RedHot Cyber

WWW.REDHOTCYBER.COM

Cybersecurity is about sharing. Recognize risk, combat it, share your experiences, and incentivize others to do better than you.

From Cybercrime to Cyber Organized Crime (COC)

Edited by Edoardo Faccioli

DARKLAB

RHC INTELLIGENCE LABORATORY

DARKLAB IS A SUBGROUP OF THE RED HOT CYBER COMMUNITY SPECIALIZING IN CYBER THREAT MONITORING. Dark Lab was established with the main goal of spreading knowledge about cyber threats to improve the country's digital awareness and defenses.

INTRODUCTION

Edoardo Faccioli

Cybercrime represents a constantly expanding universe, capable of attracting not only the interest of individual computer-savvy hackers, but also of traditional criminals and well-structured organizations with complex and large-scale objectives.

I decided to write this report to provide a detailed overview of the current state of cybercrime, analyzing how organized crime and mafias also exploit this context to increase their power and expand the boundaries of their activities, both territorially and virtually.

In the first part, we will examine the underground environment of the web, where multiple illicit activities can be found: from drug and narcotics dealing to child pornography and scams of various kinds. In the second part, we will focus on the phenomenon of Cyber Organized Crime (COC), analyzing the groups that have attracted the most law enforcement attention. We will conclude by exploring how social networks represent a powerful tool for mafias, enabling them to build consensus, especially among young people.

INDEX OF CONTENTS

PREFACE

The growing presence of the Internet in our lives has fostered the development of criminal actions that have been adapted and perfected by new technologies.

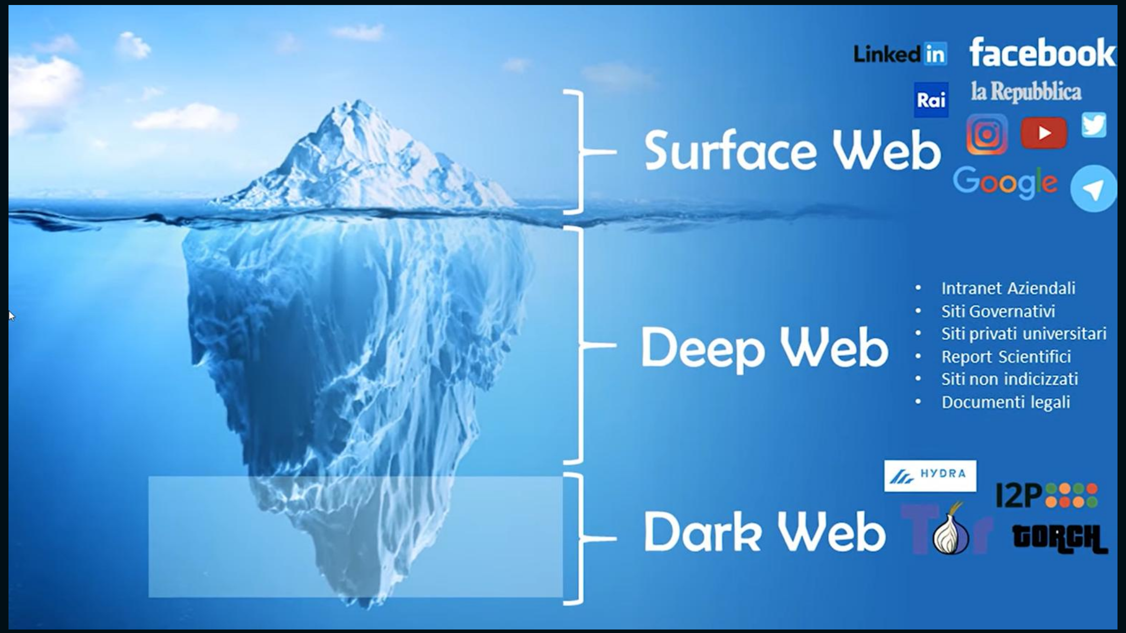
Surely we have all, at least once, heard of the Deep Web and Dark Web, but what exactly are these two realities, and what lurks within these more “hidden” and “secret” sections of the web?

The Deep Web represents the part of the Internet where URLs or site addresses are not indexed by common search engines, such as Google or Bing. Despite this, it is easily accessible through common browsers, provided you know the exact addresses.

The Dark Web, on the other hand, constitutes an even darker section, accessible only through specific tools such as TOR or I2P. This part of the Web is designed to ensure anonymity and privacy. Here, too, accessing web portals requires knowing the correct addresses.

The rise of black markets on the web, along with the increasing prevalence of tools for using and investing in cryptocurrencies, has attracted the interest of organized crime, both Italian and international.

Below we present an image that illustrates how vast these two often unexplored realities of the Web can be.



Specifically on this darkness, particularly on the Dark Web, designed to ensure confidentiality and anonymity, that many of the major criminal activities take shape. These include fraud, scams (of a romantic or financial nature), theft, the sale of illegal materials (sensitive and personal information, credit cards, drugs, and weapons), and the dissemination of child pornography. These activities often require money laundering operations and make extensive use of cryptocurrencies, a growing industry.

As early as the second half of 2022, the DIA (Anti-Mafia Investigative Directorate, in italian Direzione Italiana Antimafia), in its semi-annual reports, highlighted the links between cybercrime and mafias. The latter, which have always been adept at adapting and exploiting new technologies to increase their profits, have found the Dark Web and the possibility of making payments in cryptocurrencies-with no geographic limits and reduced controls-an ideal opportunity to expand, collaborate with other criminal groups, and significantly increase their earnings.

One phenomenon that should not be underestimated is the steadily growing phenomenon of ransomware, which generates ever-increasing profits from ransom demands. Recent international law enforcement operations, such as the famous Operation Cronos, have exposed the sophisticated organization of these criminal networks, which are capable of handling huge flows of money with great efficiency.

This scenario highlights how technological evolution represents not only an asset but also a significant challenge to global security. It is important to understand that cybercriminals, increasingly, do not act alone, but are recruited or become collaborators with large, well-structured organizations that have far-reaching criminal objectives.

THE SHADOW CONE

How It Is Exploited By Cybercrime.

Within the Deep Web, and particularly the Dark Web, are numerous web portals dedicated to the buying and selling of illicit material. The use of cryptocurrencies, which makes it possible to cross national borders to trade goods and services without financial intermediaries, coupled with the TOR system, designed to ensure privacy and anonymity, has undoubtedly fostered the growth of these illegal markets. But let's look more specifically at what criminals can find or offer for sale on these web portals.

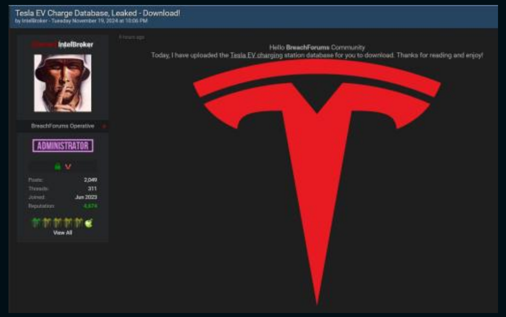
Research shows that cyber crime is basically a transposition of traditional crime into the cyber domain. The illegal markets we will discuss range from identity theft to the sale of illegal materials, such as unregistered weapons, false documents, stolen credit cards, hacking and extortion activities, financial fraud, child pornography, underground gambling, and last but not least, money laundering.

It is good to remember that in any case in this "shadow" area of the Web there are no guarantees or securities therefore everything you find or read should always be viewed very carefully and critically thought through.

When one first enters the Dark Web, the first thing one usually explores are the forums. Many of these are freely accessible, while other, more niche ones, where the material and discussions are decidedly more "black" and "underground," require payment of a membership fee, which can range from $100 to $500. Alternatively, access may be granted through a "recommendation" or "guarantee" from a member who is already a member and well-connected in the community.

Forums, in their structure, are very similar to each other. They usually feature a general chat and a section devoted to general topics, ranging from the news of the day to comics, such as anime and music, to technology topics such as programming. Another section is reserved for so-called "Leaks," where you can find posts containing data of various kinds, such as accounts, databases, logs of various kinds, and even cases of doxing, which is the sharing of private information about people or companies.

Many of these platforms also offer Escrow services or sections dedicated to buy and sell the data mentioned earlier, facilitating the exchange of money and materials among members.



Tesla EV Charge Database, Leaked - Download!
by IntelBroker - Tuesday November 19, 2024 at 10:06 PM

IntelBroker

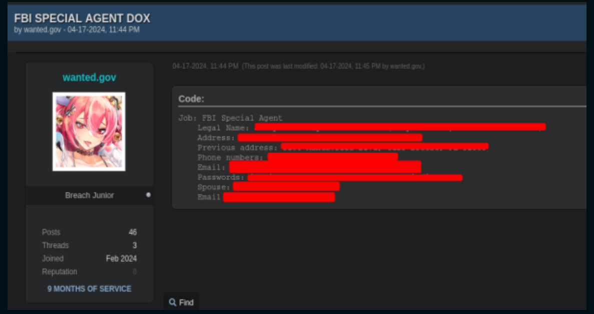
BreachForums Operative

ADMINISTRATOR

Posts: 2,049
Threads: 311
Joined: Jun 2023

View All

Hello **BreachForums** Community
Today, I have uploaded the Tesla EV charging station database for you to download. Thanks for reading and enjoy!



FBI SPECIAL AGENT DOX
by wanted.gov - 04-17-2024, 11:44 PM

wanted.gov

Breach Junior

Posts 46
Threads 3
Joined Feb 2024
Reputation 0

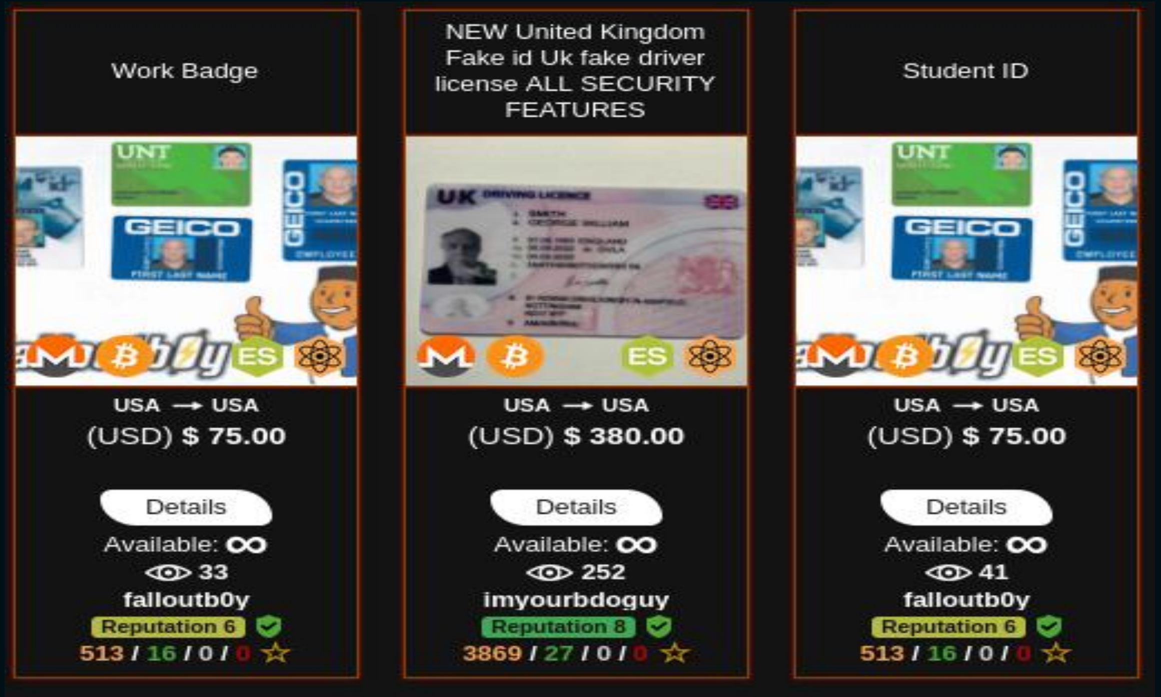
9 MONTHS OF SERVICE

04-17-2024, 11:44 PM (This post was last modified: 04-17-2024, 11:45 PM by wanted.gov.)

Code:

```
Job: FBI Special Agent
    Legal Name: [redacted]
    Address: [redacted]
    Previous address: [redacted]
    Phone numbers: [redacted]
    Email: [redacted]
    Passwords: [redacted]
    Spouse: [redacted]
    Email [redacted]
```

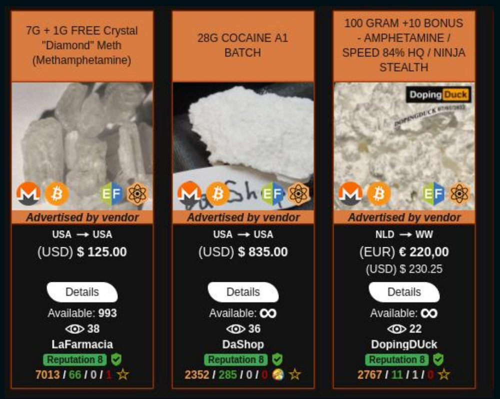
Find



Work Badge
USA → USA
(USD) $ 75.00
Details
Available: ∞
33
falloutb0y
Reputation 6
513 / 16 / 0 / 0 ☆

NEW United Kingdom Fake id Uk fake driver license ALL SECURITY FEATURES
USA → USA
(USD) $ 380.00
Details
Available: ∞
252
imyourbdoguy
Reputation 8
3869 / 27 / 0 / 0 ☆

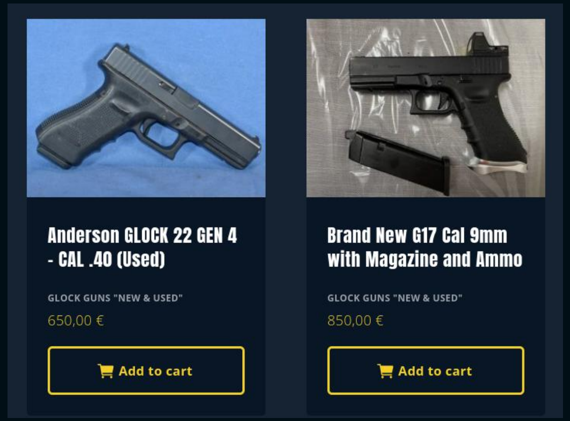
Student ID
USA → USA
(USD) $ 75.00
Details
Available: ∞
41
falloutb0y
Reputation 6
513 / 16 / 0 / 0 ☆



7G + 1G FREE Crystal "Diamond" Meth (Methamphetamine)
Advertised by vendor
USA → USA
(USD) $ 125.00
Details
Available: 993
38
LaFarmacia
Reputation 8
7013 / 66 / 0 / 1 ☆

28G COCAINE A1 BATCH
Advertised by vendor
USA → USA
(USD) $ 835.00
Details
Available: ∞
36
DaShop
Reputation 8
2352 / 285 / 0 / 0 ☆

100 GRAM +10 BONUS - AMPHETAMINE / SPEED 84% HQ / NINJA STEALTH
Advertised by vendor
NLD → WW
(EUR) € 220,00
(USD) $ 230.25
Details
Available: ∞
22
DopingDUck
Reputation 8
2767 / 11 / 1 / 0 ☆

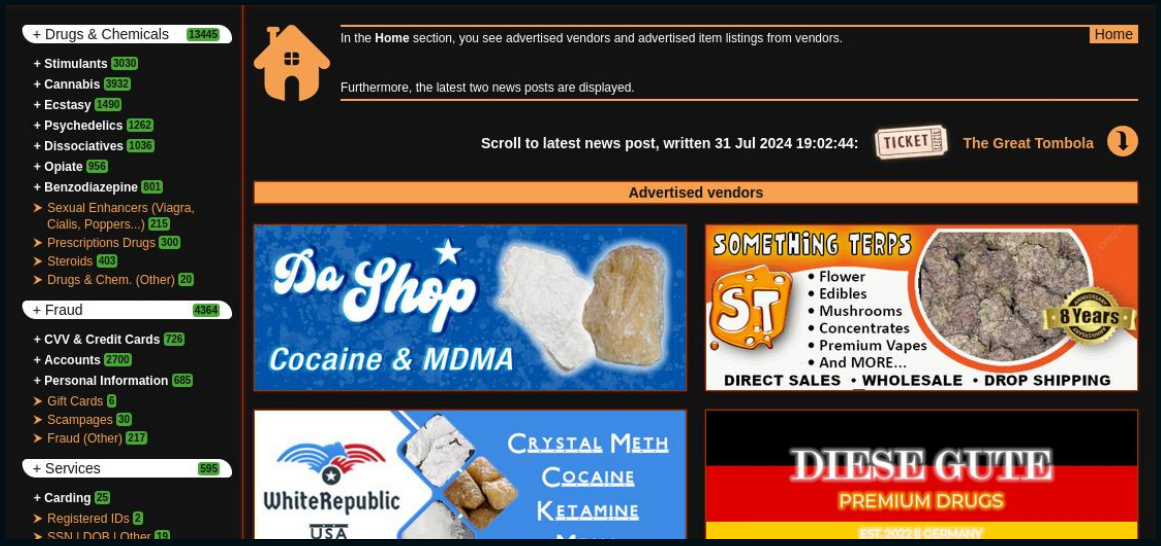


Anderson GLOCK 22 GEN 4 - CAL .40 (Used)
GLOCK GUNS "NEW & USED"
650,00 €
Add to cart

Brand New G17 Cal 9mm with Magazine and Ammo
GLOCK GUNS "NEW & USED"
850,00 €
Add to cart

Darknet Markets, on the other hand, go beyond selling information, typical of the "Leaks" sections, by offering a wide range of illegal materials, including drugs, weapons, stolen credit cards, and fake documents.

Payments take place almost exclusively in cryptocurrencies, such as Bitcoin, Ethereum, or Monero, to ensure greater anonymity and security in transactions. Unlike forums, where users can publish posts freely, in Darknet Market listings are published directly by the market itself, maintaining centralized control over content and transactions.



+ Drugs & Chemicals 13445
- + Stimulants 3030
- + Cannabis 3932
- + Ecstasy 1490
- + Psychedelics 1262
- + Dissociatives 1036
- + Opiate 956
- + Benzodiazepine 801
- ➤ Sexual Enhancers (Viagra, Cialis, Poppers...) 215
- ➤ Prescriptions Drugs 300
- ➤ Steroids 403
- ➤ Drugs & Chem. (Other) 20

+ Fraud 4364
- + CVV & Credit Cards 726
- + Accounts 2700
- + Personal Information 685
- ➤ Gift Cards 6
- ➤ Scampages 30
- ➤ Fraud (Other) 217

+ Services 595
- + Carding 25
- ➤ Registered IDs 2
- ➤ SSN | DOB | Other 19

Home

In the **Home** section, you see advertised vendors and advertised item listings from vendors.

Furthermore, the latest two news posts are displayed.

Scroll to latest news post, written 31 Jul 2024 19:02:44: TICKET The Great Tombola

Advertised vendors

Forum and Darknet Market generate a profitable and growing market. According to the report carried out by **Chainalysis** cryptocurrency movements related to the buying and selling of services offered by Darknet Markets reached $1.7 Billion in 2023 signaling growth compared to 2022 when the infamous hydra market closed.

Within the Darknet Markets, the phenomenon of carding, or the buying and selling of stolen/cloned credit cards, is developing rapidly. Criminals obtain card data through traditional or hacking techniques, such as phishing, malware, or database theft, and resell them on the dark web. These cards can be used for online transactions or money withdrawals, even requiring the physical card to be shipped.

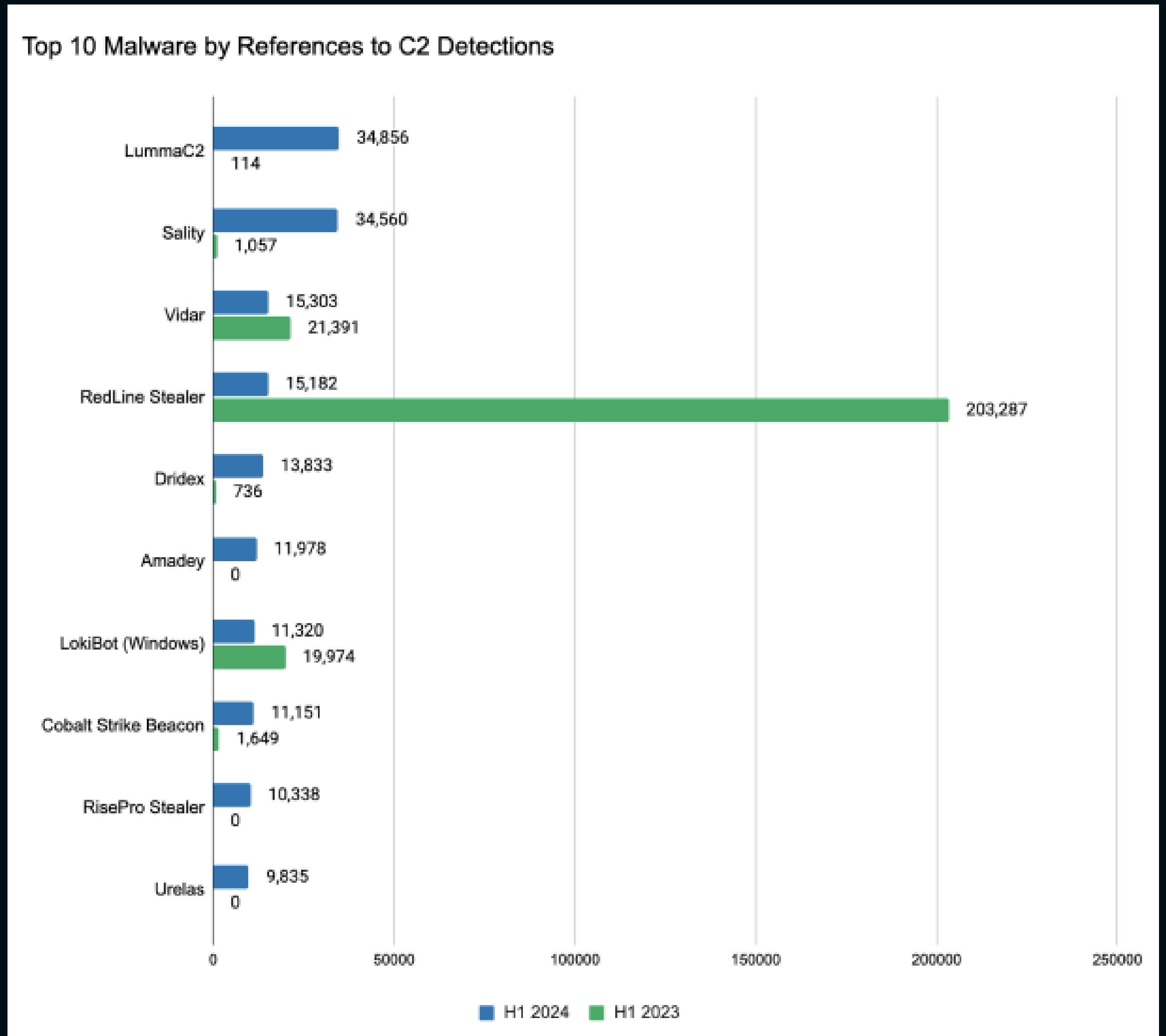
According to a 2023 NordVPN report, which analyzed 6 million stolen cards, the average selling price for a stolen card is $10.08. The most expensive cards are Danish cards, with an average price of $11.54, while Italian cards rank third to last, with an average value of $8.98.

As with other criminal activities on the dark web, carding exploits cryptocurrency payment methods, making it extremely difficult to track transactions.

Malware, Ransomware & Infostealer

Within the dark web, the buying and selling of sensitive information and data stolen from victims' electronic devices by malware known as Infostealers is becoming increasingly popular. This malicious software, once installed on the target device, extracts as much information as possible, which is sent in the form of logs to a Command and Control (C2) server. From there, the data is distributed to dedicated portals or Telegram channels accessible to the criminals upon payment of a monthly or annual subscription, with costs of several hundred dollars that can vary depending on the type of service requested. This operating model is known as MaaS (Malware as a Service).

According to a recent report by Recorded Future on malware trends, in the first half of 2024 (H1 2024), LummaC2 surpassed RedLine in terms of the prevalence of C2 servers detected, taking the top spot among malware of this type.



Top 10 malware (Fonte Recorded Future)

The ease of use and accessibility of these tools allow even the least technologically savvy criminals to steal sensitive information from numerous victims and then use it for different illicit purposes.

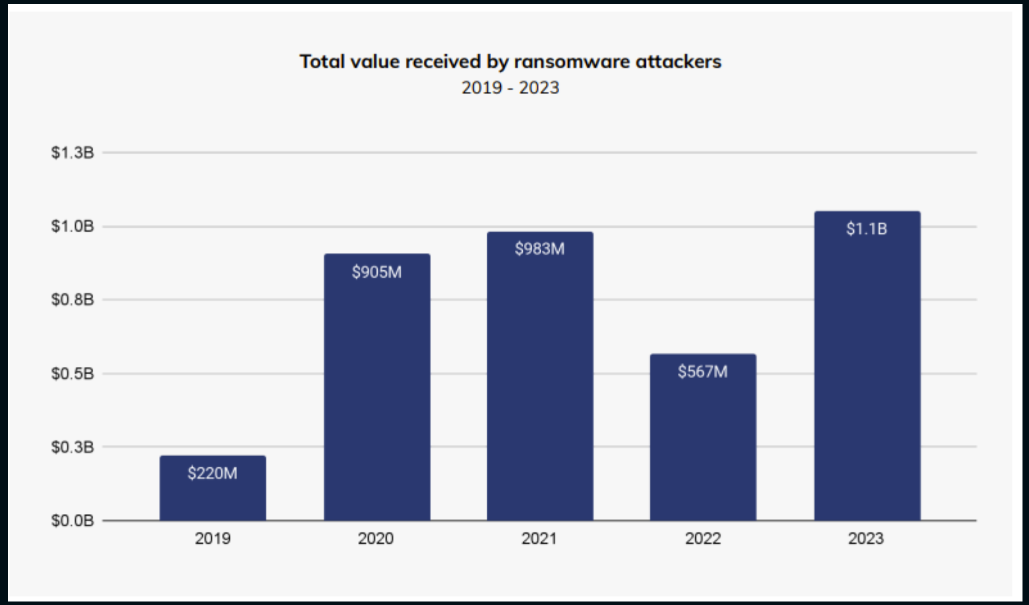
Ransom Gangs are achieving remarkable success in spreading ransomware, achieving significant results. The victims of a ransomware attack can belong to any industry: financial institutions, hospitals, universities, and many other organizations. These criminal communities are often well-organized and structured, with numerous affiliates physically executing the attacks.

When a victim is hit by ransomware, they end up with their technology systems encrypted, rendering the data within them unusable. The criminal's goal is to force the victim to pay a ransom to obtain the decryption key needed to restore access to the data and systems. However, many attacks include a data exfiltration phase prior to encryption, allowing attackers to engage in double extortion: in addition to the ransom for decryption, they may demand an additional payment to prevent public dissemination or sale of the stolen sensitive data.

This strategy makes ransomware attacks particularly devastating, both in terms of the operational impact and the legal and reputational implications for the affected organizations.

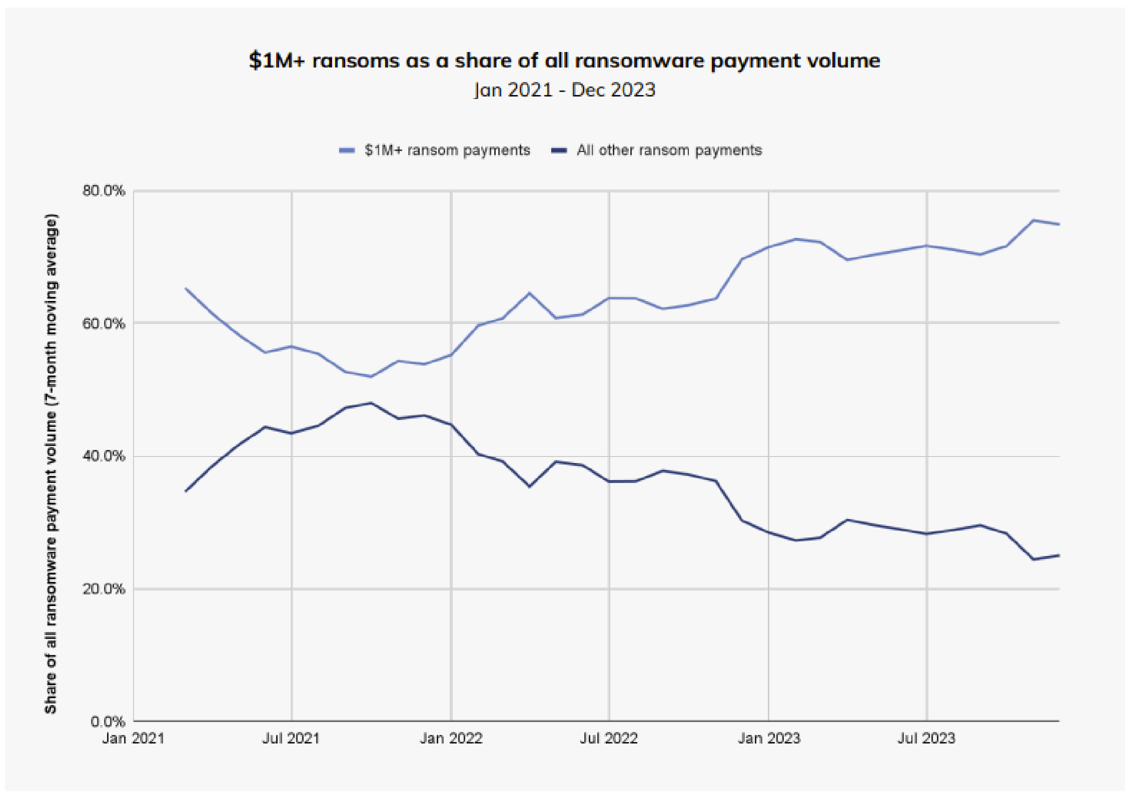
The ransomware phenomenon represents one of the most lucrative and problematic areas of cybercrime, characterized by an immediate and tangible impact because of its nature and the ways in which it spreads and affects victims. Ransom demands generate a great deal of stress and, in recent times, are becoming increasingly high. This is because the attacking groups carefully inform themselves and often adjust the amount demanded based on the turnover of the targeted company.

According to Chainalysis' latest annual report, which analyzes the ransomware phenomenon in 2023 and previous years, there is a growing trend, with economic volumes exceeding $1 billion.



The value of ransoms obtained by ransomware cybergangs (source chainalysis)

Such a large volume of money has also been made possible by the strategy of attacking large, high-turnover companies, allowing attackers to demand ransoms that often exceed $1 million.



Source - Chainalysis

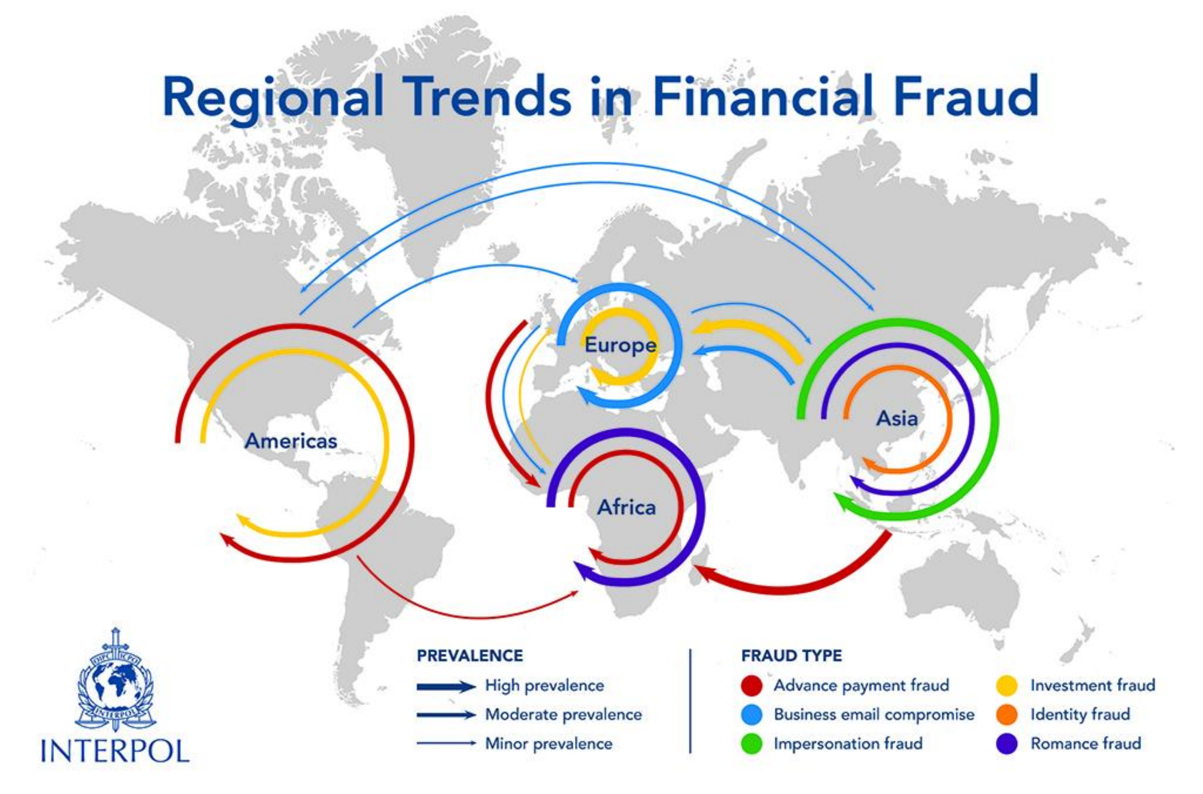
BEYOND THE UNDERGROUND

SCAM, Human Trafficking and Exploitation, CSAM (Child Sexual Abuse Material) - Child Pornography

Exposure to the Internet and the ease with which we can all access and use it has facilitated the expansion and growth of online scams, commonly known as **SCAM**.

These scams can take many different forms, and every day criminals devise new techniques to deceive their victims. The scam industry is constantly expanding, aided by the rise of identity theft, which allows scammers to gather a great deal of information about their victims before implementing their strategy. In addition, real guides and tutorials are available on the dark web explaining how to carry out scams successfully.

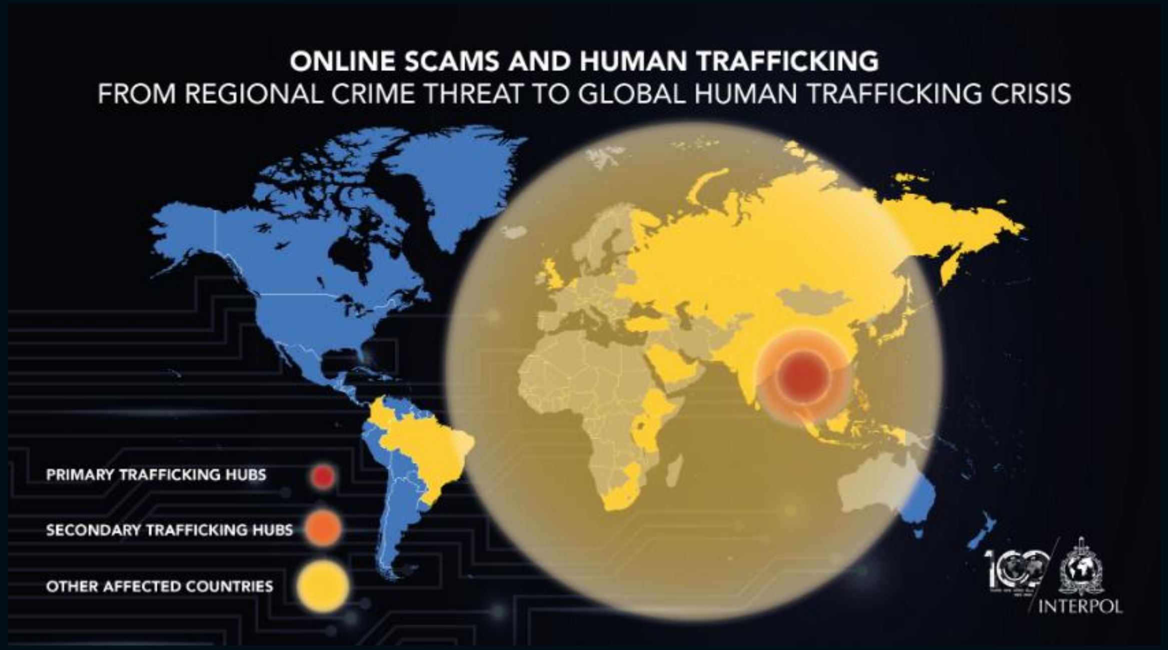
According to Chainalysis' report, the total economic value of this criminal market exceeded $4 billion by 2023. Among the fastest-growing types of scams are romantic and financial scams, both in traditional and blockchain-based finance. In addition, more common scams continue to be prevalent, such as those related to online purchases of goods, fake job offers, blackmail, and all those related to social engineering techniques that can also be implemented by telephone.



Source - Europol

The link between online scams, particularly fake job offers and romance scams, and human trafficking has become increasingly evident, with a significant increase in this type of crime.

According to Interpol, as early as 2023 a global security warning has been issued due to the rapid growth of this phenomenon. More and more people, attracted by seemingly lucrative job offers, agree to move to other countries with paid travel, guaranteed housing and the false promise of a better future. However, once they arrive at their destination, they find themselves trapped and forced to work in technology centers dedicated to online and telephone scams.


ONLINE SCAMS AND HUMAN TRAFFICKING
FROM REGIONAL CRIME THREAT TO GLOBAL HUMAN TRAFFICKING CRISIS
PRIMARY TRAFFICKING HUBS
SECONDARY TRAFFICKING HUBS
OTHER AFFECTED COUNTRIES
INTERPOL

Source – Europol

Traffickers use technological tools such as social networks, dating sites, and job offer portals to lure victims, furthering the spread of the phenomenon known as e-trafficking. People who fall into these traps not only end up in hubs dedicated to scams, but often, once they arrive in the country indicated by the criminals, they are forced to repay the alleged debt incurred for travel expenses. This debt becomes the pretext for forcing them into slave labor or, in many cases, prostitution.

One of the most widespread crimes that Italian law enforcement agencies try to combat on a daily basis is that related to child pornography crimes, which are very present on the Web.

According to Europol, child pornography materials can be classified mainly into two categories:

1. **Materials found on networks that promote privacy and anonymity, such as the TOR network.** Numerous sites and forums dedicated to the exchange of Child Sexual Abuse Material (CSAM), often distributed for free or through payments in cryptocurrencies such as Bitcoin or Monero, can be found on these platforms. Groups on Telegram used for sharing this material are also common.
2. **Live streaming of child abuse, in which victims, often lured online, are forced to spend a lot of time in front of a camera to perform activities at the request of or imposed by their exploiters.**

To obtain this type of material and be able to sell it, criminals use a practice called online ***grooming***. This consists of a process of seducing and grooming the minor, which involves:

- Victim selection;
- The building of trust through apparent friendship and manipulation;
- The collection of as much information as possible about the victim, both online and offline, in order to deceive the victim.

The ultimate goal is to obtain child pornography through direct online exchanges or, in the worst cases, to meet the victim physically to sexually abuse him or her.

The economics related to **Child Sexual Abuse Material (CSAM)** is not easy to analyze, as it is mainly based on the exchange of material rather than direct payment. However, there has also been a growing use of cryptocurrencies in this area, which provide a high level of privacy in transactions, making law enforcement investigations increasingly complex.

According to analysis conducted by Chainalysis and IWF (Internet Watch Foundation), prices for purchasing child pornography generally range from $10 to over $70. The trend shows an increased use of low-cost material, however, accompanied by an increase in the overall amount of content available.

More than 275,000 URLs containing child abuse material were reported in 2023, an 8 percent increase from 2022. This figure underscores the continued growth of the phenomenon, requiring ever-increasing efforts to counter the spread and ensure the protection of victims.

TOWARD THE COC

Expansion into the cyberspace of Cyber Organized Crime

Mafia organizations are constantly evolving and effectively adapting to the context in which they operate. Today, mafias have profoundly changed the way they operate, seeking to infiltrate the social fabric in an increasingly silent but equally effective way, pursuing their own economic and power interests.
To integrate themselves into the country's business fabric, criminal organizations use capital obtained through traditional or more modern illicit activities, such as those related to cybercrime. This evolution has fostered an increasing interaction between organized crime and new technologies.

Italian mafia, drug trafficking and gambling.

According to DEA reports, as early as 2023 it had emerged that mafia organizations were exploiting new technologies for drug trafficking, which continues to be the main business in terms of revenue for these criminal entities. Against this backdrop, Italian mafias could further expand their international drug trafficking network, which is already very extensive due to the presence of numerous affiliates in drug production and transit countries. In particular, there has been an increase in trafficking from West African countries.

In addition, the extremely high profits from drug trafficking require an expansion of money laundering systems. For this reason, an activity increasingly used by criminal organizations is unregulated and illicit **online gambling**. This practice is facilitated by the possibility of setting up *"cards"* companies with registered offices in tax havens, which allow both money laundering and further illicit gains.

Back in 2018, the District Anti-Mafia Directorate had coordinated an operation conducted by the State Police, known as "Operation Bruno", which led to the arrest of 13 individuals in both Italy and Romania accused of crimes ranging from criminal conspiracy to abusive access to computer systems to laundering proceeds from massive phishing campaigns. This operation highlighted how the 'ndrangheta was also beginning to move into the field of cybercrime.

Online Fraud and Albanian Organized Crime.

The Albanian Mafia also has narcotics trafficking as its main criminal activity. These are well-equipped and structured organizations that base their strength on ties of trust and kinship. These mafias have contacts both in Italy and abroad, which allows them to expand rapidly outside their home country. Criminal activities in the field of immigration and human trafficking have also been reported. However, the aspect that has brought the Albanian mafia closest to cybercrime concerns **online and telephone scams**.

An operation called *"Dream Earnings"* coordinated between Italian and Albanian police, was concluded in 2023, dismantling a criminal organization of more than 50 people. The scam consisted of contacting victims by phone through call centers located in Tirana, Albania, and convincing them to invest sums of money in fraudulent financial proposals, promising quick gains.

The criminals were also very adept at using *social engineering* techniques, which allowed them to tune in to their victims and gain their trust. In some cases, they were even able to work remotely on the targeted people's computers, increasing the effectiveness of their frauds and amplifying the economic damage. Criminals also converted the victim's money into *cryptocurrencies* so they could not be easily tracked and facilitate transfers from different wallets. The total value of the amounts moved is estimated to be around several tens of millions of euros.

BLACK AXE and CyberCrime

The Nigerian mafia has also approached cybercrime, establishing itself in various European and non-European contexts. In addition to conducting the classic illicit activities typical of mafia organizations, such as narcotics trafficking, smuggling, extortion, prostitution, and kidnapping, this mafia is able to generate huge profits through online scams. These frauds range **from the most common financial scams to sophisticated romance scams**, often carried out through dating platforms.

Precisely because their scams are not limited by geographic boundaries, Interpol has identified the Black Axe group as a major criminal actor responsible for computer fraud and other cybercrime-related activities. To understand the extent and influence of this group, one can refer to Operation *Jackal III*, conducted by Interpol: a campaign that involved 21 countries spread over 5 continents, leading to 300 arrests, the identification of 400 suspects, and the blocking of more than 720 bank accounts used for criminal activities.

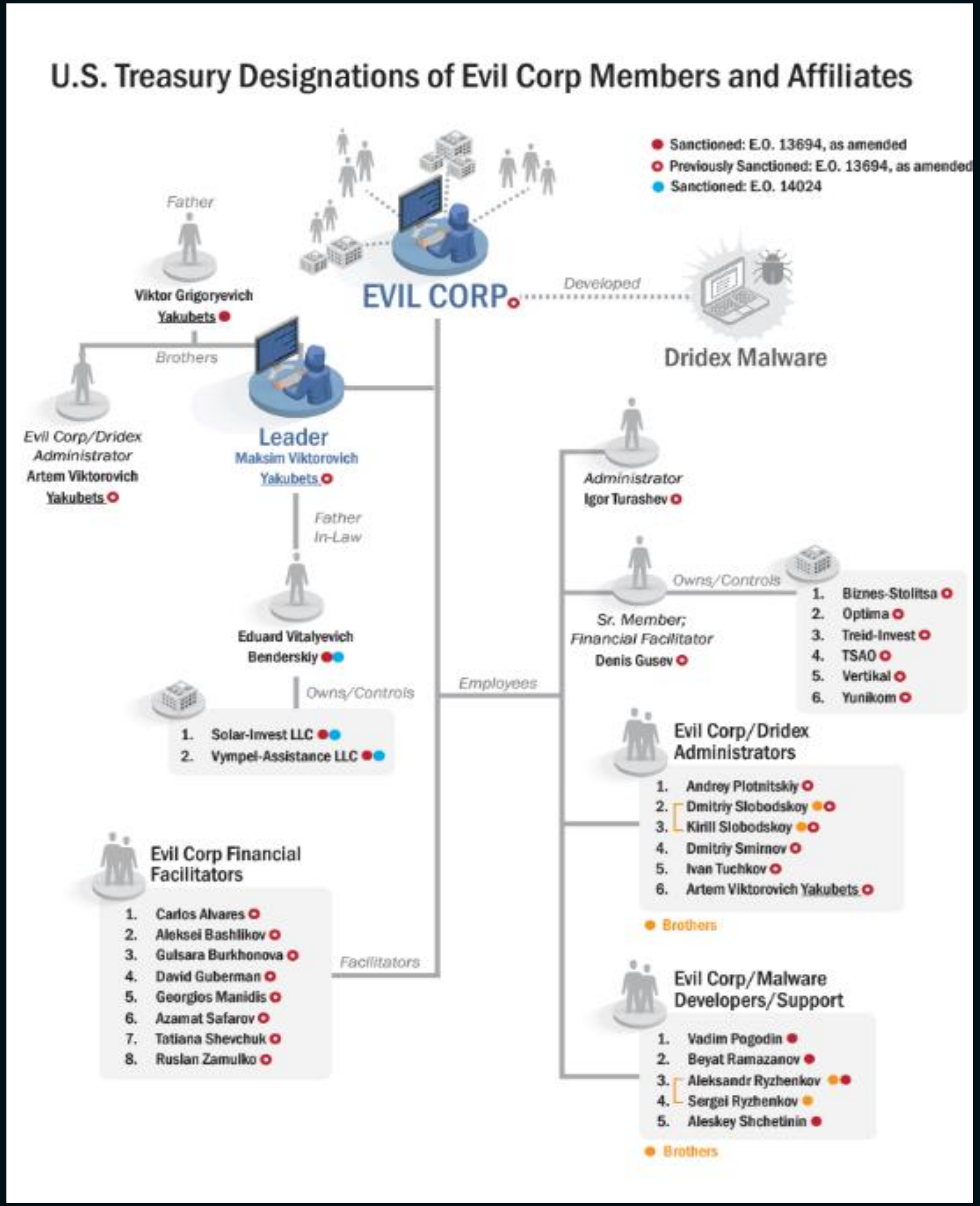
The volume of online fraud from West Africa is steadily increasing. These organizations manage to launder large sums of money through a sophisticated money laundering network, which includes numerous Money Mules distributed in various countries around the world. The ***Money Mules***, by opening bank accounts in their own names, allow the transfer of funds without arousing suspicion to either the victims or the lending institutions.

Techniques used to move laundered money include the purchase of valuable assets, such as cars, and the increasing use of cryptocurrencies, which offer anonymity and difficulty in tracking.

Ransomware Gang & Threat Actor

Ransomware groups and organizations specializing exclusively in cybercrime are also becoming increasingly large and sophisticated. These groups, while not sharing the typical characteristics of traditional mafias, operate with a corporate-like structure, aiming to maximize their "profits." They possess a well-defined hierarchy and sophisticated web portals that allow them to communicate with affiliates, provide advanced technological tools, and manage criminal operations in a coordinated manner.

Shining a light on the inner workings of these criminal groups was Operation Cronos and the sanctions applied against the organization known as Evil Corp and its connection to Lockbit. These groups plan their attacks very carefully, analyzing their targets in detail and following a methodical approach at every stage of the attack.



source: U.S. Department of the treasury

Their structures are organized in such a way as to clearly divide the tasks: there are figures in charge of managing online communities, "*mediators*" who facilitate coordination with victims and other organizations, highly competent developers who design and implement malware, and finally money laundering experts.

The money laundering system of these groups makes use of advanced technologies in the field of decentralized finance (DeFi) and tools such as cryptocurrencies, but also leverages traditional Money Mule networks, which ensure the movement of funds without arousing suspicion.

Social Media & Mafia

The mafias, in addition to transforming the spaces in which they operate, are also radically changing the way they promote and recruit new members. Through social networks, these criminal organizations exploit powerful tools to achieve various goals: recruiting new affiliates, flaunting wealth and power, intimidating opponents and, at the same time, fueling a glamorous imagery that is particularly attractive to the new generations.

Platforms such as YouTube, Instagram, Facebook and TikTok, each with its own peculiarities, allow mafias to adapt their messages to the audience and context. These digital channels therefore become strategic vehicles for:

Building a digital Criminal identity

Criminal organizations promote an image of success, wealth, and power through the publication of content that showcases money, luxury, and coveted lifestyles. This type of communication aims to build a real digital "brand identity", capable of attracting and seducing young people.

source: Fondazione Magna Grecia “Le mafie nell’era digitale”

1. **Recruitment and sense of belonging**
   Sharing content that exhibits success and power aims to elicit a sense of belonging in viewers, facilitating recruitment and the affiliate process.

2. **Intimidating propaganda and control of power**
   Through social networks, mafias can spread intimidating messages and strengthen the perception of their control over the territory, combining the virtual world with the real one. This convergence of online and offline life helps to solidify their authority and prestige.

The strategic use of new technologies therefore allows mafias to amplify their power and influence, creating a digital ecosystem that supports them in their illegal activities and social control.

BIBLIOGRAPHY

- Semestral Reports DIA: https://direzioneinvestigativaantimafia.interno.gov.it/relazioni-semestrali/
- Report Crypto Crime 2024: https://go.chainalysis.com/crypto-crime-2024.html
- Report NordVPN: https://s1.nordcdn.com/nord/misc/0.71.0/vpn/brand/research-lab/payment-card-details-theft/Payment-card-research-report.pdf
- Report Recorded Future: https://www.recordedfuture.com/research/h1-2024-malware-and-vulnerability-trends-report
- Interpol SCAM: https://www.interpol.int/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology
- Interpol Human Trafficking: https://www.interpol.int/News-and-Events/News/2023/INTERPOL-issues-global-warning-on-human-trafficking-fueled-fraud
- CSAM Europol: https://www.europol.europa.eu/crime-areas/child-sexual-exploitation
- IWF: https://www.iwf.org.uk/annual-report-2023/trends-and-data/reports-analysis/
- DEA 2023: https://direzioneinvestigativaantimafia.interno.gov.it/wp-content/uploads/2024/06/Rel-Sem-I-2023.pdf
- Operation Bruno: https://www.poliziadistato.it/articolo/15265ac487b649954752027145
- Operation Dream Earnings: https://questure.poliziadistato.it/it/Pordenone/articolo/85264c241cb62df8327157748
- Interpol Jackal III: https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-operation-strikes-major-blow-against-West-African-financial-crime
- Operation Cronos: https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos
- Evil Corp Sanctions: https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos
- “Fondazione magna grecia Le mafie nell'era digitale”: https://fondazionemagnagrecia.it/wp-content/uploads/2023/10/12000.31Ravvedutoebook.pdf