



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

October 24, 2026

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 22, 2026*; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

| This Week's ZeroFox Intelligence Reports 2

- ZeroFox Intelligence Flash Report – Yandex Strikes in Russia Unlikely to Impact Threat Actors 2
- ZeroFox Intelligence Flash Report – SITREP #45 – Escalations by Houthis and Iran Ahead of U.S. Mid-Terms – October 19, 2026 2
- ZeroFox Intelligence Flash Report – FBI Suspects Ransomware Negotiator Aided ShinyHunters 2
- ZeroFox Intelligence Flash Report – AI-Discovered PHP Vulnerability 2

| Cyber and Dark Web Intelligence Key Findings 4

- PHP Urges Admins to Prepare for Critical Patches After Reported Vulnerability Leak 4
- NVIDIA RTX 5090 Shipment Goes Missing in Brazil 4
- Cyberattack Forces Bullhorn to Shut Down Staffing Platform 4

| Exploit and Vulnerability Intelligence Key Findings 6

- Broadcom Wi-Fi WPS vulnerability 6
- CVE-2026-106173 6

| Ransomware and Breach Intelligence Key Findings 8

- Ransomware Group, Industry, Regional Trends 8
- Notable Data Breaches this Week 10

| Physical and Geopolitical Intelligence Key Findings 12

- Physical Security Intelligence: Global 12
- Physical Security Intelligence: United States 12

| Appendix A: Traffic Light Protocol for Information Dissemination 13

| Appendix B: ZeroFox Intelligence Probability Scale 14

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – Yandex Strikes in Russia Unlikely to Impact Threat Actors

Overnight on October 7–8, 2026, drone strikes almost certainly launched by Ukrainian forces struck a Yandex data center in the Ryazan Oblast of Russia. On October 9, 2026, Yandex confirmed that several data center modules were completely disabled at its Kaluga facility, and on October 11, 2026, a strike on the company's data center near Vladimir caused what Yandex described as a complete shutdown. These three sites constitute half of Yandex's six data centers. The data center losses caused a near-total collapse of Yandex services on October 11, 2026, with most systems still operating roughly 90 percent below baseline on October 13, 2026. The Yandex disruptions have likely had limited impact on ransomware and digital extortion (R&DE) threat actors. Threat actor traffic was disrupted but did not disappear; instead threat actors likely pivoted to other services to maintain their infrastructure. Although the strikes almost certainly caused significant disruptions to Yandex, its cloud services, and its large client base in Russia, the Ukrainian drone strikes are very unlikely to have major impacts on Russian threat actor infrastructure or activity.

ZeroFox Intelligence Flash Report – SITREP #45 – Escalations by Houthis and Iran Ahead of U.S. Mid-Terms – October 19, 2026

Since October 1, Iran has launched its highest number of attacks against commercial shipping in the Strait of Hormuz (SoH) since the war began in March. Iran is likely escalating its attacks to target a wider array of assets across a broader geographic area. This pattern suggests an effort by Iran to sustain elevated oil prices and pressure the United States to abandon its policy to increase SoH transits. There is an unlikely chance that the Iranian escalation triggers a U.S. military response. The probability of such a response increases after the U.S. mid-term elections or if Iranian policy causes a sharp decline in the SoH transits. A Saudi Arabian-backed offensive to recapture territory lost to Houthi rebels in Yemen has likely stalled, while Houthi attacks against Saudi Arabia, Presidential Leadership Council territory, and in the Red Sea have increased. These attacks are likely designed to pressure Saudi Arabia into pursuing a political settlement. Saudi Arabia is likely pressuring other external actors to join its effort to back the Yemeni government. Further entry by outside actors into the Houthi conflict will likely lead to an escalation in Houthi attacks on Red Sea shipping and against regional states.

ZeroFox Intelligence Flash Report – FBI Suspects Ransomware Negotiator Aided ShinyHunters

On October 8, 2026, the Federal Bureau of Investigation (FBI) arrested an executive from a Canadian cybersecurity firm in connection with an ongoing investigation into the ShinyHunters ransomware and digital extortion (R&DE) threat collective. Another executive from a second cybersecurity company very likely played an active role in shinywire[.]com, the now-defunct ShinyHunters victim extortion site. The shinywire[.]com site was active from at least May 2026 and was no longer online as of October 16, 2026. The most recent arrest came two weeks after ShinyHunters claimed a breach of the FBI jobs portal, which contained a reported 2–3TB of data and very likely included personal information on thousands of FBI employees and their families. Ransomware negotiators and incident mitigation service providers very likely represent a secondary threat layer, and these most recent examples are not isolated. ZeroFox recommends that victims maintain vigilance when choosing professional mitigation services.

ZeroFox Intelligence Flash Report – AI-Discovered PHP Vulnerability

On October 21, 2026, the PHP Foundation released emergency patches for two critical PHP core vulnerabilities, CVE-2026-109618 and CVE-2026-109619 (“PHP2Shell”), and allows unauthenticated remote code execution (RCE). Multiple parties reportedly independently discovered the flaws in August 2026 using frontier artificial intelligence (AI) models, which reportedly also reduced the effort required to build working exploits. ZeroFox has observed reporting of early exploitation attempts of both CVEs, urgent patching warnings from U.S. and European government agencies, and several government websites taken offline as a precaution. ZeroFox assesses that organizations running end-of-life PHP versions face the highest exposure risk, as no official patch is available for those versions at the time of writing. ZeroFox assesses with moderate confidence that exploitation of unpatched and end-of-life PHP deployments will almost certainly continue and expand in the coming weeks, and that this event will very likely accelerate AI-assisted vulnerability discovery and exploitation.

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



PHP Flaws Prompt Government Websites to Go Offline as Precaution

What we know:

- Government agencies and other organizations across the world temporarily took their websites and online services offline as a precaution after two vulnerabilities were found in the PHP language, which powers a large portion of the internet's websites.
- A major tech company reportedly detected attempts to exploit the flaws against its honeypot infrastructure.

Background:

- The shutdowns reportedly affected government portals, hospitals, schools, and other public-facing services, as well as some Wikimedia systems.
- The outages were largely precautionary and do not indicate that the affected organizations were compromised.
- [PHP has released fixes](#) for supported versions, while PHP 8.1 and older remain end-of-life and require migration to a supported release.

Analyst note:

- Continued exploitation attempts are very likely against internet-facing PHP systems that remain unpatched, particularly older or unsupported deployments.
- The public availability of patches and technical details of proof-of-concept (PoC) are likely to accelerate vulnerability scanning and exploit development, while AI-assisted analysis can further reduce the time required for threat actors to reverse-engineer the vulnerabilities.



NVIDIA RTX 5090 Shipment Goes Missing in Brazil

What we know:

- A Brazilian electronics distributor has reported two pallets of Zotac NVIDIA RTX 5090 graphics cards, valued at approximately BRL 2.5 million (USD 470,000, as of writing), as missing after arriving at Guarulhos International Airport in Brazil.
- The incident reportedly comes amid limited RTX 5090 supply and sharply elevated prices, with the GPU reportedly selling for more than twice its USD 2,000 launch price in some markets.

Background:

- Semiconductors have become a focal point of the U.S.–China strategic relations on national security grounds, with U.S. export controls restricting China's access to certain advanced computing chips and reports of suspected smuggling networks circumventing these restrictions.
- Additionally, high-value artificial intelligence (AI) hardware has become the target of cargo theft, including cyber-enabled schemes that exploit compromised logistics accounts, carrier impersonation, phishing, and shipment rerouting.
- ZeroFox observed that, since the start of the year, the transport and logistics sector—primarily in North America and Europe and Russia—experienced approximately 600 cyber incidents.

Analyst note:

- As of writing, the incident's cause remains unconfirmed.
- The GPU's high value and limited availability are also likely to create an opportunity for illicit resale through gray market channels attracting buyers (such as nation-state entities) seeking hardware outside normal distribution channels.



Cyberattack Forces Bullhorn to Shut Down Staffing Platform

What we know:

- American staffing software company Bullhorn restored services to its major platforms on October 19, 2026, after temporarily disabling access to its recruitment software ecosystem on October 17 to contain a cyber incident.
- The incident caused a system-wide outage of its applicant tracking system (ATS) and customer relationship management (CRM), automation, back-office, and talent platform services.

Background:

- More than 10,000 customers worldwide reportedly use Bullhorn's platform for recruitment, candidate tracking, onboarding, and payroll.
- The company has reportedly not yet determined whether customer data was exfiltrated.

Analyst note:

- The outage is unlikely to have caused any major disruptions to recruitment and related business operations, as services were restored shortly after.
- However, if data theft is confirmed, personally identifiable information (PII) of candidates and exposed application programming interface (API) credentials are likely to be used for recruitment-themed phishing, identity fraud, and follow-on credential theft.

| **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 eight new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog: CVE-2025-61624, CVE-2026-102764 on [October 16](#) and CVE-2026-96652, CVE-2026-96654, CVE-2026-96655, CVE-2026-96656, CVE-2026-106931, and CVE-2026-110936 on [October 20, 2026](#). Additionally, CISA released several Industrial Control Systems (ICS) advisories on [October 20, 2026](#). Furthermore, [BeyondTrust patched](#) a critical zero-day vulnerability in Remote Support that enables remote attackers to perform file operations. Broadcom disclosed a Wi-Fi Protected Setup (WPS) vulnerability that enables unauthorized network access, and NGINX released patches addressing five vulnerabilities (including three memory safety flaws that enable RCE).



Broadcom Wi-Fi WPS vulnerability

What happened: A flaw in Broadcom's WPS software enables devices to join Wi-Fi networks without manually entering a password.

- **What this means:** The flaw stems from Broadcom's code mishandling the reassembly of fragmented WPS setup messages. This can enable an attacker within radio range to send crafted messages that corrupt router memory and potentially execute code as root without authentication or device pairing.
- **Affected products:**
 - The affected products are [listed in this advisory](#).



CRITICAL

CVE-2026-106173

What happened: A path traversal vulnerability in Fortinet FortiSIEM could enable an unauthenticated remote attacker to write arbitrary files to the appliance.

- **What this means:** Successful exploitation likely leads to RCE or commands via specially crafted packets. A public PoC exploit is available.
- **Affected products:**
 - FortiSIEM versions 7.0 through 7.5

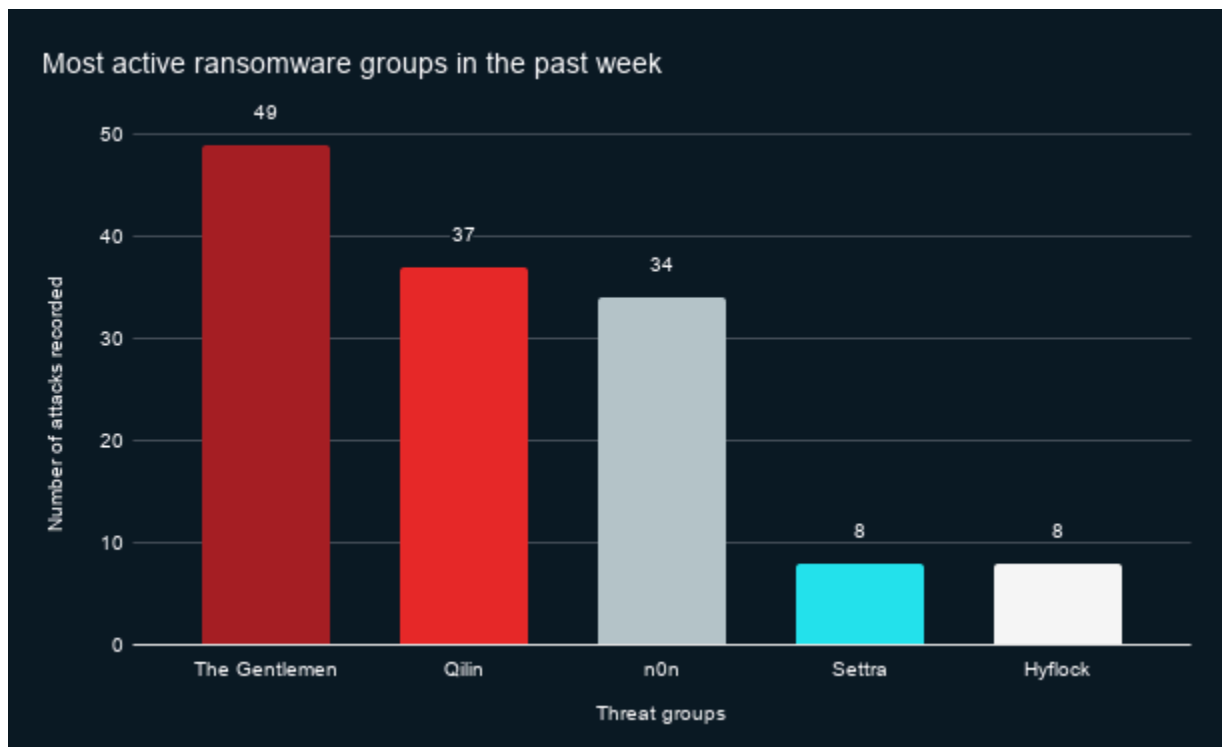
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



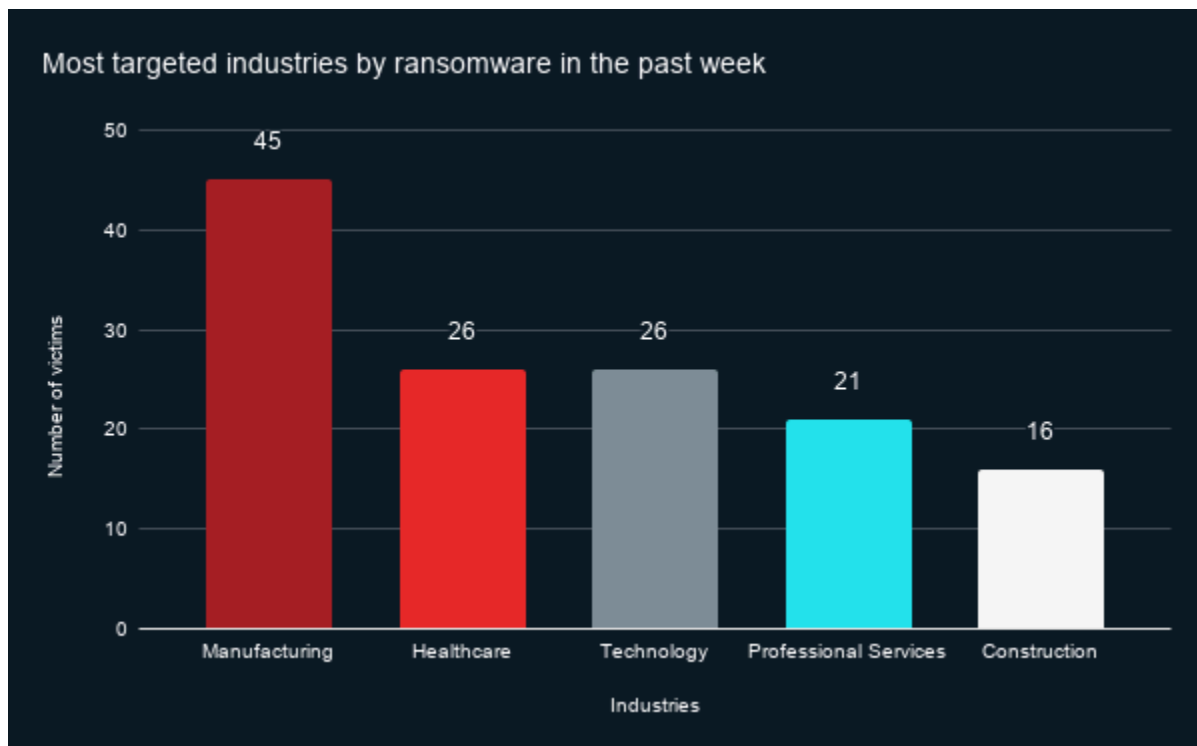
Ransomware Group, Industry, Regional Trends

Last week in ransomware: In the past week, The Gentlemen, Qilin, n0n, Settra, and Hyflock were the most active ransomware groups. ZeroFox observed close to 209 ransomware victims disclosed, most of whom were located in North America. The Gentlemen accounted for the largest number of attacks, followed by Qilin.



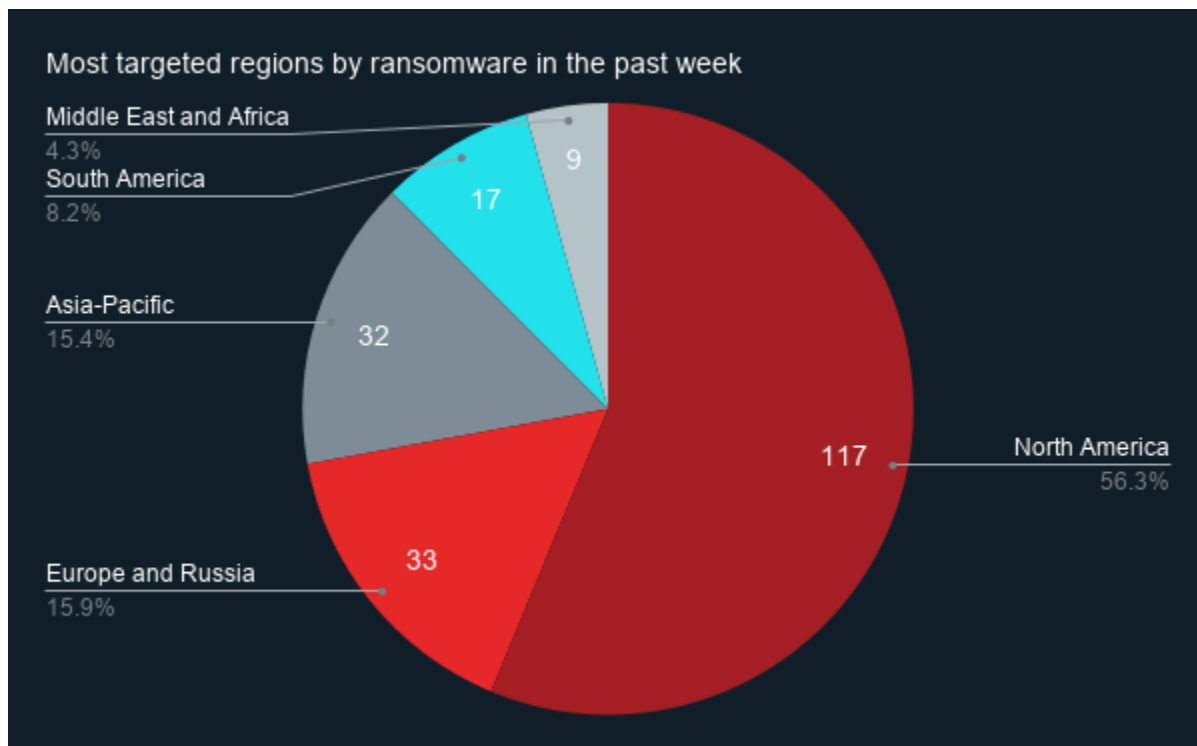
Source: ZeroFox Internal Collections

Industry ransomware trends: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by healthcare, technology, professional services, and construction.



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. There were at least 117 ransomware attacks observed in North America, while Europe and Russia accounted for 33, Asia-Pacific for 32, South America for 17, and Middle East and Africa for nine.



Source: ZeroFox Internal Collections



Notable Data Breaches this Week

Targeted Entity	<u>State Bank of India (SBI)</u>	<u>Educational Testing Service (ETS)</u>	<u>Burger King Japan</u>
Compromised Entities/Victims	3,897 customer records	Millions of current and former California public school students enrolled during the three school years preceding 2025–2026.	More than 11.18 million customer records
Compromised Data Fields	Personally identifiable information (PII), customer identifiers, and loan records	Student full names, dates of birth, home addresses, and documented disability statuses	Names, dates of birth, gender, email addresses, phone numbers, and order history
Suspected Threat Actor	Siriusim	Unknown	Unknown
Country/Region	India	United States	Japan
Industry	Financial Services	Education	Food and Beverage / Retail
Possible Repercussions	Phishing and social engineering attacks, including fraudulent loan repayment scams	Targeted social engineering and phishing, exploitation of vulnerable demographics, vendor due diligence	Targeted phishing and fraud, as well as impersonation of Burger King Japan

Three major breaches observed in the past week

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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%