



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

February 24, 2025

Scope Note

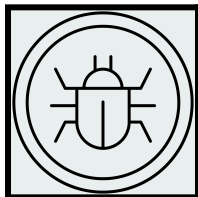
ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary 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 12:00 PM (EST) on February 21, 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
New Malware Used in Cyber Espionage Campaign Against a South American Ministry	3
Russian Threat Actor Targets Cloud Service Accounts with Device Code Phishing	3
Venture Capital Firm Targeted in Social Engineering Attack	4
 Exploit and Vulnerability Intelligence Key Findings	6
CVE-2024-12356	6
CVE-2025-1265	7
 Ransomware and Breach Intelligence Key Findings	9
This Week's Focus: CISA Releases Advisory on Ghost Ransomware	9
Genea Investigates Breach After Suspicious Network Activity	10
 Physical and Geopolitical Intelligence Key Findings	12
Physical Security Intelligence: Global	12
Physical Security Intelligence: United States	13
 Appendix A: Traffic Light Protocol for Information Dissemination	15
 Appendix B: ZeroFox Intelligence Probability Scale	16

| **Cyber and Dark Web Intelligence** |

| Cyber and Dark Web Intelligence Key Findings



New Malware Used in Cyber Espionage Campaign Against a South American Ministry

What happened: Threat actors have been using a new malware strain called FinalDraft in a sophisticated cyber espionage campaign to target the foreign ministry of a South American country. The malware is known to exploit email drafts for covert communication, enabling attackers to exfiltrate data, inject malicious code, and access different systems while avoiding detection.

- **What this means:** FinalDraft evades traditional security measures by hiding commands in email drafts instead of sending them to receivers, thereby also making forensic analysis difficult. The attackers also stored stolen OAuth tokens in databases comprising settings information for persistent access, enabling long-term espionage. Infrastructure analysis revealed links to telecommunications providers and a Southeast Asian university's storage system, likely suggesting that the campaign orchestrators have breached and compromised other supply chains, indicating a wider scale of attack.

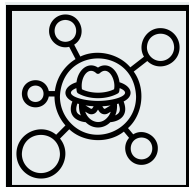


Russian Threat Actor Targets Cloud Service Accounts with Device Code Phishing

What happened: A Russian-linked threat actor tracked as Storm-237 has been targeting user accounts of a popular cloud-based subscription service through device code phishing, impersonating trusted individuals to gain access to sensitive information across multiple sectors.

- **What this means:** This phishing campaign has been ongoing since August 2024 and primarily targets individuals in government, non-governmental organizations (NGOs), IT services, defense, telecommunications, health, and energy sectors in Europe, North America, Africa, and the Middle East. The attackers impersonate prominent individuals relevant to the victim's organization via messaging platforms like WhatsApp, Signal, or the organization's collaboration application, building rapport before sending fake meeting invitations—making it harder for victims to recognize malicious intent. By exploiting a commonly used authentication method, this attack bypasses security measures and targets critical sectors—leaving them vulnerable to data theft, espionage, or disruption.

Meanwhile, [Russian threat actors have been conducting phishing campaigns](#) that take advantage of the legitimate "Linked Devices" feature in the Signal messaging app to gain unauthorized access to targeted accounts.



Venture Capital Firm Targeted in Social Engineering Attack

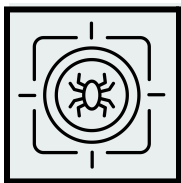
What happened: Investigations continue as venture capital firm Insight Partners recently suffered a social engineering attack. [The company confirmed third-party access](#) to its information systems but has not yet determined the entire scope of the incident.

- **What this means:** Insight Partners is a venture capital firm managing over USD 90 billion in regulatory assets with investments in more than 800 software companies, which may attract threat actors looking to target data related to its employees, financial processes, and trade secrets. If the threat actor gains access to the company's databases, they are likely to exfiltrate it and leverage this information against Insight Partners in ransomware attacks. Additionally, the threat actor is likely to advertise possession of data or initial access on deep and dark web forums to garner the interest of other financially motivated actors.

| **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. The Cybersecurity and Infrastructure Security Agency (CISA) released a total of nine industrial control system (ICS) advisories on [February 18](#) and [February 20](#). CISA also added four [vulnerabilities](#) to its [Known Exploited Vulnerabilities \(KEV\) catalog](#). Microsoft mitigated a [high-severity elevation of privilege vulnerability](#) (CVE-2025-24989) in Power Pages, which hackers exploited as a zero-day in attacks. [Palo Alto Networks warned](#) that attackers are chaining CVE-2025-0111 with CVE-2025-0108 and CVE-2024-9474 to exploit PAN-OS firewalls. Researchers warned about [two security flaws \(CVE-2025-26465 and CVE-2025-26466\)](#) in OpenSSH that could enable machine-in-the-middle (MitM) and denial-of-service (DoS) attacks under specific conditions. Atlassian released [patches for 12 critical and high-severity flaws](#) in Bamboo, Bitbucket, Confluence, Crowd, and Jira.



CRITICAL

CVE-2024-12356

What happened: A critical vulnerability has been discovered in Privileged Remote Access (PRA) and Remote Support (RS) products, which can allow an unauthenticated attacker to inject commands that are run as a site user.

- **What this means:** The vulnerability in PRA and RS products allows unauthenticated attackers to exploit the flaw by injecting malicious commands into the system. These commands would execute with the privileges of a site user, enabling the attacker to perform unauthorized actions or access sensitive information, leading to possible data breaches or other forms of compromise on the system.
- **Affected products:**
 - RS and PRA 24.3.1 and earlier

**CRITICAL****CVE-2025-1265**

What happened: An OS command injection vulnerability exists in Elseta's Vinci Protocol Analyzer with a CVSS score of 9.9/10.0. The impacted product is deployed in critical manufacturing and communications systems across the globe.

- **What this means:** Successful exploitation of this vulnerability could allow an attacker to escalate privileges and perform code execution on the affected system. Elseta recommends affected users update to version 3.2.3.19 or later.

Affected products:

- Vinci Protocol Analyzer versions prior to 3.2.3.19

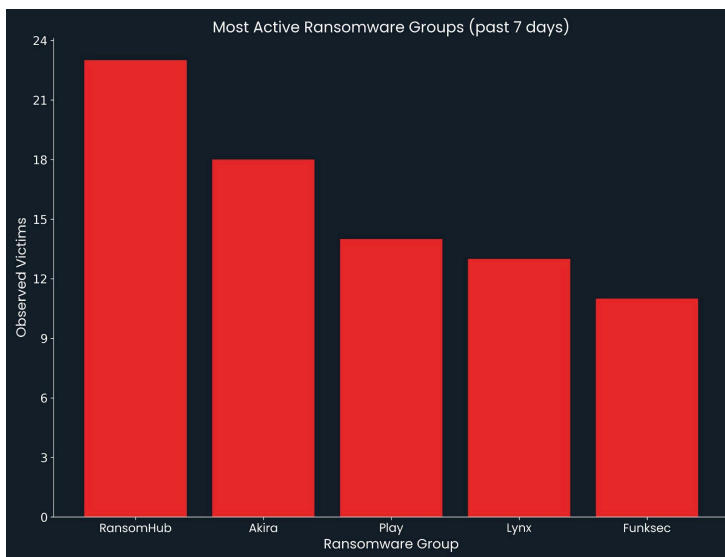
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



This Week's Focus: CISA Releases Advisory on Ghost Ransomware

What happened: This week, ZeroFox observed at least 142 ransomware victims disclosed, most of which were located in North America; the manufacturing sector was the most affected followed by construction and healthcare, while the most active group was the RansomHub ransomware group. CISA and partners have released an advisory addressing the FBI's observations about known Ghost ransomware indicators of compromise and tactics, techniques, and procedures identified through investigations as recently as January 2025. The joint advisory addresses threat actors using Ghost ransomware to obtain initial access to networks by exploiting applications associated with multiple Common Vulnerabilities and Exposures (CVEs), including CVE-2018-13379, CVE-2010-2861, and CVE-2009-3960.



Source: ZeroFox Internal Collections

- **What this means:** Ghost ransomware actors are still actively exploiting vulnerabilities—some of which date back over a decade—indicating that many organizations have yet to patch known weaknesses. The ransomware group has been proliferating since 2021 and is likely specifically targeting organizations with outdated versions of software and firmware on their internet-facing services, compromising organizations across more than 70 countries. Compromised data encrypted with Ghost ransomware variants is likely unrecoverable without access to the decryption key. Since Ghost actors have exploited well-known CVEs and target networks where available patches have not been applied, greater focus on improving cybersecurity practices globally is likely to hinder the ransomware from financially crippling key entities like critical infrastructure, technology, manufacturing, and government networks.



Genea Investigates Breach After Suspicious Network Activity

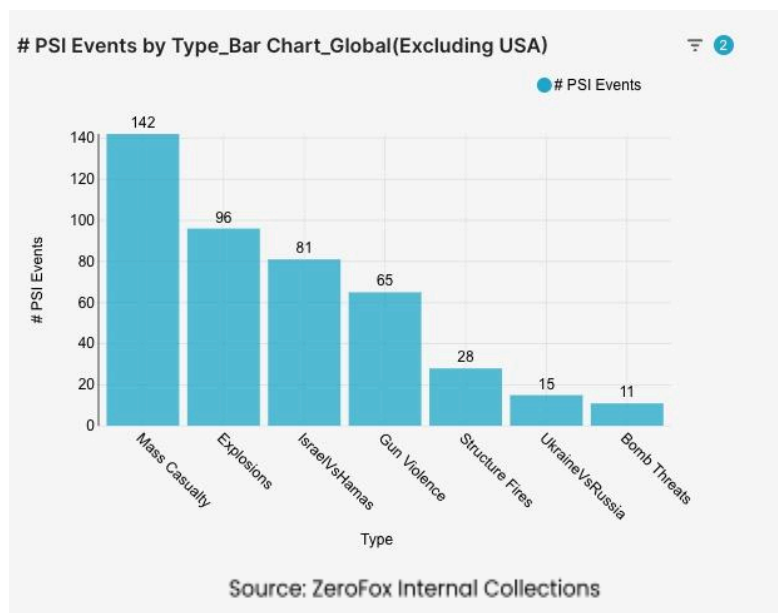
What happened: Genea, one of the leading fertility services providers in Australia, recently revealed that its network was breached by unknown attackers. The company detected "suspicious activity" on its systems and initiated an urgent investigation into the incident. During this investigation, Genea confirmed that unauthorized third parties had gained access to data stored on compromised systems. The extent of the breach, including what data was accessed and how deeply the attackers penetrated the network, is still unknown.

- **What this means:** This breach potentially compromised sensitive and personal data related to individuals seeking fertility treatments. Fertility clinics typically store confidential information such as medical records, treatment plans, genetic data, personal identification details, and financial information. If this data is stolen, it could lead to severe privacy violations, as sensitive medical histories and reproductive choices may be exposed. For individuals seeking fertility treatments, the consequences can be dire and include identity theft, financial fraud, or even blackmail. The stolen data could be used by threat actors to impersonate patients, gain access to their insurance or financial accounts, or exploited for malicious purposes. Additionally, genetic data could be misused for discriminatory practices or sold on the black market, increasing the long-term risks for those affected. Genea has stated that it will notify those individuals whose personal data was compromised.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global



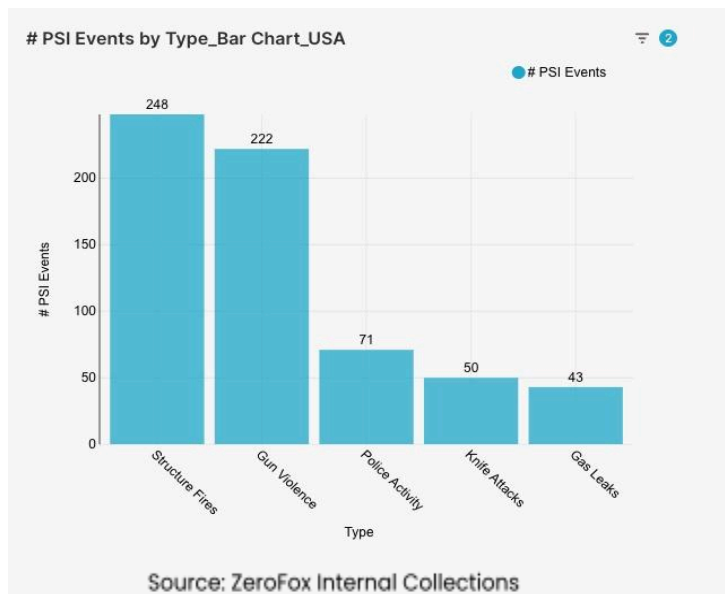
What happened: Excluding the United States, there was a 9 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Lebanon, India, and Palestine (in that order). Approximately 68 percent of these events were explosions, and the three aforementioned countries accounted for roughly 37 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring

countries) increased by 25 percent from the previous week. Events related to Russia's war in Ukraine also increased by 25 percent. The top three most-alerted subtypes were explosions, which saw a 23 percent increase from the previous week; gun violence, which increased by 12 percent; and structure fires, which decreased by 28 percent. Global protest activity increased by 12 percent.

- **What this means:** The chance of a lasting [ceasefire](#) between Israel and Hamas continues to dwindle, as not all hostages have been released and not all troops have withdrawn from previously agreed-upon areas. For instance, Lebanon was the top contributor to explosions this week due to Israeli [drone attacks](#) conducted despite the ceasefire. Overall, this activity has likely led to the increase seen in both IsraelVsHamas alerts as well as explosion alerts. In [Ukraine](#), attacks have continued despite U.S. and Russian leaders meeting in Saudi Arabia to discuss possibilities to end the war. Drones, missiles, and North Korean artillery cannons have been launched by Russia this week, while Ukrainian President Zelenskyy expressed his displeasure at being excluded from the Saudi Arabian peace talks. This week India has again seen several bomb threats, leaving it with the second-highest amount of mass casualty-tagged alerts. For instance, two Mumbai-bound express trains received [bomb threats](#) on February 18, prompting authorities to halt the trains at two different stations in Uttar Pradesh. Police continue to investigate the country's influx of hoax bomb threats against various institutions and infrastructure.

Physical Security Intelligence: United States

What happened: This week, the most alerted U.S. sub-types were structure fires, gun violence, and police activity. New York and California reported 36 percent of the total alerts in the structure fires category with 53 and 37 alerts, respectively. Gun violence came in a close second, with California (27 alerts) and New York (22 alerts) contributing 22 percent of the total alerts. Police activity was the third most-alerted subtype this week; California and Texas accounted for 24 percent of the total, contributing 9 and 8 alerts, respectively.



Additionally, knife attacks increased by 35 percent compared to the previous week.

- **What this means:** The United States saw a 19 percent increase in the structure fires incident category compared to last week. A February 16 residential fire in [Queens](#), New York, resulted in the death of three people, and two people were killed in a residential fire in New Jersey. Additionally, fire in an [Abington](#), Pennsylvania, manufacturing plant led to explosions and thick black smoke emanating from the site. People in the vicinity were asked to evacuate or shelter-in-place due to possible contamination of the air. While it was later confirmed there were no air contaminants, the cleanup from the fire and explosions is expected to take several weeks. Despite a decrease of 2 percent, gun violence remained a significant concern and continued to be a top incident category this week. ZeroFox also reported several physical security incidents this week related to this subtype, including a 16-hour standoff with a suspect who shot and injured a 12-year-old in [Clare County](#), Michigan, this week. School threats are incidents that occur when police activity takes place near the vicinity of the school or in the school itself. Police presence at schools is becoming more prevalent as incidents of gun brandishing, threats of a mass shooting, or bomb threats are on the rise. Last week, two teenage girls were arrested in [Houston](#) after the FBI thwarted their plans to use pipe bombs at a school, potentially averting a mass casualty incident. The week saw a 26 percent increase in the alerts relating to gas leaks in

the country. The gas leaks can mainly be attributed to the outdated infrastructure of the houses and the fluctuating temperatures. (The contraction of pipes in the cold and their expansion in the heat can lead to cracking and gas leaks.) Finally, this week also saw an increase in the knife attacks subtype, with a 35 percent increase in such alerts compared to the previous week.

| 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%