Quorum Cyber

Threat Intelligence Agenda 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	19/07/2023	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	

Agenda Ransomware

Overview

Agenda ransomware (also known as Qilin), is a malware family that has actively targeted various industry sectors including healthcare, education, manufacturing, and real estate, since at least July 2022. The group behind the ransomware operates via the Ransomware-as-a-Service (RaaS) model and has been observed using different programming languages, including Rust and Go, to evade detection. The Rust variant of the Agenda ransomware was first observed in December 2022 and includes intermittent encryption tactics to deliver faster encryption and detection evasion capabilities. Agenda ransomware operators apply the double-extortion model, threatening to leak stolen data if the ransom is not paid. Further, the group, and its affiliates, earn between 80% to 85% of the ransom payments. Agenda RaaS provided affiliates with an admin panel that allowed them to customise binary payloads for each victim.

The malware gains initial access to systems through phishing emails and password-protected files hosted on cloud storage services.

In May 2023, a threat actor, named 'Qilin', advertised the Agenda/Qilin RaaS programme in underground forums, including Club2CRD, Cracked Forum, and XSS (eX DamageLab), as well as Telegram[1]. These reports indicated that the Agenda/Qilin affiliates accessed target systems via phishing emails embedded with malicious links. Subsequent to gaining access, the ransomware operators conducted lateral movement within the infected network to search for files to encrypt. Following the encryption of the victim's files, the operators deployed a ransom note that contained instructions regarding how to receive the decryption keys.

As is the case with other notorious ransomware strains, such as LockBit, Agenda ransomware avoids targets in specific geographic locations by reviewing the system language settings of the ransomware platform. This involves a list of all languages 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 penalties from inside the CIS, provided they avoid attacking its organisations.

Impact

Successful exploitation by Agenda 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 the Agenda ransomware. EDR solutions can alert system users of potential breaches and stop further progress before the malware can do significant damage.

[1] Cybersecurity Services, Solutions & Products. Global Provider | Group-IB

Targeted Products

Windows OS.

Containment, Mitigations & Remediations

As mentioned previously, a primary method of reducing the threat of Agenda 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

Agenda Ransomware Associated File Hashes (SHA256):

- 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6
- e90bdaaf5f9ca900133b699f18e4062562148169b29cb4eb37a0577388c22527
- 55e070a86b3ef2488d0e58f945f432aca494bfe65c9c4363d739649225efbbd1
- 2c5a3bc9c10c2f856c80f39e7bc8446f3f64003ee01413e7761e8df5a0dd3241
- 5592c91362b538d7592216ec062b518a587f25e192c935c92d1346a8325845e7
- 6964610d95c57d566f04cb19825596b2351f11f348c05c81fdbed85eb16e04f8
- 9c9a264f5f1a78753f7f80ee6143d6c8967fa1375821bc09187767756d366800
- f95e02028e7b3fa33b8a0b4b07cf413ca825bc56221a2435f83771d5fadcc91c
- fd7cbadcfca84b38380cf57898d0de2adcdfb9c3d64d17f886e8c5903e416039

Threat Group

At the time of writing, minimal details have been ascertained regarding the threat actor group responsible for Agenda ransomware operations. However, initial reporting and analysis has revealed the following attributes of the group:

- The group behind the ransomware operates via the RaaS model
- Agenda ransomware authors have been observed using different programming languages, including Rust and Go
- Agenda ransomware operators apply the double-extortion model, threatening to leak stolen data if the ransom is not paid
- The group, and its affiliates, earn between 80% to 85% of the ransom payments.

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.

Mitre Methodologies

Initial Access

T1091 - Replication Through Removable Media[2]

T1566.002 - Spearphishing Link[3]

Execution

T1059 - Command and Scripting Interpreter[4]

T1204.001 - User Execution: Malicious Link[5]

Defence Evasion

T1112 - Modify Registry[6]

T1562.001 - Impair Defenses: Disable or Modify Tools[7]

Credential Access

T1552.001 - Unsecured Credentials: Credentials In Files[8]

Discovery

T1012 - Query Registry[9]

T1018 - Remote System Discovery[10]

T1082 - System Information Discovery[11]

Lateral Movement

[2] Replication Through Removable Media, Technique T1091 - Enterprise | MITRE ATT&CK®
[3] Phishing: Spearphishing Link, Sub-technique T1566.002 - Enterprise | MITRE ATT&CK®
[4] Command and Scripting Interpreter, Technique T1059 - Enterprise | MITRE ATT&CK®
[5] User Execution: Malicious Link, Sub-technique T1204.001 - Enterprise | MITRE ATT&CK®
[6] Modify Registry, Technique T1112 - Enterprise | MITRE ATT&CK®
[7] Impair Defenses: Disable or Modify Tools, Sub-technique T1562.001 - Enterprise | MITRE ATT&CK®
[8] Unsecured Credentials: Credentials In Files, Sub-technique T1552.001 - Enterprise | MITRE ATT&CK®
[9] Query Registry, Technique T1012 - Enterprise | MITRE ATT&CK®
[10] Remote System Discovery, Technique T1018 - Enterprise | MITRE ATT&CK®
[11] System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®

T1091 - Replication Through Removable Media[12]

Collection

T1005 - Data from Local System[13]

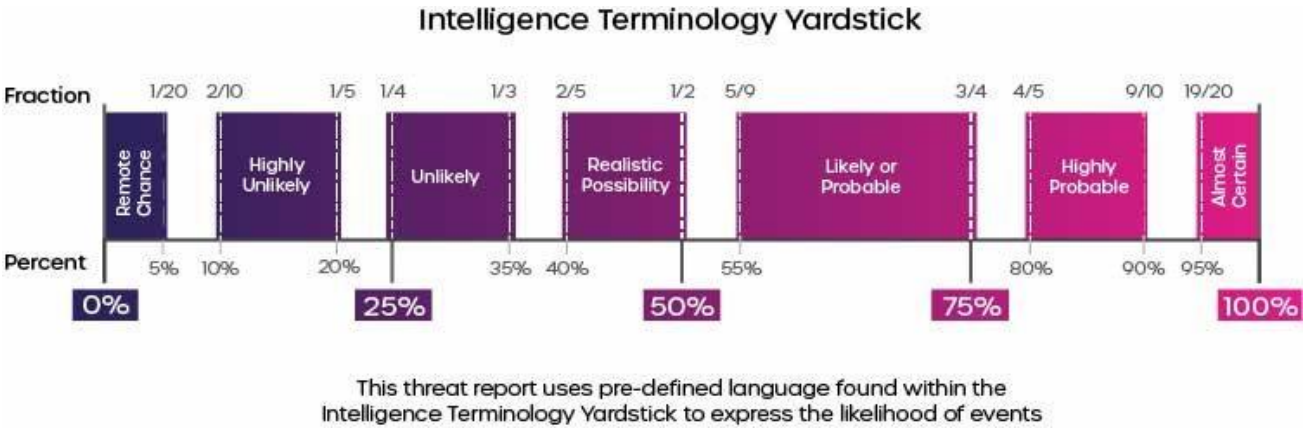
Impact

T1486 - Data Encrypted for Impact[14]

Further Information

- Group-IB Qilin Blog

Intelligence Cut-off Date (ICoD): 07/06/2023 10:00 UTC



[12] Replication Through Removable Media, Technique T1091 - Enterprise | MITRE ATT&CK®
[13] Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®
[14] Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®