Keyloggers

ETHICAL HACKING

EEL-4789

GROUP 2:

WILLIAM LOPEZ

HUMBERTO GUERRA

ENIO PENA

ERICK BARRERA

JUAN SAYOL

Contents

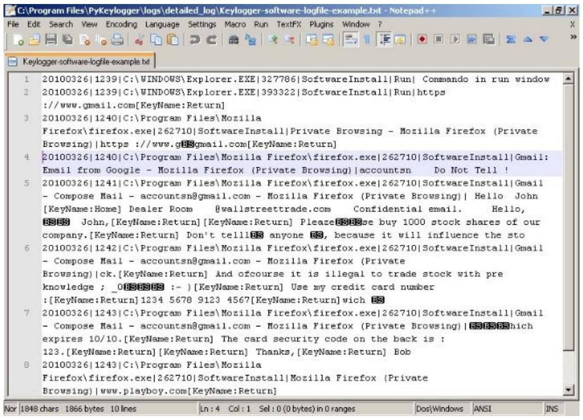
Abstract: Keyloggers

In this paper we provide an explanation of key loggers, the different types and the history. We will explain Keyloggers and their main features, as well as a comparison and tactics and techniques for using such tools. Also, how these tools can be used for good causes like monitoring the web activity of children to ensure their protection as well as other more illegal uses like unauthorized spying and password cracking. Finally, we will code a key logger that will keep track of the user entered information in Firefox.

Introduction

Keyloggers have somewhat of a bad reputation in the technology world because more often it’s associated with illegal spying and theft of personal and monetary information. In reality even though that’s one of the main uses, it can be used for other more appropriate and legal tasks. One clear example of this would be at a company’s security policy which clearly states that the workers activities can be monitored with Keylogger and can be used to monitor an employee who is under suspicion of being a malicious insider. By logging his activity on his workstation the company may be able to confirm their suspicions or clear his name. Sometimes a simple and inexpensive tool like Keyloggers may save companies millions in damages. The same concept may be applied to a more family based used like monitor the activities of under aged children on the web which may help to the child's safety from online predators and dangers. There are different types of Keyloggers divided into 2 main groups Hardware Keyloggers and Software Keyloggers. Hardware Keyloggers are small electronic devices used for capturing the data in between a keyboard device and I/O port.

Usually these devices have built in memory where they store the keystrokes so this means they must be retrieved by the person who installed it in order to obtain the information. An advantage of these Keyloggers is that they are undetectable by anti-viral software or scanners since it works on the hardware platform. Software Keyloggers track systems, collect keystroke data within the target operating system, store them on disk or in remote locations, and send them to the attacker who installed the Keyloggers.


C:\Program Files\PyKeylogger\logs\detailed_log\Keylogger-software-logfile-example.txt - Notepad++
File
Edit
Search
View
Encoding
Language
Settings
Macro
Run
TextFX
Plugins
Window
?
Keylogger-software-logfile-example.txt
Nor
1848 chars 1866 bytes 10 lines
Ln : 4 Col : 1 Sel : 0 (0 bytes) in 0 ranges
Dos\Windows
ANSI
INS

```
20100326|1239|C:\WINDOWS\Explorer.EXE|327786|SoftwareInstall|Run| Commando in run window
20100326|1239|C:\WINDOWS\Explorer.EXE|393322|SoftwareInstall|Run|https
://www.gmail.com[KeyName:Return]
20100326|1240|C:\Program Files\Mozilla
Firefox\firefox.exe|262710|SoftwareInstall|Private Browsing - Mozilla Firefox (Private
Browsing)|https ://www.gBSgmail.com[KeyName:Return]
20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail:
Email from Google - Mozilla Firefox (Private Browsing)|accountsn    Do Not Tell !
20100326|1241|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
- Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)| Hello  John
[KeyName:Home] Dealer Room    @wallstreettrade.com    Confidential email.     Hello,
BSBS  John,[KeyName:Return][KeyName:Return] PleazeBSBSse buy 1000 stock shares of our
company.[KeyName:Return] Don't telllBS anyone BS, because it will influence the sto
20100326|1242|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
- Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private
Browsing)|ck.[KeyName:Return] And ofcourse it is illegal to trade stock with pre
knowledge ; _0BSBSBS :- )[KeyName:Return] Use my credit card number
:[KeyName:Return]1234 5678 9123 4567[KeyName:Return]wich BS
20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
- Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)|BSBSBShich
expires 10/10.[KeyName:Return] The card security code on the back is :
123.[KeyName:Return][KeyName:Return] Thanks,[KeyName:Return] Bob
20100326|1243|C:\Program Files\Mozilla
Firefox\firefox.exe|262710|SoftwareInstall|Mozilla Firefox (Private
Browsing)|www.playboy.com[KeyName:Return]
```

The main advantage of software Keyloggers compared to the hardware Keyloggers is that they can run for an indefinite amount of time while the info is being transmitted remotely eliminating the need to personally obtain the information like it's the case with hardware Keyloggers. In this paper we will implement and explain our own custom coded software Keylogger.

History

Keylogging, often referred to as Keyboard Capturing or Keystroke logging, is the action of recording or monitoring every key pressed on a keyboard. Even though these devices are relatively new to us, Keyloggers have already been with us almost half of a century. Their exact history cannot be known perfectly, for it is believed that they first were used by the government and obviously they do not release any exact day. In fact, it can be established that the first terrorists' cyber-attacks started with Keylogging activities. In Moscow and St. Petersburg spies started installing Keyloggers in the US Embassy and Consulate buildings in 1970, as a method of capturing information to be used in malicious manner. Another anecdote about Keylogging actions goes to November, 1983, when an early keystroke logger written by Perry Kivolowitz was posted to the Usenet news. This posting appears to be a motivating factor in restricting access on UNIX systems. As it can be seen, Keylogging activities were directly related to governmental monitoring. However, since the beginning of the 21st century, Keyloggers have become one of the most technology devices used for surveillance, government wide and beyond.

Security

Security using Keyloggers will monitor email, internet, chats or anything that requires a keystroke. This will help capture all information in image and/or text form. Keyloggers are a type of malicious malware that track the users' keystrokes and captures the characters that are pressed in and writes the information to a file. Even though that both hardware and software Keyloggers are known, software Keyloggers are the ones that are being widely used due to the inexpensive and easier to implement onto a computer. Each different operating system will have an adapted Keyloggers which suits the I/O. Monitoring keystrokes will help with the work flow, investigation theft, review performance, prevent harassment, missing data and prevent personal use. Work flow will increase due to the fact that the employees will be motivated, this will weed out the employees that want to go on Facebook or check their personal emails which might cause a security leak. If there is some type of deleted file or missing information the security personnel can detect which computer that is missing such important information and figure out what went wrong. Employees knowing all this will show performance at their job from the amount of keystrokes they had to do. If someone is being harassed then this will increase the chances of finding out whom and when the incident occurred. In the end this will prevent personal use and increase safety and security with other benefits.

Implementation

The implementation of Keylogger and design are based upon many factors: the type of operating system, the lifespan of a Keylogger, where it is infecting and the level of footprint on a machine. The Keylogger infiltration is depended on the user operating system or a attaching a physical Keylogger device. Software Keyloggers are made to ensure proper installation by web browser exploit for example. Security vulnerabilities vary depending on the browser being used and the attacker can identify and exploit the weaknesses. An attack can be executed by utilizing JavaScript which could be a user side language.

When the Keylogger has been implemented it can focus on its execution. Keylogger implement each technique differently, most use a common execution technique known as hooking. Hooking reroutes the information to its location and returns the information back to the system routine. Hooks can be executed in any operating systems for utmost functions.

Keyloggers that are well-made can be executed in the user-mode of operating systems which uses a variation of hooks. Every keystroke are flagged through a message mechanism that gets transferred from the keyboard device to the windows procedures, during the process the hook can grab the information before the information reaches windows procedures. Keyloggers can be developed into implementing a global hook or a local depending on which information the person wants to retrieve from the keystrokes.

Conclusion

This paper went over most issues regarding Keystroke logging. Although Keyloggers have a bad reputation in society, the research done to elaborate this paper shows how these devices can be used not always in a malicious way of action such as illegal spying and theft of personal information. At a company level, Keyloggers can be used to monitor any suspicious activity that may cause a serious liability to the company's benefit. Workers who are under doubt can be explicitly be discover or clear their names. This helps the company ensure their interests before any bigger security issue happens, making them save larger quantities of money. Another legal way of using a Keylogger is in a closer and more personal level, home. Any head of household wants their children going on the internet without any consent of what they are watching, what websites are they surfing in, and most important who they are in contact with. Nowadays, there are a lot of people looking for victims online. Child's predator, kidnappers, and so all are always seeking innocent children, and Keyloggers can be very helpful in order to minimize those kinds of attacks from occurring. In this paper it is also discussed the different kinds of Keyloggers and their advantages compared to one another. The Keystroke loggers can be divided into 2 main groups Hardware Keyloggers and Software Keyloggers. The main advantage of hardware Keyloggers is that they are invisible to any antiviral software or scanner.

How our Keylogger POC works:

Our Keylogger will be targeting the Firefox application process (firefox.ee) in the victim's computer.

However, it is not limited to just Firefox and it can be adjusted to any other popular browser with minor alterations to the source code.

The Keylogger is structured as a client-server model.

Client

The client consists of a library: (library.dll) and an executable (loader.exe).

The library contains most of the client-sided Keylogger code as well as an add-on to allow attackers to spawn a shell on the victim and execute commands remotely.

More specifically, once the library is loaded in the target process, it will intercept any calls to the GetMessage() Windows API function, and filter/log any key press messages. These messages are then saved to a temporary log file which is then uploaded to the server once the file has enough key presses collected.

The advantages of injecting a library in a process instead of having a standalone executable to do the Keylogging are obvious. First, any packets generated by the Keylogger will seem to be coming from the target process (firefox.exe) in this case. Second, a library will not show in the task manager like an executable will.

The loader executable performs a simple task: load (inject) the library to the target process (firefox.exe) and exit. The loader waits until the target process is running to perform the actual injection.

Keylogger Source Code Link

https://github.com/Erickbarrera/SimpleKeylogger

Server

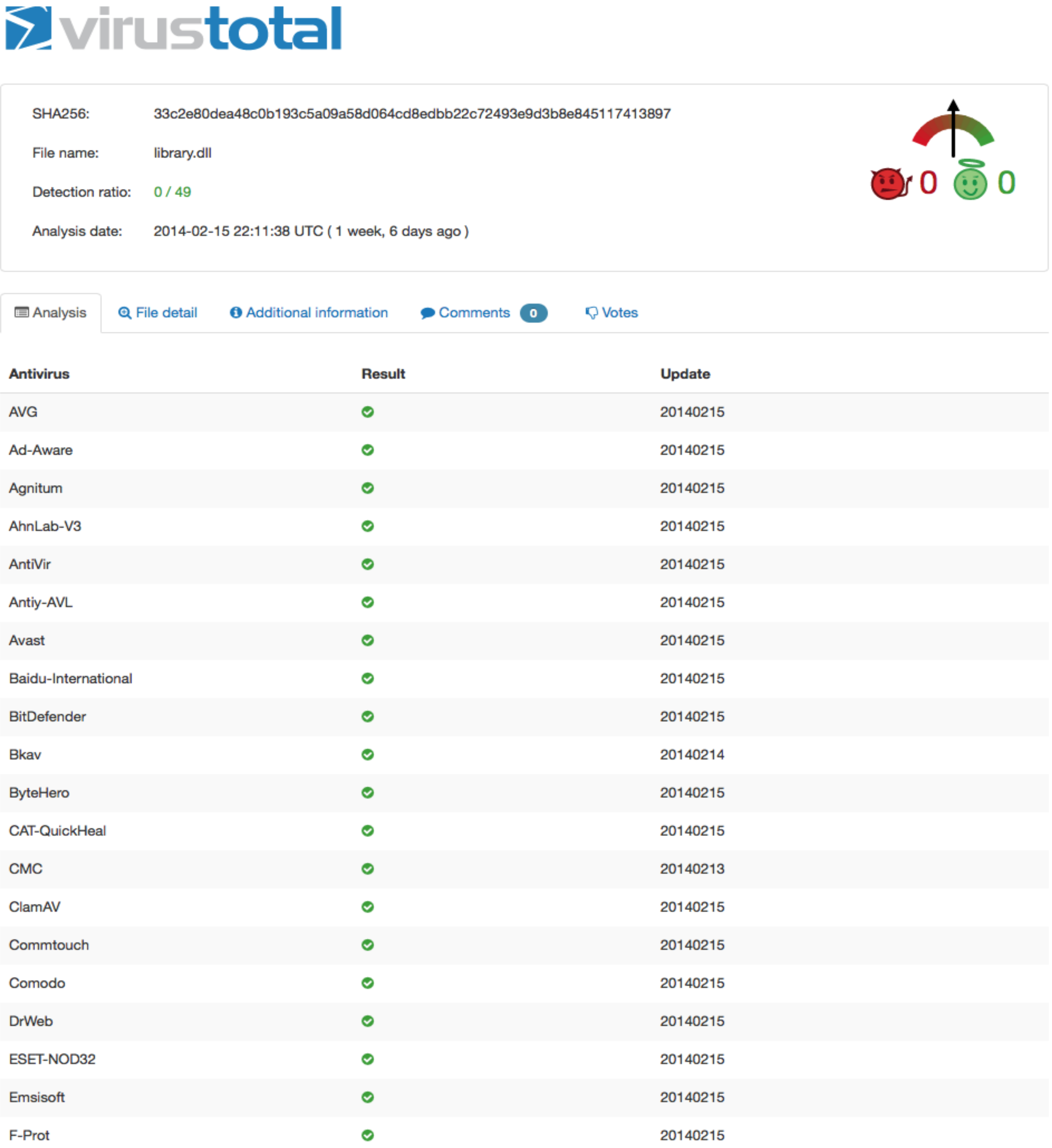
The server consists of a few PHP scripts that facilitate the viewing and uploading of Keylogger logs. The Keylogger client uses the script "upload.php" to post the log files to the server. The "upload.php" script takes care of saving the file and renaming it for easy access later.

The server provides the attacker a single place to look at all the Keylogger client's logs and the date on which they were uploaded.

An optional add-on is to have a server running a tool like netcat. The Keylogger client library is always attempting to connect to a predefined IP address and PORT in order to allow a listening program full access to a shell in the victim's computer. Netcat is one of many programs that can be used to listen for the Keylogger library connection attempts.

Although this proof of concept can be further improved, it provides the full functionality of a basic Keylogger with a few nice features.

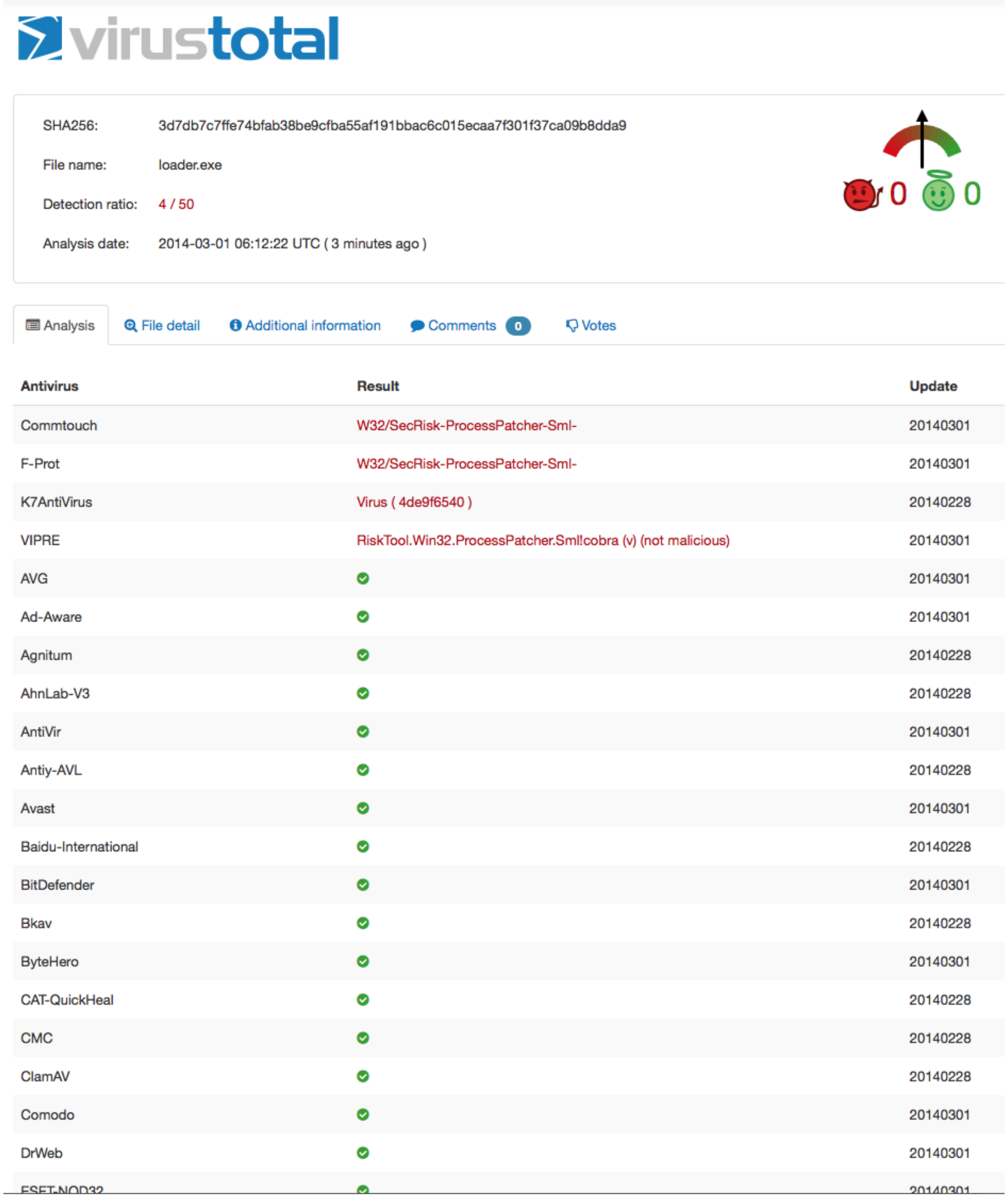
Antivirus Scan Results



virustotal

SHA256:	33c2e80dea48c0b193c5a09a58d064cd8edbb22c72493e9d3b8e845117413897
File name:	library.dll
Detection ratio:	0 / 49
Analysis date:	2014-02-15 22:11:38 UTC (1 week, 6 days ago)

Antivirus	Result	Update
AVG	✓	20140215
Ad-Aware	✓	20140215
Agnitum	✓	20140215
AhnLab-V3	✓	20140215
AntiVir	✓	20140215
Antiy-AVL	✓	20140215
Avast	✓	20140215
Baidu-International	✓	20140215
BitDefender	✓	20140215
Bkav	✓	20140214
ByteHero	✓	20140215
CAT-QuickHeal	✓	20140215
CMC	✓	20140213
ClamAV	✓	20140215
Commtouch	✓	20140215
Comodo	✓	20140215
DrWeb	✓	20140215
ESET-NOD32	✓	20140215
Emsisoft	✓	20140215
F-Prot	✓	20140215



SHA256: 3d7db7c7ffe74bfab38be9cfba55af191bbac6c015ecaa7f301f37ca09b8dda9

File name: loader.exe

Detection ratio: 4 / 50

Analysis date: 2014-03-01 06:12:22 UTC (3 minutes ago)

Antivirus	Result	Update
Commtouch	W32/SecRisk-ProcessPatcher-Sml-	20140301
F-Prot	W32/SecRisk-ProcessPatcher-Sml-	20140301
K7AntiVirus	Virus (4de9f6540)	20140228
VIPRE	RiskTool.Win32.ProcessPatcher.Sml!cobra (v) (not malicious)	20140301
AVG	✓	20140301
Ad-Aware	✓	20140301
Agnitum	✓	20140228
AhnLab-V3	✓	20140228
AntiVir	✓	20140301
Antiy-AVL	✓	20140228
Avast	✓	20140301
Baidu-International	✓	20140228
BitDefender	✓	20140301
Bkav	✓	20140228
ByteHero	✓	20140301
CAT-QuickHeal	✓	20140228
CMC	✓	20140228
ClamAV	✓	20140228
Comodo	✓	20140301
DrWeb	✓	20140301
ESET-NOD32	✓	20140301

As shown in the results above, antivirus software is completely oblivious to our Keyloggers and fails to detect it. This un-detectability can be contributed to the fact that our code and file signatures have not yet been added to the antivirus software definitions database.

References

1. http://securityresearch.in/index.php/projects/malware_lab/malware-keyloggers/

2. http://www.ijcsmc.com/docs/papers/March2013/V2I3201322.pdf

3. http://www.wellresearchedreviews.com/computer-monitoring-software-reviews.html

4. http://blog.opensecurityresearch.com/2012/10/hacking-keyloggers.html

5. http://www.keylogger.org/

6. http://christopher-wood.com/papers/KeyloggersInCybersecurityEducation.pdf

7. http://securityresearch.in/index.php/projects/malware_lab/malware-keyloggers/

8. http://www.ijcsmc.com/docs/papers/March2013/V2I3201322.pdf

9. http://adventuresinsecurity.com/images/Keystroke_Logging.pdf

10. http://en.wikipedia.org/wiki/Keystroke_logging Keylogging history.