Microsoft Security

2022 in review

DDoS attack trends and insights

Cybercriminals constantly innovate, adapt, and evolve. In 2022, distributed denial-of-service attack (DDoS) attackers continued to refine their techniques while increasing the sophistication of their operations.

Here is what we have observed:

Lessons from Ukraine

In the first half of 2022, the cyberthreat landscape centered around the war in Ukraine and the rise of nation state attacks and hacktivism worldwide.

February

Ukraine suffers the largest DDoS attack in the country's history, with damages impacting government websites and bank web services[1].

March + April

Nation state attackers and hacktivists looking to disrupt Ukraine's allies heavily target UK financial services with a significant increase in DDoS attacks[2].

As the conflict continued, attacks rippled through various Western countries, including the UK, US, and Germany.

Hacktivist spotlight: Killnet

Killnet[3], a vocal supporter of Russia's war in Ukraine, uses DDoS attacks as its primary weapon to create chaos across Western government, healthcare, education, and financial sectors.

Special Report: Ukraine

Microsoft shares insights into cyberattacks against Ukraine, highlighting details in the attack and context around the scope, scale, and methods of Russia-based nation state attackers.

Get report

Guide: Understanding and Responding to Distributed Denial-of-Service Attacks

The Cybersecurity & Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and Multi-State Information Sharing and Analysis (MS-ISAC) published a guide[4] to help governments and organizations respond effectively against DDoS attacks, especially those launched by hacker groups like Killnet.

Get guide

August

Hacktivists launch DDoS attacks against Taiwanese websites ahead of House Speaker Nancy Pelosi's arrival in Taiwan[5].

Non-political attacks

Beyond attacks with political motives, DDoS attacks also impacted a wide range of industries. In particular, the gaming industry continued to be highly targeted.

March

DDoS attackers bring down the game servers of Among Us, preventing players from accessing the popular multiplayer game for a few days[6].

October

A new version of RapperBot (heavily inspired by the Mirai botnet) targets game servers running Grand Theft Auto: San Andreas[7].

Attack volume trends

In total, Microsoft mitigated upwards of 520,000 unique attacks against our global infrastructure during 2022.

1,435
Average number of attacks per day in 2022.

2,215
Highest number of attacks in a day in 2022.
(September 22, 2022)

680
Lowest number of attacks in a day in 2022.
(August 22, 2022)

Attack vectors

TCP (transmission control protocol) attacks were the most frequent form of DDoS attack encountered in 2022, with combined UDP (user datagram protocol) attacks (UDP flood and UDP amplification) and packet anomaly attacks having a significant presence as well.

63% TCP | 15% Packet anomaly | 22% UDP

Included TCP attack vectors

- TCP SYN
- TCP ACK
- TCP floods
- Etc.

13%
UPD flood

Included UDP flood attack vectors

Spoofed floods account for 53% of the UDP flood attack volume.

9%
UDP amplification

Included UDP amplification attack vectors

- CLDAP
- NTP
- DNS

TCP popularity attracts attention

Most services use TCP, so the high rate of TCP flood attacks makes sense, though Microsoft has observed a significant uptick in DDoS attacks in the gaming industry, which primarily uses UDP.

TCP reflected amplification attacks on the rise

This new attack vector takes advantage of improper TCK stack implementation in middleboxes, such as firewalls and deep packet inspection devices, to elicit amplified responses that can reach infinite amplification in some cases.

April 2022

Microsoft monitors a reflected amplified SYN+ACK attack[8] on an Azure resource in Asia. The attack reached 30 million packets per second (pps) and lasted 15 seconds.

Attack throughput was not very high, however there were 900 reflectors involved, each with retransmissions, resulting in a high pps rate that can bring down the host and other network infrastructure.

Attack duration

Most attacks in 2022 were short. Typically, the longer the attack was, the less often we saw that category of attack.

11%
More than 1 hour

89%
Less than 1 hour

2-minute drill

Attacks spanning 1-2 minutes account for 26% of the 2022 DDoS attacks. This is not a new trend, as shorter attacks requiring fewer resources are more challenging to mitigate for legacy DDoS defenses.

Did you know?

1. Attackers often use multiple short attacks over numerous hours to make the most impact using the fewest resources.
2. Short attacks take advantage of the time it takes systems to detect the attack and for mitigation to kick in. While time to mitigation may only take 1-2 minutes, the information from those short attacks can make it into the backend of services, impacting legitimate usage.
3. If a short attack causes a reboot of the systems, multiple internal attacks can be triggered as every legitimate user tries to reconnect simultaneously.

Attack source destination

As with previous years, most attacks were launched against US-based resources, with India, East Asia, and Europe making up a large portion of the remaining attacks.

Attractive targets

The rising adoption of smartphones and the popularity of online gaming in Asia will likely contribute to increased exposure to DDoS attacks. This also applies to countries accelerating digital transformation and cloud adoption.

What's ahead for 2023?

In 2023, cybercrime will likely continue to rise as new threats and attack techniques emerge. Here are the four biggest DDoS trends we anticipate:

Trend 1

Attackers will use DDoS as distractions to hide more sophisticated attacks (such as data breaches) launched at the same time.

Trend 3

We expect to see a rise in DDoS attacks from account takeovers where malicious actors will gain unauthorized access to resources to launch DDoS attacks.

Trend 2

While not new, internet of things (IoT) DDoS botnet attacks will continue to cause significant disruption.

Trend 4

As geopolitical tensions continue to emerge globally, we will likely continue to see DDoS being used as a primary tool for cyberattacks by hacktivists.

Tips for protecting and responding against DDoS attacks

Proactive planning and preparation can go a long way toward helping 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.

#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.

#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?

See how you can protect yourself from DDoS attacks that are becoming more frequent, sophisticated, and inexpensive to launch.

Learn more

[1] https://venturebeat.com/security/ddos-attack-was-largest-ever-in-ukraine-russia-suspected/
[2] https://www.finextra.com/newsarticle/40955/uk-finance-suffers-surge-in-ddos-attacks
[3] https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/
[4] https://www.cisa.gov/uscert/ncas/current-activity/2022/10/28/joint-cisa-fbi-ms-isac-guide-responding-ddos-attacks-and-ddos
[5] https://www.nbcnews.com/tech/security/taiwanese-websites-hit-ddos-attacks-pelosi-begins-visit-rcna41144
[6] https://www.pcmag.com/news/ddos-attack-takes-among-us-servers-offline-for-entire-weekend
[7] https://thehackernews.com/2022/11/warning-new-rapperbot-campaign-aims-to.html
[8] https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/

To get the latest cyberthreat insights from Microsoft Security Insider, go to Microsoft.com/security-insider.

Microsoft Security