DDoS Threat Landscape

Ron Winward

Security Evangelist

Radware

May 12, 2016

⊕ Overview

Attack Methods

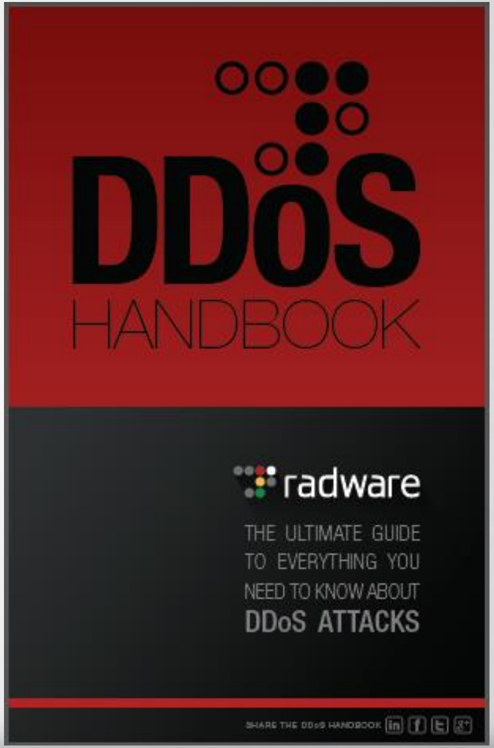
Anonymous Toolkit 2016

Online Services (Booters / Stressers)

Strategies for Survival

DDoS Handbook

- A history and overview of DDoS
- Review of attack types and tools
- DDoS Mitigation Considerations
- DDoS Dictionary



DDoS HANDBOOK

radware

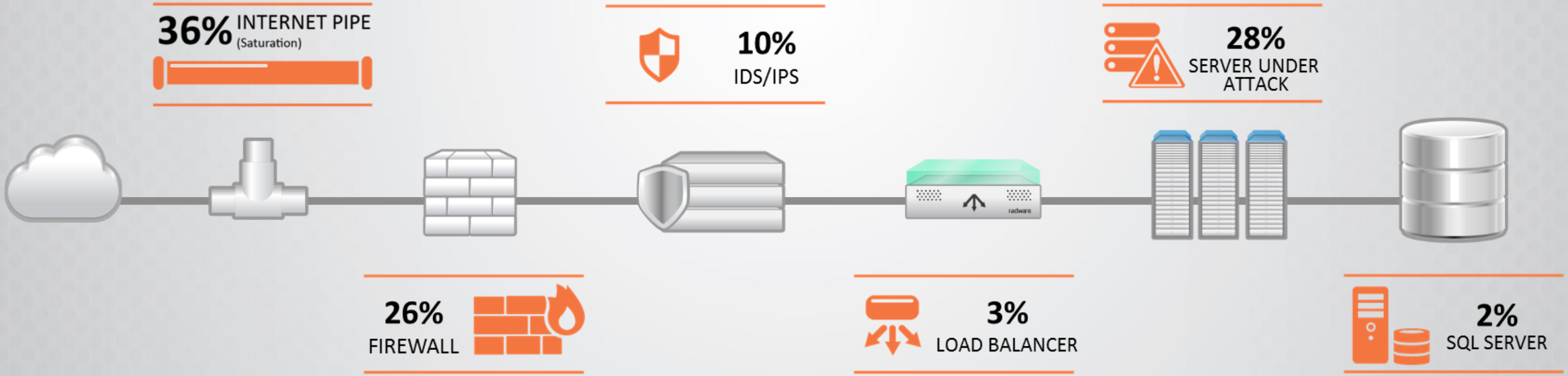
THE ULTIMATE GUIDE
TO EVERYTHING YOU
NEED TO KNOW ABOUT
DDoS ATTACKS

SHARE THE DDoS HANDBOOK

DDoS Failure Points within the Network

Security Products Now Cause of 36% of Downtime

- Internet Pipe Saturation remains single greatest failure point
- Stateful firewalls jump from 15% to 26%
- Last third take down targeted web/SQL servers



36% INTERNET PIPE (Saturation)

10% IDS/IPS

28% SERVER UNDER ATTACK

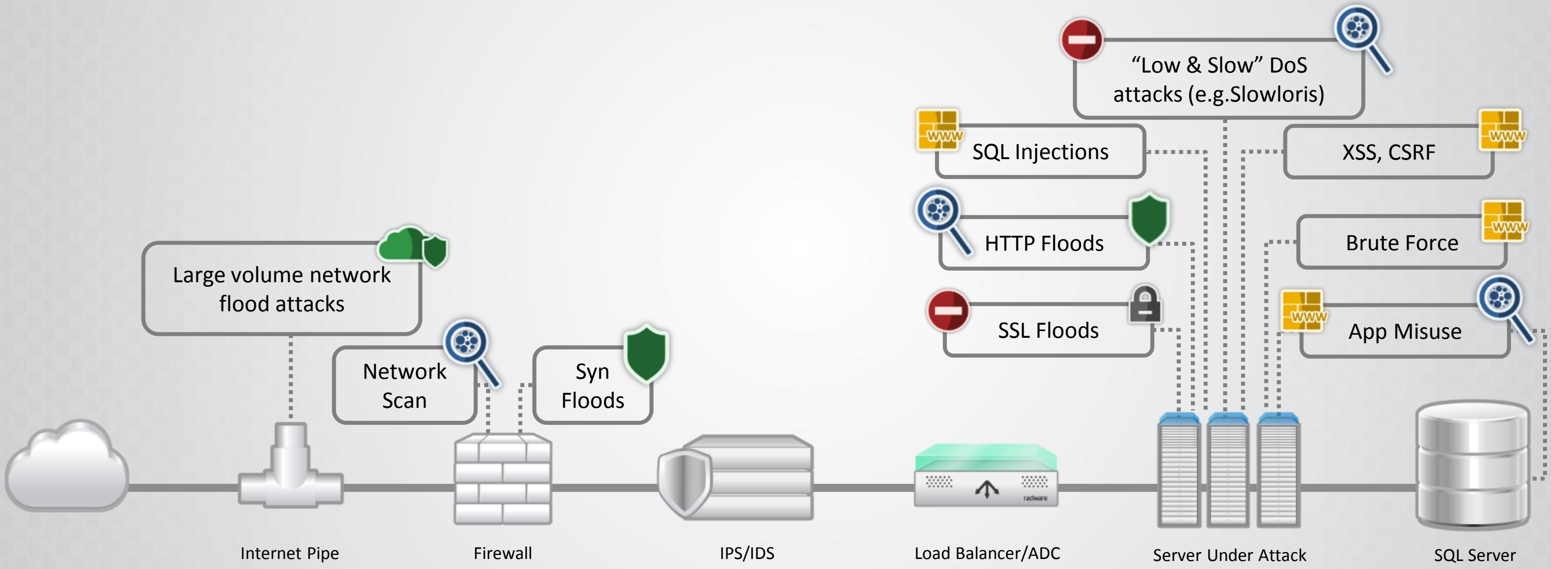
26% FIREWALL

3% LOAD BALANCER

2% SQL SERVER

Complexity of Attacks Continues to Grow

Multi-vector attacks target all layers of the infrastructure



On-Demand Cloud DDoS | DoS protection | Behavioral analysis | IPS | SSL protection | WAF

Overview

Attack Methods

Anonymous Toolkit 2016

Online Services (Booters / Stressers)

Strategies for Survival

Types of Attacks

Attacks Targeting Network Resources

- UDP
- ICMP
- IGMP
- Reflection
  - DNS, SSDP, NTP, etc

Attacks Targeting Server Resources

- TCP Weaknesses
- SYN Floods
- TCP RST
- TCP PSH+ACK Flood
- Low and Slow
  - Sockstress, Slowloris

Our current research shows an even split between network and application-layer attacks

Types of Attacks (cont.)

Encrypted Attacks

- HTTPS Floods
- THC-SSL-DOS

Attacks Targeting App Resources

- HTTP Flood
- DNS Flood
- Slow HTTP GET Request
- Slow HTTP POST Request
- REGEX
- Hash Collision

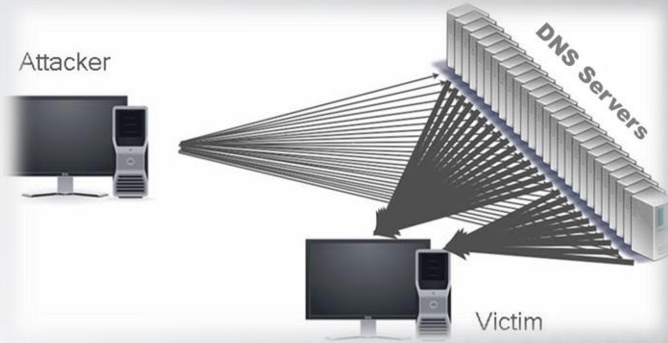
UDP Floods

- User Datagram Protocol (UDP)
- Connectionless protocol
- Doesn’t exploit a specific vulnerability
- Typically spoofed source IPs, often packets are sent to random dest ports
- Server has to respond with ICMP unreachables
- Compute resources are consumed
- Network capacity is consumed

ICMP Floods

- Internet Control Message Protocol (ICMP)
- Connectionless protocol
- Doesn’t exploit a specific vulnerability
- Can be any type of ICMP message
- Volumetric in nature
- Target has to try and process all of the requests
- This is why we have ICMP policers on routers ☺
  - The premise holds true for all devices that have to respond

Reflection Attacks



- DNS, SSDP, NTP, etc.
- Most common attacks today
- Leverage the disparity between a request and a reply
- Amplification can be huge
- Source IP of the request is spoofed as the target’s IP
- Target is overwhelmed

TCP Weaknesses

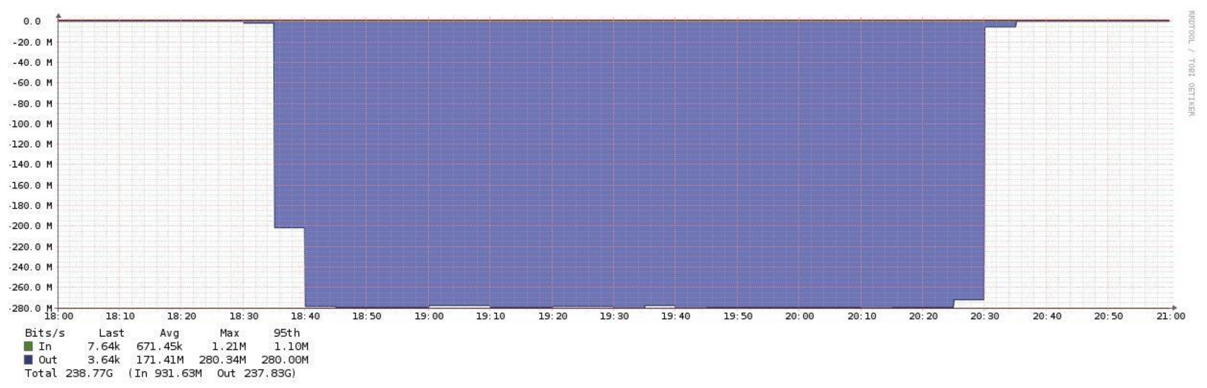
- Protocol exploits
- Misuse of the six control bits, SYN, ACK, RST, PSH, FIN and URG
- TCP requires a 3-way negotiation in order for a session to be established
  - SYN, SYN-ACK, ACK
  - Each request creates a half-open connection
- Attacks will often send packets in the wrong order to consume resources on the target while it tries to interpret what’s happening

SYN Floods

- One of the most common vectors
- Attacker floods the target with SYN packets from spoofed source IPs
- Target opens a thread and assigns buffers to prepare for each connection
- Target sends a SYN-ACK back to the spoofed requestor
- No response, so target sends more SYN-ACKs until it times out
- Server is unable to timeout old sessions before new ones can be handled

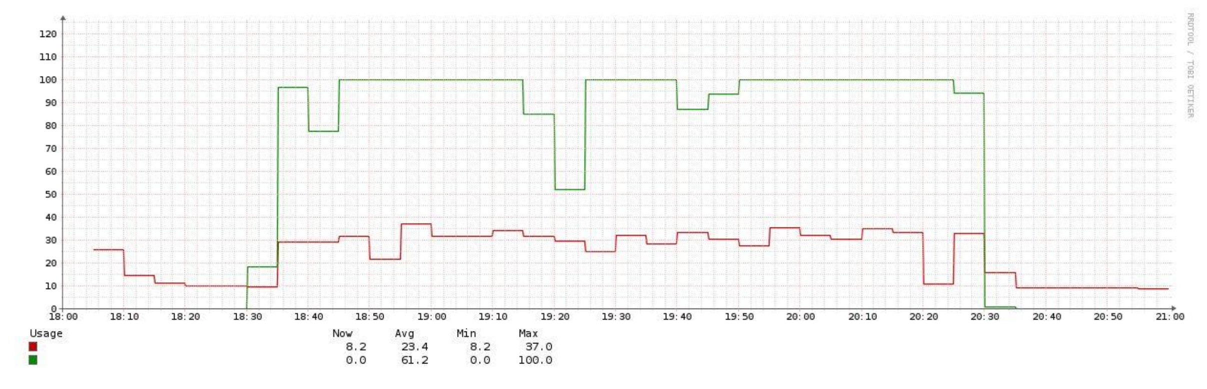
SYN Flood Impact on Firewall

Bandwidth



```
Bits/s     Last     Avg      Max      95th
🟩 In      7.64k  671.45k    1.21M    1.10M
🟦 Out     3.64k  171.41M  280.34M  280.00M
Total 238.77G  (In 931.63M  Out 237.83G)
```

CPU Impact



```
Usage                          Now     Avg     Min     Max
🟥                              8.2    23.4     8.2    37.0
🟩                              0.0    61.2     0.0   100.0
```

HTTP GET Flood

- Most common application layer attack
- Multiple machines continually download the content from a target
- Target server exhausts resources trying to deliver the content and handle the connections
- Slow HTTP GET attack also exists

Low and Slow Attacks

- Common Application Layer attack
- Essentially holding open connections
- Can be launched from a single machine
- Slowloris
  - Opens connections and sends a partial request
  - Eventually sends more of the request but not complete request
  - Connections stay open and max concurrent connections is exhausted

THC-SSL-DOS

- Developed by hacking group The Hackers Choice (THC)
- Low and Slow + Encrypted
- Initiates a regular SSL handshake
- Immediately requests the renegotiation of the encryption key
- Continues process until exhaustion
- How will you see this if it’s an encrypted attack?
  - Low and slow, so difficult to distinguish from real traffic!
- Single PC can take down a server

Overview

Attack Methods

Anonymous Toolkit 2016

Online Services (Booters / Stressers)

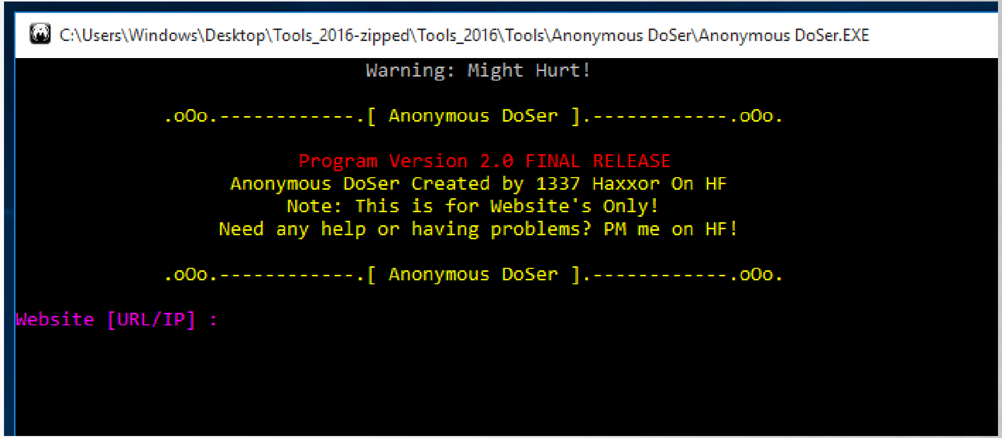
Strategies for Survival

Anonymous Tools for 2016

- Anonymous DoSer
- Anonymous Ping Attack
- BlackOut
- BlackBurn
- ByteDoS
- FireFlood
- Generic DDoS
- GoodBye
- HOIC
- LOIC
- XOIC
- Pringle DDoS
- rDoS
- Unknown DoSer

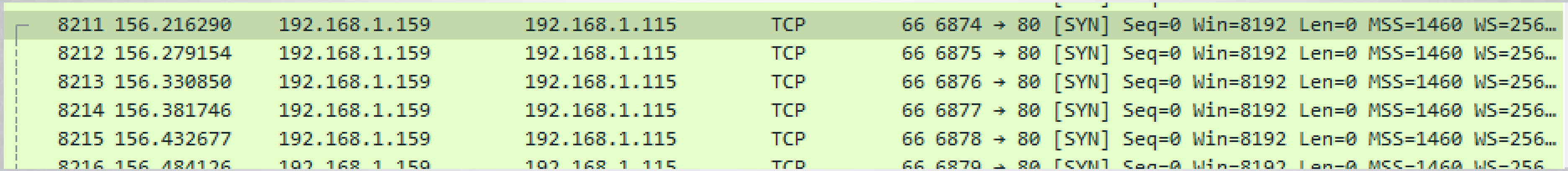
Anonymous DoSer

- TCP SYN Flood
- Launched from a client



C:\Users\Windows\Desktop\Tools_2016-zipped\Tools_2016\Tools\Anonymous DoSer\Anonymous DoSer.EXE

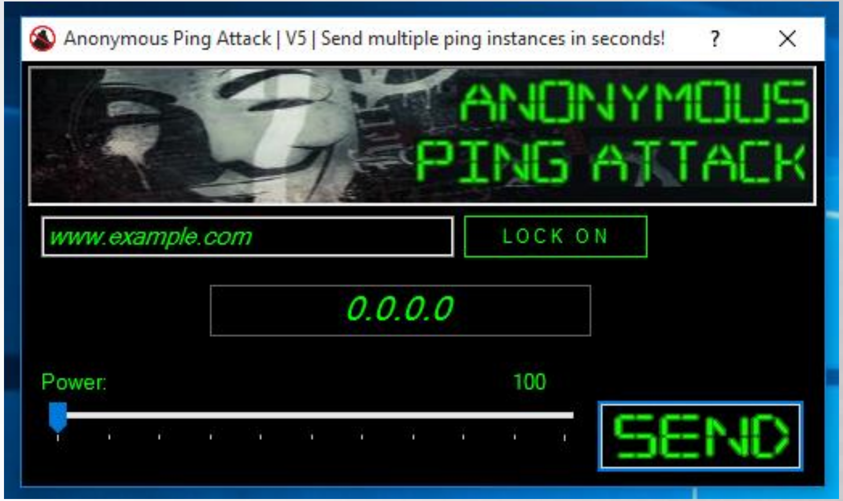
```
                          Warning: Might Hurt!

             .oOo.------------.[ Anonymous DoSer ].------------.oOo.

                       Program Version 2.0 FINAL RELEASE
                 Anonymous DoSer Created by 1337 Haxxor On HF
                      Note: This is for Website's Only!
                 Need any help or having problems? PM me on HF!

             .oOo.------------.[ Anonymous DoSer ].------------.oOo.

Website [URL/IP] :
```



```
8211 156.216290    192.168.1.159    192.168.1.115    TCP    66 6874 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
8212 156.279154    192.168.1.159    192.168.1.115    TCP    66 6875 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
8213 156.330850    192.168.1.159    192.168.1.115    TCP    66 6876 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
8214 156.381746    192.168.1.159    192.168.1.115    TCP    66 6877 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
8215 156.432677    192.168.1.159    192.168.1.115    TCP    66 6878 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
8216 156.484126    192.168.1.159    192.168.1.115    TCP    66 6879 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
```

Anonymous Ping Attack

- ICMP Ping tool

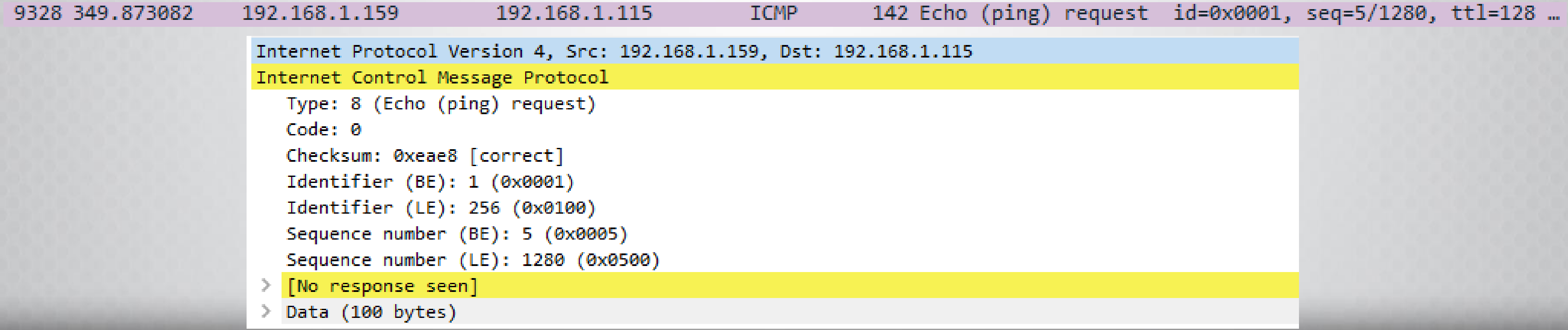


Anonymous Ping Attack | V5 | Send multiple ping instances in seconds!

www.example.com

0.0.0.0

Power: 100



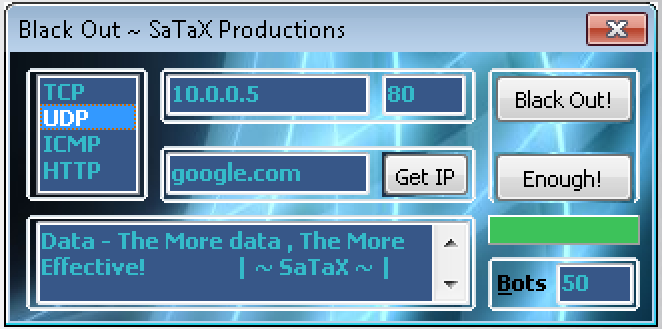
```
9328 349.873082    192.168.1.159        192.168.1.115        ICMP       142 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 …
```

```
Internet Protocol Version 4, Src: 192.168.1.159, Dst: 192.168.1.115
Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0xeae8 [correct]
   Identifier (BE): 1 (0x0001)
   Identifier (LE): 256 (0x0100)
   Sequence number (BE): 5 (0x0005)
   Sequence number (LE): 1280 (0x0500)
 > [No response seen]
 > Data (100 bytes)
```

Black Out

- TCP
- UDP
  - (QUIC)
- ICMP
- HTTP
  - “GET /”

- Customizable text in payload



Black Out ~ SaTaX Productions

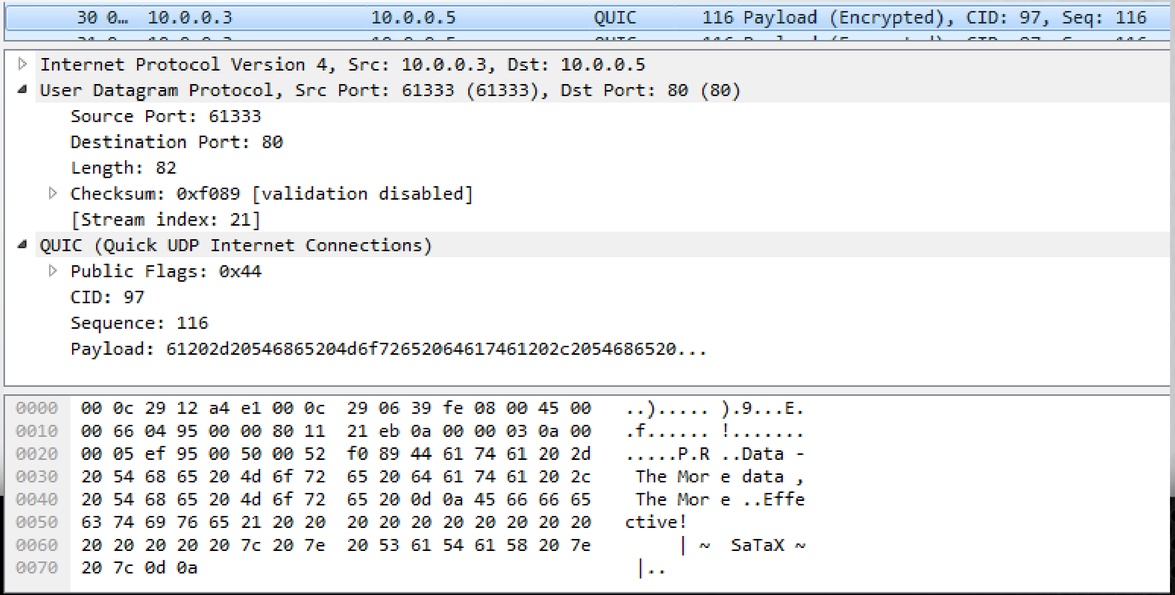
TCP
UDP
ICMP
HTTP

10.0.0.5 80

google.com

Data - The More data , The More Effective! | ~ SaTaX ~ |

Bots 50



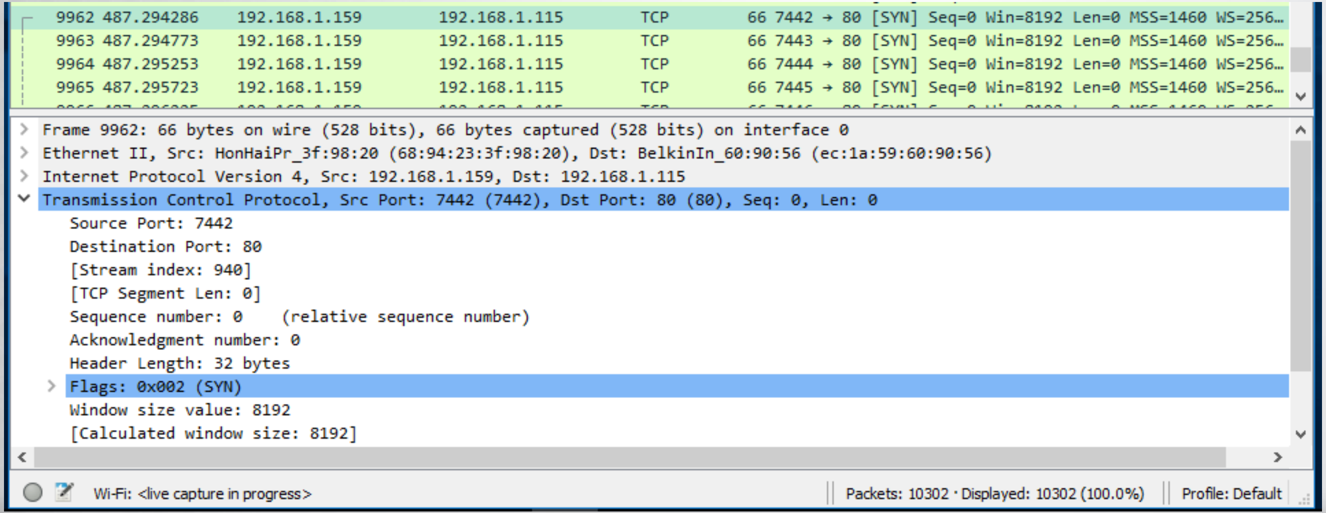
```
30 0…  10.0.0.3          10.0.0.5          QUIC      116 Payload (Encrypted), CID: 97, Seq: 116
```

```
▷ Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.5
◢ User Datagram Protocol, Src Port: 61333 (61333), Dst Port: 80 (80)
    Source Port: 61333
    Destination Port: 80
    Length: 82
  ▷ Checksum: 0xf089 [validation disabled]
    [Stream index: 21]
◢ QUIC (Quick UDP Internet Connections)
  ▷ Public Flags: 0x44
    CID: 97
    Sequence: 116
    Payload: 61202d20546865204d6f726520646174612c2054686520...
```

```
0000  00 0c 29 12 a4 e1 00 0c  29 06 39 fe 08 00 45 00   ..)..... ).9...E.
0010  00 66 04 95 00 00 80 11  21 eb 0a 00 00 03 0a 00   .f...... !.......
0020  00 05 ef 95 00 50 00 52  f0 89 44 61 74 61 20 2d   .....P.R ..Data -
0030  20 54 68 65 20 4d 6f 72  65 20 64 61 74 61 20 2c    The Mor e data ,
0040  20 54 68 65 20 4d 6f 72  65 20 0d 0a 45 66 66 65    The Mor e ..Effe
0050  63 74 69 76 65 21 20 20  20 20 20 20 20 20 20 20   ctive!
0060  20 20 20 20 20 7c 20 7e  20 53 61 54 61 58 20 7e        | ~  SaTaX ~
0070  20 7c 0d 0a                                          |..
```

BBHH (Black Burn)

- SYN Flood
- Few options



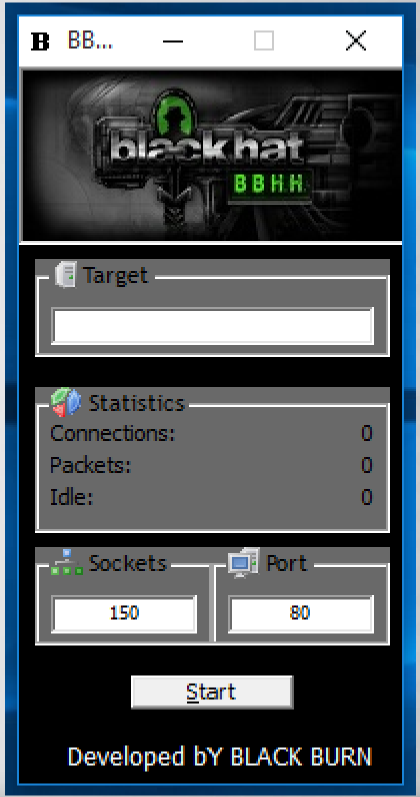
```
9962 487.294286    192.168.1.159       192.168.1.115        TCP         66 7442 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
9963 487.294773    192.168.1.159       192.168.1.115        TCP         66 7443 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
9964 487.295253    192.168.1.159       192.168.1.115        TCP         66 7444 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
9965 487.295723    192.168.1.159       192.168.1.115        TCP         66 7445 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
```

```
> Frame 9962: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: HonHaiPr_3f:98:20 (68:94:23:3f:98:20), Dst: BelkinIn_60:90:56 (ec:1a:59:60:90:56)
> Internet Protocol Version 4, Src: 192.168.1.159, Dst: 192.168.1.115
v Transmission Control Protocol, Src Port: 7442 (7442), Dst Port: 80 (80), Seq: 0, Len: 0
     Source Port: 7442
     Destination Port: 80
     [Stream index: 940]
     [TCP Segment Len: 0]
     Sequence number: 0    (relative sequence number)
     Acknowledgment number: 0
     Header Length: 32 bytes
   > Flags: 0x002 (SYN)
     Window size value: 8192
     [Calculated window size: 8192]
```

Wi-Fi: <live capture in progress>

Packets: 10302 · Displayed: 10302 (100.0%)

Profile: Default



Target

Statistics

Connections: 0

Packets: 0

Idle: 0

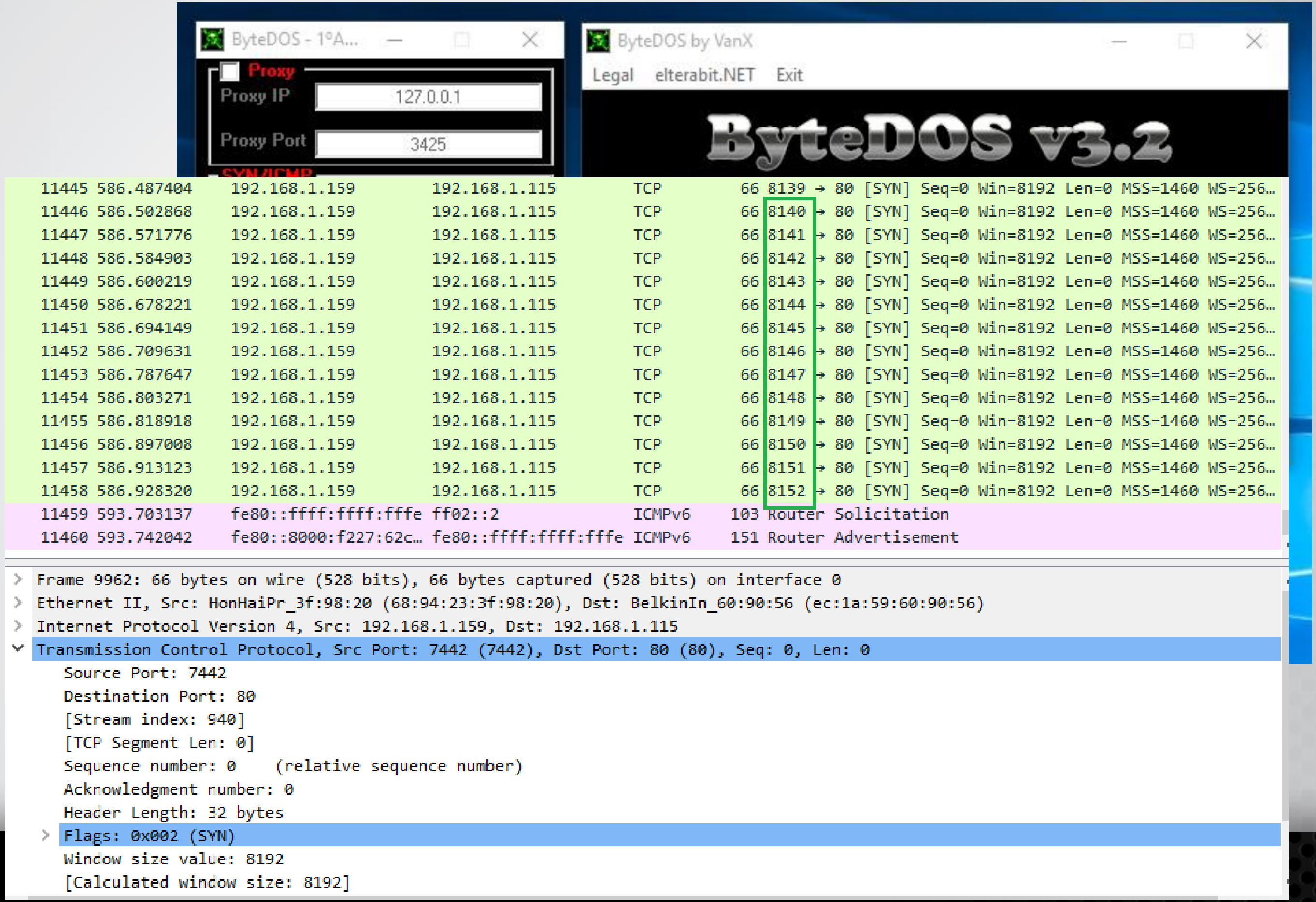
Sockets: 150

Port: 80

Developed bY BLACK BURN

ByteDoS

- SYN Flood
- ICMP Flood
- DNS Resolution



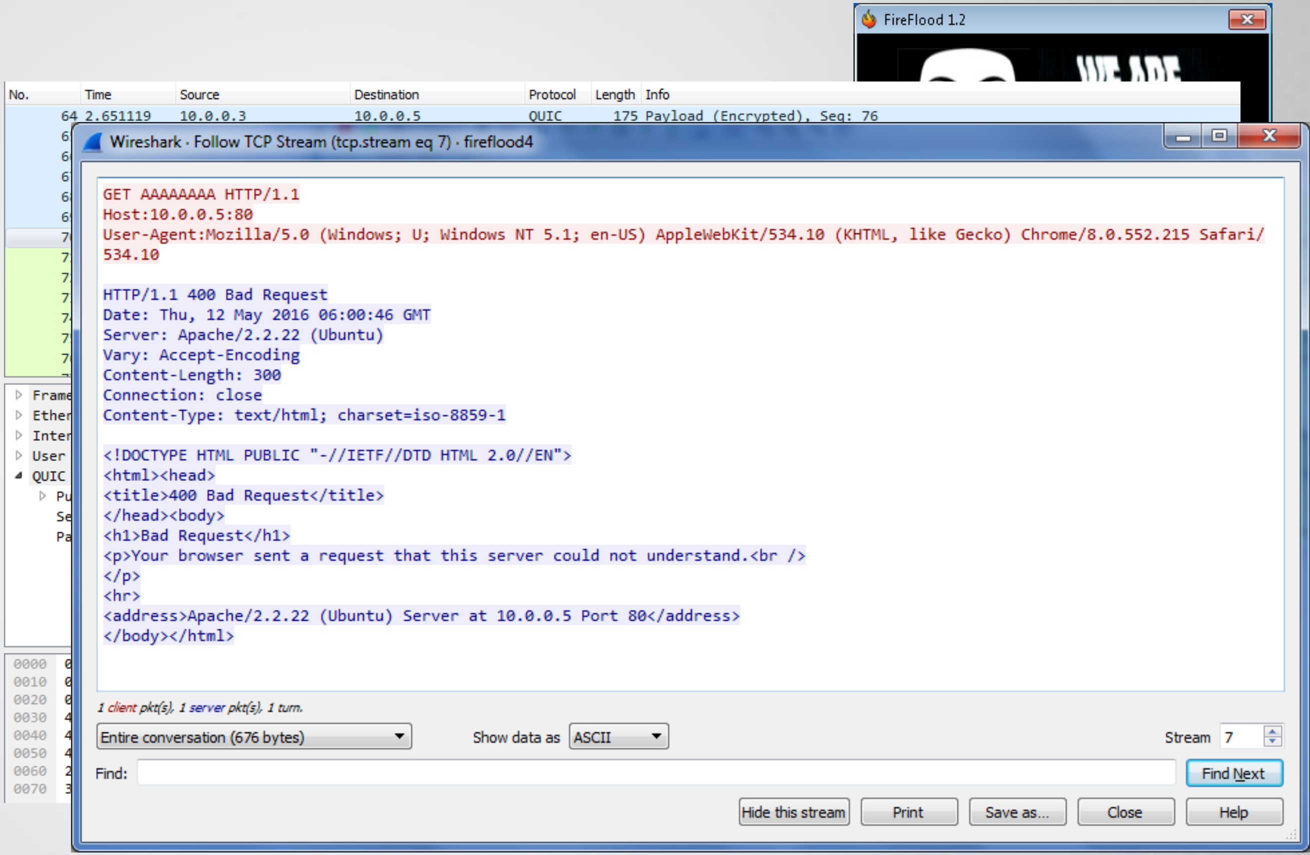
□ Proxy
Proxy IP 127.0.0.1
Proxy Port 3425

```
11445 586.487404  192.168.1.159  192.168.1.115  TCP  66 8139 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11446 586.502868  192.168.1.159  192.168.1.115  TCP  66 8140 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11447 586.571776  192.168.1.159  192.168.1.115  TCP  66 8141 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11448 586.584903  192.168.1.159  192.168.1.115  TCP  66 8142 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11449 586.600219  192.168.1.159  192.168.1.115  TCP  66 8143 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11450 586.678221  192.168.1.159  192.168.1.115  TCP  66 8144 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11451 586.694149  192.168.1.159  192.168.1.115  TCP  66 8145 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11452 586.709631  192.168.1.159  192.168.1.115  TCP  66 8146 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11453 586.787647  192.168.1.159  192.168.1.115  TCP  66 8147 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11454 586.803271  192.168.1.159  192.168.1.115  TCP  66 8148 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11455 586.818918  192.168.1.159  192.168.1.115  TCP  66 8149 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11456 586.897008  192.168.1.159  192.168.1.115  TCP  66 8150 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11457 586.913123  192.168.1.159  192.168.1.115  TCP  66 8151 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11458 586.928320  192.168.1.159  192.168.1.115  TCP  66 8152 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256…
11459 593.703137  fe80::ffff:ffff:fffe ff02::2  ICMPv6  103 Router Solicitation
11460 593.742042  fe80::8000:f227:62c… fe80::ffff:ffff:fffe ICMPv6  151 Router Advertisement
```

```
> Frame 9962: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: HonHaiPr_3f:98:20 (68:94:23:3f:98:20), Dst: BelkinIn_60:90:56 (ec:1a:59:60:90:56)
> Internet Protocol Version 4, Src: 192.168.1.159, Dst: 192.168.1.115
v Transmission Control Protocol, Src Port: 7442 (7442), Dst Port: 80 (80), Seq: 0, Len: 0
    Source Port: 7442
    Destination Port: 80
    [Stream index: 940]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 32 bytes
  > Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
```

FireFlood

- Targets web servers
- Starts with QUIC
- Switches to HTTP GET
- Embeds some browser info



```
No.  Time      Source    Destination Protocol Length Info
64 2.651119    10.0.0.3  10.0.0.5    QUIC     175 Payload (Encrypted), Seq: 76
```

```
GET AAAAAAAA HTTP/1.1
Host:10.0.0.5:80
User-Agent:Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.10 (KHTML, like Gecko) Chrome/8.0.552.215 Safari/
534.10

HTTP/1.1 400 Bad Request
Date: Thu, 12 May 2016 06:00:46 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 300
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 10.0.0.5 Port 80</address>
</body></html>
```

1 client pkt(s), 1 server pkt(s), 1 turn.

Entire conversation (676 bytes)

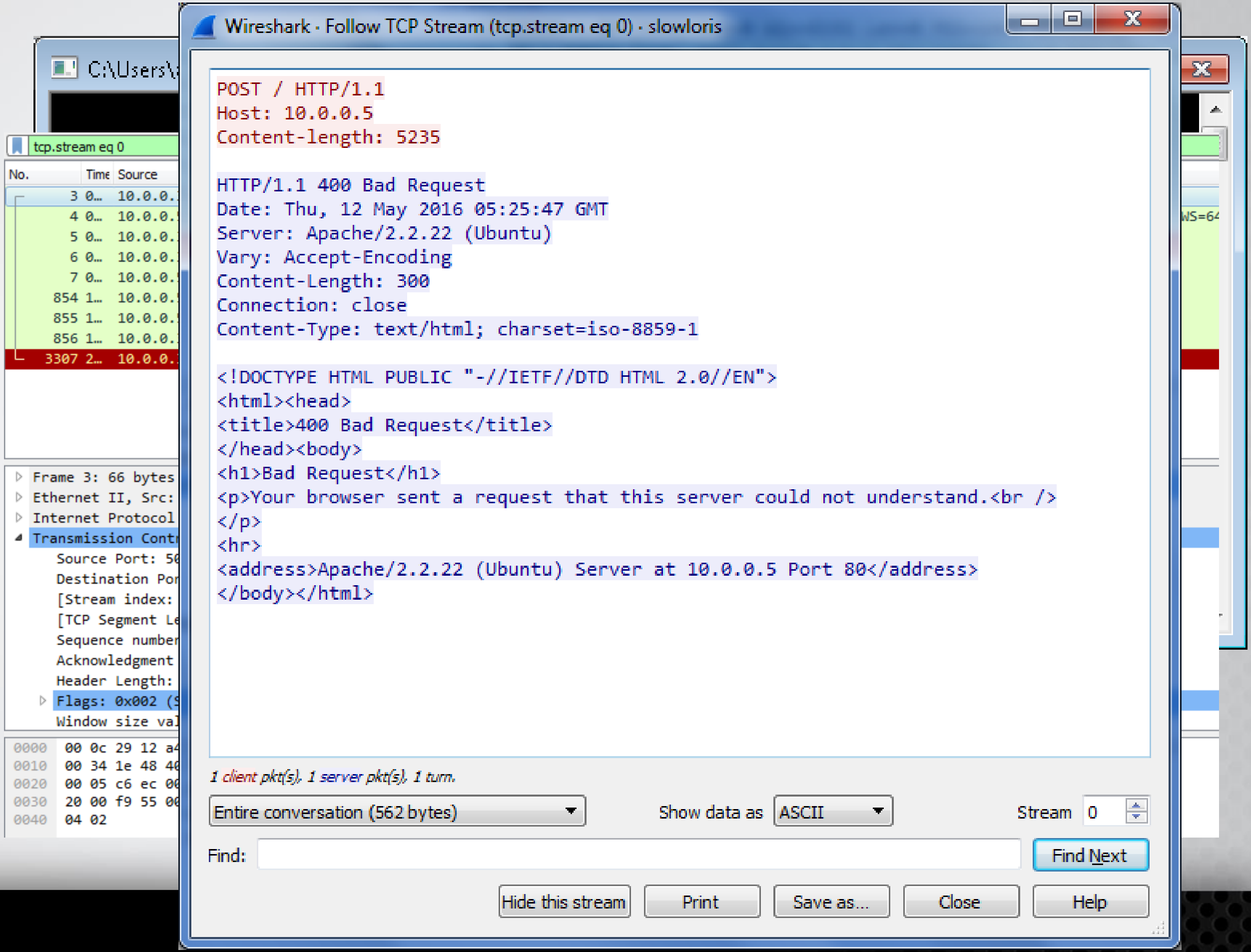
Show data as: ASCII

Stream: 7

Find:

Generic DDoS

- Slowloris attack
- You set the duration
- Meaningless POST
- Server replies
- Connections consumed



```
POST / HTTP/1.1
Host: 10.0.0.5
Content-length: 5235

HTTP/1.1 400 Bad Request
Date: Thu, 12 May 2016 05:25:47 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 300
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 10.0.0.5 Port 80</address>
</body></html>
```

1 client pkt(s), 1 server pkt(s), 1 turn.

Entire conversation (562 bytes) Show data as ASCII Stream 0

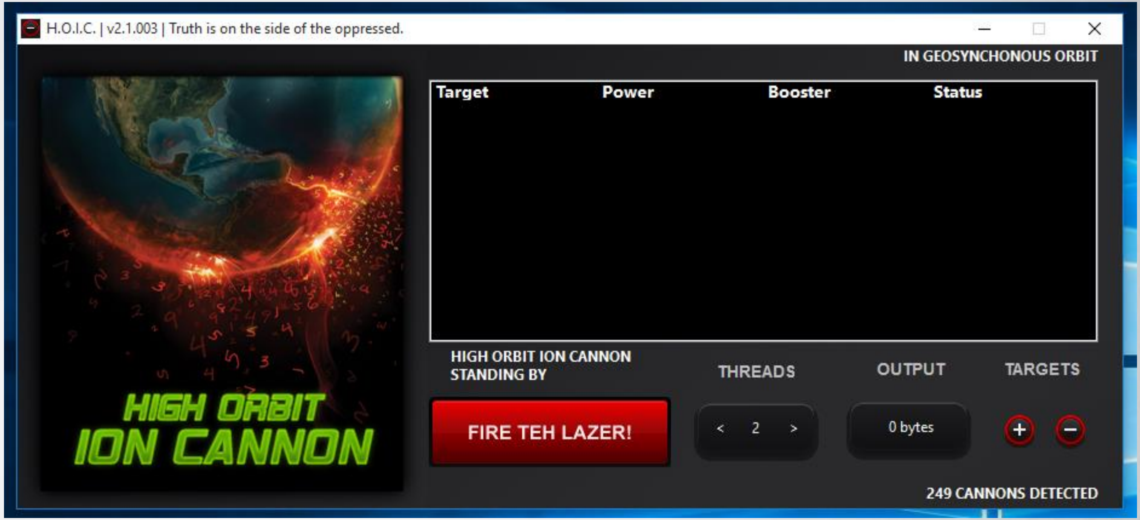
Find:

HOIC

- Sends HTTP Post and GET requests

- Allows booster scripts to enhance attacks, feeding source data into attack payload

- Very common, highly available



H.O.I.C. | v2.1.003 | Truth is on the side of the oppressed.

IN GEOSYNCHONOUS ORBIT

Target	Power	Booster	Status

HIGH ORBIT ION CANNON STANDING BY

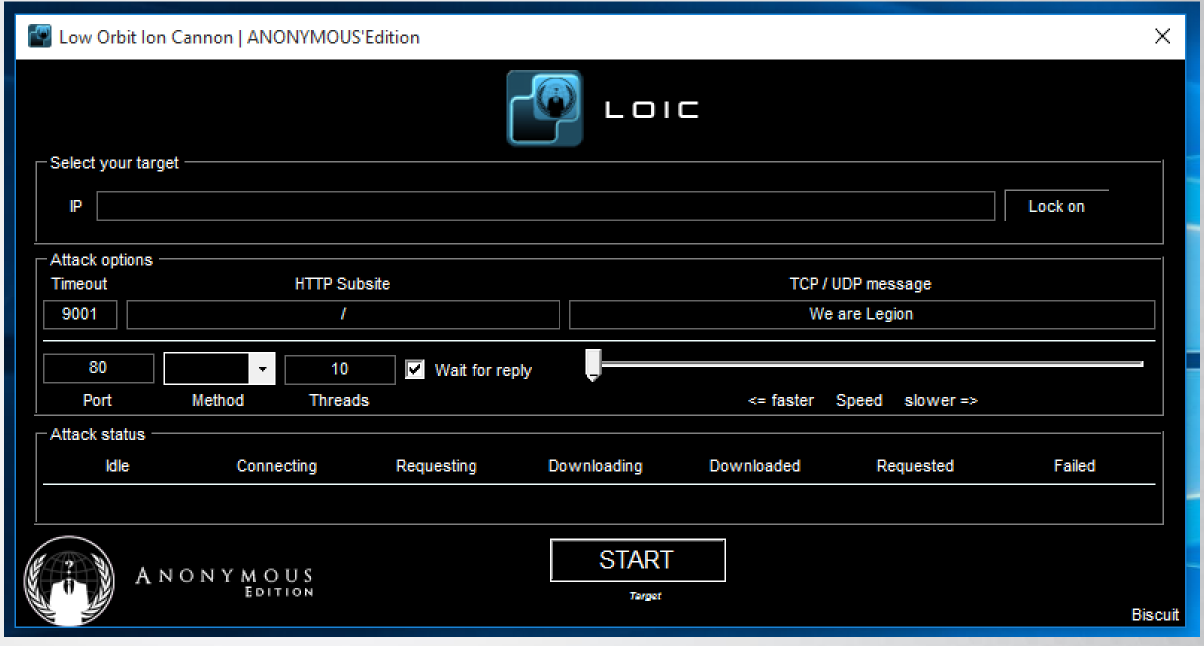
THREADS: 2

OUTPUT: 0 bytes

249 CANNONS DETECTED

LOIC

- Early flooding tool used by Anonymous
- TCP, UDP, HTTP Floods
- Hivemind feature allowing centralized control via IRC
- Does not obscure source IP



Low Orbit Ion Cannon | ANONYMOUS'Edition

Select your target

IP:

Attack options

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: We are Legion

Port: 80

Method:

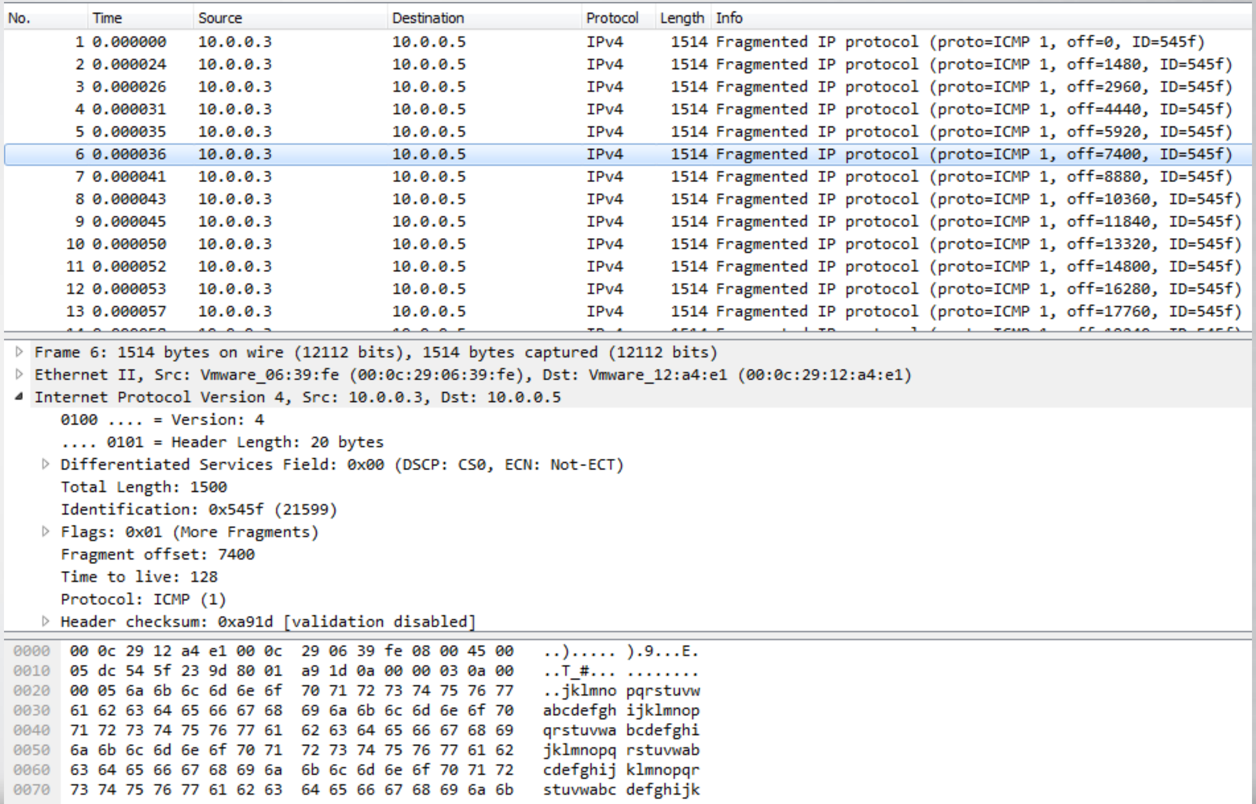
Threads: 10

☑ Wait for reply

Attack status

Pringle DDoS

- Ping tool
- Plays music!
- Otherwise not overly interesting



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=545f)
2	0.000024	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=545f)
3	0.000026	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=545f)
4	0.000031	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=545f)
5	0.000035	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=545f)
6	0.000036	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=7400, ID=545f)
7	0.000041	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=8880, ID=545f)
8	0.000043	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=10360, ID=545f)
9	0.000045	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=11840, ID=545f)
10	0.000050	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=13320, ID=545f)
11	0.000052	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=14800, ID=545f)
12	0.000053	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=16280, ID=545f)
13	0.000057	10.0.0.3	10.0.0.5	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=17760, ID=545f)

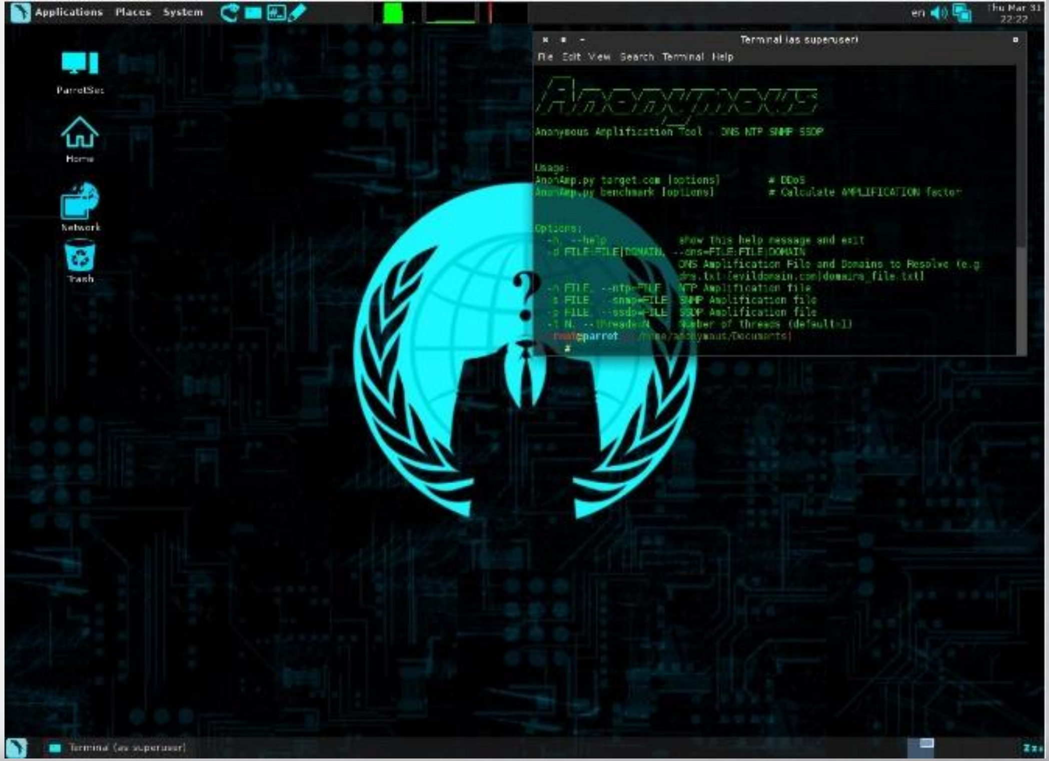
```
▷ Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▷ Ethernet II, Src: Vmware_06:39:fe (00:0c:29:06:39:fe), Dst: Vmware_12:a4:e1 (00:0c:29:12:a4:e1)
◢ Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x545f (21599)
  ▷ Flags: 0x01 (More Fragments)
    Fragment offset: 7400
    Time to live: 128
    Protocol: ICMP (1)
  ▷ Header checksum: 0xa91d [validation disabled]
```

```
0000  00 0c 29 12 a4 e1 00 0c  29 06 39 fe 08 00 45 00   ..)..... ).9...E.
0010  05 dc 54 5f 23 9d 80 01  a9 1d 0a 00 00 03 0a 00   ..T_#... ........
0020  00 05 6a 6b 6c 6d 6e 6f  70 71 72 73 74 75 76 77   ..jklmno pqrstuvw
0030  61 62 63 64 65 66 67 68  69 6a 6b 6c 6d 6e 6f 70   abcdefgh ijklmnop
0040  71 72 73 74 75 76 77 61  62 63 64 65 66 67 68 69   qrstuvwa bcdefghi
0050  6a 6b 6c 6d 6e 6f 70 71  72 73 74 75 76 77 61 62   jklmnopq rstuvwab
0060  63 64 65 66 67 68 69 6a  6b 6c 6d 6e 6f 70 71 72   cdefghij klmnopqr
0070  73 74 75 76 77 61 62 63  64 65 66 67 68 69 6a 6b   stuvwabc defghijk
```

Attack OS Distros

- Parrot OS
    - Popular OS for hacker, like Kali Linux
    - DNS
    - NTP
    - SNMP
    - SSDP

- Kali
- Cyborg
- BlackArch



```
Anonymous Amplification Tool - DNS NTP SNMP SSDP


Usage:
AnonAmp.py target.com [options]         # DDoS
AnonAmp.py benchmark [options]          # Calculate AMPLIFICATION factor


Options:
  -h, --help            show this help message and exit
  -d FILE:FILE|DOMAIN, --dns=FILE:FILE|DOMAIN
                        DNS Amplification File and Domains to Resolve (e.g
                        dns.txt:[evildomain.com|domains_file.txt]
  -n FILE, --ntp=FILE   NTP Amplification file
  -s FILE, --snmp=FILE  SNMP Amplification file
  -p FILE, --ssdp=FILE  SSDP Amplification file
  -t N, --threads=N     Number of threads (default=1)
 root@parrot  /home/anonymous/Documents]
   #
```

Overview

Attack Methods

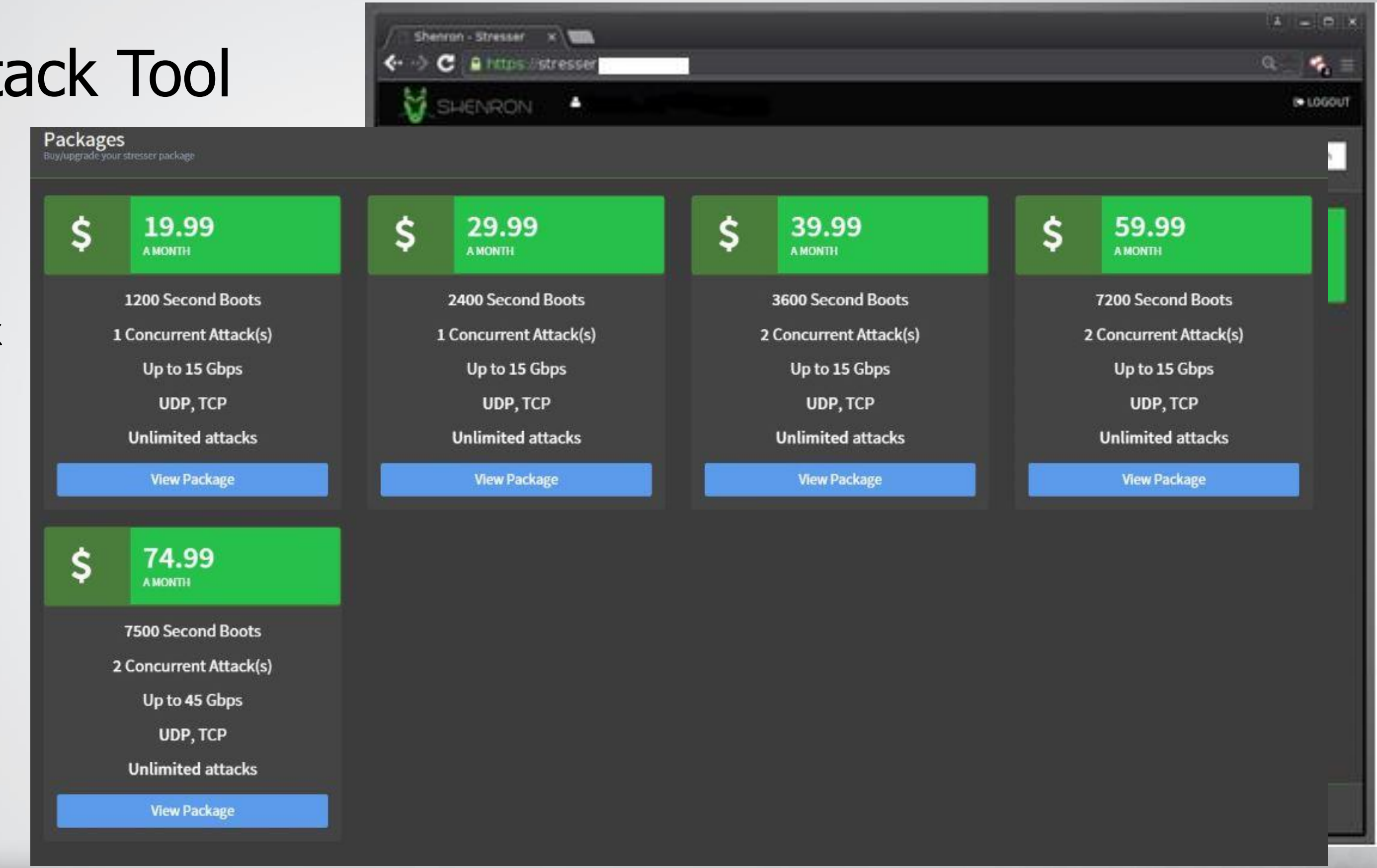
Anonymous Toolkit 2016

Online Services (Booters / Stressers)

Strategies for Survival

Shenron Attack Tool

- Lizard Squad's public stresser services
- $19.99 => 15GB attack for 1200 second
  - DNS
  - SNMP
  - SYN



Packages

Buy/upgrade your stresser package

$ 19.99 A MONTH

1200 Second Boots

1 Concurrent Attack(s)

Up to 15 Gbps

UDP, TCP

Unlimited attacks

View Package

$ 29.99 A MONTH

2400 Second Boots

1 Concurrent Attack(s)

Up to 15 Gbps

UDP, TCP

Unlimited attacks

View Package

$ 39.99 A MONTH

3600 Second Boots

2 Concurrent Attack(s)

Up to 15 Gbps

UDP, TCP

Unlimited attacks

View Package

$ 59.99 A MONTH

7200 Second Boots

2 Concurrent Attack(s)

Up to 15 Gbps

UDP, TCP

Unlimited attacks

View Package

$ 74.99 A MONTH

7500 Second Boots

2 Concurrent Attack(s)

Up to 45 Gbps

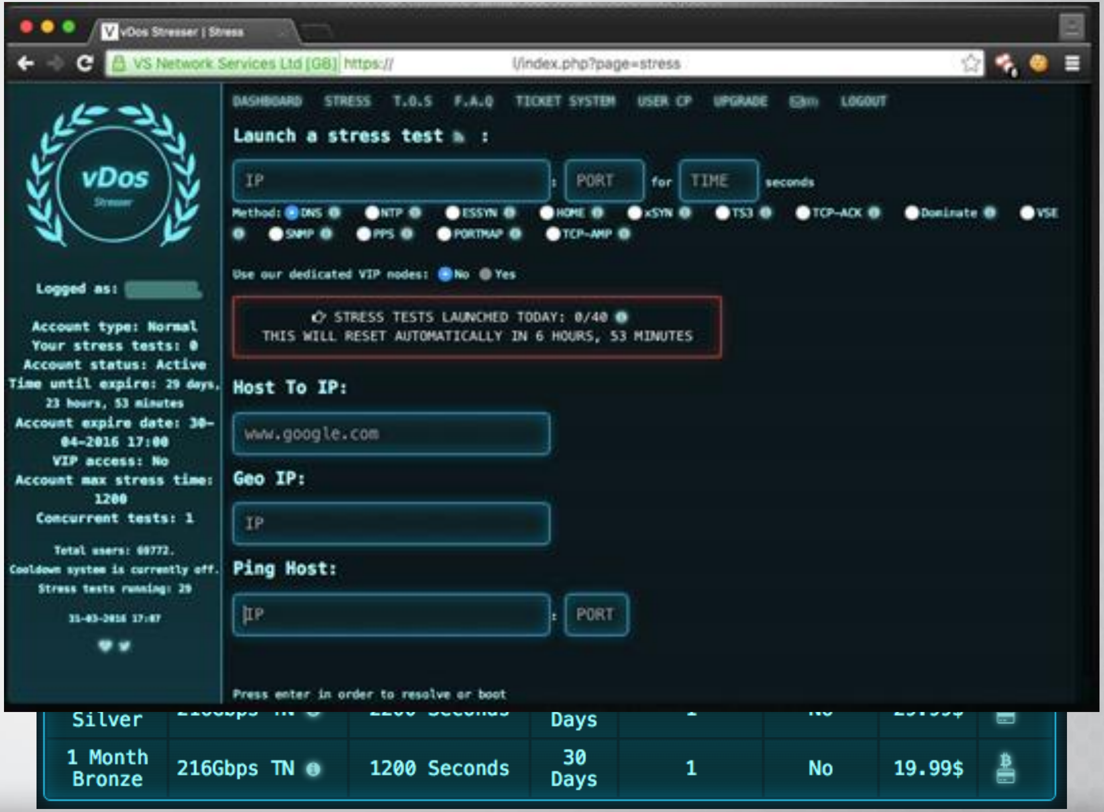
UDP, TCP

Unlimited attacks

View Package

VDoS Attack Tool

- One of the most popular tools
- $19.99 will gain access to 216 Gbps Attack Network
- DNS, NTP, ESSYN, xSYN, TS3, TCP-ACK, Dominate, VSE, SNMP, PPS, Portmap and TCP-Amp



Launch a stress test :

IP : PORT for TIME seconds

Method: ● DNS ○ NTP ○ ESSYN ○ HOME ○ xSYN ○ TS3 ○ TCP-ACK ○ Dominate ○ VSE ○ SNMP ○ PPS ○ PORTMAP ○ TCP-AMP

Use our dedicated VIP nodes: ● No ○ Yes

STRESS TESTS LAUNCHED TODAY: 0/40
THIS WILL RESET AUTOMATICALLY IN 6 HOURS, 53 MINUTES

Host To IP:

www.google.com

Geo IP:

IP

Ping Host:

IP : PORT

Press enter in order to resolve or boot

Logged as: [redacted]

Account type: Normal
Your stress tests: 0
Account status: Active
Time until expire: 29 days, 23 hours, 53 minutes
Account expire date: 30-04-2016 17:00
VIP access: No
Account max stress time: 1200
Concurrent tests: 1

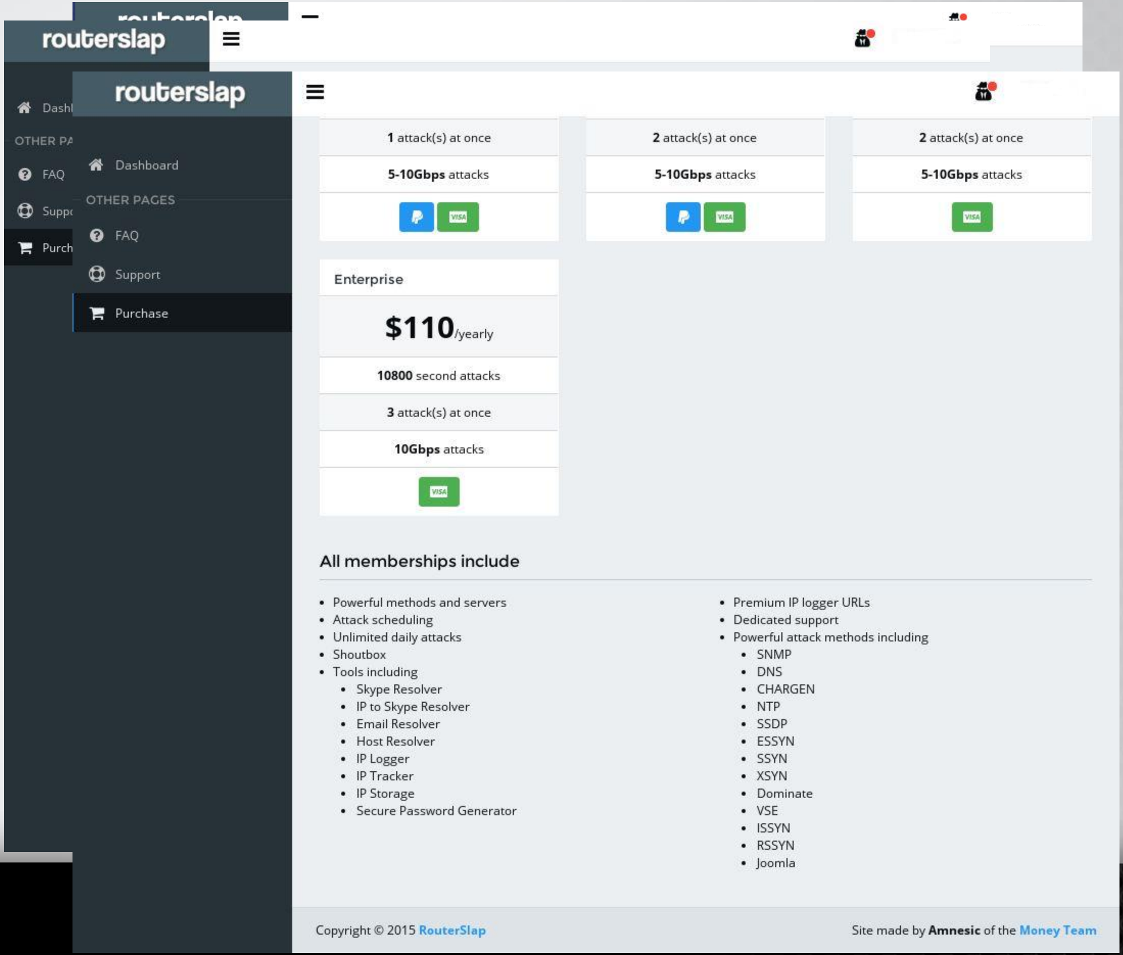
Total users: 60772.
Cooldown system is currently off.
Stress tests running: 29

31-03-2016 17:07

Silver	216Gbps TN	1200 Seconds	Days	1	No	[illegible]	
1 Month Bronze	216Gbps TN	1200 Seconds	30 Days	1	No	19.99$	

RouterSlap

- RouterSlap!
- For $6 you can get a 10-minute attack that is 5-10G
- SNMP, DNS, CHARGEN, NTP, SSDP, ESSYN, SSYN, ZXYN, Dominate, VSE, ISSYN, RSSYN, Joomla
- Attack scheduling
- Unlimited daily attacks



1 attack(s) at once	**2** attack(s) at once	**2** attack(s) at once
5-10Gbps attacks	**5-10Gbps** attacks	**5-10Gbps** attacks

Enterprise

$110/yearly

10800 second attacks

3 attack(s) at once

10Gbps attacks

All memberships include

- Powerful methods and servers
- Attack scheduling
- Unlimited daily attacks
- Shoutbox
- Tools including
  - Skype Resolver
  - IP to Skype Resolver
  - Email Resolver
  - Host Resolver
  - IP Logger
  - IP Tracker
  - IP Storage
  - Secure Password Generator
- Premium IP logger URLs
- Dedicated support
- Powerful attack methods including
  - SNMP
  - DNS
  - CHARGEN
  - NTP
  - SSDP
  - ESSYN
  - SSYN
  - XSYN
  - Dominate
  - VSE
  - ISSYN
  - RSSYN
  - Joomla

Copyright © 2015 RouterSlap

Site made by **Amnesic** of the Money Team

Overview

Attack Methods

Anonymous Toolkit 2016

Online Services (Booters / Stressers)

Strategies for Survival

Lessons Learned - Successful Attack Mitigation

Proactive Preparation and Planning is Key

Need for a Attack Mitigation solution with the **widest coverage** to **protect from multi-vector attacks,** including protection from network and application based DDoS attacks.

Consider a **hybrid solution** that integrates on-premise detection and mitigation with cloud-based protection - to block volumetric attacks.

Monitor security alerts and examine triggers carefully. Tune existing polices and protections to prevent false positives and accurate detection.

A **cyber-security emergency response plan** that includes an emergency response team and process in place. Identify areas where helped is needed from a third party.

A **single point of contact is crucial** when under attack - it will help to divert internet traffic and deploy mitigation solutions.

Thank You

ron.winward@radware.com

www.radware.com
security.radware.com