CIRT.GY Guyana National Computer Incident Response Team

AL2024_35 A New Threat Targeting Windows, Linux, and VMware ESXi Systems (02nd September 2024)

Description

Cicada3301 is a new ransomware group that targets Windows and Linux systems, especially VMware ESXi environments. They use double-extortion tactics, stealing data and encrypting devices to pressure victims into paying a ransom.

Details

Cicada3301 ransomware began promoting its operations on the RAMP cybercrime forum on June 29, 2024, but attacks were traced back to June 6, indicating initial independent operations. Written in Rust, the ransomware uses ChaCha20 and RSA encryption and has both Windows and Linux/VMware ESXi encryptors. In VMware environments, it shuts down VMs and deletes snapshots before encryption to limit recovery options. It appends a random seven-character extension to files and creates ransom notes named "RECOVER-[extension]-DATA.txt." similarities between Cicada3301 and ALPHV/BlackCat ransomware were seen, suggesting a possible rebranding or collaboration. There is also evidence linking Cicada3301 to the Brutus botnet for network access.

Indicators of Compromise (IoCs)

Organizations should monitor for the following indicators of compromise:

- **File Extensions:** Random seven-character extensions appended to encrypted files.
- **Ransom Note:** Files named "RECOVER-[extension]-DATA.txt" present in directories.

- **VM Commands:** Use of ESXi commands like esxcli and vim-cmd to shut down VMs and remove snapshots.

Remediation

To mitigate the risk posed by these attacks:

Immediate Actions:

- Isolate infected systems from the network to prevent further spread.
- Suspend all VM operations and back up any unaffected VMs.
- Conduct a comprehensive scan of your network for signs of Brutus botnet activity.

Recovery and Mitigation:

- Restore affected systems from backups if available.
- Review and strengthen access controls, particularly on VPN appliances and ESXi hosts.
- Apply patches and updates to all systems, especially those related to VMware ESXi and VPN appliances.

Preventive Measures:

- Implement robust endpoint protection and network monitoring to detect unusual activity.
- Enforce multi-factor authentication (MFA) for remote access and critical systems.
- Regularly test and update your incident response plan, ensuring it covers ransomware scenarios.

Long-term Strategy:

- Educate employees on phishing and social engineering tactics to reduce the likelihood of initial compromise.

- Conduct regular security audits and penetration testing to identify and remediate vulnerabilities.

References

Paganini, P. (2024, September 2). *A new variant of Cicada ransomware targets VMware ESXi systems*. Security Affairs. https://securityaffairs.com/167897/cyber-crime/a-new-variant-of-cicada-ransomware-targets-vmware-esxi-systems.html

Toulas, B. (2024, September 2). Linux version of new Cicada ransomware targets VMware ESXi servers. Retrieved from *BleepingComputer*. https://www.bleepingcomputer.com/news/security/cicada3301-ransomwares-linux-encryptor-targets-vmware-esxi-systems/