BREAKING CYBERSECURITY NEWS: MEDUSA RANSOMWARE USES MALICIOUS DRIVER TO DISABLE ANTI-MALWARE WITH STOLEN CERTIFICATES

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 involving the Medusa ransomware group has unveiled a sophisticated tactic where attackers utilize a malicious driver, dubbed "ABYSSWORKER," to disable endpoint detection and response (EDR) systems. This approach allows the ransomware to operate undetected, leading to potential data encryption and significant operational disruptions. Security experts are advising organizations to bolster their defenses against such advanced evasion techniques.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: The Medusa ransomware group has been observed employing a bring your own vulnerable driver (BYOVD) attack strategy. In this method, a malicious driver named "ABYSSWORKER" is deployed to disable anti-malware tools, specifically targeting EDR systems. The driver, "smuol.sys," mimics a legitimate CrowdStrike Falcon driver ("CSAgent.sys") and is signed using likely stolen, revoked certificates from Chinese companies. Once installed, it can terminate processes, delete files, and remove security callbacks, effectively blinding security products.

Identification: Elastic Security Labs identified this tactic during an investigation into a Medusa ransomware attack. They observed the ransomware being delivered via a loader packed with HeartCrypt, accompanied by the ABYSSWORKER driver designed to disable EDR vendors.

Threat Actor: The Medusa ransomware group operates as a ransomware-as-a-service (RaaS) model. Active since June 2021, they have transitioned from a closed-group operation to an affiliate-based ecosystem, allowing various cybercriminals to leverage their ransomware platform.

Affected Entities/Industries: Medusa has compromised over 300 organizations across critical infrastructure sectors, including healthcare, education, legal, insurance, technology, and manufacturing.

Potential Impact: The use of the ABYSSWORKER driver to disable EDR systems allows the ransomware to encrypt data without detection, leading to operational downtime, financial losses, data breaches and reputational damage. Additionally, Medusa employs a double extortion strategy, threatening to publicly release stolen data if ransoms are not paid.

Exploitation Methods: The attack chain involves:

- Deploying the ABYSSWORKER driver to disable security defenses.
- Utilizing a HeartCrypt-packed loader to deliver the Medusa ransomware encryptor.
- Exploiting stolen, revoked certificates to sign the malicious driver, enhancing its ability to bypass security measures.

RELATED THREAT INTELLIGENCE & IOCs

Malware Hashes (SHA256)

- 6a2a0f9c56ee9bf7b62e1d4e1929d13046cd78a93d8c607fe4728cc5b1e8d050
- b7703a59c39a0d2f7ef6422945aaeaaf061431af0533557246397551b8eed505

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Ensure all drivers are from trusted sources and verify their digital signatures.
- Implement application whitelisting to prevent unauthorized driver installations.
- Update and patch all systems and software to mitigate vulnerabilities.

Security Best Practices

- Employ multi-factor authentication (MFA) across all access points.
- Regularly back up critical data and store backups securely offline.
- Conduct regular security awareness training for employees to recognize phishing attempts and malicious attachments.

For Advanced Security Teams

- Deploy advanced threat detection tools capable of identifying anomalous driver installations.
- Monitor for signs of BYOVD attacks and unauthorized driver activities.

- Utilize endpoint detection and response (EDR) solutions that can detect and prevent tampering attempts.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/03/medusa-ransomware-uses-malicious-driver.html
- https://www.elastic.co/security-labs/abyssworker

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