Quorum Cyber

Threat Intelligence Rorschach 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	05/04/2023	Initial Report Drafted
1.1	04/07/2023	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	

Rorschach Ransomware

Overview

An emerging ransomware variant, named 'Rorschach', was recently identified as being deployed against an organisation located in the USA. Upon analysis, the ransomware has many unique features, such as the use of direct syscalls, while sharing no significant attributes with alternative ransomware strains. Moreover, the ransomware is not branded, a feature uncommon among reputable ransomware groups.

A behavioural analysis of Rorschach has indicated that the ransomware conducts some of its objectives in an automated fashion when executed on a domain controller (DC), while clearing the event logs of the target machines. Such objectives include creating a domain group policy object (GPO). In other ransomware attacks, such as those involving the deployment of LockBit 2.0, threat actors achieve this distribution by manually creating group policies on the DC that are then executed by workstations on the network. Rorschach applies the same technique but creates the group policies automatically. The ransomware was initially observed as being deployed via Dynamic-Link Library (DLL) side-loading of a Cortex XDR Dump Service Tool, a loading method which is not commonly used to load ransomware.

One of the most notable traits of Rorschach ransomware is the speed at which the malware conducts encryption. Encryption speeds have been estimated to be approximately 220,000 local drive files within a time of four minutes and 30 seconds, compared to the equivalent for LockBit 3.0, with a time of seven minutes. Rorschach uses a hybrid cryptography scheme that combines the elliptic curve cryptography using curve25519 with a stream cipher called HC-128 that's part of the eSTREAM portfolio, along with more widely used ciphers such as ChaCha20 and Salsa20. These factors allow for the assessment that Rorschach is currently one of the fastest ransomware variants being deployed in the wild.

As is the case with the LockBit ransomware family, Rorschach avoids targets in certain geographic locations by reviewing the system language settings of the ransomware platform. This involves a list of a languages used in the 12 current, former, or founding Member States of the Commonwealth of Independent States (CIS). This is in relation to the implicit sanctions of the Russian authorities that exist to allow the threat activity of a group to occur, on the conditional basis that they attack foreign targets. This is a typical strategy of malware created by developers of CIS members (former Soviet Union nations) so that the associated ransomware gangs avoid facing any penalty from inside the CIS, provided they avoid attacking its organisations.

Impact

Successful exploitation by Rorschach 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.

Vulnerability Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide additional protection against malware threats such as Rorschach ransomware. EDRs can alert system users of potential breaches and prevent further progress, prior to the malware being able to implement significant damage.

Thus far Rorschach ransomware notes delivered to the victim have been formatted in a similar manner to Yanluowang ransomware notes, although other variants have sent a note that more closely resembled the DarkSide ransomware notes (causing false attribution). The content of the note has been outlined below:

==========

Hi, since you are reading this it means you have been hacked.

In addition to encrypting all your systems, deleting backups, we also downloaded your confidential information.

Here's what you shouldn't do:

1) *Contact the police, fbi or other authorities before the end of our deal.*
2) *Contact the recovery company so that they would conduct dialogues with us. (This can slow down the recovery, and generally put our communication to naught). Don't go to recovery companies, they are essentially just middlemen who will make money off you and cheat you.We are well awae of cases where recovery companies tell you that the ransom price is 5 million dollars, but in fact they secretly negotiate with us for 1 million dollars, so they earn 4 million dollars from you. If you approached us directly without intermediaries you would pay 5 times less, that is 1 million dollars.*
3) *Do not try to decrypt the files yourself, as well as do not change the file extension yourself !!! This can lead to the impossibility of their decryption.*

Here's what you should do right after reading it:

1) *If you are an ordinary employee, send our message to the CEO of the company, as well as to the IT department.*
2) *If you are a CEO, or a specialist in the IT department, or another person who has weight in the company, you should contact us within 24 hours by email.*

If you do not pay the ransom, we will attack your company again in the future.In a few weeks, we will simply repeat our attack and delete all your data from your network, WHICH WILL LEAD TO THEIR UNAVAILABILITY!

As a guarantee that we can decrypt the files, we suggest that you send several files for free decryption.

Mails to contact us(Write the decryption ID in the title of your message):

==========

Affected Products

Windows OS.

Containment, Mitigations & Remediations

It is strongly recommended that employees receive training on how to detect markers of phishing emails. A common initial ingress mechanism utilised by ransomware groups is the distribution of phishing emails, along with malicious attachments. While user awareness, through the utilisation of regular phishing training, would assist in reducing the likelihood of successful exploitation, in-house training will not be able to prevent attacks led by threat actors with stolen credentials obtained via stealware. Additional technical controls should also be explored. These controls could encompass the implementation of multi-factor authentication (MFA) for all users, conditional access policies and web proxies filtering on low- or non-reputation domains.

One main method of reducing the threat of ransomware variants 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 needed to run the business and to keep a copy offline in case back-ups are impacted by the attack[1]. 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 little disruption. However, this does not nullify the fact that customer and employee data may have also been lost, and potentially released as ransomware threat actors often operate via the double extortion technique.

Indicators of Compromise

Rorschach Associated File Hashes (MD5):

- cy.exe (2237ec542cdcd3eb656e86e43b461cd1)PA - Dump Service Tool (benign file)
- winutils.dll (4a03423c77fe2c8d979caca58a64ad6c) - Loader and injector into notepad.exe
- config.ini (6bd96d06cd7c4b084fe9346e55a81cf9) - Encrypted ransomware payload

Rorschach Associated File Hashes (SHA1):

- 29f16c046a344e0d0adfea80d5d7958d6b6b8cfa
- 048b3942c715c6bff15c94cdc0bb4414dbab9e07
- 3b1a2847e006007626ced901e402f1a33bb800c7
- 71ed640ebd8377f52bda4968398c62c97ae1c3ed
- ee827023780964574f28c6ba333d800b73eae5c4
- 091f4bddea8bf443bc8703730f15b21f7ccf00e9
- 885a734c7869b52aa125674cb430199b2645cda0
- 9290478cda302b9535702af3a1dada25818ad9ce
- cd19c2741261de97e91943148ba8c0863567b461
- 76fb0d08fd5b9c52cb9da118ce5561cc0462555f
- 933ad0a7d9db57b92144840d838f7b10356c7e5
- dc8b9bc46f1d23779d3835f2b3648c21f4cf6151
- e8bb26f62983055cfb602aa39a89998e8f512466
- b93d649e73c21efea10d4d811b711316206c0509
- 74e4b2f7abf9dbd376372c9b05b26b02c2872e4b

[1] Offline backups in an online world - NCSC.GOV.UK

Threat Landscape

Ransomware continues to be one of the prominent threats facing all industry sectors. Recent attacks, as well as the developing nature of the ransomware threat landscape, suggest that the threat is growing as cybercriminal groups are becoming more comfortable demanding ever-increasing ransom quantities.

Threat Group

Although no official threat actor group attribution has been made at the time of writing, the Rorschach operator has yet to hide behind any alias and appears to have no affiliation to any known ransomware groups. This is a rare phenomenon in the ransomware threat landscape where reputation matters, and self-promotion is rampant.

Rorschach does not exhibit any clear-cut overlaps with any of the known ransomware groups but does appear to draw inspiration from some of them. Such similarities have been noted below:

- Rorschach autonomously performs tasks that are usually manual in ransomware strains, such as creating a domain group policy (LockBit 2.0)
- Rorschach applies a hybrid-cryptography scheme that is the basis of its encryption speed (Babuk)
- Rorschach ransom note content contains significant similarities to previous ransomware families (DarkSide and Yanluowang)
- The list of services to be stopped in Rorschach's configuration is similar to other ransomware variants (Babuk)
- The list of CIS languages used to halt the malware is identical to other ransomware families (LockBit 2.0)
- Rorschach employs an I/O Completion Ports method of thread (LockBit 2.0).

Mitre Methodologies

Resource Development
T1588.003 - Obtain Capabilities: Code Signing Certificates[2]

Execution
T1106 - Native API[3]

Persistence
T1556.001 - Modify Authentication Process: Domain Controller Authentication[4]
T1574.002 - Hijack Execution Flow: DLL Side-Loading[5]

Privilege Escalation
T1574.002 - Hijack Execution Flow: DLL Side-Loading[6]

Defense Evasion
T1070.001 - Indicator Removal: Clear Windows Event Logs[7]

[2] Obtain Capabilities: Code Signing Certificates, Sub-technique T1588.003 - Enterprise | MITRE ATT&CK®
[3] Native API, Technique T1106 - Enterprise | MITRE ATT&CK®
[4] Modify Authentication Process: Domain Controller Authentication, Sub-technique T1556.001 - Enterprise | MITRE ATT&CK®
[5] Hijack Execution Flow: DLL Side-Loading, Sub-technique T1574.002 - Enterprise | MITRE ATT&CK®
[6] Hijack Execution Flow: DLL Side-Loading, Sub-technique T1574.002 - Enterprise | MITRE ATT&CK®
[7] Indicator Removal: Clear Windows Event Logs, Sub-technique T1070.001 - Enterprise | MITRE ATT&CK®

T1556.001 - Modify Authentication Process: Domain Controller Authentication[8]
T1574.002 - Hijack Execution Flow: DLL Side-Loading[9]

Credential Access
T1556.001 - Modify Authentication Process: Domain Controller Authentication[10]

Discovery
T1083 - File and Directory Discovery[11]

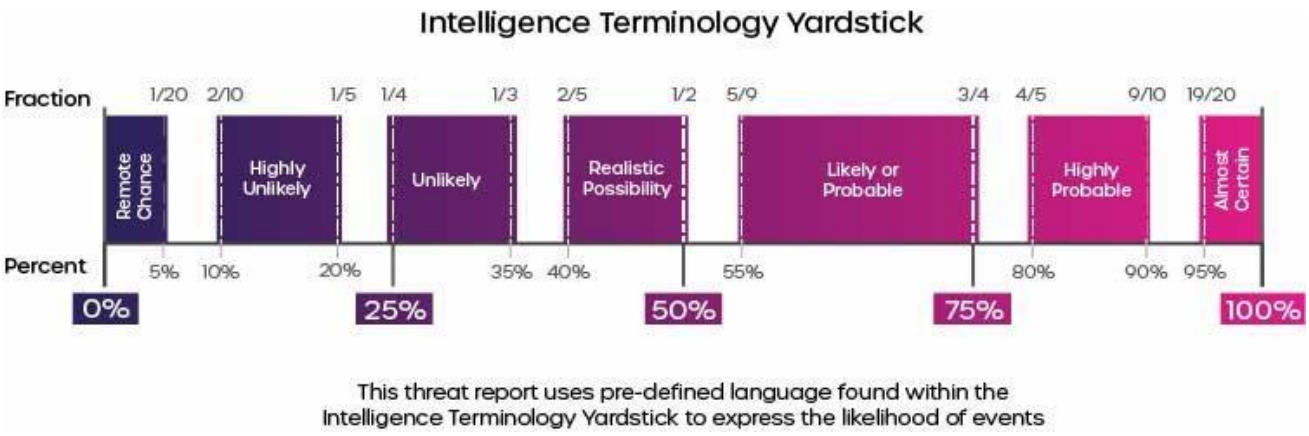
Collection
T1005 - Data from Local System[12]

Impact
T1486 - Data Encrypted for Impact[13]

Further Information

- Check Point Research Report

Intelligence Cut-off Date (ICoD): 04/07/2023 10:00 UTC



[8] Modify Authentication Process: Domain Controller Authentication, Sub-technique T1556.001 - Enterprise | MITRE ATT&CK®
[9] Hijack Execution Flow: DLL Side-Loading, Sub-technique T1574.002 - Enterprise | MITRE ATT&CK®
[10] Modify Authentication Process: Domain Controller Authentication, Sub-technique T1556.001 - Enterprise | MITRE ATT&CK®
[11] File and Directory Discovery, Technique T1083 - Enterprise | MITRE ATT&CK®
[12] Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®
[13] Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®