



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

December 23, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. 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 December 20, 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	2
ZeroFox Intelligence Flash Report – CIOp Claims Responsibility for Zero-Day Exploitation	2
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 21	2
 Cyber and Dark Web Intelligence Key Findings	4
Iranian Company Founder Arrested for Supporting IRGC and Procuring U.S. Tech for Military Drones	4
Germany Disrupts BADBOX Malware	4
CISA and EPA's Advisory on Internet-Exposed HMIs Risks to WWS Sector	5
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2024-53677	7
CVE-2022-23227	8
 Ransomware and Breach Intelligence Key Findings	10
This Week in Ransomware: Rhode Island Cyberattack and LockBit 4.0 Release News	10
Repercussions and Recovery Following Massive Data Breaches	11
 Physical and Geopolitical Intelligence Key Findings	14
Physical Security Intelligence: Global	14
Physical Security Intelligence: United States	15
 Appendix A: Traffic Light Protocol for Information Dissemination	16
 Appendix B: ZeroFox Intelligence Probability Scale	17

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Flash Report – CI0p Claims Responsibility for Zero-Day Exploitation](#)

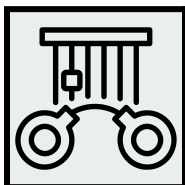
On December 15, 2024, the ransomware group CI0p reportedly claimed responsibility for a recent series of data theft attacks that targeted organizations using Cleo managed file transfer (MFT) software solutions. In October 2024, Cleo divulged a vulnerability tracked as CVE-2024-50623 that permitted unrestricted file uploads and downloads. A second vulnerability was discovered in December 2024 (tracked as CVE-2024-55956). While ZeroFox cannot verify CI0p's claims, they are likely true given that the collective has not historically sought unwarranted attention. At the time of writing, the extent of the attacks and any ongoing extortion activity is unclear. If CI0p's claims are legitimate, there is a roughly even chance that additional organizations will be compromised in the coming weeks before they are named on the victim leak site to apply additional extortion pressure.

[ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 21](#)

The Underground Economist is an intelligence-focused series illuminating dark web findings from our ZeroFox Dark Ops intelligence team.

| **Cyber and Dark Web Intelligence** |

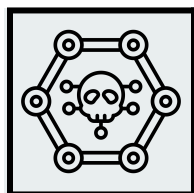
| Cyber and Dark Web Intelligence Key Findings



Iranian Company Founder Arrested for Supporting IRGC and Procuring U.S. Tech for Military Drones

What happened: An individual and their co-defendant (founder of an Iranian company) have been charged with conspiring to illegally export advanced electronic components from the United States to Iran. These components were allegedly used to help develop drone technology for the Iranian Revolutionary Guard Corps (IRGC). The two defendants have been charged with circumventing U.S. export controls and sanctions to supply sensitive technology to an Iranian company that develops technology the IRGC uses in its one-way attack drones.

- **What this means:** The co-defendant is also charged with providing material support to a foreign terrorist organization, which resulted in the deaths of three U.S. service members on a military base in Jordan. The actions of the defendants illustrate the complex networks and covert strategies used to evade restrictions, potentially fueling further instability and terrorism. The drones developed with the technology supplied by the accused have become a critical tool for the IRGC in carrying out attacks against military targets and civilian infrastructure.

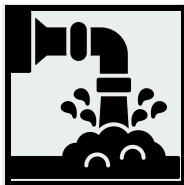


Germany Disrupts BADBOX Malware

What happened: Germany's Federal Office of Information Security (BSI) [dismantled](#) a sophisticated malware operation called BADBOX. This malware strain was reportedly pre-installed on 30,000 devices, including phones, tablets, and smart home devices. BADBOX, likely originating from China, collected sensitive data, introduced additional malware, and was involved in ad fraud. The infected devices were also exploited as proxies to mask other cyberattacks. In a recent [update](#), BadBox malware has now infected a total of 92,000 devices despite law enforcement action.

- **What this means:** At the time of writing, BSI had blocked communication to up to 30,000 devices infected with BADBOX malware. Digital picture frames, media players, and other IT products with outdated firmware are increasingly targeted by cybercriminals. According to the BSI, BadBox malware was already installed on the respective devices when they were purchased and has infected over 192,000 devices globally, despite a sinkhole operation by

the BSI that disrupted one of its C2 servers. Researchers report the malware strain is now targeting certain popular brands, likely expanding beyond lesser-known devices. The BSI has urged internet providers to block malicious traffic and users to disconnect their affected devices.



CISA and EPA's Advisory on Internet-Exposed HMIs Risks to WWS Sector

What happened: Cybersecurity and Infrastructure Security Agency (CISA) and the Environmental Protection Agency (EPA) [released](#) a joint fact sheet providing Water and Wastewater Systems (WWS) facilities with recommendations for limiting the exposure of Human Machine Interfaces (HMIs) and securing them against malicious cyber activity. The EPA and CISA have urged WWS facilities to inventory internet-exposed devices, disconnect them from the internet when possible, and secure those that remain connected with strong usernames and passwords.

- **What this means:** According to [CISA](#), there are approximately 152,000 public drinking water systems in the United States, including 50,000 community water systems, and more than 16,000 wastewater treatment systems. Over 80 percent of the U.S. population receives their potable water from these drinking water systems, and approximately 75 percent have their sanitary sewerage treated by these wastewater systems. The WWS sector is vulnerable to various threats, including physical attacks, cyberattacks, and contamination with harmful agents. Such incidents could result in widespread illness, casualties, and service disruptions. In the past, threat actors have [demonstrated](#) the capability to find and exploit internet-exposed HMIs with cybersecurity weaknesses, making strengthening HMIs essential. The ability to supply water and manage wastewater are considered National Critical Functions. These functions are vital to the United States, and any disruption, corruption, or dysfunction of the systems could have a debilitating effect on national security, economic stability, and public health and safety.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, industrial control systems (ICS), and government services. Radare2 contains a command injection vulnerability ([CVE-2024-11858](#)) caused by insufficient input validation when handling Pebble Application files. Maliciously crafted inputs can inject shell commands during command parsing, leading to unintended behavior during file processing. ColdFusion versions 2023.6, 2021.12, and earlier are [affected](#) by an Improper Access Control vulnerability that could result in an arbitrary file system read. An attacker could leverage this vulnerability to access or modify restricted files. Exploitation of this issue does not require user interaction, but the admin panel must be exposed to the internet. CISA has [added](#) this vulnerability and CVE-2024-35250 to its Known Exploited Vulnerabilities (KEV) Catalog. The [CVE-2024-25623](#) vulnerability allows a threat actor to impersonate an account on a remote server that satisfies all of the following properties: allows the attacker to register an account; accepts arbitrary user-uploaded documents and places them on the same domain as the ActivityPub actors; and serves user-uploaded documents in response to requests with an "Accept" header value of the Activity Streams media type. Versions 4.2.7, 4.1.15, 4.0.15, and 3.5.19 contain a fix for this issue. [CVE-2023-34990](#) is a relative path traversal in Fortinet FortiWLM versions 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 that allows an attacker to execute unauthorized code or commands via specially crafted web requests. Recently, CISA added one new vulnerability to its KEV Catalog based on evidence of active exploitation.



CRITICAL

CVE-2024-53677

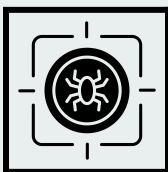
What happened: A recently patched critical vulnerability in Apache Struts 2, a widely-used open-source framework for building Java-based web applications, is being actively exploited. Publicly available proof-of-concept (PoC) exploits of the bug detail how to target vulnerable devices. The vulnerability resides in the framework's file upload functionality, where a path traversal flaw can be leveraged. Attackers can manipulate file upload parameters, allowing them to upload malicious files to the targeted system. This exploitation could have severe consequences, including the execution of remote code on the affected server.

- **What this means:** Given the widespread use of Apache Struts in critical systems, the vulnerability presents a significant risk across various sectors. The potential for remote

code execution could lead to data breaches, service disruptions, and unauthorized access to sensitive information. For organizations, this could result in severe financial losses and reputational damage, particularly if customer data or critical infrastructure is compromised. Moreover, the ability to execute remote code could allow attackers to establish a foothold for further malicious activity, such as deploying ransomware or conducting espionage. Users are strongly advised to upgrade to version 6.4.0 to ensure security.

➤ **Affected products:**

- Apache Struts versions 2.0.0 through 2.3.37 (end-of-life), 2.5.0 through 2.5.33, and 6.0.0 through 6.3.0.2.



CRITICAL
CVE-2022-23227

What happened: NUUO NVRmini2 through 3.11 allows an unauthenticated attacker to upload an encrypted TAR archive, which can be abused to add arbitrary users because of the lack of `handle_import_user.php` authentication. When combined with another flaw (CVE-2011-5325), it is possible to overwrite arbitrary files under the web root and achieve code execution as root. CISA has added this vulnerability to its KEV Catalog.

- **What this means:** By leveraging the vulnerabilities, an attacker could achieve code execution with root privileges, effectively gaining full control of the affected device. It enables unauthorized users to compromise the security of the system, potentially leading to data breaches, system tampering, or further exploitation of the network infrastructure.
- **Affected products:**
 - NUUO NVRmini2 versions through 3.11

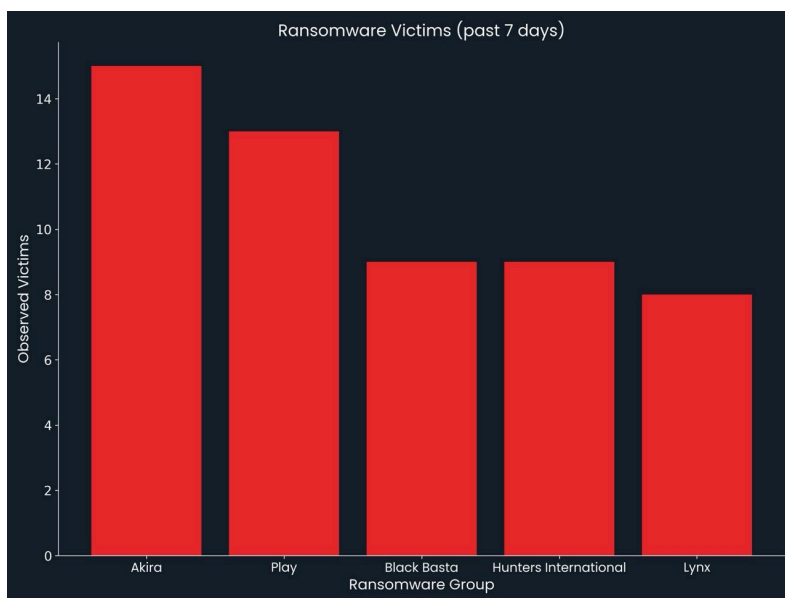
| Ransomware and Breach Intelligence |

Ransomware and Breach Intelligence Key Findings



This Week in Ransomware: Rhode Island Cyberattack and LockBit 4.0 Release News

What happened: In the past seven days, ZeroFox has observed over 120 ransomware attacks primarily targeting the manufacturing sector, with the Akira ransomware group accounting for the highest number. Over 65 percent of these targeted entities are located in North America. Meanwhile, the attack on Rhode Island's RIBridges system, managed by Deloitte, was [claimed](#) by the Brain Cipher ransomware group. RIBridges is a modern integrated eligibility system used to manage a variety of public assistance programs, including Medicaid, SNAP, and TANF. The ransomware attack compromised the system, infecting it with malicious code that led to the exposure of sensitive data. After Deloitte confirmed the attack, the system was taken offline to prevent further damage, rendering online access to services unavailable for affected citizens. On December 19, 2024, ZeroFox [reported](#) that, according to the LockBit 3.0 ransomware data leak site, the next version (LockBit 4.0) will be released by February 3, 2025.



Source: ZeroFox Internal Collections

- > **What this means:** The ransomware attack in Rhode Island may have exposed personally identifiable information (PII), including names, addresses, Social Security numbers (SSNs), and banking details of residents who use RIBridges. While the full extent of the data exposure is still being assessed, it is highly probable that cybercriminals accessed this sensitive information. According to the Brain Cipher ransomware site, the group has [access](#) to more than 1 TB of data from Deloitte. As a result, the attack has put many Rhode Islanders at risk of identity theft and fraud. Residents enrolled in various assistance programs—such as Medicaid, SNAP, and child care support—cannot access their accounts through the RIBridges web portal or mobile app. Deloitte and state officials are working

with law enforcement to investigate the attack, but the disruption is significant for those relying on these services. Impacted individuals will receive letters informing them of the attack and are encouraged to take security precautions, such as resetting passwords, placing fraud alerts, and freezing credit accounts. At the time of writing, it is unclear whether the Brain Cipher ransomware group demanded a ransom for the stolen data. With LockBit 4.0 set to be released by February 3, 2025, there are several key developments to watch for. As one of the most prominent ransomware groups, LockBit's evolution typically signals more advanced attack techniques, including refined encryption methods, enhanced evasion strategies, and potentially more destructive payloads. The upcoming version could further increase the scale and sophistication of ransomware campaigns, posing an increased threat to organizations worldwide.



Repercussions and Recovery Following Massive Data Breaches

What happened: The Interlock ransomware group claimed [responsibility](#) for exfiltrating 2.6 terabytes of data (2.1 million files) from Texas Tech University System (TTUHSC) and publishing it on their dark web portal on October 27, 2024. In response, TTUHSC is now notifying affected individuals and urging vigilance for suspicious financial or healthcare activity. A new Ledger phishing [campaign](#) is tricking users into entering their recovery phrases under the pretext of verifying security after a fake data breach. Recovery phrases, if stolen, allow full access to cryptocurrency wallets, enabling attackers to drain funds. The emails appear legitimate but redirect victims to malicious verification pages designed to steal their recovery phrases. Meta Platforms has recently been [fined](#) EUR 251 million by the Irish Data Protection Commission (DPC) for a 2018 data breach affecting 29 million Facebook accounts. The breach, caused by a vulnerability in Facebook's "View As" feature, exposed sensitive user information, including names, emails, and phone numbers. This penalty follows a [previous](#) fine in 2024 for storing users' passwords in plaintext and comes amid other legal settlements related to misuse of personal data. On December 16, 2024, hackers [leaked](#) 2.9 GB of Cisco's data on BreachForums, part of a larger 4.5 TB dataset allegedly exposed due to a misconfigured Cisco resource. IntelBroker claimed responsibility for accessing the data, which includes sensitive information from major companies like Verizon. Cisco denied a breach of core systems but acknowledged the issue stemmed from an unprotected DevHub resource.

- **What this means:** The data breach incident at TTUHSC exposed sensitive data of 1.4 million patients, including medical and billing records, financial data, and SSNs, creating risks of identity theft and targeted social engineering attacks. Furthermore, the breach increases the likelihood of ransomware extortion or the sale of stolen data on the dark web. The fake data breach phishing campaign is particularly dangerous as it involves the theft of users' recovery phrases, which are the keys to accessing their cryptocurrency wallets. Once attackers obtain the recovery phrase, they can easily transfer the cryptocurrency to their own accounts, leading to significant financial losses for victims who unknowingly provide sensitive information. In Meta's case, lax data protection has likely left sensitive user information vulnerable to exploitation, such as identity theft, financial fraud, and privacy violations. Additionally, breaches like these can lead to legal consequences, regulatory fines, and long-term reputational damage. Cisco's data leak exposes critical infrastructure and security tools used by major organizations worldwide, including its core networking and security platforms. The leaked information can likely provide hackers with detailed access to sensitive systems, allowing for future cyberattacks, exploitation, or unauthorized access. The leak further increases the risk of the remaining data being sold and used maliciously by other threat actors.

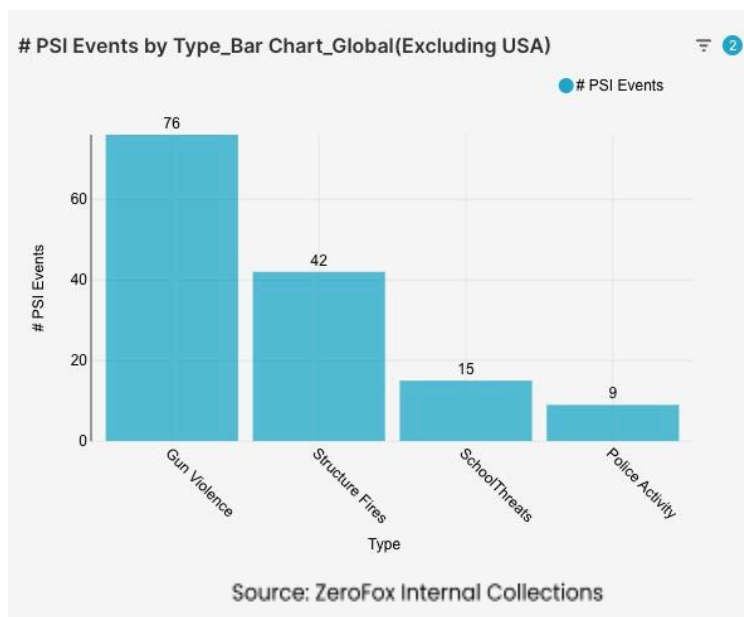
| Physical and Geopolitical Intelligence |

| Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 14 percent decrease in the mass casualty incidents perpetrated across the globe this week. Palestine, Mexico, and India were the highest contributors in this category; approximately 48 percent of the alerts were explosions. General alerts pertaining to the Israel-Hamas War (including protest, raids, and involvements in the neighboring countries) increased by 12 percent. Notably, Israel and Palestine accounted for 38 percent of all the explosions.

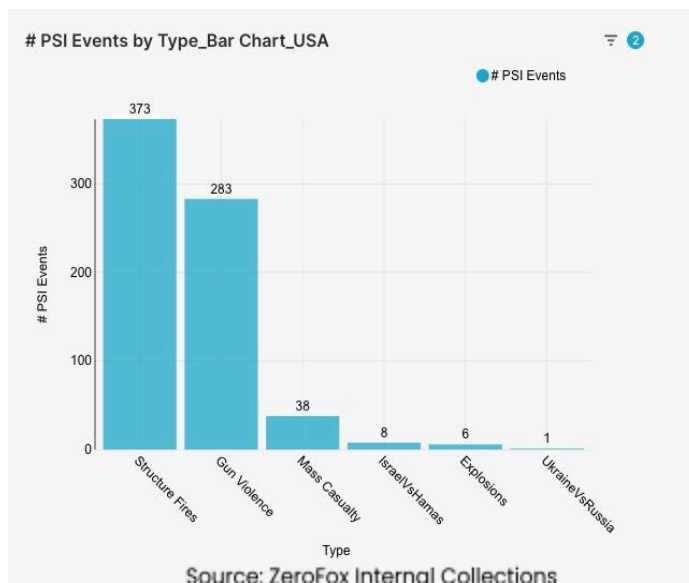
Additionally, the alerts pertaining to the ongoing Russia-Ukraine war increased by 8 percent. The three most-alerted subtypes were explosions, gun violence, and structure fires. Compared to the last week, all the subtypes decreased, with explosions decreasing by 17 percent, gun violence by 3 percent, and structure fires by 2 percent.



- **What this means:** With no ceasefire in sight, the conflict between Israel and Hamas continues with multiple explosions and lives lost. Earlier this week an explosion in the Nuseirat camp killed 33 people. Khalil Oweida School and Ahmed bin Abdul Azin School in Khan Younis, both run by the United Nations, were targeted with air strikes, and 69 people were killed in the incident. Additionally, shelling continued across the borders this week in the Russia-Ukraine conflict. Places of strategic importance were struck across the border, with one attack targeting a Russian oil depot in [Oryol](#). On December 18, 2024, an explosion was recorded in the [Sevastopol](#) region of Ukraine. Russia witnessed a larger number of explosions in its territory this week compared to weeks prior. In Mexico, 17 incidents of gun violence were reported this week, with a mass casualty incident in Veracruz in which four people were fatally shot—including the Mayor of [Tancanhuitz](#) municipality. In another incident in Buenavista municipality of [Michoacan](#), two soldiers were killed and five others were injured after a concealed IED exploded. As per the statistics, there was a significant decrease in violence across the world this week compared to last week.

Physical Security Intelligence: United States

What happened: This week, the most alerted subtypes were structure fires, gun violence, and police activity. New York and California recorded the highest number of alerts in this category (65 and 34 alerts, respectively) contributing to 27 percent of the total alerts. Gun violence this week saw a 13 percent increase compared to the previous week, with Illinois recording 35 alerts in this category. New York and California came in second with 15 alerts each. All three states combined contributed to 30 percent of the alerts. School threats showed a 24 percent decrease this week, and active shooter-related incidents stayed the same as the previous week.



- What this means:** Structure fires remain the most alerted subtype; the cold winter brings heaters and flammable decor, leading to fires in residential dwellings. Fire-related deaths have been on the rise in the United States; there have been [21 deaths](#) in 2024, up from nine in 2022, and several people died in fire-related incidents across the United States in the past week. This week also saw an increase in gun violence-related incidents; in Maryland, one person was killed and [eight](#) others were shot and injured by a man in the suburban town of Towson. Similarly, six people were injured and two fatally shot (one of whom was a teacher) by a student on Monday at the [Abundant Life Christian School](#) in Madison, Wisconsin. Police activity involves law enforcement presence for generalized threats or for unknown reasons, which often happen at schools; there was a large-scale police response to a hoax call made describing a threat at [Tuttle High School](#) in Tuttle, Ohio. Protests across the state decreased this week compared to the last, and active shooter-related incidents remained the same this week.

| 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%