Kasseika Ransomware Deploys BYOVD Attacks, Abuses PsExec and Exploits Martini Driver

Date: 17th April 2024 | Severity: High

Summary

- A newly discovered ransomware operation dubbed “Kasseika” has been seen deploying Bring Your Own Vulnerable Driver (BYOVD) attacks to encrypt files after disabling antivirus software. The ransomware exploits the Martini driver, part of TG Soft’s VirtIT Agent System, to disable the security solutions protecting the targeted machine.
- Security analysts first discovered Kasseika in December 2023 and found that the ransomware strain has many similar features to BlackMatter, like attack chains and source code. BlackMatter’s source code was never leaked in public after it shut down in 2021. Still, it seems likely that Kasseika was developed by the former members of the threat group or sophisticated ransomware actors who bought its code.

Attack Vectors

- The attack chain initializes with a phishing email that is targeted at employees of an organization in an attempt to steal their account credentials, later to be used for initial access to the corporate network.
- Once the initial access is obtained, the ransomware operators exploit the Windows PsExec tool to execute malicious .bat files on the compromised and other systems that they have accessed through lateral movement.
- The batch file is responsible for checking if a “Martini.exe” process is present to terminate it to avoid getting interfered with. Finally, it downloads the vulnerable “Martini.sys” driver onto the machine.
- This driver is important for the execution of Kasseika as it will not proceed further if the Martini service creation fails or is not found on the system.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Hashes	• e0bac7cc1e2b02dda06b8a09f07abee6 • c98a5a4bfd53c87c5aac5659f7f505c1 • 713b1c97b09d0e633ede2f62556e78b9 • 22f8fa1b42e487f6f6d6c6a62bba65267e2d292f80989031f8529558c86a9119 • ae635a4dd36a2bf7047b6a63605a9d20aae4bcc313d93068e5e0b6676a32a39f • c33acab1ddbee95302f0d54feb1c49c40dec807cec251fb6d30d056f571155e0 • e7bf904f19581c7eebbbe06f997c3b3f7c1b7739 • 82110672dbde14a73aca43e15e4c85291fe1606f • c67835ca9504049a350fdb023ec7975cccce1674 • 8a0cd4fb3542458849e20c547a684578dd7fdd4317021dacf5517f607f8ceea7

Recommendation

- Block all threat indicators at your respective controls.
- Search for Indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Maintain cyber hygiene by updating your anti-virus software and implementing a patch management lifecycle.
- Along with network and system hardening, code hardening should be implemented within the organization so that their websites and software are secure. Use testing tools to detect any vulnerabilities in the deployed codes.
- Enable two-factor authentication.
- In a ransomware attack, the adversary will often delete or encrypt backups if they have access to them. That's why it's important to keep offline (preferably off-site), encrypted backups of data and test them regularly.
- Emails from unknown senders should always be treated with caution.
- Never trust or open links and attachments received from unknown sources/senders.
- Updates for operating systems, applications, and firmware should be installed as soon as possible.
- Check the active directories, servers, workstations, and domain controllers for new or unfamiliar accounts.
- To create safe distant connections, consider installing and utilizing a virtual private network (VPN).

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/a/kasseika-ransomware-deploys-byovd-attacks-abuses-psexec-and-expl.html
- https://www.rewterz.com/rewterz-news/rewterz-threat-alert-kasseika-ransomware-disables-antiviruses-by-leveraging-byovd-attacks-active-iocs
- Kasseika ransomware uses antivirus driver to kill other antiviruses (bleepingcomputer.com)