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

SNMP	1,390,505
SSDP	1,196,798
WS-Discovery	781,147
TFTP	661,810
DNS Resolver	389,956

ATTACKERS' FAVORITE PORTS

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

TOP IOT PORT SEARCHES TCP PORT

TCP Port #
23
60001
8080
5555
2323
80
22

TOP REFLECTOR SEARCHES UDP PORT

UDP Port #
69
623
5683
5353
53
523
520

WHERE DO ATTACKS ORIGINATE?

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

TOP COUNTRIES

- CHINA 739,223
- USA 448,169
- REPUBLIC OF KOREA 440,185
- INDIA 268,864
- RUSSIA 253,609
- TAIWAN 199,656

TOP ASNS

Chinanet	289,601
Guangdong Mobile Communication Co. Ltd.	167,831
Korea Telecom	158,004
DLIVE	145,535
Data Communication Business Group	127,260

DDOS WEAPONS MOBILIZE

Mobile carriers are hosting more DDoS weapons than ever.

Guangdong Mobile Communication Co. Ltd
Top reflected amplifier source

Claro S.A.
Top malware drone source

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

1. China 24%
2. Brazil 9%
3. Iran 6%
4. Taiwan 4%
5. Thailand 4%
6. Other 53%

TOP ASNS HOSTING DDOS BOTNET AGENTS

- CHINA UNICOM China169 Backbone
- No.31, Jin-rong Street
- Data Communication Business Group
- TOT Public Company Limited
- Telfônica Brasil S.A.
- Iran Telecommunication Company PJS

TOP COUNTRIES WHERE ATTACKING BOTNET AGENTS ARE OBSERVED

1. Brazil
2. Thailand
3. Hong Kong
4. India
5. Russia

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

1. United States
2. Hong Kong
3. Argentina
4. Romania
5. Hashemite Kingdom of Jordan
6. South Korea

TOP ASNS HOSTING MALWARE DROPPERS

1. Hostwinds LLC.
2. Telecom Argentina S.A.
3. Parfumuri Femei.com SRL
4. ColoCrossing
5. Jordan Data Communications Company LLC
6. Korea Telecom

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

SNMP
United States
Republic of Korea
India
Brazil
Japan

SSDP
China
Republic of Korea
Venezuela
Taiwan
Japan

WS-Discovery
Vietnam
Brazil
Republic of Korea
United States
China

TFTP
China
United States
Canada
India
Russia

DNS Resolver
Russia
United States
China
Brazil
Ukraine

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.

Over 800,000
WS-Directory hosts available for exploitation

UP TO 95X
Observed amplification factor

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

Which camera/DVR manufacturers are exploited the most?

Dahua	IntelBras	Hikvision
112,000 devices	42,000 devices	31,000 devices

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.

A10-GR-70344-EN-01 FEB 2020