



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

June 24, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the cyber threat landscape. 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 12:00 PM (EDT) on June 21, 2024**; 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 – New Malicious Tool Advertises Comprehensive Personal Information	2
 Cyber Intelligence Key Findings	4
Ukraine Dismantles Pro-Russia Spyware Operation amid Rising Cybersecurity Threats	4
Barriers to Single Sign-On (SSO) Adoption for Small and Medium-Sized Businesses	4
IntelBroker Leaks Database Allegedly Belonging to AMD	5
 Deep and Dark Web Intelligence Key Findings	7
Threat Actor Group Targets Canadian Telecommunications Sector	7
Owners of USD 430 Million "Empire Market" Charged	7
 Exploit and Vulnerability Intelligence Key Findings	9
CVE-2024-34102	9
CVE-2024-37079 & CVE-2024-37080	10
 Ransomware and Breach Intelligence Key Findings	12
Ransomware Intelligence: Linux Version of RansomHub Ransomware Targets VMware ESXi VMs	12
Breach Intelligence: Healthcare Facilities Targeted	12
 Physical and Geopolitical Intelligence Key Findings	15
Physical Security Intelligence: Global	15
Physical Security Intelligence: United States	16
 Appendix A: Traffic Light Protocol for Information Dissemination	17
 Appendix B: ZeroFox Intelligence Probability Scale	18

| This Week's ZeroFox Intelligence Reports

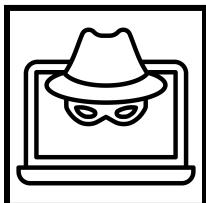
ZeroFox Intelligence Flash Report – New Malicious Tool Advertises Comprehensive Personal Information

On June 16, 2024, a positive-reputation actor known as “spam_assistant” announced a new tool called Data Fusion in the dark web forum Exploit. According to the advertisement, Data Fusion is capable of providing buyers with a significant amount of both personally identifiable information (PII) pertaining to individuals and organizational tax data. Unlike similar deep and dark web (DDW) services offering the sale of PII, Data Fusion is allegedly capable of creating bespoke background reports that summarize the requested data. PII such as that advertised by spam_assistant is an integral aspect of many forms of cyberattack. Personal details are used to inform and enhance sophisticated social engineering attacks, such as spear phishing and business email compromise, or to enable fraudulent activity like identity theft and tax-related scams. Given the high and continuous demand for sensitive data such as PII, threat actors are almost certain to continue pursuing innovative, automated tools able to draw from an increasingly expansive repository of both publicly available information and illicit data leaks.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

[Ukraine Dismantles Pro-Russia Spyware Operation amid Rising Cybersecurity Threats](#)



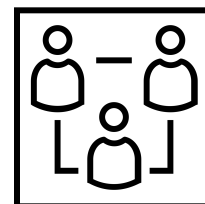
What happened: The Security Service of Ukraine (SSU) dismantled infrastructure used by two pro-Russia Ukrainian residents to hack soldiers' devices and deploy spyware. Ukrainian authorities discovered thousands of mobile numbers and Telegram accounts under the control of SIM farm-like infrastructure that were abused by Russian intelligence services. One of the pro-Russia residents targeted Ukrainian soldiers with phishing SMS messages that contained spyware links, leading to compromised data and communications. The second individual managed a similar operation, running 15,000 social media accounts and selling access on dark web forums, primarily to Russian intelligence.

- **What this means:** Spyware installation on soldiers' devices is likely to compromise data and battlefield communications, posing significant security risks. Moreover, this operation's use of it to spread pro-Kremlin propaganda shows the multifaceted cyber warfare strategies employed by Russia amid the ongoing Russia-Ukraine war. Such incidents are likely to inspire other state-sponsored actors to exploit technology and social media to gather intelligence or spread misinformation that can influence their targets. Additionally, the campaign involved cryptocurrency payments and sophisticated software, indicating a high level of organization and funding. To contain excesses amid the Russia-Ukraine cyberwarfare, prosecutors at the International Criminal Court are reportedly [investigating](#) alleged Russian attacks on Ukrainian civilian infrastructure and their potential classification as war crimes. Some of these cyberattacks—such as those disrupting power, water, emergency services, and air raid warnings in Ukraine—have endangered lives.

[Barriers to Single Sign-On \(SSO\) Adoption for Small and Medium-Sized Businesses](#)

What happened: CISA released a report to help small and medium businesses deal with the challenges of single-sign-on (SSO) adoption. The report also summarizes views of vendors and customers and provides a set of recommendations for encouraging SSO adoption.

- **What this means:** SSO is a user authentication and access control system that allows users to access multiple applications, tools, and systems with just one set of credentials. By centralizing the authentication process, SSO streamlines identity management and simplifies the user experience by only needing to remember one



username and password for all accounts. Furthermore, SSO can reduce password duplication across various platforms, consequently reducing the potential for password leakage.

IntelBroker Leaks Database Allegedly Belonging to AMD

What happened: On June 18, ZeroFox Intelligence observed “IntelBroker” leaking a database allegedly associated with Advanced Micro Devices (AMD), a well-known U.S.-based semiconductor manufacturing company, on BreachForums. The actor claims the compromised data includes future AMD products, spec sheets, employee databases, customer databases, property files, ROMs, source code, firmware, and finances. AMD is currently [investigating](#) these claims.

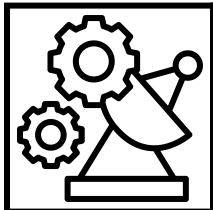


➤ **What this means:** The semiconductor industry is a lucrative target for notorious cyber threat actors due to an increasing demand for semiconductor chips from multiple industries. It faces heightened cyberattack risks due to its valuable intellectual property, intensified by geopolitical tensions and restrictions on advanced chipmaking technology. The leaked database (which allegedly contains information on AMD’s future products) highlights this threat, as it is likely to attract actors sponsored by states looking to lessen their dependence on other countries for their semiconductor needs.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Threat Actor Group Targets Canadian Telecommunications Sector

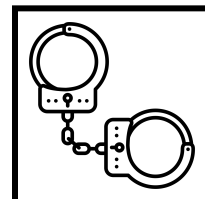


What happened: On June 13, 2024, threat actor group “UserSec” announced a campaign targeting the Canadian telecommunications provider Telus Communications. The distributed-denial-of-service (DDoS) attack was announced on the group’s Telegram channel. UserSec claimed the “large scale” attack was initiated in cooperation with threat actors “NoName(057)16” and “CyberArmy of Russia.”

- **What this means:** UserSec is a pro-Russian hacktivist group that was first observed on Christmas Day 2023 when it carried out a DDoS attack against multiple Swedish airports. The group has conducted around one dozen attacks focused exclusively on North Atlantic Treaty Organization (NATO) nations, including multiple attacks against U.S.-based targets. UserSec, NoName(057)16, and CyberArmy of Russia frequently target infrastructure, such as telecommunications companies, to maximize the impact of their strikes.

Owners of USD 430 Million “Empire Market” Charged

What happened: The U.S. District Court in Chicago has charged two alleged administrators of Empire Market, a prominent dark -web marketplace, for their role in operating the illicit platform. They allegedly facilitated over four million transactions totaling more than USD 430 million, via which vendors sold drugs, malware, stolen credentials, counterfeit goods, and more. The market operated with categories like “Drugs,” “Fraud,” “Counterfeit Items,” and “Software and Malware,” with detailed sub-categories for specific illicit products. Buyers could rate vendors based on various criteria, including “stealth”, and the administrators also employed moderators to handle disputes.



- **What this means:** This indictment is the latest in a recent wave of infrastructure disruptions and judicial action taken against dark web threat actors by law enforcement operations across the globe. The two administrators were indicted on grounds of drug trafficking, computer fraud, access device fraud, counterfeiting, and money laundering. The arrest of Empire Market’s administrators is significant as it disrupts a major hub for illegal activities on the dark web, impacting the sale and distribution of illicit goods worldwide. The closure of Empire Market not only affects buyers and sellers directly involved in illegal transactions but also sends a message about the risks associated with participating in underground economies.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in software solutions, networking, and government security domains. CISA released four Industrial Control Systems (ICS) advisories this week, highlighting vulnerabilities in YokogawaCARELWestermo and RAD Data Communications products. CVE-2024-5650 (CVSS base score: 8.5) in vulnerable versions of Yokogawa CENTUM could [allow](#) an attacker to execute arbitrary programs. CVE-2023-3643 (CVSS score: 9.8) in Boss-Mini's version 1.4.0 (Build 6221) could [allow](#) an attacker to manipulate an argument path, which would lead to information disclosure. CVE-2024-37183 (CVSS score: 5.7) [affects](#) version 4.21.0 of L210-F2G Lynx and could crash the device being accessed or may allow remote code execution if exploited. RAD Data Communications' SecFlow-2 is [infected](#) with CVE-2019-6268 (CVSS score: 7.5), which lets an attacker obtain files from the operating system by crafting a special request. A new vulnerability (CVE-2024-0762) in Phoenix SecureCore UEFI firmware [affects](#) devices with various Intel CPUs. A critical vulnerability [dubbed](#) "CosmicSting" affecting Adobe Commerce and Magento websites, CVE-2024-34102 (CVSS score: 9.8), remains largely unpatched after a security update was released, leaving millions of sites vulnerable to attacks. Threat actors have been [observed](#) exploiting this SolarWinds Serv-U path-traversal vulnerability, using publicly available proof-of-concept (PoC) exploits.

Notable vulnerabilities:

CVE-2024-34102



What happened: Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8, and earlier are affected by an Improper Restriction of XML External Entity Reference ("XXE") vulnerability that could result in arbitrary code execution.

➤ **What this means:** An attacker could exploit this vulnerability by sending a crafted XML document that references external entities. Exploitation of this issue does not require user interaction. This **CRITICAL**-severity vulnerability has been assigned a 9.8 CVSS score.

➤ **Affected products:**

- Adobe Commerce version 2.4.7
- Adobe Commerce version 2.4.6-p5
- Adobe Commerce version 2.4.5-p7
- Adobe Commerce version 2.4.4-p8 and earlier

CVE-2024-37079 & CVE-2024-37080

What happened: CVE-2024-37079 and CVE-2024-37080 are **CRITICAL** (CVSS score: 9.8) heap-overflow vulnerabilities in vCenter Server's DCERPC protocol that allow remote code execution via crafted packets. VMware has released the details of the patches in an [advisory](#) issued on June 18.

- **What this means:** Security updates are available for VMware vCenter Server 8.0 U2d, 8.0 U1e, and 7.0 U3r, and patches have been released for Cloud Foundation.
- **Affected products:**
 - VMware vCenter Server version 7.0
 - VMware vCenter Server version 8.0
 - VMware Cloud Foundation version 4.x
 - VMware Cloud Foundation version 5.x.

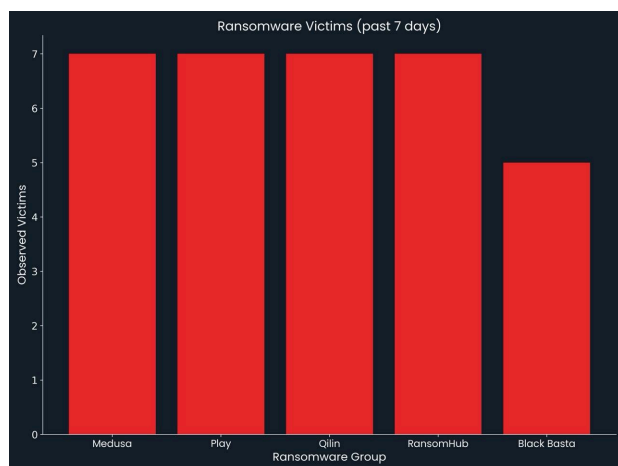


Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: Linux Version of RansomHub

Ransomware Targets VMware ESXi VMs



Source: ZeroFox Internal Collections

What happened: In the past week, ZeroFox has observed over 85 ransomware attacks conducted by Medusa, Play, Qilin Eldorado, and RansomHub ransomware groups; over 55 percent of these targeted the manufacturing sector in North America and Europe. In other news, RansomHub ransomware group has expanded its operations by developing a specialized Linux encryptor specifically designed to target VMware ESXi environments used in corporate settings. The threat group also has a new ESXi variant, which has been

observed since April 2024 and marks a strategic shift from its previously Go-based encryptors for Windows and Linux to a C++ program derived from the now-defunct Knight ransomware. ZeroFox has [identified](#) what appears to be a work-in-progress leak site in the DDW for a new ransomware group called "Locker Leaks."

- **What this means:** RansomHub's development of a specialized VMware ESXi encryptor signifies a targeted escalation in ransomware tactics against enterprises heavily reliant on virtualized environments. This variant poses a significant threat as it can encrypt entire VMware ESXi infrastructures, potentially paralyzing critical IT systems and services. The encryptor's advanced features (such as command-line options for customization and exclusion settings) enhance its effectiveness in tailored attacks, enabling the threat group to demand substantial ransom payments for decryption keys and severely impacting business continuity and security posture.

Breach Intelligence: Healthcare Facilities Targeted

What happened: Consulting Radiologists, a Minnesota-based healthcare provider, [suffered](#) a cyberattack in February that compromised the personal and medical information of over 500,000 patients. Meanwhile, the Los Angeles County Department of Public Health [experienced](#) a phishing attack between February 19 and 20, 2024, wherein a hacker obtained login credentials from 53 employees. This breach



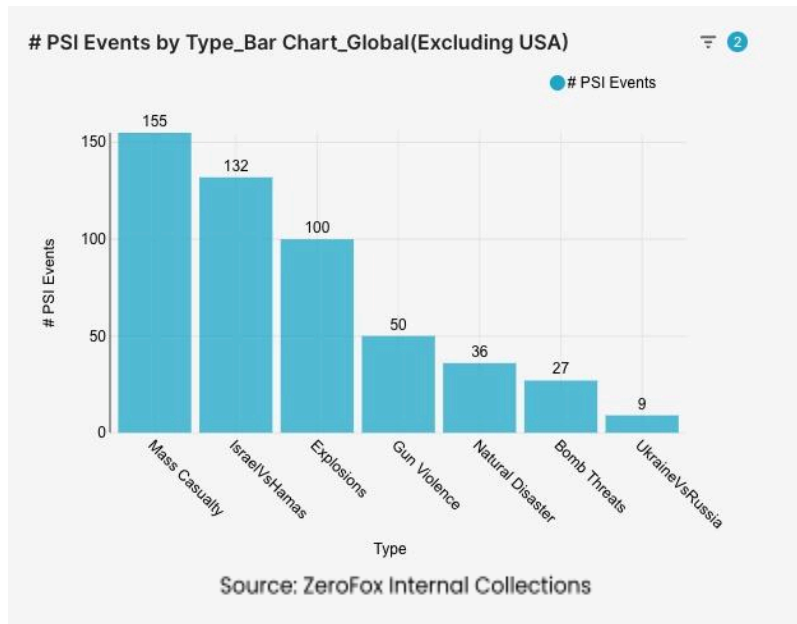
potentially exposed the PII of over 200,000 individuals, including clients and employees. Both organizations have notified affected individuals, with Consulting Radiologists stating there is currently no evidence of misuse of the disclosed information. Among notable incidents from other industries this week, AMD (Advanced Micro Devices) is now [investigating](#) claims of data breach. As mentioned earlier in this report, ZeroFox Intelligence [observed](#) IntelBroker claiming responsibility for the breach.

- **What this means:** The Consulting Radiologists breach is critical due to the vast amount and sensitivity of the data compromised, which includes names, addresses, dates of birth, Social Security numbers, health insurance information, and medical records. This data can lead to identity theft, fraud, misuse of medical services, financial scams, and sophisticated phishing attacks targeting affected individuals or related healthcare providers. Similarly, the incident at the Los Angeles County Department of Public Health poses significant risks of identity theft and fraud. The department's immediate response, including disabling compromised accounts and launching an investigation, is likely to mitigate the breach's effects. However, the U.S. healthcare industry continues to be a frequent target of ransomware attacks and data breaches. The implications of such attacks include extortion, targeted financial scams, and, more importantly, disruption to emergency services. Meanwhile, the supposed AMD leak is significant because of the cyberthreats looming over the semiconductor industry, intensified by geopolitical tensions and restrictions on advanced chipmaking technology. The leaked database with alleged information on AMD's future products highlights this threat, as the database is likely to attract actors sponsored by states looking to reduce their dependence on other countries for their semiconductor needs.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

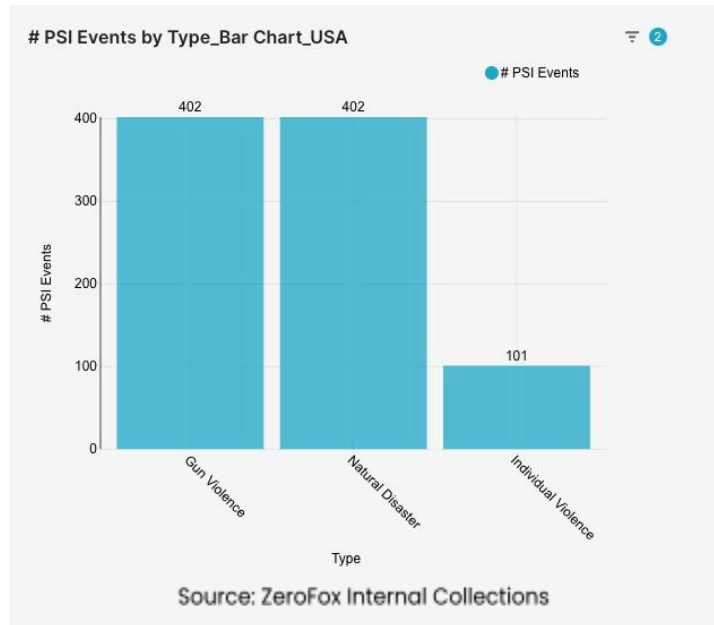


What happened: Excluding the United States, there was a 2 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, India, and Lebanon; approximately 65 percent of these events were explosions. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 26 percent from the previous week. Additionally, events related to Russia's war in

Ukraine decreased by 10 percent. The top three most-alerted subtypes were explosions, which saw a 20 percent decrease from the previous week; gun violence, which decreased by 4 percent; and natural disasters, which decreased by 25 percent. Notably, bomb threats saw an increase of 170 percent.

- **What this means:** The drastic percentage increase in bomb threats, as well as India having the second-highest mass casualty alert type this week, are both due to hoax bomb threats in the country over the past few days; over 50 [hospitals](#) and 41 [airports](#) received threatening emails claiming that explosive devices had been planted at the various locations, although nothing was found upon investigation. An online group called "KNR" is suspected to be behind these emails, as the group reportedly issued similar threats to several schools in the Delhi region in May. This week also saw the dissolution of the Israeli war [cabinet](#) by President Netanyahu, which may explain the decrease in alerts with the "IsraelVsHamas" tag as the leader attempts to regroup; the war cabinet will supposedly be replaced by a reduced "kitchen cabinet" that will conduct sensitive discussions and consultations. Additionally, as Lebanon was also one of the top contributors to mass casualty events this week, it is important to note that [Hezbollah](#) leader Hassan Nasrallah has declared the group as being ready for a war with "no restraint and no rules and no ceilings" in the event of a major attack by Israeli forces.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were gun violence, natural disaster, and individual violence. Gun violence alerts are instances in which there is a confirmed or likely confirmed victim, and individual violence typically involves stabbings. The top two states that had the most gun violence alerts were Illinois and California, which together made up one-third of this week's nationwide total (32 percent). Gun violence across the United States overall decreased by 5 percent from the week prior. The top two contributors to natural disaster alerts this week

were California and New York, and natural disaster alerts across the country increased by 15 percent. The top contributing states to individual violence were New York and California.

- **What this means:** While gun violence and natural disasters remained the top two alerted subtypes, individual violence took third place, which is used when alerting stabbings. For instance, a mass-stabbing occurred in [Indianapolis, IN](#), this week in which nine people were injured as a result of a disturbance between two groups. Gun violence instances across the country saw a small decrease overall, but several of the events were very lethal, including mass shootings in [Rochester Hills, MI](#); [Round Rock, TX](#); [Philadelphia, PA](#); and two in [Chicago, IL](#); all of the listed instances combined resulted in 44 people shot. California has continued to be affected by [wildfires](#), as this week saw structural damage and evacuations in the northern part of the state due to rapidly-spreading new fires. Similarly, New Mexico's South Fork Fire, which was first reported Monday morning in Ruidoso, has now burned more than 15,000 acres and is zero percent contained, causing Governor Michelle Lujan Grisham to [declare](#) a state of emergency.

Interested in more ZeroFox Threat Intelligence? ZeroFox produces timely, relevant, and actionable [intelligence reporting](#) regularly to keep your team informed on developments in the threat landscape.

| 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%