



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

December 11, 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 December 8, 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 – New Underground Market Comes Online Just in Time for the Holidays	2
ZeroFox Intelligence Brief – The Underground Economist: Volume 3, Issue 24	2
ZeroFox Intelligence Brief – An Introduction to Nation-State Cyber Threats	2
ZeroFox Intelligence Brief – Ransomware & Digital Extortion – ALPHV Targeting	2
 Cyber Intelligence Key Findings	4
Agent Raccoon Backdoor Targets Organizations in the Middle East, Africa, and the United States	4
U.S. Navy Contractor Austal USA Targeted in a Cyberattack	4
AI-Driven Operation Doppelganger Propagates Disinformation to U.S., Ukrainian, and German Audience	4
 Deep and Dark Web Intelligence Key Findings	7
#Opsrael Newest Attack on TelCom	7
ColdFusion Vulnerability Still Persists	7
Water/Wastewater Continue to be Targeted	8
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2023-6360	11
CVE-2023-5803	11
 Ransomware and Breach Intelligence Key Findings	13
Play Ransomware Gang Most Active	13
Breach Disclosure: Podruzhka	13
 Appendix A: Traffic Light Protocol for Information Dissemination	14
 Appendix B: ZeroFox Intelligence Probability Scale	15

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Brief - New Underground Market Comes Online Just in Time for the Holidays](#)

In this Intelligence Brief, ZeroFox researchers provide an overview of a new underground market known as OLVX Marketplace that is gaining notoriety just in time for the holidays.

[ZeroFox Intelligence Brief - The Underground Economist: Volume 3, Issue 24](#)

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

[ZeroFox Intelligence Brief - An Introduction to Nation-State Cyber Threats](#)

In this Intelligence Brief, ZeroFox researchers provide an overview of the distinction between different state-linked threat actors and how advanced persistent threats are defined.

[ZeroFox Intelligence Brief - Ransomware & Digital Extortion - ALPHV Targeting](#)

In this Intelligence Brief, ZeroFox researchers provide updates on ALPHV targeting, including a profile of the group, regional targeting statistics, associated IOCs and TTPs, and recommendations for protecting against the group's activities.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

Agent Raccoon Backdoor Targets Organizations in the Middle East, Africa, and the United States

What happened: Cybersecurity researchers have observed an unknown threat actor distributing a new backdoor called Agent Raccoon. Agent Raccoon conducts backdoor attacks through scheduled tasks in the form of Google Updates, allowing command executions like file downloads and uploads. This threat actor is reportedly targeting education, real estate, retail, non-profit, telecom, and government organizations in the United States, the Middle East, and Africa.



- **What this means:** Researchers are yet to zero in on how these entities were breached but have identified certain tools used—such as a version of Mimikatz called Mimilite and Ntospay.

U.S. Navy Contractor Austal USA Targeted in a Cyberattack

What happened: Austal USA, a ship-building contractor for the U.S. Department of Defense (DoD) and the Department of Homeland Security (DHS), has reportedly confirmed a cyberattack and is currently mitigating the situation. Earlier this week, ZeroFox Intelligence observed Hunters International Ransomware group claim to have breached Austal USA.



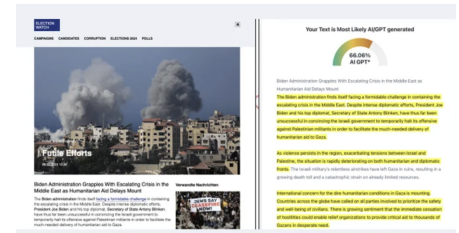
- **What this means:** The group has allegedly leaked some data as proof of the attack and is threatening to release more data supposedly stolen from the navy contractor. However, Austal USA has stated that no personal or classified information was compromised in the attack.

AI-Driven Operation Doppelganger Propagates Disinformation to U.S., Ukrainian, and German Audience

What happened: Russia-origin AI-powered Doppelganger is disseminating disinformation among audiences in Ukraine, the United States, and Germany through an extensive network of fraudulent

websites and social media, including approximately 800 inauthentic social media accounts. Reportedly, the operation has been crafted to curate content that propagates anti-LGBTQ+ sentiments and subverts Ukraine's military and international relations. In a recent campaign, Doppelganger created genuine-looking fake news articles, likely with the help of generative AI.

- **What this means:** Despite the vastness of the operation, researchers have not observed significant audience engagement. However, they have stated the importance of monitoring Doppelganger for further enhancements of tools and tactics, particularly if this should be used to create scalable misinformation campaigns that impact public sentiment on the war and social and economic issues.



Deep and Dark Web Intelligence

| Deep and Dark Web Intelligence Key Findings

#OpIsrael Newest Attack on TelCom

What happened: On December 4, pro-Palestine hacktivist group Anonymous Collective posted to its Telegram channel that it carried out a Distributed Denial-of-Service (DDoS) attack against Cosmote, one of Greece's largest telecommunication service providers. The group claimed its reason for the attack is Greece's allyship with Israel generally and the Greek government's alleged purchase of Predator surveillance malware from Israel specifically. This is the latest reported attack in a line of recent DDoS attacks by Anonymous Collective as part of its longstanding #OpIsrael campaign. On November 24 and 27, the group claimed responsibility for DDoS attacks against Kornit Digital and Eliahu, respectively. Kornit Digital is an Israeli-American international manufacturing company, and Eliahu is an Israeli-based private insurance and financial group.



Source:
<https://www.radware.com/security/threat-advisories-and-attack-reports/opisrael-a-decade-in-review/>

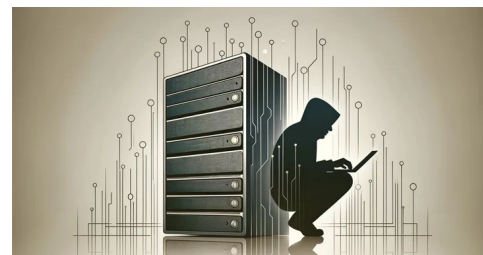
- **What this means:** Anonymous Collective has been perpetrating yearly attacks as part of #OpIsrael for over a decade, primarily leveraging DDoS attacks to disrupt Israel's digital information infrastructure and to cause significant financial damage to Israeli institutions in order to bring attention to the Palestinian cause. Although the operation's impact and relevance have varied over time, the current Israel-Palestine conflict – the region's most violent in several decades – could provide the Collective more ammunition than it has previously had. This may include developing stronger TTPs, which are illustrated in these most recent attacks. For example, #OpIsrael attacks normally take place in April every year; currently, #OpIsrael attacks align with the ongoing conflict, with Anonymous actors also posting on a Telegram channel on December 5 encouraging others to commit DDoS attacks against Israel. Additionally, the collective has historically only targeted Israeli institutions as part of #OpIsrael; however, the December 4 attack targeted a foreign government due to its association with and support of Israel. ZeroFox will continue to monitor the evolution of these TTPs into the new year.

ColdFusion Vulnerability Still Persists

What happened: On December 5, the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory detailing the recent exploitation of a critical vulnerability in Adobe ColdFusion by unidentified threat actors, which granted them initial access to at least two U.S. federal

government servers at an unnamed Federal Civilian Executive Branch (FCEB) agency. The vulnerability, identified as CVE-2023-26360, ultimately allowed the threat actors to drop malware using HTTP POST commands into the public-facing servers running versions 2018 Update 15 and earlier and 2021 Update 5 and earlier. Both of these versions were outdated when the compromises occurred between June and July of this year, despite the agency having been mandated to patch the vulnerability in May. CISA analysis indicates that the exploitation was likely aimed at obtaining information on the broader network infrastructures, and no successful data exfiltration or lateral movement could be confirmed.

- **What this means:** While CVE-2023-26360 was previously exploited as a zero-day until March when Adobe released updated versions of ColdFusion, the threat actors have remained successful in compromising those entities who have not installed the updates. Prioritizing immediate software updates and conducting regular vulnerability scans are crucial for U.S. government entities, particularly leading up to the 2024 presidential election.



Source:
<https://thehackernews.com/2023/12/hackers-exploited-coldfusion.html>

Water/Wastewater Continue to be Targeted

What happened: An Iranian state-affiliated threat actor is targeting critical infrastructure in the U.S., with an emphasis on waste and water systems (WWS). The group CyberAv3ngers, who are likely affiliated with the Iranian Revolutionary Guard Corps (IRGC), has conducted attacks against WWS targets in multiple states since late November 2023. The attacks are primarily targeted against infrastructure that uses Unitronics Vision Series programmable logic controllers (PLC). In addition to the WWS sector, Unitronics PLC is used by numerous critical infrastructure sectors that present a vulnerability to state actors.



Source: <https://www.iranintl.com/en/2023/11/269249>

- **What this means:** The series of attacks coincides with a broader campaign by Iranian and HAMAS-affiliated APT groups in response to the Israel-HAMAS conflict. Unitronics is an Israeli-owned company whose product appears to have been specifically targeted by CyberAv3ngers. IRGC is an Iranian military organization that is active throughout the Middle East and elsewhere. The open targeting of U.S. critical infrastructure by an IRGC-affiliated threat actor represents an escalation in the ongoing cyber conflict that

grew from the Israel-Hamas War. There is a moderate likelihood this activity continues and spreads to other vulnerable infrastructure that relies upon Unitronics PLC.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

CVE-2023-6360

What happened: A **CRITICAL** vulnerability identified this week was for the 'My Calendar' WordPress Plugin, version < 3.4.22 is affected by an unauthenticated SQL injection vulnerability in the 'from' and 'to' parameters in the '/my-calendar/v1/events' rest route.

- **What this means:** Versions below 3.4 are only impacted if the external API has been enabled and the vulnerability has been addressed in version 3.4.22.



Source:
`hXXps://wordpress[.]org/plugins/my-calendar/`

CVE-2023-5803

What happened: A **HIGH** CVE identified this week was a vulnerability that has a Cross-Site Request Forgery (CSRF) vulnerability in Business Directory Team Business Directory Plugin – Easy Listing Directories for WordPress allows Cross-Site Request Forgery. This issue affects Business Directory Plugin – Easy Listing Directories for WordPress: from n/a through 6.3.10.

- **What this means:** Users should update to the latest version of the plugin immediately. Should an organization fall victim to this vulnerability, an attacker would be able to execute controls in line with the victim's permissions.



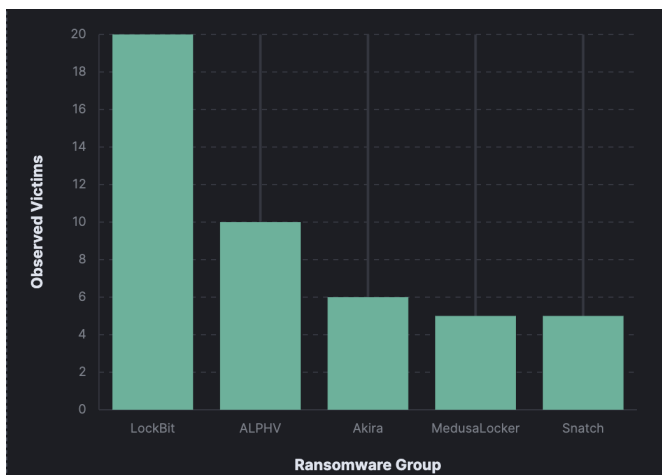
Source:
`hXXps://wordpress[.]org/plugins/business-directory-plugin/`

| Ransomware and Breach Intelligence |

Ransomware and Breach Intelligence Key Findings

Lockbit Ransomware Gang Most Active

What happened: ZeroFox Intelligence has once again observed the LockBit ransomware gang as the most active over the past week, with over 20 victims identified during that time. The group has targeted organizations in a wide variety of industries, including biotechnology, manufacturing, real estate, and retail, which are located in the United States, the Netherlands, and the United Kingdom. LockBit 3.0—currently the most prolific extortion operation—has been equipped with worm-like capabilities that enable self-propagation across a compromised network.



Source: ZeroFox Internal Collections

The strain is renowned for its speed of compromise, leveraging strong cryptography to render thousands of files inaccessible to users within seconds. Backups are removed to prevent file recovery attempts.

- **What this means:** Organizations should adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege, implement secure password policies with phishing-resistant MFA, complex passwords, and unique credentials, and deploy robust External Attack Surface Management solutions for ongoing Lockbit-targeted discovery.

Breach Disclosure: Podrzhka

What happened: Podrzhka, a Russia-based online store of cosmetics and perfumes company, had 2,183,173 email addresses and hashed passwords exposed, which were subsequently shared on a deep web platform. The threat actor noted that the data dump is from August 1, 2023. Other notable data fields observed in this package include gender, name, physical address, date of birth, and user activity. The threat actor did not disclose the ultimate source of the data breach or how it was exploited.



Source: hXXps://podrygka[.]ru/

- **What this means:** Impacted users should update their passwords immediately and remain vigilant against phishing attempts.

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%