Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

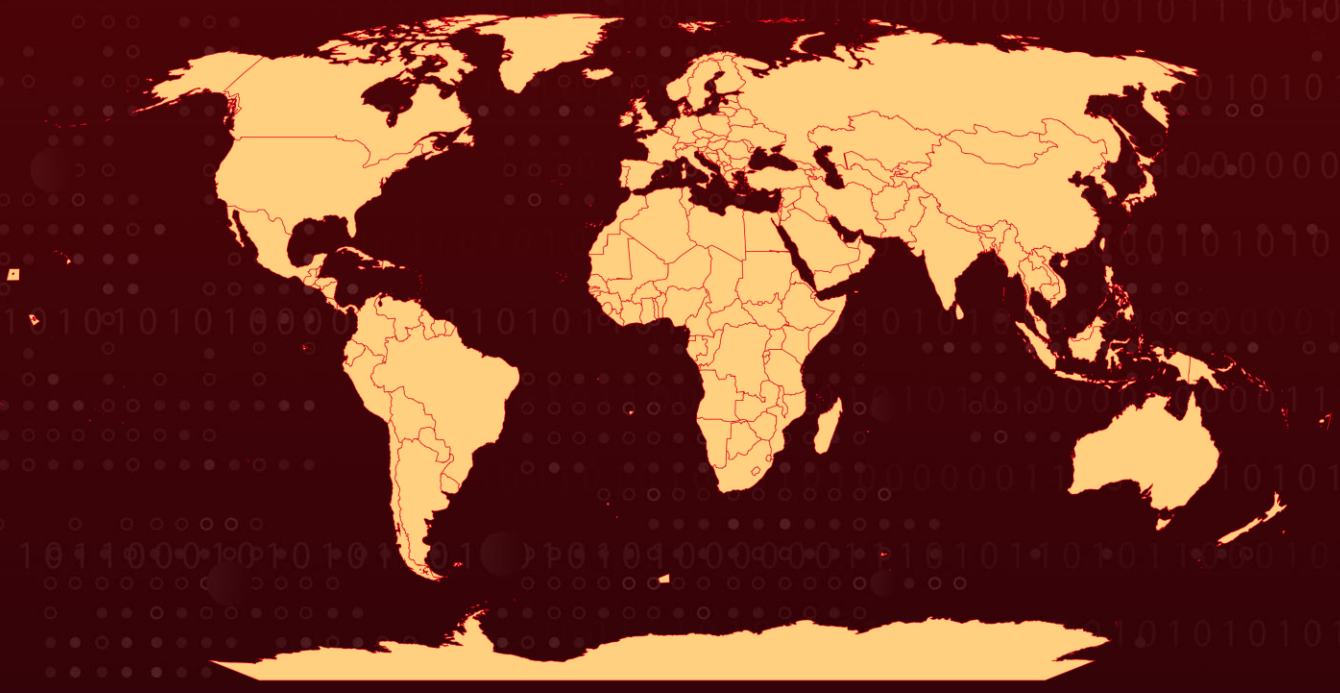
Agenda Ransomware Targets VMWare vCenter & ESXi Servers Globally

Date of Publication	Admiralty Code	TA Number
March 27, 2024	A1	TA2024119

Summary

Attack Began: December 2023
Targeted Countries: Worldwide
Malware: Agenda ransomware (aka Qilin, Water Galura)
Targeted Industries: Finance, Law, Construction, Healthcare, Real estate, and Technology
Affected Platform: VMWarce vCenter and ESXi servers
Attack: Agenda ransomware, also known as Qilin, active since 2022, targets global victims across industries. Their latest tactic leverages a custom script to infect VMWare environments, potentially crippling virtual machines and causing data loss. Organizations should be aware of this threat and take steps to protect themselves.

Attack Regions



Attack Details

#1

The Agenda Ransomware group, also known as Qilin or Water Galura, was discovered in 2022 and has since remained active and continually developed. It has been targeting victims globally with a particular focus on the US, Argentina, Australia, and Thailand. Their ransomware attacks have impacted various industries, including finance and law.

#2

Recent observations indicate an increase in Agenda ransomware detections since December 2023, suggesting heightened activity or expanded targeting. Agenda's virulence lies in its ability to spread laterally across VMWare vCenter and ESXi servers. When executed with a specific command (--spread-vcenter), the ransomware triggers a custom PowerShell script embedded within its code. This script facilitates the ransomware's propagation across these VMWare servers, potentially infecting virtual machines and disrupting the entire virtual environment.

#3

It also employs defense evasion tactics such as terminating VM clusters and leveraging vulnerable SYS drivers like YDark and Spyboy's Terminator. The ramifications of such an attack can be devastating. Widespread infection of virtual machines can lead to critical data loss, causing significant financial harm. Additionally, the disruption of services running on virtual environments can further cripple an organization's operations.

Recommendations

Keep Software Up-to-Date: Ensure that all software, including operating systems, applications, and security tools, is regularly updated with the latest patches and security updates. This helps to address known vulnerabilities that attackers may exploit.

Conduct Regular Data Backups and Test Restoration: Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom. Regularly test the restoration process to verify the integrity and availability of backups.

Endpoint Protection: Deploy advanced endpoint protection solutions that include anti-malware, anti-phishing, and behavior-based detection capabilities. Ensure that endpoint security software is configured to detect and block malicious activities, including attempts to exploit vulnerabilities.

Network Segmentation: Implement network segmentation to restrict the lateral movement of attackers within the network. Segment critical systems and sensitive data from less secure areas of the network to minimize the impact of a successful breach.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0008 Lateral Movement	TA0001 Initial Access	TA0002 Execution
TA0040 Impact	TA0005 Defense Evasion	TA0003 Persistence	TA0004 Privilege Escalation
T1059.003 Windows Command Shell	T1059 Command and Scripting Interpreter	T1021.004 SSH	T1021 Remote Services
T1570 Lateral Tool Transfer	T1486 Data Encrypted for Impact	T1480 Execution Guardrails	T1211 Exploitation for Defense Evasion
T1543.003 Windows Service	T1543 Create or Modify System Process	T1566 Phishing	T1059.001 PowerShell

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	73b1fffd35d3a72775e0ac4c836e70efefa0930551a2f813843bdfb32df4579a, e4cbee73bb41a3c7efc9b86a58495c5703f08d4b36df849c5bebc046d4681b70, afe7b70b5d92a38fb222ec93c51b907b823a64daf56ef106523bc7acc1442e38, dd50d1f39c851a3c1fce8abdf4ed84d7dca2b7bc19c1bc3c483c7fc3b8e9ab79

References

https://www.trendmicro.com/en_us/research/24/c/agenda-ransomware-propagates-to-vcenters-and-esxi-via-custom-pow.html

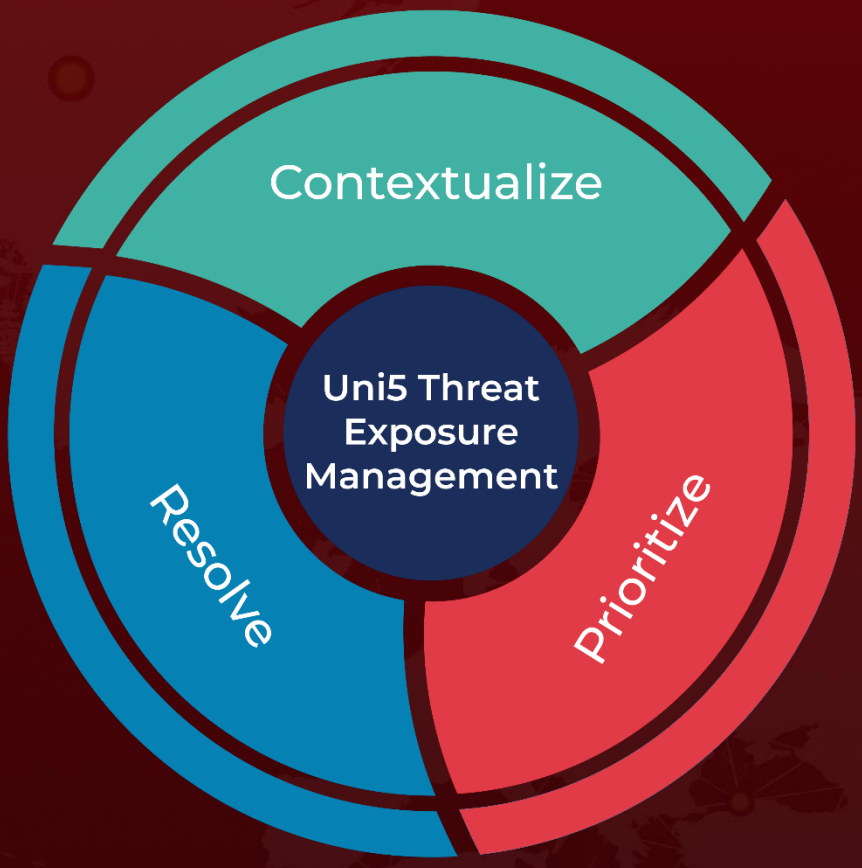
https://documents.trendmicro.com/assets/txt/ioc-agenda-ransomwareJwTLz0J.txt

https://www.hivepro.com/threat-advisory/agenda-ransomware-made-its-return-with-a-rust-variant/

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

March 27, 2024 • 5:30 AM

More at www.hivepro.com