THREAT ADVISORY

September 4, 2024

Cicada3301 Ransomware Targeting Linux-Based ESXi Servers

SUMMARY

A ransomware-as-a-service (RaaS) operation is posing as the legitimate Cicada 3301 organization and has already listed 19 victims on its extortion site. The new ransomware is employing techniques similar to BlackCat ransomware did. It uses robust encryption methods, exploits system utilities to disable security measures. The ransomware is distributed via a RaaS platform and targets a wide range of file extensions.

TECHNICAL DETAILS

Cicada3301 is a new ransomware variant, first seen in June 2024 and has been active in exploiting vulnerabilities in small to medium-sized businesses (SMBs). This ransomware is written in Rust, allowing it to operate on both Windows and Linux/ESXi platforms, showcasing its versatility and broader attack surface. Cicada3301 operates under a ransomware-as-a-service (RaaS) model, with its developers actively recruiting affiliates on underground forums.

Cicada3301 incorporates several advanced features from BlackCat, such as using ChaCha20 for encryption and manipulating system utilities like fsutil, IISReset.exe, and wevtutil to disrupt system recovery and erase traces of its activity. Additionally, it can execute remote commands using embedded credentials via PsExec, enhance network traffic capacity for malicious operations, and terminate processes related to backup and recovery to prevent data restoration.

The ransomware specifically targets a range of 35 file extensions important to enterprise operations, ensuring the encryption of valuable data, including: sql, doc, rtf, xls, jpg, jpeg, psd, docm, xlsm, ods, ppsx, png, raw, dotx, xltx, pptx, ppsm, gif, bmp, dotm, xltm, pptm, odp, webp, pdf, odt, xlsb, ptox, mdf, tiff, docx, xlsx, xlam, potm, and txt.

The use of the EDRSandBlast tool was also used by Cicada3301 to exploit vulnerabilities in signed drivers, a technique previously used by the BlackByte group, to evade endpoint detection and response (EDR) systems.

INDICATORS OF COMPROMISE (IOCs)

SHA-1:

- c08a863c2e5288d4ce2a9d46a725518f12711a7
- 54a8fe5c70ed0007fdd346a9a75977fd9f8ad24a

RECOMMENDATIONS

- Utilize advanced endpoint protection solutions to detect and block ransomware behaviors, including the misuse of legitimate tools for malicious activities.
- Ensure all systems and software are regularly updated to patch vulnerabilities that could serve as entry points for ransomware.
- Maintain frequent backups of critical data, and regularly test recovery processes to confirm they are effective in ransomware scenarios.
- Implement network segmentation to contain the spread of ransomware within isolated network segments.

- Enforce policies that restrict the execution of scripts, such as PowerShell, that attackers commonly exploit.
- Conduct user training to raise awareness of phishing risks and strengthen defenses against social engineering attacks.
- Deploy continuous monitoring tools to identify early indicators of compromise and enable rapid response to mitigate threats.
- Secure and monitor the use of administrative tools like PsExec, ensuring that management interfaces are not publicly accessible.

REFERENCES

- https://blog.morphisec.com/cicada3301-ransomware-threat-analysis
- https://www.morphisec.com/hubfs/ThreatAnalysis_CICADA3301_3.pd
- 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/