Cyber Security Report

Hackers Exploit Keyloggers to Breach Critical Systems

Protecting Businesses and Their Customers from Cyber Threats

February 2025

EndpointLock™
Desktop and Mobile Security

February 2025

Hackers Exploit Keyloggers to Breach Critical Systems

A recent high-profile cyberattack on LastPass, one of the world's leading password managers, exposed a major security risk: keyloggers installed on personal devices. Hackers successfully stole a master password, gaining access to highly restricted corporate databases—all by infecting a senior engineer's home computer with keylogging malware.

Unfortunately, this type of attack is becoming increasingly common, putting both businesses and their customers at risk.

How the Attack Happened:

According to LastPass, hackers:

- Targeted a senior DevOps engineer's home computer—one of only four employees with access to critical decryption keys.
- Exploited a vulnerability in third-party software to install keylogging malware.
- Captured every keystroke entered on the compromised device, including the master password for LastPass's internal system.
- Bypassed multi-factor authentication (MFA) using the stolen credentials, ultimately gaining access to sensitive corporate cloud storage.

Two Major Security Risks Businesses Face

1. Personal Devices Accessing Corporate Data

Many organizations—including banks, hospitals, universities, and government agencies—allow employees to access corporate data from personal devices. While this increases productivity and reduces costs, it also introduces security vulnerabilities.

◈ 67% of companies report they have likely suffered a data breach due to employees accessing sensitive company data on personal devices.[3]

2. The Stealthy Nature of Keyloggers

Keyloggers are among the most dangerous malware components in cyberattacks. Once installed, they:

✓ Operate undetected for months—or even years.
✓ Evade traditional antivirus software.
✓ Capture every keystroke, including usernames, passwords, and financial data.

How to Stop Keyloggers Before They Strike

The most effective way to combat keyloggers is by using keystroke encryption technology, such as EndpointLock™.

✅ Real-time Encryption – Encrypts keystrokes the moment they are typed, making them unreadable to keyloggers.
✅ Keystroke Transport Layer Security (KTLS™) Protocol – Ensures that sensitive information, like usernames and passwords, is protected from cyber threats.
✅ Multi-Device Protection – Secures both corporate and personal devices, preventing hackers from capturing critical credentials.

Prevent Attacks Like LastPass—Before They Happen

If EndpointLock™ had been installed on the compromised device in the LastPass breach, keyloggers would have been rendered useless—blocking hackers from stealing passwords, bypassing authentication, or accessing sensitive corporate data.

Businesses that prioritize cybersecurity can protect their employees, customers, and reputation by proactively securing every keystroke.

Ready to Strengthen Your Security?

Contact us today to learn how EndpointLock™ Keystroke Encryption can safeguard your business and customers from keylogging threats.

Visit www.advancedcybersecurity.com to discover how keystroke encryption can transform your security strategy.

References:

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