Cyber Security Report

Keystroke Encryption in Healthcare

Protecting Electronic Health Records in the Healthcare Industry

February 2025

Advanced Cyber Security Corp.

EndpointLock™ Keystroke Encryption

The urgent need for Keystroke Encryption to protect patient data

The Shortcomings of Traditional Encryption Methods

The industry's definition of End-to-End Encryption, which includes encrypting data at rest and in transit is not sufficient for the goal of achieving true HIPAA compliance in today's threat landscape. These methods fail to address the vulnerability that exists with unencrypted keystrokes.

Keylogging malware can exploit this weakness, silently capturing every keystroke, including sensitive information like login credentials and patient data, before it's encrypted. This poses a significant threat as 80% of keyloggers can bypass many traditional security measures. **(**TechJury**)**

The vulnerability of unencrypted keystrokes was starkly illustrated by the LastPass breach, where a hacker stole a master password by keylogging a senior engineer's computer. Despite LastPass employing robust security measures like antivirus, VPN, EDR, MFA, and a segmented database, the keylogger still compromised their system. This incident underscores the need for keystroke encryption to supplement traditional security practices and protect against this increasingly prevalent attack vector. (PC Magazine)

Expert Insight

"Current measures predominantly focus on encrypting data in transit or at rest; however, they fall short of protecting data at its point of entry: the keystroke level. This gap in security architecture leaves a window open for keyloggers and malware to capture unencrypted inputs directly from users' keyboards." **-Dr. Massimiliano (Max) Pala, PhD: World-Renowned Cryptologist and Cybersecurity Expert**

HHS Highlights the Dangers of Keyloggers

January 7, 2025 - HIPAA Journals §164.308

"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 17, 2024 - Health Sector Cybersecurity Coordination Center (HC3): Report: 202412171700

"Malicious software can be deployed by cyberattackers to intercept a victim's keystrokes. This can include credentials as they are being entered as part of a valid login attempt."

December 19, 2024, HIPAA Journals.

"Malware, such as keyloggers, is used to harvest credentials and is commonly distributed in phishing emails, spoofed websites, and fake and pirated software. Keyloggers can record keystrokes as they are typed on a keyboard, and many other types of malware have credential harvesting capabilities."

Recent Healthcare Breaches Linked to Known Keyloggers

According to experts, keyloggers are leveraged in most healthcare breaches. These are a few:

1. **Vanderbilt University Medical Center**

    - Keylogger infiltrated administrative workstations.
    - Captured login credentials and patient demographic information.
    - Root cause: third-party vendor vulnerability.
2. **Common Spirit Health**
    - Financial billing software compromised by keylogger malware.
    - Exfiltration of patient financial and insurance data.
3. **Massachusetts General Hospital**
    - Security scans detected a keylogger linked to a compromised email account.
    - Risk of unauthorized access to electronic health records.

Industry Data

- According to Sophos, nearly 50% of malware detections in 2023 were keyloggers, often used to steal credentials, extort victims, and deploy ransomware.
- Expert Insights reported in February 2024 that 60% of phishing attacks involved keylogger software.

Mitigating the Threat of Keyloggers

Keystroke encryption provides a critical layer of defense by securing data at the point of entry. Even if a keylogger successfully infiltrates a device, keystroke encryption renders captured keystrokes meaningless, thwarting attempts to harvest sensitive information.

_____