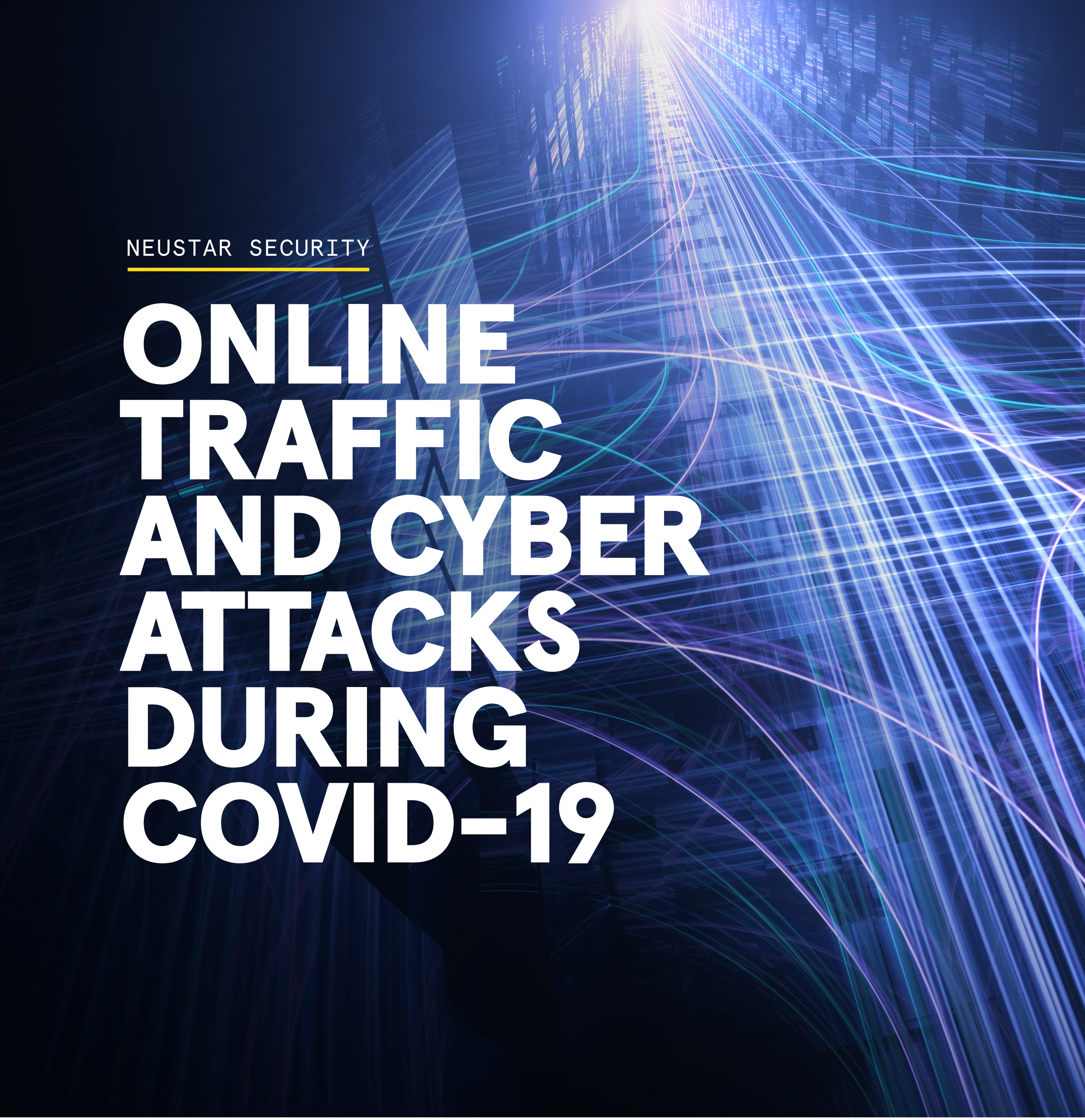


NEUSTAR SECURITY

ONLINE TRAFFIC AND CYBER ATTACKS DURING COVID-19

neustar Security

Life has changed dramatically since COVID-19 entered our lives. Previously unknown phrases like "social distancing" have become common parlance. The sudden appearance of masked individuals no longer signals a possible robbery in process. We have traded happy hour gatherings at our favorite watering hole for group conference over video chat.

Given Neustar's position in providing navigation for internet requests made to the Domain Name System, or DNS (via the global UltraDNS network) to threat detection and Distributed Denial of Service (DDoS) mitigations (with UltraDDoS Protect), we have had a front row seat from which to observe the challenges posed by COVID-19. In this paper, we will consider what is different, both in terms of traffic in general and in attacks specifically. We will contrast these findings with what we have seen in 2019 and even 2018, to get a clearer picture of just how much things have changed.

DNS:
Where Connections Begin

Neustar UltraDNS network spans across 30 globally distributed nodes and includes top-level domain (TLD) and second-level domain (SLD) name servers as well as public open resolvers. Although the overall goal of the Domain Name System (DNS) is to resolve commonly known domain names to the actual IP address of the target server, the different parts of the system are designed to do different things. Each of these services deliver data, which is vital to observing internet trends, and their different "viewpoints" enable unique perspectives.

TLD SERVERS

Top-level domain names reside in root servers, at the top of the DNS hierarchy. In the example "www.example.com," the top-level domain is the ".com" portion of the URL. While the TLD is a key portion of the address, it is usually somewhat generic.

SLD SERVERS

Second-level domain names are served here. In the example "www.example.com,"the second-level domain name is "example." These names serve as primary differentiators for businesses and are also known as authoritative name servers.

PUBLIC OPEN RESOLVERS

These servers, also referred to as recursive servers (RCSV), can be used by networked devices to query the DNS instead of—or in conjunction with—the servers operated by the local ISP.

To observe the effect of the pandemic on the internet, we begin with a look at the aggregate traffic by week across all three services.

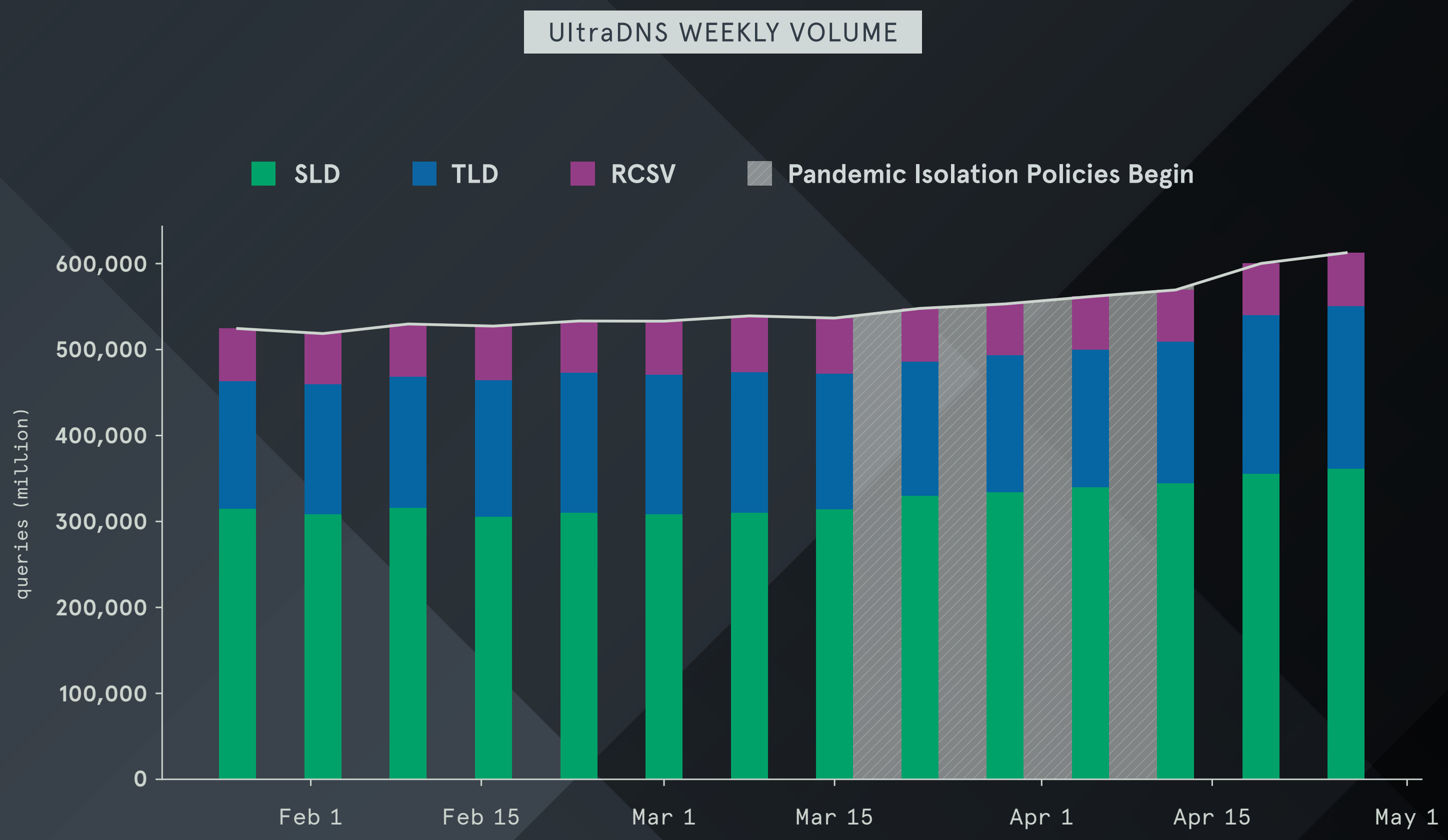


Figure 1: Aggregate weekly traffic from Neustar UltraDNS network

Figure 1 displays aggregate traffic during the weeks most closely associated with the pandemic. The figure shows a noticeable rise in traffic in mid-March, which correlates with the dates that US schools and organizations began to implement isolation policies. Interestingly, query numbers continue to rise, showing a sharp uptick about a month after isolation policies begin to take hold.

By diving more deeply into this data, we can see the pandemic effect more clearly. In Europe, which was hit by the pandemic earlier, you can see a clear rise as isolation took hold, and then another uptick about a month later.

AGGREGATE DAILY NODE VOLUME

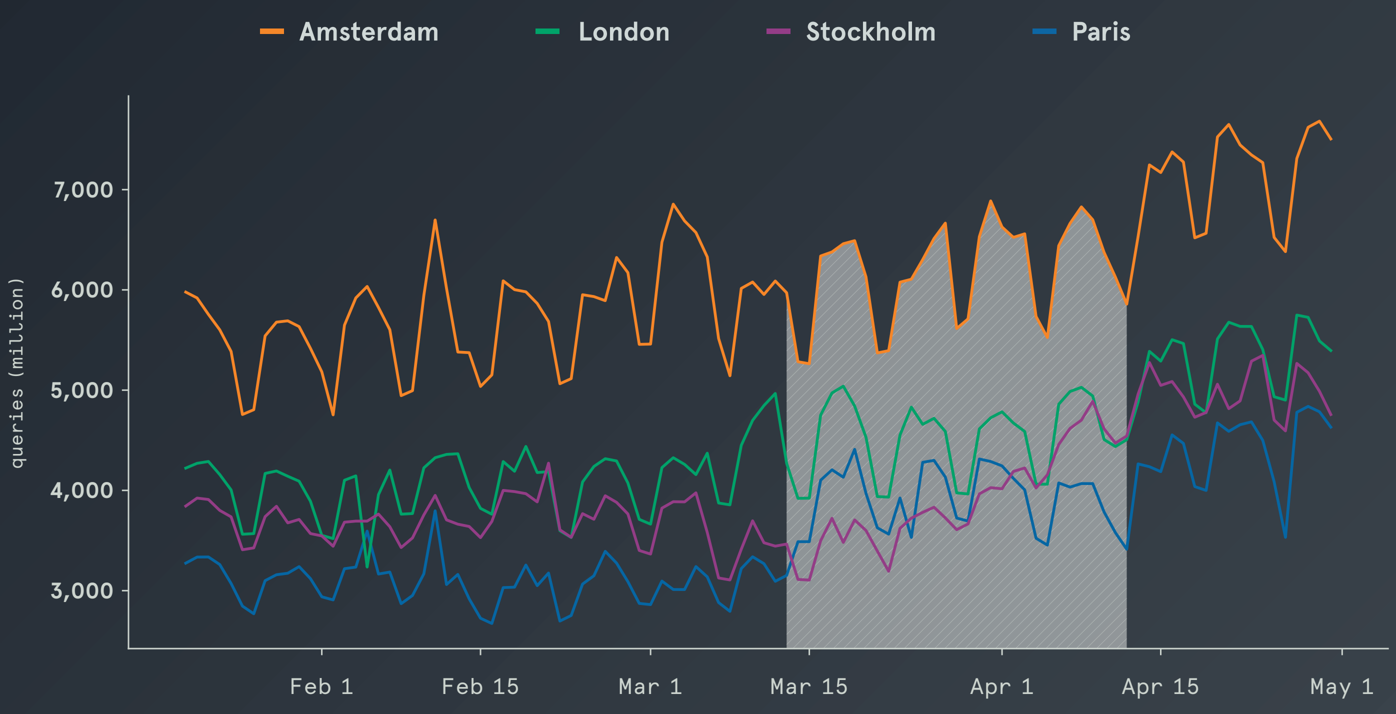
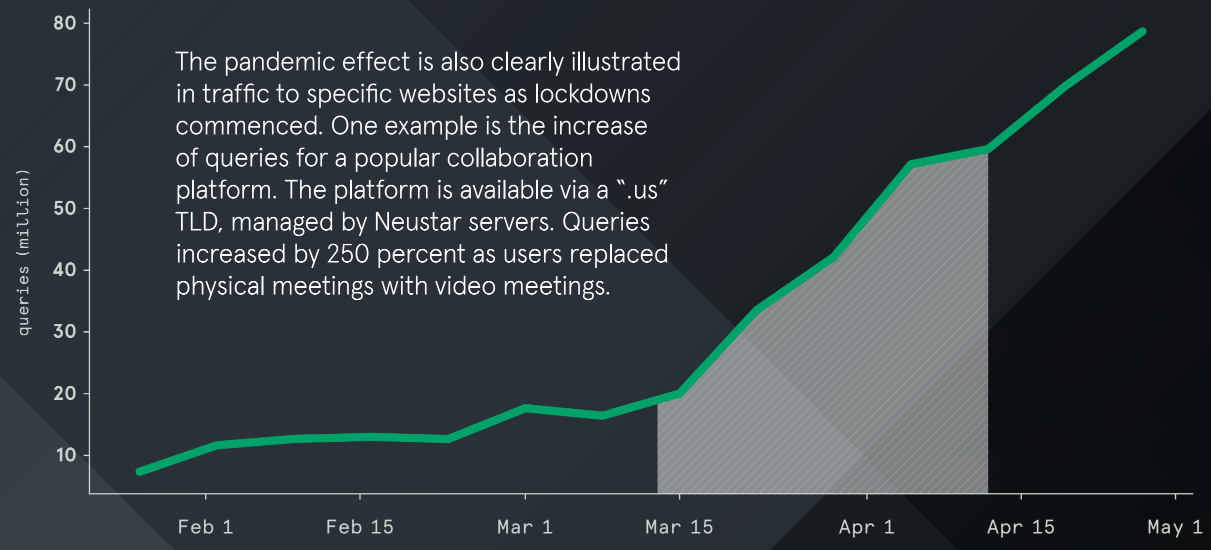


Figure 2: Weekly aggregate queries from UltraDNS European nodes

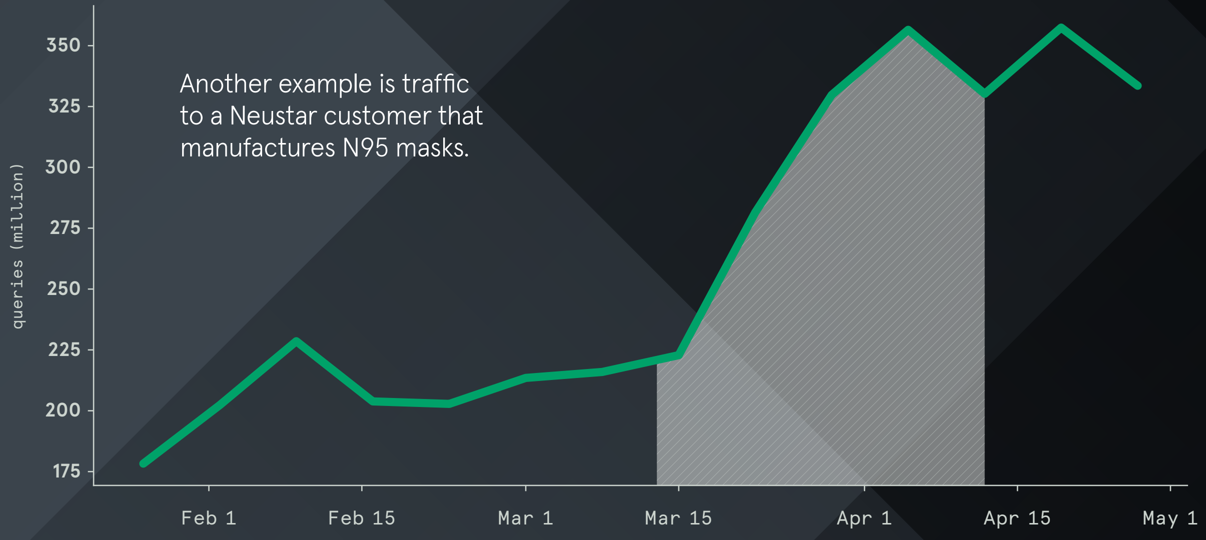
POPULAR ONLINE COLLABORATION PLATFORM WEEKLY VOLUMES



The pandemic effect is also clearly illustrated in traffic to specific websites as lockdowns commenced. One example is the increase of queries for a popular collaboration platform. The platform is available via a ".us" TLD, managed by Neustar servers. Queries increased by 250 percent as users replaced physical meetings with video meetings.

Figure 3: TLD queries for a popular online collaboration platform

N95 MASK MANUFACTURER WEEKLY VOLUMES

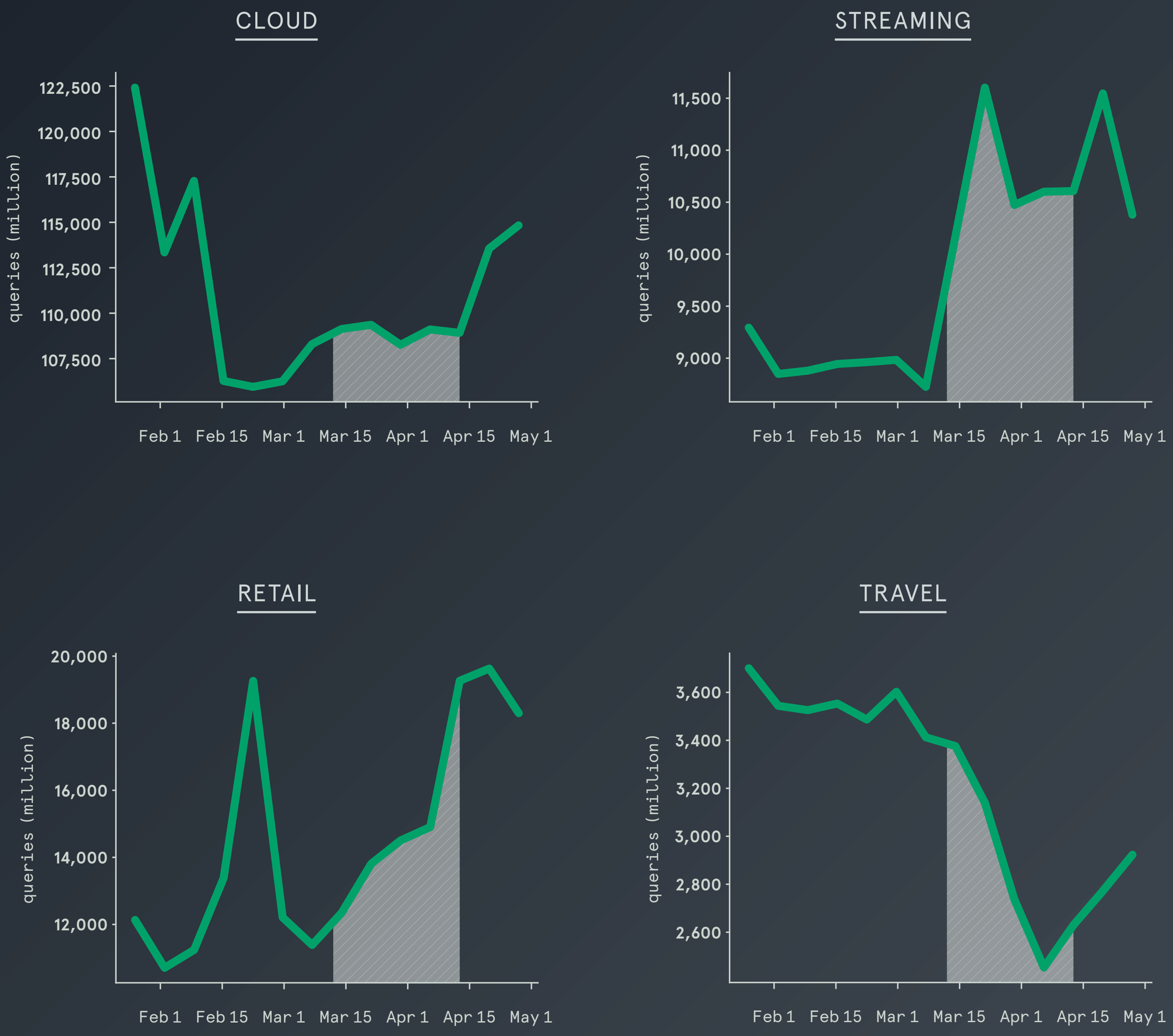


Another example is traffic to a Neustar customer that manufactures N95 masks.

Figure 4: SLD queries for N95 mask manufacturer

Of course, not all industries have been affected equally. As you might expect, queries to retail companies and streaming services have seen a large increase during the one-month period, while the travel industry saw a decline initially, but appears to be recovering.

DNS TRAFFIC QUERIES BY VERTICAL



CLOUD

STREAMING

RETAIL

TRAVEL

DDoS Attacks:

Growing in Every Dimension

At first glance, it may seem logical to posit that, as internet traffic rises, so too should the number of attacks. Neustar expected an increase, but we're seeing a dramatic upturn in attacks using virtually every metric that we measure. We have observed an increase in the overall number of attacks as well as in attack severity, which considers the volume of attack (measured in tera- or gigabits per second, which congests bandwidth) and attack intensity (measured in millions of packets-per-second, which targets infrastructure). When considering the attacks on direct UltraDDoS Protect customers, combined with attacks on customers to whom we offer a SoC-as-Service and attacks on our own UltraDNS platform, Neustar has mitigated more than double the number of attacks in Q1 2020 than in Q1 2019, a 100 percent increase. As we have moved into Q2 2020, we have seen the largest volumetric attack that Neustar has ever mitigated—indeed one of the largest in internet history—at 1.17 Tbps. We've also frequently seen other intense attacks, regularly topping 300 Mpps, throughout this period.

Neustar has mitigated more than double the number of attacks in Q1 2020 than in Q1 2019, a 100 percent increase.

Looking at the bi-weekly charts below, it is easiest to see the "pandemic effect" in aggregate as you look across the top three metrics: attack numbers, attack volume, and attack intensity.

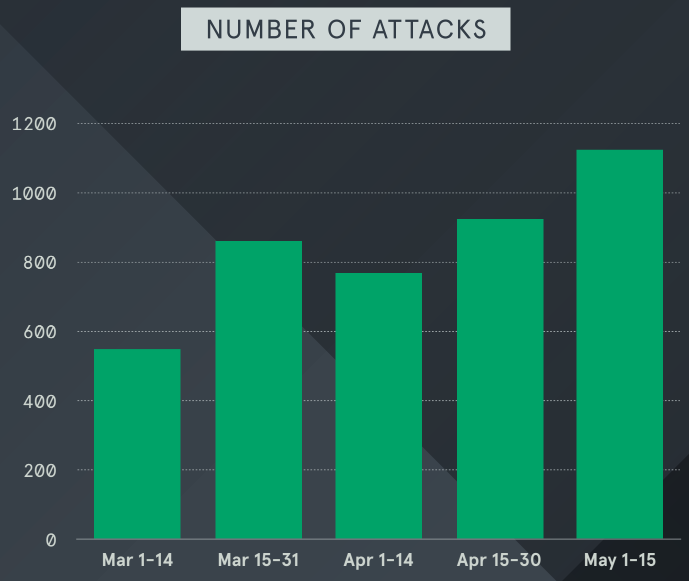

NUMBER OF ATTACKS

Figure 5: Biweekly attack metrics

One interesting way to visualize these trends is to consider how each one rises and falls in comparison to the others. In the first two weeks of May, for example, the maximum intensity of attacks was fairly low, as was the maximum volume of attacks. But any sense that things were starting to quiet down are dispelled when you consider the number of attacks between May 1 and May 15. During this period, Neustar mitigated a larger number of attacks than any other period in Q1 2020.

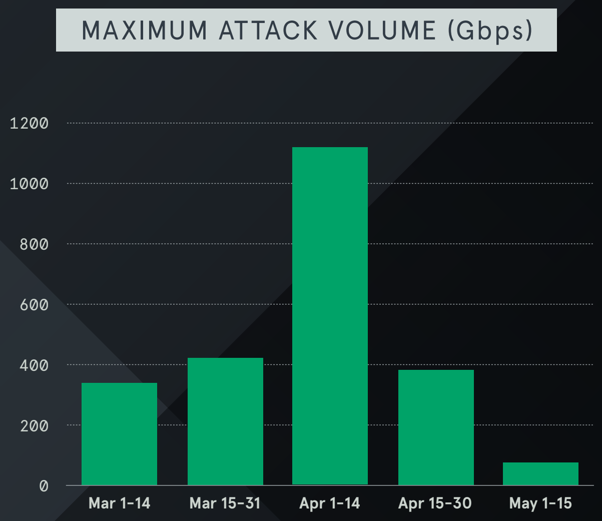

MAXIMUM ATTACK VOLUME (Gbps)

Figure 6: Biweekly attack volumes

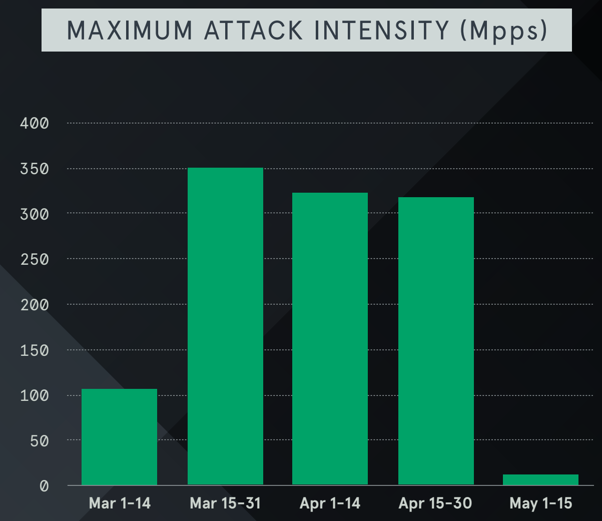

MAXIMUM ATTACK INTENSITY (Mpps)

Figure 7: Biweekly attack intensity

What Does It All Mean?

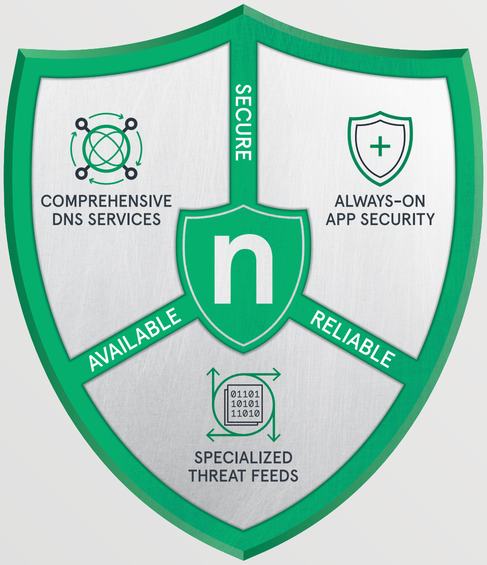
The degree to which all of us have become suddenly reliant on the internet is intuitively easy to understand. A quick look at the trends in DNS queries validates the assumptions. But the burgeoning number of attacks put the threats to this increasingly vital resource into high relief.

- In February 2020, the FBI issued a Private Industry Notification (PIN) informing businesses about a potential DDoS attack that targeted a state-level voter registration and information site.
- The US Department of Health and Human Services was targeted by a DDoS attack on March 15—just as the population needed a source of accurate information.
- A recent report from Europol warns of cybercriminals finding new targets, saying: "The pandemic may multiply the damaging impact of a successful attack against certain institutions, which reinforces the necessity for effective cyber resilience."

While many DDoS and other types of attacks focus on corporate assets, the DNS infrastructure upon which the internet depends may also be threatened. As employees are forced to work from home, there has been an increase in DNS hijacking, a technique in which DNS settings redirect the user to a website that might look the same on the surface but often contains malware disguised as something useful. Neustar has always been aware of both the mission-critical nature of DNS as well as possible attacks upon it; in fact, Neustar's award-winning UltraDDoS Protect platform was originally built to protect our UltraDNS infrastructure, and the resources are often co-located.

If COVID-19 has taught us anything, it's how quickly things can change. Organizations, from schools and hospitals to retail and communications, are struggling to retool and scale their offerings to meet challenges that were unheard of just a few short months ago. This process of forced change is made even more difficult by the new reality of working from home. Adding more security on top of an already precarious situation seems impossible, but it doesn't need to be.

Neustar's UltraDNS platform is a rock-solid industry leader, built from the ground up with security in mind. Neustar offers complete DDoS protections in whatever form fits your needs, from on-demand router-based mitigation to always-on web asset protection.



Don't take chances. Get protection from Neustar, and remain Always-on, *Ultra* Secure.

About Neustar

Neustar is an information services and technology company and a leader in identity resolution providing the data and technology that enables trusted connections between companies and people at the moments that matter most. Neustar offer industry-leading solution marketing, risk, communication, security, and registry that responsibly connect data on people, devices, and locations, continuously corroborated through billions of transactions. Neustar serves more than 8,000 clients worldwide, including 60 of the Fortune 100. Learn how your company can benefit from the power of trusted connections.

www.home.neustar