GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

SANS Security Essentials
(GSEC)

Keystroke Logging Investigation

© SANS Institute 2004, Author retains full rights.

Richard Lee

SANS Security Essentials Version 1.4b
Option 2

Submitted: 2004.06.25

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

Keystroke logging tools come in a couple of formats being either hardware or software based. The tools are not inherently bad and can have a positive impact in a security toolkit or they can be a major vulnerability to an individual system or an entire network. I am going to discuss the use of keystroke logging tools in a security program and the action to take upon discovering the use of a suspected keystroke logging software program which is being used maliciously.

The case study is of an individual who was using keystroke logging software to invade the privacy of a former employee. As is often the case the information originated as a complaint from outside the company. Once the complaint was received it became necessary to initiate an investigation into his activities and see if it had been used on corporate systems as well.

Keystroke Loggers in a Corporate Security Tool Chest

Why use a keystroke logger: There are many ways an individual can hide what they are doing on a computer system. These include encryption software such as PGP which makes the information unreadable or steganography tools that hide the existence of the information within other items such as audio files or images. Both of these examples utilize passwords or phrases to unlock the information and make it legible. Sometimes it is necessary to monitor what an individual is doing while at work such as accessing data they are not authorized to view or disseminate. While often their activities can be pieced back together using logs and other investigative techniques if the person is logged onto another server it may not leave artifacts on the workstation. These are all situations where a keystroke logger may be a viable alternative to gather the required evidence of the suspect activity.

The company I work for has over 800 servers running every imaginable operating system and in excess of 5000 desktops running a Windows XP Professional environment which has been significantly locked down for the average user.

It is important to ensure you have the proper authorization before installing any software or hardware device that is capable of capturing what could be argued to be confidential or private information. It is important to have a banner on login that states the company owns the computer equipment, it is for business use and that there is no expectation of privacy. Failure to do so could result in criminal charges. A case in point was reported by InformationWeek on March 24, 2004, “Larry Lee Ropp, a former employee at Bristol West Insurance Group/Coast National Insurance Co. in Anaheim, Calif., has been indicted on federal wiretapping charges for allegedly installing an electronic device on a company PC that recorded every keystroke made by another employee at the company.”

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Ropp claimed to be a whistleblower working on behalf of the California Department of Insurance, a claim which was denied by a representative of the Insurance Department. The Public Affairs Office for the U.S. Attorney, Central District of California, stated that this was the first instance in the United States where a defendant had been charged with illegally using a hardware device known as a keystroke logger.

Keystroke Logger – Hardware: A hardware based keystroke logger is a device which is inserted between the keyboard and the keyboard port on the motherboard. This method requires the surreptitious installation of the device usually after hours when the work area is vacant. This can be a difficult task in an area that is manned 24 / 7. It does have the advantage of not interacting with the operating system and therefore other than examining the cable from the keyboard to the motherboard it is unlikely to be detected. Some of the other advantages and disadvantages include:

Advantages:

- No requirement for a privileged account to install the device.
- Captures and records all keystrokes including BIOS passwords.
- Easy installation, no technical requirements
- Operating System independent
- Not detectable by anti-virus software or other security related vulnerability scanning software.

Disadvantages:

- Require access to the computer system
- Limited storage space dependant on available onboard memory
- Inability to associate a date and time to the keystrokes.

Figure 1 shows an example of a “KeyGhost Security Keyboard” which has the keystroke capture device embedded in the keyboard. The keyboards come in all brand names and the Professional SE keyboard comes with 128 bit encryption and will hold in excess of 2,000,000 keystrokes.



Figure 1

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Figure 2 shows an example of the “KeyGhost SX”, KeyGhost SX 2MB will hold in excess of 2,000,000 keystrokes in its self contained plug. It also uses 128 bit encryption in the storage of its data.

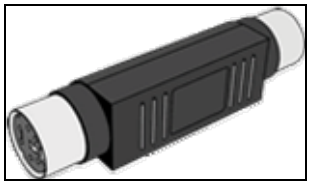


Figure 2

Figure 3 shows an example of “KeyGhost Pro SE 2MB”, which will also hold in excess of 2,000,000 keystrokes and uses 128 bit encryption.



Figure 3

Keystroke Logger – Software: A software based keystroke logger is a program installed onto a computer system that is designed to monitor the behaviour of the user. As opposed to the hardware based device a software based logger can monitor much more than just the keystrokes of the user. Because it is software based and interacting with the operating system it is easier to detect with anti-virus software or other security related vulnerability scanning software. Some of the other advantages and disadvantages include:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Advantages:

- Difficult to detect without specialized software
- Can sometimes be installed remotely
- No physical device to install
- No limit on the size of the log files.
- Log files can be retrieved in a number of ways including: email, ftp or physically from the computer system.
- Numerous types and price ranges
- Date, time and often a program can be associated to the keystrokes.
- Can include other surveillance options such as screen shots taken on a predetermined schedule (i.e. every 5 minutes).

Disadvantages:

- May be detectable by anti-virus software or other security related vulnerability scanning software.
- May require privileged account to install software
- May interfere with in-house or obscure/unusual software causing software conflicts and unexpected error messages or blue screens of death.
- Does not capture keystrokes prior to the startup of the operating system and as a result would not ascertain a BIOS password or Logon userid or password.
- Technical ability may be required to install the software.
- May function differently or not at all depending on the operating system.
- Requirement to know the system it will be installed on prior to arriving at the site.

For more information on Keystroke Loggers you can visit the following sites:

http://www.keyghost.com/ for the Home page for KeyGhost products.

http://www.blazingtools.com/bpk.html will take you to the homepage for Blazing Saddles "Perfect Keylogger."

http://www.pestpatrol.com/Support/About/About_KeyLoggers.asp will take you to the Pest Patrol web page on Keyloggers. This site deals with software keystroke loggers and includes the following:

- Overview of Keyloggers
- Uses of a Keylogger
- How a Keylogger works
- How to find a Keylogger manually

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- How to remove a Keylogger manually
- Matrix: Keyloggers

http://skrasavi.ds.uiuc.edu/Info/Keyloggers.pdf for a paper titled "Keyloggers – content monitoring exploits" by Serge V. Krasavin

http://reviews-zdnet.com.com/4520-6033_16-4206694.html takes you to a ZDNet article titled, "Warning: We know what you're typing (and so does the FBI).

Case Study

Background: Corporate security received information from a local law enforcement agency that it had received a complaint from a female that was being harassed by an employee, hereinafter referred to as the suspect, of the company. The suspect and the female complainant, hereinafter referred to as the victim, had been dating while the victim was an employee of the company. They had since broken off the relationship and the victim was being stalked by the suspect. The suspect had changed some of the victim's passwords for some online accounts. Subsequent to this complaint other complaints were received at Corporate Security about the suspect bothering other female employees of the company.

Initial Response: It was decided by Corporate Security to open an internal investigation file on the suspect and start by taking a forensically sound image of the suspect's corporate workstation. The suspect was a local Administrator on a Windows XP Professional desktop computer. The image was taken surreptitiously after working hours utilizing a hardware write block device and Guidance Software's EnCase Forensic Edition (EFE). The image was then taken back to the Corporate Security Lab where an analysis was initiated using EFE.

The image was added to the EFE case and a keyword search was conducted using the last name of the victim which was very unique. There were in excess of 25,000 hits on the surname. One of the features of EFE is that it allows you to view all of the image files on a system in a "gallery" view. While reviewing the images, several screen shots of the suspect's corporate computer screen were observed. After further examination of the images, numerous screen shots of the victim's computer screen and another unknown individual's computer screen were found.

It was also noted that the suspect was utilizing two email clients. The corporate standard, Lotus Notes, and Mozilla an HTML based client. The mail folder was copied out to an export folder and then imported into Paraben Software's e-mail examiner. One of the emails indicated, "Perfect Keylogger was installed successfully." There were several hundred emails to the suspect's home email

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

account with a subject line of, “Perfect Keylogger report: (followed by a date, system ID and User).”

At this point the investigation branches into a few directions. First, we had to determine what software was being used to capture the victim’s keystrokes. Once that was determined, we had to research the product to determine its capabilities and any artifacts that are left behind to identify its use on a system. Second, we needed to determine if it had been used within the corporation, possibly on the systems of the ladies who had complained about being bothered by the suspect. Third, we had to continue the forensic examination of the suspect’s system to gather whatever evidence could be located which might be used in a court case or arbitration hearing.

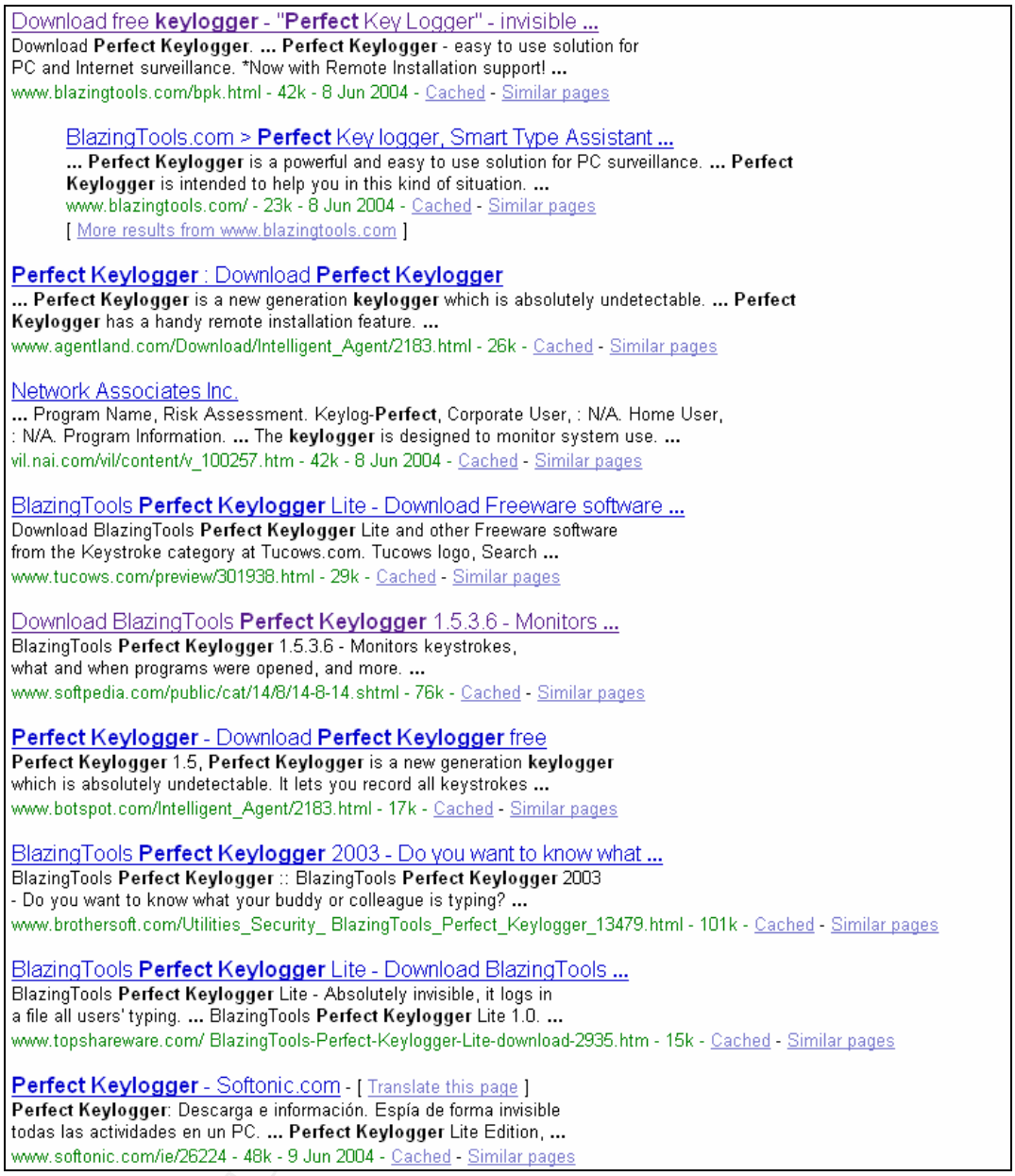
The Keystroke Logger Software: A further keyword search was conducted on the suspect’s computer image using EFE for the keywords: “logger”; “keystroke” and “home08”. “home08” was part of the suspect’s home email account address. There were hundreds of hits on the keyword “logger” which were associated to a program referred to as “Perfect Keylogger.”

It was time to do some research on the Internet. I conducted a Google search on “Perfect Keylogger” and determined it was a product of BlazingTools Software. The results of the search and a couple of the hits have been included as screen shots below (Figures 4, 5 & 6)

In unallocated space on the suspect’s hard drive we discovered a fragment from the purchase of the “Perfect Keylogger” software from BlazingTools Software. It included the following information: License name; license code; order id and cost being $44.90 (US). This showed that he had purchased the full version (while at work on a corporate computer system) and had not downloaded the freeware limited version.

Once it had been determined what software we were dealing with, we needed to carry out some research on the product itself. We started by purchasing the full version of Perfect Keylogger Build 1.5.3.6. We used the following software in our evaluation of Perfect Keylogger: VMware Workstation Version 4.5.1 build-7568; Windows XP Professional Version 2002 Service Pack 1; and InCtrl5 – version 1.0.0.0.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Download free **keylogger** - "**Perfect** Key Logger" - invisible ...
Download **Perfect Keylogger**. ... **Perfect Keylogger** - easy to use solution for PC and Internet surveillance. *Now with Remote Installation support! ...
www.blazingtools.com/bpk.html - 42k - 8 Jun 2004 - Cached - Similar pages

BlazingTools.com > **Perfect** Key logger, Smart Type Assistant ...
... **Perfect Keylogger** is a powerful and easy to use solution for PC surveillance. ... **Perfect Keylogger** is intended to help you in this kind of situation. ...
www.blazingtools.com/ - 23k - 8 Jun 2004 - Cached - Similar pages
[More results from www.blazingtools.com]

Perfect Keylogger : Download **Perfect Keylogger**
... **Perfect Keylogger** is a new generation **keylogger** which is absolutely undetectable. ... **Perfect Keylogger** has a handy remote installation feature. ...
www.agentland.com/Download/Intelligent_Agent/2183.html - 26k - Cached - Similar pages

Network Associates Inc.
... Program Name, Risk Assessment. Keylog-**Perfect**, Corporate User, : N/A. Home User, : N/A. Program Information. ... The **keylogger** is designed to monitor system use. ...
vil.nai.com/vil/content/v_100257.htm - 42k - 8 Jun 2004 - Cached - Similar pages

BlazingTools **Perfect Keylogger** Lite - Download Freeware software ...
Download BlazingTools **Perfect Keylogger** Lite and other Freeware software from the Keystroke category at Tucows.com. Tucows logo, Search ...
www.tucows.com/preview/301938.html - 29k - Cached - Similar pages

Download BlazingTools **Perfect Keylogger** 1.5.3.6 - Monitors ...
BlazingTools **Perfect Keylogger** 1.5.3.6 - Monitors keystrokes, what and when programs were opened, and more. ...
www.softpedia.com/public/cat/14/8/14-8-14.shtml - 76k - Cached - Similar pages

Perfect Keylogger - Download **Perfect Keylogger** free
Perfect Keylogger 1.5, **Perfect Keylogger** is a new generation **keylogger** which is absolutely undetectable. It lets you record all keystrokes ...
www.botspot.com/Intelligent_Agent/2183.html - 17k - Cached - Similar pages

BlazingTools **Perfect Keylogger** 2003 - Do you want to know what ...
BlazingTools **Perfect Keylogger** :: BlazingTools **Perfect Keylogger** 2003 - Do you want to know what your buddy or colleague is typing? ...
www.brothersoft.com/Utilities_Security_ BlazingTools_Perfect_Keylogger_13479.html - 101k - Cached - Similar pages

BlazingTools **Perfect Keylogger** Lite - Download BlazingTools ...
BlazingTools **Perfect Keylogger** Lite - Absolutely invisible, it logs in a file all users' typing. ... BlazingTools **Perfect Keylogger** Lite 1.0. ...
www.topshareware.com/ BlazingTools-Perfect-Keylogger-Lite-download-2935.htm - 15k - Cached - Similar pages

Perfect Keylogger - Softonic.com - [Translate this page]
Perfect Keylogger: Descarga e información. Espía de forma invisible todas las actividades en un PC. ... **Perfect Keylogger** Lite Edition, ...
www.softonic.com/ie/26224 - 48k - 9 Jun 2004 - Cached - Similar pages

Figure 4

© SANS

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

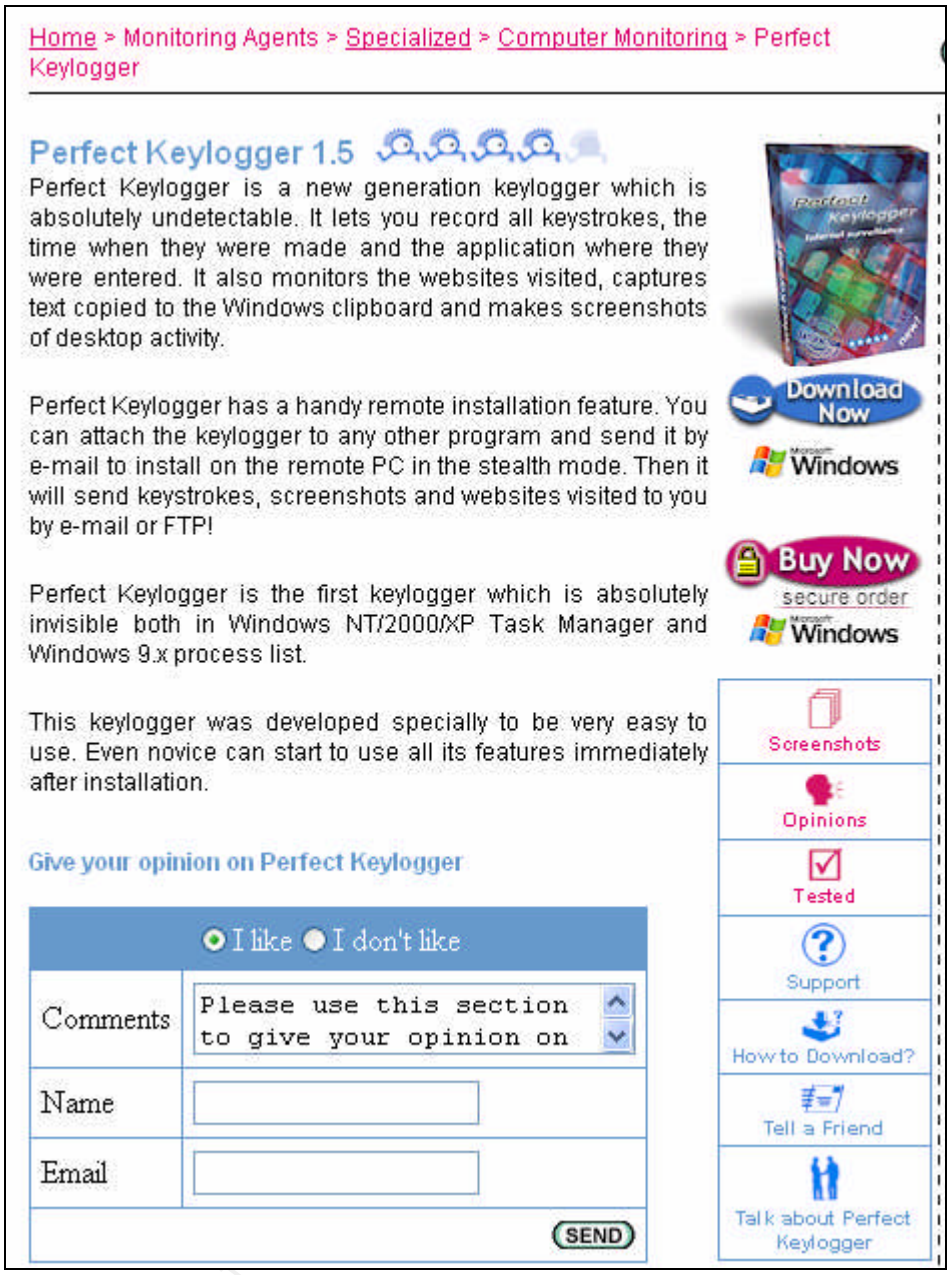


Figure 5

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

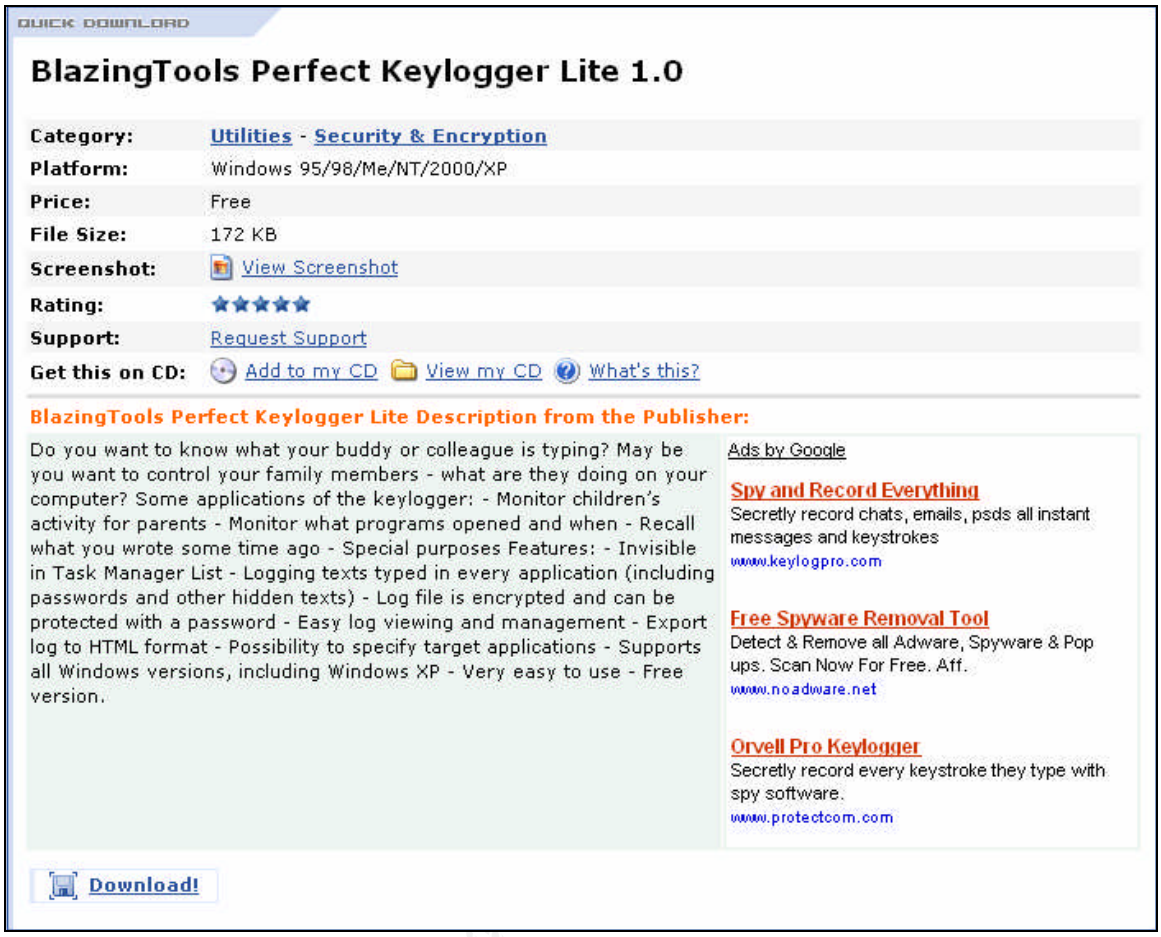


Figure 6

The Research Process: The software was installed on a lab system not connected to the corporate network. This system would be used to evaluate the program and create the remote installation file. The lab system also had a VMware installation with Windows XP Professional as the operating system. This system would be the target system on which the remote installation would take place.

The purchased software was installed onto the lab system. This is demonstrated in figures 7 – 10.

You can see from figure 7 that the remote installation is created using a wizard. Little knowledge is required of the user to create the remote installation deployment package. Tests were conducted creating the package with the host program being an executable file (sol.exe) as well as a power point presentation both with successful installations of the remote package. It should be noted that you have to configure the options on the system where the original installation was initiated. These settings are then used by the remote package.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

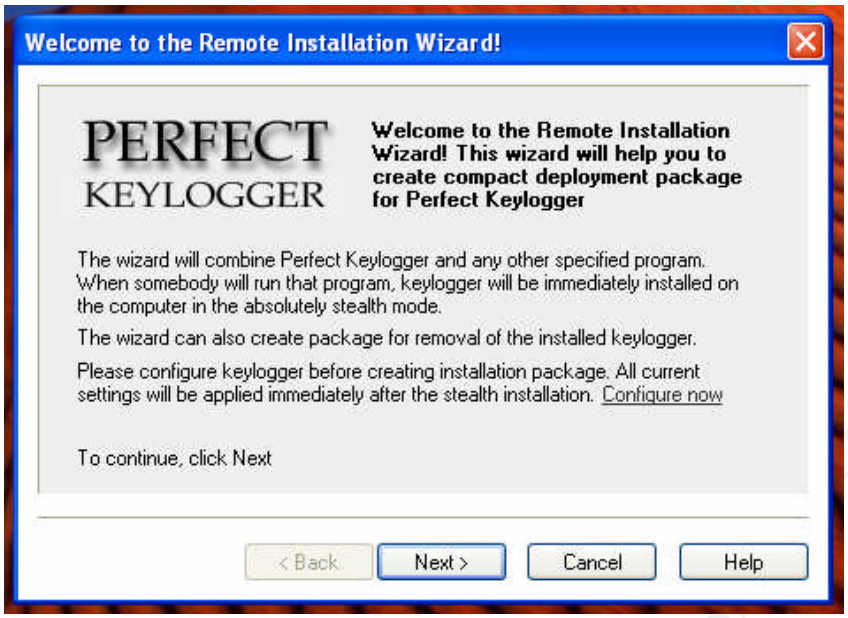


Figure 7

One of the options shown in figure 8 is the ability to have the remote installation email the individual that initiated the remote installation. It also shows the program has been designed to close antispyware programs, antivirus software and firewalls on the startup of the remote package.

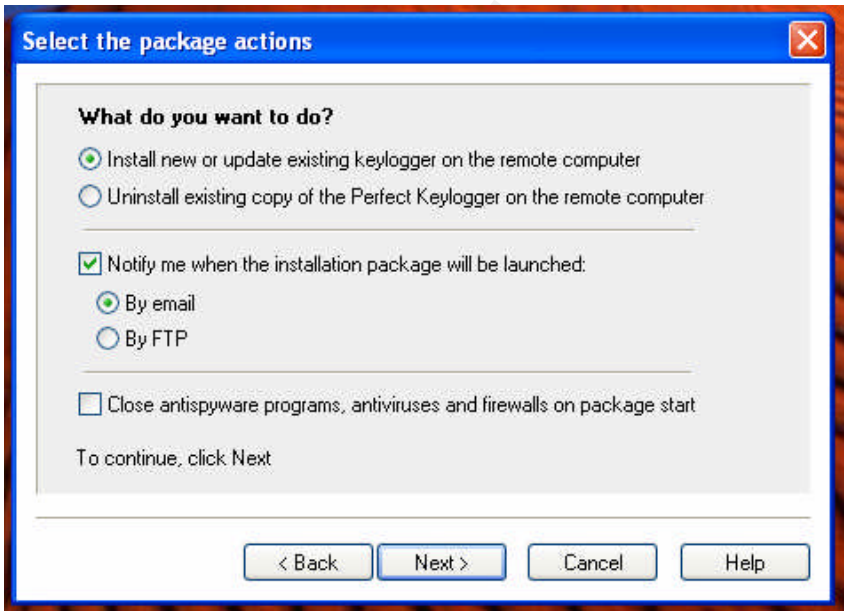


Figure 8

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Figure 9 shows the ability to piggyback the remote Keylogger onto the program of the user's choice. It also allows the installer to place the installation wherever the user chooses and to determine how long the program will remain installed if only a limited installation is desired.

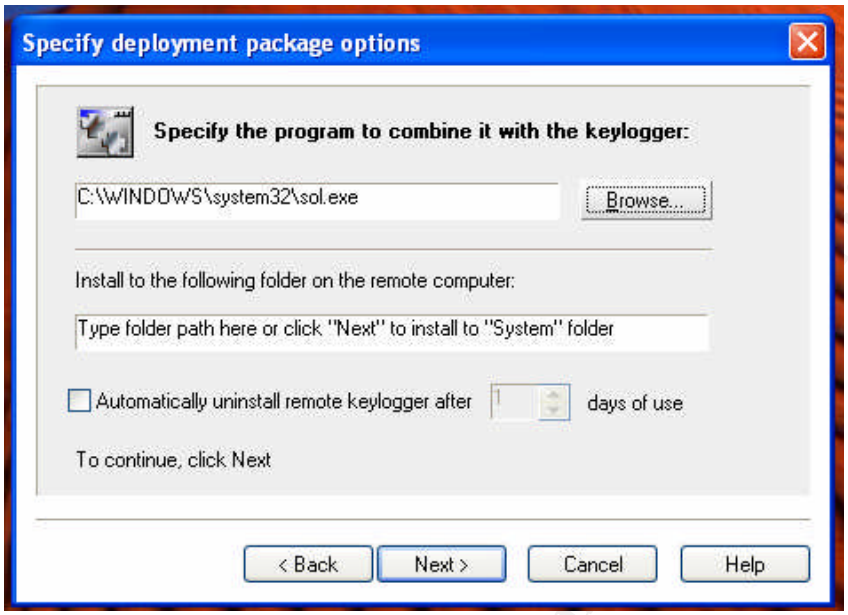


Figure 9

Figure 10 shows the installation package that was created "inst_sol.exe." This is one of the artifacts that can be found on a compromised system. An installation package beginning with "inst_" this can, however, be changed by renaming the file before sending it to the target to be compromised. An informed user would change the name prior to sending it to someone to install on their system. An inexperienced user may send it as it was saved, which, was what happened in this investigation.

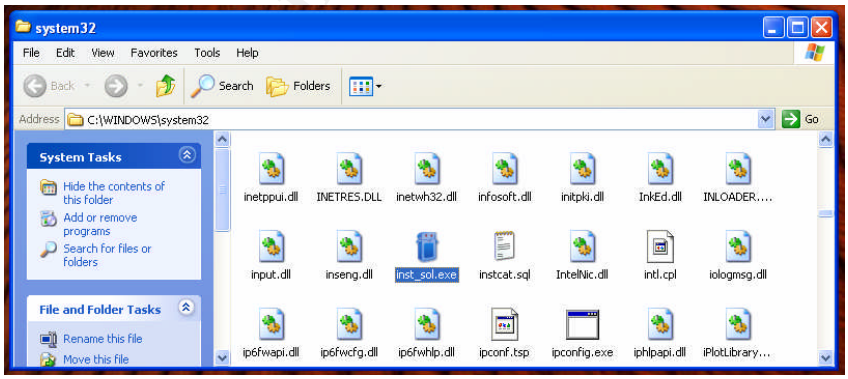


Figure 10

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Figure 11 is the final screen in the creation of the remote installation package and gives the inexperienced user options on deploying the remote package.

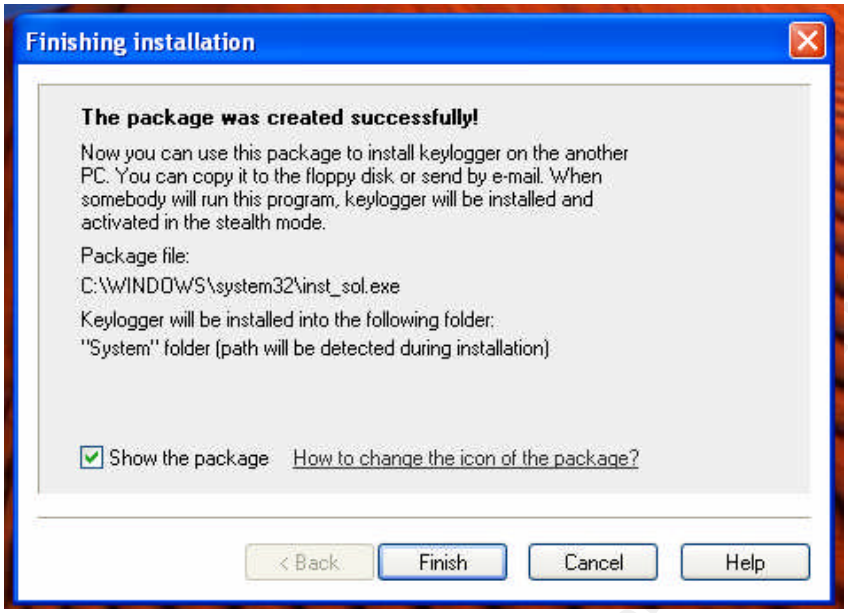


Figure 11

Reading the Help File from the initial installation on the Lab machine shows that Perfect Keylogger can easily be installed on a LAN from the Administrator's PC. The help file takes you through the seven steps including the Registry Keys that need to be created.

Perfect Keylogger's features include:

- Visual surveillance (screen shots)
- Capturing screen information on every mouse click
- Logging text typed into every application or specific applications
- Websites logging
- AOL, ICQ, AIM and Yahoo chat logging
- Clipboard logging
- Sending log and screenshots by e-mail in the hidden mode
- Stealth uploading of logs by FTP using Microsoft's Internet Explorer
- Log file can be encrypted using a password
- Monitoring of all users of the PC, even if you don't know their passwords
- Log can be exported to HTML format
- Supports all Windows versions including XP

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Perfect Keylogger can be fully hidden from the user, including in the:

- List of applications, available if you press Alt+Tab
- Task Manager in Windows NT/2000/XP (also available through Ctrl+Alt+Del)
- Add/Remove Programs List
- Start Menu

E-mailing the captured logs can be done at time frames set by the individual creating the remote installation package. All the information captured can be sent via e-mail using several different options which include:

- Send the log file only when it reaches a certain size.
- Clear the logs after the e-mail has been sent successfully.
- The format of the log files either HTML or encrypted raw log format.
- Perfect Keylogger even recommends free SMTP mail services that can be used with Perfect Keylogger. It should be noted it will not work with Hotmail or Yahoo mail as they do not use SMTP servers.

Perfect Keylogger also allows for ALERTS where you can type in keywords that will trigger an ALERT e-mail whenever the keyword is typed.

Once the remote installation package was created the software was installed in the VMware session on the Lab computer. Prior to the installation the software program “InCtrl5” was installed and run in the VMware session (See Appendices A, B & C for a description of the program and the results of running it during the installation of Perfect Keylogger”).

Once Perfect Keylogger was installed it emailed the fact that it had been installed. See figure 12. It provides the name of the computer, the IP address, the user who installed it and the date and time of installation.

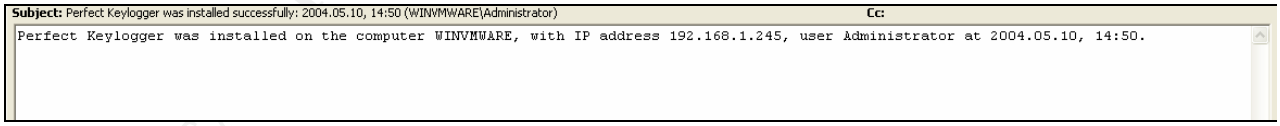


Figure 12

Figures 13 and 14 show some examples of the data sent back to the creator of the remote installation. Figure 13 shows an email with attached log and screenshots.

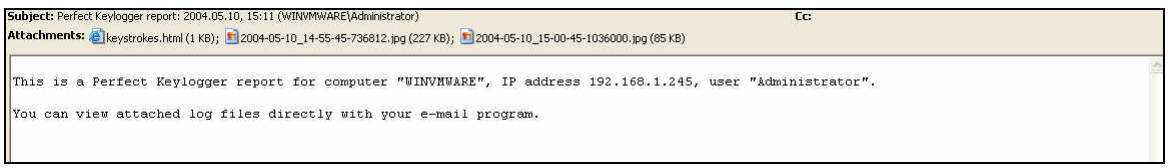


Figure 13

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Figure 14 shows one of the screenshots captured by the software. Note in the top right corner the box which includes the following information: Computer Name, User, Date and Time the screenshot was taken.



Figure 14

It was noted that the software names the screenshot images by the date and time it was taken, in the following format: “yyyy-mm-dd_hh-mm-ss.jpg”

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

We then installed Symantec's Norton Antivirus software into the VMware session to see if the Perfect Keylogger software would be detected, which it was, see figure 15. We also tested to see if it would be detected by Ad-aware 6, which again it was detected.

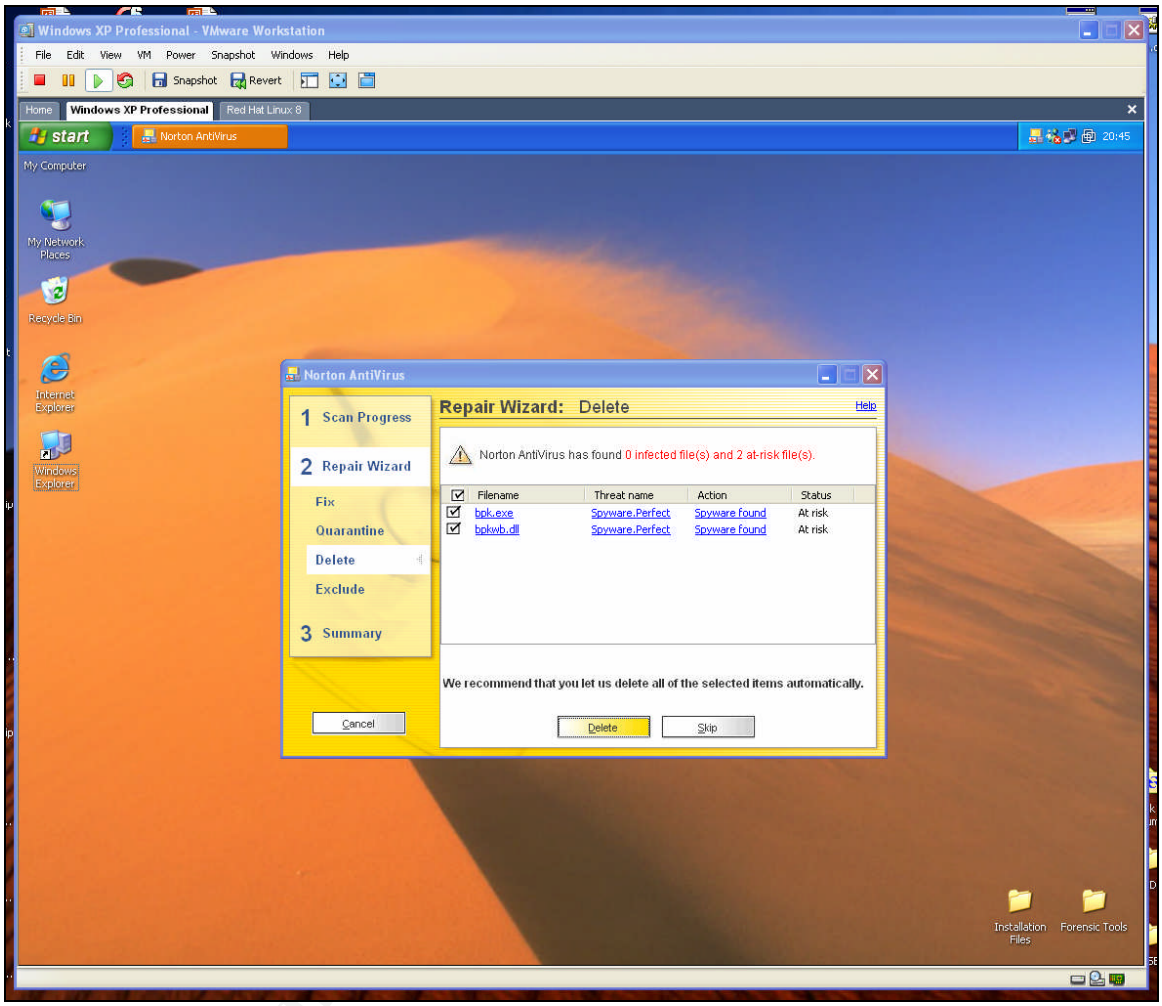


Figure 15

Once we had determined what software was being used and had installed it on a test system and monitored its behaviour for a couple of days, it was determined we would install it on a corporate system to see if it would be detected by our antivirus software. The result of this test was that it was not detected by our antivirus software even though the option to, "Close antispyware programs, antiviruses and firewalls on package start" had not been selected. (This was interesting as this program might then be useful in some corporate investigations if it wasn't going to be detected, without our altering the antivirus software on the desktop)

At this point in the investigation we had to determine if it had been installed on any corporate workstations. Ad-aware 6 was placed onto a couple of USB thumb drives and the computer systems of the female employees who had complained

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

about being bothered by the suspect were checked with Ad-aware 6 after normal working hours. We also checked the computer systems of the suspect's immediate supervisors to see if he might be monitoring their activity. Perfect Keylogger was not discovered on any of these systems. We also previewed one of the systems with EFE to see if any of the artifacts placed on the system by the software were present. This again proved to be a negative search. Our conclusions at this point were that the keystroke software had not been placed on any of the corporate systems by the suspect.

Interestingly several days after the installation of the Perfect Keylogger software onto the corporate system a new version of the antivirus software was distributed throughout the corporation. This version did detect the installation of the keystroke software on the corporate workstation although it could not remove it. After the installation of the new antivirus software no complaints were received by corporate security of any suspicious software in the suspect's work area. This would tend to confirm our belief that it had not been installed on any corporate workstations by the suspect.

Another method of determining if the software was installed on a corporate computer would have included the use of EFE or another tool capable of creating an MD5 Hash and comparing the created hashes to a set of suspect files or file system. I will discuss how it could be completed using EFE. Once we had established which files had been created using InCtrl5, I would image or preview the known system with the suspect files using EFE. I would then locate the files and using EFE create an MD5 hash value of each of the Perfect Keylogger files. I would then use EFE to create a hash set of the files. I could then use EFE to preview a system that I felt might have Perfect Keylogger installed on it and do a hash analysis to see if any of the Perfect Keylogger known hashes matched any of the file hashes on the machine being previewed. **Note:** To do this effectively you would need to do a couple of remote installations using different options to see which files upon installation were always the same. Any change to the file will create a completely different MD5 hash value. If this method is done each time you discover a new malicious tool or unauthorized program on your network, over time you would develop a good set of hash values for use during your forensic examinations including hacker investigations.

The examination of the suspect's computer system using EFE continued. It was determined that the suspect was checking his home email account at the office using his Mozilla software. As indicated earlier the Mozilla directory was copied out of the image and the email account was examined using Paraben Software's e-mail examiner forensic software package. All of the e-mail associated to this investigation and the associated attachments were printed and a thorough examination of the e-mail was conducted including the creation of a time line (The print job filled 3 three inch binders). Through the examination of the e-mail it was determined that another female's, hereinafter referred to as victim 2, computer had the Perfect Keylogger software installed on it and was sending

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

logs to the suspect's home e-mail account. There was a screen shot from victim 2's computer showing an e-mail with an attachment starting with "inst_". Victim 2 was determined to be a friend of the first victim. Although the Perfect Keylogger software had been removed from the suspect's computer during the analysis of his system using EFE the uninstall program was found to still be on the suspect's computer.

Several new keyword searches were conducted using EFE on the image of the suspect's hard drive. These included the following: BPK.EXE, BPKR.EXE, RINST.EXE, INST.DAT, BPK.BIN, KW.DAT, BPKHK.DLL and BPKWB.DLL. All of which are files created during the installation of the software. Using this method we were able to discover in unallocated space the installation date and times for the original installation of the software on the suspect's corporate workstation. This gave us a start date for our timeline. By reviewing the suspect's e-mails and the screenshots and log information from the victim's computers we were able to construct an accurate timeline of the suspect's monitoring of the victims online activities as well as personal items they discussed in their private e-mails or chat conversations. We were also able to find where the suspect had changed several online passwords used by the first victim. He also had enough information to access online bank accounts at two banks where the first victim had bank accounts.

Once we had the electronic evidence, we completed our investigation by contacting the two victims and interviewing them to let them know how much information the suspect had gathered on their online activities. They were encouraged to change all their online passwords.

Conclusion

It was determined through the investigation that the suspect had installed unauthorized software onto his corporate workstation and had used this software to monitor the activities of a former employee. It was also determined that he had not used the software to monitor any corporate workstations. The result of the investigation was that the suspect was terminated from the employment of the corporation and should he grieve his termination we will be well prepared for any arbitration hearing.

The suspect's behaviour in this case was criminal as it was a contravention of Section 342.1(1) of the Criminal Code of Canada which states:

> "Every one who, fraudulently and without colour of right,
>
> (*a*) obtains, directly or indirectly, any computer service,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

(*b*) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,

(*c*) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (*a*) or (*b*) or an offence under section 430 in relation to data or a computer system, or

(*d*) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (*a*), (*b*) or (*c*)

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction."

Section 430(1.1) states "Every one commits mischief who wilfully

(*a*) destroys or alters data;

(*b*) renders data meaningless, useless or ineffective;

(*c*) obstructs, interrupts or interferes with the lawful use of data; or

(*d*) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto."

In this situation we advised the victims of the events that had occurred and the evidence we had in our possession, which if they decided to proceed with criminal charges we would turn over to the appropriate law enforcement agency.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

"About Key Loggers (Key Loggers)." PestPatrol, Inc.
URL: http://www.pestpatrol.com/Support/About/About_KeyLoggers.asp

"KeyGhost – The Hardware Keylogger." KeyGhost Limited.
URL: http://www.keyghost.com/

Krasavin, Serge V. "Keyloggers – content monitoring exploits."
URL: http://skrasavi.ds.uiuc.edu/Info/Keyloggers.pdf

Martin's Annual Criminal Code 2004. Aurora, Ontario: Canada Law Book Inc., 2004

"Perfect Keylogger – easy to use solution for PC and Internet surveillance." BlazingTools Software. URL: http://www.blazingtools.com/bpk.html

Sullivan, Laurie. "Former Insurance Company Employee Indicted As PC Snooper." InformationWeek. 24 March 2004. URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=18401663

Vermosi, Robert. "Warning: We know what you're typing (and so foes the FBI)." ZDNet. 5 December 2001.
URL: http://reviews-zdnet.com.com/4520-6033_16-4206694.html

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix “A”

Overview of InCtrl5

Virtually every modern program has an install utility that installs or updates files, records data in the Registry, and possibly updates INI files or other essential text files. Likewise, modern programs include an uninstall utility that should precisely reverse the effects of the install utility. When a newly-installed program causes existing applications to fail, or when the supplied uninstall utility can't complete its task, you need a record of exactly what the original install utility did. If you use InCtrl5 to track all your installations, you'll have that record when you need it.

InCtrl5 records a "snapshot" of your system before the install utility runs. Afterward, it records another snapshot, compares the two, and reports the differences in HTML format, plain text, or comma-separated values format.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix “B”

Installation Report: i_bpk2003

Generated by InCtrl5, version 1.0.0.0
Install program: C:\Documents and Settings\Administrator\Desktop\i_bpk2003.exe
4.27.2004 10:35 AM

Registry
****

Keys ignored: 0
---
* (none)

Keys added: 5

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Perfect Keylogger
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\

Keys deleted: 4

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\l
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\l
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\l
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\l

Values added: 2

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Perfect Keylogger "DisplayName"
Type: REG_SZ
Data: BlazingTools Perfect Keylogger
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Perfect Keylogger "UninstallString"
Type: REG_SZ
Data: C:\Program Files\BPK\RALun.exe

Values deleted: 5

HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache "@C:\WINDOWS\system32\SHELL32.dll,-9216"
Type: REG_SZ
Data: My Computer
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache "@shell32.dll,-12693"
Type: REG_SZ
Data: Favorites

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache "@shell32.dll,-21785"
Type: REG_SZ
Data: Shared Documents
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache "@shell32.dll,-21786"
Type: REG_SZ
Data: Start Menu
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache "LangID"
Type: REG_BINARY
Data:

Values changed: 3

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\Component Categories\{00021493-0000-0000-C000-000000000046}\Enum "Implementing"
Old type: REG_BINARY
New type: REG_BINARY
Old data: 1C, 00, 00, 00, 01, 00, 00, 00, D4, 07, 04, 00, 02, 00, 1B, 00, 10, 00, 1B, 00, 31, 00, 00, 02, 06, 00, 00, 00, 01, 24, D0, 30, 81, 6A, D0, 11, 82, 74, 00, C0, 4F, D5, AE, 38, 83, 31, 68, 32, A0, 48, 1B, 44, A3, 42, 7C, 2A, 44, 0A, 94, 78, F3, 31, EE, C4, 68, 47, D2, 11, BE, 5C, 00, A0, C9, A8, 3D, A1, 61, 4E, A2, EF, 78, B0, D0, 11, 89, E4, 00, C0, 4F, C9, E2, 6E, 62, 4E, A2, EF, 78, B0, D0, 11, 89, E4, 00, C0, 4F, C9, E2, 6E, 64, 4E, A2, EF, 78, B0, D0, 11, 89, E4, 00, C0, 4F, C9, E2, 6E
New data: 1C, 00, 00, 00, 01, 00, 00, 00, D4, 07, 04, 00, 02, 00, 1B, 00, 10, 00, 23, 00, 04, 00, C8, 03, 06, 00, 00, 00, 01, 24, D0, 30, 81, 6A, D0, 11, 82, 74, 00, C0, 4F, D5, AE, 38, 83, 31, 68, 32, A0, 48, 1B, 44, A3, 42, 7C, 2A, 44, 0A, 94, 78, F3, 31, EE, C4, 68, 47, D2, 11, BE, 5C, 00, A0, C9, A8, 3D, A1, 61, 4E, A2, EF, 78, B0, D0, 11, 89, E4, 00, C0, 4F, C9, E2, 6E, 62, 4E, A2, EF, 78, B0, D0, 11, 89, E4, 00, C0, 4F, C9, E2, 6E, 64, 4E, A2, EF, 78, B0, D0, 11, 89, E4, 00, C0, 4F, C9, E2, 6E
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\Component Categories\{00021494-0000-0000-C000-000000000046}\Enum "Implementing"
Old type: REG_BINARY
New type: REG_BINARY
Old data: 1C, 00, 00, 00, 01, 00, 00, 00, D4, 07, 04, 00, 02, 00, 1B, 00, 10, 00, 1B, 00, 31, 00, 55, 03, 01, 00, 00, 00, 25, 8C, 5C, 4D, 75, D0, D0, 11, B4, 16, 00, C0, 4F, B9, 03, 76
New data: 1C, 00, 00, 00, 01, 00, 00, 00, D4, 07, 04, 00, 02, 00, 1B, 00, 10, 00, 23, 00, 05, 00, 2A, 01, 01, 00, 00, 00, 25, 8C, 5C, 4D, 75, D0, D0, 11, B4, 16, 00, C0, 4F, B9, 03, 76
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG "Seed"
Old type: REG_BINARY
New type: REG_BINARY
Old data: 40, E1, 3A, E2, 51, 1C, 25, 3C, A1, ED, 5F, FE, 7A, E7, FC, 57, BC, 86, 42, 6E, 10, B9, 13, 11, 5A, D7, 40, 1D, 07, 7F, 4C, 8E, BD, 82, 86, 38, 34, 74, 01, 59, E9, 92, D3, DD, 33, 22, C9, 7F, 90, 9D, B8, 0C, A8, 4E, E0, D4, 2F, 9C, 37, 12, 05, 90, 1D, 02, 4E, DC, A2, 72, 8E, D0, B1, 77, 50, 15, 0A, 4C, AD, 14, 2D, DA
New data: 74, 72, 72, ED, 1B, E3, C0, 77, 9C, 25, CC, FF, 60, 64, 18, FA, 34, C9, 07, F5, 31, 8F, 40, B9, 32, ED, BB, 41, AE, 47, 1E, 91, D5, C3, 2C, BD, FA, F6, A4, 1D, 8A, 5B, 8E, D8, CA, 97, DE, D8, C2, 33, AA, DF, 5A, 9F, DD, 4C, 03, 7D, 13, 02, 4E, 75, EA, 0C, 3F, 1E, 9D, D1, 69, 80, 41, 0D, B0, 3E, 79, 49, 4F, 3E, A2, 7D

Disk contents

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

****

Drives tracked: 1
---
* c:\

Folders added: 1
---
c:\Program Files\BPK

Files added: 15
---
c:\Program Files\BPK\bpk.chm
Date: 4.27.2003 6:25 AM
Size: 152,215 bytes
c:\Program Files\BPK\downloads.url
Date: 4.27.2003 6:25 AM
Size: 159 bytes
c:\Program Files\BPK\inst.bin
Date: 4.27.2003 6:25 AM
Size: 39,936 bytes
c:\Program Files\BPK\install.log
Date: 4.27.2003 6:26 AM
Size: 520 bytes
c:\Program Files\BPK\license.txt
Date: 4.27.2003 6:25 AM
Size: 3,215 bytes
c:\Program Files\BPK\order.url
Date: 4.27.2003 6:25 AM
Size: 158 bytes
c:\Program Files\BPK\RAL.exe
Date: 4.27.2003 6:25 AM
Size: 393,216 bytes
c:\Program Files\BPK\RALhk.dll
Date: 4.27.2003 6:25 AM
Size: 8,704 bytes
c:\Program Files\BPK\RALi.dll
Date: 4.27.2003 6:25 AM
Size: 215,040 bytes
c:\Program Files\BPK\RALr.exe
Date: 4.27.2003 6:25 AM
Size: 15,872 bytes
c:\Program Files\BPK\RALun.exe
Date: 4.27.2003 6:25 AM
Size: 40,960 bytes
c:\Program Files\BPK\RALvw.exe
Date: 4.27.2003 6:25 AM
Size: 90,112 bytes
c:\Program Files\BPK\RALwb.dll
Date: 4.27.2003 6:25 AM
Size: 40,960 bytes
c:\WINDOWS\Prefetch\I_BPK2003.EXE-36CBA6DB.pf
Date: 4.27.2004 10:29 AM
Size: 16,830 bytes
c:\WINDOWS\Prefetch\SETUP.EXE-25FFB9EF.pf
Date: 4.27.2004 10:29 AM

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Size: 11,572 bytes

Files changed: 3
---
c:\Documents and Settings\Administrator\ntuser.dat.LOG
Old date: 4.27.2004 10:29 AM
New date: 4.27.2004 10:35 AM
Old size: 1,024 bytes
New size: 1,024 bytes
c:\WINDOWS\system32\config\SECURITY.LOG
Old date: 4.27.2004 10:23 AM
New date: 4.27.2004 10:32 AM
Old size: 1,024 bytes
New size: 1,024 bytes
c:\WINDOWS\system32\config\software.LOG
Old date: 4.27.2004 10:28 AM
New date: 4.27.2004 10:35 AM
Old size: 1,024 bytes
New size: 1,024 bytes

INI file
****

Ini files tracked: 4
---
* C:\boot.ini
* c:\windows\control.ini
* c:\windows\system.ini
* c:\windows\win.ini

Text file
****

Text files tracked: 2
---
* c:\windows\system32\autoexec.nt
* c:\windows\system32\config.nt

InCtrl5, Copyright © 2000 by Ziff Davis Media, Inc.
Written by Neil J. Rubenking
First published in PC Magazine, December 5, 2000.InCtrl5 Report on Installation of "inst_sol"

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix “C”

Installation Report: inst_sol

Generated by InCtrl5, version 1.0.0.0
Install program: C:\Documents and Settings\Administrator\Desktop\inst_sol.exe
6.10.2004 4:43 PM

Registry
****

Keys ignored: 0
---
* (none)

Keys added: 24

HKEY_CURRENT_USER\Software\Microsoft\Solitaire
HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A}
HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A}\InprocServer32
HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A}\ProgID
HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A}\Programmable
HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A}\TypeLib
HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A}\VersionIndependentProgID
HKEY_CLASSES_ROOT\Interface\{1E1B2878-88FF-11D3-8D96-D7ACAC95951A}
HKEY_CLASSES_ROOT\Interface\{1E1B2878-88FF-11D3-8D96-D7ACAC95951A}\ProxyStubClsid
HKEY_CLASSES_ROOT\Interface\{1E1B2878-88FF-11D3-8D96-D7ACAC95951A}\ProxyStubClsid32
HKEY_CLASSES_ROOT\Interface\{1E1B2878-88FF-11D3-8D96-D7ACAC95951A}\TypeLib
HKEY_CLASSES_ROOT\PK.IE
HKEY_CLASSES_ROOT\PK.IE\CLSID
HKEY_CLASSES_ROOT\PK.IE\CurVer
HKEY_CLASSES_ROOT\PK.IE.1
HKEY_CLASSES_ROOT\PK.IE.1\CLSID
HKEY_CLASSES_ROOT\TypeLib\{1E1B286C-88FF-11D3-8D96-D7ACAC95951A}
HKEY_CLASSES_ROOT\TypeLib\{1E1B286C-88FF-11D3-8D96-D7ACAC95951A}\1.0
HKEY_CLASSES_ROOT\TypeLib\{1E1B286C-88FF-11D3-8D96-D7ACAC95951A}\1.0\0
HKEY_CLASSES_ROOT\TypeLib\{1E1B286C-88FF-11D3-8D96-D7ACAC95951A}\1.0\0\win32
HKEY_CLASSES_ROOT\TypeLib\{1E1B286C-88FF-11D3-8D96-D7ACAC95951A}\1.0\FLAGS
HKEY_CLASSES_ROOT\TypeLib\{1E1B286C-88FF-11D3-8D96-D7ACAC95951A}\1.0\HELPDIR
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A}

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Values added: 23

HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\RarSFX0\sol.exe"
Type: REG_SZ
Data: Solitaire Game Applet
HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A} "(Default)"
Type: REG_SZ
Data: IE Plugin Class
HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A}\InprocServer32 "(Default)"
Type: REG_SZ
Data: C:\WINDOWS\System32\bpkwb.dll
HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A}\InprocServer32 "ThreadingModel"
Type: REG_SZ
Data: Apartment
HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A}\ProgID "(Default)"
Type: REG_SZ
Data: PK.IE.1
HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A}\TypeLib "(Default)"
Type: REG_SZ
Data: {1E1B286C-88FF-11D3-8D96-D7ACAC95951A}
HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A}\VersionIndependentProgID "(Default)"
Type: REG_SZ
Data: PK.IE
HKEY_CLASSES_ROOT\Interface\{1E1B2878-88FF-11D3-8D96-D7ACAC95951A} "(Default)"
Type: REG_SZ
Data: IViewSource
HKEY_CLASSES_ROOT\Interface\{1E1B2878-88FF-11D3-8D96-D7ACAC95951A}\ProxyStubClsid "(Default)"
Type: REG_SZ
Data: {00020424-0000-0000-C000-000000000046}
HKEY_CLASSES_ROOT\Interface\{1E1B2878-88FF-11D3-8D96-D7ACAC95951A}\ProxyStubClsid32 "(Default)"
Type: REG_SZ
Data: {00020424-0000-0000-C000-000000000046}
HKEY_CLASSES_ROOT\Interface\{1E1B2878-88FF-11D3-8D96-D7ACAC95951A}\TypeLib "(Default)"
Type: REG_SZ
Data: {1E1B286C-88FF-11D3-8D96-D7ACAC95951A}
HKEY_CLASSES_ROOT\Interface\{1E1B2878-88FF-11D3-8D96-D7ACAC95951A}\TypeLib "Version"
Type: REG_SZ
Data: 1.0
HKEY_CLASSES_ROOT\PK.IE "(Default)"
Type: REG_SZ
Data: IE Class
HKEY_CLASSES_ROOT\PK.IE\CLSID "(Default)"
Type: REG_SZ

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Data: {1E1B2879-88FF-11D3-8D96-D7ACAC95951A}
HKEY_CLASSES_ROOT\PK.IE\CurVer "(Default)"
Type: REG_SZ
Data: PK.IE.1
HKEY_CLASSES_ROOT\PK.IE.1 "(Default)"
Type: REG_SZ
Data: IE Plugin Class
HKEY_CLASSES_ROOT\PK.IE.1\CLSID "(Default)"
Type: REG_SZ
Data: {1E1B2879-88FF-11D3-8D96-D7ACAC95951A}
HKEY_CLASSES_ROOT\TypeLib\{1E1B286C-88FF-11D3-8D96-D7ACAC95951A}\1.0 "(Default)"
Type: REG_SZ
Data: BPK IE Plugin Type Library
HKEY_CLASSES_ROOT\TypeLib\{1E1B286C-88FF-11D3-8D96-D7ACAC95951A}\1.0\0\win32 "(Default)"
Type: REG_SZ
Data: C:\WINDOWS\System32\bpkwb.dll
HKEY_CLASSES_ROOT\TypeLib\{1E1B286C-88FF-11D3-8D96-D7ACAC95951A}\1.0\FLAGS "(Default)"
Type: REG_SZ
Data: 0
HKEY_CLASSES_ROOT\TypeLib\{1E1B286C-88FF-11D3-8D96-D7ACAC95951A}\1.0\HELPDIR "(Default)"
Type: REG_SZ
Data: C:\WINDOWS\System32\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{1E1B2879-88FF-11D3-8D96-D7ACAC95951A} "(Default)"
Type: REG_SZ
Data: PK IE Plugin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "bpk"
Type: REG_SZ
Data: C:\WINDOWS\System32\bpk.exe

Values changed: 2

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections "SavedLegacySettings"
Old type: REG_BINARY
New type: REG_BINARY
Old data: 3C, 00, 00, 00, 17, 00, 00, 00, 01, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 04, 00, 00, 00, 00, 00, 00, 00, 90, C8, 73, EA, 32, 23, C4, 01, 01, 00, 00, 00, C0, A8, 01, F5, 00, 00, 00, 00, 00, 00, 00, 00
New data: 3C, 00, 00, 00, 18, 00, 00, 00, 01, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 04, 00, 00, 00, 00, 00, 00, 00, 90, C8, 73, EA, 32, 23, C4, 01, 01, 00, 00, 00, C0, A8, 01, F5, 00, 00, 00, 00, 00, 00, 00, 00
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG "Seed"
Old type: REG_BINARY
New type: REG_BINARY
Old data: A4, CD, 7E, D2, 99, C4, 25, 74, FD, 88, DC, 1D, C5, D8, F2, 40, 60, 38, C5, B3, F1, 9D, 90, E3, 8A, 9D, 73, 9F, 94, AF, 3D, B3, 14, A9, 8F, 9C, AC, EA, 51, 96, 97, BA, 73, F7, E6, A3, 5E, F3, 1E, 43, A6, 13, 81, 30, 69, 20, 49, E9, B2, B0, 41, 91, 29, 7F, 84, 21, E5, CD, 65, 66, 5A, E2, FA, 54, B0, BF, 71, 32, F2, BC
New data: 40, 84, 41, C6, 35, 49, A5, BD, 3B, 0D, D0, B1, C3, 84, 2D, 82, 09, 66, 0C, 0F, 43, 45, 3D, 3E, 28, 62, B2, FF, 77, F3, 23, B2, 72, 7C, 5E, 8E, CD, 71, CD, 62, 71, EB,

© SANS Institute 2004, Author retains full rights.

6F, 4F, 5D, 75, 3A, A7, CE, 59, 46, 97, D3, 27, 87, E6, 56, 37, F4, 84, C2, 6B, E2, CB, 2C, E3, 95, 5F, D4, 36, 2C, 9A, B6, B0, 53, C5, E8, 7F, C7, 16

Disk contents

****

Drives tracked: 1

---

* c:\

Folders added: 1

---

c:\Documents and Settings\Administrator\Local Settings\Temp\RarSFX0

Files added: 12

---

c:\Documents and Settings\Administrator\Local Settings\Temp\RarSFX0\sol.exe
Date: 8.23.2001 6:00 AM
Size: 56,832 bytes
c:\WINDOWS\Prefetch\BPK.EXE-06BA93D1.pf
Date: 6.10.2004 4:39 PM
Size: 11,162 bytes
c:\WINDOWS\Prefetch\INST_SOL.EXE-1A76F0E8.pf
Date: 6.10.2004 4:39 PM
Size: 19,234 bytes
c:\WINDOWS\Prefetch\RINST.EXE-23998D38.pf
Date: 6.10.2004 4:39 PM
Size: 18,870 bytes
c:\WINDOWS\Prefetch\SOL.EXE-1E26D500.pf
Date: 6.10.2004 4:39 PM
Size: 9,570 bytes
c:\WINDOWS\system32\bpk.exe
Date: 6.10.2003 4:39 PM
Size: 393,216 bytes
c:\WINDOWS\system32\bpkhk.dll
Date: 6.10.2003 4:39 PM
Size: 8,704 bytes
c:\WINDOWS\system32\bpkr.exe
Date: 6.10.2003 4:39 PM
Size: 15,872 bytes
c:\WINDOWS\system32\bpkwb.dll
Date: 6.10.2003 4:39 PM
Size: 40,960 bytes
c:\WINDOWS\system32\inst.dat
Date: 6.10.2003 4:39 PM
Size: 732 bytes
c:\WINDOWS\system32\kw.dat
Date: 6.10.2003 4:39 PM
Size: 10 bytes
c:\WINDOWS\system32\pk.bin
Date: 6.10.2003 12:30 PM
Size: 3,676 bytes

Files changed: 6

---

c:\Documents and Settings\Administrator\ntuser.dat.LOG

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Old date: 6.10.2004 4:34 PM
New date: 6.10.2004 4:39 PM
Old size: 1,024 bytes
New size: 1,024 bytes

c:\Documents and Settings\Administrator\Cookies\index.dat
Old date: 6.10.2004 4:33 PM
New date: 6.10.2004 4:39 PM
Old size: 32,768 bytes
New size: 32,768 bytes

c:\Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat
Old date: 6.10.2004 4:33 PM
New date: 6.10.2004 4:39 PM
Old size: 49,152 bytes
New size: 49,152 bytes

c:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
Old date: 6.10.2004 4:33 PM
New date: 6.10.2004 4:39 PM
Old size: 114,688 bytes
New size: 114,688 bytes

c:\WINDOWS\system32\config\software
Old date: 6.10.2004 3:36 PM
New date: 6.10.2004 4:39 PM
Old size: 11,010,048 bytes
New size: 11,010,048 bytes

c:\WINDOWS\system32\config\software.LOG
Old date: 6.10.2004 4:33 PM
New date: 6.10.2004 4:39 PM
Old size: 1,024 bytes
New size: 1,024 bytes

INI file
****

Ini files tracked: 4
---

* C:\boot.ini
* c:\windows\control.ini
* c:\windows\system.ini
* c:\windows\win.ini

Text file
****

Text files tracked: 2
---

* c:\windows\system32\autoexec.nt
* c:\windows\system32\config.nt

InCtrl5, Copyright © 2000 by Ziff Davis Media, Inc.
Written by Neil J. Rubenking
First published in PC Magazine, December 5, 2000.

© SANS Institute 2004, Author retains full rights.