RA World Ransomware

Date: 26th April 2024 | Severity: Medium

Summary

RA World Ransomware Attack Windows Using Hacked Domain Control & Anti-AV Tactics.

Attack Vectors

- Threat actors use hacked domain control to host malicious content by leveraging legitimate domains to evade detection by security measures. Anti-AV tactics are employed to bypass the antivirus software and tools that enable the execution of malicious code without detection.
- Together, all these tactics enhance the stealth and effectiveness of cyber-attacks, allowing threat actors to compromise systems and steal sensitive information more easily.
- Recently, cybersecurity researchers at Trend Micro discovered that RA World (previously the RA Group) ransomware has been attacking Windows using hacked domains and Anti-AV tactics.
- The RA World ransomware, once known as the RA Group, broke into global organizations in April 2023. Researchers identified that this ransomware group mainly targeted US firms, but besides the US firms, it also struck in-Germany, India, Taiwan. This ransomware group mainly targets healthcare, insurance, and financial businesses.
- RA World operators' breach through compromised domain controllers allowed the components in SYSVOL to be dropped for GPO. The deployment of Stage1.exe via PowerShell indicated altered Group Policy settings enabling script execution. The malware may have infiltrated Group Policy, allowing it to run on multiple machines within the domain.
- Here, Stage1.exe scans for the domain controllers by halting if conditions are met, like the matching host names. It also checks for Finish.exe and Exclude.exe in %WINDIR%\Help, which indicates the past compromise or exclusion. Ransomware checks for Stage2.exe in %WINDIR%\Help. If absent, then it copies pay.txt and Stage2.exe from a hardcoded SYSVOL Path which indicates a targeted attack with a company domain name.
- This strategy involves initial payload presence on one machine, then execution on others via Group Policies which helps in revealing a multi-stage approach to compromise the network targeted.

  T1543.003 – The program checks for safe mode, then creates MSOfficeRunOncelsls service with Stage2. exe, configuring it for Safe Mode with Networking.

T1562.009 – It configures BCD for Safe Mode, starts the machine. If already in Safe Mode, Stage2.exe decrypts pay.txt to Stage3.exe, the ransomware payload.

T1070.004 – After execution, cleanup deletes remnants and creates registry keys.

T1485 – RA World deploys SD.bat to wipe the Trend Micro folder by using WMIC for disk info and leaving a log.

Besides this, T1070 – After deletion, the ransomware removes Safe Mode with the Networking option.

T1529 – It forcibly reboots the computer.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 4866d6994c2f8b4dadfaabc2e2b81bd86c12f68fdf0da13d41d7b0e30bea0801 • 51da3acc6c7089bd0f1df9d9902e183db0d1342552404c3c1b898b168399b0bc • 31ac190b45cc32c04c2415761c7f152153e16750516df0ce0761ca28300dd6a4 • 9479a5dc61284ccc3f063ebb38da9f63400d8b25d8bca8d04b1832f02fac24de

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the IPs to Network team to block in the firewall.
- Block the Domain in the Proxy.
- 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.
- Limit administrative rights to employees.
- Keep security products updated.
- Back up essential data routinely.
- Exercise caution with emails, attachments, URLs, and program execution.
- Encourage users to report suspicious emails and files promptly.

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.trendmicro.com/en_us/research/24/c/multistage-ra-world-ransomware.html
- https://www.fortinet.com/blog/threat-research/ransomware-roundup-ra-world
- https://gbhackers.com/ra-world-ransomware/