

EGO MARKET WHEN GREED FOR FAME BENEFITS LARGE- SCALE BOTNETS

 Masarah Paquet-Clouston
GOSECURE 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
- 




Montreal, May 2017

nsec.io



AGENDA

1. Malware behind: Linux/Moose Recap
 2. Honeypot environment built for analysis
 3. The man-in-the-middle attack on the Botnet
 4. The Linux/Moose's operations
 5. Linux/Moose's buyers
 6. Overview of sellers
 7. Potential profitability
- 

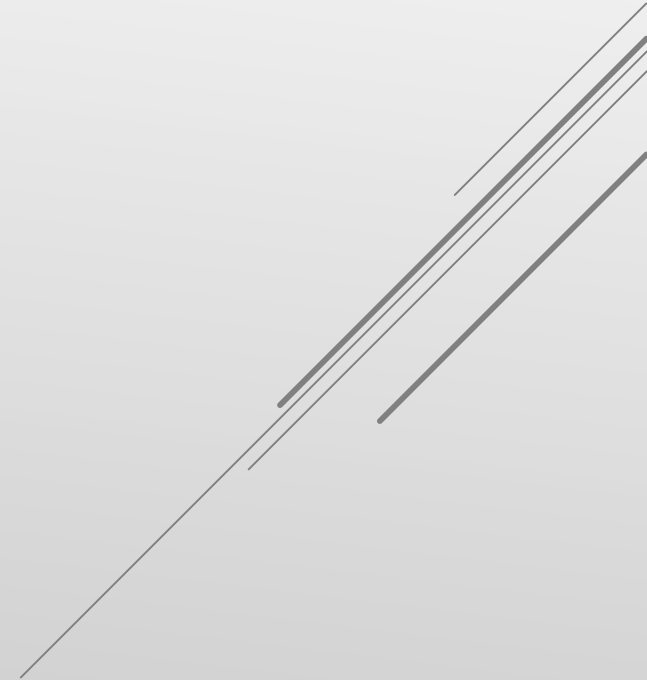
JOINT RESEARCH



Two additional authors:

- David Décary-Hétu, Université de Montréal
- Thomas Dupuy, ESET

THE STORY OF LINUX/MOOOSE



LINUX/MOOSE IN A NUTSHELL

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

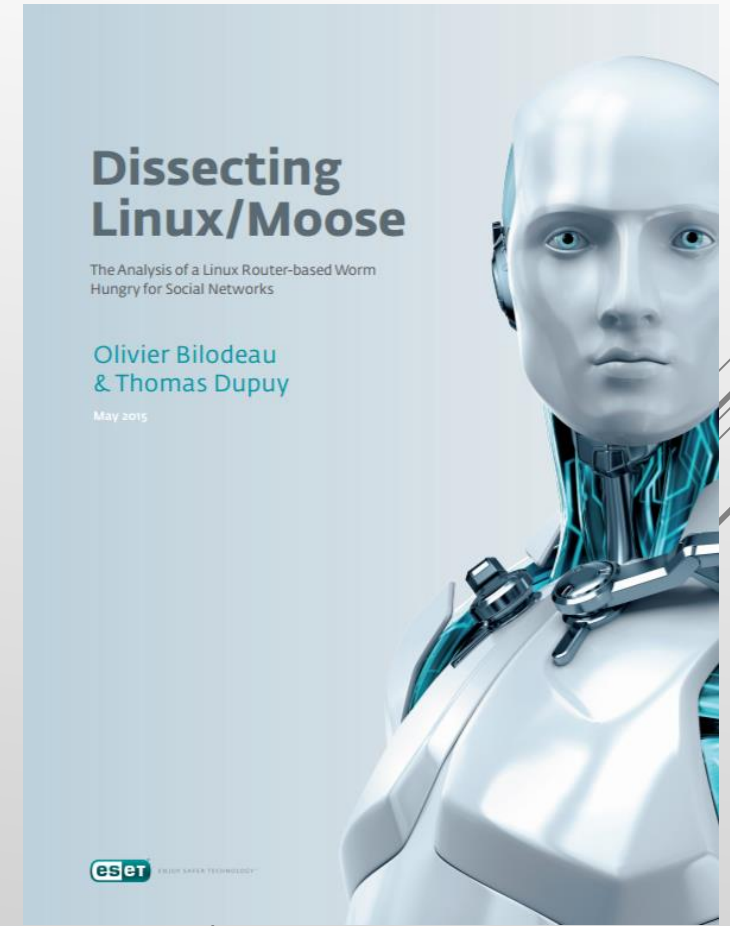
VISITING SOCIAL MEDIA SITES!?



LINUX/MOOSE

Timeline

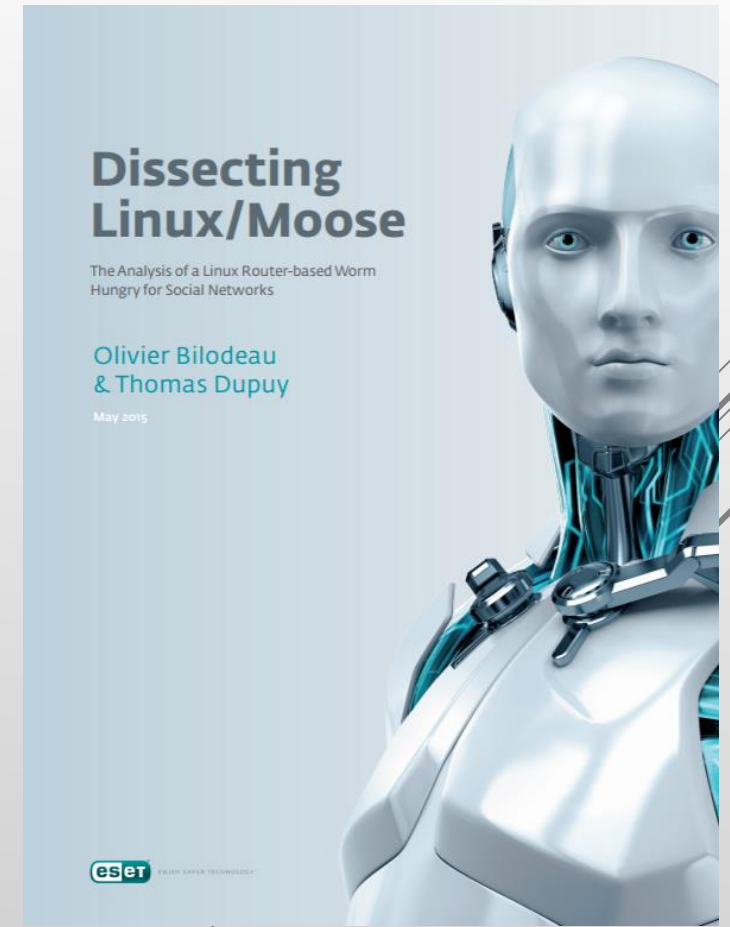
- ▶ November 2014: Discovery by ESET
- ▶ Early 2015: Thoroughly reversed-engineered
- ▶ May 2015: Paper published
- ▶ June 2015: C&C down
- ▶ September 2015: New version



LINUX/MOOSE

Gory details

- ▶ Extensive ESET Paper
- ▶ Virus Bulletin 2015 presentation
- ▶ Botconf 2015 presentation

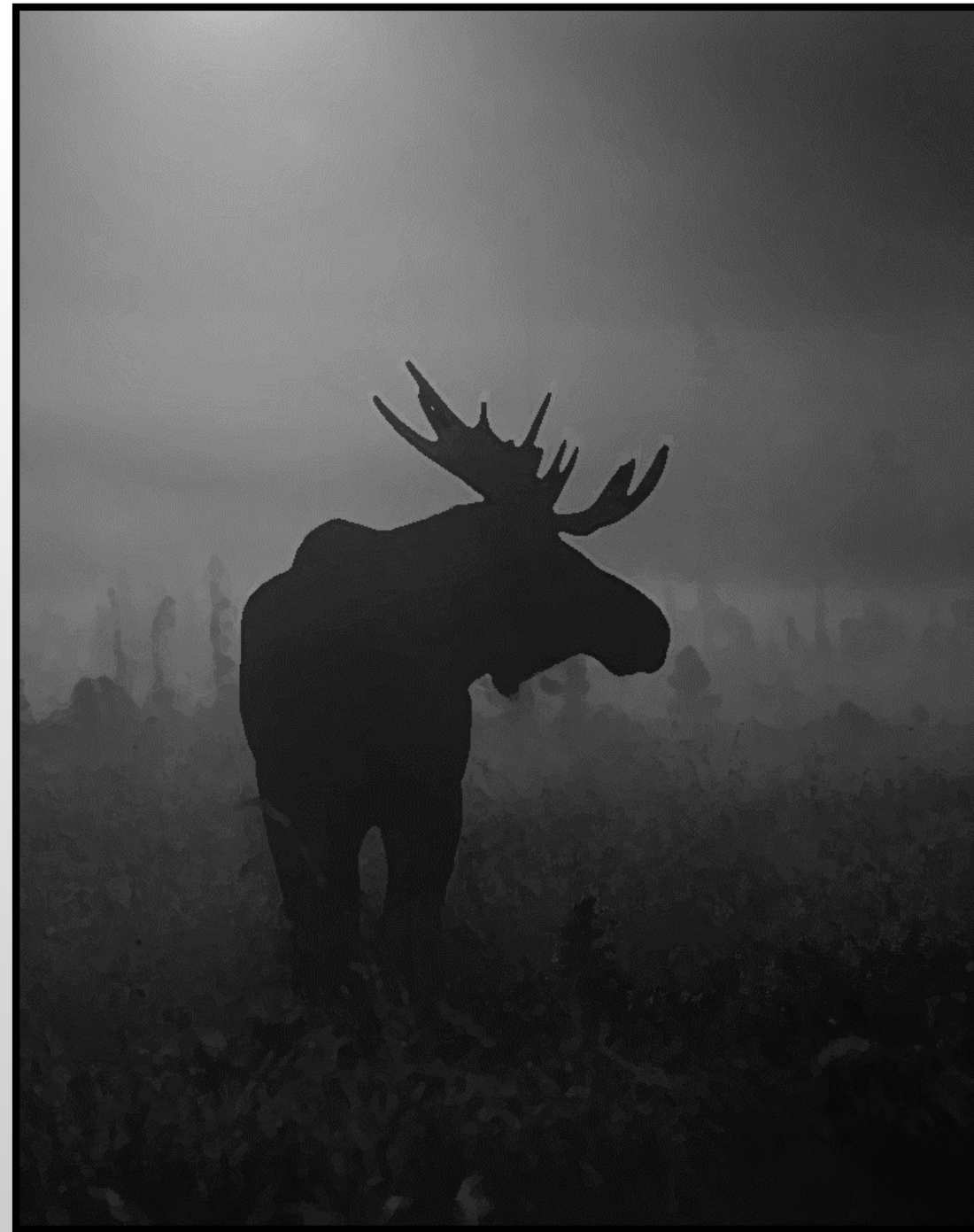


0x1C_mips_bfc2a99450977dc7ba2ec0879fb17c612e248ece

Edit As: Hex Run Script Run Template

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
2:8FB0h:	72	6F	72	00	70	61	73	73	77	6F	72	64	20	69	73	20	ror.password is
2:8FC0h:	77	72	6F	6E	67	00	00	00	70	61	73	73	77	6F	72	64	wrong...password
2:8FD0h:	3A	00	00	00	75	74	68	65	6E	74	69	63	61	74	69	6F	:...uthenticatio
2:8FE0h:	6E	20	66	61	69	6C	65	64	00	00	00	00	73	68	0D	0A	n failed....sh..
2:8FF0h:	00	00	00	00	70	73	0D	0A	65	63	68	6F	20	2D	6E	20ps..echo -n
2:9000h:	2D	65	20	22	48	33	6C	4C	30	57	6F	52	6C	44	22	0D	-e "H3lL0WoRlD".
2:9010h:	0A	63	68	6D	6F	64	0D	0A	00	00	00	00	48	33	6C	4C	.chmod.....H3lL
2:9020h:	30	57	6F	52	6C	44	00	00	65	6C	61	6E	32	00	00	00	0WoRlD..elan2...
2:9030h:	65	6C	61	6E	33	00	00	00	63	68	6D	6F	64	3A	20	6E	elan3...chmod: n
2:9040h:	6F	74	20	66	6F	75	6E	64	00	00	00	00	63	61	74	20	ot found....cat
2:9050h:	2F	70	72	6F	63	2F	63	70	75	69	6E	66	6F	0D	0A	00	/proc/cpuinfo...
2:9060h:	47	45	54	20	2F	78	78	2F	72	6E	64	65	2E	70	68	70	GET /xx/rnde.php
2:9070h:	3F	70	3D	25	64	26	66	3D	25	64	26	6D	3D	25	64	20	?p=%d&f=%d&m=%d
2:9080h:	48	54	54	50	2F	31	2E	31	0D	0A	48	6F	73	74	3A	20	HTTP/1.1..Host:
2:9090h:	77	77	77	2E	67	65	74	63	6F	6F	6C	2E	63	6F	6D	0D	www.getcool.com.
2:90A0h:	0A	43	6F	6E	6E	65	63	74	69	6F	6E	3A	20	4B	65	65	.Connection: Kee
2:90B0h:	70	2D	41	6C	69	76	65	0D	0A	0D	0A	00	6C	6F	00	00	p-Alive.....lo..
2:90C0h:	31	32	37	2E	30	2E	30	2E	31	00	00	00	2F	70	72	6F	127.0.0.1.../pro
2:90D0h:	63	00	00	00	2F	70	72	6F	63	2F	25	73	2F	63	6D	64	c.../proc/%s/cmd
2:90E0h:	6C	69	6E	65	00	00	00	00	6B	69	6C	6C	20	25	73	00	line....kill %s.
2:90F0h:	2F	65	74	63	2F	69	6E	69	74	2E	64	2F	72	63	53	00	/etc/init.d/rcS.
2:9100h:	2F	68	6F	6D	65	2F	68	69	6B	2F	73	74	61	72	74	2E	/home/hik/start.
2:9110h:	73	68	00	00	2F	65	74	63	2F	63	72	6F	6E	74	61	62	sh../etc/crontab
2:9120h:	00	00	00	00	2F	65	74	63	2F	63	72	6F	6E	2E	68	6Fetc/cron.ho
2:9130h:	75	72	6C	79	2F	78	00	00	2F	65	74	63	2F	72	63	2E	urly/x../etc/rc.
2:9140h:	64	2F	72	63	00	00	00	00	31	39	32	2E	31	36	38	2E	d/rc....192.168.
2:9150h:	31	2E	33	00	25	64	00	00	53	79	73	20	69	6E	69	74	1.3.%d..Sys init
2:9160h:	3A	20	4F	4B	00	00	00	00	2D	6E	6F	62	67	00	00	00	: OK....-nobg...
2:9170h:	4E	6F	20	73	79	6E	63	00	42	61	64	20	69	6E	69	74	No sync.Bad init
2:9180h:	00	00	00	00	25	64	20	25	64	20	25	64	0A	00	00	00%d %d %d....
2:9190h:	03	01	A8	C0	03	01	A8	C0	03	01	A8	C0	00	00	00	00	..`À..`À..`À....
2:91A0h:	2F	62	69	6E	2F	73	68	00	2D	63	00	00	65	78	69	74	/bin/sh.-c..exit
2:91B0h:	20	30	00	00	00	00	74	40	00	00	00	20	00	00	00	01	0....t@... ..

Elan = Moose in French



LOTUS ELAN



SLOVAK MUSIC GROUP CALLED ELAN



FOLLOWING THE ESET REPORT

BBC Sign in Menu

NEWS

Home Video World US & Canada UK Business Tech Science Mag

Technology

'Moose' malicious worm targets home routers

28 May 2015 | Technology

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

RISK ASSESSMENT —

The Moose is loose: Linux-based worm turns routers into social network bots

Malware can infect IoT devices—including medical devices—with weak authentication.

InformationWeek
DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home News & Commentary Authors Slideshows Video Radio Reports White Papers Events

ANALYTICS ATTACKS / BREACHES APP SEC CAREERS & PEOPLE CLOUD ENDPOINT IoT MOBILE OPERATIONS

PERIMETER

5/27/2015

Moose Malware Uses Linux Routers for Social Network Fraud

Moose is sophisticated enough to do DNS hijacks, DDoSes, and work penetration...so why is it wasting its time on Instagram?

Malware targeting Linux routers is exploiting them not through a vulnerability per se, but rather by simply brute-forcing weak passwords, as reported by researchers at ESET. The malware, which researchers have identified as Linux/Moose, could be used for a wide variety of purposes -- including phishing, DDoSing, and deep network penetration -- but so far attackers appear to be using it for tame social networking fraud.

THE COMMAND & CONTROL (C&C) SERVERS WENT **DARK**

Until September 2015

Three thin, parallel diagonal lines in a light gray color, extending from the bottom right towards the top right of the image.

THIS TALK IS ABOUT...

Understanding Linux/Moose and the market it evolves in

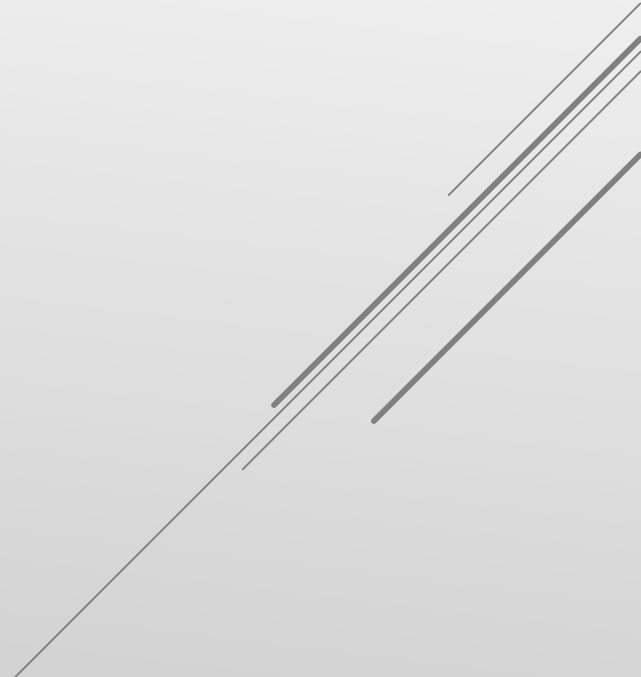


Catching Linux/Moose v2.0

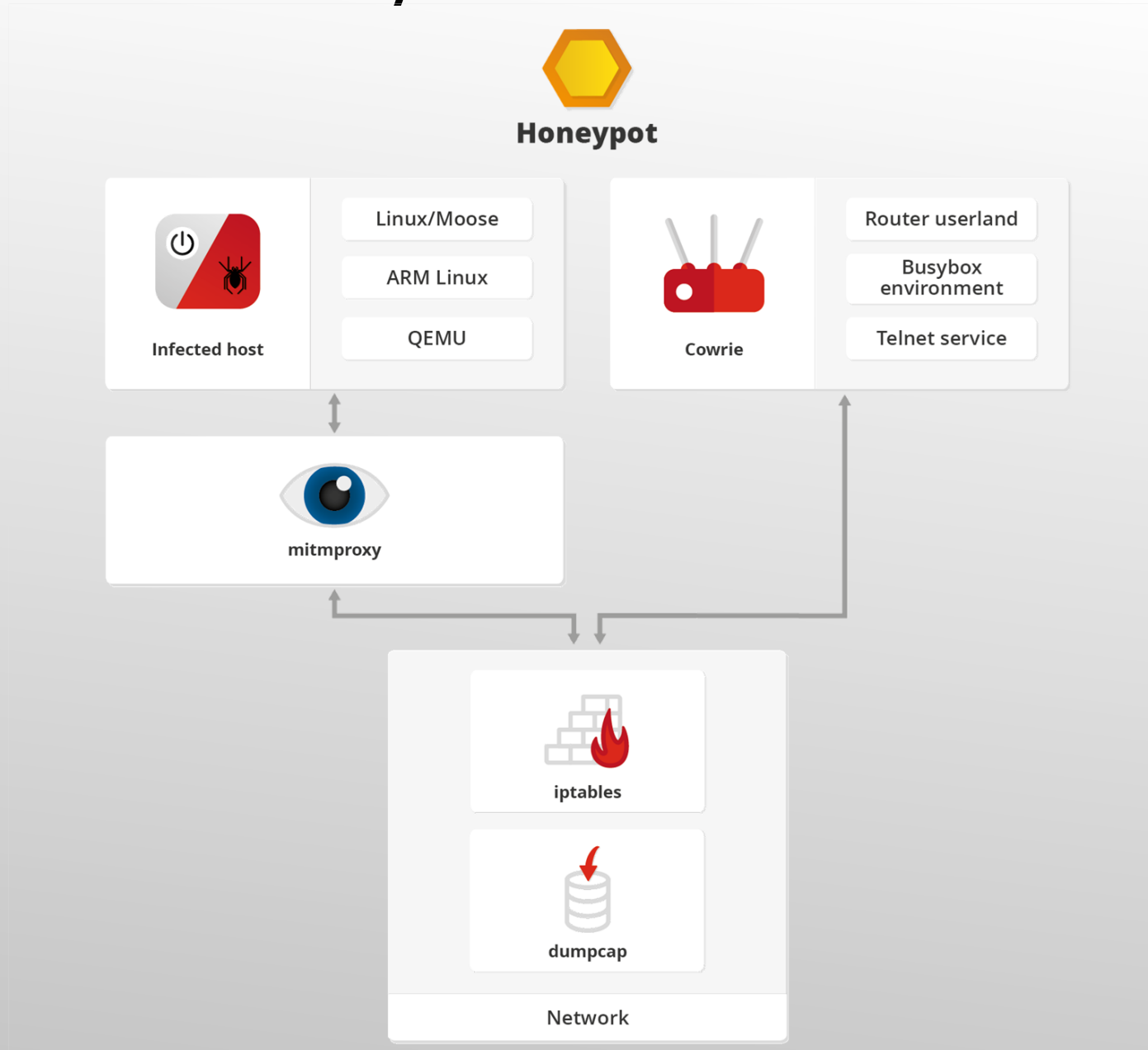


LINUX/MOOSE HONEYPOT

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

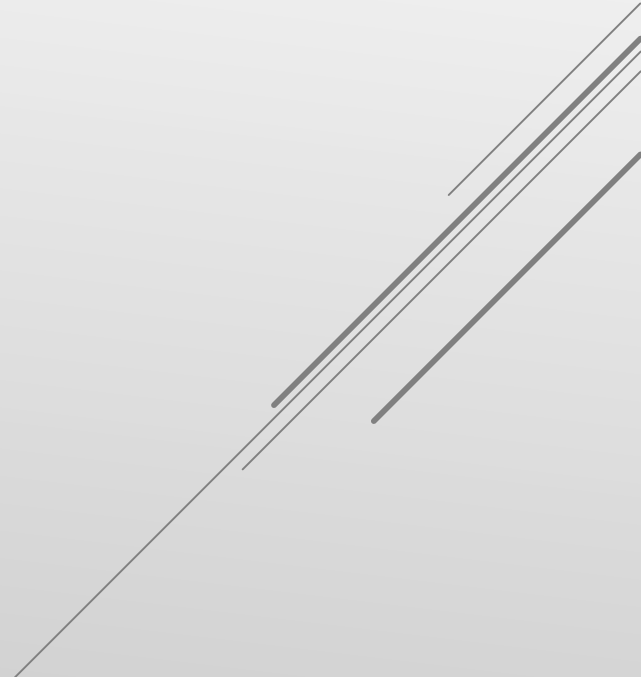


CATCHING LINUX/MOOSE




HONEYPOT COMPONENTS

▶ Cowrie

- ▶ Python / Twisted
 - ▶ Emulated filesystem and commands output
 - ▶ Actively maintained
 - ▶ Easy to modify
 - ▶ Machine parsable logs (JSON)
 - ▶ Real-time log replay mechanism
 - ▶ No Telnet Support...
- 
- A series of parallel diagonal lines in the bottom right corner of the slide, consisting of several thin lines in different shades of gray.

CONTRIBUTED TELNET TO COWRIE

 micheloosterhof / cowrie

 Watch ▾

86

 Star

734

 Fork

148

 Code

 Issues 40

 Pull requests 4

 Projects 2

 Wiki

 Pulse

 Graphs

Basic Telnet support implemented

[Browse files](#)

A squash merge of GoSecure/cowrie telnet-poc branch:
<https://github.com/GoSecure/cowrie/tree/telnet-poc>

Rebased on current upstream master.


August 2016 update: Resolved several conflicts when rebasing

 master

 obilodeau committed with micheloosterhof on Aug 14

1 parent [bae5889](#)

commit [640652207d181fe529bcf1ed1e4e8b0202fc04cf](#)

 Showing **13 changed files** with 461 additions and 38 deletions.

Unified

Split

COWRIE HONEYPOT PROJECT



Michel Oosterhof

@micheloosterhof



Following

I merged Telnet support into the [#cowrie](#) SSH honeypot. Thanks [@obilodeau](#) ! Check `cowrie.cfg.dist` for options.

RETWEETS

6

LIKES

11



7:11 AM - 22 Aug 2016



6

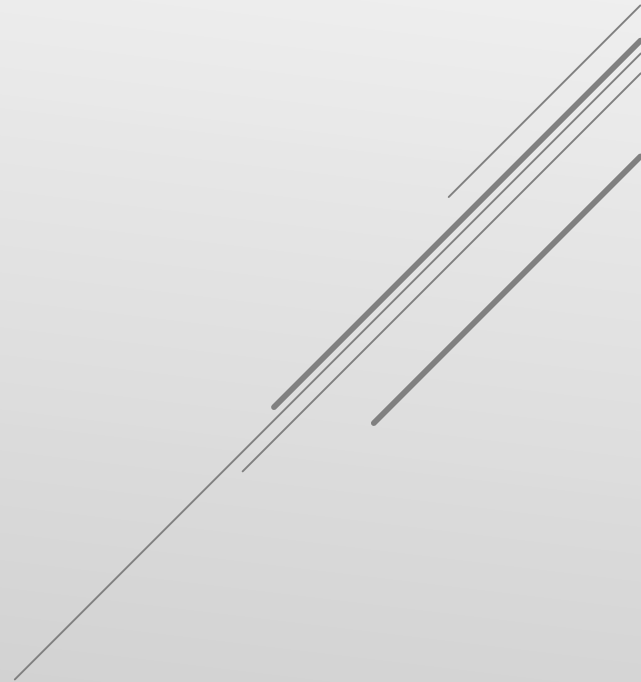


11

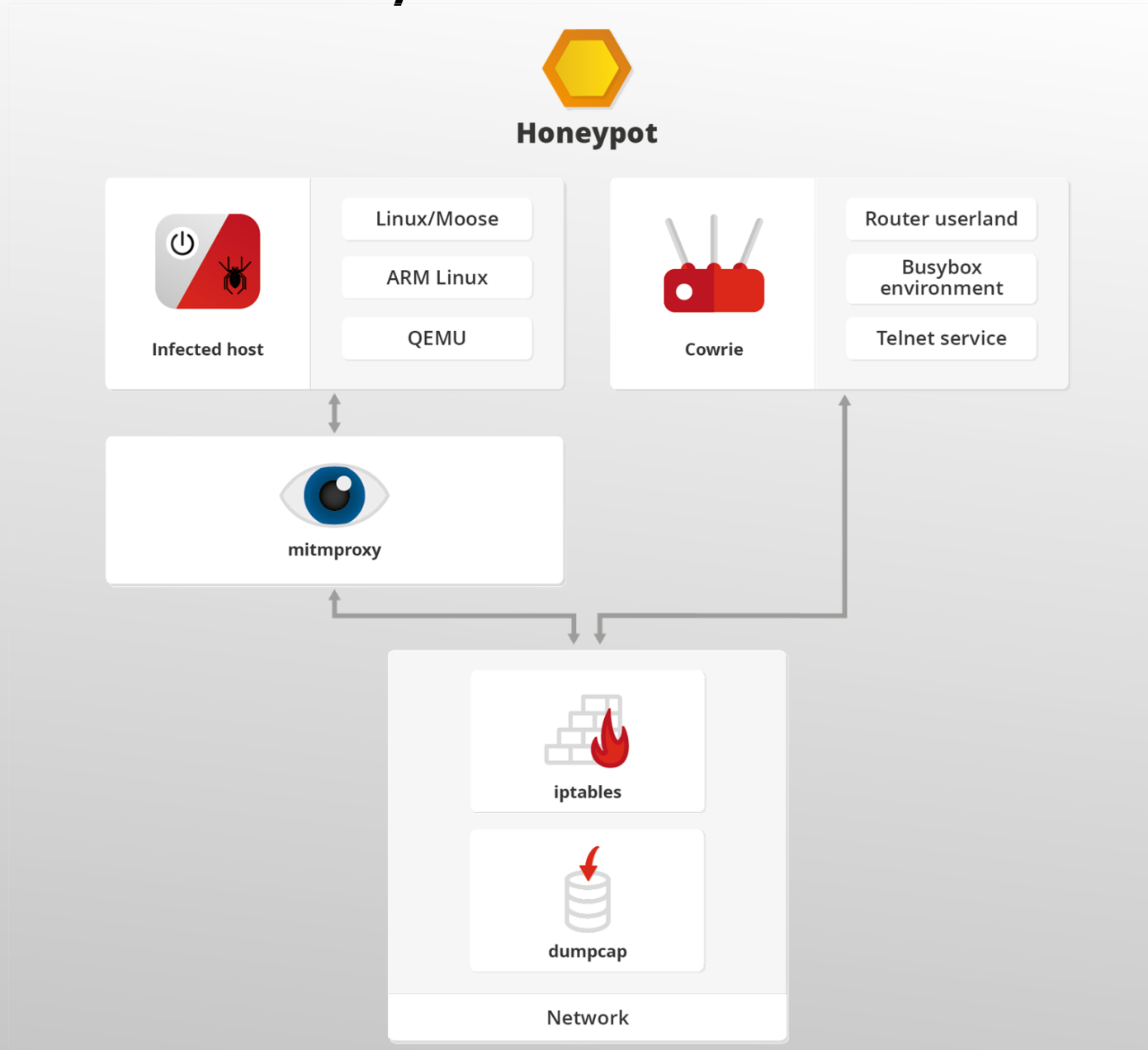


HONEYPOT COMPONENTS

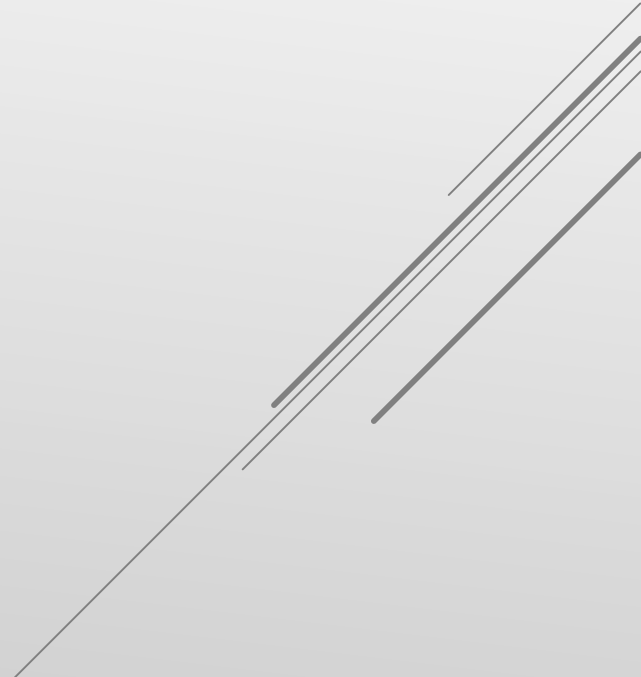
- ▶ Infected host
 - ▶ QEMU
 - ▶ Debian Linux ARM image
 - ▶ Plant Linux/Moose binary
 - ▶ Run it




CATCHING LINUX/MOOSE



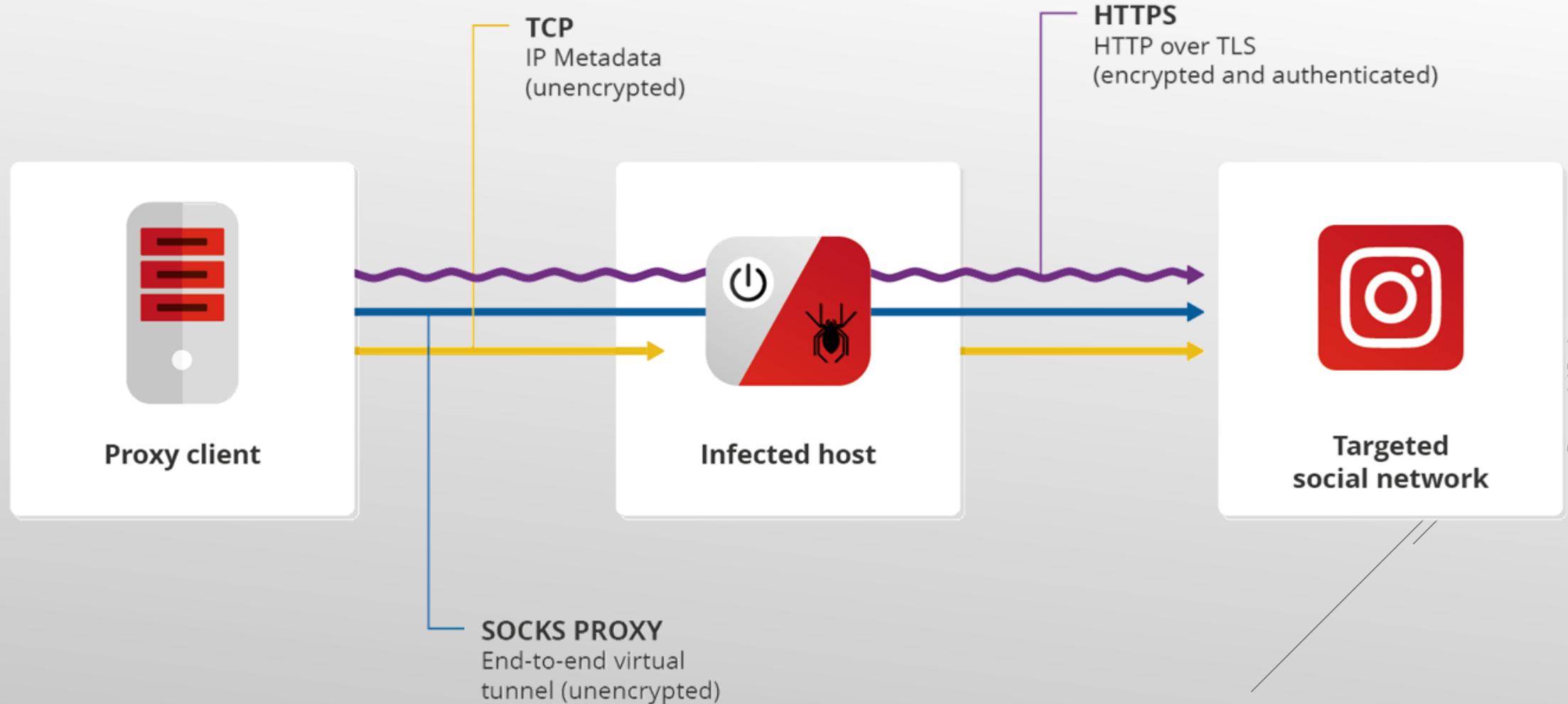
Attacking Linux/Moose



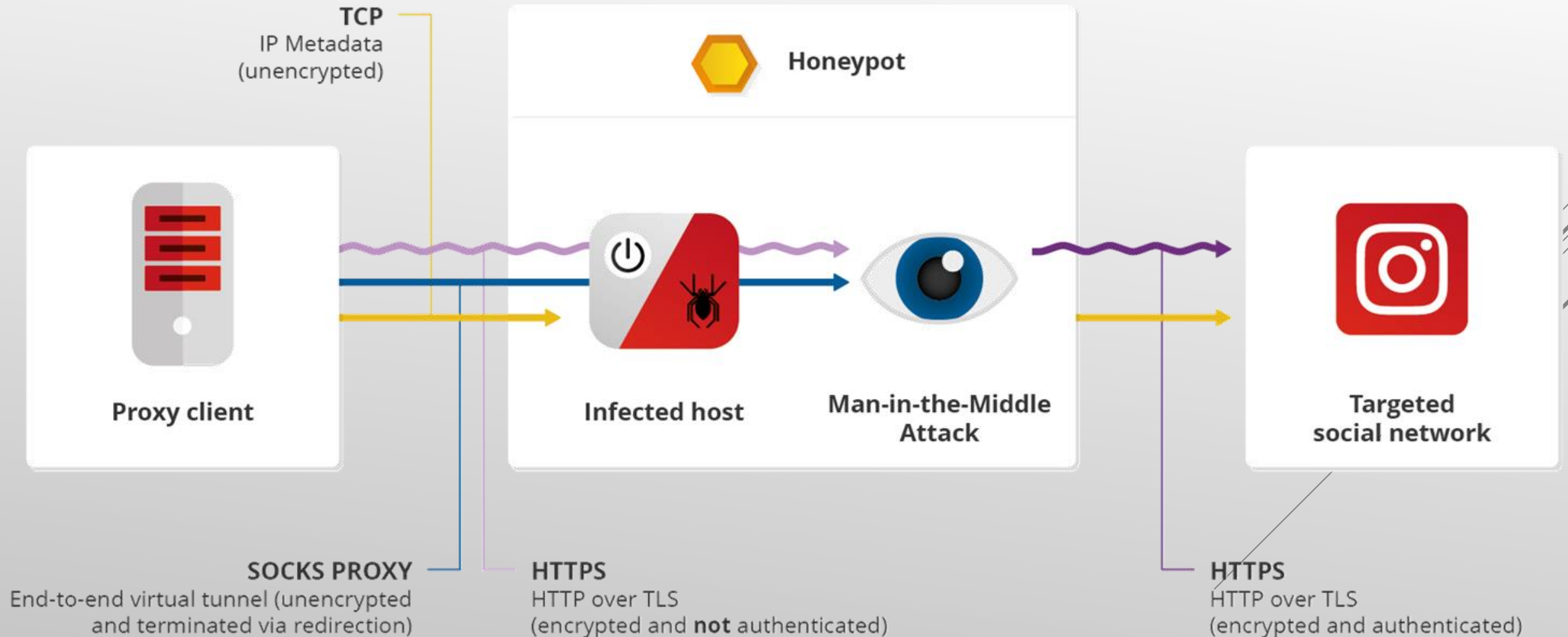
STRIPPING THE “S” FROM HTTPS

- ▶ Once infected, HTTPS traffic was flowing to social networks
 - ▶ Possible to extract targeted sites via X.509 Certificate Common Name (CN)
 - ▶ Limits what we can study
- 

HOW THE BOTS ARE RELAYING TRAFFIC



HTTPS MAN-IN-THE-MIDDLE ATTACK

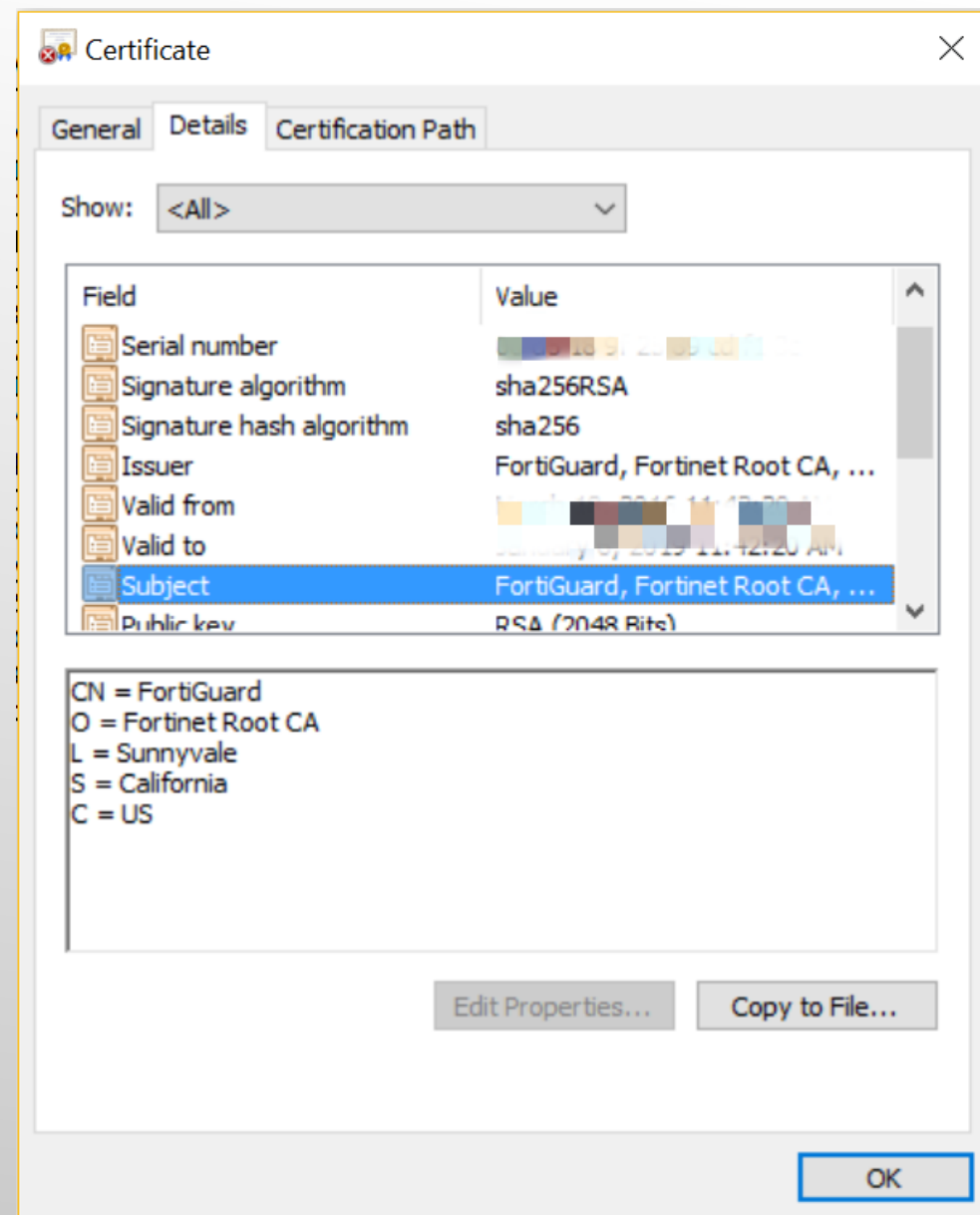


MOUNTING THE ATTACK

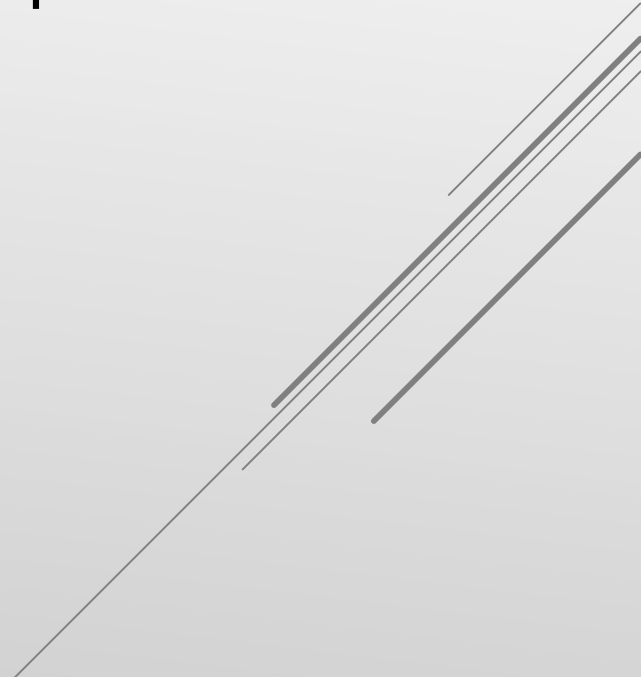
- ▶ Redirect outgoing HTTP/HTTPS to mitm process
 - ▶ Avoid trapping C&C traffic
 - ▶ Craft a Certificate Authority
 - ▶ Cross fingers
- 
- A series of several thin, parallel diagonal lines in the bottom right corner of the slide, extending from the bottom edge towards the right edge.

A HINT OF SOCIAL ENGINEERING

- Mimic a TLS inspection security appliance in your Certificate Authority



A FAILURE

- ▶ Patched bettercap: to disable HSTS Bypass
 - ▶ Used lots of resources
 - ▶ Segfaults
 - ▶ No machine parsable logs
- 
- A series of several thin, parallel diagonal lines in the bottom right corner of the slide, extending from the middle of the right edge towards the bottom right corner.

TRYING MITMPROXY

- ▶ mitmproxy in transparent proxy mode
 - ▶ Running for months
 - ▶ Has a library to parse logs
- 

MAN-IN-THE-MIDDLE A BOTNET

Success!

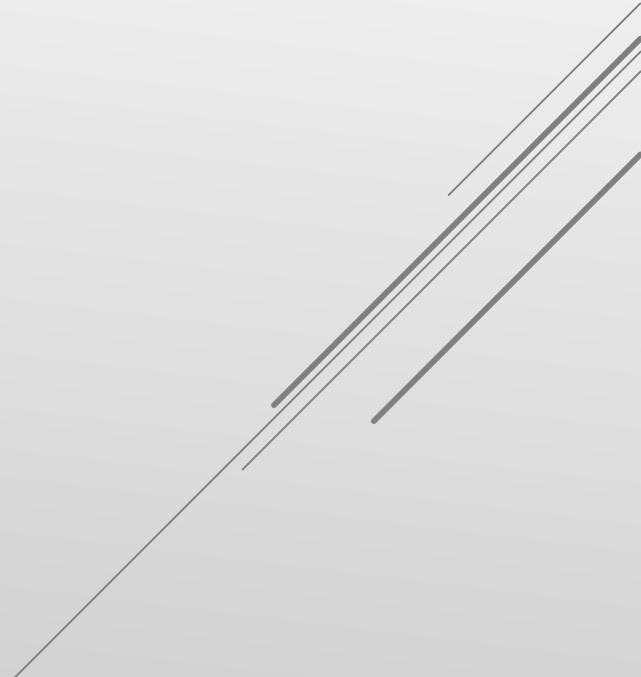
Botnet operators disregarded the “Certificate Error” generated by our fake certificate

Several thin, parallel diagonal lines in a light gray color are positioned in the bottom right corner of the slide, extending from the bottom edge towards the right edge.

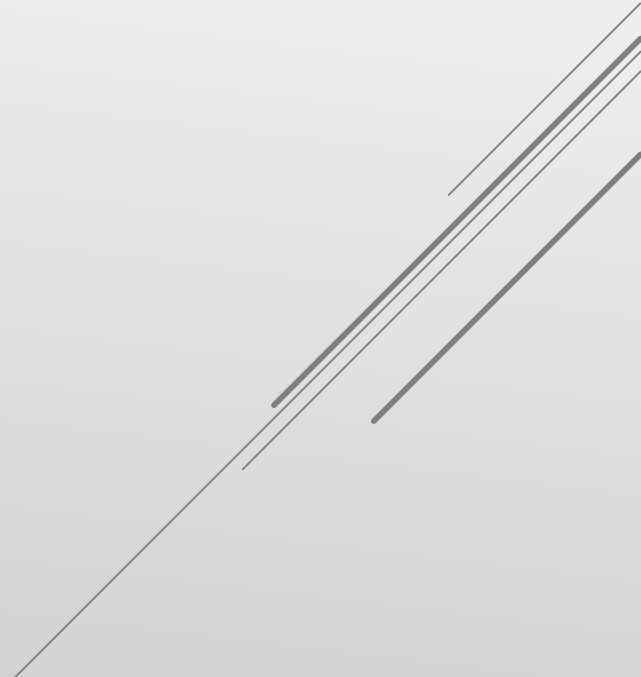


SO,

WHERE ARE WE AT?



WE HAVE

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

OUR FINDINGS

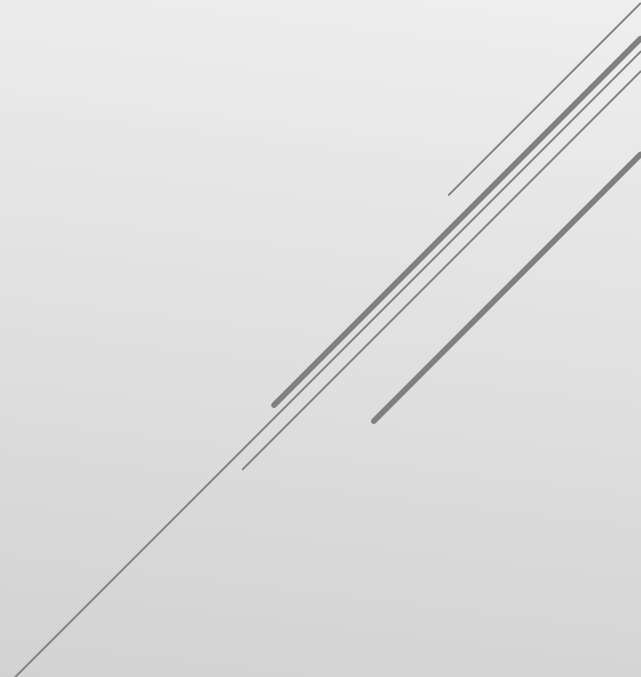


Linux/Moose Botnet



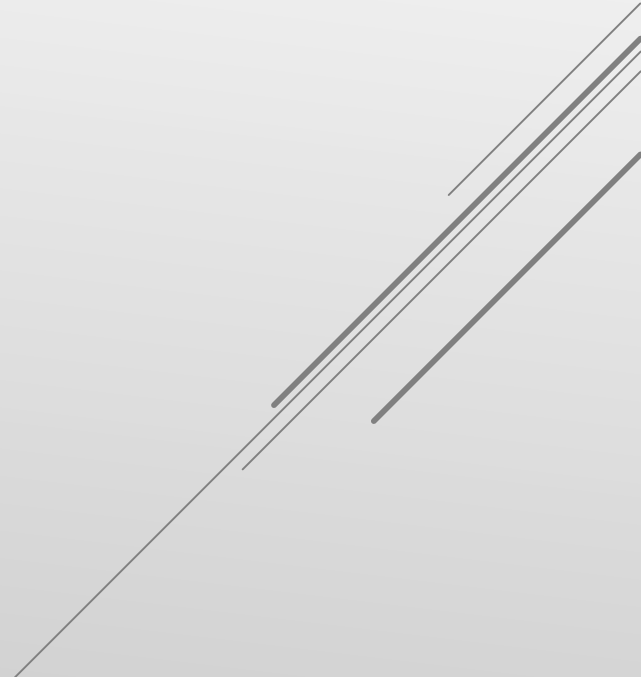


Stealthy



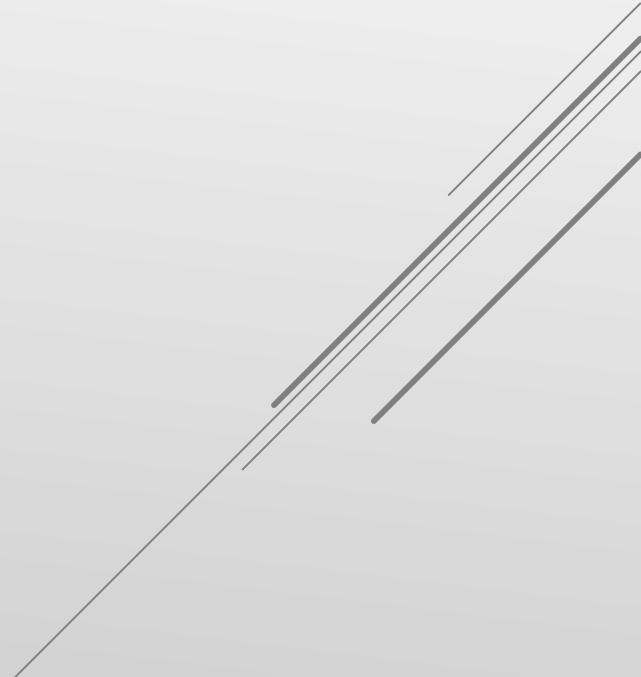
LINUX/MOOSE

- ▶ No x86 version
- ▶ No ad fraud, DDoS or spam
- ▶ No persistence mechanism

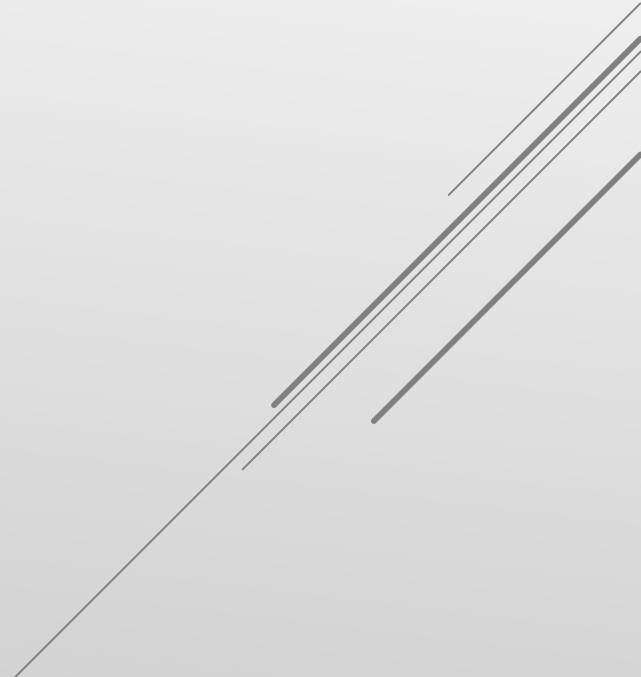




**Constantly
adapting**

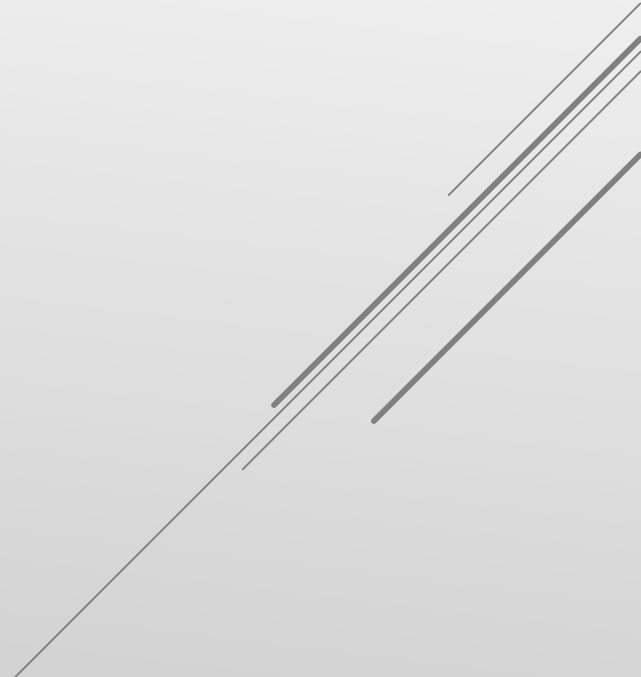


CHANGES AFTER ESET'S REPORT

- ▶ C&C IP Address
 - ▶ Provided via command-line (on infection)
 - ▶ Obfuscated (XOR + packed as Int)
 - ▶ Proxy service port changed
 - ▶ Updated bot vetting process
 - ▶ New HTTP-looking protocol with C&C
- 




**No direct
victims**



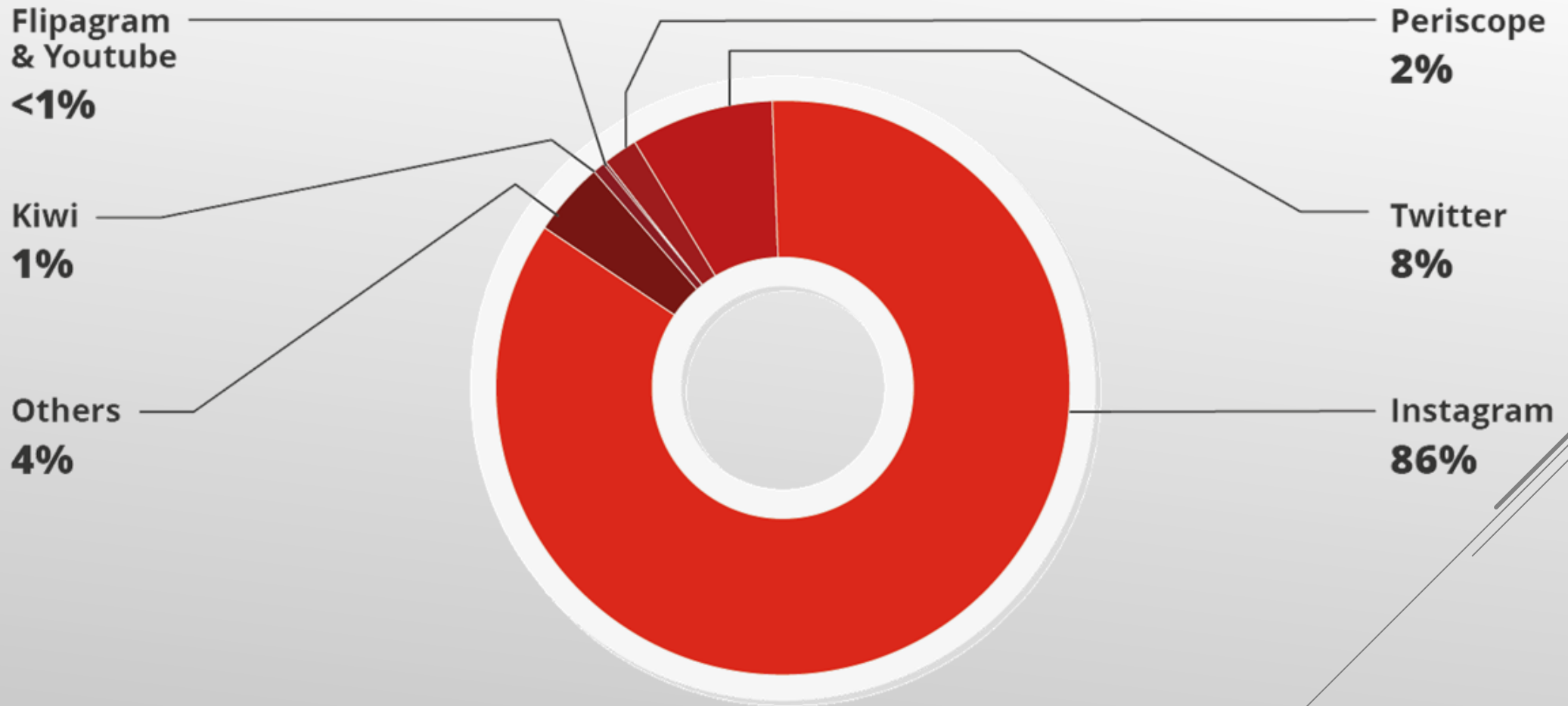
ON LINUX/MOOSE EXISTENCE

Social media fraud:

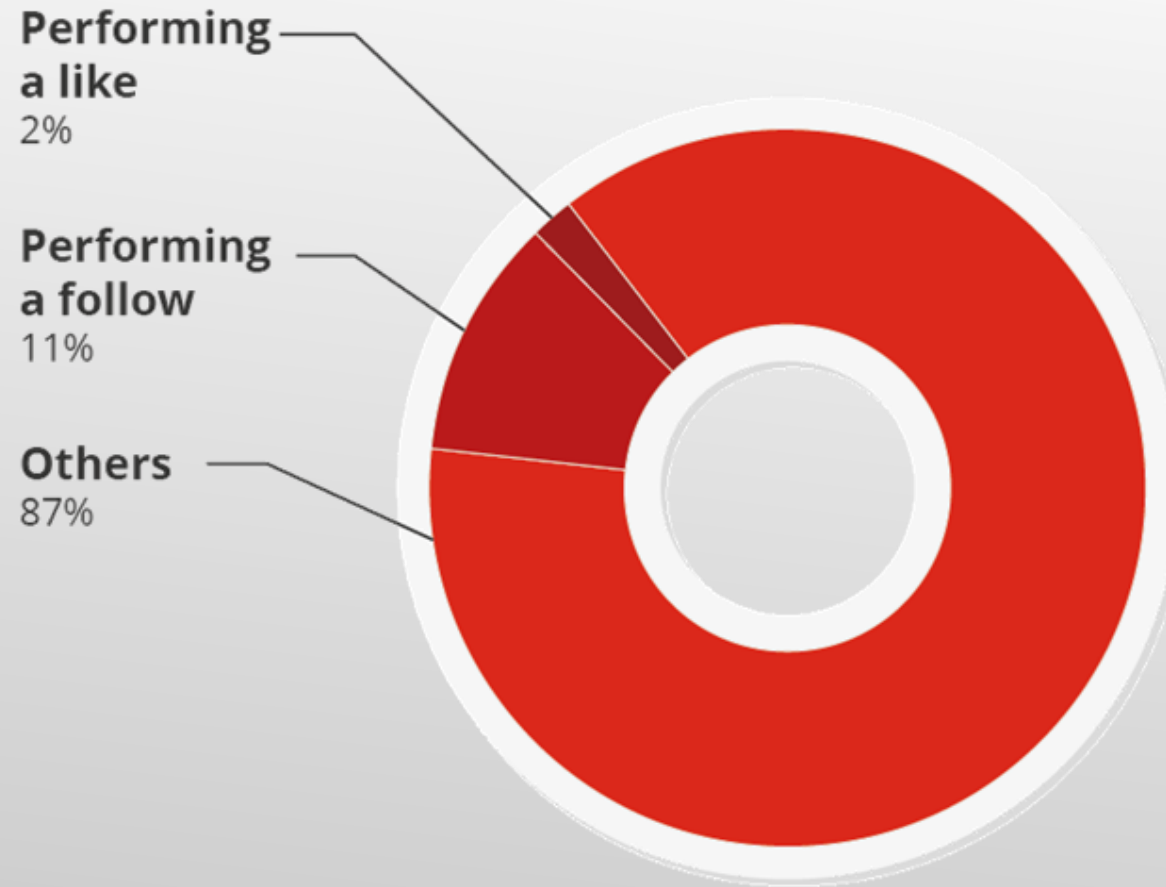
“The process of creating false endorsements of social networks accounts in order to enhance a user’s popularity and visibility.”

A series of thin, parallel diagonal lines in the bottom right corner of the slide, extending from the bottom edge towards the right edge.

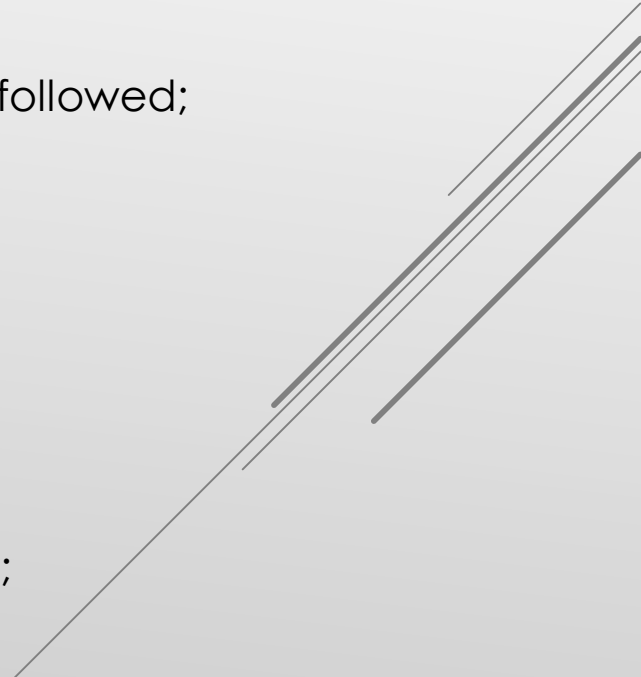
LINUX/MOOSE'S TRAFFIC



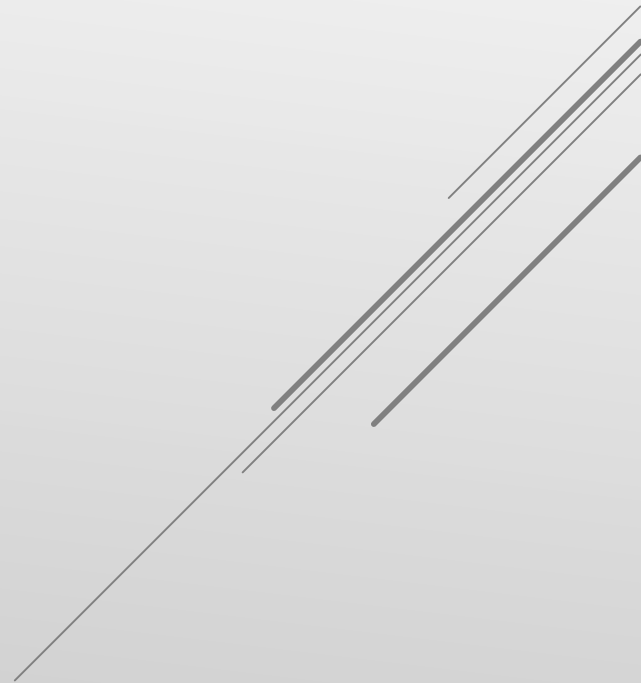
WHAT IT DOES ON INSTAGRAM



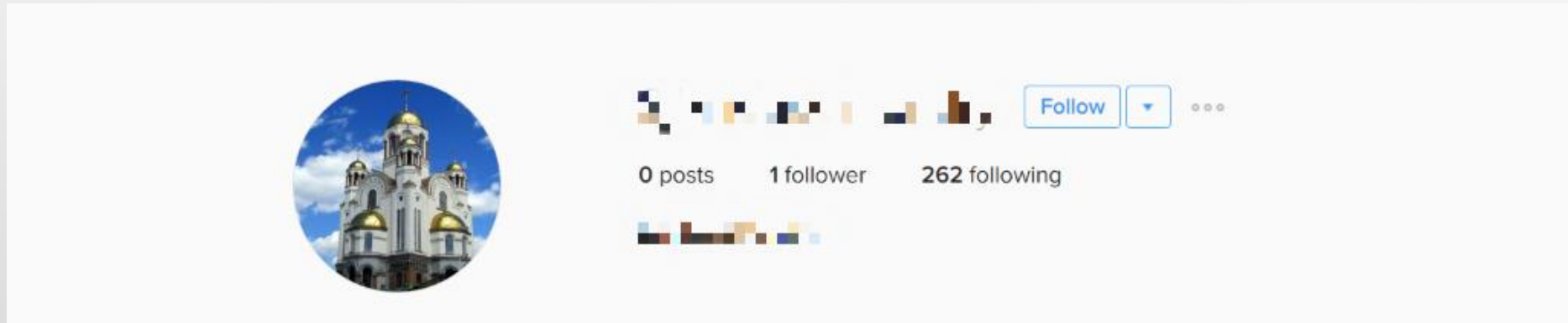
VARIOUS *MODUS OPERANDI*

1. Visiting own inbox
 2. Looking at potential recipients to send a message
 3. Visiting own personal timeline
 4. Visiting own inbox
 5. Looking at potential recipients to send a message
 6. Visiting again own inbox
 7. Loading the feed of the account of the targeted account to be followed;
 8. Requesting basic information about the account;
 9. Searching for the targeted account to be followed;
 10. Searching again for the targeted account;
 11. Requesting basic information about the account;
 12. Looking at the friendship status with the account;
 13. Loading the feed of the account;
 14. Requesting a list of other accounts, according the profile loaded;
 15. Following the targeted account;
- 

SUCCESS RATE: **89%**

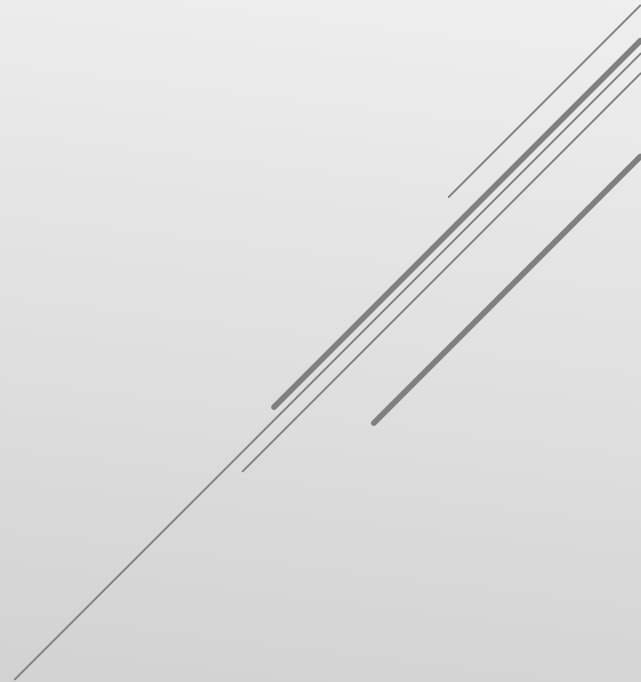


BUT... FOLLOWS DON'T LAST



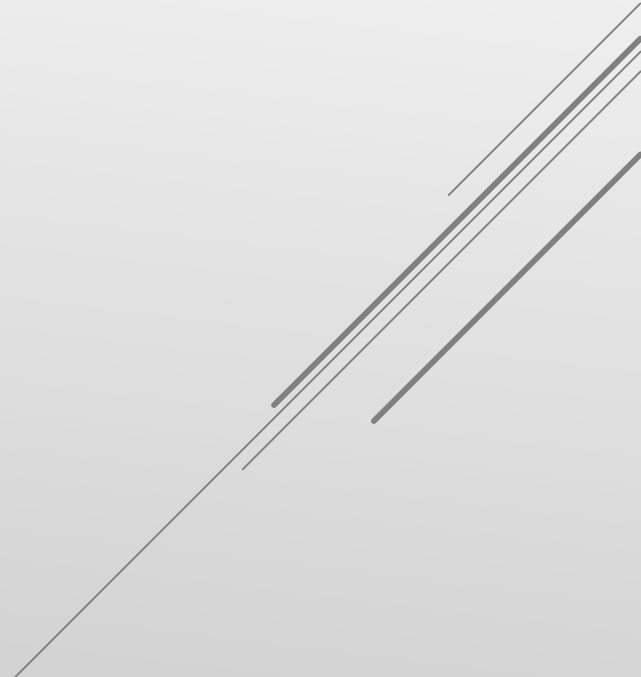
Of 1,732 fake accounts, 1,247 (72%) were suspended by Instagram

BUYERS ARE GETTING RIPPED OFF!



BUYERS

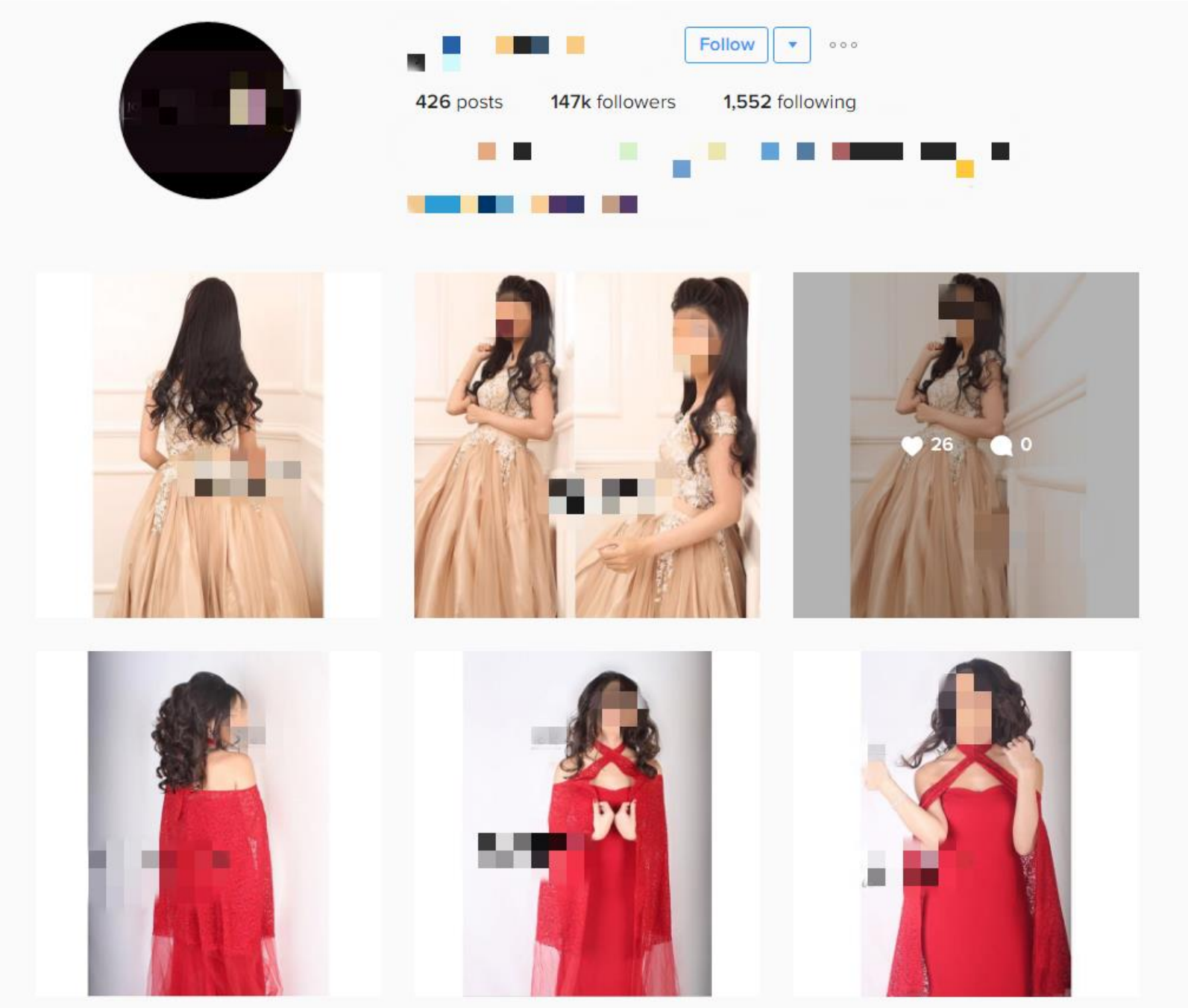
WHO ARE THEY?



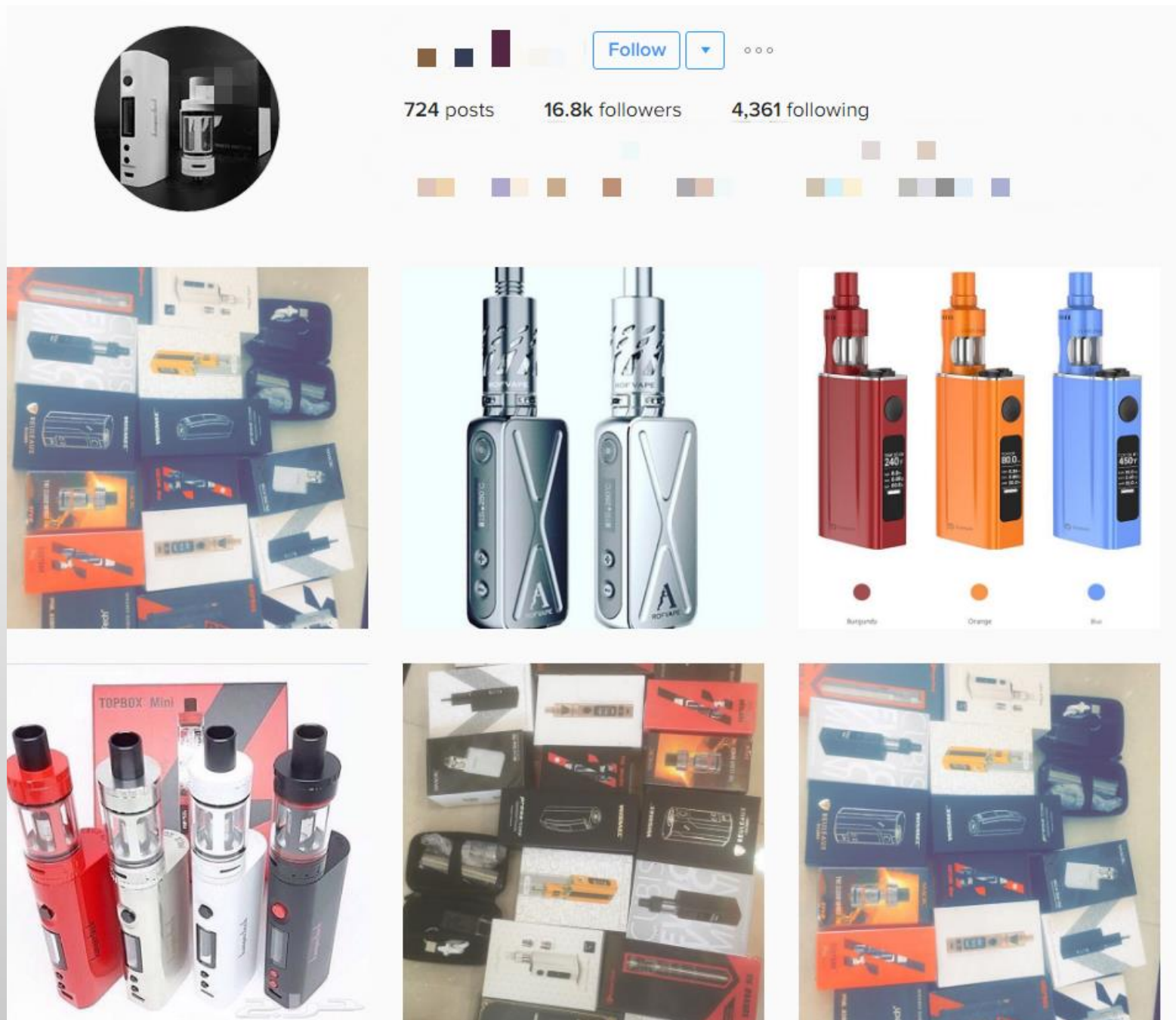
DETERMINING POTENTIAL BUYERS:

- ▶ Profiles on which follows were performed by Linux/Moose
 - ▶ Active profiles with lots of followers AND no reaction when new pictures are posted
 - ▶ Went through 500 profiles
- 
- A series of thin, parallel diagonal lines in the bottom right corner of the slide, extending from the middle of the right edge towards the bottom right corner.

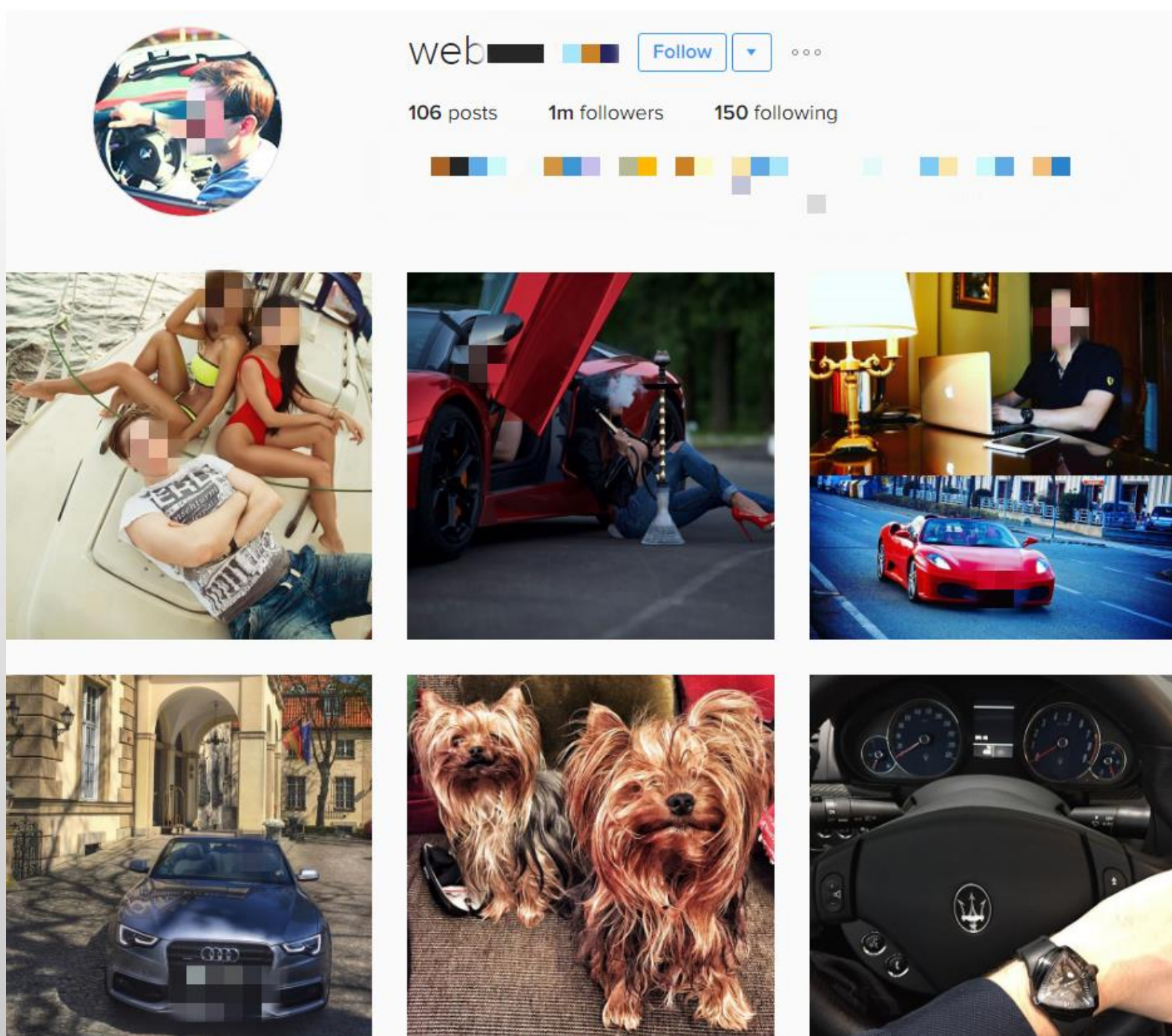
FOR EXAMPLE



BUSINESS-RELATED ACCOUNTS



BUSINESS-RELATED
ACCOUNTS,
BUT CENTERED
AROUND
AN INDIVIDUAL



ASPIRING CELEBRITIES





Follow



745 posts

1m followers

10 following



Follow



265 posts

633k followers

6,289 following



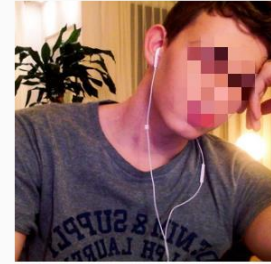
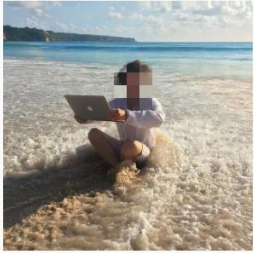
Follow



126 posts

101k followers

6,830 following



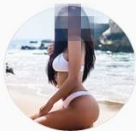
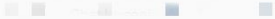
Follow



221 posts

547k followers

43 following



Follow



22 posts

112k followers

71 following



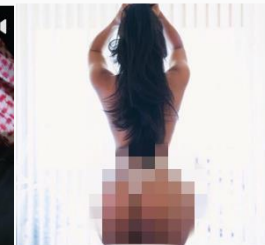
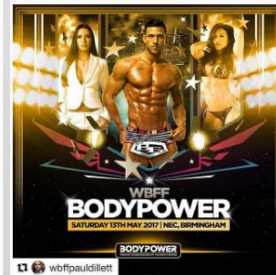
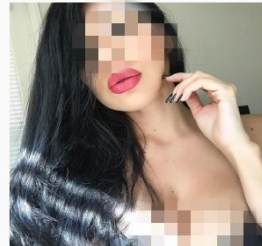
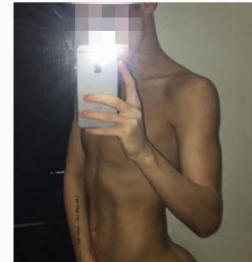
Follow



833 posts

243k followers

409 following

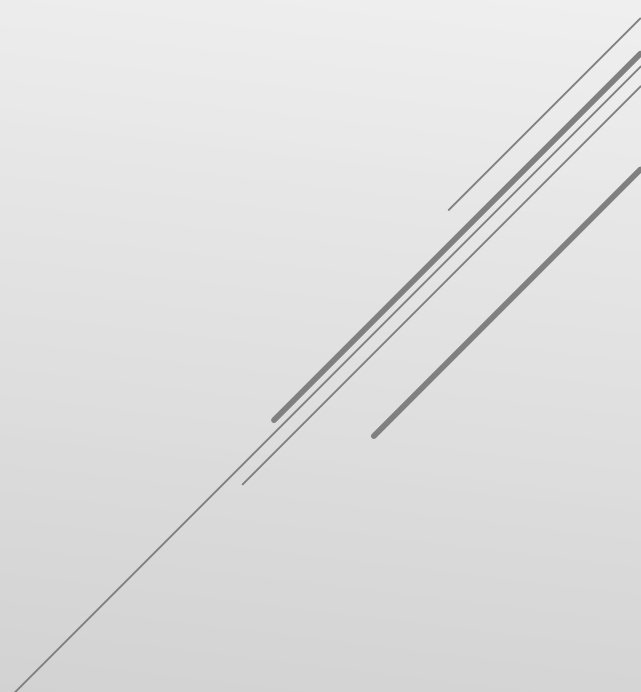


EGO MARKET?

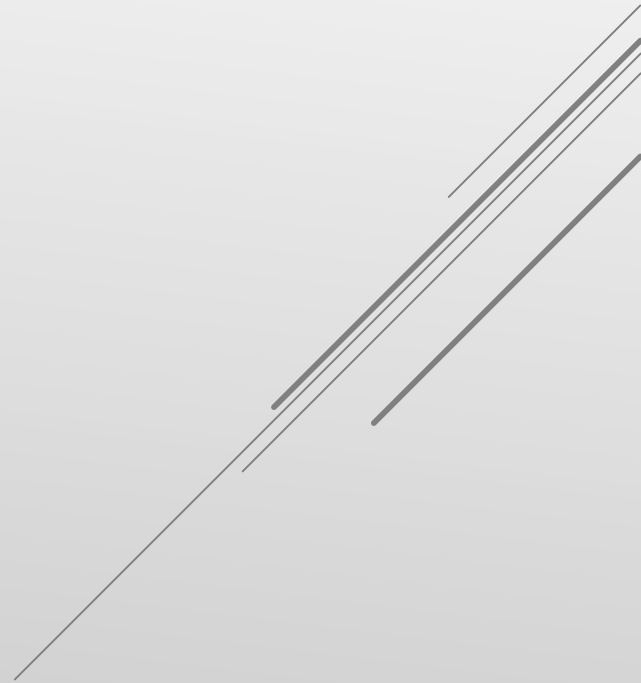


NO DIRECT VICTIMS

- ▶ Only those that get fooled by the “false popularity”
- ▶ Making criminal money by selling to
COMMON PEOPLE!!

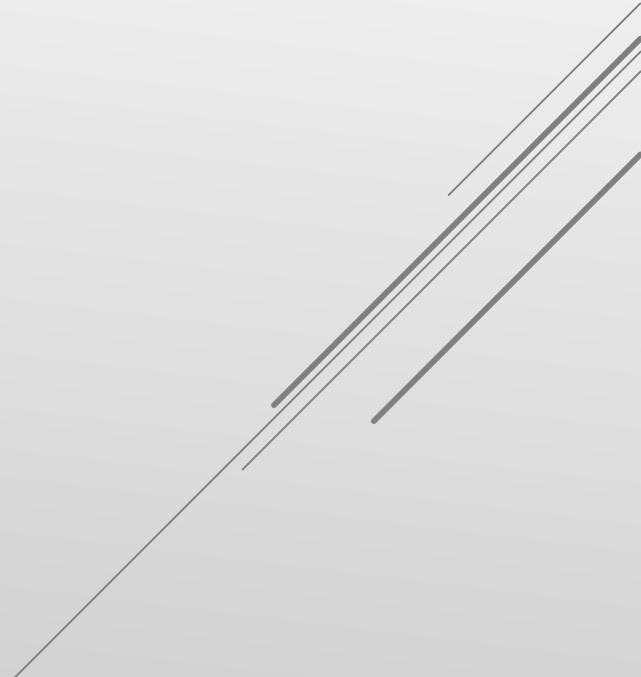


SELLERS

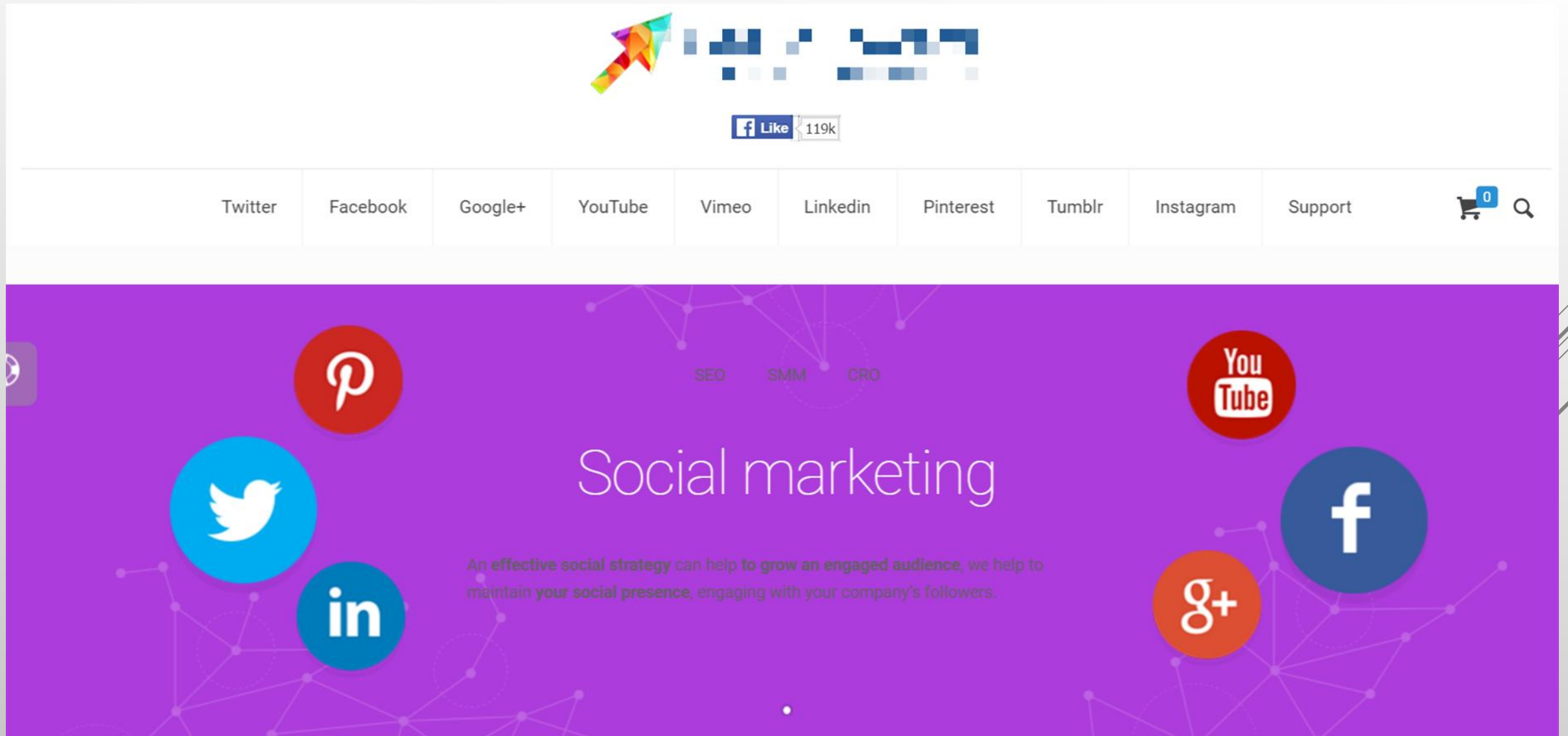




**Hiding in
plain sight**



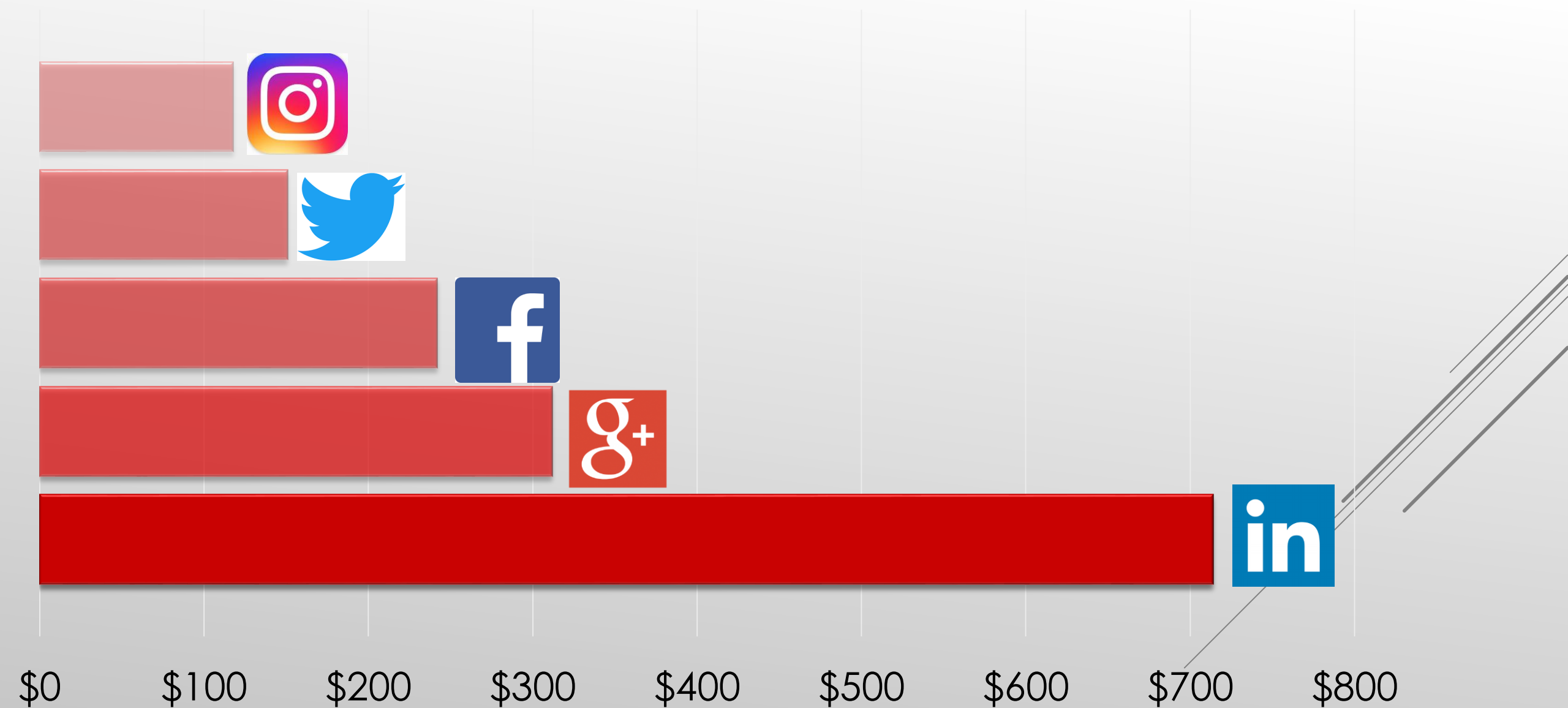
WEBSITES



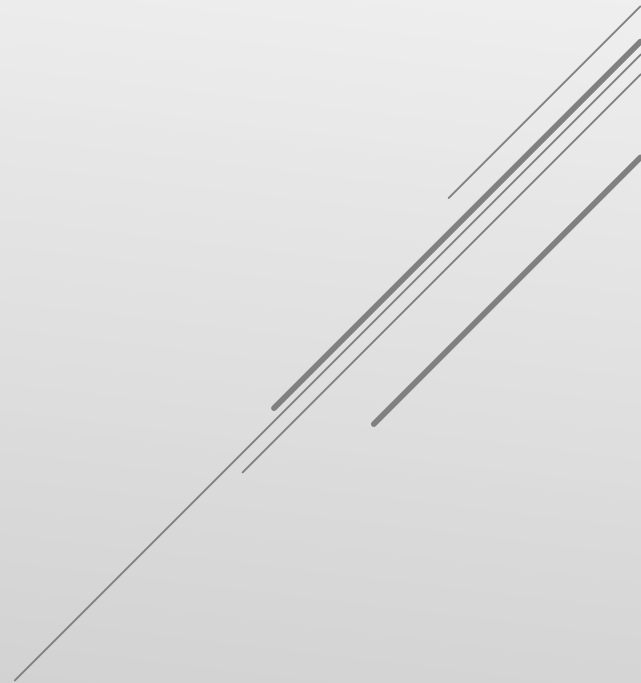
PRICE BUNDLES

100 Followers	500 Followers	1,000 Followers	5,000 Followers	10,000 Followers	50,000 Followers
\$2.95	\$6.95	\$9.95	\$39.95	\$64.95	\$249.95
Instant delivery guaranteed	Instant delivery guaranteed	Instant delivery guaranteed	Instant delivery guaranteed	Instant delivery guaranteed	Instant delivery guaranteed
Quality profiles	Quality profiles	Quality profiles	Quality profiles	Quality profiles	Quality profiles
100% safe	100% safe	100% safe	100% safe	100% safe	100% safe
Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now


PRICE FOR 10,000 FOLLOWS





HERE IS A LITTLE STORY





FOUND A SELLER THAT SOLD


 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

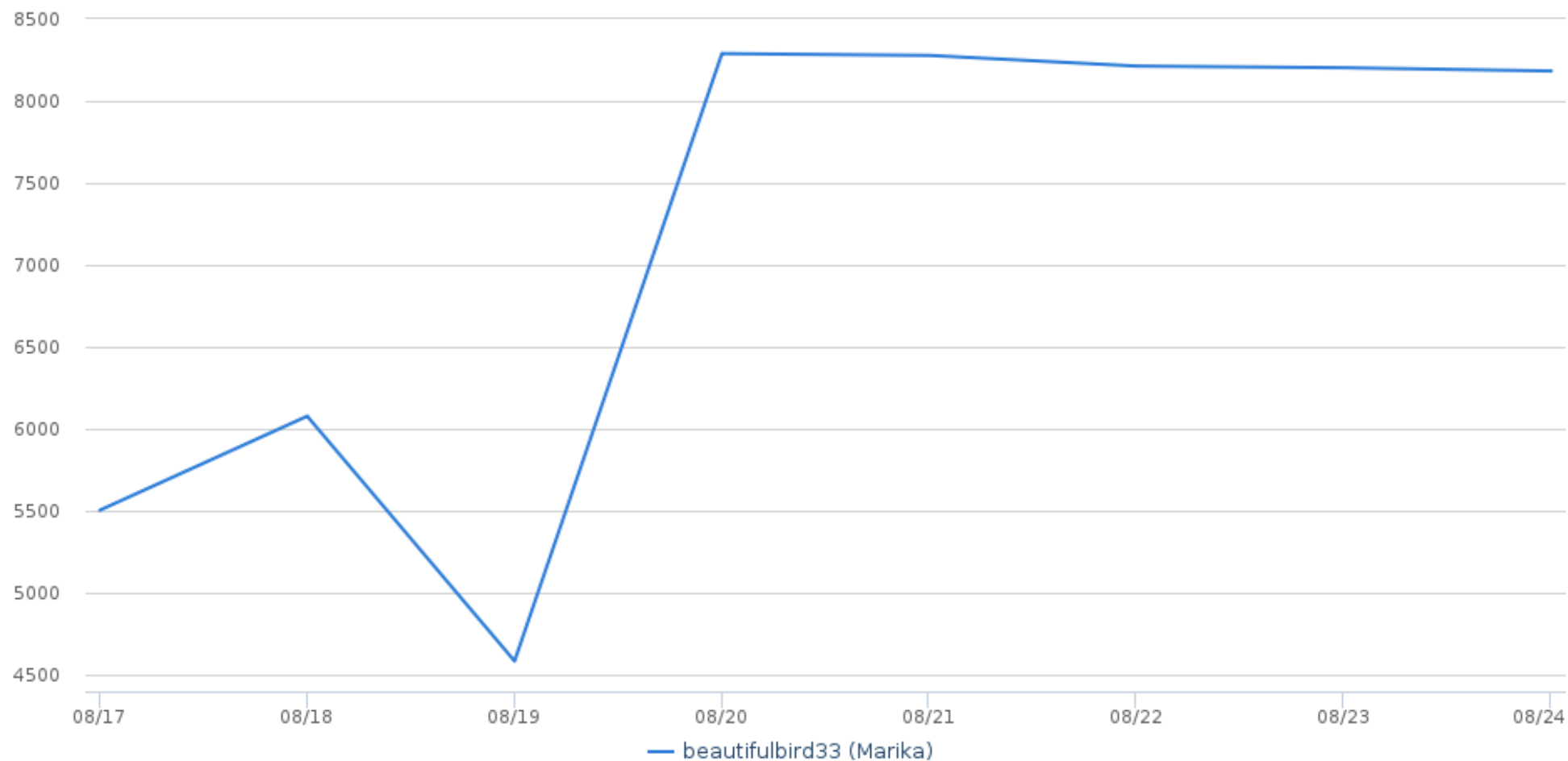


Marika I'm a young photographer. Just starting on social media. Follow me for outstanding seasonal photos. For now: White and Cold; Gloomy and Sparkling.


8 posts

8,054 followers

72 following



1.



Hi,

I bought 6000 followers from your website last week. They were provided throughout the weekend.

However, since Monday, I have lost 500 followers. Could you please provide these 500 followers again?


My account is : beautifulbird33

I need these 500 followers for a contest in winter photography.

Regards,

Marika

2.




À moi

...

sure , adding:)

3.



A

Hey,


I lost 1100 followers a few days back. Can you push me up again?

Thanks,

Mari

...

4.

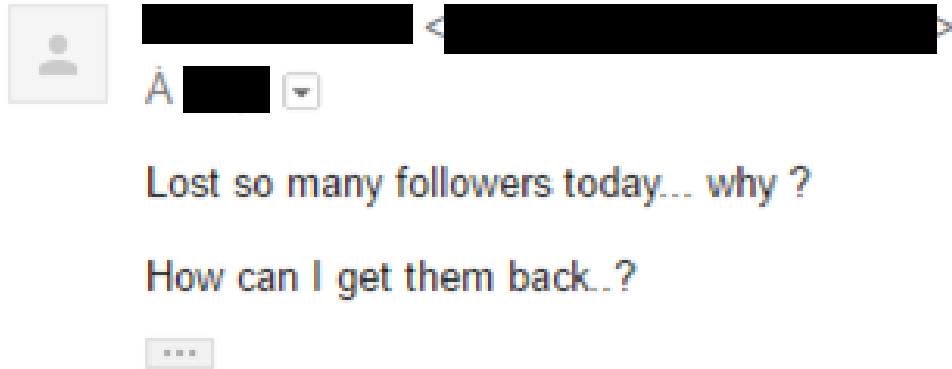


À moi

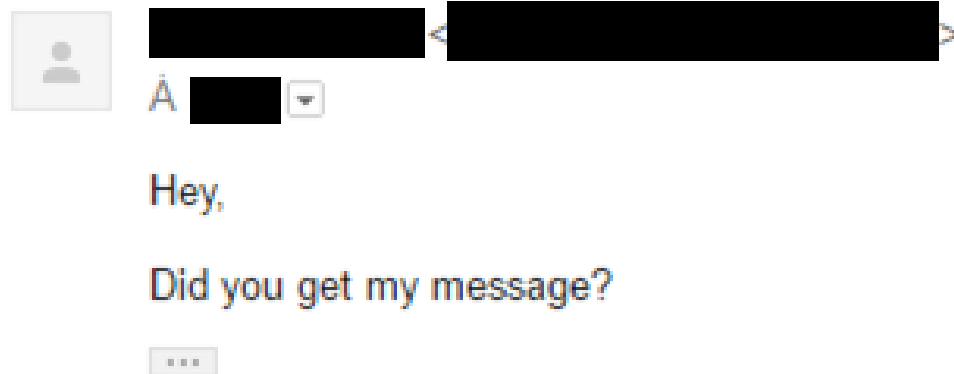
...

im adding , well followers are not forever but im adding them whenu ask for

5.



6.





beautifulbird33

Edit Profile

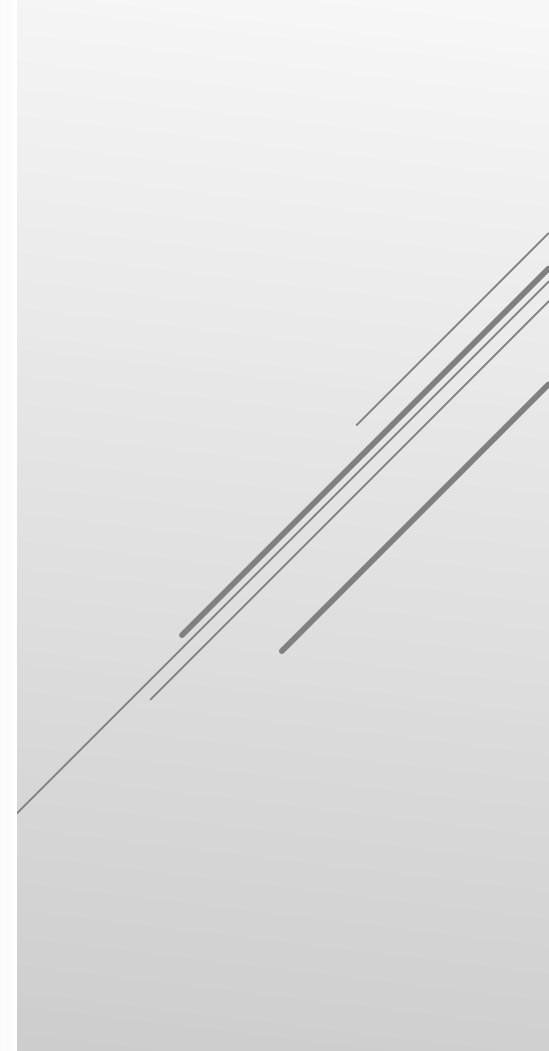
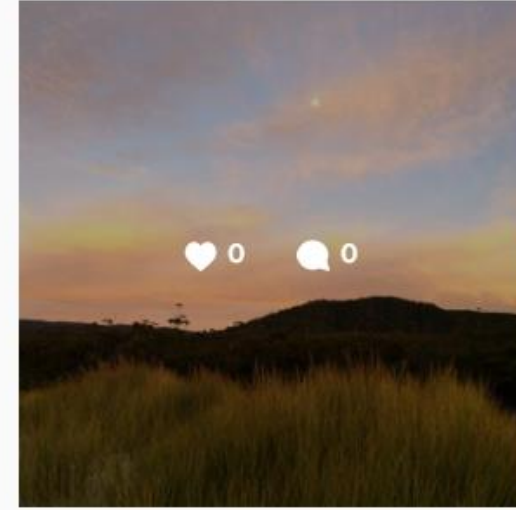


11 posts

1,198 followers

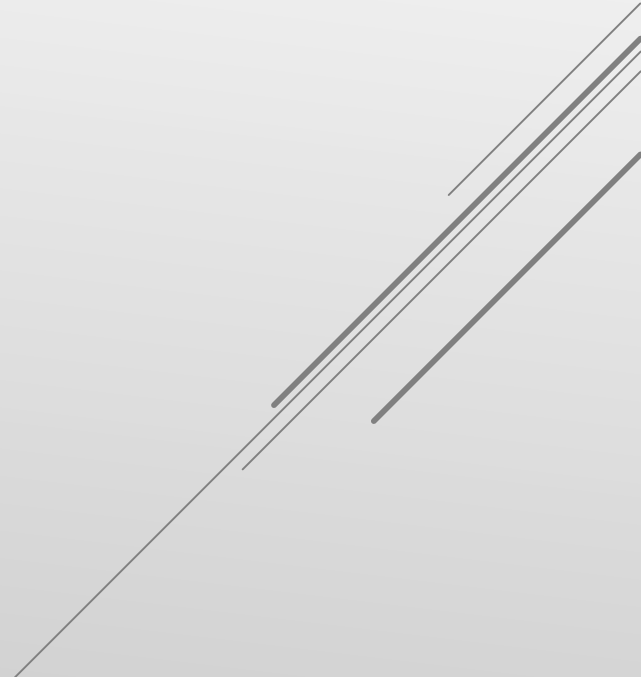
72 following

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





**Large potential
profitability**



POTENTIAL REVENUE OF LINUX/MOOSE

On average, our honeypots performed **1,186 follows** per month on Instagram

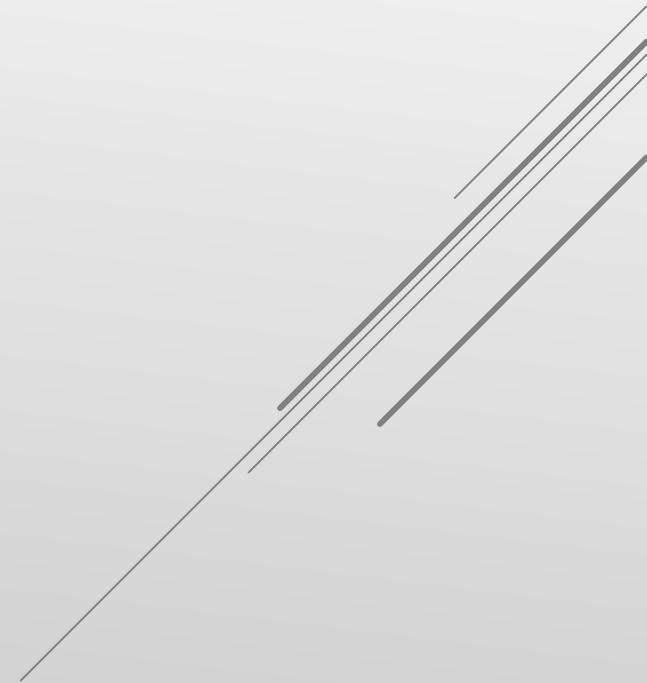
On average, the price is US \$112.67 for 10,000 follows

Or US \$0.0011 per follow

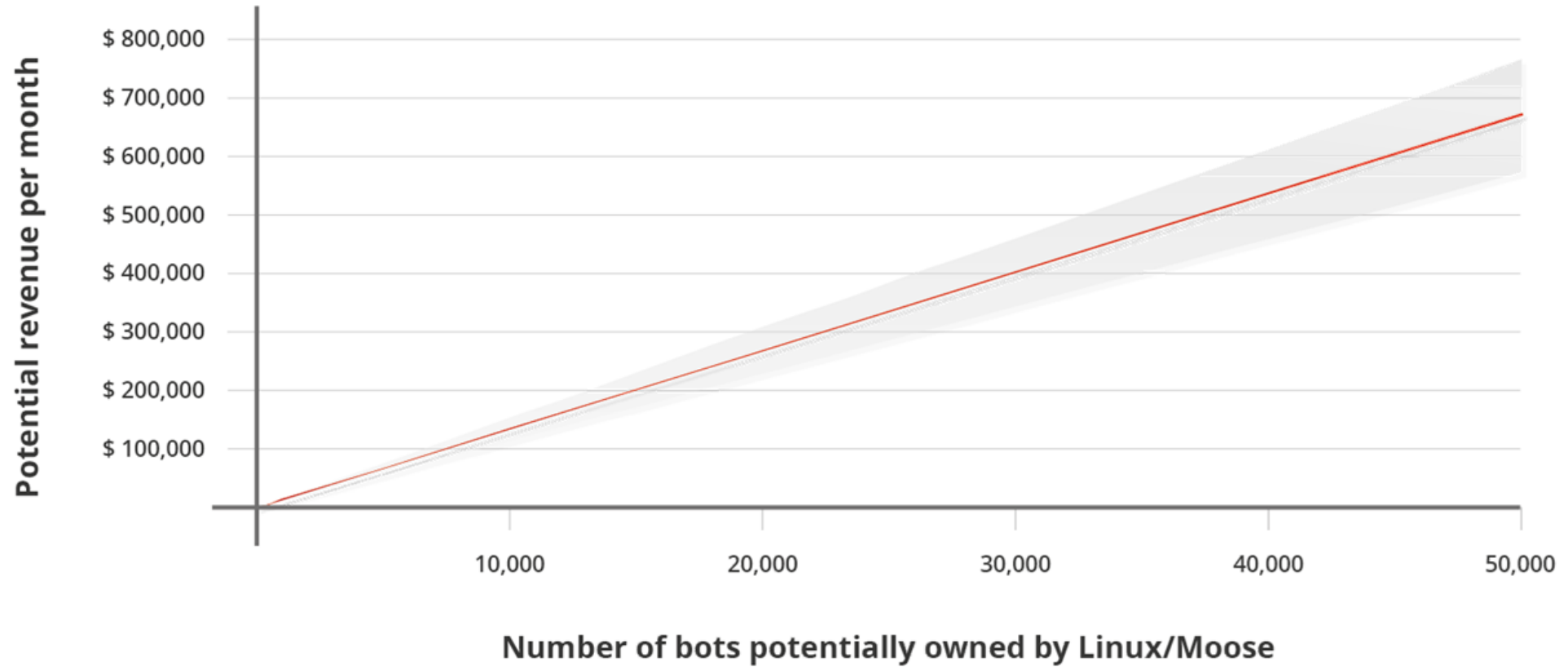


LINUX/MOOSE POTENTIAL REVENUE

13.05\$ per month per bot



Linux/Moose Potential Revenue







Linux/Moose Botnet



Stealthy



**Constantly
adapting**



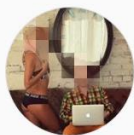
**No direct
victims**



**Hiding in
plain sight**



**Large potential
profitability**



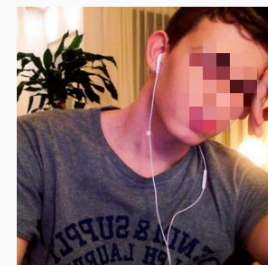
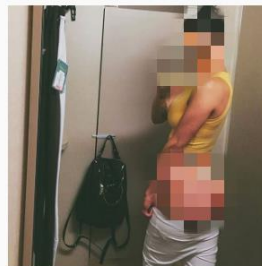
745 posts 1m followers 10 following



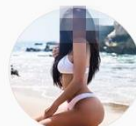
265 posts 633k followers 6,289 following



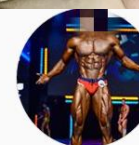
126 posts 101k followers 6,830 following



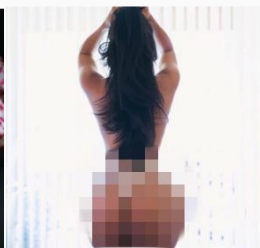
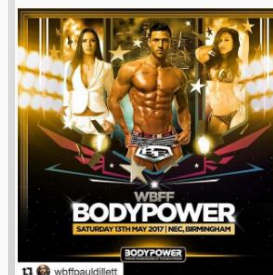
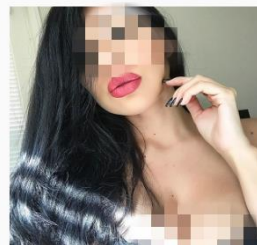
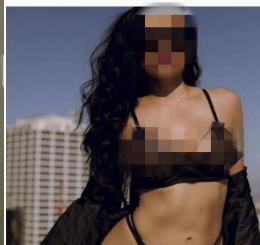
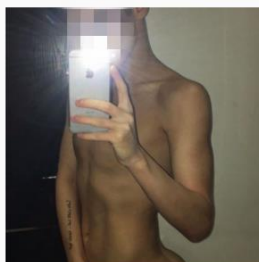
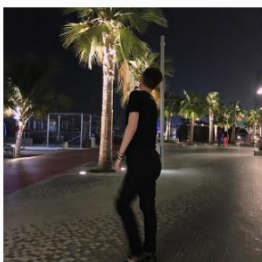
221 posts 547k followers 43 following



22 posts 112k followers 71 following



833 posts 243k followers 409 following



SO PERFECT THAT

- Could not raise any interest from:
 - law enforcement
 - hosting providers (takedown)



AND

We lost faith in Humanity

QUESTIONS?

- ▶ Masarah Paquet-Clouston
- ▶ mcpc@gosecure.ca
- ▶ @masarahclouston
- ▶ Olivier Bilodeau
- ▶ obilodeau@gosecure.ca
- ▶ @obilodeau

Linux/Moose IoCs:

<https://github.com/eset/malware-ioc/tree/master/moose>

Ego Market Research (paper and blog):

<https://gosecure.net/blog/>

THANKS!