ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

June 13, 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 June 11, 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

Peace Talks Stall – SITREP #39: June 5, 2026

Clashes between Israel and Hezbollah in Lebanon are very likely holding up U.S. and Iranian negotiations on ending the war. There is a roughly even chance fighting in Lebanon causes the U.S.-Iran ceasefire to collapse while increasing the possibility the conflict spreads, particularly to the Red Sea. A full return to conflict remains unlikely as both sides have refrained from reigniting the conflict, despite repeated flare-ups. Since the last report, the United States has reportedly made revisions to the Memorandum of Understanding (MOU) on ending the war in Iran. Iran is unlikely to respond until matters in Lebanon are resolved. The status quo does not bode well for the global economy, as it requires the Strait of Hormuz (SoH) to remain closed. Consequently, the negative economic impacts of the war will likely intensify as the stalemate persists. Iran will likely move ahead with formalizing a toll system in the SoH so that it can financially benefit from the impasse.

ZeroFox Intelligence Brief – The Malicious Insider Threat

Intentional, or malicious, insider threats represent a significant attack vector in which likely disgruntled employees compromise organizations by misusing access to sensitive networks and data or abusing advantageous positioning to enact harm against the employer. An individual's likelihood of becoming an insider threat is often signaled by predisposing factors, such as their specific organizational positioning and access alongside various personal and professional vulnerabilities. Threat actors almost certainly monitor social media and dark web forums for disgruntled employees, whom they target to exploit as a means of gaining entry into specific corporate environments. Malicious insiders often execute highly structured operations that mirror external adversary tactics, utilizing their unique, high-level credentials and proprietary insights to facilitate their activities. Malicious insider threats will almost certainly continue to pose a significant risk—with detrimental effects that span beyond just a targeted organization—throughout 2026, as opportunities for insiders to "switch sides" are becoming increasingly accessible on social media and the dark web.

ZeroFox Intelligence Flash Report – Qilin's Latest Spree of Alleged Victims

Between June 2–5, 2026, ransomware and digital extortion (R&DE) threat actor Qilin claimed 15 new victims across nine countries in 72 hours; its targets spanned the healthcare, hospitality, manufacturing, consumer services, and critical infrastructure sectors. Qilin (also known as Agenda) is a sophisticated Russian-language R&DE threat collective that primarily offers

ransomware-as-a-service (RaaS) to affiliates and targets high-value critical infrastructure with a double extortion model. On June 4, 2026, Qilin posted sensitive data samples allegedly from Avcon Jet—an Austrian-based and major European aviation company offering business jet management and chartered flights internationally—on its dark web leak site. ZeroFox assesses that Qilin will very likely conclude Q2 2026 as the most active ransomware collective globally. This would signify both dominance in the first half of 2026 and an unbroken 12-month period as the leading ransomware threat actor, beginning in Q2 2025.

ZeroFox Intelligence Assessment – Group of Seven (G7) Summit

The 2026 G7 summit returns to Évian-les-Bains, France, which hosted the 2003 G8. The threat picture is shaped by the active conflict in Iran and Ukraine, persistent domestic unrest in France, and the venue's unique cross-border geography, with the nearest international airport situated in Switzerland and outside French jurisdiction. France's security services have a strong track record at G7-class events (including its most recent G7 in 2019 and the 2024 Summer Olympics). Therefore, the principal physical risk to the 2026 G7 summit is not the venue itself; rather, it stems from anti-G7 mobilization nearby, lone-actor terrorism, and spillover effects of the Iran conflict. The cyber risk to the summit is almost certainly elevated. Iranian-aligned actors have been targeting G7 members since March, and pro-Russian collectives have been targeting the event since Russia was removed from the group in 2014. Russian-aligned actors have frequently targeted the government, banking, and transportation infrastructures of G7 members in retaliation for their support of Ukraine. Cyberattacks against G7 infrastructure, sponsors, and delegations—including distributed denial-of-service (DDoS), website defacement, credential theft, and event-themed phishing—are very likely. Russian-linked disinformation operations targeting France's information environment are almost certain.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

PCPJack Hijacks Cloud Servers to Establish Distributed Email Relay Network

What we know:

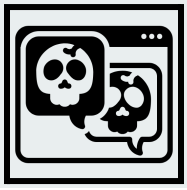
- Threat actor PCPJack has reportedly hijacked servers of three major cloud platforms to create a covert Simple Mail Transfer Protocol (SMTP) email relay network.
- Approximately 230 active proxy nodes were discovered, potentially suggesting the email operation had already reached a large scale.

Background:

- The operation was discovered using exposed directories on the group's command-and-control (C2) server that contained source code, deployment tools, logs, scanners, and active configurations.
- PCPJack was first discovered in April 2026, when researchers reportedly took steps to remove processes and artifacts associated with the TeamPCP threat group.

Analyst note:

- The campaign's use of hijacked cloud servers as SMTP relays likely enables malicious emails to bypass standard security filters as they originate from trusted infrastructure.
- Additionally, given PCPJack's focus on credential theft, the SMTP infrastructure is likely to support campaigns aimed at acquiring high-value credentials such as developer secrets, cloud access keys, Application Programming Interface (API) tokens, putting software maintainers, developers, and workflows at risk.



Russian Threat Groups Exploit Patched WinRAR Flaw in Ukraine Campaign

What we know:

- Two Russia-aligned threat groups, "Gamaredon" and "SHADOW-EARTH-066", are reportedly exploiting a patched WinRAR path traversal vulnerability (CVE-2025-8088) to target Ukrainian organizations.
- The campaigns deploy information-stealing malware strains to harvest browser credentials and documents.

Background:

- SHADOW-EARTH-066 delivers the GIFTEDCROOK infostealer in-memory. Notably, the group has shifted exfiltration from Telegram to dedicated C2 servers following Russia's blocking of the platform.
- Meanwhile, Gamaredon's delivers GammaSteel, a real-time file monitoring infostealer.

Analyst note:

- Unknown LNK files in Startup folders, unexpected PowerShell execution via cmd.exe, and unusual outbound C2 traffic are very likely Indicators of Compromise (IOCs).
- The threat groups are also likely prioritizing gaining initial access over immediate intelligence value with the exploitation of a long-patched vulnerability, reserving the access and stolen data for future high-value attacks.

ShinyHunters Targets Oracle PeopleSoft in Data Theft Campaign

What we know:

- The ShinyHunters extortion group is reportedly targeting Oracle PeopleSoft servers in an ongoing data theft attack, which has affected over 100 organizations, mostly in the education sector.

Background:

- PeopleSoft—used by large organizations to manage student administration, supply chain management, procurement, human resources, payroll, and finance—was reportedly exploited using a “gadget chain” of old and zero-day vulnerabilities.
- The IoCs are listed here.

Analyst note:

- Operational disruptions—including payments, fee processing, scholarships, and procurement—are likely in the near term at affected organizations.
- If ransom demands go unmet, ShinyHunters will very likely publish portions of the stolen data, with students and faculty being the most exposed demographic.
- The compromised data is likely to be weaponized in financially motivated phishing and social engineering campaigns.

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 three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on June 5, June 8, and June 9, 2026. Additionally, on June 9, 2026, CISA released three Industrial Control Systems (ICS) advisories, which feature a total of four vulnerabilities: CVE-2026-6866, CVE-2024-3596, CVE-2025-40946, and CVE-2026-41125. Microsoft released security updates addressing 200 flaws and three publicly disclosed zero-day vulnerabilities. The updates include 33 critical vulnerabilities: 28 related to remote code execution (RCE), four associated with elevation of privilege, and one concerning information disclosure. Google promoted Chrome 149 with patches for 429 vulnerabilities, of which most were use-after-free and insufficient validation of untrusted input issues. Additionally, numerous inappropriate implementation, insufficient policy enforcement, and out-of-bounds flaws were also addressed. Critical security flaws have been disclosed in Vertiv uninterruptible power supply (UPS) network cards and Trane Tracer SC+ HVAC controllers used in data centers. Unauthenticated attackers can remotely exploit these vulnerabilities to bypass authentication, execute arbitrary code, or trigger denial-of-service conditions.

HIGH

CVE-2026-28318

What happened: This is an already-patched denial-of-service (DoS) vulnerability targeting a SolarWinds Serv-U vulnerability, enabling attackers to crash the service without authentication.

- **What this means:** Unauthenticated attackers can exploit this vulnerability to trigger a DoS state and crash the Serv-U service and abruptly halt secure file transfer operations across the organization.
  - **Affected products:** Serv-U versions 15.4.2, 15.5, and 15.5.1, which have reached End-of-Life (EoL)

HIGH

CVE-2026-20230

What happened: Cisco has released security updates to patch a Unified Communications Manager (Unified CM) flaw, which reportedly enabled attackers to gain root privileges. The flaw was fixed in Cisco Unified CM versions 14SU6 and 15SU5.

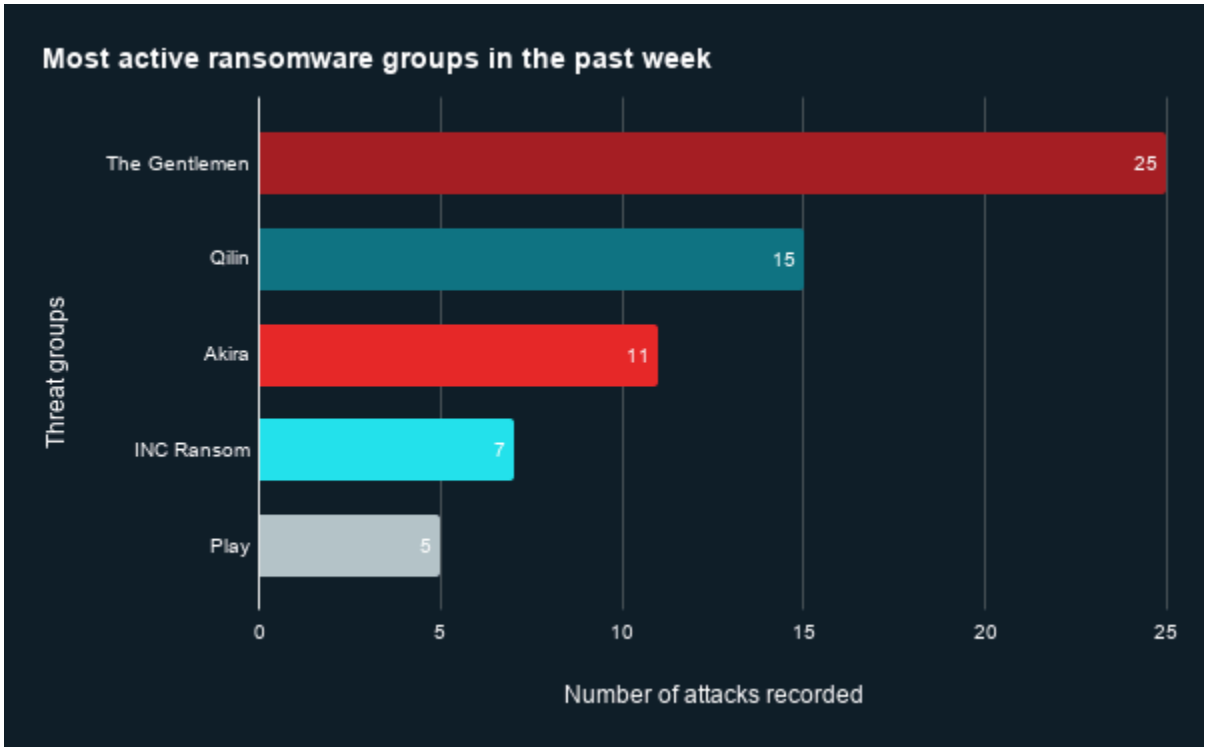
- **What this means:** Attackers can execute a full root-level system compromise, take complete control of telephony infrastructure, and intercept communications.
  - **Affected products:** Cisco Unified CM and Unified CM SME if they have the WebDialer service enabled

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

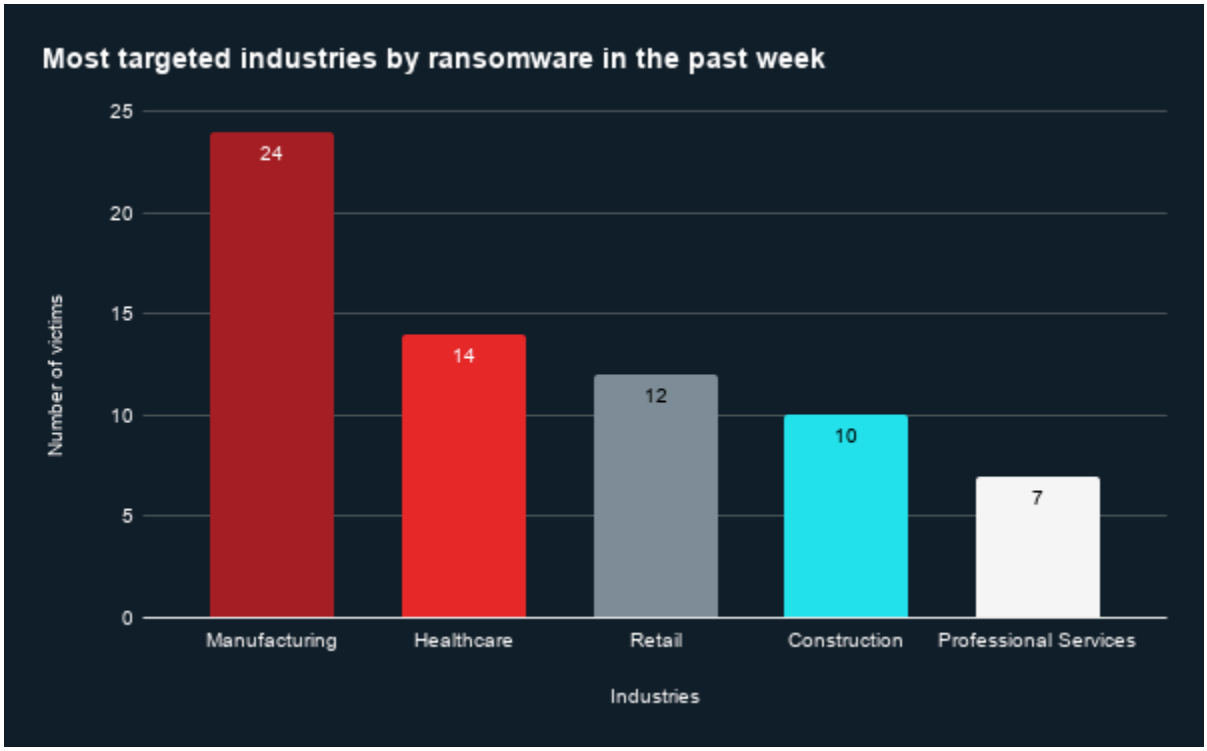
Ransomware Group, Industry, and Regional Trends

Last week in ransomware: In the past week, The Gentlemen, Qilin, Akira, INC Ransom, and Play were the most active ransomware groups. ZeroFox observed close to 108 ransomware victims disclosed, most of whom were located in North America. The Gentlemen ransomware group accounted for the largest number of attacks, followed by Qilin.



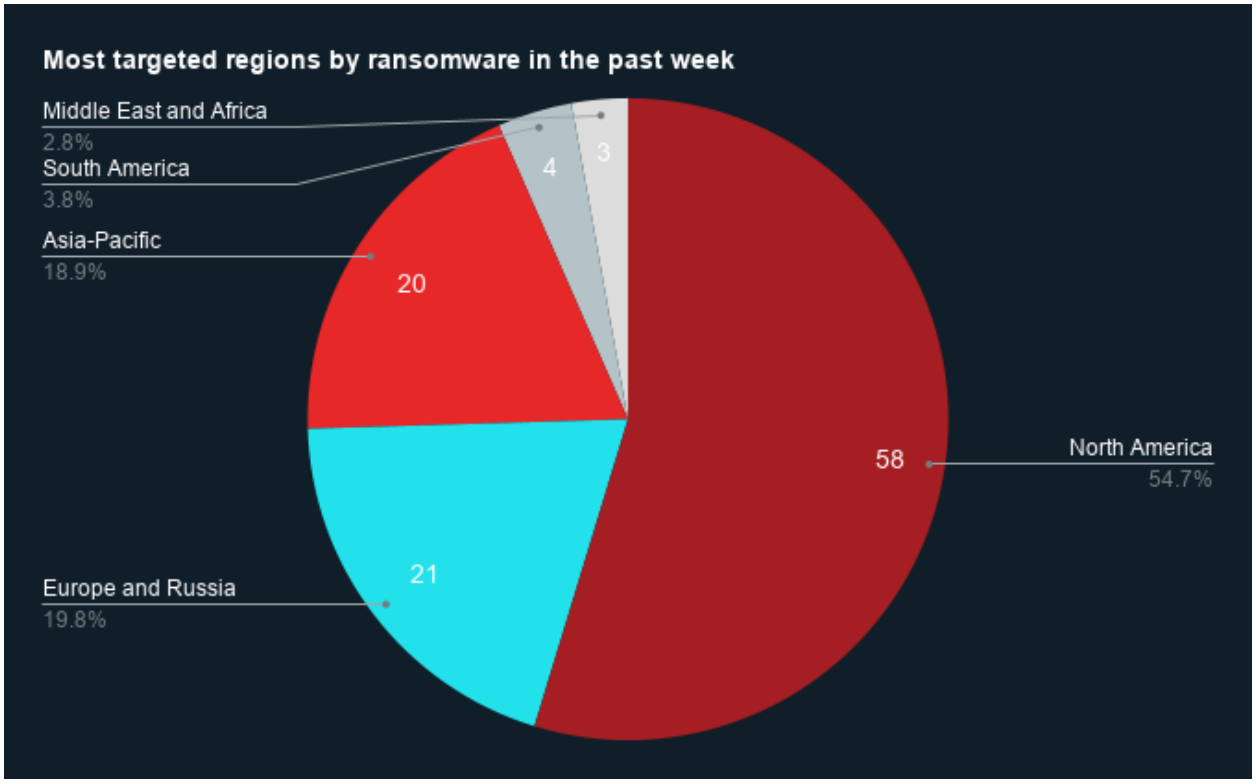
Source: ZeroFox Internal Collections

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



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 58 ransomware attacks observed in North America, while Europe and Russia accounted for 21, Asia-Pacific (APAC) for 20, South America for four, and the Middle East and Africa for three.



Source: ZeroFox Internal Collections

Major Data Breaches Reported in the Past Week

Targeted Entity	Nottingham University	Tchap	Oxford University
Compromised Entities/Victims	Current students and alumni	French public sector and civil servants (73,467 user accounts)	Alumni, research staff, and employer users of CareerConnect platform
Compromised Data Fields	Personally identifiable information (PII), National Insurance (NI) numbers, protected characteristics, email address, postal address, financial information, and university-related details such as course information and student ID	643,459 messages from 876 chat rooms (including communications involving the Interior, Finance, and Defense ministries), 13.5 GB of files, hardcoded credentials, and plaintext meeting invitations with active Zoom and Webex links and access details	PII, email addresses, and encrypted passwords (for users who do not sign in using Single Sign-On)
Suspected Threat Actor	ShinyHunters	PwnForums user misere	N/A
Country/Region	United Kingdom	France	United Kingdom
Industry	Education	Government	Education
Possible Repercussions	Operational disruptions to administrative and financial processes, public exposure of stolen data, and financially motivated phishing and social engineering campaigns	Data likely to be leveraged for nation-state espionage, political leverage, and policy influence. French government personnel are very likely to be targeted in social engineering and spear phishing campaigns	Brute-force attacks, account takeover attempts, identity theft, social engineering, and phishing

Three major breaches observed in the past 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%