KeyLogger Spyware

How it is used by Hackers to monitor what you type?

Keystroke logging, or keylogging, is a data collection software that can record anything you type on your computer. Threat actors can use this attack to obtain information regarding your bank account numbers, credit card information, and login credentials like passwords on your computer.

A keylogger email attachment attack occurs once a hacker sends malicious code in a phishing email. Victims open the link, and the hacker installs the keylogger immediately. This article will detail keylogging, how it works, and how to detect an attack.

What is a Keylogging Attack?

A keylogger keeps track of the keys users hit on their keyboard, usually within a textbox from the email, so it can log the personal credentials and other information through the software. Though "keylogger" generally has a negative connotation, this software can be a helpful, legal, and legitimate tool for analyzing and debugging computer activity in certain circumstances.

Keystroke logging intercepts or alters electronic data to collect information from the application, which a victim utilizes as usual since they understand the inputs to go straight to the intended recipient rather than a malicious log. In most cases, hacker keyloggers write down keystrokes before passing the data through encryption to another computer, where the keylogger stores and unencrypts the information.

This type of threat comes through more than phishing campaigns. Malware and ransomware can encrypt and transfer the information elsewhere. WannaCry encrypts files on an affected machine until the victim pays a Bitcoin ransom.

There are a lot of great methods to use to keep yourself protected. Here are a variety of tricks we suggest you utilize and keep in mind when setting up your server:

1. Only open email attachments if you are sure you know it comes from a secure email source.
2. Inspect genuine appearing emails as well, since spear phishing emails tend to look believable at first glance but can steal your data just the same.
3. Update and enable anti-virus and anti-phishing software for constant, real-time malware protection.
4. Use strong passwords to prevent hackers from guessing correctly and hacking your system.
5. Be cautious of websites with fake sign-in pages where they steal your data directly from your computer.

How Can Hackers Use Email in a KeyLogging Attack?

Keyloggers use email most popularly when initiating this threat type. When you open these emails, you will see language like “You will lose all of your data” and “Act immediately.” As a result, you might act quickly and open links in the email, inputting information that the keylogger hacker can then track. This urgent language is a part of social engineering attack techniques, as this type of phishing attack tricks users out of thinking about their actions, causing them to move quickly and without thought, making the attack effective and successful.

Hackers will disguise keylogger email attachments that infect your computer once opened. Application downloads can permit malware to enter your system through this malicious software. Most commonly, malware keylogging attacks come in the form of Trojan Horses that look like regular emails and files but download viruses once opened.

What Other Methods Do Hackers Utilize to Send KeyLoggers?

The easiest way to initiate a keylogger attack would be through email attachments and downloads, but hackers might prefer to use other methods that could be equally efficient and effective. Here are the most popular other options:

- Doppelganger Domains appear like actual, legitimate websites that victims use. However, when users try to get to the popular website, the domain redirects them to these phishing pages, where hackers download malware and malicious files without the victim's knowledge. DNS management protects these counterfeit, identical websites from detection, which can make identification and avoidance difficult.

- Fake Chat Programs can be loaded onto phony apps that appear like Facebook or MSN. Users download the application and unknowingly permit hackers to log their input information. Google Play and the App Store make releasing apps for others to download easy, so this technique gets used frequently.

How Can I Detect a KeyLogging Attack?

Most firewalls and anti-virus software cannot detect or recognize keylogging attacks, which can be problematic since most companies rely on those services to ensure email security. These protective measures make keylogging a considerable threat to corporate networks.

Fortunately, you can suspect and identify keylogger attacks by observing your server closely. A keylogger could monitor your device if you notice slow Internet speeds, lost keystrokes, disappearing mouse cursors, and general web browser problems.

Consider installing a Virtual Private Network (VPN) on all business devices. A VPN can block any noticeable threats from entering your software and putting your company at risk. Protect your data and login credentials by enabling the VPN before any inputs.

Your task manager might pick up on a new, unrecognized process when logging your information that could be a keylogger. Check for keylogger installation by opening the Command System on your server and typing "netstat -a > C:\Users\username\Desktop" (make sure you put your username in that slot). Save the file to your desktop, open it, and choose to edit the file. If you see "TCP - LISTENING," a program, typically a keylogger, could be listening in for your connections on the computer.

Keep Learning About KeyLogger Attacks

Hackers use keyloggers to capture login and password information on personal computers via email attachment downloads. Typically, keyloggers utilize phishing email attacks to get you to download attachments or open up malicious links so that their applications can install themselves and track your keystrokes. Hackers have developed fake applications and websites that can threaten your company if you input data into the server.

Various email security best practices are available to keep your server safe against keylogging attacks. Look out for any odd computer behavior that could indicate someone or something else is meddling with the settings on your computer. Avoid unintentionally installing keyloggers on your computer by downloading the attachment from unknown sources. Keep your anti-virus software up-to-date and enable real-time email protection software. Make sure to have strong passwords and test them against dictionary attacks, as sandboxing malware can help you guarantee a certain degree of phishing protection.