ZCorum™

DDoS Attacks

Evolution to Revolution

A Brief Timeline of Network Distributed Denial of Service

Introduction

Denial of Service attacks are one of the darker outcomes of modern internet technology. The denial of service attack floods the targeted network with superfluous requests or data and overloads the system. The targeted network cannot respond or simply crashes, blocking access for legitimate users. Think of an attack as similar to a group of people crowding the entrance to a shop, blocking the entire doorway and making it impossible for customers to enter.

Beginning Days

This reign of attack culture didn't start in a dark room with a hacker in a black hoodie and an evil grin, but as an experiment in 1974 by a 13-year-old student.

His school was located across the street from the Computer-Based Education Research Laboratory (CERL) at the University of Illinois. He had learned about a new command that could be run on CERL's terminals. The command, called "external" or "ext", allowed communication with external devices connected to the terminals. However, when the command was run on a terminal with no external devices connected, it would cause the terminal to lock up and remain that way until a shutdown and a power-on regained functionality for the terminal.

Curious to know what it would be like for a room full of users to be locked out at once, he wrote a program that would send the "ext" command to all the terminals at the same time. Walking across the street to CERL to test his program on the terminals there, his program caused a denial of service attack in which all thirty-one CERL users were locked out of their terminals and forced to power off. This attack was one of the first denial of service attacks ever recorded. But more would follow.

From Denial to Distributed Denial - The Attacks Spread

In 2014, the DoS attack celebrated its 40th birthday. Born as the handiwork of a teenaged "computer geek," these attacks have since exploded in quantity and sophistication.

Throughout the 1980s and 90s denial of service attacks continued to spread to more networks and more users. With everything from self-replicating buggy code in computer programs to viruses sent via email, the attacks began causing disruption worldwide.

Then in 1999, denial of service attacks suddenly strengthened to become Distributed denial of service attacks. A tool called "Trinoo" was used to disable the internal network of the University of Minnesota for over two days. Trinoo was a network of compromised machines called "Masters" and "Daemons" that allowed an attacker to send a DoS instruction to a few Masters. The Masters forwarded instructions to the hundreds of other machines, the Daemons. The Daemons then started a data flood against whatever target IP address the hacker wanted to bring down.

This multi-system attack was a gateway that opened up the flood of larger scale denial of service attacks. The distributed nature of a DDoS attack made it more powerful, and harder to identify and block its source. This was a new weapon in the hacker's arsenal.

By the new millennium, DDoS had captured the public's attention. In the year 2000, a major DDoS attack occurred, when CNN, Dell, E-Trade, eBay, and Yahoo! were all attacked by fifteen-year-old hacker Michael Calce. Calce, known by his online identity as 'Mafiaboy', compromised the networks of several universities and used their servers to conduct the DDoS attack against the major corporations. The teenager flooded the websites with an overwhelming amount of traffic, leaving behind an estimated $1.2 billion in damage.

From Kids to Political Causes

As attack technology evolved, so too did motivations and participants. Recent years have brought a steady rise in the number of DDoS attacks—fueled by shifting motives.

- In 2007, the republic of Estonia in northern Europe, had government services, financial institutions, and media outlets hit by a DDoS attack. This devastated the country's institutions. The motive was response to political conflict with Russia.

- In 2012, Bank of America, JPMorgan Chase, Citigroup, U.S. Bank, Wells Fargo, and PNC were all hit by a series of over 200 DDoS attacks. A hacker activist group demanded that an anti-Islam video be removed from YouTube. The attacks impacted the banks, affecting expenses, customer service, branding, and revenue.

- In 2013, Spamhaus, an organization that fights against spam, was hit by a teenage hacker-for-hire in Britain. He was paid to launch a DDoS attack against Spamhaus and drove traffic to the site at a rate of 300 Gbps. The attack lasted for almost a week. The attack caused major issues for the London Internet exchange.

- In 2014 Hong Kong, two pro-democracy sites were hit with a 500 Gbps DDoS attack that was executed with five botnets.

- In 2015, GitHub, a hosting service for software development, was targeted in an attack that went on for several days. The DDoS attack was traced to China and targeted projects centered on bypassing state censorship.

- In 2017, the Czech Republic's parliamentary elections failed temporarily because of DDoS attacks during the vote count.

- In 2020, Amazon Web Services reported a massive 2.3 terabit-per-second DDoS attack that was targeting an unnamed controversial customer. The attack lasted for three days.

Evolving Tools

But it's not just the number of DDoS attacks that are occurring, but the scale and methods of the attacks is also intensifying. A Distributed Denial of Service strike of one gigabit per second is enough to knock most organizations off the internet, but now attack sizes are far above that and harder to combat. Attack tools are evolving and also increasingly easy to access; the pool of attackers—and potential targets—is larger than ever.

- In 2016, Dyn, a DNS provider, was the target of a DDoS attack using compromised IoT devices like cameras, smart TVs, radios, printers, and even baby monitors. These devices were used to flood the Dyn servers. The attack disrupted major sites, including Airbnb, Netflix, PayPal, Visa, Amazon, and The New York Times. Another attack involving 600,000 compromised IoT devices brought to the forefront the vulnerabilities of these types of devices.

Today's Hackers

Since that first attack in 1974, denial of service attacks have been the most persistent and damaging to internet service providers. These attacks used to require a special set of skills and capabilities. That's not the case anymore. It is possible to unleash havoc even if a person knows practically nothing about computer programming or networks. The current trend is now to pay for DDoS-as-a-Service where highly skilled hackers are hired to take down any target. It's faster and easier. These DDoS attack services for hire are closing the gap between skilled and amateur hackers and fueling a surge in threats.

As the bad guys keep creating more DDoS attacks, they're also watching for new vulnerabilities in unguarded and poorly configured DNS servers. This trend is here to stay, at least for now. And while there's no cure-all for this battle yet, remaining informed and up to date with security advancements will defend your network until then.

More Resources

If you would like to learn more about DDoS Protection Solutions from ZCorum visit our website or read our two product sheets:

Corero SmartWall DDoS Protection

ZCorum™

4501 North Point Parkway,
Suite 125
Alpharetta, GA 30022

Toll Free: 1-800-909-9441
info@ZCorum.com

ZCorum provides broadband Internet and communication solutions to telcos, cable companies, utilities, and municipalities, assisting in all facets of broadband implementation, integration, engineering and consulting, network monitoring and diagnostics. ZCorum also offers wholesale, privatelabeled Internet services, including data and VoIP provisioning, email, Web hosting, and 24x7 support for end-users, enabling service providers to compete effectively in their local rural and suburban markets. ZCorum is headquartered in Alpharetta, GA.