radware

Q1, 2021 | MAY 2021

Quarterly DDoS Attack Report

Radware's Quarterly DDoS Attack Report provides an overview of attack activity witnessed during the first quarter of the calendar year, 2021. It analyzes DDoS attack activity by industries, attack vectors, DDoS attacks on applications, and on-premise vs. cloud.

Table of Contents

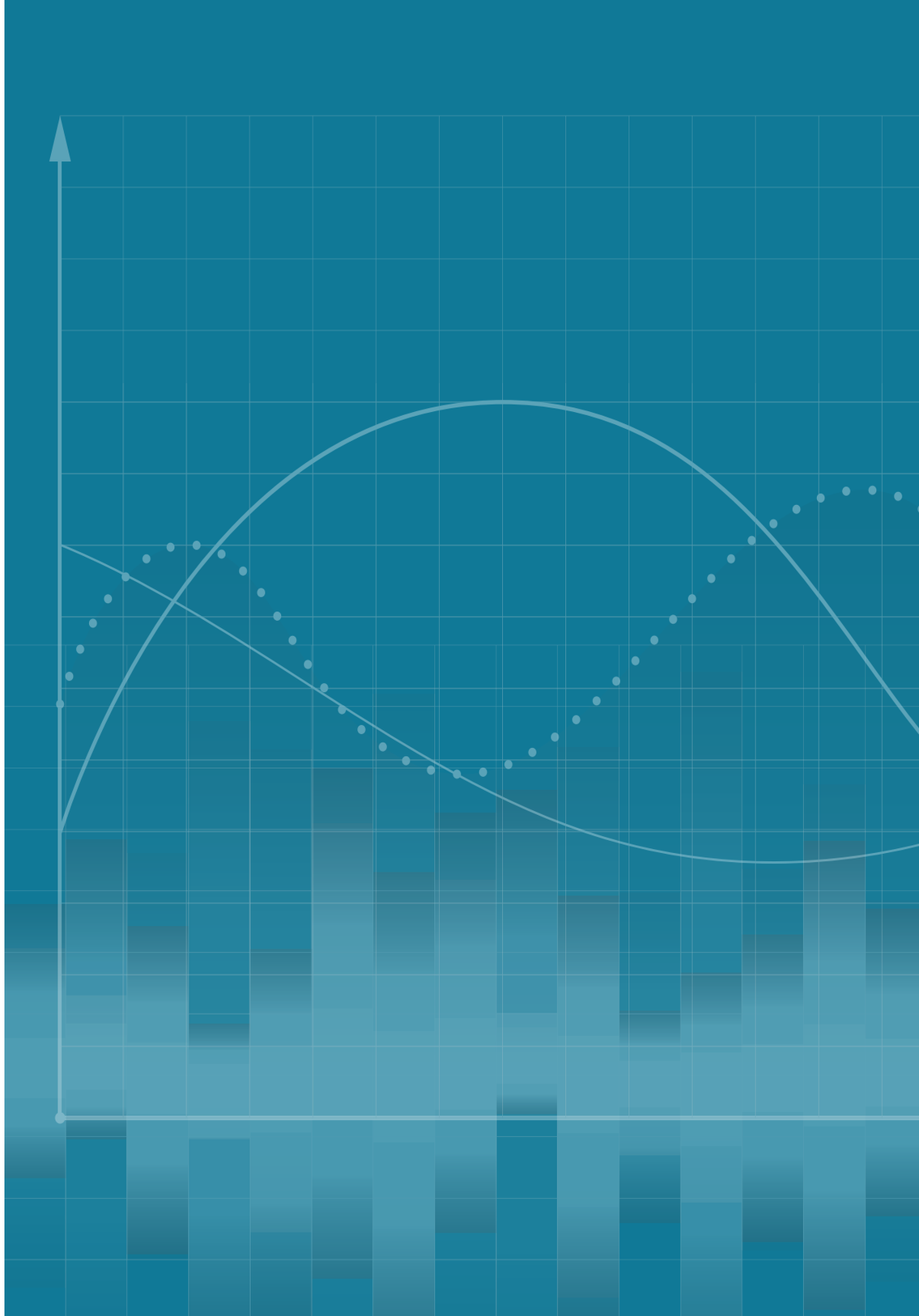
Overview

The first half of Q1 was characterized by large attacks on finance and a continuation of the 2020 ransom DDoS campaign. By the end of 2020, the extortionists started circling back to earlier victims who did not pay ransom in earlier attempts, reusing their attack research and increasing the pace of their campaign in an attempt to benefit from the surging Bitcoin value [1].

Biotechnology and pharmaceutical experienced continuous waves of minor attacks targeting their operations, thereby continuing the trend from the previous quarter. Other industries experienced similar attacks as well.

To overcome the pandemic, organizations began relying on remote operations, teleworking and remote access infrastructure. As a result, DDoS actors found new opportunities and began targeting the back-end of the communication infrastructure of organizations. Several global organizations had branches/remote offices impacted during this period, with actors leveraging new tactics to impact organizational productivity by targeting internet connectivity and remote access. With limited bandwidth, attackers can achieve more impact and disrupt a branch or an organization's operations.

Attacking the public assets of organizations provides increased visibility, but typically these assets are better protected and harder to bring down. Public-facing assets remained an essential target throughout Q1 of 2021, as actors attempted to impact an organization's reputation or to send a political message.



Quarterly Trends

Compared to Q4 of 2020, the total attack volume in Q1 of 2021 increased by 31% while the total number of attacks decreased by 2%. The largest recorded attack in Q1 of 2021 was 295Gbps, up from 260Gbps in Q4 of 2020.

The total volume and total packets for March of 2021 were similar to levels witnessed in November of 2020. The period between December and February was characterized by larger volumes and higher amounts of packets, caused mainly by the intensity of the attacks from the second wave of the ransom DDoS campaign.

The average attack size in Q1 of 2021 was down from over 315Mbps in December to levels just below 150Mbps. December of 2020 had the lowest number of attacks over the previous six months (see blue line in Figure 1). February and March of 2021 had a great number of attacks that were smaller in volume compared to December and January.

The relative number of attacks larger than 10Gbps (see Figure 4) has a similar evolution compared to the average attack size. In March of 2021, one in every 1,000 attacks was greater than 10Gbps compared to three per 1,000 attacks in December of 2020.

FIGURE 1: *Monthly total volume and packets per month - October 2020 to March 2021*

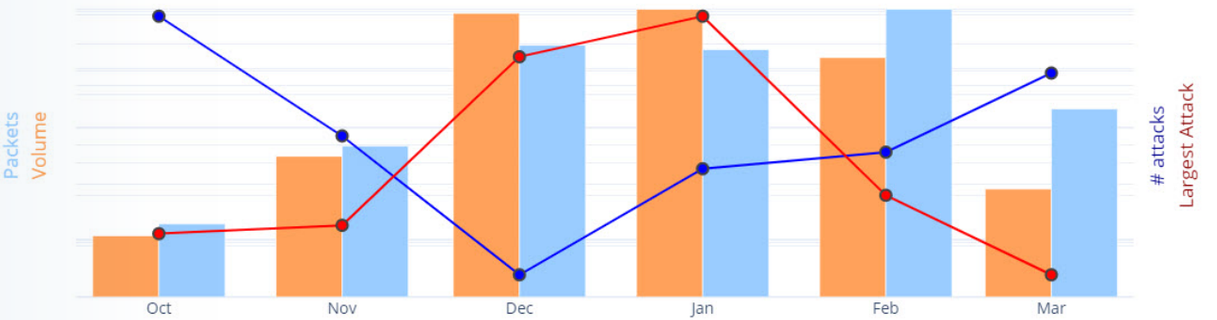


FIGURE 2: *Monthly average attack size (Mbps)*

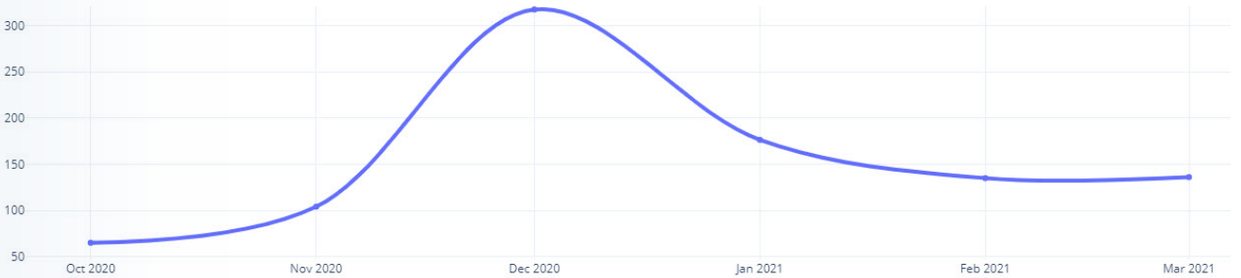


FIGURE 3: *Daily attacks and volume*

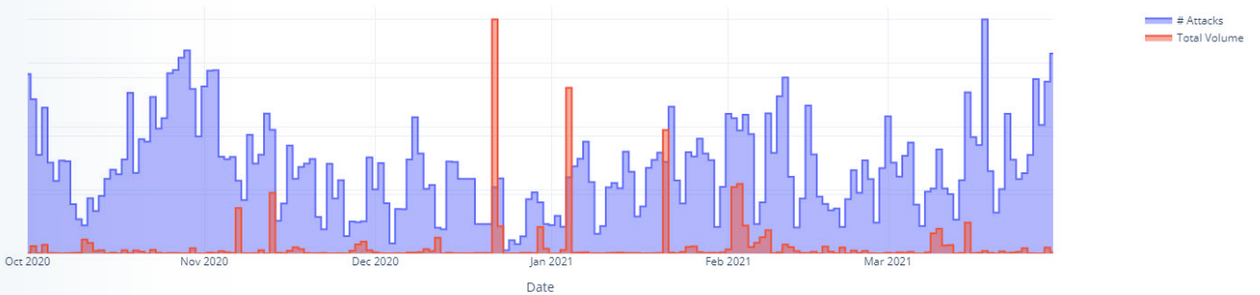
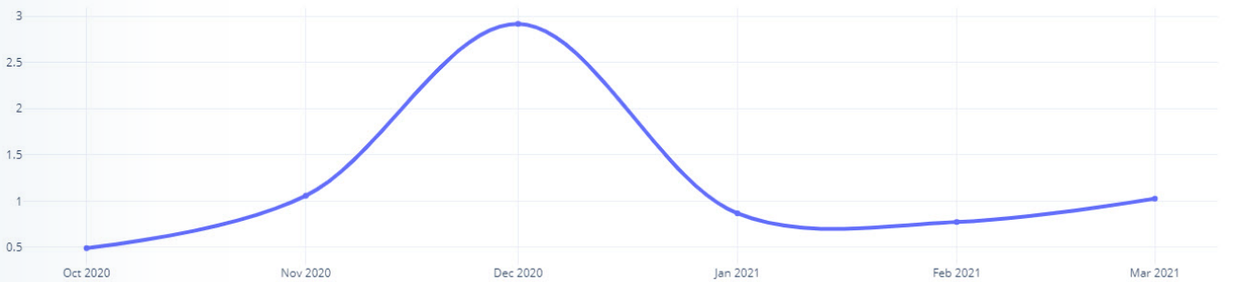


FIGURE 4: *Attacks larger than 10Gbps, normalized in part per mille of total monthly attacks*



Industries

Healthcare was dominated by biotechnology and pharmaceutical attacks in the first half of Q1 of 2021, while the activity moved to a smaller number of attacks targeting hospitals in the second half of the quarter. The public assets of large biotechnology organizations were the primary targets and resulted in the most significant attacks targeting the healthcare vertical for the quarter. Public-facing assets remained an important target for actors seeking to impact an organization's reputation or send a political message.

The government sector experienced a lower number of attacks, but higher volumes in February and March of 2021. This is in contrast to Q4 of 2020, when this sector experienced high numbers of low-volume assaults. Both periods were dominated by attacks on North American-based government institutions with fewer and smaller attacks in Europe, Asia and Latin America.

FIGURE 5a: *Attack and volume by industry for Q1 of 2021*

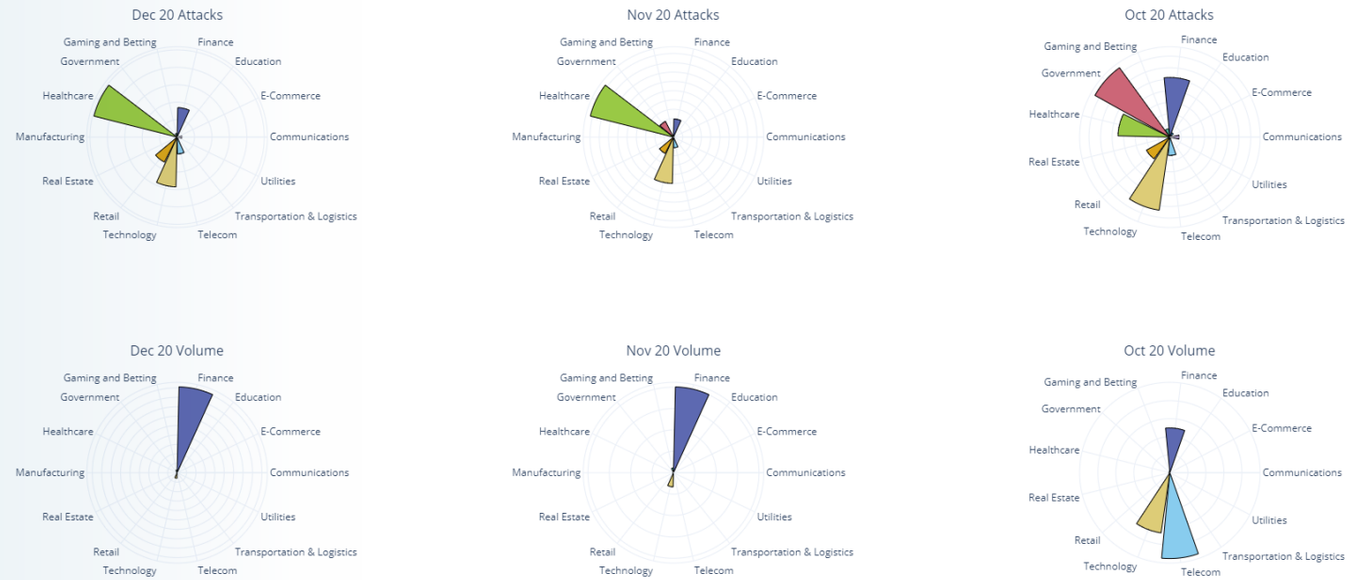


FIGURE 5b: *Attack and volume by industry for Q4 of 2020*

Industries *(continued)*

Attacks on finance changed from infrequent, high-volume attacks in December and January to smaller, more frequent global attacks in March, impacting more offices and branches of multinational organizations (see **Figure 5a, Figure 5b,** and 6).

Healthcare attacks began to slow in March, but this industry has continued to experience regular attacks since November of 2020. These attacks primarily targeted branches of international organizations (see Figure 7).

Government experienced high attack activity in October, but the largest volumes were noted in February and March (see Figure 8).

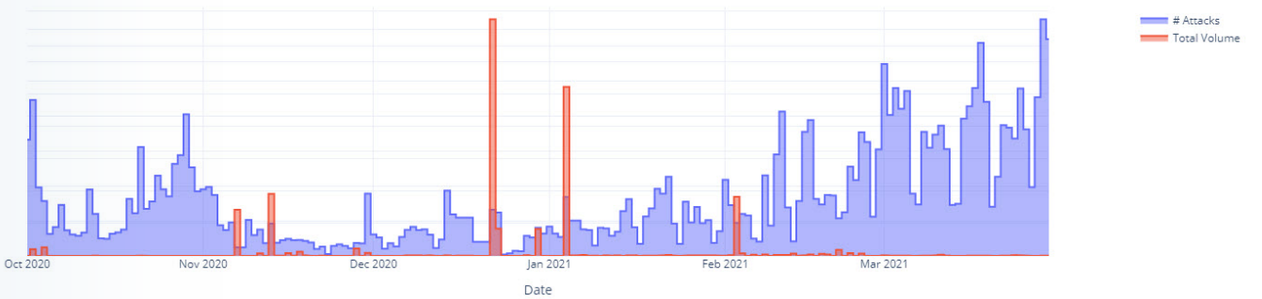


FIGURE 6: *Daily attacks and volume for finance*

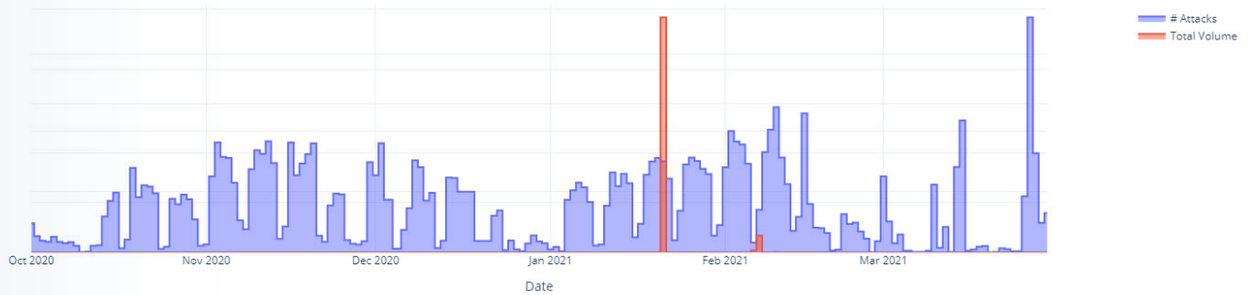


FIGURE 7: *Daily attacks and volume for healthcare*

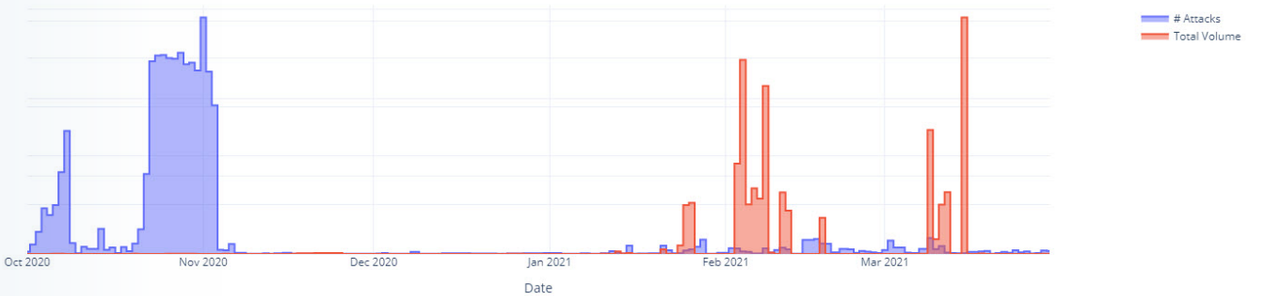


FIGURE 8: *Daily attacks and volume for government*

Attack Vectors and Applications

More than 50% of the attack volume targeted HTTPS and nearly 20% targeted HTTP. DNS and NTP represented more than 10% of attack volume. NTP primarily targeted (UDP port 123 in destination) for abuse in reflection attacks; the network suffering the NTP reflection is typically collateral damage and not the intended victim. DNS had to endure the fastest packet rate from a single attack vector at 151.36Mpbs. Other noteworthy attack vectors were Chargen, RDP, SSDP, Memcached and ARMS.

UDP Fragment and UDP Floods accounted for more than 90% of the volume in Q1 of 2021. More specific UDP amplification attack vectors such as NTP and DNS accounted for 7% of total volume while TCP out-of-state took less than one percent.

The average packet size of TCP attacks is much smaller compared to UDP attack packets. UDP Fragment attacks averaged at 1269 bytes per packet while TCP out-of-state averaged at 315 bytes. Many TCP attack vectors such as SYN-ACK, TCP Zero Seq, FIN-ACK and RST Floods average below 100 bytes per packet.

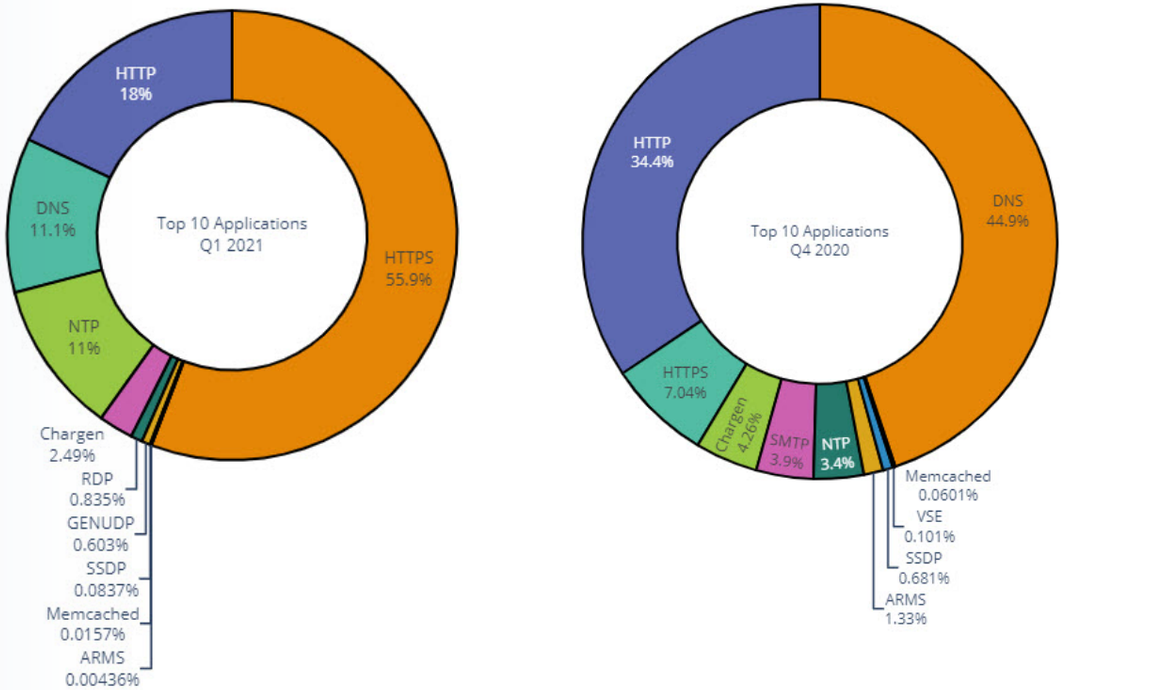


FIGURE 9: *Top 10 attack volume by application,* ***Q1 of 2021 and Q4 of 2020***

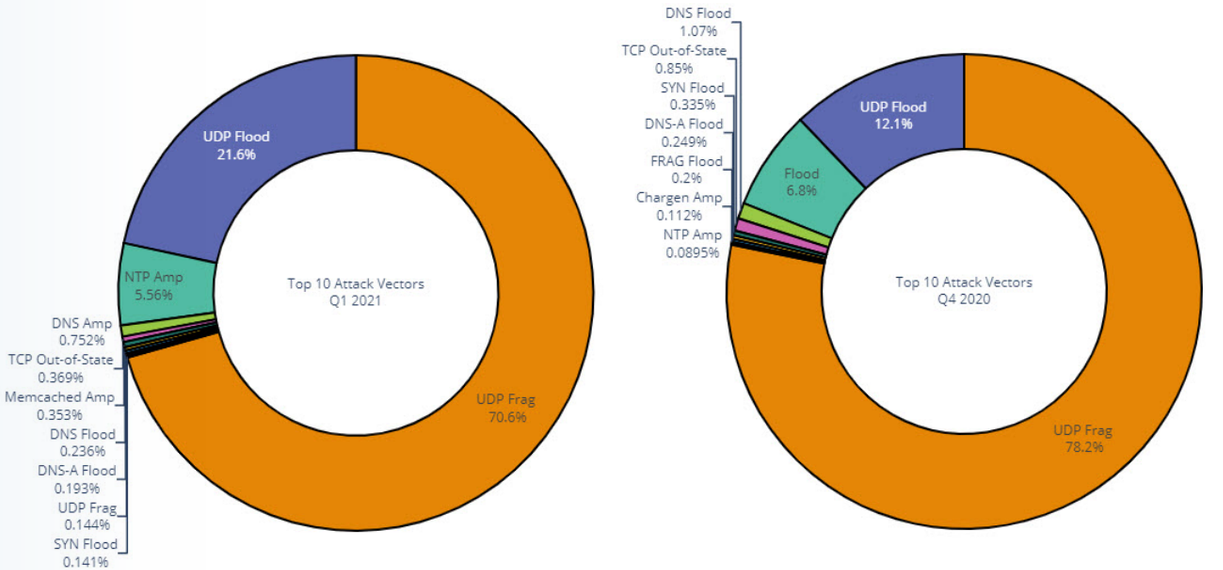


FIGURE 10: *Top 10 attack vectors by volume, Q1 of 2021 and Q4 of 2020*

Attack Vectors and Applications *(continued)*

TCP attacks typically target resource exhaustion or attempt to overrun network equipment GPUs, while UDP Floods are typically leveraged for trying to saturate internet connections. In reality, the use of attack vectors is mostly based on the availability of reflectors and amplification hosts and the most popular vectors provided by booter and stresser services.

UDP is still the most leveraged protocol for DDoS attacks, which is not surprising since UDP traffic can be easily spoofed and most of the amplification attack vectors are UDP-based. IP and TCP were more prominent in Q4 of 2020, while in Q1 of 2021, 99% of the total attack volume consisted of UDP traffic.

TOP ATTACK VECTORS: HTTPS

Attacks targeting port 443, HTTPS, were primarily UDP-based amplification attacks in Q1 of 2021.

In Q4 of 2020, the attack vectors targeting HTTPS were more diverse and equally spread with TCP- and UDP-based attacks and application-level HTTPS Connection Floods.

FIGURE 11: *Attack protocol volume, Q1 of 2021 and Q4 of 2020*

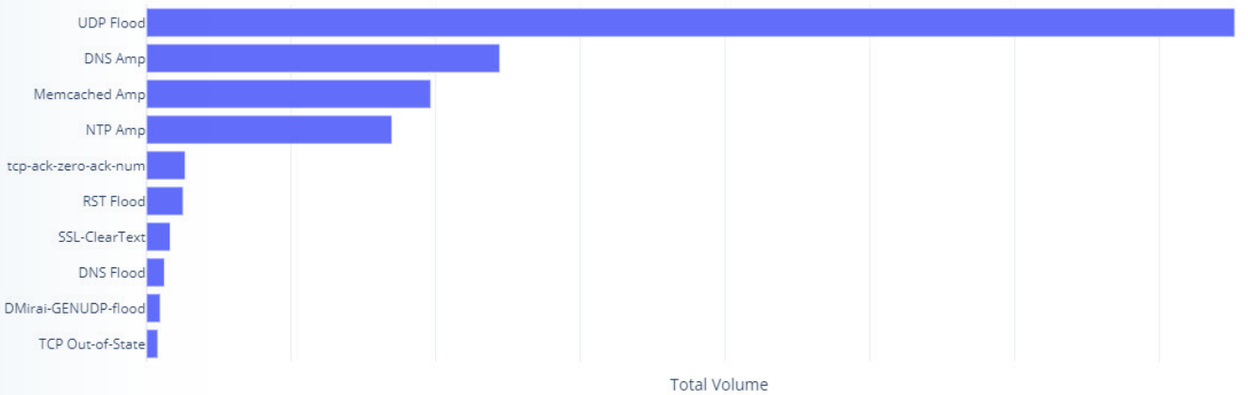


FIGURE 12: *Top 10 attack vectors targeting HTTPS in **Q1 of 2021***

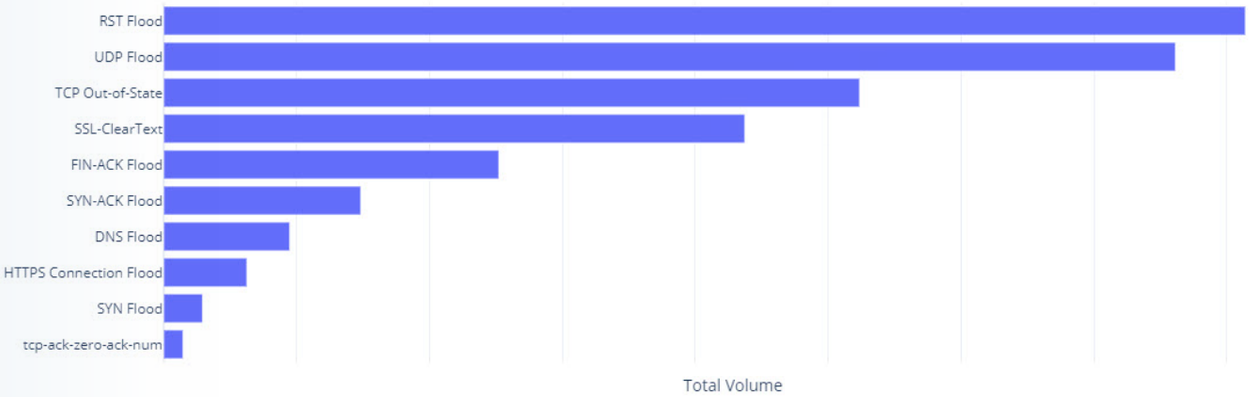


FIGURE 13: *Top 10 attack vectors targeting HTTPS in **Q4 of 2020***

Attack Vectors and Applications *(continued)*

TOP ATTACK VECTORS: HTTP

Port 80 attacks were dominated by UDP Floods, DNS Amplification and DNS Flood attack vectors in Q1 of 2021, aligning with the top 3 attack vectors of Q4 of 2020.

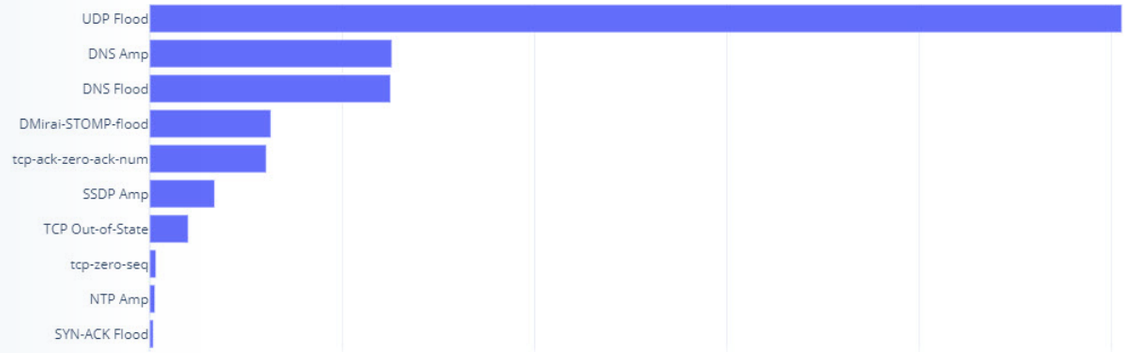


FIGURE 14: Top 10 attack vectors targeting HTTP in **Q1 of 2021**

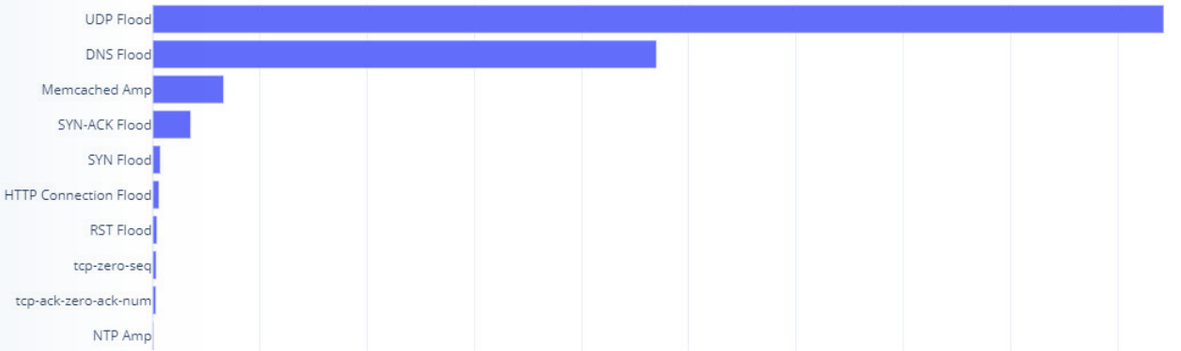


FIGURE 15: Top 10 attack vectors targeting HTTP in **Q4 of 2020**

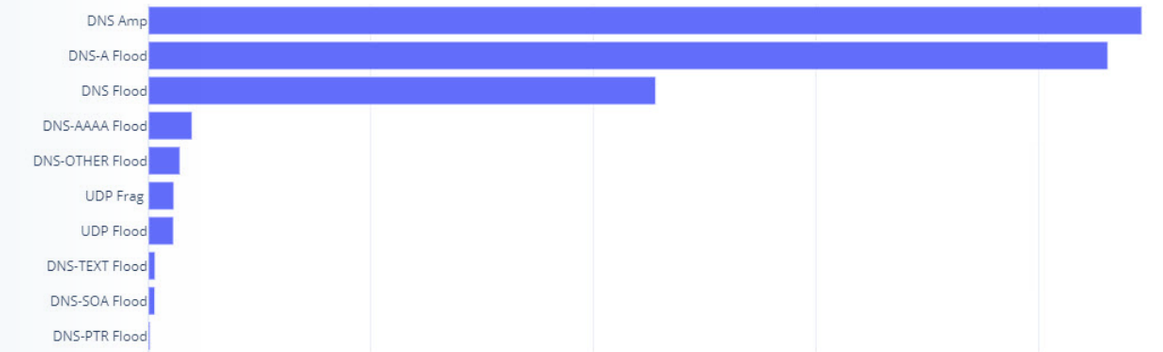


FIGURE 16: Top 10 attack vectors targeting DNS in **Q1 of 2021**

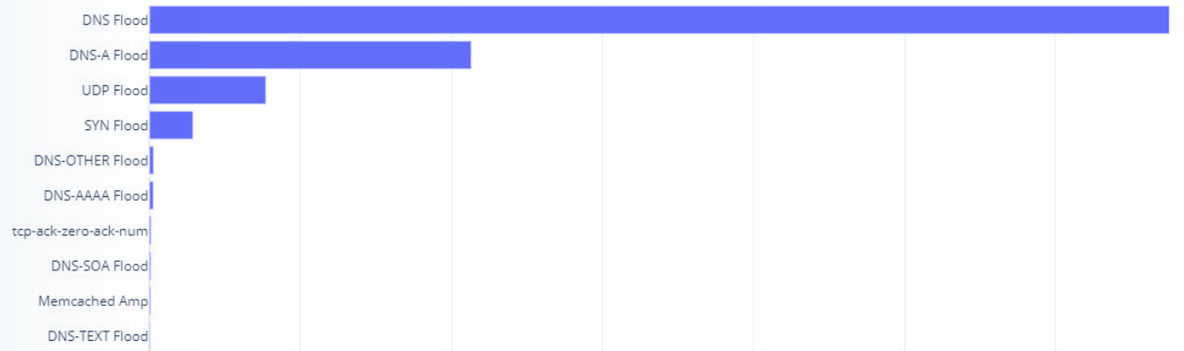


FIGURE 17: Top 10 attack vectors targeting DNS in **Q4 of 2020**

On-Premise vs. Cloud Mitigated

More than 85% of attacks were mitigated on-premise in Q1 of 2021. The 15% attacks mitigated in the cloud represent over 92% of the total volume and almost 84% of the packets.

As expected, on-premise devices will divert to the cloud when attack volumes are close to the saturation level of the internet connection. In hybrid deployments, the cloud will handle the volumetric attacks while on-premise will typically handle low-and-slow and low-volume DoS attacks, as well as anomalies and intrusions.

In conclusion, on-premise detection and mitigation will fail to prevent 15% of the attacks. If latency introduced by cloud protection is important, 85% of the attacks can be mitigated by on-premise equipment.

Intrusions made up 73% of all malicious events with the majority mitigated on-premise. The cloud scrubbing centers are responsible for mitigating 94% of DoS events.

FIGURE *18:* *Cloud versus on-premise CPE statistics for **Q1 of 2021***

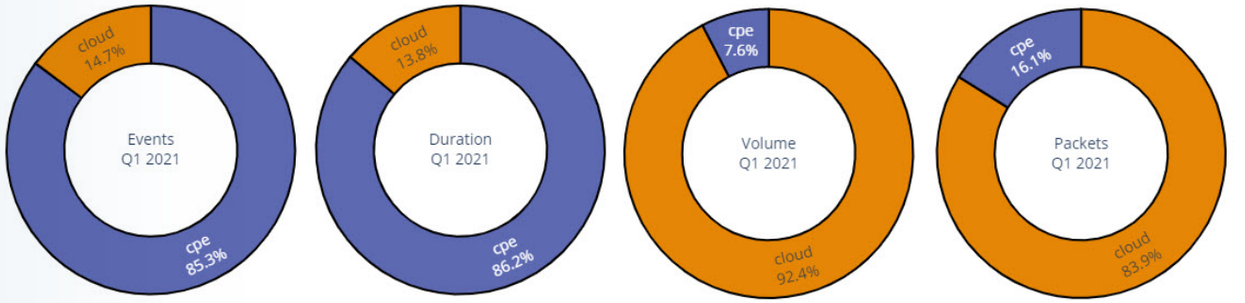


FIGURE 19: *Attack categories by origin for **Q1 of 2021***

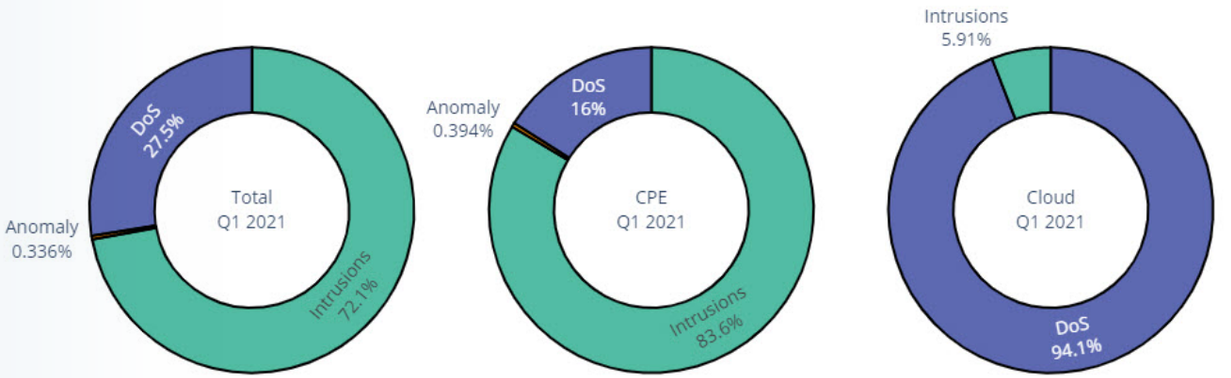


FIGURE 20: *Top overall intrusions blocked in Q1 of 2021*

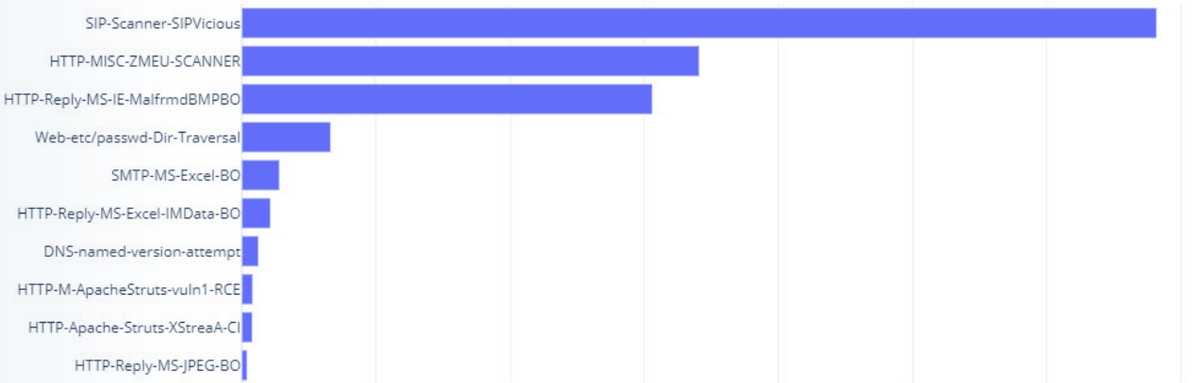
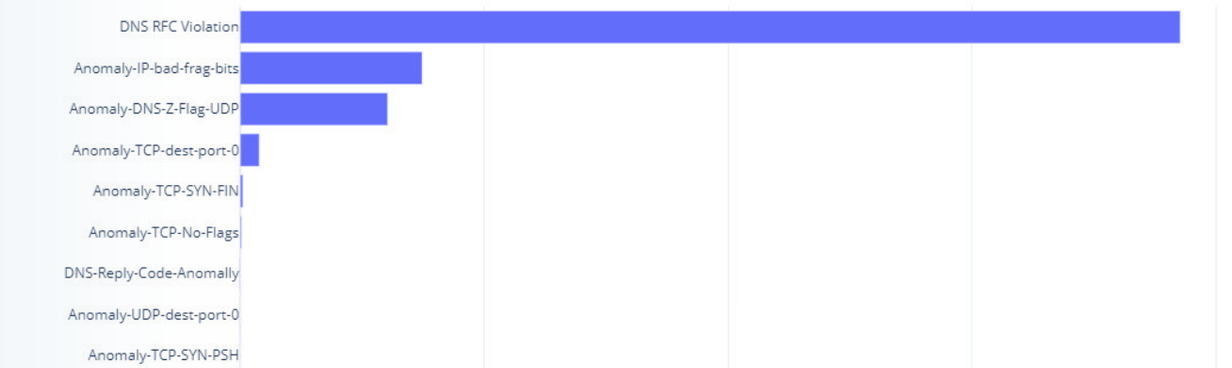


FIGURE 21: *Top overall anomalies blocked in Q1 of 2021*



Attacks Initiated During Business Hours

In October of 2020, government was the most attacked vertical, but starting in November, healthcare dominated the number of attacks until finance superseded healthcare in March of 2021 **(Figure 5)**. The attacks on healthcare were smaller in size and the median attack size ranged from a couple of Mbps up to 3Gbps.

The temporal distribution of attacks on several healthcare organizations **(Figure 9)** has a distinctive pattern with the highest concentration of attacks from Monday to Friday and a significantly lower concentration on Saturdays and Sundays. Only a few attacks were recorded during the holidays, compared to the period before and after.

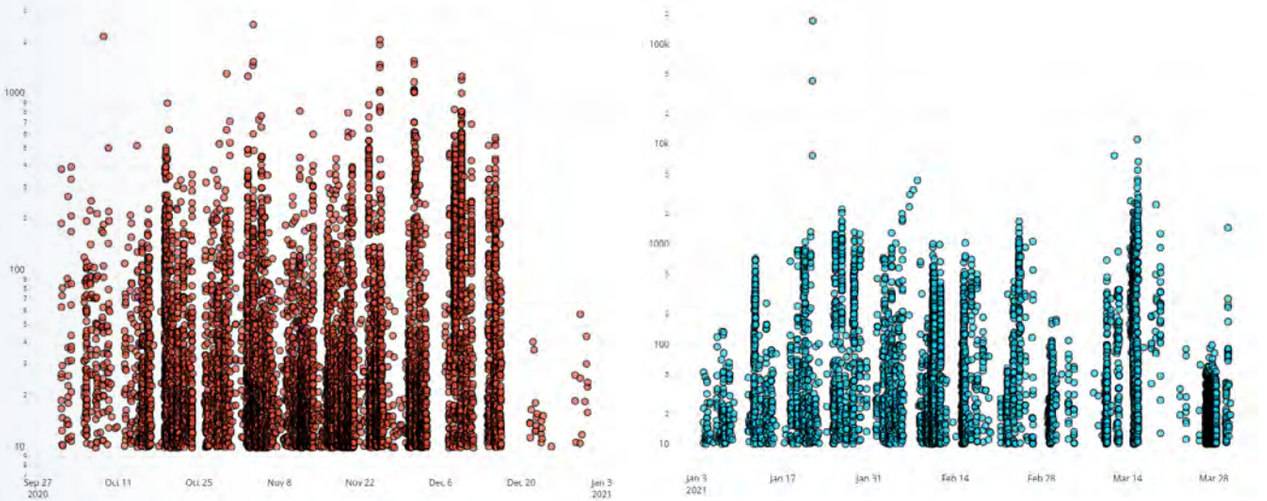


FIGURE 22: *Q4 of 2020 and Q1 of 2021 healthcare attacks larger than 10Mbps (log scale)*

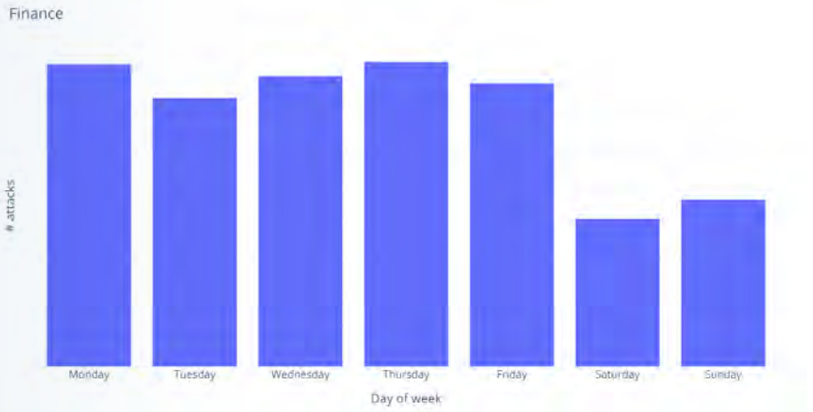


FIGURE 23: *Attacks per day of the week for finance*

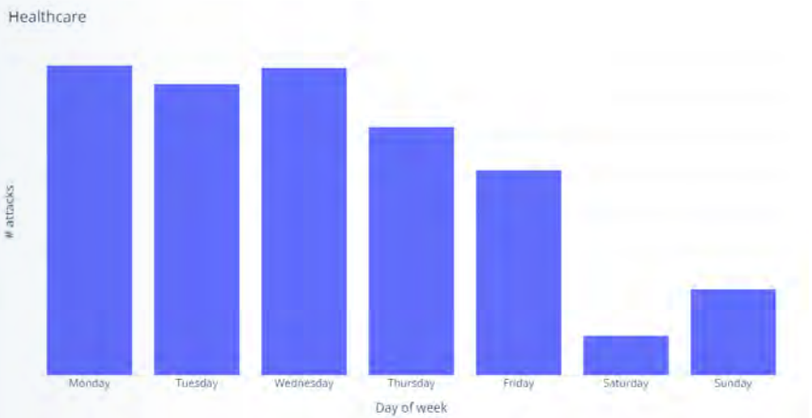


FIGURE 24: *Attacks per day of the week for healthcare*

Attacks Initiated During Business Hours *(continued)*

Several organizations in healthcare, finance and retail demonstrated similar temporal distributions and had consistently higher concentrations of attacks during weekdays across Q4 of 2020 and Q1 of 2021.

FEWER ATTACKS DURING THE NIGHT

The number of attacks initiated at night is lower than the number of attacks undertaken during office hours and is consistent across time zones.

This observation becomes more apparent, as can be seen in the charts to the right with shifted time axis using UTC for EMEA (Figure 25), UTC+7 for APAC (Figure 26) and UTC-7 for the Americas (Figure 27).

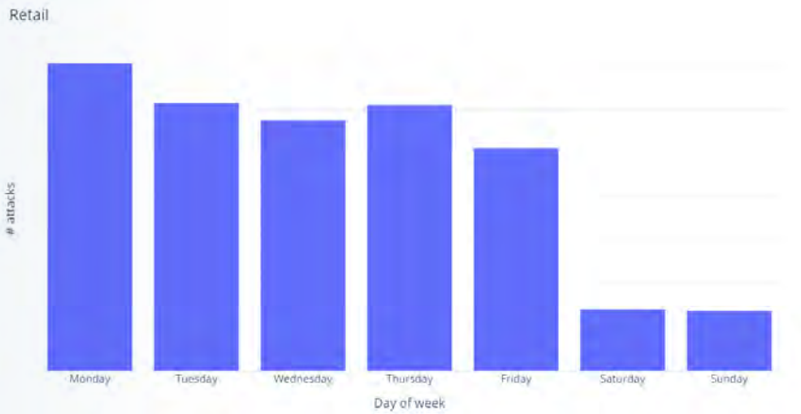


FIGURE 25: *Attacks per day of the week for retail*

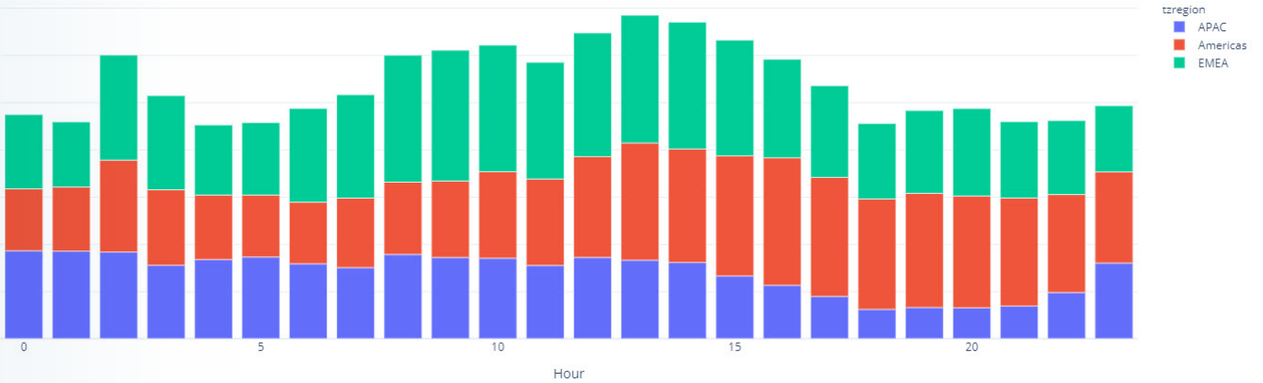


FIGURE 26: *Number of attacks based on hour of the day*

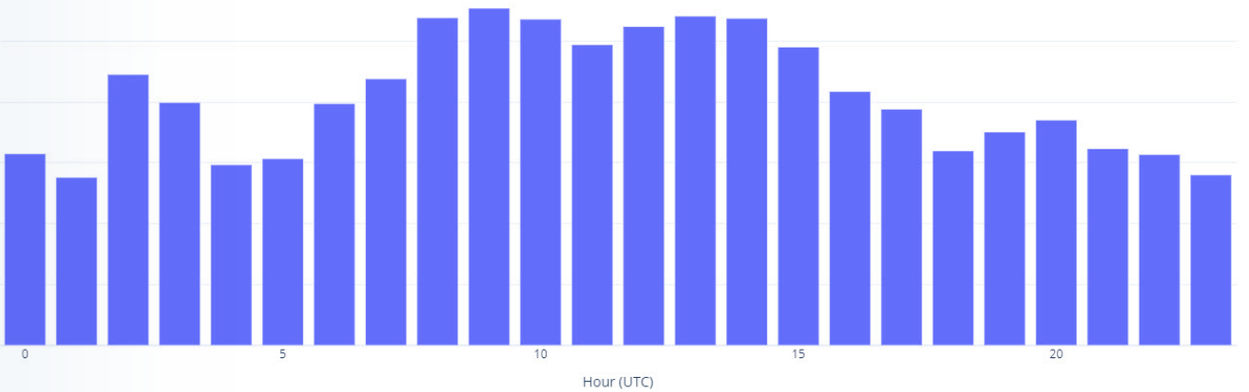


FIGURE 27: *Attacks initiated per time of the day for EMEA (UTC timescale)*

Conclusion

The first quarter of 2021 was characterized by the continuation of the 2020 ransom DDoS campaign, with high-volumetric attacks targeting the finance sector. Biotechnology and pharmaceutical continued to experience attacks, however the threat landscape shifted from fewer, high-volumetric attacks to minor attacks characterized by lower volumes.

Overall, the number of attacks held steady (down 2% from Q4 of 2020), but attack volumes increased by 31%. In fact, the occurrence of major attacks of 10Gbps or more tripled in Q1 of 2021 versus December of 2020. The largest attack in Q1 of 2021 was 295Gbps.

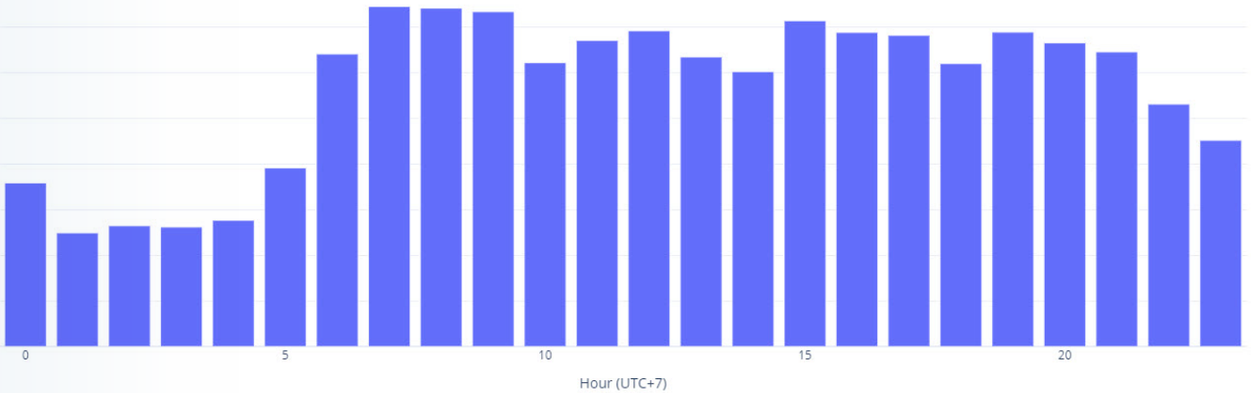


FIGURE 28: *Attacks initiated per time of the day for APAC (UTC+7 timescale)*

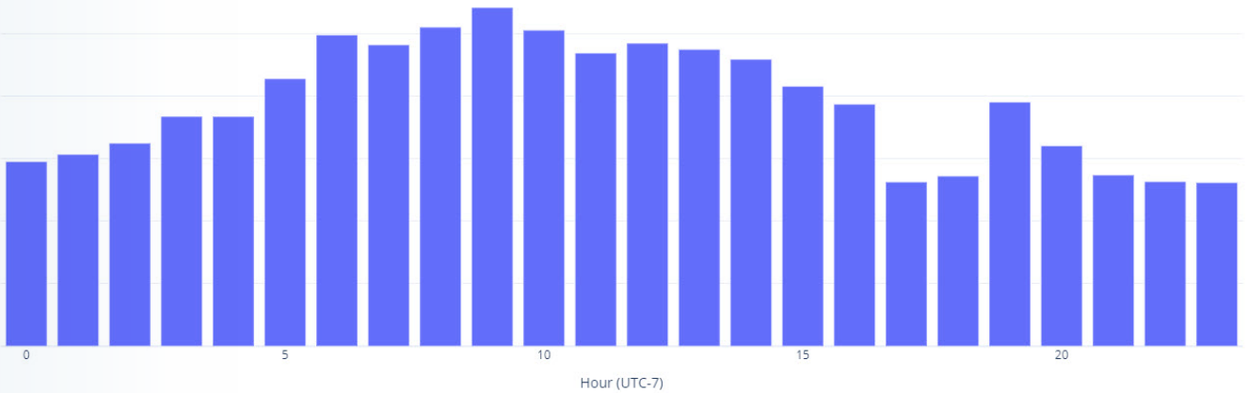


FIGURE 29: *Attacks initiated per time of the day for the Americas (UTC-7 timescale)*

References

[1] Radware, “Ransom DDoS Campaign: Circling Back,” 22 January 2021. [Online]. Available: https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/ddos-extortions-back/.

Methodology and Sources

The data for this report was collected from a sampled set of Radware devices deployed in Radware cloud scrubbing centers and on-premise managed devices in Radware hybrid and peak protection services.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware’s solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our Security Research Center that provides a comprehensive analysis of DDoS attack tools, trends and threats. This document is provided for information purposes only.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services or processes described herein are subject to change without notice.