Analysis of a DDoS Attack

corero
FIRST LINE OF DEFENSE

December 2014

© 2014 Corero

Methodology around DDoS Detection & Mitigation

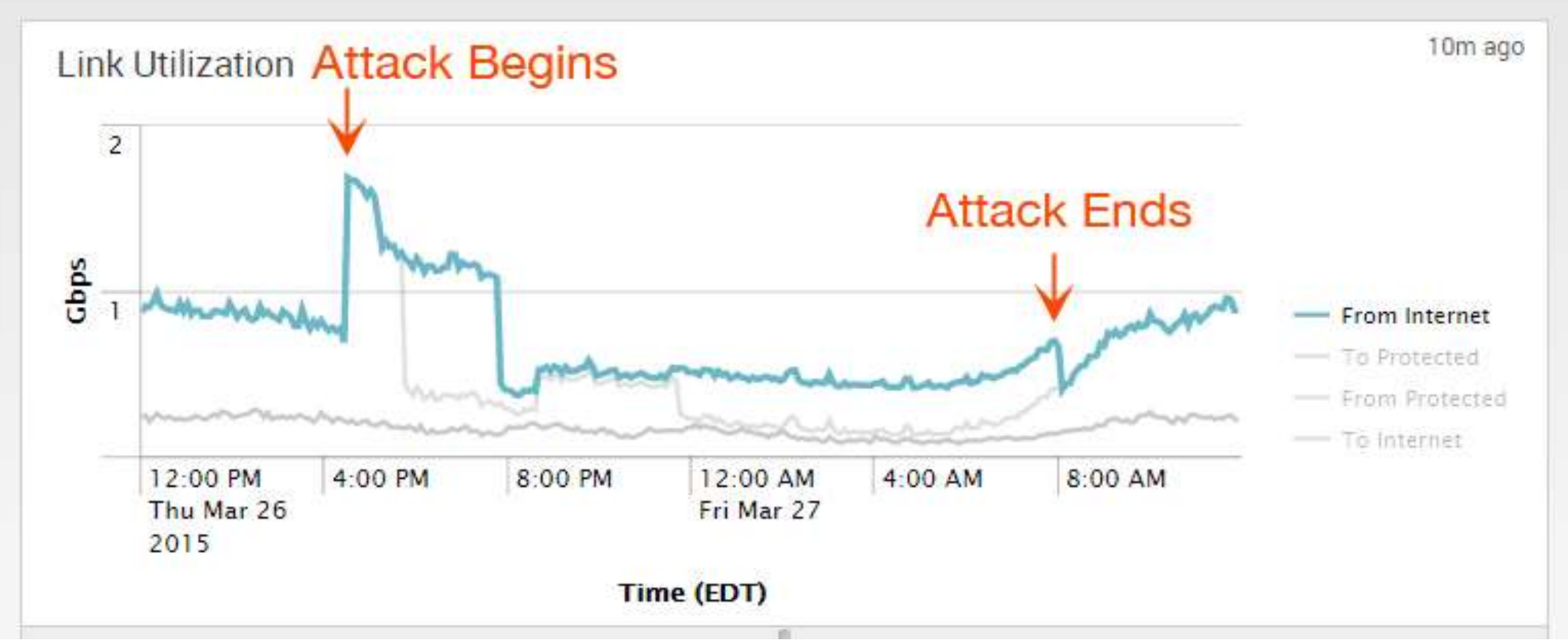
- Corero methodology for DDoS protection
  - Initial Configuration
  - Monitoring and Detection
  - Real-time Mitigation
  - Alerting and Reporting
  - Forensic analysis
  - Custom Mitigation
  - Configuration Optimization

Majority of the protection occurs here (Automatic)

© 2014 Corero

corero
FIRST LINE OF DEFENSE

Example of an Actual Attack



© 2014 Corero

corero
FIRST LINE OF DEFENSE

Network parameters over average:

- **External Port PPS Received**: 158624, which was 49% higher than the 15 min average of 106415
- **External Port BW Received:** 967, which was 34% higher than the 15 min average of 722
- **Internal Port PPS Transmitted:** 158628, which was 49% higher than the 15 min average of 106415
- **Internal Port BW Transmitted:** 967, which was 34% higher than the 15 min average of 722
- **UDP Flows:** 198343, which was 557% higher than the 15 min average of 30207
- **ICMP Flows:** 24386, which was 392% higher than the 15 min average of 4955
- **IP addresses:** 491582, which was 2% higher than the 15 min average of 482795
- **UDP Setup Rate:** 3180, which was 208% higher than the 15 min average of 1032
- **ICMP Setup Rate:** 162, which was 57% higher than the 15 min average of 103, yet below the min threshold of 2000

© 2014 Corero

Anomalous Vectors:

- Destination Port(s):53
  - made up 37.7% of the traffic (by pps), which was 1658% higher than the 15 min average of 2.2% for those port(s)
- Source Port(s):53
  - made up 31.0% of the traffic (by pps), which was 1503% higher than the 15 min average of 1.9% for those port(s)
- PDU Length(s):112261
  - made up 11.7% of the traffic (by pps), which was 51300% higher than the 15 min average of 0.2% for those PDU Length(s)
- PDU Length(s):24798
  - made up 11.7% of the traffic (by pps), which was 51300% higher than the 15 min average of 0.2% for those PDU Length(s)
- SIP/DIP ratio:1.18
  - which was 10% higher than the 15 min average of 1.07

© 2014 Corero


Link Utilization
Attack engaged by 4:33pm
Flow Usage
Packets per Second
Setup Rates
Top 10 Rule Types Blocked
Top 10 Rule Types Detected
002009 engaged by 4:33pm
Blocked Events
Detected Events
Time (EDT)

© 2014 Corero

Initial Analysis

Attack analysis:

- Throughout the attack the primary victim port was port 53 (DNS)
- The attacking protocol was UDP
- The initial phase of the attack lasted approximately 90 minutes
- Predominantly targeted 192.179.83.xxx with an even DIP spray
- Note: Each victim DIP receives approximately 0.5% of the attack (1/255)

© 2014 Corero

corero
FIRST LINE OF DEFENSE

dip

>100 Values, 100% of events

Selected Yes No

Reports

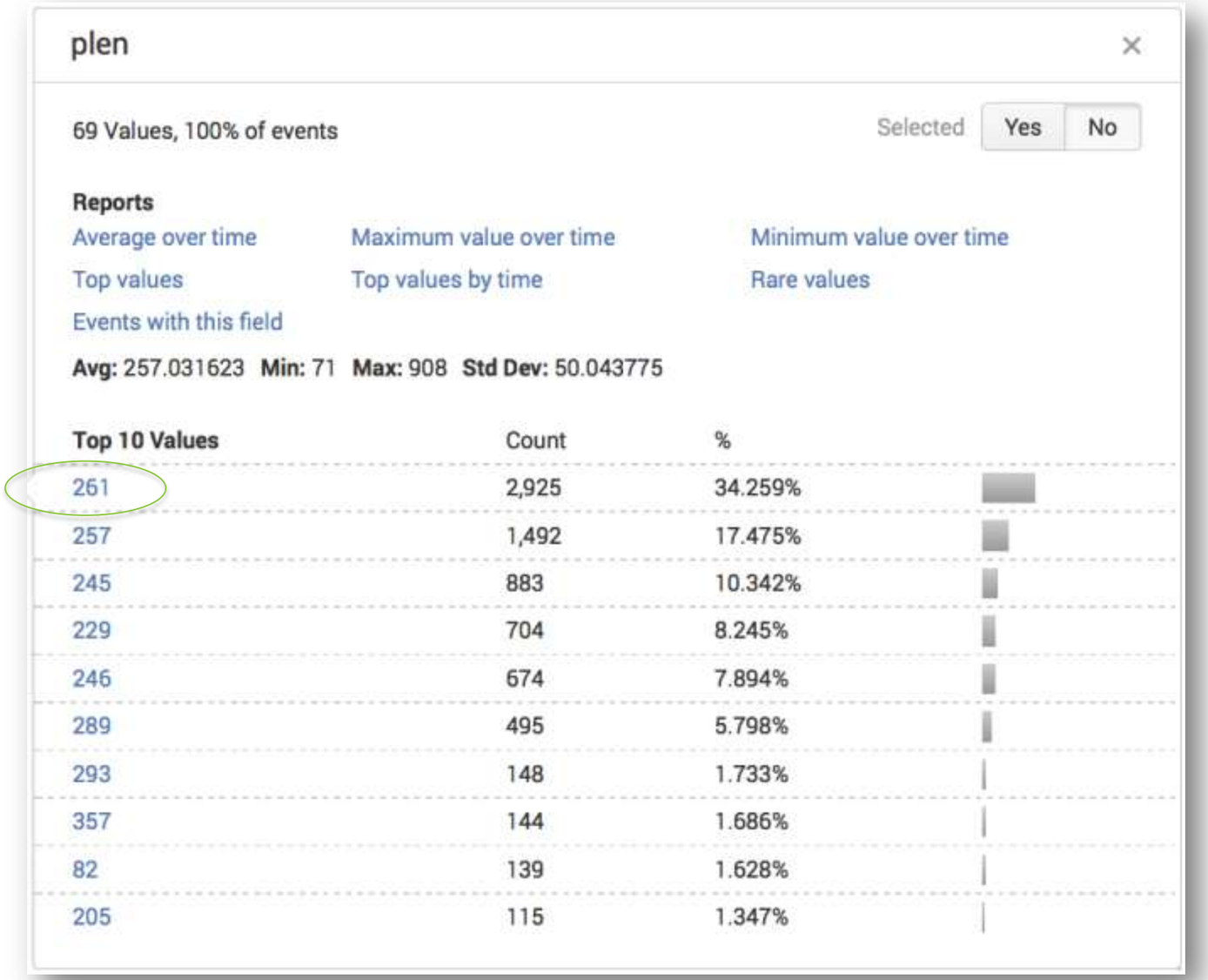
Top values | Top values by time | Rare values

Events with this field

Top 10 Values	Count	%
192.179.83.105	48	0.562%
192.179.83.168	46	0.539%
192.179.83.137	43	0.504%
192.179.83.135	41	0.48%
192.179.83.138	41	0.48%
192.179.83.130	40	0.468%
192.179.83.3	40	0.468%
192.179.83.186	39	0.457%
192.179.83.82	39	0.457%
192.179.83.116	38	0.445%

© 2014 Corero www.corero.com

The typical length of these packets was ~260 bytes:



plen

69 Values, 100% of events

Selected Yes No

Reports

Average over time | Maximum value over time | Minimum value over time

Top values | Top values by time | Rare values

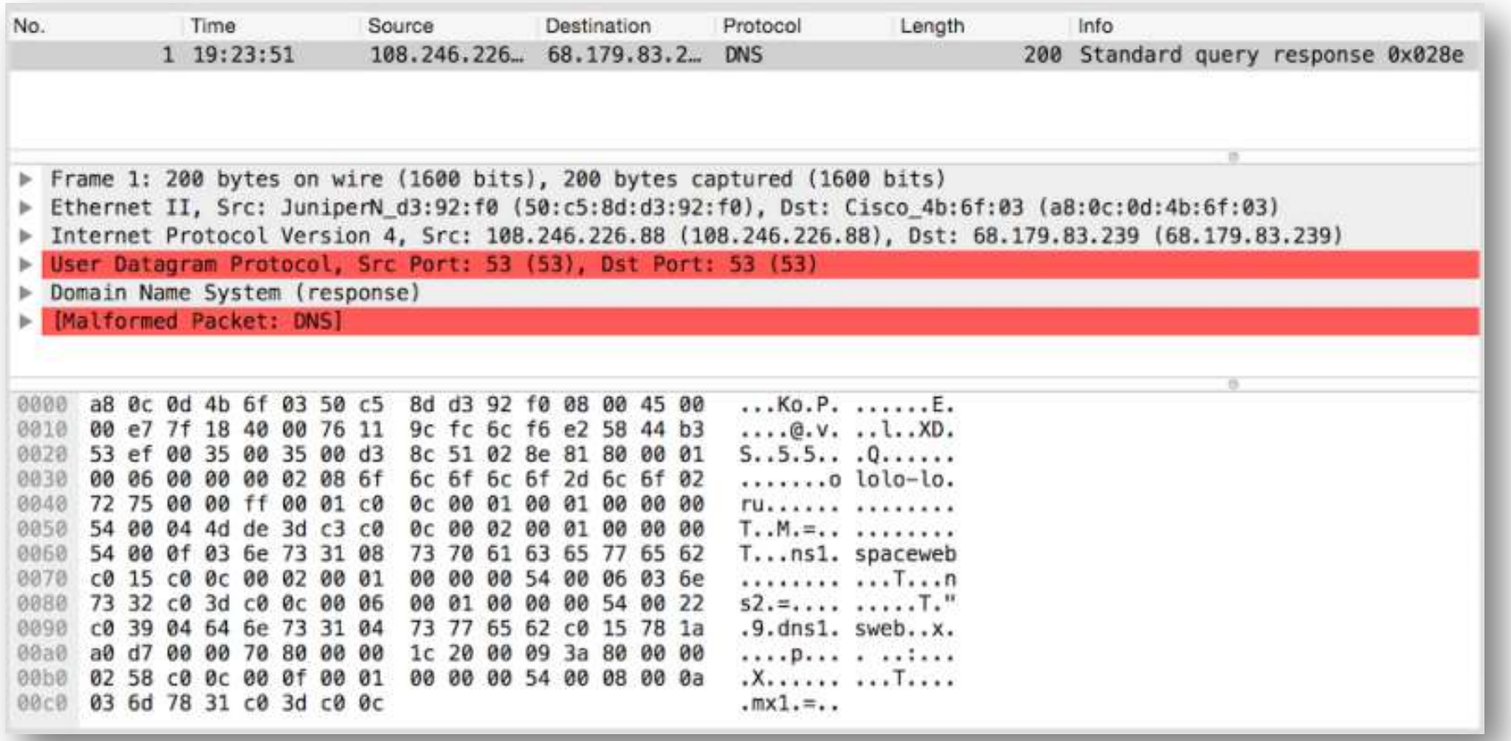
Events with this field

Avg: 257.031623 **Min:** 71 **Max:** 908 **Std Dev:** 50.043775

Top 10 Values	Count	%
261	2,925	34.259%
257	1,492	17.475%
245	883	10.342%
229	704	8.245%
246	674	7.894%
289	495	5.798%
293	148	1.733%
357	144	1.686%
82	139	1.628%
205	115	1.347%

© 2014 Corero

Nature of Multi-vector Attacks



No.	Time	Source	Destination	Protocol	Length	Info
1	19:23:51	108.246.226…	68.179.83.2…	DNS	200	Standard query response 0x028e

```
▶ Frame 1: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits)
▶ Ethernet II, Src: JuniperN_d3:92:f0 (50:c5:8d:d3:92:f0), Dst: Cisco_4b:6f:03 (a8:0c:0d:4b:6f:03)
▶ Internet Protocol Version 4, Src: 108.246.226.88 (108.246.226.88), Dst: 68.179.83.239 (68.179.83.239)
▶ User Datagram Protocol, Src Port: 53 (53), Dst Port: 53 (53)
▶ Domain Name System (response)
▶ [Malformed Packet: DNS]
```

```
0000  a8 0c 0d 4b 6f 03 50 c5  8d d3 92 f0 08 00 45 00   ...Ko.P. ......E.
0010  00 e7 7f 18 40 00 76 11  9c fc 6c f6 e2 58 44 b3   ....@.v. ..l..XD.
0020  53 ef 00 35 00 35 00 d3  8c 51 02 8e 81 80 00 01   S..5.5.. .Q......
0030  00 06 00 00 00 02 08 6f  6c 6f 6c 6f 2d 6c 6f 02   .......o lolo-lo.
0040  72 75 00 00 ff 00 01 c0  0c 00 01 00 01 00 00 00   ru...... ........
0050  54 00 04 4d de 3d c3 c0  0c 00 02 00 01 00 00 00   T..M.=.. ........
0060  54 00 0f 03 6e 73 31 08  73 70 61 63 65 77 65 62   T...ns1. spaceweb
0070  c0 15 c0 0c 00 02 00 01  00 00 00 54 00 06 03 6e   ........ ...T...n
0080  73 32 c0 3d c0 0c 00 06  00 01 00 00 00 54 00 22   s2.=.... .....T."
0090  c0 39 04 64 6e 73 31 04  73 77 65 62 c0 15 78 1a   .9.dns1. sweb..x.
00a0  a0 d7 00 00 70 80 00 00  1c 20 00 09 3a 80 00 00   ....p... . ..:...
00b0  02 58 c0 0c 00 0f 00 01  00 00 00 54 00 08 00 0a   .X...... ...T....
00c0  03 6d 78 31 c0 3d c0 0c                           .mx1.=..
```

- Thursday 26th @ 8:35pm - the attack evolved to mostly target a specific IP address 192.179.83.193
- During this next period the attack also switched to a different major vector of spoofed SIP TCP SYN flood attack.
  - Note: This SYN flood used low source port numbers (below 1024)
- SYN flood was the dominant vector - from ~8:42pm on the 26th until ~8:00am on the 27th

© 2014 Corero

corero FIRST LINE OF DEFENSE

Network parameters over average:

At time:03/26/2015:20:42:00 - Protection Group:Cluster1_1

- **External Port PPS Received**: 303595, which was 208% higher than the 15 min average of 98715
- **External Port BW Received**: 416, which was 12% higher than the 15 min average of 373
- **Internal Port PPS Transmitted**: 249009, which was 427% higher than the 15 min average of 47272
- **Internal Port BW Transmitted**: 386, which was 45% higher than the 15 min average of 266
- **TCP Flows**: 4620643, which was 8113% higher than the 15 min average of 56262
- **IP Addresses**: 3539764, which was 741% higher than the 15 min average of 420802
- **TCP Setup Rate:** 237089, exceeded the static threshold of 100000

© 2014 Corero

corero FIRST LINE OF DEFENSE

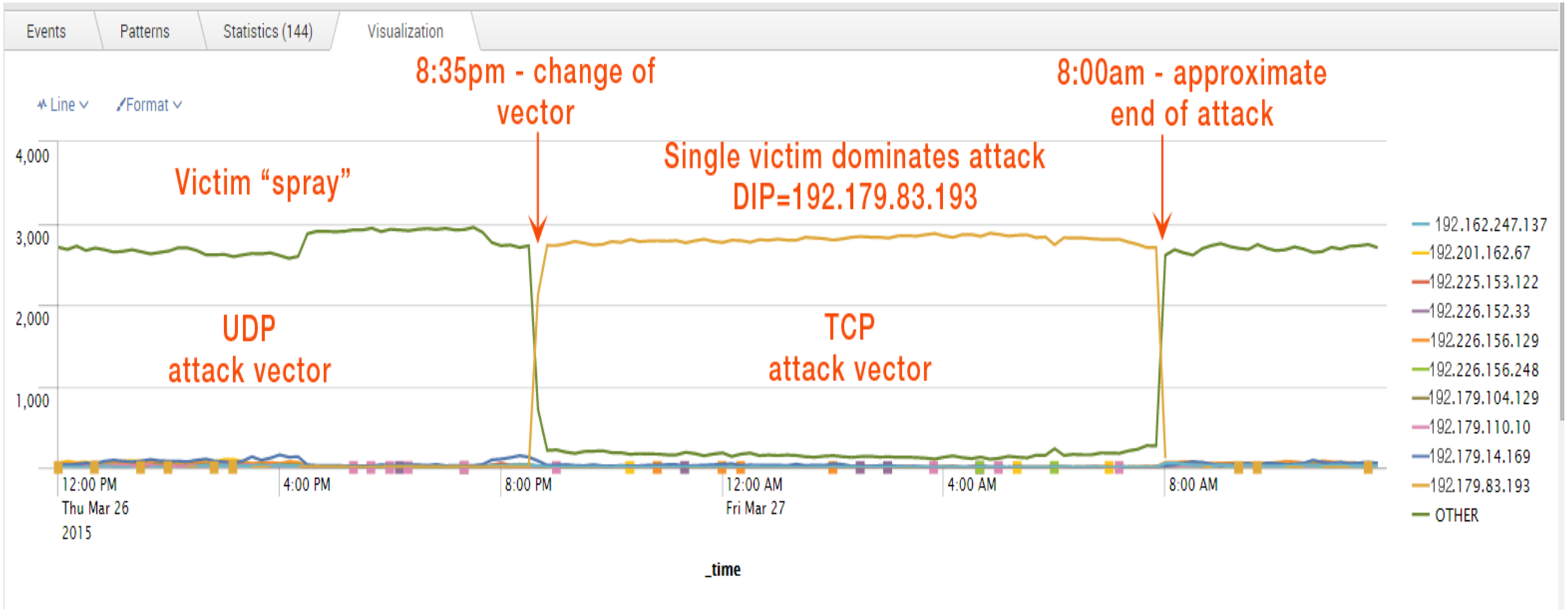
Anomalous Vectors:

At time:03/26/2015:20:42:00 - Protection Group:Cluster1_1

- **Destination IP(s)**:
  - 192.179.83.193 made up 67.3% of the traffic (by pps), which was 43186% higher than the 15 min average of 0.2% for those IP(s).
- **Source Port(s)**:
  - 1 made up 16.3% of the traffic (by pps), which was 99999% higher than the 15 min average of 0.0% for those port(s).
- **TCP Flag(s)**:
  - 2 made up 67.7% of the traffic (by pps), which was 13139% higher than the 15 min average of 0.5% for those TCP Flag(s).
- **PDU Length(s)**:
  - 66 made up 69.3% of the traffic (by pps), which was 1939% higher than the 15 min average of 3.4% for those PDU Length(s).
- **PDU Length(s)**:
  - 52 made up 69.3% of the traffic (by pps), which was 1939% higher than the 15 min average of 3.4% for those PDU Length(s).
- **SIP/DIP ratio**:
  - 4.28 which was 234% higher than the 15 min average of 1.28

© 2014 Corero

Example of change of victim DIP



© 2014 Corero

corero
FIRST LINE OF DEFENSE

corero
FIRST LINE OF DEFENSE

Thank You!

Two major vectors:

1. DNS reflection UDP – subnet spray (3+ hours)
2. TCP SYN flood – single victim DIP (12+ hours)

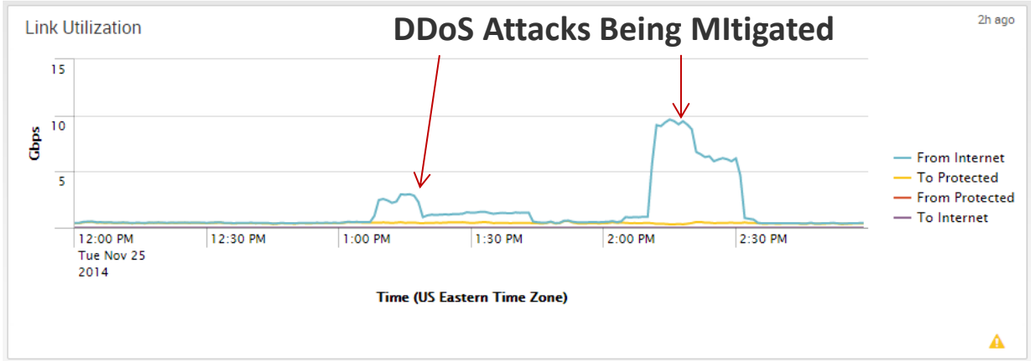
- In a optimized SecureWatch configuration system that was ready for production mitigation it should have been possible to mitigate the majority of this 15 hour attack automatically without operator intervention.
- In the case if unexpected issues or inquiries the Corero SOC would have been available to assist.
- The automatic mechanisms leveraged would include:
- Rule cns-002009 (UDP rate limit) & Rule cns-001020 (New IP setup rate)
- In addition more selective smart-rule and flex-rule mitigations are available for this type of attack.
- Optional additional protection for a long running attack such as this would have been flex-rule assist from the Corero SOC (note: customer's own team can also apply this protection).
- In addition, as illustrated above, comprehensive forensic information and dashboards are available during the attack to provide detail information on the traffic anomaly and verify that mitigations are effective or to drive optional optimization of thresholds and filter if necessary.

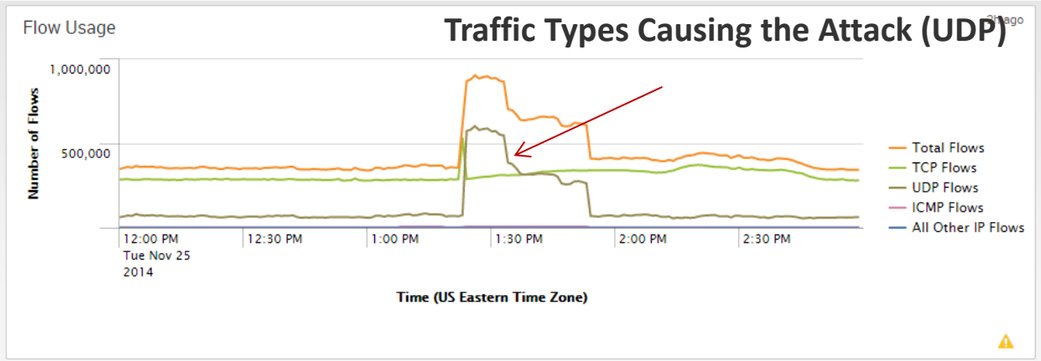
© 2014 Corero

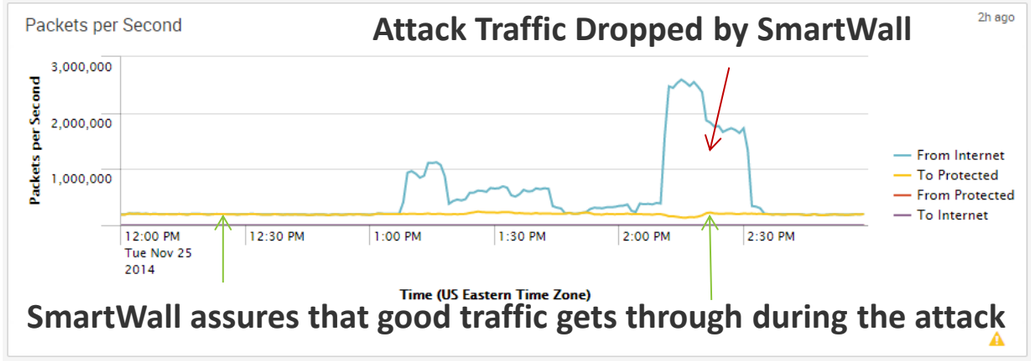
corero FIRST LINE OF DEFENSE

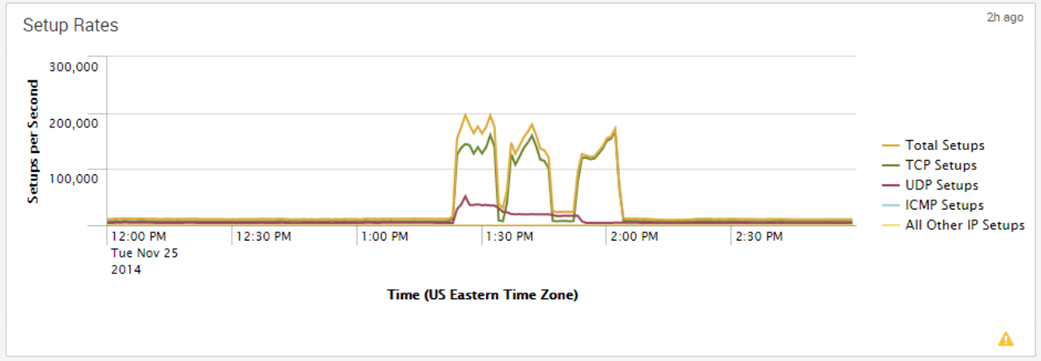
Turn-key DDoS Visibility

Network Level Visibility

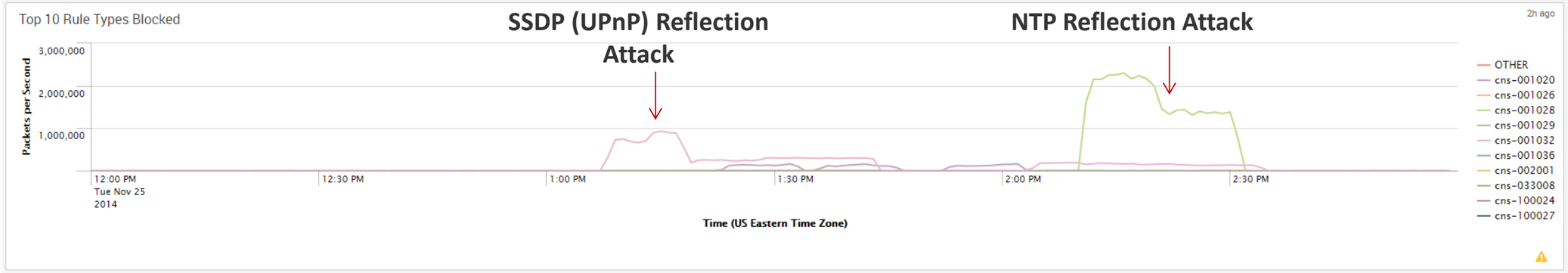








Security Visibility

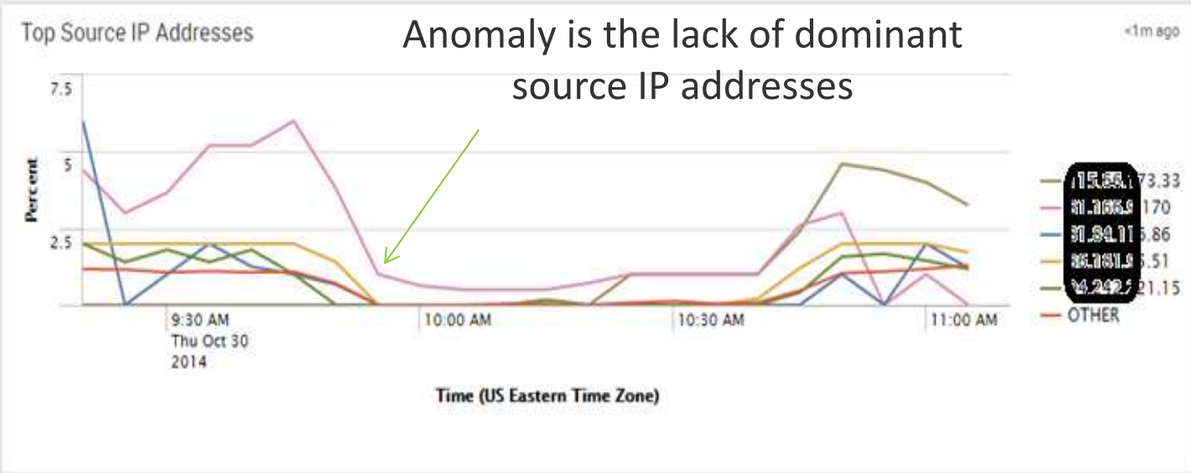


© 2014 Corero

corero FIRST LINE OF DEFENSE

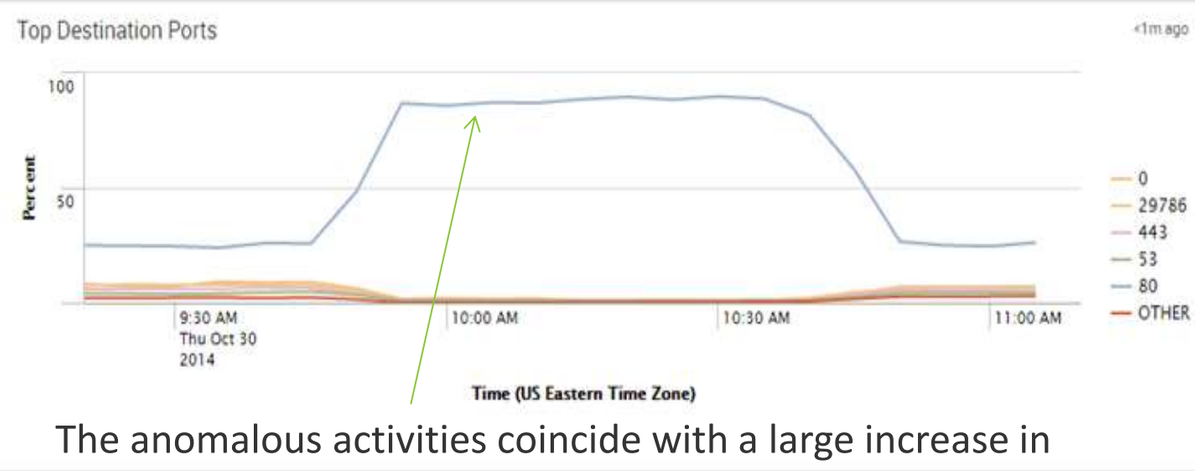
Attack Diagnosis and Analysis

Start of an attack
Anomaly is the lack of dominant source IP addresses



Two server IP addresses being targeted

Rapid increase in traffic from source port 123 indicates an NTP reflection attack



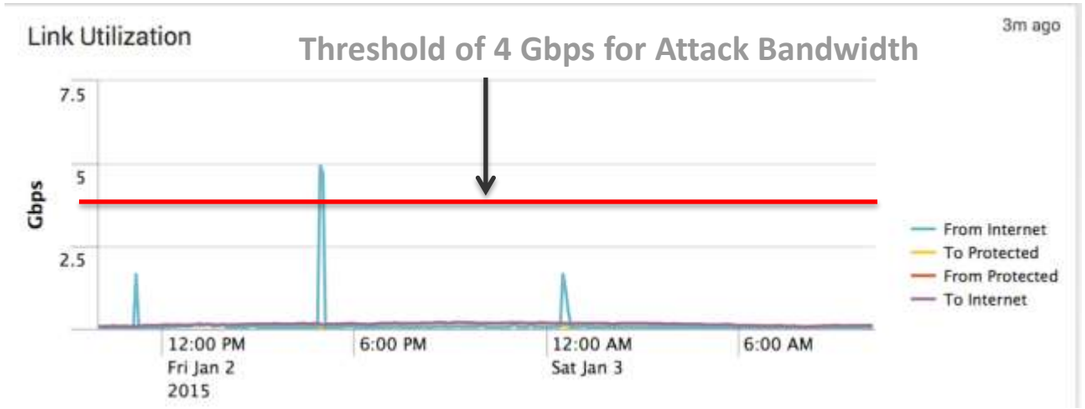
The anomalous activities coincide with a large increase in traffic to port 80 – HTTP service under attack

© 2015 Corero

corero
FIRST LINE OF DEFENSE

Alerting - Proactive Reporting

Providers can set up to be alerted of early warning signs of a possible attack



E-mail alert generated by SecureWatch Analytics notifying the provider about the destination IP under attack

From: <securewatchalert@corero.com>
Date: Saturday, January 3, 2015 at 12:32 AM
Subject: Corero Securewatch Alert: IP=a.b.c.d

{ip:‘a.b.c.d.',bandwidth_current:‘4911.6',bandwidth_threshold:‘4000',current_pps:'686418'}

Upon receiving the alert, the provider can investigate further and possibly take additional actions on a per destination IP basis.
This is an opportunity for the provider to deliver services to its customers.

© 2015 Corero

corero FIRST LINE OF DEFENSE