



# **| Brief |**

## **The Underground Economist: Volume 5, Issue 14**

B-2025-07-18a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor,  
Ransomware

**July 18, 2025**

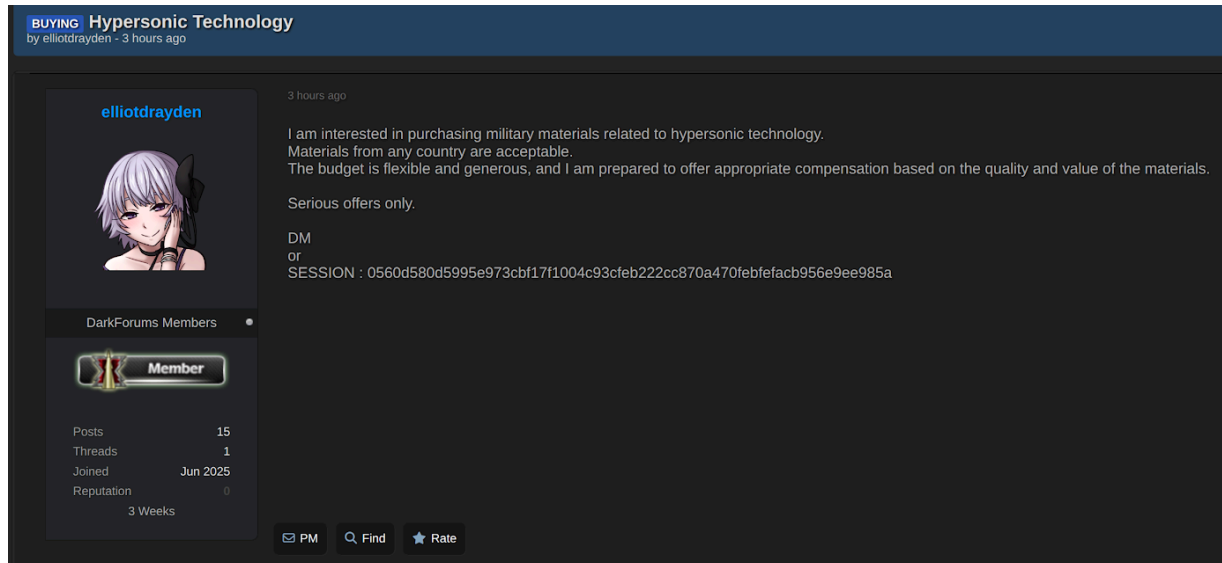
*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 2:00 PM (EDT) on July 18, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

# **Brief | The Underground Economist: Volume 5, Issue 14**

## **| Interest in and Alleged Access to Hypersonic Technology Information**

On July 15, 2025, an actor known as “elliotdrayden” posted on the deep web forum DarkForums expressing interest in purchasing military-related information associated with “hypersonic technology.” Elliotdrayden did not further specify the type of information they are seeking, which state military it should be associated with, or their intended subsequent exploitation. In response to the post, another actor known as “Kaught” claimed to have access to compromised data allegedly exfiltrated from the U.S. Department of Defense.

According to Kaught, the data was obtained on July 15, 2025, via the exploitation of a vulnerability (CVE-2025-0731) found within a Supervisory Control and Data Acquisition (SCADA) National Reconnaissance Office (NRO) satellite uplink associated with the U.S. National Security Agency (NSA). This network breach allegedly revealed hypersonic technology developed under Defense Advanced Research Projects Agency’s (DARPA) budget.

**elliotdrayden's DarkForums post**

*Source: ZeroFox Intelligence*

Kaught specified that acceptable payment for the alleged dataset would include USD 150,000 worth of either Bitcoin or Monero cryptocurrency or a “minimum” of 10 kilograms in gold bullion (equal to approximately USD 1.1 million, as of the writing of this report). Kaught further outlined the following payment delivery instructions:

- Digital delivery – AES-256 encrypted file transfer within 24 hours of receiving cryptocurrency payment.
- Physical delivery – Handover to take place at one of two “neutral locations”: either Panama City in July 2025 or Dubai in August 2025. Kaught also specified the need for biometric and retinal scan authentication, as well as private security escort, but no further detail was offered surrounding how this would take place.

As of this writing, it is unknown whether elliotdrayden and Kaught conversed further or if a sale occurred. However, there is a likely chance that Kaught’s advertisement is either fabricated or greatly exaggerated, owing to both the unlikely timing of the alleged NSA compromise and the unusual payment methods requested. If the offering is not legitimate, there is a roughly even chance that it is either associated with a law enforcement (LE) honeypot operation attempting to attract individuals seeking illicit information or a low-effort scam seeking to capitalize on a novel request for hypersonic

technology. This is made more likely by the overly polished language and heavy use of adjectives, which is not often observed within such posts.

## **| B-2 Strategic Bomber Blueprints and Phantom Windows Zero-day Vulnerability Advertised for Sale**

On July 14, 2025, a newly registered actor using the alias “user35” posted on the dark web forum Exploit, advertising the sale of “exclusive and classified” blueprints associated with the B-2 Spirit bomber, alongside a Windows remote code execution (RCE) zero-day vulnerability. The joint offering is advertised by user35 as the “ultimate Cyber/Stealth package.”


- The B-2 Spirit is a strategic long-range bomber operated exclusively by the U.S. Air Force. On June 22, 2025, the U.S. military attacked three Iranian nuclear sites utilizing B-2 Spirit aircraft under Operation Midnight Hammer.<sup>1</sup>

The actor claims this package (priced at USD 45,000) is the “most comprehensive non-government technical dossier” on the B-2 aircraft. The package allegedly includes the following documents:

- Radar absorbent natural (RAM) manufacturing guides
- Flight control system-related sequences, vulnerabilities, and algorithms
- Confidential structural engineering stress maps, modification guides, and other configurations
- Pilot debrief transcripts and undocumented procedures
- The “most advanced” Windows penetration tool, with several sophisticated capabilities

---


<sup>1</sup> <https://www.zerofox.com/intelligence/flash-report-tentative-israel-iran-ceasefire-established/>




### [EXCLUSIVE] B-2 Spirit Classified Blueprints + "PHANTOM" Windows 0Day RCE Exploit - The Ultimate Cyber/Stealth Package


By user35, 20 hours ago in [Other] - everything else


Start new topic







**user35**  
byte  
  
Paid registration  
2 posts  
Joined  
06/12/25 (ID: 201900)  
Activity  
выручология / malware  
Autogrant  
0


Posted 20 hours ago


 **B-2 "SPECTER" STEALTH BOMBER - FULL TECHNICAL PACKAGE**  
The most comprehensive non-governmental technical dossier ever assembled on the world's most advanced strategic bomber

 **Core Documentation Includes:**

-  **Radar-Absorbent Material (RAM) Manufacturing Bible**  
Exact chemical formulations including classified nanoparticle additives  
Layer application protocols with micron-level precision diagrams  
Thermal curing schedules for optimal stealth performance
-  **Flight Control System Master Key**  
Full firmware decompilation with annotated vulnerabilities  
Terrain-following radar source code with emergency override sequences  
Electronic warfare system algorithms (tested against S-400/S-500 systems)
-  **Structural Engineering Secrets**  
Airframe stress maps showing critical failure points under combat loads  
Weapon bay modification guides for "non-standard" payload configurations  
Fuel system vulnerabilities including emergency dump backdoors

 **Never-Before-Seen Additions:**  
Pilot debrief transcripts from stealth penetration tests  
Maintenance crew "black book" of undocumented procedures  
2023 avionics upgrade package with debug menus

 **"NIGHTFALL" WINDOWS ZERO-DAY EXPLOIT SUITE**  
The most advanced Windows penetration tool ever developed outside nation-state programs

 **Core Capabilities:**

### user35's Exploit post

Source: ZeroFox Intelligence

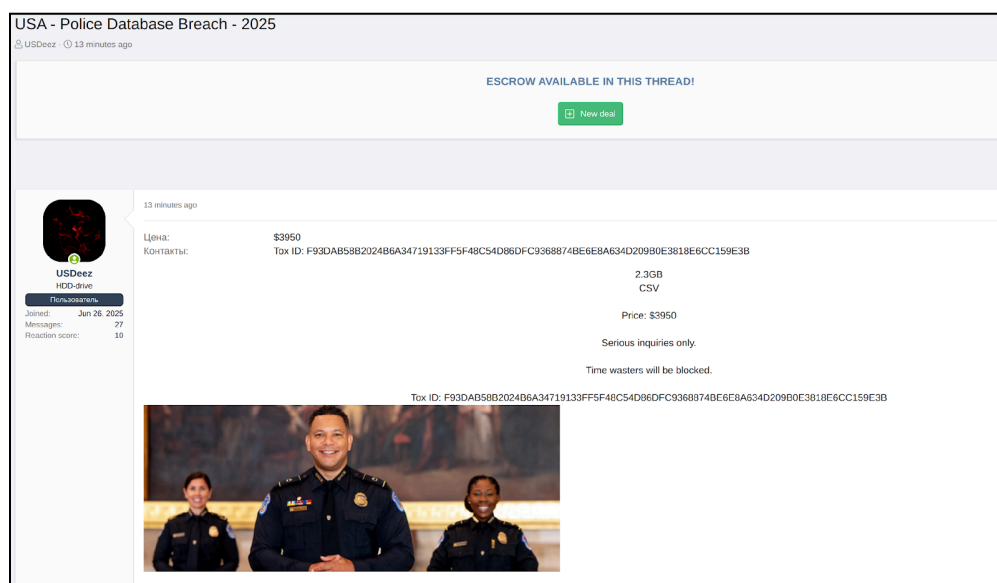
User35 demands preliminary escrow payment for the offering, which will allegedly grant a buyer access within 72 hours to a "demonstration video", a 120-page "technical sample pack", and third-party validation from auditors. No further information is offered specifying the nature of this validation or the entities referred to as auditors. User35 also claims potential buyers will undergo an unspecified verification process intended to prevent purchases being made by LE entities or researchers.

There is a likely chance User35's advertisement represents an attempt to scam users seeking classified military information by exploiting recent and extensive media coverage of the B-2 bomber and the U.S. military. This is made further likely by the actor's lack of a credible reputation within the forum, the lack of any sample information being offered, and the seemingly AI-generated post. If user35 is in fact in possession of the information claimed, the offering would most likely appeal to intelligence services associated with countries opposed to the United States, the West, or Israel, as well as various terrorist groups operating throughout the Middle-East.

## | Data Related to U.S. Police Advertised for Sale on Dark Web Forum

On July 9, 2025, an actor named “USDeez” posted in the Russian-speaking dark web forum XSS, advertising the sale of 2.3 gigabytes of data related to a U.S. police database for USD 3,950. USDeez claimed that the data is from 2025, though no further details were provided. The source of the data was not disclosed, but USDeez claims it is associated with an unspecified network breach.

- USDeez joined XSS in January 2025 and has established a positive reputation on the forum, which has likely stemmed from contributing to posts made by users and advertising other types of data for sale on the site.



### **USDeez's XSS post**

*Source: ZeroFox Intelligence*

USDeez shared approximately 100 lines of the data as a sample. The majority of the information comprises personally identifiable information (PII) seemingly associated with individuals employed by various U.S. government departments. Some of the fields include:

- Name and ZIP code
- Agency phone numbers

- Cell phone data
- Supervisors' cell phone numbers
- Supervisors' email addresses
- Supervisors' first and last names
- IP addresses

ZeroFox frequently observes advertisements posted in deep and dark web (DDW) forums for the sale of alleged access to data related to U.S. public entities.

- On June 11, 2025, the actor "shine" posted three times in the deep web forum DarkForums advertising network access to U.S. government institutions via RCE.
- Similarly, on May 19, 2025, shine posted in DarkForums advertising access to an unspecified U.S. government organization with an alleged annual revenue of USD 80 billion.

Obtaining data related to U.S. public entities is very likely to be perceived as potentially lucrative by malicious cyber actors seeking to conduct digital extortion or targeted social engineering campaigns. Further, the information would also likely appeal to actors inclined to doxx or physically target members of LE entities.

There is a likely chance that the data advertised by USDeez constitutes genuine PII. While much of the information offered within the sample is very likely publicly available, its pairing with more sensitive PII—such as supervisors' phone numbers, IP addresses, and working relationships—alludes to the compromise of U.S. police department networks.

As of the writing of this report, no comments or reactions have been observed within the thread; however, it is likely that any interested party would contact the seller directly via the private messaging platform Tox, as requested by USDeez.

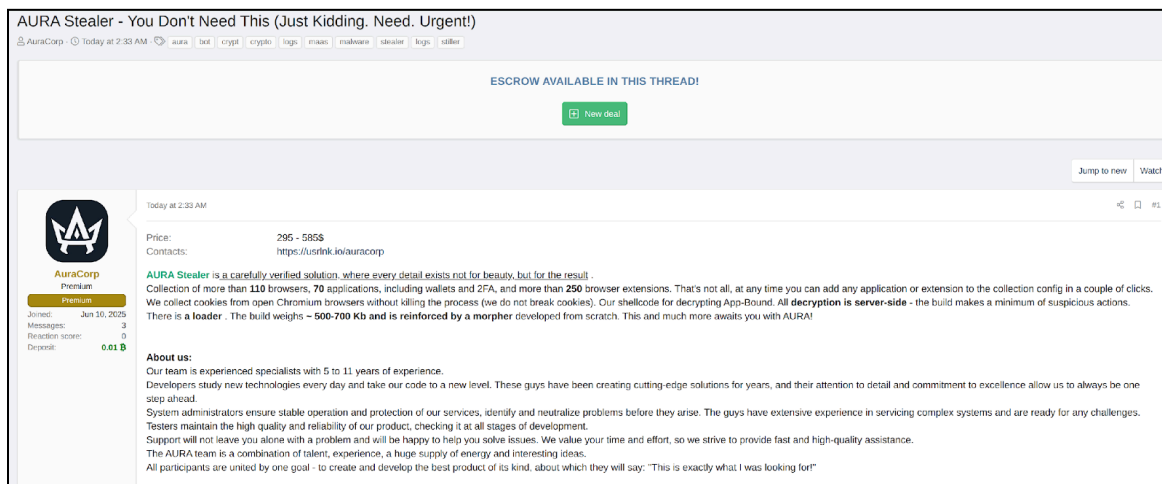
## **| New Stealer-as-a-Service AURA Advertised on XSS**

On July 7, 2025, the actor "AuraCorp" announced on the Russian-speaking dark web forum XSS a new Stealer-as-a-Service (SaaS) platform called "AURA". According to the advertisement, AURA can steal data from 110 different browsers, over 250 browser extensions, 70 applications—including cryptocurrency wallets and two-factor authentication (2FA) tools—and cookies from Chromium-based browsers. The post has



been receiving a considerable amount of interest, and ZeroFox has observed fellow XSS actors speculating that AURA developers are linked to the well-known Aurora Stealer.

- Aurora Stealer is a prominent infostealer malware that has been in use since 2022 and is designed to exfiltrate credentials, browser data, and cryptocurrency wallets from victims.



### **AuraCorp's XSS post (translated from Russian)**

*Source: ZeroFox Intelligence*

AuraCorp is offering two subscription plans for AURA SaaS: the basic plan for USD 295 per month and an advanced version for USD 585 per month.

- The basic plan includes one bulk upload of stolen data; searches by keyword, country, date and time; and selects specific browser extensions for infection. The plan allows for a single custom-configuration for specific data theft, incorporation of a label on the malware build, a customized malware build, and connection to a Telegram bot.
- The advanced version offers three bulk uploads, three additional configurations, five additional tags to a build and worker links, and a list of user agents. Moreover, it allows for the creation of five new builds and five Telegram bots, as well as access to more log-filtering options.

The speculation about the AURA developers' links to Aurora Stealer will almost certainly generate interest among potential threat actors seeking new infostealer malware. With



popular SaaS offerings like StealC and the “experienced” version of LummaC2 being priced at USD 200 and USD 500 per month, respectively,<sup>2</sup> AURA’s price point likely seeks to create a perception of a premium product; this is likely reflective of the advanced features available, even though users have to build their own list of targeted devices through phishing and other methods.

**Web:**  
At the entrance, you will be greeted by a panel built using the popular and beautiful Tabler web template. You will get an intuitive and pleasant interface that has already proven itself among many users. We believe that the modern design and well-thought-out structure of the panel will please you and create conditions for comfortable work. A few facts:

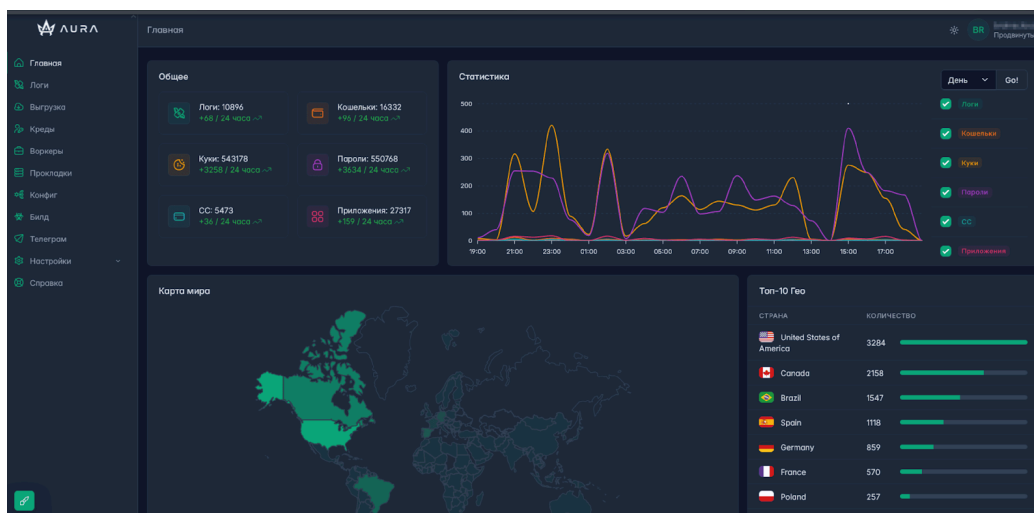
- The panel is fast. Database queries pass through a caching layer and occur almost instantly.
- Each user's data is securely protected by strict access policies.
- To maintain the database's performance, it is regularly optimized and cleaned.
- We use powerful servers, which ensures the speed of our systems and high uptime.
- In our panel you can customize the color scheme, choose a light or dark theme, font and much more to suit your taste.

**Build:**

- The build is written in C++ (NtAPI/WinAPI + CRT/STL). The build weight is ~500-700 Kb (different in each build after morphing), compressed by packers to 170-250 Kb.
- Linked statically, runs on the entire Win7 - Win11 line. No dependencies, works on clean systems.
- Parts of the code that are critical to speed or stealth are built on NtAPI, while less demanding ones are built on WinAPI.
- Imports are hidden, functions are obtained dynamically and cached in an encrypted hash table. Function addresses are not stored in plain text and are decrypted immediately before calling. The build contains only CRT imports and fake imports (changed during reassembly).
- The strings are encrypted and decrypted at runtime.
- Double trigger protection (dynamic mutex based on DGA principle).
- Configurable Sleep before startup.
- AntiVM/Sandbox. Standard checks of virtualized environment. Can be enabled or disabled in the panel.
- AntiDebug. Nasty anti-debugging methods tightly integrated with our technologies. Will make even seasoned reversers spit at the monitor. You can't disable anti-debugging in the panel.
- ApiHammering. Background noise to simulate legitimate activity and randomize runtime behavior. Random WinAPI calls and file system interactions (creating, writing, reading files) are scattered throughout the code that are not relevant to the task.
- Powerful grabber with flexible collection customization. The panel allows you to set the initial collection path, search masks, recursion level, file size limit, archive folder, and other parameters depending on the collection type.
- Very fast and compact Wildcard engine for searching files by masks from the config. When others offer search only by file extensions, we allow building more complex rules with different nesting levels (for example, `folder\folder\abc\def\*.txt`). And also relative paths with an exit from the initial directory to the level above (for example, `..folder\*.txt`), this is useful for collecting by process name, when the initial collection folder is unknown.
- The grabber has a built-in protection against collecting duplicates - the paths of the read files are cached in the hash table. In case of incorrect configuration of the config, you will not receive a log with duplicate files.
- When the grabber is running, nothing is dropped onto the disk, the archives are assembled in RAM. The log is transferred to the server in parts, even if the build catches a runtime detection, some of the data will already be on the server and you will not lose the entire log.
- All traffic between the build and C2 is encrypted with AES-256 and goes via the HTTPS protocol (its own wrapper over WinHTTP).
- In case of connection loss, the build cyclically waits for an internet connection, after which it continues from where it stopped. In case of problems with the laying, it selects a random working one and continues sending.
- Protection against leaking of unencrypted file. If you run the build without crypt, a captcha window will appear. After entering the captcha, the build will work in the normal mode. After crypt/packing, the captcha does not appear.
- **Build does not knock in CIS countries (former USSR)! Checking the layout and language of the system + checking the IP on the server.**

## Features of AURA SaaS (machine-translated from Russian)

Source: ZeroFox Intelligence



## AURA’s user interface posted on XSS

Source: ZeroFox Intelligence

<sup>2</sup> <https://www.zerofox.com/blog/an-introduction-to-stealer-logs/>

## **| Recommendations**

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

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

	<b>Red</b>	<b>Amber</b>
<b>WHEN SHOULD IT BE USED?</b>	<b>Sources may use</b> <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> <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.
<b>HOW MAY IT BE SHARED?</b>	<b>Recipients may NOT share</b> <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> <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. <b>Note that</b> <b>TLP:AMBER+STRICT</b> restricts sharing to the organization only.
	<b>Green</b>	<b>Clear</b>
<b>WHEN SHOULD IT BE USED?</b>	<b>Sources may use</b> <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> <b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
<b>HOW MAY IT BE SHARED?</b>	<b>Recipients may share</b> <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> <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%