USB KeyLogger Malware

Jose, Jason, Edward

Keylogger Definition

A keylogger, or keystroke logger, is a type of spyware that monitors and records keystrokes on a computer or mobile device. Keylogging can be executed through either software or hardware and is used for both legal and illegal purposes.

How Keyloggers Work

Keyloggers function by capturing the interactions a user has with their keyboard. This allows the recording of every email, instant message, search query, password, username, or other typed sequences.

Reasons for Keylogger Usage

Keyloggers are often used for malicious purposes, such as ransomware attacks where the attacker gains control of a system, encrypts it, and demands ransom for its release. Malicious hardware like flash drives can also be employed, capable of running files on older operating systems, acting as a human interface device, loading malware, being configured as a boot device, or functioning as an ethernet adapter. Techniques like social engineering trick users into plugging in malicious hardware. For instance, 'Juice Jacking' involves hacking public USB charging ports. USB devices can be used in various ways for attacks, including reprogrammed microcontrollers (like Rubber Ducky,

a commercial keystroke injection attack platform), USB Killers which trigger electrical surcharges to destroy devices, and Cold Boot Attacks where data is extracted from RAM using a USB flash drive.

Types of Keyloggers

Keyloggers are commonly spread online via phishing scams, Trojan viruses, and fake websites, aiming to obtain personal information. They fall into two broad categories: software-based and hardware-based.

Software-Based Keyloggers

These keyloggers often have rootkit functionality, allowing them to hide within systems to track activity and forward data to cybercriminals. They can monitor clipboard activity, location data, or even access microphones and cameras. Software keyloggers operate at various levels, including the kernel level (affecting the core operating system), API level (intercepting signals from the keyboard to programs), screen level (taking screenshots), and browser level (recording web form entries).

Hardware-Based Keyloggers

Hardware keyloggers have a physical component and are not detectable by antivirus software. They are implemented in various ways, like keyboard overlays in ATM skimming attacks, physical drives delivered via USB or Mini PCI cards, external

recording devices like cameras, and even acoustic methods that record distinct sounds made by different keyboard keys.

Preventing Keylogging Attacks

To mitigate keylogging risks, enable two-factor authentication, avoid downloading unknown files, consider using virtual keyboards, use password managers, consider voice-to-text conversion software, and use antivirus software with anti-spyware and anti-keylogger protection.

Legal and Ethical Aspects of Keyloggers

Keyloggers are used by corporations for system troubleshooting or employee monitoring, by parents for monitoring children's activities, and even by suspicious spouses. While legal if the device owner installs it, concerns arise when malicious actors use keyloggers, as they can capture sensitive information and send it to remote servers. Hardware keyloggers, embedded in PCs or as keyboard plugins, are particularly insidious.