certin
Enhancing Cyber Security in India

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

CURRENT ACTIVITIES

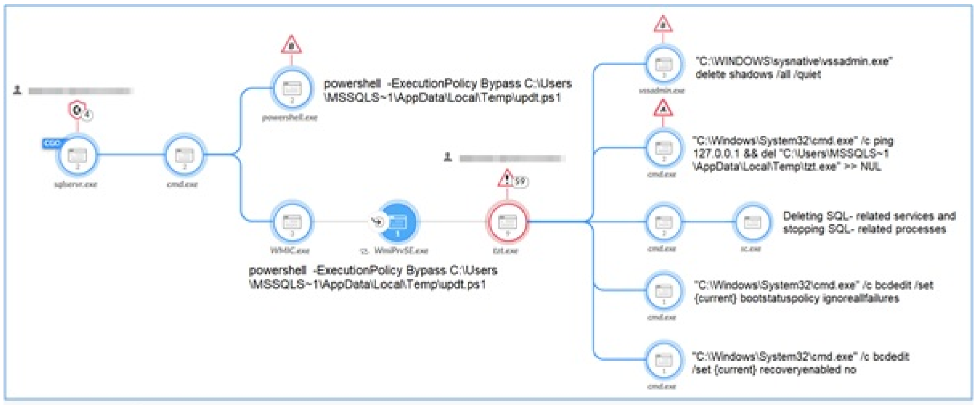
Mallox Ransomware Targeting Unsecured MS SQL Servers

Original Issue Date:July 25, 2023

It has been observed that Mallox Ransomware is currently targeting unsecured Microsoft SQL Servers, using them as entry points into victims ICT infrastructures to distribute the ransomware.It has also been observed that the threat actor group has used brute force techniques on publicly exposed MS SQL instances to gain initial access to the victims network infrastructure.

Mallox ransomware, like many other ransomware threats, follows the double extortion technique: it steals data before encrypting an organization's files and then threatens to publish the stolen data on the leak site as leverage to convince victims to pay the ransom fee.

The following figure shows the process of the Mallox Ransomware attack.



```
powershell -ExecutionPolicy Bypass C:\Users
\MSSQLS~1\AppData\Local\Temp\updt.ps1

powershell -ExecutionPolicy Bypass C:\Users
\MSSQLS~1\AppData\Local\Temp\updt.ps1

"C:\WINDOWS\sysnative\vssadmin.exe"
delete shadows /all /quiet

"C:\Windows\System32\cmd.exe" /c ping
127.0.0.1 && del "C:\Users\MSSQLS~1
\AppData\Local\Temp\tzt.exe" >> NUL

"C:\Windows\System32\cmd.exe" /c bcdedit /set
{current} bootstatuspolicy ignoreallfailures

"C:\Windows\System32\cmd.exe" /c bcdedit
/set {current} recoveryenabled no
```

Figure 1: Process of Mallox Ransomware (Source: Palo Alto)

Securing the Microsoft SQL server instances is essential to prevent Mallox Ransomware attacks. Hence, the following steps are recommended to secure Microsoft SQL Server instances.

1. **Do not expose SQL Servers on the default port (1433) over the Internet:** The default port (1433) is well known and is often targeted by hackers and malicious actors looking for vulnerable servers to exploit. Instead, consider using a VPN or other secure connection to access your SQL servers.

2. **Disable the sa account:** The sa (system administrator) account has the highest level of privileges in SQL Server. Disable this account or change its password to something very strong to reduce the risk of unauthorized access.

3. **Audit SQL CLR Assemblies:** Disable SQL CLR assemblies if not needed. Establish an auditing procedure to regularly check the existing CLR assemblies and remove any unwanted assemblies.

4. **Use a firewall:** Use a firewall to restrict access to your SQL servers. Only allow incoming traffic from trusted networks and IP addresses. Block all incoming traffic on port 1433 except for authorized users.

5. **Keep your SQL Server up to date:** Install the latest updates and patches for your SQL Server instance to keep it secure and protect against known vulnerabilities.

6. **Use strong and unique passwords:** Make sure that all SQL logins have strong and unique passwords that are difficult to guess. Use a combination of upper and lower case letters, numbers, and special characters.

7. **Use account lockout policies:** Configure account lockout policies to lock out SQL Server logins after a certain number of failed login attempts. This can help protect against brute force attacks.

8. **Use SSL/TLS to encrypt data in transit:** Use SSL/TLS to encrypt data in transit between clients and your SQL servers. This can help protect against eavesdropping and other types of attacks.

9. **Monitor your SQL Server:** Use SQL Server auditing to track and log all activity on your SQL Server instance. This can help you detect and respond to security threats in a timely manner.

Indicators of Compromises Related to Mallox Ransomware Activities:

IP Addresses

103[.]96[.]72[.]140
80[.]66[.]75[.]36
80[.]66[.]75[.]37
80[.]66[.]75[.]126
80[.]66[.]75[.]116
80[.]66[.]75[.]51
80[.]66[.]76[.]33
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
89[.]117[.]55[.]149
5[.]181[.]86[.]241
185[.]170[.]144[.]153
80[.]66[.]76[.]30
80[.]66[.]76[.]34
80[.]66[.]76[.]21
80[.]66[.]88[.]16
80[.]66[.]76[.]91
45[.]93[.]201[.]74
45[.]93[.]201[.]68
80[.]66[.]75[.]172

Hashes

```
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
9a3050007e1c46e226e7c2c27d4703f6396280386329044919a0d0ca9661b3b
d6c51935d0597b44f45f1b36d65d3b01b6401593f95cb4c2786034072ad89b63
586d4f86615cb3a8709ae1c08dde35087580814c1d1315af3d7b932639ff48e0
8e974a3be94b7748f7971f278160a74d738d5cab2c3088b1492cfbbd05e83e22
3fa36079fdc548db1b5122450c2e4c9e40c37059de116d1c03f6459b13fc2dc4
D15f12a7cf2e8ec3d6fceabfab64956c7e727caab91cff9c664f92b5c8552570
0427a9f68d2385f7d5ba9e9c8e5c7f1b6e829868ef0a8bc89b2f6dae2f2020c4
4cbac922af3cfaba5fa7a3251bd05337bffd9ed0ada77c55bb4f78a041f4ebf2
10f96f64659415e46c3f2f823bdb855aab42d0bfced811c9a3b72aea5f22d880
5ccff9af23c18998221f45396732539d18e330454327d1e7450095c682d8c552
77fdce66e7f909300e4493cbe7055254f7992ba65f9b7445a6755d0dbd9f80a5
ee08e3366c04574f25909494ef276e65e98d54f226c0f8e51922247ca3cfade9
2fd3c8fab2cfaaabf53d6c50e515dd5d1ef6eceeebdd5509c23030c4d54cb014
603846d113ef1f588d9a3a695917191791fbad441f742bcfe797813f9fc5291e
a5085e571857ec54cf9625050dfc29a195dad4d52bea9b69d3f22e33ed636525
9b833d5b4bdbc516e4773c489ced531b13028094ce610e96ebc30d3335458a97
b9e895830878124e20293f477549329d4d8752ff118f4fe893d81b3a30852c0b
cd80506f971b95b3b831cef91bb2ec422b1a27301f26d5deac8e19f163f0839a
c0e35b19f97021416e3724006511afc95d6aa409404e812d8c62b955bc917d3c
342930d44aed72f826a3f0f4a3964158f2bd86fb53703fb3daa6c937b28a53e4
 9ee35c6eb97230cd9b61ba32dba7befea4122f89b3747d2389970050a1d019f9
 e7e00e0f817fcb305f82aec2e60045fcdb1b334b2621c09133b6b81284002009
 e3f63ab8ef91e0c52384c0e3e350db2427c8cb9237355800a3443b341cf8cf4f
 f7e8a0eac54dd040e2609546fca263f2c2753802ff57e7c62d5e9ccfa04bdb1a
 e7178a4bad4407316b85894307df32fdf85b597455364eb8ec4d407749e852ce
 dcc9e23fd6ac926eb9ee7e0ee422dacd2059b4a42c8642d32bdf4f5c8eb33f6a
 fead3d518752ddb4d2407f16ca5f3c9b3c0bf01972a2618369d02913f7c6af1a
 0901a9920c9f0c74fb2170524477693d62c8493715520ae95143abd8055e7a39
 ba97fd533e8a552664695434227b24ca1e2e661c360a7a0a40ff59ba6b8fe949
 53da732df7599f5ad21a26b669500788a827f3a8358dcdca10997d2b8187c95c
 189c9c4603defb14fa8c942f5ff7814804654269917640478686530f91c4b66c
 fd0030883b9e74b383ee6381a2aaa7e2e5b93a00003b555e2f7c8b7be65ab176
 d22b3218c4b7f13fe114854d1dbda02c3ad94a1b6c69daa1cf6a504ada8b8bca
 b6447b0636085fcb41fd574e84500958f21dfe87fe06b0813fb9399d63f28851
 5c34f6fa6eada3197404bf95eced9d288688537598629158a4f4e18d6882cb9b
 d81b0425d4ec49bad194b8dc750524c2a29994fe972e733376349f47961cfa62
 1e2515efb64200258752d785863fd35df6039441a80cb615dfff4fbdffb484ec
 777a5782426e5b42e0e5e8445dd9602d123e8acc27aca4daa8e9c053f3d5b899
 9e3684be0b4c2dc93f962c03275e050fed57d9be6411396f51bdf8d4bb5e21c0
 cb47327c7cce30cff8962c48fa3b51e57e331e1592ea78b21589164c5396ccd9
```

References

https://unit42.paloaltonetworks.com/mallox-ransomware/
https://www.cyberswachhtakendra.gov.in/alerts/ransomware.html
https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2022.pdf

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email:info@cert-in.org.in
Phone: +91-11-24368572

Postal Address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India