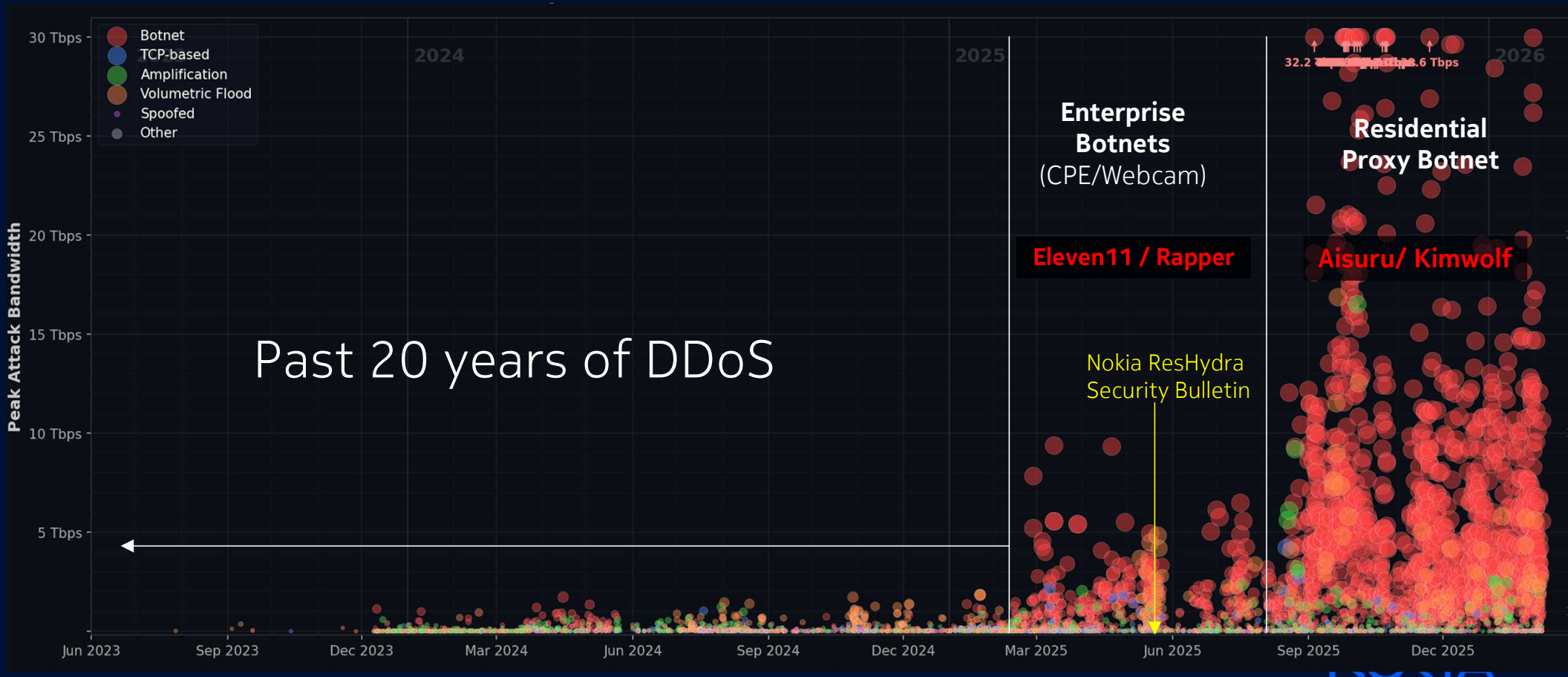
Latest DDoS trends
and how to
MITIGATE

Serkan Gencel
IP Consulting Engineer

 © 2026 Nokia

How DDoS changed over the last 12-18 months

Deepfield Secure Genome® tracking DDoS and botnet activity globally



Kimwolf and Ipidea

Kimwolf was exploiting Ipidea security holes / local scanning (Synthient Jan 2026)

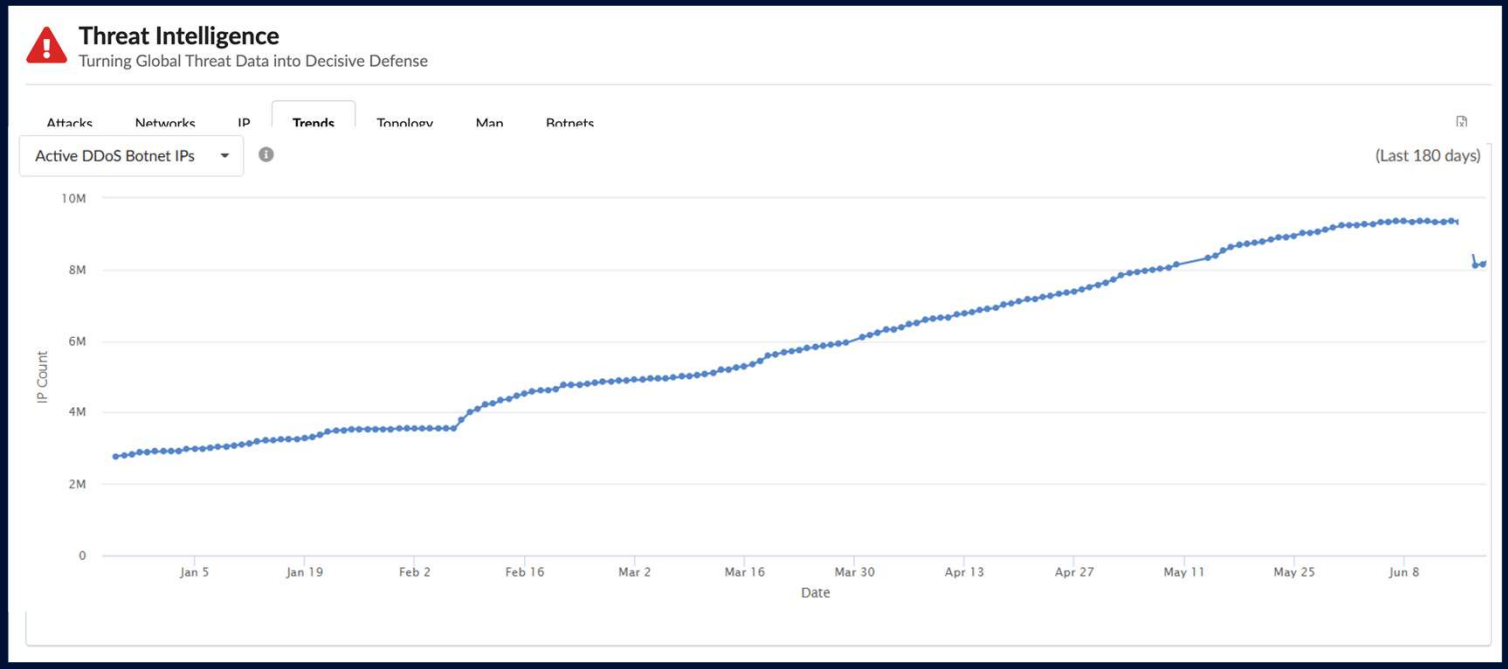


https://synthient.com/blog/a-broken-system-fueling-botnets



https://krebsonsecurity.com/2026/01/the-kimwolf-botnet-is-stalking-your-local-network/

Active botnet IPs: Up from 1M to 9M over the last 9 months!

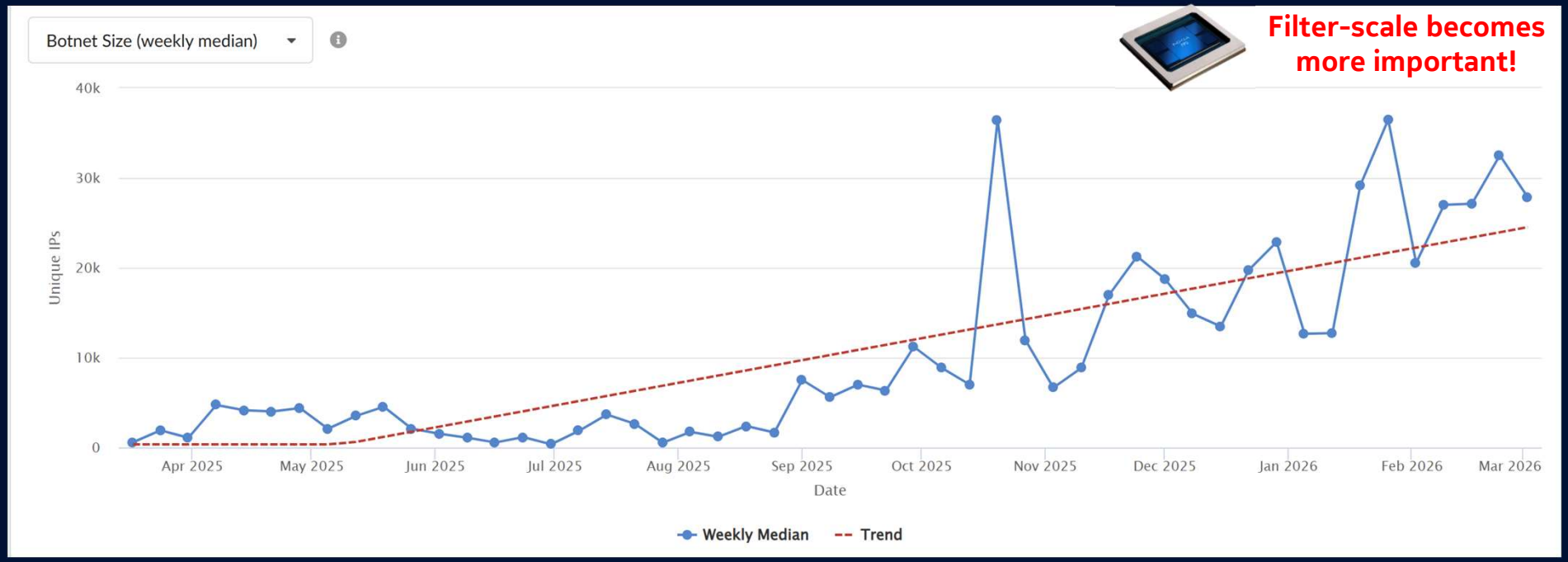


Fueled by explosive growth of residential proxy services – which is fueled by AI

Problem: Significant portion of proxy nodes **exploitable** by botnets or provide access to vulnerable home IoT

DDoS trends: median number of unique bots per attack

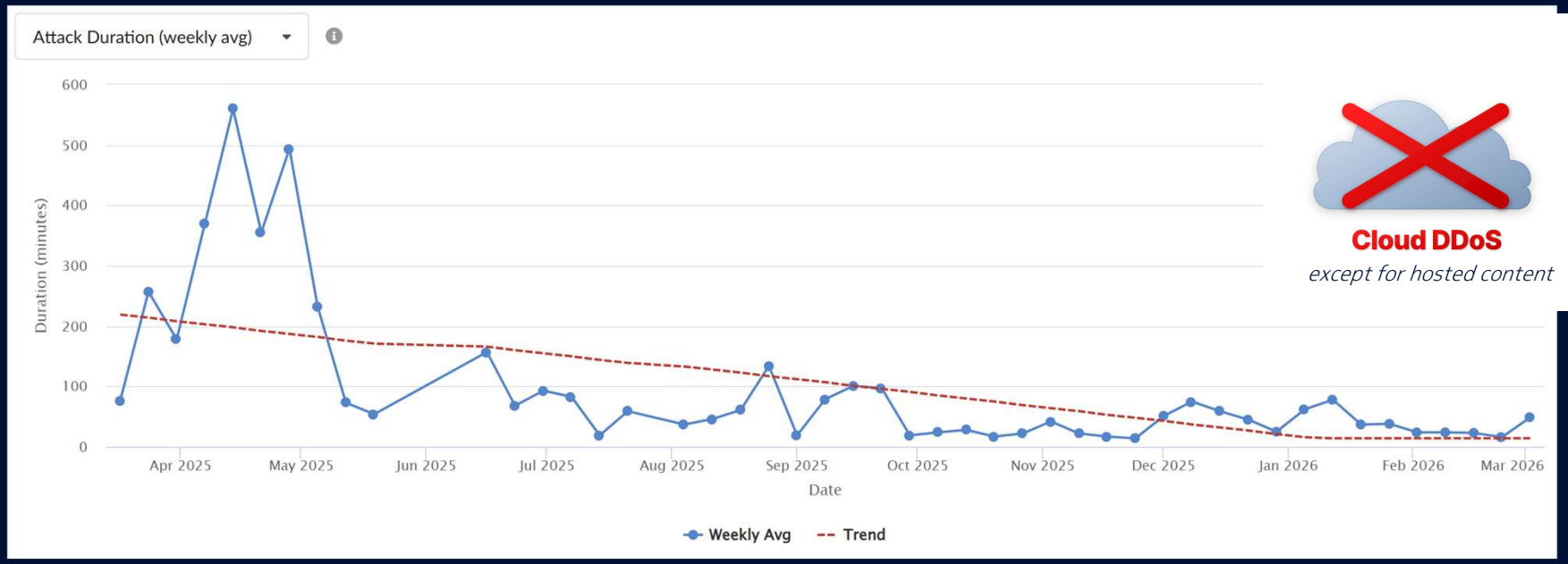
Grown from a few thousands to tens of thousands and more since August 2025



Data from Deepfield Secure Genome

DDoS trends: attack duration

Most attacks changed to multiple short (<5minute) bursts



Data from Deepfield Secure Genome

Questions every network owner should ask:

What is required to block these attacks?

Are we ready to defend against these attacks?

NOKIA

What is required today for a good DDoS protection solution?

1 Scale

- Block hyper-volumetric attacks **at network edge** – with large-scale filtering
- For carpet-bomb & multiple simultaneous attacks

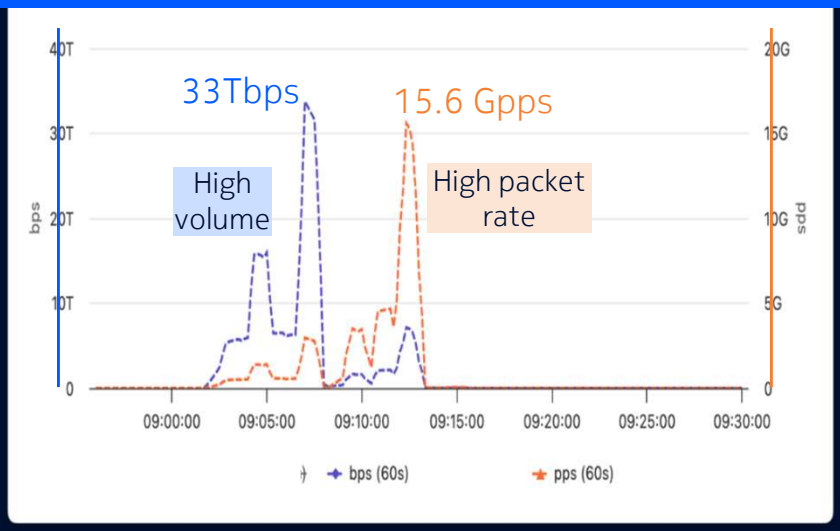
2 Automation

- Fast detection and mitigation
- Adapting fast to algorithmic attack changes

3 Intelligence for reliable DDoS protection

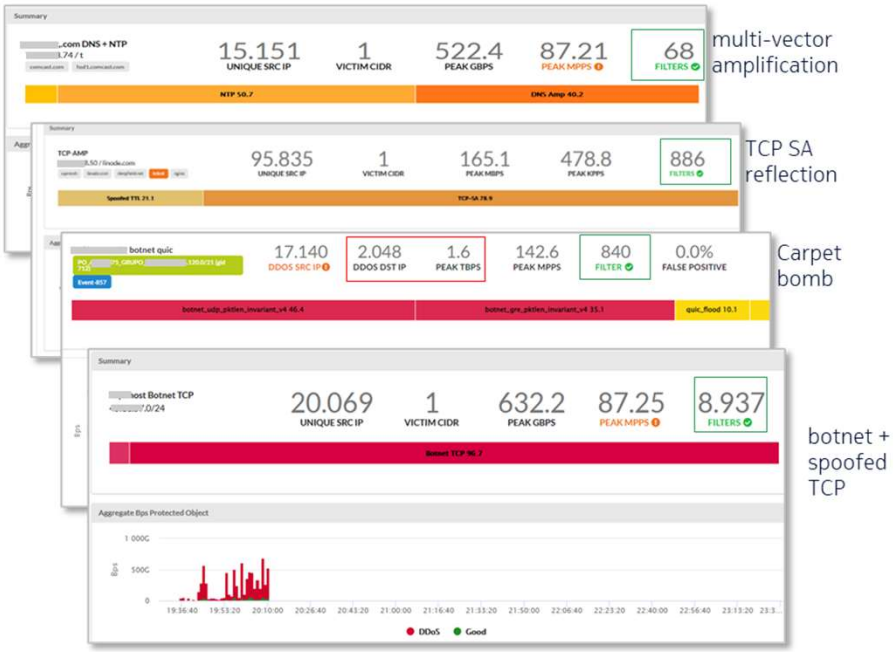
- No false positives - not every burst is an attack
- No false negatives - not all legitimate-looking traffic is good
- And neutralizing active bots in your network

9 Oct 2025: Aisuru botnet attack to gaming companies



1) Source: Deepfield ERTS and Genome research team
2) https://www.nokia.com/blog/the-internet-commons-under-siege-why-33-tbps-ddos-attacks-are-everyones-problem/

Dynamic DDoS mitigation at network edge with Defender



Surgical Edge Mitigation filtering:

- Filtering always includes match on:
  - **dst address** matchlist with one or more /32's or subnets
- and optional additional L3-L4 match-criteria:
  - **protocol** UDP, TCP, ICMP, GRE,…
  - **fragments:** < 0.5% in peace-time, MUCH higher in attacks.
  - **TCP flags:** S, SA, A, R, P, invalid combinations,…
  - **src** and/or **dst protocol**: match on values/ranges or invariants
  - **packet length:** ranges or invariants
  - **TTL:** suspicious ranges or invariants
  - **src address** for top Botnet/proxy/malicious hosts
Top subnets for geo-blocking
- Baseline policers optionally as 'last resort': SYN, SYN-ACK, TCP, UDP
- Filter installation using **Netconf** or BGP **FlowSpec**
- **Closed-loop dynamic filter adaptation** to adapt to changes in attack traffic (changes in traffic patterns and/or destinations)
- **Automated roll-up** of dst subnet for efficient mitigation of carpet-bombs

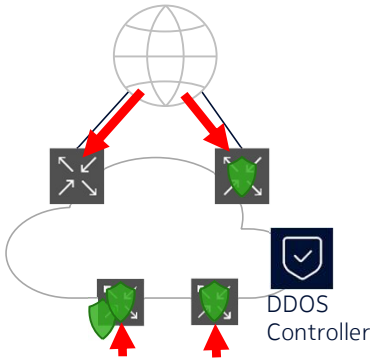
© 2026 Nokia

DDOS mitigation options: edge-based vs Scrubber

Mitigate on edge when you can…

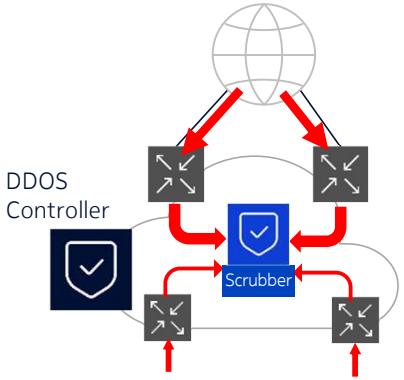
- Leveraging filtering power of Edge routers

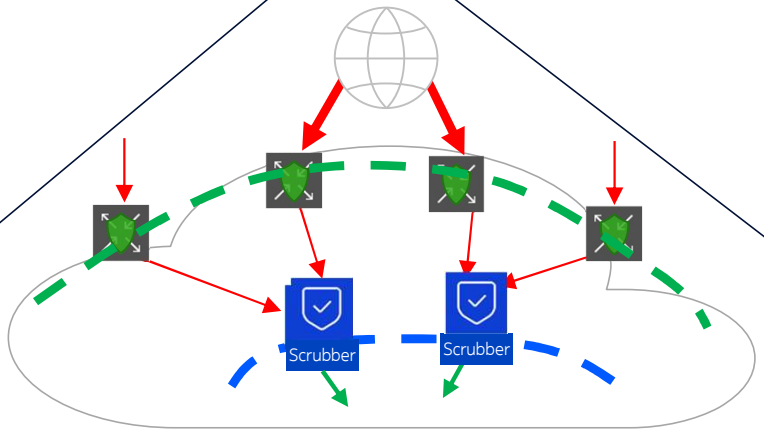
Fastest Mitigation | Highest **Scale** | **Cost** efficient



Mitigate on Scrubber if you

- If Edge routers can not be used , use Offramp Scrubber



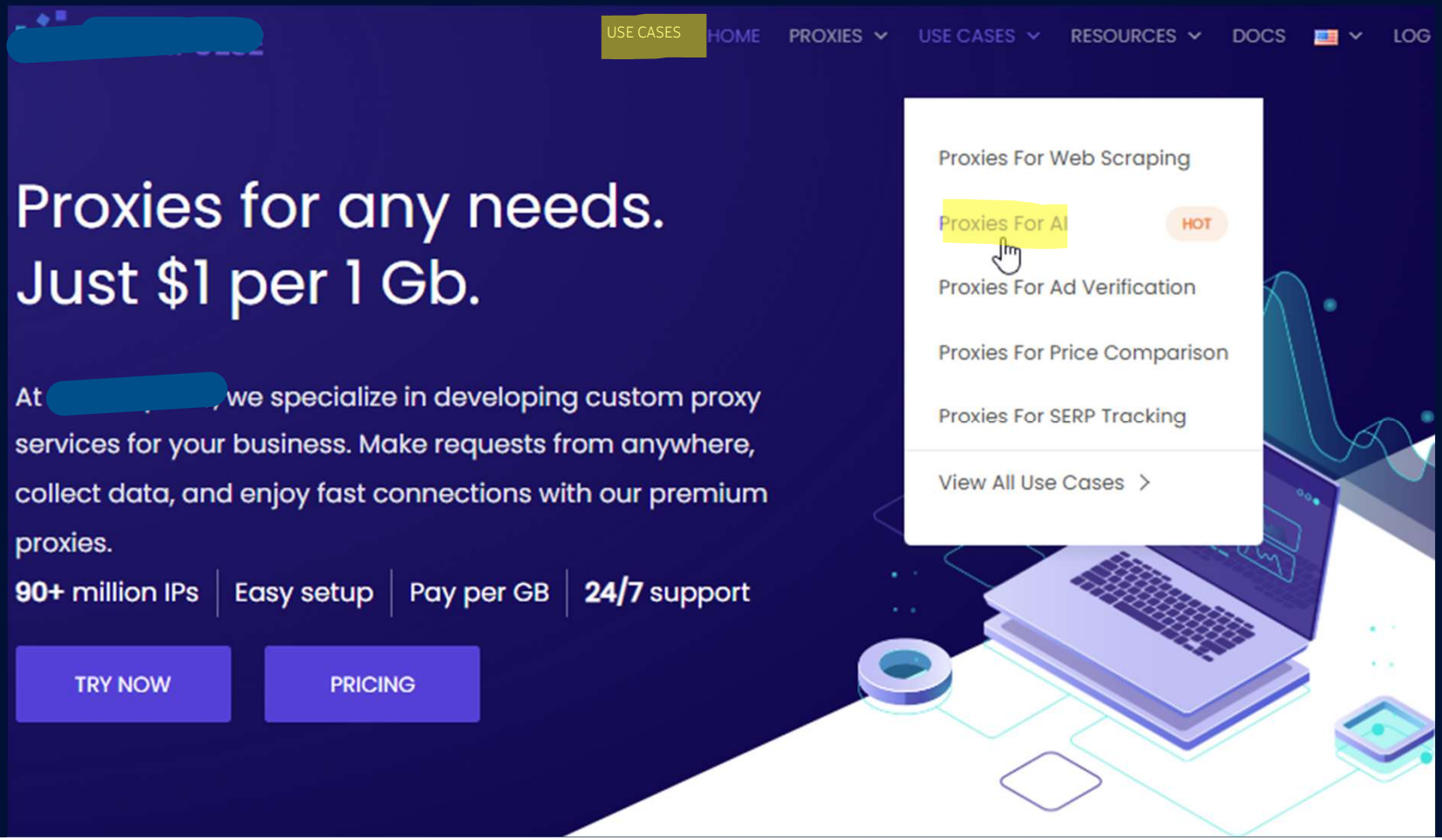


Or combine edge mitigation + Scrubber

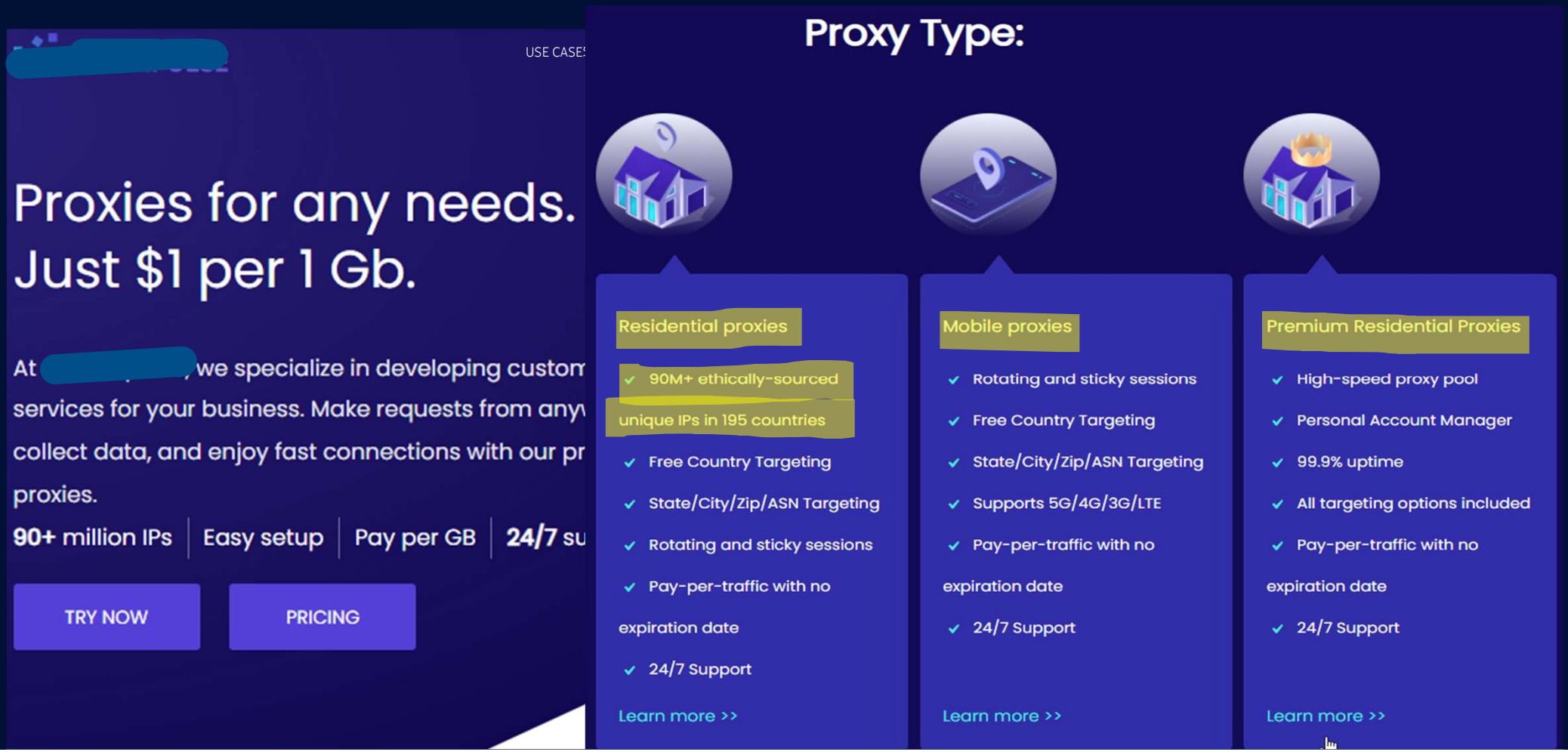
© 2026 Nokia

How to neutralize DDoS Bots within your network?

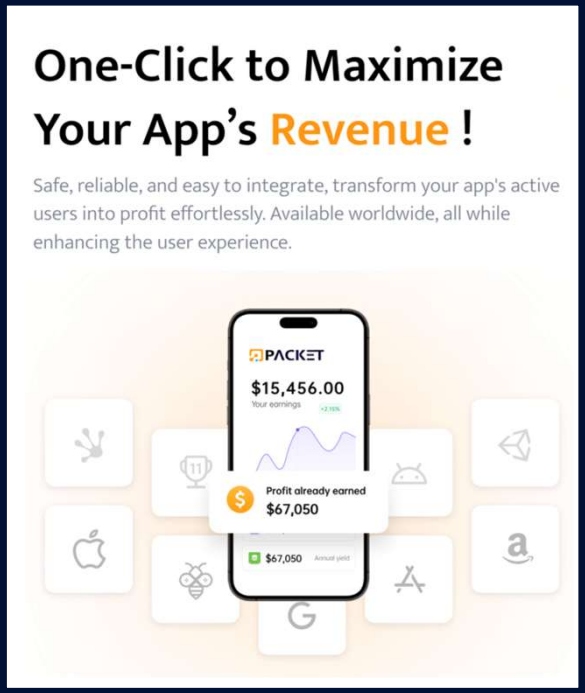
What are Residential Proxy Services – catalyst for recent botnet growth



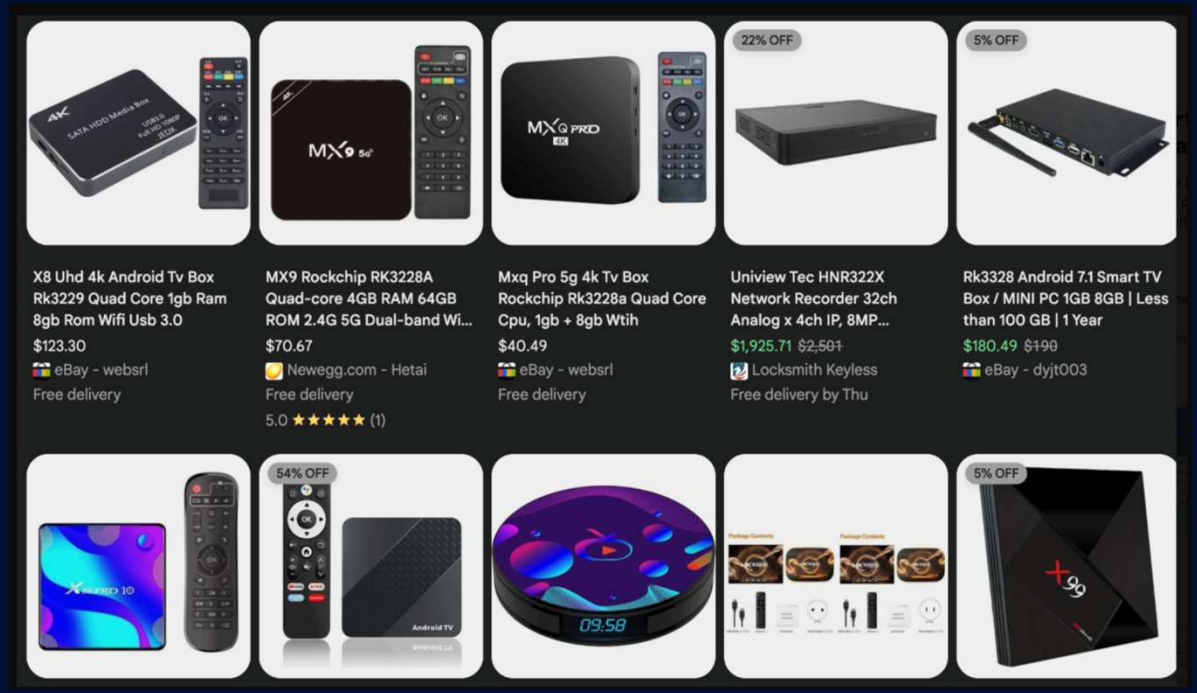
What are Residential Proxy Services – catalyst for recent botnet growth



Residential Proxy DDoS: examples of affected devices



Attacks from smartphones
(SDKs downloaded)

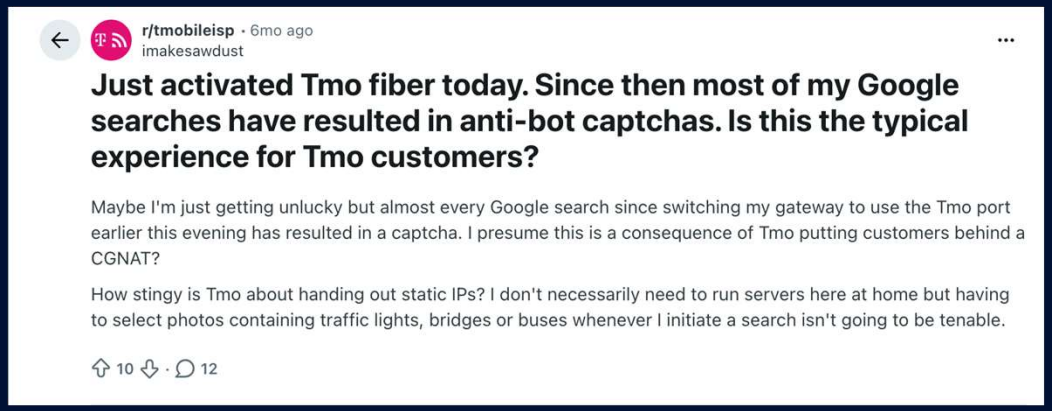


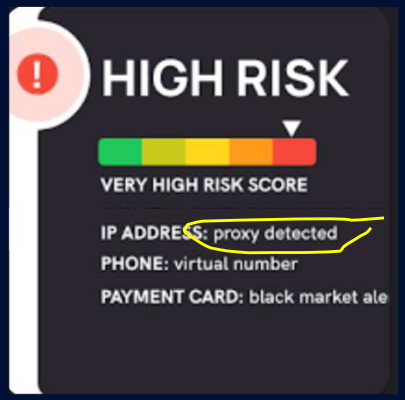
Attacks from factory-compromised Android devices

NOKIA

More reasons telcos and cloud providers should care

Outages, reputational damage and bad customer experience





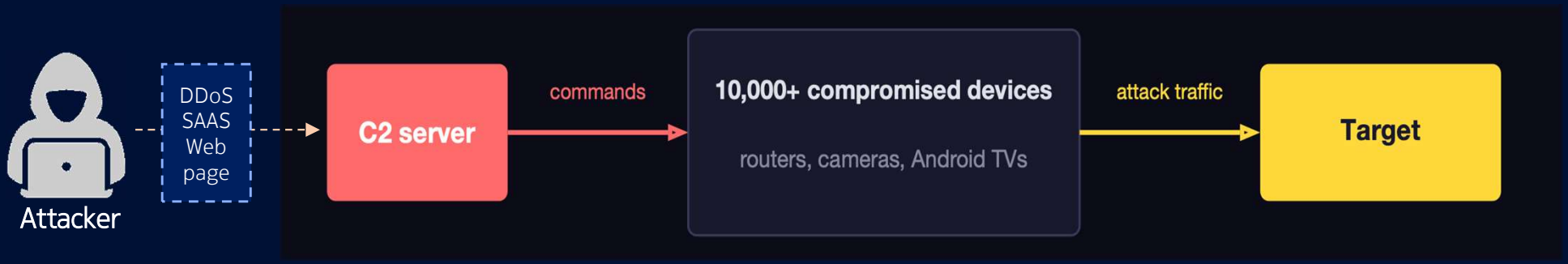
Commercial IP reputation providers flag CGNAT IPs as high threats, leading to more failed or delayed transactions

How to stop this?



© 2026 Nokia

How botnets operate…



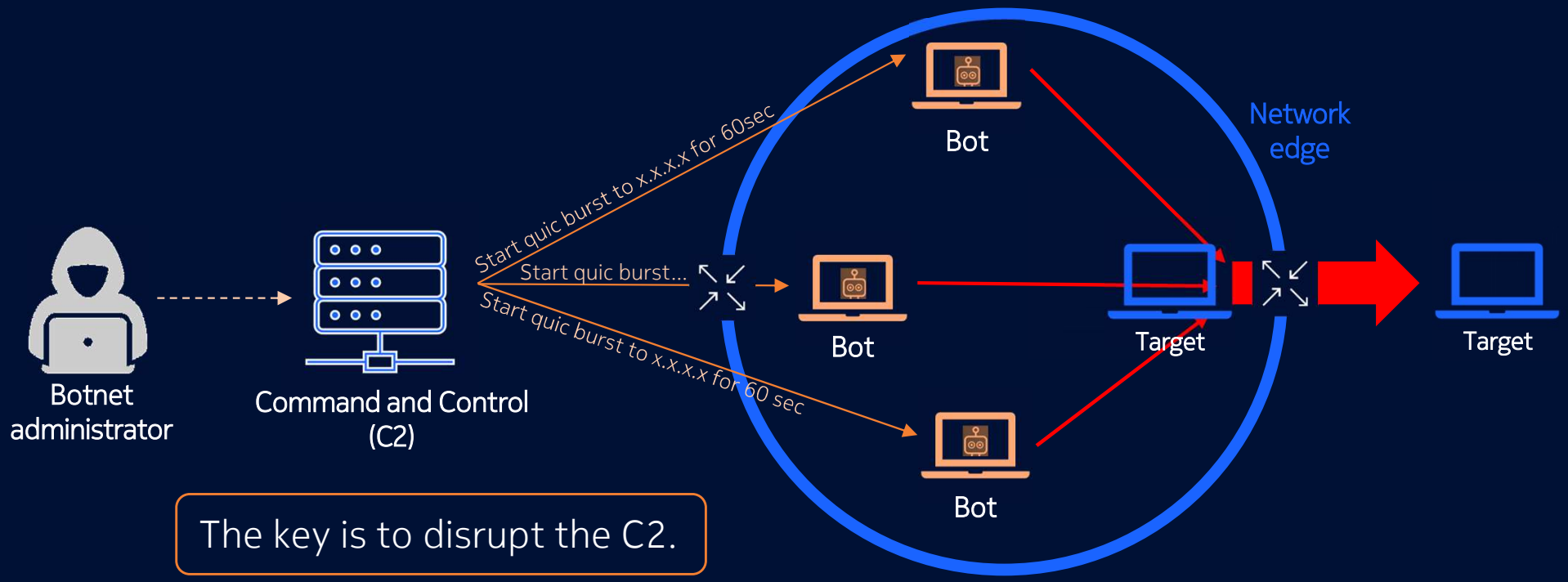
- Someone sends an attack command trough (web-interface fronting) Command and Control (C2) server
  → Tens of thousands of devices attack in unison.

  Example attack command to launch 60-second burst of HTTP traffic to X.X.X.X :

```
cecbot-monitor C2 attack command – cecbot ( http_l7 ) [2026-04-09T06:36:17Z]
• 49.13.211.149/32 (AS24940/hetzner.de/DE) | HTTP/:* | 60s
```

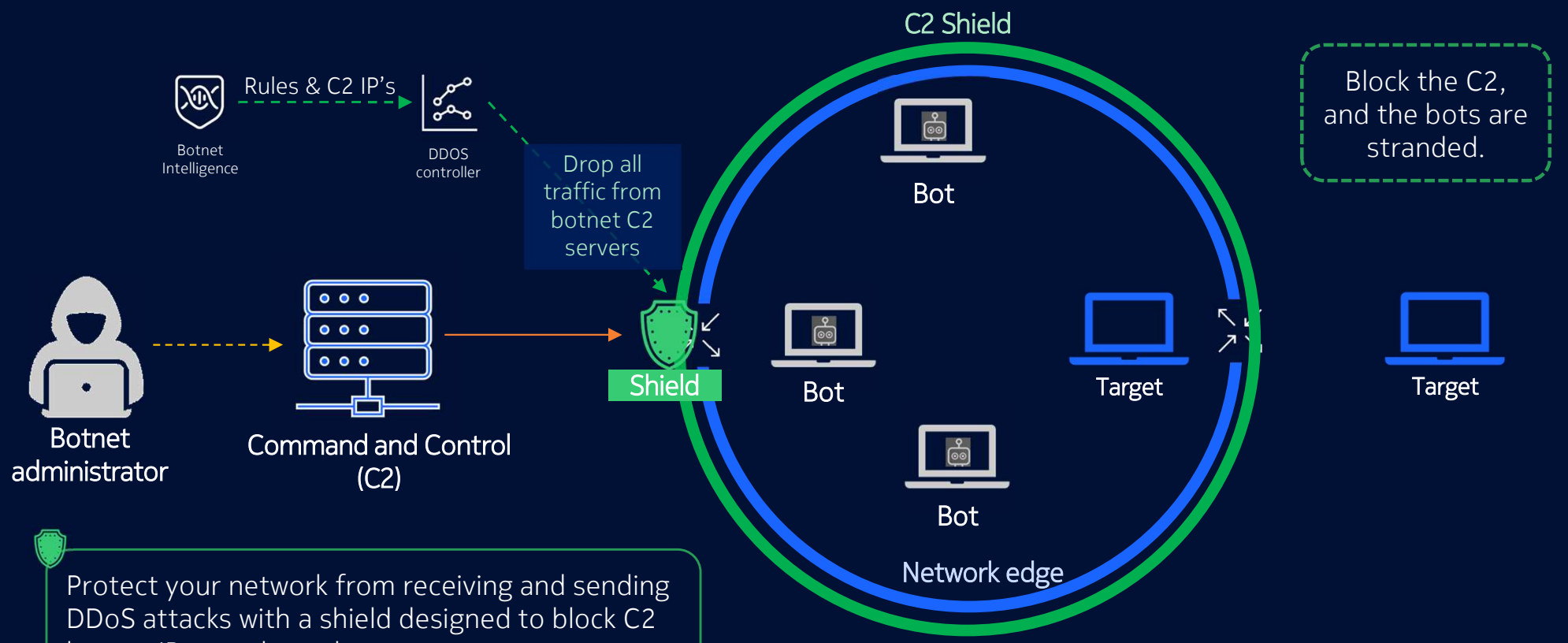
C2 = command and control, the server that tells the botnet what to do

Botnet attacks are coordinated by Command and Control servers



The key is to disrupt the C2.

Shield: Solves on-net botnet problem before it enters the network

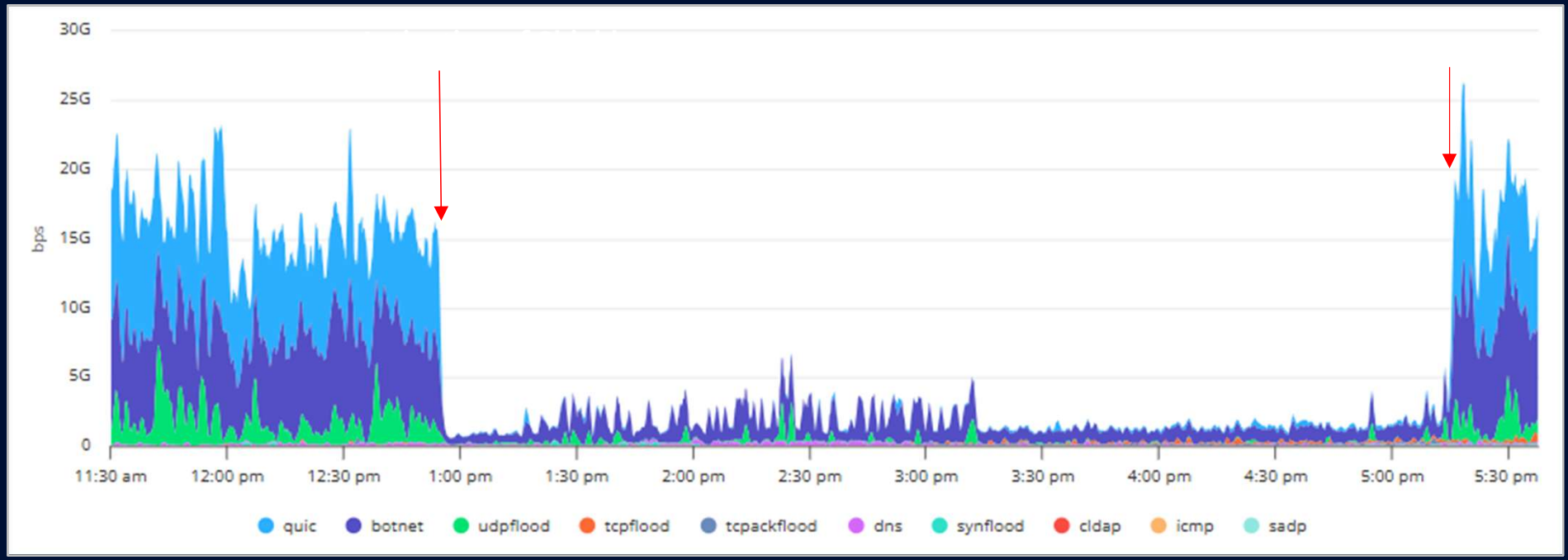


Protect your network from receiving and sending DDoS attacks with a shield designed to block C2 botnet IPs on a boundary

The effects of applying C2 inbound filtering in customer network

Immediate and dramatic

Oubound DDoS traffic




NOKIA