COMCAST BUSINESS
Solutions
PROVIDER

2021

Comcast Business DDoS threat report

Comcast Business DDoS Mitigation Service

Special Report on Multi-vector DDoS Attacks

24,845

Total multi-vector attacks (targeting Layer 3, 4, and 7 simultaneously) experienced by Comcast Business DDoS Mitigation Service customers

About This Report

The 2021 Comcast Business DDoS Mitigation Service customer report focuses on multi-vector attacks that target Layers 3, 4, and 7 simultaneously. Although a small percentage of the overall attacks experienced by our customers, we believe the sophistication and potential damage caused by these attacks warrants a deeper look.

242 Gbps
Rate of largest attack

30D 23H 59M
Duration of longest mitigated attack

75 Mbps
Rate of average attack

607 TB
Volume of largest mitigation

4,982 TB
Total traffic scrubbed

74 TB
Total malicious traffic blocked

Key takeaways

2021 was another record year for global DDoS attacks. At 9.84 million, the number was lower than the 10.1 million attacks in 2020 but still represented a 14 percent increase over the 2019 numbers.

A few factors account for the slight decrease in global attacks from 2020 to 2021. First, 2020 was a full lockdown year where the world operated remotely, giving threat actors a unique landscape against which to launch unprecedented numbers of DDoS attacks. Second, cryptocurrency had an incredible year in 2021, creating a lucrative opportunity for threat actors to redirect their botnet resources, the ones typically used in DDoS attacks, to crypto mining activities.

The number of DDoS attacks is likely much higher than reported, as some corporations have extensive internal resources to withstand attacks without noticeable disruptions and typically don't publicly report the total number of attacks against their networks, applications, and infrastructure.

Numbers trend up for Comcast Business DDoS Mitigation Service customers

At Comcast, the total number of customers who experienced attacks in 2021 rose by 41 percent compared to 2020, and the total number of multi-vector DDoS attacks targeting Layers 3, 4, and 7 simultaneously increased by 47 percent over the same period.

> "Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."
>
> - Jürgen Stock, INTERPOL Secretary General

Comcast Business DDoS Mitigation Service customer trends

Susceptible targets

73%

Of all multi-vector attacks targeted four industries

For two years in a row, vulnerabilities during the COVID-19 pandemic made the education, finance, government, and healthcare sectors key targets.

Low-volume attacks

98%

Of all multi-vector attacks were under 5 Gbps

Bad actors often strike at low volumes to avoid detection, degrade site performance, impact availability, and map out network vulnerabilities for reconnaissance.

Hit-and-run attacks

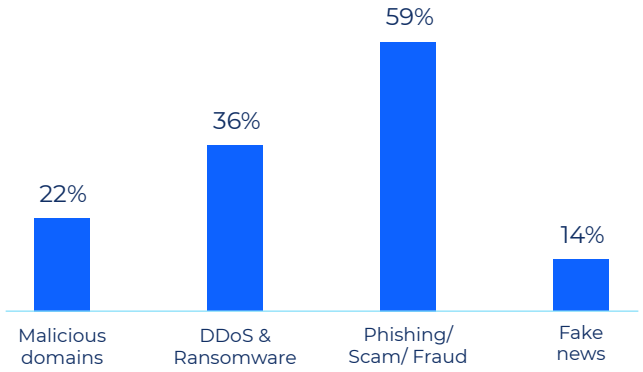
69%

Of all multi-vector attacks lasted under 10 minutes

Short duration, repeat attacks give IT organizations less time to respond, quickly overwhelming defenses and taking down attacked sites. Short duration attacks are harder to detect.

A busy year for attackers

Distribution of COVID-19 inflicted cyberthreats based on member countries feedback - Interpol 2020



COVID-19 created one of the most extensive and vulnerable threat surfaces we have seen in decades. The swiftness and magnitude of the pandemic left businesses, corporations, schools, and critical infrastructure services scrambling to maintain continuity. Overnight, students went online, offices moved home, meetings became virtual, and businesses found digital routes to customers.

The demand for connectivity exploded, and according to McKinsey, enterprises accelerated their digital transformation by an average of 4-6 years.

COVID-19 impact on the threat surface

The last two years have seen us through dramatic changes, bringing us to another new normal in 2021. Over 300 million unique users connected to the Internet for the first time, and the number of connected devices increased by 33 percent.

The average business reports that 60 percent of its workforce is now remote, significantly driving up cloud-based and collaborative technology usage. Despite nationwide school openings in 2021, 57 percent of households with school-age children continue to use some form of online learning. And because of changed shopping habits, the online retail market will top 1 trillion dollars in 2022.

A buffet of opportunities for threat actors

The very infrastructure required to support the post-COVID-19 live-work-play world is in the direct crosshairs of attackers. It's no surprise that the increase in our digital dependence directly correlates with the size, complexity, and frequency of cyberattacks, especially DDoS attacks, which reached 9.84 million worldwide in 2021.

332M
Unique new users connected to the Internet

33%
Increase in connected devices

60%
Of workforces are currently working remotely

57%
Of households are still using some form of remote learning

$1T
The expected size of the online retail market in 2022

9.84M
2021 DDoS attacks worldwide (single and multi-vector)

DDoS becomes a bigger priority

Becoming harder to fight

In a Neustar and IDG joint study of IT professionals, respondents said that DDoS attacks were the sixth most difficult attacks to defend against. Almost half find them the most prevalent threat to their organization and, 44 percent expect things to worsen in the next two years.

Evolving into a lucrative business

Although most companies don't report extortion attempts, they're on the rise and, unfortunately, here to stay. Ransomware operators are adding DDoS Extortion to their list of services as additional stressors or motivators. According to Cloudflare, 25 percent of their customers in Q4 2021 received a ransom note from attackers to stop the DDoS assault.

Death by a thousand cuts

As this year's data shows, DDoS attacks are evolving. Criminals increasingly use repeat short-duration vectors, often part of multi-vector attacks, as a misdirection tactic to distract IT teams while testing and exploiting other network vulnerabilities to steal customer data, activate malware, or install viruses.

44%

Expect the fight against DDoS attacks to get tougher in the next two years

28%

Expect DDoS attacks to be a higher priority than they are today

125%

Increase in DDoS extortion attacks from 2019-2020

76%

Of companies are targets of multiple attacks

44%

Of companies experienced malware activation during multi-tactic DDoS attacks

Multi-vector attacks are on the rise

Throughout 2021, Comcast Business DDoS Mitigation Services successfully identified and helped defend our customers from 24,845 multi-vector attacks targeting Layers 3, 4, and 7 simultaneously, a 47 percent increase over 2020. Overall, 69 percent of our customers were targets of DDoS attacks, a 41 percent increase over 2020.

The data shows that DDoS attackers were indiscriminate and persistent. Although threat actors focused heavily on a few vertical segments like education, finance, government, and healthcare, they spared no one. Everyone was fair game — from tow truck drivers to churches, utility companies, IT companies, online gambling sites, and manufacturing operations.

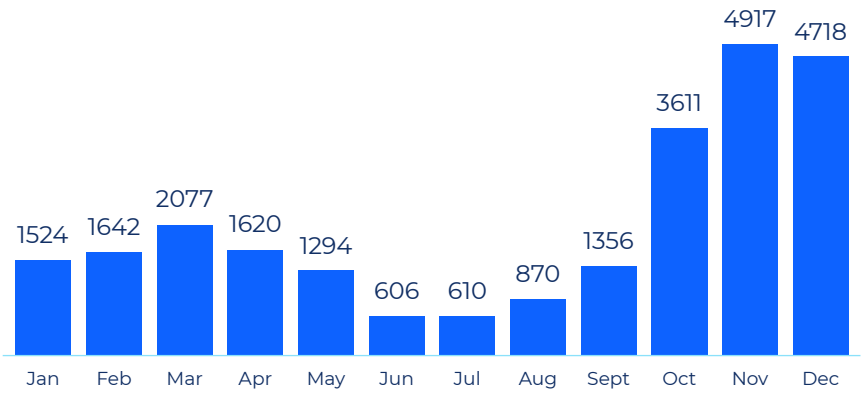
24,845 ↑ 47% YoY

Total simultaneous Layer 3, 4, and 7 multi-vector mitigations

69% ↑ 41% YoY

Of all Comcast Business DDoS Mitigation Service customers experienced attacks in 2021

Frequency of multi-vector attacks targeting Layers 3, 4, and 7 simultaneously



Multi-vector attacks by industry

The pandemic skewed industry-level DDoS attack trends significantly. According to INTERPOL, COVID-19 saw a dramatic shift in targets from individuals to governments and critical health infrastructure. But as the pandemic shifts to the next phase and we move towards recovery, threat actors will readjust their focus once again.

Verticals in the crosshairs

Going forward, experts agree that the hyper focus on COVID-19 related motivations will wane. The addition of ransomware and ransom DDoS to the threat actors' arsenal of tools will influence the next set of vulnerable targets — the financial, technology, infrastructure, and consumer goods sectors, already high on the list, will become even bigger targets. At the same time, the current favorites — healthcare and education — remain in the mix.

Attackers were indiscriminate but methodical

Even though DDoS attacks are notoriously inexpensive to launch, threat actors still want to maximize their return on investment. True to form, they used industry-specific seasonal trends and activities to guide attacks and maximize impact.

Attacks on the education customers followed the cadence of a typical school year — starting strong in January, taking a significant dip over the summer when schools were out and ramping back up in the fall.

COVID-19, school re-openings, and vaccine availability drove healthcare attacks. The first half of the year stayed low primarily due to improving COVID-19 numbers. But starting in September, customers experienced a rapid increase in attacks due to schools re-opening for in-person instruction followed by the booster vaccine rollouts. Attacks stayed steady through November and December as Omicron cases hit.

As expected, the holiday buying season with increased online transactions dictated the attack cadence of our financial customers. Overall, this sector experienced a 3X uptick in attacks during November and December compared to the rest of the year.

While attacks on other verticals fluctuated, attacks on our information technology customers grew steadily, ending the year at 10X the January numbers. We believe attacks on the information technology and finance sectors will continue to rise over the next few years, and both verticals will be highly susceptible to ransom DDoS attacks.

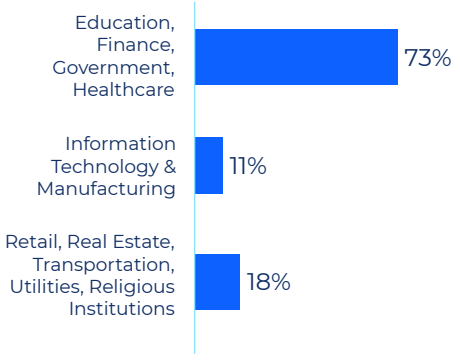
10x

Growth in multi-vector attacks on the information technology sector (between Jan - Dec 2021)

3x

Growth in multi-vector attacks on the finance sector (between Jan - Dec 2021)

Distribution of multi-vector attacks by industry



Multi-vector attacks by the numbers

55%
Of customers were victims of multi-vector attacks

15
# of attack vectors used in the largest multi-vector attack

The size and complexity of multi-vector attacks grew

Fifty-five percent of our customers were targets of multi-vector attacks, compared to 2020, where most customers experienced single vector attacks. The number of vectors deployed in a single multi-vector attack increased from 5 to 15, and the number of amplification protocols used in multi-vector attacks increased from 3 to 9.

Short, repeated assaults on customer networks and Internet properties

In line with the industry, most of our customers experienced hit-and-run attacks throughout the year. Eleven percent experienced these attacks every month of the year. Majority of the attacks lasted under 10 minutes, with a handful of outliers lasting over 50 hours (about two days).

Low-volume DDoS, the trojan horse for data breaches

Threat actors design low-volume attacks to fly under the radar of IT teams and cause damage on multiple levels. They can degrade website performance over time, and because they go largely undetected, most organizations don't even know they are victims until they start hearing complaints from their customers. Over 98 percent of all attacks on our customer base were under 500Mbps.

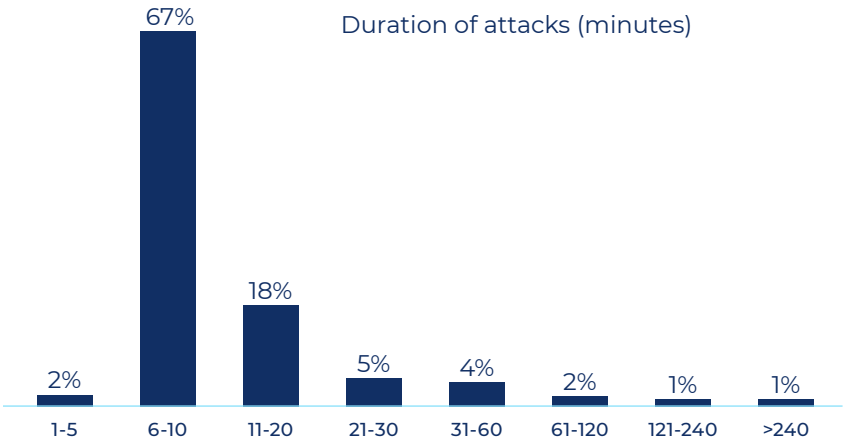
Often part of a multi-vector attack that exhausts and distracts IT resources, low-volume vectors are used with precision to map out network vulnerabilities and carry out other criminal activities like data theft or malware activation.

According to a Neustar survey of IT professionals and executives, only 28 percent of respondents felt confident in their abilities to spot small-scale attacks.

99% Of customers experienced repeat attacks

69% Of all attacks lasted for 10 minutes or less

9 Number of amplification protocols used



Layer 7 multi-vector attacks tend to use a lower volume of traffic than attacks using Layers 3-4 only. Network protocols used for DDoS attacks typically generate over 1 Gbps of malicious traffic, versus 100 Mbps or less for multi-vector attacks that include L7 protocols. However, L7 multi-vector attacks can be more destructive because they directly target application and server resources.

Summary

Multi-vector attacks grew 47 percent

During 2021 we vigilantly monitored activities across all our Comcast DDoS Mitigation Service customers to identify and mitigate 24,845 multi-vector DDoS attacks targeting Layers 3, 4, and 7 simultaneously. The number represented a 47 percent growth YoY.

The number of customers attacked grew 41 percent

Overall, 69 percent of our customers experienced DDoS attacks, a 41 percent growth over 2020. The largest and most severe attack was delivered at a rate of 242 Gbps. Any attack delivered at that rate would, within minutes, saturate even high bandwidth Ethernet Dedicated Internet (EDI) circuits. Education, Finance, Healthcare, and Government sectors were the most targeted in 2021.

Multi-level, multi-vector attacks are increasing in frequency

Fifty-five percent of all customers experienced multi-vector attacks targeting Layers 3, 4, and 7 simultaneously, and the number of vectors deployed in a single multi-vector attack increased from 5 to 15. The amplification protocols used in multi-vector attacks increased from 3 to 9.

Comcast Business DDoS Mitigation Service provided real-time detection of high and low-volume attacks

A cloud-based scalable offering, Comcast DDoS Mitigation Services provided real-time detection of volumetric or flood, State/TCP Exhaustion, and Application Layer attacks on Comcast Business EDI circuits. The services mitigated attacks within seconds of detection, providing our customers comprehensive defense against high-volume DDoS attacks that targeted bandwidth, “low and slow” attacks that targeted applications and infrastructure, and concurrent, multi-vector attacks.

Our geographically distributed high-performance, high-capacity scrubbing centers allowed us to route a total of 4,982 TB of customer traffic to the center closest to the impacted customers, minimizing network latency and maximizing redundancy. We kept threat actors and 74 TB of malicious traffic from impacting the bandwidth of our customers’ networks, disrupting their services, or worse, breaching their perimeters to commit secondary attacks.

01: Detect

Detects the DDoS attack fingerprint

02: Drop

Drops or Rate Limits Layer 3 and Layer 4 malicious traffic at the peering edge

03: Divert

Route Layer 7 traffic to Multivendor Scrubbing Centers

04: Deliver

Clean traffic is delivered to the customer

Final thoughts

> “Unlike other cyber-attacks that can be blocked with patches or security appliances, the defense calculus for a DDoS attack is different because no organization can prevent or block all DDoS attacks on its own.”
>
> - Rajpreet Kaur, Gartner Senior Analyst

DDoS attacks, when they occur, can be costly and organizations have a lot to lose. Anyone can launch one for as little as the price of a cup of coffee. A few hundred dollars can bring massive networks to their knees, prevent businesses from reaching customers or meeting SLAs, cause devastating financial and reputational damage, and in some cases, force businesses to close their doors.

Measuring risk

How do you determine if you are at risk or, more importantly, willing to take the risk and shoulder the costs?

Cost depends on the target's business and the level and duration of disruption it suffers. Heavily trafficked sites like gaming, web hosting, and e-commerce sites whose livelihoods depend on availability can potentially lose hundreds of thousands, if not millions of dollars, for every minute of downtime. Schools and first responders have critical civic and community missions to fulfill. If you think about the risk and cost of reputational damage or lost opportunity, that becomes a little harder to measure.

Some don't think about the risk and cost because they don't believe they fit the profile of a victim. They may be too small or not have a significant online presence. Or they may simply weigh the residual risk of DDoS and rank it lower against stolen credentials and malware.

Consider the following before you dismiss the threat of DDoS or feel you can weather the risk.

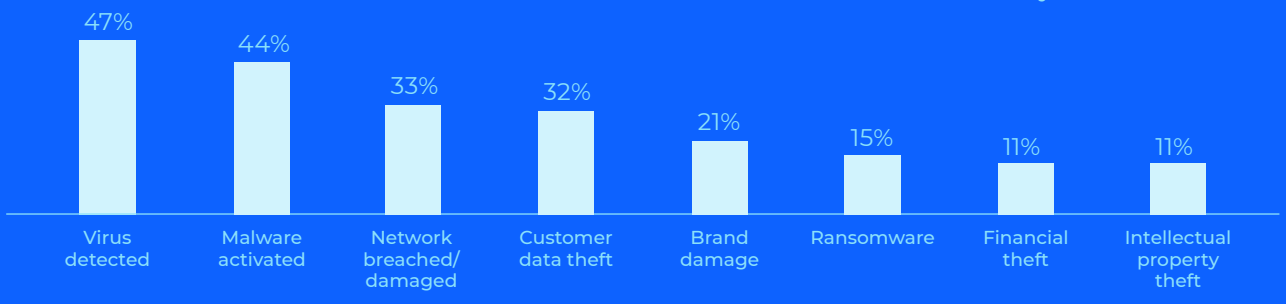
There is no such thing as islands of cyberattacks. Threat actors constantly combine strategies for maximum impact against easy, unprotected targets. They may launch repeated short burst attacks or a significant multi-vector attack to distract or consume the resources of an IT organization. And while the organization is at capacity defending itself, threat actors may use several small-volume attacks to map out network vulnerabilities for follow-on data breaches.

Evidence supports a direct link between DDoS attacks and security breaches. Forty-seven percent of respondents in a Neustar survey detected viruses on their networks after a DDoS attack, and 11 percent reported financial theft.

Even if you are a small business and think you are at a lower risk, you could be in the supply chain for a larger organization. You can be sure that your business partners are watching their threat risk factors and are increasingly concerned about doing business with companies that are not.

With threat actors constantly innovating, organizations must stay vigilant to protect their infrastructure from bad actors determined to cause financial and reputational damage.

Data breach or theft suffered as a result of a DDoS attack - Neustar survey



References

- https://datareportal.com/reports/6-in-10-people-around-the-world-now-use-the-internet
- https://www.businessinsider.com/ecommerce-sales-first-trillion-dollar-year-2022-covid-pandemic-adobe-2021-3
- https://www.bleepingcomputer.com/news/security/extortion-ddos-attacks-grow-stronger-and-more-common/
- https://www.netscout.com/threatreport/
- https://www.cdn.neustar/resources/whitepapers/security/neustar-cyber-threats-trends-2020-report.pdf
- https://www.nisc.neustar/nisc-survey-results/
- https://www.hiscox.co.uk/cyberreadiness
- https://www.itu.int/en/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx
- https://data.census.gov/cedsci/
- https://www.accenture.com/us-en/insights/security/cost-cybercrime-study
- https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/
- https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf
- https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
- https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

COMCAST BUSINESS
Solutions
PROVIDER