

Behind the Scenes:
The Industry of Social Media Manipulation Driven by Malware

Masarah Paquet-Clouston, Olivier Bilodeau
GoSecure Research



Back in 2015-2016

ESET Mitacs





Université de Montréal

Linux/Moose Botnet

450977dc7ba2ec0879fb17c612e248ece

Run Script ▾ Run Template ▾

3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00	70	61	73	73	77	6F	72	64	20	69	73	20	ror.password is
6E	67	00	00	00	70	61	73	73	77	6F	72	64	wrong...password
00	75	74	68	65	6E	74	69	63	61	74	69	6F	:...uthenticatio
61	69	6C	65	64	00	00	00	00	73	68	0D	0A	n failed....sh..
00	70	73	0D	0A	65	63	68	6F	20	2D	6E	20	....ps..echo -n
22	48	33	6C	4C	30	57	6F	52	6C	44	22	0D	-e "H3lL0WoRlD".
6D	6F	64	0D	0A	00	00	00	00	48	33	6C	4C	.chmod......H3lL
52	6C	44	00	00	65	6C	61	6E	32	00	00	00	0WoRlD..elan2...
6E	33	00	00	00	63	68	6D	6F	64	3A	20	6E	elan3...chmod: n
66	6F	75	6E	64	00	00	00	00	63	61	74	20	ot found....cat
6F	63	2F	63	70	75	69	6E	66	6F	0D	0A	00	/proc/cpuinfo...
20	2F	78	78	2F	72	6E	64	65	2E	70	68	70	GET /xx/rnde.php
25	64	26	66	3D	25	64	26	6D	3D	25	64	20	?p=%d&f=%d&m=%d
50	2F	31	2E	31	0D	0A	48	6F	73	74	3A	20	HTTP/1.1..Host:
2E	67	65	74	63	6F	6F	6C	2E	63	6F	6D	0D	www.getcool.com.
6E	6E	65	63	74	69	6F	6E	3A	20	4B	65	65	.Connection: Kee
6C	69	76	65	0D	0A	0D	0A	00	6C	6F	00	00	p-Alive.....lo..
2E	30	2E	30	2E	31	00	00	00	2F	70	72	6F	127.0.0.1.../pro
00	2F	70	72	6F	63	2F	25	73	2F	63	6D	64	c.../proc/%s/cmd
65	00	00	00	00	6B	69	6C	6C	20	25	73	00	line....kill %s.
63	2F	69	6E	69	74	2E	64	2F	72	63	53	00	/etc/init.d/rcS.
6D	65	2F	68	69	6B	2F	73	74	61	72	74	2E	/home/hik/start.
00	2F	65	74	63	2F	63	72	6F	6E	74	61	62	sh../etc/crontab
00	2F	65	74	63	2F	63	72	6F	6E	2E	68	6F	..../etc/cron.ho
79	2F	78	00	00	2F	65	74	63	2F	72	63	2E	urly/x../etc/rc.
63	00	00	00	00	31	39	32	2E	31	36	38	2E	d/rc....192.168.
00	25	64	00	00	53	79	73	20	69	6E	69	74	1.3.%d..Sys init
4B	00	00	00	00	2D	6E	6F	62	67	00	00	00	: OK....-nobg...
73	79	6E	63	00	42	61	64	20	69	6E	69	74	No sync.Bad init
00	25	64	20	25	64	20	25	64	0A	00	00	00	....%d %d %d....
C0	03	01	A8	C0	03	01	A8	C0	00	00	00	00	..¨À..¨À..¨À....
6E	2F	73	68	00	2D	63	00	00	65	78	69	74	/bin/sh.-c..exit
00	00	00	74	40	00	00	00	20	00	00	00	01	0....t@... ....



Linux/Moose ?



Linux/Moose
An IoT botnet that conducts social media manipulation

Social Media Manipulation

LA PRESSE .CA

DÉBATS VIDÉOS

21°C MONTRÉAL Changer de vil

ACTUALITÉS INTERNATIONAL AFFAIRES SPORTS AUTO ARTS CINÉMA S

Politique Grand Montréal Régional Justice et faits divers Santé Éducation Enquêtes Interna

Accueil > Actualités > Enquêtes > Comment devenir influenceuse (en trichant)

Publié le 14 juin 2019 à 05h00 | Mis à jour le 14 juin 2019 à 10h43

Comment devenir influenceuse (en trichant)



ÉMILIE BILODEAU, MARTIN TREMBLAY
La Presse

PARTAGE
Partager 12 K
Tweeter

Quinze mille abonnés achetés. Des mentions « J'aime » générées par des robots. Des photos truquées. Notre journaliste a multiplié les méthodes controversées pour faire mousser la popularité de son personnage



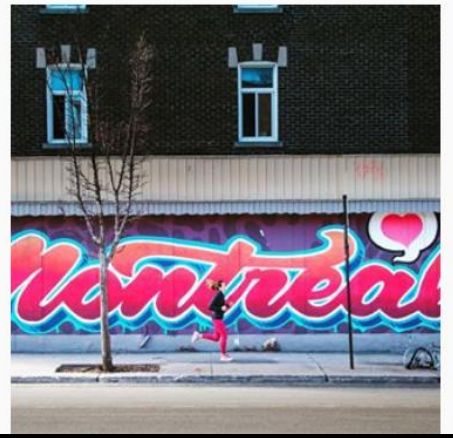
the.pretty.runner Follow ···

57 posts 14k followers 426 following

The Pretty Runner
Enquête de La Presse+
Journaliste 🖊: Émilie Bilodeau
Photographe 📷: Martin Tremblay
Pour lire le reportage complet, cliquez ici ⬇
plus.lapresse.ca/screens/e3969255-e91e-42d8-936e-286adddec4e2__7C___0.html?...

POSTS TAGGED





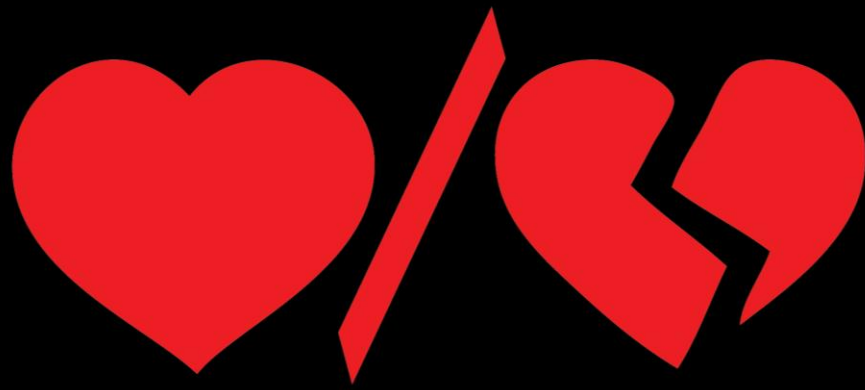


DEFCON

like
4like

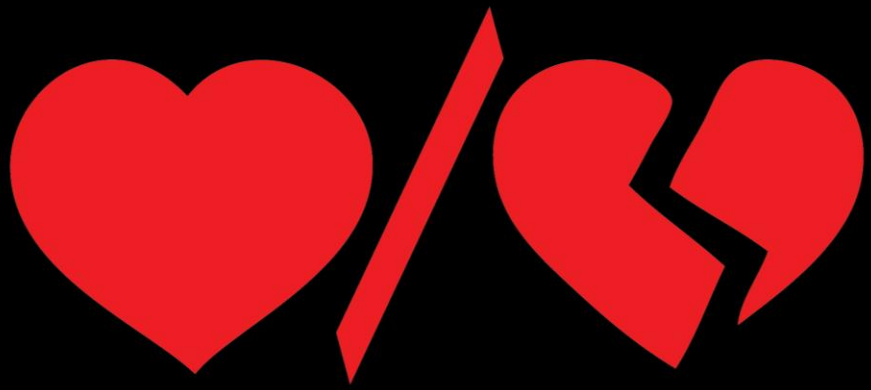
DEFCON

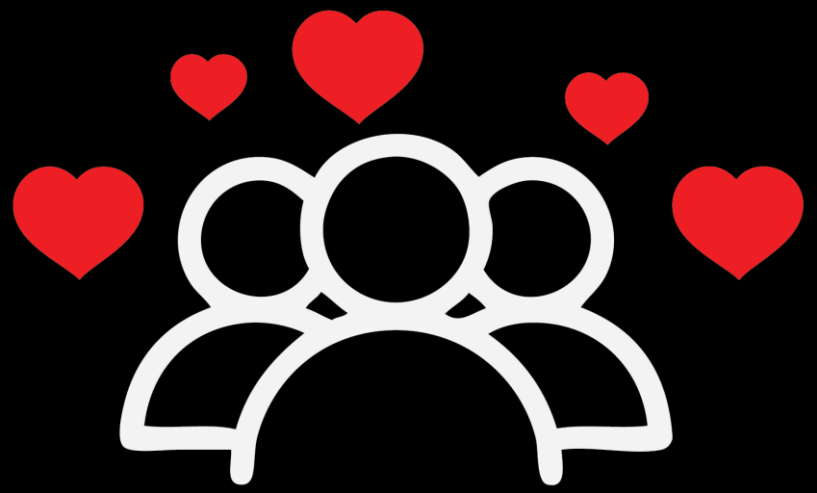
like
4like



DEFCON

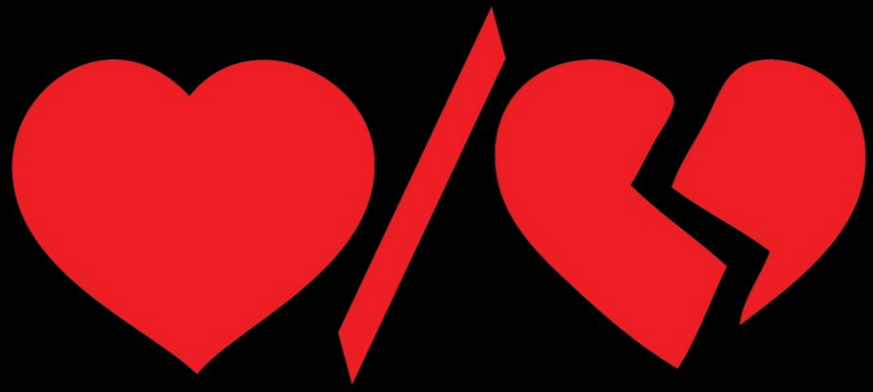
like
4like

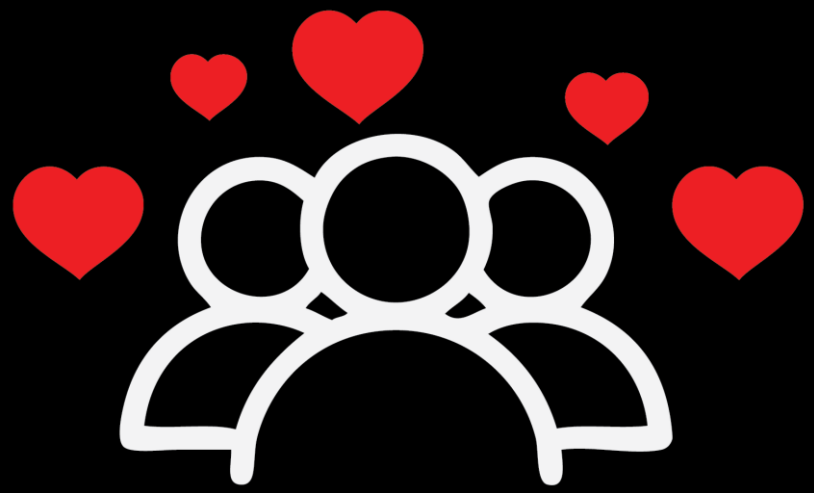




DEFCON

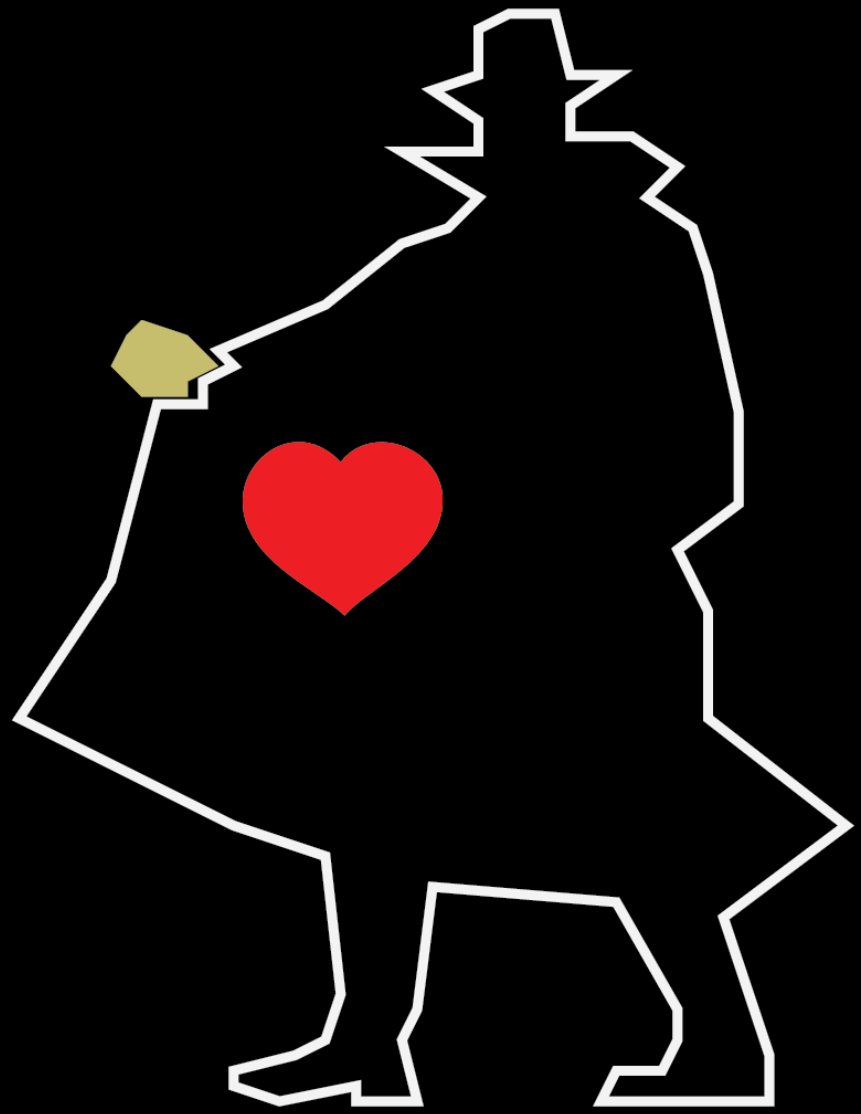
like 4like







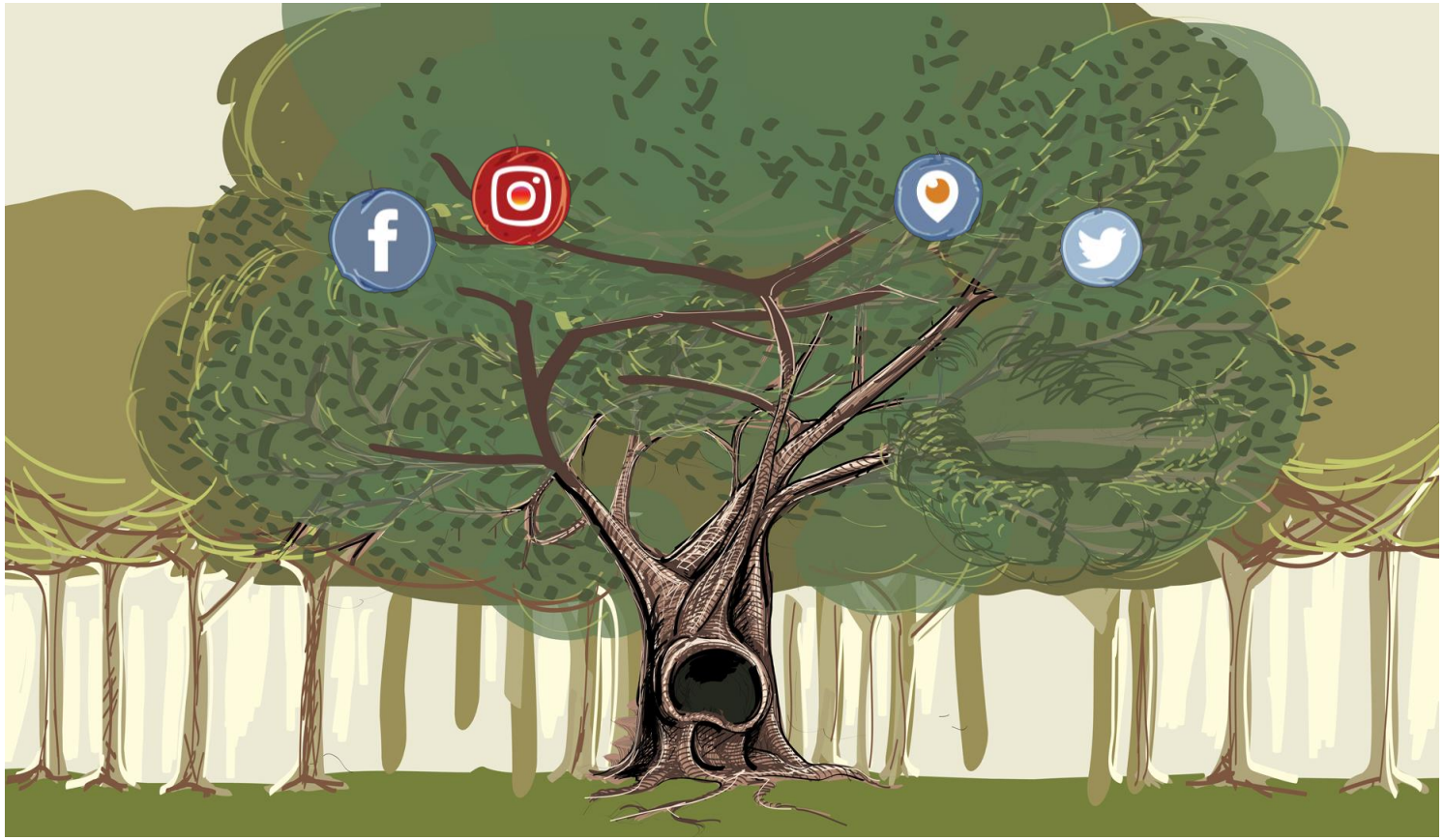
DEFCON



DEFCON



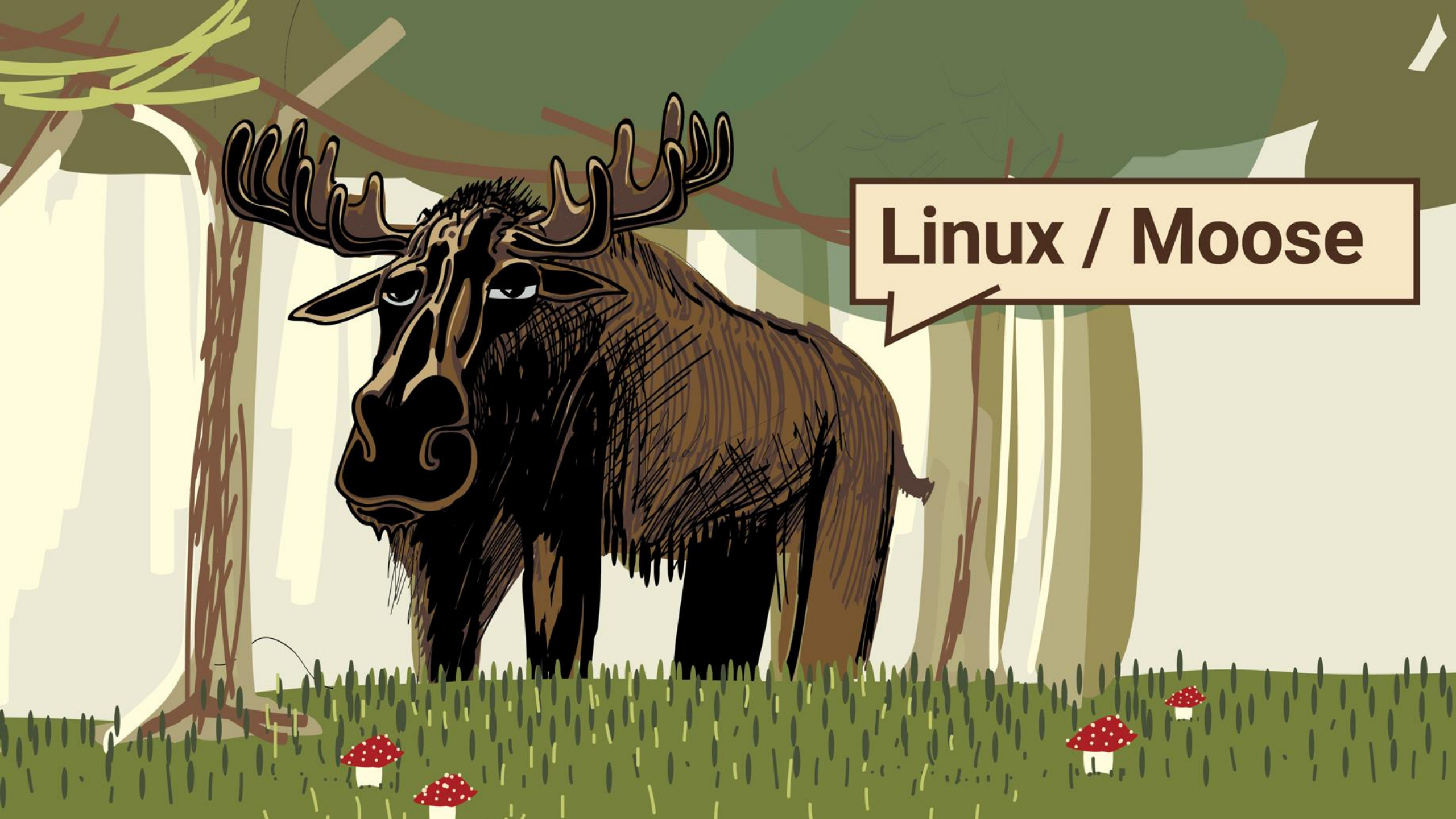


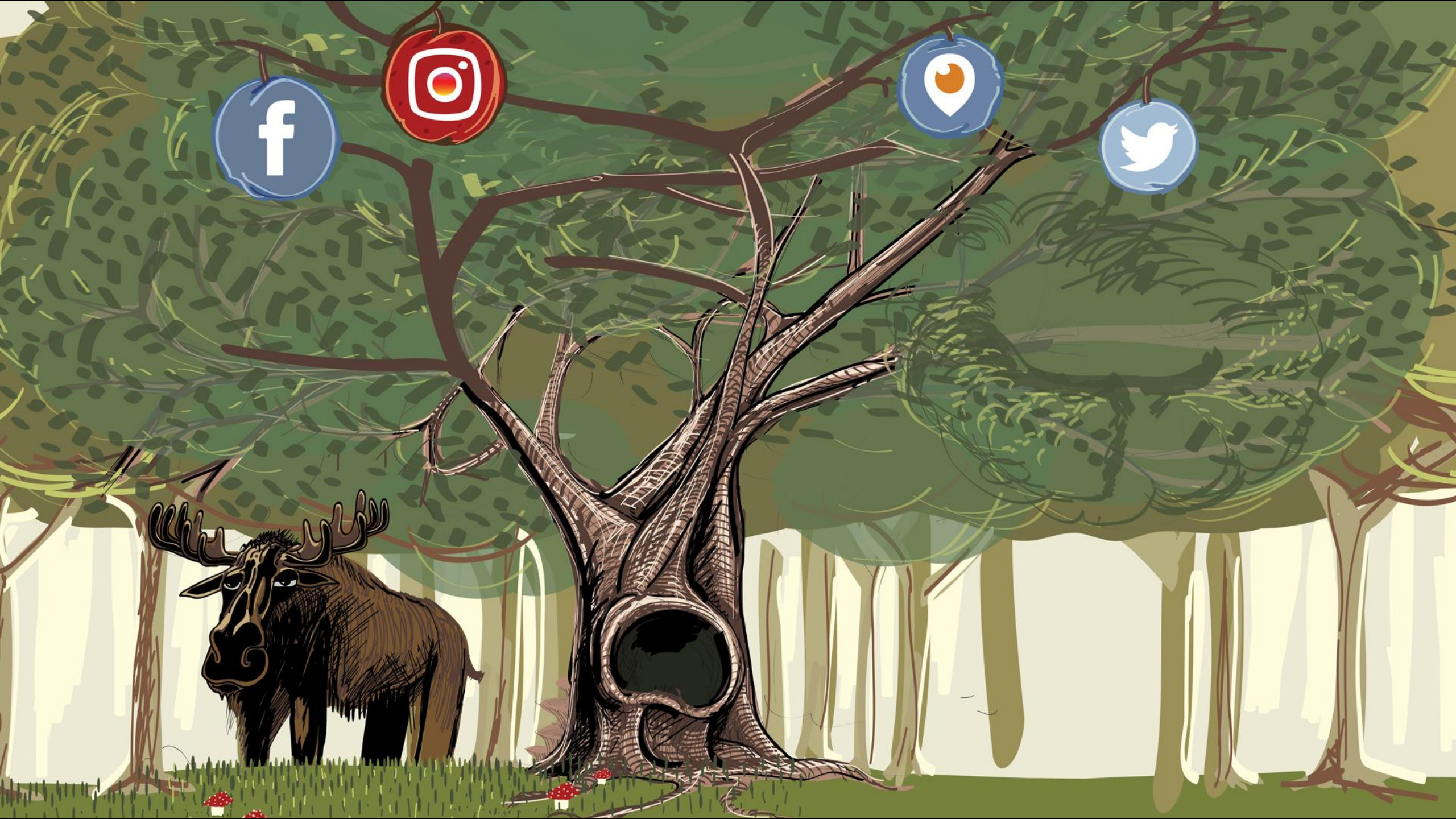


The Ecosystem of Social Media Manipulation

Presentation is about:

- A four-year long investigation
- Various investigative techniques
- A mapping of all actors involved


Linux / Moose



Linux/Moose

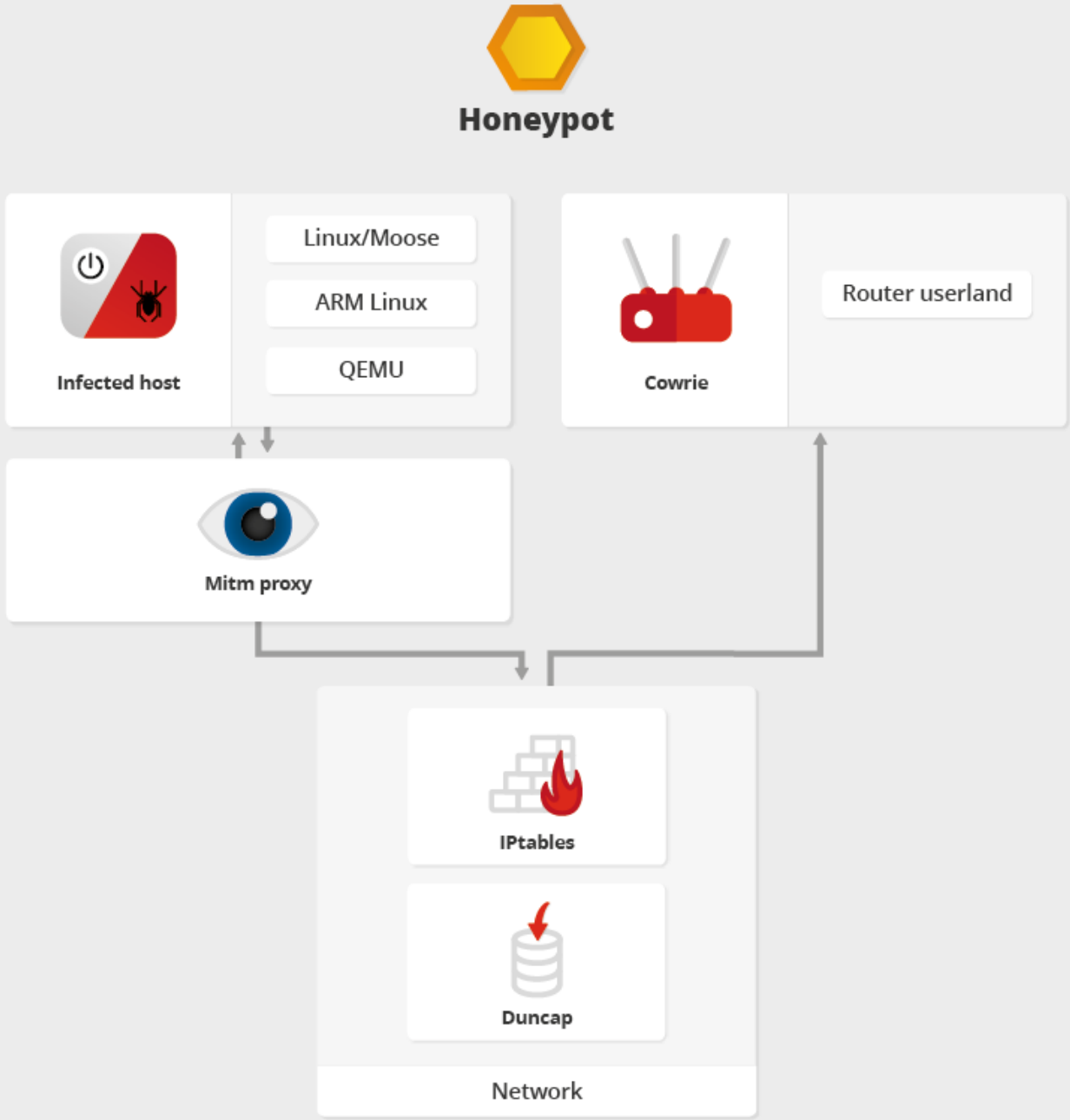
- Affects routers / Internet of Things (IoT)
  - Embedded Linux systems with busybox userland
- Worm-like behavior
  - Telnet credential brute force
- Payload: Proxy service
  - SOCKSv4/v5, HTTP, HTTPS

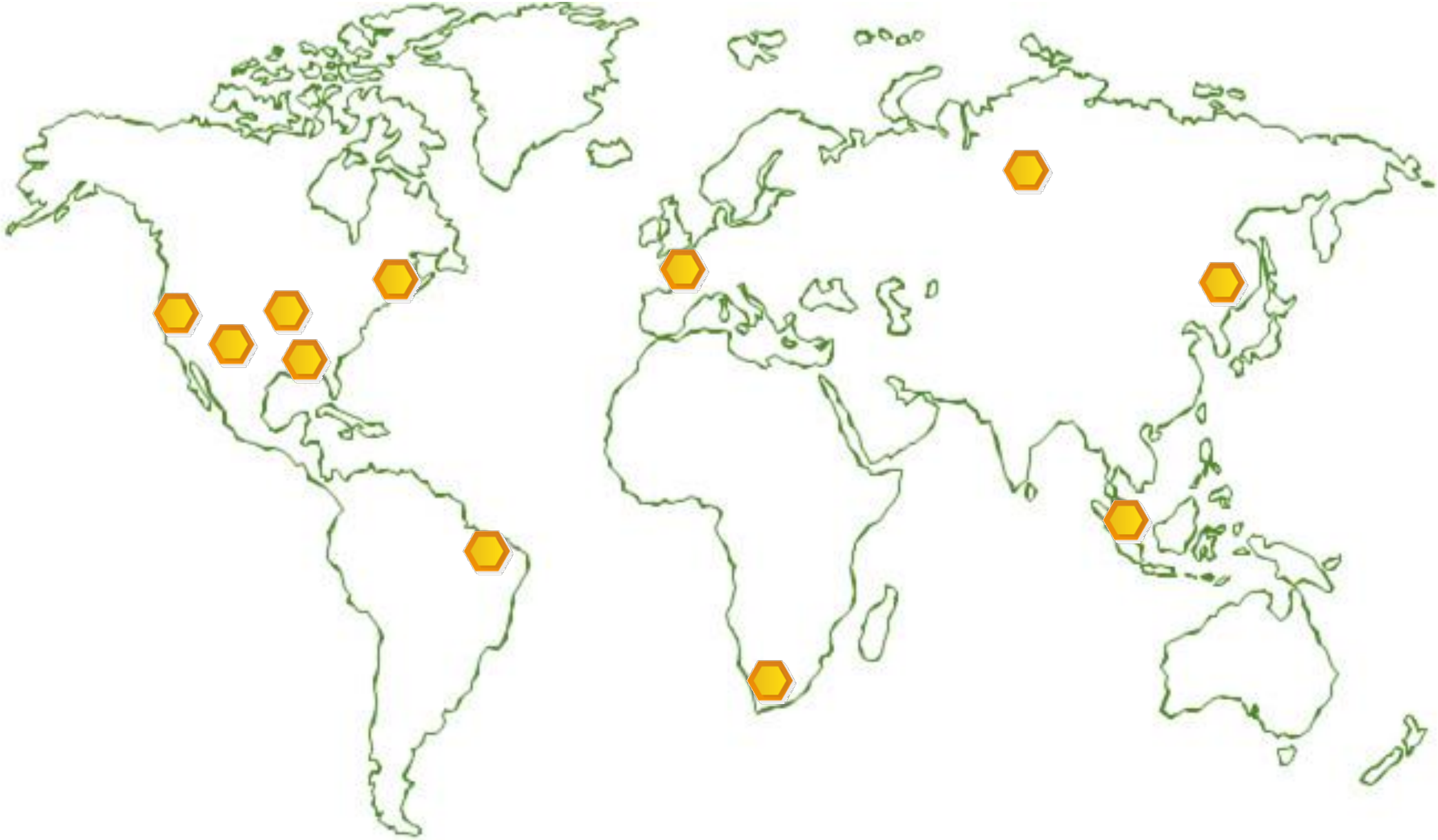


Honeypots

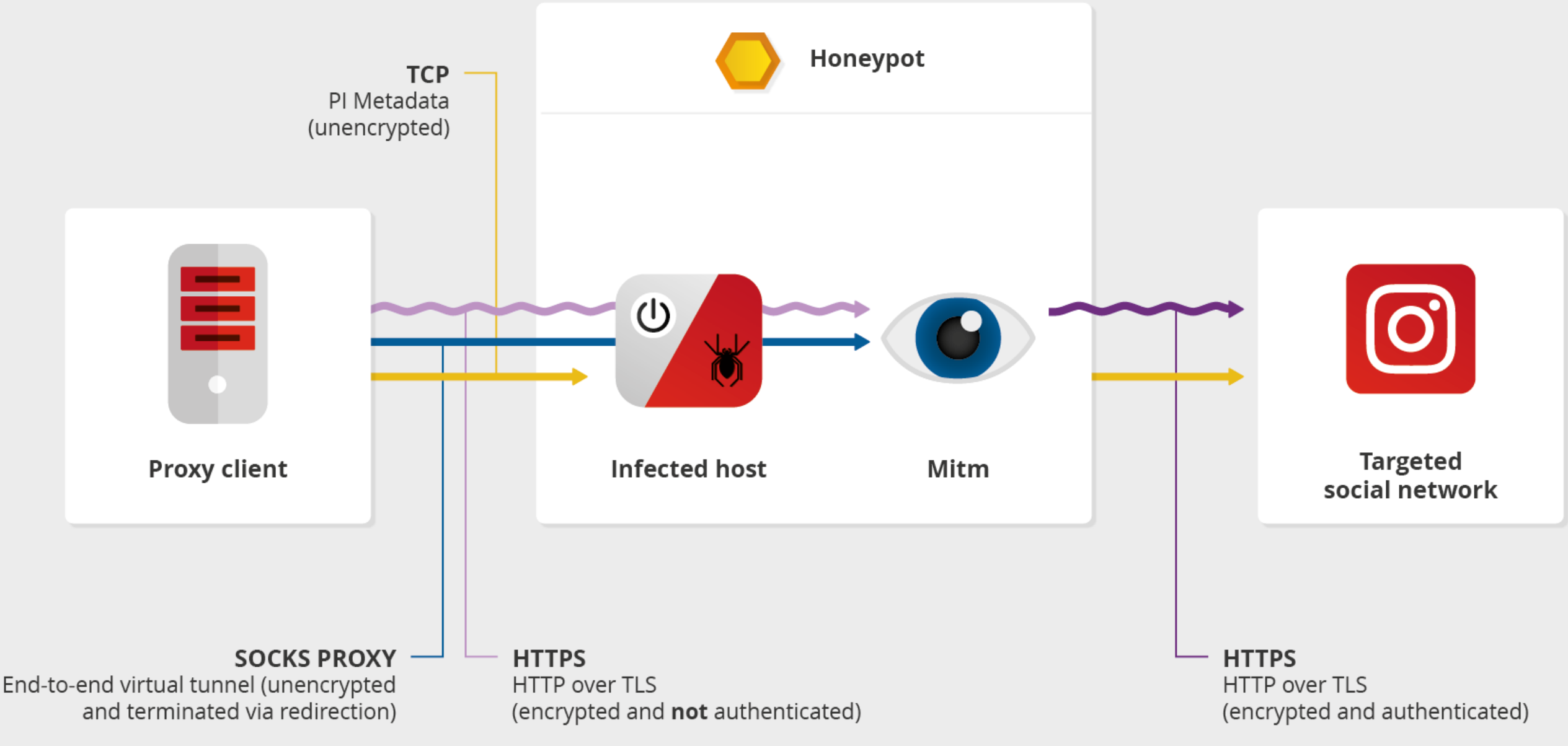
- Software-based
- Low interaction
- Side-loaded an ARM virtual machine
  - Which we infected







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




Accessed the raw traffic!

What did we have?

- Several infected hosts actively used by operators
- HTTPS traffic in plaintext
- C&C traffic
- Publicly available seller market





EGO
MARKET

When Greed
for Fame Benefits
Large-Scale Botnets

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 provides a deeper understanding of the illicit market for SMF. It conducts a market price analysis for SMF, describes the operations of a supplier – an Internet of things (IoT) botnet performing SMF – and provides a profile of the potential customers of such fraud. The paper explains how an IoT botnet conducts social network manipulation and illustrates that the fraud is driven by OSN users, mainly entertainers, small online shops and private users. It also illustrates that OSN strategy to suspend fake accounts only cleans the networks a posteriori of the fraud and does not deter the crime – the botnet – or the fraud – SMF – from happening. Several solutions to deter the fraud are provided.

CCS Concepts

Human-centered computing → Collaborative and social computing → Collaborative and social computing theory, concepts and paradigms → Social media • Security and privacy → Intrusion/anomaly detection and malware mitigation → Malware and its mitigation • → Human and societal aspects of security and privacy

Keywords

Social media fraud (SMF); Online social networks (OSN); IoT botnets; Market analysis.

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 content online. In some cases, however, actors elect to buy their fan base, a strategy that is part of social media fraud (SMF). SMF is the process of creating likes, follows, views or any other online actions on OSN like Facebook, Twitter, YouTube and Instagram to artificially increase an account's fan base. This method falsifies social media data and creates disinformation that could lead to a decrease in users' trust in OSN. This paper studies the illicit market where SMF services are bought and sold to better understand the potential impact of that market on OSN. With a research method that combines computer sciences and social sciences, this paper evaluates the supply and demand for SMF services. The supply analysis is two-fold: a market price analysis for SMF services and an in-depth evaluation of the operations of an IoT botnet acting as a supplier in the market. The demand analysis contains a profiling of 'potential customers' of SMF, retrieved from accounts found in the IoT botnet communications. The results provide an in-depth understanding of the extent to which social media data can be trusted and who contributes to falsifying it.

The following text presents a literature review of what is known about SMF and social network manipulation by botnets. Then the research methodology is developed, followed by the result and the discussion section.

2. LITERATURE REVIEW

OSN have been the target of various malicious activities such as identity theft [3], spam campaigns [22] and political online manipulation [12]. Those behind the malicious activities exploit the trust relationship between OSN users to manipulate, distort,


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

Whitelisted IPs

Reseller model?

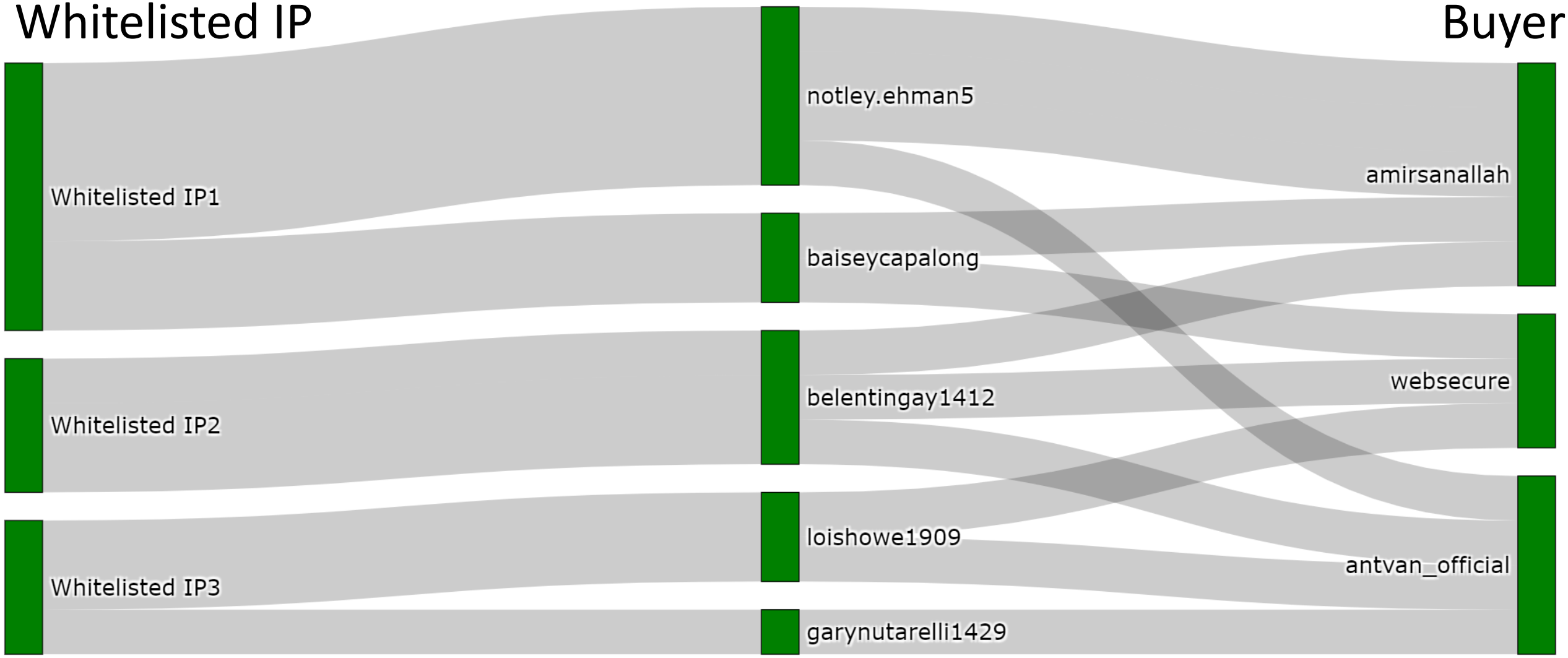




Traffic analysis



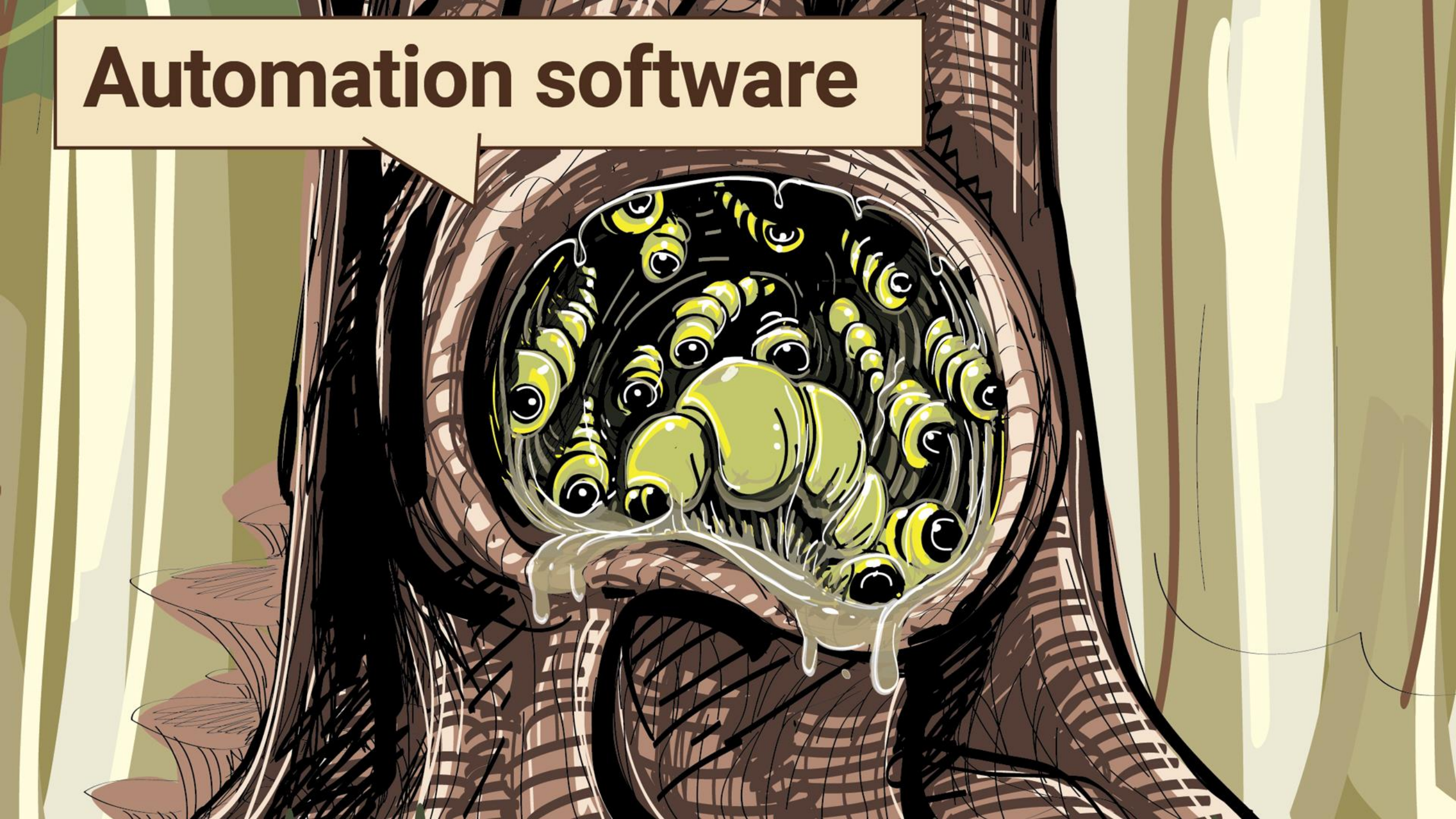
Variables	
	Honeypots used
	Websites targeted
	TLS fingerprints
	User agents
	API calls
	Timestamps
	Accounts created on social networks
	Accounts followed on social networks

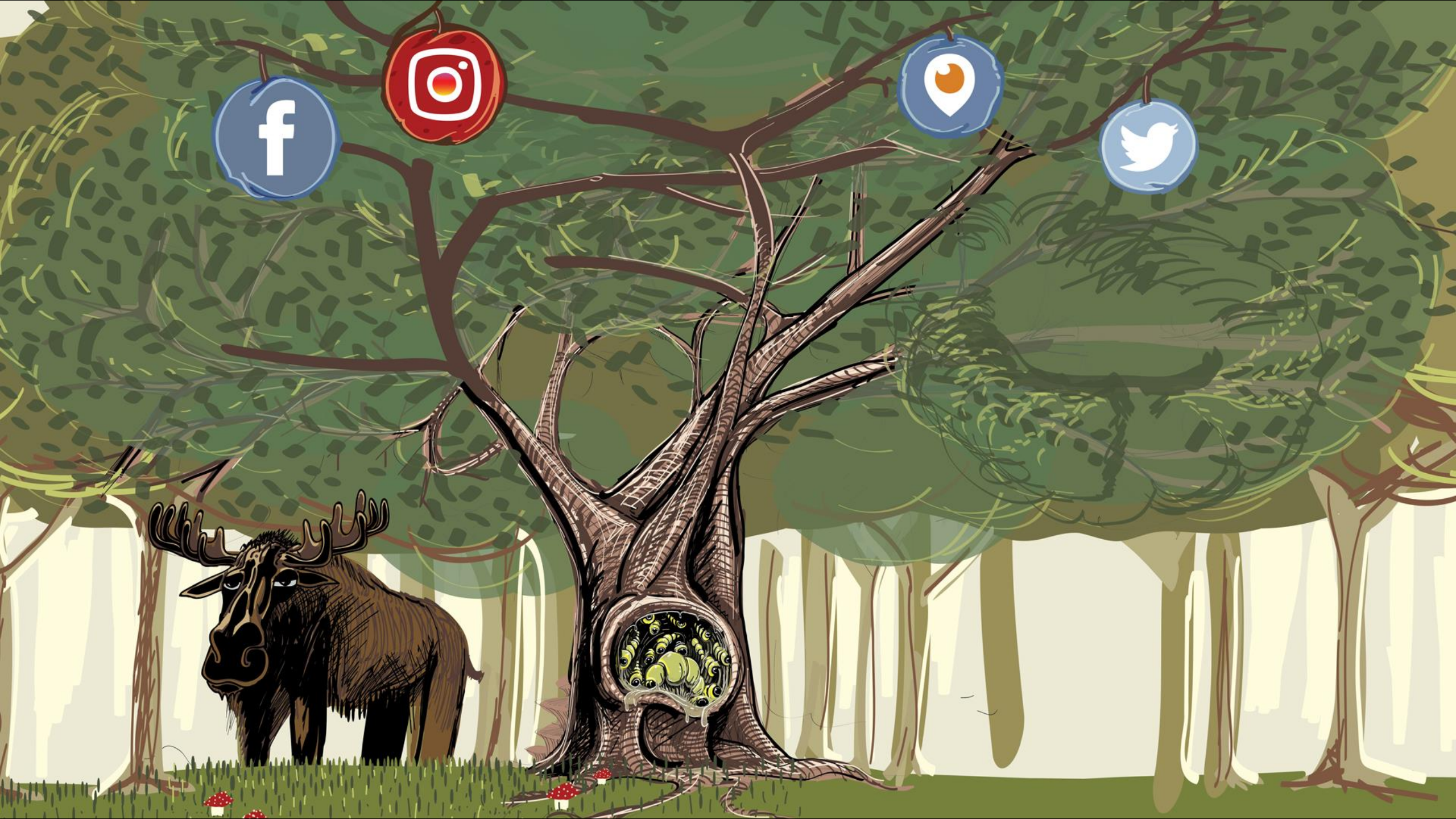

Whitelisted IP
Buyer
Whitelisted IP1
Whitelisted IP2
Whitelisted IP3
notley.ehman5
baiseycapalong
belentingay1412
loishowe1909
garynutarelli1429
amirsanallah
websecure
antvan_official
Fake account

Where do we stand?

- Fake accounts
  - Pinned to a given honeypot
  - Originate from a single whitelisted IP address
- Whitelisted IP addresses
  - Runs on Windows servers
  - RDP is actively used




Automation software



Automation Software

- We tried to find the Linux/Moose provider
  - Based on User-Agents: Mobile and Desktop
  - Socks proxy support
- Found different features
  - Proxy-type HTTP / Socks
  - Per account User-Agents (Mobile and Desktop)
  - Custom browsing patterns
- Found different business models
  - Unlimited accounts
  - One-time fee / Pay-per-month / Pay-per-account



GramDominator

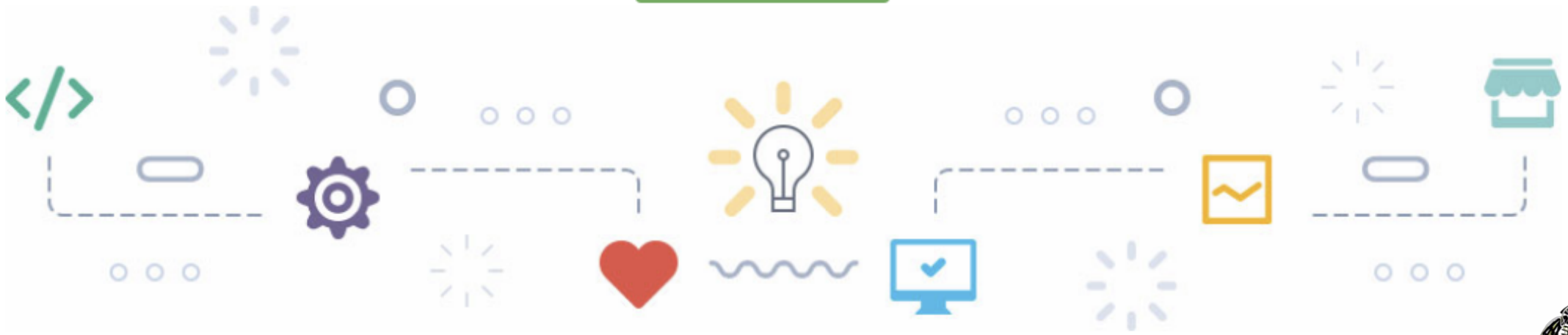
HOME FEATURES PRICING FREE MOBILE APPS BECOME AN AFFILIATE HELP JOIN FB GROUP LOGIN

Everything You Need

to increase Instagram traffic and sales

Not just scheduling but complete automation

Buy Now



- Filter people to follow by specific text in description
- Unfollow users who are following back (all your followers)
- Unfollow users (all your following)
- Unfollow inactive profiles who has not posted within last xx days
- Unfollow custom list of users
- Unfollow only users not following you back
- Auto add to blacklist once unfollowed
- Multiple photos posting from multiple accounts (Give each photo it's own caption...)
- Find and repost photos by keywords
- Find and repost custom list of photos
- Find and repost photos of specific users
- Find and repost photos of followers of specific users

hasntags in photo caption...)

- Comment on a user's photos
- Comment on custom list of photos (your own list of photo IDs)
- Comment on popular photos
- Proxy support (public/private/socket/http...)
- Tasks scheduling and continuous automation
- Import and export data (all activities done with your accounts for your campaigns)
- White-list users (special list of users who should not be unfollowed...)
- Blacklist users (unwanted users who should not be followed)
- Spintax support
- Tasks Randomization
- Run several Instagram accounts at the same time
- Plus much more...



```
1033            objInstagramUser.DataBaseid = (int)x.Id;
1034            if (!string.IsNullOrEmpty(x.DevUid))
1035            {
1036                objInstagramUser.guid = x.DevUid.Replace("android-", "");
1037            }
1038            objInstagramUser.UserAgentMobile = x.MobileUserAgent;
1039            if (string.IsNullOrEmpty(objInstagramUser.UserAgentMobile))
1040
1041        public string PhoneId { get; private set; }
1042
1043        // Token: 0x1700004F RID: 79
1044        // (get) Token: 0x060000C8 RID: 200 RVA: 0x0000A8D0 File Offset: 0x00008AD0
            public string Useragent
1045        {
1046            get
1047            {
1048                return string.Format(ConstantVariable.UseragentCommonFormat, new object[]
1049                {
1050                    ConstantVariable.IgVersion,
1051                    this.AndroidVersion,
1052                    this.AndroidRelease,
1053                    this.Dpi,
1054                    this.Resolution,
1055                    this.ManufacturerBrand,
1056                    this.Model,
1057                    this.Device,
1058                    this.Cpu,
1059                    ConstantVariable.UseragentLocale
1060                });
1061            }
1062        }
1063
1064
1065
1066
1067
1068
```



Windows PowerShell (x86)

```
PS C:\Users\jake\Desktop\gram> [Reflection.Assembly]::LoadFile("C:\Users\jake\Desktop\gram\BaseLib.dll")

GAC    Version        Location
---    -------        --------
False  v4.0.30319     C:\Users\jake\Desktop\gram\BaseLib.dll


PS C:\Users\jake\Desktop\gram> $devGen = new-object BaseLib.DeviceGenerator
PS C:\Users\jake\Desktop\gram> $devGen.Useragent
Instagram 40.0.0.14.95 Android (24/7.0; 640dpi; 1440x2560; HUAWEI; LON-L29; HWLON; hi3660; en_US)
PS C:\Users\jake\Desktop\gram> $devGen = new-object BaseLib.DeviceGenerator
PS C:\Users\jake\Desktop\gram> $devGen.Useragent
Instagram 40.0.0.14.95 Android (23/6.0.1; 640dpi; 1440x2560; samsung; SM-G930F; herolte; samsungexynos8890; en_US)
PS C:\Users\jake\Desktop\gram> $devGen = new-object BaseLib.DeviceGenerator
PS C:\Users\jake\Desktop\gram> $devGen.Useragent
Instagram 40.0.0.14.95 Android (24/7.0; 640dpi; 1440x2560; HUAWEI; LON-L29; HWLON; hi3660; en_US)
PS C:\Users\jake\Desktop\gram>
```



THE SOCIAL DOMINATOR

Social | English

Accounts Manager

DashBoard

Aut

Pub

Pro

Sett

Oth

Account Details

Add Account | Import Multiple Accounts | Select | Update | Export | Delete

SOCIAL NETWORK	USER NAME	STATUS	GROUP NAME	PROXY ADDRESS	FRIENDSHIP COUNT

THE SOCIAL DOMINATOR

Accounts Manager

Account Details

Social | English

Add Account | Import Multiple Accounts | Select | Update | Export | Delete

Info | Error List

7/9/2019 2:18:32 PM	Instagram	synchronizing Feeds Successful.
7/9/2019 2:18:28 PM	Instagram	Started Feeds synchronization.
7/9/2019 2:18:28 PM	Instagram	synchronizing Followings Successful.
7/9/2019 2:18:23 PM	Instagram	Started Followings synchronization.
7/9/2019 2:18:23 PM	Instagram	synchronizing Followers Successful.
7/9/2019 2:15:51 PM	Instagram	Started Followers synchronization.
7/9/2019 2:15:31 PM	Instagram	Account login status : Success
7/9/2019 2:15:30 PM	Instagram	Login successful.
7/9/2019 2:15:29 PM	An error occured in exception handler for the webrequest. Code: 405	
7/9/2019 2:14:55 PM	Instagram	details updated successfully.

Loaded Memory : 4096 MB

Available Memory : 1814 MB



C:\Users\User\D

IDA Vi

Address

.rdata:100
.rdata:100
.rdata:100
.data:1001
.data:1001
.data:1001
.data:1001
.data:1001
.data:1001
.data:1001
.data:1001
.data:1001
.data:1001

RunAsDate v1.37 - Run a program with the specified date/time
Copyright (c) 2007 - 2019 Nir Sofer

AddThis

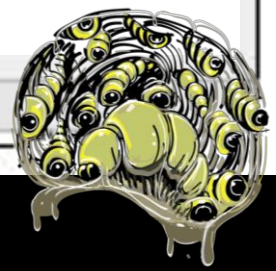
Follow Liker 10.1.9 (Instagram Edition) - Instagram -

File Tools Theme Help

Status: N/A

Username	Password	Proxy	Media	Following
	********	N/A	N/A	N/A

Close About



Automation Software Summary



	Architecture	Browser	Packer	Our Target?
GramDominator / Socinator	.Net	CEF	Not packed	No socks proxy support
FollowAdder	Xojo / REALBasic	CEF	Obscure Xojo framework	No unlimited accounts
MassPlanner	C++ / .Net	CEF	Themida / WinLicense 2.x	Only one overridable User-Agent
FollowingLike	.Net	BotSocial, a custom browser in .Net	ILProtector	Custom User-Agent feature too recent
FollowLiker	Java compiled to native code	HtmlUnit Java Library	Excelsior JET	Doesn't interact with Instagram similarly

DEFCON

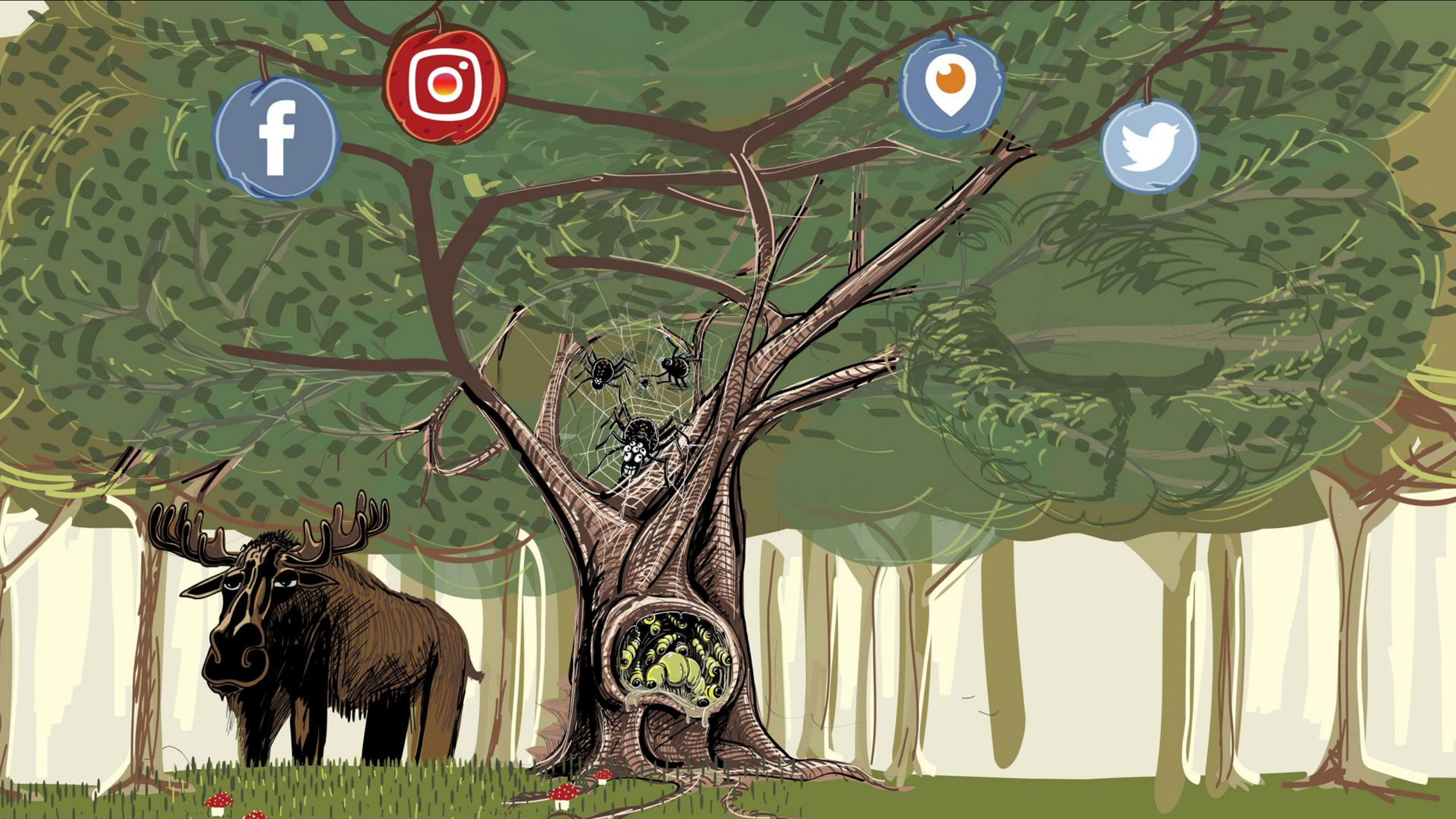
Where do we stand?

Found several automation software vendors

Reseller model is not at the botnet level



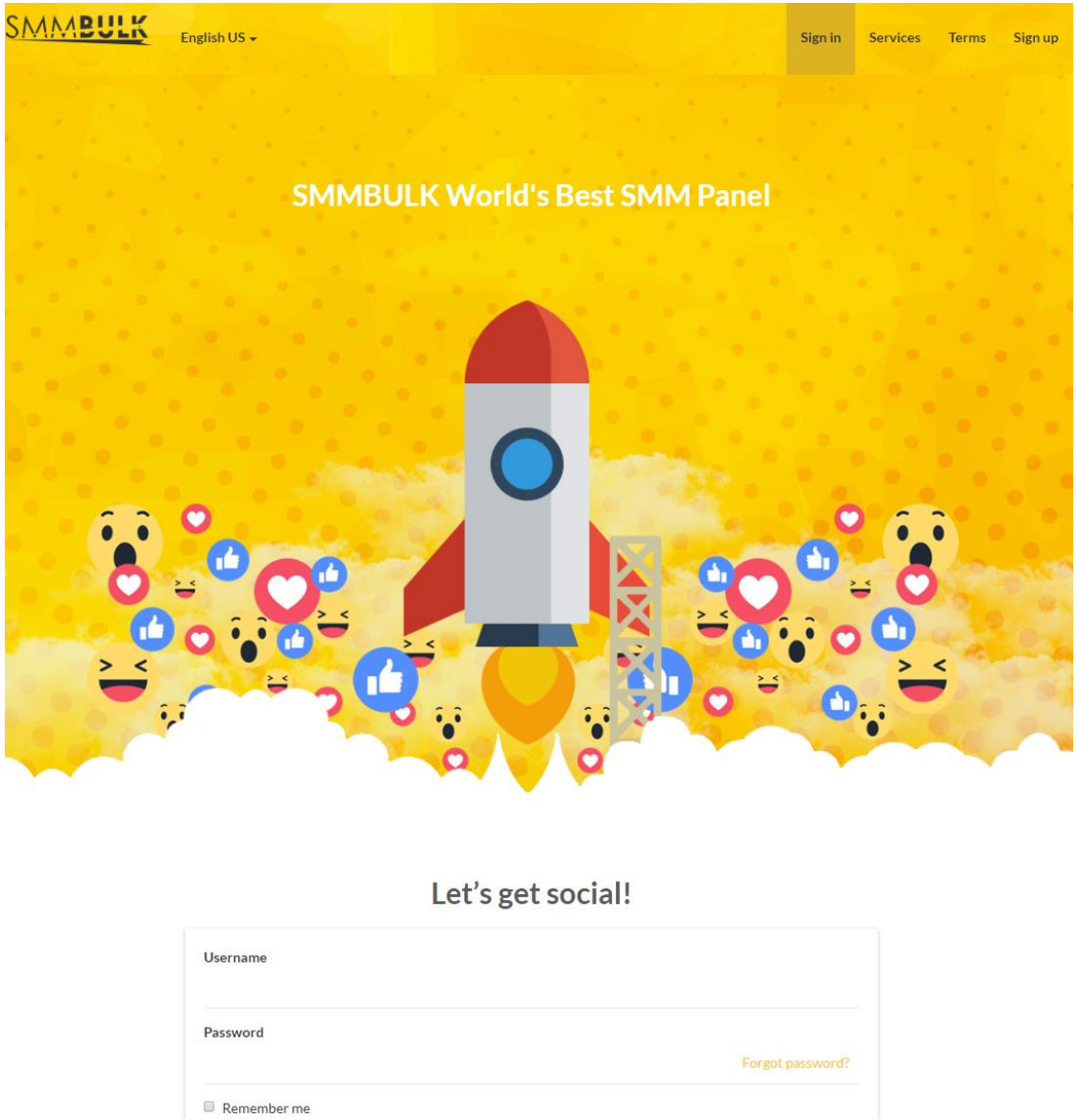

Reseller panels



Found in the decrypted traffic

```
<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},
```





	😘 SMMBULK 😘				
259	Website Hosting (Monthly) | PACKAGE 1	3.00	1	1	3$ per month 2 GB Web Space 500GB Bandwidth 20 Email Accounts 10 MySQL Databases cPanel Control Panel 10 Sub Domains 10 FTP Accounts plz contact us after order
	Instagram likes				
249	IG Likes APP1	0.70	100	1500	instagram likes app1 min 50 max 5k fast real
	Instagram Views				
253	IG Video View APP1	0.02	500	250000000	Views From REAL profile Speed 10k-50k per days min 100 max 10000000 start : 1 min to 30 min
	IG Followers (Guaranteed)				
254	IG Followers APP1 MAX 50k	5.00	10	70000	min 10 max 50k speed : 10k - 30k / day auto refill 20 day real
255	IG Followers APP2 MAX 100k	5.00	10	100000	min 10 max 100k real auto refill 20 day speed : 10k to 30k per day
257	IG Followers APP4 MAX 350k	2.50	50	350000	min 50 max 350k start : 0 to 10 min speed : 10k to 40k per day real



Category

PROMOTION (Cheap Services)

Service

Instagram Followers [30K] [R20] (70 Rs) — $1.20 per 1000

Description

(84 Rs per 1000)

- Quality = Normal !
- Start Time = Up to 12 Hours !
- Speed = Up to 4k Per Day !
- Refill = 20 Days !
- Min = 200 !
- Max = 30K !
- Specs = Refill Starts after 24 to 48 Hours from request !

Link

https://www.instagram.com/yolopouylet123/

Quantity

30000

Min: 200 - Max: 30000

Drip-feed

Charge

$36.00

Submit

What's new on SmmRoyal

NEW July 06, 2019

IG Update (06 July 19)

We are Aware that you guys are Facing issues with your IG Orders especially IG Likes Orders.

You Just need to know that Instagram added AI Interface to their System (Artificial Intelligence) and they are detecting any Robotic Activity and blocking accounts.

Our developers are currently working hard to bypass this new update.

Please note that this issue affected all platforms on the SMM is leading the way to find a quick solution.

- Thanks for your trust

SMM TEAM



Reseller panels

- Sell popularity in bulk
- All look alike



Simple Investigation N=343

Fingerprint of the web application

Domain registration information

HTML content

IP address



RISKIQ 188.165.29.223 Tours Upgrade

First Seen 2018-01-10
Last Seen 2019-07-24
ASN OVH SAS
Netblock 188.165.0.0/16
Ovh-Sas Routable Categorize

FILTERS

DOMAIN (1,273 / 1,273)

- 0rders.com 1
- 1001servis.com 1
- 10xyourmedia... 1
- 13igpromoter.... 1
- 1kview.com 1

Show More

UNIQUE RESOLVE (1 / 1,273)

- Show Uni... 1,273

STATUS

SOURCE (2 / 1,280)

- riskiq 1,273
- pingly 7

RESOLUTIONS

Show : 25 ◄ 1-25 of 1,273 ► Sort : Last Seen Descending Download Copy

Resolve	First	Last	Source	Tags
perfectpanel.com	2019-03-13	2019-07-24	pingly, riskiq	
igadder.com	2019-05-31	2019-07-24	riskiq	
fastypanel.com	2019-01-08	2019-07-24	riskiq	
plentysmm.com	2019-07-18	2019-07-24	riskiq	
iglikespro.com	2019-07-05	2019-07-24	riskiq	
smm1000.com	2019-01-31	2019-07-24	riskiq	
karyale.com	2019-01-25	2019-07-24	riskiq	
valar-smm.com	2019-01-12	2019-07-24	riskiq	
gusmm.com	2019-01-08	2019-07-24	riskiq	



The best SMM panels platform

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

Features

User panel for your customers

Where they can place orders, see orders history, add funds to balance, submit support tickets, etc.

Accept online payments

Seamlessly integrates with PayPal, Skrill, WebMoney, Perfect Money, Payza, Bitcoin, etc.

Orders processing

Connect any APIs for automated orders processing or manage orders manually.

Easy customisation

Set any currency. Change site language. Chose theme. Edit content, menu, SEO attributes and other options.

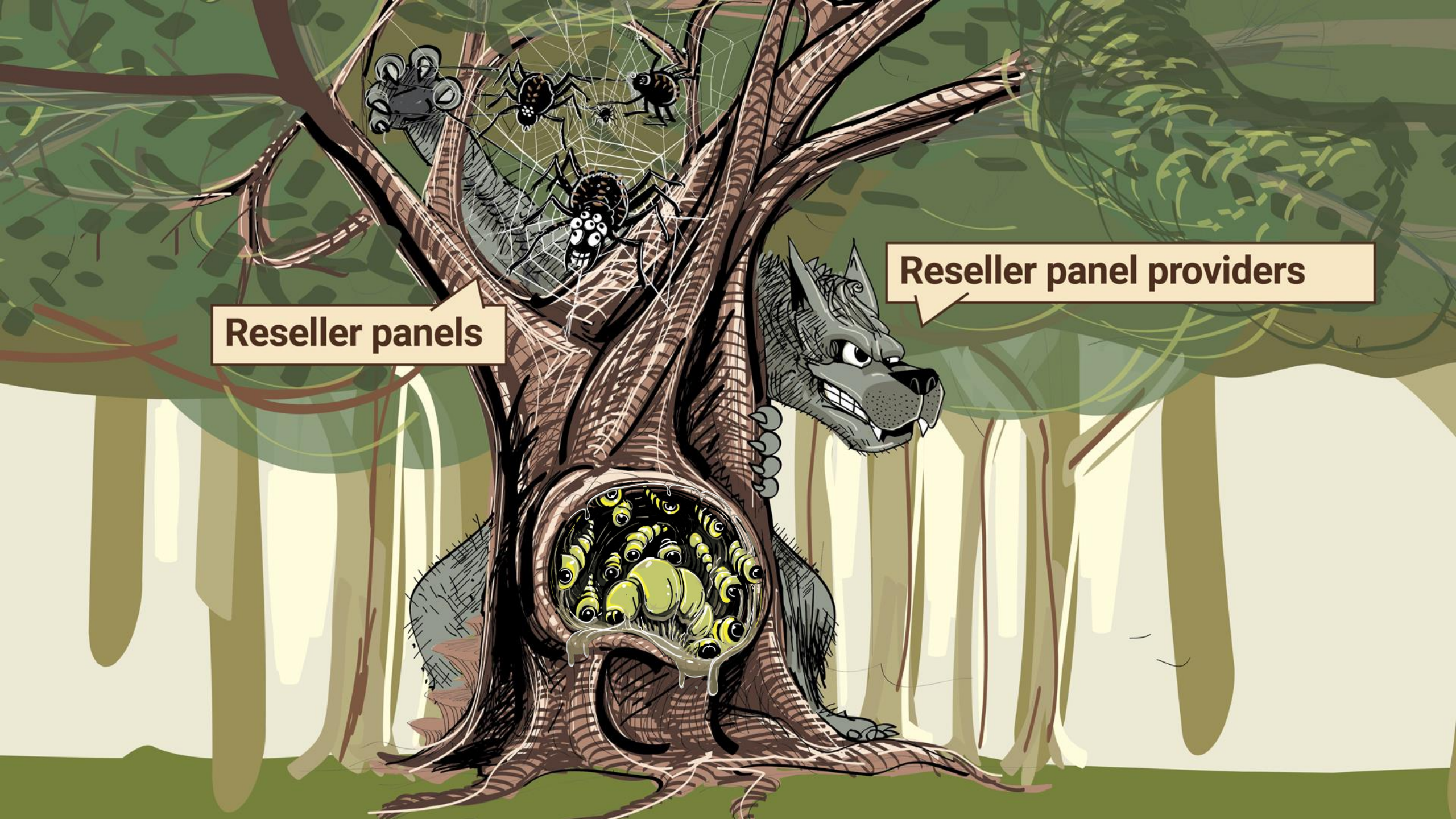
User API

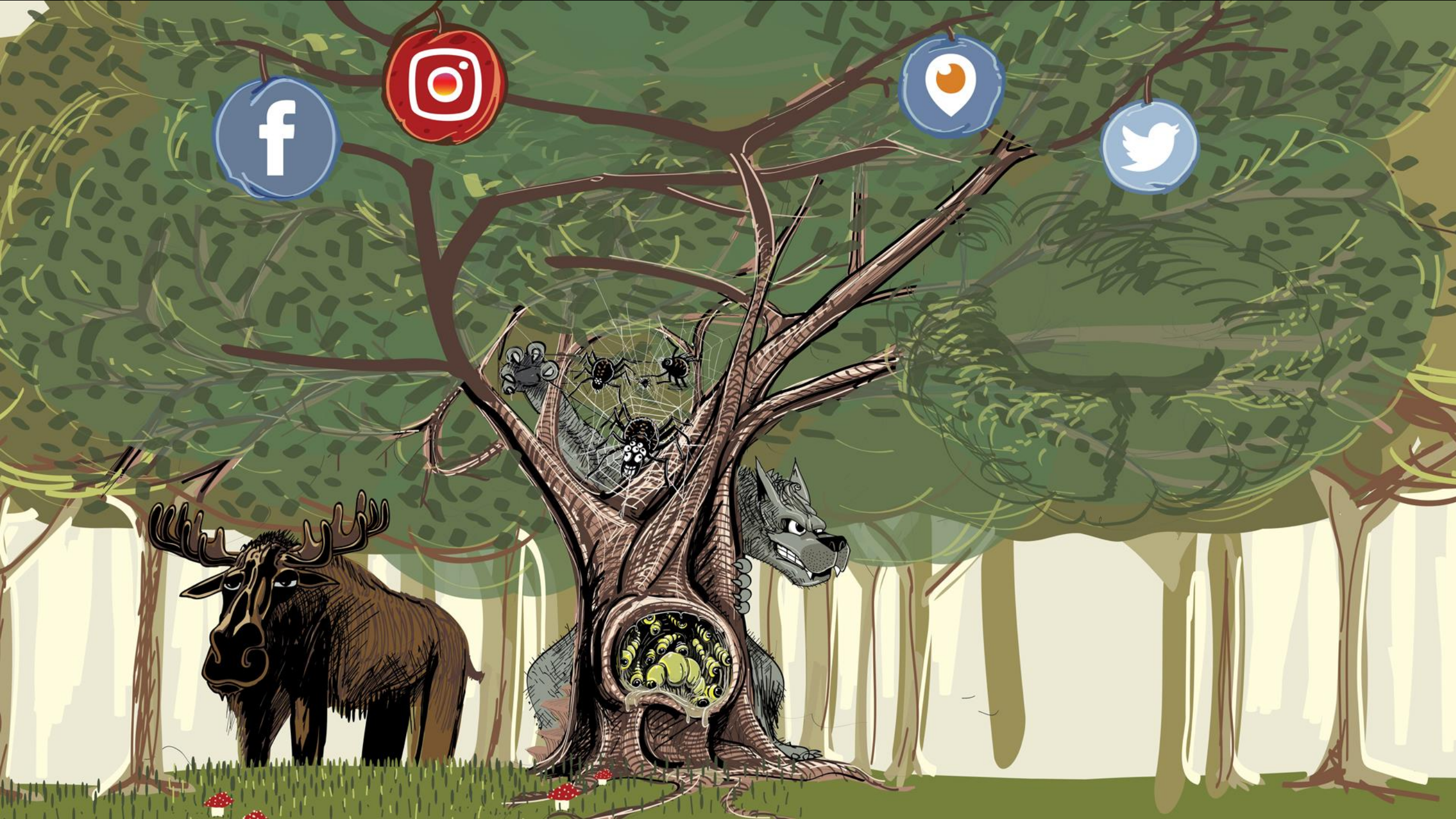
Easy-to-integrate API for your customers.

Powerful admin dashboard

Manage users, services, orders, tickets. Configure automation. Review stats. And many more.




Reseller panels
Reseller panel providers



Reseller Panel Providers

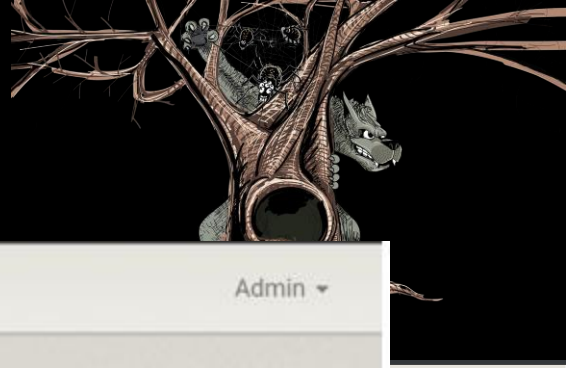


All in one solution :

- Ready to go software
- Provides web hosting
- Domain name sometimes included

Features:

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



Dashboard Settings Funds Load History Users Orders Broadcasts Refill Requests API Fetch Support Automate Admin

Admin

Create

Show

UserID
13
12
11
10
9
8
7

tion

Select an API

Select an API

https://indiansmm.com//api/v2

https://smmpapa.com/api/v2

smmpapa

https://cheapsmmindia.in/api/v2

https://cheapsmmindia.in/api/v2

https://smmlites.com/api/v2

https://indianSMM.com

https://jl.com/

demo

https://justanotherpanel.com/api/v2

FAQs Terms & Conditions Privacy Policy About Us Contact Us Version: ADVANCED

Several conversations by reseller panel owners on BlackHatWorld about *THE main provider*



May 11, 2019 #6

aixboss
Registered Member

Joined: Oct 14, 2018
Messages: 55
Likes Received: 6
Gender: Male

Jemham said: ↕

what are the SMM panel that you're using guys ? I've been using few lately but I'm not satisfied

mostly all panels using the same provider
the only difference is prices.....
many panel holders not refund money when not working the service...
They lie and keep the money or selling fake offers
If anyone knows this provider he is welcome to contact me privately.
a good one is justotherpanel but the support takes a very long time for response messages.

Several conversations by reseller panel owners on BlackHatWorld about *THE main provider*



Apr 17, 2018 #4



Daltonmediastudio
Jr. VIP
Jr. VIP

Joined:	Aug 27, 2016
Messages:	340
Likes Received:	59
Gender:	Male
Occupation:	Egypt
Location:	Online
Home Page:	https://smmfansfaster.com/

no one will reveal the main provider
for them he is their hidden ghost

Several conversations by reseller panel owners on BlackHatWorld about *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

Several conversations by reseller panel owners on BlackHatWorld about *THE main provider*



Jan 6, 2019 #19

ellay
Jr. VIP
Jr. VIP

Joined: Nov 25, 2017
Messages: 1,245
Likes Received: 416
Home Page: https://www.smmstudia.com

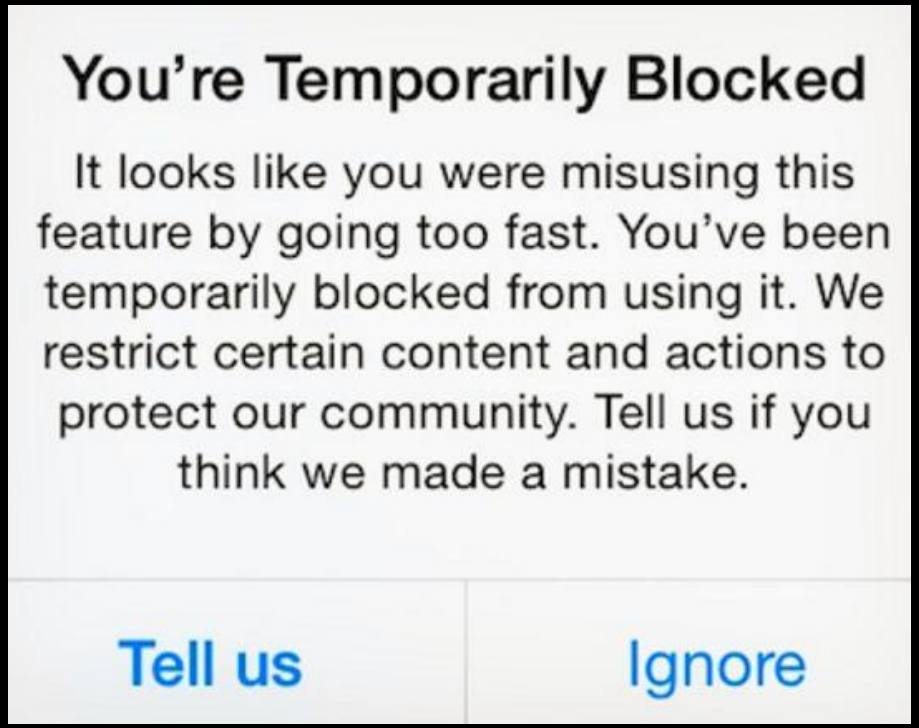
There cannot be 1 provider. They are several. Some panels also are providers. Big panels provide the most of the services and they are reselling each other services. (connected via API)

Where do we stand?



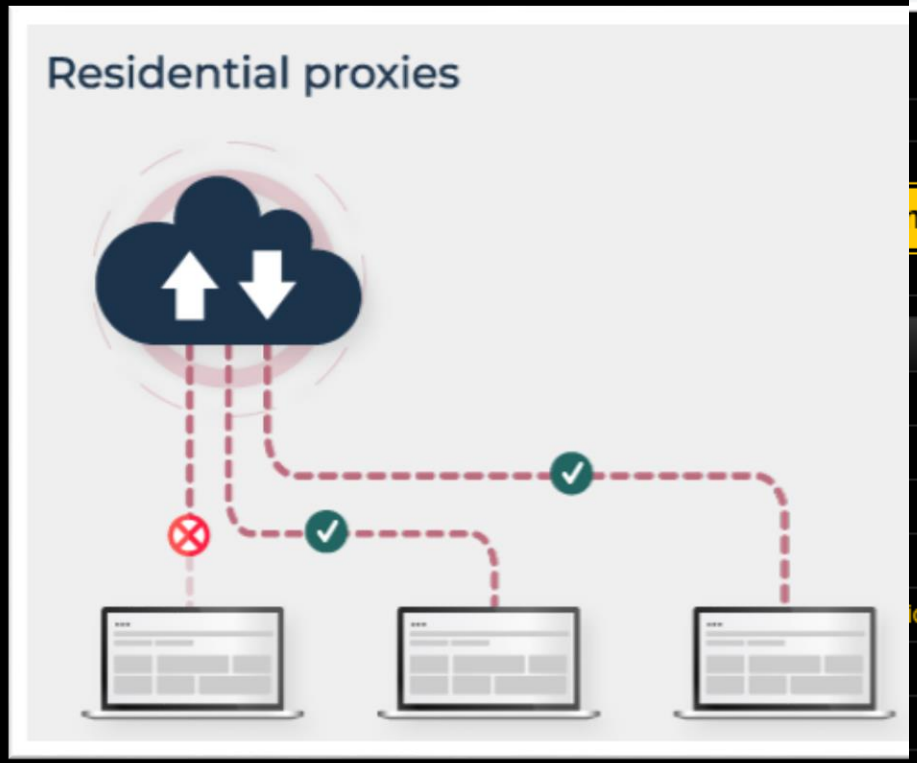
- A system of resellers and reseller panel providers
- Automation software to create and orchestrate fake accounts

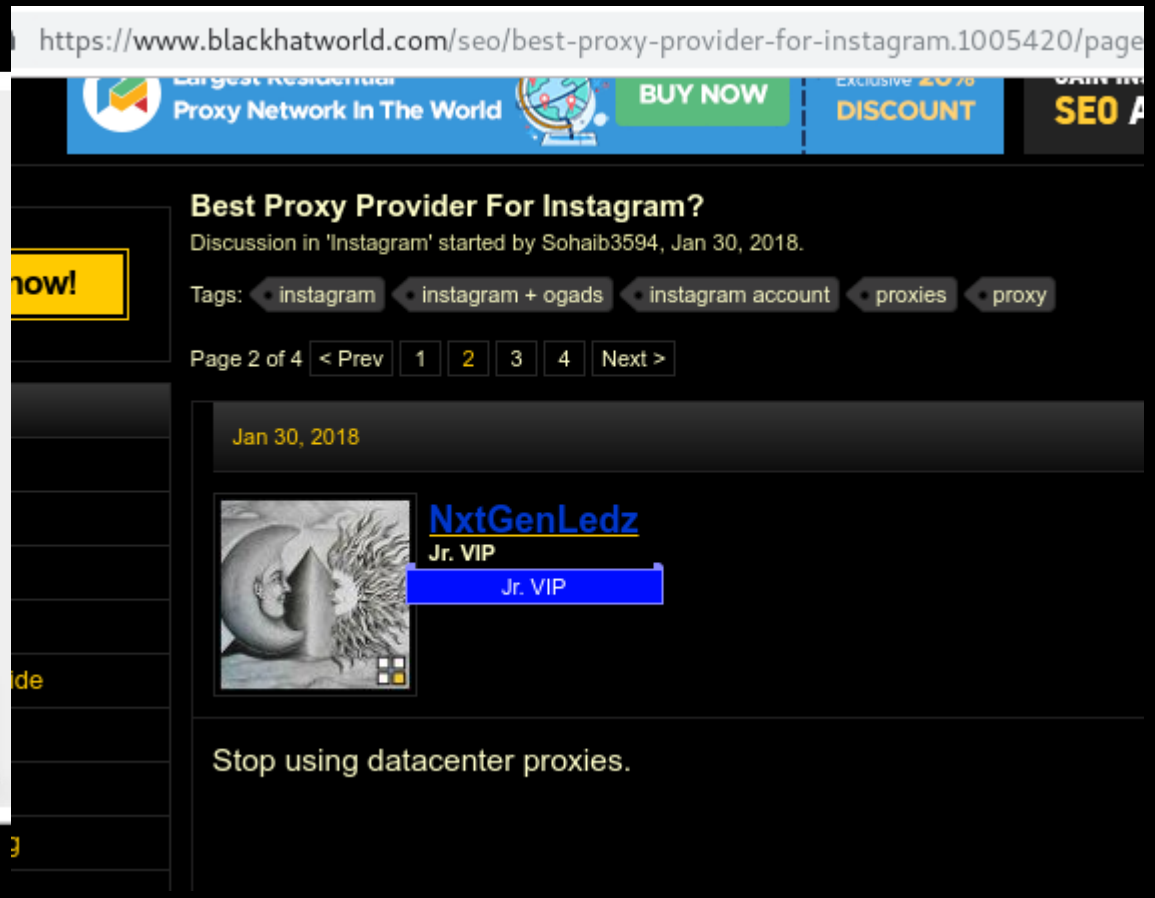




Working around Blocks

- Automation software supports proxy lists





A New Actor Enters the Game



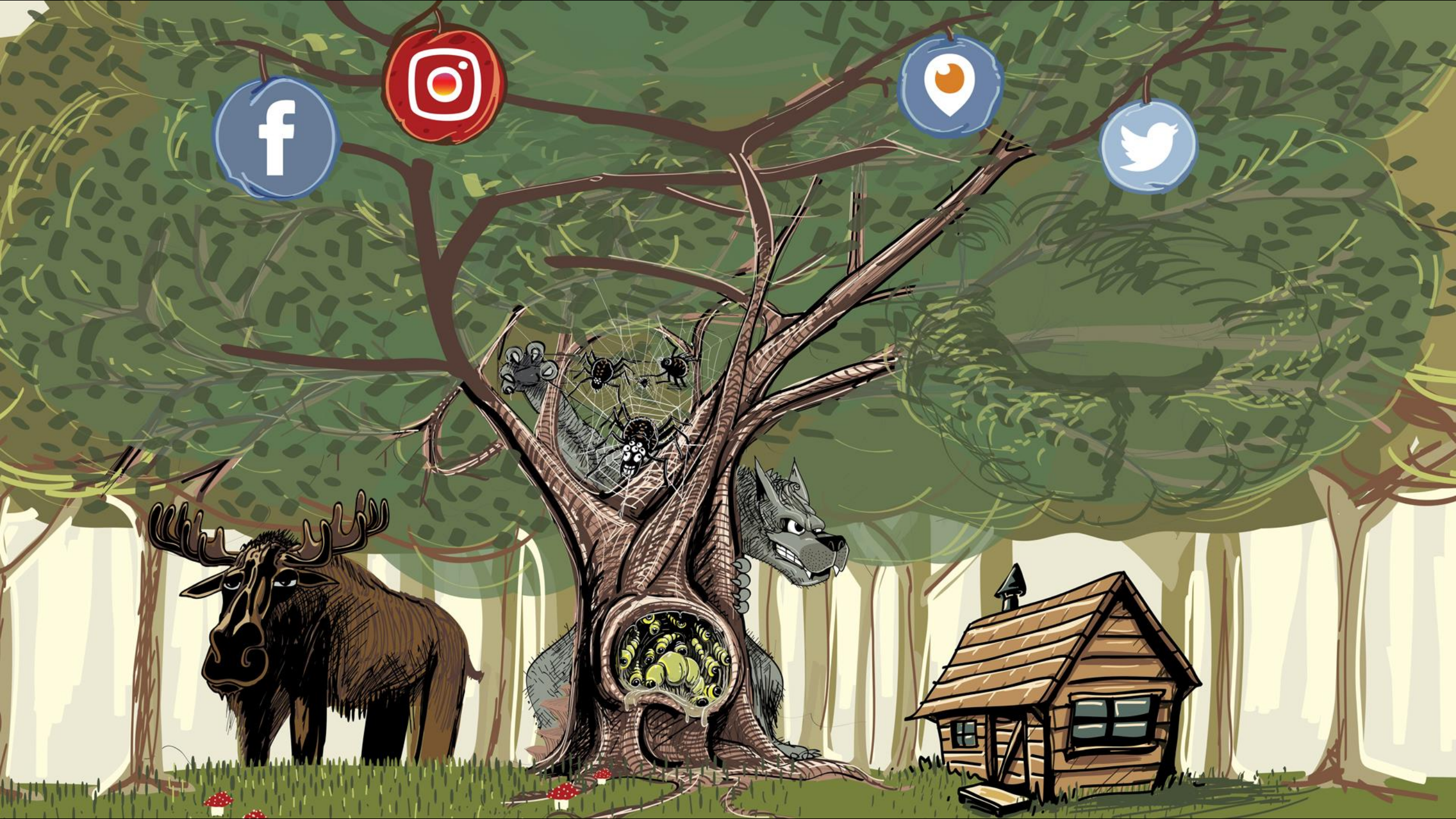
Previously Studied Botnet



Residential Proxy Services

Residential proxy services





Recommended residentia | Buy Highest Quality Insta | Monetize inactive app use | Buy Reverse Backconnect

Incognito

Luminati is honored to receive, from the leading industry research firm Frost & Sullivan the Market Leadership Award 2019

Luminati

Networks Tools Use cases Resources Pricing Contact Log in Sign up

Residential Proxy Network

Luminati provides the most advanced Residential Proxy service offering the fastest and largest real-peer IP network in the world.



Start Now

Start Your 7-day Free Trial Today!

Use cases



Ad Verification Services

Verify advertisements and affiliate link compliance along with the absence of malware



Price Comparison

Aggregate and compare accurate pricing data for retail, travel and eCommerce to ensure a competitive advantage with geo-located IPs



Market Research Services

Analyze business and market environments worldwide for well-informed decision making



Web Data Extraction

Collect accurate data using 35+ million rotating IPs from across the globe, never getting blocked or misled



Brand Protection

Protect your brand and all online assets by ensuring proper use of copyright content

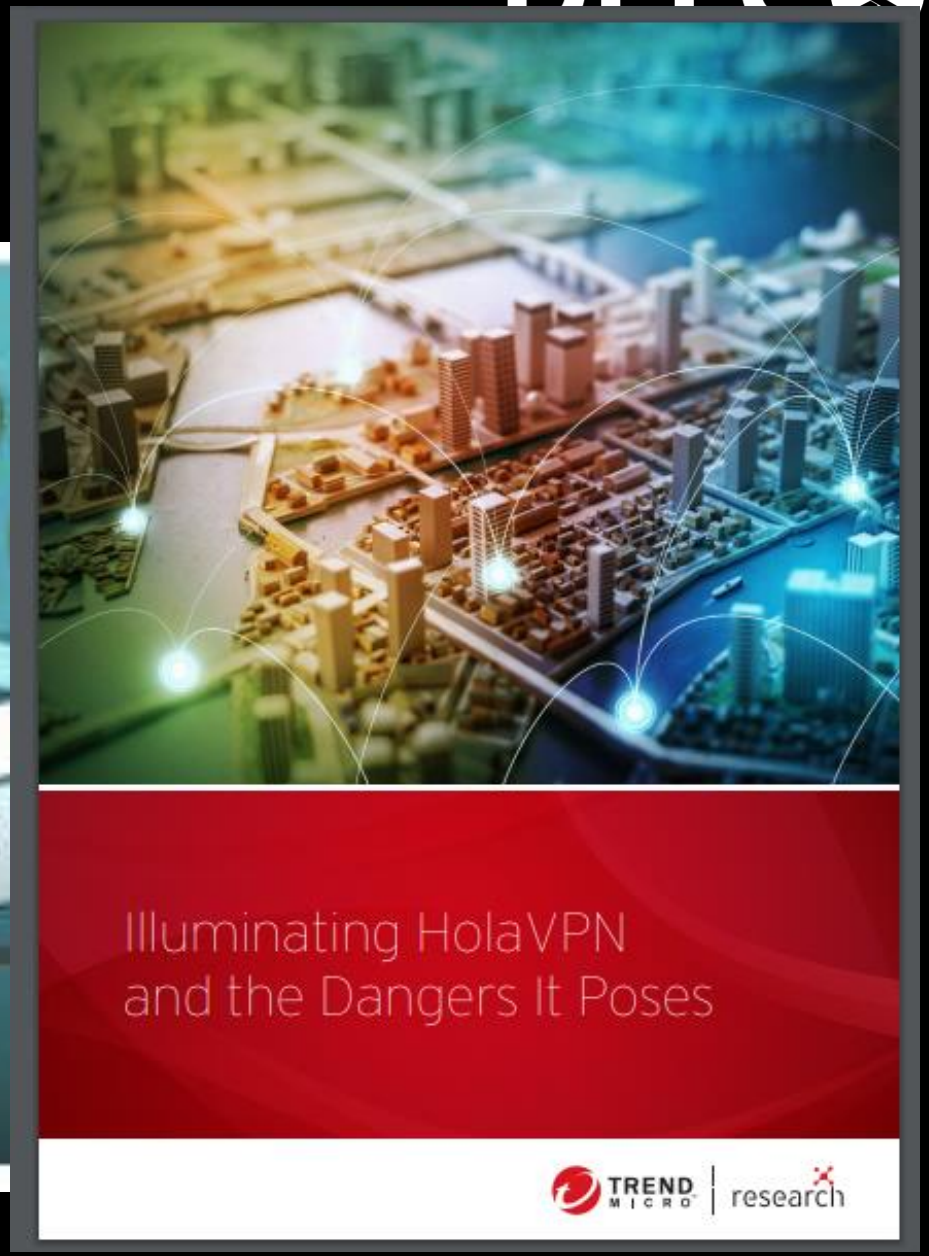


Account Management

Manage social media accounts including Facebook, Twitter, Linkedin, Craigslist, eBay and more, without getting banned o disabled

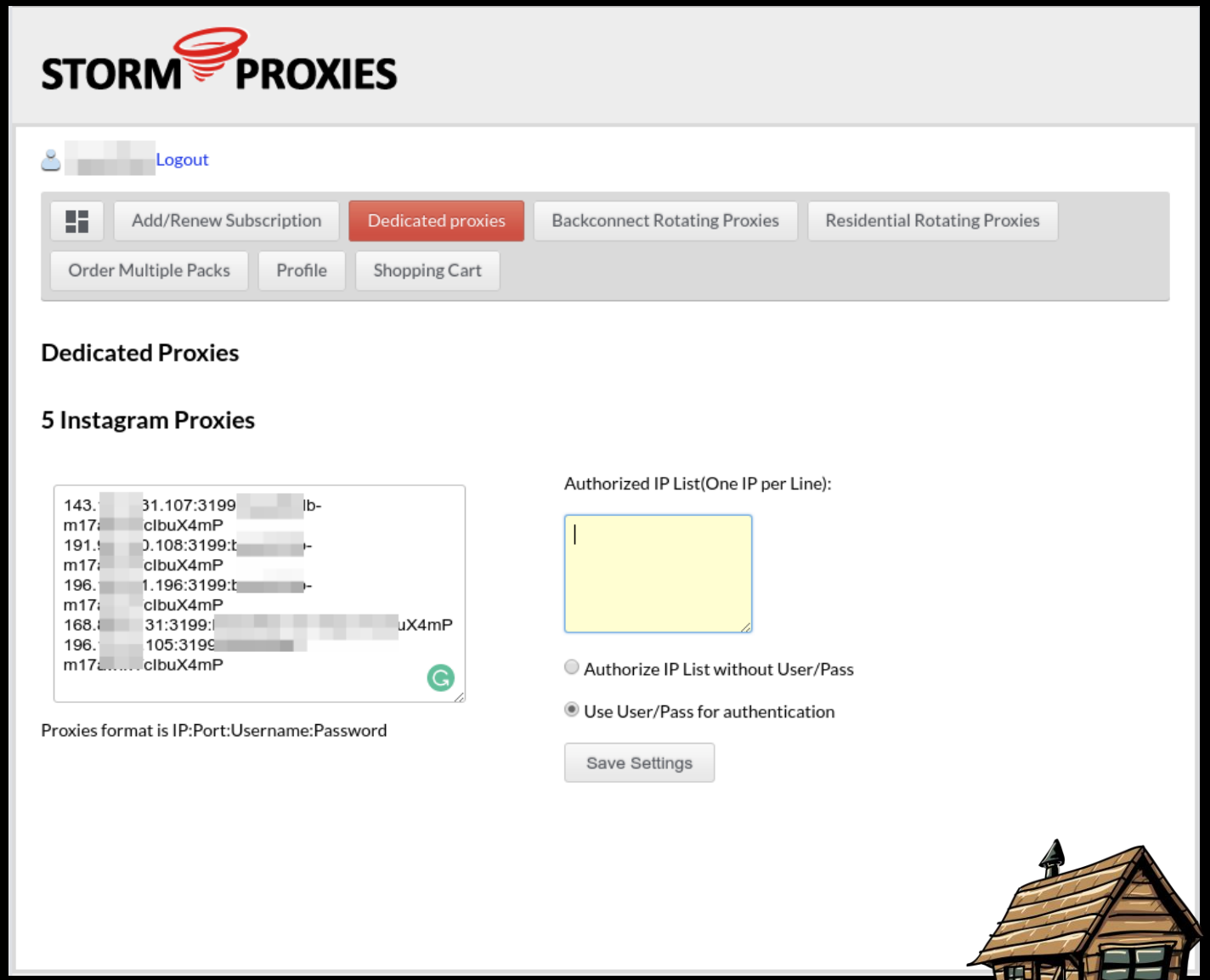
Shocking Business Model





Storm Proxies

- Received IPs from USA: Kansas City, Lincoln NE and Sunnyvale CA
- ISPs have conflicting information:
  - Digital Energy Technologies Chile with Org Host1Plus
  - Victoria Mahe with Org Joe's Datacenter, LLC
- Traceroute leads to the US



Storm Proxies (cont)

- Uses Squid for proxying
- Doesn’t protect scans to localhost
- Linux system
- Most likely Debian Jessie
  - Exim 4.84_2
  - Squid 3.4.8

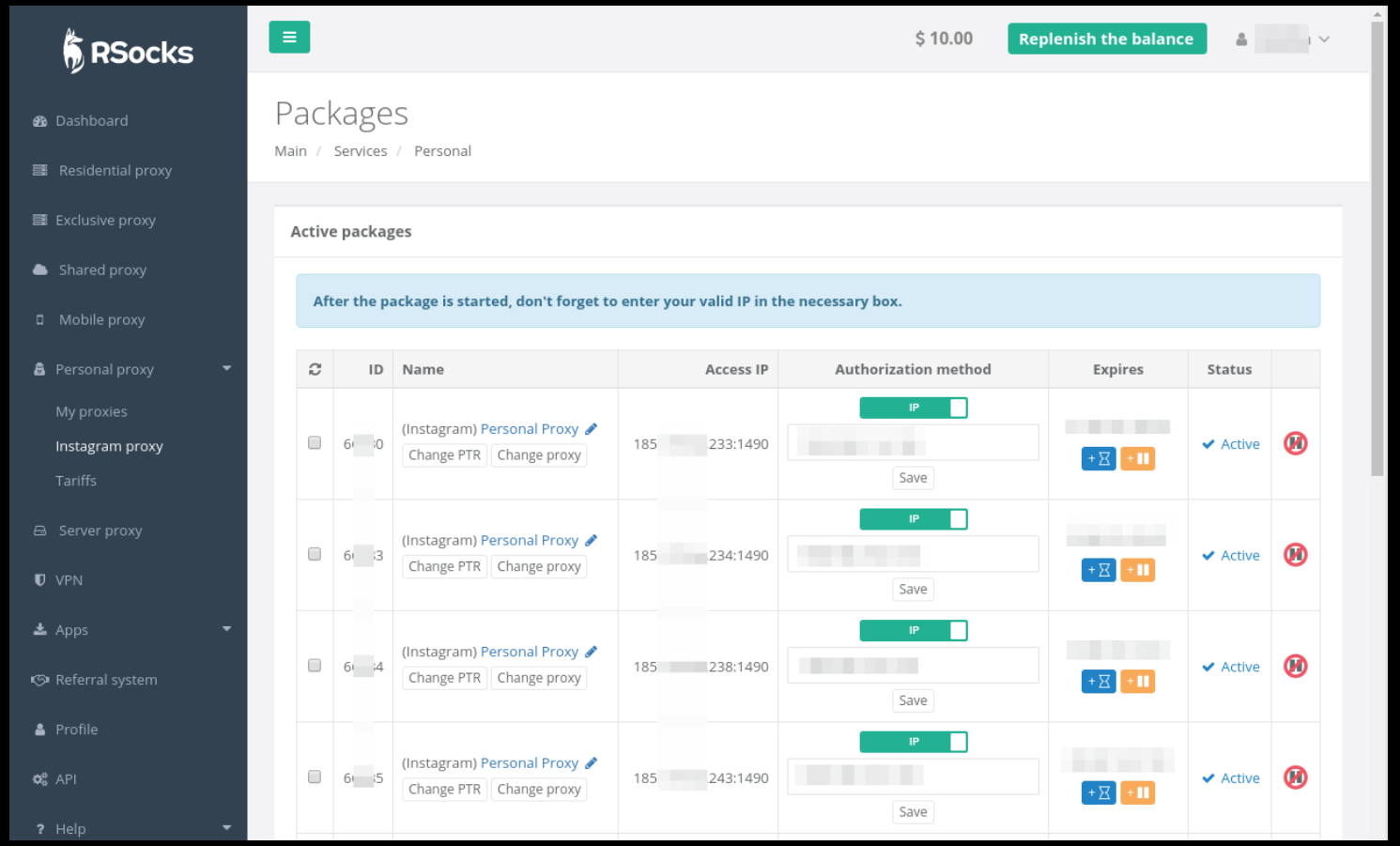
```
Nmap scan report for 191 [redacted] 108
Host is up (0.071s latency).
Not shown: 65531 closed ports
PORT      STATE    SERVICE    VERSION
111/tcp   open     rpcbind    2-4 (RPC #100000)
3199/tcp  open     http-proxy Squid http proxy 3.4.8
11211/tcp filtered unknown
46082/tcp open     status     1 (RPC #100024)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
Network Distance: 16 hops
```

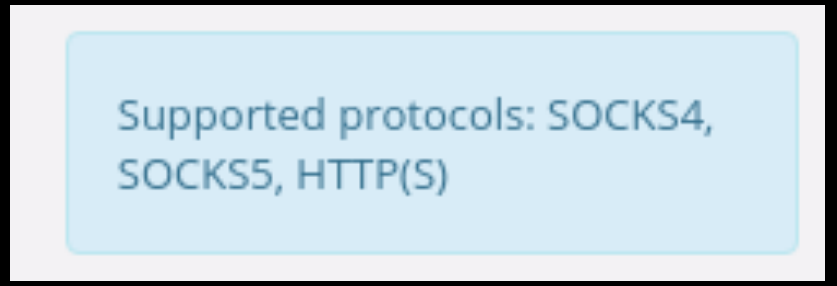
```
"IP";"FQDN";"PORT";"PROTOCOL";"SERVICE";"VERSION"
"127.0.0.1";"localhost";"25";"tcp";"smtp";"Exim smtpd 4.84_2"
"127.0.0.1";"localhost";"111";"tcp";"rpcbind";"2-4 (RPC #100000)"
```



RSocks

- Received IPs all from same subnet in Russia
- ISP: Adman LLC
- Traceroute confirms Russia







RSocks (cont)

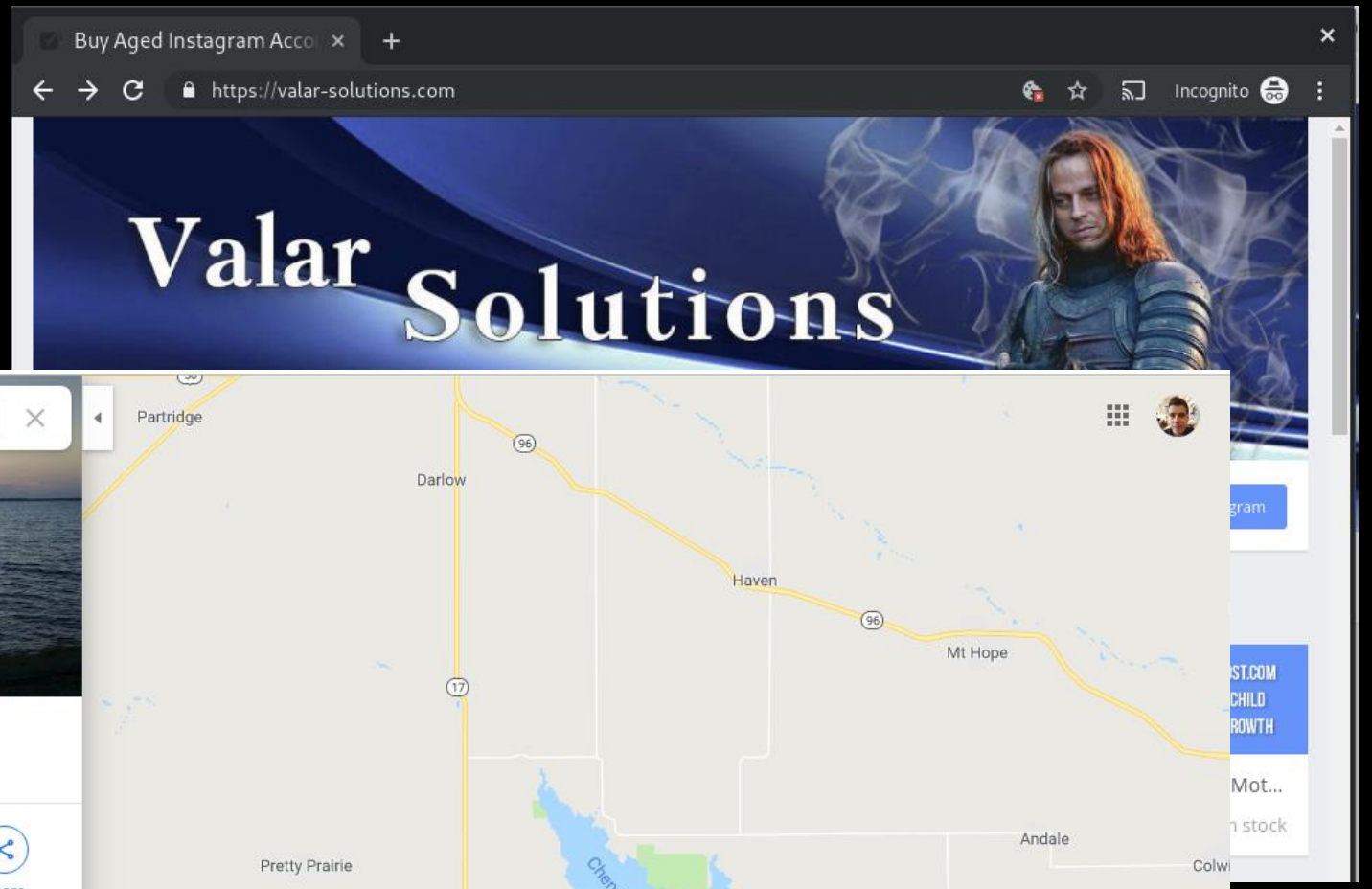
- Exposes SSH on 3389
- Doesn’t protect scans to localhost
- Unable to fingerprint proxy service
- Most likely Debian Jessie
  - SSH banner deb8u7

```
"127.0.0.1";"localhost";"3000";"tcp";"tcpwrapped";""
"127.0.0.1";"localhost";"3128";"tcp";"tcpwrapped";""
"127.0.0.1";"localhost";"3306";"tcp";"tcpwrapped";""
"127.0.0.1";"localhost";"3389";"tcp";"ssh";"OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)"
"127.0.0.1";"localhost";"3986";"tcp";"tcpwrapped";""
"127.0.0.1";"localhost";"4899";"tcp";"tcpwrapped";""
"127.0.0.1";"localhost";"5000";"tcp";"tcpwrapped";""
"127.0.0.1";"localhost";"5009";"tcp";"tcpwrapped";""
```



Valar Solutions

- Received a single IP from France
  - Scaleway, D
- Traffic goes d
  address in th
  - AT&T Inter





Valar (cont)

- Uses 3Proxy
  - on 1067 non-continuous ports
  - Identified by nmap
  - Confirmed by error message strings that match source code
- Protects from localhost scans
  - Both IPv4 and IPv6
- IPv6 sealed from outside
- Proxy entry is Debian 9
  - Nginx + OpenSSH

```
Nmap scan report for 140-[redacted]-212.rev.cloud.scaleway.com (212.[redacted].140)
Host is up (0.099s latency).
Not shown: 64467 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
80/tcp    open     http       nginx 1.10.3
10012/tcp open     http-proxy 3Proxy http proxy
10028/tcp open     http-proxy 3Proxy http proxy
10058/tcp open     http-proxy 3Proxy http proxy
10121/tcp open     http-proxy 3Proxy http proxy
10134/tcp open     http-proxy 3Proxy http proxy
10135/tcp open     http-proxy 3Proxy http proxy
10154/tcp open     http-proxy 3Proxy http proxy
10365/tcp open     http-proxy 3Proxy http proxy
10710/tcp open     http-proxy 3Proxy http proxy
10750/tcp open     http-proxy 3Proxy http proxy
10806/tcp open     http-proxy 3Proxy http proxy
10905/tcp open     http-proxy 3Proxy http proxy
10912/tcp open     http-proxy 3Proxy http proxy
```



Residential Proxy Providers Summary

	Infrastructure	Geoip / Whois	Powered by Malware?
Luminati	Leveraging willing participants' phones	Unknown	Unlikely
Storm Proxies	Debian 8 (Jessie) with Squid	Misleading information	Unlikely
RSocks	Debian 8 (Jessie) with unknown proxy	Small unknown ISP	Unlikely
High Proxies	CentOS/RHEL 7 with Squid	Misleading information	Unlikely
Valar Solutions	Debian 9 (Stretch) with 3Proxy. Tunnel between France and USA. IPv6.	Legit AT&T Internet Services	Unlikely



For More

Resident Evil: Understanding Residential IP Proxy as a Dark Service

Xianghang Mi*, Xuan Feng*, Xiaojing Liao*, Baojun Liu†,
XiaoFeng Wang*, Feng Qian*, Zhou Li‡, Sumayah Alrwais§, Limin Sun¶, Ying Liu†
*Indiana University Bloomington, †Tsinghua University, ‡IEEE Member,
§King Saud University, ¶Institute of Information Engineering, CAS
*{xmi, xf1, xliao, xw7, fengqian}@indiana.edu, †lbj15@mails.tsinghua.edu.cn,
liuying@cernet.edu.cn, ‡lzcarl@gmail.com, §salrwais@ksu.edu.sa, ¶sunlimin@iie.ac.cn,

***Abstract*—An emerging Internet business is residential proxy (RESIP) as a service, in which a provider utilizes the hosts within residential networks (in contrast to those running in a datacenter) to relay their customers' traffic, in an attempt to avoid server-side blocking and detection. With the prominent roles the services could play in the underground business world, little has been done to understand whether they are indeed involved in Cybercrimes and how they operate, due to the challenges in identifying their RESIPs, not to mention any in-depth analysis on them.**

In this paper, we report the *first* study on RESIPs, which sheds light on the behaviors and the ecosystem of these elusive gray services. Our research employed an infiltration framework, including our clients for RESIP services and the servers they visited, to detect 6 million RESIP IPs across 230+ countries and 52K+ ISPs. The observed addresses were analyzed and the hosts behind them were further fingerprinted using a new profiling system. Our effort led to several surprising findings

owners) as intermediaries to circumvent the restrictions imposed by target services, for the purposes such as aggressive resource access (e.g., registering multiple accounts), data scraping, and others. This emerging market gives rise to a new service model we call *Residential IP Proxy as a Service* (RPaaS), offered by companies like Luminati [3], StormProxies [49], Microleaves [38], etc. These providers all control a large number of residential hosts, which they claim joined their services willingly, to proxy their customers' communication with any Internet target. Once abused, these residential proxies can outperform conventional public proxies or even anonymity networks to help their clients masquerade as clean and benign sources to communicate with the targets. Such communication may violate the target's service terms at the very least (e.g.,



Where do we stand?

- IoT botnet or residential proxy services
- Automation software
- Reseller panels and reseller panel providers

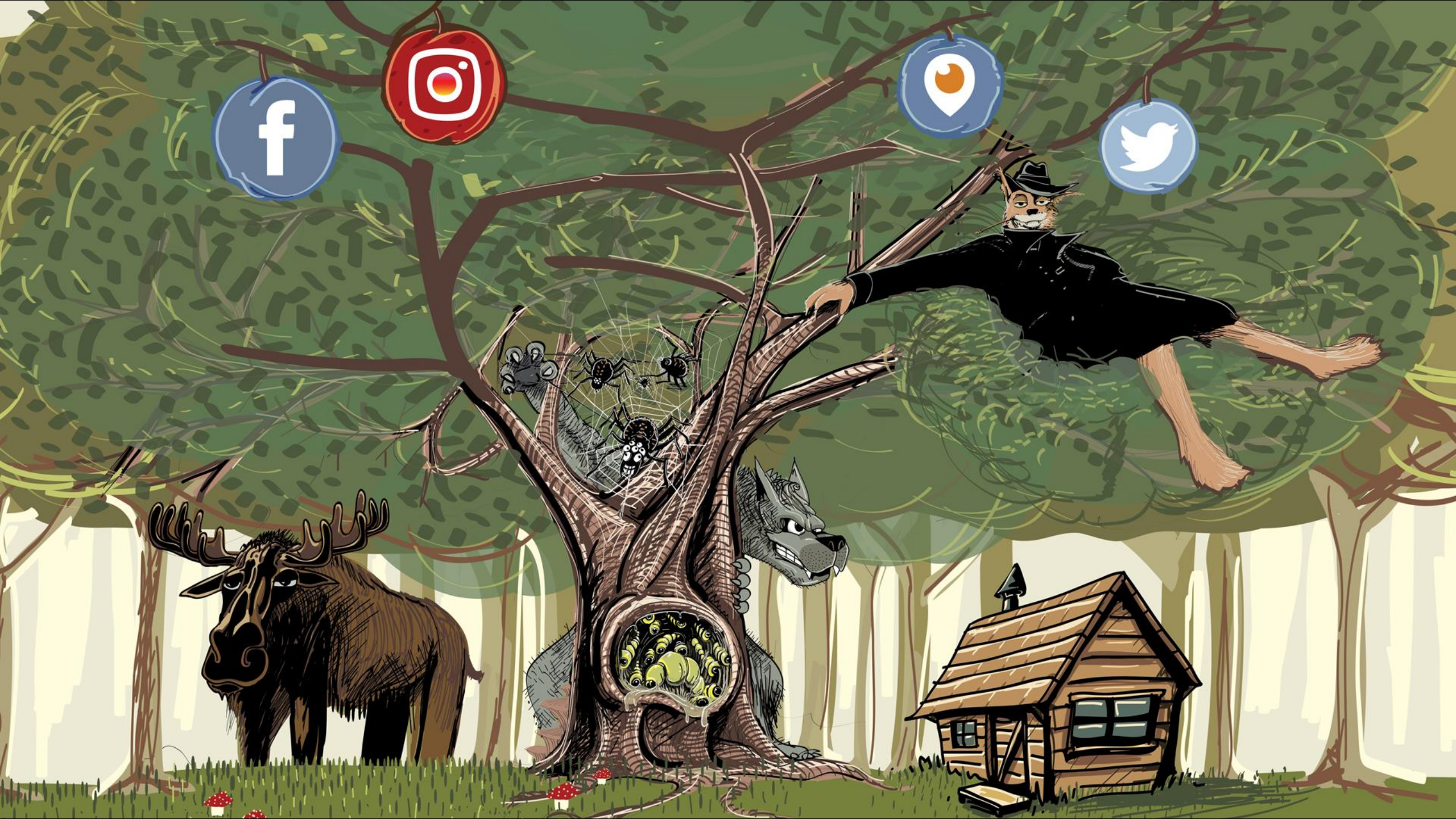






Who buys from reseller panels?


Customer-facing sellers



Devumi will be performing scheduled maintenance on January 30th. We apologize in advance for any inconvenience.

Devumi SOCIAL MEDIA MARKETING

TWITTER YOUTUBE SOUNDCLOUD ALL SERVICES Log in ORDER NOW

Accelerate Your Social Growth

Quickly gain followers, viewers, likes & more
with our blend of marketing tactics.

GET STARTED NOW

Your Social Media Success Starts Right Here

From trending tweets, to viral videos. We make it happen.



Español

Attorney General James Announces Groundbreaking Settlement With Sellers Of Fake Followers And "Likes" On Social Media

Settlement is First in the Country to Find that Selling Fake Followers and "Likes" Is Illegal Deception and that Fake Activity Using Stolen Identities Is Illegal Impersonation

Attorney General's Press Office: (212) 416-8060

nyag.pressoffice@ag.ny.gov

Press Release Archive

- July 2019
- June 2019
- May 2019

Devumi will be performing scheduled maintenance on January 30th. We apologize in advance for any inconvenience.

Devumi SOCIAL MEDIA MARKETING

TWITTER YOUTUBE SOUNDCLOUD ALL SERVICES Log in ORDER NOW

Devumi.top is no longer accepting new clients

If you're interesting in buying views, we suggest choosing a well rated and reliable service provider.

Find The Best Alternative

SocialBoss.Org - innovative social media promotional solutions (Instagram, Twitter, YouTube ...).

InstaGrowing.Net - High-Quality Instagram Likes, Views and Followers

YoutubeGrow.Com - High-Quality Youtube Views, Subscribers and Likes

Your Social Media Success Starts Right Here

From trending tweets, to viral videos. We make it happen.


Buyers



Potential Buyers

Linux/Moose

86% of the relayed traffic focused on Instagram

List of potential customers:

522 accounts

Method:

Content analysis



Entertainment Industry (20%)



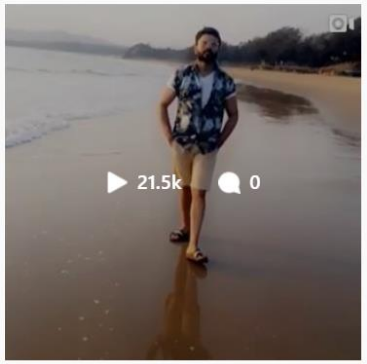


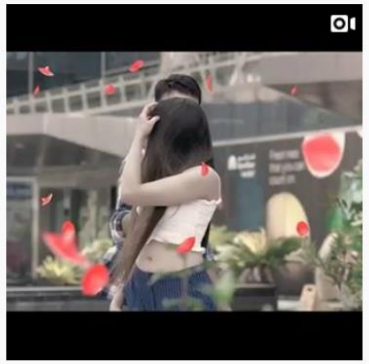
being_gg_official Follow

1,265 posts 446k followers 1,984 following

Gaurav Goyal
https://youtu.be/Z2u9rWR-2EU

POSTS IGTV TAGGED















zain_aliraqofficial Follow

272 posts 30.9k followers 78 following

Zain Al Iraqi
اغنيتي الجديدة دهن العود
youtu.be/ipQBsMbpNoQ

POSTS TAGGED













Selling Products and Services (21%)



asian_wardrobe **Follow**

69 posts **41** followers **64** following

Asian Wardrobe
PLEASE FOLLOW kuro_neko !! This shop is close!

POSTS TAGGED



kuro_meow ~Pre-order~
Code: CA003











johan_silverman_paris **Follow**

884 posts **11.4k** followers **269** following

JOHANSILVERMAN
ARTISAN FINE JEWELRY made in Italy

POSTS TAGGED

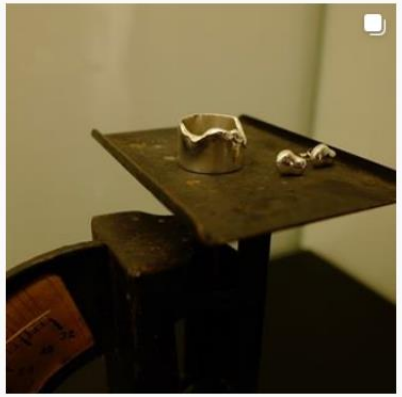




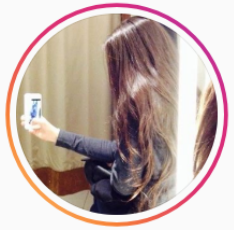








Personal Profiles (26%)



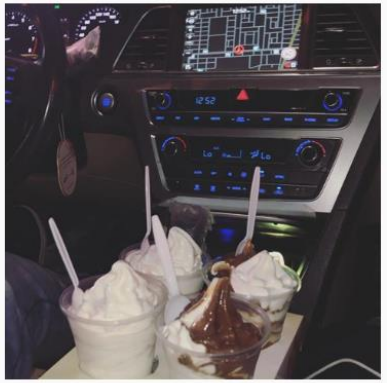
x12.ii **Follow**

218 posts **12.6k** followers **599** following

فيف
الاحساء
Simple life
انا كما انا لا اشبه الا نفسي.

POSTS TAGGED










hashtagandyr **Follow**

190 posts **17.4k** followers **665** following

Andy Rouhafzai

POSTS TAGGED








The Unexpected Ones



fadel.albarwari Follow

1,368 posts 90.6k followers 13 following

اللواء فاضل البرواري
General fadhil ALbarwari head of Iraqi special operations forces
Snapchat:/fadhil.barwary
www.facebook.com/FadelalBarwari

POSTS TAGGED















lanicayetano Follow

150 posts 6,624 followers 30 following

Lani Cayetano
She believed she could, so she did - R. S.Grey 🙏💃
CHRISTian, Wife, Rep., 2nd District of Taguig
www.facebook.com/176006225765209/posts/2646661925366281?s=596733469&sf...

POSTS TAGGED

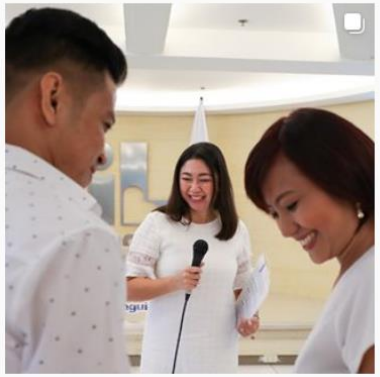












The Fascinating Ones





valeria_karat **Follow**

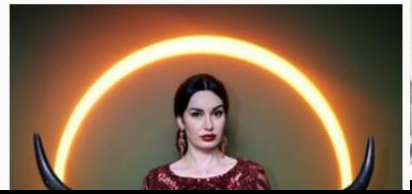
956 posts **141k** followers **1** following

Валерия Карат - Королева Магии
Ясновидящая/Целитель/Экстрасенс
запись 👉@valeria_karat_nyc
♠ READING
♦ PSYCHIC
♣ SPIRITUAL
♥ MAGIC
+1(332)255-6761 505 Brighton Beach Avenue
youtu.be/h404gT8p6WQ

POSTS TAGGED







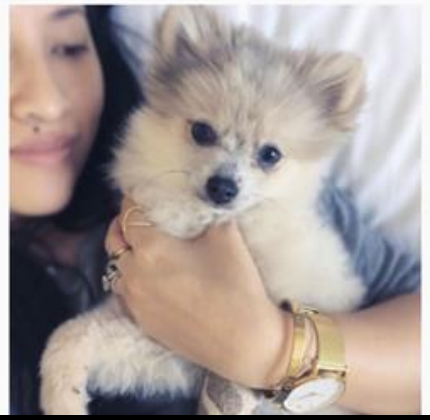
dogswithmoremoneythanyou **Follow**

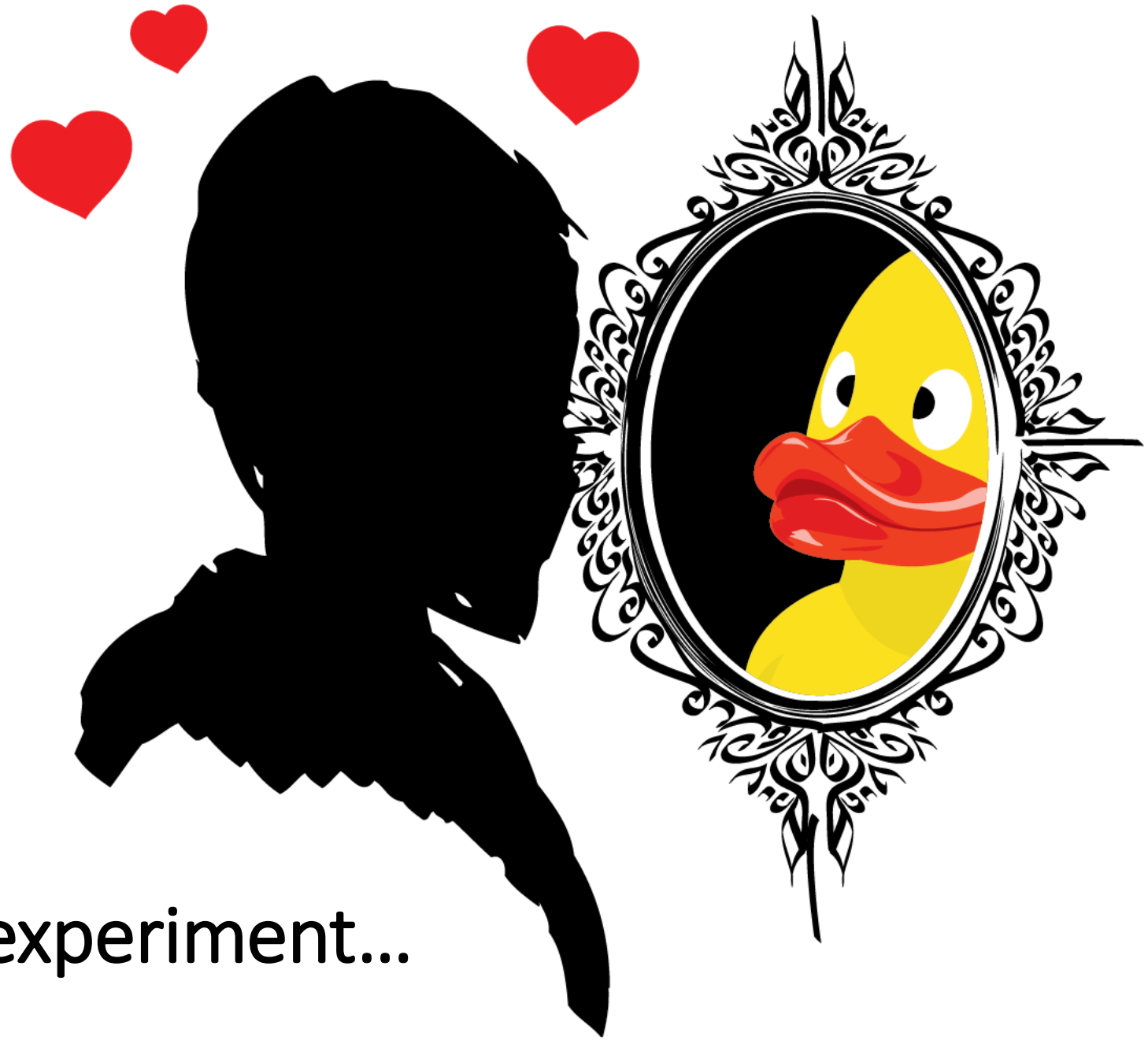
26 posts **5,500** followers **87** following

Dogs With More Money Than You You want to hate them but they're just so damn cute 💎💸👸💸💎 #dogswithmoremoneythanyou or tag to get featured!



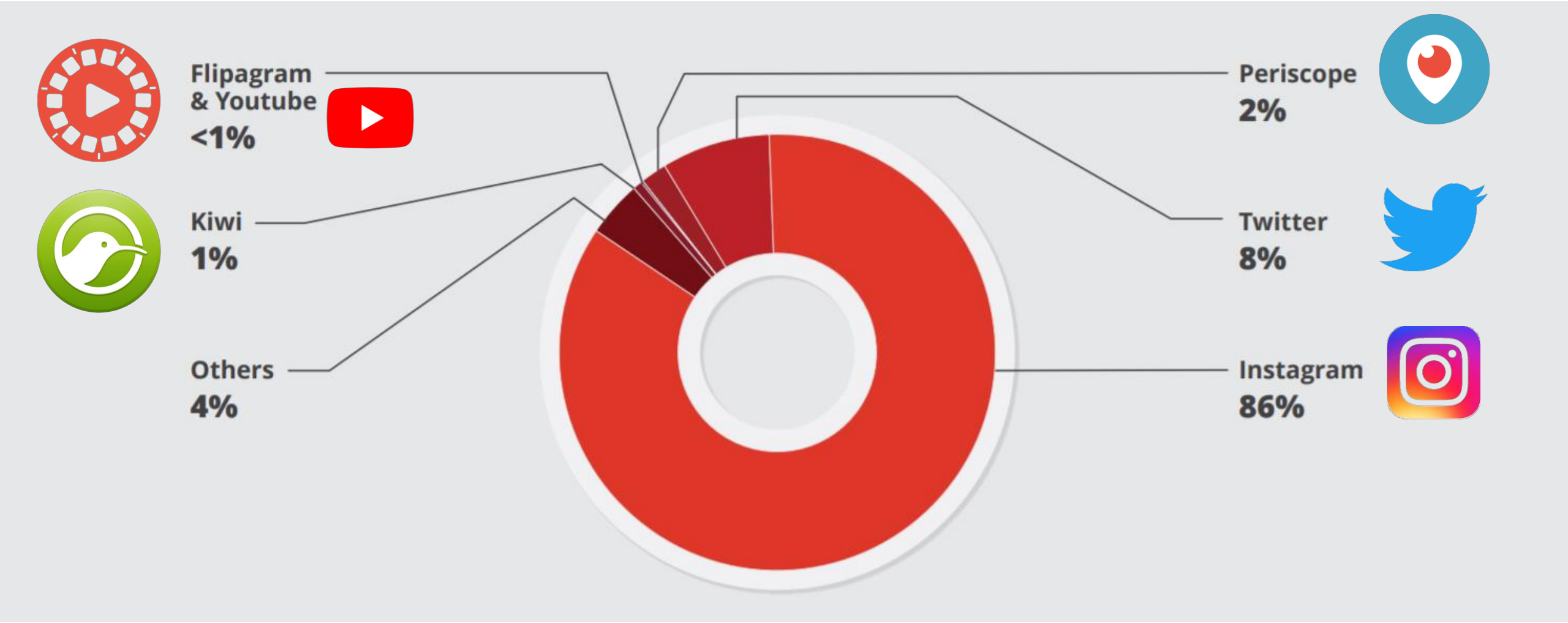




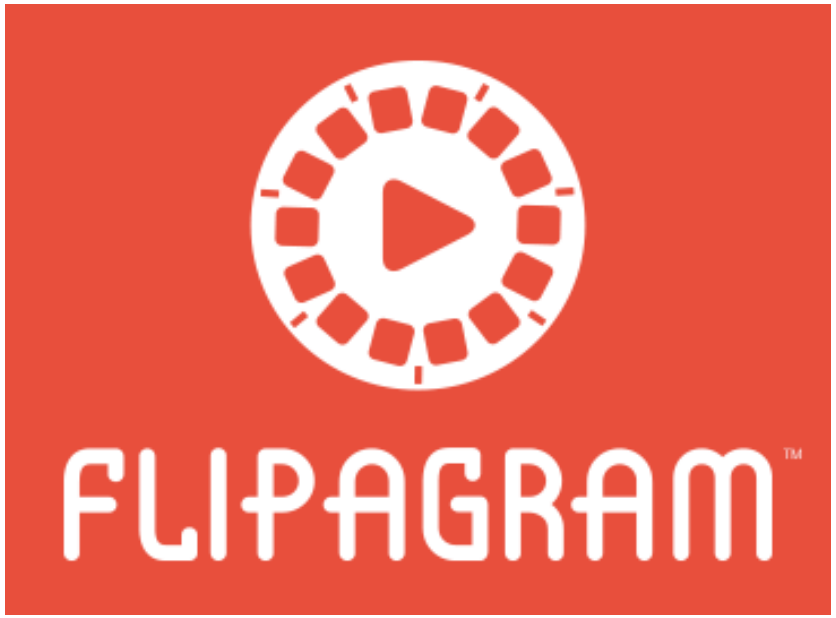



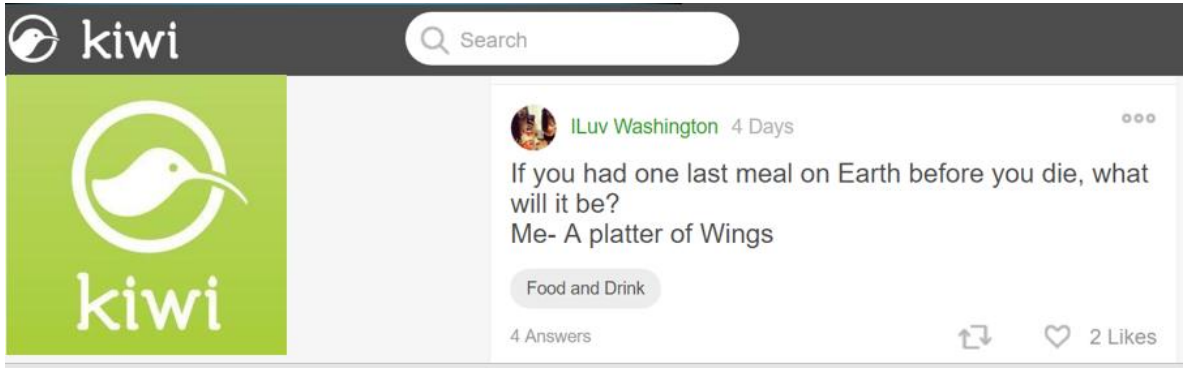
We made an experiment…

Linux/Moose's Targeted Social Networks




Periscope


FLIPAGRAM™


kiwi
Search
kiwi
ILuv Washington 4 Days
If you had one last meal on Earth before you die, what will it be?
Me- A platter of Wings
Food and Drink
4 Answers
2 Likes





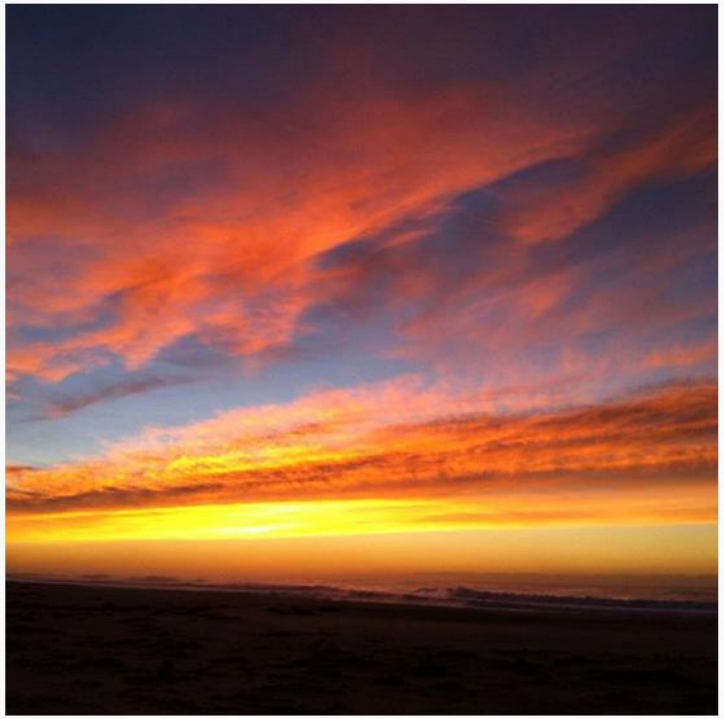
beautifulbird33

Edit Profile

Marika I'm a young photographer. Just starting on social media. Follow me for outstanding seasonal photos. For now: White and Cold; Gloomy and Sparkling.

8 posts **8,054** followers **72** following

POSTS TAGGED





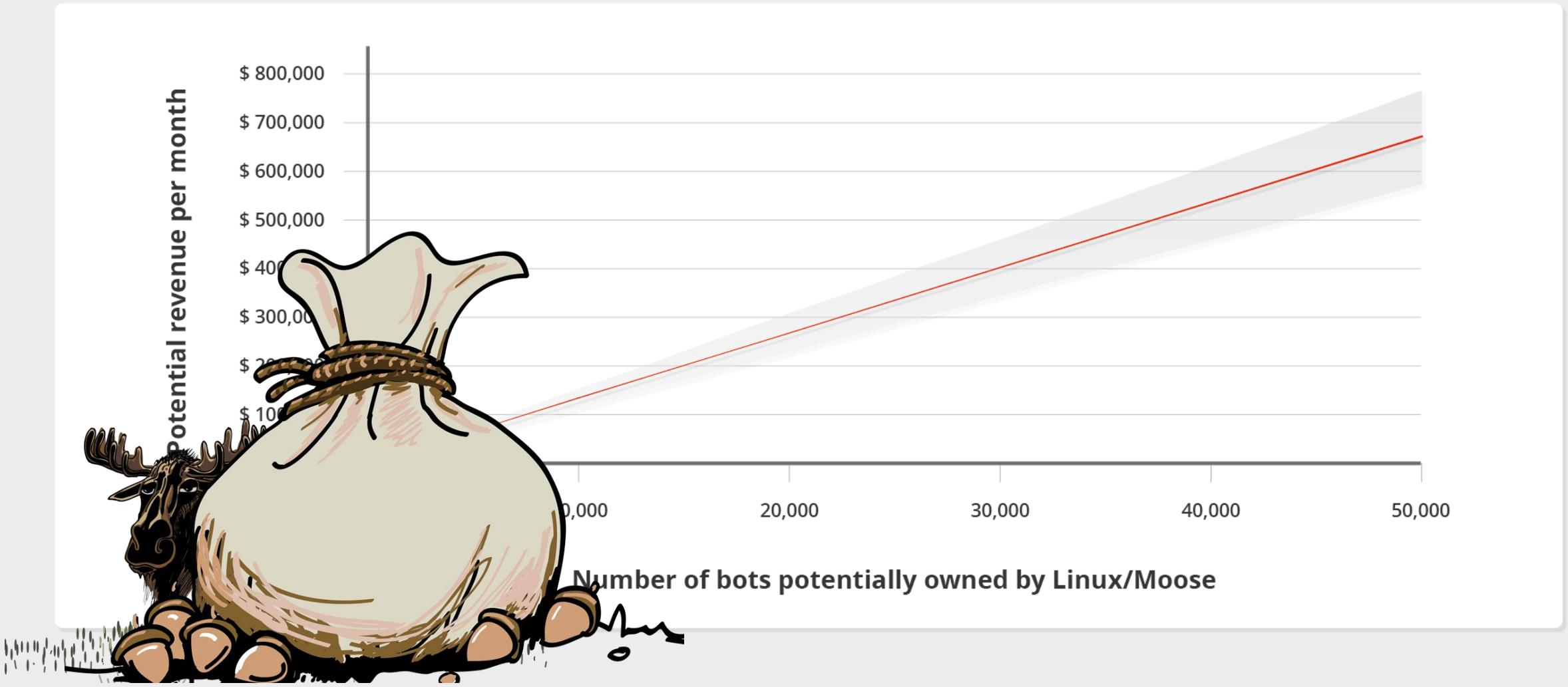


```
<HTTPFlow
  request = Request(GET 173.252.91.17:443/beautifulbird33/)
  response = Response(200 OK, text/html, 4.76kB)>
173.252.91.17
{   'client_conn': {   'address': {   'address': (  ■ ■ ■.■■.■■.■■, ■■■■,
                                      'use_ipv6': False},
                       'clientcert': None,
                       'ssl_established': True,
                       'timestamp_end': None,
                       'timestamp_ssl_setup': ■■■■
```

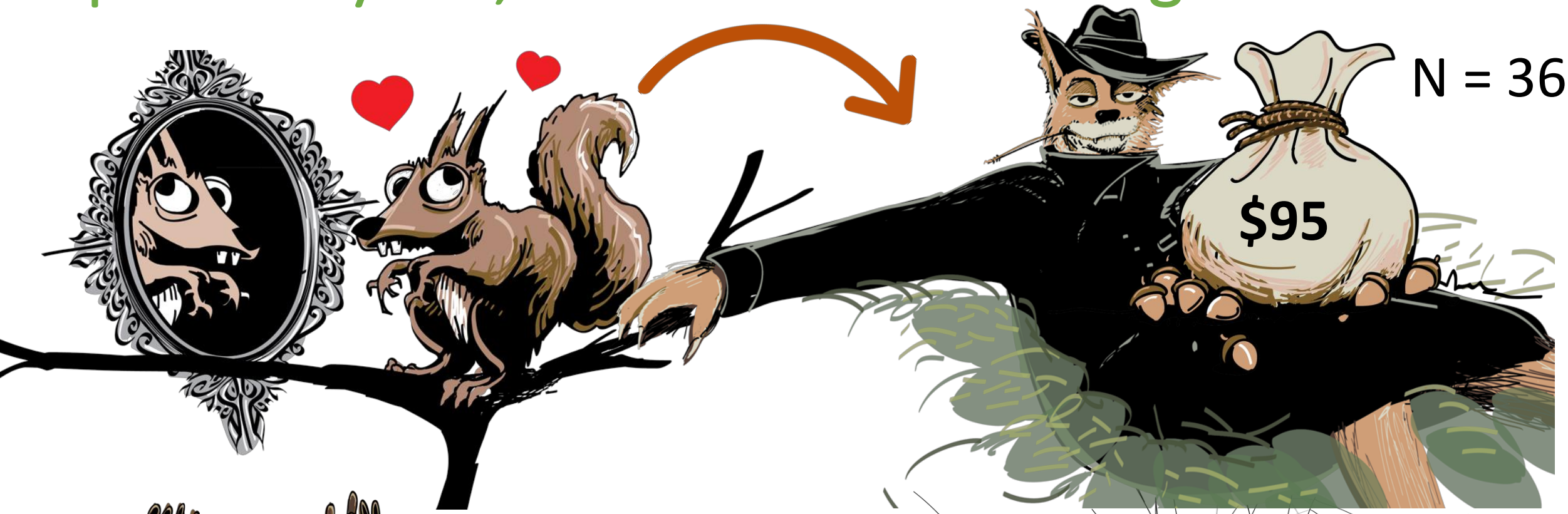



Revenue

In 2016


$ 800,000
$ 700,000
$ 600,000
$ 500,000
$ 400,000
$ 300,000
$ 200,000
$ 100,000
Potential revenue per month
20,000
30,000
40,000
50,000
Number of bots potentially owned by Linux/Moose

Squirrel buys 10,000 followers on Instagram



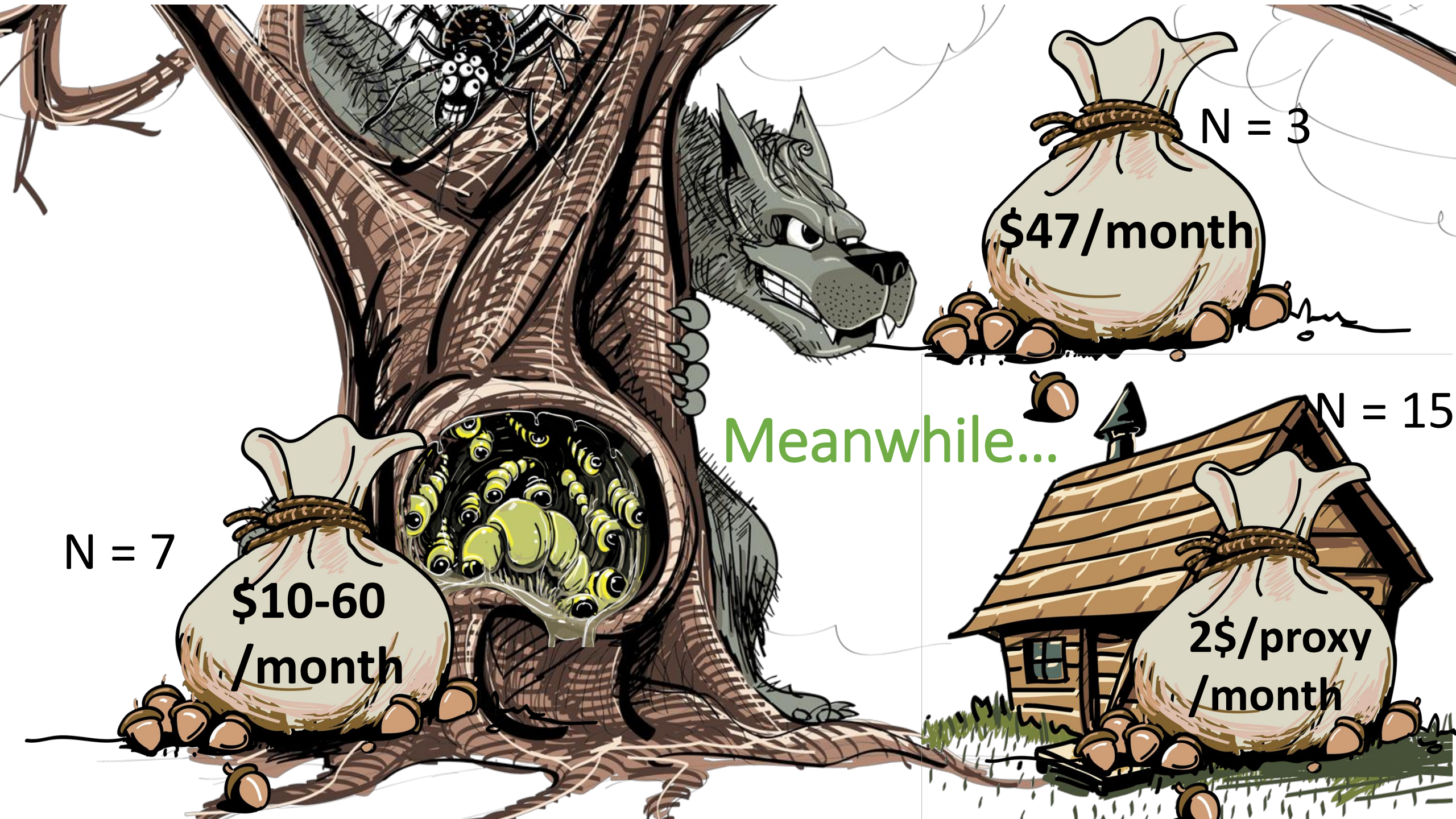
N = 36

Cheapest reseller panel





N = 33


N = 3
$47/month
Meanwhile...
N = 15
2$/proxy
/month
N = 7
$10-60
/month

To fulfill an order of 100,000 followers on Instagram

Each bot (honeypot) performed, on average,
1,186 follows per month on Instagram



85 bots per month
or
2,529 bots a day



Linux/Moose makes 100,000 follows on Instagram per day

Creates 100k followers per day at

$22.5/10,000 follows

Median price reseller

$250 per day

$82,125 per year



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 =)

-> $1,000 a day at $22.5/10,000 follows

-> That is 45 orders of 10,000 follows

-> 450,000 follows a day

-> 11 382 bots

1 client = $365 000/year




The Ecosystem of
social media manipulation
GoSecure
POWERED BY COUNTERTACK



What to do next?

GoSecure
POWERED BY COUNTERTACK



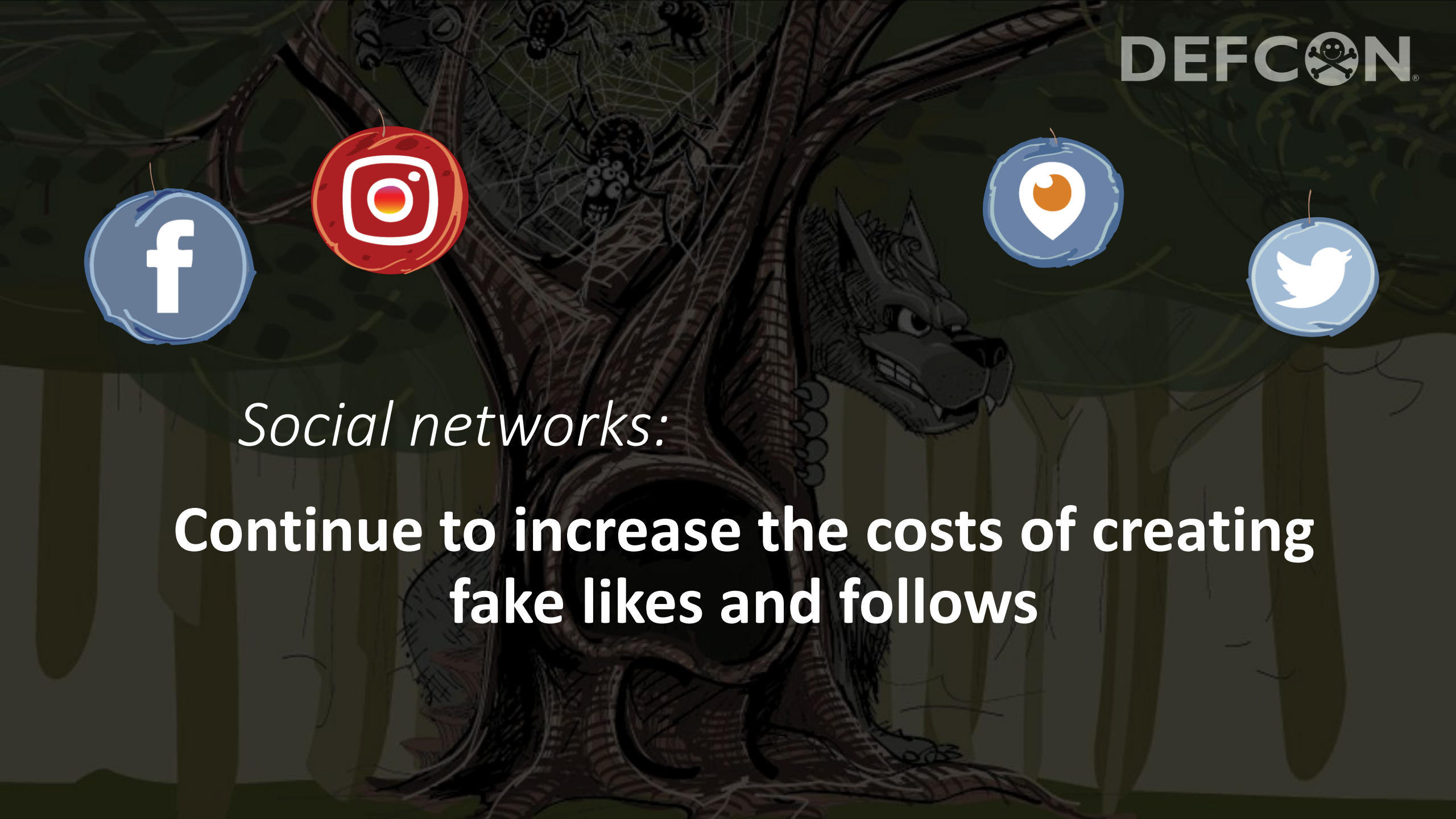
Policy makers:

Regulate the sale of social media manipulation



Law enforcement:

Target the middle-man



Social networks:

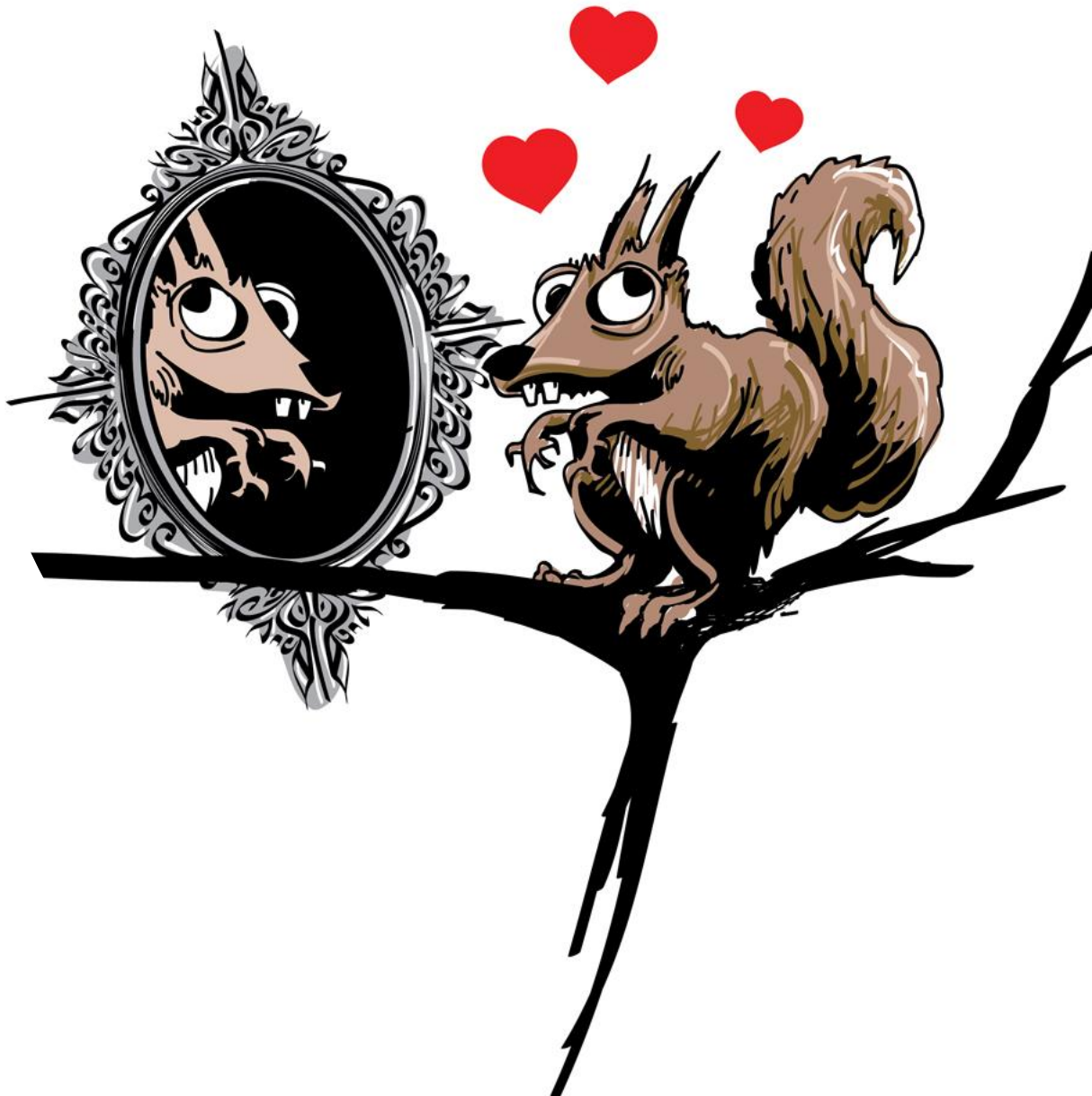
Continue to increase the costs of creating fake likes and follows

Individuals (you)

Focus on the content rather than the container!

What is this person bringing to society? Is this post legit?

What are the sources?





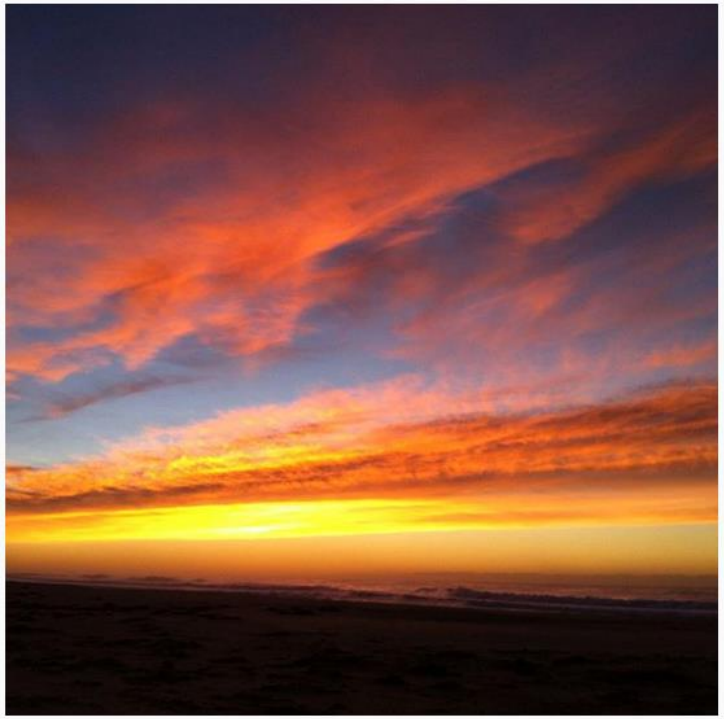
beautifulbird33

Edit Profile

Marika I'm a young photographer. Just starting on social media. Follow me for outstanding seasonal photos. For now: White and Cold; Gloomy and Sparkling.

8 posts **8,054** followers **72** following

POSTS TAGGED









beautifulbird33 Edit Profile

11 posts **442** followers **990** following

Marika

I'm a young photographer. Just starting on social media. Follow me for outstanding seasonal photos.

For now: Summertime! but still quite cold..

POSTS IGTV SAVED TAGGED





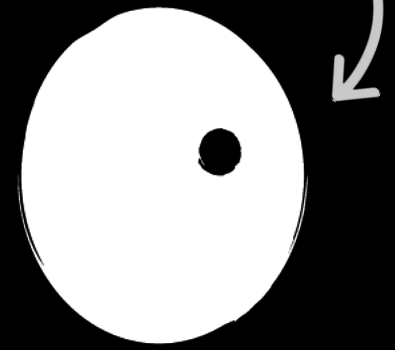


Thank you! Questions?

Masarah Paquet-Clouston
mcpc@gosecure.net
@masarahclouston

Olivier Bilodeau
obilodeau@gosecure.net
@obilodeau

Artwork



jeremie@tunghat.ca

https://gosecure.net/blog/

https://nsec.io/