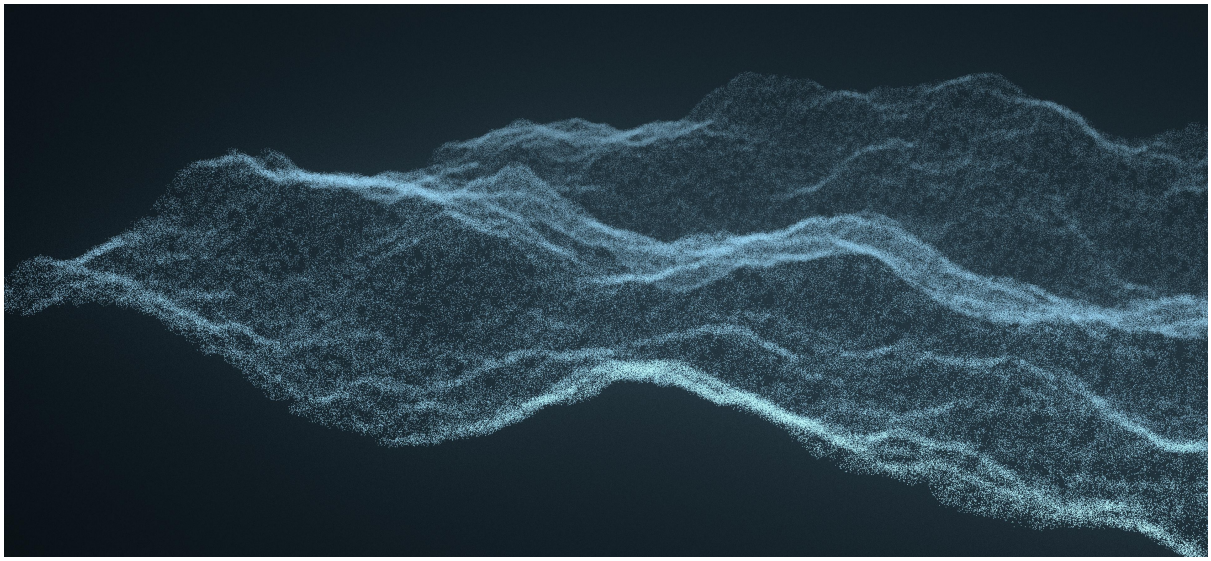


Vidar Analysis:

July 2nd, 2023. Written and Analyzed by Av4x

Twitter:

@av4xor

(*Skip to end for IOC list*)

Introduction:

Vidar is a very popular infostealer that first appeared in 2018 and is a branch of Arkei, another infostealer, but built with more capabilities. One of the more interesting components of Vidar is the ability to use “pads”, which essentially act as virtual dead-drops that tell a Vidar sample where it’s Command-and-Control (C2) is located. While

Vidar has been known to use Telegram channels to do this, Mastadon and Steam profiles have also been used.

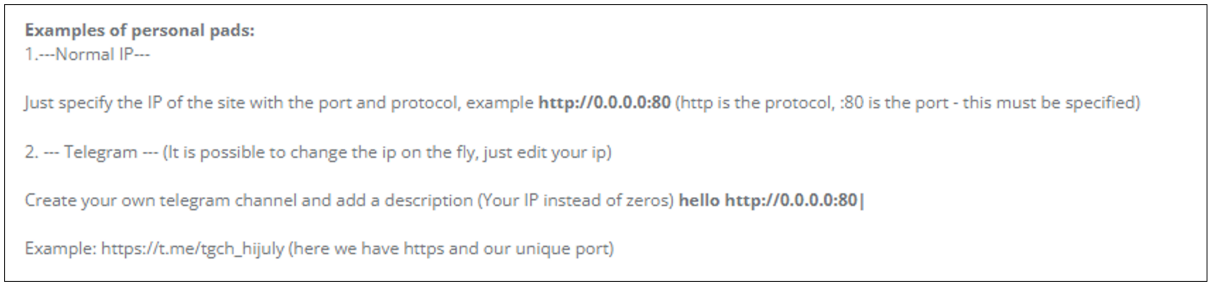


Figure 1, Source: (eSentire Threat Intelligence Malware Analysis: Vidar Stealer)

The main focus of this article is the documenting of the Steam profiles used. Why? During analysis of samples, I found that every single Steam profile found was still active whereas the vast majority of Telegram channels used as dead-drops no longer existed. In January 2023, ishaughnessy gave more insight into why this is on the Emerging Threats forum:

> *After contacting Steam regarding this C2 distribution method, they've concluded that it is important for users to be able to share information via their profile and will not be taking action. As of 2023/01/18 all of the above steam profiles are still active after reporting the accounts for abuse.*

Source: Vidar Stealer Picks Up Steam!

While Steam's stance is disappointing, and provides a more or less "bulletproof" dead-drop (the first Steam profile seen from 2021 is still up), the fact that all Steam profiles are still available for viewing as well as the fact that Steam stores past account names, means that these profiles provide a large number of IOCs for collection.

Through enumerating profiles on Steam and using VirusTotal's hunting capabilities, I managed to gather a decent sized collection of these C2 "pads". Whether on Telegram or Steam, the names of these pads have no obvious pattern to them and are probably by the C2 operator:

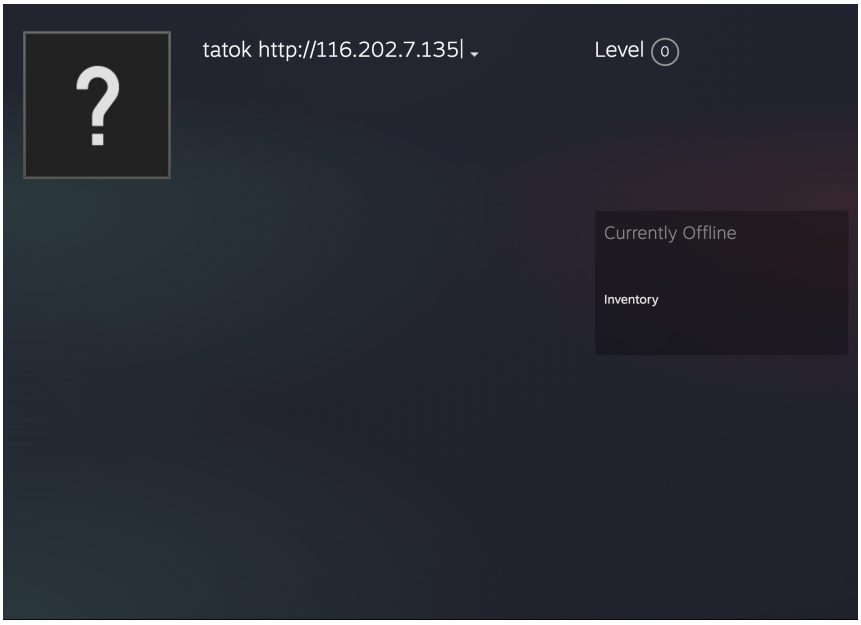
Examples:

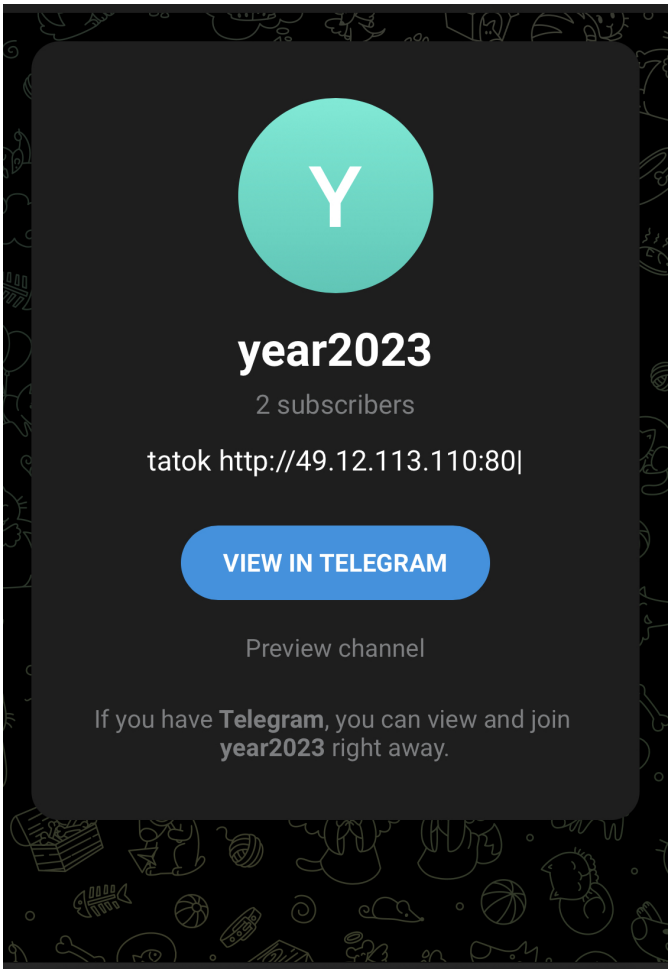
- tr0ck
- looking_glassbot
- Duckword
- Motafan
- libpcre
- broadcast
- mastersbots

Samples seemed to nearly always contain both a Telegram channel and a Steam account, forming pairs. I don't recall a single sample I looked at which contained only a Telegram channel or vice versa.

Example Pairs (Steam/Telegram):

- broadcast/mastersbots
- tatok/year2023start
- himars/mantarlars
- way2me/task4manager





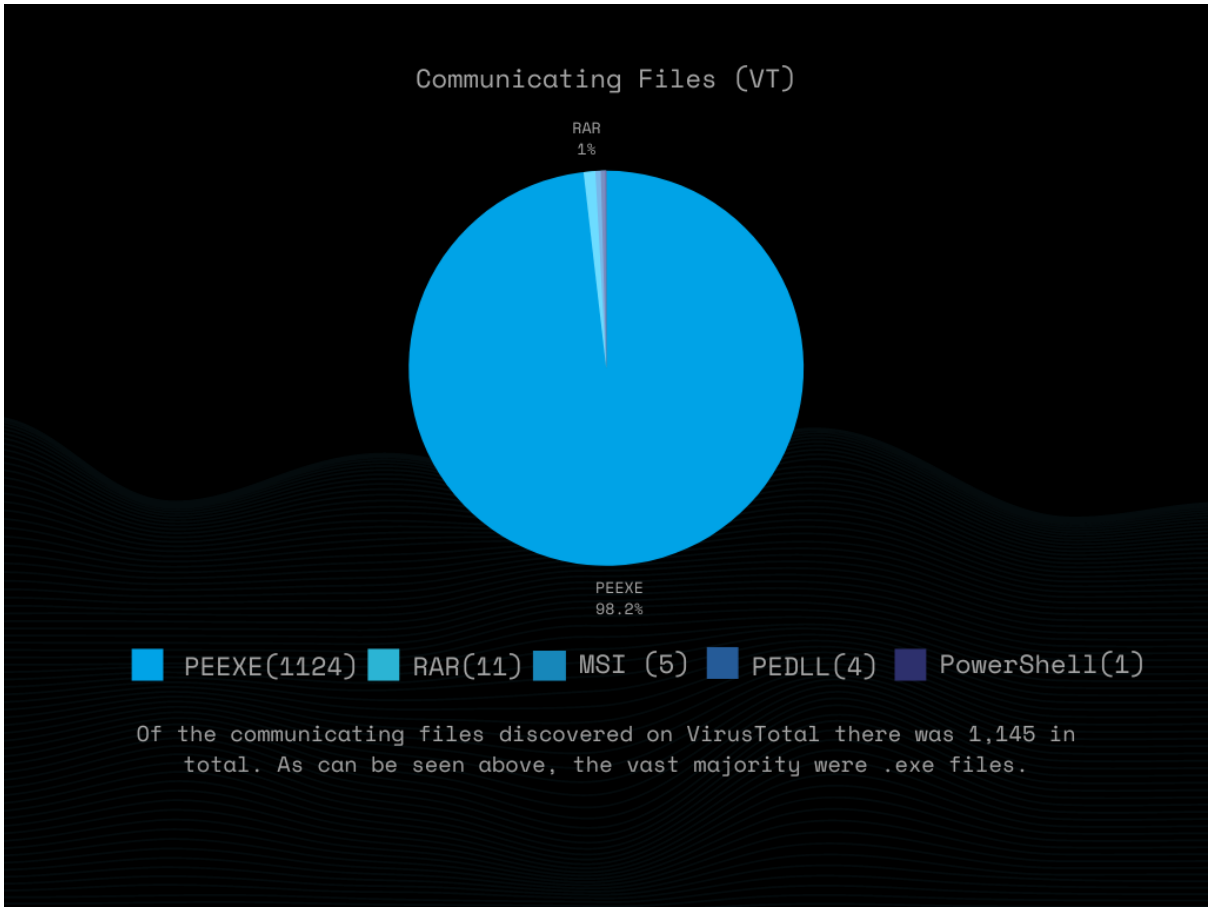
With 2 exceptions, all of the Telegram channels currently active followed similar patterns:

- Description is the name of associated Steam account, but with different IP address.
    - Only one account has a name not associated with Steam. Where the pair is r0chnu/prescilliouns, the description showed “prescillious”.
- All Telegram channels contained the IP address plus port 80.
    - Only one channel (t[.]me/motafan) had port 27015 (associated with Steam).
- All channels had 1 - 3 subscribers

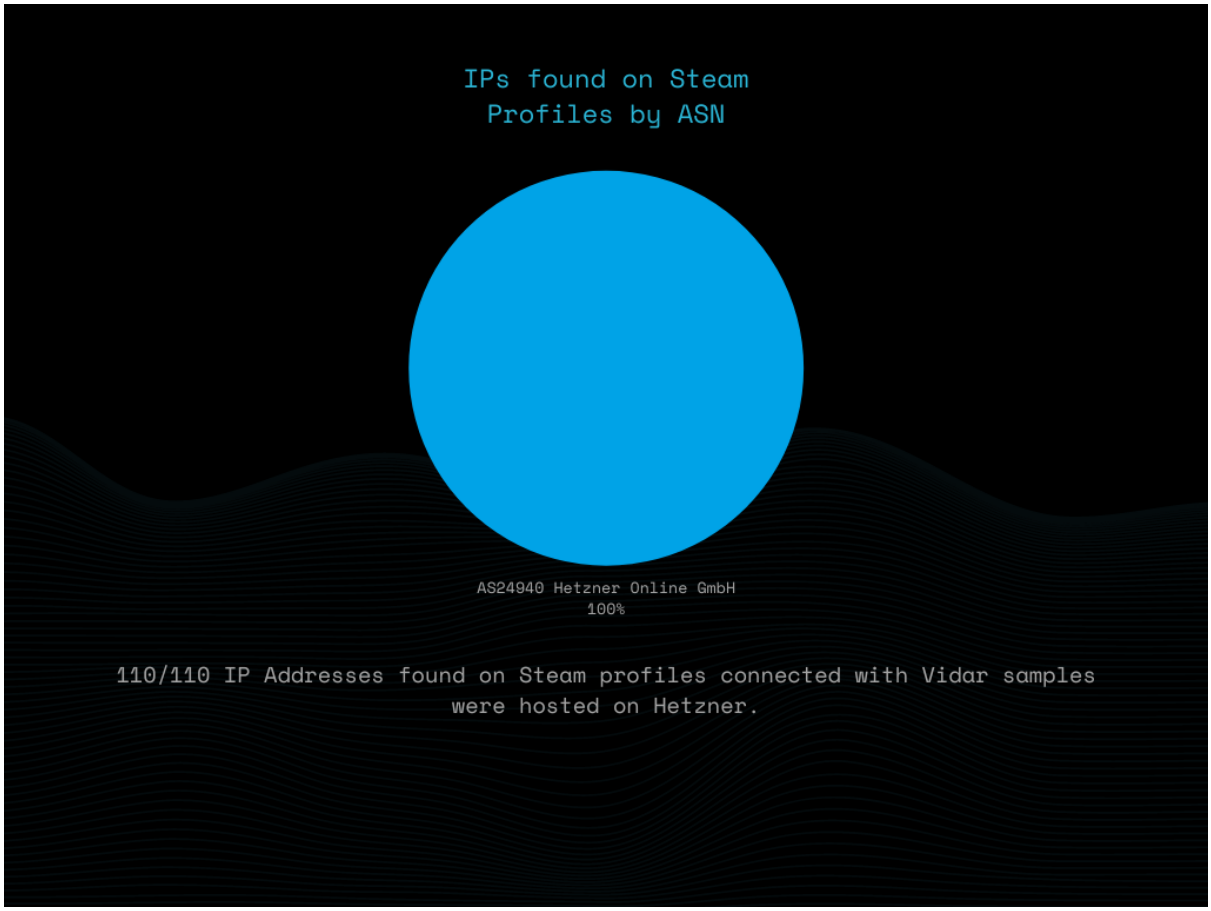
Only 9 out of 38 Telegram channels were still active.

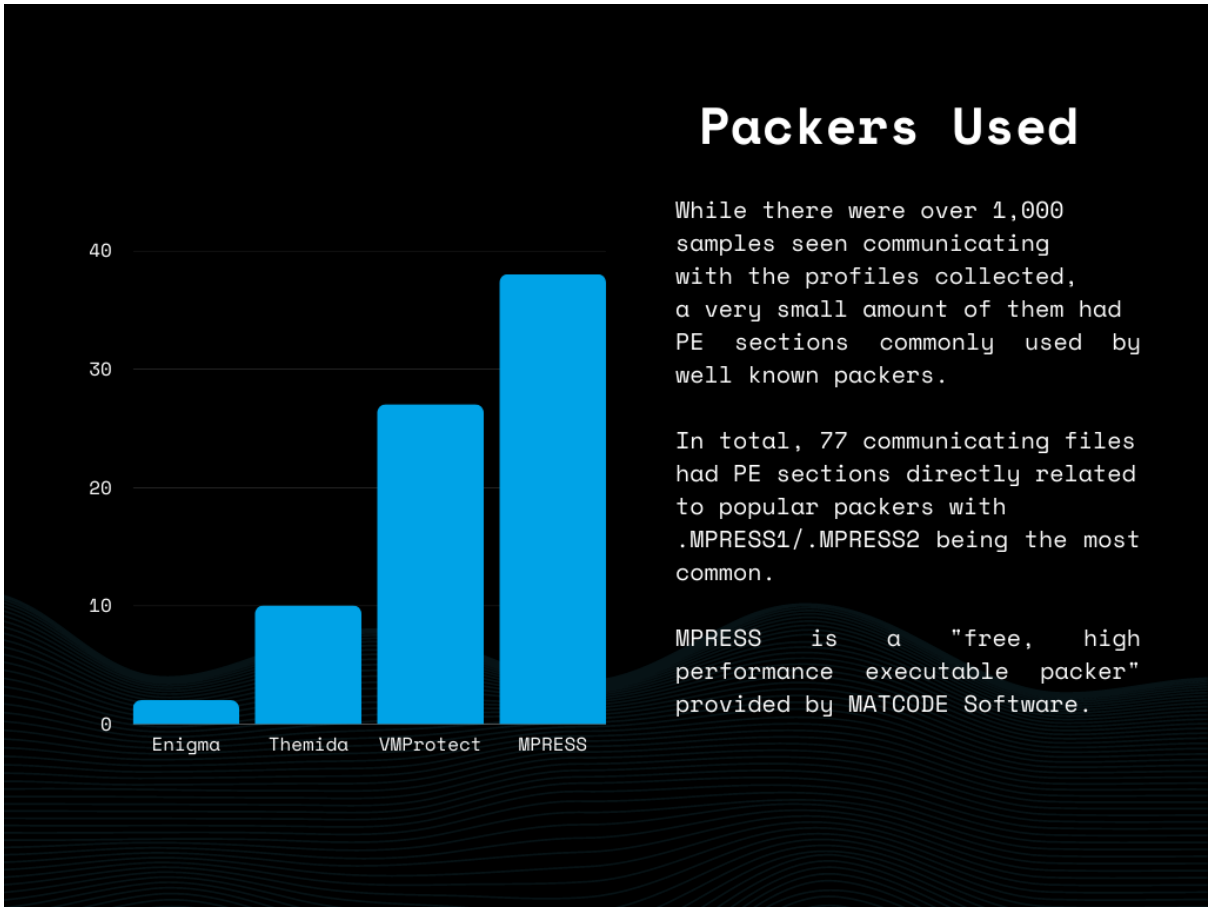
Statistics:

In total, 75 profiles/channels used by Vidar were found, with 38 being Telegram channels and 37 of them Steam profiles. Additionally, 110 C2 addresses were gathered. After enriching the data collected, I made these useless graphs because I haven’t made a graph in years:


Communicating Files (VT)
RAR
1%
PEEXE
98.2%
PEEXE(1124)
RAR(11)
MSI (5)
PEDLL(4)
PowerShell(1)
Of the communicating files discovered on VirusTotal there was 1,145 in total. As can be seen above, the vast majority were .exe files.


Files Seen & Detected by Months
This graph displays files submitted to VirusTotal and detected based on the date they were first seen.
The first file was on November 21st, 2021 and is marked as SmokeLoader. It's the first sample in this collection which contacted Steam and Telegram.
As can be seen, Vidar infections have risen tremendously since then.
600
400
200
0
9/2021 - 12/2021
1/2022 - 9/2022
10/2022 - 1/2023
1/2023 - 04/2023
4/2023 - 7/2023


IPs found on Steam
Profiles by ASN
AS24940 Hetzner Online GmbH
100%
110/110 IP Addresses found on Steam profiles connected with Vidar samples
were hosted on Hetzner.



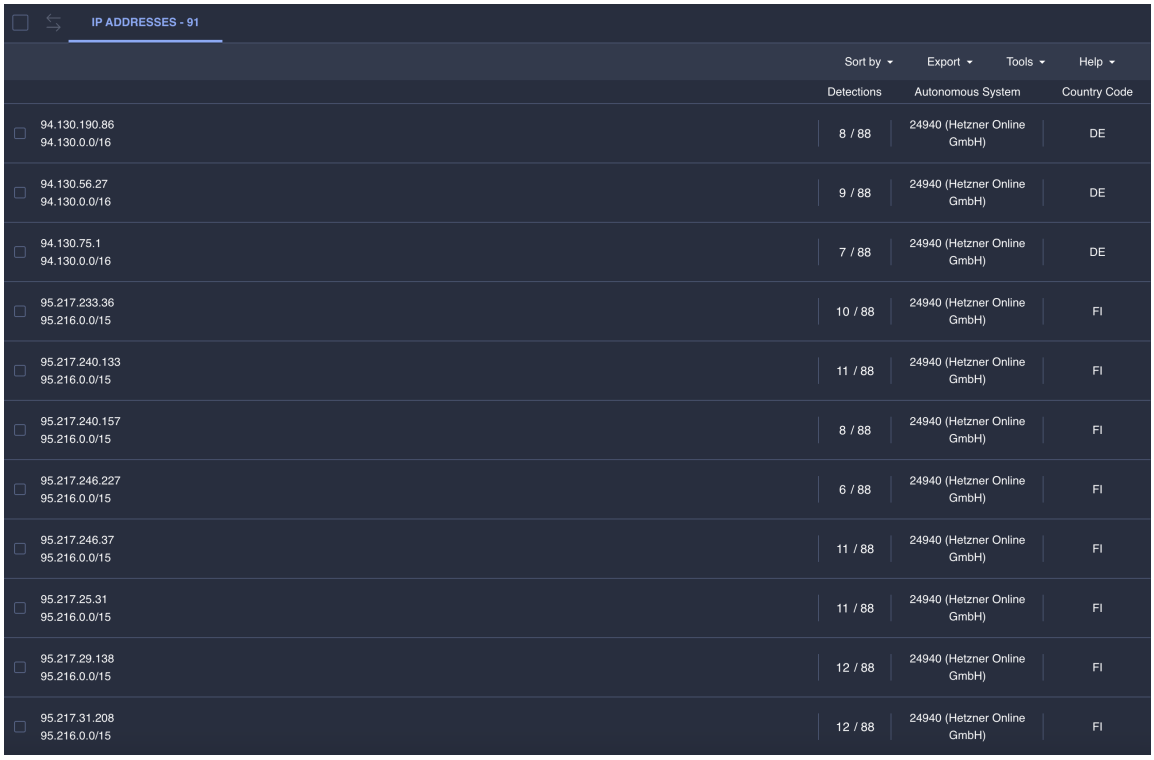
Findings:

1. Nearly all samples analyzed were shown on VirusTotal as having both the Steam profile and the associated Telegram channel embedded within the same sample, with few exceptions. However, Telegram was frequently shown as the only contacted URL on VirusTotal.

Embedded URLs (3)

Scanned	Detections	Status	URL
2023-06-15	2 / 90	200	https://steamcommunity.com/profiles/76561199511129510
2023-06-13	1 / 89	200	https://t.me/rechnungsbetrag
2023-06-22	12 / 90	200	http://88.99.87.20/

2. All IP addresses found on Steam profiles were hosted on Hetzner and either located in Germany or Finland.



IP ADDRESSES - 91

Sort by | Export | Tools | Help

	Detections	Autonomous System	Country Code
94.130.190.86 94.130.0.0/16	8 / 88	24940 (Hetzner Online GmbH)	DE
94.130.56.27 94.130.0.0/16	9 / 88	24940 (Hetzner Online GmbH)	DE
94.130.75.1 94.130.0.0/16	7 / 88	24940 (Hetzner Online GmbH)	DE
95.217.233.36 95.216.0.0/15	10 / 88	24940 (Hetzner Online GmbH)	FI
95.217.240.133 95.216.0.0/15	11 / 88	24940 (Hetzner Online GmbH)	FI
95.217.240.157 95.216.0.0/15	8 / 88	24940 (Hetzner Online GmbH)	FI
95.217.246.227 95.216.0.0/15	6 / 88	24940 (Hetzner Online GmbH)	FI
95.217.246.37 95.216.0.0/15	11 / 88	24940 (Hetzner Online GmbH)	FI
95.217.25.31 95.216.0.0/15	11 / 88	24940 (Hetzner Online GmbH)	FI
95.217.29.138 95.216.0.0/15	12 / 88	24940 (Hetzner Online GmbH)	FI
95.217.31.208 95.216.0.0/15	12 / 88	24940 (Hetzner Online GmbH)	FI

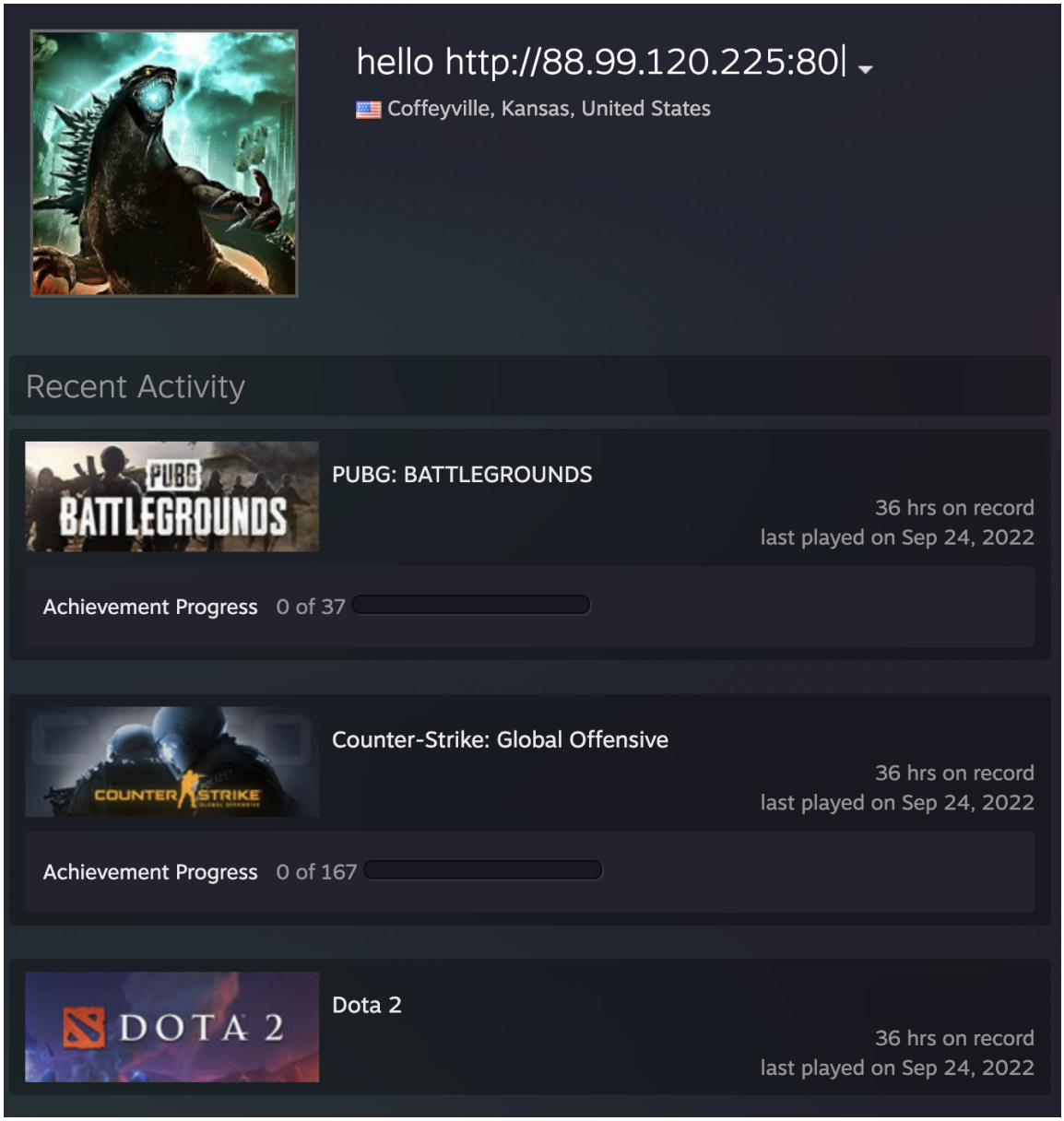
3. Steam profiles are still actively being created and used by Vidar for dead-drops. I discovered the most profiles roughly two months ago and more profiles have been created since.
4. The first sample seen associated with any of the Steam or Telegram accounts found was submitted to VirusTotal on November 10th, 2021 and identified as SmokeLoader. It contacted Telegram, Koyuspace (a fork, of a fork, of Mastadon), and Steam.

   No other samples associated with any of the other discovered profiles were submitted to VirusTotal until almost exactly a year later on November 21st, 2022.

   a. Sample: 66bf743babad7405d2426b25bf8d1bb493f6d9048b55ede138d36a3b8a2f9c8e

5. 3 Steam profiles were discovered without any related samples found on VirusTotal. The most interesting of these was the third “hello” profile discovered.

   This account had a profile picture (only one other does), 3 games are marked as “played” (with the same exact amount of hours and on the same day), and a past name was used on the account which does not contain an IP address.



I realize the unique aspects of this profile really don't mean much, especially since it doesn't appear to have been used at all, but I mainly just found it interesting that this profile seemed to have been made to look more legitimate.

IOCs

IPs:

```
116.202.0.132
116.202.181.154
116.202.185.129
```

```
116.202.2.42
116.202.4.70
116.202.5.245
116.202.6.237
116.202.6.47
116.202.7.135
116.202.8.130
116.203.11.245
116.203.11.45
116.203.13.214
116.203.15.76
116.203.164.141
116.203.165.188
116.203.165.219
116.203.166.104
116.203.166.131
116.203.166.139
116.203.166.2
116.203.167.3
116.203.240.51
116.203.6.107
116.203.69.150
116.203.7.201
116.203.7.45
116.203.7.73
116.203.9.69
128.140.35.86
128.140.41.121
128.140.94.214
135.181.203.71
142.132.228.165
142.132.236.84
157.90.21.41
157.90.244.205
159.69.178.243
167.235.75.60
168.119.236.82
168.119.243.28
195.201.237.253
195.201.251.109
195.201.253.168
195.201.255.246
195.201.44.125
195.201.45.110
195.201.45.16
195.201.45.53
195.201.46.32
195.201.47.75
49.12.117.107
49.12.118.167
49.12.119.56
49.12.8.228
5.75.142.250
5.75.147.195
5.75.149.127
5.75.159.217
5.75.188.254
5.75.210.95
```

```
5.75.213.23
5.75.234.249
5.75.250.52
65.109.168.175
65.109.225.236
65.109.9.93
78.46.148.93
78.46.238.118
78.47.172.233
78.47.216.96
78.47.225.61
78.47.226.24
78.47.228.65
78.47.233.145
88.198.116.74
88.198.120.151
88.198.152.171
88.198.194.199
88.198.77.204
88.198.95.89
88.99.120.225
88.99.120.56
91.107.199.176
91.107.199.224
91.107.232.62
94.130.190.118
94.130.190.86
94.130.56.27
94.130.75.1
95.216.183.16
95.217.233.36
95.217.240.133
95.217.240.157
95.217.246.227
95.217.246.37
95.217.25.224
95.217.25.31
95.217.29.138
95.217.29.31
95.217.31.208
49.12.113.110
116.202.183.154
23.88.36.149
142.132.230.215
142.132.168.13
78.46.254.12
142.132.183.252
49.13.50.61
162.55.53.95
```

Accounts:

```
https://steamcommunity.com/profiles/76561199471222742
https://t.me/nemesisgrow
https://steamcommunity.com/profiles/76561199492257783
https://t.me/justsometg
https://steamcommunity.com/profiles/76561199501059503
https://t.me/mastersbots
https://steamcommunity.com/profiles/76561198272578552
https://t.me/libpcre
https://steamcommunity.com/profiles/76561199482248283
https://t.me/dionysus_tg
https://steamcommunity.com/profiles/76561199445991535
https://t.me/traduttoretg
https://steamcommunity.com/profiles/76561199441933804
https://t.me/dishasta
https://steamcommunity.com/profiles/76561199494593681
https://t.me/auftriebs
https://steamcommunity.com/profiles/76561199486572327
https://t.me/zaskullz
https://steamcommunity.com/profiles/76561199439725733
https://t.me/samuelljax
https://steamcommunity.com/profiles/76561199474840123
https://t.me/mantarlars
https://steamcommunity.com/profiles/76561199443972360
https://t.me/ttruelive
https://steamcommunity.com/profiles/76561199472399815
https://t.me/litlebey
https://steamcommunity.com/profiles/76561199441999914
https://t.me/dahuasecurit
https://steamcommunity.com/profiles/76561199476091435
https://t.me/gurutist
https://steamcommunity.com/profiles/76561199471266194
https://t.me/jetbim
https://t.me/jetbim2
https://steamcommunity.com/profiles/76561199459255837
https://t.me/iseepass
https://steamcommunity.com/profiles/76561199446766594
https://t.me/ibommat
https://steamcommunity.com/profiles/76561199480821604
https://t.me/robertotalks
https://steamcommunity.com/profiles/76561199472266392
https://steamcommunity.com/profiles/76561199489580435
https://t.me/tabootalks
https://steamcommunity.com/profiles/76561199469016299
https://t.me/traveltickетshop
https://steamcommunity.com/profiles/76561199439929669
https://t.me/asifrazatg
https://steamcommunity.com/profiles/76561199458928097
https://t.me/robloxblackl
https://steamcommunity.com/profiles/76561199467421923
https://t.me/year2023start
https://steamcommunity.com/profiles/76561199478503353
https://t.me/noktasina
https://steamcommunity.com/profiles/76561199263069598
https://t.me/cybehost
https://steamcommunity.com/profiles/76561199514261168
https://t.me/kamaprimo
https://steamcommunity.com/profiles/76561199235044780
```

```
https://t.me/headlist
https://steamcommunity.com/profiles/76561199469677637
https://t.me/tgdatapacks
https://steamcommunity.com/profiles/76561199436777531
https://t.me/headshotsonly
https://steamcommunity.com/profiles/76561199499188534
https://t.me/nutalse
https://steamcommunity.com/profiles/76561199508624021
https://t.me/looking_glassbot
https://steamcommunity.com/profiles/76561199497218285
https://t.me/tg_duckworld
https://t.me/motafan
https://steamcommunity.com/profiles/76561199520592470
https://steamcommunity.com/profiles/76561199511129510
https://t.me/rechnungsbetrag
https://t.me/prescilliouns
https://steamcommunity.com/profiles/76561199510444991
https://t.me/task4manager
```