SECURITY ADVISORY

September, 2024

Cicada3301: Cross-Platform Ransomware

Context

A new and formidable threat has emerged in the cybersecurity landscape: a Rust-based ransomware variant known as Cicada3301. This advanced malware targets both Windows and Linux systems, reflecting its cross-platform versatility and raising alarms across diverse IT environments. Cicada3301 is linked to a notorious adversarial group with a history of attacking critical sectors, including government, healthcare, and financial institutions.

The sophistication of Cicada3301 lies not only in its cross-platform capabilities but also in its execution of a double-extortion strategy. Initially, the ransomware infiltrates corporate networks to exfiltrate sensitive data, followed by the encryption of the victim's devices. The attackers then leverage both the encryption key and the threat of publicly releasing the stolen data to coerce organizations into paying the ransom.

A key concern is Cicada3301's advanced evasion techniques, particularly its ability to bypass traditional endpoint detection and response (EDR) systems. The ransomware employs sophisticated methods, such as weaponizing vulnerable signed drivers, to evade detection and complicate mitigation efforts. This dual-layered approach and its EDR evasion tactics significantly amplify the threat posed by Cicada3301, underscoring the critical need for robust, multi-faceted cybersecurity defenses. Organizations must be vigilant and proactive in their security measures to effectively counter this evolving and dangerous adversary.

Mitigation

Defending against the Cicada3301 attack requires immediate and proactive measures:

Monitor and Update EDR: Stay informed about EDR bypass techniques and regularly update your EDR systems. Keep your EDR engine independent from your EPP (Endpoint Protection Platform) to reduce the risk of both systems being evaded if one is compromised.

Block High-Risk Sources: Use geo-blocking and filtering to restrict access from high-risk countries, ASNs, and TLDs to reduce exposure to potential attacks.

Secure and Test Backups: Implement regular, automated backups with secure storage and periodically test restoration processes to ensure data integrity and availability.

Technical Details

Cicada3301's sophisticated capabilities and strategic design pose a significant threat to enterprise environments. For a detailed understanding of this advanced ransomware, the technical specifics of Cicada3301 are outlined below:

Encryption Mechanism:

- **Encryption Algorithm:** Cicada3301 employs AES-256 for encrypting files. The symmetric key used in this process is further encrypted with RSA, ensuring a robust layer of security against unauthorized access.
- **File Encryption:** The ransomware specifically targets documents, databases, and configuration files, rendering these files inaccessible without the decryption key. Encrypted files are marked with a random seven-character extension and accompanied by ransom notes labeled RECOVER-[extension]-DATA.txt.

Execution and Disruption:

- **Delay Mechanism:** The ransomware includes a sleep parameter to delay execution, complicating detection and mitigation efforts.
- **Virtual Machine Impact:** Cicada3301 can encrypt VMware ESXi virtual machines, often without shutting them down beforehand. By issuing ESXi commands to shut down VMs and delete snapshots prior to encryption, the ransomware maximizes disruption and damage, reflecting a strategic intent to cause extensive operational harm.

Additional Characteristics:

- **Cross-Platform Compatibility:** Capable of executing on both Windows and Linux systems, highlighting its broad reach.
- **Command and Control (C2) Infrastructure:** The ransomware connects to a remote C2 server to receive encryption keys and exfiltrate stolen data.
- **Self-Destruct Mechanism:** Post-encryption, Cicada3301 deletes itself to evade detection and forensic analysis, complicating recovery efforts.

Tactics, Techniques and Procedures

The following TTPs have been observed in relation to Cicada3301:

- **Initial Access (TA0001):** Spear-phishing emails with malicious attachments or links.
- **Execution (TA0002):** Execution of the ransomware binary on the victim's system.
- **Persistence (TA0003):** Use of scheduled tasks or cron jobs to maintain persistence.
- **Privilege Escalation (TA0004):** Exploitation of vulnerabilities to gain elevated privileges.
- **Defense Evasion (TA0005):** Obfuscation techniques and self-deletion after encryption.
- **Credential Access (TA0006):** Harvesting of credentials from memory or configuration files.
- **Discovery (TA0007):** Network and system reconnaissance to identify high-value targets.
- **Lateral Movement (TA0008):** Use of legitimate admin tools for lateral movement across the network.
- **Collection (TA0009):** Gathering of sensitive data before encryption.
- **Exfiltration (TA0010):** Exfiltration of data to a remote C2 server.
- **Impact (TA0040):** File encryption to disrupt operations and demand ransom payment.

Cyber Threat Intelligence

Cicada3301 is likely linked to a sophisticated adversarial group with a history of targeting high-profile organizations, possibly operating from Eastern Europe. This group is known for employing advanced tools and techniques. The ransomware bears significant similarities to the now-defunct BlackCat (ALPHV) operation, both in its development and in its technical behaviors.

Cicada3301's tools and tactics exhibit overlap with those of BlackCat, including the use of ChaCha20 for encryption, and utilities such as fsutil and IISReset.exe to manage encrypted files and services. The ransomware also utilizes advanced evasion techniques, such as weaponizing vulnerable signed drivers to bypass endpoint detection and response (EDR) systems, a method previously adopted by the BlackByte ransomware group.

The ransomware primarily targets small to medium-sized businesses (SMBs) through opportunistic attacks exploiting system vulnerabilities. Additionally, there are indications that Cicada3301 may be associated with the Brutus botnet for initial access to enterprise networks, suggesting a strategic continuity from BlackCat's operations to the current Cicada3301 campaign.

References

IOCs:

- https://www.truesec.com/hub/blog/dissecting-the-cicada
- https://otx.alienvault.com/pulse/66d53853b84baa0892b5c178

Public Intelligence:

- https://thehackernews.com/2024/09/new-rust-based-ransomware-cicada3301.html
- https://www.bleepingcomputer.com/news/security/linux-version-of-new-cicada-ransomware-targets-vmware-esxi-servers/
- https://www.techrepublic.com/article/vmware-esxi-ransomware-cicada3301/
- https://securityaffairs.com/167897/cyber-crime/a-new-variant-of-cicada-ransomware-targets-vmware-esxi-systems.html
- https://www.pcrisk.com/removal-guides/30895-cicada-3301-ransomware

Act now to protect your business!

Contact CyberStash today to learn about eclipse.xdr and our round-the-clock managed detection and response service.