

# **RSA**®Conference2019

San Francisco | March 4–8 | Moscone Center



**BETTER.**

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

#RSAC

**RSA**®Conference2019

## Research Context



# Research Context

## *New York Attorney General to Investigate Firm That Sells Fake Followers*

By Nicholas Confessore

Jan. 27, 2018

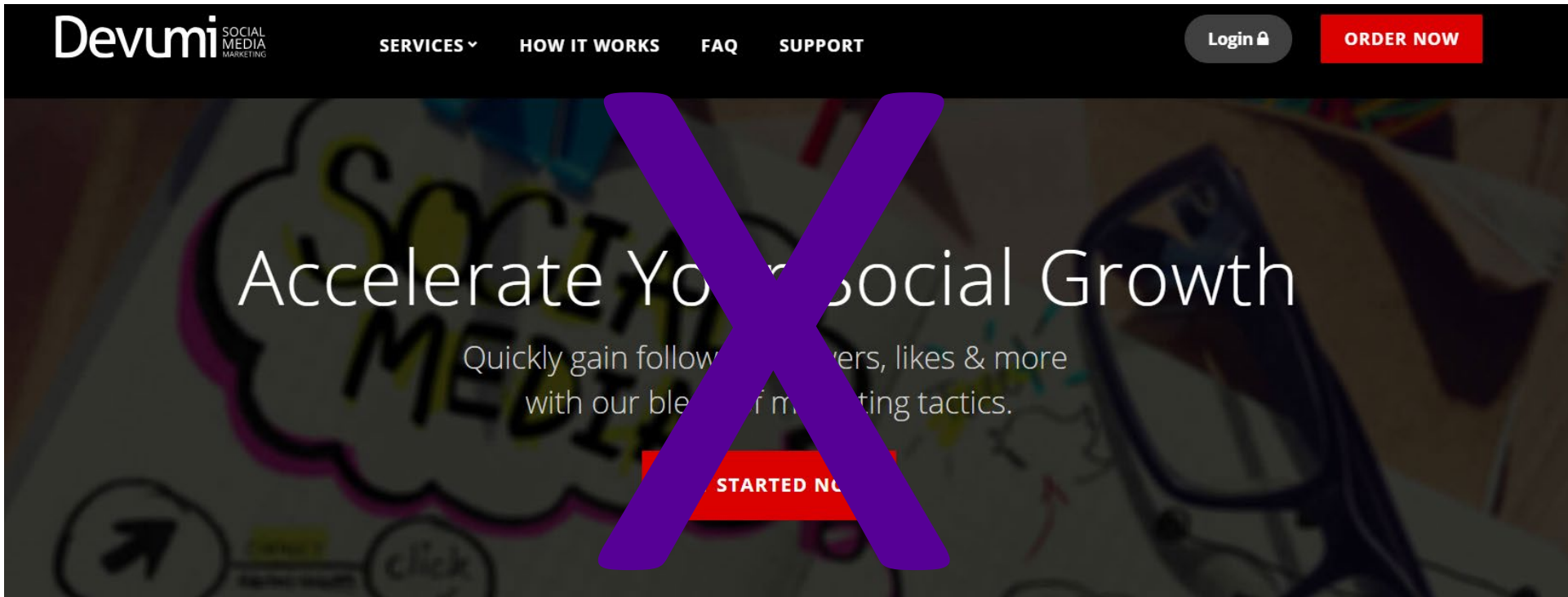


The New York attorney general, Eric T. Schneiderman, on Saturday opened an investigation into a company that sold millions of fake followers on social media platforms, some of them copying real users' personal information.

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 Demuvi!



There is so much more behind this industry

**RSA**®Conference2019

# Uncover the supply chain behind social media fraud

*Main Providers : botnets*



# The Main Providers

## Linux/Moose

An IoT botnet that conducts social media fraud

# Recap of Linux/Moose

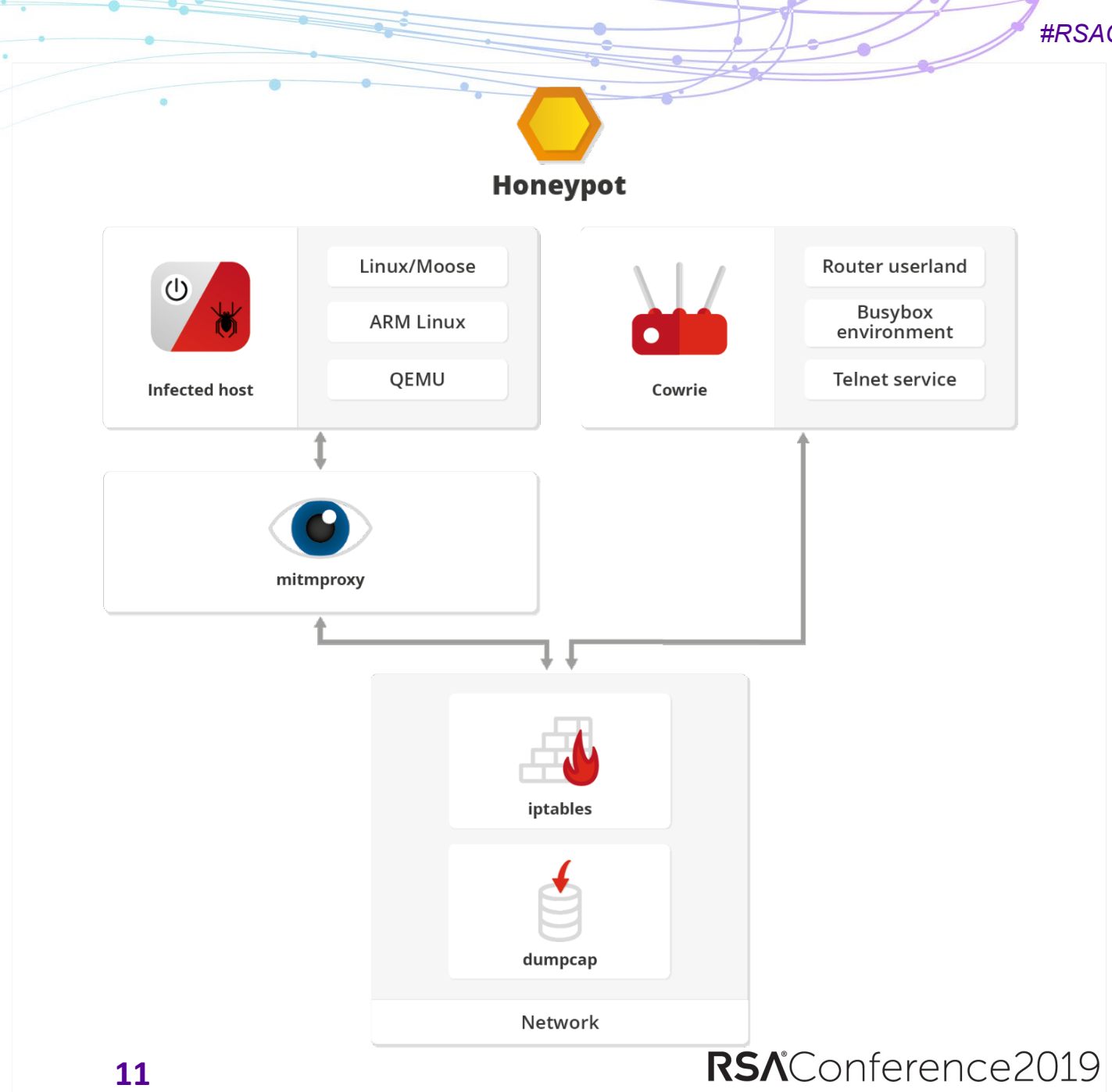
- Affects routers / Internet of Things (IoT)
  - Embedded Linux systems with busybox userland
- Worm-like behavior
  - Telnet credential brute force
- Payload: Proxy service
  - SOCKSv4/v5, HTTP, HTTPS
- Used to proxy traffic to social media sites (mainly Instagram)

LIKE



# Catching Linux/Moose

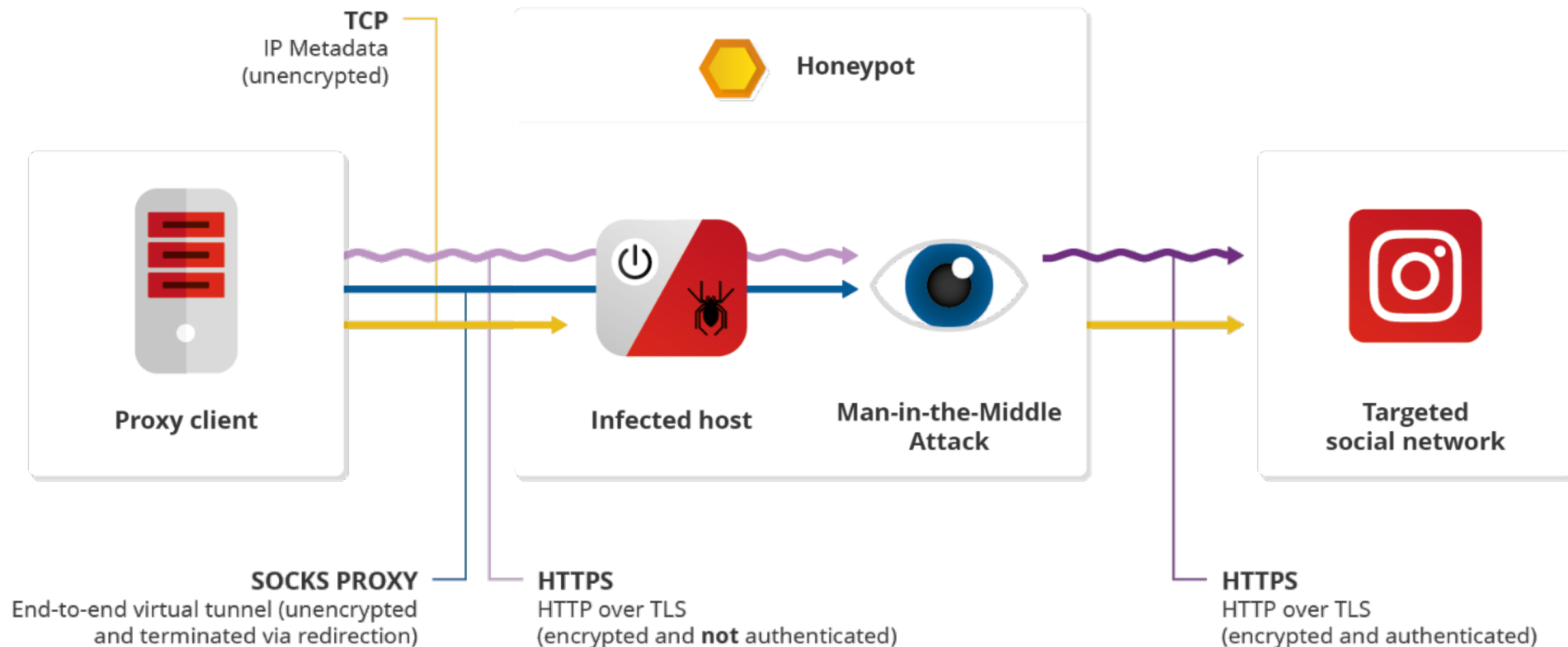
- Software-based
- Low interaction
- Side-loaded an ARM virtual machine
  - Which we infected



# Linux/Moose Honeypots



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



# Investigating Linux/Moose

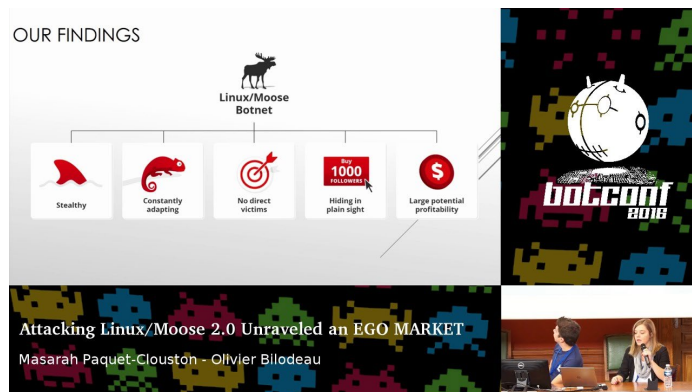
- Built and infected IoT honeypots (10 in 5 countries)
- Conducted a man-in-the-middle-attack



Accessed the raw traffic



# At the time...



## Linux/Moose Botnet

# 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 Olivier Bilodeau

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

<b>Masarah Paquet-Clouston</b> GoSecure Research 800 Boulevard René-Lévesque Ouest #1860, Montréal, QC H3B 1X9 mcpcc@gosecure.ca	<b>Olivier Bilodeau</b> GoSecure Research 800 Boulevard René-Lévesque Ouest #1860, Montréal, QC H3B 1X9 obilodeau@gosecure.ca	<b>David Décary-Héту</b> Université de Montréal 2900 Boulevard Édouard-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 provides a deeper understanding of the illicit market for SMF.

#### 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

**RSA**®Conference2019

# The Untold Feature of Linux/Moose

*Whitelisted IP addresses*



# Untold Feature of Linux/Moose

## Seven whitelisted IPs

- Reseller model?



# Testing the Reseller Model Hypothesis

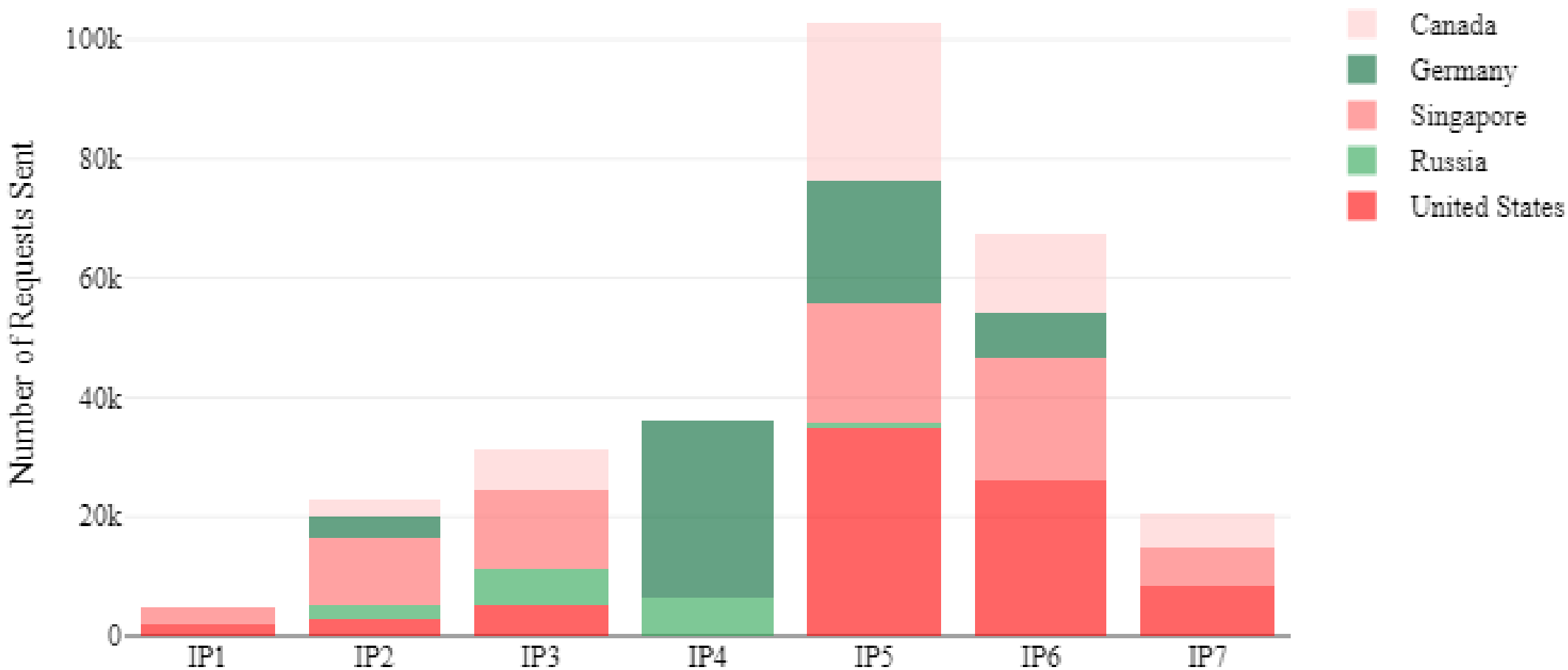
*Investigate similarities in traffic sent by each whitelisted IP based on these variables:*

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



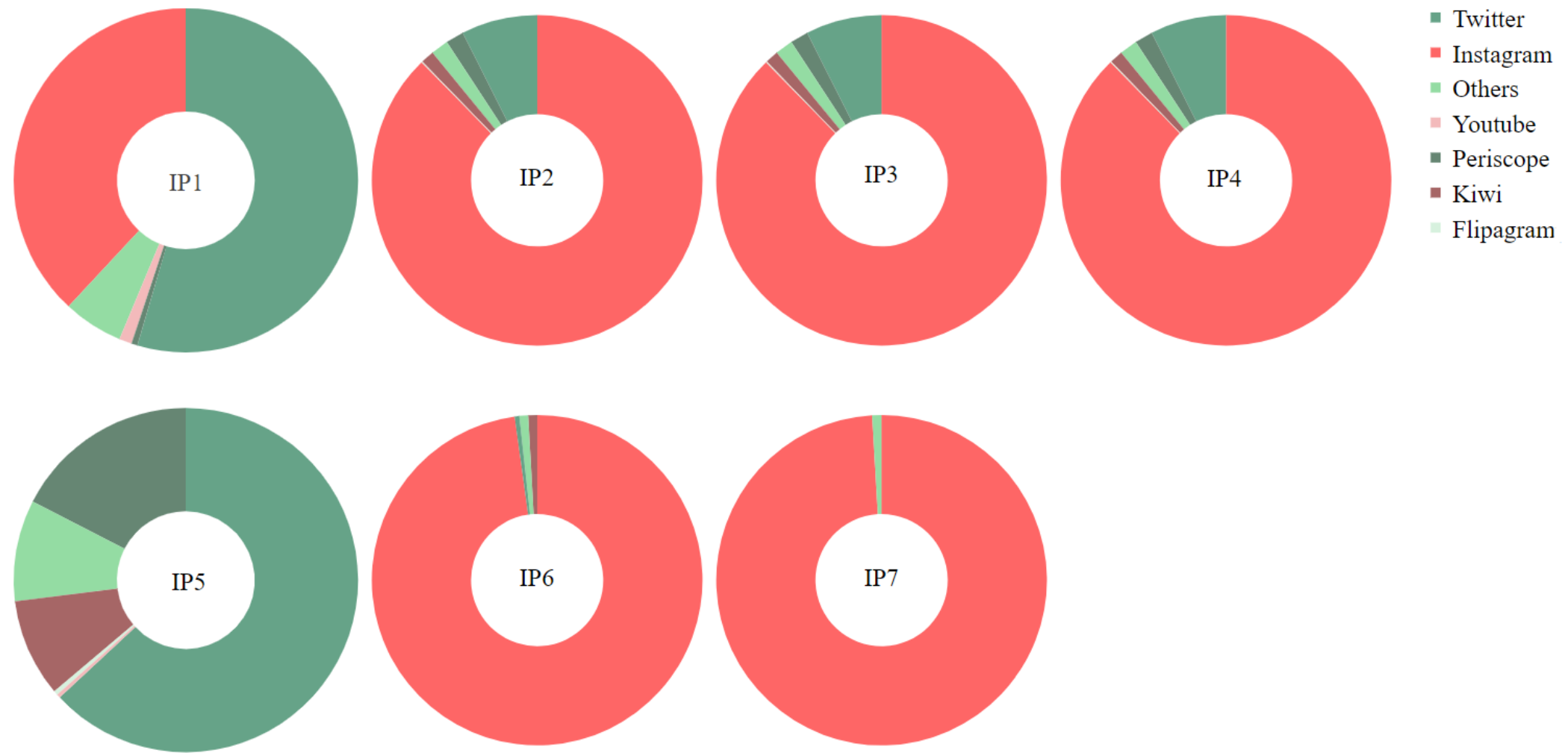
# Honeypots Used

Where Whitelisted IP addresses sent Traffic Requests in the World



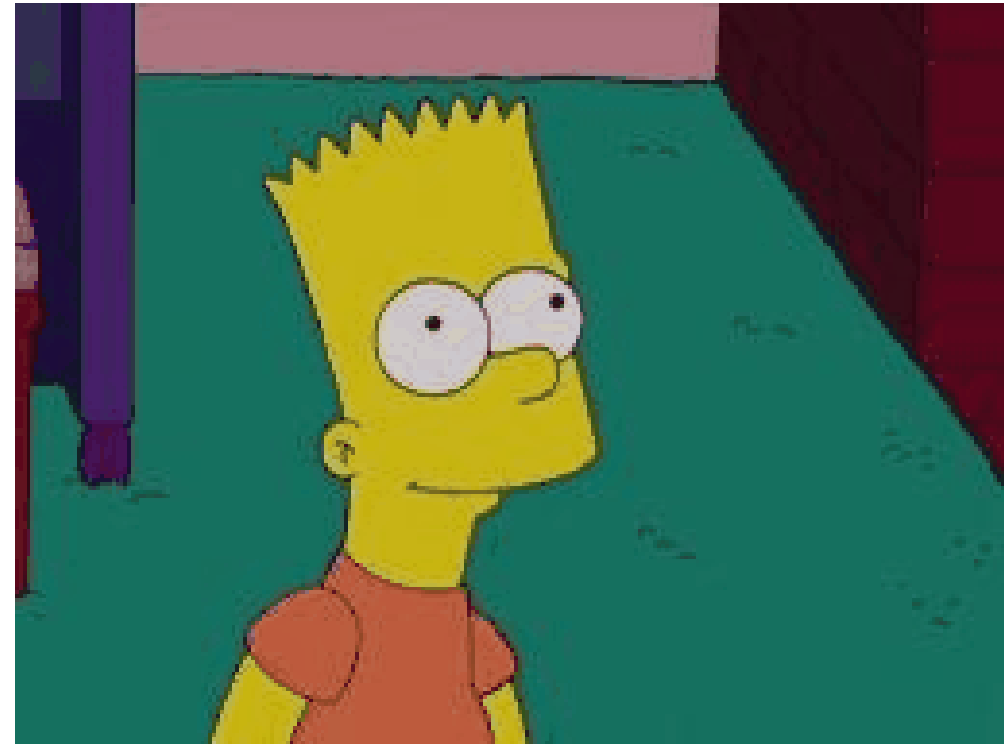
# Websites Targeted

OSN Targeted per Whitelisted IP Address



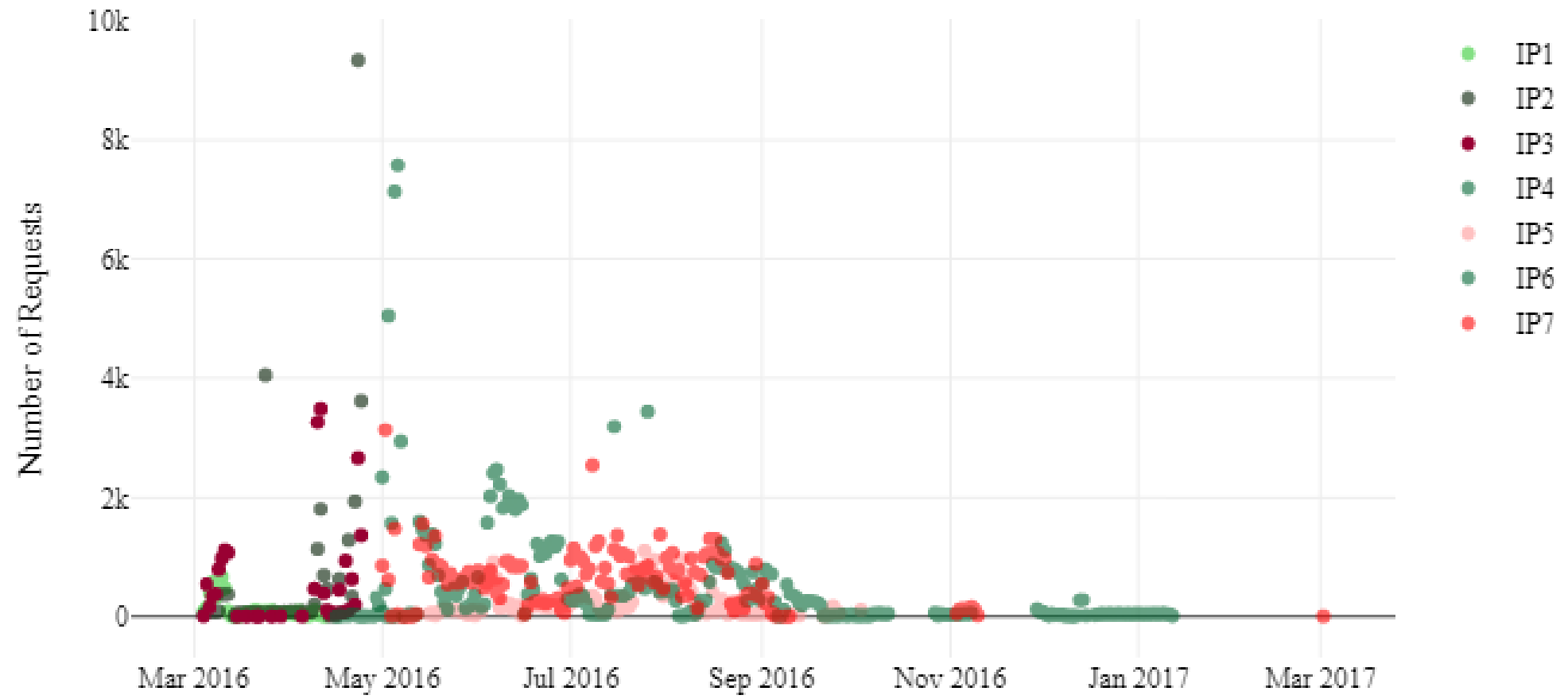
# Other Options

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



# Timestamps

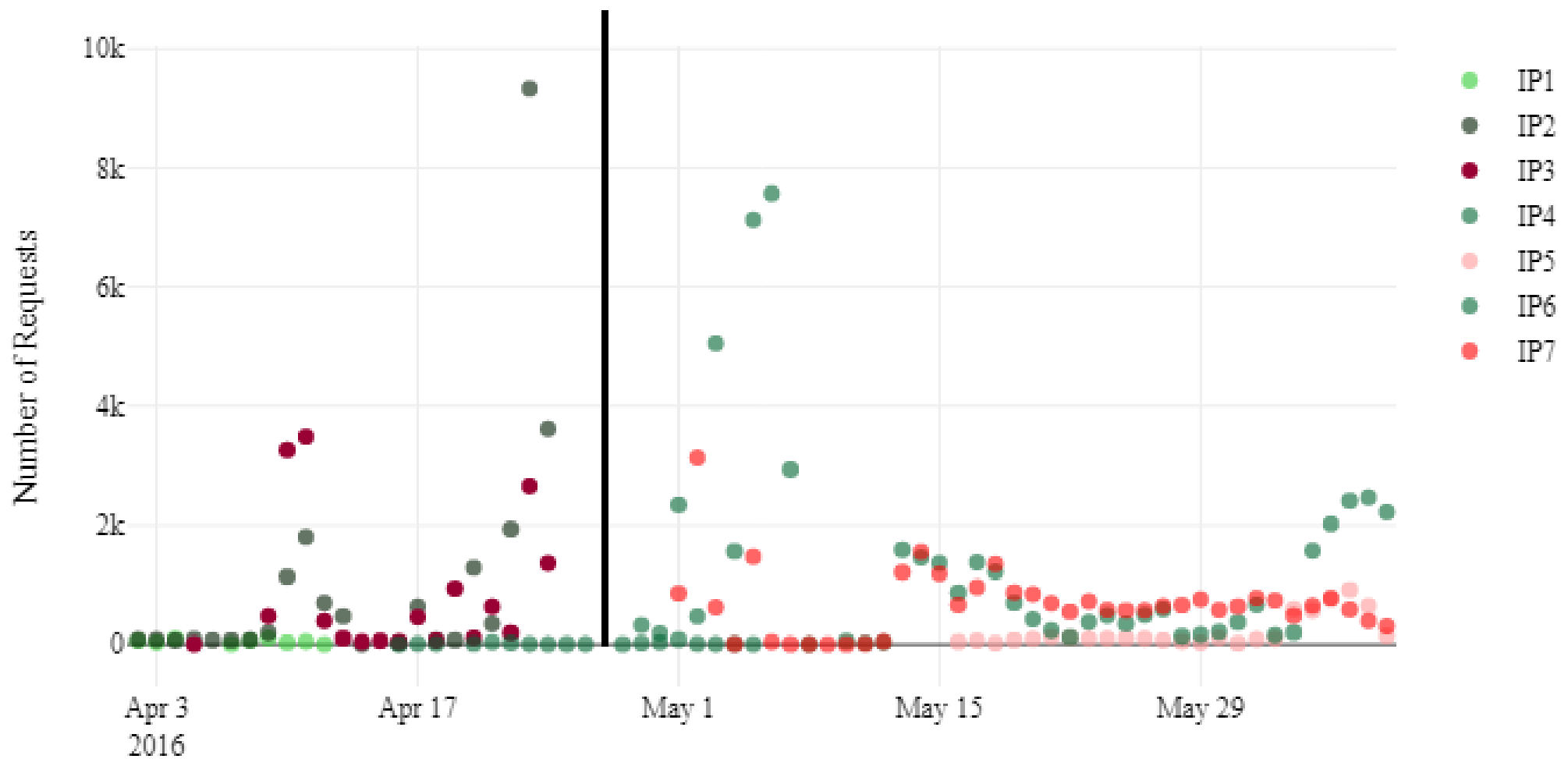
Number of Requests sent per Whitelisted IP Address





# Timestamps

Number of Requests sent per Whitelisted IP Address

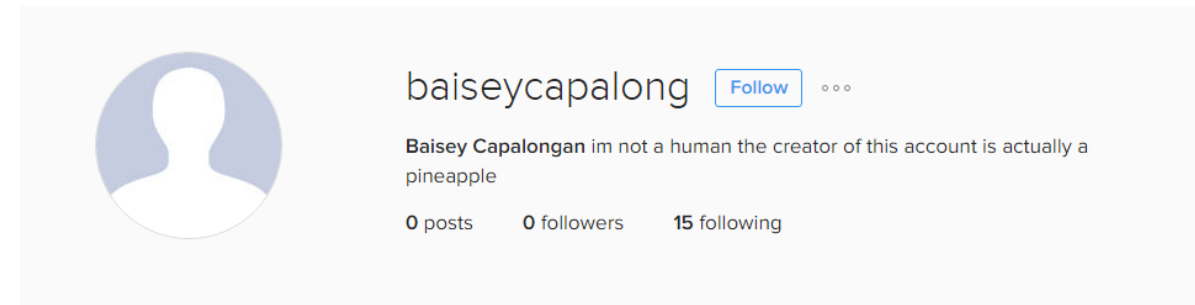
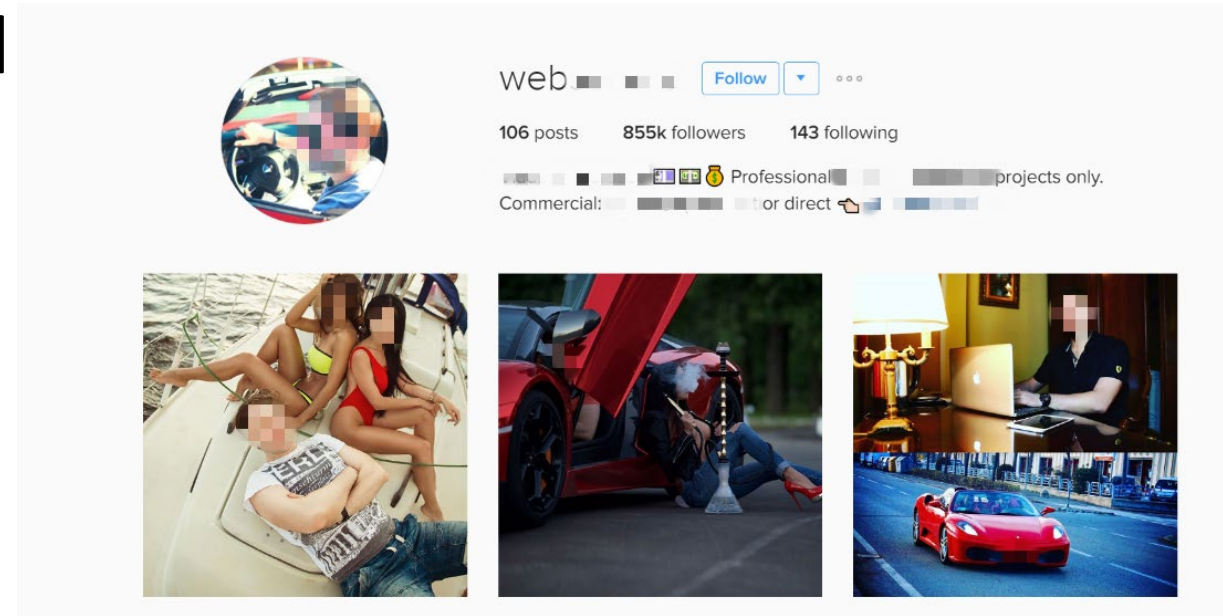


# Accounts Created and Accounts Followed

Different whitelisted IPs followed  
the same accounts →

AND

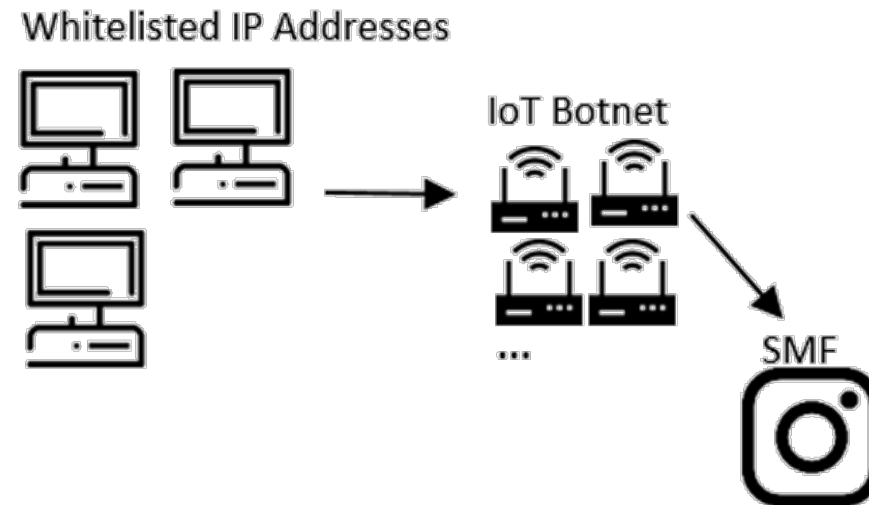
List of fake accounts per  
whitelisted IP →



# Purpose of the Whitelisted IPs

Fake account management !

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



**RSA**®Conference2019

# Uncover the supply chain behind social media fraud

*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

**Socialnavy.com**[Sign in](#)[Services](#)

**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 Resslerer.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 \*\*\*

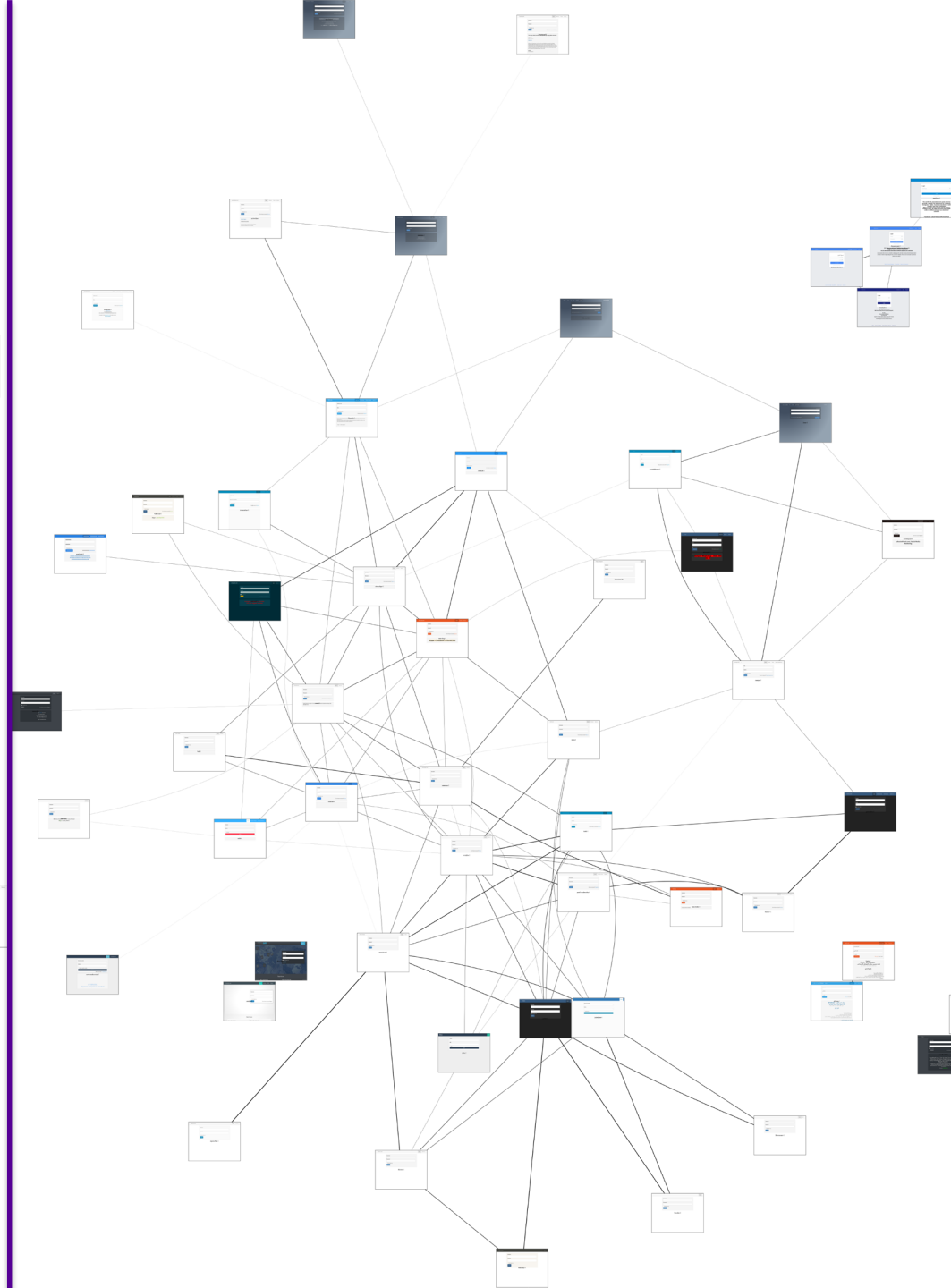
You can resell our social media marketing (SMM) services to your own panel or resell on Fiverr ,Seoclerks and more others social stores.

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

# 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
<input type="checkbox"/>	<a href="#">ip228.ip-54-37-92.eu</a>	2018-04-19	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">takipcidestegim.com</a>	2018-06-24	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">bayimarket.com</a>	2018-04-30	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">takipdeposu.com</a>	2018-04-19	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">turuncubayi.com</a>	2018-10-02	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">privatesmm.com</a>	2018-04-19	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">smmfollows.com</a>	2018-04-19	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">smmlite.com</a>	2018-04-19	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">auto-sm.com</a>	2018-04-19	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">medyabayim.com</a>	2018-05-03	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">viasmm.com</a>	2018-05-15	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">vinasocial.com</a>	2018-09-05	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">sosyalbayin.com</a>	2018-09-05	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">sosyalbayilik.com</a>	2018-04-19	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">buzpromoter.com</a>	2018-05-30	2018-10-03	riskiq
<input type="checkbox"/>	<a href="#">perfectpanel.com</a>	2018-04-18	2018-10-03	pingly, riskiq



**RSA**®Conference2019

# Uncover the supply chain behind social media fraud

*Software Panel Seller*



# The Software Panel Seller

**Perfect Panel**

Features

Pricing

Demo

FAQ

Sign in

Get started

## The best SMM panels platform

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

# 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>

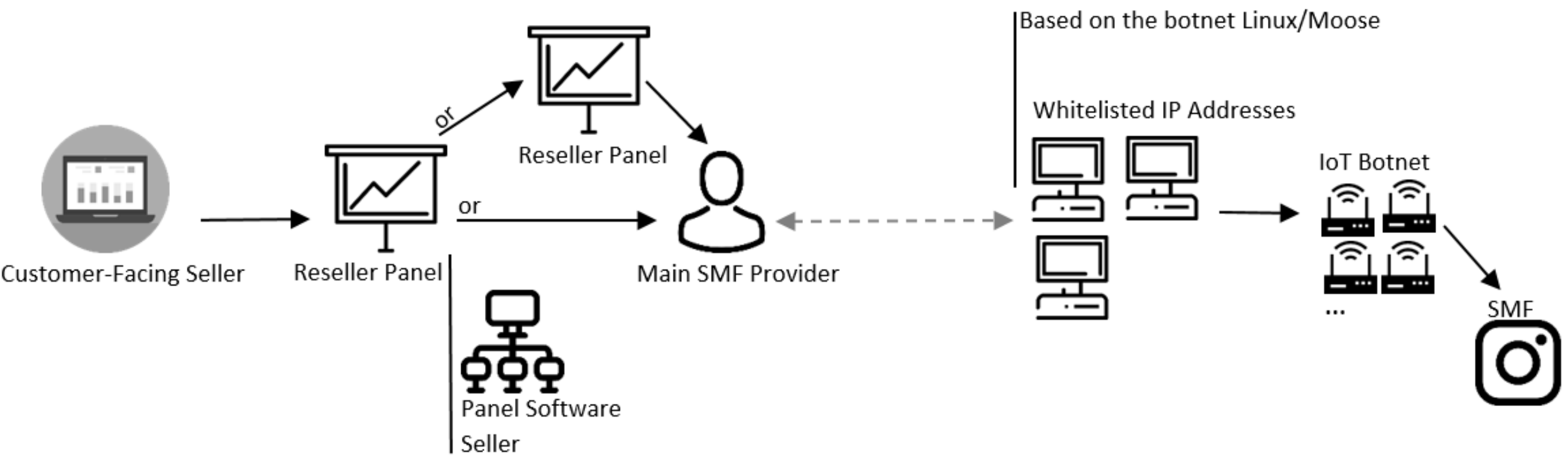
Guys, unless you're spending \$1k/day on smm panels, you don't need to search for the original supplier: a) he wouldn't be interested in your volumes; b) you just need to find the most reliable reseller from the most cheap resellers - and get it on with it, that would be enough =)

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 a supply chains: many actors are involved in reselling social media fraud
- We conclude that potentials target to disrupt social media fraud are **software panel sellers**

# Apply

- **Next week, you should:**

Change Telnet default credentials of all devices within the organization !

- **Within the next year, you should:**

Educate the public of such threat, ensure other individuals do not only use “followers” as indicators of credibility

# RSA<sup>®</sup>Conference2019

San Francisco | March 4–8 | Moscone Center



**BETTER.**

SESSION ID: SEM-M03C

## Thank you! Questions?

**Masarah Paquet-Clouston**

Cybersecurity Researcher  
GoSecure CounterTack  
@masarahclouston

**Olivier Bilodeau**

Cybersecurity Research Lead  
GoSecure CounterTack  
@obilodeau

#RSAC