



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN
November 25, 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 November 22, 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
The Underground Economist: Volume 4, Issue 19	2
 Cyber and Dark Web Intelligence Key Findings	4
NSO Group Used Another WhatsApp Zero-Day After Being Sued	4
Threat Actors Declare Cyberattack Against American Cyberspace	5
U.S. Senate Panel Holds Hearing on Suspected Chinese Hacking Incidents	5
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2024-0012	8
CVE-2024-8933	9
 Ransomware and Breach Intelligence Key Findings	11
Ransomware Happenings in the Past Week	11
High-Profile Breaches Target Finance, Healthcare, Automobile, and Telecom Companies	12
 Physical and Geopolitical Intelligence Key Findings	15
Physical Security Intelligence: Global	15
Physical Security Intelligence: United States	16
 Appendix A: Traffic Light Protocol for Information Dissemination	17
 Appendix B: ZeroFox Intelligence Probability Scale	18

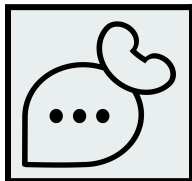
| This Week's ZeroFox Intelligence Reports

[The Underground Economist: Volume 4, Issue 19](#)

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

| **Cyber and Dark Web Intelligence** |

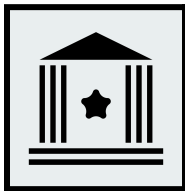
| Cyber and Dark Web Intelligence Key Findings



NSO Group Used Another WhatsApp Zero-Day After Being Sued

What happened: Israeli cyber intelligence firm NSO Group (NSO) allegedly exploited multiple zero-day vulnerabilities in WhatsApp, including a previously unknown exploit called "Erised," to install its Pegasus spyware on targeted devices using zero-click attacks. According to court documents, NSO repeatedly deployed a series of exploits targeting WhatsApp zero-days, despite WhatsApp proactively blocking NSO's access to affected devices and patching the targeted vulnerabilities. These attacks occurred even after NSO was sued by WhatsApp for its surveillance practices. NSO has [admitted](#) that it developed and sold Pegasus spyware—specifically its zero-click installation vector called "Eden," which was part of a family of WhatsApp-based vectors known collectively as "Hummingbird." This is not the first instance in 2024 of NSO making headlines about operations involving its spyware. As a part of its quarterly update process, in July 2024, Apple reportedly [notified](#) users across 98 countries—including prominent journalists and politicians—about a possible "mercenary spyware" attack utilizing Pegasus.

- **What this means:** Pegasus, a spyware platform developed by NSO, allows its customers to secretly monitor, track, and extract sensitive data from the devices of victims, posing serious risks to personal privacy and security and exposing individuals to exploitation, manipulation, and even physical harm. Despite being sued by WhatsApp for its surveillance practices, NSO continued deploying zero-click attacks. NSO released a statement in response to the allegations where it [maintained](#) that it "does not operate or utilize its products," while also indicating that it is not responsible for how users utilize the spyware and has no access to any data gathered during the software installation. However, Pegasus has found its way to the phones of Catalan politicians, journalists, activists, UK government officials, Finnish diplomats, and U.S. Department of State employees. It has created significant waves in the political landscape of various countries when investigations alleged the use of Pegasus in politically motivated campaigns. When used for espionage purposes, this spyware can compromise sensitive materials and risk such information falling into the hands of adversarial states, deepening any existing geopolitical conflict or even contributing to unrest within a country.



Threat Actors Declare Cyberattack Against American Cyberspace

What happened: Pro-Palestine hacker group Hunt3r Kill3r, which has ties to several pro-Russian hacker factions, has issued a statement declaring its intention to retaliate against the United States. On November 21, 2024, Hunt3r Kill3r, along with several pro-Russian allies, [launched](#) an electronic operation called #RED_EYE_OP targeting American cyberspace. The operation includes groups such as Moroccan Dragons, Keymous, Eagle Cyber Was Here, Server Killers, and Fighter Black Hat. The alleged cyberattacks are presented as retaliation for recent events in the Middle East and in response to what Hunt3r Kill3r allegedly perceives as the United States' decision to "expand" the ongoing Russia-Ukraine war.

- **What this means:** The launch of #RED_EYE_OP reflects how geopolitical tensions (such as U.S. support for Israel and Ukraine) can prompt digital retaliation from groups with aligned interests. The involvement of groups like Hunt3r Kill3r and its allies in retaliatory efforts against the United States signals that these digital conflicts are not limited to state actors; rather, they are increasingly involving ideologically motivated non-state actors. The announcement of a potential cyber retaliation could escalate tensions in multiple ways. First, potentially successful attacks are likely to disrupt critical U.S. infrastructure, financial systems, or other strategic sectors through cyberattacks. Second, it is likely to lead to further destabilization in the cyber domain, with more groups launching coordinated efforts to disrupt the United States or its allies in the context of the Russia-Ukraine war. Moreover, the growing number of actors involved in cyber warfare complicates the global security landscape, as governments and corporations face increasingly sophisticated and unpredictable cyber threats. This also raises concerns about the targeting of civilian infrastructure and the broader impacts on international relations, particularly if such attacks were to spread or escalate in scope.



U.S. Senate Panel Holds Hearing on Suspected Chinese Hacking Incidents

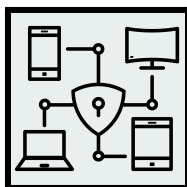
What happened: A U.S. Senate Judiciary subcommittee held a hearing to address the growing concerns surrounding Chinese hacking incidents, particularly focusing on recent attacks targeting U.S. telecom companies. The hearing aimed to assess the risks these cyberattacks pose to national security, democracy, and the economy.

- > **What this means:** The recent hearing addressed several threats posed by China-linked entities and current China-affiliated activities. The threats posed by Chinese cyber actors targeting U.S. institutions raise serious national security concerns. These attacks compromise sensitive communications, as seen in the Salt Typhoon attack targeting prominent U.S. figures this month. The risks also extend beyond hacking, as economic ties between China and American companies create vulnerabilities that China can reportedly manipulate—likely to advance its geopolitical goals. The hearing also discussed recent cyberattacks in which China-linked hackers gained access to the networks of multiple U.S. telecom companies, stealing sensitive communications data that included surveillance records. These hackers reportedly targeted political figures, including presidential and vice-presidential candidates, raising alarms about the vulnerabilities in U.S. telecommunications infrastructure. U.S. authorities, including the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), confirmed that the hackers had exploited backdoor access to law enforcement's surveillance systems, potentially compromising sensitive national security data. The hearing underscored the broader implications of these incidents, with lawmakers and experts calling for greater transparency and security in handling foreign cyber 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, industrial control systems (ICS), and government services. CISA has [added](#) five vulnerabilities to its Known Exploited Vulnerabilities (KEV) [catalog](#) and released [seven](#) ICS advisories. Researchers have [discovered](#) a few vulnerabilities that allow a local attacker to gain root privileges in the needrestart package, a utility that scans a system to identify services needing a restart after a software update, (CVE-2024-48990, CVE-2024-48991, CVE-2024-48992, and CVE-2024-11003) and a related issue in libmodule-scandeps-perl (CVE-2024-10224). Apple has addressed two zero-day vulnerabilities in its [advisory](#). CVE-2024-10924 is an authentication bypass [vulnerability](#) in the Really Simple Security (Free, Pro, and Pro Multisite) plugins for WordPress affecting versions 9.0.0 to 9.1.1.1. [CVE-2024-11120](#) is an OS command injection vulnerability affecting certain end-of-life (EOL) GeoVision devices. Chinese hackers BrazenBamboo exploited a zero-day vulnerability in Fortinet's FortiClient Windows VPN client. The [flaw](#), reported in July 2024, reportedly has no CVE assigned and remains unpatched by Fortinet. CVE-2024-21287 is a [zero-day](#) vulnerability in Agile Product Lifecycle Management (PLM) version 9.3.6 that can be exploited remotely without authentication. [CVE-2024-52940](#) is a vulnerability in popular remote desktop application AnyDesk that could expose users' IP addresses. The flaw affects AnyDesk versions 8.1.0 and earlier on major operating systems.



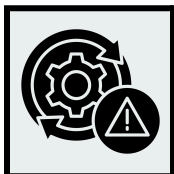
CRITICAL

CVE-2024-0012

What happened: A critical authentication bypass vulnerability in Palo Alto Networks' PAN-OS software allows attackers with network access to the management web interface to escalate privileges to administrator level. The flaw impacts PAN-OS versions 10.2, 11.0, 11.1, and 11.2 on PA-Series, VM-Series, CN-Series firewalls, and Panorama devices but excludes Prisma Access and Cloud NGFW.

- **What this means:** Threat actors can likely target this bug to gain control over critical infrastructure firewalls, granting them the ability to alter security policies, disable protections, or create backdoors for persistent access. Given its applicability to widely deployed systems, this flaw poses a high-value opportunity for state-sponsored attackers and ransomware groups aiming to disrupt operations or exfiltrate sensitive data.
- **Affected products:**
 - PAN-OS 10.2 versions < 10.2.12-h2

- PAN-OS 11.0 versions < 11.0.6-h1
- PAN-OS 11.1 versions < 11.1.5-h1
- PAN-OS 11.2 versions < 11.2.4-h1

**HIGH****CVE-2024-8933**

What happened: An improper enforcement of message integrity during transmission in a communication channel vulnerability exists that could cause retrieval of password hash and lead to denial-of-service and loss of confidentiality and integrity of controllers. CISA has addressed this flaw as a part of a recent ICS advisory involving six other vulnerabilities. Schneider Electric is establishing a remediation plan for all future versions of Modicon M340, Modicon MC80, and Modicon Momentum Unity MIE Processor that will include a fix for the CVE-2024-8933 vulnerability.

- **What this means:** To be successful, the attacker needs to inject themselves inside the logical network while a valid user uploads or downloads a project file into the controller.
- **Affected products:**
 - Modicon M340 CPU (part numbers BMXP34*): All versions
 - Modicon MC80 (part numbers BMKC80): All versions
 - Modicon Momentum Unity MIE Processor (171CBU*)

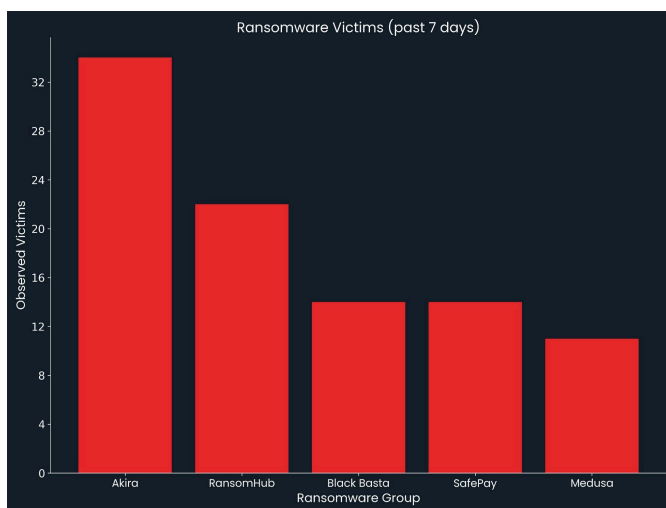
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



Ransomware Happenings in the Past Week

What happened: The Akira ransomware group hit a record high, [revealing](#) over 30 new victims in a single update to its target list; the group uses a ransomware-as-a-service (RaaS) model to steal and encrypt sensitive data. Meanwhile, the U.S. Department of Justice (DOJ) [charged](#) an individual linked to Phobos ransomware, which extorted over USD 16 million from global entities. Additionally, CISA, the FBI, and Australia's ACSC [released](#) insights on BianLian ransomware's tactics and indicators to aid defense against this data extortion group. Helldown ransomware has been [exploiting](#)



Source: ZeroFox Internal Collections

Helldown ransomware has been [exploiting](#) vulnerabilities in Zyxel firewalls, likely leveraging CVE-2024-42057 and possibly an undocumented flaw, to breach corporate networks. Attackers encrypt files, steal large data sets, and use compromised accounts to move laterally and disable defenses. In the past week, ZeroFox has observed over 200 ransomware attacks, the majority of which were claimed by Akira. The most affected sector was manufacturing, while the most targeted region was North America. ZeroFox also observed new ransomware groups, including [SafePay](#), [Termite](#), and [Chort](#).

- **What this means:** The surge in Akira's attacks shows a significant escalation in its ransomware operations, especially as it has surpassed its total number of 2023 victims within just a few months. The latest victims span various industries and countries; around 25 were U.S.-based targets, along with others from Canada, Europe, and other countries. Large-scale and intricate ransomware operations, like Phobos, aim to exfiltrate data for financial gain and evade detection by consistently adapting new strategies. Since May 2019, authorities have regularly [recorded](#) Phobos ransomware incidents impacting state, local, tribal, and territorial (SLTT) governments. The operation hacked large corporations, schools, hospitals, nonprofits, and a federally recognized tribe, and they extorted more than USD 16 million in ransom payments. The DOJ charges will set a precedent for potential

similar threats, discouraging other threat actors from following in Phobos' footsteps and strengthening response tactics against such ransomware attacks. Meanwhile, BianLian (which is likely Russia-based) has targeted U.S. critical infrastructure sectors since 2022 by exploiting remote desktop protocol (RDP) credentials and using tools like file transfer protocol (FTP) and Rclone for data exfiltration, emphasizing the group's technical proficiency and the risks posed to essential services. Helldown's exploitation of Zyxel firewalls exposes severe risks from unpatched enterprise hardware, particularly for small to medium-sized firms. The ransomware's rapid evolution pressures vendors like Zyxel to strengthen security measures and highlights the urgent need for proactive patching.



High-Profile Breaches Target Finance, Healthcare, Automobile, and Telecom Companies

What happened: Finastra [confirmed](#) a cybersecurity incident after an attacker used compromised credentials to access its Secure File Transfer Platform (SFTP) on November 7, 2024. A threat actor named "abyss0" claims to have stolen 400GB of data, though the post advertising it has since been deleted. The firm is investigating the breach's scope. A data breach at a French hospital [exposed](#) the medical records of 750,000 patients after a threat actor using stolen credentials accessed an electronic patient record (EPR) system. The hacker, known as "nears", claimed to have targeted multiple healthcare facilities, compromising over 1.5 million records in total. ZeroFox [observed](#) that threat actor "EnergyWeaponUser", in collaboration with "IntelBroker", claimed to have leaked a database associated with the U.S.-based automobile manufacturer Ford Motor Company (Ford) on the predominantly English-language dark web forum BreachForums. The actor allegedly exposed 44,000 records, including customer names, physical locations, and products purchased. A newly identified threat actor, "Liminal Panda", has been [spying](#) on mobile networks in Asia and Africa for over four years. The group exploits outdated telecom systems to collect call records, text messages, and sensitive data on large groups or specific individuals.

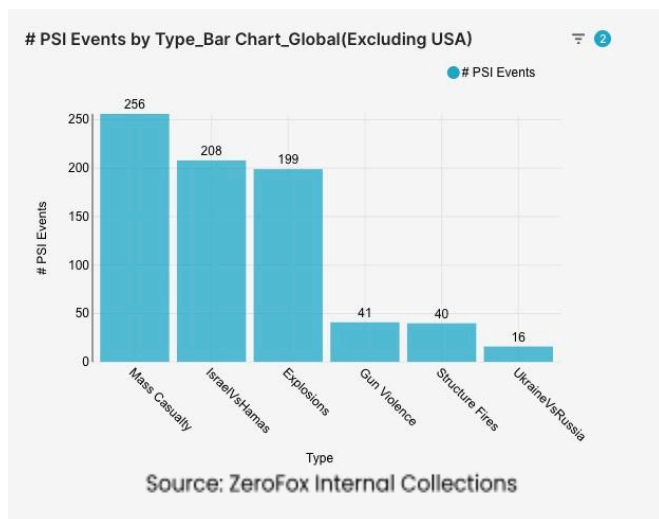
- **What this means:** As a major provider of technology solutions to banks, lenders, and traders, Finastra's exposure of sensitive information could disrupt financial operations and compromise data security. The deletion of the post creates uncertainty about whether the data is truly secure or if the removal was strategic, possibly signaling a completed transaction or fear of detection. The exposure of sensitive medical records not only threatens patient privacy but also opens avenues for targeted fraud, social engineering, and broader healthcare disruptions, demonstrating a pressing need for enhanced security practices in critical sectors. A potential breach involving Ford, carried out by

EnergyWeaponUser and IntelBroker, raises significant concerns about data security within large corporations and their third-party suppliers. Even though Ford's systems were [reportedly](#) not compromised, the leak of customer data—including names, locations, and purchase details—could expose affected individuals to phishing, fraud, and social engineering attacks. Liminal Panda's command-and-control (C2) infrastructure mimics the Global System for Mobile Communications (GSM), a widely used mobile communication standard, to covertly exfiltrate data. By leveraging outdated systems in telecom networks, the group conducts surveillance and gathers intelligence. These attacks undermine personal privacy, facilitate espionage, and expose critical vulnerabilities in global telecommunications infrastructure, particularly in regions relying on legacy systems.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

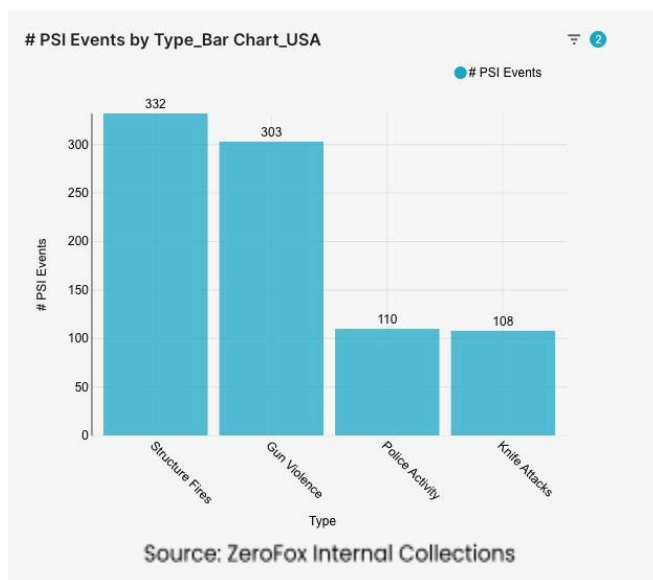
Physical Security Intelligence: Global



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 Lebanon, Israel, and Palestine (in that order). Approximately 78 percent of these events were explosions, and the three aforementioned countries accounted for about 56 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) increased by 19 percent from the previous

week. Events related to Russia's war in Ukraine increased by 60 percent. The top three most-alerted subtypes were explosions, which saw a 12 percent increase from the previous week; gun violence, which decreased by 36 percent; and structure fires, which increased by 60 percent. Global protest activity decreased by 6 percent, and the top contributing country was the United Kingdom (UK).

- What this means:** Mass casualty events, explosions, and alerts with the UkraineVsRussia qualifier tag all saw significant increases this week, which comes after U.S. President Joe Biden gave Kyiv the green light to use American-made [ATACMS](#) missiles inside of Russia. On Tuesday, Russia's Defense Ministry said Ukraine fired six ballistic missiles at a facility in Bryansk, which marks the first time Ukraine has used the longer-range American weapons to strike targets. The permission to use said weapons was given in response to Russia's recent recruitment of thousands of [North Korean](#) soldiers. Alerts with the IsraelVsHamas tag saw an increase this week as well, as the death toll in the [Gaza](#) Strip has now surpassed 44,000, according to local officials. Additionally, the International Criminal Court has decided to issue arrest [warrants](#) for Israeli Prime Minister Benjamin Netanyahu, his former defense minister, and Hamas' military chief, accusing them of crimes against humanity. As for protest activity, the majority of this week's alerts came out of the UK; [farmers](#) there have taken to the streets of London demanding the government scrap inheritance tax rules on land ownership, which they say will destroy family-run farms.



Physical Security Intelligence: United States

What happened: In the past week, the top three most-alerted incident subtypes were structure fires, gun violence, and police activity. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, police activity involves law enforcement presence for generalized threats or for unknown reasons, and structure fires are fires that affect man-made buildings. The top two states that had the most gun violence alerts were

Illinois and California, which together made up 22 percent of this week's nationwide total. Gun violence across the United States overall decreased by 9 percent from the week prior. Police activity alerts decreased by 7 percent, and the top contributing state was California. Structure fires increased by 3 percent, and the top two states for this subtype were California and New York. Notably, knife attacks increased by 29 percent, and the top contributing states were New York and California as well.

- > **What this means:** As suspected, structure fires did see an increase due to winter weather approaching, which calls for higher usage of heating devices that can cause fires. Additionally, with the coming holiday season, cooking-related fires are expected to increase as well. According to FEMA, the top three [causes](#) of residential fires are cooking (50 percent of all fires), heating equipment (12.5 percent), and electrical malfunction (6.3 percent); Thanksgiving is the peak day for cooking fires. Knife attacks also increased notably this week, as evidenced by multiple instances of stabbings. One such case involved a stabbing spree in [New York City](#) in which a suspect killed two men and critically wounded a woman; on Sunday night, two separate stabbings within 20 minutes of each other in [Glendale](#), CA, left four people injured. However, gun violence and police activity alerts did decrease somewhat, which is expected, as homicides, aggravated assaults, and robberies are typically lower in [November](#).

| 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%