ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

May 23, 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 May 21, 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 - Grafana Labs Source Code Theft and Extortion Attempt 2
- ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 11 2

Cyber and Dark Web Intelligence Key Findings **4**
- GitHub Discloses Unauthorized Access to Internal Repos 4
- Banana RAT Campaign Targets Brazilian Banking Customers 4
- Grafana Discloses GitHub Environment Compromise, Source Code Stolen 5

Exploit and Vulnerability Intelligence Key Findings **7**
- CVE-2026-8153 7
- CVE-2026-45829 8

Ransomware and Breach Intelligence Key Findings **10**
- Ransomware Group, Industry, and Regional Trends 10
- Significant Data Breaches Reported Over the Past Week 13

Appendix A: Traffic Light Protocol for Information Dissemination **14**

Appendix B: ZeroFox Intelligence Probability Scale **15**

This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report - Grafana Labs Source Code Theft and Extortion Attempt

On May 17, 2026, Grafana Labs disclosed that its private code was stolen from a GitHub repository using a known vulnerability called a "Pwn Request." The breach was claimed by ransomware and digital extortion (R&DE) collective CoinbaseCartel; however, Grafana Labs refused to pay the ransom demanded. CoinbaseCartel first appeared in September 2025, focusing exclusively on data theft and extortion—removing proprietary information from servers before demanding ransom. CoinbaseCartel reportedly shares infrastructure, including a domain, with the Scattered Lapsus$ Hunters (SLSH) ecosystem, suggesting it is very likely an offshoot of the SLSH and likely operates as the data theft extortion affiliate for the larger SLSH collective. This attack very likely signifies a further diversification within the SLSH ecosystem. SLSH is already the dominant English-language R&DE collective and has previously splintered into specializations; more brand diversification within the ecosystem is very likely in 2026 and beyond.

ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 11

The Underground Economist is an intelligence-focused series illuminating Dark Web findings in digestible tidbits from our ZeroFox Dark Ops intelligence team.

ZEROFOX

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

GitHub Discloses Unauthorized Access to Internal Repos

What we know:

- GitHub is investigating unauthorized access to its internal repositories, with the activity resulting in the exfiltration of 3,800 internal repositories of the platform so far.
- However, the company has clarified it has not found evidence of impact to repositories belonging to customer enterprises.

Background:

- GitHub detected and contained a compromise of an employee device via a poisoned Visual Studio (VS) Code extension.
- Threat group "TeamPCP," which has been attributed to the ongoing ShaiHulud supply chain attack, has listed GitHub's alleged source code and internal organizations for sale on a cybercrime forum.
- As a security measure, the platform has rotated affected credentials.

Analyst note:

- The stolen data, currently open for bids over USD 50,000, is likely to be of interest to nation-state and other high-profile threat groups.
- Threat actors are likely to study the source code (if legitimate) to detect vulnerabilities, abuse harvested credentials and Continuous Integration and Continuous Delivery (CI/CD) pipeline access to infiltrate downstream systems, and manipulate legitimate GitHub packages to push malicious code to unsuspecting developers.

Banana RAT Campaign Targets Brazilian Banking Customers

What we know:

- Financially motivated threat group SHADOW-WATER-063 is reportedly targeting Brazilian banking customers with a remote access trojan (RAT) called Banana RAT.
- The campaign uses phishing links and fake invoice files distributed through WhatsApp and malicious domains to infect victims and steal money in real time.

Background:

- Victims are tricked into downloading a fake invoice file (Consultar_NF-e.bat) that launches hidden PowerShell commands and executes malware directly in memory using fileless techniques.
- Banana RAT gives attackers full remote control over infected systems, including screen monitoring, keystroke logging, and the ability to freeze user input during fraudulent banking activity.

Analyst note:

- The infrastructure used to generate hundreds of malware variants at scale may enable more resilient and scalable fraud campaigns against Brazilian financial institutions.
- The campaign could strengthen Latin American cybercrime ecosystems by increasing demand for malware obfuscation services, stolen banking access, and fraud enablement tools.

Grafana Discloses GitHub Environment Compromise, Source Code Stolen

What we know:

- Open-source analytics and visualization application Grafana Labs has disclosed that a threat actor gained unauthorized access to its GitHub environment and downloaded its source code.
- Extortion group CoinbaseCartel has claimed responsibility for the attack.

Background:

- Grafana says it has invalidated the compromised credentials.
- The company has also refused to pay the ransom demanded by the attackers threatening to publish the stolen database.
- The company clarified that no personal or customer information has been affected and its operations remain uninterrupted.

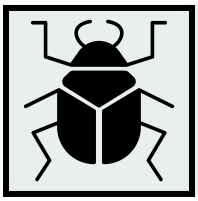
Analyst note:

- Source code compromise is likely to enable threat actors to find vulnerabilities (if any), login logic, or infrastructure details that can be exploited in future attacks.

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 vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on May 15 and May 20, 2026. Additionally, on May 19, 2026, CISA released five Industrial Control Systems (ICS) advisories, which includes CVE-2026-4293, CVE-2026-8598, CVE-2026-8602, CVE-2026-0300, and CVE-2025-3465. A proof-of-concept (PoC) exploit for a privilege escalation zero-day, dubbed "MiniPlasma," has been released. The flaw reportedly abuses a Driver ("cldflt.sys") to obtain SYSTEM-level access on certain fully patched systems. Four vulnerabilities, collectively called "Claw Chain," have been discovered in OpenClaw. The flaws enable attackers to move from initial access to credential theft, privilege escalation, and persistent backdoor deployment. CVE-2026-42897 is an actively exploited spoofing vulnerability. The flaw enables threat actors to execute arbitrary code via cross-site scripting (XSS) to target Outlook on the web. Open-source web content management system (CMS) Drupal has announced an emergency security release for a high-severity vulnerability affecting Drupal core versions 8 and later, warning that exploits could emerge within hours of disclosure. A PoC exploit has been released for the "PinTheft" Linux privilege escalation vulnerability affecting the kernel's Reliable Datagram Socket (RDS) component. The flaw enables local attackers to gain root privileges under specific conditions, primarily impacting Arch Linux systems with the RDS module enabled. CVE-2024-12802 is a vulnerability in SonicWall Gen6 SSL-VPN appliances that enables attackers with valid credentials to bypass multi-factor authentication (MFA) protections through the User Principal Name (UPN) login format. A vulnerability in Anthropic Claude Code's network sandbox could have allowed attackers to bypass outbound traffic restrictions through a SOCKS5 hostname null-byte injection flaw. Threat actors are reportedly actively exploiting CVE-2026-42945, a critical heap buffer overflow vulnerability dubbed "Nginx Rift" affecting NGINX shortly after public PoC code was released.



CRITICAL

CVE-2026-8153

What happened: This is a command injection vulnerability in the Dashboard Server interface of Universal Robots PolyScope 5—an operating system (OS) for collaborative robots.

- **What this means:** The flaw enables an unauthenticated attacker with network access to execute remote commands on the system and gain full control of the robot system. Successful exploitation is very likely to result in manipulation of robot operations and potential physical safety hazards to personnel operating affected systems.
    - **Affected products:** PolyScope 5 versions prior to 5.25.1

CRITIAL

CVE-2026-45829

What happened: This is an authentication bypass vulnerability in ChromaDB. The flaw enables a crafted request to fetch and execute a malicious model before authentication is verified, meaning the payload executes successfully even as the request is ultimately rejected.

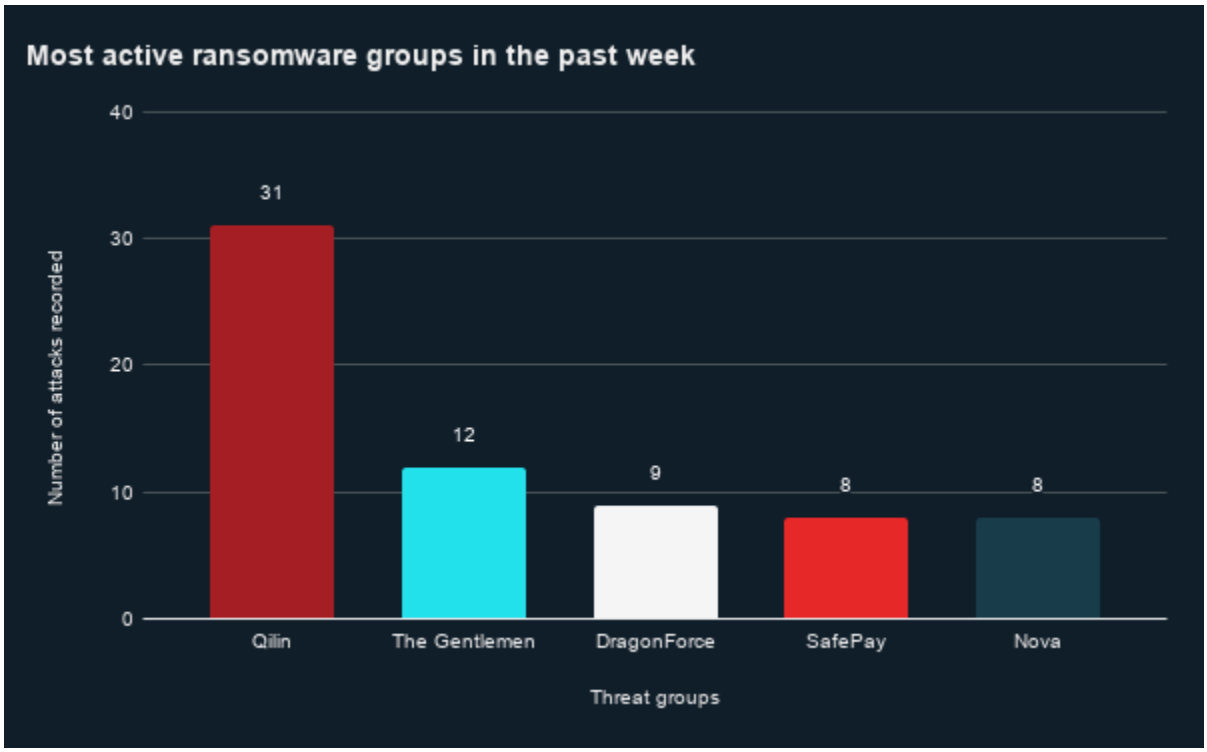
- **What this means:** Successful exploitation is very likely to result in arbitrary code execution on exposed instances. Given ChromaDB's privileged access to artificial intelligence (AI) pipelines, a compromised instance is likely a significant downstream risk to connected systems and sensitive data.
    - **Affected products:** ChromaDB Python FastAPI server versions 1.0.0 through 1.5.8 exposed over HTTP

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

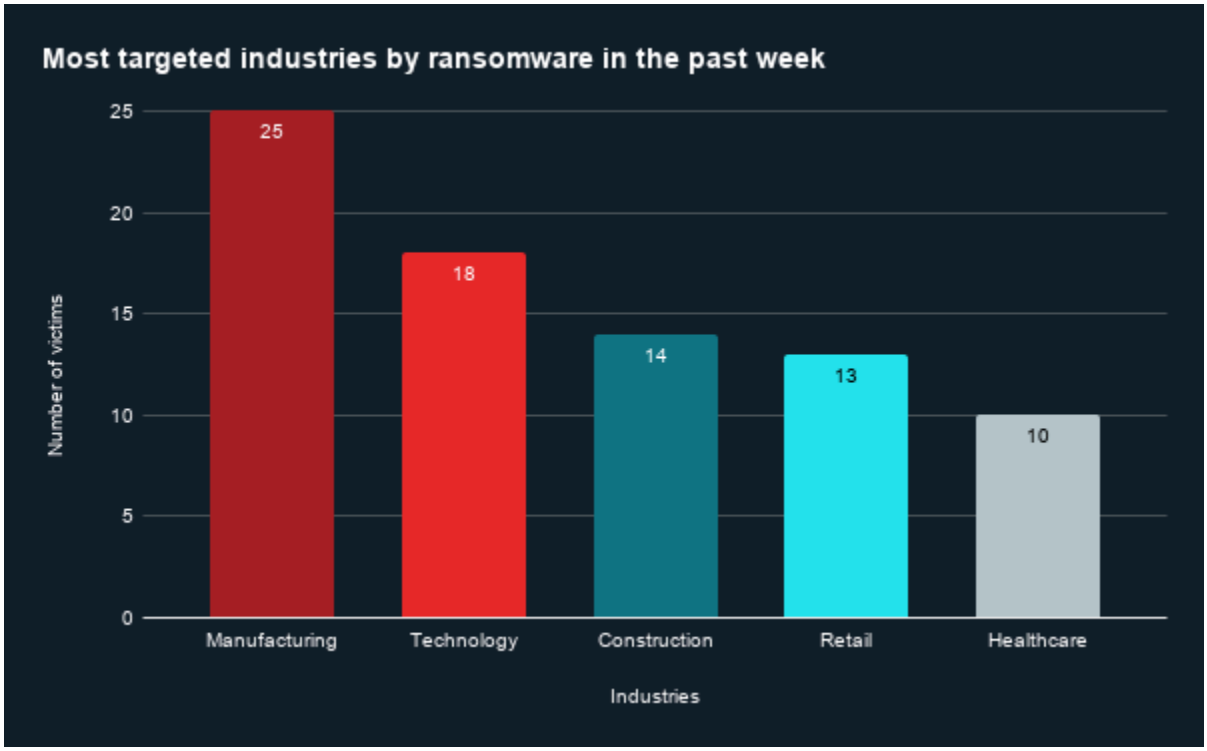
Ransomware Group, Industry, and Regional Trends

Last week in ransomware: In the past week, Qilin, The Gentlemen, DragonForce, SafePay, and Nova were the most active ransomware groups. ZeroFox observed close to 125 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by The Gentlemen.



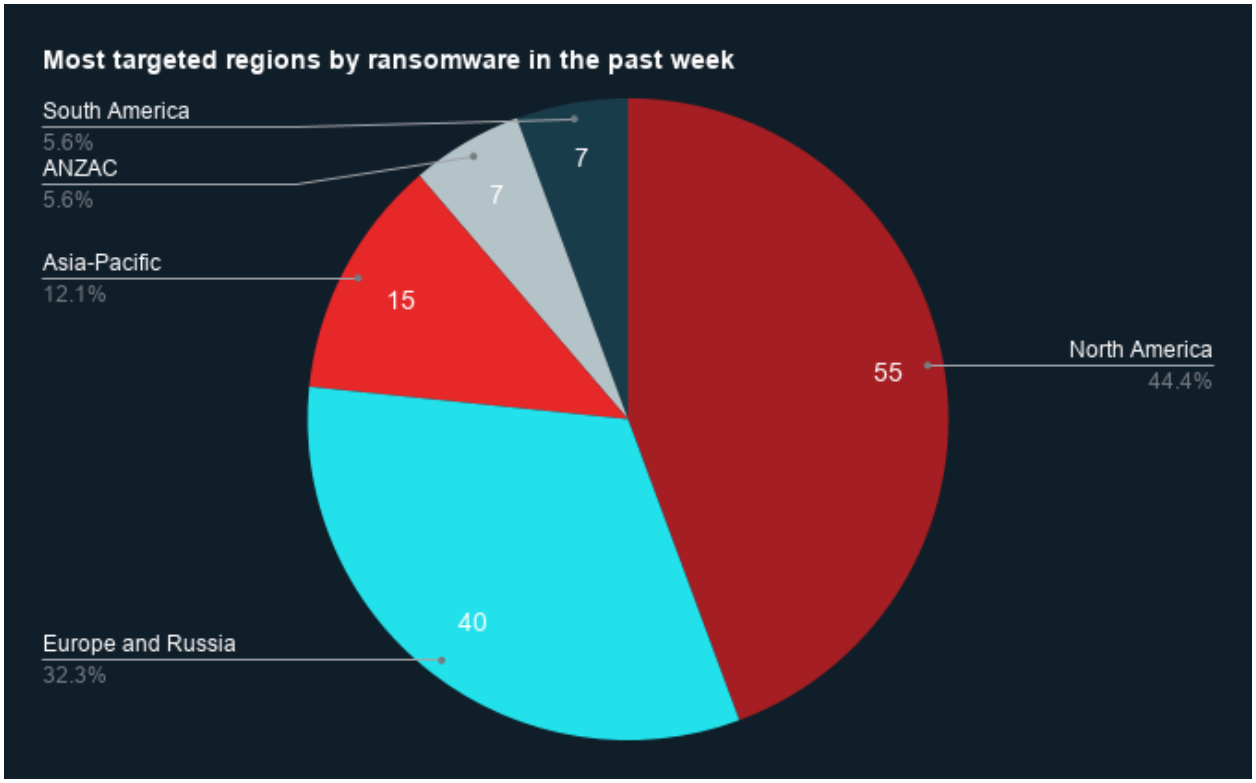
Source: ZeroFox Internal Collections

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

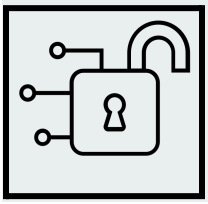


Source: ZeroFox Internal Collections

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 55 ransomware attacks observed in North America, while Europe and Russia accounted for 40, Asia-Pacific (APAC) for 15, Australia and New Zealand (ANZAC) for seven, and South America for seven as well.



Source: ZeroFox Internal Collections



Significant Data Breaches Reported Over the Past Week

Targeted Entity	Extant Aerospace	CTT Correios de Portugal	NYC Health + Hospitals Corporation
Compromised Entities/Victims	3,012 individuals	468,000 records of individuals	1.8 million current and former patients and employees
Compromised Data Fields	Names, addresses, dates of birth, Social Security numbers (SSNs)	Personally identifiable information (PII), including email addresses, full names, phone numbers, system metadata, shipping address, and parcel tracking codes	Protected Health Information (PHI), including health insurance details, biometric data, and billing and claims information and PII, including SSNs, and financial data
Suspected Threat Actor	N/A	Boogeyman	N/A
Country/Region	United States	Portugal	United States
Industry	Defense/Aerospace, Manufacturing	Logistics	Healthcare
Possible Repercussions	Potential operational impact to U.S. defense supply chain and targeted social engineering against defense sector personnel	Parcel phishing campaigns impersonating CTT, financial fraud targeting exposed individuals, tampering of packaging, and resale of combined PII and logistics data	Identity theft, financial and medical fraud, long-term exposure of sensitive personal identifiers

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%