corero

UKNOF44

NOC Consideration: Dance of Multi-Vector DDoS Attacks

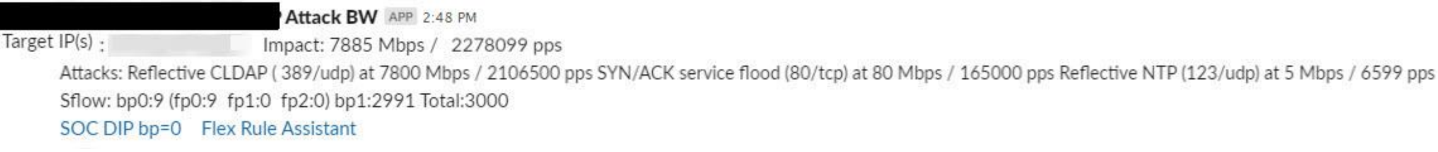
Aseem Sharma
Security Services Manager

Overview

- “Incident Inc.” a hosting provider.
- In conjunction with their own NOC, they work closely with Corero.
- We get same alerts as their NOC does.

Incident Detected

- Alert received from onsite alerting system.



[redacted] Attack BW APP 2:48 PM

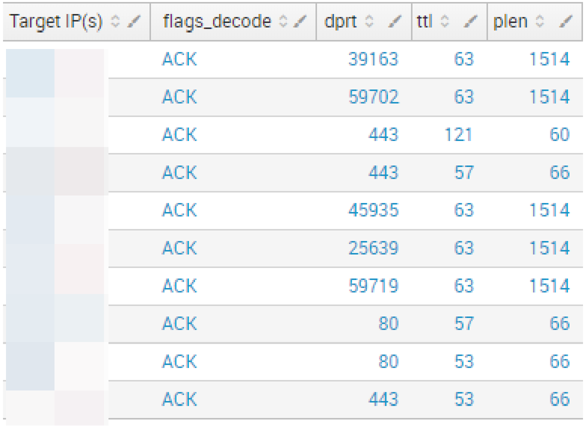
Target IP(s) : [redacted] Impact: 7885 Mbps / 2278099 pps

Attacks: Reflective CLDAP (389/udp) at 7800 Mbps / 2106500 pps SYN/ACK service flood (80/tcp) at 80 Mbps / 165000 pps Reflective NTP (123/udp) at 5 Mbps / 6599 pps

Sflow: bp0:9 (fp0:9 fp1:0 fp2:0) bp1:2991 Total:3000

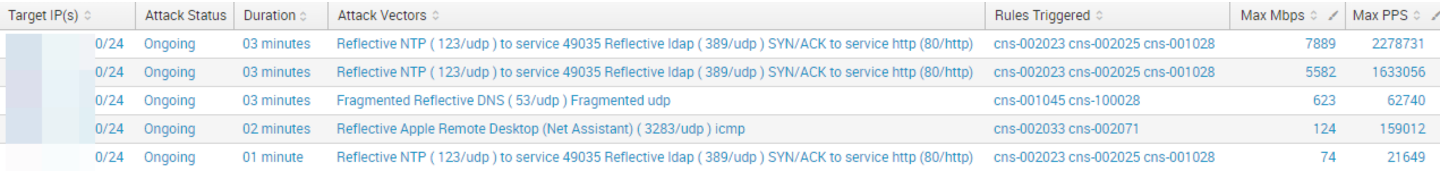
SOC DIP bp=0 Flex Rule Assistant

- Review of allowed traffic



Target IP(s)	flags_decode	dprt	ttl	plen
[redacted]	ACK	39163	63	1514
[redacted]	ACK	59702	63	1514
[redacted]	ACK	443	121	60
[redacted]	ACK	443	57	66
[redacted]	ACK	45935	63	1514
[redacted]	ACK	25639	63	1514
[redacted]	ACK	59719	63	1514
[redacted]	ACK	80	57	66
[redacted]	ACK	80	53	66
[redacted]	ACK	443	53	66

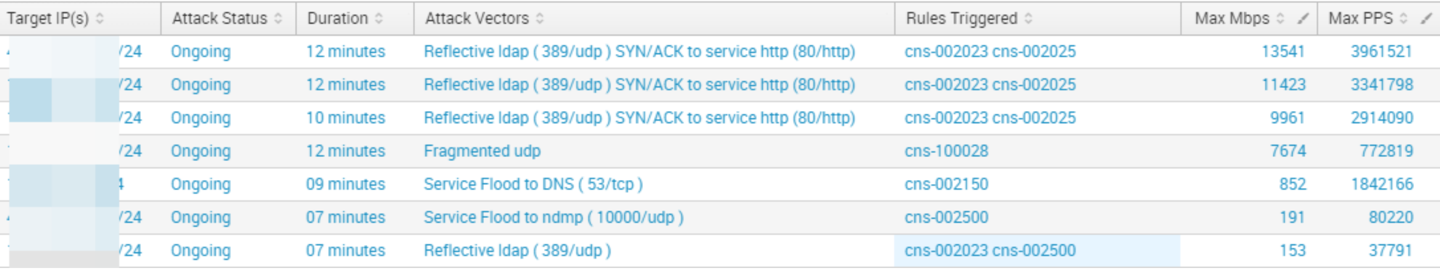
Incident Lifecycle



Target IP(s)	Attack Status	Duration	Attack Vectors	Rules Triggered	Max Mbps	Max PPS
[redacted]0/24	Ongoing	03 minutes	Reflective NTP (123/udp) to service 49035 Reflective ldap (389/udp) SYN/ACK to service http (80/http)	cns-002023 cns-002025 cns-001028	7889	2278731
[redacted]0/24	Ongoing	03 minutes	Reflective NTP (123/udp) to service 49035 Reflective ldap (389/udp) SYN/ACK to service http (80/http)	cns-002023 cns-002025 cns-001028	5582	1633056
[redacted]0/24	Ongoing	03 minutes	Fragmented Reflective DNS (53/udp) Fragmented udp	cns-001045 cns-100028	623	62740
[redacted]0/24	Ongoing	02 minutes	Reflective Apple Remote Desktop (Net Assistant) (3283/udp) icmp	cns-002033 cns-002071	124	159012
[redacted]0/24	Ongoing	01 minute	Reflective NTP (123/udp) to service 49035 Reflective ldap (389/udp) SYN/ACK to service http (80/http)	cns-002023 cns-002025 cns-001028	74	21649

- Sharp increase in attack traffic targeting multiple /24s
- We check with their NOC to see if things are going OK at their end.

Incident Lifecycle

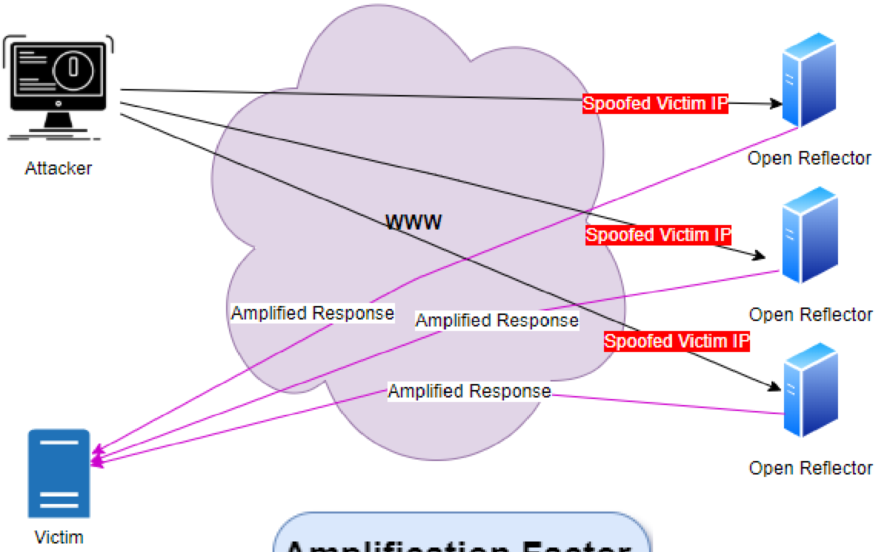


Target IP(s)	Attack Status	Duration	Attack Vectors	Rules Triggered	Max Mbps	Max PPS
[redacted]/24	Ongoing	12 minutes	Reflective ldap (389/udp) SYN/ACK to service http (80/http)	cns-002023 cns-002025	13541	3961521
[redacted]/24	Ongoing	12 minutes	Reflective ldap (389/udp) SYN/ACK to service http (80/http)	cns-002023 cns-002025	11423	3341798
[redacted]/24	Ongoing	10 minutes	Reflective ldap (389/udp) SYN/ACK to service http (80/http)	cns-002023 cns-002025	9961	2914090
[redacted]/24	Ongoing	12 minutes	Fragmented udp	cns-100028	7674	772819
[redacted]4	Ongoing	09 minutes	Service Flood to DNS (53/tcp)	cns-002150	852	1842166
[redacted]/24	Ongoing	07 minutes	Service Flood to ndmp (10000/udp)	cns-002500	191	80220
[redacted]/24	Ongoing	07 minutes	Reflective ldap (389/udp)	cns-002023 cns-002500	153	37791

- Change of vector
  - Increase in Reflective CLDAP
  - Fragmented Attacks
  - New Service floods
  - Reduction in Reflected NTP

Attack Analysis

- Anatomy of Reflective Attacks



Amplification Factor

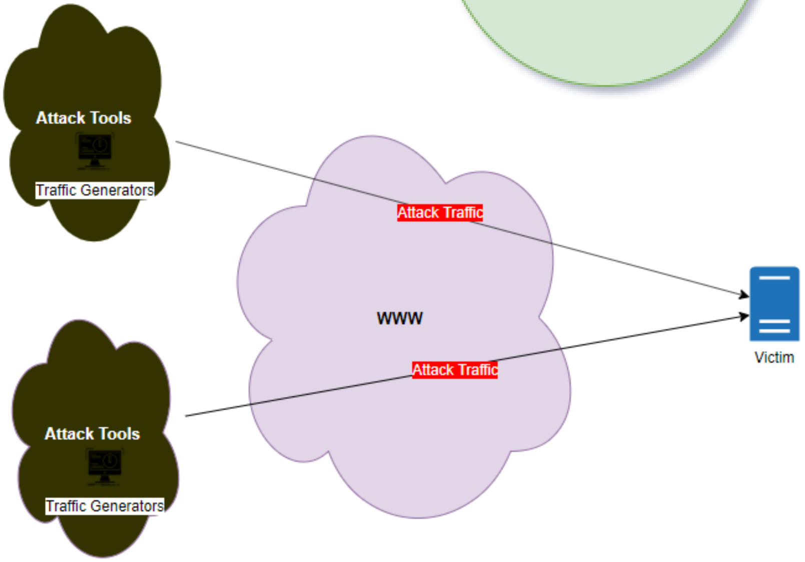
CLDAP	- x46 to x55
NTP	- ~x556
SSDP	- ~x30
Memcache	- x10k to x50k

Attack Analysis

- Anatomy of Service Attacks

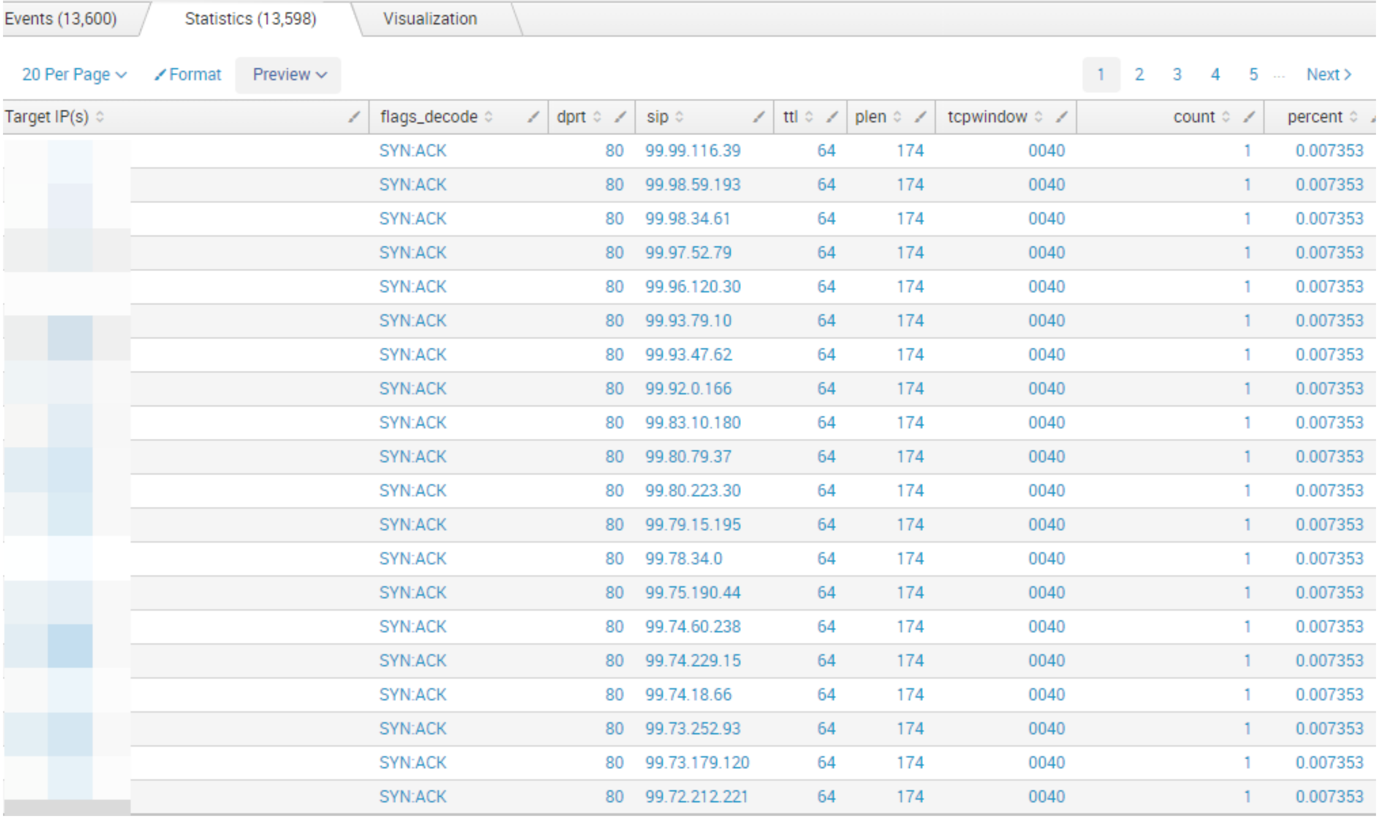
~25%

Of all attacks are Service Floods in past 3 months



Attack Analysis

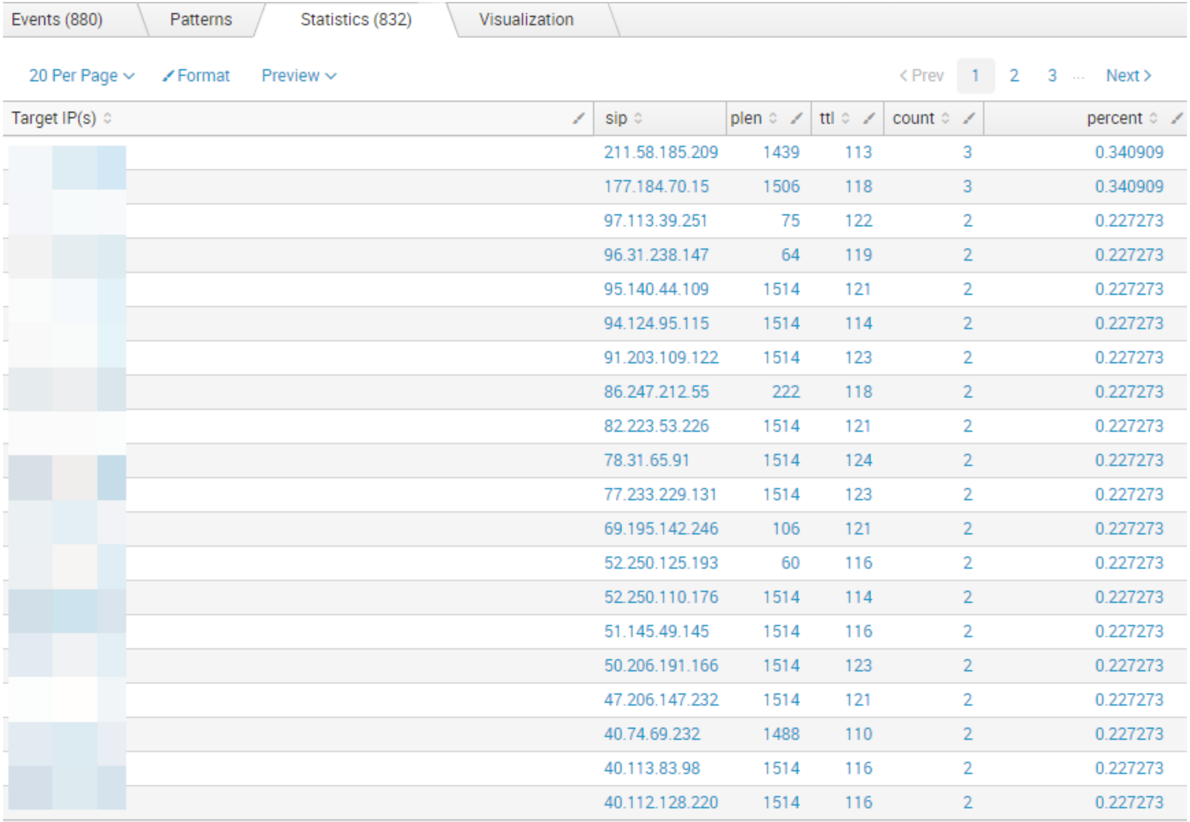
- Vector 1 : SYN/ACK service flood to HTTP



Target IP(s)	flags_decode	dprt	sip	ttl	plen	tcpwindow	count	percent
[redacted]	SYN:ACK	80	99.99.116.39	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.98.59.193	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.98.34.61	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.97.52.79	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.96.120.30	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.93.79.10	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.93.47.62	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.92.0.166	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.83.10.180	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.80.79.37	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.80.223.30	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.79.15.195	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.78.34.0	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.75.190.44	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.74.60.238	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.74.229.15	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.74.18.66	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.73.252.93	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.73.179.120	64	174	0040	1	0.007353
[redacted]	SYN:ACK	80	99.72.212.221	64	174	0040	1	0.007353

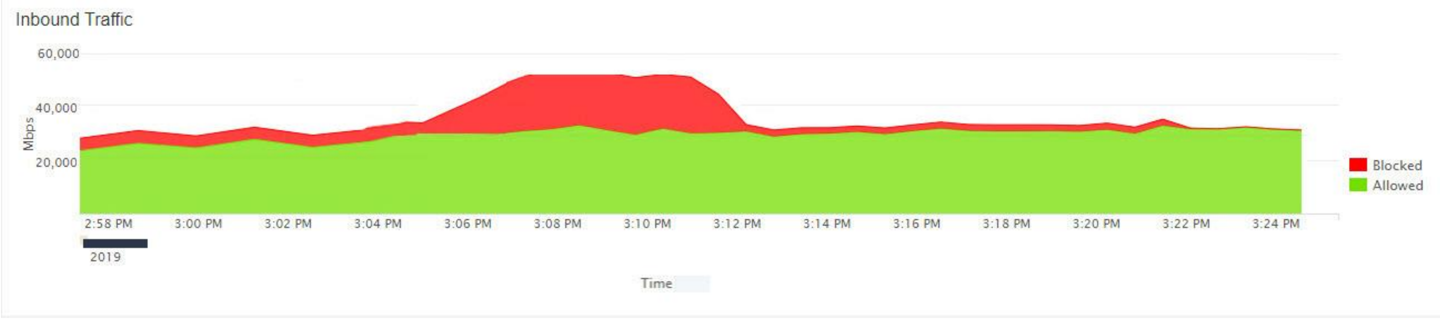
Attack Analysis

- Vector 2 : Reflective CLDAP



Target IP(s)	sip	plen	ttl	count	percent
[redacted]	211.58.185.209	1439	113	3	0.340909
[redacted]	177.184.70.15	1506	118	3	0.340909
[redacted]	97.113.39.251	75	122	2	0.227273
[redacted]	96.31.238.147	64	119	2	0.227273
[redacted]	95.140.44.109	1514	121	2	0.227273
[redacted]	94.124.95.115	1514	114	2	0.227273
[redacted]	91.203.109.122	1514	123	2	0.227273
[redacted]	86.247.212.55	222	118	2	0.227273
[redacted]	82.223.53.226	1514	121	2	0.227273
[redacted]	78.31.65.91	1514	124	2	0.227273
[redacted]	77.233.229.131	1514	123	2	0.227273
[redacted]	69.195.142.246	106	121	2	0.227273
[redacted]	52.250.125.193	60	116	2	0.227273
[redacted]	52.250.110.176	1514	114	2	0.227273
[redacted]	51.145.49.145	1514	116	2	0.227273
[redacted]	50.206.191.166	1514	123	2	0.227273
[redacted]	47.206.147.232	1514	121	2	0.227273
[redacted]	40.74.69.232	1488	110	2	0.227273
[redacted]	40.113.83.98	1514	116	2	0.227273
[redacted]	40.112.128.220	1514	116	2	0.227273

Incident Conclusion



98%

Attacks are less than

10Gbps

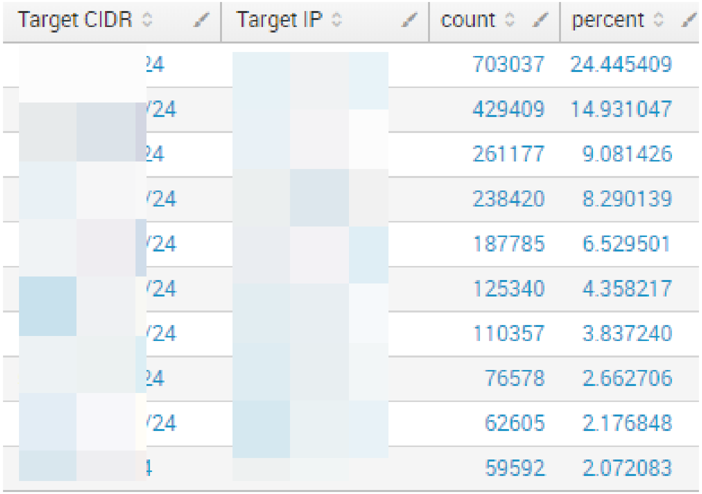
(2018 Trend Report)

81%

Of attacks last 10 minutes

or less

Bandwidth Consideration

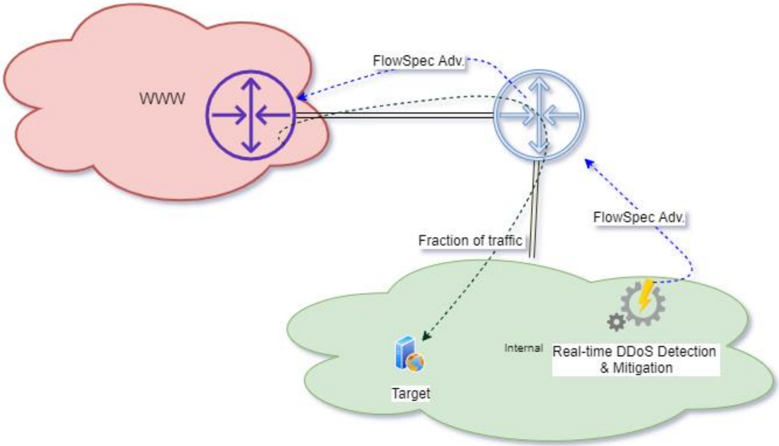


Target CIDR	Target IP	count	percent
[redacted]	[redacted]	703037	24.445409
[redacted]	[redacted]	429409	14.931047
[redacted]	[redacted]	261177	9.081426
[redacted]	[redacted]	238420	8.290139
[redacted]	[redacted]	187785	6.529501
[redacted]	[redacted]	125340	4.358217
[redacted]	[redacted]	110357	3.837240
[redacted]	[redacted]	76578	2.662706
[redacted]	[redacted]	62605	2.176848
[redacted]	[redacted]	59592	2.072083

- ‘Incident Inc.’ content on attack being mitigated automatically.
- Risk of link saturation?
- Caution: Increase in attack may result in good traffic being squeezed out…

Upstream considerations

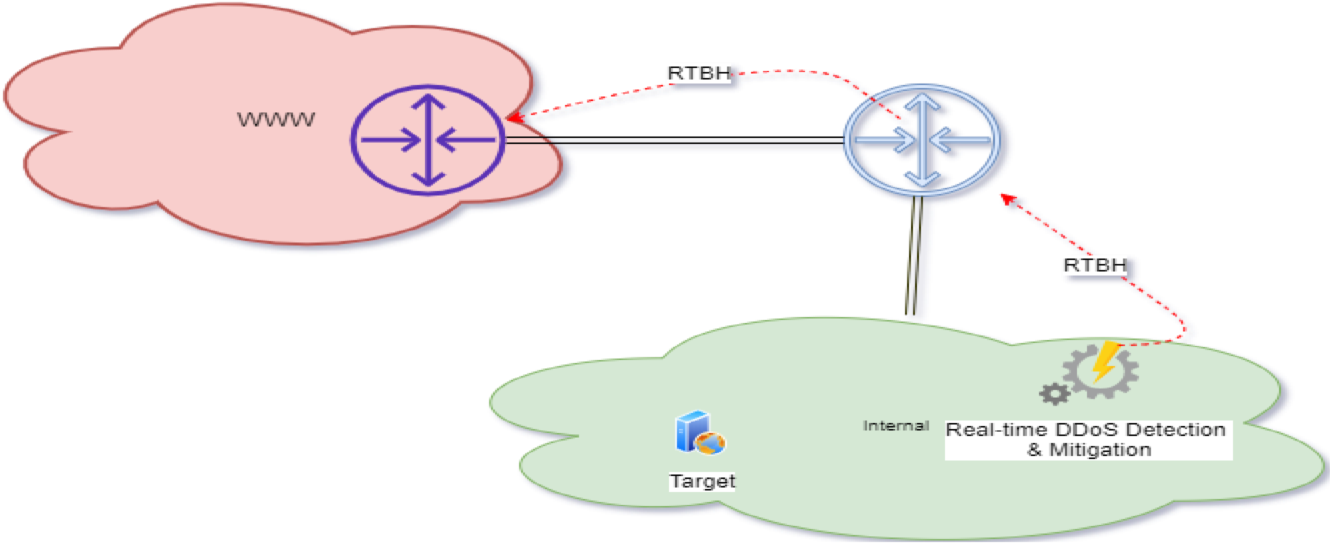
FlowSpec



- May provide slightly granular relief.
- Implementation varies by the vendor. (L3/L4 filtering)
- Prior agreements may be required – 'Incident Inc.' did not have one…
- Intelligent DDoS Mitigation solutions should have this feature built-in.

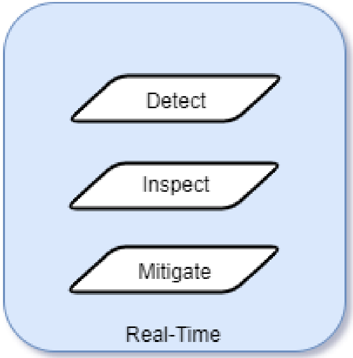
Upstream considerations
RTBH

- Option of last resort. – Destination will become unavailable!
- Will drop ALL traffic – good or bad.
- Consideration: NAT IP….
- ‘Incident Inc.’ decides NOT to do this.



Takeaway #1 – Real-Time Operations

- Detection of specific vectors is the key.
- Real-time detection and classification essential for effective DDoS mitigation.
- Always-ON protection ensures ALL attacks are dealt with.
- Opportunity for Service providers to ‘clean’ traffic for their customers

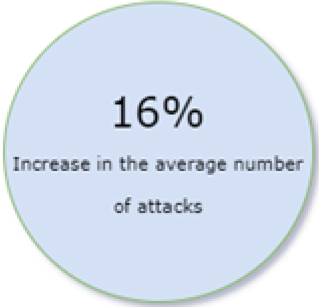


Takeaway #2 – Smart Alerting

- NOC Assist
  - DDoS mitigation solutions must support NOC's decision making.

  - This is paramount in formation of any effective DDoS defense strategy.
- Better Analytics helps NOC take data driven decisions.
- Corero's SOC for example relies on Smart alerting and Autonomics to provide highest standards of service to our end clients.

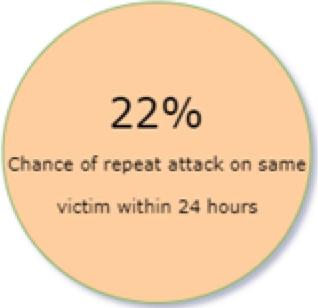
Conclusion



16%

Increase in the average number of attacks

- Always-on protection is the key deterrence against multi-vector DDoS attacks



22%

Chance of repeat attack on same victim within 24 hours

- Sub-Second detection and mitigation = high uptime!
- Smart-Alerting and rich analytics supports NOCs (Organizations) in making cognizant data driven decisions.

Questions?