



Swascan

TINEXTA GROUP

Russian Market: Il mercato nero dei Criminal Hacker che guarda all'Italia

www.swascan.com

info@swascan.com

Sommario

Disclaimer	3
Introduzione: market e informazioni sottratte	4
L'analisi	4
Come funzionano i market	9
Perché questi luoghi rappresentano un pericolo.....	11
Credenziali Italiane in vendita.....	16
Phishing.....	22
Conclusioni.....	24
About us.....	25

Disclaimer

La ricerca svolta da Swascan si è basata su siti contenenti dati e numeriche fonti di ricerche OSINT e CLOSINT tramite Threat Intelligence.

Questa pubblicazione non rappresenta necessariamente lo stato dell'arte – data la natura transitoria delle fonti – e Swascan si riserva la prerogativa di aggiornamento periodico.

Fonti di terze parti sono citate a seconda dei casi. Swascan non è responsabile del contenuto delle fonti esterne, compresi i siti web esterni a cui si fa riferimento in questa pubblicazione.

La presente pubblicazione ha uno scopo puramente informativo. Essa deve essere accessibile gratuitamente.

Né Swascan né alcuna persona che agisca per suo conto è responsabile dell'uso che potrebbe essere fatto delle informazioni contenute in questa pubblicazione.

Introduzione: market e informazioni sottratte

La vendita illegale di informazioni sensibili, come password, dati bancari e carte di credito, è in aumento, con conseguenze potenzialmente devastanti per i privati e le aziende coinvolte.

Le campagne di phishing mirate ai brand nostrani e la presenza di accessi RDP a infrastrutture corporate italiane all'interno del Dark web evidenziano l'ampiezza del problema nel contesto italiano. Questo quanto portato alla luce dagli esperti di Swascan nella loro analisi di Russian Market – un vero e proprio eCommerce del Criminal Hacking – che permette a chiunque di comprare e vendere informazioni sensibili. In particolare, quelle che fanno riferimento ad aziende e persone del nostro territorio.

L'analisi

Tutto quello che è stato rilevato e categorizzato in questo market può essere utilizzato per commettere vari tipi di crimini informatici, come il furto di identità, l'hacking e il phishing, mettendo a rischio la sicurezza finanziaria e personale delle vittime.

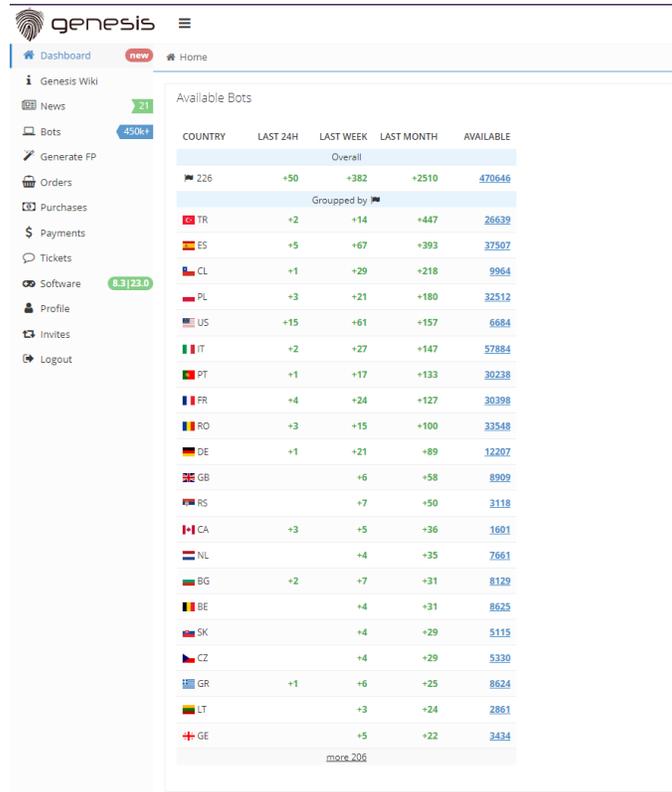
Negli ultimi anni, inoltre, abbiamo assistito a un crescente aumento delle campagne di phishing volte alla cattura di informazioni personali come password e carte di credito o alla distribuzione di malware quali RAT (Remote Access Trojan) o Infostealer.

Questo fenomeno ha suscitato una forte attenzione da parte delle forze dell'ordine, che hanno recentemente collaborato per chiudere due tra le più grandi reti di criminalità informatica, "Breached Forum" e "Genesis Market".

La chiusura di questi forum da parte delle autorità internazionali è un importante passo avanti nella lotta contro il crimine informatico. Ad esempio, Genesis Market è stato chiuso dall’FBI, che ha collaborato con le forze dell’ordine di diversi paesi per individuare e arrestare gli amministratori del forum nell’operazione ribattezzata “Cookie Monster”.

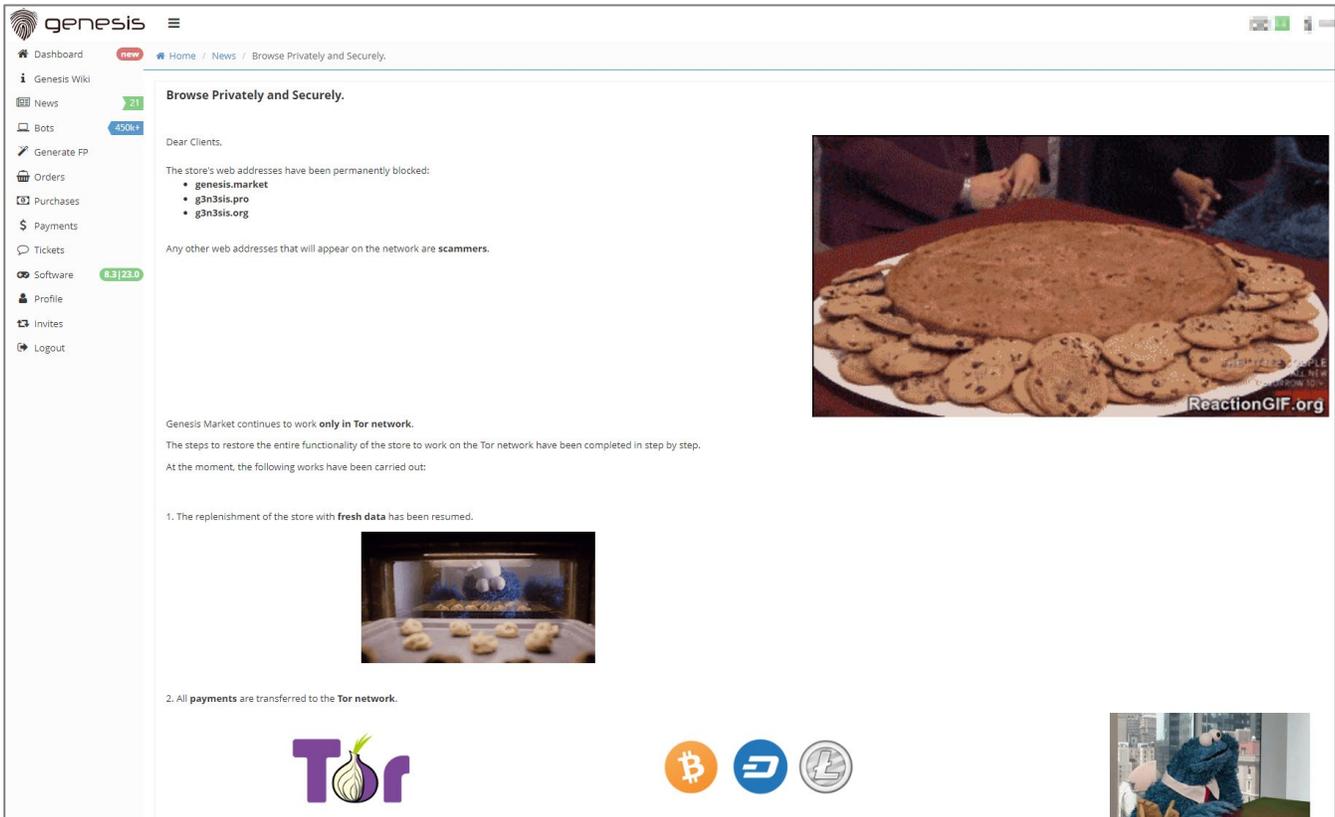


Tuttavia, sembrerebbe che al momento Genesis stia lentamente tornando sul Darkweb, difatti, come mostrato nella screen seguente, si può notare come la mole di dati disponibili sia inferiore rispetto alla norma. Questo potrebbe derivare dal fatto che il sito principale e parte dell’infrastruttura sia stata compromessa dall’operazione Cookie Monster.



COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
226	+50	+382	+2510	470646
Grouped by				
TR	+2	+14	+447	26639
ES	+5	+67	+393	37507
CL	+1	+29	+218	9964
PL	+3	+21	+180	32512
US	+15	+61	+157	5684
IT	+2	+27	+147	57884
PT	+1	+17	+133	30238
FR	+4	+24	+127	30398
RO	+3	+15	+100	33548
DE	+1	+21	+89	12207
GB		+6	+58	8909
RS		+7	+50	3118
CA	+3	+5	+36	1601
NL		+4	+35	7861
BG	+2	+7	+31	8129
BE		+4	+31	8625
SK		+4	+29	5115
CZ		+4	+29	5330
GR	+1	+6	+25	8624
LT		+3	+24	2861
GE	+5	+22		3434
more 206				

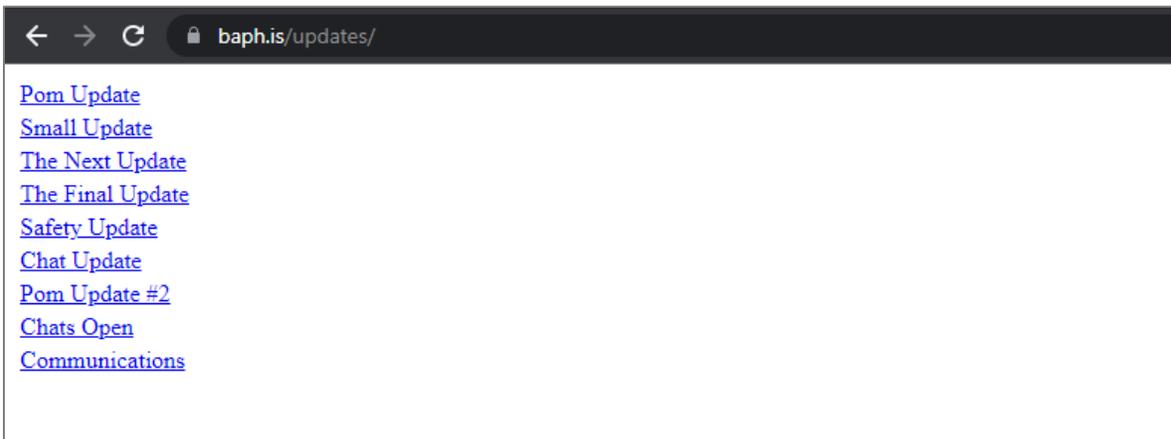
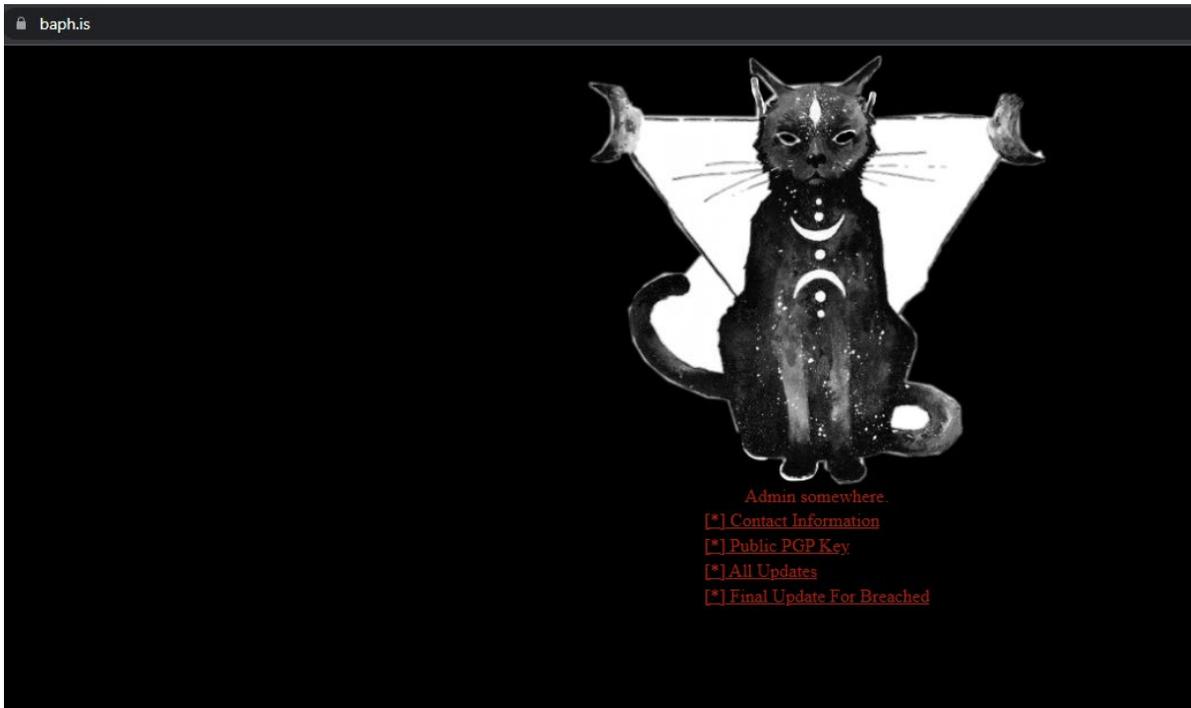
Possiamo inoltre notare nella sezione news come venga specificato che tutti gli altri siti presenti sul deepweb non siano leciti:



The screenshot shows the Genesis Market website interface. The header includes the 'genesis' logo and navigation links for 'Dashboard', 'Home', 'News', and 'Browse Privately and Securely'. A sidebar on the left lists various site features like 'Genesis Wiki', 'News', 'Bots', 'Generate FP', 'Orders', 'Purchases', 'Payments', 'Tickets', 'Software', 'Profile', 'Invites', and 'Logout'. The main content area is titled 'Browse Privately and Securely' and contains a message to clients stating that certain web addresses (genesis.market, g3n3s1s.pro, g3n3s1s.org) are permanently blocked and that other addresses are scammers. It also mentions that the store works only on the Tor network and lists steps for restoration, such as replenishing with fresh data and transferring payments to the Tor network. The page features several images: a large platter of cookies, a tray of dough balls in a bakery, the Tor logo, and icons for Bitcoin, Dash, and Litecoin. A small GIF of a person in a blue hoodie is visible in the bottom right corner.

Breached forum invece, che era uno dei più grandi forum al mondo per la compravendita di informazioni personali, ha visto, a seguito di una collaborazione internazionale tra forze dell'ordine, l'arresto del suo amministratore principale Conor Brian Fitzpatrick aka "Pompompurin" e, in seguito, il forum è stato chiuso prontamente dall'altro Admin "Baphomet" per problemi di sicurezza.

Allo stato attuale, l'unico Admin rimasto, Baphomet, sta pubblicando aggiornamenti sul suo sito personale facendo pensare ad un possibile ritorno del forum:



Come funzionano i market

Ma come funzionano questi forum e perché sono così pericolosi? In primo luogo, questi forum permettono a chiunque di comprare e vendere informazioni personali senza alcuna verifica o controllo. Questo significa che chiunque può acquistare informazioni rubate e usarle per commettere crimini come il furto di identità, l'hacking e il phishing.

In secondo luogo, questi forum sono estremamente difficili da chiudere. I loro amministratori spesso si nascondono dietro anonimi nickname e utilizzano tecnologie come la crittografia per nascondere le loro attività. Questo rende difficile per le autorità internazionali individuare e arrestare gli amministratori di questi forum.

Infine, questi forum sono estremamente redditizi per i loro amministratori. Vendere informazioni personali rubate può generare enormi profitti, e i proprietari di questi forum spesso guadagnano centinaia di migliaia di dollari al mese. Questo significa che hanno un forte incentivo per continuare le loro attività illegali.

Ma basterà la chiusura di questi due forum per lanciare un segnale a tutti quei Threat Actor propensi all'apertura di un nuovo market a scopi di lucro?

La risposta è semplice, questi due forum, seppur estremamente noti nel mondo underground sono soltanto la punta dell'iceberg. Difatti altri forum/market stanno prendendo il controllo della scena, uno fra tutti Russian Market.



Russian Market può essere considerato come un'alternativa al portale (recentemente chiuso) Genesis: il portale non presenta una sezione di Forum (come in Breached, dove avvengono spesso discussioni e scambi di informazione tra i vari utenti), ma si presenta come un vero e proprio store digitale di credenziali estrapolate da botnet, carte di credito, wallet e accessi remoti a computer compromessi. Inoltre, a differenza di Breached e altri forum, le informazioni che vengono vendute non sono postate dagli utenti ma vengono vendute direttamente dai proprietari del market stesso.

Per poter diventare parte del team di vendita, è necessario contattare l'Admin ed essere approvati una volta che le informazioni che si vuole vendere saranno verificate:

How to become member of the team and start selling ?

Simply create account and contact the admin over support page
with us you are able to upload your own bases . all you will need to get approval for it after you upload

Nel market sono inoltre rimborsabili tutti gli accessi acquistati che non sono più validi (fatto eccezione dei dati relativi alle botnet).

SSH Tunnel not work.

All SSH Tunnels checked before sale, recheck config you firewall.
If ssh tunnel invalid also - ask refund.

What time refund RDP ?

Time to refund after purchase is **10 minutes**.

Perché questi luoghi rappresentano un pericolo

I rischi derivanti da questo mercato sono molteplici, è possibile infatti pensare agli accessi RDP/SSH in vendita. Questi potrebbero difatti essere il primo punto di accesso, per Threat Actor più esperti, a reti corporate con il conseguente rischio di un attacco informatico con lo scopo di caricare remotamente un Ransomware.

Mask	Country	State / City	Details	Info	Vendor	Blacklist	Price	Action
		Beijing Beijing	OS: Win2008/7 Proc: - RAM: - GB @: - / - Mbit/s	Admin: No Paypal: - NAT: -	am###img [Diamond]	BL	\$ 4.00	Buy
		California Los Angeles	OS: Win2008/7 Proc: Intel/Amd RAM: 2 GB @: 1 / 1 Mbit/s	Admin: No Paypal: Yes NAT: Yes	JS###ow [platinum]	BL	\$ 7.00	Buy
		Oregon Portland	OS: Windows Proc: - RAM: - GB @: - / - Mbit/s	Admin: - Paypal: - NAT: -	RDP [Diamond]	BL	\$ 10.00	Buy
		Distrito Federal Caracas	OS: Windows Proc: - RAM: - GB @: - / - Mbit/s	Admin: - Paypal: - NAT: -	RDP [Diamond]	BL	\$ 10.00	Buy
		Guangdong Shenzhen	OS: Win2008/7 Proc: - RAM: - GB @: - / - Mbit/s	Admin: No Paypal: - NAT: -	am###img [Diamond]	BL	\$ 4.00	Buy
		Delhi New Delhi	OS: Windows2012/2016/10 Proc: Intel Core E8 Xeon B430 RAM: 16 GB @: 51.37 / 45.81 Mbit/s	Admin: No Paypal: No NAT: No	dst###ok [platinum]	BL	\$ 6.00	Buy
		National Capital Territory of Delhi Delhi	OS: - Proc: - RAM: - GB @: - / - Mbit/s	Admin: - Paypal: - NAT: -	XR###DP silver	BL	\$ 5.00	Buy
		Bangkok Bangkok	OS: Windows2012/2016/10 Proc: Intel Core E8 Xeon B430 RAM: 16 GB @: 51.37 / 45.81 Mbit/s	Admin: No Paypal: No NAT: No	dst###ok [platinum]	BL	\$ 4.00	Buy
		South West Singapore	OS: Win2008/7 Proc: Intel/Amd RAM: 2 GB @: 1 / 1 Mbit/s	Admin: No Paypal: Yes NAT: Yes	JS###ow [platinum]	BL	\$ 4.00	Buy
		South West Singapore	OS: Win2008/7 Proc: - RAM: - GB @: - / - Mbit/s	Admin: No Paypal: - NAT: -	am###img [Diamond]	BL	\$ 6.00	Buy

Nella sezione relativa agli accessi RDP sono presenti un totale di circa 15'200 accessi a potenziali pc/server compromessi. Prendendo in considerazione l'Italia, ad esempio, sono presenti 74 accessi a postazioni di lavoro mentre i due paesi con più accessi in vendita risultano Cina e Stati Uniti con rispettivamente 2'809 e 2'746 accessi RDP disponibili.

Le credenziali estrapolate dalle botnet, invece, possono essere utilizzate per diversi obiettivi: uno fra tutti, il furto di identità. Il rischio che un attaccante possa entrare ad esempio nei portali personali di un utente ed impersonarlo è molto alto. Oltre al rischio di furto di account social si aggiunge tutta una serie di rischi legati alle informazioni presenti che potrebbero, nei casi peggiori, portare al furto vero e proprio di identità digitale.

Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price	Action
Raccoon	Zimbabwe ISP: Freeport Investments	...	-	-	archive.zip	2023.05.05 0.29Mb	Mo###yf [Diamond]	\$ 10.00	Buy
Raccoon	Zimbabwe ISP: Angola (Eraso) Peer	...	-	-	archive.zip	2023.05.05 0.39Mb	Mo###yf [Diamond]	\$ 10.00	Buy
Raccoon	Botswana ISP: RAIN GROUP HOLDINGS (PTY) LTD	...	-	-	archive.zip	2023.05.05 0.25Mb	Mo###yf [Diamond]	\$ 10.00	Buy
Raccoon	Zimbabwe ISP: Zambia Telecommunications Company Ltd aka ZANTEL	...	-	-	archive.zip	2023.05.05 0.16Mb	Mo###yf [Diamond]	\$ 10.00	Buy
Raccoon	Zimbabwe ISP: Airtel Zambia	...	-	-	archive.zip	2023.05.05 0.25Mb	Mo###yf [Diamond]	\$ 10.00	Buy
Raccoon	Botswana ISP: RAIN GROUP HOLDINGS (PTY) LTD	...	-	-	archive.zip	2023.05.05 0.23Mb	Mo###yf [Diamond]	\$ 10.00	Buy
Raccoon	Zimbabwe ISP: MTN	...	-	-	archive.zip	2023.05.04 0.13Mb	Mo###yf [Diamond]	\$ 10.00	Buy

Inoltre, la possibilità di poter acquistare questi dati puntualmente alle proprie esigenze aumenta il rischio di attacco cyber contro aziende.

È difatti possibile acquistare dati che rispettino i propri parametri di ricerca:



The image shows a search interface for a credential marketplace. It features several filter categories: Stealer (All), System (All), Country (All), State (All), City (All), Zip (empty), ISP (ADSL Maroc te), Outlook (@domain.com), and Per page (10). There are also search buttons for Mask, Cookie, Email, and Links. A search result for 'accounts.google.com' is displayed, with a checkbox for 'ONLY WITH COOKIES'. A price slider is set between 0 \$ and 10 \$, and a 'Search' button is visible at the bottom right.

Un attaccante potrebbe quindi cercare degli accessi per un determinato portale o per un determinato dominio così da poter poi proseguire con un attacco informatico o con la vendita delle credenziali trovate ad altri Threat Actor (i venditori di queste credenziali “corporate” sono gergalmente definiti “Access Broker”).

Inoltre, il numero di credenziali estrapolate da botnet in vendita è così alto da lasciare una grande scelta ad eventuali acquirenti: basti pensare che su un totale di quasi 7 milioni di botnet circa 122’600 provengono dall’Italia mentre i paesi maggiormente impattati risultano India e Brasile con rispettivamente 802’513 e 596’785 botnet disponibili.

Ultimo, ma non per importanza, è il rischio relativo ai wallet e alle carte di credito in quanto potrebbero facilmente rovinare la situazione finanziaria di un utente.

Type	Bin	Bank	Class	Level	EXP	Database	Country	State	City	Zip	SSN	DOB	Vendor	Price	Action
VISA		BANK	DEBIT	PREPAID		May-us-good (REFUND 5 min)	USA	NY	FT WALTON BCH				fe####un (platinum)	\$ 10.00	Buy
VISA		BANK	CREDIT	CLASSIC		May-us-good (REFUND 5 min)	USA	MS	SPRING				fe####un (platinum)	\$ 10.00	Buy
VISA		BANK	DEBIT	CLASSIC		May-us-good (REFUND 5 min)	USA	MO	PORT NECHES				fe####un (platinum)	\$ 10.00	Buy
VISA		BANK	CREDIT	CLASSIC		May-us-good (REFUND 5 min)	USA	MA	Spearfish				fe####un (platinum)	\$ 10.00	Buy
VISA		BANK	DEBIT	PREPAID		May-us-good (REFUND 5 min)	USA	WA	Lafayette				fe####un (platinum)	\$ 10.00	Buy
MasterCard		BANK	DEBIT	STANDARD		May-us-good (REFUND 5 min)	USA	MA	LAWTON				fe####un (platinum)	\$ 10.00	Buy
VISA		BANK	CREDIT	CLASSIC		May-us-good (REFUND 5 min)	USA	FL	BRANDON				fe####un (platinum)	\$ 10.00	Buy
MasterCard		BANK	CREDIT			May-us-good (REFUND 5 min)	USA	MO	Lester				fe####un (platinum)	\$ 10.00	Buy
VISA		BANK	CREDIT	CLASSIC		May-us-good (REFUND 5 min)	USA	MI	ARLINGTON				fe####un (platinum)	\$ 10.00	Buy
VISA		BANK	DEBIT	CLASSIC		May-us-good (REFUND 5 min)	USA	CA	FLOWER MOUND				fe####un (platinum)	\$ 10.00	Buy

first name;last name;address;city;state;zip;ssn;dob;dl;login_email,url_site;score;password

Name	City	State	ZIP	URL	Score	Vendor	Qty.	Price	Action
	Haslet	TX		www.nerdwallet.com With DL_CS,BG pdf Files	752	ac####92 (platinum)	1	\$ 13.00	Buy
	Potomac	MD		www.nerdwallet.com With DL_CS,BG pdf Files	830	ac####92 (platinum)	1	\$ 20.00	Buy
	Upper Marlboro	MD		www.nerdwallet.com With DL_CS,BG pdf Files	807	ac####92 (platinum)	1	\$ 20.00	Buy
	Carmichael	CA		www.wallethub.com DL	646	Yahooze bronze	1	\$ 10.00	Buy
	Royal Palm Beach	FL		www.wallethub.com DL	631	Yahooze bronze	1	\$ 10.00	Buy
	Downey	CA		www.wallethub.com DL	829	Yahooze bronze	1	\$ 10.00	Buy
	Sacramento	CA		www.wallethub.com NO DL	755	Yahooze bronze	1	\$ 10.00	Buy
	Sunrise	FL		www.wallethub.com DL	698	Yahooze bronze	1	\$ 10.00	Buy
	Carmichael	CA		www.wallethub.com DL BIG PDF	644	Yahooze bronze	1	\$ 12.00	Buy
	Redding	CA		www.wallethub.com DL	812	Yahooze bronze	1	\$ 12.00	Buy

Anche in questo caso i numeri sono imponenti: sono infatti disponibili all'acquisto un totale di circa 393'000 carte di credito di cui 2'591 italiane. I paesi maggiormente impattati risultano Stati Uniti e Francia con rispettivamente 316'756 e 12'478 carte disponibili.

Russian Market inoltre fornisce ai propri utenti una serie di tool utili, ad esempio, alla riformattazione di cookie esfiltrati da botnet e checker di carte di credito:

NETSCAPE TO JSON COOKIE CONVERTER

Example:

```
.srvstackadpt.com TRUE / 0 13356116559876796 sa-user-id s%3AD-84654764-bf93-4de8-7a35-40e32f639386.X5VbT00%2FbKxewRiKwzV505GaUpnFkGdo%2BiqSKNo
.srvstackadpt.com TRUE / 0 13356116559876894 sa-user-id v2 s%3AD-84654764-bf93-4de8-7a35-40e32f639386%24p%7MRf%2Fb3p4De14oChpbRSh%2Bku9L7LnBw5GjEAE
.thecustomdroid.com TRUE / 1 13229972727034036 __cfduid dca95b1c924aa1fccb69c9f2acc0c41051553963125
.sharethis.com TRUE / 0 13230059491602241 __stid 2GADG1yfmEAAAASUkkAw==
.jzofo.com TRUE / 0 13229973097031314 __cfduid df1cc726d9612cfac12491931f13e02c1553963495
.justanswer.com TRUE / 0 13229973097031782 __cfduid d84789d8c2e811f6e550bdc0800852e1553963495
.updato.com TRUE / 0 13261509108000000 __gacls ID=6b7c44f1f608e4607-1553963508S-ALNI_MZ10ocKiqJnimEuaKf-Zs2RevR9w
.updato.com TRUE / 0 132232305919000000 __qca PO-1439793344-1553963510656
.bidrio TRUE / 0 13261494719648636 bito AAatUE65PzQAABdxK5wOca
.pipplo.com TRUE / 0 13229973122862938 did 54F0R9Lkg_TTgLn
```

```
.bit.ly TRUE / 0 13214340525584899 __bit j3i8l-6783c404d3ae2cb87a-00m
.mediafire.com TRUE / 0 13230502201666420 __cfduid d6737159057711f707c6dbc6480df45c1554492600
.mediafire.com TRUE / 0 13259446203666516 ukey 9ufh9bba8q9fqlw1itegbzqzd49ez5y9
.technofizi.net TRUE / 1 13230549355271281 __cfduid d28e4beaeaa80db74280585bd217b14011554539752...
```

[Convert Now!](#)

BIN CHECKER

Example:

```
5457497
5457497921800000
5457497921800000|03|15|416
5457497921800000|03|15|416|Maria De La Torre|Canada|ON|Brampton|L6Z0C7|5 Copperfield
```

FREE

```
545749
```

[Check Now](#)

Credenziali Italiane in vendita

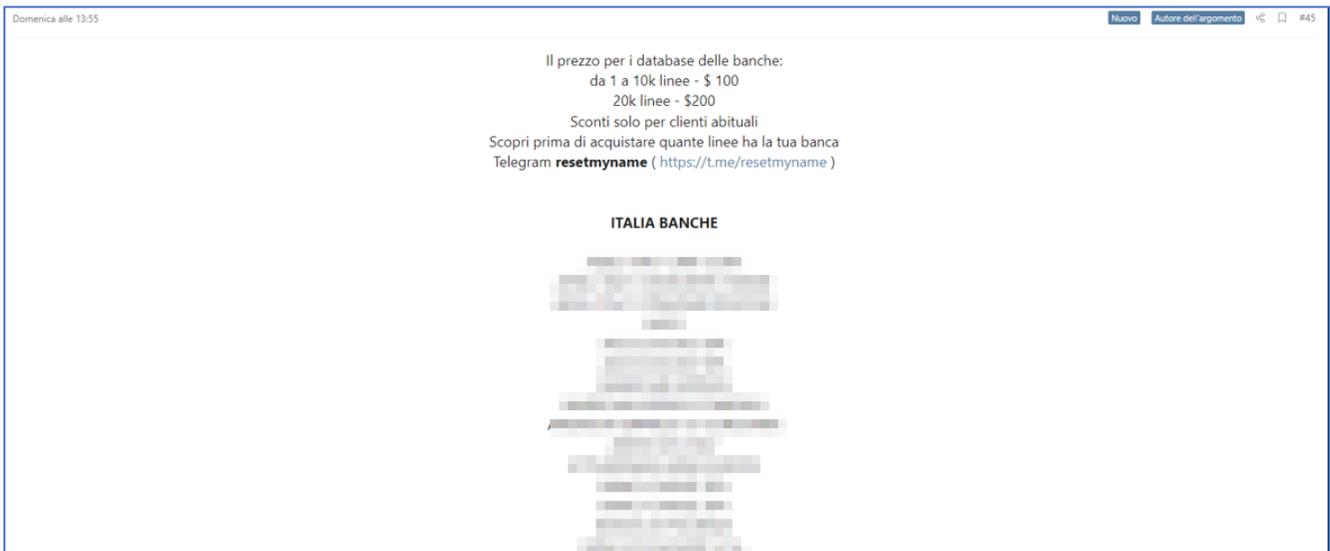
Negli ultimi anni, il fenomeno della vendita di credenziali personali e aziendali sul deep e darkweb, come abbiamo notato negli esempi sopra riportati, ha assunto proporzioni preoccupanti anche in Italia. Sono infatti sempre di più le persone e le aziende che si trovano a subire attacchi informatici, che portano alla perdita di dati sensibili e all'acquisto illecito di informazioni personali. Oltre a password e informazioni personali, sono sempre più diffusi anche i documenti, come carte d'identità e passaporti, che vengono venduti illecitamente sul web. Questi dati, una volta acquisiti, possono essere utilizzati per scopi illeciti come il furto di identità e la creazione di false identità, o ancora per accedere a informazioni riservate o effettuare transazioni finanziarie fraudolente.

Tra le informazioni più ricercate e vendute ci sono anche i dati relativi alle carte di credito, che vengono acquistate a prezzi molto bassi rispetto al loro valore reale. Le conseguenze dell'acquisto di queste informazioni possono essere devastanti, con il rischio di subire prelievi non autorizzati o di effettuare acquisti online senza il consenso del titolare della carta.

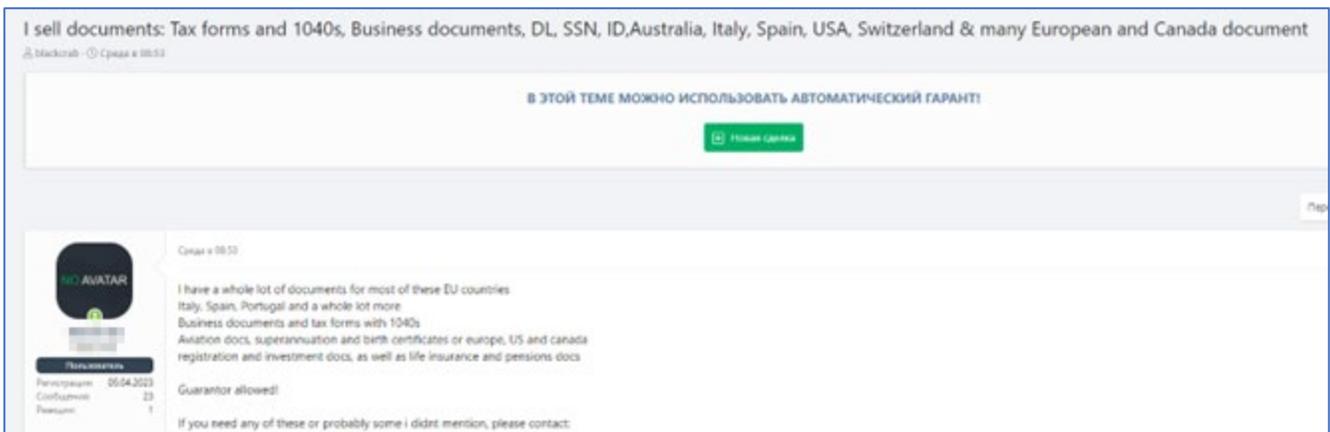
Le credenziali vendute riguardano principalmente account di posta elettronica, password di accesso a social network, conti bancari e carte di credito. Ma non solo: sempre più spesso vengono messe in vendita anche informazioni aziendali riservate come, accessi RDP alla loro infrastruttura, contratti di lavoro e dati sensibili sui dipendenti e fornitori.

Di seguito alcuni esempi di dati in vendita su diversi forum underground.

Nell'esempio seguente possiamo notare come sia in vendita un database di contatti telefonici di clienti di banche italiane:



Di seguito invece un esempio di documenti aziendali in vendita provenienti da diversi paesi:



Qui di seguito invece dei template per documenti falsi in vendita:

More than 1000 templates available from different countries

Available Templates

- Bank statements
- Identity Cards
- Driver Licenses
- Drop-Off receipts
- Utility Bills
- Passports
- much more...

Available Countries - USA, [Italy](#), France, Australia, Canada, Turkey, Poland, Germany, Greece and more...

Required fonts are included for all documents

All documents are fully editable with Photoshop.

Pricing

- Utility Bill - \$15
- Identity Card - \$20
- Bank Statement - \$15
- Drop-Off Receipt - \$20
- Drivers License - \$25
- Passport - \$20

Qui invece alcuni esempi di botnet e dati di italiani in vendita:

Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price	Action
Redline	Piedmont ISP: INTERBUSINESS	[Redacted]	-	-	archive.zip	2023.05.03 0.26Mb	Monsterlog [Diamond]	\$ 10.00	Buy
Redline	Lombardy ISP: LINKEM-NETWORK	[Redacted]	-	-	archive.zip	2023.05.03 0.20Mb	Monsterlog [Diamond]	\$ 10.00	Buy
Redline	Lombardy ISP: INTERBUSINESS	[Redacted]	-	-	archive.zip	2023.05.02 0.27Mb	Monsterlog [Diamond]	\$ 10.00	Buy
Redline	Emilia-Romagna ISP: INTERBUSINESS	[Redacted]	-	-	archive.zip	2023.05.02 0.15Mb	Monsterlog [Diamond]	\$ 10.00	Buy
Redline	Lombardy ISP: INTERBUSINESS	[Redacted]	-	-	archive.zip	2023.05.03 3.13Mb	Monsterlog [Diamond]	\$ 10.00	Buy
Redline	Lazio ISP: LINKEM-NETWORK	[Redacted]	-	-	archive.zip	2023.05.03 0.12Mb	Monsterlog [Diamond]	\$ 10.00	Buy

ITALY 35 MILLION DATA
 5 toney · 29.03.2023

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТИ!

[Новая сделка](#)

29.03.2023

NO AVATAR

Пользователь

Регистрация: 31.07.2021
 Сообщения: 32
 Реакции: 7

order	orderEmail	shpFirstName	shpLastName	shpPhone	shpStreet	shpCity	shpState	shpZip	orderDate	shippingMethod	trackNumber
1	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
2	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
3	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
4	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
5	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
6	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
7	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
8	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
9	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
10	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
11	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
12	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
13	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
14	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
15	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
16	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
17	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
18	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
19	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
20	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
21	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
22	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
23	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
24	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
25	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
26	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
27	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
28	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
29	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
30	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
31	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
32	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
33	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
34	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
35	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

07.02.2023

825k Consumatori Italia
[Data di nascita, IP, Sesso]
PM o Telegram me https://t.me/Data_nim0ri

First_Name,Last_Name,Email,Phone,DOB,Gender,Zip_Code,IP

Fransco							
Linda,C							
Giovan							
Anselm							
Alessa							
Rita,Rit							
Robert							
Rossan							
reby71							
Silvia,R							
Franco							

CSV leak

articolo

17.04.2023

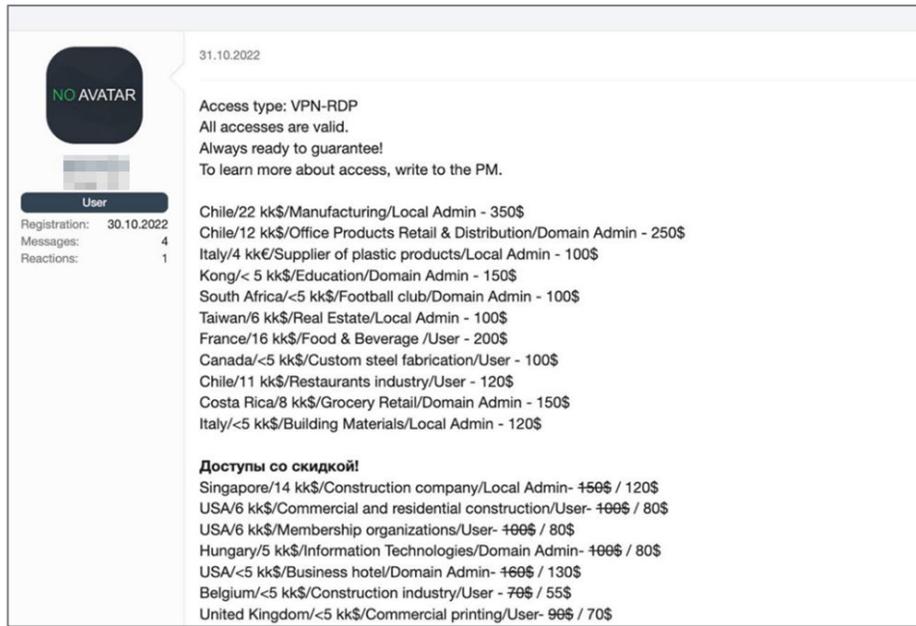
the first technical information portal for Italian construction. The most authoritative and complete free source of news, technical regulations, building products and materials, procurement...

sample:

1115	M	Gabriele					
1119	M	Arch	Cesa				
1121	F	Jessica	Pa				
1122	M	igiromini					
1124	M	Sig	Riccar				
1125	M	Antonio					
1127	F	Arch	Floria				

Registración: 27.02.2023
 Сообщения: 14
 Реакции: 15

In fine, un esempio di accessi VPN-RDP corporate in vendita da un Access Broker:



31.10.2022

Access type: VPN-RDP
All accesses are valid.
Always ready to guarantee!
To learn more about access, write to the PM.

User
Registration: 30.10.2022
Messages: 4
Reactions: 1

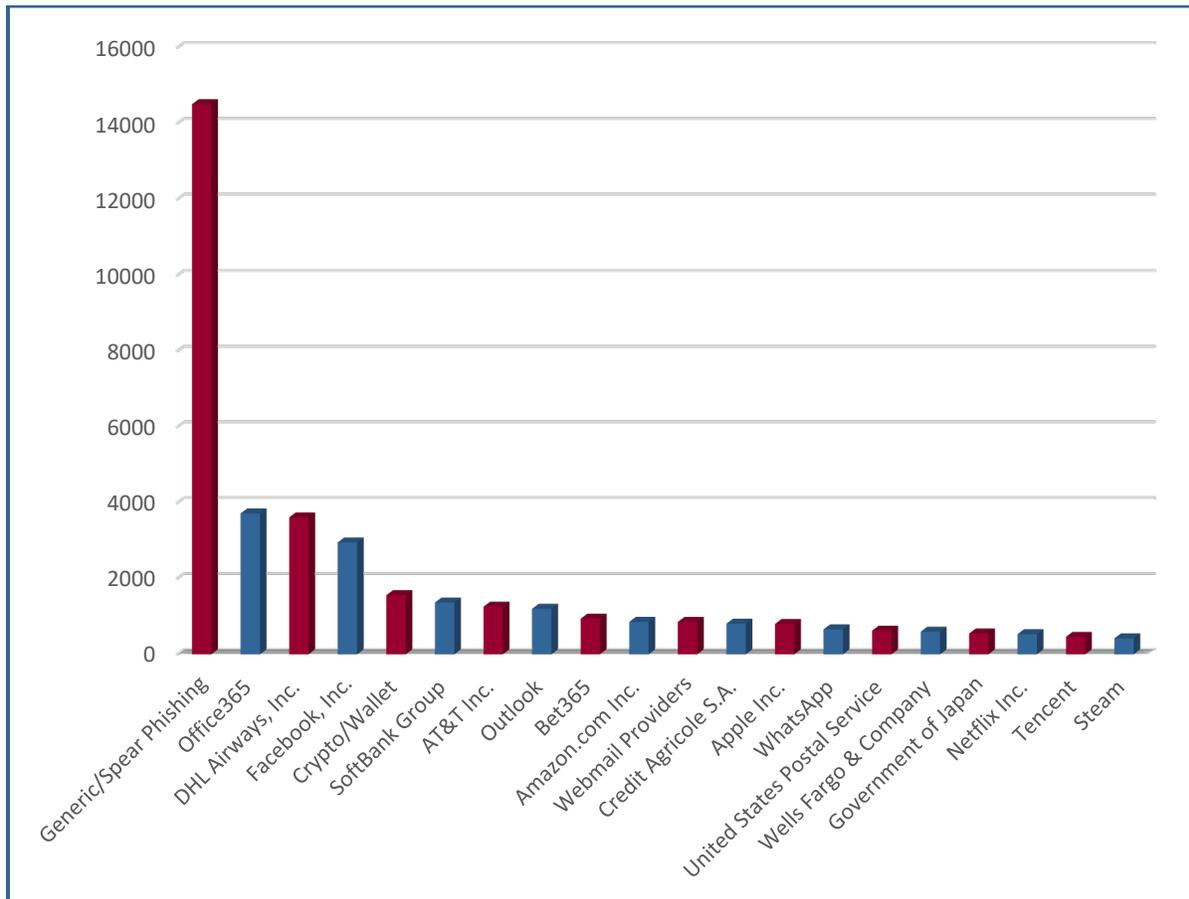
Chile/22 kk\$/Manufacturing/Local Admin - 350\$
Chile/12 kk\$/Office Products Retail & Distribution/Domain Admin - 250\$
Italy/4 kk\$/Supplier of plastic products/Local Admin - 100\$
Kong/< 5 kk\$/Education/Domain Admin - 150\$
South Africa/<5 kk\$/Football club/Domain Admin - 100\$
Taiwan/6 kk\$/Real Estate/Local Admin - 100\$
France/16 kk\$/Food & Beverage /User - 200\$
Canada/<5 kk\$/Custom steel fabrication/User - 100\$
Chile/11 kk\$/Restaurants industry/User - 120\$
Costa Rica/8 kk\$/Grocery Retail/Domain Admin - 150\$
Italy/<5 kk\$/Building Materials/Local Admin - 120\$

Доступы со скидкой!
Singapore/14 kk\$/Construction company/Local Admin- ~~150\$~~ / 120\$
USA/6 kk\$/Commercial and residential construction/User- ~~100\$~~ / 80\$
USA/6 kk\$/Membership organizations/User- ~~100\$~~ / 80\$
Hungary/5 kk\$/Information Technologies/Domain Admin- ~~100\$~~ / 80\$
USA/<5 kk\$/Business hotel/Domain Admin- ~~100\$~~ / 130\$
Belgium/<5 kk\$/Construction industry/User - ~~70\$~~ / 55\$
United Kingdom/<5 kk\$/Commercial printing/User- ~~90\$~~ / 70\$

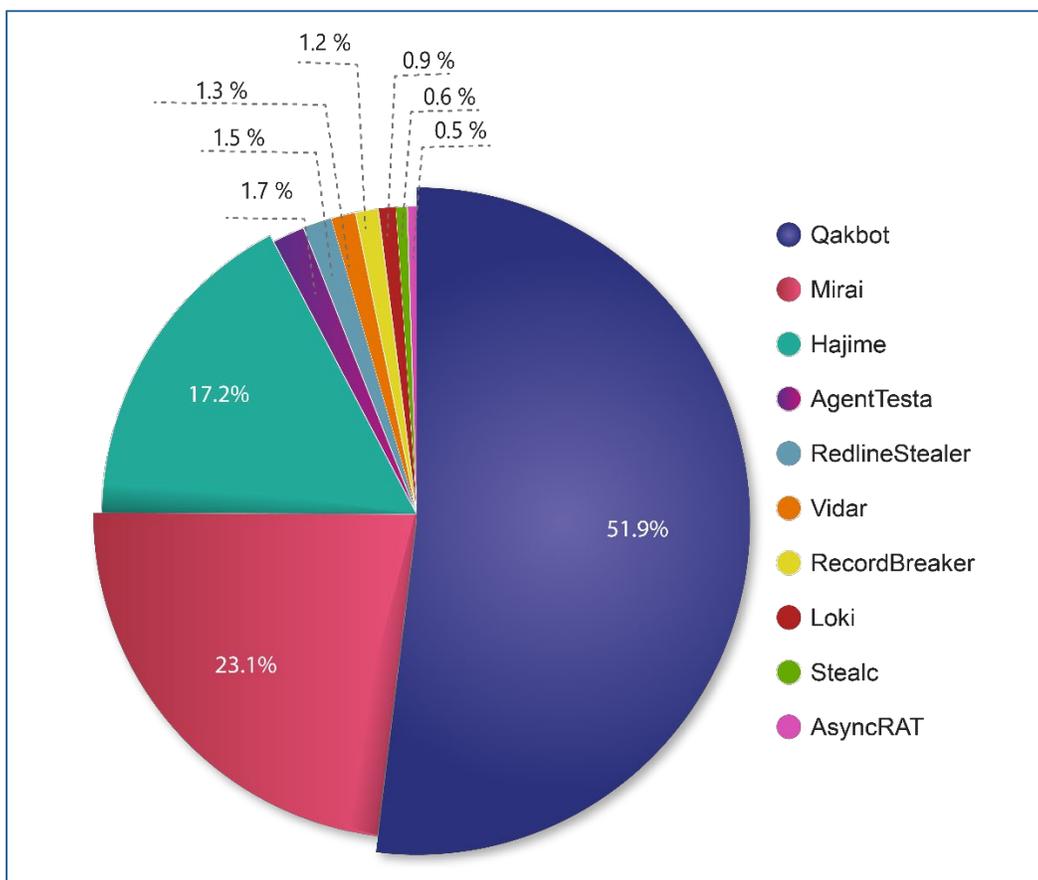
Ma da dove arrivano tutte queste credenziali?

Phishing

Sicuramente uno dei metodi più utilizzati dagli attaccanti è quello del phishing. Difatti soltanto nel mese di aprile sono stati registrate un totale di circa 50'950 campagne di phishing volte alla cattura di credenziali e carte di credito. Le campagne più diffuse risultano essere le seguenti:



Per quanto concerne invece la distribuzione di malware, che possono avvenire sia tramite un attacco phishing sia tramite il download di software da fonti non autorevoli abbiamo quanto segue:



Conclusioni

Il mondo dei forum che vendono le credenziali è un ambiente pericoloso e illegale. La chiusura di Breached forum e Genesis Market è un segnale importante di come le autorità internazionali stiano prendendo sul serio la lotta contro questi criminali informatici ma, nonostante gli sforzi, la minaccia è più che mai attiva.

Per proteggere le proprie informazioni personali, è importante adottare misure di sicurezza informatica adeguate, come l'utilizzo di password complesse, l'utilizzo di autenticazione a due fattori, evitare di condividere informazioni personali su siti web non sicuri. Inoltre, è consigliabile monitorare regolarmente i propri dispositivi tramite l'utilizzo di sistemi A/V o EDR in grado di poter bloccare prontamente minacce note e non.

About us

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 **Cyber Competence Center** premiato con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo.

Da ottobre 2020, **Swascan** è parte integrante del Gruppo **Tinexta S.P.A.** azienda quotata sul segmento STAR di Borsa Italiana

Swascan è diventata 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.

Analysis by:

Martina Fonzo
Riccardo Michetti

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