Swascan

TINEXTA GROUP

DarkWeb Analysis 2022

www.swascan.com

info@swascan.com

SOMMARIO

Chi Siamo 03

Executive Summary 04

Il Contesto 06

Distribuzione Geografica Degli Utenti Sul Darkweb 09

1. Hacking Tools 14
   - Xss 14
   - Exploit.In 17
   - 0day.Today 18

2. Droga 23
   - Smokersco 24
   - The Grass Company 29
   - Weareamsterdam 32

3. Carding 34
   - Empire Market 34
   - Cardingteam 37
   - Simple Cash 38

4. Identity Leaks E Credential Access 40
   - Onion Identity Services 40
   - General Documents Center 42
   - Money Cashier 45

5. Armi 47
   - Athos78 48
   - The Dark Market 50
   - Botmans World 52

Hire A Killer On Darkweb 55
   - Perché Assumere Un Assassino Sul Darkweb? 57
   - Listino Prezzi 59
   - Il Modulo D'ordine 61
   - Come Sfuggire Ai Controlli 62

Conclusioni 63

Cyber Security Framework 64

Cyber Threat Intelligence 65

Come Difendersi 73

CHI SIAMO

Swascan è una Cyber Security Company nata da un'idea di Pierguido Iezzi e Raoul Chiesa. Da ottobre 2020, Swascan srl è parte integrante del Gruppo Tinexta S.P.A.

Swascan

Swascan è una Cyber Security Company nata da un'idea di **Pierguido Iezzi** e **Raoul Chiesa**. La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di Cyber Security Testing e Threat Intelligence, oltre ad un centro di eccellenza di Cyber Security Research; centro premiato con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo. **Da ottobre 2020, Swascan srl è parte integrante di Tinexta Group**, diventando protagonista attiva del primo polo nazionale di Cyber Security: non solo una azienda, ma un gruppo italiano, un nuovo hub nazionale specializzato nei servizi di identità digitale e sicurezza digitale.

Tinexta Group

Un Gruppo dinamico e in forte espansione, **quotato sul segmento STAR di Borsa Italiana.** Erede di Tecnoinvestimenti, Tinexta S.p.A. è da sempre al fianco di cittadini, imprese e Pubblica Amministrazione per favorirne la crescita e la modernizzazione.
Leader nel settore della digitalizzazione avanzata, tramite le società controllate opera in quattro aree di business: Digital Trust (Infocert, Sixtema, Visura), Cybersecurity (Swascan, Yoroi e il ramo d'azienda R&D Corvallis), Credit Information & Management (Innolva, ReValuta) e Innovation & Marketing Services (WarrantHub, Co.Mark.

EXECUTIVE SUMMARY

Uscito dall'appannaggio degli addetti al settore da almeno un decennio, il Dark web è oggi più che mai una realtà parallela della rete che opera sotto la premessa di un maggiore anonimato e una filosofia libertariana delle regole.

Ovviamente non si può accedere al Dark Web semplicemente tramite una ricerca Google, ma è necessario utilizzare un browser apposito chiamato TOR, dove la comunicazione viene crittografata ed ogni nodo della rete conosce solo il precedente e il successivo, nessun altro. La rete Tor è composta da relays gestiti da organizzazioni e individui in tutto il mondo.

Ci sono tre tipi di relay nel sistema di navigazione Tor:

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

Tuttavia, la struttura della rete Tor prevede che gli indirizzi IP dei relay Tor siano pubblici: questo, facilita il blocco da parte dei governi, i quali inseriscono nelle blacklist gli indirizzi IP di questi nodi Tor pubblici.

Per questo motivo, molti utenti si connettono tramite Bridges: si tratta di nodi non indicati nell'elenco pubblico come parte della rete Tor, strumenti "nel mezzo" essenziali per l'elusione della censura nei paesi che bloccano regolarmente gli indirizzi IP di tutti i relay Tor elencati pubblicamente.

Un anonimato che ben si sposa con attività che necessitano di un alto grado di confidenzialità e segretezza – proprio come le attività di compravendita di dati rubati.

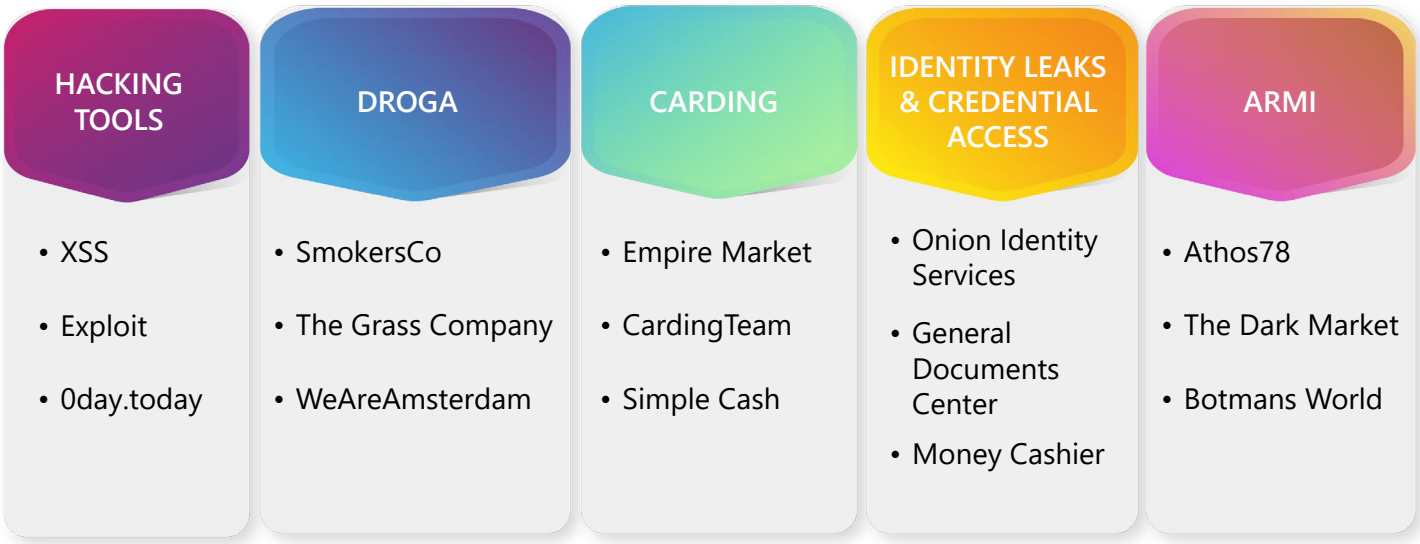
L'economia di questa realtà, infatti, ruota attorno ai Black Markets, veri e propri "mercati dell'illecito", che offrono al loro interno una vasta gamma di prodotti e servizi, tra cui un elevatissimo numero di sostanze illecite, dalla marijuana all'eroina, passando per tutta una serie di droghe sintetiche e farmaci (antidepressivi, stimolanti, antipsicotici, antidolorifici, sonniferi, ormoni, ecc.), fino ad arrivare all'acquisto di servizi come sicari su commissione e la vendita di servizi di Criminal Hacking (Malware, Ransomware, renting di Command&Control, ecc).

In questo contesto il SOC di Swascan ha intrapreso un'analisi delle tendenze, prezzi dei prodotti e metodi di pagamento utilizzati. L'analisi trae conclusioni circa il comportamento degli utenti nei mercati nel Darkweb e il potenziale di questi mercati in futuro. In particolare, sono stati raccolti, attra-

verso specifiche ricerche OSINT & CLOSINT, i dati che riguardano le 5 sostanze e servizi più venduti sul Darkweb nel 2022:

1. Hacking tools
2. Droga
3. Carding
4. Identity leaks e credential access
5. Armi

Per ognuna di queste 5 categorie, sono stati selezionati 3 mercati sul Darkweb che vendono i relativi prodotti:



L'approccio metodologico utilizzato è stato il seguente:

1. Identificazione dei maggiori siti Darkweb che si occupano della vendita dei servizi sopra citati;
2. Individuazione ed analisi delle sostanze e servizi offerti;
3. Clusterizzazione delle informazioni relativamente agli acquirenti in termini di:
    - Area geografica
    - Domanda e offerta

IL CONTESTO

Quando si parla di Black Markets probabilmente il primo a cui si pensa è Silk Road, un mercato online raggiungibile sotto rete Tor attraverso il quale si vendevano svariati prodotti e servizi per lo più illeciti, diventato poi il più grande mercato di droga a livello mondiale. Il mercato ha funzionato con successo per quasi due anni sotto la guida di "Dread Pirate Roberts", pseudonimo sotto cui si celava il proprietario, generando milioni di dollari di entrate fino al 3 ottobre 2013, quando il sito viene chiuso dall'FBI e a seguito dell'arresto del presunto fondatore e direttore Ross William Ulbrich, dal cui portafoglio virtuale vengono sequestrati più di 26.000 Bitcoin, per un controvalore di circa 3,6 milioni di dollari. Ai primi di novembre del 2013 è annunciata la riapertura di Silk Road da parte dello stesso pseudonimo, accogliendo gli utenti con il seguente messaggio:

«è con grande gioia che vi annuncio un nuovo capitolo della nostra avventura. Silk Road è risorto dalle ceneri e ora è pronto ad accogliervi»

L'accesso avviene tramite registrazione: è sufficiente fornire un nome utente, una password, un codice identificativo per le transazioni e rispondere a un CAPTCHA per accedere all'homepage e usufruire di tutti i servizi offerti.

Secondo la denuncia penale dell'FBI presentata nel processo di Ross William Ulbright, il mercato di Silk Road stimava quasi 150.000 acquirenti e quasi 4.000 venditori (USA v. Ross Ulbricht, 2013). La base di utenti si trovava più pesantemente negli Stati Uniti, ma includeva individui provenienti da tutto il mondo. Oltre alla possibilità di acquistare merce illegale, il sito forniva una funzionalità di messaggistica che consentiva ad acquirenti e fornitori di interagire e discutere sugli effetti della droga, modalità di utilizzo dei bitcoin, dare valutazioni ai fornitori. Questo ha reso il sito non solo un paradiso per il libero scambio del contrabbando, ma un deposito di informazioni su una vasta gamma di argomenti.

Tuttavia, nonostante questo sia stato smantellato, la vendita di merce illegale sul Darkweb non si è arrestata.

I fornitori (e i mercati in cui operano) sfruttano la crittografia e l'anonimato forniti dal Darknet per nascondere le loro attività illecite e sfuggire alle forze dell'ordine. La maggior parte delle volte le transazioni sono condotte utilizzando criptovalute per rendere più difficile il tracciamento dei loro guadagni e offuscare ulteriormente le loro identità.

Alcuni fornitori sul Darkweb sono veri esperti di programmazione o cybersecurity che fanno fortuna vendendo malware ed exploit che consentono agli operatori meno sofisticati di lanciare potenti attacchi informatici contro obiettivi aziendali. Altri sono semplicemente truffatori, che vendono account personali rubati o condividono credenziali ad un prezzo vantaggioso.

Ogni mercato sul Darkweb è un'impresa criminale organizzata che trae profitto dallo scambio di beni e servizi illeciti. Questi mercati sono gestiti da gruppi sofisticati che utilizzano tecniche di sicurezza all'avanguardia per nascondere le loro identità.

In pochi minuti, chiunque può scaricare il browser Tor, navigare in un mercato sul Darkweb, creare un account fornitore e iniziare a mettere in vendita beni o servizi illeciti. Tuttavia, alcuni mercati richiedono ai fornitori di presentare domanda tramite referral, fornire una prova della reputazione di un altro mercato, acquistare una licenza o fornire un deposito in contanti; questo al fine di garantire che solo fornitori affidabili possano operare.

Di seguito riportiamo le categorie di prodotti che è possibile trovare in questi mercati:

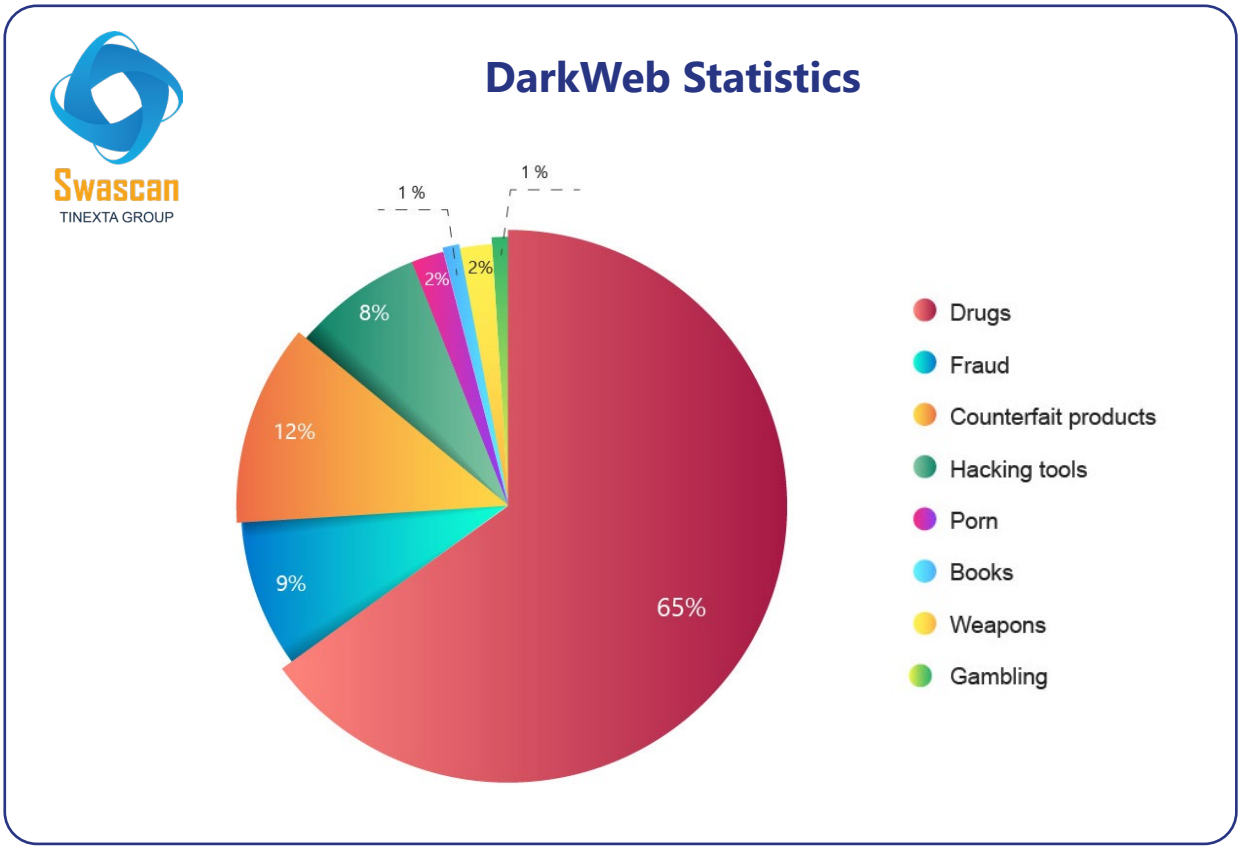
1. **Tools di hacking, spam e phishing:** vulnerabilità zeroday, exploit kit, strumenti di hacking, accessi a database protetti. Questi consentono ai threat actors con conoscenze tecniche minime di lanciare attacchi informatici efficaci.

2. **Kit di malware e ransomware:** in questa categoria rientrano botnet che possono essere utilizzati per spam o attacchi DDoS, remote access trojan, che possono fornire all'attaccante accesso remoto ad un computer, keyloggers usati per spiare le attività ed infiltrarsi o impossessarsi degli account, rootkits che forniscono all'attaccante accesso ad un computer, proxy malware.

3. **Tutorials**: vendita di guide dettagliate che insegnano ad altri truffatori come rubare denaro e commettere frodi, spesso utilizzando prodotti e servizi forniti dal venditore stesso. Gli argomenti comuni per guide e tutorial includono hacking, truffe con carte di credito, distribuzione di attacchi di malware e ransomware.

4. **Merce illecita:** traffico di droga, denaro, armi, merce non acquistabile sul Clearweb.

In breve, la maggior parte degli articoli venduti sul Darkweb sono di natura illegale e hanno prezzi significativamente inferiori rispetto al loro reale valore di mercato.

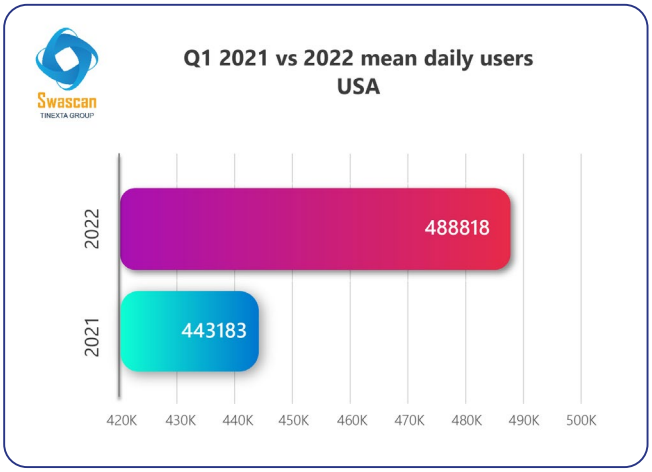


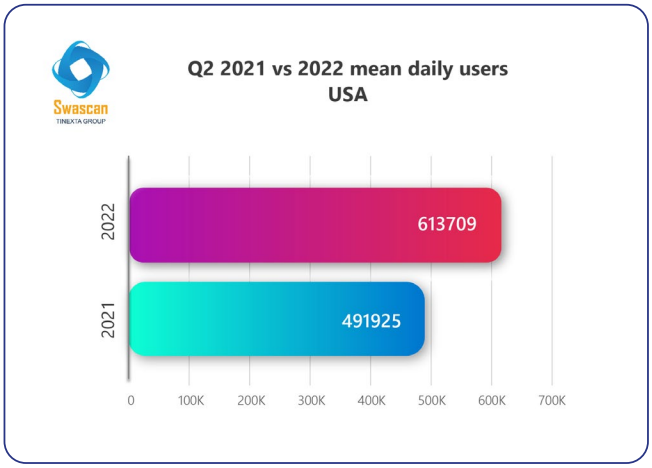
Di seguito riportiamo gli articoli più richiesti e i loro prezzi:

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

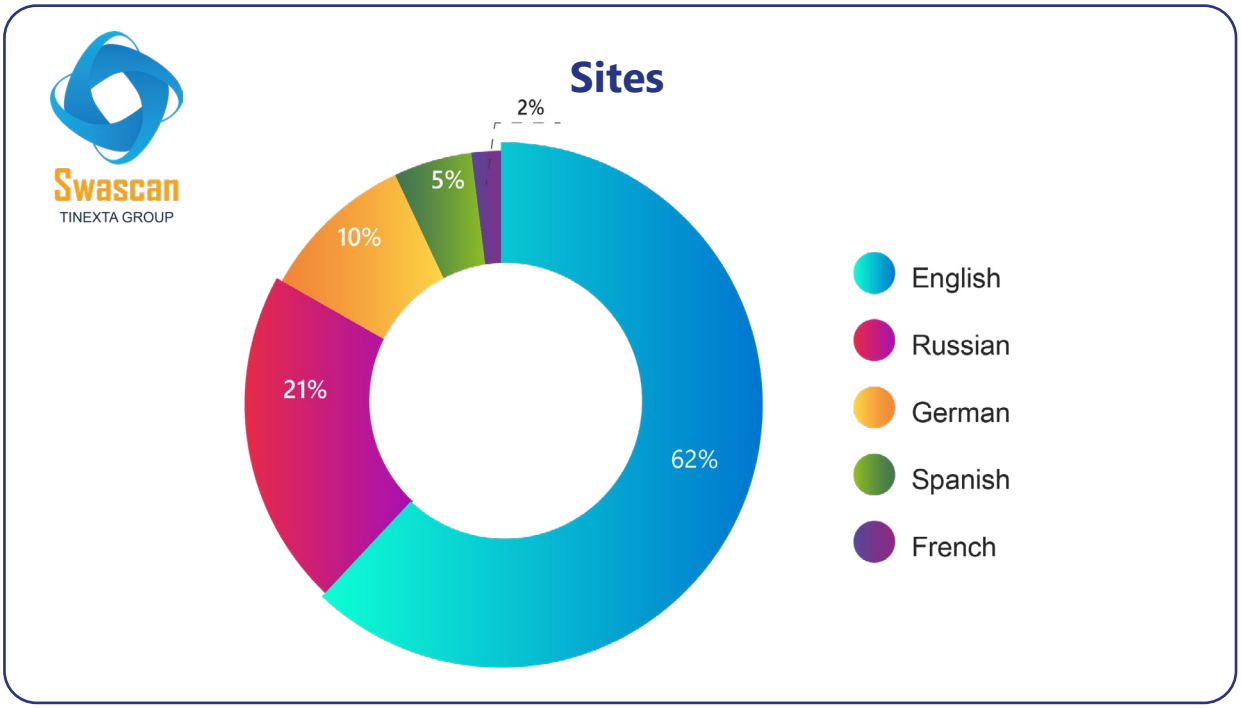
DISTRIBUZIONE GEOGRAFICA DEGLI UTENTI SUL DARKWEB

Nel corso delle analisi è stato possibile riscontrare come la maggior parte degli utenti sul Darkweb risulti attiva negli Stati Uniti. Riportiamo di seguito un confronto tra il Q1 e Q2 nel 2021 e 2022 che mostra la crescita costante di utenti attivi.

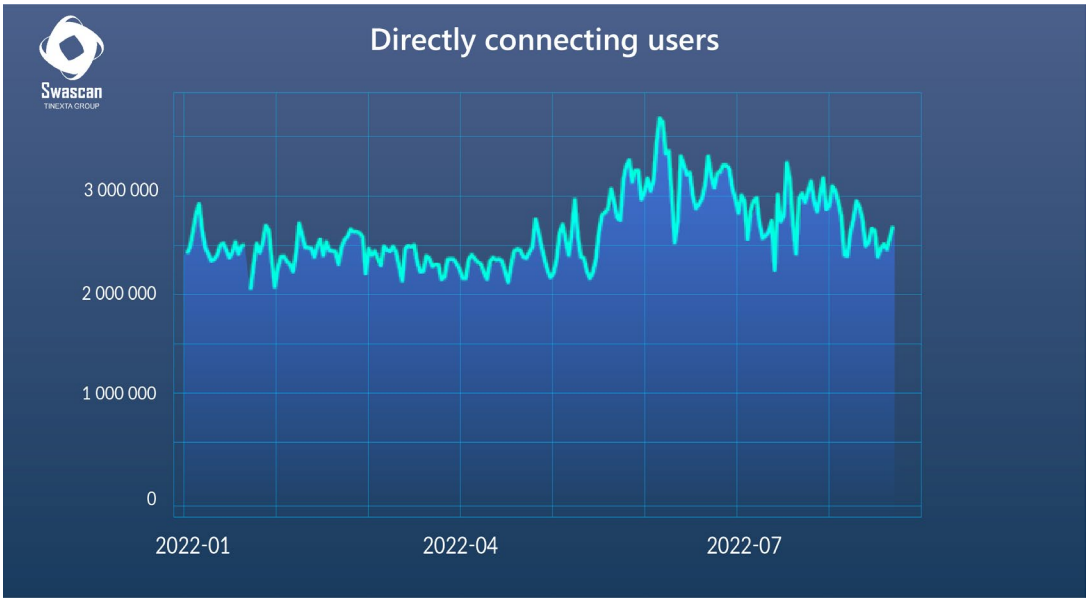


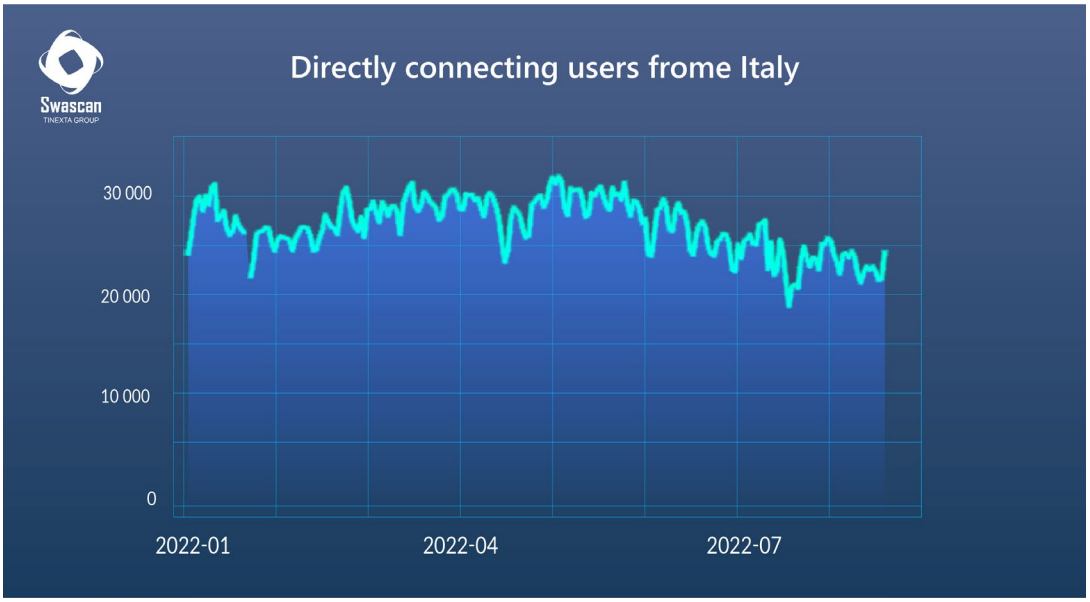


In linea con il grafico sopra, infatti, la lingua più usata sul Darkweb risulta essere l'inglese: su 100 markets analizzati a campione, 62 utilizzano l'inglese come lingua principale.

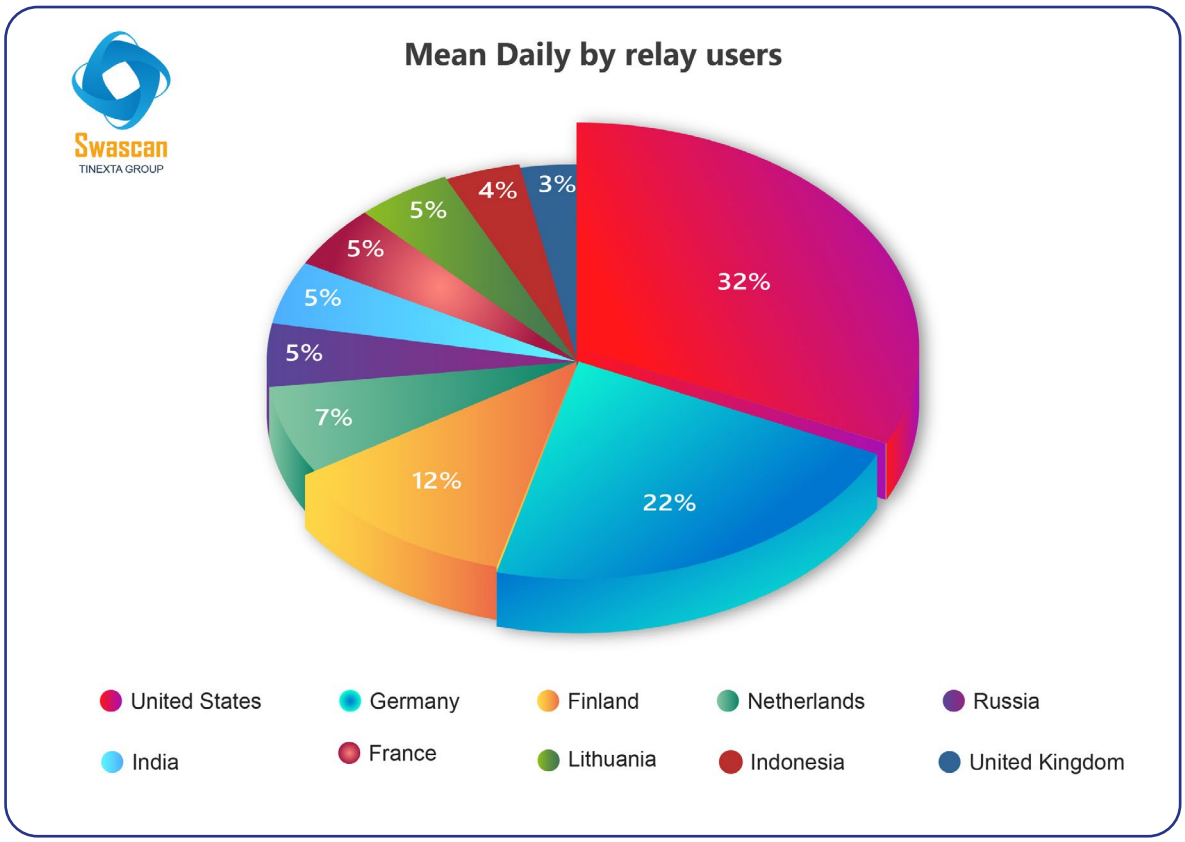


Nei grafici di seguito, il numero degli utenti connessi da tutto il mondo sul Darkweb, con particolare focus sull'andamento in Italia, e la distribuzione geografica nel periodo intercorso tra gennaio ed agosto 2022. L'analisi è stata svolta differenziando gli utenti connessi in **"relay users"** e **"bridge users".**

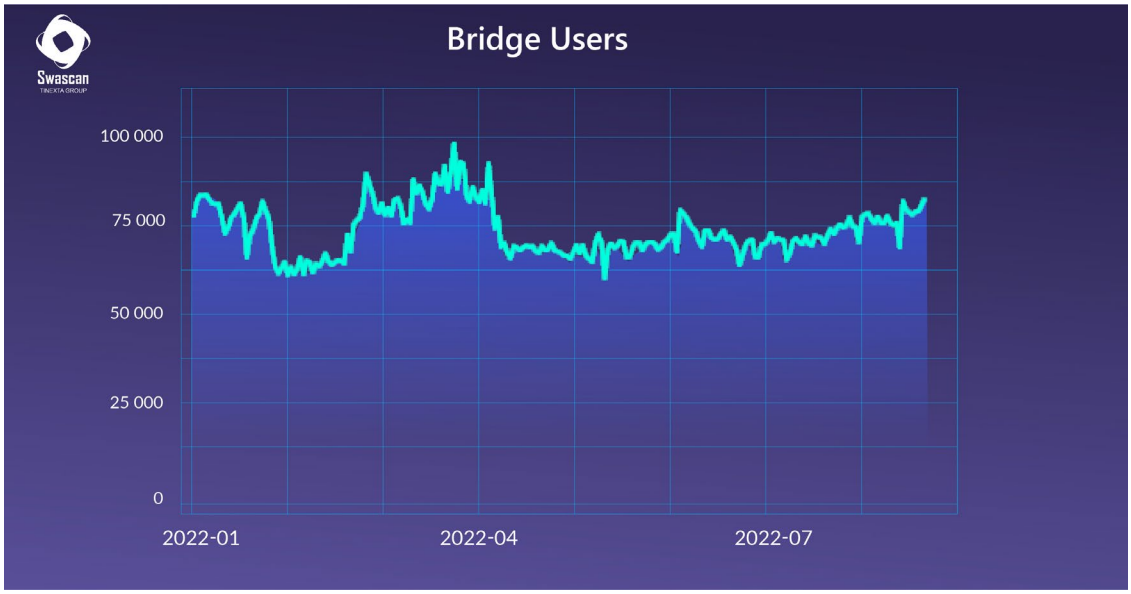


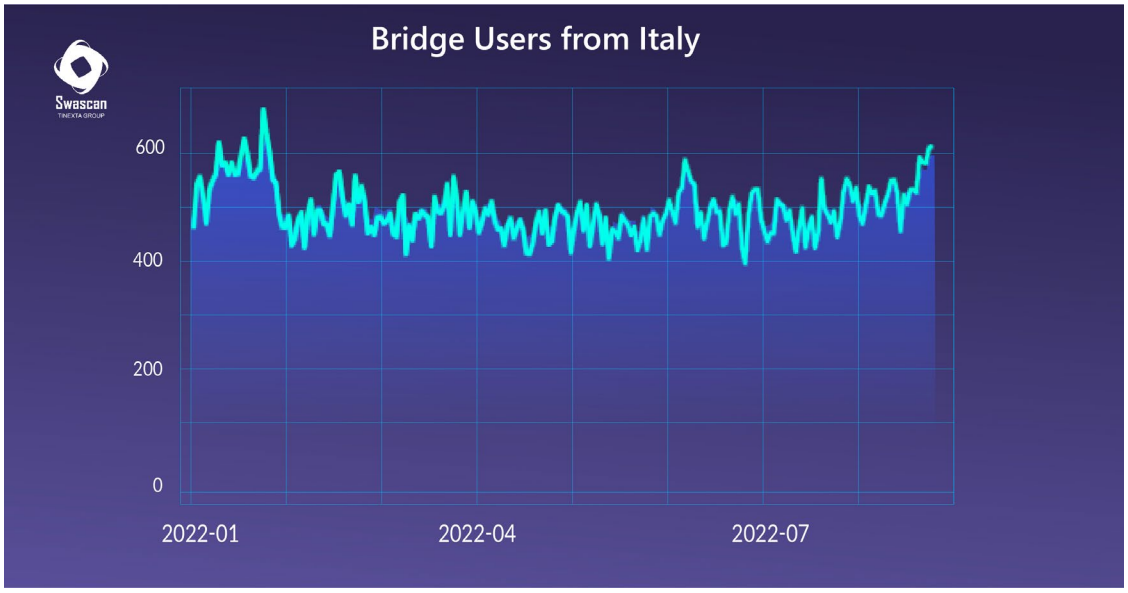


Di seguito, i top 10 countries da cui i relay users si sono connessi nel periodo tra **gennaio – agosto 2022.**

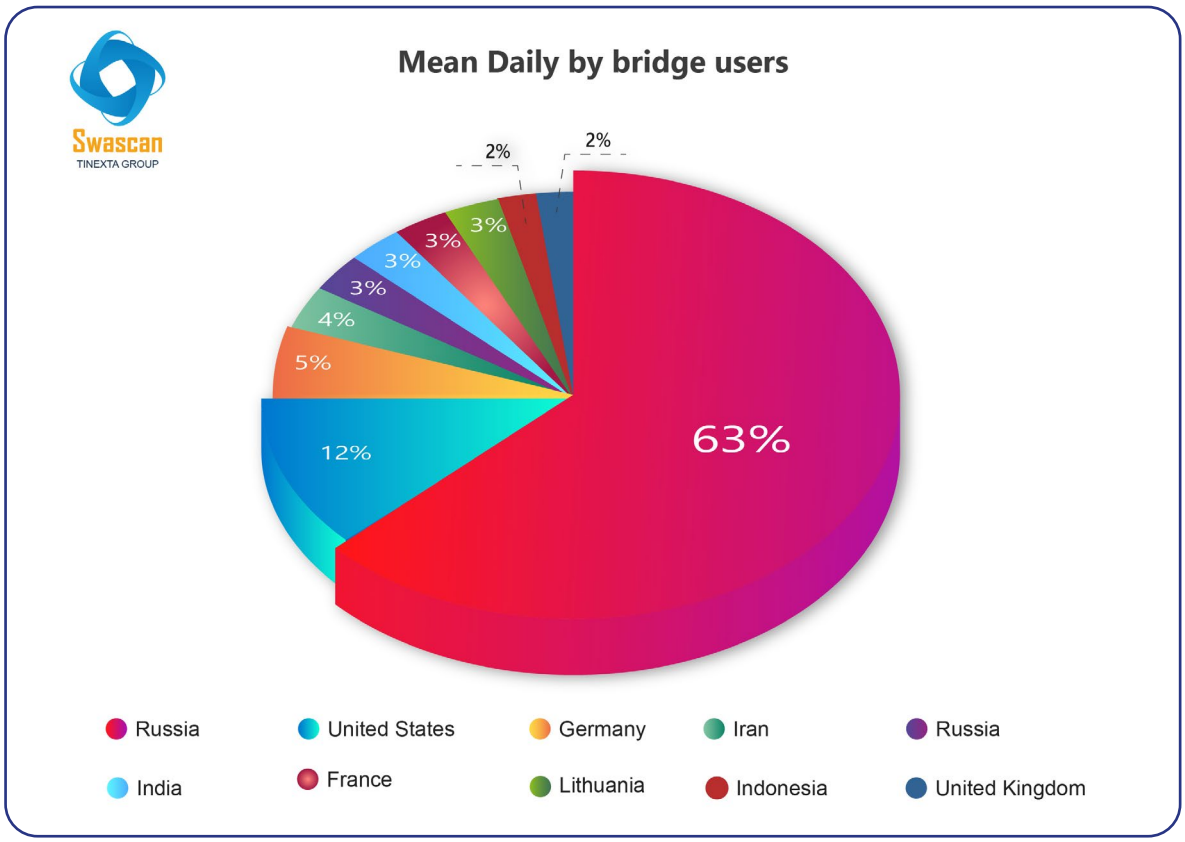


PAESE	Mean daily by relay users January – August 2022
United States	617024
Germany	426501
Finland	216980
Russia	122835
India	101739
Netherlands	100994
France	90441
Indonesia	88673
United Kingdom	81430
Lithuania	62448


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

Di seguito, i top 10 countries da cui i **bridge users** si sono connessi nel periodo tra **gennaio – agosto 2022.**



PAESE	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

Dopo un breve excursus sul mondo del Darkweb, **il SOC & Threat Intelligence Team di Swascan** ha analizzato i dati relativi alle 5 sostanze e servizi più venduti sui mercati underground nel 2022, al fine di comprendere come agiscono i venditori:

1. **Hacking tools**
2. **Droga**
3. **Carding**
4. **Identity leaks e credential access**
5. **Armi**

1. Hacking tools

L'analisi sulle tendenze di vendita e dei prezzi osservate sui mercati del dark web rivela come un'ampia gamma di strumenti e servizi sia disponibile per la vendita a un costo accessibile: il phishing, uno dei vettori di cyberattacco più diffusi, è in vendita a partire da 2$.

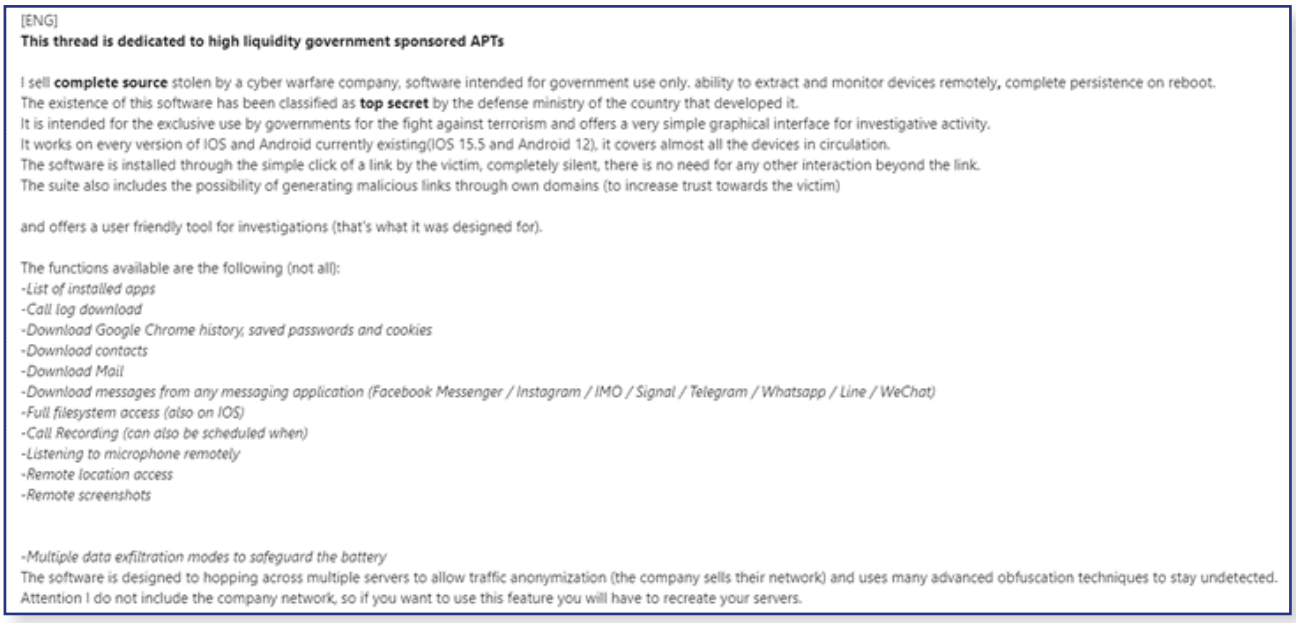
A tal proposito, infatti, anche se tra la merce a disposizione al primo posto per numero regnano gli stupefacenti, a breve distanza troviamo innumerevoli hacking tools e pacchetti di dati sensibili illegalmente ottenuti. In particolar modo, si vendono exploit kits per phishing, ransomware exploit kits, DdoS-for-hire, RDP, Command&Control, ecc. Di seguito riportiamo esempi di vendita su tre forum underground:

XSS

Forum di hacker russo creato nel 2013 e rilanciato nel 2018, considerato uno dei forum di hacking di lingua russa più popolari. Il nome è l'acronimo di Cross-site scripting (XSS), con cui si indica lo sfruttamento di vulnerabilità nelle applicazioni web.

Il sito è stato creato e progettato allo scopo di condividere informazioni su exploit, vulnerabilità zero-day, malware e network penetration. Il contenuto principale include exploit malware, vulnerabilità, carding, access sales e database di credenziali. Tuttavia, il forum è utilizzato anche da gang ransomware per reclutare nuovi membri.

Riportiamo di seguito esempi di post apparsi sul forum underground. Nel primo caso si vende la capacità di estrarre e monitorare dispositivi da remoto. L'esistenza di questo software è stata classificata come top secret dal ministero della Difesa del paese che lo ha sviluppato; infatti, è destinato all'uso esclusivo dei governi per la lotta al terrorismo.



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

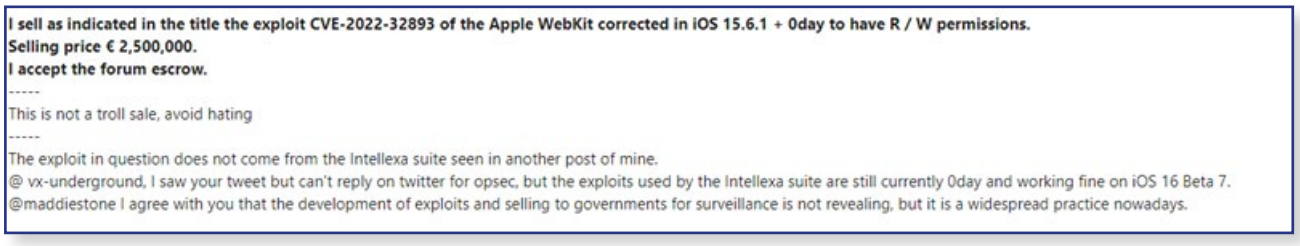
I sell **complete source** stolen by a cyber warfare company, software intended for government use only. ability to extract and monitor devices remotely, complete persistence on reboot.
The existence of this software has been classified as **top secret** by the defense ministry of the country that developed 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 un altro caso si vende l'exploit CVE-2022-32893 dell'Apple WebKit corretto in iOS 15.6.1 comprensivo di 0day ad un prezzo di vendita € 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.

I documenti trapelati online mostrano l'acquisto e la documentazione di iOS Remote Code Execution 0day exploit ad un prezzo di $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

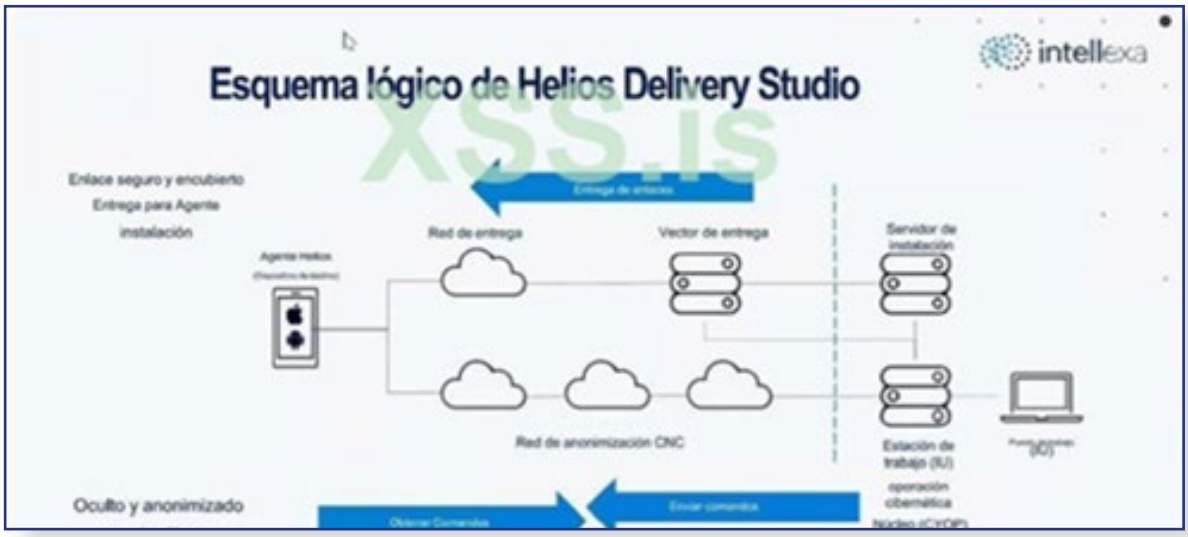
intellexa

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

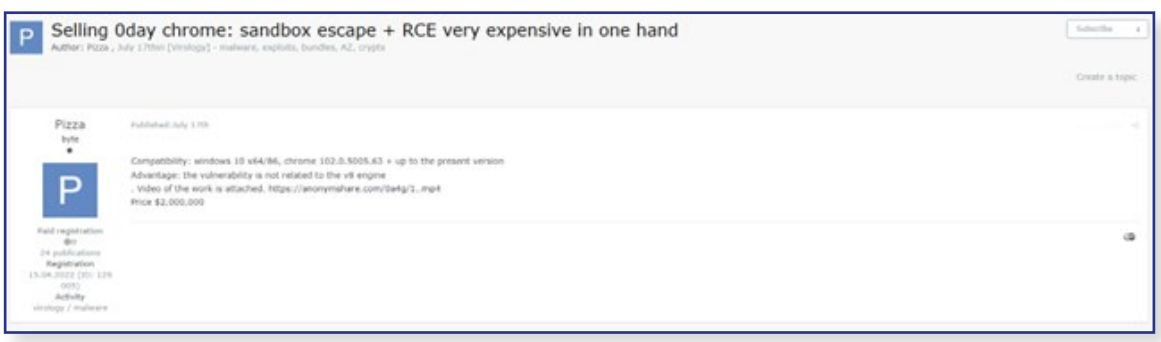


EXPLOIT.IN

Exploit.in è un forum creato nel 2005 che ospita discussioni su diversi argomenti di criminalità informatica come social engineering, sicurezza e vulnerabilità, hacking dei social network, crittografia, malware, programmazione per il cracking. Il sito si concentra principalmente sulla condivisione di vulnerabilità dei sistemi informatici, per scopi di hacking. Funziona anche come un mercato in cui gli utenti possono acquistare e vendere prodotti digitali illeciti come malware e vari servizi di hacking e carding.

Una delle caratteristiche più importanti di questo forum russo, che possiamo considerare uno dei più critici in termini di attacchi informatici, è la vendita all'asta, rendendo Exploit.in il forum Darkweb preferito dagli hacker ransomware.

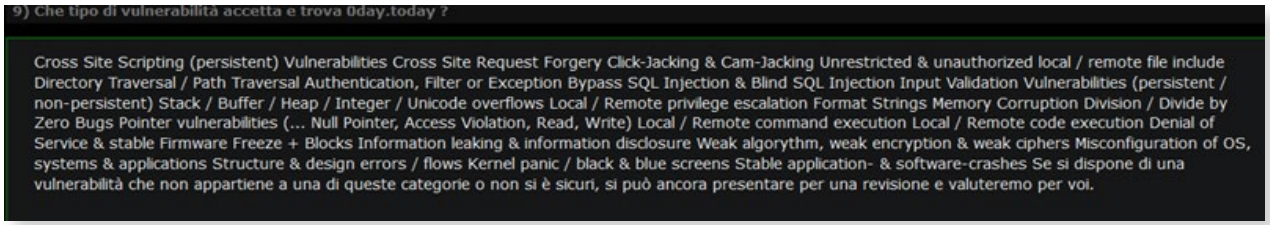
Riportiamo di seguito esempi di vendite sul mercato underground con i relativi prezzi:



0DAY.TODAY

0day.today nasce il 13 Maggio 2008 ed è un database regolarmente aggiornato con la descrizione delle vulnerabilità critiche da sfruttare. Ad ogni vulnerabilità viene assegnato un rischio, da basso a critico. Presenta anche la suddivisione per piattaforma: BSD, Linux, QNX, OSX, Solaris, Unix, Windows.

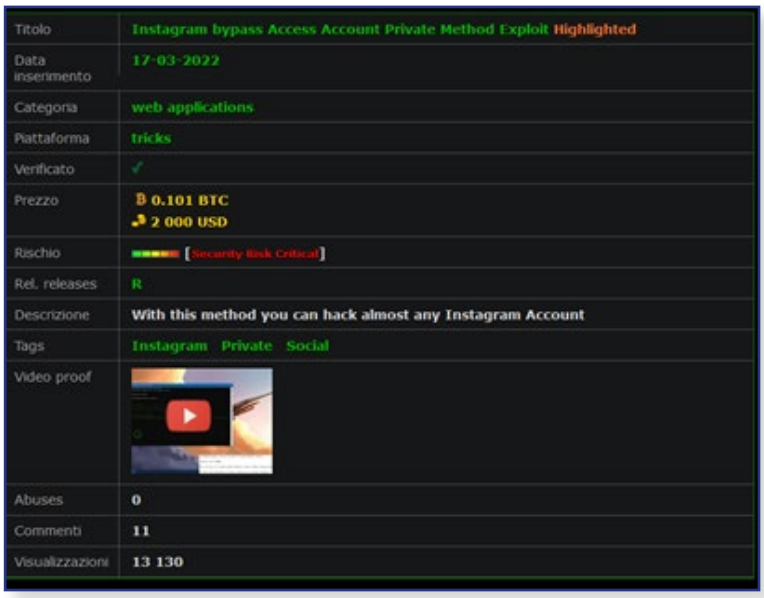
Di seguito riportiamo le vulnerabilità in vendita sul mercato:



Il sito è diviso in 6 categorie:

1. Private exploits and 0day exploits market

Di seguito l'esempio di vendita di accesso per un account Instagram privato:



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

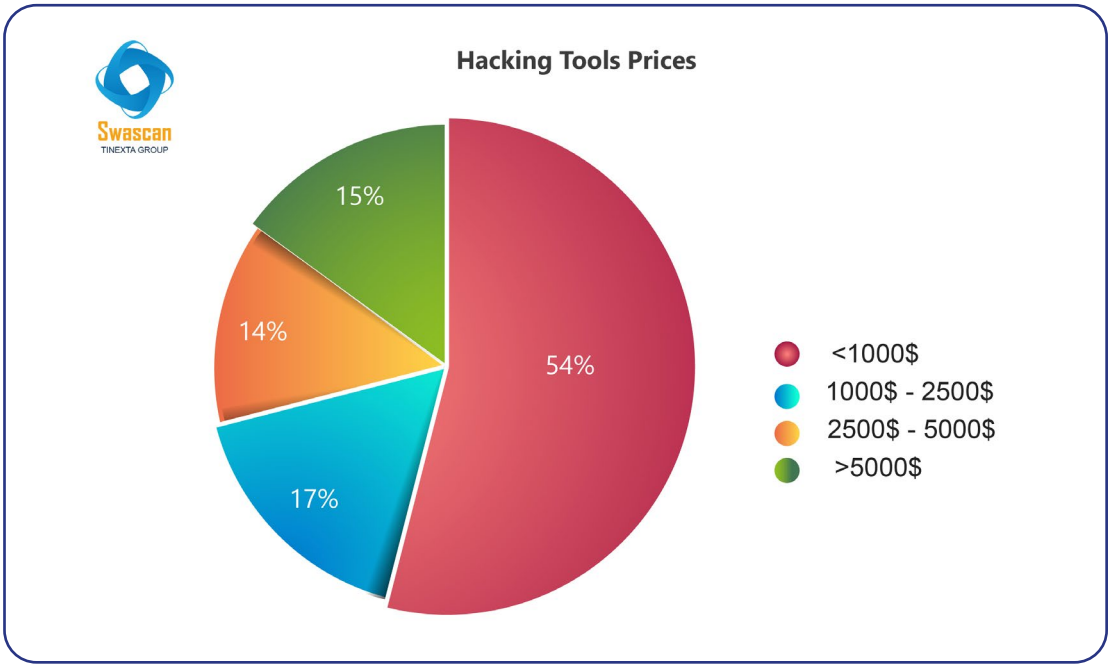
Titolo	Nginx 1.20.0 - Denial of Service Exploit [Highlight]
Data inserimento	11-07-2022
Categoria	dos / poc
Piattaforma	multiple
Verificato	✓
Prezzo	FREE
Rischio	[Security Risk Medium]
Rel. releases	R
CVE	CVE-2021-23017
Abuses	0
Commenti	0

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

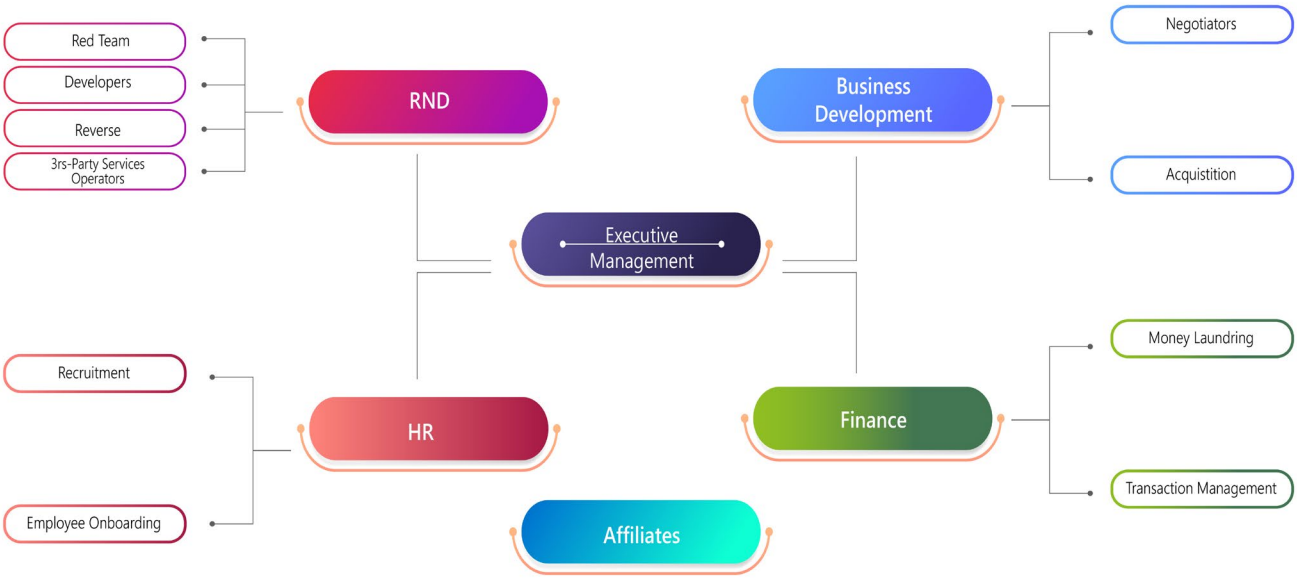
Su 100 annunci pubblicati in vendita, è stata realizzata una media dei prezzi offerti:



Questo scenario evidenzia un'elevata criticità che mostra come il mercato stia indirettamente diventando un mercato di professionisti, imprenditori del cybercrime: costituiti come vere e proprie aziende. Chiaro esempio di ciò sono le due gang ransomware LockBit e Conti, caratterizzate da:

- competenze
- ransomware
- tool (exploit/0day)
- infrastruttura
- centro governance

Questi assumono personale attraverso regolari colloqui e operano colpendo aziende per poi pubblicare i loro dati qualora queste non paghino l'importo richiesto. A tal proposito, Cybertint ha realizzato graficamente la possibile struttura della gang Conti, che ha attualmente cessato la propria attività: com'è possibile notare in figura, la struttura è la stessa di vere e proprie aziende.

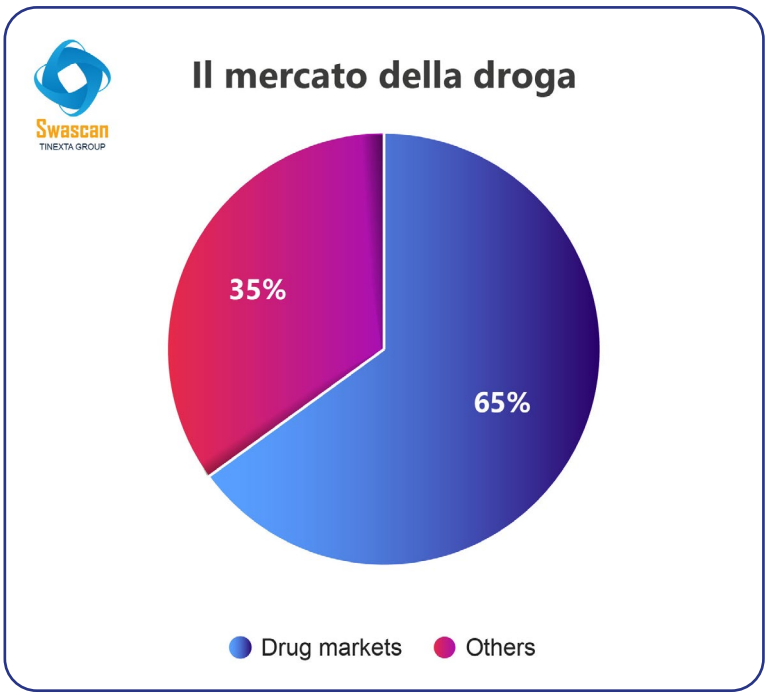


Recentemente, il gruppo ransomware LockBit è stato vittima di un attacco DDoS da parte di Entrust che ha impedito l'accesso al sito su cui condivide informazioni e dati delle aziende. Anche qui, il processo di recruiting di "dudosers" non è mancato:

Successivamente, sempre sul forum XSS, LockBitSupp, account di LockBit, ha annunciato che il gruppo è tornato ad operare dopo aver allestito un'infrastruttura più ampia per consentire l'accesso ai dati sottratti senza che eventuali azioni DDoS possano ostacolarne l'attività. Questo ha suggerito alla gang criminale una nuova tattica: prendendo spunto da quanto accaduto, infatti, LockBit ha deciso di adottare la tattica della tripla estorsione per mettere più pressione alle vittime. Oltre alla cifratura dei file e alla pubblicazione dei dati è previsto dunque un eventuale attacco DDoS.

2. Droga

Il mercato underground della droga è il più grande per numero di prodotti in vendita e numero di venditori, con una crescita progressiva del fenomeno nell'arco degli ultimi anni. Questi mercati online offrono una gamma di narcotici differenti che vanno dalle droghe comuni fino a sostanze chimiche utilizzate per la fabbricazione di nuove sostanze o per altri scopi illeciti, dando una vastissima scelta al cliente. Di seguito un confronto del mercato della droga rispetto agli altri, e l'analisi di tre mercati che vendono queste sostanze:



SmokersCo

"Il nostro negozio offre le migliori varietà di cannabis e marijuana medica per tutte le condizioni mediche - disponibile online ai prezzi più bassi, garantito! Se ti stai chiedendo come ordinare erba online, sei nel posto giusto. Non è mai stato così facile ricevere cannabis medica direttamente a casa tua."

SmokersCo è un negozio sotto rete Tor che offre una grande varietà di marijuana e hashish. Gli elementi chiave che lo distinguono da altri markets sono la facilità con cui è possibile acquistare marijuana online in Europa, caratteristica che attira quotidianamente nuovi acquirenti, a cui viene offerta anche la possibilità di acquistare tramite telefono cellulare, pagando tramite Bitcoin o Monero. Gli amministratori del sito attualmente in procinto di lanciare un sistema di affiliazione con il quale è possibile creare più campagne e ricevere una parte del profitto dalla società.

Sebbene questo sito sia un negozio di venditori, funziona praticamente come i mercati darknet generici: prima di acquistare qualsiasi cosa, bisogna registrare un account (nessun indirizzo email richiesto).

I prodotti sono suddivisi in due diverse categorie, erba e hashish. Tuttavia, i prodotti disponibili all'interno delle categorie sono soggetti a continue modifiche, motivo per cui gli amministratori del sito consigliano di controllare frequentemente gli eventuali aggiornamenti.

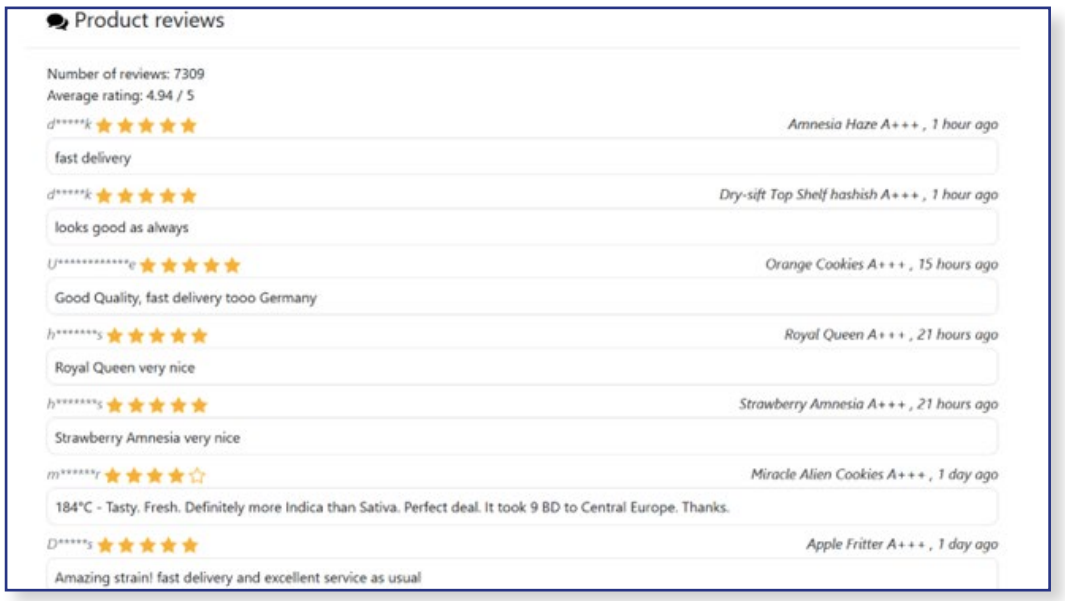
Un'altra caratteristica interessante del sito la fruizione di una varietà di guide e tutorial per coloro che potrebbero essere nuovi alle operazioni del mercato darknet. Questi includono tutorial dettagliati su come acquisire Bitcoin da Localbitcoins o Coinbase. Si possono anche trovare tutorial sull'uso di PGP, sia per principianti che per utenti più esperti. Queste guide includono istruzioni ed esempi su come utilizzare Gpg4Win e Kleopatra.

Infine, c'è anche un'ampia sezione per guide ed esercitazioni generali sulla sicurezza, offrendo dunque la possibilità alle persone che lo desiderano di familiarizzare con le procedure di sicurezza di base.

Un altro vantaggio di SmokersCO è che include recensioni per tutte le vendite: queste recensioni sono pubbliche e possono essere visualizzate da chiunque, offrendo ai nuovi acquirenti un'esperienza riepilogativa dei clienti precedenti.

In merito ai prodotti, il negozio conta oggi più di 12 diverse varietà di marijuana e 4 diversi tipi di hashish importati direttamente dal Marocco.

Oggi SmokersCo., con più di 7300 recensioni sul loro sito web, è posizionato tra i migliori negozi in Europa per l'acquisto di droga online.



Altra caratteristica che attira nuovi utenti è il supporto offerto al cliente, garantendo una risposta entro un massimo di 24 ore dal lunedì al venerdì. In merito alle condizioni d'acquisto, se per posta la droga viene persa o rubata, verrà inviato un pacchetto sostitutivo in modo gratuito, o in alternativa un rimborso del 100%.

Si definiscono "il mercato con i prezzi più bassi online", offrendo tutti i prodotti ad un prezzo fisso di 18$, senza l'applicazione della tassa del 6% dei mercati darknet.

"Lavoriamo solo con agricoltori che coltivano cannabis con metodi biologici. Tutti i nostri prodotti sono rigorosamente testati per il controllo di qualità in-house. Nessuna muffa, nessun problema. Siate certi che otterrete solo il top del raccolto!"

Attualmente spediscono dalla Spagna con una spedizione standard per tutti gli ordini non superiori a 50 grammi e con un tempo di spedizione stimato tra 4 e 7 giorni lavorativi. Il numero di tracking non viene fornito per ordini di piccole quantità.

Per spedizioni superiori a 50 grammi si opta per la modalità express: in questo caso il tempo di spedizione stimato è tra 2 e 6 giorni lavorativi, con numero di tracking disponibile e si consiglia di inserire il numero di telefono.

I paesi da cui vengono presi in carico ordini sono i seguenti: Austria, Belgio, Bulgaria, Croazia, Cipro, Repubblica ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, Islanda, Irlanda, Italia, Lettonia, Liechtenstein, Lituania, Lussemburgo, Malta, Monaco, Moldova, Montenegro, Paesi Bassi, Norvegia, Polonia, Portogallo, Romania, Serbia, Slovacchia, Slovenia, Spagna, Svezia, Svizzera e Turchia. Dal 9 agosto il negozio non spedisce più al di fuori dell'Unione Europea.

L'indirizzo di spedizione deve essere un appartamento o una casa privata con una cassetta postale visibile, ed in caso di soggiorno in un edificio è necessario specificare correttamente quale sia il numero civico. È necessario mettere il vero nome. Non spediscono ad alberghi, imprese, università.

Come una vera e propria azienda, il mercato underground presta particolare attenzione al cliente: difatti, è possibile che in alcuni casi la droga perda un po' di peso a causa del processo di essiccazione continua. In questo caso, SmokersCo. consiglia di pesare direttamente tutte le confezioni prima di aprirle ed inviare una foto: se il peso risulterà inferiore, verrà inviato un pacco con la quantità mancante. In condizioni di bassa qualità del prodotto, è necessario mandare una foto a prova del fatto per ottenere un rimborso.

Di seguito le tre tipologie maggiormente vendute:

1. Sativa

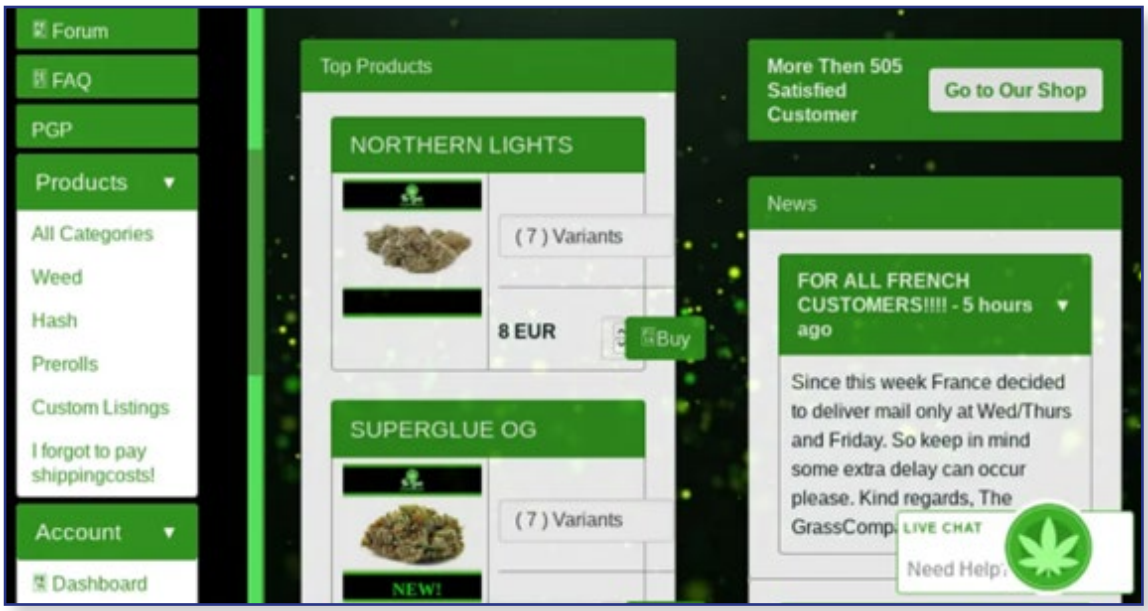
2. Indica

3. Hybrid

The Grass Company

The Grass Company è uno dei negozi di venditori nato nel 2018 che si dedica solo ad un tipo esplicito di prodotto: come suggerisce il nome, questo prodotto è la Cannabis e il negozio si occupa prettamente del suo commercio.

Il team di Grass Company cerca di migliorare costantemente la propria piattaforma, aggiungendo di volta in volta molte nuove funzionalità, quali un forum e una live chat.



La homepage mostra la lista dei prodotti più venduti e una lista delle notizie pubblicate dal team del negozio. La barra laterale di sinistra è dove sono tutte le informazioni importanti, tra cui l'elenco delle categorie dei prodotti, che facilita la ricerca in base ai tipi.

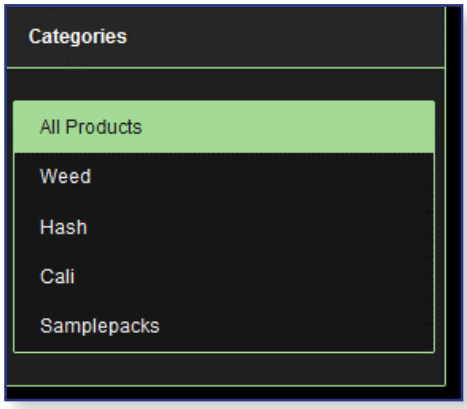
Il negozio Grass Company può essere visualizzato senza registrazione, che è invece richiesta per effettuare ordini. Il processo di registrazione è abbastanza semplice e richiede solo un nome utente e una password.

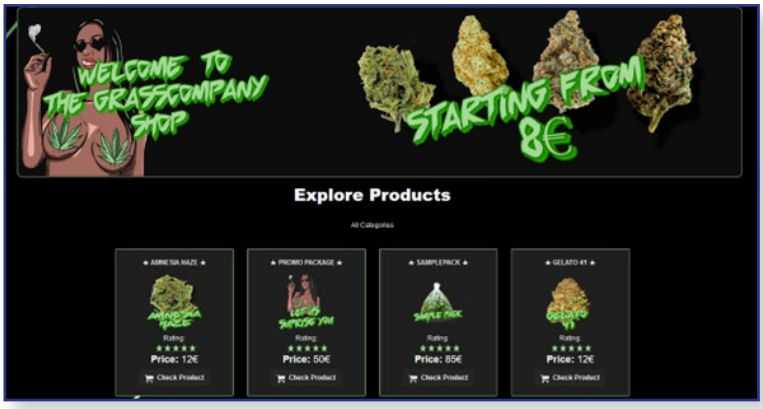
In merito agli acquisti, originariamente, solo Bitcoin (BTC) era accettato su The Grass Company; recentemente, il team ha aggiunto Monero (XMR) e Litecoin (LTC) come modalità di pagamento ag-

giuntive. Viene fornita anche una valutazione dei fornitori, con quante vendite ha realizzato ed altri dettagli del prodotto venduto.

Il sito riporta anche una valutazione media generica dei clienti, prodotti, ordini e feedback:

"TheGrassCompany è orgogliosa di annunciare il lancio del nostro nuovo webshop, che vende i prodotti di THC di più alta qualità a prezzi scontati. Con gli ultimi aggiornamenti, sarà più facile e veloce per tutti di fare un ordine con BTC o pagamenti XMR con pochi passaggi. Abbiamo un'ampia varietà di prodotti disponibili, tra cui varietà di erba Classic, Hash e le nostre varietà premium Cali. Tutti i prodotti sono curati dai nostri amorevoli coltivatori con le varietà accuratamente selezionate. Oltre a ottimi prezzi, TheGrassCompany offre la spedizione gratuita su ordini superiori a 25gr con Track and Trace gratuito per la vostra tranquillità. Vienici a trovare oggi per approfittare di queste offerte incredibili!"





La spedizione è garantita in tutto il mondo fatta eccezione per India, Australia e USA. Il tempo stimato di arrivo per i paesi vicino al Belgio è di 2-3 giorni, per gli altri paesi europei 4-5 giorni e per i paesi fuori dall'Europa 7-10 giorni lavorativi. Viene garantito un rimborso del 50% in caso di mancato arrivo del prodotto.

Viene garantita inoltre spedizione gratuita e free tracking per tutti gli ordini in Europa. Le spese di spedizione al di fuori dell'Europa ammontano a 6 euro, con una quantità massima di 19 gr per busta. Per ordini superiori a 20 grammi non viene addebitato alcun costo di spedizione.

In molti casi il prezzo applicato è lo stesso, anche se Hash, Amnesia Haze e le più economiche Northern Lights hanno prezzi diversi dagli altri prodotti.

Il prezzo minimo è di 8 euro al grammo e un massimo di 6000 euro per 1Kg.

Di seguito riportiamo i prezzi nel dettaglio:

1 grammo = 8 euro
2,5 grammi = 22 euro
5 grammi = 44 euro
10 grammi = 85 euro
25 grammi = 200 euro
50 grammi = 380 euro
100 grammi = 750 euro
250 grammi = 1800 euro
500 grammi = 3250 euro
1000 grammi = 6000 euro

WeAreAmsterdam

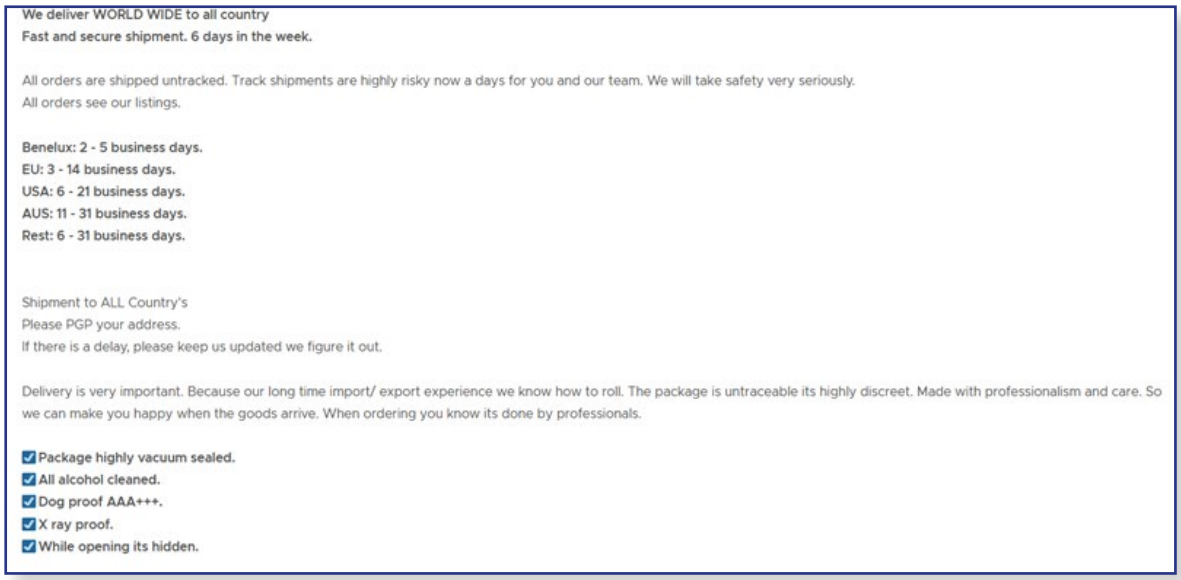
WeAreAmsterdam è un fornitore tedesco con un sito di shop dedicato alla cannabis e altri prodotti correlati alla droga. La sua vetrina sul Darkweb elenca attualmente circa 70 articoli e offre spedizioni in tutto il mondo, compresi Stati Uniti e Australia. Pur avendo solo due anni, gli amministratori hanno collezionato oltre 20.000 vendite in 20 diversi mercati, diventando uno dei fornitori più affermati e duraturi nella storia dei mercati Darknet.

Come la maggior parte dei negozi, è possibile navigare il negozio istantaneamente, senza il bisogno di creare un account se si vuole solo controllare i prodotti e prezzi.

Una volta che si ha un account si ha la possibilità di accedere a una lista di tutti i propri ordini, i quali possono avere tre diversi stati:

- In attesa (l'ordine è stato effettuato ed è ora in attesa del deposito)
- Pagato (l'importo è stato pagato per intero ed è ora in fase di preparazione per la spedizione)
- Spedito (L'ordine è stato spedito al tuo indirizzo).

Se si effettua un ordine, questo andrà saldato entro 60 minuti o verrà automaticamente annullato. WeAreAmsterdam dà limiti larghi per i tempi di consegna, dipende dalla destinazione e può variare di volta in volta. Tuttavia, il sito offre un contatto per informarsi sulla data di spedizione stimata.


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.

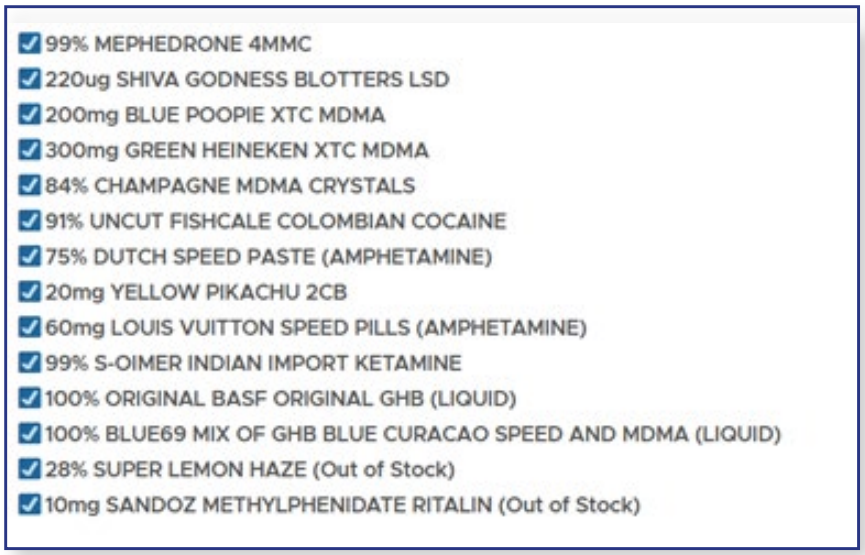
Gli elenchi dei prodotti su WeAreAMSTERDAM sono divisi in cinque diverse categorie:

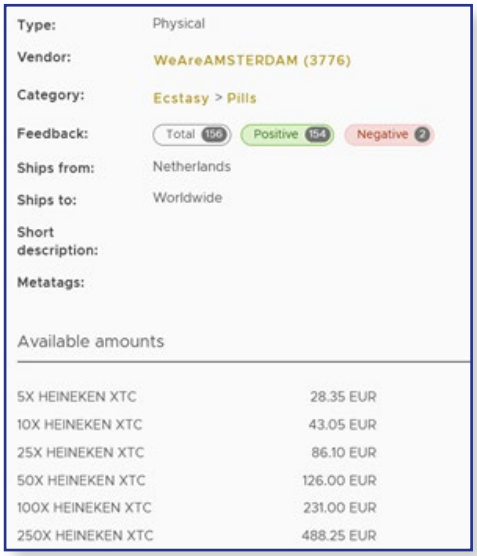
- Simulants 30
- Cannabis & hashish 0
- Ectasy 23
- Dissociatives 14
- Psychedelics 15

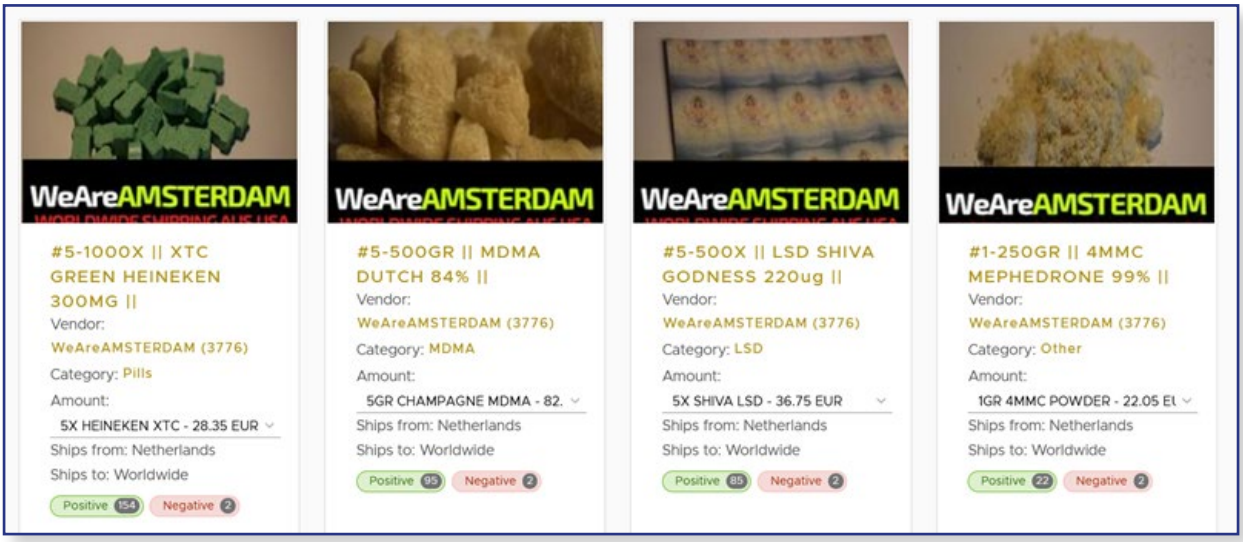
Tutti gli articoli sono disponibili per essere spediti in tutto il mondo. Solo gli ordini all'ingrosso sono dotati di informazioni di monitoraggio. Il venditore offre un rimborso parziale o un costo di rispedizione solo a coloro che hanno completato almeno un acquisto di successo con loro.

WeAreAMSTERDAM accetta sia Bitcoin (BTC) che Monero (XMR) per il pagamento. Usano il tradizionale sistema di deposito del conto, consigliando di depositare solo fondi sufficienti per coprire un ordine alla volta.

Il negozio è universalmente riconosciuto dalla comunità darknet come fornitore legittimo con quasi un decennio di esperienza di vendita su diversi mercati.







3. Carding

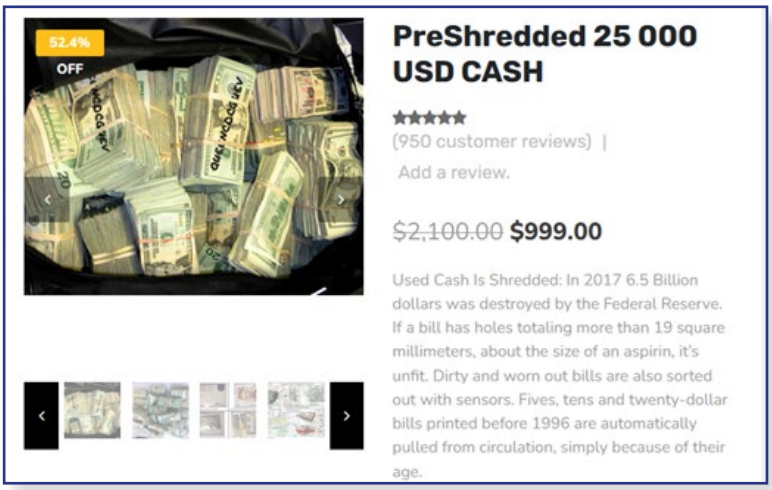
Con il termine Carding si fa riferimento all'utilizzo di carte di credito rubate o dei soli codici delle stesse, sottratti in diversi modi. Nei paesi dove le carte di credito in vendita nei forum undergound sono più diffuse, lo sono anche i furti. Ecco perché negli Stati Uniti bastano 1,50 dollari, mentre l'Europa è il mercato più salato per gli acquirenti di carte rubate: il loro costo è, in media, di 8 dollari. Nel Darkweb come nei mercati legali, a definire il prezzo è il rapporto fra domanda e disponibilità del prodotto. Ovviamente i criminali informatici sono maggiormente interessati alle carte con le quali è possibile rubare più denaro, oppure a quelle con sistemi di controllo bancario meno stringenti. Di seguito tre esempi di mercati underground che si occupano di carding:

Empire Market

"Alla gente piace il darknet perché ci sono un sacco di soldi da fare. Con alto profitto arriva il rischio. Se ci scegliete rispetto ad altri servizi il vostro rischio è quasi zero. Se non riesci a gestire il piccolo rischio o l'ansia ti consigliamo sempre di investire il tuo denaro in una banca. Ricorda che non è difficile raddoppiare o triplicare i tuoi soldi rapidamente sulla darknet, ecco perché alla gente piace. Ma non fare mai niente che ti metta a disagio."

Empire è un mercato Darknet lanciato nel febbraio 2018. Modellato sul mercato AlphaBay, sequestrato, il negozio si occupa di prodotti illeciti, vietando però la vendita di fentanyl e azioni terroristiche. Qui gli utenti cercano di acquistare maggiormente prodotti relativi a Carding, trasferimenti di denaro, droga, denaro falso, armi, carte regalo, documenti falsi e servizi di hacking. I prodotti possono essere acquistati utilizzando Bitcoin. La registrazione non è obbligatoria e si offrono rimborsi completi e/o parziali, spedizione in oltre 200 paesi e un team di supporto 24/7.

Gli amministratori del negozio dichiarano di vendere solo il 5% dei loro contanti: il 95% passa attraverso le aziende che possiedono e poi nei loro conti bancari; il restante 5% viene venduto su TOR per ottenere bitcoin. Sembrerebbe una parte molto piccola, ma c'è un motivo: l'acquisto di centinaia di migliaia di bitcoin ogni settimana porterebbe l'attenzione su di loro.



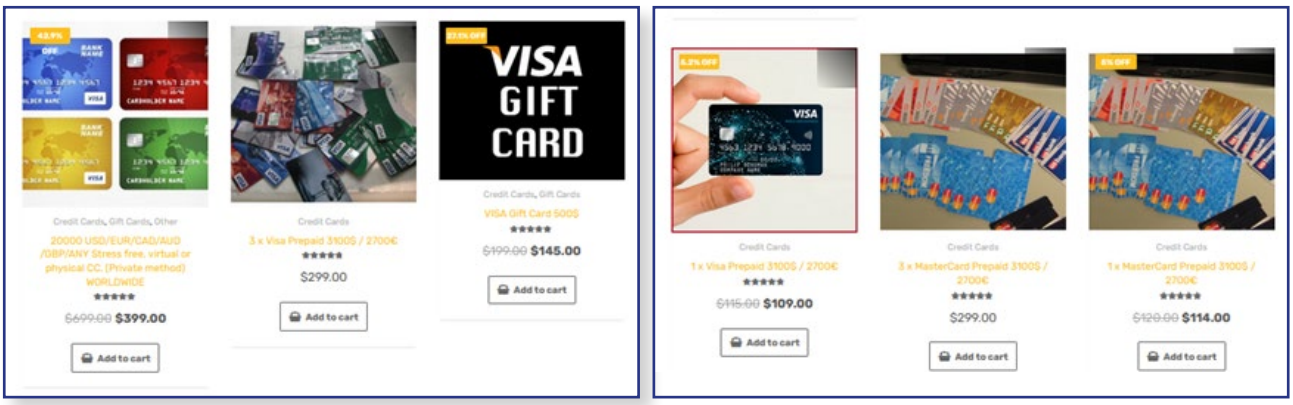
Nelle FAQ si legge: *"Da dove viene questo denaro? È reale o contraffatto? Questo è 100% reale, valuta rubata dalla FED prima che potrebbe essere triturato. Non hai assolutamente alcun rischio. Ogni anno vengono selezionati miliardi di dollari per lo smaltimento. Nessuno rintraccia i soldi che dovrebbero essere distrutti. Depositarlo in distributori automatici, conti bancari o bancomat con completa sicurezza."*

La dimensione massima dell'ordine è di $ 100.000. Bitcoin (BTC) e Monero (XMR) sono le valute principali. Tuttavia, dal 31 luglio 2022 sono consentite anche Litecoin, Binance coin, TetherUSDT, Tron, Doge coin, Ethereum. Una volta che si acquista la merce sarà contrassegnata come in elaborazione, il venditore ha 12 ore per completare l'ordine inviando l'articolo e contrassegnarlo come spedito altrimenti verrà annullato. Una volta che l'ordine è stato contrassegnato come spedito, l'acquirente può finalizzarlo una volta ricevuto l'acquisto, contestarlo se c'è un problema o estendere l'impegno, se necessario.

È presente una sezione dedicata a chi desidera diventare venditore, pagando una commissione. Tutti i fornitori saranno testati e controllati. I fornitori sono tenuti a configurare una 2FA per proteggere il proprio account.

La possibilità di tracking viene fornita il giorno stesso a seguito dell'acquisto e può essere trovato nella ricevuta nell'e-mail di conferma che si riceve. La maggior parte dei fornitori spedisce il pacchetto entro 1h dalla ricezione della notifica di pagamento in Escrow. Gli ordini di grandi dimensioni vengono spediti in scatole con etichettatura per farli apparire come un pacchetto Ebay o Amazon.

Riportiamo di seguito un esempio di carte vendute sul sito:



CardingTeam

"Siamo un gruppo di hacker professionisti con più di 15 anni di esperienza. Abbiamo una vasta esperienza in questo settore e vi offriamo questi servizi illimitati per fare soldi. Offriamo una varietà di servizi di hacking. È possibile acquistare carte online, trasferimenti di denaro, carding tutorial, e molti altri servizi."

Carding Team è un negozio di carte di credito underground aggiornato quotidianamente, con prezzi che arrivano fino ad un massimo di 200$. "Vogliamo che i nostri clienti ricevano le ultime novità del mondo del carding il prima possibile".

Nel dettaglio:

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

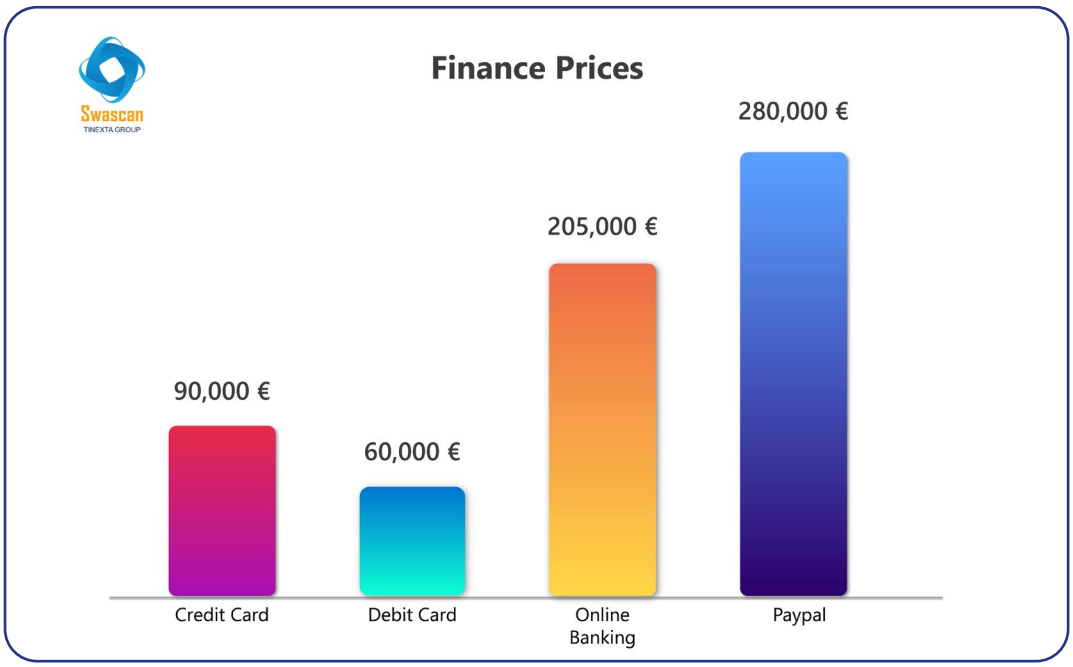
Simple Cash

"La prima regola per avere successo nel campo carding e hacking è quello di mantenere un basso profilo"

Altro mercato underground che si occupa di carding. La modalità di invio dei prodotti avviene all'interno di biglietti di auguri, riviste, libri.

Di seguito, esempi di carte in vendita:

A valle dell'analisi condotta, riportiamo una media dei prezzi offerti nei mercati Darkweb:



4. Identity leaks e credential access

Hai mai riutilizzato la stessa password per più di un account? È probabile che la risposta di tutti a questa domanda sia sì. A questo punto entrano in gioco i criminali informatici, che acquistano combinazioni di e-mail e password dai mercati nel Darkweb e tenteranno di accedere a molti altri siti per vedere se quella password è stata riutilizzata. A tal proposito, qualsiasi account che contenga informazioni finanziarie può avere valore per un criminale.

A differenza del mercato della droga, il mercato dei documenti contraffatti e credential access sembra essere più concentrato, con meno venditori che operano nella nicchia. Quando si analizzano i documenti messi in vendita, possiamo vedere come ci sono due tipi principali: documenti fisici e scansioni. In merito ai documenti fisici, i venditori affermano che saranno accettati dalle autorità come reali, presentandosi come copie esatte con tutte le caratteristiche di sicurezza che vengono replicate. Le scansioni, invece, sono copie di documenti reali - da utilizzare per la frode di identità. Durante la nostra ricerca, il range di prezzo varia da 250$ a 1500$, con una vasta gamma di paesi tra cui scegliere. Le carte d'identità contraffatte possono essere acquistate a partire da 300$ per una carta d'identità europea e 250$ per una patente di guida europea. Riportiamo di seguito tre esempi di siti sotto rete onion che vendono identity leaks e credential access:

ONION IDENTITY SERVICES

"Tutti i passaporti che vendiamo sono direttamente dall'autorità emittente, sono originali al 100%, solo con la tua foto. Le licenze ID Card e Driver sono repliche professionali, ma con tutte le caratteristiche di sicurezza (Microprint, UV, Holo)"

Il mercato effettua spedizione dalla Germania e non richiede spese di spedizione. I prodotti in vendita sono divisi in 3 categorie:

1. **Passaports**
2. **ID Cards**
3. **Driver Licenses**

Per ognuna delle categorie sono presenti prezzi differenti in base al paese per il quale è richiesto il prodotto. Si riporta di seguito una lista dei prezzi medi:

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

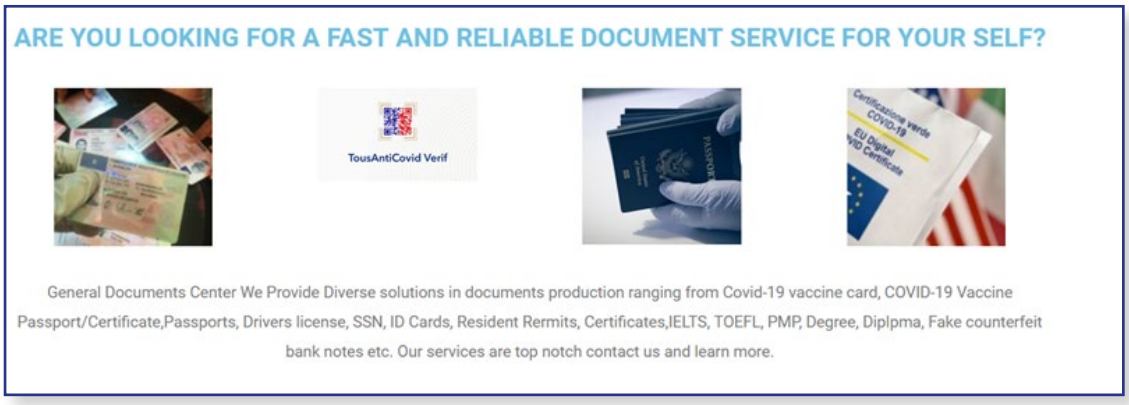
Norway Drivers License	550 EUR
Denmark Drivers License	550 EUR
Netherlands Drivers License	550 EUR
UK Drivers License	500 EUR
Lithuanian ID Card	500 EUR

Come funziona la vendita? Dopo aver acquistato un documento d'identità o un passaporto gli amministratori richiedono l'invio di un messaggio con età e sesso dell'acquirente inseriti in modo da poter trovare un set di dati corrispondente. È possibile richiedere ed utilizzare i documenti in qualsiasi paese, ma gli amministratori si raccomandano di cercare di evitare di usarlo nel paese di emissione, poiché un'altra persona vive già lì con quel documento. Non sono presenti limitazioni di utilizzo con i documenti acquistati. In merito alle tempistiche di spedizione, sono necessari circa 14 giorni per carte d'identità e patenti di guida, mentre 21 giorni per i passaporti.

I passaporti hanno una validità di 4-5 anni nei Paesi Bassi, mentre in tutti gli altri 8-10 anni. Non è possibile fare richiesta per una riduzione di prezzo.

GENERAL DOCUMENTS CENTER

"Abbiamo 17 anni di esperienza in questa rete di documenti reali e falsi, sappiamo che la tua visita a questa pagina non è accidentale. Sappiamo che avete le vostre diverse ragioni per contattarci e voler acquistare i nostri prodotti. Siamo una rete molto grande di che forniscono al mondo con documenti reali e falsi. Siamo partner i governi e altri alti funzionari,ci occupiamo di investimenti, raccogliere capitali, prestiti e molte altre opportunità di business"



Il mercato garantisce un elevato livello di privacy in relazione a tutte le informazioni personali che vengono raccolte. *"Puoi essere certo che le tue informazioni non saranno mai vendute a nessun altro cliente o viste da nessuna parte su Internet. Useremo le tue informazioni solo per lo scopo per cui sono destinate."*

Di seguito alcune categorie vendute:

1. Covid Greenpass e PCR test:

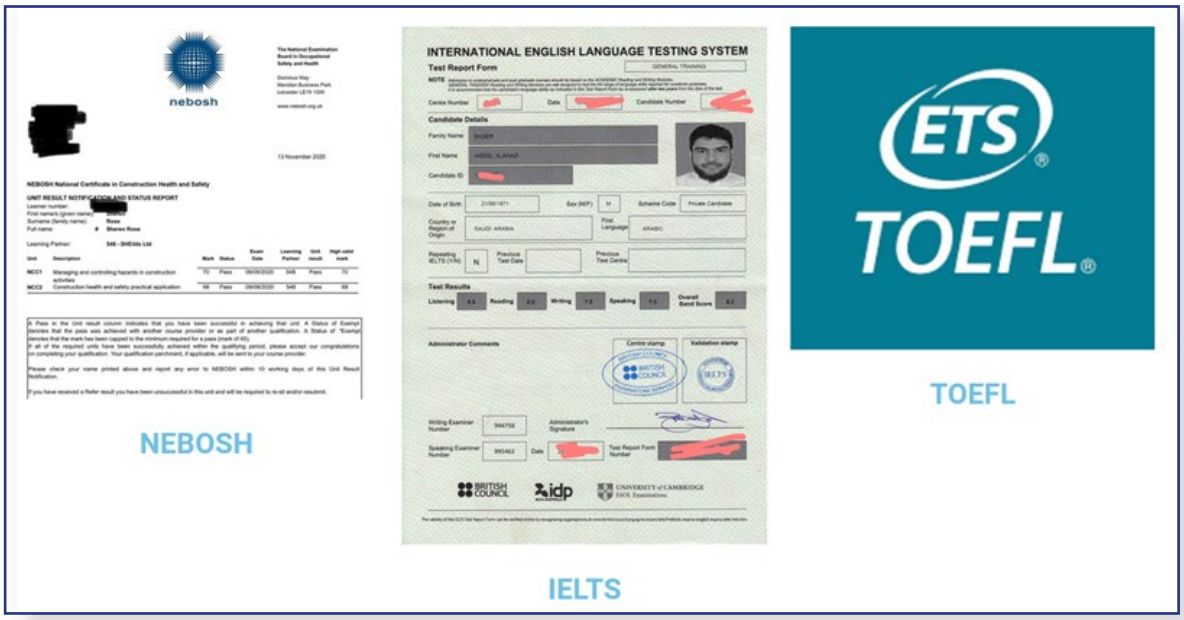
in questa sezione possiamo notare in particolare come vi è la sollecitazione delle persone in merito ad evitare la somministrazione del vaccino per i pericoli che questo può comportare, spingendo piuttosto all'acquisto del certificato. Nel black market si legge: *"La Corea del Sud ha recentemente visto i pericoli dei vaccini influenzali dopo che un certo numero di persone nel paese è morto a seguito di vaccinazioni influenzali stagionali. Un rapporto di Yonhap News Agency ha detto che ci sono stati 48 morti di vaccinazione influenzale a partire da ottobre, tra cui un ragazzo di 17 anni e un uomo anziano dalla città sud-orientale di Daegu. Come misura precauzionale, acquista il Passaporto Covid, non fare il vaccino."*

2. Documenti real e fake:

"Per il documento reale registreremo tutte le informazioni del titolare nel presunto sistema di database e il titolare utilizzerà legalmente il documento senza problemi"

3. Certificati di ogni tipo:

Certificati di formazione, carte internazionali, certificati di adozione, certificati di battesimo, certificati di nascita, certificati di morte, certificati di divorzio, certificati di matrimonio, diplomi di scuola superiore e molto altro ancora.



In ogni caso, "qualità" sembra essere la parola d'ordine, motivo per cui gli amministratori del negozio affermano che ogni documento venduto è stampato e testato con le stesse macchine governative ed è registrato nel sistema all'interno dei paesi a cui hanno accesso. I documenti hanno tutte le caratteristiche di sicurezza e sono tutti leggibili quando introdotti in un lettore, applicazioni NFC e RFID e scanner per controlli di frontiera, aeroporti e polizia.

MONEY CASHIER

"Il nostro team lavora direttamente con i funzionari governativi e produce documenti registrati e passaporti per i nostri clienti e abbiamo anche i nostri avvocati di immigrazione che seguono tutto il processo di documenti come la verifica dei passaporti reali e altri si assicura che le tue informazioni siano imputate in governo sistema di database"

Riportiamo di seguito una lista dei prodotti offerti dal mercato underground:

- **Counterfeit USD**
- **Passports**
- **Counterfeit AUD**
- **Counterfeit Pound sterling**
- **Counterfeit EURO**
- **Drivers License**
- **IDs**
- **Counterfeit CAD**
- **Social Security Cards & numbers USA**
- **Wire Transfers**
- **Counterfeit money**

In merito all'acquisto, le caratteristiche:

- **Spedizione gratuita in tutto il mondo su tutti gli ordini superiori a $500**
- **30 giorni soddisfatti o rimborsati**
- **Garanzia internazionale**
- **Checkout sicuro al 100% tramite PayPal / MasterCard / Visa**

"Tutte le caratteristiche segrete dei passaporti reali, degli ID e delle licenze dei conducenti sono accuratamente duplicate e contraffatte per una sicurezza del 100% quando si utilizza. Siamo professionisti unici nella produzione di documenti falsi"

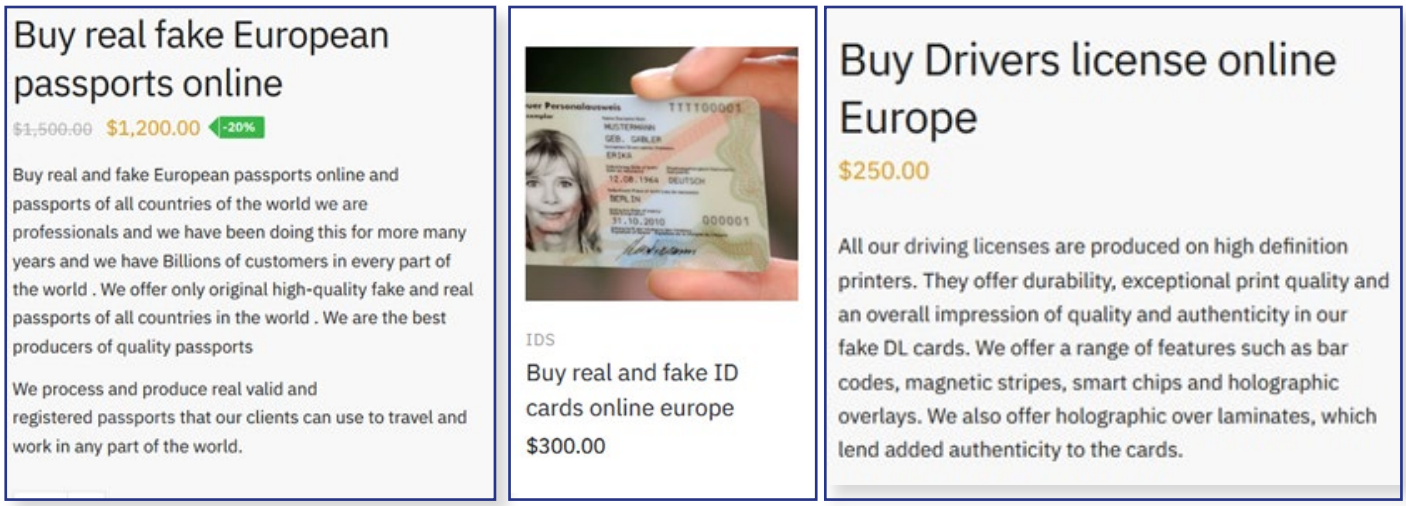
Le spedizioni si effettuano in tutto il mondo. Viene offerta la consegna in giornata per i clienti degli Stati Uniti e del Canada. Gli ordini europei e australiani richiedono da 3 a 7 giorni per l'arrivo del pacchetto. Dopo ogni acquisto o ordine dal sito, si riceve una fattura con un numero di tracking e dettagli di spedizione in modo da poter controllare lo stato dell'ordine e sapere quando avverrà la consegna.

Gli amministratori forniscono anche consigli in merito alla sicurezza verso i fornitori e assistenza clienti 24/7 tramite la chat dal sito raggiungibile sotto rete onion o direttamente tramite Whatsapp sul numero fornito.

Per quanto riguarda le modalità di pagamento e funzionamento, si accettano solo pagamenti Western Union e Money Gram. Tuttavia, non è possibile procedere al pagamento se l'ordine è inferiore al limite minimo, che è fissato a 200-$250. Di solito si richiede un documento solo se si sta effettuando un ordine di oltre $ 1.000. In tal caso, è sempre possibile dividere un ordine in ordini più piccoli, in modo da evitare di inserire documenti personali. È inoltre possibile richiedere consegne dirette a domicilio solo per ordini superiori a $ 500.

In generale, il prezzo minimo che si può trovare sul sito è $300, mentre il prezzo più alto $25.000.

Il negozio garantisce un rimborso o sostituzione del prodotto entro 12 giorni in caso di merci che arrivano al cliente in condizioni difettose o danneggiate, o nel caso il cliente non sia soddisfatto dell'acquisto. Nei casi in cui la perdita, il danno o il ritardo sia dovuto a un indirizzo di consegna errato fornito da parte dell'acquirente, il rimborso non può essere erogato.



Anche in questo caso, i fornitori sono in grado di produrre sia patenti di guida reali che false, ma si consiglia ai clienti l'acquisto di documenti reali se si vuole legalmente utilizzare il documento. Tutti i documenti sono prodotti su stampanti ad alta definizione.

5. Armi

Negli stessi forum è possibile anche acquistare armi e munizioni da tutto il mondo: USA, Canada, Germania, United Kingdom, Francia, Svizzera, Svezia, Netherlands, Norvegia, Danimarca, Finlandia, Italia, Austria, Spagna, Australia, Russia, India, Giappone, China, e molti altri paesi ancora.

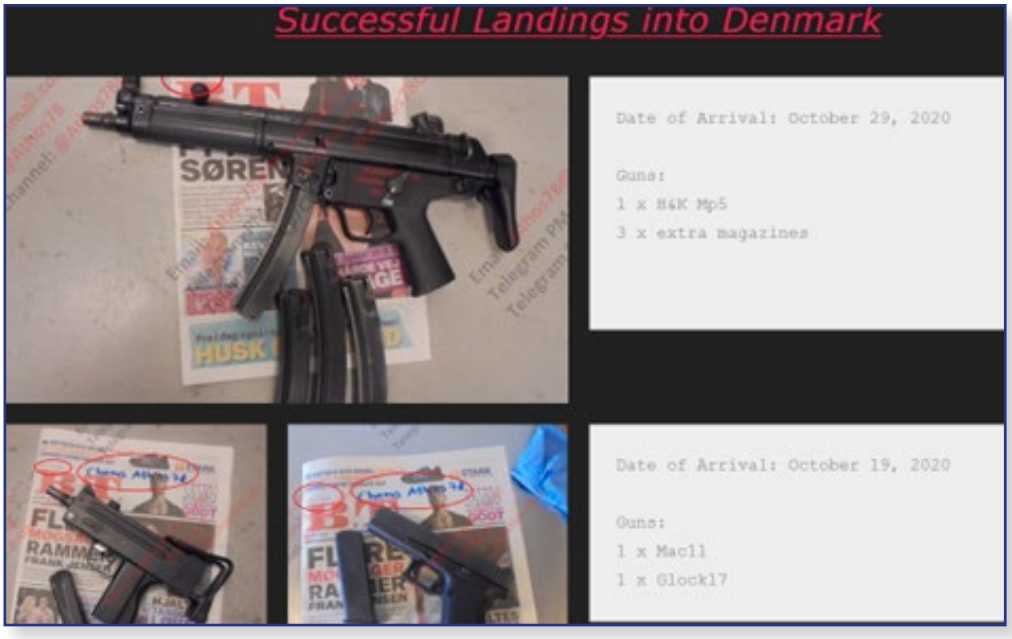
Questo studio fornisce uno snapshot della disponibilità di armi in tre darknet markets. Nel complesso, sono state identificate 125 armi, tra cui pistole, fucili, mitragliatrici, fucili, munizioni, esplosivi e accessori come i silenziatori. I mercati vendevano anche altre armi come taser, spray al peperoncino e coltelli, manuali di armi fai da te, armi chimiche, biologiche, nucleari e radiologiche. I dati hanno permesso di stimare il costo delle armi fino ad un massimo di 2400$. La maggior parte delle volte, le armi sono nuove e inutilizzate. È possibile decidere il luogo di consegna delle armi: ci si raccomanda di optare per un posto remoto, non visibile e difficilmente raggiungibile.

ATHOS78

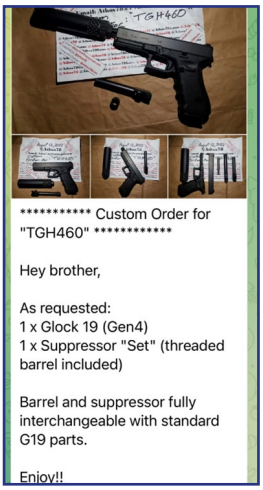
Sito di armi illegali che offre prodotti a coloro che:

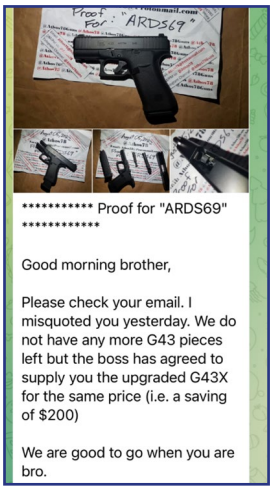
- **vivono in un paese in cui il possesso di armi è vietato**
- **hanno la fedina penale sporca**
- **vogliono stare lontano dagli occhi della polizia**
- **hanno bisogno di spedire le armi in modo inosservato**

Il sito ha un'intera pagina dedicata alla prova dell'arrivo delle armi vendute nei vari paesi. Riportiamo di seguito uno screenshot che dimostra l'acquisto da parte di un cliente:



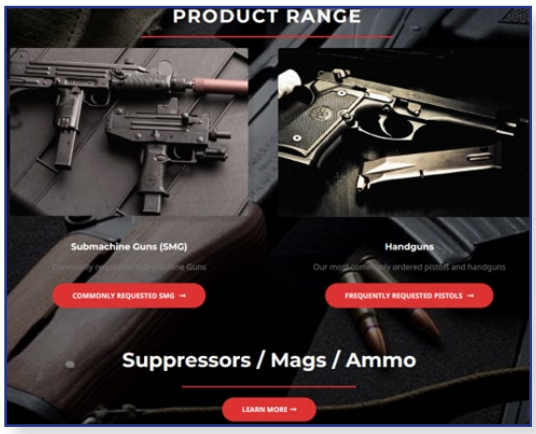
Gli amministratori hanno anche una pagina dedicata ad un campione di armi che possono essere fornite ai clienti. È possibile interagire con il venditore e chiedere di fare un video mentre scrive una parola in codice che si sceglie o chiedere loro di strappare un angolo di carta in modo da provare la loro esistenza, oppure scattare le foto con il prodotto da diverse angolazioni. A tal proposito, il mercato presenta un canale Telegram attivo da febbraio 2020 dove si interagisce con i clienti, si riportano fatture di ordini, foto a prova della vendita e spedizione, video dei fornitori che mostrano le armi.

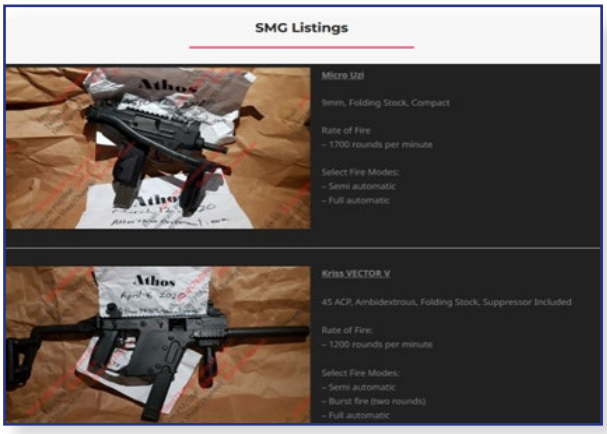


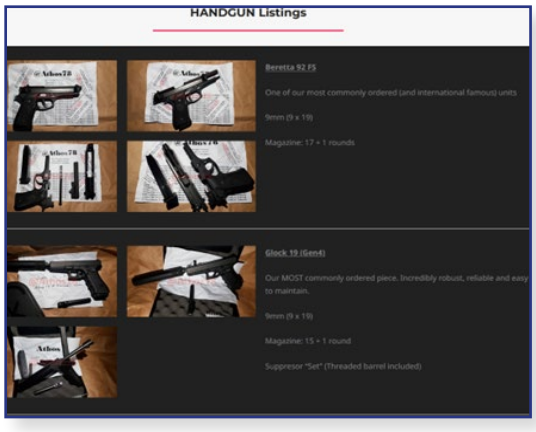


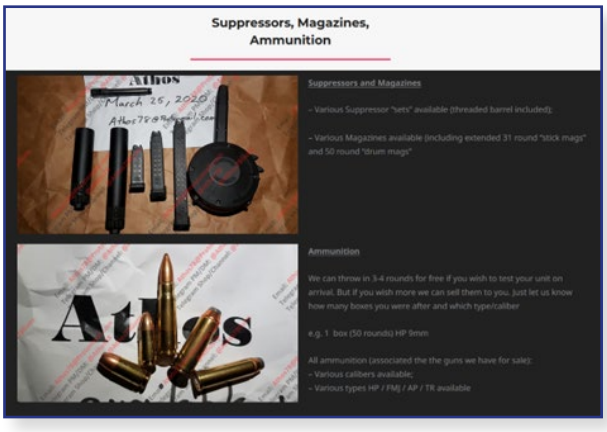
Sono presenti tre categorie di prodotti acquistabili:

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









Di seguito riportiamo una media dei prezzi offerti sul mercato:

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

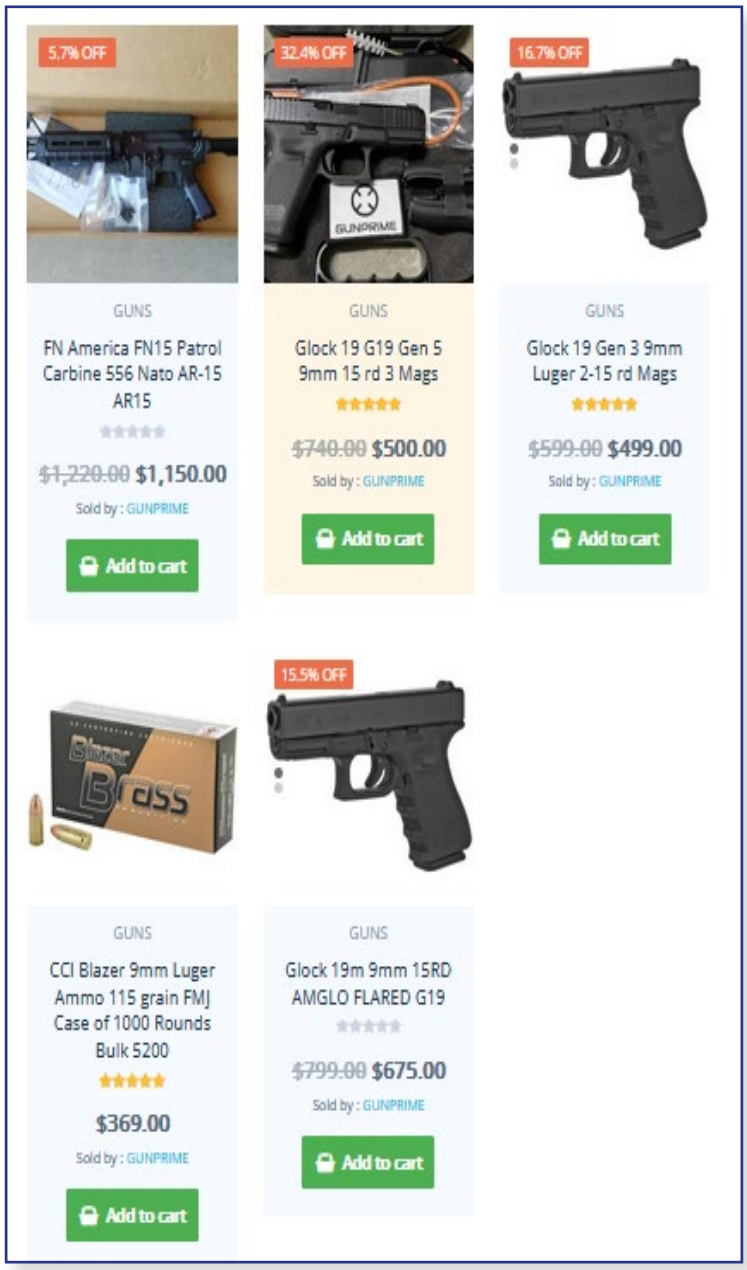
"I nostri venditori sono il cuore del Dark Market. Forniscono prodotti di alta qualità verificati che separano un mercato darknet da un negozio Clearnet. I nostri fornitori sono selezionati a mano dal nostro team al fine di offrire un catalogo di prodotti all'avanguardia"

THE DARK MARKET è un mercato darknet lanciato nel marzo 2020 che offre prodotti nelle seguenti categorie: contraffazioni, farmaci, carte di credito, documenti, elettronica, carte regalo, pistole, servizi di hacking, trasferimenti di denaro e altro ancora.

I fornitori sono scelti dagli amministratori del sito. Anche se il mercato si occupa di prodotti illeciti, ha vietato la vendita e riproduzione di materiale e/o attività terroristiche. Tutti i venditori devono avere una chiave PGP prima di iniziare a vendere per comunicare con l'amministratore. L'autenticazione *a*

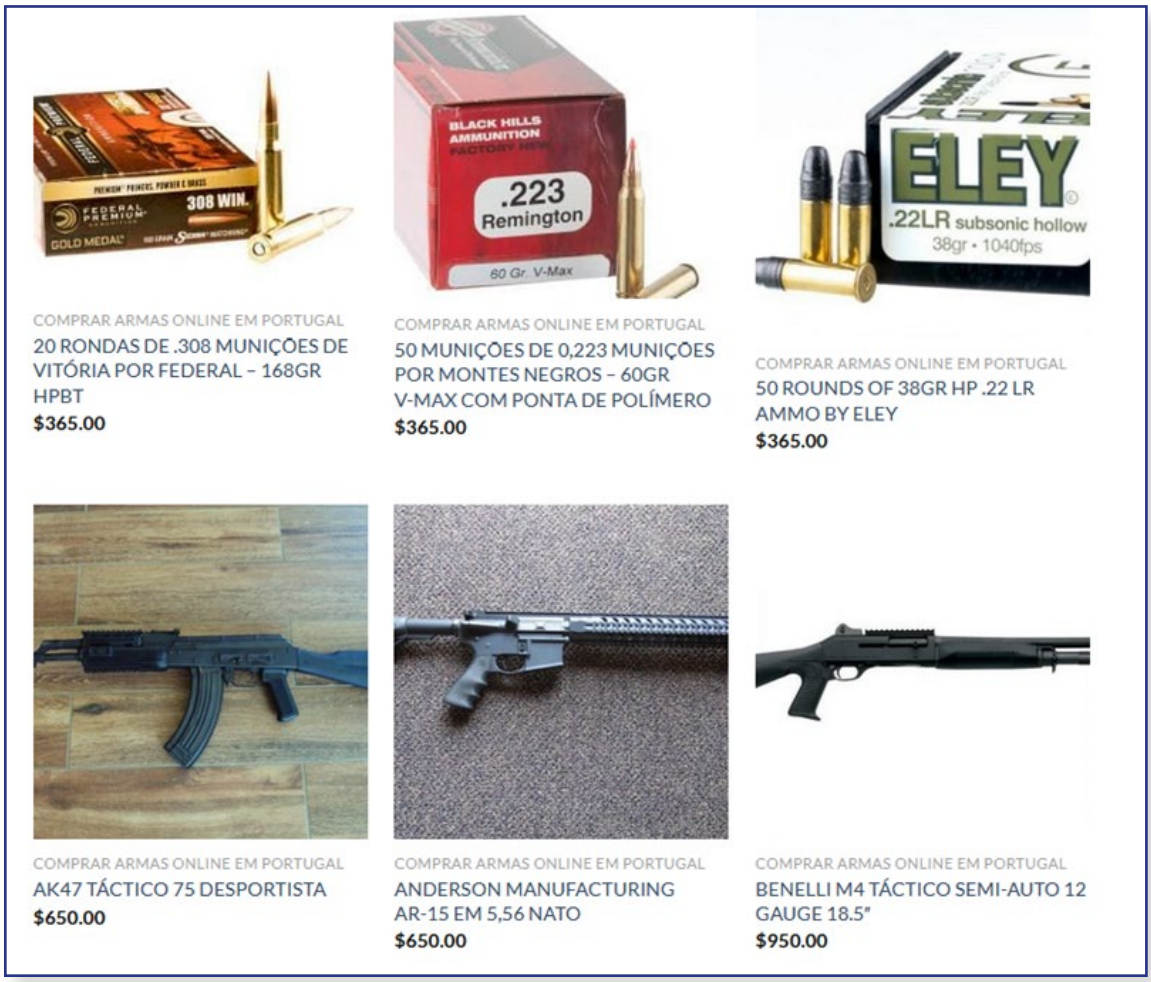
due fattori (2FA) è obbligatoria per tutti i fornitori, i quali devono pagare $ 400 per poter iniziare a vendere sul sito. La commissione del fornitore non è rimborsabile, questo per proteggere il mercato dai truffatori. Non è consentito chiedere i soldi prima dell'arrivo del prodotto all'acquirente e non è consentito trattare al di fuori del mercato. Qualsiasi venditore sorpreso a trattare al di fuori del mercato, utilizzando app di terze parti, sarà immediatamente bannato.

Tutti i venditori spediscono in tutto il mondo con un sistema di tracking mandato via e-mail entro 1h dopo il pagamento. La maggior parte dei fornitori spedisce il pacchetto entro 1h dalla ricezione della notifica di pagamento in Escrow.



BOTMANS WORLD

"Botmans Ammunition World ha reso lo shopping per le armi da fuoco più vantaggioso offrendo una selezione di pistole accessibili per l'acquisto sul web"



Il sito risulta attivo da ottobre 2021, ed è possibile acquistare diversi tipi di armi, tra cui munizioni, pistole, fucili, revolver, con un range di prezzi che parte da 10$ fino a 2500$.

Le armi vengono spedite in 5 - 8 giorni lavorativi (15 - 18 giorni lavorativi per l'Alaska).

Gli acquirenti di armi da fuoco devono avere almeno 21 anni, fatta eccezione per alcune armi per cui è concessa la vendita anche a coloro che hanno 18 anni. Il negozio non si assume responsabilità se le armi violano leggi presenti nel paese dell'acquirente.

Sul sito sono inoltre disponibili corsi online sulla sicurezza delle armi da fuoco per una migliore procedura di addestramento

Progettato da "istruttori di armi da fuoco", come si definiscono sul sito, questo corso online sulla sicurezza delle armi da fuoco include la parte teorica di cfsc e crfsc. Combina video qualificati, diapositive informative e quiz pertinenti per aiutarti nella preparazione. Diversi studenti utilizzano questo corso teorico online per integrare il loro coaching sulla sicurezza delle armi da fuoco prima di frequentare un corso o come revisione e aggiornamento.

Il corso si concentra su:

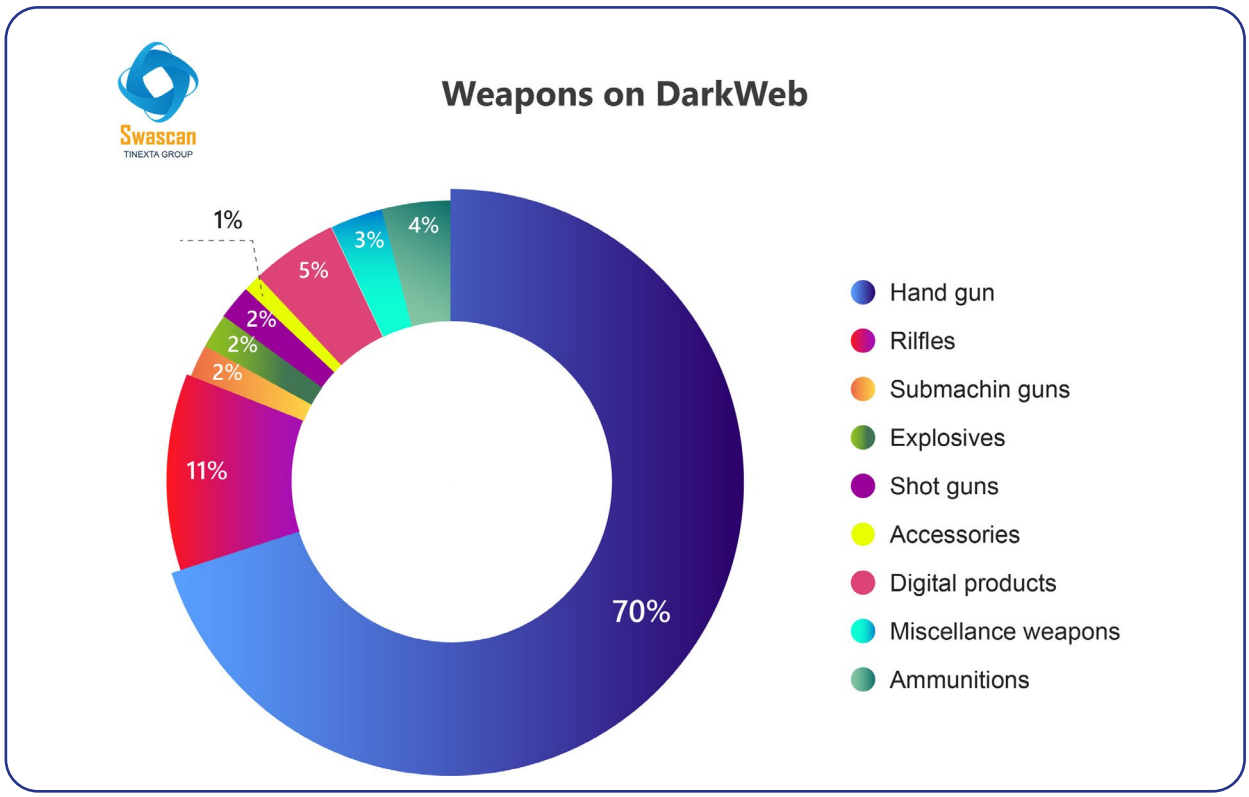
- **L'evoluzione delle pistole, parti principali, tipi e azioni**
- **Sicurezza di base delle armi da fuoco**
- **Armi da fuoco operative**
- **Procedure di movimentazione e trasporto sicure**
- **Tecniche e procedure di utilizzo**

- **Cura delle armi da fuoco**
- **Stoccaggio, visualizzazione, trasporto e manipolazione sicuri di armi da fuoco**
- **Munizioni**
- **Responsabilità del proprietario/utilizzatore di armi da fuoco**
- **Video e prove pratiche**

Come negli acquisti sul clearweb, per attirare acquirenti vengono forniti pacchetti: se questo corso online sulla sicurezza delle armi da fuoco viene acquistato in combinazione con altri corsi, si riceve la possibilità di ripetere i test gratuitamente, altrimenti è necessario pagare $60.

Gli amministratori offrono anche l'opzione in caso di covid-19, estendendo le date per il completamento del corso in caso di positività. Per l'esame scritto è necessario un punteggio di superamento del 70%.

A seguito dell'analisi sui tre siti, riportiamo una visualizzazione grafica della vendita di armi presente sul Darkweb:



HIRE A KILLER ON DARKWEB

Cosa potresti comprare se sapessi che nessuno sta guardando? Quando la conversazione si sposta sull'argomento del DarkWeb e su ciò che vi si può procurare, le prime cose che vengono in mente sono probabilmente gli oggetti illegali sopra citati: droghe, documenti, armi...

Ma i beni materiali non sono le uniche cose che le persone acquistano negli angoli irrintracciabili di Internet. Ogni tanto arrivano notizie di qualcuno che ha tentato di usare il lato oscuro del web per un altro scopo: l'omicidio. Quando pensiamo al DarkWeb, infatti, la maggior parte di noi immagina un luogo ombroso e sinistro, un luogo "Dark", appunto. Tuttavia, la stragrande maggioranza delle persone non l'ha mai effettivamente visitato, o addirittura saprebbe come farlo; tutto ciò che sappiamo è che il suo mantello di anonimato è un'altra arma nell'arsenale criminale moderno, e mentre può servire per scopi perfettamente innocenti, l'attività illegale che si svolge nell'ombra potrebbe essere ancora più oscura di quanto si possa sospettare.

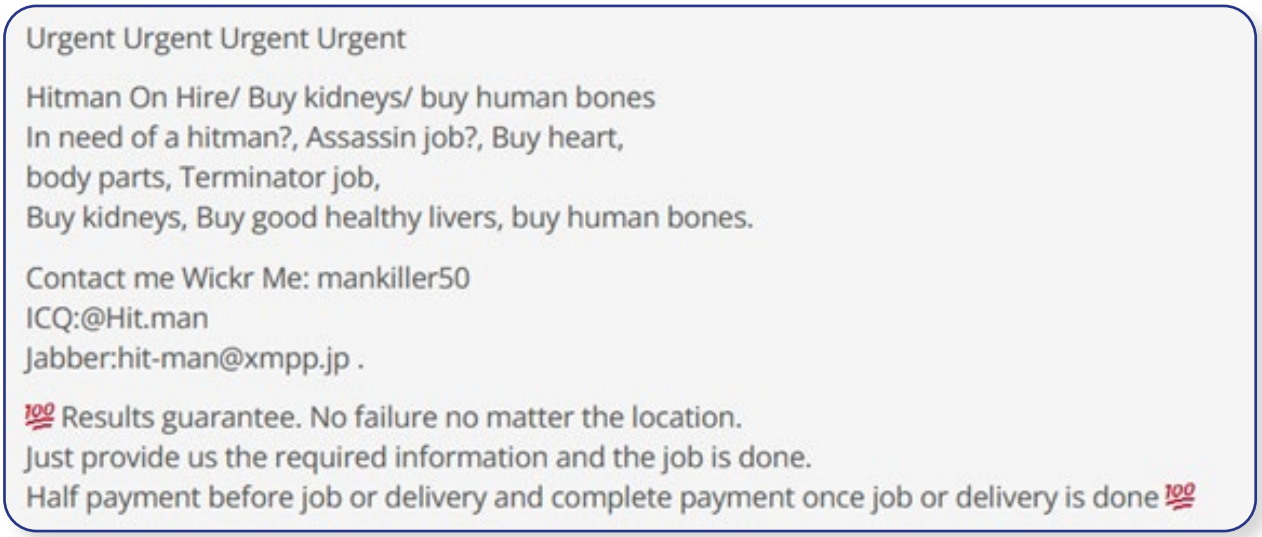
Difatti, il suo emergere negli ultimi dieci anni ha permesso la proliferazione dei Killing Forum, con la presenza di sicari all'interno. A differenza della maggior parte dei siti Internet tradizionali, i siti sotto rete Tor utilizzano una tecnologia che consente un'interazione online tra Client e Server nascondendo la propria identità e posizione, sia reciprocamente e sia dalle forze dell'ordine. Sebbene la maggior parte dei siti di omicidi a pagamento sul dark web siano probabilmente truffe, le persone continuano a cercare di sollecitare assassini a contratto. Nonostante i frequenti resoconti di arresti da parte dei media, il numero di annunci per questo tipo di servizi e la creazione di nuovi Killing Forum continua ad essere un trend in crescita.

In alcuni forum DarkWeb, i killer si descrivono come ***"i più affidabili, sicuri e potenti sul mercato. Abbiamo migliaia di clienti soddisfatti e centinaia di sicari. Se stai cercando di uccidere qualcuno, picchiarlo, rapirlo non farlo da solo! Vediamo se possiamo farlo per voi ad un prezzo basso".***

Le caratteristiche che offrono:

1. Mercato anonimo, sicuro e complesso
2. 0% di anticipo, bisogna solo fornire la prova di avere i bitcoin
3. Miglior rapporto qualità-prezzo e centinaia di sicari tra cui scegliere
4. Feedback positivo ovunque, nessuna lamentela
5. Comunicazione criptata tra clienti e sicari
6. Visualizzazione dello stato di avanzamento della richiesta
7. Supporto PGP per la sicurezza aggiuntiva
8. Built-in mixer per aumentare la sicurezza bitcoin
9. Sicurezza del 100% sul compimento del lavoro. Se un lavoro non si può svolgere, gli amministratori del forum non lo prendono
10. Chat tra i membri del forum

Il mercato è utilizzato da migliaia di membri di gang e sicari. I clienti sono completamente anonimi: nessun nome, nessun numero di telefono, nessun indirizzo e-mail, nessun conto bancario e nessuna carta di credito.


Urgent Urgent Urgent Urgent

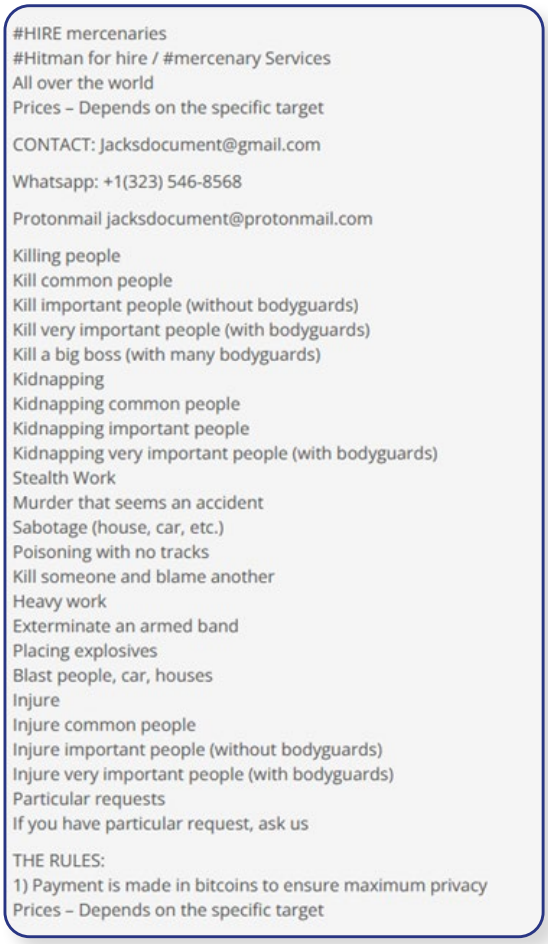
Hitman On Hire/ Buy kidneys/ buy human bones
In need of a hitman?, Assassin job?, Buy heart,
body parts, Terminator job,
Buy kidneys, Buy good healthy livers, buy human bones.

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 💯

Perché assumere un assassino sul DarkWeb?

Su alcuni Killing Forum, quali "Hitmen Cyber Team" o "Jabba Syndacate", i sicari mettono in guardia dai killers che si potrebbero assumere da altre parti, affermando che gli altri richiedono un anticipo del 50% prima che il colpo venga eseguito, evidenziando la possibilità che se il killer scappa con i soldi non si può andare dalla polizia. Nel servizio svolto nei forum DarkWeb non si forniscono anticipi: si fornisce la prova dei fondi, si svolge il lavoro e si paga solo a compimento dello stesso. Nessun incontro rischioso e pericoloso tra clienti e sicari: non c'è il rischio di essere arrestato da poliziotti sotto copertura o di essere ricattato in quanto l'identità del cliente è nascosta.



#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

"È semplice, è conveniente, sicuro, anonimo, ti esclude dalla lista delle forze dell'ordine del sospettato. Dopo che ci hai fornito i dettagli sull'obiettivo e ci hai mostrato la prova che hai fondi disponibili, assegneremo un sicario sul posto di lavoro. Egli darà una stima della data dell'assassinio: in quella data il cliente può viaggiare in una città diversa e visitare qualche centro commerciale che ha telecamere di sorveglianza per avere un alibi forte".

Una volta che il lavoro è stato portato a termine, il killer invia una conferma, e si può richiedere fino a due settimane per confermare personalmente che il lavoro è stato svolto prima di rilasciare i fondi per il sicario.

Per fare la richiesta è sufficiente compilare un semplice modulo inviando l'immagine del bersaglio da colpire e la sua posizione.

La prova dei fondi può essere fornita inserendola in un deposito cauzionale sicuro, a scelta del cliente. I fondi rimangono lì fino a quando non si è soddisfatti del lavoro.

All'interno dei Marketplace si trovano inoltre consigli su come utilizzare i servizi hitmen: un cliente dovrebbe seguire alcune regole per evitare di essere arrestati o truffati

- Regola numero 1: Rimanere anonimi. "Non lasciare che il killer sappia chi sei. Non dare nome, numero di telefono, indirizzo e-mail, carta di credito o conto bancario e nascondere il tuo IP con VPN o Tor Browser. Se il killer viene arrestato, non potrà dire chi l'ha assunto".

- Regola numero 2: Non incontrare i sicari di persona. "Internet è pieno di notizie su persone arrestate quando hanno cercato di incontrare un sicario di persona".

- Regola numero 3: Usa sempre una comunicazione che mantiene segreta la tua identità. "Non comunicare mai con un killer utilizzando una vera e-mail o un numero di telefono".

- Regola numero 4: Mai pagare in anticipo. "Nessun anticipo del 50%, né denaro prima che l'omicidio sia fatto. Per dimostrare di avere bitcoin pronto per l'uccisione è possibile utilizzare un deposito di garanzia esterno".

Difatti, uno dei sistemi che ha reso sicuri i pagamenti in Bitcoin per i clienti e commerciali è quello che si definisce Bitcoin Escrow, una sorta di filtro di sicurezza per le parti che lo utilizzano in modo da non poter cadere in truffe online. Utilizzando un escrow, il compratore non manderà i Bitcoin direttamente al venditore, ma ad un deposito, che rimarrà bloccato finché l'acquirente non sarà soddisfatto del servizio. Se c'è una controversia, l'amministratore del deposito cauzionale interviene e arbitra l'affare

a pagamento. Sebbene sia nato come un servizio a scopi leciti, ci sono escrows sul DarkWeb utilizzati per richieste illegali che accettano bitcoin e forniscono pieno anonimato per il cliente e il venditore. In primo luogo, si crea una transazione di impegno in cui si inserisce il prezzo, la descrizione del lavoro, e il tempo previsto per la realizzazione.

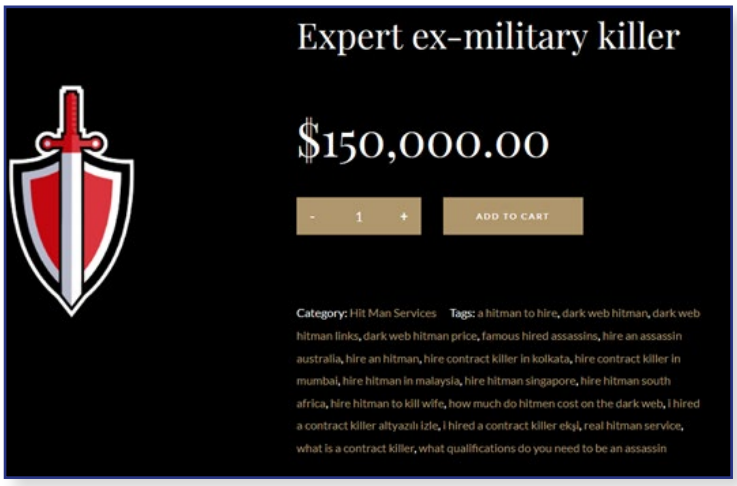
Successivamente, si inseriscono i bitcoin nel deposito, per mostrare al killer che si possiedono i fondi.

Una volta che il killer compie il lavoro, si rilasciano i fondi al killer. Se il killer non riesce a svolgere il lavoro si richiedono i fondi indietro dall'amministratore di garanzia. Al contrario, se il killer svolge il lavoro e il cliente si rifiuta di pagare, il killer invierà un reclamo all'amministratore del deposito insieme alla prova dello svolgimento del lavoro, e chiederà l'invio del denaro previsto.

Listino prezzi

Si parla di crime-as-a-service, ovvero di crimini che vengono commissionati a specialisti attraverso il web. Questi mercati underground, possedendo centinaia di hitmen, offrono prezzi differenti che differiscono da sicario a sicario. Ogni killer può stabilire i propri prezzi per i servizi che fornisce, dato il suo livello di abilità.

Alcuni criminali meno qualificati hanno prezzi più bassi, mentre ex-militari esperti che possono abbattere obiettivi più importanti avranno prezzi più elevati.



Di seguito una media dei prezzi delle opzioni più comuni che è possibile trovare sui forum DarkWeb:

SERVIZIO	PREZZO MEDIO
ASSASSINIO mediante:	
Pistola	15.000$
Coltello	22.000$
Avvelenamento	40.000$
Avvelenamento indolore	42.000$
Tortura	50.000$
Morte "accidentale"	20.000$
AGGRESSIONI:	
Acido	4.000$
Deturpazione facciale	3.000$
Paralizzare	10.000$
Castrazione	30.000$
Altre modalità:	
Rapina	2.000$
Pestaggio	2.000$
Incendio doloso	8.000$
Sequestro di persona	15.000$

In ogni caso, i prezzi variano in base a numerose variabili. Per esempio, come si legge in un forum DarkWeb, in un comune Shen-Buzhri del Cantone di Ginevra il marito ha ordinato l'omicidio della moglie a tre nativi del Kosovo che dovevano ricevere 400 mila franchi. In un altro caso, la suocera e la moglie ordinarono l'assassinio del marito per 50 mila franchi, mentre il proprietario di un ristorante ne ha pagati 20 mila per la liquidazione del concorrente.

I prezzi variano anche in base al paese. In forum russi, ad esempio, attuano in media i seguenti prezzi:

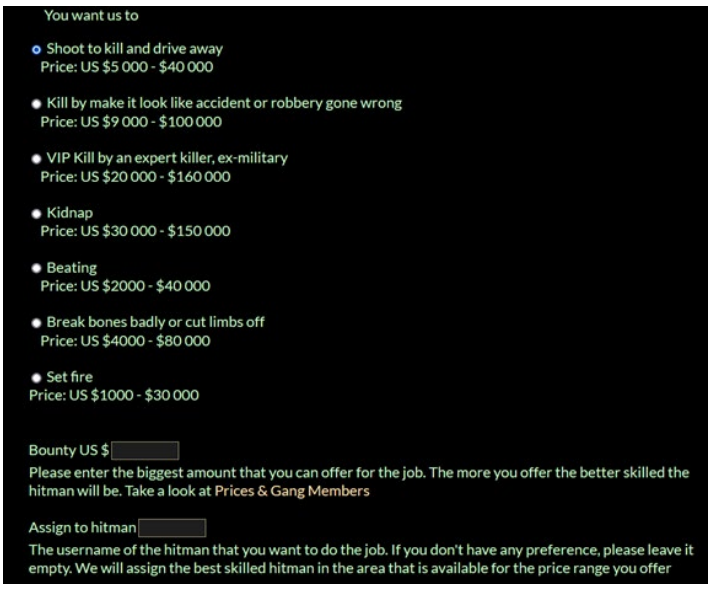
- omicidio di un cittadino comune 8000-10000$
- omicidio di un mediocre uomo d'affari 12000-18000$
- omicidio di un deputato da 40000 $
- omicidio dell'oligarca da 80000$

In generale, il prezzo dipenderà dalla complessità dell'ordine e ogni volta sarà ristabilito.

Il modulo d'ordine

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

Per ottenere un preventivo su quanto si dovrebbe offrire si può chiedere una domanda sul forum di discussione: gli amministratori del forum si raccomandano di non specificare il nome o l'indirizzo di destinazione sul forum stesso in quanto visibile a tutti, ma indicare solamente il paese, la difficoltà del lavoro richiesto ed altre informazioni generiche che possono essere utili ai fini dell'attività. Verrà assegnato il miglior killer per il lavoro tenendo conto della difficoltà dello stesso, dei costi e del luogo.



Come sfuggire ai controlli

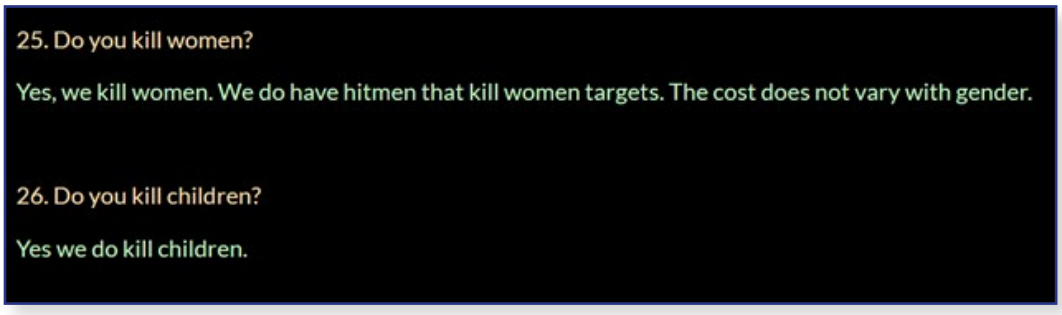
Nella sezione FAQ di uno di questi forum, una domanda è la seguente: "Perché LEO (acronimo di Law Enforcement Officers, utilizzato più in generale per tutte le forze dell'ordine, quali polizia, FBI, NSA, tutti gli agenti che lavorano per il governo per catturare i criminali) non riuscirà a catturare i membri della nostra banda con l'immissione di ordini falsi?"

La risposta che si legge è che prima di attaccare un obiettivo, i membri delle gang effettuano indagini di base. Una volta che un ordine viene inviato, un membro della gang viene mandato sul posto: sembrerà un normale civile, disarmato, che guida e cammina per strada nella zona. Una volta identificato l'obiettivo, il sicario si guarderà intorno alla ricerca di furgoni o auto sospette che possano proteggere l'obiettivo stesso.

Le gang criminali effettuano, inoltre, dei test a tutti i membri che si iscrivono come sicari: non fanno affidamento su immagini o video, perché questi possono essere falsi, si recano sul posto per controllare l'effettiva esecuzione della richiesta: "La polizia sotto copertura, non potendo arrecare danno agli innocenti, fallirebbe il test".

"Ecco perché la polizia non fa ordini falsi. È un casino troppo grande se falliscono, e una ricompensa troppo piccola, se prendono un solo sicario dopo il loro obiettivo, il meccanismo continuerà a funzionare, e la loro vittima sarà già morta".

Altra domanda frequente riguarda la tipologia di lavori accettati dalle gang. Generalmente, nei forum non si accettano lavori su minori di 16 anni. Altre eccezioni potrebbero essere politici di alto livello e alcuni individui famosi ben protetti, leader ecc. La valutazione viene effettuata caso per caso. Tuttavia, come è possibile notare nell'immagine di cui sotto, alcuni forum uccidono liberamente anche donne e bambini, senza una variazione di prezzo.



CONCLUSIONI

La proliferazione dei black market così come del numero degli oggetti in vendita sta rapidamente assumendo dimensioni preoccupanti. Siamo di fronte a merci – di ogni genere – vendute a prezzi molto accessibili.

Dobbiamo riflettere su quanto – oltre alle classiche attività illecite presenti all'interno del Darkweb – il cyber crime in senso lato stia divenendo sempre più ready to use.

Non è riduttivo immaginare come, aggiungendo all'equazione un vero e proprio e-commerce di strumenti di hacking ready to use, il cyber crime continui a proliferare.

È un definitivo cambio di paradigma, se fino a qualche anno fa chi s'incaricava di creare malware e altri strumenti atti al cyber crimine era poi anche l'utilizzatore finale, oggi chi ha acquisito sufficienti competenze e skill per portare a termine il primo step ha cambiato il proprio "business model". Si limita a vendere il proprio "prodotto" a criminali terzi. Le competenze sono in vendita.

Il mantra di motivazione, opportunità e mezzi non è cambiato, ma se prima opportunità e mezzi erano limitati ad un ristretto numero di Criminal Hacker, oggi, con la creazione di questa sorta di mercato libero del cyber crime opportunità e mezzi sono incrementati a dismisura.

CYBER SECURITY FRAMEWORK

L'approccio migliore per aumentare la resilienza del perimetro passa per i tre pilastri della Cyber Security moderna. Per questo motivo vanno solidificati e rispettati i tre canoni di:

- **Sicurezza Predittiva**
- **Sicurezza Preventiva**
- **Sicurezza Proattiva**

Sicurezza Predittiva

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

Sicurezza Preventiva

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

Sicurezza Proattiva

1. Security Operation Center
2. Incident Response Team

CYBER THREAT INTELLIGENCE

Questa ricerca è stata possibile grazie alle copetenze del **SoC e Threat intelligence team** di swascan e della piattaforma di threat intelligence.

Le informazioni sulle Cyber minacce a cui potrebbe essere esposta un'azienda, o Cyber Threat Intelligence, sono i dati che vengono utilizzati per comprendere le minacce che hanno colpito, vogliono colpire o stanno per prendere di mira il proprio perimetro aziendale.

Queste informazioni vengono utilizzate per preparare, prevenire e identificare possibili Cyber attacchi che cercano di fare breccia e acquisire dati sensibili aziendali (o in alternativa, semplicemente essere disruptive).

L'utilità della **Cyber Threat Intelligence** è evidente. Aiuta le aziende ad acquisire conoscenze preziose sulle minacce direttamente più incombenti, a costruire meccanismi di difesa efficaci (Cyber Resillience) e a mitigare i rischi che potrebbero danneggiare i profitti e la reputazione.

Gli attacchi mirati richiedono una difesa mirata e la **Cyber Threat Intelligence** offre la capacità di **difendersi** in modo più proattivo

Cyber Threat Intelligence: nel dettaglio

La **Cyber Threat Intelligence** rappresenta la capacità di Intelligence sviluppata in ambito Cyber Security. Include la raccolta e l'analisi di informazioni al fine di caratterizzare possibili minacce cyber dal punto di vista tecnico, in relazione a contesti operativi specifici.

Il servizio di Cyber Threat Intelligence di Swascan ha lo scopo di individuare le eventuali informazioni pubbliche disponibili a livello **OSINT** e **CLOSINT**, relative ad un determinato target.

Con il termine **OSINT**, acronimo di Open Source Intelligence, si fa riferimento al processo di **raccolta d'informazioni attraverso la consultazione di fonti di pubblico dominio, definite anche "fonti aperte".**

Fare **OSINT** significa descrivere l'informazione disponibile e aperta al pubblico, attraverso un processo di ricerca, selezione, vaglio e reporting, verso uno specifico destinatario al fine di soddisfare una necessità informativa.

La fase più importante del processo di **OSINT** è quella di **"vagliare" le fonti rilevanti ed affidabili. Questo viene fatto partendo da diverse tipologie di fonti di pubblico dominio.**

L'OSINT quindi si distingue dalla banale ricerca d'informazioni perché applica un processo di gestione delle informazioni con lo scopo di creare una specifica conoscenza in un determinato ambito/contesto.

Con il termine **CLOSINT** si fa invece riferimento alla Close Source Intelligence, **cioè al processo di raccolta d'informazioni attraverso consultazione di "fonti chiuse", non accessibili al pubblico o aree "riservate"**

Cyber Threat Intelligence: la portata dell'analisi

L'attività di Cyber Threat Intelligence viene effettuata attraverso un processo di ricerca, individuazione e selezione delle informazioni disponibili pubblicamente con OSINT/CLOSINT a livello di:

- **Target**
- **Asset Digitali**
- **IP**

Email e informazioni relative ai dipendenti di una azienda

Lo scopo? **L'obiettivo è quello di fornire una "actionable intelligence"**, ovvero un'informazione analizzata, contestualizzata, tempestiva, accurata, rilevante e predittiva. Il fine è di determinare l'eventuale esposizione ai rischi della Cyber Security.

Cyber Threat Intelligence: il perimetro

Il perimetro della Cyber Threat Intelligence di Swascan è relativo a:

- Advanced Intelligence: Include eCrime Intelligence e 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 Defense.
  - ....
- Compromised Credential;
- Honeypot Intelligence;
- Financial Fraud Intelligence.

Il servizio di Cyber Threat Intelligence (CTI) permette di cercare, monitorare e analizzare i soggetti di interesse (SOI) in diverse fonti, tra cui:

- DarkWeb communities e marketplaces (TOR-based);
- Underground communities e marketplaces (Internet-based);
- Social media networks, come ad esempio Facebook, Twitter, Linkedin, etc.;
- Messaggistica istantanea, come ad esempio Viber, Telegram, QQ, WeChat, etc.;
- Internet Relay Chat (IRC);
- Integrated Intelligence Repositories (IOCs, TTPs, Security Incidents).

Cyber Threat Intelligence: La fase di analisi

L'attività prevede la raccolta e l'analisi delle informazioni relative ad una serie di macro aree critiche.

Data Breach

Il primo bacino di dati presi in considerazione arriva dai Data Breach, sempre più onnipresenti anche nella cronaca di tutti i giorni.

Vengono analizzati i dati grezzi di: esfiltrazioni che hanno avuto **in oggetto, il diretto interessato e delle terze parti.** Sono naturalmente comprese anche le email compromesse.

A seconda dei casi è possibile fornire:

- **Password utilizzata**
- **Hash della password**
- **Record privo di password, ma del quale vi è traccia nel Deep e nel Dark Web**

Le statistiche ci insegnano che, **una percentuale variabile tra il 60% e l'80% degli utenti, utilizza la stessa password** – o varianti facilmente indovinabili della stessa – sul sistema aziendale (autenticazione Active Directory, Casella e-mail, accesso VPN, accesso Web Remoto, Intranet, etc).

Il rischio è che **un agente esterno (Criminal Hacker)** acquisisca le credenziali compromesse e tenti di accedere in maniera non autorizzata agli asset digitali dell'azienda.

Un secondo scenario è invece relativo ai **Social Network,** ovvero alle credenziali compromesse di dipendenti e collaboratori dell'azienda su piattaforme come Linkedin, Facebook, Twitter, etc… In questo contesto, i Criminal Hacker possono accedere ai Social Network interessati come un dipendente o collaboratore dell'azienda. Così spacciandosi per quella data persona inviano malware ad altri colleghi, dipendenti o collaboratori dell'azienda target.

Lo scopo è quello di perpetrare attacchi mirati verso gli asset digitali e le comunicazioni – **email e/o Social Network –** dell'azienda.

Network Hygiene

Con" Network Hygiene" si intende la presenza di attività malevole o sospette all'interno del perimetro digitale del Cliente. In funzione del tipo di evidenza riscontrata, la keyword è associabile alla "IP Reputation", vale a dire alla reputazione di determinati indirizzi IP noti a livello mondiale, alle diverse comunità di cyber security ed aziende di antivirus. Questo per aver svolto attività illegali o per facilitare indirettamente dette attività (a causa di errori di configurazione e/o implementazione) con tutte le conseguenze legali (civili e penali) del caso.

In funzione delle diverse lacune di Network Hygiene, le conseguenze possono essere molteplici:

- Abuso di form web per richiesta informazioni, con conseguente utilizzo fraudolento dei sistemi del Cliente per l'invio massivo di "email spam";
- Utilizzo dei sistemi mal configurati per redirect di DNS ed intercettazione di tutto il traffico dati;
- Abuso dei sistemi mal configurati per "attacchi ponte" (launchpad), con conseguenti responsabilità di tipo civile e, soprattutto, penale;

DarkWeb

Il **DarkWeb** storicamente era uno dei luoghi più nascosti della rete, dove soltanto i pionieri del Criminal Hacking underground si avventuravano. Oggi, mimando il successo del retail online, il **Darkweb si è dotato di una delle chiavi per il successo della sua controparte legale, le garanzie.** Questi eCommerce operano su piattaforme che permettono di recensire i "prodotti", lasciare una valutazione e ottenere garanzie di acquisto. Il tutto poi è incorniciato da un'interfaccia intuitiva e responsive facilmente navigabile.

Qui la fanno da padrone le cripto valute grazie alle loro caratteristiche che permettono grande anonimato e scarsa tracciabilità.

Tra la merce al primo posto per numero di inserzioni troviamo innumerevoli hacking tools, **ma anche pacchetti di dati sensibili illegalmente ottenuti.**

Per questo motivo l'analisi delle istanze sul Dark Web è fondamentale. Il tool rintraccia i cyber criminali, su forum del cyber crime, che hanno parlato dell'azienda (domini, indirizzi IP, brand o nomi di Executives).

La gravità e l'impatto vanno valutati in funzione di cosa è emerso dall'analisi e presa dei dati sul DarkWeb.

Botnet Activity

Per botnet si intende una collezione di dispositivi connessi alla Rete compromessi da un threat actor.

Questi agiscono come un moltiplicatore di forza per tutti coloro (dal singolo fino al gruppo organizzato di criminal hacker) che intendono sferrare cyber attacchi per violare dei sistemi o causare disservizi.

Il loro utilizzo più frequente è negli attacchi DDoS (Distributed Denial of Service). Qui mettono a frutto la potenza computazionale complessiva delle macchine infette. Il fine è di inviare enormi volumi di spam, sottrarre credenziali su ampia scala e per spiare persone e organizzazioni.

I criminal hacker costruiscono le loro reti di bot infettando dispositivi connessi alla rete attraverso un malware e li controllano utilizzando un server di C&C (Command and Control).

Ciò che rende ancora più pericoloso questo metodo di attacco è che una volta compromesso un singolo device, tutti i dispositivi presenti sulla stessa Rete sono esposti al rischio d'infezione.

Un attacco **botnet** ben congeniato può sicuramente risultare devastante. Basti ricordare il tristemente noto Mirai che, nel 2016, aveva colpito e di fatto "spento" colossi come CNN e Netflix. In quel caso Mirai si era appoggiato a numerosissimi dispositivi IoT, in particolare le telecamere di sicurezza, ma non è escluso che possa utilizzare asset aziendali ben più comuni.

Proprio quest'ultimo aspetto è uno dei più grandi fattori per l'incremento nell'utilizzo di queste tecniche. Permette, infatti, all'aggressore di utilizzare l'hardware della vittima e la sua elettricità per estrarre criptovalute, come Bitcoin o Ethereum.

Come se non bastasse il "bot hardener" (il gestore della botnet) può utilizzare la sua rete botnet per istruirla. Questo per rubare le credenziali (e-banking, Intranet aziendale, Responsabilità legali civili e penali, furto di informazioni, spionaggio industriale, etc.).

Miscellaneuos Risks

In questa categoria di digital risk rientrano diverse sottocategorie: **Ip Reputation** (vedi sotto), **Passive DNS, etc.** Gli impatti variano in funzione del tipo di informazione che è presente all'esterno del perimetro aziendale del Cliente.

IP Reputation

La "reputazione" di un indirizzo IP pubblico è assimilabile alla sua "storia in rete". Questo indica lo storico delle azioni malevole che sono state effettuate, o sono transitate, o hanno avuto come destinazione finale, detto indirizzo IP. Responsabilità legali civili e penali, furto di informazioni, spionaggio industriale, etc

Passive DNS

È un **tipo di attacco di medio-alto livello,** tramite il quale si effettuano cambi di configurazione ai DNS del Cliente. Intercettazione del traffico internet e/o redirect dello stesso.

Brand Names

Indica la presenza di istanze relative ai brand del **Cliente sul Dark Web.** Può essere indicatore di frodi in corso o già commesse.

Executives

Indica la presenza di istanze relative **ai nomi degli Executives, comunicati dal Cliente sul Dark Web** o in altre basi di dati. In funzione del tipo di istanza, può rappresentare differenti tipologie di impatto.

Threat Intelligence

I servizi Swascan di Cyber Threat Intelligence e **Domain Threat Intelligence** sono la risposta alla sicurezza preventiva.

COME DIFENDERSI

Sicurezza Predittiva

1. Identifica le minacce aziendali fuori dal perimetro aziendale operando a livello di Web, Darkweb e Deepweb;
2. Ricerca eventuali minacce emergenti;
3. Effettua attività di Early Warning;
4. Fornisce le evidenze alla Sicurezza Preventiva;
5. Indica le aree di attenzione alla Sicurezza Proattiva.

Sicurezza Preventiva

1. Verifica e misura il Rischio Cyber;
2. Definisce i piani di remediation;
3. Indica il Rischio esposto al Layer di Sicurezza Proattiva;
4. Fornisce le aree di Investigazione alla Sicurezza Predittiva.

Sicurezza Proattiva

1. Identifica le minacce cyber che operano nel perimetro aziendale;
2. Contrasta e blocca gli attacchi informatici;
3. Gestisce i Cyber Inciden;
4. Fornisce le evidenze alla Sicurezza Preventiva;
5. Indica le aree di investigazione alla Sicurezza Predittiva.

Analysis by:

Martina Fonzo
Riccardo Micchetti

Technical Contributors:

Soc Team Swascan

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

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