Linux/Moose endangered or extinct?

An update on this atypical embedded Linux botnet

by Olivier Bilodeau
$ apropos

- Statically linked stripped ELF challenges
- Moose DNA (description)
- Moose Herding (the Operation)
- A Strange Animal
- Latest Developments
$ whoami

- Malware Researcher at ESET
- Infosec lecturer at ETS University in Montreal
- Previously
  - infosec developer, network admin, linux system admin
- Co-founder Montrehack (hands-on security workshops)
- Founder NorthSec Hacker Jeopardy
Static/stripped ELF primer

- No imports (library calls) present
- All the code bundled together down to kernel syscall
- Disassembler (if available for arch) doesn’t help much
Linux/Moose binary in IDA
printf family
WE HAVE TO GO
DEEPER!
Ecosystem makes it worst [for reversers]

- GCC and GNU libc is always changing so compiled binaries always change
- Little IDA FLIRT signatures available (if any)
- µClibc, eglibc, glibc, musl, ...
A Failed Attempt

- Map syscalls with IDA script
- But libc is too big it is still too much
Better Solution

- Reproduce environment (arch, libc/compiler versions)
- Build libraries w/ symbols under same conditions
- Use bindiff to map library functions
- Focus on malware code
<table>
<thead>
<tr>
<th>similarity</th>
<th>confid</th>
<th>change</th>
<th>EA primary</th>
<th>name primary</th>
<th>EA secondary</th>
<th>name secondary</th>
<th>con</th>
<th>algorithm</th>
<th>matched bacteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>00419BE0</td>
<td>sub_419BE0_282</td>
<td>00037E60</td>
<td>strncmp</td>
<td></td>
<td>MD index matching</td>
<td>21</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>00423F20</td>
<td>sub_423F20_444</td>
<td>00034C20</td>
<td>fget</td>
<td></td>
<td>edges flowgraph</td>
<td>18</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>00422BD0</td>
<td>sub_422BD0_435</td>
<td>0002D650</td>
<td>__stdio_WRITE</td>
<td></td>
<td>edges flowgraph</td>
<td>17</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>0041B634</td>
<td>sub_41B634_308</td>
<td>0003E7A4</td>
<td>inet_pton4</td>
<td></td>
<td>edges flowgraph</td>
<td>21</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>004261A0</td>
<td>sub_4261A0_471</td>
<td>0002D790</td>
<td>__stdio_adjust_position</td>
<td></td>
<td>edges flowgraph</td>
<td>21</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>00423010</td>
<td>sub_423010_438</td>
<td>0002E1B0</td>
<td>__stdio_trans2w_o</td>
<td></td>
<td>edges flowgraph</td>
<td>17</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>004277D0</td>
<td>sub_4277D0_485</td>
<td>0003F2E0</td>
<td>__encode_dotted</td>
<td></td>
<td>edges flowgraph</td>
<td>17</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>00424790</td>
<td>sub_424790_448</td>
<td>000362F0</td>
<td>fget_unlocked</td>
<td></td>
<td>edges flowgraph</td>
<td>19</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>00424050</td>
<td>sub_424050_445</td>
<td>00035B0</td>
<td>__stdio_openlist_dec_use</td>
<td></td>
<td>edges flowgraph</td>
<td>44</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>0041B734</td>
<td>sub_41B734_310</td>
<td>0003E89C</td>
<td>inet_ntop</td>
<td></td>
<td>edges flowgraph</td>
<td>63</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>004176FC</td>
<td>sub_4176FC_237</td>
<td>000107E4</td>
<td>opendir</td>
<td></td>
<td>edges flowgraph</td>
<td>11</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>00424FF0</td>
<td>sub_424FF0_456</td>
<td>0003EE60</td>
<td>inet_aton</td>
<td></td>
<td>edges flowgraph</td>
<td>17</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>004189B0</td>
<td>sub_4189B0_260</td>
<td>00030540</td>
<td>_ppfs_init</td>
<td></td>
<td>edges flowgraph</td>
<td>16</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>00419670</td>
<td>sub_419670_268</td>
<td>00036810</td>
<td>fwrite_unlocked</td>
<td></td>
<td>edges flowgraph</td>
<td>15</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>00415628</td>
<td>sub_415628_259</td>
<td>0002FDA8</td>
<td>_vfprintf_internal</td>
<td></td>
<td>address sequence</td>
<td>136</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>00419318</td>
<td>sub_419318_265</td>
<td>000354F0</td>
<td>putchar</td>
<td></td>
<td>address sequence</td>
<td>50</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>00425F00</td>
<td>sub_425F00_469</td>
<td>0002CF30</td>
<td>fseeko64</td>
<td></td>
<td>edges flowgraph</td>
<td>32</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>0041FD70</td>
<td>sub_41FD70_384</td>
<td>0004E960</td>
<td>raise</td>
<td></td>
<td>edges flowgraph</td>
<td>15</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>004224C0</td>
<td>sub_4224C0_431</td>
<td>00024690</td>
<td>wcsnrtombs</td>
<td></td>
<td>edges flowgraph</td>
<td>19</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>00423DC0</td>
<td>sub_423DC0_443</td>
<td>00034AC0</td>
<td>getc</td>
<td></td>
<td>instruction count</td>
<td>48</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>0041340D</td>
<td>sub_41340D_307</td>
<td>0003E640</td>
<td>inet_ntop4</td>
<td></td>
<td>edges flowgraph</td>
<td>11</td>
</tr>
<tr>
<td>0.99</td>
<td>0.99</td>
<td>-I--E-</td>
<td>004285E0</td>
<td>sub_4285E0_495</td>
<td>00051DD0</td>
<td>__fixdfs</td>
<td></td>
<td>edges flowgraph</td>
<td>13</td>
</tr>
</tbody>
</table>
Moose DNA

aka Malware description

Hang tight, this is a recap
Linux/Moose...

Named after the string "elan" present in the malware executable

```
00028fc3  6E 67 00 00 00 70 61 73 73 77 6F 72 64 3A 00 00 00
00028fd4  75 74 68 65 6E 74 69 63 61 74 6F 72 64 3A 00 00 00
00028fe5  6C 65 64 00 00 00 73 68 6F 00 00 00 70 73 73
00028ffe  6D 0A 63 68 66 6F 20 20 20 20 2D 20 2D 20 20 20
00029007  4C 30 57 66 52 6C 6F 20 0D 0A 63 68 66 6F 0D 0A
00029018  00 00 00 00 48 33 6C 4C 30 57 66 52 6C 6F 00 00
00029029  5D 56 61 6C 32 00 00 00 65 6C 61 6E 66 69 63
0002903a  6C 66 3A 20 33 3A 3A 20 33 3A 3A 20 33 3A 3A
0002904b  00 63 61 74 69 63 6b 20 2F 2F 2F 2F 2F 2F 2F
0002905c  6F 3D 0A 00 47 45 44 54 20 2F 78 78 78 78 78
0002906d  2F 72 66 6F 6D 65 74 25 20 26 26 26 26 26 26
```
Elan is French for
The Lotus Elan
Elán

The Slovak rock band (from 1969 and still active)
Network capabilities

- Pivot through firewalls
- Home-made NAT traversal
- Custom-made Proxy service
  - only available to a set of whitelisted IP addresses
- Remotely configured generic network sniffer
- DNS Hijacking
Worm-like behavior

- Tries to replicate via aggressive scanning
- Will dedicate more resources to scan near current external IP
- Will also scan on LAN interfaces
- Will not reinfect an infected device
- Can replicate across architectures
- C&C is made aware of new compromises
Closely-related IP addresses (random scan in the same /15 of the router's external IP address)

192.168.1.0/24
10.13.3.0/24
Other interfaces
(linear scan from .0 to .255)
Compromise Protocol

1. Victim info
2. Obfuscated commands
3. Unscramble commands
4. Commands sent to victim via telnet

C&C server
Linux/Moose infected
Victim
Anti-Analysis

- Statically linked binary stripped of its debugging symbols
- Hard to reproduce environment required for malware to operate
- Misleading strings (getcool.com)
Moose Herding

The Malware Operation
Via C&C Configuration

- Network sniffer was used to steal HTTP Cookies
  - Twitter: twll, twid
  - Facebook: c_user
  - Instagram: ds_user_id
  - Google: SAPISID, APISID
  - Google Play / Android: LAY_ACTIVE_ACCOUNT
  - Youtube: LOGIN_INFO
Via Proxy Usage Analysis

- Nature of traffic
- Protocol
- Targeted social networks
4% Operator (HTTP)
0% Others
18% HTTP
77.64% HTTPS
75%+ HTTPS but...
HTTP/1.1 301 Moved Permanently
Content-Type: text/html
Date: xxxxx
Location: https://instagram.com/hookahleague/
Server: nginx
Content-Length: 178
Connection: keep-alive

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
An Example
An Example (cont.)
An Example (cont.)
An Example (cont.)
Anti-Tracking

- Whitelist means we can’t use the proxy service to evaluate malware population
- Blind because of HTTPS enforced on social networks
- DNS Hijacking's Rogue DNS servers never revealed
A Strange Animal
Different focus

- not in the DDoS or bitcoin mining business
- no x86 variant found
- controlled by a single group of actors
Missing "features"

- No persistence mechanism
- No shell access for operators
Thought big, realized little?

- In social network fraud, network sniffer irrelevant
- DNS Hijacking possible but only for few devices
- No ad fraud, spam, DDoS, etc.
Latest Developments
Whitepaper Impact

- Few weeks after the publication the C&C servers went dark
  - After a reboot, all affected devices should be cleaned
  - But victims compromised via weak credentials, so they can always reinfect
Alive or dead?

Paper released

Start Date: 2015-01-01  End Date: 2015-09-09  Port: 10073
Alive or dead? (cont.)

- On the lookout for Moose v2
- Looked at over 150 new samples targeting embedded Linux platforms
- Linux/Aidra, Linux/Dofloo (AES.DDoS), Linux/DNSAmp (Mr.Black), Linux.Gafgyt and Linux/Tsunami
- Still no Moose update...
Yay! except...
Moose level-up

MOOSE
STAGE 2

200 HP

Total Awesomeness 2000

You are already dead. Best to turn back now, there is just no point to keep going because MOOSE just PANS!!!!!!!
HA HA HA HA HA!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

100,000,000,000,000

YOU GET THE PICTURE HERE!???

There once was a MOOSE that came from Scandinavia. Its destiny is to ANNIHILATE a very power on in the UNIVERSE, HACKERWORLD ...

Weakness: resistance

Retired card:
Update

New sample this Saturday

- New proxy service port (20012)
- New C&C selection algorithm
- Lots of differences
- Still under scrutiny
Conclusion

Embedded malware

- Not yet complex
- Tools and processes need to catch up
- A low hanging fruit
- Prevention simple
Questions?

Thank you!

- @obilodeau
- and special thanks to Thomas Dupuy (@nyx__o)