MAZEBOLT

DDoS Threat Landscape Report

Q2 2024



Executive Summary

- DDoS attacks are becoming more sophisticated as well as more prevalent.
- Online services can easily be disrupted for prolonged periods of time - even for those using the best DDoS protection solutions.
- The SEC and DORA regulations are requiring organizations to act.
- Looking at the financial damages and regulatory fines, the risk and liability have dramatically increased.

Impact of New Techniques and DDoS-for-Hire Services

During Q2 of 2024, Distributed Denial of Service (DDoS) attacks continued to be a significant threat to organizations worldwide. The number and frequency of attacks is continuing to increase quarter over quarter. These attacks were characterized by:



Greater
Complexity & Scale



Advances in
Attack Techniques



Availability of
DDoS-for-Hire Services

Political Motivation Continues to Drive DDoS Attacks

Throughout Q2, the main motive for many of the large-scale DDoS attacks continued to be geopolitical conflict. The second most common motive behind DDoS attacks was internal political conflict – primarily in Europe.

A string of DDoS attacks was seen across Europe, due to the recent elections to the European Parliament and the elections in France. These attacks were initiated by various politically motivated groups.

Breakdown by Industry

The attacks impacted many sectors, concentrating primarily on finance, healthcare, and government services:

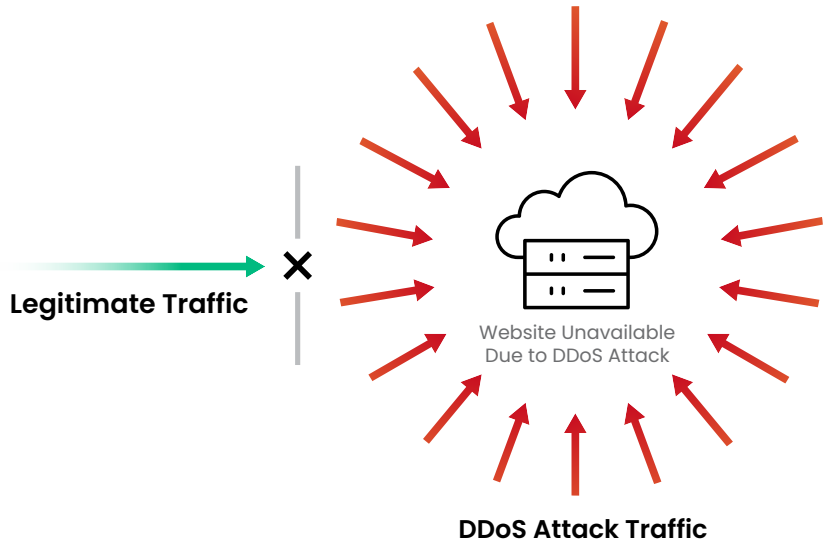
INDUSTRY	ATTACK PATTERNS
Finance	Financial institutions experienced a surge in targeted DDoS attacks aimed at disrupting their online services and availability, causing financial and reputational damages. The attacks highlighted vulnerabilities in DDoS protections.
Healthcare	Healthcare providers faced DDoS attacks targeting patient management systems and telemedicine platforms, causing organizations to seek improved protection for their infrastructure.
Government	Government websites and services were frequently targeted, often coinciding with political events or public announcements. The attacks aimed to erode the public trust and disrupt administrative functions.

Advanced DDoS Vulnerability Management Reduces the Risk

Q2 2024 underscored the persistent and evolving nature of DDoS attacks. As attackers leveraged new techniques and exploited emerging vulnerabilities, organizations across various sectors faced significant challenges in protecting their digital assets.

The quarter emphasized the importance of advanced DDoS threat management systems, enablement of DDoS protection testing, robust mitigation strategies, and collaborative efforts to counter the ever-growing threat of DDoS attacks.

What is a DDoS Attack?



Drill-Down:
Top DDoS Threats in Q2 2024

The following tables provide an overview of some of the most significant Q2 DDoS attacks, as they were reported in the news. To learn about attacks in Q1, see here.

April 2024

Date of Attack	Country/ State	Vertical	Companies Affected	Attacker	Press Headlines
April 3	Sydney	Community	Sydney's Indian Support Centre	Malaysian "hacktivist" group	Link
April 4	South Korea	Gaming	Professional esports organization T1, during the League of Legends Champions Korea (LCK) playoffs	Unknown	Link
April 9	Israel	TV	Israel National News TV channel	Mujahideen Cyber Army	Link
April 10	United Kingdom	Financial	UK trade unions	Malaysian "hacktivist" group RipperSec	Link
April 12	Albania	Media	Citizens Channel	Coordinated group, referred to as a "digital army"	Link
April 25	Poland	Government	Targeted various sectors: government, transportation, banking, judiciary, manufacturing, air transport, and media	NoName057	Link
April 26	Russia	Government	Meduza (Russian independent media site)	Not confirmed	Link
April 29	Russia	Government	Russia's ruling United Russia party	Ukraine's military intelligence agency, the GUR	Link
April 29	Moldova	Government	Government website	NoName057	Link

May 2024

Date of Attack	Country/ State	Vertical	Companies Affected	Attacker	Press Headlines
May 1	Russia	Government	United Russia, Russia's ruling political party	Ukraine's Main Directorate of Intelligence	Link
May 2	Ukraine	Banking	Monobank	Unidentified hackers	Link
May 2	Sweden	Government	Swedish government infrastructure	NoName057, Anonymous Sudan, Russian Cyber Army Team, and Killnet	Link
May 6	Globally	Gaming	Final Fantasy XIV video game	Not confirmed	Link
May 8	Japan + North America	Gaming	Video game series Final Fantasy	Not confirmed	Link
May 8	Republic of Kosovo	Government	Governmental websites	Russian hackers	Link
May 26	United States	Internet	Wayback Machine	Not confirmed	Link
May 27	Bulgaria	Ports Infrastructure Company	Bulgarian Ports Infrastructure Company	Russian Cyber Army	Link
May 29	Spain	Transportation	TRAM Barcelona	NoName057	Link
May 30	United States	Internet	The Internet Archive	Not confirmed	Link

June 2024

Date of Attack	Country/ State	Vertical	Companies Affected	Attacker	Press Headlines
June 6	Netherlands	Government	Dutch party websites	HackNeT	Link
June 9	Ireland	Government	The websites for Irish Rail, Bus Éireann, Transport for Ireland, the Houses of the Oireachtas, the Leap Card, and voter registration portal Voter.ie	Pro-Russian hacking groups	Link
June 10	Europe	Government	European political parties	HackNeT	Link
June 11	Malta	Communication	MaltaToday	Unknown third-party	Link
June 20	Poland	TV	Euro 2024 broadcast	Russian hackers	Link
June 25	Switzerland	Financial	Cardano Blockchain	Not confirmed	Link
June 26	Croatia	Government	The Ministry of Finance, the Tax Administration, the Croatian National Bank (HNB), the Economic Bank of Zagreb (PBZ), and the Zagreb Stock Exchange (ZSE)	NoName057	Link
June 27	United States	Supply Chain	Polyfill Supply Chain	Not confirmed	Link

Trends to Watch Out For in Q3

The DDoS landscape throughout Q3 is expected to be characterized by:

Multi-Faceted Extortion

DDoS is combined with ransomware to amplify threat levels. First, a ransomware attack encrypts data and threatens leakage. Second, a DDoS attack disrupts services, increasing the pressure for the victim to pay the ransom.

Impact of AI

MazeBolt research shows that DDoS attacks are adapted and automated so that they identify security vulnerabilities more quickly and can execute the attacks efficiently, without detection.

Hacktivists Motivated by Political Tensions

DDoS attacks will continue to be initiated by hacktivists who are motivated by regional conflicts, a nationalistic drive, and ideological tensions.

State Sponsorship

Nation states fund threat actors, including criminal groups and hacktivists, and provide guidance on how to effectively initiate DDoS attacks.

About MazeBolt

MazeBolt RADAR™ is a patented DDoS Vulnerability Management solution. Using thousands of non-disruptive DDoS attack simulations and without affecting online services, it can identify and enable the remediation of vulnerabilities in deployed DDoS defenses. RADAR enables organizations and governments to maintain the uninterrupted business continuity of online services. Using RADAR's patented vulnerability simulation technology, enterprises have unparalleled visibility into their DDoS protection solutions so they can be confident that damaging DDoS attacks can be prevented - before they happen. Read more at www.mazebolt.com

MAZEBOLT