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 2020. 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/**

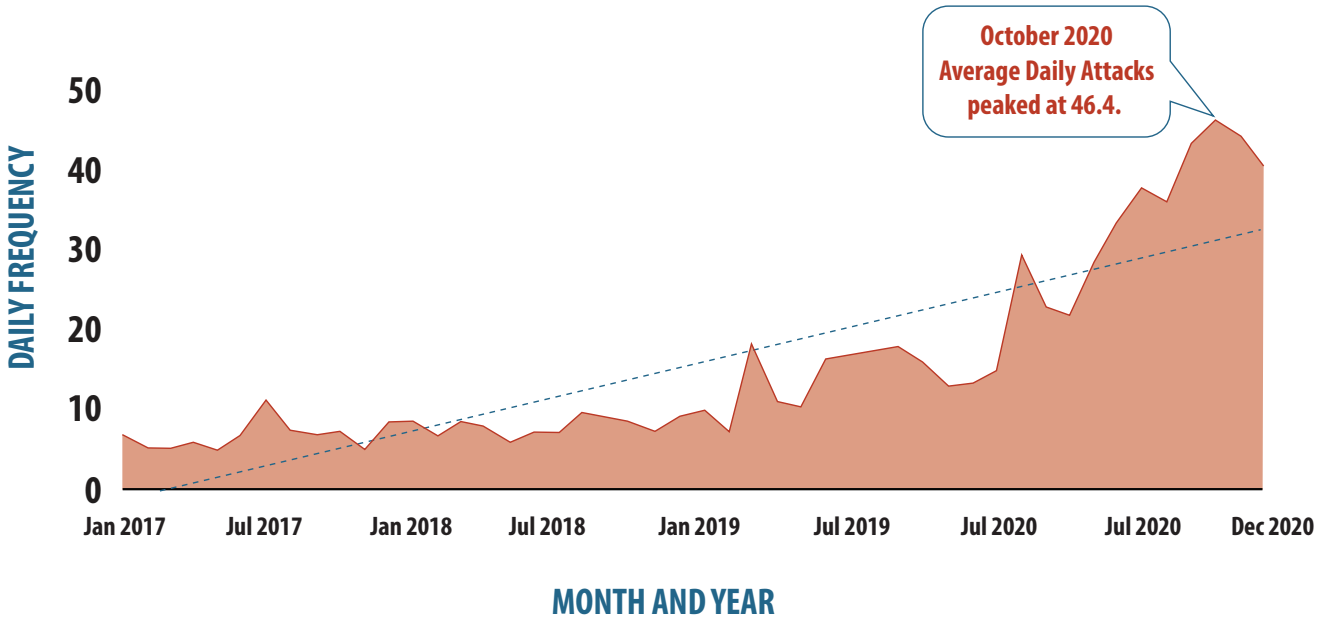
MANAGED DDoS PROTECTION HIGHLIGHTS

ATTACK COUNT
140% increase

AVERAGE DURATION
4.2% increase

AVERAGE ATTACK SIZE
33% decrease

ATTACK FREQUENCY ROLLING TREND



SDN MANAGED DDoS PROTECTION: KEY TRENDS January 1 - December 31, 2020

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.

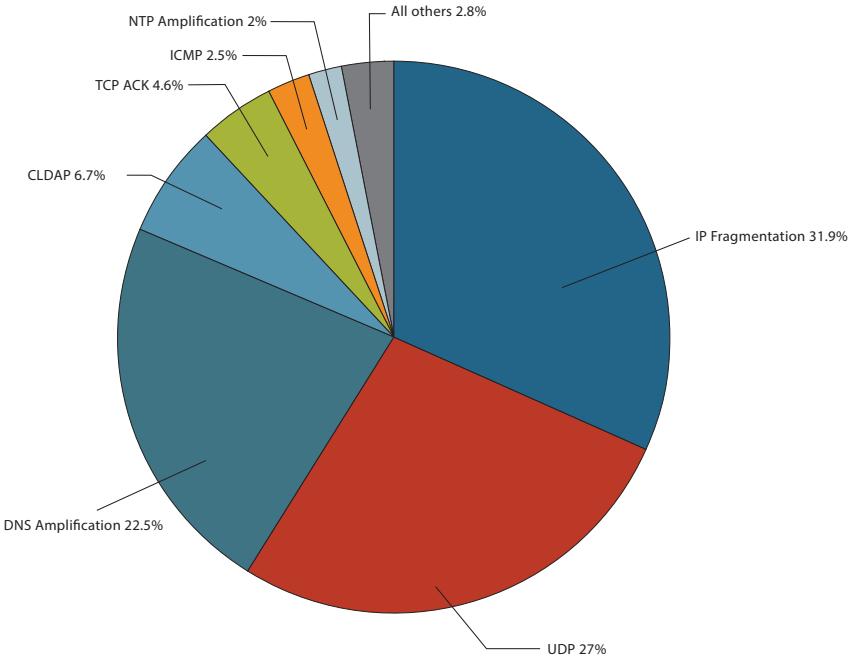
Examples: Syn Flood, Ping of Death

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.

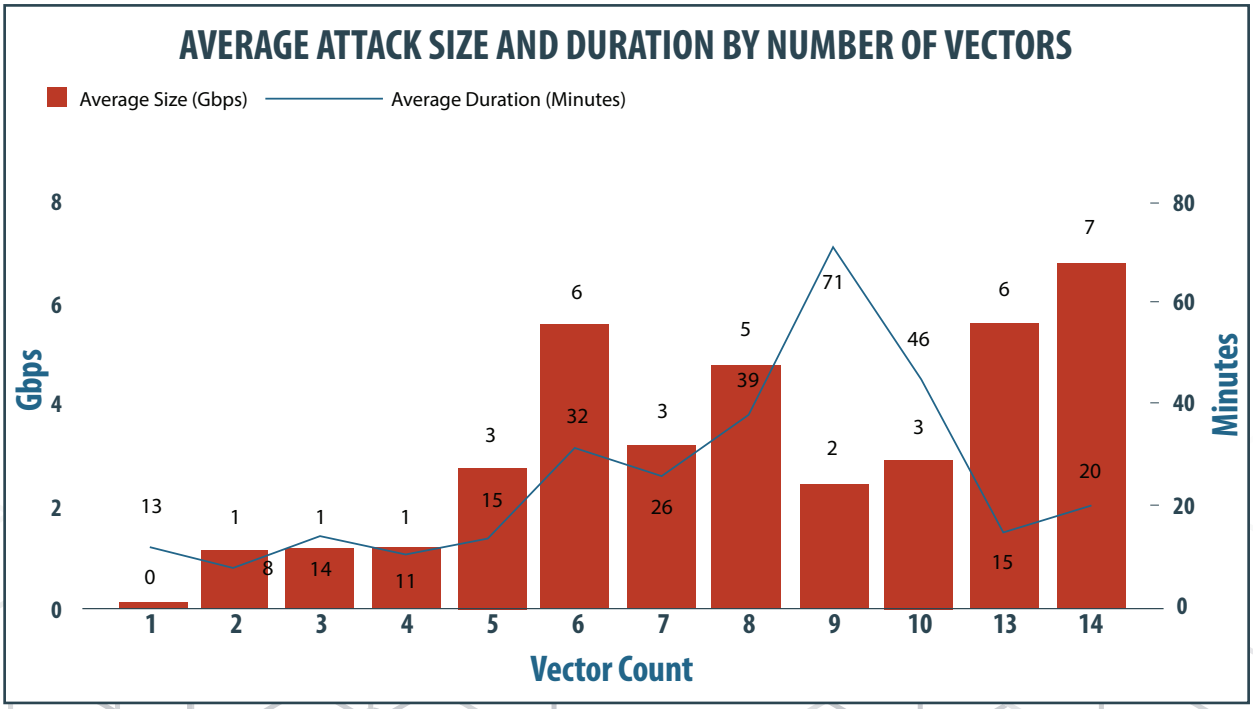
Examples: HTTP Flood, Attack on DNS Services

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

2020 ATTACKS BY VECTOR



AVERAGE ATTACK SIZE AND DURATION BY NUMBER OF VECTORS



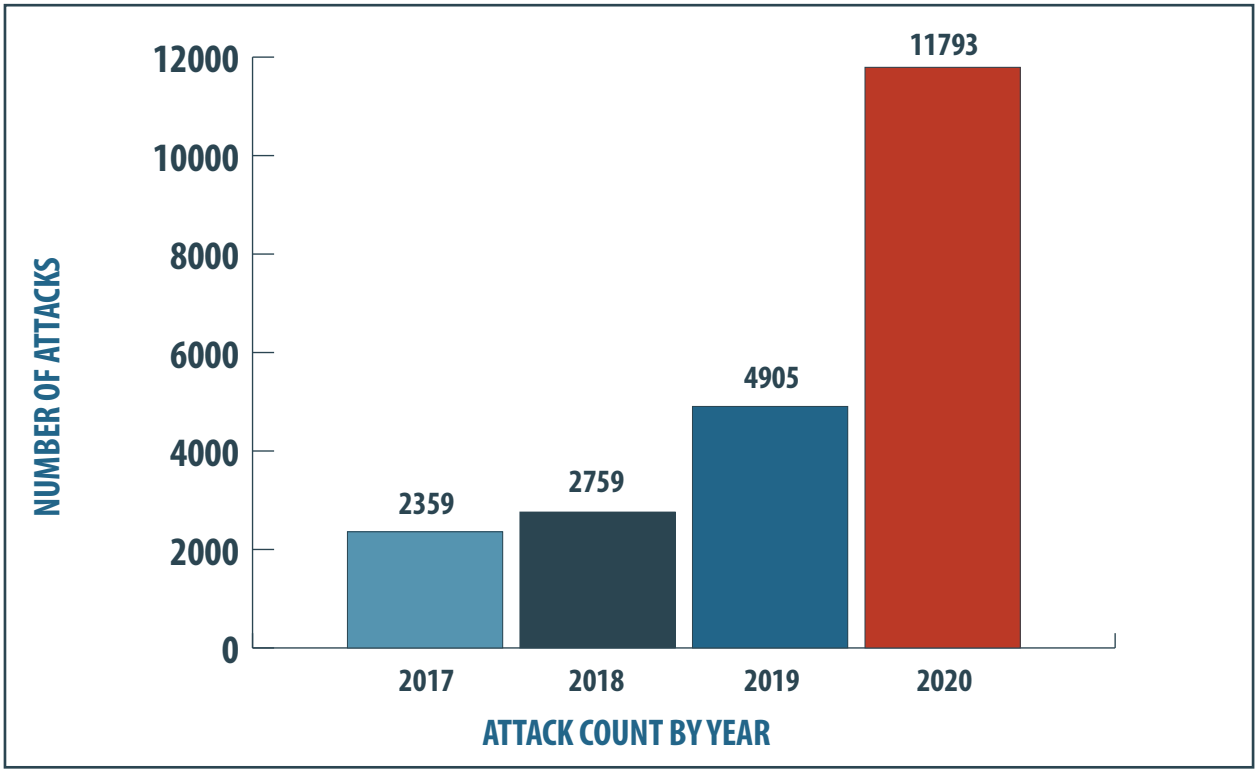
SDN MANAGED DDoS PROTECTION: KEY TRENDS January 1 - December 31, 2020

1.32 GBPS
Average Attack Size in 2020

13 MINUTES
Average Attack Length for 2020

14
Most Vectors Seen with a Single Attack

YEAR OVER YEAR COUNTS January 1 - December 31, 2020



DDOS ATTACKS: RECORD NUMBERS IN 2020*

Hackers and scammers didn't take the pandemic off. The opposite appears to be true.

DDoS attackers focused on COVID-era lifelines such as healthcare, e-commerce and educational services with complex, high throughput attacks designed to overwhelm and quickly take them down as reported by NETSCOUT.

The first half of 2020 witnessed a radical change in methodology to shorter, faster, harder-hitting complex multi-vector attacks according to their threat intelligence lead, Richard Hummel.

In 2020, online platforms and services were under attack worldwide.

SDN Communications also saw attacks increase as the year went on with some of the largest attack counts and number of vectors used since we began Managed DDoS Attack Protection back in January of 2017.

* https://www.netscout.com/threatreport

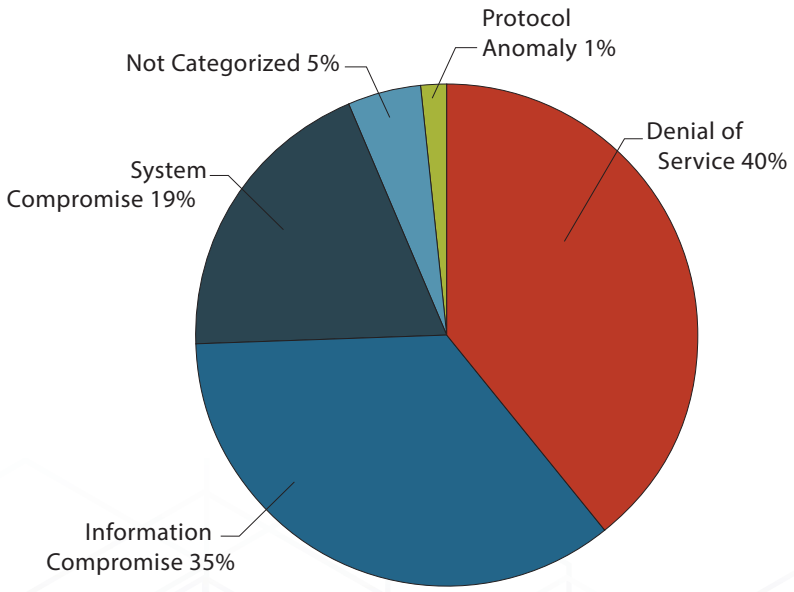
SDN MANAGED FIREWALL: KEY TRENDS January 1 - December 31, 2020

TOP ATTACKS

Attack Name	Impact Category
#1 OpenVAS.Web.Scanner	Information Disclosure
#2 icmp_flood	Denial of Service
#3 udp_flood	Denial of Service
#4 ip_src_session	Denial of Service
#5 HTTP.Server.Authorization.Buffer.Overflow	System Compromise
#6 Lethic.Botnet	System Compromise
#7 tcp_src_session	Denial of Service
#8 SSLAnonymous.Ciphers.Negotiation	Information Disclosure
#9 Web.Server.Password.Files.Access	Information Disclosure

2020 saw Denial of Service profiles enter into the top attacks and DDoS was the top impact category in 2020 bumping off Information Disclosure which was a strong first in 2019.

IMPACT CATEGORIES BY COUNT January 1 - December 31, 2020



CATEGORY DESCRIPTIONS

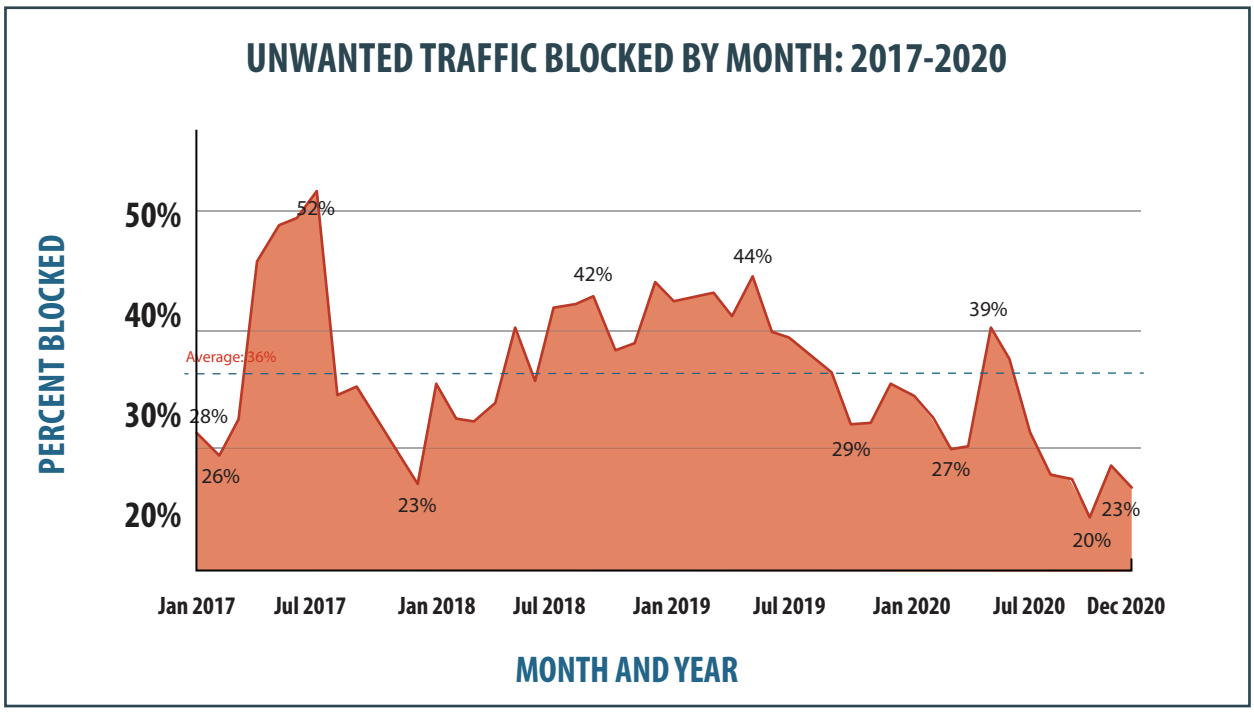
Distributed Denial of Service: DDoS attacks attempt to make your online services unavailable by overwhelming them with traffic from multiple sources.

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



27.9% of all SDN Managed Firewall Traffic was flagged as malicious or spam and was filtered out in 2020. This is actually down from 36.6% in 2019.

While it is impossible to determine what specifically caused the decline in malicious traffic, we speculate the reduction is due to the shifting work environment. Less traffic traversing corporate firewalls due to an increase in remote work might explain the decline in total malicious traffic.

2020 MANAGED FIREWALLS AND REMOTE WORKERS

Although the traffic flagged as malicious or spam in 2020 was down by almost 10% over 2019, don't be fooled into thinking there were fewer attacks. With more people working remotely, employees weren't able to take complete advantage of the security provided by managed firewalls.

Professional and recreational fraudsters alike are busier than ever. In 2020 they had plenty of time to try to cheat you and your employer out of valuable information and money, and they demonstrated creativity in shaping their fraudulent pitches around the dominating subject of the day: COVID-19.

Businesses may wonder how they can better protect their employees in a remote working environment. An option you may want to consider is SD-WAN (software-defined WAN).

SD-WAN uses software-defined infrastructure to connect a company's networks that are geographically distributed and oftentimes difficult to manage. This notable technology can enhance and complement features in your network such as increased agility, security and simplicity of management.

Interested? Go to our site and click on **CONTACT.**

EMAIL SPOOFING: WHAT IT IS AND HOW TO SPOT IT

After the recent hurricanes that struck Texas, Florida and Puerto Rico, there were unsettling reports about fraudsters spoofing caller identification numbers to make scam calls about flood insurance.

In other words, the bad guys disguised their phone numbers to trick the people they called out of information or money.

Despicable, yes. Uncommon, no.

Spoofing attacks come in other forms, too, including texts and emails. Spoofing is even common on social media sites. A fraudster will open an account on Facebook, for example, and copy and use someone else's information. Then, they'll try to trick the victim's friends out of information or money.

Spoofed email is probably a bigger threat, however, and it can be difficult to detect. Spoofing an email typically refers to when a sender poses as a trustworthy source to get something from the recipient.

"It's a type of phishing attack where they spoof an email address," said Chad Pew, manager of IT at SDN Communications in Sioux Falls. "They're either doing it for financial gain or for information."

It's often part of a phishing scheme, which is a deceitful attempt to gain information or access to a network. The spoofing part is when the fakers disguise their messages to come from a legitimate source. For example, the fraudsters will alter the email's "from" address.

CEOs and other business executives are frequent targets because they control resources and usually have access to valuable information. However, spoofed emails can target anyone. They aren't always straight-out requests for information; they might come camouflaged as a bogus alert that encourages action.

Everyone should beware of email headers with spelling errors or messages that look unprofessional and ask for payment or sensitive information.

If you're in any doubt about the authenticity of a request from a business or an organization, look up the sender's contact information independently – don't rely on contact information provided in the suspect message. Then, contact the company directly for verification.

You can take other precautions too; a good place to start is using spam filters.

Security experts at SDN and elsewhere also recommend using a strong and different password for every connected device. That way, if one site gets hacked with pilfered information, other sites can't be easily compromised, too.

Also, use two-factor authentication whenever possible so that stealing a password isn't enough to misuse an account. Hackers also might need a code from a mobile phone to get into your account.

Businesses, in particular, should use tools that filter and protect email access to their networks.

Pew suggests businesses establish an SPF, or Sender Policy Framework, record to help detect email spoofing. It lists in an accessible form which mail servers are permitted to send emails on behalf of a domain.

SDN's spam filtering system stops hundreds, possibly thousands of fraudulent emails every day. Still, emails with deceptive requests can get through the best mechanical protections. Employees are often the last point of defense.

In addition to good equipment and policies, businesses need to invest in good, ongoing training to help employees recognize email threats and other cybersecurity risks. Everyone needs to stay informed and be on guard.

Unfortunately, cybercrime has become so prevalent that it's a good rule of thumb to view any emailed or phoned request for personal or corporate information with a healthy degree of suspicion.

SDN has created a simple infographics for you to share with employees to help educate them on how to identify spoofing attempts. If you'd like to request a set go to:

sdncommunications.com/cybersecurity-posters-2

THE BIGGEST STORY OF 2020

COVID-19 RELATED CYBER ATTACKS

Hackers seized on the pandemic as an opportunity to accelerate attacks on remote workers in new ways. Scammers revised their usual themes, deploying COVID-19 phishing emails to gain access to personal information, commit fraud or download ransomware.

$161 MIL. lost to fraud in COVID-related schemes by Americans, as of October 2020. This tally is likely undercounted. Phishing scams related to COVID relief were popular.

Bloomberg.com

65% of ransomware infections are delivered via phishing. It's the easiest way to get an unsuspecting victim to click and pay.

idagent.com

THE TAKEAWAY

Scammers and hackers will continue to evolve their phishing attempts, taking advantage of the latest news headlines. Be alert and aware. Offenders are ready to pivot their methods and trick you and your employees into clicking that malicious link.

LOOKING AHEAD TO 2021

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 2021?

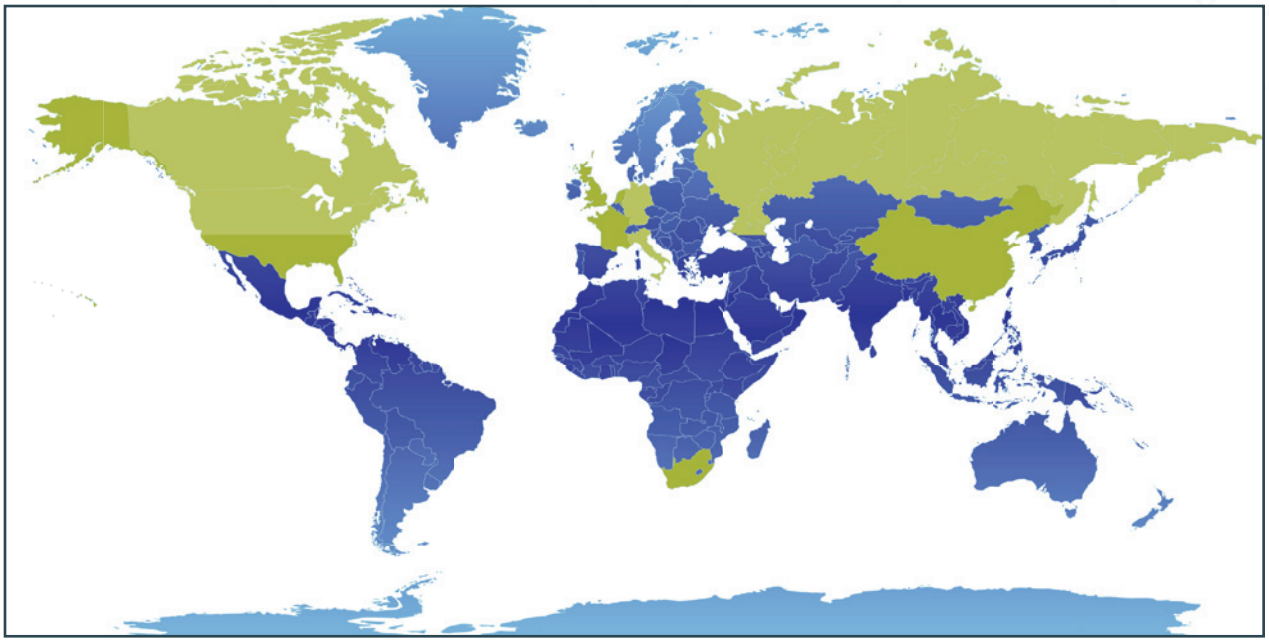
Business Email Compromise (BEC) continues to grow in popularity. Hackers have broadened their sights to include targets of all sizes. Small and medium businesses are just as likely to be hit as large companies.

COVID-19 will continue to be weaponized until the pandemic is under control. In 2020, 21% of fraud experiences had a COVID-19 connection. Hackers will ride this wave as long as they can. Then, they will pivot again.

Ransomware will get worse and worse. Hackers are having too much success to give up this favorite tactic. To combat it, businesses need education, the tools to catch it and the right partner to manage the firewalls that can keep malicious spam at bay.

Sources:
https://www.natlawreview.com/article/banks-top-concern-bec-business-email-compromise-aka-spearphishing
https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-21-security-predictions-for-2021.html

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



#1 UNITED STATES
#2 CHINA
#3 NETHERLANDS
#4 GERMANY
#5 CANADA
#6 RUSSIAN FEDERATION
#7 UNITED KINGDOM
#8 JAPAN
#9 ITALY
#10 SOUTH AFRICA

TAKEAWAYS

- The fox is in the hen house. In 2019 the majority of attacks originated in the United States. This grew in 2020 to 62.86% according to SDN Managed Firewall data.
- In 2020, attackers targeted COVID-era lifelines such as e-commerce, healthcare and educational services.

GLOBAL TRENDS FROM NETSCOUT BY ARBOR*

- Cybercriminals launched record-breaking attacks at online platforms and services during the pandemic – More than 929,000 DDoS attacks occurred in May worldwide, representing the single largest number of attacks ever seen in a month.
- Bad actors focused on shorter, more complex attacks – Super-sized 15-plus vector attacks increased 2,851% since 2017, while the average attack duration dropped 51% from the same period last year.

* 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. The NETSCOUT report was released Sept. 29, 2020.

SDN COMMUNICATIONS®

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