A10

Always Secure. Always Available.

The Global State of DDoS Weapons, Threat Intelligence and Attack Mitigation

ITNOG6 – Bologna 16th September 2022

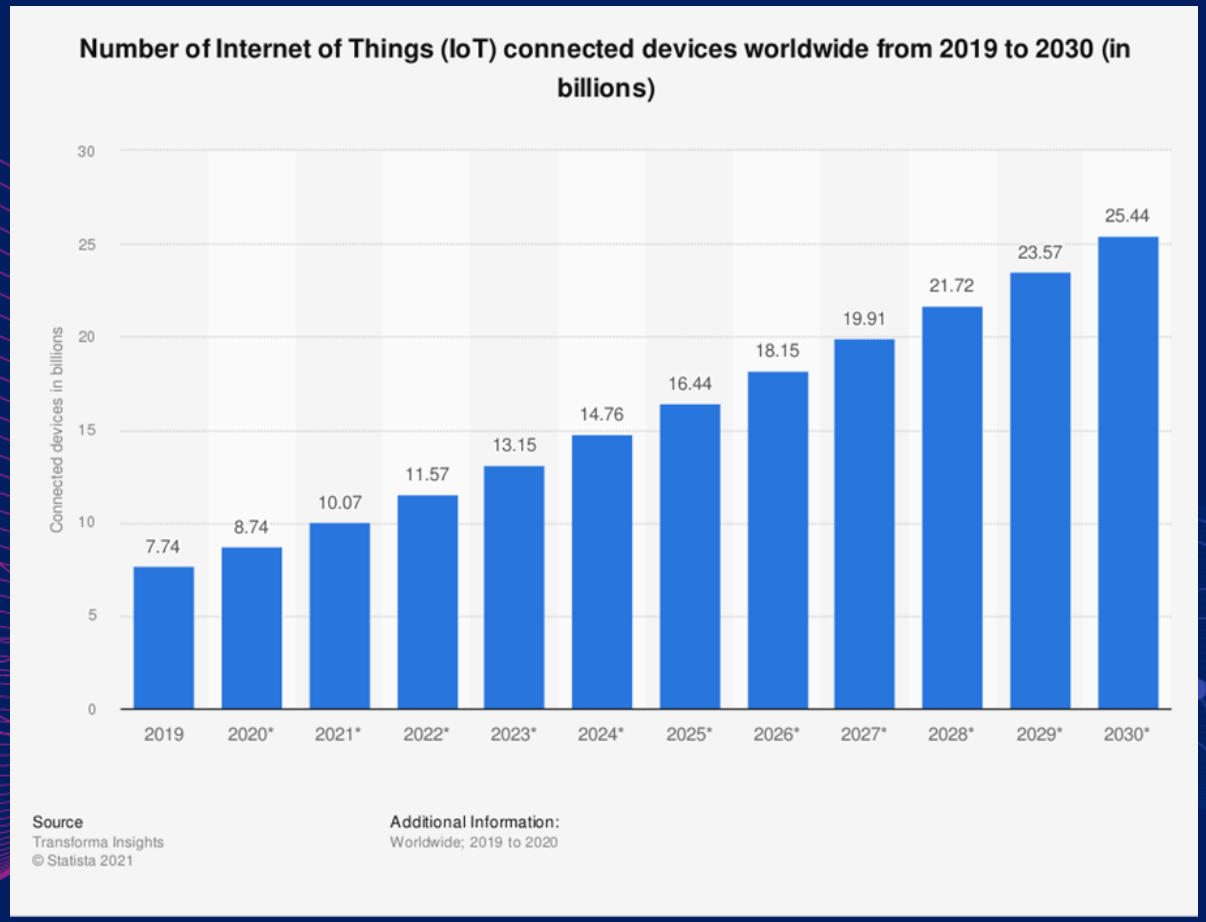
Roberto Lucarelli – Senior System Engineer A10 Networks
rlucarelli@a10networks.com

A10 Security Research

Agenda

- The Evolution of DDoS Attacks
- A10 Research Key Insights and Trends
- A10 Research Spotlights
- The Need for a Proactive DDoS Defense Strategy

The Attack Surface is Growing



IoT Proliferation

Shift to Cloud

WFH

5G Deployment

Most attacks are much smaller and fly under the radar for Enterprises

15% faced over 100 attacks in a year during the pandemic[1]

69% reported DDoS attacks that were under 10 Gbps[1]

Sources: *IDC*

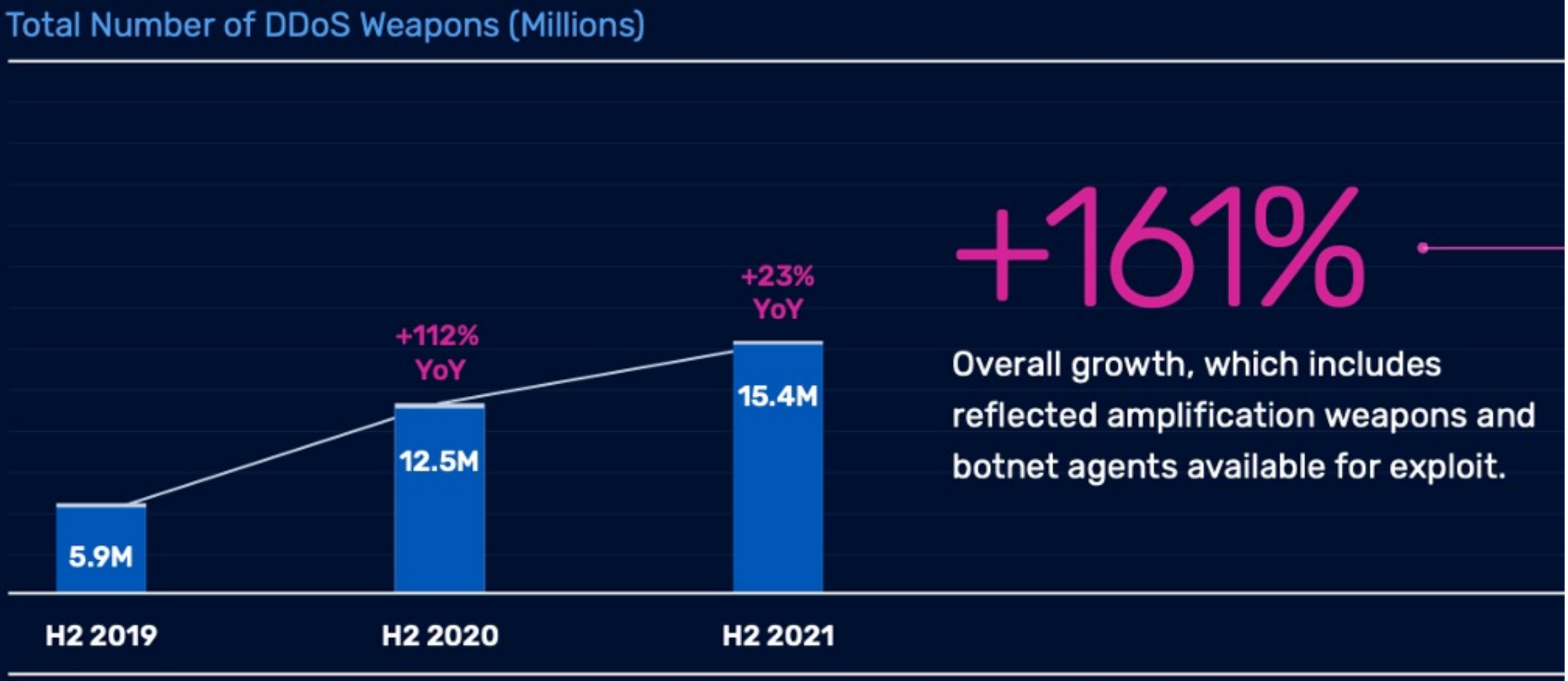
Tracked by A10 Networks

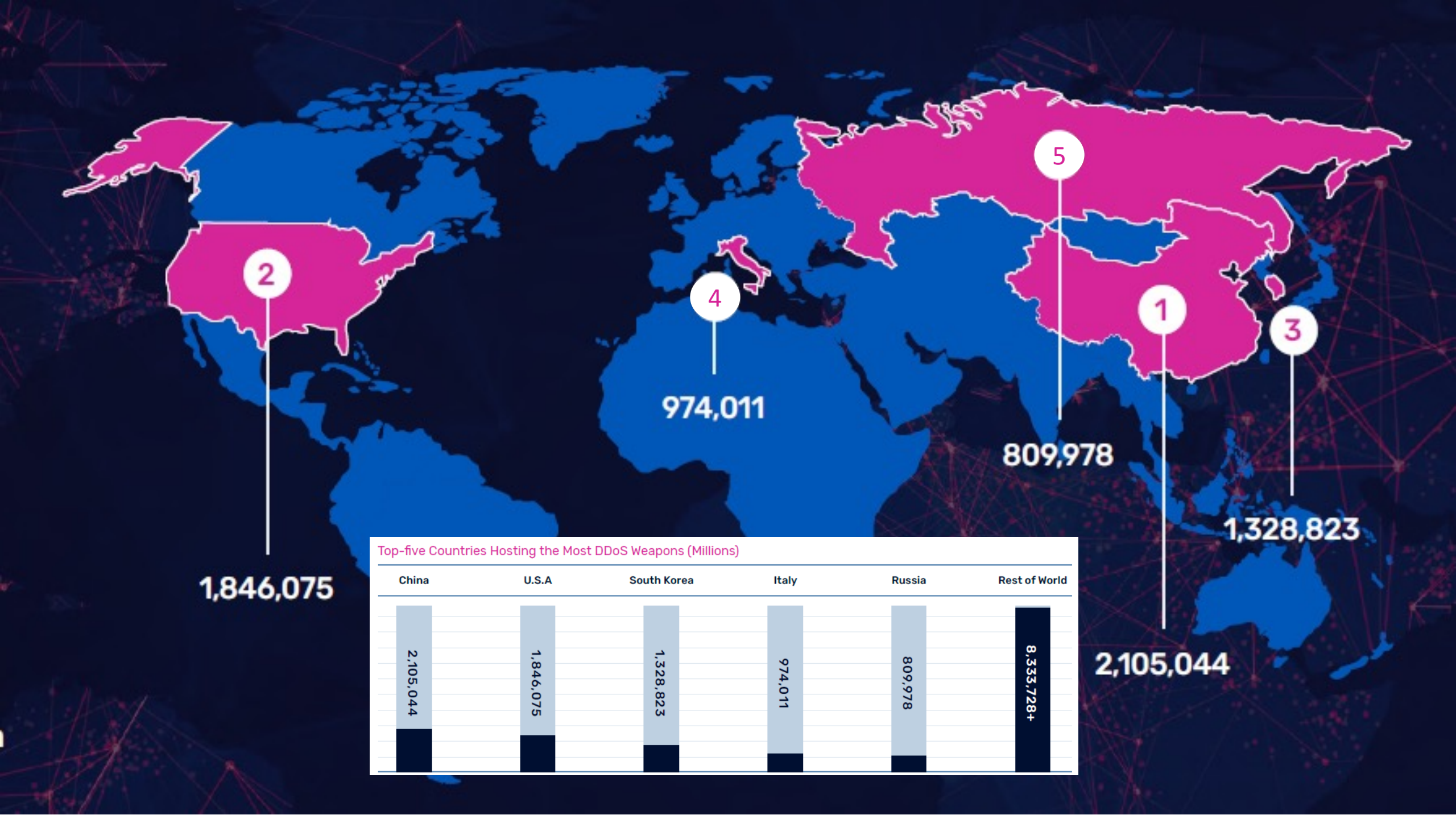
Approximately

15.4 Million

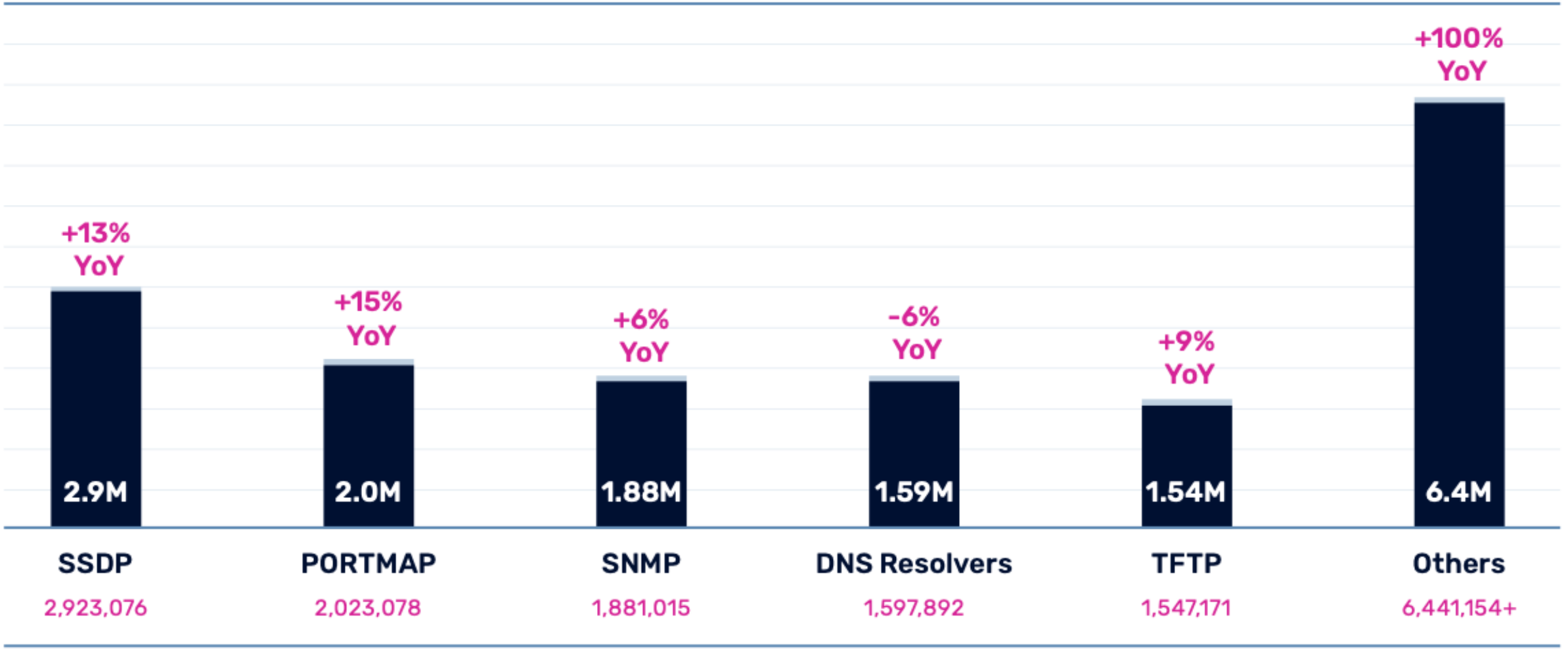
Unique DDoS Weapons

DDoS weapons tracked by A10 Networks almost tripled in two years.




2
1,846,075
4
974,011
5
809,978
1
2,105,044
3
1,328,823
Top-five Countries Hosting the Most DDoS Weapons (Millions)
China
2,105,044
U.S.A
1,846,075
South Korea
1,328,823
Italy
974,011
Russia
809,978
Rest of World
8,333,728+

Top Tracked DDoS Weapons by Size



30x

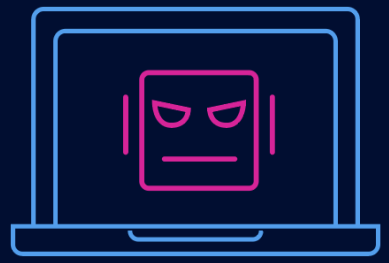
SSDP-based DDoS attacks can generate more than 30x traffic volume making them some of the most devastating attacks

Tracked by A10 Networks

Approximately

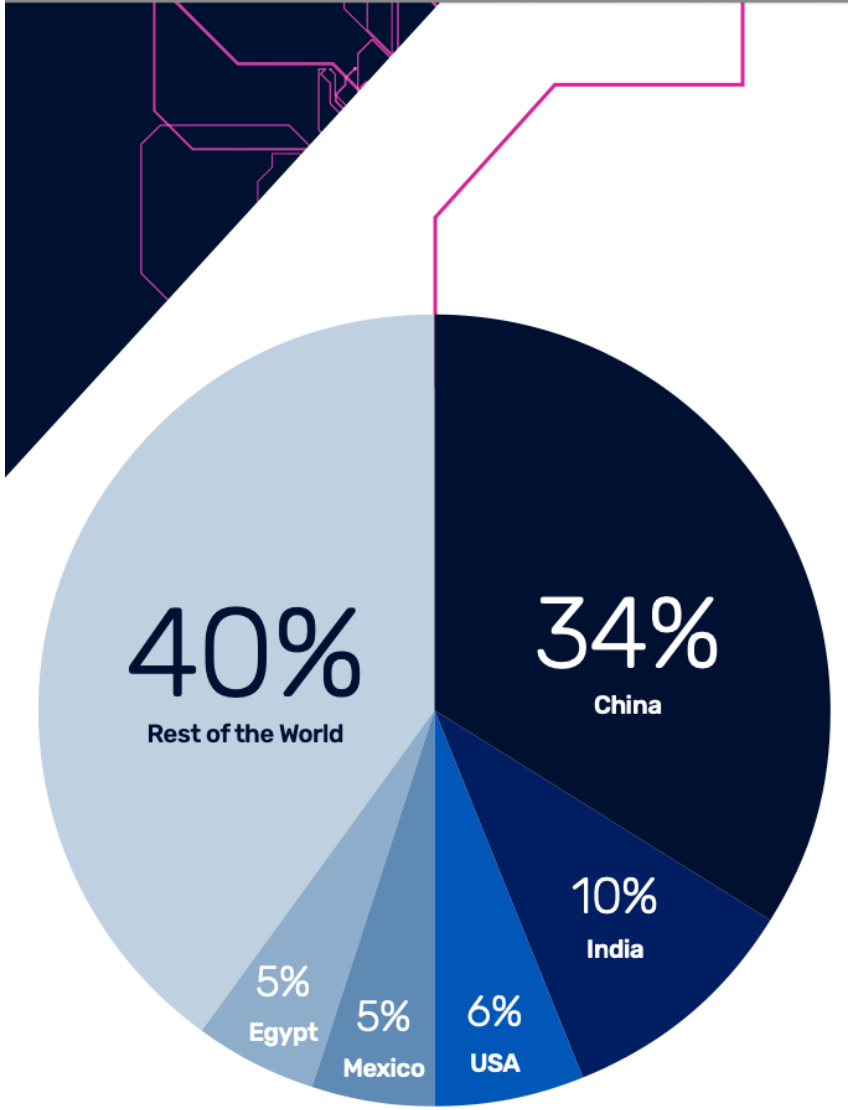
423,096

Botnet agents that are repeatedly used in DDoS attacks



Top Hosts of Drones and Botnets

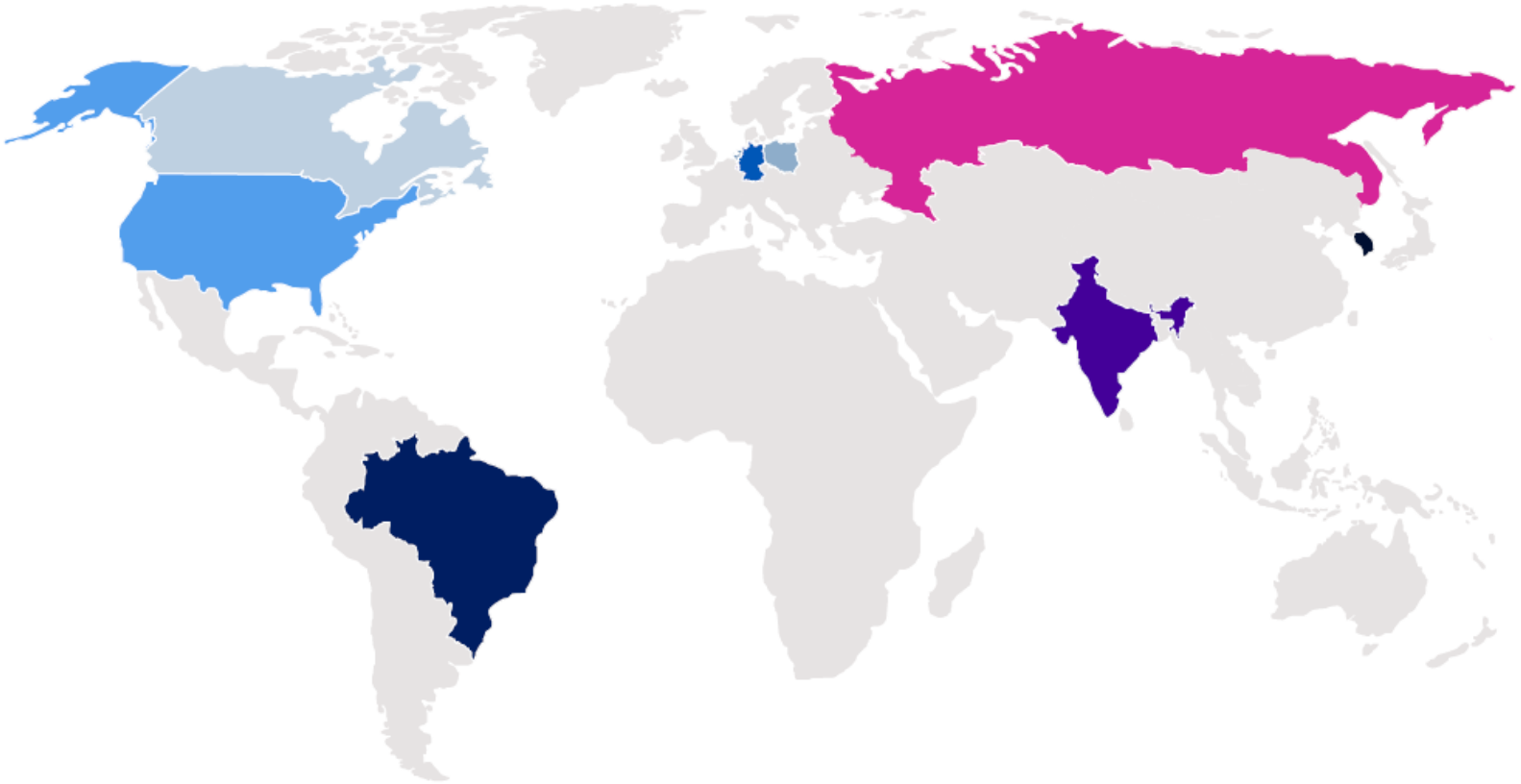
- A10 Networks scans for hosts exhibiting malware-infected characteristics
  - Accumulates knowledge of repeatedly used hosts in DDoS attacks
- The total number of bots experienced a decrease for the second year in a row
  - China experienced a 42% decrease
  - India experienced a 33% decrease
  - The United States experienced a 3% increase
- The decrease can be attributed to factors including:
  - Large-scale security updates to patch CVEs in IoT
  - Botnet takedowns



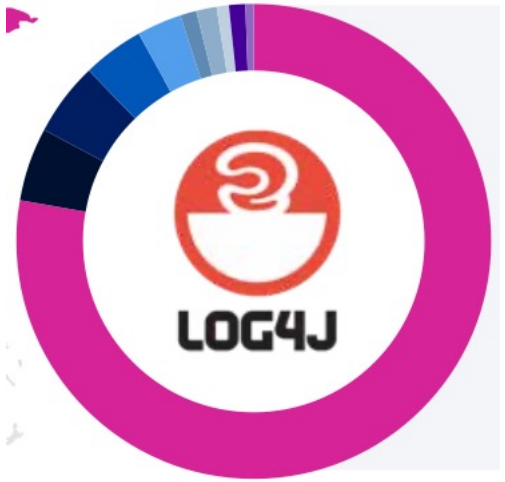
Top Countries/Regions Hosting DDoS Botnet Agents

Research Spotlights
Log4J and Cyber Warfare

Spotlight – The Log4j Vulnerability and DDoS



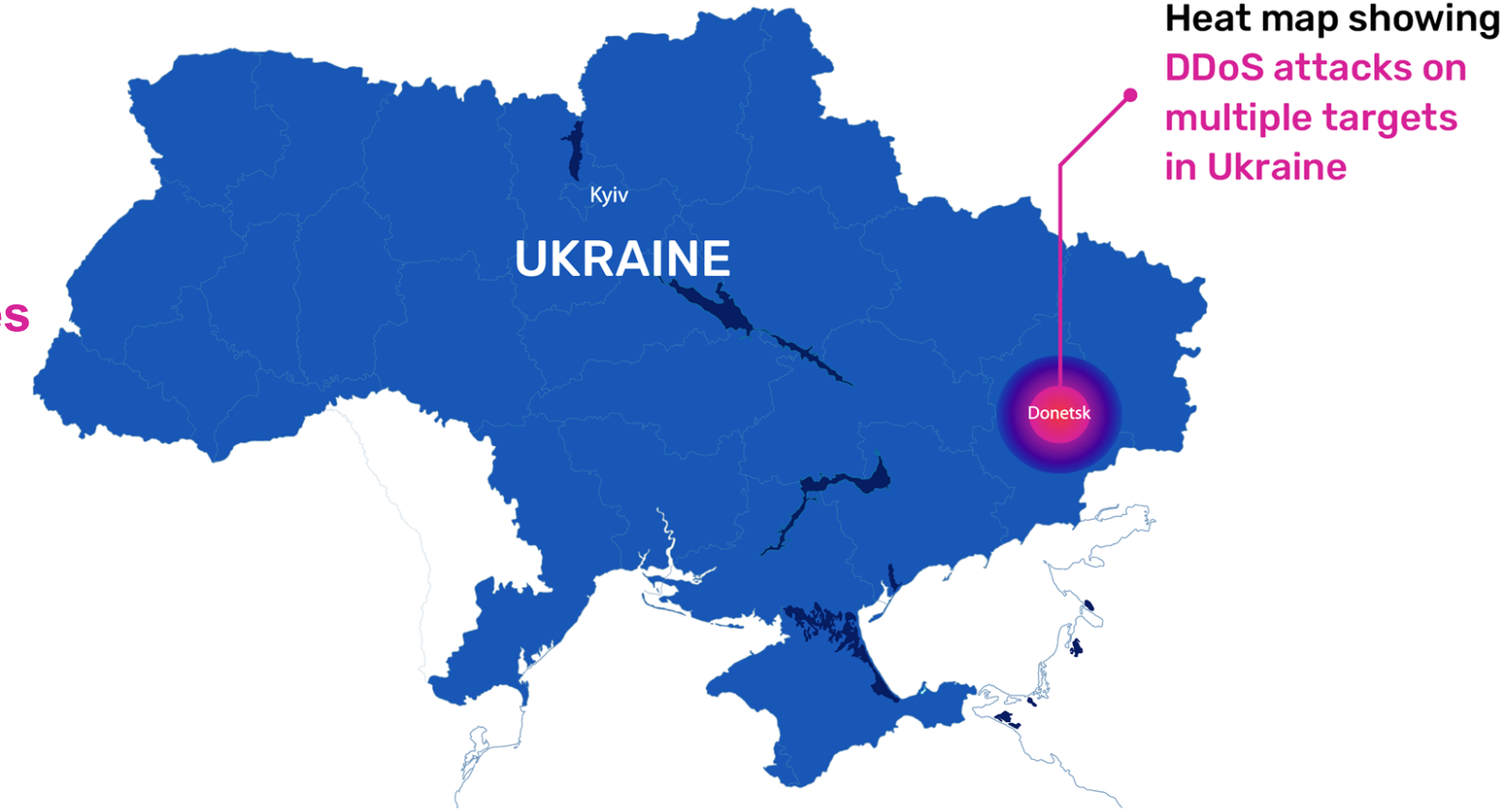
- Russia
- South Korea
- Brazil
- Germany
- United States
- Netherlands
- Poland
- Canada
- India
- Luxembourg



More than 75% Log4J Scanners originated from Russia

Spotlight - Cyber Warfare and DDoS

Apple Remote Desktop (ARD) protocol on UDP port 3,283. This protocol has an **amplification factor of 34 times** larger than the original request.



DDoS Defense is Essential to Ensure Critical Services and Infrastructure are Protected

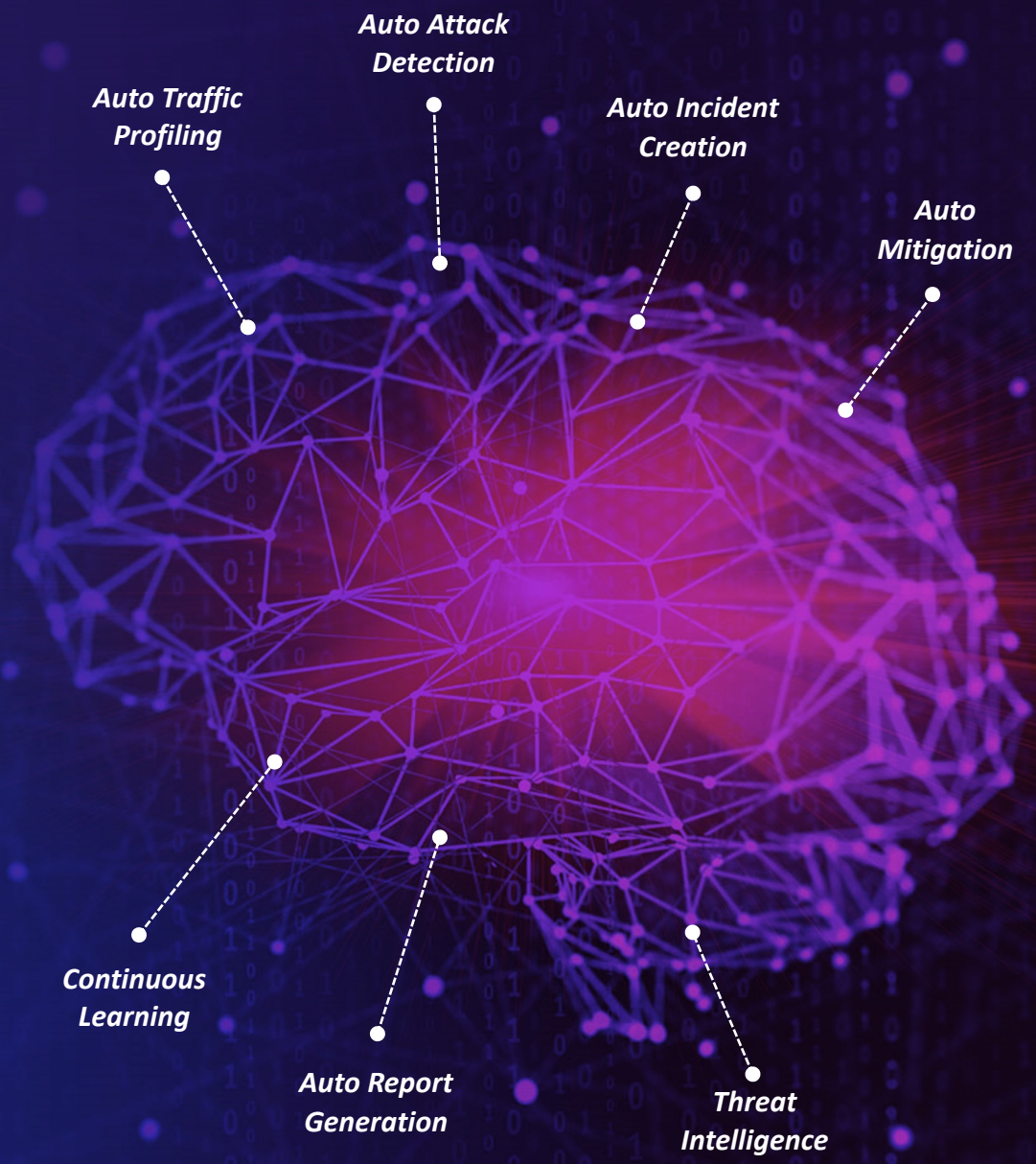
Proactive DDoS Defense Is the Only Way Forward

Automate DDoS Defenses
to protect against all DDoS attacks including zero-day attacks

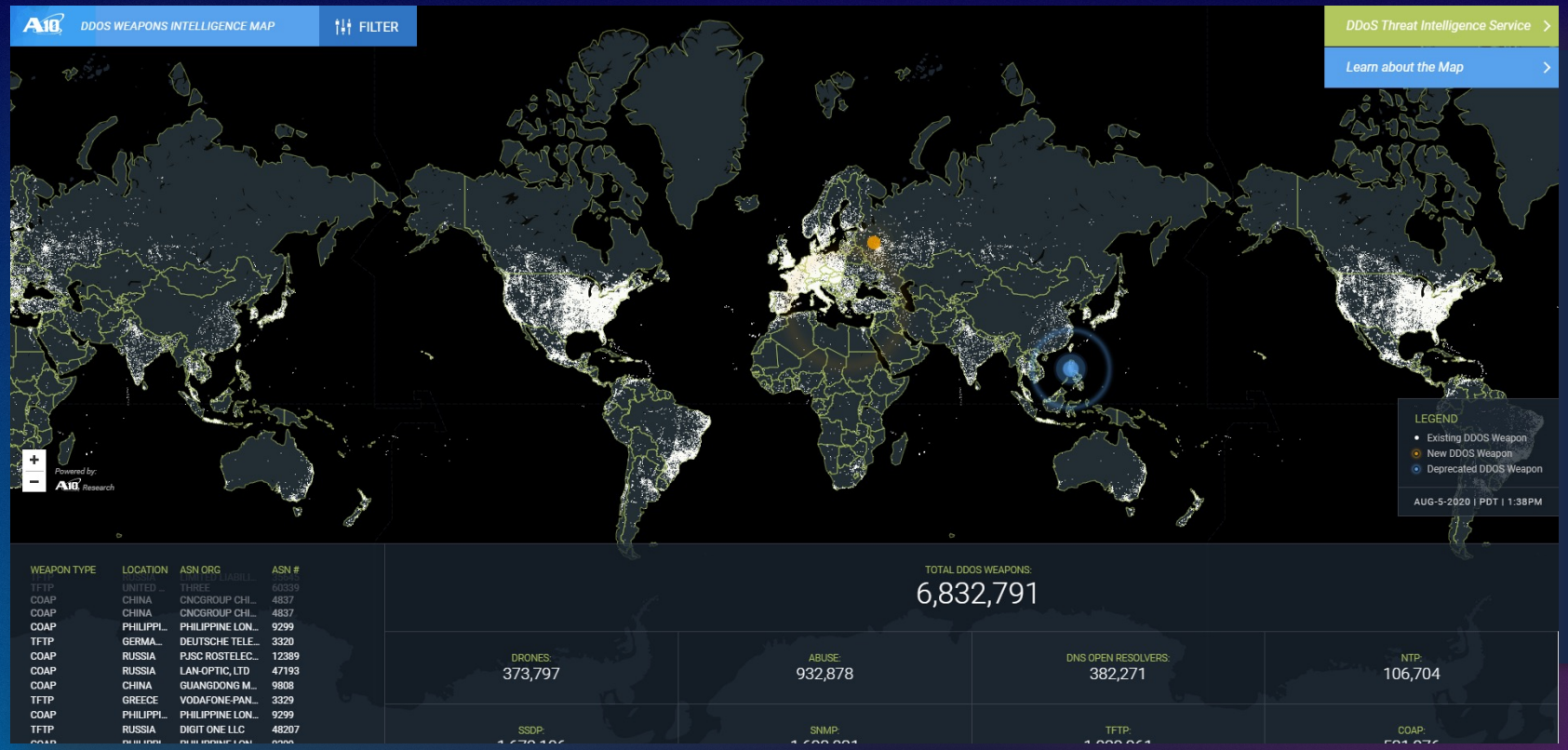
Implement Zero Trust
to identify, isolate and stop the spread of malware and the propagation of DDoS

Monitor your Network
to ensure networks are not weaponized and used against the internet

Modern DDoS Protection Requires
Intelligent Automation
& Machine Learning



DDoS Weapons Intelligence Map



Helps visualize the DDoS Threat landscape

- Provides proactive insights into where the next attack might come from

Visualizes DDoS weapons including drones, amplification sources and more

View the map at https://threats.a10networks.com/