Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

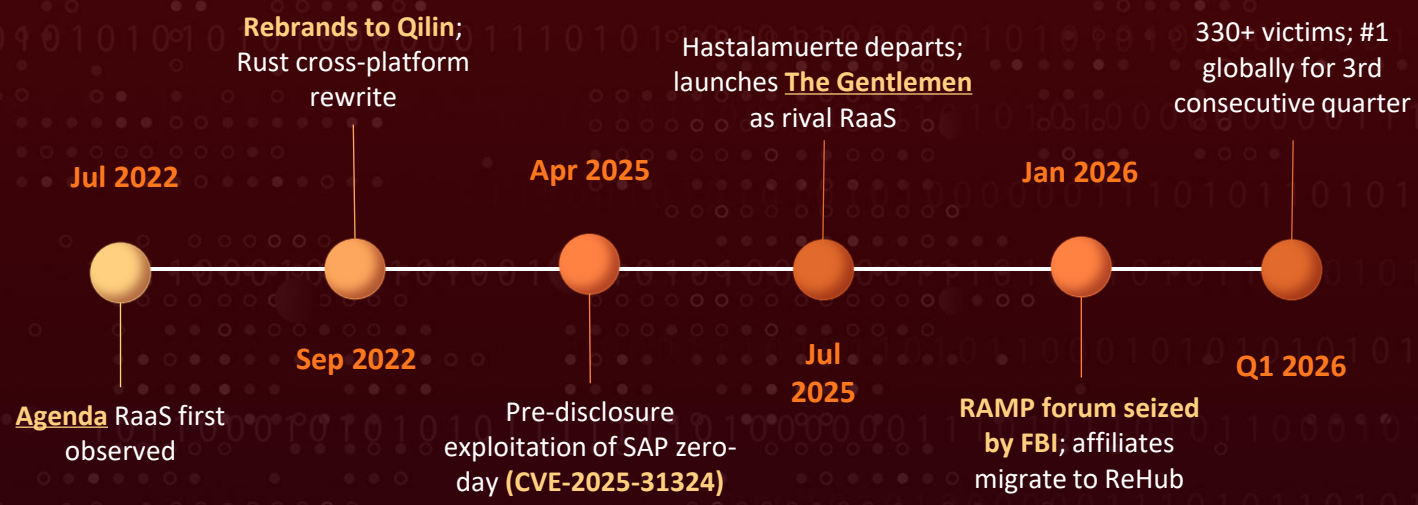
Qilin Rising: Continued Global Dominance and Expanded Tradecraft

Date of Publication	Admiralty Code	TA Number
June 4, 2026	A1	TA2026155

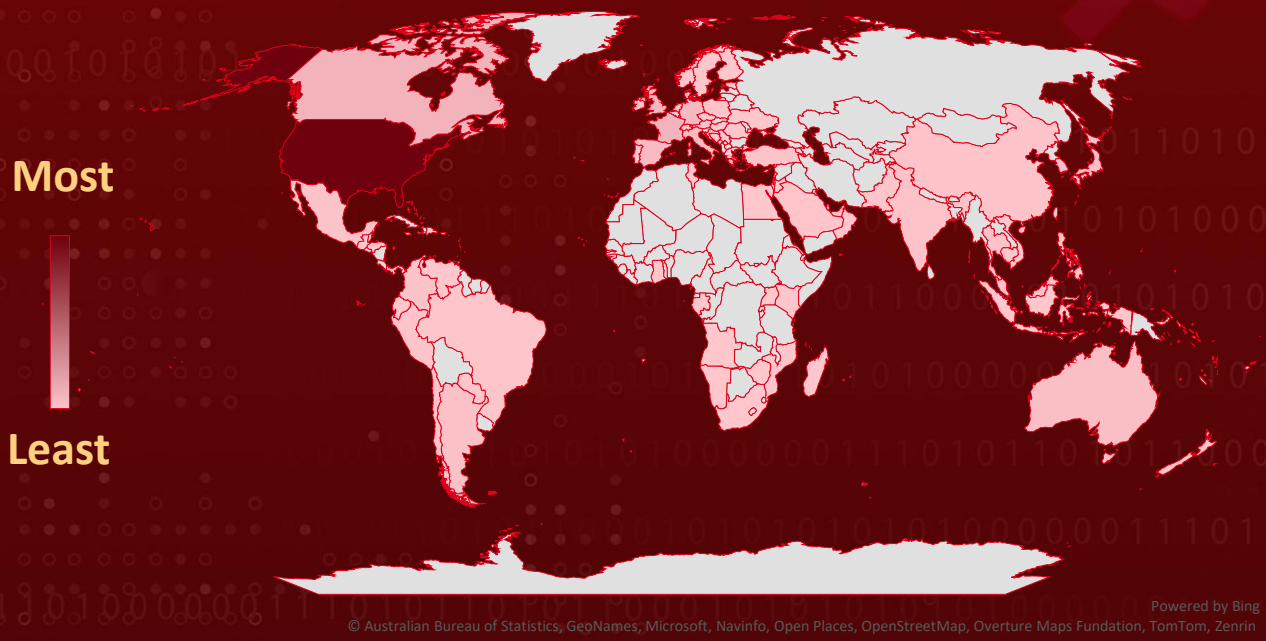
Summary

First Active: July 2022
Targeted Regions: Global (Except CIS countries)
Targeted Platforms: Windows, Linux, and VMware ESXi
Targeted Industries: Business Services & Consulting, Manufacturing, Healthcare, Retail, Financial Services, Legal, Real Estate, Technology, Government, Education, Hospitality, Transportation, Food Service, Agriculture, Insurance, Media, Associations, Energy, Charitable Organizations
Malware: Qilin Ransomware (aka Agenda, Water Galura, Phantom Mantis, Gold Feather)
Attack: Qilin remains the world's most active ransomware operation, holding the top global ranking for three consecutive quarters through Q1 2026 with over 1800 cumulative victims by late May 2026. The group has matured into a triple-extortion model adding DDoS and a "Call Lawyer" negotiation feature, demonstrated zero-day capability by exploiting SAP NetWeaver via CVE-2025-31324 three weeks before public disclosure, and weathered the departure of top affiliate "Hastalamuerte" who launched the breakaway group The Gentlemen. Law-enforcement actions including the RAMP forum seizure have introduced friction without slowing recruitment.

Ransomware Timeline



Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-55591	Fortinet FortiOS Authorization Bypass Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2024-21762	Fortinet FortiOS SSL-VPN Out-of-Bounds Write Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2023-27532	Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication Cloud Connect	✗	✓	✓
CVE-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver Visual Composer	✓	✓	✓

Attack Details

#1

Qilin has solidified its position as the most active ransomware operation in the world, holding the top global ranking for three consecutive quarters through Q1 2026 with over 330 leak-site victims, a figure exceeding the combined output of the bottom fifty groups, and a cumulative count of over 1,800 by late May 2026. This dominance has been driven by the broader consolidation of the ransomware ecosystem, where the top ten groups now claim roughly 71% of all victims, a sharp reversal from the fragmented landscape of 2025. Qilin has been the principal beneficiary of this consolidation, absorbing displaced affiliates following the disruption of BlackSuit, 8Base, and weakened mid-tier operators, and maintaining operational consistency in negotiations and decryption to preserve its standing across the affiliate economy.

#2

A significant structural event occurred in July 2025 when "Hastalamuerte," Qilin's most prolific affiliate and a veteran operator previously associated with Embargo, LockBit, and Medusa, departed the program following a public payment dispute on the RAMP underground forum. Hastalamuerte subsequently launched The Gentlemen as an independent RaaS brand, taking with him an inventory of approximately 14,700 pre-compromised FortiGate devices and roughly 20 experienced operators. Despite this loss, Qilin has retained its market position by continuing to recruit displaced affiliates from disrupted programs and refining its locker tooling, demonstrating the resilience of its core infrastructure and brand reputation.

#3

Qilin's extortion model has matured from double-extortion into a fully developed triple-extortion framework. In addition to file encryption and data leakage, affiliates now routinely deploy DDoS attacks against the victim's remaining infrastructure to sustain operational pressure during negotiations. The negotiation panel has also been enhanced with a "Call Lawyer" feature that connects victims directly with legal consultants positioned to push for rapid settlement, exploiting regulatory disclosure pressure and legal liability concerns as additional coercion levers. These developments mark a deliberate shift toward professionalized, multi-vector extortion rather than pure ransomware deployment.

#4

Affiliate operations have been disrupted by significant law-enforcement actions affecting the broader Russian-speaking ransomware ecosystem. The RAMP underground forum, historically Qilin's primary recruitment and coordination platform, was seized by the FBI in January 2026, with affiliate activity migrating to ReHub and other successor platforms. While these actions have introduced friction, Qilin's affiliate inflow has continued largely uninterrupted, with new affiliates onboarding through successor forums and private referral channels.

#5

Qilin operators have refined their evasion tradecraft with the increasing adoption of Windows Subsystem for Linux (WSL) for executing components from a Linux runtime context on Windows hosts, a technique that deliberately evades endpoint detection tools lacking WSL visibility. Initial access has also expanded to include exploitation of zero-day and known vulnerabilities in public-facing applications. Affiliates have also expanded credential-harvesting capabilities, particularly Chrome credential-extraction routines that target browser-stored credentials for SaaS platforms, OWA, and Microsoft 365, enabling rapid pivot from on-premises compromise to cloud and email environments.

#6

Lateral movement has been streamlined through the embedded deployment of a signed Sysinternals PsExec binary contained directly within the Qilin encryptor itself. Once initial reconnaissance via PowerShell Active Directory enumeration (Get-ADComputer, Test-Connection) identifies domain-joined hosts, the embedded PsExec is dropped to disk and used to push the ransomware payload to every reachable system using harvested credentials. This embedded deployment model reduces dependence on external tool transfer, shortens the dwell-to-encryption window, and complicates detection that relies on identifying standalone admin-tool downloads.

#7

Given Qilin's sustained dominance, professionalized affiliate management, triple-extortion model, and continued tradecraft evolution, organizations should treat the group as a top-tier threat through 2026. Defensive priorities should now include extending EDR coverage to WSL environments, monitoring for embedded PsExec execution patterns originating from non-administrative source processes, deploying behavioral detection over signature-based controls given Qilin's heavy use of signed binaries and living-off-the-land techniques, segmenting Active Directory and ESXi management networks, and reviewing incident response playbooks to account for DDoS pressure and legal-channel coercion during active negotiations.

Recommendations

Patch Internet-Facing Services: Prioritize timely patching of FortiGate appliances (CVE-2024-21762, CVE-2024-55591), SAP NetWeaver Visual Composer (CVE-2025-31324), Veeam Backup & Replication (CVE-2023-27532), and all exposed VPN, RDP, and remote-access infrastructure. Qilin affiliates rely heavily on exploitation of edge-facing CVEs and stolen credentials for initial access, and have demonstrated capability to exploit zero-day vulnerabilities prior to public disclosure.

Enforce Phishing-Resistant MFA on All Remote Access: Apply hardware-based or FIDO2 MFA across VPNs, RDP gateways, OWA/Microsoft 365, and all privileged accounts. Qilin affiliates routinely reuse credentials harvested from infostealer logs and Chrome credential extraction, and unprotected remote-access services remain the most exploited initial access vector.

Harden and Monitor Active Directory: Treat Domain Controllers as the crown jewel of the Qilin kill chain, since the group's embedded PsExec deployment relies on AD-joined host enumeration via Get-ADComputer and Test-Connection. Restrict interactive and network logons on DCs, monitor for unusual ADMIN$ writes, abnormal RPC-launched binaries, and bulk PowerShell Active Directory enumeration originating from non-administrative source hosts.

Extend EDR Coverage to WSL and Hybrid Environments: Qilin affiliates leverage Windows Subsystem for Linux (WSL) and legitimate remote management tools like AnyDesk, ScreenConnect, and Splashtop to deploy Linux ransomware variants on Windows hosts, deliberately evading endpoint detection tools that lack WSL or cross-platform visibility. Ensure EDR platforms have explicit WSL telemetry coverage, restrict remote management utilities to approved administrators, and correlate endpoint and network telemetry for faster detection of cross-platform lateral movement.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a Qilin ransomware attack, up-to-date backups enable recovery without paying the ransom.

Prepare for Triple-Extortion Pressure: Qilin's negotiation playbook now includes DDoS attacks and lawyer-mediated settlement pressure in addition to data leakage. Update incident response playbooks to account for these vectors, pre-coordinate with DDoS mitigation providers, brief legal and communications teams on regulatory disclosure pressure tactics, and rehearse decision-making under multi-vector coercion scenarios.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1078: Valid Accounts	
	T1133: External Remote Services	
	T1190: Exploit Public-Facing Application	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
	T1110: Brute Force	T1110.003: Password Spraying
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1569: System Services	T1569.002: Service Execution
	T1106: Native API	
	T1204: User Execution	T1204.002: Malicious File
	T1072: Software Deployment Tools	
Persistence	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1037: Boot or Logon Initialization Scripts	T1037.004: RC Scripts
Privilege Escalation	T1068: Exploitation for Privilege Escalation	

Tactic	Technique	Sub-technique
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
	T1027: Obfuscated Files or Information	
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1497: Virtualization/Sandbox Evasion	
	T1480: Execution Guardrails	
	T1112: Modify Registry	
	T1218: System Binary Proxy Execution	
Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
Discovery	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1046: Network Service Discovery	
	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.002: Domain Account
	T1135: Network Share Discovery	
	T1482: Domain Trust Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1016: System Network Configuration Discovery	

Tactic	Technique	Sub-technique
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
		T1021.004: SSH
		T1021.006: Windows Remote Management
	T1570: Lateral Tool Transfer	
	T1080: Taint Shared Content	
Collection	T1005: Data from Local System	
	T1039: Data from Network Shared Drive	
	T1074: Data Staged	T1074.001: Local Data Staging
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	T1090.003: Multi-hop Proxy
	T1105: Ingress Tool Transfer	
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
	T1219: Remote Access Software	
Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
Impact	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1489: Service Stop	
	T1491: Defacement	T1491.001: Internal Defacement
	T1485: Data Destruction	
	T1498: Network Denial of Service	
	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	68[.]65[.]122[.]246, 104[.]21[.]63[.]167, 184[.]174[.]96[.]74, 184[.]174[.]96[.]67, 180[.]131[.]145[.]73, 88[.]119[.]174[.]107, 177[.]54[.]223[.]24, 176[.]113[.]115[.]209, 176[.]113[.]115[.]97, 188[.]119[.]66[.]189, 31[.]41[.]244[.]100, 85[.]209[.]11[.]49
SHA256	A51C8FCDE0BCC9FE8273F99C8B23E63CA4CD0F66B22CADD0BCB0F3ADB0FA05FA, A4E3F6633F3ECECD39F0BA8C9644962BB0DD677EE0ECF22A99986D5C80E34BD7, 1306A6B3D73CD4DDE97DC3D6407AE783A91C5F312AE77E5CF88674FC99C7CAF0, e90bdaaf5f9ca900133b699f18e4062562148169b29cb4eb37a0577388c22527, d7e4bb95401a19f9bf7ca280a4e743229998494790ab129b31b2a6c1cebebec7, 93c16c11ffca4ede29338eac53ca9f7c4fbcf68b8ea85ea5ae91a9e00dc77f01, 54ff98956c3a0a3bc03a5f43d2c801ebcc1255bed644c78bad55d7f7bebd294, 9e1f8165ca3265ef0ff2d479370518a5f3f4467cd31a7b4b006011621a2dd752, e4882b8e8e414e983cf003a5c4038043002a004b63c4f0844a15268332597e80, 117fc30c25b1f28cd923b530ab9f91a0a818925b0b89b8bc9a7f820a9e630464, 555964b2fed3cced4c75a383dd4b3cf02776dae224f4848dcc03510b1de4dbf4, 0629cd5e187174cb69f3489675f8c84cc0236f11f200be384ed6c1a9aa1ce7a1, bf9fc34ef4734520a1f65c1ec0a91b563bf002ac63982cbd2df10791493e9147, cd27a31e618fe93df37603e5ece3352a91f27671ee73bdc8ce9ad793cad72a0f, 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6,

TYPE	VALUE
SHA256	8e1eb0ad22236e325387fdb45aea63f318a672c5d035a21d7b3a64eeafb4c5a2, aa0772fc6784799d59649654879c2b4a23919cda410bede0162751e6d6d6b558, ebb2a1b46a13c308ffe62dda4d9da316d550433707b2c2a38ad710ea4456c608, ceed9fdce420c0558e56bb705664d59f67d62c12d7356ca86439082616638b256, 5e9fc42cf65e1a87e953d00cb2755d3b5b00c1414259534c3a85742295bb6ff9, a25097d2ae808df410c2f35d725a500fb680f38605e62c9e3b619e389ef6733f, c26ce932f3609ecd710a3a1ca7f7b96f1b103a11b49a86e9423e03664eaabd40, 411b2ed12df1ace6559d3ea666c672617ce23e2ace06806bb53c55bcccb83303
MD5	64ca549e78ad1bd3a4bd2834b0f81080, eb6fff4ee0f03ae5191f11570ff221c5, 923c5af6fd29158b757fb876979d250b, 31edb01d243e8d989eb7e5aeeeef54dc, a7ab0969bf6641cd0c7228ae95f6d217, 417ad60624345ef85e648038e18902ab, e01776ec67b9f1ae780c3e24ecc4bf06, 63b89a42c39b2b56aae433712f96f619, d0a711e4a51891ddf00f704d508b1ef2, 14dec91fdcaab96f51382a43adb84016, 88bb86494cb9411a9692f9c8e67ed32c, 470d0261d18ed69990ce94f05d940de1, d67303ba66bcb4dd89de87c83f3f831f, 440810b008eed766f085b69b1723f54b, 6b7eeb860917aa44982d8bd2d971aff1, a42d36f1af2c396e645ffa356fa47a1e, e1d41939dc4cc4116cc3439a01cfb666, 1410b418a078559581725d14fa389cdd, 08a2405cd32f044a69737e77454ee2da, 0d68a310f4265821900249bec89364c2, 11d795baafa44b73766e850d13b8e254, 144183a4217ae0914ba0c865858d07cd, 19ff6488a259d750ec18902fe75a713b, 1bde76f3197123dcc2ecd0bfef567484, 1c4bea81c0da22badd9b7eab574c51cd, 2020979e080d7ac9c0403172573c7de8, 24a8fcd08d9e40d32929b57de9b15385, 2bb209ccfc5103eccab523c875050cfa, 2f76a29d4e4292d7f29a29345717812c,

TYPE	VALUE
MD5	37155f0bca29ccd6b6d4f5b2bc42eb4d, 3b10127e65fa3e215d21e0a2e7fd32be, 420a2c53386678396f972f09cc7f3a5c, 4a3f22021e4415e8211633fb3735a046, 4ea8adecc5bd45a76cc61430c560924f, 53c8a4f0497929de4a5039b2c14bf426, 575b26c1cc06609722f98e2beaed6a8a, 5862f9fc9c9a0d766eba29eb4945f619, 59d756280b06cf113ca43abc0050edd5, 5cffa3126b9effc279d32b2cf4ef2278, 64a590760fdbb84356544cc90ac3d50f, 670fe8faaede4e2e033311fb662d2a4a, 6f893b1cc5cf534c59eabe932c1bf21e, 6fc6164b3a08669992acad3764fb1922, 826a8e8c05983aa3a884d7abcfa473ac, 88630916b0c6633ca28c8896416a93ee, 8ca5c9745e8a0e18167a9b932821645a, 964c13b68dc6b6b918b66a9a10469d2a, 996c394d0f6d6967df9542c52f6f4661, 9befad1d56d2bd8195813aea1f37f921, 9ea321b6a0f069caab7092cfe1cbbde0, 9f510626c7327a7c2328bc5131726638, a6302fdb63e2244c1246a73a7d65d09e, a7e7d00d531cb7ca27d0f3bee448573f, ab05a1925fee8334a2114811d5283364, b04e8ee43aba85fa5c585b9335c953c2, b4a6152514919a637c22a58bea316fc7, bed0f34673cc93560c17e3ab04ea5d19, d1c331c17ddd4abe0d53755461c1ec9a, d309e3d77ed6a336eb3ad263ddf9db90, d6e7547ad7dfd1fbc62e8282aebcc391, dd42c3e017889c107a81da78d87dc8af, e4c1add9f7606e3fa57976b908b4b375, ea1f8794c73b26724314e5356f1f4128, f588802958c35fe18eb87bc36651a3d1, f982da00c547913fd0ae7d0da0fc77e7, Fdc6848dad660414bed9ad1b381cf6e3, 3158a3849ea2695d6ec5aea6512fd030, 348b0ce6af4698061678c8e92b4b2675
SHA1	493ff413528f752c5fce3ceabd89d2ab37397b86, c2dfbf554e068195ecc40bebd0617ce09ad65784, 6b3e3ff0495d39c85eca41f336bfd5ff92c97412, 05f60fc706754b317ffc7839a2b0490f7cd6f71d, 002971b6d178698bf7930b5b89c201750d80a07e, e18e6f975ef8fce97790fb8ae583caad1ec7d5b3, 3ef805009f8694e78699932563c09ac3b6bc08a5,

TYPE	VALUE
SHA1	50927809fa3f1ec408d7a1715a714831f41160db, d9ea05933353d1f32b18696877a3396140022f03, a85d9d2a3913011cd282abc7d9711b2346c23899, 82f8060575de96dc4edc4f7b02ec31ba7637fa03, 890581fca724935118606a4d92dbc206f9eff04c, 34bfe0c8aa61f90ca03b7e80271d5a8afae0be4b, 9692644974071cd484455e355f8d79ce8c486e20, d4e3a066e1c1a21e3d44f2ef81a94aec42f5df11, 5914e976598ece1a271a60615a17420319a77812, 6e35dfdf0d09a0313a33fcc6c77f4fe00a79b9dc, 081cd6c242d472db9148fd0ce33346f7a3e87ac2
Domains	cloudflariz[.]com, cloudflariz[.]com/comm.php, cloudflariz[.]com/auload.php
URLs	hxxp[:]//184[.]174[.]96[.]74/rs64c[.]exe, hxxps[:]//88[.]119[.]174[.]107[:]22443/file[.]ext
File Names	hosts.exe, dato.exe, dato.lnk, vvvivyyl.exe, rs64c.exe, decryptor_399060b2.exe, enc.exe, update.exe, inter.exe, BackupsFrst.exe1, 99.dll, 31edb01d243e8d989eb7e5aeeeef54dc.virus,
File Paths	C:\Users[USER]\AppData\Local\Temp\vvvivyyl.exe, C:\ProgramData[Unique ID]_crypt.exe, C:\ProgramData\svchost[.]exe
Ransom Note Filename	README-RECOVER-[rand].txt, README-RECOVER-[rand]_2.txt, [Unique ID]-RECOVER-README.txt
Tor Leak Site	ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd[.]onion

Recent Breaches

https://www.novajoy.com
https://www.clinicamaitenes.cl
https://www.oc.hu
https://www.mainstreethomesearch.com
https://www.roofingsolutionsla.com
https://www.williamdavis.co.uk
https://www.shocco.org
https://www.hamistergroup.com
https://www.buy.alphagroup.nz
https://www.brandedproducts.com.au
https://www.pgtradingco.com
https://www.asrllp.com
https://www.global-retool-group.com
https://www.sponsellergroup.com
https://www.expocredit.com
https://semgrep.dev
https://www.roto-immobilien.at
https://www.vernonginsburg.com
https://www.snyderpkg.com
https://www.porteryett.com
https://www.cjarchitects.net
https://www.czcollections.com
https://www.hamerchilds.co.uk
https://www.vialagro.com.ar
https://www.airconditioning-florida.com
https://www.mrdsllc.com
https://www.rtesllc.com
https://www.mrdrywallservices.com
https://www.wnslowery.com
https://www.lexus.ua
https://www.rcrindustrialflooring.com
https://www.gartengestaltung-mueller.at
https://www.ajj.cl
https://www.salterhealthcare.com
https://www.mbsl.qc.ca
https://www.monir.ca
https://www.mpag.gov.my
https://www.fqueralt.com
https://www.pnsbinsbroker.com.my
https://www.originaltaylorporkroll.com
https://www.buckeyepaper.com
https://www.bangorwholesalelaminates.com
https://www.bcaremedicalcenter.com
https://www.nre.co.th
https://www.commonpartgroupings.com

Patch Links

https://fortiguard.fortinet.com/psirt/FG-IR-24-535

https://fortiguard.fortinet.com/psirt/FG-IR-24-015

https://www.veeam.com/kb4424

https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html

References

https://www.dexpose.io/qilin-ransomware-targets-clinica-maitenes-in-chile/

https://malware.news/t/qilin-ransomware-targets-clinica-maitenes-in-chile/107533

https://x.com/_venarix_/status/2061773911713304884

https://hivepro.com/threat-advisory/Qilin-Ransomware-Surge:-A-Growing-Global-Threat-to-Critical-Sectors/

https://hivepro.com/threat-advisory/agenda-ransomware-group-escalates-attacks-with-new-multi-stage-loaders/

https://www.rapid7.com/blog/post/tr-post-ramp-allegations-fragmentation-ransomware-underground-rebuild/

https://hivepro.com/threat-advisory/the-gentlemen-ransomware-a-rapidly-scaling-raas-threat/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

June 4, 2026 • 11:00 PM

More at www.hivepro.com