Microsoft Security

Protecting yourself from holiday-season DDoS attacks

While distributed denial-of-service (DDoS) attacks happen all year round, the holidays are one of the most popular times and where some of the most high-profile attacks occur.

DDoS refresher

DDoS attacks are carried out by individual devices (bots) or network of devices (botnet) that have been infected with malware and used to flood websites or services with high volumes of traffic. DDoS attacks can last a few hours, or even days.

Rise of the hacktivists

Politically motivated attackers, also known as "hacktivists," use DDoS attacks to disrupt political processes.

What?	Why?	How?
A DDoS attack floods a site or server with errant traffic to disrupt service or knock it offline.	Criminals use DDoS attacks to extort site owners for financial, competitive advantage, or political reasons.	Thanks to the cybercrime as a service business model, a DDoS attack can be ordered from a DDoS subscription service for as little as $500.[1]

Example:
In a February 2022 prelude to invasion, anti-Ukraine hacktivist attackers launched what has been described as the largest DDoS attack in history against Ukrainian banking and government websites.[2]

3 reasons why DDoS attacks are so common during the holidays

1. Organizations typically have reduced resources dedicated to monitoring their networks and applications—providing easier opportunities for threat actors to execute an attack.
2. Traffic volume is at an all-time high, especially for e-commerce websites and gaming providers, making it harder for IT staff to distinguish between legitimate and illegitimate traffic.
3. For attackers seeking financial gain, the opportunity for more lucrative payouts can be higher during the holidays as revenues are at the highest and service uptime is critical.

The peril of holiday-season attacks

Any website or server downtime during the peak holiday season can result in lost sales and customers, high recovery costs, or damage to your reputation. The impact is even more significant for smaller organizations as it can be harder for them to recover after an attack.

DDoS attack categories

In general, a DDoS attack falls under three primary categories, with a variety of different cyberattacks within each category. New DDoS attack vectors emerge every day as cybercriminals leverage more advanced techniques, such as AI-based attacks.

Volumetric attacks

Targets bandwidth. They are designed to overwhelm the network layer with traffic.

Example
A DNS (domain name server) amplification attack, which uses open DNS servers to flood a target with DNS response traffic.

Protocol attacks

Targets resources. They exploit weaknesses in the layer 3 and layer 4 protocol stack.

Example
A SYN (synchronization packet flood) attack, which consumes all available server resources (thus making a server unavailable).

Resource layer attacks

Targets web application packets. They disrupt the transmission of data between hosts.

Example
An SQL injection attack, which inserts malicious code into strings that are later passed to an instance of SQL Server for parsing and execution.

Attackers can use multiple attack types, including ones from different categories, against a network.

Tips for protecting and responding against DDoS attacks

While you cannot completely avoid being a target of a DDoS attack, proactive planning and preparation can help you more effectively defend against an attack.

#1 Evaluate your risks and vulnerabilities

Start by identifying the applications within your organization that are exposed to the public internet. Also, be sure to note the normal behavior of your application so you can respond quickly if it begins behaving differently than expected.

Holiday-season complications

Remember, higher levels of traffic around the holidays may make abnormalities harder to detect.

#2 Make sure you're protected

With DDoS attacks at an all-time high during the holidays, you need a DDoS protection service with advanced mitigation capabilities that can handle attacks at any scale. Look for service features such as traffic monitoring; adaptive real-time tuning; DDoS protection telemetry, monitoring, and alerting; and access to a rapid response team.

#3 Create a DDoS response strategy

Having a response strategy is critical to help you identify, mitigate, and quickly recover from DDoS attacks. A key part of the strategy involves assembling a DDoS response team with clearly defined roles and responsibilities. This DDoS response team should understand how to identify, mitigate, and monitor an attack and be able to coordinate with internal stakeholders and customers.

The value of simulated attacks

We recommend running attack simulations to test how your services will respond to an attack. During testing, validate that your services or applications continue to function as expected and there's no disruption to the user experience. Identify gaps from both a technology and process standpoint and incorporate them in the DDoS response strategy. We recommend that you perform such tests in staging environments or during non-peak hours to minimize the impact on the production environment.

#4 Reach out for help during an attack

If you think you are experiencing an attack, reach out to the appropriate technical professionals, such as an established DDoS response team, for help with attack investigation during an attack as well as post-attack analysis once it has concluded.

#5 Learn and adapt after an attack

While you'll likely want to move on as quickly as possible if you've experienced an attack, it's important to continue to monitor your resources and conduct a retrospective after an attack. Make sure your post-attack analysis considers the following:

- **Was there any disruption to the service or user experience due to a lack of scalable architecture?**
- **Which applications or services suffered the most?**
- **How effective was the DDoS response strategy, and how can it be improved?**

Don't let DDoS attacks ruin your holidays!
Prepare for the upcoming holiday season with the 2022 holiday DDoS protection guide.

Get the latest insights from Microsoft Security:

Visit Microsoft Security Insider

1 Microsoft Digital Defense Report 2022 | Microsoft Security 2 Ukraine Suffers Biggest DDoS Attack on Record in Russia Standoff - Bloomberg