What Is DDoS and Why Should We Care?

DDoS (Distributed Denial of Service)

DDoS is an attempt to exhaust the resources available to a network, application, or service so that genuine users cannot gain access.

Beginning in 2010, and driven in no small part by the rise of Hacktivism, we've seen a renaissance in DDoS attacks that has led to innovation in the areas of tools, targets and techniques. Today, the definition of a DDoS attack continues to grow more complicated. Cyber criminals utilize a combination of very high volume attacks, along with more subtle and difficult to detect infiltrations that target applications as well as existing network security infrastructure such as firewalls and IPS.

What Are the Different Types of DDoS Attacks?

Distributed Denial of Service attacks vary significantly, and there are thousands of different ways an attack can be carried out (attack vectors), but an attack vector will generally fall into one of three broad categories:

Volumetric attacks attempt to consume the bandwidth either within the target network/service, or between the target network/service and the rest of the Internet. These attacks are simply about causing congestion.

TCP State-Exhaustion attacks attempt to consume the connection state tables which are present in many infrastructure components such as load-balancers, firewalls and the application servers themselves. Even high capacity devices capable of maintaining state on millions of connections can be taken down by these attacks.

Application Layer attacks target some aspect of an application or service at Layer-7. These are the deadliest kind of attacks as they can be very effective with as few as one attacking machine generating a low traffic rate (this makes these attacks very difficult to pro-actively detect and mitigate). Application layer attacks have come to prevalence over the past three or four years and simple application layer flood attacks (HTTP GET flood etc.) have been some of the most common denial of service attacks seen in the wild.

How Are DDoS Attacks Used?

Today's sophisticated attackers are blending volumetric, state exhaustion and application-layer attacks against infrastructure devices all in a single, sustained attack. These cyber attacks are popular because they are difficult to defend against and often highly effective. The problem doesn't end there. Attackers are using DDoS tools to distract the network and security teams while simultaneously trying to inject advanced persistent threats such as malware into the network, with the goal of stealing IP and/or critical customer or financial information.

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECHD_002_EN-2001 05/2020