

# IP Trends in Internet Peering and Security Analytics / Mitigation

Ivo Lansky

Snr. Director, Central/East Europe, Türkiye and Central Asia

Nokia IP Business, Networks Infrastructure

The Nokia logo is centered within a large white circle on a dark teal background. The logo itself consists of the word "NOKIA" in a white, sans-serif font, with a distinctive gap between the 'O' and 'K'.

NOKIA

# Internet & IP Peering Trends in Europe and Central Asia

## Traffic Growth

- Europe – East Asia (25 Tbps)
- IXP POP Design (10 / 100 / 400 / 800 GE), Leaf / Spine / Chassis, ...

## Geopolitical Factors

- Public Peering common in both West and East Europe ...  
... but Central Asia countries still mostly regulated and w/ private peerings only
- ~50% Europe - Asia Internet traffic routed via Central Asia / Kazakhstan & Russia

## Security

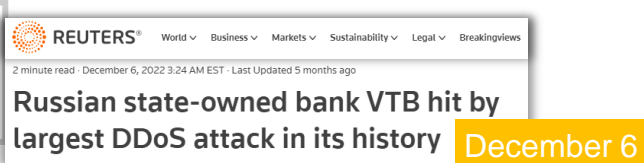
- Big Data DDoS Analytics and Auto-mitigation

# DDoS spares no one – targeting all Network/services/customer

segment



**UK government assess Russian involvement in DDoS attacks on Ukraine**



**Russian state-owned bank VTB hit by largest DDoS attack in its history**

December 6

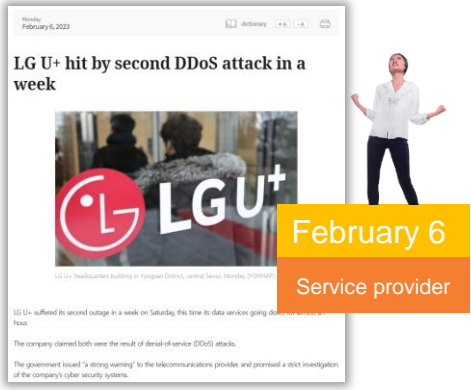
Customers



**Hackers infect TP-Link router firmware to attack EU entities**

May 16


Customers



**LG U+ hit by second DDoS attack in a week**

February 6


Service provider



**Overwatch 2 and Battle.net Servers are Experiencing a DDoS Attack**

April 8

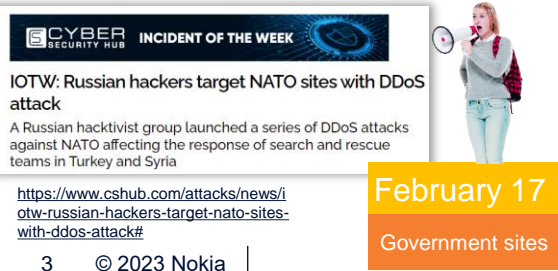
Gaming company



<https://koreajoongangdaily.joins.com/2023/02/06/business/industry/Korea-LG-U-DDoS/20230206175514381.html>

<https://thenerdstash.com/overwatch-2-ddos-attack-blizzard-servers-down/>


<https://www.bleepingcomputer.com/news/security/hackers-infect-tp-link-router-firmware-to-attack-eu-entities/>



**IOTW: Russian hackers target NATO sites with DDoS attack**

February 17

Government sites



**DDoS attacks strike Indian airports. Here's how the threat was mitigated**

April 16

Critical infra



**Worst cyberattack in Greece disrupts high school exams, causes political spat**

May 30

Education



<https://www.cshub.com/attacks/news/iotw-russian-hackers-target-nato-sites-with-ddos-attack#>

<https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/ddos-attacks-strike-indian-airports-heres-how-the-threat-was-mitigated/99461876>

<https://abcnews.go.com/International/wireStory/worst-cyberattack-greece-disrupts-high-school-exams-causes-9962310>



# The nature of DDoS changed dramatically over last year

## 2002–2022:

- Majority **DDoS is crafted or spoofed** using amplification/reflection
  - ‘Easy’ to mitigate based on packet pattern match or protocol challenges

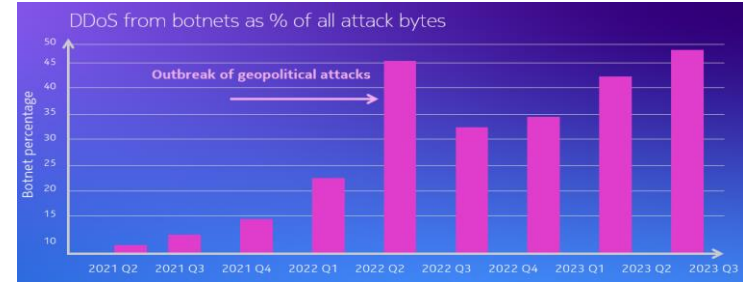
## Today:

- **Botnets** generate most complex attacks and most DDoS volume
  - Top Botnet device types: webcams, DVRs, routers, NAS, business IOT,...
- **Exponential Botnet DDoS Growth driven by:**
  - Exponential growth in IOT devices
  - Growth in CVE’s
  - Dramatic drop in DDoS Black Market prices
  - Botnet traffic comes from anywhere

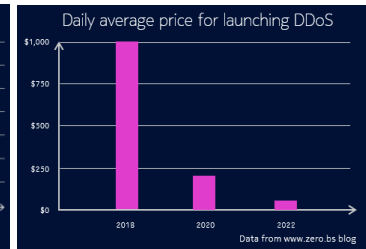
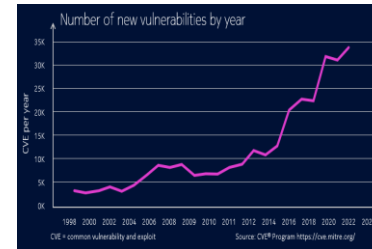
## Trend:

- Roll-out of **symmetric GE/10GE access will make things worse...**

**Botnet DDoS protection requires 360° edge monitoring and protection**



Source: Nokia Deepfield



## The Botnet DDoS detection challenge...

- is no longer about looking what's **inside** the packet
  - instead, it's about **who/what** is sending the packet
- ... has become a Big Data challenge**

# Nokia's Deepfield Defender DDoS protection solution

Scalable cost-performant DDoS Protection

## 1 Plug-and-Play DDoS Detection

- Zero Touch DDoS classification based on big data principles
- No manual thresholds nor baselines setup

## 2 Use IP silicon to filter DDoS attacks

- Scalable and cost-efficient DDoS protection compared to DPI based scrubbers
- Surgical DDoS mitigation
- DDoS protection lifecycle orchestration



Nokia Deepfield

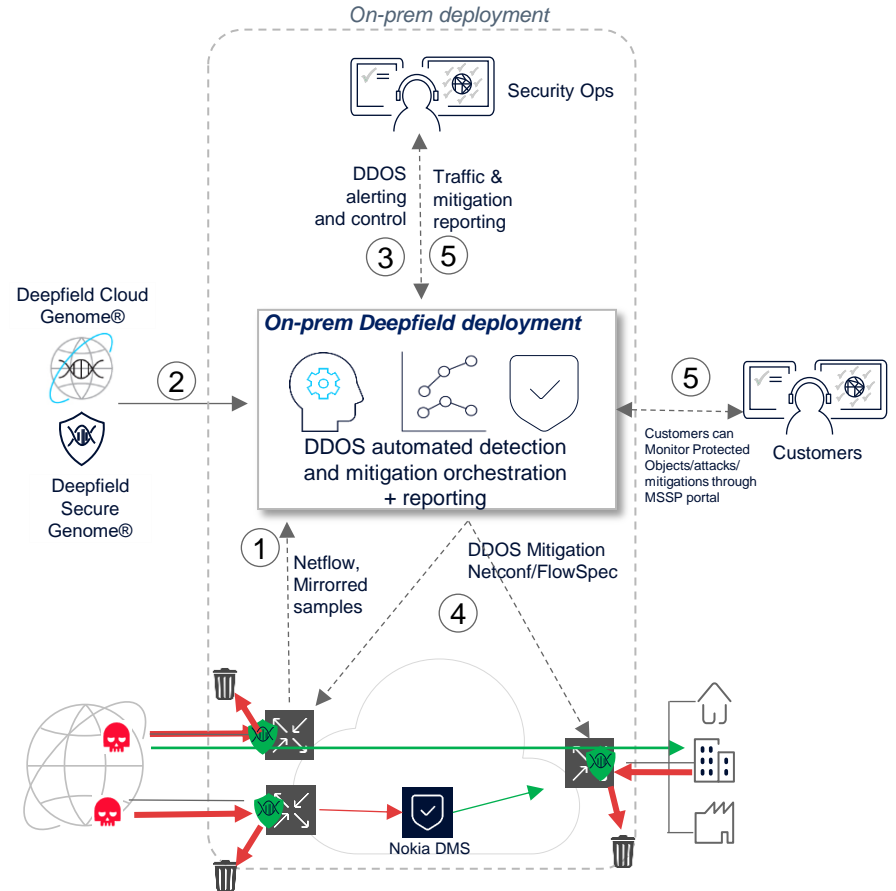


Nokia Routers or  
Defender Mitigation  
System (DMS)

# Nokia Deepfield Defender

A high-scalable **software platform** combining

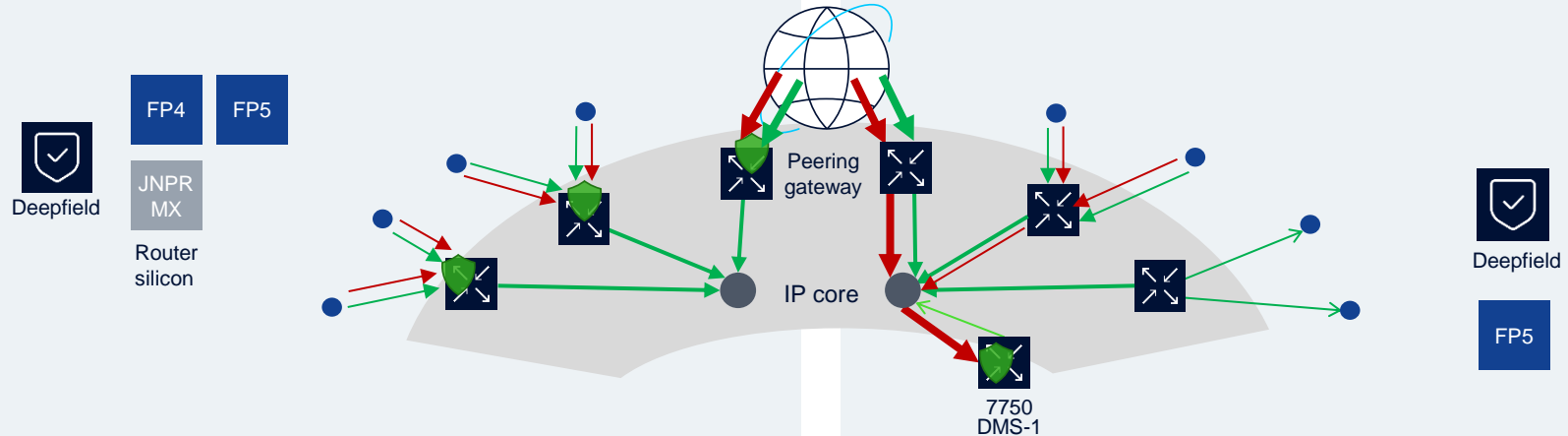
- ① **Telemetry** (Netflow or mirrored traffic samples) from your routers
- ② **big data** based security map of the Internet to provide
- ③ **Automated DDOS detection** for high-volume/high-packet rate DDoS attacks
- ④ **Fast DDoS filtering at line-rate**
  - leveraging Nokia IP silicon
  - on all Nokia edge routers or Nokia DMS
- ⑤ **Flexible Reporting**
  - Including MSSP Portal for participants to see attacks & mitigations to their Protected Objects



# Deepfield - IP silicon based DDOS mitigation options

## Edge router-based mitigation

## Alternative: Off-ramp to Deepfield Mitigation System (DMS)



### Mitigation at the edge:

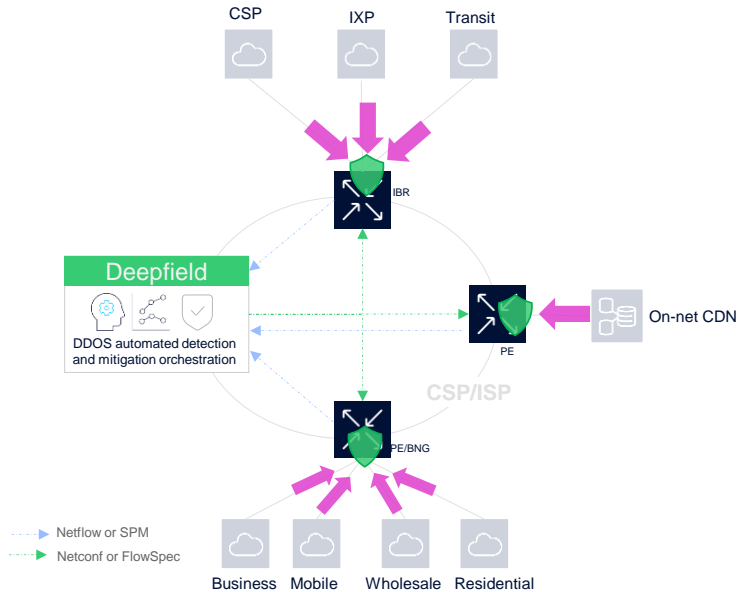
Use existing routers (Nokia SR or Juniper MX) to drop DDoS traffic at the edge.

### Scrubbing Center approach:

Deploy dedicated FP5 based Defender Mitigation System (DMS) to provide terabit-class scrubbing

# On-Net DDoS Protection solution for CSP/ISP networks

Making the Network part of your DDoS Protection Architecture with Nokia Deepfield



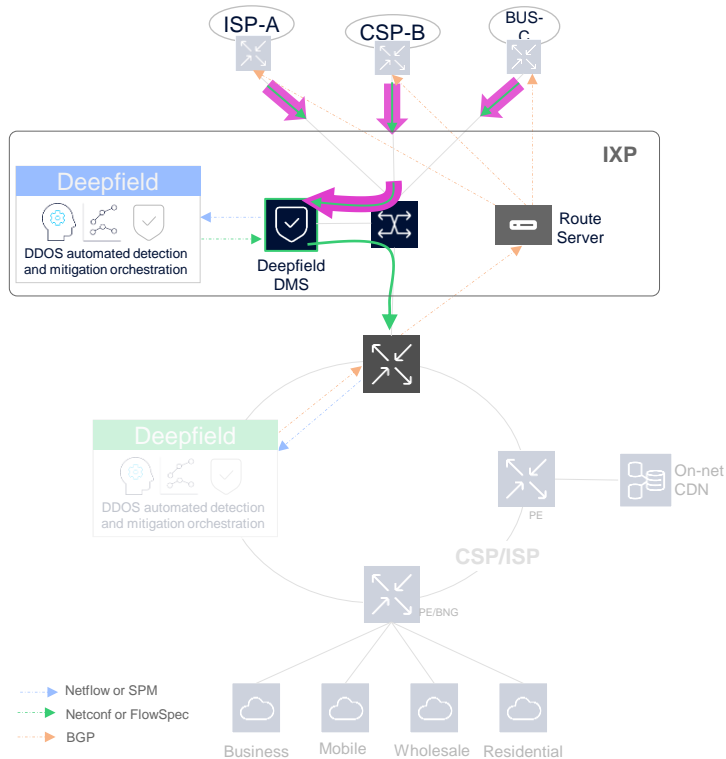
- 360° Monitoring – covering all network edges
- Big Data based DDoS detection
  - Fast, reliable, working out-of-the-box
  - Covering Botnet DDoS next to traditional DDoS
- IP Silicon based DDoS mitigation
  - Surgical Edge mitigation @Line-rate using Nokia FP4/FP5 (or Juniper) routers
  - or divert through Nokia DMS mitigation appliance

But for huge attacks (that would congest your peering links) or when you don't have the resources for on-prem DDoS mitigation: → **complement with DDoS service from upstream provider**



# Premium DDoS protection as part of IXP Service

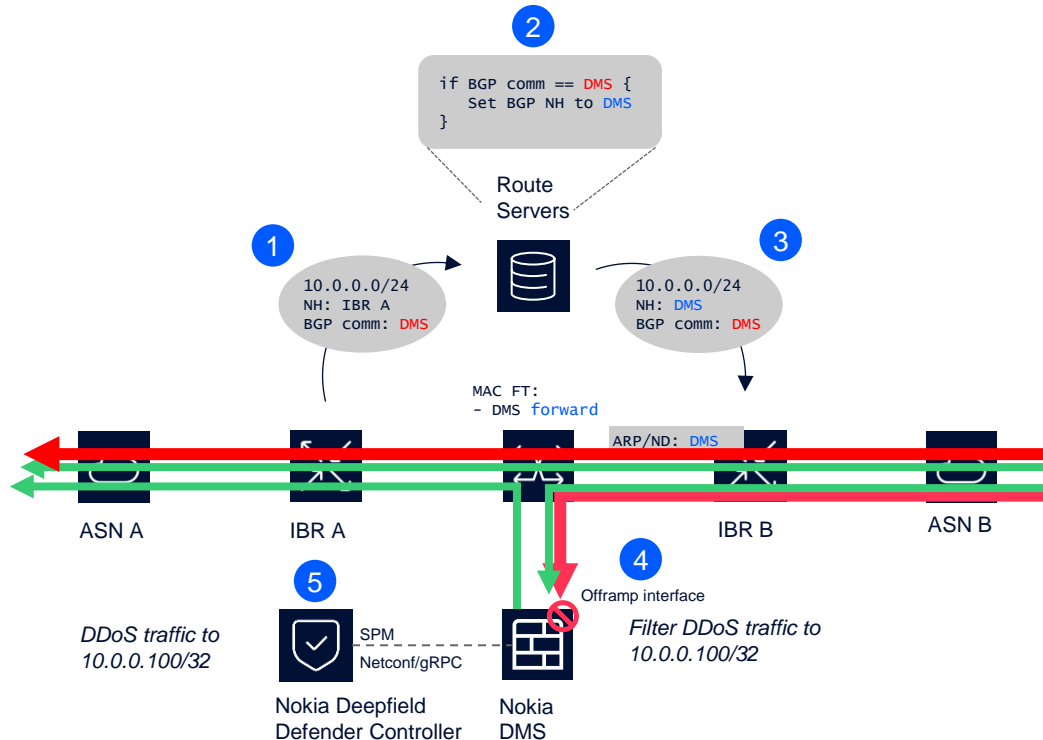
with Nokia Deepfield



- Advanced on-demand protection against volumetric DDoS attacks
  - Using Nokia Deepfield for simple integration in existing connectivity services (no need to redefine LAN)
- Benefits for IXP:
  - Differentiating value-added service add-on to connectivity services
  - Low operational cost (activated by Customer, auto-mitigation by Nokia system)
  - Lower TCO compared to the traditional scrubbing-based solutions
- Benefits for IXP customers
  - Superior granular DDoS protection vs rudimentary RTBH/'drop-all'
  - Customer keeps control to start/stop protection 'on-demand'
  - Fast Protection (<1min from service activation)
  - Optional access to web-portal to see DDoS traffic mitigation details

# Premium on-demand DDoS protection as part of IXP Service

## Technical solution with Nokia Deepfield



- 1 IBR A advertises the prefix under attack (or the entire prefix) tagged with the **DMS** BGP community
- 2 The Route Servers set the BGP next hop to the **DMS** offramp interface
- 3 All peers learn the DMS's MAC address via ARP/ND provided by the IXP's switching infra
- 4 Nokia DMS receives the traffic and send a sampled copy (SPM) to Nokia Deepfield Defender Controller
- 5 Nokia Deepfield Defender Controller automatically classifies the DDoS traffic and pushes the required action to the DMS to filter out the malicious traffic

# Budapest Internet Exchange deploys 400GE IP interconnect

Providing exceptional customer experience and sustainable capacity growth



## Budapest Internet Exchange (BIX)

- Carrier-neutral Internet exchange in Hungary, Central Europe and Balkans regions
- Needed to modernize, add capacity, lower power consumption

## Why Nokia?

- Ready for 800GE upgrades
- Power efficiency and cost savings
- High reliability
- Improved performance and user experience

## Solution

- FP-5 based 7750 SR-s system for IP interconnection and peering
- Starting with 400GE interfaces with ability to scale to 800GE



[Link to press release](#)



**THANK YOU!**

Oct-12, 2013

**NOKIA**