UNDER EMBARGO UNTIL THURSDAY, OCTOBER 24th AT 9:00 AM ET

New Qilin.B Ransomware Variant Boasts Enhanced Encryption and Defense Evasion

Executive Summary

Researchers at anti-ransomware solutions provider Halcyon have documented a new version of the Qilin ransomware payload dubbed *Qilin.B* for tracking.

According to the *Power Rankings: Ransomware Malicious Quartile* report, Qilin (aka Agenda) is a ransomware-as-a-service (RaaS) operation that emerged in July of 2022 that can target both Windows and Linux systems. Qilin operations include data exfiltration for double extortion.

Key aspects of the new Qilin.B variant include:

- **Enhanced Encryption:** Qilin.B combines *AES-256-CTR* encryption for systems with *AESNI* capabilities while retaining *Chacha20* for other systems, and uses *RSA-4096* with *OAEP* padding to protect encryption keys, making file decryption without the private key or captured seed values impossible.
- **Security Evasion:** Written in *Rust*, Qilin.B terminates services associated with security tools, clears Windows Event Logs to hinder forensic analysis, and deletes itself to reduce traces of its presence, making detection and response or attempts to reverse-engineer the payload more difficult.
- **Corrupting Backups:** Qilin.B disrupts system backup efforts by deleting volume shadow copies (VSS) which thwarts critical recovery mechanisms.

Inside Qilin.B

Qilin.B is a new, more advanced version of the Qilin ransomware family. It builds on previous iterations by incorporating additional encryption capabilities and more sophisticated operational tactics.

Notably, **Qilin.B** now supports **AES-256-CTR** encryption for systems with **AESNI** capabilities, while still retaining **Chacha20** for systems that lack this support. Additionally, **RSA-4096** with **OAEP padding** is used to safeguard encryption keys, making file decryption without the attacker's private key or captured seed values impossible.

Key Features and TTPs

File Encryption & Mechanism

- **Encryption Methods**: Qilin.B uses either **AES-256-CTR** or **Chacha20**, based on system support. The ransomware appends a configurable string to encrypted files, which also serves as a **company_id**. This is used by affiliates to identify and track specific targets.
- **Ransom Notes**: For every directory processed, Qilin.B generates ransom notes titled **"README-RECOVER-[company_id].txt"** containing instructions to access a Tor website for payment details and decryption.

Execution Flow

Once executed with the correct password (e.g., **build1.exe --password [random_password_string]**), Qilin.B performs the following:

1. Verifies administrative privileges.
2. Detects virtual machine environments.
3. Checks for **AESNI** instruction set support.
4. Loads its configuration.
5. Creates a mutex for process exclusivity.
6. Generates an autorun registry entry to ensure persistence.
7. Prioritizes its process and begins terminating critical processes related to security and backup.
   Continuously removes **Windows Event Logs** to evade detection.

Process and Service Termination

Qilin.B terminates or disables services associated with security, backup, and virtualization. The services it targets include those with the following patterns:

- **Examples**: veeam, vss, sql, sophos, acronisagent, sap.

File Selection and Enumeration

Qilin.B uses **GetLogicalDrives()** and **EnumResourceW()** to locate mounted drives and shares for encryption. It also enumerates network folders located in **%APPDATA%\Roaming\Microsoft\Windows\Network Shortcuts** and the **%DESKTOP%** folder.

- **Excluded Directories**: It avoids encryption of critical system directories, including windows, system volume information, intel, netlogon, and program files.

Backup Disruption

Qilin.B disrupts backup operations by deleting **volume shadow copies** using the command:

```
vssadmin delete shadows /all /quiet
```

Defense Evasion

Qilin.B employs several evasion techniques:

- **Log Clearing**: The ransomware clears **Windows Event Logs** to hinder forensic analysis, executed with the following PowerShell command:

```
Get-WinEvent -ListLog * | Where-Object {$_.RecordCount} | ForEach-Object {[System.Diagnostics.Eventing.Reader.EventLogSession]::GlobalSession.ClearLog($_.LogName)}
```

- **Self-Deletion**: After execution, Qilin.B deletes itself to reduce traces of its presence on the system.
- **Rust Compilation**: Being compiled in Rust makes Qilin.B naturally harder to reverse-engineer.

Persistence

Qilin.B maintains persistence by adding the following **AUTORUN** registry entry to ensure it executes upon system reboot:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<rand6char> = "<path>\qilin.exe" --password <password> --no-vm --no-admin
```

System Modifications

Qilin.B modifies system settings to share network drives between elevated and non-elevated processes by adding the following registry entry:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
EnableLinkedConnections = 1

This allows mapped drives to be accessed by processes with different privilege levels.

Indicators of Compromise (IOCs)

Note: these will be unique for each attack and contain compromised user credentials of the target.

File System IOCs:

- **Ransomware Binary**:
  - SHA256: XXXXXXXXXXXXXX [redacted]
- **DLL Payload**:
  - SHA256: XXXXXXXXXXXXXXX [redacted]
- **Ransom Note**:
  - Filename: **"README-RECOVER-[company_id].txt"**
- **Encrypted Files**:
  - File extension: **".[company_id]"** (configurable company name for tracking purposes)

Conclusion

Qilin.B's combination of enhanced encryption mechanisms, effective defense evasion tactics, and persistent disruption of backup systems marks it as a particularly dangerous ransomware variant. By leveraging **AES-256-CTR**, **Chacha20**, and **RSA-4096**, along with advanced anti-forensic techniques, Qilin.B poses a significant threat to enterprise networks. Early detection through process monitoring and identification of IOCs is critical to mitigating its impact.