EGO MARKET
WHEN GREED FOR FAME BENEFITS LARGE-SCALE BOTNETS

Masarah Paquet-Clouston
Olivier Bilodeau
GoSecure Inc.
Masarah Paquet-Clouston  Olivier Bilodeau

- Researcher at GoSecure Inc.
- Master student in Criminology at Université de Montréal
- Treasurer for the Northsec conference
- Security Research Lead at GoSecure Inc.
- VP training for the Northsec Conference and CTF
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
Two additional authors:
- David Décary-Hétu, Université de Montréal
- Thomas Dupuy, ESET
THE STORY OF LINUX/MOOSE
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
Elan = Moose in French
LOTUS ELAN
SLOVAK MUSIC GROUP CALLED ELAN
'Moose' malicious worm targets home routers

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

Malware can infect IoT devices—including medical devices—with weak authentication.
THE COMMAND & CONTROL (C&C) SERVERS WENT DARK

Until September 2015
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

Infected host
Linux/Moose
ARM Linux
QEMU

Cowrie
Router userland
Busybox environment
Telnet service

mitmproxy

iptables
dumpcap

Network
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...
CONTRIBUTED TELNET TO COWRIE

Basic Telnet support implemented
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

obiodeau committed with micheloosterhof on Aug 14

Showing 13 changed files with 461 additions and 38 deletions.
I merged Telnet support into the #cowrie SSH honeypot. Thanks @obilodeau ! Check cowrie.cfg.dist for options.
HONEYPOT COMPONENTS

- Infected host
  - QEMU
  - Debian Linux ARM image
  - Plant Linux/Moose binary
  - Run it
CATCHING LINUX/MOOSE

Honeypot

Infected host
- Linux/Moose
- ARM Linux
- QEMU

Cowrie
- Router userland
- Busybox environment
- Telnet service

mitmproxy

Network
- iptables
- dumpcap
Attacking Linux/Moose
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

- **TCP**: IP Metadata (unencrypted)
- **HTTPS**: HTTP over TLS (encrypted and authenticated)
- **SOCKS PROXY**: End-to-end virtual tunnel (unencrypted)
HTTPS MAN-IN-THE-MIDDLE ATTACK

TCP
IP Metadata (unencrypted)

Proxy client

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

Honeypot

Infected host

Man-in-the-Middle Attack

Targeted social network

HTTPS
HTTP over TLS (encrypted and not authenticated)

HTTPS
HTTP over TLS (encrypted and authenticated)
MOUNTING THE ATTACK

- Redirect outgoing HTTP/HTTPS to mitm process
- Avoid trapping C&C traffic
- Craft a Certificate Authority
- Cross fingers
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
TRYING MITMPROXY

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

Botnet operators disregarded the “Certificate Error” generated by our fake certificate.
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
- Constantly adapting
- No direct victims
- Hiding in plain sight
- Large potential profitability
LINUX/MOOSE

- No x86 version
- No ad fraud, DDoS or spam
- No persistence mechanism
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
Social media fraud:

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

- Performing a like: 2%
- Performing a follow: 11%
- Others: 87%
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
FOR EXAMPLE
BUSINESS-RELATED ACCOUNTS
BUSINESS-RELATED ACCOUNTS, BUT CENTERED AROUND AN INDIVIDUAL
ASPIRING CELEBRITIES
EGO MARKET?
NO DIRECT VICTIMS

- Only those that get fooled by the “false popularity”
- Making criminal money by selling to COMMON PEOPLE!!
SELLERS
Buy 1000 FOLLOWERS

Hiding in plain sight
Social marketing

An effective social strategy can help to grow an engaged audience, we help to maintain your social presence, engaging with your company's followers.
<table>
<thead>
<tr>
<th></th>
<th>100 Followers</th>
<th>500 Followers</th>
<th>1,000 Followers</th>
<th>5,000 Followers</th>
<th>10,000 Followers</th>
<th>50,000 Followers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Followers</td>
<td>$2.95</td>
<td>$6.95</td>
<td>$9.95</td>
<td>$39.95</td>
<td>$64.95</td>
<td>$249.95</td>
</tr>
<tr>
<td>Instant delivery guaranteed</td>
<td>Quality profiles</td>
<td>Quality profiles</td>
<td>Quality profiles</td>
<td>Quality profiles</td>
<td>Quality profiles</td>
<td>Quality profiles</td>
</tr>
<tr>
<td>Quality profiles</td>
<td>100% safe</td>
<td>100% safe</td>
<td>100% safe</td>
<td>100% safe</td>
<td>100% safe</td>
<td>100% safe</td>
</tr>
<tr>
<td>100% safe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Buy Now**
PRICE FOR 10,000 FOLLOWS

- Instagram
- Twitter
- Facebook
- Google+
- LinkedIn
HERE IS A LITTLE STORY
FOUND A SELLER THAT SOLD
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
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

Hey,

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

Thanks,

Mari

À moi

... sure, adding:

À moi

... im adding, well followers are not forever but im adding them when u ask for
5. Lost so many followers today... why?
   How can I get them back?...

6. Hey,
   Did you get my message?...
Marika I'm a young photographer. Just starting on social media. Follow me for outstanding seasonal photos. For now: Summertime! but still quite cold.
AND...
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

Number of bots potentially owned by Linux/Moose

Potential revenue per month

$ 800,000
$ 700,000
$ 600,000
$ 500,000
$ 400,000
$ 300,000
$ 200,000
$ 100,000

$ 10,000
$ 20,000
$ 30,000
$ 40,000
$ 50,000
Linux/Moose Botnet

- Stealthy
- Constantly adapting
- No direct victims
- Hiding in plain sight
- Large potential profitability

Buy 1000 Followers
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!