Uncovering the Wholesale Industry of Social Media Fraud
From Botnets to Bulk Reseller Panels

Masarah Paquet-Clouston
Olivier Bilodeau
GoSecure Research

vb 2018
MONTREAL
3 – 5 October 2018

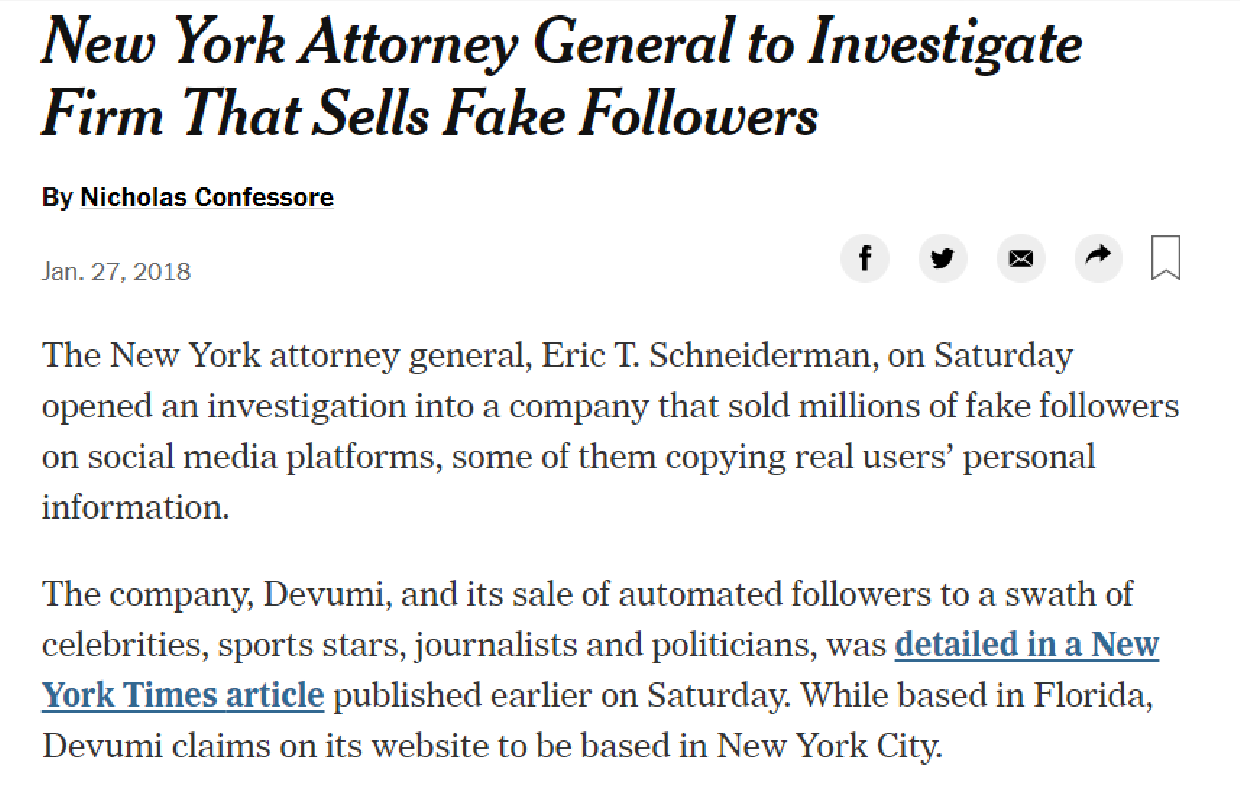
GoSecure
CounterTack

Who Am I?

- Security researcher at GoSecure
- PhD candidate in criminology at SFU
- Organization committee of the NorthSec (nsec) Conference

nsec

Research Context



New York Attorney General to Investigate Firm That Sells Fake Followers

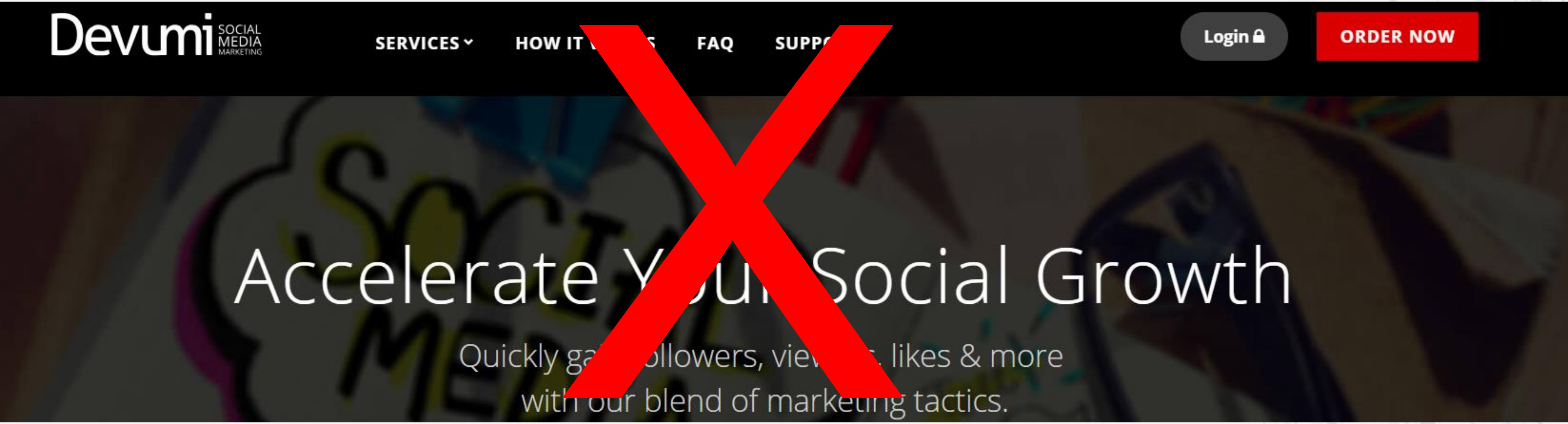
By Nicholas Confessore

Jan. 27, 2018

The New York attorney general, Eric T. Schneiderman, on Saturday opened an investigation into a company that sold millions of fake followers on social media platforms, some of them copying real users' personal information.

The company, Devumi, and its sale of automated followers to a swath of celebrities, sports stars, journalists and politicians, was **detailed in a New York Times article** published earlier on Saturday. While based in Florida, Devumi claims on its website to be based in New York City.

The Followers’ Factory (New York Times Inv.)

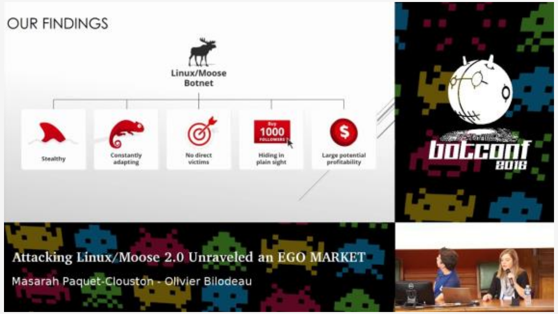


Accelerate Y Social Growth

Quickly ga ollowers, vie likes & more with our blend of marketing tactics.

GoSecure CounterTack

At the time


OUR FINDINGS

Attacking Linux/Moose 2.0 Unraveled an EGO MARKET

Masarah Paquet-Clouston - Olivier Bilodeau

Linux/Moose Botnet

GoSecure

EGO MARKET

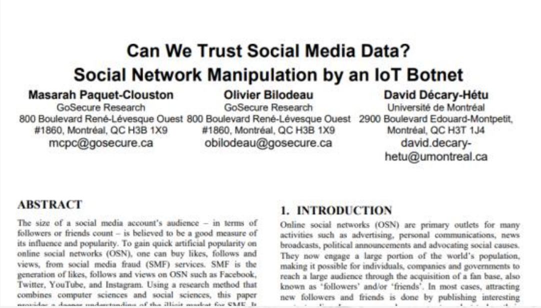
When Greed for Fame Benefits Large-Scale Botnets

ATTACKING LINUX/MOOSE UNRAVELED AN EGO MARKET

Masarah Paquet-Clouston
Olivier Bilodeau
GoSecure Inc.

Masarah Paquet-Clouston
- Researcher at GoSecure Inc.
- Master student in Criminology at Université de Montréal
- Treasurer for the Northsec conference

Olivier Bilodeau
- Security Research Lead at GoSecure Inc.
- VP training for the Northsec Conference and CTF


Can We Trust Social Media Data? Social Network Manipulation by an IoT Botnet

Masarah Paquet-Clouston
GoSecure Research
800 Boulevard René-Lévesque Ouest
#1860, Montréal, QC H3B 1X9
mcpc@gosecure.ca

Olivier Bilodeau
GoSecure Research
800 Boulevard René-Lévesque Ouest
#1860, Montréal, QC H3B 1X9
obilodeau@gosecure.ca

David Décary-Hétu
Université de Montréal
2900 Boulevard Edouard-Montpetit,
Montréal, QC H3T 1J4
david.decary-hetu@umontreal.ca

ABSTRACT

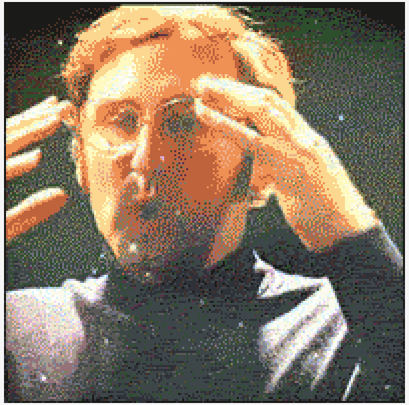
The size of a social media account's audience – in terms of followers or friends count – is believed to be a good measure of its influence and popularity. To gain quick artificial popularity on online social networks (OSN), one can buy likes, follows and views, from social media fraud (SMF) services. SMF is the generation of likes, follows and views on OSN such as Facebook, Twitter, YouTube, and Instagram. Using a research method that combines computer sciences and social sciences, this paper

1. INTRODUCTION

Online social networks (OSN) are primary outlets for many activities such as advertising, personal communications, news broadcasts, political announcements and advocating social causes. They now engage a large portion of the world's population, making it possible for individuals, companies and governments to reach a large audience through the acquisition of a fan base, also known as 'followers' and/or 'friends'. In most cases, attracting new followers and friends is done by publishing interesting

We thought….

Targeting Demuvi!



There is so much more behind this industry….

Today's Presentation

Uncover the supply chain behind social media fraud

The Main Providers

Linux/Moose

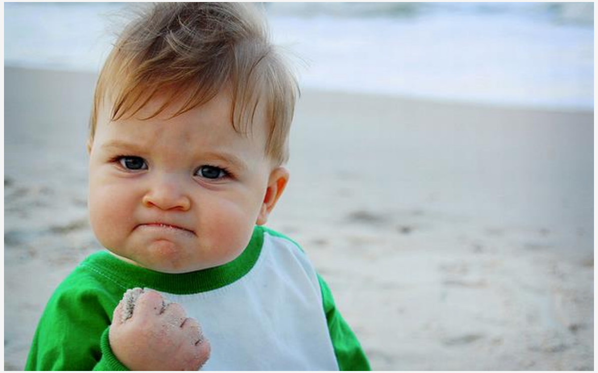
An IoT botnet that conducts social media fraud

Recap of Linux/Moose

- Affects routers / Internet of Things (IoT)
    - Embedded Linux systems with busybox userland
- Worm-like behavior
    - Telnet credential brute force
- Payload: Proxy service
    - SOCKSv4/v5, HTTP, HTTPS
- Used to proxy traffic to social media sites (mainly Instagram)

Investigating Linux/Moose

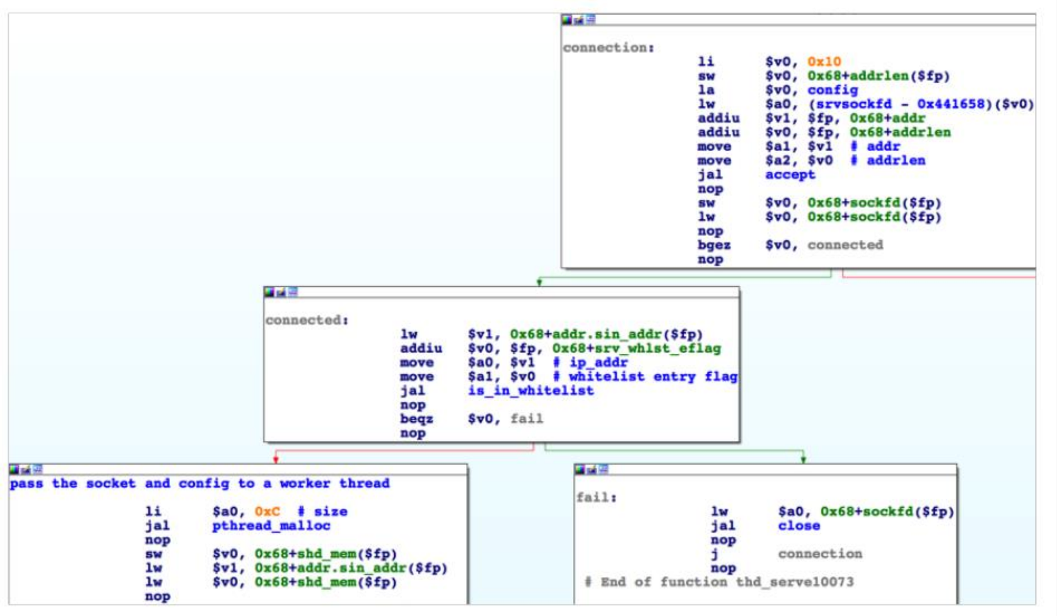
- Built and infected IoT honeypots (10 in 5 countries)
- Conducted a man-in-the-middle-attack



Accessed the raw traffic

Untold Feature of Linux/Moose

Seven Whitelisted IPs



```
connection:
                li      $v0, 0x10
                sw      $v0, 0x68+addrlen($fp)
                la      $v0, config
                lw      $a0, (srvsockfd - 0x441658)($v0)
                addiu   $v1, $fp, 0x68+addr
                addiu   $v0, $fp, 0x68+addrlen
                move    $a1, $v1  # addr
                move    $a2, $v0  # addrlen
                jal     accept
                nop
                sw      $v0, 0x68+sockfd($fp)
                lw      $v0, 0x68+sockfd($fp)
                nop
                bgez    $v0, connected
                nop
```

```
connected:
                lw      $v1, 0x68+addr.sin_addr($fp)
                addiu   $v0, $fp, 0x68+srv_whlst_eflag
                move    $a0, $v1  # ip_addr
                move    $a1, $v0  # whitelist entry flag
                jal     is_in_whitelist
                nop
                beqz    $v0, fail
                nop
```

```
pass the socket and config to a worker thread

                li      $a0, 0xC  # size
                jal     pthread_malloc
                nop
                sw      $v0, 0x68+shd_mem($fp)
                lw      $v1, 0x68+addr.sin_addr($fp)
                lw      $v0, 0x68+shd_mem($fp)
                nop
```

```
fail:
                lw      $a0, 0x68+sockfd($fp)
                jal     close
                nop
                j       connection
                nop
 # End of function thd_serve10073
```

Reseller Model?

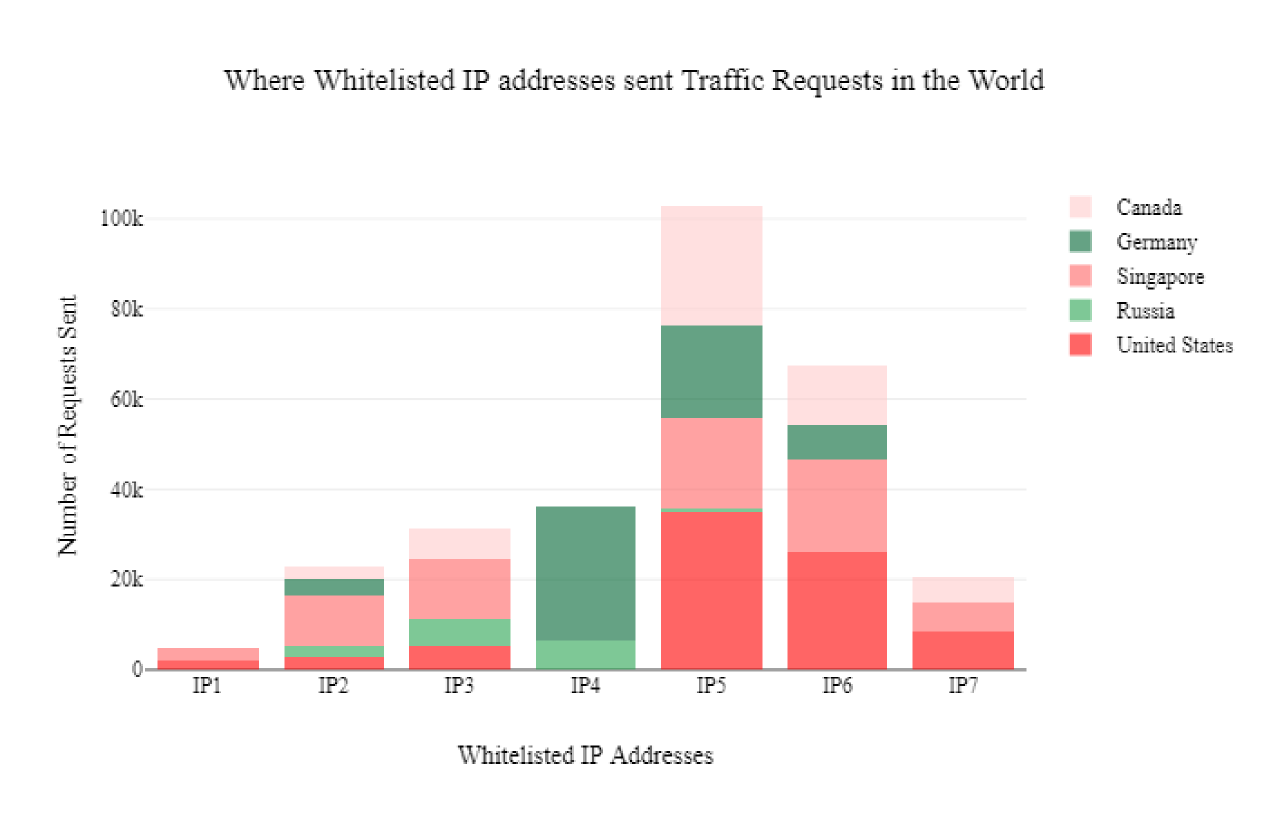
Testing the Reseller Model Hypothesis

Investigate similarities in traffic sent by each whitelisted IP based on these variables:

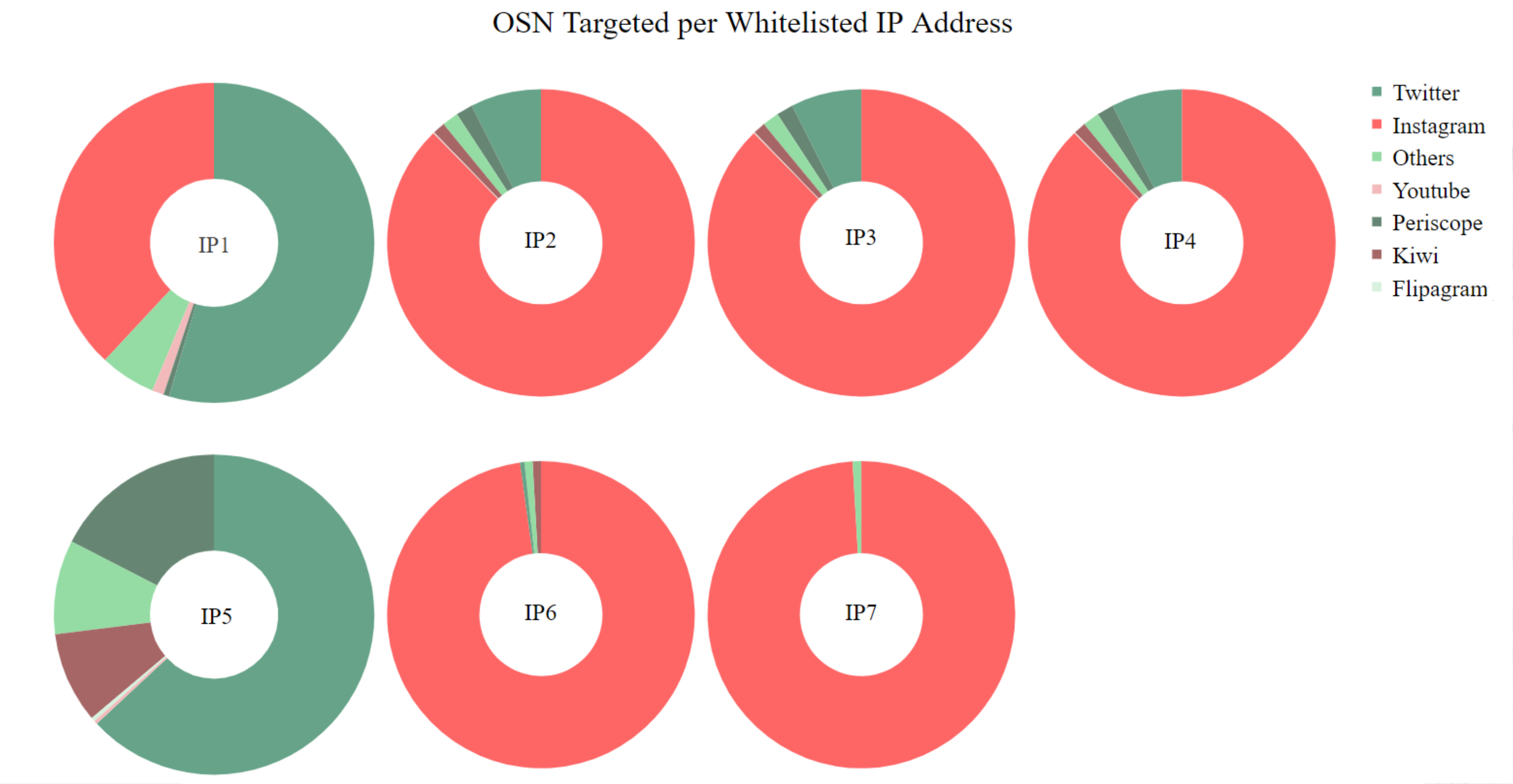
- Honeypots used
- Websites targeted
- TLS fingerprints
- User agents
- API calls
- Timestamps
- Accounts created on social networks
- Accounts followed on social networks

Any other ideas?

Honeypots Used



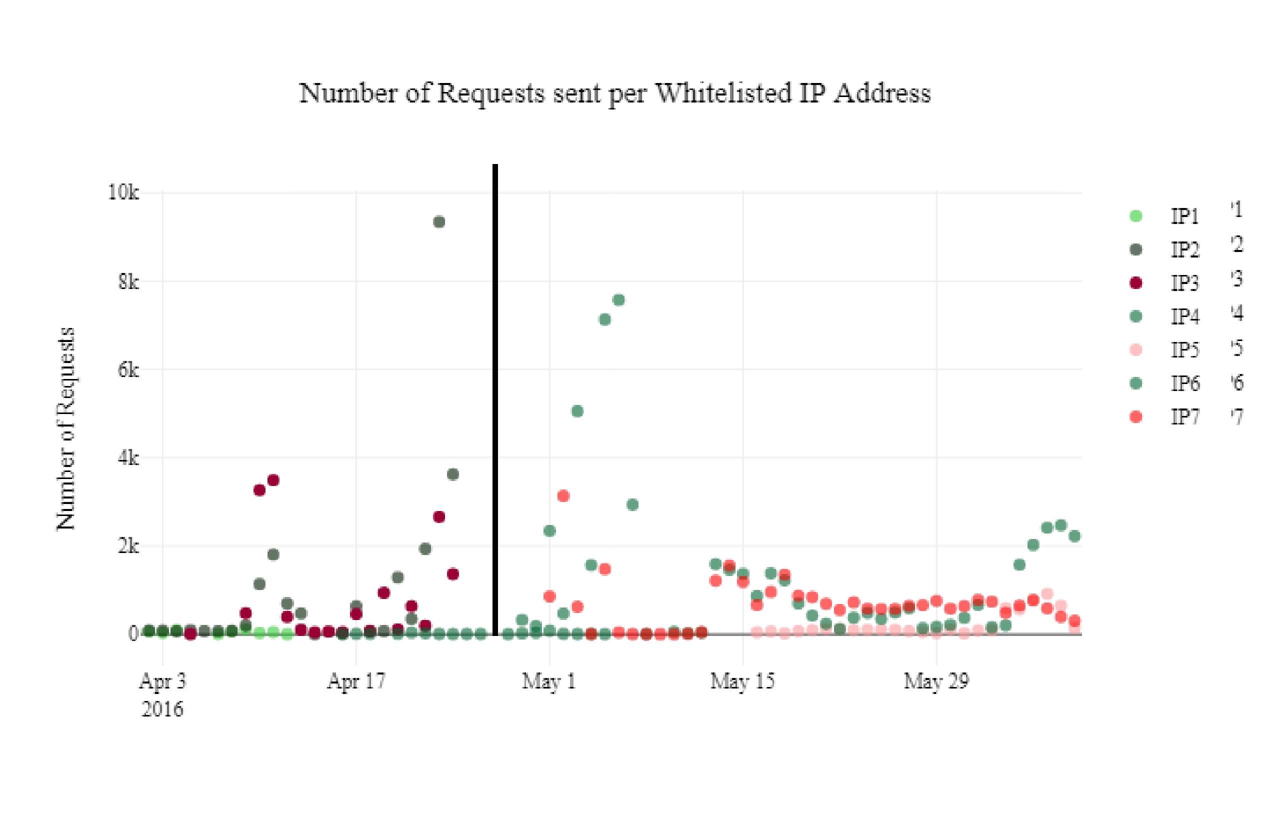
Websites Targeted



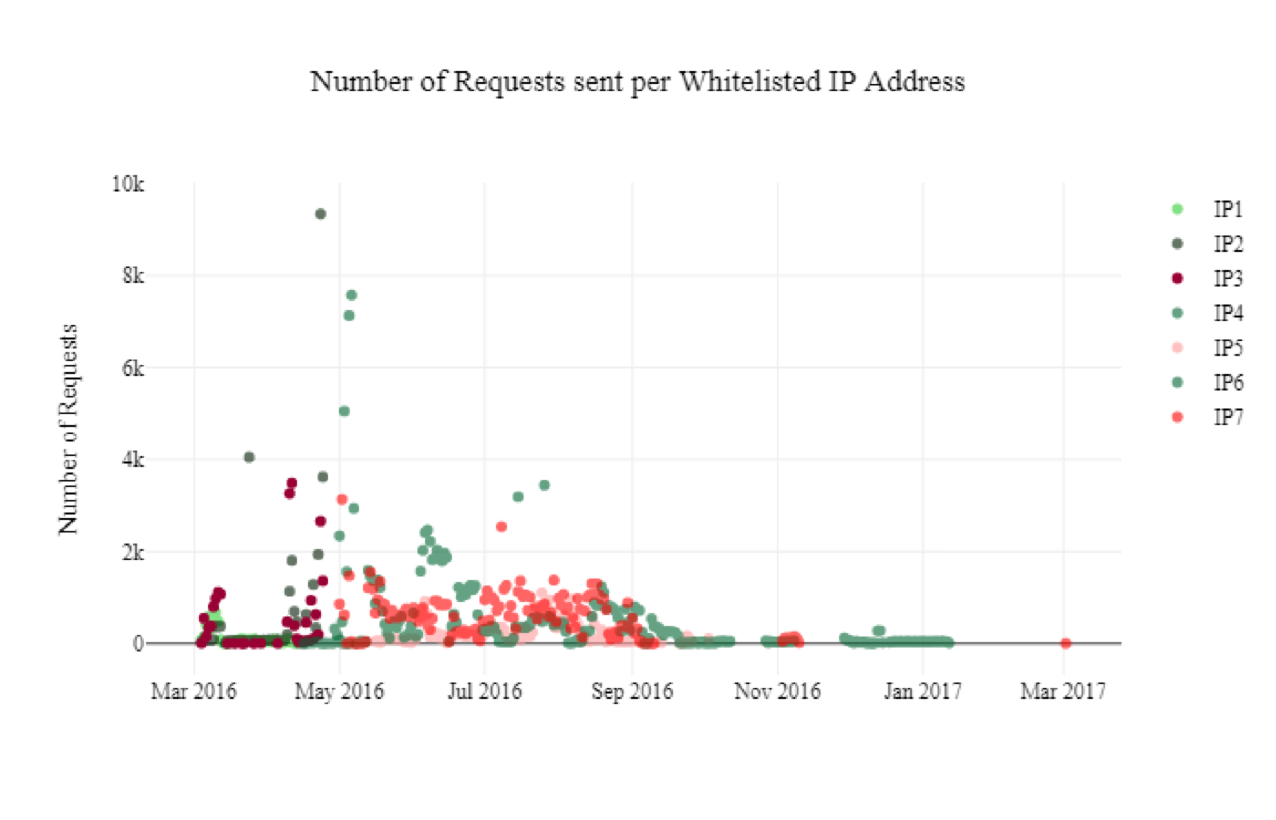
Other Variables

- TLS fingerprinting
  https://github.com/synackpse/tls-fingerprinting/tree/master/fingerprints
- User agents
- API calls

Timestamps


Number of Requests sent per Whitelisted IP Address
Number of Requests
10k
8k
6k
4k
2k
0
Apr 3
2016
Apr 17
May 1
May 15
May 29
IP1 '1
IP2 '2
IP3 '3
IP4 '4
IP5 '5
IP6 '6
IP7 '7

Timestamps



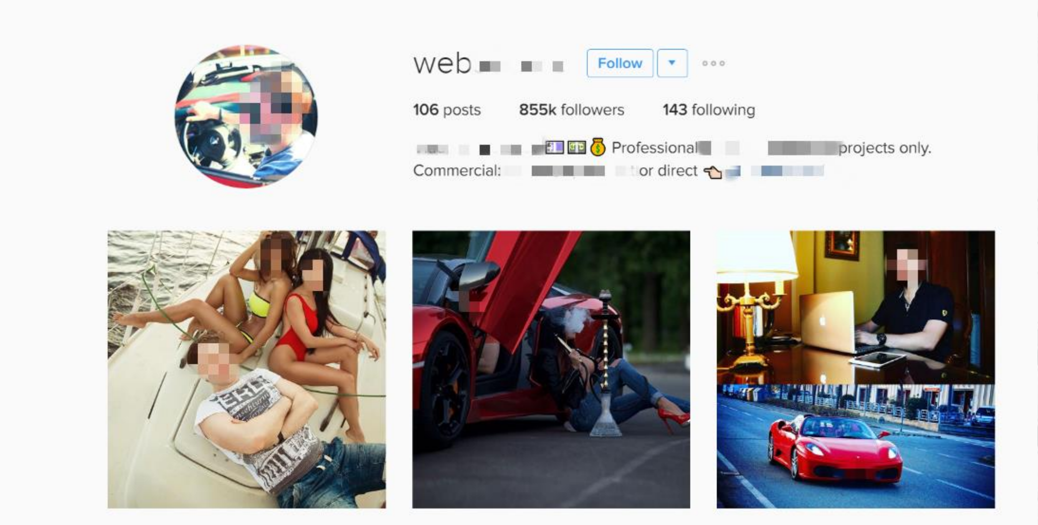
Number of Requests sent per Whitelisted IP Address
Number of Requests
10k
8k
6k
4k
2k
0
Mar 2016
May 2016
Jul 2016
Sep 2016
Nov 2016
Jan 2017
Mar 2017
IP1
IP2
IP3
IP4
IP5
IP6
IP7

Accounts Created and Accounts Followed

Whitelisted IPs followed the same accounts →

AND

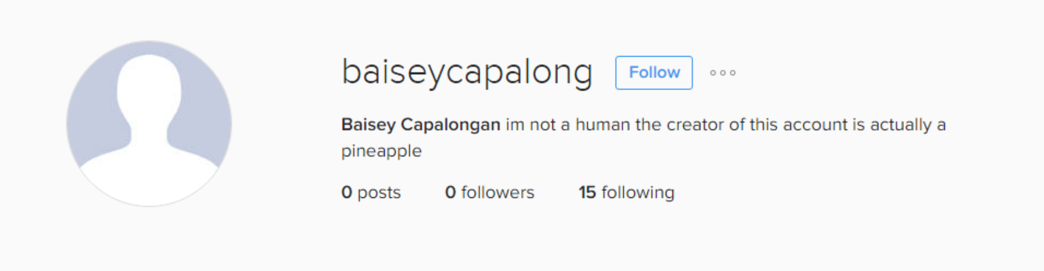
List of fake accounts per whitelisted IP →



web [redacted] Follow

106 posts 855k followers 143 following

[redacted] Professional [redacted] projects only.
Commercial: [redacted] or direct [redacted]



baiseycapalong Follow

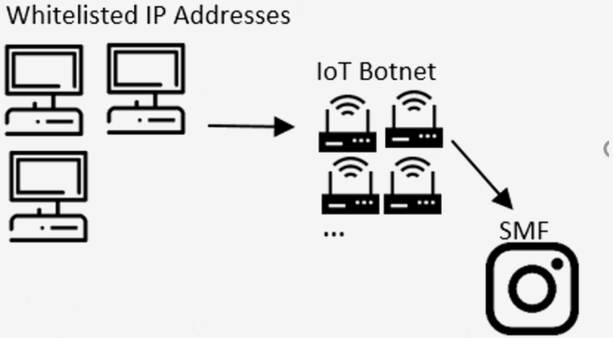
Baisey Capalongan im not a human the creator of this account is actually a pineapple

0 posts **0** followers **15** following

Purpose of the Whitelisted IPs

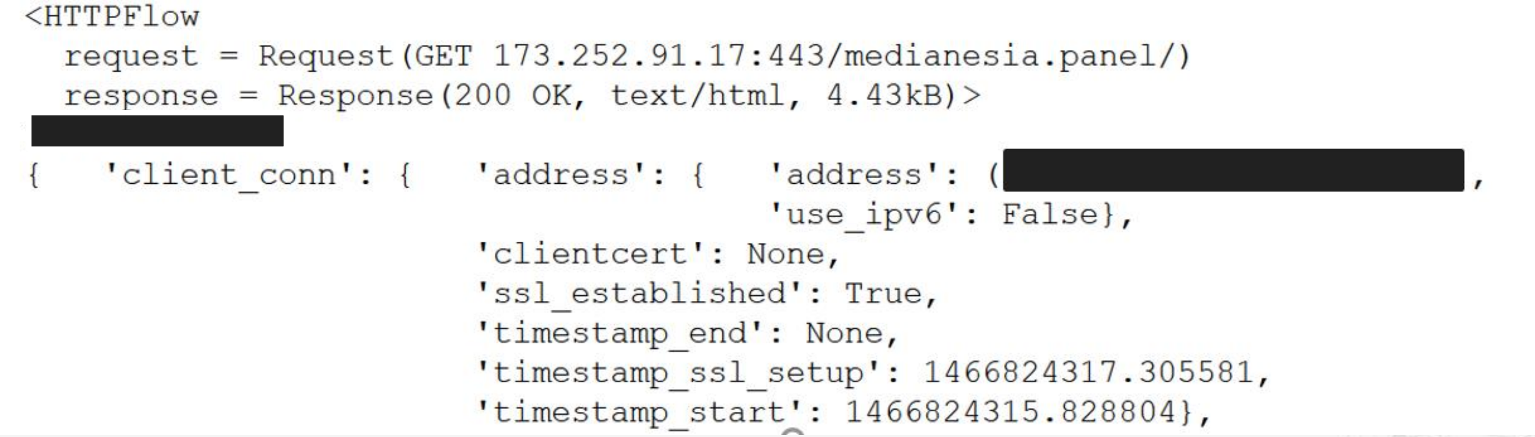
Fake account management !

Most likely: windows servers with proxy-aware Instagram fat-client is used to manage fake accounts and the flows of interactions with social networks



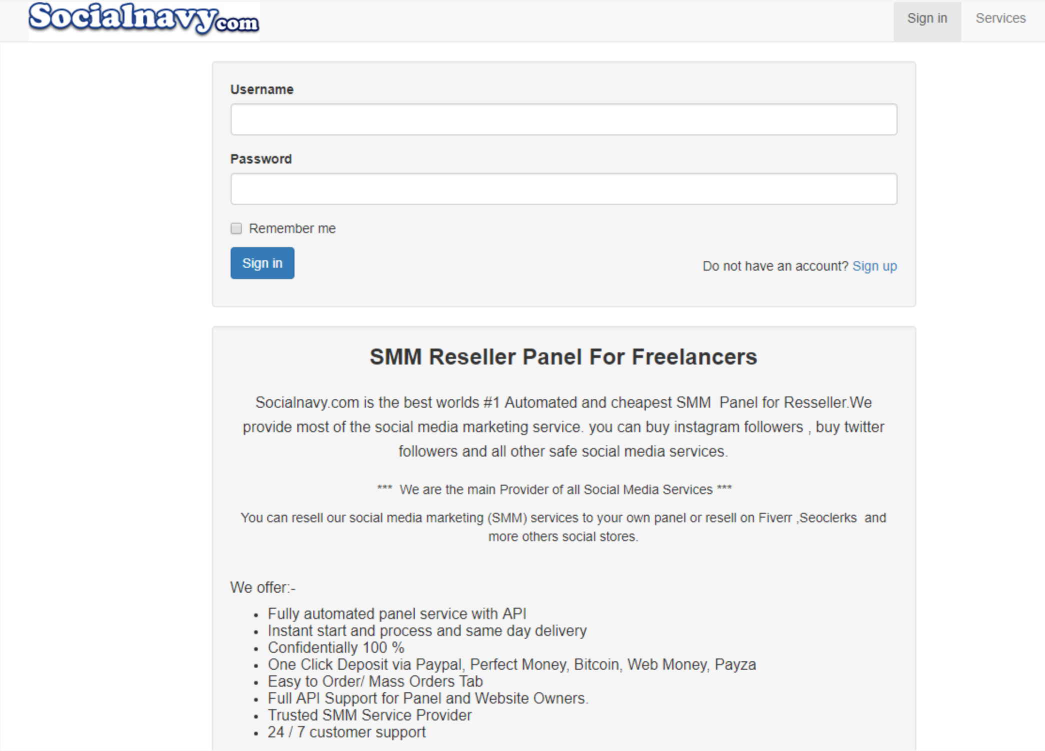
Let’s look at other actors

Found in the decrypted traffic : reseller panels



```
<HTTPFlow
  request = Request(GET 173.252.91.17:443/medianesia.panel/)
  response = Response(200 OK, text/html, 4.43kB)>
[redacted]
{   'client_conn': {   'address': {   'address': ([redacted],
                                      'use_ipv6': False},
                       'clientcert': None,
                       'ssl_established': True,
                       'timestamp_end': None,
                       'timestamp_ssl_setup': 1466824317.305581,
                       'timestamp_start': 1466824315.828804},
```

Bulk Reseller Panels



Username

Password

□ Remember me

Sign in

Do not have an account? Sign up

SMM Reseller Panel For Freelancers

Socialnavy.com is the best worlds #1 Automated and cheapest SMM Panel for Resseller.We provide most of the social media marketing service. you can buy instagram followers , buy twitter followers and all other safe social media services.

*** We are the main Provider of all Social Media Services ***

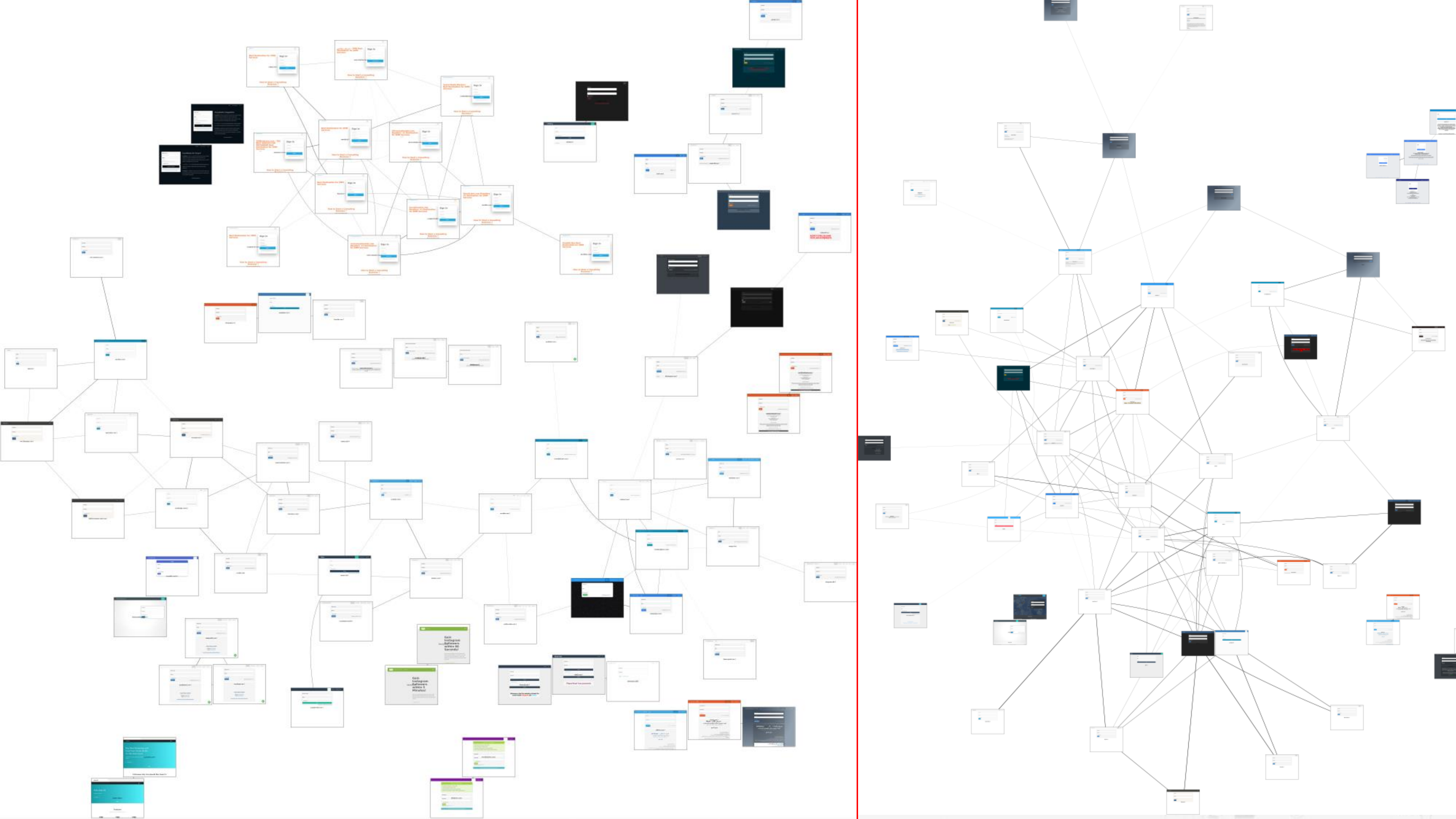
You can resell our social media marketing (SMM) services to your own panel or resell on Fiverr ,Seoclerks and more others social stores.

We offer:-

- Fully automated panel service with API
- Instant start and process and same day delivery
- Confidentially 100 %
- One Click Deposit via Paypal, Perfect Money, Bitcoin, Web Money, Payza
- Easy to Order/ Mass Orders Tab
- Full API Support for Panel and Website Owners.
- Trusted SMM Service Provider
- 24 / 7 customer support

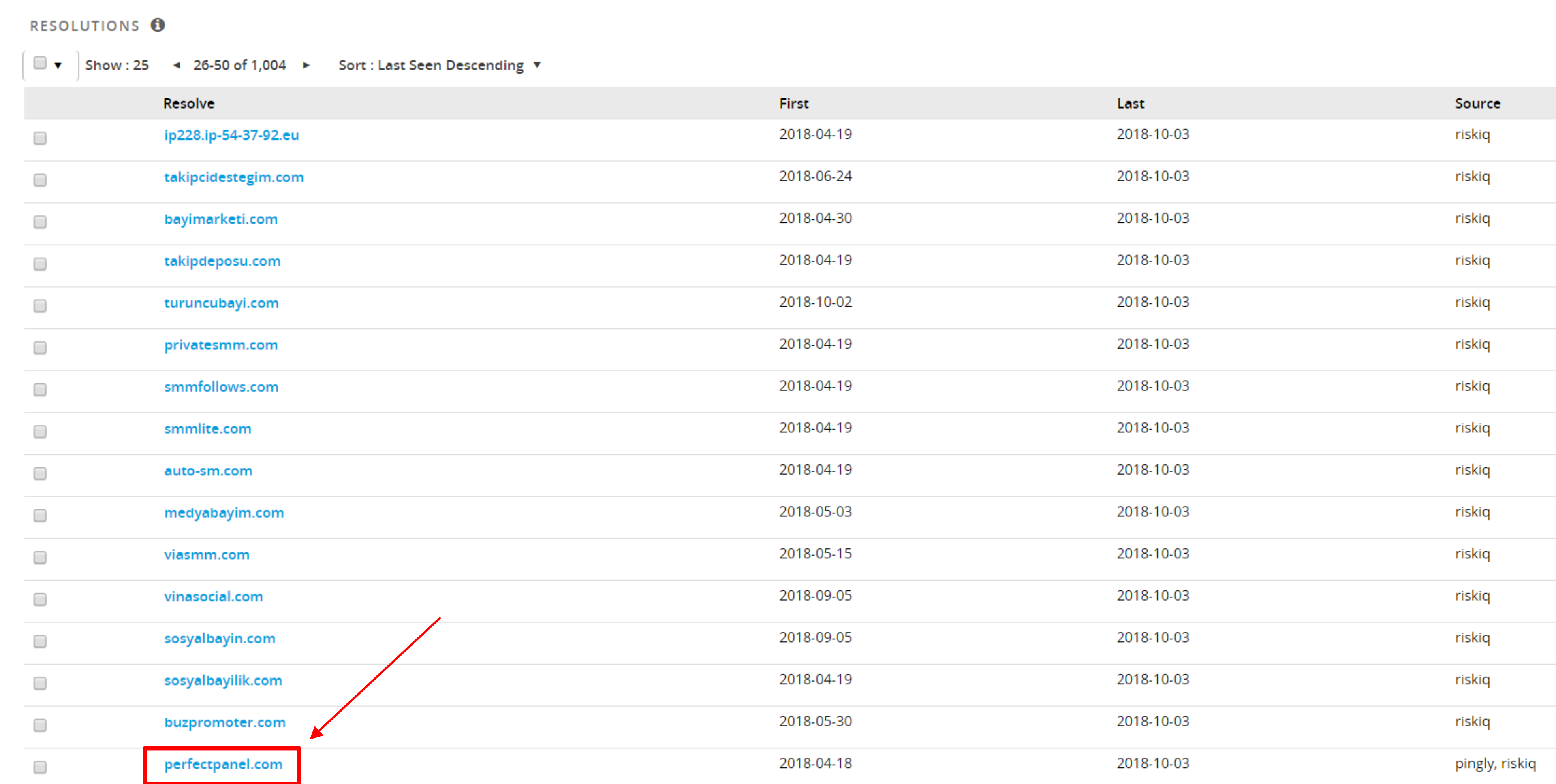
343 panels

- ❑ Fingerprint of the web application
- ❑ Domain registration information
- ❑ IP address
- ❑ HTML content


Gain Instagram Followers within 60 Seconds!
Gain Instagram Followers within 5 Minutes!

2/3 of Dataset

- Coded in PHP
- Used similar combinations of client-side JavaScript libraries
- Hosted on the same IP address belonging to OVH

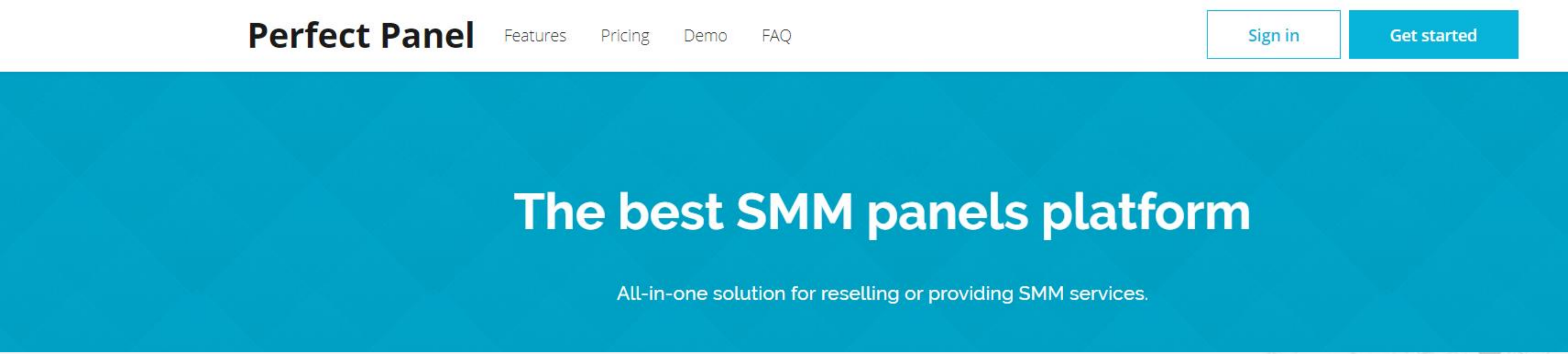


RESOLUTIONS ℹ

☐ ▾ Show : 25 ◂ 26-50 of 1,004 ▸ Sort : Last Seen Descending ▾

	Resolve	First	Last	Source
☐	ip228.ip-54-37-92.eu	2018-04-19	2018-10-03	riskiq
☐	takipcidestegim.com	2018-06-24	2018-10-03	riskiq
☐	bayimarketi.com	2018-04-30	2018-10-03	riskiq
☐	takipdeposu.com	2018-04-19	2018-10-03	riskiq
☐	turuncubayi.com	2018-10-02	2018-10-03	riskiq
☐	privatesmm.com	2018-04-19	2018-10-03	riskiq
☐	smmfollows.com	2018-04-19	2018-10-03	riskiq
☐	smmlite.com	2018-04-19	2018-10-03	riskiq
☐	auto-sm.com	2018-04-19	2018-10-03	riskiq
☐	medyabayim.com	2018-05-03	2018-10-03	riskiq
☐	viasmm.com	2018-05-15	2018-10-03	riskiq
☐	vinasocial.com	2018-09-05	2018-10-03	riskiq
☐	sosyalbayin.com	2018-09-05	2018-10-03	riskiq
☐	sosyalbayilik.com	2018-04-19	2018-10-03	riskiq
☐	buzpromoter.com	2018-05-30	2018-10-03	riskiq
☐	perfectpanel.com	2018-04-18	2018-10-03	pingly, riskiq

The Software Panel Seller

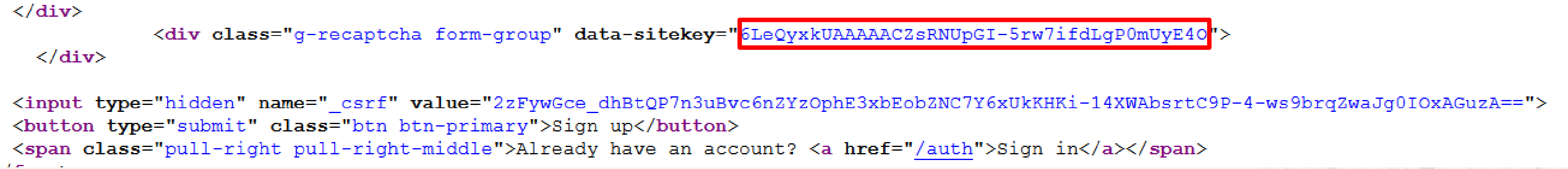


The best SMM panels platform

All-in-one solution for reselling or providing SMM services.

Confirm Hypothesis

On 17 July 2018, 486 websites were up and were accepting signups (out of the 977 domains hosted on the OVH IP address), and from them, 99% used the same reCAPTCHA SiteKey



```
</div>
            <div class="g-recaptcha form-group" data-sitekey="6LeQyxkUAAAAACZsRNUpGI-5rw7ifdLgP0mUyE4O">
  </div>

<input type="hidden" name="_csrf" value="2zFywGce_dhBtQP7n3uBvc6nZYzOphE3xbEobZNC7Y6xUkKHKi-14XWAbsrtC9P-4-ws9brqZwaJg0IOxAGuzA==">
<button type="submit" class="btn btn-primary">Sign up</button>
<span class="pull-right pull-right-middle">Already have an account? <a href="/auth">Sign in</a></span>
```

GoSecure CounterTack

Service

All in one solution :

- Ready to go software
- Provides web hosting
- You only need a domain name

Features:

- API to receive orders
- API to send orders
- Track your workers

Montly price based on the number of orders made, ranging from $50 up to $200 per month.

The Enigma

- How a panel connects itself to the Linux/Moose IoT botnet?

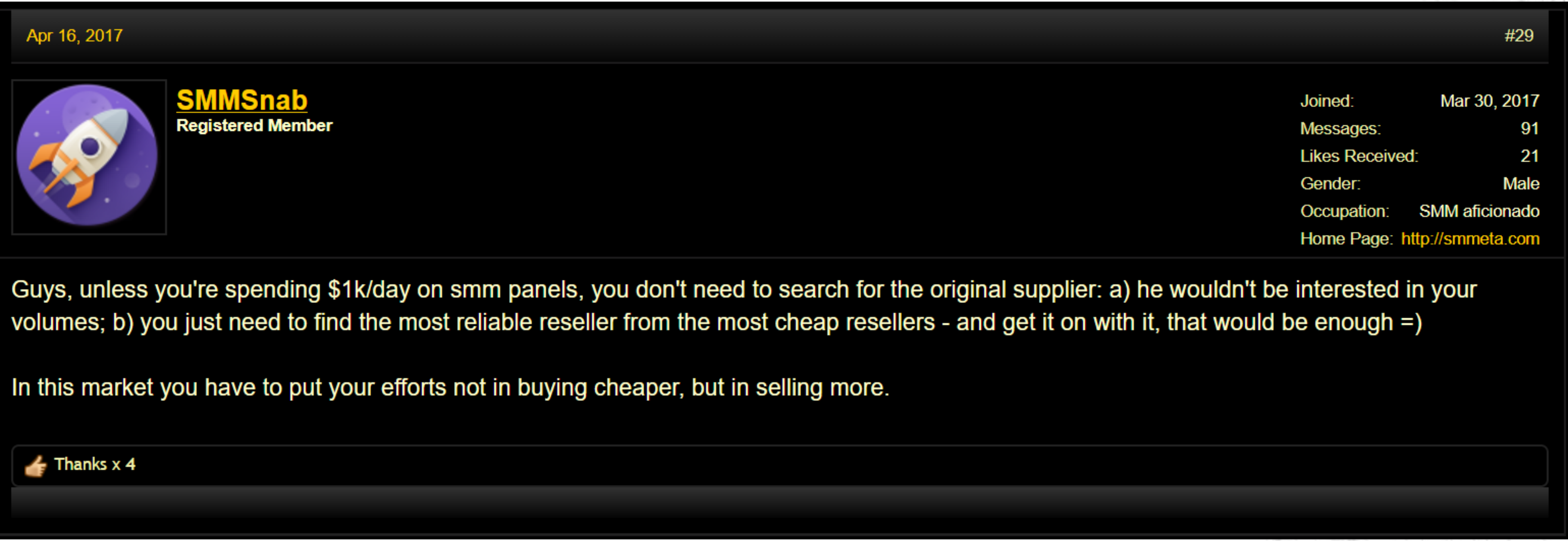
Two possibilities:

- The fat client fetches the orders by itself
- RDP tunnel is created between the client (e.g. OVH IP) and the whitelisted IP address servers

Black Hat World
BlackHat Seo Forum

Even owners of reseller panels seem to have a hard time finding a main provider!

Finding the Main Provider



Apr 16, 2017 #29

SMMSnab
Registered Member

Joined:	Mar 30, 2017
Messages:	91
Likes Received:	21
Gender:	Male
Occupation:	SMM aficionado
Home Page:	http://smmeta.com

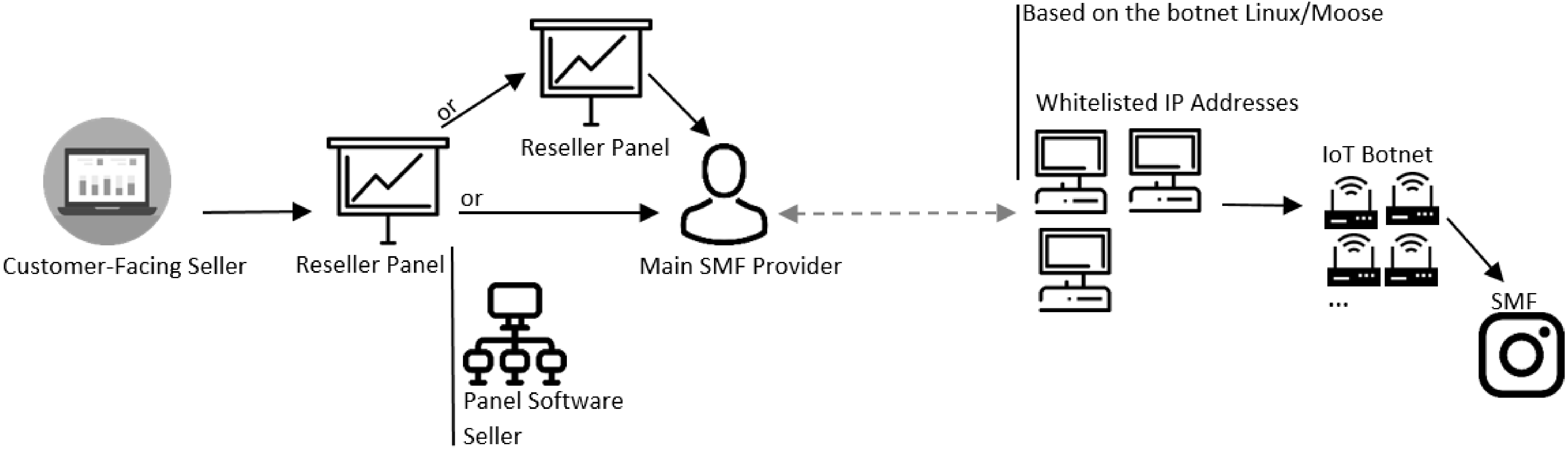
Guys, unless you're spending $1k/day on smm panels, you don't need to search for the original supplier: a) he wouldn't be interested in your volumes; b) you just need to find the most reliable reseller from the most cheap resellers - and get it on with it, that would be enough =)

In this market you have to put your efforts not in buying cheaper, but in selling more.

Thanks x 4

GoSecure CounterTack

Social Media Fraud Supply Chain



Revenue Division in the Chain

	Customer-Facing Websites	Reseller Panels
Medium Price for 1,000 followers on Instagram	$ 13	$ 1

Customer-facing sellers: 92% of profit margin (if no other costs incurred)
Reseller panel owners: $1 per 1,000 followers
Main SMF provider: Revenue < $1 per 1,000 followers

Thank you !

Questions?

@masarahclouston

✉ mcpc@gosecure.ca