Qilin Ransomware Analysis: Critical TTPs and Defense

By Sıla Özeren Hacıoğlu

Published: 2025-02-14 · Archived: 2026-04-05 23:50:32 UTC

Qilin is a ransomware group that emerged in July 2022 and operates under a Ransomware-as-a-Service (RaaS) model. The group quickly gained notoriety following its high-profile $50 million ransom demand during an assault on Synnovis—a leading pathology services provider—which resulted in significant disruptions across key NHS hospitals in London. Originally an offshoot of the Agenda ransomware (developed in Go), Qilin has evolved into a more robust, Rust-based variant that incorporates advanced techniques in malware construction and evasion.

In this blog, we will analyze the tactics, techniques, and procedures (TTPs) of the Qilin ransomware group, providing detailed insights into their operational evolution, methods of attack, and the potential defense strategies that can help mitigate their impact.

Analyzing Qilin Ransomware's Advanced Tactics, Techniques, and Procedures (TTPs)

This section provides a comprehensive analysis of these TTPs, offering insights into how Qilin Ransomware operates and the tools they employ.

TA0001: Initial Access Methods

Adversaries operating the Qilin ransomware adopt a multi-pronged strategy to breach target networks, relying on both misconfigurations and software vulnerabilities. Their techniques, while tailored to specific environments, echo methods observed in other high-profile ransomware groups, underscoring a broader trend in cyber intrusions.

T1133 External Remote Services

One common approach of Qilin ransomware operators involves targeting remote access services, particularly within Fortinet devices. In many deployments, organizations run firewall clusters with varied software versions—a practice that can inadvertently leave one or more units exposed to known security flaws. Once a FortiGate device is compromised, attackers can exploit its SSL VPN functionality to pivot deeper into the network, often moving laterally to failover servers that maintain connectivity even during service disruptions.

Additionally, brute-force attacks on VPN endpoints are sometimes deployed to gain unauthorized entry, although attackers typically erase log data post-intrusion, complicating forensic validation of these attempts.

T1190 Exploit Public-Facing Application

TL:DR;

- Exploited CVE: CVE-2023-27532
- Affected Product: Veeam Backup & Replication Veeam Cloud Connect
- Description: Vulnerability in Veeam Backup & Replication component allows encrypted credentials stored in the configuration database to be obtained.
- PoC for Exploitation: Publicly Available on Github
- Solution Builds:
    - 12 (build 12.0.0.1420 P20230223)
    - 11a (build 11.0.1.1261 P20230227)

Another known initial access vector used by Qilin involves compromising internet-exposed applications. A pertinent example is the exploitation of the CVE-2023-27532 vulnerability in Veeam Backup & Replication software.

By taking advantage of this security flaw, attackers can retrieve encrypted credentials stored within the configuration database, effectively bypassing standard authentication protocols. This technique not only grants access to the backup infrastructure but also paves the way for broader network compromise.

TA0002: Execution

T1204.002 – User Execution: Malicious File

Upon gaining access to the network, the ransomware payload is systematically deployed to the C:\temp directory, where it is stored under the filename w.exe—a commonly observed tactic used to blend in with legitimate system files.

The ransomware executable is designed to r*equire a specific password*, which is passed as a command-line argument during execution. This password is *subsequently hashed using the SHA-256 cryptographic algorithm*, and the resulting hash is compared against a *pre-defined hash value embedded within the ransomware's configuration*. If the hashes match, the ransomware proceeds with its execution; otherwise, it terminates.

At this point, you might ask: can the password be cracked if it is embedded in the .conf file?

SHA-256 is widely regarded as a robust cryptographic hash function. If the password chosen is sufficiently complex (i.e., has high entropy), then cracking the hash via brute force or dictionary attacks becomes computationally infeasible with current technology. Essentially, the design assumes that any attempt to reverse-engineer or "crack" the hash will be thwarted by the sheer complexity of the password.

Additionally, the ransomware supports optional command-line arguments that can be utilized to activate or modify specific functionalities.

These arguments may include parameters for customizing encryption routines, defining target directories, enabling persistence mechanisms, or configuring communication with a command-and-control (C2) server. This modular design allows the ransomware to adapt its behavior based on the attacker's objectives, making it more versatile and potentially more dangerous.

TA0004: Privilege Escalation

T1078.002 Valid Accounts: Domain Accounts

There are publicly available proofs of concept that demonstrate how to exploit CVE-2023-27532 to gain access to the backup server.

While these exploits have been successfully demonstrated, there is no confirmed evidence that Qilin operators have specifically used the exact exploit linked here.

- A Publicly Known Proof of Concept for CVE-2023-27532

T1134 Access Token Manipulation

Following its initial execution, the ransomware initiates privilege escalation to achieve SYSTEM-level access, a critical step for gaining unrestricted control over the compromised system. This is accomplished through the use of an embedded Mimikatz module, a well-known tool for credential dumping and token manipulation. The module specifically targets critical Windows processes such as

- lsass.exe (Local Security Authority Subsystem Service),
- winlogon.exe (Windows Logon Application), and
- wininit.exe (Windows Initialization Process) to extract user tokens. These tokens, which represent the security context of privileged accounts, are then impersonated or stolen to facilitate the creation of new processes with elevated privileges.

Once the Qilin ransomware successfully acquires the stolen token, it leverages this elevated security context to spawn new processes. This allows the malware to bypass standard user access controls (UAC) and execute malicious operations with the highest level of system authority, such as disabling security software, encrypting files across restricted directories, or establishing persistence mechanisms.

In addition to token manipulation, the Qilin ransomware employs advanced techniques to manipulate symbolic links, a feature of the Windows file system that allows for the redirection of file paths. Specifically, it configures the system to resolve symbolic links for both remote and local objects using the following commands:

fsutil behavior set SymlinkEvaluation R2R:1 (enables remote-to-remote symbolic link resolution)
fsutil behavior set SymlinkEvaluation R2L:1 (enables remote-to-local symbolic link resolution)

This combination of token manipulation and symbolic link exploitation enhances the ransomware's ability to operate stealthily and extend its reach across networked environments, making detection and mitigation more challenging.

TA0005: Defense Evasion

T1070 Indicator Removal

As part of its defense evasion strategy, the Qilin ransomware employs a multi-phase approach to eliminate forensic artifacts and evade detection. Prior to initiating the encryption process, it systematically deletes all system logs to prevent security tools and analysts from identifying its initial execution and lateral movement. Once the

encryption process is complete, the ransomware further erases all system events, targeting critical logs such as Windows PowerShell and Windows System logs. This ensures that traces of its malicious activities, including command execution, process creation, and file modifications, are thoroughly obfuscated.

To maintain persistent stealth, the ransomware operates a separate thread dedicated to periodically cleaning Windows Event Logs. This thread executes a PowerShell command designed to enumerate and clear all event logs with recorded entries.

The command is structured as follows:

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

This script retrieves a list of all event logs with recorded entries (Get-WinEvent -ListLog *), filters them based on their record count, and iteratively clears each log using the EventLogSession.ClearLog method. By leveraging PowerShell's native capabilities, the ransomware ensures comprehensive log removal while minimizing the risk of triggering security alerts associated with the use of external tools.

Note that this technique not only hinders forensic analysis but also disrupts security monitoring systems that rely on event logs for threat detection and incident response.

T1562.001 Impair Defenses: Disable or Modify Tools

Within the Qilin configuration file, the threat actor can specify substrings or regular expressions for process names to be terminated, as well as service names to be stopped or denied.

Key configuration parameters include:

- process_black_list: Substrings of process names targeted for termination.
- win_services_black_list: Substrings/expressions for names of services to be halted or denied.

TA0007: Discovery

T1087.002 Account Discovery: Domain Account

The ransomware employs a systematic approach to enumerate domain-connected hosts as part of its discovery phase.

Initially, it executes a PowerShell script designed to query the Active Directory (AD) for a list of all computers joined to the domain. The script utilizes the Get-ADComputer cmdlet from the ActiveDirectory module, extracting the DNSHostName property of each computer object.

The command is structured as follows:

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

If the initial attempt fails—likely due to the absence of the ActiveDirectory module or insufficient permissions—the ransomware proceeds to install the RSAT-AD-PowerShell module, a prerequisite for executing Active Directory-related cmdlets.

This is achieved through a series of commands designed to install the necessary tools:

"powershell" -Command "ServerManagerCmd.exe -i RSAT-AD-PowerShell ; Install-WindowsFeature RSAT-AD-PowerShell ; Add-WindowsCapability -Online -Name 'RSAT.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0'"

These commands ensure the installation of the Remote Server Administration Tools (RSAT) for Active Directory, enabling the ransomware to leverage PowerShell for AD enumeration. Once the module is successfully installed, the ransomware retries the initial command to compile the list of domain-connected hosts.

This multi-step process demonstrates the ransomware's adaptability and persistence in gathering critical information about the target environment. By enumerating domain-connected hosts, the malware can identify potential targets for lateral movement, privilege escalation, or further exploitation, thereby enhancing its operational effectiveness within the compromised network.

TA0008: Lateral Movement

T1021.002 Remote Services: SMB/Windows Admin Shares

The Qilin ransomware exhibits worm-like propagation capabilities across local networks, activated when the -spread command-line argument is supplied. To facilitate this, it embeds a copy of Sysinternals PsExec (version 2.43) within its payload, which it deploys to the %Temp% directory under a randomly generated filename. This ensures the tool remains undetected by traditional file-based detection mechanisms.

The malware begins by performing domain reconnaissance to identify potential targets. It then leverages PsExec to establish connections to each discovered host using the following command:

%Temp%\<PSEXEC_NAME>.exe -accepteula \\<HOST_IP> -c -f -h -d <LOCKER_PATH> <LOCKER_ARGS> --spread-process

If user credentials are provided, the command is modified to include authentication details:

%Temp%\<PSEXEC_NAME>.exe -accepteula \\<HOST_IP> -u <USER_NAME> -p <PASSWORD> -c -f -h -d <LOCKER_PATH> <LOCKER_ARGS> --spread-process

Parameters:

- PSEXEC_NAME: Randomly generated filename for the embedded PsExec executable.
- HOST_IP: IP address of the target host.
- USER_NAME and PASSWORD: Credentials for authenticating to the target host.

- LOCKER_PATH: Path to the ransomware executable on the local system.
- LOCKER_ARGS: Command-line arguments for launching the ransomware on the remote host.

To optimize its network propagation, Qilin modifies the Windows registry to increase the number of outstanding network requests per client. It sets the MaxMpxCt registry parameter to 65535, enabling the malware to maximize its concurrent connections and accelerate its spread across the network.

In more advanced scenarios, Qilin extends its propagation capabilities by leveraging VMware vCenterfor self-distribution. This is triggered using the following command-line argument:

-spread-vcenter

This allows the ransomware to exploit virtualized environments and further expand its reach.

This multi-faceted approach to lateral movement and propagation underscores Qilin's sophistication, combining traditional tools like PsExec with registry manipulation and virtualization platform exploitation to achieve widespread network compromise.

TA0040: Impact

T1490 Inhibit System Recovery

Within the backup management console, the threat actor performs a series of manual operations to compromise backup integrity:

- Deletes Tape Backups: Erases physical or virtual tape-based backups, effectively removing an essential offline data recovery mechanism.
- Disables Scheduled Backup Jobs: Prevents future automated backups, ensuring that no new recovery points are created.
- Removes Backup Jobs: Eliminates existing configurations that could potentially be re-enabled or restored.

In addition, the malware systematically disrupts the Volume Shadow Copy Service (VSS)—a critical Windows service that maintains point-in-time copies of data—by executing the following command sequence:

```
# Initiates the VSS service if it is not already running.
net start vss

# Changes the startup mode to manual, reducing its resilience against subsequent commands.
wmic service where name='vss' call ChangeStartMode Manual

# Purges all existing shadow copies without prompting for confirmation, effectively erasing historical backup snapshots.
vssadmin.exe Delete Shadows /all /quiet
```

```
# Terminates the VSS service to prevent further operations.
net stop vss

# Permanently disables the service, ensuring that no new shadow copies can be created.
wmic service where name='vss' call ChangeStartMode Disabled
```

This coordinated sequence of actions not only eliminates current backup data but also prevents the creation of new recovery points, significantly hindering any efforts to restore lost data in the event of a security breach.

T1486 Data Encrypted for Impact

After establishing control of the target system, Qilin ransomware initiates a comprehensive encryption process that targets both local files (as defined in its configuration) and all network-shared data. The process begins by encrypting data stored on the host machine as well as any attached drives, including mapped network shares. The encryption is carried out in multiple streams using one of the following cryptographic algorithms:

- AES-256 CTR: Employed when hardware acceleration is available via AES-NI, ensuring efficient processing and robust encryption.
- ChaCha20: Used as an alternative in environments where AES-NI hardware support is not present, providing a high level of security.

To secure the cryptographic material, the encryption keys, nonces, and additional parameters are encrypted using RSA-4096 as specified in the configuration. The resulting RSA-encrypted block is appended to the encrypted file, thereby safeguarding the keys necessary for decryption and making unauthorized recovery extremely challenging.

In some instances, the ransomware may perform multiple encryption passes on the same file—a strategy referred to as "Multipass mode." This mode can operate in different configurations, such as "fast," "per cent," and "normal" modes, further complicating decryption efforts and ensuring that remnants of the original data are thoroughly obfuscated.

After the encryption phase, Qilin ransomware executes a cleanup routine to overwrite free disk space, thereby eliminating any residual data remnants that could potentially aid in recovery attempts. This is achieved using the Windows cipher tool with the command:

```
cipher /w:"X:\"
```

(where X: represents the target disk).

Additionally, the ransomware logs detailed execution data, including the encryption status and process specifics, providing a comprehensive record of the attack's progression for potential forensic analysis.

T1529 System Shutdown/Reboot

As a final disruptive measure, the ransomware initiates a reboot of the backup server following encryption—hindering recovery efforts. In some incidents, the threat actor has also rebooted VPN servers to further disrupt

operations.

How Does Picus Help Against Qilin Ransomware Threat Group?

We also strongly suggest simulating ransomware groups, including Qilin and the rest of the Top 10 Ransomware Groups of 2025**,** to test the effectiveness of your security controls against their attacks using the Picus Security Validation Platform. You can also test your defenses against hundreds of other ransomware variants, such as Phobos, ALPHV, and LockBit, within minutes with a 14-day free trial of the Picus Platform.

Picus Threat Library includes the following threats for Qilin Ransomware**.**

Threat ID	Threat Name	Attack Module
41029	Agenda Ransomware Campaign Variant - 2	Windows Endpoint
55934	Agenda Ransomware Campaign Variant - 1	Windows Endpoint
22877	Qilin Ransomware Download Threat	Network Infiltration
90918	Qilin Ransomware Email Threat	E-mail Infiltration

Defense Strategies Against Qilin Ransomware Attacks

Below are four key defense strategies to help mitigate the threat posed by Qilin ransomware attacks:

Timely Patch Management and Vulnerability Mitigation

Ensure all systems—especially those exposed to public networks—are regularly updated. Patching vulnerabilities in commonly targeted applications (e.g., Fortinet devices or Veeam Backup & Replication software) minimizes entry points for attackers exploiting known CVEs. This proactive approach reduces the risk of initial access through exploited weaknesses.

Deploy Advanced Endpoint Detection and Response (EDR) Solutions

Use EDR and next-generation antivirus tools that monitor for unusual behaviors—such as unauthorized process execution, log clearance, and lateral movement. These solutions can detect the atypical command executions and privilege escalation techniques employed by Qilin ransomware, helping to isolate and remediate compromised endpoints early in the attack chain.

Continuously Test and Validate Security Controls

Enhance your security posture by regularly testing the effectiveness of your prevention and detection controls. Use Breach and Attack Simulation (BAS) solutions, such as the Picus Security Control Validation (SCV) product, to simulate real-world attack scenarios. This continuous validation process reveals control gaps and provides actionable recommendations, ensuring that your defenses remain robust against evolving threats.

Implement Network Segmentation and a Zero Trust Model

Limit lateral movement by segmenting networks and enforcing strict access controls. With a zero trust approach—including multi-factor authentication and least privilege access—if an endpoint is breached, attackers are confined to a limited portion of the network. This containment helps prevent the spread of ransomware across critical systems.

Maintain Regular, Immutable Offline Backups and an Incident Response Plan

Regularly back up critical data using air-gapped or immutable storage that ransomware cannot alter or delete. Coupled with a well-practiced incident response plan (including network isolation procedures), this strategy ensures you can restore systems quickly, even if attackers disable local recovery options like Volume Shadow Copies.

By integrating these layered defenses, organizations can significantly reduce the risk and potential impact of Qilin ransomware attacks.

Conclusion

The Qilin ransomware group continues to prove its disruptive capability by leveraging advanced techniques—from initial access via vulnerable Fortinet devices and exploitation of public-facing applications, through meticulous execution and lateral movement, to the final devastating impact on system recovery and data encryption.

Understanding these detailed techniques is critical for cybersecurity professionals to implement robust defenses and countermeasures. As ransomware threats evolve, continuous vigilance, proactive monitoring, and comprehensive incident response planning are key to protecting critical infrastructure against adversaries like Qilin.
