Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

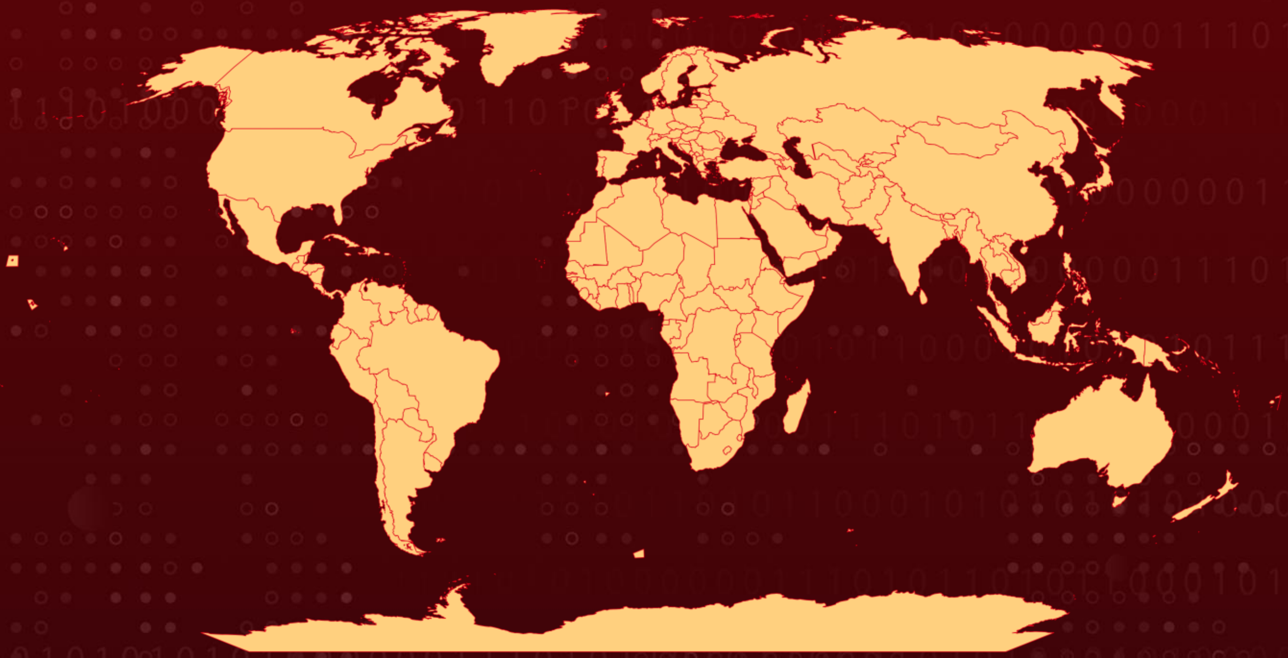
Mallox Ransomware A Resurgent Threat Exploiting MS-SQL Flaws

Date of Publication	Admiralty Code	TA Number
December 21, 2023	A1	TA2023515

Summary

Attack Began: December 2023
Attack Region: Worldwide
Malware: Mallox Ransomware (aka TargetCompany, Fargo, and Tohnichi)
Attack: Mallox is a resilient Ransomware-as-a-Service (RaaS) threat, utilizing tactics like exploiting MS-SQL vulnerabilities and employing brute force attacks. Operating with a prolonged presence, Mallox's recent variant, "Mallox.Resurrection," exhibits consistent functionalities, emphasizing the importance of cybersecurity basics for defense.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2019-1068	Microsoft SQL Server Remote Code Execution Vulnerability	Microsoft SQL Server	✗	✗	✓
CVE-2020-0618	Microsoft SQL Server Remote Code Execution Vulnerability	Microsoft SQL Server	✗	✗	✓

Attack Details

#1

Mallox is a persistent and evolving ransomware threat operating under a Ransomware-as-a-Service (RaaS) model, is first appeared in February 2021. The group utilizes underground forums like Nulled and RAMP to recruit affiliates and advertise its services. Known for its longevity, Mallox focuses on exploiting vulnerabilities, particularly in MS-SQL (Microsoft SQL Server) and ODBC (Open Database Connectivity) interfaces, with a specific emphasis on unpatched instances.

#2

The group gains initial access through methods like brute force attacks and phishing emails, leveraging tools such as Cobalt Strike and Sliver. After infiltrating a system, Mallox executes PowerShell commands to run batch scripts and download its ransomware payload. Recent variants, designated "Mallox.Resurrection," exhibit a consistent set of core functionalities, excluding certain file types and processes from encryption.

#3

The ransomware alters Boot Configuration Data (BCD) settings to impede system recovery. Encrypted files receive the ".mallox" extension, and victims are provided with ransom notes guiding them on obtaining a decryption tool through TOR. Despite facing challenges, including the release of a public decryptor for earlier versions, Mallox remains a persistent threat. Its continued reliance on exploiting unpatched MS-SQL interfaces underscores the importance of cybersecurity basics.

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 Mallox ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Patch and Update Software: Ensure all software, especially critical applications and services like MS-SQL, is up to date with the latest security patches. Mallox 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: Implement a robust data backup strategy that includes regular backups of critical data and systems. Ensure backups are stored offline or in a secure, isolated environment to prevent them from being compromised in the event of an attack. Regularly test the restoration process to verify the integrity and availability of backups.

Strong Access Controls and Authentication: Implement robust access controls and use strong, unique passwords for all accounts, especially those associated with MS-SQL interfaces. Consider multi-factor authentication to add an extra layer of security.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0040 Impact	**TA0042** Resource Development	**T1047** Windows Management Instrumentation	**T1027** Obfuscated Files or Information
T1190 Exploit Public-Facing Application	**T1588.005** Exploits	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities
T1110 Brute Force	**T1059.001** PowerShell	**T1059** Command and Scripting Interpreter	**T1489** Service Stop

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	104[.]21.76.77, 104[.]237.62.211, 172[.]67.191.103, 64[.]185.227.155, 80[.]66.75.37

TYPE	VALUE
SHA1	3d434b7cc9589c43d986bf0e1cadb956391b5f9a, 9295a02c49aa50475aa7876ca80b3081a361ff7d, 3fa79012dfdac626a19017ed6974316df13bc6ff , 7e7957d7e7fd7c27b9fb903a0828b09cbb44c196 , 08a236455490d5246a880821ba33108c4ef00047, 0d2711c5f8eb84bd9915a4191999afd46abca67a, 0e45e8a5b25c756f743445f0317c6352d3c8040a, 11d7779e77531eb27831e65c32798405746ccea1, 246e7f798c3bfba81639384a58fa94174a08be80, 273e40d0925af9ad6ca6d1c6a9d8e669a3bdc376, 2a6f632ab771e7da8c551111e2df786979fd895d, 2c49fa21b0a8415994412fe30e023907f8a7b46e, 33c24486f41c3948fbd761e6f55210807af59a1f, 4c863df8ea7446cb7fba6e582959bc3097f92b5c, 4fcfb65cb757c83ed91bc01b3f663072a52da54b, 5229a5d56836c3d3fc7fb12a43a431b5c90f771d, 552862af77b204ac1f69b9e25937cc60e30e6c0f, 5d0b9521cca0c911d49162e7f416a1463fbaefae, 5d9cc0bc652b1d21858d2e4ddd35303cd9aeb2a3, 63408c84c5d642cf1c5b643a97b84e22e18323c0, 643918830b87691422d6d7bd669c408679411303, 65d7cb5f1770b77b047baf376bd6b4cf86c5d42c, 88eef50d85157f2e0552aab07cac7e7ec21680f5, 88f8629423efe84e2935eb71d292e194be951a16, 9d182e17f88e26cb0928e8d07d6544c2d17e99f5, a8886c9417b648944d2afd6b6c4941588d670e3c, db3fd39fc826e87fa70840e86d5c12eef0fe0566, ee15c76e07051c10059a14e03d18a6358966e290, fb05a6fafc28194d011a909d946b3efa64cdb4cf
TOR Address	http[:]//wtyafjyhwqrgo4a45wdvvwhen3cx4euie73qvlhkhvlrexljoyuklaad[.]onion/
SHA 256	60784ab7fec3f23066a996f3347b721a09eb677b63dbc5e1bb2bfc920fa3f13d, 9b24ee3dd5f50e65ea15aaa3946e76281c4f9d519524dc659f2bcdfb62241316, 142f2b232fa96e71379894d1bb6cb242c0f33886c1802922163901e70fdc3320, 0901a9920c9f0c74fb2170524477693d62c8493715520ae95143abd8055e7a39, 634043ca72cd2b6a4d7a1cfe2aa12b7cd8c8348055fbc38c7d8006602ac66b87, b7a5068f9d696d6767bfddaea222649ff3541af306f93bce23c0aa6edd892534, 64e560f40df031149c745ecaf44ce379aa44373d80a0ee3c4bd0abf7955df88e,

TYPE	VALUE
SHA 256	b8bd3cc96bfea60525d611e38b4de30c59d82d1df54a873fc9998533945063ff, 601a2f402efcf27db4f9343a60e411959f92cdbb7802bbf4030df7b671c559e3, fa450286a4aa25579c8da7684051e7cdda3ba249ff03da71689e5138fd9f5c73

Patch Details

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1068

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618

Recent Breaches

https://adiva-tw.com
https://www.vct.co.in
https://www.duhocaau.vn
https://www.bozovich.com
https://www.garuda-indonesia.com
https://contecsystems.com
https://www.westcargo.com.br
https://www.franklins.co.nz
https://ovovovov.com

References

https://www.sentinelone.com/blog/mallox-resurrected-ransomware-attacks-exploiting-ms-sql-continue-to-burden-enterprises/

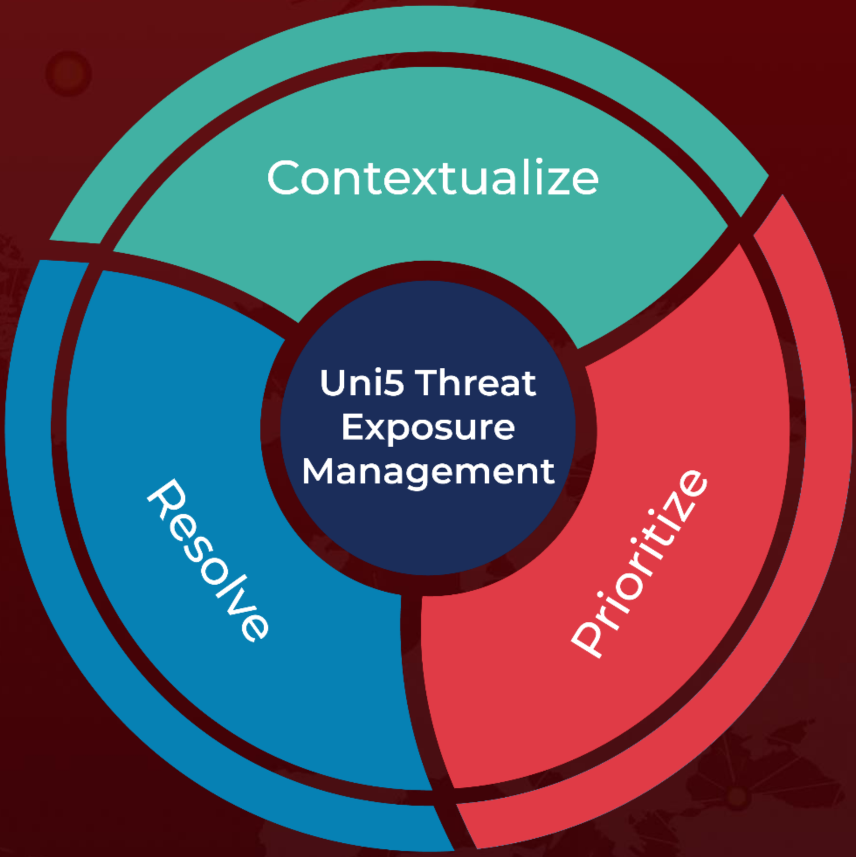
https://www.hivepro.com/threat-advisory/targetcompany-ransomwares-fud-obfuscation-maneuvers/

https://www.hivepro.com/threat-advisory/mallox-ransomware-is-ramping-up-its-operation/

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

December 21, 2023 • 7:00 AM

More at www.hivepro.com