



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

November 20, 2023

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 November 17, 2023*; 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 Brief – APT41 Primer	2
ZeroFox Intelligence Flash Report – Active Exploitation of Juniper RCE Vulnerabilities	2
ZeroFox Intelligence Brief – Ransomware & Digital Extortion – LockBit Targeting	2
ZeroFox Intelligence Flash Report – Anonymous Sudan Increases Attack Tempo	2
ZeroFox Intelligence Flash Report – GhostSec Hactivist Group Launches GhostLocker Ransom-as-a-Service	2
 Cyber Intelligence Key Findings	4
LockBit Ransomware Spills Over 40 GB of Boeing Data	4
Ducktail Malware Targets the Fashion Industry	4
DP World Cyberattack Blocks Thousands of Containers in Ports	4
 Deep and Dark Web Intelligence Key Findings	7
Hacking Group DarkCasino Exploits WinRAR Security Flaw	7
BlackCat Ransomware Gang Targets Dragos	7
New Phishing Campaign Targeting Middle Eastern Governments	8
 Exploit and Vulnerability Intelligence Key Findings	10
CVE-2023-20273	10
CVE-2023-5217	10
 Ransomware and Breach Intelligence Key Findings	12
LockBit Ransomware Gang Most Active	12
Data Breach of Italian Consumers	12
 Appendix A: Traffic Light Protocol for Information Dissemination	13
 Appendix B: ZeroFox Intelligence Probability Scale	14

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Brief – APT41 Primer](#)

In this Intelligence Brief, ZeroFox researchers provide a primer on APT41, its characteristics, recent activities, and TTPs.

[ZeroFox Intelligence Flash Report – Active Exploitation of Juniper RCE Vulnerabilities](#)

In this Intelligence Flash Report, ZeroFox researchers discuss the CISA addition of five Juniper Junos operating system vulnerabilities to its Known Exploited Vulnerabilities Catalog.

[ZeroFox Intelligence Brief – Ransomware & Digital Extortion – LockBit Targeting](#)

In this Intelligence Brief, ZeroFox researchers provide an overview of the LockBit ransomware strain, including its targeting, intrusion vectors, and initial access brokers, based on its primary role in ransomware and digital extortion.

[ZeroFox Intelligence Flash Report – Anonymous Sudan Increases Attack Tempo](#)

In this flash report, ZeroFox researchers report on an increased frequency of attacks associated with cyber threat group Anonymous Sudan during Q3 and Q4 2023.

[ZeroFox Intelligence Flash Report – GhostSec Hacktivist Group Launches GhostLocker Ransom-as-a-Service](#)

In this flash report, ZeroFox researchers delve into recent ransomware-as-a-service developments from the GhostSec hacktivist group, including how ransomware groups may leverage these developments and GhostSec's plans for selling access.

| Cyber Intelligence |

Cyber Intelligence Key Findings

LockBit Ransomware Spills Over 40 GB of Boeing Data

What happened: On October 26, 2023, ZeroFox Intelligence observed Russia-linked ransomware group LockBit listing Boeing as a victim on its darknet leak site. LockBit claimed to have stolen a “tremendous amount of data” from the aerospace company. On November 2, Boeing reportedly confirmed that it was aware of the attack. Boeing’s name was removed from the list thereafter, indicating that negotiations between the two parties had begun. However, on November 12, LockBit published over 43 GB of data allegedly stolen from Boeing, including backups for various systems, after the company reportedly refused to pay a ransom.



Source: [hXXps://www.boeing.com/](https://www.boeing.com/)

- **What this means:** At this time, Boeing has confirmed that this impacts the company’s parts and distribution business; however, it has not indicated whether defense or other sensitive data had been impacted.

Ducktail Malware Targets the Fashion Industry

What happened: A Vietnam-linked threat actor group has been targeting marketing professionals in the fashion industry who are trying to shift companies. Victims across the world are lured with documents purportedly related to projects associated with prominent fashion brands, usually containing images relating to those clothing companies. However, the package also contains the Delphi-written Ducktail malware, which steals cookies and account details after accessing the victims’ ads and business accounts.



Source: [hXXps://fortune.com/2014/09/22/fashion-industry-big-data-analytics/](https://fortune.com/2014/09/22/fashion-industry-big-data-analytics/)

- **What this means:** This can present challenges for would-be job seekers as leveraging these high-profile brands makes the jobs appear lucrative, and the information shared by applicants could be used for malicious purposes once harvested.

DP World Cyberattack Blocks Thousands of Containers in Ports

What happened: International logistics firm DP World Australia has reportedly disclosed that a cyberattack is affecting normal operations in



Source: [hXXps://www.bleepingcomputer.com/news/security/dp-world-cyberattack-blocks-thousands-of-containers-in-ports/](https://www.bleepingcomputer.com/news/security/dp-world-cyberattack-blocks-thousands-of-containers-in-ports/)

several Australian ports. The company is currently collaborating with cybersecurity professionals to re-establish landside freight operations at its ports. DP World has engaged the Office of the Australian Information Commissioner in response to the incident and is investigating the nature of data access, exfiltration, and the possibility of personal information compromise.

- **What this means:** As observed with disruptions that have occurred at other ports, the potential to disrupt shipping operations on a global scale is large, with containers either being stalled or rerouted through less efficient transport and the costs of shipping increasing rapidly as a result.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Hacking Group DarkCasino Exploits WinRAR

Security Flaw

What happened: A hacking group dubbed DarkCasino has recently established credibility as a new advanced persistent threat group, particularly after it was attributed to the zero-day exploit of a WinRAR security flaw since April of this year. DarkCasino was originally the name for a phishing campaign conducted by APT group EvilNum but has evolved into an autonomous, economically motivated group.

- **What this means:** The origins and evolution of cybercriminal groups, trends, and motives are changing as technology advances and may often remain undetected for significant periods of time. This highlights the continued importance of implementing consistent cybersecurity awareness measures for companies and individuals alike.



Source:
<https://thehackernews.com/2023/11/experts-uncover-darkcasino-new-emerging.html>

BlackCat Ransomware Gang Targets Dragos

What happened: ALPHV, aka BlackCat Ransomware group, has reportedly published data stolen from a U.S.-based cybersecurity company Dragos (dragos[.]com), after allegedly breaching the company via a third party. However, representatives from Dragos state that there is no evidence that the company was breached. These allegations come after the company thwarted a different ransomware attack in May of this year.

- **What this means:** Breaches of high-profile cybersecurity providers, such as the recent ones of Dragos and Okta, offer threat actors credibility among the cybercriminal community. Regardless of whether ALPHV penetrated Dragos's system for a second time, the rapid spread of the allegations before definitively proven false still allows the threat actor to profit from the disinformation, even if temporarily, and degrades the reputation of the targeted company.



Source:
<https://thecyberexpress.com/dragos-data-breach-exposed-by-blackcat/>

New Phishing Campaign Targeting Middle Eastern Governments

What happened: Government entities in the Middle East are the targets of a new phishing campaign employing the IronWind downloader. The activity is attributed to threat actor TA402 (aka Molerats and Gaza Cyber Gang), which shares TTP overlap with pro-Hamas hacking group APT-C-23.

- **What this means:** TA402 has been noted as a sophisticated and capable threat group focused on cyber espionage in the Middle East and primarily operates in the interest of the Palestinian Territories, though no direct link between TA402 operators and Hamas has been identified. Since the declaration of war between Israel and Hamas in October 2023, illicit cyber activity in the region has rapidly increased on both sides of the conflict, leaving open the question as to what role the group could play as the conflict deepens and potentially spreads throughout the region. Additionally, the current phishing campaign indicates that the Israel-Hamas war has not hindered TA402's operations so far.



Source:
<https://thehackernews.com/2023/11/new-campaign-targets-middle-east.html>

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

CVE-2023-20273

What happened: A **HIGH** vulnerability identified this week in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands into the underlying operating system with root privileges.

- **What this means:** Organizations should implement access controls for impacted systems after careful review to ensure that there are no interruptions to production services, in addition to the HTTP Server feature on all internet-facing systems being disabled or restricting its access to only trusted source addresses.

CVE-2023-5217

What happened: Another **HIGH** CVE identified this week was a vulnerability that has been found that involves a Heap buffer overflow in vp8 encoding in libvpx in Google Chrome prior to 117.0.5938.132 and libvpx 1.13.1 allowing a remote attacker to exploit heap corruption via a crafted HTML page potentially.

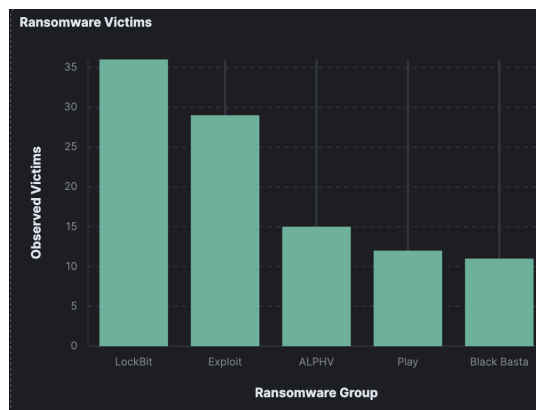
- **What this means:** Organizations should update thread counts and resolutions to ensure allocations are updated correctly and ensure that VP8 is disabled to avoid a crash.

Ransomware and Breach Intelligence

| Ransomware and Breach Intelligence Key Findings

LockBit Ransomware Gang Most Active

What happened: ZeroFox Intelligence continues to observe the LockBit 3.0 ransomware gang as the most active over the past week, with over 35 victims identified during that time. This is in keeping with observations over the past several weeks as well. The group has targeted organizations in a wide variety of industries, including education, retail, logistics, energy, and education, which are located in the United States, Europe, Asia, and South America.



Source: ZeroFox Internal Collections

- **What this means:** LockBit continues to be one of the most prolific ransomware groups in existence, with success against organizations of all sizes utilizing double-extortion techniques of deploying ransomware on an organization's systems in tandem with exfiltrating data from the organization.

Data Breach of Italian Consumers

What happened: A database of Italian consumers, comprising 136,660 email addresses being exposed, was subsequently shared on a deep web platform. No passwords were found in this breach. Other notable data fields observed in this package include name, gender, and phone number. The threat actor did not disclose the ultimate source of the data breach or how it was exploited.



- **What this means:** Organizations or users with impacted accounts should institute immediate password changes and enable multifactor authentication for all affected accounts.

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%