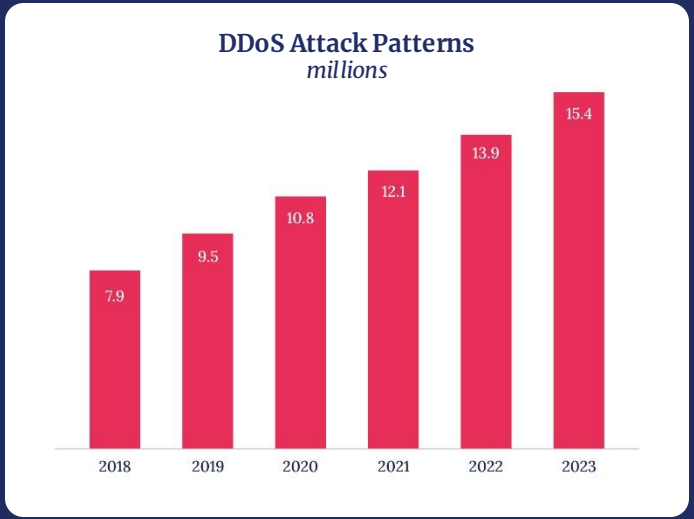
Network Infrastructure Attacks

Simon Kuhn
Head of engineering
NaWas

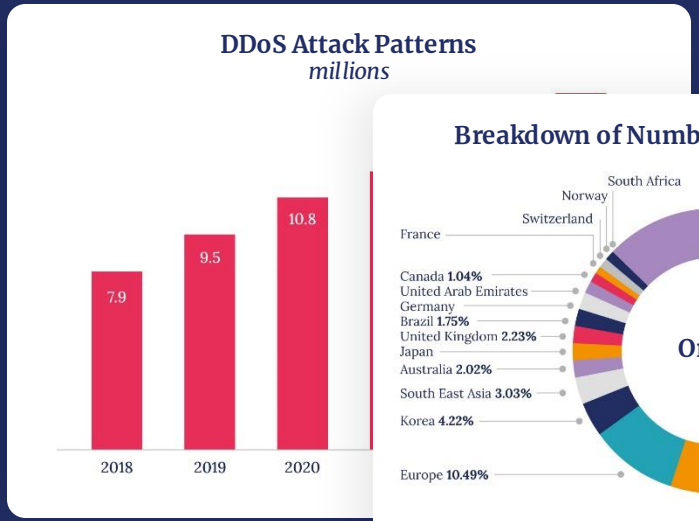
www.nbip.nl/nawas

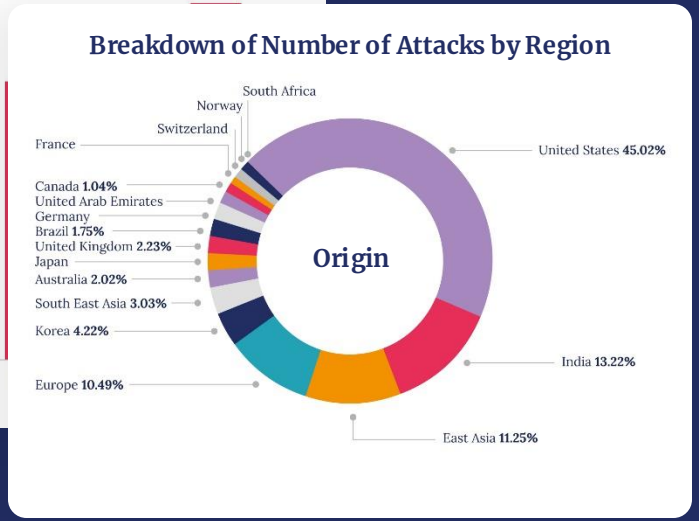
Fun Facts about DDoS



NBIP nationale beheersorganisatie internet providers

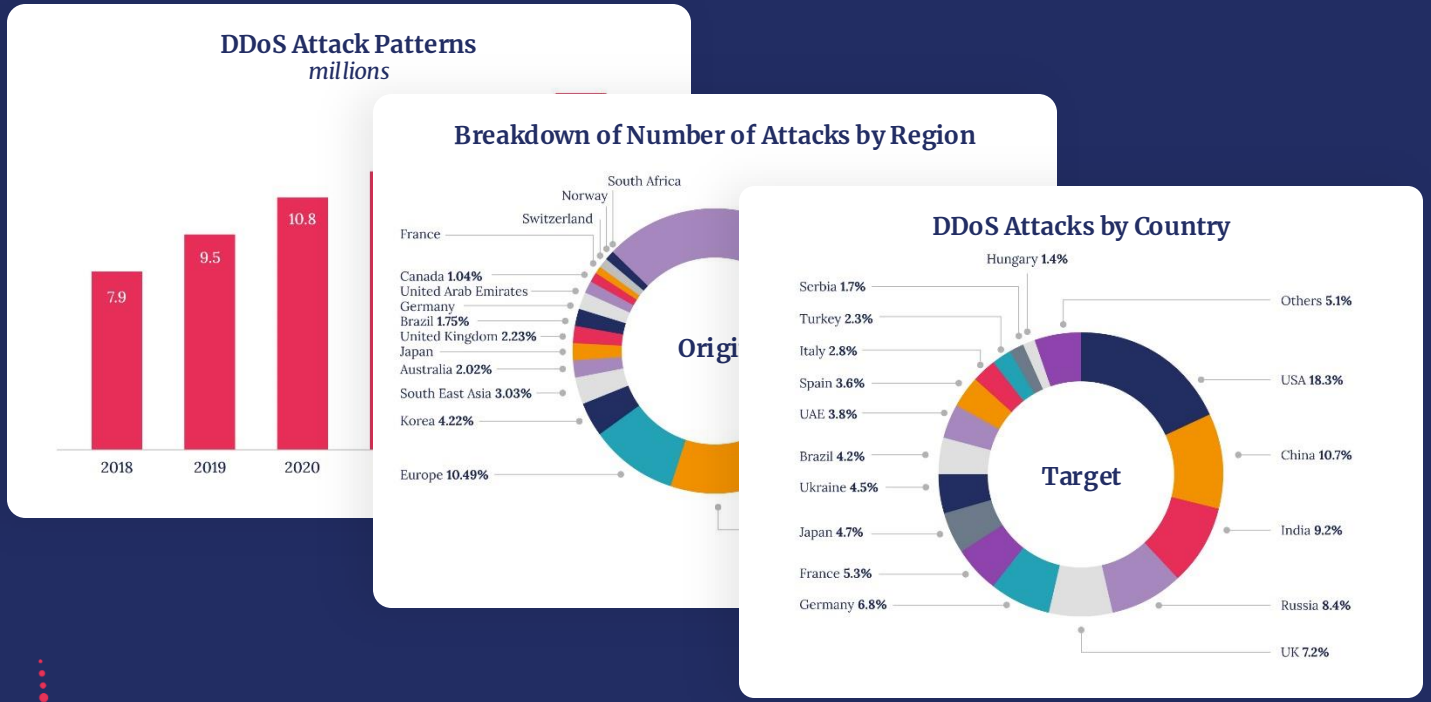
Fun Facts about DDoS





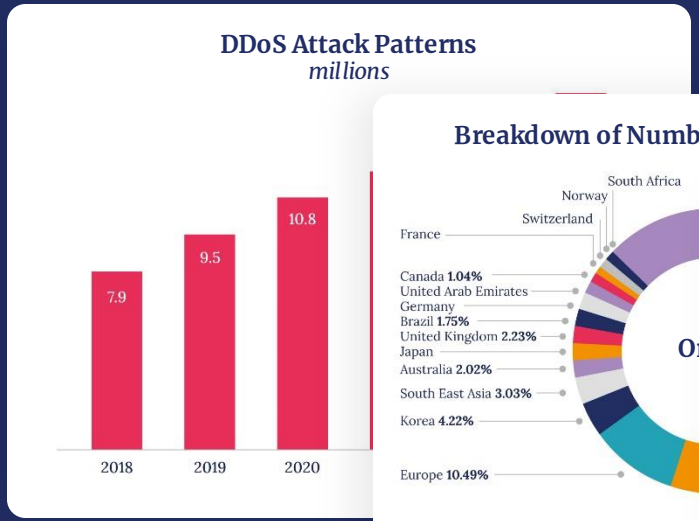
NBIP nationale beheersorganisatie internet providers

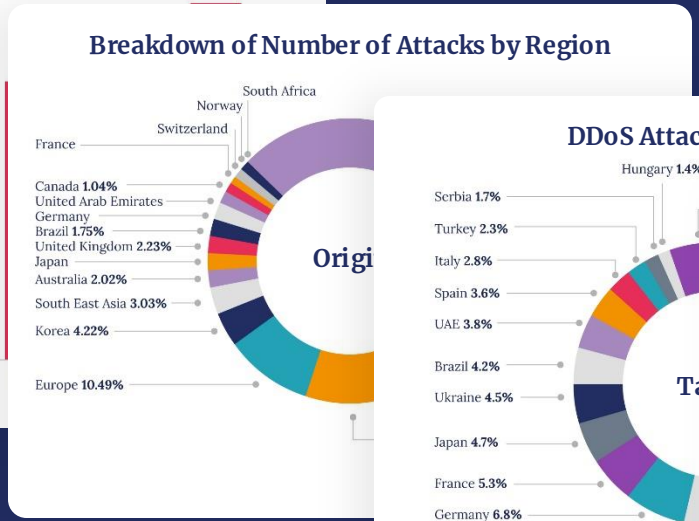
Fun Facts about DDoS

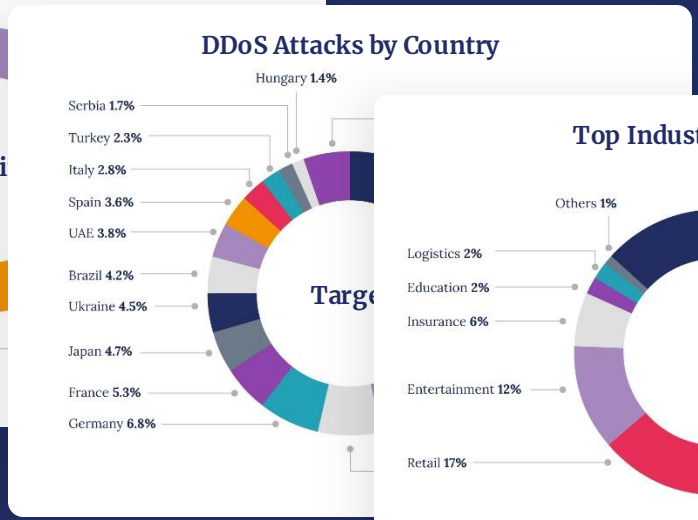


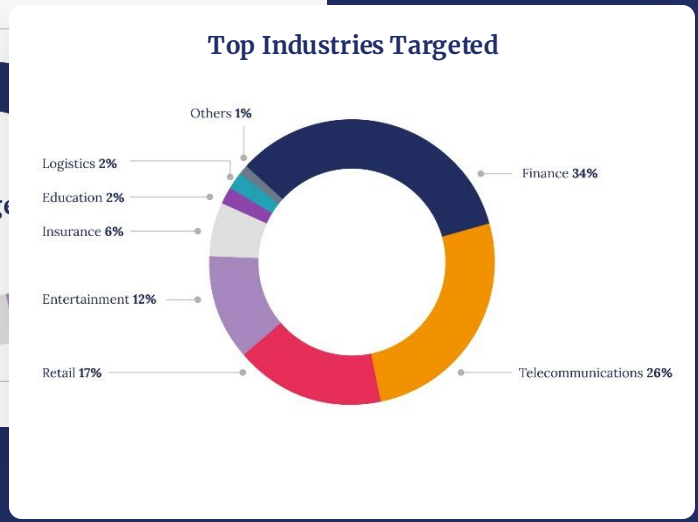
NBIP nationale beheersorganisatie internet providers

Fun Facts about DDoS



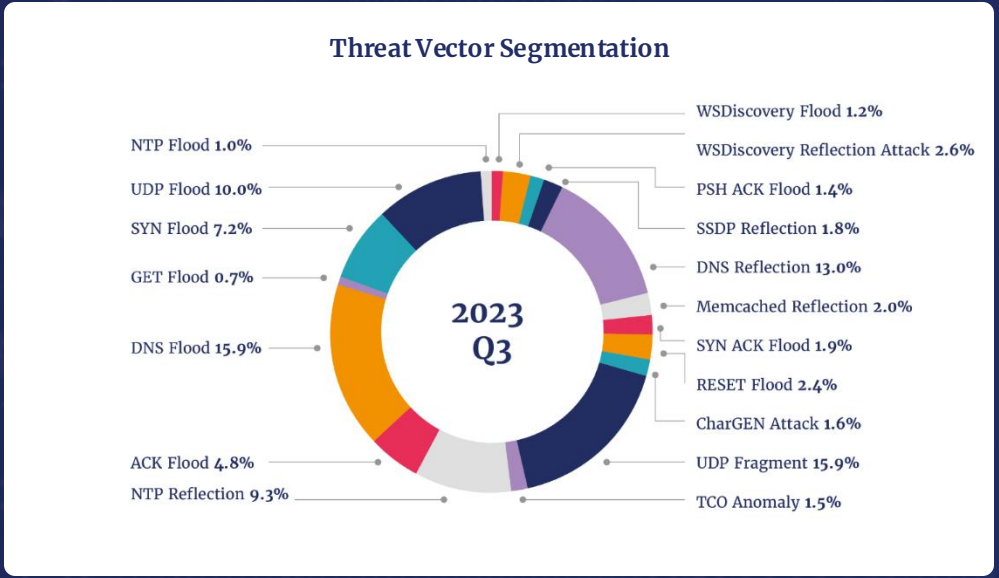






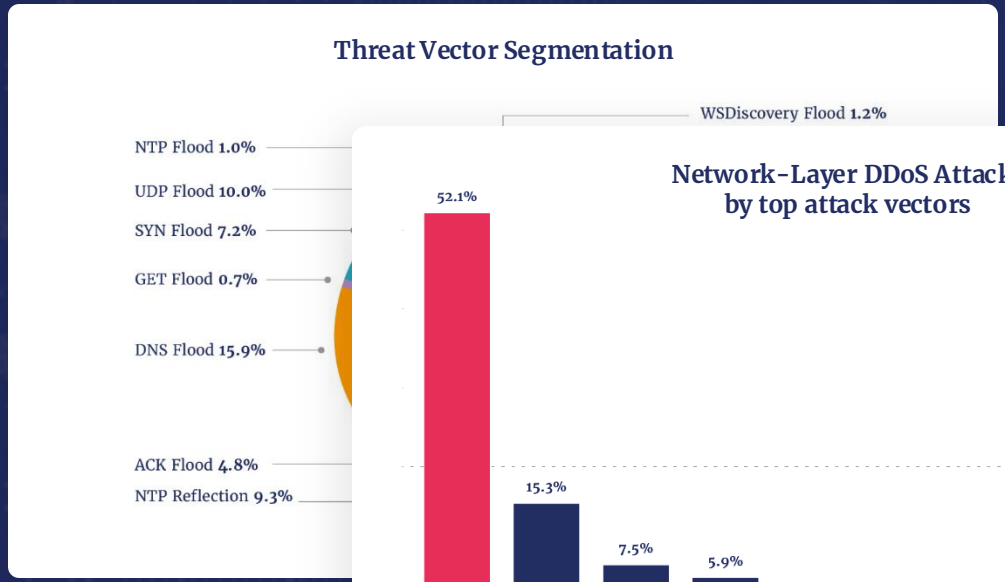
NBIP nationale beheersorganisatie internet providers

DDoS Reporting – most common vectors



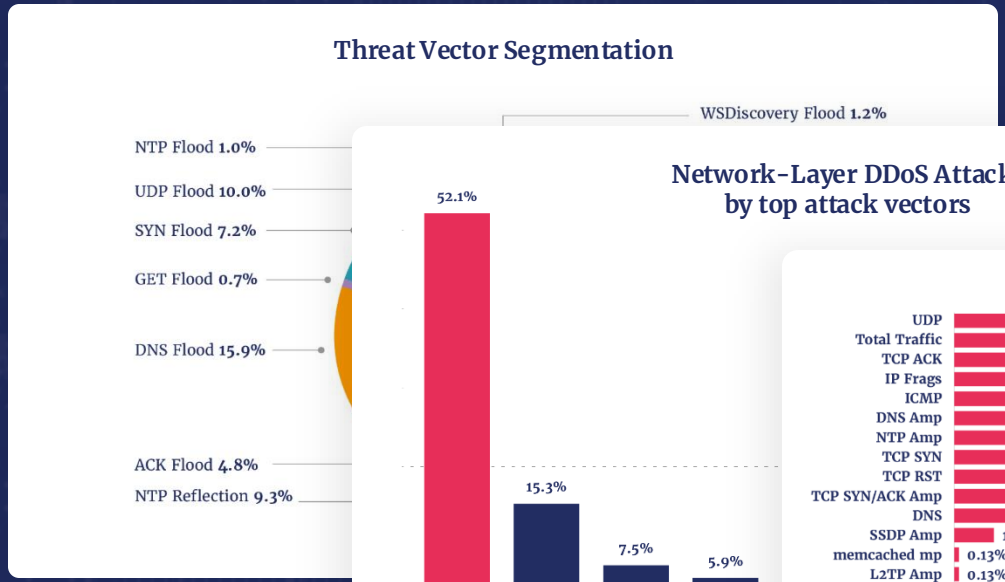
NBIP nationale beheersorganisatie internet providers

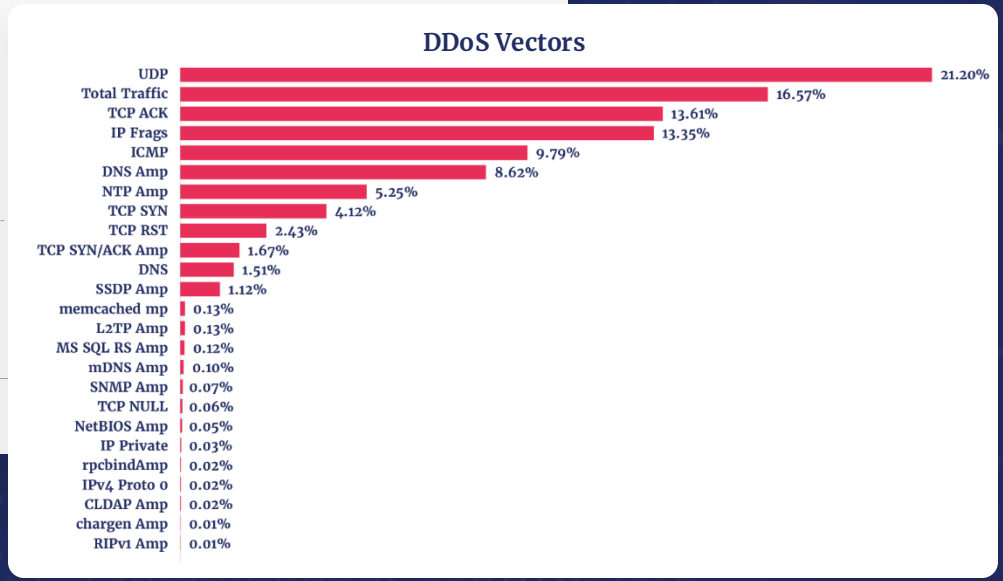
DDoS Reporting – most common vectors



NBIP nationale beheersorganisatie internet providers

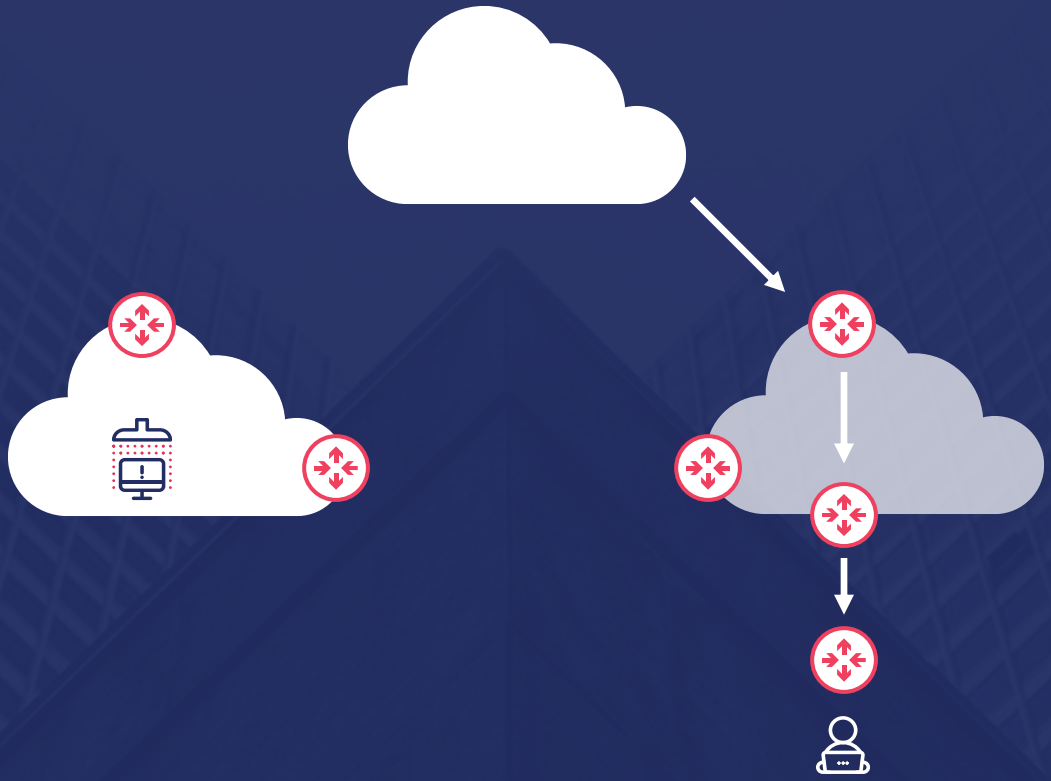
DDoS Reporting – most common vectors





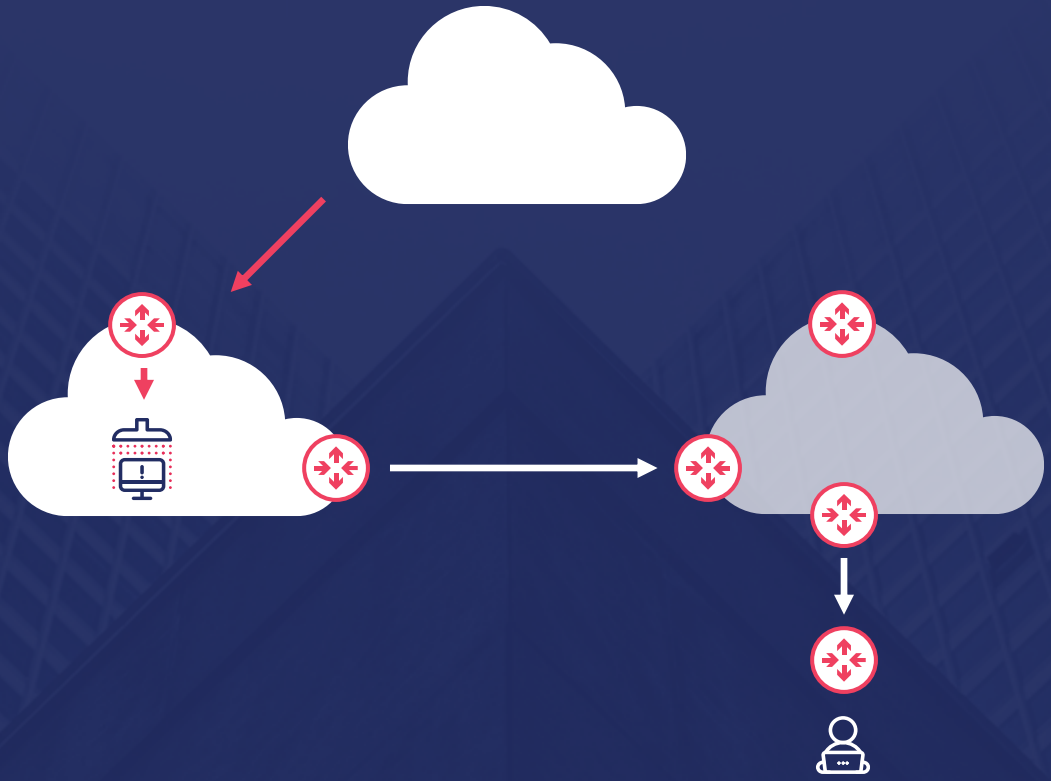
NBIP nationale beheersorganisatie internet providers

NaWas Architecture



NBIP nationale beheersorganisatie internet providers

NaWas Architecture



NBIP nationale beheersorganisatie internet providers

Detection of target

NBIP nationale beheersorganisatie internet providers

Detection of target

NBIP nationale beheersorganisatie internet providers

ICMP types to keep an eye on

TYPE 3

Destination Unreachable

0 Destination network unreachable
1 Destination host unreachable
2 Destination protocol unreachable
3 Destination port unreachable
4 Fragmentation needed and DF flag set
5 Source route failed

TYPE 5

Redirect Message

0 Redirect datagram for the Network
1 Redirect datagram for the host
2 Redirect datagram for the Type of Service and Network
3 Redirect datagram for the Service and Host

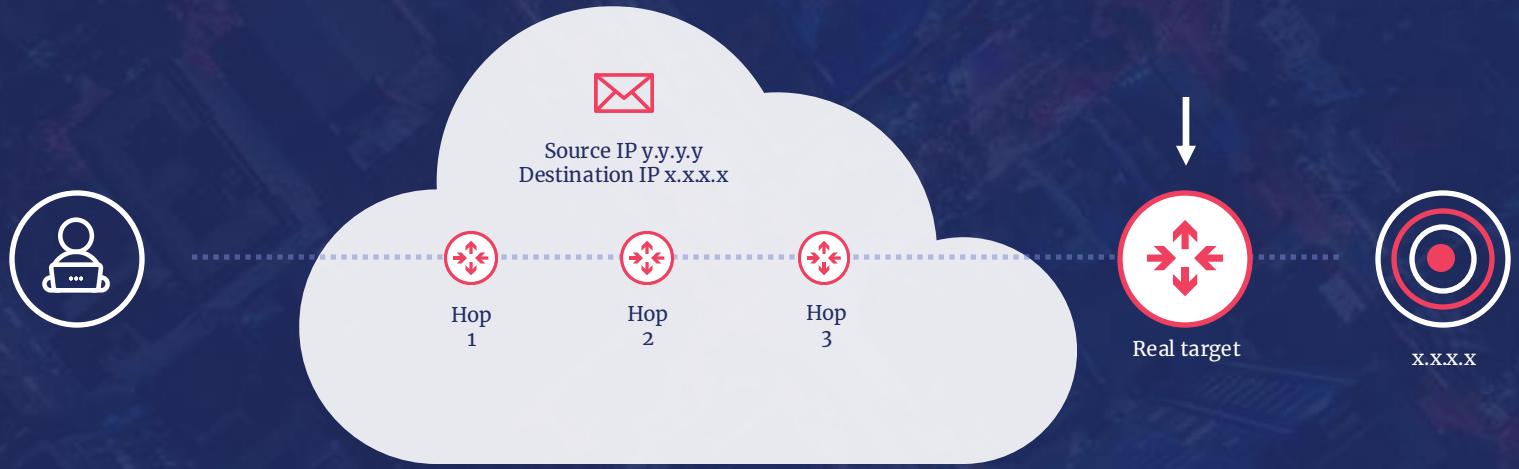
TYPE 11

Time Exceeded

0 Time to live exceeded in transit
1 Fragment reassembly time exceeded

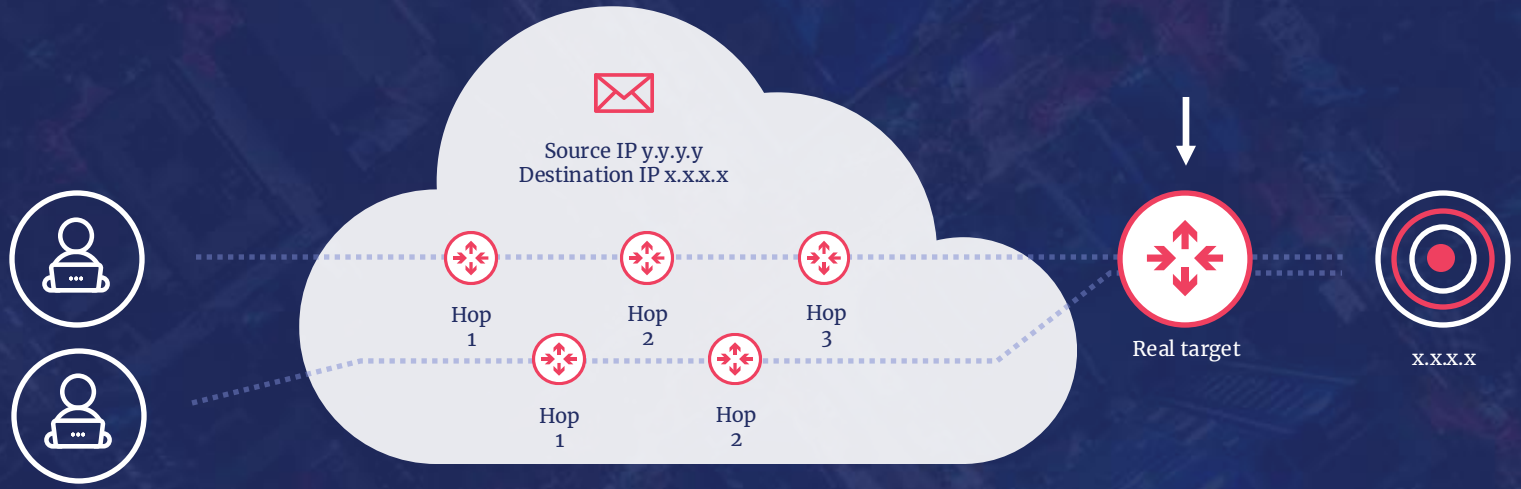
NBIP nationale beheersorganisatie internet providers

Detection of target



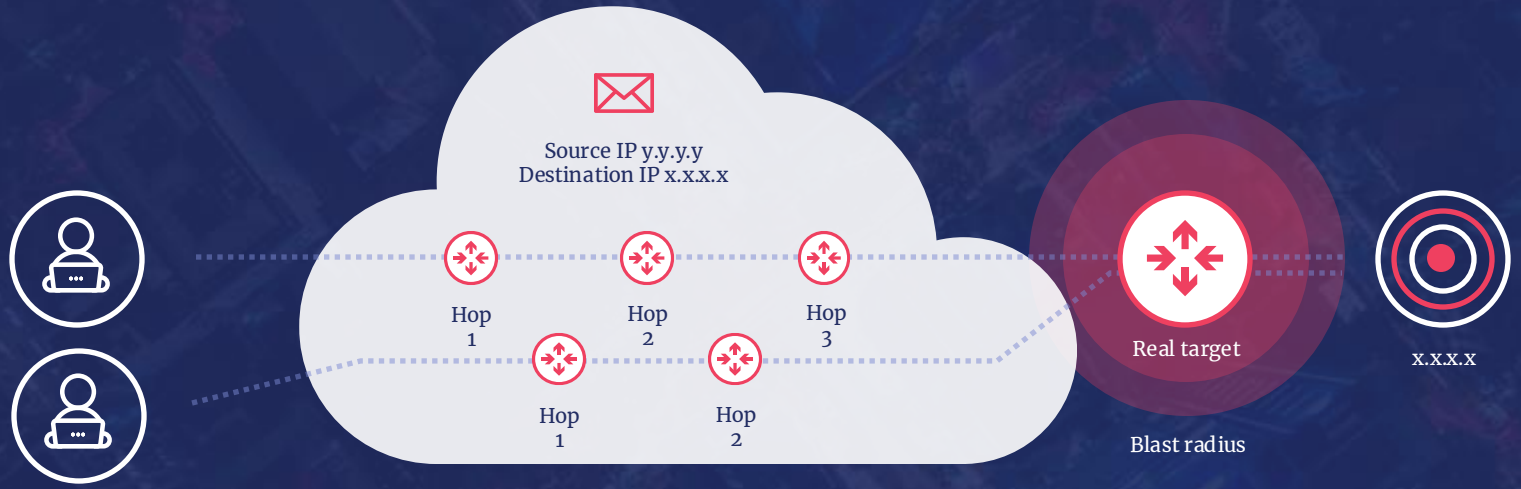
NBIP nationale beheersorganisatie internet providers

Detection of target



NBIP nationale beheersorganisatie internet providers

Detection of target



NBIP nationale beheersorganisatie internet providers

Detection of target

NBIP nationale beheersorganisatie internet providers

BGP

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.12.1	192.168.12.2	TCP	60	37019 > 179 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
2	0.000819	192.168.12.2	192.168.12.1	TCP	58	179 → 37019 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460
3	0.009725	192.168.12.1	192.168.12.2	TCP	60	37019 → 179 [ACK] Seq=1 Ack=1 Win=16384 Len=0
4	0.020192	192.168.12.1	192.168.12.2	BGP	111	OPEN Message
5	0.028136	192.168.12.2	192.168.12.1	TCP	54	179 → 37019 [ACK] Seq=1 Ack=58 Win=16327 Len=0
6	0.032618	192.168.12.2	192.168.12.1	BGP	111	OPEN Message
7	0.035073	192.168.12.2	192.168.12.1	BGP	73	KEEPALIVE Message
8	0.038837	192.168.12.1	192.168.12.2	TCP	60	37019 → 179 [ACK] Seq=58 Ack=77 Win=16308 Len=0
9	0.042187	192.168.12.1	192.168.12.2	BGP	73	KEEPALIVE Message
10	0.049259	192.168.12.1	192.168.12.2	BGP	73	KEEPALIVE Message
11	0.051291	192.168.12.1	192.168.12.2	BGP	131	UPDATE Message, UPDATE Message

```
▸ Frame 7: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
▸ Ethernet II, Src: fa:16:3e:17:10:52 (fa:16:3e:17:10:52), Dst: fa:16:3e:34:1b:14 (fa:16:3e:34:1b:14)
▾ Internet Protocol Version 4, Src: 192.168.12.2, Dst: 192.168.12.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 59
    Identification: 0xb489 (46217)
  ▸ Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
  ▾ Time to Live: 1
      ▸ [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (6)
    Header Checksum: 0x2b20 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.12.2
    Destination Address: 192.168.12.1
▸ Transmission Control Protocol, Src Port: 179, Dst Port: 37019, Seq: 58, Ack: 58, Len: 19
▸ Border Gateway Protocol - KEEPALIVE Message
```

```
0000  fa 16 3e 34 1b 14 fa 16  3e 17 10 52 08 00 45 c0   ..>4....>..R..E.
0010  00 3b b4 89 40 00 01 06  2b 20 c0 a8 0c 02 c0 a8   .;..@...+ ......
0020  0c 01 00 b3 90 9b 02 58  2b 5c dd 3a 49 45 50 18   .......X+\.:IEP.
0030  3f c7 ed 08 00 00 ff ff  ff ff ff ff ff ff ff ff   ?...............
0040  ff ff ff ff ff ff 00 13  04                       .........
```

NBIP nationale beheersorganisatie internet providers

Unintended consequences

Host	Loss%	Snt	Last	Avg	Best	Worst	StDev
1. 62-3-100-30.dsl.in-addr.zen.co.uk	0.0%	74	0.4	0.5	0.4	0.8	0.1
2. ???							
3. lag-8.p2.thn-lon.zen.net.uk [MPLS: Lbl 24012 Exp 0 S 1 TTL 1]	0.0%	74	12.6	13.7	12.0	32.0	3.4
4. lag-2.br1.thn-lon.zen.net.uk	0.0%	74	17.7	14.2	11.8	35.4	4.4
5. bbr02.lon01.networklayer.com	0.0%	74	12.1	13.5	11.7	30.0	3.2
6. ae5.cbs01.tg01.lon01.networklayer.com [MPLS: Lbl 205039 Exp 0 S 1 TTL 1]	64.4%	74	12.8	15.1	12.6	21.3	2.9
7. ae0.cbs01.xn01.fra01.networklayer.com [MPLS: Lbl 126402 Exp 0 S 1 TTL 1]	41.1%	74	26.7	25.3	23.4	43.4	3.4
8. ae0.cbs02.ic01.mil02.networklayer.com [MPLS: Lbl 809963 Exp 0 S 1 TTL 1]	1.4%	74	32.5	35.7	32.5	61.2	5.4
9. ae7.cbs01.ic01.mil02.networklayer.com [MPLS: Lbl 288384 Exp 0 S 1 TTL 1]	21.9%	73	34.9	35.4	32.6	65.7	5.4
10. 61.13.2da9.ip4.static.sl-reverse.com [MPLS: Lbl 423005 Exp 0 S 1 TTL 1]	30.1%	73	242.4	244.3	242.3	254.7	2.6
11. af.13.2da9.ip4.static.sl-reverse.com [MPLS: Lbl 499542 Exp 0 S 1 TTL 1]	0.0%	73	242.3	244.1	241.8	257.6	3.7
12. cb.12.6132.ip4.static.sl-reverse.com	0.0%	73	242.8	244.1	242.5	254.5	2.5
13. po2.fcr01.sr03.sng01.networklayer.com	30.1%	73	261.2	277.6	260.8	547.7	52.5
14. sip3.nexmo.com	0.0%	73	242.4	243.4	242.1	258.0	2.5

Takeaways

Regularly review Infrastructure protection policies

Consider your architecture changes

Understand impact of throttling certain ICMP packets

ICMP is your Frenemy

NBIP nationale beheersorganisatie internet providers

Together Smarter and Stronger

NBIP nationale beheersorganisatie internet providers