



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

December 18, 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 15, 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 Flash Report – ALPHV and NoEscape Affiliates Very Likely Pivoting to Alternative Operations	2
ZeroFox Intelligence Flash Report – Anonymous Russia Announces War Against NATO	2
ZeroFox Intelligence Flash Report – SiegedSec Hacktivist Group Creates New Data Leak Site	2
ZeroFox Intelligence Flash Report – Network Access Sale Linked to Chandrayaan-3 Mission	2
 Cyber Intelligence Key Findings	4
Russian Cyber Actor Star Blizzard Continues Worldwide Spear-Phishing Campaigns	4
Lazarus Group Is Still Juicing Log4Shell, Using RATs Written in 'D'	4
Cybercriminals Use Wyoming Shell Companies for Global Hacks	4
 Deep and Dark Web Intelligence Key Findings	7
China Continues to Target U.S. Critical Infrastructure via Volt Typhoon Campaign	7
Iran's Parliament Approves Cooperation Bill with Russia	7
NoEscape Ransomware Operation Allegedly Exit Scammed Affiliates, Actor N0_Esc4pe Banned on Forums	8
 Exploit and Vulnerability Intelligence Key Findings	10
CVE-2023-6657	10
CVE-2023-48371	10
 Ransomware and Breach Intelligence Key Findings	12
LockBit Ransomware Gang Most Active	12
Breach Disclosure: D3scene	12
 Appendix A: Traffic Light Protocol for Information Dissemination	13

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Flash Report - ALPHV and NoEscape Affiliates Very Likely Pivoting to Alternative Operations](#)

In this flash report, ZeroFox researchers analyze how disruption to the operations of prolific R&DE collectives ALPHV (aka BlackCat) and NoEscape will very likely drive former affiliates to pivot to other R&DE offerings and how similar collectives will likely look to leverage this.

[ZeroFox Intelligence Flash Report - Anonymous Russia Announces War Against NATO](#)

In this flash report, ZeroFox researchers discuss Anonymous Russia's announcement that it would be targeting NATO with a cyber war, which may impact NATO-aligned countries as a result.

[ZeroFox Intelligence Flash Report - SiegedSec Hacktivist Group Creates New Data Leak Site](#)

In this flash report, ZeroFox researchers provide updates on the SiegedSec hacktivist group, which has targeted NATO-affiliated countries, and its recent new leak site.

[ZeroFox Intelligence Flash Report - Network Access Sale Linked to Chandrayaan-3 Mission](#)

In this flash report, ZeroFox researchers report on the announcement of the sale of likely network access to an unnamed India-based organization that has an ongoing partnership with India's Chandrayaan-3 mission.

| Cyber Intelligence |

Cyber Intelligence Key Findings

Russian Cyber Actor Star Blizzard Continues Worldwide

Spear-Phishing Campaigns

What happened: In a joint advisory, CISA and other international cybersecurity agencies are warning about Russia-based actor Star Blizzard (SEABORGIUM/CallistoGroup/TA446/COLDRIVER/TAG-53/BlueCharlie) using spear-phishing attacks to academia, defense, and governmental organizations, NGOs, think tanks, and politicians in the United Kingdom and other geographical areas of interest.



- **What this means:** Star Blizzard engages with its targets through online networking platforms to first establish trust and then deploys phishing links to steal login credentials. The group steals emails and attachments from the victim's inbox and also accesses the victim's mailing list data and contacts list for follow-on targeting or further phishing activity.

Lazarus Group Is Still Juicing Log4Shell, Using RATs Written in 'D'



What happened: Andariel, a subset of Lazarus, is reportedly exploiting Log4Shell globally and is targeting organizations with a new remote access Trojan (RAT) written in the D programming language, useful in avoiding detection and analysis. Andariel initiated attacks recently by exploiting exposed VMware Horizon servers vulnerable to Log4Shell, a two-year-old historical flaw in Apache Log4j (CVE-2021-44228).

- **What this means:** This vulnerability, rated 10 out of 10 on the CVSS bug severity scale, is of maximum severity. Given the widespread use of the Log4J Java library it affected, researchers estimate that hundreds of millions of systems were impacted when initially discovered.

Cybercriminals Use Wyoming Shell Companies for Global Hacks

What happened: Cybercriminals are utilizing Wyoming-based limited liability companies (LLCs) for global cyberattacks involving distributed denial of services (DDoS). Cybercriminals reportedly take advantage



of Wyoming's lax regulations for setting up anonymous shell companies as foreign cybercriminals seek to mask their identity and pass internet traffic off as originating from the United States.

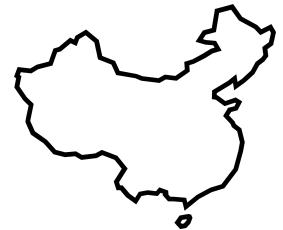
- **What this means:** Reporters have identified instances of Wyoming LLCs being implicated in high-profile hacking activities, including DDoS attacks targeting news organizations and nonprofits worldwide.

Deep and Dark Web Intelligence

| Deep and Dark Web Intelligence Key Findings

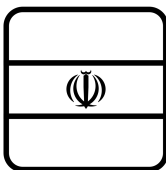
China Continues to Target U.S. Critical Infrastructure via Volt Typhoon Campaign

What happened: This week, officials released more details on recent activity targeting U.S. critical infrastructure by threat actors affiliated with China's People's Liberation Army (PLA). The threat actors reportedly compromised the computer systems of approximately two dozen critical infrastructure entities over the past year, including transportation, communication, and water and power utilities. These compromises – part of an ongoing cyber campaign dubbed "Volt Typhoon" – are likely aimed at intelligence gathering to cause future logistical disruptions amid rising U.S.-China tensions in the Pacific. Notable targets of the campaign within the last year include a key shipping port on the West Coast and a water utility system in Hawaii. The U.S. government and Microsoft first detected the Volt Typhoon roughly a year ago and have since observed the threat actors predominately utilizing TTPs such as living-off-the-land (LOTL) binaries and hands-on keyboard activities to conduct their attacks.



- **What this means:** While the Volt Typhoon has been active since at least 2021 and has previously attacked other verticals outside of U.S. critical infrastructure, the current U.S.-China geopolitical context matters in this case. This is particularly true when considering the location of the campaign's more recent U.S. targets being in, and within close proximity to the Indo-Pacific. This suggests that China is preparing to act in the event of a conflict with the United States amid increased military operations surrounding Taiwan. Logistically speaking, the threat actors' specific use of LOTL binaries, which allows them to remain undetected by blending in with usual network activity, highlights the importance of robust defense methods such as stronger multi-factor authentication (MFA) policies, among others.

Iran's Parliament Approves Cooperation Bill with Russia



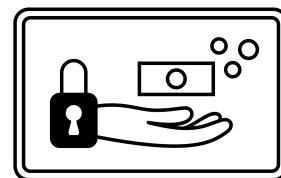
What happened: On December 10, 2023, the Iranian Parliament approved an Information Security Deal with Russia. The bill aimed at fostering cooperation with Russia in the realm of information security, as both countries are accused of extensive cyber attacks. The bill holds nine articles, focusing on combating cyber threats, fortifying information security measures, and fostering collaboration between Iran and Russia.

- **What this means:** In recent years, Iran and Russia have strengthened their political, military, communication, and cyber ties, prompting concerns among Western countries and their allies. This bill formalizes long-standing cooperation between the two nations and comes as the US presidential cycle is heating up. Both nations have a history of conducting influence operations against the U.S. elections; this legislation elevates the risk of those operations going into 2024. The concern lies with the potential targeting of "election infrastructure, campaigns, and voters" by authoritarian regimes.

NoEscape Ransomware Operation Allegedly Exit Scammed

Affiliates, Actor N0_Esc4pe Banned on Forums

What happened: On December 10, 2023, the actor N0_Esc4pe was banned on XSS for allegedly exit scamming affiliates of the NoEscape ransomware operation. The actor has also been banned on Exploit and RAMP. Affiliates of the ransomware operation stated on the major underground forums that the ransomware panel and data leak site blog were inaccessible, and the actor N0_Esc4pe had not been online in days but still owed them money.



- **What this means:** ZeroFox has confirmed that the ransomware data leak site is inaccessible, and the date of the last reported victim was December 4, 2023. NoEscape ransomware, a possible rebrand of Avaddon ransomware that shut down in 2021, launched in June 2023 and has since reported over 100 victims on their data leak site in the last six months. It is possible the ransomware operation ceased due to recent law enforcement attention of ransomware groups with the takedown of RagnarLocker ransomware, Ransomed[.]vc affiliates allegedly getting arrested, and ALPHV ransomware's data leak site blog going offline briefly, which brought on claims of law enforcement involvement. It is likely that another rebrand of this ransomware will emerge in the future under a new name. However, since the actor exits scammed affiliates, they have harmed their credibility, and affiliates may be wary of joining a rebrand of this ransomware operation.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

[CVE-2023-6657](#)



What happened: A vulnerability classified as **CRITICAL** has been found in SourceCodester Simple Student Attendance System 1.0. This affects an unknown part of the file /modals/student_form.php. The manipulation of the argument id leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-247365 was assigned to this vulnerability.

➤ **What this means:** There are currently no countermeasures known against this vulnerability, which may impact confidentiality and availability.

[CVE-2023-48371](#)

What happened: A **CRITICAL** CVE identified this week was a vulnerability where the ITPison OMICARD EDM's file uploading function does not restrict the upload of files with dangerous characteristics.

- **What this means:** An unauthenticated remote attacker can exploit this vulnerability to upload and run arbitrary executable files to perform arbitrary system commands or disrupt service.



| Ransomware and Breach Intelligence |

Ransomware and Breach Intelligence Key Findings

LockBit Ransomware Gang Most Active

What happened: The LockBit and Play ransomware groups were observed by ZeroFox Intelligence as the most active over the past week, with over 20 victims identified during that time apiece. The LockBit group has targeted several organizations in the energy industry, along with other industries, which are located in the United States and Europe. The Play ransomware group has also been targeting organizations in the United States, with victims including those in the entertainment, transportation, and engineering industries, among others.



Source: ZeroFox Internal Collections

- **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: D3scene



What happened: D3scene, a Germany-based gaming community forum, had 970,423 email addresses exposed, which were subsequently shared on a deep web platform. 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

WHEN SHOULD IT BE USED?

Red

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.

Amber

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.

WHEN SHOULD IT BE USED?

Green

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.

Clear

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%