ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

October 25, 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 (EDT) on October 23, 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 Brief - Underground Economist: Volume 5, Issue 21

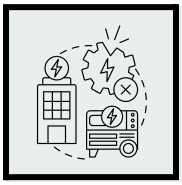
The Underground Economist is an intelligence-focused series that highlights dark web findings from our ZeroFox Dark Ops intelligence team.

.

ZEROFOX
Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



AWS Restores Services After Global Outage Disrupts Major Platforms

What we know:

- Amazon announced its Amazon Web Services (AWS) cloud service is now back to normal after an outage on October 20 disrupted businesses and websites worldwide.
- AWS traced the issue to a malfunction in a subsystem used for monitoring network load balancers.
- Services were largely restored by late afternoon Pacific Time on October 20, 2025, though some lingering delays were reported.

Background:

- The issue reportedly stemmed from Domain Name System (DNS) resolution problems affecting AWS's DynamoDB API in the US-EAST-1 region.
- The disruption brought down several major websites and apps.
- Many global companies depend on AWS infrastructure for core operations and user services.

What is next:

- AWS is likely conducting a post-incident review to prevent a recurrence of the subsystem fault.
- Businesses affected will likely reassess disaster recovery and multi-region strategies.
- AWS will likely roll out resilience updates and possibly, new monitoring safeguards.
- Some delayed or queued workloads are likely to continue experiencing residual slowdowns.
- AWS could implement new fault-tolerance measures or update monitoring systems based on findings.

Russian Hackers Leak Secret RAF and Navy Base Files in UK MoD Contractor Breach

What we know:

- Russian hackers have breached a UK Ministry of Defence (MoD) contractor and stolen hundreds of sensitive military documents.
- The stolen data, now leaked on the dark web, includes details of eight Royal Air Force (RAF) and Royal Navy bases.

Background:

- The attackers, believed to be from the Russian group Lynx, bypassed MoD's cyber defenses by targeting a third-party contractor.
- Among the compromised sites is RAF Lakenheath, the base of the U.S. F-35 jets.

Analyst note:

- Leaked base layouts and staff information are likely to be used in hostile state intelligence gathering, physical targeting, or cyber reconnaissance.
- The suspected link to Lynx suggests a ransomware attempt, with the data likely stolen to pressure the MoD or sold as part of a double-extortion scheme.

DOJ Warns of Phishing and Spoofing Scams Following Typhoon Halong

What we know:

- The U.S. Department of Justice (DOJ) has warned the public and victims of Typhoon Halong that fraudsters may target them in phishing and impersonation scams under the guise of disaster relief efforts.

Background:

- Typhoon Halong's devastating floods in Alaska have left over 1,500 people displaced. The DOJ's warning states that fraudsters use phishing to steal personal and financial information and spoofing to pose as trusted agencies or charities to obtain money fraudulently.

Analyst note:

- Fraudsters are likely to impersonate well-known charities, government officials, insurance company representatives, and others through email, website, or caller ID spoofing to seek financial and other personal details from victims and steal money.
- They are also likely to solicit investments into non-existent businesses promising initiatives such as the rebuilding of homes.

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) added 18 Industrial Control System (ICS) advisories on October 21 and October 23, and six vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on October 20 and October 22. Oracle has released 374 security patches across its product portfolio as part of the October 2025 Critical Patch Update . ConnectWise has released a security update for its Automate platform to fix flaws that could enable attackers to intercept or alter agent communications in certain on-premises setups. A high-severity flaw in the abandoned async-tar Rust library, tracked as CVE-2025-62518, enables unauthenticated remote code execution (RCE) via the exploitation of a desynchronization issue during TAR file extraction. A cyber espionage group known as "Bitter APT" is reportedly exploiting an unpatched WinRAR vulnerability to deliver a malicious backdoor that enables RCE on targeted systems. The SessionReaper flaw, tracked as CVE-2025-54236, in Adobe Commerce is reportedly being actively exploited by hackers. An out-of-bounds write flaw in Dolby's Unified Decoder could enable RCE during audio data processing, even without user interaction. Microsoft issued out-of-band security updates to fix a critical WSUS vulnerability, CVE-2025-59287, after proof-of-concept exploit code was publicly released.

CRITICAL

CVE-2025-9242

What happened: Nearly 76,000 WatchGuard Firebox security appliances remain exposed online and are vulnerable to a flaw that enables unauthenticated RCE. Most affected devices are reportedly in Europe and North America.

- **What this means:** Attackers are likely to exploit this flaw to gain control of network gateways, potentially leading to data breaches, ransomware attacks, or wider network compromise.
- **Affected products:**
  - WatchGuard Firebox OS versions 11.10.2 through 11.12.4_Update1, 12.0 through 12.11.3, and 2025.1

CRITICAL

CVE-2025-6542 and CVE-2025-8750

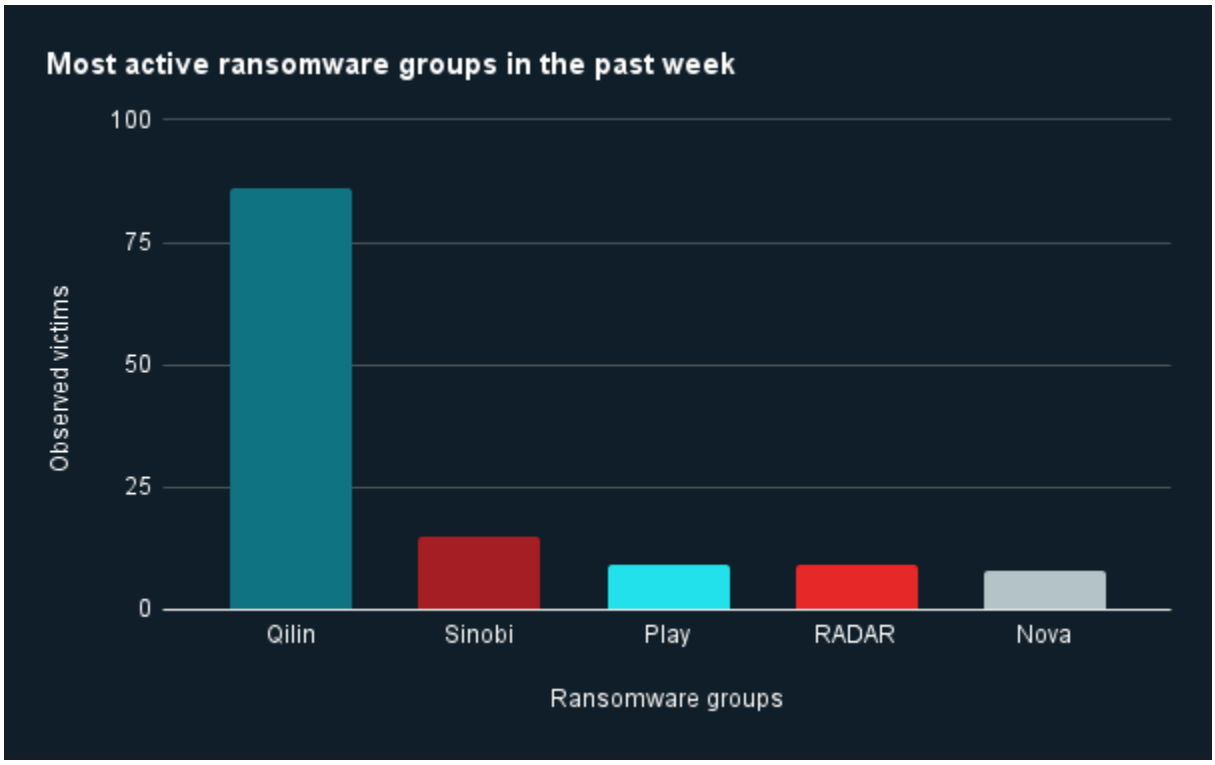
What happened: TP-Link has disclosed two command injection flaws in its Omada gateway devices, of which CVE-2025-6542 enables unauthenticated RCE.

- **What this means:** The vulnerabilities enable attackers to run arbitrary operating system (OS) commands, leading to full system compromise and data theft. If exploited, the flaws could disrupt small business networks and expose sensitive information.
- **Affected products:**
  - The affected products are listed in this advisory.

Ransomware and Breach Intelligence

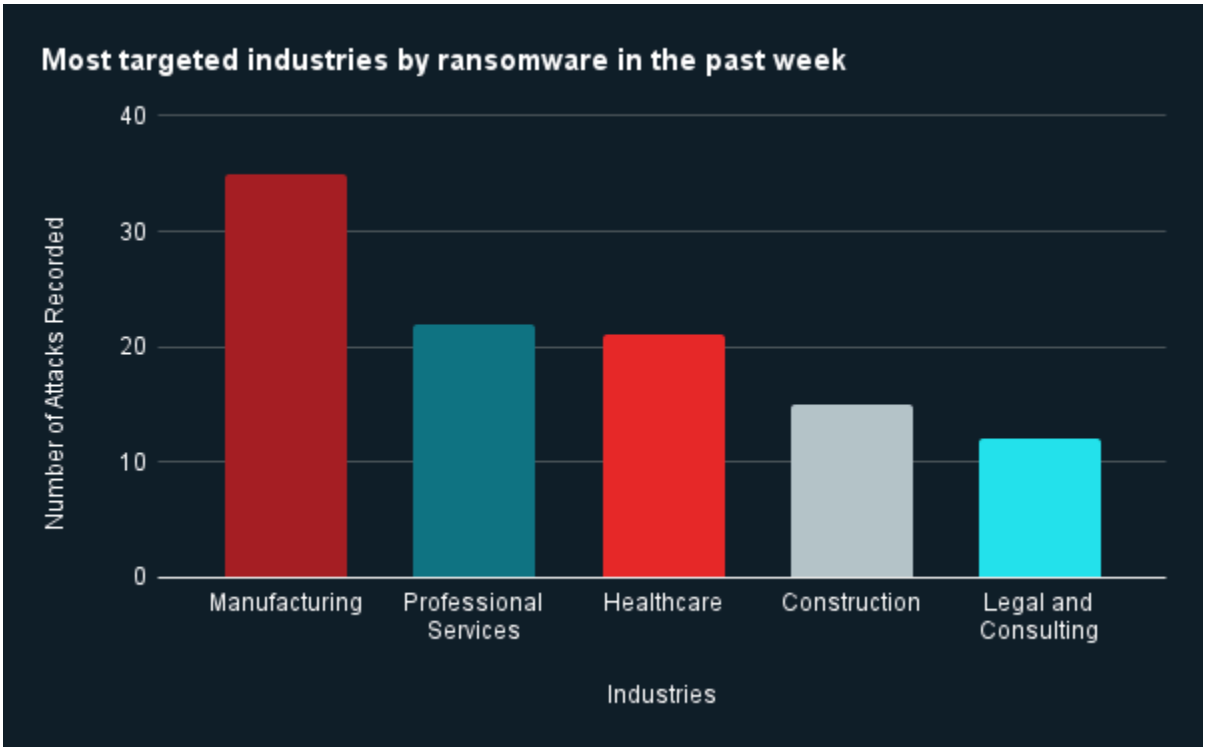
Ransomware and Breach Intelligence Key Findings

Ransomware Roundup: Trends, Industries, and Regions



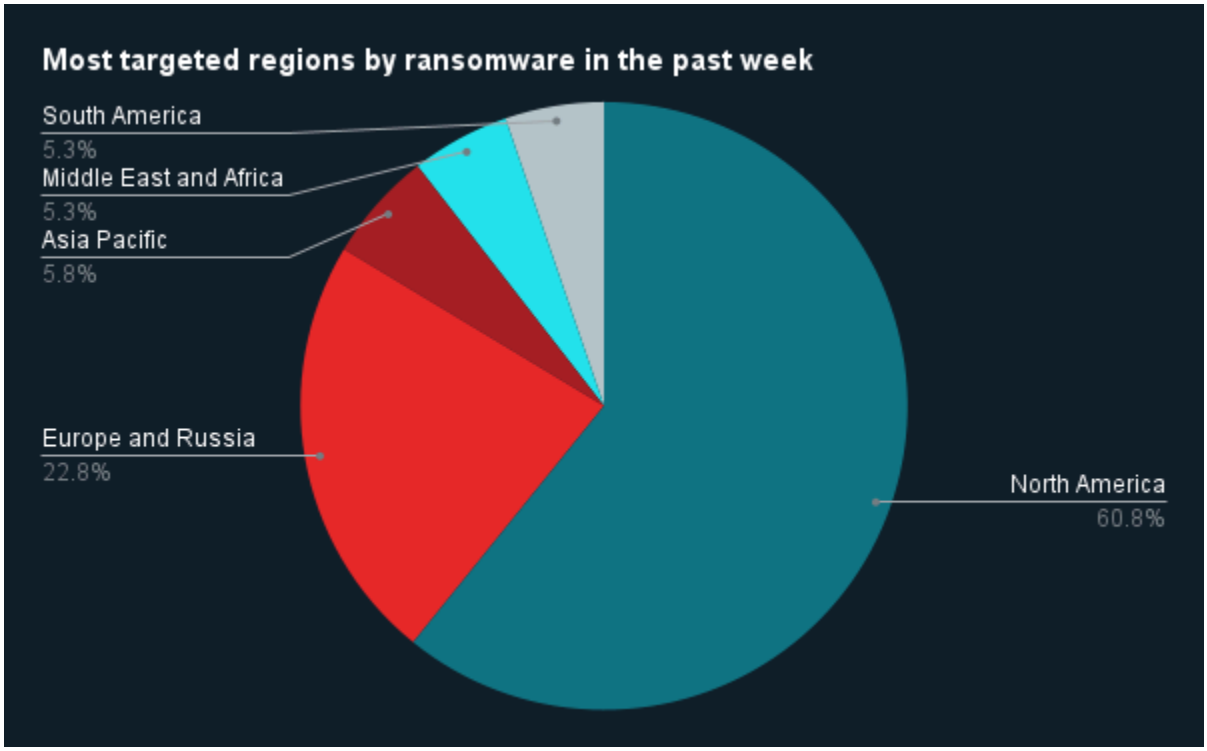
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Sinobi, Play, RADAR, and Nova were the most active ransomware groups. ZeroFox observed close to 165 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by Sinobi.



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. There were at least 104 ransomware attacks observed in North America, while Europe and Russia accounted for 39, Asia-Pacific (APAC) for 10, Middle East and Africa for nine, and South America for nine.

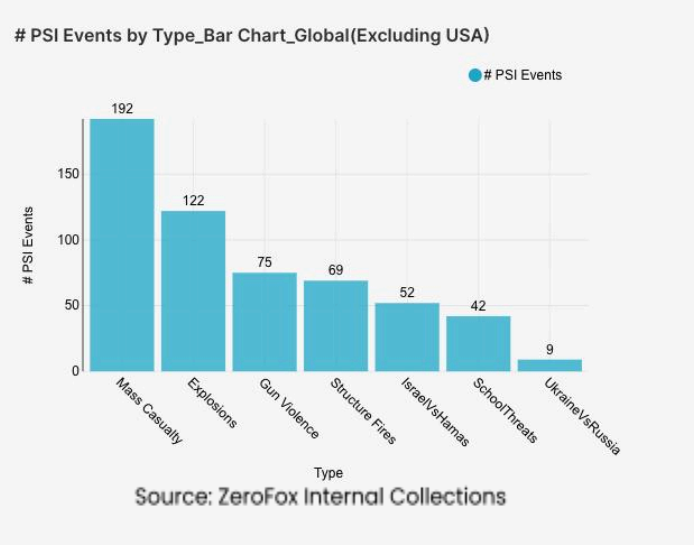
Major Data Breaches Hits Several Industries

Targeted Entity	Verisure	Sotheby's	Toys "R" Us Canada
Compromised Entities/victims	35,000 current and former Verisure's Alert Alarm customers in Sweden	Unavailable	Unspecified number of Toys "R" Us Canada customers
Compromised Data Fields	Personally identifiable information (PII), including names, addresses, email addresses, and Social Security numbers (SSNs)	Full names, SSNs, and financial account information	PII like full name, physical address, email address, and phone number
Suspected Threat Actor	Unavailable	Unavailable	Unavailable
Country/Region	Sweden	United States	Canada
Industry	Security	Professional Services	Retail
Possible Repercussions	Identity theft, social engineering, and fraudulent activities (such as opening accounts or applying for credit in victims' names)	Unauthorized transactions and loan applications, tax fraud, and phishing and other social engineering attacks	Phishing, social engineering, identity scams like impersonation, doxxing, and physical stalking of victims

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

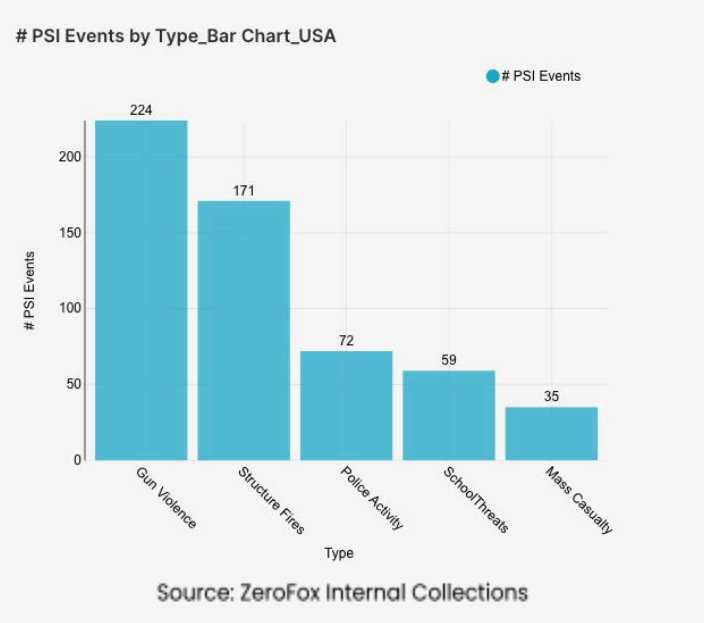


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 19 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being Pakistan, the Palestinian Territories, and India, in that order. Approximately 64 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 30 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including raids and attacks) decreased by 21 percent from the previous week. Events related to Russia's war in Ukraine decreased by 10 percent. The top three most-alerted subtypes were explosions, which saw a 17 percent increase from the previous week; gun violence, which increased by 4 percent; and structure fires, which increased by 60 percent. Notably, threats related to schools increased by 35 percent.

- **What this means:** The global security environment saw an overall increase in mass casualty events this week, with over two-thirds of these incidents being attributed to explosions, and many of these events being concentrated in areas with ongoing instability. For instance, with the Israel-Hamas conflict, there have already been some breaches in the current ceasefire, after the Israel army conducted strikes in Gaza on October 19 after its troops came under fire from Hamas fighters. Despite this flare-up, the ceasefire continues to hold, as evidenced by the decrease in overall alerts related to the war this week. Structure fires increased dramatically this week, with India being the top contributor due to Diwali celebrations; firefighters were deployed across Delhi, taking action on a total of over 400 calls, indicating a state of high alert during the festival. Additionally, a fire that resulted in 14 victims broke out in Maharashtra's Navi Mumbai township on October 21. Lastly, school threats saw an increase this week, driven largely by cyber threats—the education sector was recently revealed to be the top threat target for cyber criminals in 2025. Both ongoing conflicts and individual attacks underscore the complex nature of global physical security.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, and police activity. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, police activity involves law enforcement presence for generalized threats or for unknown reasons, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were Illinois and New York, which together made up 27 percent of this week's nationwide total. Gun violence across the United States overall increased by 4 percent from the week prior. Police activity alerts increased by 29 percent, and the top contributing states were California and New York. Structure fires decreased by 10 percent, and the top two states for this subtype were California and New York.

- **What this means:** Within the last seven days, as evidenced by the increase in overall gun violence, the United States saw 10 mass shootings. In Chicago, Illinois, alone, there were at least four killed and 14 wounded in shootings over the weekend, reflecting the ever-pervasive issue of routine gun violence.

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%