



HC3: Threat Profile

June 18, 2024 TLP:CLEAR Report: 202406181500

Qilin, aka Agenda Ransomware

Executive Summary

Qilin is a ransomware-as-a-service (RaaS) offering in operation since 2022, and which continues to target healthcare organizations and other industries worldwide. The group likely originates from Russia, and was recently observed recruiting affiliates in late 2023. The ransomware has variants written in Golang and Rust, and is known to gain initial access through spear phishing, as well as leverage Remote Monitoring and Management (RMM) and other common tools in its attacks. The group is also known to practice double extortion, demanding ransom payments from victims to prevent data from being leaked.

Background

The Qilin ransomware operation was initially launched as “Agenda” in July 2022. However, by September, it had rebranded under the name Qilin, which it continues to operate as to this day. It operates as a ransomware-as-a-service (RaaS) offering in which affiliates leverage its tools and infrastructure to carry out ransomware attacks in exchange for 15-20% of the proceeds. In 2023, Qilin’s typical ransom demand was between \$50,000 and \$800,000, according to Group-IB. The group has steadily increased its activity over the past year, claiming responsibility for more than 60 ransomware attacks since January 2024. Researchers have identified dark web posts associated with Qilin in 2022 by a user who is likely connected to the RaaS group. In October 2023, Qilin was observed [recruiting affiliates on a hacking forum](#) and specifically excluding CIS countries from its targets. Qilin’s recruitment post includes details about its functionalities, including the encryption algorithms ChaCha20, AES-256, and RSA4096.

Technical Details

There are multiple variants of Agenda ransomware written in different programming languages. The malware was originally written in the Go programming language (also referred to as Golang). In general, malware written in the Golang has become common among threat actors. However, researchers recently discovered updated versions of the ransomware written in Rust. While the ransomware primarily targets Windows machines, a [Linux version](#) was identified in December 2023 targeting VMware ESXi servers.

To gain initial access, Agenda ransomware targets its victims through phishing and spear phishing emails. The actors are also known to leverage exposed applications and interfaces such as Citrix and remote desktop protocol (RDP). According to observations from Trend Micro, Agenda ransomware group uses Remote Monitoring and Management (RMM) tools, and Cobalt Strike for deployment of the binary.

The Agenda ransomware executable has the ability to propagate via PsExec and SecureShell, while also making use of different vulnerable SYS drivers for defense evasion. Agenda ransomware has some customization options, which include changing the filename extensions of encrypted files (such as “.MmXReVlxLV”) and the list of processes and services to terminate. The ransomware supports multiple encryption modes, all of which are controlled by the operator. The ransomware also employs various code obfuscation methods, such as renaming functions, altering control flows, and encrypting strings.

Agenda actors practice double extortion and operate a data leak site (DLS) where victims are posted. Victims are directed to communicate with the attackers via dark web portals or encrypted messaging services, ensuring the attackers’ anonymity and complicating law enforcement efforts to track interactions. Payments are demanded in cryptocurrencies, such as Bitcoin or Monero. However, even after payment, there is no guarantee that victims will receive the decryption tools required to recover their data.

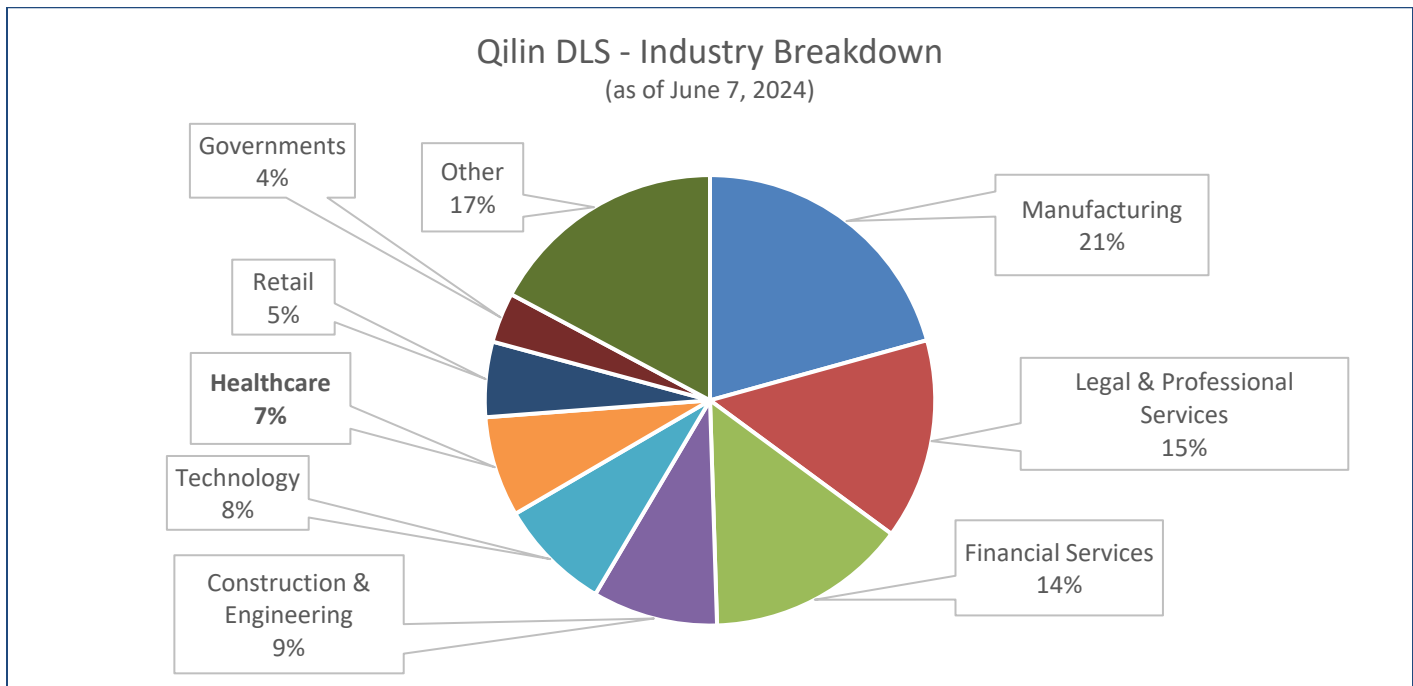


HC3: Threat Profile

June 18, 2024 TLP:CLEAR Report: 202406181500

Industry Targeting

Qilin is known to target organizations in various countries and industries, including education, healthcare and critical services, with geographical regions targeted including Australia, Canada, the United Kingdom, and the United States, among others. The group’s targeting appears to be opportunistic rather than targeted. According to a trusted third party’s monitoring of the Qilin DLS, healthcare victims accounted for just over 7% of the more than 100 victims appearing on the DLS, and the most targeted industries included Manufacturing, Legal and Professional Services, and Financial Services, as of June 7, 2024.



Impact to HPH Sector

HC3 has identified at least fifteen incidents involving Qilin/Agenda ransomware in the Healthcare and Public Health Sector (HPH) sector worldwide since October 2022, around half of which impacted HPH sector organizations in the United States. Most recently, on June 3, 2024, a United Kingdom-based pathology and diagnostic services provider fell victim to a Qilin ransomware attack, which impacted healthcare services at multiple major hospitals in London, according to [open-source reports](#).

Overall, U.S. HPH sector victim organization revenues range from USD \$6 million to USD \$40 million, while victim states include Indiana, Florida, Ohio, Georgia, Minnesota, Nevada, and Arizona. These U.S. HPH victim organizations include dental clinics, a healthcare communications company, an emergency medicine specialist, a radiology company, a home healthcare provider, a neurology center, and a cardiovascular medicine clinic.

Analyst Comment

While the Qilin RaaS group is likely a financially-motivated cyber criminal group with Russian origins and/or Russian-speaking members, a “qilin” (Chinese: 麒麟) is a legendary hooved chimerical creature that appears in Chinese mythology. An alternative spelling of the word, “Kylin” is also an operating system developed by academics at the National University of Defense Technology in the People’s Republic of



HC3: Threat Profile

June 18, 2024 TLP:CLEAR Report: 202406181500

China (PRC) since 2001. The first versions were intended for use by the Chinese military and other government organizations.

Additionally, while HC3 is aware of a single U.S. HPH victim appearing both on the LockBit 3.0 data leak site (DLS) and the Qilin DLS, there are no publicly known connections between these two RaaS operations at this time. Additionally, while re-victimization occasionally occurs across multiple RaaS groups, this instance would not be considered re-victimization, but rather a single incident where multiple RaaS groups are claiming to possess data allegedly exfiltrated from the victim to demand a ransom payment. Earlier this year, numerous existing LockBit victims also appeared on a new Dispossessor DLS, for example.

Mitigations

The following resources and guidance are provided by various elements of the federal government to assist the health sector in defending against, mitigating the effects of, and reporting ransomware attacks:

- DHS/CISA Stop Ransomware: <https://www.cisa.gov/stopransomware>
- FBI Cybercrime: <https://www.fbi.gov/investigate/cyber>
- FBI Internet Crime Complaint Center (IC3):
<https://www.ic3.gov/Home/ComplaintChoice/default.aspx/>
- FDA - Medical Device Security Information: <https://www.fda.gov/medical-devices/digital-healthcenter-excellence/cybersecurity>
- H-ISAC White Papers: <https://h-isac.org/category/h-isac-blog/white-papers/>
- 405(d) Resource Library: <https://405d.hhs.gov/resources>
- HC3 Products: <https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html>

Furthermore, the FBI recommends the following steps:

- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Regularly back up data, air gap, and password-protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system-defined or system-recognized scheduled tasks for unrecognized “actions.” (For example, review the steps each scheduled task is expected to perform.)
- Review anti-virus logs for indications that they were unexpectedly turned off.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multi-factor authentication where possible.
- Regularly change the passwords to network systems and accounts and avoid re-using passwords for different accounts.
- Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.



HC3: Threat Profile

June 18, 2024 TLP:CLEAR Report: 202406181500

- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.

Indicators of Compromise (IOCs)

| Type | Indicator |
|---------|--|
| MD5 | 64ca549e78ad1bd3a4bd2834b0f81080 |
| SHA-1 | 493ff413528f752c5fce3ceabd89d2ab37397b86 |
| SHA-256 | 93c16c11ffca4ede29338eac53ca9f7c4fbcf68b8ea85ea5ae91a9e00dc77f01 |
| MD5 | eb6fff4ee0f03ae5191f11570ff221c5 |
| SHA-1 | c2dfbf554e068195ecc40bebd0617ce09ad65784 |
| SHA-256 | 54ff98956c3a0a3bc03a5f43d2c801ebcc1255bed644c78bad55d7f7beebd294 |
| MD5 | 923c5af6fd29158b757fb876979d250b |
| SHA-1 | 6b3e3ff0495d39c85eca41f336bfd5ff92c97412 |
| SHA-256 | 9e1f8165ca3265ef0ff2d479370518a5f3f4467cd31a7b4b006011621a2dd752 |
| MD5 | 31edb01d243e8d989eb7e5aeef54dc |
| SHA-1 | 05f60fc706754b317ffc7839a2b0490f7cd6f71d |
| SHA-256 | e4882b8e8e414e983cf003a5c4038043002a004b63c4f0844a15268332597e80 |
| MD5 | a7ab0969bf6641cd0c7228ae95f6d217 |
| SHA-1 | 002971b6d178698bf7930b5b89c201750d80a07e |
| SHA-256 | 117fc30c25b1f28cd923b530ab9f91a0a818925b0b89b8bc9a7f820a9e630464 |
| MD5 | 417ad60624345ef85e648038e18902ab |
| SHA-1 | e18e6f975ef8fce97790fb8ae583caad1ec7d5b3 |
| SHA-256 | 555964b2fed3cced4c75a383dd4b3cf02776dae224f4848dcc03510b1de4dbf4 |
| MD5 | e01776ec67b9f1ae780c3e24ecc4bf06 |
| SHA-1 | 3ef805009f8694e78699932563c09ac3b6bc08a5 |
| SHA-256 | 0629cd5e187174cb69f3489675f8c84cc0236f11f200be384ed6c1a9aa1ce7a1 |
| MD5 | 63b89a42c39b2b56aae433712f96f619 |
| SHA-1 | 50927809fa3f1ec408d7a1715a714831f41160db |
| SHA-256 | bf9fc34ef4734520a1f65c1ec0a91b563bf002ac63982cbd2df10791493e9147 |
| MD5 | d0a711e4a51891ddf00f704d508b1ef2 |
| SHA-1 | d9ea05933353d1f32b18696877a3396140022f03 |
| SHA-256 | cd27a31e618fe93df37603e5ece3352a91f27671ee73bdc8ce9ad793cad72a0f |
| MD5 | 14dec91fdcaab96f51382a43adb84016 |
| SHA-1 | a85d9d2a3913011cd282abc7d9711b2346c23899 |
| SHA-256 | 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6 |
| MD5 | 88bb86494cb9411a9692f9c8e67ed32c |
| SHA-1 | 82f8060575de96dc4edc4f7b02ec31ba7637fa03 |



HC3: Threat Profile

June 18, 2024 TLP:CLEAR Report: 202406181500

| Type | Indicator |
|---------|--|
| SHA-256 | c26ce932f3609ecd710a3a1ca7f7b96f1b103a11b49a86e9423e03664eaabd40 |
| MD5 | 470d0261d18ed69990ce94f05d940de1 |
| SHA-1 | 890581fca724935118606a4d92dbc206f9eff04c |
| SHA-256 | 411b2ed12df1ace6559d3ea666c672617ce23e2ace06806bb53c55bcccb83303 |
| MD5 | d67303ba66bcb4dd89de87c83f3f831f |
| SHA-1 | 34bfe0c8aa61f90ca03b7e80271d5a8afae0be4b |
| SHA-256 | 8e1eb0ad22236e325387fdb45aea63f318a672c5d035a21d7b3a64eeafb4c5a2 |
| MD5 | 440810b008eed766f085b69b1723f54b |
| SHA-1 | 9692644974071cd484455e355f8d79ce8c486e20 |
| SHA-256 | aa0772fc6784799d59649654879c2b4a23919cda410bede0162751e6d6d6b558 |
| MD5 | 6b7eeb860917aa44982d8bd2d971aff1 |
| SHA-1 | d4e3a066e1c1a21e3d44f2ef81a94aec42f5df11 |
| SHA-256 | ebb2a1b46a13c308ffe62dda4d9da316d550433707b2c2a38ad710ea4456c608 |
| MD5 | a42d36f1af2c396e645ffa356fa47a1e |
| SHA-1 | 5914e976598ece1a271a60615a17420319a77812 |
| SHA-256 | ceed9fdce420c0558e56bb705664d59f67d62c12d7356ca8643908261638b256 |
| MD5 | e1d41939dc4cc4116cc3439a01cfb666 |
| SHA-1 | 6e35dfdf0d09a0313a33fcc6c77f4fe00a79b9dc |
| SHA-256 | 5e9fc42cf65e1a87e953d00cb2755d3b5b00c1414259534c3a85742295bb6ff9 |
| MD5 | 1410b418a078559581725d14fa389cdd |
| SHA-1 | 081cd6c242d472db9148fd0ce33346f7a3e87ac2 |
| SHA-256 | a25097d2ae808df410c2f35d725a500fb680f38605e62c9e3b619e389ef6733f |

File Names

| Type | Indicator | Last Submission |
|-----------|--|----------------------------|
| File Name | decryptor_399060b2.exe | 2024-05-26 21:32:55 UTC |
| File Name | enc.exe | 2024-05-26 12:28:54 UTC |
| File Name | 8e1eb0ad22236e325387fdb45aea63f318a672c5d035a21d7b3a64eeafb4c5a2 | 2024-05-15 10:47:47 UTC |
| File Name | 555964b2fed3cced4c75a383dd4b3cf02776dae224f4848dcc03510b1de4dbf4.elf | 2024-05-15 07:15:47 UTC |
| File Name | 99.dll | 2024-05-09 23:37:37 UTC |
| File Name | update.exe | 2024-04-26 06:35:03 UTC |
| File Name | inter.exe | 2024-04-17 23:55:45 UTC |
| File Name | ceed9fdce420c0558e56bb705664d59f67d62c12d7356ca8643908261638b256 | 2024-04-14 12:26:28 UTC |



HC3: Threat Profile

June 18, 2024 TLP:CLEAR Report: 202406181500

| Type | Indicator | Last Submission |
|-----------|--|-------------------------|
| File Name | e1d41939dc4cc4116cc3439a01cfb666 | 2024-04-14 12:11:53 UTC |
| File Name | BackupsFrst.exe1 | 2024-04-06 07:27:26 UTC |
| File Name | 2023-12-15_63b89a42c39b2b56aae433712f96f619_revil | 2024-03-14 12:45:31 UTC |
| File Name | update.exe | 2024-03-09 17:31:18 UTC |
| File Name | 31edb01d243e8d989eb7e5aeef54dc.virus | 2024-02-24 22:05:23 UTC |
| File Name | 2023-11-14_d0a711e4a51891ddf00f704d508b1ef2_revil | 2024-01-27 11:50:20 UTC |
| File Name | 0629cd5e187174cb69f3489675f8c84cc0236f11f200be384ed6c1a9aa1ce7a1.elf | 2024-01-19 02:31:04 UTC |
| File Name | c26ce932f3609ecd710a3a1ca7f7b96f1b103a11b49a86e9423e03664eaabd40.dll | 2023-12-24 08:14:00 UTC |
| File Name | 55ee6bb3deb3385052d7f57e6a48c3c5bba0f558f0d17653908550ffe37e1bea | 2023-12-14 12:41:48 UTC |
| File Name | 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6.exe | 2023-11-23 09:09:40 UTC |
| File Name | enc.exe | 2022-06-18 17:55:23 UTC |

Detection Names

| Detection Name | Vendor |
|-------------------------------------|--------------------------|
| Gen:Variant.Ransom.Agenda.1 | BitDefender |
| Gen:Variant.Ransom.Agenda.1 (B) | Emsisoft |
| W32/QilinCrypt!tr.ransom | Fortinet |
| HEUR:Trojan-Ransom.Linux.Qilin.a | Kaspersky |
| Trojan:Win64/AgendaGoLauncher.A!dha | Microsoft |
| Ransom:Win32/QilinCrypt.PA!MTB | Microsoft |
| Ransom:Win32/Qilin.MA!MTB | Microsoft |
| Ransom:Linux/Qilin.A!MTB | Microsoft |
| Ransom.Qilin | Symantec |
| Gen:Variant.Ransom.Agenda.1 | Trellix (FireEye) |
| Trojan.Win64.AGENDA.SVT | Trend Micro |
| Ransom.Win32.AGENDA.SMYXDLM | Trend Micro |
| Ransom.Win32.AGENDA.YXECJT | Trend Micro |
| Ransom.Linux.AGENDA.YXDLOT | Trend Micro |
| Ransom.Win32.AGENDA.THIAIBB | Trend Micro |
| Ransom.Win32.QILIN.R002C0XK523 | Trend Micro |
| HEUR:Trojan-Ransom.Linux.Qilin.a | ZoneAlarm by Check Point |



HC3: Threat Profile

June 18, 2024 TLP:CLEAR Report: 202406181500

MITRE ATT&CK Tactics & Techniques

| Tactic | Technique | ID |
|----------------------|---|---------------------------|
| Initial Access | Valid Accounts | T1078 |
| | Phishing | T1566 |
| | Spearphishing Attachment | T1566.001 |
| | Spearphishing Link | T1566.002 |
| | Exploit Public-Facing Application | T1190 |
| Execution | Scheduled Task/Job | T1053 |
| | Command and Scripting Interpreter | T1059.003 |
| | PowerShell | T1059.001 |
| Persistence | Boot or Logon Initialization Scripts | T1037 |
| Privilege Escalation | Exploitation of Vulnerabilities | T1068 |
| | Abuse Elevation Control Mechanism | T1548 |
| Defense Evasion | Process Injection | T1055 |
| | Rootkit | T1014 |
| | Exploitation for Defense Evasion | T1211 |
| | Execution Guardrails | T1480 |
| | Virtualization/Sandbox Evasion | T1497 |
| | Obfuscated Files or Information | T1027 |
| | OS Credential Dumping, LSASS Memory | T1003.001 |
| Discovery | System Information Discovery | T1082 |
| | Application Window Discovery | T1010 |
| | Network Service Scanning | T1046 |
| | Remote System Discovery | T1018 |
| Lateral Movement | Remote Services, Remote Desktop Protocol, SSH | T1021.001 |
| | | T1021.004 |
| | Lateral Tool Transfer | T1570 |
| Execution | System Services: Service Execution | T1569.002 |
| Collection | Data from Local System | T1005 |
| Exfiltration | Exfiltration Over Other Network Medium, Exfiltration Over Bluetooth | T1011.001 |
| Command and Control | Data Obfuscation, Junk Data | T1001.001 |
| | | |
| Impact | Data Encrypted for Impact | T1486 |
| | Data Destruction | T1485 |
| | Inhibit System Recovery | T1490 |
| | Disk Wipe | T1561.001 |

References

Abrams, Lawrence. "Linux version of Qilin ransomware focuses on VMware ESXi." BleepingComputer. December 3, 2023. <https://www.bleepingcomputer.com/news/security/linux-version-of-qilin-ransomware->

[TLP:CLEAR, ID# 202406181500, Page 7 of 10]



HC3: Threat Profile

June 18, 2024 TLP:CLEAR Report: 202406181500

[focuses-on-vmware-esxi/](#)

Bleih, Adi. "Qilin Ransomware: Get the 2024 Lowdown." Cyberint. March 26, 2024.

<https://cyberint.com/blog/research/qilin-ransomware/>

Broadcom. "Qilin ransomware remains an active threat in the landscape" March 27, 2024.

<https://www.broadcom.com/support/security-center/protection-bulletin/qilin-ransomware-remains-an-active-threat-in-the-landscape>

Cook, Victoria. "'Russian criminals' behind hospitals cyber attack." BBC News. June 5, 2024.

<https://www.bbc.com/news/articles/cxee7317kgmo>

Cimpanu, Catalin. "Two of China's largest tech firms are uniting to create a new 'domestic OS'" ZDNet.

December 11, 2019. <https://www.zdnet.com/article/two-of-chinas-largest-tech-firms-are-uniting-to-create-a-new-domestic-os/>

Croft, Daniel. "Victorian court systems allegedly breached by Qilin ransomware gang." Cyber Daily

Australia. January 4, 2024. <https://www.cyberdaily.au/security/9983-victorian-court-systems-allegedly-breached-by-qilin-ransomware-gang>

Hern, Alex. "Who are Qilin, the cybercriminals thought behind the London hospitals hack?" The Guardian.

<https://www.theguardian.com/technology/article/2024/jun/05/who-are-qilin-the-cybercriminals-thought-behind-the-london-hospitals-hack>

Kichatov, Nikolay. "You've been kept in the dark (web): exposing Qilin's RaaS program." Group-IB. May 15,

2023. <https://www.group-ib.com/blog/qilin-ransomware/>

Mohamed Fahmy, Nathaniel Gregory Ragasa, Earle Maui Earnshaw, Bahaa Yamany, Jeffrey Francis

Bonaobra, Jay Yaneza. "New Golang Ransomware Agenda Customizes Attacks." Trend Micro. August 25, 2022. https://www.trendmicro.com/en_us/research/22/h/new-golang-ransomware-agenda-customizes-attacks.html

Nathaniel Gregory Ragasa. "Ransom.Win32.AGENDA.THIAFBB." TrendMicro. November 08, 2022.

<https://www.trendmicro.com/vinfo/hk/threat-encyclopedia/malware/ransom.win32.agenda.thiafbb>

Prof. Geller. "Mythical Creatures: Qilin" Mythology.net. January 17, 2017. <https://mythology.net/mythical-creatures/qilin/>

SalvageData. "Qilin (Agenda) Ransomware: Complete Guide." September 4, 2023.

<https://www.salvagedata.com/qilin-agenda-ransomware/>

SentinelOne. "Agenda (Qilin) Ransomware: In-Depth Analysis, Detection, and Mitigation."

<https://www.sentinelone.com/anthology/agenda-qilin/>

SOCRadar. "Dark Web Profile: Qilin (Agenda) Ransomware." June 6, 2024. <https://socradar.io/dark-web-profile-qilin-agenda-ransomware/>



HC3: Threat Profile

June 18, 2024 TLP:CLEAR Report: 202406181500

VirusTotal. "File submission details for enc.exe." August 22, 2022.

<https://www.virustotal.com/gui/file/93c16c11ffca4ede29338eac53ca9f7c4fbcf68b8ea85ea5ae91a9e00dc77f01>

VirusTotal. "File submission details for decryptor_399060b2.exe." May 28, 2024.

<https://www.virustotal.com/gui/file/54ff98956c3a0a3bc03a5f43d2c801ebcc1255bed644c78bad55d7f7beebd294>

VirusTotal. "File submission details for update.exe." April 2, 2024.

<https://www.virustotal.com/gui/file/9e1f8165ca3265ef0ff2d479370518a5f3f4467cd31a7b4b006011621a2dd752/>

VirusTotal. "File submission details for 31edb01d243e8d989eb7e5aeef54dc.virus." April 20, 2024.

<https://www.virustotal.com/gui/file/e4882b8e8e414e983cf003a5c4038043002a004b63c4f0844a15268332597e80/>

VirusTotal. "File submission details for enc.exe." June 10, 2024.

<https://www.virustotal.com/gui/file/117fc30c25b1f28cd923b530ab9f91a0a818925b0b89b8bc9a7f820a9e630464>

VirusTotal. "File submission details for

555964b2fed3cced4c75a383dd4b3cf02776dae224f4848dcc03510b1de4dbf4.elf." June 11, 2024.

<https://www.virustotal.com/gui/file/555964b2fed3cced4c75a383dd4b3cf02776dae224f4848dcc03510b1de4dbf4>

VirusTotal. "File submission details for 2023-12-15_63b89a42c39b2b56aae433712f96f619_revil." June 11, 2024.

<https://www.virustotal.com/gui/file/bf9fc34ef4734520a1f65c1ec0a91b563bf002ac63982cbd2df10791493e9147/>

VirusTotal. "File submission details for

55ee6bb3deb3385052d7f57e6a48c3c5bba0f558f0d17653908550ffe37e1bea." June 5, 2024.

<https://www.virustotal.com/gui/file/55ee6bb3deb3385052d7f57e6a48c3c5bba0f558f0d17653908550ffe37e1bea/>

VirusTotal. "File submission details for

cd27a31e618fe93df37603e5ece3352a91f27671ee73bdc8ce9ad793cad72a0f." June 11, 2024.

<https://www.virustotal.com/gui/file/cd27a31e618fe93df37603e5ece3352a91f27671ee73bdc8ce9ad793cad72a0f>

VirusTotal. "File submission details for

37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6.exe." June 8, 2024.

<https://www.virustotal.com/gui/file/37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6>



HC3: Threat Profile

June 18, 2024 TLP:CLEAR Report: 202406181500

VirusTotal. "File submission details for c26ce932f3609ecd710a3a1ca7f7b96f1b103a11b49a86e9423e03664eaabd40.dll." March 9, 2024.
<https://www.virustotal.com/gui/file/c26ce932f3609ecd710a3a1ca7f7b96f1b103a11b49a86e9423e03664eaabd40>

VirusTotal. "File submission details for update.exe." April 26, 2024.
<https://www.virustotal.com/gui/file/411b2ed12df1ace6559d3ea666c672617ce23e2ace06806bb53c55bccb83303>

VirusTotal. "File submission details for d67303ba66bcb4dd89de87c83f3f831f.virus." May 16, 2024.
<https://www.virustotal.com/gui/file/8e1eb0ad22236e325387fdb45aea63f318a672c5d035a21d7b3a64eeafb4c5a2>

VirusTotal. "File submission details for 99.dll." June 10, 2024.
<https://www.virustotal.com/gui/file/aa0772fc6784799d59649654879c2b4a23919cda410bede0162751e6d6d6b558>

VirusTotal. "File submission details for inter.exe." April 21, 2024.
<https://www.virustotal.com/gui/file/ebb2a1b46a13c308ffe62dda4d9da316d550433707b2c2a38ad710ea4456c608>

VirusTotal. "File submission details for ceed9fdce420c0558e56bb705664d59f67d62c12d7356ca8643908261638b256." April 15, 2024.
<https://www.virustotal.com/gui/file/ceed9fdce420c0558e56bb705664d59f67d62c12d7356ca8643908261638b256>

VirusTotal. "File submission details for 5e9fc42cf65e1a87e953d00cb2755d3b5b00c1414259534c3a85742295bb6ff9." April 24, 2024.
<https://www.virustotal.com/gui/file/5e9fc42cf65e1a87e953d00cb2755d3b5b00c1414259534c3a85742295bb6ff9>

VirusTotal. "File submission details for BackupsFrst.exe1." April 13, 2024.
<https://www.virustotal.com/gui/file/a25097d2ae808df410c2f35d725a500fb680f38605e62c9e3b619e389ef6733f>

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. [Share Your Feedback](#)