June 19, 2025

# Threat Intelligence Summary

## AGENDA

- Top Threats Overall
- Top Threats by Sector
- Top Threat Actors Overview
- Sector Overviews
- Top Phishing Tactics by Sector
- Top 5 TTPs Overview
- Phishing TTPs by Sector
- DDoS/DOS Top Threat Actors
- DDoS TTPs and Sector Threats
- Sector DDoS Threat Breakdown
- Top Malware Threats Overview
- Malware Threats by Sector

# Top Threats Overall

### Ransomware

Malicious software that encrypts data to extort payment, causing operational disruption and financial loss across sectors.

### Phishing-Related Threats

Deceptive emails and messages designed to steal credentials and deliver malware, widely used to gain unauthorized access.

### Supply Chain Attacks

Compromise of trusted third-party vendors or software to infiltrate multiple organizations, increasing attack surface.

### Malware-Related Threats

Various malicious software including trojans, spyware, and info-stealers targeting sensitive data and systems.

### OT/Zero-Day Exploits

Attacks exploiting vulnerabilities in operational technology and previously unknown software flaws to disrupt critical systems.

# Top Threats by Sector

**Critical Infrastructure**

Advanced Persistent Threats (APTs), Insider Threats, Zero-Day Exploits in OT systems are primary concerns targeting energy, utilities, and oil/gas sectors.

**Education**

Phishing for Credentials, Spyware and Keyloggers, Social Engineering Scams dominate threats targeting educational institutions.

**Manufacturing**

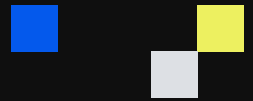
Industrial Espionage via Malware, Supply Chain Compromise, and OT System Exploits are critical threats impacting manufacturing.

**Retail**

Point-of-Sale (PoS) Malware, E-commerce Skimming (Magecart), and Credential Harvesting are prevalent attacks in retail.

**Healthcare**

Data Breaches via Phishing, Insider Threats, and Medical Device Vulnerabilities remain top threats to healthcare sector security.



# Top Threat Actors Overview

## Cl0p

Active in 7 sectors including Healthcare, Government, Finance, Education, Manufacturing, Retail, and Tech. Uses zero-day exploits like MOVEit and GoAnywhere, and employs double extortion tactics.

## RansomHub

Targets 6 sectors such as Government, Finance, Manufacturing, Retail, Critical Infrastructure, and Tech. Utilizes custom ransomware, RDP/VPN exploits, and EDR evasion techniques like EDRKillshifter.

## LockBit

Operates in 4 sectors: Government, Finance, Education, Manufacturing. Known for Ransomware-as-a-Service (RaaS), exploiting weak passwords and unpatched systems globally (excludes Russia/CIS).

## PLAY

Targets Government, Finance, Education, and Critical Infrastructure. Uses double extortion, Cobalt Strike, and Linux-based ESXi attacks with zero-day exploits since 2022.

## Akira

Active in 3 sectors: Government, Critical Infrastructure, Tech. Employs cross-platform ransomware, RDP/VPN exploits, and phishing. Reported earnings exceed $42M from over 250 attacks.

# Sector: Healthcare Threat Actors

**Qilin**

Targets 12.2% of attacks on healthcare; uses spear-phishing, Cobalt Strike, and double extortion.

**Incransom (INC)**

25.4% of attacks hit healthcare; focuses on small providers, exploits CVE-2023-3519.

**Everest**

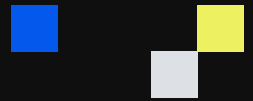
57.1% focus on healthcare; employs double extortion, targets vulnerable systems.

**BianLian**

60% of victims in healthcare; exploits RDP, unpatched vulnerabilities.

**Medusa**

Names 15 victims in Q1 2025; uses phishing, CVE-2024-1709 exploits.



# Sector: Government Threat Actors

**PLAY**

Targets government since 2022; uses Cobalt Strike, exploits unpatched software to infiltrate and disrupt government operations.

**LockBit**

Global government targeting (excludes Russia/CIS); exploits weak passwords and operates a Ransomware-as-a-Service (RaaS) model for persistent attacks.

**RansomHub**

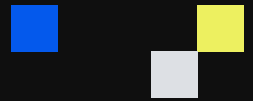
Hits critical infrastructure including government; utilizes RDP/VPN exploits and custom ransomware to compromise systems.

**Cl0p**

Exploits zero-day vulnerabilities such as MOVEit; impacts government data with double extortion ransomware attacks.

**Akira**

Targets government entities via RDP/VPN weaknesses; has generated over $42M from 250+ attacks using cross-platform ransomware and phishing.



# Sector: Finance Threat Actors

**Cl0p**

Extorted $500M+; targets finance via MOVEit, GoAnywhere vulnerabilities.

**LockBit**

Hits finance, avoids Russia/CIS; uses sandbox evasion, email filters.

**PLAY**

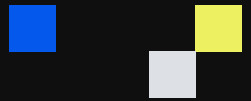
Targets finance with double extortion, Cobalt Strike for lateral movement.

**RansomHub**

Focuses on finance as critical infrastructure; custom ransomware, RDP exploits.

**ALPHV (BlackCat)**

Rust-based ransomware; creative, complex attacks on finance.



# Sector: Education Threat Actors

**LockBit**

Frequently targets universities and schools; exploits weak passwords, unpatched systems.

**PLAY**

Hits education with double extortion; targets sensitive student data.

**Rhysida**

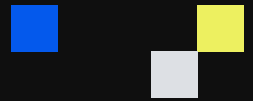
Specializes in education; known for K-12 and university attacks, uses phishing.

**Cl0p**

Exploits MOVEit vulnerabilities; impacted education institutions in 2023-2024.

**Medusa**

Targets education alongside healthcare; uses CVE-2024-1709, phishing.



# Sector: Manufacturing Threat Actors

**Cl0p**

Targets manufacturers via MOVEit, GoAnywhere; disrupts supply chains.

**LockBit**

Hits manufacturing globally; exploits OT systems, unpatched software.

**Qilin**

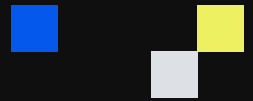
Active in manufacturing; uses spear-phishing, double extortion.

**RansomHub**

Targets industrial sectors; custom ransomware, RDP/VPN exploits.

**BianLian**

Exploits manufacturing’s legacy systems; focuses on RDP vulnerabilities.



# Sector: Retail Threat Actors

**ALPHV (BlackCat)**

Targets retail for payment data; uses Rust-based ransomware and phishing techniques to compromise systems.

**RansomHub**

Employs spear-phishing and double extortion; targets e-commerce staff with fake customer support emails to infiltrate systems.

**Cl0p**

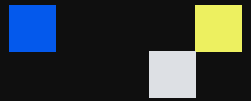
Exploits MOVEit vulnerabilities; sends malicious links mimicking retail platforms to steal payment information.

**Lynx**

Emerging group claiming retail victims in 2024; uses custom encryptors and evades endpoint detection and response (EDR) systems.

**Scattered Spider**

Focuses on rapid exploitation via SMS phishing and fake Okta login pages, targeting retail employees for credential theft.



# Sector: Critical Infrastructure Threat Actors

**RansomHub**

Targets energy/utilities; uses EDRKillshifter and RDP/VPN exploits to infiltrate critical infrastructure systems.

**PLAY**

Hits critical infrastructure with Linux-based ESXi attacks and zero-day exploits, focusing on operational disruption.

**Akira**

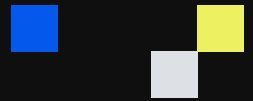
Targets energy with double extortion tactics, phishing campaigns, and exploits ESXi vulnerabilities for maximum impact.

**Qilin**

Claimed attacks on U.S. satellite communications and energy firms; uses spear-phishing and data exfiltration techniques.

**Hunters International**

Conducts methodical high-stakes attacks on critical infrastructure, focusing on energy and utilities sectors.



# Sector: Technology/IT Threat Actors

**Medusa**

Targets tech with phishing; uses CVE-2024-1709, fake SaaS login pages for credential theft.

**Cl0p**

Distributes trojans; exploits GoAnywhere, phishing for software supply chain attacks.

**RansomHub**

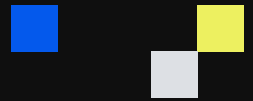
Uses spear-phishing, smishing; targets developers with fake code repository alerts.

**Akira**

Deploys spyware; uses spear-phishing for IP theft, mimics tech support emails.

**FOG**

Targets tech alongside other sectors; over 100 victims, uses cloud-based lures.



# Top Phishing Tactics by Sector

**Credential Harvesting**

Fake login pages target users across sectors including healthcare, government, finance, education, manufacturing, retail, critical infrastructure, and tech to steal credentials.

**Spear-Phishing**

Tailored phishing attacks exploit specific roles or data in seven sectors: healthcare, government, finance, education, manufacturing, retail, and critical infrastructure.

**Business Email Compromise (BEC)**

Spoofed emails target financial or operational actions, appearing in seven sectors such as healthcare, government, finance, manufacturing, retail, critical infrastructure, and tech.

**Malware Delivery via Phishing**

Emails deliver keyloggers, spyware, or other malware to victims across seven sectors including healthcare, government, finance, education, manufacturing, retail, and critical infrastructure.

**Smishing**

SMS-based phishing attacks target mobile users in seven sectors: healthcare, government, finance, education, manufacturing, retail, and critical infrastructure.

# Top 5 TTPs Overview

### Email Spoofing (T1566.001)

Attackers forge sender addresses to mimic trusted entities (e.g., executives, vendors), commonly used in Business Email Compromise (BEC) and spear-phishing attacks.

### Malicious Links/Attachments (T1204.002)

Emails or SMS contain links to fake login pages or attachments with embedded malware, widely used in credential harvesting and malware delivery.

### Social Engineering (T1566)

Crafting convincing messages using personal or contextual details (e.g., patient data, invoice numbers) to deceive users, a core element of spear-phishing and BEC tactics.

### Domain Spoofing (T1583.001)

Creating lookalike domains (e.g., bankofamerica-login.com) to host fake portals, facilitating credential harvesting attacks.

### Exploitation of Trusted Relationships (T1199)

Leveraging compromised accounts or trusted vendor relationships to send phishing emails, increasing the success rate of BEC and spear-phishing campaigns.

# Phishing TTPs by Sector

| | |
|---|---|
| **Healthcare** | Spear-Phishing for patient data, BEC targeting hospital admins, credential harvesting via fake EHR portals, malware delivery via phishing emails, smishing for staff credentials. Threat actors include Qilin, Incransom, Medusa, Scattered Spider, Volt Typhoon. |
| **Government** | BEC spoofing officials, spear-phishing for employee credentials, smishing targeting public servants, malware via fake policy updates, credential harvesting via spoofed SSO pages. Threat actors include LockBit, Sandworm, ChamelGang, Cyber Army of Russia, NoName057(16). |
| **Finance** | Credential harvesting via fake banking portals, BEC for wire fraud, spear-phishing targeting financial advisors, smishing for account access, malware via phishing links. Threat actors include LockBit, RansomHub, Cl0p, Scattered Spider, Lazarus Group. |
| **Education** | Phishing for student/faculty credentials, social engineering scams for tuition fraud, spear-phishing targeting research data, smishing aimed at students, malware via fake academic links. Threat actors include Rhysida, Medusa, LockBit, Scattered Spider, Volt Typhoon. |

# DDoS/DOS Top Threat Actors

**NoName057(16)**

Known for slow DoS and TCP floods attacks, targeting government, healthcare, and critical infrastructure sectors, often motivated by geopolitical conflicts.

**KillNet**

Focuses on TCP SYN floods and application-layer attacks, primarily disrupting healthcare, government, and financial services aligned with Russian interests.

**Anonymous Sudan**

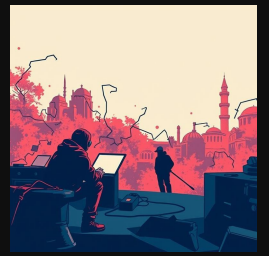
Uses volumetric UDP floods and botnets to launch hyper-volumetric DDoS attacks mainly targeting healthcare, retail, education, and energy sectors with hacktivist motives.

**Cyber Army of Russia**

Conducts multi-vector DDoS campaigns including HTTP floods and SSDP amplification, targeting government, healthcare, critical infrastructure, and finance for political disruption.

**Sandworm (APT)**

A Russia-linked advanced persistent threat group deploying volumetric and protocol attacks focusing on critical infrastructure, government, and manufacturing sectors.



# DDoS TTPs and Sector Threats

**Volumetric Attacks (T1498.002)**

These attacks saturate bandwidth using UDP/TCP floods and amplification techniques like SSDP, overwhelming network capacity and causing service outages across sectors.

**Application-Layer Attacks (T1498.001)**

HTTP floods and slow DoS attacks exhaust server resources by targeting application layers, degrading service availability for government, finance, and healthcare sectors.

**Protocol Attacks (T1498)**

TCP SYN/ACK floods exploit network protocol weaknesses to disrupt communications, affecting critical infrastructure and technology sectors with targeted network disruptions.

**Botnet Usage (T1584.005)**

Attackers leverage botnets like Mirai and cloud-based virtual machines to launch hyper-volumetric DDoS attacks, amplifying attack scale and complexity across all major sectors.

# Sector DDoS Threat Breakdown

### Healthcare DDoS TTPs & Actors

Volumetric (UDP Floods), Application-Layer (HTTP Floods), Slow DoS (Slowloris), Protocol (TCP SYN Floods), Botnets (Mirai). Actors: Anonymous Sudan, KillNet, Cyber Army of Russia, NoName057(16), RansomHub.

### Finance DDoS TTPs & Actors

Application-Layer (HTTP Request Smuggling), Volumetric (UDP Floods), Protocol (TCP SYN Floods), Slow DoS (Slowloris), Botnets (IoT). Actors: NoName057(16), KillNet, Anonymous Sudan, Darknet Parliament, Cyber Army of Russia.

### Government DDoS TTPs & Actors

Volumetric (SSDP Amplification), Application-Layer (HTTP Floods), Protocol (TCP SYN/ACK Floods), Slow DoS (RUDY), Botnets (Cloud VMs). Actors: NoName057(16), Cyber Army of Russia, KillNet, Anonymous Sudan, Mysterious Team Bangladesh.

### Education DDoS TTPs & Actors

Volumetric (UDP Floods), Application-Layer (HTTP Floods), Protocol (TCP SYN Floods), Slow DoS (Slow HTTP POST), Tool Usage (Raven Storm). Actors: Anonymous Sudan, NoName057(16), KillNet, Mysterious Team Bangladesh, Cyber Army of Russia.

# Sector DDoS Threat Breakdown Continued

| | |
|---|---|
| **Manufacturing** | TTPs: HTTP Floods, SSDP Amplification, TCP ACK Floods, Slowloris, Spear-Phishing for DDoS setup. Threat Actors: NoName057(16), KillNet, RansomHub, Anonymous Sudan, Laurionite use volumetric floods, TCP floods, spear-phishing, and slow DoS attacks. |
| **Retail** | TTPs: UDP Floods, HTTP Floods, TCP SYN Floods, HTTP Request Smuggling, SMS Phishing for Botnet Recruitment. Threat Actors: Anonymous Sudan, NoName057(16), KillNet, Scattered Spider, DragonForce use floods, smishing, and application-layer DDoS to disrupt retail platforms. |
| **Critical Infrastructure (Energy, Utilities, Oil/Gas)** | Threat Actors: Cyber Army of Russia, NoName057(16), Sandworm, CYBERAV3NGERS, Anonymous Sudan. TTPs: SSDP Amplification, HTTP Floods, TCP SYN/ACK Floods, Mirai Botnets, SCADA-Specific Floods used to disrupt grids and OT systems. |
| **Technology/IT** | Threat Actors: NoName057(16), KillNet, Anonymous Sudan, RansomHub, Darknet Parliament. TTPs: API-Targeted HTTP Floods, UDP Floods, TCP SYN Floods, Slowloris, Cloud-based Botnets used to disrupt SaaS, cloud, and tech infrastructure. |

# Top Malware Threats Overview

### Trojans

LockBit: Black Basta, Cl0p: Dridex, Qilin: DarkGate, Lazarus Group (APT): AppleJeus, FIN7: Carbanak

### Spyware

Medusa: AgentTesla, Volt Typhoon (APT): ShadowPad, RansomHub: NetSupport RAT, Rhysida: Remcos, Scattered Spider: Vidar

### Info-Stealers

Cl0p: Lumma Stealer, LockBit: RedLine Stealer, ALPHV (BlackCat): Raccoon Stealer

### Wipers

Sandworm (APT): WhisperGate, Industroyer2, CYBERAV3NGERS: BiBi Wiper

### PoS Malware

Cl0p: SocGholish (Magecart variant), FIN6: FrameworkPOS

# Malware Threats by Sector

### Healthcare

TTPs: Spear-Phishing (T1566.001), Exploit Public-Facing Apps (T1190) like CVE-2024-1709, PowerShell execution (T1059), Data Exfiltration (T1041), Obfuscated Files (T1027). Threat Actors: Qilin, Medusa, Cl0p, Volt Typhoon, FIN11 targeting EHR systems and patient data.

### Finance

TTPs: Spear-Phishing (T1566.001), Exploit Public-Facing Apps (T1190), Command & Control (T1071), Credential Dumping (T1003), Obfuscated Files (T1027). Threat Actors: Cl0p, Lazarus Group, LockBit, FIN7, RansomHub using banking trojans & info-stealers.

### Government Entities

TTPs: Phishing (T1566), User Execution (T1204.002), RDP Lateral Movement (T1021), Data Destruction (T1485), Credential Dumping (T1003). Threat Actors: Sandworm, LockBit, ChamelGang, TA505, NoName057(16) deploying trojans, wipers, spyware.

### Education

TTPs: Phishing (T1566), User Execution (T1204.002), Data Exfiltration (T1041), Exploit Public-Facing Apps (T1190), Persistence (T1547). Threat Actors: Rhysida, Medusa, LockBit, Volt Typhoon, Cobalt Group targeting student & research data.

# Malware Threats by Sector Continued

### Manufacturing TTPs & Actors

Spear-Phishing with fake vendor emails, Exploit OT Systems targeting ICS/SCADA, Lateral Movement via SMB, Data Exfiltration of trade secrets, and Impair Defenses disabling EDR/AV. Actors: Sandworm, Qilin, LockBit, ChamelGang, Laurionite.

### Critical Infrastructure TTPs & Actors

Spear-Phishing with fake maintenance alerts, Exploit OT Systems targeting SCADA/PLC, Data Destruction via wipers, Lateral Movement over RDP, and Command & Control for persistence. Actors: Sandworm, Volt Typhoon, CYBERAV3NGERS, ChamelGang, Laurionite.

### Retail TTPs & Actors

Phishing with fake order confirmations, Smishing for malware delivery, Exploit Public-Facing Apps targeting APIs & e-commerce, Data Exfiltration of payment data, and Code Injection via Magecart. Actors: ALPHV, Cl0p, Scattered Spider, RansomHub, FIN6.

### Technology/IT TTPs & Actors

Spear-Phishing with fake software updates, Exploit Public-Facing Apps from cloud misconfigs, Data Exfiltration targeting IP & client data, Code Injection in SaaS apps, and Persistence via scheduled tasks. Actors: Medusa, Cl0p, Lazarus Group, Volt Typhoon, RansomHub.