ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

August 30, 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 August 28, 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 17

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

Monthly Geopolitical Assessment September 2025

Nationwide social unrest is very likely in France, triggered either by governmental collapse or large anti-government protests Russia is likely looking to continue its war in Ukraine without further U.S. tariffs on its leading trade partners and to avoid a ceasefire that would more likely benefit Ukraine. After nearly six months of tariff uncertainty, there is finally a slowdown in tariff-related supply chain disruptions as U.S. trade policy takes a clearer form. U.S. military deployments to counter transnational drug cartels in Latin America over the coming months are likely. These are predicated on an assessment that other global security threats to the United States have lessened and that LATAM regional governments are likely incapable of handling the threat, making drug cartels the leading U.S. national security priority for the foreseeable future. U.S. tariffs on India are influencing efforts to end Russia's war in Ukraine. They also play a role in the ongoing tariff-related discussions between the United States and China, as well as any potential retaliatory tariff response from other BRICS nations.

ZEROFOX
Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

CISA Publishes Advisory on China-Linked Cyber Threats

What we know:

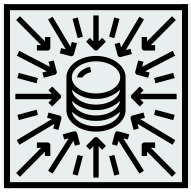
- The Cybersecurity and Infrastructure Security Agency (CISA) has published an advisory on China-linked advanced persistent threat (APT) actors targeting global networks, including telecom, government, military, transportation, and lodging sectors.
- These actors have been observed exploiting compromised routers, virtual private server (VPS) infrastructure, and edge devices to pivot through trusted connections, modify routing, and mirror traffic, enabling persistent access into telecom and internet service providers (ISP) networks.
- CISA expects these actors to keep adapting tactics, techniques, and procedures (TTPs) and expand to other devices as new vulnerabilities emerge.

Background:

- Their activities reportedly overlap with those of groups such as “Salt Typhoon”, “OPERATOR PANDA”, “RedMike”, “UNC5807”, and “GhostEmperor”, and their presence has been observed worldwide.
- The advisory alleges that the Chinese private sector provides products and services to China’s People’s Liberation Army (PLA) and other entities to further hacking operations.
- The advisory provides indicators of compromise (IoC), TTPs, and mitigations to help strengthen defenses against high-profile attacks and identify threats.

What is next:

- As targets adopt mitigations, these actors are likely to shift their TTPs and infrastructure and exploit any vulnerabilities to maintain persistence.
- With access to telecom and other networks, China’s intelligence services are likely using stolen data to track communications and physical movement of foreign targets in surveillance campaigns.



Hacktivist Group Claims DDoS Attack on ICJ's Website

What we know:

- Hacktivist group "Keymous+" has claimed to have targeted the official website of the International Court of Justice (ICJ) in a distributed denial-of-service (DDoS) attack.

Background:

- Keymous+ identifies itself as a North African group and has been targeting organizations in Europe, North Africa, the Middle East, and parts of Asia since late 2023.
- The varied range of targets indicates a lack of a solid ideological agenda.

Analyst note:

- The group stated that the alleged attack on the ICJ was a response to its Vice President Julia Sebutinde's statement that seemingly implied support for Israel. Keymous+ will likely keep targeting entities that support or align with Israeli policies.

1,200 Arrested in Africa Cybercrime Sweep

What we know:

- Operation Serengeti 2.0, a joint law enforcement campaign between African countries and the United Kingdom, led to arrests of more than 1,200 cybercriminals who targeted nearly 88,000 victims.
- The campaign dismantled over 11,000 malicious infrastructures and recovered USD 97.4 million from ransomware, scams, and business email compromise (BEC) schemes.

Background:

- Authorities shut down an illegal crypto mining operation in Angola, dismantled a USD 300 million scam and trafficking network in Zambia, and took down a USD 1.6 million inheritance fraud scheme in Côte d'Ivoire.

Analyst note:

- With many actors likely unapprehended, criminals will rebuild their infrastructures using bulletproof hosting services and other services to evade future law enforcement action.

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. CISA added four vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on August 25 and August 26. CISA also released 12 Industrial Control System (ICS) advisories on August 26 and August 28. Docker patched a vulnerability in Docker Desktop that had enabled containers to access the Docker Engine API without authentication, risking privilege escalation. Commvault has released security patches for four vulnerabilities that enable remote code execution (RCE) attacks, including a high severity vulnerability tracked as CVE-2025-57790. A flaw in Git due to improper handling of carriage return characters in configuration files can enable threat actors to execute arbitrary code and access sensitive data. An actively exploited FreePBX zero-day vulnerability has now been patched. The vulnerability impacted systems with the Administrator Control Panel (ACP), which are widely used by call centers, businesses, and service providers. A vulnerability in FujiFilm Healthcare Americas Corporation's Synapse Mobility software can be leveraged to escalate privileges, bypass authentication, and access protected medical data.

CRITICAL

CVE-2025-7775

What happened: Over 28,200 Citrix NetScaler ADC and Gateway instances are vulnerable to this critical RCE flaw that is already being actively exploited. Citrix has released security updates, and CISA confirmed the bug had been abused as a zero-day.

- **What this means:** Unpatched systems could enable attackers to gain full control of enterprise networks, enabling data theft, service disruptions, and follow-on ransomware or espionage campaigns.
- **Affected products:**
  - The affected products are listed in this advisory.

CRITICAL

CVE-2025-26496

What happened: A Type Confusion vulnerability in Salesforce Tableau Server and Tableau Desktop on Windows and Linux enables Local Code Inclusion (LCI). An attacker with local access could

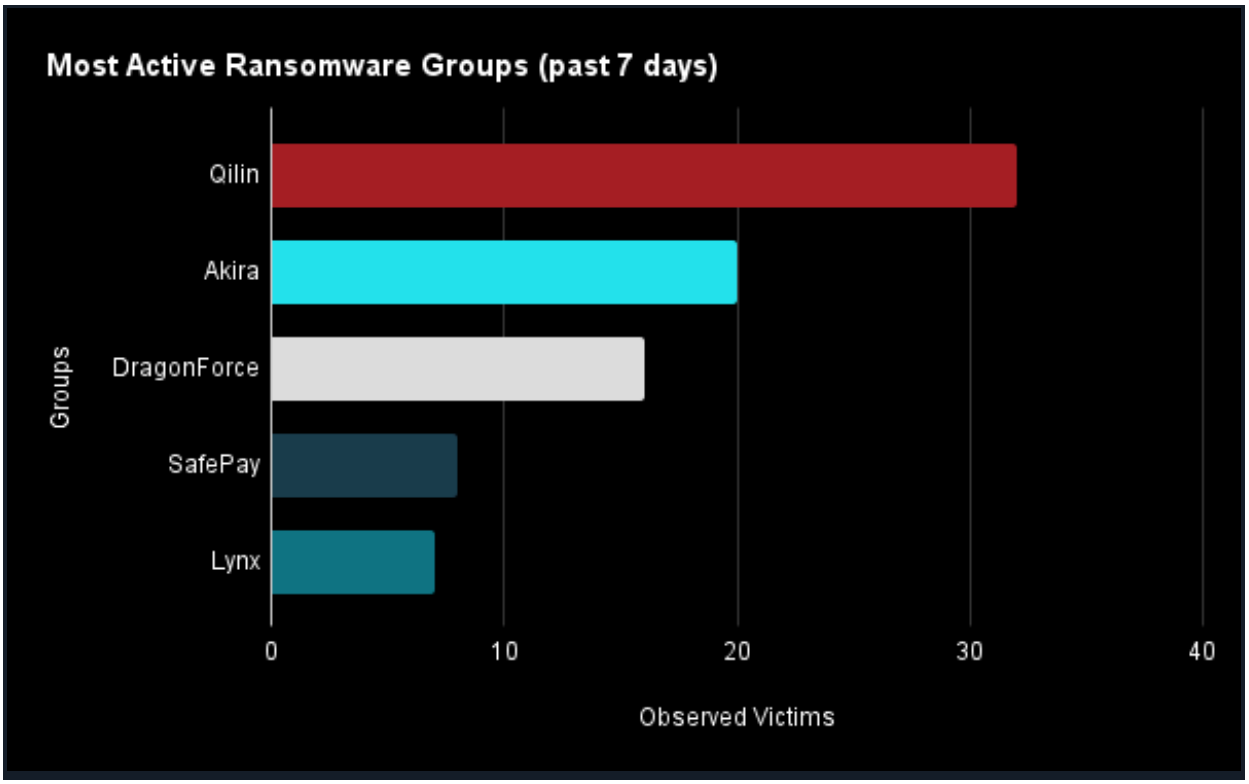
exploit the flaw to make Tableau misinterpret uploaded files, potentially executing unintended code.

- **What this means:** Since Tableau is widely used for business intelligence and data analytics, exploitation could lead to privilege escalation, system compromise, and exposure of sensitive enterprise data, posing significant risks to organizations.
- **Affected products:**
  - Tableau Server & Tableau Desktop: before 2025.1.4, before 2024.2.13, before 2023.3.20

Ransomware and Breach Intelligence

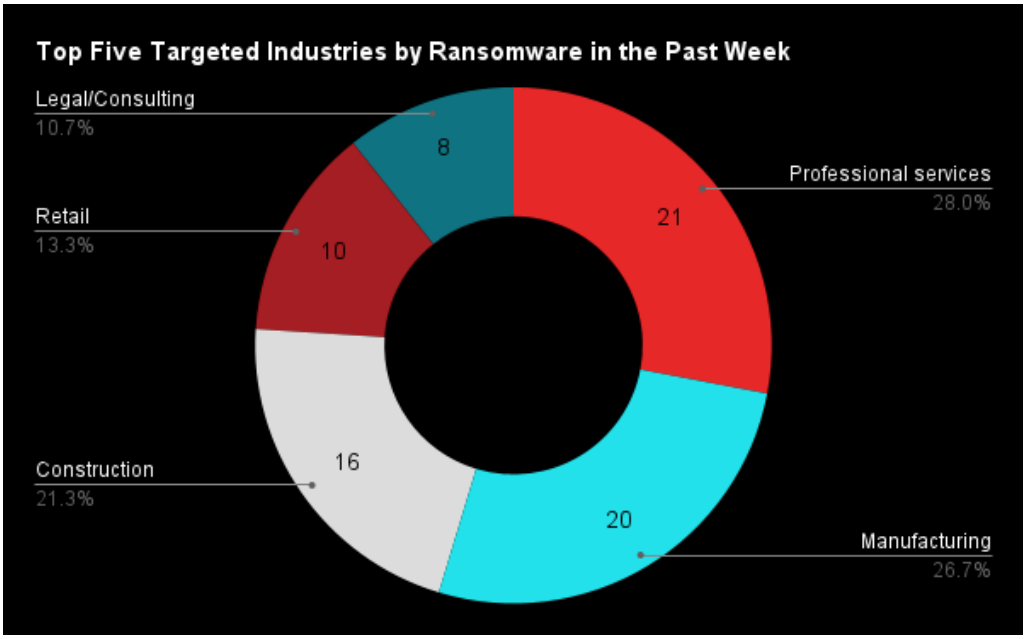
Ransomware and Breach Intelligence Key Findings

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



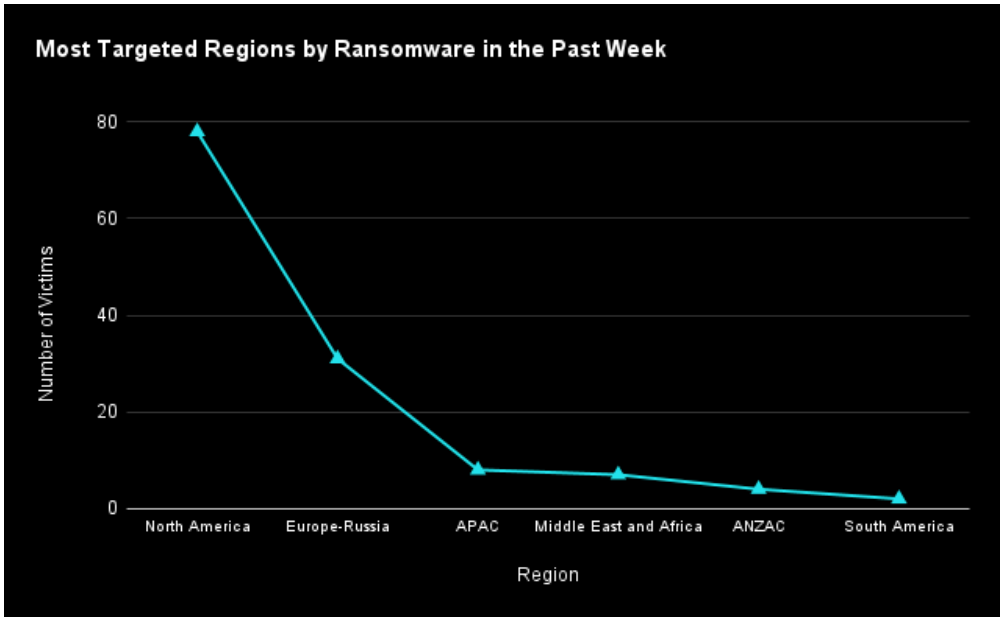
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Akira, DragonForce, SafePay, and Lynx were the most active ransomware groups. ZeroFox observed at least 130 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by Akira.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that professional services was the industry most targeted by ransomware attacks, followed by manufacturing, construction, retail, and. legal/consulting.



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-Russia. There were at least 78 ransomware attacks observed in North America, while Europe-Russia accounted for 31, Asia-Pacific (APAC) for eight, Middle East and Africa for seven, Australia and New Zealand (ANZAC) for four, and South America for five.

Recap of major ransomware events observed in the past week: Threat actor "Storm-0501" has shifted from traditional ransomware to targeting the cloud, focusing on data theft, cloud-based encryption, and extortion. Researchers have uncovered PromptLock, the first AI-powered ransomware, which leverages OpenAI's gpt-oss-20b via the Ollama API to generate Lua scripts for data theft and encryption across popular operating systems. Research shows that the Hook Android malware has evolved into a hybrid threat that combines ransomware and spyware to steal data and is spread through phishing campaigns and GitHub distribution. Nissan Japan has confirmed a data breach after the Qilin ransomware group claimed to have stolen 4 TB of data from its subsidiary CBI, including designs, financial records, and internal documents. DaVita, a kidney dialysis provider, has confirmed that a ransomware attack led to the theft of personal and health data belonging to nearly 2.7 million people.

Major Data Breaches in the Past Week

Targeted Entity	Healthcare Services Group (HSGI)	Ohio Medical Alliance	Intel
Number of Firms/Victims Affected	600,000 individuals	957,434 records	270,000 employees
Compromised Data Fields	Full name, Social Security number (SSN), driver's license number, state identification number, financial account information, account access credentials	SSNs, IDs, health files, and sensitive internal notes	Access to sensitive corporate and supplier information
Suspected Threat Actor	Yet to be determined	Yet to be determined	Yet to be determined
Country/Region	United States	United States	United States
Industry	Healthcare	Healthcare	Technology
Possible Repercussions	Identity theft, financial fraud, account takeover, tax fraud, loan or credit application fraud, phishing and social engineering, and SIM swapping	Identity theft, financial fraud, account takeover, employment fraud, phishing and social engineering, and blackmail or extortion	Identity theft, corporate espionage, supply chain compromises, BEC, insider threat exploitation, phishing and social engineering, credential stuffing, financial fraud, and data extortion

Three major breaches observed in the past week

Other major data breaches observed in the past week: A May data breach at Farmers Insurance affected 1.1 million customers after hackers accessed a third-party vendor's database. French

retailer Auchan has disclosed a cyberattack that exposed data from hundreds of thousands of loyalty accounts, which is also likely tied to the ongoing Salesforce breach campaign. ZeroFox has observed that the threat group "scattered lapsus$ hunters" is claiming responsibility for multiple data breaches and is actively selling both recent and older databases across diverse global sectors. Hackers carried out a large-scale data theft campaign breaching Salesloft and stole OAuth and refresh tokens linked to the Drift artificial intelligence (AI) chat agent.

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%