SDN COMMUNICATIONS®

2017 QUARTER 4 + YEAR IN REVIEW

CYBER THREAT LANDSCAPE

Cybersecurity Intelligence Report

EXECUTIVE SUMMARY

This report contains observations and insights from our SDN Managed DDoS Protection service and SDN Managed Firewall service. This report covers SDN services from October 1 - December 31, 2017 (Q4 2017) and a full year review of 2017. It represents a unique view of the cybersecurity trends SDN is seeing in the region. Sign up to receive the report every quarter at **sdncommunications.com/threat-landscape/**.

SDN MANAGED DDoS PROTECTION: KEY TRENDS October 1 - December 31, 2017

Total Number of Attacks

834

Quarter over Quarter

.2% increase

in total attacks over Q3 2017.

Average Daily Number of Attacks

9.4

Average Duration

16

Minutes

Peak Attack Size

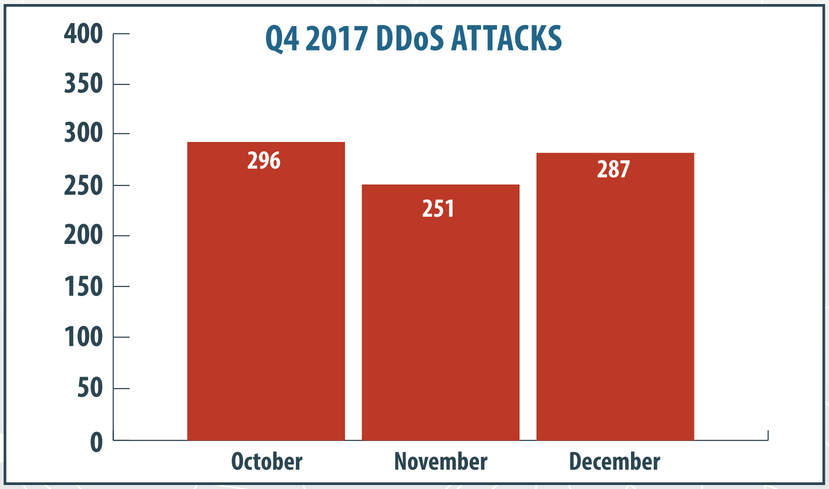
52.8

Gigabits per second (GBPS)

Average Attack Size

1.46

Gigabits per second (GBPS)



Quarter over Quarter

6% decrease

in average attack size from Q3 2017.

SDN MANAGED DDoS PROTECTION: KEY TRENDS October 1 - December 30, 2017

Q4 TOP FOUR DDoS ATTACK VECTORS

#1 UDP

#2 IP Fragmentation

#3 DNS Amplification

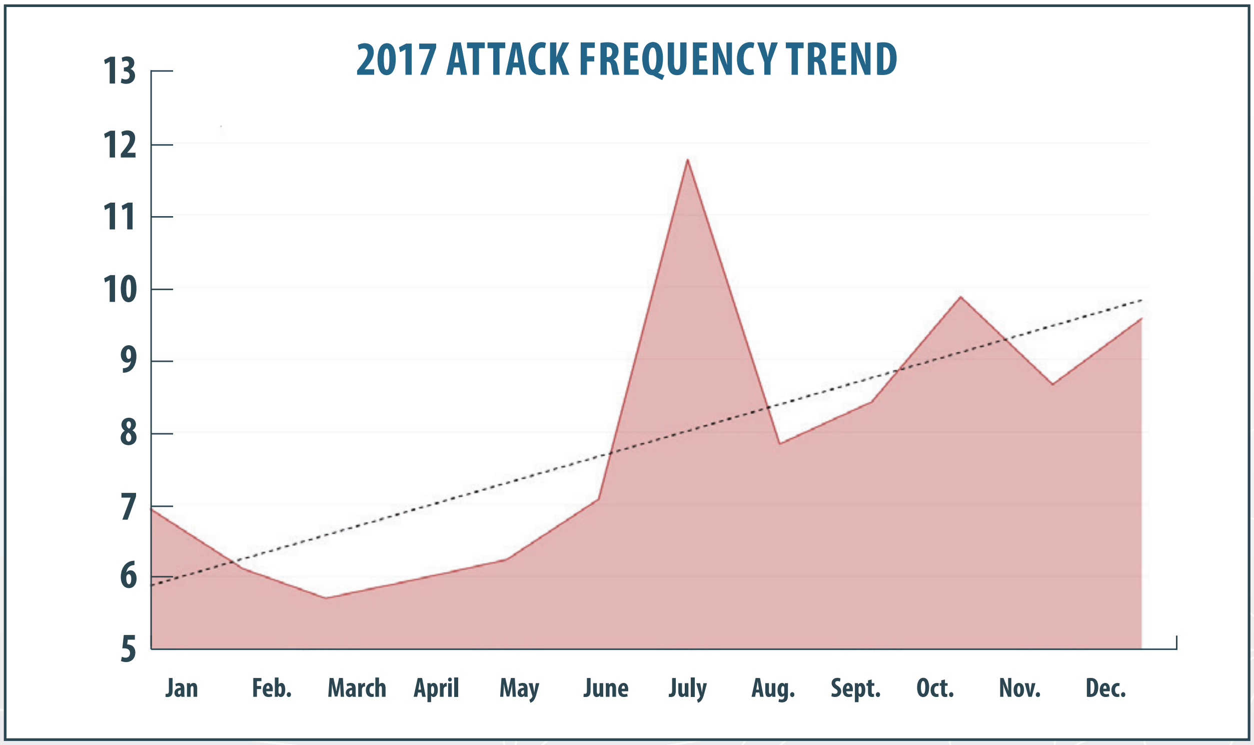
#4 ICMP

An **attack vector** is the means which hackers gain unauthorized access to a device or a network. They use it to assault or exploit a network, computer or device. Attack vectors help unauthorized elements to exploit the vulnerabilities in the system or network.

UDP Traffic Flood attacks were the most common attack in 2017. A UDP request with a spoofed source address is broadcast to random ports on a large number of computers. When the computers find no application on the requested ports, they flood the target host with "ICMP destination unreachable" packets. (arbornetworks.com)

DDOS: A REVIEW OF 2017 ATTACKS January 1 - December 30, 2017

At the beginning of 2017 SDN Communications set out to educate our customers on the threats we can identify in the region. It's valuable information when you know what you are up against. Overall, attacks continue to grow and SDN's Managed Service customers get the benefit of added protection. Here is what we saw in 2017.



After the spike in attacks in July, the frequency remained on an upward trend for the rest of 2017.

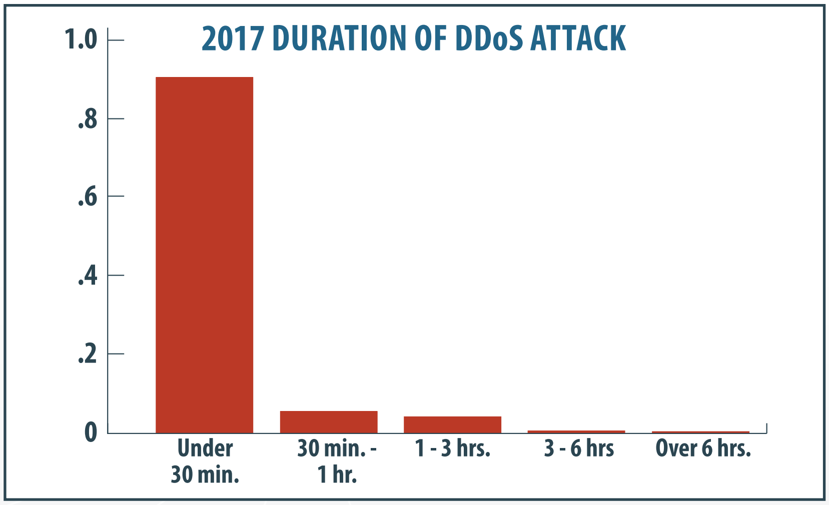
SDN MANAGED DDoS PROTECTION: 2017 TRENDS January 1 - December 30, 2017

2775
Total Number of Attacks in 2017

8
Daily Average Attacks for 2017

52.8 GBPS
Largest Attack Size in 2017

A LOOK AT ATTACKS BY DURATION January 1 - December 30, 2017



Although the majority of attacks within 2017 were under 30 minutes in duration, it isn't uncommon for attackers to repeatedly start and stop DDoS attempts in order to make mitigation more complex.

TAKEAWAYS - BEST DEFENSE: A LAYERED APPROACH

- **90%** of attacks in 2017 were under 30 minutes of duration
- A "low and slow" attack of only **1 GBPS** can take nearly any organization offline.
- High bandwidth attacks can only be mitigated in the cloud by a DDoS protection service, away from the intended target.
- According to Arbor's 2018 Global Threat Landscape report, online gaming remains the leading impetus for DDoS attacks. Criminals demonstrating attack capabilities took second place, with extortion rounding out the top three motivators for attack.

SDN MANAGED FIREWALL: KEY TRENDS October 1 - December 30, 2017

TOP 10 ATTACKS

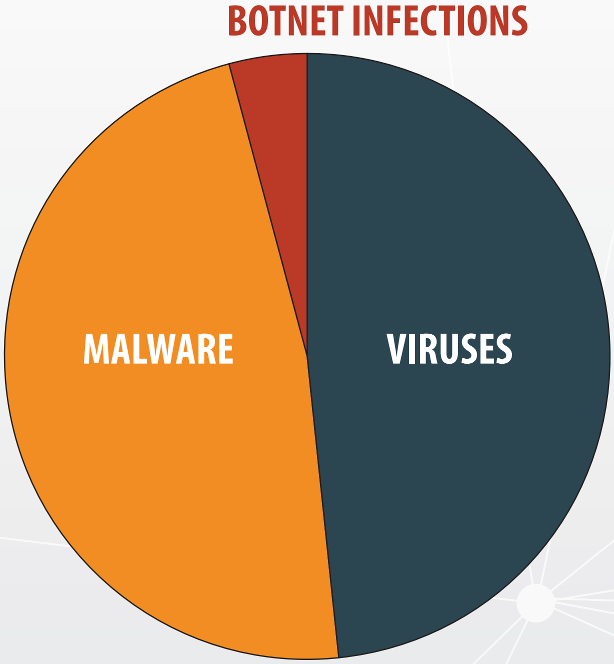
#1 Apache.Struts.Jakarta.Multipart.Parser.Code.Execution	Apache Struts vulnerability
#2 Bash.Function.Definitions.Remote.Code.Execution	Bash vulnerability
#3 Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Apache Struts vulnerability
#4 ip_dst_session	DDoS style attack
#5 udp_dst_session	DDoS style attack
#6 ip_src_session	DDoS style attack
#7 udp_src_session	DDoS style attack
#8 udp_flood	DDoS style attack
#9 OpenSSL.Heartbleed.Attack	Open SSL vulnerability
#10 HTTP.URI.SQL.Injection	SQL Vulnerability

MANAGED FIREWALL PREVENTED October 1 - December 30, 2017

BOTNET INFECTIONS	13,183
VIRUSES	156,538
MALWARE	154,280

27% OF ALL

SDN Managed Firewall Traffic
was flagged as malicious or spam
and was filtered out.

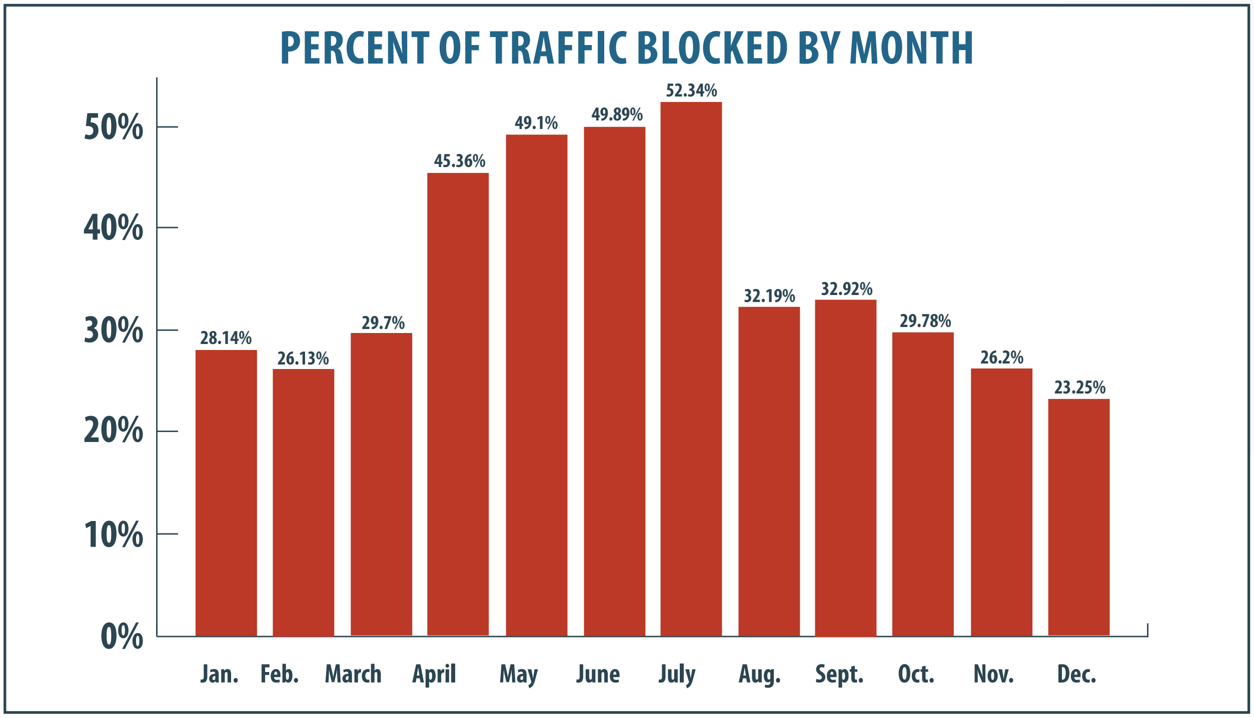


Botnet infection - Botnets infect computers and are controlled remotely using Command and Control. Interconnected computers are then used in mass spam campaigns or DDoS attacks.

Virus - A type of malicious software that infects computers. Viruses can cause system failure, waste computer resources or corrupt data.

Malware - Malicious software that infects a computer and can be used to gain access to data, disrupt the computer or feed unwanted advertising to the user.

MANAGED FIREWALL - A LOOK AT 2017 OVERALL



DDoS ATTACKS: Understanding the role of Managed Firewalls and Managed DDoS Protection in the battle

DDoS attackers target your IP address and try to overwhelm your system. Managed DDoS Protection blocks malicious traffic as the traffic enters your network and mitigates it.

Managed Firewall's also have a DDoS protection component but it protects devices that are behind the internet firewall. Managed Firewalls can't protect the circuit itself. If a circuit would become saturated, your service would either perform very poorly or it may not be able to connect or receive connections at all. In this situation, the Managed Firewall would prevent malicious traffic from getting to devices inside the customer network.

Both Managed DDoS Protection and Managed Firewall DDoS protection need to be fine tuned while working closely with the customer to ensure legitimate traffic is getting through.

TAKEAWAYS

- The challenge facing cybersecurity leaders and professionals certainly isn't lessening. Cybersecurity experts must be vigilant, aware and thorough in their use of layered security.
- Patch management needs to be a top priority for cybersecurity leaders and professionals. Updating systems routinely is a key component of staying safe and secure.
- The sheer volume of information coming through your network is nothing to take lightly. Implementing the necessary safeguards will pay off in the long run.

2017 OWASP TOP 5 - APPLICATION SECURITY RISKS

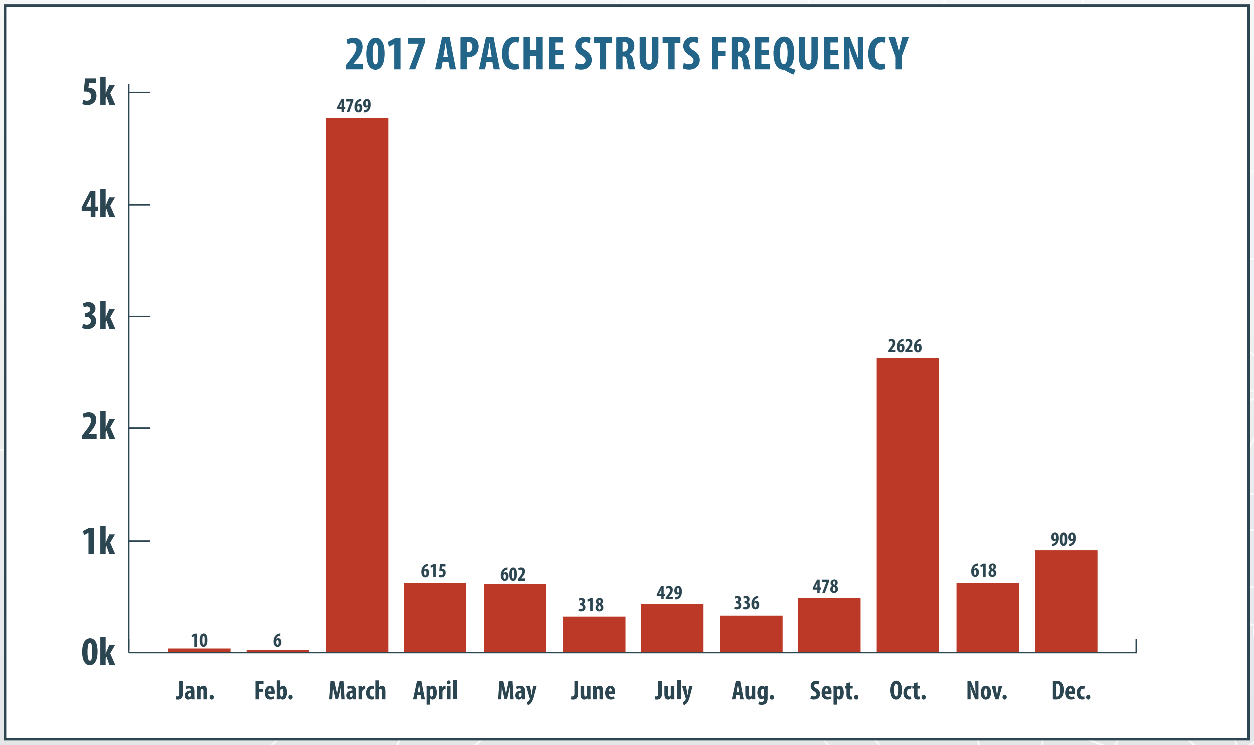
The Open Web Application Security Project (OWASP) highlights the most prominent application security risks currently found within your everyday business environment. OWASP analyzes data submitted by more than 40 firms that focus on application security as well as an industry survey submitted by over 500 individuals to generate this list.

1	**Injection**	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query.
2	**Broken Authentication**	Application functions related to authentication and session management are often implemented incorrectly.
3	**Sensitive Data Exposure**	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII.
4	**XML External Entities (XXE)**	Many older or poorly configured XML processors evaluate external entity references within XML documents.
5	**Broken Access Control**	Restrictions on what authenticated users are allowed to do are often not properly enforced.

This is a high-level overview. See the entire Top 10 List at **owasp.org** to get more information on how these attacks are carried out and what you can do to remain secure.

APACHE STRUTS IN 2017

The Apache Struts vulnerabilities were made public knowledge in March of 2017. Here you can see the drastic increase in Apache Struts-related attack attempts identified and blocked by SDN's Managed Firewall service.



A HIGH-LEVEL LOOK AT MELTDOWN AND SPECTRE

Meltdown is specific to Intel-based CPUs while Spectre affects all CPUs, including Intel, AMD, & ARM. Apple processors are an ARM-based architecture design and are affected by Meltdown as well. That means it affects smartphones and tablets in addition to PCs and servers. Both are hardware vulnerabilities.

	Meltdown	Spectre
Architecture	Intel, Apple, ARM	Intel, Apple, ARM, AMD
Entry	Execute code on system	Execute code on system
Process	Privilege escalation and speculative execution	Branch prediction and speculative execution
Impact	Read system memory	Read contents of applications in arbitrary locations within memory
Action	Patching	Patching

Meltdown and Spectre Q & A

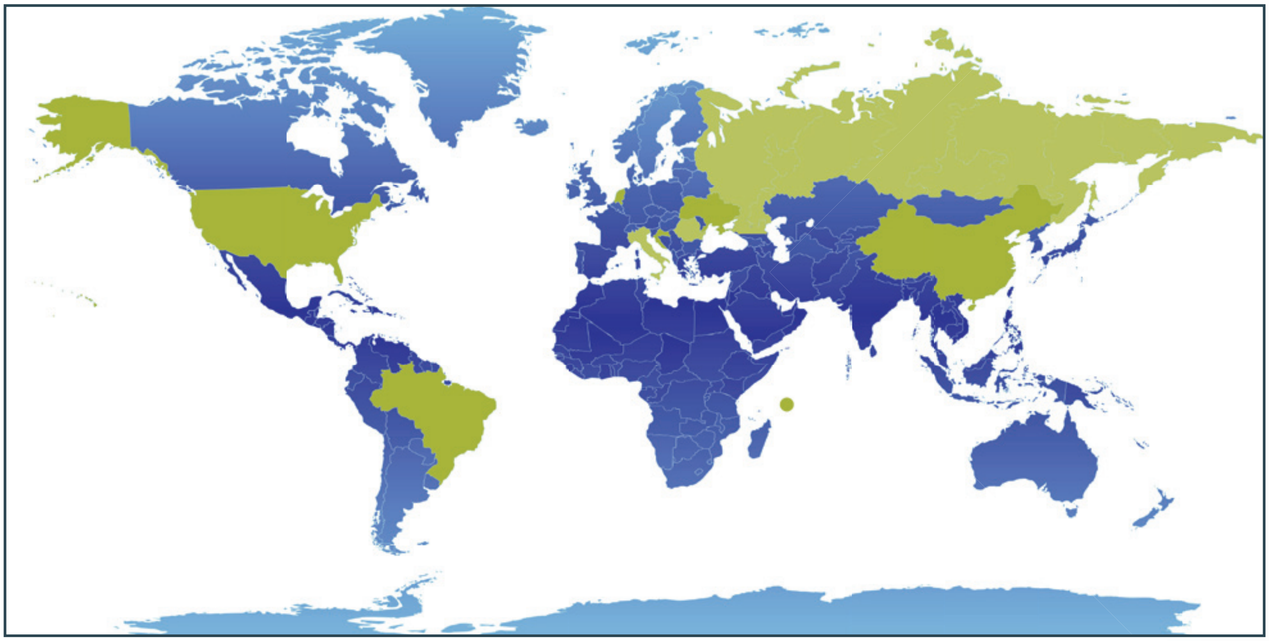
Q: Am I affected?
A: Yes.

Q: What is the difference between Meltdown and Spectre?
A: Meltdown "melts" the security boundaries of applications by accessing system memory. Spectre tricks other applications into granting access to their memory.

Q: What information is vulnerable?
A: Whatever information is contained in the memory of your computer. This could range from passwords to files and other sensitive information.

Q: How can I secure myself?
A: Implement patches as soon as they are available.

TOP 10 THREAT EVENTS BY COUNTRY AS SEEN BY SDN FIREWALLS



#1 UKRAINE
#2 UNITED STATES
#3 SEYCHELLES
#4 NETHERLANDS
#5 CHINA
#6 CROATIA
#7 BRAZIL
#8 ROMANIA
#9 ITALY
#10 RUSSIA

OTHER HELPFUL CYBERSECURITY TERMINOLOGY

Passive Attack – An attack perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system or its resources, data, or operations.

Redundancy – Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.

Speculative Execution – An optimization technique where a computer system performs a task that isn't necessarily needed at the moment, but could be needed in the future. In other words, when there are extra resources available the processor works ahead and predicts tasks you may need in the future to prevent a delay when that task is called upon.

Receive the Threat Landscape Report digitally by signing up at **sdncommunications.com/threat-landscape/**.

SDN COMMUNICATIONS®

www.sdncommunications.com • 2900 W. 10th Street, Sioux Falls, SD 57104 • 1.800.247.1442