Hackers target Microsoft SQL servers in Mimic ransomware attacks

Date: 10th January 2024 | Severity: Medium

Summary

A group of financially motivated Turkish hackers targets Microsoft SQL (MSSQL) servers worldwide to encrypt the victims' files with Mimic (N3ww4v3) ransomware.

These ongoing attacks are tracked as RE#TURGENCE and have been directed at targets in the European Union, the United States, and Latin America.

Initial access to the servers entails conducting brute-force attacks, followed by the use of xp_cmdshell configuration option to run shell commands on the compromised host. This activity mirrors that of a prior campaign dubbed DB#JAMMER that came to light in September 2023.

This stage paves the way for the retrieval of a PowerShell script from a remote server that's responsible for fetching an obfuscated Cobalt Strike beacon payload.

The post-exploitation toolkit is then used to download the AnyDesk remote desktop application from a mounted network share for accessing the machine and downloading additional tools such as Mimikatz to harvest credentials and Advanced Port Scanner to carry out reconnaissance.

Always refrain from exposing critical servers directly to the internet," the researchers cautioned. "With the case of RE#TURGENCE attackers were directly able to brute force their way into the server from outside the main network.".

Attack Vectors

- OS Credential Dumping
- Network Service Scanning
- Account Manipulation.
- Brute Force
- Modify Registry.
- Create Account.
- Remote Access Software'

- Data Encrypted for Impact
- Exfiltration Over Web Service
- Boot or Logon Autostart Execution.
- Command and Scripting Interpreter.

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	9F3AD476EDA128752A690BD26D7F9A67A8A4855A187619E74422CC08121AD3D3 A222BA1FD77A7915A61C8C7A0241222B4AD48DD1C243F3548CAEF23FE985E9C2 1ED02979B3F312C4B2FD1B9CFDFB6BEDE03CD964BB52B3DE017128FE00E10D3C F328C143C24AFB2420964740789F409D2792413A5769A33741ED956FCE5ADD3E 1C7B82B084DA8B57FFEEF7BDCA955C2AA4A209A96EC70E8D13E67283C10C12A5 31FEFF32D23728B39ED813C1E7DC5FE6A87DCD4D10AA995446A8C5EB5DA58615 D0C1662CE239E4D288048C0E3324EC52962F6DDDA77DA0CB7AF9C1D9C2F1E2EB
IP address	• 45.148.121.87 • 88.214.26.3
Domain	• seruvadessigen.3utilities.com

Recommendation

Submit the File Hash to the Antivirus team to update their database with the file hashes.

Submit the IP & Domain to network team block the Ip in all perimeter firewall.

Make regular backups of important and critical files.

Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.

Update and Patch operating system, applications, and security software's up to date with latest patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

https://www.bleepingcomputer.com/news/security/hackers-target-microsoft-sql-servers-in-mimic-ransomware-attacks/

https://thehackernews.com/2024/01/turkish-hackers-exploiting-poorly.html