ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

July 18, 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 July 16, 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**
- Ceasefire Collapse Likely Temporary – SITREP #42: July 15, 2026 2
- ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 15 2

Cyber and Dark Web Intelligence Key Findings **4**
- Telegram Shortlink Domain t[.]me Restored 4
- World Leaks Publishes Blueprints and Supplier Data of Indian Nuclear Plant 4
- CISA Warns of Active Exploitation of SharePoint Vulnerabilities 5

Exploit and Vulnerability Intelligence Key Findings **7**
- CVE-2026-53412 7
- CVE-2026-50656 **9**

Ransomware and Breach Intelligence Key Findings **10**
- Ransomware Group, Industry, and Regional Trends 10
- Notable Data Breaches from the Week 13

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

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

© 2026 ZeroFox, Inc. All rights reserved.

This Week's ZeroFox Intelligence Reports

Ceasefire Collapse Likely Temporary – SITREP #42: July 15, 2026

The ceasefire between the United States and Iran has effectively collapsed, with both sides re-instating mutual blockades of the Strait of Hormuz (SoH) and resuming intense targeting mirroring that seen at the start of the war. The drop in oil prices to pre-war levels over the last month likely contributed to the resumption in Iranian hostilities. Deteriorating economic conditions are therefore likely to coerce the United States to return to negotiations, while further military damage to Iran is likely to do the same. Even with a return to negotiations and a halt in the airstrikes, broader uncertainty is very unlikely to end; the most likely scenario in the near term is a version of the ceasefire that breaks down periodically. An expansion of U.S. targeting to include Iranian civilian critical infrastructure, which was largely spared during the initial hostilities, is likely an indication that the U.S. calculus has shifted and the Trump administration is prepared for a more prolonged conflict. Iran is likely to leverage its ability to elevate economic costs, through both blockades of the SoH and attacks on Gulf assets as it did before. Maintaining leverage over the key Middle Eastern industries that utilize the SoH is almost certainly part of Iran's strategy to end the conflict on terms it finds acceptable.

ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 15

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

© 2026 ZeroFox, Inc. All rights reserved.

ZEROFOX

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

© 2026 ZeroFox, Inc. All rights reserved.

Cyber and Dark Web Intelligence Key Findings

Telegram Shortlink Domain t[.]me Restored

What we know:

- Telegram's shortened t[.]me domain has been restored following a day-long serverHold suspension on July 13, 2026.
- The outage blocked the one-click t[.]me links used to join public Telegram groups.

Background:

- Domain registrar DomainMe clarified that Telegram's shortened domain was put on hold due to U.S. sanctions on First VPN Service, which also included a t[.]me link to the provider's public Telegram group.
- First VPN Service is known to be used by cybercriminals in ransomware operations.

Analyst note:

- The domain registrar likely suspended the entire t[.]me domain instead of the single sanctioned URL, as failing to adhere to U.S. sanctions attracts heavy fines for domain registrars.

World Leaks Publishes Blueprints and Supplier Data of Indian Nuclear Plant

What we know:

- The World Leaks ransomware group has published approximately 858,000 files allegedly linked to Reliance Group, including around 19,000 files related to India's largest nuclear power plant in Kudankulam .

Background:

- The leaked data allegedly includes facility blueprints, control room layouts, supplier information, inspection records, equipment reviews, and insurance documents.
- Reliance Group, one of the plant's contractors, reportedly confirmed a "partial breach" involving a server hosted by data center provider Yotta.

© 2026 ZeroFox, Inc. All rights reserved.

- The leaked documents reportedly do not include information related to the nuclear reactors' core systems, which are supplied by Russia's state-owned nuclear corporation Rosatom.

Analyst note:

- The leaked documents are likely to provide intelligence on the plant's supporting infrastructure and contractors even if they exclude data on the nuclear reactors' core systems.
- Such information is likely to be of interest for cybercriminals and state-sponsored threat actors to conduct supply chain targeting and espionage and plan physical sabotage against the facility or suppliers.

CISA Warns of Active Exploitation of SharePoint Vulnerabilities

What we know:

- The Cybersecurity and Infrastructure Security Agency (CISA) has warned that threat actors are actively exploiting three SharePoint vulnerabilities (namely, CVE-2026-32201, CVE-2026-45659, and CVE-2026-56164) to gain unauthorized access to on-premises SharePoint Server instances.
- Additionally, CISA has also highlighted CVE-2026-55040 and CVE-2026-58644 as newly disclosed vulnerabilities that are not yet known to be exploited but should be patched promptly.

Background:

- The flaws reportedly involve remote code execution (RCE) and post-exploitation activities, including theft of Internet Information Services (IIS) machine keys, deserialization attacks, persistence, and malware deployment.

Analyst note:

- The exploitation of multiple SharePoint vulnerabilities indicates that internet-facing SharePoint servers are attractive targets for unauthorized access.
- Newly disclosed flaws CVE-2026-55040 and CVE-2026-58644 are also likely to attract threat actor interest in the near term.

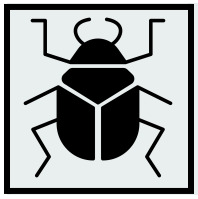
© 2026 ZeroFox, Inc. All rights reserved.

Exploit and Vulnerability Intelligence

© 2026 ZeroFox, Inc. All rights reserved.

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 nine new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on July 10, July 13, July 14, and July 15. Additionally, on July 14, 2026, CISA released four Industrial Control Systems (ICS) advisories. CVE-2026-56291 is an actively exploited unauthenticated arbitrary file upload vulnerability in the Balbooa Forms Joomla extension (versions prior to v2.4.1) that enables attackers to upload malicious Hypertext Preprocessor (PHP) files and achieve RCE. CVE-2026-48939 is a similarly exploited unauthenticated arbitrary file upload flaw in the iCagenda Joomla extension (versions prior to v4.0.8 and v3.9.15) enabling malicious PHP uploads and RCE. Progress Software issued an urgent warning regarding a "credible external security threat" targeting internet-facing on-premises ShareFile Storage Zone Controllers. Zimbra Collaboration Suite Classic Web Client versions prior to v10.1.19 reportedly contain a stored cross-site scripting vulnerability through which a specially crafted email executes malicious code upon opening, potentially exposing mailbox data, session tokens, and account settings; Zimbra has released a remedial security update.



CRITICAL

CVE-2026-53412

What happened: This is an account takeover vulnerability in Zoom Desktop Client and Meeting SDK for Windows. Zoom has released patches for the vulnerability.

- **What this means:** The flaw can reportedly enable an unauthenticated attacker to hijack user accounts through network access. Given Zoom's widespread enterprise adoption, this vulnerability presents a high-priority patching obligation, particularly for organizations handling sensitive communications.
- **Affected products:**
  - The affected products are listed here.

© 2026 ZeroFox, Inc. All rights reserved.

HIGH

CVE-2026-50656

What happened: The flaw is a race condition that could enable attackers to gain SYSTEM-level privileges and execute arbitrary code, even on fully patched Windows systems.

- **What this means:** A local attacker can leverage the flaw to spawn a shell with SYSTEM-level privileges and execute arbitrary code on the affected host.
- **Affected products:**
  - The affected products are listed in this advisory.

© 2026 ZeroFox, Inc. All rights reserved.

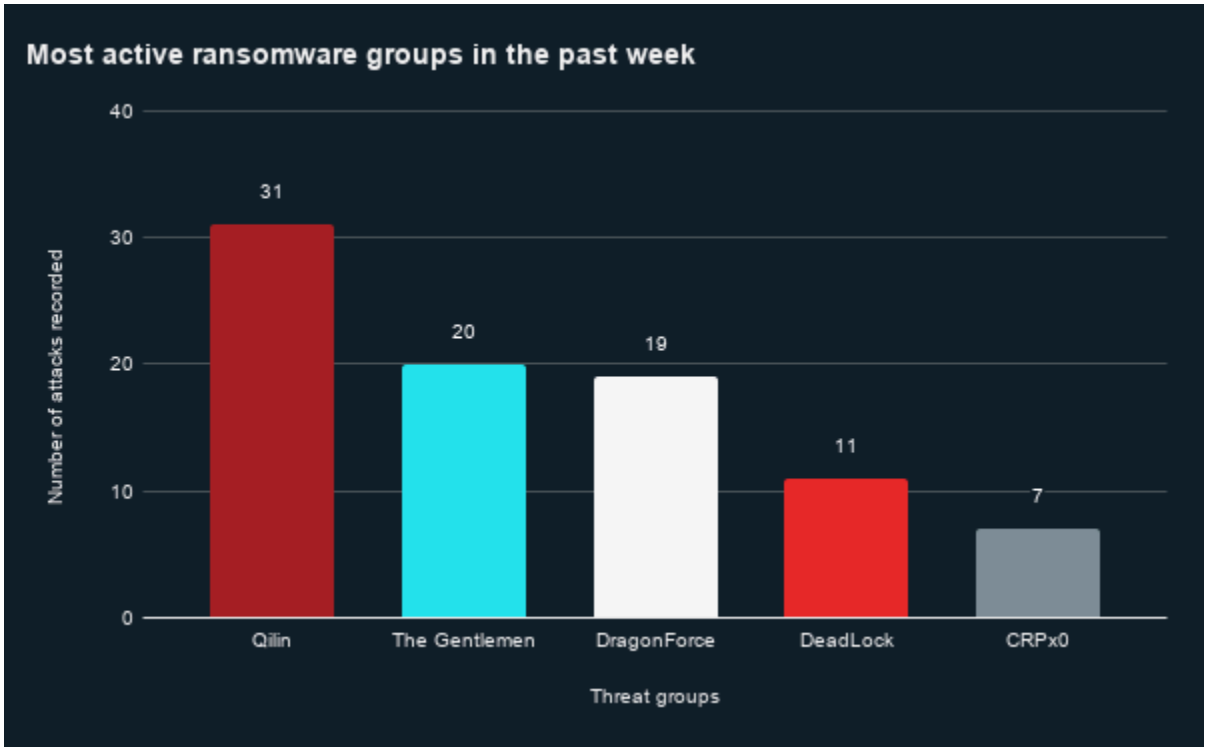
Ransomware and Breach Intelligence

© 2026 ZeroFox, Inc. All rights reserved.

Ransomware and Breach Intelligence Key Findings

Ransomware Group, Industry, and Regional Trends

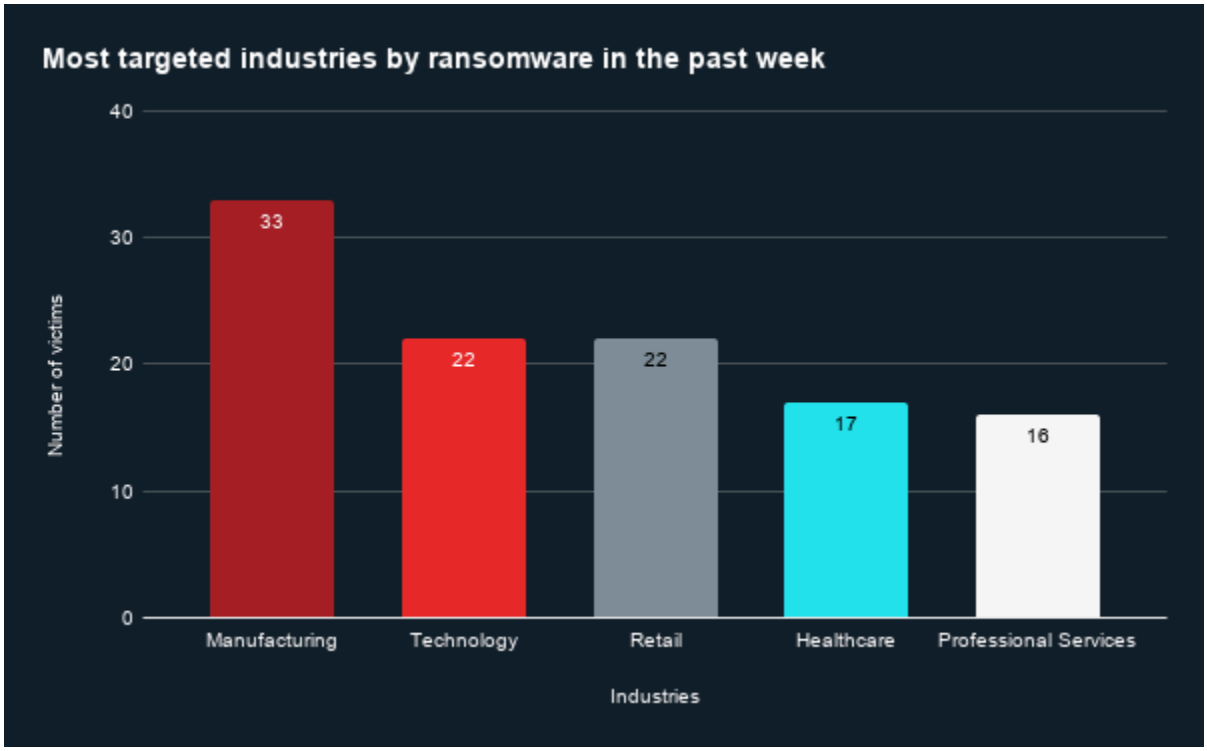
Last week in ransomware: In the past week, Qilin, The Gentlemen, DragonForce, DeadLock, and CRPx0 were the most active ransomware groups. ZeroFox observed close to 195 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by The Gentlemen.



Source: ZeroFox Internal Collections

© 2026 ZeroFox, Inc. All rights reserved.

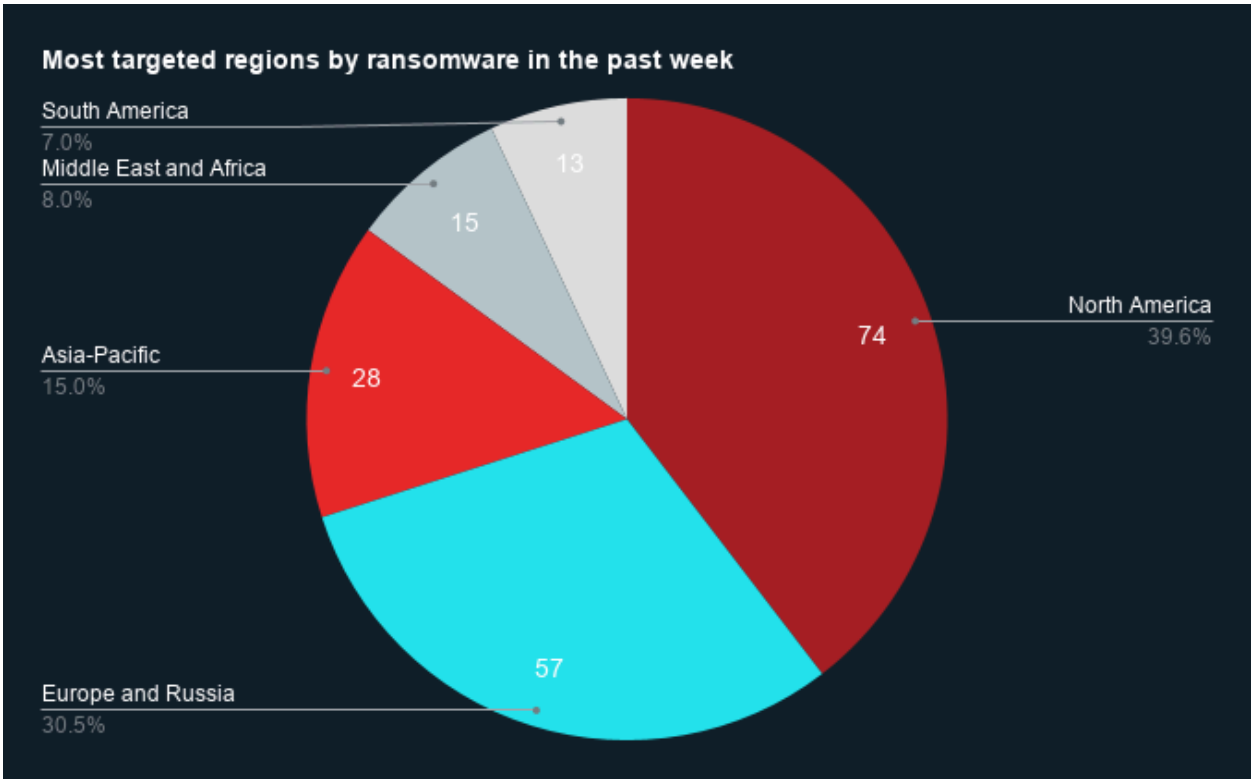
Industry ransomware trends: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by technology.



Source: ZeroFox Internal Collections

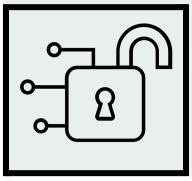
© 2026 ZeroFox, Inc. All rights reserved.

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 74 ransomware attacks observed in North America , while Europe and Russia accounted for 57, Asia-Pacific for 28, Middle East and Africa for 15, and South America for 13.



Source: ZeroFox Internal Collections

© 2026 ZeroFox, Inc. All rights reserved.



Notable Data Breaches from the Week

Targeted Entity	Lidl	AssuranceAmerica	Partnered Health
Compromised Entities/Victims	Lidl online shop customers in Germany, Belgium, and the Netherlands	6,998,886 individuals	Patients across at least 16 Partnered Health family medical clinics in Australia
Compromised Data Fields	First and last names, phone numbers, email addresses, dates of birth, and customer numbers	Names, contact information, automobile insurance policy and account information, driver and vehicle information, claims-related information, and driver's licence numbers	Personally identifiable information (PII) and protected health information (PHI)
Suspected Threat Actor	N/A	N/A	N/A
Country/Region	Europe	United States	Australia
Industry	Retail	Insurance	Healthcare
Possible Repercussions	Phishing and identity fraud	Insurance fraud. Exposed individuals are likely to be targeted in social engineering attacks with threat actors impersonating AssuranceAmerica employees	Medical fraud targeting exposed patients, social engineering, phishing, and identity theft using PII and PHI

Three major breaches observed in the past week

© 2026 ZeroFox, Inc. All rights reserved.

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.

© 2026 ZeroFox, Inc. All rights reserved.

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%

© 2026 ZeroFox, Inc. All rights reserved.