

Introduction to Spyware Keyloggers

Sachin Shetty 2005-04-14

Spyware overview

Spyware is a categorical term given to applications and software that log information about a user's online habits and report back to the software's creators. The effects of these programs range from unwanted pop-up ads and browser hijacking to more dangerous security breaches, which include the theft of personal information, keystroke logging, changing dialup ISP numbers to expensive toll numbers, and installing backdoors on a system that leave it open for hackers.

Spyware usually gets into the computer through banner ad-based software where the user is enticed to install the software for free. Other sources of spyware include instant messaging, various peer-to-peer applications, popular download managers, online gaming, many porn/crack sites, and more. Note that most, but not all, spyware is targeted exclusively at Microsoft's Internet Explorer web browser. Users of modern Web browser alternatives, such as Mozilla's Firefox and Apple's Safari, are generally not affected by spyware at all.

The most recent delivery methods used by malicious spyware require no permission or interaction with the users at all. Dubbed as "drive-by downloads," [\[ref 1\]](#) the spyware application is delivered to the user without his knowledge simply when he visits a particular website, opens some zipped files, or clicks on a malicious pop-up ad that contains some active content such as ActiveX, Java Applets, and so on. Spyware can also be hidden in image files or in some cases has been shipped along with the drivers that come with a new hardware device.

Spying techniques

Depending upon the nature of the information gathered, each piece of spyware may function differently. Some spyware applications simply gather information about a user's surfing habits, purely for marketing purposes, while others are far more malicious. In any case, the spyware attempts to uniquely identify the information sent across a network by using a unique identifier, such as a cookie on the user's hard disk or a Globally Unique Identifier (GUID). [\[ref 2\]](#) The spyware then sends the logs directly to a remote user or a sever that is collecting this information. The collected information typically includes the infected user's hostname, IP address, and GUID, along with various login names, passwords and other keystrokes.

Types of keyloggers

As mentioned, keyloggers are applications that monitor a user's keystrokes and then send this information back to the malicious user. This can happen via email or to a malicious user's server somewhere on the Internet. These logs can then be used to collect email and online banking usernames and passwords from unsuspecting users or even capture source code being developed in software firms.

While keyloggers have been around for a long time, the growth of spyware over the last few years means they warrant renewed attention. In particular, this is due to the relative ease at which a computer can become infected -- a user simply has to visit the wrong website to become infected.

Keyloggers can be one of three types:

1. **Hardware Keyloggers.** These are small inline devices placed between the keyboard and the computer. Because of their size they can often go undetected for long periods of time -- however, they of course require physical access to the machine. These hardware devices have the power to capture hundreds of keystrokes including banking and email username and passwords.
2. **Software using a hooking mechanism.** This type logging is accomplished by using the Windows function `SetWindowsHookEx()` that monitors all keystrokes. The spyware will typically come packaged as an executable file that initiates the hook function, plus a DLL file to handle the logging functions. An application that calls `SetWindowsHookEx()` is capable of capturing even autocomplete passwords.
3. **Kernel/driver keyloggers.** This type of keylogger is at the kernel level and receives data directly from the input device (typically, a keyboard). It replaces the core software for interpreting keystrokes. It can be programmed to be virtually undetectable by taking advantage of the fact that it is executed on boot, before any user-level applications start. Since the program runs at the kernel level, one disadvantage to this approach is that it fails to capture autocomplete passwords, as this information is passed in the application layer.

Analyzing a keylogger

There are many different keyloggers available, including the Blazing Tools Perfect Keylogger [ref 3], Spector [ref 4], Invisible Keylogger Stealth [ref 5], and Keysnatch [ref 6]. Most of these have more or less the same set of features and way of functioning. Therefore, we will focus on one particular tool in our examples, the one from Blazing Tools.

The Blazing Tools Perfect Keylogger will be analyzed in this paper because it has been found hidden in so many Trojans on the Internet. It's a good example of a common hook-type keylogger. Although Blazing Tools markets its products to IT administrators and parents, the presence of their keylogger in many Trojans illustrates how people can package legal code and use it for malicious activities. The following features of the "Perfect Keylogger" are of use to anyone trying to spy on an unsuspecting user:

1. **Stealth Mode.** In this mode no icon is present in the taskbar and the keylogger is virtually hidden.
2. **Remote Installation.** The keylogger has a feature whereby it can attach to other programs and can be sent by e-mail to install on the remote PC in stealth mode. It will then send keystrokes, screenshots and websites visited to the attacker by e-mail or via FTP.
3. **Smart Rename.** This feature allows a user to rename all keylogger's executable files and registry entries.

This keylogger was installed on a test PC. The following capture, with the help of a tool such as SNAPPER [ref 7], shows the changes in the files after installing the keylogger, as shown below in Figure 1.

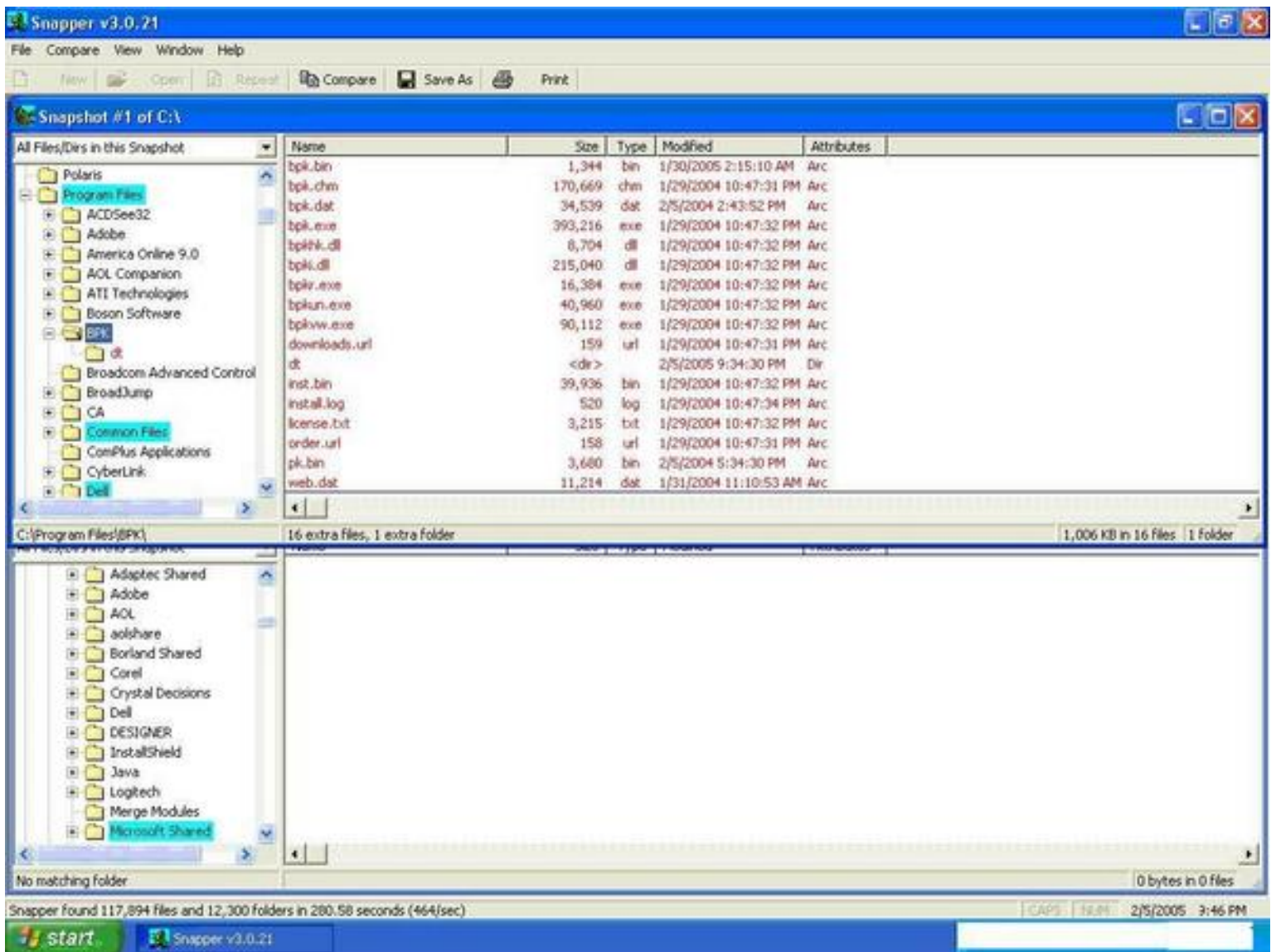


Figure 1. File changes made by the Perfect Keylogger.

With the help of a free anti-spyware application such as Microsoft Antispyware [ref 8], the registry entries made by the keylogger as well as its DLLs and EXEs can be seen below in Figure 2.

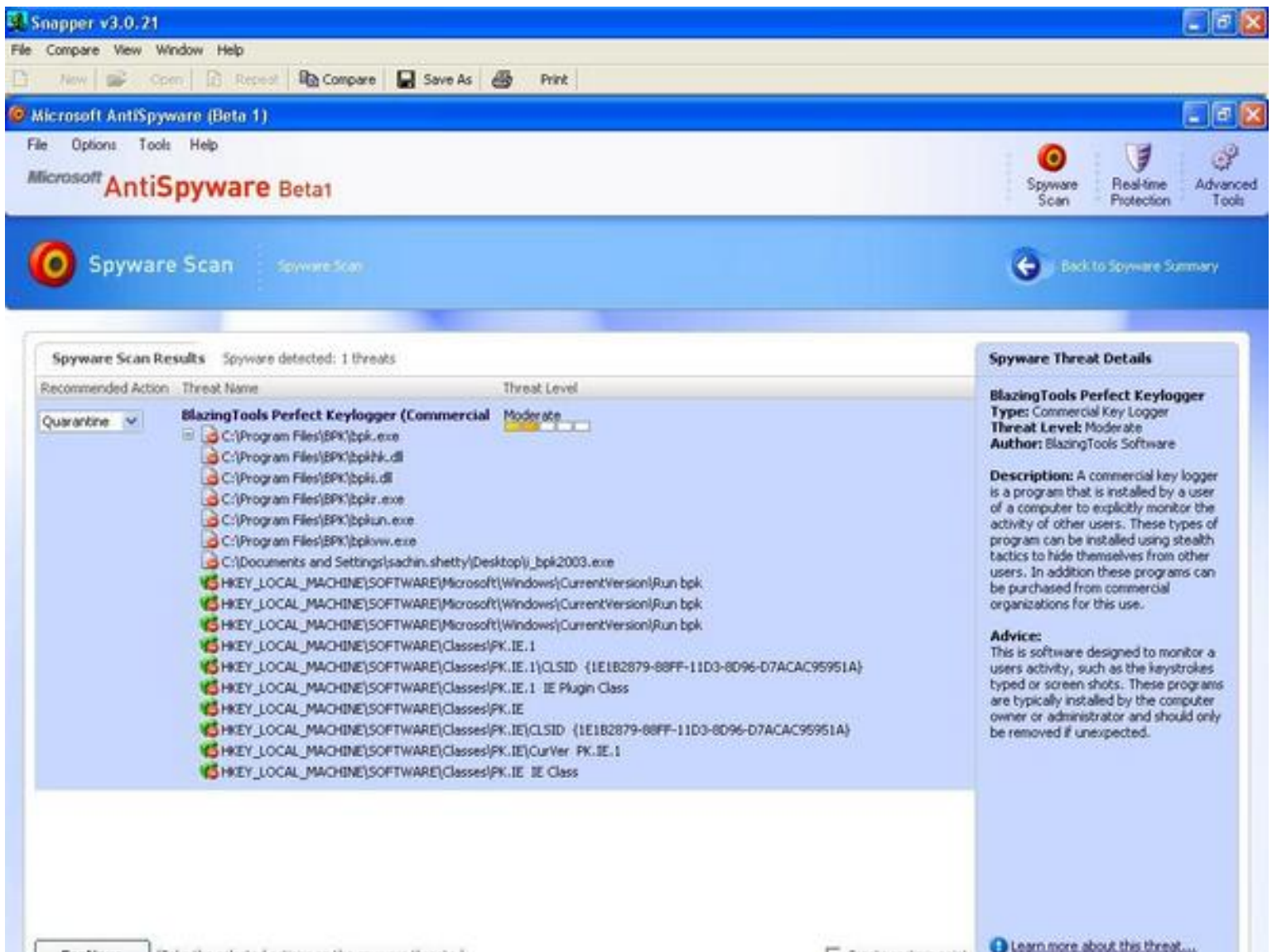


Figure 2. Registry entries, .dll files and .exe files of Keylogger.

The keylogger also runs as a background process which can be seen with the help of a tool such as SysInternals' Process Explorer [ref 9], as shown below in Figure 3.

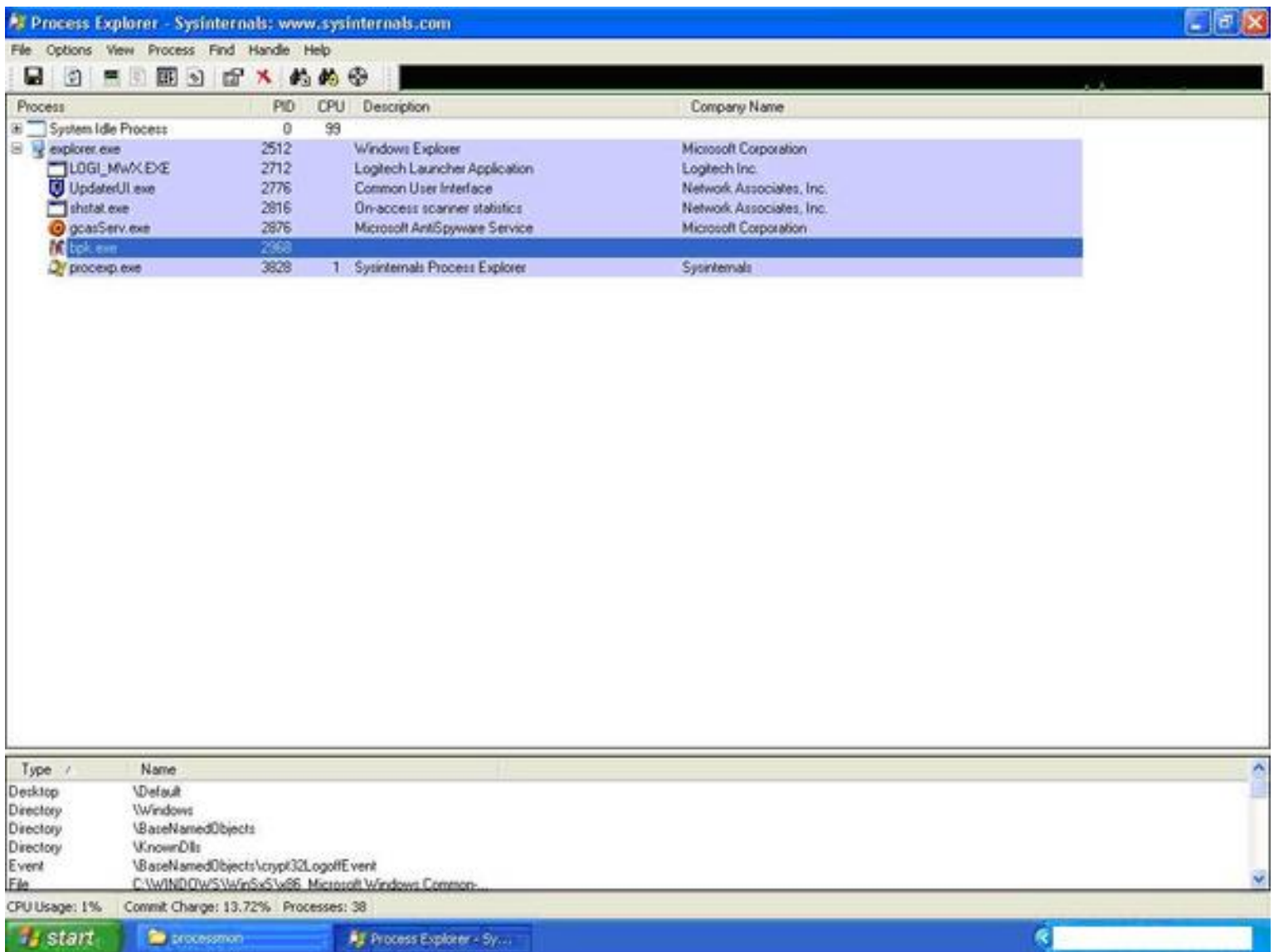


Figure 3. Spyware process running in the background.

This same keylogger was next installed on a different test PC through another program's installer and then configured to send keystrokes captured in an email to a test email-id. Ironically, the program used for this example was Spybot Search & Destroy [ref 10], a legitimate freeware tool that does a good job of detecting spyware. This is a good example of how other legitimate applications can also be used to install spyware, unbeknownst to the reader.

The procedure as described above is the Remote Installation feature. The information sent by email was then captured with the help of a network sniffer. For ease-of-use, Ethereal [ref 11] and the corresponding TCP stream is shown below in Figure 4 and Figure 5.

The screenshot displays the Wireshark interface with the following details:

No.	Time	Source	Destination	Protocol	Info
363451	0.363451	165.212.11.125	202.149.209.186	SMTP	Response: 220 uadvq137.cms.us

The details pane for the selected packet shows:

- Ethernet II, Src: 00:a0:c5:5e:41:77, Dst: 00:50:ba:3c:e3:7e
- Internet Protocol Version 4, Src Addr: 165.212.11.125 (165.212.11.125), Dst Addr: 202.149.209.186 (202.149.209.186)
- Hypertext Transfer Protocol, Content-Type: text/plain

The raw data pane shows the following hexadecimal and ASCII values:

```

00  ba 3c e3 7e 00 a0 c5 5e 41 77 08 00 45 00  .P.<~.. ^Aw..E.
02  d3 c6 00 00 30 06 69 0e a5 d4 0b 7d ca 95  .....0. i....}..
0a  00 19 08 ba d1 da b8 26 36 73 a1 88 50 18  .....&6s..P.
00  0e 76 00 00 32 32 30 20 75 61 64 76 67 31  ...v..22 0 uadvq1
07  2e 63 6d 73 2e 75 73 61 2e 6e 65 74 20 45  37.cms.u sa.net E

```

Figure 4. Ethereal captures the keylogger's outgoing email.

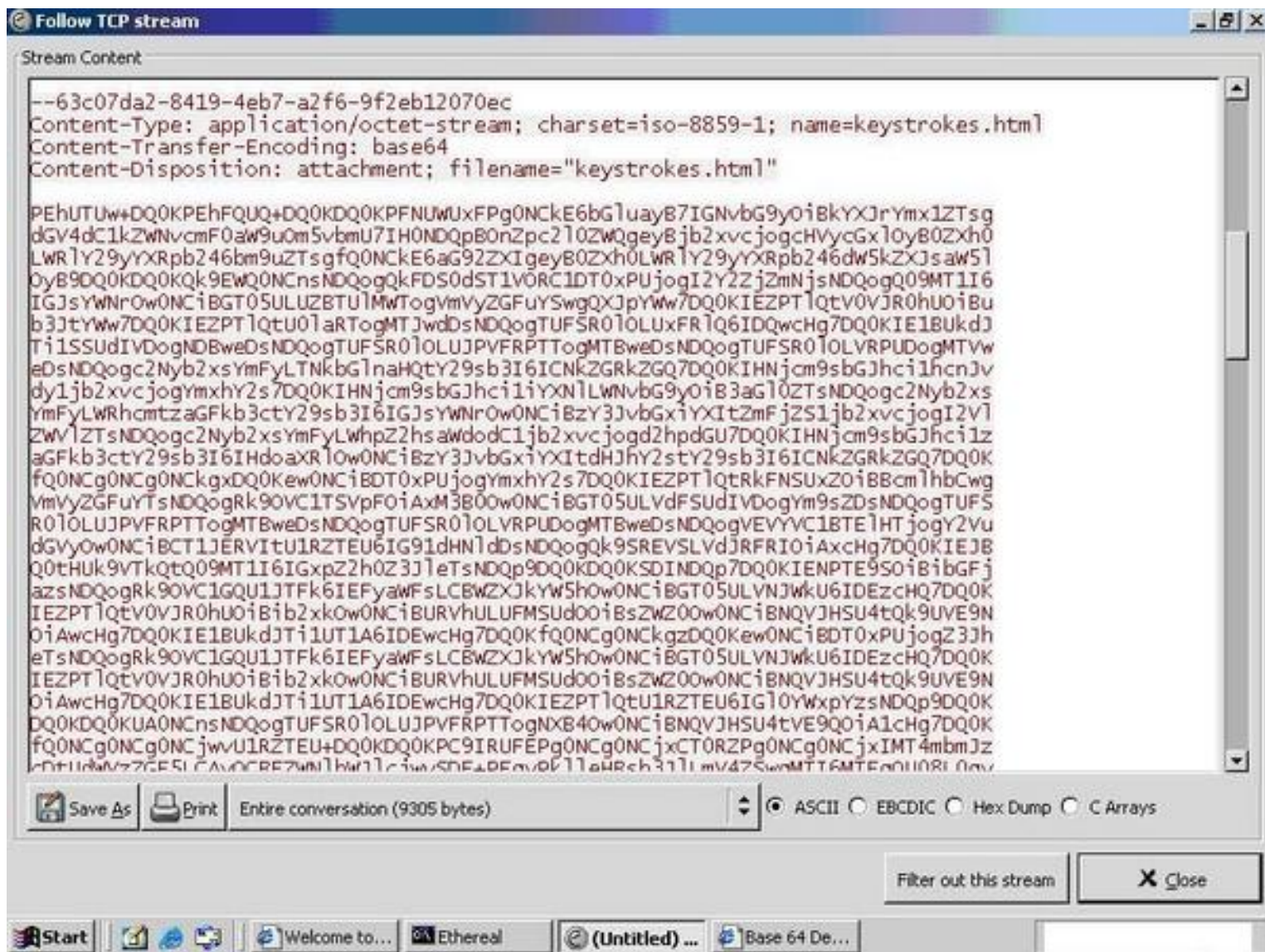


Figure 5. TCP stream of Ethereal capture.

Since the content of this email is base64 encoded, the actual output can be seen only after decoding it with a base64 decoder. After passing the output through a base64 decoder, the part of the output of significance is shown as follows:

Tuesday, 28 December

!explore.exe, 12:11 AM

Paladion Networks: The Internet Security Architects - Microsoft Internet Explorer

```
sachin.shetty
```

```
sachin123
```

```
[PASSWORD CAPTURED: sachin123]
```

It can be seen that the email-id (sachin.shetty) and the password (sachin123) are captured. Similarly, the keylogger can be used to capture all types of passwords including passwords used for proxies, email accounts, and online banking applications. It can also capture programming code typed by a developer, instant messaging text, and the URLs of websites visited by the user.

New approaches

With the market being inundated with new anti-spyware products, spyware creators have now resorted to unorthodox methods of sustenance. One such example is the nasty ability of the spyware code to keep reinstalling itself. Although anti-spyware applications can remove the spyware's registry entry from one location, most of them are found lacking in cleaning hidden registry entries that try to have the software reinstalled on boot. Another approach is to make the spyware application load into memory very early in the boot process (before the Operating System loads user-level processes). In this case, when a user tries to uninstall the software with an anti-spyware application, the OS will not allow this as it tries to protect the integrity of a running program (spyware) that it doesn't control. [\[ref 12\]](#)

Detection and removal

A spyware application is inherently very different in behavior and operation from a traditional

virus or a worm, and therefore to most antivirus software, it may appear as a legitimate program. The fact is, virus signatures are very different from spyware signatures. Firewalls also are ineffective in dealing with them as spyware is either piggybacked with legitimate applications, hidden in a regular image file, or can occur as normal port 80 web traffic.

Therefore, the essence of any spyware prevention exercise is first to ensure the operating system is fully patched to known vulnerabilities. The best prevention, aside from switching to less vulnerable operating systems like Mac OS X and Linux, is to educate users that it is not safe to click on anything and everything found on the Web, and they must also install only what is needed. Freebies on the Internet, ones which are often typically advertised in pop-up banners, must be totally abstained from. Other methods of avoiding spyware are to ensure the browser used is configured securely, and to have at least one good spyware detection and removal tool installed. Microsoft Antispyware, Ad-Aware [ref 13], PestPatrol [ref 14], and Spy Sweeper [ref 15] are some of the free tools that help in detecting and removing spyware.

Please note that spyware is largely, but not exclusively, a problem with Microsoft's Internet Explorer. The user of more modern, feature-rich browsers such as Mozilla Firefox can virtually eliminate the spyware problem altogether. However, it is still the case that some websites are coded to only work with IE, and therefore switching to Firefox may not be a solution for 100% of a user's web surfing needs.

Preventing keystroke capture

Since this article has looked at keyloggers, it was found worthwhile to include a section on how to avoid keystroke capture. Keyloggers, both hardware and software, are basically designed to capture what a user types on the keyboard. On the web application side, one method to avoid keystroke capture is to use a virtual keyboard for entering the username and password. A virtual keyboard is analogous to a graphical keypad where a user clicks on the characters rather than types them on the keyboard. This approach may not be practical for every user, for obvious reasons. However, it can be still be useful for very sensitive applications. Note however that even this approach is not completely secure, as some keyloggers are designed to capture screenshots on every mouse-click. Thus, the password of the user can still be found out when a virtual keyboard is used by looking at the screenshots and getting all the characters clicked corresponding to the mouse click. To avoid this, some virtual keyboards also have a feature that allows a user to enter a character by hovering the mouse cursor over a letter for a few seconds. Thus the user can enter the password without even clicking the mouse button. An example of a virtual keyboard is shown below in Figure 6.

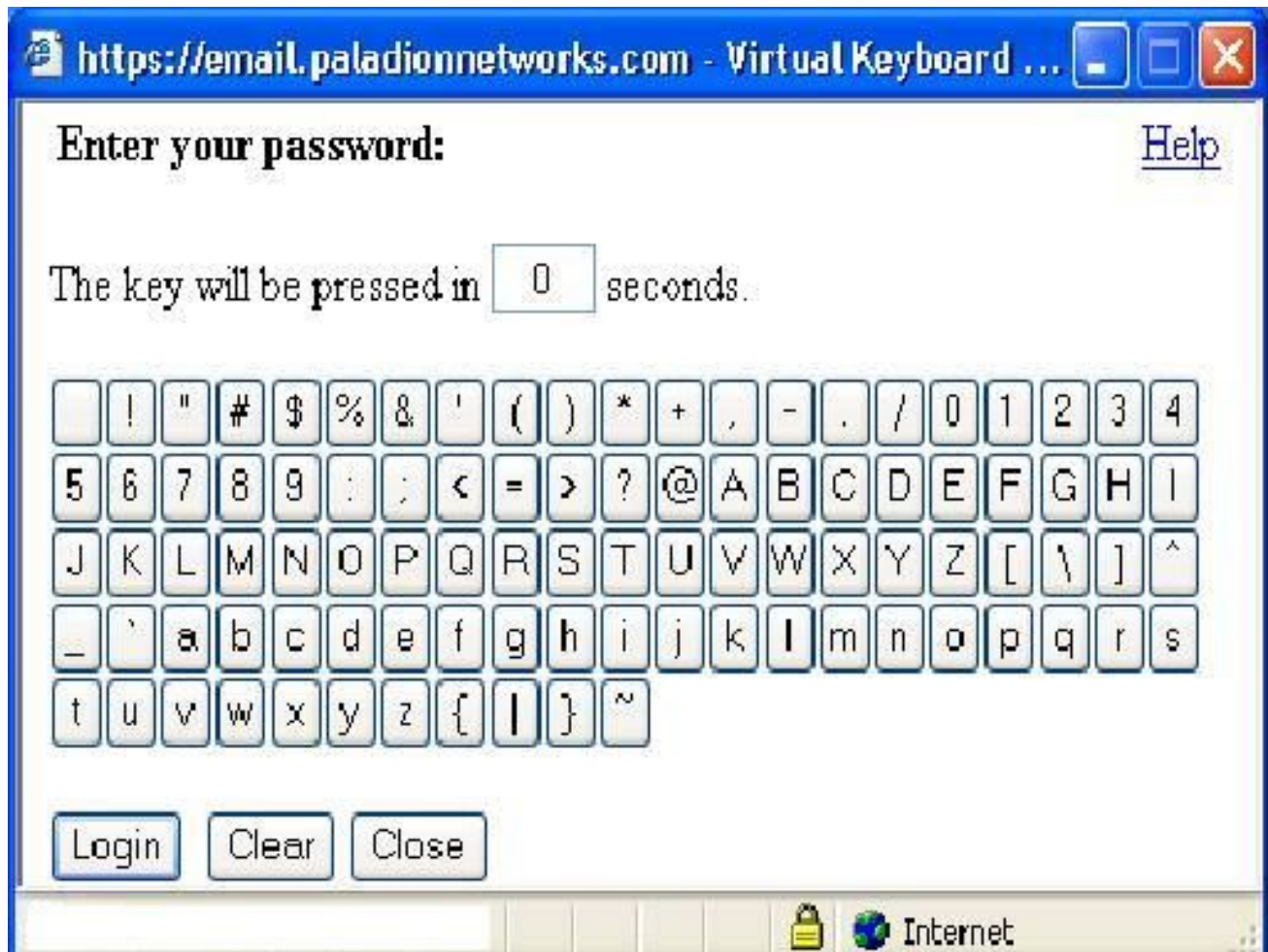


Figure 6. A virtual keyboard.

Another method of avoiding keystroke capture is to ask the user to enter the characters of the password randomly. For example, an application can ask the user to enter the 1st, 3rd and 5th (odd placed) characters of the password and then the characters in the even places. However this sequence has to change every time or else anyone capturing the password can easily reconstruct the original password -- and additionally, the application must support this approach. The disadvantage of this method is that the keylogger still captures all the characters in the password and the malicious person can easily crack it by simply trying different combinations.

Anti-keylogging software

To prevent keyloggers on the desktop level two types of anti-keylogging software is available from various vendors:

1. **Signature based anti-keylogger.** These are applications that typically identify a keylogger based on the files or DLLs that it installs, and the registry entries that it makes. Although it successfully identifies known keyloggers, it fails to identify a keylogger whose

signature is not stored in its database. Some anti-spyware applications use this approach, with varying degrees of success.

2. **Hook based anti-keyloggers.** A hook process in Windows uses the function `SetWindowsHookEx()`, the same function that hook based keyloggers use. This is used to monitor the system for certain types of events, for instance a keypress/mouse-click -- however, hook based anti-keyloggers block this passing of control from one hook procedure to another. This results in the keylogging software generating no logs at all of the keystroke capture. Although hook based anti-keyloggers are better than signature based anti-keyloggers, note that they still are incapable of stopping kernel-based keyloggers.

Summary

With the vast proliferation of spyware in recent years, there has been a growing list of websites and malicious users trying to cash in by installing keyloggers and stealing personal information. Identity theft has become rampant.

The need of the hour is to be aware of such common practices in spyware, and recognize it for what it is: malicious code that should always be avoided. The first step in evaluating ways to combat spyware should be to consider an alternate Web browser, such as Firefox, Safari, Opera, and others. If this is not possible, then steps to detect, combat and remove keylogging spyware must always be taken.

References

- [ref 1]
Sophos, "Sophos virus analyses," <http://www.sophos.com/virusinfo/analyses/>
- [ref 2]
Audit My PC.com, "GUID - Globally Unique Identifier," <http://www.auditmypc.com/acronym/GUID.asp>
- [ref 3]
Blazing Tools Software, "Perfect Keylogger," <http://www.blazingtools.com/bpk.html>
- [ref 4]

Spector keylogger, <http://www.spector.com>

[ref 5]

Invisible Keylogger Stealth keylogger, <http://www.amecisco.com/iks2000.htm>

[ref 6]

Keysnatch keylogger, <http://www.fileheaven.com/Keysnatch/download/2975.htm>

[ref 7]

Snapper, <http://www.users.globalnet.co.uk/~ashwobla/snapper/>

[ref 8]

Microsoft Antispyware, <http://www.microsoft.com/athome/security/spyware/software/default.aspx>

[ref 9]

Process Explorer by SysInternals, <http://www.sysinternals.com/ntw2k/freeware/procexp.shtml>

[ref 10]

Spybot Search & Destroy anti-spyware, <http://security.kolla.de/>

[ref 11]

Ethereal, <http://www.ethereal.com>

[ref 12]

Source: <http://www.macnewsworld.com/story/35748.html>

[ref 13]

Ad-Aware anti-spyware, <http://www.lavasoftusa.com/software/>

[ref 14]

PestPatrol Home Edition anti-spyware, <http://www.pestpatrol.com/Products/PestPatrolHE/>

[ref 15]

Spy Sweeper anti-spyware, <http://www.webroot.com/>

[ref 16]

Mozilla Firefox browser, <http://www.mozilla.org/products/firefox/central.html>

[[ref 16](#)]

Safari browser for Mac OS X, <http://www.apple.com/macosx/features/safari/>

Further reading on spyware

Germain Jack, "New Era of Deadly Spyware Approaches"

<http://www.macnewsworld.com/story/35748.html>

Gibson Steve, "Opt Out"

<http://grc.com/optout.htm>

Martin Kelly, "When Spyware Crosses the Line"

<http://www.securityfocus.com/columnists/250>

Gibson Steve, "The Anatomy of File Download Spyware"

<http://grc.com/downloaders.htm>

Cheveallier Lester, "Spyware & Network Security"

<http://www.sans.org/rr/whitepapers/basics/437.php>

InformIT, "Malware"

<http://www.informit.com/guides/printerfriendly.asp?g=security&seqNum=23>

Microsoft MSDN

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winui/winui/>

[windowsuserinterface](#)

[/windowing/hooks/hookreference/hookfunctions/callnexthookex.asp](#)

About the author

[Sachin Shetty](#) is a specialist in Application Security and BS7799 consulting, and works as an Information Security Consultant at [Paladion Networks](#).

[Privacy Statement](#)

Copyright 2006, SecurityFocus