



ORPHEUS

# Thematic Areas

## Healthcare and Public Sector

January 2026

# Contents

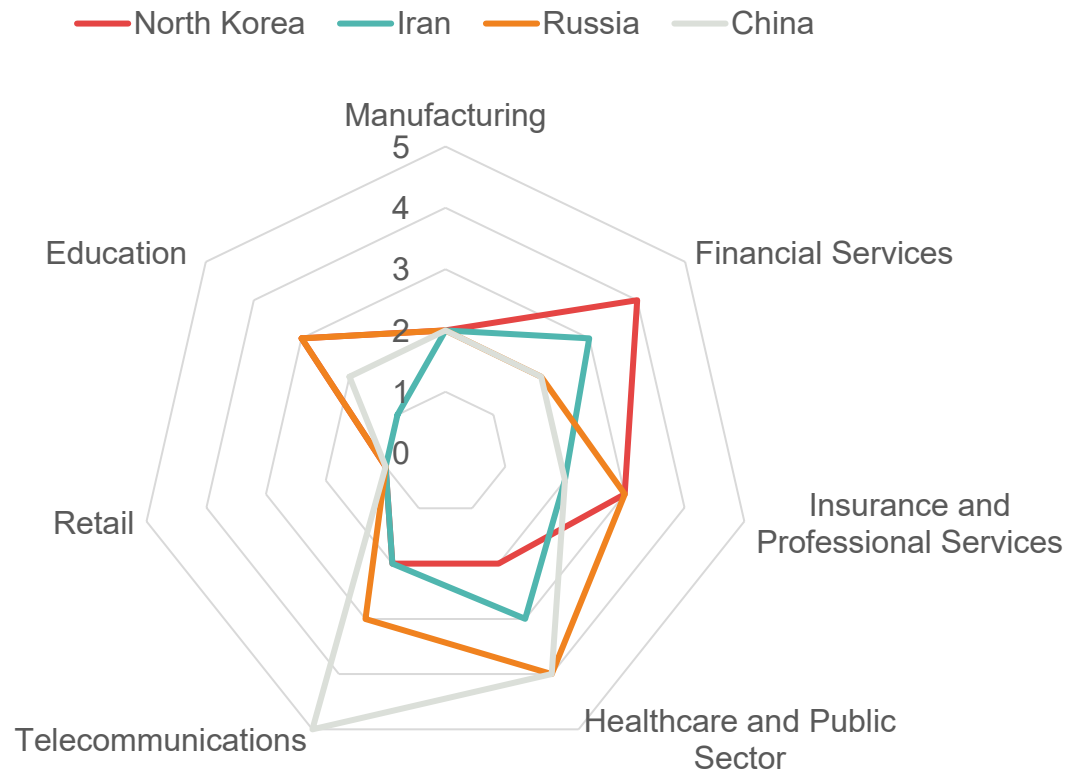
---

<u>01. Nation-State threat across sectors</u>	3
<u>02. Cybercrime threat across sectors</u>	4
<u>03. Hacktivist threat across sectors</u>	5
<u>04. Significant TTPs and IOCs</u>	6
<u>05. Ransomware Statistics</u>	7
<u>06. Monthly Threat Roundup</u>	8
<u>08. Healthcare and Public Sector</u>	9

This document contains confidential information & materials proprietary to Orpheus Cyber and is intended solely for the use of the individual or entity to whom it is addressed for the purposes contained within.

# Nation-State threat to sectors

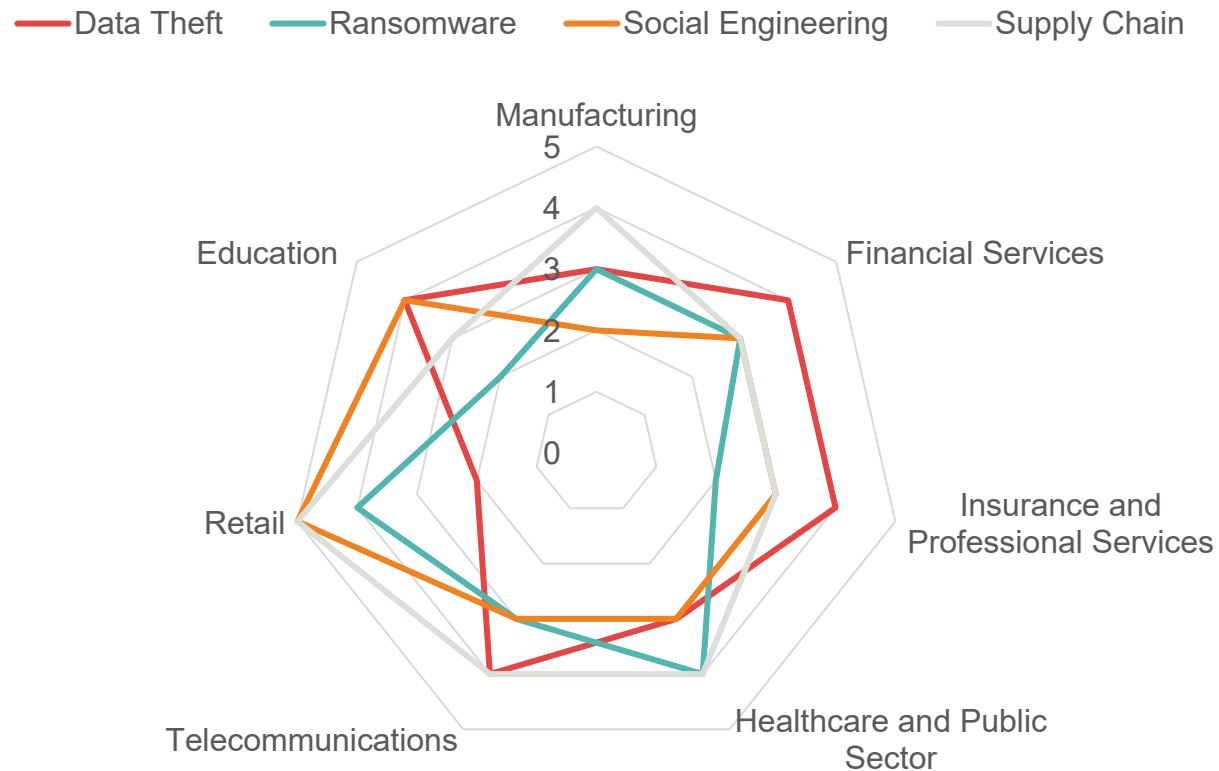
The radar below illustrates, based on internal reporting, which nation-state each sector is most exposed to between China, Russia, Iran and North Korea, based on their relative targeting intensity.



- Overall, most APTs refined existing strategies, while North Korea added AI-generated malware development to its toolkit.
- Targeted campaigns against government entities and public sector remained the greatest nation-state threat globally, with increased targeting of US government institutions by China-linked threat groups.
- Social engineering, especially targeted spear-phishing to deliver existing and novel malware, and vulnerability exploits remain common TTPs for state-sponsored actors.

# Cybercrime threat to sectors

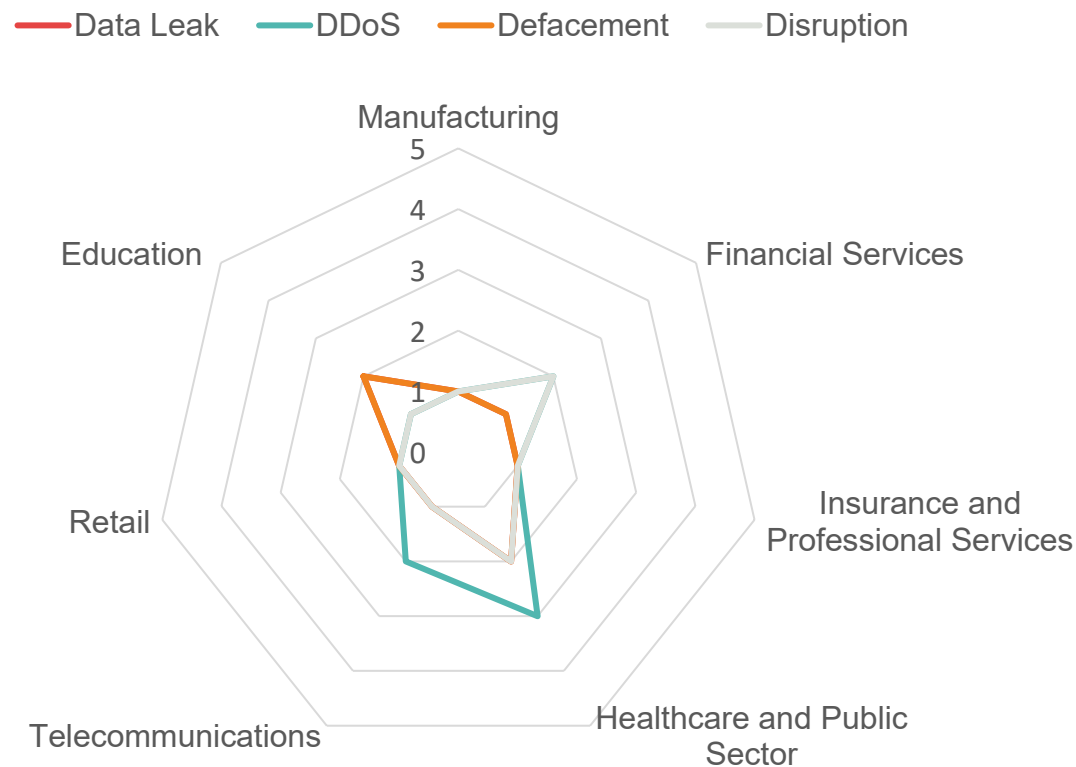
The radar below illustrates, based on internal reporting, which cybercrime threat each sector is most exposed to between data theft, ransomware, social engineering and supply chain compromise



- Cybercriminal threats remained consistent across sectors, with sustained data leak extortion and ransomware campaigns.
- Targeting remains primarily opportunistic and financially-motivated, emphasising targeting in sectors with low tolerance for downtime such as manufacturing and healthcare.
- High activity from Qilin, Everest and Akira in the telecom, manufacturing and healthcare sectors. Everest expands its operations, increasingly acting as an Initial Access Broker (IAB).
- Emphasis on supply chain compromise and social engineering techniques for initial access.
- Elevated service disruption to maximise impact and ransom negotiations through the targeting of overlooked physical access control systems and essential services.

# Hacktivist threat to sectors

The radar below illustrates, based on internal reporting, which hacktivist-related threat each sector is most exposed to, between data leak, DDoS, defacement and disruption of operations or services.



- Hacktivist TTPs have remained relatively consistent over the last 12 months.
- Most Distributed Denial of Service (DDoS) attacks are easy to mitigate with the correct technology in place, and pro-Russian hacktivists will target organisations without protection. This said, Cloudflare reported an increase in frequency and size of DDoS attacks in Q3 2025.
- #OpUK launched in January 2026, a coordinated pro-Russian hacktivist campaign responding to UK support for Ukraine and NATO partners. It relies primarily on repeated low-complexity DDoS attacks against government, public services, and commercial organisations to generate disruption and visibility rather than lasting impact. Targeting is broad and opportunistic, with threat actors favouring organisations lacking mature DDoS protection, reinforcing OpUK's role as a messaging and pressure operation rather than a technically advanced cyber threat.
- While recent government warnings relating to ICS/OT targeting are valid, in January, the observable activity from named hacktivist campaigns (such as #OpUK) was largely focused again on web-layer disruption (DDoS) and opportunistic website outages of government, finance, and public-facing services, with no widely reported, confirmed ICS/OT breaches attributed to these groups in January 2026 specifically.

# Significant TTPs in focus

## Cloud Infrastructure under continuous target

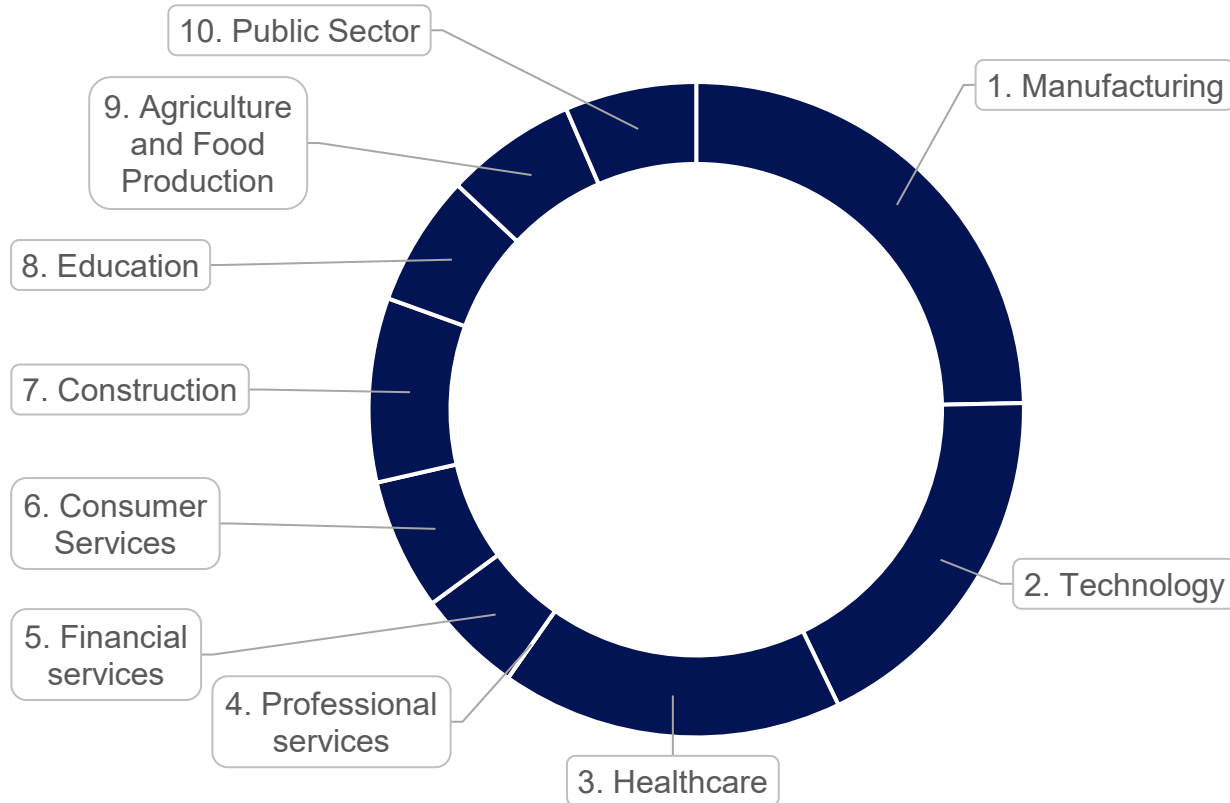
- Designed as a cloud-native malware framework, the VoidLink malware prioritises long-term, stealthy access to Linux systems operating in public cloud and containerised environments, viz. Amazon Web Services (AWS), Google Cloud, Microsoft Azure, Alibaba, and Tencent.
- Actively detects major cloud providers and container platforms, tailoring its execution to match the underlying infrastructure and reduce the likelihood of detection.
- Built with a flexible, modular architecture that allows operators to introduce new functionality, adjust behaviour, or deploy plugins at runtime without reinstalling the malware.

## MITRE TTPs | VoidLink Framework

Technique Name	MITRE TTP ID	Description
Command and Scripting Interpreter: Unix Shell	T1059.004	Threat actors may use VoidLink to execute Unix shell commands on compromised Linux systems to perform discovery, credential access, and task execution. By leveraging native shell interpreters commonly used in cloud and container environments, VoidLink activity can blend into legitimate administrative or automation workflows, reducing the likelihood of detection while enabling flexible follow-on actions.
Boot or Logon Autostart Execution: Kernel Modules and Extensions	T1547.006	Threat actors may use VoidLink to load malicious kernel modules on compromised Linux systems to maintain persistent, high-privilege access that survives reboots and hides malicious activity from monitoring tools.
Rootkit	T1014	Threat actors may use VoidLink rootkit components to hook system calls, hide processes, ports, and files, and evade user-space monitoring.
Obfuscated Files or Information	T1027	Threat actors may use VoidLink to obfuscate binaries, plugin data, and C2 communications to evade static detection.
Process Injection	T1055	Threat actors may use VoidLink to inject code into legitimate processes, allowing malicious modules to run in trusted contexts and evade detection.
Application Layer Protocol: Web Protocols	T1071.001	Threat actors may use HTTP/HTTPS to communicate with VoidLink C2 servers, blending malicious traffic with legitimate web activity.
Indicator Removal on Host	T1070.001 / T1070.006	Threat actors may remove or manipulate logs and timestamps to reduce visibility and hinder forensic investigation.
Unsecured Credentials: Credentials in Files / Private Keys / Container API	T1552.001 / T1552.004 / T1552.007	Threat actors may use VoidLink to access credentials stored in files, private keys, or container service accounts to expand access across hosts and cloud infrastructure.

# Ransomware Statistics for January 2026

## Top 10 impacted Sectors



## Victims by Country Percentile

COUNTRY	RANSOMWARE VICTIMS
United States	48%
United Kingdom	5%
Canada	4%
Germany	4%
Italy	3%
Spain	3%
France	2%
Turkey	2%
India	2%
Taiwan	2%

# Monthly Threat Roundup

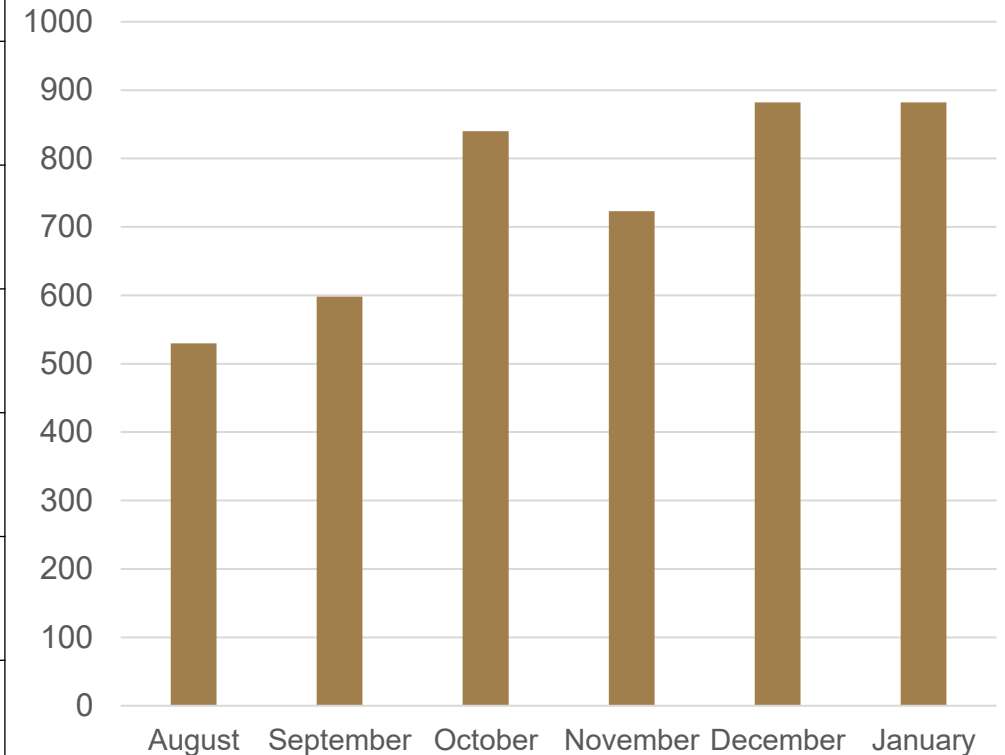
## New Observed Threat Groups: 8

Threat Actor Name	Discovery Date	DLS	Victims	Comment
0apt	28/01/2026	Yes	0	The group appears unreliable. Most, if not all, of its alleged victims cannot be verified and appear to be randomly selected organizations.
Cry0	19/01/2026	Yes	0	No Victims/Activity Reports
Datakeeper	14/01/2026	Yes	0	RaaS (First Appeared 2018) this is a new location.
Fletchen	03/01/2026	Yes	0	Bitcoin Tumbler (Bitcoin Mixer). Bitcoin Blender   JokerMix
Orion	14/01/2026	Yes	0	No Victims/Activity Reports
Aware	06/01/2026	Yes	0	Child Group of Global / Eldorado
Thegreenbloodgroup	21/01/2026	Yes	0	No Victims/Activity Reports

## Total Events

Category	Count
Year (Time of Reporting)	945
Month (January)	702

## Monthly Event Count





**ORPHEUS**

**HEALTHCARE AND  
PUBLIC SECTOR**

# Executive Summary

## Threat to sector



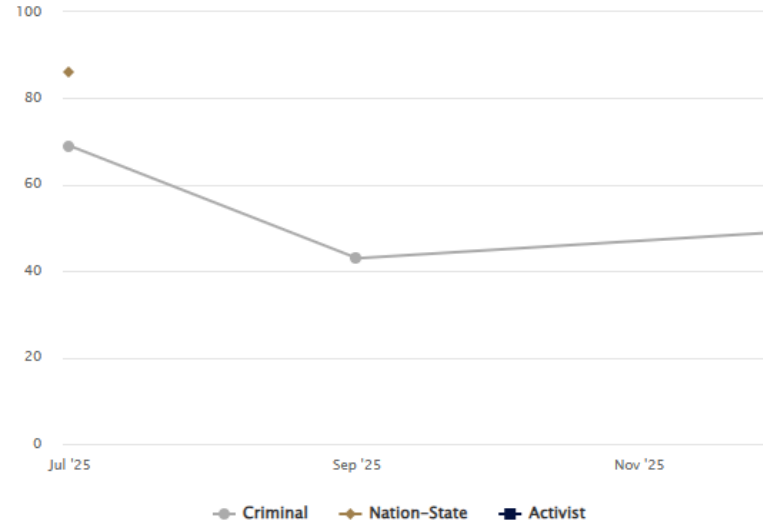
## Significant TTPs

- Variety of initial access vectors demonstrated by the use of spearphishing, vulnerability abuse and credential harvesting
- Elevated TTP sophistication from state-sponsored actors with multi-stage malware delivery campaigns, exploitation of recently disclosed vulnerabilities and deployment of a variety of backdoors including KONNI, LOTUSLITE DLL backdoor, RustyWater RAT and DynoWiper
- Expansion of compromise impact with triple extortion and highly disruptive ransomware operations.

## Key Takeaways

- Nation-states continue to heavily target government institutions and national infrastructure for political intelligence collection and espionage
- Threat to the sector remains consistent with sustained activity from financially-motivated cybercriminals in increasingly disruptive ransomware campaigns
- Healthcare entities remain high-impact extortion targets due to low tolerance for downtime that can result in real-life-threatening situations

## Severity



## Sector Trend Analysis

Based on Orpheus intelligence reporting for the period

Cybercriminals remain the most damaging and consistent threat to the healthcare sector, taking advantage of sensitive medical data and low tolerance for operational downtime in financially-motivated campaigns.

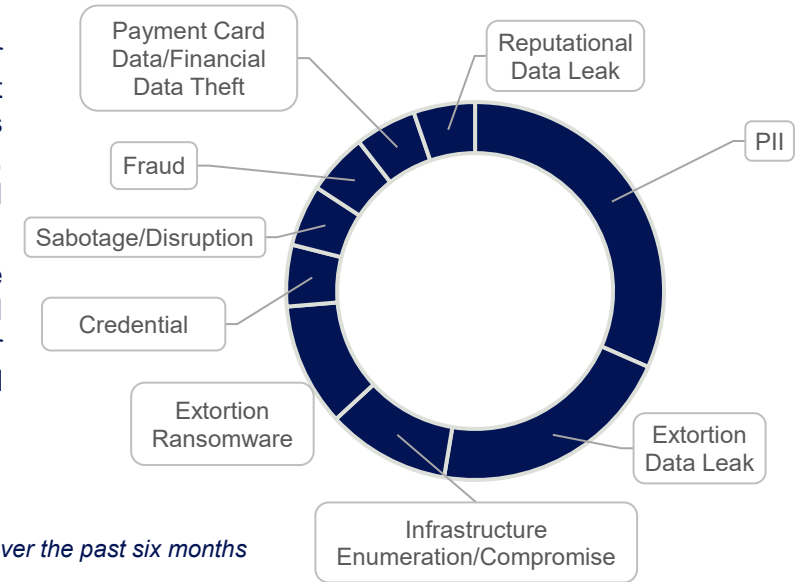
Nation-state-sponsored threat actors continue to focus their targeting on the public sector, notably government entities, for espionage and intelligence gathering campaigns.

## Objective Trend Analysis

The theft and exploitation of PII for extortion data leaks remain the most common objectives of threat actors targeting the healthcare sector, indicating heightened financial motivation.

Government organisations are more likely to be targeted for political intelligence collection and other information theft in espionage-based campaigns.

## Threat Actor Objectives



Analysis based on Orpheus intelligence reporting over the past six months

# Healthcare and Public Sector

	Cybercriminals	State-sponsored / APT	Hacktivists
Intent	Medium/High	Very High	Very High
Capability	Medium	Very High	Low
Objectives	Focus on PII theft, infrastructure compromise and extortion data leak, high financial motivation	Cyber espionage; political, military and economic intelligence gathering; critical infrastructure compromise	Disruption of Services and attain notoriety, amplify message/cause
TTPs and IAV	Triple extortion, leveraging the long-term disruptive consequences of ransomware incidents	Vulnerability exploitation in trusted Windows tools; spear-phishing; wiper malware	Volumetric and Protocol DDoS floods
Assessment	The sector remains a high-impact extortion target due to the sensitivity of data and low tolerance for operational downtime	Threat to governments and critical national infrastructure remains very high, especially from Russia and China; increased targeting of US government by China compared to December 2025	Low threat to healthcare sector but may cause temporary service interruption of services. Due to high potential human impact, healthcare is often targeted by pro-Russian hacktivists nexused around the war in Ukraine. Local Government is frequently targeted across the UK, EU and US

# Healthcare and Public Sector

## State-Sponsored

- Intent – Very High
- Capability – Very High

### Key events

- Throughout 2025, Russia-aligned adversaries abused Viber to deliver malicious ZIP archives to Ukrainian military and government entities.
- North Korean Kimsuky QR code phishing (Quishing) campaign targets US government entities and research institutions focused on North Korea policy.
- Chinese Salt Typhoon breaches email systems of US congressional committee staffers.
- Chinese Mustang Panda targeted US government with a politically themed ZIP archive containing a loader executable to sideload and execute a DLL backdoor LOTUSLITE.
- DynoWiper malware campaign on Poland's power grid in late December 2025 attributed to Russian FSB-linked Dragonfly.
- Widespread active exploitation of CVE-2025-8088 and CVE-2025-6218 in popular Windows file archiver WinRAR linked to Russia and China-sponsored groups, including RomCom and Paper Warewolf.

### Notable TTPs

- Spear-phishing using malicious ZIP files
- Exploitation of vulnerabilities for initial access
- Credential harvesting
- Wiper malware targeting critical infrastructure
- Malware: KONNI, LOTUSLITE DLL backdoor, RustyWater RAT, DynoWiper ransomware

### Key Takeaways

- Nation-states continue to heavily target government institutions and national infrastructure with targeted spear-phishing campaigns using geopolitical lures, favouring reliable execution techniques over vulnerability exploits to achieve initial access.
- Evolution of spear-phishing tactics to include QR code (Quishing) and Viber messaging platform to target government, military, and policy entities.
- Exploitation of vulnerabilities continues to be a tactic of Russia and China-linked threat groups for espionage, credential theft, and infrastructure disruption.

# Healthcare and Public Sector

## Cybercriminals

- Intent – Medium/High
- Capability – Medium

### Key events

- Belgian Hospital AZ Monica was severely disrupted after a cyber incident. Although no initial access vector was publicly disclosed, the organisation likely suffered a ransomware incident.
- Researchers found that threat actors targeting the healthcare sector increasingly expanded to triple extortion by extorting patients.

### Notable TTPs

- Disruptive ransomware with long-lasting operational impacts (delays and service disruption lasting after incident recovery)
- Triple extortion with encryption, threat of data leak and extortion of patients

### Key Takeaways

- The healthcare and public sectors continue to be targeted for the sensitive, personal and medical information they store.
- Healthcare entities remain high-impact extortion targets due to low tolerance for downtime that can result in real-life-threatening situations. Coupled with lasting service delivery consequences long after recovery of the incident and typically weaker security postures, the sector is highly coveted by financially-motivated cybercriminals.
- Public sector organisations, notably government-adjacent entities, are of particular interest to state-sponsored threat actors for political intelligence collection; however, low hanging fruits are highly likely to be targeted by cybercriminals for extortion, with an emphasis on access through supply chain compromise and social engineering.

# Healthcare and Public Sector

## Hacktivists

- Intent – VERY HIGH
- Capability – LOW

### Key events

- UK public sector organisations were among the most frequently targeted during January, with local councils and central government bodies experiencing repeated DDoS attacks under the #OpUK banner. Disruption was limited to public-facing websites and online services
- In late January 2026, a new Russian hacktivist alliance (“Russian Legion” with affiliates) launched “#OpDenmark,” a campaign demanding Denmark cancel an aid package to Ukraine. They flooded Danish government websites and energy sector sites with traffic, even hitting parts of the national grid’s IT network in an effort to force policy changes. Danish authorities reported brief outages on some municipality sites and energy company portals, but no critical infrastructure failures.
- In one instance, a pro-Russia Telegram channel called out an NHS software supplier, leading to a mild DDoS attempt on its login portal (quickly mitigated by the ISP).

### Notable TTPs

- Volumetric DDoS attacks.
  - UDP/TCP Floods, SYN flood, HTTP\_Loris
  - Typically targets webpages and login portals
  - DNS Amplification attacks
- Rudimentary Wiper malware
- Targeting of exposed virtual network computing (VNC) services.

### Key Takeaways

- In late January 2026, healthcare providers were urged to strengthen their cyber defences after the NCSC warned that hacktivist groups might broaden campaigns to essential services. While no major UK hospital outages were attributed to hacktivists that month, the NHS and Integrated Care Boards took the threat seriously, reviewing DDoS protection and emergency response plans in case medical systems were targeted.
- No incidents impacted patient care but served as a reminder of hacktivists’ willingness to target the healthcare sector’s digital infrastructure as a form of protest.

# Intent

Descriptor	Abbr.	Definition
Very Low	<b>VL</b>	Activity would likely only occur as a result of exceptional circumstances that cannot be currently foreseen. Very low levels of activity observed / expected.
Low	<b>L</b>	Activity would likely only occur in exceptional circumstances that are considered highly unlikely. Low levels of activity observed / expected.
Medium Low	<b>ML</b>	Effort-to-reward and risk-to-reward ratios for activity make it highly unattractive, making intent, on balance, less probable. Low levels of activity observed / expected.
Medium	<b>M</b>	Targeted activity has the potential to meet some or all threat actor objectives, but there are no specific indications that threat actor activity is occurring. Intent is considered plausible, but not probable. Some level of activity observed / expected.
Medium High	<b>MH</b>	Targeted activity has a high potential to meet threat actor objectives, indicating high likelihood of considerable intent to carry out malicious activity. Some level of activity observed / expected.
High	<b>H</b>	Widely dispersed activity should be considered a priority on part of threat actors. High levels of activity observed / expected.
Very High	<b>VH</b>	Widely dispersed activity is a clearly established key priority on part of threat actors. Very high levels of activity observed / expected.

# Capability

Descriptor	Abbr.	Definition
Very Low	<b>VL</b>	Can carry out random acts of disruption or destruction by running tools they do not understand.
Low	<b>L</b>	Can minimally use existing, well-known, easy-to-find techniques and programs/scripts to search for and exploit weaknesses in computers. Rely on others to develop malicious tools, delivery mechanisms, and execution strategy and often do not fully understand the tool they are using. Lack the ability to conduct their own reconnaissance and targeting research.
Medium Low	<b>ML</b>	Can proficiently use existing attack frameworks and toolkits to search for and exploit vulnerabilities in computers or systems. Typically have a working knowledge of networks, operating systems, and possibly even defensive techniques. Will typically exhibit some operational security. Rely on others to develop malicious tools and delivery mechanisms, but capable of planning execution strategy. Proficient in the tools they are using and how they work and can even make minimal modifications as needed.
Medium	<b>M</b>	Can develop their own tools or scripts from publicly known vulnerabilities to target systems and users. Very adept at IT systems and have a solid understanding of defensive techniques and operational security. Rely on others to identify weaknesses and vulnerabilities in systems, but capable of creating their own tools, delivery mechanisms, and execution strategies.
Medium High	<b>MH</b>	Can focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode rootkits, frequently use data mining tools, target corporate executives and key users for the purpose of stealing personal and corporate data. Actors in this category are very adept at IT systems and software development, and are experts with security systems, defensive techniques, attack methods, and operational security
High	<b>H</b>	Typically, criminal or state actors who are organized, highly technical, proficient, well-funded professionals working in teams to discover new vulnerabilities and develop exploits. Demonstrate sophisticated capability to create and script unique programs and codes targeting virtually any form of technology. Deep knowledge of networks, operating systems, programming languages, firmware, and infrastructure topologies. Will demonstrate operational security. Largely responsible for the discovery of 0-day vulnerabilities and the development of new attack techniques.
Very High	<b>VH</b>	State actors who create vulnerabilities through an active program to “influence” commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest

# Threat to Sectors Metrics

Descriptor	Score	Definition
Very Low	1	Threat to the sector is minimal, Rare or incidental activity, no clear focus on the sector. Little to no evidence of active targeting of the sector. Impact is non-existent or minimal.
Low	2	Early or limited interest. Small number of attempts. Activity is infrequent and or unsophisticated. The sector is not a primary target but can be a secondary or collateral target. Victims are typically low-hanging fruits, targeted opportunistically.
Medium	3	Repeated, deliberate targeting of the sector. The sector faces an ongoing, although of limited-sophistication threat. Threat actors demonstrate intent and capability but impact remains moderate.
High	4	Sustained, well resourced campaigns against the sector. The threat is significant and persistent and the sector is a clear, deliberate target. Campaigns show elevated sophistication and impact can be severe such as exfiltration of sensitive data, long-lasting disruption and reputational harm.
Critical	5	Continuous, strategic targeting tied to national objectives. Threat poses an immediate and systemic threat to the sector. Campaigns are sustained, highly sophisticated and have long-lasting impact.

# Accreditations

- Orpheus is a highly accredited Cyber Threat Intelligence company – for example we are one of only six companies accredited for CTI by both the FCA and Bank of England.
- We use our Threat Intelligence capabilities to deliver predictive and actionable cyber risk mitigation.
- Our Threat-led attack surface management covers both you and your Third Parties / Supply chain so that you can stop cyber attacks before they happen.
- We are trusted by major global organisations to help protect their vital assets.
- We deploy award winning technologies including Machine Learning.
- Our approach to vulnerability management fuses Threat intelligence and Machine Learning to prioritise mitigation of the CVE's that matter most.
- Recent work for the UK Ministry of Defence.



# Clients



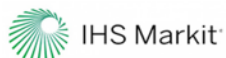
Morgan Stanley



BILL & MELINDA  
GATES foundation



Goldman  
Sachs



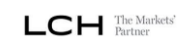
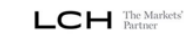
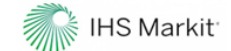
LCH The Markets  
Partner



# Accreditations



# Trusted By Industry Leaders



Thank you  
Any questions?



ORPHEUS

CONTACT US:

[orpheus-cyber.com](http://orpheus-cyber.com)

