



Weekly Intelligence Brief

Classification: TLP:GREEN

February 26, 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 23, 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	3
ZeroFox Intelligence Flash Report – ALPHV Extortion Campaigns Continue into 2024	3
ZeroFox Intelligence Flash Report – LockBit Disrupted by Law Enforcement Agencies	3
ZeroFox Intelligence Flash Report – iSoon Data Leak Provides a Glimpse of Chinese State Cyber Espionage Priorities, Tools, and Tradecraft	3
ZeroFox Intelligence Flash Report – Indian Farmers' Protests and the Risk of Internet Shutdowns	4
ZeroFox Intelligence Brief – Social Engineering Series: Email Phishing	4
ZeroFox Intelligence Brief – Social Engineering Series: Non-Email Phishing	4
 Cyber Intelligence Key Findings	7
Winter Vivern Cyber Espionage Campaign Targets Critical Infrastructure of EU Countries	7
Iranian Hackers Target Middle East Policy Experts with New BASICSTAR Backdoor	7
North Korean Hackers Linked to Defense Sector Supply Chain Attack	8
 Deep and Dark Web Intelligence Key Findings	10
New Ransomware Group Emerges: Trisec Ransomware	10
New Ransomware Group Emerges: Mogilevich Ransomware	10
Actor Cyclops Advertised Knight 3.0 Ransomware Source Code	11
 Exploit and Vulnerability Intelligence Key Findings	13
CVE-2023-3457	13
CVE-2024-1783	13
 Ransomware and Breach Intelligence Key Findings	15
LockBit Taken Down by Law Enforcement	15
Threat Actor Leaks Argentine Airlines Data	15
 Physical and Geopolitical Intelligence Key Findings	17
Physical Security Intelligence: Global	17
Physical Security Intelligence: United States	17
 Appendix A: Traffic Light Protocol for Information Dissemination	19
 Appendix B: ZeroFox Intelligence Probability Scale	20

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Flash Report – ALPHV Extortion Campaigns Continue into 2024](#)

Ransomware and digital extortion (R&DE) collective ALPHV is continuing extortion campaigns in 2024, with its attack tempo very likely back on an upward trajectory following a recent disruption. Since the law enforcement (LE) activity reported by ZeroFox on December 19, 2023, the proportion of ALPHV attacks targeting entities based in North America has increased significantly—from a 2023 average of approximately 59 percent to 85 percent. It is likely that the specific targeting of North America and the increasing attack tempo contributed to the U.S. Department of State offering a series of financial rewards on February 15, 2024, for information related to ALPHV perpetrators. ALPHV attacks are very likely to continue over the next two months, targeting mostly North America-based organizations. There is a roughly even chance that the current upward trajectory in activity will plateau or decline as a result of continued LE attention and scrutiny.

[ZeroFox Intelligence Flash Report – LockBit Disrupted by Law Enforcement Agencies](#)

R&DE collective LockBit's leak site was seized by LE agencies in a joint operation between 11 countries dubbed "Operation Cronos." LockBit's affiliate panel, source code, chats, and victim information have also reportedly been seized, with a free decryption key released for victims. As many as 22 known LockBit onion site links are either offline or displaying a seizure message. However, some of the collective's other dark web sites remain operational. The extent to which LockBit's infrastructure has been disrupted or degraded in the long term is unclear. Given the ongoing and developing nature of the operation, it is possible additional LE activity will further disrupt LockBit's operational infrastructure.

[ZeroFox Intelligence Flash Report – iSoon Data Leak Provides a Glimpse of Chinese State Cyber Espionage Priorities, Tools, and Tradecraft](#)

The iSoon data disclosures reveal the priorities, tools, and tradecraft of ongoing cyber espionage and influence operations perpetrated by China nation-state actors, shedding light on the relationship between government contractors and the breadth of cyber tools at the Chinese government's disposal. Although the authenticity of the documents remains unverified, preliminary analysis suggests iSoon is a Chinese Ministry of Public Safety-affiliated organization that, as of 2022, was tasked with offensive red team operations and monitoring Twitter (now X) to "curb illegal opinions" and to use accounts for "public opinion guidance and control." Not much is known about the GitHub

account and the user “I-S00N” that posted the leaked information (behavior consistent with both whistleblowing and disinformation campaigns), making it difficult to ascertain the ultimate goal of these disclosures.

ZeroFox Intelligence Flash Report – Indian Farmers’ Protests and the Risk of Internet Shutdowns

Over 200 farming unions are attempting to march on India’s capital, demanding agricultural reforms. Police have constructed numerous blockades on major highways and throughout New Delhi, severely impacting travel. An impending nationwide strike on February 16 will include slow-roll protests on major roadways and possible rallies in major cities. Organizers have voiced a willingness to continue the movement for months if needed. Internet shutdowns are frequently used by Indian security forces to halt the spread of protest-related news, but they have major economic consequences.

ZeroFox Intelligence Brief – Social Engineering Series: Email Phishing

Social engineering allows threat actors to take advantage of fundamental human attributes that are seen as weak aspects of a network’s attack surface and prone to manipulation, such as cognitive biases and emotional triggers that can be used by the attacker. Phishing is almost certainly the most commonly-employed method of social engineering. Successful attacks facilitate data theft or the deployment of malicious software via unauthorized network access. Techniques, tactics, and procedures (TTPs) vary significantly over time and between attacks, though the vast majority of phishing attacks leverage a form of pretexting and ultimately rely on the victim’s active participation. Email phishing is almost certainly the most commonly-leveraged method of communication observed in phishing attacks and offers the attacker a number of advantages, such as the ability to use attachments to deliver malicious payloads.

ZeroFox Intelligence Brief – Social Engineering Series: Non-Email Phishing

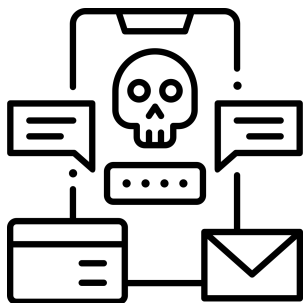
Numerous different communication methods are used in phishing attacks, enabling threat actors to conduct highly-bespoke campaigns targeting specific individuals, organizations, industries, or regions. Threat actors leverage voice phishing, SMS phishing (aka smishing), QR Code phishing, and USB phishing as alternative delivery methods to email phishing. Each of these offers the attacker unique opportunities and has different strengths and weaknesses. The methods adopted by threat actors conducting phishing attacks will continue to evolve alongside the communication channels used by individuals and organizations and will adapt in response to increased public awareness of

contemporary threats, modern security protocols, and the fundamental ways that people interact with technology.

| Cyber Intelligence |

Cyber Intelligence Key Findings

Winter Vivern Cyber Espionage Campaign Targets Critical Infrastructure of EU Countries



What happened: In October, the Russia-linked Winter Vivern group exploited cross-site scripting (XSS) flaws in Roundcube webmail servers across Europe in a campaign targeting government, military, and critical infrastructure in Georgia, Poland, and Ukraine. The threat group (aliases: TAG-70, TA473, and UAC-0114) used a Roundcube zero-day exploit, employing sophisticated social engineering to gain unauthorized access to mail servers in over 80 organizations. The campaign aimed to gather intelligence on European political and military affairs, potentially

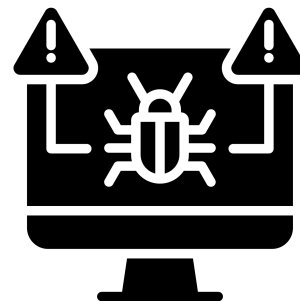
undermining security and alliances.

- **What this means:** Winter Vivern, suspected of serving Belarus and Russia's interests, has been active in cyber espionage since December 2020, with geopolitical motives evident in its targeting of Ukraine, Iran, and Georgia. Ukrainian targeting is likely driven by the ongoing conflict with Russia and aims to expose sensitive information on Ukraine's war efforts, alliances, and internal rifts. The focus on Iranian embassies is likely an attempt to assess Iran's diplomatic engagements, particularly its support for Russia in the Ukrainian conflict. Similarly, targeting Georgian entities is likely aimed at discovering foreign policy objectives as Georgia pursues European Union (EU) and NATO accession following Russia's 2022 Ukraine incursion. Notable attacks on the logistics and transportation industries likely hint at the strategic importance of disrupting supply chains in the conflict.

Iranian Hackers Target Middle East Policy Experts with New BASICSTAR Backdoor

What happened: Iran-based threat actor Charming Kitten, known for its social engineering attacks, has reportedly targeted Middle East policy experts with a new backdoor called BASICSTAR. The threat actor deploys the backdoor through a fake webinar portal. The attack strategy often involves RAR archives containing LNK files, enticing recipients to join fake webinars on topics of interest.

- **What this means:** BASICSTAR is a Visual Basic Script (VBS) malware known for its ability to gather system information, receive commands from a remote server, and download fake PDF files. Charming Kitten is highly dedicated to surveillance, thoroughly researching its targets to optimize its tactics.



Charming Kitten stands out for its frequent campaigns and use of human operators to support its activities.

North Korean Hackers Linked to Defense Sector Supply Chain Attack



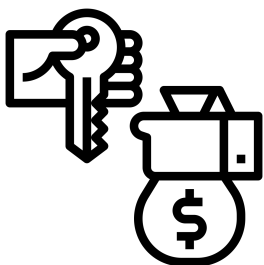
What happened: German and South Korean federal agencies have jointly issued a warning about an ongoing cyber espionage campaign orchestrated by North Korea that is targeting the global defense sector. These attacks aim to steal advanced military technology data, aiding North Korea in modernizing its conventional arms and developing new military capabilities. The threat actor initially infiltrated the target by compromising a web server maintenance firm, employing tactics like stealing SSH credentials, lateral network movement, and exploiting vulnerabilities.

- **What this means:** The federal agencies recommend taking several security measures to counter these attacks by North Korean cyber units, including limiting access for remote maintenance, maintaining audit logs, implementing robust Patch Management System (PMS) procedures, using SSL/TLS for website security, enforcing multi-factor authentication for VPNs, and educating against social engineering tactics.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

New Ransomware Group Emerges: Trisec Ransomware



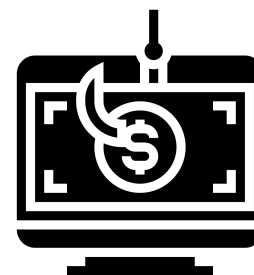
What happened: On February 19, 2024, ZeroFox observed a new leak site for the Trisec ransomware group, which includes the data of an Irish branch of Toyota called Cogans Toyota, Karolinska Institute, and an Italy-based veterinary hygienist AIVI. Trisec ransomware claims to be a cybercrime group that engages in a diverse range of activities, including both state-sponsored and financially-motivated attacks. The group has allegedly announced Operation Pied Piper of Hamelin and left a secret

message on its website.

- **What this means:** Trisec has already shown atypical TTPs. The cybercriminal group gave Cogans Toyota Ireland more than 20 days as a deadline for negotiations, which suggests that Trisec is very confident in its systems and tactics. This organization claims to be both privately and state-funded and likely also functions as a mercenary group, performing self-driven attacks and offering its services for sale. Since the group is relatively new, investigation entities have yet to disclose anything meaningful about its operations, structure, members, or systems. However, initial observations point to the organization being very resourceful and dangerous.

New Ransomware Group Emerges: Mogilevich Ransomware

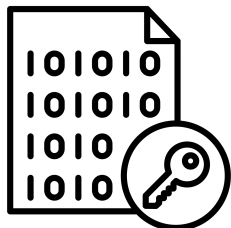
What happened: On February 21, 2024, ZeroFox observed a new ransomware group and associated leak site called Mogilevich ransomware. Mogilevich claims it is “dedicated” to data extortion, and its agenda is to “severely punish” companies that do not secure their infrastructure. The group also claims it is hacking these companies purely for economic interest. ZeroFox observed an update on the leak site on the same day targeting INFINITI USA, an automotive manufacturing company.



- **What this means:** Despite recent disruptions of several R&DE collectives leading to a rise in ransomware-as-a-service (RaaS) projects as replacements, ZeroFox has observed two new leak sites (Mogilevich and Trisec) within two days of each other. Of the two, Trisec appears to have more sophisticated capabilities than Mogilevich at this time. ZeroFox will continue to monitor both groups’ activities for any shifts, as their operations are still new. Additionally, it is not uncommon for members of a disrupted group to join a similar group

or create an offshoot of the same group under a different name. Previous LockBit members have likely taken this route with Mogilevich and Trisec after the February 19 seizure of LockBit's leak site. However, it is still too early to draw definitive conclusions.

Actor Cyclops Advertised Knight 3.0 Ransomware Source Code



What happened: On February 18, 2024, moderately credible threat actor "Cyclops" advertised the sale of Knight 3.0 ransomware source code on the predominantly Russian language dark web forum RAMP. The actor stated Knight 3.0 includes malware source code and a command and control panel. Cyclops did not list a specific price for the set and encouraged interested buyers to communicate via TOX or Jabber.

➤ **What this means:** Cyclops was the representative for Cyclops ransomware before it was rebranded to Knight ransomware. Cyclops selling the source code suggests that Knight ransomware operations will likely cease. If a threat actor purchases this source code, they will likely make small changes and launch a new ransomware variant. It is also possible that whoever buys the source code will rebrand Knight ransomware under a new name without making any changes to the code.

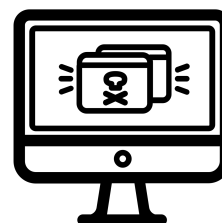
| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

[CVE-2023-3457](#)

What happened: A flaw in SourceCodester AC Repair and Services System 1.0 affects an unknown functionality of the file index.php. This **CRITICAL** vulnerability has a CVSS base score of 9.8.

- **What this means:** Manipulating the argument “username” leads to SQL injection, allowing threat actors to gain access to classified data. Threat actors can remotely launch an attack exploiting this vulnerability. ZeroFox assesses this vulnerability is likely to be targeted by hackers because its exploit has been disclosed to the public.



[CVE-2024-1783](#)



What happened: A vulnerability classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130/9.3.5u.6698_B20230810. This **CRITICAL** vulnerability has a CVSS base score of 9.8.

- **What this means:** The manipulation of the argument http_host leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.

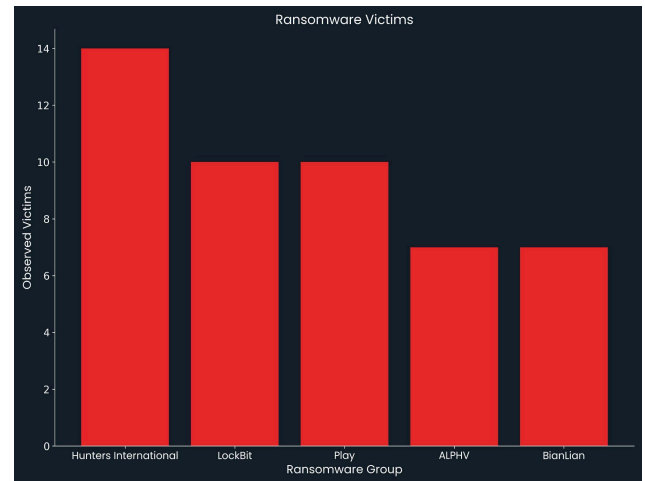
Ransomware and Breach Intelligence

| Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: LockBit Taken Down by Law Enforcement

What happened: In a joint operation between 11 countries dubbed “Operation Cronos,” law enforcement seized LockBit’s ransomware leak site. Two alleged operators have been arrested, and a list of affiliates has been revealed. Officials have also released a free decryptor tool for LockBit’s victims.

- **What this means:** The extent of degradation or disruption to LockBit’s infrastructure and whether the effect is long-term are unclear. Operation Cronos has also unveiled and halted the production of LockBit-NG-Dev, which was potentially the upcoming LockBit 4.0 and reportedly in its last stages of development.



Source: ZeroFox Internal Collections

Breach Intelligence: Threat Actor Leaks Argentine Airlines Data

What happened: ZeroFox observed threat actor “sombriaman1919” targeting Argentine Airlines (Aerolíneas Argentinas). The threat actor claims to have leaked 49,982 lines of data associated with the airline company on predominantly English-language dark web forum BreachForums.



- **What this means:** The sample data posted by sombriaman1919 indicates that the data package includes personally identifiable information (PII) like names, email addresses, and phone numbers. Affected users should be wary of unsolicited communication involving targeted emails or calls from unknown sources, as threat actors might use the leaked PII for spear phishing attacks.

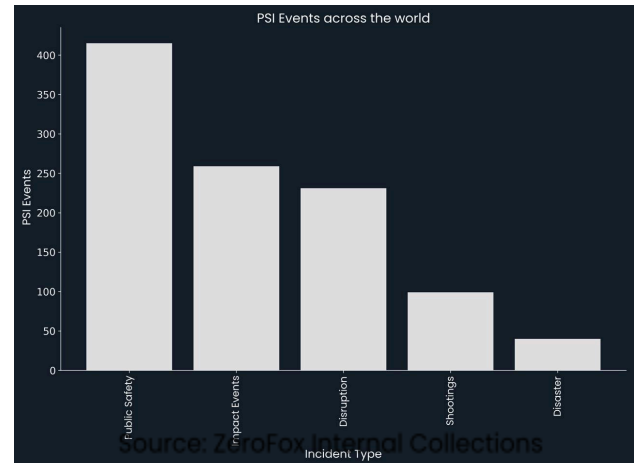
| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

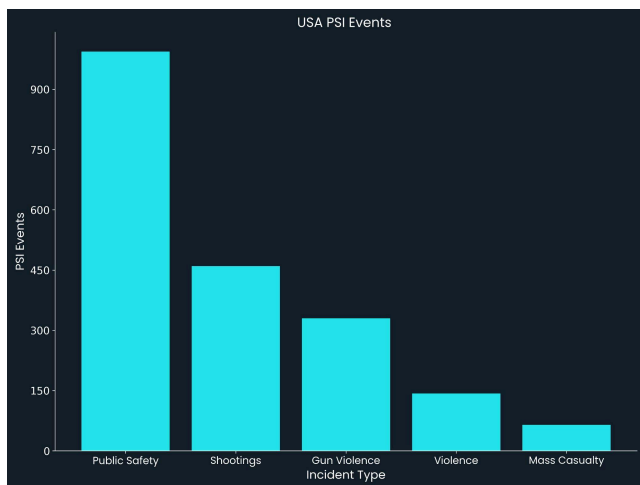
Physical Security Intelligence: Global

What happened: EU member states have agreed in principle to a 13th round of sanctions against Russia. The measures will add over 200 Russian individuals and entities to the EU's sanctions list. This package is relatively simple; the EU avoided pushing for tougher sanctions, likely to avoid opposition from Hungary. The sanctions will take effect before February 24, the two-year anniversary of Russia's invasion of Ukraine.

- **What this means:** The EU has expanded its sanctions list by adding the names of approximately 200 individuals who are prohibited from traveling to the EU and has instituted asset freezes on both individuals and companies. The latest move comes with Russia's advancements on the battlefield and Ukraine's challenges in acquiring Western-supplied ammunition.



Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: A shooting incident in suburban Minneapolis resulted in the death of two Burnsville police officers and a firefighter. College Achieve Charter School and Public School 25, both in Paterson, NJ, received threats on February 20. On February 23, the U.S. Embassy was alerted of a bomb threat.

- **What this means:** The Minneapolis shooting occurred when the officers were responding to a call for help. Meanwhile, the bomb threat targeting College Achieve Charter School caused the administration to shut the school down for a day; students at

Public School 25 sheltered in place. The bomb threat issued to the U.S. Embassy was reportedly first communicated to television stations.

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%