



# ZEROFOX<sup>®</sup>

*Weekly Intelligence Brief*

Classification: TLP:GREEN

January 20, 2025

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 January 17, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# | Weekly Intelligence Brief |

|                                                                                                     |           |
|-----------------------------------------------------------------------------------------------------|-----------|
| <b>  This Week's ZeroFox Intelligence Reports</b>                                                   | <b>2</b>  |
| ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 1                               | 2         |
| <b>  Cyber and Dark Web Intelligence Key Findings</b>                                               | <b>4</b>  |
| CISA Publishes Guidance on Priority Considerations in Product Selection for OT Owners and Operators | 4         |
| International LE Operation Removes Chinese Malware from Thousands of Computers                      | 4         |
| Joint Collaboration on AI Cybersecurity                                                             | 5         |
| <b>  Exploit and Vulnerability Intelligence Key Findings</b>                                        | <b>8</b>  |
| CVE-2024-50603                                                                                      | 8         |
| CVE-2025-0070                                                                                       | 9         |
| <b>  Ransomware and Breach Intelligence Key Findings</b>                                            | <b>11</b> |
| CI0p Reveals Cleo Victim List; FunkSec Group's New Collaboration and More                           | 11        |
| Data Breaches and Security Failures                                                                 | 12        |
| <b>  Physical and Geopolitical Intelligence Key Findings</b>                                        | <b>15</b> |
| Physical Security Intelligence: Global                                                              | 15        |
| Physical Security Intelligence: United States                                                       | 16        |
| <b>  Appendix A: Traffic Light Protocol for Information Dissemination</b>                           | <b>17</b> |
| <b>  Appendix B: ZeroFox Intelligence Probability Scale</b>                                         | <b>18</b> |

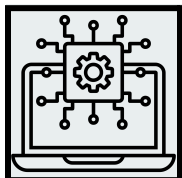
## **| This Week's ZeroFox Intelligence Reports**

### **[ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 1](#)**

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

# | **Cyber and Dark Web Intelligence** |

## | Cyber and Dark Web Intelligence Key Findings



### **CISA Publishes Guidance on Priority Considerations in Product Selection for OT Owners and Operators**

**What happened:** Cybersecurity and Infrastructure Security Agency (CISA)—along with the United States and international partners—released a [Secure by Demand](#) joint guidance. This guidance focuses on helping customers identify manufacturers dedicated to continuous improvement and achieving a better cost balance, as well as on how operational technology (OT) owners and operators should integrate Secure by Design elements into their procurement process. CISA and partners have warned that cyber threat actors, when compromising OT components, target specific OT products rather than specific organizations.

- **What this means:** Critical infrastructure and industrial control systems are prime targets for cyberattacks because of their significance to national security. Many OT products, including those used in several critical infrastructure firms, are not designed and developed with Secure by Design principles and commonly have weaknesses, such as weak authentication, known software vulnerabilities, limited logging, insecure default settings and passwords, and insecure legacy protocols. Cyber threat actors can easily exploit these weaknesses across multiple victims to gain access to control systems. When procuring products, OT owners and operators should select products from manufacturers who prioritize security elements identified in this guidance. By rigorously enforcing purchasing standards that require and prioritize buying products that incorporate these security elements, critical infrastructure organizations can help mitigate current and emerging cyber threats and begin to move away from legacy environments.

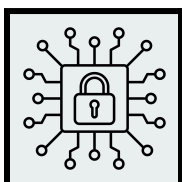


### **International LE Operation Removes Chinese Malware from Thousands of Computers**

**What happened:** The U.S. Department of Justice and the Federal Bureau of Investigation, in partnership with international law enforcement (LE), launched a multi-month operation to remove the PlugX malware from thousands of infected computers worldwide. The malware, deployed by a group of hackers allegedly associated with the Chinese government and known as “Mustang Panda” and “Twili Typhoon,” was used to steal information from compromised systems. Court

documents revealed that the Chinese government funded this hacking group to develop and deploy the malware, which has been active since at least 2014. This operation targeted computer systems in the United States, Europe, and Asia, as well as Chinese dissident groups.

- **What this means:** The PlugX malware grants hackers remote access to the infected machine, allowing them to control and manipulate it as if they had physical access. This capability enables them to steal sensitive data, such as login credentials, intellectual property, emails, and classified government or corporate documents. The malware can also facilitate further attacks by deploying additional malicious payloads, enabling surveillance, data exfiltration, or even sabotage of systems. The stolen information can likely be used for espionage, financial gain, or to disrupt targeted organizations, with potential impacts ranging from corporate theft to national security breaches. This widespread hack and long-term infection of thousands of computers—including many home computers in the United States—likely suggest a concerted effort by Chinese state-sponsored actors to gather strategic intelligence and gain an advantage over their adversaries. The removal of PlugX malware from thousands of infected devices globally demonstrates that both the U.S. government and its international partners are actively engaged in defending against sophisticated cyberespionage campaigns.



## Joint Collaboration on AI Cybersecurity

**What happened:** The AI Cybersecurity Collaboration Playbook provides guidance to organizations across the artificial intelligence (AI) community—including AI providers, developers, and adopters—for sharing AI-related cybersecurity information voluntarily with CISA and other partners through the Joint Cyber Defense Collaborative (JCDC). While focused on strengthening collaboration within the JCDC, the playbook also identifies actionable information-sharing categories applicable to broader critical infrastructure stakeholders and other sharing mechanisms. CISA encourages organizations to adopt the playbook's guidance to enhance their own information-sharing practices, contributing to a unified approach to AI-related cybersecurity threats across critical infrastructure.

- **What this means:** Companies can likely benefit from enhanced coordination and government support as well as gain the ability to collaborate on AI cybersecurity issues within a trusted environment by sharing information through JCDC. JCDC provides a mechanism for communication on vital cybersecurity matters across critical infrastructure sectors, enabling companies to discuss and address shared challenges on AI

cybersecurity. JCDC's convening capabilities help organizations access valuable threat intelligence, mitigation strategies, and a collaborative cybersecurity environment. Through the information shared, JCDC expedites coordinated responses to cyber threats and helps government partners gather information necessary to determine whether national incident response mechanisms should be activated. Additionally, JCDC produces and distributes relevant cyber threat intelligence, vulnerability management insights, and mitigation strategies, empowering companies to better manage and neutralize emerging threats.

# | **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, and government services. CISA has released [16](#) Industrial Control Systems [advisories](#) and added [six vulnerabilities](#) to its Known Exploited Vulnerabilities [catalog](#) this week. Delta Electronics DRASimuCAD expects a specific data type when opening files, but the program will accept data of the wrong type from specially crafted files. Successful exploitation of [CVE-2024-12834](#) could crash the device or potentially allow remote code execution (RCE). [CVE-2024-7344](#) is a vulnerability in the Howyar Unified Extensible Firmware Interface (UEFI) Application "Reloader" (both 32-bit and 64-bit versions) that allows the execution of unsigned software from a hardcoded path. In this month's Patch Tuesday updates, [Microsoft](#) addressed 159 security vulnerabilities, including eight zero-day flaws (three of which are actively being exploited in attacks). [CVE-2024-55591](#) is a vulnerability that has been undergoing mass exploitation by threat actors aiming to breach corporate and enterprise networks. Ivanti has released security updates [to fix multiple vulnerabilities](#) affecting Avalanche, Application Control Engine, and Endpoint Manager, including four critical flaws that could result in information disclosure. SAP has released [security patches](#) for 14 vulnerabilities. [CVE-2024-12084](#) is a heap-based buffer overflow flaw found in the rsync daemon. This issue is due to improper handling of attacker-controlled checksum lengths (s2length) in the code.



### CRITICAL

### CVE-2024-50603

**What happened:** Threat actors have exploited a critical RCE vulnerability, CVE-2024-50603, in Aviatrix Controller instances. This vulnerability arises due to improper input sanitization in certain API actions, allowing attackers to inject malicious commands into system-level operations. By crafting specific API requests, attackers can gain remote access to the affected systems without needing authentication. Once inside, they can install backdoors, crypto miners, or potentially other types of malicious software, compromising the security of the affected systems.

- **What this means:** This vulnerability highlights the risks posed by improper input validation in APIs, especially when they provide access to critical system-level functions. Attackers can bypass authentication and gain control of vulnerable systems remotely, leading to potential data breaches, unauthorized access, or exploitation of resources for malicious purposes like crypto mining. The exploitation of this flaw can have significant

consequences for organizations relying on Aviatrix Controller. To mitigate these risks, users are urged to upgrade to the patched versions (7.1.4191 or 7.2.4996) to secure their systems and prevent further exploitation.

➤ **Affected products:**

- Aviatrix Controller prior to 7.1.4191 and 7.2.x prior to 7.2.4996



**CRITICAL**

**CVE-2025-0070**

**What happened:** SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker to obtain illegitimate access to the system by exploiting improper authentication checks, resulting in privilege escalation.

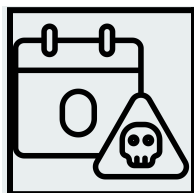
- **What this means:** On successful exploitation the SAP NetWeaver vulnerability can likely allow attackers to escalate privileges to gain unauthorized access to sensitive data and system controls. This can lead to data compromise and operational disruption.

➤ **Affected products:**

- SAP NetWeaver Application Server for ABAP versions KRNL64NUC 7.22, 7.22EXT, 7.53, and 8.04
- SAP NetWeaver Application Server for ABAP KERNEL versions 7.22 through 9.14

# **Ransomware and Breach Intelligence**

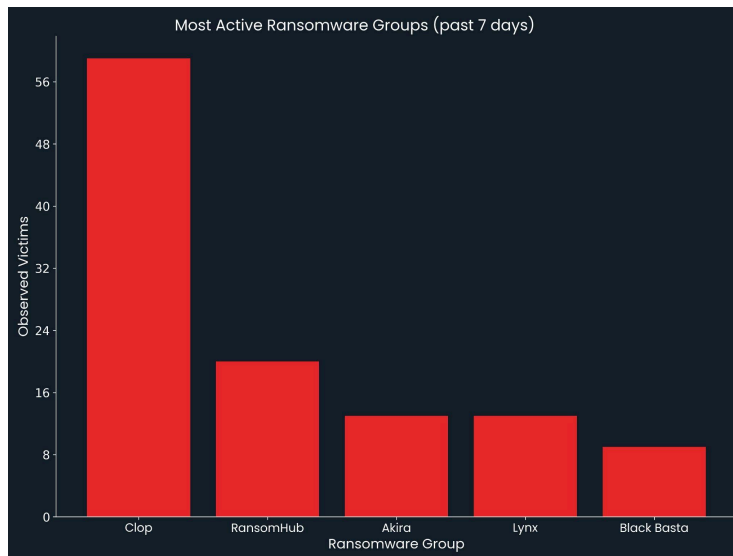
## Ransomware and Breach Intelligence Key Findings



### CI0p Reveals Cleo Victim List; FunkSec Group's New Collaboration and More

**What happened:** In the past week, ZeroFox observed more than 175 ransomware attacks, most of which were detected in North America. The most affected sector was manufacturing, followed by construction, while the most active ransomware group was CI0p. Last week, the CI0p ransomware group disclosed [59 victims](#) impacted by the Cleo data breach teased in December 2024. CI0p had previously warned that it would reveal the names of the organizations that

failed to initiate negotiations with the group. CI0p also announced it would release [a fresh list](#) of victims in the upcoming days. It is unclear whether the new list will also be related to the Cleo cyberattack. Meanwhile, cybersecurity researchers have discovered an [AI-driven ransomware group](#) named "Funksec" that compromised over 85 victims globally at the end of last year. This group employs double extortion tactics, combining data theft and encryption, and identifies itself with the "Free Palestine" movement. On January 15, 2025, ZeroFox observed [major updates](#), including a collaboration announcement, plans for future attacks, and the launch of a forum for open discussions on topics like creating ransomware with AI.



Source: ZeroFox Internal Collections

- **What this means:** As ZeroFox predicted would be likely in its [earlier reporting](#), CI0p has continued to extort and leak data from the alleged victims of the Cleo zero-day exploit cyberattack. Cleo customers should upgrade the affected tools to the latest release versions and continue to follow the guidelines provided by their internal security teams and the software provider to avoid similar attacks. The disclosure of the Cleo cyberattack victim list came on January 13 and 14, 2025, during the "Old New Year" in Russia, according

to the Julian calendar once followed in the country. Announcing the imminent release of a “new part of the companies list,” ClOp is likely trying to leverage the attention it has gained from the Cleo attack to further cement its reputation. Funksec, on the other hand, is likely setting a precedent for other ransomware groups. Funksec’s [FunkLocker](#) is a sophisticated ransomware tool with advanced double encryption and the ability to bypass security programs, allowing it to modify critical system files without authorization. It further developed its arsenal by launching a data-sorting service and an “[AI platform](#),” which includes tools for malware creation, hacking knowledge-sharing, and AI-powered interactions. The latest version of FunkLocker, [FunkLocker V1.5](#), comprises more advanced features that will likely aid the group in evading detection and spreading infection stealthily and rapidly. Collaboration with other threat actors will likely make its attacks more complicated. The forum is also likely to encourage other actors to follow suit in leveraging AI to build ransomware.



## Data Breaches and Security Failures

**What happened:** Crewmen of some [French submarines](#) accidentally gave out sensitive information like the location of their base, when they were at sea, training schedules, and patrol timings by tracking their fitness through an application on their smartwatches. Rigorous security checks prior to allowing crewmen in top secret facilities had them stow their phones away but not their smartwatches, which can reportedly store information without being connected to a device. Grinding Gear Games confirmed a data breach in [Path of Exile 2](#) after a developer’s admin account, linked to an old Steam account, was compromised. The attacker accessed tools used by customer support, allowing them to set random passwords on 66 accounts. The attacker also exploited a bug to delete logs, compromising email addresses, Steam IDs, IP addresses, and other details. Wolf Haldenstein Adler Freeman & Herz LLP recently confirmed it was impacted by a [data breach](#) on December 13, 2023, that exposed the personal information of nearly 3.5 million individuals. Hackers accessed sensitive data, including Social Security numbers, employee IDs, and medical details. The firm’s investigation was reportedly delayed, and many affected individuals have yet to be notified due to missing contact information. The breach was disclosed nearly a year later due to forensic investigation delays.

- **What this means:** In the French submarine incident, the fitness trackers stored not only important location data but also personally identifiable information that can allow any

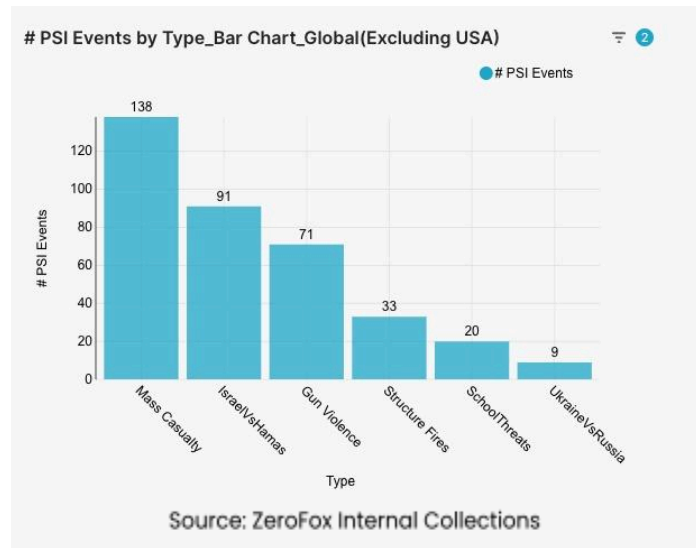
likely threat actor to identify many of the crewmen by their names and public profiles. The submarines reportedly have the capacity to store 16 nuclear missiles, making this breach a likely global threat if the situation is not mitigated to increase operational security.

Although the Path of Exile 2 hackers did not expose passwords, the compromised admin account's connection to an old Steam account was enough to grant the attacker access to sensitive tools and data. In response, the developers have banned the use of third-party accounts—like Steam accounts—being linked to staff admin tools. This move minimizes the attack surface by reducing dependencies on external platforms that might have different or less stringent security protocols. Additionally, the introduction of "significantly more stringent" IP restrictions ensures that only authorized and verified networks can access administrative systems, adding an extra layer of defense against unauthorized access. The law firm's exposed data, including Social Security numbers, medical information, and employee IDs, increases the risk of phishing, scams, and identity theft. Delays in notifying impacted individuals likely compounds these risks, as affected individuals can remain unaware of their data's exposure.

# **| Physical and Geopolitical Intelligence |**

## Physical and Geopolitical Intelligence Key Findings

### Physical Security Intelligence: Global

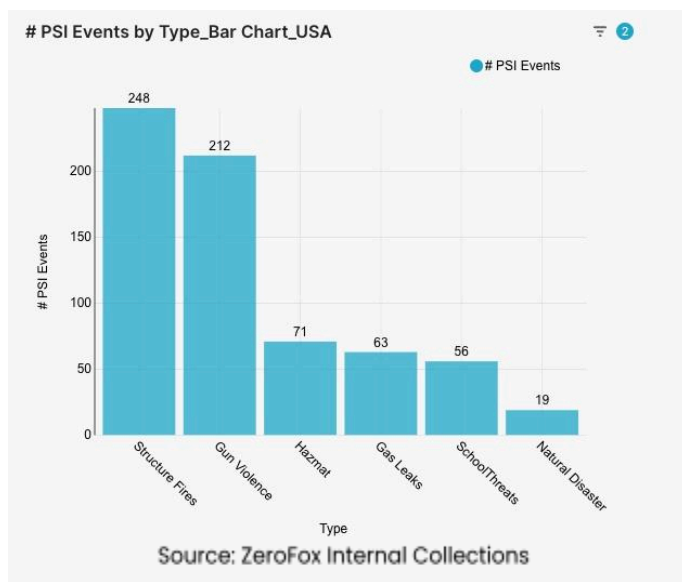


**What happened:** Excluding the United States, there was a 14 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Palestine and Mexico. Approximately 75 percent of these events were explosions, and the two aforementioned countries accounted for approximately 37 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and involvement in neighboring countries) decreased by 3 percent from the previous week. Events

related to the Russia-Ukraine war increased by 29 percent. This week, all subtypes showed an increase in alerts compared to the last. Explosions increased by 32 percent, gun violence increased by 18 percent, and structure fires increased by 18 percent. Global protest activity increased by 7 percent.

- > **What this means:** This week, while Palestine had the highest number of mass casualty alerts, overall events with the "IsraelVsHamas" tag decreased slightly. This may be due to a [ceasefire](#) deal announced earlier this week between Israel and Hamas, which would have started a six-week truce on Sunday. However, at least 78 Palestinians have been killed in Israeli strikes since the announcement. At this time, Israel has said its Cabinet will not meet to approve the ceasefire and hostage release deal with Hamas, claiming the militant group was creating a "last-minute crisis." Prime Minister Benjamin Netanyahu's office did not elaborate on what this crisis entails. Mexico had the second highest number of mass casualty alerts, with the main concern being gun violence and mass shootings. On January 14, 2025, five people were shot in [Huitzilac](#), a town which has been overrun by cartels and gang violence in recent years.

## Physical Security Intelligence: United States



**What happened:** In the past week, the top three most-alerted incident subtypes were structure fires, gun violence, and gas leaks. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, gas leaks refer to a release of contained hazardous materials into any area where gas should not be present, and structure fires are fires that affect man-made buildings. The top two states that had the most gun violence alerts were California and Pennsylvania, which together made up 19 percent of this week's nationwide total. Gun violence across the United States decreased by 4

percent from the week prior. Gas leak alerts increased by 29 percent, with the top contributing states being Florida and Texas. Structure fires increased by 3 percent, with the top contributing states for this subtype being California and New York. Notably, national school-related threats increased by 51 percent, with Georgia being the highest contributing state.

- > **What this means:** This week, gas leaks replaced police activity in the top three most-alerted subtypes due to several large-scale hazmat incidents. These include leaks in the [Colonial Pipeline](#) (Paulding County, GA), [Inwood Road](#) (Dallas, TX), and [Roaring Springs](#) (Grand Canyon, AZ), potentially due to unprecedented temperature and weather fluctuations. Alerts with the "SchoolThreats" tag saw a significant increase, with Georgia being the largest contributor; one such event in the state this week was a "credible threat" to the [Twiggs County](#) School District, which sent three campuses into a lockdown on January 15, 2025. Different areas of the country are seeing opposite ends of the weather spectrum, with the [Los Angeles](#) wildfires having now burned over tens of thousands of acres, incinerating homes and businesses, killing at least 25 people, and displacing at least 100,000 more. Conversely, Georgia is experiencing the largest snow event to hit [Atlanta](#) since 2018, with several more winter storms predicted to sweep across the [East Coast](#) next week. Both the intense wildfires and extreme cold are said to be consequences of climate change.

## | Appendix A: Traffic Light Protocol for Information Dissemination

|                         | Red                                                                                                                                                                                                    | Amber                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> 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?   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> 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.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                         | Green                                                                                                                                                                                                  | Clear                                                                                                                                                                                                                                                                                                                        |
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| HOW MAY IT BE SHARED?   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> 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%         |