



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

March 8, 2025

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 6:00 AM (EST) on March 6, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 Cyber and Dark Web Intelligence Key Findings	3
Cybercriminals Use Tech Support Scam to Deploy Ransomware	3
Operator of Darknet Market Nemesis Sanctioned for Synthetic Opioid Sales	4
Polish Space Agency POLSA Hit by Cyberattack	4
 Exploit and Vulnerability Intelligence Key Findings	6
CVE-2025-22224	7
CVE-2025-1914	7
 Ransomware and Breach Intelligence Key Findings	10
Ransomware Overview: Top Actors, Industry Impact, and Key Updates	10
Data Breaches Hit Football Club, Media, and Tech Giants	13
 Physical and Geopolitical Intelligence Key Findings	15
Physical Security Intelligence: Global	15
Physical Security Intelligence: United States	16
 Appendix A: Traffic Light Protocol for Information Dissemination	17
 Appendix B: ZeroFox Intelligence Probability Scale	18

| **Cyber and Dark Web Intelligence** |

| Cyber and Dark Web Intelligence Key Findings



Cybercriminals Use Tech Support Scam to Deploy Ransomware

What we know:

- Cybercriminals have been impersonating tech support to gain access to victims' systems via emails and popular collaboration applications and deploy ransomware from groups like Black Basta and Cactus.
- The scam involves bombarding the target systems with emails, following which the owner of the system gets a call, seemingly from IT support, asking them to grant the support assistant access to the system.
- Once the attacker (disguised as the support assistant) gains access to the system, they download harmless-looking malicious files that deploy a backdoor called BackConnect, giving the attacker complete control over the system.

What is next:

- If cybercriminals gain access to the victims' computers, they could likely install ransomware to lock files and demand ransom.
- They are also likely to steal sensitive data, monitor activities, or use the compromised system for further attacks.
- Threat actors may also access third-party information stored in the infiltrated systems, which could be leveraged in extortion scams.
- Once an actor has gained access to a system, they could sell that access to other threat actors, who could leverage it in cyber espionage activities.

Background:

- Researchers have found close links between the BackConnect backdoor and Black Basta's ransomware attacks.
- The support scam has reportedly been active since 2024 and has claimed multiple targets, including organizations in North America—a significant number of which are located in the United States.

Recommendations:

- Users of popular collaboration applications must watch out for email bombardment or any other similar unusual activity and report it to their respective IT desks immediately.
- It is also important to verify calls or messages seemingly from IT support.

**Operator of Darknet Market Nemesis Sanctioned for Synthetic Opioid Sales****What we know:**

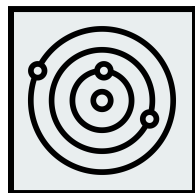
- The U.S. Treasury Department has sanctioned the sole administrator of darknet market Nemesis, which facilitated the sale of nearly USD 30 million worth of drugs around the world between 2021 and 2024—including to the United States.

Background:

- Nemesis was the subject of an international law enforcement operation and was taken down in 2024. Before its takedown by law enforcement, the market—which had built-in money laundering features—had over 30,000 active users and 1,000 vendors, including narcotics traffickers and cybercriminals who openly traded in illegal drugs and services.

Analyst note:

- Dark web marketplaces are accessed via anonymity-enhancing browsers. This anonymity facilitates illicit activities that are not restricted to the cyber realm and extend to crimes such as drug and human trafficking, physical violence services, and the sale of false identification documents. There are very likely more marketplaces akin to Nemesis that engage in malicious activities, which could have physical repercussions for targeted victims.

**Polish Space Agency POLSA Hit by Cyberattack****What we know:**

- The Polish Space Agency (POLSA) experienced a cyberattack in which threat actors reportedly gained unauthorized access to its IT infrastructure.

Background:

- The targeted POLSA systems were secured, and authorities launched “intensive operational activities” to identify the perpetrators of the attack. Warsaw has previously accused Moscow of targeting Polish systems to destabilize the country, as Poland actively supplies military aid to Ukraine.

Analyst note:

- Given the Polish stance in the Russia–Ukraine war and POLSA’s close association with the European Space Agency (ESA), it is likely that the threat actors in this incident are politically motivated. Additionally, last month, a Polish astronaut was included in a crew that will participate in Ignis, a joint venture between POLSA and the ESA, thereby further solidifying Poland’s relationship with several European allies of Ukraine.

| **Exploit and Vulnerability Intelligence** |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. On March 4, 2025, the Cybersecurity and Infrastructure Security Agency (CISA) [released eight Industrial Control Systems \(ICS\) advisories](#). These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. This advisory addressed several flaws, including those that could allow a malicious actor to execute arbitrary code with escalated privileges, achieve remote code execution, and access files or directories outside the authorized scope. CISA also added a total of nine vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on [March 3](#) and [March 4, 2025](#). Meanwhile, [Qualcomm released a security advisory](#) addressing many vulnerabilities involving memory corruption issues—with some of them assigned critical severity. [MediaTek also released details of security vulnerabilities](#) and patches affecting MediaTek Smartphone, Tablet, AIoT, Smart display, and Smart platform, among others. For Qualcomm and MediaTek, the companies have informed original equipment manufacturers to incorporate patches at the time of manufacturing. [WordPress URL Media Uploader plugin is vulnerable](#) (CVE-2025-1662) to Server-Side Request Forgery. This enables authenticated attackers with author-level access and above to make web requests to arbitrary locations originating from the web application, which can be used to query and modify information from internal services.



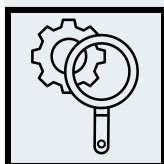
CRITICAL

CVE-2025-22224

What happened: Patches have been released for three previously exploited VMware zero-day vulnerabilities: CVE-2025-22224 (VMCI heap overflow), CVE-2025-22225 (ESXi arbitrary write), and CVE-2025-22226 (HGFS flaw allowing memory leaks).

- **What this means:** These flaws could enable attackers with admin or root access to escape the virtual machine sandbox and take full control over affected VMware environments, including ESXi, vSphere, Workstation, Fusion, and cloud-based platforms.
- **Affected products:**
 - VMware ESXi
 - VMware Workstation Pro / Player (Workstation)
 - VMware Fusion
 - VMware Cloud Foundation

- VMware Telco Cloud Platform



HIGH

CVE-2025-1914

What happened: Google has patched this out-of-bounds memory access vulnerability in V8 in Google Chrome.

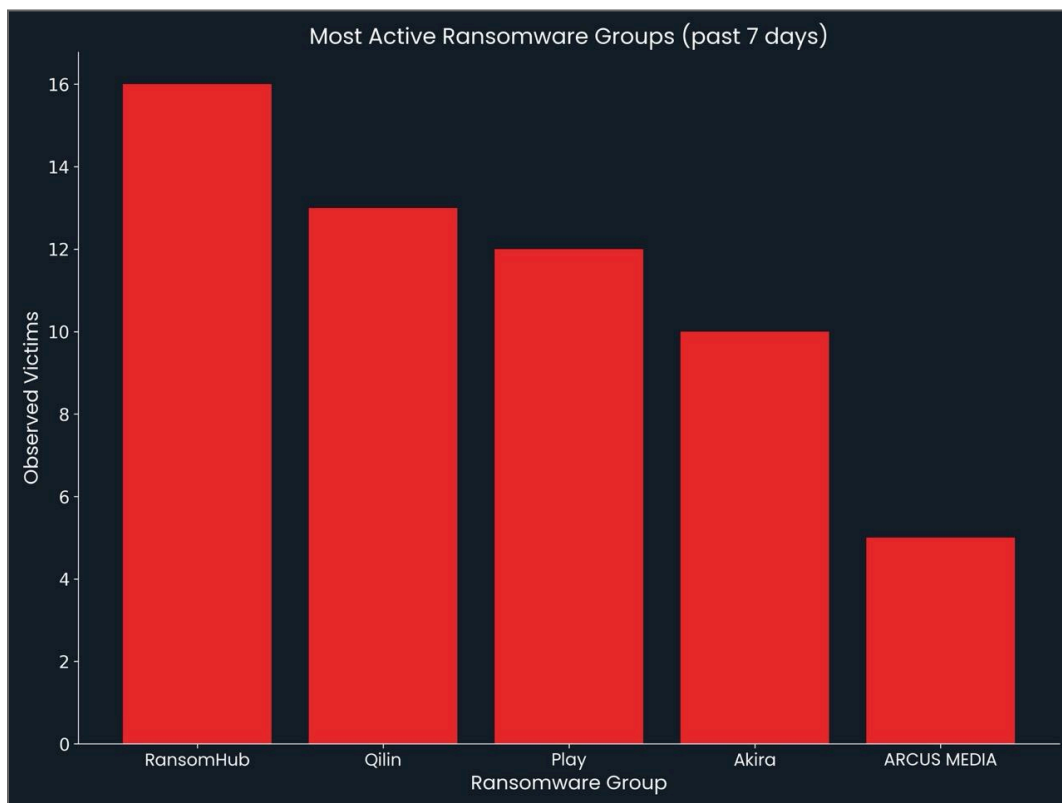
- **What this means:** Threat actors could exploit this bug to steal sensitive data or help them bypass browser security by tricking users into visiting a malicious website.
- **Affected products:**
 - V8 in Google Chrome versions prior to 134.0.6998.35

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

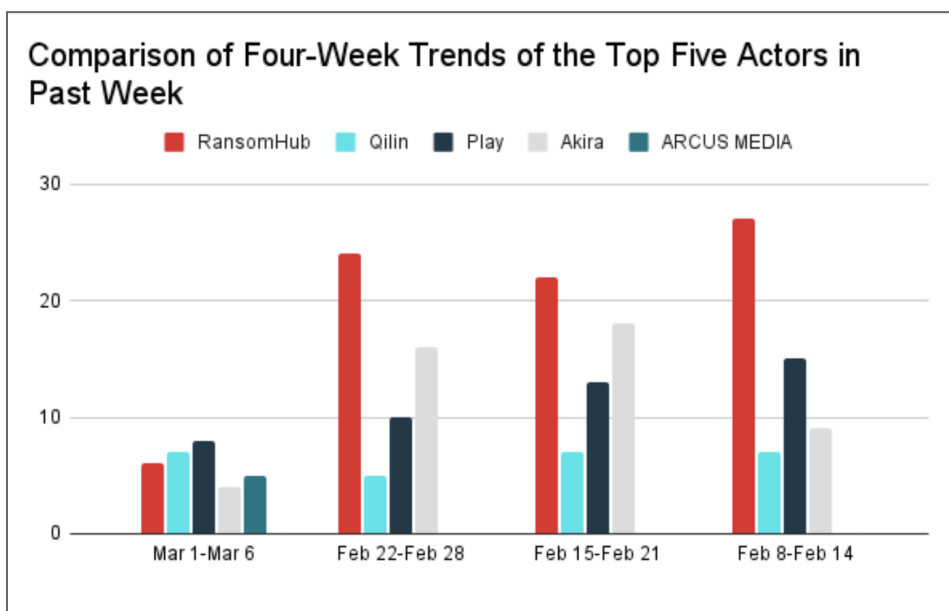


Ransomware Overview: Top Actors, Industry Impact, and Key Updates



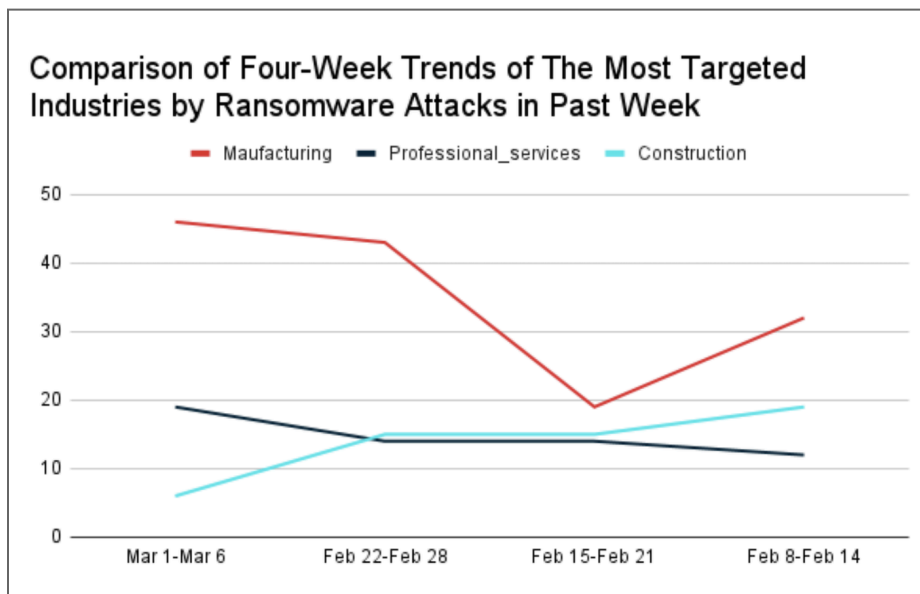
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, RansomHub, Qilin, Play, Akira, and ARCUS MEDIA were the most active ransomware groups. ZeroFox observed at least 224 ransomware victims disclosed, most of which were located in North America. The RansomHub ransomware group accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

- **What this means:** Over the past four weeks, RansomHub has been the most active group, carrying out at least 79 attacks, followed by the Akira and Play ransomware groups. Based on recent trends, it is likely that RansomHub will maintain or even increase its attack frequency in the near term.



Source: ZeroFox Internal Collections

Ransomware trends in industries: Over the past four weeks, ZeroFox has observed that the majority of ransomware victims belong to the manufacturing sector, followed by the professional services sector. The manufacturing sector, in particular, has consistently seen a high number of attacks, with at least 140 incidents recorded (over the four weeks).

Recap of major ransomware events observed in the past week: Canada's largest zoo, Toronto Zoo, [has disclosed further details](#) about the data stolen in a January 2024 ransomware attack that affected personal and financial information of its employees, former employees, volunteers, and donors. A subsidiary of Indian multinational Tata has reportedly been targeted by the Hunters International ransomware gang, which claims to have stolen 730,160 files totaling 1.4 TB. The group is [threatening to release the data unless a ransom is paid](#) but has not publicly disclosed the amount or provided supporting documents. Scammers are [posing as the BianLian ransomware group](#), sending fake ransom notes to U.S. companies through traditional mail via the United States Postal Service (USPS). Russian-speaking ransomware group [Qilin has claimed responsibility](#) for the cyberattack that disrupted Lee Enterprises' operations in early February. Threat actors using Black Basta and Cactus ransomware are [utilizing the same BackConnect module](#) to maintain control over infected hosts, suggesting that affiliates from Black Basta may have shifted to Cactus.



Data Breaches Hit Football Club, Media, and Tech Giants

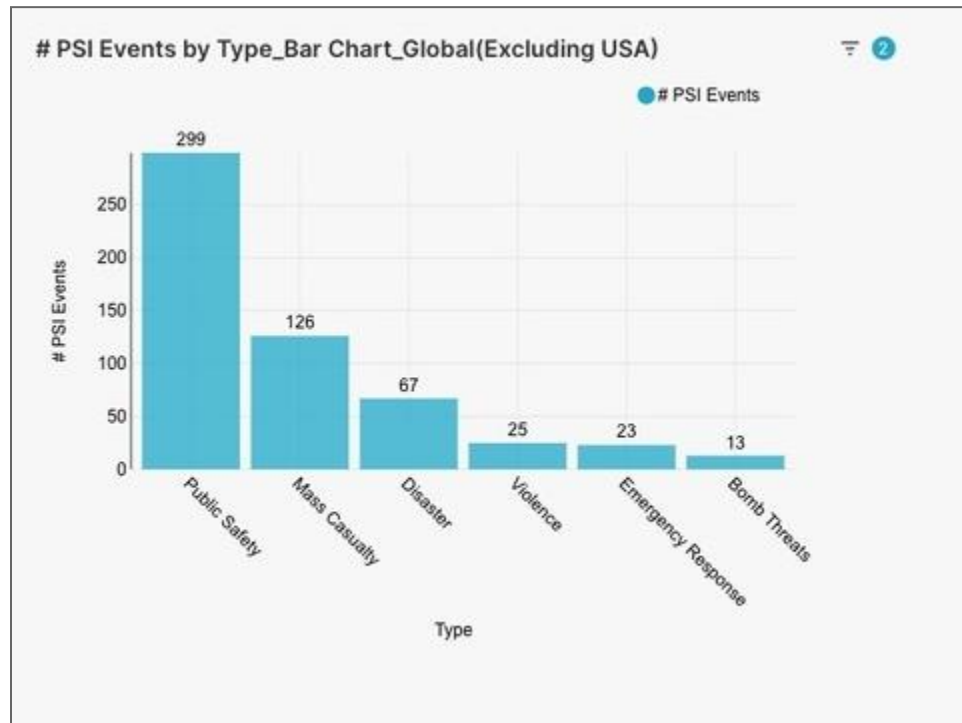
Targeted Entity	Leeds United Football Club	HighWire Press	Renesas Electronics Corporation
Amount of Compromised Data	Yet to be determined	26 million rows of data	11,000 confidential files
Compromised Data Fields	Payment card details	Not disclosed	Confidential future product plans, source codes (c/c++) for various Renesas products, engineering and design blueprints, internal research documents, invoices & financial data, internal business communications, and emails
Suspected Threat Actor	Yet to be determined	Grep	Rey
Country	United Kingdom	United States	Japan
Industry	Media/Entertainment	Media/Entertainment	Technology
Possible Repercussions	Financial losses, credit card fraud, carding, skimming, card-not-present (CNP) fraud, and transaction manipulation	Identity theft, phishing attacks, intellectual property theft, financial fraud, social engineering, malware attacks, and ransomware	Intellectual property theft, corporate espionage, ransomware attacks, supply chain attacks, financial fraud, phishing attacks, and social engineering

Three major breaches observed in the past weeks

| Physical and Geopolitical Intelligence |

| Physical and Geopolitical Intelligence Key Findings

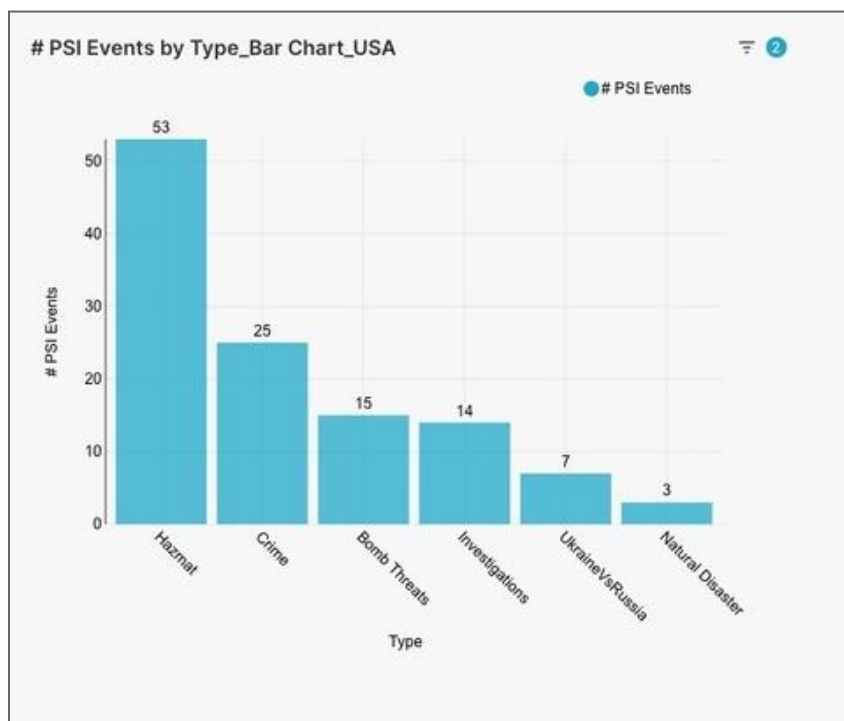
Physical Security Intelligence: Global



Source: ZeroFox Internal Collections

In the past week, ZeroFox observed at least 299 alerts about public safety events around the globe and at least 126 alerts related to mass casualty events. On February 23, 2025, Germany held general elections, with the Christian Democratic Union (CDU) led by Friedrich Merz winning the most votes (around 28 percent). The CDU and the Social Democrats (SPD) of outgoing Chancellor Olaf Scholz, who won 16 percent of the vote, are now [very likely to form a coalition government](#). Two smaller parties failed to get above 5 percent, and now their votes will be shared among the larger parties in Parliament. This will allow the CDU and SPD to form a two-party coalition without needing a third party to gain a majority.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

ZeroFox observed at least 53 hazmat-related alerts and at least 25 crime-related alerts in the United States in the past week. According to a senior administration official, the United States is [temporarily halting all aid to Ukraine](#) until Ukraine demonstrates its “commitment to peace negotiations with Russia.” The order reportedly takes effect immediately. It will impact more than USD 1 billion in arms and ammunition plus aid worth millions of dollars, which could have facilitated Ukraine’s purchase of military equipment directly from U.S. defense companies. Meanwhile, CISA has clarified misunderstandings regarding a [directive to halt offensive cyber operations against Russia](#), stating that it continues to monitor “all cyber threats to U.S. Critical Infrastructure, including from Russia.” On March 4, 2025, [President Donald Trump delivered a nearly two-hour address](#) to a joint session of Congress, marking six weeks into his second term. He addressed topics like immigration, tariffs, inflation, and the economy and declared that “America is back.” Additionally, President Trump addressed a message from Ukrainian President Volodymyr Zelenskyy regarding ongoing negotiations with Russia, indicating a potential shift in U.S. involvement.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%