ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

November 29, 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 November 27, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Weekly Intelligence Brief

This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report - Scattered Lapsus$ Hunters Announce Return

On November 24, 2025, ZeroFox observed that the threat collective "Scattered Lapsus$ Hunters" (SLSH) had seemingly resumed activity through a new Telegram channel after nearly a month of silence. Multiple posts on the Telegram channel suggest that SLSH is offering financial incentives and actively recruiting insiders who can provide initial access to corporate networks. Recent messages on the channel likely indicate an escalation of border threats of disruption compared to previous publications. SLSH's recent activity on Telegram almost certainly indicates clear intent to continue and likely escalate its previously observed operations, such as conducting data breaches and data leaks, publicly exposing corporations, and actively recruiting insiders.

ZeroFox Intelligence Flash Report - UK Sanctions Prominent Bulletproof Hosting Provider

On November 19, 2025, the United Kingdom's National Crime Agency (NCA), in coordination with partners in Australia, New Zealand, Canada, and the United States, announced sanctions against a Russian citizen for operating a bulletproof hosting (BPH) service. The BPH operates under the names "Media Land LLC" and "ML.Cloud LLC". Both of these companies are based in Russia and provide virtual and physical servers for cybercriminals to maintain digital privacy and evade law enforcement (LE) takedowns. BPH is a marketing term used by underground Internet Service Providers (ISPs) to promote services that aid cybercriminals in the conduct of their operations. The sanctioning will likely have a limited impact on cybercriminals' operational environment. Considering that this BPH is based in Russia, it is highly unlikely that any legal action to take down its operations will occur.

ZeroFox Intelligence Flash Report - Powerful New RaaS from Scattered Lapsus$ Hunters

On November 19, 2025, reports surfaced of the emergence of an in-development build of new ransomware-as-a-service (RaaS) platform "ShinySp1d3r". The new RaaS build is the result of a collaboration between notorious ransomware and digital extortion (R&DE) collectives Scattered Spider, Lapsus$, and ShinyHunters. The threat actors, known collectively as Scattered Lapsus$ Hunters (SLSH), have been responsible for at least 51 cyberattacks over the past year as both individual groups and as a collective. While the ShinySp1d3r encryptor has some features common to other encryptors, it also boasts features that have never been seen before in the RaaS space. The

development of ShinySp1d3r represents a leap in capability for SLSH and suggests a successful merger into a fully functional collective.

.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Cyberattack Hits CodeRED Platform, Disrupts Emergency Alerts

What we know:

- Threat actors have targeted CodeRED emergency notification platform, disrupting emergency alerts across the United States.
- The breach reportedly exposed personally identifiable information (PII), although no public leaks have yet been confirmed by the company.

Background:

- Threat group INC Ransom has claimed to have breached the platform's company and encrypted its files.
- The company behind CodeRED is rebuilding the platform using a March 31, 2025, backup, which may mean that some accounts created after the backup date will be unretrievable.

What is next:

- While the platform is being rebuilt, threat actors are likely to exploit operational uncertainty by impersonating CodeRED and its company through phishing emails and SMS spoofing.
- These campaigns could impersonate public safety personnel, emergency responders, and companies to obtain credentials and facilitate further compromise.

IT Systems of Multiple London Councils Disrupted in Cybersecurity Incident

What we know:

- A cybersecurity incident has disrupted the IT systems of at least three London councils, including the Westminster City Council (WCC), a major local authority with important landmarks like the Palace of Westminster (Houses of Parliament), the Buckingham Palace, and 10 Downing Street.

Background:

- Multiple systems, including phone lines, have been impacted in the incident. At least two councils have activated emergency plans to ensure residents receive critical services.

- Authorities said they are investigating potential data compromise but added that it was too early to identify the perpetrators or their motives.

Analyst note:

- Shared IT infrastructure can create single points of failure, enabling widespread service disruption and likely exposing sensitive data on high-value individuals in areas like Westminster.

Shai-Hulud Supply Chain Attack Floods Npm with Malicious Packages

What we know:

- A massive Shai-Hulud supply-chain attack has flooded the npm registry with over 500 trojanized packages, compromising over 25,000 developer secrets within three days.

Background:

- The malware strain harvests developer and continuous integration (CI) and continuous delivery (CD) secrets during the npm pre-install stage.
- The secrets are then saved in files such as cloud.json and truffleSecrets.json before being uploaded to attacker-created GitHub repositories labeled “Shai-Hulud” or “Sha1-Hulud: The Second Coming.”

Analyst note:

- Stolen GitHub, npm, and cloud provider secrets are likely to allow threat actors to pivot directly into developer environments, CI/CD pipelines, and cloud accounts, enabling code tampering, repository hijacking, and supply chain poisoning at scale.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) has added one vulnerability (CVE-2025-61757) to its Known Exploited Vulnerabilities (KEV) catalog. CISA has also released seven industrial control systems (ICS) advisories. Researchers have uncovered five exploitable vulnerabilities in the Fluent Bit telemetry agent that enable authentication bypass, log manipulation, and remote code execution (RCE). The flaws have now been patched in Fluent Bit versions 4.1.1 and 4.0.12. Threat actors are exploiting a recently patched WSUS flaw (CVE-2025-59287) to gain RCE on certain servers and deploy the ShadowPad backdoor. CVE-2025-61757 is now being actively exploited, enabling attackers to bypass authentication in Oracle Identity Manager and achieve RCE to run arbitrary commands. A six-month-old Firefox vulnerability (CVE-2025-13016) in the WebAssembly engine could enable attackers to execute arbitrary code on users' devices, affecting over 180 million users. The flaw was a stack buffer overflow caused by a small coding error in memory handling.

HIGH

CVE-2025-12816

What happened: This vulnerability stems from a flaw in node-forge's ASN.1 validation logic that enables malformed data to bypass cryptographic checks. If exploited, it could enable authentication bypass, tampering with signed data, and other verification failures depending on the application.

What this means: The CERT Coordination Center has issued an advisory warning of potential impacts, including authentication bypass, data tampering, and certificate misuse. With close to 26 million weekly npm downloads, the exploitation of this flaw could affect a vast number of projects.

- **Affected products:**
  - Node-forge versions 0 through 1.3.1

CRITICAL

CVE-2025-59366

What happened: ASUS has released firmware updates to fix nine security flaws in its routers, including a critical authentication bypass vulnerability affecting devices with the AiCloud feature enabled.

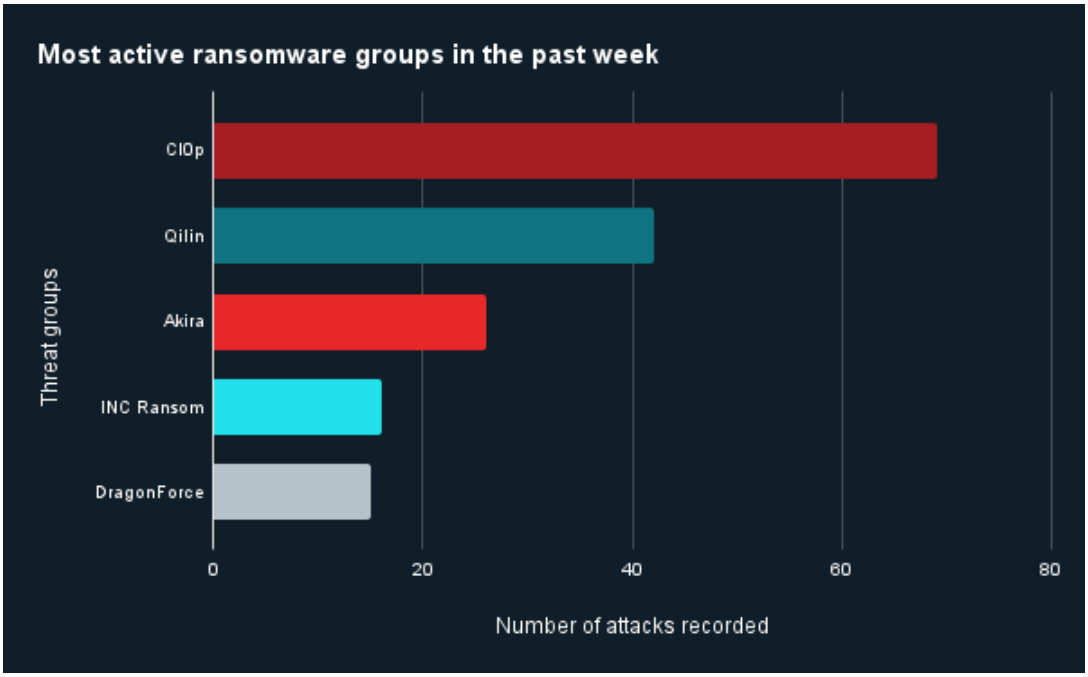
- **What this means:** If patches are not deployed, The AiCloud vulnerability could enable attackers to gain unauthorized access to affected ASUS routers leading to device takeover, data theft, service disruption, or use of compromised routers as part of a larger botnet or proxy infrastructure.
- **Affected products:**
  - Firmware versions:
    - 3.0.0.4_386
    - 3.0.0.4_388
    - 3.0.0.6_102

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

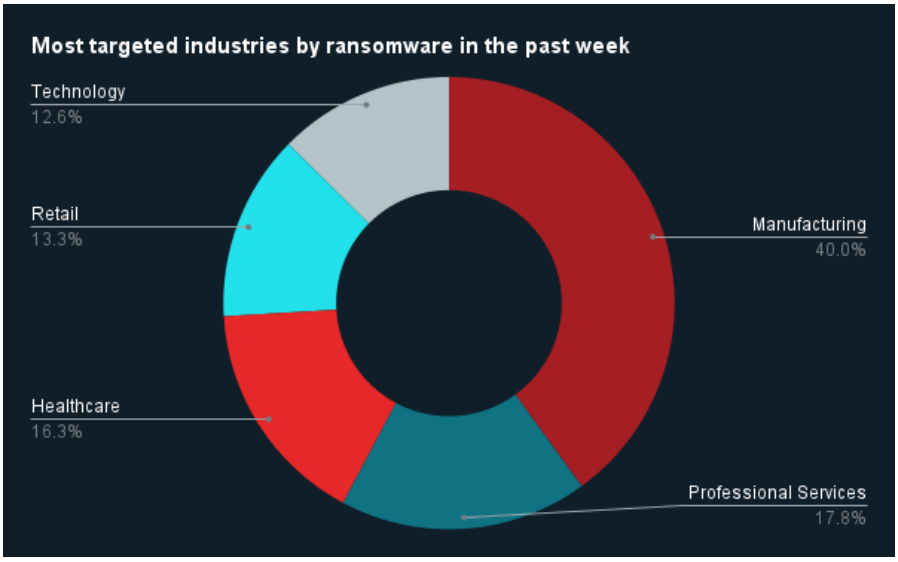
Ransomware Activity in the Past Week

Last week in ransomware: In the past week, Cl0p, Qilin, Akira, INC Ransom, and DragonForce were the most active ransomware groups. ZeroFox observed close to 208 ransomware victims disclosed. The Cl0p ransomware group accounted for the largest number of attacks, followed by Qilin.



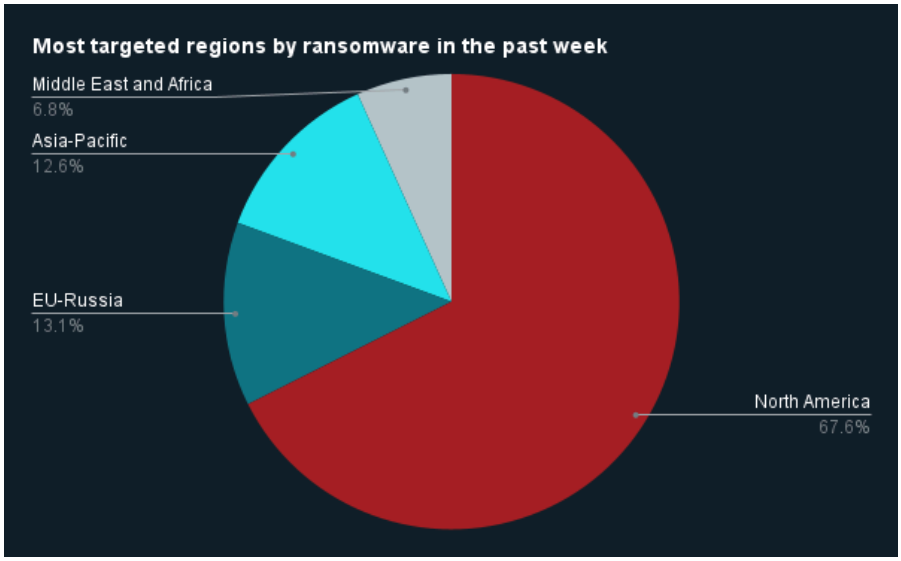
Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by professional services.



Source: ZeroFox Internal Collections

Regional ransomware trends: Over the past seven days, ZeroFox observed that North America was the region most targeted by ransomware attacks, followed by Europe and Russia and Asia Pacific (APAC) regions. There were at least 150 ransomware attacks observed in North America, while Europe and Russia and APAC accounted for 29 and 28, respectively. The Middle-East and Africa accounted for 15 attacks.



Source: ZeroFox Internal Collections

Critical Data Breaches in the Past Week

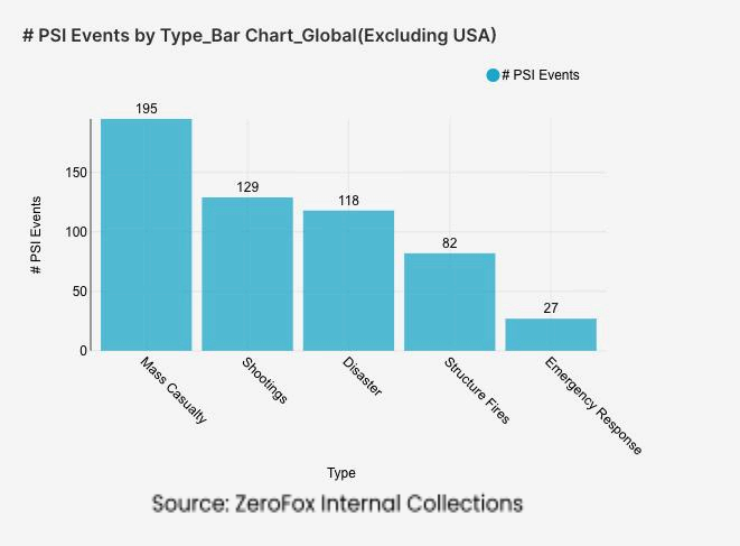
Targeted Entity	Spark Energy	SitusAMC	Adda
Compromised Entities/victims	N/A	Customers and major banks	1.86 million users
Compromised Data Fields	Supervisory Control and Data Acquisition (SCADA) systems	Corporate records and legal documents, as well as some customer data	Owner IDs, users' first and last names, phone numbers, email addresses, and passwords
Suspected Threat Actor	Inteid and Keymous+	N/A	Blinkers
Country/Region	Italy	United States	India
Industry	Retail (renewable energy supplies)	Financial Services	Real Estate, Technology
Possible Repercussions	Complete SCADA access is likely to enable attackers to move laterally across industrial networks, compromising other critical infrastructure and assets connected to the plant.	Phishing and impersonation scams aimed at borrowers, especially during mortgage payments, refinancing, or loan servicing cycles.	ID theft, social engineering, impersonation

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

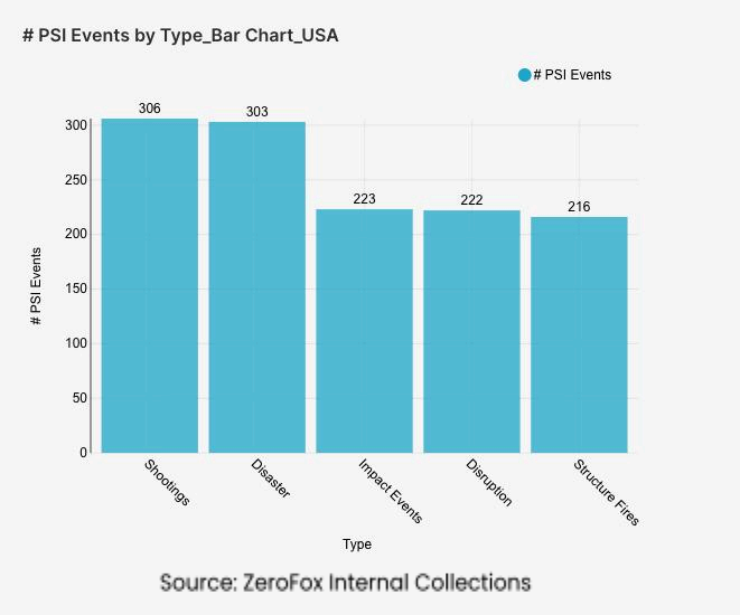
Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global



What happened: In the past week, the top three most-alerted incident subtypes globally, excluding the United States, were mass casualty, shootings, and disaster. Hong Kong officials have reported that the death toll from the November 26 Wang Fuk Court apartment fire has risen to 55, with 72 more injured, as of writing. Nearly a day later, firefighters were still battling intense heat and smoke to reach residents on the upper floors. Three men have been arrested as 26 rescue teams remain on site. On November 24, 2025, a volcano in Ethiopia's Afar region erupted for the first time in 12,000 years, sending ash across multiple countries and threatening local herders' livelihoods despite no reported casualties. Ash from the eruption drifted over Pakistan and northern India, prompting precautionary flight cancellations as authorities rerouted aircraft until the skies cleared. Guinea-Bissau's military has seized "total control," suspending elections and closing borders after both leading candidates claimed victory, deepening the country's long history of coups and political instability.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes in the United States were shootings, disaster, and structure fires. Two West Virginia National Guard members were critically injured after being shot near the White House, and the suspected gunman, who is believed to have acted alone, is in custody. Officials have not identified a motive, but the attack is likely to prompt heightened security measures around federal sites as investigators assess whether the incident signals any broader threat. A stretch of severe weather threatens major delays during what is expected to be a record Thanksgiving travel week. With 82 million people on the move, any disruption to flights or highways could quickly cascade into nationwide gridlock and place added strain on emergency services. On November 25, 2025, a tornado struck northwest Harris County near Houston, damaging over 100 homes and cutting power to thousands, though no serious injuries were reported. Meanwhile, Norovirus cases are climbing nationwide ahead of the holidays, with wastewater data showing a sharp rise driven by the GII.17 variant, raising concerns of an early and potentially intense season.

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%