Behind the Scenes:
The Industry of Social Media Manipulation Driven by Malware
SECTOR – 2019

Masarah Paquet-Clouston, Olivier Bilodeau
GoSecure Research
Back in 2015-2016

eset

Mitacs

Université de Montréal

Linux/Moose Botnet
Linux/Moose
An IoT botnet that conducts social media manipulation
Social Media Manipulation

Comment devenir influenceuse (en trichant)

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

TCP
PI Metadata (unencrypted)

Proxy client

SOCKS PROXY
End-to-end virtual tunnel (unencrypted and terminated via redirection)

Infected host

HTTPS
HTTP over TLS (encrypted and not authenticated)

Mitm

Honeypot

Targeted social network

HTTPS
HTTP over TLS (encrypted and authenticated)
Accessed the raw traffic!
What did we have?

• Several infected hosts used by operators
• HTTPS traffic in plaintext
• C&C traffic
• Publicly available seller market
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  
mcp@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 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. 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 “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   # ip_addr
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)
fail:
lw    $a0, 0x68+sockfd($fp)
jal    close
nop
j      connection
nop
# End of function thd_serve10073
Whitelisted IPs

Reseller model?
<table>
<thead>
<tr>
<th>Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Honeypots used</td>
</tr>
<tr>
<td>Websites targeted</td>
</tr>
<tr>
<td>TLS fingerprints</td>
</tr>
<tr>
<td>User agents</td>
</tr>
<tr>
<td>API calls</td>
</tr>
<tr>
<td>Timestamps</td>
</tr>
<tr>
<td>Accounts created on social networks</td>
</tr>
<tr>
<td>Accounts followed on social networks</td>
</tr>
</tbody>
</table>
Whitelisted IPs

Whitelisted IP1

Whitelisted IP2

Whitelisted IP3

Potential buyers

notley.ehman5

baiseyca_along

belentingay1412

loishowe1909

garynutarelli1429

amirSanallah

websecure

antvan_official

Fake accounts
Where do we stand?

Each whitelisted IP addresses have their own list of fake accounts

Additionally, the whitelisted IP addresses:

• Run on Windows servers
• Remote desktop protocol 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
  - Scales Social Network Account Management (1000s of accounts)
  - 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
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
- Hashtags 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...
objInstagramUser.DataBaseId = (int)x.Id;
if (!string.IsNullOrEmpty(x.DevUid))
{
    objInstagramUser.guid = x.DevUid.Replace("android-", ";");
}
objInstagramUser.UserAgentMobile = x.MobileUserAgent;
if (string.IsNullOrEmpty(objInstagramUser.UserAgentMobile))
{
    public string PhoneId { get; private set; }

    // Token: 0x1700004F RID: 79
    // (get) Token: 0x60000C8 RID: 200 RVA: 0x00008AD0 File Offset: 0x00008AD0
    public string Useragent { get
    {
        get
        {
            return string.Format(ConstantVariable.UseragentCommonFormat, new object[]
            {
                ConstantVariable.IgVersion,
                this.AndroidVersion,
                this.AndroidRelease,
                this.Dpi,
                this.Resolution,
                this.ManufacturerBrand,
                this.Model,
                this.Device,
                this.Cpu,
                ConstantVariable.UseragentLocale
            });
        }
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 40.0.14.95 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 40.0.14.95 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 40.0.14.95 Android (24/7.0; 640dpi; 1440x2560; HUAWEI; LON-L29; HWLON; hi3660; en_US)
<table>
<thead>
<tr>
<th>Software</th>
<th>Architecture</th>
<th>Browser</th>
<th>Packer</th>
<th>Our Target?</th>
</tr>
</thead>
<tbody>
<tr>
<td>GramDominator / Socinator</td>
<td>.Net</td>
<td>CEF</td>
<td>Not packed</td>
<td>No socks proxy support</td>
</tr>
<tr>
<td>FollowAdder</td>
<td>Xojo / REALBasic</td>
<td>CEF</td>
<td>Obscure Xojo framework</td>
<td>No unlimited accounts</td>
</tr>
<tr>
<td>MassPlanner</td>
<td>C++ / .Net</td>
<td>CEF</td>
<td>Themida / WinLicense 2.x</td>
<td>Only one overridable User-Agent</td>
</tr>
<tr>
<td>FollowingLike</td>
<td>.Net</td>
<td>BotSocial, a custom browser in .Net</td>
<td>ILProtector</td>
<td>Custom User-Agent feature too recent</td>
</tr>
<tr>
<td>FollowLiker</td>
<td>Java compiled to native code</td>
<td>HtmlUnit Java Library</td>
<td>Excelsior JET</td>
<td>Doesn’t interact with Instagram similarly</td>
</tr>
</tbody>
</table>
Where do we stand?

Found several automation software vendors

Reseller model is not at the botnet level
HTTPFlow

request = Request(GET 173.252.91.17:443/medianesia.panel/)
response = Response(200 OK, text/html, 4.43kB)

{   'client_conn': {       'address': {           'address': (IP Address, ,
           'use_ipv6': False),
         'clientcert': None,
         'ssl_established': True,
         'timestamp_end': None,
         'timestamp_ssl_setup': 1466824317.305581,
         'timestamp_start': 1466824315.828804},
Reseller panels
Let's get social!

Username
Password
Remember me

SMMBULK

World's Best SMM Panel

Website Hosting (Monthly):
Pricing:
- 250 MB Web Space
- 500 GB Bandwidth
- 20 Email Accounts
- 10 MySQL Databases
- cPanel Control Panel
- 10 Sub Domains
- 10 FTP Accounts

Contact us after order

Instagram Likes:
- 249 IG Likes App 1
  - Price: 0.70
  - Min: 50
  - Max: 1500
  - Fast real

Instagram Views:
- 253 IG Video View App 1
  - Price: 0.02
  - Min: 500
  - Max: 250,000,000
  - Views from real profiles
  - Speed: 10k-50k per day

IG Followers (Guaranteed):
- 254 IG Followers App 1 MAX 50k
  - Price: 5.00
  - Min: 10
  - Max: 50k
  - Auto refill: 20/day

- 255 IG Followers App 2 MAX 100k
  - Price: 5.00
  - Min: 10
  - Max: 100k
  - Auto refill: 20/day

- 257 IG Followers App 4 MAX 350k
  - Price: 2.50
  - Min: 50
  - Max: 550k
  - Auto refill: 10k to 50k per day
Reseller panels

• Sell popularity in bulk
• All look alike
<table>
<thead>
<tr>
<th>Simple Investigation</th>
<th>Fingerprint of the web application</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Domain registration information</td>
</tr>
<tr>
<td></td>
<td>HTML content</td>
</tr>
<tr>
<td></td>
<td>IP address</td>
</tr>
<tr>
<td>Resolve</td>
<td>First</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>perfectpanel.com</td>
<td>2019-03-13</td>
</tr>
<tr>
<td>extra-like.com</td>
<td>2019-07-29</td>
</tr>
<tr>
<td>ezyboost.com</td>
<td>2019-01-14</td>
</tr>
<tr>
<td>grampanel.com</td>
<td>2019-01-09</td>
</tr>
<tr>
<td>totalfama.com</td>
<td>2019-07-20</td>
</tr>
<tr>
<td>zawdly.com</td>
<td>2019-07-31</td>
</tr>
<tr>
<td>followiz.com</td>
<td>2019-01-07</td>
</tr>
<tr>
<td>painelmaismidia.com.br</td>
<td>2019-05-20</td>
</tr>
<tr>
<td>companyo.com</td>
<td>2019-05-23</td>
</tr>
</tbody>
</table>
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

User API
Easy-to-integrate API for your customers.

Powerful admin dashboard
Manage users, services, orders, tickets. Configure automation. Review stats. And many more.
Panel-as-a-Service

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
Conversations on BlackHatWorld about finding the main SMM provider

May 11, 2019

aixboss
Registered Member

Jenham 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.
Conversations on BlackHatWorld about finding the main SMM provider

Apr 17, 2018

Daltonmediastudio
Jr. VIP

no one will reveal the main provider for them he is their hidden ghost
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.
Conversations on BlackHatWorld about finding the main SMM provider

Jan 6, 2019

ellay
Jr. VIP

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 panel-as-a-service 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 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 geolocated 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 or 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
RSocks

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

Supported protocols: SOCKS4, SOCKS5, HTTP(S)
RSocks (cont)

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

- Received a single IP from France
  - Scaleway, Dedibox
- Traffic goes out an IPv6 address in the USA
  - AT&T Internet Services
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
# Residential Proxy Providers Summary

<table>
<thead>
<tr>
<th>Provider</th>
<th>Infrastructure</th>
<th>Geoip / Whois</th>
<th>Powered by Malware?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Luminati</td>
<td>Leveraging willing participants’ phones</td>
<td>Unknown</td>
<td>Unlikely</td>
</tr>
<tr>
<td>Storm Proxies</td>
<td>Debian 8 (Jessie) with Squid</td>
<td>Misleading information</td>
<td>Unlikely</td>
</tr>
<tr>
<td>RSocks</td>
<td>Debian 8 (Jessie) with unknown proxy</td>
<td>Small unknown ISP</td>
<td>Unlikely</td>
</tr>
<tr>
<td>High Proxies</td>
<td>CentOS/RHEL 7 with Squid</td>
<td>Misleading information</td>
<td>Unlikely</td>
</tr>
<tr>
<td>Valar Solutions</td>
<td>Debian 9 (Stretch) with 3Proxy. Tunnel between France and USA. IPv6.</td>
<td>Legit AT&amp;T Internet Services</td>
<td>Unlikely</td>
</tr>
</tbody>
</table>
Resident Evil: Understanding Residential IP Proxy as a Dark Service

Xianghang Mi*, Xuan Feng*, Xiaojing Liao*, Baojun Liu1,
XiaoFeng Wang*, Feng Qian*, Zhou Li2, Sumayah Alrwais3, Limin Sun*, Ying Liu1

1Indiana University Bloomington, 2Tsinghua University, 3IEEE Member,
4King Saud University, 5Institute of Information Engineering, CAS

*{xmi, xf1, xiao, xw7, fengqian}@indiana.edu, 1bj15@mails.tsinghua.edu.cn,
liuying@cernet.edu.cn, 1lzcarl@gmail.com, 3alrwais@ksu.edu.sa, 5sunlimin@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 serverside 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], MicroVeles [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 panel-as-a-service providers

Who buys from reseller panels?
Customer-facing sellers
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.
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
Devumi.top is no longer accepting new clients

If you’re interested 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.
Potential Buyers

Linux/Moose

86% of the relayed traffic focused on Instagram

List of potential customers:

522 accounts

Method:

Content analysis
Entertainment Industry (20%)
Selling Products and Services (21%)
Personal Profiles (26%)
We made an experiment...
Linux/Moose’s Targeted Social Networks

- Periscope: 2%
- Twitter: 8%
- Instagram: 86%
- Others: 4%
- Kiwi: 1%
- Flipagram & Youtube: <1%
beautifulbird33

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
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': 'time
        'timestamp_start': 'time
    'error': None,
    'id': 'd9d7e34a-69e8-47d8-99f2-0c174682a000',
    'intercepted': False,
    'request': {
        'first_line_format': 'relative',
        'headers': {
            ('host', 'www.instagram.com'),
            ('User-Agent', 'Mozilla/5.0 (Windows NT 5.1; rv:17.0) Gecko/20100101 Firefox/17.0'),
            ('Accept', 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8'),
            ('Accept-Language', 'en-US,en;q=0.5'),
            ('Accept-Encoding', 'gzip, deflate'),
            ('Referer', 'https://www.instagram.com/beautifulbird33'),
            ('Connection', 'keep-alive'))
            'host': '173.252.91.17',
        http_version': 'HTTP/1.1',
        'is replay': False,
        'method': 'GET',
        'path': '/beautifulbird33/',
        'port': 443,
        'scheme': 'https',
        'stickysauth': False,
        'stickeycookie': False,
        'timestamp_end': 'time
        'timestamp_start': 'time
    }

}
In 2016

Number of bots potentially owned by Linux/Moose

Potential revenue per month

$10,000 $20,000 $30,000 $40,000 $50,000 $60,000 $70,000 $80,000

0 10,000 20,000 30,000 40,000 50,000
Squirrel buys 10,000 Instagram followers

Cheapest reseller panel

N = 36

N = 33
Meanwhile…

- $47/month
- $10-60/month
- 2$/proxy/month
- N = 3
- N = 7
- N = 15
The Ecosystem of Social Media Manipulation
Other Research Avenues

• Click farms
• Compromised accounts
• Troll farms
What to do next?
Policy makers:
Look into the sale of social media manipulation
Law enforcement:

Target the middle-man
Social networks:
Continue to flag any robotic activity
AriefR Last Friday at 9:57 AM
mee too
since yesterday

Valar [CEO] Last Friday at 10:41 AM
@funniestpoke Its global issue, nobody able to reg accs now

AriefR Last Friday at 10:44 AM
Really? @Valar [CEO] tried with many proxy provider, vpn, gcloud vps, 4g, useragent, no result.

Valar [CEO] Last Friday at 10:49 AM
@AriefR Yes nothing helps

darkair  Last Friday at 10:57 AM
so no one can create new instagram accounts?

aez  Last Friday at 11:18 AM
today it work for me little bit better than yesterday
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

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
Marika
I'm a young photographer. Just starting on social media. Follow me for outstanding seasonal photos.
For now: Summertime! but still quite cold.
Thank you! Questions?

Masarah Paquet-Clouston
mcpc@gosecure.net
@masarahclouston

Olivier Bilodeau
obilodeau@gosecure.net
@obilodeau

https://gosecure.net/blog/
https://nsec.io/

Artwork
jeremie@tunghat.ca