U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0308

TRIGONA RANSOMWARE TARGETS MS SQL SERVERS

DATE ISSUED: 24th April 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

Trigona is a new strain of ransomware targeting poorly configured and public-facing Microsoft SQL (MS-SQL) servers. It disables system recovery and deletes Shadow copies, hindering recovery without the decryption key or proper backups.

BREAKDOWN

Security researchers from AhnLab discovered that Trigona ransomware targets the MS-SQL servers via brute-force or dictionary attacks to guess weak and default account credentials. It leverages existing vulnerabilities in the Windows Secondary Logon Service to escalate privileges to LocalSystem in the compromised server. The threat actors then deploy CLR Shell malware to receives commands to perform malicious activities. In the next stage, a dropper malware 'svcservice.exe' service is installed to launch the Trigona ransomware as 'svchost.exe'. The ransomware binary is configured to automatically launch on each system restart via a Windows autorun key to ensure the systems will be encrypted even after a reboot. The threat actors also launched a new tor negotiation site that accepts Monero as ransom payments and will threaten to release encrypted sensitive files on dark web leak sites if payment is unfulfilled. Finally, the ransomware renames encrypted files by adding the ._locked extension and embedding the encrypted decryption key. Trigona's ransom notes, named "how_to_decrypt.hta", are presented with computer IDs (CID) and victim IDs (VID) created in each folder with information about the attack.

REMEDIATION STEPS

- Ensure your organisation has an up-to-date Next Generation Firewall (NGFW) and Endpoint Protection to prevent unauthorised system access.
- Always reset default password and use a long and complex password for a web application or public server to mitigate brute-force attacks and enable multi-factor authentication (MFA) for any publicly-exposed service. Restrict who has access to these credentials using the Need-to-know security principle.
- Network monitoring and analysis should be conducted regularly to detect and investigate anomalous behaviour.
- Perform regular system backups and store them offline or out-of-band to mitigate ransomware attacks. Test your backups to ensure they are functioning as expected and restoration is possible.
- Check out our Ransomware Defence Strategy Guide for more tips on how to secure your environment.

REFERENCES & RESOURCES

The Bleeping Computer	https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/
Zscaler	https://www.zscaler.com/blogs/security-research/technical-analysis-trigona-ransomware
Palo Alto Unit 42	https://unit42.paloaltonetworks.com/trigona-ransomware-update/