BREAKING CYBERSECURITY NEWS: MICROSOFT TRUSTED SIGNING SERVICE ABUSED TO CODE-SIGN MALWARE

Vairav Cyber Security News Report

Date: March 24th, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A recent cybersecurity incident has surfaced where cybercriminals are exploiting Microsoft's Trusted Signing platform to code-sign malware executables using short-lived, three-day certificates including those used in a Crazy Evil Traffers crypto-theft campaign and Lumma Stealer campaigns. By leveraging these certificates, attackers can make malicious software appear legitimate, potentially bypassing security filters that typically block unsigned executables.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: Attackers are abusing Microsoft's Trusted Signing service to obtain short-lived code-signing certificates signed by "Microsoft ID Verified CS EOC CA 01", which they use to sign malware. Code-signing certificates authenticate the origin and integrity of software, and when misused, they can deceive users and security systems into trusting malicious code.

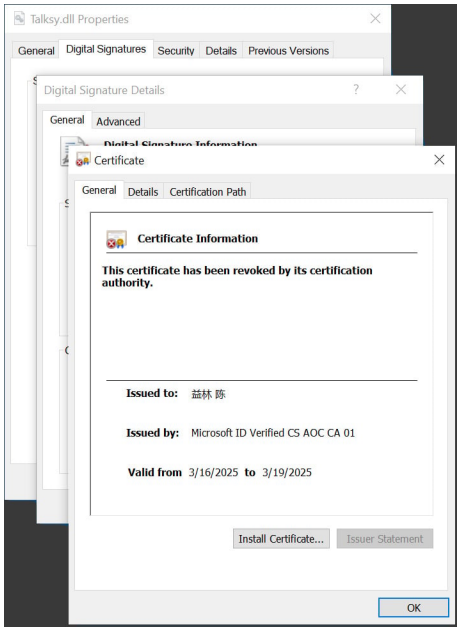

Figure 1: Signed DLL from Crazy Evil traffers campaign

Affected Entities/Industries: No particular industries or entities appear to be a target. However, this technique could be used to increase risk of malware infections on any system as Microsoft Trusted signing service includes certificate authorities that are part of the Microsoft Trusted Root Certificate program and meet WebTrust certification criteria.

Potential Impact: If an attacker manages to sign a malicious executable using Trusted Signing, the malware would appear legitimate to the operating system and security tools because it's signed with a valid Microsoft-trusted certificate. Antivirus and endpoint protection software might overlook it which could lead to supply-chain attacks, credential theft or ransomware attacks as a consequence of malware being allowed to run bypassing traditional security measures.

Exploitation Methods: Attackers exploit the Trusted Signing service to obtain legitimate-looking certificates, which are then used to sign malware.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Revoke any misused certificates identified during the investigation.
- Update security tools to detect and block malware signed with short-lived certificates.

Security Best Practices

- Implement strict code-signing policies and validate the authenticity of certificates.
- Educate users about the risks associated with trusting digitally signed files without verification.

For Advanced Security Teams

- Monitor for anomalies in certificate issuance and usage within the organization's infrastructure.
- Develop detection rules to identify and flag executables signed with short-lived or suspicious certificates.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://www.bleepingcomputer.com/news/security/microsoft-trusted-signing-service-abused-to-code-sign-malware/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com