Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

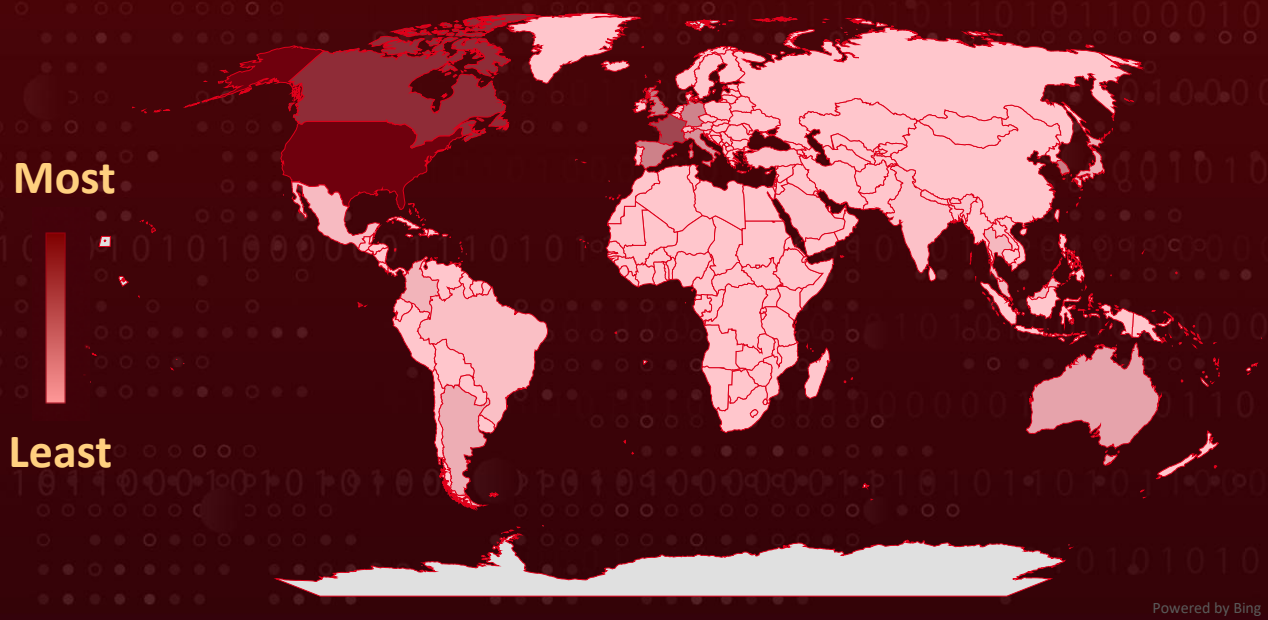
Qilin Ransomware Surge: A Growing Global Threat to Critical Sectors

Date of Publication	Admiralty Code	TA Number
October 29, 2025	A1	TA2025331

Summary

Attack Commenced: October 2025
Targeted Countries: Worldwide
Targeted Platforms: Windows and Linux
Malware: Qilin Ransomware (aka Agenda, Water Galura),
Targeted Industries: Manufacturing, Technology, Healthcare, Real Estate, Legal, Energy, Hospitality, Insurance, Business Services & Consulting, Government, Education, Retail, Financial Services, Transportation, Food Service, Pharmaceutical, Agriculture, Religion, Media, Telecommunications, Casino & Gambling, Associations, Aviation, Aerospace and Defense, Charitable Organizations, Professional Services
Attack: Qilin, also known as Agenda, has become one of the most aggressive ransomware operations of 2025, claiming over 700 victims this year, including nearly 200 in October alone, signaling a sharp escalation in attack frequency. The group employs advanced techniques, including deploying a Linux ransomware variant on Windows systems via legitimate remote management tools, exploiting vulnerable drivers, and targeting Veeam backups to cripple recovery. Attacks typically begin with phishing and credential theft, followed by stealthy lateral movement, data exfiltration, and double-extortion. Qilin's sophistication and cross-platform adaptability highlight the urgent need for stronger access controls, multi-factor authentication, and hybrid-environment monitoring.

Attack Regions



Attack Details

#1

Qilin ransomware, aka Agenda, has rapidly become one of the most prolific ransomware operations of 2025, recently intensifying its activity with nearly 200 confirmed victims in October alone. This surge, combined with new cross-platform capabilities, marks a significant escalation in its threat level. First observed in 2022 and expanding in 2023, Qilin operates under a ransomware-as-a-service (RaaS) model that enables affiliates to conduct attacks using its infrastructure. Affiliates reportedly keep up to 85% of ransom proceeds, fueling a high operational tempo and broad victim base. In 2025 alone, Qilin has claimed over 700 victims across critical sectors such as manufacturing, healthcare, financial services, and government, with major incidents in the United States, France, Canada, and the United Kingdom.

#2

A major 2025 advancement is Qilin's ability to execute a Linux ransomware variant on Windows systems by abusing legitimate remote management and file-transfer tools like AnyDesk, ScreenConnect, and Splashtop. This cross-platform execution bypasses Windows-centric detection mechanisms and enhances stealth in hybrid environments. The group also employs Bring Your Own Vulnerable Driver (BYOVD) techniques to gain elevated privileges and evade endpoint defenses by loading signed but exploitable drivers. Additionally, Qilin targets backup systems, particularly Veeam servers, to steal credentials and disable recovery through tailored PowerShell scripts and SQL commands.

#3

Intrusions often begin with phishing campaigns that use fake CAPTCHA pages to deploy infostealers for credential harvesting. Stolen credentials enable lateral movement via legitimate administrative channels, followed by installation of SOCKS proxy backdoors that hide command-and-control traffic. Attackers then perform reconnaissance, escalate privileges, create hidden accounts, and leverage renamed SSH or remote tools to access Linux hosts. The campaign culminates in rapid encryption and data exfiltration, leveraging double-extortion tactics to pressure victims.

#4

Qilin's operational sophistication, cross-platform capabilities, and use of legitimate tools highlight the urgent need for improved hybrid-environment visibility, stricter access control on remote management utilities, mandatory multi-factor authentication, and monitoring for unsigned driver loads or anomalous administrative behavior.

Recommendations

Enforce Multi-Factor Authentication (MFA): Apply MFA across all remote access services, VPNs, and privileged accounts to prevent unauthorized logins using stolen credentials.

Restrict and Monitor Remote Management Tools: Limit the use of applications like AnyDesk, ScreenConnect, and Splashtop to approved administrators and actively monitor for new or unauthorized installations.

Detect and Block BYOVD Exploits: Enable driver signing enforcement and restrict driver installation privileges to system administrators. Continuously monitor for unsigned or vulnerable driver loads that could allow privilege escalation. Maintain an updated inventory of drivers to identify and remove risky versions.

Enhance Endpoint and Network Visibility: Deploy extended detection and response (XDR) or EDR tools to identify unusual cross-platform activity, such as Linux binaries executed on Windows. Correlate endpoint and network telemetry for faster detection of lateral movement or data exfiltration attempts.

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.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0040 Impact	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access

T1078 Valid Accounts	**T1133** External Remote Services	**T1110** Brute Force	**T1110.003** Password Spraying
T1003 OS Credential Dumping	**T1482** Domain Trust Discovery	**T1018** Remote System Discovery	**T1033** System Owner/User Discovery
T1087.002 Domain Account	**T1087** Account Discovery	**T1057** Process Discovery	**T1222** File and Directory Permissions Modification
T1222.001 Windows File and Directory Permissions Modification	**T1046** Network Service Discovery	**T1219.002** Remote Desktop Software	**T1082** System Information Discovery
T1059.001 PowerShell	**T1048** Exfiltration Over Alternative Protocol	**T1537** Transfer Data to Cloud Account	**T1484.001** Group Policy Modification
T1484 Domain or Tenant Policy Modification	**T1021.001** Remote Desktop Protocol	**T1021.002** SMB/Windows Admin Shares	**T1021** Remote Services
T1105 Ingress Tool Transfer	**T1562.001** Disable or Modify Tools	**T1562** Impair Defenses	**T1070.001** Clear Windows Event Logs
T1070 Indicator Removal	**T1490** Inhibit System Recovery	**T1489** Service Stop	**T1486** Data Encrypted for Impact
T1112 Modify Registry	**T1053** Scheduled Task/Job	**T1547.001** Registry Run Keys / Startup Folder	**T1547** Boot or Logon Autostart Execution
T1059.003 Windows Command Shell	**T1219** Remote Access Software		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	c150e4ab20d59affc62b916c2c90686f43040a9f
SHA256	c0f7c2bb04aa09dae62f0e5feeb7c9c867685abc788ae6b0e6928ad7979dbcaf, e46bde83b8a3a7492fc79c22b337950fc49843a42020c41c615b24579c0c3251, f488861f8d3d013c3eef88983de8f5f37bb014ae13dc13007b26ebbd559e356e, 3dba9ba8e265faefce024960b69c1f472ab7a898e7c224145740f1886d97119f, 15e5bf0082fbb1036d39fc279293f0799f2ab5b2b0af47d9f3c3fdc4aa93de67, 331d136101b286c2f7198fd41e5018fcadef720ca0e74b282c1a44310a792e7f, 549a1ae688edfcb2e7a254ac3aded866b378b2e829f1bb8af42276b902f475e6, 454e398869e189874c796133f68a837c9b7f2190b949a8222453884f84cf4a1b, e38d4140fce467bfd145a8f6299fc76b8851a62555b5c0f825b9a2200f85017c, 5f0253f959d65c45a11b7436301ee5a851266614f811c753231d684eb5083782, e14ba0fb92e16bb7db3b1efac4b13aee178542c6994543e7535d8efaa589870c, 16f83f056177c4ec24c7e99d01ca9d9d6713bd0497eeedb777a3ffefa99c97f0, 5fff877789223fa9810a365dfdeafe982c92f346ecd20e003319c3067becd8ba, 8fe746dd277e644fa0337db3394f0eadfafe57df029e13df9feef25c536adf4d , dbe9ed8e8e8cdff3670e7205cb9f11b5a0fa9d1983a6c6bab67527d8775c4ffd, 38ddde36929a2ddf13b1844973550072c41004187eaa2456f86e20aa93036b18, a068f595472c4f94baf1c2a8fba6831a327514e24ec4b38e1eee2cf1646b1591, e129dd5cc80f39b24db489df999c847335d169910bd966814d2f81b0b1bbc365,

TYPE	VALUE
SHA256	dd29138bf369863c33402a3fc995458ab5fc015a13a9378022131ab31d940c9f, d1347f4dccebf2fcd672dcef9c66c91b9d3f12b9881e3e390626927718fda616, 912018ab3c6b16b39ee84f17745ff0c80a33cee241013ec35d0281e40c0658d9, 6ce228240458563d73c1c3cbbd04ef15cb7c5badacc78ce331848f5431b406cc, e705f69afd97f343f3c1f2bc6027d30935a0bfd29ff025c563f6f8c1f9a7478e, 792182b7c5a56e5ccefd32073dc374e66c6a4e7981075e3804f49a276878e0fb
IPv4	85[.]239[.]34[.]91, 86[.]106[.]85[.]36
Domain	regsvchst[.]com, holapor67[.]top, mimikatzlogs@anti[.]pm, mimikatz@anti[.]pm
URLs	hxxp[:]//185[.]141[.]216[.]127/tr.e, hxxps[:]//pub-2149a070e76f4ccabd67228f754768dc[.]r2[.]dev/I-Google-Captcha-Continue-Latest-27-L-1[.]html, hxxps[:]//pub-959ff112c2eb41ce8f7b24e38c9b4f94[.]r2[.]dev/Google-Captcha-Continue-Latest-J-KL-3[.]html, hxxps[:]//chatgptitalia[.]net/, hxxps[:]//45[.]221[.]64[.]245/mot/, hxxps[:]//104[.]164[.]55[.]7/231/means.d,
TOR Address	hxxp[:]//ozsxj4hwxub7gio347ac7tyqqozvfioty37skqilzo2oqfs4cw2mgtyd[.]onion, hxxp[:]//kbsqoivihgdmwczmxkbovk7ss2dcynitwhhfu5yw725dboqo5kthfaad[.]onion, hxxp[:]//securo45z554mw7rgrt7wcgv5eenj2xmxyrsdj3fcjsvindu63s4bsid[.]onion

Recent Breaches

https://microbix.com
https://productivetool.com
https://lorberlaw.com
https://henriettaezeokelaw.com
https://doubleoakconstruction.com

https://izaki.co.il
https://medimpact.com
https://mickestridhmaskin.se
https://infracom.com.au
https://applied-tech.com
https://sarpc.org
https://northernlighttech.com
https://omrin.nl
https://kaufmanstigger.com
https://essentialcabinetrygroup.com
https://sugarlandtx.gov
https://zacho-lind.dk
https://dohabritishschool.com
https://promasa.hn
https://mainetti.com

References

https://www.trendmicro.com/en_us/research/25/j/agenda-ransomware-deploys-linux-variant-on-windows-systems.html

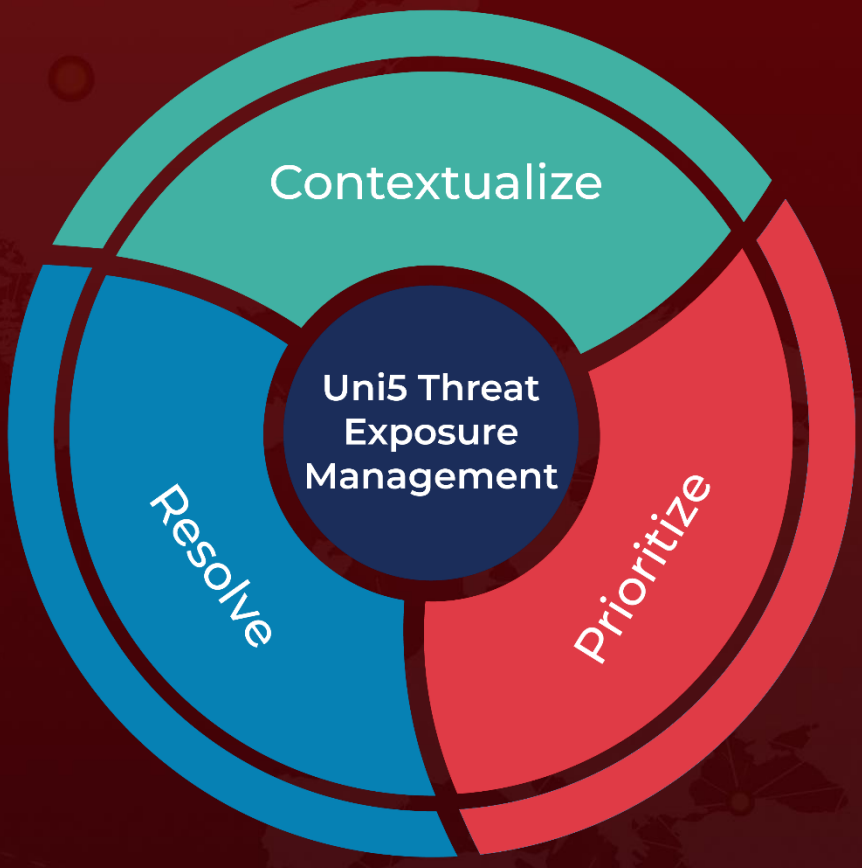
https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases/

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

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 29, 2025 . 11:30 PM

More at www.hivepro.com