Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

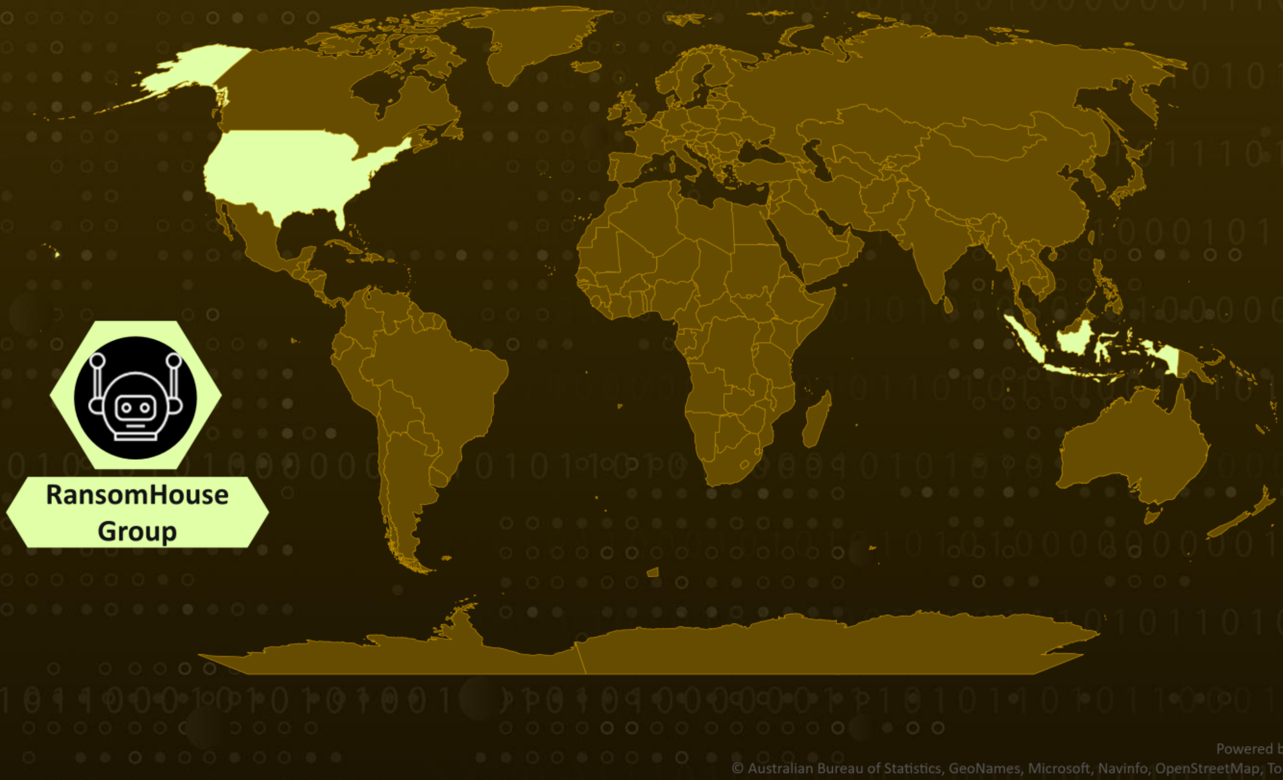
RansomHouse's MrAgent Reshaping Automation in Cyber Attacks

Date of Publication	Admiralty Code	TA Number
February 21, 2024	A1	TA2024069

Summary

First Seen: December 2021
Threat Actor: RansomHouse group
Malware: MrAgent, Mario Ransomware
Targeted Industries: Construction, Engineering, Healthcare, Electric Utilities, Financial Services
Attack Region: USA, Indonesia
Attack: The RansomHouse group, operating as a Ransomware-as-a-Service (RaaS) entity, has recently introduced a sophisticated tool named 'MrAgent' aimed at automating the deployment of its data encrypter across multiple hypervisors.

Attack Regions


RansomHouse Group
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 The RansomHouse group has deployed a sophisticated tool called 'MrAgent,' designed to streamline the deployment of its data encrypter across numerous hypervisors. RansomHouse falls under the category of a Ransomware-as-a-Service (RaaS) entity, which emerged in December 2021, infiltrating corporate networks with various ransomware variants.

#2 Notably, the RansomHouse group is renowned for utilizing a distinctive ransomware strain named Mario ESXi, in conjunction with the aforementioned MrAgent. This ransomware shares code elements with Babuk, following the leak of Babuk's source code. MrAgent operates at its core by identifying the host system, disabling its firewall, and automating the simultaneous deployment of ransomware across multiple hypervisors, compromising all managed virtual machines.

#3 The tool facilitates customizable configurations for ransomware deployment, directly received from the command and control (C2) server. These configurations include tasks such as setting passwords on the hypervisor, specifying encrypter command details and arguments, scheduling encryption events, and modifying the welcome message displayed on the hypervisor's monitor.

#4 Communication with victims is conducted through the RansomHouse group's Tor-based chat room, providing bilingual support in English and Chinese. In a significant incident of ransom extortion in mid-October 2023, the RansomHouse group exploited vulnerabilities in a company, resulting in the unauthorized acquisition of approximately 60 GB of sensitive data, including customer personal information.

#5 The initial ransom demand was set at $500,000. It is noteworthy that RansomHouse adopts a tactic of generating unique chat links for each victim, serving as a deliberate strategy to elude tracking efforts and introduce an additional layer of complexity to their operational procedures.

Recommendations

Data Backups: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Continuous Monitoring and Analysis: Establish continuous monitoring and analysis protocols to promptly detect any unusual network behavior, potentially indicating a long-term cyber espionage operation.

Network Segmentation: Employ network segmentation to isolate critical systems and sensitive data, limiting the lateral movement of an attacker within the network in case of a successful infiltration.

Heighten Awareness: Familiarize yourself with common phishing tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0042** Resource Development	**TA0007** Discovery
TA0008 Lateral Movement	**TA0009** Collection	**TA0010** Exfiltration	**TA0011** Command and Control
TA0040 Impact	**T1016** System Network Configuration Discovery	**T1021.001** Remote Desktop Protocol	**T1021.002** SMB/Windows Admin Shares
T1059.004 Unix Shell	**T1071** Application Layer Protocol	**T1078.002** Domain Accounts	**T1190** Exploit Public-Facing Application
T1486 Data Encrypted for Impact	**T1560** Archive Collected Data	**T1567.002** Exfiltration to Cloud Storage	**T1583.004** Server
T1588.001 Malware			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	8189c708706eb7302d7598aeee8cd6bdb048bf1a6dbe29c59e50f0a39fd53973, bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce70f82f2c, 3934b3da6bad0b4a28483e25e7bab919d7ed31f2f51cca22c56535b9f8183a0e, afe398e95a75beb4b0508c1bbf7268e8607d03776af0b68386d1e2058b374501, 2c1a4fe4a2ac4f0a49052f9521458136eb477fe23665dc4b7076fbd32de3005d, 2c1475f1b49a8b93a6c6217be078392925535e084048bf04241e57a711f0f58e, 0a77e537c64336f97a04020e59d17d09d459d1626a075878e2b796d1e1033038, d36afcfe1ae2c3e6669878e6f9310a04fb6c8af525d17c4ffa8b510459d7dd4d

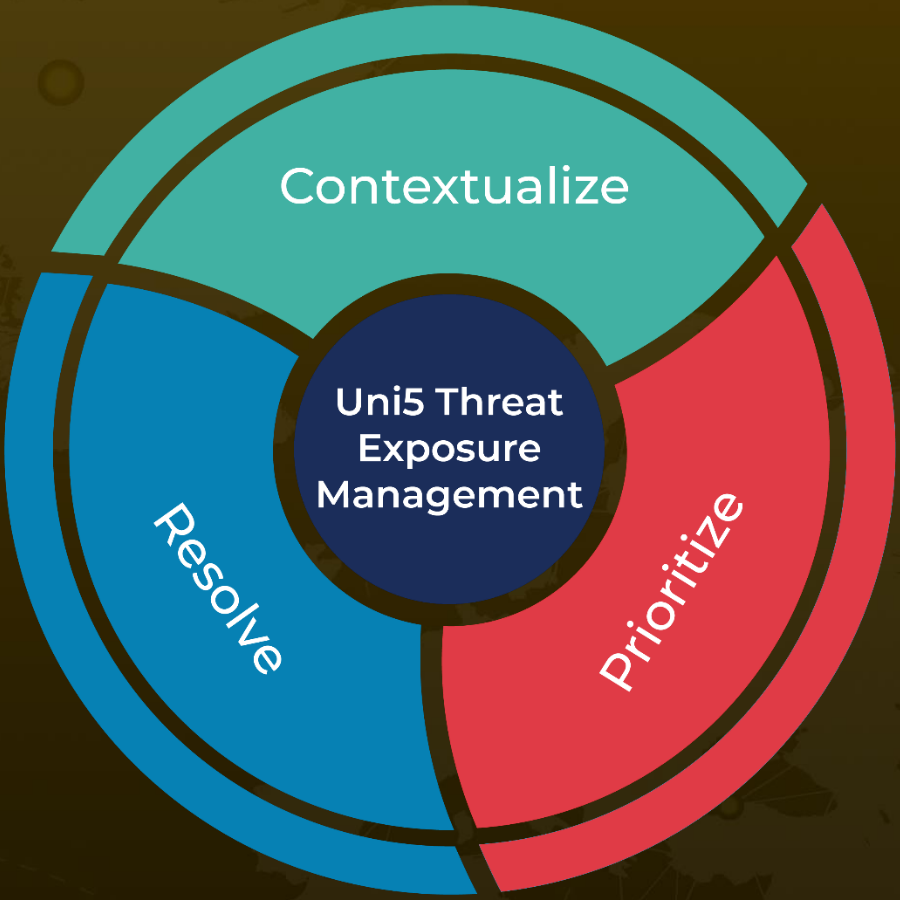
References

https://www.trellix.com/blogs/research/ransomhouse-am-see/

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

February 21, 2024 • 8:30 PM

© 2024 All Rights are Reserved by Hive Pro®

More at www.hivepro.com