Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

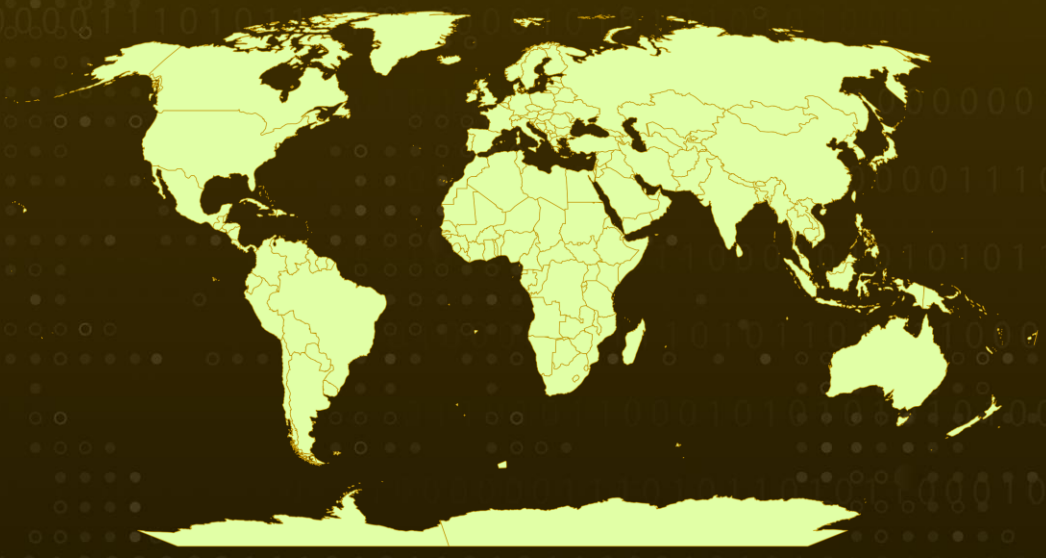
Trigona Ransomware Targets Improperly Managed MS-SQL Servers

Date of Publication	Admiralty Code	TA Number
April 13, 2023	A1	TA2023184

Summary

Attack Began: October 2022
Attack Region: Worldwide
Malware: Trigona ransomware
Attack: Trigona ransomware is installed on vulnerable MS-SQL servers that are not properly managed, allowing attackers to execute malicious commands and encrypt files without distinguishing file extensions.

Attack Regions



Attack Details

#1 The Trigona ransomware is being installed on MS-SQL servers that are not being properly managed. "Improperly managed" means that the servers are exposed to the internet and are vulnerable to brute force or dictionary attacks. Once the attacker gains control of the system, they can install malicious code or execute harmful commands.

#2 The attacks are aimed at MS-SQL servers that are not being properly managed. Reports are generated on the number of attacks and the malicious codes used in these attacks. Before installing the Trigona ransomware, the attacker uses CLR Shell malware to exploit vulnerabilities that allow them to perform malicious actions with high privileges.

#3 The Trigona ransomware is a new type of ransomware that does not distinguish between file extensions when encrypting files. The encrypted files are given the "._locked" extension and a ransom note is created, which instructs the user to download the Tor browser and contact a specific address for data recovery.

Recommendations

Ensure that all MS-SQL servers are properly managed and are not exposed to the internet. This can be done by implementing firewalls and using virtual private networks (VPNs) to protect the servers from external attacks. Additionally, strong passwords, two-factor authentication, and regular software updates can help to reduce the likelihood of brute force or dictionary attacks.

In case of a ransomware attack, having a recent backup of data is crucial. Regularly backup all critical data on MS-SQL servers and store the backups in a secure location. This can help to mitigate the damage caused by ransomware attacks.

Employees can inadvertently contribute to the vulnerability of MS-SQL servers by engaging in risky behaviors such as clicking on suspicious links or downloading malicious files. Educate employees on the importance of cybersecurity, how to identify and report suspicious activity, and how to use MS-SQL servers securely. This can help to prevent attacks and mitigate their impact.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0040 Impact
T1560 Archive Collected Data	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	T1496 Resource Hijacking
T1068 Exploitation for Privilege Escalation	T1098 Account Manipulation	T1078 Valid Accounts	T1033 System Owner/User Discovery
T1112 Modify Registry			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	1cece45e368656d322b68467ad1b8c02 530967fb3b7d9427552e4ac181a37b9a 1e71a0bb69803a2ca902397e08269302 46b639d59fea86c21e5c4b05b3e29617 5db23a2c723cbceabec8d5e545302dc4
Website	hxxp://3x55o3u2b7cjs54eifja5m3ottxntlubhjzt6k6htp5nrocjmsxxh7ad[.]onion/

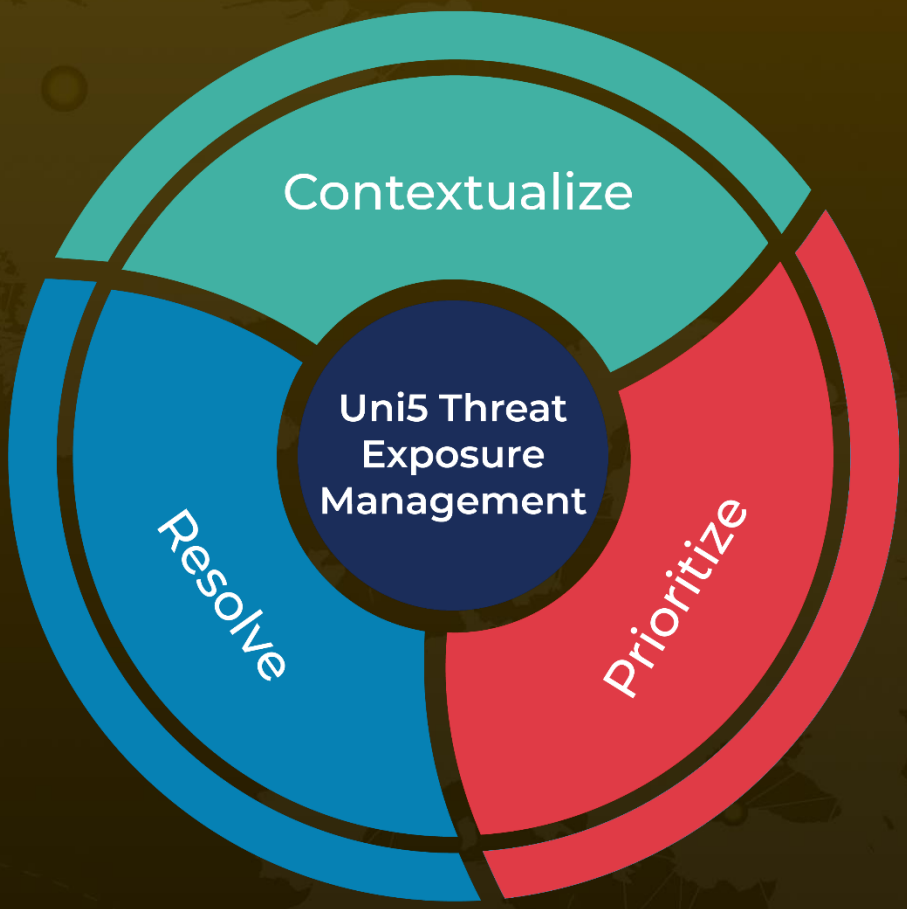
References

https://asec.ahnlab.com/ko/51168/

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

April 13, 2023 • 6:00 AM

More at www.hivepro.com