flare

Stealer Logs & Corporate Access

By Eric Clay

Table Of Contents

Introduction

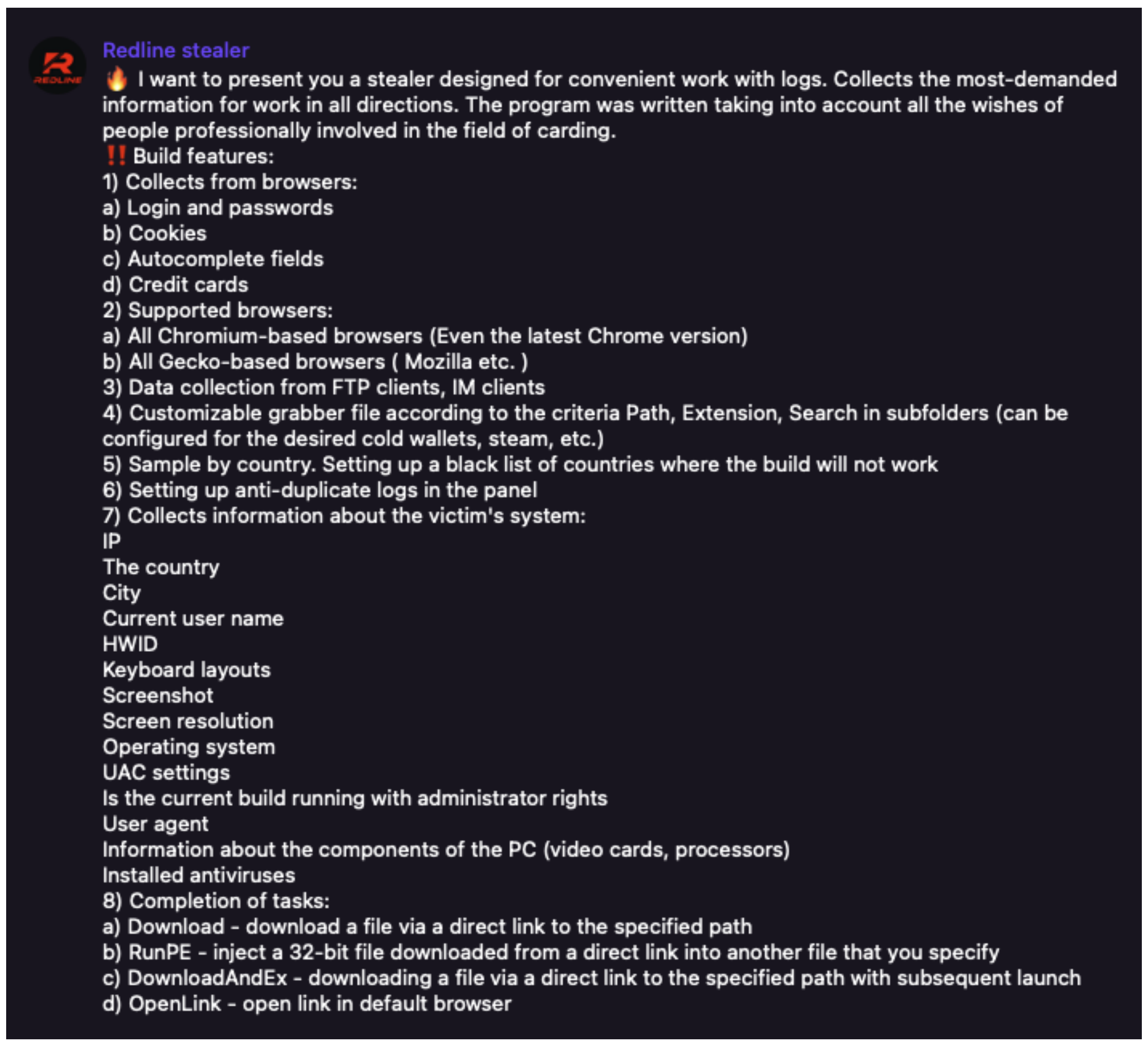
The exponential growth of infostealer malware has been one of the core trends in cybercrime for the past three years. Infostealer variants such as Redline, Raccoon, Titan, Aurora, and Vidar can infect consumer and corporate computers and pull credentials from the device's browsers. These "stealer logs" are then packaged together and given away or sold on **dark web markets** and **Telegram channels**.

The explosive growth of Infostealer malware represents an ongoing and significant threat to all organizations. Employees regularly save corporate credentials on personal devices or access personal resources on organizational devices, increasing the risk of infection. A complex ecosystem exists in which Malware as a Service (MaaS) vendors sell infostealer malware on illicit Telegram channels, threat actors distribute it through fake cracked software or phishing emails, and they then sell infected device accesses on specialized dark web marketplaces.

When compared to more "traditional" forms of dark web risk, such as credential stuffing, infected devices pose a unique risk; once infostealer malware infects a device, it employs several complex obfuscation techniques and begins exfiltrating data back to a dedicated command and control infrastructure. The data exfiltrated typically includes:

- The web browser's fingerprint (including all passwords and forms saved in the browser)
- Operating system information
- ISP information
- Cryptocurrency wallet logins
- Potentially confidential or sensitive files

This Flare research report examines multiple data sets including more than 19.6 million stealer logs and aims to understand how many infostealer infections contain access to corporate credentials, what the average price of infostealers with banking access is, and how prominent consumer applications appear in infostealer logs.



Redline stealer
🔥 I want to present you a stealer designed for convenient work with logs. Collects the most-demanded information for work in all directions. The program was written taking into account all the wishes of people professionally involved in the field of carding.
‼️ Build features:
1) Collects from browsers:
a) Login and passwords
b) Cookies
c) Autocomplete fields
d) Credit cards
2) Supported browsers:
a) All Chromium-based browsers (Even the latest Chrome version)
b) All Gecko-based browsers (Mozilla etc.)
3) Data collection from FTP clients, IM clients
4) Customizable grabber file according to the criteria Path, Extension, Search in subfolders (can be configured for the desired cold wallets, steam, etc.)
5) Sample by country. Setting up a black list of countries where the build will not work
6) Setting up anti-duplicate logs in the panel
7) Collects information about the victim's system:
IP
The country
City
Current user name
HWID
Keyboard layouts
Screenshot
Screen resolution
Operating system
UAC settings
Is the current build running with administrator rights
User agent
Information about the components of the PC (video cards, processors)
Installed antiviruses
8) Completion of tasks:
a) Download - download a file via a direct link to the specified path
b) RunPE - inject a 32-bit file downloaded from a direct link into another file that you specify
c) DownloadAndEx - downloading a file via a direct link to the specified path with subsequent launch
d) OpenLink - open link in default browser

Threat actor promotes RedLine stealer malware

Key Findings

- Based on our analysis of more than 19.6 million stealer logs, at least **1.91%** of stealer logs contain access to credentials for business applications commonly used by organizations all around the world such as Salesforce, Hubspot, AWS, GCP, domains containing Okta, and DocuSign representing **376,107** logs in our sample.

    - (Please note that this statistic reflects user credentials of these applications for sale, and does not indicate that credentials belonging to employees of the listed organizations have been compromised or that the organization's themselves have suffered a data breach).

- 48,173 logs contain access to a resource that includes "okta.com" representing almost certain access to corporate resources.

- Stealer logs containing access to financial services accounts such as banking and retirement portals fetched a significantly higher price on Genesis Market than those with access to consumer applications only (average of **$112** for financial services-related logs versus an average of **$15** across all logs for sale).

- More than **200,000** stealer logs contain access to OpenAI credentials, representing **1%** of all stealer logs analyzed.

- Russian Market and VIP Telegram rooms represented the most common sources of corporate access in our sample data.

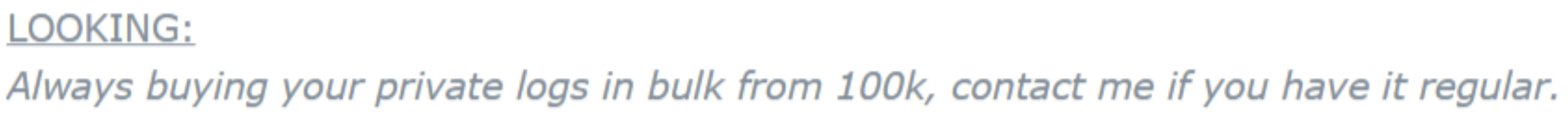
- In our sample of stealer logs, **46.9%** had access to Gmail credentials, representing more than eight million infected devices.

The Tiers of Infostealer Access

To make stealer logs easier to understand, we divided them into tiers based on the type of credentials contained in the stealer log and the type of access that the threat actor is likely attempting to gain by using the credentials present: Tier 1 Logs: Corporate IT and Business Application Access, Tier 2 Logs: Infected Devices and Banking, and Tier 3 Logs: Consumer Applications & Stealer Logs.

Tier 1 Logs: High-Value Corporate Credentials

Many employees save passwords in their browsers. When infostealer malware infects their computers, it simultaneously compromises all credentials saved in the browser. This can include CRMs, credentials for RDP, VPNs, SaaS application access, and other corporate devices. Threat actors most highly value corporate credentials, and initial access brokers often target these to exploit and expand access before reselling on top-tier dark web forums such as Exploit and XSS.



LOOKING:

Always buying your private logs in bulk from 100k, contact me if you have it regular.

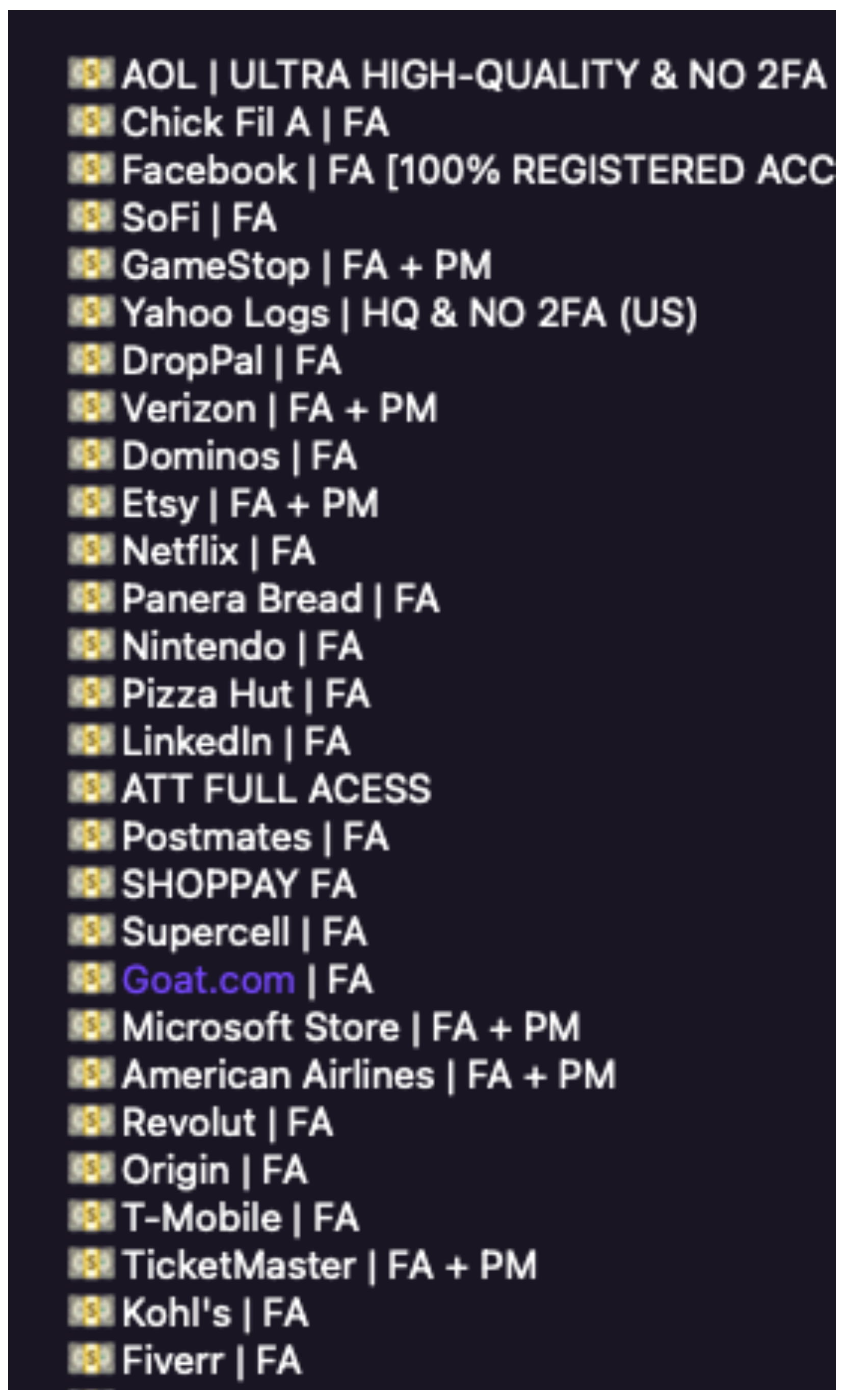
Post from the dark web forum Exploit In where an initial access broker looks to purchase bulk stealer logs

Tier 2 Logs: Banking and Financial Services Credentials

These logs have available credentials for major consumer banks, which threat actors can use to directly steal or spend money from consumer accounts. Cybercriminals also highly value these, as they fetch an average of $112 on Genesis Market (compared to an average of $15 across all logs for sale). In some cases, threat actors will target personal or business banking accounts and resell access on Telegram or dark web markets.

Tier 3 Logs: Consumer Applications

These logs are useful because threat actors can use them to gain access to consumer VPN applications, streaming services, and other applications in order to save money on monthly subscriptions. These are the lowest-valued logs, typically selling for about $10–$15 per log file.



💵 AOL | ULTRA HIGH-QUALITY & NO 2FA
💵 Chick Fil A | FA
💵 Facebook | FA [100% REGISTERED ACC
💵 SoFi | FA
💵 GameStop | FA + PM
💵 Yahoo Logs | HQ & NO 2FA (US)
💵 DropPal | FA
💵 Verizon | FA + PM
💵 Dominos | FA
💵 Etsy | FA + PM
💵 Netflix | FA
💵 Panera Bread | FA
💵 Nintendo | FA
💵 Pizza Hut | FA
💵 LinkedIn | FA
💵 ATT FULL ACESS
💵 Postmates | FA
💵 SHOPPAY FA
💵 Supercell | FA
💵 Goat.com | FA
💵 Microsoft Store | FA + PM
💵 American Airlines | FA + PM
💵 Revolut | FA
💵 Origin | FA
💵 T-Mobile | FA
💵 TicketMaster | FA + PM
💵 Kohl's | FA
💵 Fiverr | FA

Threat actor lists logs with consumer application access for sale

Where are Stealer Logs Distributed?

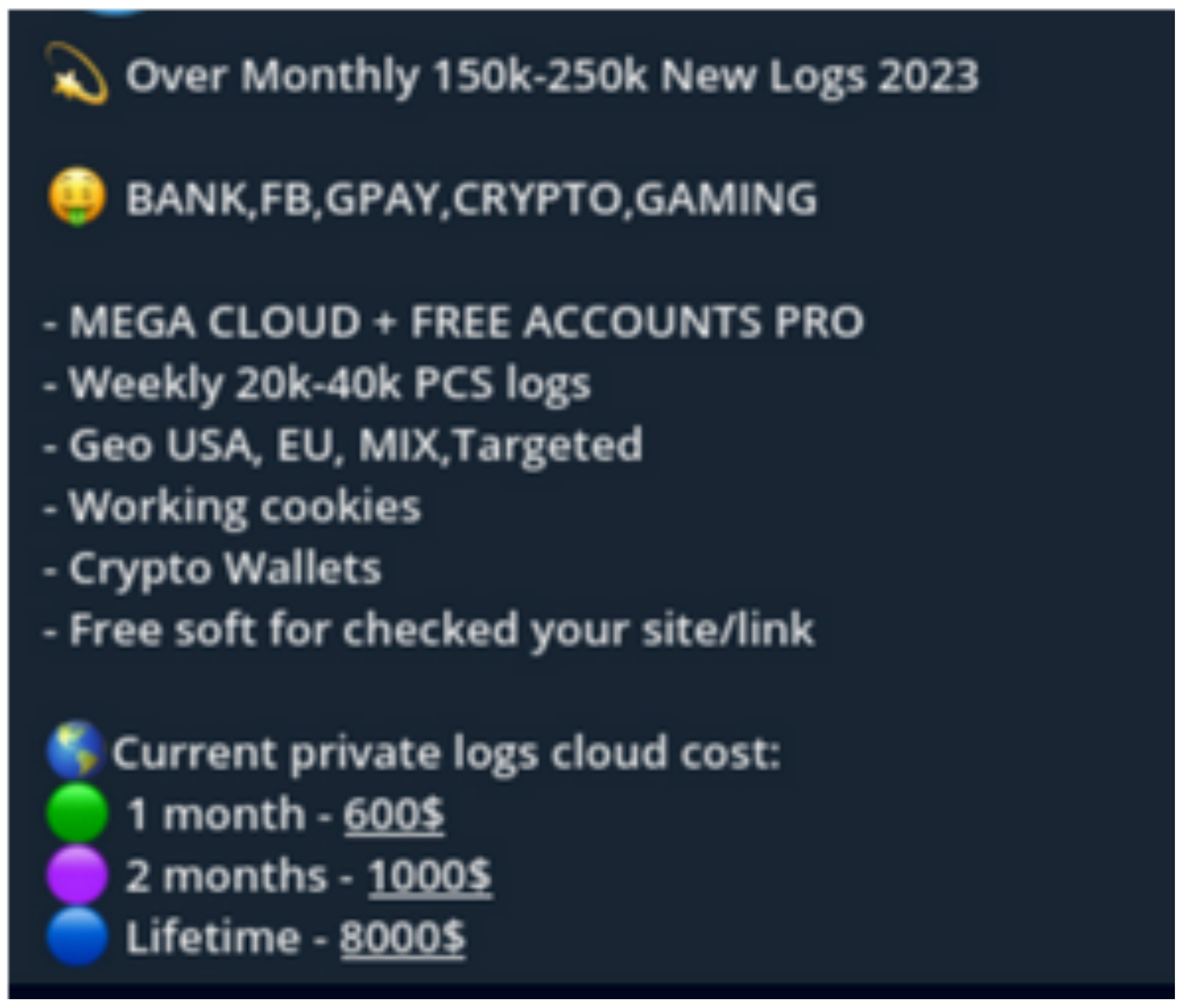
We can generally categorize stealer log distribution into four buckets, each with its own pricing system and value proposition to the threat actor.

Public Telegram "Logs" Channels

These are publicly available Telegram channels that provide terabytes of stealer logs per month, mostly "Tier 3" logs that contain access to consumer applications. These are advertisements for pay-to-play private Telegram rooms (in much the same way that Costco and Trader Joe's give out free food samples). VIP Channels often cost several hundred dollars per month and have additional access requirements.

Private Telegram Channels

Threat actors host these rooms in order to distribute vast quantities of logs with a monthly subscription model that monetizes access. These are often higher-value logs, with far fewer threat actors having access to them. We suspect this is the primary way that cybercriminals monetize stealer logs on Telegram. These channels are invitation-only and typically limited to 25–30 users, with hundreds of thousands of logs posted per month directly into the channel or provided through MEGA for large file sizes.



💫 Over Monthly 150k-250k New Logs 2023

🤑 BANK,FB,GPAY,CRYPTO,GAMING

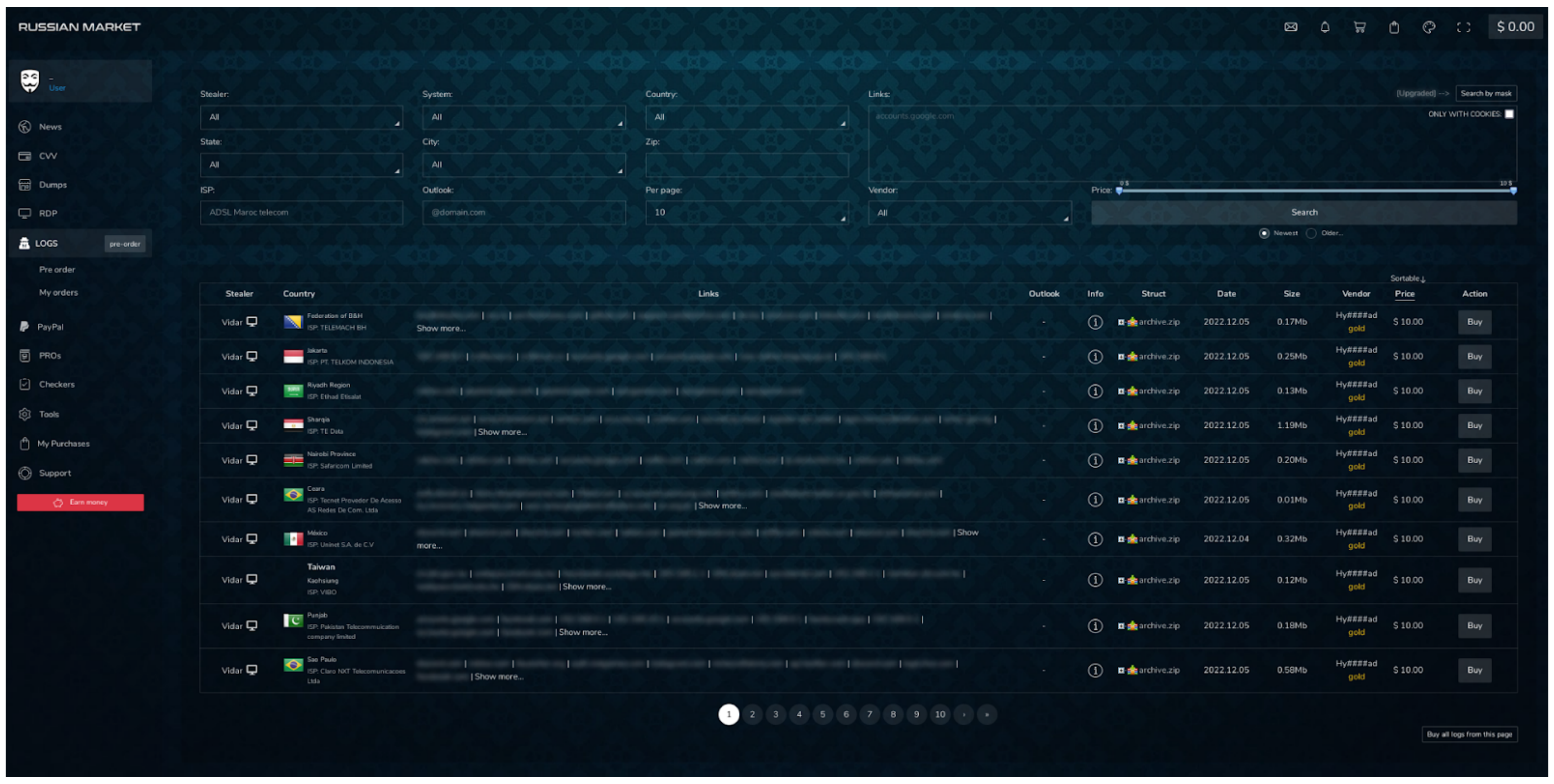
- MEGA CLOUD + FREE ACCOUNTS PRO
- Weekly 20k-40k PCS logs
- Geo USA, EU, MIX,Targeted
- Working cookies
- Crypto Wallets
- Free soft for checked your site/link

🌎 Current private logs cloud cost:
🟢 1 month - 600$
🟣 2 months - 1000$
🔵 Lifetime - 8000$

Threat actor's advertisement for a subscription stealer log Telegram channel

Russian Market

Russian Market is a dark web marketplace specializing in the sale of access to devices and information. Russian Market prices all logs equally at $10 per log and operates on the dark web.



Stealer: All
System: All
Country: All
Links: accounts.google.com
(Upgraded) -->
ONLY WITH COOKIES: □
State: All
City: All
Zip:
ISP: ADSL Maroc telecom
Outlook: @domain.com
Per page: 10
Vendor: All
Price: 0 $ – 10 $
● Newest ○ Older...

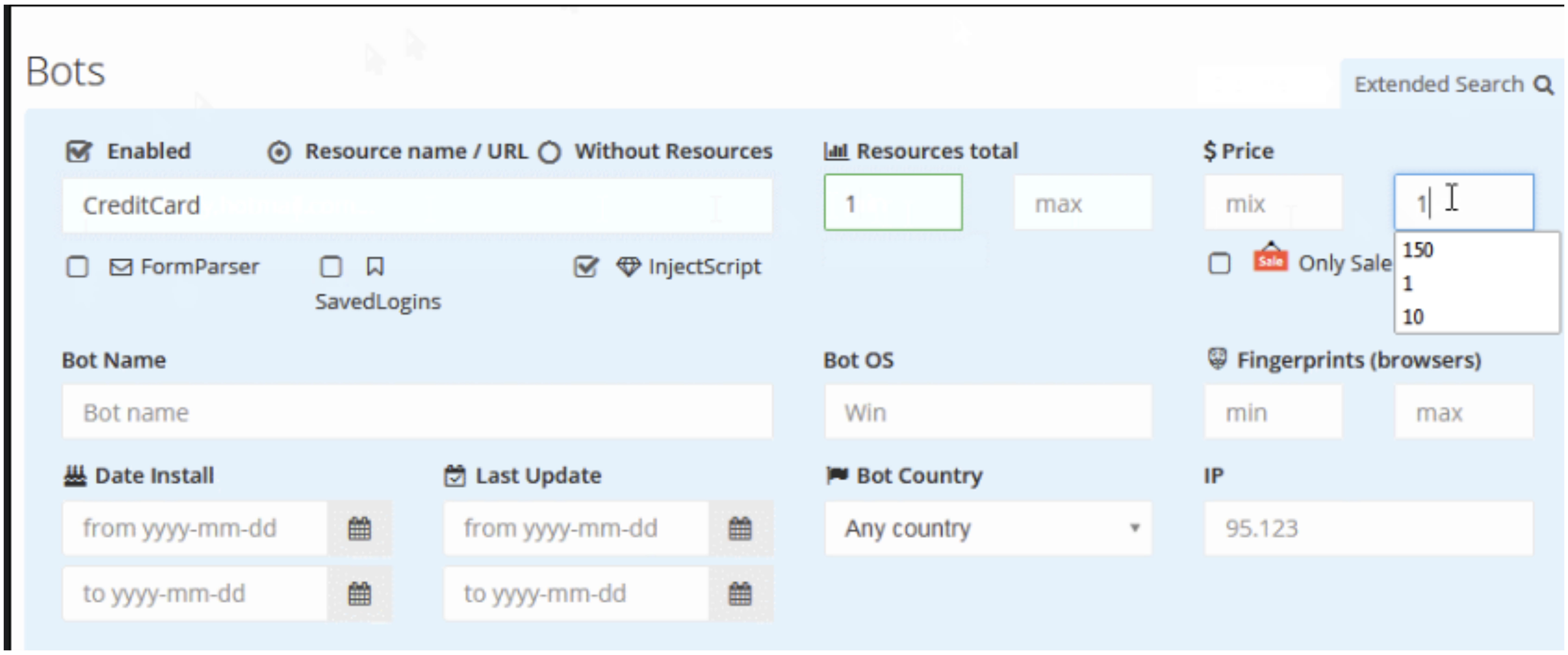
Stealer	Country	Links	Outlook	Info	Struct	Date	Size	Vendor	Sortable↓ Price	Action
Vidar	Federation of B&H ISP: TELEMACH BH	[redacted] Show more...	-	ⓘ	archive.zip	2022.12.05	0.17Mb	Hy####ad gold	$ 10.00	Buy
Vidar	Jakarta ISP: PT. TELKOM INDONESIA	[redacted]	-	ⓘ	archive.zip	2022.12.05	0.25Mb	Hy####ad gold	$ 10.00	Buy
Vidar	Riyadh Region ISP: Etihad Etisalat	[redacted]	-	ⓘ	archive.zip	2022.12.05	0.13Mb	Hy####ad gold	$ 10.00	Buy
Vidar	Sharqia ISP: TE Data	[redacted] | Show more...	-	ⓘ	archive.zip	2022.12.05	1.19Mb	Hy####ad gold	$ 10.00	Buy
Vidar	Nairobi Province ISP: Safaricom Limited	[redacted]	-	ⓘ	archive.zip	2022.12.05	0.20Mb	Hy####ad gold	$ 10.00	Buy
Vidar	Ceara ISP: Tecnet Provedor De Acesso AS Redes De Com. Ltda	[redacted] | Show more...	-	ⓘ	archive.zip	2022.12.05	0.01Mb	Hy####ad gold	$ 10.00	Buy
Vidar	México ISP: Uninet S.A. de C.V	[redacted] | Show more...	-	ⓘ	archive.zip	2022.12.04	0.32Mb	Hy####ad gold	$ 10.00	Buy
Vidar	Taiwan Kaohsiung ISP: VIBO	[redacted] | Show more...	-	ⓘ	archive.zip	2022.12.05	0.12Mb	Hy####ad gold	$ 10.00	Buy
Vidar	Punjab ISP: Pakistan Telecommuication company limited	[redacted] | Show more...	-	ⓘ	archive.zip	2022.12.05	0.18Mb	Hy####ad gold	$ 10.00	Buy
Vidar	Sao Paulo ISP: Claro NXT Telecomunicacoes Ltda	[redacted] | Show more...	-	ⓘ	archive.zip	2022.12.05	0.58Mb	Hy####ad gold	$ 10.00	Buy

The homepage of Russian Market

Genesis Market

Genesis Market operated as a clear web market prior to the recent law enforcement takedown. More recently, it has operated entirely on Tor. Compared to Telegram channels, Genesis Market provides structured, parsed log data and an interface that enables threat actors to seamlessly clone the browser fingerprint of a victim. Prices vary across Genesis Market listings based on the perceived value of the device.

The number of consumer applications is directly proportional to what we see as the most common use case among malicious actors for stealer logs. Most actors are not looking to hack into corporate environments; instead, they are searching for easy access to basic consumer applications to save a few dollars or, in more sophisticated cases, compromise a bank account to purchase cryptocurrency or drain the account.



Bots

Extended Search

☑ Enabled ● Resource name / URL ○ Without Resources
CreditCard

□ FormParser □ SavedLogins ☑ InjectScript

Resources total
1
max

$ Price
mix
1
150
1
10

□ Only Sale

Bot Name
Bot name

Bot OS
Win

Fingerprints (browsers)
min
max

Date Install
from yyyy-mm-dd
to yyyy-mm-dd

Last Update
from yyyy-mm-dd
to yyyy-mm-dd

Bot Country
Any country

IP
95.123

Genesis Market visitors can search for bots with certain features

Tier 1 Logs: Corporate IT Consumer SaaS Application Access

There is a subset of logs that we believe are valued because they have access to corporate IT environments. Initial access brokers who sell access to corporate IT environments on dark web forums such as Exploit In and XSS specifically seek out these stealer logs as a way to facilitate initial access.

In order to determine whether an infected device has corporate access at scale, we came up with certain indicators that we believe are likely to be highly correlated with corporate access. By looking at stealer logs that contain access to SaaS applications commonly used by organizations, we can establish a baseline for how common access to corporate SaaS resources is across our data set. We believe the following credentials contained in a stealer log make it highly likely that it contains access to a business resource:

1. **Corporate IT Infrastructure**

- signin.aws.amazon.com
- console.cloud.google.com

2. **Business Contract & Financial Applications**

- accounts.intuit.com
- account.docusign.com
- Subdomains including Okta

3. **CRM and Customer Data Applications**

- app.hubspot.com
- login.salesforce.com

Please note that this represents only a small number of applications that could indicate corporate access. Our numbers should serve as a baseline for potential access, not as a definitive estimate. We believe if additional applications were factored in, 2–3% or more of stealer logs would likely contain corporate access.

1. Corporate IT Infrastructure

We began by searching our database of stealer logs for logins that had access to AWS Management and Google Cloud Consoles. This turned up 181,785 results, or 0.92% of our log sample. Compared to Google Cloud Console, logs containing AWS console access were significantly overrepresented, likely as a result in substantially higher AWS adoption among consumers.

Compared to other potentially compromised infrastructure, AWS Management and Google Cloud Consoles represent a particularly high degree of risk given potential access to core infrastructure used in both internal and SaaS applications, along with data stored in cloud storage.

- We found 179,411 AWS Console credentials out of 19.4 million logs sampled.
- We found 2,344 Google Cloud credentials in the same sample.
- The vast majority of these credentials appeared in public and private Telegram rooms, with slightly more than **75%** appearing on Telegram, **24%** on Russian Market, and less than **1%** on Genesis Market, closely mirroring our sample data.

2. Business Contracts and Financial Applications

Another classification we used was business financial applications such as Intuit Quickbooks and DocuSign. We identified 80,099 stealer logs that had access to one of these applications, with the majority being DocuSign credentials at 64,548. Access to these applications was found overall in 0.4% of stealer logs.

- Logs containing access to QuickBooks and DocuSign accounts were overrepresented in public Telegram and Russian Market compared to our overall collection, potentially representing variance in the way that threat actors on those sources infect hosts.
- We identified 64,548 logs with DocuSign credentials and 15,591 with access to QuickBooks.

3. CRM and Customer Data Applications

The last category we reviewed was stealer logs providing access to CRM environments. For this exercise, we reviewed the two largest CRM providers, Salesforce and Hubspot, to identify logs with credentials to those providers.

- Logs containing access to Salesforce accounts: 23,267.
- Logs containing access to Hubspot accounts: 42,783.
- Logs containing access to CRM total: 66,050.
- Percentage of logs containing access to a CRM: 0.03%.

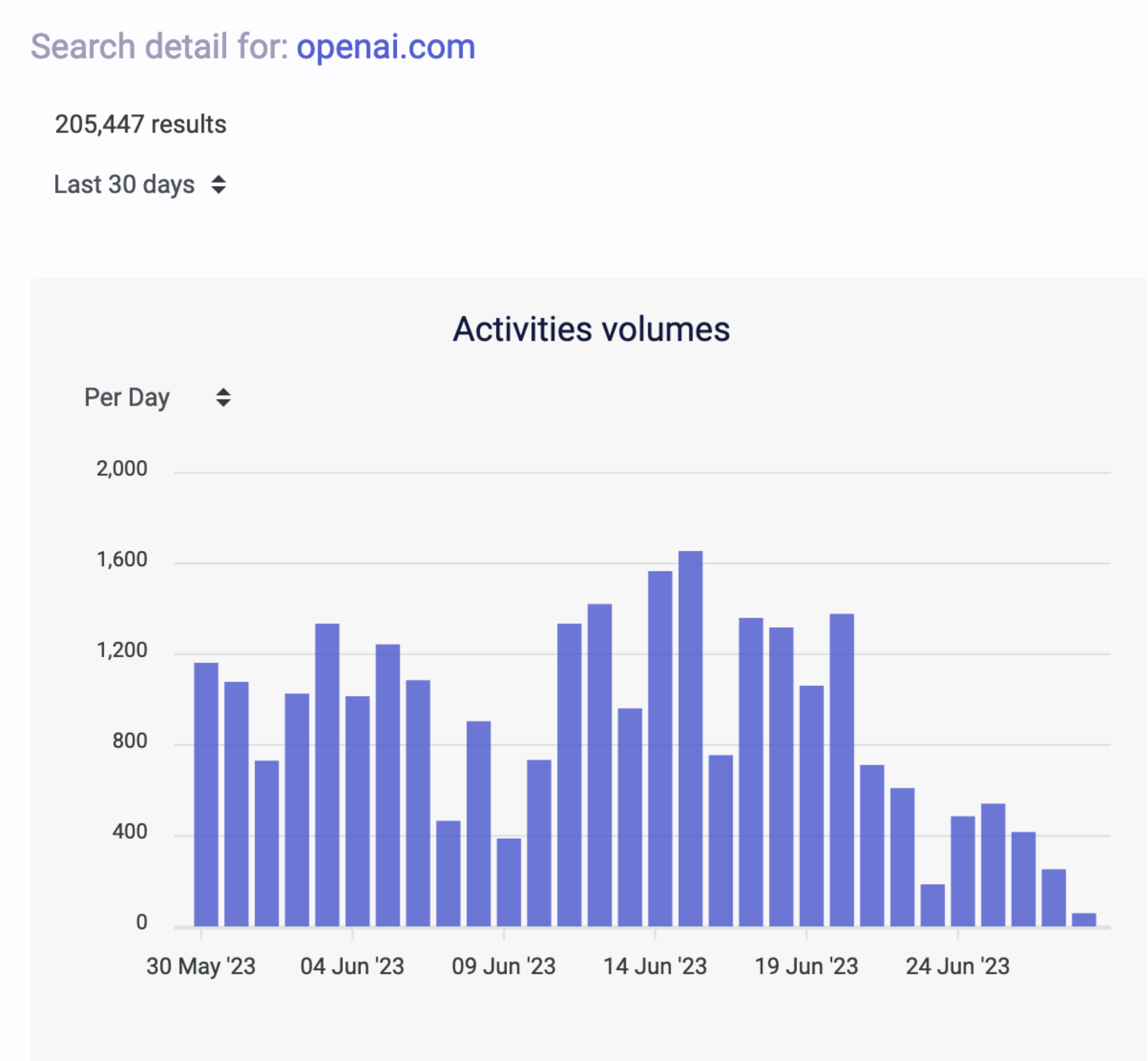
CRM credentials were the second most unusual form of credential to show up out of the three categories we reviewed, despite the fact that teams across marketing, sales, business operations, and customer success often have access to CRM environments.

Bonus: OpenAI and ChatGPT Stealer Logs

Businesses and consumers both use ChatGPT. Considering that in many cases employees may put sensitive information into ChatGPT, we thought it would be interesting to see how many compromised credentials are present in stealer logs that contain “openai.com.”

We found more than 200,000 logs containing OpenAI credentials, representing another significant vector that attackers could use to harvest both corporate and personal information. More than 180,000 OpenAI credentials were leaked in 2023, while only 20,000 were leaked in 2022, demonstrating the rapid rise of interest in ChatGPT and GPT-4 among consumers and businesses.

ChatGPT can be particularly high-risk since conversations are saved by default, potentially exposing sensitive corporate intellectual property and other data should the account be compromised.



Search detail for: openai.com

205,447 results

Last 30 days

Flare shows the number of stealer logs with compromised OpenAI credentials

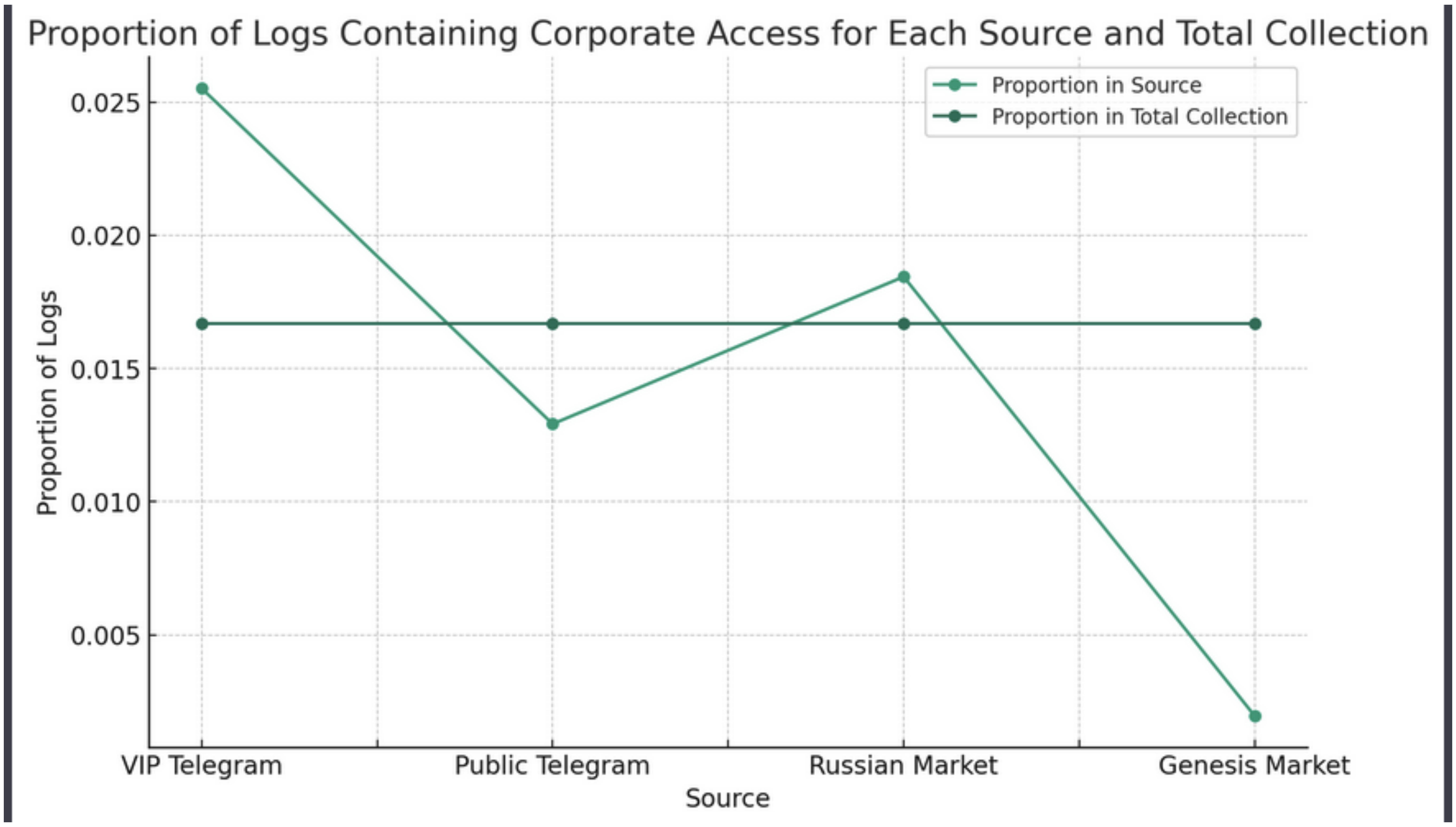
Key Findings

Based on the limited sample of three types of corporate credentials we looked at there are a few conclusions that can be drawn, and some data can be extrapolated with less confident results.

- It is highly likely that at least 1.91% of stealer logs contain corporate access, given that we found 376,107 logs (excluding OpenAI) with credentials that indicate a high likelihood of accessing business resources. If we were to factor in dozens of other common corporate resources, this would likely bring the number well above 2%.

- Logs containing corporate access were overrepresented on Russian Market and VIP Telegram channels, indicating that the methods attackers use to harvest logs may incidentally or intentionally have more corporate targeting. Additionally, public Telegram channels may deliberately post lower value logs, saving high-value logs for paying customers.

- Based on evidence from the dark web forum Exploit.IN, we rate it as highly likely that initial access brokers (IABs) are using stealer logs as a principal source to gain an initial foothold to corporate environments that can then be auctioned off on top-tier dark web forums.



Graph shows proportion of stealer logs containing corporate access for each source and total collection

This chart maps the proportion of stealer logs with corporate access against the proportion of stealer logs representing our total collection, showing that VIP Telegram channels have far more corporate credentials than other sources.

Tier 2 Logs: Infected Devices and Banking

Our second tier of logs is focused on financial services and banking applications. These are the second most highly valued type of stealer logs. Threat actors can use these credentials to directly access consumer financial accounts and purchase cryptocurrency or wire funds.

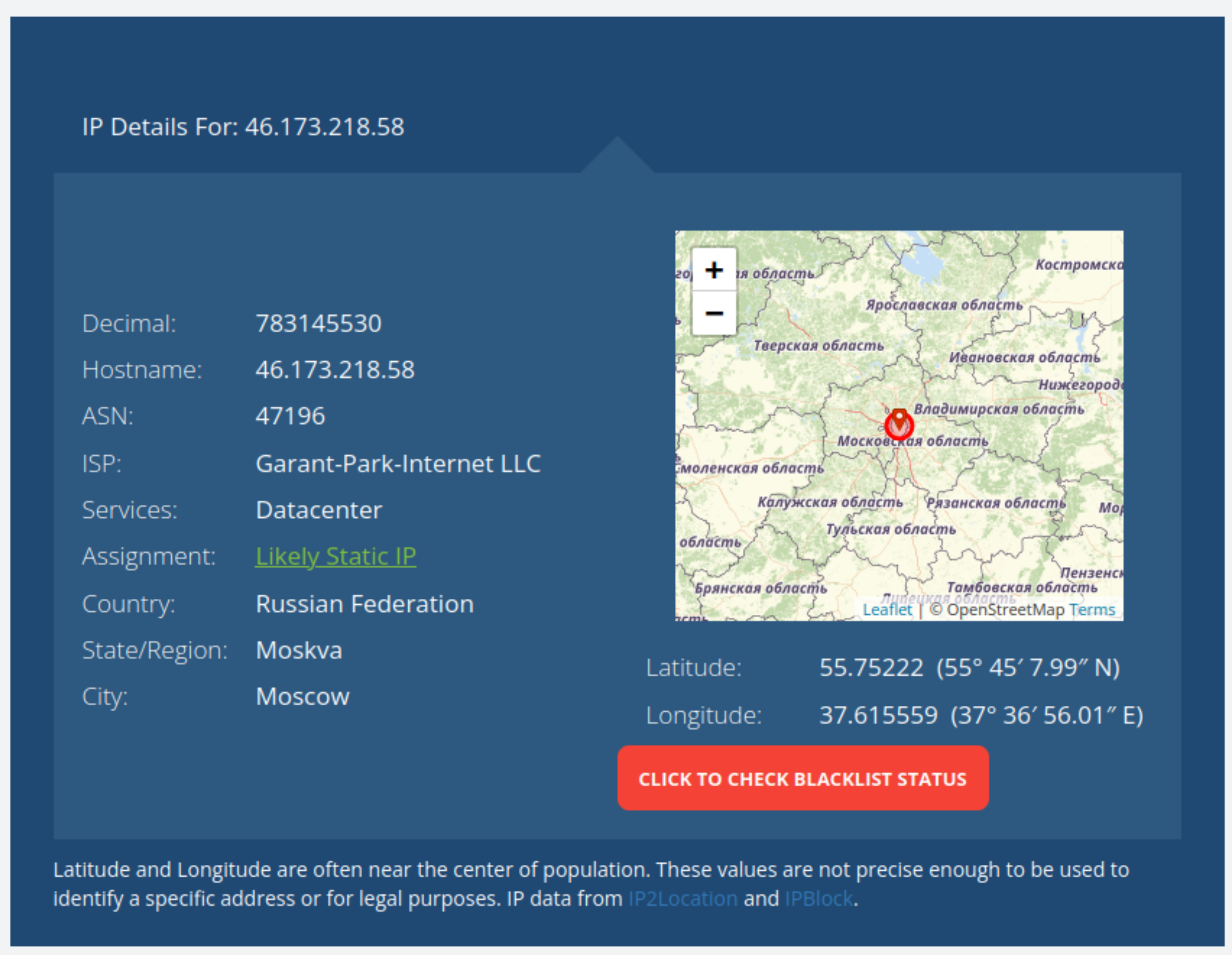
We analyzed 213 financial services companies to determine what percentage had logs with their domains included in a stealer log and how the price for those logs was different from consumer application logs.

In addition, the ability to mimic a browser fingerprint also opens the door for threat actors to potentially utilize the data in session replay attacks, bypassing 2FA and MFA controls through impersonation. This is directly due to users clicking the "remember this browser" checkbox which saves an active session token in the browser.

A Quick Sidebar on Genesis Market

For this analysis, we focused on results from Genesis Market, a dark web illicit market that specializes in selling logs from infected devices. Genesis is unique in that its pricing model varies based on the resources available in the stealer log, creating an opportunity to determine how much threat actors value certain resources (credentials) in a log.

The market is set up for usability and includes a simple solution that allows even unsophisticated threat actors to download and mimic the browser fingerprint of a victim. Genesis includes the ability to sort devices by country, contact alleged 24/7 customer support, and provides extensive support documentation. Genesis is a prime example of the increasing commodification of cybercrime, in which highly specialized threat actors each carry out individual, niche roles. Genesis proved particularly relevant since logs are sold individually, and the price varies based on the resources that the log has access to.


IP Details For: 46.173.218.58

Decimal: 783145530
Hostname: 46.173.218.58
ASN: 47196
ISP: Garant-Park-Internet LLC
Services: Datacenter
Assignment: Likely Static IP
Country: Russian Federation
State/Region: Moskva
City: Moscow

Latitude: 55.75222 (55° 45′ 7.99″ N)
Longitude: 37.615559 (37° 36′ 56.01″ E)

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address or for legal purposes. IP data from IP2Location and IPBlock.

The IP details for Genesis Market show and address in Russia

Infected Devices and Financial Services Credentials

We used two data sets for this analysis. We used the first data set to ascertain the price of logs on Genesis Market and analyzed 213 banks. The second data set focused on the top 50 U.S. financial services institutions and analyzed how many logs contained credentials to consumer bank accounts in our data set of 19.6 million stealer logs.

We wanted to determine how the presence of a financial services credential changes the value of a stealer log. To perform this analysis, we selected 213 random mid to large enterprise banks (greater than 5,000 employees) in the United States and identified stealer logs that have been for sale in the past two years to identify instances where an infected device had access to banking credentials.

It is worth noting that the relevant infected devices had both personal and corporate banking credentials, which caused some deviation in our analysis. We also wanted to see what the price differential was for infected devices with corporate credentials compared to those without.

Key Findings

- The average infected device for sale on Genesis Market that included a financial services login was listed for **$112.27**, compared with **$14.31** for those without
- Out of our sample of **213** financial institutions, we found that **46** had either employee or customer credentials for sale in the past **two** years.
- The median number of resources (unique application credentials) per device without financial logins was **35**; with financial credentials it was **335**.
- Several infected devices had been sold with likely corporate subdomains, indicating that threat actors may have been able to leverage them to launch attacks against the specific banks, representing 1.4% of our sample. Subdomains that we believe indicated likely corporate access included:
    - am1.virtualworkspace
    - sf.virtualworkspace
    - live.cloud.app
- The top 50 U.S. banks have 201,350 stealer logs associated with consumer banking logins, putting these accounts at risk for account takeover attacks. Given our limited sample size and the number of banks and credit unions in the U.S., this likely results in a vast understatement of the number of logs containing financial account access.

Tier 3 Logs: Consumer Applications & Stealer Logs

Finally, we analyzed the 50 most commonly appearing domains in our stealer log sample. A few things stand out specifically. First, Google, Gmail, Facebook, and Microsoft rank at the very top of the list and commonly have associated stealer logs. More broadly, almost all of these credentials are for typical consumer applications.

Top 50 domains appearing in the stealer log sample and percentage of logs that they appeared in:

Google

- gmail.com: 46.59%
- accounts.google.com: 42.05%
- google.com: 43.01%

Facebook

- facebook.com: 35.63%
- www.facebook.com: 21.79%
- m.facebook.com: 16.92%

Microsoft

- live.com: 34.14%
- login.live.com: 30.31%
- signup.live.com: 10.98%
- account.live.com: 9.45%
- hotmail.com: 13.77%
- outlook.com: 6.19%
- microsoftonline.com: 10.36%
- login.microsoftonline.com: 10.20%

Amazon

- amazon.com: 13.74%
- www.amazon.com: 9.64%

Netflix

- netflix.com: 17.13%

- www.netflix.com: 12.00%
- com.netflix.android: 7.42%

Roblox

- roblox.com: 15.17%
- www.roblox.com: 11.46%

Instagram

- instagram.com: 17.94%
- www.instagram.com: 12.41%
- instagram.android: 7.62%
- com.instagram.android: 7.62%

Steam

- steamPowered.com: 13.00%
- store.steampowered.com: 9.70%
- help.steampowered.com: 7.45%

Twitch

- twitch.tv: 12.47%
- www.twitch.tv: 9.01%

Paypal

- paypal.com: 12.10%
- www.paypal.com: 9.18%

Epic Games

- epicgames.com: 10.32%
- www.epicgames.com: 7.01%

Spotify

- spotify.com: 9.11%
- accounts.spotify.com: 6.73%

LinkedIn

- linkedin.com: 8.97%

Apple

- apple.com: 8.71%
- idmsa.apple.com: 6.68%

Zoom

- zoom.us: 7.09%

Blizzard Entertainment

- battle.net: 6.03%

The results were a mix of streaming applications, music, video games, and email accounts. There are likely some corporate accounts in here as well (for example accounts.google.com could be used for both corporate and personal applications). In the end the vast majority of logs published only contain access to common consumer applications, with only a small number used to drain bank accounts, and an even smaller number that are used for gaining access to corporations.

Sidebar: Steam, Infostealers, and CSGO Skins

Many infostealer variants have specific modules which are designed to extract steam credentials stored outside of the browser. The reason? Many players of the popular game Counter Strike Global Offensive have hundreds or thousands of dollars worth of "weapons skins" on their accounts which can be sold or traded for a profit, creating another lucrative source of revenue for log harvesters and buyers. This can be easily defeated by ensuring that steam authenticator is enabled for every transaction.

Research Limitations

There are several limitations to this analysis that are worth pointing out.

- We did not look for crossover between multiple corporate access domains present in the same log extensively. For example we didn't check logs that had access to AWS Console to see if they also had access to a credential for Okta. We did some basic testing and found the crossover to be low enough that we don't believe it impacts the results substantially.
- We only looked at seven specific corporate credentials that might be saved in a browser out of thousands, this limited our data considerably.
- Some credentials, such as those for AWS console may be used by students or for personal projects. We believe the vast majority likely indicate corporate access, but some may not.

About Flare

Flare is the proactive external cyber threat detection solution for organizations. Our AI-driven technology constantly scans the online world, including the dark and clear web, to discover unknown events, automatically prioritize risks and deliver actionable intelligence you can use instantly to improve security.

Want to learn about how Flare can support your external risk monitoring?

flare.io • hello@flare.io

Free Trial

Book a Demo

flare