NETSCOUT

Issue 5: Findings from 1H 2020

# NETSCOUT THREAT INTELLIGENCE REPORT

## CYBERCRIME: EXPLOITING A PANDEMIC

EDITOR'S NOTE

## The COVID-19 pandemic drove a mass movement to virtualized work and play, giving adversaries a much larger playground of opportunity.

Their response to this opportunity reminds me of a Daft Punk song titled, "Harder, Better, Faster, Stronger". The first half of 2020 witnessed a radical change in DDoS attack methodology to shorter, faster, harder-hitting complex multi-vector attacks. A shift that we anticipate will continue. Attackers increased attacks against online platforms and services crucial in an increasingly digital world, such as ecommerce, educational platforms, financial services, and healthcare services. Though it shouldn't surprise anyone, attackers come in all levels of sophistication and age, as evidenced by the recent arrest of a 16-year old student who disrupted a school's online learning platform, blocking entry to approximately 170,000 students.[1]

No matter the target, adversary, or tactic used, it remains imperative that defenders and security professionals remain vigilant in these challenging days to protect the critical infrastructure that connects and enables the modern world.

**Richard Hummel**
Threat Intelligence Lead, NETSCOUT

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 cyber threat 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.

CONTENTS



CONTRIBUTORS

**Richard Hummel**
**Carol Hildebrand**
**Hardik Modi**
**Roland Dobbins**
**Steinthor Bjarnason**
**Jon Belanger**
**Peter Arzamendi**
**ReversingLabs (Partner)**

# The COVID-19 pandemic created a seismic shift in how we work and live and added rocket fuel to the growth in DDoS attacks.

During the shutdown, the world was hit by the single largest number of monthly attacks we've ever seen—929,000 DDoS attacks in May alone. As seen by our Active Threat Level Analysis System (ATLAS®), NETSCOUT Threat Intelligence observed 4.83 million DDoS attacks in the first half of 2020, up 15 percent from 2019. Even more telling, DDoS attack frequency jumped 25 percent during the pandemic lockdown months of March through June.

Attackers targeted COVID-era lifelines such as ecommerce, healthcare, and educational services with complex, high-throughput attacks designed to quickly overwhelm and take down targeted entities with short, burst attacks. Unsurprisingly, as schools closed and online usage increased, we also saw a surge in attacks on broadband networks, which translates largely to online gaming.

**The impact of this activity extends beyond the visible risks to critical services and cost of attack mitigation, however. DDoS attacks consume significant amounts of bandwidth and throughput—traffic that we all pay for.**

## KEY FINDINGS

### Pandemic Profiteers

Cybercriminals pounced on pandemic-driven vulnerabilities, launching an unprecedented number of shorter, faster, more complex attacks. ASERT saw more than 929,000 DDoS attacks in May, the single largest number of attacks we've ever seen over any 31-day period. Moreover, attack frequency jumped 25 percent during key pandemic lockdown months.

**4.83 MILLION**

DDoS attacks in the first half of 2020

### The Hidden Impact of DDoS Traffic

Of all the unprecedented DDoS numbers we saw, the sheer magnitude of bandwidth and throughput consumed by DDoS attacks took the prize. To measure the impact of that activity, we created the DDoS Attack Coefficient (DAC), which represents the total sum of DDoS traffic traversing any given region or country in one minute. Why does this matter? DDoS attackers don't pay for it—we do. The cost of that activity trickles down to every internet-connected entity, enterprises and individuals alike.

**▲ 15%**

Growth in DDoS attack frequency in 1H 2020

**▲ 25%**

Growth in DDoS attack frequency during pandemic lockdown

### Complex Multivector Attacks on the Rise

Complex 15-plus vector attacks have spiked 126 percent year over year and 2,851 percent since 2017. Meanwhile, the average duration of attacks fell 51 percent from the first half of 2019. This adds up to a giant headache for defenders, giving them less time to react to more difficult mitigation scenarios. At the same time, we saw a 43 percent decrease in single-vector DDoS attacks in 1H 2020.

**▲ 2,851%**

Growth in 15+ vector attacks since 2017

# DDoS Global Attack Trends

**Attack Size**

**1.12 TBPS** Largest attack in 1H 2020

**▲ 77%** Growth in max attack size in 1H 2020 from 1H 2019

**Attack Duration**

**▼ 51%** Decrease in attack duration in 1H 2020 from 1H 2019

**92%** Of attacks were less than an hour

**The COVID-19 pandemic is a worldwide health crisis—but to cybercriminals, it's a sterling business opportunity. And they have taken full advantage, unleashing an enormous number of shorter, faster, more complex attacks designed to increase their return on investment (ROI).**

We saw 4.83 million attacks in the first half of 2020, up 15 percent from 2019. But during the pandemic lockdown period from March through June 2020, DDoS attack frequency jumped 25 percent. Indeed, in May, we observed more than 929,000 DDoS attacks, the single largest number of attacks we've seen over any 31-day period to date.

Meanwhile, average attack duration plummeted more than 50 percent. Why? It's all about the money. Shorter attacks consume fewer resources for the bad guys and, even better (from their point of view), narrow the response window for defenders.

Attacks were also more complex, as super-sized 15-plus vector attacks grew 2,851 percent from 2017, when such attacks were considered outliers. This adds up to some bad math for defenders: Shorter duration + increased complexity = less time to respond to increasingly difficult-to-mitigate attacks. Such scenarios only highlight the vital role of advanced and automated DDoS technology.

# Global Impact of DDoS Traffic

**DDoS traffic: A cost of doing business online**

It's one thing to say that 4.8 million attacks hit the world in the first six months of 2020, but what impact does it have on global infrastructure? After all, both service providers and enterprises need to plan for this. Think of it as a cost of doing business in the digital economy.

While the impact of volumetric DDoS attacks is usually described in terms of attack traffic bandwidth, throughput, or the number of packets per second (pps) is often of equal or greater importance. Bandwidth-oriented attacks can flood network links and crowd out legitimate internet traffic. Throughput-based attacks, on the other hand, impede the ability of network infrastructure devices such as routers, switches, and load balancers, to forward legitimate network traffic, as well as degrade the ability of servers to process and respond to user requests.

That's why, while we did observe another terabit-class attack[2] during this period, it's not the most significant metric of the past six months. That honor goes to the sheer magnitude of bandwidth and throughput consumed by DDoS attacks overall.[3]

To better understand the true impact of DDoS attack traffic, we began by calculating the incremental bits per second (bps) and pps of observed DDoS attacks in order to create a monthly baseline of DDoS attack bandwidth and throughput.*

Case in point: The impact of surging attacks during the height of the pandemic lockdown. For the critical period between March 11 and April 11, 2020, we observed a whopping 1.01 petabits per second (Pbps) and 208 giga packets per second (Gpps) of aggregate DDoS attack traffic—a 14 percent increase in attack size and a staggering 31 percent increase in attack throughput relative to the average observed over the previous 4 months.

**Between March 11 and April 11, 2020 DDoS attack traffic surged.**

Attack Size*

▲ 14%

Attack Throughput*

▲ 31%

Aggregate DDoS Attack Traffic

1.01 PBPS

208 GPPS

*The data in this report reflects a rate underlying the DAC. It is our intention to develop a coefficient as our methodology progresses.

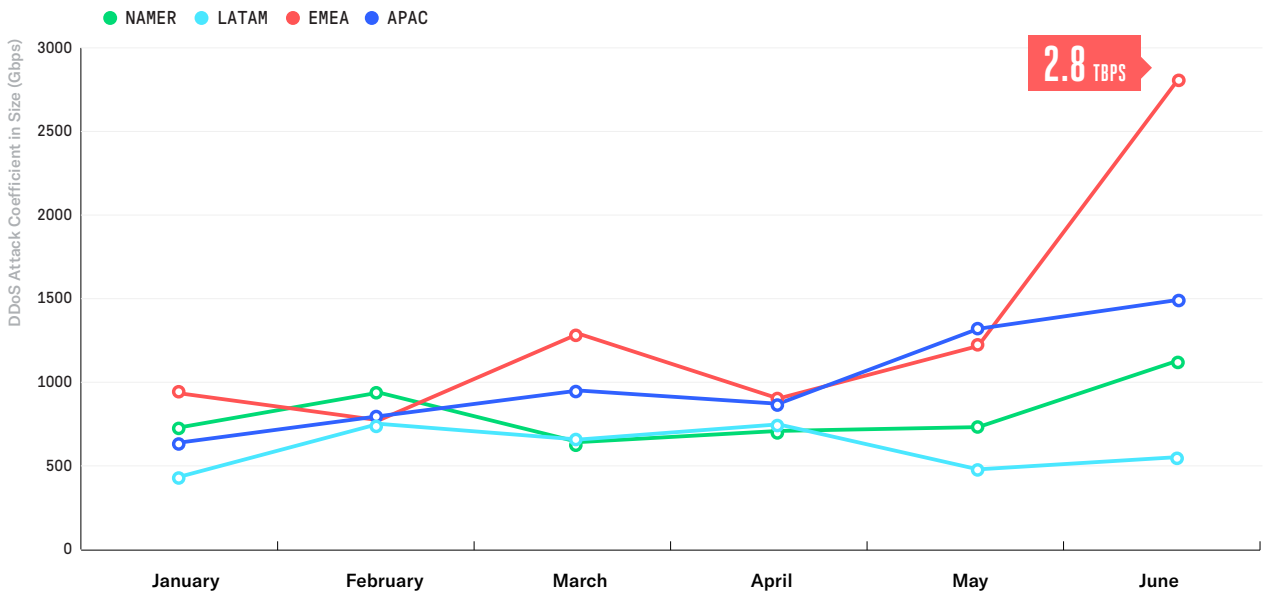



*Figure 1: Six Months of Bandwidth DAC*

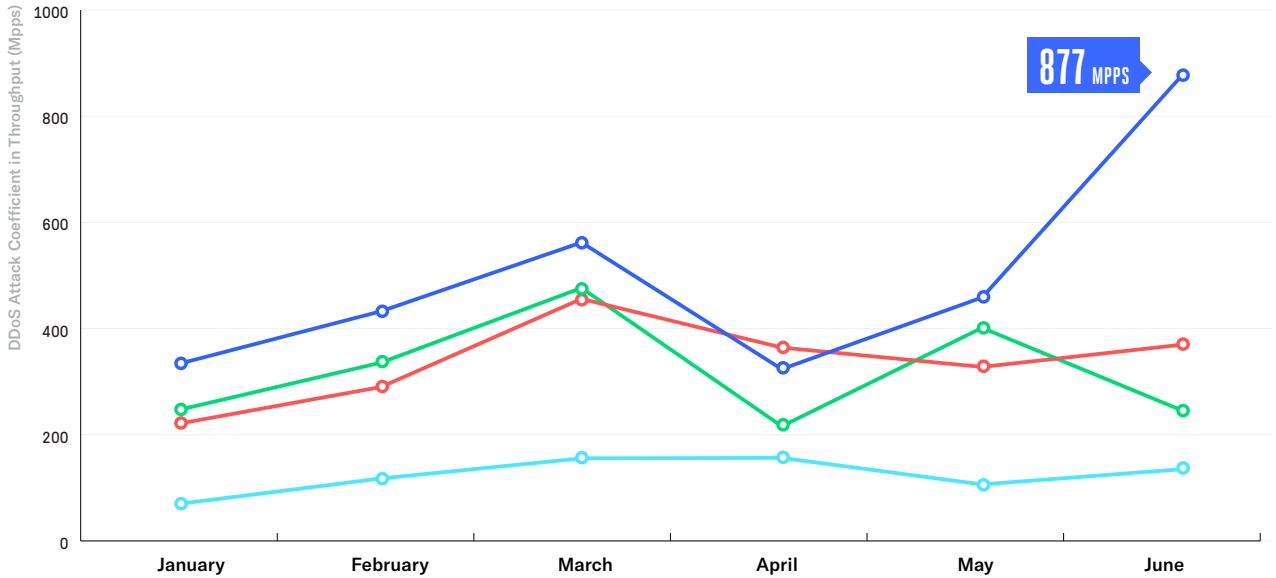



*Figure 2: Six Months of Throughput DAC*

**From there, we wanted to understand how much traffic on the global internet is due solely to DDoS attacks.**

To find out, we created the DDoS Attack Coefficient (DAC). DAC represents the total sum of DDoS traffic traversing any given region or country in one minute. If we observed no DDoS attacks in a region for a one-minute interval, the DAC would be zero. But that's not what we saw.

And the fact is, we all pay for it—because DDoS attackers do not. This traffic essentially imposes an enormous and unending tax on every internet-connected organization and individual across the globe.

Figure 1 and 2 show regional DAC from January of 2020 through June 2020. The charts clearly highlight the spike in both bandwidth and throughput at the start of the COVID-19 pandemic. Slight declines as the new norm takes effect are followed by significant growth in June.

# Super-Sized Multivector Attacks

**The rising popularity of attacks using 15 or more vectors makes sense for a number of reasons.**

For one thing, the economics of attack versus defense are simply unfair. On the attacker side, booter/stressor services are so cheap and easily available that a ten-minute attack can be rented for as little as 35 cents.[4]

*Figure 3: Percentage Change in 15+ Multivector Attacks*

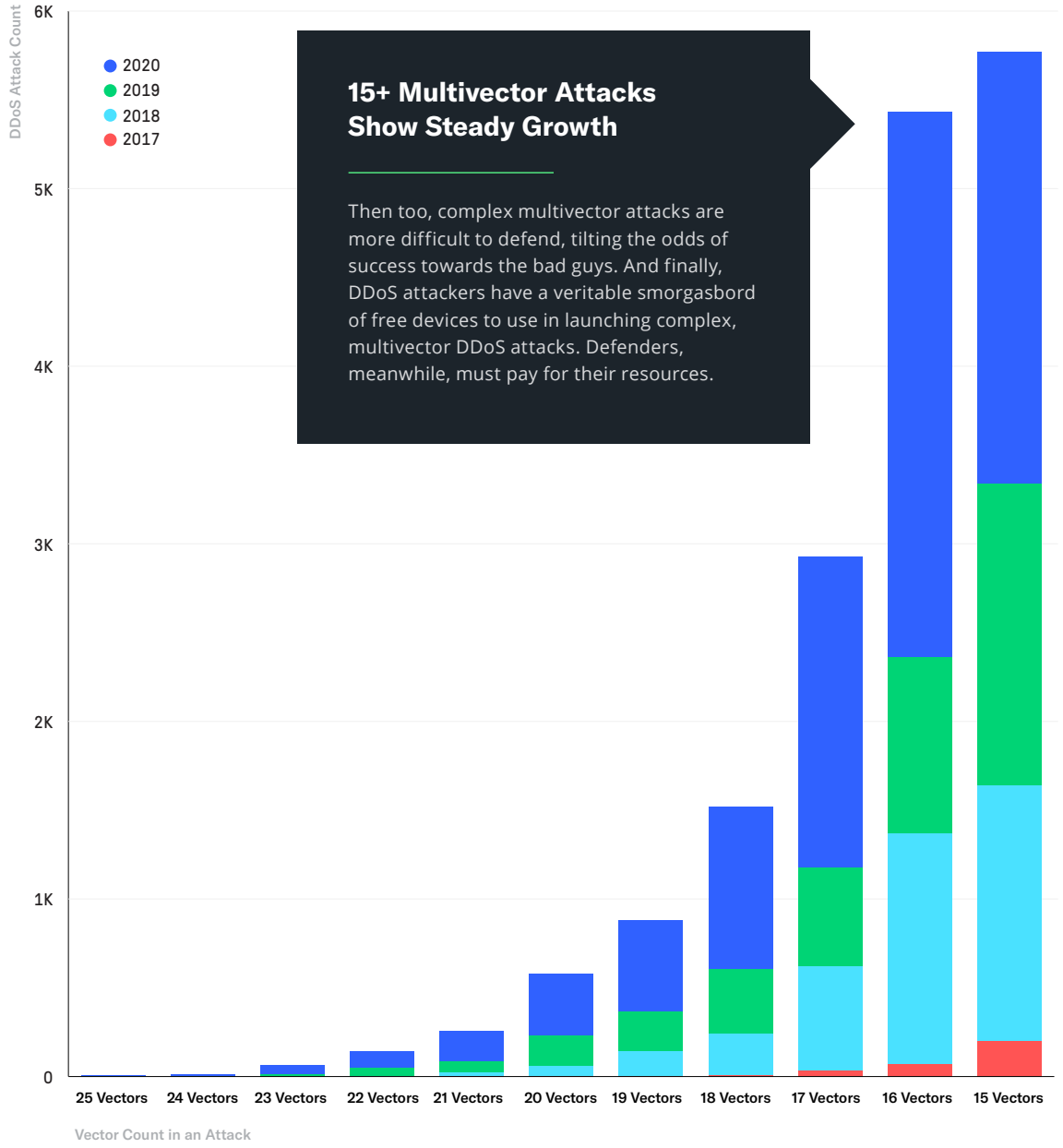
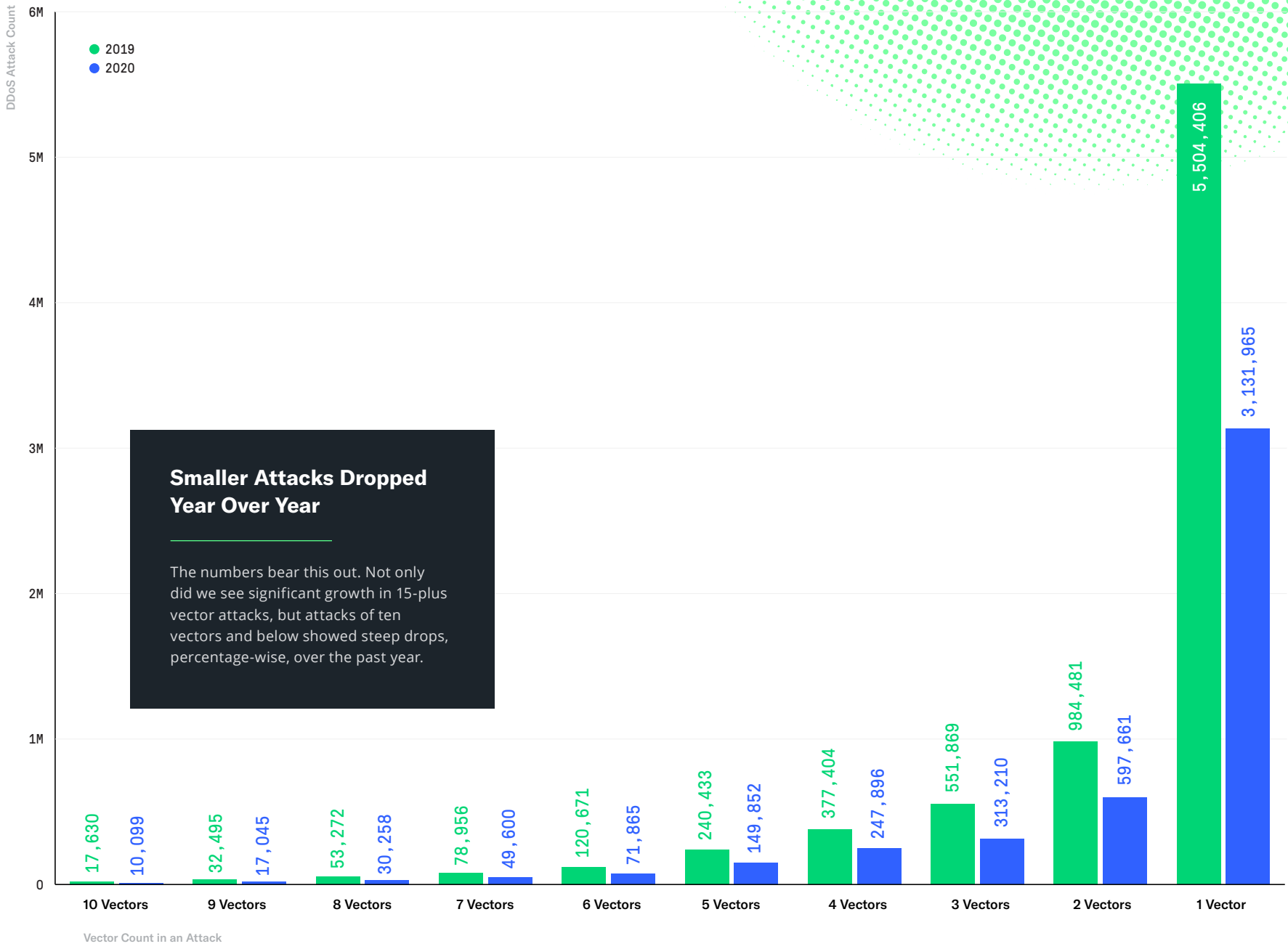


*Figure 4: 1 to 10 DDoS Attack Vector Decline*




## Smaller Attacks Dropped Year Over Year

The numbers bear this out. Not only did we see significant growth in 15-plus vector attacks, but attacks of ten vectors and below showed steep drops, percentage-wise, over the past year.

# Periodic Table of DDoS Attack Vectors

The 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.

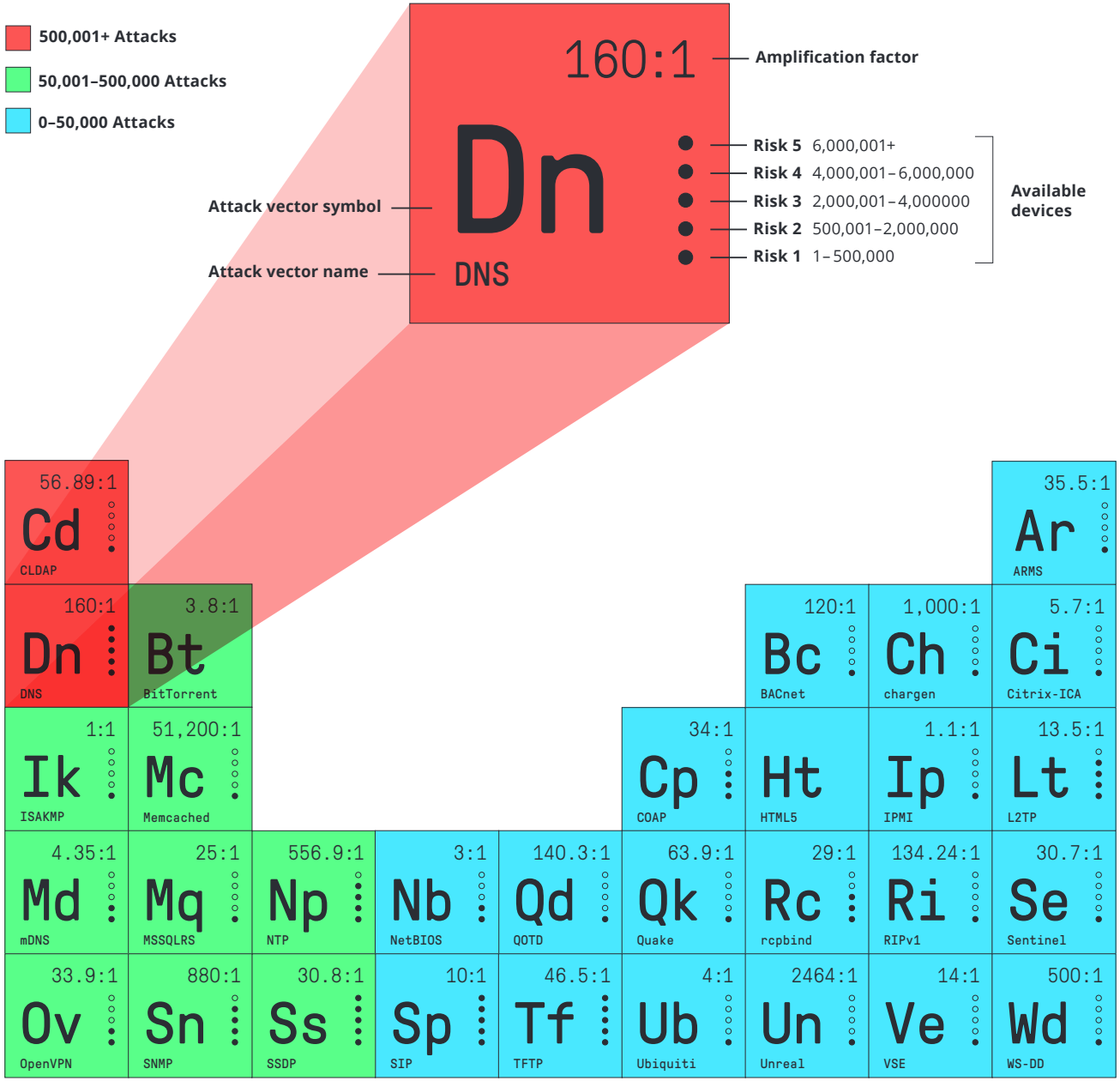



*Figure 5: Periodic Table of Attack Vectors*

## Six-Month Availability of UDP Reflectors/Amplifiers

When it comes to rating the tools of the DDoS attack trade, we once again looked at the entirety of the UDP reflection/amplification DDoS attack vectors to determine how many possible devices existed for attackers to leverage and abuse. Though there are a few surprising spikes, the vast majority remained relatively flat, indicating that unfortunately, attackers aren't going to run out of options any time soon. Figure 6 depicts the availability of reflectors/amplifiers adversaries may use for attacks.

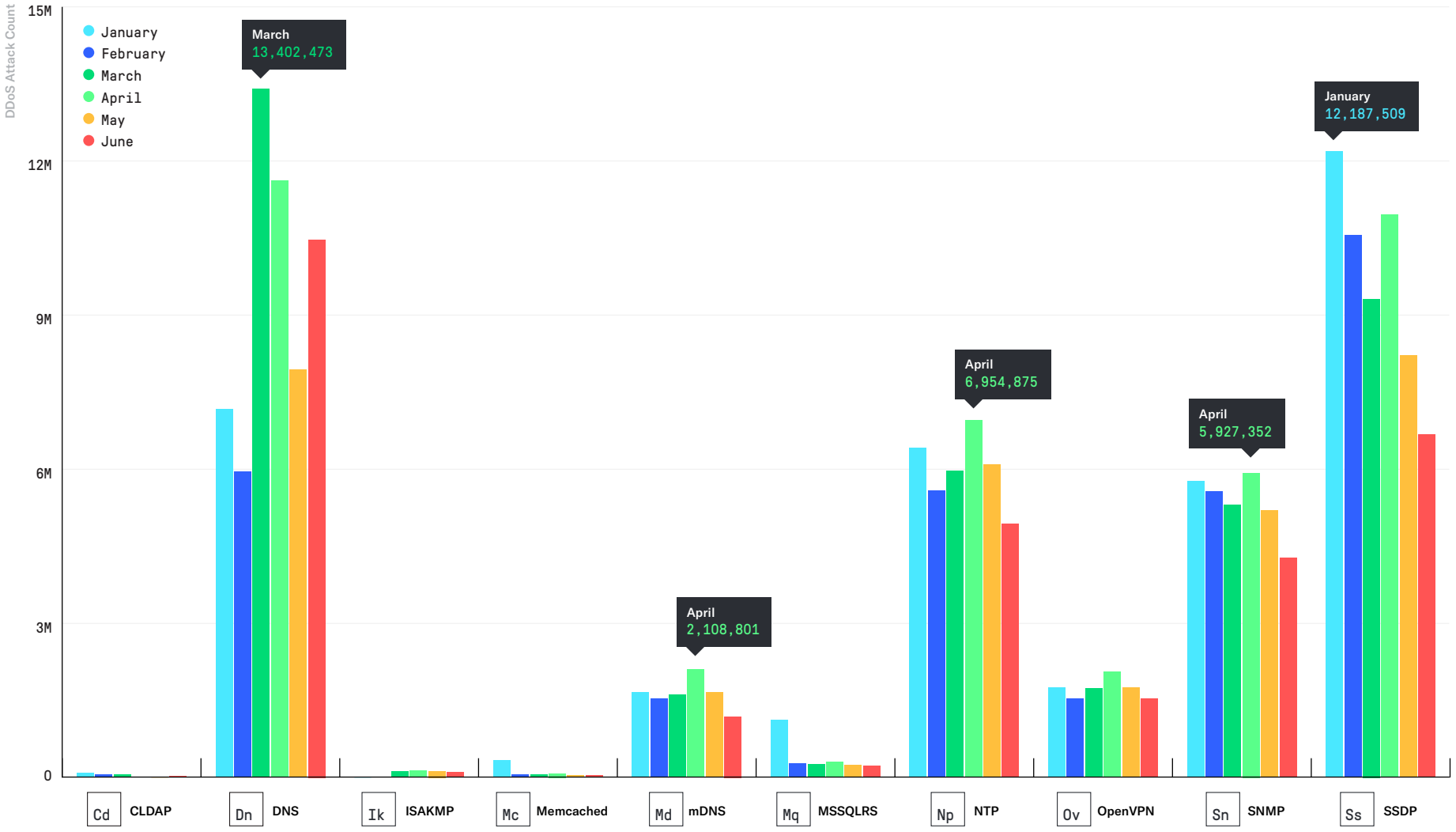
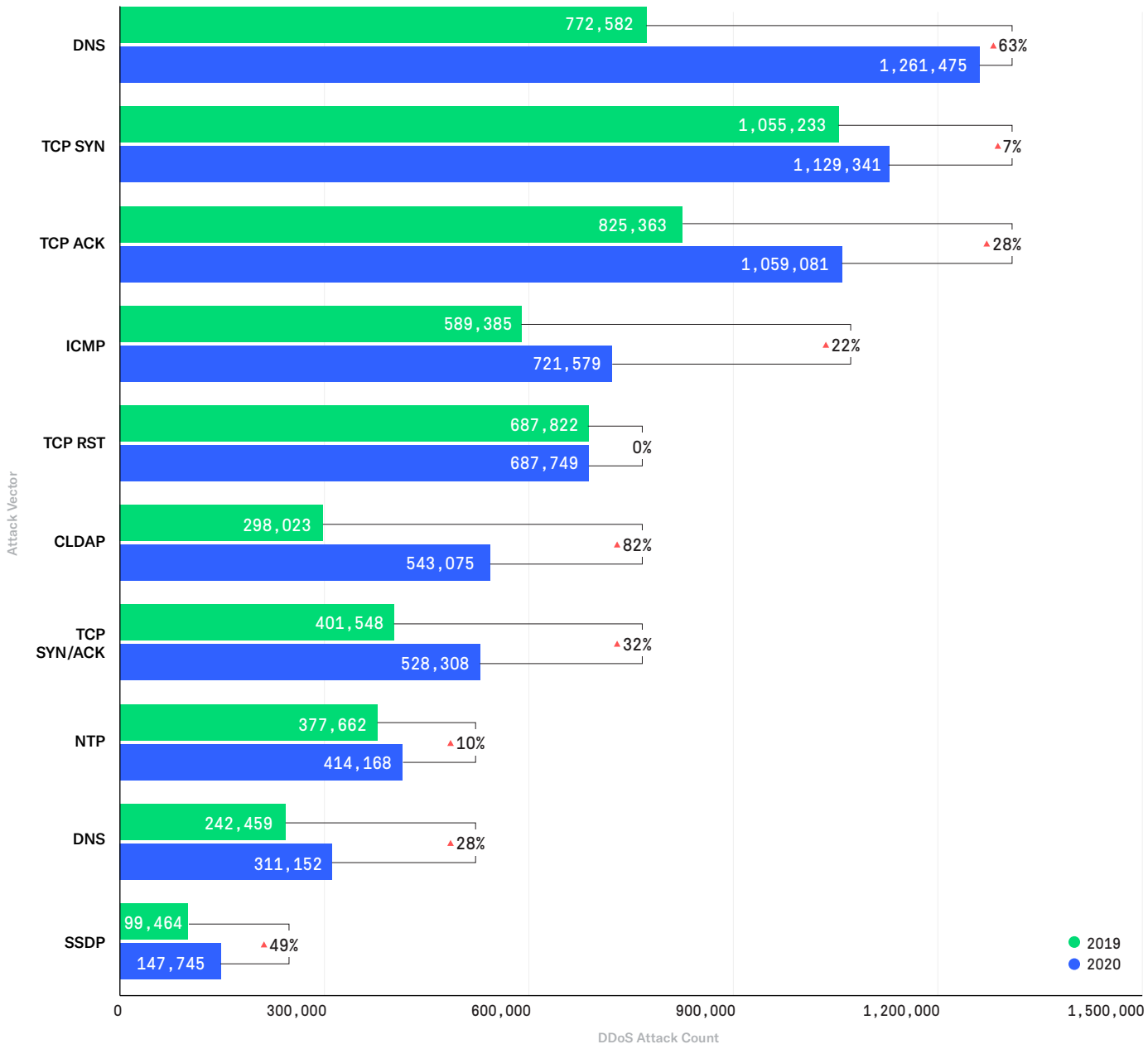



*Figure 6: Six-month availability of UDP reflectors/amplifiers*

*Figure 7: Top DDoS Vectors by Attack Count*




## Top DDoS Vectors by Attack Count

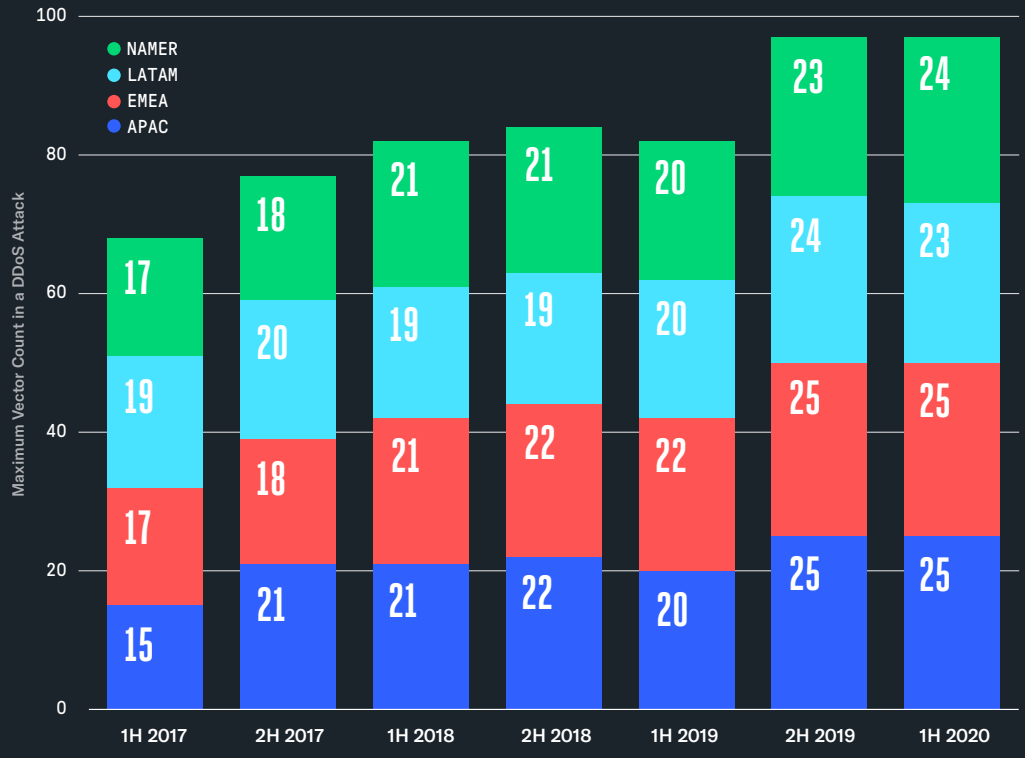
Though UDP reflection/ amplification continues to be a dominant attacker tactic, TCP-based attacks also grew significantly, increasing the difficulty of mitigation for defenders. Notably, DDoS attacks that successfully take down a service or system often result in what we call "sympathetic attacks."

In other words, a normal flood-type attack may disrupt a service where users are trying to connect. Because the service is unreachable, it generates a sympathetic TCP SYN flood. It's also common to see ICMP packets as users or other connected services query the status of the unavailable service or system.

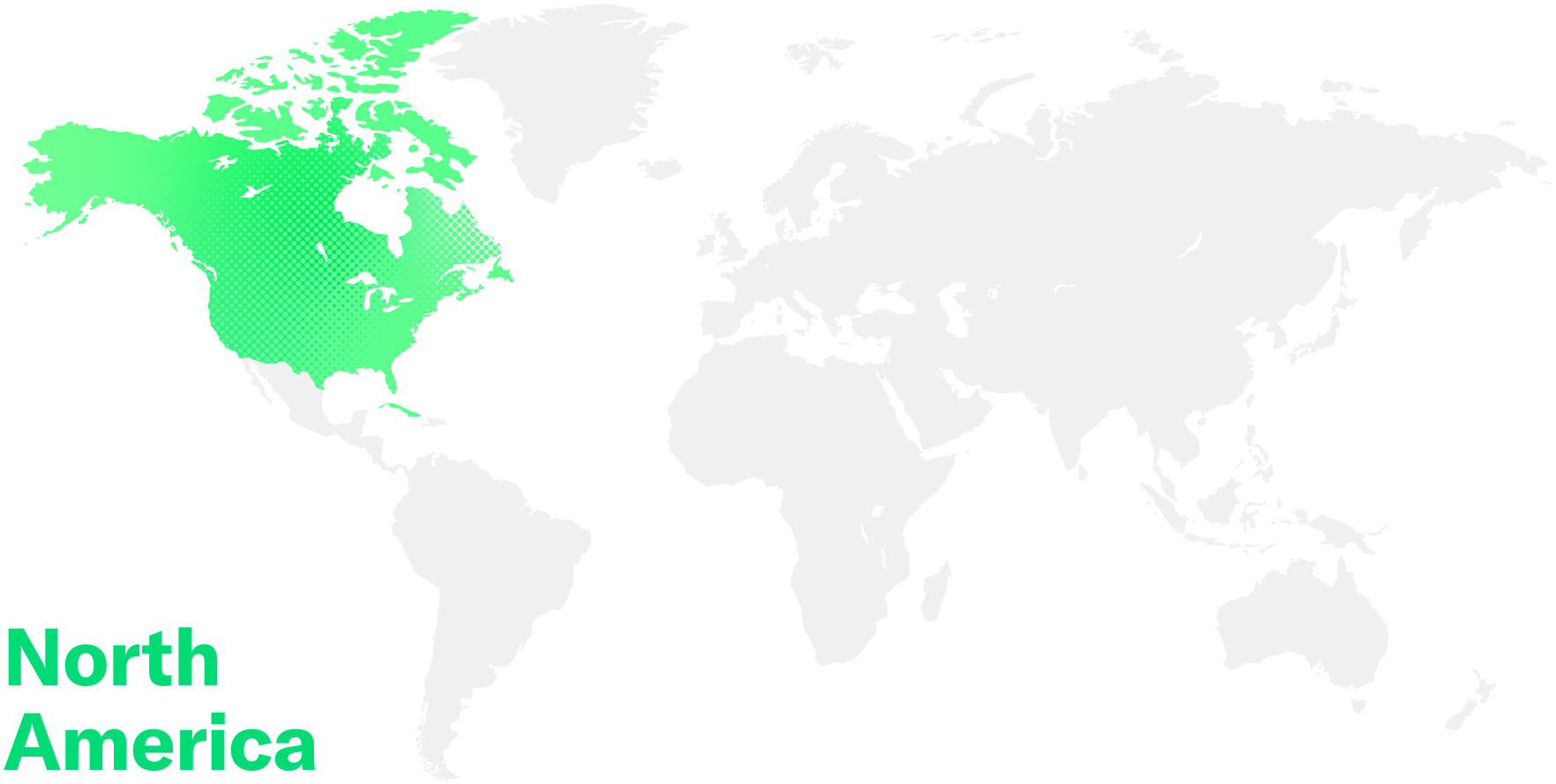
# Regional Attacks

**Broadly speaking, regional numbers continue the new attacker mantra: Pour on high-throughput, short-duration attacks that narrow the mitigation response window. Use multivector attacks as smokescreens and to increase mitigation difficulty. And remember: if it's important to you, it's important to them. That puts pandemic-era mainstays such as ecommerce, cloud, educational services, and healthcare in the cross hairs.**

*Figure 8: Regional Growth of Multivector Attacks*




For the most part, attack frequency surged, with EMEA leading at a 43 percent growth rate. Attack size grew less consistently; APAC, which sustained a 1.1 Tbps attack, understandably exhibited the largest increase. The throughput story was consistent—every region showed an increase in throughput, clear evidence of the overall shift to high pps attacks designed to overwhelm network hardware and applications. Similarly, average attack duration dropped across every region, as attackers employed an effective 'hit and run' method that not only conserves resources, but also shortens the time available for defenders to respond. And finally, we saw clear evidence that the surge in complex multivector attacks was not isolated to one region or country. A look back over three years reveals a clear and ever-expanding pattern of increased attack complexity.



# North America

**There is a middle-of-the pack look to North America, as the region saw growth in attack frequency, size, and throughput, but not at quite the same rate as other regions.**

Still, the overall trend of higher-throughput attacks of shorter duration continued to hold true. Meanwhile, attackers targeted industries vital to pandemic life. Nonstore Retailers, which includes ecommerce shopping, experienced 20 percent growth in frequency, while attacks on Educational Services grew 13 percent.

RELATIVE TO 1H 2019

| | | | |
|---|---|---|---|
| Attack frequency ▲ 20% | Max throughput ▲ 23% | 24 | |
| Max attack size 428 GBPS | Average duration ▼ 22% | Max vectors used in a single attack | |

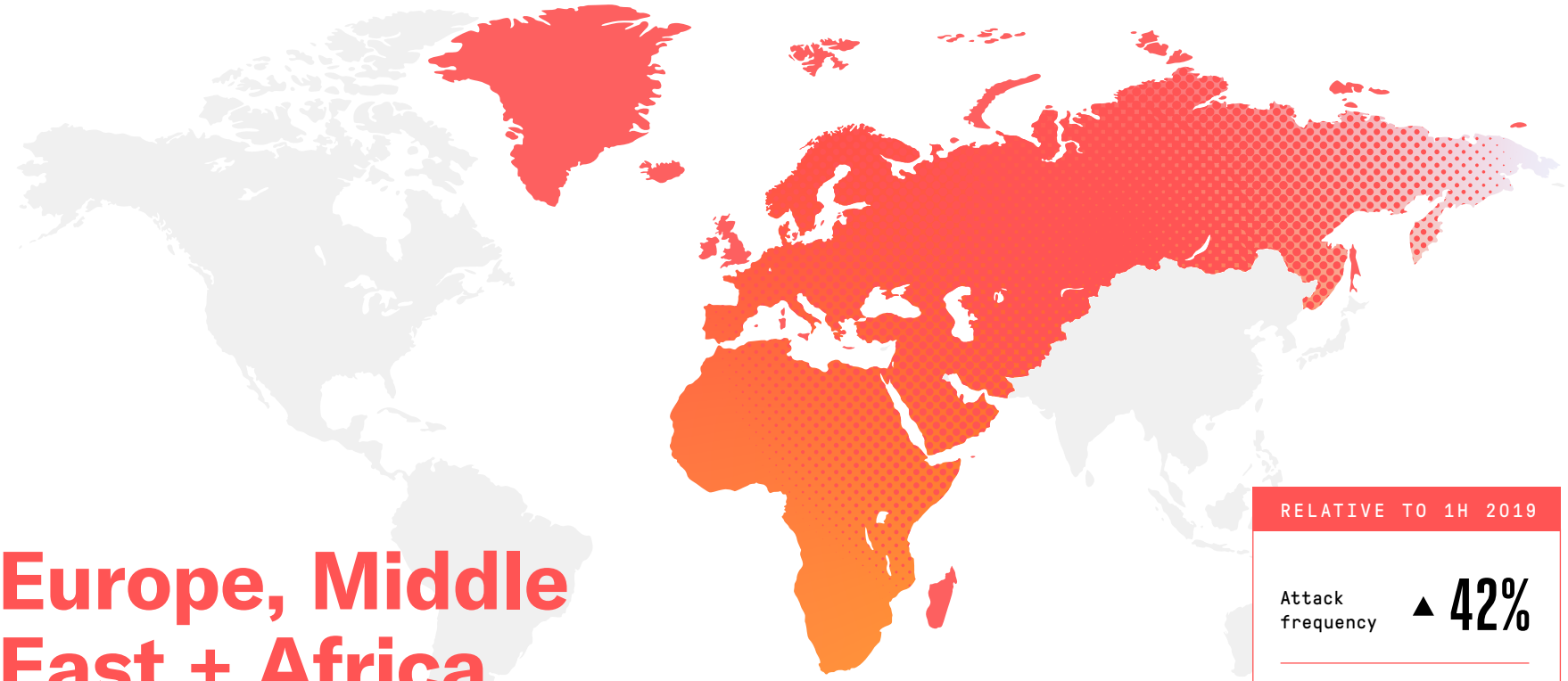
# Latin America

**Attackers targeted LATAM hospitals and doctors' offices, striking these vital services when healthcare systems were most stressed.**

Attacks grew on hospitals by 80 percent, while Ambulatory Health Care Services (aka doctors' offices and diagnostic labs) experienced a 30 percent increase. Even worse, those attacks were increasingly high-bandwidth, high-throughput affairs that are more difficult to mitigate. The max attack size on hospitals, for example, mushroomed 2,788 percent, while max throughput shot up by 863 percent.

RELATIVE TO 1H 2019

| | | | |
|---|---|---|---|
| Attack frequency ▲ 23% | Max throughput ▲ 154% | 23 | |
| Max attack size 365 GBPS | Average duration ▼ 42% | Max vectors used in a single attack | |



# Europe, Middle East + Africa

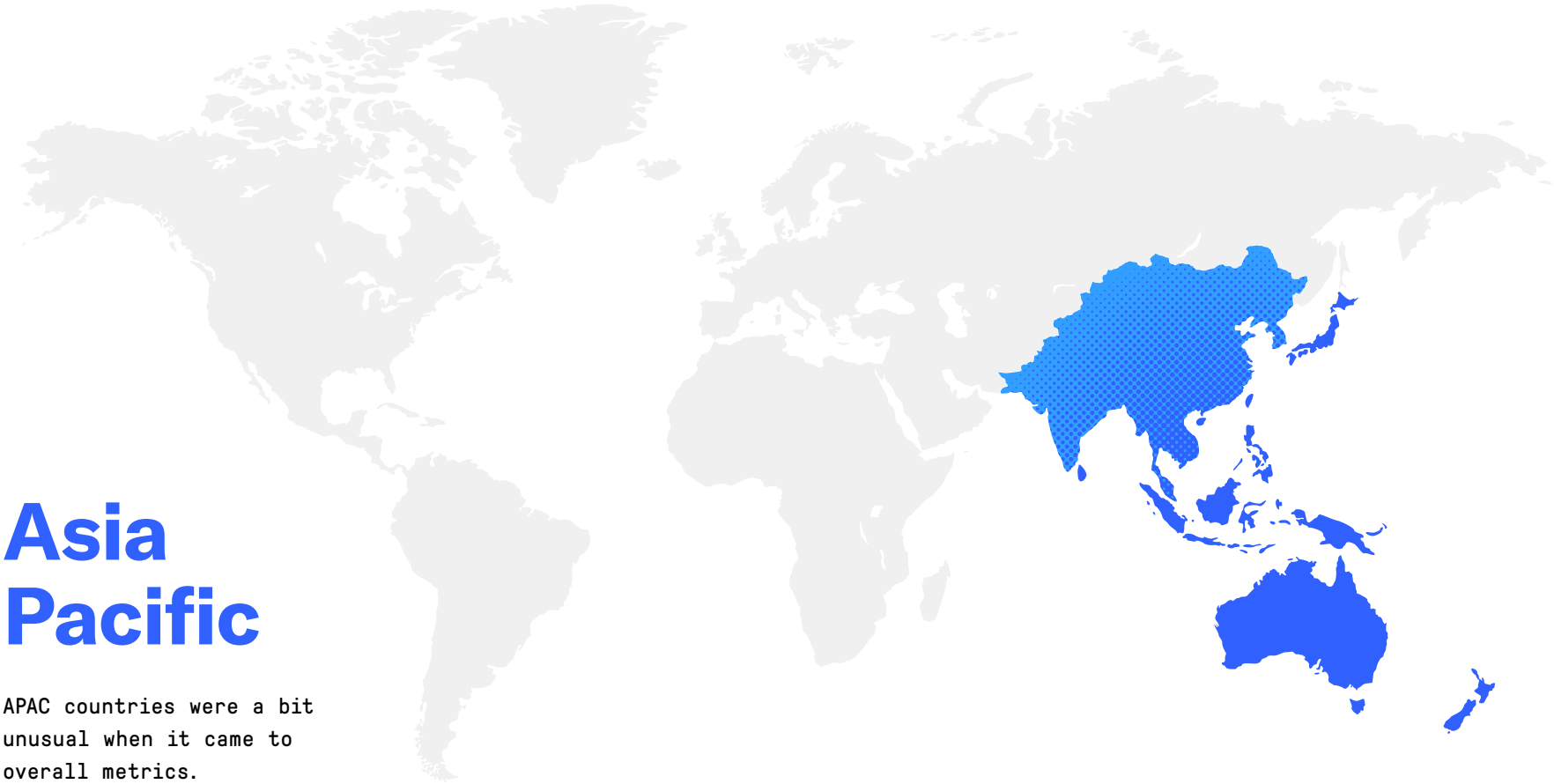
**Turkey experienced significant DDoS-related turmoil, both in terms of speed and overall impact.**

Likely a result of ideological conflict, Turkey's max attack size grew by 339 percent, while the max attack throughput ballooned by nearly 1,000 percent. At the same time, attack counts dropped 82 percent. So that means the country's companies and ISPs faced a significant increase in high-bandwidth, high-throughput DDoS traffic crossing their networks.

Germany and France also had outlier increases, although not at quite the same scale. Germany endured a 233 percent increase in attack frequency, while max attack size grew by 226 percent. In France, meanwhile, attack frequency jumped more than 100 percent, while max throughput grew by 275 percent.

Meanwhile, EMEA also experienced attacks on pandemic lifeline industries. Nonstore Retailers experienced significant across-the-board increases in frequency, size, and throughput. Data Processing, Hosting, and Related Services, which includes cloud-based services, also saw increased attention, with 30 percent more attacks that were 43 percent larger and had 52 percent higher throughput.

| RELATIVE TO 1H 2019 | |
|---|---|
| Attack frequency | ▲ 42% |
| Max attack size | 586 GBPS |
| Max throughput | ▲ 28% |
| Average duration | ▼ 9% |
| Max vectors used in a single attack | 25 |



# Asia Pacific

**APAC countries were a bit unusual when it came to overall metrics.**

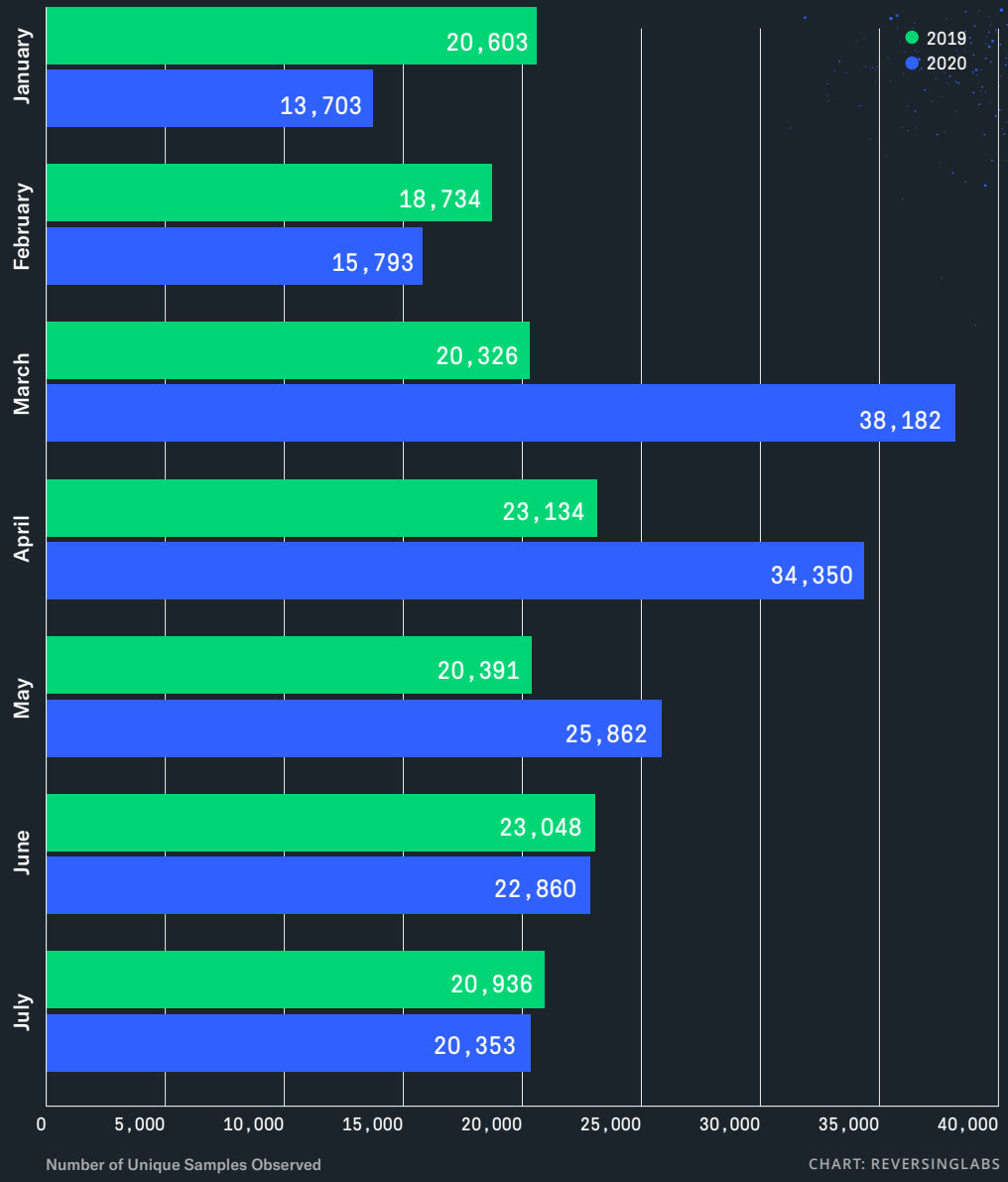
While attacks targeting Japan grew 229 percent, both max attack size and throughput dropped significantly—48 percent and 84 percent, respectively. China, meanwhile, saw only a 25 percent drop in attack frequency, while max throughput dropped 51 percent.

But when it comes to top vertical industry targets—ecommerce, education, cloud services, and healthcare—the COVID-era attacker mantra held true. Attacks on ecommerce increased by 191 percent, with high-throughput campaigns proving particularly popular—a 154 percent increase. Meanwhile, attack size and throughput for hospitals grew by 98 percent and 100 percent, respectively.

RELATIVE TO 1H 2019

| | | | |
|---|---|---|---|
| Attack Frequency ▼ 15% | Max throughput ▲ 12% | 25 | |
| Max attack size 1.1 TBPS | Average duration ▼ 71% | Max vectors used in a single attack | |

*Figure 9: Mirai 2019 vs. 2020*




# IoT

**Malicious authors continued their impressively efficient efforts to syphon in the latest IoT exploits and churn out new Mirai-based variants. Mirai still rules the ever-expanding IoT-based malware world, and the pandemic effect triggered massive growth in Mirai-based variants in March.**

These variants included the use of several older and new exploits. Just recently, a Mirai variant called "sora" was updated to include F5 BIG-IP remote code execution vulnerability (CVE-2020-5902). Most IoT botnets tend to be short-lived—once the command and control (C2) IP address is burned, the botnet is burned. However, the cost and time to set up a new Mirai botnet is minimal.

# Top 5: Mirai Variants, Brute-Force Username/Password Combinations, and Exploitation Attempts

TOP 5

## Mirai Variants

We saw a new set of top 5 Mirai variants compared with 2019. Digging into our honeypot, Table 1 is the top 5 Mirai variants observed by our honeypots during the first half of 2020. These Markers are good ways to identify variants being used.

| Mirai Variants | Unique Sources |
|---|---|
| CORONA | 9,160 |
| RETARD | 4,030 |
| UNSTABLE | 2,625 |
| KYTON | 2,201 |
| ARES | 1,964 |

*Table 1: Top 5 Mirai Variants*

TOP 5

## Username/Password Combinations

Our honeypot network saw little change in the five passwords being used to compromise IoT devices (Table 2) compared with those used in 2019. Not surprisingly, the top five passwords observed by our honeypots were included with the original Mirai botnet back from 2016—a clear sign of the original Mirai source's ongoing value for creating variants.

| Username/Password | Unique Sources |
|---|---|
| root/xc3511 | 68,140 |
| guest/12345 | 57,289 |
| admin/admin | 57,100 |
| root/vizxv | 45,408 |
| guest/guest | 44,663 |

*Table 2: Top 5 Username/Password Combinations*

TOP 5

## Exploits

Botnet operators also reused common IoT vulnerabilities in their attempts to compromise and enroll devices into botnets. While new exploits are continuously being folded into new variants, a majority of the exploit attempts observed by our honeypot network are older exploits, as shown in Table 3. Similar to the telnet passwords, we saw little change to the top five exploits year over year.

| Exploit | Unique Sources |
|---|---|
| **Realtek SDK**<br>Miniigd UPnP SOAP Command Execution | 21,175 |
| **Huawei Router HG532**<br>Arbitrary Command Execution | 16,633 |
| **Hadoop YARN Resource Manager**<br>Command Execution | 2,348 |
| **D-Link DSL**<br>OS Command Injection | 940 |
| **MVPower DVR**<br>Shell Command Execution | 849 |

*Table 3: Top 5 Exploits*

**While Mirai variants are the most dominant IoT bots seen on the internet today, several non-Mirai IoT malware are also causing a ruckus.**

# Gafgyt

**Gafgyt is a multi-architecture IoT bot with several similarities to Mirai.**

Gafgyt has used telnet with default/factory credentials and exploits to spread to vulnerable IoT devices. Like Mirai, Gafgyt supports several TCP, UDP, and HTTP based DDoS attacks. Gafgyt is continuously undergoing development with new exploits and credentials, as shown by the numerous variants running wild on the internet (Figure 10).

We saw a significant spike in Gafgyt samples from February through June, although January through February decreased compared with 2019. The spike in the number of samples is likely related to the increase in consumer devices brought online as the remote work skyrocketed during that time frame.

*Figure 10: Gafgyt 2019 vs. 2020*

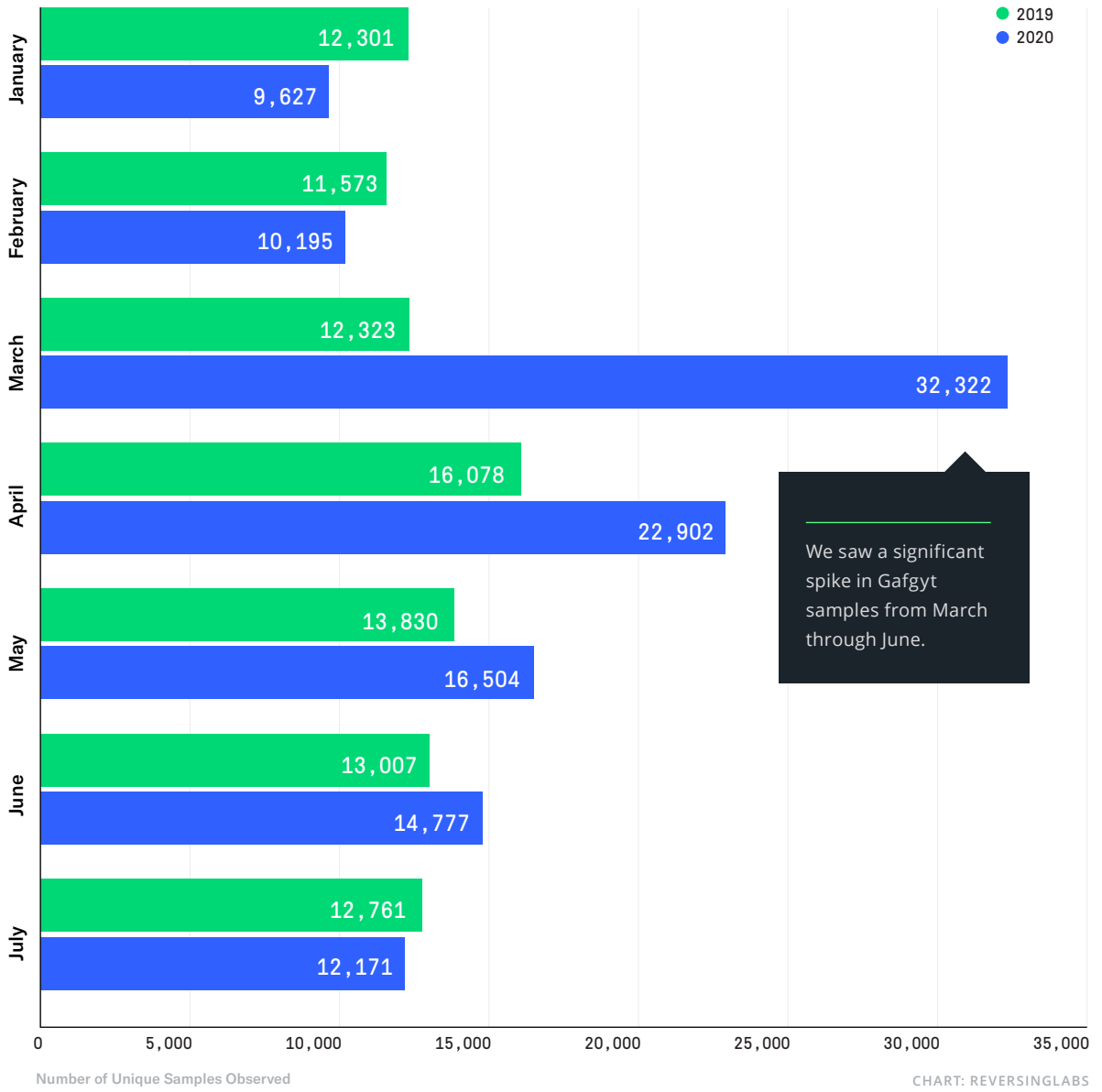


*Figure 11: Linux 2019 vs. 2020*

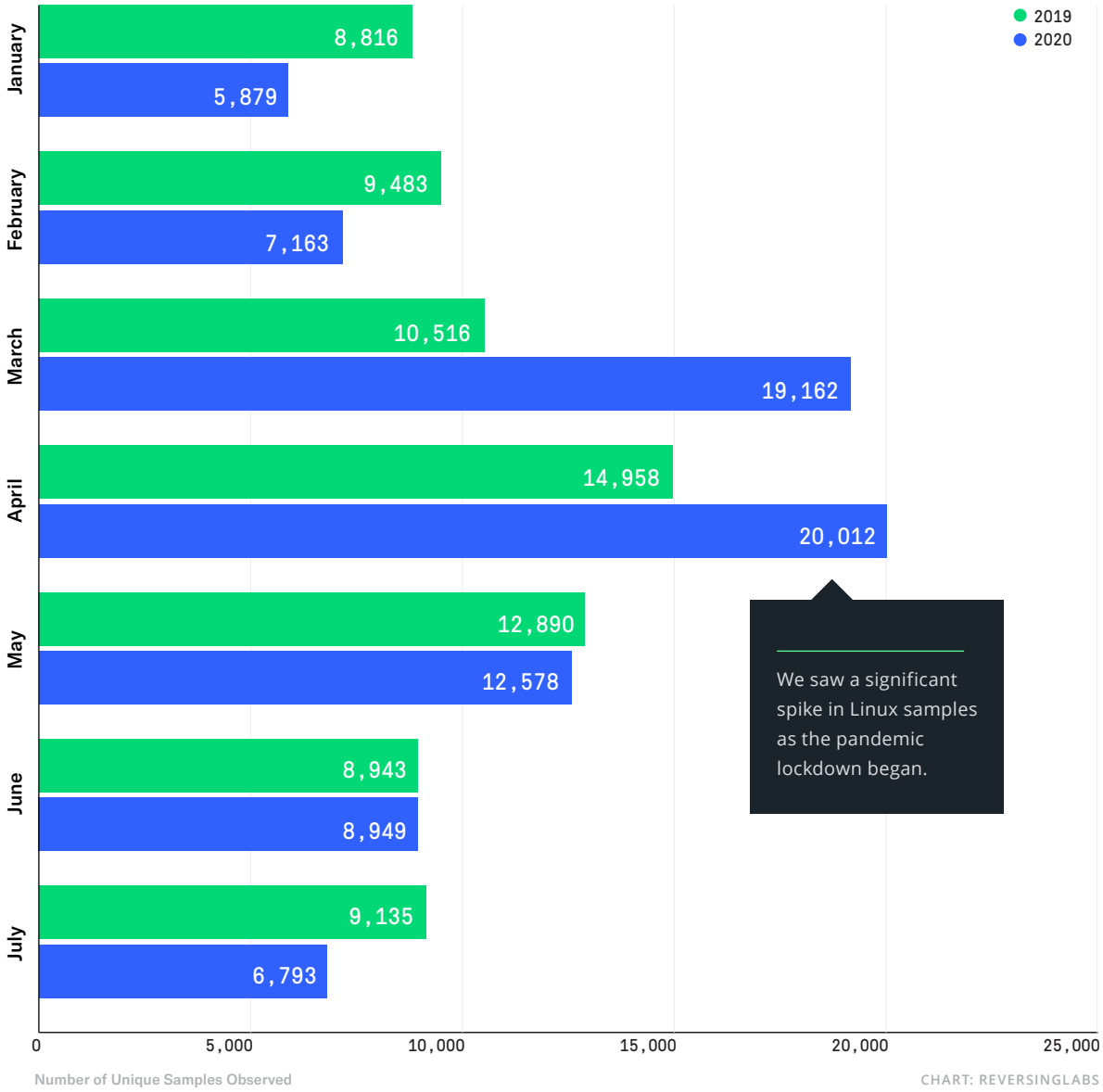



CHART: REVERSINGLABS

# Linux

**We are also seeing an uptick in Linux-based malware, as shown in Figure 11.**

The ever-growing presence of Linux in internet data centers and general-purpose computers has made these systems a lucrative target for malware authors. With the release of Windows Linux Subsystem (WLS)[5] , you can now run a full Linux environment on your Windows desktop or server.[6] Using Microsoft's Visual Studio, you can also cross-compile your code to run on Windows or Linux, and leverage WLS to test and debug your Linux binary on the same system.

We are starting to see malware authors take advantage of these features to target not only Windows, but Linux as well. Let's look at some examples of recent Linux-based malware. The popular TrickBot malware ported the Anchor framework to Linux. Anchor_Linux, as it's called, is used as a pivot to infect Windows systems that are connected to the compromised Linux server. The NSA and FBI released details about a Linux-based malware called Drovorub.[7] Drovorub supports data exfiltration, port forwarding, and arbitrary command execution on the infected system.

# Lucifer

**ASERT researchers discovered a Linux port for Lucifer, a hybrid cryptojacking and DDoS malware.[8]**

Lucifer is capable of standard ICMP, TCP, and UDP-based flooding attacks, including the ability to spoof the source IPs of attack packets. Additionally, Lucifer supports HTTP application-layer attacks, including basic HTTP GET- and POST-floods, as well as multiple versions of HTTP 'CC' DDoS attacks. Arbitrary command execution on the infected system is also supported by Lucifer. Similar to Trickbot, Lucifer can also be used to infect other Windows systems connected to the same network.

As several IoT devices are based on a Linux distribution, it would not be a huge stretch for a creative malware author to recompile the Linux versions of their malware to run on IoT-based devices, using common IoT vulnerabilities as an infection method. This would trigger a new wave of cross-platform malware targeting all the major devices and operating systems.

This is certainly the case with the Lucifer bot. The fact that it can run on Linux-based systems means that it can potentially compromise and make use of high-performance, high-bandwidth servers in internet data centers (IDCs), with each node packing a larger punch in terms of DDoS attack capacity than is typical of most bots running on Windows or IoT-based Linux devices.

Unsurprisingly, we anticipate seeing the number of Linux and cross-platform malware increase in 2020 and beyond.

# 4.8 million DDoS attacks hit the world in the first six months of 2020—and at what price?

**Those attacks consumed enormous amounts of bandwidth and throughput, and both service providers and enterprises must absorb that traffic as a cost of doing business in the digital economy.**

Cybersecurity math has always favored the bad guys. The latest example is the trend towards fast but complex multivector attacks. Shorter duration + increased complexity = less time to respond to increasingly difficult-to-mitigate attacks.

Today's new normal means that our increased reliance on remote connectivity won't disappear any time soon. Recent attacks on educational platforms are likely just an opening salvo as school season commences.

High-profile DDoS attacks on regional financial service entities[9] could well signal continued interest in companies that rely on online transactions. Such scenarios only highlight the vital role of advanced and automated DDoS technology.

## APPENDIX

[1] securityboulevard.com/2020/09/teenager-arrested-for-last-weeks-ddos-attacks-on-miami-dade-public-school-network/

[2] netscout.com/blog/asert/netscout-arbor-confirms-17-tbps-ddos-attack-terabit-attack-era

[3] netscout.com/blog/asert/measuring-cruellest-month

[4] csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html

[5] docs.microsoft.com/en-us/windows/wsl/

[6] docs.microsoft.com/en-us/windows/wsl/install-on-server

[7] media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF

[8] netscout.com/blog/asert/lucifers-spawn

[9] netscout.com/blog/asert/high-profile-ddos-extortion-attacks-september-2020

## 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-2002 09/2020

NETSCOUT