Swascan
TINEXTA GROUP

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

www.swascan.com
info@swascan.com

Sommario

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

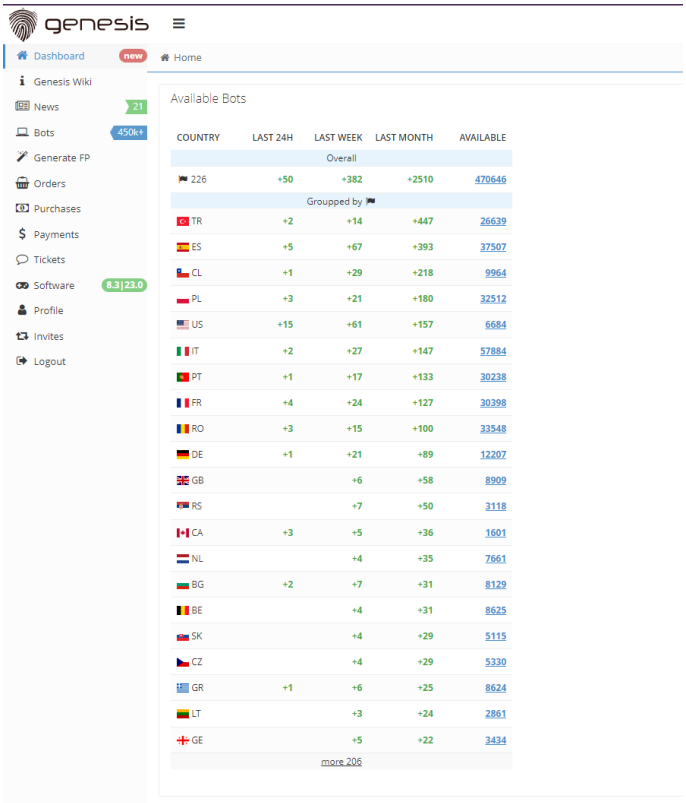
Tutto quello che è stato rilevato e categorizzato in questo market può essere utilizzate per commettere vari tipi di crimini informatici, come il furto di identità, l'hacking e il phishing, mettendo a rischio la sicurezza finanziaria e personale delle vittime.

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.

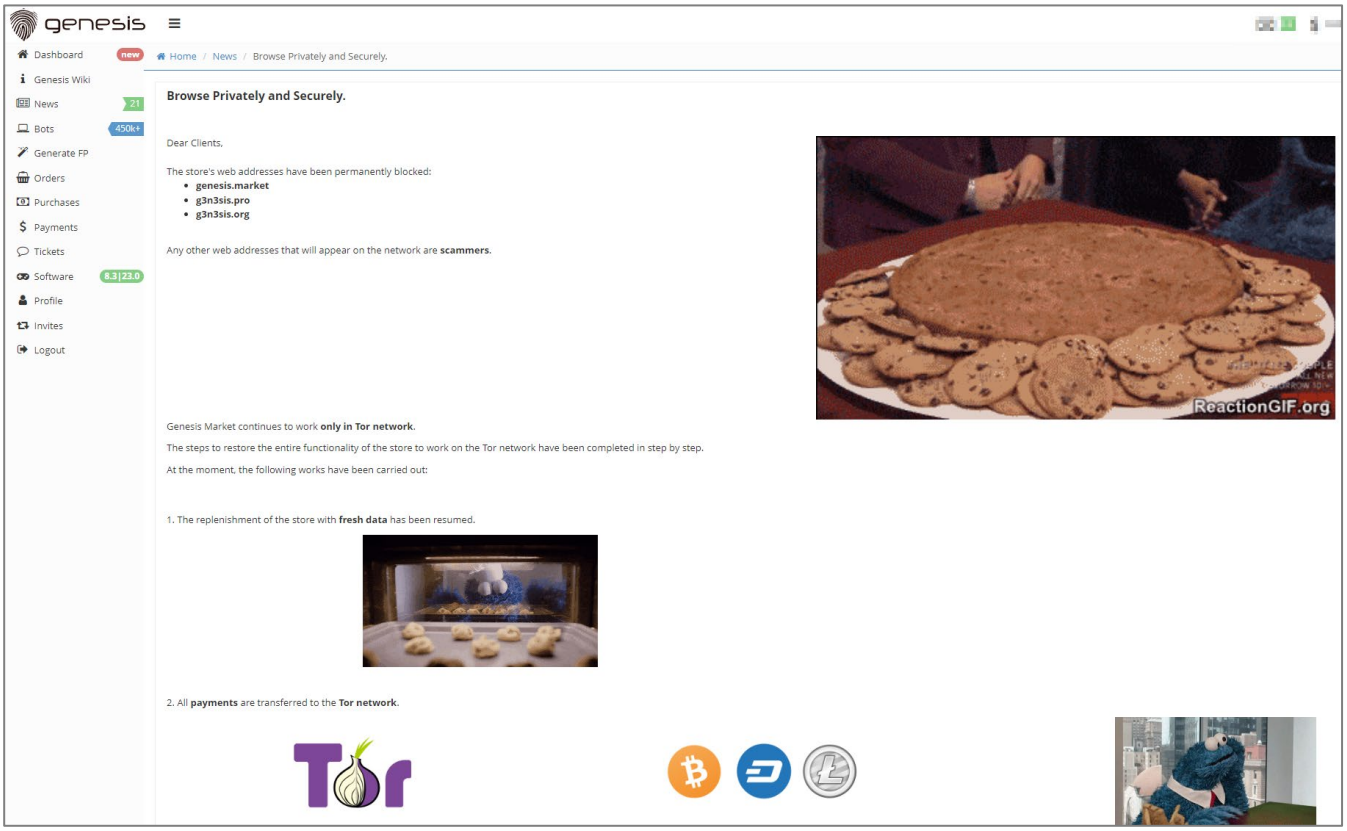
Questo fenomeno ha suscitato una forte attenzione da parte delle forze dell'ordine, che hanno recentemente collaborato per chiudere due tra le più grandi reti di criminalità informatica, "Breached Forum" e "Genesis Market".

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.

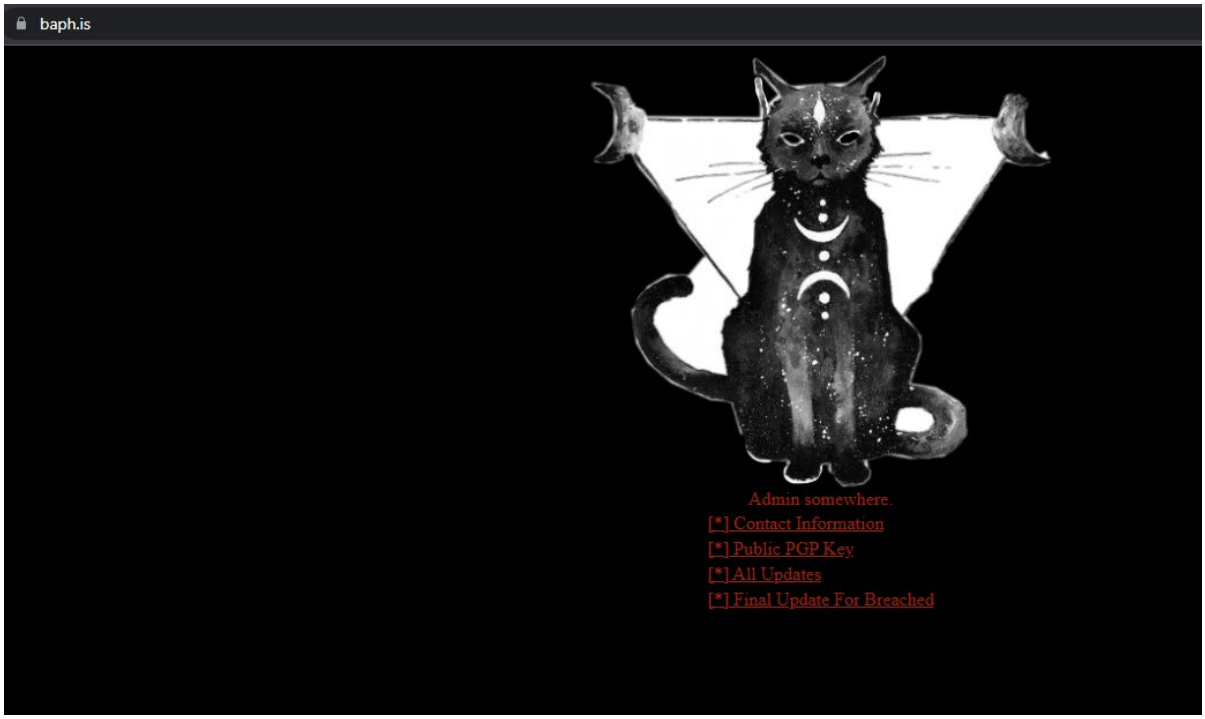


Possiamo inoltre notare nella sezione news come venga specificato che tutti gli altri siti presenti sul deepweb non siano leciti:



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:


baph.is
Admin somewhere.
[*] Contact Information
[*] Public PGP Key
[*] All Updates
[*] Final Update For Breached


baph.is/updates/
Pom Update
Small Update
The Next Update
The Final Update
Safety Update
Chat Update
Pom Update #2
Chats Open
Communications

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.

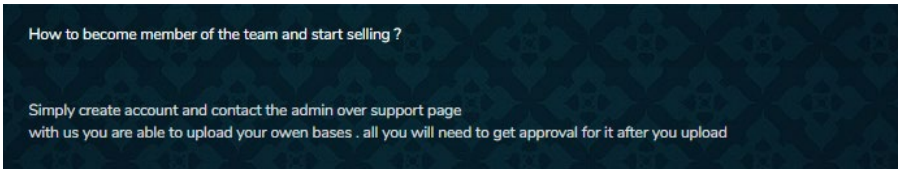
Infine, questi forum sono estremamente redditizi per i loro amministratori. Vendere informazioni personali rubate può generare enormi profitti, e i proprietari di questi forum spesso guadagnano centinaia di migliaia di dollari al mese. Questo significa che hanno un forte incentivo per continuare le loro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

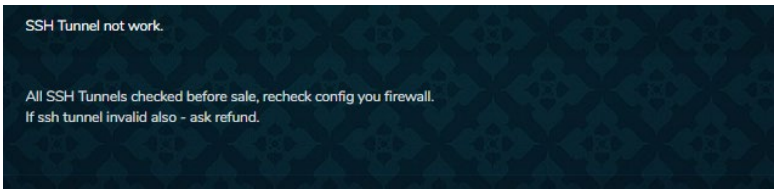
La risposta è semplice, questi due forum, seppur estremamente noti nel mondo underground sono soltanto la punta dell'iceberg. Difatti altri forum/market stanno prendendo il controllo della scena, uno fra tutti Russian Market.

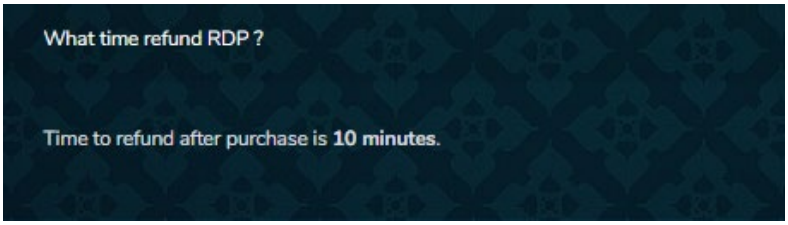
Russian Market può essere considerato come un'alternativa al portale (recentemente chiuso) Genesis: il portale non presenta una sezione di Forum (come in Breached, dove avvengono spesso discussioni e scambi di informazione tra i vari utenti), ma si presenta come un vero e proprio store digitale di credenziali 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:



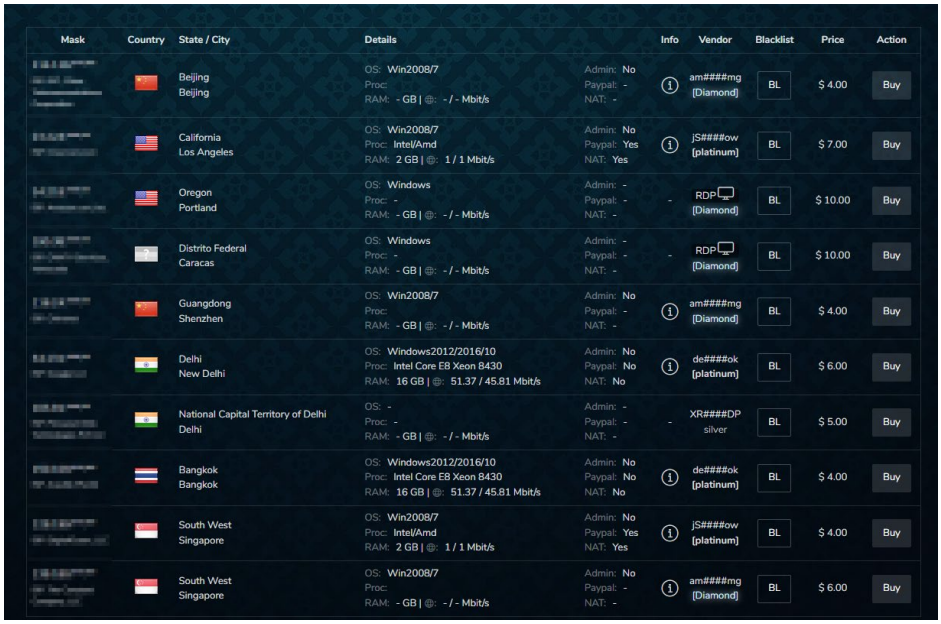
Nel market sono inoltre rimborsabili tutti gli accessi acquistati che non sono più validi (fatto eccezione dei dati relativi alle botnet).





Perché questi luoghi rappresentano un pericolo

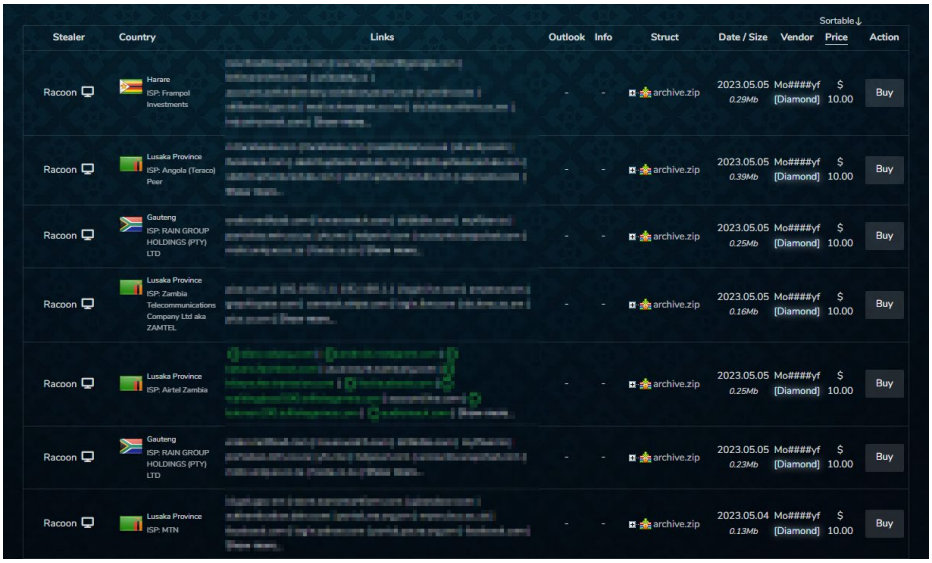
I rischi derivanti da questo mercato sono molteplici, è possibile infatti pensare agli accessi RDP/SSH in vendita. Questi potrebbero difatti essere il primo punto di accesso, per Threat Actor più esperti, a reti corporate con il conseguente rischio di un attacco informatico con lo scopo di caricare remotamente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



Mask	Country	State / City	Details		Info	Vendor	Blacklist	Price	Action
[redacted]		Beijing Beijing	OS: Win2008/7 Proc: RAM: - GB | : - / - Mbit/s	Admin: No Paypal: - NAT: -		am####mg [Diamond]	BL	$ 4.00	Buy
[redacted]		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
[redacted]		Oregon Portland	OS: Windows Proc: - RAM: - GB | : - / - Mbit/s	Admin: - Paypal: - NAT: -	-	RDP [Diamond]	BL	$ 10.00	Buy
[redacted]		Distrito Federal Caracas	OS: Windows Proc: - RAM: - GB | : - / - Mbit/s	Admin: - Paypal: - NAT: -	-	RDP [Diamond]	BL	$ 10.00	Buy
[redacted]		Guangdong Shenzhen	OS: Win2008/7 Proc: RAM: - GB | : - / - Mbit/s	Admin: No Paypal: - NAT: -		am####mg [Diamond]	BL	$ 4.00	Buy
[redacted]		Delhi New Delhi	OS: Windows2012/2016/10 Proc: Intel Core E8 Xeon 8430 RAM: 16 GB | : 51.37 / 45.81 Mbit/s	Admin: No Paypal: No NAT: No		de####ok [platinum]	BL	$ 6.00	Buy
[redacted]		National Capital Territory of Delhi Delhi	OS: - Proc: - RAM: - GB | : - / - Mbit/s	Admin: - Paypal: - NAT: -	-	XR####DP silver	BL	$ 5.00	Buy
[redacted]		Bangkok Bangkok	OS: Windows2012/2016/10 Proc: Intel Core E8 Xeon 8430 RAM: 16 GB | : 51.37 / 45.81 Mbit/s	Admin: No Paypal: No NAT: No		de####ok [platinum]	BL	$ 4.00	Buy
[redacted]		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
[redacted]		South West Singapore	OS: Win2008/7 Proc: RAM: - GB | : - / - Mbit/s	Admin: No Paypal: - NAT: -		am####mg [Diamond]	BL	$ 6.00	Buy

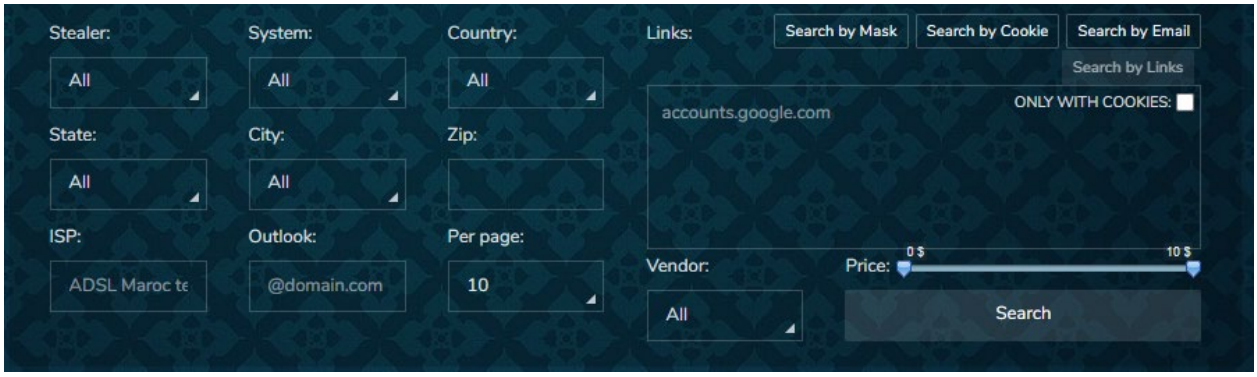
Nella sezione relativa agli accessi RDP sono presenti un totale di circa 15’200 accessi a potenziali pc/server compromessi. Prendendo in considerazione l’Italia, ad esempio, sono presenti 74 accessi a postazioni di lavoro mentre i due paesi con più accessi in vendita risultano Cina e Stati Uniti con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



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:

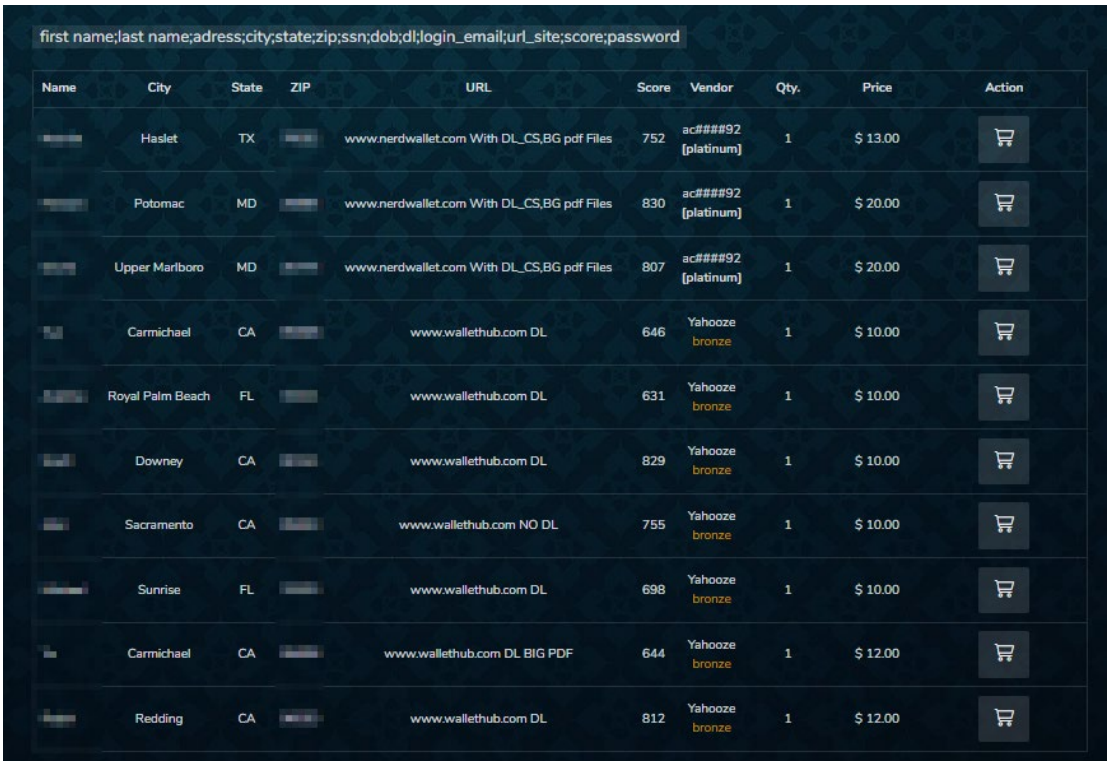


Un attaccante potrebbe quindi cercare degli accessi per un determinato portale o per un determinato dominio così da poter poi proseguire con un attacco informatico o con la vendita delle credenziali trovate ad altri Threat Actor (i venditori di queste credenziali "corporate" sono gergalmente definiti "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	[redacted]	BANK	DEBIT	PREPAID	[redacted]	May-us-good (REFUND 5 min)		NY	FT WALTON BCH	[redacted]			fe####un (platinum)	$ 10.00	Buy
VISA	[redacted]	BANK	CREDIT	CLASSIC	[redacted]	May-us-good (REFUND 5 min)		MS	SPRING	[redacted]			fe####un (platinum)	$ 10.00	Buy
VISA	[redacted]	BANK	DEBIT	CLASSIC	[redacted]	May-us-good (REFUND 5 min)		MO	PORT NECHES	[redacted]			fe####un (platinum)	$ 10.00	Buy
VISA	[redacted]	BANK	CREDIT	CLASSIC	[redacted]	May-us-good (REFUND 5 min)		MA	Spearfish	[redacted]			fe####un (platinum)	$ 10.00	Buy
VISA	[redacted]	BANK	DEBIT	PREPAID	[redacted]	May-us-good (REFUND 5 min)		WA	Lafayette	[redacted]			fe####un (platinum)	$ 10.00	Buy
MasterCard	[redacted]	BANK	DEBIT	STANDARD	[redacted]	May-us-good (REFUND 5 min)		MA	LAWTON	[redacted]			fe####un (platinum)	$ 10.00	Buy
VISA	[redacted]	BANK	CREDIT	CLASSIC	[redacted]	May-us-good (REFUND 5 min)		FL	BRANDON	[redacted]			fe####un (platinum)	$ 10.00	Buy
MasterCard	[redacted]	BANK	CREDIT	-	[redacted]	May-us-good (REFUND 5 min)		MO	Lester	[redacted]			fe####un (platinum)	$ 10.00	Buy
VISA	[redacted]	BANK	CREDIT	CLASSIC	[redacted]	May-us-good (REFUND 5 min)		MI	ARLINGTON	[redacted]			fe####un (platinum)	$ 10.00	Buy
VISA	[redacted]	BANK	DEBIT	CLASSIC	[redacted]	May-us-good (REFUND 5 min)		CA	FLOWER MOUND	[redacted]			fe####un (platinum)	$ 10.00	Buy

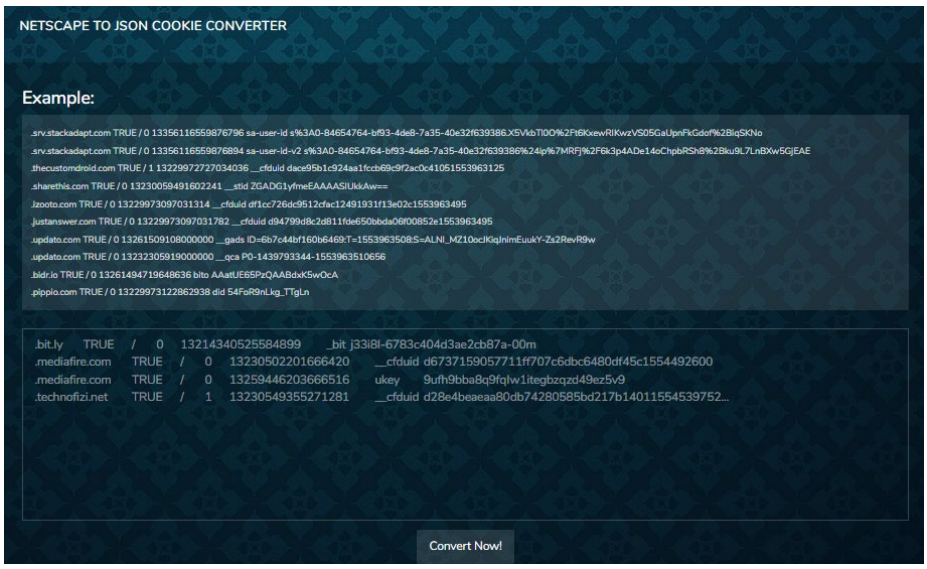


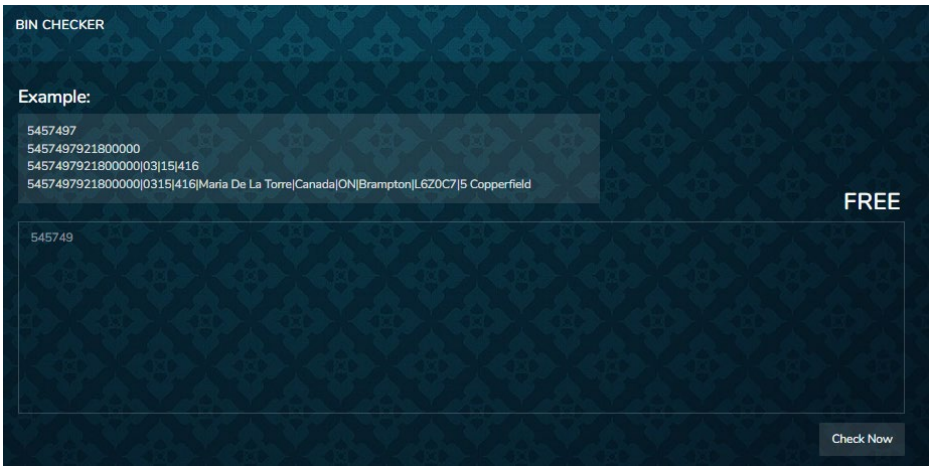
first name;last name;adress;city;state;zip;ssn;dob;dl;login_email;url_site;score;password

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

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:





Credenziali Italiane in vendita

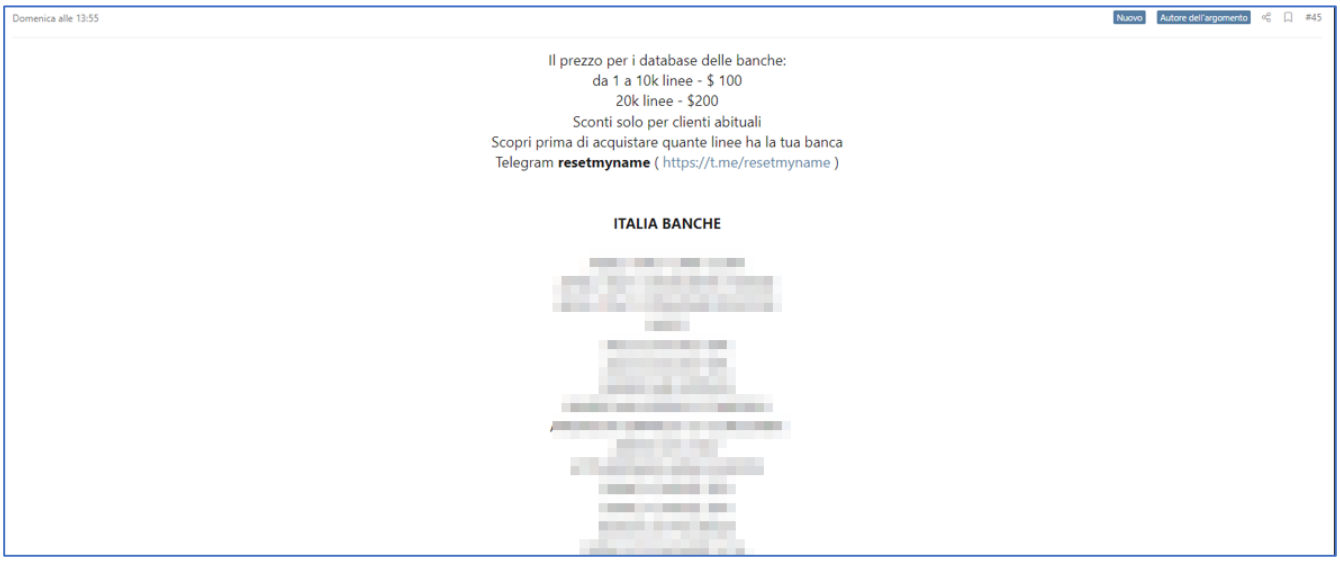
Negli ultimi anni, il fenomeno della vendita di credenziali personali e aziendali sul deep e darkweb, come abbiamo notato negli esempi sopra riportati, ha assunto proporzioni preoccupanti anche in Italia. Sono infatti sempre di più le persone e le aziende che si trovano a subire attacchi informatici, 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.

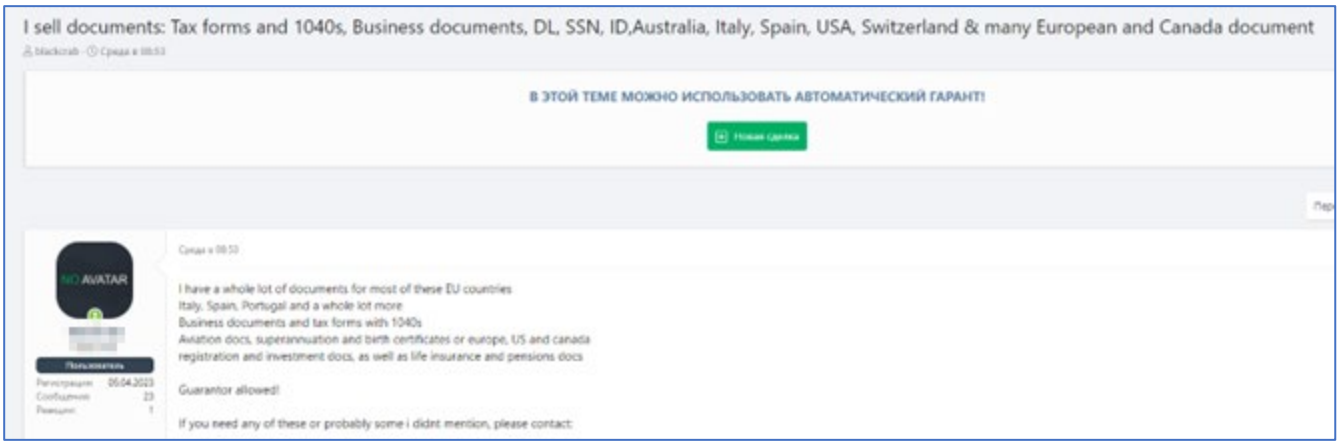
Le credenziali vendute riguardano principalmente account di posta elettronica, password di accesso a social network, conti bancari e carte di credito. Ma non solo: sempre più spesso vengono messe in vendita anche informazioni aziendali riservate come, accessi RDP alla loro infrastruttura, contratti di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

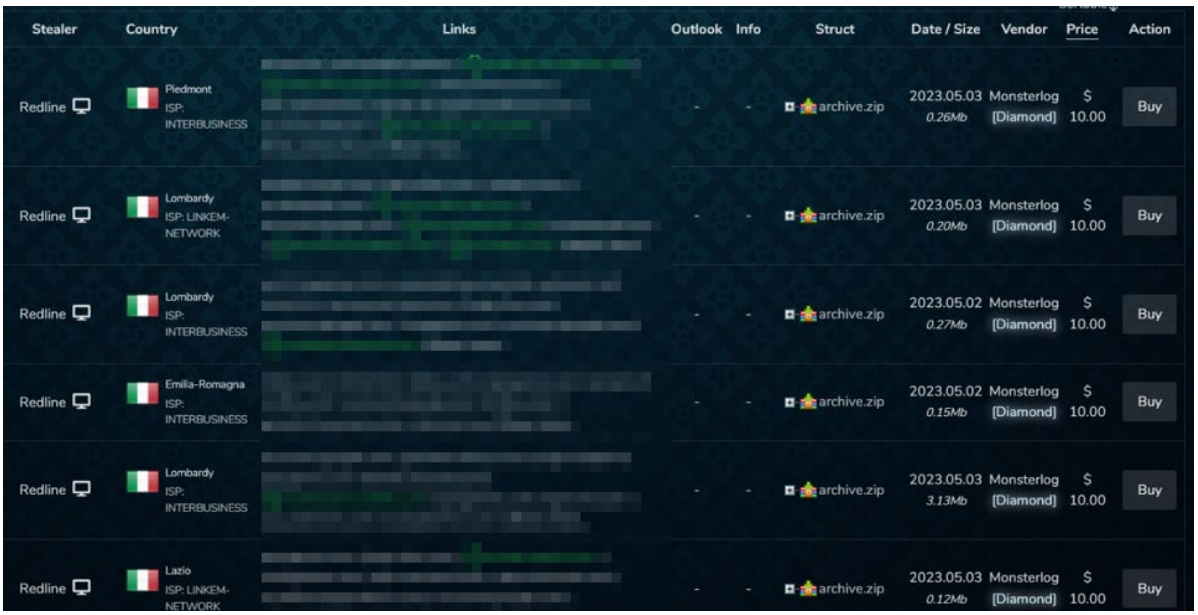


Di seguito invece un esempio di documenti aziendali in vendita provenienti da diversi paesi:

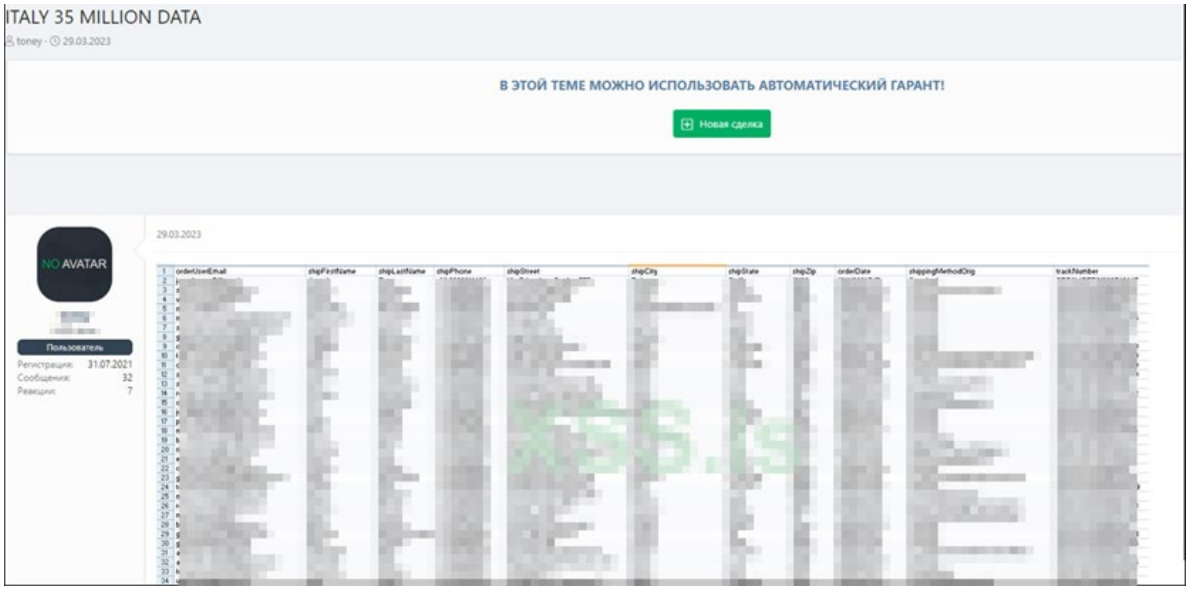


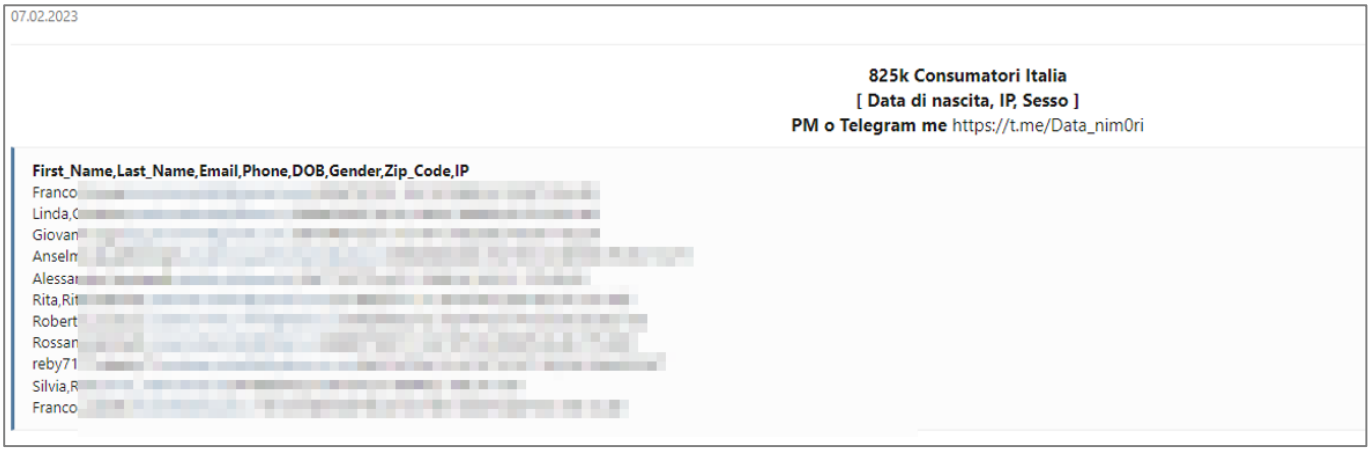
Qui di seguito invece dei template per documenti falsi in vendita:

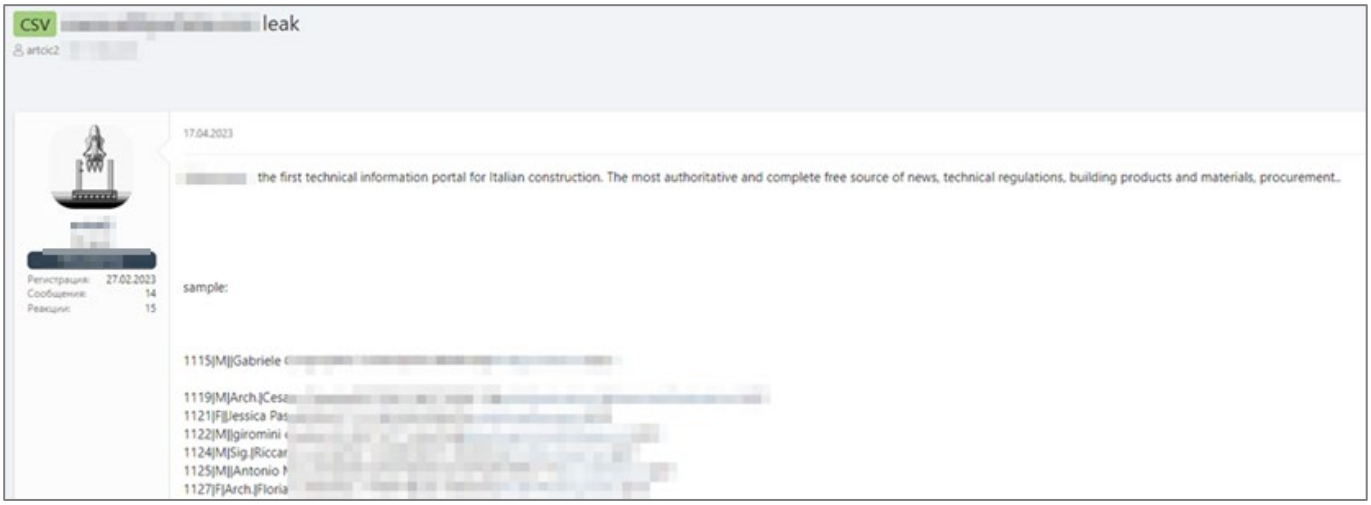
Qui invece alcuni esempi di botnet e dati di italiani in vendita:



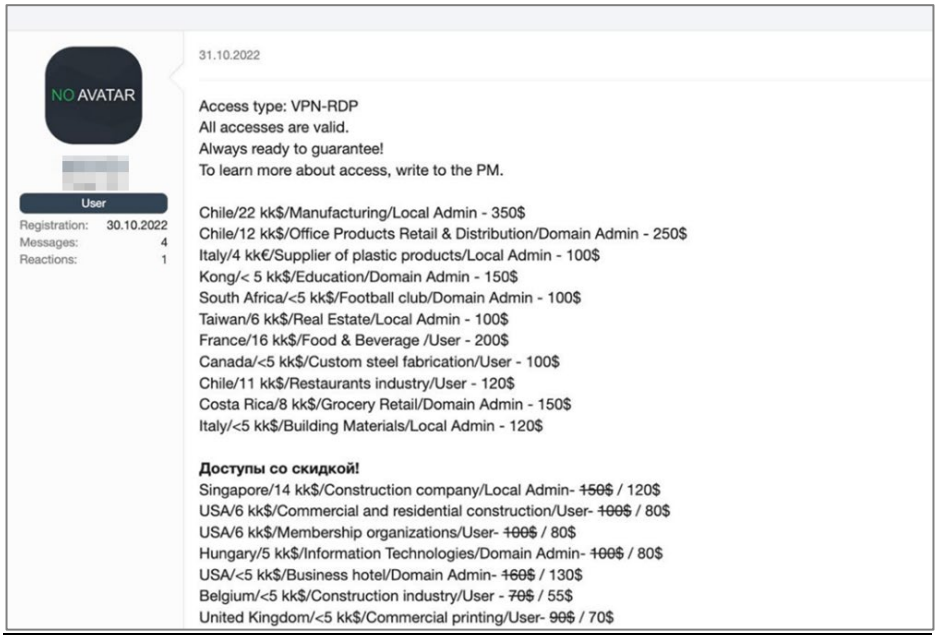
Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price	Action
Redline	Piedmont ISP: INTERBUSINESS		-	-	archive.zip	2023.05.03 0.26Mb	Monsterlog [Diamond]	$ 10.00	Buy
Redline	Lombardy ISP: LINKEM-NETWORK		-	-	archive.zip	2023.05.03 0.20Mb	Monsterlog [Diamond]	$ 10.00	Buy
Redline	Lombardy ISP: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




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


CSV
leak
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:

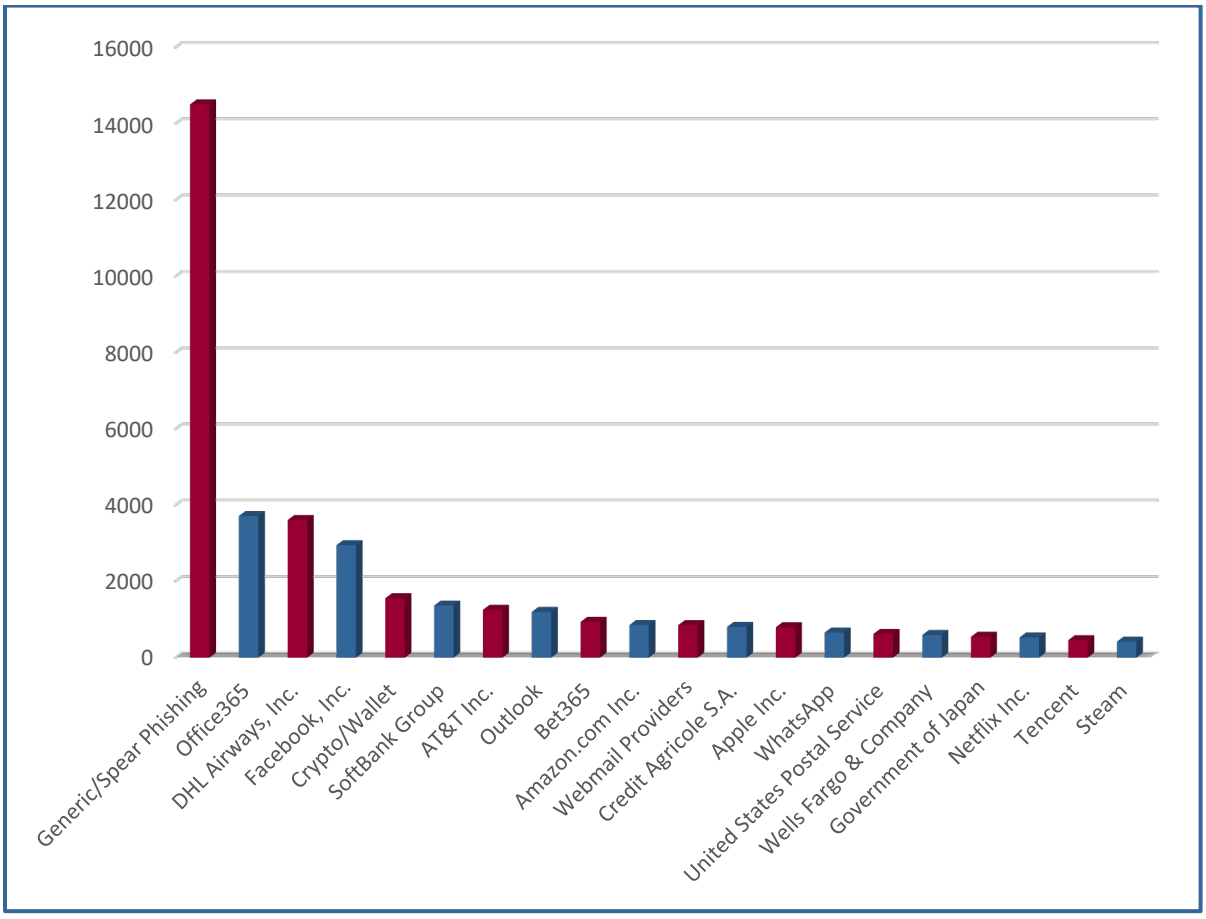
In fine, un esempio di accessi VPN-RDP corporate in vendita da un Access Broker:



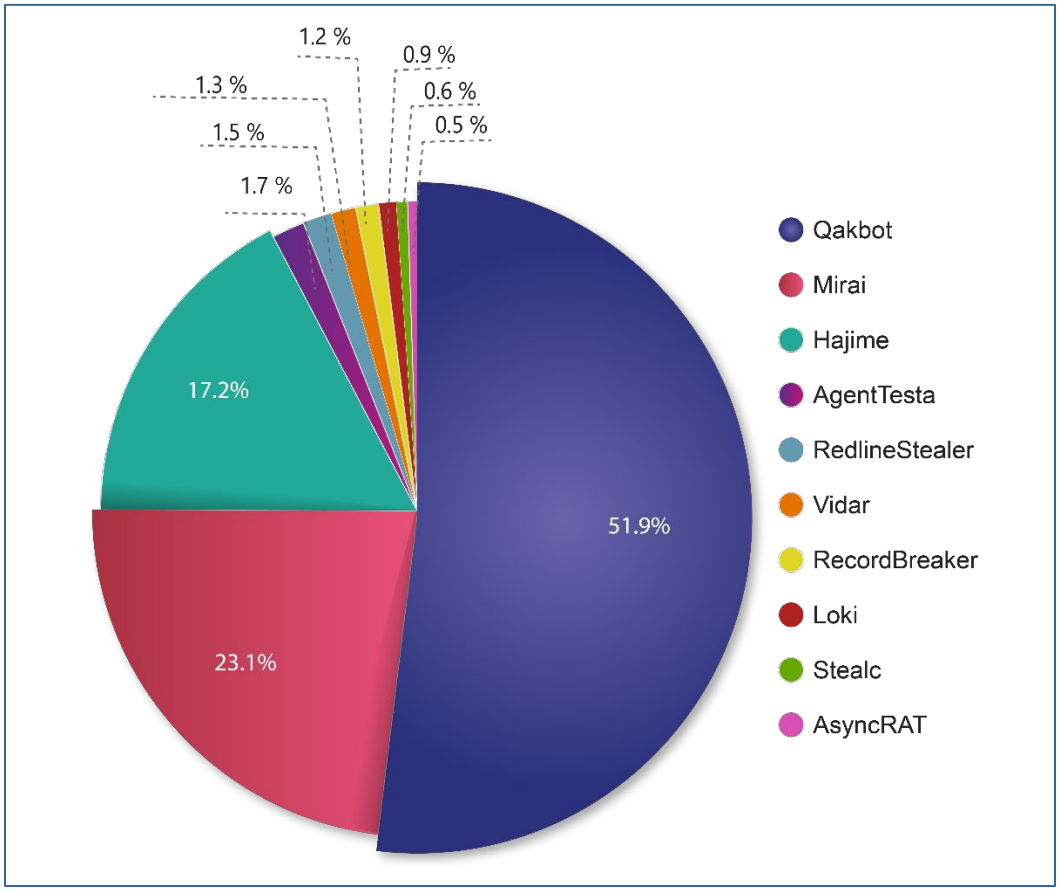
Ma da dove arrivano tutte queste credenziali?

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