TINEXTA CYBER

ANALISI DARKWEB

2024

www.tinextacyber.com

Sommario

INTRODUZIONE

Nel vasto mondo dei mercati sul deep web e sul dark web, una serie di attività illecite prospera al di sotto della superficie del web convenzionale. Qui, l'economia sotterranea fiorisce attraverso la compravendita di prodotti e servizi illegali, alimentando una rete intricata e spesso pericolosa di transazioni illecite. Questi mercati sono spazi virtuali in cui gli individui possono accedere in modo anonimo per acquistare o vendere una vasta gamma di beni illegali, da droghe a informazioni di carta di credito rubate, da malware a identità rubate.

In questa analisi, esploreremo quattro categorie principali di mercati Dark Web: droga, carding, malware/phishing/ransomware e identity leaks e credential access. Ogni categoria sarà esaminata attraverso tre mercati rappresentativi, selezionati per fornire un'immagine chiara e comprensibile del funzionamento e dell'ecosistema di tali mercati.

Di seguito sono riportati alcuni dati significativi relativi al Dark Web, che mettono in luce la sua impattante presenza e gli aspetti critici legati alla sua esistenza. La tabella seguente presenta statistiche rilevanti riguardanti la dimensione del mercato del Dark Web, l'utilizzo, gli attacchi informatici, l'impatto sulle imprese e i mercati del Dark Web.

Dimensione del mercato	Entro il 2028, il mercato globale del dark web dovrebbe raggiungere $1,3 miliardi con un tasso di crescita annuale (CAGR) del 22,3%
Utilizzo e diffusione	Il deep web e il dark web possiedono collettivamente il 96% di internet, mentre il restante 4% comprende il surface web
Hosting su Tor	Tor ospita circa 30.000 siti web nel dark web
Attività nel dark web	Tra il 2017-2020 le attività nel dark web su internet sono aumentate del 300%
Danneggiamenti da ransomware	Sono stimati danni globali da ransomware di$265 miliardi entro il 2031
Violazioni della sicurezza informatica	L'errore umano causa il 90% degli attacchi informatici registrati
Transazioni di Bitcoin	Il Bitcoin è utilizzato nel 98% delle transazioni sul Dark Web

L'oscurità del dark web continua ad attrarre un numero significativo di utenti, con oltre 2,5 milioni di visitatori giornalieri stimati nel 2023. Questo sottobosco digitale, noto per la sua clandestinità, vede una vasta partecipazione, con la Germania emergere come il paese con il maggior numero di utenti giornalieri di Tor, il browser che consente l'accesso al dark web, proprio in quell'anno. Tuttavia, questa oscurità non è senza conseguenze, con un aumento impressionante delle frodi basate su ransomware nel 2023, che ha generato quasi 176 milioni di dollari in perdite. Tra gli utenti del dark web, prevale una forte predominanza maschile, con il 84,7% degli utenti identificati come uomini, mentre il 9,4% sono donne. Tra le fasce d'età, il gruppo più comune tra gli utenti del dark web si situa tra i 36 ei 45 anni, rappresentando il 23,5% della popolazione attiva in questo sottobosco digitale.

Un'analisi condotta da NordVPN fornisce una panoramica dettagliata sui prezzi e sulle caratteristiche delle carte di pagamento vendute sui mercati del dark web. Attraverso l'analisi di quasi sei milioni di carte, vengono evidenziate le tendenze nei prezzi medi, le principali metodologie di acquisizione delle carte e i paesi con il maggior numero di carte compromesse.

Categoria	Dato
Numero totale di carte analizzate	5,953,651
Prezzo medio delle carte vendute	$7.01
Valore totale del dataset	$18.5 milioni
Paesi con maggior numero di carte	USA (3,461,444 carte, 58.1% del totale) India (3.7%) UK (2.8%) Messico (2.6%)
Prezzo medio più alto per paese	Danimarca ($11.54) Giappone, Portogallo, Ucraina (oltre $11)
Prezzo medio più basso per paese	Argentina e Nuova Zelanda (meno di $2.50)
Carte con informazioni aggiuntive	62.8% (es. indirizzo, numero di telefono)
Carte ottenute tramite hacking	62.8%
Carte ottenute tramite brute force	37.2%

L'Italia si posiziona in una fascia intermedia in termini di prezzo medio delle carte di pagamento compromesse, con un prezzo medio di $8.98.

Questi dati offrono una visione approfondita delle dinamiche nel dark web, illustrando le differenze nei prezzi e nelle pratiche di acquisizione a livello globale.

Stupefacenti e farmaci

Il mercato underground delle sostanze stupefacenti registra il più alto numero di prodotti in commercio e di venditori, evidenziando un costante aumento nel corso degli ultimi anni. Queste piattaforme online presentano una vasta gamma di narcotici, che spaziano dalle sostanze più comuni alle materie prime utilizzate per la produzione di nuovi composti o per altri fini illeciti, offrendo ai clienti un'ampia scelta. Di seguito esamineremo il panorama del mercato delle droghe rispetto ad altri settori, approfondendo l'analisi di tre mercati che si occupano della vendita di queste sostanze.

Market #1

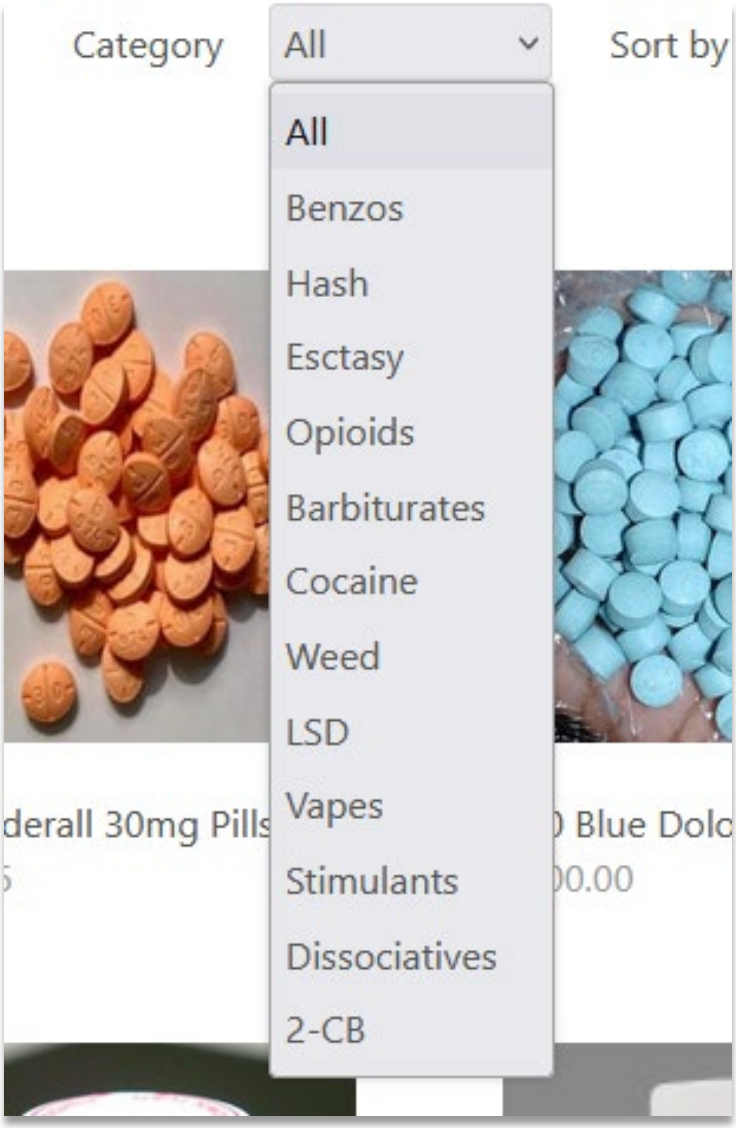
Il primo mercato illegale si presenta come un negozio online che offre una vasta gamma di droghe di alta qualità, operante da diversi anni e vantando un'ampia esperienza nel settore, con oltre 10.000 vendite confermate in tutto il dark web. La sua offerta comprende sostanze come erba, cocaina, idrocodone, eroina, ketamina, Ozempic, metanfetamina cristallina, Adderall, Ritalin, Vyvanse, MDMA, pentobarbitale, vape e sostanze chimiche di ricerca.

L'enfasi è posta sulla qualità dei prodotti offerti, che vengono pubblicizzati come di alto livello. La gamma di sostanze disponibili è ampia e variegata, coprendo diverse esigenze e preferenze degli utenti.

L'aspetto più rilevante è la promozione della sicurezza e della fiducia, come indicato dal messaggio "Active for years now". Questo suggerisce che il negozio abbia una reputazione consolidata nel settore e che i clienti possano fare affidamento sulla qualità e sulla riservatezza del servizio offerto.

La menzione della vasta esperienza e delle numerose vendite confermate, infatti, potrebbe essere interpretata come un tentativo di rassicurare i potenziali acquirenti sulla affidabilità e sulla stabilità del negozio.

Il negozio offre 48 prodotti diversi, così suddivisi per categorie:



100 Fentanyl Pills 1mg
$280.00

10g Ketamine Crystals
$290.00

100 Adderall 30mg Pills
$245.95

100 Blue Dolophin Pills 295mg
$300.00

100 Green Grenade XTC Pills
$300.00

100 Ritalin Pills
$250.00

100 Oxycontin 80mg Pills
$299.99

120 Pills hydrocodone 10mg
$280.00

100 Phillip Plein 250 MG
$249.00

50 Mitsubishi XTC Pills 220 MG
$250.00

2 Pens Ozempic 1mg
$280.00

100 2CB Pills 25MG
$289.00

60 Vials Fentanyl Liquid
$240.97

5 Grams Argentine Cocaine
$230.00

10 Grams Flake Cocaine
$530.00

100ML Nembutal Oral Liquid
$390.00

L'offerta del prodotto è presentata in modo chiaro e diretto, con un'enfasi sulla possibilità di acquistare il prodotto online senza la necessità di una prescrizione medica. Vengono fornite informazioni essenziali sul farmaco, compresa la sua natura come stimolante del sistema nervoso centrale e le sue principali indicazioni terapeutiche per il trattamento dell'ADHD e della narcolessia.

100 Ritalin Pills

$250.00

Quantity

1

ADD TO CART

Buy Ritalin Online | Order Ritalin 10mg And 20Mg Online Without Prescription At Pure Meds Shop

Buy Ritalin Online. Ritalin is a brand name for methylphenidate, a central nervous system stimulant medication. It's commonly prescribed to treat attention-deficit hyperactivity disorder (ADHD) and narcolepsy. Here are some key points about Ritalin:

1. **Treatment of ADHD:** Ritalin is widely used to manage symptoms of ADHD in children, adolescents, and adults. It works by affecting certain neurotransmitters in the brain, such as dopamine and norepinephrine, which play roles in attention, focus, and impulse control. Ritalin helps improve attention span, concentration, and behavioral control in individuals with ADHD.
2. **Narcolepsy:** In addition to ADHD, Ritalin is sometimes prescribed to treat narcolepsy, a sleep disorder characterized by excessive daytime sleepiness and sudden sleep attacks. By stimulating specific areas of the brain and increasing wakefulness, it helps individuals with narcolepsy stay awake during the day.
3. **Forms and Dosage:** Ritalin is available in various forms, including immediate-release tablets, extended-release tablets, and long-acting capsules. Dosage and administration depend on individual needs, the specific condition being treated, and the formulation prescribed by a healthcare professional.
4. **Usage and Effects:** Ritalin is a stimulant medication that can increase alertness and focus. However, it can also have side effects such as decreased appetite, difficulty sleeping, increased heart rate, and, in some cases, increased anxiety or irritability. It's crucial to take Ritalin exactly as prescribed and to communicate any side effects to the prescribing doctor.
5. **Controlled Substance:** Ritalin, like other stimulant medications, has a potential for abuse and dependency if misused. Therefore, its use should be strictly monitored and prescribed by a healthcare professional.

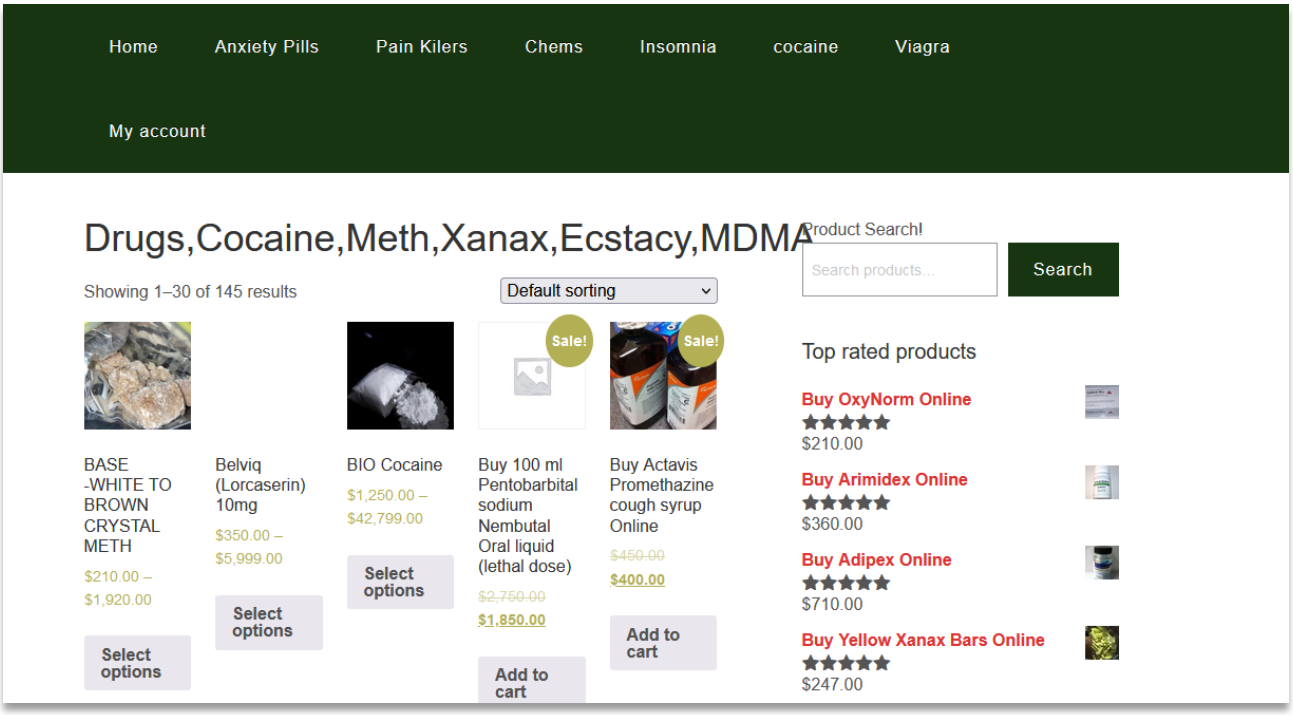
As with any medication, it's important to follow the prescribed dosage and guidelines provided by a doctor. Regular check-ups and communication with the healthcare provider are essential to monitor the medication's effectiveness, manage side effects, and make any necessary adjustments to the treatment plan.

Il mercato offre anche un servizio clienti dedicato, evidenziato dalla possibilità di contattare il negozio in qualsiasi momento per risolvere eventuali dubbi o domande. Il contatto con il servizio clienti è reso facile attraverso diverse opzioni. Gli acquirenti possono inviare un'email all'indirizzo indicato, oppure vi è la possibilità di contattare il servizio clienti tramite Telegram, offrendo dunque un'alternativa più immediata e informale per comunicare con il negozio, consentendo agli acquirenti di ottenere assistenza in tempo reale tramite chat.

I prezzi dei prodottii variano da 195 a 750 dollari. Il negozio accetta pagamenti tramite Bitcoin (BTC), Ethereum (ETH) e Tether (USDT). Questi metodi di pagamento offrono agli acquirenti diverse opzioni per effettuare transazioni in modo sicuro e anonimo.

Nel canale Telegram, oltre alla vendita di droghe, è evidente la presenza di offerte per documenti e carte di credito sia in Europa che negli Stati Uniti. Questo indica un'ampia gamma di servizi illegali offerti dal canale. Attivo da marzo 2024, il canale conta attualmente 1518 iscritti, suggerendo un certo grado di popolarità e di attività del mercato.

Market #2

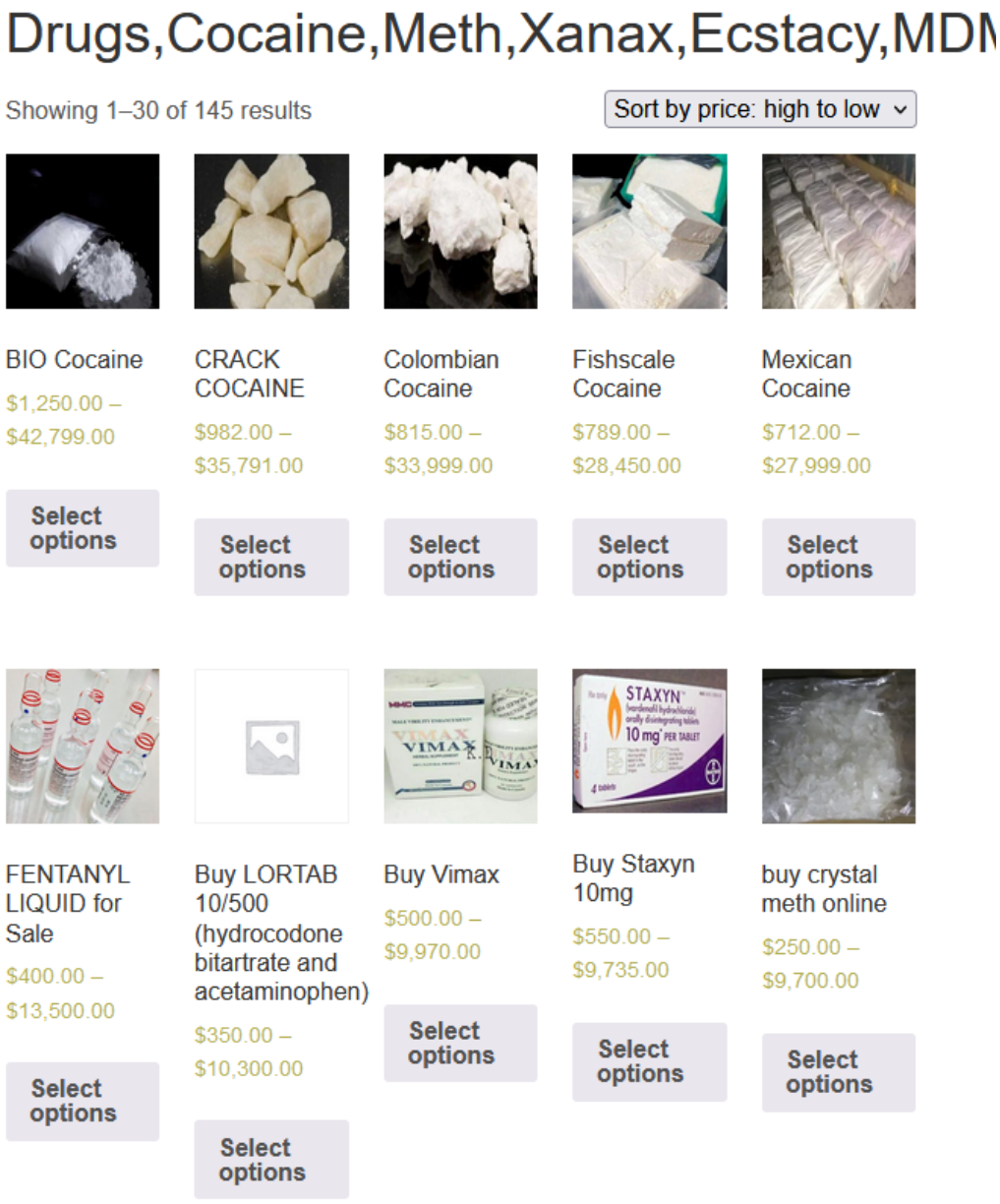


Il secondo esempio analizzato come un mercato significativo nel mondo underground, offrendo una vasta gamma di prodotti tra cui droghe, medicinali per l'ansia e il dolore, psichedelici e altri farmaci.

Possiamo notare come questi mercati funzionano come veri e propri negozi: assicurano un'elevata sicurezza, promettendo un servizio rapido, sicuro e discreto direttamente a casa o sul luogo di lavoro del cliente, con oltre 1000 prodotti disponibili "difficili da trovare altrove".

L'azienda afferma di avere una sua rete di fornitori e magazzini strategici, garantendo consegne veloci. La promessa di qualità è centrale nel loro approccio, con un'attenzione particolare alla soddisfazione del cliente e alla disponibilità di prodotti di alta qualità.

La gamma di prodotti disponibili include farmaci per vari scopi, come il trattamento di ansia, dolore e altre condizioni. Tra questi troviamo farmaci come OxyContin, Nembutal pentobarbital, Adderall, Ritalin, Tramadol, Ketamine, Morfina, Cocaina, Eroina, Metanfetamine, Fentanyl, Xanax, Ecstasy, MDMA e Viagra.



Anche in questo caso viene fornito un supporto clienti attraverso vari canali di comunicazione come telefono, email e chat online durante gli orari lavorativi.

Questo shop accetta esclusivamente pagamenti tramite Bitcoin e altre criptovalute, sottolineando l'importanza della sicurezza e dell'anonimato per i propri clienti. Questo approccio riflette

l'orientamento del mercato underground verso transazioni finanziarie cifrate e decentralizzate per garantire la riservatezza degli acquirenti.Per coloro che sono nuovi nell'ambito delle criptovalute, il negozio fornisce istruzioni dettagliate su come acquistare e inviare Bitcoin utilizzando tre popolari piattaforme: Binance, Coinbase e Cash App.

Le quantità minime di ordine sono stabilite a $150 per gli Stati Uniti e a €300 per l'Unione Europea, con tariffe di spedizione variano in base alla destinazione e alle opzioni di consegna scelte. Ad esempio, le spedizioni negli Stati Uniti possono richiedere 3-5 giorni lavorativi e avere una tariffa standard di $50 o una spedizione notturna per $100. Per l'Unione Europea, le consegne standard richiedono 5-7 giorni lavorativi e hanno una tariffa di 210 Euro, mentre la spedizione express, più veloce, costa 610 Euro.

Per altre parti del mondo, si prevedono tempi di consegna di 7-10 giorni e una tariffa di spedizione di $150. Il negozio richiede solo le informazioni di indirizzo o le coordinate GPS per garantire una consegna discreta.

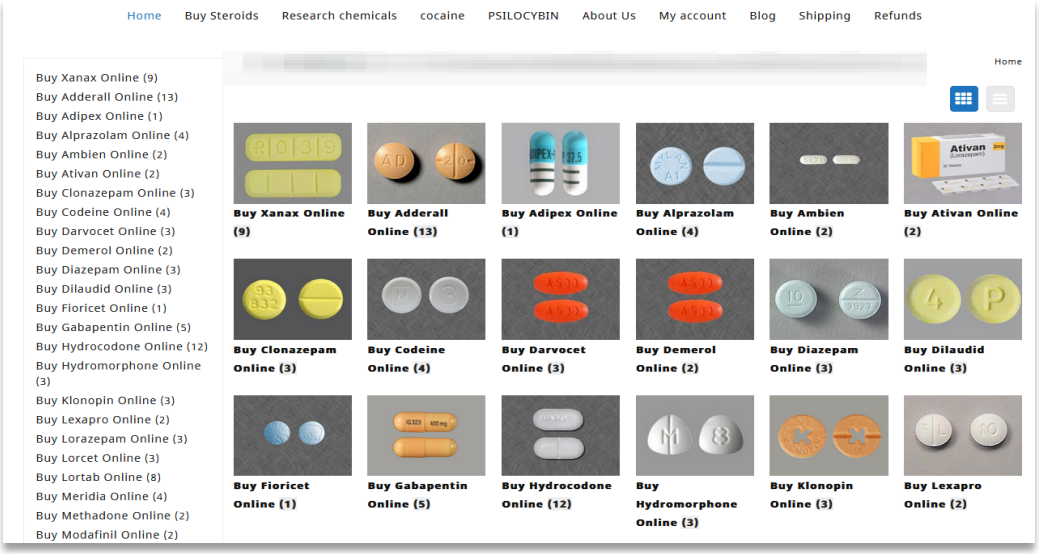
Il negozio afferma di rinominare i pacchetti come “integratori” per garantire la sicurezza. Per essere idonei per un rimborso, la richiesta deve essere effettuata entro 30 giorni dalla data di acquisto e avviene come in un qualsiasi negozio.

Sul sito vi è anche una sezione dedicata a chi vuole diventare un fornitore, dove richiesto il pagamento di una quota di iscrizione di $2,500.

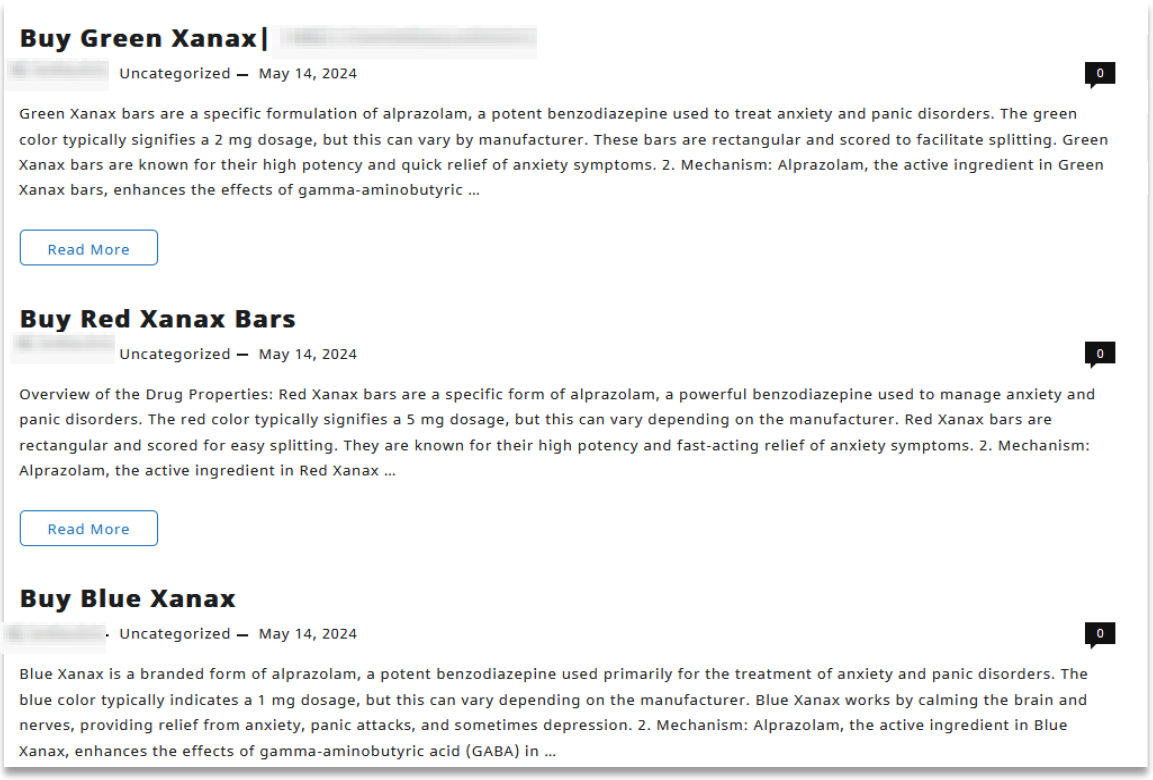
Infine, è curioso notare come i canali telegram dei du mercati appena analizzati condividano esattamente le stesse immagini e offerte, nonostante quest’ultimo sia stato creato a maggio.

Market #3

Il terzo e ultimo esempio tracciato nel dark web si presenta come una "risorsa affidabile e conveniente" per l'acquisto di farmaci su prescrizione e altri prodotti farmaceutici di qualità nell'Unione Europea.



Questo shop online offre una parte dedicata al blog, aggiornata quotidianamente, che fornisce informazioni aggiornate e approfondite su una varietà di argomenti correlati alla salute e ai farmaci.



Buy Green Xanax|

Uncategorized — May 14, 2024 0

Green Xanax bars are a specific formulation of alprazolam, a potent benzodiazepine used to treat anxiety and panic disorders. The green color typically signifies a 2 mg dosage, but this can vary by manufacturer. These bars are rectangular and scored to facilitate splitting. Green Xanax bars are known for their high potency and quick relief of anxiety symptoms. 2. Mechanism: Alprazolam, the active ingredient in Green Xanax bars, enhances the effects of gamma-aminobutyric ...

Read More

Buy Red Xanax Bars

Uncategorized — May 14, 2024 0

Overview of the Drug Properties: Red Xanax bars are a specific form of alprazolam, a powerful benzodiazepine used to manage anxiety and panic disorders. The red color typically signifies a 5 mg dosage, but this can vary depending on the manufacturer. Red Xanax bars are rectangular and scored for easy splitting. They are known for their high potency and fast-acting relief of anxiety symptoms. 2. Mechanism: Alprazolam, the active ingredient in Red Xanax ...

Read More

Buy Blue Xanax

Uncategorized — May 14, 2024 0

Blue Xanax is a branded form of alprazolam, a potent benzodiazepine used primarily for the treatment of anxiety and panic disorders. The blue color typically indicates a 1 mg dosage, but this can vary depending on the manufacturer. Blue Xanax works by calming the brain and nerves, providing relief from anxiety, panic attacks, and sometimes depression. 2. Mechanism: Alprazolam, the active ingredient in Blue Xanax, enhances the effects of gamma-aminobutyric acid (GABA) in ...

Tutti gli ordini vengono spediti dalla struttura in Germania, con una consegna standard entro circa 5 giorni. La tariffa di spedizione standard è di €50, coprendo imballaggio, gestione e consegna. Per coloro che necessitano di consegne più veloci, è disponibile l'opzione di spedizione express al costo di €200, garantendo la consegna entro 24-48 ore.

Alcune limitazioni si applicano a determinati prodotti non idonei al rimborso per motivi di igiene o sicurezza.

L'analisi dei tre mercati della droga disponibili sul dark web mostra come questi sono spesso presentati come veri e propri negozi online, completi di un'ampia selezione di sostanze stupefacenti, descrizioni dettagliate dei prodotti e varie opzioni di pagamento. Tuttavia, dietro questa facciata di "negozio virtuale" si nascondono gravi rischi. Questi mercati offrono un accesso relativamente facile a sostanze illegali, con la possibilità di effettuare acquisti in modo anonimo utilizzando criptovalute. Tuttavia, ciò comporta un'alta probabilità di coinvolgimento in attività illegali. Infine, c'è da considerare il rischio di truffe o frodi da parte dei venditori, con la possibilità di ricevere prodotti contraffatti o di non ricevere affatto la merce pagata.

CARDING

Il carding è una delle attività criminali più diffuse e lucrative nel dark web e consiste nell'acquisizione, vendita e utilizzo fraudolento di dati di carte di credito rubate.

Il processo inizia con l'acquisizione dei dati delle carte di credito. Questi vengono rubati attraverso vari metodi, tra cui il phishing, il malware, l'hacking di database aziendali e una volta ottenuti, i dati rubati vengono venduti su marketplace del dark web, dove i venditori offrono pacchetti di carte a prezzi variabili in base alla qualità e alla quantità delle informazioni.

Gli acquirenti, che possono essere sia individui che organizzazioni criminali, utilizzano questi dati per effettuare acquisti online fraudolenti o clonare carte fisiche. I venditori spesso vantano recensioni e valutazioni positive per attirare nuovi acquirenti e costruire una reputazione solida.

I principali attori di questo mercato includono:

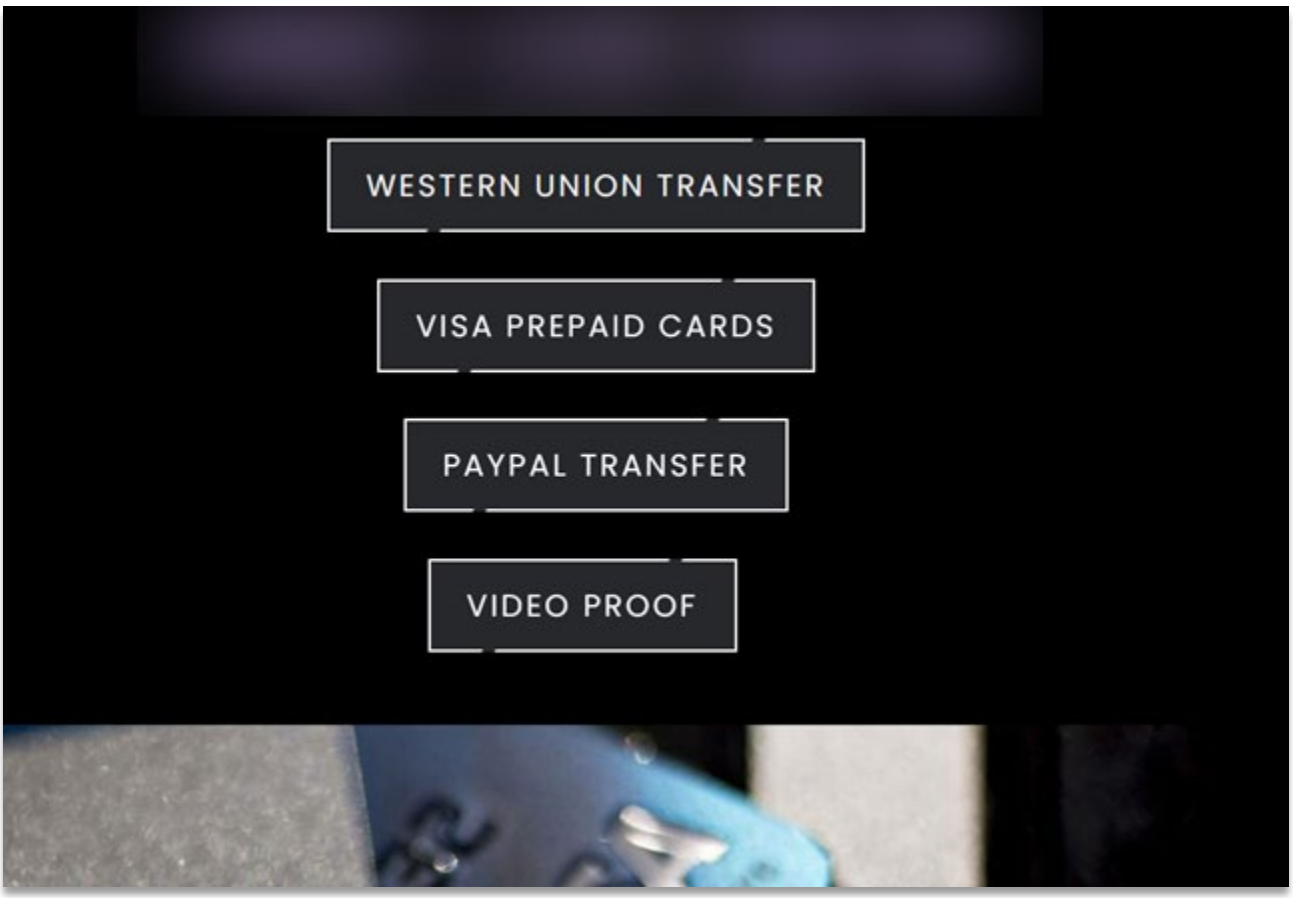
- **Venditori:** Sono i fornitori di dati rubati e operano in modo simile ai rivenditori legittimi, mantenendo inventari, offrendo sconti e promozioni, e fornendo supporto clienti.
- **Acquirenti:** Comprendono sia individui che organizzazioni criminali che acquistano dati per uso personale o per rivenderli a terzi.
- **Marketplace:** Piattaforme come Alphabay e Dreammarket (prima di essere sequestrate) sono state i principali luoghi di scambio per queste attività. Questi mercati offrono strumenti per la comunicazione, la valutazione dei venditori e la gestione delle transazioni.

Modello di Business

Il modello di business del carding sul dark web si basa su diversi fattori chiave. L'anonimato è garantito dall'uso di criptovalute come Bitcoin per effettuare transazioni anonime. La reputazione dei venditori è costruita attraverso feedback positivi, incentivando nuovi acquirenti. Oltre alla vendita di dati di carte, molti venditori offrono servizi di consulenza per money laundering e la prevenzione del rilevamento.

Carding Market #1

Il primo mercato è un esempio di marketplace che offre operazioni che includono la vendita di carte di credito rubate, trasferimenti PayPal e Western Union fraudolenti, e consulenza di vario genere. Operano dal 2016 e sono cresciuti costantemente, adattandosi ai cambiamenti del mercato e mantenendo un'ampia base di clienti. L'ultimo aggiornamento del sito è al 12/05/2024, mostrando dunque di essere costantemente attivi.



Durante la loro attività su piattaforme come Alphabay e Dreammarket, hanno accumulato oltre 7000 recensioni positive, dimostrando la loro affidabilità e competenza nel fornire servizi di carding. Nonostante la chiusura di questi marketplace, il gruppo ha saputo adattarsi, creando un proprio sito web per continuare le operazioni.

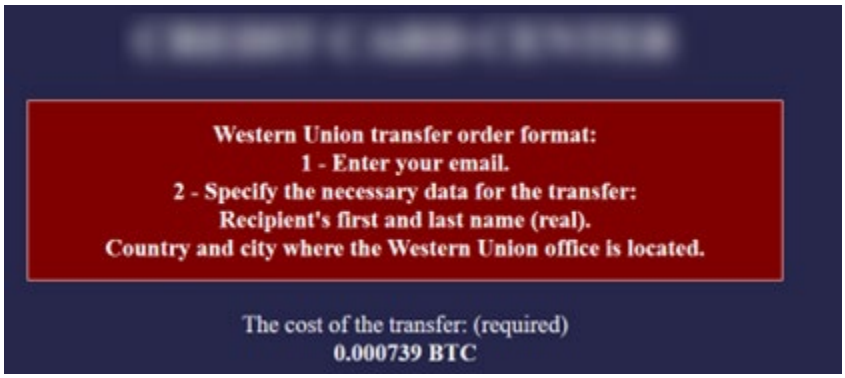
I dettagli delle carte vengono inviati via email entro 20 minuti dall'acquisto, e le carte possono essere utilizzate per pagamenti online su siti come Amazon. Per coloro che preferiscono prelevare contanti da un ATM, è possibile richiedere la consegna fisica delle carte.

I trasferimenti di denaro sono gestiti attraverso un sistema di ordini automatico e possono essere effettuati in Bitcoin, con la possibilità di utilizzare altre criptovalute previa richiesta. Il gruppo offre anche pagamenti con escrow per garantire la sicurezza delle transazioni. Promettono rimborsi in caso di problemi con le carte o i trasferimenti, dimostrando un impegno a lungo termine nei confronti dei loro clienti. Per garantire la legittimità delle loro operazioni, affermano che ogni carta e trasferimento viene ì verificato prima della consegna.

Le tempistiche di consegna sono rapide: le consegne fisiche dipendono dal paese di destinazione, i trasferimenti PayPal sono completati in 45 minuti e quelli Western Union in 120 minuti. Inoltre, il gruppo fornisce consigli utili su come utilizzare i servizi in modo sicuro, raccomandando l'uso di account PayPal regolari per evitare limitazioni e rassicurando sull'uso di ID reali per i trasferimenti Western Union, grazie alla verifica dei mittenti.

Il servizio di trasferimento di denaro Western Union (WU) si presenta come “senza rischi” per il cliente. Il servizio garantisce un tempo massimo di transazione di 2 ore dopo la conferma del pagamento. Alla conclusione della transazione, il cliente riceve un MTCN (Money Transfer Control Number) valido e le informazioni sul mittente. È disponibile in 200 paesi e territori in tutto il mondo, il che rende questo servizio accessibile e pratico per una vasta gamma di clienti internazionali.

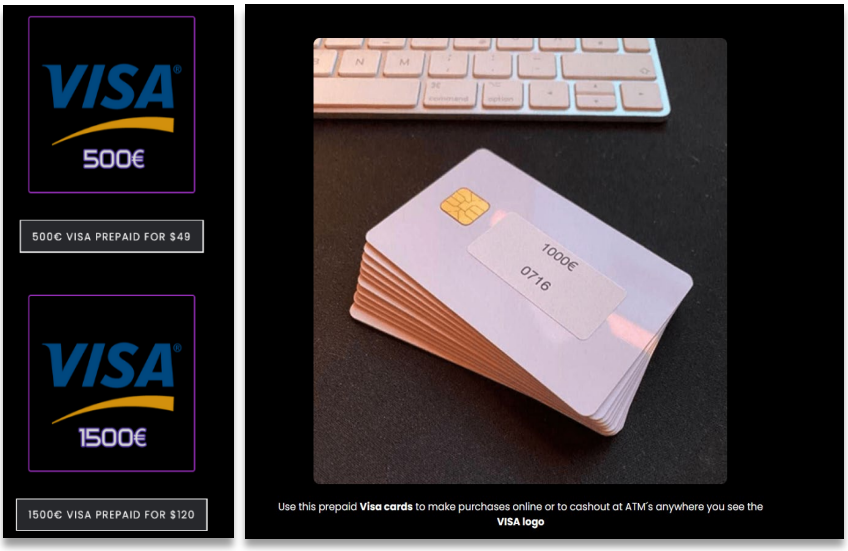
Di seguito alcuni prezzi:



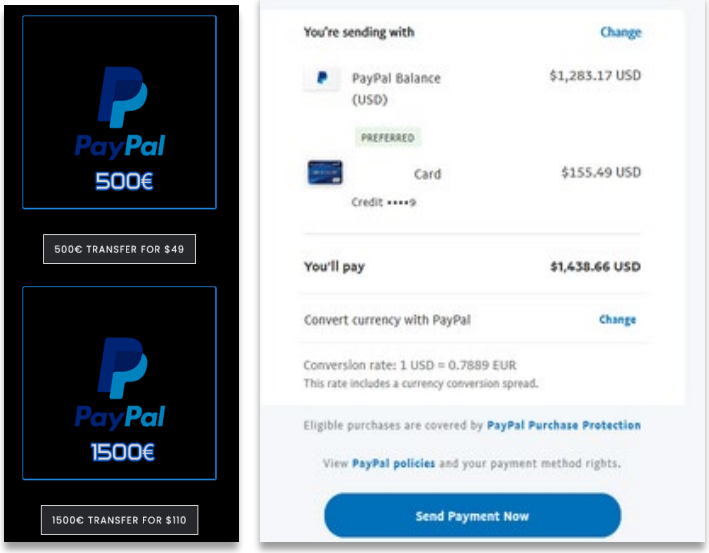
Le carte prepagate Visa presenti nel mercato sono progettate per essere utilizzate sia per acquisti online che per prelievi presso ATM ovunque sia presente il logo Visa. Queste carte non sono collegate a persone fisiche reali e vengono fornite con un saldo predefinito in euro. La conversione della valuta viene gestita automaticamente dalla carta quando viene effettuato un acquisto.

Dopo il pagamento, le informazioni della carta (Nome, Numero di Carta, Data di Scadenza e CVV) vengono inviate via email entro 15 minuti. Per chi richiede la carta fisica, viene effettuata una spedizione express in oltre 150 paesi. I tempi di spedizione variano a seconda del paese di destinazione. Le carte possono essere utilizzate per almeno 90 giorni e non sono ricaricabili. In caso

di esaurimento del credito, è necessario acquistare una nuova carta e hanno un limite giornaliero di utilizzo di 2500 €.

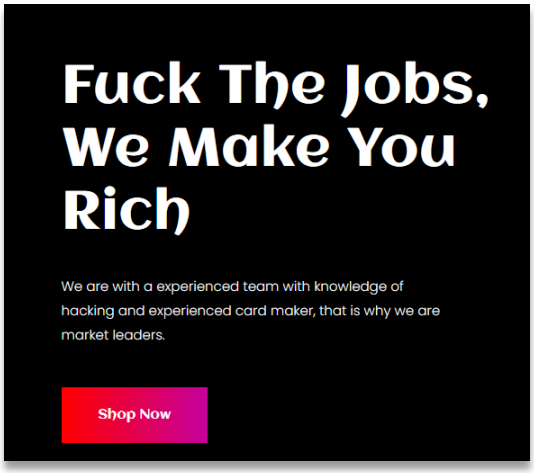


Un altro servizio offre trasferimenti di denaro su account PayPal in modo rapido, dichiarando di essere il metodo più veloce per ottenere fondi. Il mercato afferma che i fondi trasferiti non provengono da account hackerati. I trasferimenti vengono effettuati utilizzando il metodo "goods & services" di PayPal, non "friends & family" (F&F). I trasferimenti richiedono tra i 20 e i 60 minuti per essere completati e offre una garanzia di sostituzione entro 48 ore.



Carding Market #2

Il servizio offerto a questo mercato viene descritto come un "paradiso per i beni digitali", offrendo una vasta gamma di prodotti digitali con alcune caratteristiche distintive, quali spedizione mondiale, supporto 24/7 e la possibilità di acquistare in modo anonimo.



La spedizione dei prodotti viene effettuata in un arco di tempo che varia dai 3 ai 10 giorni, a seconda della località del cliente. Un team di supporto è disponibile 24 ore su 24, 7 giorni su 7.

Attivo dal 2016, offre prodotti che si suddividono in due categorie: Credit Cards e Prepaid Cards.

Il mercato offre una varietà di carte di credito e carte prepagate, suddivise in diverse categorie basate su limiti di prelievo giornalieri e di spesa. Le principali categorie di carte sono:

1. **Carte di Credito**:
    - **Visa**
    - **MasterCard**
    - **American Express (AmEx)**
    - **Discover**
    - **Maestro**
    - **Diners Club – International**

2. **Carte Prepagate**:
    - **Visa**
    - **MasterCard**

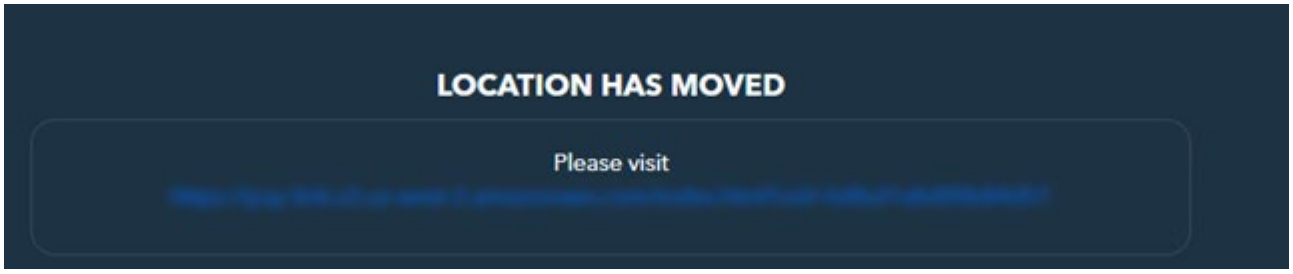
Prezzi per Categorie di Carte di Credito

Categoria	Tipo	Prezzo
Visa	Regular	$65.00
	Standard	$95.00
	Plus	$125.00
MasterCard	Regular	$85.00
	Standard	$115.00
	Plus	$145.00
American Express (AmEx)	Regular	$55.00
	Standard	$85.00
	Plus	$115.00
Discover	Regular	$60.00
	Standard	$90.00
	Plus	$120.00
Maestro	Regular	$70.00
	Standard	$100.00
	Plus	$130.00
Diners Club - International	Regular	$70.00
	Standard	$100.00
	Plus	$130.00

Prezzi per Categorie di Carte Prepagate:

Categoria	Tipo	Prezzo
Visa	Classic	$75.00
	Standard	$105.00
	Plus	$135.00
MasterCard	Classic	$90.00
	Standard	$125.00
	Plus	$160.00

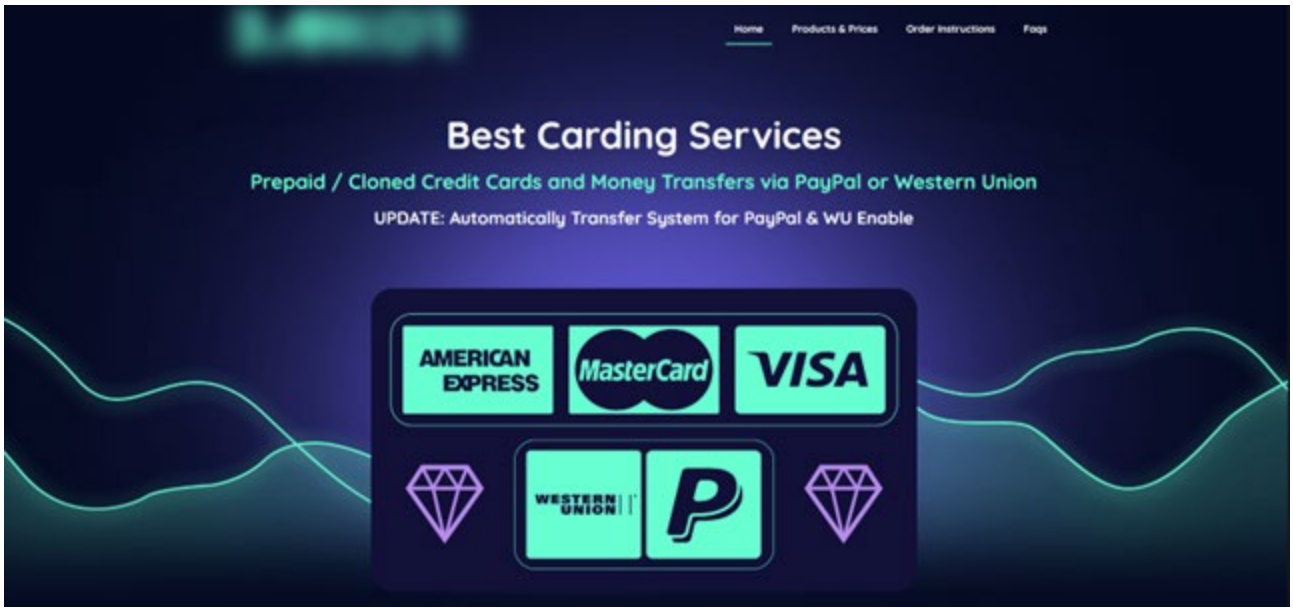
Quando clicchiamo sul link per simulare un pagamento, esce questo avviso per il pagamento:



Le principali reti di carte di credito come Visa, MasterCard, American Express, Discover, Maestro e Diners Club International offrono una varietà di livelli di servizio e vantaggi, dai limiti di prelievo giornalieri alle opzioni di acquisto senza limiti, fornendo agli utenti flessibilità nelle transazioni finanziarie.

Carding Market #3

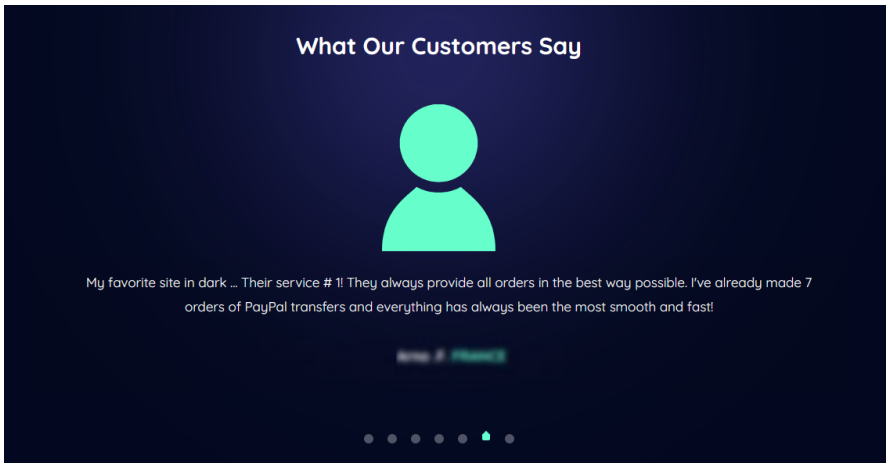
Un altro di questi mercati, opera dal 2015, offrendo una serie di prodotti e servizi illeciti, tra cui carte di credito prepagate o clonate provenienti dagli Stati Uniti e dall'Europa.



Il modus operandi di questo mercato coinvolge un team esperto nell'inserimento di dispositivi di skimming negli sportelli bancomat degli Stati Uniti e dell'Europa. Questi dispositivi sono progettati per catturare in modo subdolo le informazioni delle carte di credito degli utenti ignari, che vengono poi utilizzate per creare carte di credito clonate per transazioni fraudolente.

Inoltre, conduce attacchi di phishing su PayPal. Questi attacchi coinvolgono la distribuzione di email ingannevoli ai titolari di account PayPal, allettandoli a divulgare informazioni sensibili dell'account sotto falsi pretesti. Una volta ottenute, queste informazioni vengono sfruttate per accedere e svuotare i saldi degli account delle vittime.

Nonostante la natura illegale delle sue operazioni, questo mercato si presenta come un punto di riferimento fidato e sicuro all'interno del DarkNet, rivolgendosi a una clientela alla ricerca di anonimato e guadagni finanziari illeciti. Promesse di spedizioni in tutto il mondo, protezione della privacy garantita e supporto clienti attivo 24 ore su 24 vengono utilizzate per attirare individui ignari a interagire con i loro servizi.



Ci sono 4 opzioni disponibili sul mercato:

Carte di Credito Prepagate:

Le carte di credito prepagate offrono agli utenti una modalità sicura e flessibile per gestire le proprie finanze. Queste carte non sono associate a un conto bancario e consentono agli utenti di caricare denaro sulla carta in anticipo, stabilendo così un limite di spesa.

Carte di Credito Clonate:

Le carte di credito clonate sono associate a un conto bancario esistente e hanno una durata di utilizzo limitata. Queste carte sono create duplicando le informazioni di una carta di credito esistente e possono essere utilizzate per fare acquisti online o in negozio, nonché per prelevare contanti dagli sportelli ATM. Tuttavia, il mercato underground consiglia di utilizzare tutto il denaro caricato sulla carta entro il periodo di validità, che di solito è di 30 giorni dalla prima transazione.

Trasferimenti di Denaro PayPal:

I trasferimenti di denaro tramite PayPal offrono una modalità rapida e affidabile per inviare fondi tra utenti: i trasferimenti avvengono entro 2 ore dal momento del pagamento.

Trasferimenti di Denaro Western Union:

I trasferimenti di denaro tramite Western Union consentono di inviare fondi in tutto il mondo dove è disponibile il servizio Western Union.

Per quanto riguarda la spedizione, ci sono diverse modalità:

Spedizione Gratuita
Costo: Gratuito
Tempo di Spedizione: 5-8 giorni

Spedizione Express
Costo: $20
Tempo di Spedizione: 3-5 giorni

Spedizione Con Consegna Il giorno seguente
Costo: $40
Tempo di Spedizione: 1-2 giorni

Le opzioni di spedizione offerte forniscono ai clienti la flessibilità di scegliere la velocità di consegna più adatta alle proprie esigenze, come funziona in un vero e proprio negozio.

Infine, il sito presenta una sezione dedicata alle FAQ che fornisce una panoramica dettagliata dei servizi offerti da questa piattaformaLa piattaforma accetta esclusivamente pagamenti in Bitcoin, considerati il metodo più anonimo e popolare per questo tipo di transazioni. Bankor offre la possibilità di ricevere le carte direttamente a casa propria o di optare per la consegna in un punto di ritiro, garantendo così un livello aggiuntivo di anonimato.

Per quanto riguarda il trasferimento di denaro tramite PayPal o Western Union, l'azienda assicura la sicurezza dei fondi provenienti da account puliti e verificati, garantendo che non vi sia traccia dell'origine dei fondi. Inoltre, offre una garanzia per le carte difettose e una varietà di opzioni per il prelievo giornaliero, a seconda del tipo di carta.

Per quanto riguarda la sicurezza, le carte prepagate sono considerate a rischio zero, mentre le carte clonate comportano un rischio maggiore per coloro che non hanno esperienza nell'utilizzo di questo tipo di carte. Bankor offre anche la possibilità di ricevere le informazioni digitali delle carte senza la necessità di ricevere la carta fisica e consente il ricaricamento delle carte prepagate, anche se viene applicata una commissione del 10%.

Tuttavia, l'utilizzo delle carte clonate comporta rischi aggiuntivi, soprattutto nell'uso online, e l'azienda sconsiglia tale pratica a coloro che non hanno esperienza.

Infine, per l'acquisto di Bitcoin, Bankor consiglia varie piattaforme online, tra cui localbitcoins.com, coinbase.com o cex.io.

MALWARE/PHISHING/RANSOMWARE

Tra la vasta gamma di prodotti che possiamo trovare, primari sono i kit di malware, phishing, ransomware, la vendita e la ricerca di exploit e zero-day. Vari tipi di malware, come trojan, InfoStealer, spyware e worm, sono venduti a criminali informatici. Questi strumenti vengono utilizzati per diverse finalità malevole, tra cui il furto di dati sensibili. La disponibilità di malware su queste piattaforme facilita la proliferazione di attacchi sofisticati, rendendo più difficile la difesa per le vittime.

Il phishing è una tecnica di ingegneria sociale che induce le vittime a rivelare informazioni sensibili, come credenziali di accesso e dati finanziari, attraverso comunicazioni ingannevoli che sembrano legittime. I kit di phishing sono venduti completi di modelli di email, pagine di login false e strumenti di automazione, rendendo accessibili queste tecniche anche ai cybercriminali meno esperti. Questo ha portato a un aumento delle campagne di phishing su larga scala, con gravi ripercussioni per la sicurezza delle informazioni.

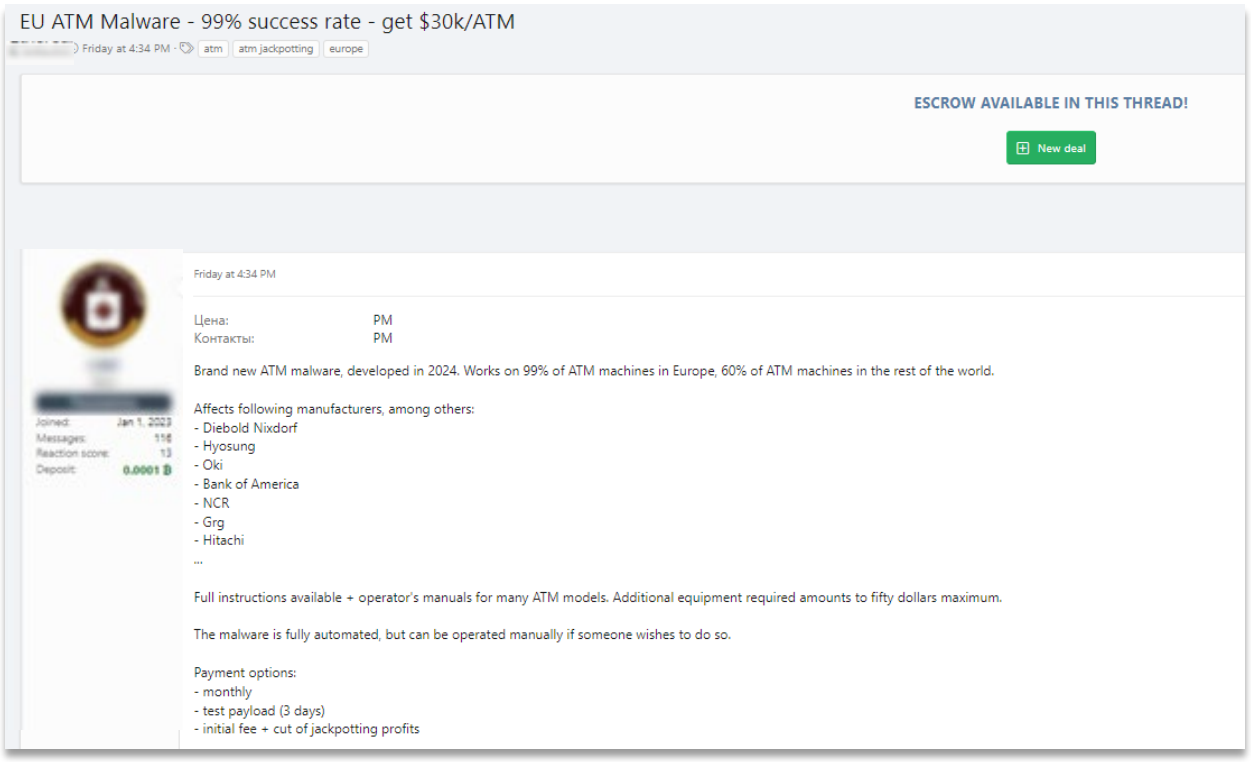
I mercati underground offrono anche ransomware-as-a-service (RaaS), un modello in cui sviluppatori esperti forniscono il malware a criminali meno competenti in cambio di una percentuale del riscatto. Questo ha reso il ransomware una delle minacce più pervasive e distruttive, colpendo individui, aziende e infrastrutture critiche in tutto il mondo.

Infine, gli exploit sono codici che sfruttano vulnerabilità in software o sistemi operativi per ottenere accesso non autorizzato o eseguire codice malevolo. Le vulnerabilità zero-day sono sconosciute ai produttori del software, rendendole particolarmente preziose e pericolose: l'accesso a questi strumenti permette di eseguire attacchi altamente sofisticati, che possono rimanere non rilevati per lunghi periodi.

Di seguito alcuni esempi di post su tre dei forum più famosi.

Malware market #1

Il post di seguito promuove un malware ATM sviluppato nel 2024, capace di compromettere una vasta gamma di macchine in tutta Europa (99%) e nel resto del mondo (60%). Il malware è compatibile con numerosi produttori di ATM, tra cui Diebold Nixdorf, Hyosung, Oki, Bank of America, NCR, Grg, e Hitachi, tra gli altri. Questo livello di compatibilità suggerisce un'ampia ricerca e sviluppo da parte degli autori del malware per assicurare la sua efficacia su vari modelli e marchi di ATM.

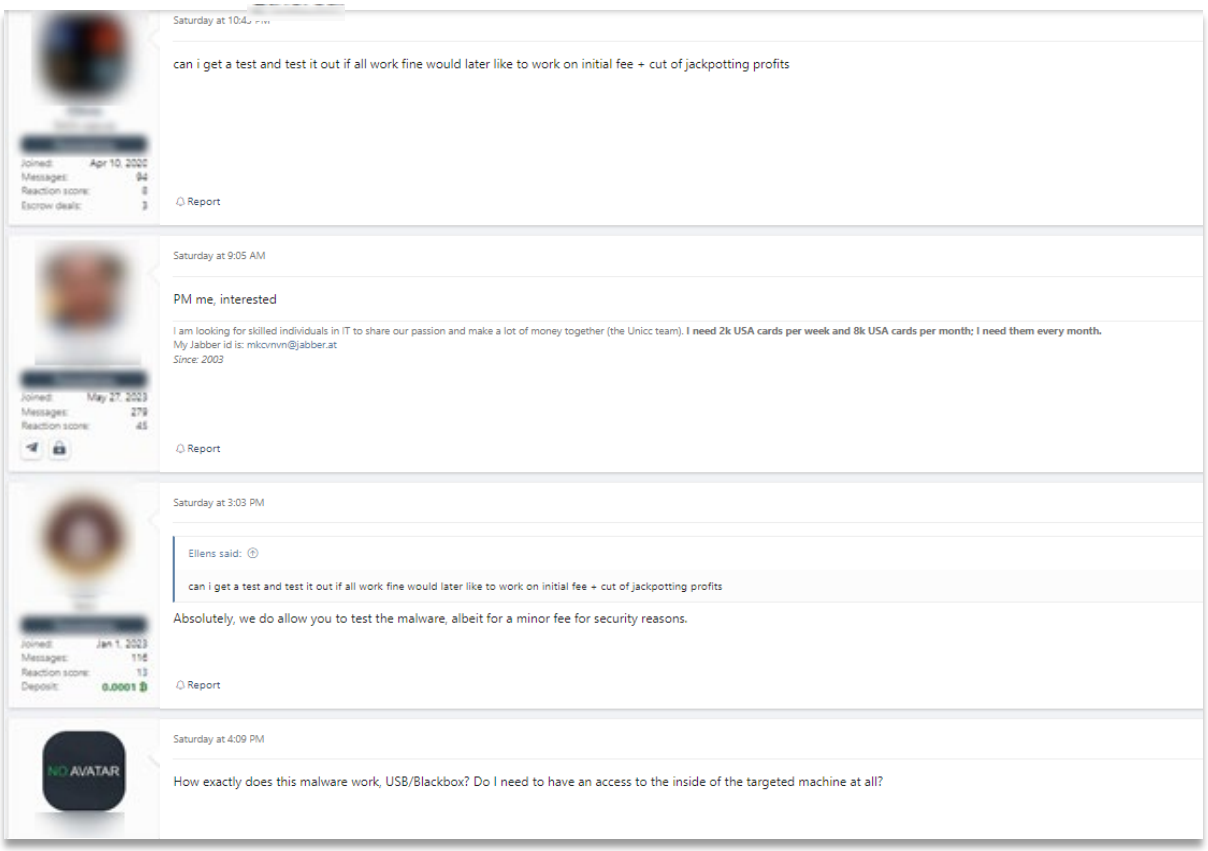


Viene descritto come completamente automatizzato, ma con la possibilità di essere operato manualmente se necessario, e vengono fornite istruzioni dettagliate e manuali operativi per molti modelli di ATM, rendendo più semplice l'implementazione anche per chi ha poca esperienza.

Il post afferma che eventuali risorse aggiuntive necessarie avrebbero un costo massimo di cinquanta dollari, indicando che l'attacco è relativamente economico da realizzare. Questo fattore potrebbe contribuire a un aumento degli attacchi, poiché abbassa significativamente la barriera economica all'entrata per i criminali.

Il venditore offre diverse opzioni di pagamento, tra cui:

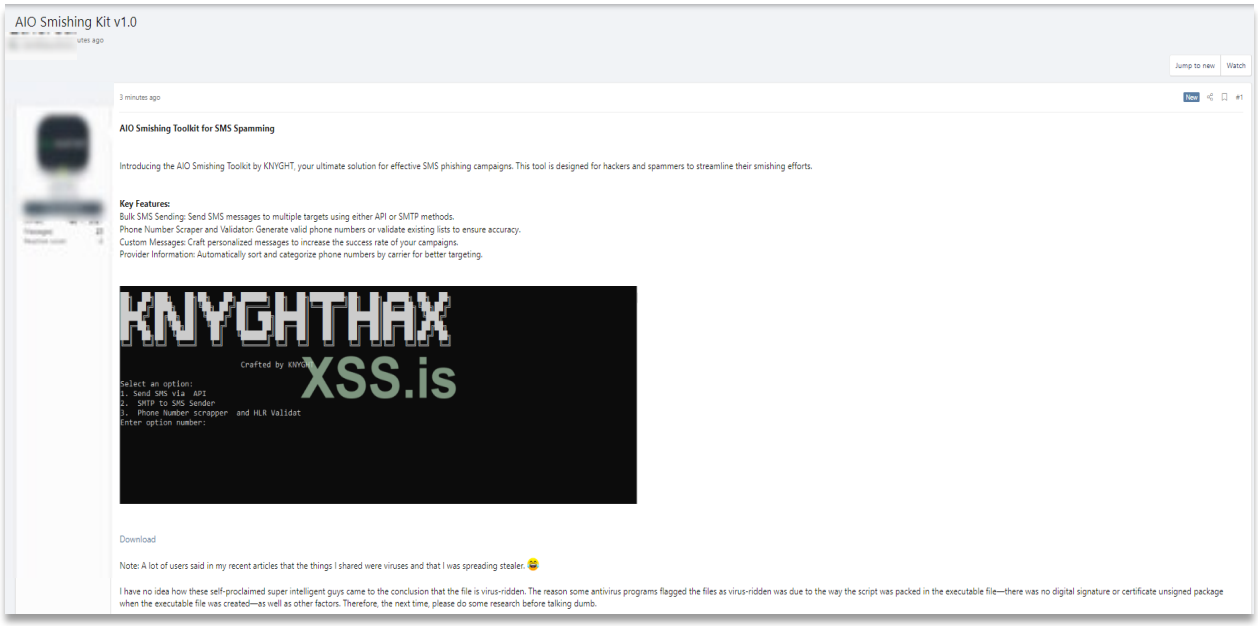
- Abbonamento mensile
- Test di tre giorni del payload
- Tariffa iniziale più una percentuale dei profitti ottenuti dal jackpotting



Queste opzioni flessibili indicano un modello di business ben pianificato, volto a massimizzare i profitti e a rendere l'offerta attraente per diversi tipi di clienti, dai piccoli criminali ai gruppi organizzati. La pubblicazione di questo annuncio è infatti un chiaro segnale di come il crimine informatico stia diventando sempre più sofisticato e accessibile.

Altro annuncio pubblicato su questo mercato, scritto in modo dettagliato e con un tono che cerca di tranquillizzare i potenziali acquirenti, offre un toolkit completo per condurre campagne di smishing. Il toolkit promette di semplificare il processo di invio di messaggi fraudolenti a un gran numero di destinatari, rendendo queste campagne più efficaci e meno dispendiose in termini di tempo e risorse. Gli utenti possono scegliere tra metodi API o SMTP per eseguire questa operazione, offrendo flessibilità a seconda delle esigenze e delle risorse a disposizione.

Include inoltre un Phone Number Scraper and Validator e la possibilità di creare messaggi personalizzati per le loro campagne, aumentando le probabilità che le vittime cadano nella trappola. I messaggi personalizzati possono sembrare più autentici e legittimi, inducendo le vittime a cliccare sui link malevoli o a fornire informazioni sensibili. Il toolkit può automaticamente ordinare e categorizzare i numeri di telefono per operatore telefonico. Questo permette un targeting più preciso, adattando i messaggi in base al provider del destinatario e aumentando l'efficacia complessiva della campagna.



Le funzionalità avanzate, il basso costo e la facilità d'uso rendono questo toolkit particolarmente pericoloso. Per contrastare efficacemente questa minaccia, è essenziale che le aziende, gli operatori di telecomunicazioni e i consumatori adottino misure proattive di protezione e consapevolezza. Solo attraverso uno sforzo concertato e continuo sarà possibile mitigare l'impatto di strumenti di smishing come questo.

Di seguito invece un annuncio che offre un servizio avanzato di gestione di Evilginx, un toolkit di phishing noto per la sua capacità di aggirare l'autenticazione a due fattori catturando i cookie di sessione della vittima. Questo consente agli attaccanti di accedere agli account senza bisogno di conoscere le credenziali o di passare attraverso la 2FA. Per coloro che vogliono configurare Evilginx2 (versione 3.0 o successiva), il post menziona che ci sono ulteriori passaggi per migliorare la sicurezza operativa (OPSEC). Questo indica che il venditore fornisce non solo il toolkit, ma anche supporto esperto per l'implementazione e l'uso sicuro del software.

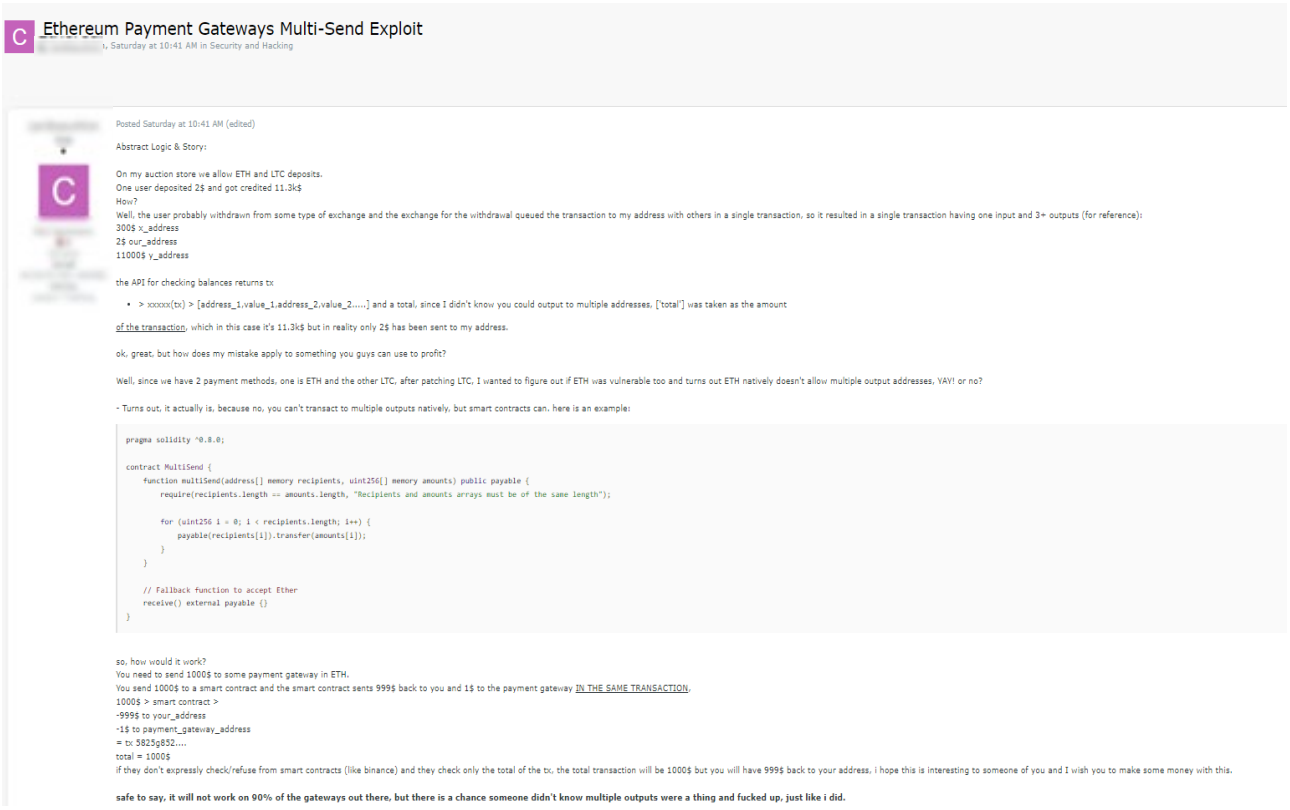
Le tecniche di phishing avanzate che aggirano la 2FA possono compromettere account che gli utenti ritengono altamente sicuri, come quelli bancari e di posta elettronica.

Malware market #2

L'altro forum molto famoso e noto in particolar modo per la vendita di exploit e 0day è il secondo mercato tracciato.

Nel post di seguito si condivide con la community una potenziale misconfiguration da sfruttare negli smart contract per transazioni ETH e LTC, che consentirebbe la manipolazione degli output verso diversi wallet.

L'incidente descritto nel post riguarda un utente che ha depositato solo 2$ ma è stato erroneamente accreditato con 11.3k$, si condivide pertanto le informazioni a disposizione con la community che potrà ricercare tali misconfiguration e potenzialmente abusarne.



Ethereum Payment Gateways Multi-Send Exploit

[redacted], Saturday at 10:41 AM in Security and Hacking

Posted Saturday at 10:41 AM (edited)

Abstract Logic & Story:

On my auction store we allow ETH and LTC deposits.
One user deposited 2$ and got credited 11.3k$
How?
Well, the user probably withdrawn from some type of exchange and the exchange for the withdrawal queued the transaction to my address with others in a single transaction, so it resulted in a single transaction having one input and 3+ outputs (for reference):
300$ x_address
2$ our_address
11000$ y_address

the API for checking balances returns tx

- > xxxxx(tx) > [address_1,value_1,address_2,value_2.....] and a total. since I didn't know you could output to multiple addresses, ['total'] was taken as the amount

of the transaction, which in this case it's 11.3k$ but in reality only 2$ has been sent to my address.

ok, great. but how does my mistake apply to something you guys can use to profit?

Well, since we have 2 payment methods, one is ETH and the other LTC, after patching LTC, I wanted to figure out if ETH was vulnerable too and turns out ETH natively doesn't allow multiple output addresses, YAY! or no?

- Turns out, it actually is, because no, you can't transact to multiple outputs natively, but smart contracts can. here is an example:

```
pragma solidity ^0.8.0;

contract MultiSend {
    function multiSend(address[] memory recipients, uint256[] memory amounts) public payable {
        require(recipients.length == amounts.length, "Recipients and amounts arrays must be of the same length");

        for (uint256 i = 0; i < recipients.length; i++) {
            payable(recipients[i]).transfer(amounts[i]);
        }
    }

    // Fallback function to accept Ether
    receive() external payable {}
}
```

so, how would it work?
You need to send 1000$ to some payment gateway in ETH.
You send 1000$ to a smart contract and the smart contract sents 999$ back to you and 1$ to the payment gateway IN THE SAME TRANSACTION.
1000$ > smart contract >
-999$ to your_address
-1$ to payment_gateway_address
= tx: 5825g852....
total = 1000$
if they don't expressly check/refuse from smart contracts (like binance) and they check only the total of the tx, the total transaction will be 1000$ but you will have 999$ back to your address. I hope this is interesting to someone of you and I wish you to make some money with this.

safe to say, it will not work on 90% of the gateways out there, but there is a chance someone didn't know multiple outputs were a thing and fucked up, just like i did.

L'annuncio di vendita di un exploit 0day per Local Privilege Escalation (LPE) su Windows è un'espressione di un mercato attivo per vulnerabilità informatiche, che rappresenta una minaccia significativa per la sicurezza informatica. Il venditore offre il codice sorgente completo di uno 0day LPE funzionante su Windows 10, Windows 11 e tutte le versioni di Windows Server. L'annuncio sottolinea che si tratta di un exploit LIVE, il che significa che è attivamente sfruttabile e non è ancora stato rilevato o corretto da Microsoft e invita potenziali acquirenti a contattarlo su diverse piattaforme per ulteriori dettagli e per visualizzare un video di dimostrazione.

Il prezzo richiesto per l'exploit è di $100.000 e il venditore fornisce diversi modi di contatto, inclusi un canale Telegram, un account XMPP e un ID TOX, offrendo così diversi canali per una potenziale transazione.

L'esistenza di un potenziale exploit zero-day per una vasta gamma di sistemi Windows rappresenta una minaccia significativa tramite cui un attaccante eseguire azioni dannose come l'installazione di malware, il furto di dati sensibili o il danneggiamento del sistema.

Il post di seguito riguarda la vendita di un exploit 0day per dispositivi iOS, con un particolare focus su iMessage che sfrutta una vulnerabilità senza la necessità di alcuna azione da parte dell'utente. Il payload dell'attacco è inviato tramite SMS e offre un controllo completo sul dispositivo iOS.

L'annuncio offre ulteriori dettagli e una prova di veridicità tramite contatto su Telegram, contattando l'utente indicato, sottolineando che i "time wasters" (ossia coloro che non sono seriamente interessati all'acquisto) devono astenersi.

[Vendi] iOS Exploit 0day 0Click

[redacted], 3 maggioin [Software]: malware, exploit, bundle, cripte

[redacted]

Attività
xaxaxe / hacking
Deposito
0.000100Ƀ

Pubblicato3 maggio

#0day #Sfrutta

Sfruttamento di iMessage

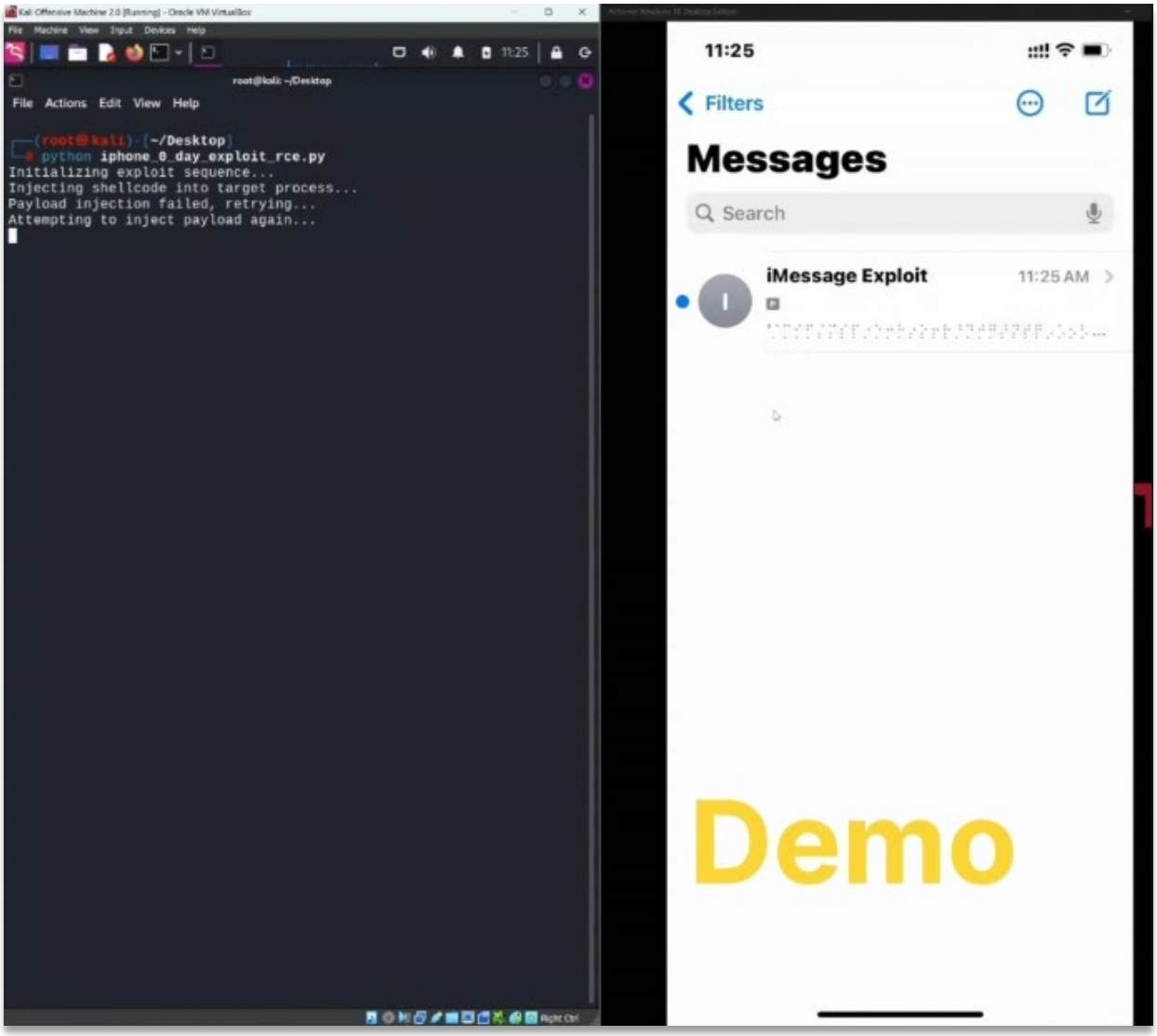
#Tipo di attacco: 0click
#Carico utile: SMS
#Controllo sul dispositivo
#supporta iOS 17.x

Disponibile per la vendita

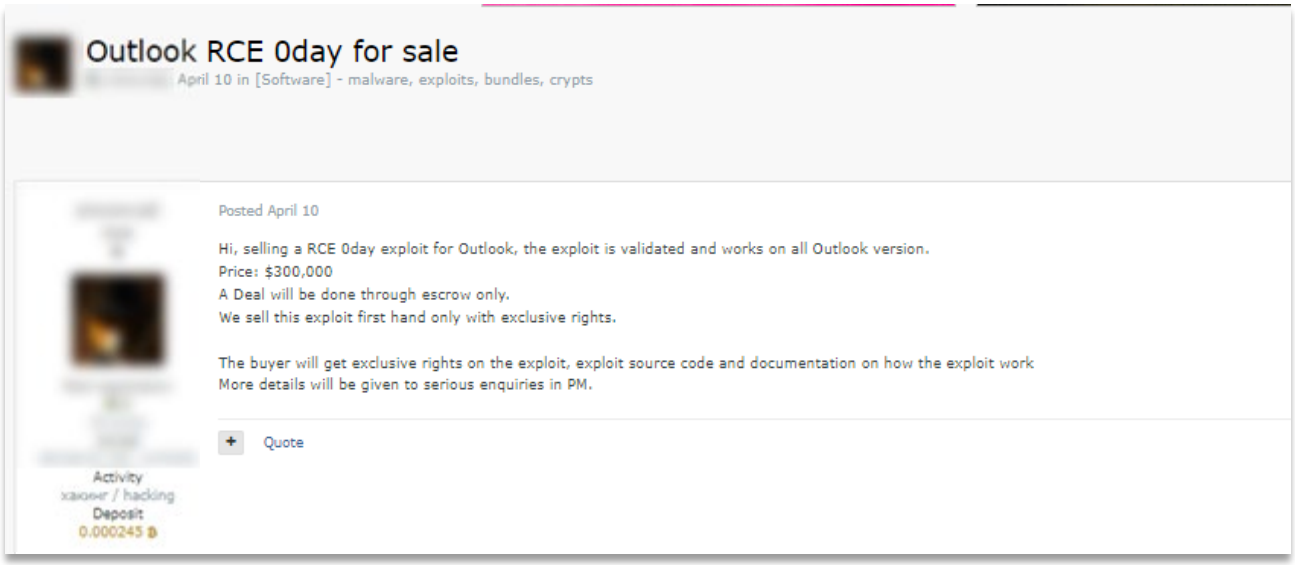
PoC e ulteriori dettagli contattaci **telegramma : DimitryCBL**

Chi vuole può prendere da me il PoC e guardarlo e porre qualsiasi domanda relativa all'exploit.
Quindi discutere sull'acquisto dell'exploit

perditempo state alla larga.



Un altro annuncio offre un exploit RCE zero-day per Microsoft Outlook che consente l'esecuzione di codice da remoto, il che significa che un attaccante può potenzialmente prendere il controllo del computer della vittima senza che essa sia a conoscenza di ciò che sta accadendo. Il prezzo richiesto è di $300,000.



Per aggiungere ulteriore pericolo, il venditore impone condizioni rigide: l'acquirente otterrà diritti esclusivi sull'exploit, il codice sorgente e la documentazione dettagliata su come funziona. Questo significa che l'exploit potrebbe essere utilizzato per scopi malevoli senza alcuna restrizione. Inoltre, l'annuncio specifica che la transazione avverrà esclusivamente tramite escrow.

Un attacco utilizzando questo exploit potrebbe portare al furto di dati sensibili, alla diffusione di malware e al controllo completo del sistema della vittima. Questo potrebbe avere conseguenze finanziarie e reputazionali gravi per gli individui colpiti. La vendita di un exploit zero-day di questo tipo mette in luce una serie di problemi più ampi nella comunità della sicurezza informatica, rivelando il buio mondo del mercato nero del cybercrime, dove le vulnerabilità vengono comprate e vendute come merci.

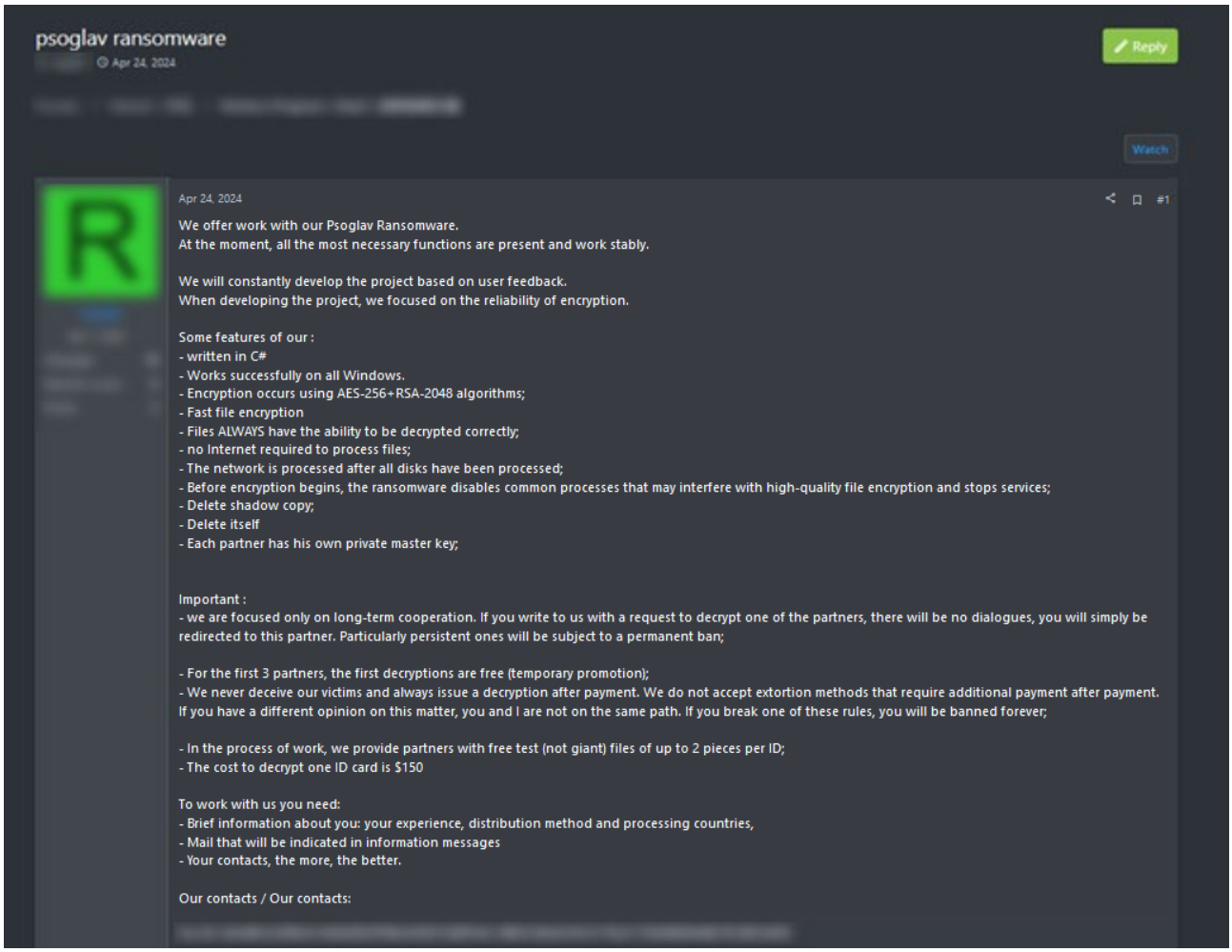
Malware market #3

A differenza di altri forum che invece non consentono la pubblicazione di port riguardanti attività Ransomware, su questo mercato troviamo anche annunci di questo tipo.

Il post di seguito offre un'ampia panoramica del ransomware Psoglav, evidenziando le sue caratteristiche, le modalità operative e le condizioni di cooperazione per i potenziali partner. Psoglav è presentato come uno strumento sofisticato e potente, progettato per crittografare i file delle vittime e richiedere un riscatto per la decrittografia. Il ransomware è dichiarato funzionante su tutte le versioni di Windows.

Psoglav utilizza una combinazione di algoritmi di crittografia avanzati: AES-256 e RSA-2048 e

promette una rapida crittografia dei file, assicurando al contempo che i file possano essere sempre decrittografati correttamente una volta pagato il riscatto. Questo è un punto cruciale per mantenere una sorta di "fiducia" tra i criminali informatici e le loro vittime.



Una caratteristica distintiva di Psoglav è la capacità di funzionare senza necessitare di una connessione Internet per la crittografia dei file. Questo rende il ransomware più difficile da rilevare e bloccare, poiché non comunica con server esterni durante l'operazione. Prima di iniziare la crittografia, Psoglav disabilita i processi comuni e i servizi che potrebbero interferire con l'operazione. Questo garantisce che la crittografia avvenga senza interruzioni e massimizza l'efficacia dell'attacco.

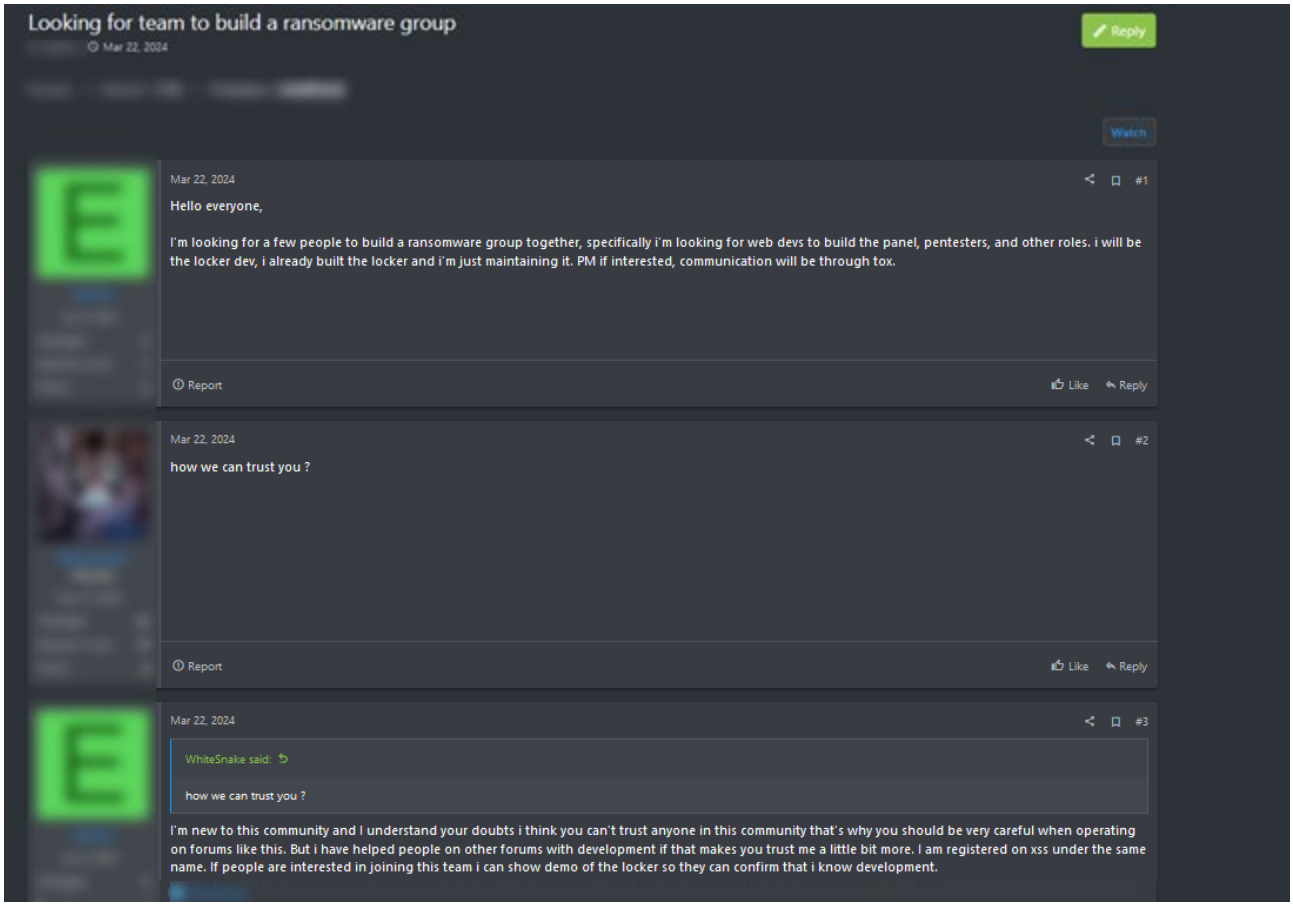
Dopo aver completato la crittografia, Psoglav si elimina automaticamente. Questo riduce il rischio di rilevamento e analisi forense del malware, proteggendo ulteriormente l'operazione.

Il team di Psoglav si dichiara interessato solo a collaborazioni a lungo termine e per incentivare nuovi partner, le prime tre collaborazioni includono decrittografie gratuite come promozione temporanea: una strategia volta ad attrarre rapidamente nuovi affiliati.

Per collaborare con il team di Psoglav, i potenziali partner devono fornire una breve descrizione della loro esperienza, i metodi di distribuzione utilizzati e i paesi in cui operano e un indirizzo email per le comunicazioni informative e altri dettagli di contatto. Maggiori sono i dettagli forniti, migliore sarà la comunicazione e la cooperazione.

Questo tipo di annunci evidenzia la necessità di una vigilanza continua e di misure di sicurezza proattive da parte di individui e organizzazioni per proteggersi da tali minacce. La complessità e la professionalità dietro questi annunci dimostrano l'evoluzione continua delle tecniche di ransomware e l'importanza di rimanere aggiornati sulle migliori pratiche di sicurezza informatica.

Possiamo inoltre notare come gli annunci non si limitano alla vendita di servizi o strumenti, ma vi è anche la ricerca attiva di collaboratori con competenze specifiche per la creazione di un team ransomware. L'autore del post cerca di formare un gruppo composta da diversi esperti, evidenziando la necessità di sviluppatori web, pentester e altri ruoli chiave per portare avanti l'operazione ransomware.



L'obiettivo principale del post è dunque reclutare individui con competenze diverse per costruire un gruppo ransomware. L'autore si presenta come il responsabile dello sviluppo del locker e afferma di essere nuovo nel forum. Per costruire fiducia, l'autore menziona di aver aiutato altre persone su altri forum con lo sviluppo. Viene anche indicata la presenza su un altro noto forum, il primo mercato, suggerendo una reputazione preesistente che può essere verificata.

L'autore specifica che le comunicazioni avverranno tramite Tox e offre una dimostrazione del ransomware già sviluppato per confermare le sue competenze in sviluppo. Questo è un tentativo di legittimare la propria proposta e attrarre collaboratori seri mostrando una prova concreta delle capacità tecniche.

Il post rappresenta un tentativo strategico di costruire un team specializzato per condurre operazioni ransomware. L'approccio dell'autore, come un vero e proprio annuncio nel surface web, combina trasparenza, prove di competenza e canali di comunicazione sicuri, ed è progettato per attrarre professionisti del cybercrimine disposti a collaborare su progetti ad alto rischio e potenzialmente molto remunerativi. La dinamica descritta nel post evidenzia l'evoluzione delle minacce ransomware verso modelli operativi più organizzati e professionali, aumentando così la necessità di strategie di difesa sempre più sofisticate da parte delle vittime potenziali.

IDENTITY LEAKS & CREDENTIAL ACCESS

Questi mercati illeciti facilitano anche la compravendita di dati personali e credenziali di accesso sottratti a milioni di utenti in tutto il mondo. Informazioni sensibili come numeri di carte di credito, password, documenti di identità e dati sanitari vengono messe in vendita, alimentando un fiorente ecosistema criminale. Questo commercio clandestino non solo mette a rischio la privacy e la sicurezza delle persone coinvolte, ma fornisce anche gli strumenti necessari per ulteriori attacchi informatici, frodi finanziarie e furti di identità su larga scala.

Leak Market #1

Il forum è progettato per offrire un accesso graduale alle informazioni in base al livello di abbonamento scelto, creando così un sistema a più livelli che permette agli utenti di accedere a dati sempre più esclusivi man mano che aumentano il loro investimento.

L'abbonamento VIP, al costo di $260, offre un accesso completo a tutte le discussioni a pagamento e alla sezione premium del forum. Questo significa che possono visualizzare tutti i link e i contenuti senza la necessità di accumulare crediti o interagire attivamente ai post, come mettere like o rispondere alle discussioni. L'upgrade del profilo ai livelli Premium e Gold elimina ulteriormente qualsiasi barriera di accesso, permettendo agli utenti di navigare liberamente tra i contenuti senza restrizioni.

Un'altra opzione di abbonamento offerta da Leakbase è l'accesso al canale Telegram privato, anch'esso al costo di $260. Questo canale esclusivo offre un flusso continuo di dati aggiornati e di alta qualità, che non sono disponibili sul forum. Inoltre, il canale contiene archivi di dati unici e di grandi dimensioni inclusi nel pacchetto Gold, offrendo così una risorsa aggiuntiva per gli utenti. Questo accesso esclusivo garantisce che gli abbonati siano sempre all'avanguardia nel mercato dei dati rubati, con informazioni che non sono reperibili pubblicamente.

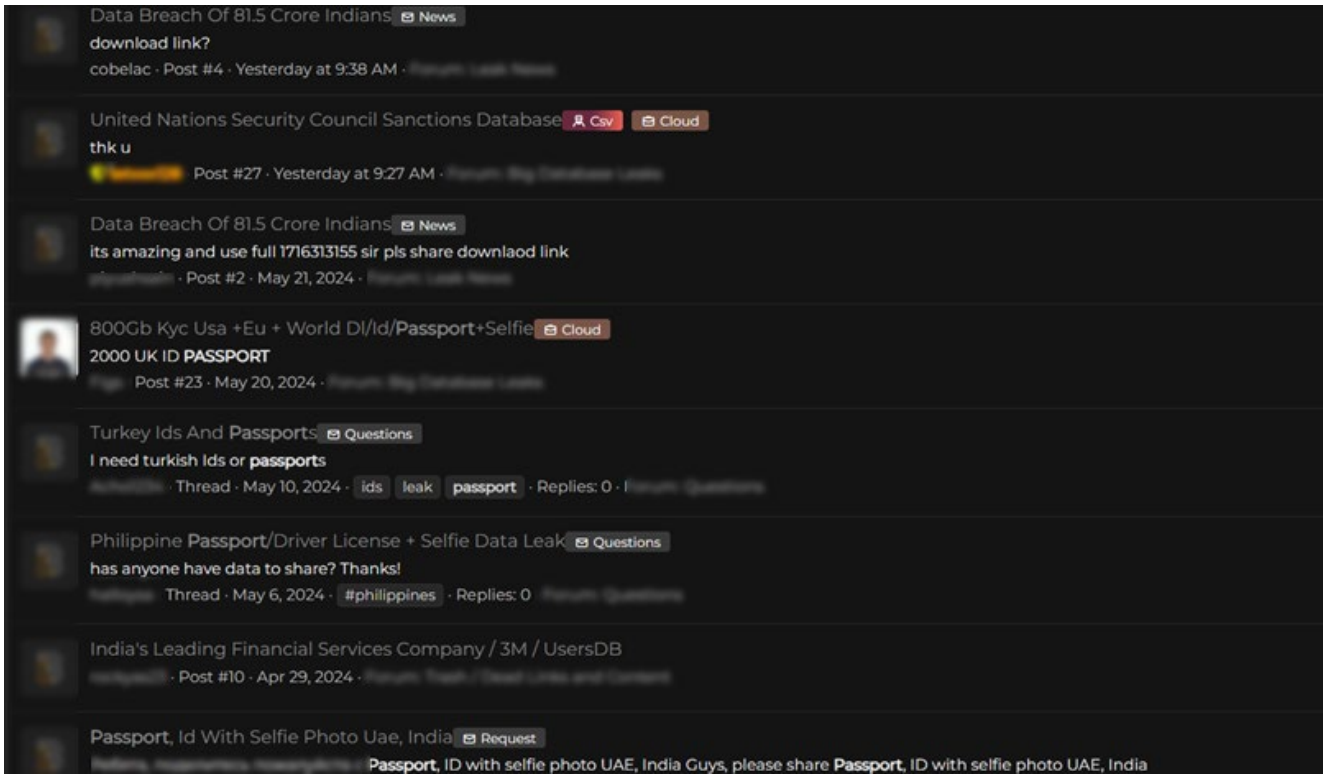
L'offerta più completa è rappresentata dal GoldPack, disponibile al prezzo di $450. Questo pacchetto include un vasto database di circa 3TB, log di circa 10TB, e pacchetti con milioni di credenziali.

La peculiarità del GoldPack è che gran parte del materiale disponibile è stato raccolto direttamente dal team di questo mercato garantendo così la qualità e l'unicità delle informazioni. Gli utenti del GoldPack beneficiano di aggiornamenti costanti e permanenti, senza necessità di pagamenti

ricorrenti. L'abbonamento include anche lo stato premium, eliminando la necessità di acquistare crediti per accedere ai contenuti e l'accesso al gruppo Telegram.

Come abbiamo potuto vedere, in questi forum gli utenti pubblicano richieste di informazioni specifiche o offrono grandi quantità di dati rubati, creando un ecosistema in cui la domanda e l'offerta di dati illegali prosperano. In uno di questi forum, Leakbase, la vendita di credenziali e documenti è primaria. In particolar modo, i dati che si possono trovare sono:

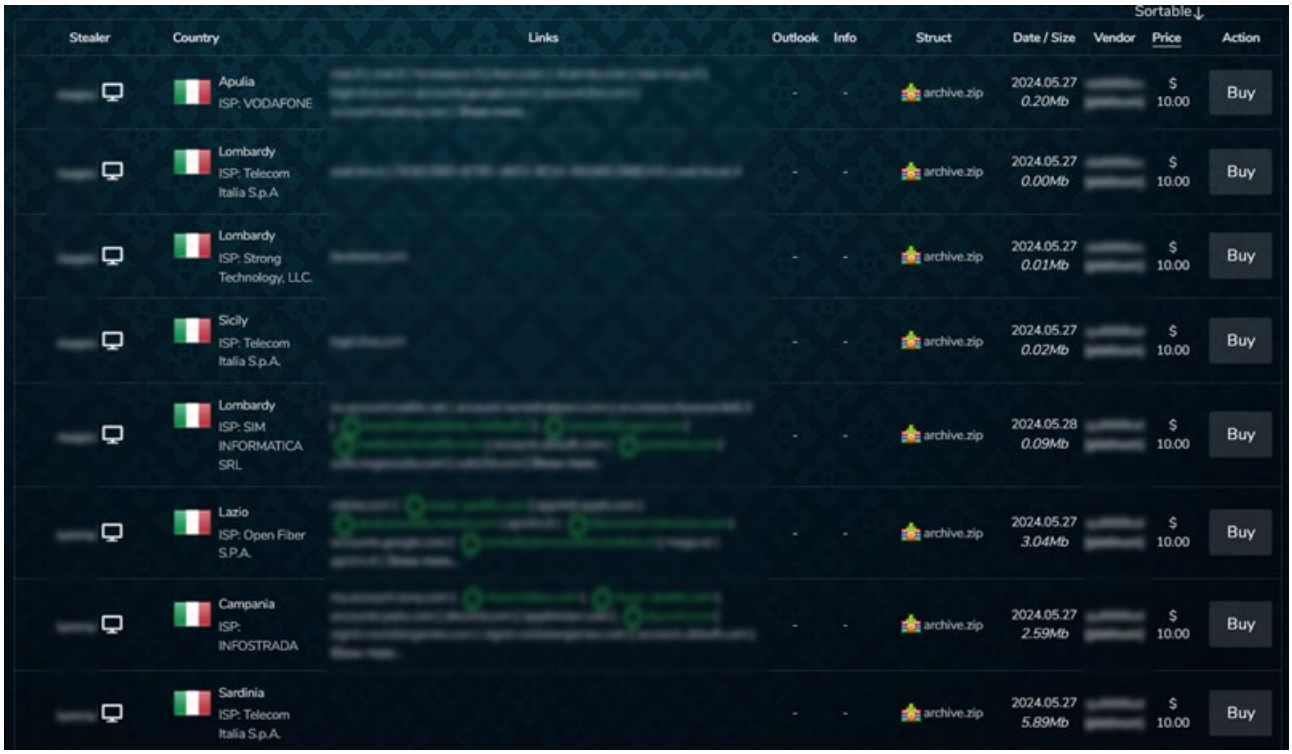
1. ***Dati Personali e di Identità**:*
    - Gli utenti cercano frequentemente informazioni dettagliate come numeri di passaporto, carte d'identità, patenti di guida, e documenti con foto. Questi dati sono particolarmente preziosi per attività di furto d'identità e frodi finanziarie. Ad esempio, richieste per ID e passaporti turchi o filippini come nello screen di seguito indicano un interesse specifico per documenti di identità autentici, utilizzabili per creare false identità.
2. ***Database di Grandi Dimensioni**:*
    - Vi è una forte domanda per database massicci contenenti milioni di record. Ad esempio, un data breach che coinvolge milioni di persone rappresenta un tesoro di informazioni utilizzabili per scopi illeciti su larga scala. Questi database possono includere dati personali, finanziari, e persino informazioni di sicurezza sociale, che sono estremamente vulnerabili a furti e abusi.
3. ***Dati Governativi e Diplomatici**:*
    - Anche le informazioni di natura governativa e diplomatica sono oggetto di scambio. Come nello screen riportato sotto a livello di esempio, database delle sanzioni del Consiglio di Sicurezza delle Nazioni Unite possono essere utilizzati per attività di spionaggio o per eludere restrizioni legali internazionali. Questi dati sono particolarmente sensibili e possono avere gravi implicazioni geopolitiche.



Leak Market #2

La sezione "Logs" sul forum di breach offre un elenco dettagliato di dati rubati provenienti da tutto il mondo: solo per l'Italia ne troviamo 65.027. Ogni voce nella lista include informazioni sullo stealer, la regione in cui è stato rubato il dato, il paese, i link associati al dato rubato e informazioni specifiche.

Questi dati rubati includono informazioni sensibili come email, dati di accesso a siti web, e altre informazioni personali che possono essere utilizzate per scopi fraudolenti.



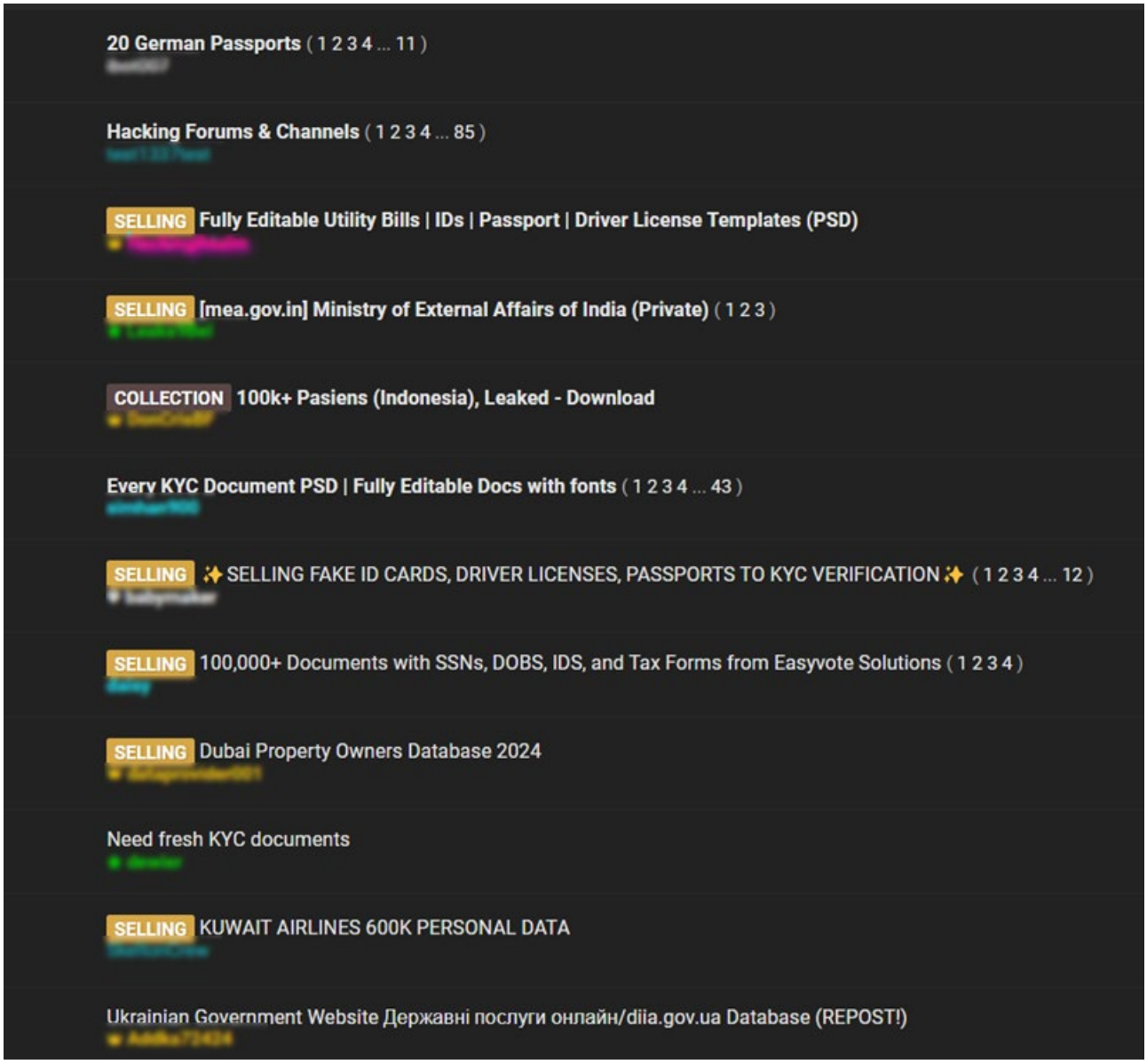
Gli stealer presenti sul secondo mercato includono una varietà di malware e software dannosi che mirano a rubare dati sensibili dagli utenti. Tra i principali stealer presenti sulla piattaforma, troviamo:

1. **Lumma**: 2.701.202 evidenze
2. **Risepro**: 1.329.147 evidenze
3. **Vidar**: 967.035 evidenze
4. **Redline**: 612.425 evidenze
5. **Stealc**: 408.104 evidenze
6. **Raccoon**: 329.214 evidenze

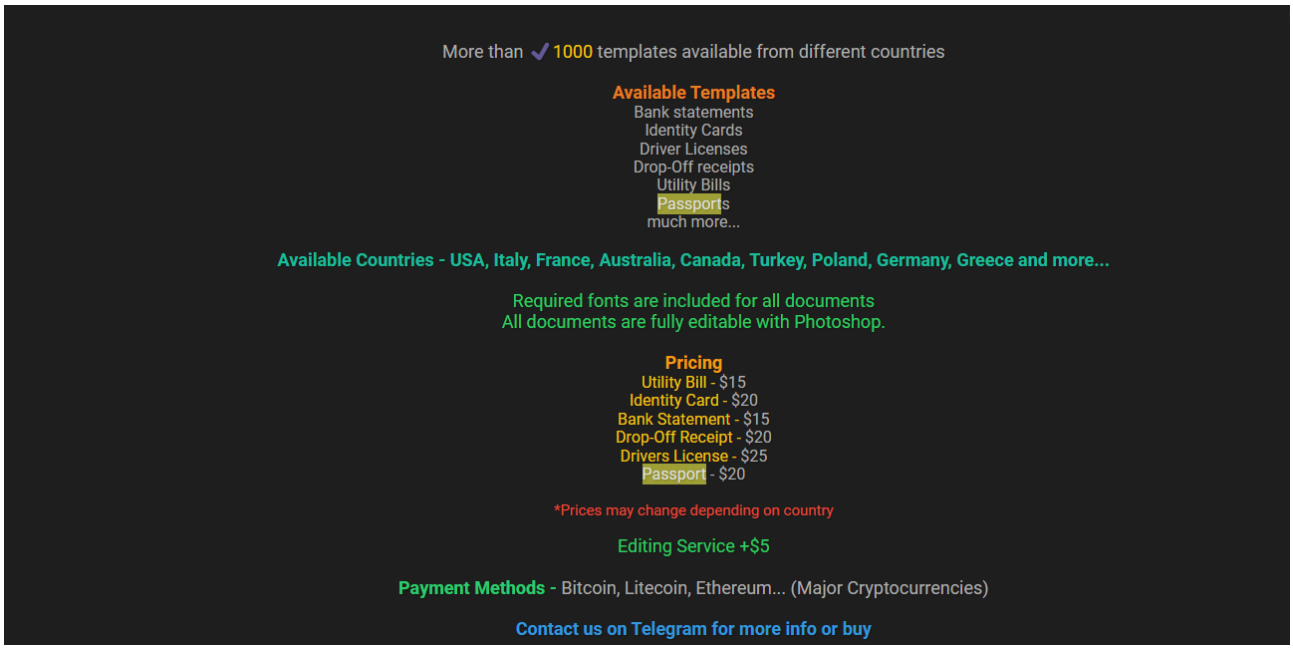
Questi stealer rappresentano una seria minaccia per la sicurezza informatica degli utenti, poiché sono progettati per rubare informazioni sensibili come dati bancari, password e informazioni personali e la vendita sui mercati underground di log ne amplifica la portata.

Leak Market #3

Il terzo mercato è un mercato online specializzato nella vendita e scambio di dati rubati e informazioni sensibili. Questo forum underground è un punto di riferimento per chi cerca di acquistare, vendere o condividere dati compromessi, documenti falsificati e altri materiali illeciti. Le principali categorie includono account compromessi, discussioni su hacking, vendita di documenti. Ogni categoria è ulteriormente suddivisa in thread che presentano offerte specifiche o richieste di dati.



Un esempio di annuncio che si può trovare si presenta come nello screen di seguito, dove vengono offerti oltre 1000 template provenienti da vari paesi. Questi documenti includono estratti conto bancari, carte d'identità, patenti di guida, ricevute di consegna, bollette e passaporti. La vasta gamma di opzioni permette agli acquirenti di trovare esattamente ciò di cui hanno bisogno per diversi scopi fraudolenti, che possono spaziare dal furto d'identità alla creazione di documenti fittizi per ingannare istituzioni finanziarie o enti governativi.



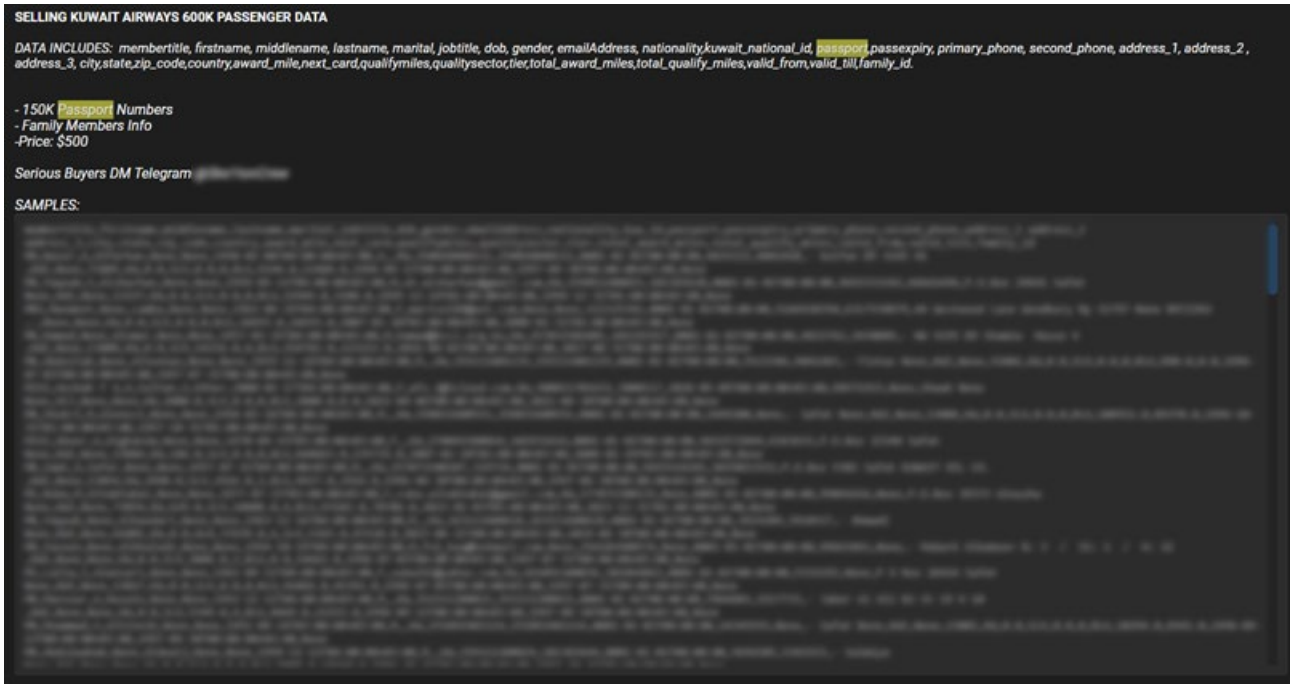
Il venditore elenca i paesi di origine dei documenti, menzionando nazioni come USA, Italia, Francia, Australia, Canada, Turchia, Polonia, Germania e Grecia, tra gli altri. Questa varietà geografica amplia il potenziale mercato, rendendo i servizi offerti appetibili a una clientela internazionale. I documenti sono completamente modificabili con Photoshop e vengono forniti con i font necessari per garantire un alto livello di autenticità visiva, essenziale per evitare il rilevamento in contesti ufficiali.

Viene presentato un listino prezzi dettagliato, con i costi dei documenti che variano in base alla tipologia e al paese di origine. Le bollette costano $15, le carte d'identità $20, gli estratti conto bancari $15, le ricevute di consegna $20, le patenti di guida $25 e i passaporti $20. Il prezzo può variare in funzione del paese, riflettendo probabilmente la complessità e il rischio associato alla falsificazione di documenti di determinate nazioni. Inoltre, il venditore offre un servizio di editing al costo aggiuntivo di $5, fornendo supporto professionale per personalizzare ulteriormente i documenti secondo le esigenze specifiche dell'acquirente e le transazioni sono accettate in criptovalute come Bitcoin, Litecoin ed Ethereum.

Altro esempio è il post di seguito che offre in vendita un database contenente dati di passeggeri Kuwait Airways, comprendente informazioni come nome, cognome, stato civile, professione, data di nascita, genere, email, nazionalità, numero di passaporto, numero di telefono, indirizzo e molti altri dettagli personali. Inoltre, il venditore specifica che il database include 150.000 numeri di passaporto e informazioni sui membri della famiglia dei passeggeri.

Il prezzo del database è fissato a $500 e il venditore invita gli acquirenti a contattarlo tramite Telegram.

Come prova della genuinità del database, vengono forniti alcuni esempi di dati di passeggeri Kuwait Airways, con informazioni dettagliate su diverse persone.



Questo mercato è una rappresentazione dettagliata del crimine informatico, dove avviene quotidianamente il commercio di dati rubati e documenti falsi. La struttura del forum e la vasta gamma di offerte dimostrano l'esistenza di un mercato altamente organizzato e in continua espansione, nonostante i frequenti tentativi di smantellamento da parte delle autorità. Questo mercato è sostenuto da una domanda costante di informazioni sensibili.

CONCLUSIONE

L'analisi delle categorie di mercati, dalla droga al carding, dal malware al furto di identità e credenziali, rivela un panorama complesso e in continua evoluzione dell'economia digitale illecita. Ogni categoria rappresenta un settore lucrativo per coloro che operano nell'ombra, offrendo una gamma di prodotti e servizi illeciti a una clientela sempre più ampia.

Attraverso l'esame abbiamo potuto osservare da vicino le dinamiche commerciali, le sfide e le implicazioni di queste attività illegali. Tuttavia, ciò che emerge chiaramente è che la natura volatile e clandestina dei mercati Dark Web rende difficile per le autorità rintracciarli tempestivamente: Breach Forum è un esempio lampante delle sfide che le autorità affrontano nel contrastare i mercati illegali. Nonostante i ripetuti sforzi per smantellare il forum, continua a operare e a fornire una piattaforma per il commercio di dati sensibili e documenti falsi. Questo evidenzia la difficoltà nel monitorare e regolare tali attività nell'ambiente digitale oscuro e decentralizzato.

Inoltre, l'analisi rivela una crescente professionalizzazione e specializzazione delle attività illecite. Da fornitori di droga a esperti di hacking e venditori di dati personali, ciascuna categoria di mercato è supportata da una vasta rete di attori specializzati.

CREDITS

Analysis by:

Riccardo D'Ambrosio
Riccardo Michetti
Martina Fonzo

Technical Contributors:

Soc team di Tinexta Cyber

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

www.tinextacyber.com
info@tinextacyber.com

Milano
Vetra Building, Via Fernanda Wittgens, 2, 20123

+39 02 6666 1442