Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Inside Story: A Disgruntled Employee Gets His Revenge

In a time when computer viruses and worms continue to steal the media spotlight, it isn't surprising that many companies have already implemented the security defenses required to protect against these external threats. In fact, antivirus software and firewalls are the two most common security technologies used in all organizations. While these threats certainly deserve our attention, too much focus on external threats can cause us to overlook the most dangerous and costly threat of all - the disgruntled company inside...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
CounterTack Active Forensics for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

GIAC Certified Incident Handler (GCIH)
Practical Assignment Version 4.0: Exploit in a Lab

The Inside Story:
A Disgruntled Employee Gets His Revenge

Heather Kratt
December 8, 2004

© SANS Institute 2005, Author retains full rights.

Introduction....4
Part One: Statement of Purpose....4
Part Two: The Exploit....5
Exploit No. 1: Social Engineering....5
Name....5
Common Vulnerabilities and Exposure (CVE) Number....5
Other Advisories....5
Variants....5
Vulnerable Operating Systems....5
Protocols / Services / Applications....5
Description....5
Attack Signatures....6
Solutions or Mitigation Strategies....7
References....7
Exploit No. 2: Win-Spy Software 8.1 Pro....8
Name....8
Common Vulnerabilities and Exposure (CVE) Number....8
Other Advisories....8
Variants....8
Vulnerable Operating Systems....8
Protocols / Services / Applications....8
Description....9
Attack Signatures....9
Solutions or Mitigation Strategies....11
References....11
Exploit No. 3: Citrix GoToMyPC Personal....12
Name....12
Common Vulnerabilities and Exposure (CVE) Number....12
Other Advisories....12
Variants....12
Vulnerable Operating Systems....12
Protocols / Services / Applications....12
Description....13
Attack Signatures....14
Solutions or Mitigation Strategies....16
References....16
Part Three: Stages of the Attack Process....17
Reconnaissance....18
Scanning....19
Exploiting the System....20
Social Engineering....20
Win-Spy Software 8.1 Pro....21
Citrix GoToMyPC Personal....29
Keeping Access....37
Covering Tracks....39
Network Diagram....40
Part Four: The Incident Handling Process....41
Preparation....41

© SANS Institute 2005 Author retains full rights.

Identification 44
Containment 48
Eradication 50
Recovery 51
Lessons Learned 52
Conclusion 54
References 55

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Introduction

In a time when computer viruses and worms continue to steal the media spotlight, it isn't surprising that many companies have already implemented the security defenses required to protect against these external threats. In fact, antivirus software and firewalls are the two most common security technologies used in all organizations.[1] While these threats certainly deserve our attention, too much focus on external threats can cause us to overlook the most dangerous and costly threat of all – the disgruntled company insider.

According to the 2004 CSI / FBI Computer Crime and Security Survey, security breaches appear "fairly evenly split between those originating on the outside and those originating within the organization."[2] The 2003 CSI / FBI Computer Crime and Security Survey reported that 77% of organizations that experienced any kind of security breach suspected a disgruntled employee.[3] Although the number of external and internal threats is fairly equal, the cost associated with either type of attack is significantly different. The average cost of an attack originating from outside an organization is $57,000, while the average cost of damages incurred from an insider attack is an astounding $2.7 million dollars![4]

In this paper, I will present the fictional story of a disgruntled employee who exacts revenge on his employer by stealing sensitive customer information and posting it on a public website. While the character is fictional, the security risk he represents is quite real. I will describe his motive for attacking his employer's network, analyze the tools and techniques that he used to circumvent existing security measures, and detail the steps involved in the attack process.

I will also explain the incident handling process, and how the company's incident handling team responded to this situation. I will explain how the attack was detected, the steps taken to identify the source of the attack, and some actions that can be taken to mitigate future risk from this type of attack.

Part One: Statement of Purpose

The intent of the attack described in this paper is to simulate one possible way that a disgruntled employee can bypass existing security measures and cause costly damage to an employer. The disgruntled employee will use a combination of social engineering and commercial software tools to steal sensitive customer information.

The disgruntled employee's attack will start with the use of social engineering, which is the act of obtaining information through deception. He will accomplish this by taking advantage of his position on the company help desk team. Through persuasion, and

[1] Gordon, Loeb, Lucyshyn, & Richardson (2004); p. 11
[2] Gordon, Loeb, Lucyshyn, & Richardson (2004); p. 9
[3] SecurityPipeline (2004)
[4] Ernst & Young (2003), p. 2

© SANS Institute 2005 Author retains full rights.

against company policy, he will convince another employee to give him his network password. He will also convince that employee to give him his workstation's IP address. By doing so, the attacker will gain the username, password and IP address required to perform the next stage of his attack.

The second step of his attack involves the use of a commercial keystroke logger. Using the information he gathered during his social engineering attack, the attacker will remotely and secretly install the keystroke logger on his victim's workstation. By doing so, he will gain the user's password to the restricted customer database.

The final step of his attack involves the use of a commercial HTTP tunneling tool. Because most companies allow the HTTP protocol through their firewalls, this tool enables users to bypass security measures by simply piggybacking the use of a prohibited action or protocol on one that is allowed. Our attacker will use this tool to remotely access the company network and complete his attack.

While the commercial tools and techniques used in this simulation might normally seem innocuous, I will demonstrate the real threat they pose to any organization. The purpose of this story is to bring awareness to security risks that are often underestimated.

Part Two: The Exploit

This section describes the combination of exploits that will be used in this attack. Three exploits will be used: social engineering, Win-Spy Software 8.1 Pro, and Citrix GoToMyPC Personal.

Exploit No. 1: Social Engineering

Name: Social Engineering

Common Vulnerabilities and Exposure (CVE) Number: N/A

Other Advisories: N/A

Variants: N/A

Vulnerable Operating Systems: N/A

Protocols / Services / Applications: N/A

Description:

Social engineering is the act of obtaining information through deception. It exploits a vulnerability in our own human nature – the tendency to trust others. A social engineer might pretend to be an employee seeking innocuous information, try to convince you

© SANS Institute 2005 Author retains full rights.

that an exception to the rule is okay because of the urgency of the situation, or just act like he or she belongs somewhere he or she really shouldn't be.

A skillful intruder can use social engineering to gain access to a protected network or system. After all, the easiest way for an intruder to get past an organization's technological and physical security obstacles is to simply go around them. With the help of unsuspecting employees, this has proven to be a very successful technique.

Kevin Mitnick is a perfect example of just how powerful social engineering is. Mitnick is a well-known hacker who broke into the systems of some of the largest corporations in the world, including Motorola, DEC, Novell, and Sun Microsystems.[5] According to his own testimony to the U.S. Senate Governmental Affairs Committee, Mitnick, who had spent 20 years circumventing security measures, claims that he has "successfully compromised all systems that I targeted for unauthorized access save one."[6] While Kevin Mitnick is certainly technically savvy, he owes most of his hacking success to what has been deemed "the art of persuasion."

Attack Signatures:

Because social engineering is an attack on human nature, there are no technical signatures that we can use to detect this type of attack. There are, however, specific communication techniques used in these attacks that can help us to recognize it. As cited in Kevin Mitnick's "Art of Deception," there are six basic tendencies of human nature that can be exploited in a social engineering attack.[7] Those basic tendencies are:

1. Authority: People have a tendency to comply with authority figures. For example, an attacker might persuade you to help him by misrepresenting himself as an Information Technology (IT) employee, as an executive in the company, or as an employee who supports an executive.

2. Liking: People have a tendency to help those they like, so the attacker might try to convince the victim that they have something in common. For example, an attacker might develop a bond with his victim by claiming to have similar interests, hobbies, beliefs, goals, attitudes, hometowns, etc.

3. Reciprocation: People have a tendency to help those who have already done something to help them. For example, an attacker might pose as a member of the support staff, and claim to have done something to protect you or your system. In return, the attacker will persuade his victim to perform a favor that is not as innocuous as it might seem.

4. Consistency: People have a tendency to comply when they have already made a verbal promise or commitment to do so. For example, after an attacker convinces

[5] U.S. Department of Justice (1999)
[6] U.S. Congress Testimony (2000)
[7] Mitnick (2002), pp. 246 - 249

© SANS Institute 2005 Author retains full rights.

you to verbally comply with a company policy, he might persuade you to form your future passwords in such a way that they can be easily guessed.

5. Social Validation: People have a tendency to comply when the behavior seems to be supported by their peers. For example, an attacker might convince you to comply with a fictional survey by claiming that other employees have already done so.

6. Scarcity: People tend to comply when the object being sought is in short supply, is creating competition, or is only available for a limited time. For example, an attacker might send an email to company employees, claiming that the first people to respond will win something. By coaxing users to register on a bogus website, usernames and passwords can be easily captured.

Solutions or Mitigation Strategies:

User awareness training and security policies are the best defense to social engineering. Employees need to understand what social engineering is, how to respond to suspicious inquiries, and the company policies that have been implemented to protect sensitive information.

User awareness should be an ongoing training program in all organizations. Only through constant reminders and management support can employees be truly effective in identifying these types of attacks and respond appropriately. Employees should be encouraged to always err on the side of caution and think before they act. When they answer the phone, respond to an email, or hold the door open for somebody, they should think about what they are doing. Is somebody asking for sensitive information? Do they trust the source? Do they know the person who just followed them into the building? Regular user awareness training will help all employees to think defensively and avoid social engineering attacks.

Security policies establish accountability and provide clear guidelines for employees. In addition to publishing security policies, all employees should be trained to ensure they understand their role and how the policies apply to them. Employees should be required to report potential security incidents and given clear instructions on how to report that information. Employees also need to understand the consequences of violating these security policies. Security is often regarded as the IT department's responsibility, so it needs to be made clear that these policies apply to all employees, not just those in technical positions. Employees should be reminded that each individual plays a key role in the security of their organization and that it is a shared and very important responsibility.

References:

For more information about social engineering, refer to the following sources:

Organization: U.S. Computer Emergency Readiness Team (CERT)
Title: Cyber Security Tip ST04-014
URL: http://www.us-cert.gov/cas/tips/ST04-014.html

© SANS Institute 2005 Author retains full rights.

Organization: Wikipedia: The Free Encyclopedia
Title: Definition: Social Engineering (Computer Security)
URL: http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29

Organization: U.S. Congress
Title: Mr. Kevin Mitnick (Testimony to Senate Governmental Affairs Committee)
URL: http://www.globalsecurity.org/security/library/congress/2000_h/030200_mitnick.htm

Organization: CSO: The Resource for Security Executives
Title: Anti-Social Engineering
URL: http://www.csoonline.com/read/100702/machine.html

Organization: EnterpriseITplanet.com
Title: An Hour with Kevin Mitnick
URL: http://www.enterpriseitplanet.com/security/features/article.php/3333481

Exploit No. 2: Win-Spy Software 8.1 Pro

Name: Win-Spy Software 8.1 Pro

Common Vulnerabilities and Exposure (CVE) Number: N/A

Other Advisories: N/A

Variants:

Information about more than 200 commercial keylogger applications can be found at SpywareGuide.com:

http://www.spywareguide.com/product_list_category.php?pageNum_Rs_product=0&totalRows_Rs_product=182&category_id=3

Vulnerable Operating Systems:

Microsoft Windows 98
Microsoft Windows ME
Microsoft Windows NT 4
Microsoft Windows 2000
Microsoft Windows XP

Protocols / Services / Applications: N/A

© SANS Institute 2005 Author retains full rights.

Description:

Win-Spy Software 8.1 Pro is a commercial computer surveillance tool. It enables the person who installs it to secretly monitor keystrokes and capture screenshots, giving them full view into another user's activity on that computer. Worried parents, suspicious spouses, and controlling employers are often the advertising targets of these commercial monitoring tools. A cyber attacker, however, can just as easily use these tools for malicious purposes.

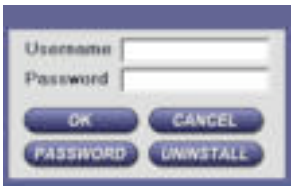
This tool includes remote installation capability, which enables the attacker to either trick a person into installing the tool or to secretly install it without the victim's knowledge. By secretly monitoring a person's keystrokes and capturing screenshots, an attacker can steal usernames, passwords, and other sensitive information.

Attack Signatures:

Although Win-Spy Software 8.1 Pro uses a stealth install, there are distinct signs that can help to determine its presence on a system:

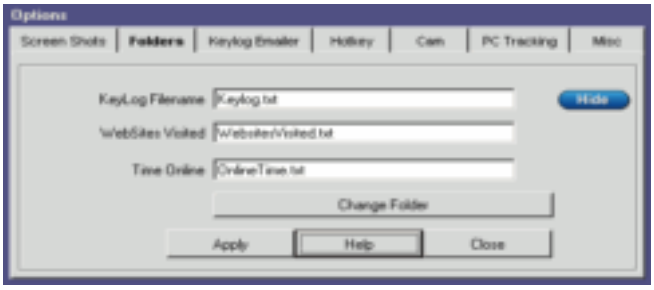
System Tray Icon: The retail version of this software will not add any distinguishing icons to the system tray. The free evaluation version, however, will add the following icon to the system tray:

Login Hotkey: The default login hotkey for the Win-Spy management console on a local install is Crtl-Shift-F12. There are only three other configuration options for that hotkey: Alt-Shift-F12, Ctrl-Shift-W, or Shift-Alt-Up Arrow. Any one of these four key-combinations will display the following login menu:



The current hotkey configuration is also stored in `c:\%windir%\system32\wskey.txt`.

Log Files: Win-Spy creates log files for keystrokes, website activity, and time spent online. Although there is an option to hide the log files, the default setting leaves them unhidden. On a local install, these log text files are stored by default in the `c:\program files\accessories\temp*` directory with the following default file names:



© SANS Institute 2005 Author retains full rights.

On a remote install, the log files are stored by default in the `c:\program files\accessories\common` directory with the same default file names.

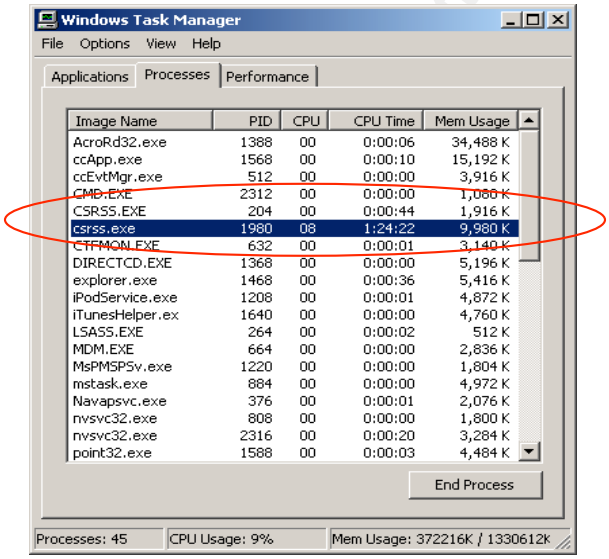
Screen Captures: Win-Spy captures screenshots at the default interval of every 50 seconds. On a local install, the screen captures are stored by default in the `c:\program files\accessories\temp*` directory with a file name similar to the following: `31 Oct 04 18_13_06 Dirk Smith.rna`

On a remote install, the screen captures are stored by default in the `c:\program files\accessories\common` directory.

Remote Install / Uninstall Files: The default file name for a remote install is `joke.exe`. Win-Spy recommends emailing this install file to users, but it can also be installed via other methods, such as a login script or startup folder. The default file name for a remote uninstall is `remove.exe`.

System Process: The Win-Spy application runs as `c:\%windir%\system32\dll\csrss.exe`. Csrss.exe is also the name of a default process in Windows, the client / server run-time subsystem, which is correctly located in the `c:\%windir%\system32\` directory. Csrss.exe is the user-mode portion of the Win32 subsystem, responsible for console windows, creating or deleting threads, and some parts of the 16-bit virtual MS-DOS environment.[8]

Because `csrss.exe` is a critical system process, it cannot be terminated via the Task Manager. The authors of malicious code often take advantage of that fact and use the `csrss.exe` name. Therefore, if more than one instance of the `csrss.exe` process is running on a system (see the following example), or more than one copy of that file is found on the system, it is quite possible that Win-Spy is installed, or that the system is infected with some other spyware or malicious code.



[8] Microsoft (2003)

© SANS Institute 2005 Author retains full rights.

Solutions or Mitigation Strategies:

The best defense against Win-Spy Software 8.1 Pro is to prevent its installation in the first place. Most anti-spyware, antivirus and anti-adware scanners, as well as personal firewalls, are unable to detect this threat. Win-Spy claims to be "immune to anti-spyware" because of its use of random filenames for most of its program files and its ability to "seek and destroy anti-spyware."[9] Limiting administrator access to systems, protecting active logon sessions, and blocking dangerous file attachments can help to prevent this type of attack.

If a user has administrator rights to a workstation, that user can intentionally install Win-Spy and monitor the activity of all other users who login to that workstation. That administrative user can also be tricked into running the remote Win-Spy installation file, which will then put all users who login to that workstation at risk of being secretly monitored. Because regular non-administrator users are prevented from making these intentional or accidental system-wide changes, limiting administrator access will help to prevent the installation of this software.

Protecting active logon sessions is crucial to protecting the integrity of any system account. An attacker doesn't need much time to install spyware, add new accounts, copy data, or perform some other adverse action with an unattended account. Users should be reminded to never leave an active logon session unattended, and to instead lock their console or log out completely before walking away from their desk. Password protected screensavers can help to automate this process.

Win-Spy can be installed on a remote system by emailing an executable installation file with the default name of `joke.exe` to an unsuspecting user. Users should be reminded to never open a file attachment that they were not expecting or from somebody that they do not know, as this is a very common way of spreading viruses and other malicious code. Because there is generally no legitimate reason to send executable files via email, this problem can be prevented by blocking dangerous file attachments before they ever reach a user's inbox. This can be accomplished by filtering file attachments at the email gateway, server, or client level.

References:

For more information about Win-Spy Software 8.1 Pro and computer surveillance, refer to the following sources:

Organization: BC Computing
Title: Win-Spy Software 8.1 Pro
URL: http://www.win-spy.com/index.htm

Organization: PC World
Title: Fight Back Against Surveillance Software
URL: http://www.pcworld.com/howto/article/0,aid,114738,pg,1,00.asp

[9] BC Computing (2004)

© SANS Institute 2005 Author retains full rights.

Organization: Wikipedia: The Free Encyclopedia
Title: Definition: Computer Surveillance
URL: http://en.wikipedia.org/wiki/Computer_surveillance

Organization: Network Magazine
Title: Special Report – The Pros and Cons of Employee Surveillance
URL: http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8703003&pgno=1

Organization: CNN
Title: More Employers Taking Advantage of New Cyber-Surveillance Software
URL: http://archives.cnn.com/2000/US/07/10/workplace.eprivacy/

Exploit No. 3: Citrix GoToMyPC Personal

Name: Citrix GoToMyPC Personal

Common Vulnerabilities and Exposure (CVE) Number: N/A

Other Advisories: N/A

Variants:

Other commercial HTTP tunneling tools include:

- HTTP-Tunnel Remote Anywhere (http://www.http-tunnel.com/html/solutions/http_tunnel/remote.asp)
- NetworkStreaming SupportDesk (http://networkstreaming.com/products/supportdesk.html)
- WAN Strategies Remote Workplace (http://www.remoteworkplace.com/rwfeatures.html)

Vulnerable Operating Systems:

Windows 95
Windows 98
Windows CE
Windows ME
Windows NT
Windows 2000
Windows XP

Protocols / Services / Applications:

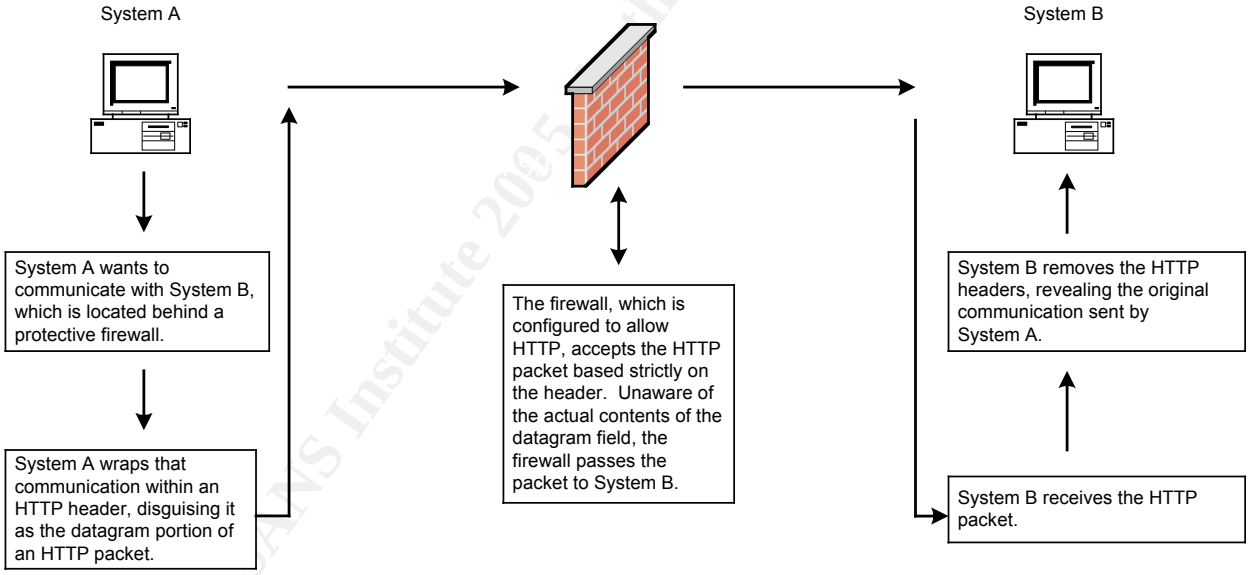
© SANS Institute 2005 Author retains full rights.

HyperText Transfer Protocol (HTTP) is the primary application layer protocol used for web-based communications. HTTP enables a web browser client to request a response from a web server, such as the process of opening a simple web page. SSL-encryption HTTP (HTTPS) is the secured version of the HTTP protocol, which works by encrypting the session data that passes between the web browser and the web server. Both HTTP (port 80) and HTTPS (port 443) are essential to one of our favorite pastimes: surfing the web.

Due to the popularity of the web, most organizations allow the use of HTTP(S) on their networks. Even organizations that use firewalls to restrict and control network traffic typically allow their network clients to pass outbound HTTP(S) requests through the firewall. This makes HTTP(S) a perfect candidate for tunneling.

Tunneling is the process of transporting some protocol or data across a network by wrapping it in another protocol that both the sending and receiving ends understand. HTTP(S) tunneling wraps that data in HTTP(S) protocol headers, making it appear to be a standard HTTP(S) network packet. Because most firewalls will accept HTTP(S) packets, HTTP(S) tunneling can be used to bypass existing security measures, such as the firewall itself and intrusion detection systems.

The following diagram illustrates the basic concept of HTTP tunneling:



Description:

Citrix GoToMyPC Personal is a commercial remote control application. It is a web-based service that essentially acts as the middleman between you and the remote system that you would like to connect to. The service consists of a host, a client viewer, and the GoToMyPC web and communication servers. The host software runs on any Windows-based system, and the client viewer software runs on Windows, Macintosh, and Unix systems.

© SANS Institute 2005 Author retains full rights.

The GoToMyPC host monitors for remote access connection requests by sending outgoing HTTP "pings" to the GoToMyPC broker site (poll.gotomypc.com) at regular intervals. If a viewer client is waiting to connect, the communication channel will be established. By initiating that outbound connection, the host system is enabling a reverse HTTPS tunnel. While this feature is marketed as a convenience for remote users, it is a serious security concern because it enables users to bypass existing security measures.

Attack Signatures:

Because Citrix GoToMyPC Personal uses HTTPS tunneling, its use can be difficult to detect at the network level. GoToMyPC generates only outbound HTTP(S) requests on ports 80, 443 and/or 8200. Because this is pretty typical traffic for most networks, it probably won't arouse much suspicion. There are a few indicators at the network level, however, that can help to determine whether or not GoToMyPC or HTTP(S) tunneling is being used to remotely access systems in your environment:

- A GoToMyPC host monitors for remote access connection requests by sending outgoing HTTP "pings" to the GoToMyPC broker site (poll.gotomypc.com) at regular intervals. So, any client attempts to communicate with that broker site should be investigated.
- Typical HTTP traffic consists of a simple request and response, such as a client clicking on a web link to request the return of a specific web page from a web server. Because that traffic is generally short lived and not persistent, any HTTP session lasting longer than 60 seconds could indicate that tunneling is in use.[10]
- Because HTTPS is more interactive and persistent than HTTP, it is common for these exchanges to continue for some time and transfer large amounts of data. Any client that is generating more HTTPS traffic than it is receiving could indicate a client / server role reversal and the use of tunneling.
- Because HTTP(S) traffic should normally only be generated when a person is at that computer, monitoring for the use of HTTP(S) during irregular hours can help to identify suspect clients.

Citrix GoToMyPC Personal consists of a host, which is the computer that will be accessed remotely, and the client viewer, which is the computer that will be used to access the remote host. There are signs that can help to determine the presence of GoToMyPC on either the host or client viewer systems:

<u>System Tray Icons</u>: If GoToMyPC is running on a host computer, one of two icons will appear in the system tray, depending on whether or not a remote access session is currently in use:

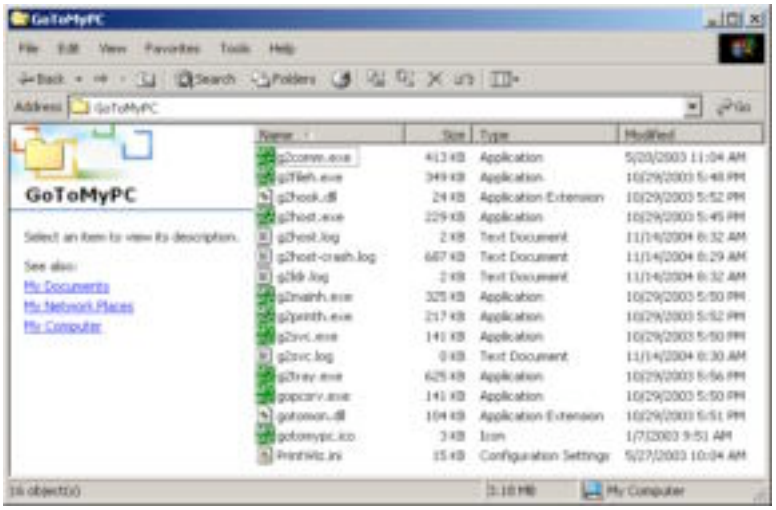
Ready for use:
Session in progress:

No system tray icons are used on the client viewer system.

[10] Kellermann and Nishiyama (2003), p. 9

© SANS Institute 2005 Author retains full rights.

Program and Log Files: On a host system, the GoToMyPC program and log files are stored in the `c:\program files\expertcity\gotomypc` folder:



On a client viewer system, the program files are stored in the current user's profile folder. An example is `c:\documents and settings\jphritz`, but the exact path can be determined with the `echo %userprofile%` command. The program files that might be installed include `gosetup.exe` and `gotomypc.exe`.

On a client viewer system, the log files are stored in a subfolder in the current user's temp directory. An example is `c:\documents and settings\jphritz\local settings\temp\g2_276`, but the exact path to the temp folder can be determined with the `echo %temp%` command. The log files that might be created include `g2viewer.log`, `gotomypc.log` and `gosetup.log`.

System Processes:

On a host system, the following system processes may be running, depending on whether or not a remote access session is currently in use:

If GoToMyPC status is "Ready for use":

- `g2tray.exe`
- `g2svc.exe`
- `g2comm.exe`

If GoToMyPC status is "Session in progress":

- `g2tray.exe`
- `g2svc.exe`
- `g2comm.exe`
- `g2host.exe`
- `g2mainh.exe`
- `g2printh.exe`
- `g2fileh.exe`

On a client viewer system, the following system processes will be running when connected to a remote host system:

© SANS Institute 2005 Author retains full rights.

- g2viewer.exe
- gotomypc.exe

Solutions or Mitigation Strategies:

To prevent the unauthorized use of Citrix GoToMyPC Personal in your environment, there are steps that can be taken at the enterprise, network and system levels. Establishing security policies for remote access and workstation software usage, blocking Internet access to the GoToMyPC broker site, limiting administrator access to systems, and using personal firewalls can all help to prevent this type of attack.

Security policies establish accountability and provide clear guidelines for employees. The establishment of remote access and workstation software usage policies can both help to deter the use of unauthorized remote access software. The remote access policy should strictly prohibit the use of any non-authorized remote access solutions. The workstation software usage policy should strictly prohibit the installation and use of any non-authorized software.

A GoToMyPC host monitors for remote access connection requests by sending outgoing HTTP "pings" to the GoToMyPC broker site (poll.gotomypc.com) at regular intervals. Blocking Internet access to the GoToMyPC broker site will essentially break the communication process, and prevent a remote viewer system from connecting to any hosts on your internal network. Blocking Internet access to the entire GoToMyPC.com domain could also help to hinder the unauthorized installation of the tool in the first place.

The GoToMyPC software is installed by visiting the gotomypc.com website and launching a signed java applet. If a user has administrator rights to a workstation, that user can freely install any unauthorized software, including GoToMyPC. Because regular non-administrator users are prevented from making this type of system-wide change, limiting administrator access will help to prevent the installation of this software.

Software, or personal, firewalls can be used to block applications and ports at the system level. By deploying a centralized personal firewall policy management server, an organization can more easily enforce which applications are used on their client systems. By blocking the use of any applications or ports that have not been explicitly approved and allowed by the company, personal firewalls can help to prevent the use of all unauthorized software.

References:

For more information about Citrix GoToMyPC Personal and HTTP(S) tunneling, refer to the following sources:

Organization: Citrix Online
Title: Citrix GoToMyPC Personal
URL: https://www.gotomypc.com/?Portal=gotomypc.com

© SANS Institute 2005 Author retains full rights.

Organization: Citrix Online
Title: Citrix GoToMyPC Personal – Technology Overview
URL: https://www.gotomypc.com/ourTechnology.tmpl?SessionInfo=137845987/71277FAFC1E316C/null

Organization: SecurityFocus
Title: Data Driven Attacks Using HTTP Tunneling
URL: http://www.securityfocus.com/infocus/1793

Organization: Developer.com
Title: Backdoors, Back Channels and HTTP(S)
URL: http://www.developer.com/tech/article.php/600451

Organization: The World Bank Integrator Unit
Title: The Digital Insider: Backdoor Trojans
URL: http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/TheDigitalInsiderDec2003/$FILE/The+Digital+Insider+Dec+2003.pdf

Part Three: Stages of the Attack Process

A successful crime usually requires careful planning and a series of coordinated steps. Prior to stealing a masterpiece, an art thief can help to ensure his success by properly preparing for the heist and his escape. By familiarizing himself with the museum, bringing the proper tools, identifying escape routes, disguising himself, and wearing gloves, the art thief increases his chance of getting away with the crime.

Similarly, when performing a cyber caper, criminals generally use a number of common steps to execute an attack. These steps include an in-depth reconnaissance of the targeted victim; a scan of the victim's computer or network to verify which vulnerabilities exist; the execution of the actual attack on the system or network; an attempt to maintain access; and the covering of tracks.

Before I detail the cyber attack process, let me introduce our fictitious attacker and the fake company he works for. Jack Phritz works for Behemoth Enterprises, a large online retailer. He has been with the company for over five years, and has worked for the help desk team the entire time. Jack is average in most ways. He receives average reviews and has been a fairly dependable employee. His technical and social skills are good, but not good enough to make him stand out.

Jack's ultimate career goal is to move into the Finance field, a job he is passionate about but lacks the actual work experience to achieve. So, during the evenings, Jack attends the local college, working towards his Bachelor of Science in Finance. He has been at it for three years, but feels confident that his hard work will pay off soon.

© SANS Institute 2005 Author retains full rights.

When a position opened up in Behemoth Enterprise's Finance department, Jack promptly applied for the job. Given his many years spent with the company and the fact that he's been working towards his Finance degree, Jack felt he was the perfect candidate for the job. In fact, he felt he had earned this opportunity and was the clear choice.

Jack applied for the position by filling out the proper paperwork, submitting a resume that detailed his years with the company, and enclosing a cover letter that described his time with the company, his efforts in school, and his passion to join the Finance team. The automated email response that Jack received assured him that his application would be reviewed and that the team would get back to him if they saw a good fit. Jack was sure he would be hearing from them soon, so he waited.

Jack waited for weeks, and still heard nothing. Then he finally heard the news. Through the company grapevine, Jack learned that the Finance position had been filled by a candidate from outside the company. Not only had the company not given Jack the opportunity to interview for the job, but they didn't even give him the courtesy of a response. It was at this point that Jack's loyalty to Behemoth Enterprises took a drastic turn.

Reconnaissance

Reconnaissance is the act of gathering information about a victim prior to attack. In our museum example, an art thief might first survey a museum for the location of specific artwork, determine how the artwork is secured to the wall, identify all building exits, count the number of security guards on duty, and gather any other details that will increase his chance of stealing the items he wants without getting caught. In cyber crime, an attacker can use various online databases and websites to gather information about an organization prior to attack.

For attacks that originate from outside an organization, reconnaissance might include the examination of public domain name registration records, DNS lookups, Google or other web-based searches, open positions posted on public job sites, or the victim's own website. By examining this public information, an attacker can gather employee names, physical addresses, telephone numbers, company email address schemes, IP addresses, server names, technologies used, and other details that will be very helpful in social engineering or technical attacks against the organization.

For attacks that originate from inside an organization, the insider has the advantage of already being privy to certain company information. According to a study performed by the U.S. Secret Service and the CERT Coordination Center, "insiders pose a substantial threat by virtue of their knowledge of and access to their employers' systems and / or databases, and their ability to bypass existing physical and electronic security measures through legitimate means."[11]

[11] Randazzo, Keeney, Kowalski, Cappelli, & Moore (2004); p. 2

© SANS Institute 2005 Author retains full rights.

Over the next couple of months, Jack performs his reconnaissance. Because Jack has worked for the company for over five years, he is already very familiar with the organization. He understands that, as a large online retailer, Behemoth Enterprises considers the customer database to be one of its most prized assets. He also knows that losing control of that database would be detrimental to the organization's bottom line.

By exploring the company intranet site, Jack discovered that the customer database is stored on a server named FINANCE_DB. He also found a web-based access request form that explained that access to the database is restricted, that a special user account and password are required to access the database, and that those accounts are managed by the corporate database team.

Jack was also able to obtain department organizational charts from the intranet, so now he had a complete employee list for the Finance department. He saw that a guy named Dirk Smith had filled the previously open position that he applied for. Because all employee Microsoft Outlook calendars are viewable by all other employees, Jack was able to determine Dirk's work schedule. He learned that on the following Tuesday morning, Dirk was not scheduled to be out of the office and was not scheduled for any meetings.

Through reconnaissance, Jack has identified a target employee, a restricted company system, and some potential opportunities for exploiting them.

Scanning

Scanning is the act of verifying which vulnerabilities exist on a specific system or in a specific environment. In our museum example, an art thief might check all of the doors and windows in the museum to see which one he can climb into now or just take note of which ones are unlocked and return later to commit his crime. In cyber crime, an attacker can use various scanning tools to accomplish a similar feat.

Scanning can help to determine which ports are open on a firewall, which services are being run on a specific system, which operating systems are in use, which phone lines have modems attached to them, and which known vulnerabilities are currently not patched on a given system. Scanning helps an attacker to confirm the existence of possible entrance points into your system or network.

The detection of scanning can sometimes offer an early warning sign that somebody intends to attack and the location the attack might come from. Many companies install network-based intrusion detection systems to monitor and report on this type of activity. Because scanning has become such common malicious behavior on the Internet, Behemoth Enterprises is used to being scanned on a regular basis. While it's something they monitor regularly, they don't necessarily respond to all external scanning attacks. Instead, they focus resources on keeping the "doors and windows" locked so that external scanning is kept to a minimal risk level.

© SANS Institute 2005 Author retains full rights.

Scanning detected from any host on the internal company network, however, will immediately raise a red flag. If scanning is detected on the internal network, the thief has moved past the doors and windows and is now checking closets and drawers. This activity presents a more active threat and is taken very seriously by the company.

Jack thought about scanning Dirk's workstation in the Finance department to confirm which vulnerabilities exist, but he knew that running a scanner on the internal network would draw attention to him. But Jack also knew that the company used a standard workstation build for all employees. This means that a vulnerability or opportunity that exists on one system will exist on all systems. So, he didn't have to scan his victim from across the network. He simply had to analyze his own machine to determine which vulnerabilities could be exploited enterprise-wide.

The standard base workstation build at Behemoth Enterprises consists of Microsoft Windows 2000 Professional with Service Pack 4, Microsoft Internet Explorer 6, Microsoft Office 2000 Professional, Norton AntiVirus 9, WinZip 8.1, and Symantec pcAnywhere 11. Other applications and tools are installed on an as needed basis.

Exploiting the System

In our museum example, the exploitation would be the actual heist. In cyber crime, it's the actual attack on the system or network.

On Tuesday morning, Jack arrived at work at his usual 8:00 AM start time. After going to get his customary morning double tall chocolate non-fat soy latte, Jack started his day by laying the groundwork for his attack against his employer.

Social Engineering

From his previous reconnaissance, Jack had targeted a potential human conduit for this attack. He knew that Dirk Smith, the new employee in the Finance department who had gotten the job Jack applied for, was not scheduled to be out of the office and not scheduled for any meetings that morning. Therefore, it was quite probable that Dirk would try to access the network at that time.

Part of Jack's regular job duties include the management of user accounts, such as password resets or the re-enabling of locked out accounts. Today, Jack would abuse this authority to initiate a social engineering attack.

Jack opened his Microsoft Active Directory Users and Computers console. He went to the account properties for Dirk Smith and selected "account is disabled." Then he sat back, sipped his "coffee," and waited for the phone to ring.

At 8:45 AM, Dirk from the Finance department called the help desk team. Jack picked up the call, "Help Desk, this is Jack. How can I help you?"

© SANS Institute 2005 Author retains full rights.

“Hi, Jack. This is Dirk over in Finance. I’m trying to login to the network, but keep getting this error. It says: ‘Your account has been disabled. Please see your system administrator.’ Can you help me with that?”

“Sure, I can help you with that. Let me take a look at your account.” Jack opens up the Microsoft Active Directory Users and Computers console again, and pretends to be reviewing the details. “Well, this is odd. Your account doesn’t appear to be disabled. Let me try logging in from my workstation and see what happens. What’s your password?”

Dirk promptly replies, “It’s diggler. D-I-G-G-L-E-R.”

“Okay, hold on while I try this.” Jack then comes back on the line to report, “It’s working fine for me. It must be something with your network connection. Let me try clearing a cache here and see what happens.” Meanwhile Jack goes back into Microsoft Active Directory Users and Computers and re-enables Dirk’s account. He says, “Okay, Dirk, try it again.”

Dirk logs in and says, “Oh, great, it’s working!”

Jack says, “Before you go, let me check one more thing to make sure this doesn’t happen to you again.” Dirk appreciates this extra effort, because he certainly can’t afford too much more downtime. Jack asks, “What’s the IP address on your workstation?”

“I don’t know. How do I tell?” asks Dirk. Jack then walks Dirk through the process of opening a command prompt and running the `ipconfig` command. Dirk then reads the IP address to Jack, “It’s 192.168.64.132.”

“Okay, let me take a look here,” Jack says as he does nothing more than doodle on his notepad. “Umm… okay, everything looks fine. That’s what I see from here. You’re all set. Is there anything else I can help you with today?“ asks Jack.

“No, that’ll do it. Thanks a lot!” says Dirk.

“Well, thank you for calling the help desk!” And with that, Jack has successfully obtained a username, password, and IP address for a workstation in the Finance department. He is now ready for stage two of his attack.

<u>Win-Spy Software 8.1 Pro</u>

From his previous reconnaissance, Jack knows that a separate username and password are required to access the customer database stored on the FINANCE_DB server. Because the corporate database team manages these accounts, not the help desk team, Jack cannot as easily obtain this password through social engineering. Instead, Jack will leverage the username, password and IP address he obtained previously to steal Dirk’s customer database password. Jack will accomplish this by remotely and secretly installing a commercial keystroke logger on Dirk’s workstation.

© SANS Institute 2005 Author retains full rights.

Jack downloads and installs a commercial keystroke logger called Win-Spy Software 8.1 Pro from the Internet. Although a free evaluation version is available, Jack decides to spend the $20 for the retail version. The difference is that the retail version won't place a distinguishing icon in the user's system tray:

Retail version adds no icon to system tray:

Free version adds this additional icon to system tray:

If Dirk were to notice that new icon, he might get suspicious and report the problem. So, Jack feels that to avoid getting caught, $20 is a wise investment.

Win-Spy Software 8.1 Pro is a very simple tool to install. After downloading the software to his own workstation, Jack simply runs the setup program.

By selecting "I Agree," Jack accepts the software license agreement and the installation continues:

Jack enters a new username and password that will be used to manage the Win-Spy application:

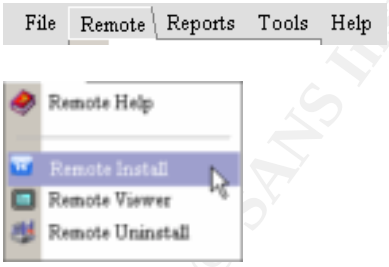
The installation is complete, and Jack is prompted to restart his workstation:

© SANS Institute 2005 Author retains full rights.

After rebooting his workstation, Jack presses Ctrl-Shift-F12 to access the Win-Spy login screen:

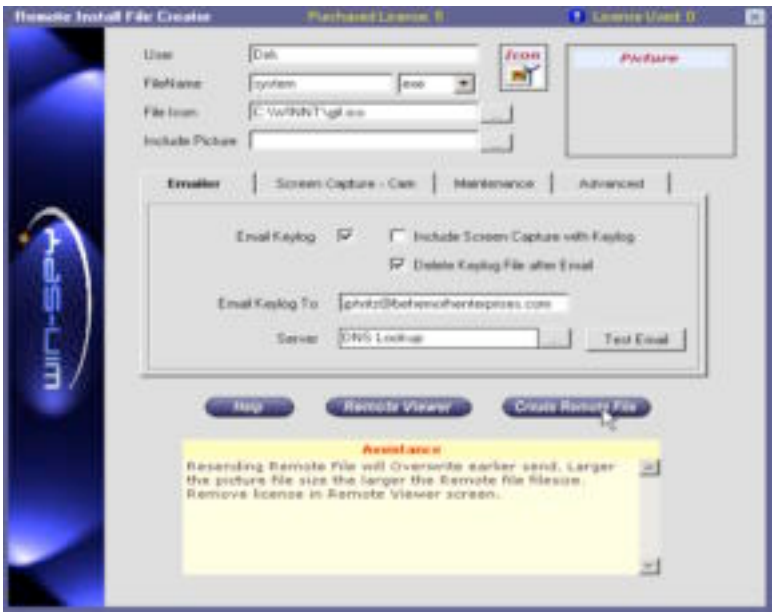
After entering his username and password, the Win-Spy management console is displayed:

Win-Spy offers remote installation capabilities. To create a remote installation file that Jack can use to install this tool on Dirk's workstation, he goes to the "Remote / Remote Install" menu:

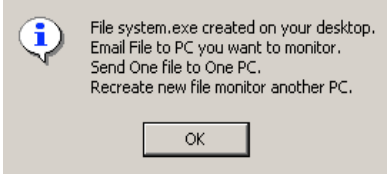


Jack enters the user name of "Dirk," changes the default filename of `joke.exe` to the less conspicuous `system.exe`, and enters his email address in the appropriate field. He then selects "Create Remote File":

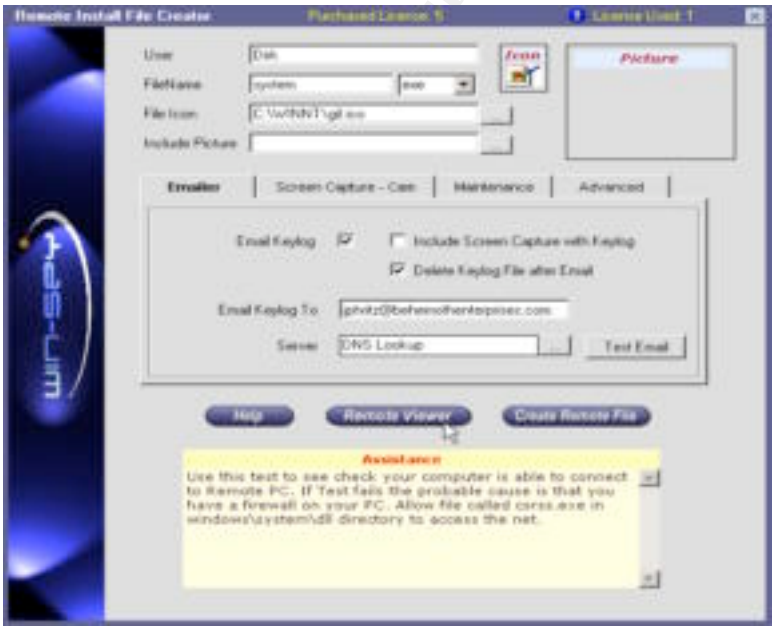
© SANS Institute 2005
Author retains full rights.



The remote installation file, called `system.exe`, has been created and placed on Jack's desktop:

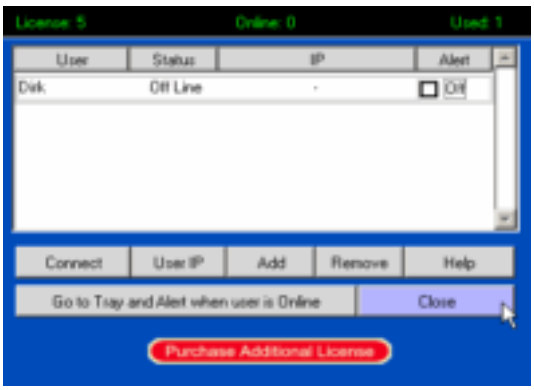


Although Win-Spy recommends emailing the remote installation file to the remote user, Jack feels that approach is too risky. For now, he will exit the Win-Spy management console. To exit, he selects "Remote Viewer":



© SANS Institute 2005
Author retains full rights.

He then selects “Close”:



Jack moves the remote installation file, `system.exe`, from his desktop into his `c:\temp` folder. Jack is now ready to secretly place the remote installation file on Dirk’s workstation.

Using the username, password and IP address obtained during his previous social engineering attack, Jack opens a command prompt and establishes a connection to Dirk’s workstation by typing the following:

```
net use * \\192.168.64.132\c$ /user:dsmith diggler
```

The connection is confirmed with the following message:

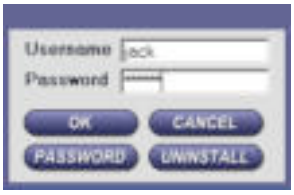
```
Drive F: is now connected to \\192.168.64.132\c$.
The command completed successfully.
```

Jack then copies the remote installation file into Dirk’s Microsoft Windows startup folder:

```
copy c:\temp\system.exe “f:\documents and settings\dsmith\start
menu\programs\startup”
```

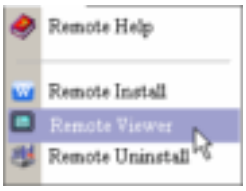
The next time Dirk logs into his workstation, everything in his startup folder, including this remote installation file, will automatically execute. The installation is completely transparent to Dirk, and his antivirus software cannot detect its presence.

The following morning, Jack opens the Win-Spy management console to see what kind of keystroke activity he has captured. He presses Crtl-Shift-F12 to bring up the login screen and then enters his username and password:

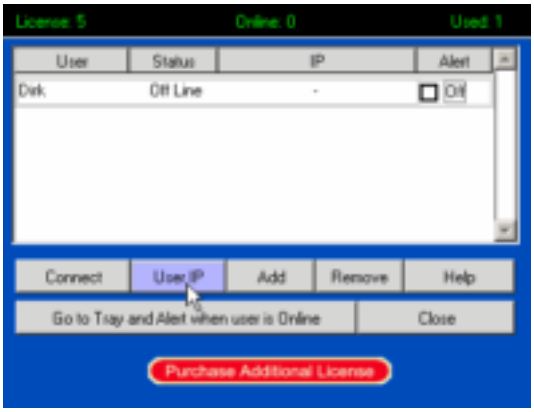


He goes to “Remote / Remote Viewer”.

© SANS Institute 2005
Author retains full rights.

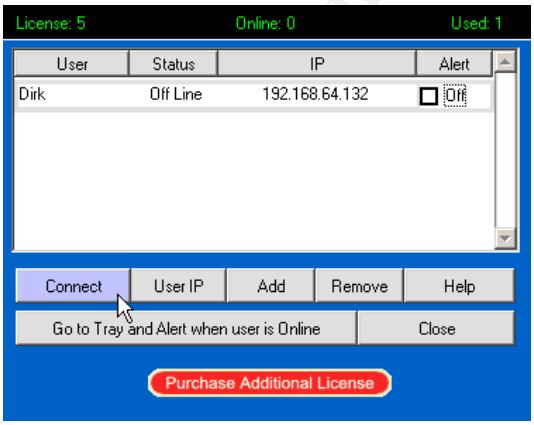


He selects “User IP”:



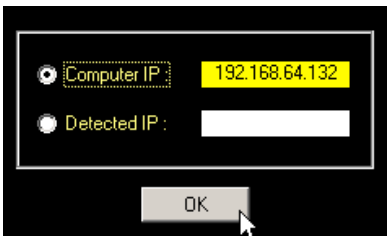
He selects “Static,” enters Dirk’s IP address of `192.168.64.132`, and selects “Save”:

He then selects “Connect”:

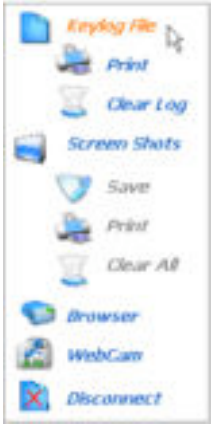


Dirk’s IP address is already highlighted, so he selects “OK”:

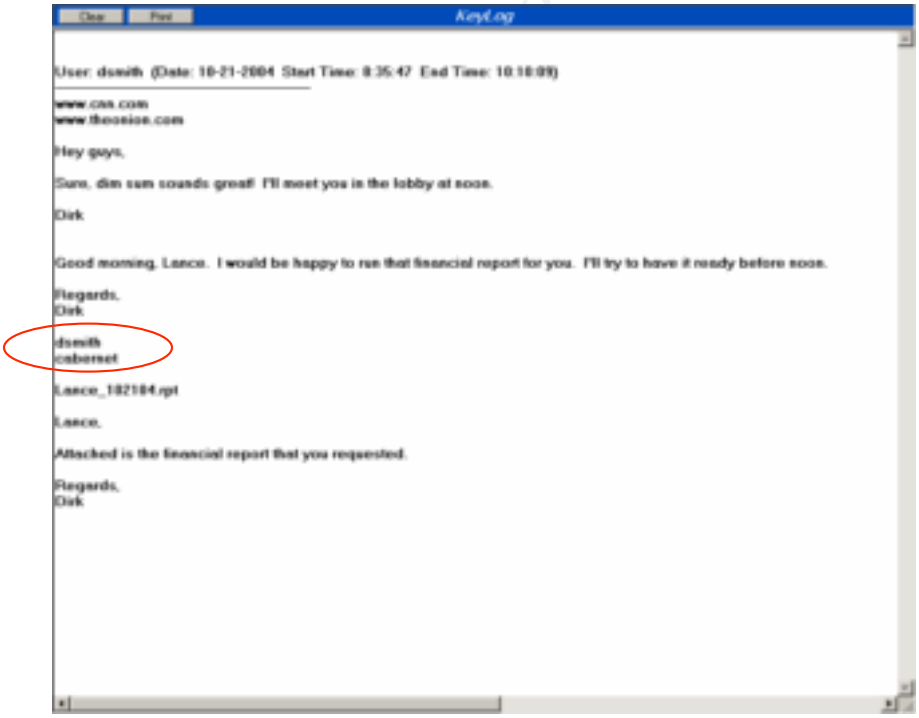
© SANS Institute 2005
Author retains full rights.



From the remote console menu that appears, Jack selects “Keylog File”:

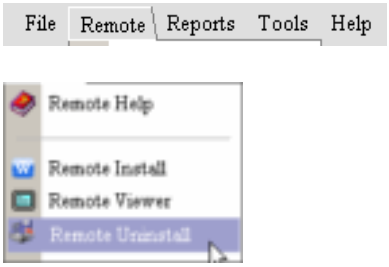


All of Dirk’s keystrokes for the morning have been captured. We can see from the keylog file that after catching up on his favorite news sites, and answering a couple of email messages, he entered a username and password required to generate a financial report. Bingo! Jack now has Dirk’s username and password for the customer database:

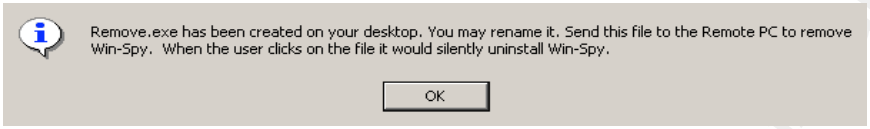


© SANS Institute 2005
Author retains full rights.

Since Jack has successfully obtained the valuable information he was looking for, he is now ready to uninstall the keystroke logger from Dirk's workstation. First, he must create an uninstall file. So, he selects "Remote / Remote Uninstall":



An uninstall file named `remove.exe` has been placed on Jack's desktop:



Jack moves the uninstall file, `remove.exe`, from his desktop into his `c:\temp` folder. Jack is now ready to secretly place the remote installation file on Dirk's workstation.

Jack opens a command prompt and establishes a connection to Dirk's workstation by typing the following:

```
net use * \\192.168.64.132\c$ /user:dsmith diggler
```

The connection is confirmed with the following message:

```
Drive F: is now connected to \\192.168.64.132\c$.
The command completed successfully.
```

Jack removes the remote installation file from Dirk's Microsoft Windows startup folder by typing the following:

```
del "f:\documents and settings\dsmith\start
menu\programs\startup\system.exe"
```

He then places the uninstall file in that folder by typing the following:

```
copy c:\temp\remove.exe "f:\documents and settings\dsmith\start
menu\programs\startup"
```

The next time Dirk logs into his workstation, everything in his startup folder, including this uninstall file, will automatically execute. The removal of WinSpy is completely transparent to Dirk.

And with that, Jack is ready for the next stage of his attack.

© SANS Institute 2005 Author retains full rights.

Citrix GoToMyPC Personal

Now that Jack has acquired the necessary username and password to access the restricted customer database, he is ready to move onto the critical stage of his attack: stealing the company's sensitive customer information. To avoid prying eyes, Jack decides that this stage of the attack should take place after normal work hours. Although Behemoth Enterprises has established a virtual private network (VPN) as the formal remote access solution, Jack knows that VPN access is logged and he wants to avoid detection. So, Jack decides to use a commercial HTTPS tunneling tool instead.

Jack signs up for a free trial version of Citrix GoToMyPC Personal, which is a commercial remote access tool that uses HTTPS tunneling. The free trial includes 60 minutes of connection time, which is plenty of time for him to accomplish the remainder of his attack.

To configure his work computer for remote access, Jack goes to www.gotomypc.com and selects "Try if for Free":

© SANS Institute 2005
Author retains full rights.

Jack enters the name and email address to be used for this account:

Jack enters and confirms the password to be used for this account:

© SANS Institute 2005
Author retains full rights.

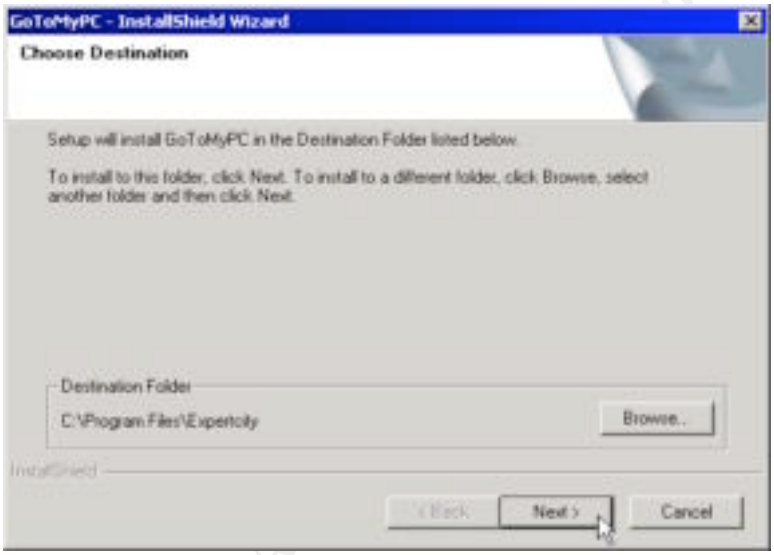
Jack enters his billing information, which is required to establish the free trial, and then clicks “Get Free Trial”:

Jack is prompted to install the GoToMyPC host on his work computer:

© SANS Institute 2005
Author retains full rights.

After accepting a security certificate for the install, the install continues:

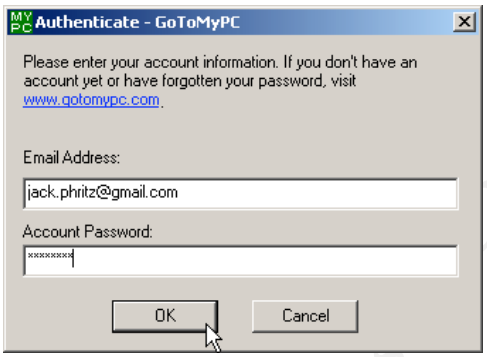
The application is installed into the `c:\program files\expertcity` folder:



© SANS Institute 2005
Author retains full rights.

The following screen is displayed once the installation is complete:

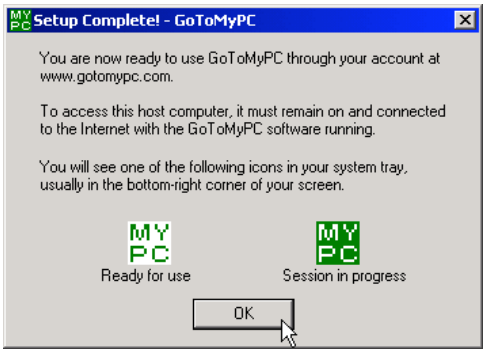
To proceed with the configuration of this host computer, Jack confirms the account information he entered earlier in the installation process:



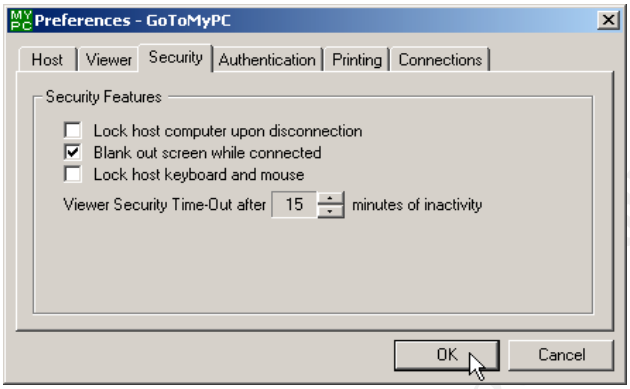
Jack assigns a nickname and access code that will be used to remotely access his work computer:

© SANS Institute 2005
Author retains full rights.

When the installation is complete, the following screen is displayed:



To help avoid detection by any passers by, Jack configures the host system to blank out the screen while remotely connected. He does this by right clicking on the GoToMyPC system tray icon, selecting "Preferences," and then selecting the following option on the "Security" tab:



© SANS Institute 2005 Author retains full rights.

© SANS Institute 2005 Author retains full rights.

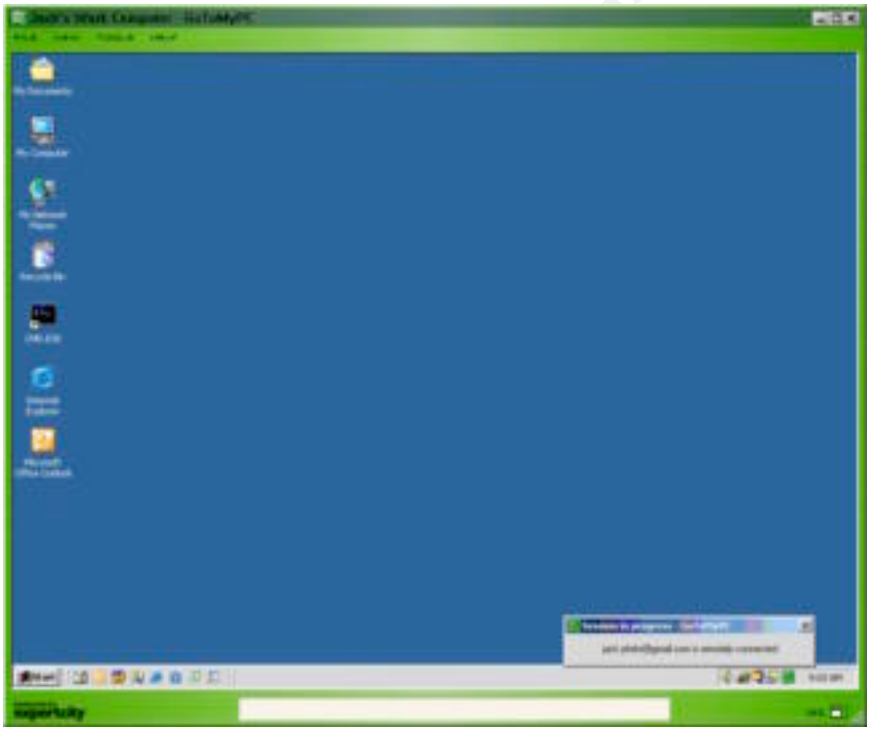
Later that night, Jack prepares for the rest of his attack by feasting on a meal of nitrates, sodium, and preservatives, conveniently packaged in the form of a frozen TV dinner. Once sufficiently energized, he is ready to login remotely to his work computer. From his home computer, Jack goes to www.gotomypc.com and enters the login account he created earlier that day:

He selects the remote computer that he wants to access, "Jack's Work Computer," which is identified by the nickname he created during the host installation process:

© SANS Institute 2005
Author retains full rights.

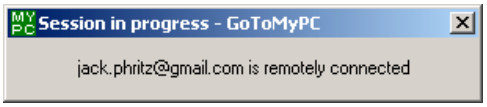
After being prompted to install the viewer client on his home computer, Jack is prompted for the access code:

The communication channel is established, and the desk of Jack's remote work computer is displayed on his home computer:



© SANS Institute 2005
Author retains full rights.

When that connection is established, the following message is displayed on Jack's work computer:



and the following icon appears in the system tray of his work computer:

And with that, Jack has successfully established a remote connection, enabling him to perform any task on the Behemoth Enterprises network just as easily as if he was physically sitting at his work computer.

Keeping Access

Once a perpetrator has gained access, they may take extra steps to ensure that they don't lose the level of access they have already worked to achieve. In our museum example, an art thief might prop open a window or make a copy of a key. In cyber crime, an attacker may take similar steps to ensure that they don't lose access to the system or network they have compromised.

Jack could have created a local administrator account on Dirk's workstation to help him more easily recapture the customer database login credentials in the future. With that administrator account, he could jump straight to the keylogger phase of this attack without having to perform any social engineering. However, because Jack only intends to perform this attack once, he doesn't feel that extra step is necessary. Instead, he decides that his primary goal is to temporarily keep access to the customer database information by making it available to him outside of the organization.

Behemoth Enterprises uses Symantec pcAnywhere as a standard internal remote desktop support solution, so Jack launches that tool to establish a connection to Dirk's computer. Since pcAnywhere is configured to use Microsoft Active Directory for authentication, Jack uses the username `dsmith` and the password `diggler`, which he acquired during the social engineering phase of his attack, to successfully establish a remote connection to Dirk's workstation. Jack then sends a Ctrl-Alt-Del to the workstation and logs in using the same username and password.

Once logged into Dirk's workstation, Jack launches BE Reporter, the custom database reporting tool used by the Finance team. When prompted for a database username and password, Jack enters the username `dsmith` and the password `cabernet`, the credentials he acquired during the WinSpy phase of his attack. The BE Reporter interface is displayed, and Jack is now in the coveted customer database.

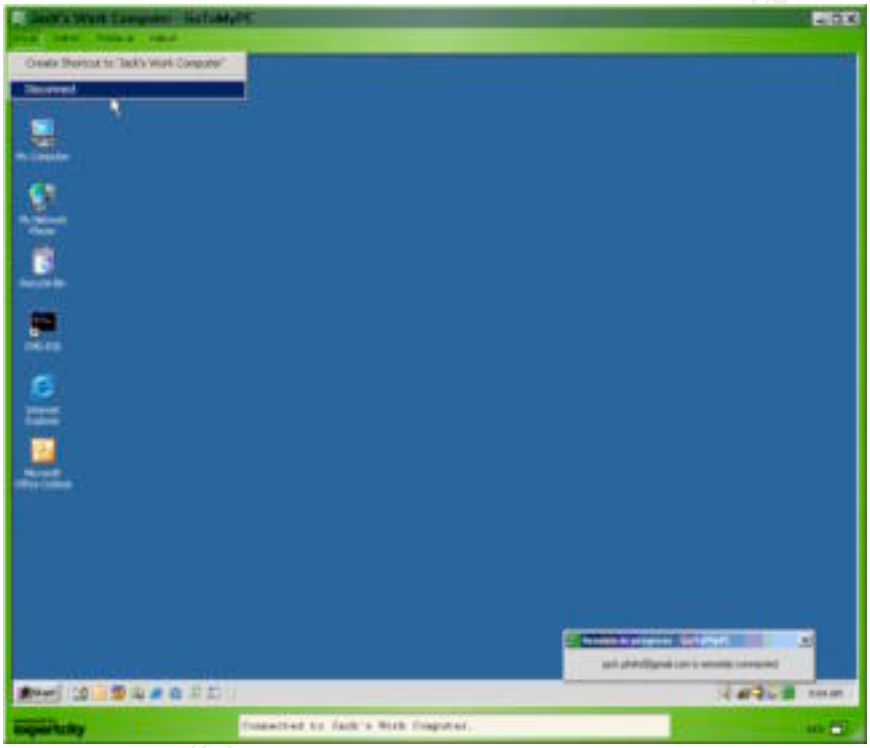
Using BE Reporter, Jack requests a database report for all customers, including name, billing address, email address and stored credit card information. After several minutes, the customer database report is complete and the results are displayed. Because the

© SANS Institute 2005 Author retains full rights.

customer credit card information is not encrypted during storage, Jack is presented with all of the sensitive customer details he requested. Jack exports a copy of the report to Dirk's local desktop in Microsoft Excel format, naming it `behemoth.xls`, and then exits the reporting tool.

Because anonymous FTP servers are often improperly configured to allow write access, Jack and his friends sometimes take advantage of that to share large or questionable files. In this case, Jack will use an anonymous FTP site that he recently discovered to host his stolen customer database report. From Dirk's workstation, he opens the Microsoft Internet Explorer browser and goes to `ftp://ftp.unsecuredsite.com`. He then drags the customer database report into the public directory on that FTP site.

Now that the customer database report is available to Jack from outside of the Behemoth Enterprises environment, he is ready to disconnect. Jack deletes the customer database report from Dirk's desktop, empties the recycle bin, and ends his pcAnywhere connection. Jack then ends his GoToMyPC remote access session to his own work machine by going to the "File / Disconnect" menu:



© SANS Institute 2005 Author retains full rights.

He then logs out of the GoToMyPC website:

From his home computer, Jack logs into various financial message boards and posts the following anonymous message:

```
Behemoth Enterprises
by: Bad_Boy

This customer privacy infringement is provided courtesy of Behemoth
Enterprises.  Enjoy!

ftp://ftp.unsecuredsite.com/pub/behemoth.xls
```

And with that, Jack has made the Behemoth Enterprises customer information available to the public.

Covering Tracks

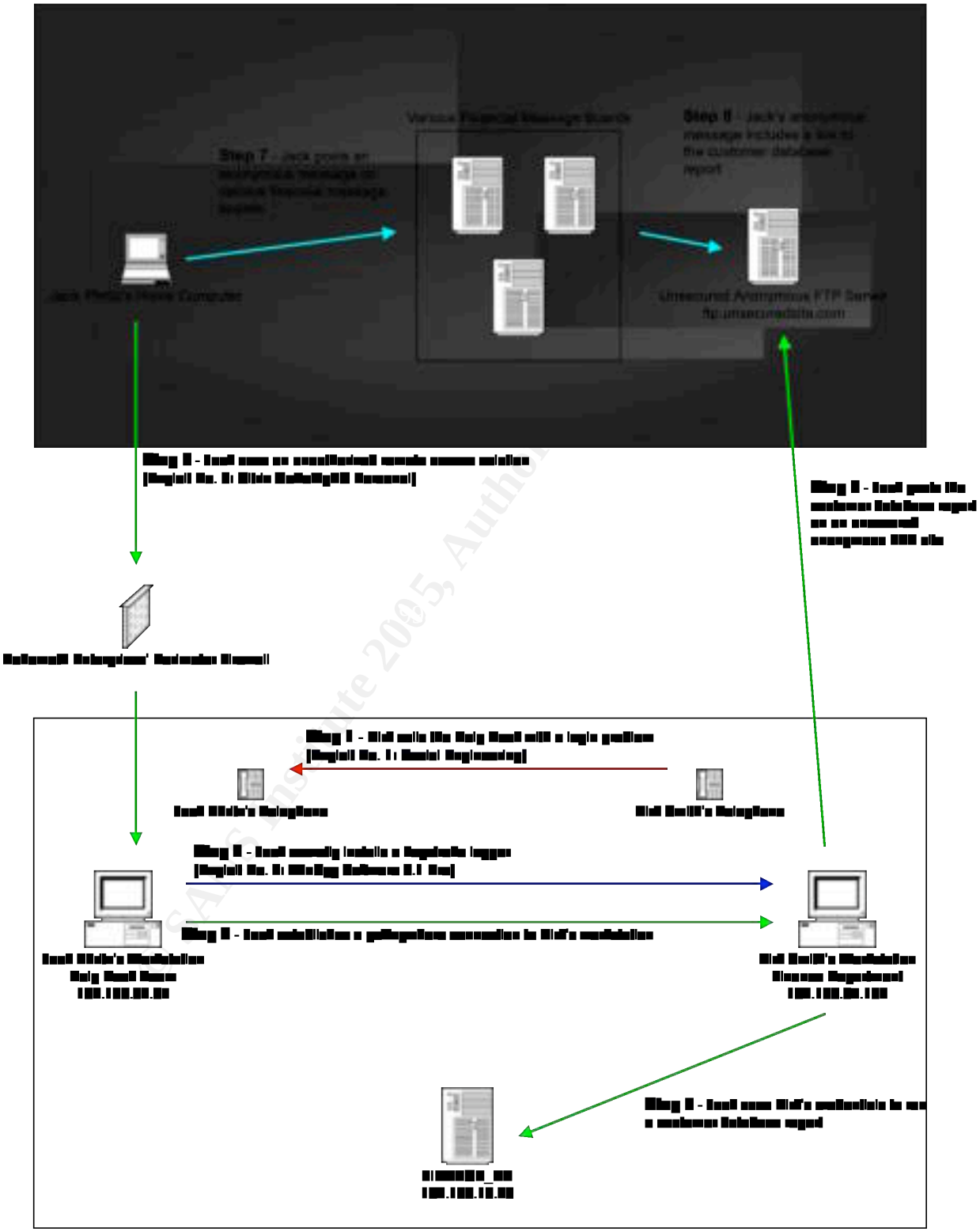
To avoid getting caught, an intruder might cover his tracks. In our museum example, the art thief might wear gloves, wipe his fingerprints off anything he has touched, and remove the videotape from the security camera. In cyber crime, an attacker may take similar steps to cover his tracks.

To avoid getting caught, Jack took several steps to cover his own tracks. After successfully capturing Dirk's customer database login credentials, Jack uninstalled the Win-Spy software application from Dirk's workstation. To prevent his own remote access activity from being logged, Jack used an unauthorized remote access solution, Citrix GoToMyPC Personal, to access his own work computer from home. Finally, because Jack performed the final stage of his attack, including generating a customer database report and posting it to an external FTP site, from Dirk's workstation, he knew that Dirk would be the primary suspect. By covering his own tracks and implicating another employee in the crime, Jack felt that he had committed the perfect crime.

© SANS Institute 2005 Author retains full rights.

Network Diagram

The following diagram illustrates the systems, networks, and eight primary steps involved in this attack:



© SANS Institute 2005 Author retains full rights.

Part Four: The Incident Handling Process

When the museum curator discovers that his prized masterpiece has been stolen, how he responds to that crime is important to the overall outcome. By quickly detecting the crime, calling the proper authorities, securing all doors and windows, and being careful not to destroy any evidence, he can help to improve the success of recovering the stolen artwork, catching the thief, and preventing future incidents.

Similarly, when responding to a cyber caper, the incident handling team will use a series of coordinated steps to ensure the best outcome. Incident handling is the process of preparing for, responding to, and learning from computer or network attacks. The primary steps involved in the incident handling process are: preparation, identification, containment, eradication, recovery, and lessons learned.

Before I detail the incident handling process, let me introduce the lead of the incident handling team: Holly Meister. Like Jack, Holly has been with Behemoth Enterprises for over five years. Unlike Jack, however, her loyalty is unconditional. Her commitment to security and her attention to detail made her the perfect candidate to lead the company's incident handling team.

Preparation

Preparation is the act of influencing behaviors, developing skills and documenting plans prior to an actual security incident. In defending against traditional crime, the museum curator might document physical security policies, train employees on suspicious behavior to watch for, post warning signs to deter theft, install a burglar alarm, and obtain the contact information for the proper authorities to call should an incident occur. By preparing for a theft in advance, the curator will be better able to respond to an incident while under pressure. In defending against cyber crime, an organization can also take a number of steps to protect itself and prepare for the appropriate response to a computer or network attack.

Behemoth Enterprises has already made great strides in protecting their environment and preparing for a cyber attack. Some of the key steps they've taken include the creation of an incident handling team, the implementation of technical and physical security measures, and the publishing of security policies.

<u>Incident Handling Team</u>

The IT Security department has established an incident handling team and appointed Holly Meister the team lead. Holly has established a dedicated core team that acts as the centralized authority on all incident handling issues. The core team manages all procedures, communications, contact lists, and the coordination of all activities that support the handling and resolution of security incidents.

Holly has also established a more dynamic global team that consists of subject matter experts from various support organizations. Those people include onsite system

© SANS Institute 2005 Author retains full rights.

administrators, database administrators, network engineers, and personnel from the workstation support, physical security, human resources, public relations, and legal teams. This global incident handling team will help to identify, resolve and defend against all security incidents as directed by the core incident handling team.

The core incident handling team has developed an enterprise incident handling policy and set of procedures. The Incident Handling Policy states that all system users and support personnel are required to immediately report all suspicious activity or potential security incidents. The team has also established a telephone hotline and team email address to help expedite incident reporting and keep all core team members involved. The policy also states that the primary objective of the incident handling team is business recovery, not criminal prosecution, so containing and resolving an incident is the team's standard approach. Procedures have also been established to help guide communications and keep management informed during all phases of incident handling; drive the actions taken by the global incident handling team to identify, contain, eradicate and recover from an incident; and ensure that all lessons learned during an incident are documented and addressed.

A conference room, affectionately referred to as the "war room," has been dedicated to the incident handling team. This room has a locking door, locking filing cabinets, white boards, speaker phones, and Internet access. Extra incident handling supplies such as policies, procedures, forms, pens, and extra notebooks for documenting the incident details are available in this room. Also available are the software and hardware tools used to support an incident, such as backup media, binary backup software, forensic software, a network hub, patch cables, external hard drives, a bootable CD-ROM, a hard drive duplicator, and a toolkit.

Technical Security

Behemoth Enterprises has taken reasonable steps to secure the company network. Some of the technical security solutions that have been implemented include a firewall, an intrusion detection service, antivirus software, and logon warning banners.

A hardware firewall, a device used to control the type of traffic allowed to pass in or out of a specific system or network, has been implemented at the network perimeter. Only the necessary services used by the organization are allowed to pass through the firewall. Those services include HTTP (port 80), HTTPS (port 443), DNS (port 53), and SMTP (port 25), all of which are used in support of standard and secure web browsing and the transport of company email.

The company uses a third-party network-based intrusion detection service to monitor and report on suspicious activity. This solution is paramount to the early detection of computer and network attacks. This service monitors for known attack signatures, such as the scanning or probing of internal network systems, and alerts the organization's Network Operations Center (NOC) of the suspicious activity.

All systems attached to the company network must run a company approved antivirus software solution with current virus definitions. Because development, test and quality assurance systems are often the source of internal virus infections, the company has

© SANS Institute 2005 Author retains full rights.

specifically stated in its antivirus policy that these systems are not excluded from this requirement.

With the support and approval of the legal department, logon warning banners have been placed on all company systems. The purpose of the warning banner is to eliminate any presumption of privacy on company systems. The warning banner specifically states that the use of company systems may be monitored and recorded, and that their use is limited to activity authorized by the company.

Physical Security

All employees and visitors require an access badge for physical access to the company premises. Behemoth Enterprises has placed security guards and access badge readers at all major entrances. Access badges are used to further restrict access to data centers and other sensitive areas within the company.

The company policy strictly prohibits the sharing of access badges or the circumvention of physical security measures, such as propping open a door or window. The policy also requires that lost or stolen access badges be reported immediately to the physical security team.

Security Policies

Behemoth Enterprises has created a number of security policies that establish accountability and provide clear guidelines for employees. All security policies are published on the company intranet and are accessible to all employees. Some of the most important policies are summarized below:

Password Policy:

- All passwords must be at least 7 characters long.
- All passwords must consist of a combination of letters, numbers and special characters.
- Under no circumstances shall a password ever be shared with another user.

Antivirus Policy:

- All systems attached to the company network must run a company approved antivirus software solution with current virus definitions.
- Development, test, and quality assurance systems are not excluded from this antivirus requirement.

Physical Security Policy:

- All employees and visitors require an access badge for physical access to company premises.
- Access badges shall not be shared under any circumstances.
- Lost or stolen access badges shall be reported immediately to the physical security team.

© SANS Institute 2005 Author retains full rights.

- Doors and windows shall not be propped open under any circumstances.

Incident Handling Policy:

- The core incident handling team is the centralized authority on all incident handling issues.
- The global incident handling team will provide support as directed by the core incident handling team.
- The primary objective of the incident handling team is business recovery, so containing and resolving an incident is the team's standard approach.
- All system users and support personnel are required to immediately report all suspicious activity or potential security incidents to the help desk or incident handling teams.
- A telephone hotline is provided to expedite the reporting of suspicious activity to the incident handling team.

Some incident handling team members argue that the most coveted resource of all is the mini-fridge in the "war room" stocked with Red Bull, Mountain Dew and various chilled coffee concoctions. One thing everyone can agree on, however, is that having all of these policies, procedures and resources in place prior to a security incident are invaluable. It streamlines the overall incident handling process by enabling the team to come together quickly during an incident and focus on the business at hand.

Identification

Identification is the process of discovering that a security incident is occurring or may have already occurred. In our museum example, the following clues might help the museum curator to detect that his prized masterpiece has been stolen or is about to be stolen: a broken window or door handle, the squeal of a burglar alarm, the sound of a car speeding off in the background, an employee's cry of "Stop, thief!", or the empty spot on the wall that the precious artwork used to occupy. In cyber crime, a similar series of progressive clues can help to identify a computer or network attack.

Levels of Detection

In cyber crime, incidents can be detected at the network perimeter, the host perimeter, or at the system level. Detecting an incident at the network perimeter is like catching the art thief while he's picking the lock on the museum door. Detecting an incident at the network perimeter is preferred, because further loss or damage can often be avoided. Firewalls, intrusion detection systems, and other perimeter systems can be used for the early detection of incidents. Behemoth Enterprises uses a firewall and an intrusion detection service to help prevent and detect suspicious activity at the network level.

Detecting an incident at the host perimeter is like catching the art thief while standing in front of the masterpiece, screwdriver in hand, and a gleam in his eye. Software, or personal, firewalls are often used to help prevent and detect suspicious activity at the

© SANS Institute 2005 Author retains full rights.

host perimeter. Personal firewalls are not currently used in the Behemoth Enterprises environment.

Detecting an incident at the system level is like catching the art thief with the prized masterpiece in his hands or discovering the empty spot on the wall where the masterpiece used to reside. Antivirus software, file integrity tools, or a user's own familiarity with the system are often used to help prevent and detect suspicious activity at the system level. Behemoth Enterprises requires the use of antivirus software on all systems.

Reporting an Incident

At Behemoth Enterprises, suspicious activity and potential incidents can be reported to the incident handling team by a variety of sources. The primary reporting sources are summarized below:

System Users:

- A system user is any authorized individual who accesses the company network or computer systems.
- System users might detect the following suspicious behavior: inability to login to an account, new or unfamiliar user accounts, missing or unfamiliar files, new or missing icons on the desktop, the receipt of strange email messages, system crashes, poor system performance, or any other unusual activity.
- Company policy requires that all system users immediately report all suspicious activity or potential security incidents to the help desk team.
- The help desk team will contact the incident handling team when it receives five or more similar problem reports in a 12 hour period, or if any single event warrants more attention.

IT Support Personnel:

- IT support personnel are responsible for the regular support of system users, workstations, servers, applications, and networks. This group includes all system administrators, the network operations team, and the help desk team.
- IT support personnel might detect the following suspicious behavior: inability to login to an administrator account, new or unfamiliar administrator accounts, missing or unfamiliar system files, system crashes, poor system performance, poor network performance, system alarm, intrusion detection alert, time gaps in audit logs, unusual access times, or any other unusual activity.
- Company policy requires that IT support personnel immediately report all potential security incidents to the incident handling team:
  - The Network Operations Center (NOC) will contact the incident handling team when it detects five or more similar network events in a 12 hour period, or if any single event warrants more attention.
  - The help desk team will contact the incident handling team when it receives five or more similar problem reports in a 12 hour period, or if any single event warrants more attention.

© SANS Institute 2005 Author retains full rights.

Vendor Alerts:

- A third-party vulnerability alerting service is used for automatic notification of new vulnerabilities in all software and hardware products used by the company.
- Automatic notification of new exploits, such as viruses, worms, or other malicious code threats, are provided by the company's antivirus vendor.

Intrusion Detection Alerts:

- A third-party network-based intrusion detection service is used to monitor and report suspicious activity to the company's Network Operations Center (NOC).
- The NOC will contact the incident handling team when it detects five or more similar network events in a 12 hour period, or if any single event warrants more attention.

Due to the nature of this attack, the incident wasn't detected until after the damage had already been done and was reported by external sources. On Thursday morning, Holly Meister arrived at work, with her usual large and powerful cup of Peet's coffee in hand, ready to take on the day's challenges. Just a few sips into her coffee, a call came into the incident handling telephone hotline. "Behemoth Incident Handling Team, this is Holly."

"Hi, Holly. This is Robert calling from the Legal department. We've been informed that a number of email messages came into our support and customer service teams this morning, alleging that potentially sensitive customer information has been posted on several Internet finance message boards. Our Vice President of Finance is on his way down to review the situation, and I wondered if you would join us."

Holly took one final and very necessary swig from her coffee, grabbed her incident handling notebook, and headed down the hall to meet Robert.

<u>Establish Chain of Custody</u>

Chain of custody is the process of handling evidence in a controlled, documented and careful manner in order to protect its integrity. To withstand legal scrutiny, such as allegations of evidence tampering or misconduct, all evidence must be under the control of one identified person at all times. Thorough and scrupulous documentation should be kept to track the collection, transfer and storage of all evidence, including the handlers and conditions surrounding those events. Chain of custody is established during the identification phase of an incident and is adhered to through the life of the evidence.

Although Behemoth Enterprises has identified business recovery, not criminal prosecution, as their primary objective and standard approach to incident handling, they still establish chain of custody for all incidents. While the majority of incidents will not lead to prosecution, regularly establishing chain of custody ensures that prosecution is always an option and provides good training for the team. The team is accustomed to

© SANS Institute 2005 Author retains full rights.

taking scrupulous notes in bound incident handling notebooks, and will typically save all evidence for at least one year, storing all physical evidence in the secured cabinets within the "war room."

Initial Assessment

When Holly arrived at Robert's office, Donald Grump, the Vice President of Finance, was already there. Robert showed Holly and Donald several printouts of email messages received earlier that morning. Although the reports came from users of various Internet finance message boards, the posted message in question was always the same:

```
Behemoth Enterprises
by: Bad_Boy

This customer privacy infringement is provided courtesy of Behemoth
Enterprises.  Enjoy!

ftp://ftp.unsecuredsite.com/pub/behemoth.xls
```

After reviewing the `behemoth.xls` file posted on `ftp.unsecuredsite.com` together, Donald confirmed that it appeared to be a legitimate company report generated by their own BE Reporter tool. Based on this initial assessment, Holly declared the situation an incident involving an information compromise.

Due to the potential business impact of this attack, Holly assigned herself as the primary incident handler for the case. While the status of most external attacks was normally communicated out to the global incident handling team, the success of this internal investigation would require more discretion. Holly advised Robert and Donald that she would inform the senior management team of the incident, and recommended that other employees only be included on a strict need-to-know basis. Additionally, when any global incident handling team members are called on for investigative support, only the most senior and trusted individuals will be involved.

After advising management of the situation, Holly returned to the incident handling "war room" to perform further investigation. Meanwhile, Robert and his legal team were tasked with contacting the administrators of the Internet finance message boards and the anonymous FTP site to advise them of the problem, request their assistance in gathering forensics, and get the information removed from public view as quickly as possible. Because the customer database report was posted on an improperly configured FTP server, Holly was able to remove the file just as easily as Jack was able to post it, but first she took the time to capture screen shots and a copy of the report in order to preserve the evidence.

With the help of subject matters experts from the corporate database, networking, and physical security teams, Holly noted the following additional observations and actions taken in her incident handling notebook:

© SANS Institute 2005 Author retains full rights.

- The timestamp on the `behemoth.xls` file posted on `ftp.unsecuredsite.com` was `11/4/04 10:14 PM`.
- The corporate database team reviewed the FINANCE_DB logs and confirmed that a customer database report was generated around that time by user `dsmith` from the IP address of `192.168.64.132`.
- The network team reviewed their logs and confirmed that Dirk Smith had not accessed the network remotely via the company VPN in over a week, and no users were connected remotely after 9:00 PM that night.
- The physical security team generated a report on all access for the last week. Nobody had accessed the building during off hours on the night in question, and nothing about Dirk's schedule seemed unusual.

Based on this initial assessment, it was clear that Dirk's customer database account was used in the attack, but further investigation would be required to determine if his workstation was involved and if he was the actual attacker. Holly updated the core incident handling team, senior management, and her notebook with the current incident status.

Containment

Containment is the process of taking the necessary action to prevent a problem from getting worse. In our museum example, after a theft has been detected, the museum employees might quickly close any doors and windows that have been propped open in order to help prevent further loss. In cyber crime, a similar series of steps can be taken to help prevent further damage from a computer or network attack.

Because Dirk's account has been implicated in this attack, our human resources global incident handling team member will interview Dirk to assess his knowledge of and involvement in the attack. Because it's possible that Dirk's account was compromised, the goal of this initial interview is to gather details, not to accuse Dirk of any wrong doing which might diminish his support for our investigation. He will, however, be advised that he cannot access any company systems until the investigation is complete. Meanwhile, Holly works with the server and corporate database teams to change Dirk's Active Directory and customer database passwords in order to prevent any further unauthorized access.

The backup of all affected systems and log data is essential to preserving evidence. Holly requested that the corporate database, networking, and physical security teams provide full backups of the systems involved in this attack and the log data provided for the investigation. Holly then visits Dirk's workstation so that she can back it up.

Before shutting down Dirk's workstation, Holly first wants to see which processes are currently running. Using her custom CD of incident handling tools, she runs the Microsoft `pulist` and `pstat` resource kit utilities. Holly notes that no unusual processes are running.

Behemoth Enterprises uses hardware drive duplicators for workstation deployment and support, but they also provide a quick and easy way for the incident handling team to

© SANS Institute 2005 Author retains full rights.

backup systems. Because doing a graceful shutdown on a system can update various file access times and destroy evidence, Holly simply pulls the power cord from the workstation. Making a bit-by-bit backup of Dirk's hard drive is then just as easy as attaching it and a blank drive to the duplicator and pressing a button. Holly logs all backups as evidence in her notebook and stores them in the "war room" storage cabinet.

After putting the hard drive back into Dirk's machine, Holly boots up the computer and logs in as Dirk so that she can review the system logs and perform further analysis on the attack. Holly notes the following additional observations and actions taken in her incident handling notebook:

- The workstation IP address is confirmed to be `192.168.64.132`, which is the address that was previously discovered in the customer database logs.
- The workstation name is identified as `FIN_dsmith`.
- By reviewing the Local Users and Groups, she confirms that no new or suspicious accounts exist.
- To help prevent any further unauthorized access to this workstation, she changes the local administrator account password.
- She launches Internet Explorer and reviews the browser history list to find that `ftp://ftp.unsecuredsite.com`, which is where the customer database report was posted publicly, was visited on the previous day.
- In the Microsoft Windows startup folder, she finds a file named `remove.exe` with the timestamp of `11/3/04 10:45 AM`. While it's not clear what this file is, it's certainly not part of the standard company workstation build and is suspicious.
- She examined the Event Viewer Security log and found no failure audits for the logon / logoff category. She did, however, find two success audits for the logon / logoff category that were initiated from another workstation named `HD_jphritz` using the primary user name of `dsmith`. The fact that Dirk's own account was being used remotely is suspicious and requires further investigation.

At this point, it seems clear that Dirk's workstation was used in the attack, but now there is a second workstation that needs to be investigated. Holly takes a break from her investigation to update the core incident handling team and senior management of the incident status.

Because Jack Phritz's workstation appears to be involved in this attack, the human resources representative will interview Jack to assess his knowledge of and involvement in the attack. Because it's possible that Jack's workstation was compromised, the goal of this initial interview is to gather details, not to accuse Jack of any wrong doing which might diminish his support for our investigation. Like Dirk, Jack will be advised that he cannot access any company systems until the investigation is complete.
Once Jack is called away from his computer, Holly moves in to backup his system and perform further analysis on the attack. Holly notes the following additional observations and actions taken in her incident handling notebook:

- The workstation IP address is identified as `192.168.32.87`.

© SANS Institute 2005 Author retains full rights.

- The workstation name is identified as `HD_jphritz`.
- By reviewing the Local Users and Groups, she confirms that no new or suspicious accounts exist.
- In the system tray, she notices the GoToMyPC icon. In the Task Manager, she also finds three unfamiliar processes running: `g2tray.exe`, `g2svc.exe` and `g2comm.exe`. It appears that Jack is running an unauthorized remote access solution.
- On Jack's desktop, she finds two unfamiliar executable files: `system.exe` and `remove.exe`. While it's not clear what these files are, `remove.exe` has the same timestamp as the file found in Dirk's startup folder.
- She launches Internet Explorer and reviews the browser history list to find that `http://www.gotomypc.com` and `http://www.win-spy.com` were visited during the week.
- After further analysis of the Win-Spy tool, it appears that Jack created the `system.exe` and `remove.exe` files in order to perform a remote installation.
- Holly asks the network team to review their logs for any recent activity that might indicate GoToMyPC was used to remotely access Jack's workstation. They discover that Jack's workstation has been sending HTTP "pings" to the GoToMyPC broker site (poll.gotomypc.com) at regular intervals since the previous day. They also notice a large amount of HTTPS traffic that was generated by his workstation from 9:30 PM until 10:30 PM on the previous night.

Holly concludes that Jack connected to Dirk's workstation on Tuesday to install a keylogger tool, that he connected again on Wednesday to uninstall that tool, and that he was remotely connected to his own workstation during the time of the attack. Holly then updates the core incident handling team and senior management with the incident status.

Eradication

Eradication is the process of removing all remnants of an attack and enhancing defenses in order to prevent further exploitation. In our museum example, the museum curator might change all of the burglar alarm codes, check for blind spots in the motion detectors, and hire a security guard to patrol the building during off hours. In order to successfully eradicate a cyber crime, it is important to understand how and why the computer or network attack occurred in the first place.

By using the information gathered during the identification and containment phases, we can try to determine the source and motive of the attack. We have already identified a number of clues, but follow-up interviews with both Dirk and Jack will help to paint a clearer picture of the attack.

By now, it seems clear that Dirk was not directly involved in this attack, and that his password was simply compromised. Although Dirk originally assured the company that he has never shared his password with anybody, when Jack was identified as a possible suspect, Dirk recalled that he worked with Jack earlier in the week to resolve a login problem and did give up his password in the process. While Dirk thought giving his password to support personnel was innocuous, his mistake clearly resulted in a

© SANS Institute 2005 Author retains full rights.

devastating loss to the company. Because Dirk's actions were in violation of company policy, he would be reprimanded. The more serious consequences, however, would be saved for Jack.

After intense interviews with Jack, the company learns that he intentionally targeted Dirk because he got the job Jack had applied for. Jack felt that the company had treated him very poorly by not acknowledging his job application, and posted the customer database report on the Internet in order to get revenge. He didn't think he would get caught, but he also didn't think it was enough to get him in any serious trouble if he did. Jack wasn't surprised to learn that he was being fired from his job, but he was very surprised to learn that the FBI was now onsite. The company decided to contact the authorities so that they could pursue prosecution in this case. The company felt it necessary to make it perfectly clear to their customers and any other would-be attackers that this behavior will not be tolerated.

The following additional steps are taken by the company to eradicate this attack and help prevent future incidents:

- Holly recommends to the Finance team that Dirk's workstation be rebuilt to ensure that no lingering dangers remain. Because the company uses a standard workstation build, this can be accomplished quickly and easily with a hard drive duplicator.
- Because attackers often target multiple machines, all users of the FINANCE_DB customer database are required to change all of their passwords immediately in order to prevent further unauthorized access. Their machines are also checked for the presence of Win-Spy.
- The network team blocks Internet access to the GoToMyPC broker site (poll.gotomypc.com) in order to prevent further unauthorized use of that remote access solution.

By using information gathered during the identification and containment phases, identifying the source of the attack, and enhancing defenses, this attack has been successfully eradicated.

Recovery

Recovery is the process of returning to normal operations and resuming business. In our museum example, recovery might entail the acquisition of a new masterpiece, hosting a new exhibit, and keeping a watchful eye out for art thieves. In cyber crime, recovery includes the validation of all restored systems, putting those systems back into operation, and monitoring to ensure that the problem doesn't occur again.

Recovering from the financial damage caused by Jack could be difficult to impossible for Behemoth Enterprises. Because this attack hurt the reputation of the company and cast doubt on its ability to protect customer privacy, the company could suffer a loss in sales for years to come. In this case, recovery goes well beyond the restoration of systems and into the more challenging realm of regaining customer trust.

© SANS Institute 2005 Author retains full rights.

The first public step the company takes to recover from this attack is a message to their customers via a direct mail campaign and a posting on their website. Per California Senate Bill 1386, any organization that stores the personal information of customers living in the state of California must publicly announce any infringement on the privacy of that data.[12] In addition to meeting a legal requirement, the company public relations department crafts the message as a formal apology and tries to ease customer fears. The company informs the public of the attack, its intentions to prosecute the attacker to the fullest extent of the law, and its ongoing commitment to customer privacy. The company also offers all customers a $20 credit toward their next purchase and to work with any individual who feels that they have been negatively impacted by the attack. Despite the company's quick response to the attack and the fact that usage of the stolen credit card information was minimized, only time will tell if these gestures can salvage the company's reputation and profit expectations.

Because it is no longer "business as usual" for Behemoth Enterprises, the company will more aggressively monitor all systems that have access to or store sensitive data to ensure that this attack isn't repeated. The workstation support team has been tasked with monitoring the access logs on the Finance department workstations. The corporate database team has been tasked with the regular monitoring of the customer database access logs. And the company's intrusion detection service has been expanded to watch for signs of HTTP tunneling, which could provide advanced warning of other potential insider attacks.

Lessons Learned

Applying lessons learned is the act of improving a process through experience. Shortly after any security incident, it is important to develop a follow-up report so that the experience can be captured. By identifying the things that worked well during an incident and those that didn't, the company is better able to validate and enhance their incident handling process.

Holly developed an incident report that detailed the identification of the attack, the steps taken to contain and eradicate the attack, the accomplishments of the incident handling team, and some areas for improvement. She then scheduled a meeting so that all involved parties could review and finalize the report. That discussion included the following process improvements:

- Password Sharing: Even though the company password policy prohibits the sharing of any passwords, Dirk gave his password to Jack without any hesitation. This is a common problem in the company, as various support teams will request this information in order to simplify the support process. All support teams must be reminded that asking any user for his password is a violation of company policy. All employees must be reminded they are ultimately responsible for protecting their own accounts and to never share a password with anybody.

[12] California State Senate (2002)

© SANS Institute 2005 Author retains full rights.

- Password Strength: Despite the fact that company policy requires all passwords to be at least 7 characters long and consist of a combination of letters, numbers and special characters, the company is not currently enforcing that policy via any technical means. Both of Dirk's passwords were weak dictionary words, which provide limited protection for the sensitive data he has access to. Although this weakness was not exploited in this particular attack, the risk has been identified and should still be addressed.
- Remote Access Policy: Although the company has established a virtual private network (VPN) as the formal remote access solution, it doesn't yet have a remote access policy. That policy should clearly state that only company approved remote access software can be used, and that the use of any unauthorized remote access software could result in termination. This policy could help to deter the use of other tunneling software in the environment.
- Workstation Software Usage Policy: The company hasn't yet established a workstation software usage policy. That policy should strictly prohibit the installation and use of any non-authorized software on company systems, which could help to deter the installation of any of the tools used in this attack.
- Limit Administrator Access: The company standard workstation configuration grants all users administrator rights to their own workstations in order to reduce support calls. Jack was able to take advantage of those administrator rights and secretly install the Win-Spy keylogger tool on Dirk's machine. Limiting administrator access to workstations will help to prevent the intentional or accidental installation of malicious code.
- Shutting Down Workstations: The company doesn't have a policy around shutting down workstations at the end of the day. If employees were required to shut down their workstations, it could have helped to prevent the unauthorized remote access during off hours.
- Outsource Credit Card Processing to Merchant Bank: Because there should never be a need for a company employee to retrieve a customer's credit card number, that information does not need to be stored in the customer database. The company should consider outsourcing credit card processing to a merchant bank. This would have prevented Jack from generating such a damaging report, and could help to deter future inside attacks against the customer database.
- Disgruntled Employees: Preventing disgruntled employees is the most difficult aspect of this attack to overcome. Because this attack was based on resentment toward the company, it's important to understand what steps can be taken to prevent similar frustrations. In this case, Jack was frustrated that the only response he received to his internal job application was an automated email response that his resume had been received. He only found out that the job was given to a company outsider by word of mouth. Reviewing the internal job application process and being more sensitive to company insiders could help to reduce employee resentment.

After reviewing the incident report, all parties agreed to the contents and Holly sent the final report to senior management and the incident handling team. The incident handling team will coordinate and implement all areas for improvement as part of the ongoing preparation phase.

© SANS Institute 2005 Author retains full rights.

Conclusion

In 1911, a company insider stole the famed Mona Lisa painting from Paris' Louvre Museum.[13] The thief claimed he stole the painting because he felt that it belonged in Italy, not France, so he took matters into his own hands. Because he was part of the team that originally secured the paintings to the wall, he understood the existing security measures, he was familiar with the museum layout, and he was known by and inconspicuous to other museum employees.[14] This allowed him to move freely around the museum, and ultimately walk away with one of the most famous and coveted paintings in the world.

Companies too often focus on external attacks and ignore the dangers that lie within their own walls. While the reported number of external and internal attacks is fairly even, the cost of a single insider attack is significantly higher at an average of $2.7 million. In this paper, I presented the fictional story of a disgruntled employee who exacts revenge on his employer. Using a combination of social engineering and commercial software tools, I showed you how a disgruntled employee can easily bypass existing security measures and cause costly damage to an employer. While the tools and techniques used in this simulation might normally seem innocuous, they pose a very real risk to any organization and prove that experienced hackers are the not the only threat organizations need to be concerned with.

Establishing an incident handling process and team prior to a security incident is invaluable to an organization. It enables the team to come together quickly during an incident and focus on the business at hand, helping to mitigate the overall damage caused by a computer or network attack. In this paper, I described the incident handling process and how a team can prepare for, identify, contain, eradicate, recover from, and learn from an insider attack. Organizations that are properly prepared for external and internal attacks will experience fewer losses and greater success in the long run.

[13] CBC News (2004)
[14] Euro Art Gallery (2002)

© SANS Institute 2005 Author retains full rights.

References

BC Computing. "Win-Spy Software 8.1 Pro."
URL: http://www.win-spy.com/index.htm (14 October 2004).

California State Senate. "Senate Bill 1386." February 2002.
URL: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html (28 October 2004).

CBC News. "Art Thefts." August 2004. URL: http://www.cbc.ca/arts/features/artthefts/ (7 December 2004).

Citrix Online. "Citrix GoToMyPC Personal."
URL: https://www.gotomypc.com/?Portal=gotomypc (3 November 2004).

Citrix Online. "Citrix GoToMyPC Personal." URL:
https://www.gotomypc.com/ourTechnology.tmpl?SessionInfo=137845987/71277FAFC1E316C/null (5 November 2004).

CNN. "More Employers Taking Advantage of New Cyber-Surveillance Software." URL:
http://archives.cnn.com/2000/US/07/10/workplace.eprivacy/ (16 October 2004).

CSO: The Resource for Security Executives. "Anti-Social Engineering." October 2002.
http://www.csoonline.com/read/100702/machine.html (21 October 2004).

DailyPast.com. "Mona Lisa Painting Stolen From Lourvre, Paris."
URL: http://www.dailypast.com/arts/mona-lisa-stolen.shtml (7 December 2004).

Developer.com. "Backdoors, Back Channels and HTTP(S)." August 2004.
URL: http://www.developer.com/tech/article.php/600451 (15 November 2004).

Distributed Systems Lab. "HyperText Transfer Protocol (HTTP) Tutorial." 2004.
URL: http://www.dslab.tuwien.ac.at/Task_Description/http.html (19 November 2004).

EnterpriseITplanet.com. "An Hour with Kevin Mitnick." March 2004.
URL: http://www.enterpriseitplanet.com/security/features/article.php/3333481
(21 October 2004).

Ernst & Young. "Global Information Security Survey 2003." July 2003. URL:
http://www.ey.com/global/download.nsf/Russia_E/Globla_Info_Sec_03$file/Global_Report.pdf (16 October 2004).

Euro Art Gallery. "Mona Lisa Stolen From the Louvre Museum in Paris." 2002.
URL: http://www.euro-art-gallery.net/topstories/mona%20lisa/Mona_lisa_stolen.htm.
(7 December 2004).

© SANS Institute 2005 Author retains full rights.

Gordon, Loeb, Lucyshyn, & Richardson. "2004 CSI / FBI Computer Crime and Security Survey." June 2004.
URL: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf (16 October 2004).

IBM. "Tunneling Through the Corporate Firewall." July 2001.
URL: http://www-106.ibm.com/developerworks/java/library/j-tunnel/?dwzone=java
(19 November 2004).

Microsoft. "Default Processes in Windows 2000." November 2003. URL:
http://support.microsoft.com/default.aspx?scid=kb;en-us;263201 (2 November 2004).

Microsoft. "Free Tool Downloads."
URL: http://www.microsoft.com./windows2000/techinfo/reskit/tools/default.asp
(1 December 2004).

Mitnick, Kevin. The Art of Persuasion. Indianapolis, Wiley Publishing, 2002. pp. 246 – 249.

Network Magazine. "Special Report – The Pros and Cons of Employee Surveillance."
URL:
http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8703003&pgno=1 (16 October 2004).

PC World. "Fight Back Against Surveillance Software."
URL: http://www.pcworld.com/howto/article/0,aid,114738,pg,1,00.asp
(15 October 2004).

Randazzo, Keeney, Kowalski, Cappelli, & Moore. "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector." August 2004.
URL: http://www.cert.org/archive/pdf/bankfin040820.pdf (24 October 2004).

SecurityFocus. "Data Driven Attacks Using HTTP Tunneling." URL:
http://www.securityfocus.com/infocus/1793 (7 November 2004).

SecurityPipeline. "Email Can Jeopardize Company Security." August 2004.
URL: http://www.securitypipeline.com/29116645 (7 December 2004).

U.S. Computer Emergency Readiness Team (CERT). "Cyber Security Tip ST04-014." July 2004. URL: http://www.us-cert.gov/cas/tips/ST04-014.html (21 October 2004).

U.S. Congress. "Mr. Kevin Mitnick (Testimony to Senate Governmental Affairs Committee)." "Cyber Attack: Is the Government Safe?" March 2000. URL:
http://www.globalsecurity.org/security/library/congress/2000_h/030200_mitnick.htm (17 October 2004).

U.S. Department of Justice. "Kevin Mitnick Sentenced to Nearly Four Years in Prison; Computer Hacker Ordered to Pay Restitution to Victim Companies Whose Systems Were Compromised."
URL: http://www.usdoj.gov/criminal/cybercrime/mitnick.htm (17 October 2004).

© SANS Institute 2005 Author retains full rights.

Wikipedia: The Free Encyclopedia. "Computer Surveillance."
URL: http://en.wikipedia.org/wiki/Computer_surveillance (23 October 2004).

Wikipedia: The Free Encyclopedia. "Social Engineering (Computer Security)."
URL: http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29 (21 October 2004).

World Bank Integrator Unit, The. "The Digital Insider: Backdoor Trojans." URL: http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/TheDigitalInsiderDec2003/$FILE/The+Digital+Insider+Dec+2003.pdf (8 November 2004).

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**