HIPAA warns healthcare organizations and hospitals of a possible vulnerability to Keylogging Spyware

HIPAA regulators discovered a vulnerability in healthcare systems that could be putting protected healthcare data at risk of keystroke stealing spyware. **EndpointLock™ Keystroke Encryption** secures vulnerable data by encrypting everything typed into a device.

HIPAA recently posted the following warnings in their January 1, 2023 Journals:

“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.”

“Surveillance malware (also known as “spyware”) enables cybercriminals to log keystrokes such as login credentials for healthcare systems. With this information, cybercriminals can remotely access the systems and exfiltrate ePHI to commit identity theft and healthcare fraud.”

According to research, 71% of healthcare facilities allow employees to use their own personal ”secondary” devices to access password protected healthcare data. This saves the hospital or practice time and improves the productivity of clinicians, makes patient care more efficient and saves on device procurement costs. However, with data breaches on the rise, there is a greater need to secure these devices.

Keylogging spyware is one of the most common, yet dangerous components of malware commonly downloaded to a device as a result of phishing, the practice of tricking unsuspecting victims into clicking on an infected link. Studies show more than 90% of all data breaches start with a phishing attack.

References:
HIPAA Journal
Health Exec

ACS
Advanced Cyber Security Corp.

Solve the HIPAA concerns of keyloggers and protect your healthcare data with keystroke encryption

Install **EndpointLock™ Keystroke Encryption** on all devices accessing the healthcare system, to help prevent exposing sensitive healthcare data and passwords that can lead to HIPAA fines.

EndpointLock™ Keystroke Encryption software encrypts everything typed into a device and stops the vulnerability of keylogging spyware. **EndpointLock™ can** protect what antivirus can't. 72% of security attacks happen because antivirus is unable to detect the malware. Hackers will always find ways to trick unsuspecting victims into downloading a keylogger onto their device, but with **EndpointLock™** installed, the spyware is rendered useless. This encryption technology is so effective against cybercrime, it's the method chosen by top Financial Institutions and the U.S. Military.

EndpointLock™ Key Benefits:

➔ Proactive approach extends protection to the keystroke. This added layer of protection is not available in any other security product.

➔ Blocks even the keyloggers not yet catalogued by antivirus (zero-day).

➔ Secures Protected Access Credentials, BYOD and Remote Login which can pose the highest threat.

➔ Scalable: EndpointLock™ can be easily deployed out across your enterprise using the same methods you currently use for software deployment.

➔ Compatible Platforms: Windows, Android and iOS

ACS
Advanced Cyber Security Corp.