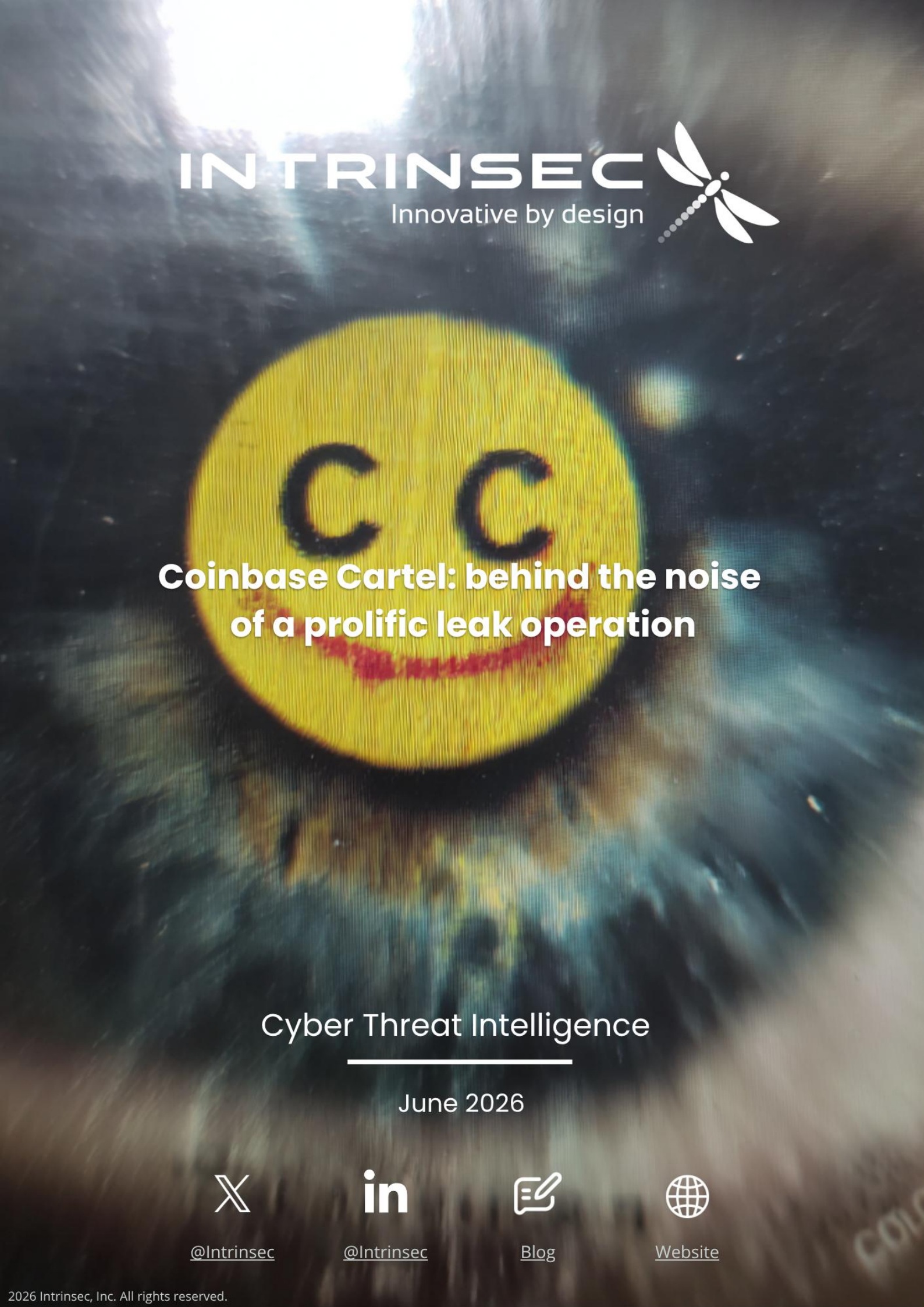
INTRINSEC
Innovative by design



Coinbase Cartel: behind the noise of a prolific leak operation

Cyber Threat Intelligence

June 2026

@Intrinsec @Intrinsec Blog Website

Table of contents

1. Key findings

Detailed in this report:

- The timeline of geographic and sectorial targeting of **victims claimed by Coinbase Cartel** indicate that the operation may **leverage supply-chain attacks**. This was also claimed by one of the online aliases promoting the operation's activities on the forum Exploit.
- The threat actor "**g77**" was the main user **promoting Coinbase Cartel inside cybercrime forums**. He is known to collaborate with other threat actors for various purposes (buying valid accesses, testing malware and tools, sending phishing, …).
- Coinbase Cartel may not directly perform technical intrusions. Potential partnerships highlighted inside cybercrime forums indicate that the operation tried to **monetize data stolen by other threat actors and to buy valid accesses in bulk**.
- We assess with high confidence that Coinbase Cartel is a **rebrand of a short-lived operation named DataVault**. This operation claimed a modus operandi of only stealing data using valid accesses acquired through strategic partnerships, which is like what we observed with Coinbase Cartel.
- Few discriminant IOCs related to the operation were identified. Based on various public and closed sources, this is consistent with the fact that the operation **does not perform encryption and only steals data in a simple extortion scheme**.

2. Introduction

Coinbase Cartel is an extortion intrusion set first observed in September 2025. The intrusion set has been gaining momentum in recent months, with several high-profile victims claiming to have been targeted in the last few months.

The group operates a dark web leak site and uses staged disclosures to pressure victims, releasing limited samples before escalating to full publication. Several high-profile victims in multiple sectors and countries were targeted since their inception. Among their ~140 victims since September 2025, several leaks have indeed been published following an announcement from the group, which seems to indicate that the group is relatively "reliable".

The group does not encrypt the victims' information systems, which is part of a broader trend in the ecosystem, with several other actors and operators following the same modus operandi. Rather, it focuses on data theft, threatening to publish or sell stolen information unless a ransom is paid. One consequence of this approach is the limited number of IOCs available regarding them.

An article by infostealers.com from 27 April 2026[1] reveals that many victims of Coinbase Cartel had prior credentials leaked by infostealers. However, in our analysis, we explored and exposed evidence suggesting that Coinbase Cartel may buy valid accesses from IABs (*Initial Access Brokers*) instead of directly using logs from infostealers. Therefore, it may be possible that it is these IABs that steal credentials using infostealers and resell/share profits with Coinbase Cartel.

[1] *https://www.infostealers.com/article/inside-the-coinbase-cartel-how-infostealer-credentials-fueled-a-100-company-ransomware-spree/*

3. Overview of the intrusion set's targeting

Since its first public revendications on its dataleak site, Coinbase Cartel managed to claim close to **143 victims** (as of 22nd June 2026). Below is a geographic and sectorial overview of the different claimed victims, which sheds light into the focus of the threat actor.

3.1. Geographic targeting

Below is the geographic distribution of organisations claimed by Coinbase Cartel. We notice a clear focus on Western organisations, with the United States and France taking the lead. The United Arab Emirates follows in third (11 claims), mainly due to a potential supply chain attack affecting real estate organisations during a short timeframe.

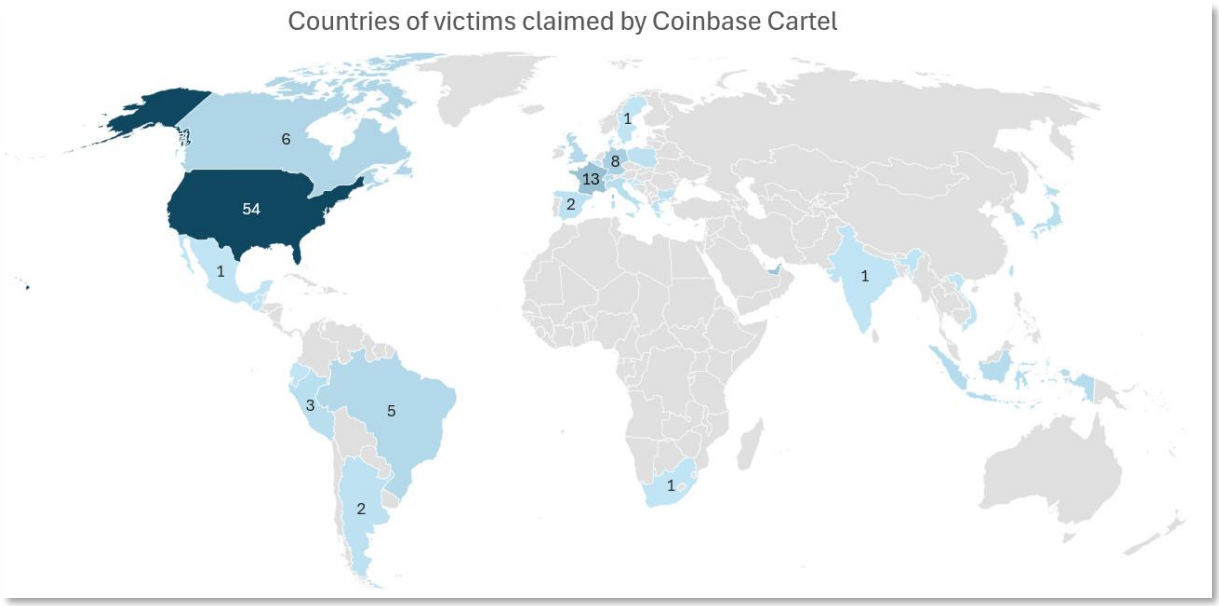


Figure 1: Countries of victims claimed by Coinbase Cartel.

For a clearer representation of smaller countries, find also below a bar chart view of the data shown on the map.

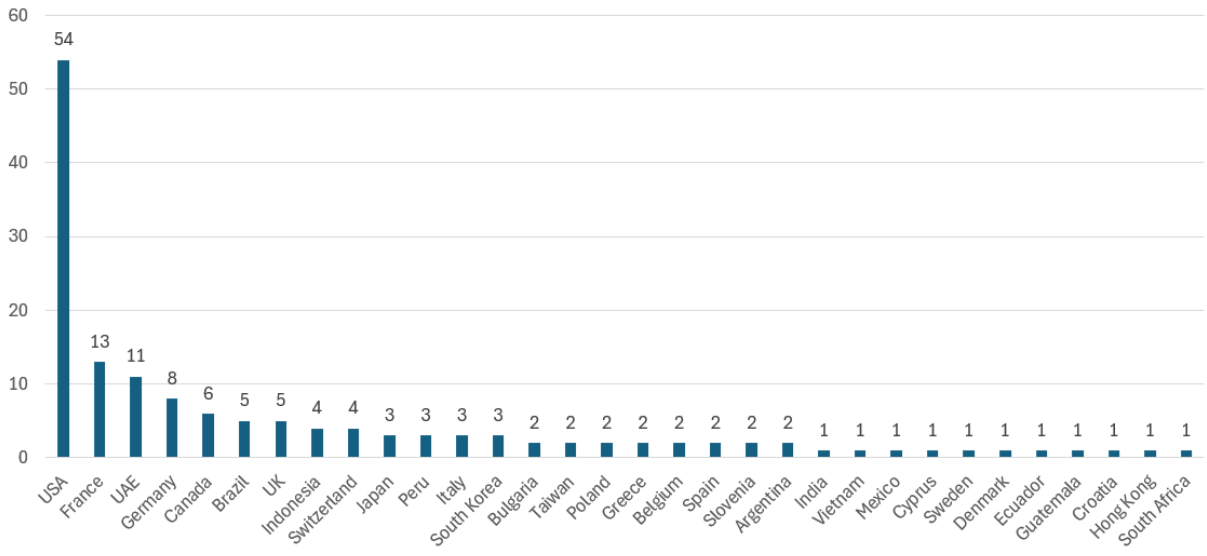


Figure 2: Bar chart view of countries of victims claimed by Coinbase Cartel.

3.2. Sectorial targeting

Find below the distribution of claimed victims' sectors. Sectors relevant to the global economy and to critical activities are most targeted. Also sectors that can handle a lot of sensitive data (health, retail) are targeted as they may be more inclined to abide to ransom demands. The real estate sector is an outlier, potentially based on a supply-chain attack affecting several UAE companies.

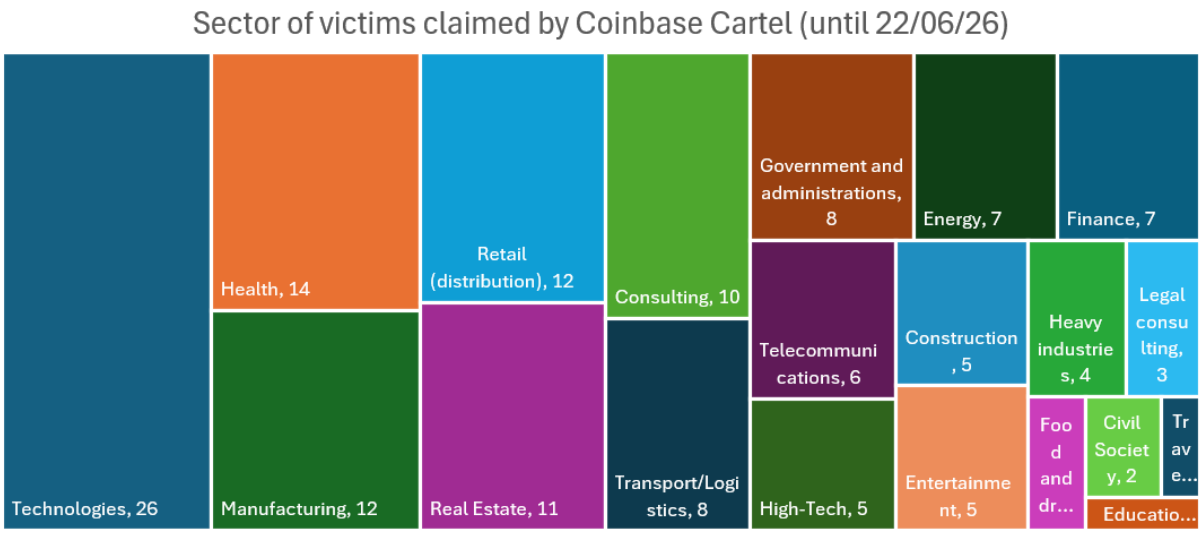


Figure 3: Sectors of victims claimed by Coinbase Cartel.

3.3 The supply-chain trail

Looking at the complete victimology and timeline of claims, we were able to **identify "waves" of sectors and countries targeted**. The first wave identified was on 13/10/2025, when 3 victims under the "transport/logistics" sector were published at the same time by

Coinbase Cartel. Then, on 09/12/2025, 10 victims in the "Real Estate" sector all located in the United Arab Emirates were published on Coinbase Cartel's website. On 11/03/2026, 3 "retail" victims were published; on 15/03/2026, 5 "genetics/health" victims were published; on 12/04/2026, another batch of 3 "retail" victims were published; on 23/04/2026, 3 victims in Peru were published; and finally, the latest wave is in the software/technology sector in May/June 2026 with 7 victims.

Figure 4: Timeline of potential supply-chains identified.

These findings suggest that **Coinbase Cartel may leverage supply chain compromises** to maximize the number of victims in a short timeframe. As we expose in the sections below (see Collaborations and demands), one threat actor known to be part of Coinbase Cartel showed signs of collaboration with Initial Access Brokers (IAB). This can alternatively suggest that it is these **IABs that perform the supply chain compromises** and **resell access in batch to Coinbase Cartel**. This analysis is coherent with observations made by Cybernews[2], were they note that this "*points toward a supply chain attack, where a third-party service provider, likely one specializing in data management or retail logistics, was the true entry point*".

We also identified a publication on the cybercrime forum Exploit by the user "Coinbase_Cartel" on 11 April 2026, which mentions that they have "**supply chain**" data for "*Lacoste, Ralph Lauren, Canada Goose, Carters, New Era, Spanx and more*", all in the retail industry.

[2] *https://cybernews.com/security/lacoste-ralph-lauren-supply-chain-data-breach/*

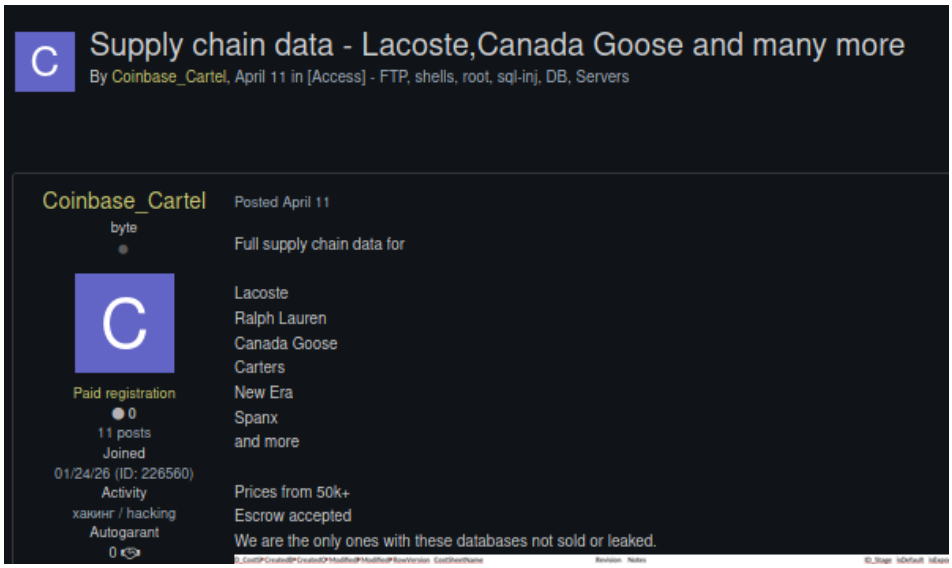


Figure 5: Supply-chain claimed by user "Coinbase_Cartel". Source: hxxps://forum.exploit.in/topic/280431

4. Profile and history of known members of Coinbase Cartel

We identified an online profile of a threat actor directly related to Coinbase Cartel. This user has a consistent history inside cybercrime forums since 2023. He also publicly tried to collaborate with other threat actors. These are useful information in assessing the capabilities of Coinbase Cartel, which we will detail below.

4.1 The "g77" profile

This profile was active on the cybercrime forum RAMP (ramp4u[.io) between September 2023 and November 2025.

On 4 November 2025, it **promoted an affiliate program for Coinbase Cartel**, directly linking this persona to the operation.

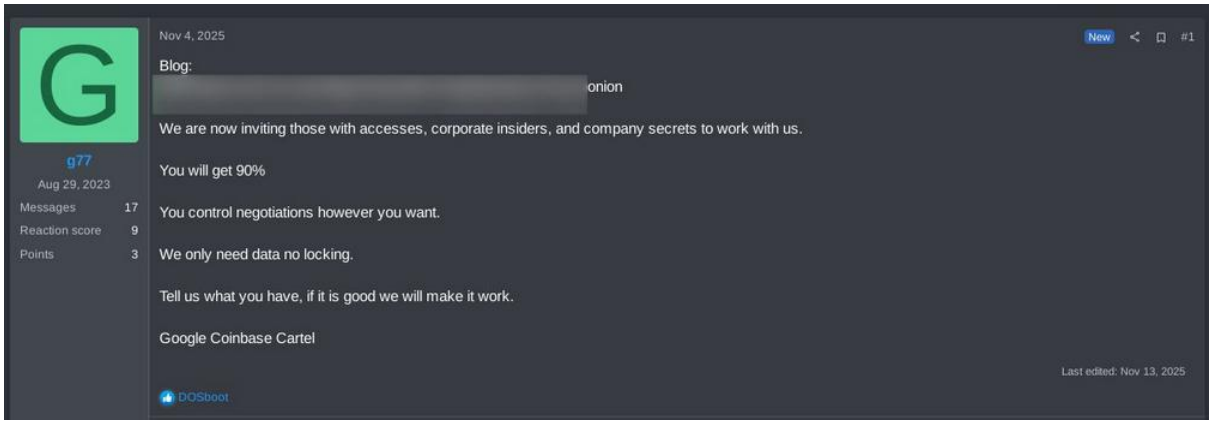


Figure 6: Promotion of Coinbase Cartel by the user "g77". Source: https://x.com/KrakenLabs_Team/status/1995509862172643366/photo/1

As such, we searched the history of this profile on Ramp to gain insight into his practices and interests. As the forum RAMP is now offline, we cannot provide direct screenshots of our findings, but we were still able to collect messages published by using partners tools.

- On 7 November 2023, g77 created a publication titled "**Looking for corp email access – I give %**", where he is looking to "*turn email accesses into $ corp only amounts are high pm me your contacts and i will add you*". On 9 January 2024, the user "Coinbase120" responded to this publication by saying "pm". There is a probability that the user Coinbase120 may have collaborated with "g77", and the name could suggest that it had an influence on the later name "Coinbase Cartel", but we cannot confirm this hypothesis.[3]

[3] *hxxps://ramp4u.io/threads/looking-for-corp-email-access-i-give.1447/ (now offline)*

- On 17 January 2024, g77 created a publication titled "**Partnership with Business Email compromise - Professional work – Proof**", where he says he "*need people who have first hand corporate email access, from networks/spam etc does not matter. Countries: ca/usa/some eu/gb - and we can look at anything else you have as long as it meets our criteria.*". No serious answers to this publication were identified as a sign of collaboration[4].

- On 18 March 2024, g77 created a publication titled "**Looking for email spammer**" where he says he is "*Looking for someone who can spam emails i will explain my offer when we talk Text only or text and pdf/image I work on % or $ send contact information if interested*". No serious answers to this publication were identified as a sign of collaboration[5].

- On 8 July 2025, g77 commented "***best panel ive seen till date. looks amazing***" on a publication by the user "clockwork_orange" titled "**UBC — Access Provisioning Infrastructure: Customization, APIs, Unlimited Scalability**". The tool is described as a "distributed system for brute-force attacks and checks", which matches the definition of a botnet.

  On 12 July 2025, g77 commented "***send contact pls***" on a publication by the user "anongod" related to malware. To which "anongod" replied "*check your dm*".[6]

- On 14 July 2025, g77 commented "***can u send me too + ur contact***" on another publication by the user "anongod" related to an offensive coding tool.[7]

Overall, these elements reveal that g77, a threat actor linked to Coinbase Cartel, showed significant interest in collaborating with other threat actors in aspects related to: **buying accesses, sending phishing emails, using already existing malware and tools**. This may indicate that similar cooperation could have taken place for the Coinbase Cartel operation.

[4] *hxxps://ramp4u.io/threads/partnership-with-business-email-compromise-professional-work-proof.1686/ (now offline)*
[5] *hxxps://ramp4u.io/threads/looking-for-email-spammer.1919/ (now offline)*
[6] *hxxps://ramp4u.io/threads/3266/ (now offline)*
[7] *hxxps://ramp4u.io/threads/3268/ (now offline)*

4.2 Online aliases and timeline

We identified the use of various aliases on cybercrime forums for the promotion of Coinbase Cartel's activities. There is a **high probability** that these aliases are operated by the same individual who operates the "g77" persona.

Combining these aliases with the "g77" persona, we get the following timeline, from September 2023 to April 2026.

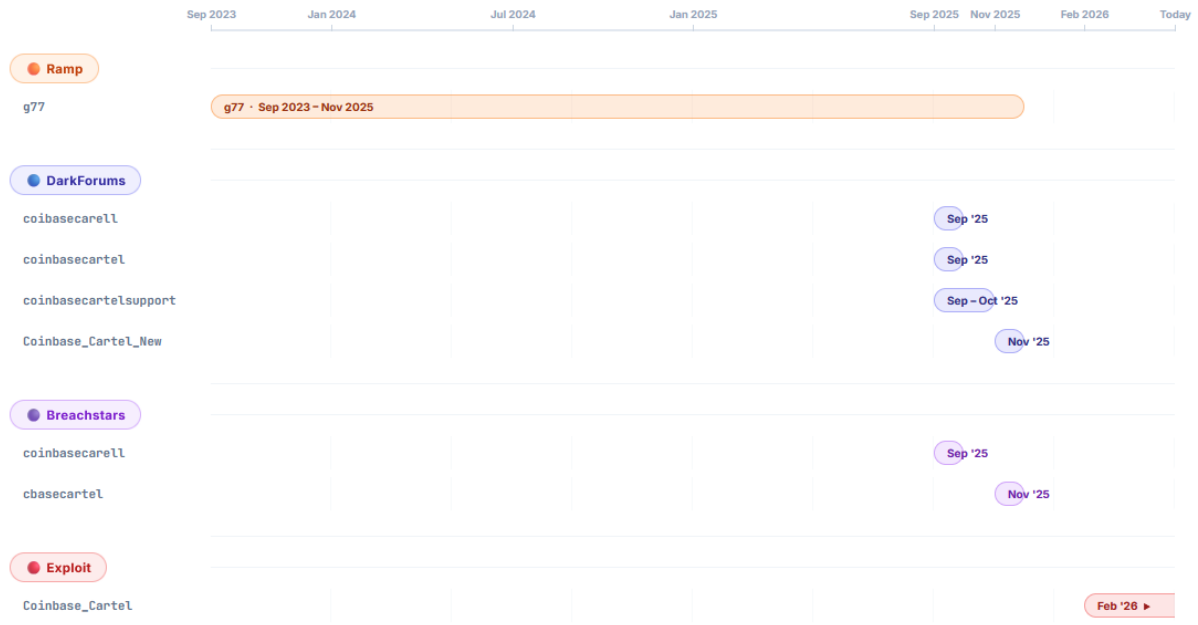


Figure 7: Timeline of aliases of "g77" and "Coinbase Cartel".

4.3 Collaborations and demands

The profile "Coinbase_Cartel" on Exploit is active since February 2026 and has published messages asking for collaboration. This is consistent behaviour observed regarding the "g77" profile, going so far as to make similar demands.

On 5 March 2026, the threat actor asked for "*teams with experience to work on a large amount of ssh and vpn accesses*", suggesting that they have a lot of accesses to sort and triage.

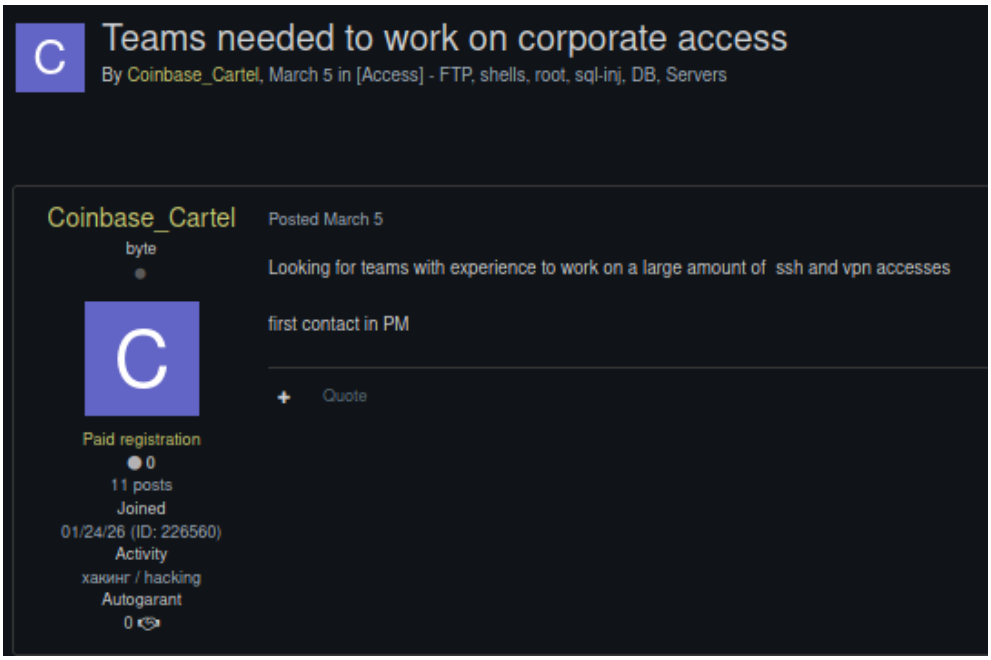


Figure 8: Cooperation announcement. Source: hxxps://forum.exploit.in/topic/277607/

On 12 February 2026, the threat actor looked to "*buy or monetize data*" already in possession of other threat actors. This suggests that Coinbase Cartel may try to **strike deals with threat actors who already stole data**, to **pressure victims into paying a ransom** (i.e. *monetize*) by claiming them on their dataleak site.

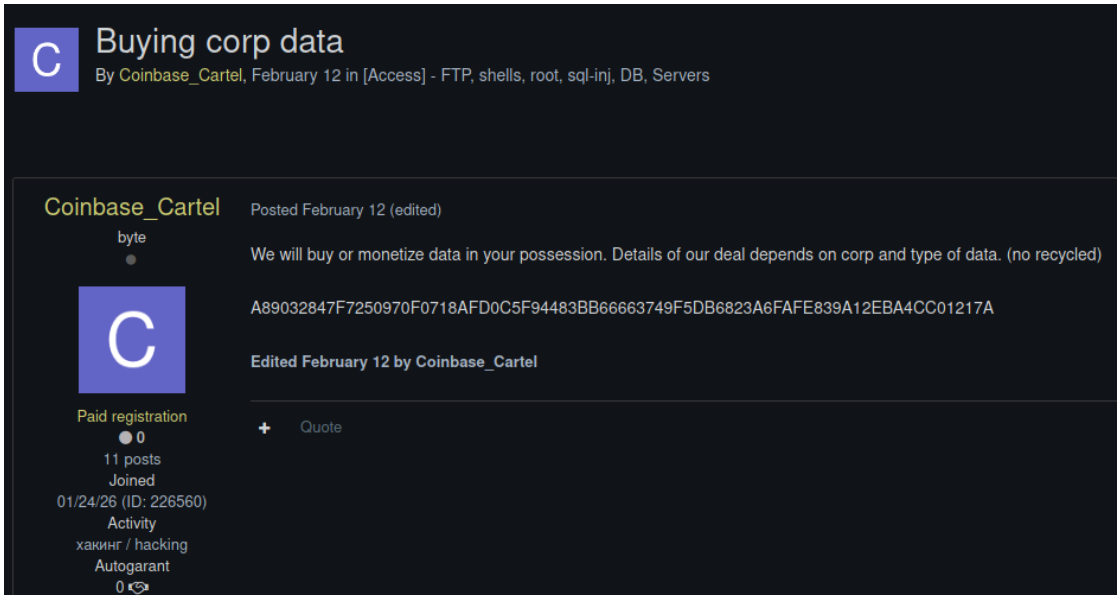


Figure 9: Cooperation announcement. Source: hxxps://forum.exploit.in/topic/275885/

A similar demand was reiterated on 21 March 2026.

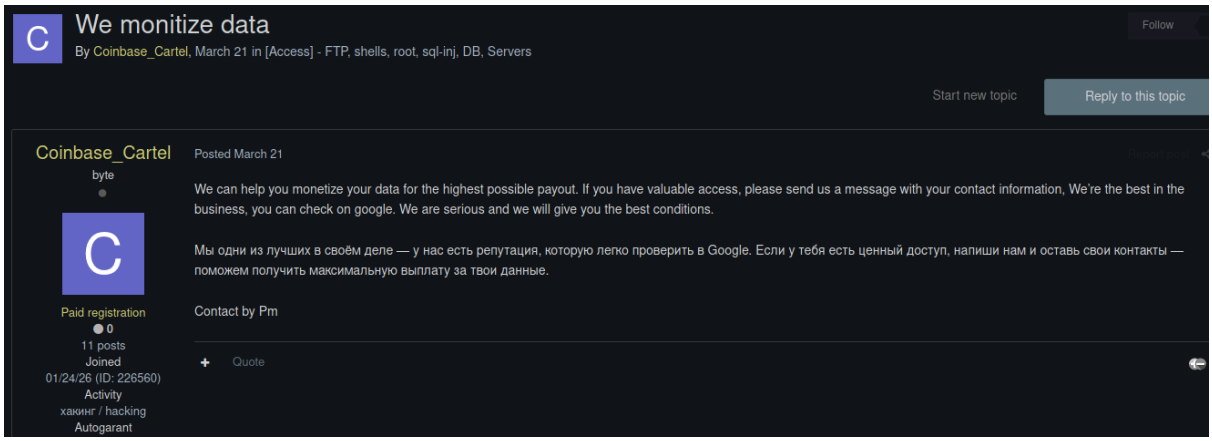


Figure 10: Cooperation announcement. Source! hxxps://forum.exploit.in/topic/278864/

On 11 April 2026, "Coinbase_Cartel" commented "**pm sent**" on a now deleted publication by the user "confirm", titled "*I need a partner for a network; I have a steady stream of US companies ranging from $50 million to $900 million, and the networks come with online CRM access*"[8]. The publication was deleted by the administrators of Exploit after "confirm" said "*Good evening, please delete this thread; the person has been found.*" just after Coinbase_Cartel's answer. This highly suggests a **direct collaboration** between the "confirm" IAB and Coinbase Cartel.

[8] *hxxps://forum.exploit.in/topic/280190/ (now deleted)*

5. A rebranding of "DataVault"

We identified that the company SK Telecom was apparently first claimed by a **short-lived leak operation named "DataVault"**. In fact, SK Telecom disclosed a databreach on April 2025[9], and on 8 May 2025, "g77" shared the onion site for DataVault, which is now offline, claiming that they "*did SK Telecom*". The bluesky account "ecrime" also noted the compromise as claimed by DataVault[10].

Figure 11: DataVault claiming SK Telecom.

To our knowledge, "g77" is the first and only threat actor that shared this onion website, and in an even broader scope, apart from ecrime, no other leak monitoring sites collected the onion before it was offline. This suggests that **g77 may be linked to the DataVault** operation.

SK Telecom was posted on Coinbase Cartel's website on 16 September 2025 and on 17 September, "coinbasecarell" on BreachStars shared a screenshot and a message claiming that "***we are DataVault***", after the user "ElChapo" claimed that Coinbase Cartel stole and repurposed SK Telecom data from DataVault[11].

[9] *https://www.msit.go.kr/eng/bbs/view.do?bbsSeqNo=42&nttSeqNo=1139*
[10] *https://bsky.app/profile/ecrime.ch/post/3lonfd3esct2l*
[11] *hxxps://breachsta.rs/topic/sk-telecom-source-code-and-data-for-sale-500k-usd-f6z1h9wbf3m2?page=2 (now offline)*

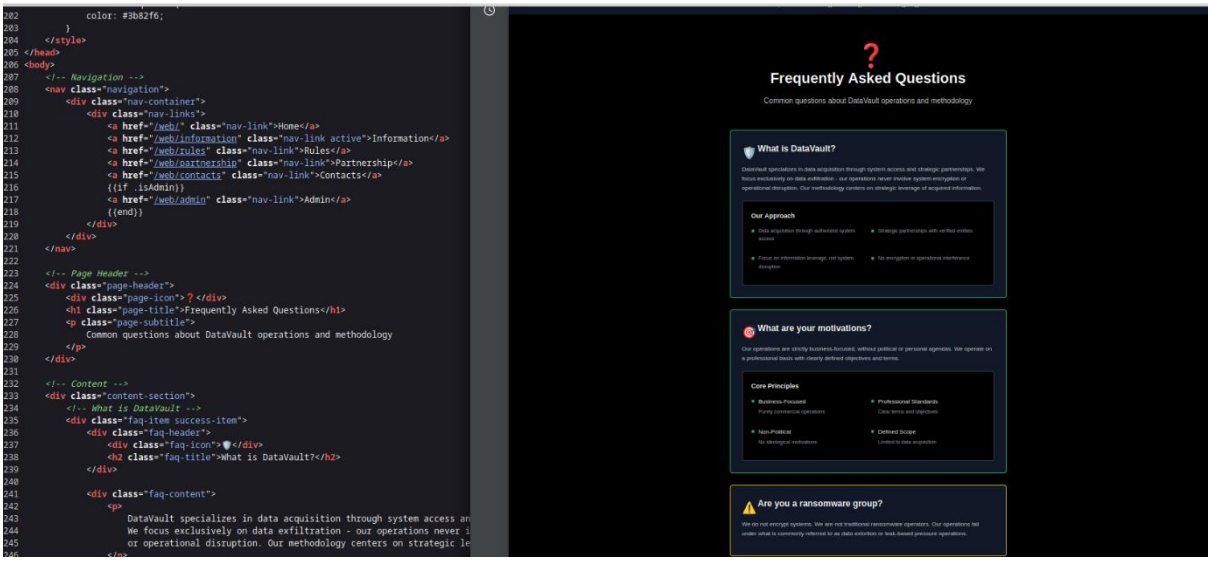


Figure 12: Landing page of DataVault's leak site. Source: hxxps://8upload.com/image/68cad76d0d2fc/DFATA.png

Interestingly, the information found on the right panel of the screenshot reveals information about **DataVault modus operandi**, which is consistent with Coinbase Cartel's modus operandi we exposed in this report.

The first section indicates that "*DataVault specializes in data acquisition through system access and strategic partnerships. We focus exclusively on data exfiltration – our operations never involve system encryption or operational disruption. Our methodology centers on strategic leverage of acquired information*".

We can translate these claims in more technical terms:

DataVault specializes in data acquisition through system access and strategic partnerships -> **Collaboration with initial access brokers to exploit valid accesses.**

We focus exclusively on data exfiltration – our operations never involve system encryption or operational disruption -> **Exfiltration after initial access, without encryption.**

Our methodology centers on strategic leverage of acquired information -> **Monetizing stolen data with simple extortion**.

In short, we suspect that the same modus operandi of DataVault is being repurposed by Coinbase Cartel, as the same threat actor(s) are behind these operations. We do not know why DataVault was taken down and needed to be rebranded into Coinbase Cartel.

6. Insights into a tool potentially used by Coinbase Cartel

We were able to come across the IP address 176.120.22[.240 (hosted by Proton66 OOO, a known bulletproof hosting provider we previously reported on[12]), which was linked to Coinbase Cartel incidents.

6.1 Ultimate RDP bruteforcer

By using internet intelligence platforms like ThreatBook, we noticed that port 9090 of this IP address exposed a web page titled "**Ultimate RDP bruteforcer**".

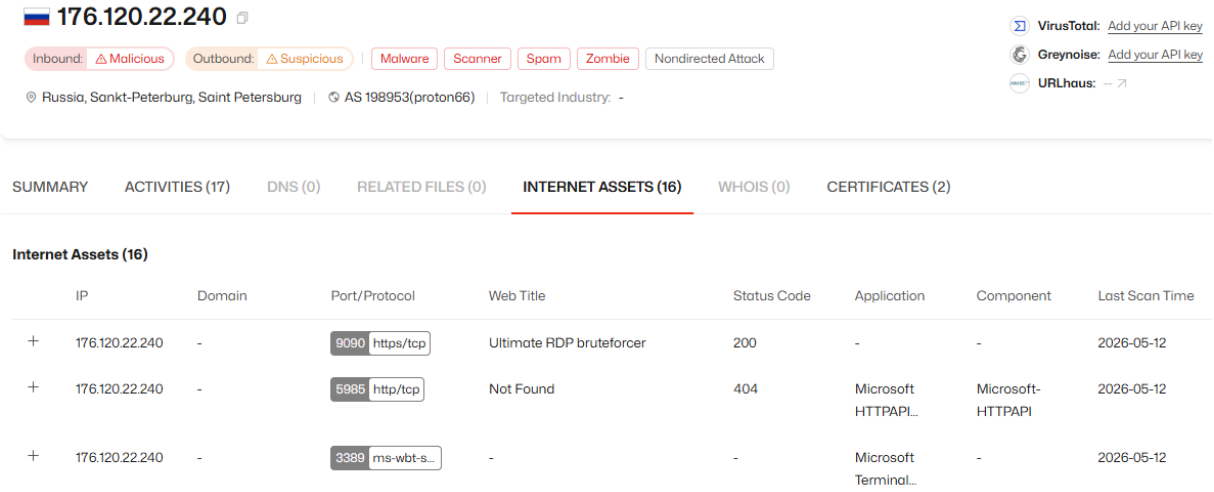


Figure 13: Ultimate RDP bruteforcer on port 9090. Source: https://i.threatbook.io/research/176.120.22.240

This is interesting because the IP address is also tagged on VirusTotal as having tone RDP connections to multiple targets 3 months ago by Pure7.

Figure 14: Flagged as attempting RDP connections. Source: https://www.virustotal.com/gui/ip-address/176.120.22.240/community

[12] *https://www.intrinsec.com/prospero-proton66-tracing-uncovering-the-links-between-bulletproof-networks/*

The name of the tool is very suggestive, and we identified more than 30 IP addresses exposing this tool on port 8050 and/or 9090 by using Shodan, Censys and Fofa searches. Find them in the Indicators of compromise section of this report.

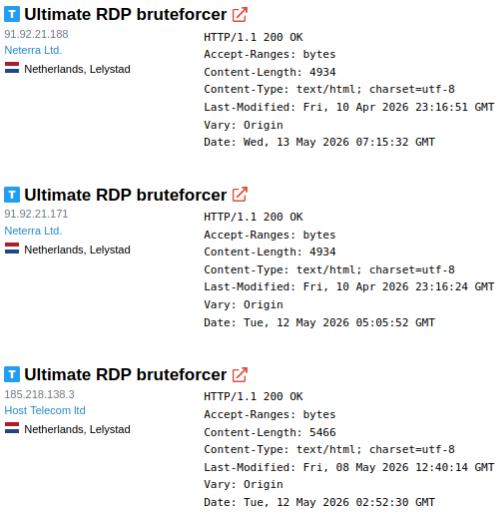


Figure 15: Ultimate RDP bruteforce on multiple IP addresses. Source: https://www.shodan.io/search?query=http.title%3A%22Ultimate+RDP+bruteforcer%22

By querying 176.120.22[.240:9090, we landed on the login page of the Ultimate RDP bruteforcer tool. However, we noticed that before landing on the login page, the panel without authentication was successfully loaded and presented on the screen. As the login page is located at "auth.html", we can access the content of the panel by **blocking requests containing "auth"** using web developer tools.

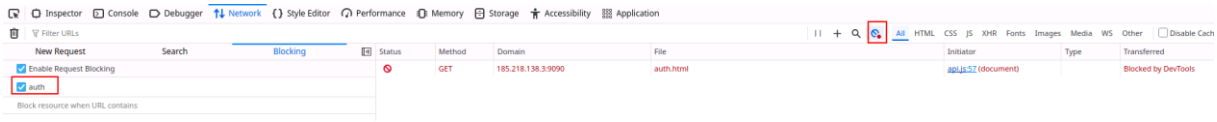


Figure 16: Blocking requests containing "auth".

The panel was therefore accessible and revealed capabilities of the tool. Below is a screenshot of the main page which showed results of a task previously launched by a threat actor. The attacker attempted bruteforce on 227 379 "targets", with 2 425 083 222 attempts in 43 hours and 6 minutes. The task was still active with an estimated remaining time of 32 hours and 12 minutes, which gives an estimated total time of 75 hours and 18 minutes (more than 3 days). Of all the attempts, the threat actor got, at the time, 8 valid credentials. The list of valid credentials is not shown probably because we were not logged in. This shows the use of this tool as a mass rdp-bruteforcer as the percentage of valid credentials obtained is very low.

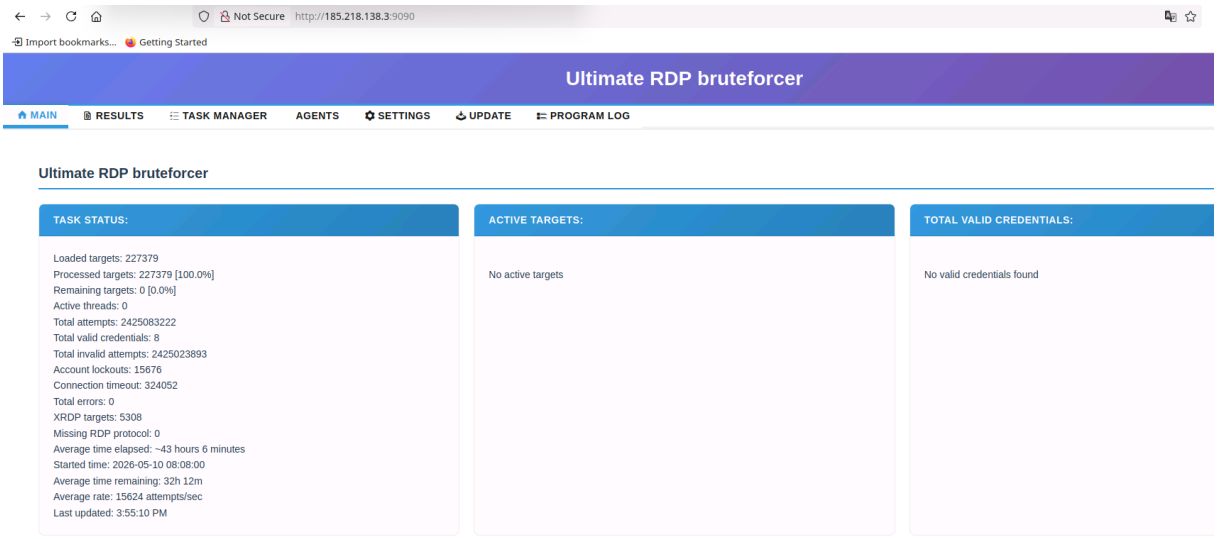


Figure 17: Main page of the Ultimate RDP bruteforcer panel.

6.2 Promotion of the tool on Exploit

We managed to locate a post promoting “Ultimate RDP bruteforcer” on the cybercrime forum Exploit. The user “darksoftware” first advertised the tool on 10 February 2026.

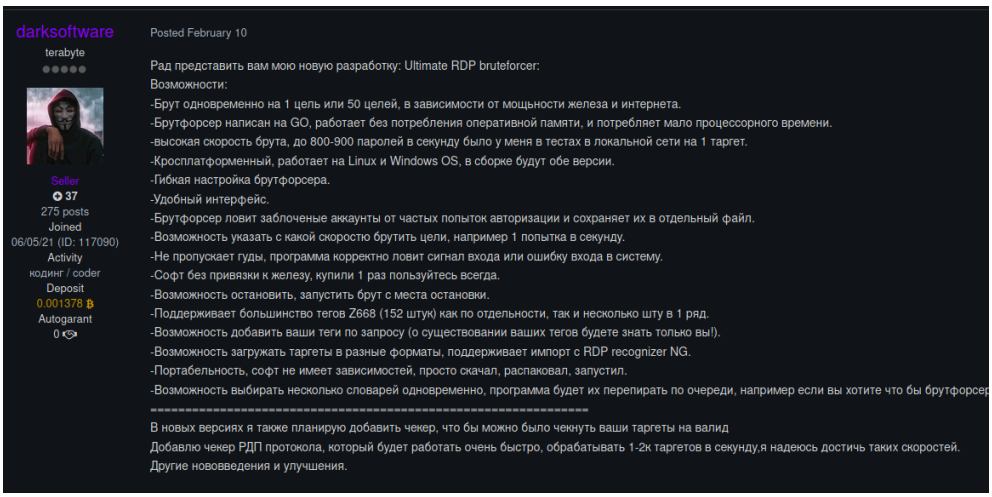


Figure 18: The user “darksoftware” promoting Ultimate RDP bruteforcer. Source: hxxps://forum.exploit.in/topic/203610/?page=4&tab=comments#comment-1650636

“darksoftware” provided screenshots showcasing the tool, which are similar to what we were able to observe inside the panel.

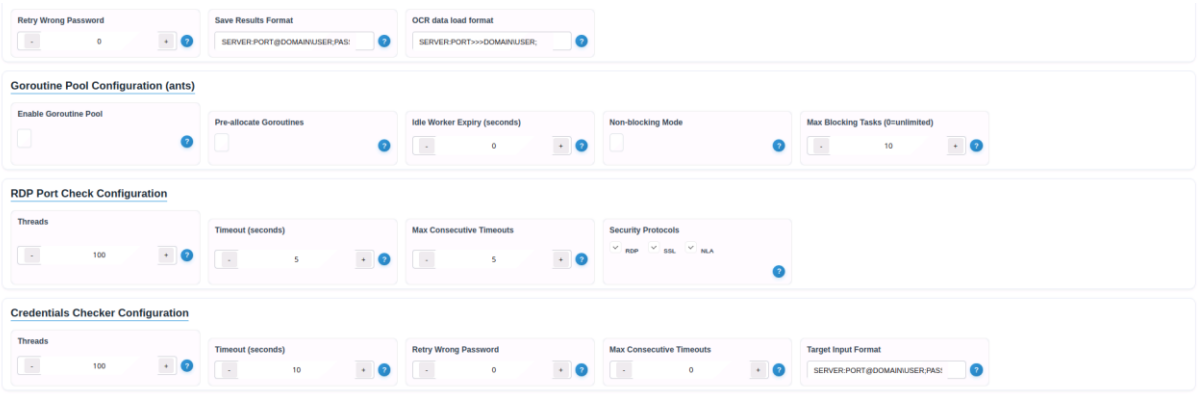


Figure 19: Example view of settings inside the panel.

Overall, the main characteristics of the tool as advertised and observed on the panel and screenshots are the following:

- Written in Go for efficiency on all hardware; supports 1–100 simultaneous targets with speeds up to 1,500 passwords/sec per target.

- Cross-platform (Windows/Linux), portable (no dependencies), and supports the latest RDP protocols.

- Built-in RDP/XRDP detector to filter out false positives and "swamped" accounts.

- Customizable brute-force speeds, multi-dictionary support, automatic domain extraction, flexible configuration.

- User-friendly web interface (EN/RU), detailed statistics, and an auto-resume launcher for crash recovery.

In the case of Coinbase Cartel, this tool may be used to obtain valid credentials on specific or indiscriminate targets. Initial access brokers for Coinbase Cartel could also leverage this tool to resell valid accesses. As we managed to identify this tool hosted on several IP addresses, with one being linked to Coinbase Cartel, we can assess that it is already being weaponised for various usage as a credential access tool. However, we cannot firmly confirm that Coinbase Cartel used it in its operations.

7. Summary of known relationships

Find below a graph summary of the relationships exposed in this brief report. We only mapped the relationships we confirmed based on our findings. There is a high probability that g77 has relationships with other threat actors.

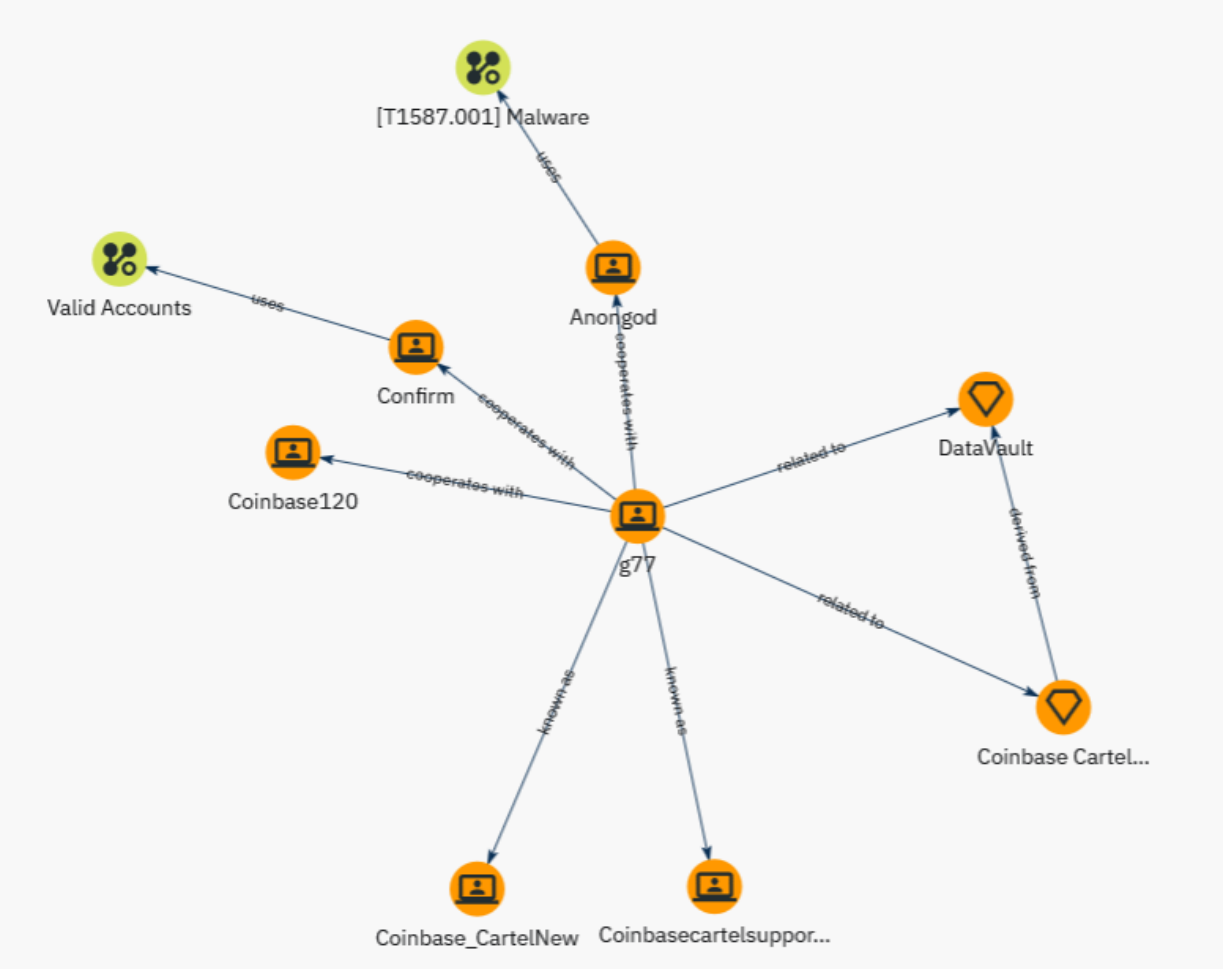


Figure 20: Summary of known relationships of Coinbase Cartel.

8. Conclusion

In this analysis, we examined the methodology, victimology and known history of Coinbase Cartel. This leak operation has targeted more than 140 victims since its inception in September 2025, with several high-profile targets in multiple countries and sectors.

The study of the victimology revealed potential supply-chain exploitation, as some victims in the same country and/or sector were claimed by the intrusion set in a small timeframe. This was further hypothesised as one of the accounts that promoted Coinbase Cartel operations on the cybercrime forum Exploit mentioned data obtained through “supply chain”.

We identified that the profile “g77” promoted the operation on the cybercrime forum Ramp before another account named “Coinbase Cartel” promoted it on Exploit. This persona was active between 2023 and 2025, showing interest in collaborating with other threat actors and wanting to use tools, malware, valid accesses.

We also identified that the short-lived “DataVault” leak operation was with a high confidence, created by the same operator(s) of Coinbase Cartel, just a few months before. This leak operation exposed its methodology on its .onion website, which is consistent with what was observed for Coinbase Cartel.

Finally, we identified the “Ultimate RDP bruteforcer” tool exposed on an IP address associated with a Coinbase Cartel attack. As its name suggest, this tool is used to bruteforce accesses and returns the list of valid credentials obtained on the chosen targets.

Overall, Coinbase Cartel was identified as a credible leak operation, mixing probable elements of cooperations with IABs. Since May, they slowed down on the number of claimed victims per month for reasons unknown, but we can suspect that as other threat actors saw the example of a successful leak operation, just like ShinyHunters, they may be willing to emulate this modus operandi in the future.

9. Actionable content

9.1 Indicators of compromise

Value	Type	Description
0576babd9d1287b0069eb3b3413701d39d6acecad88fad7948d16cea3ceafc8326	Messaging	CoinbaseCartel Session ID (Nov 2025)
1225DDE01980D7C7890A90E359EF4406D74DF7DB94F6C5F3B8378BB78444473022675C49FACB	Messaging	CoinbaseCartel TOX ID (Sep-Nov 2025)
58041B45371485934F798C77F2F9705DA735F28AC9EBA2A19B4C9DBAF462802B88E33CEF482A	Messaging	CoinbaseCartel (g77) TOX ID (Nov-Dec 2025)
A89032847F7250970F0718AFD0C5F94483BB66663749F5DB6823A6FAFE839A12EBA4CC01217A	Messaging	CoinbaseCartel TOX ID (Jan-Feb 2026)
05e82475d2756d45d18040fcf6f79babd4b6d9a9dcea4f025b320b2a7c6cbcef45	Messaging	CoinbaseCartel Session ID (Mar 2026)
A7580331D4D16453CCE86D7ADFBCF0CEED0D0D1AEA8F4DBEEBCA9E3B46308F260DE9B41BD838	Messaging	CoinbaseCartel TOX ID (Apr 2026)
fjg4zi4opkxkvdz7mvwp7h6goe4tcby3hhkrz43pht4j3vakhy75znyd[.]onion	Domain-Name	CoinbaseCartel onion dataleak site
won2bghjatxaavvf7eoepuwj74pej764mys575xan2h2uoctxnuojyyd[.]onion	Domain-Name	CoinbaseCartel download server
hvq4w4qdypuqohnet2xozipve4pkqwx7zekkkeqy5t7fkbswk34epoqd[.]onion	Domain-Name	DataVault onion dataleak site (offline)
176.120.22[.]240	IPv4	Linked to Coinbase Cartel incident, hosting Ultimate RDP Bruteforcer (AS Proton 66 OOO)
176.120.22[.]240:9090	IPv4	Ultimate RDP Bruteforcer
45.74.3[.143	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.142.195[.51	IPv4	Ultimate RDP Bruteforcer on port 9090 (not attributed to CoinbaseCartel)
45.142.195[.54	IPv4	Ultimate RDP Bruteforcer on port 8050 (not attributed to CoinbaseCartel)

45.154.244[.130	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.133	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.135	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.140	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.142	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.145	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.149	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.155	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.156	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.136	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.158	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.161	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.162	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.164	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.172	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)

45.154.244[.173	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
45.154.244[.175	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
91.92.21[.169	IPv4	Ultimate RDP Bruteforcer on port 8050 (not attributed to CoinbaseCartel)
80.66.66[.31	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
80.66.66[.68	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
86.54.25[.201	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
86.54.25[.205	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
86.54.25[.208	IPv4	Ultimate RDP Bruteforcer on port 8050 (not attributed to CoinbaseCartel)
86.54.25[.210	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
86.54.25[.212	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
87.251.64[.32	IPv4	Ultimate RDP Bruteforcer on port 9090 (not attributed to CoinbaseCartel)
87.251.64[.33	IPv4	Ultimate RDP Bruteforcer on port 9090 (not attributed to CoinbaseCartel)
87.251.64[.34	IPv4	Ultimate RDP Bruteforcer on port 9090 (not attributed to CoinbaseCartel)
87.251.64[.35	IPv4	Ultimate RDP Bruteforcer on port 9090 (not attributed to CoinbaseCartel)
87.251.64[.36	IPv4	Ultimate RDP Bruteforcer on port 9090 (not attributed to CoinbaseCartel)

87.251.64[.37	IPv4	Ultimate RDP Bruteforcer on port 9090 (not attributed to CoinbaseCartel)
88.210.63[.79	IPv4	Ultimate RDP Bruteforcer on port 8050 (not attributed to CoinbaseCartel)
91.92.21[.170	IPv4	Ultimate RDP Bruteforcer on port 8050 (not attributed to CoinbaseCartel)
91.92.21[.155	IPv4	Ultimate RDP Bruteforcer on port 8050 (not attributed to CoinbaseCartel)
91.92.21[.180	IPv4	Ultimate RDP Bruteforcer on port 8050 (not attributed to CoinbaseCartel)
91.92.21[.191	IPv4	Ultimate RDP Bruteforcer on port 8050 (not attributed to CoinbaseCartel)
91.92.21[.171	IPv4	Ultimate RDP Bruteforcer on port 8050 (not attributed to CoinbaseCartel)
91.92.21[.188	IPv4	Ultimate RDP Bruteforcer on port 8050 (not attributed to CoinbaseCartel)
91.227.114[.142	IPv4	Ultimate RDP Bruteforcer on port 9090 (not attributed to CoinbaseCartel)
91.227.114[.202	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
91.227.114[.205	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
91.227.114[.207	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
91.227.114[.210	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
91.227.114[.211	IPv4	Ultimate RDP Bruteforcer on port 8050 and 9090 (not attributed to CoinbaseCartel)
185.136.15[.55	IPv4	Ultimate RDP Bruteforcer on port 9090 (not attributed to CoinbaseCartel)

185.218.138[.3	IPv4	Ultimate RDP Bruteforcer on port 9090 (not attributed to CoinbaseCartel)

9.2 Tactics, Techniques and Procedures

ID	Tactic	Detail
T1650	Acquire Access	Coinbase Cartel probably bought valid accesses from IABs.
T1583.003	Acquire Infrastructure: Virtual Private Server	Coinbase Cartel used IP addresses of bulletproof and legitimate hosting providers to exfiltrate data.
T1588.001	Obtain Capabilities: Malware	Coinbase Cartel (as the g77 persona) showed willingness to use malware developed by other threat actors.
T1588.002	Obtain Capabilities: Tool	Coinbase Cartel (as the g77 persona) showed willingness to use tools developed by other threat actors.
T1078	Valid Accounts	Coinbase Cartel has probably used VPN/CRM accesses bought from Initial Access Brokers.
T1078.002	Valid Accounts: Domain Accounts	Coinbase Cartel has probably used valid credentials leaked by stealer malware.
T1110	Brute Force	An IP address associated with Coinbase Cartel hosted **"Ultimate RDP bruteforcer"**, a tool used to brute force credentials.
T1133	External Remote Services	Coinbase Cartel used valid VPN accesses.
T1090.002	Proxy: External Proxy	Coinbase Cartel used known residential proxies to access victim systems.
T1665	Hide Infrastructure	Coinbase Cartel used VPN and Proxy services to mask their real IP addresses.
T1041	Exfiltration Over C2 Channel	Coinbase Cartel exfiltrated data using C2 IP addresses.
T1657	Financial Theft	Coinbase Cartel monetizes stolen data by asking for a ransom.

9.3 Recommendations

- **Block IOCs:** Block the IOCs provided in the "Indicators of compromise" section of this analysis and subscribe to a CTI feed to obtain fresh IOCs related to cyber threats. Intrinsec offers its own CTI feed to enhance your detection and response capabilities: https://www.intrinsec.com/en/cyber-threat-intelligence-feeds/
- **Leverage Threat Intelligence:** Subscribe to a threat intelligence service to be alerted on relevant evolution surrounding this threat actor, and other leak/ransomware operations. Intrinsec offers access to its Threat Intelligence platform for exclusive insights: https://www.intrinsec.com/threat_intelligence_platform/
- **Monitor leaked corporate accesses**: Monitor leaked corporate accesses to revoke and reset compromised passwords, preventing unauthorized access to your assets. Intrinsec offers dataleak and credential monitoring services: https://www.intrinsec.com/data-leak-detection/
- **Pre-compromise:** Pre-compromise mitigations involve proactive measures and defenses implemented to prevent adversaries from successfully identifying and exploiting weaknesses during the Reconnaissance and Resource Development phases of an attack. These activities focus on reducing an organization's attack surface, identify adversarial preparation efforts, and increase the difficulty for attackers to conduct successful operations.
- **User Account Management:** User Account Management involves implementing and enforcing policies for the lifecycle of user accounts, including creation, modification, and deactivation. Proper account management reduces the attack surface by limiting unauthorized access, managing account privileges, and ensuring accounts are used according to organizational policies.
- **Multi-factor Authentication:** Implement multi-factor authentication (MFA) across all account types, including default, local, domain, and cloud accounts, to limit unauthorized access, even if credentials are compromised. MFA provides a critical layer of security by requiring multiple forms of verification beyond just a password.
- **Password Policies:** Set and enforce secure password policies for accounts to reduce the likelihood of unauthorized access. Strong password policies include enforcing password complexity and preventing password reuse.
- **User Training:** User Training involves educating employees and contractors on recognizing, reporting, and preventing cyber threats that rely on human interaction, such as phishing, social engineering, and other manipulative techniques. Comprehensive training programs create a human firewall by empowering users to be an active component of the organization's cybersecurity defenses.
- **Privileged Account Management:** Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. These audits should also include if default accounts have been enabled, or if new local accounts are created that have not been authorized.

- **Account Use Policies:** Account Use Policies help mitigate unauthorized access by configuring and enforcing rules that govern how and when accounts can be used. These policies include enforcing account lockout mechanisms, restricting login times, and setting inactivity timeouts.
- **Application Developer Guidance:** Application Developer Guidance focuses on providing developers with the knowledge, tools, and best practices needed to write secure code, reduce vulnerabilities, and implement secure design principles. By integrating security throughout the software development lifecycle (SDLC), this mitigation aims to prevent the introduction of exploitable weaknesses in applications, systems, and APIs.
- **Active Directory Configuration:** Implement robust Active Directory (AD) configurations using group policies to secure user accounts, control access, and minimize the attack surface. AD configurations enable centralized control over account settings, logon policies, and permissions, reducing the risk of unauthorized access and lateral movement within the network.
- **Restrict Web-Based Content:** Restricting web-based content involves enforcing policies and technologies that limit access to potentially malicious websites, unsafe downloads, and unauthorized browser behaviors. This can include URL filtering, download restrictions, script blocking, and extension control to protect against exploitation, phishing, and malware delivery.
- **Network Segmentation:** Network segmentation involves dividing a network into smaller, isolated segments to control and limit the flow of traffic between devices, systems, and applications. By segmenting networks, organizations can reduce the attack surface, restrict lateral movement by adversaries, and protect critical assets from compromise.
- **Disable or Remove Feature or Program:** Disable or remove unnecessary and potentially vulnerable software, features, or services to reduce the attack surface and prevent abuse by adversaries. This involves identifying software or features that are no longer needed or that could be exploited and ensuring they are either removed or properly disabled.
- **Limit Access to Resource Over Network:** Restrict access to network resources, such as file shares, remote systems, and services, to only those users, accounts, or systems with a legitimate business requirement. This can include employing technologies like network concentrators, RDP gateways, and zero-trust network access (ZTNA) models, alongside hardening services and protocols.
- **Network Intrusion Prevention:** Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool and will likely be different across various malware families and versions.
- **Filter Network Traffic:** Traffic to known anonymity networks and C2 infrastructure can be blocked through the use of network allow and block lists.

- **Data Loss Prevention:** Data Loss Prevention (DLP) involves implementing strategies and technologies to identify, categorize, monitor, and control the movement of sensitive data within an organization. This includes protecting data formats indicative of Personally Identifiable Information (PII), intellectual property, or financial data from unauthorized access, transmission, or exfiltration.

10. Sources

- *https://cybersecuritynews.com/coinbase-cartel-targets-high-value-sectors/*
- *https://www.fortiguard.com/threat-actor/6386/coinbase-cartel-ransomware*
- *https://businessinsights.bitdefender.com/coinbase-cartel-ransomware-group-extortion-tactics*
- *https://cybernews.com/security/lacoste-ralph-lauren-supply-chain-data-breach/*
- *https://www.linkedin.com/pulse/new-threat-actor-coinbase-cartel-joe-shenouda-m2lue/*
- *https://www.infostealers.com/article/inside-the-coinbase-cartel-how-infostealer-credentials-fueled-a-100-company-ransomware-spree/*