ISSUE 6: FINDINGS FROM 2H 2020

NETSCOUT THREAT INTELLIGENCE REPORT

DDoS in a Time of Pandemic

Including the 16th annual Worldwide Infrastructure Security Report (WISR)

NETSCOUT

CONTENTS

INTERACTIVE VISUALS

View any chart in this report as an interactive visualization by clicking the associated "View Live Chart" button.

A note from the editor:

Against the backdrop of an unprecedented shift toward online workforce participation across the globe, NETSCOUT's ATLAS Security Engineering & Response Team (ASERT) observed a huge upsurge in distributed denial-of-service (DDoS) attacks, brute-forcing of access credentials, and malware targeting of internet-connected devices.

We observed multiple record-breaking events: the most DDoS attacks launched in a single month (929K), the most DDoS attacks in a single year (more than 10 million), and monthly DDoS attack numbers that regularly exceed the 2019 averages by 100,000 to 150,000 attacks. Combined with the weaponization of new reflection/amplification DDoS attack vectors allowing the abuse of misconfigured RDP over UDP, Plex Media SSDP, DTLS services, an increasingly complex threat landscape rapidly emerged. And if that weren't enough, a new threat actor known as Lazarus Bear Armada launched a global DDoS extortion campaign, using network reconnaissance to launch multivector attacks on critical pandemic infrastructure elements such as VPN concentrators, authoritative and recursive DNS servers, and upstream internet service providers' (ISPs') peering and customer aggregation routers.

In the face of this chaos, service providers and security experts rose to the occasion and stalwartly defended the critical infrastructure of our online world. By leveraging world-class engineering skills and key platforms such as NETSCOUT's ATLAS, our online access withstood the record-breaking attacks of 2020. Businesses remained connected to their employees, students continued their education via distance learning, and ecommerce revenue increased by leaps and bounds. Such perseverance and commitment has helped users and organizations not only to survive, but also to thrive in this permanently altered digital landscape.

Richard Hummel
Threat Intelligence Lead, NETSCOUT

Contributors: *Richard Hummel, Carol Hildebrand, Hardik Modi, Chris Conrad, Roland Dobbins, Steinthor Bjarnson, Jon Belanger, Gary Sockrider, Philippe Alcoy, Tom Bienkowski*

Partners: REVERSINGLABS neustar

NETSCOUT CYBER THREAT HORIZON

If you are looking for real-time data on global DDoS attacks, Cyber Threat Horizon is an invaluable (and free) tool.

Today's cyberthreat landscape is constantly evolving, requiring visibility into malicious threats. True situational awareness requires a global view beyond your organizational perspective. NETSCOUT Cyber Threat Horizon is a free tool composed of highly curated, real-time global threat data presented in a way that allows you to understand how it impacts your organization.

01 Introduction

Executive Summary

Not all world records are cause for celebration—just look at the DDoS attack numbers from 2020.

As the COVID-19 pandemic triggered a massive shift in internet usage, cybercriminals quickly pounced, launching more than 10 million DDoS attacks aimed at crippling targets with a heavy reliance on online services. Attack frequency spiked 20 percent year over year and 22 percent for the last six months of 2020.

Research from both NETSCOUT's ATLAS Security Engineering & Response Team (ASERT) and the 16th annual Worldwide Infrastructure Security Report (WISR) survey shows that the COVID-19 pandemic was the clear catalyst for this year's unprecedented DDoS attack activity. Vital pandemic industries such as ecommerce, streaming services, online learning, and healthcare all experienced increased attention from malicious actors targeting the very online services essential to remote work and online life. According to data from the WISR, 83% of enterprises that suffered a DDoS attack reported that firewalls and/or VPN devices contributed to an outage due to the traffic, a year-over-year increase of more than 20 percent.

In mid-August, Lazarus Bear Armada (LBA) launched one of the largest campaigns of DDoS extortion attacks yet seen. Unsurprisingly, the number of DDoS extortion attacks reported by enterprise WISR respondents ballooned by 125 percent. LBA's work was likely also influenced by the exigencies of the pandemic: the group's victims included businesses involved in COVID-19 testing and vaccine development—enticing targets given their combination of both deep pockets and urgent deadlines. In addition to conventional attacks on internet-facing services, the cybercriminals also focused on disrupting ongoing operations within a company, such as the inbound/outbound use of VPNs, firewalls, and cloud-based tools by employees working from home.

83%

Of enterprises that suffered a DDoS attack reported that overloaded firewalls and/or VPN concentrators contributed to the outage

Key Findings

01

DDoS crosses the 10 million attack threshold

For the first time in history, the annual number of observed DDoS attacks crossed the 10 million threshold, with NETSCOUT's ASERT seeing 10,089,687 attacks over the course of the year.

02

A new normal: More than 800,000 attacks per month

As the pandemic lockdown took effect, DDoS attacks exceeded 800,000 in March and remained above that threshold for the rest of the year. Indeed, cybercriminals launched 929,000 DDoS attacks in May, the single largest number of monthly attacks we've ever seen. That is a significant increase from the highest monthly total observed in the six months prior—732,000 attacks in December 2019.

03

Global DDoS extortion campaign

LBA launched a global campaign of DDoS extortion attacks that took down the New Zealand stock exchange in its debut attack. From there, LBA broadened its target base considerably to include financial services and financial-adjacent entities, healthcare, communications service providers, internet service providers (ISPs), large technology companies, and manufacturing. The downstream effect was significant, with the number of DDoS extortion attacks reported by WISR respondents increasing by 125 percent year over year. The campaign remains active as adversaries have begun retargeting previously targeted organizations. The adversary cites the victim's failure to pay the original extortion demand as the cause for renewed attacks.

04

UDP-based DDoS attack vectors fuel attack increases

New reflection/amplification DDoS vectors that leverage abusable commercial products and open-source User Datagram Protocol (UDP) capabilities continued to be discovered across the internet, fueling the next generation of attacks. Cyber actors exploited and weaponized at least four such DDoS attack vectors in 2020. As these new vectors become available, adversaries such as LBA co-opt them, as was the case with the Microsoft Remote Desktop Protocol (RDP)-over-UDP vector weaponized in late 2020. The total number of vectors used in individual attacks has soared, with a record-setting 26 attack vectors deployed in a single attack in 2020.

05

Botmasters exploit pandemic vulnerabilities

Malware king Mirai continued to thrive in an Internet of Things (IoT)-rich environment, as remote work and online learning shifted core workforce access away from enterprise-grade protection and toward consumer-grade devices. A surge in brute-forcing and malware samples circulating in the wild paints a very clear picture, with adversaries attempting to absorb more devices into their botnets to further strengthen the frequency, size, and throughput of DDoS attacks worldwide.

This all adds up to a year of unprecedented DDoS attack activity across an already-booming cybercrime economy.

And as we know, adversaries thrive on constant innovation. Attacks will only grow more complex, and threat actors will continue to discover and weaponize new attack vectors designed to exploit the vulnerabilities exposed by this enormous digital shift. Protecting our connected world has never been more important.

NUMBER OF ATTACKS 2H 2020

10,089,687

▲ **20%** Increase year over year

▲ **22%** Increase in the last six months of 2020

02

DDoS Global Attack Trends

As the global pandemic forced a significant portion of the world into lockdown, our ability to shift work and life online proved to be a vital lifeline.

Unfortunately, such sudden and major changes often expose new vulnerabilities, and the COVID-19 pandemic was no exception. Armed with an ever-improving set of tools that lowered the bar to entry for launching more-complex, higher-throughput attacks, cybercriminals eagerly leveraged new weaknesses, setting the stage for a banner year for DDoS activity.

For the first time in history, the annual number of DDoS attacks crossed the 10 million threshold, with ASERT observing a staggering 10,089,687 attacks over the course of the year. This represents a 20 percent increase in attacks year over year, but that includes the prepandemic months of January, February, and most of March. For the second half of 2020, which was entirely pandemic-ridden, attacks rose 22 percent year over year.

"When the COVID pandemic hit, the numbers skyrocketed as attackers took aim at distracted and heavily internet-dependent companies. Then they rose again when the DDoS extortion campaign started, leading to a rash of ransom-related DDoS attacks."

CARLOS MORALES, CHIEF TECHNOLOGY OFFICER OF SECURITY SOLUTIONS, NEUSTAR, INC. (NETSCOUT PARTNER)

2020 STATISTICS

1.12 TBPS
Max attack size (EMEA)

581 MPPS
Max throughput (APAC)

3,753,883 ATTACKS
Largest regional attack frequency (EMEA)

39.83 MIN
Average global attack duration

As cybercriminals quickly exploited pandemic-driven opportunities, another kind of "new normal" emerged. Not only did DDoS attack frequency increase by nearly 1.6 million attacks year over year, but monthly DDoS attack numbers also spiked. Starting in March, as widespread pandemic lockdowns took effect, monthly attack frequency increased by between 100,000 and 200,000 compared with the previous six months, consistently exceeding 800,000 attacks per month.

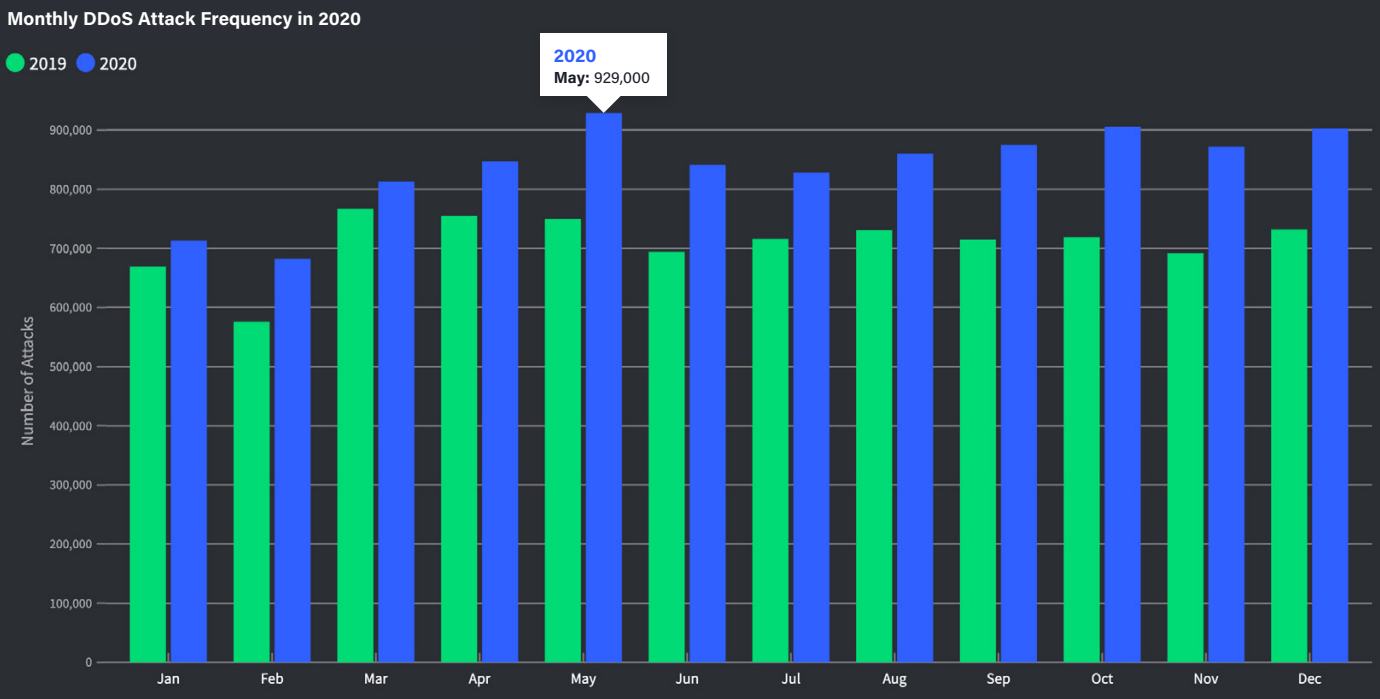


Figure 1: Monthly DDoS Attack Frequency 2020

Data: Cyber Threat Horizon

VIEW LIVE CHART

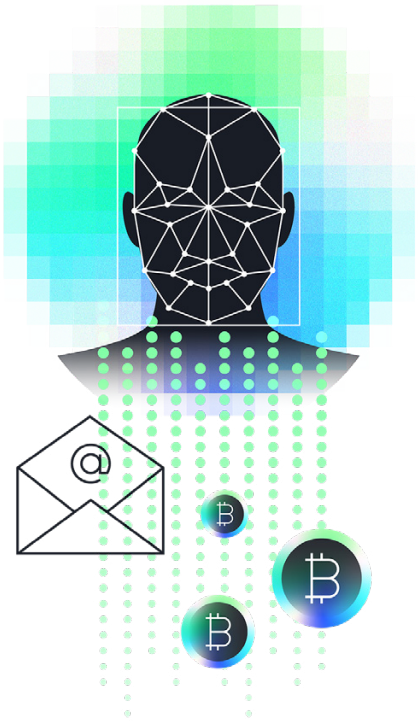
ATTACK FREQUENCY

709,666
Average monthly attacks in 2019

839,083
Average monthly attacks in 2020

NEARLY 130,000
More attacks per month on average

LBA DDoS Extortion Campaign



Against the backdrop of a significant uptick in DDoS attacks during the pandemic, a threat actor given the moniker Lazarus Bear Armada (LBA) kicked off a long-running DDoS extortion campaign in mid-August of 2020. LBA launched DDoS attacks against organizations across a wide array of geographies and industries, demanding "protection" payments via Bitcoin in exchange for (supposedly) refraining from further attacks against the targets.

The attackers made extensive use of multivector DDoS attacks against not only applications and services, but also network and remote-access infrastructure elements. Unlike many DDoS extortionists, LBA often followed through on threats to repeatedly attack targeted organizations if they fail to pay. Attacks associated with this DDoS extortion campaign ranged in size from 50 Gbps to 450 Gbps. LBA demonstrated a certain amount of persistence, revisiting targets weeks and months after initial contact with a second extortion email that threatened further consequences should the targeted organization fail to acquiesce to their payment demands.

DDoS Attack Vectors Used by LBA

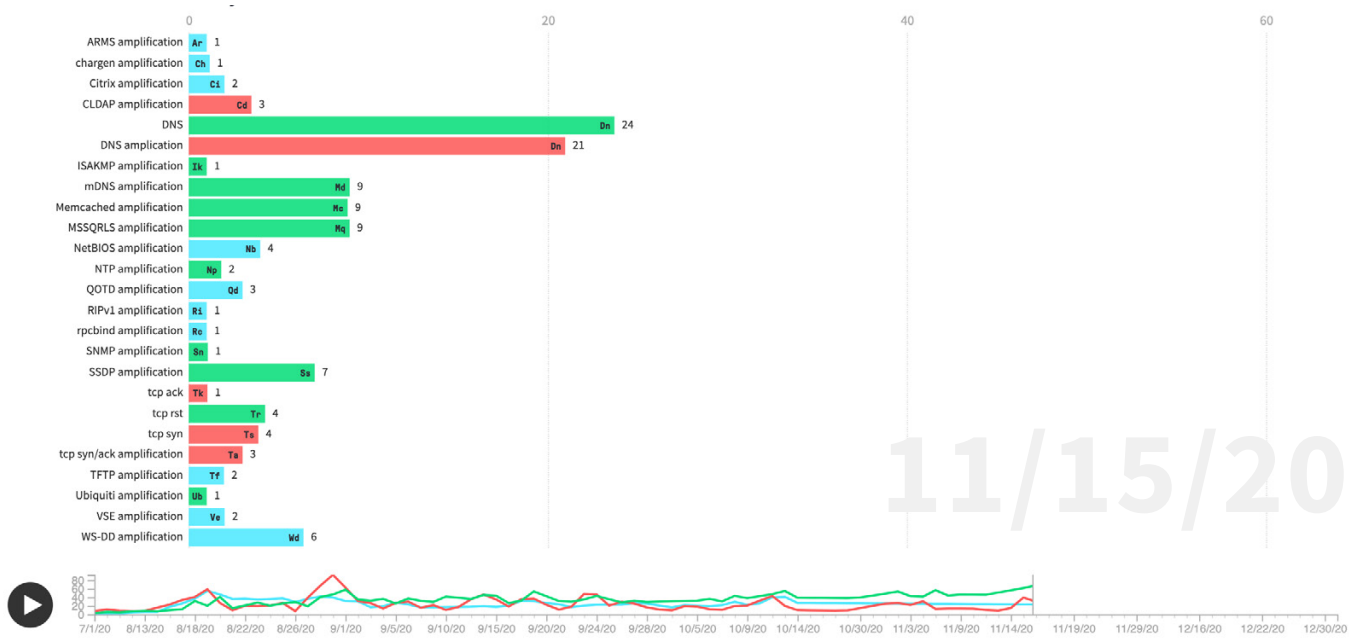


Figure 2: DDoS Attack Vectors Used by LBA

Data: Cyber Threat Horizon

VIEW ANIMATION

Industries Targeted by LBA

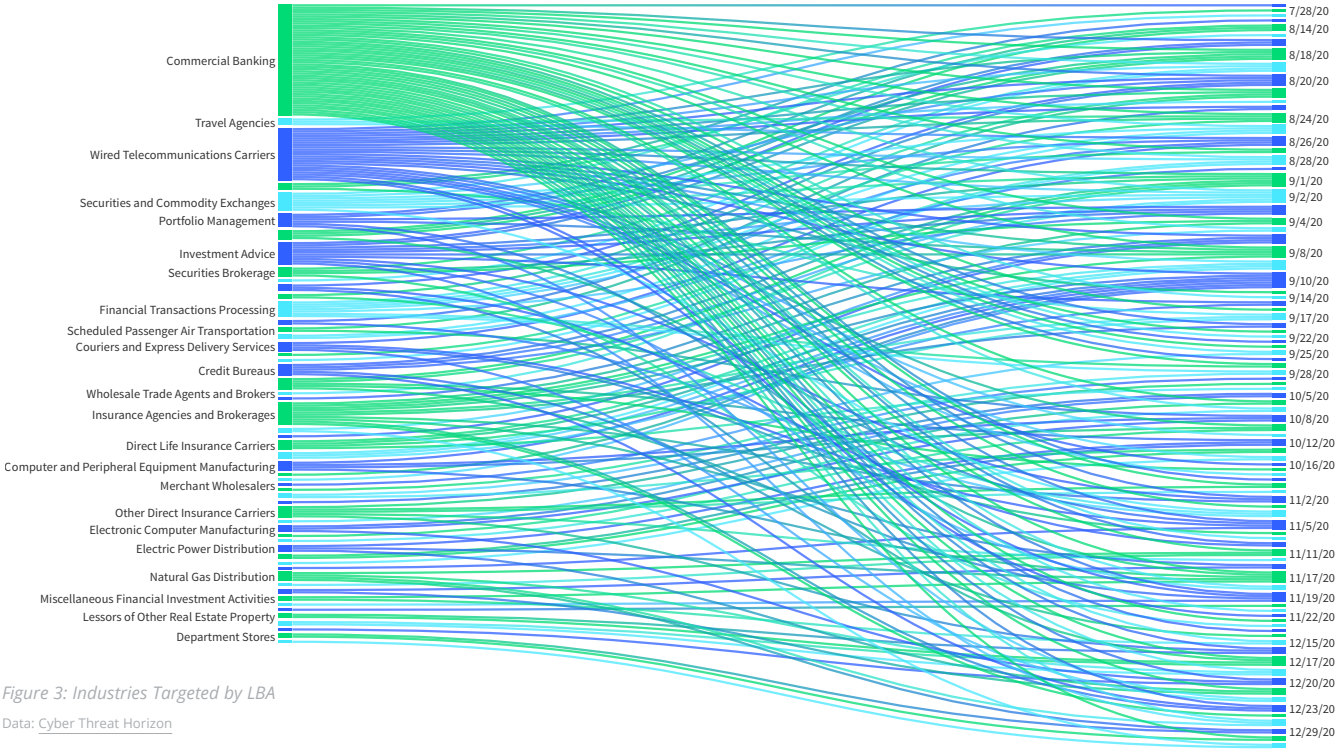


Figure 3: Industries Targeted by LBA

Data: Cyber Threat Horizon

VIEW LIVE CHART

LBA Attacks

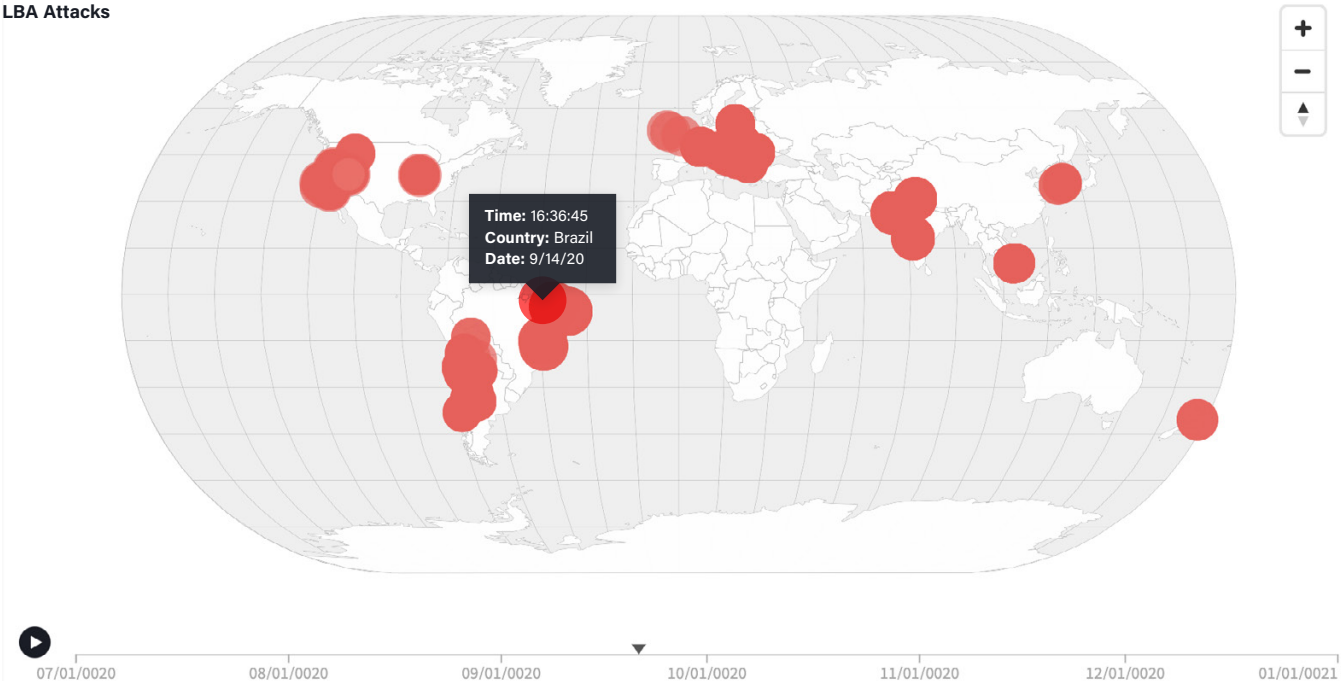


Figure 4: LBA Attacks

Data: Cyber Threat Horizon

VIEW ANIMATION

Vertical Industry Attacks

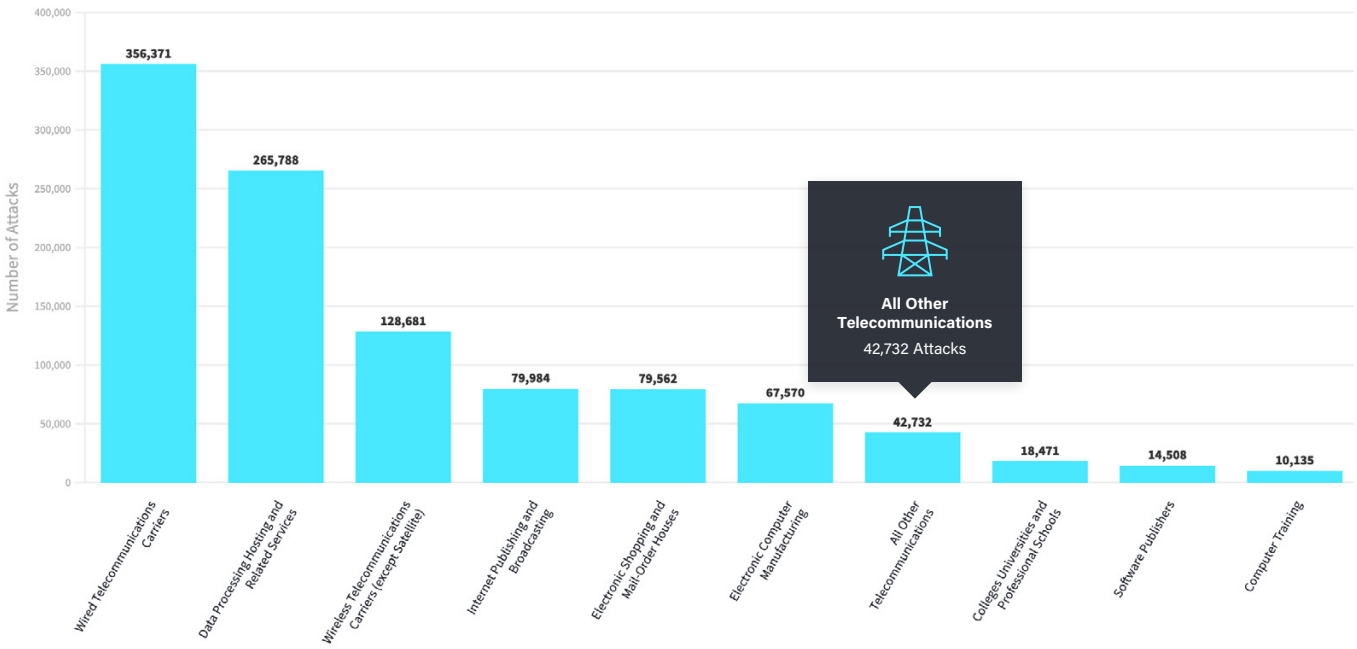
We analyzed attack data by North American Industry Classification System (NAICS) codes, which group companies into 22 broad categories that contain multiple large subvertical sectors. The top 10 vertical industries under attack in the second half of 2020 further illustrates the enormous impact COVID-19 had on DDoS attack activity. Threat actors always have embraced an opportunistic pivot, and this was no exception as they enthusiastically flocked to the ensuing smorgasbord of new opportunities.

The top three listed sectors fall under the category of Old Faithfuls, because attacks on both subscribers and their operational infrastructures are inherent to their role as connectivity providers. However, the fourth sector—Internet Publishing and Broadcasting—is by no means a usual suspect in our top 10. Its presence can be summed up in two words: Netflix and Zoom. Similarly, online shopping, which grew an impressive 44 percent in 2020, represents another pandemic stalwart that came under increased attack, as did online learning. Interestingly, this activity was seen not only at the usual hot spots of colleges and universities but also at the high school and middle school level. With DDoS-for-hire services both readily available and incredibly cheap, it seems likely that budding online delinquents set about playing hooky on an internet scale.

UNUSUAL SUSPECT

Internet Publishing and Broadcasting is by no means a usual suspect in our top 10. Its presence can be summed up in two words: Netflix and Zoom.

Top 10 Vertical Industry Targets



VIEW LIVE CHART

Figure 5: Top 10 Vertical Industry Targets

Data: Cyber Threat Horizon

DDoS Attack Vectors

The Periodic Table of Attack Vectors

Research into attack vectors and how attackers leverage them illuminates the ever-evolving nature of the DDoS threat landscape. This table sorts vectors by attack numbers, as well as digging into details about risk level and amplification factors.

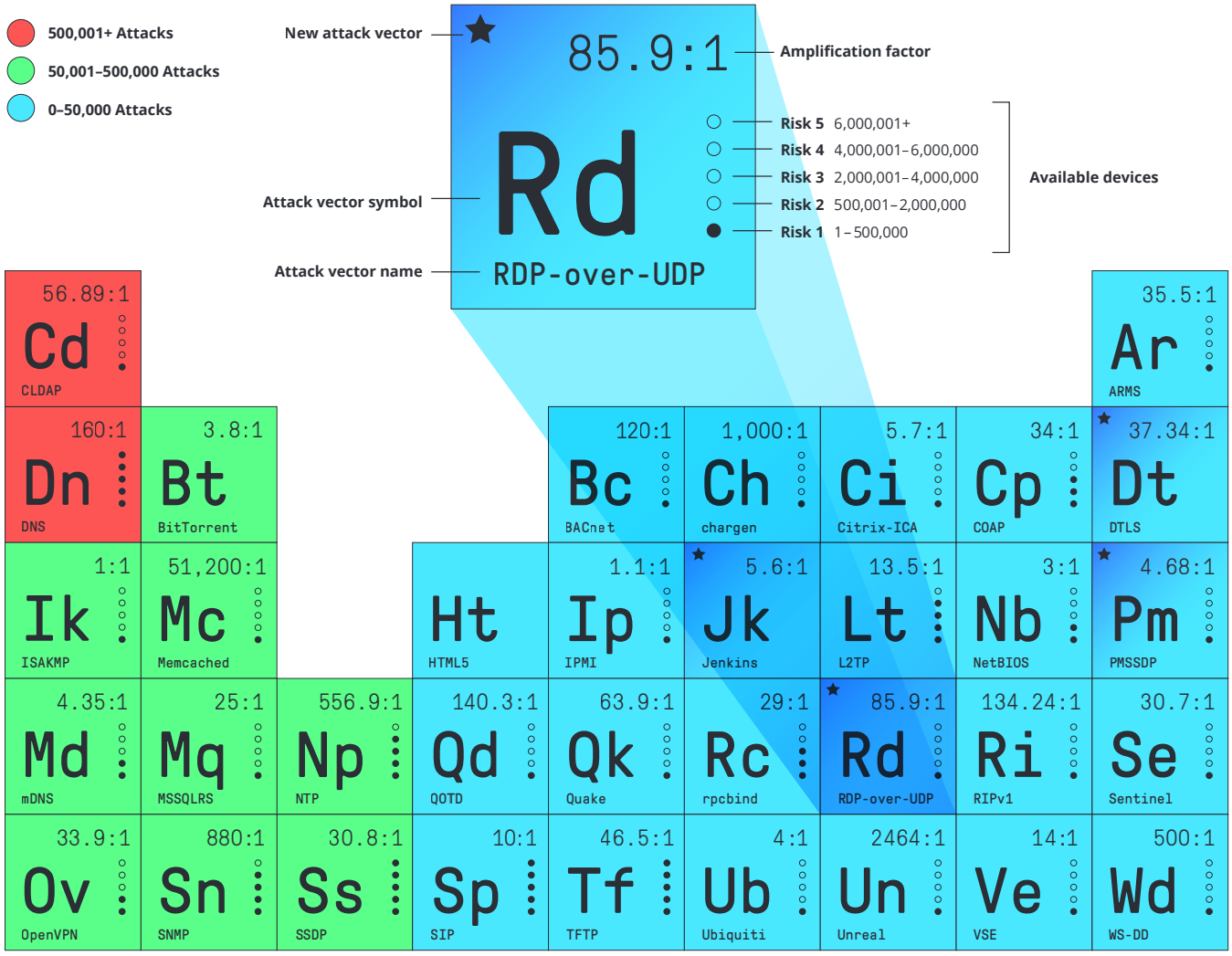
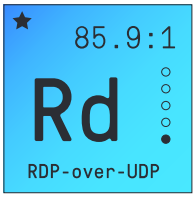


Figure 6: Periodic Table of Attack Vectors

Abusable open-source and commercial applications and services based on UDP remained a valuable asset for attackers, who mined them to discover new reflection/amplification DDoS attack vectors to power a new wave of attacks. Here's a rundown of the latest attack vectors:

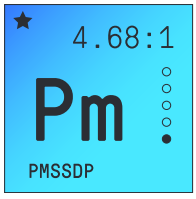


Microsoft Remote Desktop Protocol (RDP)

Included in Microsoft Windows operating systems, RDP is intended to provide authenticated remote virtual desktop infrastructure (VDI) access to Windows-based workstations and servers. The RDP service can be configured by Windows systems administrators to run on TCP/3389 and/or UDP/3389.

When enabled on UDP/3389, the Microsoft Windows RDP service may be abused to launch UDP reflection/amplification attacks with an amplification ratio of 85.9:1. The amplified attack traffic consists of non-fragmented UDP packets sourced from UDP/3389 and directed toward the destination IP address(es) and UDP port(s) of the attacker's choice. In contrast to legitimate RDP session traffic, the amplified attack packets are consistently 1,260 bytes in length and are padded with long strings of zeros. Approximately 33,000 abusable Windows RDP servers have been identified to date.

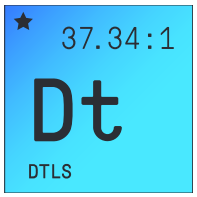
Observed attack sizes range from ~20 Gbps to ~750 Gbps. As is routinely the case with newer DDoS attack vectors, it appears that after an initial period of employment by advanced attackers with access to bespoke DDoS attack infrastructure, RDP reflection/amplification has been weaponized and added to the arsenals of booter/stresser DDoS-for-hire services, placing it within the reach of the general attacker population.



Plex Media SSDP (PMSSDP) Reflection/Amplification

Plex Media Server is a personal media library and streaming system that runs on modern Windows, macOS, and Linux operating systems, along with variants customized for special-purpose platforms such as network-attached storage (NAS) devices, external RAID storage units, and digital media players. Plex Media Server instances can potentially be abused as part of possible DDoS attacks if they have been deployed either on a public-facing network demilitarized zone; in an internet data center (IDC); or with manually configured port-forwarding rules that forward specific UDP ports from the public internet to devices running Plex Media Server.

These actions can have the effect of exposing a Plex Universal Plug and Play (UPnP)-enabled service-registration responder to the general internet, where it can be abused to generate reflection/amplification DDoS attacks. To differentiate this particular attack vector from generic Simple Service Directory Protocol (SSDP) reflection/amplification, it has been designated as Plex Media SSDP (PMSSDP) reflection/amplification. To date, approximately 37,000 abusable PMSSDP reflectors/amplifiers have been identified on the public internet.



DTLS Reflection/Amplification

Datagram Transport Layer Security (DTLS) is a version of the TLS protocol implemented on the stream-friendly UDP transfer protocol for securing datagram-based applications to prevent eavesdropping, tampering, or message forgery. While an anti-spoofing mechanism was designed into DTLS from the outset, it was described in the relevant standards documents as "recommended", rather than "mandatory". As a result, some implementations don't leverage the anti-spoofing mechanism by default, and thereby can be abused to launch reflection/amplification DDoS attacks.

The default configuration for DTLS services running on Citrix Application Delivery Controllers (ADCs) with older software versions did not initially enforce the anti-spoofing mechanism by default, resulting in a population of Citrix ADCs that were abusable as DTLS reflectors/amplifiers. It also led to this vector being initially mischaracterized as being Citrix-specific, when in reality there are other DTLS implementations that, if misconfigured, can also be abused to launch DTLS reflection/amplification attacks. Although Citrix issued patched software, a population of abusable DTLS reflectors/amplifiers remains that is still being leveraged by attackers.

Jenkins Reflection/Amplification

A popular open source automation server used in almost all modern deployments, Jenkins servers support using a UDP multicast/broadcast network discovery protocol to locate other Jenkins instances. Upon receiving a packet containing any payload (1 byte is enough) on UDP port 33848, the Jenkins server will respond with full information on the deployment. An attacker can therefore generate a spoofed UDP packet and send it to the Jenkins server, generating a reflection/amplification attack with an amplification factor up to 5.6:1.

However, the servers generally are so underpowered and fragile that they tend to fall over when abused as reflectors/amplifiers, especially when they're stimulated to generate continuous streams of packets. As a result, this attack is generally self-limiting, because vulnerable Jenkins servers will quickly collapse when used as reflectors, resulting in collateral damage to the Jenkins servers.

Top DDoS Vectors by Attack Count

UDP-based reflection/amplification attacks continue to dominate the list of most popular attack vectors, with TCP ACK flood attacks coming in a close second. This represents a changing of the guard, given that TCP SYN floods were dominant in previous years. However, Domain Name System (DNS) reflection/amplification attack frequency rose steadily over approximately the past 18 months and became the top vector of choice in 2020.

2020 Top DDoS Attack Vectors by Attack Count

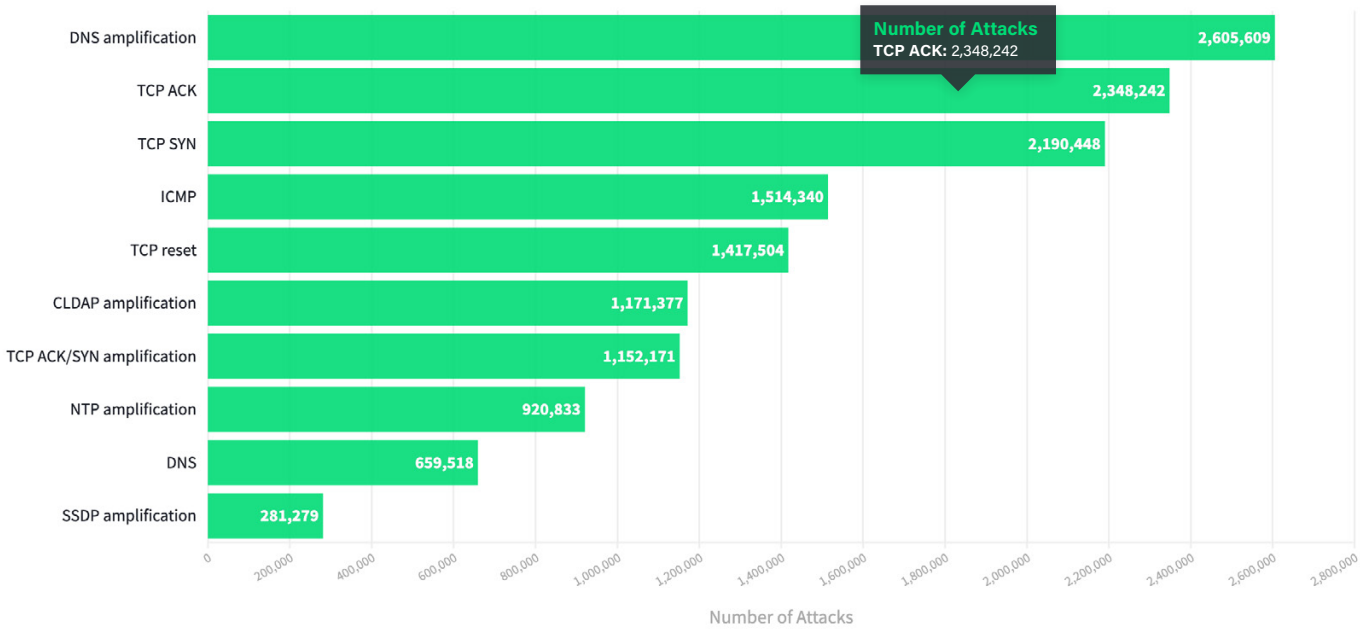


Figure 7: 2020 Top DDoS Attack Vectors by Attack Count

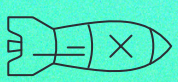
Data: Cyber Threat Horizon

Some perceived TCP SYN and ICMP floods may be legitimate clients trying to connect to downed servers/services. These are called "sympathetic attacks."

VIEW LIVE CHART

CLOSE UP

DNS ATTACK



COST

Up to six figures

IMPACT

Lost sales, lost customers, impacted productivity, legal liability, brand damage

Source: Neustar

Multivector Attacks: More of a Bad Thing

When we look at all these high-level statistics, it seems as if they move in only one direction: up and to the right. During the second half of 2020, the epic number of overall attacks drove increases at all levels, from single-vector attacks to those using 25 vectors. In particular, we noted the growing prevalence of 15-plus vector attacks. Adversaries often leveraged between 15 and 25 vectors to launch complex, high-volume attacks that combined multiple different attack vectors aimed at differing layers of enterprise and service provider infrastructures.

Attacks that used 15 to 25 vectors increased between 9 percent and 312 percent, with particular growth noted in attacks that used 15 to 21 vectors.

▲ 9-312%

Increase in attacks that used 15 to 25 vectors

Percent Change in Multivector Attacks

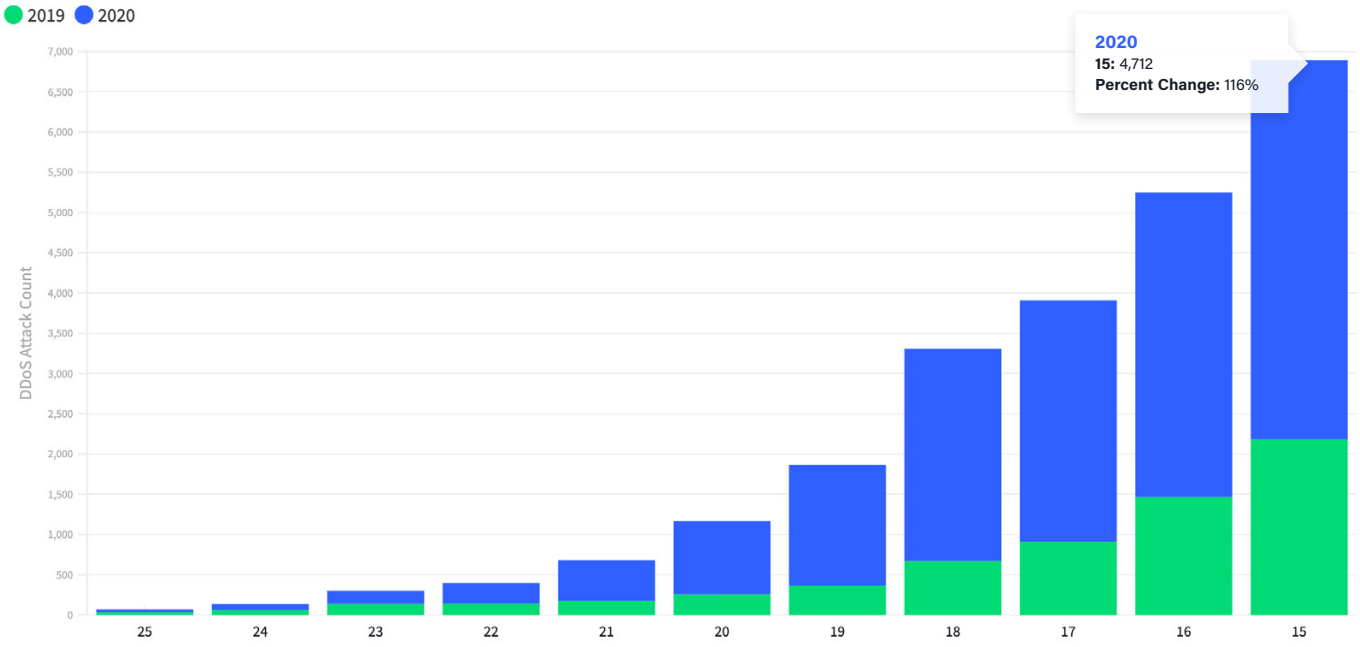


Figure 8: Percent Change in Multivector Attacks

Data: Cyber Threat Horizon

VIEW LIVE CHART

Impact of DDoS Traffic

This was a record-breaking year for DDoS attacks—and that has to have an impact on global infrastructure, particularly since DDoS attackers don't pay for transit costs. Instead, that cost is generally passed down to everyone who uses the internet. So we continued to dig into the details of how much traffic on the global internet is due solely to DDoS attacks.

Once again, we looked at the totality of activity in both bandwidth (bits per second) and throughput (packets per second) to gauge just how much aggregate traffic crosses internet pipelines in any given minute of time. Known as the DDoS Attack Coefficient (DAC), this measurement illustrates the continual presence of DDoS traffic across all regions. In essence, it shows the "DDoS tax" that we all end up paying.

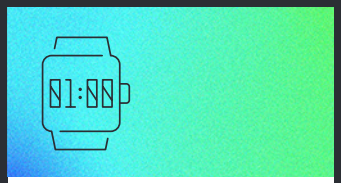
DDoS Attack Coefficient: Max Bandwidth

Month	APAC	EMEA	LATAM	NAMER	Regional Breakdown
Jul	774.11 Gbps	1,997.13 Gbps	372.93 Gbps	1,263.73 Gbps	
Aug	1,486.81 Gbps	1,440.46 Gbps	298.35 Gbps	764.94 Gbps	
Sep	2,333.20 Gbps	1,414.91 Gbps	575.01 Gbps	778.37 Gbps	
Oct	1,282.53 Gbps	1,741.49 Gbps	636.64 Gbps	627.40 Gbps	
Nov	1,354.52 Gbps	1,446.17 Gbps	591.92 Gbps	758.90 Gbps	
Dec	972.32 Gbps	1,454.99 Gbps	759.88 Gbps	777.18 Gbps	

Figure 9: DDoS Attack Coefficient: Max Bandwidth

Data: Cyber Threat Horizon

VIEW LIVE TABLE



TOP MAX BANDWIDTH

IN ONE MINUTE

APAC
2,333.20 Gbps (Sep)

EMEA
1,741.49 Gbps (Oct)

LATAM
759.88 Gbps (Dec)

NAMER
1,263.73 Gbps (Jul)

Comparing the minute-by-minute aggregate DDoS attack traffic to the aggregate DDoS traffic of an entire month further highlights the sheer volume and throughput this type of malicious traffic inflicts worldwide. In our previous report, we showed a simple calculation of bandwidth and throughput without factoring in the duration of DDoS attacks; in one 31-day window we observed 1 Pbps of bandwidth and 208 Gpps. However, by factoring in attack duration with bandwidth and throughput, the DAC shows an even starker picture of the massive amount of attack traffic traversing the internet.

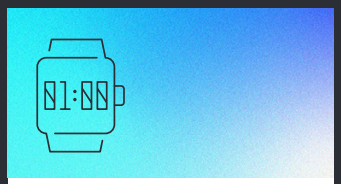
DDoS Attack Coefficient: Max Throughput

Month	APAC	EMEA	LATAM	NAMER	Regional Breakdown
Jul	474.23 Mpps	704.08 Mpps	74.97 Mpps	223.35 Mpps	
Aug	287.58 Mpps	544.21 Mpps	73.90 Mpps	200.91 Mpps	
Sep	1,337.13 Mpps	523.45 Mpps	165.22 Mpps	167.06 Mpps	
Oct	822.93 Mpps	732.84 Mpps	171.57 Mpps	180.48 Mpps	
Nov	522.15 Mpps	560.87 Mpps	176.37 Mpps	256.84 Mpps	
Dec	360.81 Mpps	540.30 Mpps	211.77 Mpps	315.35 Mpps	

Figure 10: DDoS Attack Coefficient: Max Throughput

Data: Cyber Threat Horizon

VIEW LIVE TABLE



TOP MAX THROUGHPUT

IN ONE MINUTE

APAC
1,337.13 Mpps (Sep)

EMEA
732.84 Mpps (Oct)

LATAM
211.77 Mpps (Dec)

NAMER
315.35 Mpps (Dec)

03

Regional DDoS Attacks

Regional statistics generally mirror the unprecedented nature of DDoS activity in 2020, with surging numbers of high-volume, short-duration attacks.

Attackers widened their target profile beyond usual-suspect industries as the massive shift to online work and play opened up promising new avenues of attack. And as the world leaned even more heavily on pandemic-era mainstays such online streaming, ecommerce, cloud, and online learning, attackers naturally followed. For instance, Internet Publishing and Broadcasting, a sector inhabited by both Netflix and Zoom, appeared in each region's top 10 list of most-attacked vertical industries.

KEY TAKEAWAYS

01

Attack frequency ballooned, with Latin America (LATAM) leading with a 50 percent growth rate. Indeed, LATAM showed disproportionate growth nearly across the board, likely reflecting significant political and ideologically motivated activity in the region.

02

We continued to see a fairly consistent growth in throughput as attackers pumped up the packets per second in an effort to overwhelm network resources and applications. North America was the sole outlier with a 67 percent decrease in throughput, which may be a result of more UDP-type attacks being launched compared with other types such as TCP-based attacks.

03

Attack duration dropped across every region as attackers launched short burst attacks that narrowed the time available for defenders to respond.

04

The use of complex multivector attacks continued to rise, with almost every region recording a new high-water mark in terms of vectors used in a single attack.

Global Map Showing Regional Attacks

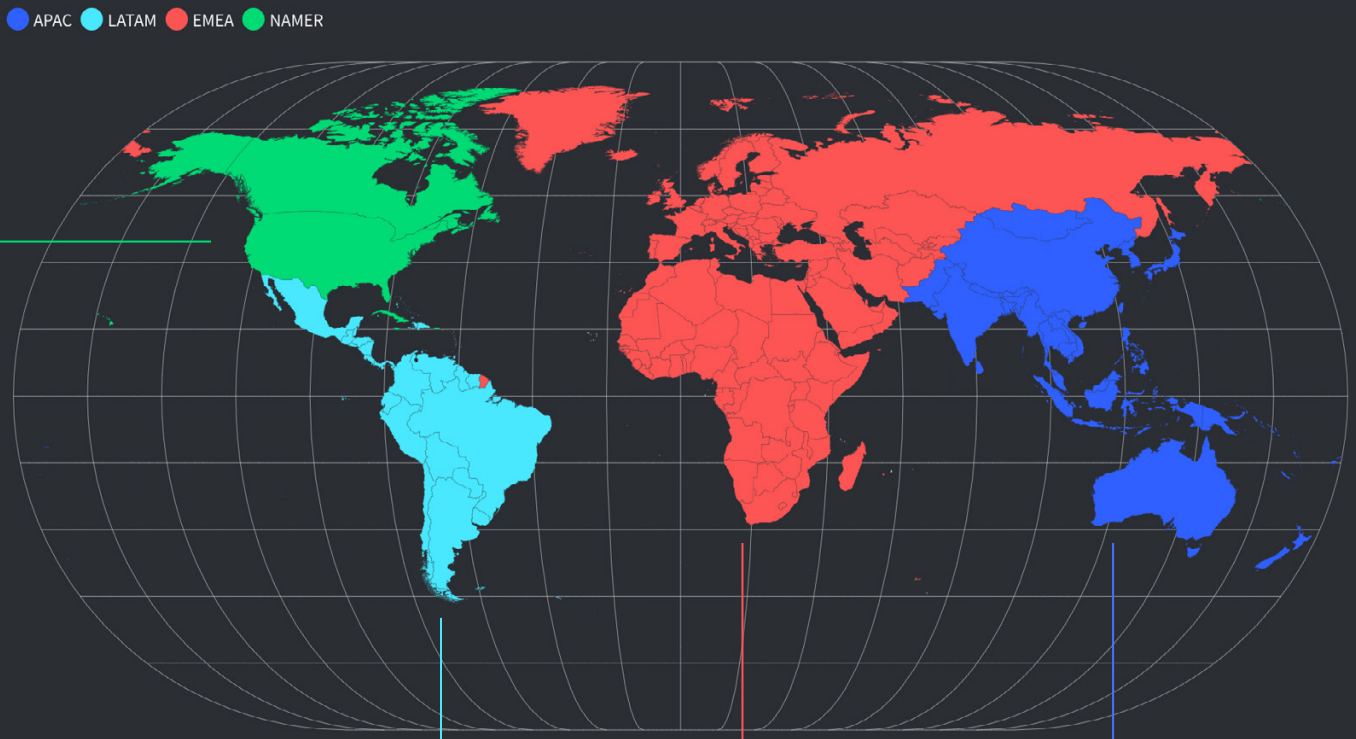


Figure 11: Global Map Showing Regional Attacks

Data: Cyber Threat Horizon

VIEW LIVE MAP

NAMER

Attack Frequency
▲ 29%

Max Attack Size
380 GBPS

Max Throughput
114 MPPS

Average Duration
▼ 21%

LATAM

Attack Frequency
▲ 50%

Max Attack Size
537 GBPS

Max Throughput
147 MPPS

Average Duration
▼ 40%

EMEA

Attack Frequency
▲ 33%

Max Attack Size
385 GBPS

Max Throughput
219 MPPS

Average Duration
▼ 14%

APAC

Attack Frequency
▼ 8%

Max Attack Size
349 GBPS

Max Throughput
581 MPPS

Average Duration
▼ 64%

Timeline of Super-Sized Multivector Attacks by Country 2017–2020

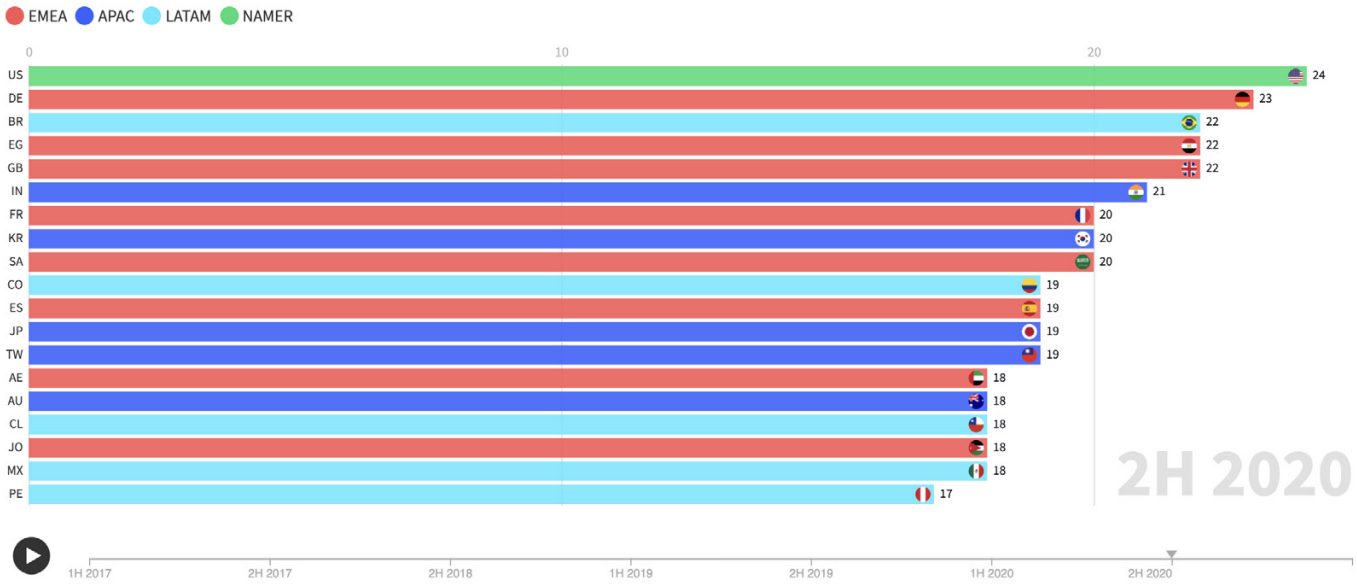


Figure 12: Timeline of Super-Sized Multivector Attacks by Country 2017–2020

Data: Cyber Threat Horizon

VIEW ANIMATION

Regional Growth of Multivector Attacks

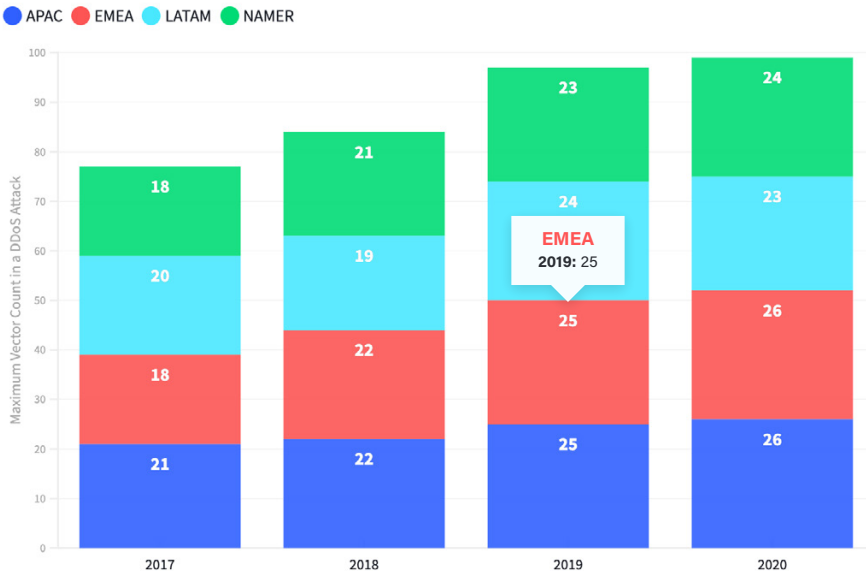
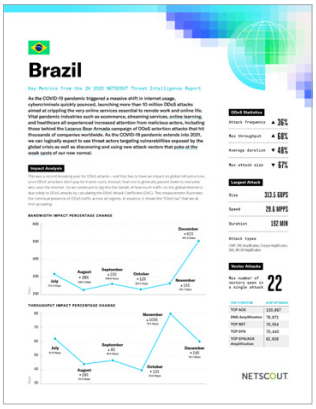


Figure 13: Regional Growth of Multivector Attacks

Data: Cyber Threat Horizon

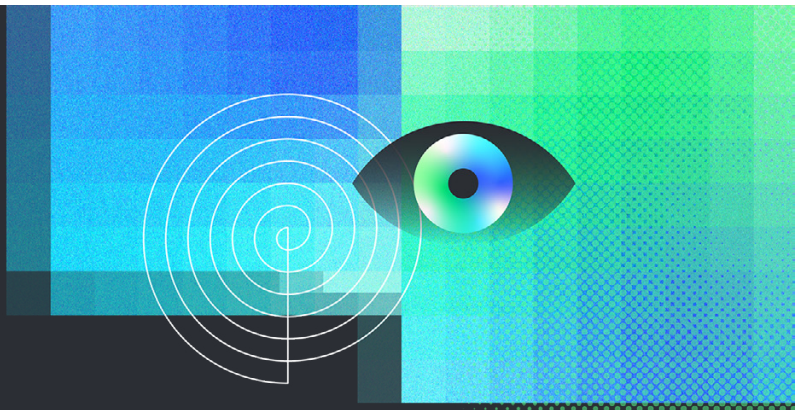
VIEW LIVE CHART



COUNTRY SNAPSHOTS

Read detailed DDoS attack stats for 19 countries across the global threat landscape.

LEARN MORE



04 IoT

A sizable portion of the global workforce likely will make some form of remote work permanent — and that's bad news when it comes to defending against inbound threats.

A review of ASERT honeypot data clearly illustrates the issue: The number of attempted Telnet and Secure Shell (SSH) brute-force logins in 2020 grew by 47 percent compared with 2019.

Although already prevalent in corporate locations, brute-force attacks pose a greater risk on home networks that lack enterprise-grade security controls, coupled with vulnerable IoT devices on the consumer network. Even worse, time is money when it comes to mitigating that risk. Our research has shown it takes 5 minutes or less for adversaries to scan and potentially compromise a new IoT device on the internet. Compare that with the time it takes to find and fix a breach: According to research conducted by IBM, it took 197 days to identify a breach, and 69 days to contain it. And each day costs more: Companies that managed to contain the breach in fewer than 30 days typically saved themselves more than US$1 million.

Why Are IoT Devices Such Juicy Targets?

There are a few factors at play. IoT devices are often deployed in a set-it-and-forget-it manner and don't get upgraded to fix vulnerabilities as they are discovered. They also typically use a set of credentials that are either hardcoded or are difficult for the end user to change. And lastly, manufacturers often neglect to integrate security into IoT devices, leaving the end user to bolt it on outside of the IoT product. This explains the continued popularity of the top five exploits, which have remained consistent year over year.

TIME IS MONEY

5 MIN

To compromise a new IoT device on the internet

266 DAYS

To identify and contain a breach

$3.86M

Average total cost of a data breach

Source: IBM

KEY TAKEAWAYS

01

In 2020, ASERT honeypots saw a 47 percent increase in brute-force activity over 2019.

02

A new set of credentials appeared in October that outlined the emergence of a new botnet.

03

Mirai and its variants continued to drive botnet activity, and 2020 was seen as the year in which Windows-based malware crossed into the Linux realm.

Mirai: Long Live the King

ReversingLabs saw the number of malware samples effectively double in 2019. In 2020, that number grew by 150,000, a 7 percent increase in an already overwhelming number of Mirai samples circulating in the wild.

Malware Sample Timeline

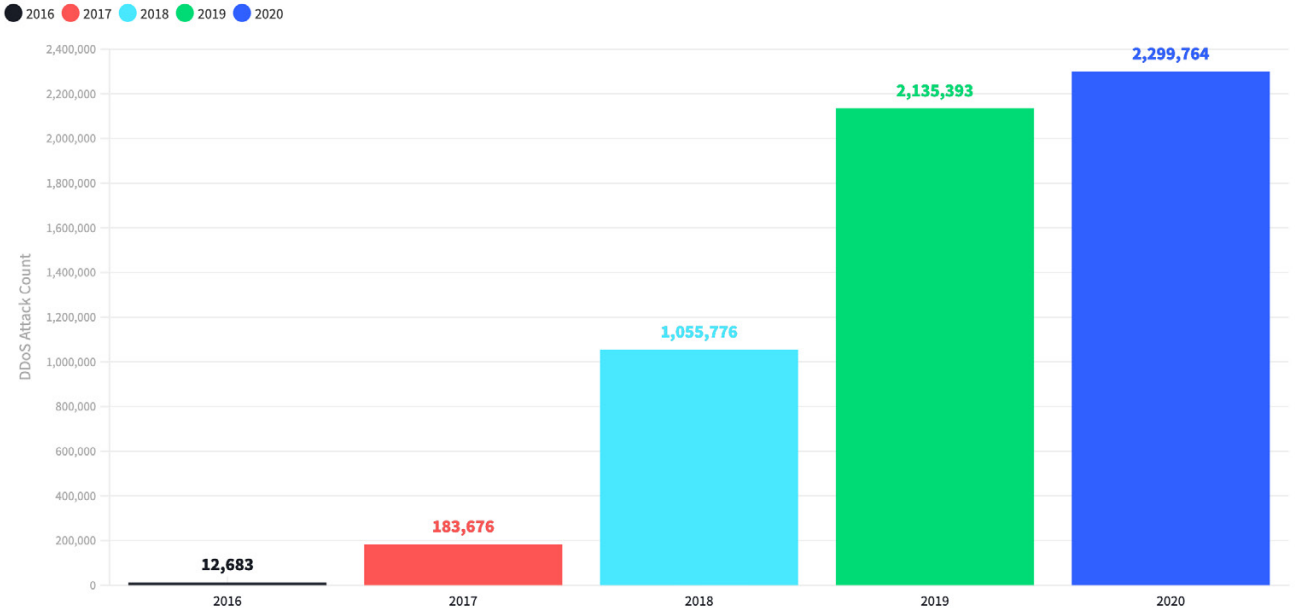


Figure 14: Malware Sample Timeline

Data: ReversingLabs

VIEW LIVE CHART

Top Five Mirai Variants

The top five Mirai variants in 2020 didn't change much from the first six months to the second half of the year. Mirai moved up into the top five, and Kyton fell out. These markers are a good way to identify variants being used.

MIRAI VARIANTS	UNIQUE SOURCES
CORONA	10,286
RETARD	4,335
UNSTABLE	3,629
MIRAI	3,271
ARES	2,911

Figure 15: Mirai Variants 2H 2020

Mirai Architectures Used in 2020

We also observed a variety of architectures used by Mirai. Looking at a representative sampling of the binaries provided by ReversingLabs, we see this distribution of architectures for 2020.

Figure 16: Mirai Architectures Used in 2020

Data: ReversingLabs

VIEW LIVE CHART

Username/Password Combinations

Out of more than 75 million brute-force attempts observed by our honeypot network in 2020, the top five combinations continue to be the original list hard coded in Mirai since 2016.

Our previous reports listed only unique sources in the brute-force attempts. We now include every attempt, to illustrate the persistent nature of automated brute-forcing bots. Although credential combinations used by Mirai are still the most frequently seen, the picture looks a bit different when considering the unique source of the brute-force login attempt. The hypothesis is that while botmasters are using more diverse username/password lists and new bots continue to enter the space, Mirai remains atop the charts due to its constant bombardment on network-connected devices.

In the second half of 2020, ASERT started tracking the impact inbound brute forcing had on our customers. In just a few months, we observed more than 75 million Telnet attempts just from indicators we collect from our honeypots. Leveraging data from our Cyber Threat Alliance (CTA) partnership, we observed more 550 million Telnet, SSH, Server Message Block (SMB), and RDP brute-force attempts in 2020.

Although the majority of these inbound attempts are against targets in the United States, the following map shows the top 10 countries targeted by Telnet brute-force attempts. Looking at the other side of the connection, we can determine where the majority of these brute-force attempts originate based on the attacking IP address.

USERNAME/PASSWORD	TOTAL ATTEMPTS
root/xc3511	5,161,000
admin/	3,273,127
root/catch99	2,146,214
default/default	1,578,778
default/	1,409,367

Figure 17: Top Five Username/Password Combinations by Total Attempts

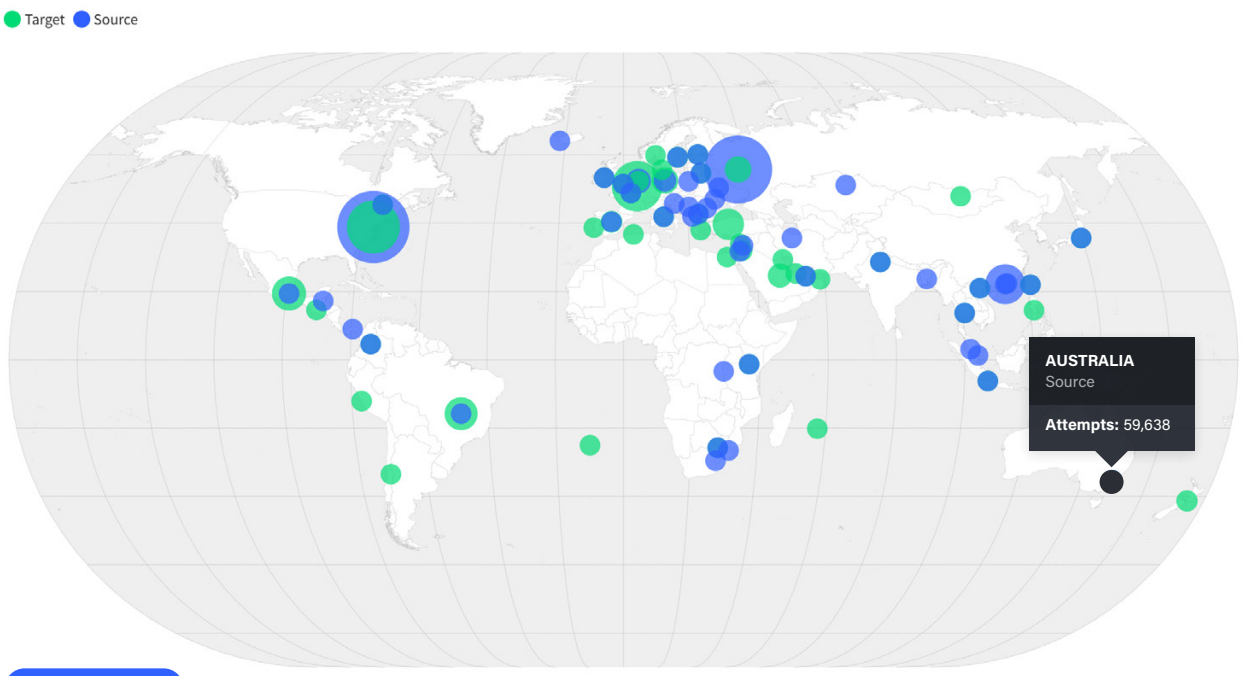
USERNAME/PASSWORD	TOTAL ATTEMPTS
guest/12345	110,467
root/xc3511	98,933
admin/admin	90,592
root/vizxv	76,392
root/root	62,518

Figure 18: Top Five Username/Password Combinations by Unique Source

550M

Telnet, SSH, Server Message Block (SMB), and RDP brute-force attempts in 2020

Top 50 Telnet Brute-Force Targets and Sources



VIEW LIVE MAP

Figure 19: Top 50 Telnet Brute-Force Targets and Sources

Data: Cyber Threat Horizon

The Birth of a New Botnet

Amidst the onslaught of brute forcing, ASERT observed a new set of credentials plow their way into the top five in October 2020. The username/password combinations were previously low volume, and the spike in usage likely indicates a new botnet or concentrated effort to compromise a specific set of devices. The continued use of these credentials following the initial wave in October indicates that it will likely stick around and eventually find its way into other botnets and automated brute-forcing tools.

Top five originating countries responsible for the explosion in Hikvision-related brute-force attempts

01 VIETNAM
02 RUSSIA
03 TAIWAN
04 CHINA
05 BRAZIL

Emergence of a New Botnet

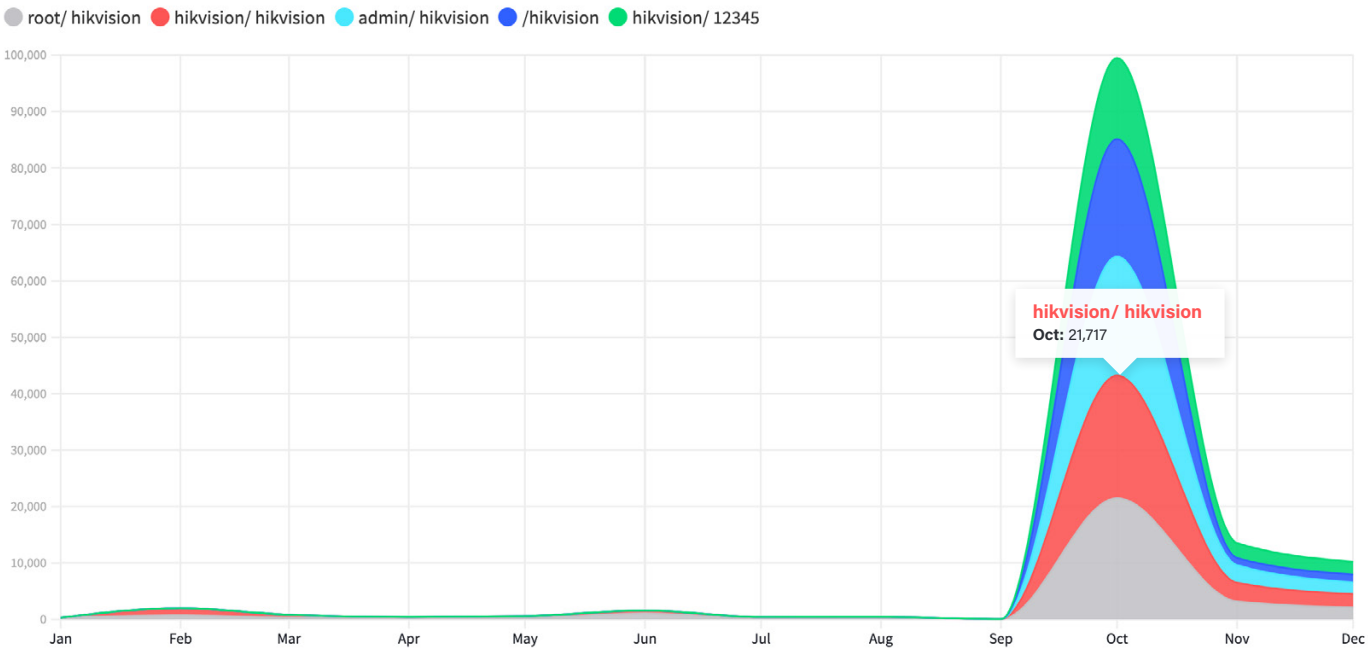


Figure 20: Emergence of a New Botnet

Data: Cyber Threat Horizon

VIEW LIVE CHART

05

Worldwide Infrastructure Security Report (WISR)

Add network and internet connectivity to the list of essential workers for 2020 as the COVID-19 pandemic reinforced our absolute need for online access. That vital importance naturally attracted the attention of malicious actors, who always want the things most important to network operators and enterprises.

Indeed, the changes wrought by the pandemic emerged as an important catalyst affecting DDoS attack activity in 2020. This translates to a significant uptick in DDoS attacks overall, as well as an increase in ransomware and DDoS extortion attacks, such as those launched by the LBA threat actors. And as attackers broadened their target base to exploit vulnerabilities exposed by a massive shift to remote work and play, we saw an increased demand for managed DDoS protection services from companies suddenly in need of protection.

NETSCOUT's 16th annual Worldwide Infrastructure Security Report (WISR) delivers insights from a global survey of network, security, and IT decision makers across enterprise and service provider organizations. It focuses on the operational challenges they face daily from network-based threats and the strategies adopted to address and mitigate them.

Key Findings

01

DDoS attackers exploited pandemic-driven vulnerabilities

Nearly half of survey respondents reported an increase in DDoS attacks during the pandemic, many of which targeted vulnerabilities exposed by a significant shift to online services. 83 percent of enterprises that suffered a DDoS attack reported that overloaded firewalls and/or VPN devices contributed to an outage, a 21 percent jump year over year. These devices need to be protected, because they perform a vital role for organizations deploying pandemic-related work/learn-from-home scenarios. Defenders also reported increased attack complexity, with 57 percent of service providers reporting multivector attacks in 2020.

02

Global surge of DDoS extortion attacks

For both service providers and enterprises, DDoS extortion attacks and ransomware attacks were high on the list of threats experienced and future concerns. Survey data reflected the global impact of the LBA DDoS extortion campaign, with the number of DDoS extortion attacks reported by enterprise WISR respondents growing by 125 percent. Meanwhile, about a quarter of enterprises reported a ransomware attack in 2020, up from 15 percent in 2019.

71% Of service providers say DDoS attacks were top threat in 2020

75% Of enterprises reported DDoS attacks on key pandemic infrastructure such as routers, firewalls, and VPN concentrators

03

Attacks sourced from within cloud services and mobile devices

Although inbound attacks on publicly exposed service infrastructure remains a top concern for service providers, 31 percent of respondents also noted the increase in outbound/cross-bound DDoS attacks from on-net customers and devices, reported by 31 percent of service providers. Cloud services also are being used to launch attacks. Nearly 40 percent of service providers saw DDoS attacks moving both to and from public cloud services, while nearly three quarters of service providers saw botnet traffic originating from both outside and inside their networks. Moreover, approximately one quarter of service providers saw mobile devices being used to launch attacks targeting infrastructure, services, or customers.

And while that's bad, nearly half couldn't even tell whether mobile devices were being used as sources, indicating a lack of visibility. With more than half of all internet traffic now originating on mobile devices, this gap is a serious concern.

04

Demand surges for managed DDoS protection services

Increases in the size, frequency, and complexity of DDoS attacks resulted in a significant increase in demand for managed DDoS mitigation services. Managed security service providers (MSSPs) saw an increase of as much as 69 percent in enterprise demand for managed DDoS protection services. Moreover, that demand came from a much broader range of enterprise customers. Notably, respondents reported increased interest from both the education and healthcare sectors—two pandemic lifelines that experienced increased interest from threat actors.

Service Provider

Service Provider Concerns

Service providers managed enormous spikes in legitimate network traffic such as streaming video, video conference calls, and gaming while simultaneously defending a commensurate increase in DDoS attacks targeting critical network infrastructure and services. And although DDoS attacks remain the top threat service providers are concerned about, respondents also expressed growing concern over the increasing complexity of those attacks. Thanks to IoT botnets, reflection/amplification techniques, and DDoS-for-hire services, attacks are more distributed, complex, and powerful than ever before. Indeed, 57 percent of respondents reported multivector attacks in 2020. In a trend that continues from the previous year, 31 percent reported outbound/ cross-bound DDoS attacks from on-net customers and devices.

41%

Of service providers were concerned with bandwidth saturation increases from pandemic-staple over-the-top (OTT) services such as streaming video, conference calls, and gaming

Service Provider Threats Experienced and Concerns

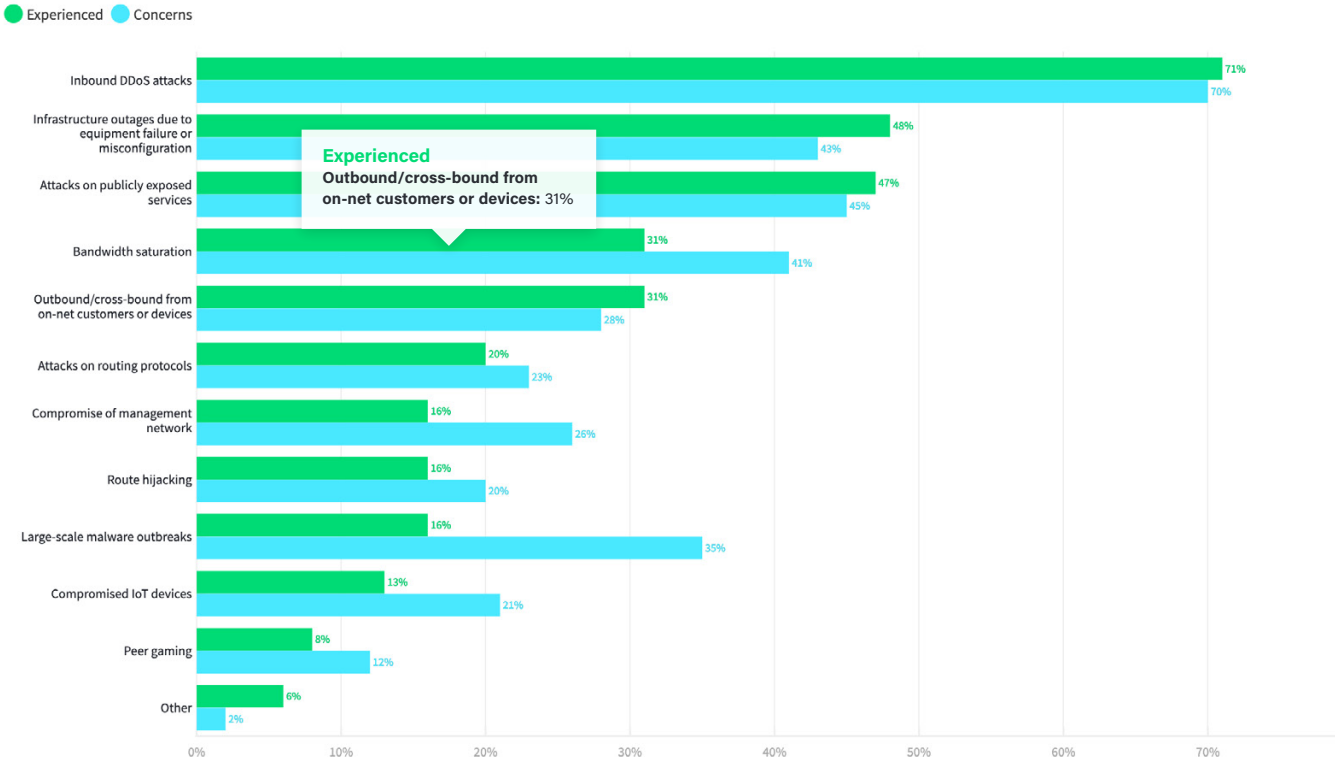


Figure 21: Service Provider Threats Experienced and Concerns

Data: Worldwide Infrastructure Security Report

VIEW LIVE CHART

Smart Marketing for Cybercriminals

In today's booming cybercrime economy, DDoS-for-hire services have never been easier or cheaper to use. Anybody with an internet connection can hire a software-as-a-service (SaaS)-based service for a little as US$7 for an attack. And as the WISR research shows, these savvy businesspeople know the value of marketing. The top attack motivation was cybercriminals launching attacks to show off their capabilities, while criminal extortion attempts took the third spot on the list. In a sense, many DDoS attacks are advertisements for illegal DDoS-for-hire services. Meanwhile, online gaming-related attacks continued to show a strong presence, likely mirroring an overall surge in online gaming during the pandemic.

Attack Motivation

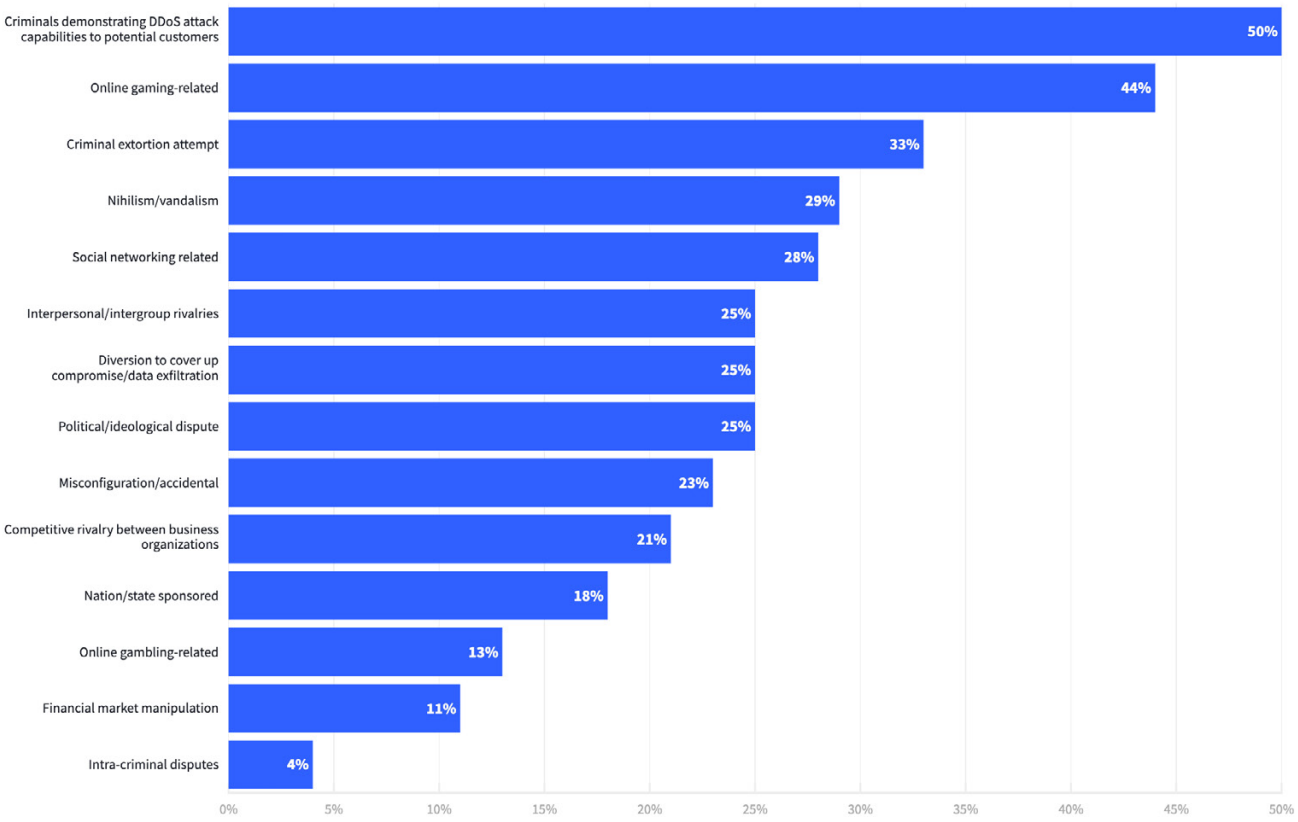


Figure 22: Attack Motivation

Data: Worldwide Infrastructure Security Report

VIEW LIVE CHART

Pandemic Attacks Broaden Demand for Managed Security Services

By forcing a global switch to remote work and heavy reliance on online services, the pandemic increased the risk profile for a wider variety of vertical industries. At the same time, threat actors were able to easily and cheaply access increasingly sophisticated attack tools via for-hire services. The result? More attacks aimed at a wider target range—and broad demand for managed security services. MSSPs saw a significant increase in enterprise demand for managed DDoS protection services from companies of all sizes, and from vertical industries that up until now didn't consider DDoS a significant threat.

Increase in Demand for DDoS Mitigation Services

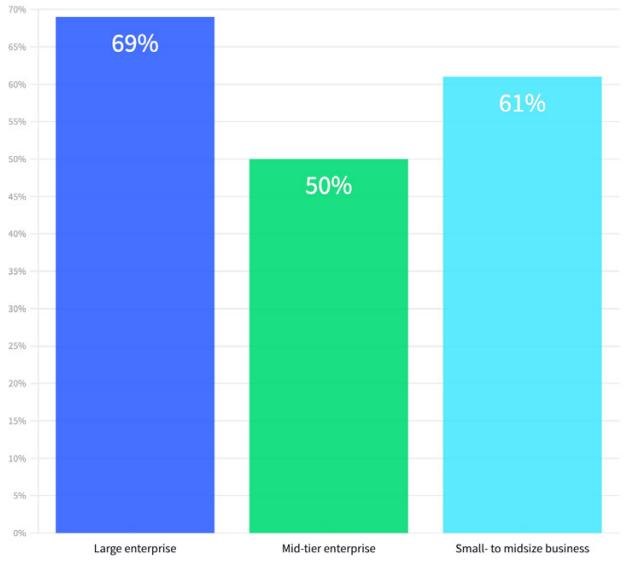


Figure 23: Increase in Demand for DDoS Mitigation Services

Data: Worldwide Infrastructure Security Report

VIEW LIVE CHART

In particular, respondents noted a marked increase in demand from the education and healthcare sectors. These sectors, both lynchpins for vital pandemic-driven online services, sustained increases in DDoS attacks and DDoS extortion attempts. More than half of MSSP respondents reported interest from government, cloud/hosting providers, and financial services customers, while 40 percent of MSSPs have seen interest from education, ecommerce, and ISPs. Meanwhile, more than 20 percent reported requests from healthcare, media and entertainment, and retail.

MSSPs also reported some changes in the types of DDoS protection they offer customers. One notable difference is that 11 percent of MSSPs reported offering third-party DDoS mitigation services to their customers, which could indicate that the MSSPs themselves can't keep up with their customer demands for protection. Moreover, the number of MSSPs now offering multiple tiers of DDoS protection services has more than tripled year over year. Considered in conjunction with the increase of third-party offerings, it looks as if MSSPs are adding more-advanced, value-added custom services.

TOP FIVE VERTICAL INDUSTRY TARGETS

01 Financial Services

02 Government

03 Education

04 Hosting/Cloud

05 Ecommerce

Types of DDoS Protection Services

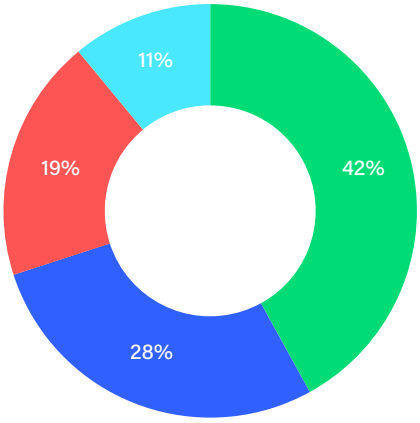


Figure 24: Types of DDoS Protection Services

Data: Worldwide Infrastructure Security Report

VIEW LIVE CHART

Threat Detection Tools Used, and Their Effectiveness

When it came to threat detection, NetFlow-based analyzers remained a perennial favorite, with inline DDoS solutions moving up to third place while next-generation firewalls took second place.

Unsurprisingly, those top three tools were also rated the most effective, although not in the same order: Inline DDoS solutions were more effective than next-generation firewalls, although the latter was used slightly more frequently. Because using a wide array of deployed threat detection tools creates a massive number of alerts, it's no surprise to see the increased use and importance of security information and event management (SIEM) platforms.

Threat Detection Tools Used Versus Their Effectiveness

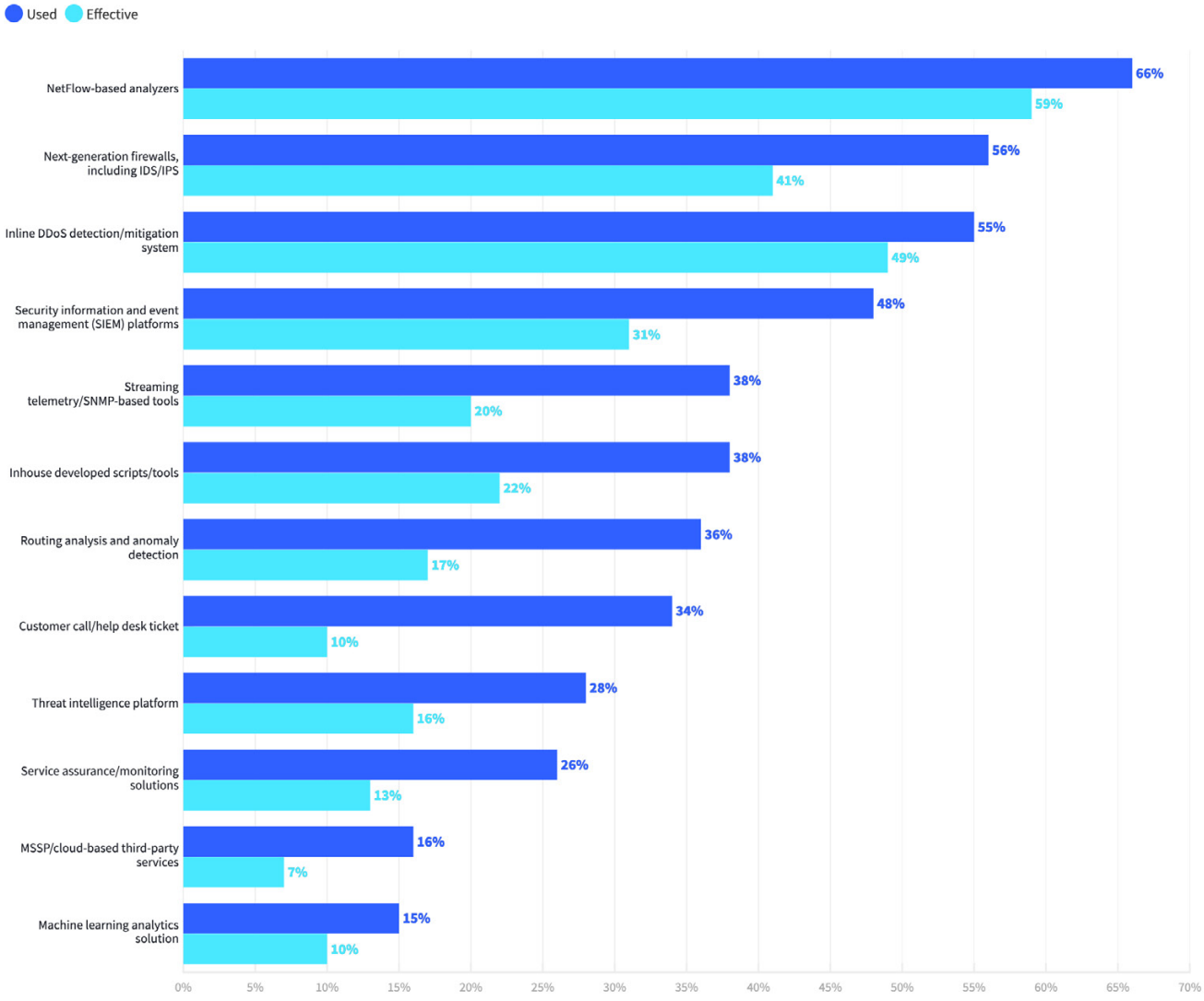


Figure 25: Threat Detection Tools Used Versus Their Effectiveness

Data: Worldwide Infrastructure Security Report

VIEW LIVE CHART

Enterprise

Enterprise Concerns

Enterprises found themselves defending a more distributed and vulnerable environment in 2020 as the shift to remote work and online collaboration services introduced vulnerabilities that attackers quickly exploited. This new reality is reflected in some interesting shifts in the enterprise threats and concerns expressed for 2020. The top four threats experienced by enterprises all had clear ties to the pandemic, with DDoS attacks topping the list. Enterprises continue to rate ransomware as a top threat, and 2020 saw DDoS extortion attacks leapfrog from 10th to fourth place in the list of experienced threats, with the number of respondents reporting such attacks growing by 125 percent.

Enterprises also don't expect a drop in these threats; respondents rated both DDoS and ransomware attacks as top concerns for 2021. However, DDoS was the only threat in which experience nearly matched concern. Note that for ransomware, half are concerned but only a quarter experienced it. Meanwhile, accidental data loss—the biggest threat faced by enterprise network operators in 2019—dropped to seventh place in 2020.

▲ 125%

Increase in DDoS extortion attacks in 2020

Enterprise Threats Experienced and Concerns

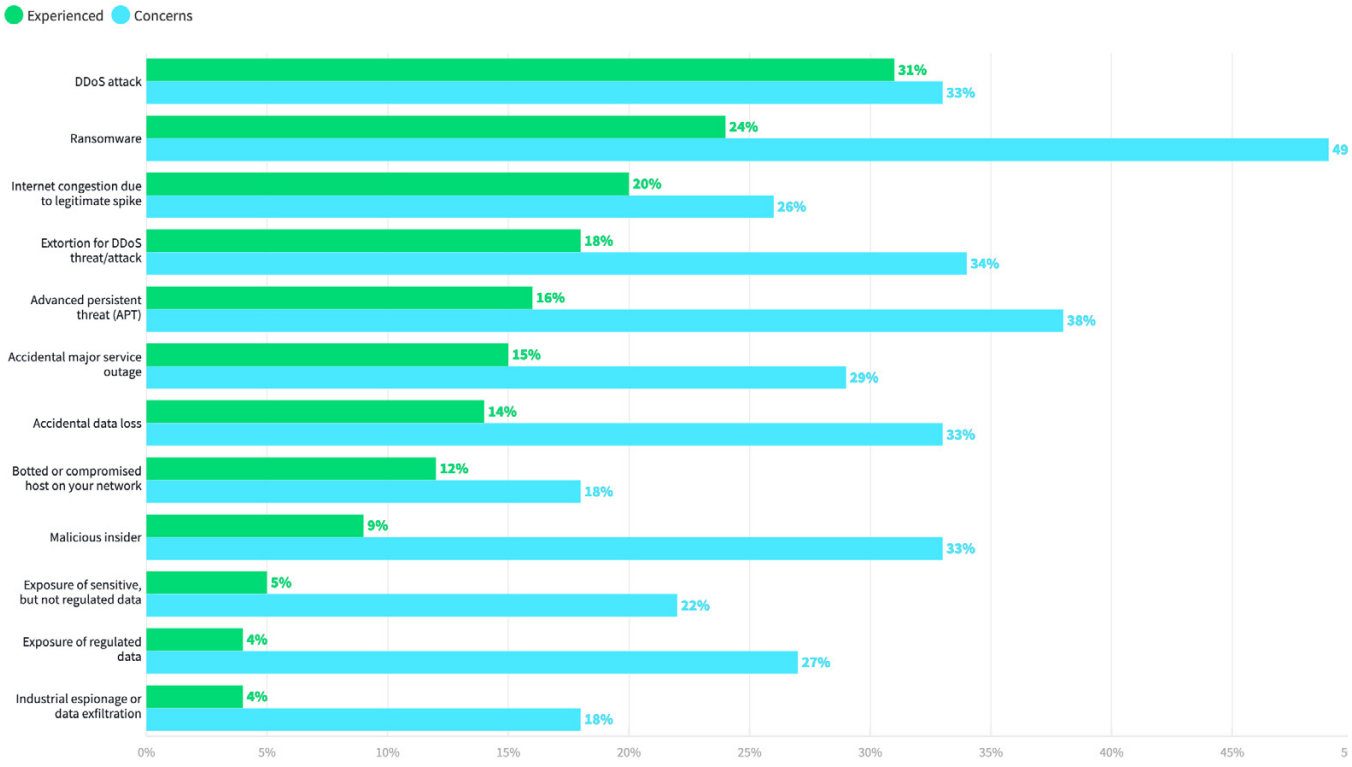


Figure 26: Enterprise Threats Experienced and Concerns

Data: Worldwide Infrastructure Security Report

VIEW LIVE CHART

Pandemic-Related Concerns

With organizations abruptly executing work/learn-from-home scenarios, it's not surprising to see the top enterprise concerns were inbound DDoS attacks from external networks, and infrastructure outages. This result likely reflects respondents' new dependence on devices such as firewalls and VPN concentrators as critical elements of network infrastructure. However, these devices cannot handle massive amounts of inbound communication, and a relatively small DDoS attack can easily bring them down.

Pandemic-Related Concerns

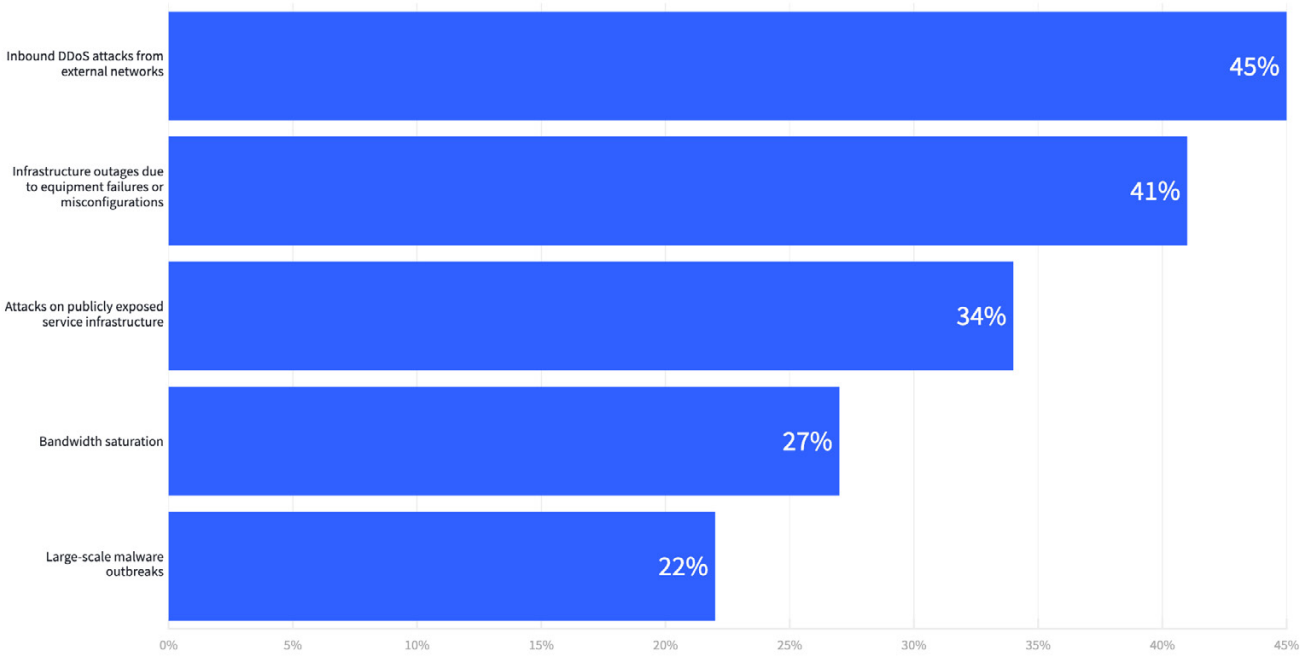


Figure 27: Pandemic-Related Concerns

Data: Worldwide Infrastructure Security Report

VIEW LIVE CHART

Overall DDoS Attack Trends

Cybercriminals are unerring in their ability to hit you where it hurts, a fact that WISR respondents made abundantly clear. More than two-thirds of enterprises reported DDoS attacks that targeted customer-facing services and applications, while 75 percent saw attacks targeting their infrastructure. In both cases, these attacks directly affect the organization's ability to service customers, thus impacting revenue and profitability. More than two thirds of enterprises reported more complex DDoS attacks in 2020, with a significant jump in multivector attacks—58 percent in 2020 compared with 38 percent in 2019.

Meanwhile, the number of respondents reporting a DDoS attack that exceeded their internet bandwidth rose slightly from 43 percent to 50 percent, reflecting the increase in DDoS attack frequency and the expanding target base.

IoT concerns

With botmasters compromising and subsuming IoT devices at an astonishing rate, it is no surprise that infected/compromised IoT devices were a top IoT concern for half of the surveyed enterprises. Software patching and maintenance stole the second spot this year, increasing from 39 to 47 percent. Meanwhile, detection/identification of IoT devices fell to the third spot for 42 percent of enterprise respondents.

Firewalls still don't work for DDoS

Although they are an effective perimeter security tool against certain kinds of threats, firewalls were not designed for DDoS attacks. And yet, companies continue to rely on them, with 62 percent of enterprises reporting they use next-gen firewalls to detect threats against their networks. Entirely unsurprisingly, respondents also continue to note a high failure rate when it comes to DDoS defense.

ENTERPRISE ATTACK CATEGORIES BY THE NUMBERS

59%
Volumetric attacks

25%
State-exhaustion

16%
Application layer

Enterprise Reporting Firewall Failures in DDoS Attacks

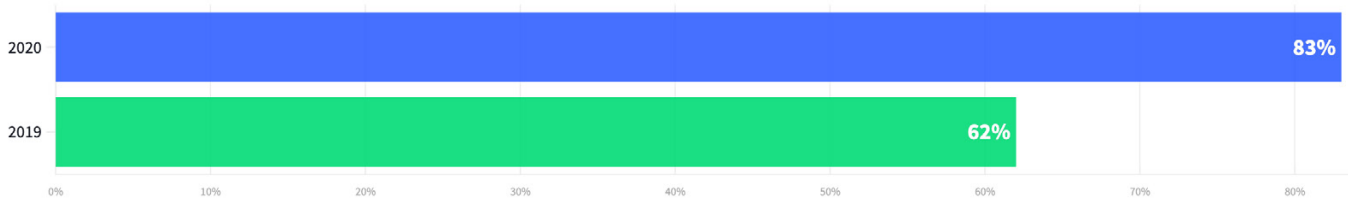
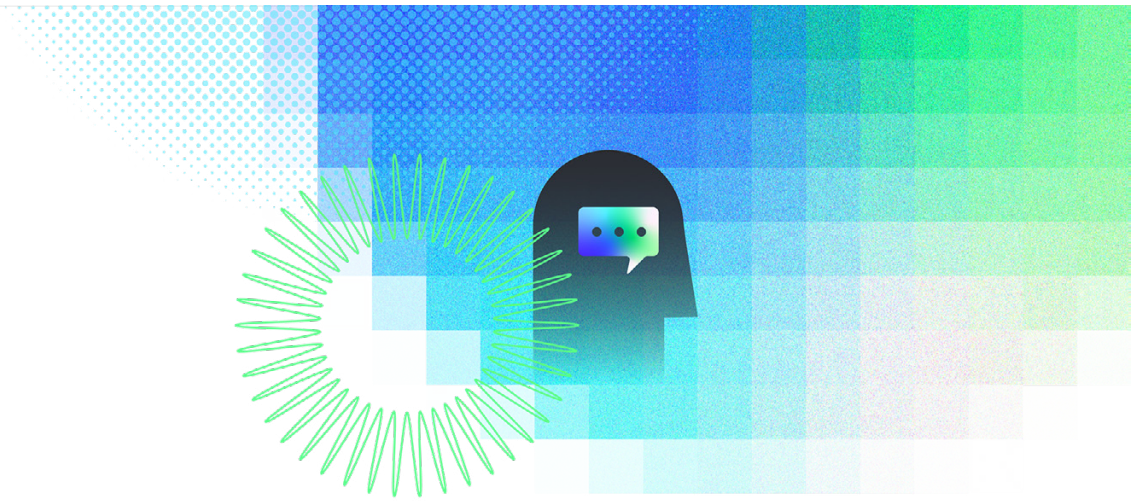


Figure 28: Enterprises Reporting Firewall Failures in DDoS Attacks

Data: Worldwide Infrastructure Security Report

VIEW LIVE CHART



06 Conclusion

As the COVID-19 pandemic extends into 2021, we can logically expect to see threat actors target vulnerabilities exposed by the global crisis, as well as discover and use new attack vectors that poke at the weak spots of our new normal. After all, cybercrime is a multi-billion-dollar business. These adversaries are smart and motivated, and we can count on them to discover and weaponize new vectors, or throw new techniques onto existing ones.

The growing global complexity of it all means that there will always be challenges. It is imperative that defenders and security professionals remain vigilant to protect the critical infrastructure that connects and enables the modern world. The ASERT team continues to monitor the threat landscape and report on new discoveries, from malware under development to the increasingly sophisticated tools and techniques used. We hope you find the information useful in protecting your business over the coming year.

VIEW WEBSITE MORE RESOURCES

ABOUT NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) helps assure digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility and insights customers need to accelerate and secure their digital transformation. Our approach transforms the way organizations plan, deliver, integrate, test, and deploy services and applications. Our nGenius™ service assurance solutions provide real-time, contextual analysis of service, network, and application performance. Arbor Smart DDoS Protection by NETSCOUT products help protect against attacks that threaten availability and advanced threats that infiltrate networks to steal critical business assets. To learn more about improving service, network, and application performance in physical or virtual data centers, or in the cloud, and how NETSCOUT's performance and security solutions powered by service intelligence can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT on Twitter, Facebook, or LinkedIn.

SECR_001_EN-2101

NETSCOUT