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 information covers SDN services throughout 2019. 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/**

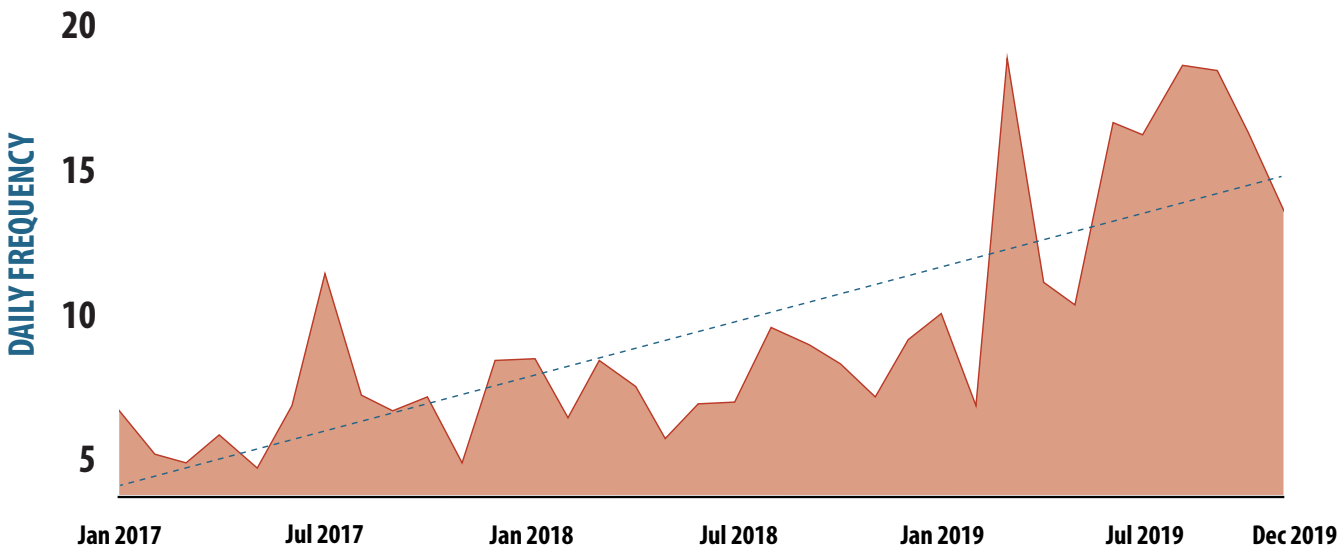
MANAGED DDoS PROTECTION HIGHLIGHTS

ATTACK COUNT
77.8% increase

AVERAGE DURATION
32.1% decrease

AVERAGE ATTACK SIZE
7.3% increase

ATTACK FREQUENCY ROLLING TREND



SDN MANAGED DDoS PROTECTION: KEY TRENDS January 1 - December 31, 2019

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.

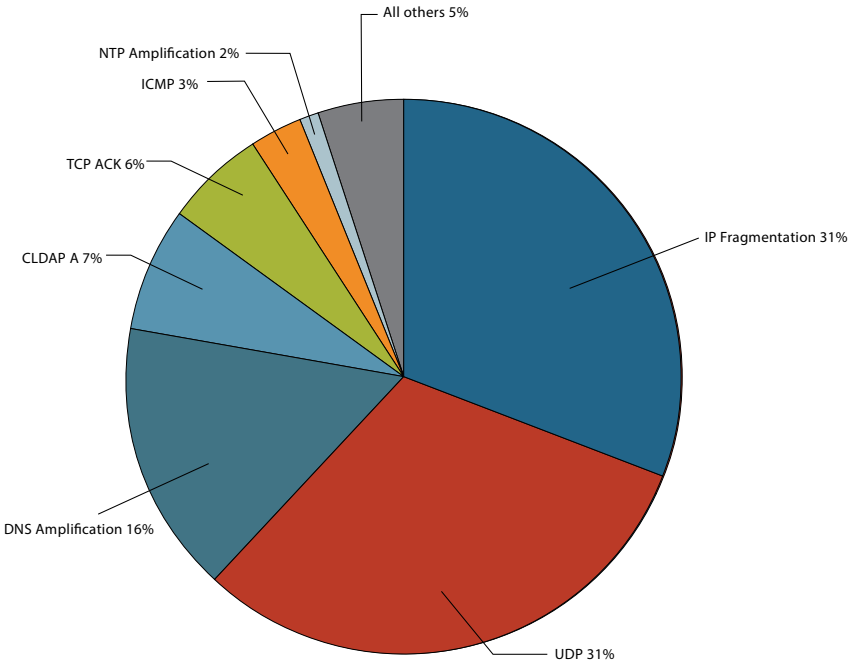
Examples: Syn Flood, Ping of Death

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.

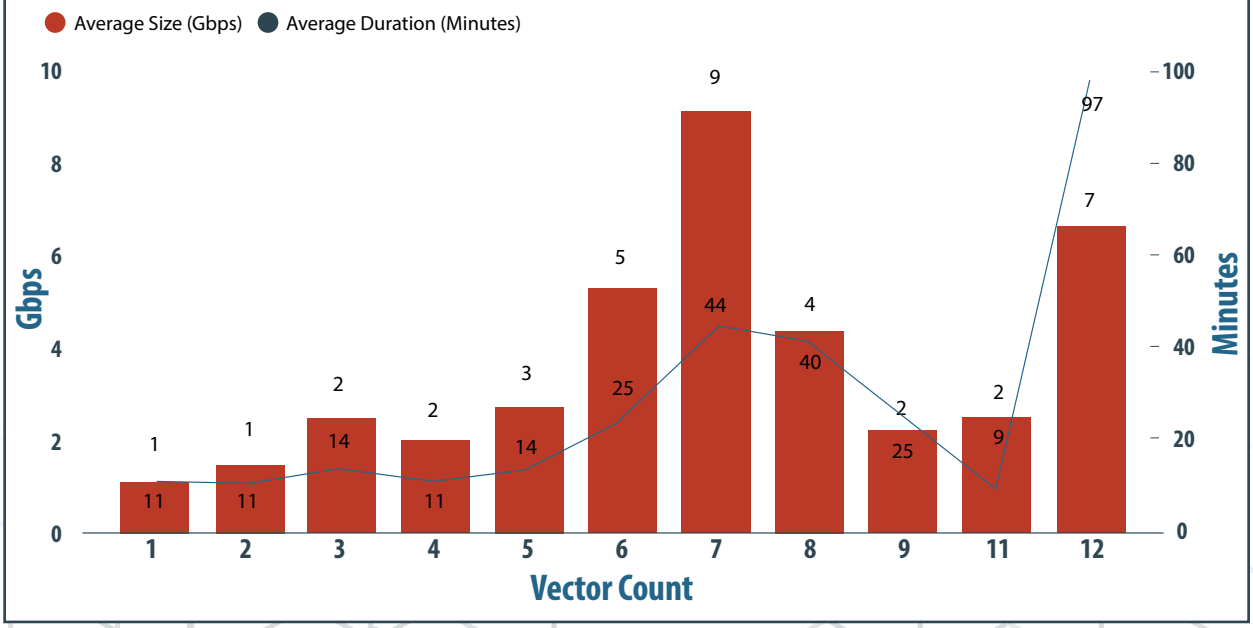
Examples: HTTP Flood, Attack on DNS Services

91% of all DDoS attacks in 2019 were multi-vector attacks.

2019 ATTACKS BY VECTOR



AVERAGE ATTACK SIZE AND DURATION BY NUMBER OF VECTORS



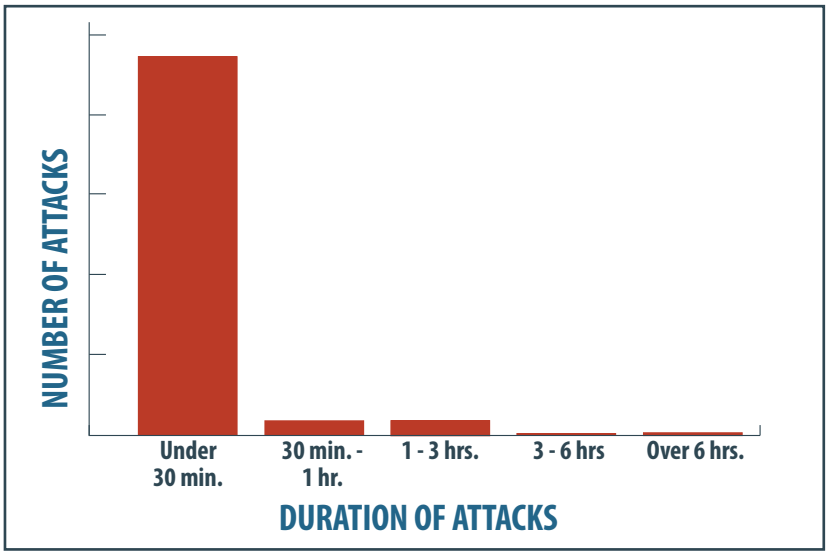
SDN MANAGED DDoS PROTECTION: KEY TRENDS January 1 - December 31, 2019

46 GBPS
Largest Attack Size in 2019

13 MINUTES
Average Attack Length for 2019

12
Most Vectors Seen with a Single Attack

NUMBER OF ATTACKS BY DURATION January 1 - December 31, 2019



90%
of attacks seen throughout 2019 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 it 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 not 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.

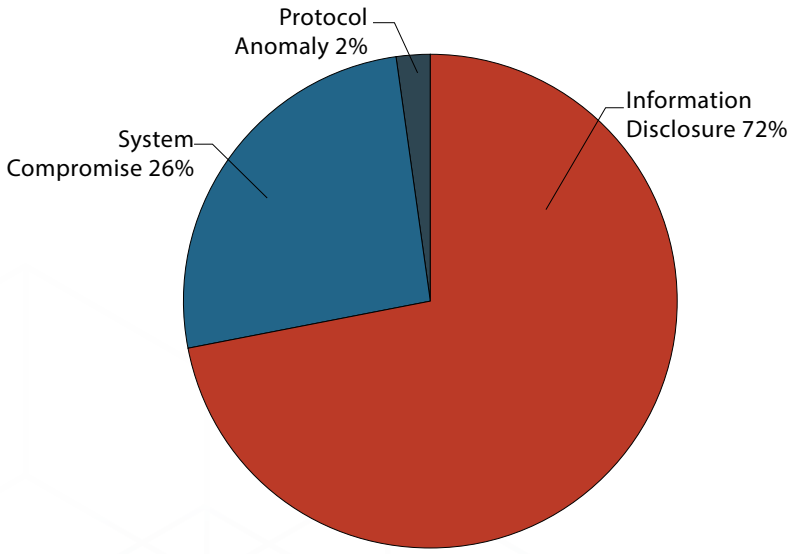
SDN MANAGED FIREWALL: KEY TRENDS January 1 - December 31, 2019

TOP 10 ATTACKS

Attack Name	Impact Category	Severity
#1 Bash.Function.Definitions.Remote.Code.Execution	System Compromise	● ● ● ● ●
#2 Generic.XXE.Detection	System Compromise	● ● ● ● ●
#3 HTTP.Request.URI.Directory.Traversal	Information Disclosure	● ● ● ● ●
#4 HTTP.URI.SQL.Injection	System Compromise	● ● ● ● ●
#5 NETGEAR.WNR2000v5.Unauthorized.Hidden.avi.Stack.Overflow	System Compromise	● ● ● ● ●
#6 OpenVAS.Web.Scanner	Information Disclosure	● ● ● ● ●
#7 PHP.Diescan	Information Disclosure	● ● ● ● ●
#8 TCP.Split.Handshake	Protocol Anomaly	● ● ● ● ●
#9 Web.Server.Password.Files.Access	Information Disclosure	● ● ● ● ●
#10 ZmEu.Vulnerability.Scanner	Information Disclosure	● ● ● ● ●

Information Disclosure attacks accounted for 47% of all attacks in 2018. That increased to 72% of all attacks in 2019. Information Disclosure attackers work remotely to gain sensitive information from vulnerable systems.

IMPACT CATEGORIES BY COUNT January 1 - December 31, 2019



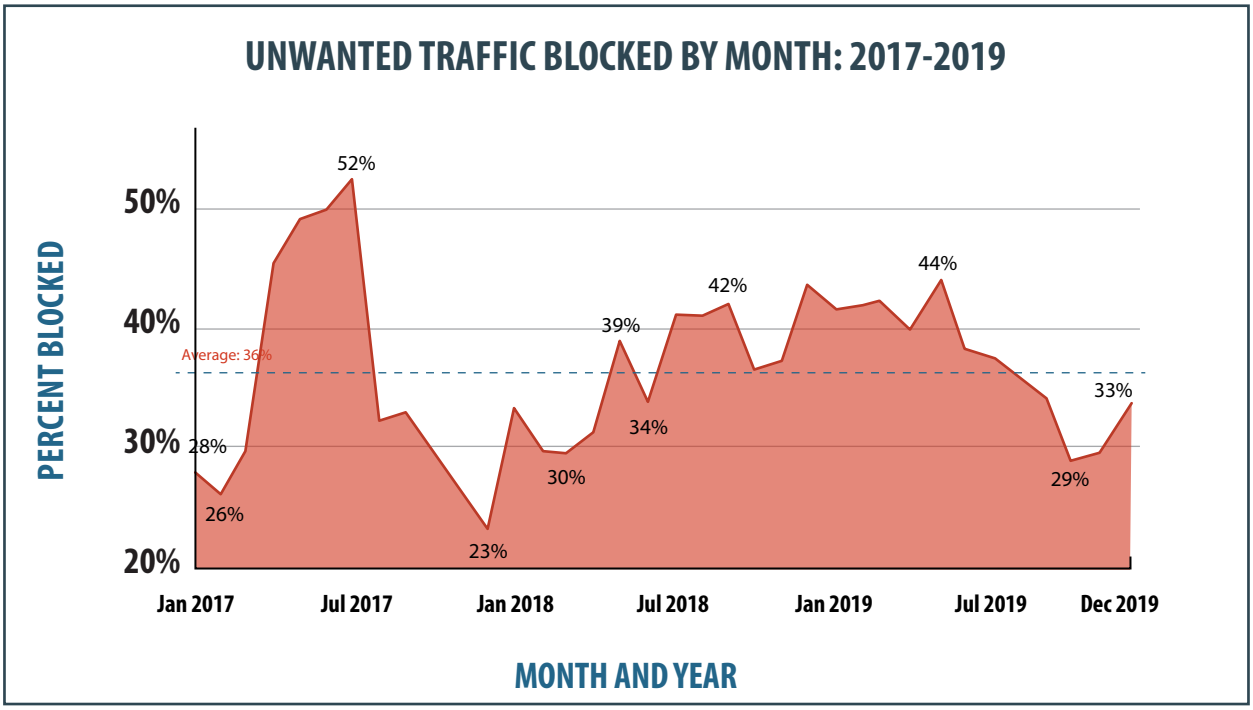
CATEGORY DESCRIPTIONS

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

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

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

SDN MANAGED FIREWALL: KEY TRENDS



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 2019.

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.

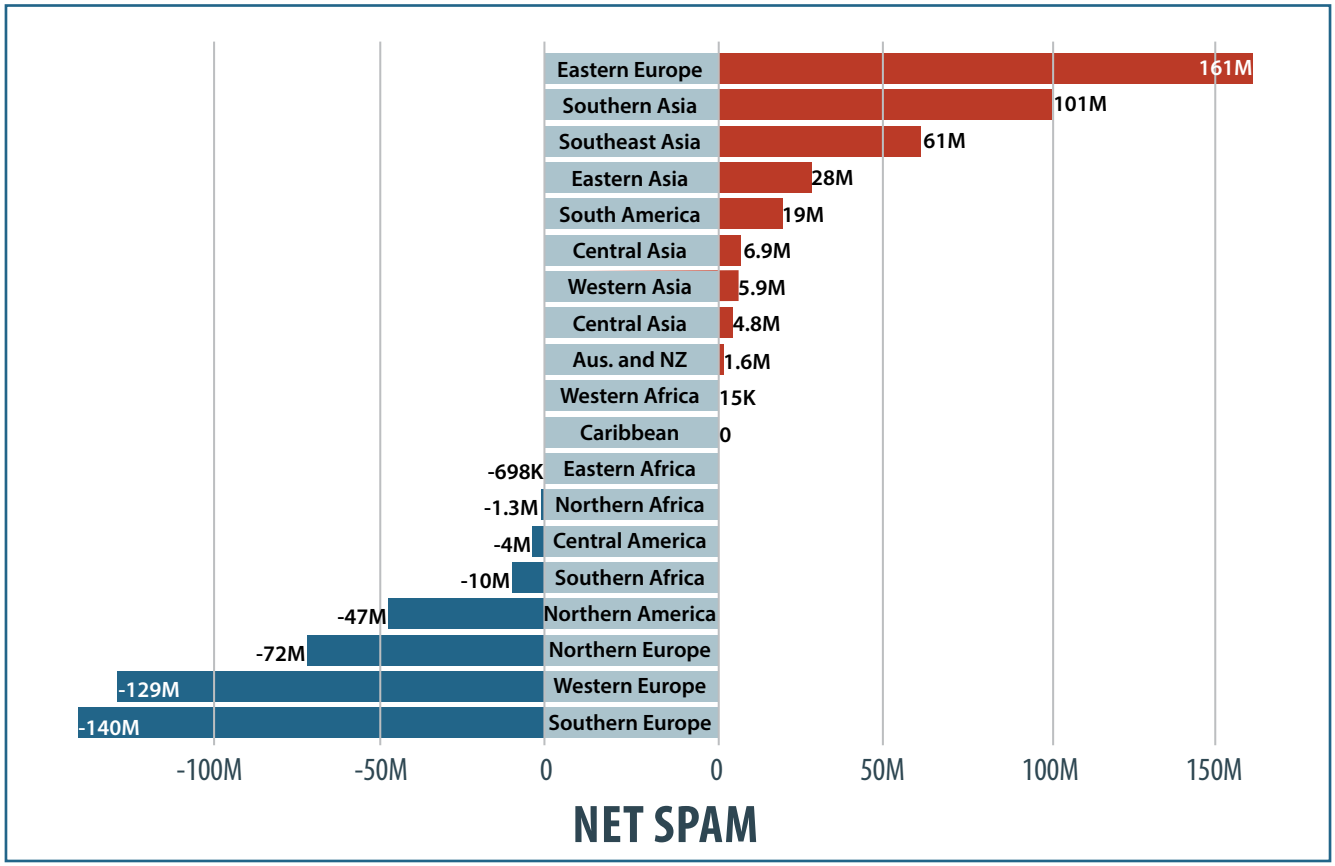
ACTIVE FORTINET NETWORK SECURITY EXPERT CERTIFICATIONS:

NSE 7 – Network Security Architect
Certified to integrate Fortinet products to deploy and administer 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

SPAM, NOT JUST A NUISANCE, IT COULD BE MALICIOUS

Spam has been around as long as email itself. It may seem like just a nuisance, but it could be masking malicious activity. Let's take a look at which countries are the largest creators and largest targets for spam as collected by Fortinet for their Q4 2019 Threat Landscape Report.



Net spam volume exported from world regions (total out – total in).

THE TAKEAWAY

Call, don't click. If you get a suspicious email you weren't expecting, call to verify it's legitimate. Any link clicked could install Ransomware, malware or nasty viruses designed to disrupt or even steal data from you. A well-managed firewall is your first line of defense when it comes to stopping spam and malicious emails.

Proactive prevention is essential in today's business environment. If you only address network issues when there is a problem, your business will end up spending more money (repairs often cost a premium because work needs to be done quickly and employees can't function at full capacity) and losing valuable time. With Managed Firewall Services from SDN, a problem can often be solved before it ever impacts the business. That saves you in the long run.

Also, consider that the more time you spend repairing damage from an attack, the less time you have to focus on your core business competencies. Being able to keep the focus on the mainstay of your business is worth the investment.

THE BIGGEST STORIES OF 2019

NATION ACTORS

From The Washington Post to Forbes, stories of state-sponsored hacking seemed to take the headlines in 2019. North Korea, China, Iran, and others continue to use techniques to steal funds and consumer records, hack critical infrastructure and disrupt business in America.

$70 MIL.

Amount two Russian hackers siphoned from bank accounts including U.S. banks, municipalities, schools, an Ohio dairy, and an order of Catholic nuns in Chicago.

www.usatoday.com/story/news/politics/2019/12/05/two-russian-hackers-charged-thefts-totaling-70-million/2618437001/

$2 BIL.

Amount the United Nations reports North Korea has generated for its weapons programs stealing from banks and cryptocurrancy exchanges.

www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

THE TAKEAWAY

The techniques remain the same. Phishing, exploiting vulnerabilities in hardware and software, and cracking poorly crafted passwords. Be vigilant and don't forget your cyber security basics.

LOOKING AHEAD TO 2020

The reality is businesses and employees alike must understand the cyber threat landscape in order to keep up with the growing reliance on the internet and all of its connected devices. What should we all be aware of in 2020?

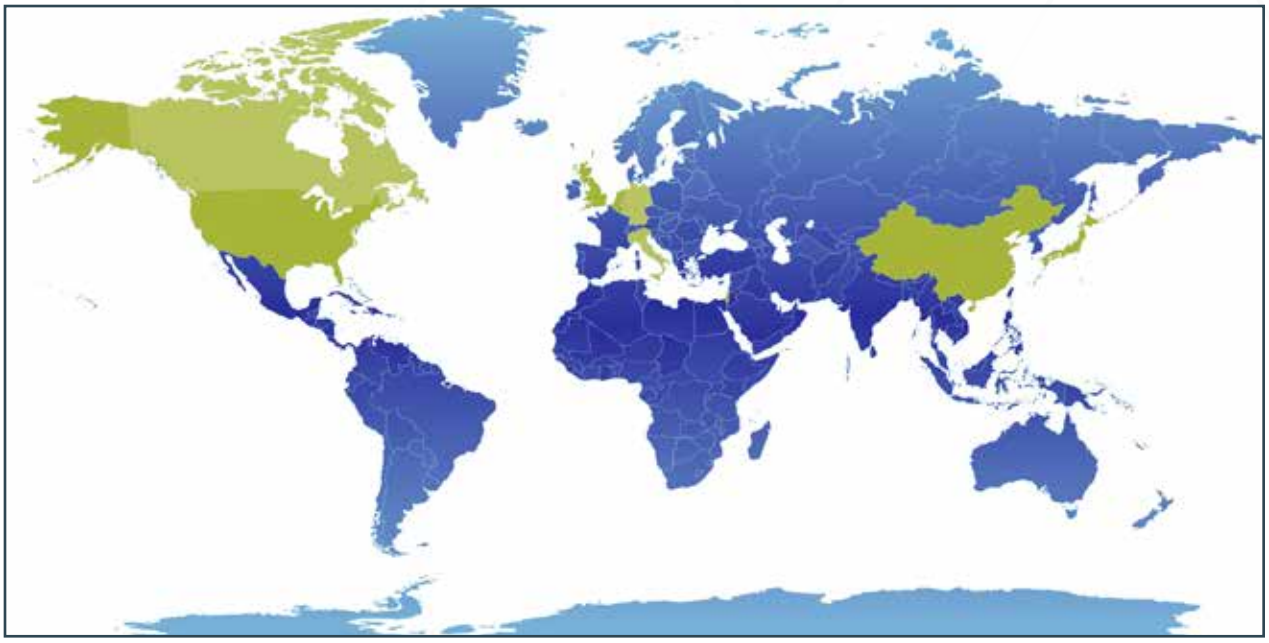
Hacking gets easier all the time. You no longer have to be technical to exploit vulnerabilities or steal data. Reasonably priced toolkits are becoming increasingly accessible to even the entry level hacker.

Local governments will continue to be vulnerable and will continue to get hit with ransomware. New Orleans, Baltimore and Atlanta are just a few of the examples that have made the news. Reduced budgets have made them targets but the end result makes it so cities can no longer afford to be unprepared.

More organizations will seek outside help with their cybersecurity defenses. A $(ISC)^2$ Cybersecurity Workforce Study shows, "59 percent say their organization is at extreme or moderate risk due to cybersecurity staff shortage." As a result, businesses and organizations will need to turn to outside help for their cybersecurity needs.

Sources:
thehill.com/opinion/cybersecurity/479316-2020-cybersecurity-predictions-evolving-vulnerabilities-on-the-horizon
www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0%5Ch

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



#1 UNITED STATES
#2 CHINA
#3 GERMANY
#4 CANADA
#5 JAPAN
#6 ITALY
#7 BELGIUM
#8 UNITED KINGDOM
#9 ISREAL
#10 NETHERLANDS

TAKEAWAYS

- Distributed Denial of Service (DDoS) isn't going away as a security concern. In fact, it's a growing issue. While there are fluctuations in size and frequency – overall it continues to grow as an attack medium in size and complexity.
- We are not in a safe corner of our world in the Midwest. We see the same sort of trends in our region as well. Trends at the national and world levels are mirrored in our Managed DDoS Protection and Managed Firewall systems as well.

GLOBAL TRENDS FROM NETSCOUT BY ARBOR*

- 8.4 MILLION - That is the number of DDoS attacks NETSCOUT Threat Intelligence saw last year alone: more than 23,000 attacks per day, 16 every minute.
- Attackers weaponized seven new or increasingly common UDP reflection/amplification attack vectors in 2019. They also combined new variations of well-known attack vectors—all while remaining operationally efficient and launching pinpoint-focused DDoS attacks.
- 20.4 billion IoT devices are forecast to connect to the internet in 2020 with an ever-growing selection of malware strains to choose from. Vulnerable IoT devices intensify the threat.

* NETSCOUT is powered by Active Threat Level Analysis System (ATLAS®) 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.

SDN COMMUNICATIONS®

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