SDN COMMUNICATIONS®

JAN. - JUNE 2020

CYBER THREAT LANDSCAPE

Cybersecurity Intelligence Report

EXECUTIVE SUMMARY

This report contains observations and insights from SDN's Managed DDoS Protection service and SDN Managed Firewall service. This report covers SDN services from January 1 – June 30, 2020. It represents a unique view of the cybersecurity trends SDN is seeing in the region. Sign up to receive the report twice a year at **sdncommunications.com/threat-landscape/**.

SDN MANAGED DDoS* PROTECTION: KEY TRENDS January 1 - June 30, 2020

Q1 & Q2 2020 Total Number of Attacks

4420 high alerts

Easily on pace to exceed the total number of attacks reported in 2019 (4905). DDoS attacks continue to be a top cybersecurity concern.

Attack Count Year over Year

108% increase

Average Duration

39.2% increase

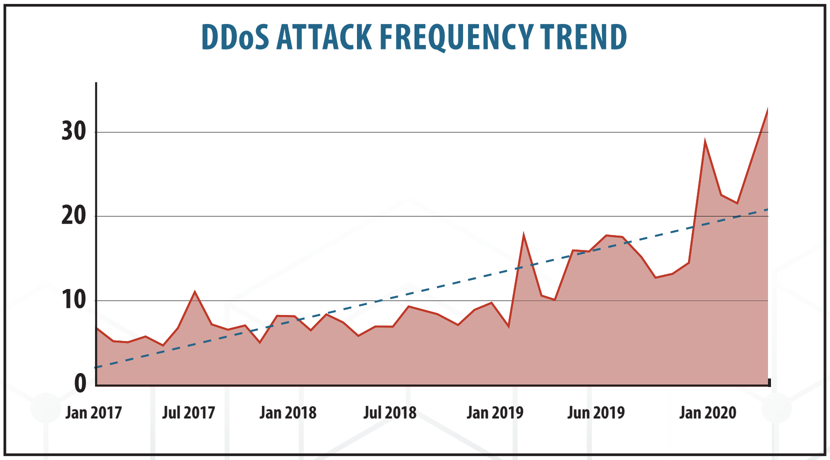
Average Attack Size Change**

42% decrease

Peak Attack Size**

66.42 Gbps

DDoS ATTACK FREQUENCY TREND



*These results exclude identified tests, global alerts not related to specific customer objects, and likely false positives where the single attack vector is total traffic.

** Attack size is the traffic crossing the network edge directed to an endpoint during the detected anomalous activity.

SDN MANAGED DDoS PROTECTION: KEY TRENDS January 1 - June 30, 2020

THREE TYPES OF DDoS ATTACKS

Volumetric Attacks focus entirely on consuming the bandwidth of a network or the connection a network maintains to the rest of the internet. This is the most common type of DDoS attack.

Examples: NTP Amplification, DNS Amplification, UDP Flood, TCP Flood

Protocol Attacks render a target inaccessible by consuming all the resources available on a server or the resources on the intermediate communication equipment, such as firewalls and load balancers.

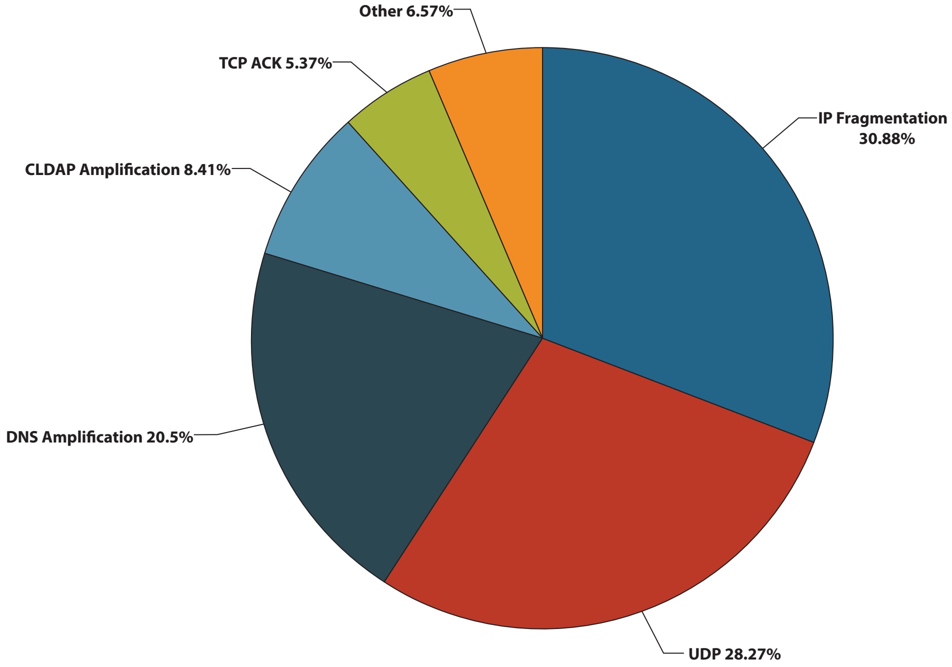
Examples: Syn Flood, Ping of Death

Application-Layer Attacks target a specific weakness found in an application or service at Layer 7. These attacks are the most effective due to taking the "low and slow" approach and circumventing flow-based monitoring solutions.

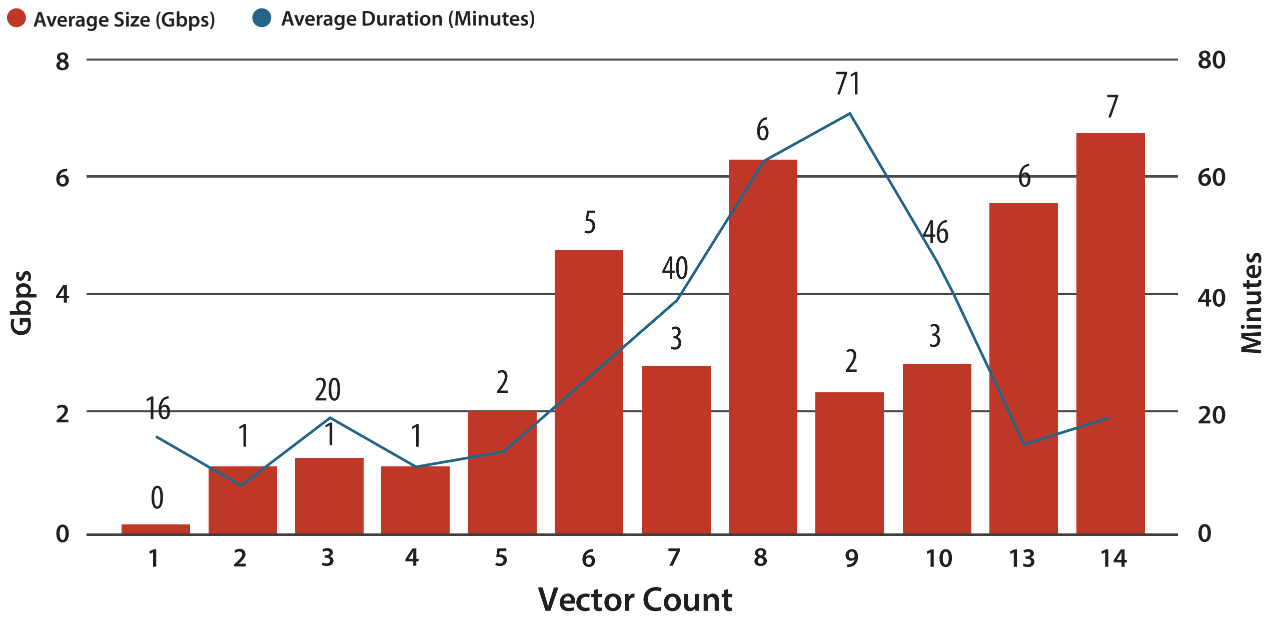
Examples: HTTP Flood, Attack on DNS Services

95% of all DDoS attacks in the first half of 2020 were multi-vector attacks.

2020 Q1 & Q2 ATTACKS BY VECTOR



AVERAGE ATTACK SIZE BY NUMBER OF VECTORS



The number of vectors used in DDoS attacks continues to increase. Employing six or more attacks at a time has become commonplace.

SDN MANAGED FIREWALL: KEY TRENDS January 1 - June 30, 2020

TOP 10 ATTACKS

#1 Bash.Function.Definitions.Remote.Code.Execution	Remote code execution
#2 ip_dst_session	Denial of service
#3 ip_src_session	Denial of servie
#4 Novell.NetBasic.Scripting.Server.Directory.Traversal	Information disclosure
#5 OpenVAS.Web.Scanner	Port scan attack
#6 SSL.Anonymous.Ciphers.Negotiation	Information disclosure
#7 tcp_dst_session	Denial of service
#8 tcp_src_session	Denial of service
#9 Web.Server.Password.Files.Access	Information disclosure
#10 ZGrab.Scanner OpenVAS.Web.Scanner	Information disclosure

Scanning attacks have a relatively low severity when compared with other types of attacks since they aren't inherently dangerous to a network. They can be a sign that a more sophisticated attack is being created and tailored to any vulnerabilities found within the port scan.

MANAGED FIREWALL PREVENTED

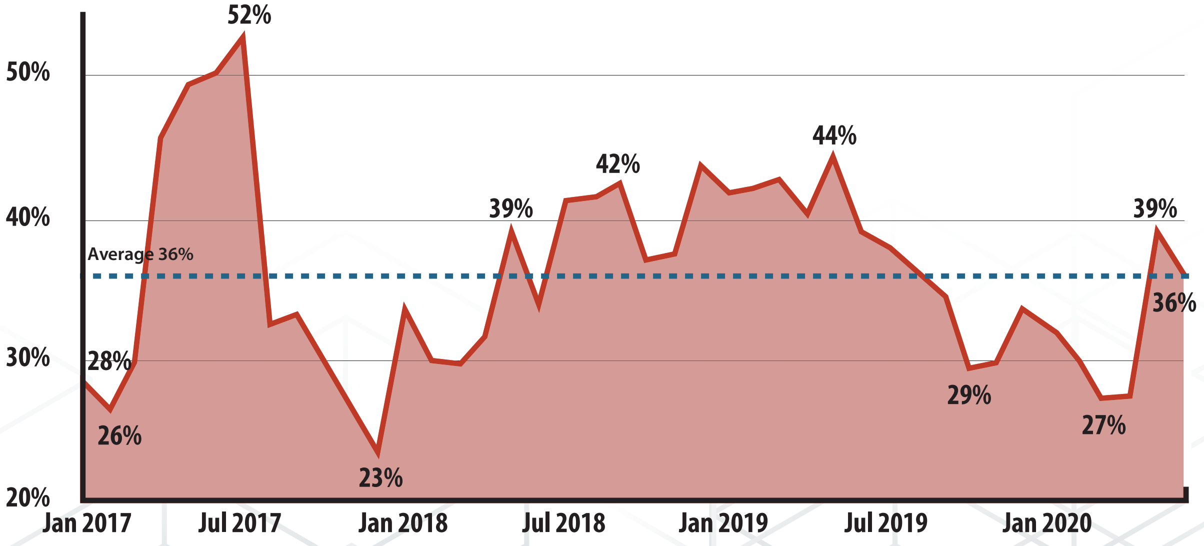
YEAR-OVER-YEAR CHANGE IN BLOCKED TRAFFIC

2020 Q1 & Q2	31.80%
2019 Q1 & Q2	41.04%
2018 Q1 & Q2	32.83%

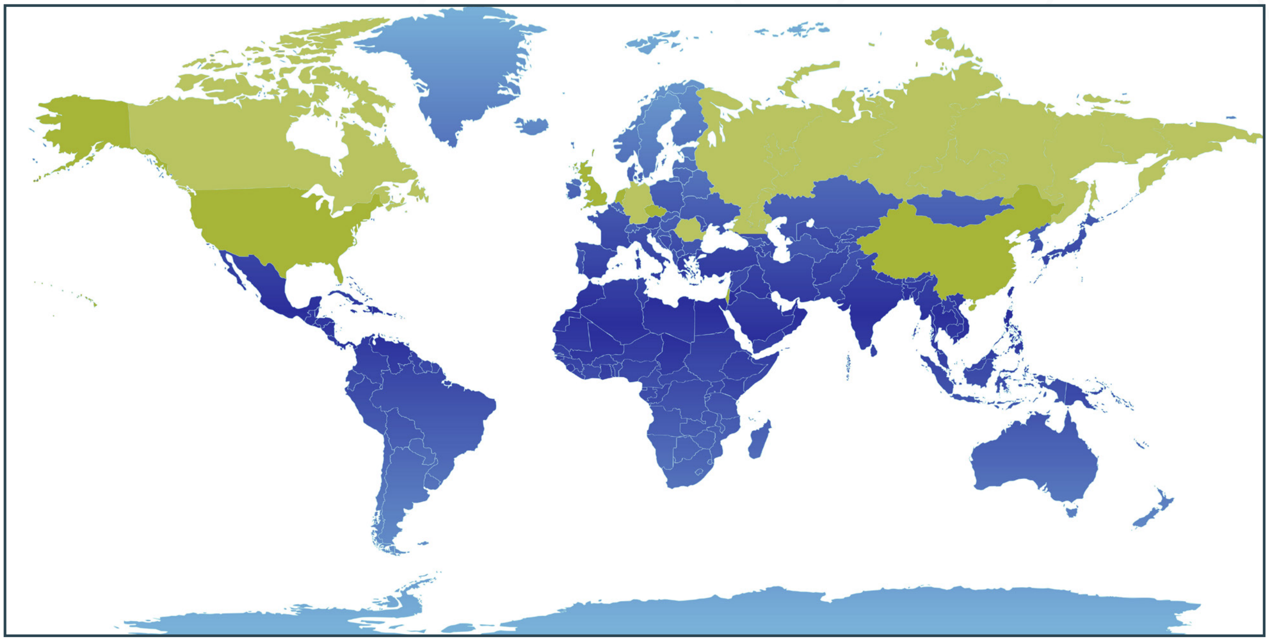
31.8% OF ALL

SDN Managed Firewall traffic was flagged as malicious or spam and was filtered out in Q1 & Q2.

UNWANTED TRAFFIC BLOCKED BY MONTH



TOP 10 THREAT EVENTS BY COUNTRY AS SEEN BY SDN MANAGED FIREWALLS



#1 UNITED STATES
#2 CANADA

#3 NETHERLANDS
#4 CHINA

#5 GERMANY
#6 RUSSIA

#7 ROMANIA
#8 UNITED KINGDOM

#9 CZECH REPUBLIC
#10 ISRAEL

TAKEAWAYS

- Businesses need to defend themselves against attacks and protect their customers as attackers increasingly target customer-facing services and applications as well as publicly exposed service infrastructure.
- Attackers not only widely weaponized six or more DDoS attack vectors but also added new variations to existing attack vectors.

GLOBAL TRENDS FROM NETSCOUT BY ARBOR*

- Nation-state groups proliferate globally while cybercriminals seem one step ahead of the game, targeting not only enterprises and service providers but also their customers.
- But that does not mean your specific organization cannot dramatically improve its security and risk posture in the coming year. There are so many things comanies can do, from the very basics, such as patching, to taking the time to understand the business network architecture and traffic flows.

* NETSCOUT is powered by Active Threat Level Analysis System (ATLAS®) and is a collaborative partnership with more than 330 service provider customers who share anonymous traffic data with Arbor Networks to deliver a comprehensive, aggregated view of global traffic and threats.