Qilin Ransomware and The NHS Foundation Trust: Cyber Threat Analysis and Global Implications

---

Research and analysis by Galih Samoeri

EXECUTIVE SUMMARY

A ransomware attack occurred on June 3, 2024 executed by Qilin against Synnovis, a pathology service providing diagnostic laboratory solutions for Guy's and St. Thomas' NHS Foundation Trust and King's College Hospital NHS Trust. The attack was responsible for the theft of 400 GB of sensitive patient data and more significantly, caused massive disruption to vital medical services including delays in critical surgeries negatively affecting frontline workers and patient welfare.

Similar to most ransomware groups, Qilin utilises double extortion tactics, where they not only encrypt victim data but exfiltrate sensitive data and employ it as leverage for payment. The exfiltrated information is threatened to be leaked unless ransom demands are met. The attacker demanded a £40 million ransom payment from The NHS, capitalising the urgency of medical care to increase the pressure of payment demands. This incident represents a concerning confirmation in the growing trend of cyberattacks against healthcare infrastructure globally, where severe healthcare service delays have direct consequences and effect on patient lives.

THREAT ACTOR PROFILE

Qilin, also known as Agenda, is a Ransomware-as-a-Service (Raas) first emerged in October 2022. Although not conclusive, intelligence analysts and researchers have linked their operation to Russia based criminal syndicates. They have claimed responsibility for more than 60 cyberattacks in 2024 alone primarily targeting healthcare, financial institutions and critical infrastructure with a wide reach internationally spanning 25+ countries. Most recent data shows Qilin's ransom demands are within the range of $50,000 - $50,000,000. Confirmed attacks include: International Electro Mechanical Services in the US, Felda Global Ventures Holdings Berhad in Malaysia, Bright Wires in Saudi Arabia, PT Sarana Multi Infrastruktur (Persero) in Indonesia, Casa Santiveri in Spain.

Known Tactics, Techniques & Procedures (TTPs)

- **Initial Access:** Phishing emails, RDP brute-force attacks, exploiting unpatched vulnerabilities
- **Execution:** Deployment of custom ransomware payloads specifically for Windows and Linux
- **Persistence:** Utilising scheduled tasks (Windows) and cron jobs (Linux) and registry modifications.
- **Exfiltration:** Rclone or MEGASync to exfiltrate sensitive data before encrypting
- **Impact:** Double extortion; encrypting files and threatening to release sensitive information

DETAILS OF ATTACK on Synnovis (NHS)

- **Initial Access:** Unconfirmed - historical data from prior attacks shows Qilin relying on spear-phishing and credential theft to gain access to networks.
- **Execution:** After gaining access, attackers leveraged stolen admin credentials (T1078) to perform privilege escalations and execute payloads using PowerShell (T1059)
- **Data Exfiltration & Encryption:** 400GB of patient-sensitive data was stolen before encryption

- **Operational Impact:** Delayed surgeries due to inaccessible pathology reports, disrupted blood transfusions and test processing. Decreased efficiency for frontline workers due to service backlogs.

MITRE ATT&CK FRAMEWORK MAPPING:

INITIAL ACCESS		
T1566	Phishing	Utilise malicious email attachments to gain access.
EXECUTION		
T1053.005	Scheduled Task	Scheduled tasks to run malicious programs at a predetermined time
T1059	Command and Scripting Interpreter	Leverage command-line interfaces or scripting languages to execute commands or malicious code.
T1204.001	User Execution - Malicious Link	Entice users to click on malicious links that lead to the execution of harmful payloads.
PERSISTENCE		
T1078	Valid Accounts	Maintain access by using valid user credentials, allowing attackers to persist undetected.
PRIVILEGE ESCALATION		
T1078.002	Domain Accounts	Elevate privileges by exploiting domain accounts, granting elevated access within a network.
DEFENSE EVASION		
T1562.001	Disable or Modify Tools	Disable or alter security tools to prevent detection or hinder their effectiveness.
T1070.004	Indicator Removal: File Deletion	Remove traces of malicious activity by deleting associated files or logs.
T1070.001	Indicator Removal: Clear Windows Event Logs	Erase entries in Windows event logs to evade detection and remove evidence of malicious actions.
DISCOVERY		
T1135	Network Share Discovery	Scan the network for shared drives or resources to map the attacker's movement path.
LATERAL MOVEMENT		
T1021.001	Remote Desktop Protocol	Attacker utilised RDP to move laterally through the network.
COMMAND AND CONTROL		
T1071	Application Layer Protocol	Use standard application protocols, such as HTTP or HTTPS, to communicate with remote systems without raising suspicion.

EXFILTRATION		
T1048	Exfiltration Over Alternative Protocol	Exfiltrate sensitive data by using protocols not typically associated with data transfer, to bypass network monitoring.
IMPACT		
T1486	Data Encrypted for Impact	Encrypt data to disrupt access or hold it hostage for ransom, causing operational disruption.
T1489	Service Stop	Disable or stop essential services to disrupt operations or cause further damage to the network.

***Please note due to the limited transparency in the investigation, the TTPs are incomplete. Shown are identified TTPs and those the attacker likely utilised.*

Indicators of Compromise (IOCs)

Type	Indicator	Description
URL	hxxp://194.165.16[.]55:80/a	Used to download Cobalt Strike
URL	security-socks777[.]com	Contacted Cobalt Strike Server
URL	security-socks[.]expert	Contacted Cobalt Strike Server
URL	jango-pulse[.]com	Contacted Cobalt Strike Server
URL	blm-wiki[.]com	Contacted Cobalt Strike Server
IP	194.165.16[.]55	IP address recorded for the URLs security-socks777[.]com and security-socks[.]expert
IP	188.114.96[.]3	IP address recorded for the URL blm-wiki[.]com
Folder	C:\PerfLogs	Preferred folder of the attacker for placing tools and their output
File	C:\PerfLogs\update.exe	Ransomware binary
File	FileZilla_3.66.5_win64-setup.exe	Used to install FileZilla for data exfiltration
File	FileZilla_3.64.0_win64-setup.exe	Used to install FileZilla for data exfiltration
File	PCHunter64.exe	-
File	Powertool64.exe	-
File	ipscan.exe	Angry IP Scanner
File	netscan_portable.exe	-
File	WinPcap_4_1_3.exe	Used with masscan
File	mimikatz.exe	-

File	adfind.exe	-
File	ShareFinder.ps1	

RELEVANT COMPARISON

A similar cyberattack also targeting a medical diagnostics lab occurred 2 months prior to the Synnovis attack against SynLab Italia. Although unconnected to Qilin, Extortion group Black Basta was responsible for the theft of 1.5 TB of data including sensitive medical analysis patients data (toxicology, advanced blood analysis), customer data, and employees personal documents.

The attack forced suspension of all activities at sampling points, medical centres, and laboratories. Although the residual impact of the attack was not nearly as catastrophic as the London hospitals, this underscores a larger trend that healthcare services are increasingly becoming prime targets for cyberattacks.

FACTOR	QILIN (NHS, UK)	BLACK BASTA (SYNLAB, ITALY)
Date	June 3, 2024	April 18, 2024
Attack Type	Ransomware	Ransomware
Victim	NHS Synnovis (UK)	SynLab (IT)
Data Stolen	400 GB patient data	1.5 TB patient and employee data
Impact	Delayed surgeries, blood test failures, operational downtime	Service interruptions, operational downtime
Ransom Demand	£40,000,000	Undisclosed
Known Tactics Used	Double extortion, RDP brute force, phishing	Double extortion, phishing

Key Takeaways:

- Healthcare services is a Prime Target
- Qilin's attack had direct consequences on patient health, whilst Black Basta primarily caused financial and reputational damage
- Double extortion remains the primary method of extortion with Qilin being more aggressive in its ransom demand

MITIGATION & DEFENSIVE STRATEGIES

To mitigate future risks of ransomware attacks, the following security best practices should be applied across hospitals and other critical organisations:

Short-Term Mitigation Measures:

- Patch vulnerabilities immediately to prevent exploit-based access.
- Implement phishing-resistant MFA (FIDO2 keys) to block credential theft.
- Block known IOCs (IP addresses, domains, file hashes) via firewalls and SIEM solutions.
- Reset admin credentials & enforce least-privilege access to limit lateral movement.

Long-Term Defensive Strategies:

- Deploy EDR solutions (CrowdStrike, SentinelOne) to detect and stop ransomware behavior.
- Implement network segmentation to isolate critical hospital systems from internet-facing services.
- Enhance threat intelligence monitoring by tracking ransomware trends and adapting defenses accordingly.
- **Conduct Red Team exercises** to simulate real-world ransomware scenarios and emulate known adversaries that target specific sectors and improve response readiness.
- Long-Term Strategies: (Stronger authentication, EDR solutions, AI-driven anomaly detection.)

CONCLUSION & FINAL ASSESSMENT

The Qilin ransomware attack against NHS Synnovis serves as a critical warning about the growing threat landscape in healthcare cybersecurity. This attack not only caused financial and operational damage but also had lifelong consequences for patient care, with delayed treatments leading to irreversible health complications.

The comparison with Black Basta's attack in Italy specified above, suggests that ransomware targeting hospitals is becoming more frequent and aggressive. As cybercriminals continue to exploit outdated systems, weak security postures, and high ransom payouts, healthcare providers must adopt proactive security measures to prevent future incidents.

Without immediate improvements in cyber resilience, network segmentation, and rapid response strategies, ransomware will continue to disrupt essential medical services, therefore putting lives at risk on a global scale.