NETSCOUT

DDoS and the Good News/Bad News

First, the bad—adversaries continued to innovate and alter strategies aimed at taking down DDoS protections with direct-path DDoS attacks and high-powered server-class botnets. Meanwhile, a little good news came in the way of a decrease in some reflection/amplification vectors, floating overall DDoS attack numbers down. Despite this decrease, the bad news tells us we must remain vigilant to combat ever-changing attacker methodologies and tactics. To learn more about the constantly changing DDoS threat landscape explore the interactive report.

9.7M

DDoS ATTACKS IN 2021

A 3% decline from 2020, but a 14% increase over 2019

$9-$12M

IN POTENTIAL REVENUE LOSS

From DDoS extortion of VoIP provders

Free!

The BARRIER TO ENTRY FOR DDoS ATTACKS IS NONEXISTENT

The most prominent DDoS-for-hire services provide DDoS attacks ranging from no cost to greater than $6,500 for terabit-class attacks

Adversaries Engage in Asymmetric Warfare

Triple extortion. Highly targeted attacks. High-powered botnet armies. DDoS for hire. Adversaries wasted no time in 2021 creating new attacks or building upon the effectiveness of long-time favorites: They engaged in DDoS attack operations via any means necessary to take down their opponents, with a notable increase in targeting specific organizations to disrupt operations.

A Triple Threat

An unprecedented three DDoS extortion campaigns (LBA, Fancy Lazarus, and REvil copycat) operated simultaneously in 2021, showcasing a continued trend of monetizing DDoS—a trend quickly adopted by numerous ransomware gangs to run triple extortion schemes.

A Flood of Attacks

A rebalancing of the scales brought TCP-based flood and direct-path (non-spoofed) DDoS attacks in line with the three-year running champion—reflection/amplification DDos attacks.

DDoS as a Homing Missile

By singling out specific organizations, individuals, and applications/services, adversaries launched the equivalent of bombs to take out a target—wreaking havoc on everything around the target and walking away with a payday.

The Rise of Server-Class Botnet Armies

In a blast from the past, botmasters exploited high-powered servers running vulnerable software and services, conscripting them into server-class botnet armies capable of launching high-powered direct-path DDoS attacks—a feat not easy or always possible with IoT botnets.

DDoS-for-Hire Free-for-All

With a wide range of cost to no-cost options, underground DDoS-for-hire services offered a vast range of configurable options, power, and attack types to anyone with an internet connection and a potential victim.

The Intersection of Encryption, State, and DDoS Defense

DDoS attacks are really attacks on capacity and state—a fact not unknown to adversaries, who ramped up the potency of attacks by disrupting layer-4 TLC-encrypted applications and services.

From flooding victims with bogus traffic to high-powered botnets capable of launching millions of packets per second, adversaries aimed at taking down individuals and organizations alike with devastating effect. See how adversaries adapted in 2021.

Threat Intelligence Report Issue 8, Findings from 2H 2021

EXPLORE INTERACTIVE REPORT

NETSCOUT

SECIG_016_EN-2201 03/2022