[7]

DEFENDING THE DIGITAL YOU: HOW TO FIGHT ONLINE IDENTITY THEFT

Your very identity as a human being is increasingly intertwined with IT security. Your academic transcripts, driving record, credit history, employment background — they're all stored in easily hacked computers. Here's a look at the growing problem of identity theft, and how to combat it.

"THE INDIVIDUAL IS THE CENTRAL, RAREST, MOST PRECIOUS CAPITAL RESOURCE OF OUR SOCIETY."

- Peter Drucker

by TONY ALAGNA & HOWARD SCHMIDT

This book is devoted to bolstering corporate security, but what about defending your identity as an individual? Losing control of the data that defines your life — now that's the ultimate security dilemma.

But don't kid yourself: even if identity theft doesn't specifically happen

THE INTERNET IS THE 21ST CENTURY VERSION OF THE WILD WEST, A LAWLESS DODGE CITY WHERE HACKERS AND CRIMINALS STEAL FROM THE VULNERABLE AND THE UNSUSPECTING. INSTEAD OF NOTORIETY, THEFT IS THE NEW GOAL OF MOST CYBERCROOKS.

to you, everyone has a stake in halting the problem. Its occurrence incurs social costs and affects the corporate bottom line. For example, many companies maintain policies by which they reimburse individuals any money that is stolen from their banking or credit card accounts. These companies either eat the cost, or pass it along to all customers.

Online identity theft is defined as criminals using the Internet as a medium for stealing a user's private identifying credentials, often for the purpose of further theft or fraud. This thievery has been around as long as the Internet, but the nature of the threat has changed dramatically.

In the past, the biggest perceived threat was a precocious teenager taking down a major website like Yahoo, with a "distributed denial of service attack." Viruses were an act of vandalism, like graffiti. Malicious code and hacker attacks were about glory, vandalism and anarchy. They were typically created and deployed by isolated and random individuals.

In his cautionary book about technology, *The Greening of America,* Charles A. Reich wrote: "What we have is technology, organization, and administration out of control, running for their own sake...We have turned over to this system the control and direction of everything — the natural environment, our minds, our lives." When was this book published? In 1970! Imagine what Reich would say now, 35 years later.

Today, we have the Internet, and it's a far scarier place than it was as recently as five years ago. The Internet is the 21st century version of the Wild West, a lawless Dodge City where hackers and criminals steal from the vulnerable and the unsuspecting. Instead of notoriety, theft is the new

goal of most cybercrooks. Whether it's stealing intellectual property, corporate assets, money or identity, hacking is about robbing people.

The incidence of cybertheft has risen sharply. Exacerbating the problem is that more and more of these attacks are being perpetrated by organized crime. Many losses have been traced back to gangsters, even directly to the bank accounts of specific crime entities. It is believed that organized crime elements in Russia and Eastern Europe are behind a substantial percentage of Internet stealing. These days, Tony Soprano won't whack you; he'll hack you.

THE THREAT DEFINED

There are two general techniques by which consumers are being exploited. These techniques differ, but the goal of each is the same — to get consumer's usernames, passwords, identifying credentials or sensitive information. These two techniques are malicious code and phishing.

- **Malicious Code.** Malicious code is the worms, Trojan horses and viruses that often attack computer networks. Many of them are designed to steal. In 2003, about 78% of worms contain a backdoor which is built to listen to keystrokes, capture a screen, see what it is being logged onto, take over the system, and steal what it can. This trend continues to rise in 2004 while worms, Trojan horses, keystroke loggers and eavesdropping software are propagated all throughout the Internet. Many of these backdoors planted by worms over the past few years are still sitting on unsuspecting machines and stealing from its victim.

- **Phishing.** Worms and viruses are not new to the Internet user, although their ability to do harm and commit theft has increased substantially. Phishing, or spoof sites, are less well known, but no less dangerous. In conducting a phishing expedi-

Insider Notes: Get users to use more secure computing practices, such as not clicking on unknown email, running the latest antivirus software, using a personal firewall, and ensuring that the site is encrypted.

> tion, a spammer will send out millions of emails that look like they came from a legitimate source, usually a financial source or an ecommerce entity.

This email contains a misleading link or URL that takes the unsuspecting user to a web page that looks exactly like the login of the consumer's bank. When an unwitting "customer" enters in their username and password and "login" they either go nowhere, or, in more sophisticated scams, they are redirected back to the real site.

The goal of phishing is to trick the user into entering their username and password into a fake site that is being hosted from some random IP address. Mobsters can then capture this data and use it to accomplish several sinister things, such as steal directly, open up credit cards in consumer's names or buy merchandise online.

Unfortunately, forensics on the Internet is sometimes unclear. It is difficult to know what method was used when one specific individual has lost their identity or password, and current security products have limited scope.

IDENTITY THEFT'S IMPACT ON COMPANIES

The same type of attacks are being used against both individuals and companies. The plague of identity theft has impacted companies in two important ways. First, as alluded to above, most banks and financial institutions have what is referred to as a "make-whole" policy. This policy states that if money is stolen out of a customer's bank account, the bank will refund the money, often in full.

Since it is impractical for a bank to investigate every incident of theft, most have established a dollar amount under which it will provide a total refund with no questions asked. Unfortunately, information about these make-whole policies is beginning to become well known. Hacker sites have been found that list banks that have these make-whole policies along with the maximum theft amount that the banks will make good, "no questions asked." The result is that the hackers are enabled to rob banks with impunity.

In addition to these small, but unstoppable losses, phishing attacks have begun to erode confidence in online marketing channels. As more people get burned in these scams, trust in the Internet, as a legitimate channel of commerce, wanes. If people start distrusting their email, or the website that they are on, or, in the extreme sense, the Internet itself, it will create serious problems for companies relying on the Internet.

While this trend will have a critical impact on companies such as Lending Tree, Amazon.com and others that are pure Internet entities, the impact will be broad based since the Internet has proven to be a very cheap way to conduct business, especially within financial services. Banks want people to do business online because of how inexpensive it is to service them. However, this business relies heavily on customer's trust in this channel. Online identity theft impacts companies immediately, by stealing money from them. It also impacts them over time by eroding not only their brand, but the key thing that makes Internet commerce possible, trust in the channel.

THE TRADITIONAL BUSINESS RESPONSE

The traditional business response was to deny everything. This was not a "head-in-the-sand" policy, but one developed from witnessing the experience of others. There was a major "hack attack" against a large U.S. bank that the bank acknowledged. The immediate losses to the bank from the attack were not significant with respect to its size and were all made good. However, the publicity from this attack, whether fairly applied or not, labeled the bank as insecure and vulnerable. Its very largest customers began to leave because of this bad publicity. The policy adopted after that has been to deny and cover-up. In essence treat these attacks as PR problems with a PR solution.

A CHANGE IN RESPONSE

The traditional "head-in-the-sand" policies have begun to change. Some of this is in response to state and federal regulations that are forcing compa-

Insider Notes: Understand the problem and the types of attacks that are infiltrating your environment and plaguing your online customers. Realize their pervasiveness and the real danger that they pose.

ONCE AN IDENTITY IS STOLEN FROM THE I.T. ENVIRONMENT, ALL TYPES OF FRAUD CAN OCCUR, INCLUDING MASSIVE LOSSES IN CORPORATE INTELLECTUAL PROPERTY.

nies to disclose attacks such as these. But even more so, it's in response to the sheer number of attacks occurring. The growth of these attacks has followed an exponential curve over the past 18 months and is reaching epidemic proportions. Consumers are fed up and beginning to lose their enthusiasm for the Internet. Companies have finally begun to take this problem seriously and respond. Their first response has been to admit that there is a problem; their second is to explore new techniques and methodologies such as:

- **Education.** Get users to use more secure computing practices, such as not clicking on unknown email, running the latest antivirus software, using a personal firewall and ensuring that the site is encrypted. These commonly preached computing practices, even when perfectly followed, are only a step in the right direction, not a solution.
- **Organizational cooperation.** Companies, even arch competitors, are uniting in anti-phishing organizations to try to stop phishing and spoof sites. This includes looking out for what appears to be spoof sites and informing each other of their existence.
- **New technologies.** This includes old technologies being implemented in new ways, emerging hot fixes and brand new "shift the trend" technologies. Behavioral technologies are the future.

Another problem is that current best practices using existing security software is not good enough; they are still vulnerable against the new, evolving techniques that bad guys are using to fool people.

This appears, at first blush, to be a problem restricted to individual Internet users. However, the general adoption of advanced communication technologies and mobile computing by corporations has extended corporate networks beyond its perimeter firewall. Hence, the corporate network is no longer a contained LAN that can be defined and protected. Road warriors, telecommuters and contractors can access corporate resources

everywhere. This has made the corporate environment susceptible to what used to be user-based attacks. Once an identity is stolen from the IT environment, all types of fraud can occur, including massive losses in corporate Intellectual property.

TWOFOLD ACTION LIST

There are two key points that readers should take from this chapter. Understand the problem and the types of attacks that are infiltrating your environment and plaguing your online customers. Realize their pervasiveness and the real danger that they pose.

Identify what you are currently doing about these problems, and identify what else can be done. Determine how best to address these problems from both a policy and procedural recommendation as well as from a technology recommendation.

DEFINING MALICIOUS CODE

Probably the most important thing to know about malicious code definitions is that there is no clear agreement among experts about how to exactly define, name or categorize malicious code.

Take for example, four of the biggest malicious code outbreaks of 2004: MyDoom, Netsky, Bagel and Sobig. These pieces of "malware" were commonly called "worms," yet they are all mass mailer attacks — meaning they propagate through the email. A worm is classically defined as a type of malicious code that can propagate or infect machines without the user's help or needing the user to do anything. A virus, on the other hand, needed a user to take some type of action, like opening an email, for the virus to continue spread.

Many of the variants of these four big mass mailing outbreaks required the user to take some action, in some cases even opening an attachment. Why are these things called "worms," when they more closely fit the definition of

Insider Notes: Consider an infection by any "malware" tool to be a full invasion, because everything the infected machine does or has stored is sent back to the criminal.

a virus? I suspect a marketing decision somewhere decided "worm" would be the sexier word to describe many different types of malicious code attacks.

There also are conflicting definitions for the words Trojan and spyware. A Trojan is classically defined as malware that comes disguised as something else, which is an incredibly broad definition. Almost all malware comes disguised as something else, meaning that it won't have a name like HeyImavirus.exe. When malicious code experts use the word Trojan, they are generally referring to Remote Access Trojans, which are backdoor programs that give an attacker full access to the infected machine. Trojans are similar to commercial Remote Access utilities and have extreme takeover capabilities — e.g., accessing the file system, gaining full view of everything on the screen, capturing keystrokes, hijacking the mouse, turning on the victim's webcam or microphone and recording what is seen or heard.

Consider an infection by any "malware" tool to be a full invasion, because everything the infected machine does or has stored is sent back to the criminal. Spyware is again a broadly used word that can encompass many genres of malicious code, including adware, Trojans, keyloggers, dialers, browser hijackers, etc. Unfortunately, some vendors in this space like to include even relatively benign privacy violations such as cookies.

Cookies, in rare cases, can be harmful, but you should know that having a small amount of text gathered about a user's surfing habits pales in comparison to utilities such as Trojans that have stolen gigabytes of proprietary source code with disastrous consequences for the victimized corporation.

One more piece of definition confusion: a single piece of malicious code might have multiple names depending on who you talk to. Why would one individual worm have three names; Lovsan, MS Blast or Blaster? The answer is that the separate antivirus firms detect the worm at different times and sometimes in different parts of the world, and do not cooperate fully. Making matters worse, they pick up many more worms than make the headlines, and they cannot tell which handful will be the next big one. If they could, maybe naming for at least some percentage would become more standardized.

In the face of this lack of clarity, maybe it is more important to focus on the capabilities or attributes of the malicious code and how it can negatively affect your computing environment, as opposed to being hung up on a name or category. Attacks are blending many elements of different types of malcious code, and many outbreaks will not fit cleanly into one box or another.

BYPASSING ANTIVIRUS TECHNOLOGY

Bypassing antivirus (AV) is actually trivial for malicious code. Antivirus heuristics are generally ineffective against new types of malicious code. Most experts in the security community do not believe that antivirus has effective heuristics or effective behavioral technology because if it did, it wouldn't constantly need updates. That means, whenever a new worm, a new Trojan or a new piece of malicious code came out, the antivirus would not need an update to be able to detect it or clean it off your machine.

An effective behavioral solution should be able to detect new or modified malware even being years out of date. But antivirus is reactive. A virus breaks out, then, some time later, antivirus will be able to detect it, hopefully before infection gets to your machine.

Antivirus is signature-based technology. If antivirus were using effective behavioral techniques, they wouldn't be able to name the malicious code that they found either. The fact that they call a piece of malicious code "Blaster" means that a human looked at it, analyzed it, created a signature for it and named it. There is no program inside of antivirus that is doing some auto naming that gives it cute names like that.

In addition, if one of the antivirus companies had more effective heuristics or behavioral technology, they would broadcast it widely every time a new piece of malicious code came out. They would say how they protected

Insider Notes: Cookies, in rare cases, can be harmful, but you should know that having a small amount of text gathered about a user's surfing habits pales in comparison to utilities such as Trojans that have stolen gigabytes of proprietary source code with disastrous consequences for the victimized corporation.

their customers without needing an update at zero hour or zero minute or zero day (the first day that a malicious code comes out on the Internet). You do not see those types of press releases because it is not happening.

How does malicious code get around antivirus technologies from a "signature perspective?" Two ways:

❶ **Malicious code propagates faster than the antivirus infrastructure can handle.** The worm " SQLSlammer," for example, spread through the entire Internet and infected 90% of vulnerable systems in eight minutes. That is faster than the antivirus update infrastructure. Even if antivirus already has the signature for it and was trying to distribute that signature at the same exact time as the worm came out, the worm can actually propagate faster than antivirus can update its infrastructure. Worms and other malicious code have gotten too fast. Malicious code can move with more speed than an update because of their small size, exponential spread and push distribution.

❷ **Malicious code writers are well aware of antivirus programs.** Antivirus is everywhere. Up-to-date or not, almost every computer has either current antivirus or some type of remnants of old antivirus on it. So, antivirus is not a secret to malicious code writers who react to it in several ways. If they know that there is a known signature for their malicious code, they do simple modifications of their binary to bypass antivirus. They usually can bypass antivirus by modifying their binary by only a couple of bytes, which creates a variant.

There is a current worm that has 900 variants, because it is trivial to make a variant. Just open up the binary, take a hex editor, modify a few bytes, make sure that the thing still works, and then pop it back out to the "wild" and it's a new variant that antivirus hasn't seen and will not detect. Creating variants will eventually break the back of antivirus companies because they will not be able to forever keep up, as signature lists become impractical.

Another simple method of creating a variant is to use file compression technology. Antivirus firms try to make their signature-based systems accommodate popular file compression utilities, such as Winzip, and still

pick up malware obscured by these tools. However, if the malicious code writers use a compression utility that is less common and/or they password protect the compressed file, antivirus will again miss it.

Keep in mind, many types of malicious code are freely available for anyone to download off the Internet. Often, when malware is downloaded, it will state exactly which engines have been modified to bypass and test against. There are tools that even a novice can use to help modify malicious code to bypass antivirus. It is a trivial thing to accomplish, it takes five minutes, and the signature is changed. With access to the source code, it is even easier to change its signature because just adding a few dummy programming loops here and there will result in a different binary and a new variant of malicious code that existing antivirus signatures will not see.

ANTIVIRUS HEURISTICS

Antivirus does have a form of heuristics. What's meant by that is the AV software can look for smaller and smaller signatures. In theory, by signaturizing an entire file, the modification of just one binary byte would break that signature (depending on the brittleness of the signaturization system). To have more flexible signaturization, smaller signatures, dispersed across different parts of the binary, are required. This can potentially make modifying a variant slightly more difficult for the modifier and it may allow antivirus to pick up a variant of malicious code that is built by a kit.

For example, if the antivirus is looking for the string "I love beer" inside a piece of malicious code in the middle of the binary, the next variant that works slightly differently (but still has 'I love beer" in the middle of the binary) might be identified. That's because that key portion of the small signature is unchanged. In this way, a malware creation tool may leave signs

Insider Notes: Keep in mind, many types of malicious code are freely available for anyone to download off the Internet. Often, when malware is downloaded, it will state exactly which engines have been modified to bypass and test against. There are tools that even a novice can use to help modify malicious code to bypass antivirus.

that allow antivirus software to pick up variants that come from the same tool or "family," but only if those smaller signatures remain unchanged.

That is what antivirus means by heuristic. It is hoping that its smaller signatures remain throughout variants of malicious code.

Malicious code writers almost always modify the worm in such a way that it will bypass antivirus. In fact, it is often tested. In the "read me" sections of downloaded malicious code, it will state that it was tested against specific antivirus products with a certain signature database on a specific date and was not detected. If malicious code writers know about it, it is a trivial effort for them to bypass these signature-based antivirus technologies.

ATTACK SCENARIOS — ATTACKING THE LAN

Malicious code writers had to evolve their technologies since the mid-90s because most environments that they enter are now behind network address translations ("nat") or they are "natted" in some way either by a proxy, a router or a firewall. Even home computers often have a LAN and a private IP address. Malicious code writers realized that to communicate with the Internet they had to evolve from an old model that was based on the assumption that each machine had its own IP address on the Internet. In 1996, a machine infected with a piece of malicious code had its own address, so the code could just open up a port and listen, and anyone on the Internet could talk to that machine.

However, when computers were put behind a router or firewall, communication with any non-trusted computer was stopped. A computer behind a router, firewall or proxy has to talk out to a computer on the Internet; it has to initiate the first part of the communication. Therefore, listening is no good in that environment. Malicious code landing on a machine and listening doesn't matter because no machine will be able to talk to it unless they are also trusted behind the same firewall or on the same subnet.

Malicious code writers evolved their technology to be able to communicate within the limitations of this new environment. They developed a number of mechanisms to use to talk within this firewall and/or router

environment. One of the most popular is called reverse-connecting malicious code, or inside out connecting malicious code.

There is a piece of malicious code on the Internet called Beast — it is a reverse-connecting remote access Trojan. In some versions of Beast, its first order of business is to look in its registry for any proxy setting that it might have. Proxy settings are there almost always (if the proxy has ever been successfully logged-into at all, then that data will be there). The malicious code grabs these proxy settings, and then injects inside of Internet Explorer where it will initiate its connection sequence outbound, out to the Internet, and it will do it in an encrypted channel.

Through this process, the malicious code is "trusted" by the corporate firewall, the corporate proxy and the corporate routers. It is allowed to talk to whatever machine it wants, because it initiated the connection sequence outbound. The hacker may hard code an IP address or server (often an IRC server) that it wants this malicious code to talk back to as to obscure the originator of the infection.

EMBEDDING MALICIOUS CODE — BEATING THE FIREWALL

Using embedded code is a hacker technique that has existed for some time but has seen an upswing in popularity with recent malware, such as the MyDoom worm. Originally used to provide stealth capability (avoid being listed in Task Manager, for example), embedded code also gives an important advantage to malware: inheriting the credentials of the host (infected) process. This is particularly effective for bypassing personal firewalls. Be

Insider Notes: Using embedded code is a hacker technique that has existed for some time but has seen an upswing in popularity with recent malware, such as the MyDoom worm. Originally used to provide stealth capability (avoid being listed in Task Manager, for example), embedded code also gives an important advantage to malware: inheriting the credentials of the host (infected) process. This is particularly effective for bypassing personal firewalls. Be aware of the fact that Internet Explorer is a popular target host for malware, because it is almost always excluded from restrictions in personal firewalls.

IF EMBEDDING MALICIOUS CODE ATTACKS A SYSTEM WITH A PERSONAL FIREWALL, THE SYSTEM WILL FUNCTION FINE AND THE VICTIM WILL NOT KNOW THAT ANYTHING SUSPICIOUS HAPPENED ON THE MACHINE.

aware of the fact that Internet Explorer is a popular target host for malware, because it is almost always excluded from restrictions in personal firewalls.

In general, "embedded code" refers to an executable component infecting an already running, valid, process. There are numerous techniques for getting this done; some examples are using Windows Hooks (coaxing the OS to do the code injection), using CreateRemoteThread (a more direct approach), and there are also a plethora of spots in the registry listing components where an application should load automatically (legitimately intended for plugins and extensions).

There are also some more covert mechanisms, such as directly allocating memory in another process and stimulating code execution therein. When these techniques are used, the embedded code is part of the host process, rather than being a distinct process of its own. This avoids being visible to the end-user, as mentioned before, but also since credentials (for doing things like accessing the Internet) are done at a process-level, it means the embedded component will now be able to perform actions in the same manner as its host.

As I stated, Explorer is a vulnerable target, because it tends to be excluded from personal firewall restrictions. Ostensibly, this is because the user experience would be damaged by having to approve every network action, since IE is obviously network-intensive.

This carte blanche to use the network is precisely what is desirable. By effectively becoming part of Internet Explorer, almost any action can be done without scrutiny. The user has a disincentive to use aggressive checks with IE because it would render IE unusable. Moreover, how does even the human know which network actions are needed for the normal functioning of IE, versus ones that are possibly malicious in intent?

Internet Explorer has an additional advantage in that it provides numerous extensibility hooks that can be exploited to get malicious code running within it easily. The Windows shell, Explorer, is also popular for the same reasons, but to a lesser extent.

The embedded code technique is particularly effective against personal firewalls, when combined with the reverse-connecting technique. Since restrictions are even more relaxed for outbound connections, this technique is effective against even dedicated (hardware) firewalls in addition to personal (software) firewalls.

It's useful to realize that the embedded code technique does not alter the binary image of the host process, so it is not useful to apply signatures there. Signatures could be used against loaded DLLs, however this is not a general technique, since malware can also embed itself into the host without being a file-based entity at all.

Simply put, personal firewalls prompt the user when an application requires network usage, therefore making it suspicious to the user. Using embedding techniques, malicious code can hide inside an application that has already been approved or trusted by the firewall. When malicious code embeds in these trusted applications, it can perform any network connectivity operation without the user being alerted. If embedding malicious code attacks a system with a personal firewall, the system will function fine and the victim will not know that anything suspicious happened on the machine.

THE ANATOMY OF AN ATTACK

Trojans can be distributed in a myriad of ways: inside a worm that infects one million machines; insertion into a macro of a Word document and emailed out to 2,000 corporate users; insertion into an MP3 that takes advantage of the player vulnerability on a machine; or posted on a Napster

Insider Notes: Trojans can be scripted to do many nefarious things. They can look for credit card numbers, for mother's maiden names, or for specific information, such as a company name, and target that company by tracking all visits to that company's internal websites.

FROM A CORPORATE DEFENSIVE PERSPECTIVE, NO MATTER WHAT TYPE OF "BEST PRACTICE" DEFENSE IS THROWN AT IT, THE MALICIOUS CODE WILL STILL BE ABLE TO COMMUNICATE JUST FINE.

file sharing networks for 50,000 downloads. Wherever or however the endpoint is infected, a Trojan has compromised the system and it is talking back to this central place, which is likely to be an IRC chat server that is already set up. Trojans can be scripted to do many nefarious things. They can look for credit card numbers, for mother's maiden name, or for specific information, such as a company name, and target that company by tracking all visits to that company's internal websites.

The only ways that Trojans can be contained from a defensive point of view are somewhat unrealistic — e.g., not to allow any network connectivity. If users can access www.myfavoritesearchpage.com, they can see the Internet, and so can the malicious code. From a corporate defensive perspective, no matter what type of "best practice" defense is thrown at it, the malicious code will still be able to communicate just fine. It will bypass gateway antivirus, by being a variant; it will bypass desktop antivirus, by being a variant; it will bypass desktop firewalls, by injecting itself or tricking the user; it will bypass a corporate proxy, by grabbing the password settings; it will bypass network based intrusion detection, by using custom protocols and encryption and rendering itself invisible to intrusion detection techniques. It will bypass corporate firewalls and corporate routers by initiating its connection sequence outbound. So it doesn't matter what defensive layers are thrown at these things. Normal readily downloadable off-the-Internet malicious code can bypass every available endpoint protection mechanism as well as every best practice corporate defense mechanisms.

ATTACK SCENARIOS: THE UNMANAGED ENVIRONMENT

There are many different types of remote access solutions for mobile employees. There is SSL VPN, which is a web-based VPN device. There are also different types of webmail as well as Outlook Web Access. Also, some bigger companies like Citrix have secure gateways. Classic IPsec

VPNs, as well as different types of portals and intranets and extranets, can also be used for mobile computing.

The quality that all remote access has in common, regardless of the method used, is that it is an endpoint machine and is as vulnerable as any other system on the Internet. In some cases, they are managed machines — a corporate issued asset that is managed by the corporate IT that has all of the corporate security provisioned security programs.

Corporate resources can now be accessed from anywhere, with most places far from trustworthy. The danger here is extreme, because mobile computing environments plug into random places and in unmanaged systems. Vendors are aware of this security threat, and they're increasingly recommending the deployment of different types of security and scanning technologies. The problem is that most security technologies are not readily deployable. Antivirus is a very large application, so it is not practical to have anyone who is logging-in remotely to download this software and then scan the hard drive for half an hour before they can access email. Antivirus-type technologies in the "unmanaged space" must be behavioral, small, fast and transactional. Some are emerging in the marketplace.

However, the vulnerability in this mobile communication model is obvious. Besides the general threat of malicious code, these machines have no physical access restrictions. Anybody can load whatever they want on it (the risk of a keystroke-logger, regardless of whether it has network connectivity, is huge). A person can walk up five minutes before it was used and five minutes after it was used and capture everything that was done on that machine between those two time points.

Insider Notes: Corporate resources can now be accessed from anywhere, with most places far from trustworthy. The danger here is extreme, because mobile computing environments plug into random places and in unmanaged systems. Vendors are aware of this security threat and they're increasingly recommending the deployment of different types of security and scanning technologies.

The threat of malicious code is even greater in this unmanaged machine space. Sometimes the people using IPsec VPNs feel safe because this technology prevents split-tunneling (the ability for two or more applications to be communicating simultaneously while the VPN connection is going). Preventing split-tunneling only creates an illusion of safety.

A reverse-connecting Trojan functions in the same way in this environment as it does in a corporate environment, by initiating its connection sequence inside out. So, if users can see the Internet, then so can the malicious code. Even without Internet access, malicious code can be scripted to steal or perform actions whenever it comes back online. Malicious code is basically winning in every environment regardless of the situational defenses. All situational defenses can do is minimize the types of attacks; it cannot stop attacks.

STOPPING WORMS — IS PATCHING THE ANSWER?

A general definition of a worm is that it self-propagates. Historically, with viruses, the user had to do something, such as open an attachment, to be infected. Worms just infect and keep propagating without the user's help. Nowadays, worms and viruses are blended — they can share traits. Any way that a file can get on a machine, so can malicious code.

There is a false notion that patch management — compliance techniques — can immunize against malicious code attacks. This is not true. There are many different infection vectors for worms that have nothing to do with vulnerabilities and patches. Malicious code can thrive even in a fully patched environment. Patch management is a "band-aid," not a fix.

A mass mailer worm does not have to use any vulnerability to attack a system. MyDoom was one of the more widespread worms of 2004, yet it required no vulnerabilities. Getting an email with an attachment is not a violation of any vulnerability on the system.

Because of the flexibility of the operating system, many of the things that malicious code does are completely normal and within the range of the rules of the operating system. Trojans, spyware and keyloggers almost never need vulnerabilities to perform their nefarious activities.

In addition, the time between vulnerability identification and the introduction of a worm that takes advantage of that vulnerability is decreasing rapidly. A development period that took 60 days from announcement to worm, now takes nine days. There are also worms that use zero day or unreleased vulnerabilities.

PHISHING

Phishing is the act of using spoofed sites to trick Internet users into thinking they are on a legitimate site so that they provide login, credit card, or other important personal identity items. A spoof or phish site is usually a good copy of a legitimate site.

Users are lead to this site by an email that is often mass mailed to millions of users, which is spam for the purpose of phishing. This email also will resemble a well known company and declare that the users must go to that site for some important reason such as "we need to verify your information." Large financial institutions have been a visible and often hit target because of both their large Internet presence and abundant theft possibilities.

Phishing is a quick-hit scam operation. Some users identify it for what it is and report the site. A spoof site is usually shut down within 12 hours after it is discovered by the victimized corporation, but that is usually sufficient time to collect enough personal data from unwitting users to be profitable. Also, phishing scams can utilize hundreds of sites at once so that its lifecycle is greatly enhanced. These scams often utilize the free web hosting services provided by many ISPs, and they are recently attracted to foreign ISPs. The foreign ISPs are sometimes not as responsive to spoofing complaints and tend to keep the site alive longer and provide less help in efforts to catch the perpetrators.

Insider Notes: There is a false notion that patch management – compliance techniques – can immunize against malicious code attacks. This is not true. There are many different infection vectors for worms that have nothing to do with vulnerabilities and patches. Malicious code can thrive even in a fully patched environment. Patch management is a "band-aid," not a fix.

The lure that Phishers use to trick users is referred to as a "ruse." These ruses fall under two categories; the victim needs to come to the site for something good, or the victim needs to come to the site to prevent something bad. The positive ruses are less common and include messages like "click to register for your prize" and "you have pictures, click to view them." Much more common are the negative ruses that have themes around an urgency to verify account data before the account is closed.

THE PERFECT CRIME?

Tracing the criminals behind these spoof sites is extremely difficult, because there is so little information left behind. The free hosting sites require no identification, nor do the hotmail email addresses. The FBI, which is extremely concerned with this activity, can only follow them by following the dollars. They cannot actually stop the scam itself. The FBI and other federal agencies have not been very effective in tracking these people down; they almost always get away, so there is not a strong deterrent against running this scam. Some of the paths traced from spoofing have pointed to Russian organized crime.

CAN SPAM FILTERS HELP?

People who feel that they are protected because they have a spam filter are grossly mistaken. There are a number of techniques used by phishing scams to get around and through spam filters. Some of these include: encoding, encrypting, dynamic frames and redirection. In redirection, the phisher creates an empty page with a link to the phish page. All of this is transparent to the end-user.

Another popular technique is to create a link that is not a spoof site, or sending misleading URLs. A misleading URL can be an address embedded in a descriptive field, using HTML text that sounds similar to the target URL (Citi-Bank), or using obscure URL formatting that includes the target's name (citi.bank.com@geocity.com/updateyouraccount). An end-user that clicks on this page will be taken to a phish site.

However, this is a very large vulnerability. As spam filter technology improves, so will the technology of the phisher. The higher the level of defense, the more the problem proliferates. In essence, this is an Internet

con which is based on social engineering and end-user general naiveté. It is unlikely that spam will ever cease to be a problem as every proposed counter measure has immediate weaknesses, and in some cases those weaknesses have even been demonstrated. Spam filters of today have a heavy reliance on text analysis, which can be defeated by either encoding HTML messages or basing the entire message in graphics. There are no existing Artificial Intelligence engines good enough to reliably decipher what is contained in an image-only message.

THE NEW PHISHING TECHNOLOGIES

Phishing has evolved as rapidly as the techniques used to attack it. Spoofers now use frames, pop-ups, and more technical implementations. In addition, they have become more knowledgeable. They now steal legitimate marketing lists from a target and use that to "validate" a phishing attack and improve the odds in their favor.

For example, an end user that has just signed up with a bank would be more susceptible to a "request" from that bank to verify information. Increased knowledge about a target improves the effectiveness of phishing attacks.

Spoofers are now also utilizing pictures and messages that are difficult to distinguish from those from legitimate sources. They have also begun to use instant messaging as a medium to get users to spoof sites, which is referred to as "spim." Finally, new tool kits are now readily available to help the spoofer wannabe build fake websites. However, the majority of spoof sites are still unsophisticated.

BLENDED ATTACKS

Increasingly, phishers are combining malicious code with their phish pages. Up to 10% of the recent phishing attacks were found to have a malicious code component. Remember the goal is always theft. Thus, the people the bad guys can't trick into giving away their information could

Insider Notes: To stop phishing, a behavioral approach must be employed. Using behavioral technologies that are installed locally on the machine, like a toolbar, will catch the attack in real time and block it.

THREAT TO GLOBAL EMAIL SYSTEM AND BANKS GROWING

By Stephen Lange Ranzini

Junk email is becoming a global menace.

According to data released at a recent meeting of the Organization of Economic Coordination and Development (OECD), the global cost of junk email messages was estimated to be $200 billion in 2004, while the number of junk messages exceeded 3 trillion, roughly triple the number in 2003.

Mark Sunner, Chief Technology Officer of MessageLabs, a global outsourced hoster of email services for large businesses which handles 70 million emails for its clients per day, released data at the OECD meeting that indicates in July, 2004, fully 94.5% of all email globally was junk email.

MessageLabs data also indicates that between 1 in 10 and 1 in 14 of all emails globally are viruses. More ominously, MessageLabs indicates that every virus launched this year has a zombie network backdoor, or "Remote Access Trojan" (RAT). Once activated, a RAT allows malicious spammers to seize control of compromised PCs and load key-logging devices to detect passwords and user ids typed by PC users. The latest version of RATs also are enabled with software that allows the nefarious criminal minds that control the RATs to load additional software to compromised PCs, creating networks of zombie PCs called Zombie Bot Networks.

MessageLabs' Sunner also asserted that one major ISP informed him that 30% of all users are harboring Remote Access Trojans. This would mean that 200 million PCs globally (30% of the 665 million global email users) are controlled by Remote Access Trojans. Potentially up to 30% of all PC users who use Internet banking are also compromised.

Several experts at the OECD meeting indicated that they were quite impressed by the technical quality of these Next Generation RATs. The newer Remote Access Trojan key-loggers are down to just 2 kilobytes in

size. They are being placed not just in malicious junk emails but on compromised websites and even innocent looking websites that offer brand name products at low prices.

A recent example purported to sell bicycles cheaply, and had a high placement in Google price-based searches as a result. It is not recommended that consumers use any website that is not fully trusted. However, even trusted names may be compromised. ICANN, the rules making body of the Internet, recently changed domain transfer rules to eliminate the requirement that changes of domain registration must be confirmed with the domain administrator of record. German hackers used this vulnerability recently to take over the German eBay website. If consumers become widely aware of these threats, they are likely to discontinue use of search engines such as Google or Yahoo to shop online or to search online for useful information. Linking to an untrusted website from a search engine is also not recommended. This will greatly reduce the value of the Internet to all users.

Enrique Salem, SVP Network & Gateway Security Solutions of Symantec, one of the leading virus and junk email blocking technology vendors, estimates that a majority of all junk email is generated through these Zombie Bot Networks or open relays. When compromised, each zombie PC in a Zombie Bot Network turns into an open relay. The value of a compromised zombie PC grows dramatically if it is connected to a high-speed Internet network such as a broadband network. Therefore, cheap broadband Internet access is driving the growth of junk email, theft and the utility of Zombie Bot Networks. Microsoft has formed a working group to try to combat these Zombie Bot Networks, but faces an uphill battle.

Symantec's Salem estimates that the typical spammer generates 200 million junk email messages per day and only requires 400 purchases at $20 each to generate the $8,000 in revenue required to break-even on a commercial offering.

However, we note that the value of a stolen credit card number using a trojan key logger averages $100 in the black market, so only 80 credit

cards need to be stolen each day to generate a profit for the malicious spammer. Each identity theft can cause between $2,000 and $10,000 in losses to consumers and banks. We postulate that the theft of an entire online identity via RATs could be worth $500 to $1,000 on the black market. Therefore, a RAT-based identity theft would only need just 8 to 16 per day to generate a profit for the malicious spammer.

WHAT CAN BANKS AND CORPORATIONS DO NOW?

For companies, internal misuse of corporate networks by employees to generate junk email is also on the rise. To determine if your network is a source of junk email, register with America Online's free Complaint Feedback Loop tool at http://postmaster.aol.com. Besides keeping up with the latest required patches, which is admittedly a near impossible task due to the frequency with which they are released, corporate users should ensure that email server programs typically used are up-to-date.

For example, Sendmail version 8.9 or later is required to block open relay attacks. Corporate users should also ensure that Port 25 is always closed (this prevents a corporate email network from becoming an open proxy, which is highly sought after by spammers because it allows them to send junk email from your corporate server).

Spammers don't believe that they will be caught, they believe that they will get off even if they are caught, and can cover their tracks very effectively due to the security holes in the underlying architecture of the Internet. A new paradigm to rescue the global email system is urgently required.

The author is President of University Bank, Ann Arbor, Michigan. He is also the U.S. delegate to the United Nations global standard setting body for the financial services industry, UN CEFACT TBG 5 (Finance) and a member of the Security Committee of the Financial Services Technology Consortium, the R&D collaborative of the nation's largest banks.

still be victims of a keylogger or Trojan attack. Recent browser vulnerabilities have made Trojans a strong weapon for the phishers, because some vulnerabilities will allow malicious code to be planted just by the act of browsing to the phish site.

WHAT CAN COMPANIES DO?

The Internet is too highly a profitable way to conduct business for companies to give up on it. They have responded to these attacks as best they can. Many have established an incidental response team within their organization. When they are attacked, they can at least analyze the site itself, work with the ISP to shut it down and contact the FBI. Typically they can do little more. Attacks not only are common, but they are fast. By the time that a company reacts to shut it down, it has already accomplished its goals and identities have been compromised.

One important tool in this campaign against phishing is based on the fact that a website is copyrighted. Therefore, a spoof site does infringe on copyright laws. This allows legal action to be taken against the person managing the site and is referred to as a Digital Millennium Copyright Act (DMCA) complaint.

There are also anti-phishing organizations. Financial Services Technology Consortium (FSTC) is a group of banks focused on stopping phishing for the financial services industry. There also is antiphishing.org, which sponsors anti-phishing working groups of vendors and customers who get together to develop standards and techniques to fight this problem.

A promising approach is a behavioral technology that can detect phish sites as soon as the user encounters them and then blocks them real time. One such technology is currently used inside of eBay's Account Guard, which is a part of its toolbar.

The industry will also have a new powerful tool at its disposal, and it is called the Phish Reporting Network. This site is a place where companies who are victims of phish attacks can submit sites and large ISP's can block these sites. Blocking sites wherever possible and as soon as possible is important because shutting sites down is just not fast enough.

Unfortunately, protecting against phishing attacks often comes down to having the most sophisticated defense, so that spoofers will attack and steal from another target. Phishing attacks are technologically simple for crimi-

nals to carry out, so it would be unwise for a company to be considered the "low hanging fruit."

It has been said that some of the most successful businesses on the Internet simply applied a tried-and-true business model and created an online version of it. Unfortunately, age-old crimes also seem to be gaining success with the help of the Internet. The bad guys are using the Internet to steal, and quite frankly they are, for the most part, getting away with it. The current defenses do little to prevent the techniques used to commit online identity theft.

Malicious code is a powerful weapon for criminals. Everyday, there are more and more computers with antivirus software loaded and updated, fully patched operating systems, and firewalls built straight into the OS, but the attacks only increase. Malicious code writers can defeat all of our current countermeasures. Catching malicious code with signatures is too late; they have already spread around the world and done their damage.

Phishing attacks are at their root an almost laughably simple trick. Fake an email and fake a website and, sure enough, some users will hand over their credit card number and then some. The fact is that phishing works, and the phishers are evolving their techniques real time to be more advanced and harder to stop. Companies trying to battle the problem are finding that they have a tough place to start — they don't know how many phish sites are out there trying to victimize their customers. Some analysis of this problem has showed that there are three times as many sites out there as are being found. Shutting these sites down after they are found is too late; they have already done their damage.

THE ANTI-FRAUD TOOL OF THE FUTURE

The only way these problems can be solved is with effective behavioral technology. Using behavioral technology on new or modified malicious code will stop the attack from ever doing damage to the local machine or allowing it to propagate to others.

Behavioral technologies can be fast and small, because they don't have the weight of a large signature list slowing down their scan times and bulking

up their file size. To stop phishing, a behavioral approach must be employed. Using behavioral technologies that are installed locally on the machine, like a toolbar, will catch the attack in real time and block it. As distribution of these types of tools increase, the number of sites found and shutdown will increase dramatically.

Behavioral approaches are the future.

■ ■ ■

As the Chief Technical Officer and Founder of WholeSecurity, Tony is the visionary behind the patent-pending behavioral technologies that drive the company's endpoint security solutions. He is considered an expert in information security and specializes in the areas of malicious code and phishing. In recognition of his contributions to the security industry, Tony was recently named Information Technologist of the Year by the Austin Chapter of the Association of Information Technology Professionals (AITP) and he serves as a member of the InfoWorld CTO Network. As a sought after public speaker, Tony often addresses executive forums, speaks at security events and serves on conference panels. He actively advises lawmakers, industry analysts, financial organizations and corporations on cyber-threats and how to defend against them.

Tony can be reached at 512-874-7451 or tony.alagna@wholesecurity.com.

Howard A. Schmidt has recently joined eBay as Vice President and Chief Information Security Officer. He retired from the federal government after 31 years of public service. He was appointed by President Bush as the Vice Chair of the President's Critical Infrastructure Protection Board and as the Special Adviser for Cyberspace Security for the White House in December, 2001. Prior to the White House, Howard was Chief Security Officer for Microsoft Corp., where his duties included CISO, CSO and overseeing the Security Strategies Group.