BLOG

Five Most Famous DDoS Attacks and Then Some

A10 Staff | January 21, 2022

Updated: May 30, 2024

Distributed denial of service (DDoS) attacks are now everyday occurrences. Whether a small non-profit or a huge multinational conglomerate, the online services of the organization—email, websites, anything that faces the internet—can be slowed or completely stopped by a DDoS attack. For data center, colocation, hosting and other service providers, DDoS attacks threaten the infrastructure that provides network and service availability to all its tenants, subscribers and customers, and can target the most valuable customers.

A successful DDoS attack can seriously damage brand reputation and cost hundreds of thousands or even millions of dollars in revenue. Moreover, DDoS attacks are sometimes used to distract cybersecurity operations while other criminal activity, such as data theft or network infiltration, is underway.

Geopolitical events, such as the ongoing war in Ukraine, have demonstrated the efficacy of both state-sponsored and grass roots cybercriminals in launching politically motivated DDoS attacks against critical infrastructure and government agencies. Through A10 Defend Threat Control, our proprietary DDoS-specific intelligence platform, we've witnessed significant and sustained attacks across the globe on various networks and internet assets.

The number of active DDoS weapons has hovered around 15.1 million for the past several years. Further insights gained via Threat Control can be seen in the 2024 DDoS Weapons Report.

DDoS Attacks Getting Bigger, More Frequent

The online threat landscape continues to evolve at an accelerating pace with hackers launching more distributed denial of service attacks than ever before, taking aim at new targets, and creating new botnets. The demand for solutions for a wide range of business needs and the rollout of 5G technologies has accelerated the proliferation of Internet of Things (IoT) around the world, creating a huge pool of unsuspecting and under protected new recruits for botnet armies used to launch attacks on massive scales.

DDoS attacks are expected to continue to increase in number and complexity as botnets and inexpensive DDoS-as-a-service platforms proliferate.

Related Resources

Is Implementing AI Complex? What Enterprise Leaders Should Know

The Importance of DDoS Threat Intelligence and Collaborative Data Sharing

Cyber Warfare: Nation State Sponsored Cyber Attacks

During the past few years, we have seen a surge in notable DDoS attacks causing significant disruptions in various industries and costing organizations millions of dollars. Organization leaders don't want to be told they are under a DDoS attack. They want to be prepared and stay ahead of potential threats to minimize system downtime and safeguard brand reputation.

One of the biggest factors in 2020 DDoS attacks was the COVID-19 lockdown, which drove a rapid shift to online for everything from education and healthcare to consumer shopping and office work, giving hackers more targets than ever before. Because of the haste of this transition, many of these businesses and workers turned out to be significantly under protected from attacks due to the difficulty of maintaining cybersecurity best practices in an emergency scenario.

In 2021, the scale of these attacks hit record highs. In November 2021, Microsoft mitigated a DDoS attack targeting an Azure customer with a throughput of 3.45 Tbps and a packet rate of 340 million PPS – believed to be the largest DDoS attack ever recorded. In 2021, we also saw the increased use of DDoS to demand ransom payments for stopping the attacks — or not launching them in the first place.

Throughout 2022 to today, Ukraine has been bombarded both physically and digitally, with DDoS attacks paving the way for other data breaches, critical infrastructure downtime, or espionage activity.

In late 2023, a new DDoS attack with record levels was executed. This attack method – HTTP/2 Rapid Reset Layer – was a new method of targeting servers that could bypass the traditional methods of DDoS protection, such as rate limiting or basic blocklists. This was a reminder that the DDoS defense must continue to innovate, and more comprehensive protection is required for DDoS vendors to effectively defend against modern, sophisticated DDoS attacks.

Though not exclusive to 2024, we've seen a continuous rise in carpet-bombing attacks. This could be attributed to two reasons. One, thwarting the source of the attack is difficult, and two, identifying intended targets can be difficult. Carpet-bombing attacks spread across a wide range of IP addresses versus certain targets. This means while the overall volume of malicious traffic generated is still the same, and still dangerous, it is more difficult for existing DDoS defenses to detect because typical threshold-based checks won't flag the traffic. Carpet-bombing attacks also may have a complex network of bots, including the bots themselves (foot soldiers carrying out commands), command and control center (the brains and source of evil), and proxy bots (the middlemen who take initiatives created by C&C). While one can identify the bots executing the attacks, that won't necessarily help in stopping the overall attack. You must find a way to trace it back to the middlemen, and then ultimately back to the Command & Control servers.

In 2024, one of A10's large service provider customers in Eastern Europe was faced with such an attack and reached out to A10 to learn more about the strange behavior its DDoS equipment was seeing. It wanted to receive further intelligence to dig deeper into adjustments that could be made on their end.

Advanced DDoS mitigation and detection capabilities are essential in reducing the impact of carpet-bombing attacks, but more can be done. Using AI and leveraging our proprietary zero-atrophy data gathering and validation techniques, we gained critical insights into the attack methods. Analysts believe that the most practical and effective way of leveraging generative AI is through analytics and insights, often in the form of threat intelligence. By integrating traditional DDoS mitigation with AI-enhanced analytics, we can provide comprehensive protection against sophisticated DDoS attacks. To quote the Mandalorian, "This is the [new] way."

A Brief History of DDoS Attacks

The first known distributed denial of service attack occurred in 1996 when Panix, now one of the oldest internet service providers, was knocked offline for several days by a SYN flood, a technique that has become a classic DDoS attack. Over the next

few years DDoS attacks became common and Cisco predicts that the total number of DDoS attacks will double from the 7.9 million seen in 2018 to something over 15 million by 2023.

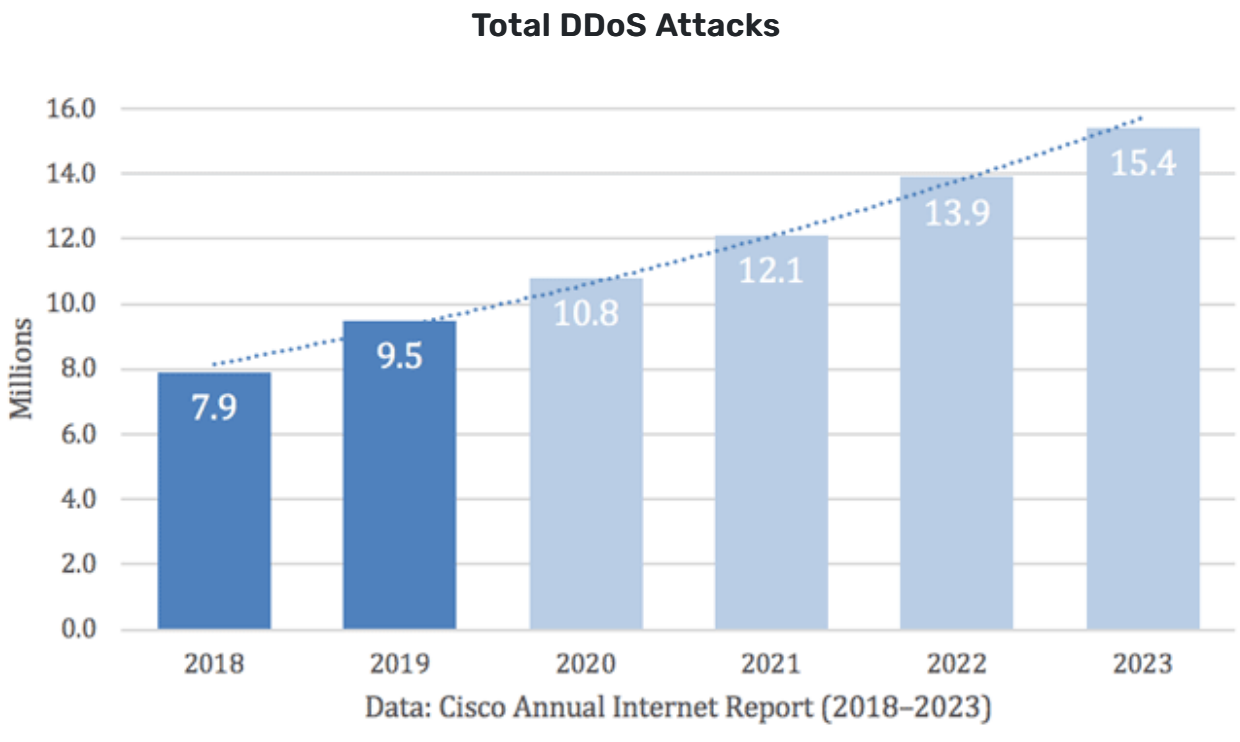

Figure 1. Cisco's analysis of DDoS total attack history and predictions.

However, it's not just the number of DDoS attacks that are increasing. Threat actors are creating ever bigger botnets – the armies of hacked devices that are used to generate DDoS traffic. As the botnets get bigger, the scale of DDoS attacks is also increasing. A distributed denial of service attack of one gigabit per second is enough to knock most organizations off the internet but we're now seeing peak attack sizes in excess of one terabit per second generated by hundreds of thousands or even millions of suborned devices.

The Cost of DDoS Attacks

Given that IT services downtime costs companies anywhere from $300,000 to over $1,000,000 per hour, you can see that the financial hit from even a short DDoS attack could seriously damage your bottom line. To understand what impact a distributed denial of service attack could have on your organization and your cybersecurity planning, please see our white paper How to Analyze the Business Impact of DDoS Attacks.

The Top-Five Most Famous DDoS Attacks (for Now)

To provide insight into what these attacks are like "in the wild," we're going to take a look at some of the most notable DDoS attacks to date. Our choices include some DDoS attacks that are famous for their sheer scale, while others are because of their impact and consequences.

1. Novel DDoS Attack: HTTP/s Rapid Reset Hits Multiple Targets, 2023

In Q3 of 2023, AWS, Google, and Cloudflare all experienced DDoS attacks of record-breaking size from botnets that were significantly smaller than what had previously been seen. This was concerning and pointed to new methods being used. Further investigation revealed that the attack exploited a feature in HTTP/2 that allows for rapid request cancellation using the RST_STREAM frame, which can eventually overwhelm servers by continuously opening and closing streams, leading to resource exhaustion.

Interestingly, this style of DDoS attack is better suited to be stopped with ADC reconfigurations. This is because this DDoS attack doesn't rely on overwhelming

servers with the number of requests (or packets of data being sent), but rather, it overwhelms by leveraging the amount of headers within the packets of data that are being sent. DDoS-specific solutions are not usually configured to examine details of the packet. Rather, they are configured to scrutinize other fields that are more indicative of incoming DDoS attacks. An ADC, on the other hand, usually focuses on looking at the requests themselves, as they need to establish sessions between the clients and servers, so they are more naturally suited to counter this DDoS attack style. The HTTP/2 rapid reset DDoS attacks are a reminder that DDoS is still here, and it's becoming more advanced.

2. The Google Attack, 2020

On October 16, 2020, Google's Threat Analysis Group (TAG) posted a blog update concerning how the threats and threat actors are changing their tactics due to the 2020 U.S. election. At the end of the post, the company snuck in a note:

in 2020, our Security Reliability Engineering team measured a record-breaking UDP amplification attack sourced out of several Chinese ISPs (ASNs 4134, 4837, 58453, and 9394), which remains the largest bandwidth attack of which we are aware.

Mounted from three Chinese ISPs, the attack on thousands of Google's IP addresses lasted for six months and peaked at a breath-taking 2.5Tbps! Damian Menscher, a Security Reliability Engineer at Google, wrote:

The attacker used several networks to spoof 167 Mpps (millions of packets per second) to 180,000 exposed CLDAP, DNS, and SMTP servers, which would then send large responses to us. This **demonstrates the volumes a well-resourced attacker can achieve:** This was four times larger than the record-breaking 623 Gbps attack from the Mirai botnet a year earlier.

3. The AWS DDoS Attack in 2020

Amazon Web Services, the 800-pound gorilla of everything cloud computing, was hit by a gigantic DDoS attack in February 2020. This was the most extreme recent DDoS attack ever and it targeted an unidentified AWS customer using a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) reflection. This technique relies on vulnerable third-party CLDAP servers and amplifies the amount of data sent to the victim's IP address by 56 to 70 times. The attack lasted for three days and peaked at an astounding 2.3 terabytes per second.

Why the AWS Attack Matters

While the disruption caused by the AWS DDoS Attack was far less severe than it could have been, the sheer scale of the attack and the implications for AWS hosting customers potentially losing revenue and suffering brand damage are significant.

4. The Mirai Krebs and OVH DDoS Attacks in 2016

On September 20, 2016, the blog of cybersecurity expert Brian Krebs was assaulted by a DDoS attack in excess of 620 Gbps. Krebs' site had been attacked before. Krebs had recorded 269 DDoS attacks since July 2012, but this attack was almost three times bigger than anything his site or the internet had seen before.

The source of the attack was the Mirai botnet, which, at its peak later that year, consisted of more than 600,000 compromised IoT devices such as IP cameras, home routers, and video players. The Mirai botnet had been discovered in August that same year but the attack on Krebs' blog was its first big outing.

The next Mirai botnet attack on September 19 targeted one of the largest European hosting providers, OVH, which hosts roughly 18 million applications for over one million clients. This attack was on a single undisclosed OVH customer and was driven by an estimated 145,000 bots, generating a traffic load of up to 1.1 terabits per

second. It lasted about seven days. But OVH was not to be the last Mirai botnet victim in 2016.

Why the Mirai Krebs and OVH Attacks Matter

The Mirai botnet was a significant step up in how powerful a DDoS attack could be. The size and sophistication of the Mirai network was unprecedented as was the scale of the attacks and their focus.

5. The Mirai Dyn DDoS Attack in 2016

Before we discuss the third notable Mirai botnet DDoS attack of 2016, there's one related event that should be mentioned. On September 30, someone claiming to be the author of the Mirai software released the source code on various hacker forums and the Mirai DDoS platform has been replicated and mutated scores of times since.

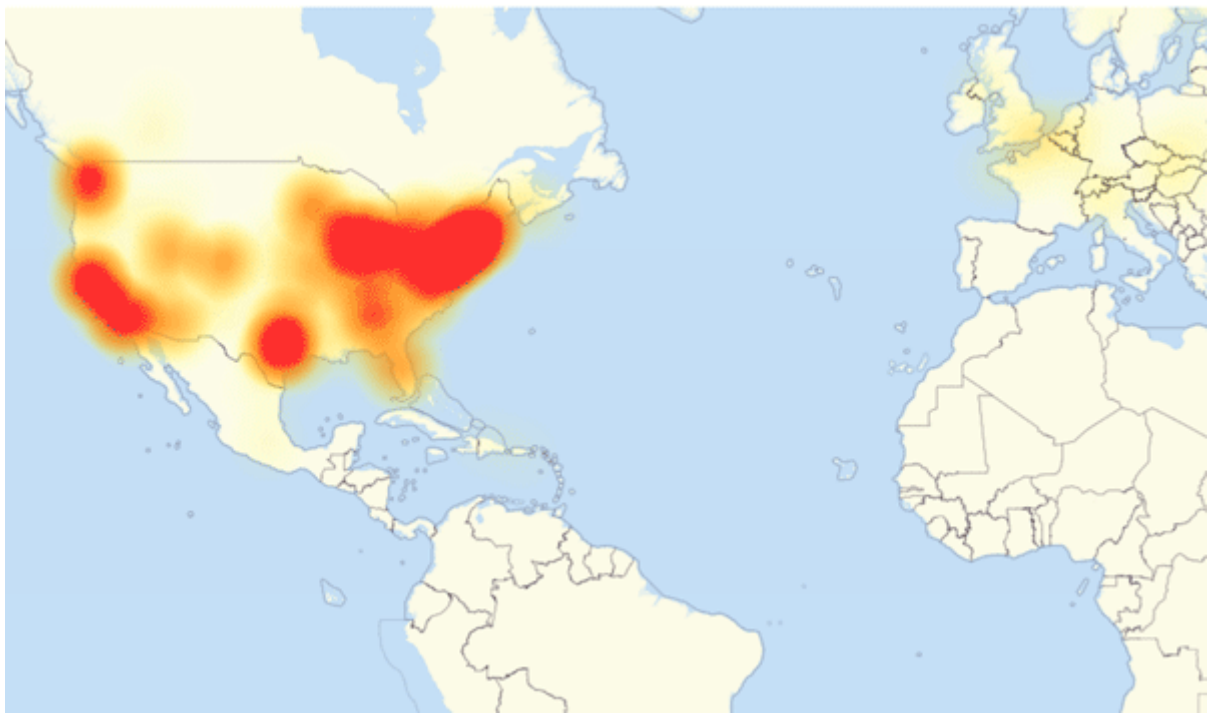

Figure 2. A map of internet outages in Europe and North America caused by the Dyn cyberattack October 2, 2016 / Source: DownDetector (CC BY-SA)

On October 21, 2016, Dyn, a major domain name service (DNS) provider, was assaulted by a one terabit per second traffic flood that then became the new record for a DDoS attack. There's some evidence that the DDoS attack may have actually achieved a rate of 1.5 terabits per second. The traffic tsunami knocked Dyn's services offline rendering a number of high-profile websites including GitHub, HBO, Twitter, Reddit, PayPal, Netflix, and Airbnb, inaccessible. Kyle York, Dyn's chief strategy officer, reported, "We observed 10s of millions of discrete IP addresses associated with the Mirai botnet that were part of the attack."

Why the Mirai Dyn Attack Matters

Mirai supports complex, multi-vector attacks that make mitigation difficult. Even though the Mirai botnet was responsible for the biggest assaults up to that time, the most notable thing about the 2016 Mirai attacks was the release of the Mirai source code enabling anyone with modest information technology skills to create a botnet and mount a distributed denial of service attack without much effort.

6. The GitHub Attack in 2018

On Feb. 28, 2018, GitHub, a platform for software developers, was hit with a DDoS attack that clocked in at 1.35 terabits per second and lasted for roughly 20 minutes. According to GitHub, the traffic was traced back to "over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints."

The following chart shows just how much of a difference there was between normal traffic levels and those of the DDoS attack.

Figure 3. Chart of the February 2018 DDoS attack on GitHub. Source: Wired

Even though GitHub was well prepared for a DDoS attack, their defenses were overwhelmed. They simply had no way of knowing that an attack of this scale would be launched. As GitHub explained in the company's incident report: "Over the past year, we have deployed additional transit to our facilities. We've more than doubled our transit capacity during that time, which has allowed us to withstand certain volumetric attacks without impact to users … Even still, attacks like this sometimes require the help of partners with larger transit networks to provide blocking and filtering."

Why the GitHub Attack Matters

The GitHub DDoS attack was notable for its scale and the fact that the attack was staged by exploiting a standard command of Memcached, a database caching system for speeding up websites and networks. The Memcached DDoS attack technique is particularly effective as it provides an amplification factor – the ratio of the attacker's request size to the amount of DDoS attack traffic generated – of up to a staggering 51,200 times.

Other Notable Distributed Denial of Service Attacks

7. A European Gambling Company, 2021

In February, Akami announced that they had dealt with "three of the six biggest volumetric DDoS attacks" the company has ever recorded. The DDoS attacks were

attempts at extortion. The hackers launch a DDoS attack the target can't help but notice and then demand payment not to do it again and at an even greater scale. In this case the threat attack weighed in at 800Gbps.

Why the Gambling Company Attack Matters

This attack was notable not just for its scale but also for its novelty. The attackers used a previously unseen DDoS attack vector that was based on a networking protocol known as protocol 33, or Datagram Congestion Control Protocol (DCCP). This attack was volumetric and by abusing protocol 33, the exploit was designed to bypass defenses focused on traditional Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) traffic flows.

8. Occupy Central, Hong Kong DDoS Attack in 2014

The multi-day PopVote DDoS attack was carried out in 2014 and targeted the Hong Kong-based grassroots movement known as Occupy Central, which was campaigning for a more democratic voting system.

In response to their activities, attackers sent large amounts of traffic to three of Occupy Central's web hosting services, as well as two independent sites, PopVote, an online mock election site, and Apple Daily, a news site, neither of which were owned by Occupy Central but openly supported its cause. Presumably, those responsible were reacting to Occupy Central's pro-democracy message.

The attack barraged the Occupy Central servers with packets disguised as legitimate traffic. It was executed using not one, but five botnets and resulted in peak traffic levels of 500 gigabits per second.

Why the Occupy Central Attack Matters

Although, it was reported that the attackers were probably connected to the Chinese government, there has never been conclusive proof and, perversely, the attack could have been intended to make the Chinese government look bad. The attack may have also provided cover for hackers who managed to extract Occupy Central staff details from a database to mount an extensive subsequent phishing campaign.

9. The CloudFlare DDoS Attack in 2014

In 2014, CloudFlare, a cybersecurity provider and content delivery network, was slammed by a DDoS attack estimated at approximately 400 gigabits per second of traffic. The attack, directed at a single CloudFlare customer and targeted on servers in Europe, was launched using a vulnerability in the Network Time Protocol (NTP) protocol, which is used to ensure computer clocks are accurate. Even though the attack was directed at just one of CloudFlare's customers, it was so powerful it significantly degraded CloudFlare's own network.

Why the CloudFlare Attack Matters

This attack illustrates a technique where attackers use spoofed source addresses to send fake NTP server responses to the attack target's servers. This type of attack is known as a "reflection attack," since the attacker is able to "bounce" bogus requests off of the NTP server, while hiding their own address. Due to a weakness in the NTP protocol, the amplification factor of the attack can be up to 206 times, making NTP servers a very effective DDoS tool. Shortly after the attack, the U.S. Computer Emergency Readiness team explained NTP amplification attacks are, "especially difficult to block" because "responses are legitimate data coming from valid servers."

10. The Spamhaus DDoS Attack in 2013

In 2013, a huge DDoS attack was launched against Spamhaus, a nonprofit threat intelligence provider. Although Spamhaus, as an anti-spam organization, is regularly attacked and had DDoS protection services already in place, this attack—a reflection attack estimated at 300 gigabits of traffic per second—was large enough to knock its website and part of its email services offline.

Why the Spamhaus Attack Matters

The cyberattack was traced to a member of a Dutch company named Cyberbunker, which had apparently targeted Spamhaus after it blacklisted the company for spamming. This illustrates that companies or rogue employees can mount DDoS attacks with immense brand damaging and serious legal consequences.

11. The Six Banks DDoS Attack in 2012

On March 12, 2012, six U.S. banks were targeted by a wave of DDoS attacks: Bank of America, JPMorgan Chase, U.S. Bank, Citigroup, Wells Fargo, and PNC Bank. The attacks were carried out by hundreds of hijacked servers from a botnet called Brobot with each attack generating over 60 gigabits of DDoS attack traffic per second.

At the time, these attacks were unique in their persistence. Rather than trying to execute one attack and then backing down, the perpetrators barraged their targets with a multitude of attack methods in order to find one that worked. So, even if a bank was equipped to deal with a few types of DDoS attacks, they were helpless against other types of attack.

Why the Six Banks Attack Matters

The most remarkable aspect of the bank attacks in 2012 was that the attacks were, allegedly, carried out by the Izz ad-Din al-Qassam Brigades, the military wing of the Palestinian Hamas organization. Moreover, the attacks had a huge impact on the affected banks in terms of revenue, mitigation expenses, customer service issues, and the banks' branding and image.

Holistic DDoS Attack Protection with A10 Defend

Even though new types of distributed denial of service attacks appear frequently, A10 Defend employs advanced defense strategies that protect against all kinds of cyberattacks including new, novel DDoS attacks that could bring down your online and in-house services. Visit the DDoS protection solution page to learn more.

For additional insight, including the top reflector searches and DDoS research insights performed by attackers, download the complete A10 Networks report, DDoS Attackers Uncovered: Understanding the DDoS Landscape.

Categories: NETWORK SECURITY

Previous Post

Catch Up or Leap Forward: Bridging the Digital Divide

Next Post

Zero Trust Architecture: 5 Reasons You Need It

A10 Staff | January 21, 2022