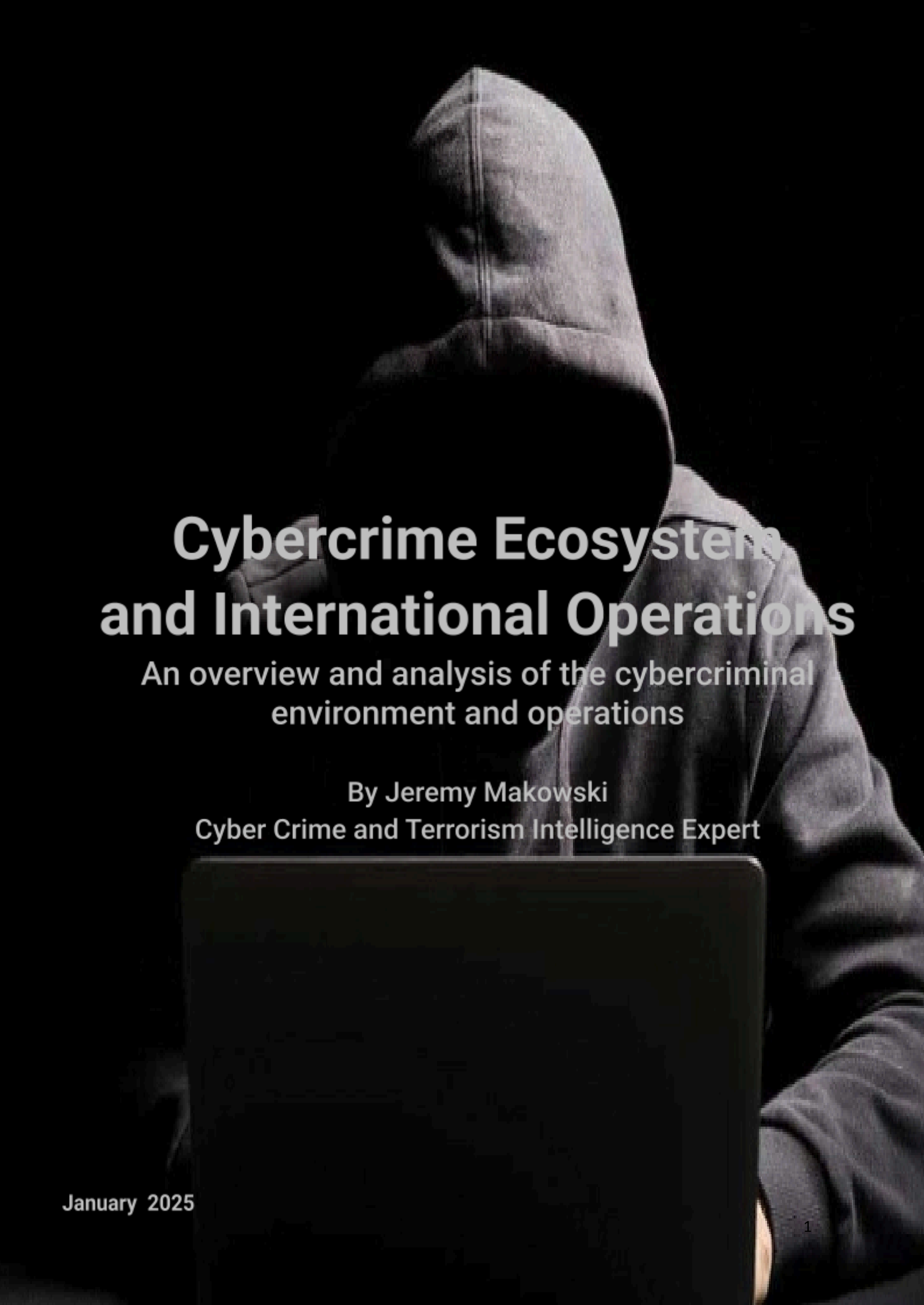


Cybercrime Ecosystem and International Operations

An overview and analysis of the cybercriminal environment and operations

By Jeremy Makowski
Cyber Crime and Terrorism Intelligence Expert

January 2025

Table of Contents

Executive Summary 3
1. Cybercrime Ecosystem 4
    1.1 Cyberspace Structure 4
    1.2 Cybercriminal Platforms 6
    1.3 Cybercrime Organizational Structure: 16
2. Cybercriminal's Modus Operandi and Operations 19
    2.1 Open Source Intelligence 19
    2.2 Social Engineering 21
    2.3 Malware and Exploits 29
        2.3.1 Ransomware 29
        2.3.2 Data Collection Malware 31
        2.3.3 Exploits and Vulnerabilities 34
    2.4 Generative Artificial Intelligence and Deepfake Technology 37
    2.5 Fraud and Money Laundering 40
    2.6 Network Access and Data Breach 42
3. Cybercriminals' Psychology 44
        3.1 Motivations 44
        3.2 Way of Thinking and Cognitive Bias 44
        3.3 Behavioral Characteristics 44
        3.4 Psychological Profiles 45
4. Geographical Distribution of Cybercrime 47
    4.1 Western Europe and North American Countries 47
    4.2 Eastern Europe Countries 48
    4.3 Middle East and African Countries 50
    4.4 South American Countries 51
    4.5 Asian Countries 52
5. Conclusion 53
6. About The Author 54

Executive Summary

Due to its profound financial and security impacts, Cybercrime stands out as one of the most significant cyber threats states face. It affects every sector of activity, fuels a shadow economy, and imposes heavy economic burdens. Cybercrime continues to grow as a major threat to the global economy. According to Cybersecurity Ventures, it was projected to cost the world USD 9.5 trillion in 2024, with estimates rising to $10.5 trillion by 2025. This alarming growth stems primarily from two factors. The first is the rapid expansion of cyberspace, driven by an ever-increasing number of computers, servers, and connected devices, which generate vast amounts of data to manage daily. The second factor is the accelerated digitization of financial transactions and applications, including platforms like PayPal, Revolut, Google Wallet, and cryptocurrencies such as Bitcoin, Ethereum, and Tether.

While cybersecurity solutions from major companies like Microsoft, Cisco, Check Point, Palo Alto, Symantec, and others help mitigate risks and anticipate certain cyberattacks, they fall short of fully avoiding and eliminating threats, widely considered impossible. No matter how advanced, every system has vulnerabilities, and cybercriminals have exploited this reality for decades. As defense technologies evolve, so too do the tactics of cybercriminals, who continually adapt their modus operandi to infiltrate government and private sector networks and systems. Moreover, they increasingly capitalize on unpatched security flaws and zero-day exploits. The difficulty in combating cybercrime lies in anticipating trends and managing the amount of crimes committed. Despite considerable combat work undertaken by governments and much greater international cooperation with cyber entities within agencies such as Interpol, Europol, ENISA, UN, and NATO, this fight remains complex and difficult to counter daily. While many publications focus on the technical intricacies of cyberattacks, they often neglect the strategic and organizational aspects of cybercriminal operations. This paper sheds light on how cybercriminals think, plan, and execute their activities to maximize profits.

1. Cybercrime Ecosystem

1.1 Cyberspace Structure

Gripping cyberspace's foundational structure is crucial to better understanding the cybercrime ecosystem. Broadly, cyberspace is categorized into three distinct layers: the Surface Web, the Deep Web, and the Darknet.



The Surface Web encompasses the portion of the Internet that is easily accessible to the public using standard web browsers and popular search engines like Google Chrome, Internet Explorer, or Firefox. This layer provides access to widely used platforms and open resources like Facebook, YouTube, Instagram, and Gmail. Various threat actors operate within the Surface Web, leveraging its accessibility to pursue diverse objectives.

The Deep Web refers to the largest part of the internet not indexed by regular search engines such as Google Chrome. Around 90% of the sources on the internet need to be indexed by Google. Indeed, many web pages are considered to belong to the Deep Web as they do not use common top-level domains (TLDs), like .com, .co, and .org, and are not indexed by regular search engines. The sources on the deep web are usually services that require restricted access, such as online banking, mail servers, or private social media pages. From the infrastructure perspective, deep web websites are reachable by regular URLs or IP addresses; however, they can require access to the public website pages through secure access (user/password).

The Darknet refers to underground networks overlayed on the internet. It is reachable with the help of a specific browser or software. The Onion Router (Tor) and The Invisible Internet Project (I2P) are the most popular darknet networks. These two browsers allow access to underground websites, usually indexed by repositories and search engines. The main goal of these networks is to remain anonymous and keep privacy with the help of advanced encryption systems.

TOR network, which is the most active and popular, is a decentralized network operating on the principle of volunteering. A user wishing to join the TOR network as an active actor and not just a simple user needs to implement a script on his machine that allows him to turn it into one of the many nodes of the network. All the New York traffic between nodes is encrypted, and each node only knows the destination of the next node and not the complete path to the final server (Figure 1).

The TOR network comprises three types of nodes: entry, middle, and exit. These nodes act as relays like routers on traditional Internet networks. They allow data to be transferred via a predefined path that changes randomly each time a user makes a new request (Figure 2).

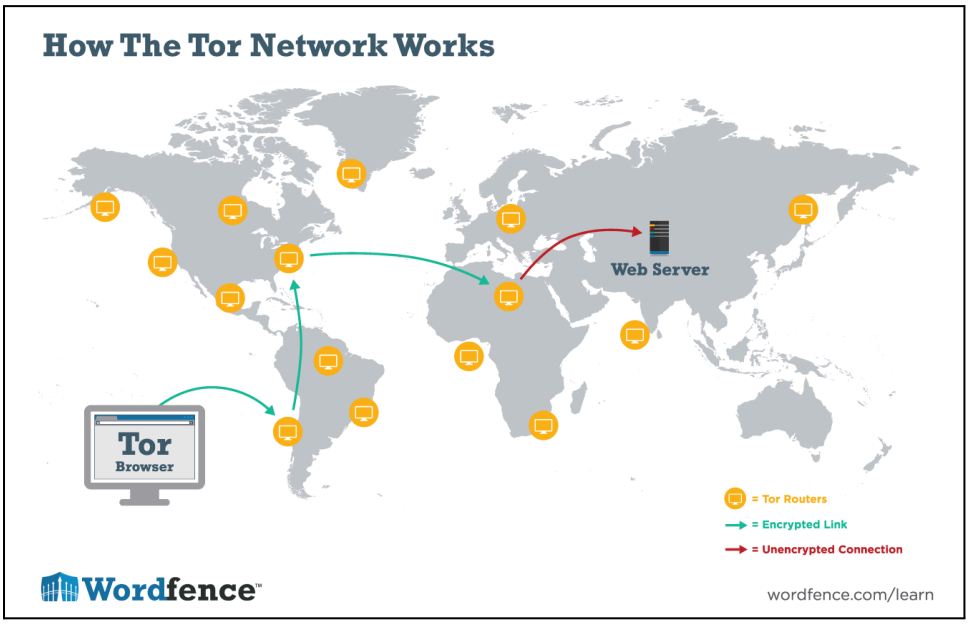


Figure 1 - ToR Network World Map

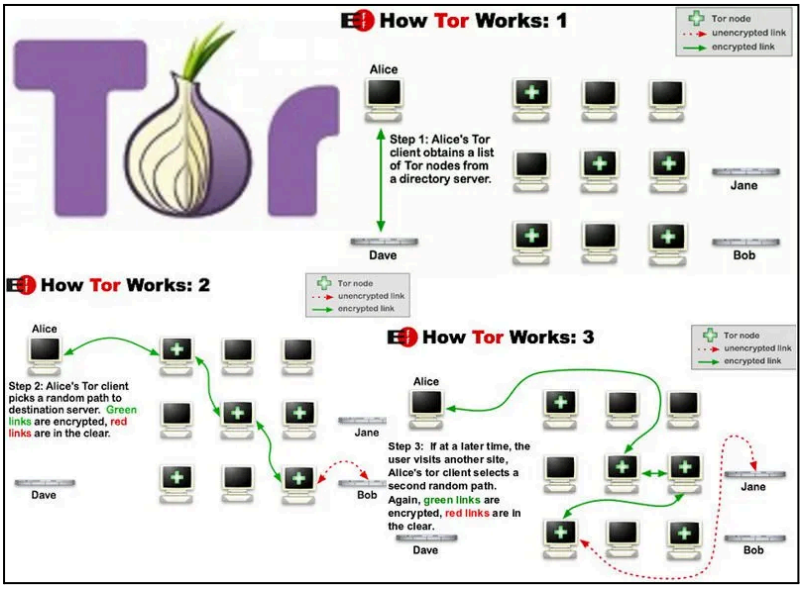


Figure 2 - TOR network structure

The I2P network itself is also made up of a set of nodes, called "routers", connected by one-way inbound and outbound virtual paths called "tunnels" (as shown on the tunnel routing page). Each router is uniquely identified by a cryptographic RouterIdentity, which is usually durable.

Routers exchange messages using established transport protocols such as TCP and UDP. Client applications are assigned their cryptographic identifiers, called "destinations, " allowing them to send and receive messages. These clients can connect to any router and request a temporary allocation, or "lease," of tunnels, which facilitate the transmission of messages across the network (Figure 3).

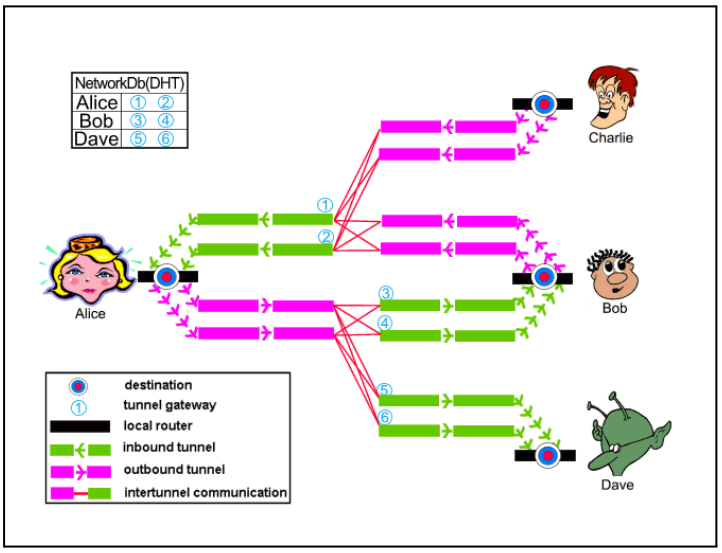


Figure 3 - I2P network structure

1.2 Cybercriminal Platforms

The cybercrime ecosystem is vast and varied. Cybercriminals usually operate in multiple playgrounds depending on their activities and modus operandi. Several criminal platforms exist, including forums, auto-selling marketplaces, black markets, and crypto messaging apps. These online crime platforms are generally easily accessible. However, some require privileged access, which can be obtained by payment or contact.

1.2.1 Forums

Cybercriminal forums are arguably among the most important platforms in terms of criminal activity. They number in the hundreds. However, not all have the same level of activity and interest in criminal activities. In cyberspace, there are many cybercriminal forums in all languages for all types of illegal activities hosted on the web and the dark web. In this cybercriminal jungle, we can roughly classify them into three main categories: the so-called technical forums with threat actors offering malware and exploits for sale, forums for exchanging and selling hacked networks and databases, and financial fraud and carding forums. Cybercriminal forums are arguably among the most important platforms for criminal activity.

They number in the hundreds. However, not everyone has the same training and interest in criminal activities. In cyberspace, there are many cybercriminal forums in all languages and for all types of illegal activities hosted on the web and the dark web (Figure 4). In this cybercriminal jungle, they can be roughly classified into three main categories, among which are the so-called technical forums with threat actors offering malware and exploits for sale, forums for the exchange and sale of network access and hacked databases, and finally, financial fraud and carding forums (Figures 5,, 6, and 7). These forums are usually built with different sections like malware, databases, fraud, market, etc. Their accession depends on the forum policy. Some content is accessible to all, while others require prior registration using a nickname and an email address. In addition, some more exclusive forums (generally with more exciting content) are only accessible by payment or sometimes even by internal contact. These rules usually help to filter user registrations to reduce the number of script kiddies and allow people to be more likely to be active in cybercriminal operations.



Figure 4 - Linke Base worldwide cybercriminal forums repository

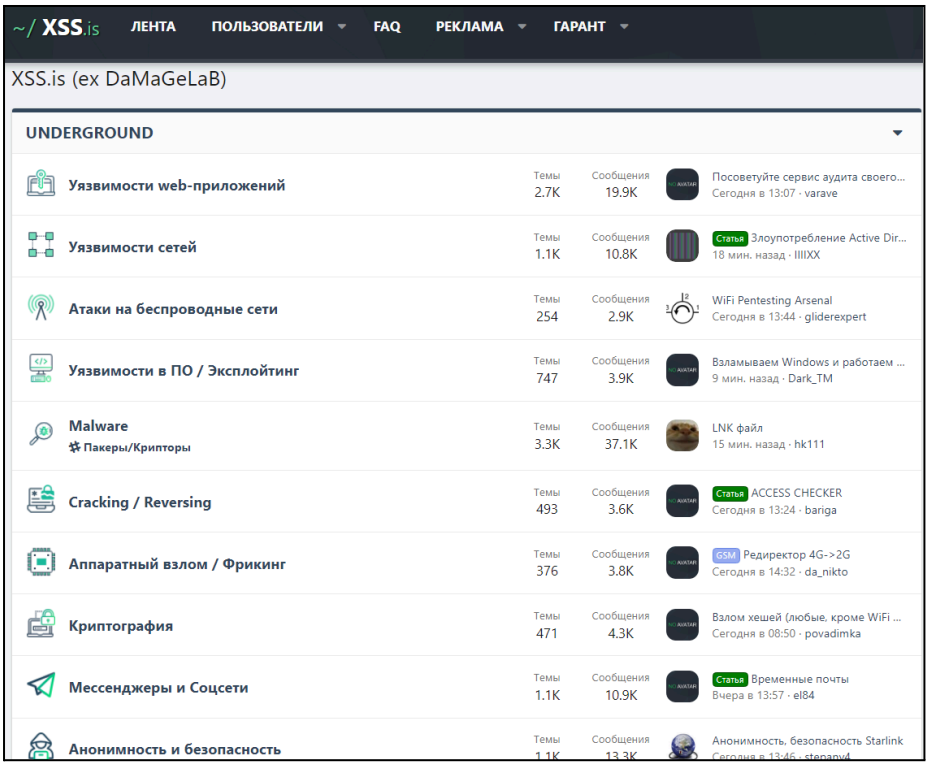


Figure 5 - One of the most popular Russian-speaking technical hacking forums (XSS.IS)

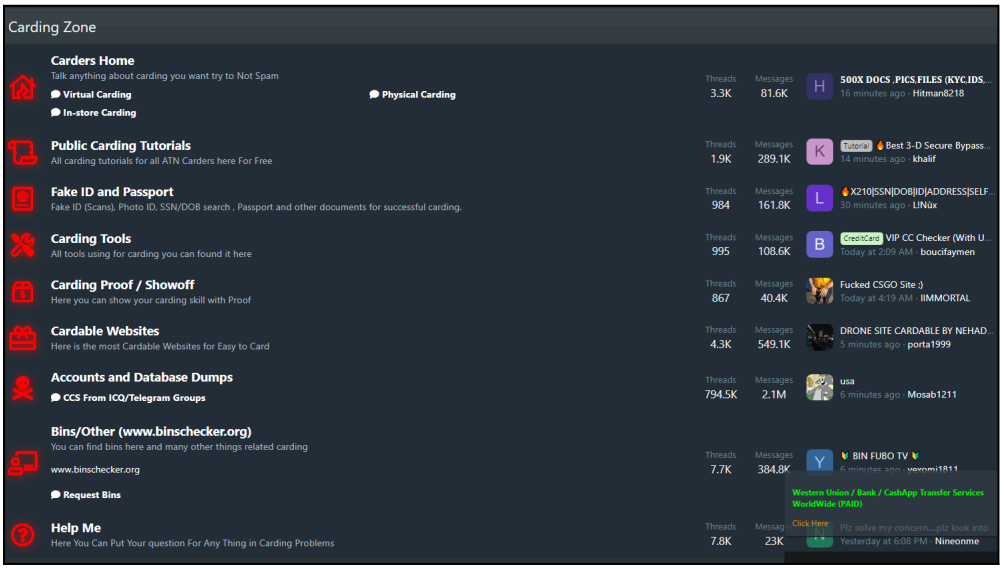


Figure 6 - A well-known English-speaking carding forum (Altenen Carding)

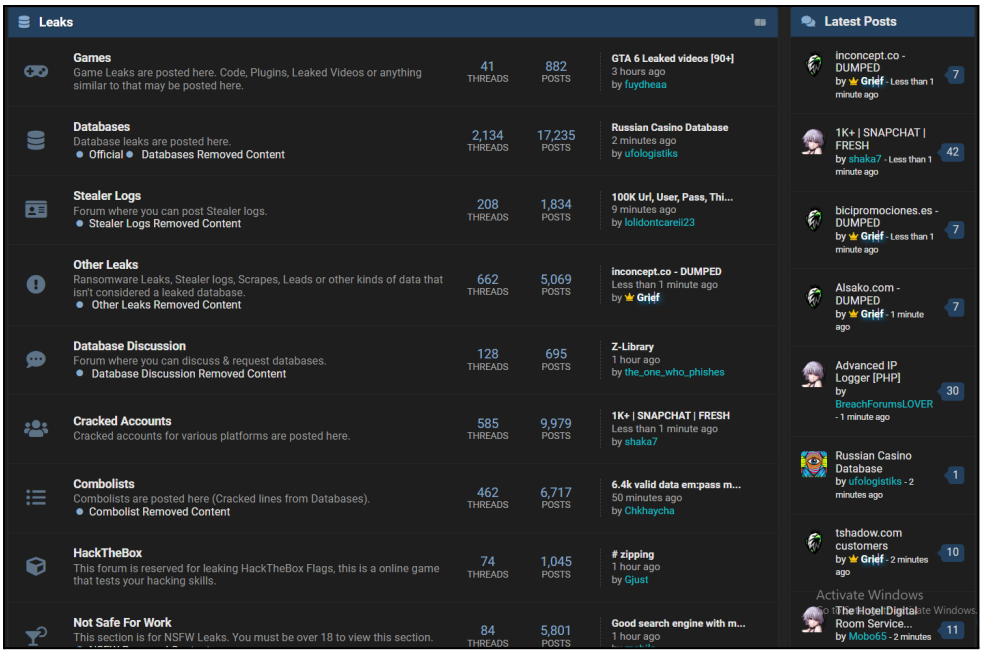


Figure 7 - One of the most popular data leak forums replacing raidforums (breachforums)

The management of cybercrime forums is generally based on a hierarchical structure with actors among the following:

- **Administrator** (aka admin): He manages the operations and administers the forum (Figure 8).
- **Moderator** (aka mod): There are usually several, depending on the forum size. They generally manage one of the multiple criminal sections of the forum (malware, databases, fraud...) (Figure 9).
- **VIP user:** This type of user usually has access to more sections on the forum (with more exclusive content) by paying fees (Figure 10).
- **User**: Refer to the majority of people registering on the forum.

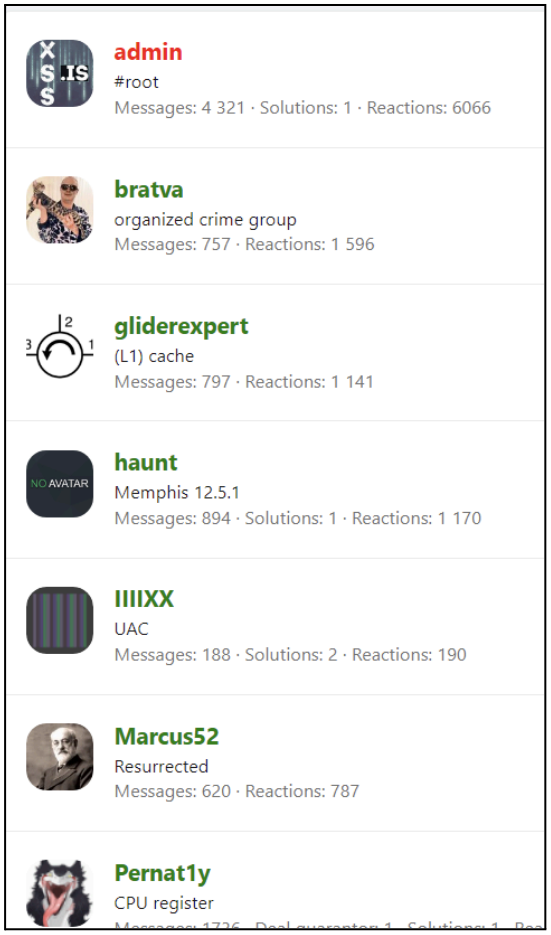


Figure 8 - List of Admin and moderators on a Russian hacking forum (xss.is)



Figure 9 - Moderator recruitment post on a carding forum (Altenen)



Figure 10 - VIP user packages for sale on a hacking forum (breachforums)

1.2.2 Automatic Selling Marketplace

The Automatic Selling Marketplace is an online platform designed for the automated trading of fraudulent digital assets. These marketplaces are typically operated by cybercriminal groups managing botnets comprising tens of thousands of infected devices. They enable cybercriminals to purchase stolen digital assets with minimal or no interaction with the platform administrators. These platforms generally follow a similar structure. A comprehensive database stores vast quantities of stolen digital assets, while a control panel allows users to search for specific criteria, such as credit card type, issuing bank, or country. The assets sold on these platforms often include credit card numbers, bank account details, and application logins. Users usually deposit cryptocurrency into their accounts to make a purchase, ensuring they maintain a positive balance. Once an asset is selected, the transaction is processed automatically, and the corresponding credit is deducted from the user's account (refer to Figures 11, 12, and 13).

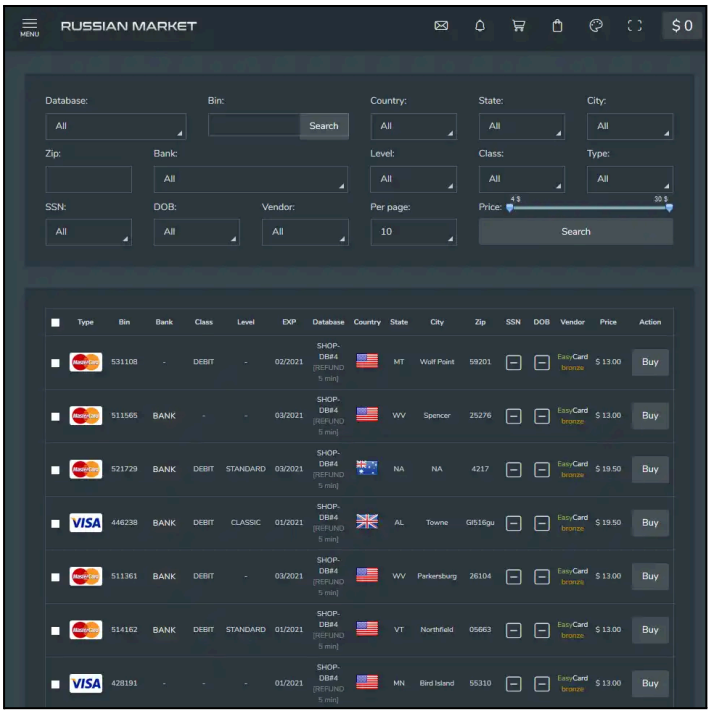


Figure 11 - Automatic Selling Credit Cards Russian Market

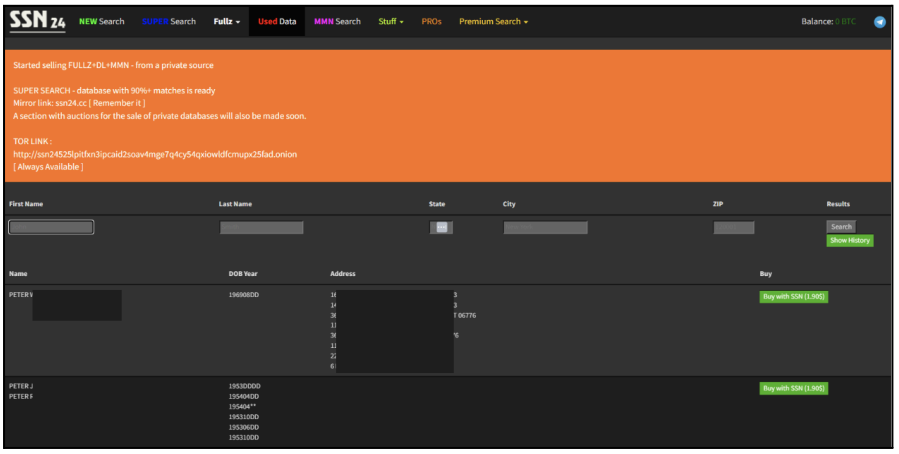


Figure 12 - Automatic selling PII market

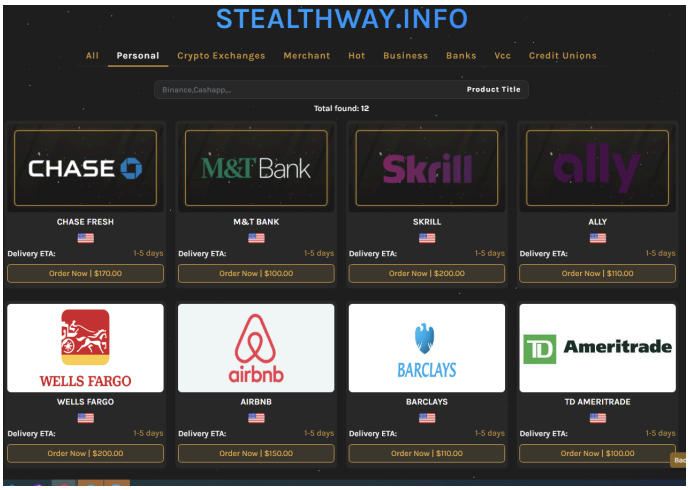


Figure 13 - Automatic selling market Bank accounts

1.2.3 Black Markets

Underground markets offer cybercriminals the opportunity to sell illegal products. Each market, depending on its mode of operation, allows sellers to have a store within the market or to sell through it. Sellers usually offer for sale different types of drugs, weapons, credit cards, banking credentials, exploit kits, malware, personal identity information, medicines, weapons, fake currency, and documents. Usually, each seller has a profile with details of the products they are selling and, most of the time, their PGP encryption key so buyers can send them private messages and encrypt the marketplace. Additionally, typically, to purchase items, users must transfer money in cryptocurrency to a wallet. Finally, generally, sellers can be evaluated based on their quality and service. However, it is essential to understand that some sellers open multiple accounts and play with their avatars by writing positive reviews to increase their reputation. It is essential to understand that there are also many scammers in these markets and that purchased items do not always exist (Figures 14, 15, and 16).

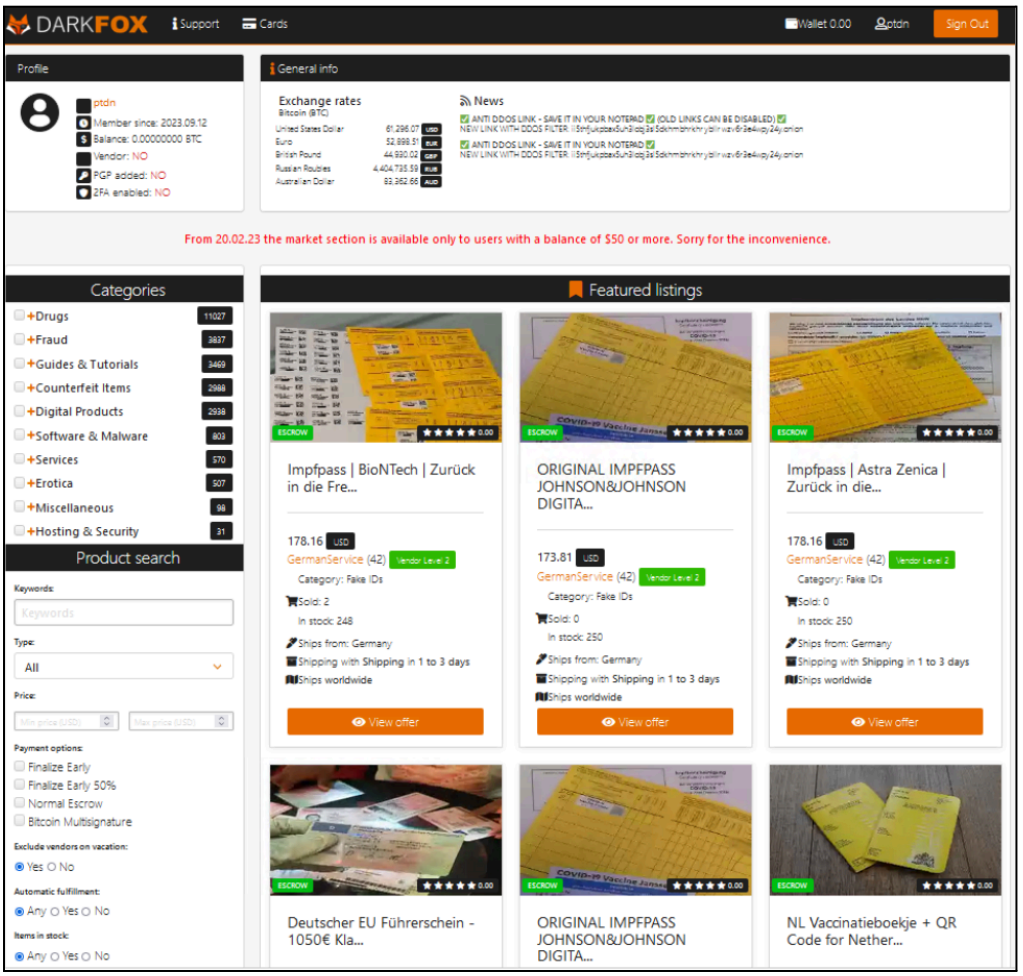


Figure 14 - Example of a darknet criminal market (Source: Darkfox)

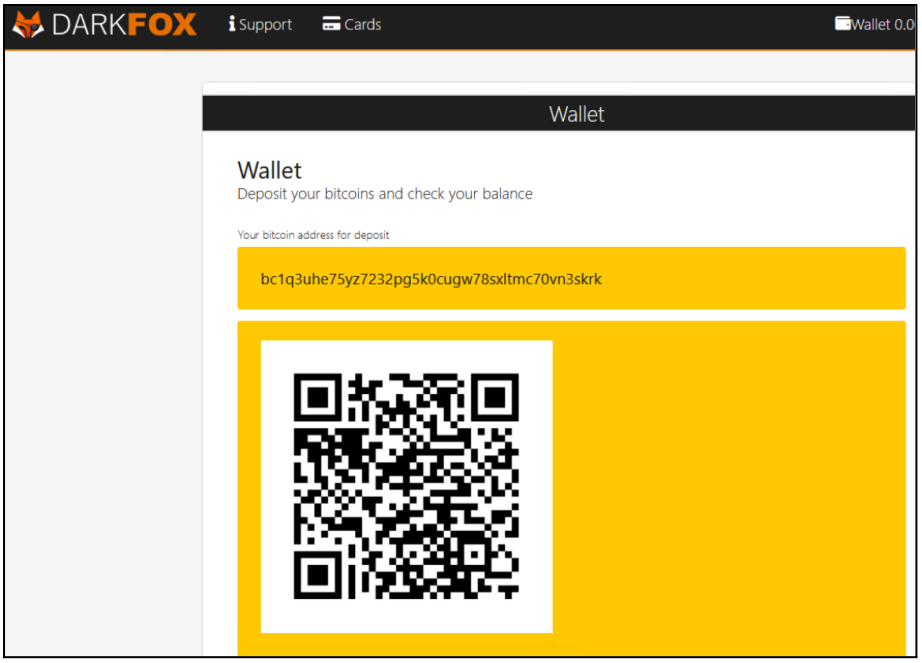


Figure 15 - A QR code on a darknet criminal market wallet to transfer cryptocurrencies (Source: Darkfox)

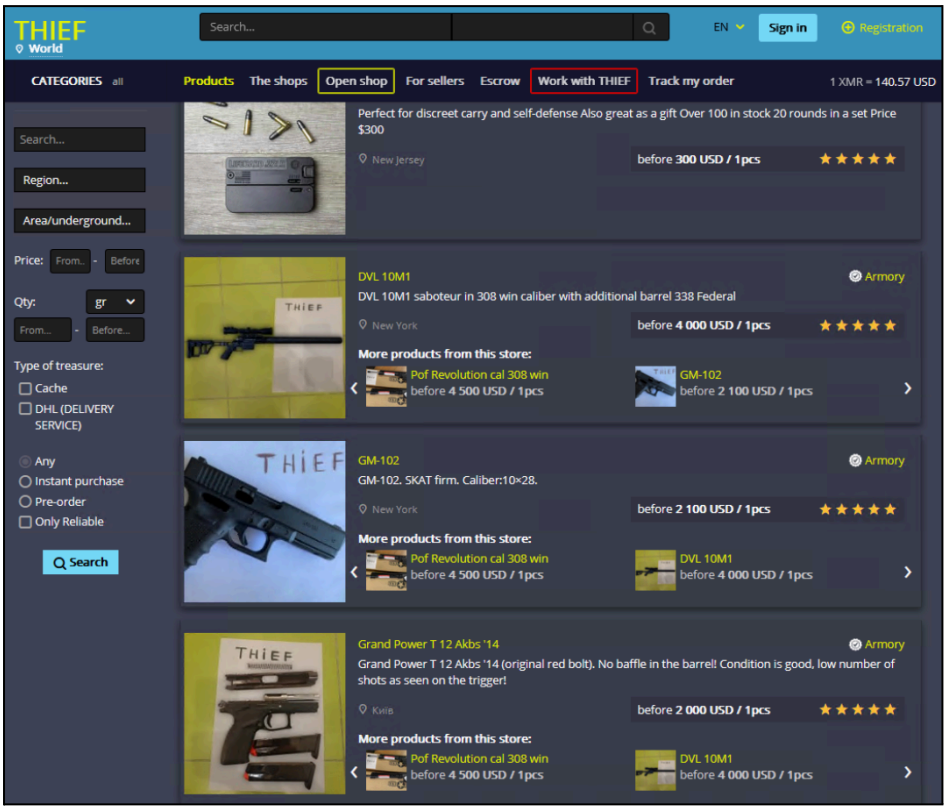


Figure 16 - Example of a darknet criminal weapons market (Source: Thief)

1.2.4 Encrypted Messaging Applications

For many years, encrypted messaging apps have become essential platforms for cybercriminals. From WhatsApp to Telegram, WeChat, TOX, Signal, Threema, or Jabber, these platforms allow cybercriminals to communicate with each other, sell illegal items, and create groups. They are an extension of the classic darknet (TOR or I2P) because they are easier to use and designed for smartphones, making them more flexible. Of all these applications,

Telegram has gained the most popularity among cybercriminals over the past decade. Although its servers are spread across the globe, Telegram's development team is based in the United Arab Emirates, the parent company, Telegram Group Inc., is registered in the British Virgin Islands, and the legal representative for data protection law is Telegram U.K. Holdings Ltd, a company based in the United Kingdom. Its popularity can be attributed to several factors. The application can be used on smartphones and computers. The application provides an end-to-end encryption service and hides the phone number used in the application to delete messages (Figures 17 and 18). This application allows features such as secret chat mode to send secure messages with an automatic deletion feature after a few seconds or minutes. Additionally, Telegram allows the creation of different groups and channels malicious actors use to promote and sell illegal items or services, distribute hacked databases, and recruit people for illegal activities (Figure 19).

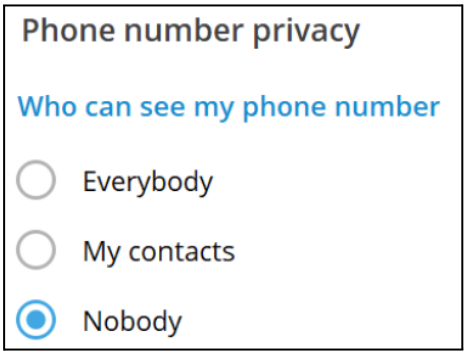


Figure 17 - Telegram phone number privacy settings

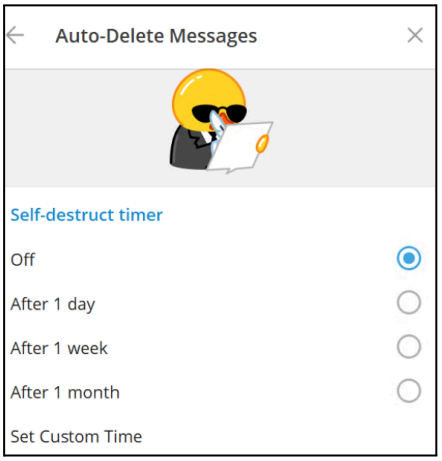


Figure 18 - Telegram Auto-Delete Messages settings

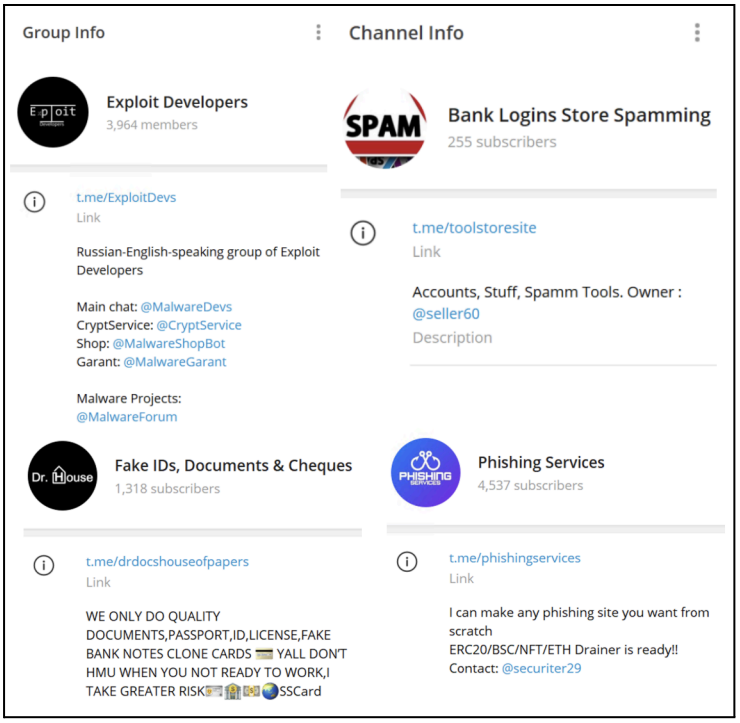


Figure 19- Examples of different Telegram groups offering illegal items or services

1.3 Cybercrime Organizational Structure:

Like the business world, cybercriminal networks often operate with a clear organizational structure, defined roles, and a chain of command. At the top of the hierarchy is usually a leader or network manager responsible for planning and orchestrating cyberattacks, fraud, or trafficking. This leader ensures all members understand their role and maintains effective organizational communication. Cybercriminal networks are, therefore, well organized, which generally allows them to carry out large-scale operations generating large profits. While the goals can vary, from cyberattacks to fraud or arms trafficking, the fundamental structure of cybercrime remains largely consistent. Specific roles and functions may differ depending on the criminal domain, but generally speaking, the typical structure is as follows:

Leadership and Strategic Planners

- **Roles**: Organization leaders, strategists, and financiers.
- **Responsibilities:**
    - Setting goals and targets for the organization.
    - Funding operations, often through investments in tools or services.
    - Negotiating partnerships or alliances with other criminal groups.
    - Maintaining high-level anonymity to evade law enforcement.

Developers and Technical Specialists

- **Roles:** Software developers, malware creators, and tool engineers.
- **Responsibilities:**
    - Creating malware (e.g., ransomware, trojans, spyware).
    - Designing hacking tools, exploits, and frameworks.
    - Updating and maintaining systems to bypass security measures.
    - Innovating to keep up with cybersecurity defenses.

Cyber Operators (Hackers)

- **Roles:** Hackers, penetration testers, and system operators.
- **Responsibilities:**
    - Executing attacks, such as phishing campaigns, system intrusions, and data breaches.
    - Gaining unauthorized access to networks and systems.
    - Managing botnets or other compromised systems.

Analysts and Data Handlers

- **Roles:** Data miners, analysts, and data brokers.
- **Responsibilities:**
    - Sorting and analyzing stolen data.
    - Identifying valuable assets, such as credit card details or intellectual property.
    - Packaging and selling stolen information on the dark web.

Money Launderers

- **Roles:** Financial operatives, "money mules," and cryptocurrency experts.
- **Responsibilities:**
    - Moving and converting illicit earnings to legitimate funds.
    - Using cryptocurrencies, shell companies, or online payment systems to obscure transactions.
    - Establishing complex financial networks to avoid detection.

Recruiters

- **Roles:** Talent scouts, social engineers, and human resource specialists.
- **Responsibilities:**
    - Recruiting skilled individuals for various roles.
    - Targeting potential operatives through forums, dark web platforms, or even legitimate job postings.
    - Maintaining connections with freelancers or smaller criminal groups.

Affiliates and Partners

- **Roles:** Contracted operators or external service providers.
- **Responsibilities:**
    - Participating in "as-a-service" operations, such as Ransomware-as-a-Service (RaaS).
    - Renting out infrastructure (e.g., bulletproof hosting or botnets).
    - Collaborating with other groups for large-scale operations.

Technical and Support Staff

- **Roles:** IT support, logistics, and translators.
- **Responsibilities:**
    - Providing technical support for tools or operations.
    - Managing communications and logistics.

2. Cybercriminal's Modus Operandi and Operations

2.1 Open Source Intelligence

Open Source Intelligence (OSINT) has been a powerful tool for cybercriminals for many years. The vast majority of people today have what could be called an online digital footprint corresponding to various digital assets such as telephone numbers, email addresses, physical addresses, IP addresses, public records, and other data posted online voluntarily or not. These digital assets are a real gold mine for many cybercriminals who exploit them for criminal and financial purposes.

Today, it is very easy to find many free OSINT tools on the Internet that collect and identify a certain amount of data related to individuals, IT infrastructure and networks, or an organization. Among the most popular OSINT tools used by cybercriminals in their operations are Shodan, Maltego, Contactrout, Rocketreach, TheHarvester, OSINT Framework, SpiderFoot, Google Dorks, Recon-ng, Censys, WHOIS Lookup, Builtwith, DNSDumpster, Have I Been Pwned, FOCA, and Nmap (Figure 20, 21,22, and 23).

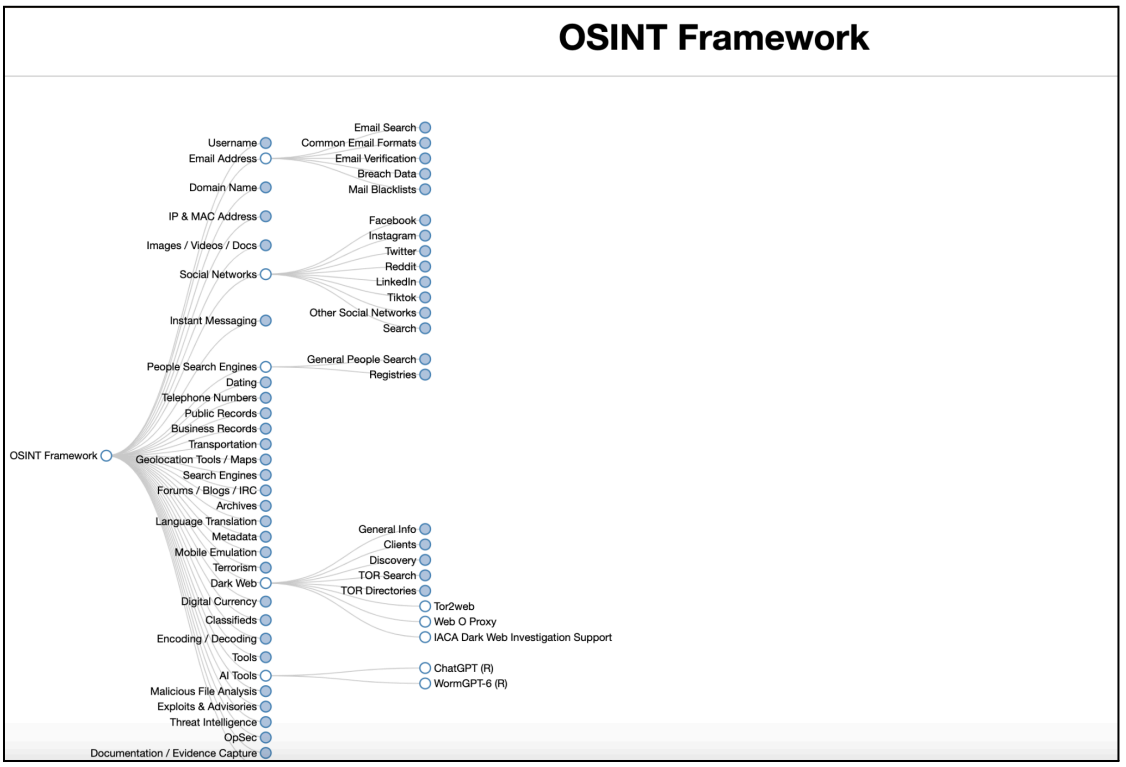


Figure 20 - OSINT Framework repository

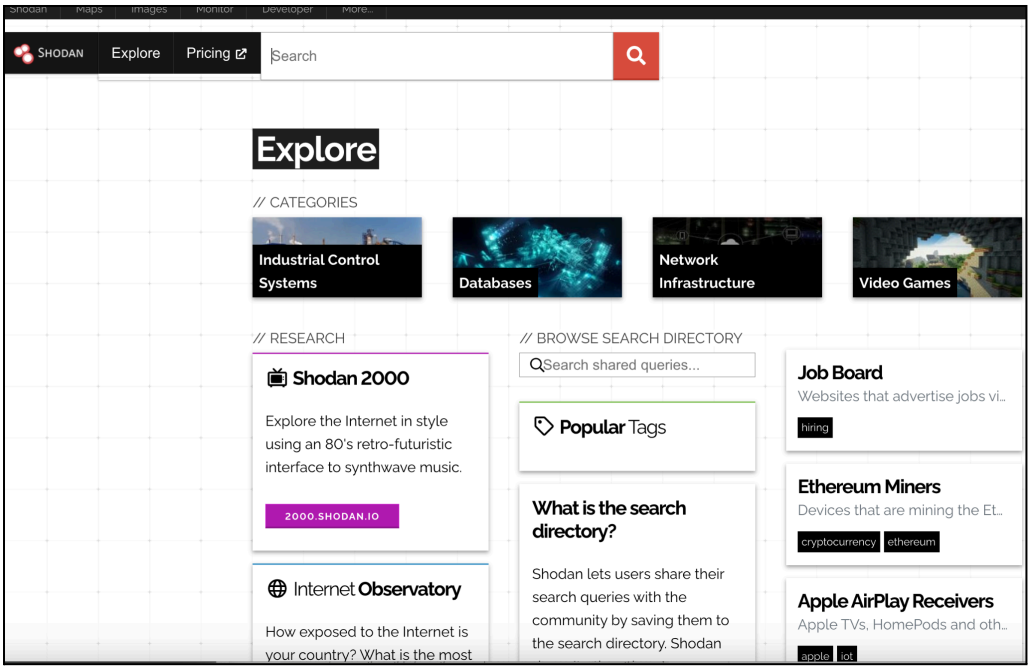


Figure 21 - Shodan IoT search engine

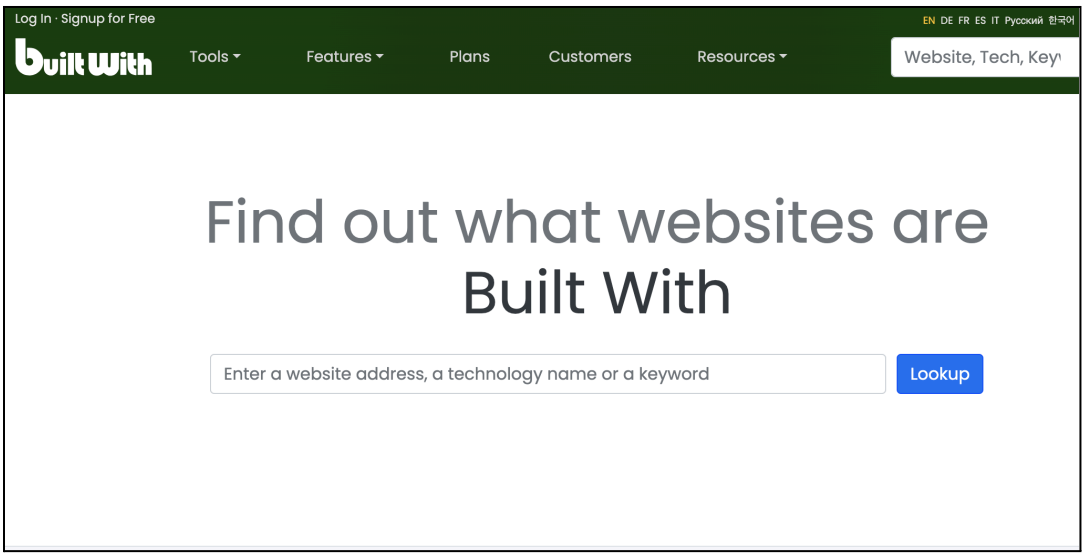


Figure 22 - Built with technology discovery

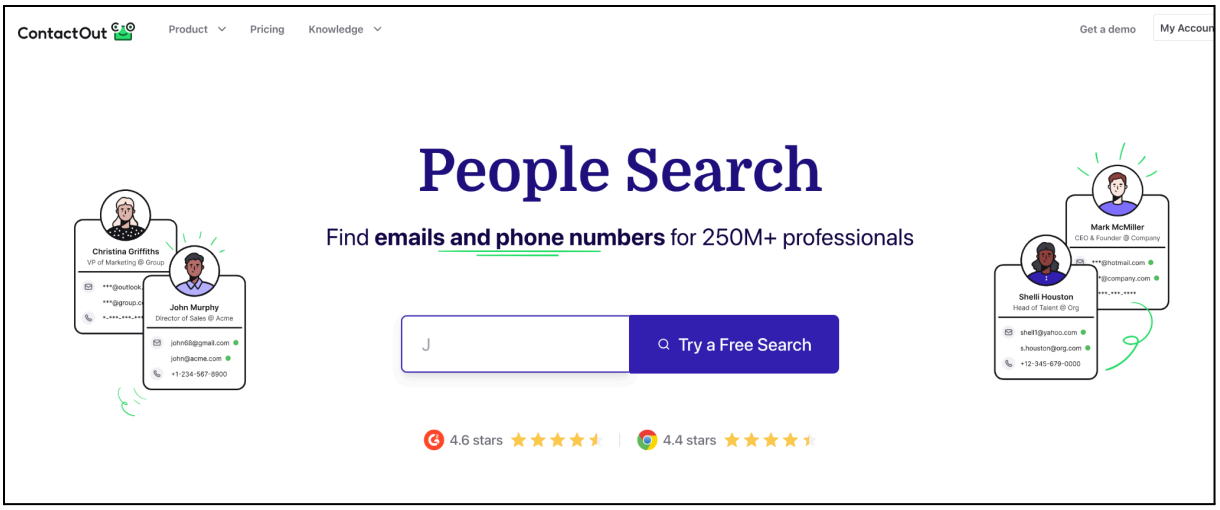


Figure 23 - Contactout people search engine

These tools allow cybercriminals to operate social engineering and phishing campaigns to collect more lucrative personal and financial information.

2.2 Social Engineering

Social engineering is one of threat actors' most well-known techniques to exploit human vulnerabilities. It refers to a wide range of malicious activities carried out through human interactions, including using psychological manipulation to trick users into making security errors or disclosing sensitive information. Social engineering attacks usually involve the following stages:

Collection: This first step typically involves collecting strategic and technical information about the target, such as key people, potential entry points, and security weaknesses.

Approach: This first step involves establishing a voice or written contact with the victim and building a trusted relationship.

Manipulation: This step is a logical continuation of the previous one. Once the trusted relationship has been established and the victim's weaknesses have been detected, the threat actor can psychologically manipulate his victim to obtain what he wishes to obtain from him.

Disengagement: This last step implies that once the threat actor has obtained the information or actions carried out by the victim in his favor, he stops being in touch with the victim in the most natural way possible, depending on the context and the cover story created.

Psychological manipulation is the key to social engineering success. To carry out their attacks, the most experienced threat actors often study human behavior in cyberspace. They exploit human weaknesses by relying, among other things, on the victims' lack of confidence and their poor or weak knowledge of the cyber environment. Indeed, in the same way that some people feel vulnerable on board a plane because they do not control the environment, the same phenomenon can be observed in cyberspace. Cyberspace is a vast ocean of devices, connections, systems, applications, and actors that is difficult for many people to understand and control. Suppose that humans have more or less succeeded in getting used to cyberspace and its codes (websites, applications, QR codes, 2FA, cookies, etc…); nonetheless, they need to be better informed of the risks and threats incurred. This phenomenon is even more marked among seniors who have not been able to adapt to this new world. Psychological manipulation of the victim can be carried out based on the following principles.

Emotions: Emotional manipulation generally gives the threat actor a strategic advantage when interacting with his victim. When in a heightened emotional state, the victim is much more likely to take irrational or risky actions without realizing it. Threat actors generally use the following emotions to convince their victims: fear, curiosity, excitement, guilt, anger, and sadness.

Emergency: Urgent situations or requests are another reliable tool in a threat actor's arsenal. A victim can compromise themselves under the cover of a serious problem that requires immediate action.

Confidence: Confidence and credibility are essential during a social engineering attack. The threat actor generally does in-depth research on his victim, allowing him to create a story that is easy to believe and unlikely to arouse suspicion.

Besides these types of manipulation, threat actors can also use more direct methods to access a network or an organization's computer, such as frequenting the public restaurant or rest area of a large office building or replacing the free Wi-Fi network by impersonating it to create a honeypot to collect information about users.

Email and SMS phishing are threat actors' most popular and effective social engineering techniques. The creators of phishing campaigns generally seek to play on factors of importance, urgency, security, curiosity, or fear among victims. Threat actors pose as trusted institutions or individuals to trick their victims into revealing sensitive information, clicking links to malicious websites, or opening attachments containing malware. To lend credibility to their actions, many threat actors include false secure connection signals to trick the victim into believing that the site they enter their data into is secure (Figure 24).

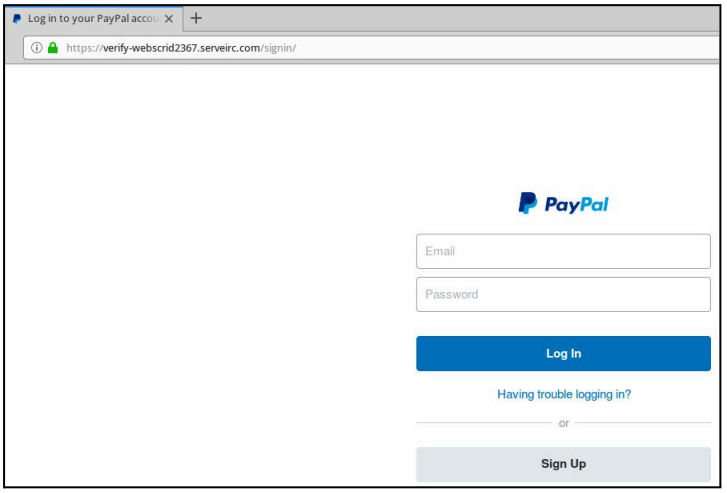


Figure 24 - A phishing page that uses https:// and has the green padlock.

There are several types of phishing attacks, but the most popular are the following:

Email phishing is the most traditional form, using an email to urge you to reply or follow up by other means. Web links, phone numbers, or malware attachments can be used (Figure 25). This type of campaign can target a specific category of people (customers of a company or subscribers to a service) or a wider audience with a certain percentage of success on large volumes of email sending.

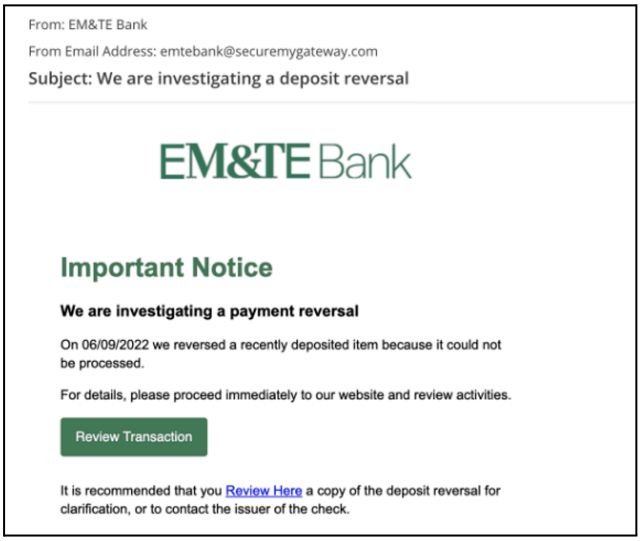


Figure 25 - Bank account verification phishing email example (Source: Keepnet Labs)

SMS phishing (Smishing) is done via text or instant messaging. Typically, threat actors distribute links to redirect to a malicious website or download malicious software stealthily. The emergence of smishing as a tactic results directly from employees using smartphones to access both their text messages and corporate emails (Figure 26). As with email phishing, threat actors generally obtain lists of telephone numbers from hacked customer databases to target a category of person.

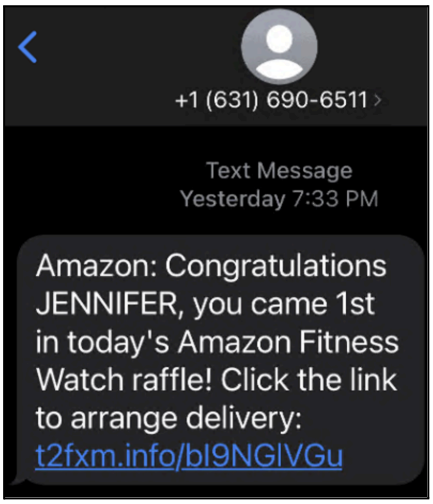
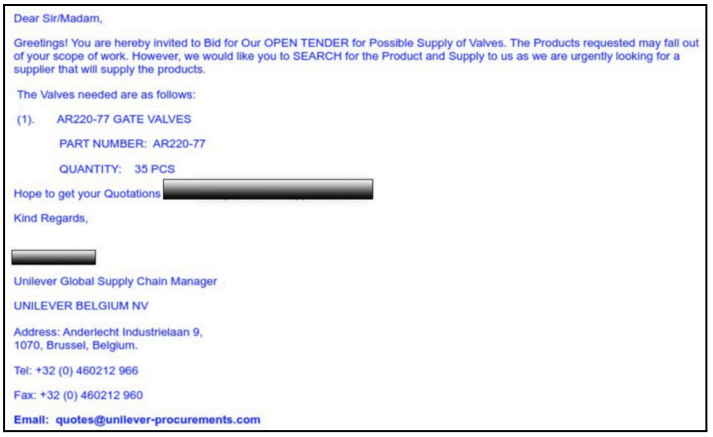


Figure 26 - Amazon SMS phishing example (Source: SafetyDetectives)

Business email compromise (BEC) is one of the most financially damaging online social engineering techniques. It exploits the fact that everyone relies on email to conduct their activities, both personal and professional. In a BEC scam, scammers typically send an email from someone within an organization by spoofing their email address and sending what may be considered a legitimate request addressed to a victim within the same organization or being a customer, supplier, or financial partner (Figure 27).


Dear Sir/Madam,

Greetings! You are hereby invited to Bid for Our OPEN TENDER for Possible Supply of Valves. The Products requested may fall out of your scope of work. However, we would like you to SEARCH for the Product and Supply to us as we are urgently looking for a supplier that will supply the products.

The Valves needed are as follows:

(1). AR220-77 GATE VALVES

PART NUMBER: AR220-77

QUANTITY: 35 PCS

Hope to get your Quotations [redacted]

Kind Regards,

[redacted]

Unilever Global Supply Chain Manager

UNILEVER BELGIUM NV

Address: Anderlecht Industrielaan 9,
1070, Brussel, Belgium.

Tel: +32 (0) 460212 966

Fax: +32 (0) 460212 960

Email: quotes@unilever-procurements.com

Figure 27 - A BEC email targeting a multinational manufacturing organization with email impersonation from a third-party vendor. (Source: Fortra PhishLabs)

Quishing (QR code phishing) is a technique where hackers embed malicious links or files in QR codes to evade detection. The threat can bypass email filters that lack QR code detection or reading capabilities. Unlike emails containing a visible link or attachment, it can also make it more challenging for users to diagnose a threat (Figure 28).

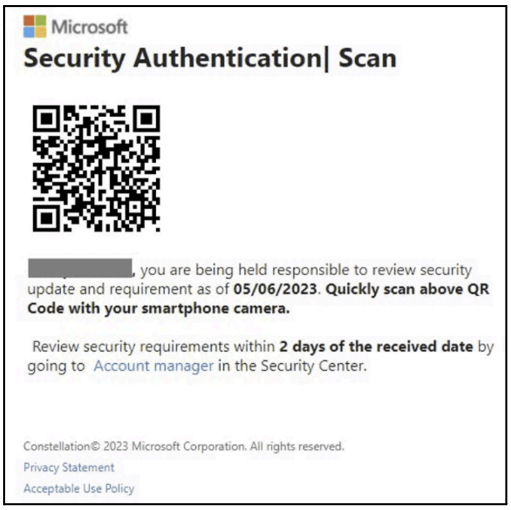


Figure 28 - Microsoft 365 Phishing email example (Source: Vade)

Voice phishing (Vishing) plays on human weakness and psychological manipulation. While classic phishing or smishing can be identified through careful review of the inbound message, threat actors use vishing because of the difficulty of the challenge it poses to the victim to discern the legitimacy of the caller. Vishing specialists often pose as people from customer support, IT, or financial services. They then seek to contact target people and try to extort them. This technique requires a certain amount of self-confidence on the part of the threatening actor because, at some point, he is supposed to be in vocal contact with the victim (Figure 29).

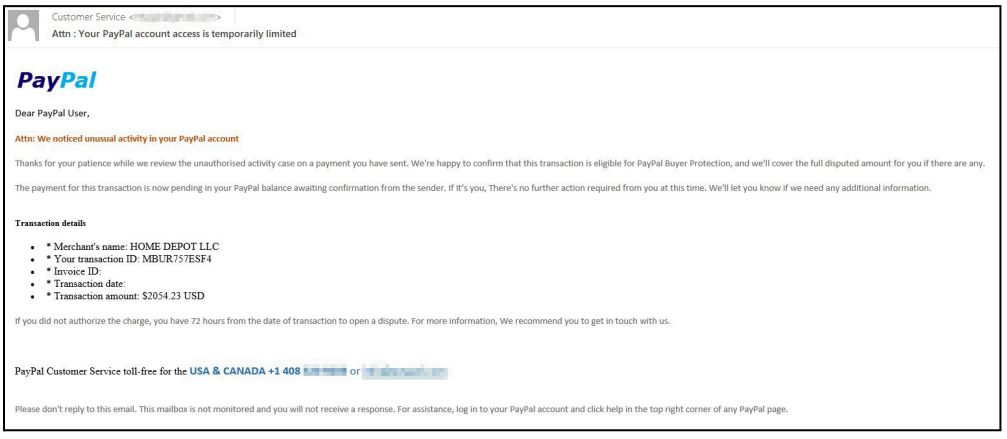


Figure 29 - Fake PayPal notification regarding order cancellation with emergency contact support

Many threat actors offer services or seek to recruit fishing specialists on cybercriminal platforms (Figures 30 and 31).



Figure 30 - A threat actor looking to hire social engineer specialists for calls on a cybercrime forum.



Figure 31 - Professional social engineering service on a cybercrime forum

Pretexting is a social engineering attack in which a scammer invents a pretext or fabricated scenario, usually posing as a person from a public institution such as a tax authority, to trick a victim into providing sensitive personal or financial information. , such as their social security number. In this type of attack, a threat actor can also physically access your data by posing as a supplier, delivery person, or contractor to gain the trust of your staff (Figure 32).

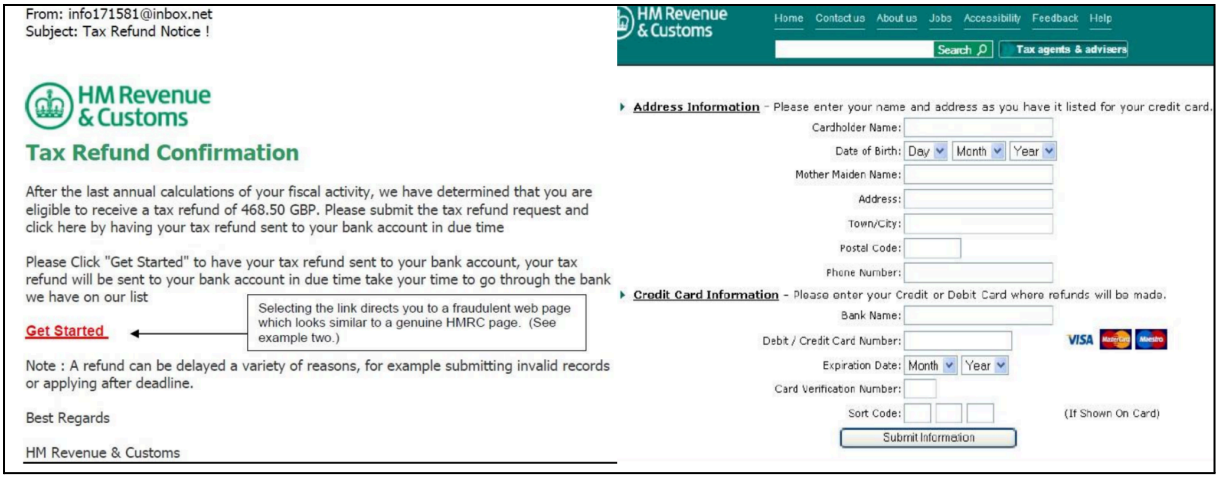


Figure 32 - Fake UK Revenue and Customs phishing pages to collect financial data

Spear phishing uses personalized information to target particular users. This information is collected through different means (leaked databases, open source, etc.). The attacks target high-value targets such as celebrities, senior executives, and high-ranking government officials. To make themselves credible, they generally pose as a known institution, a person from the same company, or the same public entity (Figure 33).

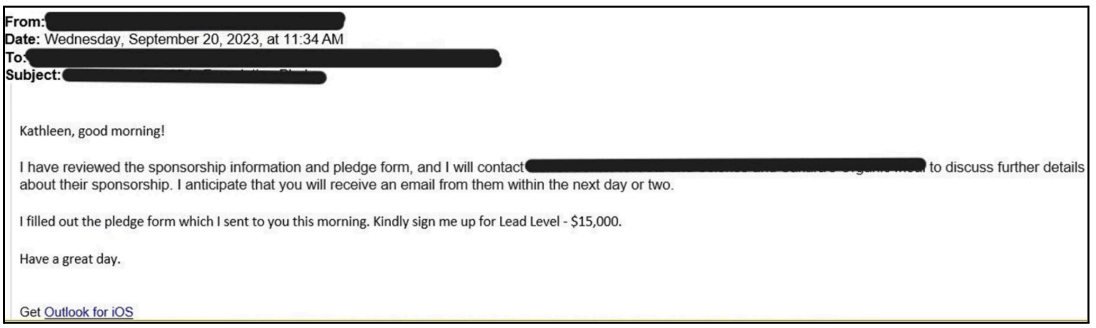


Figure 33 - Spear Email phishing example (Source: Vade)

Angler phishing is performed on social media. An attacker imitates a trusted company's customer service team. They intercept your communications with a brand to hijack and divert your conversation into private messages, where they then advance the attack (Figure 34).

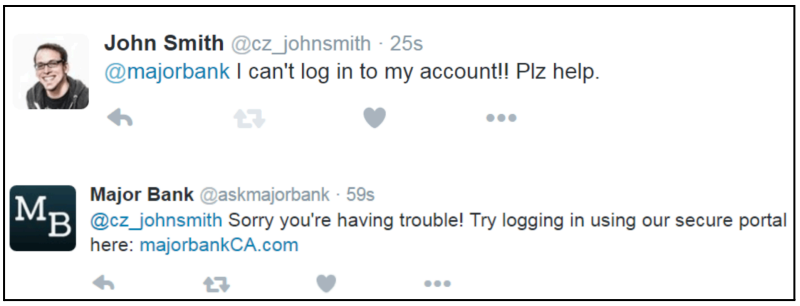


Figure 34 - Angler phishing example on X social network (Source: Proofpoint)

Search engine phishing involves indexing links to fake websites at the top of search results. These may be paid ads or legitimate optimization methods for manipulating search rankings (Figure 35).

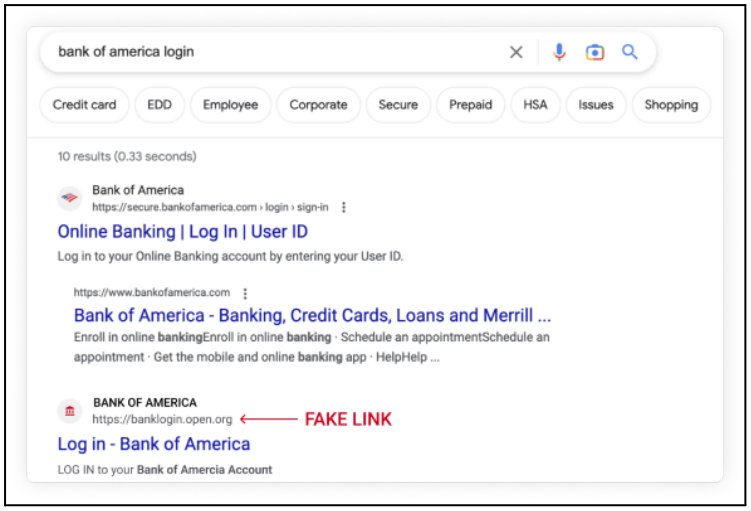


Figure 35 - Search engine phishing example (Source: Keeper)

In-session phishing interrupts everyday web browsing with fake login pop-ups for pages you're visiting. The baiting attack involves exploiting victims' curiosity to trick them into exposing their data. Typically, threat actors lure and manipulate their victims with the help of tempting advertisements and free offers. The attack usually involves infecting the victim with malware. One of the most popular hacking methods is attaching email attachments containing details about a free offer or fraudulent freeware. Another popular form of baiting is using physical media to spread malware. Some threat actors use USB drives to infect them with malware, often leaving them statically in areas where potential victims are sure to see them and are lured by curiosity to see what the connector contains to a personal or professional computer. Social engineering, phishing, vulnerability exploitation, and supply chain attacks are among the most popular attack vectors cybercriminals use to penetrate networks and systems of public and private organizations.

2.3 Malware and Exploits

Malware and developing exploits to exploit vulnerabilities are integral parts of cybercriminals' arsenal and are important, if not indispensable, tools in continuing their operations.

2.3.1 Ransomware

When it comes to malware, ransomware is by far the most trending and damaging malware of the last decade. Ransomware attacks have evolved significantly in terms of modus operandi and attack vectors. Ransomware is one of the biggest cybercrime threats, if not the biggest. With ransom demands far exceeding the cost of development, ransomware attacks are very lucrative for cybercriminals. For several years now, cybercriminals operating ransomware have been practicing double extortion, which consists of encrypting the data and systems of victims after having previously collected a large amount of internal and confidential data generally of great value in terms of business. Cybercriminals are, therefore, doubly winning by demanding a ransom and threatening the victim to make the information public if they do not pay the ransom, which can be increased by cybercriminals when they tell their victims that they own a lot of confidential information. They can also easily try to sell the stolen data on the darkweb to increase their profits. This aspect of the attack adds psychological pressure on victims who are already stressed due to the loss of access to their systems and data. There are many ransomware groups, but a limited number of groups with varying consistency carry out most attacks (Figure 36). Additionally, ransomware as a service has been proliferating on the dark web for several years, making it more widespread and a cyber weapon accessible to many cybercriminals who are not ransomware specialists (Figure 37).

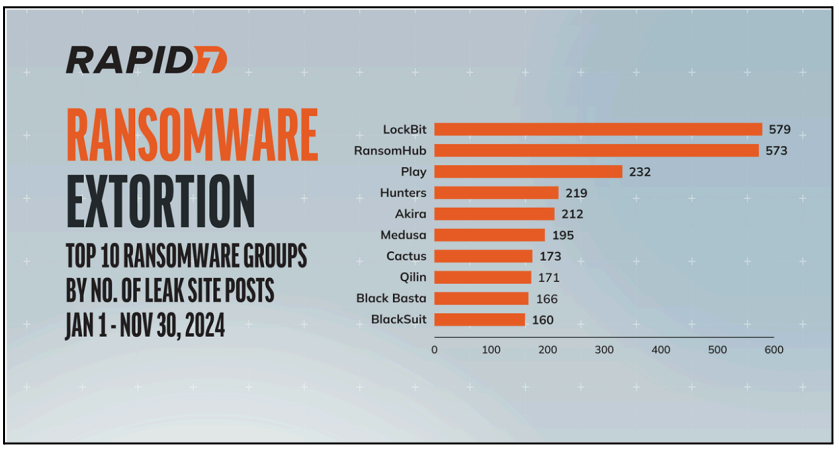


Figure 36 - TOP active ransomware groups in 2024 (Source: Rapid7)

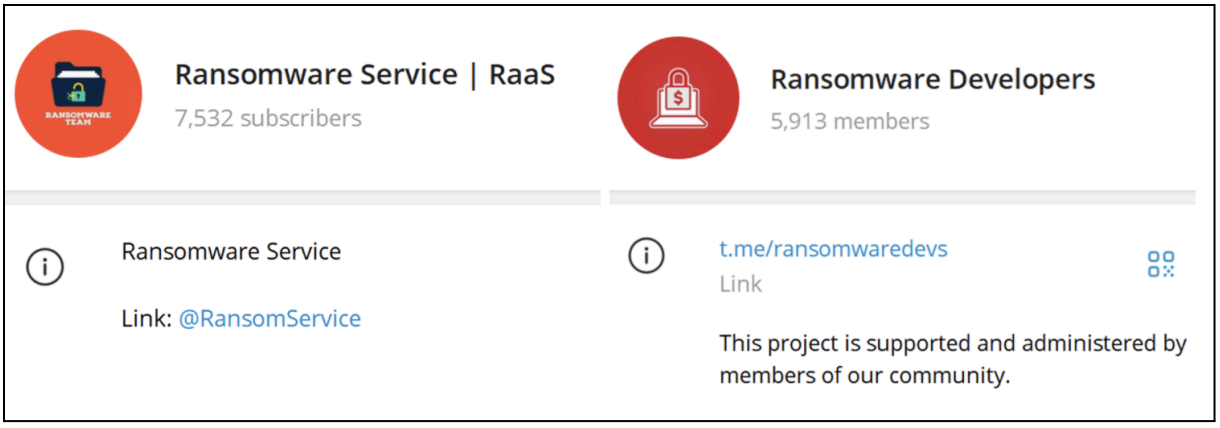


Figure 37 - Ransomware services on Telegram

Several sites list ransomware attacks with the victims' names, which allows us to observe the evolution of the threat by country, sector of activity, and period (Figure 38). Ransomware attacks will undoubtedly continue to be among the most used by cybercriminals in the years to come, with increasingly sophisticated operating methods adapted to cybersecurity systems.

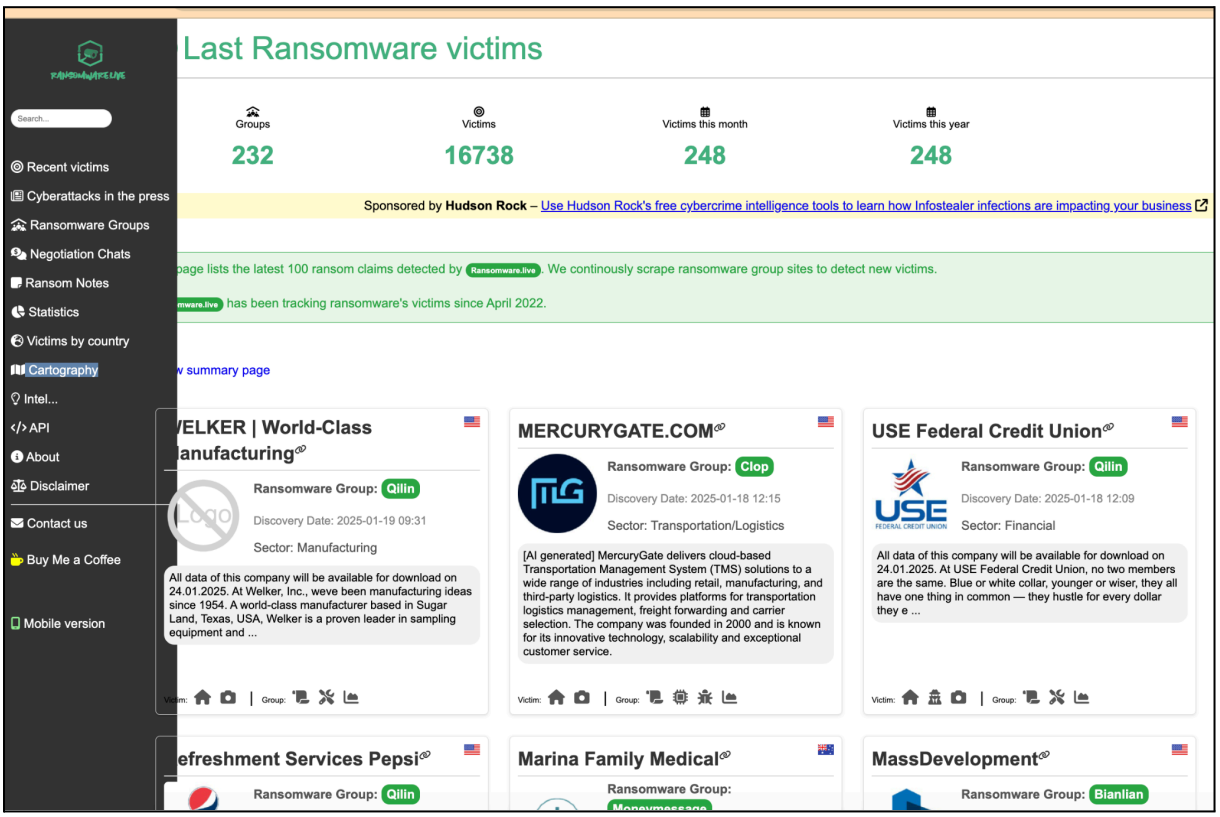


Figure 38 - A live ransomware tracker website (Source: ransomware.live)

2.3.2 Data Collection Malware

With increased personal and financial data, data collection malware has been a strong trend in the cybercriminal world for several years. Cybercriminals have developed different types of malware capable of searching for, identifying, and collecting a certain type of data, which is then generally stored and used for fraudulent purposes or resold on the dark web. According to an analysis by the threat-hunting company ANYRUN, stealer malware took the lead in 2024. It dominated in 2024 with 51,291 detections, compared to second place in 2023 with only 18,290. Loaders followed with 28,754 detections, while RATs held on to third place with 24,430. Lumma Stealer was the most detected malware family, with 12,655 detections (Figure 39).

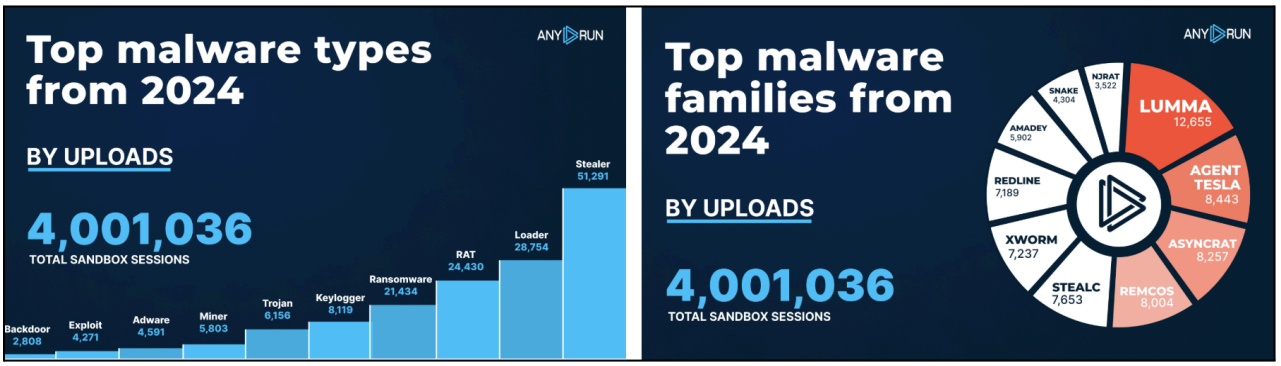


Figure 39 - Top malware types and families (Source ANYRUN)

Data collection malware is malicious software designed to gather sensitive information from a victim's system, network, or environment without their consent. This type of malware is often used in cyber espionage, financial theft, or other malicious activities. Below are its characteristics and functions:

Characteristics of Data Collection Malware

- **Stealthy Operation:**
  - Operates covertly to avoid detection by the user or security software.
  - Employs obfuscation techniques like encryption or polymorphism to evade antivirus systems.
- **Targeted Data Gathering:**
  - It focuses on data types such as credentials, financial information, browsing history, and system configurations.
  - Some are designed for mass collection, while others target specific entities or industries.
- **Persistence Mechanisms:**
  - Installs itself in ways that ensure it survives system reboots or software updates.

    - Creating scheduled tasks.
    - Can use techniques like rootkits or registry modification to remain hidden.
- **Exfiltration Capabilities:**
    - Uses secure channels (e.g., encrypted communications) to send stolen data to a remote command-and-control (C2) server.
    - Using legitimate protocols like HTTPS, DNS tunneling, or file-sharing services to blend in with normal traffic.
- **Versatility:**
    - Often modular, allowing attackers to add or change functionality after deployment.
    - It can adapt based on the environment it is deployed in.
- **Delivery Mechanisms:**
    - Spread through phishing emails, malicious websites, infected software, USB drives, or network vulnerabilities.

Functions and Work of Data Collection Malware

- **Data Harvesting:**
    - It collects sensitive user information such as usernames, passwords, email addresses, credit card numbers, and personal identification numbers.
    - Targets system information, including logs, clipboard data, and screenshots.
- **Credential Stealing:**
    - Exploits browser vulnerabilities or uses keyloggers to capture credentials entered into websites or applications.
- **Network Monitoring:**
    - Monitors and records network traffic to intercept sensitive data being transmitted.
- **Database or File Extraction:**
    - Targets local or network databases to exfiltrate customer data, intellectual property, or financial records.
    - May search for specific file types or keywords.
- **Keylogging:**
    - Records keystrokes to capture typed information like passwords, search queries, or chat messages.
- **Clipboard Monitoring:**
    - Monitors the clipboard to capture copied information, such as credit card details or cryptocurrency wallet addresses.

- **Exfiltration of Data:**
    - Compresses and encrypts collected data before transmitting it to a remote server controlled by the attacker.
- **Screen Capture and Webcam Recording:**
    - Takes screenshots or records video/audio from a device to gather additional sensitive information.
- **Browser and Email Data Theft:**
    - Extracts saved browser credentials, browsing history, or email contents.

On the dark web, many cybercriminals offer to sell or recruit people to develop malware projects such as RAT, stealer, and others. The price of this malware generally varies depending on the features included (screenshot, form grabber, keylogger...) and the sophistication (AV bypass, encryption...) and can thus range from several hundred to several thousand dollars (Figure 40 and 41)

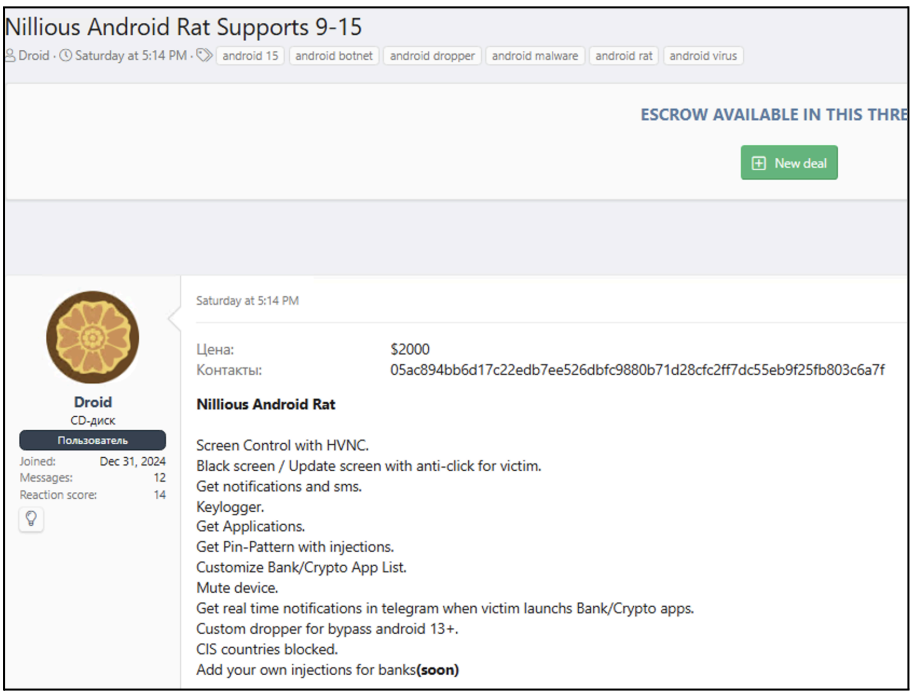


Figure 40 - Android RAT for sale on a cybercrime forum

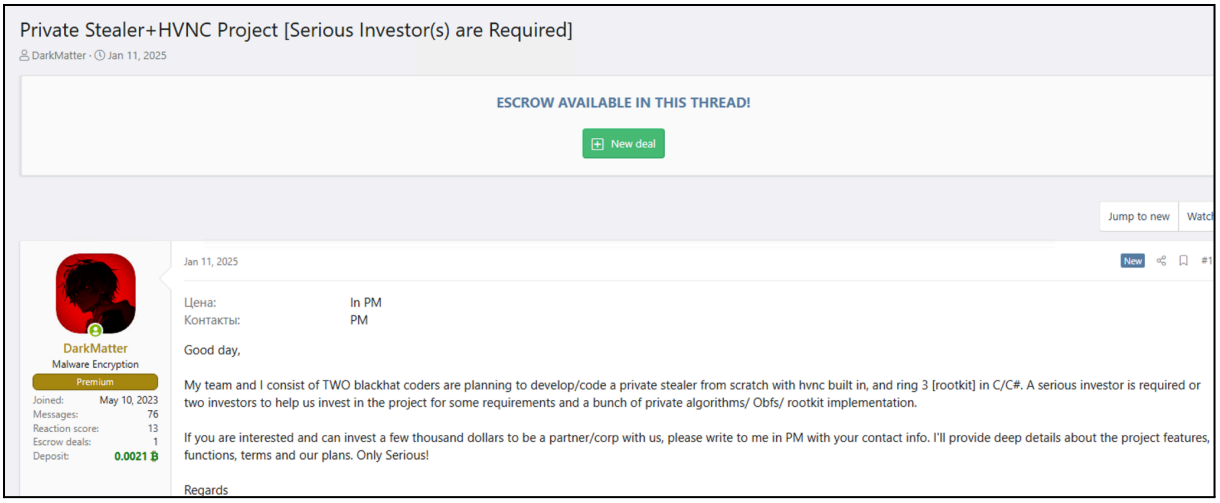


Figure 41 - A cybercriminal offering to join a private stealer development project on a cybercrime forum

2.3.3 Exploits and Vulnerabilities

Vulnerabilities and exploit development are an integral part of the cybercriminals' arsenal. Most cyberattacks by cybercriminals exploit known or unknown flaws and vulnerabilities, often allowing them to be the entry point within the network, system, and/or device. The exploit market is a key part of the cybercrime ecosystem, where code or exploitation techniques that exploit software, hardware, or systems vulnerabilities are developed, traded, and sold. This market operates primarily on the dark web and other underground forums. Below are details on the development, use, and sale of exploits in this ecosystem:

Development of Exploits

Skilled cybercriminals with deep technical expertise in reverse engineering, software development, and vulnerability analysis often develop exploits (Figure 42).

- **Exploits:**
  - **Zero-Day:** These target vulnerabilities unknown to the software vendor and are the most valuable in the exploit market.
  - **Known Vulnerabilities**: Older vulnerabilities are often exploited when users fail to update or patch their systems.
  - **Bug Bounties Gone Rogue:** In some cases, legitimate researchers may sell their discoveries on the dark web instead of reporting them to vendors.

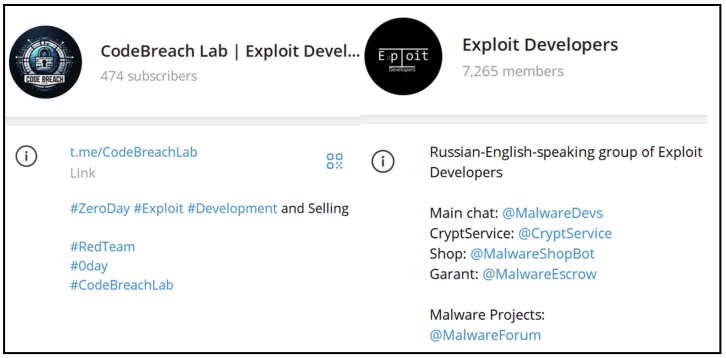


Figure 42 - Exploit development service on Telegram

Sale of Exploits

Over the last ten years, the sale of exploits for vulnerabilities has become more widespread. However, it is not always easy to find reliable and quality exploits. Several underground markets on the Internet and Telegram have a higher or lower level of exploits (Figure 43).

- **Dark Web Forums and Marketplaces:**
  - **Exploits** are sold on specialized dark web forums or marketplaces like exploit shops.
  - **Prices and access** are often controlled via cryptocurrencies for anonymity.
- **Exploit Brokers:** Brokers act as intermediaries between buyers and sellers, connecting those looking to monetize exploits with interested parties, including nation-states.

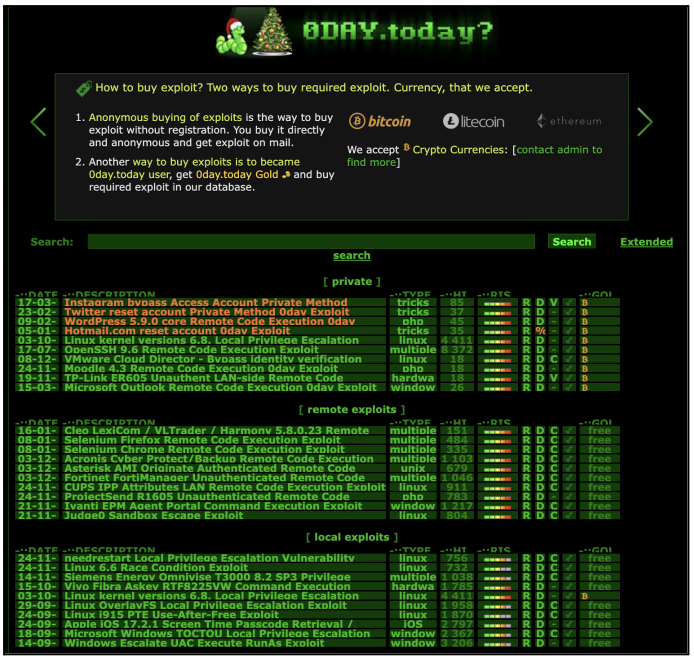


Figure 43 - A darkweb market selling exploits

- **Subscription Models:**
    - **"Exploit-as-a-Service"** offers access to a portfolio of exploits for a recurring fee (Figure 44).
    - **Exploit kits** bundle multiple exploits with user-friendly interfaces, allowing less skilled cybercriminals to launch attacks.
- **Price: The value of an exploit depends on:**
    - **Type of Exploit:** Zero days are the most expensive, ranging from tens of thousands to millions of dollars.
    - **Target System**: Exploits targeting critical systems (e.g., operating systems, IoT devices) or popular platforms (e.g., Windows, iOS, Android) are more valuable.
    - **Ease of Use:** Plug-and-play exploits fetch higher prices due to their accessibility to non-technical users.

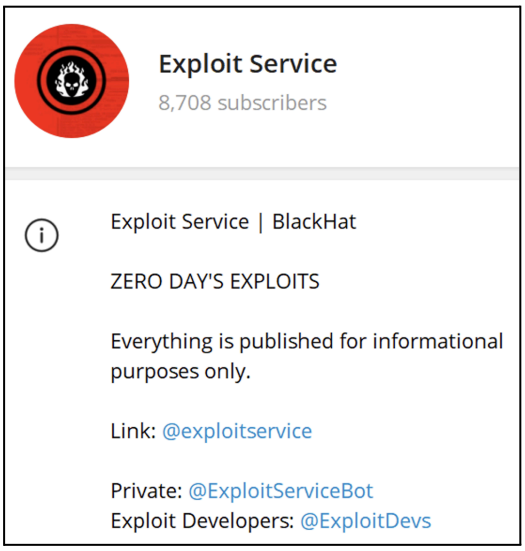


Figure 44 - Exploit service for sale on Telegram

Uses of Exploits

- **Financial Fraud:** Exploits are used to steal financial information (e.g., credit card details, online banking credentials).
- **Ransomware:** Deployment: Many ransomware campaigns use exploits to compromise systems and deploy payloads.
- **Botnet Creation:** Exploits infect devices, turning them into part of a botnet for DDoS attacks or other malicious purposes.

Exploit Market Trends

- **Increased Automation:** Many exploit kits now automate attacks, broadening their usability.
- **Focus on IoT and Mobile Devices:** As traditional systems become more secure, attackers increasingly target less protected IoT devices and mobile platforms (Figure 45).
- **Collaboration with Malware Developers:** Exploit developers often collaborate with malware creators to deliver exploits alongside malicious payloads.
- Underground Training: Some forums offer tutorials and training for aspiring exploit developers, expanding the pool of cybercriminals capable of creating and using exploits.



Figure 45- Remote code execution (RCE) IoT for sale on a cybercrime forum

2.4 Generative Artificial Intelligence and Deepfake Technology

Generative AI has enabled significant technological advances, but it has also been misused by cybercriminals to conduct various fraudulent activities. AI has become a topic of considerable interest among the cybercriminal community, who seek to use it for illicit purposes, including social engineering to deceive victims through a person's voice and image. Generative AI can analyze publicly available data (e.g., social media profiles, forums, and professional networks) to create detailed profiles of potential targets. In addition, AI models can identify patterns, preferences, and vulnerabilities (e.g., hobbies, emotional states, or common online habits) from user data to tailor social engineering attacks. AI can help cybercriminals generate highly personalized phishing emails that mimic the writing style or tone of a trusted friend or colleague, making the attack harder to detect.

The use of AI in attacks aimed at tricking the victim into believing that the person on the other end of the line or in the video is the same person is commonly called “Deepfake.” Deepfakes are photos and videos manipulated using AI to make people appear to be saying or doing something they never did or appear to be in places where they have not been. Deepfake's quality can vary depending on the tools used and the time spent working on the image or video created (Figure 46).

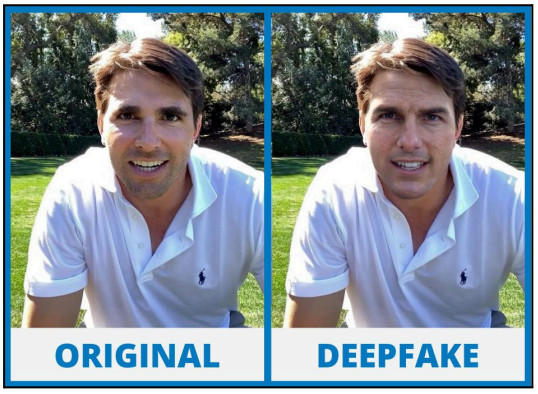


Figure 46- Real and AI-generated images (Source: Maverick)

There are several types of DeepFake, such as Textual, Audio, Video, Social Media, and Live or real-time (Figure 47).

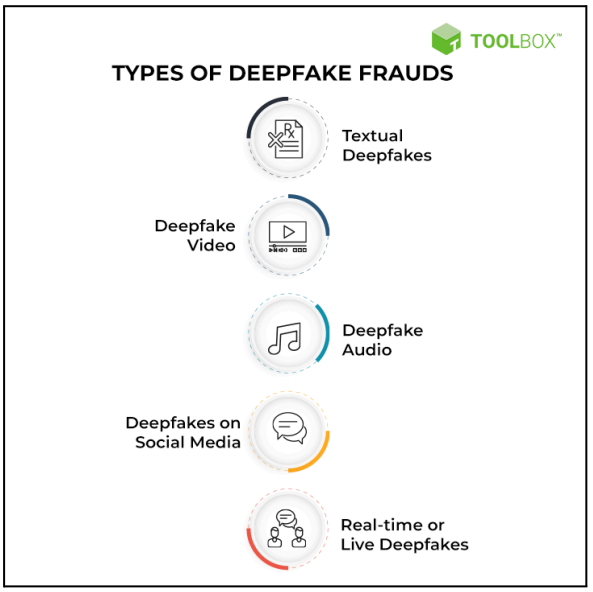


Figure 47 - Different types of DeepFake (Source: ToolBox)

If a DeepFake relies on AI, machine learning is essential in its creation. Convolutional neural networks (CNN) are a subset of powerful AI built in part on the human mind, capable of detecting trends in information, and can be used for image and speech recognition. Creating a deepfake video can be defined as follows:

- First, a large amount of actual video footage must be sent to a deep neural network, which is gradually trained to recognize a person's rhythms and detailed characteristics. This gives the algorithm a realistic representation of an individual's appearance from different perspectives.

- Secondly, it combines with the learning algorithm facial and vocal models generated by the AI obtained from the neural input of the network.

While many think creating a deepfake requires complex tools and technical skills, this is untrue. They can also be created with basic knowledge of computer graphics, which can help to democratize the use of deepfakes. Thanks to advances in AI, deepfakes have become more convincing than ever and are often used to fool people. Some deepfakes look realistic, so it's no surprise that criminals misuse this technology in inventive ways to facilitate scams. Indeed, thanks to AI software like the one presented above, it is possible today and will be even more possible in the long term to impersonate a person's vocal and physical identity and make them say or do what they want. In the coming years, if appropriate security measures are not found and implemented, AI will make manipulating people even more critical, which could lead to a sharp increase in scams, influence campaigns, and illegal activities. Cybercriminals use deepfake technology to create realistic videos or audio mimicking public figures, executives, or even victims to commit fraud, such as impersonating CEOs for business email compromise (BEC) scams or extortion (Figure 48).



Figure 48 - A threat actor asking on a cybercrime forum about using AI for a Vishing attack (Source: Exploit. in)

Apart from using AI to make deepfakes for fraud purposes, several cybercriminals have hijacked generative AI tools like ChatGPT, using them to create phishing campaigns and other types of cyberattacks more efficiently and on a larger scale (Figure 49)

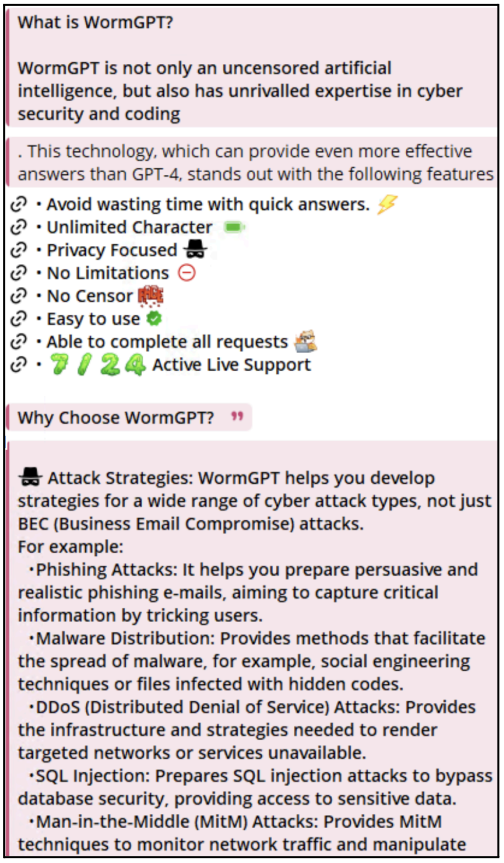


Figure 49 - WormGPT advertising on Telegram

2.5 Fraud and Money Laundering

Money laundering is the process of illegally acquiring money and hiding it to give the impression that it was generated from legitimate sources. Money laundering usually comes from activities such as drug and sex trafficking, terrorist activities, and other illicit means. In a traditional money laundering system, we can distinguish different stages to conceal money acquired illegally. The following steps are usually part of the money laundering process:

- **Investment:** Money is brought into the financial system by dividing it into different deposits and investments.
- **Layering:** The money is mixed to create distance between it and the perpetrators.
- **Integration:** The money is returned to the owners as legitimate income or own money.

Since the emergence of cryptocurrencies, hackers, criminals, and terrorists quickly realized that these virtual currencies would facilitate money laundering despite specific state regulations set over the years. Owning, exchanging, and investing cryptocurrencies can be helpful for threat actors who do not lack the imagination to transform dirty money into proper and legal funds. Money launderers can convert their cryptocurrencies into private coins to conceal their operations since digital assets like Monero and ZCash are harder to track. While many exchanges and governments prohibit using private coins, money launderers can always find ways to transfer these tokens and hide their funds. Based on the data analyzed by the blockchain compliance company,

Based on data analyzed by the blockchain compliance company Chainalysis[1], illicit cryptocurrency addresses sent $22.2 billion worth of cryptocurrencies to services, a significant decrease from the $31.5 billion sent in 2022. The company adds that some of this decline can be attributed to an overall decrease in the volume of crypto transactions, both legitimate and illicit. However, the decline in money laundering activity was more pronounced, at 29.5%, compared to the 14.9% decline in total transaction volume (Figure 50).

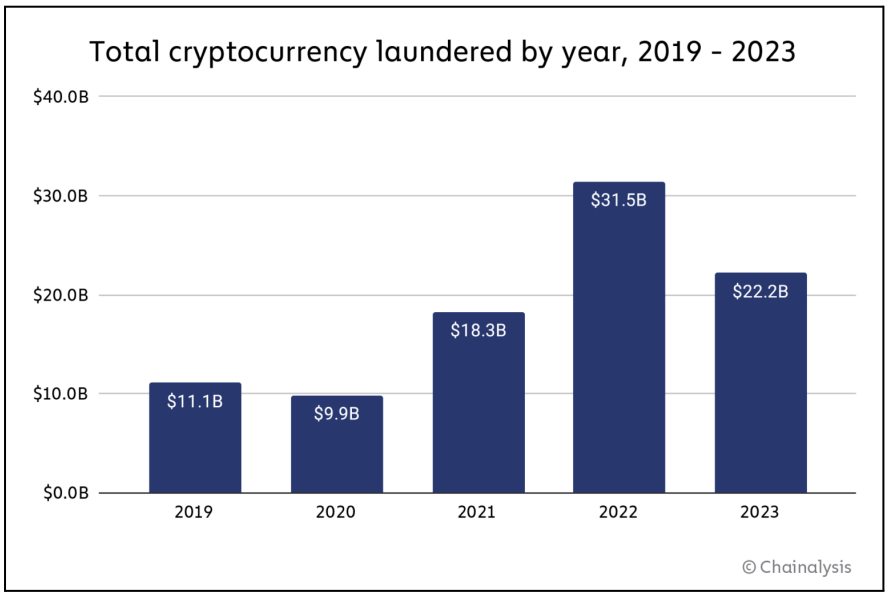


Figure 50 - Total cryptocurrency laundered between 2019 and 2023 (Source: Chainalysis)

Money launderers have been increasingly using Initial Coin Offerings (ICOs), a popular fundraising method used primarily by start-ups wishing to offer products and services. Some ICOs have generated massive returns for investors. However, other ICOs have become frauds or were financed using illegal funds.

[1] https://www.chainalysis.com/blog/2024-crypto-money-laundering/

Unlike investments with traditional funds, it is more complicated or almost impossible for start-up creators to verify the source of their investor's cryptocurrency funds. In addition, some founders open the capital to anyone who wants to invest in their project, which makes things even easier for money launderers (Figure 51).

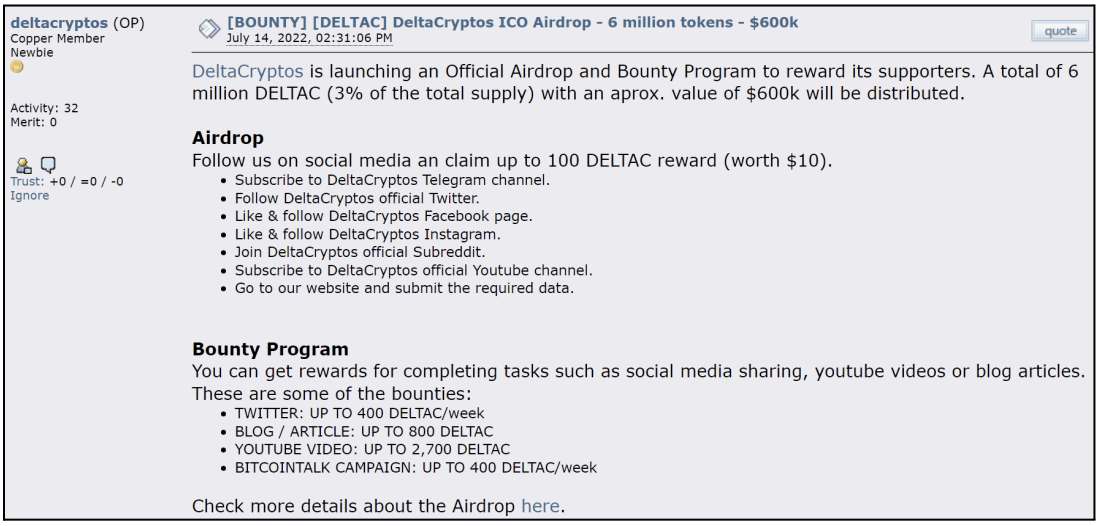


Figure 51 - Example of an ICO project initiated in 2022 on a cryptocurrency forum

2.6 Network Access and Data Breach

Exploitable access points in company networks and systems are a prime target for cybercriminals seeking to capitalize on such vulnerabilities. Many cybercriminals focus on collecting personal information and hunting for valuable documents or reports that can be sold to the highest bidder. While gaining direct access to corporate networks often requires significant effort, an easier alternative has emerged: purchasing access to previously compromised networks. This has created a thriving underground market where intermediaries and brokers trade access to breached networks across various industries, including the energy sector. The most popular access types commonly sold on the darkweb include SSH, cPanel, RDP, Citrix, SMTP, and FTP. Prices are usually determined by the size or revenue of the target company and the number of connected devices (Figure 52, 53 and 54). According to IBM[2], the average total data breach cost increased from $4.45 million to $4.88 million in 2023, a 10% increase and the largest increase since the COVID-19 pandemic. Additionally, more than half of organizations that suffer a breech face a severe shortage of security personnel, representing a 26.2% increase from the previous year.

[2] https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec



Figure 52 - Network access (VPN) to a US multi-sector company for sale on cybercrime forum

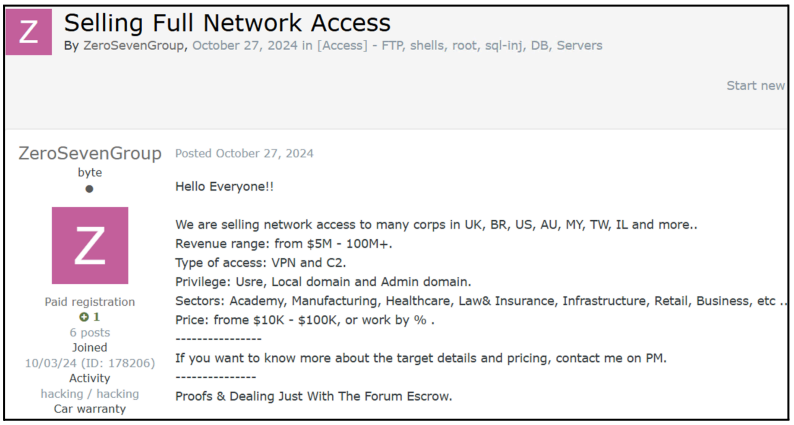


Figure 53 -Network access (VPN and C2) to multiple companies worldwide for sale on a cybercriminal forum

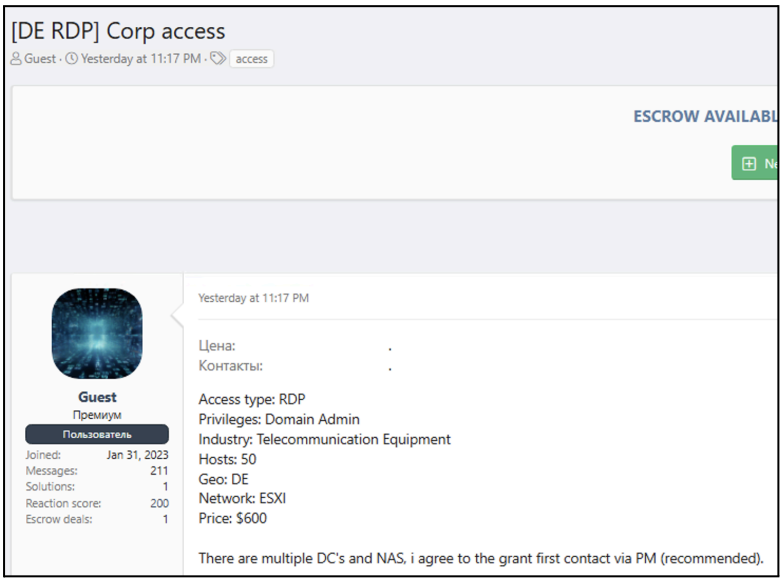


Figure 54 -Network access (RDP) to a telecommunication company for sale on a cybercriminal forum

3. Cybercriminals' Psychology

To successfully fight cybercrime, it is also very important to understand the psychology of cybercriminals. Understanding their mindset can help develop strategies to combat this phenomenon. The psychology of cybercriminals involves a mix of personal motivations, behavioral tendencies, and cognitive processes that influence the planning and execution of cybercriminal activities. The main psychological factors that play an important role in the psychology of cybercriminals:

3.1 Motivations

- **Financial Gain:** The most common driver targeting valuable data, intellectual property, or direct monetary theft.
- **Revenge:** Cyberattacks as a way to harm specific individuals, organizations, or governments.
- **Recognition or Status:** Demonstrating technical skills to earn respect or notoriety in online communities.
- **Thrill-Seeking:** Some cybercriminals are motivated by the challenge and excitement of bypassing security systems.
- **Curiosity:** Young or inexperienced individuals may start as hobbyists exploring systems before transitioning into criminal activities.

3.2 Way of Thinking and Cognitive Bias

- **Rationalization:** Many cybercriminals justify their actions by believing that large corporations or governments are worth targeting or will not suffer significant damage.
- **Overconfidence and risk perception**: Some cybercriminals, having high confidence in their skills and the anonymity offered by networks like TOR or using tools like VPNs, tend to underestimate the likelihood of being detected and stopped.
- **Moral disengagement:** They may compartmentalize their actions, dissociating them from ethical, moral, and victim impact concerns.

3.3 Behavioral Characteristics

- **Opportunistic Behavior:** Some cybercriminals look for easy-to-use solutions, such as systems with weak security, default credentials, or unpatched vulnerabilities.
- **Adaptability:** They continually learn and evolve their tactics, techniques, and procedures (TTPs) to counter evolving cybersecurity measures.

3.4 Psychological Profiles

Some traits are common to cybercriminals:

- **Introversion and isolation:** many operate alone or in small groups and spend much time online.
- **Intelligence:** cybercriminals often have advanced problem-solving and technical skills.
- Lack of empathy: The vast majority of cybercriminals are little concerned with the harm caused to victims and the consequences their actions have on them (financial, psychological, etc.).
- **Ego:** need for validation or the thrill of outwitting systems and demonstrating their capabilities and know-how.

Beyond these typical profiles and characteristics of cybercriminals, there are also cultural factors. Cultural factors significantly influence the psychology and behavior of cybercriminals, shaping their motivations, techniques, and ethical boundaries. These factors include societal values, norms, legal frameworks, and socio-economic conditions. Here's how they manifest:

Motivations Shaped by Socioeconomic Context

- Economic Hardship: In countries with high unemployment or poverty rates, individuals may use cybercrime to achieve financial stability.
- Cultural Acceptance of Illicit Activities: In some cultures, cybercrime might be considered a lesser or acceptable offense, especially if it targets foreign entities or "wealthy" nations.

Perception of Ethics and Legitimacy

- **Cultural Relativism:** What is deemed unethical in one culture may be seen as clever or innovative in another. For example, hacking into a system might be celebrated as a sign of technical skill in certain communities.
- **Collectivism vs. Individualism:** In collectivist cultures, cybercrime may be rationalized as an act for the greater good, such as targeting governments or corporations seen as exploitative.

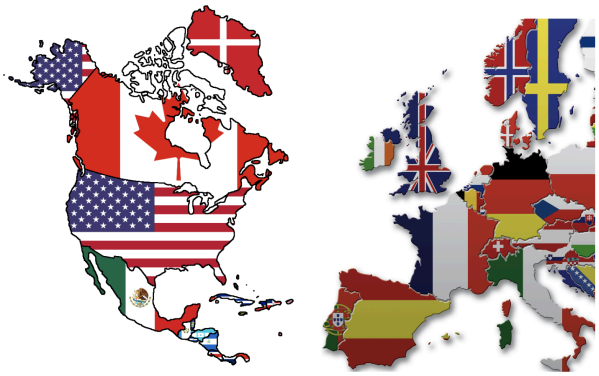
Globalization and Cultural Collaboration

- **Cybercrime Networks:** Cybercriminals often form cross-cultural networks, utilizing differences in laws and enforcement to their advantage. For instance, one group might operate in a country with lax cybersecurity laws while targeting victims elsewhere.
- **Cultural Adaptation:** Cybercriminals tailor their attacks to exploit cultural nuances, such as phishing emails that mimic local linguistic and social customs.

4. Geographical Distribution of Cybercrime

4.1 Western Europe and North American Countries

Cybercrime is a pervasive threat in North America and Western Europe, fueled by the region's economic importance and digital infrastructure. Many cyberattacks targeting these regions originate from countries worldwide, particularly in Eastern Europe, Africa, and Asia. This increase in cybercrime is largely due to large investment and commercial banks, multinational corporations, and industries generating substantial revenues, making them lucrative targets for cybercriminals. However, Western countries are not only victims; they are also often part of the cyberattack ecosystem.



Contrary to popular belief, many malicious infrastructures, including command and control (C&C) servers, are based in Europe (Figure 55). Despite strong collaboration between European Union member states, cybercriminals frequently establish or operate compromised servers in countries such as the **Netherlands** and **Germany.** The **UK,** in particular, has a notable presence of cybercriminal activity. A high-profile example occurred in 2022 when two young British men were arrested during an international investigation into the Lapsus$ gang. The group had orchestrated large-scale breaches, targeting major technology companies like Microsoft. This case highlights cybercrime's evolving and transnational nature, which requires strong international cooperation and proactive cybersecurity measures.

Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Countr
2025-01-13 14:40:25	185.77.174.191	QakBot	Offline	AS34920 SIMPLY-ROMFORD	GB
2024-03-26 23:30:12	158.220.95.215	Pikabot	Offline	AS51167 CONTABO	GB
2024-03-26 23:30:07	213.199.41.33	Pikabot	Offline	AS51167 CONTABO	DE
2024-03-05	84.46.240.42	Pikabot	Offline	AS51167 CONTABO	DE
2023-08-16 17:22:14	173.206.129.159	QakBot	Offline	AS6407 PRIMUS-AS6407	CA
2023-08-11 15:22:42	75.156.126.33	QakBot	Offline	AS852 TELUS Communications	CA
2023-08-12 11:22:45	86.222.77.167	QakBot	Offline	AS3215 France Telecom - Orange	FR
2023-08-05 18:23:16	86.222.92.165	QakBot	Offline	AS3215 France Telecom - Orange	FR

Figure 55 - Some C&C servers delivering malware are located in North America and Europe.

4.2 Eastern Europe Countries



Eastern Europe is one of the most active hotbeds of cybercriminal activity, with Russian-speaking actors demonstrating exceptional technical expertise and well-organized structures, particularly among ransomware groups. The Russian-speaking cybercrime ecosystem extends beyond **Russia,** encompassing individuals from countries of the former Soviet Union, including **Ukraine, Belarus, Moldova, Latvia, and Kazakhstan.** While "Russian-speaking cybercriminals" often refer to a broader group rather than just individuals from Russia, cultural and linguistic nuances help experts distinguish them. Their slang, forum interactions, and communication styles reveal subtle differences. The ongoing war between Russia and Ukraine has also caused friction within the cybercriminal community, exemplified by divisions within groups such as the former Conti ransomware organization. Russian cybercriminals, except Advanced Persistent Threat (APT) groups, operate primarily on Russian-language forums such as XXS.is and Exploit. In, Ramp (Figure 56), and Telegram channels. These platforms serve as key hubs for collaboration, recruitment, and the exchange of illicit tools and services, highlighting the sophistication and adaptability of this ecosystem.

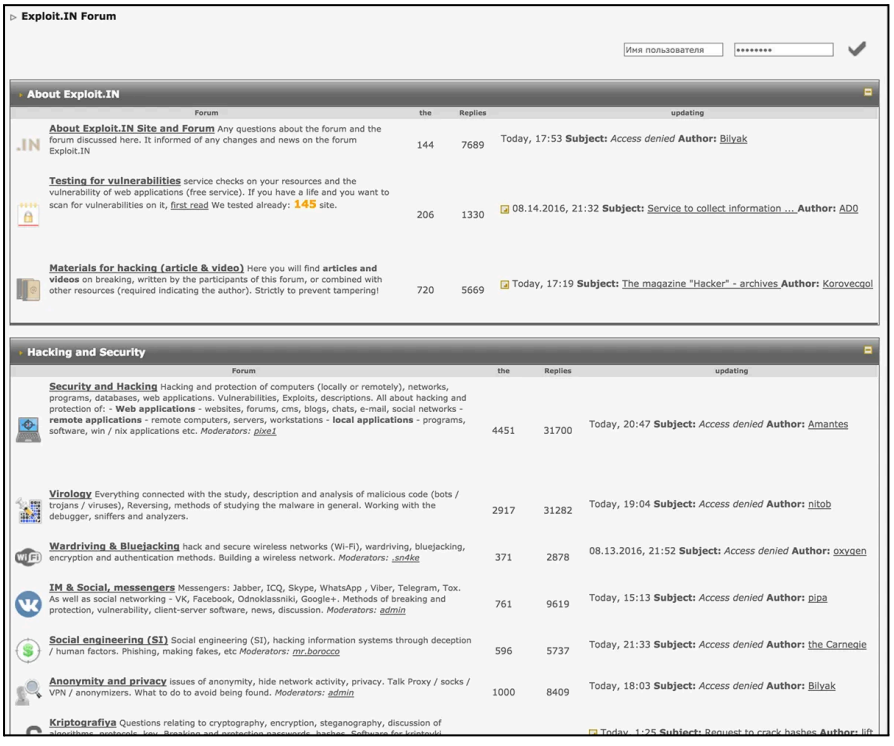


Figure 56 - Russian-speaking cybercrime forum (Source: exploit.in)

Russian-speaking cybercriminals are frequently linked to platforms that trade stolen credentials obtained through malware like Stealer and RAT. These platforms are highly organized and continuously updated with logs from hundreds of thousands of compromised computers and servers worldwide (Figure 57). A key driver of this extensive online criminal activity is the low-income levels in these regions. Many cybercriminals on Russian-speaking forums hail from former Soviet Union countries with low living standards, turning to hacking as a fast and relatively low-risk way to earn money.

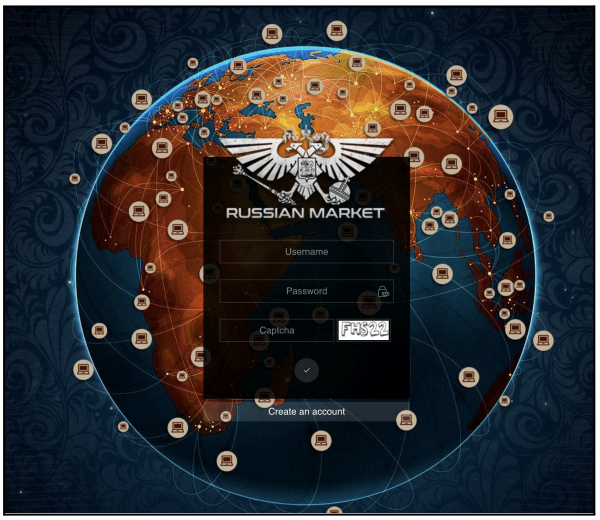


Figure 57 - A darkweb logins market (Source: Russian market)

4.3 Middle East and African Countries

Cybercriminal activity in the Middle East and Africa shows significant geographic variation, with some countries experiencing higher incidences due to various factors such as internet penetration rates, economic development, and cybersecurity infrastructure. South Africa stands out as a major hub for cybercrime on the continent. According to Interpol's Africa Cyber Threat Assessment 2024, South Africa accounts for 22% of all cyberattacks on the continent, and 25% of dark web messages target organizations in the country, particularly government entities.[3]



Kenya recorded 114 cyberattacks on critical infrastructure in 2024, with 657.8 million cyberthreats detected between July and September 2024.

Egypt Represents 13% of cyberattacks in Africa.

Ghana saw a 997% increase in data breaches in Q1 2024 compared to Q4 2023, totaling 1.2 million breaches.[4]

Nigeria is also a major player in Africa's cybercrime landscape. The Global Cybercrime Index ranked Nigeria fifth in the world, making it the highest-ranked African country. The country has been linked to various cybercrime activities, including online scams and fraudulent schemes such as sextortion and romance scams.

Although **Israel** is not considered a cybercrime hub, it is a known source of online scams such as binary options, Forex and cryptocurrencies, call center scams, real estate and investment fraud, and BEC scams.

In the Maghreb, **Morocco** has become a focal point for specific cyber threats. The INTERPOL report highlighted that Morocco is the African nation most affected by Trojans and bank robbers, with 18,827 detections. Furthermore, Morocco ranks second on the continent for ransomware attacks, accounting for 8% of all detected attacks. Furthermore, the Global Cybercrime Index ranked Morocco seventh in Africa and 48th globally, with a score of 0.45 out of 100.

Gulf countries are more often victims. With their abundant natural resources and strong economic activity, they attract the covetousness of many cyber criminals.

[3]https://techtrendske.co.ke/2024/11/25/south-africa-accounts-for-22-of-all-cyberattacks-in-africa/?utm_source=chatgpt.com
[4] https://toptechgh.com/overview-of-africas-cyber-threat-landscape-in-2024/?utm_source=chatgpt.com

4.4 South American Countries

Cybercrime activity in South America varies significantly from one country to another. Still, certain trends have been identified in specific South American countries due to technical expertise, socio-economic conditions, and the strength of legal enforcement. In 2024, countries in South America experienced varying levels and types of cybercrime activity.



Brazil faced a significant increase in cybercrime, particularly ransomware attacks. According to the Group IB annual report, the number of ransomware incidents in Brazil increased by 19% compared to the previous year. The country is a hub for developing banking malware targeting online financial transactions. Brazilian hackers are also known for credit card fraud and ATM skimming.

Argentina appears to have been one of the Latin American countries most targeted by malware on computers and mobile devices in 2024. Additionally, Argentina has seen increased phishing campaigns targeting financial institutions and local businesses. Cybercriminals often leverage social engineering techniques to steal personal and banking information.

Chilian, cybercriminals often target businesses and government institutions through ransomware attacks and data breaches, taking advantage of weak cybersecurity measures.

Colombian cybercriminals are known for executing business email compromise (BEC) schemes and intercepting and redirecting payments by impersonating legitimate organizations.

Paraguay has witnessed an increase in crypto-jacking incidents and fraudulent cryptocurrency schemes, driven by a growing interest in digital assets. These scams frequently exploit unsuspecting investors.

Cybercriminals actively engage in e-commerce fraud and selling counterfeit goods online in **Peru.**

Uruguay has experienced a rise in financial fraud, particularly through cloned payment cards to withdraw cash from ATMs.

Economic instability in **Venezuela** has fueled gift card fraud and cryptocurrency scams, often targeting victims abroad.

Finally, cybercriminals commonly use social media platforms in **Bolivia** to execute scams and identity theft schemes.

4.5 Asian Countries



The geographic distribution of cybercriminal activity in the Asian region varies considerably due to significant differences in terms of economic development, internet penetration, digital infrastructure, and regulatory environments. Moreover some countries are more prepared than others due to a better cybersecurity culture and development.

Cybercriminal activities in **China** encompasses a range of illicit activities, including hacking, online fraud, and data breaches, both within the country and beyond its borders, as well as industrial espionage, targeting intellectual property and government systems around the world. Les competence techniques des hackers Chinois sont generalement eleve utilisant un certain niveau de sophistication

Japan and South Korea are rather the major sources of cybercrime. Due to their high level of digitalization and wealth, they are often targeted by ransomware and phishing attacks. These countries have robust cybersecurity measures but face persistent threats.

India is a source and target of cybercrime, with a growing number of hacking groups and financial fraud schemes. Large-scale attacks target critical infrastructure, banks, and e-commerce platforms. In **Pakistan,** cybercriminal operations often focus on fraud, phishing, and politically motivated attacks. Cross-border cyberattacks with India are a notable aspect.

Malaysia, Indonesia, and Vietnam are emerging hubs for cybercriminal activities due to weaker cybersecurity frameworks and rapid digitalization. Common activities include phishing, ransomware, and digital fraud. Indonesia has probably the highest rate of scams and phishing in the region. The **Philippines** is known for online scams and fraud targeting victims from all over the world. The country hosts cybercriminal call centers and fraudulent activities related to financial scams.

Finally, regarding **Singapore**, despite the Interpol cyber center and strong development of the cybersecurity culture, the country is seen as a victim rather than a source due to its wealth and role as a financial center.

5. Conclusion

As this paper shows, cybercrime is a complex phenomenon involving many social, economic, cultural, psychological and technological factors. As new technologies emerge, cybercriminals use them to their advantage while governments, cyber authorities, and police services worldwide are constantly on alert. Cybercriminals are willing to circumvent security systems for financial gain, challenges, or simply for their ego. They know very quickly how to adapt to the new defense systems put in place by companies and institutions. Cybercrime presents many challenges, and cybercriminals are often one step ahead of security authorities. In the years to come, governments will, therefore, have to try to reverse this trend by anticipating and better managing cyber threats, whatever they may be, by using artificial intelligence and other technologies useful in the fight against increasingly numerous and sophisticated cyber threats.

6. About The Author



I am a cyber intelligence expert who has worked in various environments over the past ten years, including academia, high-tech, military, and law enforcement. My field of expertise is cyber intelligence, including strategy, collection, research, analysis, and leading Cyber HUMINT operations on criminal and terrorist activities within cyberspace. I have trained many civilian analysts and Military and Law Enforcement officers on the Deep and Dark Web environments, Cyber intelligence collection, and Cyber HUMINT operations.