Avast Business

Avast partner educational series

DDOS & website redirects

16 September 2021

Avast Business

About the author

Rob Krug,
Senior Security Architect,
Avast Business

Rob has been in the network engineering and security space for over 30 years. His background includes extensive work with telecommunications, network design and management, and most importantly, network security. Specializing in security vulnerabilities, Rob has extensive experience in cryptography, ethical hacking, and reverse engineering of malware. Rob served in the U.S. Navy and also worked as a Data Security Analyst and Director of Engineering for multiple international service providers and vendors. Rob has designed, implemented, and maintained some of the most complex and secure networks imaginable.

What is a DoS attack?

A denial-of-service attack (DoS attack) is a cyberattack in which the perpetrator (a single hacker or a group of hackers) seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Denial of service is typically accomplished by flooding the targeted machine or resource with a large amount of requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

What is a DDoS attack?

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources (usually using one or several botnets). As a result, simply blocking a single source is an ineffective way to stop the entire attack.

A DoS or DDoS attack can be best visualized with a group of people crowding the entry door of a supermarket, making it hard for legitimate customers to enter, which disrupts the usual business.

What are DoS / DDoS attacks used for?

Criminal perpetrators often target sites or services hosted on high profile web services, such as banks or payment gateways. Revenge, black mail, or activism are related to these attacks as well. For example, during the Hong Kong Anti-Extradition Protests in June 2019, the messenger app, Telegram, was subject to a DDoS attack aimed at preventing protestors from coordinating movements.

What is a website redirect?

URL redirection or URL forwarding is used for a wide range of legitimate purposes, such as:

- URL shortening
- Preventing broken links if a resource is removed
- To allow multiple domain names to redirect requests to a single website
- Privacy protection

Avast Business

However, it can also be used for more criminal reasons, such as:

- Phishing attacks: Spam emails with links that lead to services that appear to be connected to a legitimate site, but it is actually designed to steal login information from users
- Malware distribution

About Avast Business

Avast delivers all-in-one cybersecurity solutions for today's modern workplace, providing total peace of mind. Avast provides integrated, 100% cloud-based endpoint and network security solutions for businesses and IT service providers. Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. Our easy-to-deploy cloud security solutions are built to offer maximum protection businesses can count on. For more information about our cloud-based cybersecurity solutions, visit **www.avast.com/business**.