ANNUAL

Dark Web Report

SOCRadar®
Your Eyes Beyond

socradar.io

Executive Summary

Top Takeaways

- The United States is the primary target across multiple threat types, accounting for 41.42% of ransomware attacks which is a drop from 53,30% in 2024; and 19.91% of Dark Web news which is an increase from 18,17% in 2024.

- Public Administration is the most exposed industry on the Dark Web at 12.85%, indicating sustained pressure on government institutions through data leaks. In 2024, Public Administration was on the third spot with 11,17% of the posts. We don't see a huge increase in terms of percentage but we see an upward trend.

- Data driven crime dominates the ecosystem. Data and database related threats represent 64.06% of Dark Web activity, while selling posts account for 59.32%, showing a clear focus on direct monetization.

- Last year Akira Ransomware was not even in the Top 3 but in 2025 they took the first place in terms of activity with 8.35% of ransomware attacks. In general the ransomware market is fragmented. This fragmented threat landscape is increasing unpredictability and operational risk for defenders.

- Stealer malware impacts scale driven platforms and regions. Major platforms like Facebook and Google dominate logs, while India, Brazil, and Indonesia lead infections, reflecting user scale and weak endpoint protection.

- Entry barriers across most illicit markets remain very low. Stealers, spam services, SMS abuse, and phishing panels start at minimal prices, which enables mass participation and supports large scale, low skill campaigns.

- Financial assets are valued by usability, not rarity. Widely adopted payment accounts and US or UK credit cards command higher prices due to acceptance and fraud success, while other regions stay at a lower price range.

Why the Dark Web Matters

This Annual Dark Web Report presents a structured view of illicit activity observed across major underground markets during 2025.

The Dark Web is crucial in shaping the modern cyber threat landscape. It is often romanticized as a shadowy underworld, but it is better understood as a marketplace where exploits, vulnerabilities and sensitive data are traded.

Over the years, hacking has transformed. It has shifted from being about technical brilliance and sophistication to something far simpler: leveraging opportunities. Hackers today are not spending countless hours planning detailed attacks. Instead, they are opting for a more convenient and cost-effective approach. By purchasing valid credentials on the Dark Web, they bypass the need for complex exploits.

Following this trend, we designed this report as a reference for decision makers and security teams. It focuses on measurable trends, pricing behavior, and threat concentration rather than individual cases. All findings are based on our continuous monitoring of Dark Web forums, marketplaces, and related ecosystems.

The Dark Web has become a hub for distributing everything attackers need to carry out their operations and our report covers a wide range of illicit goods and services that support threat actors.

These include malware, exploits, and zero day markets that enable initial compromise. We also examined spamming, DDoS, phishing kits, and hacking services that scale attacks and reduce attacker effort. Financial crime is addressed through analysis of credit cards, online payment accounts, money laundering services, and fraud related offerings. Personal data, digital goods, and social media accounts are included to reflect identity abuse and influence driven threats. Emerging areas such as AI tools and AI related services are also tracked to fully capture today's threat landscape.

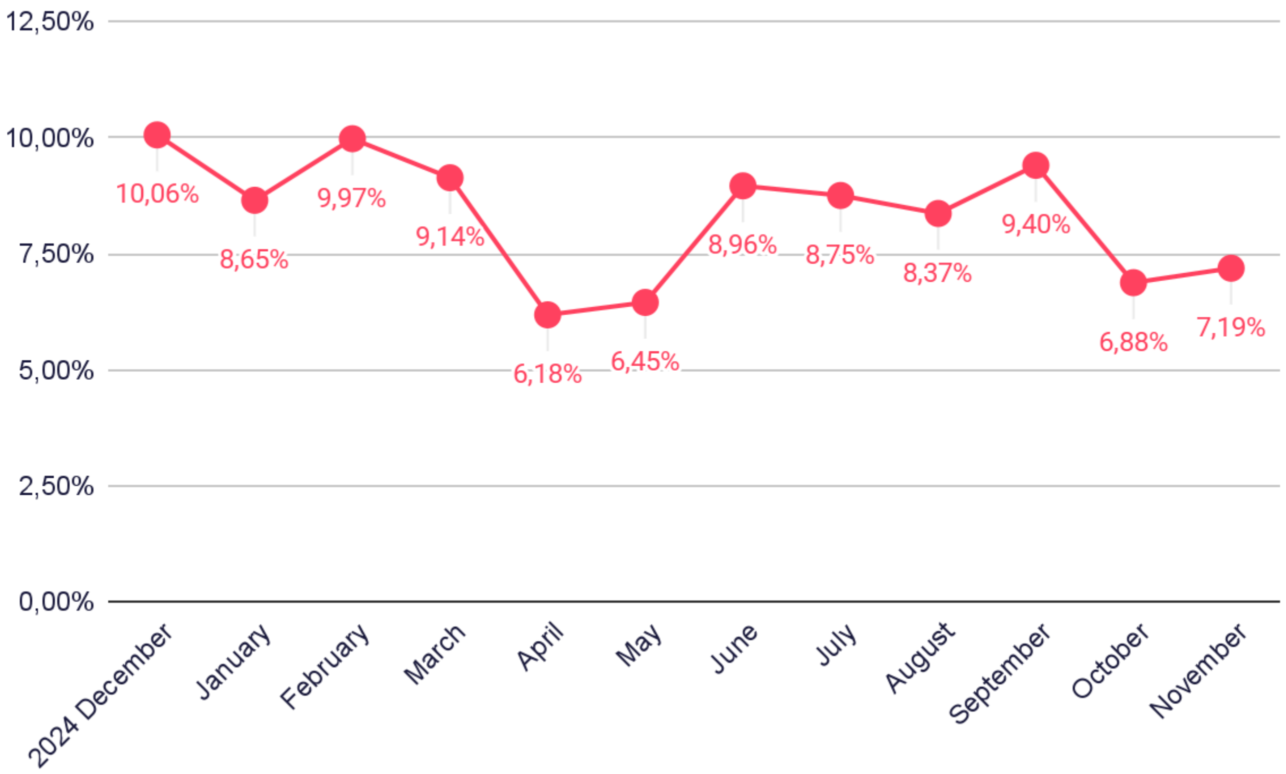
To address these challenges, organizations must fundamentally rethink their approach to cybersecurity since monitoring the Dark Web can give them the early signs of an attack.

Dark Web pricing data is inherently volatile and subject to variation based on threat actor reputation, negotiation practices, market dynamics, and point-in-time availability. To avoid overstating precision and to ensure clarity, prices in this report are presented as averages or ranges rather than exact figures. We took this approach to reflect underlying market uncertainty while improving readability and supporting intelligence assessments.

Dark Web Markets

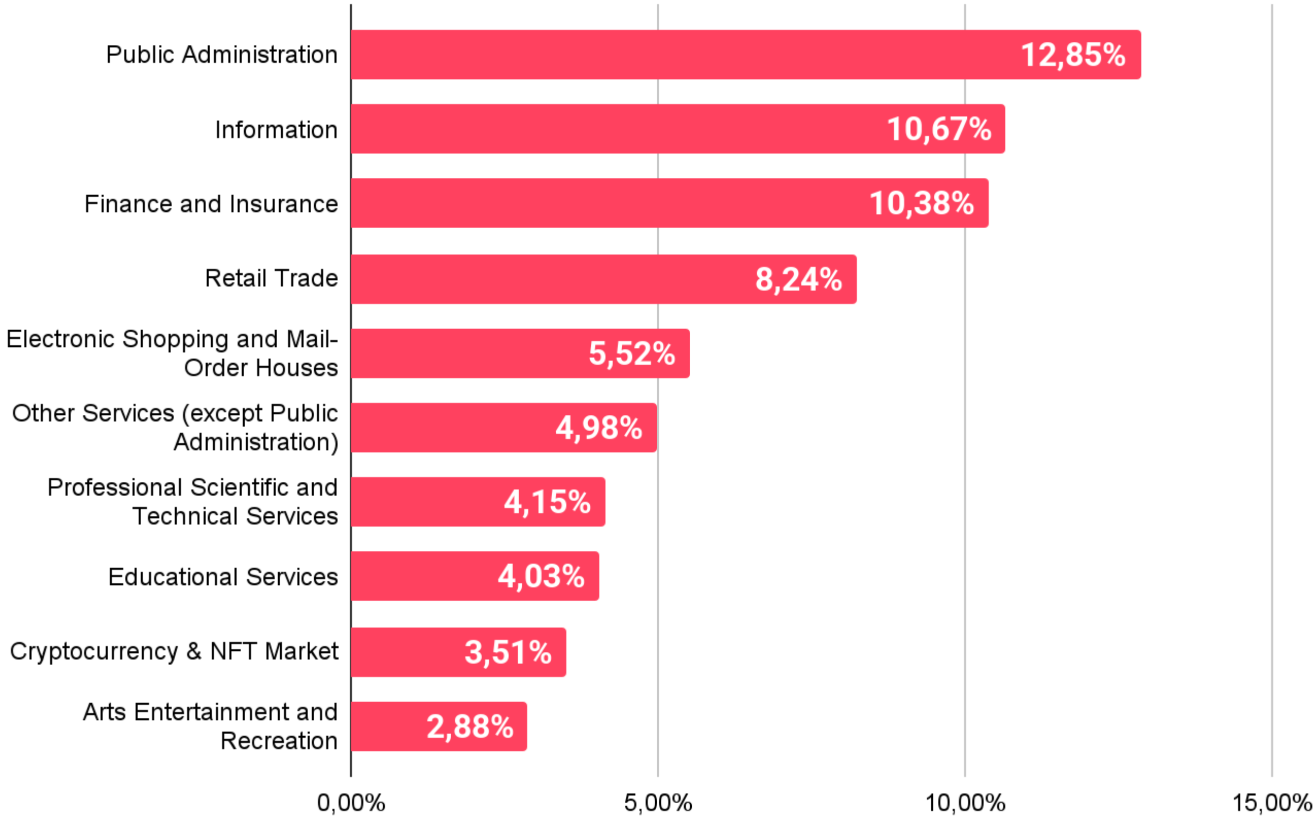
Dark Web News

Time Analysis of Dark Web News



The data for this section was collected through the SOCRadar XTI Platform. Our analysts monitor threat actor activities across various sources, including Dark Web forums and markets, Telegram groups, and ransomware group blog pages.

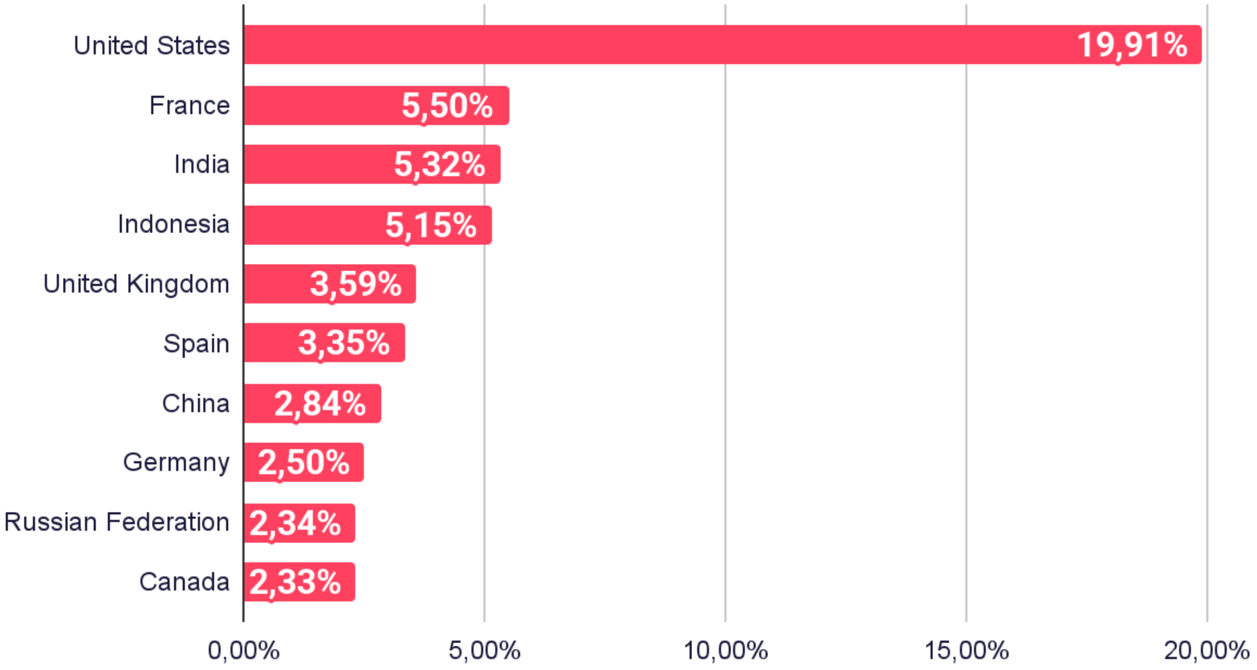
Distribution of Dark Web Threats by Industry



Posts from Dark Web forums related to Public Administrations account for the largest share of Dark Web news at 12.85%. This shows a sustained interest in government data and access possibilities.

Information, finance, and insurance follow closely, together forming a high value cluster linked to data resale, fraud, and extortion.

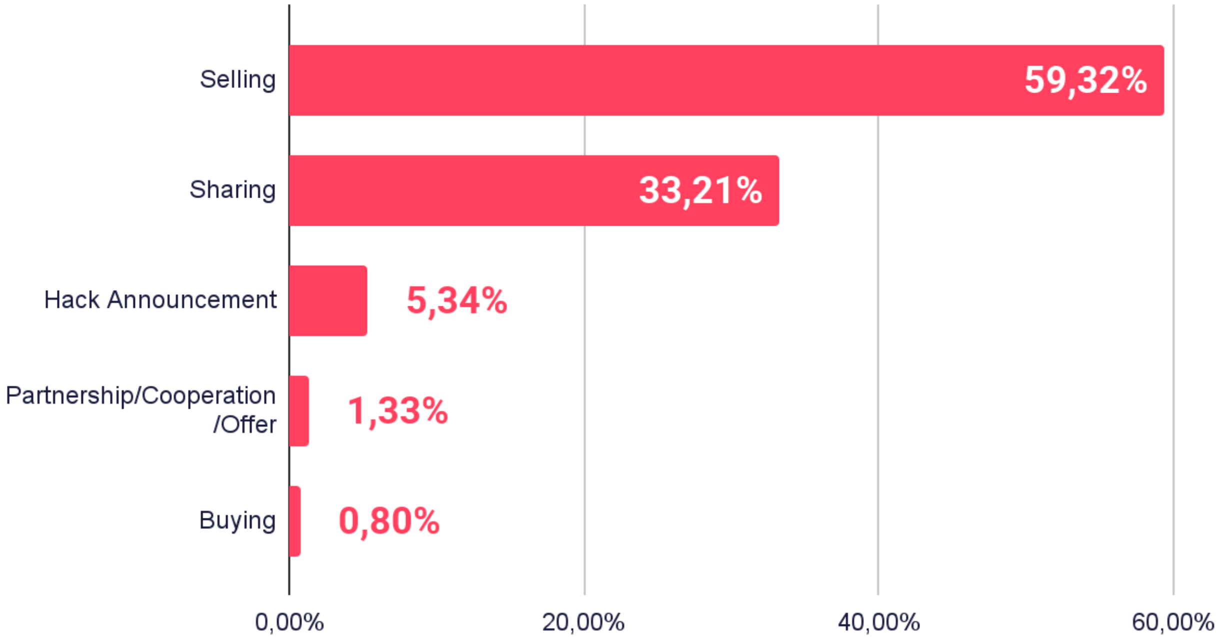
Distribution of Dark Web Threats by Primary Target Country



The United States dominates Dark Web news with 19.91%, showing its continued role as the main target for cybercriminal activity. This aligns with its large digital footprint and high value data assets.

France, India, and Indonesia follow at similar levels, which indicates broad targeting across both mature and fast growing digital markets. European countries such as the United Kingdom, Spain, and Germany maintain steady visibility, often linked to data leaks and fraud cases.

Distribution of Dark Web Threats by Threat Categories

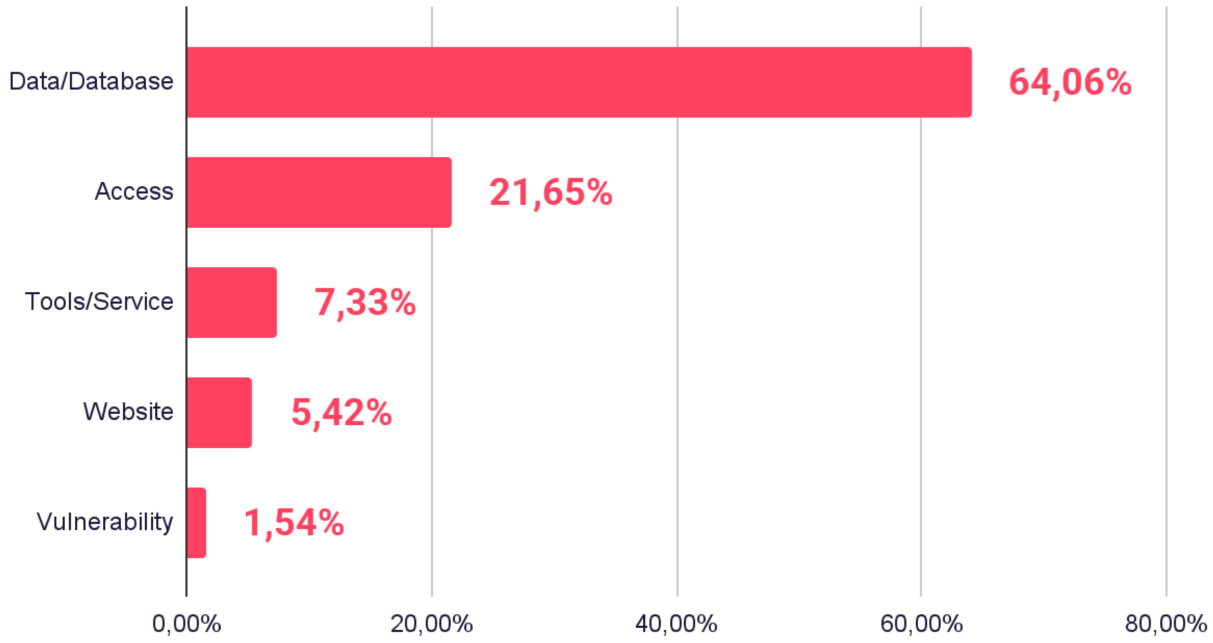


Selling dominates Dark Web news at 59.32%, confirming that most activity is driven by monetization goals.

Sharing follows with 33.21%, which is mostly related to the threat actors trying to build their reputation.

Hack announcements, Partnership posts and Buying activity appear at a marginal level since it is hard to see posts about future plans in general. These types of posts regarding upcoming operations are predominantly detected in Telegram channels where ideology-driven and hacktivist actors are more active.

Distribution of Dark Web Threats by Threat Type



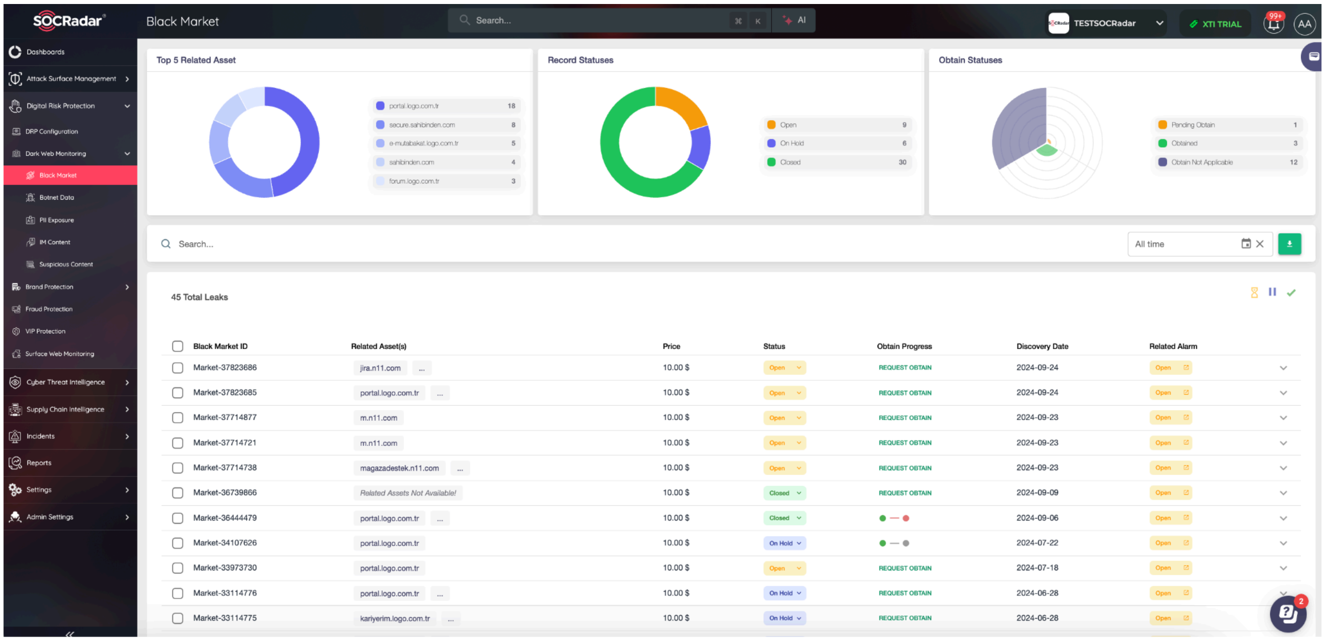
Data and database related threats dominate at 64.06%, showing that data theft remains the primary driver of Dark Web activity.

One reason for this is the ease of proving legitimacy for such claims compared to other illicit goods. Threat actors can share samples as proof to validate their offerings, which is more difficult with other types of goods for various reasons.

Access related threats follow at 21.65%, highlighting strong demand for initial access to networks and systems.

Tools and services, Website related threats and Vulnerability related posts remain limited since these types of products are harder to create.

Overall, the ecosystem prioritizes assets that enable fast monetization.



45 Total Leaks

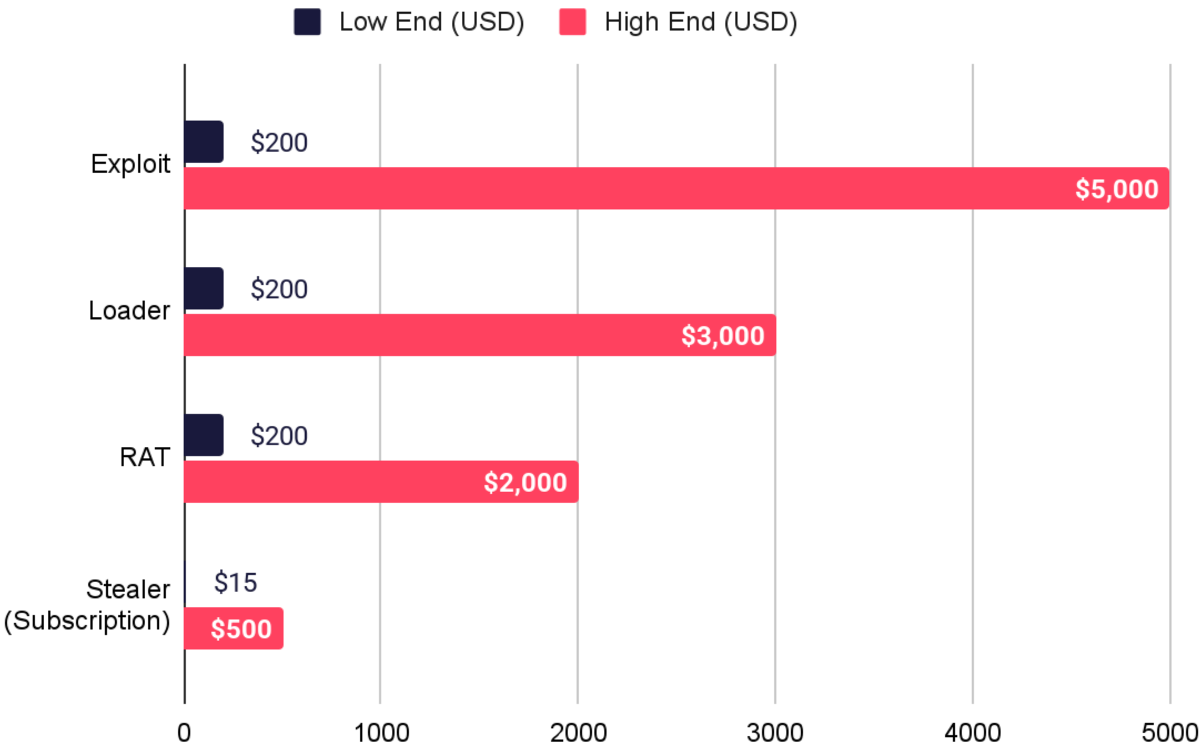
☐ Black Market ID	Related Asset(s)	Price	Status	Obtain Progress	Discovery Date	Related Alarm
☐ Market-37823686	jira.n11.com ...	10.00 $	Open	REQUEST OBTAIN	2024-09-24	Open
☐ Market-37823685	portal.logo.com.tr ...	10.00 $	Open	REQUEST OBTAIN	2024-09-24	Open
☐ Market-37714877	m.n11.com	10.00 $	Open	REQUEST OBTAIN	2024-09-23	Open
☐ Market-37714721	m.n11.com	10.00 $	Open	REQUEST OBTAIN	2024-09-23	Open
☐ Market-37714738	magazadestek.n11.com ...	10.00 $	Open	REQUEST OBTAIN	2024-09-23	Open
☐ Market-36739866	*Related Assets Not Available!*	10.00 $	Closed	REQUEST OBTAIN	2024-09-09	Open
☐ Market-36444479	portal.logo.com.tr ...	10.00 $	Closed	● — ●	2024-09-06	Open
☐ Market-34107626	portal.logo.com.tr	10.00 $	On Hold	● — ●	2024-07-22	Open
☐ Market-33973730	portal.logo.com.tr	10.00 $	Open	REQUEST OBTAIN	2024-07-18	Open
☐ Market-33114776	portal.logo.com.tr ...	10.00 $	On Hold	REQUEST OBTAIN	2024-06-28	Open
☐ Market-33114775	kariyerim.logo.com.tr ...	10.00 $	On Hold	REQUEST OBTAIN	2024-06-28	Open

SOCRadar's Advanced Dark Web Monitoring equips organizations with vital insights into hidden threats targeting key industries such as finance, insurance, and information technology, which have faced significant risks over the past year. By providing real-time monitoring of underground chatter and sensitive data exposure, SOCRadar empowers proactive defenses against Dark Web threats.

Activate your free trial today to safeguard your organization's most valuable assets.

Malware, Exploits, Tools, Services

Malicious Software and Tools



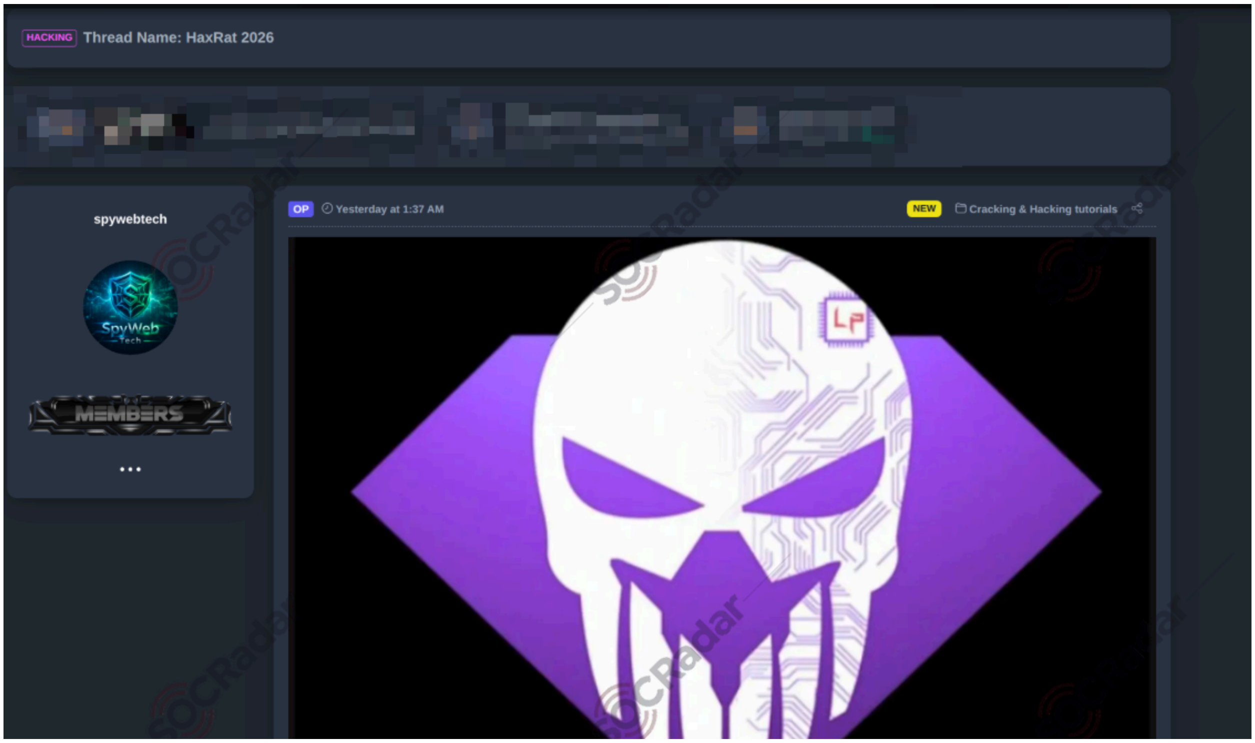
The pricing scale for malicious software and tools shows a wide range that reflects both capability and scale.

Exploits command the highest prices, reaching up to $5,000 mostly due to their direct impact.

Loaders and RATs remain mid range tools, typically priced between $200 and $3,000, which makes them accessible for more threat actors. On the lower end of these types of products, we see threat actors promoting their subscription models.

Stealers stand out with an extremely low entry point at $15, enabling mass adoption and large-scale credential theft. This pricing also applies to stealer logs when purchased in bulk. Posts promoting stealers or stealer logs are predominantly subscription-based, which accounts for the low price point.

Overall, low cost tools continue to lower the barrier to entry for cybercrime.



HACKING Thread Name: HaxRat 2026

[redacted]

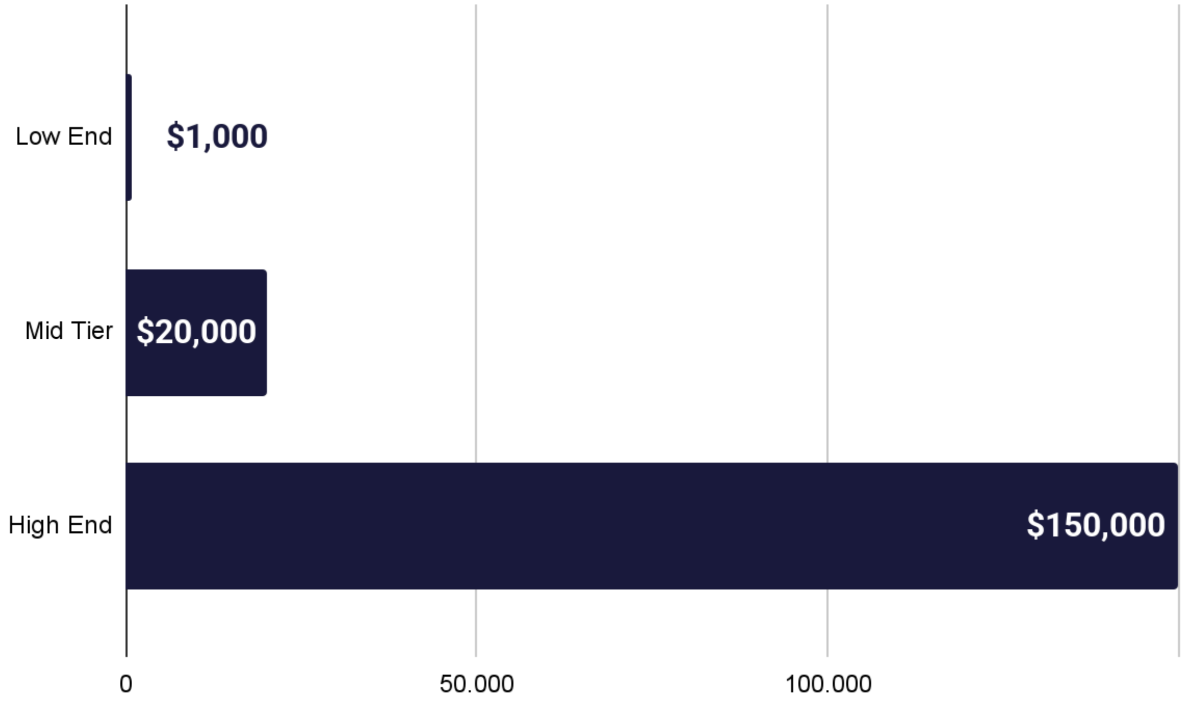
spywebtech

OP Yesterday at 1:37 AM

NEW Cracking & Hacking tutorials

A Dark Web forum post advertises an Android remote access trojan offering full device surveillance and control. The tool claims features such as screen capture, camera and microphone access, GPS tracking, SMS and call log access, file management, and APK generation, marketed under the guise of penetration testing and device administration.

0-Day Market

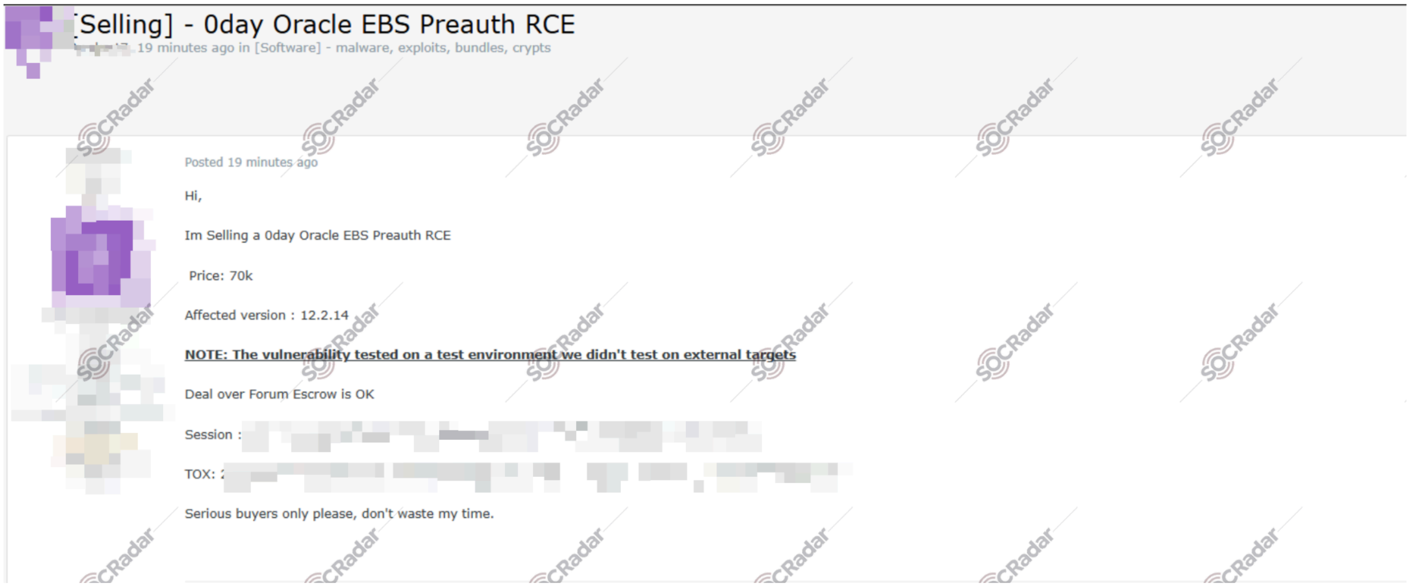


Zero day pricing shows a steep value gradient based on impact and exclusivity.

On the low-end, we can see 0-days start around $1,000 and are often limited in reliability or scope. Compared to last year, the price for low-end 0-Day posts increased from $100 to $1000 level. Zero day posts on that level are very rare now.

Mid tier prices average $20,000, reflecting usable exploits mostly for common platforms. We see another increase in mid tier as well. Average price for mid-tier 0-Days last year was around $10.000.

High-end 0-Days can reach $150,000, targeting widely deployed systems with strong defensive controls. In this tier, we see a decrease compared to last year's $200,000 level. In reality, there is no upper limit for 0-Days and these numbers only reflect the average.



[Selling] - 0day Oracle EBS Preauth RCE

[redacted] 19 minutes ago in [Software] - malware, exploits, bundles, crypts

Posted 19 minutes ago

Hi,

Im Selling a 0day Oracle EBS Preauth RCE

Price: 70k

Affected version : 12.2.14

NOTE: The vulnerability tested on a test environment we didn't test on external targets

Deal over Forum Escrow is OK

Session : [redacted]

TOX: [redacted]

Serious buyers only please, don't waste my time.

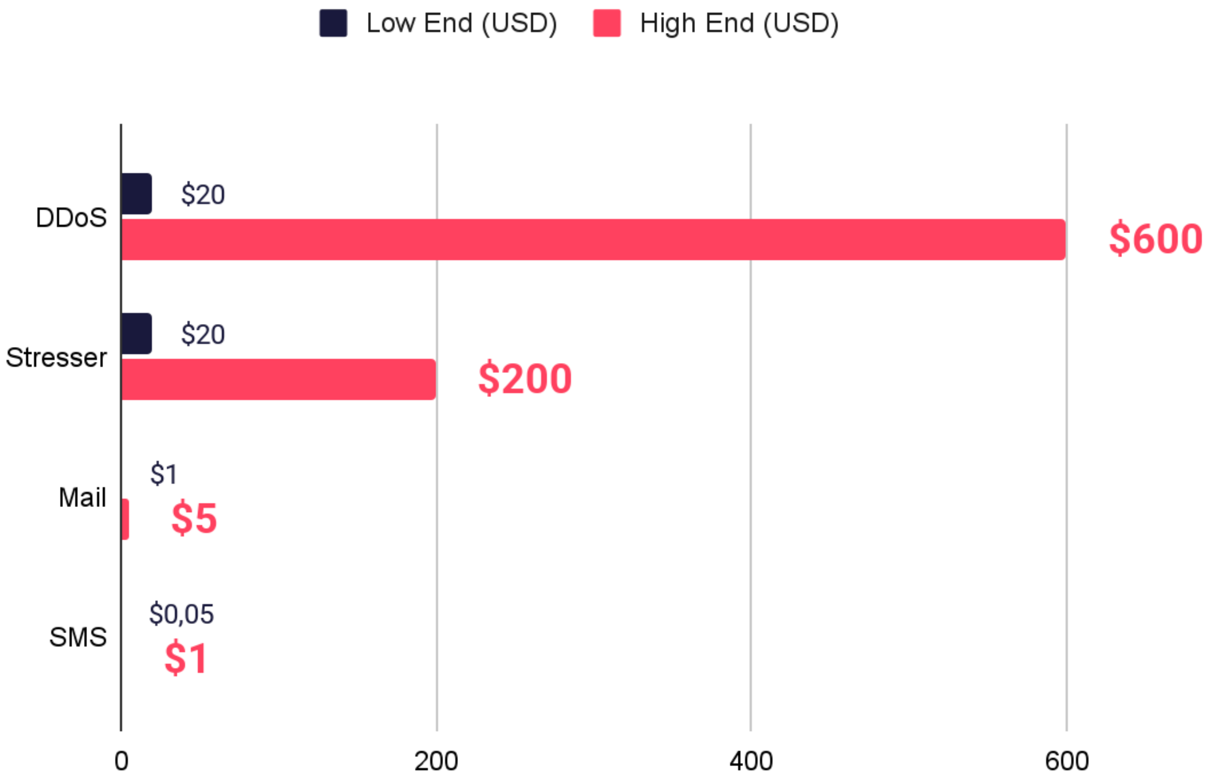
*Sale of a A 0-day vulnerability for Oracle E-Businesses - **SOCRadar Advanced Dark Web Monitoring***

A threat actor offered a 0-day vulnerability affecting Oracle E Business Suite for sale in a Dark Web forum around June 2025 for 70,000 USD.

Later on, around October-November 2025, Cl0p ransomware started a **targeted campaign** against companies using Oracle E Business Suite.

This activity is one of the most clear examples of how commercially traded 0-day exploits can move quickly from criminal marketplaces into large scale ransomware operations.

Spamming and DDoS Services



DDoS and spamming services are priced very low compared to other products, which supports high volume and low skill abuse. The main reason for this is almost all products in this category are subscription based. People can pay weekly or monthly fees for these types of services.

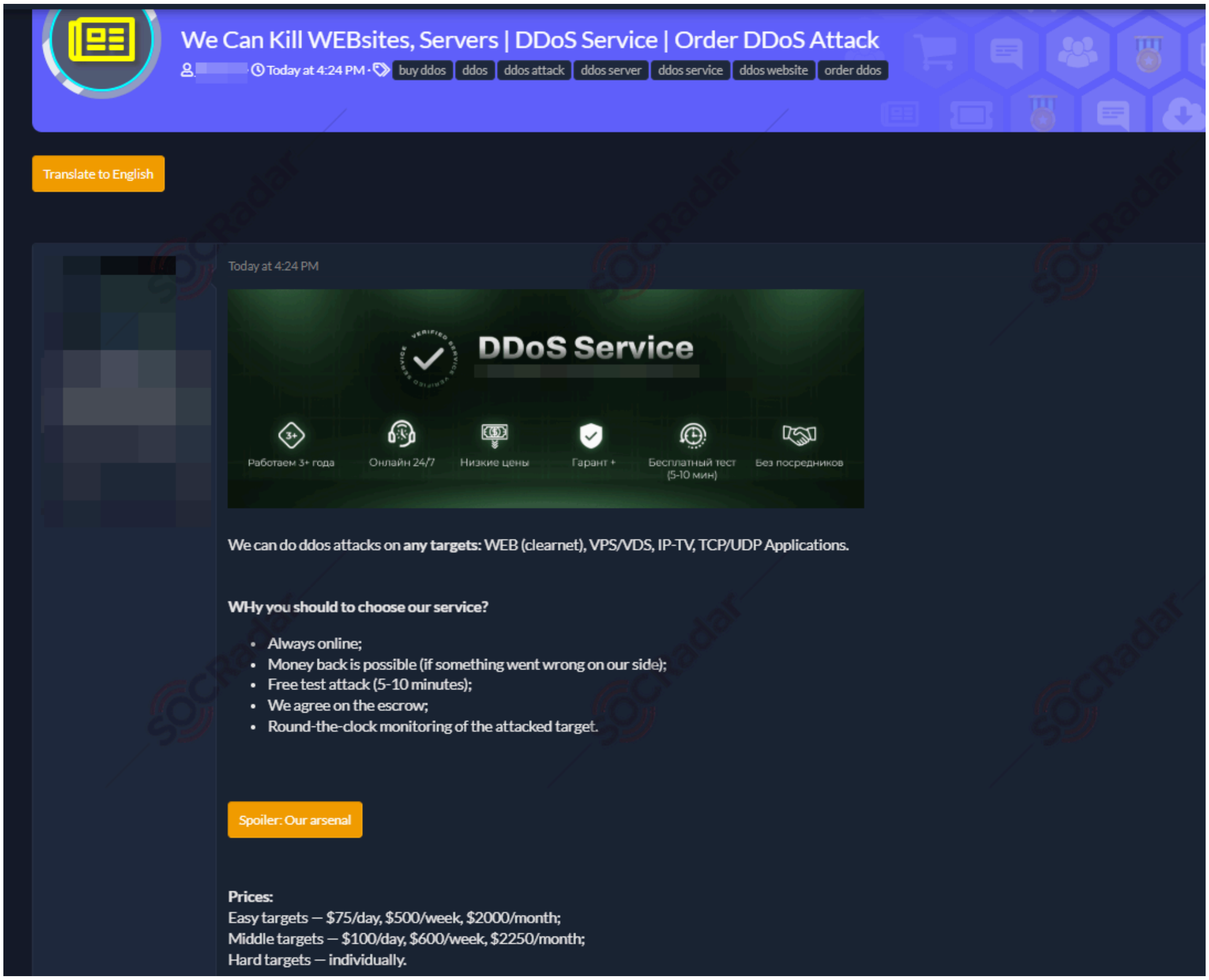
DDoS attacks mostly start at $20 and reach $600, making disruption campaigns widely accessible.

Stressers follow a similar range but remain cheaper.

Email services cost as little as $1, enabling large scale phishing and spam distribution.

SMS services are the cheapest, starting at $0.05, which lowers the barrier for smishing campaigns.

Overall, low pricing fuels mass activity and increases background noise across networks.



We Can Kill WEBsites, Servers | DDoS Service | Order DDoS Attack

[redacted] Today at 4:24 PM · buy ddos · ddos · ddos attack · ddos server · ddos service · ddos website · order ddos

Today at 4:24 PM

We can do ddos attacks on **any targets:** WEB (clearnet), VPS/VDS, IP-TV, TCP/UDP Applications.

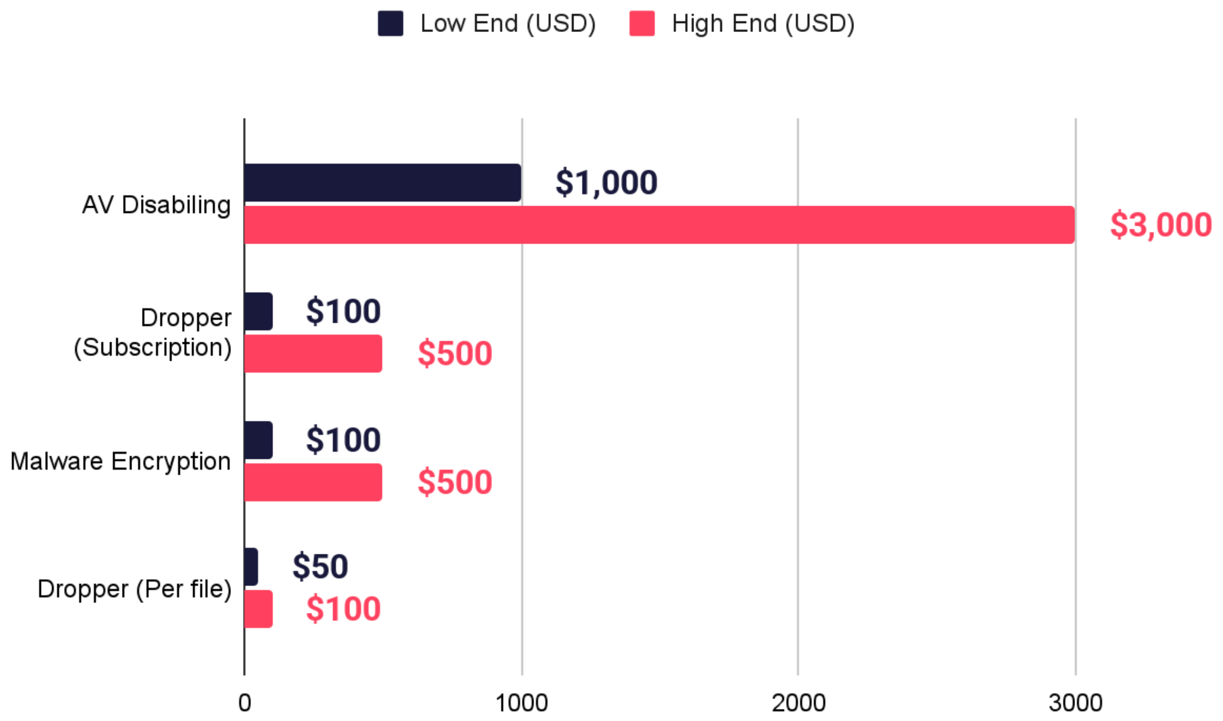
WHy you should to choose our service?

- Always online;
- Money back is possible (if something went wrong on our side);
- Free test attack (5-10 minutes);
- We agree on the escrow;
- Round-the-clock monitoring of the attacked target.

Prices:
Easy targets – $75/day, $500/week, $2000/month;
Middle targets – $100/day, $600/week, $2250/month;
Hard targets – individually.

A DDoS service being offered on a Dark Web forum - SOCRadar Advanced Dark Web Monitoring

Hacking Services



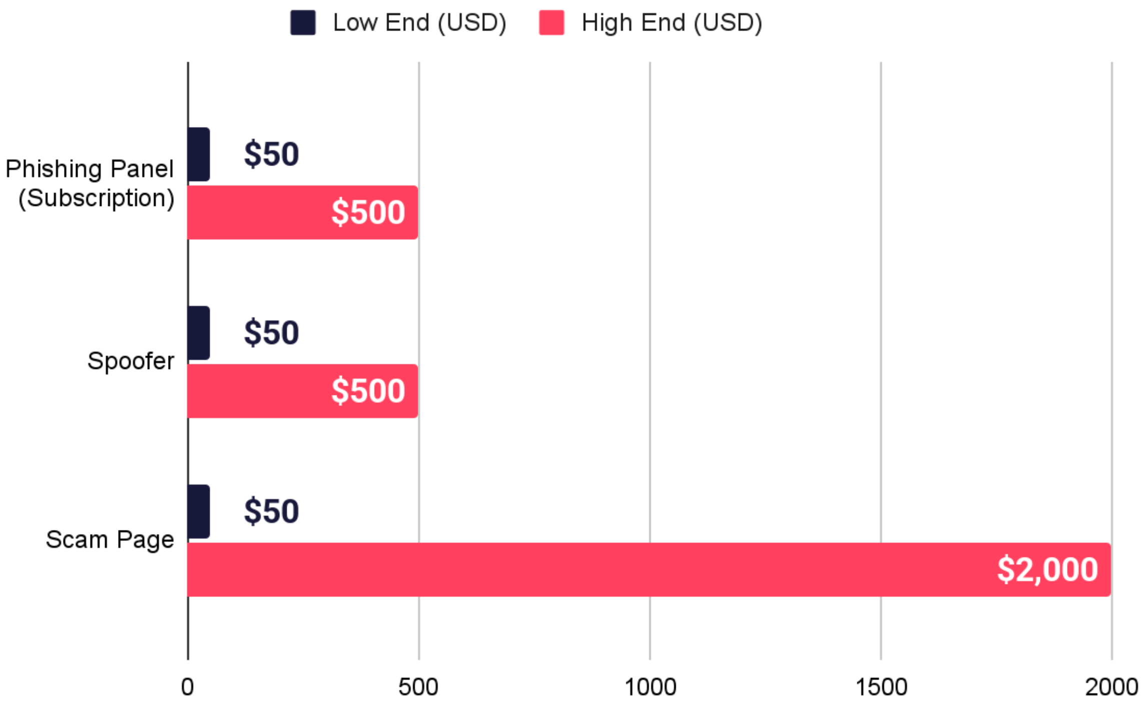
Hacking services are serving the interests of other threat actors. They can get operational support from each other to improve their attacks.

AV disabling is the most expensive service, priced between $1,000 and $3,000, which highlights its value in bypassing defenses.

Droppers and malware encryption stay in mid-level, with prices mostly below $500, supporting repeated campaign use.

When it comes to per-file pricing, Dropper prices go even lower.

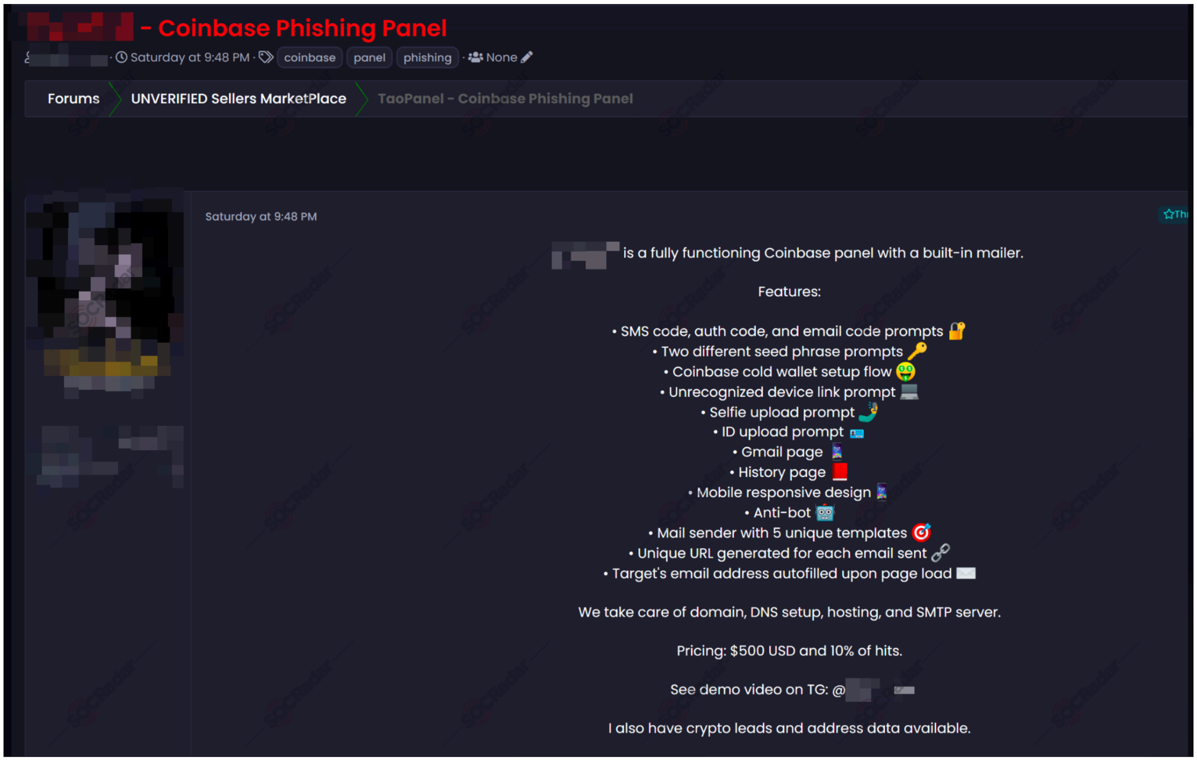
Phishing Kits and Templates



Phishing kits and templates are moderately priced, which supports sustained campaign activity.

Phishing panels and spoofers range from $50 to $500, making them accessible to low skill actors.

Scam pages show the widest range, up to $2,000, which reflects customization and brand targeting.



[redacted] - Coinbase Phishing Panel

[redacted] · Saturday at 9:48 PM · coinbase panel phishing · None

Forums › UNVERIFIED Sellers MarketPlace › TaoPanel - Coinbase Phishing Panel

[redacted]

Saturday at 9:48 PM

[redacted] is a fully functioning Coinbase panel with a built-in mailer.

Features:

- SMS code, auth code, and email code prompts 🔐
- Two different seed phrase prompts 🔑
- Coinbase cold wallet setup flow 🤑
- Unrecognized device link prompt 💻
- Selfie upload prompt 🤳
- ID upload prompt 🪪
- Gmail page 📱
- History page 📕
- Mobile responsive design 📱
- Anti-bot 🤖
- Mail sender with 5 unique templates 🎯
- Unique URL generated for each email sent 🔗
- Target's email address autofilled upon page load ✉️

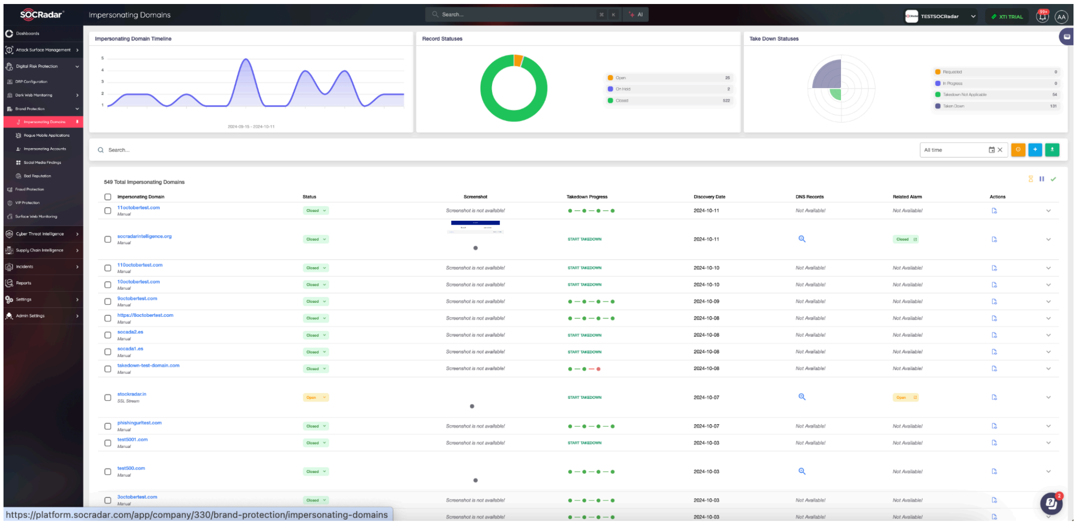
We take care of domain, DNS setup, hosting, and SMTP server.

Pricing: $500 USD and 10% of hits.

See demo video on TG: @[redacted]

I also have crypto leads and address data available.

*The sale of a sophisticated phishing panel designed to mimic Coinbase's login and security procedures - **SOCRadar Advanced Dark Web Monitoring***



Record Statuses	
Open	25
On Hold	2
Closed	522

Take Down Statuses	
Requested	0
In Progress	0
Takedown Not Applicable	54
Taken Down	131

549 Total Impersonating Domains

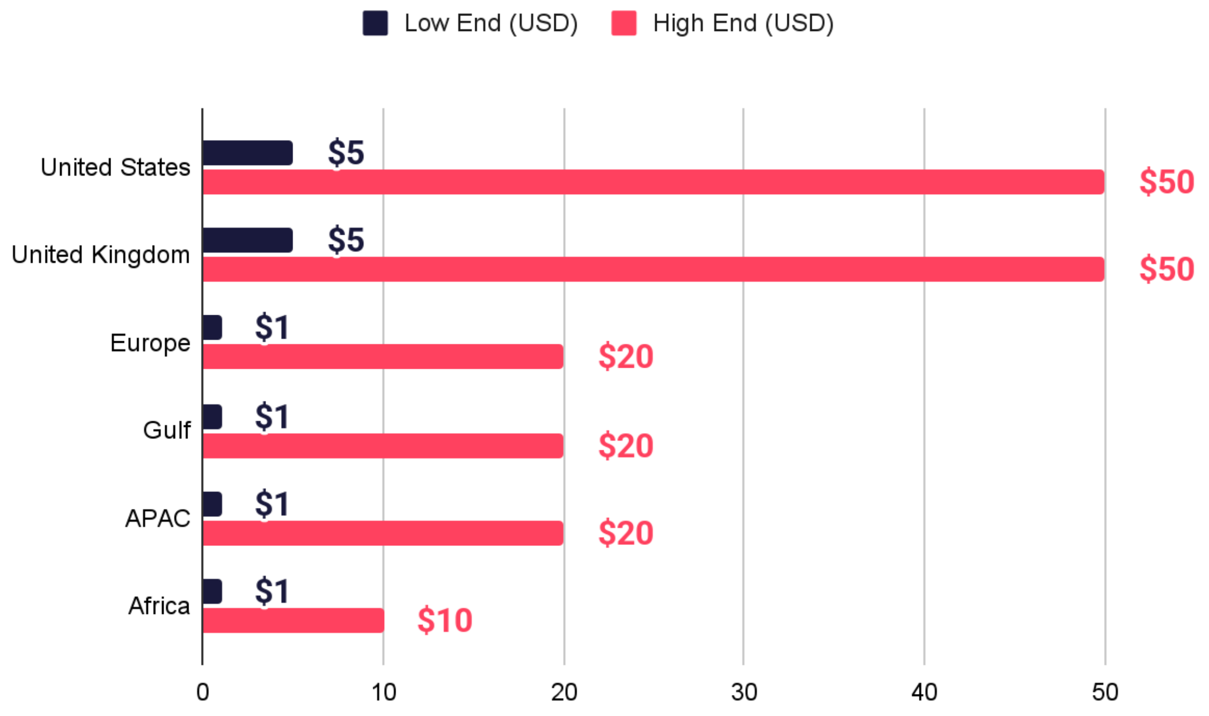
Impersonating Domain	Status	Screenshot	Takedown Progress	Discovery Date	DNS Records	Related Alarm
11octobertest.com Manual	Closed	Screenshot is not available!	● — ● — ● — ●	2024-10-11	Not Available!	Not Available!
socradarintelligence.org Manual	Closed		START TAKEDOWN	2024-10-11		Closed
110octobertest.com Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-10	Not Available!	Not Available!
10octobertest.com Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-10	Not Available!	Not Available!
9octobertest.com Manual	Closed	Screenshot is not available!	● — ● — ● — ●	2024-10-09	Not Available!	Not Available!
https://8octobertest.com Manual	Closed	Screenshot is not available!	● — ● — ● — ●	2024-10-08	Not Available!	Not Available!
socada2.es Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-08	Not Available!	Not Available!
socada1.es Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-08	Not Available!	Not Available!
takedown-test-domain.com Manual	Closed	Screenshot is not available!	● — ● — ●	2024-10-08	Not Available!	Not Available!
stockradar.in SSL Stream	Open		START TAKEDOWN	2024-10-07		Open
phishingurltest.com Manual	Closed	Screenshot is not available!	● — ● — ● — ●	2024-10-07	Not Available!	Not Available!
test5001.com Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-03	Not Available!	Not Available!
test500.com Manual	Closed		● — ● — ● — ●	2024-10-03		Not Available!
3octobertest.com Manual	Closed	Screenshot is not available!	● — ● — ● — ●	2024-10-03	Not Available!	Not Available!
		Screenshot is not available!	● — ● — ● — ●	2024-10-03	Not Available!	Not Available!

https://platform.socradar.com/app/company/330/brand-protection/impersonating-domains

With SOCRadar's AI-powered Phishing Domain Detection module**, you can swiftly identify malicious domains and protect your brand from phishing threats. **Start safeguarding your digital presence today with SOCRadar—request a free trial and see the platform in action.

Financial Services and Fraud

Credit Cards

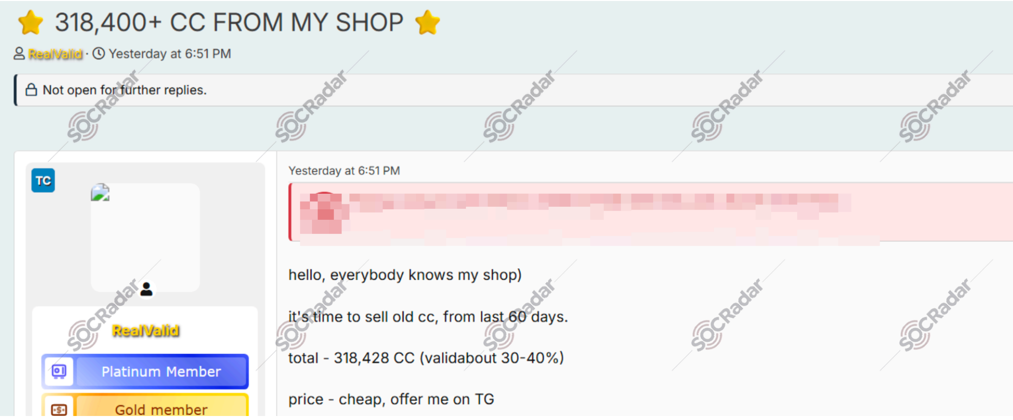


Credit card pricing shows clear regional value differences tied to fraud potential.

United States and United Kingdom cards are the most expensive, ranging from $5 to $50, reflecting higher acceptance rates.

European, Gulf, and APAC cards cluster between $1 and $20, indicating moderate demand and mixed usability.

African cards remain the lowest priced, capped at $10, which suggests limited fraud yield and higher rejection risk.



318,400+ CC FROM MY SHOP

RealValid · Yesterday at 6:51 PM

Not open for further replies.

Yesterday at 6:51 PM

[redacted]

hello, everybody knows my shop)

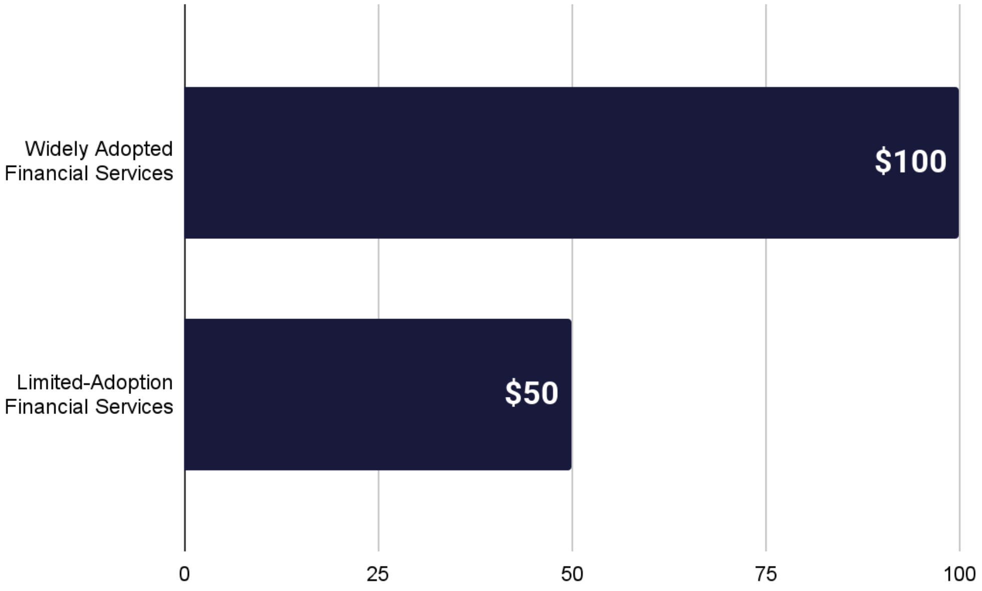
it's time to sell old cc, from last 60 days.

total - 318,428 CC (validabout 30-40%)

price - cheap, offer me on TG

*A potential data sale of approximately 320k credit card details - **SOCRadar Advanced Dark Web Monitoring***

Online Payment Accounts (PayPal, Venmo, etc.)



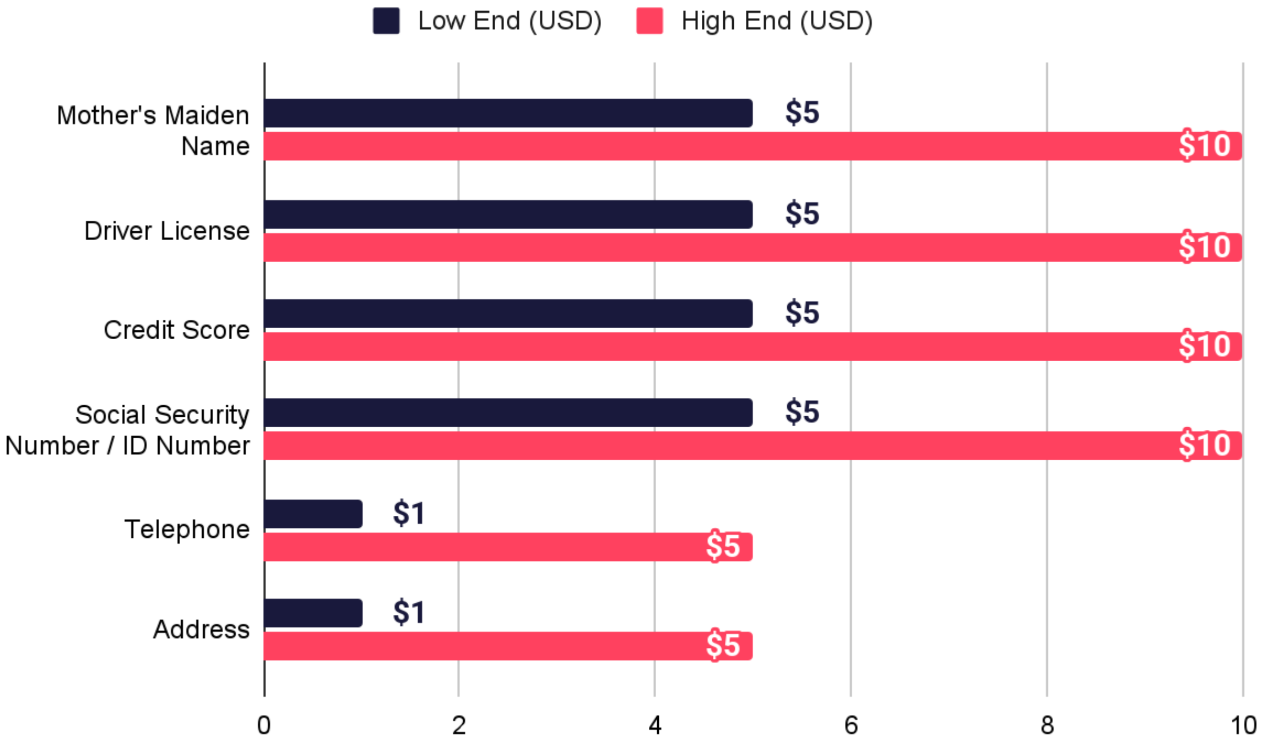
Online payment accounts show clear value differences based on adoption level.

Accounts tied to widely adopted financial services average $100, reflecting higher trust, broader merchant acceptance, and better fraud utility.

Limited adoption services average $50, which reduces their appeal for large scale fraud.

“Widely Adopted Financial Services” refers to platforms with large user bases and frequent visibility in illicit marketplaces (for example, PayPal and Revolut), while “Limited-Adoption Financial Services” includes services with smaller or more specialized user populations and less market presence (such as, ZEN and P100).

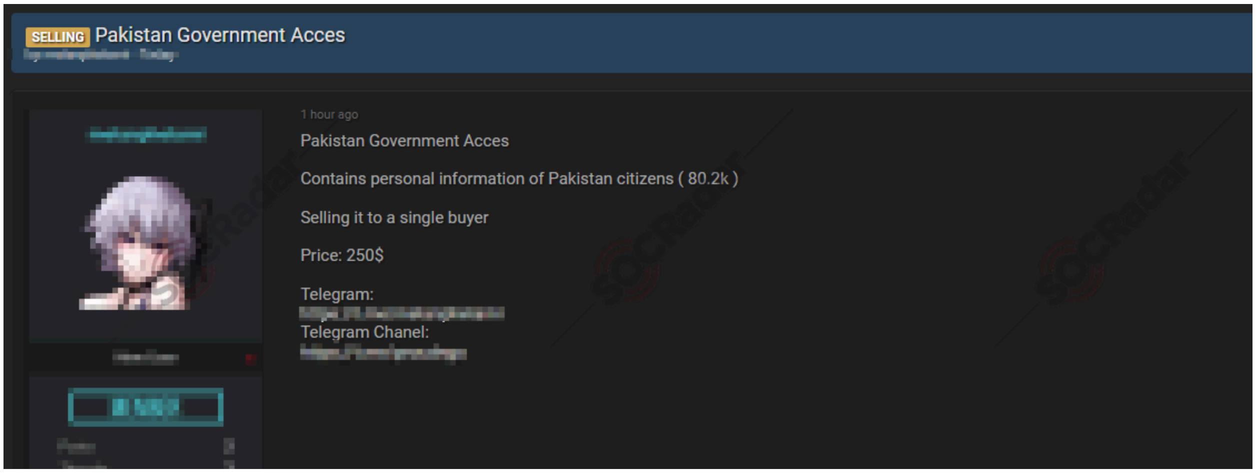
Personal Information and Documents



Core identity attributes such as mother's maiden name, driver license data, credit score, and national ID numbers are priced between 5 and 10 USD. These fields are more crucial when it comes to identity verification and account takeover.

Contact-level data such as telephone numbers and physical addresses are cheaper. We can also include email addresses to this category. Prices for such products range from 1 to 5 USD. These data points are widely available and easier to collect at scale and because of that their standalone value is limited.

It is also important to note that most of these products are sold in bulk.



SELLING Pakistan Government Acces

[redacted]

1 hour ago

Pakistan Government Acces

Contains personal information of Pakistan citizens (80.2k)

Selling it to a single buyer

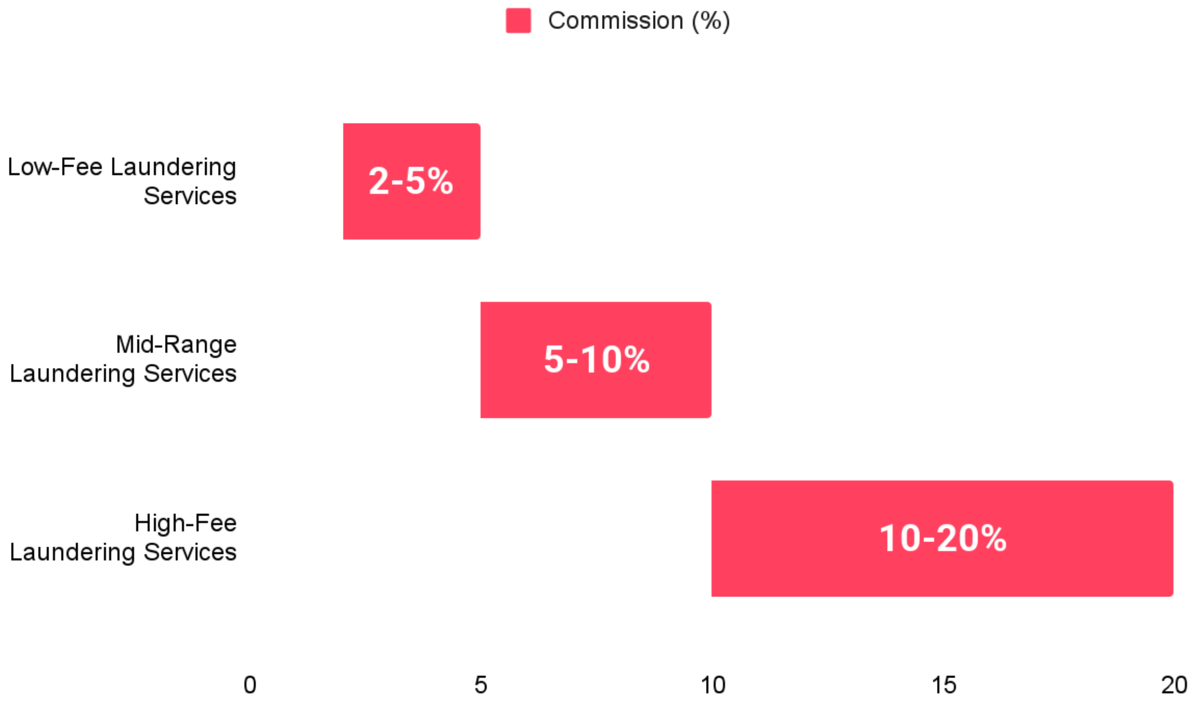
Price: 250$

Telegram:
[redacted]

Telegram Chanel:
[redacted]

*Unauthorized access sale allegedly belonging to a Pakistani government agency, including personal information of 80.2k Pakistan citizens - **SOCRadar Advanced Dark Web Monitoring***

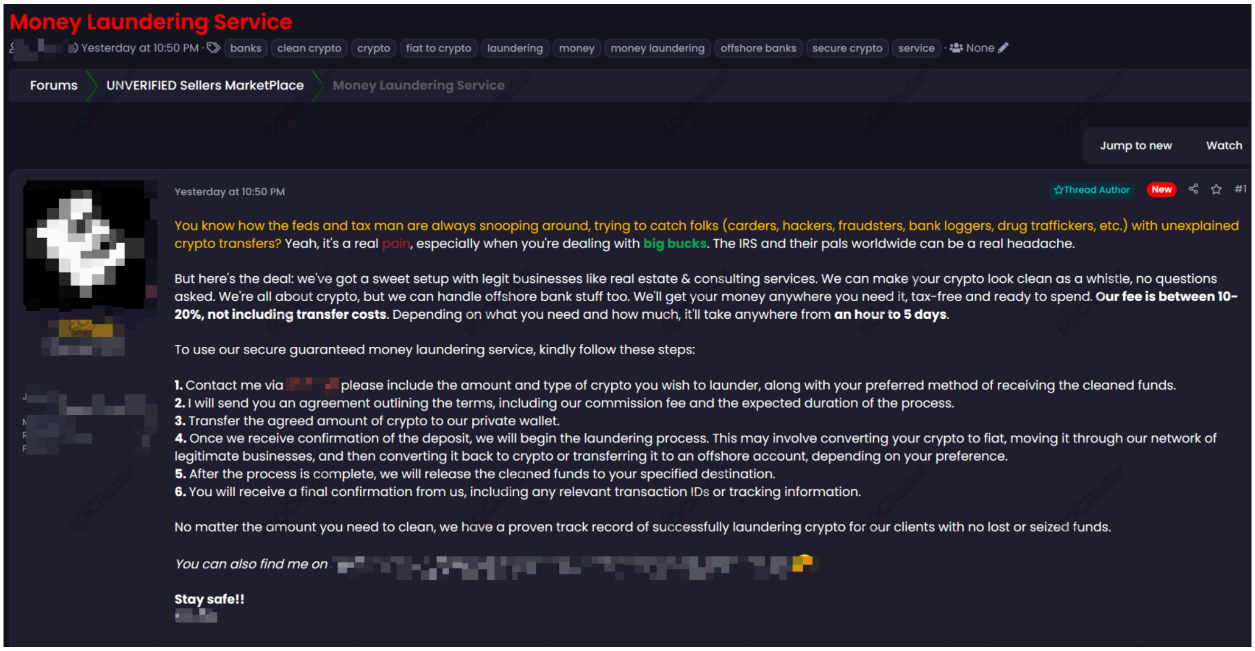
Money Laundering Services



Money laundering services observed in illicit marketplaces are commonly priced as a percentage of the total amount processed rather than a fixed fee.

We decided to group these services into low-fee (2–5%), mid-range (5–10%), and high-fee (10–20%) categories to reflect differing levels of service complexity, operational risk, and perceived reliability.

These categories describe pricing structures, not effectiveness or success rates.



Money Laundering Service

Yesterday at 10:50 PM

You know how the feds and tax man are always snooping around, trying to catch folks (carders, hackers, fraudsters, bank loggers, drug traffickers, etc.) with unexplained crypto transfers? Yeah, it's a real pain, especially when you're dealing with **big bucks**. The IRS and their pals worldwide can be a real headache.

But here's the deal: we've got a sweet setup with legit businesses like real estate & consulting services. We can make your crypto look clean as a whistle, no questions asked. We're all about crypto, but we can handle offshore bank stuff too. We'll get your money anywhere you need it, tax-free and ready to spend. **Our fee is between 10-20%, not including transfer costs**. Depending on what you need and how much, it'll take anywhere from **an hour to 5 days**.

To use our secure guaranteed money laundering service, kindly follow these steps:

1. Contact me via [redacted] please include the amount and type of crypto you wish to launder, along with your preferred method of receiving the cleaned funds.
2. I will send you an agreement outlining the terms, including our commission fee and the expected duration of the process.
3. Transfer the agreed amount of crypto to our private wallet.
4. Once we receive confirmation of the deposit, we will begin the laundering process. This may involve converting your crypto to fiat, moving it through our network of legitimate businesses, and then converting it back to crypto or transferring it to an offshore account, depending on your preference.
5. After the process is complete, we will release the cleaned funds to your specified destination.
6. You will receive a final confirmation from us, including any relevant transaction IDs or tracking information.

No matter the amount you need to clean, we have a proven track record of successfully laundering crypto for our clients with no lost or seized funds.

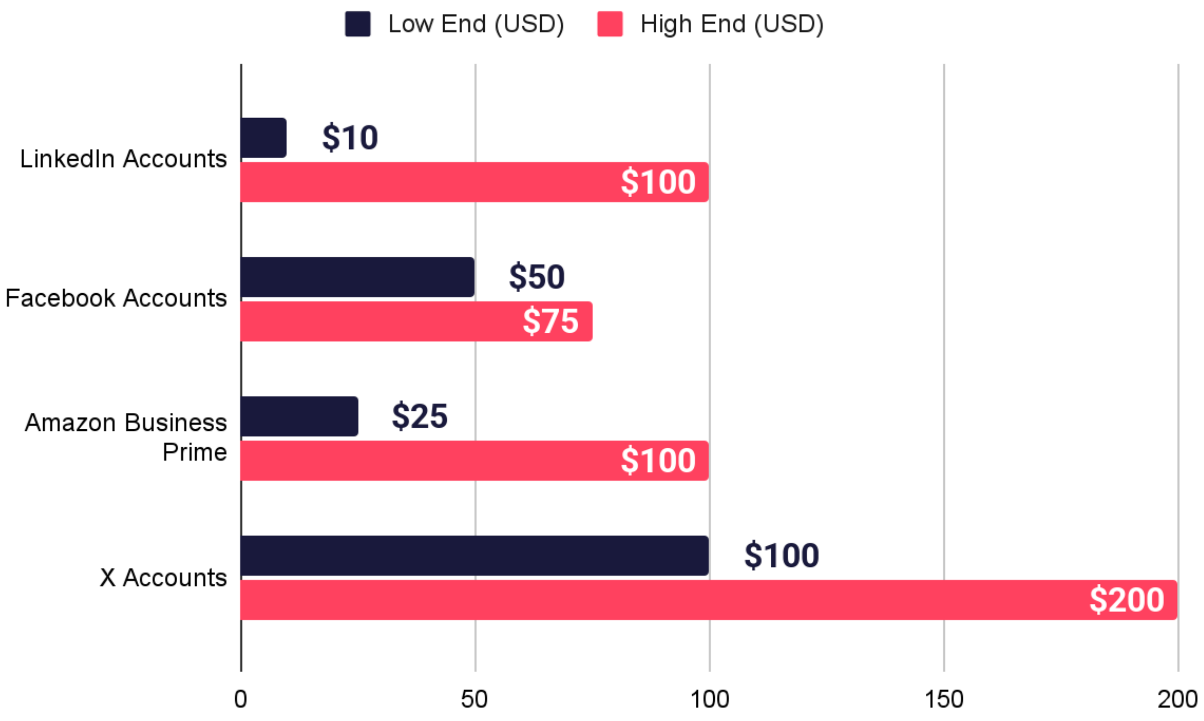
You can also find me on [redacted]

Stay safe!!
[redacted]

*Money laundering service advertisement - **SOCRadar Advanced Dark Web Monitoring***

Digital Goods

Social Media Accounts and Services



The pricing for social media accounts reflects the influence of the platform and accounts' abuse potential.

LinkedIn accounts range from $10 to $100, driven by their use in fraud, recruitment scams, and initial access attempts.

Facebook accounts remain consistently valued at $50 to $75 due to scale and advertising abuse.

Amazon Business Prime accounts reach up to $100, reflecting direct financial misuse.

X accounts are the most expensive, priced between $100 and $200, due to the platform's popularity. Verified accounts command even higher prices.

AI Market

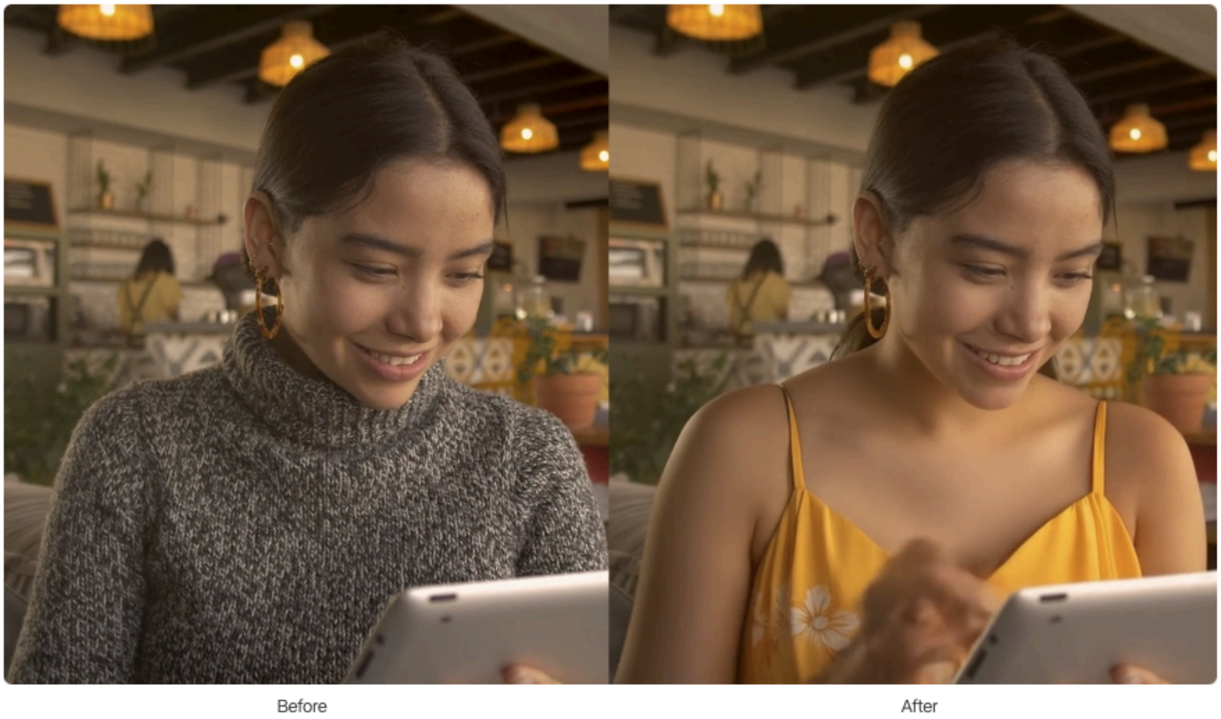
AI Tools

A major concern since AI tools became popular is their potential misuse. The fear was that publicly available models can generate phishing emails, help threat actors with their malicious intentions, create fake images and so on.

In our Annual Dark Web Report we published last year we assessed that these types of tools remain ineffective compared to the dominant focus on traditional cybercrime tools. However, the AI market has changed quite a bit.

Using these tools still requires little technical expertise. But compared to last year we have a wide range of AI-powered tools that are now openly available for better text generation, image manipulation, voice generation, and coding.

Crucially, there is no vetting, and no engagement with illicit markets to access these tools now. This fundamentally alters the threat landscape which was once restricted to well-resourced actors.



Outfit change with Runway AI

Audio and visual manipulation experienced one of the biggest leaps we saw compared to other fields of AI last year. Open-source and commercial deepfake tools can synthesize realistic faces, voices, and videos using minimal training data.

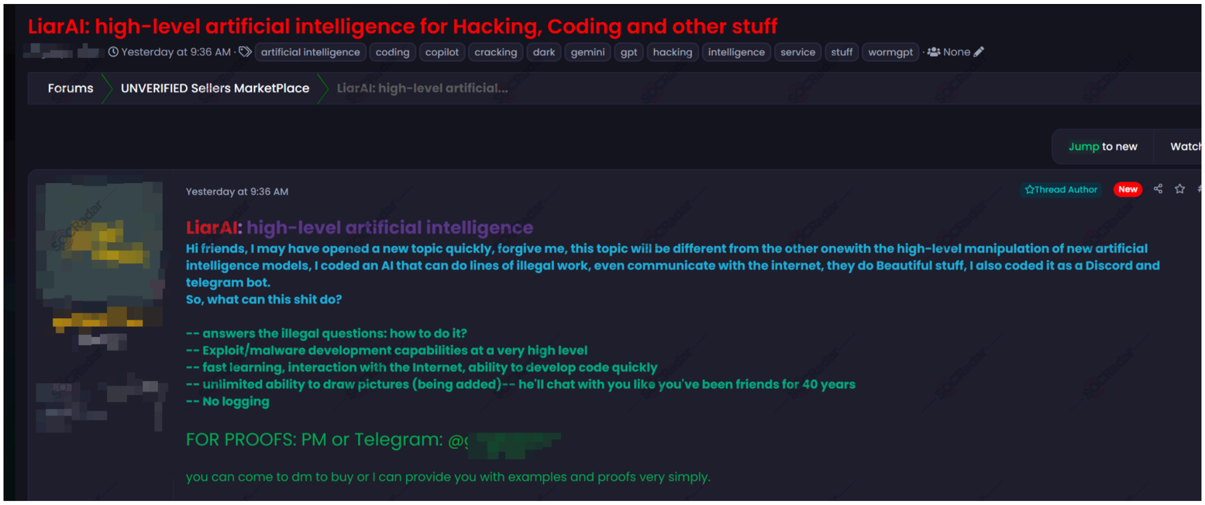
Though often promoted for entertainment or content creation, they can be repurposed for impersonation, harassment, non-consensual content, or political manipulation. Unfortunately, the lack of effective safeguards or monitoring makes abuse difficult to detect and attribute.

A fake image of captured Venezuelan leader Nicolas Maduro, Source

Cybersecurity and penetration testing tools is another domain where we saw noteworthy development. Freely available AI tools for vulnerability scanning, pentesting, and exploitation are essential for defensive security research, but also provide malicious actors with ready-made capabilities. Critically, none require access to criminal forums or bespoke malware development.

Top 10 AI-Powered Pentest Tools

Underground markets remain active and continue to traffic in explicitly malicious AI tools. Dark Web forums and encrypted messaging channels facilitate the exchange of jailbroken models, uncensored chatbots, and AI systems with safety guardrails deliberately removed. However, their actual impact and effectiveness remain unclear.



LiarAI: high-level artificial intelligence for Hacking, Coding and other stuff

Yesterday at 9:36 AM

LiarAI: high-level artificial intelligence

Hi friends, I may have opened a new topic quickly, forgive me, this topic will be different from the other onewith the high-level manipulation of new artificial intelligence models, I coded an AI that can do lines of illegal work, even communicate with the internet, they do Beautiful stuff, I also coded it as a Discord and telegram bot.
So, what can this shit do?

-- answers the illegal questions: how to do it?
-- Exploit/malware development capabilities at a very high level
-- fast learning, interaction with the Internet, ability to develop code quickly
-- unlimited ability to draw pictures (being added)-- he'll chat with you like you've been friends for 40 years
-- No logging

FOR PROOFS: PM or Telegram: @[redacted]

you can come to dm to buy or I can provide you with examples and proofs very simply.

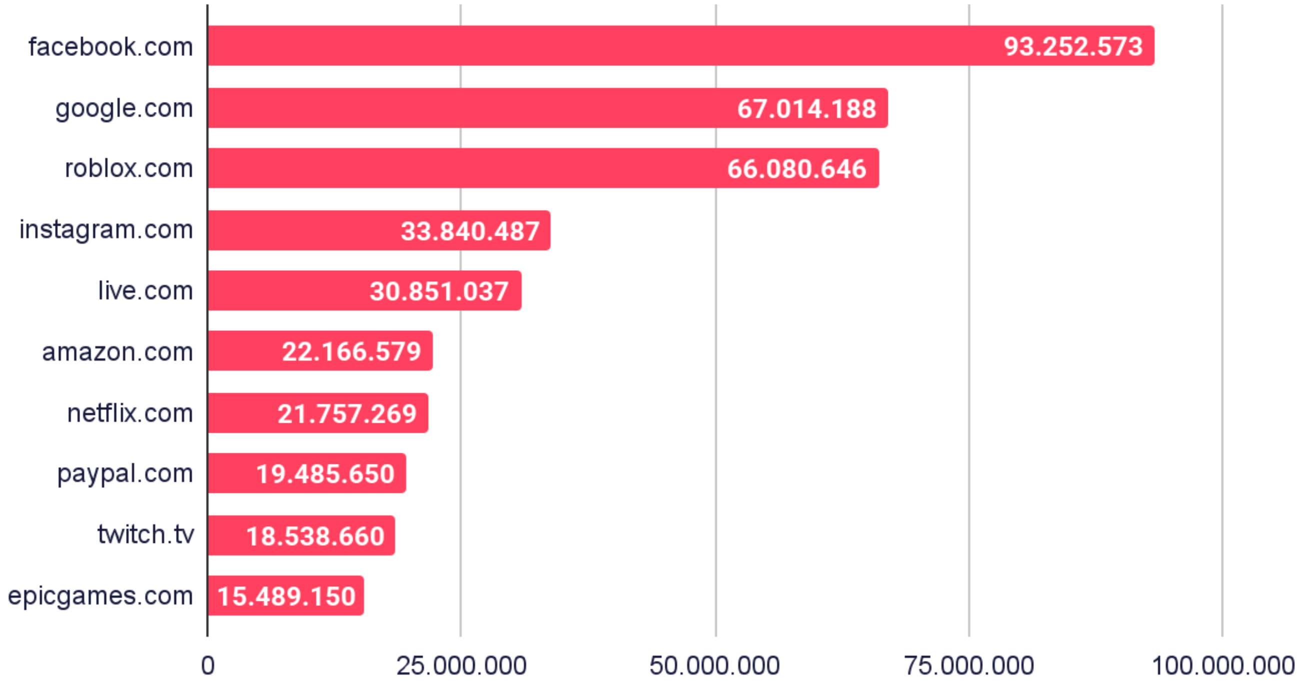
An AI tool named "LiarAI" being offered for sale on a Dark Web forum - ***SOCRadar Advanced Dark Web Monitoring***

The example tool, LiarAI, is advertised with capabilities including answering illegal questions, developing exploits and malware at a high level, interacting with the internet and generating images.

Overall, the current situation challenges existing thinking models focused on underground markets for malicious AI tools and raises difficult questions about regulation, platform governance, and responsibility.

Stealer Logs

Distribution of Stealer Logs by Domains



Stealer logs show extreme concentration on major consumer platforms. Facebook and Google lead by a wide margin, confirming their value for any type of malicious operation.

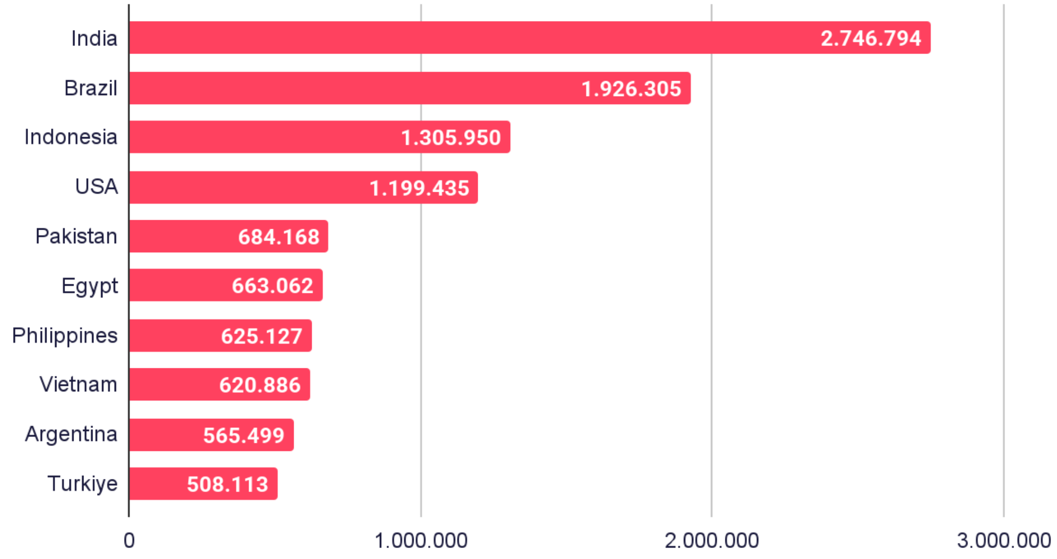
Gaming platforms such as Roblox, Twitch, and Epic Games together make up a high volume, reflecting younger user bases and weak credential hygiene.

E-commerce and streaming services, including Amazon and Netflix, remain attractive due to stored payment data and account resale value in other markets.

PayPal stands out as a direct fraud enabler rather than a secondary asset.

Overall, stealer activity focuses on platforms that combine scale, credential reuse, and immediate monetization paths across multiple fraud types.

Distribution of Stealer Logs by Country



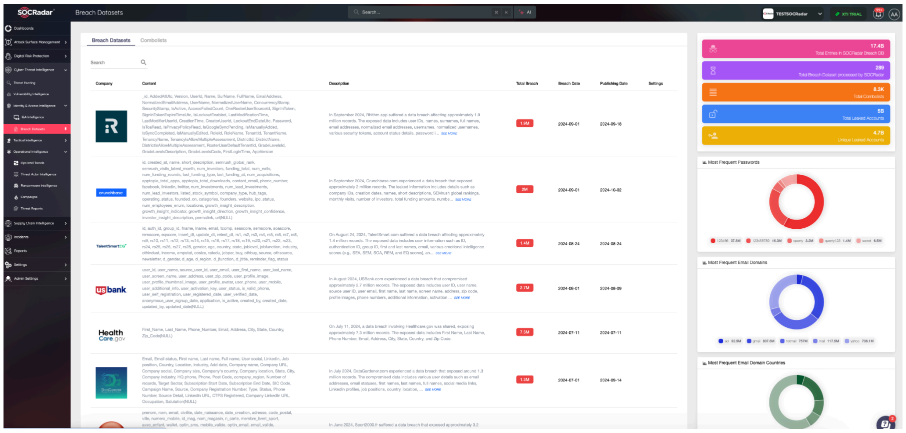
Stealer logs are heavily concentrated in emerging and densely populated markets.

India leads by a wide margin, which points to large scale malware spread and high credential reuse.

Brazil and Indonesia follow, showing similar exposure driven by consumer platforms and low endpoint protection.

The United States appears lower than expected, which suggests better detection or faster remediation rather than lower infection rates.

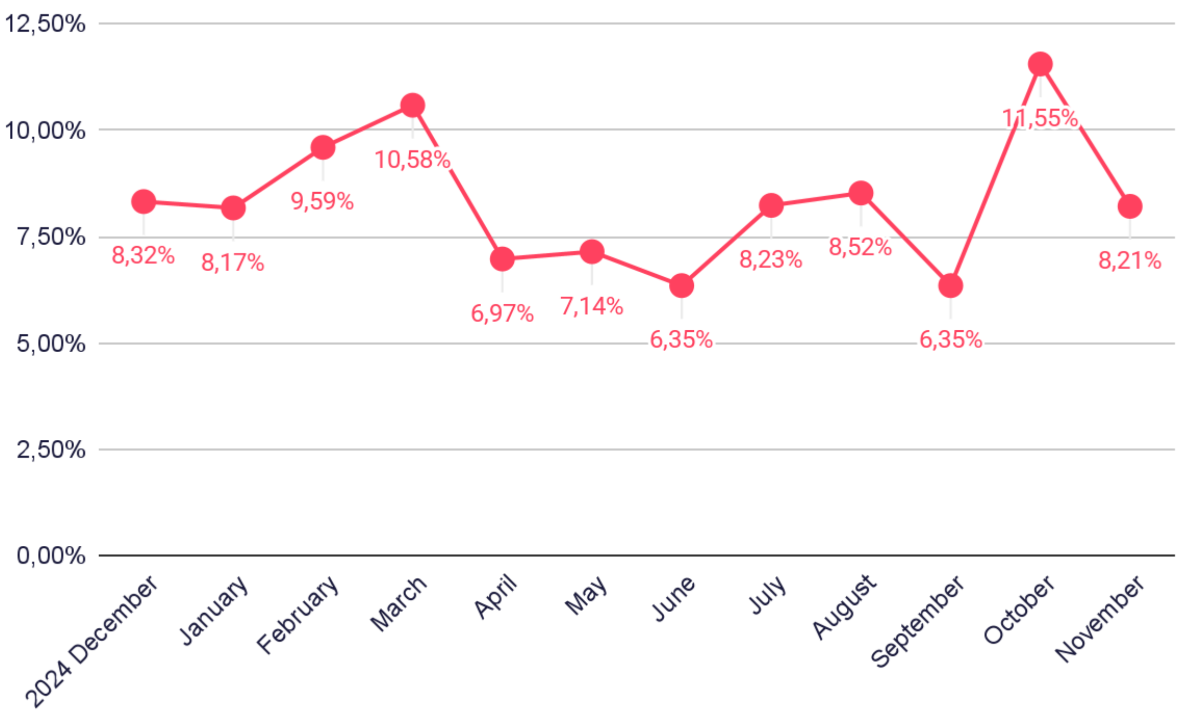
Overall, we see a stealer activity correlates with user scale and software piracy.


SOCRadar
Breach Datasets
Combolists
Most Frequent Passwords
Most Frequent Email Domains
Most Frequent Email Domain Countries

SOCRadar's Identity & Access Intelligence Module can detect stealers on your devices and identify their location, facilitating a secure working environment. Changing passwords without eliminating stealers is insufficient to secure your organization, as it will only provide new passwords to threat actors.

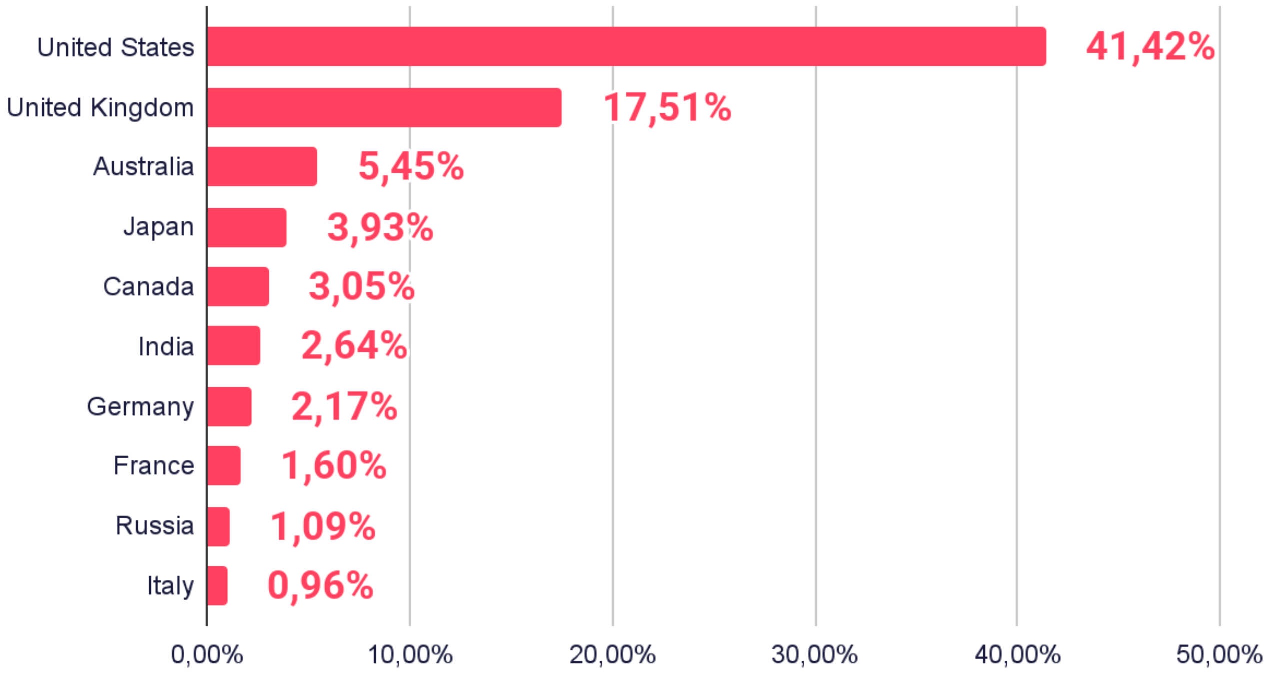
Ransomware Threat Landscape

Time Analysis of Ransomware Attacks



We've scoured ransomware groups' blog sites, leak sites, and Telegram channels to compile a trove of valuable information.

Distribution of Ransomware Attacks by Affected Country

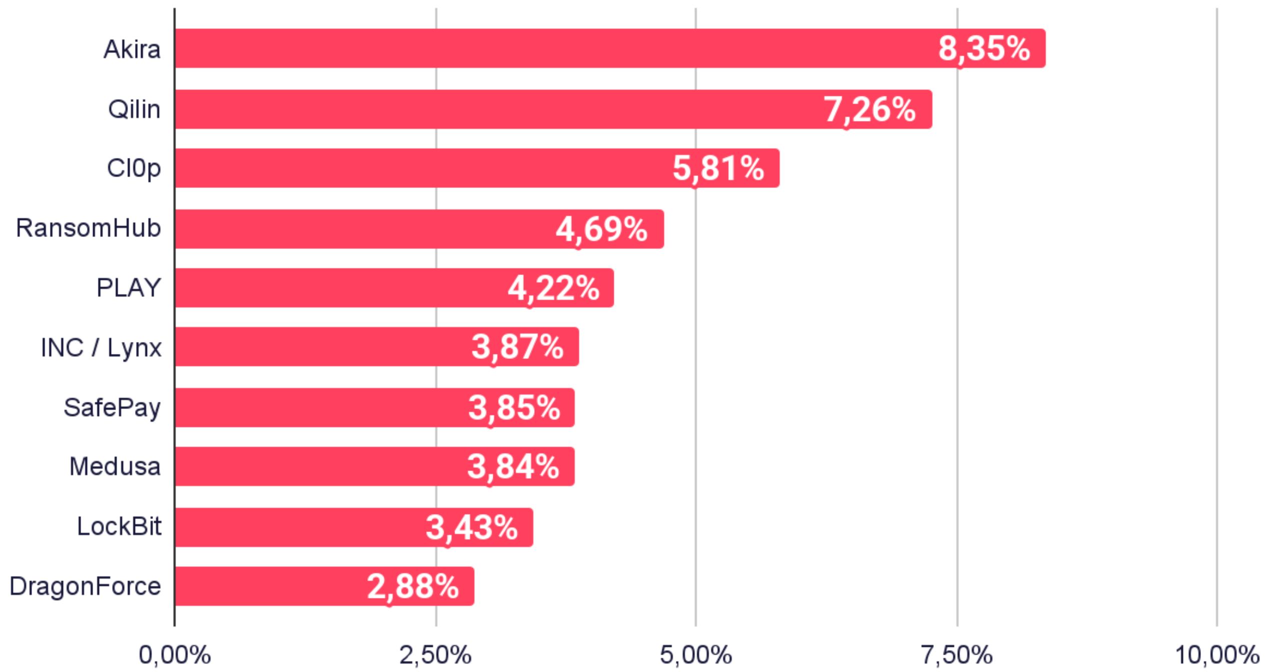


The United States is the primary ransomware target with 41.42% of observed attacks, reflecting its high concentration of large organizations and strong ransom payment capacity.

Australia and Japan show moderate exposure, often linked to critical services and manufacturing.

Overall, attackers focus on countries with payment potential.

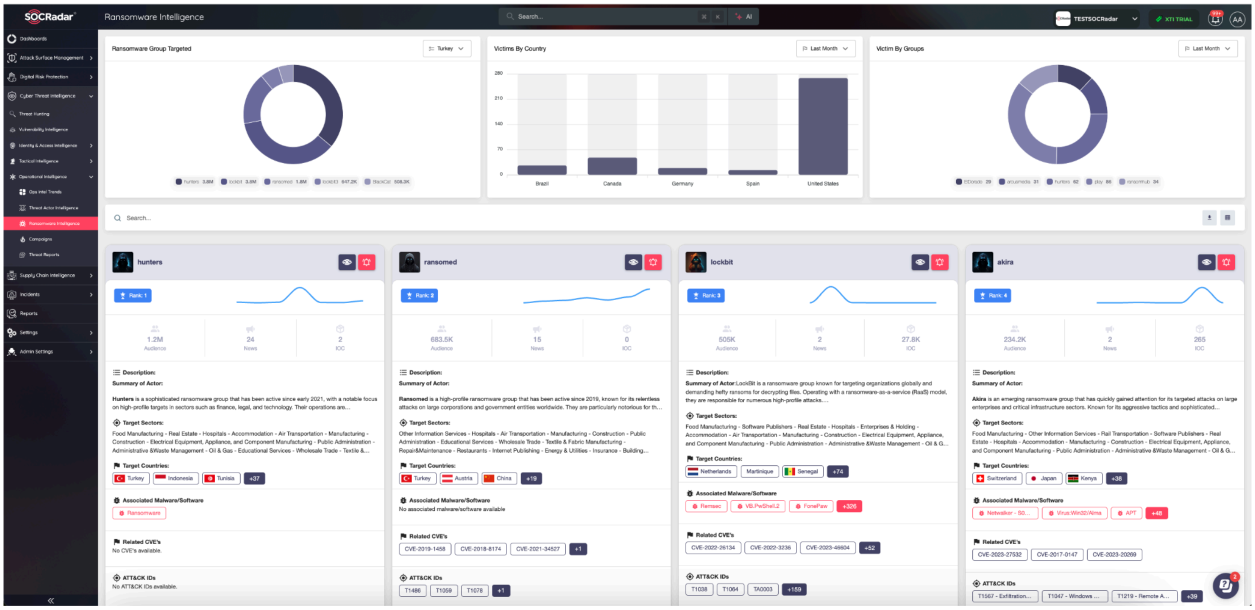
Most Active Ransomware Groups



Akira leads ransomware activity with 8.35% while Qilin and Cl0p follow closely, showing continued effectiveness in high impact campaigns and data extortion.

Top 10 actors make up almost half of ransomware incidents in 2025. This indicates a fragmented but competitive ecosystem.

This distribution among many groups increases unpredictability and complicates security efforts.



hunters

Rank: 1

1.2M Audience | 24 News | 2 IOC

Description:
Summary of Actor:
Hunters is a sophisticated ransomware group that has been active since early 2021, with a notable focus on high-profile targets in sectors such as finance, legal, and technology. Their operations are...

Target Sectors:
Food Manufacturing - Real Estate - Hospitals - Accommodation - Air Transportation - Manufacturing - Construction - Electrical Equipment, Appliance, and Component Manufacturing - Public Administration - Administrative &Waste Management - Oil & Gas - Educational Services - Wholesale Trade - Textile &...

Target Countries:
Turkey | Indonesia | Tunisia | +37

Associated Malware/Software
Ransomware

Related CVE's
No CVE's available.

ATT&CK IDs
No ATT&CK IDs available.

ransomed

Rank: 2

683.5K Audience | 15 News | 0 IOC

Description:
Summary of Actor:
Ransomed is a high-profile ransomware group that has been active since 2019, known for its relentless attacks on large corporations and government entities worldwide. They are particularly notorious for th...

Target Sectors:
Other Information Services - Hospitals - Air Transportation - Manufacturing - Construction - Public Administration - Educational Services - Wholesale Trade - Textile & Fabric Manufacturing - Repair&Maintenance - Restaurants - Internet Publishing - Energy & Utilities - Insurance - Building...

Target Countries:
Turkey | Austria | China | +19

Associated Malware/Software
No associated malware/software available

Related CVE's
CVE-2019-1458 | CVE-2018-8174 | CVE-2021-34527 | +1

ATT&CK IDs
T1486 | T1059 | T1078 | +1

lockbit

Rank: 3

505K Audience | 2 News | 27.8K IOC

Description:
Summary of Actor: LockBit is a ransomware group known for targeting organizations globally and demanding hefty ransoms for decrypting files. Operating with a ransomware-as-a-service (RaaS) model, they are responsible for numerous high-profile attacks....

Target Sectors:
Food Manufacturing - Software Publishers - Real Estate - Hospitals - Enterprises & Holding - Accommodation - Air Transportation - Manufacturing - Construction - Electrical Equipment, Appliance, and Component Manufacturing - Public Administration - Administrative &Waste Management - Oil & G...

Target Countries:
Netherlands | Martinique | Senegal | +74

Associated Malware/Software
Remsec | VB.PwShell.2 | FonePaw | +326

Related CVE's
CVE-2022-26134 | CVE-2022-3236 | CVE-2023-46604 | +52

ATT&CK IDs
T1038 | T1064 | TA0003 | +159

akira

Rank: 4

234.2K Audience | 2 News | 265 IOC

Description:
Summary of Actor:
Akira is an emerging ransomware group that has quickly gained attention for its targeted attacks on large enterprises and critical infrastructure sectors. Known for its aggressive tactics and sophisticated...

Target Sectors:
Food Manufacturing - Other Information Services - Rail Transportation - Software Publishers - Real Estate - Hospitals - Accommodation - Manufacturing - Construction - Electrical Equipment, Appliance, and Component Manufacturing - Public Administration - Administrative &Waste Management - Oil & G...

Target Countries:
Switzerland | Japan | Kenya | +38

Associated Malware/Software
Netwalker - S0... | Virus:Win32/Alma | APT | +48

Related CVE's
CVE-2023-27532 | CVE-2017-0147 | CVE-2023-20269

ATT&CK IDs
T1567 - Exfiltration... | T1047 - Windows ... | T1219 - Remote A... | +39

Explore SOCRadar's Ransomware Intelligence module and gain comprehensive insights with detailed group profiles, MITRE Visualizer, and actionable IOCs. These insights will empower you to stay ahead of evolving threats and enhance your cybersecurity strategy.

Who is SOCRadar?

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by
21.000+ companies
in 150+ countries

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.