



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

December 2, 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 29, 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 December 2024 Geopolitical Brief	2
 Cyber and Dark Web Intelligence Key Findings	4
INTERPOL and AFRIPOL Target Cybercrime in Africa, Arresting over 1,000 Suspects	4
UK Warns of Russia's Potential Use of AI in Cyberattacks	4
Zero-Days Exploited by Russian RomCom Hackers	5
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2024-38643	8
CVE-2024-11680	9
 Ransomware and Breach Intelligence Key Findings	11
Ransomware Hits Supply Chain Giant Blue Yonder, While New Elpaco Strikes with RDP Brute Force	11
Repercussions of Data Breaches Across Various Sectors	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

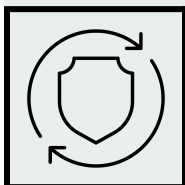
| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence December 2024 Geopolitical Brief

Israel's decision to accept a 60-day ceasefire in Lebanon significantly lowers the risk of a broader regional war. Germany is likely headed for snap elections in February 2025 after Chancellor Olaf Scholz's ruling three-party coalition collapsed. Renewed farmers' protests in France aim to derail a European Union (EU) trade agreement with Latin America. Farmers are concerned the treaty will flood European markets with cheaper agricultural products from Latin America, undercutting their prices. Indonesia is requiring Apple to commit to major local investments before it will allow iPhones to be sold in the lucrative market of over 200 million consumers.

| **Cyber and Dark Web Intelligence** |

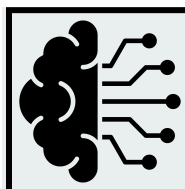
| Cyber and Dark Web Intelligence Key Findings



INTERPOL and AFRIPOL Target Cybercrime in Africa, Arresting over 1,000 Suspects

What happened: Operation Serengeti, coordinated by INTERPOL and AFRIPOL, was a major law enforcement initiative across 19 African countries, targeting a wide range of cybercrimes. Between September 2 and October 31, authorities arrested over 1,000 individuals suspected of involvement in cybercriminal activities, including ransomware attacks, business email compromise (BEC), digital extortion, and online scams. These crimes led to an estimated global financial loss of nearly USD 193 million, and approximately USD 44 million of the stolen funds were reportedly recovered. This operation resulted in the takedown of over 134,000 malicious infrastructures. The operation focused on dismantling various types of fraud schemes, from Ponzi scams and credit card fraud to online investment and multi-level marketing frauds.

- **What this means:** In Kenya, a USD 8.6 million credit card fraud exploited banking security vulnerabilities, redistributing funds globally via SWIFT. Leveraging bugs in crucial systems, like banking, leads to erosion of trust in financial institutions and the global banking network. Senegal authorities arrested eight for a USD 6 million Ponzi scheme defrauding 1,811 victims. Such fraudulent schemes take advantage of public confidence in legitimate investment opportunities and thereby, exacerbate financial insecurity. In Nigeria, the police arrested an alleged scammer accused of making a profit of USD 300,000 through fake cryptocurrency promises. Campaigns like these are likely to reduce public trust in digital assets and can deter the adoption of legitimate blockchain technologies. Suspected Cameroonian traffickers used coercion in a multi-level marketing scam, violating human rights and perpetuating modern slavery. Angola dismantled a virtual casino defrauding gamblers, undermining trust in online gaming platforms. Some 150 arrests were made, with officers seizing 200 computers and more than 100 mobile phones. Such operations will likely deter cyber criminal activity and disrupt dangerous cyber infrastructures that can likely lead to even greater damage.



UK Warns of Russia's Potential Use of AI in Cyberattacks

What happened: During the recent NATO Cyber Defence Conference, a senior UK official [warned](#) about Russia using artificial intelligence (AI) in its cyberattacks and noted possible measures to “stay one step ahead in this new AI arms race.” The measures include the launch of a new UK government-funded Laboratory for AI Security Research at the University of Oxford that will assemble a team of experts to assess the impact of AI on national security. The official also stated that besides Russia’s military effort, the state is involved in orchestrating a “hidden” cyberwar that can be both destabilizing and debilitating. Russia has targeted media, telecoms, political and democratic institutions, and energy infrastructure in the United Kingdom and continues to target other such states that lend support to or are seemingly politically aligned with Ukraine in the Russia-Ukraine war.

- **What this means:** Russian nation-state actors have relied on cyberattacks as a warfare strategy to target its geopolitical adversaries, with Russia particularly deploying cyberattacks against Ukraine since 2014. It has targeted Ukrainian mobile networks—cutting off communication for millions at a time and, on occasion, disabling the air-raid warning system in Kyiv. Russia’s scope of cyberattack has and will likely continue to expand beyond just Ukraine, with targets in countries that are perceived to be against Russia. The United Kingdom’s unwavering support for Ukraine is likely to incite more targeted cyberattacks from Russia with escalating intensity. In February 2024, a report from a cybersecurity research team highlighted how nation-state advanced persistent threats (APTs) have begun using large language models (LLMs) to enhance their operations. With rapid developments in the field of AI, several such actors—[majorly](#) from North Korea and Iran, and to a lesser extent Russia and China—are likely looking to induce more sophistication into their campaigns that will help them avoid detection and maintain persistent access to compromised systems. By exploiting AI in customized and scalable operations, these actors can enhance cyberattacks, create convincing phishing attempts, and automate malware development. Moreover, such threat actors can also leverage generative AI to procure highly realistic deepfakes in the form of audio or visual media to fuel incendiary disinformation campaigns and deepen political divides.



Zero-Days Exploited by Russian RomCom Hackers

What happened: The Russia-based threat actors dubbed as RomCom exploited two zero-day vulnerabilities—CVE-2024-9680 and CVE-2024-49039—targeting Firefox and Tor Browser users in Europe and North America. According to the National Institute of Standards and Technology’s

(NIST's) National Vulnerability Database (NVD), an attacker was able to [achieve](#) code execution in the content process by exploiting a use-after-free in animation timelines. The second [vulnerability](#) is a task scheduler elevation of privilege vulnerability.

- > **What this means:** Threat actors reportedly deployed a sophisticated attack chain using the two zero-day vulnerabilities to exploit vulnerable browsers, which required no user interaction. Victims were redirected to malicious websites, where users unknowingly downloaded backdoors, enabling attackers to run commands and deploy additional malware. The vulnerabilities allow threat actors to achieve code execution in the content process and the escalation of privilege. By deploying the RomCom backdoor, attackers likely gain persistent remote access to compromised systems, enabling data exfiltration, espionage, and subsequent financial or operational disruption in critical industries across multiple regions. RomCom has been linked, in the past, to ransomware, extortion, and credential theft, often supporting financially motivated and intelligence-gathering operations.

| **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. VMware released a high-severity security [bulletin](#) addressing five vulnerabilities in its Aria Operations product, warning of potential privilege escalation and cross-site scripting attacks. These flaws in the cloud IT operations platform could be exploited by malicious actors, making VMware products an ongoing target for advanced hacking groups. The vulnerabilities allow threat actors to achieve code execution in the content process and the escalation of privilege. [CVE-2024-11680](#) allows remote, unauthenticated attackers to make unauthorized changes to an application's configuration by sending specially crafted HTTP requests to the options[.]php file. If successfully exploited, attackers can create user accounts, upload webshells, and inject malicious JavaScript. [CVE-2023-28461](#) is an array AG/vxAG remote code execution vulnerability and is a web security bug that enables an attacker to browse the filesystem or execute remote code on the SSL VPN gateway using the flags attribute in HTTP header without authentication. CISA has [added](#) this bug to its Known Exploited Vulnerabilities (KEV) catalog. An [issue](#) was discovered in the server in Veritas Enterprise Vault before 15.2. It allows remote attackers to execute arbitrary code because untrusted data, received on a [.]NET Remoting TCP port, is deserialized. In the past week, CISA also [released](#) six Industrial Control Systems (ICS) advisories.



CRITICAL

CVE-2024-38643

What happened: QNAP recently released security bulletins addressing multiple vulnerabilities, including CVE-2024-38643 and [three](#) others that impact Notes Station 3. CVE-2024-38643 is caused by missing authentication for a critical function in Notes Station 3. If exploited, this vulnerability could allow remote attackers to gain unauthorized access and perform certain actions on the affected system. This issue has been patched in Notes Station 3 version 3.9.7 and later.

- **What this means:** If left unpatched, this vulnerability could enable attackers to compromise the affected system, potentially gaining unauthorized access, compromising security, and leading to data manipulation or other malicious activities.
- **Affected products:**
 - Notes Station 3 version 3.9.x



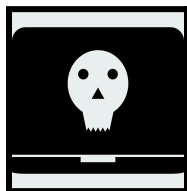
CRITICAL
CVE-2024-11680

What happened: ProjectSend versions prior to r1720 are affected by an improper authentication vulnerability. Remote, unauthenticated attackers can exploit this flaw by sending crafted HTTP requests to options.php, enabling unauthorized modification of the application's configuration.

- **What this means:** By [exploiting](#) this flaw, attackers can gain administrator-level access to compromised devices, posing serious risks to affected systems. With thousands of vulnerable ProjectSend instances still online, the failure to patch has resulted in active exploitation, including webshell deployment and unauthorized server control. As attackers increasingly use public exploits, the risk to organizations relying on self-hosted ProjectSend solutions is severe.
- **Affected products:**
 - ProjectSend versions before r1720

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

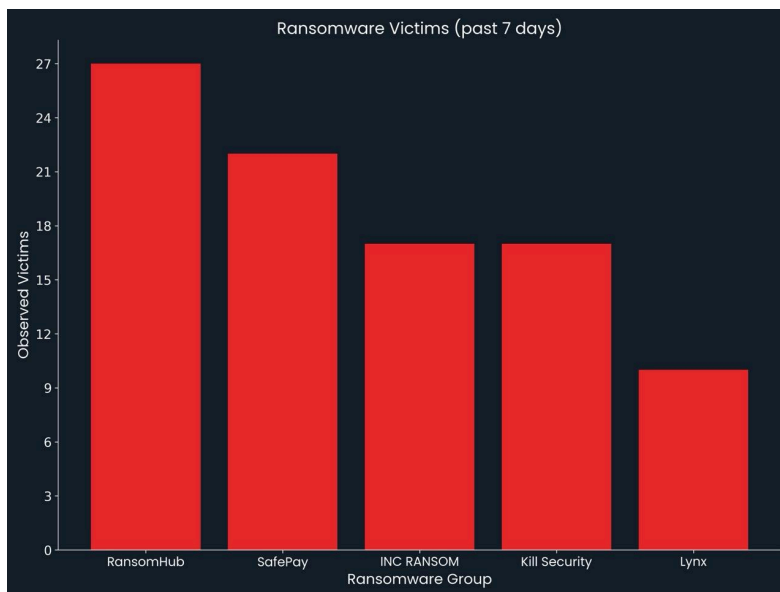


Ransomware Hits Supply Chain Giant Blue Yonder, While New Elpaco Strikes with RDP Brute Force

What happened: In the past week, ZeroFox observed over 150 ransomware attacks, most of which were detected in North America. The most affected sector was manufacturing (followed by healthcare), while the most active group was the RansomHub ransomware group. Blue Yonder, a supply chain management software provider, was targeted by a [ransomware](#) attack that impacted the company's managed services infrastructure, which supports a vast network of clients. Among those most affected were prominent UK

supermarket chains, Morrisons and Sainsbury's, as well as Starbucks in the United States, where the attack disrupted a critical backend process used for employee scheduling and time-tracking. Despite the complexity of the attack, Blue Yonder's initial [disclosure](#) indicated that no suspicious activity had been observed within its public cloud environment, implying that the attack may have been confined to its managed services infrastructure. Meanwhile, Elpaco ransomware, a variant of the Mimic strain, has been [identified](#) in attacks where hackers gained access to victims' servers via a brute force attack on Remote Desktop Protocol (RDP). Once inside, they deployed the ransomware. Elpaco takes advantage of a tool called Everything DLL, normally used for file discovery, which provides attackers with a simple graphical interface (GUI) to customize the malware's actions. Additionally, this variant allows attackers to execute system commands and disable security features on the compromised server, making it more difficult to detect and mitigate the attack.

- **What this means:** The attack at Blue Yonder has disrupted key operations for some of the world's largest retailers and manufacturers, including delays in scheduling, inventory management, order fulfillment, and time-tracking. The timing of the attack makes it even



Source: ZeroFox Internal Collections

more damaging, as businesses are already grappling with seasonal operational challenges. Global supply chains, particularly those managed through cloud-based platforms, are highly interconnected, so a disruption in one area can quickly ripple across many industries. Given Blue Yonder's essential role in managing logistics for major companies, a prolonged outage could cause significant disruptions, leading to inventory shortages, delayed deliveries, and potential loss of customer trust, further compounding the financial and reputational damage for affected businesses. On the other hand, the use of the Everything DLL and the GUI simplifies the execution and customization of Elpaco ransomware group's attacks. The group can quickly adapt the malware to suit different environments, allowing for faster and more efficient deployments. The ability to disable security tools adds an extra layer of difficulty in detecting and mitigating the attack, as it helps the ransomware evade detection while it encrypts files or steals data. The exploitation of RDP for unauthorized access also points to a common vulnerability in many organizations' IT infrastructure, especially if RDP is exposed to the internet without proper security measures like multi-factor authentication (MFA) or strong password policies.



Repercussions of Data Breaches Across Various Sectors

What happened: Unidentified hackers [breached](#) Andrew Tate's "The Real World" platform, exposing sensitive information, including usernames, private chats, and email addresses. Andrew Tate later took to [X](#) to address the incident and seemingly deny claims of the breach. HDFC Life Insurance, one of India's prominent long-term life insurance providers, has [confirmed](#) a data breach that resulted from the unauthorized sharing of sensitive customer data. The company launched an investigation after an "unknown source" shared some of the breached data. Well-regarded and established threat actor IntelBroker, in collaboration with EnergyWeaponUser, [claimed](#) to sell a database associated with Liberty Latin America, a U.S.-based telecommunications company, on predominantly English-language dark web forum, BreachForums. A cybersecurity researcher [discovered](#) an unsecured cloud storage bucket owned by SL Data Services, exposing 644,869 files (713.1 GB) with sensitive personal data, including criminal records, addresses, and family details. The files lacked encryption or password protection, and the company delayed securing the database despite repeated warnings. In other news, U.S. car insurer company Geico was [fined](#) USD 9.75 million for data breaches that exposed the personal information of 116,000 drivers. Meanwhile, Italy's data protection authority [levied](#) a fine of EUR 5 million (USD 5.20 million) on Delivery Hero-owned Foodinho for illegally processing the

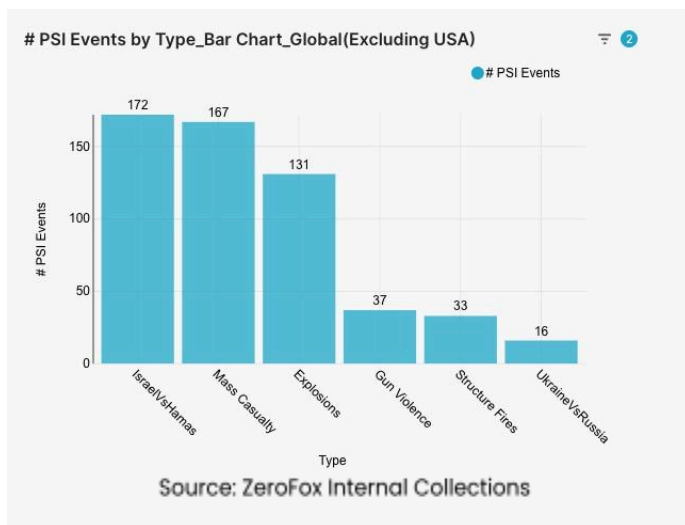
personal data of more than 35,000 riders registered on its digital platform.

- **What this means:** Exploiting a critical security flaw in The Real World platform, the hackers accessed close to 800,000 usernames and hundreds of chat servers, leaking sensitive user information. They then proceeded to flood chatrooms with pro-feminist and LGBTQ+ content, disrupting the platform and banning users, which is a likely indication that the hackers had a political motivation to conduct the attack. The exposure of sensitive user data, including private messages, email addresses, and usernames, puts members at risk of phishing, harassment, and identity theft. Meanwhile, the leak at HDFC exposes its affected customers to risks of financial fraud, extortion, and other cyberattacks from financially motivated actors. The alleged Liberty Latin breach, if true, is likely to be of interest to politically motivated actors from the People's Republic of China, who have been [targeting](#) U.S. telecommunication companies for intel gathering from government entities. The exposed SL Data Services information, including employment details, criminal histories, and family information, creates a roadmap for targeted attacks such as phishing, identity theft, and extortion. Criminals could exploit this information to impersonate victims or coerce them using private details. The severity increases as combining this with other leaked data could build complete profiles, exposing victims, their families, and associates to significant financial and personal risks. Both Geico and Foodinho had to pay fines for putting user data at risk. Such countermeasures set precedents for companies to enhance their cybersecurity framework and protect user data from unauthorized access.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

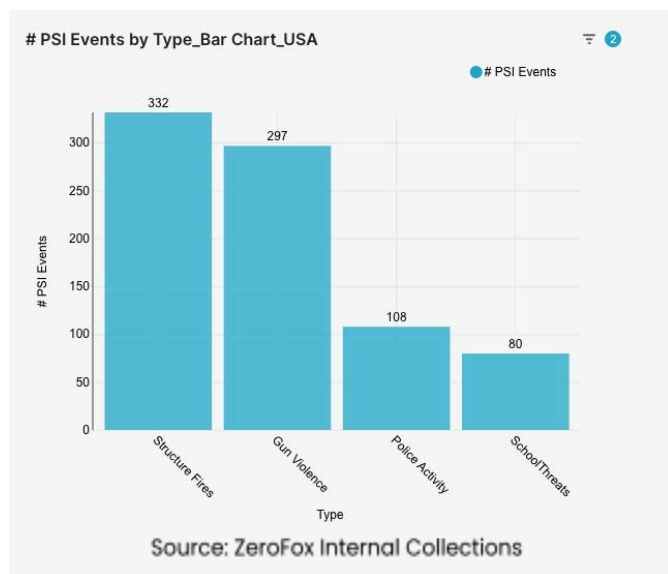


What happened: Excluding the United States, there was a 35 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Lebanon, Israel, and Palestine (in that order). Approximately 78 percent of these events were explosions, and the three aforementioned countries accounted for about 49 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 17

percent from the previous week. Events related to Russia's war in Ukraine did not increase or decrease from last week. The top three most-alerted subtypes were explosions, which saw a 34 percent decrease from the previous week; gun violence, which decreased by 10 percent; and structure fires, which decreased by 18 percent. Global protest activity increased by 18 percent, and the top contributing country was the United Kingdom (UK).

- **What this means:** Both explosions and mass casualty alerts in general decreased this week at approximately the same percentage, which corresponds to the fact that explosions typically make up a strong majority of all mass casualty alerts. A [ceasefire](#) between Israeli forces and Hezbollah took effect Wednesday morning local time, which explains the drastic decrease in explosions and mass casualty alerts. The deal stipulates a 60-day halt in hostilities during which Hezbollah fighters are expected to [retreat](#) from the Israel border while Israeli ground forces should withdraw from Lebanese territory. As for protest activity, the farmer inheritance tax [demonstrations](#) in the United Kingdom have ramped up from the previous week, with participants now blocking access to several major ports across the country. Structure fires have continued to decrease as many South American countries exit their winter season and thus are lessening their reliance on fire-hazardous heating systems.

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 New York, which together made up approximately one quarter (25 percent) of this week's nationwide total. Gun violence

across the United States overall decreased by 2 percent from the week prior. Police activity alerts also decreased by 2 percent, and the top contributing states were Texas and Pennsylvania. Structure fires did not increase or decrease from the previous week, and the top two states for this subtype were New York and Texas. Notably, school-related threats decreased by 17 percent, and general protest activity decreased by 52 percent from the previous week.

- > **What this means:** Of the top three subtypes (structure fires, gun violence, and police activity), none saw significant increases or decreases in alert numbers from the previous week, which may have been due to a combination of cooler weather and the upcoming Thanksgiving holiday, as many people take early vacations from work and school at this time. This would also explain the somewhat noteworthy decrease in school-related threats as well nationwide protest activity; this year the American Automobile Association estimated that the US would see a record number of 80 million [travelers](#) over the holidays, which is an increase of 1.7 million people compared with last year and 2 million more than in 2019. As temperatures are expected to drop over the weekend and snow begins to fall in several states, there is a larger chance of serious automobile accidents and travel delays in the next few days as well. Additionally, structure fires may see an increase as well, as the Thanksgiving holiday will likely witness cooking-related fires, and colder temperatures will increase the usage of fire-hazardous heating systems.

| 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%