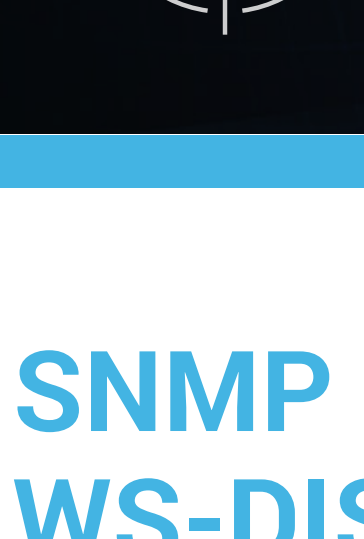


DDOS WEAPONS & ATTACK VECTORS

A10 Networks tracked nearly **6 million DDoS weapons in Q4 2019.**

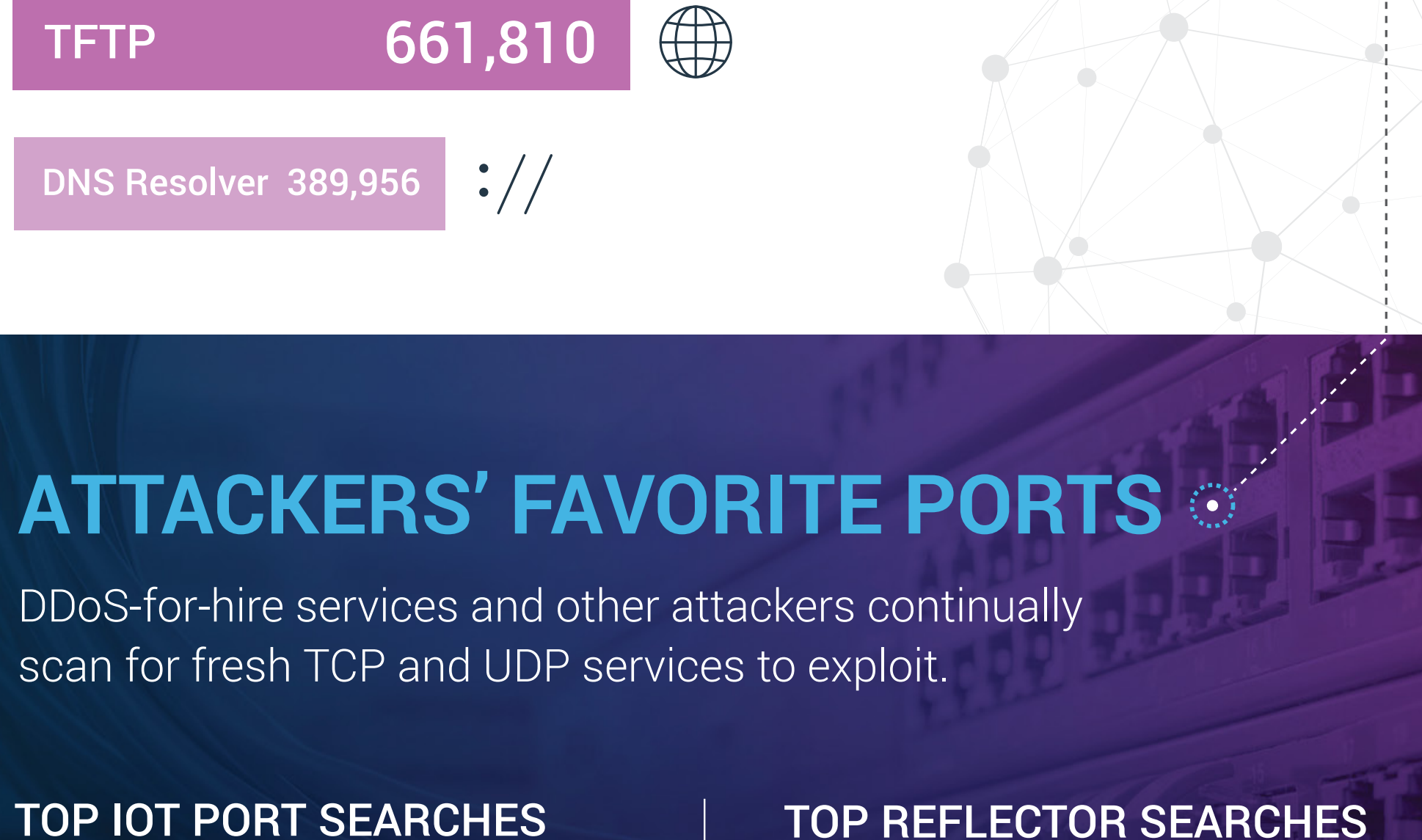
Here's what we learned and what you need to know about the threats targeting you today.



SNMP LEADS, WHILE WS-DISCOVERY TRENDS

SNMP and SSDP remain the top sources for DDoS attacks, but we tracked nearly 800,000 WS-Discovery sources for exposed reflection amplification as well.

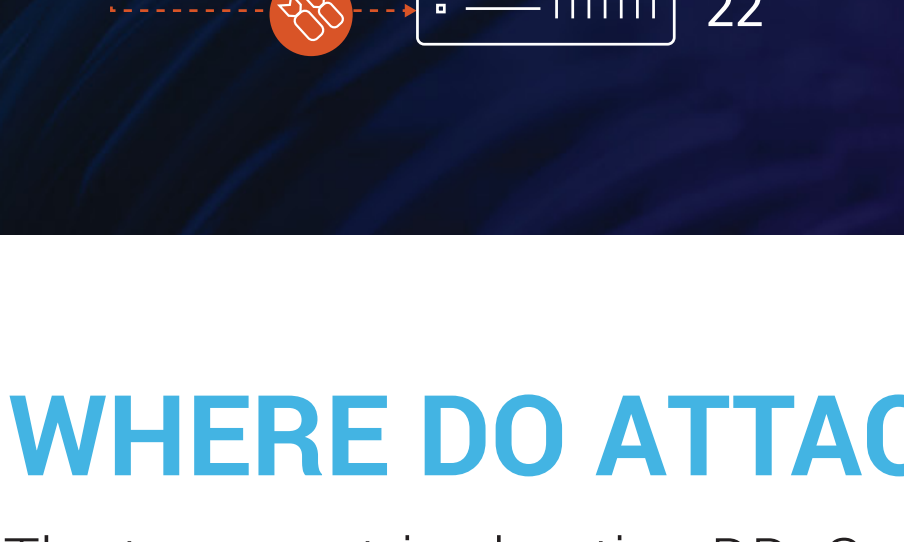
TOP TRACKED DDOS WEAPONS



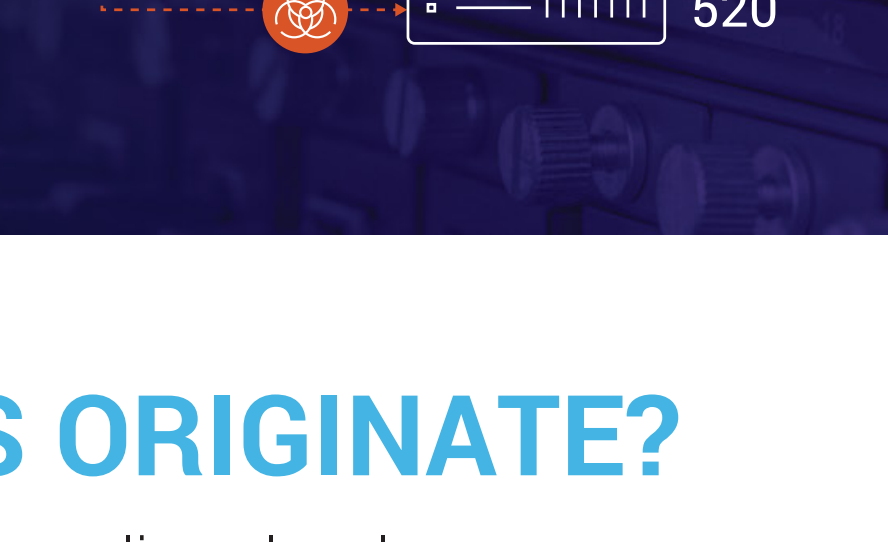
ATTACKERS' FAVORITE PORTS

DDoS-for-hire services and other attackers continually scan for fresh TCP and UDP services to exploit.

TOP IOT PORT SEARCHES



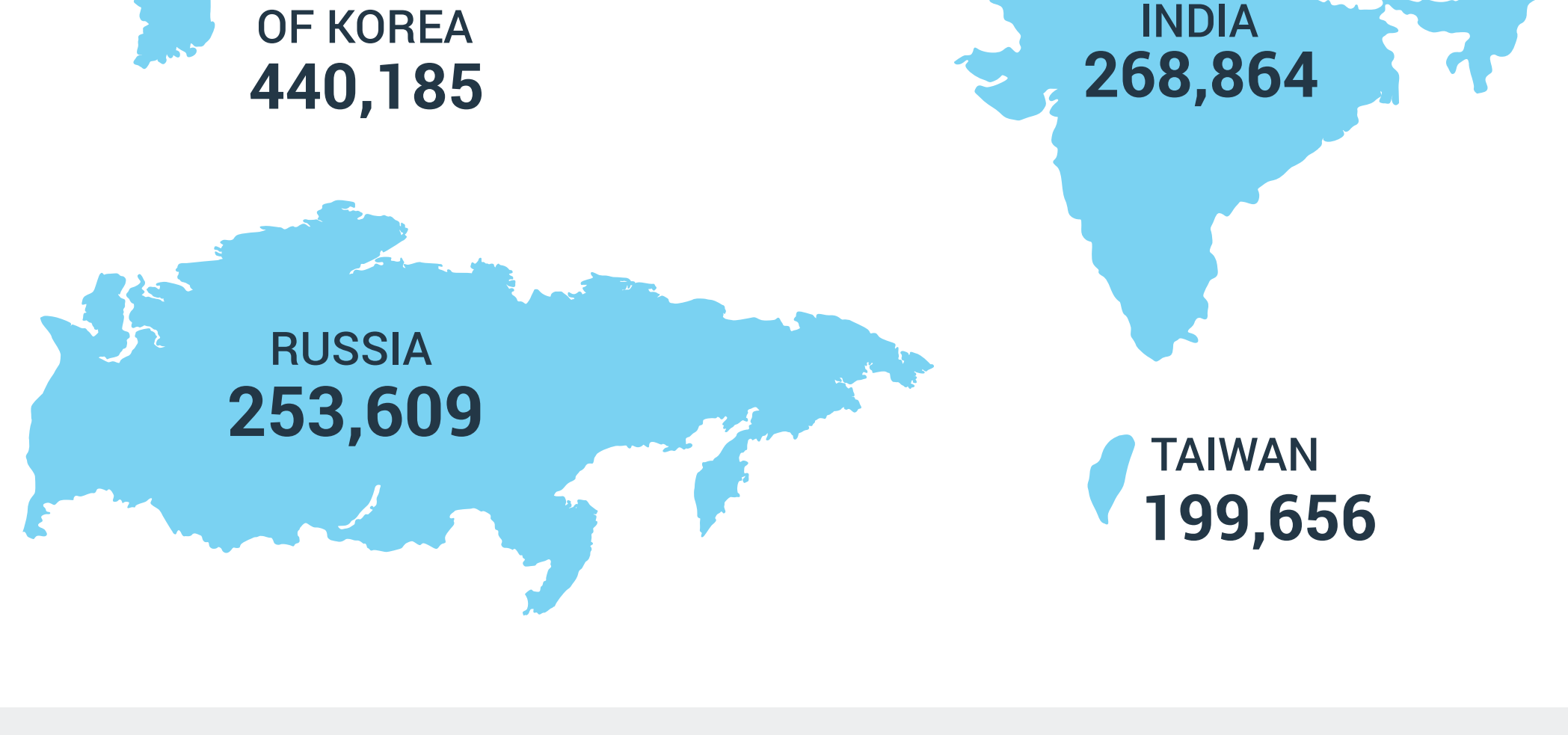
TOP REFLECTOR SEARCHES



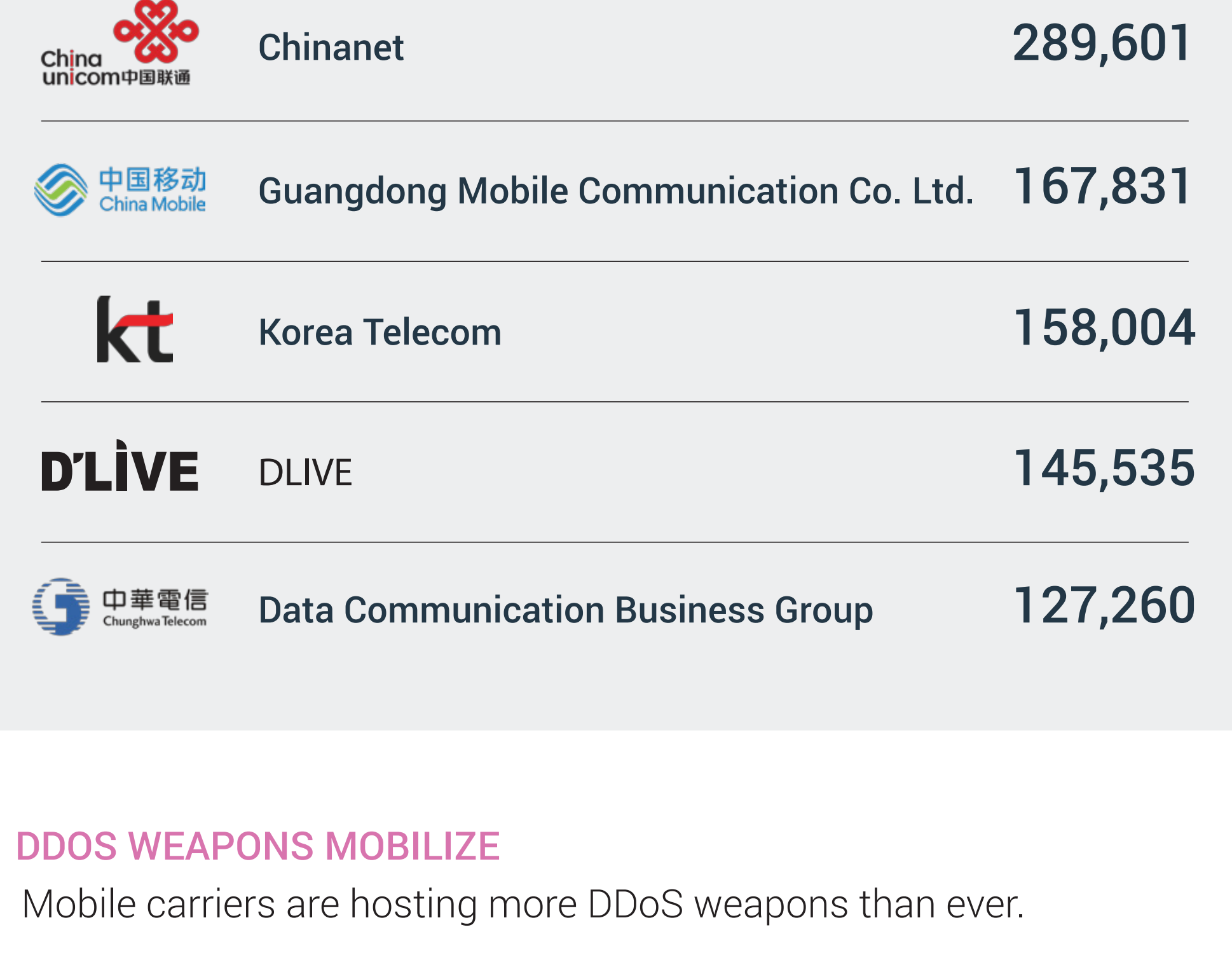
WHERE DO ATTACKS ORIGINATE?

The top countries hosting DDoS weapons align closely with the top ASNs where they connect.

TOP COUNTRIES

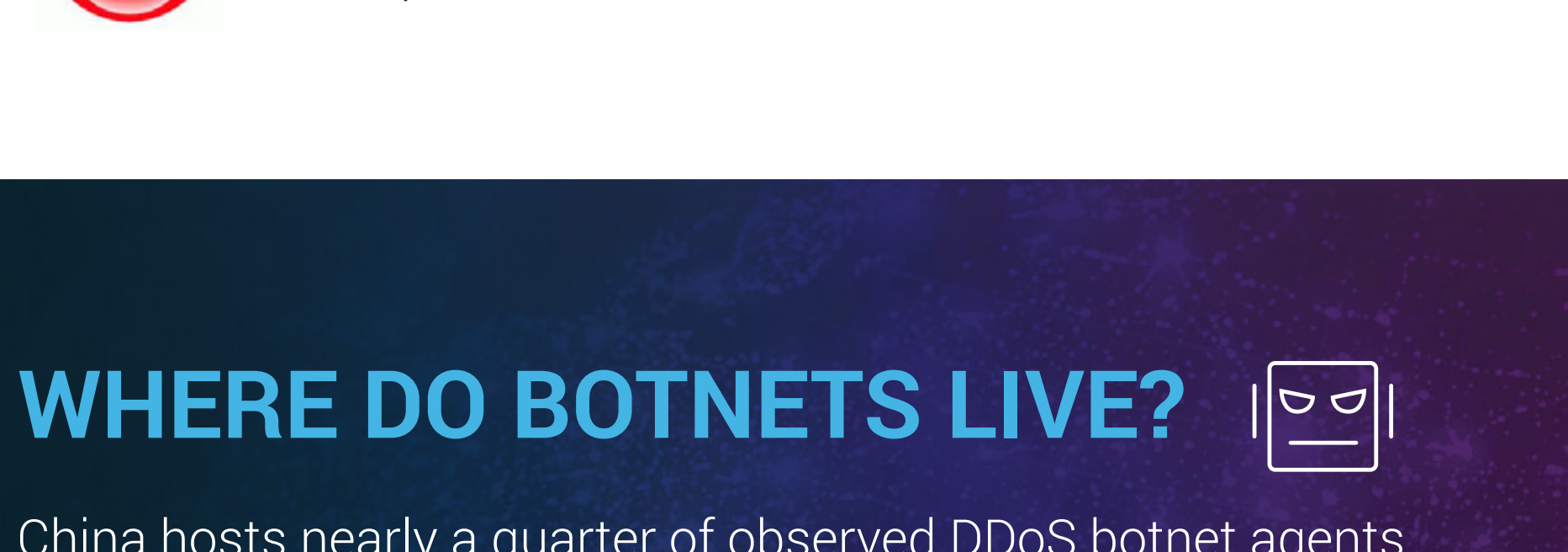


TOP ASNS



DDOS WEAPONS MOBILIZE

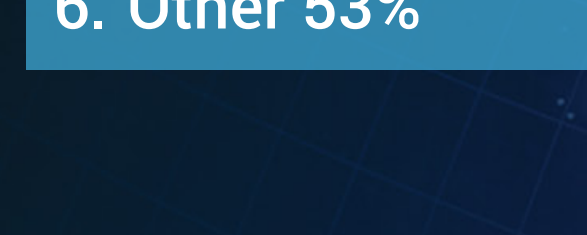
Mobile carriers are hosting more DDoS weapons than ever.



WHERE DO BOTNETS LIVE?

China hosts nearly a quarter of observed DDoS botnet agents but attacking drones are most often seen in Brazil.

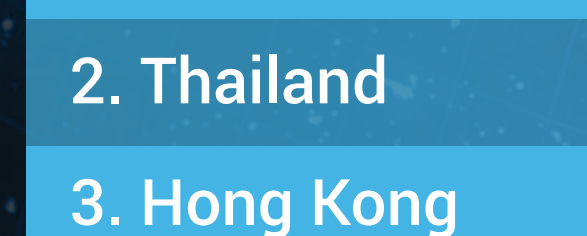
TOP COUNTRIES HOSTING DDOS BOTNET AGENTS



TOP ASNS HOSTING DDOS BOTNET AGENTS



TOP COUNTRIES WHERE ATTACKING BOTNET AGENTS ARE OBSERVED



MIRAI LOVES IOT AND CAN'T WAIT FOR 5G

Connected devices are expanding exponentially and they offer fertile ground for DDoS botnets. 5G will supercharge that growth. The Mirai malware family leads the pack so far.

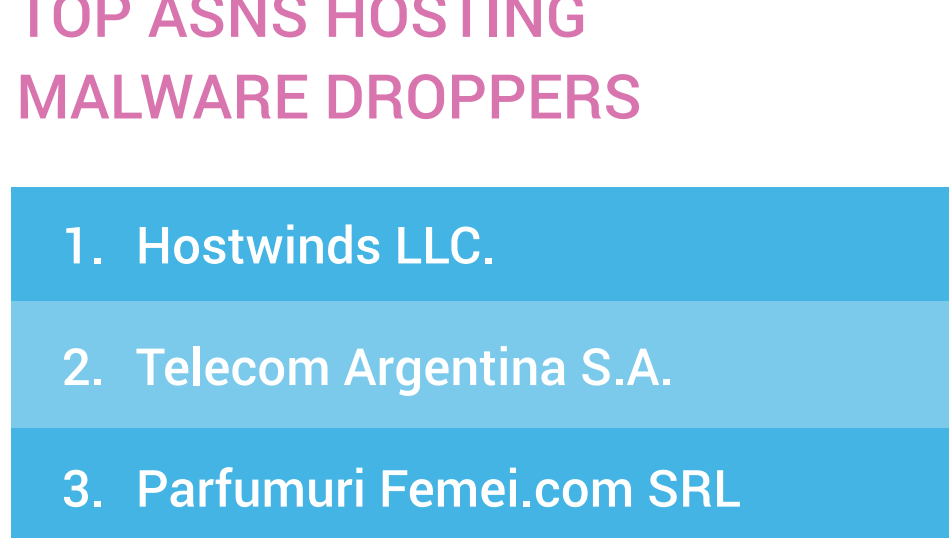
TOP MIRAI BINARIES TARGETING IOT

Family Name	Binary Name
Mirai	blxntz.x86
Mirai	a.x86
Mirai	yakuza.x86

TOP COUNTRIES HOSTING MALWARE DROPPERS



TOP ASNS HOSTING MALWARE DROPPERS



DDOS ATTACKS GET AMPLIFIED

With reflected amplification, attackers exploit UDP-based protocols to launch the largest DDoS attacks ever seen.

TOP REFLECTED AMPLIFICATION PROTOCOLS AND COUNTRIES OF ORIGIN



WS-DISCOVERY IS OPENING IOT DEVICES TO ATTACKERS

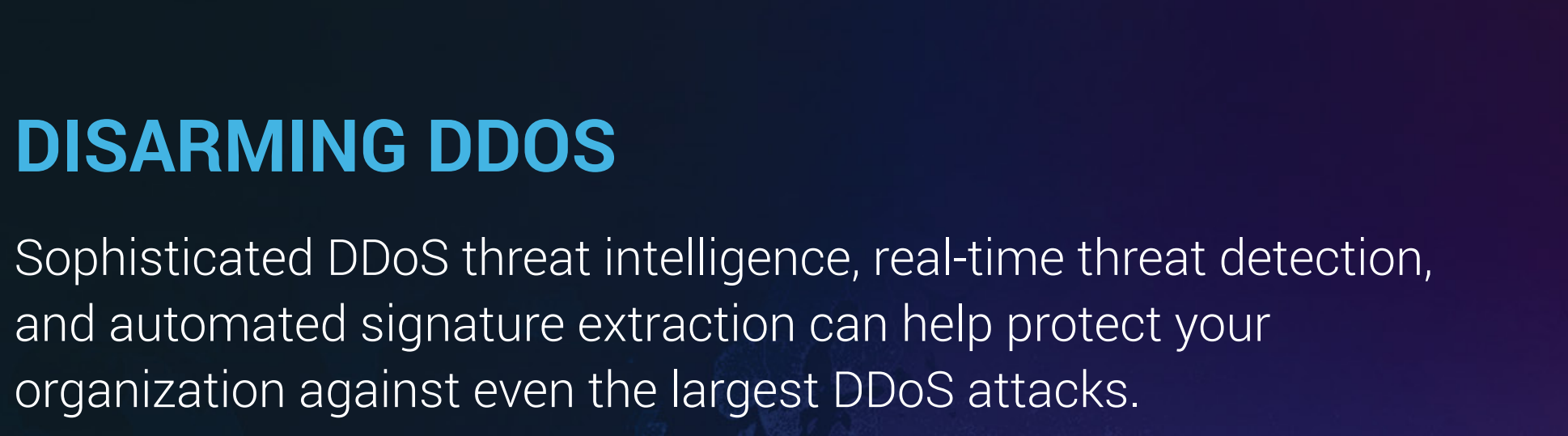
Attackers are flocking to internet-exposed IoT devices running the UDP-based WS-Discovery protocol to launch amplified reflection DDoS attacks.



IT'S NOT WHERE YOU THINK
Less than half of WS-Directory attacks respond on port 3702.

54% use high ports.

BRANDS OF CHOICE FOR WEAPONIZED WS-DISCOVERY



DISARMING DDOS

Sophisticated DDoS threat intelligence, real-time threat detection, and automated signature extraction can help protect your organization against even the largest DDoS attacks.

Learn more at <https://threats.a10networks.com>.

