Radware reports DDoS attacks up 31 pc in Q1 2021 vs. Q4 2020 - huge attacks triple

Radware's® DDoS Attack Report, finds that while the number of attacks held steady in Q1 (down 2% from Q4 2020, attack volumes increased by 31%.

The largest recorded attack in Q1 of 2021 was 295Gbps, up from 260Gbps in Q4 of 2020. In fact, the occurrence of major attacks of 10Gbps or more tripled in Q1 2021 vs. December 2020.

Radware's new quarterly report series, provides an overview of attack activity experienced by a sample of the data security vendor's customers during the first quarter of the calendar year 2021.

The report analyses DDoS attack activity by industries, attack vectors, DDoS attacks on applications and on-premise vs. cloud.

The report finds that in addition, while DDoS attacks have traditionally impacted public assets, damaging an organisation's reputation through public exposure, healthcare is different.

Those back-end infrastructure attacks are occurring more frequently during weekday business hours, with little activity over weekends or holiday periods. This impacted on day-to-day operations such as the connectivity to cloud-based applications by employees or the remote access for those still working from home.

Pascal Geenens, Director of Threat Intelligence for Radware, said: "The first half of Q1 was characterised 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 to benefit from the surging Bitcoin value."

Several global organisations had branches/remote offices impacted during this period, with actors leveraging new tactics to impact the productivity of organisations by targeting internet connectivity and remote access.

To overcome the pandemic, organisations began relying on remote operations, teleworking and remote access infrastructure. As a result, DDoS actors found new opportunities and began targeting the backend of the communication infrastructure of organisations. With limited bandwidth, attackers can achieve more impact and disrupt a branch or an organisation's operations.

Interrupting or affecting the performance of the remote access infrastructure had an increased impact on the organisations' productivity during the pandemic.

Attacking the public assets of organisations 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 for actors attempting to impact an organization's reputation or send a political message.

Select Industry Findings

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 organisations were the primary targets and resulted in the most significant attacks for the healthcare vertical for the quarter. 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 organisations. Government experienced high attack activity in October 2020, but the largest volumes were noted in February and March 2021.

Contacts

David Frost
(02) 7903 9567
mailto: david.frost@prdeadlines.com