Quorum Cyber

Threat Intelligence Vice Society Ransomware Report

TLP Status: White

☎ +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
1.0	19/01/2023	Initial Report
1.1	24/01/2023	PDF Formatting
1.2	17/04/2023	Second Draft/PDF Formatting

Related Documents

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

Document Name	Date	Version
-	-	-

Vice Society Analysis

Overview

Vice Society is an online criminal gang that has gained notoriety over the past several months by targeting multiple organisations across the world in several sectors, but most frequently those relating to education. By the end of December 2022, Vice Society had successfully targeted approximately 40 schools located in various countries around the globe, making the group an extreme threat to the entirety of the education sector.

Since Vice Society was first reported back in the summer of 2021, the gang has operated multiple versions of ransomware. From the start of their operations until July 2022, Vice Society primarily exploited victims via two main ransomware instances. These were, "HelloKitty" ransomware for targeting Linux-based systems and "Zeppelin" ransomware for targeting Windows-based systems. Since July 2022, it was reported that the gang had developed custom-branded ransomware, dubbed "PolyVice", which was likely introduced to address some issues encountered by the gang with the previously mentioned HelloKitty and Zeppelin variants. Most notably, PolyVice has improved the encryption of compromised files by using a hybrid of both asymmetric and symmetric encryption to obfuscate files.

Like other ransomware strains, initial compromise by Vice Society can occur in multiple ways. These include access via leaked credentials, spear phishing, backdoors from previous attacks, and in this instance exploitation of known vulnerabilities, such as PrintNightmare[1]: CVE-2021-34527.

Recent Vice Society targets include:

March 2023	Lewis & Clark College[2]	Vice Society Ransomware
March 2023	Berkeley County Schools	Vice Society Ransomware
February 2023	Guildford County School	Vice Society Ransomware
January 2023	Okanagan College	Vice Society Ransomware

In April 2023, Vice Society were reported to have deployed a new PowerShell script in order to automate data theft from target networks. The new data exfiltrating script uses Living off the Land binaries (LOLBins) to remain in a mode of stealth, whilst automating the extraction of target data, prior to encryption. There also exists a functionality within the automation in which folders are specifically targeted which contain more than 433 strings in English, Czech, German, Lithuanian, Luxembourgish, Portuguese, and Polish, with an emphasis on German and English.

Impact

Successful exploitation by one of Vice Society's ransomware variants will result in the encryption and exfiltration of significant amounts of data held on the compromised device or system before a ransom of a predetermined amount is issued. The ransom fee demanded will almost certainly depend on the estimated value of the compromised organisation. For example, in October 2022 UK car dealership Pendragon was issued with a £53 million ransom from a ransomware attack. The attack took place soon after the company released information of a £400 million takeover from a large stakeholder.

[1] What is PrintNightmare? The Windows print spooler exploit explained | PaperCut

[2] Vice Society nabs Lewis & Clark College as latest ransomware victim | Cybernews

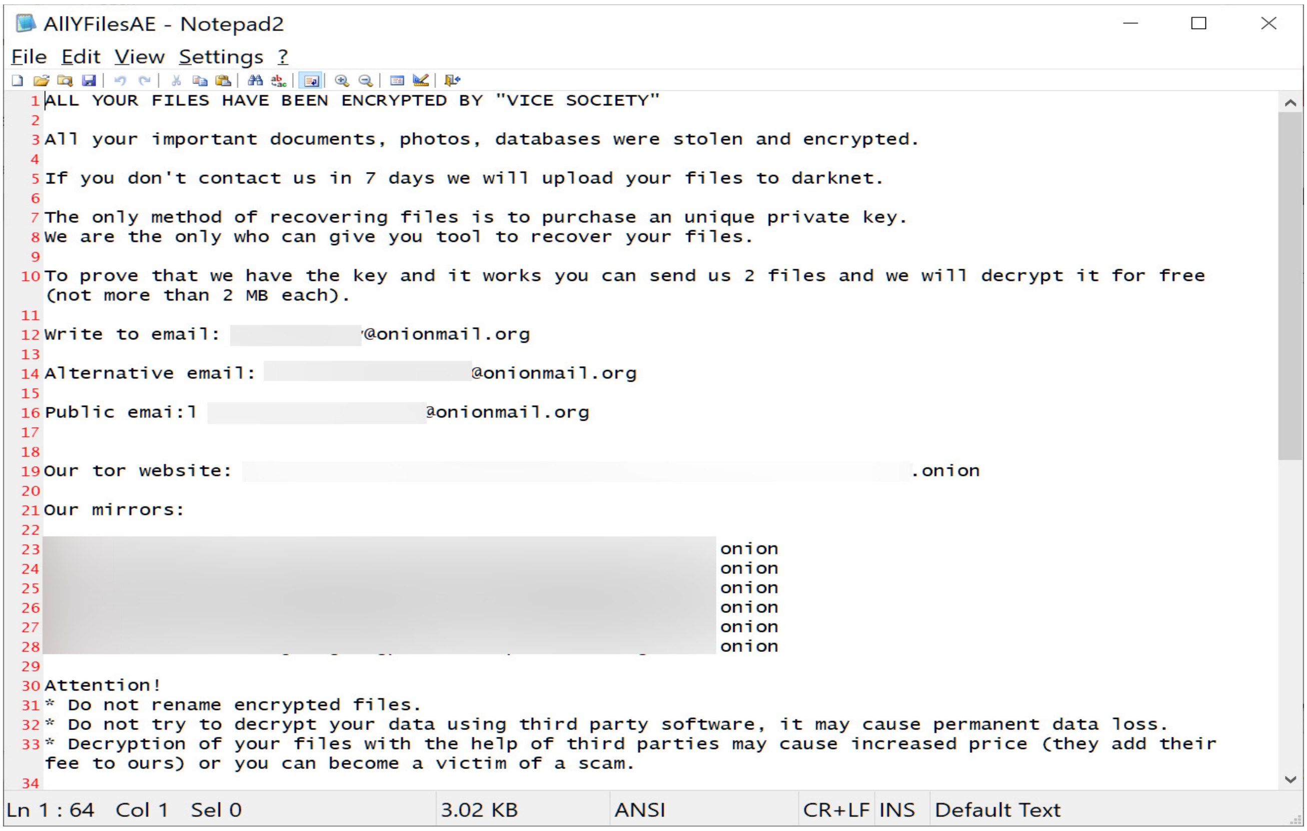
Encrypted data may include private customer data, corporate finance data and system credentials. Vice Society's double extortion strategy will almost certainly result in all stolen data being published to dark web forums, where there is a realistic possibility that stolen data will be used for initial compromise in future attacks.

Incident Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide additional protection against ransomware threats such as Vice Society's suite of ransomware. EDR tools can alert system users of potential breaches and prevent further progress before the malware can implement significant damage.

If an EDR solution is not being used, the first instance of detection is likely to be the ransom note. A copy of a typical Vice Society ransom note is found below:

Vice Society Ransom note



```
ALL YOUR FILES HAVE BEEN ENCRYPTED BY "VICE SOCIETY"

All your important documents, photos, databases were stolen and encrypted.

If you don't contact us in 7 days we will upload your files to darknet.

The only method of recovering files is to purchase an unique private key.
We are the only who can give you tool to recover your files.

To prove that we have the key and it works you can send us 2 files and we will decrypt it for free
(not more than 2 MB each).

Write to email: [redacted]@onionmail.org

Alternative email: [redacted]@onionmail.org

Public emai:l [redacted]@onionmail.org


Our tor website: [redacted].onion

Our mirrors:

[redacted]onion
onion
onion
onion
onion
onion

Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* Decryption of your files with the help of third parties may cause increased price (they add their
fee to ours) or you can become a victim of a scam.
```

Source: Bleeping Computer[3]

Vice Society – Targeted Products

- HelloKitty ransomware – Linux.
- Zeppelin ransomware – Windows OS.

[3] Vice Society ransomware gang switches to new custom encryptor (bleepingcomputer.com)

- PolyVice ransomware – Unknown: likely targets both, due to it being designed to replace both Zeppelin and HelloKitty.

Containment, Mitigations & Remediations

It is recommended that employees receive training on how to detect signs of phishing emails. A common initial ingress mechanism utilised by Vice Society is the use of spear phishing. Whilst user awareness, through the utilisation of regular phishing training, would assist in reducing the likelihood of successful exploitation, in-house training won't be able to prevent attacks led by threat actors with stolen credentials obtained via stealware or other harvesting methods. Additional technical controls should also be explored. These controls could encompass the enforcement of multi-factor authentication (MFA) for all users, conditional access policies and web proxies filtering on low- or non-reputation domains.

As previously mentioned, Vice Society has historically targeted systems by exploiting known vulnerabilities such as Print Nightmare. It is therefore strongly advised to ensure that Print Nightmare patches, provided by Microsoft, have been installed on all associated systems[4].

As mentioned previously, one main method of reducing the threat posed by Vice Society's suite of known 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[5]. 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. However, this does not nullify the fact that customer and employee data may have also been lost, and potentially released as Vice Society operates via double extortion.

Indicators of Compromise

HelloKitty Ransomware Associated Hashes (SHA-256):

- 08c6e20b1785d4ec4e3f9956931d992377963580b4b2c6579fd9930e08882b1c
- 10b9b1d8f6bafd9bb57ccfb1da4a658f10207d566781fa5fb3c4394d283e860e
- 36417f0ea6d948cbd7e003b3cefbb603d886849a8c80e0999c7969b03f2b9c28
- 66c4f54da6542339de036872e80306f345b8572a71e782434245455e03541465
- 6f191f598589b7708b1890d56b374b45c6eb41610d34f976f0b4cfde8d5731af
- 77d3b1cf6d5a0a07090cdb078dce6e3849465c9acde7e1ba66c3893fefc73d4b
- 78afe88dbfa9f7794037432db3975fa057eae3e4dc0f39bf19f2f04fa6e5c07c
- 947e357bfdfe411be6c97af6559fd1cdc5c9d6f5cea122bf174d124ee03d2de8
- 98bad23237c9a5067cc1cc7aaffe126e3c96478b5170faa4faa9748e42213408
- 99baffcd7a6b939b72c99af7c1e88523a50053ab966a079d9bf268aff884426e

[4] Microsoft fixes remaining Windows PrintNightmare vulnerabilities (bleepingcomputer.com)

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

- 9a6584a163d8c378e6f873c5544794274cce2532e91fc079b79fd73399447b03
- 9a7daafc56300bd94ceef23eac56a0735b63ec6b9a7a409fb5a9b63efe1aa0b0
- a147945635d5bd0fa832c9b55bc3ebcea7a7787e8f89b98a44279f8eddda2a77
- a23110f763cbecc6f2de868d413073d4af7a3514d5e728eac4989c33191be227
- a547d1da26b7eb8a4b439127eafa0d4fc4bbe0a27e17d14294a50a2832c96547
- b24dcfdda948b339637fe507cf032ec233288691b700e1585 cb34b4190704858
- c2498845ed4b287fd0f95528926c8ee620ef0cbb5b27865b2007d6379ffe4323
- c7d6719bbfb5baaadda498bf5ef49a3ada1d795b9ae4709074b0e3976968741e
- ccacf4658ae778d02e4e55cd161b5a0772eb8b8eee62fed34e2d8f11db2cc4bc
- dc007e71085297883ca68a919e37687427b7e6db0c24ca014c148f226d8dd98f
- de9d6e3b4aebbc8aeaa3f74a5d50d14b861209d90b4c909920b48c10fd4c77b5
- e09ead5b6ac9ec9203b9fb6c9152ba451498bb291478a69ac71ff6c36c468f9e
- e94064401b54c399d3f844fdf08f880cb8c5d74c34de9dc28733dd22dabba678
- eeb51dce12f243b332b51d7b1b11ecff155dd823ff8f9b79d6ad486cc49098ba
- ef614b456ca4eaa8156a895f450577600ad41bd553b4512ae6abf3fb8b5eb04e
- f668f74d8808f5658153ff3e6aee8653b6324ada70a4aa2034dfa20d96875 836
- fa722d0667418d68c4935e1461010a8f730f02fa1f595ee68bd0768fd5d1f8bb
- fdc2de095390ec046dc3f398a47a38670282bdc2ef76dd7fc1195ac4ee0421a8

Zeppelin Ransomware Associated File Hashes (SHA-256):

- a5847867730e7849117c31cdae8bb0a25004635d49f366fbfaebce034d865d7d
- 005b00d41740f7b0327d4d5fe0402dcfc84ae0df44a2231a89a59909eeb30b23
- 6f6e84452e4bc959418cfd63626f7961bbb7a05eabf2043236e3da45ebc73a7d

PolyVice Ransomware Associated File Hashes (SHA-256):

- 1df9b68a8642e6d1fcb786d90a1be8d9633ee3d49a08a5e79174c7150061faa8
- f366e079116a11c618edcb3e8bf24bcd2ffe3f72a6776981bf1af7381e504d61

Additional Known Vice Society Associated Domains:

- bitron[.]com
- glutz[.]com
- imacorp[.]com
- kinetic[.]ph
- afasd[.]net

- albina[.]com
- avsolutionsltd[.]com
- baysgarthschool[.]co[.]uk
- capitalpower[.]com
- cristalcontrols[.]com
- dixonsaa[.]com
- feuvert[.]es
- fiscosaudepe[.]com[.]br
- fvsra[.]org
- grandview[.]org
- gruposifu[.]com
- hollerclassic[.]com
- huntsvilletexas[.]com
- huntsvilletx[.]gov
- hydro-gear[.]com

Vice Society Associated IP Addresses:

- 194[.]34[.]246[.]90
- 198[.]252[.]98[.]184
- 5[.]161[.]136[.]176
- 5[.]255[.]99[.]59

Exploited Vulnerabilities

- **CVE-2021-1675 (CVSSv3 Score: 8.8)** - Windows Print Spooler Elevation of Privilege Vulnerability[6]
- **CVE-2021-34527 (CVSSv3 Score: 8.8)** - Windows Print Spooler Remote Code Execution Vulnerability[7]
- **CVE-2021-36958 (CVSSv3 Score: 7.8)** - Windows Print Spooler Remote Code Execution Vulnerability[8]

Threat Group

The Vice Society gang operates much like other online criminal groups by utilising the double extortion technique. This means that not only does the group encrypt the private data of the victim and demand a ransom for the keys, but they also threaten victims with the publication of the data on their own dark web site. This is likely designed to increase

[6] NVD - CVE-2021-1675 (nist.gov)
[7] NVD - CVE-2021-34527 (nist.gov)
[8] NVD - CVE-2021-36958 (nist.gov)

pressure on the victim and increase the chances of payment, as the publishing of data can cause future security concerns.

Vice Society does not currently provide a Ransomware-as-a-Service (RaaS) option for other online criminals to use. However, the code design within PolyVice has led some experts at Sentinel Labs[9] to suggest that the ransomware has been built to provide other threat actors with the ability to customise payloads with their own brands. This is known as Locker-as-a-Service (LaaS) and poses a significant threat to all sectors as multiple threat actors may have access to the ransomware.

Whilst different sources dispute the frequency of Vice Society attacks, one report by The Record states that Vice Society attacks are ranked as the fifteenth most prevalent, accounting for approximately 120 reported attacks between 15 December and January[10]. With the potential of LaaS, this figure is likely to increase over the coming months.

Several additional notorious ransomware groups have also been reported to have used the Vice Society ransomware variants, including but not limited to: Play, AvosLocker and CLOP.

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, suggests that the threat is growing as cyber-criminal groups are becoming more comfortable demanding ever increasing ransom quantities.

The new Vice Society data exfiltration script demonstrates the groups capabilities of applying optimum coding practices and a sophisticated level of scripting. The utilisation of LOLBins by the ransomware gang indicates that the group are focusing on avoiding detection and maintaining a significant level of stealth within their campaigns. Given that Vice Society also recently pivoted to the new “PolyVice” file encryptor, it is likely that the group has the resources and personnel at their disposal to continue to enhance the sophistication of their toolset. As such, the Vice Society group has now officially established itself amongst the most notorious ransomware threats to organisations worldwide, in particular those in the education sector.

[9] Custom-Branded Ransomware: The Vice Society Group and the Threat of Outsourced Development - SentinelOne

[10] Ransomware tracker: The latest figures [April 2023] (therecord.media)

Vice Society Mitre Methodologies

HelloKitty / Zeppelin Ransomware

Reconnaissance

T1595 - Active Scanning[11]

T1592 - Gathering Victim Host Information[12]

Initial Access

T1566 - Phishing[13]

T1078 - Valid Accounts[14]

T1078 - Valid Accounts[15]

Execution

T1059.001 - Command and Scripting Interpreter: PowerShell[16]

T1059.003 - Command and Scripting Interpreter: Windows Command Shell[17]

T1569.002 - System Services: Service Execution[18]

T1047 - Windows Management Instrumentation[19]

Collection

T1005 - Data from Local System[20]

Persistence

T1053 - Scheduled Task/Job[21]

T1098 - Account Manipulation[22]

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder[23]

T1078 - Valid Accounts[24]

[11] Active Scanning, Technique T1595 - Enterprise | MITRE ATT&CK®

[12] Gather Victim Host Information, Technique T1592 - Enterprise | MITRE ATT&CK®

[13] Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®

[14] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®

[15] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®

[16] Command and Scripting Interpreter: PowerShell, Sub-technique T1059.001 - Enterprise | MITRE ATT&CK®

[17] Command and Scripting Interpreter: Windows Command Shell, Sub-technique T1059.003 - Enterprise | MITRE ATT&CK®

[18] System Services: Service Execution, Sub-technique T1569.002 - Enterprise | MITRE ATT&CK®

[19] Windows Management Instrumentation, Technique T1047 - Enterprise | MITRE ATT&CK®

[20] Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®

[21] Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®

[22] Account Manipulation, Technique T1098 - Enterprise | MITRE ATT&CK®

[23] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®

[24] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®

T1574.002 - Hijack Execution Flow: DLL Side-Loading[25]

Privilege Escalation

T1055 - Process Injection[26]

T1068 - Exploitation for Privilege Escalation[27]

T1078 - Valid Accounts[28]

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder[29]

T1574.002 - Hijack Execution Flow: DLL Side-Loading[30]

Defence Evasion

T1070.001 - Indicator Removal on Host: Clear Windows Event Logs[31]

T1070.003 - Indicator Removal on Host: Clear Command History[32]

T1562.001 - Impair Defenses: Disable or Modify Tools[33]

T1564.001 - Hide Artifacts: Hidden Files and Directories[34]

T1036 - Masquerading[35]

T1055 - Process Injection[36]

T1078 - Valid Accounts[37]

T1574.002 - Hijack Execution Flow: DLL Side-Loading[38]

Credential Access

T1003.003 - OS Credential Dumping: NTDS[39]

T1212 - Exploitation for Credential Access[40]

Lateral Movement

T1021.001 - Remote Services: Remote Desktop Protocol[41]

[25] Hijack Execution Flow: DLL Side-Loading, Sub-technique T1574.002 - Enterprise | MITRE ATT&CK®
[26] Process Injection, Technique T1055 - Enterprise | MITRE ATT&CK®
[27] Exploitation for Privilege Escalation, Technique T1068 - Enterprise | MITRE ATT&CK®
[28] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®
[29] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®
[30] Hijack Execution Flow: DLL Side-Loading, Sub-technique T1574.002 - Enterprise | MITRE ATT&CK®
[31] Indicator Removal: Clear Windows Event Logs, Sub-technique T1070.001 - Enterprise | MITRE ATT&CK®
[32] Indicator Removal: Clear Command History, Sub-technique T1070.003 - Enterprise | MITRE ATT&CK®
[33] Impair Defenses: Disable or Modify Tools, Sub-technique T1562.001 - Enterprise | MITRE ATT&CK®
[34] Hide Artifacts: Hidden Files and Directories, Sub-technique T1564.001 - Enterprise | MITRE ATT&CK®
[35] Masquerading, Technique T1036 - Enterprise | MITRE ATT&CK®
[36] Process Injection, Technique T1055 - Enterprise | MITRE ATT&CK®
[37] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®
[38] Hijack Execution Flow: DLL Side-Loading, Sub-technique T1574.002 - Enterprise | MITRE ATT&CK®
[39] OS Credential Dumping: NTDS, Sub-technique T1003.003 - Enterprise | MITRE ATT&CK®
[40] Exploitation for Credential Access, Technique T1212 - Enterprise | MITRE ATT&CK®
[41] Remote Services: Remote Desktop Protocol, Sub-technique T1021.001 - Enterprise | MITRE ATT&CK®

T1080 - Taint Shared Content[42]

Command & Control

T1090.002 - Proxy: External Proxy[43]

T1090.003 - Proxy: Multi-hop Proxy[44]

Exfiltration

T1020 - Automated Exfiltration[45]

Impact

T1486 - Data Encrypted for Impact[46]

T1531 - Account Access Removal[47]

T1489 - Service Stop[48]

T1499 - Endpoint Denial of Service[49]

PolyVice Ransomware

Reconnaissance

T1592 - Gathering Victim Host Information[50]

Initial Access

T1566 - Phishing[51]

T1078 - Valid Accounts[52]

Persistence

T1037 - Boot or Logon Initialization Scripts[53]

[42] Taint Shared Content, Technique T1080 - Enterprise | MITRE ATT&CK®

[43] Proxy: External Proxy, Sub-technique T1090.002 - Enterprise | MITRE ATT&CK®

[44] Proxy: Multi-hop Proxy, Sub-technique T1090.003 - Enterprise | MITRE ATT&CK®

[45] Automated Exfiltration, Technique T1020 - Enterprise | MITRE ATT&CK®

[46] Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®

[47] Account Access Removal, Technique T1531 - Enterprise | MITRE ATT&CK®

[48] Service Stop, Technique T1489 - Enterprise | MITRE ATT&CK®

[49] Endpoint Denial of Service, Technique T1499 - Enterprise | MITRE ATT&CK®

[50] Gather Victim Host Information, Technique T1592 - Enterprise | MITRE ATT&CK®

[51] Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®

[52] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®

[53] Boot or Logon Initialization Scripts, Technique T1037 - Enterprise | MITRE ATT&CK®

Defence Evasion

T1070.004 - Indicator Removal: File Deletion[54]

T1497.001 - Virtualization/Sandbox Evasion: System Checks[55]

Credential Access

T1003 - OS Credential Dumping[56]

Impact

T1486 - Data Encrypted for Impact[57]

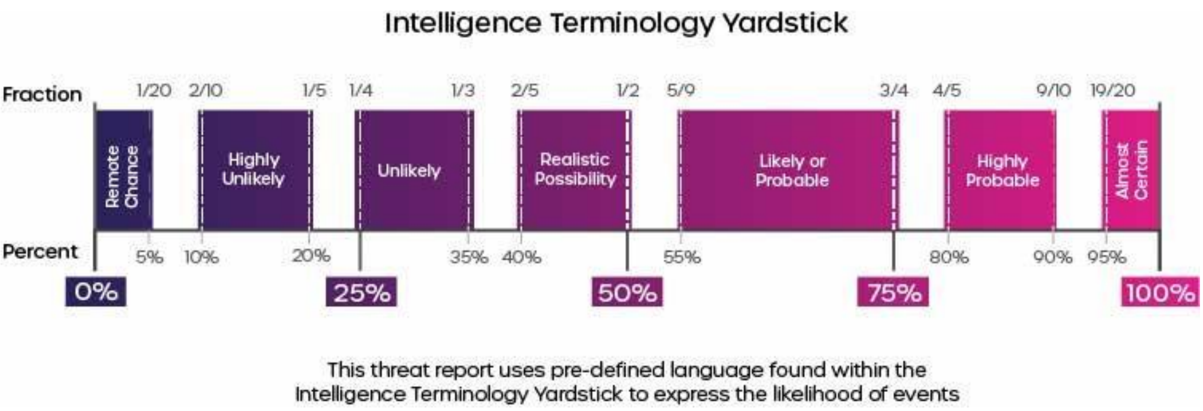
T1490 - Inhibit System Recovery[58]

T1491.001 - Defacement: Internal Defacement[59]

Additional information

- Unit42 Report

Intelligence Cut-off Date (ICoD): 17/04/2023 15:00GMT



Intelligence Terminology Yardstick

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

[54] Indicator Removal: File Deletion, Sub-technique T1070.004 - Enterprise | MITRE ATT&CK®

[55] Virtualization/Sandbox Evasion: System Checks, Sub-technique T1497.001 - Enterprise | MITRE ATT&CK®

[56] OS Credential Dumping, Technique T1003 - Enterprise | MITRE ATT&CK®

[57] Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®

[58] Inhibit System Recovery, Technique T1490 - Enterprise | MITRE ATT&CK®

[59] Defacement: Internal Defacement, Sub-technique T1491.001 - Enterprise | MITRE ATT&CK®