Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

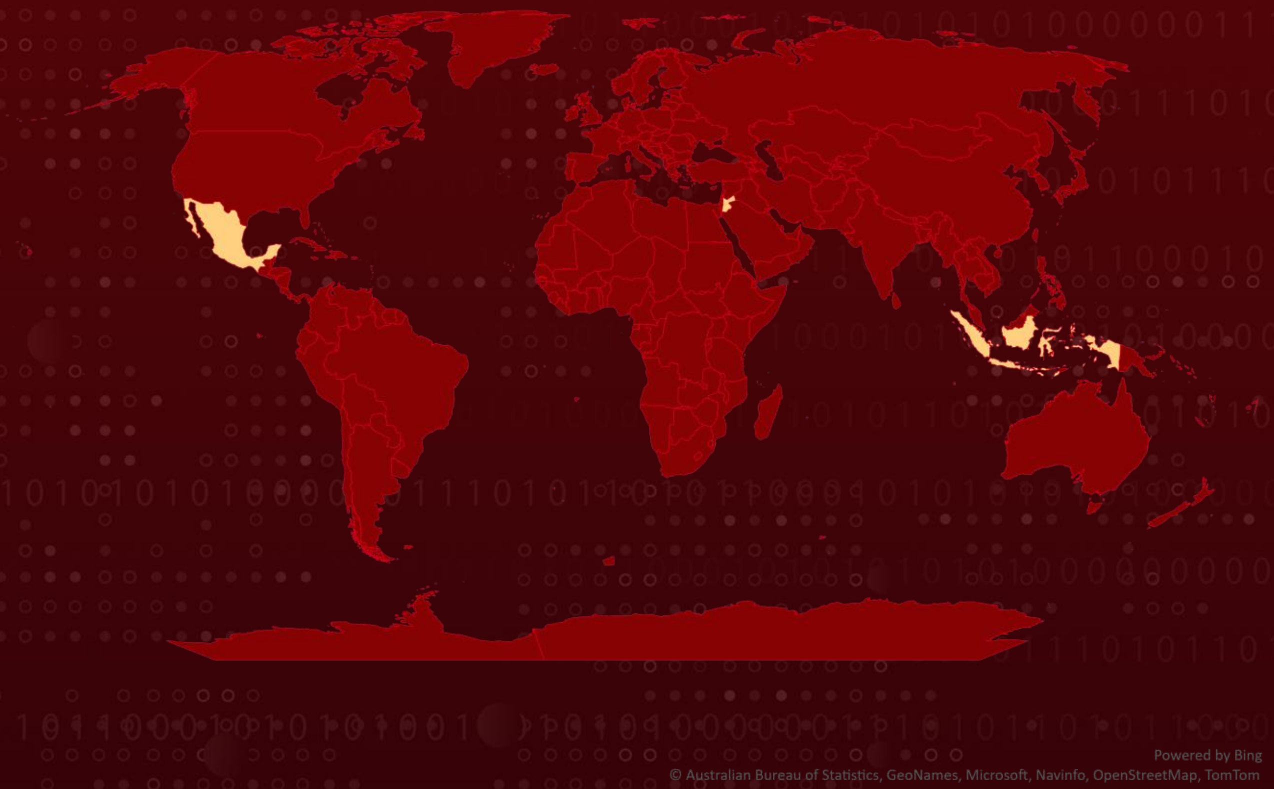
ShrinkLocker: Ransomware Exploits BitLocker for Drive Encryption

Date of Publication	Admiralty Code	TA Number
May 28, 2024	A1	TA2024209

Summary

First Appearance: May 2024
Malware: ShrinkLocker Rasnomware
Targeted Countries: Mexico, Indonesia, and Jordan
Affected Platforms: Windows
Attack: ShrinkLocker is a new ransomware strain that exploits Microsoft's BitLocker to encrypt entire drives, using a VBScript to shrink partitions and create new boot volumes. It disables Remote Desktop Protocol (RDP) and modifies registry settings to enforce encryption, making detection difficult. Instead of a ransom note, it embeds the attacker's contact email in the boot partition labels, and deletes BitLocker protectors to prevent recovery.

Attack Regions


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 ShrinkLocker is a recently discovered ransomware strain that exploits Microsoft's BitLocker feature to encrypt entire drives, rendering user data inaccessible. This technique, while not entirely new, poses significant challenges for detection and mitigation because it leverages a legitimate Windows security feature.

#2 ShrinkLocker operates using a VBScript to perform a series of sophisticated actions. It first conducts a system check using Windows Management Instrumentation (WMI) to gather OS details and ensure the system meets specific criteria before proceeding. If the target system is suitable, the script shrinks all drive partitions by 100MB and uses the stolen space to create a new boot partition. This is how it gets its name as “ShrinkLocker.” It then reinstalls boot files on these new partitions.

#3 The ransomware then uses BitLocker to encrypt the newly created partitions, making it particularly difficult for traditional defenses to detect and counteract the attack. Additionally, ShrinkLocker modifies various registry settings to disable Remote Desktop Protocol (RDP) and enforce BitLocker encryption, even on systems without a Trusted Platform Module (TPM).

#4 One distinctive aspect of ShrinkLocker is its method of demanding ransom. Instead of leaving a ransom note, it embeds the attacker’s contact email address as the label of the new boot partitions. This information is only visible through diagnostic tools or when the device is booted using a recovery environment, making it easy to overlook. Additionally, it deletes BitLocker protectors to prevent victims from recovering the encryption key, which is sent to the attacker.

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with ShrinkLocker ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Patch and Update Software: Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. ShrinkLocker affiliates often exploit known vulnerabilities to gain initial access to systems. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited and prevent unauthorized access to their networks.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, storing them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a ShrinkLocker ransomware attack, up-to-date backups enable recovery without paying the ransom. Especially BitLocker users should secure recovery keys and maintain offline backups.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0040 Impact	TA0010 Exfiltration
TA0042 Resource Development	TA0011 Command and Control	T1071 Application Layer Protocol	T1059.001 PowerShell
T1567 Exfiltration Over Web Service	T1584.001 Domains	T1584 Compromise Infrastructure	T1490 Inhibit System Recovery
T1070 Indicator Removal	T1112 Modify Registry	T1562.004 Disable or Modify System Firewall	T1562 Impair Defenses

T1027 Obfuscated Files or Information	T1486 Data Encrypted for Impact	T1529 System Shutdown/Reboot	T1070.001 Clear Windows Event Logs
T1059.005 Visual Basic	T1059 Command and Scripting Interpreter	T1047 Windows Management Instrumentation	

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps://scottish-agreement-laundry-further[.]trycloudflare[.]com/updatelog, hxxps://generated-eating-meals-top[.]trycloudflare[.]com/updatelog, hxxps://generated-eating-meals-top[.]trycloudflare[.]com/updatelogead, hxxps://earthquake-js-westminster-searched[.]trycloudflare[.]com:443/updatelog
Emails	onboardingbinder[@]proton[.]me conspiracyid9[@]protonmail[.]com
MD5	842f7b1c425c5cf41aed9df63888e768

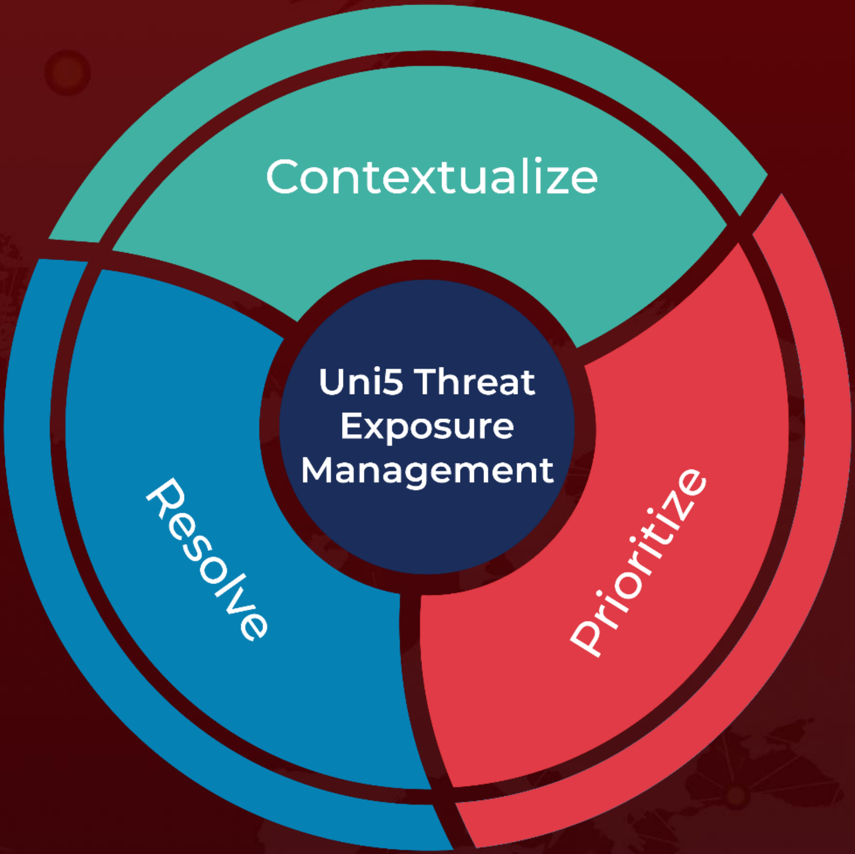
References

https://securelist.com/ransomware-abuses-bitlocker/112643/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 28, 2024 • 6:30 AM

More at www.hivepro.com