Swascan

TINEXTA GROUP

DarkWeb Analysis 2022

www.swascan.com

info@swascan.com

SUMMARY

ABOUT US

Swascan is a Cyber Security Company founded by Pierguido Iezzi and Raoul Chiesa. Since October 2020, Swascan srl has been an integral part of the Tinexta S.P.A. Group.

Swascan

Swascan is a cyber security company founded by **Pierguido Iezzi** and **Raoul Chiesa**. It is the first Italian cyber security company to own a **cyber security testing** and **threat intelligence platform,** as well as a cyber security research centre of excellence that has received several national and international awards from the most important players in the IT market and beyond. **Since October 2020, Swascan srl has been an integral part of the Tinexta Group,** becoming an active leader in the first national Cyber Security Center: not just one company, but an Italian group, a new national hub specialising in digital identity and digital security services.

Tinexta Group

A dynamic and rapidly expanding Group, **listed on the STAR segment of the Italian Stock Exchange.** The successor of Tecnoinvestimenti, Tinexta S.p.A. has always been there to support citizens, companies and public administration, promoting their growth and modernisation.
A leader in the field of advanced digitisation, it operates in four business areas via its subsidiaries: Digital Trust (Infocert, Sixtema, Visura), Cybersecurity (Swascan, Yoroi and its R&D division Corvallis), Credit Information & Management (Innolva, ReValuta) and Innovation & Marketing Services (WarrantHub, Co.Mark.

EXECUTIVE SUMMARY

No longer the preserve of industry insiders for at least a decade now, today more than ever, the dark web is a parallel world on the internet, operating under the premise of greater anonymity and a libertarian philosophy in terms of rules.

Obviously, you cannot access the dark web via a simple Google search. You need to use a special browser called TOR, where communication is encrypted and each node in the network only knows the previous and the next ones and no others. The Tor network consists of relays operated by organisations and individuals all over the world.

There are three types of relay in the Tor browser system:

- guard/middle relay;
- exit relay;
- bridge.

The structure of the Tor network still requires the IP addresses of Tor relays to be public. In turn, this facilitates blocking by governments, which blacklist the IP addresses of these public Tor nodes.

For this reason, many users connect via bridges: nodes that are not publicly listed as part of the Tor network, "in between" tools that are essential for circumventing censorship in countries that regularly block the IP addresses of all publicly listed Tor relays.

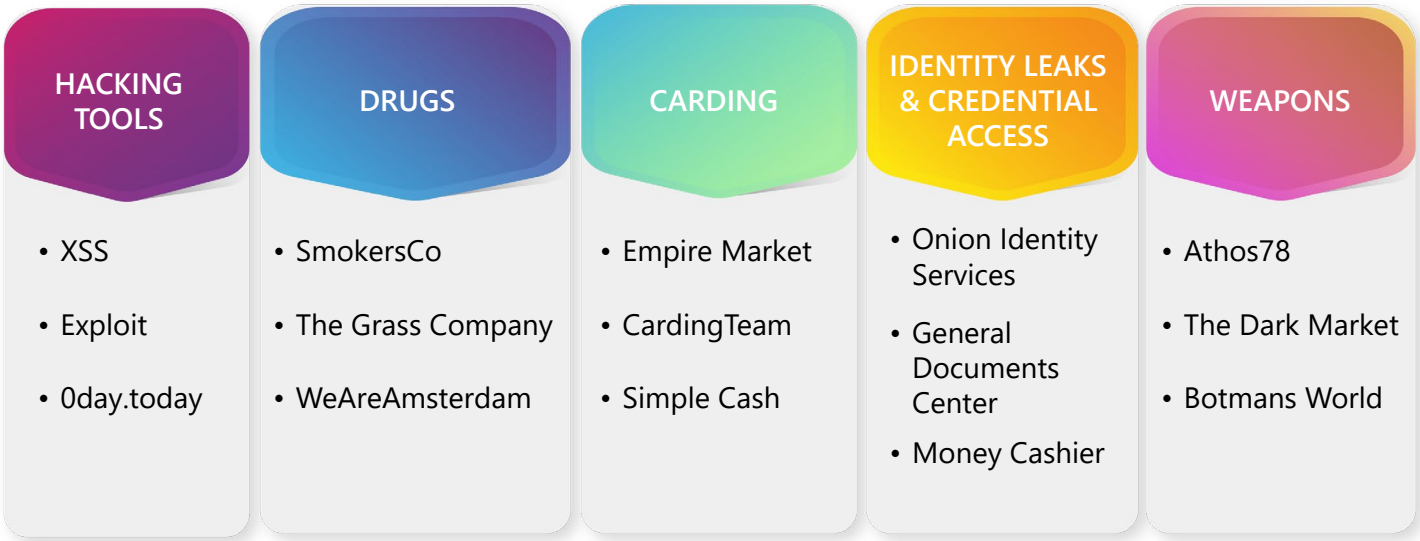
A level of anonymity that goes well with activities that require a high degree of confidentiality and secrecy - just like the buying and selling of stolen data.

The economy of this entity, in fact, revolves around black markets, veritable "illegal markets" offering a wide range of products and services, including a very large number of illicit substances, from marijuana to heroin, comprising a whole series of synthetic drugs and medication (antidepressants, stimulants, anti-psychotics, painkillers, sleeping pills, hormones etc.), up to and including the purchase of services such as hired killers and the sale of criminal hacking services (malware, ransomware, Command&Control renting etc.).

With all this in mind, the Swascan SOC analysed trends, product prices and payment methods used. The analysis draws conclusions about user behaviour in the dark web markets and the potential of these markets in the future. In particular, data were collected, through specific OSINT & CLOSINT investigations, on the top five best-selling substances and services on the dark web in 2022:

1. Hacking tools
2. Drugs
3. Carding
4. Identity leaks and credential access
5. Weapons

For each of these five categories, three markets were selected on the dark web selling the relevant products:



The methodological approach used was as follows:

1. Identification of the major dark web sites involved in the sale of the aforementioned services;
2. Identification and analysis of substances and services offered;
3. Clustering buyer-related information in terms of:
    - Geographical area
    - Supply and demand

THE CONTEXT

When talking about black markets, the first thing you probably think of is Silk Road, an online marketplace accessible under the Tor network via which a variety of mostly illegal products and services were sold, later becoming the world's largest drug market. The market operated successfully for almost two years under the leadership of "Dread Pirate Roberts", the pseudonym under which the owner hides, generating millions of dollars in revenue until 3 October 2013, when the site was shut down by the FBI and following the arrest of its alleged founder and director Ross William Ulbrich, from whose virtual wallet more than 26,000 bitcoins were seized, worth around $3.6 million. In early November 2013, the reopening of Silk Road was announced by the same pseudonym, welcoming users with the following message:

"it is with great joy that I announce a new chapter in our adventure. Silk Road has risen from the ashes and is now ready to welcome you."

Access requires registration: simply provide a username, password, transaction ID and solve a CAPTCHA to access the homepage and take advantage of all the services offered.

According to the FBI's criminal complaint filed in the trial of Ross William Ulbright, the Silk Road market was estimated to have nearly 150,000 buyers and almost 4,000 sellers (US v. Ross Ulbricht, 2013). The user base was predominantly located in the United States, but included individuals from all over the world. In addition to the possibility of buying illegal goods, the site provided a messaging feature that enabled buyers and vendors to interact and discuss the effects of the drug, how bitcoins were used, and give ratings to vendors. This turned the site not only into a haven for the free trade of smuggled goods, but a repository of information on a wide range of topics.

Nevertheless, although it has been dismantled, the sale of illegal goods on the dark web has not stopped.

Vendors (and the markets in which they operate) exploit the encryption and anonymity provided by the dark net to hide their illegal activities and evade law enforcement. Most of the time, transactions are conducted using cryptocurrencies to make it more difficult to track their earnings and further obscure their identities.

Alcuni fornitori sul Darkweb sono veri esperti di programmazione o cybersecurity che fanno fortun

Some vendors on the dark web are true programming or cyber security experts who make their fortunes selling malware and exploits that enable less sophisticated operators to launch powerful cyber attacks against corporate targets. Others are simply fraudsters, selling stolen personal accounts or sharing credentials at a bargain price.

Every marketplace on the dark web is an organised criminal enterprise that profits from the exchange of illegal goods and services. These markets are run by sophisticated groups that use state-of-the-art security techniques to conceal their identities.

In a matter of minutes, anyone can download the Tor browser, browse a marketplace on the dark web, create a vendor account and start selling illegal goods or services. Nevertheless, some marketplaces require vendors to apply via referral, provide proof of reputation from another marketplace, purchase a licence or provide a cash deposit. This is to ensure that only reputable vendors can operate.

Below are the product categories that can be found in these markets:

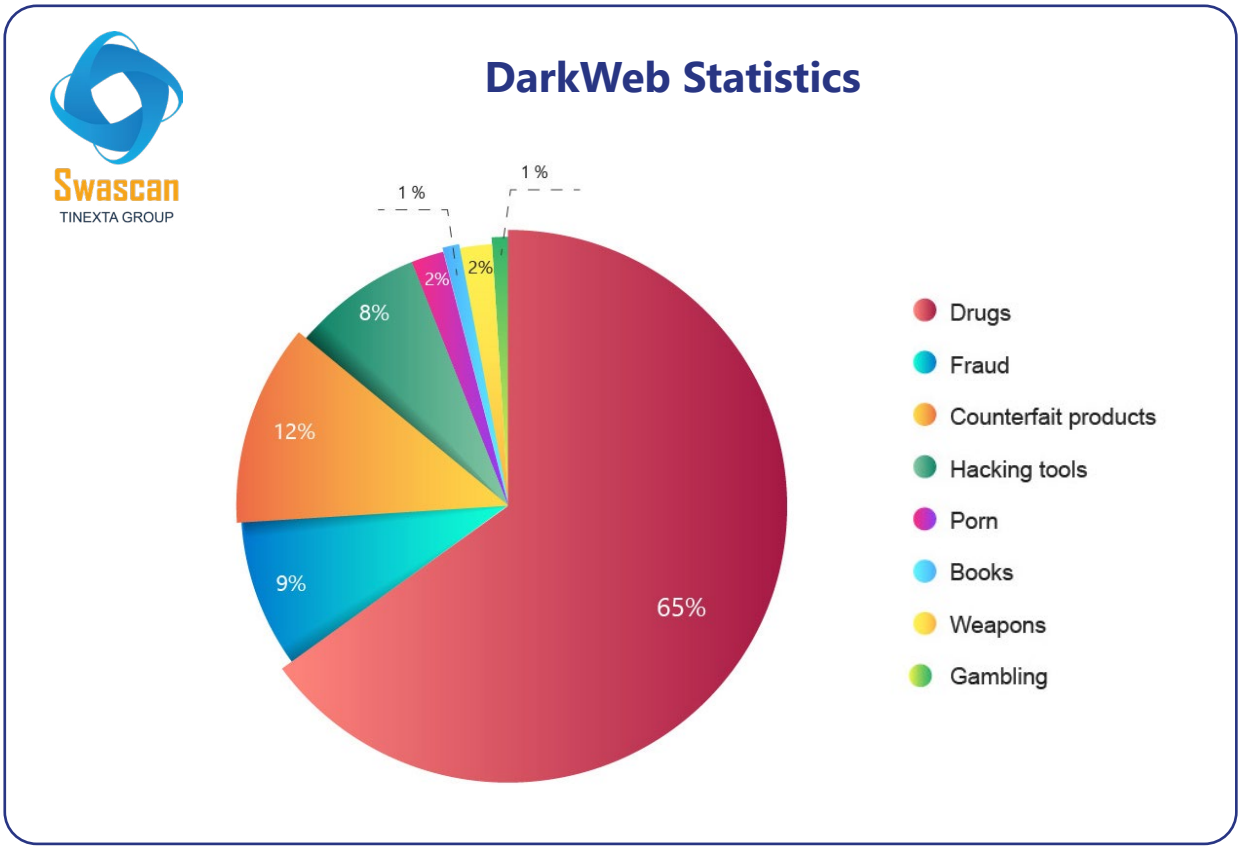
1. **Hacking, spam and phishing tools:** zero-day vulnerabilities, exploit kits, hacking tools, access to protected databases. These enable threat actors with minimal technical knowledge to launch effective cyber attacks.

2. **Malware and ransomware kits:** included in this category are botnets that can be used for spam or DDoS attacks, remote access trojans, which can provide attackers with remote access to a computer, keyloggers used to spy on activities and infiltrate or take over accounts, rootkits that provide the attacker with access to a computer, proxy malware.

3. **Tutorials:** sale of detailed guides that teach other fraudsters how to steal money and commit fraud, often using products and services provided by the vendor itself. Common topics for guides and tutorials include hacking, credit card scams, distribution of malware attacks and ransomware.

4. **Illicit goods:** trafficking drugs, money, weapons and goods that cannot be purchased on the clear web.

In short, most of the items sold on the dark web are illegal in nature and their prices are significantly lower than their real market value.

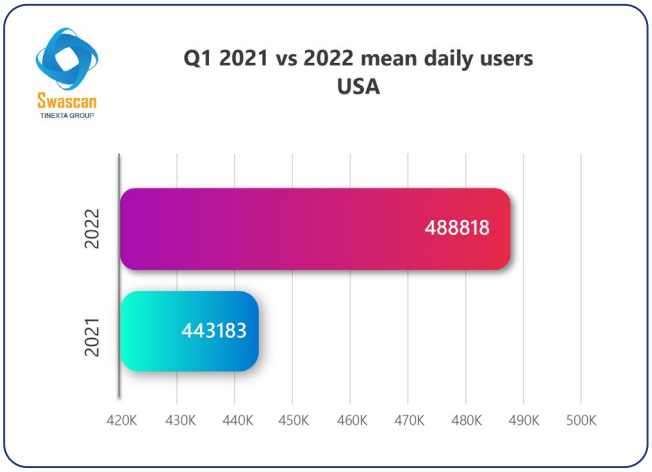


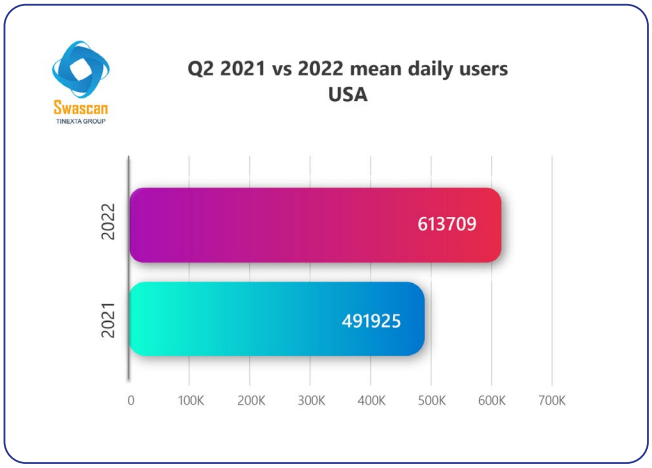
Below are the most popular items and their prices:

- Forged EU Passport – $4,000
- Hacked Verified Coinbase Account – $610
- Cloned Visa or MasterCard with PIN – $25
- Stolen Banking Login Credentials – $120

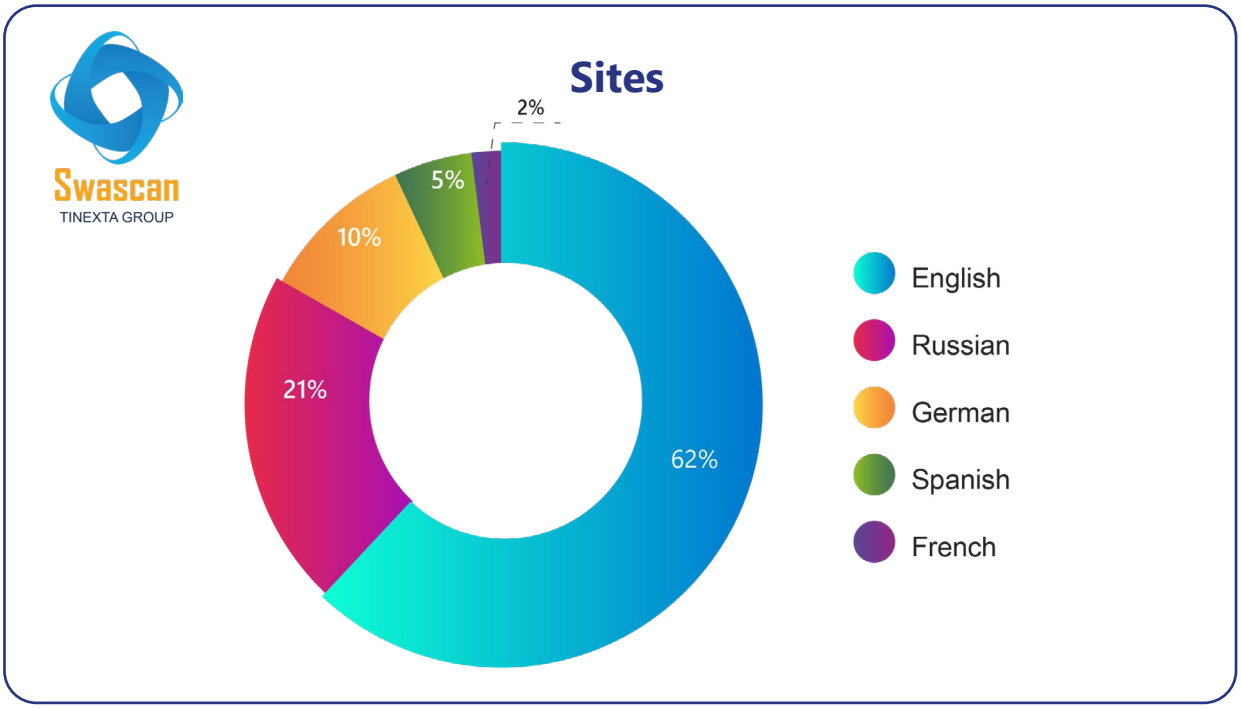
GEOGRAPHICAL DISTRIBUTION OF USERS ON THE DARK WEB

In the course of the analyses, it was found that the majority of users on the dark web are active in the United States. Below is a comparison of Q1 and Q2 in 2021 and 2022 showing the steady growth of active users.

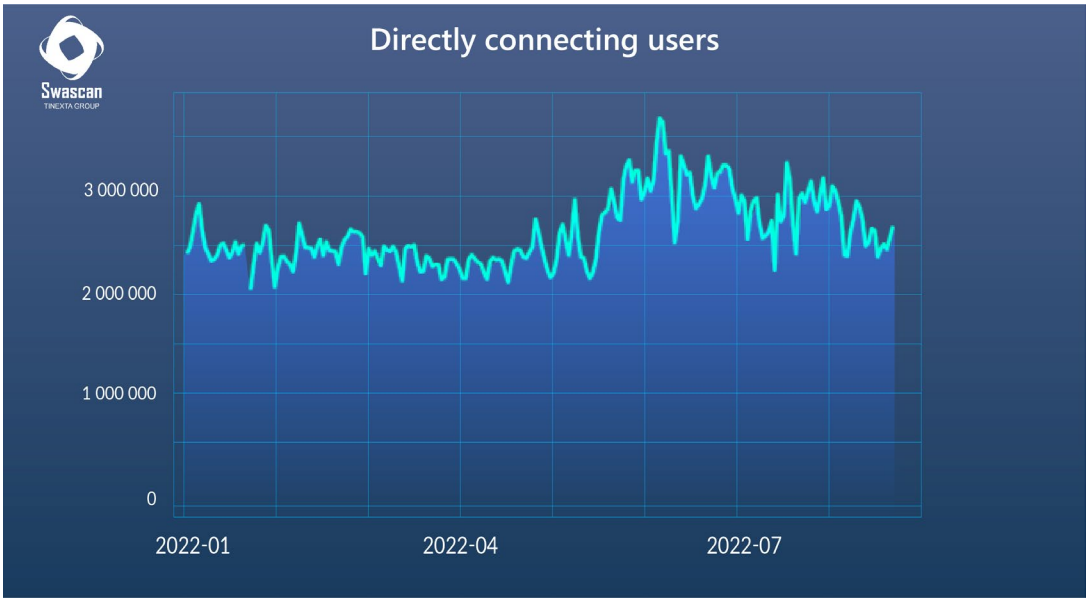


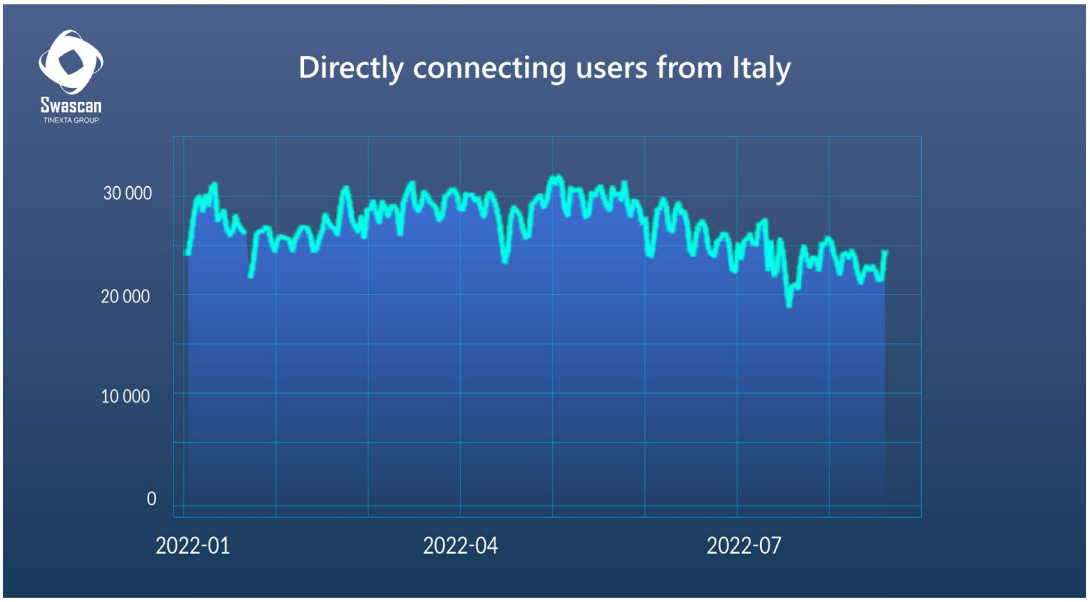


In line with the graph above, in fact, the most used language on the dark web appears to be English: out of 100. markets sampled, 62 use English as their main language.

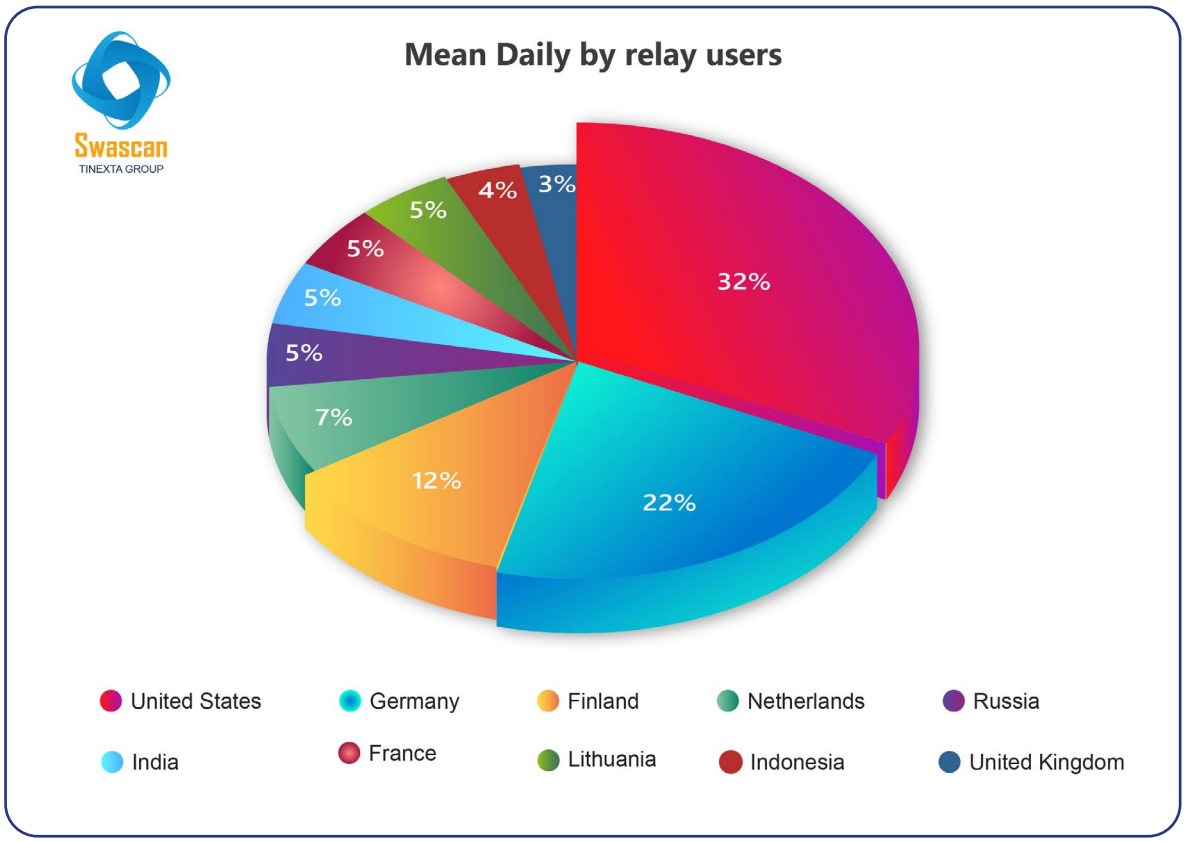


The graphs below show the number of users connected from all over the world on the dark web, with a special focus on the trend in Italy, and the geographical distribution in the period between January and August 2022. The analysis was carried out by differentiating the connected users into **"relay users"** and **"bridge users".**

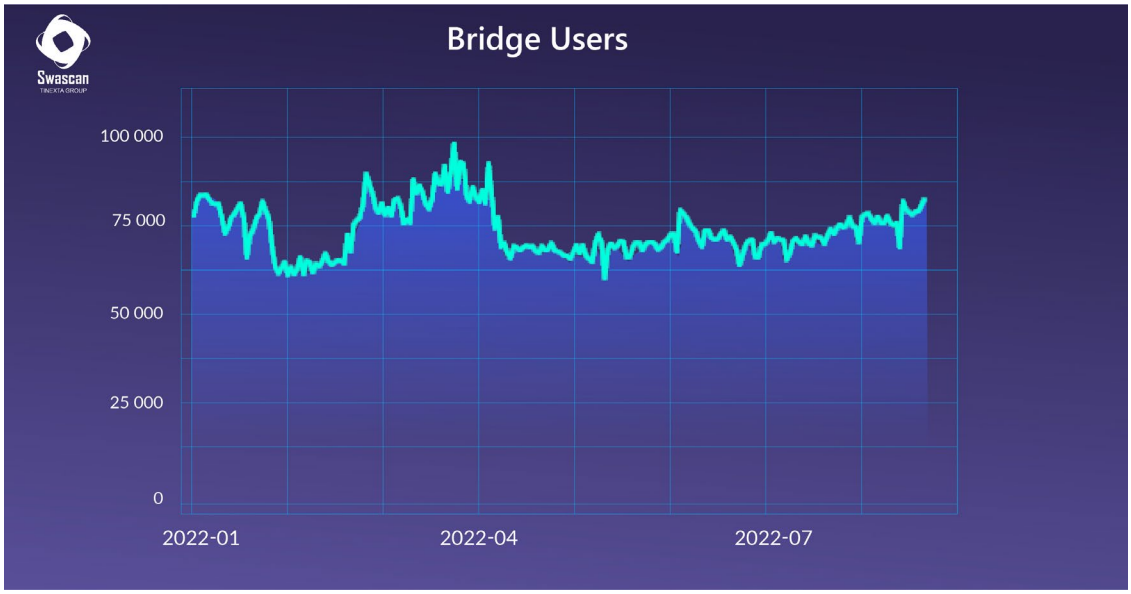


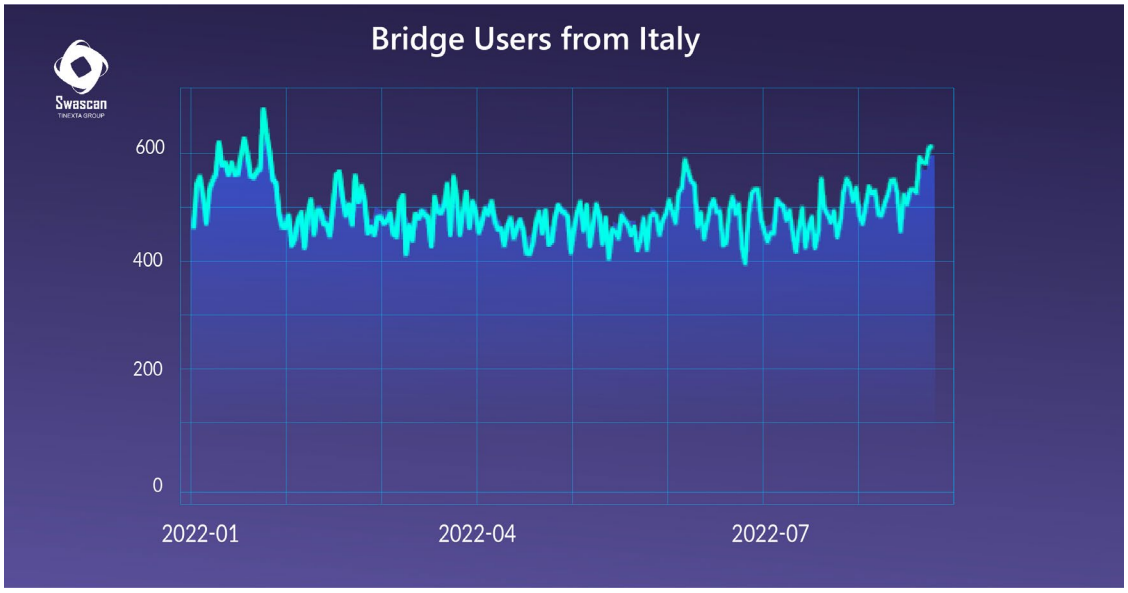


Below are the top 10 countries from which relay users connected between **January and August 2022.**

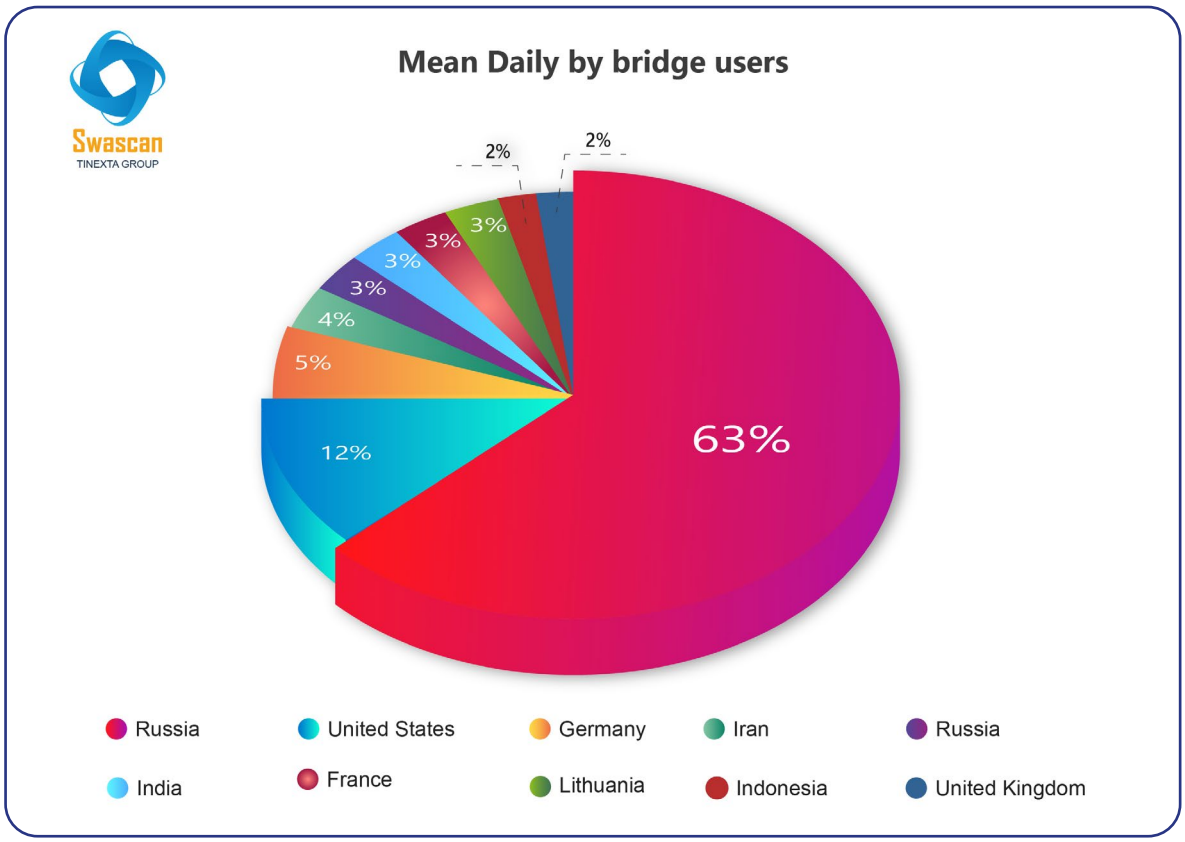


COUNTRY	Mean daily by relay users January – August 2022
United States	617024
Germany	426501
Finland	216980
Russia	122835
India	101739
Netherlands	100994
France	90441
Indonesia	88673
United Kingdom	81430
Lithuania	62448


Bridge Users
100 000
75 000
50 000
25 000
0
2022-01
2022-04
2022-07


Bridge Users from Italy
600
400
200
0
2022-01
2022-04
2022-07

Below are the top 10 countries from which bridge users connected between **January and August 2022.**



COUNTRY	Mean daily by bridge users January – August 2022
Russia	36350
United States	6976
Germany	3037
Iran	2073
France	1855
Netherlands	1642
United Kingdom	1609
China	1525
India	1426
Belarus	919

After a brief overview of the world of the dark web, Swascan's SOC & Threat Intelligence Team analysed data on the five best-selling substances and services on the underground markets in 2022, in order to understand how vendors act:

1. **Hacking tools**
2. **Drugs**
3. **Carding**
4. **Identity leaks and credential access**
5. **Weapons**

1. Hacking tools

An analysis of sales and pricing trends observed on dark web markets reveals that a wide range of tools and services are available for sale at an affordable cost: phishing, one of the most widespread cyber attack vectors, is on sale for as low as $2.

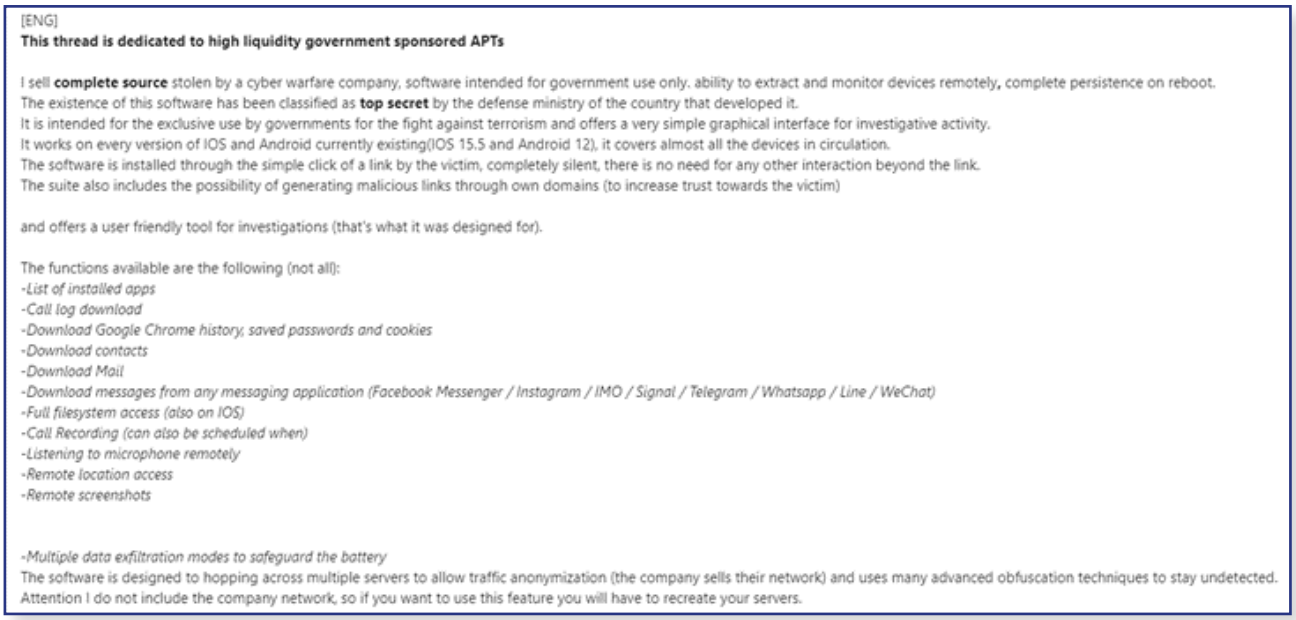
In this regard, in fact, although narcotics are in first place in terms of numbers when it comes to the goods available, close behind are countless hacking tools and packages of illegally obtained sensitive data. In particular, exploit kits for phishing, ransomware exploit kits, DDoS-for-hire, RDP, Command&Control etc. are sold. Below are examples of sales on three underground forums:

XSS

A Russian hacker forum created in 2013 and relaunched in 2018, considered one of the most popular Russian language hacking forums. The name stands for cross-site scripting (XSS), which indicates the exploitation of vulnerabilities in web applications.

The site was created and designed for the purpose of sharing information on exploits, zero-day vulnerabilities, malware and network penetration. The main contents include malware exploits, vulnerabilities, carding, access sales and credential databases. The forum is also used by ransomware gangs to recruit new members, however.

Below are examples of posts that have appeared on the underground forum. In the first case, the ability to extract and monitor devices remotely is on sale. The existence of this software has been classified as top secret by the Ministry of Defence of the country that developed it. It is, in fact, intended for the exclusive use of governments in the fight against terrorism.



[ENG]
This thread is dedicated to high liquidity government sponsored APTs

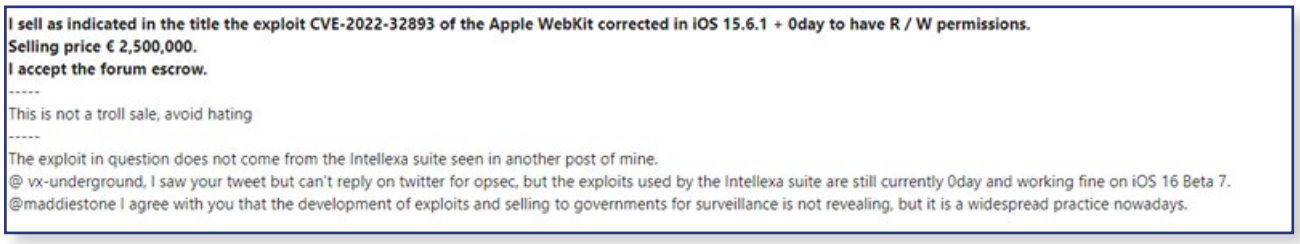
I sell **complete source** stolen by a cyber warfare company, software intended for government use only. ability to extract and monitor devices remotely, complete persistence on reboot.
The existence of this software has been classified as **top secret** by the defense ministry of the country that developed it.
It is intended for the exclusive use by governments for the fight against terrorism and offers a very simple graphical interface for investigative activity.
It works on every version of IOS and Android currently existing(IOS 15.5 and Android 12), it covers almost all the devices in circulation.
The software is installed through the simple click of a link by the victim, completely silent, there is no need for any other interaction beyond the link.
The suite also includes the possibility of generating malicious links through own domains (to increase trust towards the victim)

and offers a user friendly tool for investigations (that's what it was designed for).

The functions available are the following (not all):
-List of installed apps
-Call log download
-Download Google Chrome history, saved passwords and cookies
-Download contacts
-Download Mail
-Download messages from any messaging application (Facebook Messenger / Instagram / IMO / Signal / Telegram / Whatsapp / Line / WeChat)
-Full filesystem access (also on IOS)
-Call Recording (can also be scheduled when)
-Listening to microphone remotely
-Remote location access
-Remote screenshots

-Multiple data exfiltration modes to safeguard the battery
The software is designed to hopping across multiple servers to allow traffic anonymization (the company sells their network) and uses many advanced obfuscation techniques to stay undetected.
Attention I do not include the company network, so if you want to use this feature you will have to recreate your servers.

In another case, Apple's WebKit exploit CVE-2022-32893 fixed in iOS 15.6.1 including zero-day is sold at a price of €2,500,000.



I sell as indicated in the title the exploit CVE-2022-32893 of the Apple WebKit corrected in iOS 15.6.1 + 0day to have R / W permissions.
Selling price € 2,500,000.
I accept the forum escrow.

This is not a troll sale, avoid hating

The exploit in question does not come from the Intellexa suite seen in another post of mine.
@ vx-underground, I saw your tweet but can't reply on twitter for opsec, but the exploits used by the Intellexa suite are still currently 0day and working fine on iOS 16 Beta 7.
@maddiestone I agree with you that the development of exploits and selling to governments for surveillance is not revealing, but it is a widespread practice nowadays.

Leaked documents online show the purchase and documentation of the iOS Remote Code Execution 0day exploit at a price of $8,000,000:

NOVA Platform
Commercial Proposal

intellexa

91	Xiaomi Black Shark 4
92	Xiaomi Mi A3

Oppo* Devices

Serial	Device
93	Oppo Reno6 5G
94	Oppo F11 Pro
95	Oppo A74
96	Oppo Find X2 Pro
97	Oppo Find X2 Neo
98	Oppo A73 5G
99	Oppo Reno6 Z 5G
100	Oppo Reno5 Z
101	Oppo Reno4 Pro 5G
102	Oppo Reno4 Z 5G

Huawei* Devices

Serial	Device
103	Huawei P40 Pro
104	Huawei P30
105	Huawei P30 Pro
106	Huawei P20 Pro
107	Huawei Mate 20 Pro
108	Huawei nova 4
109	Huawei Mate 10
110	Huawei nova 5T
111	Huawei Mate 40 Pro

Honor* Devices

Serial	Device
112	Honor View 20

* It is hereby clarified that any commitment of Intellexa to support the devices listed above, shall be valid as long as such devices contain mainstream Android distribution and Google store and Google play services with Chrome browser installed on the device.

NOVA Platform
Commercial Proposal

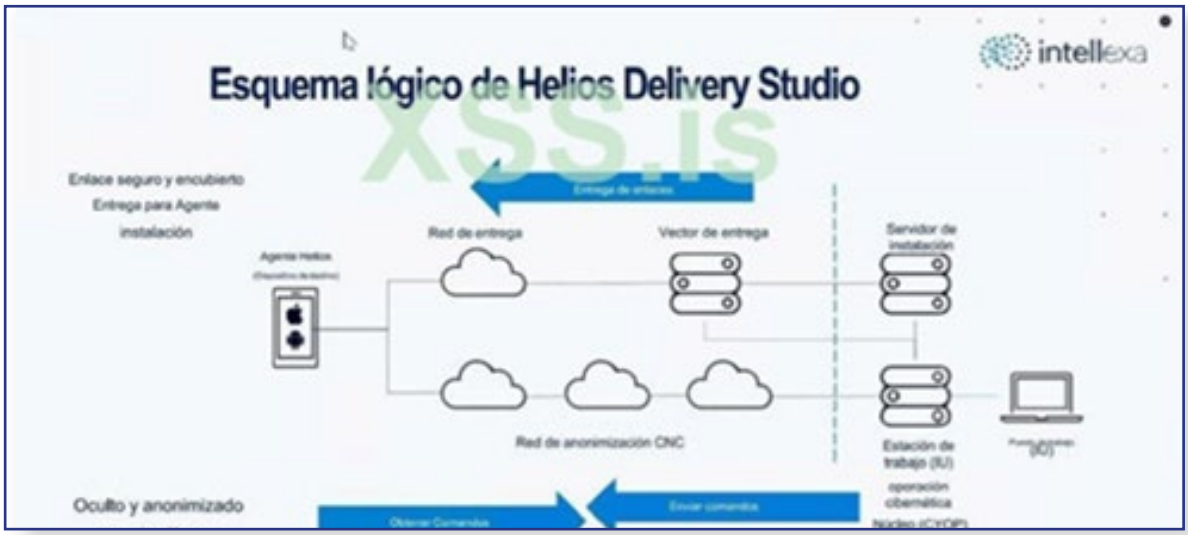
intellexa

2 Price Proposal

#	Item	Description	Qty.	Price (EURO)
1	**Nova** Remote Data Extraction from Android & iOS Devices & Analytics system	Delivery Studio: Remote 1-Click Browser based capability to inject Android & iOS payload to mobile devices through link delivery	1	Included
		Supported devices: iOS & Android supported devices (list attached)	1	
		Android Support:* • Android 12 (latest version)*** + 18 months back **iOS Support: *** • iOS latest version*** 15.4.1 + 12 months back	1	
		Agent Concurrency Scope: • 10 Concurrent infections for both OS families (iOS and Android) (i.e. total of 10 infections which may be split between iOS and Android as per the customer sole decision).	10	
		Successful infections magazine: • Magazine of 100 Successful infections.	100	
		Geographical Coverage: Inside the country for local SIM cards on iOS or Android devices.	1	
		Fusion & Analytics system Investigation platform for analysis of all Cyber data extracted by NOVA system. • Cases and targets investigation • Search, filter, analyze and manage cyber data	1	
2	**Hardware & Software**	The entire Nova Suite will be delivered turnkey: • All proprietary software and 3rd party software shall be provided by Intellexa, unless written specifically otherwise under the agreement. • Cloud services, domains and anonymization chain which will be provided and managed by customer.	1	Included
3	**Project Management**	A complete project plan will be provided by INTELLEXA to be approved and coordinated with the customer: • Delivery & Project Plan • Final Design Review • Site Acceptance Testing (Customer site) Technical, operational and methodology	1	Included
4	**Warranty**	Twelve (12) months Warranty as further detailed under section 2.2 below.	1	Included
5	**Price**			**€8,000,000**

Proprietary & Confidential

2

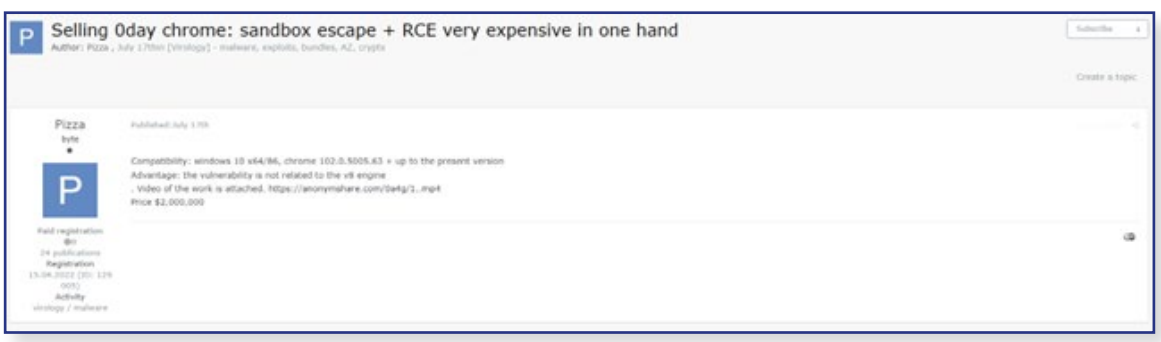


EXPLOIT.IN

Exploit.in is a forum created in 2005 that hosts discussions on various cybercrime topics such as social engineering, security and vulnerabilities, social network hacking, cryptography, malware and programming for cracking. The site focuses mainly on sharing computer system vulnerabilities, for hacking purposes. It also acts as a marketplace where users can buy and sell illicit digital products such as malware and various hacking and carding services.

One of the most important features of this Russian forum, which we can consider one of the most critical in terms of cyber attacks, is its auctioning, making Exploits.in the dark web forum of choice for ransomware hackers.

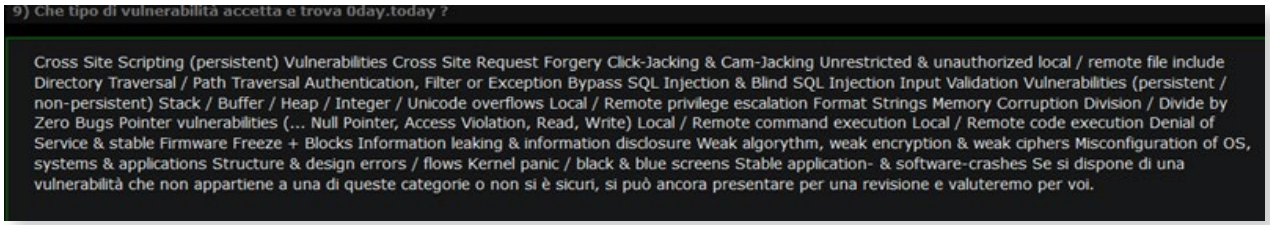
Below are examples of sales on the underground market with their prices:



0DAY.TODAY

0day.today was created on 13 May 2008 and is a database regularly updated with descriptions of critical vulnerabilities to be exploited. Each vulnerability is assigned a risk, from low to critical. It also features a breakdown by platform: BSD, Linux, QNX, OSX, Solaris, Unix, Windows.

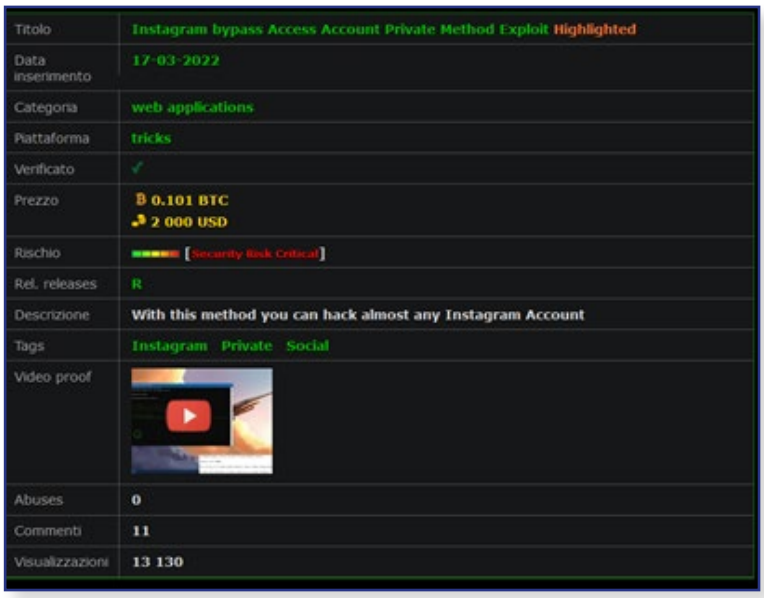
Below are the vulnerabilities for sale on the market:



The site is divided into six categories:

1. Private exploits and 0day exploits market

Below is an example of selling access to a private Instagram account:



2. Remote Exploits

25-08-2022	Zimbra Zip Path Traversal Exploit	linux	289		R	D	C	✓	FREE	metasploit
23-08-2022	Teleport 9.3.6 Command Injection Vulnerability	windows	351		R	D	C	✓	FREE	Brian Landru
22-08-2022	Microsoft Exchange Server ChainedSerializationBinder Remote Code Execution Exploit	windows	486		R	D	C	✓	FREE	zcgonvh
22-08-2022	FLIR AX8 1.46.16 Remote Command Execution Exploit	php	239		R	D	C	✓	FREE	Samy Younsi
19-08-2022	Advantech iView NetworkServlet Command Injection Exploit	windows	597		R	D	C	✓	FREE	metasploit
16-08-2022	Powershell Code Arbitary Execution Builder FUD Exploit	linux	869		R	D	-	✓	Ƀ 0.05	viper_8080
10-08-2022	AirSpot 5410 0.3.4.1-4 Remote Command Injection Exploit	hardware	502		R	D	C	✓	FREE	Samy Younsi
09-08-2022	PAN-OS 10.0 - Remote Code Execution (Authenticated) Exploit	multiple	465		R	D	C	✓	FREE	UnD3sc0n0c1
08-08-2022	ManageEngine ADAudit Plus Path Traversal / XML Injection Exploit	windows	823		R	D	C	✓	FREE	metasploit
07-08-2022	Zimbra UnRAR Path Traversal Exploit	linux	942		R	D	C	✓	FREE	metasploit

Titolo	Powershell Code Arbitary Execution Builder FUD Exploit [Highlight]
Data inserimento	16-08-2022
Categoria	remote exploits
Piattaforma	linux
Verificato	✓
Prezzo	Ƀ 0.05 BTC 1 000 USD
Rischio	[Security Risk Critical]
Rel. releases	R
Descrizione	A desired powershell(.ps1) hides the payload with special methods. It allows it to run secretly on the installed computer. Bypasses all modern antivirus protections. Completely FUD
Usage info	Run the python file via terminal.
Testato su	Kali Linux 5.15.0-kali3-amd64
Tags	payload builder powershell backdoor
Abuses	0
Commenti	0
Visualizzazioni	869

3. Local exploits

DATE	DESCRIPTION	TYPE	HITS	RISK					GOLD	AUTHOR
3-08-2022	10-Strike Network Inventory Explorer 9.3 Buffer Overflow Vulnerability	windows	221		R	D	-	✓	FREE	Ricardo Jose
2-08-2022	macOS RawCamera Out-Of-Bounds Write Vulnerability	macOS	170		R	D	C	✓	FREE	Ivan Fratric
9-08-2022	Polar Flow Android 5.7.1 Secret Disclosure Vulnerability	Android	459		R	D	-	✓	FREE	Karima Hebb
0-08-2022	Zimbra zmslapd Privilege Escalation Exploit	linux	681		R	D	C	✓	FREE	metasploit
4-08-2022	IObit Malware Fighter 9.2 Tampering / Privilege Escalation Vulnerability	windows	838		R	D	-	✓	FREE	Yehia Elghaly
6-07-2022	PCProtect Endpoint 5.17.470 Tampering / Privilege Escalation Vulnerability	windows	1 070		R	D	-	✓	FREE	Yehia Elghaly
1-07-2022	Dr. Fone 4.0.8 - (net_updater32.exe) Unquoted Service Path Vulnerability	windows	1 092		R	D	-	✓	FREE	Esant1490
1-07-2022	Kite 1.2021.610.0 - Unquoted Service Path Vulnerability	windows	1 062		R	D	-	✓	FREE	Ghaleb Al-ota
0-07-2022	Asus GameSDK 1.0.0.4 Unquoted Service Path Vulnerability	windows	1 124		R	D	C	✓	FREE	Angelo Pio Ar
7-07-2022	Xen PV Guest Non-SELFSNOOP CPU Memory Corruption Exploit	linux	1 452		R	D	C	✓	FREE	Jann Horn

Titolo	Asus GameSDK 1.0.0.4 Unquoted Service Path Vulnerability [Highlight]
Data inserimento	20-07-2022
Categoria	local exploits
Piattaforma	windows
Verificato	✓
Prezzo	FREE
Rischio	[Security Risk Medium]
Rel. releases	R
CVE	CVE-2022-35899
Abuses	0
Commenti	0
Visualizzazioni	1 124

4. Web Application

DATE	DESCRIPTION	TYPE	HITS	RISK					GOLD	AUTHOR
7-08-2022	AeroCMS v0.0.1 SQL injection Vulnerability	php	87		R	D	-	✓	FREE	nu11secur1ty
7-08-2022	WordPress Robo Gallery 3.2.1 plugin - XSS Stored Vulnerability	php	85		R	D	-	✓	FREE	nu11secur1ty
7-08-2022	WordPress Robo Gallery 3.2.1 plugin - Bypass POST comment approvement Vulnerability	php	75		R	D	-	✓	FREE	nu11secur1ty
5-08-2022	PrestaShop Ap Pagebuilder 2.4.4 SQL Injection Vulnerability	php	202		R	D	C	✓	FREE	Mohamed Ali
5-08-2022	Centreon 22.04.0 Cross Site Scripting Vulnerability	php	155		R	D	C	✓	FREE	yunaranyanc
2-08-2022	Personnel Property Equipment 2015-2022 SQL Injection Vulnerability	php	270		R	D	-	✓	FREE	nu11secur1ty
2-08-2022	FLIR AX8 1.46.16 Traversal / Access Control / Command Injection / XSS Vulnerabilities	php	284		R	D	C	✓	FREE	Samy Younsi
2-08-2022	Transposh WordPress Translation 1.0.8.1 Incorrect Authorization Vulnerability	php	283		R	D	C	✓	FREE	Julien Ahrens
6-08-2022	TypeORM 0.3.7 Information Disclosure Vulnerability	jsp	536		R	D	C	✓	FREE	Andrii Kosten
6-08-2022	Inout RealEstate 2.1.2 SQL Injection Vulnerability	php	576		R	D	-	✓	FREE	CraCkEr

Titolo	Personnel Property Equipment 2015-2022 SQL Injection Vulnerability [Highlight]
Data inserimento	22-08-2022
Categoria	web applications
Piattaforma	php
Verificato	✓
Prezzo	FREE
Rischio	[Security Risk High]
Rel. releases	R
Abuses	0
Commenti	0
Visualizzazioni	270

5. PoC/ Ddos

DATE	DESCRIPTION	TYPE	HITS	RISK					GOLD	AUTHOR
11-07-2022	Nginx 1.20.0 - Denial of Service Exploit	multiple	1 225		R	D	C	✓	FREE	Mohammed A
29-06-2022	AnyDesk 7.0.9 Arbitrary File Write / Denial Of Service Vulnerabilities	windows	1 733		R	D	-	✓	FREE	Erwin Chan
27-06-2022	dbus-broker-29 Memory Corruption Exploit	multiple	861		R	D	C	✓	FREE	Tim Weber
24-06-2022	NVIDIA Data Center GPU Manager Remote Memory Corruption Exploit	hardware	1 022		R	D	C	✓	FREE	Jeremy Brow
24-06-2022	IIPImage Remote Memory Corruption Exploit	multiple	880		R	D	-	✓	FREE	Jeremy Brow
22-06-2022	libMeshb Buffer Overflow Exploit	linux	2 038		R	D	-	✓	FREE	Jeremy Brow
22-06-2022	GtkRadiant 1.6.6 Buffer Overflow Exploit	linux	2 070		R	D	-	✓	FREE	Jeremy Brow
22-06-2022	libxml2 xmlBufAdd Heap Buffer Overflow Exploit	linux	2 070		R	D	C	✓	FREE	Felix Wilhelm
31-05-2022	Akka HTTP 10.1.14 - Denial of Service Exploit	multiple	1 126		R	D	C	✓	FREE	cxosmo
27-04-2022	Prime95 30.7 Build 9 Buffer Overflow Exploit	windows	2 369		R	D	-	✓	FREE	Yehia Elghaly

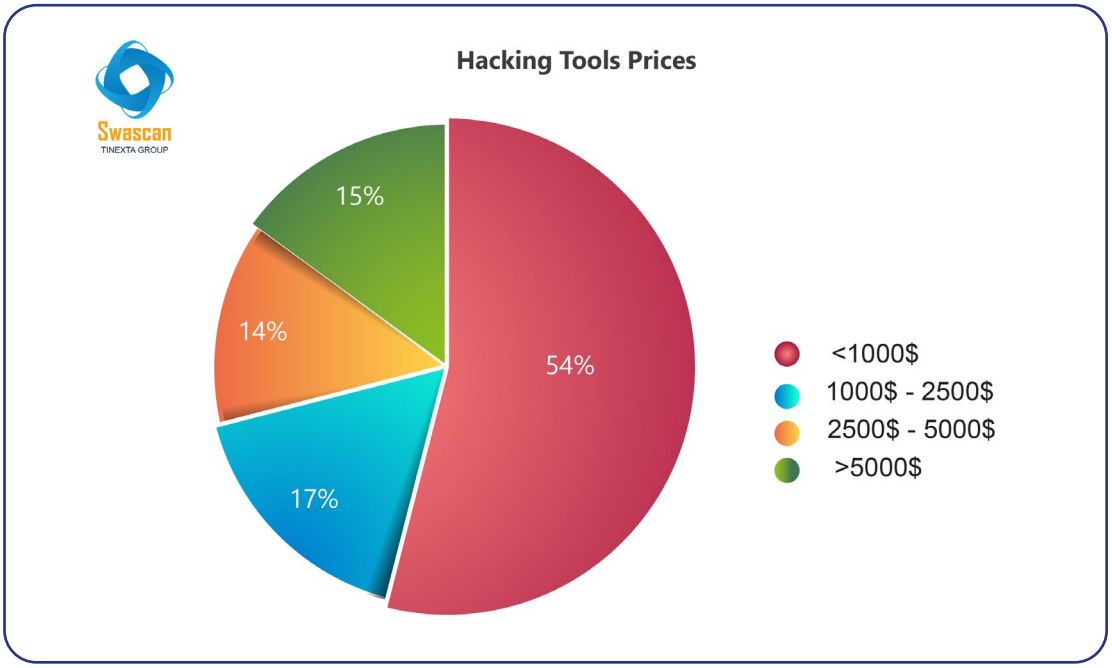
Titolo	Nginx 1.20.0 - Denial of Service Exploit [Highlight]
Data inserimento	11-07-2022
Categoria	dos / poc
Piattaforma	multiple
Verificato	✓
Prezzo	FREE
Rischio	[Security Risk Medium]
Rel. releases	R
CVE	CVE-2021-23017
Abuses	0
Commenti	0

6. Shellcode

::DATE	::DESCRIPTION	::TYPE	::HITS	::RISK					::GOLD	::AUTHOR
19-04-2022	Windows/x86 - XOR/DEC/NOT/ROR encrypted / encoded + null free reverse tcp Shellcode	win64	1 886		R	D		✓	FREE	Xenofon
11-03-2022	Linux/x86_64 - sudo enumeration Shellcode (245 bytes)	linux/x86-64	4 284		R	D		✓	FREE	Kağan Çapar
18-02-2022	Linux/MIPS - N32 MSB Reverse Shell Shellcode	linux/mips	4 145		R	D		✓	FREE	Marco Ivaldi
18-02-2022	Solaris/SPARC - setuid(0) + execve (/bin/ksh) Shellcode	solaris/spar	4 126		R	D		✓	FREE	Marco Ivaldi
18-02-2022	Solaris/SPARC - chmod(./me) Shellcode	solaris/spar	4 128		R	D		✓	FREE	Marco Ivaldi
18-02-2022	Solaris/SPARC - setuid(0) + chmod (/bin/ksh) + exit(0) Shellcode	solaris/spar	4 105		R	D		✓	FREE	Marco Ivaldi
08-02-2022	Windows/x86 - Locate kernel32 base address / Stack Crack method NullFree Shellcode	win64	4 443		R	D		✓	FREE	Tarek Ahmed
06-02-2022	Windows/x86 - Locate kernel32 base address / Memory Sieve method Shellcode (133	win64	4 375		R	D		✓	FREE	Tarek Ahmed
05-02-2022	Windows/x86 Download File / Execute Shellcode (458 bytes)	win64	4 860		R	D		✓	FREE	Techryptic
07-10-2021	Windows/x86 - Bind TCP shellcode / Dynamic PEB & EDT method null-free Shellcode (415	win64	5 978		R	D		✓	FREE	h4pp1n3ss

Titolo	Windows/x86 - XOR/DEC/NOT/ROR encrypted / encoded + null free reverse tcp Shellcode (840 bytes) [Highlight]
Data inserimento	19-04-2022
Categoria	shellcode
Piattaforma	win64
Verificato	✓
Prezzo	FREE
Rischio	[Security Risk Medium]
Rel. releases	R
Abuses	0
Commenti	0
Visualizzazioni	1 886

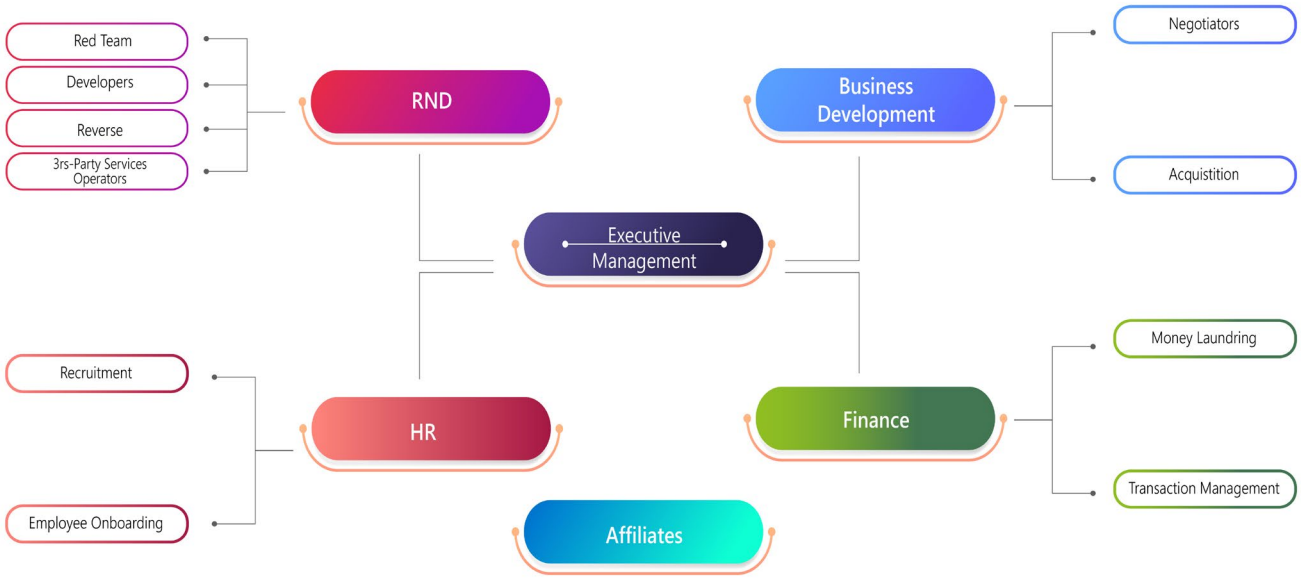
Out of 100 for sale adverts published, the prices offered have been averaged:



This scenario demonstrates a high level of criticality, showing how the market is indirectly becoming a market of professionals, cybercrime entrepreneurs: set up as real companies. Clear examples of this are the two ransomware gangs Lockbit and Conti, characterised by:

- expertise
- ransomware
- tool (exploit/0day)
- infrastructure
- governance centre

These recruit staff through regular interviews and operate by hitting companies and then publishing their details if they do not pay the required amount. In this regard, Cybertint has produced a graphic depiction of the possible structure of the Conti gang, which has currently ceased operations: as can be seen in the figure, the structure is the same as that of real companies.

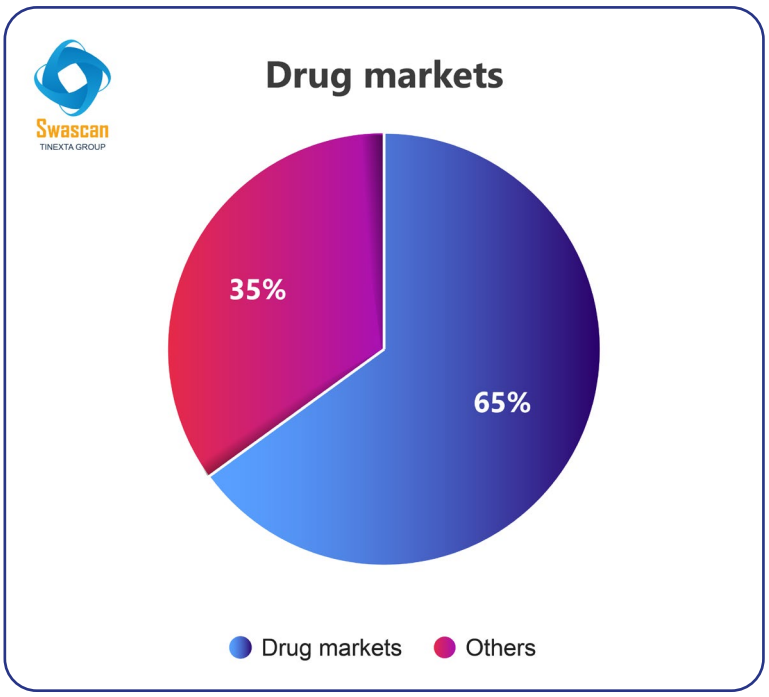


Recently, the ransomware group Lockbit was the victim of a DDoS attack by Entrust that prevented access to the site on which it shares company information and data. Here too, there was no shortage of "DDoSer" recruitment.

Subsequently, also on the XSS forum, LockBitSupp, a LockBit account, announced that the group was back in business after setting up a larger infrastructure to allow access to stolen data without any DDoS actions being able to hinder it. This gave the criminal gang an idea for a new tactic: taking a cue from what had happened, in fact, Lockbit decided to adopt the tactic of triple extortion to put more pressure on victims. In addition to encrypting the files and publishing the data, a possible DDoS attack is therefore envisaged.

2. Drugs

The underground drug market is the largest in terms of the number of products for sale and the number of vendors, with the phenomenon growing progressively over the last few years. These online marketplaces offer a range of different narcotics ranging from common drugs to chemical substances used in manufacturing new substances or for other illegal purposes, giving the customer a huge choice. Below is a comparison of the drug market with others, and an analysis of three markets selling these substances:



SmokersCo

"Our shop carries the best cannabis strains and medical marijuana for all medical conditions - available online at the lowest prices, guaranteed! If you've been wondering how to order weed online, you've come to the right place. It's never been easier to have medical cannabis delivered straight to your door."

SmokersCo is a shop under the Tor network offering a wide variety of marijuana and hashish. The key elements that set it apart from other markets are the ease with which it is possible to buy marijuana online in Europe, a feature that attracts new buyers on a daily basis, who are also offered the option of buying via mobile phone, paying with bitcoin or Monero. The site administrators are currently in the process of launching an affiliate system through which it is possible to create multiple campaigns and receive a portion of the profit from the company.

Although this site is a vendor's shop, it works pretty much like generic dark net marketplaces: before buying anything, you have to set up an account (no e-mail address required).

The products are divided into two different categories, weed and hashish. Nevertheless, the products available within the categories are subject to constant change, which is why the site administrators recommend checking frequently for updates.

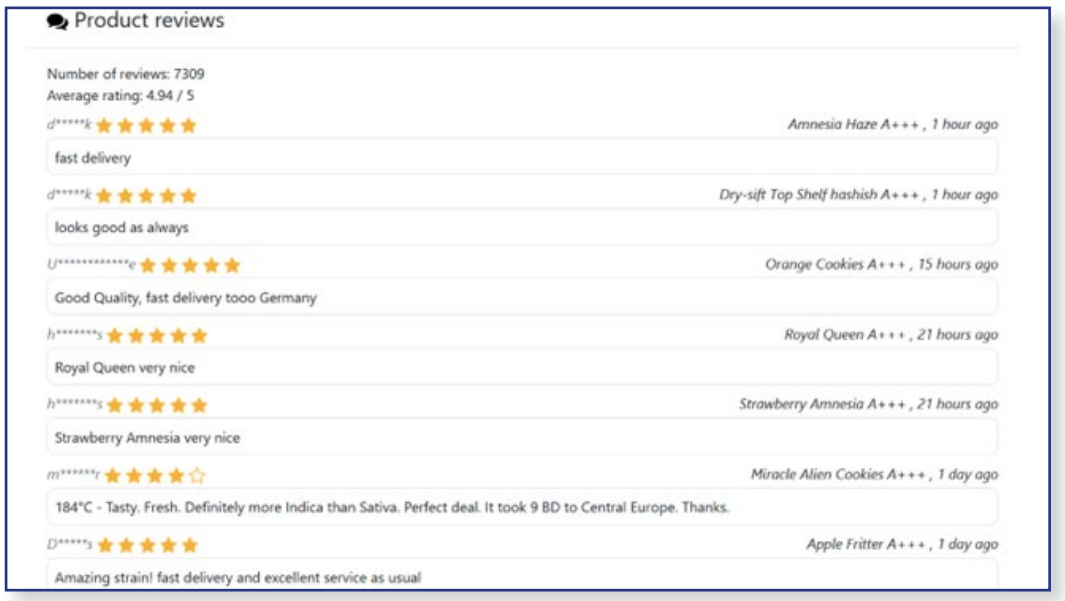
Another interesting feature of the site is the availability of a variety of guides and tutorials for those who may be new to dark net market operations. These include detailed tutorials on how to buy bitcoin from Localbitcoins or Coinbase. You can also find tutorials on the use of PGP, for both beginners and more experienced users. These guides include instructions and examples on how to use Gpg4Win and Kleopatra.

Finally, there is also a large section for guides and general safety drills, giving people the opportunity to familiarise themselves with basic safety procedures.

Another advantage of SmokersCO is that it includes reviews for all sales: these reviews are public and can be viewed by anyone, giving new buyers a summary of the experience of previous customers.

In terms of products, the shop now has more than twelve different varieties of marijuana and four different types of hashish imported directly from Morocco.

With more than 7,300 reviews on their website, SmokersCo. currently ranks among the best shops in Europe for buying drugs online.



Another feature that attracts new users is the support offered to customers, guaranteeing a response within 24 hours from Monday to Friday. As regards the conditions of purchase, if the mail order drugs are lost or stolen, a replacement package will be sent out free of charge, or alternatively a 100% refund given.

They call themselves "the marketplace with the lowest prices online", offering all products at a fixed price of $18, without applying the 6% dark net market tax.

"We only work with farmers who grow cannabis with organic methods. All of our products are rigorously tested for quality control in-house. No mold, no problem. Rest assured you'll only be getting the cream of the crop!"

They are currently shipping from Spain, with standard shipping for all orders of 50 grams or less, and the estimated shipping time is between 4 and 7 business days. No tracking number is provided for small quantity orders.

For shipments over 50 grams, express shipping is available: in this case the estimated shipping time is between 2 and 6 business days, with a tracking number available. It is recommended to enter a phone number.

Orders are accepted from the following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland and Turkey. As of 9 August, the shop no longer ships outside the European Union.

The shipping address needs to be a flat or private house with a visible mailbox. If living in a building, it is necessary to correctly specify the floor and door number. Real names must be used. The shop does not ship to hotels, businesses, universities.

Like a real company, the underground market pays special attention to customers: in fact, it is possible that in some cases the drug loses a little weight due to the continuous drying process. In this case, SmokersCo. recommends that you directly weigh all the packaging before opening and send them a photo, if the weight is less, a package with the missing quantity will be sent out. If the weed you receive is in poor condition, you need to take several photos of the condition of the product in order to receive a refund.

Below are the three best-selling types:

1. Sativa

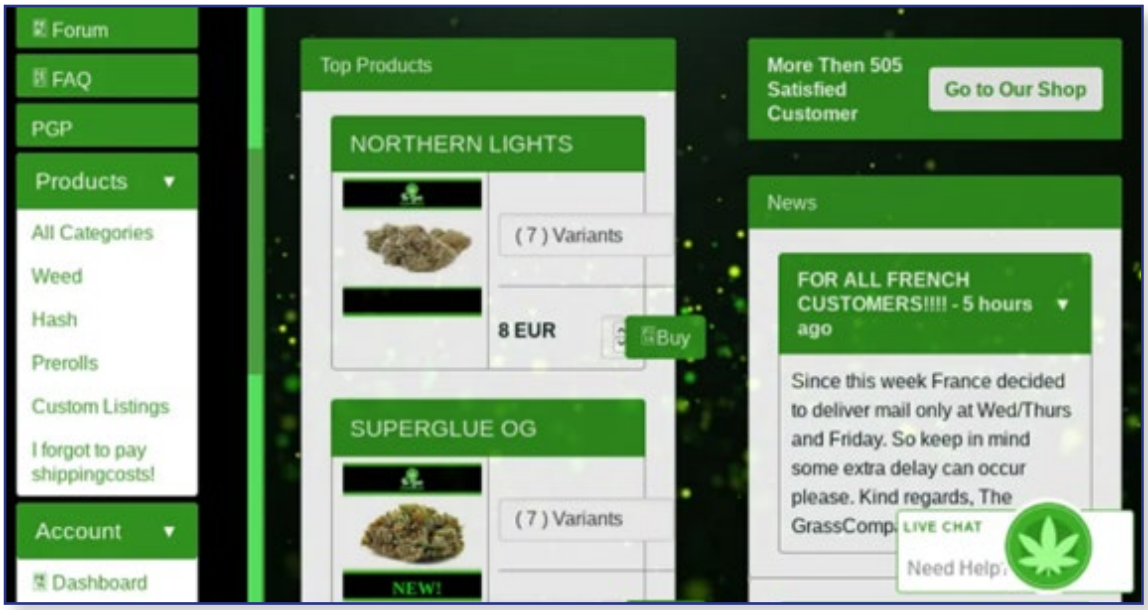
2. Indica

3. Hybrid

The Grass Company

The Grass Company is one of the vendor shops established in 2018 that is dedicated purely to one explicit type of product: as the name suggests, this product is cannabis and the shop deals in this substance exclusively.

The Grass Company team is constantly trying to improve its platform, adding many new features from time to time, such as a forum and a live chat.



The homepage shows the list of best-selling products and a list of news published by the shop team. The left sidebar is where all the important information is located, including the list of product categories, which facilitates searching by type.

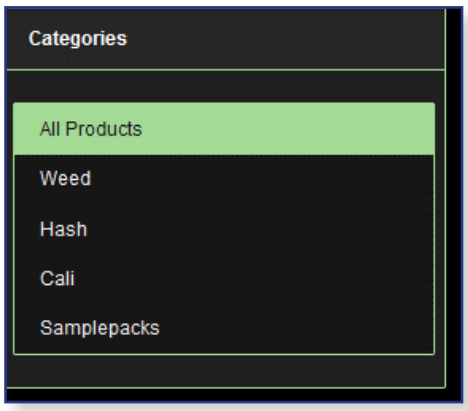
The Grass Company shop can be viewed without registration, which is, however, required in order to place orders. The registration process is quite simple and only requires a user name and password.

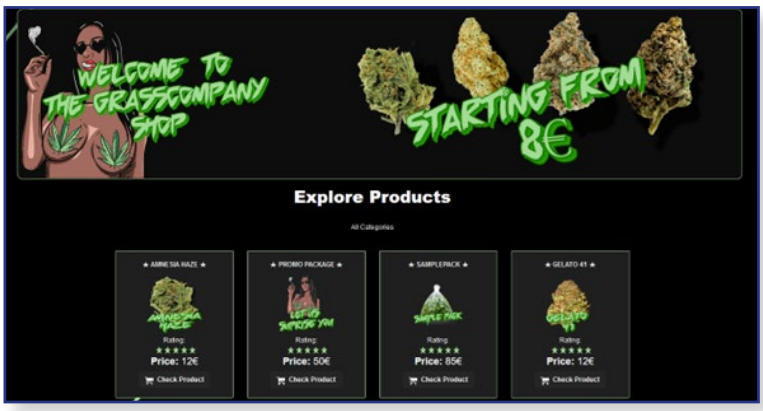
With regard to purchases, originally, only bitcoin (BTC) was accepted on The Grass Company; recently, the team added Monero (XMR) and Litecoin (LTC) as additional payment methods. An evaluation

of vendors is also provided, with how many sales they have made and other details of the product sold.

The site also features a generic average rating of customers, products, orders and feedback:

"TheGrassCompany is proud to announce the launch of our new web shop, which sells the highest quality THC products at discounted prices. With the latest updates, it will be quicker and easier for everyone to place an order with BTC or XMR payments in just a few steps. We have a wide variety of products available, including Classic weed varieties, Hash and our premium Cali varieties. All products are cared for by our loving growers with carefully selected varieties. In addition to great prices, TheGrassCompany offers free shipping on orders over 25 g with free Track and Trace for your peace of mind. Visit us today to take advantage of these incredible offers!"





Shipping is guaranteed worldwide except for India, Australia and the USA. The estimated time of arrival for countries near Belgium is 2-3 days, for other European countries 4-5 days and for countries outside Europe 7-10 working days. A 50% refund is guaranteed if the product does not arrive.

Free shipping and free tracking is also guaranteed for all orders within Europe. Shipping costs outside Europe are €6 with a maximum quantity of 19 grams per envelope. No shipping costs are charged for orders over 20 grams.

In many cases the price charged is the same, although Hash, Amnesia Haze and the cheaper Northern Lights are priced differently.

The minimum price is €8 per gram and a maximum of €6,000 per kg. The prices are detailed below:

1 gram = 8 €
2,5 grams = 22 €
5 grams = 44 €
10 grams = 85 €
25 grams = 200 €
50 grams= 380 €
100 grams = 750 €
250 grams = 1800 €
500 grams= 3250 €
1000 grams= 6000 €

WeAreAmsterdam

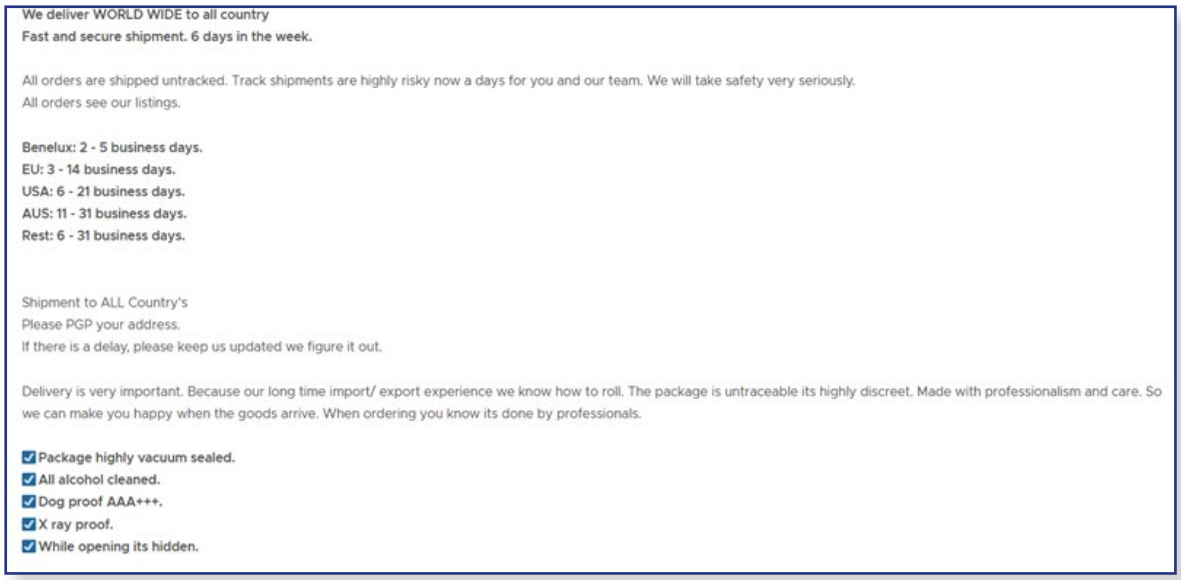
WeAreAmsterdam is a German vendor with a shop site dedicated to cannabis and other drug-related products. Its storefront on the dark web currently lists around 70 items and ships worldwide, including to the US and Australia. Despite being only two years old, the administrators have amassed more than 20,000 sales in 20 different markets, making it one of the most established and enduring vendors in the history of dark net marketplaces.

Like most shops, you can browse instantly, without the need to create an account if you just want to check products and prices.

Once you have an account, you have access to a list of all your orders, which can have three different statuses:

- Pending (the order has been placed and is now awaiting consignment)
- Paid (the amount has been paid in full and is now being prepared for shipment)
- Shipped (the order has been dispatched to your address).

If you place an order, it must be paid for within 60 minutes or it will be automatically cancelled. WeAreAmsterdam gives broad limits for delivery times, as this depends on the destination and can vary on a case-by-case basis. The site does, however, offer contact details to inquire about the estimated shipping date.


We deliver WORLD WIDE to all country
Fast and secure shipment. 6 days in the week.

All orders are shipped untracked. Track shipments are highly risky now a days for you and our team. We will take safety very seriously.
All orders see our listings.

Benelux: 2 - 5 business days.
EU: 3 - 14 business days.
USA: 6 - 21 business days.
AUS: 11 - 31 business days.
Rest: 6 - 31 business days.

Shipment to ALL Country's
Please PGP your address.
If there is a delay, please keep us updated we figure it out.

Delivery is very important. Because our long time import/ export experience we know how to roll. The package is untraceable its highly discreet. Made with professionalism and care. So we can make you happy when the goods arrive. When ordering you know its done by professionals.

- [x] Package highly vacuum sealed.
- [x] All alcohol cleaned.
- [x] Dog proof AAA+++.
- [x] X ray proof.
- [x] While opening its hidden.

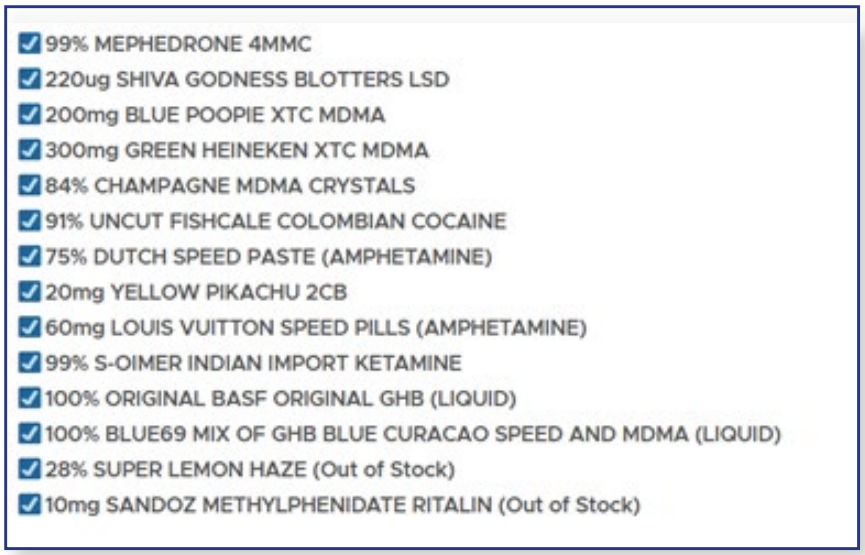
The product listings on WeAreAMSTERDAM are divided into five different categories:

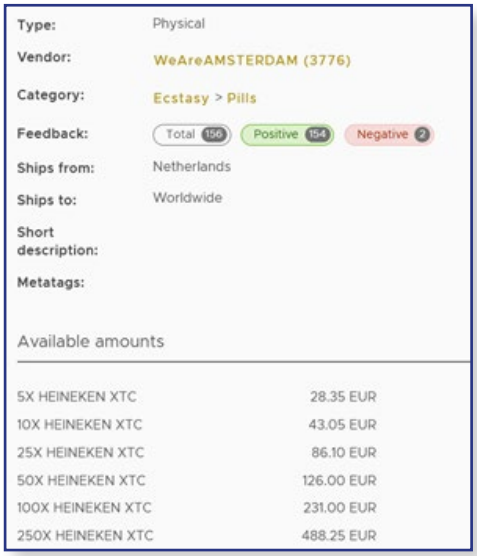
- Simulants 30
- Cannabis & hashish 0
- Ectasy 23
- Dissociatives 14
- Psychedelics 15

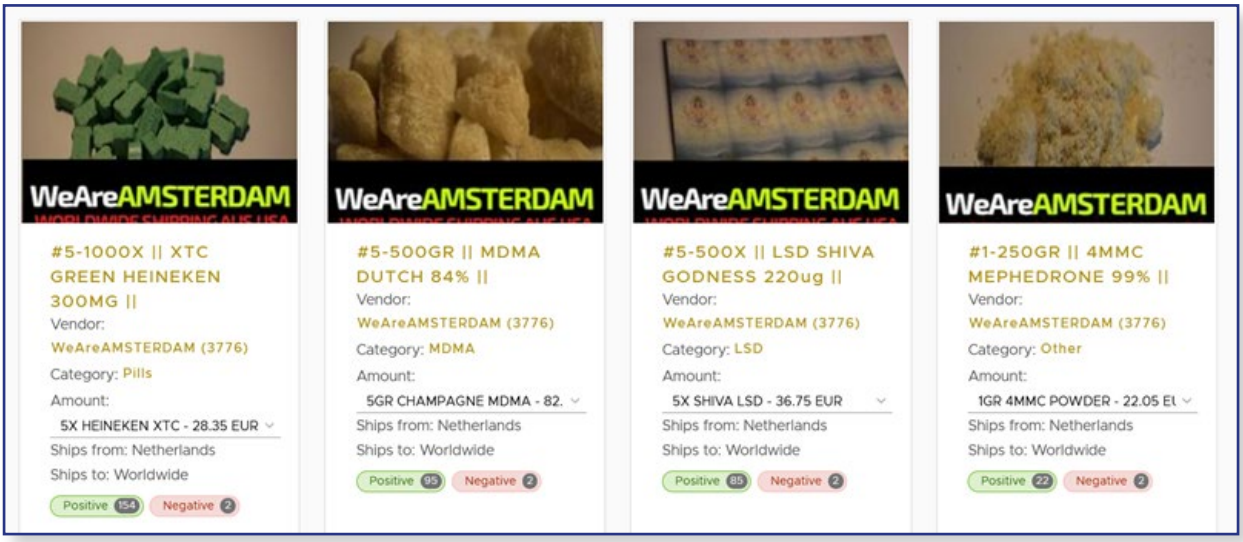
All items are available for shipment worldwide. Only wholesale orders are provided with tracking information. Vendors only offer a partial refund or reshipment fee to those who have completed at least one successful purchase with them.

WeAreAMSTERDAM accepts both bitcoin (BTC) and Monero (XMR) for payment. They use the traditional account deposit system, recommending only depositing enough funds to cover one order at a time.

The shop is universally recognised by the dark net community as a legitimate vendor with almost a decade of sales experience in various markets.







3. Carding

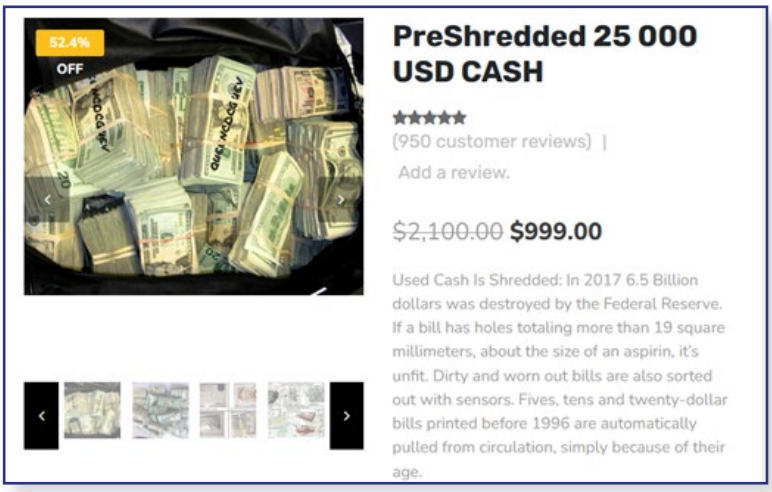
Carding refers to the use of stolen credit cards or their codes alone, stolen in various ways. In countries where credit cards for sale in underground forums are more widespread, so are thefts. That is why, in the United States, $1.50 is enough, while Europe is the most expensive market for buyers of stolen cards: they cost, on average, $8. In the dark web as in legal markets, it is the relationship between demand and availability of the product that defines the price. Cybercriminals are obviously more interested in cards with which more money can be stolen, or those with less stringent banking control systems. Below are three examples of underground markets dealing with carding:

Empire Market

"People like the dark net because there is a lot of money to be made. With high profit comes risk. If you choose us over other services, your risk is almost zero. If you can't cope with even a small risk or worry, we always recommend investing your money in a bank. Remember that it's not difficult to double or triple your money quickly on the dark net, which is why people like it. But never do anything that makes you uncomfortable"

Empire is a dark net marketplace launched in February 2018. Modelled on the AlphaBay marketplace, which was shut down, the shop deals in illegal products, but bans the sale of fentanyl and terrorist actions. Here, users are mainly looking for products related to carding, money transfers, drugs, fake money, weapons, gift cards, fake documents and hacking services. Products can be purchased using bitcoin. Registration is not compulsory and full and/or partial refunds, shipping to over 200 countries and a 24/7 support team are offered.

The shop administrators claim that they only sell 5% of their cash: 95% goes through the companies they own and then into their bank accounts; the remaining 5% is sold on TOR to obtain bitcoins. This may seem like a very small percentage, but there is a reason: buying hundreds of thousands of bitcoins every week would draw attention to them.



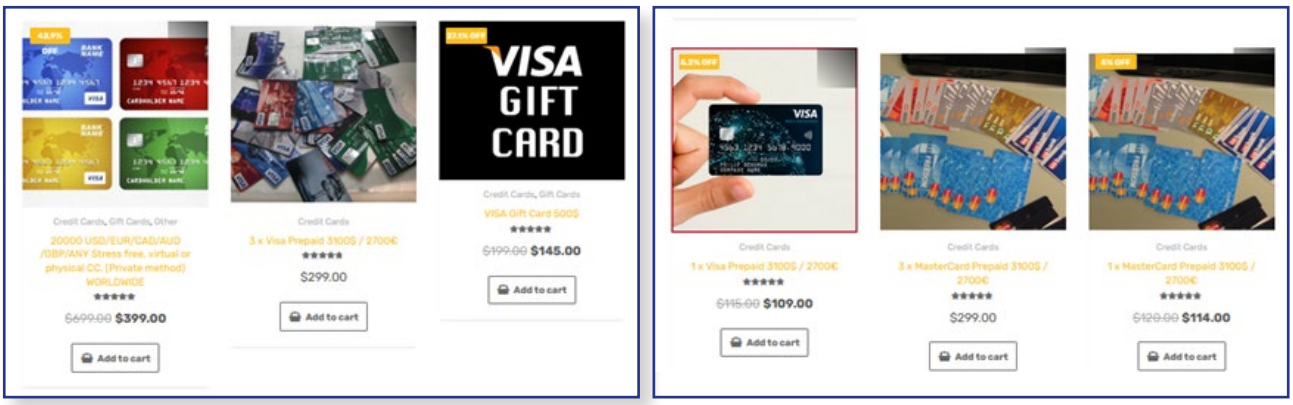
The FAQs read: "Where does this money come from? Is it real or counterfeit? This is 100% real, currency stolen from the Federal Reserve before it could be shredded. You are at absolutely no risk. Billions of dollars are selected for disposal every year. No one traces the money that is supposed to be destroyed. Deposit it in vending machines, bank accounts or ATMs with total peace of mind."

The maximum order size is $100,000. Bitcoin (BTC) and Monero (XMR) are the main currencies. However, as of 31 July 2022, Litecoin, Binance coin, TetherUSDT, Tron, Doge coin and Ethereum are also permitted. Once a purchase has been made, the goods will be marked as pending. The vendor has 12 hours to complete the order by sending the item and marking it as shipped, otherwise it will be cancelled. Once the order has been marked as shipped, the buyer can finalise it once the purchase has been received, dispute it if there is a problem, or extend the commitment if necessary.

There is a section dedicated to those who wish to become vendors, paying a commission. All vendors will be tested and checked. Vendors are required to set up a 2FA to protect their account.

Tracking is available from the day of purchase and can be found on the receipt in the confirmation e-mail you receive. Most vendors ship the package within one hour of receiving the payment notification in escrow. Large orders are shipped in boxes with labelling to make them look like an eBay or Amazon package.

Below is an example of cards sold on the site:



CardingTeam

"We are a group of professional hackers with more than 15 years of experience. We have extensive experience in this area and offer these unlimited money-making services to you. We offer a variety of hacking services. You can buy cards online, money transfers, carder tutorials, and many other services."

Carding Team is an underground credit card shop updated daily, with prices up to a maximum of $200. "We want our customers to receive the latest news from the world of carding as soon as possible."

In detail:

CVV	0$ - 80$
Transfer money price	60$ - 200$
Tutorials price	20$ - 250$

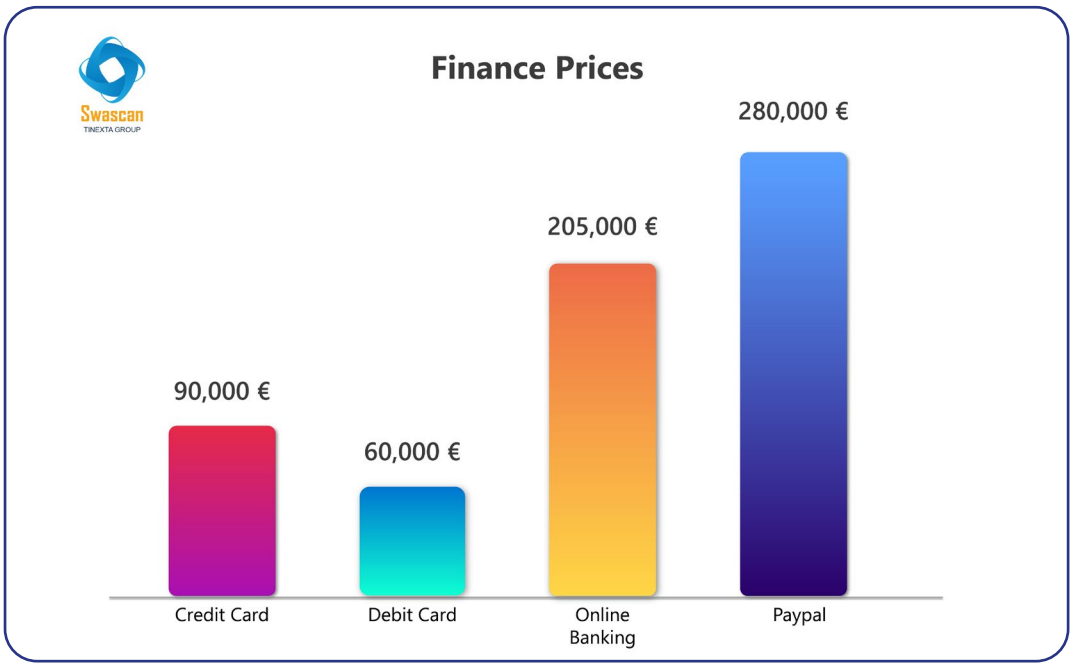
Simple Cash

"The first rule for success in carding and hacking is to keep a low profile"

Another underground market dealing with carding. Products are sent inside greeting cards, magazines, books.

Below are examples of cards for sale:

Following the analysis conducted, we can provide an average of the prices offered on Darkweb markets:



4. Identity leaks and credential access

Have you ever re-used the same password for more than one account? It is likely that everyone's answer to this question is yes. This is where cybercriminals come in, buying e-mail and password combinations from markets on the dark web and attempting to access many other sites to see if that password has been re-used. In this regard, any account containing financial information may be of value to a criminal.

Unlike the drug market, the market for counterfeit documents and credential access seems to be more concentrated, with fewer vendors operating in the niche. When analysing the documents offered for sale, we can see that there are two main types: physical documents and scans. Regarding physical documents, vendors claim that they will be accepted by the authorities as real, looking just like exact copies with all security features being replicated. Scans, on the other hand, are copies of real documents - to be used for identity fraud. During our research, the price range was from $250 to $1500, with a wide range of countries to choose from. Counterfeit identity cards can be purchased for as low as $300 for a European identity card and $250 for a European driving licence. Below are three examples of sites under the Onion network that sell identity leaks and credential access:

ONION IDENTITY SERVICES

"All passports we sell are directly from the issuing authority, they are 100% originals, just with your photo. ID Cards and Driver's Licences are professional replicas, but with all the security features (Microprint, UV, Holo)"

The market ships from Germany and does not charge postage. The products for sale are divided into 3 categories:

1. **Passaports**
2. **ID Cards**
3. **Driver's Licences**

For each of the categories there are different prices depending on the country for which the product is required. Below is a list of average prices:

1. Passaports

Lithuanian Passport	1350 EUR
Netherlands Passport	1500 EUR
Denmark Passport	1500 EUR
Great Britain Passport	1800 EUR
Canada Passport	1250 EUR

2. ID Cards

Czech ID Card	500 EUR
Netherlands ID Card	550 EUR
Denmark ID Card	550 EUR
French ID Card	550 EUR
Lithuanian ID Card	500 EUR

3. Drivers Licenses

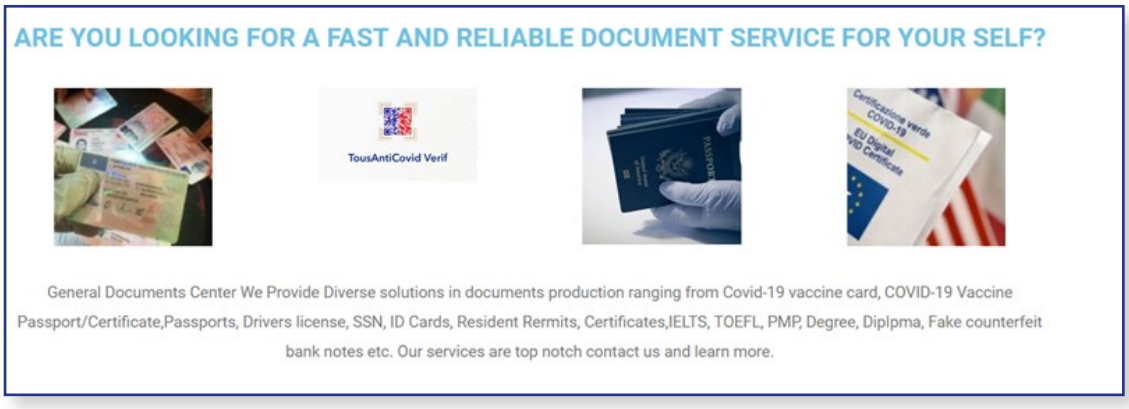
Norway Driver's Licence	550 EUR
Denmark Driver's Licence	550 EUR
Netherlands Driver's Licence	550 EUR
UK Driver's Licence	500 EUR

How does the sale work? After purchasing an identity document or passport, the administrators require a message to be sent with the buyer's age and sex entered so that a matching dataset can be found. It is possible to apply for and use the document in any country, but administrators recommend trying to avoid using it in the issuing country, since another person is already living there with that document. There are no restrictions on use with purchased documents. With regard to shipping times, it takes about 14 days for identity cards and driving licences, and 21 days for passports.

Passports are valid for 4-5 years in the Netherlands and 8-10 years in all other countries. It is not possible to request a discount.

GENERAL DOCUMENTS CENTER

"We have 17 years of experience in this network of real and fake documents. We know that your visit to this page is not accidental. We know that you have your different reasons for contacting us and wanting to buy our products. We are a very large network, supplying the world with real and fake documents. We partner with governments and other senior officials, we deal with investments, raising capital, loans and many other business opportunities."



The market guarantees a high level of privacy with regard to all personal information that is collected. ***"You can be sure that your information will never be sold to any other customer or seen anywhere on the internet. We will only use your information for the purpose for which it is intended."***

Below are some of the categories sold:

1. Covid Vaccine Certificates and PCR tests:

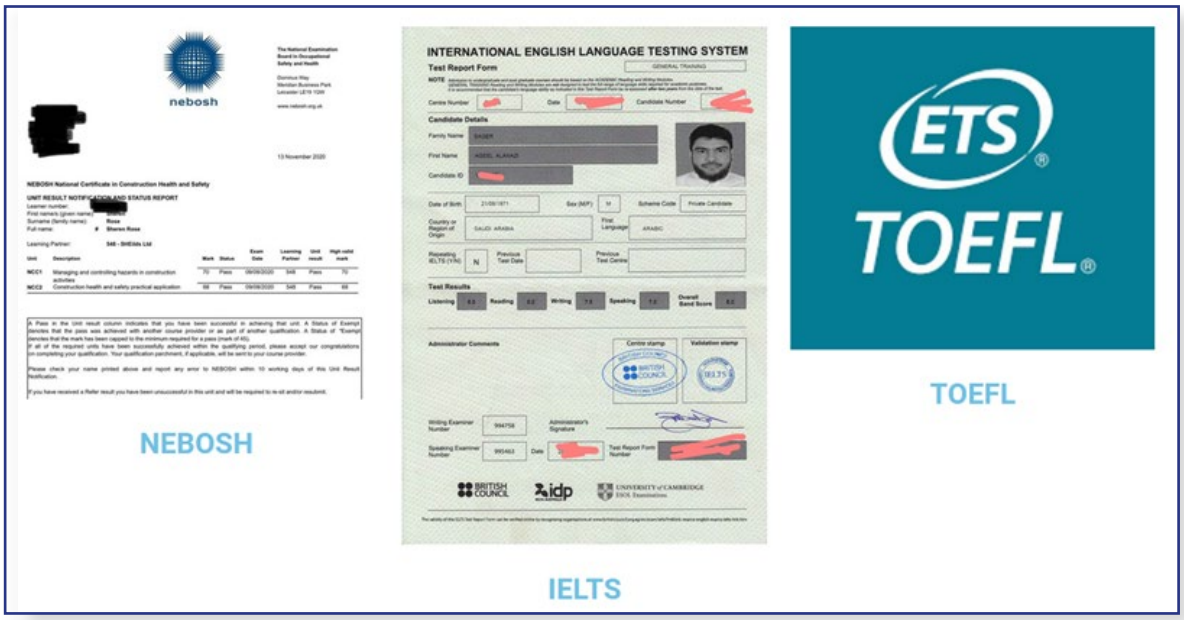
In this section, we can see in particular how people are urged to avoid being vaccinated because of the dangers it may entail, being pushed to purchase the certificate instead. The statement from the black market reads as follows: *"South Korea has recently seen the dangers of flu vaccines after a number of people in the country died as a result of seasonal flu vaccinations. A Yonhap News Agency report said there have been 48 flu vaccination-related deaths since October, including a 17-year-old boy and an elderly man from the south-eastern city of Daegu. As a precautionary measure, buy the Covid Passport, don't get the vaccination."*

2. Real and fake documents:

"for the real document we will record all the holder's information in the prospective data-base system and the holder will legally use the document without any problems"

3. All kinds of certificate:

Training certificates, international cards, adoption certificates, baptism certificates, birth certificates, death certificates, divorce certificates, marriage certificates, high school certificates and much more.



In any case, "quality" seems to be the watchword, which is why the shop administrators claim that every document sold is printed and tested on the same government machines and is registered in the system within the countries they have access to. The documents have all the security features and are all readable when introduced into a reader, NFC and RFID applications and scanners for border control, airports and police.

MONEY CASHIER

"Our team works directly with government officials and produces registered documents and passports for our customers and we also have our own immigration lawyers who oversee the entire document process such as verifying actual passports, while others make sure your information is inputted into the government database system"

Below is a list of the products offered by the underground market:

- **Counterfeit USD**
- **Passports**
- **Counterfeit AUD**
- **Counterfeit Pound Sterling**
- **Counterfeit Euros**
- **Driver's Licenses**
- **IDs**
- **Counterfeit CAD**
- **US Social Security Cards & Numbers**
- **Wire transfers**
- **Counterfeit money**

As regards the purchase: the features:

- **Free worldwide shipping on all orders over $500**
- **30-day money back guarantee**
- **International guarantee**
- **100% secure checkout via PayPal / MasterCard / Visa**

"All the secret features of real passports, IDs and driver's licences are accurately duplicated and counterfeited for 100% security when in use. We are unique professionals when it comes to producing false documents"

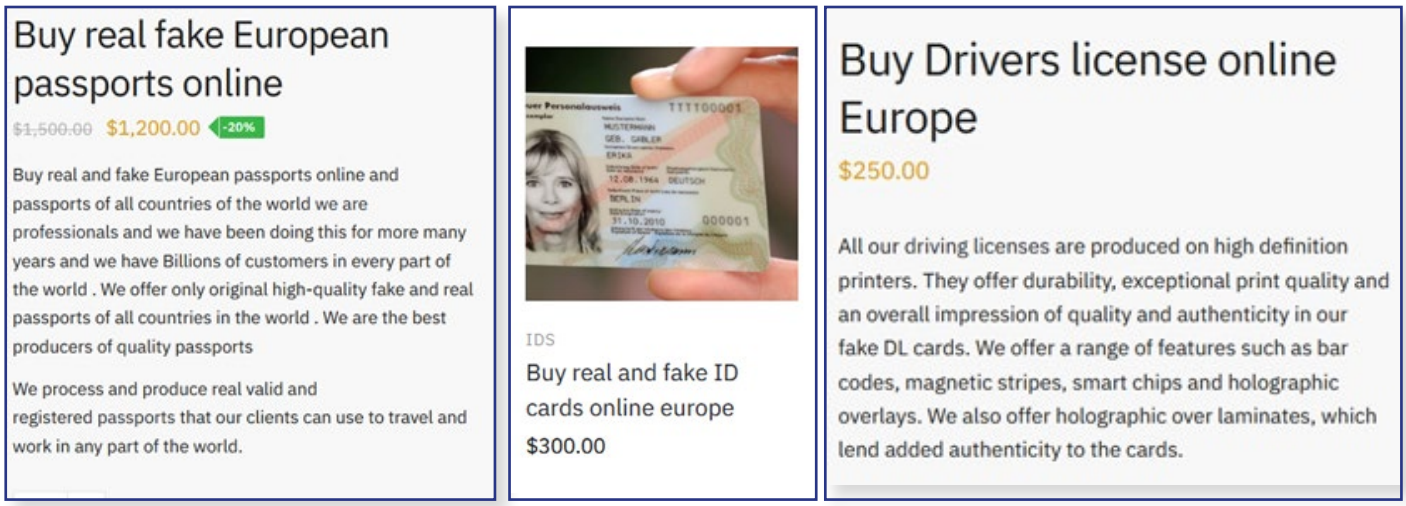
Shipments are made worldwide. Same-day delivery is offered for customers in the United States and Canada. European and Australian orders take 3 to 7 days to arrive. After each purchase or order from the site, you receive an invoice with a tracking number and shipping details so that you can check the status of your order and know when it will be delivered.

The administrators also provide security advice to vendors and 24/7 customer support via the chat from the site accessible under the Onion network or directly via WhatsApp on the number provided.

Regarding payment and operation, only Western Union and MoneyGram payments are accepted. Payment cannot be made, though, if the order is below the minimum limit, which is set at $200-$250. ID is usually only required if you are placing an order of more than $1,000. In that case, it is always possible to divide an order up into smaller orders, so as to avoid uploading personal documents. You can also only request direct home delivery for orders over $500.

In general, the lowest price that can be found on the site is $300, while the highest price is $25,000.

The shop guarantees a refund or replacement of the product within 12 days in the case of goods arriving to the customer in a defective or damaged condition, or if the customer is not satisfied with the purchase. In cases where the loss, damage or delay is due to an incorrect delivery address provided by the buyer, refunds cannot be given.



Once again, vendors are able to produce both real and fake driving licences, but customers are advised to purchase real documents if they want to use them legally. All documents are produced on high-definition printers.

5. Weapons

In the same forums it is also possible to buy weapons and ammunition from all over the world: USA, Canada, Germany, United Kingdom, France, Switzerland, Sweden, Netherlands, Norway, Denmark, Finland, Italy, Austria, Spain, Australia, Russia, India, Japan, China and many other countries.

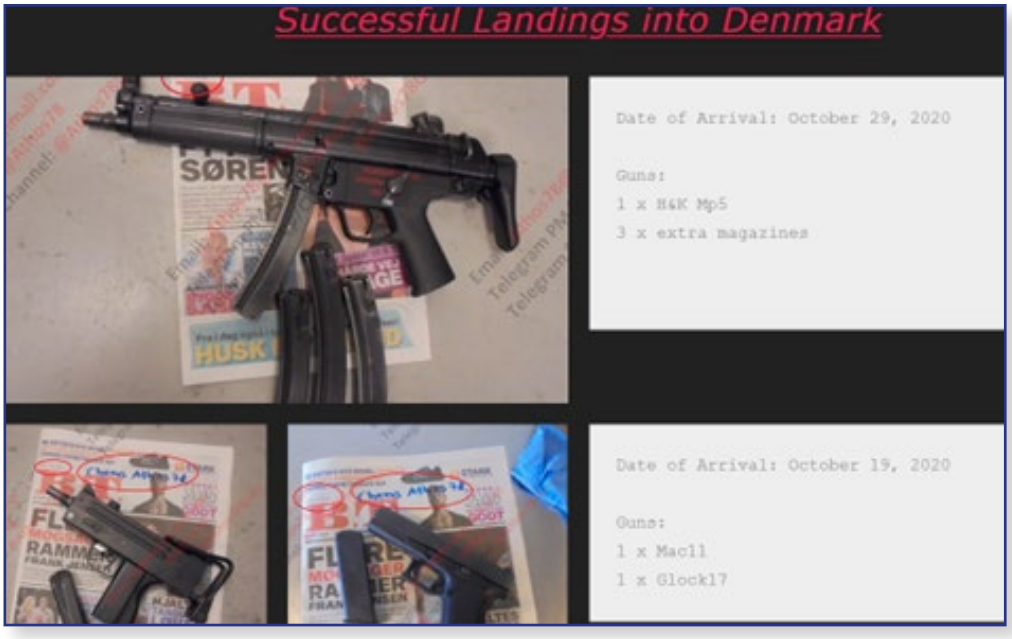
This study provides a snapshot of the availability of weapons in three dark net markets. In total, 125 weapons were identified, including handguns, rifles, machine guns, ammunition, explosives and accessories such as silencers. The markets also sold other weapons such as tasers, pepper spray and knives, DIY weapons manuals, chemical, biological, nuclear and radiological weapons. The data allowed the cost of the weapons to be estimated at up to $2,400. Most of the time, the weapons are new and unused. It is possible to decide on the place where the weapons are to be delivered: it is recommended to opt for a remote, inconspicuous and hard-to-reach place.

ATHOS78

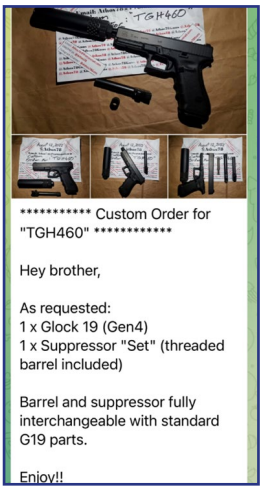
Illegal weapons site offering products to those who:

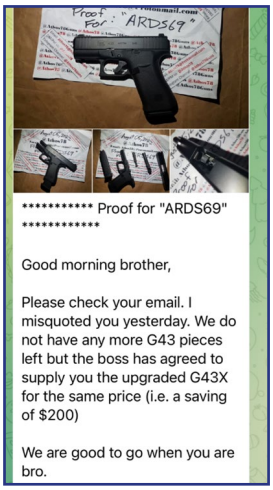
- **live in a country in which the possession of weapons is prohibited**
- **have a criminal record**
- **want to stay out of sight of the police**
- **need to ship weapons unnoticed**

The site has a whole page dedicated to the proof of arrival of weapons sold in different countries. Below is a screenshot demonstrating the purchase by a customer:



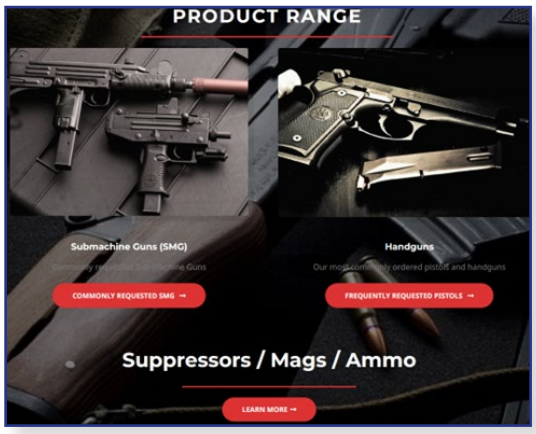
The administrators also have a page dedicated to a sample of weapons that can be supplied to customers. You can interact with the vendor and ask them to make a video while writing a code word you choose or ask them to tear off a corner of paper to prove their existence, or take pictures with the product from various angles. In this regard, the market has a Telegram channel active since February 2020 to interact with customers, showing order invoices, photos as proof of sale and shipment, and videos of vendors showing weapons.

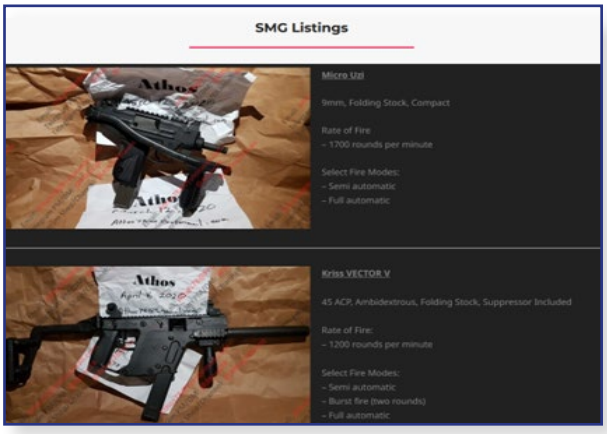


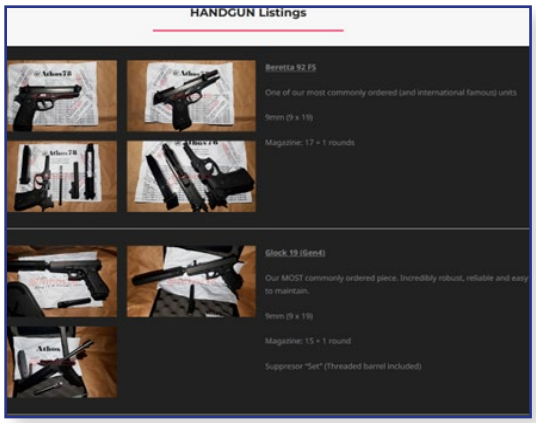


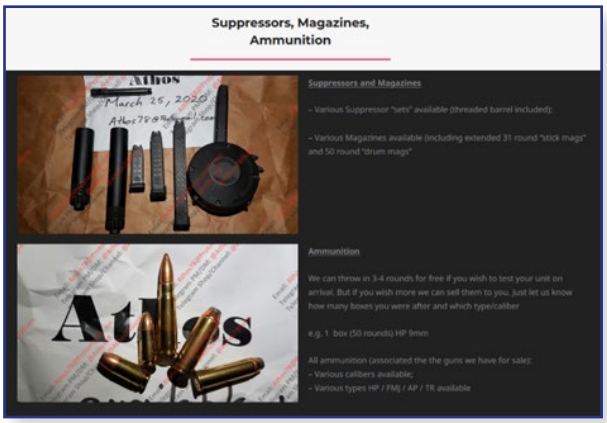
There are three categories of products that can be purchased:

- **Submachine Guns**
- **Handguns**
- **Suppressors**









Below is an average of the prices offered on the market:

Glock 20 = 1450$
Makarov = 860$
Revolver 357 = 480-1100
Glock 26 = 1450$
Beretta= 780$
FN =500$
Ak-47=2200$
Sig sauer = 525$
CZ 75= 790$
Uzi = 1800$
Glocks 19 = 1200$
Glock 17= 1050$
CZ Shadow 2 = 860$
Desert eagle =1700$

THE DARK MARKET

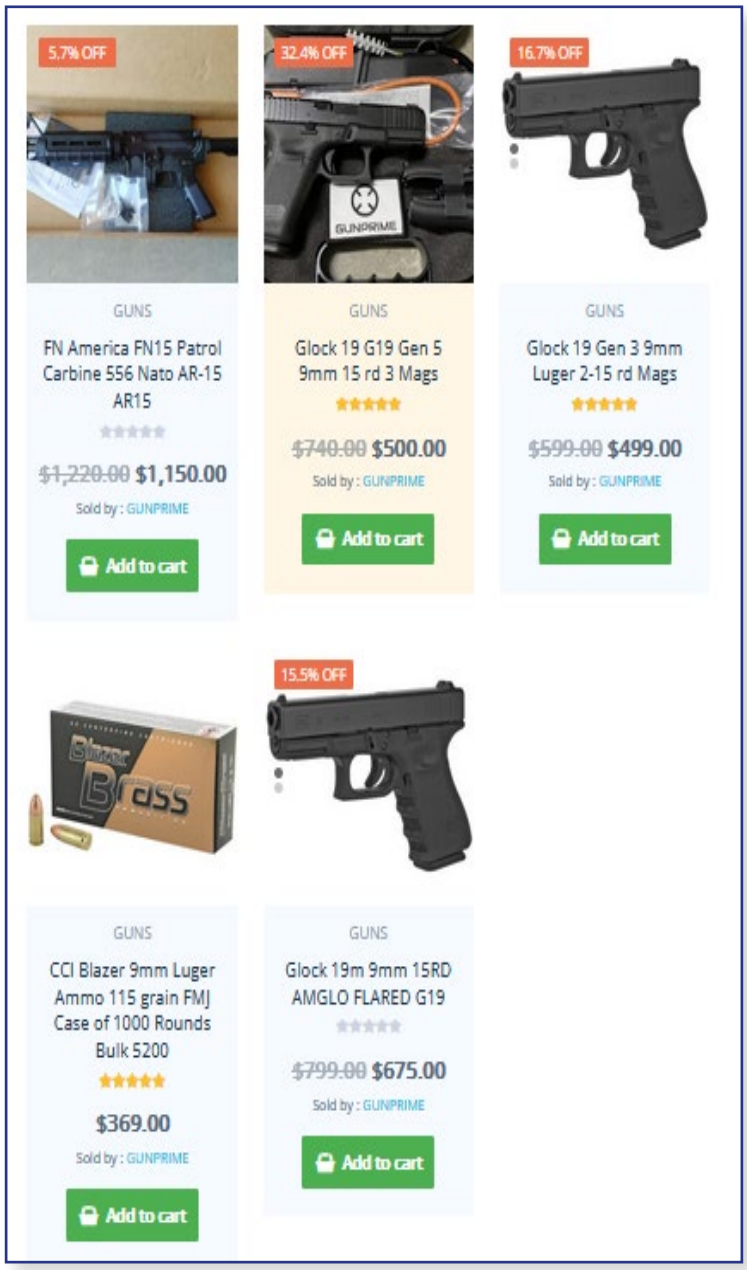
"Our vendors are the heart of the Dark Market. They provide high quality verified products that separate a dark net marketplace from a clearnet shop. Our vendors are hand-picked by our team in order to offer a state-of-the-art product catalogue."

THE DARK MARKET is a dark net marketplace launched in March 2020 offering products in the following categories: counterfeits, drugs, credit cards, documents, electronics, gift cards, guns, hacking services, money transfers and more.

Vendors are chosen by the site administrators. Although the market deals with illegal products, it has banned the sale and reproduction of terrorist material and/or activities. All vendors must have a PGP key before they start selling to communicate with the administrator. Two-factor authentication (2FA)

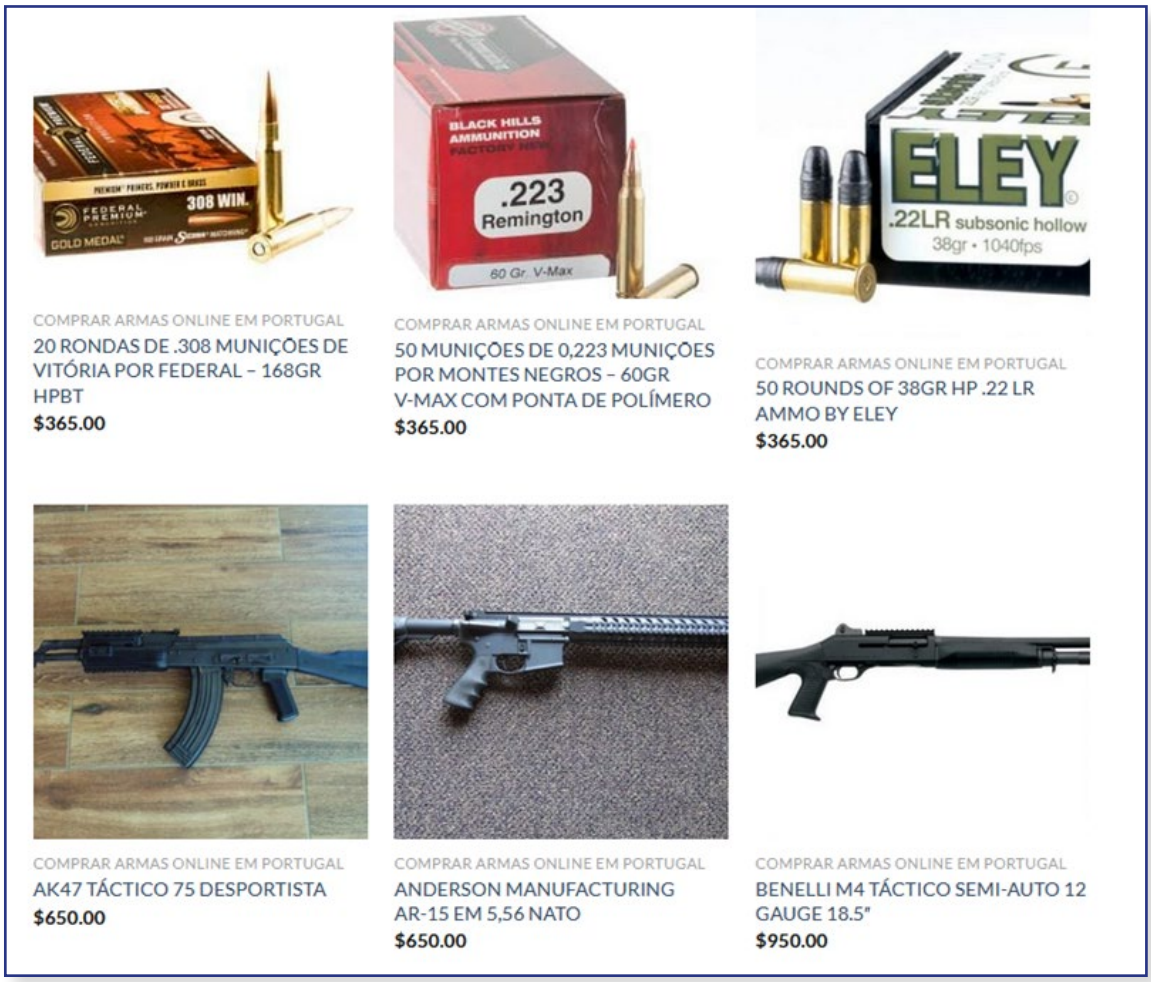
is mandatory for all vendors, who have to pay $400 in order to be able to start selling on the site. The vendor's commission is non-refundable in order to protect the market from fraudsters. The buyer cannot be asked for money before the product arrives and no transactions are allowed outside the marketplace. Any vendor caught dealing outside the market, using third-party apps, will be banned immediately.

All vendors ship worldwide with a tracking system sent by e-mail within one hour after payment. Most vendors ship the package within one hour of receiving the payment notification in escrow.



BOTMANS WORLD

"Botmans Ammunition World has made shopping for firearms more advantageous by offeringa selection of guns accessible for purchase on the web"



The site has been active since October 2021, and it is possible to purchase different types of weapons, including ammunition, handguns, rifles and revolvers, with prices ranging from $10 up to $2,500.

Weapons are shipped in 5 to 8 working days (15 to 18 working days for Alaska).

Buyers of firearms must be at least 21 years old, with the exception of some weapons which can also be sold to those who are 18 years old. The shop accepts no liability if the weapons violate laws in the buyer's country.

Online firearms safety courses are also available on the site for a better training procedure

Designed by "firearms instructors", as they call themselves on the site, this online firearms safety course includes the theoretical CFSC and CRFSC part. It combines knowledgeable videos, informative slides and relevant quizzes to help you prepare. Several students use this theoretical online course to supplement their firearms safety coaching before attending a course or as a review and refresher.

The course focuses on:

- **The evolution of guns, main parts, types and actions**
- **Basic firearms safety**
- **Operational firearms**
- **Safe handling and transport procedures**
- **Techniques and procedures for use**
- **Firearms care**

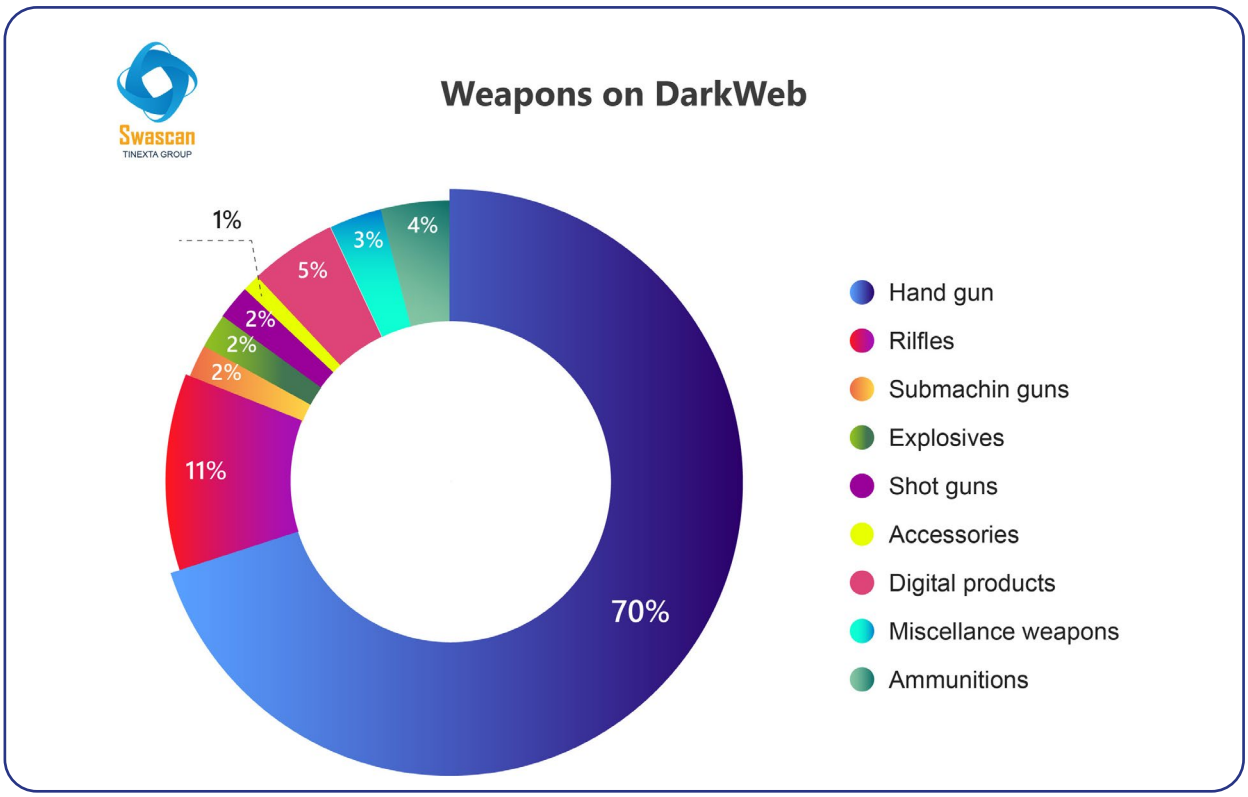
- **Safe storage, display, transport and handling of firearms**
- **Ammunition**
- **Liability of the owner/user of the firearms**
- **Video and practical tests**

As with purchases on the clear web, packages are provided to attract buyers: if this online firearms safety course is purchased in combination with other courses, you receive the opportunity to retake the tests free of charge, otherwise you have to pay $60.

Administrators also offer a COVID-19 option, extending the dates for completion of the course in the event of positive cases. A pass mark of 70% is required for the written examination.

Following the analysis of the three sites, we provide a graphic visualisation of the weapons sales present

on the dark web:



HIRING A KILLER ON THE DARK WEB

What could you buy if you knew no one was watching? When the conversation turns to the topic of the dark web and what you can get hold of there, the first things that come to mind are probably the illegal items mentioned above: drugs, documents, weapons...

But material goods are not the only things people buy in the untraceable corners of the internet. Every now and then, news emerges about someone who has attempted to use the dark side of the web for another purpose: murder. When we think of the dark web, most of us imagine a shadowy and sinister place, a "dark" place, in fact. Nevertheless, the vast majority of people have never actually visited it, or even know how to; all we know is that its cloak of anonymity is another weapon in the modern criminal arsenal, and while it may serve perfectly innocent purposes, the illegal activity that goes on in the shadows may be even darker than we could suspect.

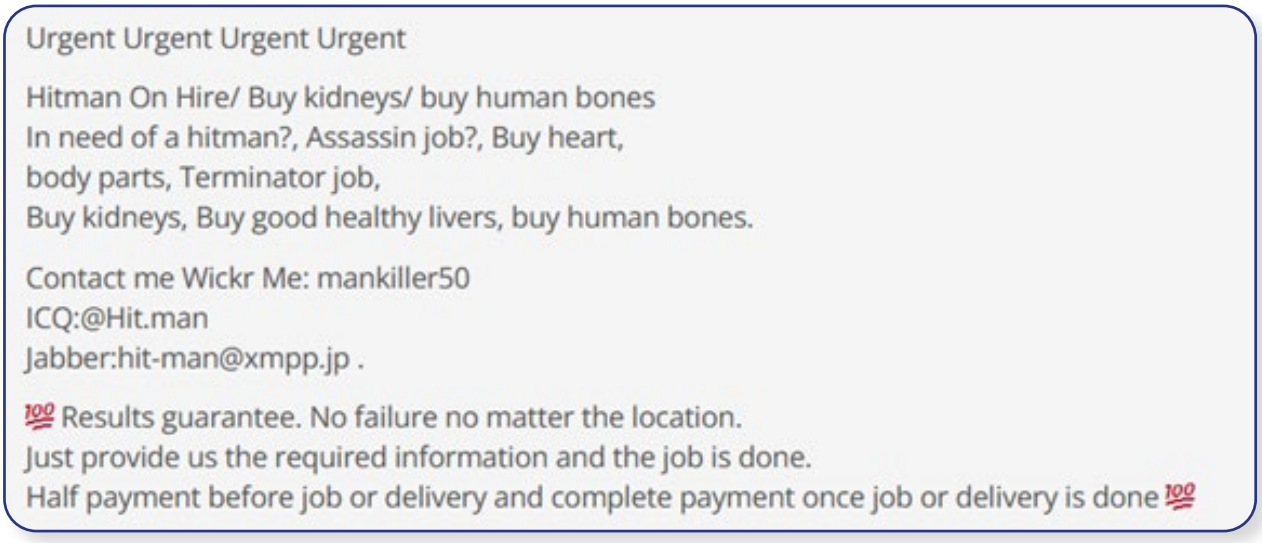
In fact, its emergence over the last ten years has enabled the proliferation of Killing Forums, with the presence of hitmen within. Unlike most traditional internet sites, sites under the Tor network use technology that allows online interaction between client and server while concealing their identity and location, both from each other and from law enforcement agencies. Although most murder-for-hire sites on the dark web are probably scams, people still try to solicit contract killers. Despite frequent reports of arrests in the media, the number of adverts for such services and the creation of new Killing Forums continues to be a growing trend.

In some dark web forums, the killers describe themselves as "***the most reliable, secure and powerful on the market. We have thousands of satisfied customers and hundreds of hitmen. If you're trying to kill someone, beat them up or kidnap them, don't do it alone! Let's see if we can do it for you at a low price.***"

The features they offer:

1. Anonymous, secure and complex market
2. 0% down payment, you just have to provide proof that you have bitcoins
3. Best value for money and hundreds of hitmen to choose from
4. Positive feedback everywhere, no complaints
5. Encrypted communication between customers and hitmen
6. Request progress display
7. PGP support for additional security
8. Built-in mixer for enhanced bitcoin security
9. 100% guarantee of the job being completed. If a job can't be done, the forum administrators don't take it on
10. Chat between forum members

The market is used by thousands of gang members and hitmen. Clients are completely anonymous: no name, no phone number, no e-mail address, no bank account and no credit card.


Urgent Urgent Urgent Urgent

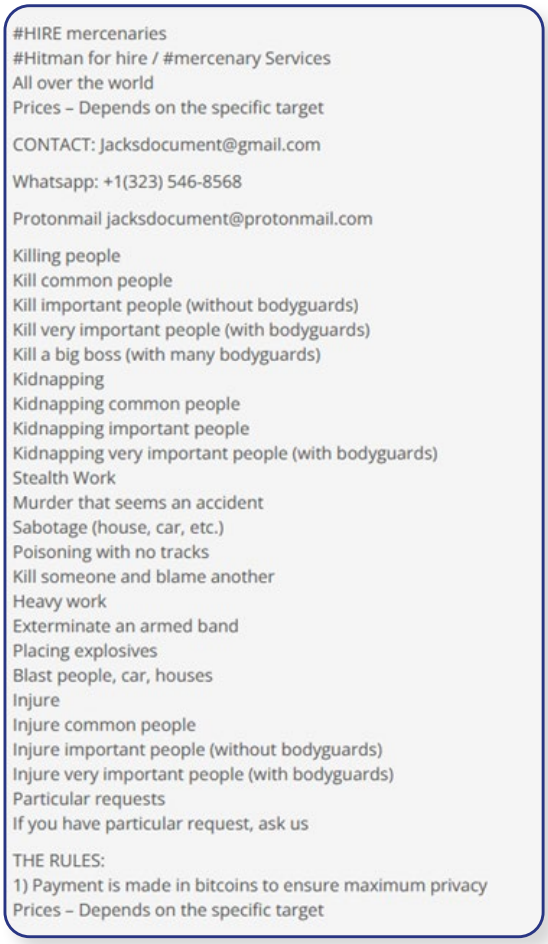
Hitman On Hire/ Buy kidneys/ buy human bones
In need of a hitman?, Assassin job?, Buy heart,
body parts, Terminator job,
Buy kidneys, Buy good healthy livers, buy human bones.

Contact me Wickr Me: mankiller50
ICQ:@Hit.man
Jabber:hit-man@xmpp.jp .

💯 Results guarantee. No failure no matter the location.
Just provide us the required information and the job is done.
Half payment before job or delivery and complete payment once job or delivery is done 💯

Why Hire a Killer on the Dark Web?

On some Killing Forums, such as "Hitmen Cyber Team" or "Jabba Syndicate", the hitmen warn of killers who might be hired elsewhere, stating that the others require a 50% down payment before the hit is carried out, pointing out the possibility that if the hitman absconds with the money, you cannot go to the police. In the service provided in the dark web forums, no advance payments are made: proof of funds are provided, the work is carried out and payment is only made upon completion. No risky and dangerous encounters between clients and hitmen: there is no risk of being arrested by undercover cops or being blackmailed as the client's identity is concealed.



#HIRE mercenaries
#Hitman for hire / #mercenary Services
All over the world
Prices – Depends on the specific target

CONTACT: Jacksdocument@gmail.com

Whatsapp: +1(323) 546-8568

Protonmail jacksdocument@protonmail.com

Killing people
Kill common people
Kill important people (without bodyguards)
Kill very important people (with bodyguards)
Kill a big boss (with many bodyguards)
Kidnapping
Kidnapping common people
Kidnapping important people
Kidnapping very important people (with bodyguards)
Stealth Work
Murder that seems an accident
Sabotage (house, car, etc.)
Poisoning with no tracks
Kill someone and blame another
Heavy work
Exterminate an armed band
Placing explosives
Blast people, car, houses
Injure
Injure common people
Injure important people (without bodyguards)
Injure very important people (with bodyguards)
Particular requests
If you have particular request, ask us

THE RULES:
1) Payment is made in bitcoins to ensure maximum privacy
Prices – Depends on the specific target

"It's simple, it's convenient, it's safe, it's anonymous, it keeps you off law enforcement's list of suspects. After you have provided us with details of the target and shown us proof that you have funds available, we will assign a hitman to the job. He will give an estimate of the date of the murder: on that date the client can travel to a different city and visit a shopping centre with CCTV to ensure they to have a strong alibi."

Once the job is done, the hitman sends a confirmation, and the client can request up to two weeks to personally confirm that the job has been done before releasing the funds to the hitman.

To put in a request, simply fill in a simple form and send a picture of the target to be hit and their location.

Proof of funds can be provided by placing it in a secure escrow, to be chosen by the client.

The funds remain there until the client is satisfied with the work.

Within the marketplaces, there is also advice on how to use hitmen's services: a client should follow certain rules to avoid being arrested or scammed.

- Rule number 1: Remain anonymous. "Don't let the killer know who you are. Don't give your name, phone number, e-mail address, credit card or bank account and hide your IP with a VPN or Tor Browser. If the killer is arrested, they will not be able to say who hired them."

- Rule number 2: Don't meet the hitmen in person. "The internet is full of news about people being arrested when they tried to meet a hitman in person."

- Rule number 3: Always use a form of communication that keeps your identity secret. "Never

- communicate with a killer using a real e-mail or telephone number."

- Rule number 4: Never pay in advance. "No 50% advance, no money before the murder is done. An external escrow can be used to prove that you have bitcoins ready for the kill."

As a matter of fact, one of the systems that has made bitcoin payments secure for customers and merchants is known as Bitcoin Escrow, a kind of security filter for parties using it so that they cannot fall for online scams. By using an escrow, the buyer doesn't send the bitcoins directly to the seller, but to an escrow, which will remain blocked until the buyer is satisfied with the service. If there is a dispute, the escrow administrator intervenes and arbitrates the deal for a fee. Although it started out

as a service for lawful purposes, there are escrows on the dark web used for illegal requests that accept bitcoin and provide full anonymity for the client and vendor. Firstly, a commitment transaction is created in which the price, job description, and expected time for completion are entered.

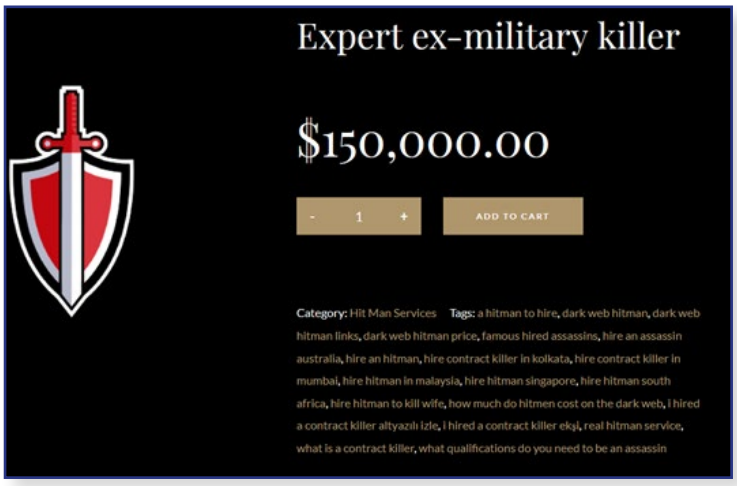
Subsequently, bitcoins are put in the escrow, to show the killer that you have the funds.

Once the killer does the job, the funds are released to them. If the killer fails to do the job, the funds are claimed back from the escrow administrator. On the contrary, if the killer performs the work and the client refuses to pay, the killer will send a complaint to the escrow administrator together with proof that the work had been carried out, and will request the money to be sent.

Price list

We talk about crime-as-a-service, i.e. crimes that are commissioned to specialists via the web. As these underground markets have hundreds of hitmen, the prices on offer that differ from hitman to hitman. Each killer can set their own prices for the services they provide, given their skill level.

Some less skilled criminals have lower prices, while experienced ex-military personnel who can take down more important targets will have higher prices.



Below is an average of the prices of the most common options that can be found on the dark web forums:

SERVICE	AVERAGE PRICE
MURDER by:	
Gun	15.000$
Knife	22.000$
Poisoning	40.000$
Painless poisoning	42.000$
Torture	50.000$
"Accidental" death	20.000$
ASSAULTS:	
Acid	4.000$
Facial disfigurement	3.000$
Paralysation	10.000$
Castration	30.000$
Other methods:	
Robbery	2.000$
Assault	2.000$
Arson	8.000$
Kidnapping	15.000$

In any case, prices vary according to many variables. For example, as reported in a dark web forum, in a Shen-Buzhri commune in the Canton of Geneva, the husband ordered the murder of his wife by three Kosovo natives who were to receive 400,000 francs. In another case, the mother-in-law and wife ordered the murder of the husband for 50,000 francs, while the owner of a restaurant paid 20,000 to get rid of their competitor.

Prices also vary by country. In Russian forums, for example, the average prices are as follows:

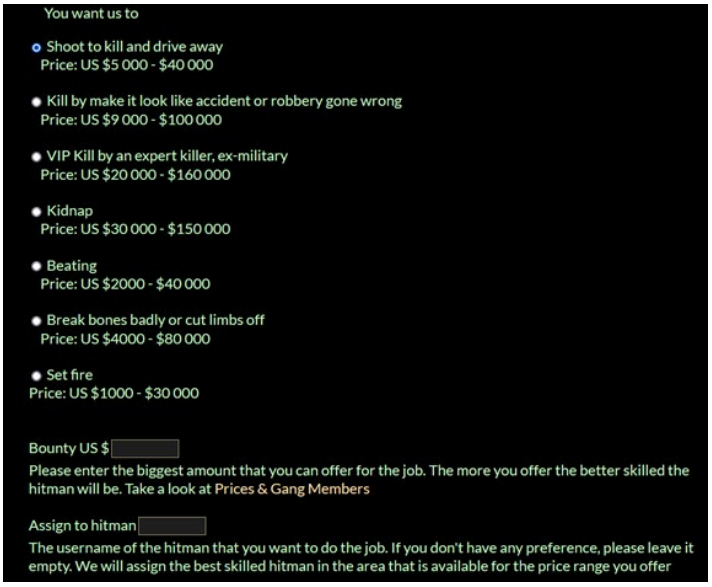
- murder of an ordinary citizen $8000-$10,000
- murder of an average businessman $12,000-$18,000
- murder of a Member of Parliament from $40,000
- murder of an oligarch from $80,000

In general, the price will depend on the complexity of the order and will be set on a case-by-case basis.

The order forms

Il modulo d'ordine è anonimo e criptato. Non verranno chieste informazioni sul cliente, è necessaria solo la destinazione.

To get an idea of what you should offer, you can ask a question on the discussion forum: the forum administrators recommend that you do not specify your name, or the destination address on the forum itself as it is visible to everyone, but only indicate the country, the difficulty of the work required and other generic information that may be useful for the purpose. The best killer for the job will be assigned, considering the difficulty of the job, cost and location.



How to evade checks

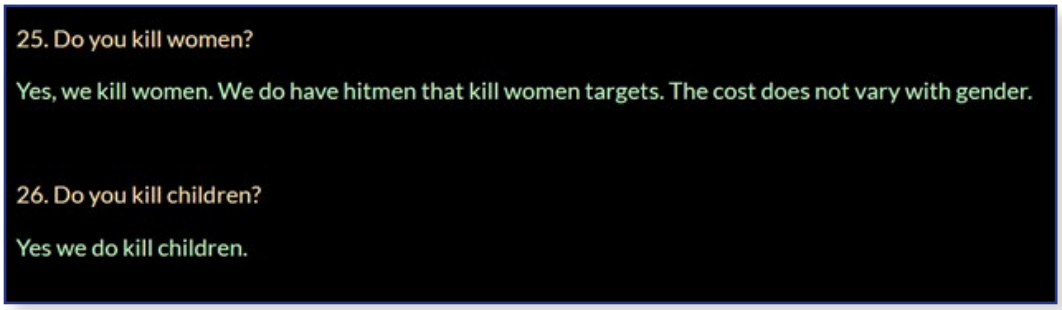
In the FAQ section of one of these forums, one of the questions is as follows: "Why aren't LEOs (an acronym for Law Enforcement Officers, used more generally for all law enforcement agencies, such as police, FBI, NSA, all agents who work for the government to catch criminals) able to catch our gang members by issuing false orders?"

The answer given is that before attacking a target, gang members carry out background investigations. Once an order is sent, a gang member is sent to the scene: they will look like a normal, unarmed civilian, driving and walking down the street in the area. Once the target has been identified, the hitman will look around for suspicious vans or cars that could be protecting the target.

Criminal gangs also test all members who sign up as hitmen: they do not rely on photos or videos, because these could be fake, they go on site to check that the request is actually carried out: "Undercover police, unable to harm innocent people, would fail the test."

"That's why the police do not make false orders. It is too much trouble is they mess up, and too small a reward. If they get one hitman after their target, the mechanism will continue to work, and their victim will already be dead."

Another frequently asked question concerns the type of jobs accepted by gangs. Generally, jobs involving minors under 16 years of age are not accepted in the forums. Other exceptions could be high-level politicians and some well-protected famous individuals, leaders etc. The assessment is made on a case-by-case basis. Nevertheless, as you can see in the image below, some forums also freely kill women and children, without any variation in price.



CONCLUSIONS

The proliferation of black markets as well as the number of items for sale is rapidly assuming worrying proportions. We are faced with goods - of all kinds - sold at very affordable prices.

We must reflect on how much - in addition to the classic illicit activities on the darkweb - cybercrime in a broad sense is becoming increasingly 'ready to use'.

It is not unrealistic to imagine how, by adding a veritable e-commerce of ready-to-use hacking tools to the equation, cyber crime continues to proliferate.

It is a definitive paradigm shift: whereas until a few years ago, those who created malware and other tools for cybercrime were then also the end users, today those who have acquired sufficient skills and expertise to complete the first step have changed their "business model". They merely sell their "product" to third-party criminals. Skills are for sale.

The mantra of motivation, opportunity and means has not changed, but whereas opportunities and means used to be limited to a small number of criminal hackers, today, with the creation of this sort of cyber crime free market, opportunities and means have increased disproportionately.

CYBER SECURITY FRAMEWORK

The best approach to increasing perimeter resilience is through the three pillars of modern cyber security. For this reason, it is important to solidify and respects the three criteria of:

- **Predictive Security**
- **Preventive Security**
- **Proactive Security**

Predictive Security

1. Domain Threat Intelligence
2. Cyber Threat Intelligence
3. Early Warning Threath Intelligence
4. Technology Monitoring
5. Social Threat Intelligence
6. Supply Chain Cyber Risk

Preventive Security

1. Vulnerability Assessment
2. Network Scan
3. Penetration Test
4. Code Review
5. Phishing Attack
6. Smishing Attack
7. Security Management
8. GRC Assessment
9. Cyber Academy
10. DevSecOps
11. Cyber Security Framework Checkup
12. Ransomware Attack Simulation
13. SOC Performance Simulation
14. Zero Day Attack Simulation
15. CISO as a Service
16. Competence Center as a Service

Proactive Security

1. Security Operation Center
2. Incident Response Team

CYBER THREAT INTELLIGENCE

This research was made possible by the expertise of **Swascan's SoC** and threat intelligence team and the threat intelligence platform.

Cyber Threat Intelligence is the data used to understand the threats that have hit, want to hit or are about to target a company's perimeter.

This information is used to prepare, prevent and identify possible cyber attacks that seek to breach and acquire sensitive corporate data (or alternatively, simply be disruptive).

The utility of **Cyber Threat Intelligence** is obvious. It helps companies gain valuable knowledge about the most directly threatening threats, build effective defence mechanisms (Cyber Resilience) and mitigate risks that could damage profits and reputation.

Targeted attacks require a targeted defence and **Cyber Threat Intelligence** offers the chance to defend yourself in a more proactive manner.

Cyber Threat Intelligence: in detail

Cyber Threat Intelligence represents the intelligence capacity developed in the cyber security field. It includes gathering and analysing information in order to characterise possible cyber threats from a technical point of view in relation to specific operational contexts.

The purpose of **Cyber Threat Intelligence** is to identify any public information, available at **OSINT** and **CLOSINT** level, relating to a specific target.

The term **OSINT,** acronym of Open Source Intelligence, it refers to the process of gathering information by consulting public domain sources also known as "open sources".

Doing **OSINT** means describing information that is available and open to the public, through a process of searching, selecting, screening and reporting, to a specific recipient in order to satisfy a need for information.

The most important step in the **OSINT** process is to "screen" relevant and reliable sources. This is done starting from different types of public domain sources.

OSINT therefore differs from an ordinary search for information because it applies an information management process with the aim of creating specific knowledge in a given field/context.

The term **CLOSINT,** on the other hand, refers to Closed Source Intelligence i.e. the process of gathering information by consulting "closed sources", not accessible to the public or in "reserved" areas.

Cyber Threat Intelligence: the scope of analysis

Cyber Threat Intelligence is carried out through a process of searching for, identifying and selecting publicly available information using OSINT/CLOSINT at the level of:

- **Target**
- **Asset Digitali**
- **IP**
- **E-mail address and information relating to employees of a company**

The aim? **The aim is to provide "actionable intelligence"** i.e. analysed, contextualised, timely, accurate, relevant and predictive information. The aim is to determine any exposure to cyber security risks.

Cyber Threat Intelligence: the perimeter

The scope of Swascan's Cyber Threat Intelligence relates to:

- Advanced Intelligence: Includes eCrime Intelligence and Domain Monitoring;
- Network Intelligence – Infected Host;
- Network Intelligence – Vulnerable Host;
- eCrime/Dark Web Intelligence: Aggregated Forum Communications and Threat Actor Library;
- Malware Intelligence: Active Malware Sandbox and Library of Binaries;
- Risk Intelligence:
  - Compromised Credit Card Feed;
  - Anti-Money Laundering Feed
  - Account Take-Over Defence.
  - ....
- Compromised Credentials;
- Honeypot Intelligence;
- Financial Fraud Intelligence.

The Cyber Threat Intelligence (CTI) service can seek out, monitor and analyse subjects of interest (SOI) in several sources, including:

- Dark web communities and marketplaces (TOR-based);
- Underground communities and marketplaces (internet-based);
- Social media networks such as Facebook, Twitter, LinkedIn etc.;
- Instant messaging, such as Viber, Telegram, QQ, WeChat etc.;
- Internet Relay Chat (IRC);
- Integrated Intelligence Repositories (IOCs, TTPs, Security Incidents).

Cyber Threat Intelligence: The analysis phase

The activity involves gathering and analysing information relating to a series of critical macro areas..

Data Breach

The first pool of data taken into account comes from data breaches, which are increasingly omni-present even in the daily news.

The raw data of: exfiltrations **aimed at the person concerned and third parties are analysed.** Compromised e-mails are also included, of course.

Depending on the case, it is possible to provide:

- **Password used**
- **Password hash**
- **Record without password, but of which there is a trace in the deep and dark web**

Statistics show that between **60% and 80% of users** use the same password - or easily guessable variants of it - on the corporate system (Active Directory authentication, e-mail, VPN access, Remote Web access, intranet etc.).

The risk is that an external agent (criminal hacker) will acquire the compromised credentials and attempt to gain unauthorised access to the company's digital assets.

A second scenario relates to **social networks** i.e. the compromised credentials of employees and contractors of the company on platforms such as LinkedIn, Facebook, Twitter etc... In this context, criminal hackers can access the affected social network as an employee or contractor of the company. Thus, posing as that person, they send malware to other colleagues, employees or contractors of the target company.

The aim is to perpetrate targeted attacks on digital assets and company communications - **Email and/or social networks.**

Network Hygiene

"Network hygiene" refers to the presence of malicious or suspicious activity within the client's digital perimeter. Depending on the type of evidence found, the keyword can be associated with the "IP reputation" i.e. the reputation of certain IP addresses known worldwide to the various cyber security communities and antivirus companies. This is for having carried out illegal activities or for indirectly facilitating such activities (due to configuration and/or implementation errors) with all legal (civil and criminal) consequences.

Depending on the various network hygiene shortcomings, the consequences can be manifold:

- Abuse of web forms for requesting information, resulting in fraudulent use of the client's systems for mass sending of "spam e-mails";
- Using badly-configured systems to redirect DNS and intercept all data traffic;
- Abuse of misconfigured systems for "bridge attacks" (launchpads), resulting in civil and, above all, criminal liability;

DarkWeb

Historically, **the darkweb** was one of the best-hidden places on the net, where only the pioneers of underground criminal hacking ventured. Today, mimicking the success of online retail, the dark web has equipped itself with one of the keys to the success of its legal counterpart, guarantees. These e-commerce shops operate on platforms that allow people to review "products", leave a rating and obtain purchase guarantees. Everything is then framed by an intuitive and responsive interface that is easy to navigate.

This is where cryptocurrencies come into their own due to their characteristics that allow for great anonymity and low traceability.

The top-ranking goods include countless hacking tools, **but also packages of illegally obtained sensitive data.**

This is why the analysis of instances on the dark web is crucial. The tool tracks down cyber criminals, on cyber crime forums, who have mentioned the company (domains, IP addresses, brands or names of executives).

The severity and impact must be assessed according to what has emerged from the analysis and interpretation of data on the dark web.

Botnet Activity

A **botnet** is defined as a collection of devices connected to the network that have been compromised by a threat actor.

These act as a force multiplier for all those (from the individual to the organised group of criminal hackers) who intend to launch cyber attacks to breach systems or cause disruptions.

Their most frequent use is in DDoS (Distributed Denial of Service) **attacks.** Here, they harness the overall computational power of the infected machines. The aim is to send huge volumes of spam, steal credentials on a large scale and spy on people and organisations.

Criminal hackers build their botnets by infecting network-connected devices with malware and control them using a C&C (Command and Control) server.

What makes this method of attack even more dangerous is that once a single device has been compromised, all devices on the same network are exposed to the risk of infection.

A well-designed **botnet** attack can undoubtedly be devastating. We only have to remember the infamous Mirai which, in 2016, struck and effectively "shut down" giants such as CNN and Netflix. In that case, Mirai relied on a large number of IoT devices, notably security cameras, but it can't be ruled out that far more common corporate assets could be used.

It is precisely this latter aspect that is one of the biggest factors in the increase in the use of these techniques. It allows the attacker to use the victim's hardware and electricity to mine cryptocurrencies, such as bitcoin or Ethereum.

As if that were not enough, the "bot hardener" (the botnet operator) can use its botnet to instruct it. This is done in order to steal credentials (e-banking, corporate intranet, civil and criminal liability, theft of information, industrial espionage etc.).

Miscellaneuos Risks

Several sub-categories fall into this digital risk category: **IP Reputation** (see below), **passive DNS** etc. The impacts vary according to the type of information that is present outside the client's corporate perimeter.

IP Reputation

The "reputation" of a public IP address is comparable to its "network history". This shows the history of malicious actions that have been carried out, have passed through said IP address or have had it as their final destination. Civil and criminal legal liability, theft of information, industrial espionage etc.

Passive DNS

This is a type of **medium to high-level attack,** via which configuration changes are made to the client's DNS. Interception and/or redirection of internet traffic.

Brand Names

Indicates the presence of instances of the **client's brands on the darkweb**. It may be an indicator of fraud in progress or already committed.

Executives

Indicates the presence of instances relating **to the names of executives, communicated by the client on the dark web** or in other databases. Depending on the type of instance, it can represent different types of impact.

Threat Intelligence

Swascan's Cyber Threat Intelligence and **Domain Threat Intelligence** services are the answer to preventive security.

HOW TO DEFEND YOURSELF

Predictive Security

1. Identifies cyber threats outside the company perimeter operating at the level of the web, dark web and deep web;
2. Searches for emerging threats;
3. Performs early warning activities;
4. Provides evidence to preventive security;
5. Indicates areas of concern to proactive security

Preventive Security

1. Checks and measures the cyber risk;
2. Defines the remediation plans;
3. Indicates the risk exposed to the proactive security layer;
4. Provides areas of investigation to predictive security.

Proactive Security

1. Identifies cyber threats operating within the company perimeter;
2. Counteracts and blocks cyber attacks;
3. Manages cyber incidents;
4. Provides evidence to preventive security;
5. Indicates areas of investigation to predictive security.

Analysis by:

Martina Fonzo
Riccardo Micchetti

Technical Contributors:

Soc Team Swascan

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

Milan
+39 0278620700
www.swascan.com
info@swascan.com
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI