FISSEA Contest 2007

Name: K Rudolph

Organization: Native Intelligence, Inc.

Address: POB 144

Glenelg, MD 21737

Phone: 410 531-1396

Email: kaie@nativeintelligence.com

Type of entry: Newsletter

Title of Entry: Security Awareness Newsletter

Description of entry: (next page)

Description of entry:

Two issues of a monthly newsletter distributed in electronic format (PDF). The first newsletter suits the FISSEA Conference theme because it's an annual "looking forward" issue.

By design, the four-page newsletters print well in both color and black and white. Regular columns include "Fast Facts" and "Grill Your Security Officer." Issues that address specific topics, e.g., Mobile Devices, also include a "What You Can Do" column that provides practical actions for protecting assets.

As part of a unified security awareness program, newsletter topics are chosen to coordinate with modules in e-learning awareness courses. Topics can be changed or new ones created to quickly meet special needs such as a breach or new requirement.

Native Intelligence, Inc.

JANUARY 2007

Inside

◆◆◆

onGuard
is published monthly by Native Intelligence, Inc.
www.nativeintelligence.com

Direct inquiries and correspondence to: onguard@nativeintelligence.com

onGuard

Security Awareness and Education in OUR Workplace

What's on the Horizon... 2007 IT Security Projections

Near the end of the year, management asks for projections for the next year. Security specialists look at past and current events to identify trends and changes in attacks and targets. This newsletter presents our best guesses on what to expect in 2007.

In 2007, attacks to steal money will continue. Attacks will be smarter and better organized. The market for malicious computer software (called "malware") and data about computer program weaknesses will continue to grow. Reports from U.S. government and industry analysts show that organized criminals are hiring hackers to break into computer systems and steal information.

THREATS

Changes in Attacks

Originally, attackers were mostly high-school loners who broke into computer systems to learn about them. This group grew to include loosely organized clubs with members who wanted to impress their peers. In 2006, attackers were more interested in money. News stories about phishing (tricking people into giving private information), identity theft, and the loss of personal information show that money-based attacks are on the rise.

Rise of Botnets

There will be more stealth software (programs hidden on computers that make the computers carry out tasks in secret). A computer with this kind of program has been "hijacked" because it is doing things that the owner doesn't know about. These computers are called zombies. Computer owners usually don't know that their machines have been hijacked. The computers work, but not as well as before. When

(see What's on the Horizon, page 2)

« page 1

What's on the Horizon

many of these hijacked, or zombie, computers are working together, they are called "Bot networks," or "botnets."

Security company CipherTrust reported that more than 180,000 PCs are turned into zombies every day. This number will rise in 2007. Unwanted spam e-mail will continue to be the main way that criminals put botnet programs on computers.

New Phishing Spots

Like other forms of dangerous software, phishing attacks will be sneakier. Security company Trend Micro described a recent attack in Germany that looked like it came from an electricity company. E-mails asked recipients to check their electric bills by clicking on an attached PDF document, which is how the real electricity company operates. The attachment had a suffix of ".pdf.exe" – that is, it had two suffixes. When victims opened the attachment, the attached program put Trojan horse software on their machines. This software watched the Internet connections, including when the victims browsed to Web pages and banks. The software then sent this information to the criminals. The attackers didn't even need a fake server – the hacked computers did the work.

Security company F-Secure believes that phishers will crack the one-time passwords that many banks are using to protect access to bank accounts. In one scheme, an account holder has a printed list of authorization codes sent by the bank. The attack fools the victim into logging into a fake bank, which asks for the victim's code. If the victim provides the code, the fake bank uses it to log into the real bank and take money out of the user's account.

More people in larger countries are aware of phishing attacks. As a result, attackers are choosing targets from smaller countries. Attackers are using languages such as Greek, Czech, and Finnish.

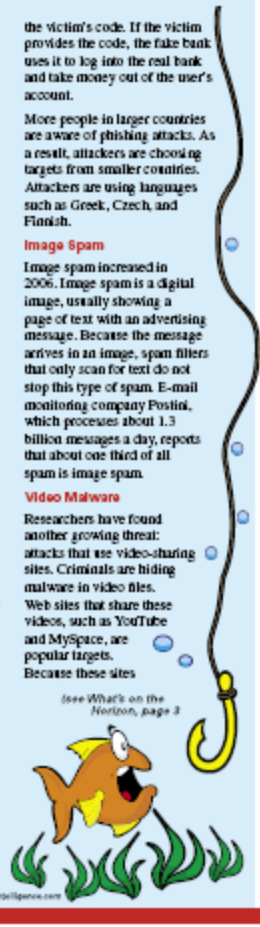
Image Spam

Image spam increased in 2006. Image spam is a digital image, usually showing a page of text with an advertising message. Because the message arrives in an image, spam filters that only scan for text do not stop this type of spam. E-mail monitoring company Postini, which processes about 1.3 billion messages a day, reports that about one third of all spam is image spam.

Video Malware

Researchers have found another growing threat: attacks that use video-sharing sites. Criminals are hiding malware in video files. Web sites that share these videos, such as YouTube and MySpace, are popular targets. Because these sites

(see What's on the Horizon, page 3



FAST FACTS!

- In 2006, a 20-year-old programmer put Trojan horse software on the systems at the China Lake Naval Facility in California. The programmer used the secretly-installed software to make the computers in the facility's network send spam and infected software to computers around the world. He also used the facility's network computers to make money by generating hits on Web sites where advertisers are paid based on the page visits. He received $60,000 before he was caught. During this time, his programs controlled more than 400,000 computers.
- Russian hackers using a 70,000-computer botnet caused a recent increase in e-mail spam that advertises penny stocks and organ enlargement pills. These hijacked computers were located in more than 160 countries.
- Phishers are starting and stopping fraudulent Web sites in a shorter time frame. This makes it harder to find and stop the attacks. The average life span of a phishing site was roughly one hour in 2006, compared to about one week in 2004. *Source: Gartner Group*
- Web users have lost $2.8 billion to phishing attempts since the attacks started several years ago. *Source: Gartner Group*

Native Intelligence, Inc.

GRILL YOUR SECURITY OFFICER

What is a CAPTCHA?

It's a Completely Automated Public Turing test to tell Computers and Humans Apart. CAPTCHAs are used on the Web to prove that a human made a request. Many CAPTCHAs display an image with distorted letters that automated Web programs can't read. Humans can see and enter the letters. CAPTCHAs prevent Internet bots (automated applications) from collecting sensitive information, registering for free email accounts (to send spam), and collecting email addresses. CAPTCHAs prevent bot-generated spam by making unknown senders pass a test before their email is delivered. Below is an example of CAPTCHA. Humans can read the word "secure" below, while computers will have difficulty deciphering the word.

Want to grill us on security issues?...

Send questions to: grill@nativeintelligence.com

from page 2

What's on the Horizon...

are so popular, malware infections spread very rapidly.

Mobile Phone Malware

Malware that attacks mobile phones will increase. F-Secure has found 179 cell phone viruses, and estimates that tens of thousands of handsets are infected. F-Secure recently detected the first malicious Java software on a cell phone. Infected Java programs could affect most mobile phone handsets, not just the high-end models. In 2006, a mobile phone attack spread by Trojan horse software caused infected cell phones to call a premium rate number in Russia. The criminal programmer received five euros ($6.04) for each call.

Other Cyber Threats

State-sponsored attacks (where governments pay other people to attack) and terrorist cyber attacks may increase. In 2006, attacks that disrupted business activity or went after trade secrets rose. Cyber terrorism and state-sponsored attacks can last longer, and use more resources, than other attacks. An attacker with enough time and money can breach any security system.

Individual attackers often have lower resources compared with the time and energy that terrorists are willing to use. Some political groups will do whatever it takes to publicize their causes. State-sponsored attacks may use more resources than a single company can spend to defend itself.

TARGETS

Wealthy Individuals – Gartner reports that wealthy PC users are now the preferred targets of online fraud. A survey of 5,000 consumers in the United States revealed more phishing attacks than ever before. The survey also found that the average loss per victim has grown from $257 to $1,244 in 2006. Scammers pay marketers for lists of rich customers. Criminals may target high-income users more often because high-income users make more online transactions than low-income users (e.g., using financial services, trading systems, and e-commerce). Phishers also use complex social engineering schemes to scam well-to-do targets. For example, in one scam, phishers find the screen names of eBay users who bid on, but didn't win, auctions for expensive furniture or cars. The phishers send the targets false offers of second chances to buy the items. If the victims respond, the phishers steal the victims' deposits.

Surveyed adults who earned more than $100,000 per year received an average of 112 phishing e-mails during the last 12 months. The per person average across all income brackets was 74 e-mails. Also, high-income adults lost an average of $4,362 to phishing schemes, nearly four times more than other victims.

Online Companies and Retailers – Attacks that impersonate bank Web sites have slowed. Attacks against Web companies such as eBay, PayPal, and online retailers are rising.

Money Mules – Phishing and identity theft attacks include an important offline component: the "money mules" used to launder the stolen money. Without the money mules, thieves can't profit from stolen credit card information. Once a thief has access to a victim's credit card and bank log-in details, the thief needs a person (the mule) in the same country as the victim to handle money transfers or to reship items to the thief.

(see What's on the Horizon, page 4)

from page 3

What's on the Horizon...

To recruit money mules, thieves contact prospective victims (mostly in the US, the United Kingdom and Australia) with job vacancy ads. The ads are distributed via spam, Internet chat rooms, job search Web sites such as Craigslist, and well-designed Web sites run by the thieves. The ads offer stay-at-home positions such as "shipping manager," "private financial receiver," or "sales representative."

The crime rings may ask the mules to sign official-looking employment contracts. Once hired, the money mules receive stolen funds into their accounts. The criminals then ask the money mules to take these funds out of their accounts and forward them overseas (minus a commission payment), normally using a wire transfer service. In some cases, the criminals tell the money mules to open multiple accounts with the same bank as the identity theft victim. Criminals may try to avoid detection by using several accounts in multiple banks to make small transfers.

Acting as a mule is illegal. When law enforcement catches up with the money mules, the money mules often have their bank accounts suspended, and some have been arrested. *Source: Bank Safe Online*

People with Health Insurance – Medical identity theft is a growing concern, and one with potentially life-threatening consequences. Medical identity theft occurs when a thief uses a victim's name and other parts of the victim's identity (e.g., insurance information) without the victim's knowledge or consent.

Thieves use this information to make false claims for medical services or goods. Medical identity theft often results in incorrect entries in existing medical records (e.g., a change in blood type, allergies, or diagnosis). Medical identity theft can also result in made-up medical records in the victim's name. Be cautious of free medical exams, co-payment waivers, or advertisements stating "covered by insurance." A health insurance card is often at least as valuable as a credit card. Criminals that find or steal insurance cards may use them to get healthcare services and drugs. Worse, it can be nearly impossible for the victim to remove false records from his or her medical history.

OTHER PROJECTIONS

Firms will take more responsibility for their customers' PC security. Some companies already offer toolbars to block phishing attacks. Banks are introducing two-factor authentication for accessing financial records online. In 2005, the Federal Deposit Insurance Corp. (FDIC) recommended that banks help consumers protect their PCs from spyware. *Source: FDIC*

Spam will continue to be a problem, because it works. In 2005, the Return on Investment (ROI) for e-mail marketing was $57.25 for every dollar spent. The ROI for all non-e-mail-related online marketing was $22.52. *Source: Peer 360/360 review*

In the US, starting in 2007, Daylight Savings Time (DST) will begin earlier and end later. DST will start on the second Sunday in March and end on the first Sunday in November. These changes in DST will require updates to Windows operating systems and Sun's Java Runtime Environment (JRE). Servers, desktops, laptops, palmtops, and all other Windows platforms will need updates by March 2007. Like Windows, Sun's JRE has its own built-in time calculation. With JRE, however, there is no easy way to create an update that can be applied to any version of the JRE. Users will have to install an updated and completely recompiled JRE. There may be many different versions of JREs on a computer. Because no vendor can be sure that the end user's applications already have a compatible version of the JRE, each computer may need dozens of updated JREs. *Source: NetworkWorld.com*

February 2007 OnGuard Newsletter:
Home PC Security

Security Awareness Resources:

For more information on workplace security awareness education, visit :
http://nativeintelligence.com

Native Intelligence, Inc.

SEPTEMBER 2006

Inside

onGuard
is published monthly by Native Intelligence, Inc.
www.nativeintelligence.com
Direct inquiries and correspondence to:
onguard@nativeintelligence.com

onGuard

Focused on Security Awareness, Training, and Motivation

Wireless Communication: Safeguarding Data in a Mobile World

Wireless communication technology has made it possible for us to access information "on the go" at work or at play – but how secure is the data we transmit and receive?

Wireless laptops, Personal Digital Assistants (PDAs), and Internet-enabled cell phones use radio waves to transmit data. Wireless access points connect wired networks to wireless signals. Access points broadcast and receive radio waves that are picked up by wireless devices (e.g., Blackberries, laptops). Most current laptops have built-in wireless adapters. To add wireless to older laptops and most desktops requires an add-on wireless adapter or wireless laptop card (e.g., an aircard).

Bluetooth

Bluetooth is a wireless technology largely used in the cell phone and wireless headset markets. Bluetooth is also available in automobiles and wireless computer keyboards, mice, and printers. Bluetooth is designed to connect devices within a short range, for example, from your ear to a cell phone in your pocket. The range can be extended to over a mile with special antennas.

Software programs can allow intruders to identify nearby Bluetooth-enabled devices. If those devices are unprotected, information can be easily stolen over the air. Theft of information over a Bluetooth link is called "Bluesnarfing." Sending an unsolicited message to a Bluetooth device is called "Bluejacking."

Bluetooth security is often the responsibility of the user. Users may not be aware that on many wireless devices the security features are not enabled by default.

(see Wireless Communication, page 2)

GRILL YOUR SECURITY OFFICER

I'm concerned about talking on my cell phone because someone might be listening in. Can people tap calls I make from my cell phone?

Older analog cell phones could be heard using a mail order police radio scanner. Today's digital cell phone transmissions are much harder to tap in to. There is a greater risk of someone overhearing your conversation. Many cordless phones are not secure. Especially the ones that use the frequencies 46 MHz or 900 MHz. Their transmissions can be picked up with a radio receiver or even a baby monitor. There is less chance of your call being eavesdropped on if you use a spread-spectrum 2.4 GHz or 5.8 MHz digital phone. Always use a wired landline phone for making confidential calls.

(see Grill Your Security Officer, page 4)

Want to grill us on security issues?...

Send questions to:
grillus@nativeintelligence.com

Securing Wireless Data Access – What You Can Do

Implementation of any wireless network is strictly prohibited without proper authorization. Wireless networks must address specific business needs not currently met by the wired network.

- Do not enable wireless or aircards while connected to internal network.
- Only use wireless access within authorized areas to connect to the public Internet.
- Always disable your wireless adapter before connecting a laptop to the wired network.
- Do not allow visitors to roam around facilities using Wireless LANS. Many Access Points can be physically reset to insecure factory default settings by pressing a reset switch on the box.
- If possible, use an encrypted connection or a Virtual Private Network (VPN). Contact IT Security for information on VPNs.
- Avoid connecting to public networks. When you connect to an open wireless network, you should have no expectation of privacy or security.
- If you have to use an open wireless connection, do not visit Web sites that require user names, passwords, or account numbers, such as online banking. Use an encrypted connection or a VPN.
- Turn off your wireless network when you're not using it.

Securing Wireless Data Access at Home

Home wireless LANs are less likely than work LANs to be configured securely. The range of wireless LANs is large enough to expose home networks, even in homes on large suburban lots. Wireless signals do not necessarily stop at the walls of a building. Thus, unauthorized users outside may be able to receive the signal and use your Internet connection. To protect your home wireless connection:

- Place your wireless base station in the center of your home, away from outside walls.
- Make sure that you have wireless security enabled on your laptops and routers — preferably Wi-Fi Protected Access (WPA). Consult your manual for specific details on these tips.
- Change the default password on your router to a strong password.
- Name your wireless network. In your access point's setup dialog, change the Service Set Identifier (SSID), which is the name of the network typically broadcast by the access point. The default setting is often the brand

(see Securing Wireless Data, page 4)

Native Intelligence, Inc.

from page 1

Wireless Communication

NOTE: The courts have held that there is no expectation of privacy with a cordless phone. Do not discuss Confidential Information on a cordless phone.

BlackBerry

BlackBerry Personal Digital Assistants (PDAs) use cell phone technology to transmit wireless data. BlackBerries have strong encryption between the handset and the enterprise server. This can protect text messaging and e-mail within our organization.

Wireless Vulnerabilities

Wireless connections are not as secure as wired ones because they do not have the protection of the physical building perimeter. Buildings protect against attack for wired networks because wires have to be physically accessed to make a connection. Wireless networks can be attacked without physical access.

Wi-Fi Hotspots (open access or open networks) — public wireless access, such as at airports, coffee shops, Internet cafés, libraries, and hotels are not Wi-Fi encrypted. There is no such thing as a trusted open network. If you or network personnel did not configure the network, and you can't identify everyone connected to it, it's an open network. Whenever you use an open network, others could be reading and using the information you see and send.

Range — many people are unaware of how far their wireless devices and networks can transmit. Wireless adaptors are low-power devices designed to have a short range. Radio waves, however, do not care about manufacturer specifications. They just keep going, becoming fainter with distance. Cheap antennas can extend wireless signals to several miles. Remember the words of General John Sedgwick right before he was killed in 1864: "They couldn't hit an elephant at this distance."

Wireless Users — may open backdoors to the private networks. An employee's laptop with a wireless network connection could be plugged into the wired company network while the wireless connection is active. If this happens, the laptop will act as a bridge from the wireless network to the company network. This can allow attackers to bypass the network firewall.

FAST FACTS!

- Research by Gartner indicates that 64% of businesses expect to increase their wireless network deployments over the next year. Security was one of their top 5 concerns, with 60% of the businesses reporting that they have inadequate security for their wireless environment.
- Travelers left 85,000 cell phones and 21,000 handheld devices in Chicago taxis during a six month period in 2005.
- Fewer than 5% of mobile device users voluntarily set password protection, unless they are required to do so by company mandated enforcement.

NOTE: Always disable your wireless adapter before connecting a laptop to the wired network. Contact IT security for support or assistance.

Threats to Wireless

Wi-Fi Jacking — if you do not turn on the security features of your wireless Internet devices, you may be the victim of "Wi-Fi Jacking." This is where criminals walk or drive through business areas (and neighborhoods) and identify unprotected wireless LANs from the street using laptop or handheld computers. When they find an unprotected network, they can hijack that wireless connection to download illegal materials, send spam, etc. This also puts the criminals closer to being able to

(see Wireless Communication, page 4)

from page 3

Grill Your Security Officer

What should I do if my BlackBerry is stolen?

Immediately report lost or stolen devices such as Blackberry Personal Digital Assistants (PDAs), laptops, and cell phones to your supervisor and IT Security. Upon notification of equipment loss, IT Security along with your department must assess the potential exposure of customer or sensitive data. Remember the theft or loss of any equipment containing Confidential Information must be reported immediately.

Remember: **REPORT LOST OR STOLEN MOBILE DEVICES IMMEDIATELY!**

from page 3

Securing Wireless Data

name of the router. Don't use your address as your SSID.

- Set the access point so that it does not broadcast the SSID. Often, this can be done by selecting a checkbox on the same setup page where the SSID name is changed.
- Turn off your wireless network when you are not using it.
- To be most secure, enable Media Access Control (MAC) filtering on your wireless access point. Add the MAC address (a unique 12-digit number) of each device, e.g., your laptop or home computer, that you want to access your Wi-Fi connection.

from page 2

Wireless Communication

hack into the victim's computer and steal information and identities.

Evil Twin Hotspots — an evil twin is a free, wireless hotspot created by a criminal. The evil twin mimics an Internet access hot spot such as the ones found at airports, coffee shops, and bookstores. Evil twin hotspots look legitimate. People connect to the twin and do online banking and send e-mail, unaware that the criminal is recording their user names, passwords, account numbers, and more.

Mobile Device Viruses — are malicious software that exploit vulnerabilities in Bluetooth, wireless encryption protocols, and other wireless technologies. Mobile viruses target handheld devices, cell phones, and wireless networks. Mobile viruses spread in the same way as traditional computer viruses: through downloading of infected programs and files such as photos, video clips, ring tones, and cell phone themes. Bluetooth-enabled mobile devices can become compromised when brought in range of an infected Bluetooth device.

Other Threats — include jamming to cause Denial of Service (DoS) and sniffing. Jamming can be on purpose or by accident. The presence of other devices, such as cordless phones, that operate in the same frequency as the wireless network can cause jamming. Sniffing is a passive attack that occurs when someone listens to or eavesdrops on network traffic. Use encryption to defend against sniffing on a wireless network.

Protecting Data Through Wireless Encryption — WEP and WPA

One of the most common ways to encrypt wireless communications is Wired Equivalent Privacy (WEP). WEP is an older specification that is fairly easy to break with programs available on the Web. Wi-Fi Protected Access (WPA or WPA2) is much more secure, but not all Wi-Fi equipment supports WPA.

NOTE: Encrypted data can be susceptible to decryption. There is no guarantee that your transmission has not been recorded and decrypted later. Because of this, some data is too sensitive to send over wireless connections. Check with IT Security if you are unsure whether your data can be safely sent over wireless.

VPNs and SSL also provide encryption. Ask IT Security for help with encryption.

October 2006:

Newsletter will focus on –
Business Continuity

Security Awareness Resources

For more information on workplace security awareness, visit:
http://nativeintelligence.com

Native Intelligence, Inc.