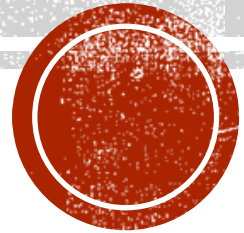
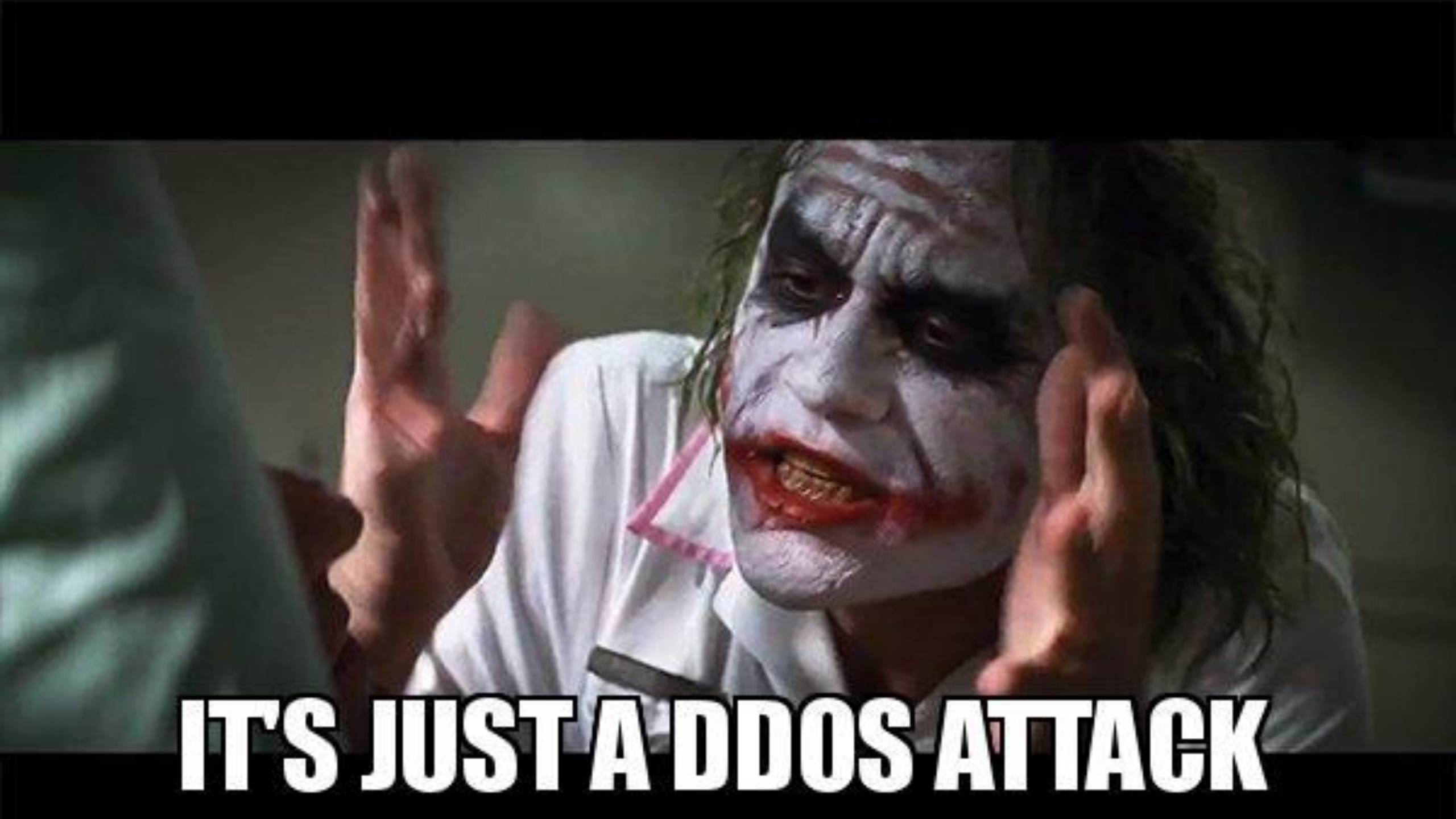
PANIC IN THE NOC – EXTORSION DDOS

Samuel Rossier / @sam0x90
BlackHat.971 Chapter Meet Up
22.02.2023




PACK


IT'S JUST A DDOS ATTACK

We are the Lazarus and we have chosen <REDACTED> as target for our next DDoS attack

Please perform a google search for "Lazarus Group" to have a look at some of our previous work.

Also perform a serch for "NZX" or "New Zealand Stock Exchange" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting at Monday next week. (This is not a hoax, and to prove it right now we will start a small attack on your DNS servers for 60min. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.)

There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

...

How you can stop this? We will refrain from attacking your servers for a small fee. The current fee is 20 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

RANSOM NOTE

We are the Lazarus and we have chosen <REDACTED> as target for our next DDoS attack

Please perform a google search for "Lazarus Group" to have a look at some of our previous work.

Also perform a serch for "NZX" or "New Zealand Stock Exchange" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting at Monday next week. (This is not a hoax, and to prove it right now we will start a small attack on your DNS servers for 60min. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.)

There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

...

How you can stop this? We will refrain from attacking your servers for a small fee. The current fee is 20 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

RANSOM NOTE

WHAT TYPE OF DDOS EXIST?

Volumetric

Saturate the bandwidth

UDP flood, spoofed-packet, amplification, etc.

BPS

Protocol/State-exhaustion

Saturate processing capacity of stateful device

L3-L4: SYN flood, ICMP flood, etc.

PPS

Application

Exhaustion of application resource or exploitation of vulnerability

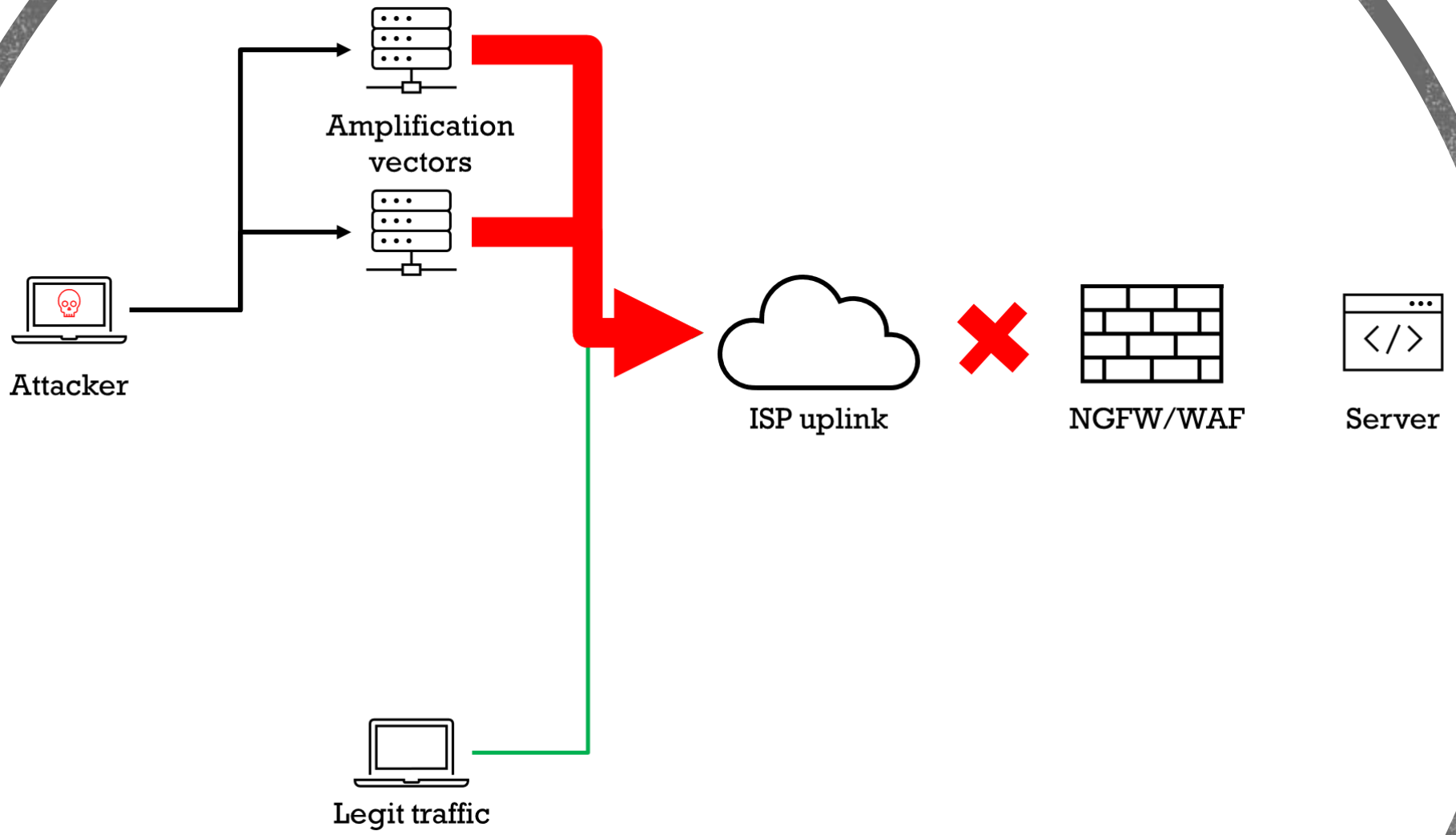
L7: HTTP flood, Slow Loris/Post, SSL renegotiation., etc.

RPS

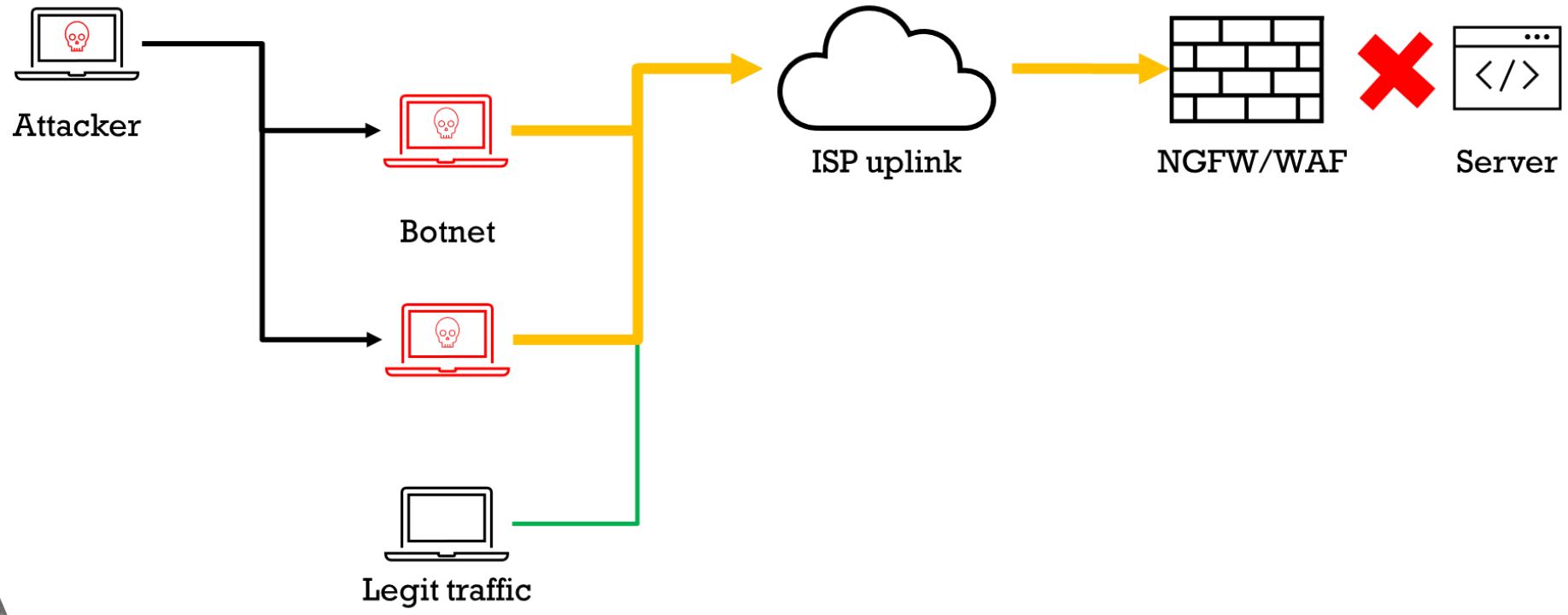
WHAT TYPE OF DDOS EXIST?

Volumetric	Protocol/State-exhaustion	Application
Saturate the bandwidth	Saturate processing capacity of stateful device	Exhaustion of application resource or exploitation of vulnerability
UDP flood, spoofed-packet, amplification, etc.	L3-L4: SYN flood, ICMP flood, etc.	L7: HTTP flood, Slow Loris/Post, SSL renegotiation., etc.
BPS	PPS	RPS

Multi-vector DDoS


Amplification vectors
Attacker
ISP uplink
NGFW/WAF
Server
Legit traffic

VOLUMETRIC



STATE-EXHAUSTION

Type

- Multi-vector DDoS:
  - Volumetric: Amplification using ARMS, DNS and NTP
  - Protocol: SYN flood

Targets

- DNS servers
- Corporate website

Measure

- 40 Gbps and 6 Mpps (others faced up to 120 Gbps)

Duration and Impact

- 3h attack, 1h offline

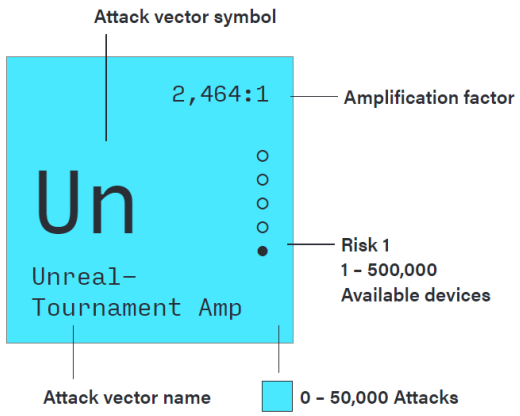
TTPs

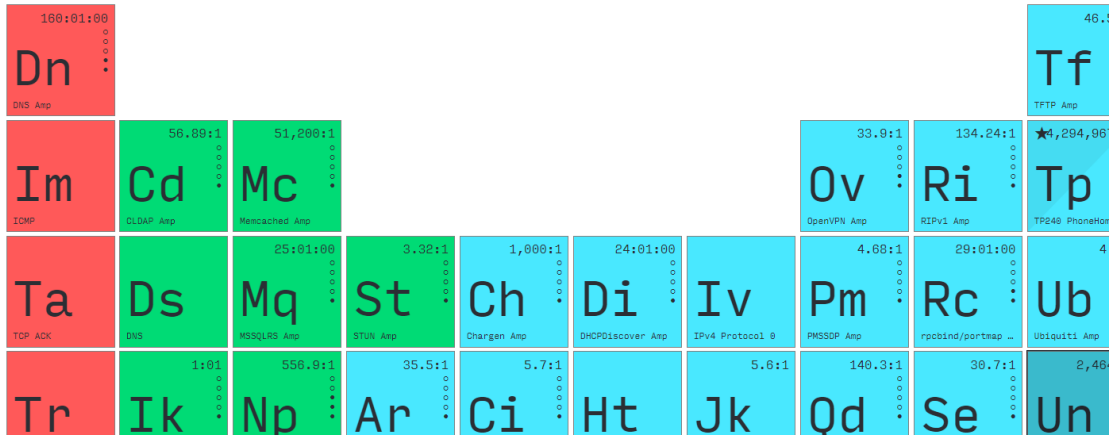
- Reconnaissance: T1589.002, T1590.002
- Impact: T1498.002, T1499.001

Unreal-Tournament Amp

Unreal Engine is a suite of creation tools for game development, architectural and automotive visualization, linear film and television content creation, broadcast and live event production, training and simulation, and other real-time applications. A vulnerability in Unreal Engine can be exploited to launch DDoS attacks.

NUMBER OF ATTACKS	19,619
AVAILABLE DEVICES	31,774

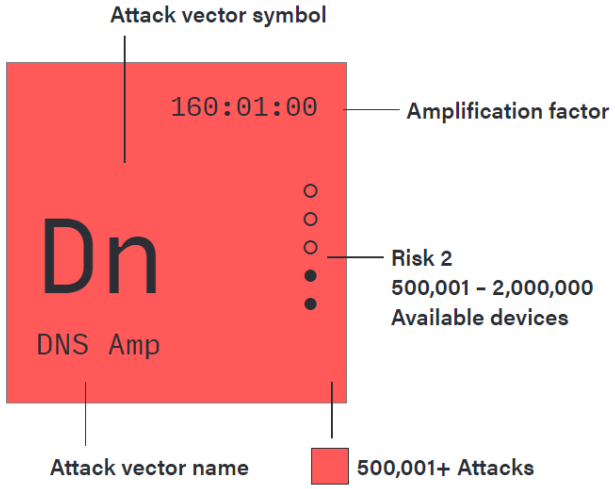


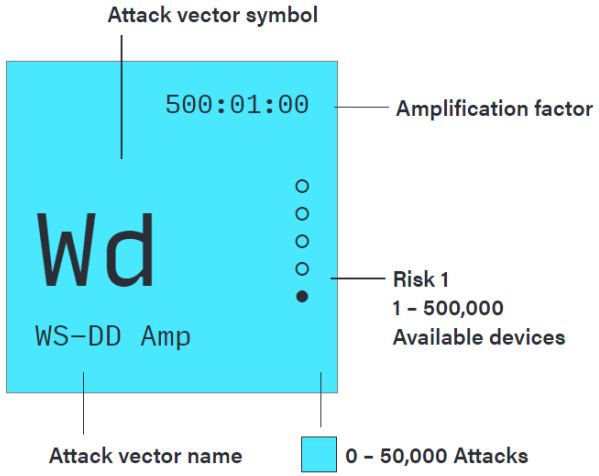


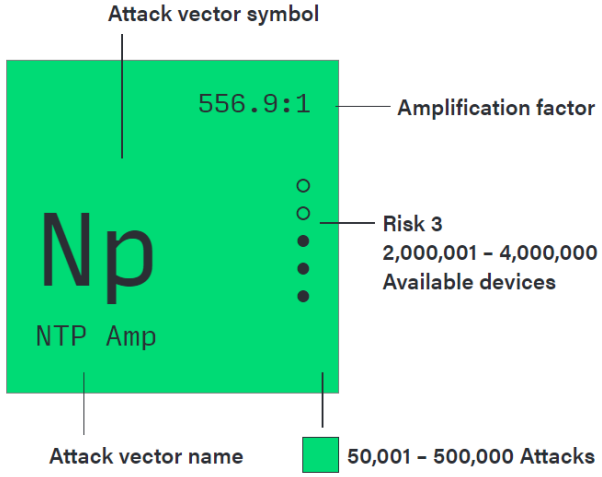
(TT)PROCEDURE FOCUS

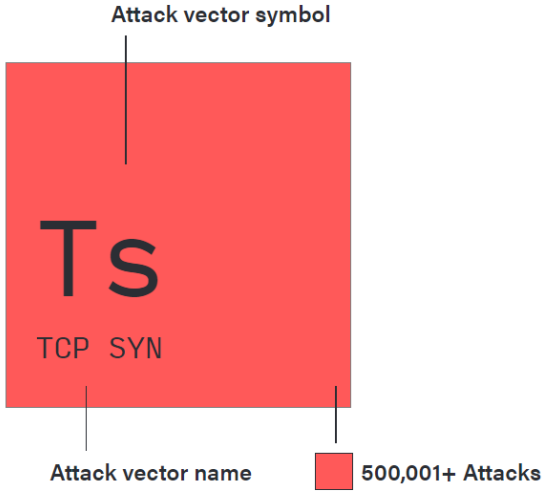
https://www.netscout.com/threatreport/ddos-attack-vectors/

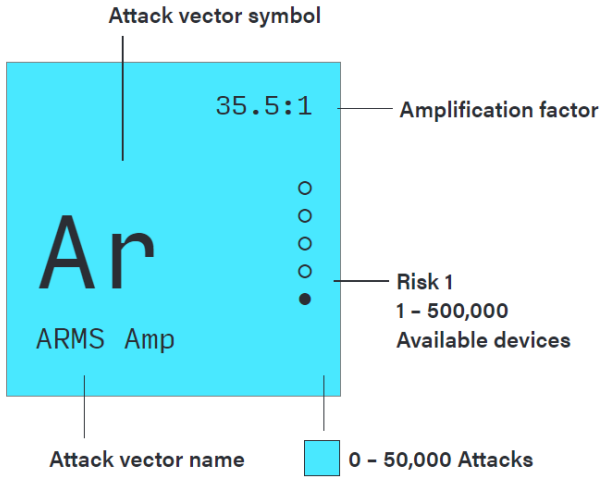
(TT)PROCEDURE FOCUS



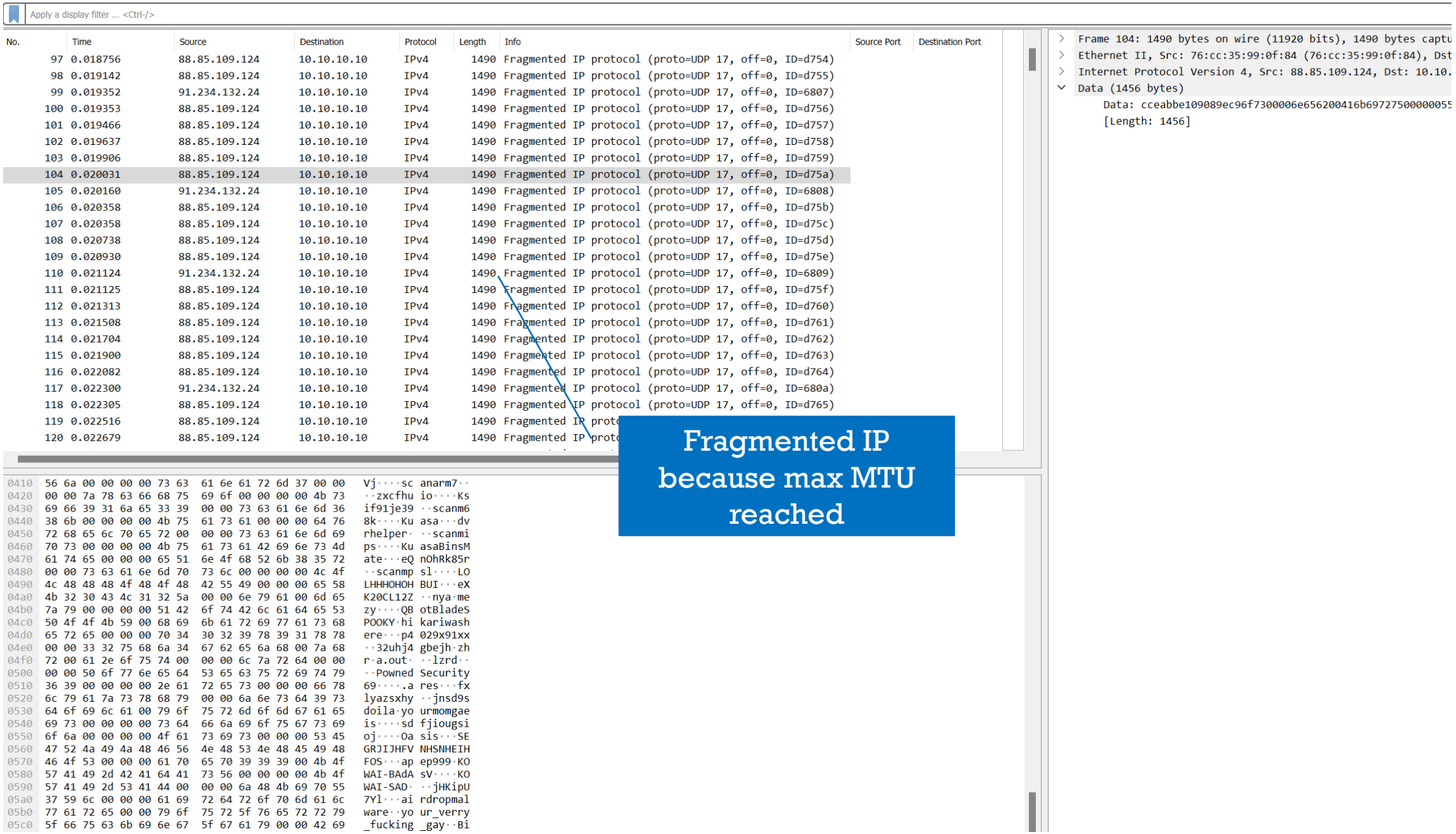








https://www.netscout.com/threatreport/ddos-attack-vectors/


Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info Source Port Destination Port
97 0.018756 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d754)
98 0.019142 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d755)
99 0.019352 91.234.132.24 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=6807)
100 0.019353 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d756)
101 0.019466 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d757)
102 0.019637 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d758)
103 0.019906 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d759)
104 0.020031 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d75a)
105 0.020160 91.234.132.24 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=6808)
106 0.020358 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d75b)
107 0.020358 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d75c)
108 0.020738 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d75d)
109 0.020930 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d75e)
110 0.021124 91.234.132.24 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=6809)
111 0.021125 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d75f)
112 0.021313 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d760)
113 0.021508 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d761)
114 0.021704 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d762)
115 0.021900 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d763)
116 0.022082 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d764)
117 0.022300 91.234.132.24 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=680a)
118 0.022305 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d765)
119 0.022516 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP
120 0.022679 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP
Frame 104: 1490 bytes on wire (11920 bits), 1490 bytes captu
Ethernet II, Src: 76:cc:35:99:0f:84 (76:cc:35:99:0f:84), Dst
Internet Protocol Version 4, Src: 88.85.109.124, Dst: 10.10.
Data (1456 bytes)
Data: cceabbe109089ec96f7300006e656200416b69727500000055
[Length: 1456]
0410 56 6a 00 00 00 00 73 63 61 6e 61 72 6d 37 00 00 Vj····sc anarm7··
0420 00 00 7a 78 63 66 68 75 69 6f 00 00 00 00 4b 73 ··zxcfhu io····Ks
0430 69 66 39 31 6a 65 33 39 00 00 73 63 61 6e 6d 36 if91je39 ··scanm6
0440 38 6b 00 00 00 00 4b 75 61 73 61 00 00 00 64 76 8k····Ku asa···dv
0450 72 68 65 6c 70 65 72 00 00 00 73 63 61 6e 6d 69 rhelper· ··scanmi
0460 70 73 00 00 00 00 4b 75 61 73 61 42 69 6e 73 4d ps····Ku asaBinsM
0470 61 74 65 00 00 00 65 51 6e 4f 68 52 6b 38 35 72 ate···eQ nOhRk85r
0480 00 00 73 63 61 6e 6d 70 73 6c 00 00 00 00 4c 4f ··scanmp sl····LO
0490 4c 48 48 48 4f 48 4f 48 42 55 49 00 00 00 65 58 LHHHOHOH BUI···eX
04a0 4b 32 30 43 4c 31 32 5a 00 00 6e 79 61 00 6d 65 K20CL12Z ··nya·me
04b0 7a 79 00 00 00 00 51 42 6f 74 42 6c 61 64 65 53 zy····QB otBladeS
04c0 50 4f 4f 4b 59 00 68 69 6b 61 72 69 77 61 73 68 POOKY·hi kariwash
04d0 65 72 65 00 00 00 70 34 30 32 39 78 39 31 78 78 ere···p4 029x91xx
04e0 00 00 33 32 75 68 6a 34 67 62 65 6a 68 00 7a 68 ··32uhj4 gbejh·zh
04f0 72 00 61 2e 6f 75 74 00 00 00 6c 7a 72 64 00 00 r·a.out· ··lzrd··
0500 00 00 50 6f 77 6e 65 64 53 65 63 75 72 69 74 79 ··Powned Security
0510 36 39 00 00 00 00 2e 61 72 65 73 00 00 00 66 78 69····.a res···fx
0520 6c 79 61 7a 73 78 68 79 00 00 6a 6e 73 64 39 73 lyazsxhy ··jnsd9s
0530 64 6f 69 6c 61 00 79 6f 75 72 6d 6f 6d 67 61 65 doila·yo urmomgae
0540 69 73 00 00 00 00 73 64 66 6a 69 6f 75 67 73 69 is····sd fjiougsi
0550 6f 6a 00 00 00 00 4f 61 73 69 73 00 00 00 53 45 oj····Oa sis···SE
0560 47 52 4a 49 4a 48 46 56 4e 48 53 4e 48 45 49 48 GRJIJHFV NHSNHEIH
0570 46 4f 53 00 00 00 61 70 65 70 39 39 39 00 4b 4f FOS···ap ep999·KO
0580 57 41 49 2d 42 41 64 41 73 56 00 00 00 00 4b 4f WAI-BAdA sV····KO
0590 57 41 49 2d 53 41 44 00 00 00 6a 48 4b 69 70 55 WAI-SAD· ··jHKipU
05a0 37 59 6c 00 00 00 61 69 72 64 72 6f 70 6d 61 6c 7Yl···ai rdropmal
05b0 77 61 72 65 00 00 79 6f 75 72 5f 76 65 72 72 79 ware··yo ur_verry
05c0 5f 66 75 63 6b 69 6e 67 5f 67 61 79 00 00 42 69 _fucking _gay··Bi
Fragmented IP because max MTU reached

Apply a display filter ... <Ctrl-/>

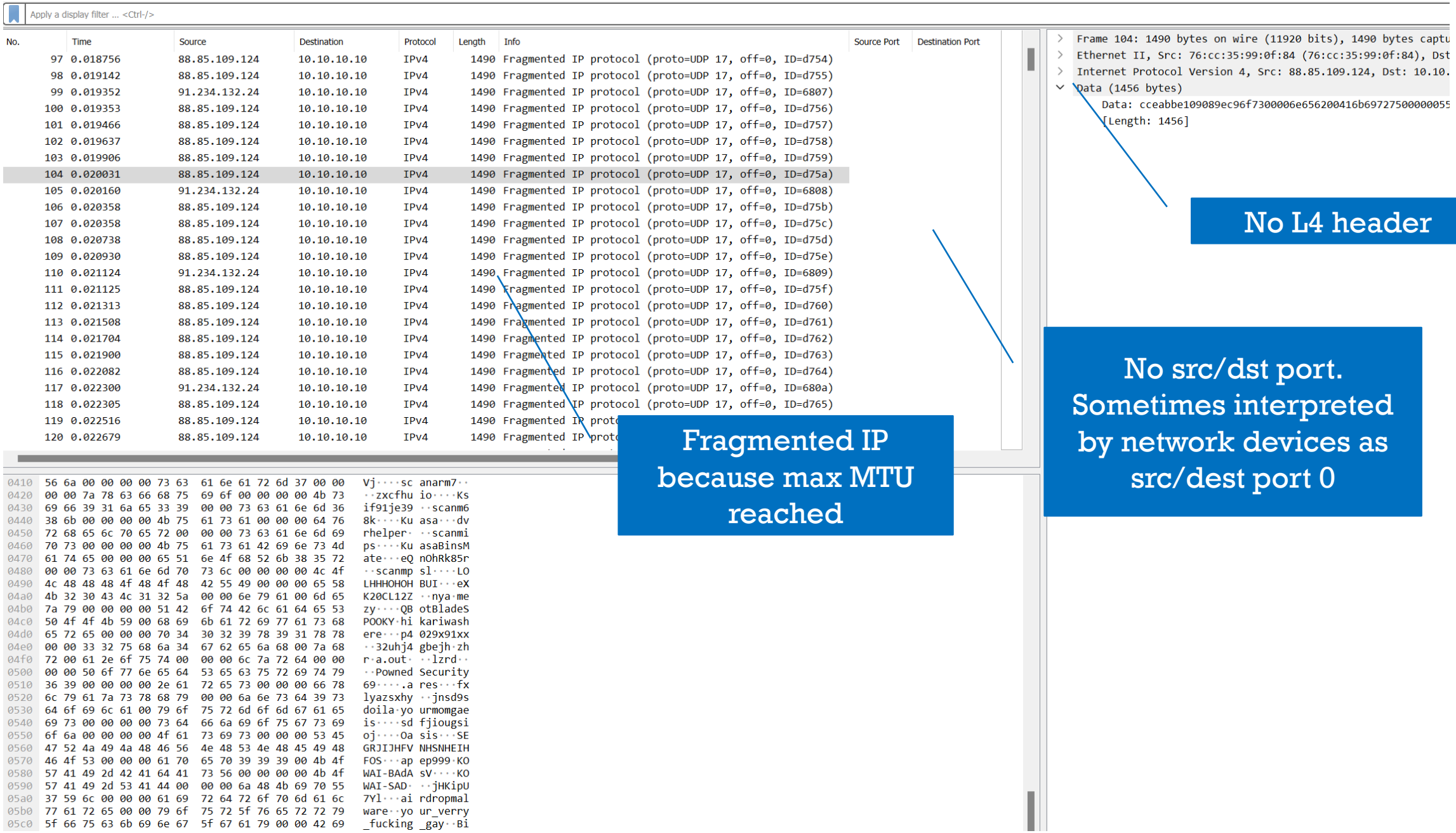
No.	Time	Source	Destination	Protocol	Length	Info	Source Port	Destination Port
97	0.018756	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d754)		
98	0.019142	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d755)		
99	0.019352	91.234.132.24	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=6807)		
100	0.019353	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d756)		
101	0.019466	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d757)		
102	0.019637	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d758)		
103	0.019906	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d759)		
104	0.020031	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d75a)		
105	0.020160	91.234.132.24	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=6808)		
106	0.020358	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d75b)		
107	0.020358	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d75c)		
108	0.020738	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d75d)		
109	0.020930	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d75e)		
110	0.021124	91.234.132.24	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=6809)		
111	0.021125	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d75f)		
112	0.021313	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d760)		
113	0.021508	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d761)		
114	0.021704	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d762)		
115	0.021900	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d763)		
116	0.022082	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d764)		
117	0.022300	91.234.132.24	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=680a)		
118	0.022305	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d765)		
119	0.022516	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP proto		
120	0.022679	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP proto		

```
0410  56 6a 00 00 00 00 73 63  61 6e 61 72 6d 37 00 00   Vj····sc anarm7··
0420  00 00 7a 78 63 66 68 75  69 6f 00 00 00 00 4b 73   ··zxcfhu io····Ks
0430  69 66 39 31 6a 65 33 39  00 00 73 63 61 6e 6d 36   if91je39 ··scanm6
0440  38 6b 00 00 00 00 4b 75  61 73 61 00 00 00 64 76   8k····Ku asa···dv
0450  72 68 65 6c 70 65 72 00  00 00 73 63 61 6e 6d 69   rhelper· ··scanmi
0460  70 73 00 00 00 00 4b 75  61 73 61 42 69 6e 73 4d   ps····Ku asaBinsM
0470  61 74 65 00 00 00 65 51  6e 4f 68 52 6b 38 35 72   ate···eQ nOhRk85r
0480  00 00 73 63 61 6e 6d 70  73 6c 00 00 00 00 4c 4f   ··scanmp sl····LO
0490  4c 48 48 48 4f 48 4f 48  42 55 49 00 00 00 65 58   LHHHOHOH BUI···eX
04a0  4b 32 30 43 4c 31 32 5a  00 00 6e 79 61 00 6d 65   K20CL12Z ··nya·me
04b0  7a 79 00 00 00 00 51 42  6f 74 42 6c 61 64 65 53   zy····QB otBladeS
04c0  50 4f 4f 4b 59 00 68 69  6b 61 72 69 77 61 73 68   POOKY·hi kariwash
04d0  65 72 65 00 00 00 70 34  30 32 39 78 39 31 78 78   ere···p4 029x91xx
04e0  00 00 33 32 75 68 6a 34  67 62 65 6a 68 00 7a 68   ··32uhj4 gbejh·zh
04f0  72 00 61 2e 6f 75 74 00  00 00 6c 7a 72 64 00 00   r·a.out· ··lzrd··
0500  00 00 50 6f 77 6e 65 64  53 65 63 75 72 69 74 79   ··Powned Security
0510  36 39 00 00 00 00 2e 61  72 65 73 00 00 00 66 78   69····.a res···fx
0520  6c 79 61 7a 73 78 68 79  00 00 6a 6e 73 64 39 73   lyazsxhy ··jnsd9s
0530  64 6f 69 6c 61 00 79 6f  75 72 6d 6f 6d 67 61 65   doila·yo urmomgae
0540  69 73 00 00 00 00 73 64  66 6a 69 6f 75 67 73 69   is····sd fjiougsi
0550  6f 6a 00 00 00 00 4f 61  73 69 73 00 00 00 53 45   oj····Oa sis···SE
0560  47 52 4a 49 4a 48 46 56  4e 48 53 4e 48 45 49 48   GRJIJHFV NHSNHEIH
0570  46 4f 53 00 00 00 61 70  65 70 39 39 39 00 4b 4f   FOS···ap ep999·KO
0580  57 41 49 2d 42 41 64 41  73 56 00 00 00 00 4b 4f   WAI-BAdA sV····KO
0590  57 41 49 2d 53 41 44 00  00 00 6a 48 4b 69 70 55   WAI-SAD· ··jHKipU
05a0  37 59 6c 00 00 00 61 69  72 64 72 6f 70 6d 61 6c   7Yl···ai rdropmal
05b0  77 61 72 65 00 00 79 6f  75 72 5f 76 65 72 72 79   ware··yo ur_verry
05c0  5f 66 75 63 6b 69 6e 67  5f 67 61 79 00 00 42 69   _fucking _gay··Bi
```

```
> Frame 104: 1490 bytes on wire (11920 bits), 1490 bytes captu
> Ethernet II, Src: 76:cc:35:99:0f:84 (76:cc:35:99:0f:84), Dst
> Internet Protocol Version 4, Src: 88.85.109.124, Dst: 10.10.
v Data (1456 bytes)
    Data: cceabbe109089ec96f7300006e656200416b69727500000055
    [Length: 1456]
```

Fragmented IP because max MTU reached

No src/dst port. Sometimes interpreted by network devices as src/dest port 0


Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info Source Port Destination Port
97 0.018756 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d754)
98 0.019142 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d755)
99 0.019352 91.234.132.24 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=6807)
100 0.019353 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d756)
101 0.019466 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d757)
102 0.019637 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d758)
103 0.019906 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d759)
104 0.020031 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d75a)
105 0.020160 91.234.132.24 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=6808)
106 0.020358 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d75b)
107 0.020358 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d75c)
108 0.020738 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d75d)
109 0.020930 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d75e)
110 0.021124 91.234.132.24 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=6809)
111 0.021125 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d75f)
112 0.021313 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d760)
113 0.021508 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d761)
114 0.021704 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d762)
115 0.021900 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d763)
116 0.022082 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d764)
117 0.022300 91.234.132.24 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=680a)
118 0.022305 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP protocol (proto=UDP 17, off=0, ID=d765)
119 0.022516 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP
120 0.022679 88.85.109.124 10.10.10.10 IPv4 1490 Fragmented IP
Frame 104: 1490 bytes on wire (11920 bits), 1490 bytes captu
Ethernet II, Src: 76:cc:35:99:0f:84 (76:cc:35:99:0f:84), Dst
Internet Protocol Version 4, Src: 88.85.109.124, Dst: 10.10.
Data (1456 bytes)
Data: cceabbe109089ec96f7300006e656200416b69727500000055
[Length: 1456]
0410 56 6a 00 00 00 00 73 63 61 6e 61 72 6d 37 00 00 Vj····sc anarm7··
0420 00 00 7a 78 63 66 68 75 69 6f 00 00 00 00 4b 73 ··zxcfhu io····Ks
0430 69 66 39 31 6a 65 33 39 00 00 73 63 61 6e 6d 36 if91je39 ··scanm6
0440 38 6b 00 00 00 00 4b 75 61 73 61 00 00 00 64 76 8k····Ku asa···dv
0450 72 68 65 6c 70 65 72 00 00 00 73 63 61 6e 6d 69 rhelper· ··scanmi
0460 70 73 00 00 00 00 4b 75 61 73 61 42 69 6e 73 4d ps····Ku asaBinsM
0470 61 74 65 00 00 00 65 51 6e 4f 68 52 6b 38 35 72 ate···eQ nOhRk85r
0480 00 00 73 63 61 6e 6d 70 73 6c 00 00 00 00 4c 4f ··scanmp sl····LO
0490 4c 48 48 48 4f 48 4f 48 42 55 49 00 00 00 65 58 LHHHOHOH BUI···eX
04a0 4b 32 30 43 4c 31 32 5a 00 00 6e 79 61 00 6d 65 K20CL12Z ··nya·me
04b0 7a 79 00 00 00 00 51 42 6f 74 42 6c 61 64 65 53 zy····QB otBladeS
04c0 50 4f 4f 4b 59 00 68 69 6b 61 72 69 77 61 73 68 POOKY·hi kariwash
04d0 65 72 65 00 00 00 70 34 30 32 39 78 39 31 78 78 ere···p4 029x91xx
04e0 00 00 33 32 75 68 6a 34 67 62 65 6a 68 00 7a 68 ··32uhj4 gbejh·zh
04f0 72 00 61 2e 6f 75 74 00 00 00 6c 7a 72 64 00 00 r·a.out· ··lzrd··
0500 00 00 50 6f 77 6e 65 64 53 65 63 75 72 69 74 79 ··Powned Security
0510 36 39 00 00 00 00 2e 61 72 65 73 00 00 00 66 78 69····.a res···fx
0520 6c 79 61 7a 73 78 68 79 00 00 6a 6e 73 64 39 73 lyazsxhy ··jnsd9s
0530 64 6f 69 6c 61 00 79 6f 75 72 6d 6f 6d 67 61 65 doila·yo urmomgae
0540 69 73 00 00 00 00 73 64 66 6a 69 6f 75 67 73 69 is····sd fjiougsi
0550 6f 6a 00 00 00 00 4f 61 73 69 73 00 00 00 53 45 oj····Oa sis···SE
0560 47 52 4a 49 4a 48 46 56 4e 48 53 4e 48 45 49 48 GRJIJHFV NHSNHEIH
0570 46 4f 53 00 00 00 61 70 65 70 39 39 39 00 4b 4f FOS···ap ep999·KO
0580 57 41 49 2d 42 41 64 41 73 56 00 00 00 00 4b 4f WAI-BAdA sV····KO
0590 57 41 49 2d 53 41 44 00 00 00 6a 48 4b 69 70 55 WAI-SAD· ··jHKipU
05a0 37 59 6c 00 00 00 61 69 72 64 72 6f 70 6d 61 6c 7Yl···ai rdropmal
05b0 77 61 72 65 00 00 79 6f 75 72 5f 76 65 72 72 79 ware··yo ur_verry
05c0 5f 66 75 63 6b 69 6e 67 5f 67 61 79 00 00 42 69 _fucking _gay··Bi
No L4 header
Fragmented IP because max MTU reached
No src/dst port. Sometimes interpreted by network devices as src/dest port 0

Apply a display filter ... <Ctrl-/>

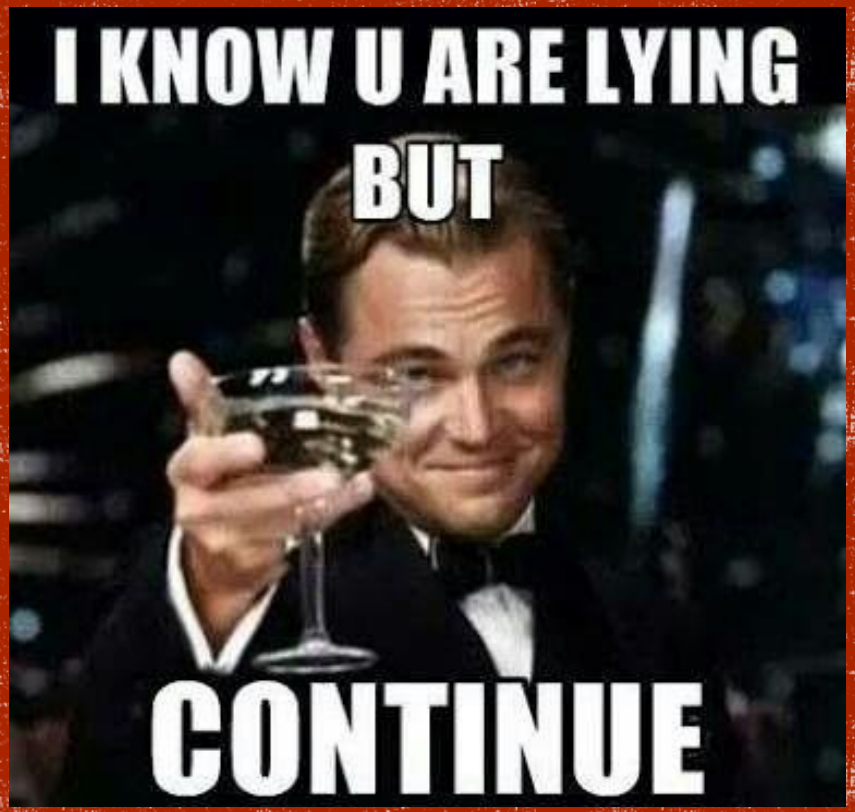
No.	Time	Source	Destination	Protocol	Length	Info	Source Port	Destination Port
97	0.018756	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d754)		
98	0.019142	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d755)		
99	0.019352	91.234.132.24	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=6807)		
100	0.019353	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d756)		
101	0.019466	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d757)		
102	0.019637	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d758)		
103	0.019906	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d759)		
104	0.020031	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d75a)		
105	0.020160	91.234.132.24	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=6808)		
106	0.020358	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d75b)		
107	0.020358	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d75c)		
108	0.020738	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d75d)		
109	0.020930	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d75e)		
110	0.021124	91.234.132.24	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=6809)		
111	0.021125	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d75f)		
112	0.021313	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d760)		
113	0.021508	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d761)		
114	0.021704	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d762)		
115	0.021900	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d763)		
116	0.022082	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d764)		
117	0.022300	91.234.132.24	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=680a)		
118	0.022305	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d765)		
119	0.022516	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d766)		
120	0.022679	88.85.109.124	10.10.10.10	IPv4	1490	Fragmented IP protocol (proto=UDP 17, off=0, ID=d767)		

```
0410  56 6a 00 00 00 00 73 63  61 6e 61 72 6d 37 00 00   Vj····sc anarm7··
0420  00 00 7a 78 63 66 68 75  69 6f 00 00 00 00 4b 73   ··zxcfhu io····Ks
0430  69 66 39 31 6a 65 33 39  00 00 73 63 61 6e 6d 36   if91je39 ··scanm6
0440  38 6b 00 00 00 00 4b 75  61 73 61 00 00 00 64 76   8k····Ku asa···dv
0450  72 68 65 6c 70 65 72 00  00 00 73 63 61 6e 6d 69   rhelper· ··scanmi
0460  70 73 00 00 00 00 4b 75  61 73 61 42 69 6e 73 4d   ps····Ku asaBinsM
0470  61 74 65 00 00 00 65 51  6e 4f 68 52 6b 38 35 72   ate···eQ nOhRk85r
0480  00 00 73 63 61 6e 6d 70  73 6c 00 00 00 00 4c 4f   ··scanmp sl····LO
0490  4c 48 48 48 4f 48 4f 48  42 55 49 00 00 00 65 58   LHHHOHOH BUI···eX
04a0  4b 32 30 43 4c 31 32 5a  00 00 6e 79 61 00 6d 65   K20CL12Z ··nya·me
04b0  7a 79 00 00 00 00 51 42  6f 74 42 6c 61 64 65 53   zy····QB otBladeS
04c0  50 4f 4f 4b 59 00 68 69  6b 61 72 69 77 61 73 68   POOKY·hi kariwash
04d0  65 72 65 00 00 00 70 34  30 32 39 78 39 31 78 78   ere···p4 029x91xx
04e0  00 00 33 32 75 68 6a 34  67 62 65 6a 68 00 7a 68   ··32uhj4 gbejh·zh
04f0  72 00 61 2e 6f 75 74 00  00 00 6c 7a 72 64 00 00   r·a.out· ··lzrd··
0500  00 00 50 6f 77 6e 65 64  53 65 63 75 72 69 74 79   ··Powned Security
0510  36 39 00 00 00 00 2e 61  72 65 73 00 00 00 66 78   69····.a res···fx
0520  6c 79 61 7a 73 78 68 79  00 00 6a 6e 73 64 39 73   lyazsxhy ··jnsd9s
0530  64 6f 69 6c 61 00 79 6f  75 72 6d 6f 6d 67 61 65   doila·yo urmomgae
0540  69 73 00 00 00 00 73 64  66 6a 69 6f 75 67 73 69   is····sd fjiougsi
0550  6f 6a 00 00 00 00 4f 61  73 69 73 00 00 00 53 45   oj····Oa sis···SE
0560  47 52 4a 49 4a 48 46 56  4e 48 53 4e 48 45 49 48   GRJIJHFV NHSNHEIH
0570  46 4f 53 00 00 00 61 70  65 70 39 39 39 00 4b 4f   FOS···ap ep999·KO
0580  57 41 49 2d 42 41 64 41  73 56 00 00 00 00 4b 4f   WAI-BAdA sV····KO
0590  57 41 49 2d 53 41 44 00  00 00 6a 48 4b 69 70 55   WAI-SAD· ··jHKipU
05a0  37 59 6c 00 00 00 61 69  72 64 72 6f 70 6d 61 6c   7Yl···ai rdropmal
05b0  77 61 72 65 00 00 79 6f  75 72 5f 76 65 72 72 79   ware··yo ur_verry
05c0  5f 66 75 63 6b 69 6e 67  5f 67 61 79 00 00 42 69   _fucking _gay··Bi
```

When you see it…

```
> Frame 104: 1490 bytes on wire (11920 bits), 1490 bytes captu
> Ethernet II, Src: 76:cc:35:99:0f:84 (76:cc:35:99:0f:84), Dst
> Internet Protocol Version 4, Src: 88.85.109.124, Dst: 10.10.
v Data (1456 bytes)
      Data: cceabbe109089ec96f7300006e656200416b69727500000055
      [Length: 1456]
```

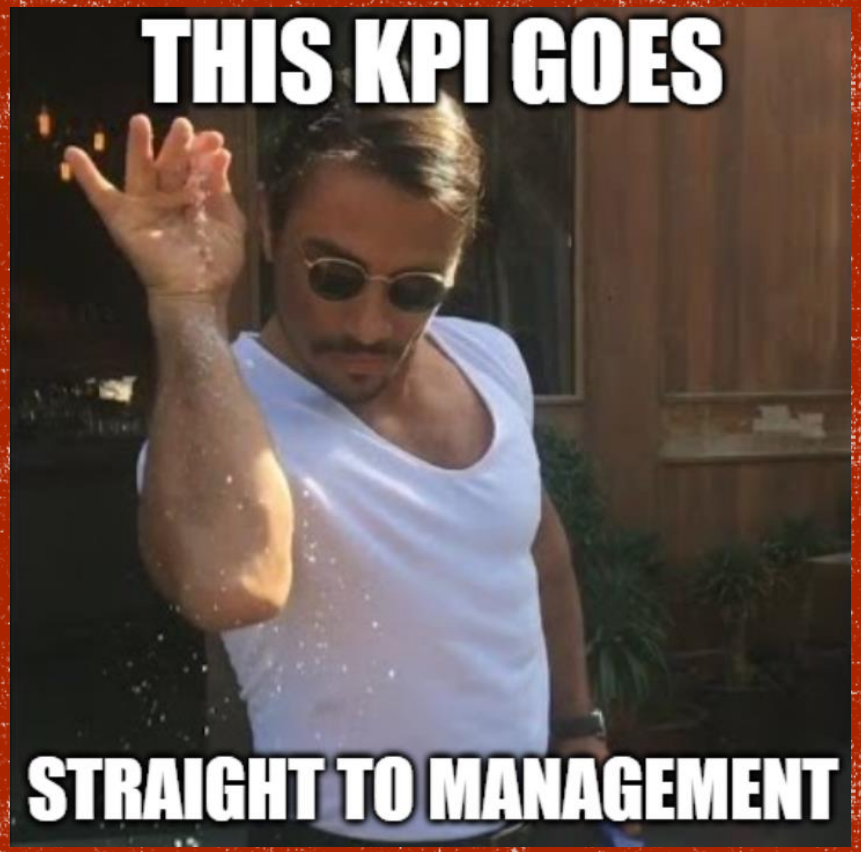
SOME FACTS…



1. Attack lasted 3 hours and they never conducted the follow-up attack as promised 1 week later

1. Attack lasted 3 hours and they never conducted the follow-up attack as promised 1 week later

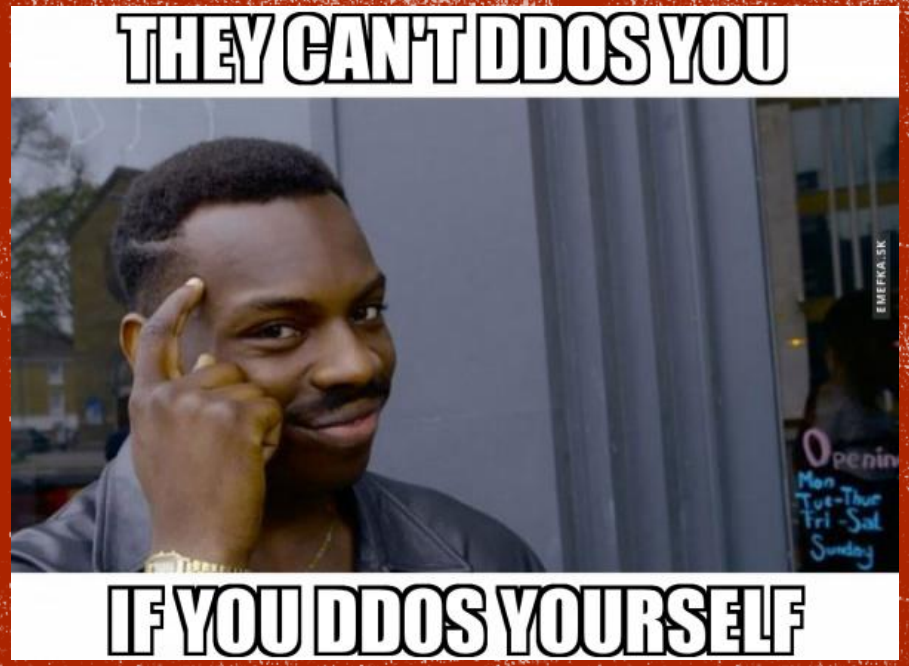
2. Ransom email was identified during incident in quarantine



1. Attack lasted 3 hours and they never conducted the follow-up attack as promised 1 week later

2. Ransom email was identified during incident in quarantine

3. MTTD: Extremely good

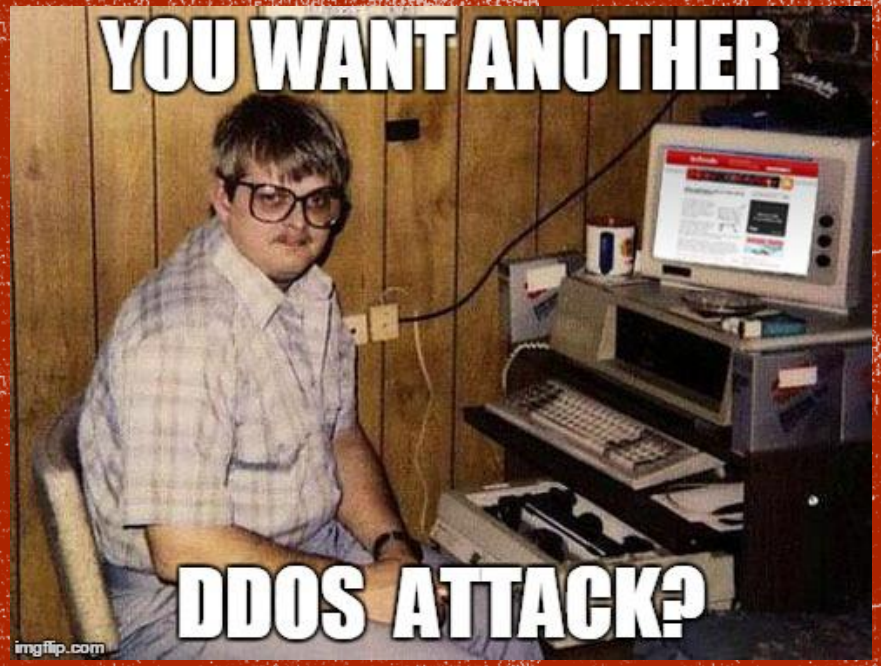


1. Attack lasted 3 hours and they never conducted the follow-up attack as promised 1 week later

2. Ransom email was identified during incident in quarantine

3. MTTD: Extremely good

4. ISPs blocked us because attacker scanned networks with spoofed IP



1. Attack lasted 3 hours and they never conducted the follow-up attack as promised 1 week later

2. Ransom email was identified during incident in quarantine

3. MTTD: Extremely good

4. ISPs blocked us because attacker scanned networks with spoofed IP

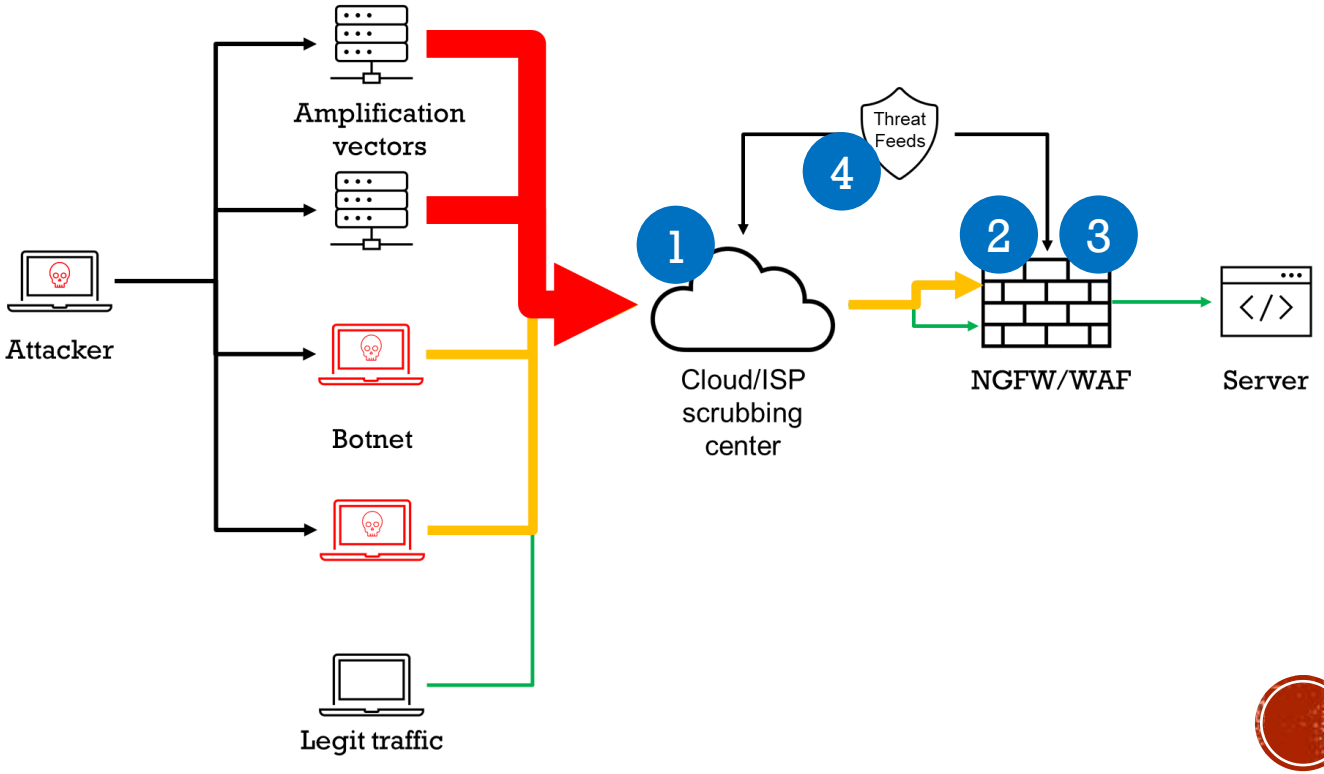
5. Attackers came back several months later:

   "Hey you didn't pay last time? we didn't forget about you"

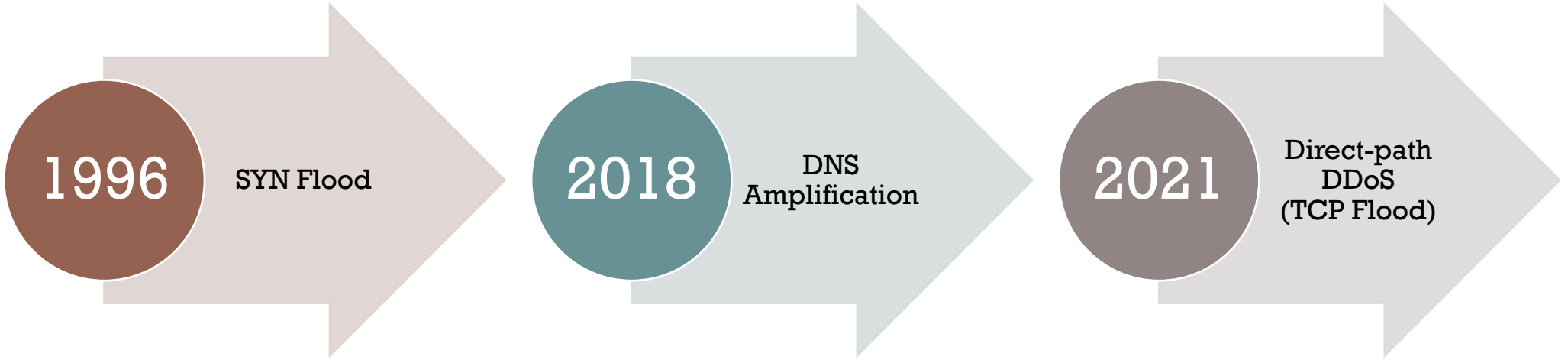
MITIGATIONS, LESSONS LEARNED

DDoS defense is layered/hybrid

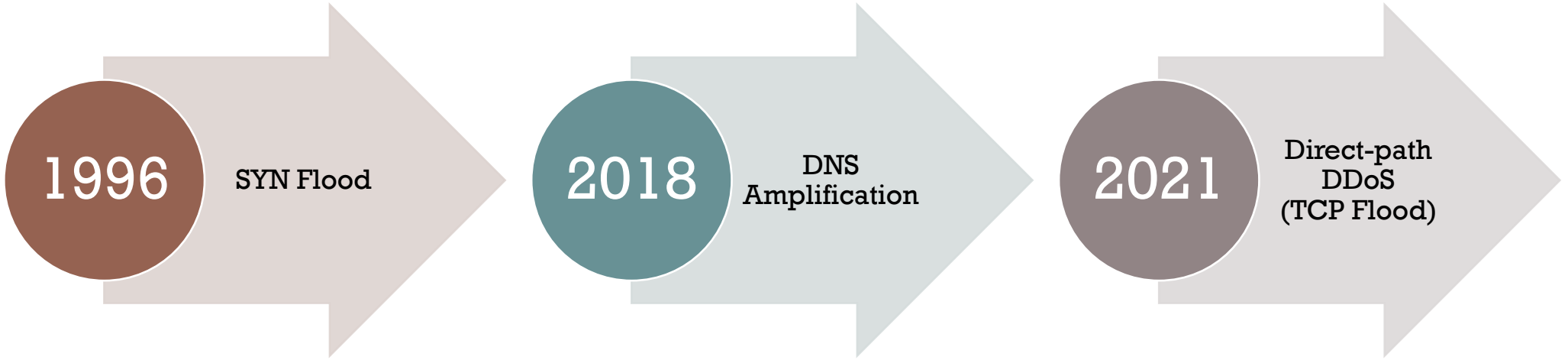
1. Volumetric
   - Scrubbing centers
2. Protocol
   - Your NGFW: SYN cookie, rate limiting, etc.
3. Application
   - Your WAF: Captcha, real-browser JS, etc.
4. Threat Feeds
   - Botnets, IPs, signatures, etc.
5. Automated response (threshold)
   - Works well if fine tuned to your environment



TRENDS

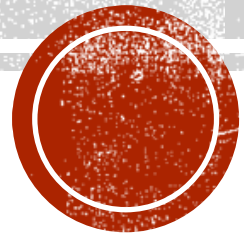

1996
SYN Flood
2018
DNS Amplification
2021
Direct-path DDoS (TCP Flood)

TRENDS

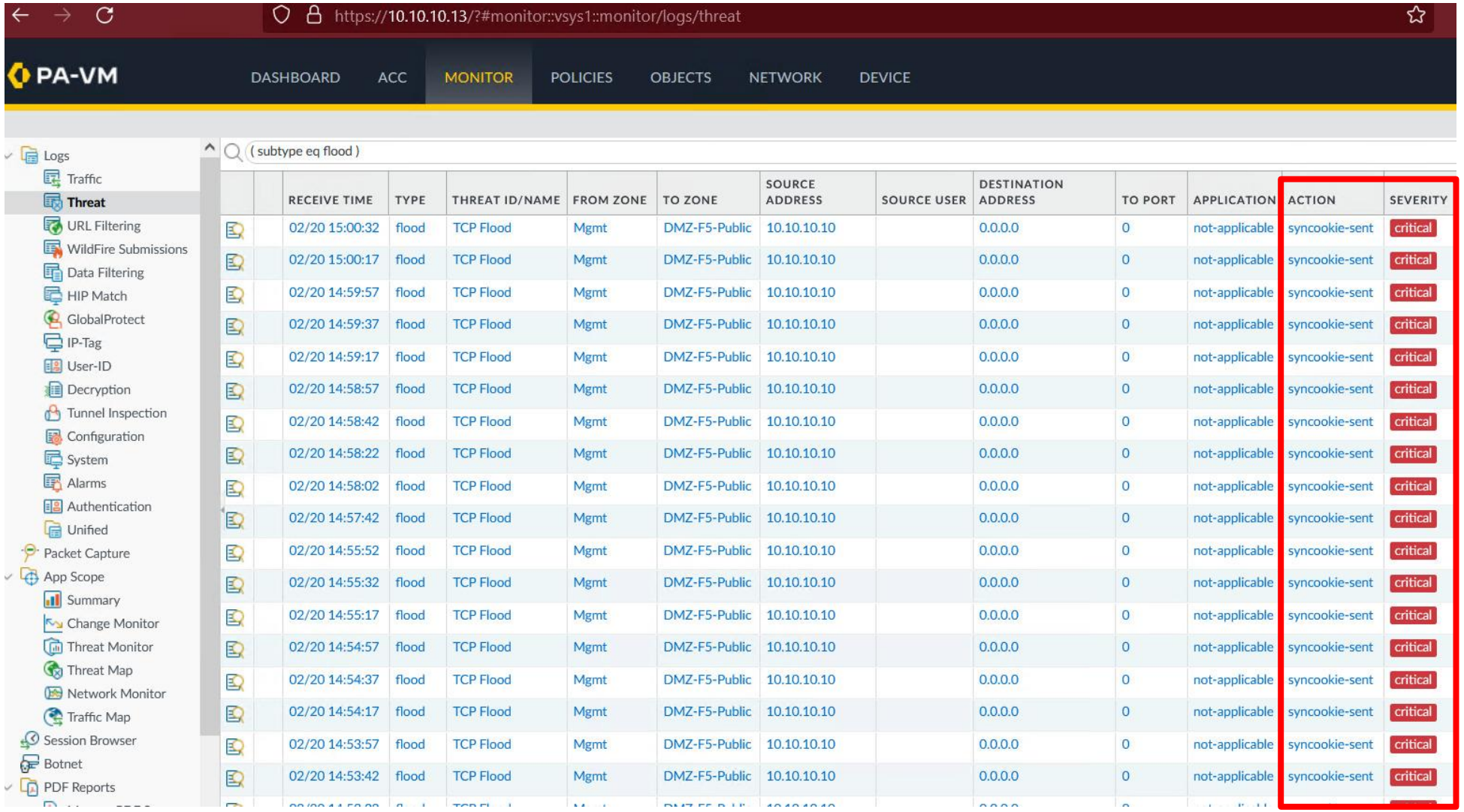


- Direct-path DDoS (TCP Flood) trendy again, but why?
  - Trends in botnet (Mirai, Killnet, Meris, ZeroBot, etc.)
  - Anti-spoofing mitigation (SAV aka Source-Address Validation, BCP38/RFC2827)

THANK YOU



MITIGATION: SYN COOKIE



RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION	SEVERITY
02/20 15:00:32	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 15:00:17	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:59:57	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:59:37	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:59:17	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:58:57	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:58:42	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:58:22	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:58:02	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:57:42	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:55:52	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:55:32	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:55:17	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:54:57	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:54:37	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:54:17	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:53:57	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical
02/20 14:53:42	flood	TCP Flood	Mgmt	DMZ-F5-Public	10.10.10.10		0.0.0.0	0	not-applicable	syncookie-sent	critical