



Weekly Intelligence Brief

Classification: TLP:GREEN

February 5, 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 (EST) on February 2, 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 - Introducing Wing, New Ransomware-as-a-Service	2
ZeroFox Intelligence Flash Report - LockBit Denies Attack Against Russian Entity	2
ZeroFox Intelligence Flash Report - Political Asylum Service to Assist Russians Fleeing to France	2
ZeroFox Intelligence February 2024 Geopolitical Brief	2
ZeroFox Intelligence Brief - Underground Economist: Volume 4, Issue 3	2
 Cyber Intelligence Key Findings	4
Scammers Use Couriers to Retrieve Cash and Precious Metals from Victims of Scams	4
"Secure by Design" Alert Urges Manufacturers to Eliminate Defects in SOHO Routers	4
Energy Giant Schneider Electric Hit by Cactus Ransomware Attack	4
 Deep and Dark Web Intelligence Key Findings	7
Former Killnet Members Claim to Announce New Killnet 2.0 Group	7
Actor "baggins.bilbo" Selling Cisco VPN Access Bundle to 75 Companies Worldwide	7
Threat Actor "DrakenSnow" Selling One-Day Windows 10-11 LPE Exploit	8
 Exploit and Vulnerability Intelligence Key Findings	10
CVE-2022-40700	10
CVE-2024-21893	10
 Ransomware and Breach Intelligence Key Findings	12
LockBit and xss Continue to Dominate the Darknet	12
Breach Disclosure: Adobe	12
 Physical and Geopolitical Intelligence Key Findings	14
Physical Security Intelligence: Global	14
Physical Security Intelligence: United States	14
 Appendix A: Traffic Light Protocol for Information Dissemination	15
 Appendix B: ZeroFox Intelligence Probability Scale	16

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Flash Report - Introducing Wing, New Ransomware-as-a-Service](#)

In this flash report, ZeroFox researchers report on the announcement of a new Ransomware-as-a-Service (RaaS) operation known as Wing on the predominantly Russian-speaking dark web forum RAMP; it is the first RaaS launched on the forum in 2024.

[ZeroFox Intelligence Flash Report - LockBit Denies Attack Against Russian Entity](#)

In this flash report, ZeroFox researchers report on allegations of a successful attack against a Russia-based organization using the LockBit malware strain, which LockBit has subsequently denied.

[ZeroFox Intelligence Flash Report – Political Asylum Service to Assist Russians Fleeing to France](#)

In this flash report, ZeroFox researchers report on a “political asylum” service claiming to assist Russians with fleeing to France that has been gaining traction on the Russian-language deep web community WWH-Club.

[ZeroFox Intelligence February 2024 Geopolitical Brief](#)

In this monthly brief, ZeroFox researchers discuss how farmer protests in Europe are spreading and are likely to remain politically relevant until at least the June 2024 European Union (EU)-wide elections. In the Middle East, a U.S. military response against Iranian interests is highly likely, while a ceasefire between Israel and Hamas appears probable. There are a number of notable elections in February, with the biggest in Indonesia likely to go to a run-off, while the prospect of social unrest related to the Pakistani elections is extremely high. Two new measures should concern financial services firms with operations in China: a corruption crackdown on the finance sector and a new national security law in Hong Kong with an emphasis on dissent and foreign influence.

[ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 3](#)

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

| Cyber Intelligence |

| Cyber Intelligence Key Findings

Scammers Use Couriers to Retrieve Cash and Precious Metals from Victims of Scams

What happened: The Federal Bureau of Investigation (FBI) released an advisory that warns the public about scams in which criminals pose as tech support or U.S. government officials. These scammers employ various tactics, such as claiming financial accounts are hacked or at risk, convincing the victims to liquidate assets into cash or to buy precious metals for protection. The scammers may use passcodes for authentication and to assure victims that their assets will be safeguarded in a protected account.



- **What this means:** The warning advises the public to verify the legitimacy of such communications to prevent falling victim to these scams. The FBI stated that the U.S. government and legitimate businesses will never instruct people to liquidate cash assets into gold or other precious metals. Victims should report such fraudulent or suspicious activities to the FBI at www.ic3.gov, mentioning details of the contact person/company and communication medium.

“Secure by Design” Alert Urges Manufacturers to Eliminate Defects in SOHO Routers

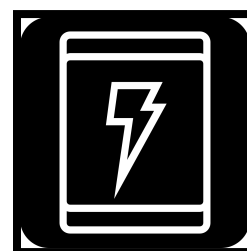


What happened: The U.S. CISA and the FBI have published guidelines on security design improvements for small office/home office (SOHO) device manufacturers. The advisory focuses on eliminating exploitable defects during the product design and development phases in web management interfaces, as well as implementing secure default device configurations.

- **What this means:** This is the third publication of the new “Secure by Design” (SbD) series of alerts. This warning was published amid ongoing attacks on SOHO routers by the China-sponsored Volt Typhoon group.

Energy Giant Schneider Electric Hit by Cactus Ransomware Attack

What happened: Schneider Electric’s Sustainability Business division reportedly suffered a ransomware attack by the Cactus hacker group. The ransomware group gained access, stole terabytes of data, and is now



extorting the company by threatening to leak the stolen data if a ransom demand is not paid.

- **What this means:** The attack also disrupted some of Schneider Electric's Resource Advisor cloud platform, which continues to suffer outages. The company says that it is actively engaged in remediation efforts to restore its business platforms to a secure environment.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Former Killnet Members Claim to Announce New Killnet 2.0 Group



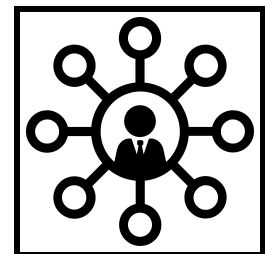
What happened: On January 28, 2024, new Telegram group “Killnet 2.0” emerged and claimed to have added several other hacktivist groups to their evolving collective, including Anonymous Russia (an original Killnet collective member), 62IX Group, and Pharanos Cyber Group. Previously, on January 26, 2024, members of the hacktivist group Писарь из Штаба (Clerk from Headquarters) claimed to have questioned their subscribers about whether or not a Killnet 2.0 community should be created. This request came after

Killmilk, head of the KillNet group, claimed to have retired from KillNet and joined Anonymous Russia.

- **What this means:** The Telegram post states that “KILLNET 2.0 is now an international decentralized hacktivist group” and “KILLNET2.0 is not only Russian hackers, it is Hackers on the side of Good from all over the World.” Previously, the original Killnet group was recognized as a pro-Russian hacktivist group that targeted entities in the United States and Europe, including government organizations. The recent changes in Killnet’s organizational structure and the formation of Killnet 2.0 may be due to ideological differences or rebranding for other strategic reasons. The emergence of Killnet 2.0, which includes Anonymous Russia, 62IX Group, and Pharanos Cyber Group, indicates that sharing resources and expertise may have been one of the group’s goals. This might potentially result in enhanced offensive cyber capabilities, particularly in the form of DoS and DDoS attacks. Additionally, the original Telegram post stated that “KILLNET2.0 is not only Russian hackers, it is Hackers on the side of Good from all over the World.” This indicates that Killnet 2.0 might have other goals and veer away from the original Killnet’s main targets.

Actor “baggins.bilbo” Selling Cisco VPN Access Bundle to 75 Companies Worldwide

What happened: On January 27, 2024, user “baggins.bilbo” advertised an auction for a Cisco VPN access bundle to 75 separate worldwide companies on predominantly Russian-language dark web forum Exploit. According to baggins.bilbo, the access bundle is provided with ip:port:login:password data. The starting bid for the access bundle was USD 400 USD, with a minimum bid of USD 50 USD and an instant purchase price of USD 800.



- **What this means:** At least two actors appear to be interested in this bundle. The bundle gives an actor and potentially larger group access to conduct attacks on a number of companies. An actor working with a ransomware group could purchase the bundle, which is likely to cause an uptick in ransomware attacks for that variant. The price of the bundle is minimal compared with the ransom an actor or ransomware group could charge a victim to stop an attack or recover data.

Threat Actor “DrakenSnow” Selling One-Day Windows 10–11 LPE Exploit



What happened: On January 28, 2024, untested threat actor “DrakenSnow” advertised a one-day Windows 10–11 Local Privileges Elevation (LPE) exploit for sale on the predominantly Russian-language dark web forum Exploit. According to the actor, the exploit is able to elevate privileges on operating systems, including Microsoft Windows 10 with all system patches installed and Microsoft Windows 11 with January system patches installed. The actor is

charging USD 5,000 for the exploit.

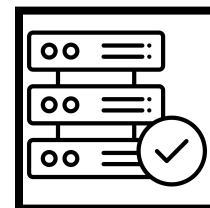
- **What this means:** This exploit sale comes after DrakenSnow advertised the sale of two zero-day vulnerabilities affecting SonicWall VPNs and Microsoft Windows and a one-day vulnerability affecting an undisclosed JetBrains product on January 7, 2024. While the validity of these recently-advertised exploits cannot be independently verified by ZeroFox, sales of this kind typically do not have much credibility. However, ZeroFox has observed their increasing prevalence on DDW (deep and dark web) forums throughout 2023 and into 2024. ZeroFox will continue to monitor for such posts, as legitimate sales can give less sophisticated cybercriminals the ability to infiltrate target systems that they normally would not be able to access.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

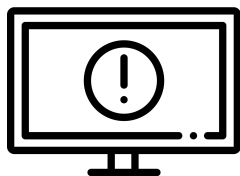
[CVE-2022-40700](#)

What happened: A Server Side Request Forgery (SSRF) vulnerability in WordPress Wpopal Core Features Plugin could allow a malicious actor to cause a website to execute website requests to an arbitrary domain controlled by the attacker. This **CRITICAL** vulnerability has a CVSS base score of 9.8.



- **What this means:** The bug could allow a malicious actor to find sensitive information of other services running on the system. No fix for this vulnerability has been issued yet.

[CVE-2024-21893](#)



What happened: An SSRF vulnerability (of **HIGH** severity) in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x), and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication.

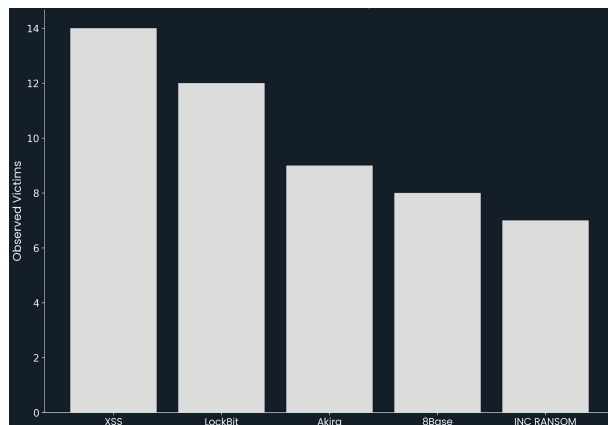
- **What this means:** Ivanti has disclosed that this **ZERO-DAY** vulnerability is being actively exploited to target some of its customers. The company has released patches for some affected systems and recommended mitigation measures for systems awaiting patches.

Ransomware and Breach Intelligence

| Ransomware and Breach Intelligence Key Findings

LockBit and xss Continue to Dominate the Darknet

What happened: Underground forum xss continues to feature the highest number of relevant posts tracked by ZeroFox, with companies across the world (the United States, United Kingdom, Russia, France, Brazil, India, and others) accounting for the targets. LockBit remains the most prolific ransomware group this week. The most prominent incident involving LockBit was its denial of an alleged successful attack against a Russia-based organization using the LockBit malware strain.



Source: ZeroFox Internal Collections

- **What this means:** As mentioned in the corresponding [ZeroFox Flash Report](#), an attack against a Russia-based organization would violate the unwritten rules about using the LockBit strain to attack entities in Russia and other Commonwealth of Independent States (CIS) countries. The negative community response to this event is almost certainly indicative of the extremely low tolerance within dark web forums for attacks against victims based in the CIS. However, the threat posed by LockBit, Clap, or the wider ransomware and digital extortion (R&DE) threat landscape to Western organizations is almost certainly unchanged.

Breach Disclosure: Adobe



What happened: An alleged data breach at Adobe exposed 152,430,379 records (email addresses and hashed passwords), which were subsequently shared on a deep web platform.

- **What this means:** Aside from email addresses, other notable data fields observed in this package include full names, IP addresses, phone numbers, physical addresses, dates of birth, browser user agents, social media profiles, gender, and user activity. The threat actor did not disclose the ultimate source of the data breach or how it was exploited.

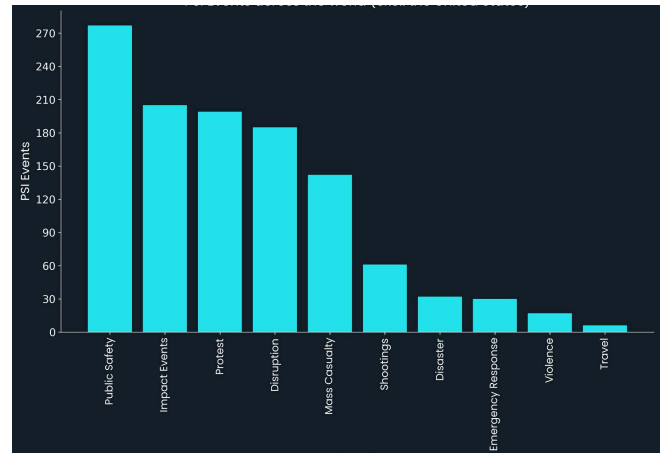
| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

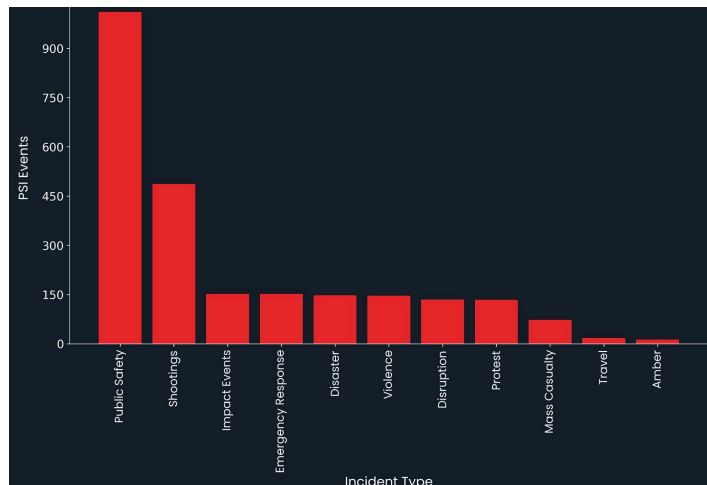
What happened: ZeroFox observed close to 300 instances of protest activity in the past week worldwide (excluding those in the United States, which have been analyzed separately below), with Europe being a major contributor to this number. Alerts relating to public safety events remained close to 300, which is similar to numbers seen last week.

- **What this means:** Farmers in Europe are increasing the intensity of their protests against rising costs and taxes and demanding reduced bureaucracy amid a significant EU summit in Brussels. Meanwhile, Germany is witnessing large turnouts in protests against controversial anti-immigrant statements attributed to the far-right party, AfD.



Source: ZeroFox Internal Collections

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: ZeroFox Intelligence observed that California, Illinois, and New York accounted for the greatest number of public safety events, shooting instances/gun violence, and protest activity.

- **What this means:** While instances of protest activity and shootings remained nearly the same as last week, a 13 percent increase was observed in the number of public safety incidents.

Interested in more ZeroFox Threat Intelligence? ZeroFox researchers produce 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%