RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SEM-M03C

The Industry of Social Network Manipulation: from Botnets to Hucksters

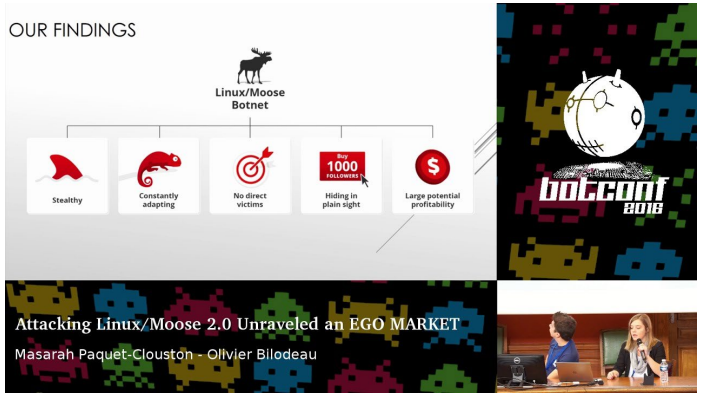
Masarah Paquet-Clouston
Cybersecurity Researcher
GoSecure CounterTack
@masarahclouston

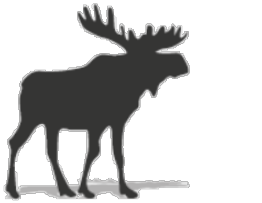
Olivier Bilodeau
Cybersecurity Research Lead
GoSecure CounterTack
@obilodeau

RSAConference2019

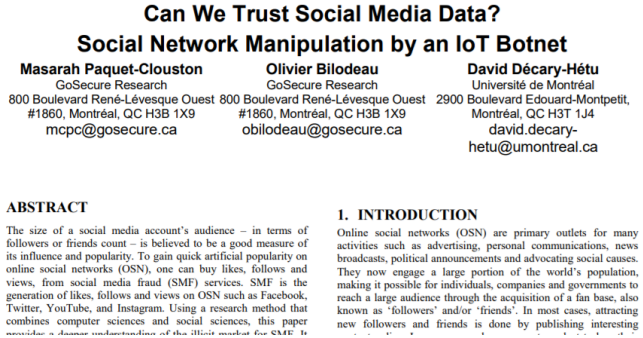
Research Context

From 2016 to 2018…





Linux/Moose Botnet



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

Research Context

New York Attorney General to Investigate Firm That Sells Fake Followers

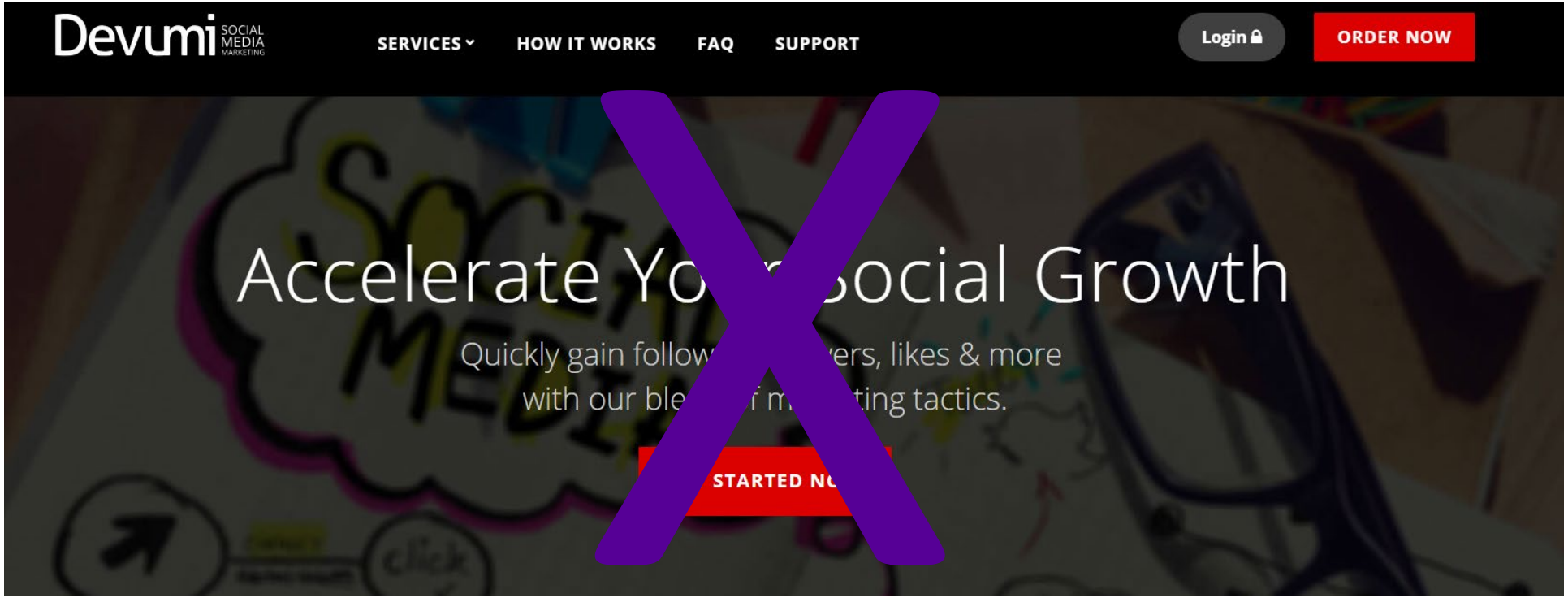
By Nicholas Confessore

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.)



We thought…

Targeting Devumi!

There is so much more behind this industry

RSAConference2019

The Beginning: Uncovering a Provider of Social Media Fraud

A short recap

The Main Providers

Linux/Moose

An IoT botnet that conducts social media fraud

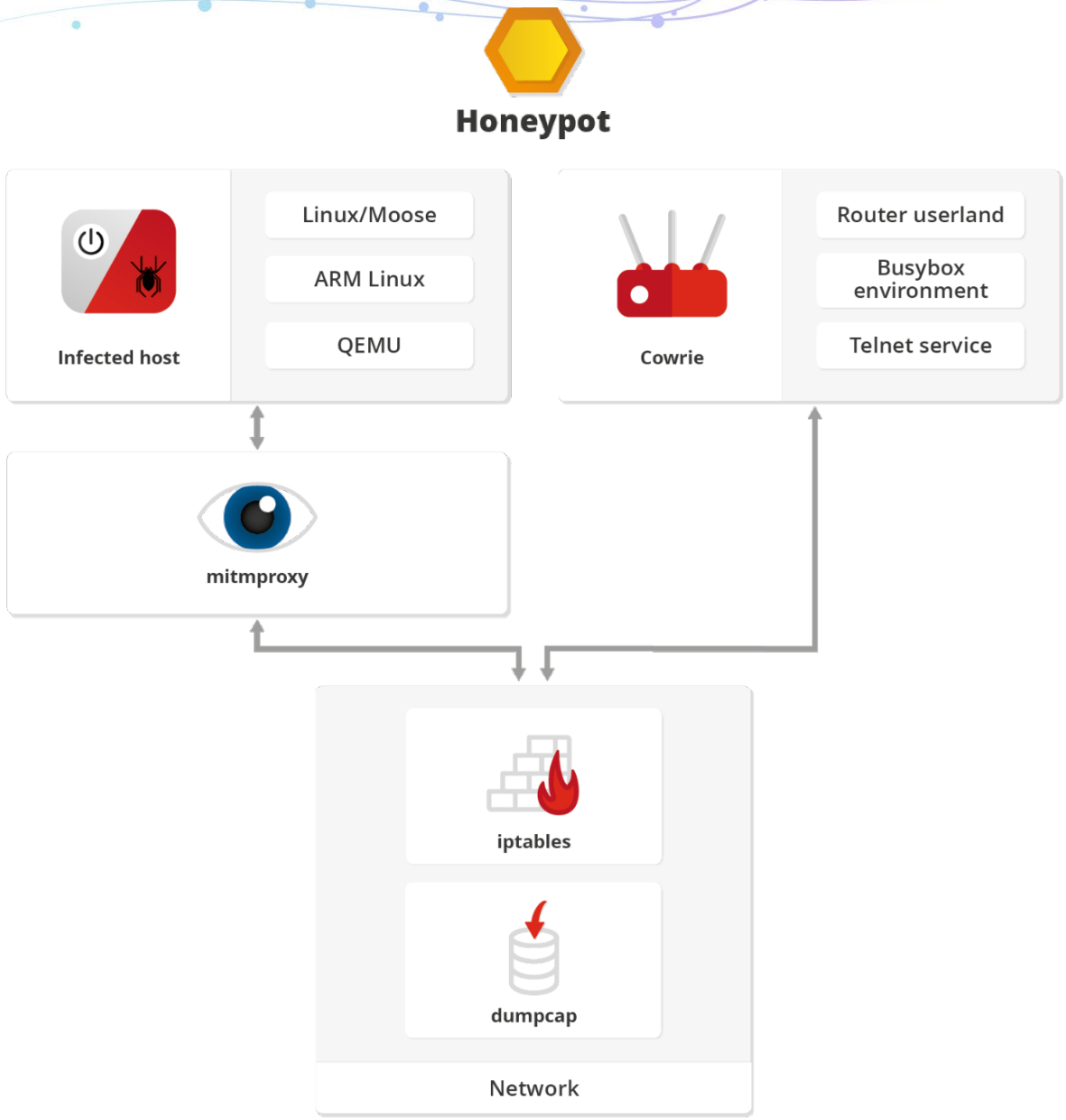
Recap of Linux/Moose

- 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)

Catching Linux/Moose

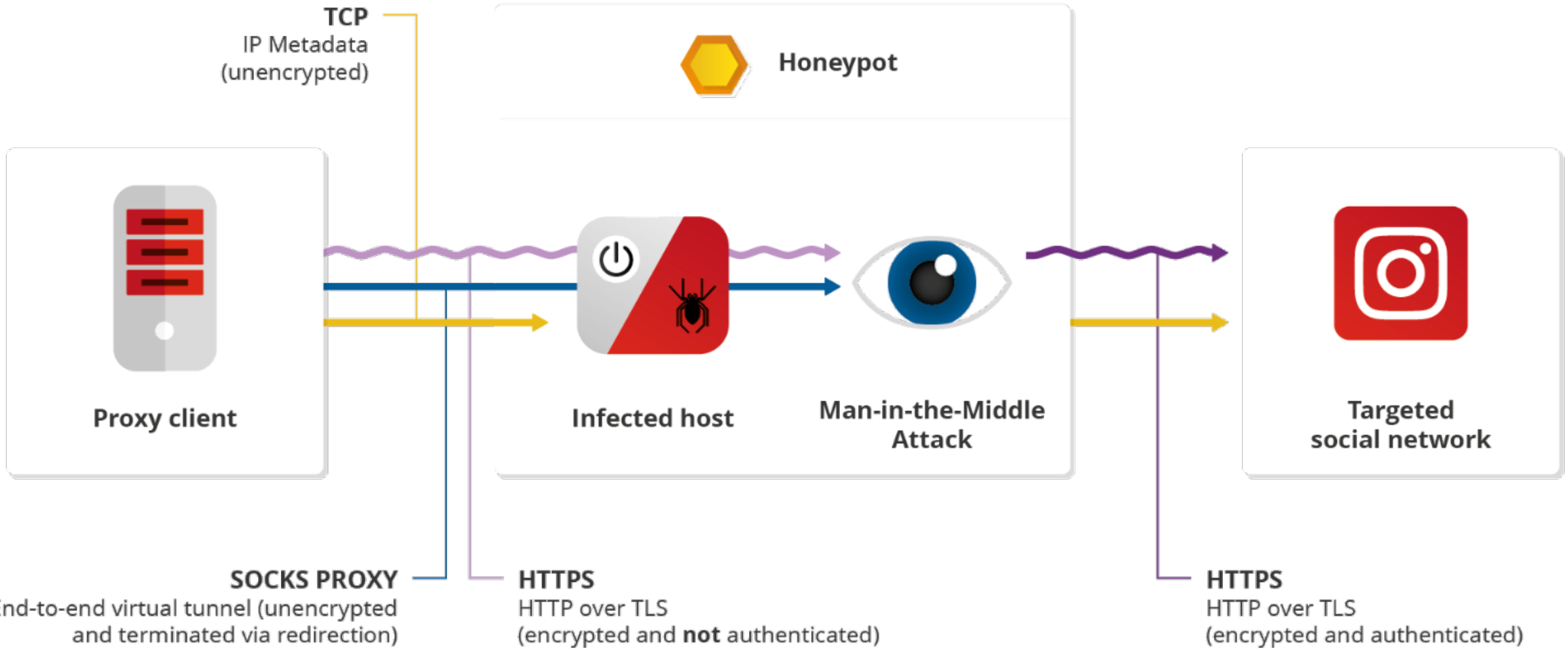
Using Honeypots

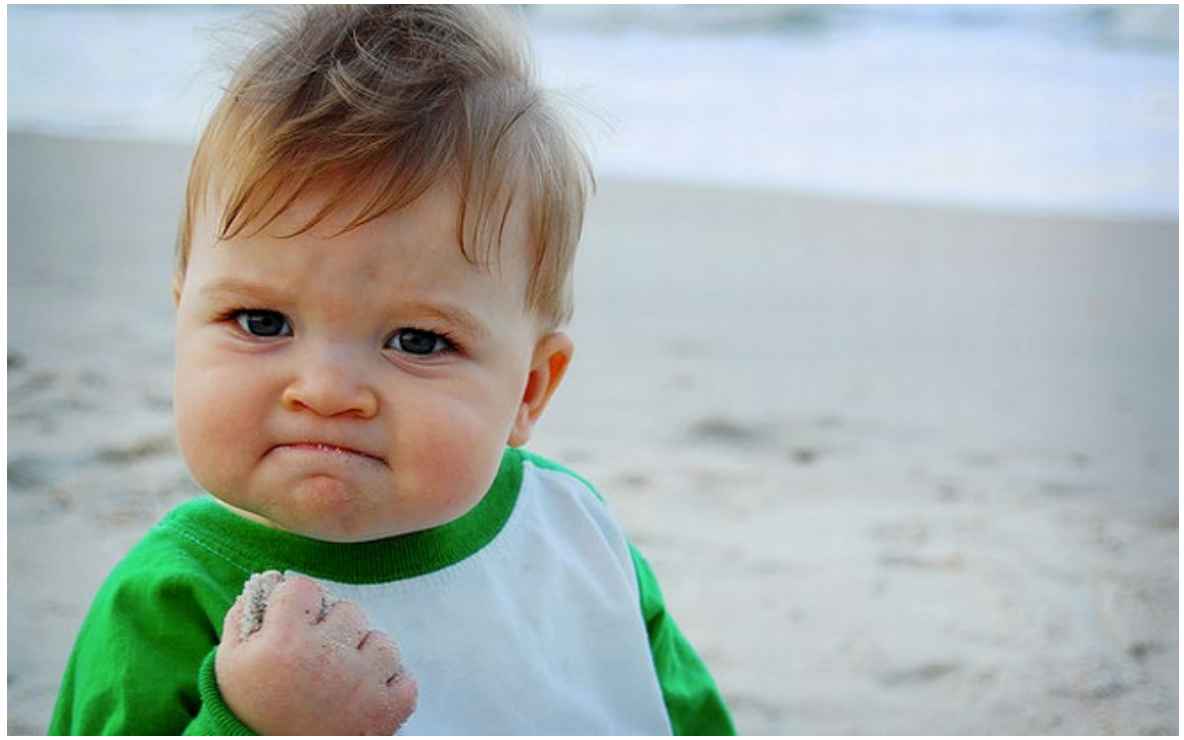
- Software-based
- Low interaction
- Side-loaded an ARM virtual machine
  - Which we infected



Linux/Moose Honeypots

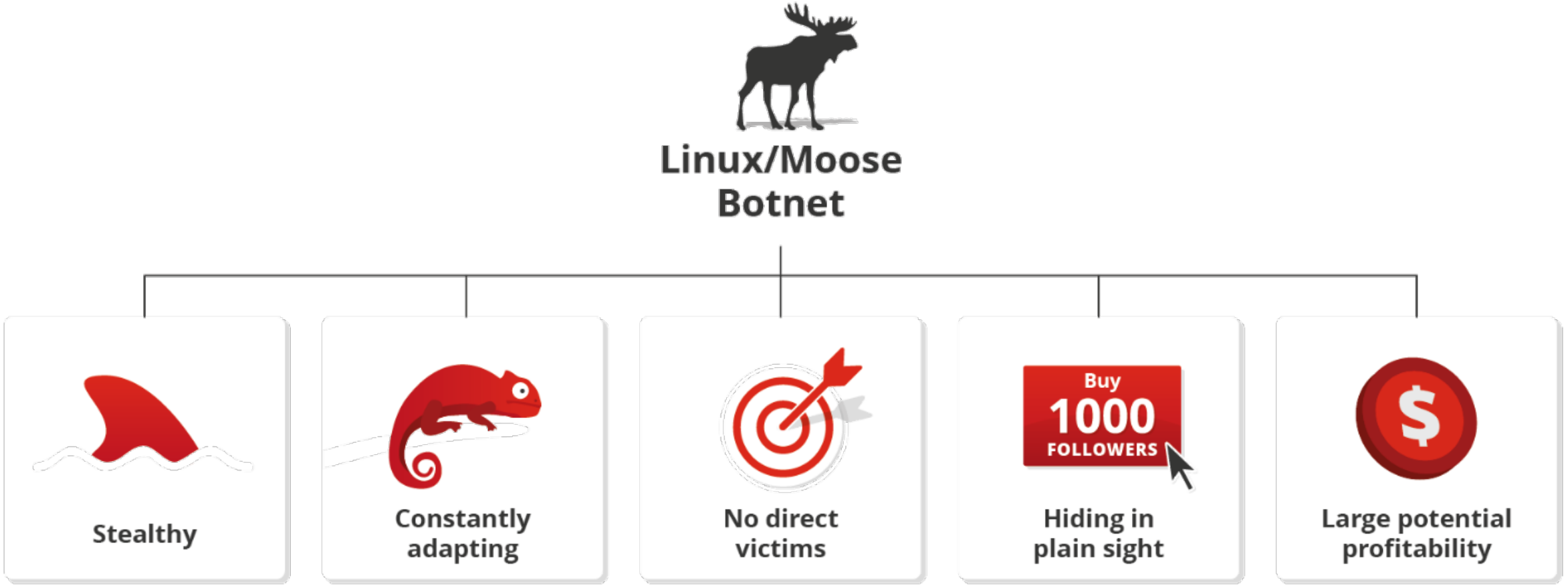
HTTPS Man-in-the-Middle (MITM) Attack





Accessed the raw traffic

At the time…


Linux/Moose Botnet
Stealthy
Constantly adapting
No direct victims
Buy 1000 FOLLOWERS
Hiding in plain sight
Large potential profitability

RSAConference2019

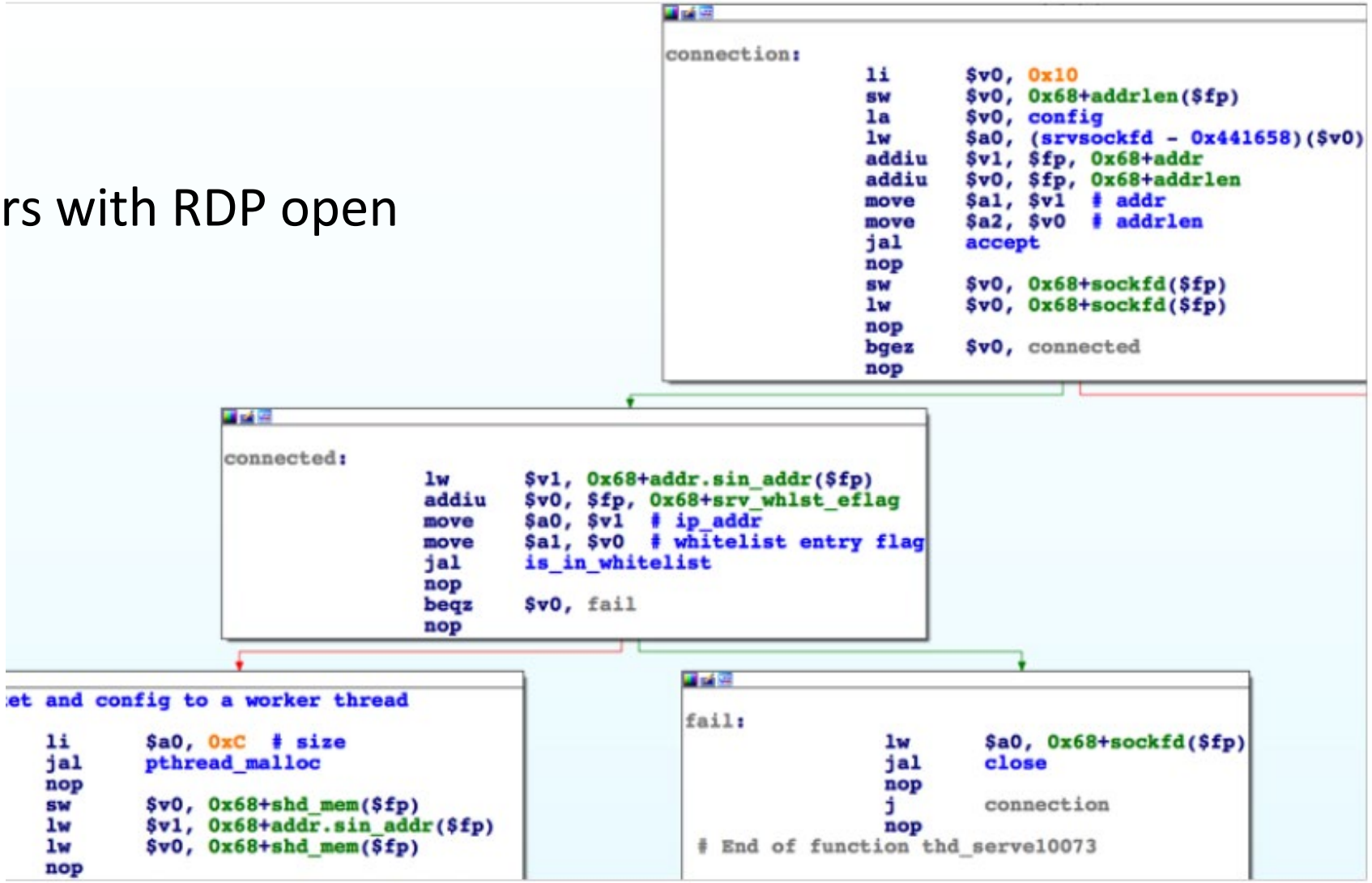
Whitelisted IP Addresses

The Untold Feature of Linux/Moose

Untold Feature of Linux/Moose

Seven whitelisted IPs

- Seven Windows Servers with RDP open
- Reseller model?

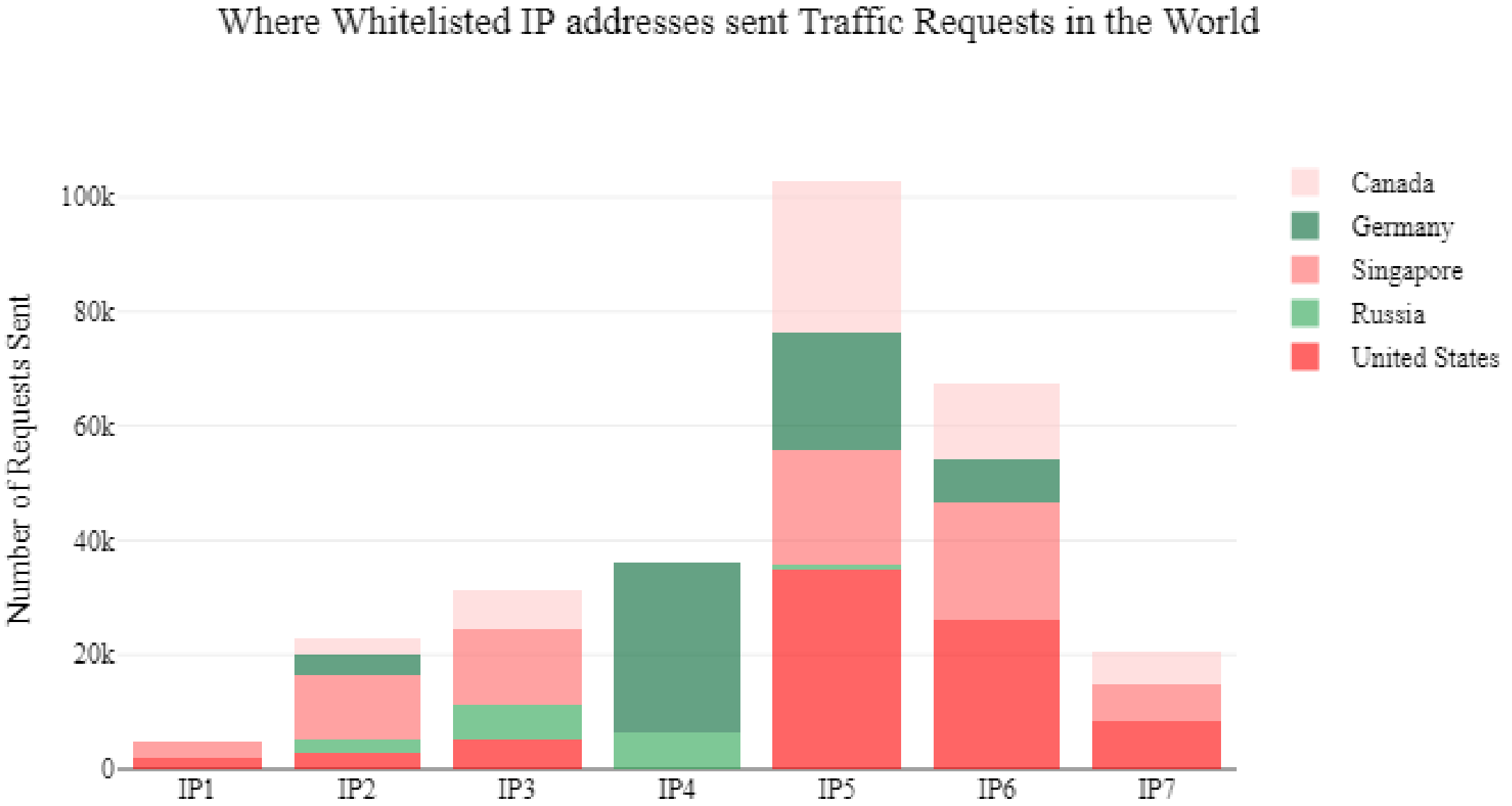


Testing the Reseller Model Hypothesis

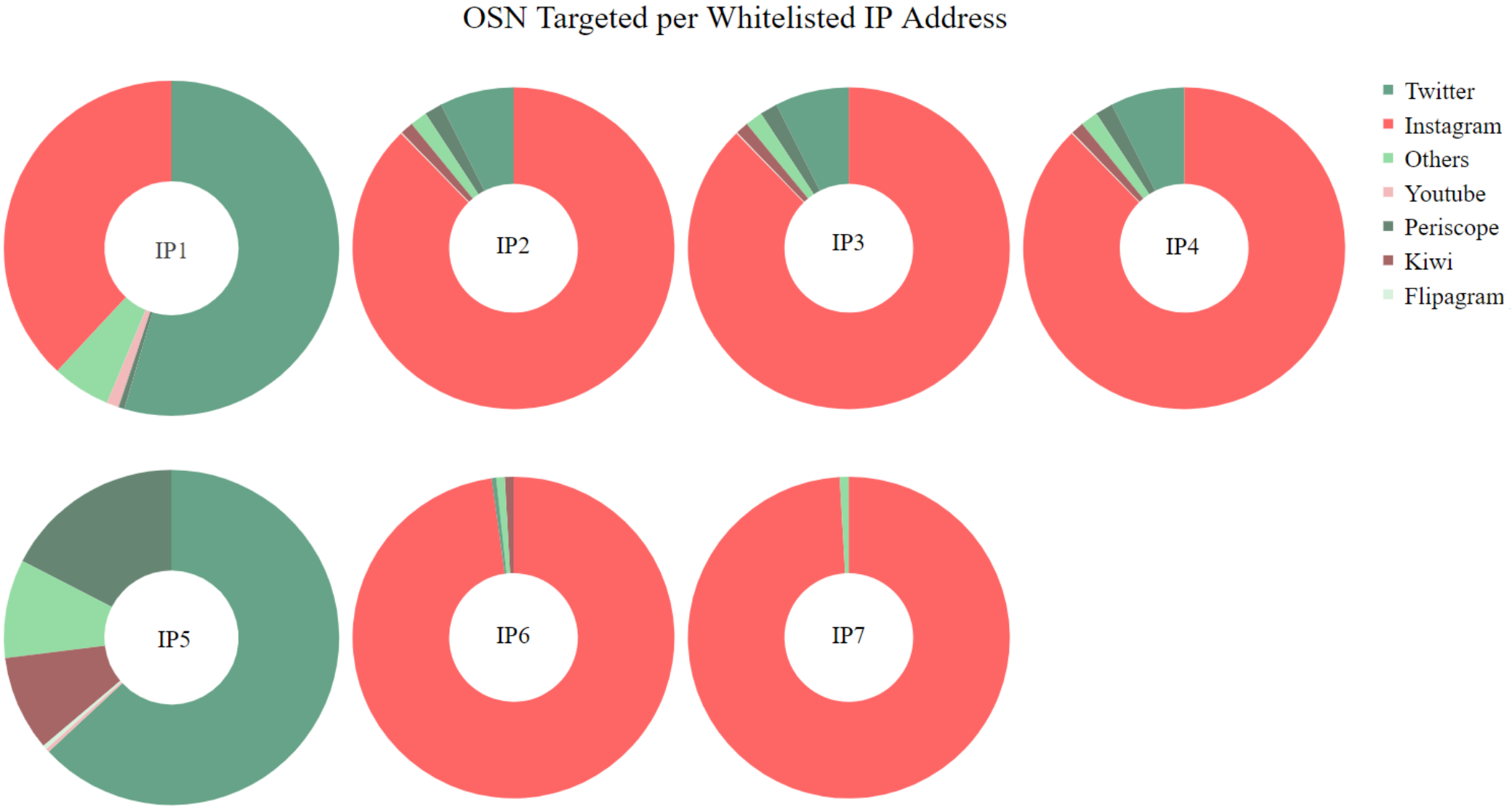
Investigate similarities in traffic sent by each whitelisted IP based on these variables:

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

Honeypots Used



Websites Targeted



Other Options

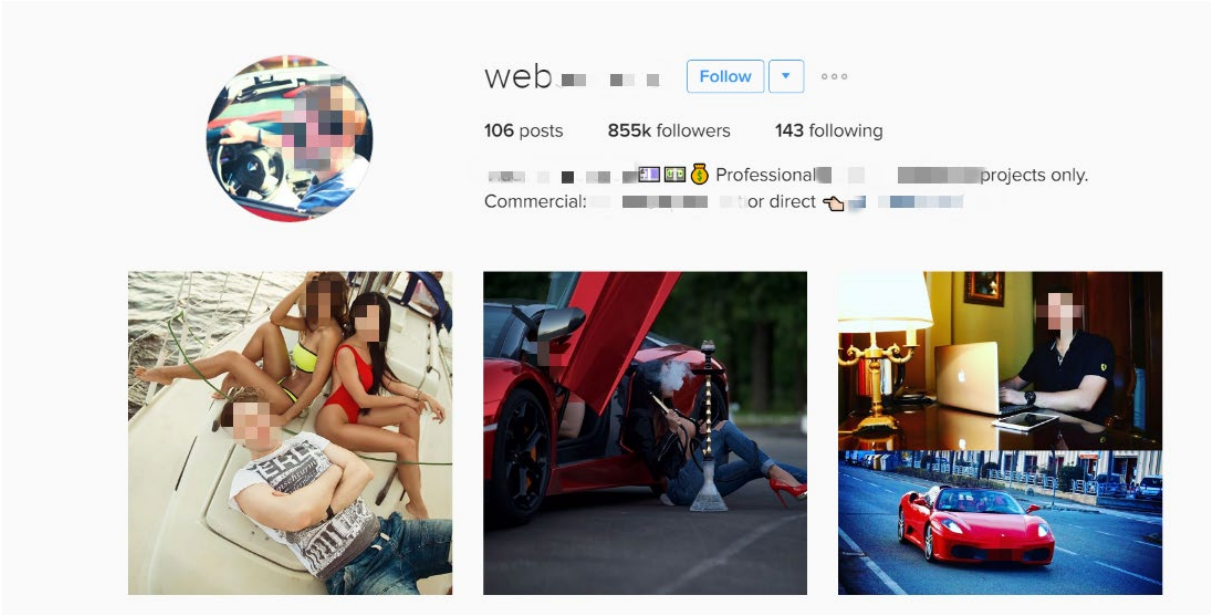
- TLS fingerprinting
  - Lee Brotherston's TLS Fingerprinting project
  - Salesforces' JA3 project
- User agents
- API calls

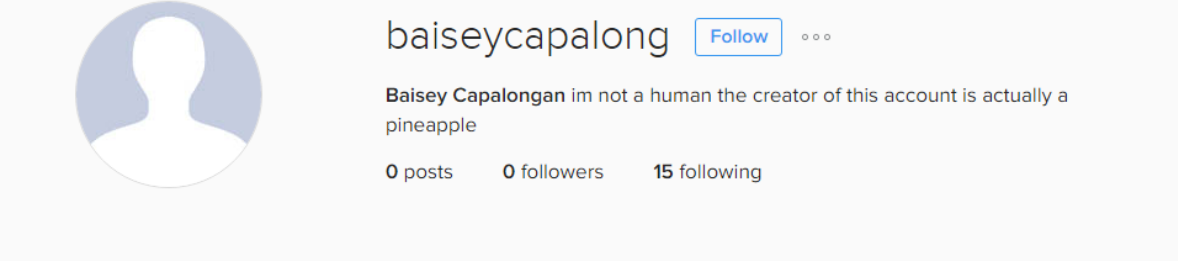
Accounts Created and Accounts Followed

Different whitelisted IPs followed the same accounts →

AND

List of fake accounts per whitelisted IP →

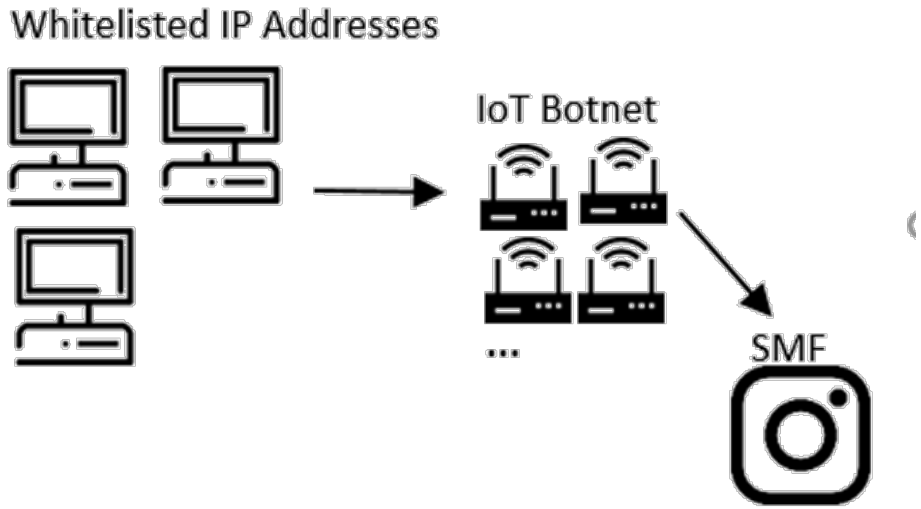




Purpose of the Whitelisted IPs

Fake account management!

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



RSAConference2019

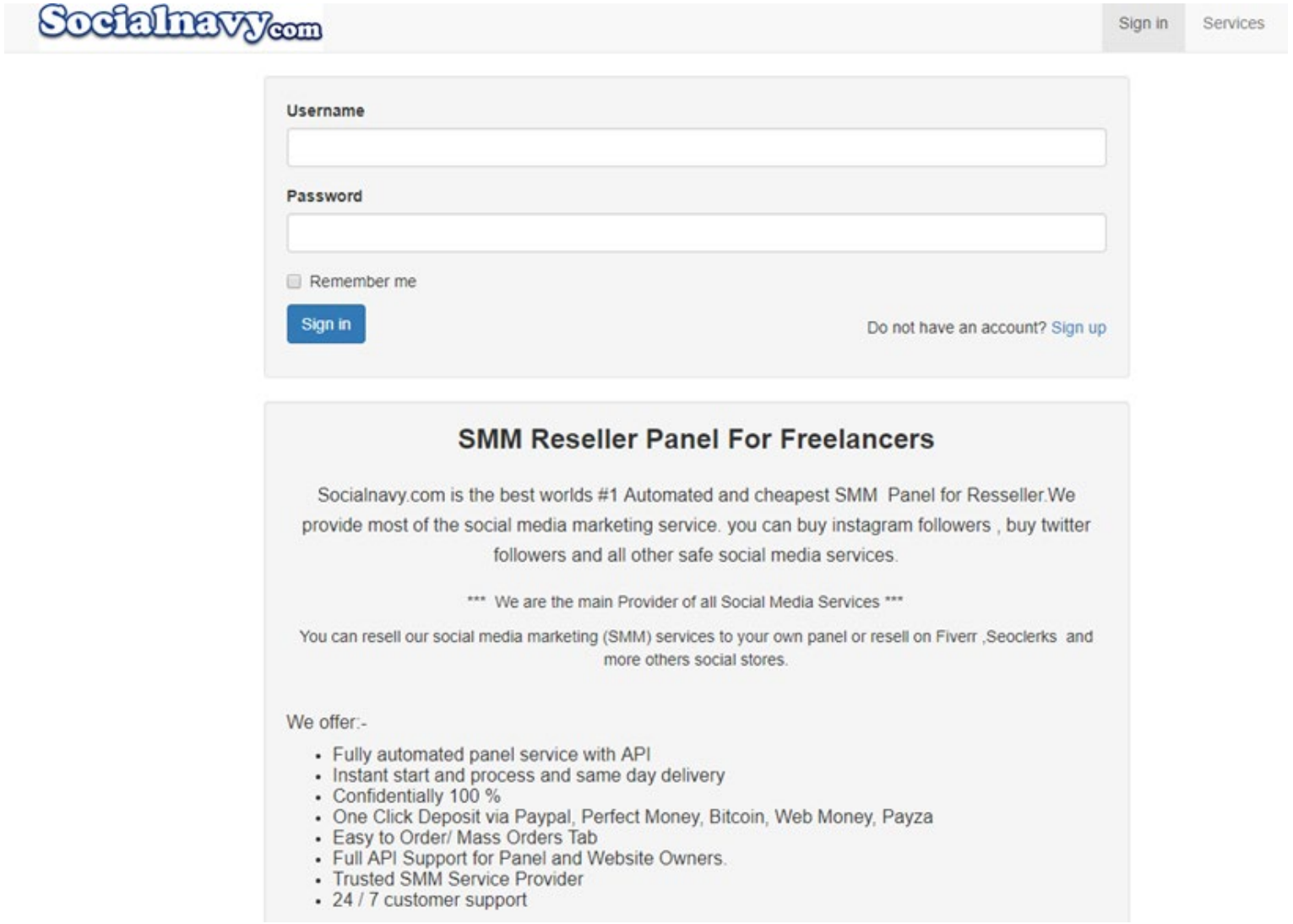
Moving on to Bulk Reseller Panels

Bulk Reseller Panels

Found in the decrypted traffic: reseller panels

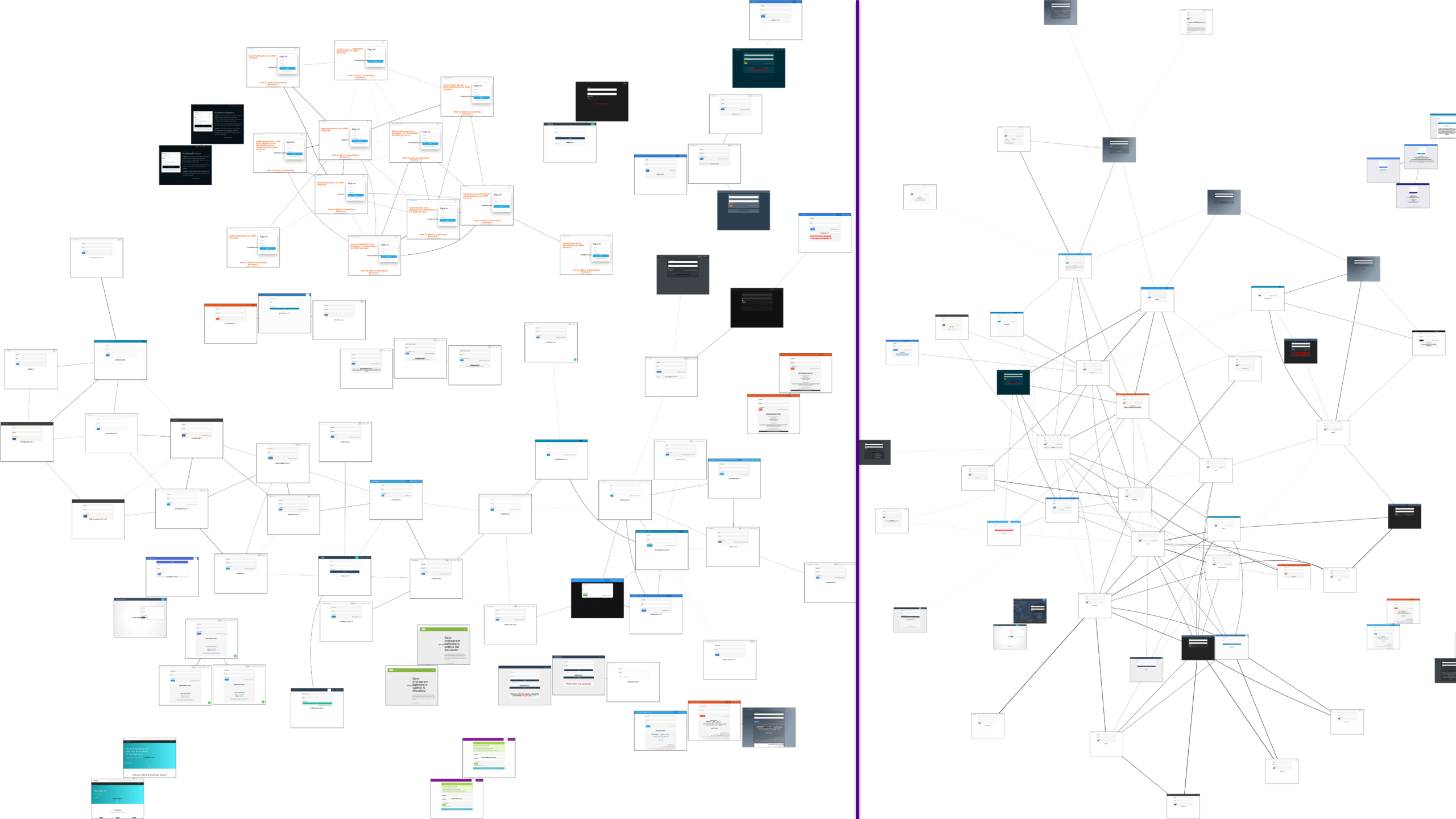
```
<HTTPFlow
  request = Request(GET 173.252.91.17:443/medianesia.panel/)
  response = Response(200 OK, text/html, 4.43kB)>
[redacted]
{   'client_conn': {   'address': {   'address': ([redacted],
                                      'use_ipv6': False},
                       'clientcert': None,
 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

Bulk Reseller Panels



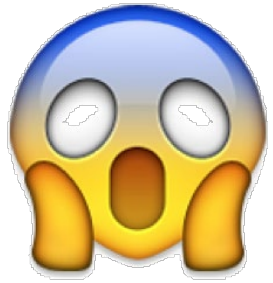
Reseller Panels (N=343)

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



2/3 of the Dataset

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



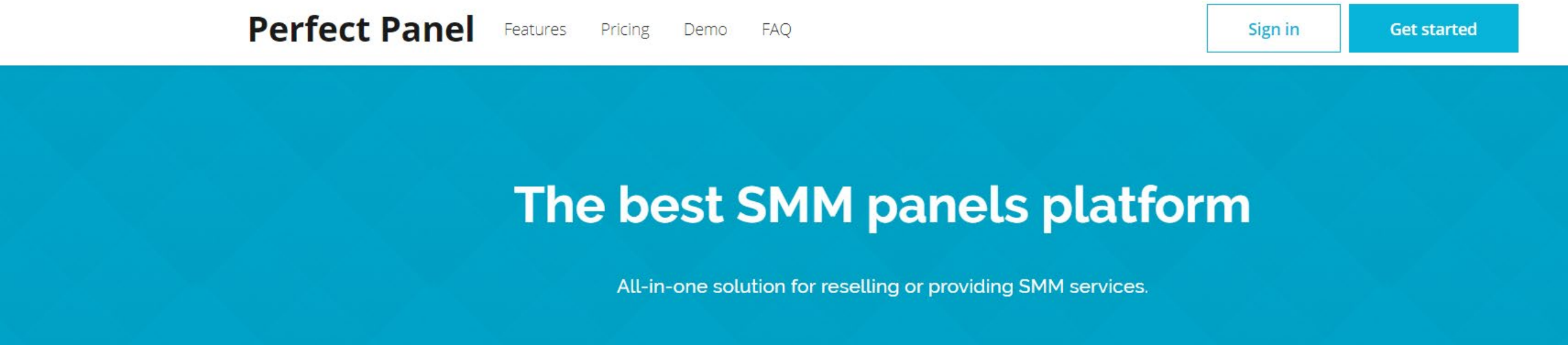
OVH IP

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

RSAConference2019

Introducing Software Panel Sellers

The Software Panel Seller



Service

All in one solution :

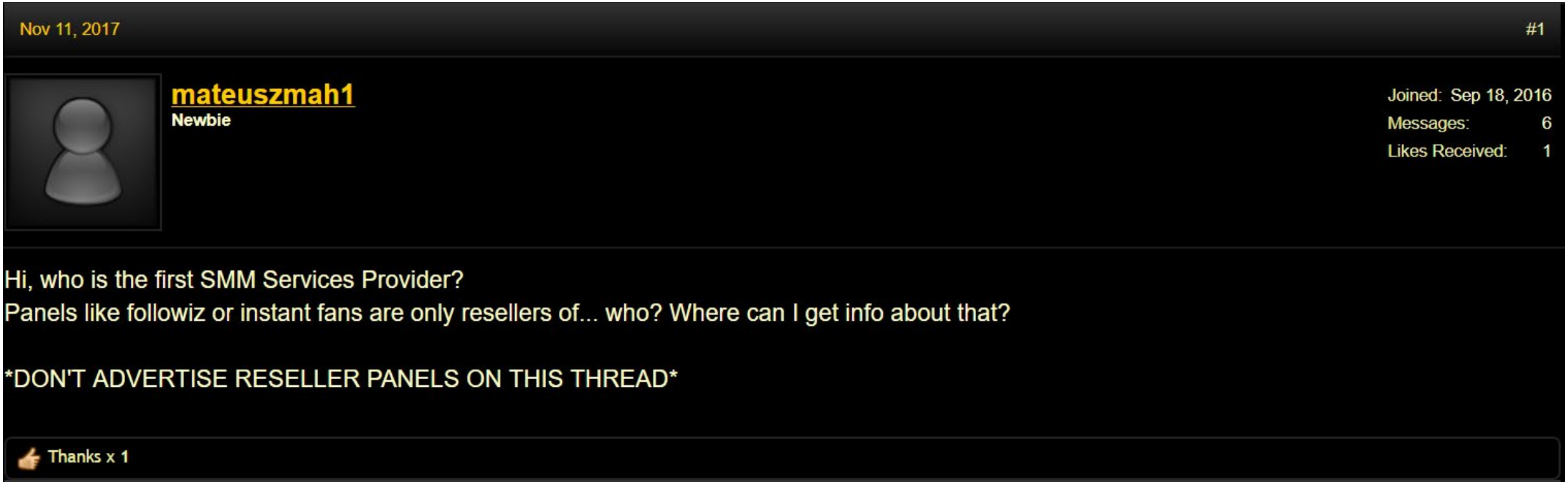
- Ready to go software
- Provides web hosting
- You only need a domain name

Features:

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

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

Finding the Main Provider



Nov 11, 2017 #1

mateuszmah1
Newbie

Joined: Sep 18, 2016
Messages: 6
Likes Received: 1

Hi, who is the first SMM Services Provider?
Panels like followiz or instant fans are only resellers of... who? Where can I get info about that?

DON'T ADVERTISE RESELLER PANELS ON THIS THREAD

Thanks x 1

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

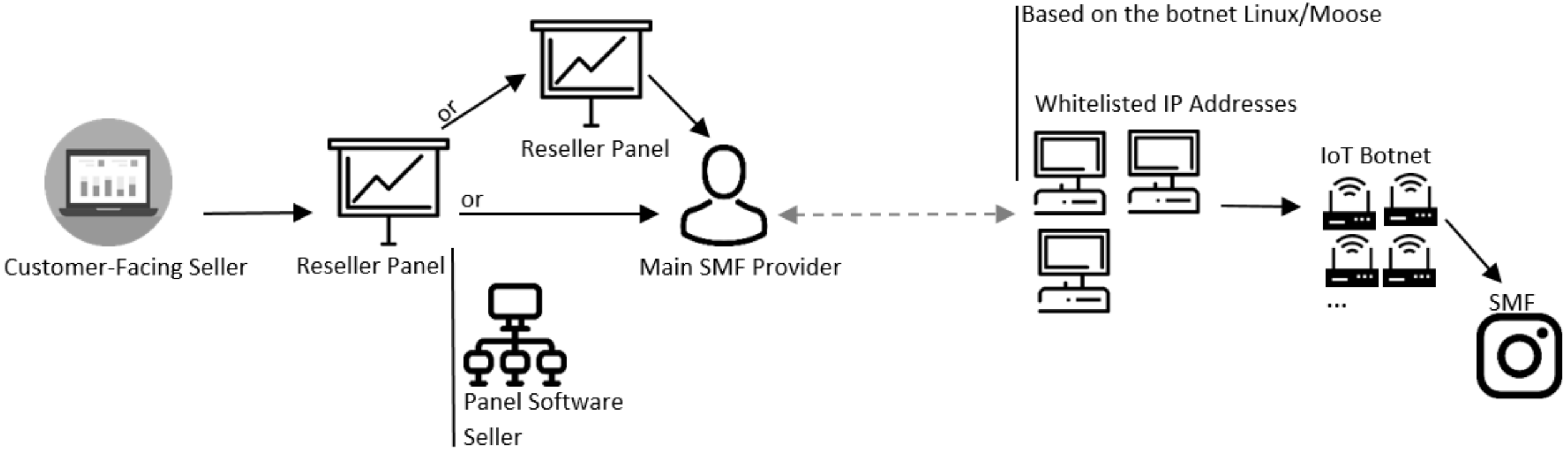
Guys, unless you're spending $1k/day on smm panels, you don't need to search for the original supplier: a) he wouldn't be interested in your volumes; b) you just need to find the most reliable reseller from the most cheap resellers - and get it on with it, that would be enough =)

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

Thanks x 4

Summary

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

Key Takeaways

- This study goes from malware analysis to market ecosystem understandings
- We find that botnets are at the end of the supply chain: many actors are involved in reselling social media fraud
- We conclude that potential targets to disrupt social media fraud are **software panel sellers**

Apply

- **Next week**, you should:
  - Contact NY's Attorney General office and tell them to get in touch with us ;-)
  - Be more skeptical of online popularity
- **Within the next year**, you should:

Educate your family about such threats and ensure other individuals do not only use "followers" as indicators of credibility

RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SEM-M03C

Thank you!
Questions?

Masarah Paquet-Clouston

Cybersecurity Researcher
GoSecure CounterTack
@masarahclouston

Olivier Bilodeau

Cybersecurity Research Lead
GoSecure CounterTack
@obilodeau