Executive Summary

6 active threat groups are currently targeting healthcare and technology sectors across the Americas, Europe, and Asia-Pacific. High priority: Qilin/AGENDA ransomware actively exploiting Ivanti VPNs and Pro-Russia hacktivist DDoS campaigns are elevated due to the 2026 Winter Olympics. Total IOC count: 280+ indicators tracked this week..

Active Threat Campaigns

Campaign	Type	Targets	Key Technique	Priority Action
Qilin / AGENDA Ransomware	Ransomware	Healthcare, Tech – Americas, EU	Exploits Ivanti Pulse Secure; deploys MONOSPY backdoor + VAPORPATH for exfil before encryption	Patch Ivanti immediately — active exploitation
TEMP.Hex · SOGU USB Malware	Espionage	Healthcare, Govt, Education – US, AU, FR, CH, HK	Chinese state group distributes SOGU implant via infected USB drives for long-term persistent access	Enforce USB device controls; scan all physical media
NoName057(16) / Russian Legion / Z-Alliance · DDoS & ICS	Hacktivism	Healthcare, Govt, OT/ICS – Europe, AU, Americas	Coordinated DDoS against Western targets; claimed ICS/SCADA intrusions into water, energy, and agricultural systems	Enable DDoS mitigation; isolate OT/ICS from internet
APT43 · QR Code Phishing	Espionage	Tech, Academia, Govt – Europe, South Korea	North Korean group uses QR codes in Google Drive lures to redirect victims to fake Microsoft/Yahoo/Gmail login portals	Train users on QR phishing; review OAuth grants
UNC5807 · Router Brute Force	Espionage	Telecoms, Govt, Academia – Americas, EU, Asia	Chinese subcluster brute-forces Telnet/SSH on exposed routers for network footholds and lateral movement	Rotate edge device credentials; disable Telnet
CIPHERFORGE · AI-Assisted C2	Espionage	Tech, Dev Environments – Global	.NET backdoor abuses OpenAI Assistants API as covert C2 channel; injects into Visual Studio; evades domain allowlisting	Apply behavioral anomaly detection on AI service traffic

Top 2 Actions This Week

1. Patch Ivanti Pulse Secure immediately. Qilin/AGENDA ransomware actors are actively exploiting known VPN vulnerabilities in healthcare environments. Apply all available patches or implement mitigating controls without delay.

2. Enforce USB device controls and enable DDoS mitigation. Block unauthorized USB media to counter TEMP.Hex/SOGU espionage, and place patient-facing portals behind CDN/WAF solutions with rate limiting to absorb hacktivist DDoS activity..

.

Resources: Google Threat Intelligence | MITRE ATT&CK (attack.mitre.org) | CISA Alerts (cisa.gov)

Report suspicious calls or emails to your IT security team immediately.