A DDoS, or distributed denial of service attack is when bad actors attempt to ‘take down’ an internet service by overwhelming the service’s infrastructure, or related services infrastructure with a sudden flood of internet traffic. This increase in traffic greatly increases the load on infrastructure, and results in great slowdowns, or with the service going down temporarily. One of the main reasons that DDoS attacks can be so problematic is because the attacking devices are often legitimate user’s devices that have been previously been taken over by malware. This is a large problem because these devices are nearly impossible to distinguish from legitimate traffic. According to Cloudflare, there are several symptoms of DDoS attacks, like a service becoming suddenly very slow. Other signs include suspicious amounts of activity coming from one or several nearby IP addresses. Another telltale sign would be many users who have the same device type, geolocation, web browser version, or other identifying characteristics. It is not uncommon for attackers to target a single page, or cause odd traffic patterns like large spikes at specific intervals. Cloudflare further elaborates on the different targets of DDoS attacks, and breaks them down according to the OSI model. According to this model, the most common layers that attackers target are the application layer. Other methods include protocol attacks and volumetric attacks. In application layer attacks, the attackers target the OSI layer where web pages are generated on the server. This is relatively fast and resource light for attackers, but can bring a web server to its knees. HTTP floods are another similar technique, that involves essentially repeatedly refreshing a webpage on many devices at once, which floods the server, and leads to denial of service. In terms of volumetric attacks, the main idea is to create congestion by eating up all the resources between the target service and the Internet. The botnet that attackers create requires cybercriminals to install the required DDoS tools onto your system, which means that they have to trick people. Some of the common ways that Malwarebytes mentions include malicious email attachments, or social network/messaging app attachments that include links that lead to malware downloads. One of the most effective ways that attackers have developed are “Drive-by downloads” or “click scams”, where victims are surfing a legitimate website that has been compromised by attackers. These compromised sites can download malware onto end user devices even without any user input, which makes it particularly effective. Click scams are also effective, because they work by tricking users into clicking on links to malware or other malicious sites by prompting them that they have an update, or that they have detected malware. An interesting method that attackers have also developed is the HTTP slow POST DoS attack, where many requests are sent very slowly. These slowly sent requests are valid ones, but the main idea is to use up connection resources rather than computational resources. Servers will wait for the entire HTTP POST header to be sent, meaning that all the incoming connections would be unavailable. These attacks are particularly dangerous because they can circumvent certain protection systems. The classic standard technique is the Nuke attack, which involves, sending invalid or modified ICMP packets with a ping utility to repeatedly send corrupt data. This corrupted data would slow down target computers until they were unusable. According to both Malwarebytes and Cloudflare, the main reasons that attackers attempt to bring down websites are to make political statements, or hold a commercial website hostage until they receive a ransom payment. Other reasons include competing websites attempting to bring down their competitors. These attacks can also be part of larger attacks and can be designed to distract administrators from a separate malware attack. According to darkreading.com, in the first quarter of 2022, there was a 46% increase in DDos attacks over the previous quarter, which has been attributed to hackers who have been disrupting Russian state interests after the invasion of Ukraine. According to the report, DDoS attacks have become more frequent, and have grown to be approximately 80 times as long as previously recorded during the end of 2021. Some of these attacks have lasted as long as several weeks, leading experts to believe that the attacks have been made with the intention of sending a message to Russia.

References

*Attention required!* (n.d.). Cloudflare - The Web Performance & Security Company | Cloudflare. <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>

*DDoS*. (n.d.). Malwarebytes Cybersecurity for Home and Business | Malwarebytes. <https://www.malwarebytes.com/ddos>

*Denial-of-service attack*. (2002, February 25). Wikipedia, the free encyclopedia. Retrieved May 3, 2022, from <https://en.wikipedia.org/wiki/Denial-of-service_attack>

Staff, D. R. (2022, April 25). *Ukraine invasion driving DDoS attacks to all-time highs*. Dark Reading. <https://www.darkreading.com/attacks-breaches/ukraine-invasion-driving-ddos-attacks-to-all-time-highs>