



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

December 25, 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 22, 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
Flash Report – ALPHV Ransomware and Digital Extortion Operations Disrupted	2
Intelligence Brief – The Underground Economist: Volume 3, Issue 25	2
 Cyber Intelligence Key Findings	4
3,500 Arrested and USD 300 Million Seized in Interpol-Run Operation HAECHI IV	4
Critical RCE Flaw in Perforce Helix Core Server	4
New Chrome Zero-Day Vulnerability Exploited in the Wild	5
 Deep and Dark Web Intelligence Key Findings	7
Hacktivist Group Anonymous Russia Claims to have Left KillMilk and has Joined a Separate Group	7
Israel-linked Group Claims Cyberattack that Shut Down 70 Percent of Iran's Gas Stations	7
ALPHV Ransomware Unseized Data Leak Site, Claims Retaliation on U.S. Critical Infrastructure	8
 Exploit and Vulnerability Intelligence Key Findings	10
CVE-2023-49797	10
CVE-2023-49760	10
 Ransomware and Breach Intelligence Key Findings	12
LockBit Ransomware Gang Most Active	12
Breach Disclosure: Poland Crypto	12
 Appendix A: Traffic Light Protocol for Information Dissemination	13
 Appendix B: ZeroFox Intelligence Probability Scale	14

| This Week's ZeroFox Intelligence Reports

[Flash Report - ALPHV Ransomware and Digital Extortion Operations Disrupted](#)

In this flash report, ZeroFox researchers provide updates around a joint international law enforcement effort to seize the victim leak site for the ALPHV ransomware group and what this likely means for the group's activities.

[ZeroFox Intelligence Brief - The Underground Economist: Volume 3, Issue 25](#)

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

3,500 Arrested and USD 300 Million Seized in Interpol-Run Operation HAECHI IV

What happened: A trans-continental police operation against financial cybercrimes, termed Operation HAECHI IV, has resulted in the arrests of 3,500 suspects and the seizure of USD 300 million worth of assets across 34 countries. The six-month operation targeted threat actors involved in seven types of cyber-enabled scams, including voice phishing, romance scams, online sextortion, investment fraud, and money laundering associated with illegal online gambling. Additionally, investigators used INTERPOL's Global Rapid Intervention of Payments (I-GRIP), a stop-payment mechanism, to detect and freeze more than 82,000 bank accounts related to fraudulent activities.



- **What this means:** Voice cloning, one of the tactics utilized in this cybercriminal operation, will continue to present challenges for law enforcement as they look to get ahead of criminal activity. The arrests this week will provide a disruption to this network of cybercriminals, who will need to look to regroup after the arrests and loss of financial resources.

Critical RCE Flaw in Perforce Helix Core Server



What happened: Perforce Helix Core Server, a source-code management platform widely used in the entertainment, government, military, technology, and government sectors, has addressed four vulnerabilities. Three of these involve denial of service (DoS) issues that can lead to financial losses in large-scale deployments, while a critical vulnerability allows arbitrary remote code execution as LocalSystem by unauthenticated attackers.

- **What this means:** Attackers exploiting this vulnerability (CVE-2023-45849) could install backdoors, access sensitive data, modify system settings, and potentially gain complete control over the affected system running a vulnerable version of Perforce Server. Users should download the latest version of Helix Core from the vendor's download portal to mitigate this situation.

New Chrome Zero-Day Vulnerability Exploited in the Wild

What happened: Google has published new security updates following reports of a new Chrome zero-day vulnerability CVE-2023-7024 being actively exploited in the wild. The high-severity flaw, a heap-based buffer overflow bug in the WebRTC framework poses risks of program crashes and arbitrary code execution. Users should update to Chrome versions 120.0.6099.129/130 (Windows) and 120.0.6099.129 (macOS and Linux) to mitigate potential threats. Additionally, users of Chromium-based browsers like Microsoft Edge, Brave, Opera, and Vivaldi are advised to apply fixes once available.



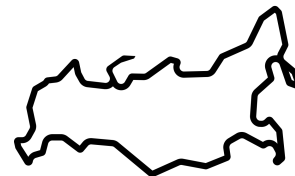
- **What this means:** If exploited, this vulnerability could lead to program crashes or arbitrary code execution.

Deep and Dark Web Intelligence

| Deep and Dark Web Intelligence Key Findings

Hacktivist Group Anonymous Russia Claims to have Left KillMilk and has Joined a Separate Group

What happened: On December 19, 2023, pro-Russian hacktivist group Anonymous Russia, a former member of pro-Russian hacktivist group Killnet, claims to have parted ways from Killnet and its leader, KillMilk. The threat actor claims to have joined Cyber Army Russia. The Cyber Army Russia hacktivist group has conducted cyberattacks against Ukraine and nations that support Ukraine.



- **What this means:** This could suggest the group's eagerness to exert influence and form alliances with the pro-Russian hacktivist community.

Israel-linked Group Claims Cyberattack that Shut Down 70 Percent of Iran's Gas Stations



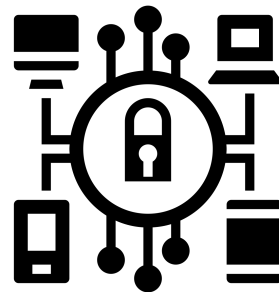
What happened: On December 19, 2023, the Israeli hacker group Gonjeshke Darande, also called Predatory Sparrow, admitted to causing significant damage to Iran's gas station infrastructure. They asserted this cyberattack was in retaliation to the aggressive actions of the Islamic Republic and its allies in the area. As a result, 70 percent of the gas stations were unable to operate. Israeli hackers have shared screenshots that demonstrate their involvement in the Iranian gas station network. These screenshots reveal specific details about individual gas stations, payment systems, management systems accessed from the central server, and other related documents.

- **What this means:** This cyberattack on Iranian gas stations demonstrates further escalation of Israeli-Iran tensions. Iran continues to struggle to get up-to-date hardware and software, often relying on Chinese-manufactured electronics or older systems no longer being patched by manufacturers, making them easier for a potential hacker to target. Pirated versions of Windows and other software are common across Iran and will likely lead to more cyberattacks fueled by the current Israel-Gaza war.

ALPHV Ransomware Unseized Data Leak Site, Claims Retaliation on U.S. Critical Infrastructure

What happened: On December 20, 2023, ZeroFox observed that the ALPHV ransomware data leak site that had been seized by law enforcement the day prior was unseized and had a note from the ransomware operators. They claimed to have moved to a new onion site and stated that they were removing all rules from their affiliate program. This would allow affiliates to target United States critical infrastructure.

- **What this means:** ALPHV has been one of the most prolific ransomware groups of 2023 and despite disruption, they continue to operate. The group was likely moving servers and creating a new blog to keep operations running while the law enforcement seizure was taking place. The removal of rules that allows affiliates to target U.S. critical infrastructure opens the doors for additional victim targeting which may cause an increase in attacks in the near future. However, affiliates may choose to focus on higher profile victims to target now which would result in an overall decrease of attacks but a more severe impact.



Exploit and Vulnerability Intelligence

| Exploit and Vulnerability Intelligence Key Findings

CVE-2023-49797

What happened: A vulnerability classified as **HIGH** has been found in a PyInstaller-built application, elevated as a privileged process, which may be tricked by an unprivileged attacker into deleting files the unprivileged user does not otherwise have access to. A user is affected if all of the following are satisfied: the user runs an application containing either ``matplotlib`` or ``win32com``; the application is run as an administrator (or at least a user with higher privileges than the attacker); and the user's temporary directory is not locked to that specific user (most likely due to ``TMP``/``TEMP`` environment variables pointing to an unprotected, arbitrary, non-default location).

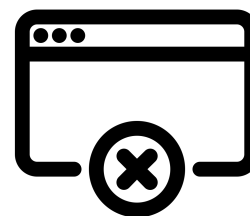


- > **What this means:** The attacker is able to very carefully time the replacement of a temporary file with a symlink. This switch must occur exactly between ``shutil.rmtree()``'s builtin symlink check and the deletion itself B: The application was built with Python 3.7.x or earlier, which has no protection against Directory Junctions links. The vulnerability has been addressed in PR #7827, which corresponds to ``pyinstaller`` `>= 5.13.1`. Users are advised to upgrade. There are no known workarounds for this vulnerability. There are currently no countermeasures known against this vulnerability.

CVE-2023-49760

What happened: A **HIGH** CVE identified this week was a Cross-Site Request Forgery (CSRF) vulnerability in Giannopoulos Kostas WPsoonOnlinePage. This issue affects WPsoonOnlinePage: from n/a through 1.9.

- > **What this means:** Currently there is no fix available for this vulnerability, and it could allow a threat actor to force higher privileged users to execute unwanted actions under their current authentication.

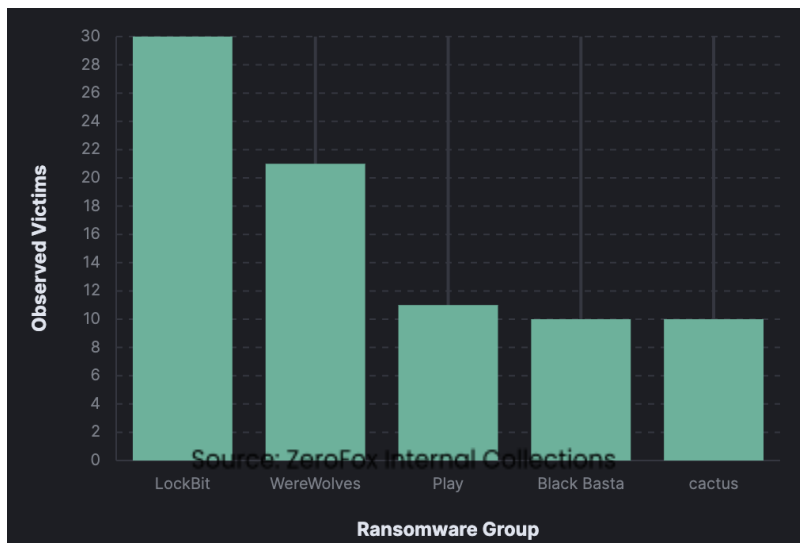


| Ransomware and Breach Intelligence |

Ransomware and Breach Intelligence Key Findings

LockBit Ransomware Gang Most Active

What happened: The LockBit ransomware group was observed by ZeroFox Intelligence as the most active over the past week, with over 30 victims identified during that time. The LockBit group has targeted several organizations in the construction industry, along with other industries, which are located in the United States and Europe. In addition, ZeroFox came across a new ransomware group called WereWolves Ransomware, which lists 21 victims. WereWolves has published six targets previously compromised by LockBit ransomware. It is reportedly claimed that WereWolves encrypts company data using a version of the LockBit3 ransomware code.



- **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: Poland Crypto



Source:
[https://rue\[e\]e/blog/poland-crypto-tax/](https://rue[e]e/blog/poland-crypto-tax/)

What happened: 1080K Poland Crypto had 1,694,720 email addresses exposed, which were subsequently shared on a deep web platform. No passwords were found in this breach. Other notable data fields observed in this package include name, and phone number. The threat actor did not disclose the ultimate source of the data breach or how it was exploited.

- **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%