Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

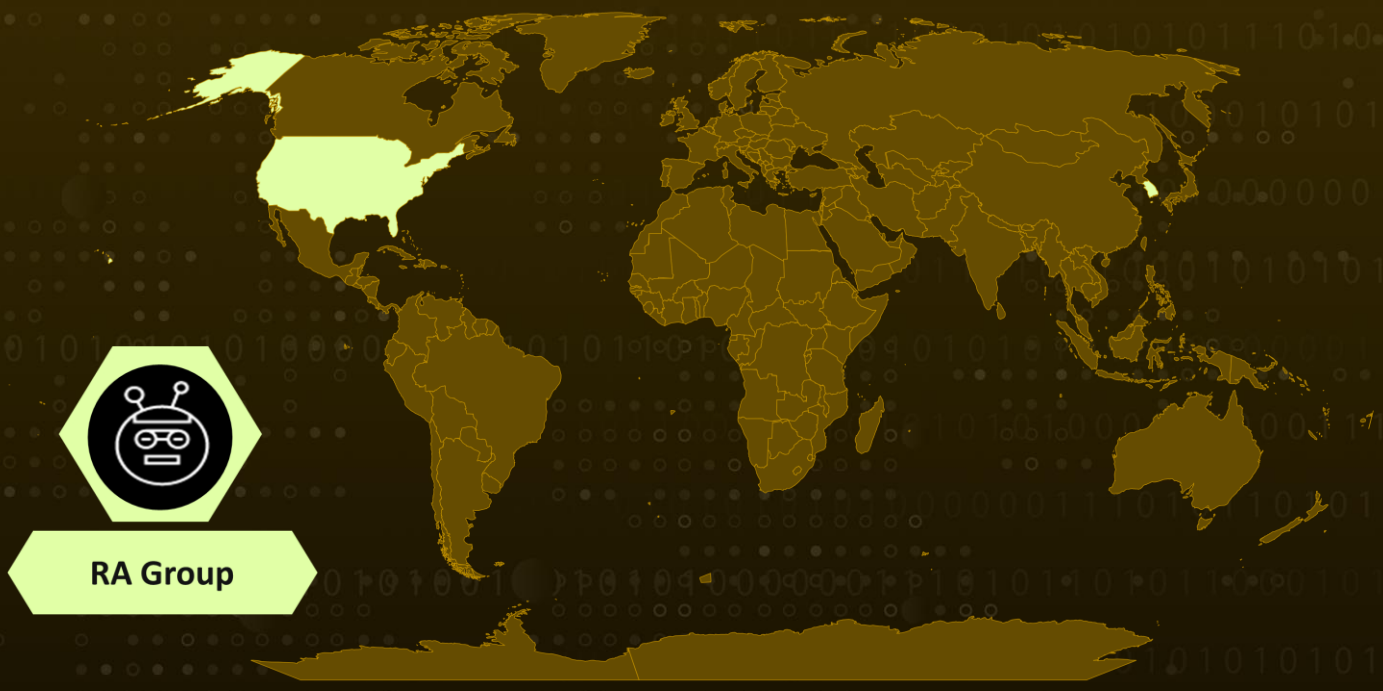
RA Group's Custom Ransomware Hits US & South Korea

Date of Publication	Admiralty Code	TA Number
May 16, 2023	A1	TA2023230

Summary

Attack Began: April 22, 2023
Actor: RA Group
Malware: Babuk Ransomware
Attack Region: United States and South Korea
Targeted Sector: Manufacturing, Wealth Management, Insurance Providers, and Pharmaceuticals.
Attack: The emergence of the RA ransomware group highlights the utilization of the recently leaked Babuk ransomware source code as they employ it to develop their variant of the malware.

Attack Regions



Attack Details

#1

In April 2023, a new ransomware group called RA Group surfaced and appears to be utilizing the leaked Babuk source code for their attacks. This code was allegedly leaked by a member of the Babuk group back in September 2021. Since then, multiple ransomware families, such as Rook, Night Sky, Pandora, Nokoyawa, Cheerscrypt, AstraLocker2, ESXIArgs, Rorschach, and RTM Locker, have emerged, all leveraging the leaked Babuk code.

#2

The operations of the RA group are rapidly expanding. So far, they have successfully targeted three organizations in the U.S. and one in South Korea, spanning multiple business sectors. The group employs double extortion tactics, increasing the likelihood of victims paying the demanded ransom.

#3

Additionally, the RA Group operates a data leak website, where they threaten to release exfiltrated data from victims who fail to comply with their specified time frame or meet their ransom requirements. One notable feature of the RA Group is its approach to customizing each attack. They use a unique ransom note titled "How To Restore Your Files.txt," tailored specifically for the targeted organization. Additionally, the executable file is named after the victim.

#4

The ransomware targets all logical drives on the victim's machine and network shares, attempting to encrypt specific folders while excluding those associated with the Windows system, boot, Program Files, and others. Encrypted files have the ".GAGUP" extension appended to their filenames, while all volume shadow copies and Recycle Bin contents are wiped to impede easy data restoration.

Recommendations

Continuously Monitor Networks for Malicious Activity: Implement robust network monitoring tools and practices to detect any signs of suspicious or malicious activity. Stay updated with the latest indicators of compromise (IOCs) by regularly updating security tools and threat intelligence feeds.

Ensure Regular Data Backups and Validate Recovery Procedures: Organizations should prioritize regular data backups to secure offline or cloud-based storage. This practice helps safeguard critical data and provides protection against data loss in the event of a successful ransomware attack. Additionally, it is crucial to regularly test and validate the organization's backup and recovery procedures to ensure they are effective. This includes performing restoration tests to verify the process and evaluate its efficiency.

Potential MITRE ATT&CK TTPs

TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0040 Impact	T1083 File and Directory Discovery	T1490 Inhibit System Recovery	T1496 Resource Hijacking
T1552 Unsecured Credentials	T1560 Archive Collected Data	T1573 Encrypted Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxp[://]hkpomcx622gnqp2qhenv4ceyrhwvld3zwogr4mnkdeudq2txf55keoad[.]onion
SHA256	3ab167a82c817cbcc4707a18fcb86610090b8a76fe184ee1e8073db152ecd45e

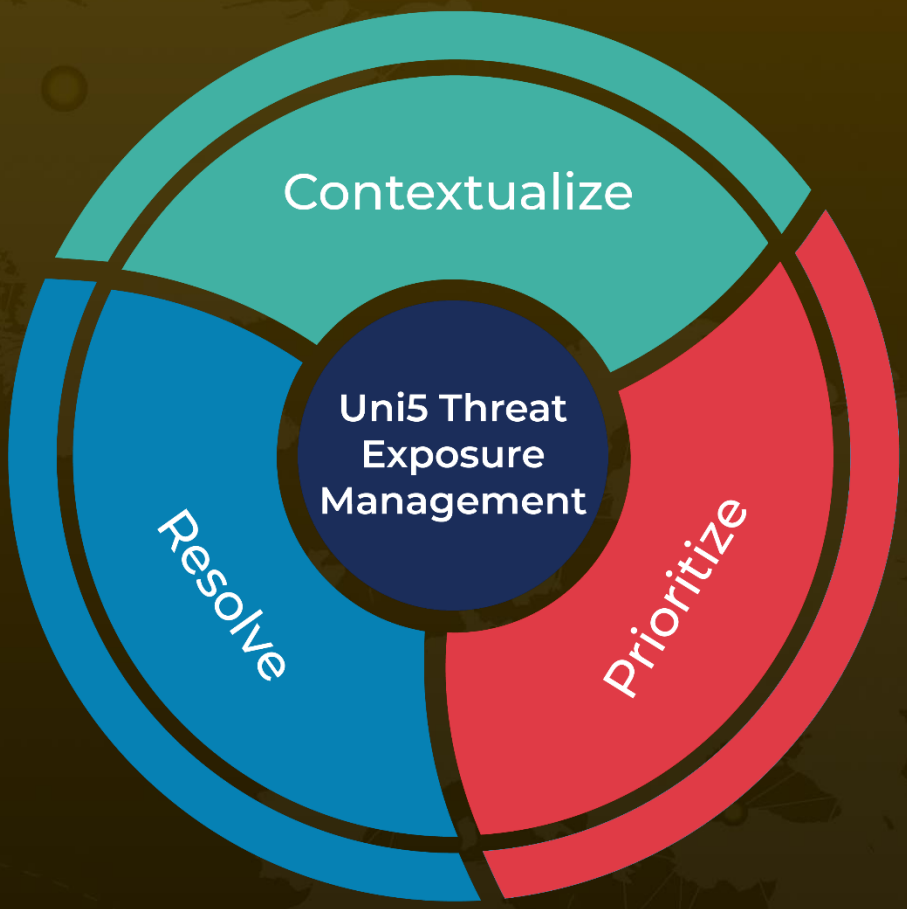
References

https://blog.talosintelligence.com/ra-group-ransomware/
https://github.com/Cisco-Talos/IOCs/blob/main/2023/05/ra-group-ransomware.txt
https://www.hivepro.com/rook-new-ransomware-in-the-market-scavenges-code-from-babuk/
https://www.hivepro.com/pandora-ransomware-targets-multiple-plants-around-the-globe/
https://www.hivepro.com/cybercrime-group-exploits-zero-day-on-windows-servers-to-deploy-nokoyawa-ransomware/
https://www.hivepro.com/the-esxiargs-ransomware-attack-is-targeting-vmware-esxi-servers-globally/
https://www.hivepro.com/a-new-rorschach-ransomware-threat-employing-hybrid-cryptography/

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

May 16, 2023 • 5:39 AM

More at www.hivepro.com