# ZEROFOX®

## *Weekly Intelligence Brief*

**Classification: TLP:GREEN**

**June 21, 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 June 19, 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 Flash Report - Mobile Numbers Advertised for Sale in Dark Web Forum

On June 7, 2025, threat actor "Machine1337" posted on the predominantly Russian-speaking dark web forum xss, advertising the sale of mobile numbers from at least 20 companies. Machine1337 claimed that the mobile numbers are "freshly scraped and verified" and offered access to a free sample of the data. It is unclear whether these numbers are associated with personal or corporate mobile phones. While access to phone numbers would not directly facilitate a cyberattack, it could enable an attacker to conduct various types of social engineering activities that can result in subsequent exploitation. The phone numbers could also aid various types of fraud activities—particularly if a buyer is able to enrich the data by correlating other types of personally identifiable information (PII) to the phone numbers.

## ZeroFox Intelligence Flash Report - Israel and Iran at War

On June 12, 2025, Israel began what it said would be days of attacks against Iranian military and nuclear sites. In the coming days, there will likely be a comprehensive campaign to destroy Iranian air defense systems, communications networks, and offensive military capabilities, as well as its nuclear weapons program. Iran will almost certainly retaliate. In addition to drone attacks against Israel, Iran will likely also launch ballistic missiles, which are generally harder to intercept. Strikes from what is left of Iran's proxies in Syria are also likely. Historically, Iran's full retaliation to military aggression has not been immediate, and its options remain extremely limited due to the government's conventional military weaknesses and degradations to its proxies. Western physical assets in the region are at risk of terror attacks, with embassies, military installations, international organizations, and Western companies in the region all being potential targets. In addition, the assets of oil companies, financial services, and telecommunications are likely targets for cyberattacks, which allows Iran plausible deniability. The Middle Eastern oil industry is particularly vulnerable, as Iran has demonstrated an ability to impact the industry's operations; there is a roughly even chance Iran will block oil supply through the strategic Strait of Hormuz (SoH).

ZEROFOX
Weekly Intelligence Brief

# Cyber and Dark Web Intelligence

# Cyber and Dark Web Intelligence Key Findings

## Iran's Largest Crypto Exchange Nobitex Hit by Major Cyberattack

**What we know:**

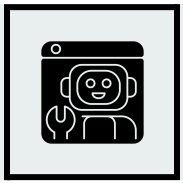
- On June 18, 2025, pro-Israel hacktivist group "Predatory Sparrow" claimed responsibility for a cyberattack on Nobitex, Iran's largest cryptocurrency exchange, reportedly stealing over USD 90 million in crypto assets.
- The group reportedly burned the crypto by sending it to vanity wallet addresses with embedded anti-Islamic Revolutionary Guard Corps (IRGC) messages.
- The group has also threatened to release source code and internal documents.
- As of this writing, the Nobitex website is down and displays a 504 Gateway Timeout error message.

**Background:**

- The group also breached Iran's Bank Sepah on June 17, reportedly leading to the destruction of data.
- Nobitex is reportedly linked to the IRGC and Iranian leadership.
- Additionally, Iran also experienced a near-total internet blackout on June 18.
- Iran's state broadcaster has recently called on its citizens to delete WhatsApp from their phones, alleging that the messaging app is gathering user data and transmitting it to Israel.

**What is next:**

- These consecutive cyberattacks signal an intensified digital offensive in the Iran-Israel conflict that targets IRGC-linked financial networks and disrupts Iran's financial operations.
- Similar politically driven cyberattacks by hacktivist groups are likely to continue.



## "WormGPT" Variants Exploiting Popular AI Tools for Illegal Acts

**What we know:**

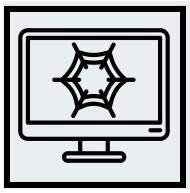
- New variants are keeping the cybercriminal AI generative tool WormGPT active—even after its shutdown in 2023—by reportedly exploiting existing large language model (LLM) tools, including Mistral AI's Mixtral, to bypass built-in safety features.

**Background:**

- WormGPT is an AI tool that runs without censorship and is used for illegal acts. New variants "zin0vich-WormGPT" and "keanu-WormGPT" have reportedly been advertised on dark web forums.

**Analyst note:**

- The re-emergence of malicious AI tools likely indicates that LLM security barriers are not able to keep cybercriminals out. "Jailbreak-as-a-service," a term used to describe LLM jailbreaking, is likely to emerge to cater to this market, lowering the technical expertise barrier required for threat actors to abuse generative AI for illegal acts.



## Law Enforcement Takes Down Long-Standing Dark Web Market

**What we know:**

- European authorities have dismantled Archetyp Market, a major dark web marketplace. The platform's infrastructure was taken offline, its administrator arrested, and assets worth EUR 7.8 million (approximately USD 9 million) seized.

**Background:**

- Archetyp Market was an illicit forum with over 600,000 users that facilitated anonymous global trade in substances like fentanyl and generated over EUR 250 million (approximately USD 288 million) in transactions.

**Analyst note:**

- Following the takedown of Archetyp Market, authorities will likely analyze seized data to identify and pursue other key actors, such as top vendors, buyers, and affiliated networks. This can likely lead to further arrests, asset seizures, and potential intelligence-sharing with international partners to dismantle related drug trafficking operations.

# Exploit and Vulnerability Intelligence

# Exploit and Vulnerability Intelligence Key Findings

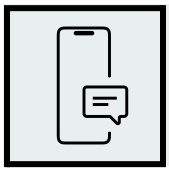
In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on June 16 and June 17, 2025. CISA also released 15 Industrial Control Systems (ICS) vulnerabilities on June 12 and June 17, as well as an advisory on SimpleHelp RMM vulnerability, warning that ransomware actors were targeting unpatched versions. Meanwhile, Veeam fixed a critical remote code execution (RCE) vulnerability, among other bugs, in some versions of Veeam Backup & Replication. Threat actor "TaxOff" has been found to be behind the exploitation of CVE-2025-2783, a now-patched Google Chrome vulnerability. Unknown threat actors were observed attempting to exploit a Zyxel vulnerability tracked as CVE-2023-28771 on June 16; the bug was previously targeted in a co-ordinated attack against Denmark's critical infrastructure nearly two years ago. A new malicious campaign has been observed actively exploiting a critical vulnerability in Langflow to deliver the Flodrix botnet malware. An out-of-bounds write vulnerability in MicroDicom DICOM Viewer enables remote code execution if a user opens a malicious file or web page. Two security vulnerabilities were identified in SinoTrack GPS devices that could enable attackers to control certain remote functions on connected vehicles and track their locations.

**HIGH**

## CVE-2023-33538

**What happened**: This is a command injection vulnerability in TP-Link wireless routers, which CISA has added to its KEV catalogue. The vulnerability could also be present in end-of-life (EOL) TP-Link router models.

- **What this means:** The bug is likely to enable execution of arbitrary code. Successful exploitation is likely to lead to system compromise or even complete takeover. Operational technology (OT) systems in critical infrastructure settings are likely to be susceptible to being targeted using the bug.
- **Affected products:**
  - TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2



**CRITICAL**

## CVE-2025-43200

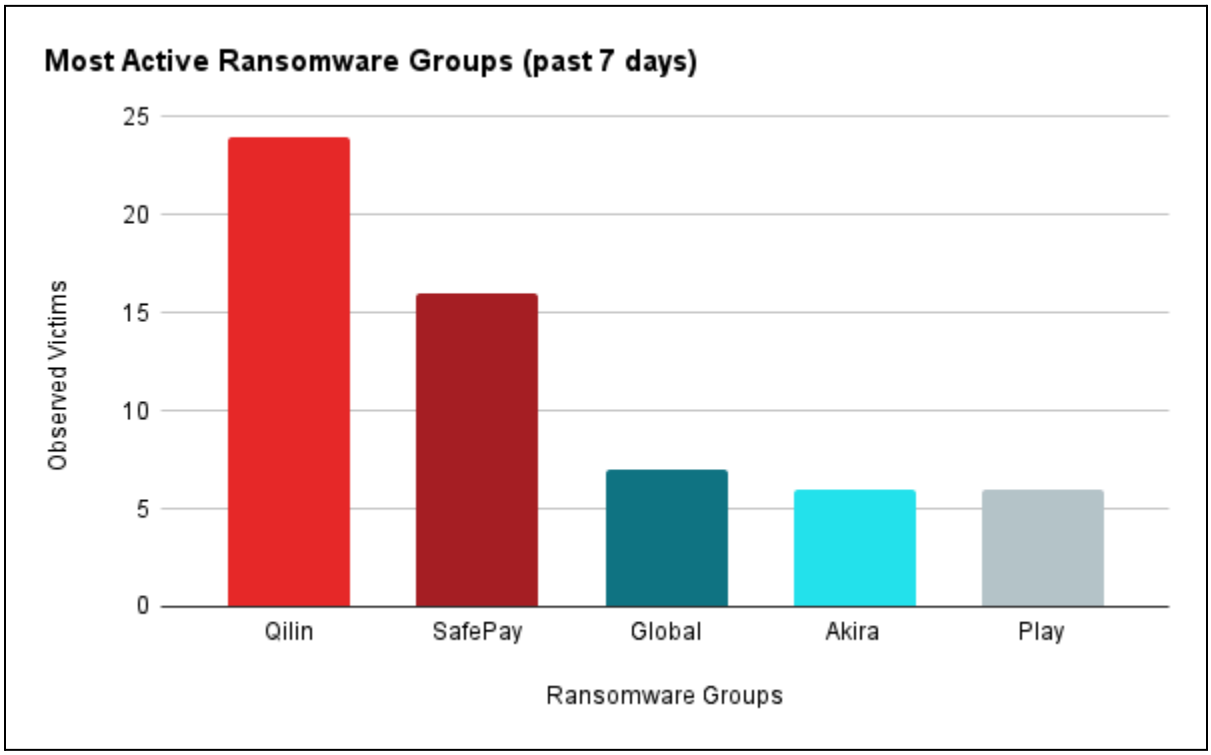
**What happened:** This vulnerability in Apple's iMessage was exploited to install Paragon's Graphite spyware in targeted victims' devices. Apple recently updated its advisory, dated February 10, 2025, to reveal that the bug was patched. Apple described the vulnerability as a logic issue in processing a malicious photo or video shared through an iCloud link.

- **What this means:** The vulnerability is likely to be exploited in unpatched devices for politically motivated attacks. At least two European journalists have reportedly already been targeted using the bug and the spyware.
- **Affected products:**
  - Versions before iOS 18.3.1 and iPadOS 18.3.1

# Ransomware and Breach Intelligence

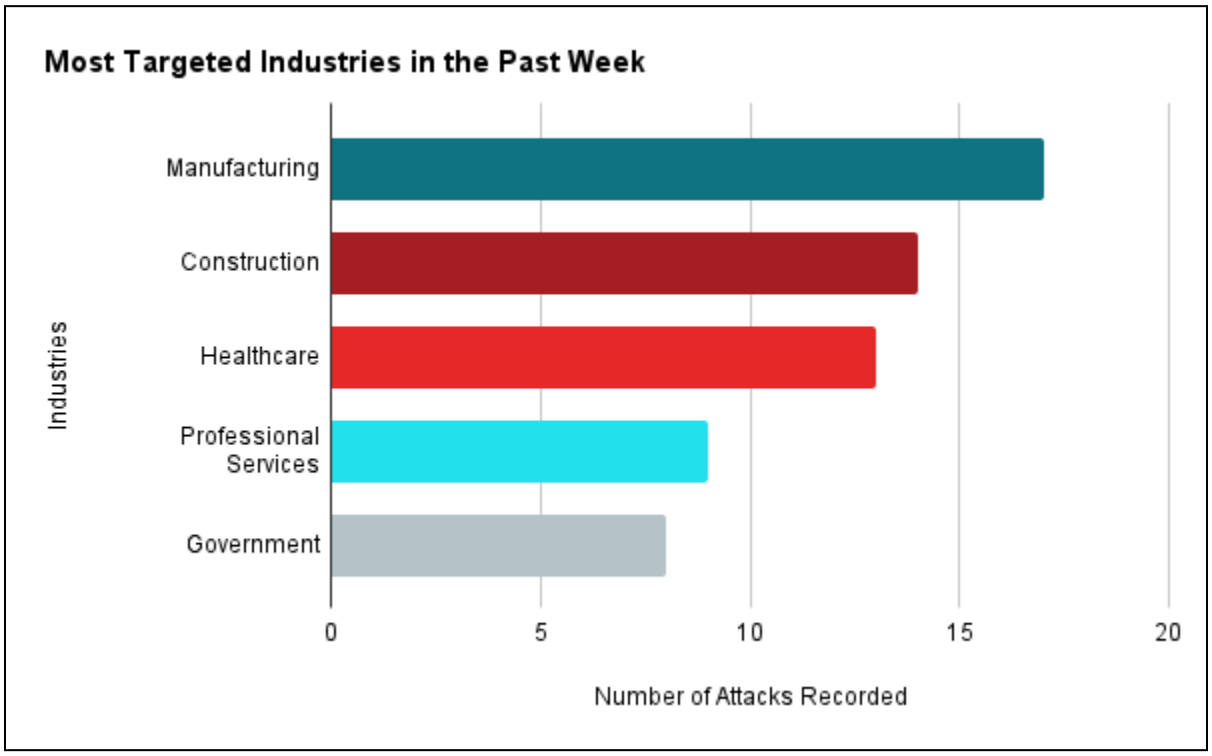
# Ransomware and Breach Intelligence Key Findings

## Ransomware Attacks and Trends in Focus



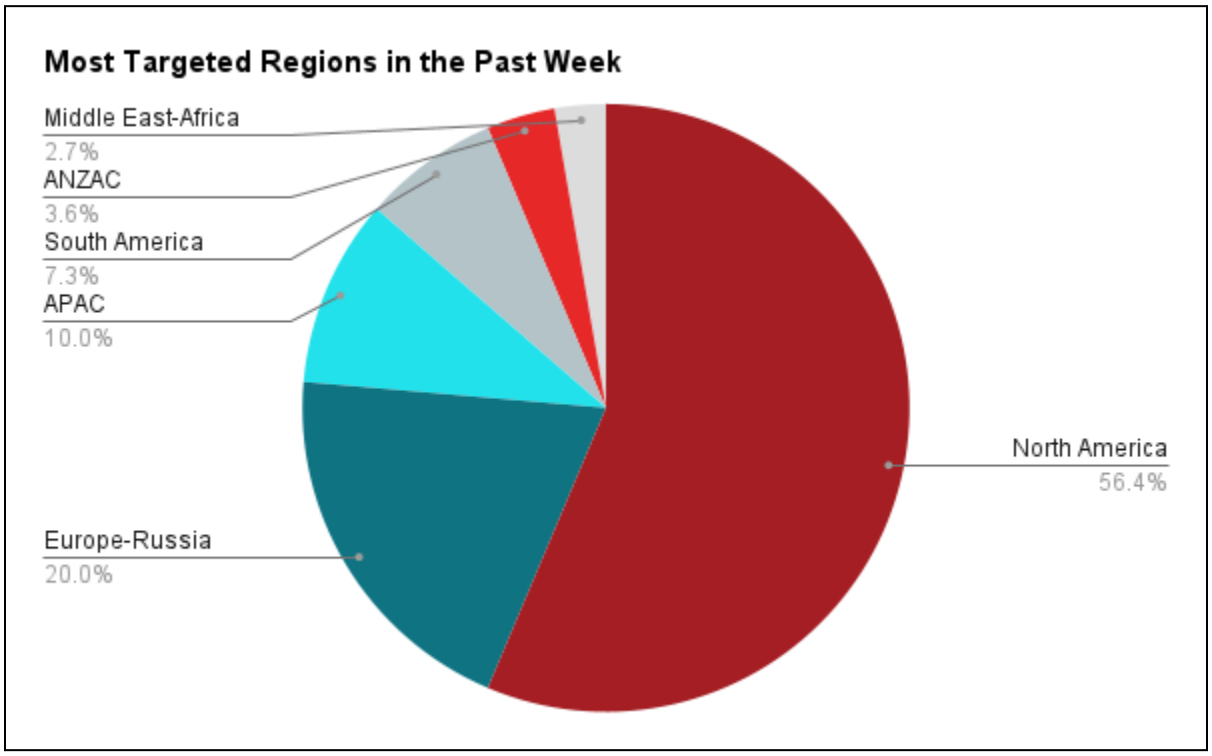

Source: ZeroFox Internal Collections

**Last week in ransomware:** In the past week, Qilin, SafePay, Global, Akira, and Play were the most active ransomware groups. ZeroFox observed at least 103 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks.




Source: ZeroFox Internal Collections

**Industry ransomware trend:** In the past week, ZeroFox observed that manufacturing, construction, healthcare, professional services, and government were the industries most targeted by ransomware attacks. The manufacturing industry was the top target, with 17 attacks identified.




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. North America saw 62 counts of ransomware attacks, while Europe-Russia accounted for 22, the Asia-Pacific (APAC) for 11, South America for eight, Australia and New Zealand (ANZAC) for four, and Middle East-Africa for three.

## Featuring Three Major Data Breaches

| Targeted Entity | Zoomcar | Email Hosting Provider cock[.]li | 16 Billion Login Package |
|---|---|---|---|
| Compromised Entities | 8.4 million users | 1 million user accounts | 16 billion users' credentials |
| Compromised Data Fields | Full name, phone number, car registration number, home address, and email address | Email addresses, timestamps, email signatures, comments, failed login attempts, vCards (electronic cards), and language preferences | Login credentials from social media, virtual private networks, developer forums, and user accounts |
| Suspected Threat Actor | N/A | N/A | N/A |
| Country/Region | India | Germany | Global |
| Industry | Transport | Technology | Technology |
| Possible Repercussions | Social engineering attempts, financial fraud, identity theft, and unauthorized access to online accounts | Identity theft, phishing, financial fraud, data resold in dark web forums, corporate espionage, and extortion | Phishing, financial fraud, supply chain attacks, and impersonation<br><br>**Note:** There is no evidence that this massive database resulted from a new breach nor that it contains new data; it is likely a compilation of data from previous breaches. |

**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% |