Quorum Cyber

Threat Intelligence NoEscape 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	07/06/2023	Initial Report Drafted.
1.1		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	

NoEscape Ransomware

Overview

NoEscape is a new Ransomware-as-a-Service (RaaS) tool which was announced in a post on a dark web forum on 22nd May 2023. Like other RaaS operations, NoEscape has an affiliate programme, where third-party contractors work to install NoEscape on target systems for a fee.

NoEscape is written in C++ and claims to be written from scratch, without recycling code from previous malware samples or ransomware products. This service has an interface which allows the customisation of compiled executables, allowing operators to choose whether they want to optimise for speed or thoroughness of encryption, which file paths to prioritise or ignore, and which services to terminate before starting encryption. NoEscape uses RSA and ChaCha20 encryption algorithms, can perform asynchronous LAN scanning, and can encrypt discovered network file shares as well as local drives. Shadow copies and system back-ups are deleted by NoEscape, which is standard practice for ransomware programmes.

This ransomware variant is compatible with Windows safe mode – a series of scripts can be run to force a victim host to reboot in safe mode, where endpoint detection and response (EDR) products can be disabled more easily before running encryption routines. Mechanisms are in place to reduce the chances of this malware running on hosts which are detected to be in CIS countries.

As a RaaS tool, NoEscape also comes with other features in addition to the standard file encryption functions, including a Tor admin panel, private chat functions for secret communications, and distributed denial-of-service (DDoS), call, and spam services at extra cost ("Available from 500k$").

Two NoEscape threat types are listed on Trend Micro's threat encyclopedia: Ransom.Win32.NOESCAPE.A and Ransom.Win32.NOESCAPE.B[1]. These were added on 18th August 2022 and 29th March 2023 respectively. As such, it is likely that some functionalities of the NoEscape RaaS tool were tested in the wild prior to the announcement of the affiliate programme on 22nd May 2023.

Impact

Successful exploitation by NoEscape 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

EDR solutions, such as Microsoft Defender, can provide additional protection against ransomware like NoEscape through raising alerts for potential breaches and assisting in containing threats.

[1] Ransom.Win32.NOESCAPE.A - Threat Encyclopedia (trendmicro.com)

If an EDR solution is not being used, the first instance of detection is likely to be the ransom note. The note will be labelled with the following file extension: HOW_TO_RECOVER_FILES.txt. A copy of a NoEscape ransom note is shown in *Figure 1*:

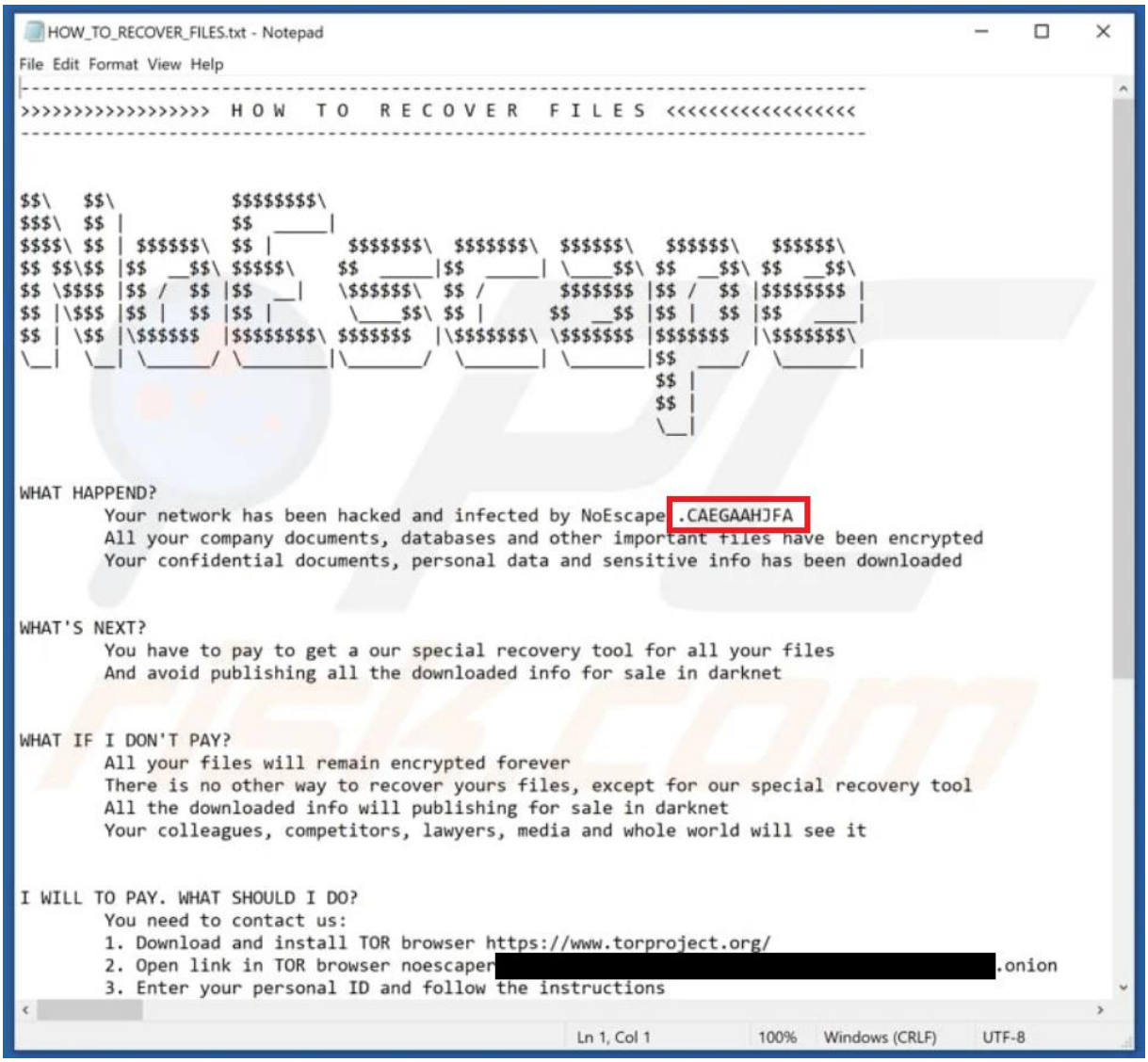


Figure 1: NoEscape ransom note[2]

Targeted Products

- VMware ESXi and Linux servers (ELF executables)
- Windows 7 and above (reflective DLL injection, .dll and .exe files)
- Windows XP (.exe files)
- Windows Server 2003 - 2022

[2] NoEscape Ransomware - Decryption, removal, and lost files recovery (updated) (pcrisk.com)

Containment, Mitigations & Remediations

It is recommended that employees receive training on how to spot signs of phishing emails. A common initial ingress mechanism utilised by ransomware groups is the distribution of phishing emails with malicious attachments. Whilst 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.

A primary method of reducing the threat of NoEscape 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 needed to run the business 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 little disruption. However, this does not nullify the fact that customer and employee data may have also been lost, and potentially released as NoEscape operates via the triple-extortion method.

Indicators of Compromise

NoEscape Ransomware Associated File Hashes (SHA-256):

- 07c70968c66c93b6d6c9a90255e1c81a3b385632c83f53f69534b3f55212ced9
- 68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccd2bc0d8
- 9d346518330eeefbf288aeca7b2b6243bc158415c7fee3f2c19694f0e5f7d51c
- 68e5caa3f0fd4adc595b1163bf0dd30ca621c5d7a6ad0a20dfa1968346daa3c8
- 16d9e969457a76874e7452e687a7b6843c65ef75d1a4404d369074ad389f6c38
- 21162bbd796ad2bf9954265276bfebea8741596e8fe9d86070245d9b5f9db6da

Threat Group

NoEscape ransomware operators run a dark web "name-and-shame" extortion blog where they post information about their victims. They employ a triple-extortion technique, threatening to leak stolen data to persuade organisations to pay the ransom. The group has been active in targeting universities, community colleges, and businesses in different countries, including the United States, United Kingdom, Italy, Belgium, Ireland, and Lebanon.

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 suggest that the threat is growing as criminal groups are becoming more

comfortable demanding ever-increasing ransom fees. Due to the significant number of targets exploited in recent months, it is likely that NoEscape ransomware operators will continue to exploit victims at a high frequency and as such will emerge into an increasingly notorious ransomware strain.

Mitre Methodologies

Resource Development
T1587.001 - Develop Capabilities: Malware[3]

Initial Access
T1190 - Exploit Public-Facing Application[4]

Execution
T1053.005 - Scheduled Task/Job: Scheduled Task[5]

Persistence
T1053.005 - Scheduled Task/Job: Scheduled Task[6]
T1098 - Account Manipulation[7]

Privilege Escalation
T1053.005 - Scheduled Task/Job: Scheduled Task[8]
T1134 - Access Token Manipulation[9]
T1548.002 - Abuse Elevation Control Mechanism: Bypass User Account Control[10]
T1562.001 - Abuse Elevation Control Mechanism: Bypass User Account Control[11]

Defence Evasion
T1070.002 - Indicator Removal: Clear Linux or Mac System Logs[12]
T1070.004 - Indicator Removal: File Deletion[13]
T1112 - Modify Registry[14]
T1134 - Access Token Manipulation[15]
T1548.002 - Abuse Elevation Control Mechanism: Bypass User Account Control[16]
T1562.001 - Abuse Elevation Control Mechanism: Bypass User Account Control[17]

Discovery
T1057 - Process Discovery[18]
T1083 - File and Directory Discovery[19]
T1120 - Peripheral Device Discovery[20]

[3] Develop Capabilities: Malware, Sub-technique T1587.001 - Enterprise | MITRE ATT&CK®
[4] Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®
[5] Scheduled Task/Job: Scheduled Task, Sub-technique T1053.005 - Enterprise | MITRE ATT&CK®
[6] Scheduled Task/Job: Scheduled Task, Sub-technique T1053.005 - Enterprise | MITRE ATT&CK®
[7] Account Manipulation, Technique T1098 - Enterprise | MITRE ATT&CK®
[8] Scheduled Task/Job: Scheduled Task, Sub-technique T1053.005 - Enterprise | MITRE ATT&CK®
[9] Access Token Manipulation, Technique T1134 - Enterprise | MITRE ATT&CK®
[10] Abuse Elevation Control Mechanism: Bypass User Account Control, Sub-technique T1548.002 - Enterprise | MITRE ATT&CK®
[11] Abuse Elevation Control Mechanism: Bypass User Account Control, Sub-technique T1548.002 - Enterprise | MITRE ATT&CK®
[12] Indicator Removal: Clear Linux or Mac System Logs, Sub-technique T1070.002 - Enterprise | MITRE ATT&CK®
[13] Indicator Removal: File Deletion, Sub-technique T1070.004 - Enterprise | MITRE ATT&CK®
[14] Modify Registry, Technique T1112 - Enterprise | MITRE ATT&CK®
[15] Access Token Manipulation, Technique T1134 - Enterprise | MITRE ATT&CK®
[16] Abuse Elevation Control Mechanism: Bypass User Account Control, Sub-technique T1548.002 - Enterprise | MITRE ATT&CK®
[17] Abuse Elevation Control Mechanism: Bypass User Account Control, Sub-technique T1548.002 - Enterprise | MITRE ATT&CK®
[18] Process Discovery, Technique T1057 - Enterprise | MITRE ATT&CK®
[19] File and Directory Discovery, Technique T1083 - Enterprise | MITRE ATT&CK®
[20] Peripheral Device Discovery, Technique T1120 - Enterprise | MITRE ATT&CK®

T1135 - Network Share Discovery[21]

Lateral Movement

T1021.002 - Remote Services: SMB/Windows Admin Shares[22]
T1210 - Exploitation of Remote Services[23]

Collection

T1005 - Data from Local System[24]

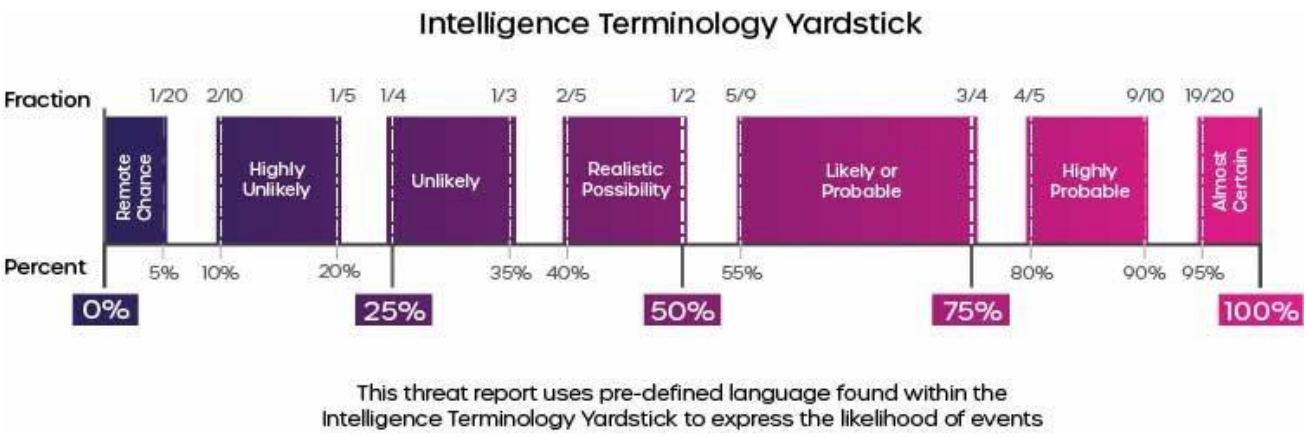
Impact

T1486 - Data Encrypted for Impact[25]
T1489 - Service Stop[26]
T1490 - Inhibit System Recovery[27]

Further Information

- PCrisk Malware Analysis
- Cyble NoEscape Ransomware Report

Intelligence Cut-off Date (ICoD): 28/06/2023 10:00 UTC



[21] Network Share Discovery, Technique T1135 - Enterprise | MITRE ATT&CK®
[22] Remote Services: SMB/Windows Admin Shares, Sub-technique T1021.002 - Enterprise | MITRE ATT&CK®
[23] Exploitation of Remote Services, Technique T1210 - Enterprise | MITRE ATT&CK®
[24] Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®
[25] Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®
[26] Service Stop, Technique T1489 - Enterprise | MITRE ATT&CK®
[27] Inhibit System Recovery, Technique T1490 - Enterprise | MITRE ATT&CK®