Hacker Breached LastPass by Installing a Keylogger on Exec's Home Computer

Studies show that a majority of breaches begin this way. Security Regulators like HIPAA are taking notice

What Happened?

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.

According to a LastPass spokesperson, “This attack targeted one of only four senior DevOps engineers who had the required high-level security authentication necessary to use the decryption keys required to access the cloud storage service -- and the attackers did so by targeting their home computer.”[1]

How It Happened

According to PC Magazine, “One lingering question had been how the culprit broke into LastPass, despite its various security safeguards. The company held its encrypted password vault data in a cloud-based backup system, which required both Amazon AWS Access Keys and the LastPass-generated decryption keys in order to enter.”

LastPass stated that only four DevOps engineers at the company possessed the necessary decryption keys through a “highly restricted set of shared folders.” However, the hacker circumvented the company’s security safeguards by serving keylogging malware to one of the DevOps engineers at their home.

“This was accomplished by targeting the DevOps engineer’s home computer and exploiting a vulnerable third-party video streaming software package, which enabled remote code execution capability and allowed the threat actor to implant keylogger malware,” LastPass said.

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. The same keylogging malware appears to have helped the hacker bypass the multi-factor authentication on the account, which contained the decryption keys required to access LastPass’s cloud backup system.[1]

Two Key Security Vulnerabilities

1. Today, a majority of companies including hospitals, banks, universities, and government agencies allow their employees to access company data from their personal devices. This practice has proven to improve productivity, make work more efficient and save on device procurement costs. However, these devices are more difficult to secure. 67% of companies say it is certain or likely that their organization had a data breach as a result of employees using their mobile devices to access their company's sensitive and confidential information.[3]

2. Keyloggers are one of the main components of malware needed to advance a breach including the attack on LastPass. Once installed, they are hard to detect by antivirus and can often remain undetected on a device for months and sometimes years monitoring everything a user types.

HIPAA recently addressed both of these vulnerabilities above in their January 1, 2023 Journal: "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."[4]

How to Stop the Threat of Keyloggers

By utilizing EndpointLock™ Keystroke Encryption software, all keystrokes are encrypted making them unreadable to keyloggers. EndpointLock's Keystroke Transport Layer Security (KTLS™) Protocol provides strong cryptography at the time of keystroke entry. This protects the initial transmission of usernames and passwords and subsequent keystrokes entered into any PC or mobile device. EndpointLock™ would have played an integral part in preventing the attacks described above by eliminated the risk of keyloggers, preventing them from being able to obtain the secure credentials needed to further this attack.

References:

1. PC Magazine
2. PC Magazine
3. https://www.ponemon.org/
4. The HIPAA Journal