مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

TargetCompany Ransomware New Linux Variant targets ESXi Environments

Tracking #:432315931

Date:06-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed the TargetCompany ransomware group, also known as Mallox, has evolved to include a new Linux variant that Targets ESXi Environments.

TECHNICAL DETAILS:

The TargetCompany ransomware group was discovered in June 2021 and is tracked by Trend Micro as "Water Gatpanapun" with a leak site under the name "Mallox."

The new Linux variant uses a custom shell script for payload delivery and execution. The script exfiltrates victim information to two different servers, providing a backup of the information. The variant can determine whether the victim's machine is running in a VMWare ESXi environment.

The TargetCompany affiliate linked to the ransomware sample points to a broader campaign targeting expansive IT systems.

Features:

- Use of a PowerShell script to bypass Antimalware Scan Interface (AMSI) and abuse of fully undetectable (FUD) obfuscator packers.
- After its execution, it drops a text file named TargetInfo.txt that contains victim information and the contents of TargetInfo.txt will be sent to a command-and-control (C&C) server.
- After its encryption routine, this variant appends the extension ".locked" on encrypted files and drops a ransom note named HOW TO DECRYPT.txt (Figure 7). This is a departure from the usual extension and ransom note file name of its Windows variant.

Indicators of compromise (IOCs):

Hash	Description
dffa99b9fe6e7d3e19afba38c9f7ec739581f656	TargetCompany Linux Variant
2b82b463dab61cd3d7765492d7b4a529b4618e57	Shell Script
9779aa8eb4c6f9eb809ebf4646867b0ed38c97e1	TargetCompany samples related to affiliate vampire
3642996044cd85381b19f28a9ab6763e2bab653c	TargetCompany samples related to affiliate vampire
4cdee339e038f5fc32dde8432dc3630afd4df8a2	TargetCompany samples related to affiliate vampire
0f6bea3ff11bb56c2daf4c5f5c5b2f1afd3d5098	TargetCompany samples related to affiliate vampire
hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x.sh	Download URL of script

hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x	Download URL of ransomware
hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/post.php	Upload URL

RECOMMENDATIONS:

- Patch Systems: Ensure all systems, particularly Linux machines, are updated with the latest security patches. Prioritize patching vulnerabilities related to shell script execution.
- Endpoint Security: Implement and maintain robust endpoint security solutions capable of detecting and blocking suspicious script execution and lateral movement.
- Network Segmentation: Segment network to limit the spread of ransomware in case of an infection.
- VMware ESXi Security: Review and strengthen security measures for your VMWare ESXi environments. Consider multi-factor authentication and restricting access to critical systems.
- Backups: Maintain regular, secure backups of your data with a reliable recovery plan in place. Test your backups regularly to ensure data can be restored effectively.
- Employee Training: Train employees on cybersecurity best practices, including identifying phishing attempts and avoiding suspicious attachments or links.
- Incident Response Plan: Develop and test a comprehensive incident response plan to effectively respond to a ransomware attack.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://www.trendmicro.com/en_us/research/24/f/targetcompany-s-linux-variant-targets-esxi-environments.html?&web_view=true