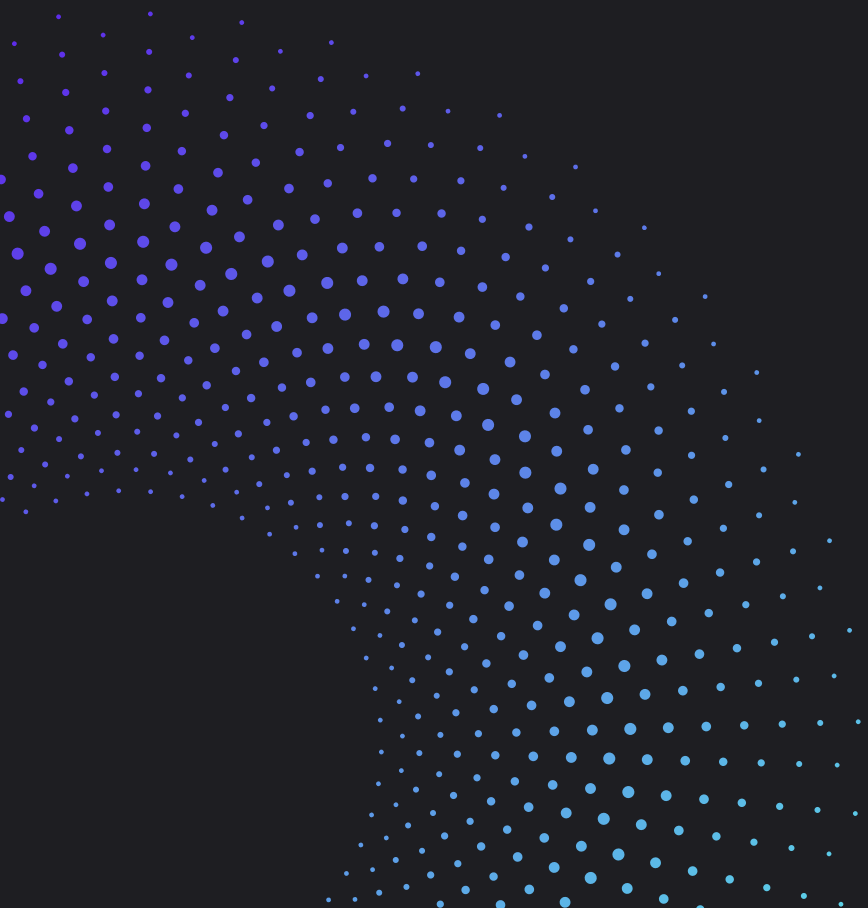
Threat Analysis

Qilin / Agenda

A RaaS collective known for double-extortion attacks on global enterprises, evolving from its original Agenda ransomware into a sophisticated, affiliate-driven threat.



WRAVEN

TABLE OF CONTENTS

Threat Snapshot

First Observed:
July 2022

Operation Type:
Ransomware-as-a-Service (RaaS)

Extortion Method:
Double Extortion:

- Encryption
- Data Exfiltration
- Public Leaks

Targets:
Windows, Linux, VMware ESXI

Payload Languages:
Golang, Rust

Affiliate Split:
80% for ransoms < $3M
85% for > $3M

Analyst Note:
Qilin (formerly “Agenda”) is a financially motivated RaaS operation known for its scalable affiliate network and aggressive double-extortion campaigns. Since its emergence in July 2022, the group has evolved into a versatile and adaptive threat capable of targeting diverse environments and using public data leaks as additional leverage in ransom negotiations.

Description

Threat Overview

Qilin (formerly Agenda) is a Ransomware-as-a-Service (RaaS) collective that emerged in mid-2022 and has since become one of the most active and capable ransomware ecosystems in operation. Initially a smaller operation focused on encrypting enterprise networks, Qilin has evolved into a full-service cybercrime platform offering affiliates custom malware builds, leak site infrastructure, data-hosting services, negotiation support, and even legal assistance tools to increase pressure on victims.

The group leverages Golang and Rust to build highly portable payloads that run across Windows, Linux, and VMware ESXi environments, with configurable encryption modes that can selectively target files, directories, or entire systems. Its operations follow a consistent cycle: compromise, lateral movement, data theft, encryption, and extortion. Unlike many RaaS competitors, Qilin supplements its campaigns with public exposure tactics, including leak site publications, press outreach, and “naming and shaming” strategies designed to intensify ransom negotiations.

Recent reporting shows a sharp increase in Qilin’s activity through 2025. It accounted for nearly 24% of ransomware incidents targeting U.S. state and local government entities in Q2, claimed the top spot in June with roughly 86 confirmed victims, and has been linked to several high-impact breaches, including the New Orleans Sheriff’s Office (842 GB of stolen data offered for sale) and the Synnovis/NHS compromise that exposed over 300 million patient interaction records.

Operational Insights

Initial Access: Affiliates typically enter networks through phishing campaigns, stolen credentials, or exploitation of exposed services such as RDP and Citrix. Qilin has also exploited vulnerabilities like CVE-2023-27532 in Veeam Backup to harvest credentials and move laterally.

Post-Compromise: Once inside, attackers perform reconnaissance, escalate privileges, and move laterally, often tailoring their behavior to the target’s environment. Staging of sensitive data for exfiltration is a standard step before encryption begins.

Description

Extortion Tactics: Qilin practices double extortion, encrypting systems while simultaneously exfiltrating and threatening to publish sensitive data. Victims are listed on a Tor-based leak site, and affiliates can use built-in negotiation tools — including a "Call Lawyer" feature — to apply additional pressure.

Ecosystem Model: The RaaS platform is designed to maximize affiliate participation. Qilin retains a 15–20% cut of ransom profits while affiliates keep the remainder. As rival groups like RansomHub have dissolved, Qilin has absorbed many of their operators and expanded its reach through aggressive recruitment on underground forums.

Adaptation and Evolution: The group continuously updates its infrastructure and tooling, adding capabilities like DDoS attacks, automated negotiation scripts, and spam campaigns. Payloads are frequently customized per victim, complicating detection and response.

INITIAL ACCESS

Affiliates gain entry through phishing, stolen credentials, or exploitation of exposed services such as RDP, Citrix, or Veeam vulnerabilities (e.g., CVE-2023-27532). These footholds often go undetected for weeks.

POST-COMPROMISE

Once inside, operators perform reconnaissance, escalate privileges, and move laterally. Their behavior is tailored to the target environment, with sensitive data staged for exfiltration before the next phase.

EXTORTION TACTICS

Qilin practices double extortion: encrypting systems while simultaneously exfiltrating sensitive data. Victims are listed on a Tor-based leak site, and affiliates use built-in negotiation tools like the "Call Lawyer" feature to apply pressure.

ECOSYSTEM MODEL

The RaaS platform maximizes affiliate participation. Qilin keeps 15–20% of ransom profits, with the rest going to affiliates. As groups like RansomHub dissolved, Qilin absorbed their operators, growing its reach and operational tempo.

ADAPTATION & EVOLUTION

Qilin's tooling evolves continuously: new capabilities include DDoS attacks, automated negotiation scripts, and spam delivery systems. Payloads are often customized per victim, complicating detection, forensics, and incident response.

Associations

Aliases / Rebrands:

Agenda → Qilin (rebrand initiated ~ Sept 2022)
GOLD FEATHER (name used by Secureworks for Qilin operations)
Phantom Mantis (alternate alias found in some threat reports)

Affiliate Ecosystem & Migrations:

After RansomHub's collapse, many of its affiliates reportedly migrated to Qilin.

ransomhub:~#

Qilin actively recruits affiliates via Russian-language underground forums, offering 80–85% revenue share to pull in high-value operators.

Suspected Collaborators:

Scattered Spider is occasionally cited as a collaborator or affiliate in some 2025 writeups (but lacking strong attribution)

Tool / Infrastructure Associations:

Use of SmokeLoader and NETXLOADER in various campaigns as delivery or staging tools.

Frequent exploitation of Fortinet, Citrix, and VMware ESXi vulnerabilities by affiliates aligns with Qilin operational patterns.

Exploited Vulnerabilities

CVE-2024-21762
Fortinet FortiOS / FortiProxy

Authentication bypass leading to remote code execution. Qilin affiliates use this to breach perimeter appliances and gain initial access before pivoting internally.

Initial Access | Perimeter | RCE

CVE-2024-47575
Fortinet FortiManager

Unauthenticated access flaw enabling attackers to push malicious configurations or scripts to managed devices. Frequently exploited as a second-stage escalation point.

Privilege Escalation | Management Plane

CVE-2023-27532
Veeam Backup & Replication

Credential extraction vulnerability abused to access backup infrastructure, disable recovery points, and pivot to hypervisors and storage systems before deployment of ransomware.

Credential Access | Backup Infra

CVE-2025-22224
VMware ESXi / Workstation

A time-of-check/time-of-use (TOCTOU) race condition leading to an out-of-bounds write. Exploitable by a local admin within a VM to execute code as the VMX process on the host.

Privilege Escalation | VM Escape

CVE-2025-22225
VMware ESXi

Arbitrary write vulnerability allowing a malicious actor with VMX process privileges to write outside intended memory bounds. Exploitation can lead to hypervisor-level privilege escalation.

Lateral Movement | Hypervisor

CVE-2025-22226
VMware ESXi / Workstation / Fusion

Out-of-bounds read in the Host-Guest File System (HGFS) component. Allows an attacker with admin privileges inside a VM to leak sensitive memory contents from the VMX process.

Information Disclosure | Post-Exploitation

Analyst Note:

Qilin’s operations show a clear pattern of exploiting edge devices, backup systems, and virtualization layers as entry points or pivot stages. These vulnerabilities often appear in widely deployed, internet-facing infrastructure, meaning patch delays can quickly become high-impact compromises.

The group also leverages post-exploitation flaws like VM escape or memory disclosure to deepen access once inside, often combining multiple CVEs in the same intrusion chain. Because affiliates frequently adapt to newly published exploits, timely patching, continuous vulnerability scanning, and strict segmentation around hypervisors and backup systems are critical defenses.

Indicators of Compromise

Leak/Blog Sites:

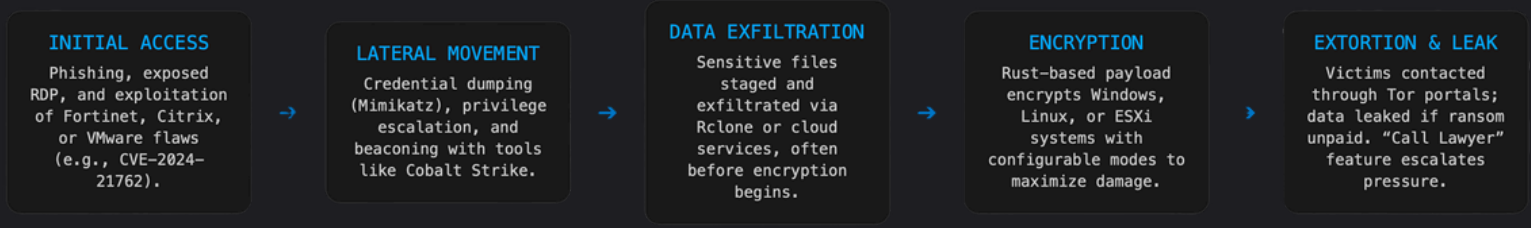
hxxp://kbsqoivihgdmwczmxkbovk7ss2dcynitwhhfu5yw725dboqo5kthfaad[.]onion/
hxxp://ozsxj4hwxub7gio347ac7tyqqozvfioty37skqilzo2oqfs4cw2mgtyd[.]onion/
hxxp://ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd[.]onion/

Tools & Tradecraft:

Credential Access: Mimikatz
Remote Access: AnyDesk
Delivery: CountLoader, Cobalt Strike, commodity RATs
Exfiltration: Rclone
Evasion: Kernel driver tampering, Safe Mode execution, log deletion

Exploited Vulnerabilities:

- CVE-2024-21762 – Fortinet FortiOS / FortiProxy
- CVE-2024-47575 – Fortinet FortiManager
- CVE-2024-55591 – VMware ESXi
- RDP brute-force and phishing campaigns are also frequently observed.



Indicators of Compromise

Host & Behavioral Artifacts:

Windows:

C:\ProgramData\Agenda\payload.exe – payload path
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Agenda – persistence key
Global\AgendaLock – mutex
Scheduled Task: Backup_Sync_Service

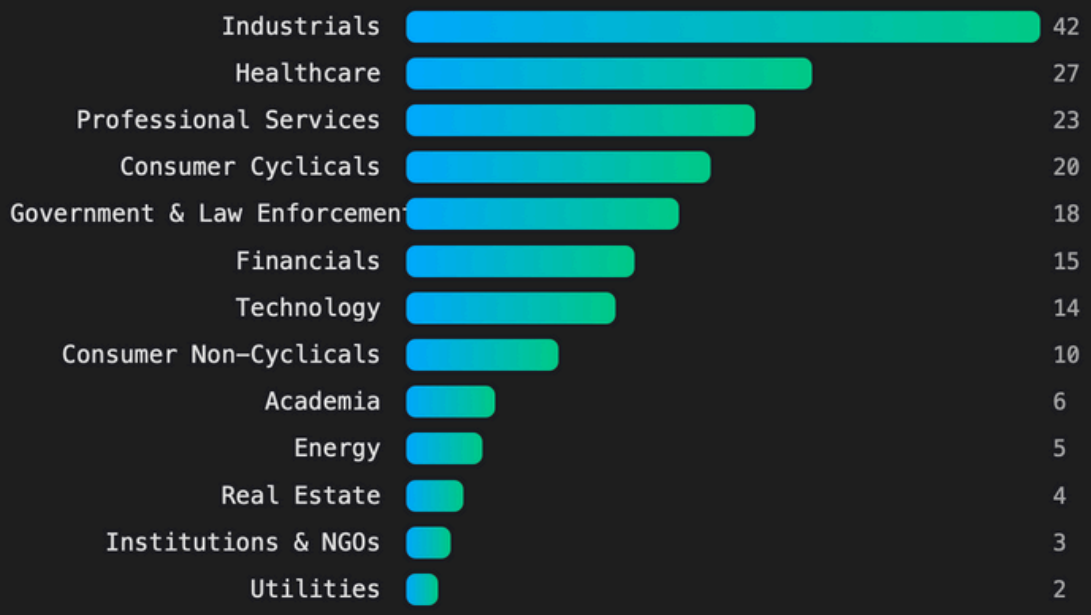
Linux / ESXi:

/etc/cron.daily/qilin_sync.sh – persistence
Rclone binary present under /usr/bin/ or /tmp/

Analyst Note:

Hashes can confirm a specific sample for Qilin, but they’re not very useful long-term. Qilin affiliates often recompile payloads, so hashes change constantly. Use them for quick triage, but rely more on behavior and infrastructure indicators.

Past Targets



Based on publicly reported incidents, leak site data, and observed activity (Jan 2024 – Sep 2025)

⚠ Regional Impact: Michigan

Victim: Saginaw Chippewa Indian Tribe of Michigan

Date: October 2, 2025

Data Exfiltrated: ~886,393 files (~331 GB)

Summary: Qilin claimed responsibility for a large-scale ransomware attack targeting the tribal government and its affiliated enterprises, exfiltrating hundreds of thousands of sensitive files. The breach demonstrates that ransomware operations are not limited to national targets, smaller organizations, regional governments, and tribal entities are now firmly within Qilin's scope.

Why It Matters: This attack highlights the tangible risk ransomware poses to Michigan-based institutions. It underscores a broader trend of ransomware actors pursuing high-impact but lower-visibility victims in the Midwest, where limited cybersecurity resources make successful extortion more likely.

Dark Web Presence

Overview:

Qilin's operations are tightly linked to a well-maintained dark web ecosystem that supports every stage of their ransomware-as-a-service (RaaS) model. From affiliate onboarding and victim negotiations to data publishing and reputation-building, their infrastructure is designed to scale and stay online, even under takedown pressure.

The group uses redundancy heavily, maintaining multiple leak sites, mirrors, and communication endpoints to ensure continuity. These services also serve as a marketing pipeline to attract new affiliates and intimidate victims.

Primary Leak Site

hxxp://ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd[.]onion/

Dark Web Presence

Dark & Grey Sites:

hxxp://kbsqoivihgdmwczmxkbovk7ss2dcynitwhhfu5yw725dboqo5kthfaad[.]onion/ - INACTIVE
hxxp://ozsxj4hwxub7gio347ac7tyqqozvfioty37skqilzo2oqfs4cw2mgtyd[.]onion/ - INACTIVE

Main Leak Site:
hxxp://ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd[.]onion/ - ACTIVE

Jabber/Coms Endpoint:
hxxp://exploit[.]im/ (qilin@exploit[.]im) - ACTIVE

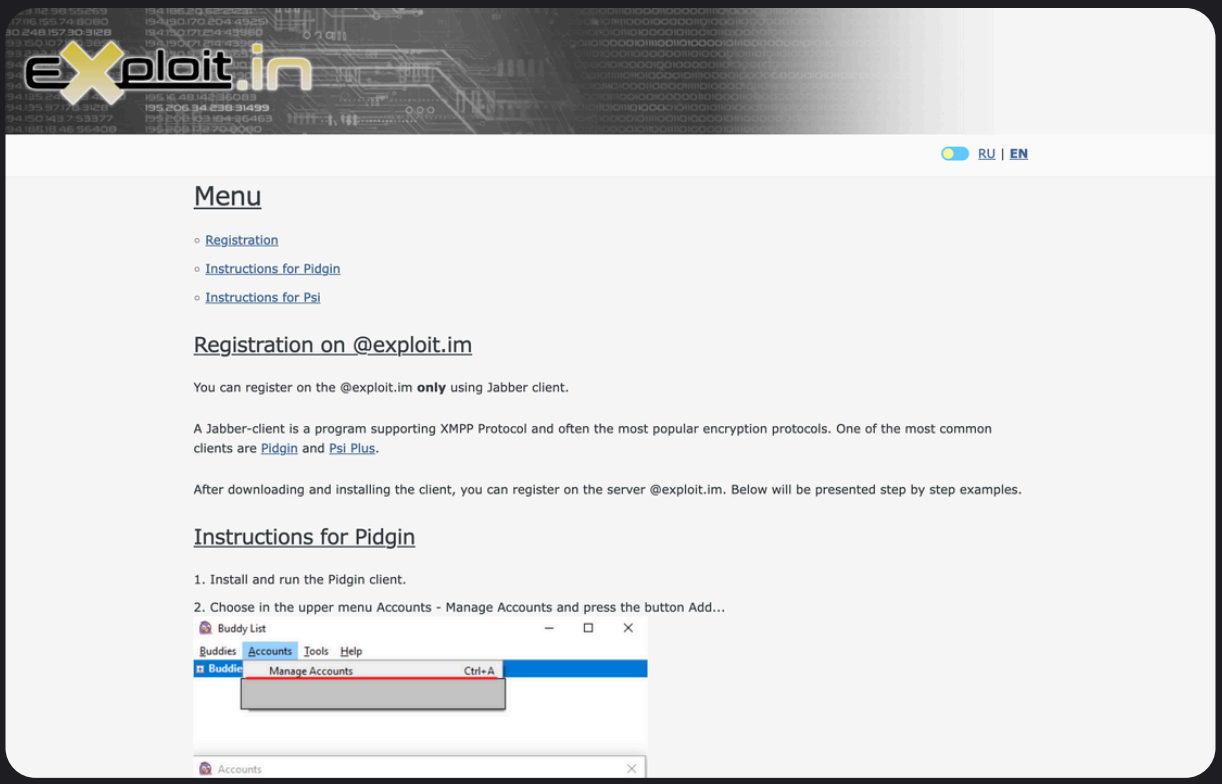
Known Communication Channels:

jabber: qilin@exploit[.]im

TOX: 7C35408411AEEBD53CDBCEBAB167D7B22F1E66614E89DFCB62EE835416F60E1BCD6995152B68

ftp://datashare:ENqh0jBHKia2L22fxzivbhRL@64[.]176[.]162[.]76

Jabber Portal



hxxp://exploit[.]im

ATT&CK Mappings

INITIAL ACCESS

T1190 Exploit Public-Facing Application Confirmed
Fortinet/Citrix edge exploits; ESXi/VMware exposure used to establish footholds.

T1566.001 Phishing: Attachment Reported
Phish with loaders (e.g., CountLoader) and macro documents to stage beacons.

T1133 External Remote Services (RDP/SSH/VPN) Reported
Use of exposed/weak RDP and VPN portals to enter environments.

T1078 Valid Accounts Reported
Re-use of stolen creds from backup systems and edge devices.

EXECUTION

T1059.001 PowerShell Reported
Scripting for staging, discovery, and pre-encryption prep.

T1059.003 Windows Command Shell Reported
Batch/cmd for tool deployment and environment changes.

T1047 Windows Management Instrumentation Likely
Remote exec and admin tasks during staging (varies by affiliate).

PERSISTENCE

T1547.001 Registry Run Keys / Startup Folder Reported
Run keys observed in Windows hosts to auto-start payloads.

T1053.005 Scheduled Task/Job (Windows Task) Reported
Scheduled jobs ensure post-reboot execution and timing of encryption.

T1219 Remote Access Software (AnyDesk) Confirmed
AnyDesk installed for persistence and hands-on-keyboard access.

PRIVILEGE ESCALATION

T1068 Exploitation for Privilege Escalation Confirmed
VMware/ESXi vulnerabilities (e.g., 2025 VMX flaws) leveraged to escalate.

T1078 Valid Accounts Reported
Use of domain/admin creds dumped from backup or AD infrastructure.

DEFENSE EVASION

T1562 Impair Defenses Confirmed
Disabling AV/EDR, safe-mode encryption, and service tampering prior to impact.

T1112 Modify Registry Reported
Changes to policy/services to weaken defenses or persist.

T1036 Masquerading Likely
Renaming tools and living-off-the-land binaries to blend with admin activity.

CREDENTIAL ACCESS

T1003 OS Credential Dumping (Mimikatz) Confirmed
LSASS dumping and token extraction for lateral movement.

T1552.001 Credentials in Files (Veeam DB) Confirmed
Extraction of stored creds from Veeam configuration to reach hypervisors/file servers.

Confidence guide — Confirmed = repeatedly observed in incidents; Reported = cited by multiple sources or artifacts; Likely = consistent with tooling/behavior but less directly observed.

ATT&CK Mappings

DISCOVERY

T1082 System Information Discovery Reported
Host profiling pre-encryption to scope targets and exclusions.

T1046 Network Service Scanning Reported
Enumerating shares, hypervisors, and management planes.

T1018 Remote System Discovery Reported
Identifying reachable servers and AD topology.

LATERAL MOVEMENT

T1021.001 Remote Services: SMB/ADMIN$ Reported
Copy & service-based execution over shares.

T1021.002 Remote Services: RDP Reported
Interactive spread with stolen admin creds.

T1021.004 Remote Services: SSH Reported
Laterals into Linux/ESXi management nodes.

COLLECTION

T1074.001 Data Staged: Local Reported
Stage archives before exfil; selective targeting to speed encryption.

T1039 Data from Network Shared Drive Reported
Sweep of shared directories and NAS prior to impact.

EXFILTRATION

T1567.002 Exfiltration to Cloud Storage (Rclone) Confirmed
Bulk data to cloud providers via Rclone; staging paths observed across campaigns.

T1048 Exfiltration Over Alternative Protocol (FTP) Confirmed
Direct FTP exfil endpoints observed (e.g., exposed FTP URLs in victim listings).

COMMAND & CONTROL

T1071.001 Application Layer Protocol: Web (HTTPS) Reported
Cobalt Strike beacons / loaders communicating over HTTPS.

T1573 Encrypted Channel Reported
TLS/obfuscated comms for C2 and staging.

T1219 Remote Access Software (AnyDesk) Confirmed
Operator hands-on-keyboard control during intrusion/negotiation.

T1105 Ingress Tool Transfer Reported
Pulling tooling from external servers to victim hosts.

IMPACT

T1486 Data Encrypted for Impact Confirmed
Cross-platform encryptors (Windows/Linux/ESXi) with configurable modes.

T1490 Inhibit System Recovery Reported
Shadow copy deletion, backup tamper, safe-mode execution prior to impact.

Confidence guide — Confirmed = repeatedly observed in incidents; Reported = cited by multiple sources or artifacts; Likely = consistent with tooling/behavior but less directly observed.

Known Tools / Programs

Qilin / Qilin.B (Rust & Golang ransomware binaries)
The ransomware families themselves; cross-platform builds for Windows, Linux, and ESXi that perform encryption and extortion.

Rclone:
Widely used for stealthy staging and exfiltration of large datasets to cloud or remote storage

Mimikatz:
Credential-dumping tool used to harvest account credentials from LSASS memory for lateral movement and privilege escalation.

AnyDesk:
Legitimate remote-access software abused to maintain interactive, hands-on access during intrusions.

Cobalt Strike (beacons / tooling):
Commercial post-exploit framework frequently used as a C2/backdoor for lateral movement and payload delivery.

CountLoader / SmokeLoader / NETXLOADER (malware loaders):
Loader families used to deliver Cobalt Strike, RATs, and other secondary payloads into compromised environments.

U.S. Department of Health and Human Services, Health Sector Cybersecurity Coordination Center (HC3).
Qilin (aka Agenda) Threat Profile. June 18, 2024.
https://www.hhs.gov/sites/default/files/qilin-threat-profile-tlpclear.pdf
Source: HHS.gov
Cybersecurity & Infrastructure Protection, State of New Jersey (Cyber NJ).
Ransomware Group Exploits Fortinet Vulnerabilities in Attacks. June 12, 2025.
https://www.cyber.nj.gov/Home/Components/News/News/1723/214
Source: cyber.nj.gov
HIPAA Journal.
Qilin Ransomware Group Exploiting Critical Fortinet Flaws. June 11, 2025.
https://www.hipaajournal.com/qilin-ransomware-group-exploiting-critical-fortinet-flaws/
Source: HIPAA Journal
Canadian Centre for Cyber Security.
Compromise and Persistent Access of Fortinet FortiOS Products (CVE-2022-42475, CVE-2023-27997, CVE-2024-21762). April 14, 2025.
https://www.cyber.gc.ca/en/alerts-advisories/compromise-persistent-access-fortinet-fortios-products-cve-2022-42475-cve-2023-27997-cve-2024-21762
Source: Canadian Centre for Cyber Security
SC Media (Security Content / CISO Stories).
New Qilin Ransomware Attacks Involve Fortinet Exploits. June 9, 2025.
https://www.scworld.com/brief/new-qilin-ransomware-attacks-involve-fortinet-exploits
Source: SC Media
Axios.
Hackers Start Leaking New Orleans Sheriff Ransomware Data. September 15, 2025.
https://www.axios.com/2025/09/15/new-orleans-sheriff-ransomware-attack-data-leak
Source: Axios
Orleans Parish Office of Inspector General (Louisiana).
OPSO Employee Says Cyberattack Led to “Substantial” Data Loss. September 2025.
https://nolaoig.gov/opso-employee-says-cyberattack-led-to-substantial-data-loss/
Source: nolaoig.gov
SOCRadar.
CVE-2024-21762 — Out-of-Bounds Write Vulnerability in Fortinet FortiOS / FortiProxy. CVE Detail Page.
https://socradar.io/labs/app/cve-radar/CVE-2024-21762
Source: SOCRadar