Quorum Cyber

Threat Intelligence Mallox Ransomware

TLP Status: CLEAR

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version	Date	Summary of Changes
0.1	21/07/2023	Initial Report Drafted
1.1	04/08/2023	PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
	dd/mm/yyyy	

Mallox Ransomware

Overview

Mallox ransomware has been observed targeting various industries and countries, including Japan, India, Thailand, Canada, the UK, Portugal, Saudi Arabia, the US, Brazil, and France. The most prominent current events involving Mallox ransomware include attacks on various companies in different sectors, such as metals and mining, manufacturing, retail, food and beverage, media and entertainment, business services, education, and consulting.

The malware employs a double-extortion technique known as "name and shame" whereby stolen data is threatened to be leaked to persuade victims to pay a demanded ransom. The ransomware is associated with MITRE techniques such as T1005 (Data from Local System) and T1486 (Data Encrypted for Impact). The Mallox ransomware payload is delivered through phishing emails with encrypted and obfuscated dynamic-link library (DLL) files to prevent reverse engineering.

Impact

Successful exploitation by Mallox ransomware will almost certainly result in the encryption and exfiltration of significant quantities of data held on the compromised system, prior to a ransom of a predetermined value being issued. The ransom amount demanded will almost certainly depend on the estimated value of the compromised organisation. Furthermore, such a compromise of data will also result in the organisation incurring a negative reputational impact. Encrypted data may include private customer data, corporate finance data and system credentials that if released can assist threat actors with future attacks.

Incident Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide additional protection against ransomware threats like that implemented by Mallox ransomware. EDR solutions can alert system users of potential breaches and stop further progress before the malware can do significant damage.

Targeted Products

Windows OS.

Containment, Mitigations & Remediations

As mentioned previously, a primary method of reducing the threat of Mallox ransomware is to detect it in the early stages through the use of an effective and monitored EDR solution. An effective EDR tool such as the Microsoft Defender suite will block ransomware attempts once detected.

Organisations can also perform routine back-ups of sensitive data that is required for business operations and to keep a copy offline in case back-ups are impacted by the attack. Therefore, if a breach occurs and the business can no longer function, a back-up is ready to use, and the business can continue to operate with minimal disruption.

Indicators of Compromise

Mallox Ransomware Associated Domains:

- knpgroup[.]com
- compassinf[.]com
- cvalley[.]net
- greenfiber[.]com
- imatica[.]com
- itwfoodequipment[.]com

Mallox Ransomware Associated File Hashes (SHA-256):

- 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

Mallox Ransomware Associated IP Addresses:

- 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

Threat Group

The Mallox ransomware group became significantly active within the ransomware ecosystem in Q2 of 2023. The group has recently been recruiting affiliates for a new Ransomware-as-a-Service (RaaS) affiliate programme. They primarily target organisations in various industry sectors, including manufacturing, retail, food and beverage, and software and IT services, in countries such as India, Saudi Arabia, Portugal, and France. The group has claimed responsibility for cyber-attacks against organisations, including the Federation of Indian Chambers of Commerce & Industry (FICCI) and PT Garuda Indonesia.

Threat Landscape

Ransomware continues to be one of the prominent threats facing the private sector. Recent attacks and the developing nature of the ransomware threat landscape suggests that the threat is growing as criminal groups are becoming more comfortable demanding ever-increasing ransom fees.

Due to the significant number of targets within the first two months of its existence[1], it is likely that Mallox ransomware will continue to exploit victims at a high frequency and as such will emerge into an increasingly notorious ransomware strain.

Mitre Methodologies

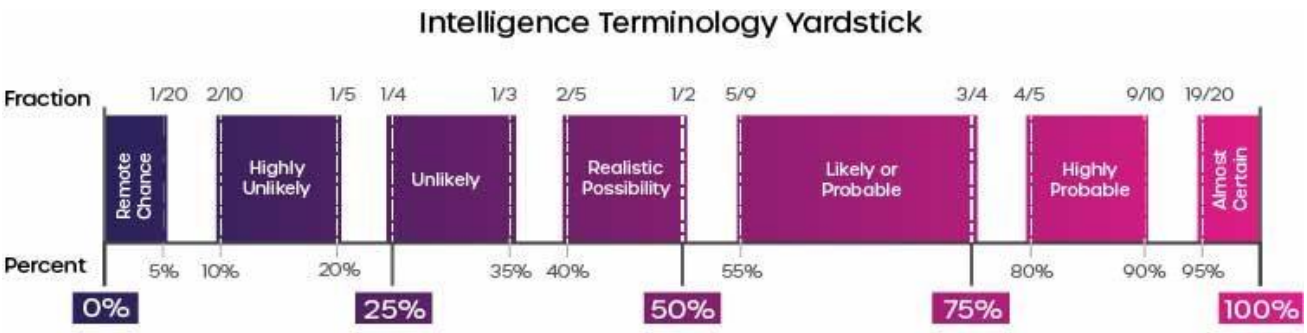
Collection

T1005 - Data from Local System[2]

Impact

T1486 - Data Encrypted for Impact[3]

Intelligence Cut-off Date (ICoD): 04/08/2023 10:00 UTC



This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events

[1] Threat Group Assessment: Mallox Ransomware (paloaltonetworks.com)
[2] Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®
[3] Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®