

KEYLOGGERS IN THE NEWS

Keyloggers have become increasingly prevalent and dangerous in today's digital age. According to recent estimates, millions of devices are infected with keylogging malware, which allows hackers to monitor and record everything a user types on their device, including usernames, passwords, and other sensitive information. This malware is growing in popularity among hackers as they can be used to steal the credentials needed in a data breach.

Below is a series of recent articles implicating keylogging software. EndpointLock™ Keystroke Encryption technology will block keylogging malware and protect sensitive personal and financial information by encrypting the keystrokes entered on any PC or mobile device.

December 5, 2023

[WHAT IS TROJAN HORSE MALWARE?](#)

Downloader Trojans: These Trojans are primarily focused on downloading and installing additional malicious software, such as ransomware or **keyloggers**, onto the infected system. Some Trojans are designed to steal sensitive information, such as login credentials, credit card details, or personal files. They often use techniques like **keylogging**, where they record keystrokes, or screen capture, where they take screenshots of the user's activities.

November 21, 2023

[BEWARE OF THE INSIDIOUS BLACK FRIDAY FRAUD](#)

Scammers will replicate the retailer website's URLs and layouts, which makes it extremely hard to spot whether it is fraudulent or not. However, majority of the time the link is fake, and clicking on it will invite an intrusion of malware on your device, making your personal information vulnerable. Once they have encouraged people to click, they will then send phishing messages and **keylogging malware** straight to your device.

November 13, 2023

[ATOM KEYLOGGER – THE BUDGET FRIENDLY MALWARE FOR ASPIRING CYBERCRIMINALS](#)

Atom Keylogger is marketed as an **affordable keylogging solution** for novice hackers and criminals. It can record keystrokes, websites visited, chats and instant messages, emails, screenshots, and more. Atom Keylogger only costs around \$15, making it appealing for criminals on a budget. It accepts payment through cryptocurrencies like Bitcoin for anonymity. The keylogger is being advertised and sold on underground cybercrime forums frequented by hackers and scammers.

October 16, 2023

[TYPES OF VIRUSES THAT CAN SNEAK INTO GOOGLE DRIVE AND HOW TO AVOID](#)

An example of the type of virus that can reach you through Drive is what is known as **a keylogger**. It is a threat that records keystrokes that you do on your device and in this way steal passwords or any confidential data that you may put, either on your computer or on your mobile.

October 10, 2023

[HOW KEYLOGGERS HAVE EVOLVED FROM THE COLD WAR TO TODAY](#)

Keyloggers have been used for espionage since the days of the typewriter, but today's threats are easier to get and use than ever.

October 1, 2023

[HOW TO HACK FACEBOOK ACCOUNTS WITHOUT PASSWORD IN 2023](#)

Keylogging is when a sneaky program secretly records the keys you press on your keyboard. This can be a problem because if someone gets a hold of what you type, they might figure out your Facebook password and enter your account.

August 24, 2023

[THREAT ACTORS GET CREATIVE, HP STUDY FINDS](#)

Spot the difference – blogger or **keylogger**: Attackers behind recent Aggah campaigns hosted malicious code within popular blogging platform, Blogspot. By hiding the code in a legitimate source, it makes it harder for defenders to tell if a user is reading a blog or launching an attack. Threat actors then use their knowledge of Windows systems to disable some anti-malware capabilities on the users' machine, execute XWorm or the AgentTesla Remote Access Trojan (RAT), and steal sensitive information.

August 16, 2023

[HOW TO HACK INTO SOMEONE'S SNAPCHAT IN 2023](#)

Keyloggers can be installed remotely through phishing emails, manipulation of social interactions, or malicious links sent via text messages. Once installed, the software remains hidden, making it challenging for victims to detect the security breach.

March 24, 2023

[ROYAL MAIL-OWNED LOGISTICS COMPANY GLS HIT BY INFESTEALING CYBER ATTACK](#)

The malware being used, Gozi, is “a well-known banking trojan which now has many variants, and capabilities such as infostealing, **keylogging** and malicious redirects,” explains Louise Ferrett, threat intelligence analyst at Searchlight Security.

March 23, 2023

[NOVEL MALWARE DISTRIBUTION TECHNIQUES LEVERAGED BY HACKERS](#)

Such methods have enabled the deployment of the Chinotto malware, which has been updated to allow screenshot capturing and **keylogging**, with obtained data exfiltrated to a remote server.

March 19, 2023

[RESEARCHERS CREATE POLYMORPHIC MALWARE BLACKMAMA WITH CHATGPT](#)

The ChatGPT-powered Blackmamba malware works as a **keylogger**, with the ability to send stolen credentials through Microsoft Teams.

March 14, 2023

[AI USED TO GENERATE POLYMORPHIC KEYLOGGER](#)

Every time BlackMamba executes, it re-synthesizes its **keylogging** capability, making the malicious component of this malware truly polymorphic.

March 12, 2023

[WHAT IS A SNAKE KEYLOGGER AND ARE YOU AT RISK?](#)

When Snake **Keylogger** is sent to a potential victim, it is contained within an attachment. If the recipient opens the attachment, they are then asked to open a DOCX file. This DOCX file contains a macro (a form of computer virus) that allows for the launch of Snake Keylogger. If the victim is using a version of Microsoft Office that has security vulnerabilities (which often come in the form of software flaws), the keylogger can exploit them and infect the device.

February 28, 2023

[HACKER BREACHED LASTPASS BY INSTALLING KEYLOGGER ON EMPLOYEE'S HOME COMPUTER](#)

LastPass, one of the most popular password managers on the market has revealed that hackers stole (ironically) a “master password” that they used to access highly restricted corporate databases and information by targeting a senior engineer's home computer. The malware then **recorded the keystrokes** on the engineer's computer, enabling the hacker to capture the master password for the employee's password vault at LastPass.

January 2023

[HIPAA JOURNAL WARNING ABOUT KEYLOGGERS](#)

Accessing password-protected accounts from secondary devices further increases the risk of a data breach. Secondary devices often lack appropriate security protections and can contain malware that **logs keystrokes and captures passwords as they are entered.**

December 12, 2022 –

[HEALTH IT SECURITY](#)

The Health Sector Cybersecurity Coordination Center (HC3) issued a detailed **brief** regarding automation and its impacts on healthcare cybersecurity and beyond. In addition, threat actors leverage credential stuffing, brute force attacks, **and keyloggers.**

2022 Report

[REBUILDING A HEALTHCARE PROVIDER'S ENVIRONMENT AFTER A RANSOMWARE ATTACK](#)

After a healthcare provider's environment—including all of its viable backups—was locked by a ransomware attack, it needed experts who could understand the problem and rapidly craft a response to get its network back up and running, recover its data, and secure the network against future threats. A malware analysis quickly determined that it was a **keylogger**, evidence that the threat actor had stolen credentials in a more systematic way than the initial an analysis suggested.
