KEYLOGGERS

T.Remina
Universal college of Emgineering and Tecchnology
3rd year
Computerscience and engineering

WHAT IS A KEY LOGGER?

A keylogger, sometimes called a keystroke logger, is a type of surveillance technology used to monitor and record each keystroke on a specific device, such as a computer or smartphone. It can be either hardware- or software-based. The latter type is also known as system monitoring software or keyboard capture software

WHY ARE KEYLOGGERS USED?

Keyloggers are often used as a spyware tool by cybercriminals to steal personally identifiable information, login credentials and sensitive enterprise data.

That said, some uses of keyloggers could be considered ethical or appropriate in varying degrees. For instance, keyloggers can also be used for the following reasons:

- By employers to observe employees' computer activities.
- By parents to supervise their children's internet usage.
- By device owners to track possible unauthorized activity on their devices.
- By law enforcement agencies to analyze incidents involving computer use.

TYPES OF KEYLOGGERS

Two main types of keyloggers are available.

Hardware-based keyloggers

A hardware-based keylogger is a small device that serves as a connector between the keyboard and the computer. The device is designed to resemble an ordinary keyboard PS/2 connector, part of the computer cabling or a USB adapter, making it relatively easy for someone who wants to monitor a user's behavior to hide the device.

Software-based keyloggers

A keylogging software program does not require physical access to the user's computer for installation. It can be purposefully downloaded by someone who wants to monitor activity on a particular computer, or it can be malware downloaded unwittingly by the user of the keyboard and its device, and then executed as part of a rootkit or remote administration Trojan. Either way, keylogging software allows an unauthorized threat actor to view the user's keystrokes, and then use this knowledge to access and compromise the device.

There are two main types of software keyloggers:

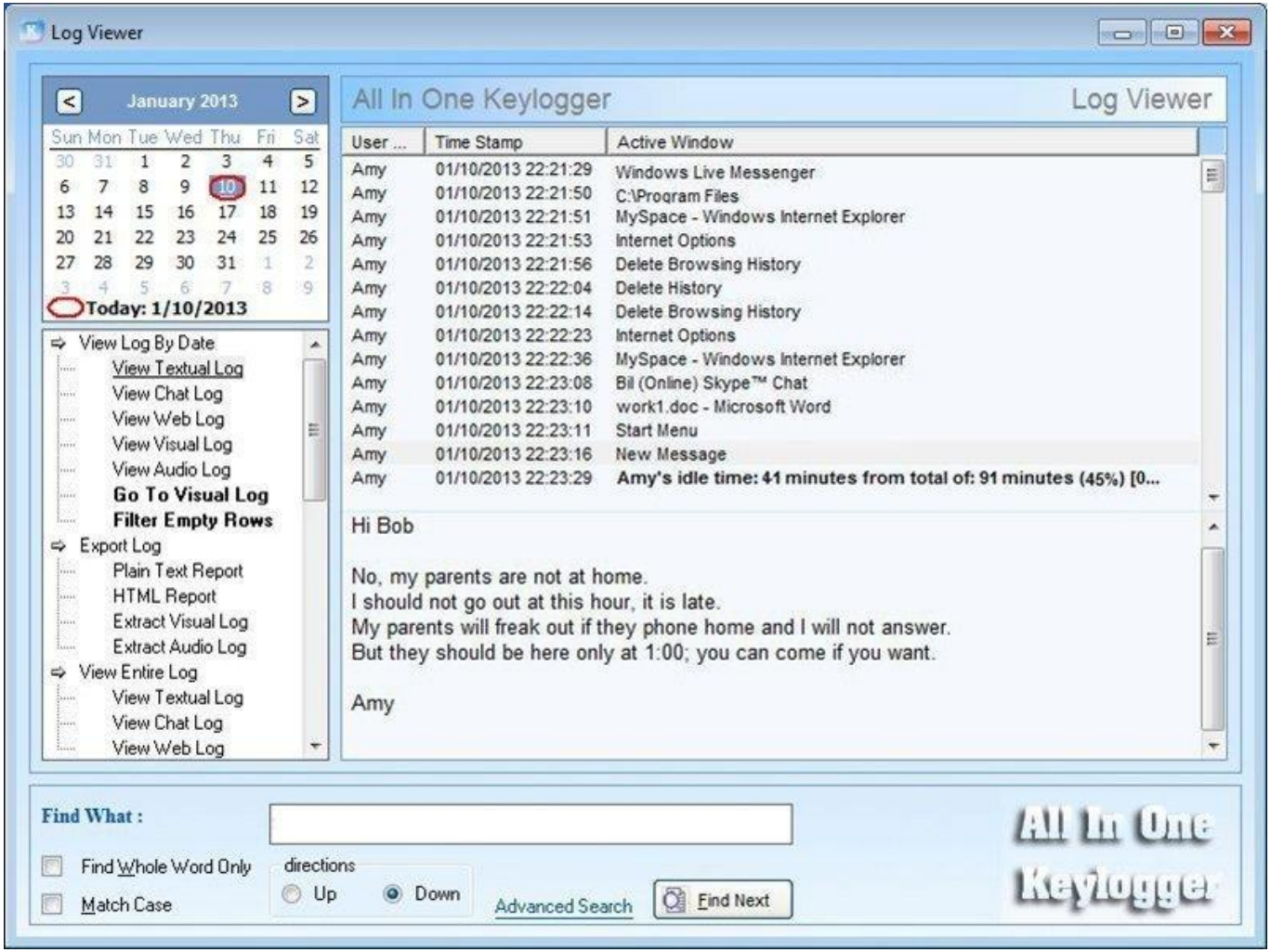
•**User mode keyloggers** use a Windows application programming interface (API) to intercept keyboard and mouse movements. GetAsyncKeyState or GetKeyState API functions might also be captured. These keyloggers require the attacker to actively monitor each key press.

•**Kernel mode keyloggers** are a more powerful and complex software keylogging method. They work with higher privileges and can be harder to locate in a system. In addition, they can modify the internal Windows system through the kernel.

Some keylogging software can use keyboard APIs to run another application, malicious script injection or memory injection.

HOW DO KEYLOGGERS WORK?

- A hardware keylogger might come in the form of a module installed inside the keyboard itself. When the user types on the keyboard, the keylogger collects each keystroke and saves it as text stored on its own hard drive, which can have a memory capacity up to several gigabytes. The person who installed the keylogger must physically remove the device to access the gathered information. There are also wireless keylogger sniffers that can intercept and decrypt data packets transferred between a wireless keyboard and its receiver.
- A common software keylogger consists of two files that get installed in the same directory: a dynamic link library file that does the recording, and an executable file that installs the DLL file and triggers it. The keylogger program records each keystroke the user types and periodically uploads the information over the internet, where the hacker can then access it.
- Some keylogging programs can also include functionality to record user data besides keystrokes, such as capturing anything that has been copied to the clipboard and taking screenshots of the user's screen or a single application.


Log Viewer
January 2013
Sun Mon Tue Wed Thu Fri Sat
30 31 1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31 1 2
3 4 5 6 7 8 9
Today: 1/10/2013
View Log By Date
View Textual Log
View Chat Log
View Web Log
View Visual Log
View Audio Log
Go To Visual Log
Filter Empty Rows
Export Log
Plain Text Report
HTML Report
Extract Visual Log
Extract Audio Log
View Entire Log
View Textual Log
View Chat Log
View Web Log
All In One Keylogger
Log Viewer
User ... Time Stamp Active Window
Amy 01/10/2013 22:21:29 Windows Live Messenger
Amy 01/10/2013 22:21:50 C:\Program Files
Amy 01/10/2013 22:21:51 MySpace - Windows Internet Explorer
Amy 01/10/2013 22:21:53 Internet Options
Amy 01/10/2013 22:21:56 Delete Browsing History
Amy 01/10/2013 22:22:04 Delete History
Amy 01/10/2013 22:22:14 Delete Browsing History
Amy 01/10/2013 22:22:23 Internet Options
Amy 01/10/2013 22:22:36 MySpace - Windows Internet Explorer
Amy 01/10/2013 22:23:08 Bil (Online) Skype™ Chat
Amy 01/10/2013 22:23:10 work1.doc - Microsoft Word
Amy 01/10/2013 22:23:11 Start Menu
Amy 01/10/2013 22:23:16 New Message
Amy 01/10/2013 22:23:29 Amy's idle time: 41 minutes from total of: 91 minutes (45%) [0...
Hi Bob
No, my parents are not at home.
I should not go out at this hour, it is late.
My parents will freak out if they phone home and I will not answer.
But they should be here only at 1:00; you can come if you want.
Amy
Find What :
Find Whole Word Only
Match Case
directions
Up
Down
Advanced Search
Find Next
All In One Keylogger

HOW TO DETECT A KEYLOGGER

- An anti-keylogger is a program designed specifically to scan for software-based keyloggers. These programs work by comparing the files on a computer against a keylogger signature base or a checklist of common keylogger attributes. Using security software such as an anti-keylogger can be more effective than an antivirus or antispyware program. The latter could incorrectly identify a keylogger as a legitimate program instead of spyware.
- That said, an antispyware application might be able to locate and disable keylogger software with lower privileges than it has. Using a network monitor will ensure the user is notified each time an application tries to make a network connection, giving a security team the opportunity to stop any possible keylogger activity.
- Checking the system's Task Manager can also help with the detection of a keylogger. However, since keyloggers can manipulate an operating system kernel, examining the Task Manager isn't necessarily enough to detect a keylogger, so it's better to use an anti-keylogger.

PROTECTION AGAINST KEYLOGGERS

- While visual inspection can identify hardware keyloggers, it is impractical and time-consuming to implement on a large scale. Instead, using a firewall can provide better protection by discovering and preventing the transfer of keystroke information from the victim's keyboard to the attacker.
- Password managers that automatically fill in username and password fields can help protect against keyloggers. Monitoring software and antivirus software can also keep track of a system's health and help prevent keyloggers.
- Extra precautions include using a security token as part of two-factor authentication to ensure an attacker cannot use a stolen password alone to log in to a user's account, or using an onscreen keyboard and voice-to-text software to circumvent using a physical keyboard. Application allowlisting can also be used to allow only documented, authorized programs to run on a system.

HOW CAN I PROTECT MYSELF FROM KEYLOGGERS?

- Avoid keyloggers by avoiding the user mistakes that lead to their ability to infect phones and computers. It starts with keeping your operating system, your applications, and web browsers up to date with the latest security patches. Always be skeptical about any attachments you receive, especially unexpected ones even if they seem to come from someone you know. When in doubt, contact the sender to ask. Keep your passwords long and complex, and avoid using the same one for different services.
- Real-time, always-on antivirus/anti-malware protection is the gold standard for preventing not only infection from a keylogger, but also from all other associated malware threats. For all platforms and devices, from Windows and Android, Mac and iPhones, to business environments, Malwarebytes is a first-line defense against the relentless onslaught of cybercriminal attacks.

ADVANTAGES AND DISADVANTAGES OF KEYLOGGING

- The advantages of keylogging include the ability to monitor and track the activities of employees, prevent malicious attacks, and collect data for marketing and research purposes. Keylogging can also be used to detect suspicious activity on a computer or mobile device, such as attempts to access restricted websites or to steal login information or passwords.
- On the other hand, the disadvantages of keylogging include the potential for misuse, the potential for invasion of privacy, and the potential for data leakage. Additionally, keylogging can be used to capture information that users might not want to share, such as credit card numbers or passwords.

THANK YOU