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
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Serge V. Krasavin

Keyloggers – content monitoring exploits

The risk to communication due to a snoopware is real. In communicating, especially in a de jure secure environment users naturally entrust their sensitive information to computers, so snoopware makes possible to collect information about people or organizations without users knowledge or consent.

Classification

There are many various types of exploits that can infringe on privacy and confidentiality at the machine level. Among them are interceptors, spies, trojans, and web bugs. Their main function is monitoring some kind of user's activity on a computer (for example, typing the text, running the applications, opening an application, Internet activity, etc.).

Such info-gathering products can be classified as *User Monitoring Tools* and as often happens in IT security such products have dual usage: exploits and user monitoring. As expected, there are obvious legal implications with these “dual purpose tools” resulting from their dichotomous nature and intent for application.
There are legitimate and legal uses for this technology. Proponents of legitimate uses for snoopware argue that the software or hardware can help management determine work time consumption on various tasks, projects, or assignments. Some companies specifically state in their IT security policies that these types of monitoring devices are used at the enterprise. Opponents argue that programs like nanny-ware and keystroke loggers prejudge employees and assume the worst about them. The similar views are expressed best on Daniel Data reviews on a hardware keylogger KeyGhost, "...most people who find about KeyGhosts express the opinion that these gadgets are pure concentrated evil in a little beige box. They may express that opinion with a delighted grin, but they express it just the same."[1]

These tools operating in the “man-in-the-middle” mode may be categorized by their implementation on *software and hardware monitoring tools*.

> Several commercial software tools already exist to help companies monitor employee Internet usage. Leading Employee Internet management products include NetSpective Websense SurfControl, SmartFilter CommandView, I-Gear and PC activity monitors and Keyboard interceptors by ANNA Ltd [2]
>
> Most popular hardware monitoring tools are KeyGhost and KeyKatcher which transparently logs the keystrokes of employees as they type away at their desktops [3]

Keyloggers/key recorders/keystroke loggers/key capture programs also belong to the same group of tools that monitor user activity on a machine level. For our purposes

© SANS Institute 2000 - 2005 Author retains full rights.

we will refer to this group as keyloggers.

Problem definition

A typical computer user who has access to the Internet in a public space insecure environment quite often does not realize that whenever she enters her password, credit card information, or other sensitive data, it could be easily captured by a monitoring device or a program installed on the machine. A user in the " de jure secure environment " having a perception of a bona fide security obviously trusts to a machine typing a password on a keyboard. Naturally, there is no way for both types of users to notice a suspicious behavior of a monitoring tool, because most of the applications have been designed to run without attracting the user's attention.

Keyloggers programs and devices present a serious threat to the security of passwords on individual and networked computing systems.

Exploit Description

Features of keyloggers

1. Non-vandals

   Keyloggers as opposite to vandal programs and devices (various nukes, trojans, DOS exploits) are operating in a non-destructive mode.

2. Covert mode of operation

   The main purpose of such exploits is to collect information in a less noticeable fashion. Therefore their presence is seldom detected. The attackers do not want to draw attention to their activities, so stealth, secrecy, and resemblance of computer equipment is vital to the successful use of these programs and devices.

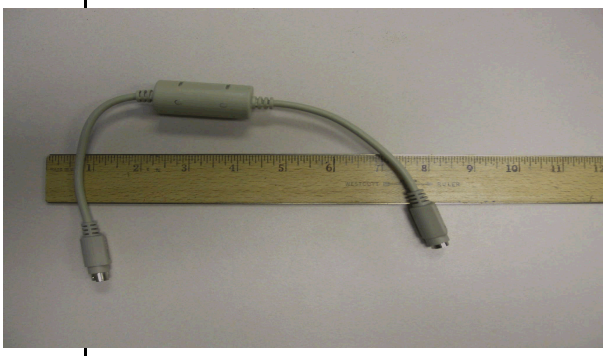
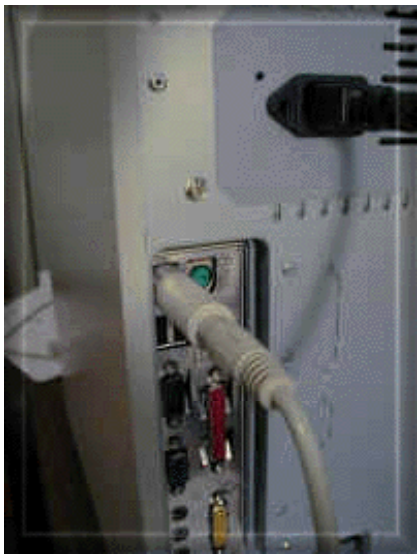
3. User unawareness

   Since there is no clear destruction activity and a clandestine mode of exploit's operation the assaulted parties are not aware of what is going on.

4. Deceptive appearance of hardware keyloggers.

   For unsophisticated user a keylogger looks like a part of an extension cord or a computer part (see pictures). Modified version of KeyGhost KeyGhost II is made injection molded to look exactly like an EMC Balun.

© SANS Institute 2000 - 2005, Author retains full rights.

KeyGhost keylogger 	KeyKatcher keylogger 
Keyboard cable with KeyGhost installed 	Keyboard cable with KeyKatcher installed 
Memory chip of KeyGhost 	

Keyloggers intend to capture users' keystrokes unseen in particular as users enter

© SANS Institute 2000 - 2005 Author retains full rights.

their *password* no matter what level of application is used (encryption application, network access, a company's email system or database fileserver).

Open code/shareware keyloggers

A search in the relatively young days of the Internet back in 1996 showed that a public demand for such tools existed in those days. The earlier keylogger programs presented a slew of programs ready to be used [4]:

> Keycopy, Keyfake, Keyread, Keytrap, Keyrec, Keylogwn(Windows) Hackkey, Bagkeys, Etit, Playback, Robokey, Record,Encore, Kcap10, Ptm229N, Qwertman, GKG, Depl, Maclife (Mac).

Such programs still can be found on any number of ftp and web sites around the world.
Among the latest freeware programs it is worth to note a nice "klogger" written by Arne Vidstrom from NTSecurity.nu (more likely to be used by hackers and penetration testing teams).

The programs with source code can be linked into other programs to make them less obtrusive.

Commercial software keyloggers

One of the better known programs is Invisible Keylogger Stealth (IKS) which is a commercial utility (more likely to be used by employers than hackers)[5]. Invisible Keylogger Stealth for Windows NT by the producer's words is the world's first keystroke recorder that can capture even NT's "trusted path" -- alt-ctrl-del logon. According to the same commercial the program has gained favorable reviews from some of the most prominent security auditors in the business.
The program is based on kernel-mode driver that runs silently at the lowest level of Windows NT operating system. The company assures the user will never find the driver except for the growing binary keystroke log file with your input of keystrokes. All keystrokes are recorded, including the "trusted" alt-ctrl-del NT logon and keystrokes into a DOS box or Java chat room.

Hardware keyloggers

The champions of hardware keyloggers are KeyGhost and KeyKatcher. The have similar appearance and purposes.

An attacker can install such device in less than 10 seconds, no matter what state the computer in - is logged out, password protected, locked or switched off. To install the keylogger the attacker simply unplugs the keyboard cable from the back of the PC, plugs it into one end of the device, then plug the other end back into the PC.

© SANS Institute 2000 - 2005, Author retains full rights.

KeyGhost characteristics

The main features of KeyGhost as advertised by a manufacturer are:

- The device can be installed even when the target computer is logged out, has a password, is locked or switched off.
- The device can be unplugged and the keystrokes retrieved on another computer.
- Over 500,000 keystrokes can be stored with STRONG 128-bit encryption in non-volatile flash memory (same as in smart cards) that doesn't need batteries to retain storage.
- The device works on any desktop PC & all PC operating systems, including Windows 3.1, 95, 98, NT, 2000, Linux, OS/2, DOS, Sun Solaris and BeOS.
- No software installation is needed at all to record or retrieve keystrokes. Recorded keystrokes can be played back into any text editor using proprietary 'keystroke ghosting' technique.
- The device plugs into computers with a small PS/2 keyboard plug or a large DIN plug.
- Unlike software keystroke recorders, KeyGhost records every keystroke, even those used to modify the BIOS before bootup.
- It is impossible to detect or disable using software.

© SANS Institute 2000 - 2005, Author retains full rights.

KeyGhost specification sheet

Model	Capacity	Ghost Playback	Encryption	Compatible with Turbo Download Adapter	Casing / Wh
KeyGhost II Professional SE	2,000,000 Keystrokes	Yes	128 bit	Yes	EMC Balun style

© SANS Institute 2000 - 2005 Author retains full rights.

KeyGhost II Professional	500,000 Keystrokes	Yes	128 bit	Yes	EMC Balun style
KeyGhost II Standard	97,000 Keystrokes	Yes	None	No	EMC Balun style
KeyGhost II Security Keyboard (Pro SE)	2,000,000 Keystrokes	Yes	128 bit	Yes	Inside Keyboard
KeyGhost II Security Keyboard (Pro)	500,000 Keystrokes	Yes	128 bit	Yes	Inside Keyboard
KeyGhost II Security Keyboard (Standard)	97,000 Keystrokes	Yes	None	No	Inside Keyboard

KeyKatcher characteristics

The KeyKatcher is a tiny recording device very similar to KeyGhost that plugs into a keyboard cable. As with KeyGhost it records everything, even BIOS passwords, where software loggers have not even started running yet. Similar to KeyGhost the device does not use system resources. It doesn't require any external power source and it installs in less than 10 seconds. The KeyKatcher records all keystrokes, and stores them in a non-volatile memory. Even if the device is unplugged, or a computer is turned off, the KeyKatcher will continue to store the information. So far KeyKatcher offers only 32,000 keystrokes and 64,000 keystrokes models, which is far less than KeyGhost capabilities.

1. Anatomy of an attack

Simple, Cheap and Effective.

In a nutshell, that is what makes form of attack so devastating.

- No special skills are required.
- The software/hardware is readily available.
- Minimal time of installation/retrieval of valuable data.
- Every keystroke is vulnerable to copying.

© SANS Institute 2000 - 2005 Author retains full rights.

- Very difficult to detect an exploit

The Keyghost plugs between the keyboard and the computer PS/2 (adapters are supplied to work with a large DIN plug). USB keyboards are not currently supported, but the manufacturer will offer USB devices soon.

The recorded keystrokes are opened with any text editor (WordPad, MSWord, Notepad, Pe for BeOS or Emacs for Linux). To access the KeyGhost menu a user types the password without backspace or editing. The device will recognize the password and opens menu in a text editor. The menu looks like this:

KeyGhostpassword

[C] safe mode

KeyGhost II Standard v6.3.8
www.keyghost.com

Menu >

1) Entire log download
2) 2) Section log download
3) 3) Wipe log
4) 4) Format memory
5) 5) Options
6) 6) Optimize speed
7) 7) Password change
8) 8) Diagnostics
9) 9) eXit

Select > 1

\- key to stop –

Keys so far is 128 out of 104672 …

Password information is recorded in the way presented below (user keystrokes are in bold):

User activity	*Screen information*

© SANS Institute 2000 - 2005, Author retains full rights.

	<ON><PWR>
User types <ctr-alt-del>	<PWR><**ctrl-alt-del**>
User types login password	**Wnt24~L4r**
A site URL	**www.americanexpress.com**
User types a user ID	**JohnDoe**
User types a password	**9ltrscr_T**

Every keyboard login procedure can be recorded as well as every form of word-processor application. The keyloggers can be linked to other programs making them more dangerous especially in a "de jure secure" environment. For example an attack could retrieve PGP data which is considered by many a user a secure application. The attacker could capture the user's passphrase or private key or deciphered messages and to covertly write the captured information to a file or send it through a network.

2. Detection

Software keyloggers

a) Local user

How can a user detect a keylogger running on their machine?

- In Windows 9x or Windows ME, there is a standard method to examine the Task list <CTRL+ALT+DEL>, which shows all processes currently running on the machine. Another command, the system configuration utility MSCONFIG <START- RUN -MSCONFIG>, opens start up options and loaded programs.
- In Windows NT the Task Manager is the standard way to check new applications running.

However, it is possible to design a program that would take advantage of a valid process name in the Task List that in reality is nothing more than a malicious keylogger program. For example scheduling agent MSTASK.EXE is a normal windows command, but an adversary might have installed a keylogger and renamed it as a scheduling agent.

- Another way to detect a keylogger program is to check the registry. For example Invisible Keylogger Stealth writes into NT's registry.

© SANS Institute 2000 - 2005, Author retains full rights.

Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\iks
Name: DisplayName
Type: REG_SZ
Value: IKS
Name: LogName
Type: REG_MULTI_SZ
Value: \%SystemRoot%\iks.dat

The IKS documentation gives instructions on how to hide this "red flag". Even with values changed and the key name IKS changed, search for the key "LogName" under Services will result in IKS's footprint.

- Commercial Security analyzers are reliable in detecting keylogger software programs. In our tests WebTrends Security analyzer gives the following warning on installed KeyKey keylogger program and offers fixes:

 **High - Unauthorized program in Run key / C:\WINNT\System32\loadkk.exe**

 localhost (xxx.xxx.xx.xx)

A potentially unauthorized program was found in the Run key on the computer. The Run key defines programs to be run at startup. Programs started from the Run key in the registry can be easily hidden from the user, and they will not be displayed in the Startup folder. The program could be a Trojan horse, exploit, or back door access program.

 **Fix - Remove program from the Run key**

If the program is unauthorized, it should be removed from the Run key.
To remove this application from the Run key in the registry, edit the following registry key value:
Hive:*HKEY_LOCAL_MACHINE*
Key:*SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
There may be several values listed under this key. Review the values and ensure that they are all authorized programs. Delete the entry for any unauthorized programs. If there are authorized programs that you would like this test to recognize as safe programs, you can edit the properties for this test by editing your test policy.

 **High - Unauthorized keyboard driver / KeyKey**

 localhost (xxx.xxx.xx.xx)

An unauthorized keyboard driver was detected on the host.
Keyboard drivers have access to all keyboard activity. An unauthorized keyboard driver can be used to collect any data entered at the keyboard, including passwords or credit card numbers."

© SANS Institute 2000 - 2005, Author retains full rights.

- Natural way for detecting a keylogger activity is to check the file size of all running tasks, since the keylogger usually writes captured information into a log file (the date would be easy to spoof as well). However, in the network environment the best way disguising a keylogger would be to store the obtained data remotely, on a network drive, thus the file size of all running tasks will keep default.

b) Network user

- Personal firewalls are good ways to detect network keylogger activity. Keyloggers usually don't fit the common detection profiles and be forced by a firewall to ask for permission to use the Internet.
  However, some programs may use the old disguise technique to use a valid application name, for example to register themselves as browser helper apps, which would then have the same permission as the browser to use port 80.
  The way to catch such a program in the act would be to deny all Internet access with a personal firewall, then use your system and see what happens.

- Another way to catch keylogger programs is with a packet sniffer/analyzer. There are a number of shareware analyzers for example a "analyzer “that will capture packets a computer sends and receives on the LAN [6]. Packet analysis can be used to scan packets for unfamiliar IP addresses and look for things a user has typed in the payload portion of the packets.

One of the popular keyboard monitors is WinWhatWhere Investigator[7]. It can be detected by a new program offered by WinWhatWhere Corporation This program detects only the unregistered version of Investigator.

Hardware keyloggers

Technically it is possible to detect a hardware keylogger by comparing consumption of the sleep mode to the average of the current consumption of the circuit for periodic events, like key detection/event detection/data logging and any other application that only requires periodic intervention by the microcontroller. However, implementation of such detection system will cost much more than a keyboard replacement.

3. Defense

Defending against software keylogger attack falls into the category of defending against viral infection generally. There are some capable antiviral/security analyzers products commercially available, and there are hygienic procedures to follow that can greatly reduce the chances of an infection.

© SANS Institute 2000 - 2005 Author retains full rights.

Is it possible to build a sufficient defense against a hardware keylogger? Theoretically yes. A similar approach used in cryptanalysis will be applicable to define an anti hardware keylogger strategy. Quite often crypto algorithms are designed using a worst-case scenario. The same scenario in a keylogger case would be an assumption that every signal traveling from/to the keyboard keys to a box is logged. Thus the defense strategies will constitute the following:

A. Noise

It is advised to program the PCs 8042 keyboard controller to send a status requests to the keyboards internal microprocessor. In case of a software keylogger such requests will immediately flag a dramatic change in a log file, which is easy to detect. In hardware keylogger case the noise will "quickly" fill up the keylogger memory. If the device has enough memory to record the megabytes of "noise" status info going back and forth, and the keystrokes, it would take enough of attacker's time to figure out where one status command ends, and a keystroke begins, and then how many hundred/thousand/million bytes that follow are more status responses before the next keystroke... However, a filtering program separating status noise and keystrokes will dramatically decrease attacker's time.

B. Keyboard configuration

PS/2 style keyboard microcontrollers support 2 other keyboard modes that PCs never use, so the random intermix of the modes will distract the hardware logger from recording the right scancodes for the keys pressed - if they even made it compatible enough to record those other modes in the first place, which is quite unlikely.

C. Avoidance of using typed passwords

For authentication purposes, instead of typing a password a user may utilize various authentication methods:

- Tokens (smartcards)
- Bioscanners
- Screen password

Development and implementation on a wide scale of new authentication techniques such as smart cards and bioscanners (retina, skin, and voice authenticators) will eventually decrease possibility of password logging procedure breach. However, now it is too early to consider implementation of such technologies at substantial scale.
A personal assistant device could be used to write the password on it and transfer to the computer in some encrypted way.
A slow, but effective method would be display a keypad and have a user to select a passphrase by clicking it in. However, it could be overseen, and

© SANS Institute 2000 - 2005, Author retains full rights.

tempest-attacked.

4. Physical security

The most efficient way to defend against a hardware keylogger is to use some sort of physical security preventing an adversary to gain access to keyboard-machine connection. Evidence tapes[8] on the back of machine and/or secure cover or a lid are examples. Of course this can be circumvented, but at least the work and time factors are on the administrator side.

The taping solution should not be seen as an easy panacea, after all what would prevent a malicious party to photograph the computer's sealed keyboard to replace with identical tape upon completion of the operation.

Recommendation

So far that is a losing battle. On Windows, there will *always* be a way to design a keylogger to get around whatever software protections anyone might put in – and if there wasn't then there are always hardware based keyloggers.
Once a trojan code, through physical security weaknesses or network security weaknesses, is allowed to run on the system, the battle is lost.

As of August 2001 no commercially available software is 100% effective against hardware keystroke logging. Thus we must rely upon the standard IT Security methods and procedures at least to reduce exposure.

The best and apparently the only way to prevent using of a keylogger is a combination of physical security of a computer box with enforcement of standard desktop security practices restricted a user to install new software.

- Physical security
  - Morning check of a keyboard cable
  - Physical protection to the back side of a machine box (special covers, evidence tape, etc)

- Software checking
  - A virus checker/security analyzer with updated definitions.
  - A properly configured software inventory program with alerting capability.
  - A file size checking programs.

- Never stay confident in your measures.

© SANS Institute 2000 - 2005 Author retains full rights.

Appendix

---

[1] KeyGhost review http://www.dansdata.com/KeyGhost2.htm 09.09.01

[2] Employee management products

NetSpective (www.telemate.net), Websense (www.websense.com), SurfControl (www.surfcontrol.com), SmartFilter (www.securecomputing.com), CommandView (www.elronsoftware.com),I-Gear (www.symantec.com), products by ANNA Ltd http://www.keyloggers.com/, http://www.softsecurity.com. 09.09.01

[3] Most popular hardware keyloggers are KeyGhost http://www.KeyGhost.com/ and KeyKatcher http://www.gadgets-inc.com/KeyKatcher_32.htm, http://www.electronickits.com/spy/finish/computer/key.htm 09.09.01

[4] Keylogger search. http://www.seds.org/pub/seds/SEDS-L/1996/seds-l.log9606b 09.09.01

[5] IKS program. http://www.amecisco.com/, 09.09.01

[6] Protocol analyzer www.hotfiles.com 09.09.01

[7] WinWhatWhere Investigator http://winwhatwhere.com/ 09.09.01

[8] Sealing keyboards with special tapes http://www.teamlogisticscorp.com/cgm08.htm 09.09.01

Additional information on Keyloggers

Keyloggers

The "Mouse and Key Recorder" can record, then replay, mouse clicks and key strokes, in any Windows application. http://www.kratronic.com/recorder/ 09.20.01
Stealth keyloggers and security program that tracks and reports all activity on user's PC http://www.geocities.com/SiliconValley/Hills/8839/index.html 09.20.01

With this ActiveX control, a user can easily make a key logger. http://dewasoft.com/OCX/KeyLog/KeyLogAX.html 09.20.01

Key Logger Based on a Global Keyboard Hook http://www.freevbcode.com/ShowCode.Asp?ID=728 09.20.01

OXD Software KeyLogger v1.0 http://www.oxdsoftware.com/keylogger.htm

© SANS Institute 2000 - 2005 Author retains full rights.

09.20.01

KeyKey http://pc-spy.com/software/?hop=serpant.pcspy 09.20.01

Detection

PC Door Guard a full-featured extensive and thorough intrusion scanner that scans any media on a PC for backdoors and trojan horses. http://www.astonsoft.com/index.htm 09.20.01

Stealth keyboard interceptor. Software with stealth keystroke logging capabilities and invisible transmission of log file to a pre-determined e-mail address http://www.softsecurity.com/ 09.20.01

iOpus surveillance software can tell who is doing what on which PC at 24 hours range. http://www.iopus.com/starr.htm 09.20.01

PC Snoop uses video capture device and/or camera attached to PC to monitor the area around a system. Its core component is *motion detection* software algorithm with user-selectable sensitivity threshold and field-of-view zone. http://www.darvision.com/products/pcsnooppro/ 09.20.01

© SANS Institute 2000 - 2005 Author retains full rights.