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 throughout 2018. It represents a unique view of the cybersecurity trends SDN is seeing in the region. Sign up to receive the reports as they are released at **sdncommunications.com/threat-landscape/**

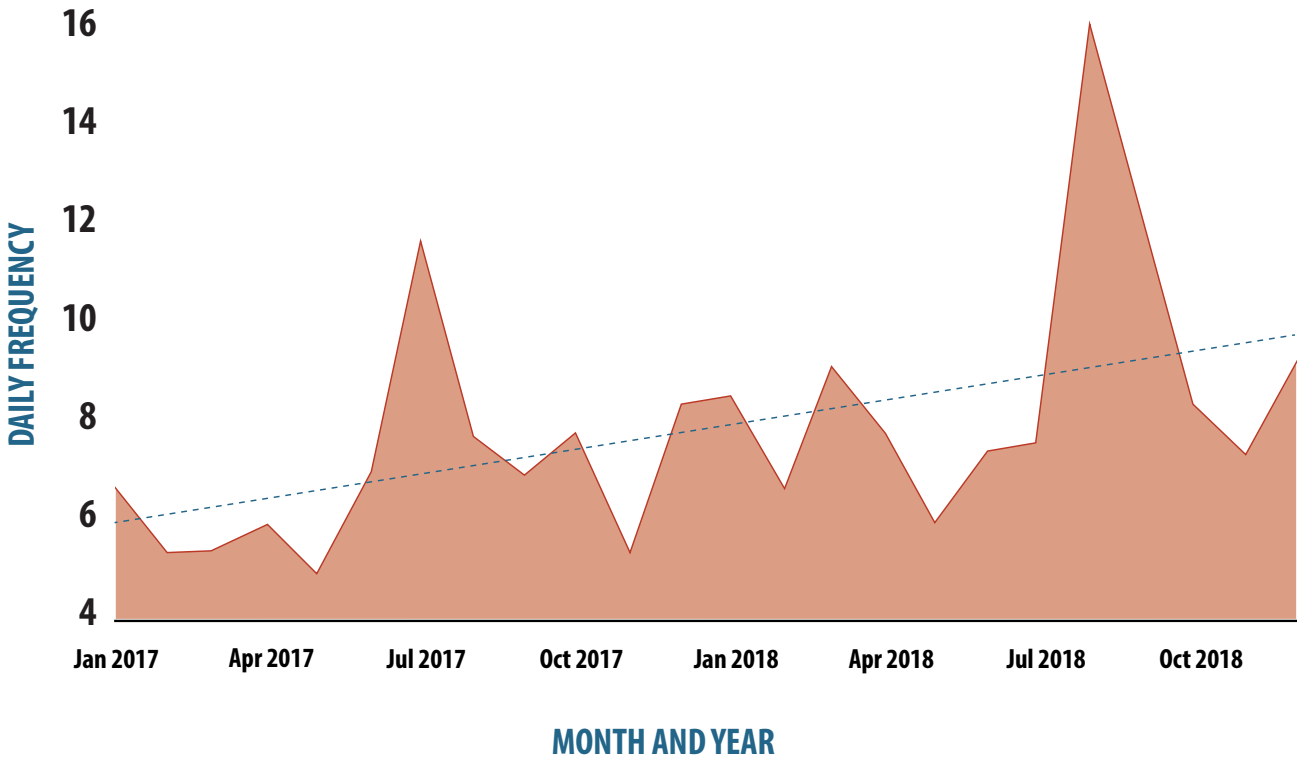
MANAGED DDoS PROTECTION HIGHLIGHTS

ATTACK COUNT
27.2% increase

AVERAGE DURATION
18.5% decrease

AVERAGE ATTACK SIZE
1.5% increase

ATTACK FREQUENCY ROLLING TREND



SDN MANAGED DDoS PROTECTION: KEY TRENDS January 1 - December 31, 2018

Vector: a path or means by which a hacker can gain access to a computer or network in order to deliver a payload or malicious outcome.

THREE TYPES OF DDoS ATTACK VECTORS

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.

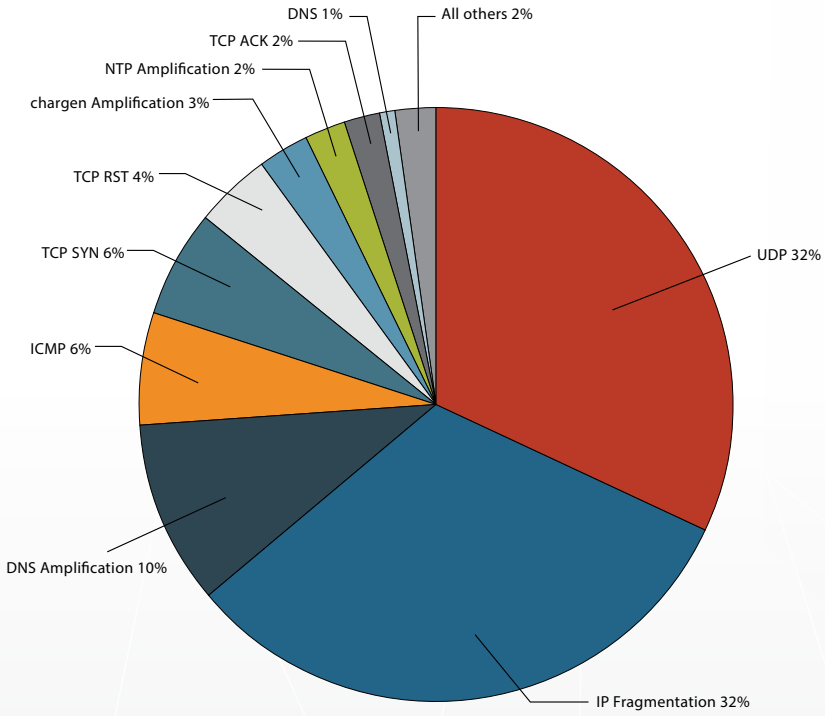
Examples: Syn Flood, Ping of Death

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.

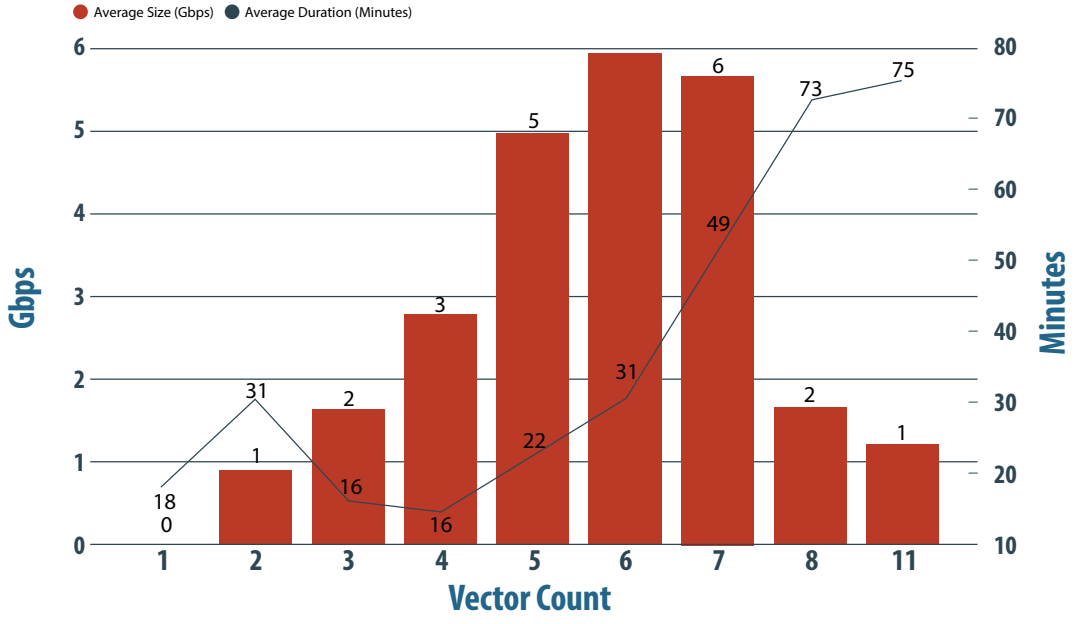
Examples: HTTP Flood, Attack on DNS Services

79% of all DDoS attacks in 2018 were multi-vector attacks.

2018 ATTACKS BY VECTOR



AVERAGE ATTACK SIZE AND DURATION BY NUMBER OF VECTORS



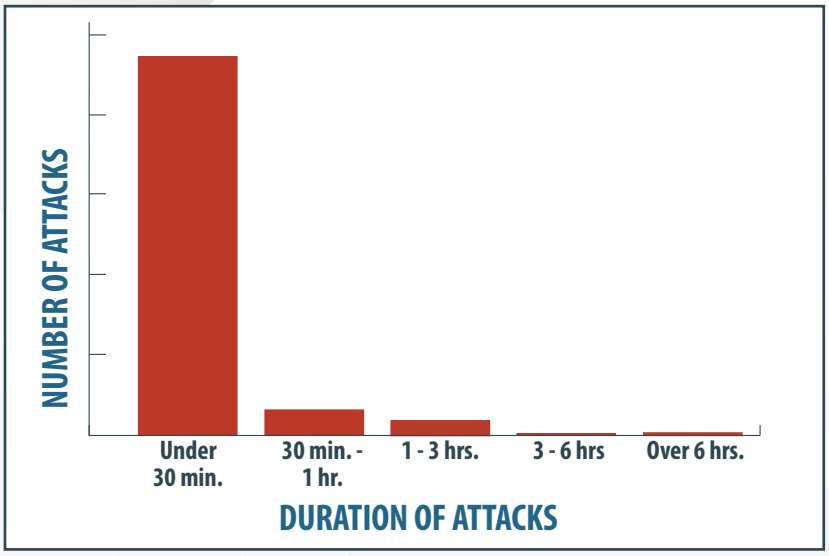
SDN MANAGED DDoS PROTECTION: KEY TRENDS January 1 - December 31, 2018

31 GBPS
Largest Attack Size in 2018

26 MINUTES
Average Attack Length for 2018

11
Most Vectors Seen with a Single Attack

NUMBER OF ATTACKS BY DURATION January 1 - December 31, 2018



90%
of attacks seen throughout 2018 were under 30 minutes in duration.

DDoS ATTACKS: Understanding the role of SDN's 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.

SDN Communications' Managed Firewalls 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.

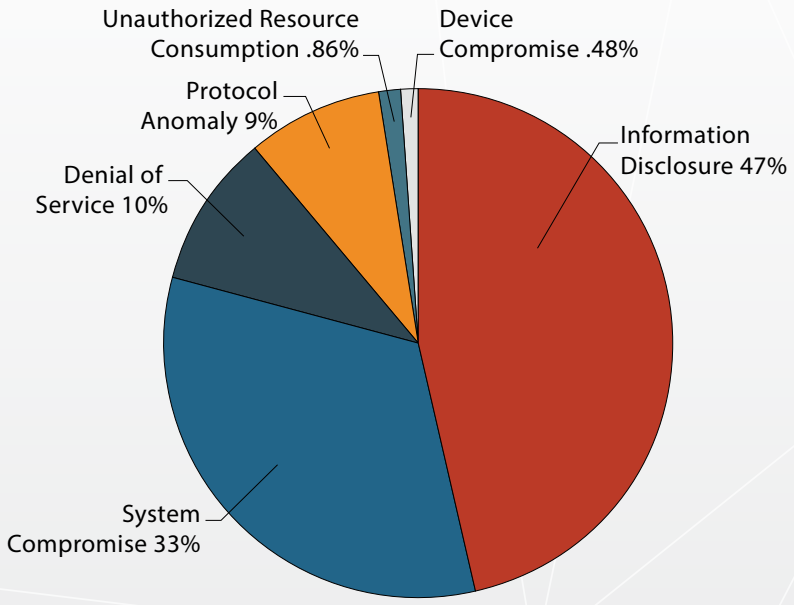
SDN MANAGED FIREWALL: KEY TRENDS January 1 - December 31, 2018

TOP 10 ATTACKS

Attack Name	Impact Category	Severity
#1 Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	System Compromise	● ● ● ● ●
#2 D-Link.DSL-2750B.CLI.OS.Command.Injection	System Compromise	● ● ● ● ●
#3 HTTP.URI.SQL.Injection	System Compromise	● ● ● ● ●
#4 MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	System Compromise	● ● ● ● ●
#5 Muieblackcat.Scanner	Information Disclosure	● ● ● ● ●
#6 OpenSSL.Heartbleed.Attack	Information Disclosure	● ● ● ● ●
#7 OpenVAS.Web.Scanner	Information Disclosure	● ● ● ● ●
#8 TCP.Split.Handshake	Protocol Anomaly	● ● ● ● ●
#9 Web.Server.Password.Files.Access	Information Disclosure	● ● ● ● ●
#10 ZmEu.Vulnerability.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.

IMPACT CATEGORIES BY COUNT January 1 - December 31, 2018



CATEGORY DESCRIPTIONS

Information Disclosure: Remote attackers can gain sensitive information from vulnerable systems.

System Compromise: Remote attackers can gain control of vulnerable systems.

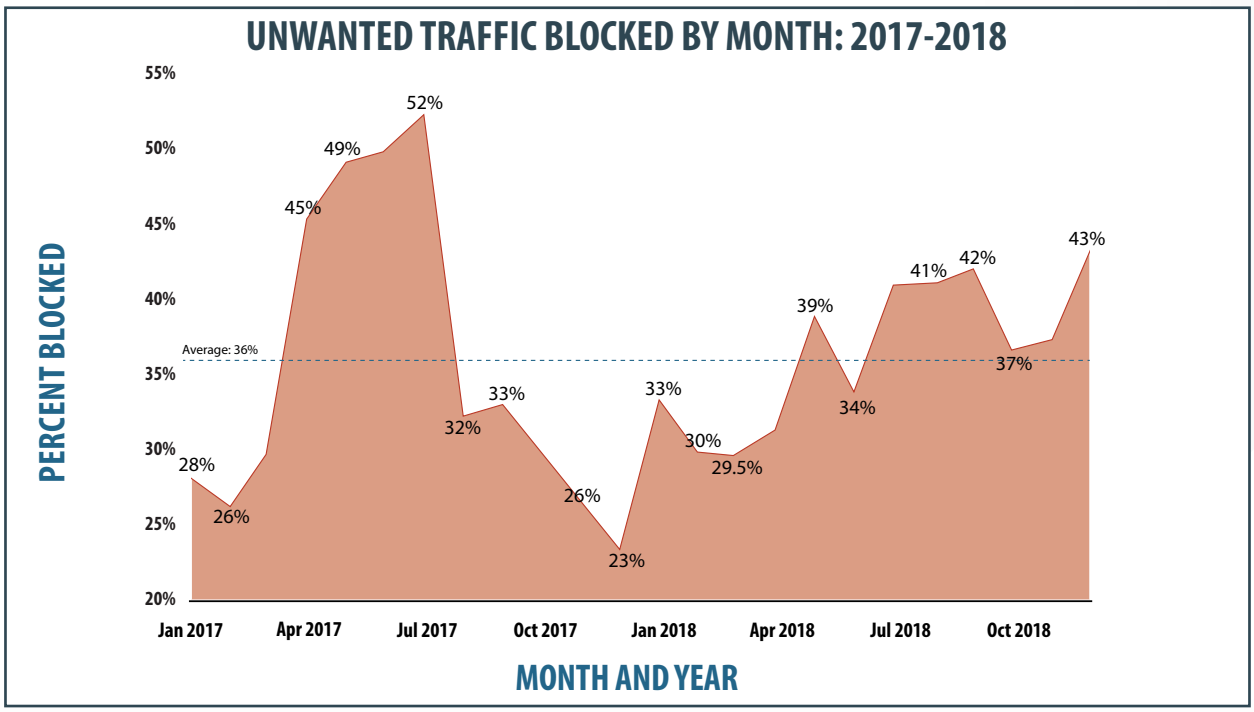
Denial of Service: DDoS-style attacks that render systems unavailable.

Protocol Anomaly: Attackers can gain system information to prepare for further attacks.

Unauthorized Resource Consumption: Remote actors can use the victim's system resources to perform certain tasks.

Device Compromise: Remote attackers can gain control of vulnerable devices.

SDN MANAGED FIREWALL: KEY TRENDS January 1 - December 31, 2018



The traffic blocked by SDN's Managed Firewall could include benign port scans from security researchers skimming the internet, port scans conducted by malicious actors, or it could include attacks like malware, viruses and botnets that have more malevolent intent.

36.6% of all SDN Managed Firewall Traffic was flagged as malicious or spam and was filtered out in 2018.

SDN EMPLOYEE CERTIFICATIONS

SDN employees are always increasing their knowledge of the ever-growing world of cybersecurity. NSE certifications validate network security skills and experience.

ACTIVE FORTINET NSE CERTIFICATIONS:

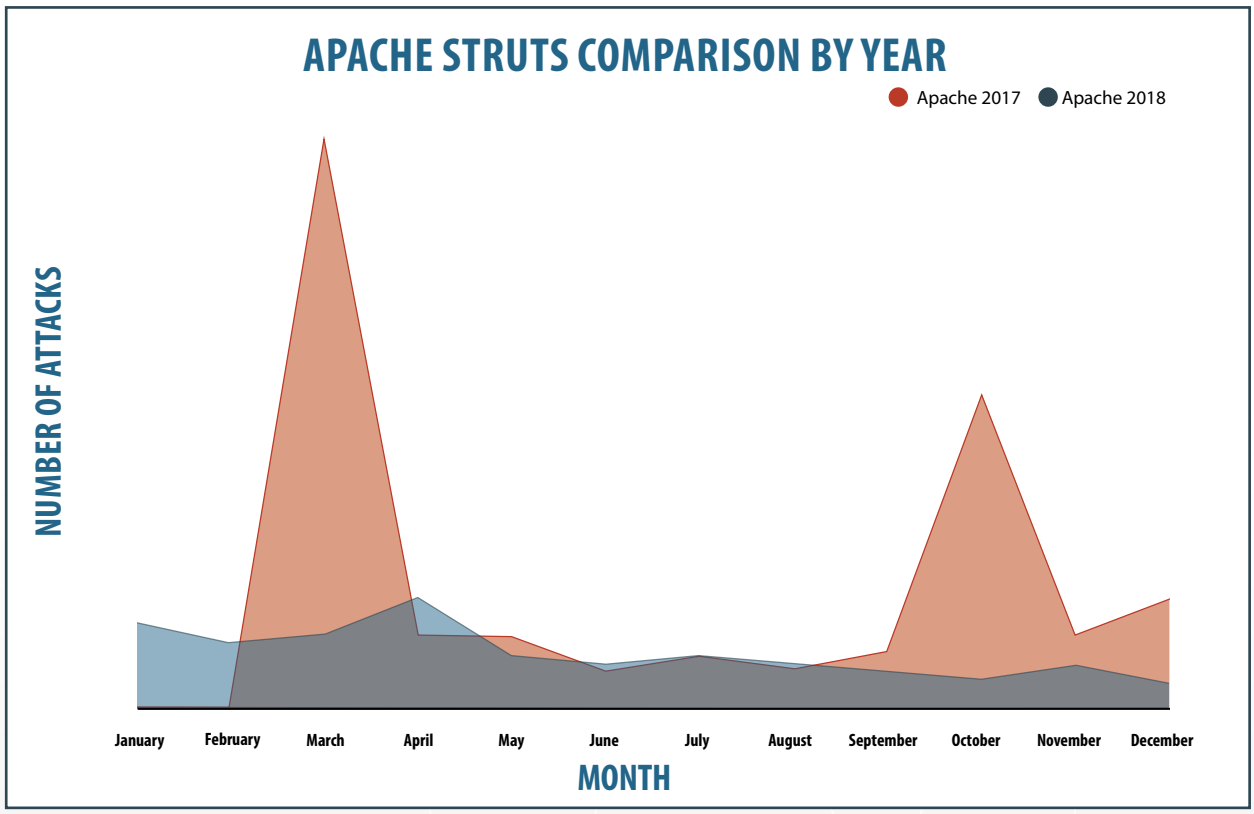
NSE 7 – Network Security Architect
Certified to integrate Fortinet products to deploy and administrate network security solutions.
SDN Communications has three NSE 7 certified Network Security Architects

NSE 4 – Network Security Professional
Certified to manage the day-to-day configuration, monitoring, and operation of FortiGate devices to support corporate network security policies.
SDN Communications currently has four NSE 4 certified Network Security Professionals

APACHE STRUTS/MELTDOWN & SPECTRE

Apache Struts in 2017 and 2018

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 SDN's Managed Firewall service identified and blocked. The spike in March of 2017 is when the news of the vulnerability initially broke. As you can see, malicious actors continued to attempt to utilize this vulnerability throughout 2018.



A Look Back at Meltdown & Spectre

MELTDOWN

SPECTRE

Last year, two vulnerabilities affected an incredible amount of cell phones, tablets, laptops, and computers manufactured within the past 20 years. Most people own more than one of these devices. When these vulnerabilities were made public, knowledge security experts knew there wasn't a simple solution. On March 15, 2019, it will be a year since these vulnerabilities were discovered and there still is no solution available.

The vulnerabilities stem from something called Speculative Execution. What this means is that instructions are executed ahead of knowing that they are required. This technique is used by most modern, high-performance processors to improve performance. Without it, processors would need to wait for prior instructions before executing subsequent ones, resulting in a drastically reduced performance.

MARRIOTT/EXACTIS

Marriott Data Breach

Scope of Attack:
- 400 million records breached
- Included 5.25 million unencrypted passport numbers

Details:
- In September 2018, Marriott received an alert from an internal security tool.
- Attackers had access to the Starwood Guest Reservation Database since 2014.
- On November 30, Marriott revealed the breach affected 500 million guests. More recently, they believe the number to be closer to 400 million.
- It has not been made public knowledge how attackers gained unauthorized access.

Information Stolen:
- Name, address, phone number, email address, passport number, date of birth, gender, loyalty program info, and reservation info were stolen.
- The hackers also stole payment card numbers and expiration dates for some individuals.

Exactis Data Breach

Scope of Attack:
- 340 Million records breached
- 2 terabytes of personal data available
- 400 different variables on a vast range of personal characteristics

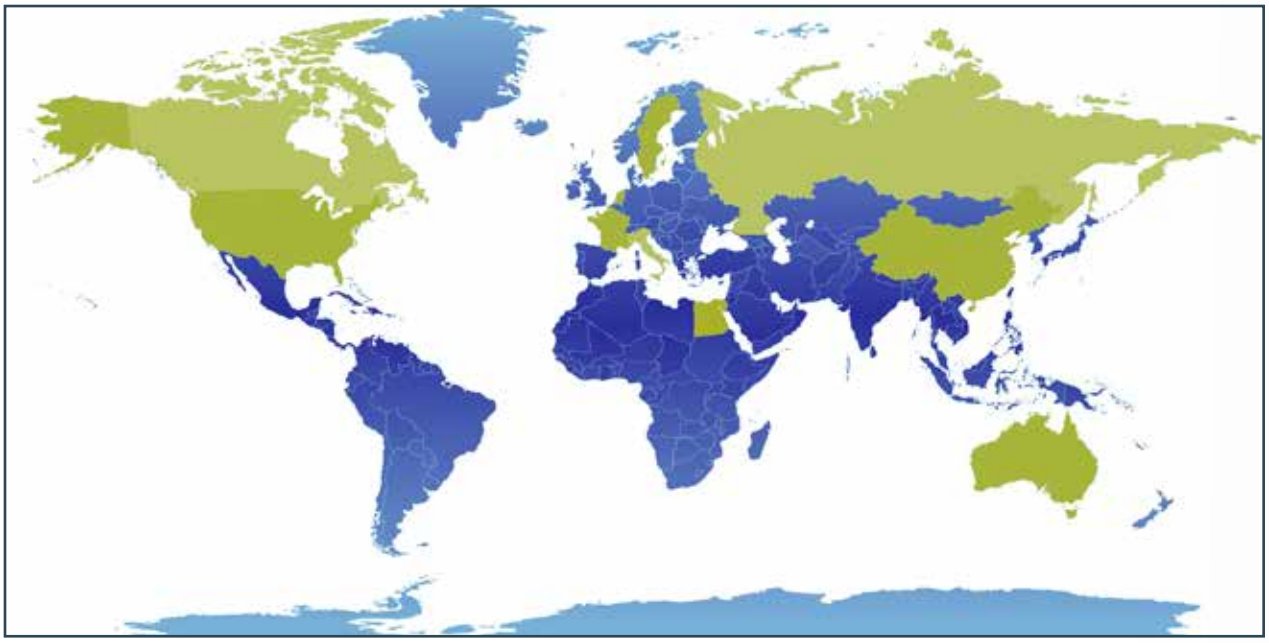
Details:
- Exactis is a data aggregation firm that boasts of holding 3.5 billion consumer, business and digital records relating to all sorts of data.
- In June 2018, it was discovered there were 2 terabytes of personal data available on a publicly accessible server.
- While it isn't obvious whether a malicious actor had accessed the database, the discovery was made using the popular cyber tool Shodan. This tool allows anyone to easily scan for internet-connected devices. Meaning if a security researcher was able to find it, others were likely able to as well.

Information Stolen:
- Email addresses, home addresses, phone numbers along with personal interests and characteristics

Important things to remember in the event of a data breach:

- Move quickly to secure your systems and fix vulnerabilities that may have caused the breach.
- Determine the source and scope of the breach.
- Consult with data breach experts and legal counsel, whether that be through internal legal staff or through a third-party company.
- Have a communications plan in place to inform affected audiences – employees, customers, investors, business partners, and other stakeholders.
- Notify local law enforcement as well as the FBI.

TOP 10 THREAT EVENTS BY COUNTRY AS SEEN BY SDN FIREWALLS



#1 UNITED STATES	#3 CHINA	#5 CANADA	#7 RUSSIA	#9 ITALY
#2 NETHERLANDS	#4 SWEDEN	#6 FRANCE	#8 EGYPT	#10 AUSTRALIA

HELPFUL RESOURCES

KnowBe4: www.knowbe4.com
KnowBe4 offers numerous free services that assist you in becoming more secure.

FTC's in-depth Data Breach Response: A Guide for Business
http://bit.ly/2ToLJ4G
Contains information such as:

- Legal requirements based on your location
- Notifying appropriate parties
- Preparing documents used for notifying affected parties

SDN Blogs: www.sdncommunications.com/blog

SDN Educational Posters:

- www.sdncommunications.com/cybersecurity-posters
- www.sdncommunications.com/cybersecurity-posters-2
- www.sdncommunications.com/cybersecurity-posters-3

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