# THREAT ADVISORY

June 2, 2023

## Trigona Ransomware targeting MS-SQL Servers

**SUMMARY**
Internet exposed Microsoft SQL (MS-SQL) servers are being targeted by threat actors using brute-force or dictionary attacks to deploy Trigona ransomware.

**TECHNICAL DETAILS**
AhnLab Security Emergency Response Center (ASEC) discovered that the Trigona ransomware is being deployed on internet exposed MS-SQL servers that are not managed well, with simple or default account credentials, which make them vulnerable to brute force or dictionary attacks. After threat actors log in, they install malware or execute malicious commands, including the CLR extended procedure feature to add and use malicious functions on the server. Subsequently, the Trigona ransomware is installed.

The Trigona ransomware is installed under the name svcservice.exe. It creates and executes the actual Trigona ransomware, svchost.exe, in the same path. It also creates and executes svchost.bat which is the batch file responsible for executing the ransomware. The svchost.bat file first creates the Trigona binary to the registry's Run key to ensure that it can run even after a reboot. It then deletes volume shadow copies and disables the system recovery feature.

Trigona encrypts files indiscriminately and modified them with a "._locked" extension and then generates the ransom a note in each folder with the filename "how_to_decrypt.hta". The note includes instructions for the victim to install a Tor browser and contact a specified address to initiate the recovery process.

Admins must use MS-SQL passwords that cannot be easily guessed and change them periodically to protect the database servers from brute force and dictionary attacks. Database servers accessible from Internet should also restrict access to these systems via Firewall or other rule, proxy, or authentication methods. Updating to the latest MS-SWL version of V3 can prevent malware infection. Failure to take these measures in advance can result in continuous infections by threat actors and malware.

**INDICATORS OF COMPROMISE (IoCs)**
*Hashes:*

- 1cece45e368656d322b68467ad1b8c02
- 530967fb3b7d9427552e4ac181a37b9a
- 1e71a0bb69803a2ca902397e08269302
- 5db23a2c723cbceabec8d5e545302dc4
- 46b639d59fea86c21e5c4b05b3e29617

**BEHAVIORS**

- Disabled system recovery feature
- Deleting shadow copies
- Updated Registry Run key to include "svchost.bat"

**RECOMMENDATIONS**

- Regularly monitor and analyze system logs to detect any unusual or suspicious activities on the server.
- Apply security patches and updates as soon as they become available to address any known vulnerabilities in the system.
- Ensure MS-SQL servers are restricted to the extent possible and require strong and complex passwords for all accounts.
- Implement access controls and user permissions to limit the privileges of user accounts and prevent unauthorized access to sensitive data.

- Regularly back up important data and store the backup copies in secure, offsite locations.

**REFERENCES**

- https://asec.ahnlab.com/en/51343/