Q1, 2019

THE STATE OF DDOS WEAPONS

SPECIAL REPORT BY A10 SECURITY RESEARCH

A10

EXECUTIVE SUMMARY

DDoS attacks continue to grow in frequency, intensity and sophistication. However, the delivery method of using infected botnets and vulnerable servers to perform crushing attacks at massive scale has not changed. Unlike traditional security methods, where attackers leverage obfuscation to prevent detection, the loud distributed nature of DDoS attacks create opportunities for defenders to take a proactive approach by focusing on the weapon's location.

Reflected Amplification Weapons

Attackers leverage vulnerabilities in the UDP protocol to spoof the target's IP address and exploit vulnerabilities in servers that initiate a reflected response. This strategy amplifies the attack by producing server responses that are much larger than the initial requests.

DDoS Botnet Weapons

Attackers leverage malware infected computers, servers and IoT devices that are under the control of a bot herder. The resulting botnet is used to initiate stateful and stateless volumetric, network, and application layer attacks.

Key Insights From This Report

- TFTP reflected amplification weapons creep into top 5 weapon category
- 414,130 weaponized IoT CoAP reflected amplifier devices identified
- DDoS weapons swelled in Spain to make it the third highest hosted country
- Uptick in scanning activity for SQL reflectors over UDP port 1434

DDoS weapons tracked by A10:

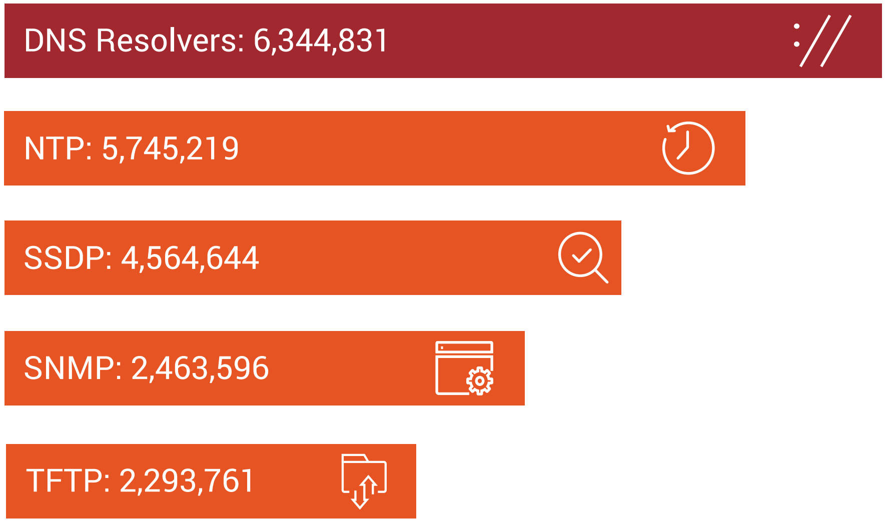
23,487,185

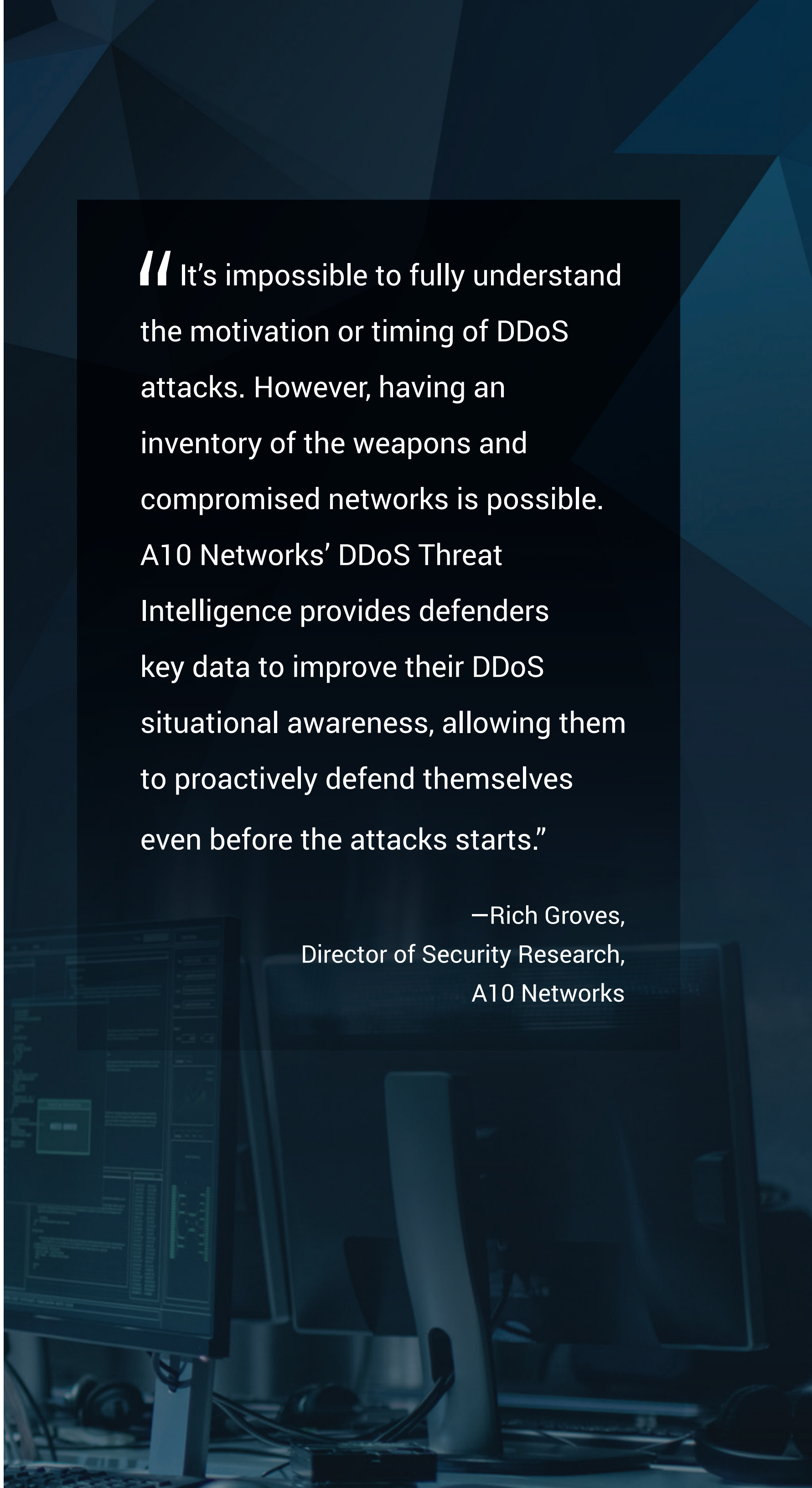
DDOS WEAPONS INTELLIGENCE

IDENTIFY AND ENUMERATE THE ORIGIN OF DDOS ATTACKS

Threat researchers gather DDoS weapons intelligence by closely monitoring attack agents orchestrated by botnet command and control (C2), deploying honeypots and scanning the internet for exposed reflection sources. A10 and our partner security researchers accumulate millions of IP addresses of exploited hosts that are regularly used in DDoS attacks. This data is used to create voluminous feeds that include tens of millions of entries. To make the data go beyond informational to actionable, A10 solutions have class-lists with millions of entries to create surgical black and white lists.

TOP TRACKED DDOS WEAPONS BY SIZE





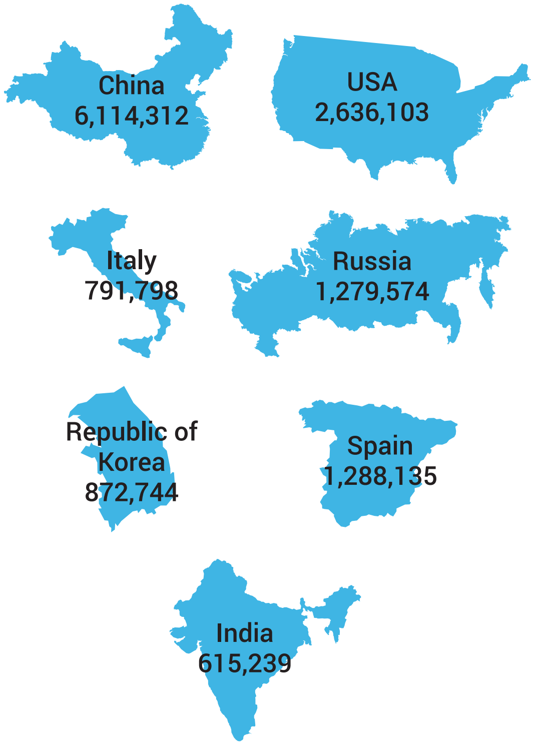
> “It’s impossible to fully understand the motivation or timing of DDoS attacks. However, having an inventory of the weapons and compromised networks is possible. A10 Networks’ DDoS Threat Intelligence provides defenders key data to improve their DDoS situational awareness, allowing them to proactively defend themselves even before the attacks starts.”
>
> —Rich Groves,
> Director of Security Research,
> A10 Networks

TOP SOURCES OF DDOS WEAPONRY

ALTHOUGH THE NATURE OF DDOS ATTACKS ARE DISTRIBUTED, WE HAVE FOUND INTERESTING DATA ABOUT WHERE THEY ORIGINATE FROM.

TOP COUNTRIES HOSTING DDOS WEAPONS

DDoS weapons are globally distributed with higher concentrations found where internet connected populations are most dense.



TOP ASN HOSTING DDOS WEAPONS

An ASN is a collection of IP address ranges that are under the control of a single administrative operator. These companies or government operators allow large numbers of weapons belonging to their users to remain connected to their network and attack other networks and computers.

China unicom中国联通	2,626,265
中国电信 CHINA TELECOM	2,154,504
vodafone	1,075,512
中華電信 Chunghwa Telecom	397,227
TIM	387,771
Rostelecom	372,422
kt	371,305

MOBILE CARRIER HOSTED DDOS WEAPONS

Mobile carriers hosting DDoS weapons skyrocket over the reporting period.

Vodafone Spain

#1 DNS resolvers source

Guangdong Mobile

#1 UDP CoAP
reflection sources

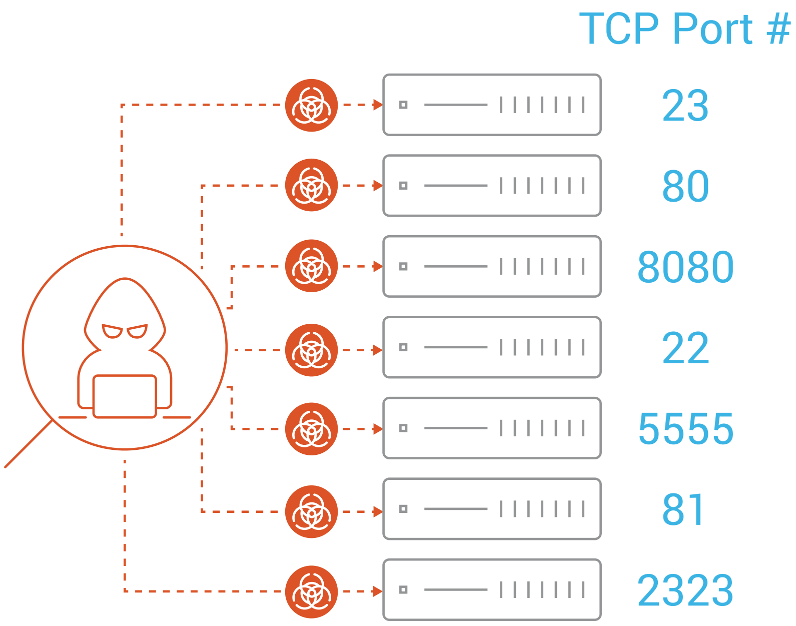
Shandong Mobile

> 500k SSDP
amplification systems

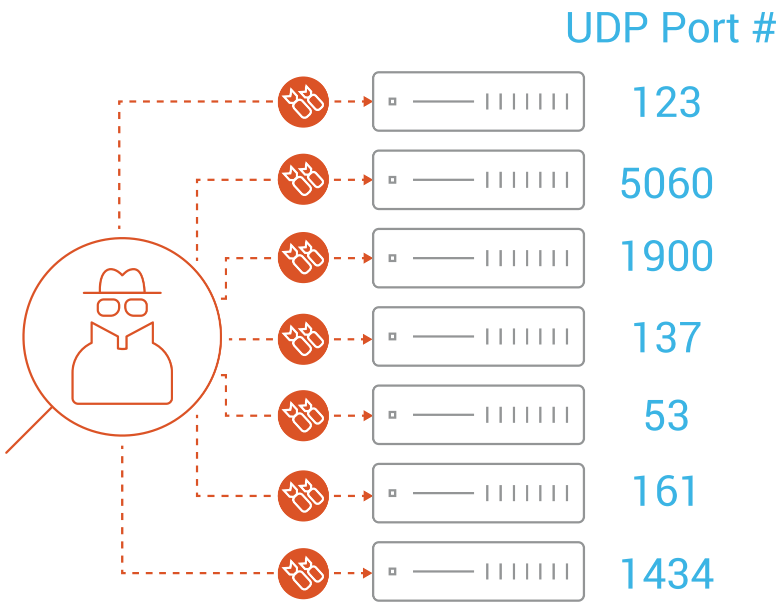
DDOS ATTACKER RECONNAISSANCE

DDoS attacks are the outputs from criminal ecosystems that include motivated attackers, DDoS-for-hire services and weapons. Attackers typically lease capacity from DDoS-for-hire services that have built an orchestration platform with pools of available DDoS weapons. DDoS-for-hire bot herders scan the internet for vulnerable IoT compute nodes through exposed TCP services and probe for available amplified UDP services to continuously replenish their weapon stock pile.

TOP TCP PORT SEARCHES



TOP REFLECTOR SEARCHES



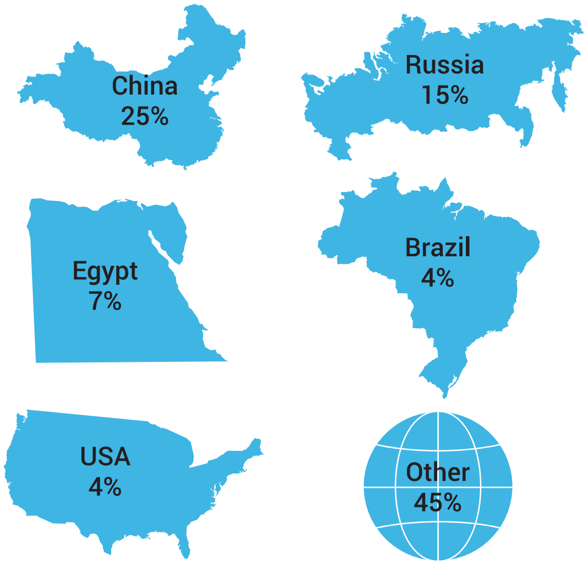
Uptick in scanning activity for SQL reflectors over UDP port 1434

DDOS BOTNET AGENTS

Compute nodes like computers, servers, routers, cameras and other IoT devices infected by malware and under the control of a malicious actor are the prized tool for motivated DDoS attackers. These weapons commonly referred to as bots or botnets provide the ultimate flexibility to DDoS attackers.

Security researchers accumulate knowledge of repeatedly used hosts in DDoS attacks, and scan for hosts exhibiting malware infected characteristics. These IP addresses deserve further scrutiny and should be treated suspiciously while under DDoS attack.

TOP COUNTRIES HOSTING DDOS BOTNET AGENTS



TOP ASN HOSTING DDOS BOTNET AGENTS

China unicom 中国联通

Rostelecom

中国电信 CHINA TELECOM

TE Data

中華電信 Chunghwa Telecom

IOT IS A HOTBED FOR DDOS BOTNETS

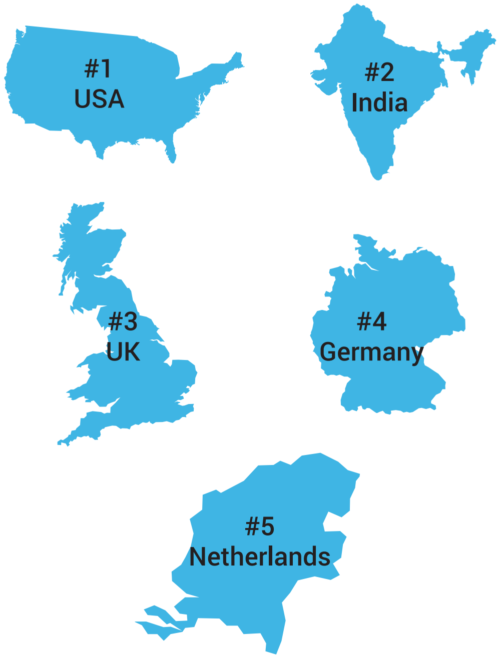
5G WILL DRAMATICALLY EXPAND ATTACK NETWORKS

It has taken just over 25 years, from the birth of the internet, to connect 55% of the 7.6 billion people on our planet. That is a linearized rate of 4.6 people per second. Compare that with IoT growing at a rate of 127 connected devices per second and accelerating. The advent of 5G, with its massive increase in bandwidth speeds, ultra-low latency, and dramatic expansion in geographic coverage, is forecast to drive a plethora of new IoT use cases and exponential growth in connected devices. With 5G, intelligent automation aided by machine learning and AI will become essential in the fast detection and mitigation of threats. IoT devices, powered by Linux, are already targeted by new strains of malware that are predominately dedicated running DDoS attacks (Eurecom)[1]. IoT is the perfect host for botnets. Let's explore the malware they leave in their wake.

TOP IOT BINARY DROPPED BY MALWARE FAMILY

Family Name	Binary Name
Mirai	sora.x86
Gafgyt	Mx86
Hajime	storm.x86

TOP COUNTRIES HOSTING MALWARE DROPPERS



TOP ASN HOSTING MALWARE DROPPERS

DigitalOcean

aruba.it

Hostwinds

DSLEXTREME

3wInfra

[1] http://www.s3.eurecom.fr/docs/oakland18_cozzi.pdf (France-based EURECOM)

THE LATEST IOT THREAT: COAP

There is a new IoT DDoS threat and it doesn't have anything to do with Mirai or malware. Once again, the industry is adopting technology with weak security, which is enabling millions of IoT device to become weaponized as reflected amplification canons. The new attack strategy is based on the UDP implementation of the Constrained Application Protocol (CoAP). This machine-to-machine (M2M) management protocol is deployed on IoT devices supporting applications such as smart energy and building automation.

From a DDoS perspective CoAP is a protocol which is implemented for both TCP and UDP and does not require authentication to reply with a large response to a small request.

A10 identified > 400K vulnerable IoT devices (exact number: 414,130)

96%

Of responses > 350 bytes

62 percent of responses > 1K

749 BYTES

Average response size

98%

Located in China

Attack from UDP port 5683 to any destination port

4K BYTES

Maximum response size

Average amplification: 35x

THE LARGEST DDOS ATTACKS HAVE ONE THING IN COMMON—AMPLIFICATION

Amplified reflection attacks take the prize when it comes to size. Amplified reflection attacks are a type of DDoS attack that exploit the connectionless nature of the UDP protocol with spoofed requests to misconfigured open servers on the internet.

This attack strategy sends volumes of small requests with the spoofed victim's IP address to exposed servers. The servers reply with large amplified responses to the unwitting victim. These particular servers are targeted because they are configured with services that can amplify the attack.

The most common types of these attacks can utilize millions of exposed DNS, NTP, SSDP, SNMP and CLDAP UDP-based services. These attacks have resulted in record-breaking colossal volumetric attacks, such as the 1.3 Tbps Memcached-based GitHub attack, and account for the majority of DDoS attacks.

Geographic distribution of top reflected amplification attack weapons

DNS RESOLVERS

China	1,495,968
Spain	1,177,411
United States	769,138
Russia	281,765
Taiwan	264,611

NTP

United States	1,306,043
China	1,082,210
Italy	492,617
Russia	393,771
Germany	273,534

SSDP

China	2,669,332
Russia	323,592
Taiwan	125,253
United States	115,090
Italy	98,463

SNMP

Republic of Korea	263,820
United States	259,959
India	143,398
China	126,336
Italy	116,188

TFTP

China	305,971
United States	292,882
Russia	272,917
Republic of Korea	240,397
Canada	102,033

DDOS ATTACKS TO GO HYPERSCALE WITH 5G

The size and sophistication of DDoS attacks have risen at an ever-accelerating pace. As new 5G networks become operational, we expect the size of attacks will dwarf these records. 5G will enable a wide variety of exciting new smart world IoT applications and use cases, but it will also increase the available DDoS weaponry available to attackers.

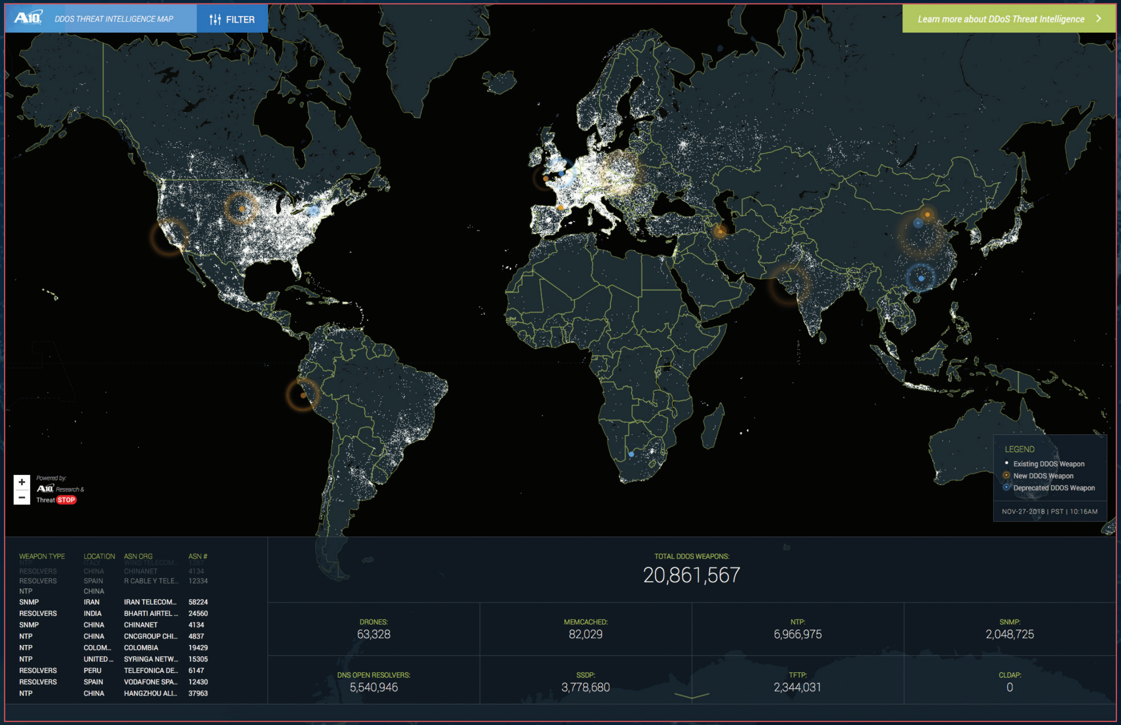
Ericsson recently predicted that, by 2024, the number of IoT with cellular connection will reach 4.1 billion. These devices will not only increase in number, but in speed. 5G, with its exponentially higher data speeds and lower latency, will be the primary driver behind this rapid expansion. Service providers will need to evolve rapidly with these growing threats and adopt intelligent automation to detect and mitigate security anomalies in a matter of seconds.

> “Proactive intelligence collection and enforcement has the unique ability to identify the infrastructure an attacker will use at the exact same time the attacker does.”
>
> —John Bambenek,
> VP of Security Research
> and Intelligence at ThreatSTOP

DDOS WEAPONS INTELLIGENCE

Sophisticated DDoS weapons intelligence, combined with real-time threat detection and automated signature extraction, will allow organizations to defend against even the most massive multi-vector DDoS attacks, no matter where they originate. Actionable DDoS weapons intelligence enables a proactive approach to DDoS defenses by creating blacklists based on current and accurate feeds of IP addresses of DDoS botnets and available vulnerable servers commonly used for DDoS attacks. A10 Networks and our partner security researchers are at the forefront of DDoS threat intelligence. A10 delivers a comprehensive and converged system to enable service providers to achieve full spectrum DDoS protection.

To learn more about A10 Networks DDoS weapons intelligence, visit our DDoS threat map at: https://threats.a10networks.com.


A10
DDOS THREAT INTELLIGENCE MAP
FILTER
Learn more about DDoS Threat Intelligence
+
−
Powered by:
A10 Research &
Threat STOP

LEGEND

- ● Existing DDOS Weapon
- ◉ New DDOS Weapon
- ◉ Deprecated DDOS Weapon

NOV-27-2018 | PST | 10:16AM

WEAPON TYPE	LOCATION	ASN ORG	ASN #
NTP	ITALY	WIND TELECOM...	1267
RESOLVERS	CHINA	CHINANET	4134
RESOLVERS	SPAIN	R CABLE Y TELE...	12334
NTP	CHINA		
SNMP	IRAN	IRAN TELECOM...	58224
RESOLVERS	INDIA	BHARTI AIRTEL ...	24560
SNMP	CHINA	CHINANET	4134
NTP	CHINA	CNCGROUP CHI...	4837
NTP	COLOM...	COLOMBIA	19429
NTP	UNITED ...	SYRINGA NETW...	15305
RESOLVERS	PERU	TELEFONICA DE...	6147
RESOLVERS	SPAIN	VODAFONE SPA...	12430
NTP	CHINA	HANGZHOU ALI...	37963

TOTAL DDOS WEAPONS:
20,861,567

DRONES:	MEMCACHED:	NTP:	SNMP:
63,328	82,029	6,966,975	2,048,725
DNS OPEN RESOLVERS:	SSDP:	TFTP:	CLDAP:
5,540,946	3,778,680	2,344,031	0

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information visit: a10networks.com
or tweet @A10Networks.

LEARN MORE
ABOUT A10 NETWORKS

CONTACT US
a10networks.com/contact

Part Number: A10-EB-14115-EN-03 FEB 2019