

NOKIA

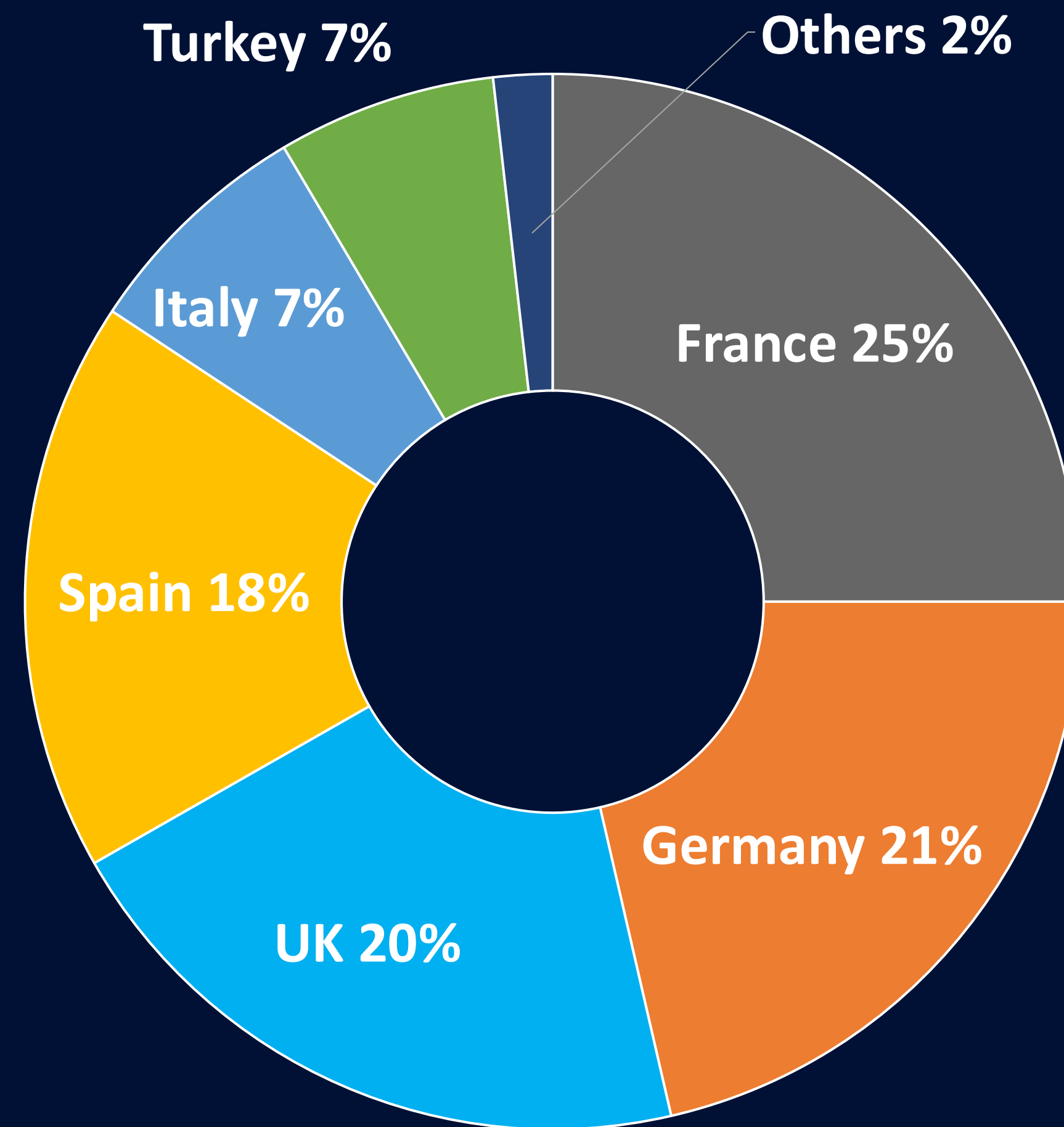
Defending the realm Deepfield in LINX

Azfar Aslam

Vice President & CTO, NI Europe



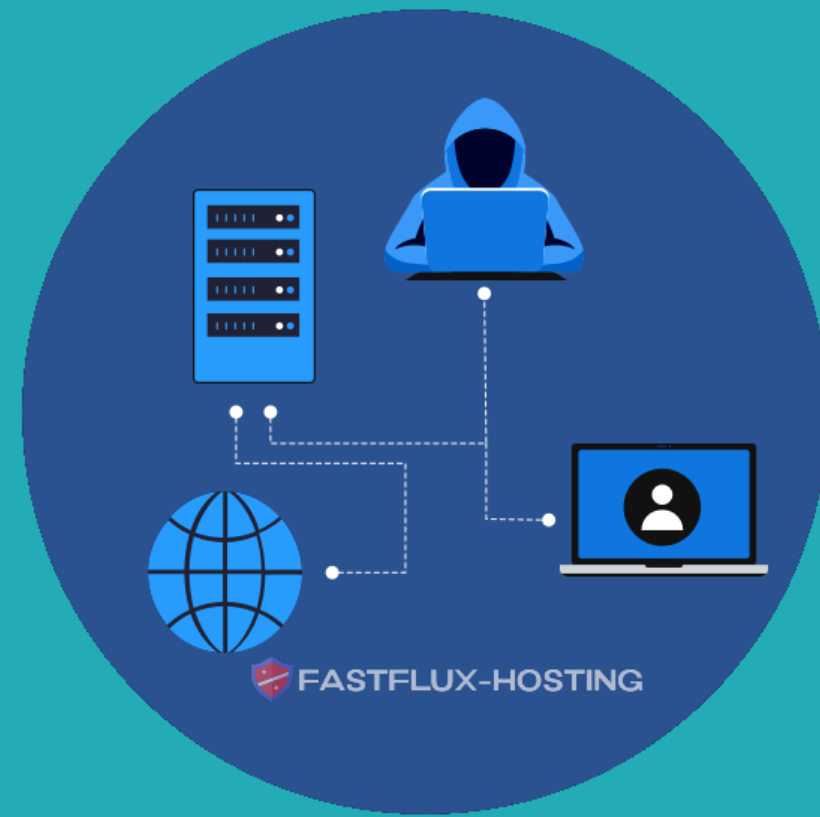
DDoS Attack Distribution Across Europe



ENISA Security report, 2023

DDoS: Shifting Attack Vectors

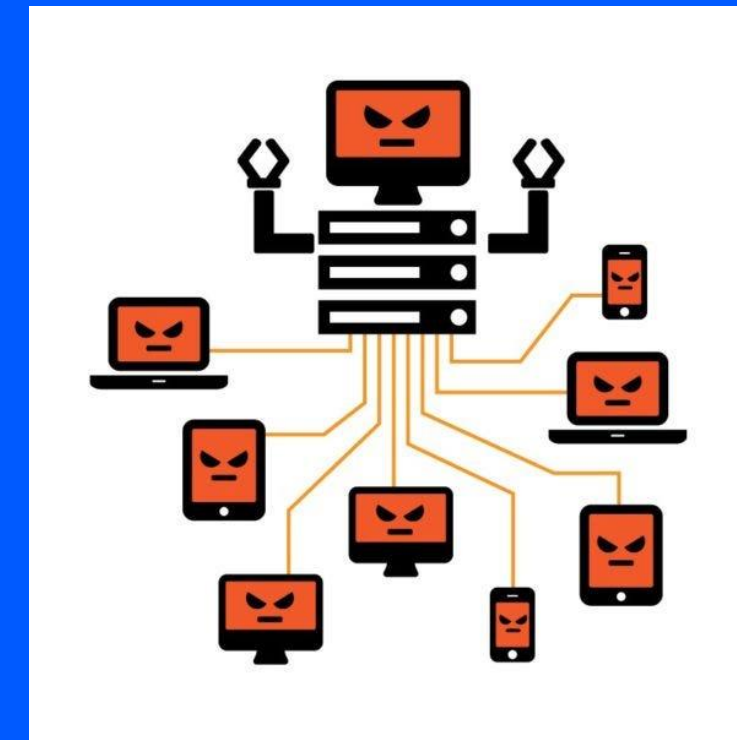
2000 – 2020
Spoofed



Small number of compromised machines generating spoofed traffic to victim or via misconfigured DNS, NTP, Memcache servers

Blocked on scrubber using SYN-cookie, port / protocol / packet size access control lists (ACLs) or policers

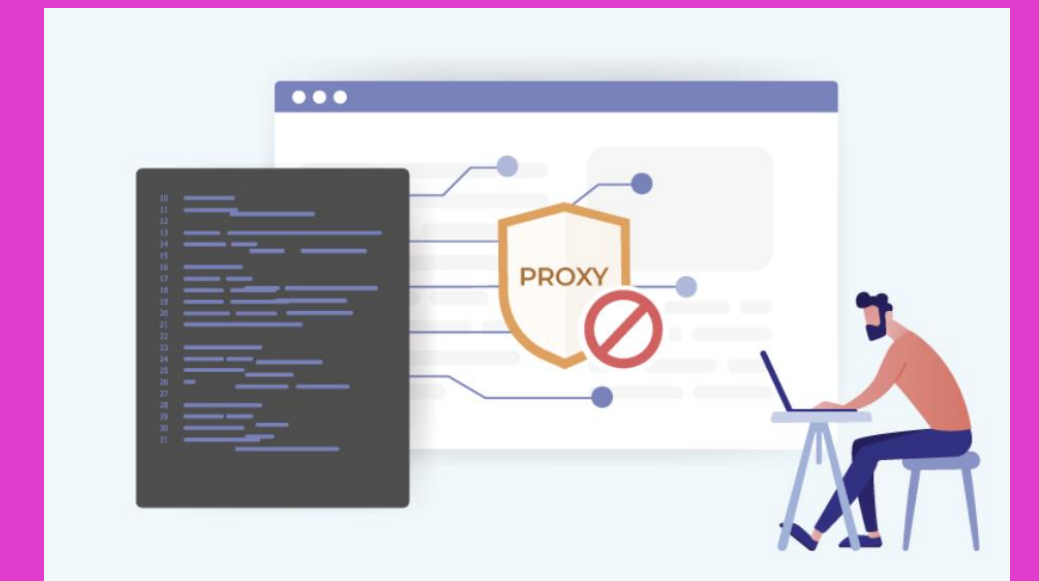
2020 – 2024
Botnet &
Industrialization
Of Attacks



Thousands of compromised IoT botnet devices generating traffic floods or sending realistic HTTP/DNS/VoIP requests to servers. GigE symmetric rollouts.

Difficult to mitigate using traditional DDoS mitigation appliances

2024+
AI & Proxies



Hundreds of thousands of residential proxies, compromised IoT sending realistic HTTP/DNS/VoIP requests to servers

High automation and attack variability. Both microburst and long-lived.

Compute

Bandwidth / Data

Speed / Automation

Attack Tools – Sophistication, Automation & Evasion

MHDDoS (on Github)

- 56 different methods
- Automated evasion for top cloud protection services
- Run through different methods



MHDDoS - DDoS Attack Script With 36 Method

(Code Lang - Python 3)

Please Don't Hit '.gov' and '.ir' Websites :)

Special graphs:

- Cloudflare (JAM-BFM)
- Cloudflare (Captcha)
- DDoS-Guard
- Incapiva
- Nooder
- Sucuri
- TOR site graph

Normal graphs:

- FDCServers NL #1 (300k rs)
- FDCServers NL #2 (300k rs)
- FDCServers US #2 (300k rs)
- FDCServers US #1 (300k rs)
- Amazon AWS (200k rs)
- TANDI (200k rs)
- Online-net (200k rs)
- Hetzner (150k rs)
- Cogent (150k rs)
- Morze (150k rs)

~ Layer 7 Dstats

JANDI
HIT - http://109.228.46.163/hit

REQUESTS PER SECOND OF 109.228.46.163



JOIN WITH US

```

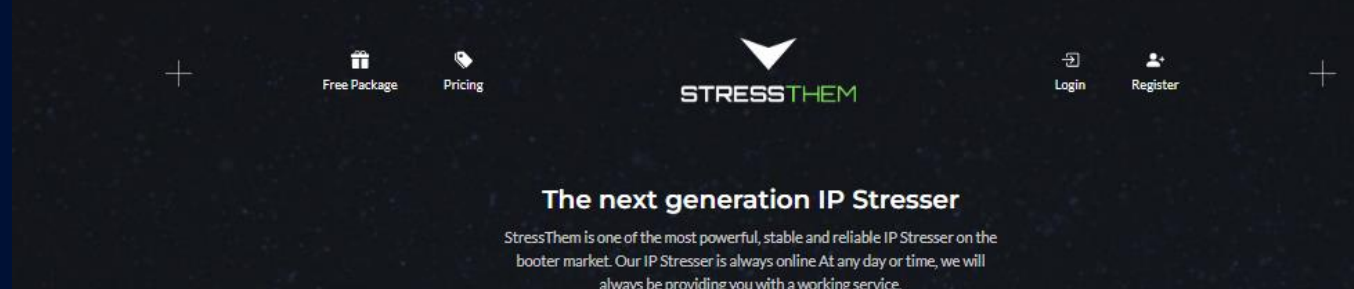
* Coded By MH_ProDev For Better Stresser
python3 start.py <method> <url> <socks_type5.4.1> <threads> <proxylist> <multiple> <timer>

> Methods:
- L3
| POD, ICMP | 2 Methods
- L4
| TCP, UDP, SYN, VSE, MEM, NTP | 6 Methods
- L7
| CFB, BYPASS, GET, POST, OVH, STRESS, OSTRESS, DYN, SLOW, HEAD, HIT, NULL, COOKIE, BRUST, PPS, EVEN, GSB, DGB, AVB | 19 Methods
- TOOLS
| CFIP, DNS, PING, CHECK, DSTAT, INFO | 6 Methods
- Other
| STOP, TOOLS, HELP | 3 Methods
- All 36 Method

example:
python3 start.py bypass https://madcraft.ir 5 872 socks5.txt 46 7126
    
```

Stressthem (aaS)

- DDoSaaS business model
- Multiple attack methods, simultaneous attacks, attack sizes
- Free trial...up to \$600/m



The next generation IP Stresser

Stressthem is one of the most powerful, stable and reliable IP Stresser on the boomer market. Our IP Stresser is always online. At any day or time, we will always be providing you with a working service.


- Try before you buy**
Give our free stress testing service a try with strong instant hitting attacks, create an account today.
- 1000 Gbit/s capacity**
With 1000 Gbit/s capacity we have one of the strongest services on the current market with packages to suit everyone.
- Anonymized payment**
At Stressthem we use Bitcoin payment processor for fast and secure payments to ensure customer privacy and security.

Create account & boot for free!

Free Testing for everyone

Try our Free Service today, we have the most powerful free IP Stresser on the market, create an account and boot for free!

Create account & boot for free!



All pricing plans

Plan	Price (USD)	Attacks Per Day	Attack Time	Consumption	Premium Methods	Premium Network
PREMIUM-1	30.00	Unlimited	20 min	1	✓	✓
PREMIUM-2	90.00	Unlimited	30 min	3	✓	✓
PREMIUM-3	150.00	Unlimited	1h	5	✓	✓
PREMIUM-4	300.00	Unlimited	30 min	3	✓	✓
PREMIUM-5	450.00	Unlimited	30 min	3	✓	✓
PREMIUM-6	600.00	Unlimited	30 min	3	✓	✓

Trends Impacting CSP/Enterprise



High Water Mark Growth (bps) YoY

Source: Nokia Deepfield 2024



Automated "Soft Spot" Attacks



Automation & "DDoS Middleware Market" Reducing the Cost

Our approach: Big data + AI/ML-driven DDoS security

Beating them at their game...

Use large,
high-quality
data sets

- Deepfield DDoS Library
- 10,000+ attacks from real networks

Maintain 'maps' of
the internet;
fingerprint apps and
traffic incl. DDoS

- Deepfield Cloud Genome®
- Deepfield Secure Genome®

Create dynamic
traffic models and
monitor traffic in
real time

- Deepfield Defender
- Mitigation Compiler Engine

Capitalize on
processing power of
network processors

- Across all FP platforms
- FP4, 5, Cx

NOKIA