

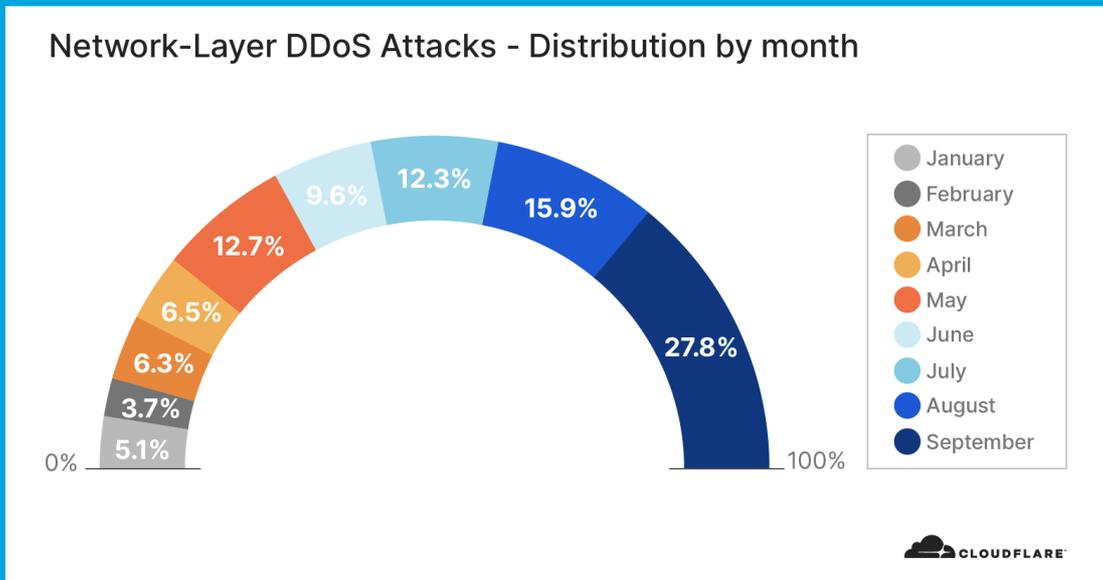


Security Newsletter

23 November 2020

[Subscribe to this newsletter](#)

Network-layer DDoS attack trends for Q3 2020



DDoS attacks are surging – both in frequency and sophistication. After doubling from Q1 to Q2, the total number of network layer attacks observed in Q3 doubled again – resulting in a 4x increase in number compared to the pre-COVID levels in the first quarter.

Here are other key network layer DDoS trends we observed in Q3:

- Majority of the attacks are under 500 Mbps and 1 Mpps – both still suffice to cause service disruptions
- We continue to see a majority of attacks be under 1 hr in duration
- Ransom-driven DDoS attacks (RDDoS) are on the rise as groups claiming to be Fancy Bear, Cozy Bear and the Lazarus Group extort organizations around the world. As of this writing, the ransom campaign is still ongoing. See a special note on this below.

Short burst attacks may attempt to cause damage without being detected by DDoS detection systems. DDoS services that rely on manual analysis and mitigation may prove to be useless against these types of attacks because they are over before the analyst even identifies the attack traffic. Alternatively, the use of short attacks may be used to probe the cyber defenses of the target. In other cases, attackers generate small DDoS attacks as proof and warning to the target organization of the attacker's ability to cause real damage later on. It's often followed by a ransom note to the target organization, demanding payment so as to avoid suffering an attack that could more thoroughly cripple network infrastructure. Whatever their motivation, DDoS attacks of any size or duration are not going away anytime soon. Even short DDoS attacks cause harm, and having an automated real-time defense mechanism in place is critical for any online business.

[Read More on Cloudflare Blog](#)

Cisco Webex bugs allow attackers to join meetings as ghost users



Now patched by Cisco, three flaws in Webex would have given intruders full access to a meeting without being seen, says IBM. When successfully exploited, IBM researchers said that the bugs would have allowed attackers to: Join a Webex meeting as a ghost without being seen on the participant list with full access to audio, video, chat, and screen sharing capabilities (CVE-2020-3419) Stay in a Webex meeting as a ghost after being expelled from it, maintaining audio connection (CVE-2020-3471) Gain access to information on meeting attendees – including full names, email addresses, and IP addresses – from the meeting room lobby, even without being admitted to the call (CVE-2020-3441)

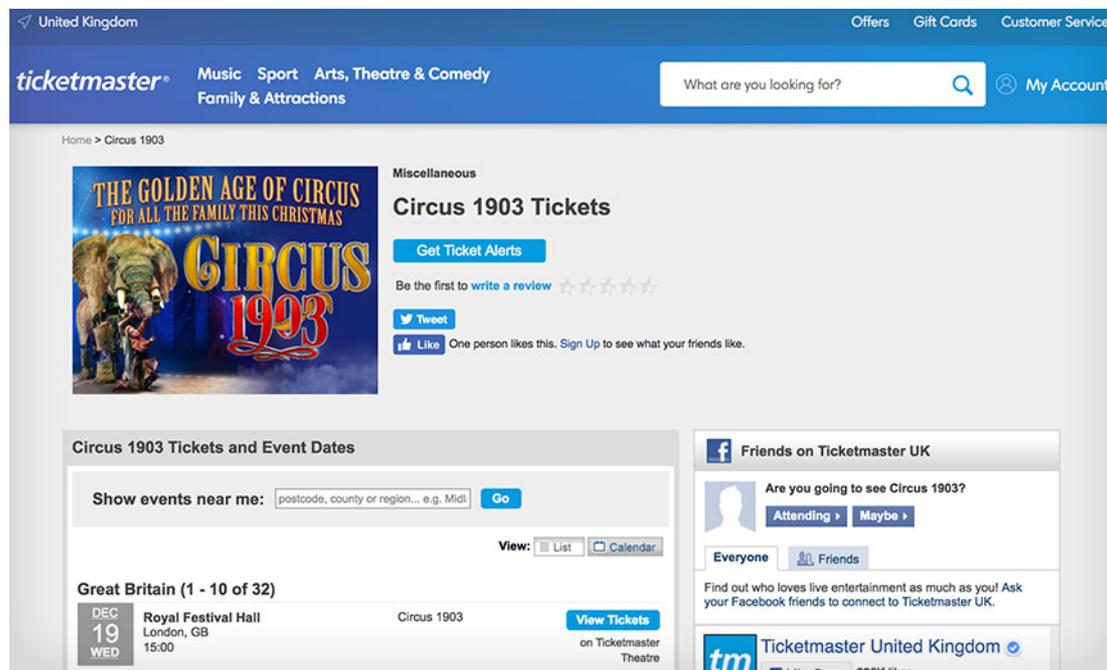
The researchers were able to successfully demonstrate attacks abusing these Webex bugs on Windows, macOS, and the iOS version of Webex Meetings applications and Webex Room Kit appliance. Mitigating circumstances include the fact that the vulnerabilities can only be exploited if attackers know the URLs of scheduled Webex meetings with unique meeting URLs and Webex Personal Rooms. However, IBM researchers say that "personal rooms may be easier to exploit because they are often based on a predictable combination of the room owner's name and organization name."

Cisco has patched the cloud-based services for Webex, where no user action is required. For customers who run an on premises version of Webex software, the company has issued patches for Webex Meetings Server. Webex users should view the following Common Vulnerabilities and Exposures (CVEs): CVE-2020-3441; CVE-2020-3471; CVE-2020-3419.

[Read More on ZDNet](#)

[Even More on BleepingComputer](#)

Ticketmaster Fined \$1.7 Million for Data Security Failures

A screenshot of the Ticketmaster UK website. The top navigation bar includes 'United Kingdom', 'Offers', 'Gift Cards', and 'Customer Service'. The main header features the Ticketmaster logo, categories like 'Music', 'Sport', 'Arts, Theatre & Comedy', and 'Family & Attractions', a search bar, and a 'My Account' link. The main content area is for 'Circus 1903' tickets, featuring a promotional image with the text 'THE GOLDEN AGE OF CIRCUS FOR ALL THE FAMILY THIS CHRISTMAS' and 'CIRCUS 1903'. Below the image are buttons for 'Get Ticket Alerts', 'Be the first to write a review', 'Tweet', and 'Like'. A section titled 'Circus 1903 Tickets and Event Dates' includes a search bar for 'Show events near me:' and a 'View Tickets' button. A table lists an event on 'DEC 19 WED' at 'Royal Festival Hall, London, GB' at '15:00'. A Facebook widget on the right asks 'Are you going to see Circus 1903?' with 'Attending' and 'Maybe' options.

Ticketmaster UK has been fined 1.25 million pounds (\$1.7 million) by Britain's privacy watchdog for its "serious failure" to comply with the EU's General Data Protection Regulation. Regulators say the company failed to properly secure chatbot software that it opted to run on a payments page, which attackers subverted, allowing them to steal payment card information. After being alerted to suspected card fraud that traced to its site, Ticketmaster UK allegedly failed to mitigate the problem for nine more weeks.

Ticketmaster UK says it plans to appeal the ruling. The company is a subsidiary of ticket sales and distribution giant Ticketmaster, owned by Live Nation Entertainment, which is based in Beverly Hills, California. The ICO, which launched its investigation in June 2018, says the fine only applies to Ticketmaster's failures following GDPR going into full effect in May 2018. As the investigation concluded before the U.K. left the EU, the ICO says it served as the lead supervisory authority for the EU and that the penalty represents a consensus decision by all data protection authorities across Europe.

The fine announced by the ICO traces to a breach that began in February 2018. Ultimately, the breach exposed personal details - including names, payment card numbers, expiration dates and CVV numbers - for approximately 9.4 million European Ticketmaster customers, including 1.5 million in the U.K. At least 60,000 Barclays Bank cards have been tied to known fraud, the ICO says, while Monzo Bank replaced 6,000 cards after it detected signs of fraudulent use. Security experts say the breach appears to have been tied to groups of attackers - collectively known as Magecart - that implant code on websites that allows them to steal payment card data.

[Read More on BankInfoSecurity](#)

- [Be Very Sparing in Allowing Site Notifications](#)
- [Facebook Messenger bug could have allowed hackers to spy on users](#)
- [Modernize secure access for your on-premises resources with Zero Trust](#)
- [German Court Slashes a GDPR Privacy Fine by 90%](#)
- [Microsoft rolls out protection for critical accounts in Office 365](#)
- [Starting next year, Chrome extensions will show what data they collect from users](#)
- [66% of companies say it would take 5 or more days to fully recover from a ransomware attack ransom not paid](#)
- [Apple Lets Some of its Big Sur macOS Apps Bypass Firewall and VPNs](#)
- [Blockchain for Voting: A Warning From MIT](#)
- [Firefox 83 boosts security with HTTPS-Only mode, zero-day fix](#)
- [Meet the hackers who earn millions for saving the web, one bug at a time](#)
- [The ransomware landscape is more crowded than you think](#)
- [Microsoft says three APTs have targeted seven COVID-19 vaccine makers](#)

#Breach Log

- [Gaming Company Capcom Confirms Ragnar Locker Ransomware Attack](#)
- [Coil payments platform leaks user emails in 'Privacy Policy' update](#)
- [Cold storage giant Americold hit by cyberattack, services impacted](#)
- [Data of 27 Million Texas Drivers Compromised in Breach](#)
- [Hacker shares 3.2 million Pluto TV accounts for free on forum](#)
- [Biotech research firm Miltenyi Biotec hit by ransomware, data leaked](#)
- [Hacker steals \\$2 million from cryptocurrency service Akropolis](#)
- [Tabcorp's IT staff put on notice days before major outage](#)

#Patch Time!

- [Researcher Discloses Critical RCE Flaws In Cisco Security Manager](#)
- [macOS Big Sur 11.0.1 Patches 60 Vulnerabilities](#)
- [Heartbleed, BlueKeep and other vulnerabilities that didn't disappear just because we don't talk about them anymore](#)

#Tech and #Tools

- [Pod Security Policies Are Being Deprecated in Kubernetes](#)
- [Inside the Cit0Day Breach Collection](#)
- [Anchoring Trust: A Hardware Secure Boot Story](#)
- [SAD DNS Explained](#)
- [AWS Flaw Allows Attackers to Find Users' Access Codes](#)
- [Multi-account AWS Organizations best practices for Financial Services](#)
- [Phonerator – An advanced valid phone number generator](#)
- [Assetnote Wordlists: wordlists for content and subdomain discovery](#)
- [Looking in Among Us](#)

- [Hacking in Among Us](#)
- [Google Cloud Service Accounts Security Best Practices](#)
- [Can't open apps on macos: an ocsf disaster waiting to happen](#)
- [Developing secure software: how to implement the OWASP top 10 Proactive Controls](#)
- [Ransomware-as-a-service: The pandemic within a pandemic](#)
- [Velociraptor DFIR tool tutorial](#)
- [Measuring Security: An OWASP Panel](#)
- [Azure Sentinel Repository](#)
- [Hunting for Malicious Packages on PyPI](#)
- [Purgalicious VBA: Macro Obfuscation With VBA Purging](#)
- [Privileged Container Escape - Control Groups release_agent](#)

This content was created by [Kindred Group Security](#). Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at <https://news.infosecgur.us>