Linux/Moose: Still breathing

welivesecurity.com/2016/11/02/linuxmoose-still-breathing/

November 2, 2016

For the past year, ESET and the security firm GoSecure combined their skills in order to research Linux/Moose further. Here's some of what was uncovered.

Editor
2 Nov 2016 - 01:20PM

For the past year, ESET and the security firm GoSecure combined their skills in order to research Linux/Moose further. Here’s some of what was uncovered.

What is a Moose – Introduction

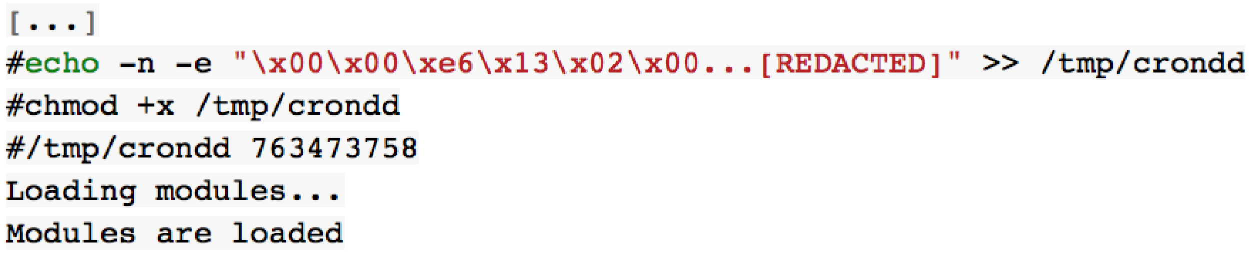
Linux/Moose is a malware family that primarily targets Linux-based consumer routers but that can also infect other Linux-based embedded systems in its path. The compromised devices are used to steal unencrypted network traffic and offer proxying services to the botnet operator. In practice, these capabilities are used to steal HTTP Cookies on popular social network sites and perform fraudulent actions such as non-legitimate “follows”, “views” and “likes”.

In May 2015 ESET released a whitepaper on the malware family we named Linux/Moose. After publication, Linux/Moose’s command and control servers went down and we lost track of the animal. A few months later, in September 2015, we got a new sample of Linux/Moose —with, as expected, some evolution after our publication.

For the past year, ESET and the security firm GoSecure combined their skills in order to research Linux/Moose further. GoSecure investigated the social media fraud aspect and shed some light on an unknown market they called “The Ego Market”. This market is highlighted in a new whitepaper published by GoSecure. This blog will cover the technical changes between the Moose variants we described in our whitepaper and the new variants that appeared in September 2015.

Moose in the bushes – Hiding the address of C&C

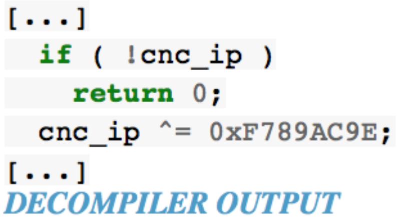
The first thing we noticed when we got the new sample was that there was no more command and control (C&C) IP address inside the binary. It seems that the operators read our report carefully and decided to make things a little bit harder for us. In this new version the C&C IP address is given as an encrypted command line argument, as shown in the following output:



```
[...]
#echo -n -e "\x00\x00\xe6\x13\x02\x00...[REDACTED]" >> /tmp/crondd
#chmod +x /tmp/crondd
#/tmp/crondd 763473758
Loading modules...
Modules are loaded
```

This new feature implies that we can no longer run the sample by ourselves; our test machines need to be compromised by an embedded device spreading the threat in-the-wild in order to retrieve the C&C IP address. The attentive reader will notice that the IP address shown is in 32-bit integer format.

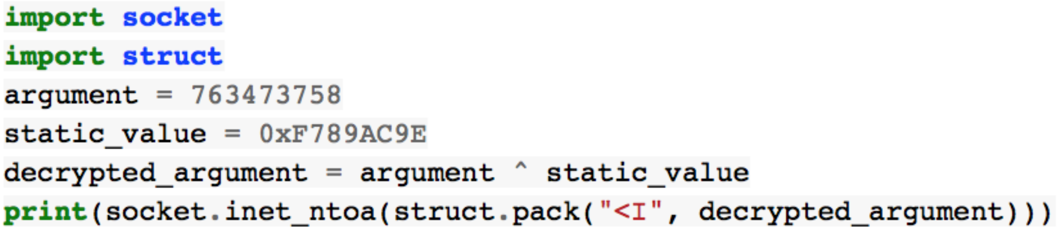
The purpose of encrypting the IP address here is, if the binary is found alone, useless without the value passed as argument. Also, the value alone makes no sense without the binary having the correct value to decrypt the argument. The value is XORed with a static value as shown in the following code:



```
[...]
  if ( !cnc_ip )
    return 0;
  cnc_ip ^= 0xF789AC9E;
[...]
```

Decompiler output

To the best of our knowledge, this value has stayed the same over the last few months. Here is a Python snippet to decrypt the C&C 32-bit Integer value:

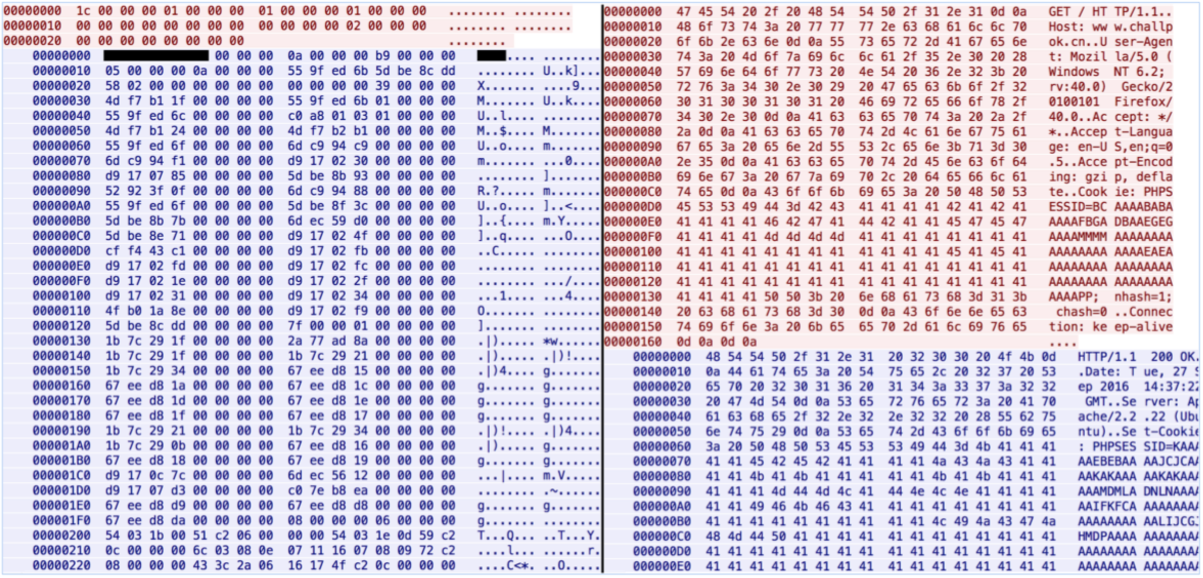


```
import socket
import struct
argument = 763473758
static_value = 0xF789AC9E
decrypted_argument = argument ^ static_value
print(socket.inet_ntoa(struct.pack("<I", decrypted_argument)))
```

Decrypt C&C IP address

Moose molted – Network communication

The network protocol changed but it kept the basis of its protocol and added new layers. Here is a quick look of a packet capture from both samples. By the look of things the main change here is from binary protocol to ASCII printable protocol. In Figure 1, on the left side there is the old network protocol and on the right side there is the new one.

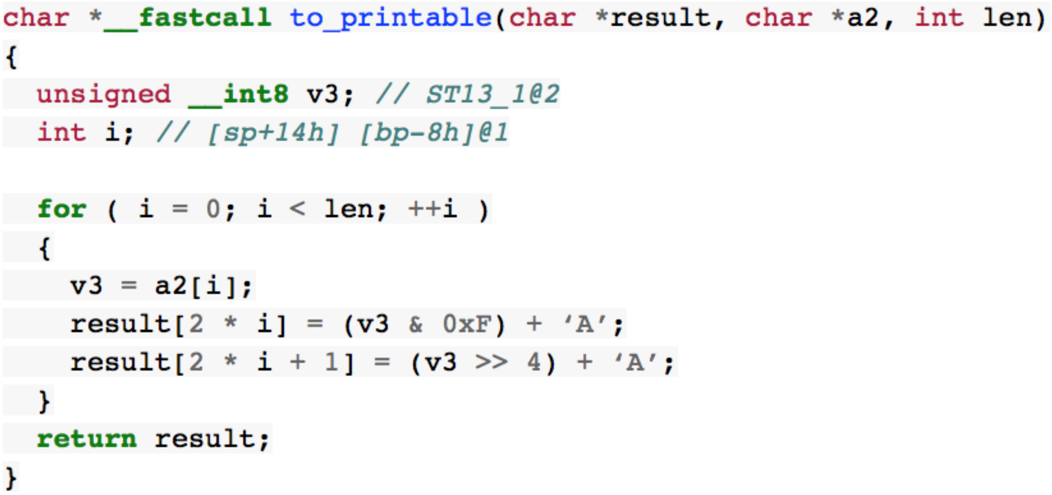


```
00000000  1c 00 00 00 01 00 00 00  01 00 00 00 01 00 00 00   ........ ........
00000010  00 00 00 00 00 00 00 00  00 00 00 00 02 00 00 00   ........ ........
00000020  00 00 00 00 00 00 00 00                            ........
    00000000  [redacted] 00 00 00  0a 00 00 00 b9 00 00 00   [redacted].... ........
    00000010  05 00 00 00 0a 00 00 00  55 9f ed 6b 5d be 8c dd   ........ U..k]...
    00000020  58 02 00 00 00 00 00 00  00 00 00 00 39 00 00 00   X....... ....9...
    00000030  4d f7 b1 1f 00 00 00 00  55 9f ed 6b 01 00 00 00   M....... U..k....
    00000040  55 9f ed 6c 00 00 00 00  c0 a8 01 03 01 00 00 00   U..l.... ........
    00000050  4d f7 b1 24 00 00 00 00  4d f7 b2 b1 00 00 00 00   M..$.... M.......
    00000060  55 9f ed 6f 00 00 00 00  6d c9 94 c9 00 00 00 00   U..o.... m.......
    00000070  6d c9 94 f1 00 00 00 00  d9 17 02 30 00 00 00 00   m....... ...0....
    00000080  d9 17 07 85 00 00 00 00  5d be 8b 93 00 00 00 00   ........ ].......
    00000090  52 92 3f 0f 00 00 00 00  6d c9 94 88 00 00 00 00   R.?..... m.......
    000000A0  55 9f ed 6f 00 00 00 00  5d be 8f 3c 00 00 00 00   U..o.... ]..<....
    000000B0  5d be 8b 7b 00 00 00 00  6d ec 59 d0 00 00 00 00   ]..{.... m.Y.....
    000000C0  5d be 8e 71 00 00 00 00  d9 17 02 4f 00 00 00 00   ]..q.... ...O....
    000000D0  cf f4 43 c1 00 00 00 00  d9 17 02 fb 00 00 00 00   ..C..... ........
    000000E0  d9 17 02 fd 00 00 00 00  d9 17 02 fc 00 00 00 00   ........ ........
    000000F0  d9 17 02 1e 00 00 00 00  d9 17 02 2f 00 00 00 00   ........ .../....
    00000100  d9 17 02 31 00 00 00 00  d9 17 02 34 00 00 00 00   ...1.... ...4....
    00000110  4f b0 1a 8e 00 00 00 00  d9 17 02 f9 00 00 00 00   O....... ........
    00000120  5d be 8c dd 00 00 00 00  7f 00 00 01 00 00 00 00   ]....... ........
    00000130  1b 7c 29 1f 00 00 00 00  2a 77 ad 8a 00 00 00 00   .|)..... *w......
    00000140  1b 7c 29 1f 00 00 00 00  1b 7c 29 21 00 00 00 00   .|)..... .|)!....
    00000150  1b 7c 29 34 00 00 00 00  67 ee d8 15 00 00 00 00   .|)4.... g.......
    00000160  67 ee d8 1a 00 00 00 00  67 ee d8 1c 00 00 00 00   g....... g.......
    00000170  67 ee d8 1d 00 00 00 00  67 ee d8 1e 00 00 00 00   g....... g.......
    00000180  67 ee d8 1f 00 00 00 00  67 ee d8 17 00 00 00 00   g....... g.......
    00000190  1b 7c 29 21 00 00 00 00  1b 7c 29 34 00 00 00 00   .|)!.... .|)4....
    000001A0  1b 7c 29 0b 00 00 00 00  67 ee d8 16 00 00 00 00   .|)..... g.......
    000001B0  67 ee d8 18 00 00 00 00  67 ee d8 19 00 00 00 00   g....... g.......
    000001C0  d9 17 0c 7c 00 00 00 00  6d ec 56 12 00 00 00 00   ...|.... m.V.....
    000001D0  d9 17 07 d3 00 00 00 00  c0 7e b8 ea 00 00 00 00   ........ .~......
    000001E0  67 ee d8 d9 00 00 00 00  67 ee d8 d8 00 00 00 00   g....... g.......
    000001F0  67 ee d8 da 00 00 00 00  08 00 00 00 06 00 00 00   g....... ........
    00000200  54 03 1b 00 51 c2 06 00  00 00 54 03 1e 0d 59 c2   T...Q... ..T...Y.
    00000210  0c 00 00 00 6c 03 08 0e  07 11 16 07 08 09 72 c2   ....l... ......r.
    00000220  08 00 00 00 43 3c 2a 06  16 17 4f c2 0c 00 00 00   ....C<*. ..O.....
```

```
00000000  47 45 54 20 2f 20 48 54  54 50 2f 31 2e 31 0d 0a   GET / HT TP/1.1..
00000010  48 6f 73 74 3a 20 77 77  77 2e 63 68 61 6c 6c 70   Host: ww w.challp
00000020  6f 6b 2e 63 6e 0d 0a 55  73 65 72 2d 41 67 65 6e   ok.cn..U ser-Agen
00000030  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00000040  57 69 6e 64 6f 77 73 20  4e 54 20 36 2e 32 3b 20   Windows  NT 6.2;
00000050  72 76 3a 34 30 2e 30 29  20 47 65 63 6b 6f 2f 32   rv:40.0)  Gecko/2
00000060  30 31 30 30 31 30 31 20  46 69 72 65 66 6f 78 2f   0100101  Firefox/
00000070  34 30 2e 30 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   40.0..Ac cept: */
00000080  2a 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   *..Accep t-Langua
00000090  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b 71 3d 30   ge: en-U S,en;q=0
000000A0  2e 35 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   .5..Acce pt-Encod
000000B0  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
000000C0  74 65 0d 0a 43 6f 6f 6b  69 65 3a 20 50 48 50 53   te..Cook ie: PHPS
000000D0  45 53 53 49 44 3d 42 43  41 41 41 41 42 41 42 41   ESSID=BC AAAABABA
000000E0  41 41 41 41 46 42 47 41  44 42 41 41 45 47 45 47   AAAAFBGA DBAAEGEG
000000F0  41 41 41 41 4d 4d 4d 4d  41 41 41 41 41 41 41 41   AAAAMMMM AAAAAAAA
00000100  41 41 41 41 41 41 41 41  41 41 41 41 45 41 45 41   AAAAAAAA AAAAEAEA
00000110  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
00000120  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
00000130  41 41 41 41 50 50 3b 20  6e 68 61 73 68 3d 31 3b   AAAAPP;  nhash=1;
00000140  20 63 68 61 73 68 3d 30  0d 0a 43 6f 6e 6e 65 63    chash=0 ..Connec
00000150  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
00000160  0d 0a 0d 0a                                        ....
    00000000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
    00000010  0a 44 61 74 65 3a 20 54  75 65 2c 20 32 37 20 53   .Date: T ue, 27 S
    00000020  65 70 20 32 30 31 36 20  31 34 3a 33 37 3a 32 32   ep 2016  14:37:22
    00000030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT..Se rver: Ap
    00000040  61 63 68 65 2f 32 2e 32  2e 32 32 20 28 55 62 75   ache/2.2 .22 (Ubu
    00000050  6e 74 75 29 0d 0a 53 65  74 2d 43 6f 6f 6b 69 65   ntu)..Se t-Cookie
    00000060  3a 20 50 48 50 53 45 53  53 49 44 3d 4b 41 41 41   : PHPSES SID=KAAA
    00000070  41 41 45 42 45 42 41 41  41 41 4a 43 4a 43 41 41   AAEBEBAA AAJCJCAA
    00000080  41 41 4b 41 4b 41 41 41  41 41 4b 41 4b 41 41 41   AAKAKAAA AAKAKAAA
    00000090  41 41 41 4d 44 4d 4c 41  44 4e 4c 4e 41 41 41 41   AAAMDMLA DNLNAAAA
    000000A0  41 41 49 46 4b 46 43 41  41 41 41 41 41 41 41 41   AAIFKFCA AAAAAAAA
    000000B0  41 41 41 41 41 41 41 41  41 41 4c 49 4a 43 47 4a   AAAAAAAA AALIJCGJ
    000000C0  48 4d 44 50 41 41 41 41  41 41 41 41 41 41 41 41   HMDPAAAA AAAAAAAA
    000000D0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
    000000E0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
```

Figure 1: Network Protocol Differences

In the old sample the configuration was sent by the C&C server to the malware, and contains various fields like bits field to determine what feature to enable, IP address fields, whitelist list field and password list field. These fields are still present in the new version, but separated in three keys (see Table 1). The operator uses the Cookie: and Set-Cookie: HTTP headers to send these config fields. This config is encrypted by a simple XOR loop like in the first version but it’s also encoded in order to be printable in the HTTP headers thanks to the following function:



```
char *__fastcall to_printable(char *result, char *a2, int len)
{
  unsigned __int8 v3; // ST13_1@2
  int i; // [sp+14h] [bp-8h]@1

  for ( i = 0; i < len; ++i )
  {
    v3 = a2[i];
    result[2 * i] = (v3 & 0xF) + ‘A’;
    result[2 * i + 1] = (v3 >> 4) + ‘A’;
  }
  return result;
}
```

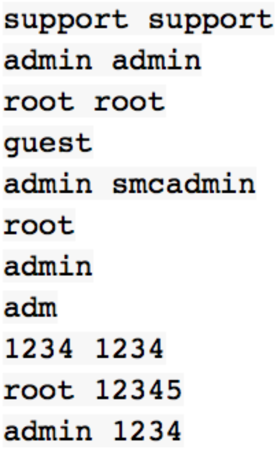
Decompiler output

Table 1 (key-value table) summarizes the main configuration of Moose v.2:

key	value
PHPSESSID	main config (local/external scan, sniffer, kill process)

key	value
LP	password list
WL	whitelist list

The PHPSESSID key contains the encrypted value of bit fields that allow to enable or disable some features on Moose (local/external scan, sniffer, kill process). The LP key contains the password list. Linux/Moose still tries to spread itself by bruteforcing Telnet credentials. There was a big change in this list, from around 300 logins and passwords in 2015 versus around 10 in 2016. See below:



```
support support
admin admin
root root
guest
admin smcadmin
root
admin
adm
1234 1234
root 12345
admin 1234
```

The WL key contains the whitelist list. Again the list was shorted from 50 to 10 IP addresses. These IP addresses are in the IoC section. Linux/Moose still has the ability to run a proxy service by listening on TCP port 20012. The previous variant used to listen on port 10073. The proxy feature allows IP addresses from the whitelist to interact with the malware.

Conclusion

Linux/Moose's authors have clearly done a lot of work to stay under the radar with the new version by hiding its C&C server location more effectively and changing the network protocol. By doing this, Moose avoids the Indicators of Compromise (IoCs) released with ESET's 2015 whitepaper. Shortening the whitelist and password list shows a more delicate approach with Moose. Still, some misleading traces are inside the binary like the fake domain www.challpok.cn found in cleartext in the list of strings or even filenames that can correspond to bitcoinminer or DDoS malware. Linux/Moose stays exclusively a memory-resident threat; rebooting the embedded device will end its execution.

Indicators of Compromise

Hashes

version 0x1F (31)

c6edfa2bf916d374e60f1b5444be6dbbee099692
c9ca4820bb7be18f36b7bad8e3044b2d768a5db8
5b444f1ac312b4c24b6bde304f00a5772a6a19a4
f7574b3eb708bd018932511a8a3600d26f5e3be9

version 0x20 (32)

34802456d10efdf211a7d486f7108319e052cd17
0685cb1d72107de63fa1da52930322df04a72dbc
2876cad26d6dabdc0a9679bb8575f88d40ebd960
f94b6cc5aea170cee55a238eaa9339279fba962f
274ef5884cb256fd4edd7000392b0e326ddd2398
c3f0044ffa9d0bc950e9fd0f442c955b71a706b6
f3daea1d06b1313ec061d93c9af12d0fe746839a

version 0x21 (33)

7767c8317fb0bbf91924bddffe6a5e45069b0182
1caac933ae6ca326372f7e5dd9fff82652e22e34
5dea6c0c4300e432896038661db2f046c523ce35
e8dc272954d5889044e92793f0f637fe4d53bb91
0843239b3d0f62ae6c5784ba4589ef85329350fa
1d1d46c312045e17f8f4386adc740c1e7423a24a
d8b45a1114c5e0dbfa13be176723b2288ab12907

version 0x22 (34)

c35d6812913ef31c20404d9bbe96db813a764886

IP addresses

Primary C&C servers

192.3.8.218
192.3.8.219

Whitelist

155.133.18.64
178.19.111.181
151.80.8.2

151.80.8.19
151.80.8.30
62.210.6.34

Moose’s IoCs are also available and updated on ESET’s malware-ioc Github repository.

2 Nov 2016 - 01:20PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion