Updated 04-01-2023

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.

March 24, 2023

ROYAL MAIL-OWNED LOGISTICS COMPANY GLS HIT BY INFOSTEALING 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 Searchligh 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.

Keyloggers in the News continued

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.