ultraviolet

THREAT ADVISORY

QILIN UNMASKED? A LOOK AT THE THREAT ACTOR BEHIND THE BRAND

November 12, 2026 **TLP:GREEN**

UltraViolet Cyber TIDE Team
tide@uvcyber.com

DIGGING INTO THE THREAT: QILIN

November 12, 2026 TLP:GREEN UltraViolet Cyber TIDE Team, tide@uvcyber.com

Executive Snapshot

Qilin is a Russia-based ransomware-as-a-service (RaaS) operation that has become one of the most active ransomware affiliate programs in the world, claiming at least 365 victim organizations in just the past three months. Active since September 2022, Qilin runs a double-extortion model, stealing data before encrypting systems and recruiting affiliates with an unusually generous payout of at least 80% of ransom proceeds.

On November 11, 2026, KrebsOnSecurity published an investigation tying Qilin's public-facing administrator persona, "Haise," to Aleksey Mikhailovich Yakovtsev, a 36-year-old man reportedly residing in St. Petersburg, Russia, built from a years-long trail of operational security mistakes across forums, messaging platforms, and leaked records. Because Russia has no extradition cooperation with the US or most Western nations, this identification is unlikely to result in near-term custody, and Qilin should be treated as a continuing, active threat with well-documented post-exploitation tradecraft worth hunting on directly.

Priorities given Qilin's continued activity:

- Ensure your security provider has visibility into credential-theft tooling and the registry changes that often stage it, since this is one of Qilin's most consistent post-exploitation behaviors.
- Watch for a second, unexpected remote-monitoring tool appearing alongside your organization's sanctioned RMM platform.
- Flag BYOVD driver loads and known AV/EDR-killer tooling as high-confidence pre-encryption signals.
- Treat native PowerShell-based log clearing as a meaningful signal in its own right, not background noise.
- Maintain tested, offline backup and recovery capability independent of production environments.

ADVERSARY PROFILE

Qilin

Water Galura / Agenda / GOLD FEATHER / AgendaCrypt

ACTIVE SINCE
2022 (4+ years)

INDUSTRIES
Manufacturing, Healthcare, Education, Government, Construction, Technology, and Financial services.

COUNTRIES
United States, Canada, United Kingdom, France, Germany, Italy, and Spain.

ATTRIBUTION
Russia, financially motivated RaaS operators

MOTIVES
Financial gain, Extortion, Data theft

NOTABLE TTPS

1. Initial access via phishing, exposed applications, and stolen credentials
2. PowerShell account enumeration with on-demand RSAT installation
3. Embedded Mimikatz with UseLogonCredential staging and pass-the-hash
4. Chrome credential harvesting across domain machines
5. Lateral movement with WMI, PsExec, RDP, and SMB
6. Second remote-monitoring tool installed beside the approved RMM
7. BYOVD, AV-killer tools, and PowerShell log clearing before encryption
8. Shadow copy deletion, backup wipe, and encryption

TIDE Team Analysis

Qilin has operated since September 2022 as a Russia-based RaaS platform, and currently stands among the most active ransomware operations being tracked industry-wide. Its structure is standard for the model: a core team maintains the ransomware builder and leak-site infrastructure, while independent affiliates, recruited historically through the Russian cybercrime forum RAMP, conduct the actual intrusions for a steep 80% cut of proceeds. That generous split has drawn in both Russian-speaking and English-speaking affiliates, which helps explain why Qilin-branded intrusions show real variation in specific tradecraft while still converging on a recognizable overall pattern.

A recent KrebsOnSecurity investigation connected the “Haise” persona to Aleksey Mikhailovich Yakovtsev through a multi-year trail of aliases, messaging activity, and leaked personal records, ultimately pointing to a St. Petersburg resident. The reporting is upfront that the attribution is circumstantial and that the named individual could not be reached for comment. For readers interested in exactly how that identification was pieced together, the original KrebsOnSecurity investigation goes into that chain in considerable depth.

Qilin’s post-exploitation behavior is where the actionable detection opportunity lives, since the initial access vector varies by affiliate. Once inside, affiliates commonly enumerate local and domain accounts via PowerShell, and have been observed triggering an on-the-fly RSAT installation specifically to enable AD enumeration when the module isn’t already present on a host. Credential access typically centers on an embedded Mimikatz module, frequently staged by first flipping the UseLogonCredential registry value to force plaintext credentials into memory, followed by pass-the-hash or pass-the-ticket authentication as domain admin. A Chrome-specific credential harvesting script, pulling saved credentials from Chrome’s local storage database across domain machines, was flagged by researchers as a notably novel capability when first observed.

Lateral movement leans on WMI, PowerShell, PsExec, RDP, and SMB, chosen specifically to resemble routine IT administration rather than stand out. Investigators have also repeatedly observed a second, unauthorized remote-monitoring tool (AnyDesk, ScreenConnect, GoToDesk, and others have all appeared) installed alongside whatever RMM platform the victim organization already uses legitimately. Defense evasion includes BYOVD techniques (a vulnerable TPwSav.sys driver was named in one documented case) to impair EDR/AV ahead of encryption, alongside open-source AV-killer tools dark-kill and HRSword.

Before encryption, Qilin affiliates have been observed systematically clearing logs using native PowerShell rather than external tools, specifically to avoid the detection signatures associated with log-wiping utilities. Persistence is established through scheduled tasks and registry run-key or startup-folder entries. Notably, some Qilin encryptor variants require a password passed as a command-line argument to execute, and at least one Linux-based encryptor has been deployed through the Windows Subsystem for Linux rather than as a native Windows binary. Post-encryption, affiliates have deleted shadow copies, disabled or wiped backup infrastructure, and in some cases overwritten free disk space to frustrate forensic recovery.

Why It Matters

Qilin's claim of 365 victims in three months makes it, by volume, one of the most consequential ransomware threats currently active, and that scale existed before this identification and is highly likely to continue after it. Organizations should not treat this week's news as a signal that the threat is resolving; historically, naming an operator has had limited operational effect on a RaaS brand's ability to keep recruiting affiliates and processing ransom payments.

The lack of a meaningful extradition or enforcement pathway between Western law enforcement and Russia is the central reason this matters. Absent a parallel action, such as formal sanctions complicating the group's ability to receive payment, or an infrastructure takedown affecting its leak site and affiliate panel, identification alone does not materially reduce near-term risk. Stakeholders should watch for whether either of those follow-on actions materializes, since that combination has had more real-world impact on similar groups historically than public attribution alone.

More practically, Qilin's post-exploitation pattern gives defenders something concrete to act on regardless of how the group's leadership situation evolves. The specific sequence, PowerShell-driven enumeration, Mimikatz staged via a registry change, a second unauthorized RMM tool, BYOVD and known AV-killer tooling, native log clearing, and password-gated encryptor execution, has recurred consistently enough across documented cases to form a reliable baseline for detection and hunting efforts, independent of which specific affiliate carries out a given intrusion.

Finally, Qilin's willingness to disguise its encryptor under a trusted brand name, and to run a Linux encryptor through WSL rather than a native Windows binary in at least one case, reflects a group actively iterating on evasion rather than running a static playbook. Detection content built against this actor should be revisited periodically rather than treated as a one-time build.

How to Respond

- ☐ Maintain tested, offline backup and recovery capability with access segmented from production credentials, since shadow copy deletion and backup infrastructure tampering are standard parts of Qilin's playbook.
- ☐ Review remote access tooling across your environment to confirm only sanctioned RMM platforms are present, since unauthorized remote access tools have been a consistent signal across multiple documented Qilin intrusions.
- ☐ Harden against credential theft staging techniques, including registry settings that can force plaintext credentials into memory, as a direct countermeasure to Qilin's typical credential access method.
- ☐ Treat BYOVD driver loads and known AV/EDR-killer tool activity (dark-kill, HRSword, or similar) as high-urgency indicators warranting immediate investigation if observed.
- ☐ Watch for formal sanctions or infrastructure action following this week's identification, since that combination, rather than naming alone, has historically had more operational impact on comparable RaaS groups.

What UltraViolet Cyber is Doing

- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity. UltraViolet is also maximizing detection coverage proactively through Equinox.
- Tracking the latest threat actor intelligence, as well as the corresponding impact on industries around the world, through TIDE's Adversary Intelligence platform.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber