THE EVOLVING DDOS LANDSCAPE

Distributed denial of service (DDoS) attacks are more frequent and damaging than ever before.

Cybercriminals use IoT technology, mobile devices, bots and malware to access networks. Damage can occur quickly and be long-lasting. Today's DDoS attacks are:

Frequent
31%
increase in the number of DDoS attacks in Q1 2021 from Q1 2020.[1]

Prevalent
5,351,930
attacks in the first half of 2021.[2]

Costly
$2.3 million
the cost of a typical attack.[3]

DDoS

What's at risk?

Network downtime and loss of productivity are the immediate perils of a DDoS attack. The associated cascade of impacts on an organization can have longer-lasting consequences:

Network downtime
83%
of outages caused by DDoS attacks targeted firewalls and VPN concentrators to help bring down the network.[4]

Productivity loss
32 days
— the longest attack in the second quarter of 2021.[5]

Network access
27 billion
connected IoT devices estimated by 2025.[6]

Who is a target?

DDoS attacks, and more recently DDoS-based ransomware attacks, should be a top concern for a variety of organizations. For example, enterprise organizations saw a 125 percent increase in DDoS extortion attacks in the past year.[7]

US-based organizations are most at risk, receiving 36 percent of all DDoS attacks worldwide — the most of any country.[8]

Several industries are under attack, including:

Financial services firms
experienced 50 percent of all DDoS extortion attacks in the first half of 2021.[9]

Retail
experienced the highest volume of application layer DDoS incidents of all industries throughout the past 12 months.[10]

Healthcare organizations
accounted for 79 percent of all reported data breaches in the first 10 months of 2020, with DDoS attacks creating cover for many of the breaches.[11]

Manufacturing
paid $1 to $2 million to recover from a breach, according to one quarter of security respondents[12], with an increase in DDoS attacks that target industrial control systems.[13]

Guard your network by:

Using threat detection to identify volumetric attacks before they impact your business. Intelligent monitoring, based on machine learning and algorithms, detects attacks based on your specific traffic patterns.

Quickly differentiating between legitimate and malicious traffic. A service provider can allow legitimate traffic to pass, while malicious traffic is rerouted and scrubbed at the IP address level.

Integrating your protection. A managed service that combines security with your dedicated Internet access offers always-updated, cloud-based protection, and a single source of support frees up internal resources. This simplifies the security process and expedites the discovery and mitigation of threats.

Read our executive brief: **DDoS mitigation: protect your network and your enterprise** to learn more about DDoS protection.

Learn more

Sources

1. Carol Hildebrand, "The Beat Goes On," NETSCOUT, May 17, 2021.

2. NETSCOUT Threat Intelligence Report: "Findings from 1H 2021," NETSCOUT 2021.

3. Seth Robinson, "DDoS Attacks on the Rise: A Closer Look at the Data," Big Data, Dec. 10, 2020.

4. Carol Hildebrand, "Latest NETSCOUT Threat Intelligence Report Highlights Unprecedented DDoS Attack Activity," NETSCOUT, Apr. 13, 2021.

5. Alexander Gutnikov, Ekaterina Badovskaya, Oleg Kupreev and Yaroslav Shmelev, "DDoS Attacks in Q2 2021," Securelist by Kaspersky, Jul. 28, 2021.

6. Satyajit Sinha, "State of IoT 2021," IoT Analytics, Sept. 22, 2021.

7. NETSCOUT Threat Intelligence Report: "Findings from 1H 2021," NETSCOUT 2021.

8. Alexander Gutnikov, Ekaterina Badovskaya, Oleg Kupreev and Yaroslav Shmelev, "DDoS Attacks in Q2 2021," Securelist by Kaspersky, Jul. 28, 2021.

9. NETSCOUT Threat Intelligence Report: "Findings from 1H 2021," NETSCOUT 2021.

10. "Retail Industry Security Incidents Soaring, Worsened by the Supply Chain Crisis," Help Net Security, Nov. 09, 2021.

11. Russell Smith, "5 Things to Know About DDoS Attacks in Healthcare," Health Tech Magazine, Sept. 16, 2021.

12. "Forrester Analytics Business Technographics Security Survey," Forrester, 2021.
Security decision-makers with network, data center, application security or security operations responsibilities who have experienced a breach in the past 12 months.

13. Dr. James Stanger, "Why DDoS Attacks are a Major Threat to Industrial Control Systems," Control Engineering, June 24, 2021.

Spectrum
ENTERPRISE