

Solutions

Minimizing exposure

As the saying goes, "prevention is better than cure". Preventing network attacks will also prevent other tasks that might follow. However, it is generally accepted that security is a process, not a product (Schneier, 2006). This means that security is an ongoing thing, rather than just something that you fire and forget, so that preventive measures implemented in 2002 does not mean that they're still going to be relevant for 2007.

Reducing the surface area

Simple security is generally better than complex security (Schneier , 2006). Complex systems will be costly and therefore might not be easily financed or implemented. Additionally, when security systems are complex, legitimate users will try to find a way around it. Simple systems, on the other hand, are easier to understand and better analyzed. A simple system will therefore have less chance of falling prey to attacks, simply because there is exposure to attack.

Understanding how a security system works means that one can also understand where a security system fails. For the attacker this means opportunities, but for the security designer this means that she has to close that flaw. When a security system is simple, it is therefore easy to close its security flaws. On the other hand, when a security system is complex, the security designer and the attacker will keep on finding new flaws in the system forever. While the security designer needs to find all flaws to have a sufficiently protected system, an attacker only needs to find one flaw to successfully attack the system. Because of this reason, with complex systems, attackers will always be a step ahead of the defender.

For example, when Oracle announced its "Unbreakable" marketing campaign in 2001, the team seemed to fail to recognize the fact that their database software is too complex to match their claims. At the time of writing (2006), Oracle is still marketing their database software as "Unbreakable" (ZDNet, 2006), having just issued a patch, which addresses 47 security issues (Secunia, 2006) in its software in July 2005.

In a secure environment, designing a new network or picking up new software, sticking to one that satisfies the requirements whilst keeping the system transparent and simple should be a priority for the network/system administrator.

A particular package's vulnerability history might also be indicative of what's to come. Qmail was written as an alternative to Sendmail because the author of this software was tired of poor security history of Sendmail (Bernstein D.J., 2006). He decided to write a better MTA which is much more resistant to network attacks. In fact, nowadays a lot of security conscious organizations nowadays make use of this package rather than Sendmail.

Adequate protection

Most modern networks are equipped with various security solutions to prevent against the majority of common Internet attacks. These solutions usually cope quite well with the majority of opportunistic attacks such as worms and so on, but how do they cope with the determined, financially backed up hacker?

Firewall

As described earlier on in this document, traditional security measures such as firewalls can be circumvented quite easily. That doesn't mean that you should ditch the firewall. The firewall is in fact a very good security solution especially at covering up vulnerable services that should never be exposed to aggressive networks such as the Internet. It means that the firewall is limited to protecting against a good number of opportunistic attacks as well as limiting scope for attack for the determined attacker. Having a well-configured firewall minimizes exposure and allows the administrator to focus on securing more sensitive or vulnerable parts of the network.

Content filtering

Content filtering can play a major role in protecting organizations and ISP customers against targeted attacks. A content filtering solution for email, which goes beyond scanning attachments using an anti-virus, can help

administrators detect and possibly block an attack from a competitor. For example, some content filtering solutions can rate executables according to their functionality. Instead of just matching executable content against a list of signatures, such software is able to identify functions that could be attributed to malicious behavior and block that. This adds an extra layer of protection against one way to bypass anti-virus. That alone is not enough, and some products also catch known exploits that bypass anti-virus software, but somehow allow access attackers to get on a victim's computer. As one can see, such products try to cover whatever conventional products don't cover – and some of these attacks are ones that a targeting intruder is going to make use of.

Intrusion prevention systems

Intrusion prevention systems allow administrators to detect and block attacks reactively. Although these systems do not prevent attacks, they do actually stop attacks from successfully exploiting vulnerabilities. There are various forms of Intrusion Prevention Systems – Network based such as Snort Inline as well as host based such as Microsoft's DEP introduced with Windows 2003 and XP SP2. One problem with Intrusion Prevention Systems is that they have a tendency to give false positives and therefore blocking legitimate activity. Similar to other security measures, they need be fine-tuned for the particular environment needed.

Patch management systems

Distribution of patches is very important in both the corporate environment and home. Most intrusions that occur due to software bugs (rather than configuration), can be prevented by installing the appropriate patch issued by the software vendor. While it does seem simple, there are a few problems with patch management:

- Not all software has automated patch notification and installation
- With an increasing number of software being installed on various servers, it is difficult to keep up with the vendor patches
- From time to time, patches are known to cause issues themselves along with fixing security issues. Therefore administrators like to test a vendor patch before applying it to their corporate servers.
- Some patches are not so easy to install. They might require manual installation.

Therefore, when choosing software, it is important for the security planner to choose one that takes patch management into consideration. This becomes a very important option especially when a major security hole in a particular software (or hardware device) is uncovered. When such a security hole is made public, a targeting attacker has a much better chance to successfully attack his victim, and while the security conscious victim is still testing the vendor patches.

Penetration testing and security auditing

One way to actively test the security of a computer or network system is to do what the attacker is supposed to do in a legitimate way i.e. perform a penetration test. These tests, performed by professional or white-hat 'hackers' will usually yield the following results:

- Proof that the computer or network system can be hacked. A professional will almost always be able to successfully attack a client's system provided that it's functional and complex enough. This of course depends on the amount of time given to the professional and also the amount of experience and

knowledge the professional has. SANS (2006) describe how to identify a good security consultant from a fake one.

- Identify one or maybe a few easy targets in the system, which allow the Penetration Tester (and also the attacker) to successfully attack a system.

- A report on the tests performed and how to fix the security issues which were identified.

Penetration testing is very good for simulating a targeted attack. Instead of the adversary financially backing up an attacker, a company is able to do the same with someone on their side (hopefully before the adversary does). This simulation might be a very good example of what can happen in real life but of course the penetration testing professional cannot perform all actions that can be done by the real attacker. While denial of service attacks are usually not allowed on a functioning system, in real life the attacker does not care whether or not she's allowed to perform denial of service attacks. Same goes with a successful attack – a real attacker might install Trojan software or "rootkits" to keep access to the victim computer – this activity might be frowned upon in a Penetration test, depending on the system being tested.

Even though a penetration test is usually very useful, especially in proving to the higher management that the network can in fact be attacked, it does not provide the same results that a complete security audit does. Penetration testing allows a professional to look at the system from an attacker's perspective – from outside – and exploiting just one vulnerability in a critical system is usually enough to gain access to sensitive information. This means that from this perspective, it is very difficult to identify all security weaknesses in a system. On the other hand, a security audit allows one to identify weaknesses in the system itself – from a designer's point of view. Such an approach should give a more thorough analysis of the system and therefore allow the security auditor to identify theoretical and practical weaknesses that the penetration testing approach does not necessarily identify. A security audit also analyzes any security policy that the organization might have. Good security policies are very important not only when a security incident occurs, but also when preventing an attack in the first place.

A security audit could involve:

- Auditing any source code – especially home-grown applications. This will allow the discovery of any developer errors that might result in security bugs. It might also uncover intentional or unintentional backdoors in the software itself.

- Auditing of network structure and design. This will allow the administrator to identify key systems which need to be better protected. Password policies and access control lists should be reviewed.

- Backups and secure storage systems should be reviewed. This will allow the administrator to identify any possible problems related to recovery of important data in case of failure.

How can cryptography help?

Cryptography is a very useful tool in the hands of a security designer. Typically, it allows two people to communicate over an insecure network such as the Internet. Cryptography can add the ability to verify that the sender of a message is indeed who he claims to be, and also to encrypt the message itself, so that only the receiver (or number of receivers) can read it.

If Company A needs to contact Company B on the Internet, its sensitive message needs to go through a number of third party routers before it reaches its destination at Company B. Now, Company A and Company B do not know if a service provider (owner of a third party router) is intercepting the messages and sending them to competitor Company C. In fact, all it takes is one corrupt service provider to compromise the messages. To make it easier for Company C, one of these service providers might also be vulnerable to hacker attacks – so that the service provider doesn't have to comply with Company C to hand it the sensitive messages. So basically Company A and Company B can only trust each one another – they cannot trust the service providers in between to deliver their messages in a secure manner. This is where cryptography is handy – it allows the two parties to trust one another and no one else.

PGP is a tool that is very good at this. When used together with email, it allows parties to communicate safely over a protocol that doesn't provide verification of the sender, integrity of the message, or ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. A targeted attack aimed towards the email system between Company A and Company B can focus on either email servers of both organizations, of the communication channels in between. Such an attack, even if it's successful in acquiring the messages whilst being transported, will fail to succeed because the technology used by PGP does not allow the attacker to read the messages.

However PGP does not protect against an attacker who has access to either of the environments where the message are being either encrypted or decrypted. This means that if the environment being used by Company B is compromised, the attacker can watch Company B decrypt the messages and effectively compromise the system. On the other hand, it is now much easier for the security designer/administrator to protect his system since the scope for attack has been sufficiently reduced.

Cryptography is not a solution for all your security issues:

- Just because a Virtual Private Network is using sufficiently secure cryptography, it doesn't mean that a determined attacker will not guess the password for a user who doesn't following basic practices.
- If, for instance, John is using PGP to communicate securely with Jane, and John accepts a new public key that claims to be from Jane without verifying the fingerprint, the PGP is compromised.
- A web application that makes use of SSL (Secure HTTP/HTTPS) can still have Cross Site Scripting, SQL injection and other vulnerabilities. These security issues can still be exploited by attackers on a "secure website" just because secure in this case means that the connection between the attacker and the web server is encrypted and cannot be eavesdropped. In fact, an attacker will probably prefer attacking a Web Application over HTTPS than over HTTP just because his attacks cannot easily be caught using protocol analyzers or Network Intrusion Detection Systems such as Snort (Snort.org, 2006).

Minimizing impact - Detecting the Attack

A well-configured Intrusion Detection System together with log analysis allows network administrators to get alerted when someone takes a fancy in probing their network. In fact, monitoring is a very good solution to the targeted attack problem. However, most of the time, the problem with monitoring is the overflow of information. For example, a default installation of Snort on a busy network will start generating various alerts, most of which are not relevant and are allowed traffic. Therefore the administrator needs to tune the IDS to her specific needs rather than just install and forget. A host based Intrusion Detection System (HIDS) which is well configured, will allow the administrator to detect any servers or workstations, which are misbehaving.

When Akamai, a distributed computer company was victim to a targeted attack (InfoWorld, 2006), it was able to detect and pinpoint the cause of the problem through the use of monitoring systems. Although the monitoring did not prevent them from becoming a victim to a large-scale network attack on their DNS system, it did give them information needed to react to the attack and probably make the necessary changes for future similar attacks.

Incident response team (IRT)

Handling a security breach is the part of a security plan that most organizations tend to forget about. The assumption that an organization cannot be breached is a very bad approach as seen earlier in this document. It does not allow the development of an approach towards security incidents and therefore leaves a company wide open once the security measures have been bypassed. Just detecting an attack is obviously not enough – an organization needs to react to the attack. If a burglar alarm is set off, and no one is there to react to it, then the burglars might as well carry on dragging your goods to their van.

The job of the Incident Response Team (Inform IT, 2006) is to react to the situation rationally and in a timely fashion as well as help fix the security problems exploited in the first place. In smaller organizations, the IRT would probably consist of selected individuals from different departments such as network administrators and human resources. The team has to be skilled and trained to handle various situations – including identifying a targeted attack and reacting to it. In this case, the team might probably have to work with the legal department depending on the case.

Sometimes the situation is not so straightforward. For example, following a web server intrusion, to fully analyze the extent of the problem, the administrator might need to make an image of the server. This means downtime, which in turn might mean losing sales – making the reaction of the administrator not so beneficial for the organization. The IRT has to be highly skilled in decision-making and reacting to such complex situations and often requires decisions to be taken in only a few seconds.

Containment

When a network attack occurs on an open network, the attacker will be able to easily leverage his position to attack other hosts on the same network. Various attacks can be employed by an attacker on the internal network:

- ARP spoofing allows the attacker to view traffic between different hosts on the same physical network segment. Any clear text traffic such as passwords (e.g. HTTP basic authentication) or traffic (such as transfer of files through Windows network shares) can be viewed by making use of this attack. There are similar attacks to achieve the same kind of access – such as DNS spoofing or MAC address flooding.

- Passwords are frequently shared across different servers and services. Guessing one password means that the attacker gains access to various other accounts by the same user.

- Less secure servers are easily accessible once inside the internal network. These networks are generally friendlier than the Internet, and therefore the administrators might open up more services that would otherwise be closed on a server exposed to the Internet.

A good solution to the problems described, is to physically separate different networks and apply access control between different sections of the network. For example, if Department A does not need to access files by Department B, there is probably no need for both departments to be on the same physical network.

Employees and third parties sometimes need physical access to the network, for example to plug in their laptop, which might present a security problem. Personal laptops do not adhere to the same security policies that the company computers follow. For example, an employee's laptop or PDA might have computer viruses or Spyware software, which can transmit sensitive information or infect other computers on the same network.

Conclusion

It is easy to fall into the extremes of either believing that targeted cyber attacks rarely happen, or that it happens to you or your company all the time. The truth is that targeted cyber attacks are used to gain leverage in competitive areas, such as software development, or simply personal relationships. The more competitive advantage you have, the more frequent such attacks are going to be. Preventing these attacks is more of a matter of good risk management rather than simply buying a few products to prevent specific well known attacks. Budgets certainly have their importance in helping prevent targeted attacks against your company. However, it is more important to have good planning from the administration's part to effectively prevent targeted cyber attacks.

About GFI

GFI is a leading software developer that provides a single source for network administrators to address their network security, content security and messaging needs. With award-winning technology, an aggressive pricing strategy and a strong focus on small-to-medium sized businesses, GFI is able to satisfy the need for business continuity and productivity encountered by organizations on a global scale. Founded in 1992, GFI has offices in Malta, London, Raleigh, Hong Kong, and Adelaide which support more than 200,000 installations worldwide. GFI is a channel-focused company with over 10,000 partners throughout the world. GFI is also a Microsoft Gold Certified Partner. More information about GFI can be found at http://www.gfi.com.