Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

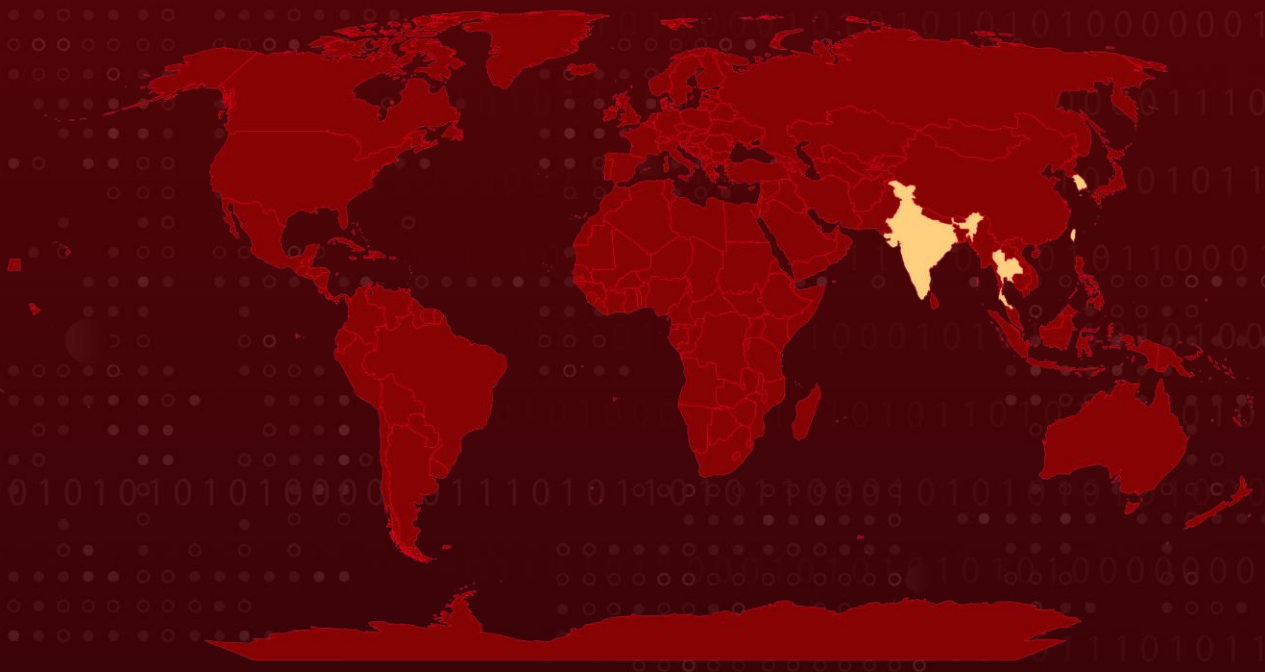
Novel TargetCompany Ransomware Linux Variant Now Attacks ESXi

Date of Publication	Admiralty Code	TA Number
June 6, 2024	A1	TA2024219

Summary

First Appearance: May 2024
Malware: TargetCompany ransomware (aka Mallox, Fargo, Water Gatpanapun, and Tohnichi)
Targeted Countries: Taiwan, India, Thailand, and South Korea
Affected Platforms: Windows, Linux, VMWare ESXi
Attack: The TargetCompany ransomware group has developed a new Linux variant using a custom shell script for payload delivery and execution, targeting VMWare ESXi environments to increase disruption and ransom payment chances. This variant exfiltrates victim data to two servers and is part of a broader campaign, with significant activity in Taiwan, India, Thailand, and South Korea. Continuous evolution of their techniques highlights the need for robust cybersecurity measures.

Attack Regions



Attack Details

#1 The TargetCompany ransomware group has introduced a new Linux variant that uses a custom shell script for payload delivery and execution, marking a departure from previous methods. This variant also exfiltrates victim information to two servers, ensuring backup. It specifically targets VMWare ESXi environments to disrupt operations and increase ransom payments.

#2 The group's activity is notably high in Taiwan, India, Thailand, and South Korea. Since its discovery in June 2021, TargetCompany, which has a leak site named “Mallox,” has evolved, using techniques like PowerShell scripts to bypass defenses.

#3 The Linux variant checks for administrative rights and uses a shell script to download and execute the payload, exfiltrating data and deleting evidence post-execution. The infrastructure involved, including an IP address hosted by China Mobile Communications, points to short-term use and a broader campaign. An affiliate known as "vampire" is linked to this variant, indicating a wider, high-ransom-demand operation.

#4 Previously, TargetCompany used its proprietary variant and the BatCloak obfuscator engine, known for full undetectability (FUD), and exploited MS-SQL vulnerabilities while employing brute force attacks. This continuous refinement of tactics underscores the importance of vigilant cybersecurity measures.

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with TargetCompany ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Patch and Update Software: Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. TargetCompany affiliates often exploit known vulnerabilities to gain initial access to systems. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited and prevent unauthorized access to their networks.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, storing them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a TargetCompany ransomware attack, up-to-date backups enable recovery without paying the ransom. Especially BitLocker users should secure recovery keys and maintain offline backups.

Access Control and Least Privilege: Enforce the principle of least privilege, ensuring that users and applications have only the minimum access required to perform their functions. This limits the potential impact of a ransomware attack.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0010 Exfiltration	TA0040 Impact
TA0007 Discovery	TA0005 Defense Evasion	TA0011 Command and Control	T1190 Exploit Public-Facing Application
T1070.004 File Deletion	T1082 System Information Discovery	T1070 Indicator Removal	T1059.004 Unix Shell
T1059 Command and Scripting Interpreter	T1105 Ingress Tool Transfer	T1048 Exfiltration Over Alternative Protocol	T1041 Exfiltration Over C2 Channel
T1486 Data Encrypted for Impact			

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x.sh, hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x, hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/post.php
SHA1	Dffa99b9fe6e7d3e19afba38c9f7ec739581f656, 2b82b463dab61cd3d7765492d7b4a529b4618e57, 9779aa8eb4c6f9eb809ebf4646867b0ed38c97e1, 3642996044cd85381b19f28a9ab6763e2bab653c, 4cdee339e038f5fc32dde8432dc3630afd4df8a2, 0f6bea3ff11bb56c2daf4c5f5c5b2f1afd3d5098

References

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

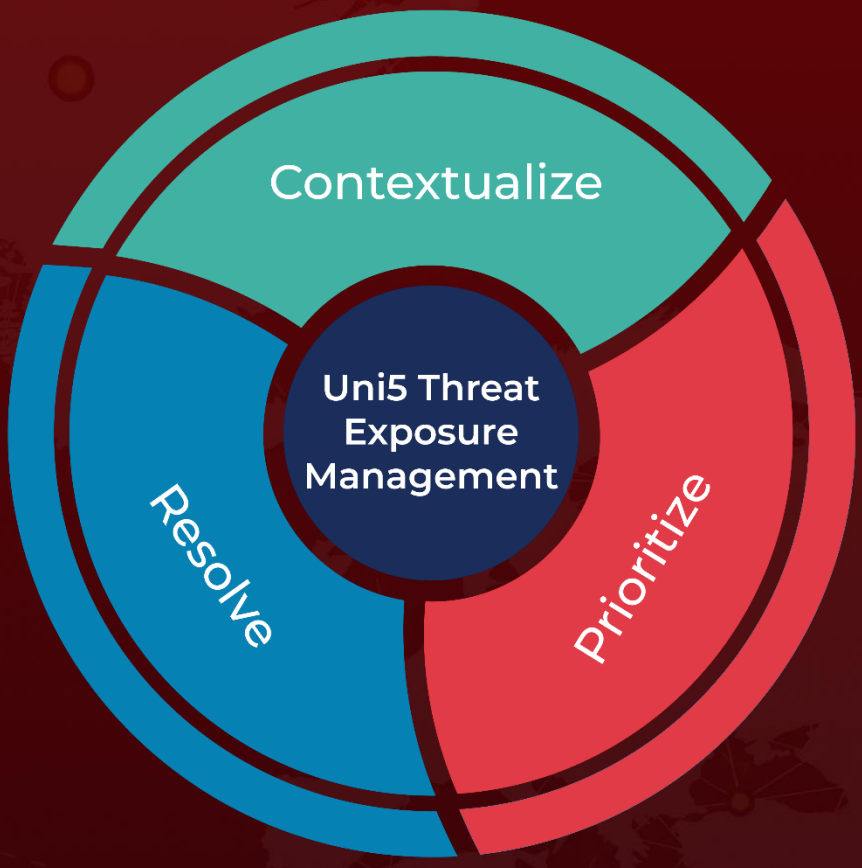
https://www.hivepro.com/threat-advisory/mallox-ransomware-a-resurgent-threat-exploiting-ms-sql-flaws/

https://www.hivepro.com/threat-advisory/targetcompany-ransomwares-fud-obfuscation-maneuvers/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 6, 2024 • 10:30 PM

More at www.hivepro.com