ShrinkLocker Ransomware

Date: 27th May 2024 | Severity: High

Summary

The ShrinkLocker ransomware was first reported by Kaspersky in May 2024. The ransomware targets organizations from various sectors, including government, pharmaceuticals, and manufacturing, in countries like Mexico, Indonesia, and Jordan. ShrinkLocker abuses Windows BitLocker to encrypt corporate systems.

Attack Vectors

Once deployed, ShrinkLocker, written in VBScript, uses Windows Management Instrumentation (WMI) to identify the target's specific Windows version, its current domain, and if the name of the operating system contains "xp", "2000", "2003", or "vista."

If the target matches the ransomware's requirements, it uses Windows' diskpart utility to shrink the size of each non-boot partition by 100 MB and splits the unallocated space into new primary partitions of 100 MB.

Then, ShrinkLocker uses the bcdboot utility to reinstall the boot files on the newly created partitions. In addition, it modifies registry entries to disable remote desktop connections or enable BitLocker encryption on systems without a Trusted Platform Module (TPM).

The Shrinklocker script also disables the standard protection devices for backing up the BitLocker key, thus preventing the victim of the attack from recovering the key. It then generates a random password and transmits it to the attacker. The VB script leaves the attackers' e-mail address in the name of newly created boot partitions so the victim can contact the hackers for a possible ransom payment. It also covers its tracks by removing created tasks and deleting system logs.

MITRE ATT&CK® TTPs:
T1059.005 - Command and Scripting Interpreter: Visual Basic
T1047 - Windows Management Instrumentation
T1059.001 - Command and Scripting Interpreter: PowerShell
T1486 - Data Encrypted for Impact
T1529 - System Shutdown/Reboot
T1070.001 - Clear Windows Event Logs
T1112 - Modify Registry
T1562.004 - Disable or Modify System Firewall
T1041 - Exfiltration Over Web Service

Indicator of compromise

INDICATOR TYPE	INDICATORS
Emails	• conspiracyid9@protonmail.com • onboardingbinder@proton.me
URLs	• https[:]//earthquake-js-westminster-searched.trycloudflare.com:443/updatelog • https[:]//generated-eating-meals-top.trycloudflare.com/updatelog • https[:]//scottish-agreement-laundry-further.trycloudflare.com/updatelog • https[:]//generated-eating-meals-top.trycloudflare.com/updatelogead
File Hashes	• 842f7b1c425c5cf41aed9df63888e768

Recommendation

- Use robust, properly configured endpoint protection to detect threats that try to abuse BitLocker;
- Implement Managed Detection and Response (MDR) to proactively scan for threats;
- If BitLocker is enabled, make sure it uses a strong password and that the recovery keys are stored in a secure location;
- Ensure that users have only minimal privileges. This prevents them from enabling encryption features or changing registry keys on their own;
- Enable network traffic logging and monitoring. Configure the logging of both GET and POST requests. In case of infection, the requests made to the attacker's domain may contain passwords or keys;
- Monitor for events associated with VBS execution and PowerShell, then save the logged scripts and commands to an external repository storing activity that may be deleted locally;
- Make backups frequently, store them offline, and test them.

Reference Links

- https://usa.kaspersky.com/about/press-releases/2024_kaspersky-uncovers-new-bitlocker-abusing-ransomware
- https://www.bleepingcomputer.com/news/security/new-shrinklocker-ransomware-uses-bitlocker-to-encrypt-your-files/
- https://securityboulevard.com/2024/05/shrinklocker-ransomware-leverages-bitlocker-for-file-encryption/