MAZEBOLT

DDoS Threat Report

Q1 2024

A review of Q1 2024 DDoS attacks

We all know DDoS attacks are growing in both number and sophistication, with the data backing it up. DDoS attacks have jumped 50% YoY since Q1 2023, and 30% of these attacks extended beyond one hour. As we leave the first quarter of 2024, attacks aren't slowing down — and one of the most interesting questions to answer is, why?
There are several factors that are converging to create today's complex DDoS landscape.

Firstly, geopolitical conflicts across multiple regions have fueled the rise of hacktivists who target a wide range of industries as well as countries. When hacktivists feel countries or organizations are aiding their adversaries or providing support to the other team, DDoS attacks are a message that's hard to misread.

One example is AnonymousSudan, a hacker group that has claimed responsibility for multiple attacks against both companies and countries this quarter, citing perceived support for Israel in its recent war against Hamas as its motivation. Victims include an alleged cyberattack against OpenAI in February, and an attack against the US Department of Justice in March.

Next, DDoS tools are easier than ever to leverage, which means even low-skilled threat actors can launch attacks. DDoS tools and scripts like "Build Your Own Botnet" are hosted on code repository sites like GitHub, and invite anyone with the inclination to participate in a DDoS attack. And if even this is too much work, we've seen an increase in groups offering DDoS-as-a-Service, carrying out a DDoS attack on behalf of someone else — in exchange for as small an amount of money as $5-10 per hour.

Another factor to be aware of is an increase in compromised IoT devices. IoT is not built for security, but instead for low cost and ease of use. With weak security measures, and security regularly considered an add-on at the final stages of development, IoT devices are easily compromised. This allows threat actors to install malware that is then used to launch DDoS attacks across a connected environment. An example from this quarter is an attack by BigPanzi, using a DDoS botnet that infected Smart TVs and set-top boxes. This is far from an anomaly. Reports have uncovered a five-fold increase in DDoS attacks that use IoT bots between 2022-2023, and that number is only growing.

Finally, we're seeing an uptick in the use of Virtual Private Servers (VPS), offering substantially larger internet connections for attackers than they can leverage with residential broadband subscribers or mobile devices. As a result, DDoS attacks can be far more powerful.

Zeroing in on the Top DDoS Threats in Q1 2024

Happy new year from NoName Ransomware Group, who allegedly attacked at least five different Finnish government organizations in early January, including the National Cybersecurity Center, and followed this crime spree up by a similar onslaught against both Germany and Ukraine.

In another act of Hacktivism in January, the Phoenix Group took responsibility for a DDoS attack targeting the US Congress. Other attacks of note include BigPanzi's IoT-based attack that allowed attackers to hijack streaming services in the UAE, and a DDoS attack against the Manta Network, which according to the company — led to longer transaction times and increased gas prices on the network.

As well as AnonymousSudan's politically-motivated attack against OpenAI, February saw a DDoS attack take down parts of the Pennsylvanian court systems in the USA, and another against the Canadian police force, the Royal Canadian Mounted Police. While there was no known impact to security operations, the RCMP called the magnitude of the breach "alarming".

The AnonymousSudan hacking group has had a busy quarter, and in March, they claimed responsibility for a DDoS attack against several French government websites which caused six hours of downtime, as well as several attacks against Alabama government agencies, and another that targeted the US Dept of Justice. Another attack by NoName took place in March, who launched an attack against the Swiss federal government immediately following a visit by Ukrainian President Volodymyr Zelensky. Finally, 5 hours of downtime was reported for the website of the US Securities and Exchange Commission (SEC), coinciding with a 4.4% drop in the price of Bitcoin, although neither the DDoS attack itself, nor a link with the Bitcoin price has been confirmed.

Unfortunately, these attacks are just the tip of the DDoS-shaped iceberg. You can view information on all the DDoS attacks during Q1 using the tables below

January 2024

Date of	Country/	Vertical	Companies Affected	Attacker	Press Headlines
2-Jan	Finland	Government	Multiple Government Agencies	NoName057	Link
5-Jan	USA	Government	US Congress Website	Phoenix group	LInk
7-Jan	Bangladesh	Government	Bangladesh Election Commission	N/A	Link
9-Jan	Germany &	Government	Multiple Government Agencies	NoName057	Link
17-Jan	Israel	Infrastructure	Bazan Group		Link
17-Jan	Switzerland	Government	Government ministries and federal offices	Pro-Russian hackers	Link
18-Jan	United Arab	Television	UAE TV streaming services	Bigpanzi botnet	Link
19-Jan	Singapore	Crypto	HTX		Link
19-Jan	USA	Crypto	Manta Network		Link
21-Jan	Ukraine	Banking	Monobank	Mantis Botnet	Link
26-Jan	Ukraine	Federal	Ukrainian State Agency	N/A	Link

February 2024

Date of Attack	Country / State	Vertical	Companies Affected	Attacker	Press Headlines
1-Feb	United Arab Emirates	Aviation	Flydubai	Anonymous Sudan	Link
1-Feb	USA	Crypto Exchange	Solana's Phantom Wallet	N/A	Link
4-Feb	USA	Gov	Pennsylvania Courts online system		Link
8-Feb	Uganda	Mobile	Mobile providers	Anonymous Sudan	Link
14-Feb	USA	Software	OpenAI	Anonymous Sudan	Link
20-Feb	United Kingdom	Education	Cambridge University	Anonymous Sudan	Link
24-Feb	Canada	Gov	Royal Canadian Mounted Police		Link
29-Feb	Switzerland	Gaming	Overwatch 2	N/A	Link

March 2024

Date of Attack	Country / State	Vertical	Companies Affected	Attacker	Press Headlines
3-Mar	Estonia	Government	Estonian Police and Border Guard Board (PPA), the tax and customs board, and the	Pro-Kremlin Hackers	Link
6-Mar	Poland		Railway Transport Office in Poland,		Link
9-Mar	Bulgaria	Mobile Network	GSMArena	Indian networks	Link
10-Mar	France	Government	French Prime Minister's Office	Anonymous Sudan	Link
12-Mar	USA	Government	Alabama government agencies	Anonymous Sudan	Link
15-Mar	USA	Bitcoin Exchange	US Securities and Exchange Commission	N/A	Link
16-Mar	Romania	Banking/	The official government sites	NoName057	Link
16-Mar	Russia	Government	President's political party	N/A	Link
17-Mar	Switzerland	Government	Swiss Federal Government Websites	NoName	Link
20-Mar	USA	Government	US Department of Justice	Anonymous Sudan	Link

Forecast for 2024: DDoS Trends to Watch Out For

With a sophisticated DDoS reality to contend with, here are our predictions for what the remainder of 2024 is going to look like in terms of its DDoS landscape.

1 **Conflict-motivated attacks:**
Whether it's related to Russia/Ukraine, Israel/Hamas/Iran, or another conflict altogether — regional conflicts will continue to inflame ideological tensions. Triggered by nationalistic drive, hacktivists will be motivated to launch DDoS attacks against countries and specific organizations.

2 **State-sponsored hackers:**
With so many threat actors willing to do the dirty work, Nation states will keep their own hands clean, while continuing to fund and provide guidance to criminal groups and hacktivists. This helps them to add a layer of plausible deniability.

3 **Targeted attacks:**
Look out for high-impact DDoS headlines, including cloud services, financial organizations, and government targets. In particular, attacks smaller than 50Mbps can often fly under the radar and be highly effective at slipping past defenses and through vulnerabilities.

4 **The rise of AI:**
When AI gets involved with DDoS attacks, they can be automated, adaptable, and agile. Botnets managed by AI can evade detection and execute DDoS attacks efficiently and effectively, and identify security vulnerabilities faster than could ever be achieved manually.

5 **Multi-faceted extortion**
Threat actors and hacktivists are combining attack methods such as ransomware and DDoS attacks to amplify threat levels. After a ransomware attack encrypts data and threatens leakage, DDoS attacks are then used as the third arm of the tripod, disrupting services to encourage the victim to pay the ransom.

No matter the size of your organization, any company with online services could be hit by a damaging DDoS attack, and fall victim to financial damages, downtime and disruption to business continuity.

To protect your business, you need to feel confident that your DDoS protection solutions have zero vulnerabilities — and yet most organizations only test their implementations once or twice each year, and often only find vulnerabilities after the fact, when they've been exploited. At this stage, you're left reacting in panic mode, trying to quell a fire as it threatens to spread.

MazeBolt takes a proactive approach to finding the vulnerabilities in DDoS configurations, continuously testing across all online services and all known attack vectors, without any disruption to business continuity.

Any vulnerabilities are flagged and prioritized alongside steps for remediation, followed by validation that the issue has been resolved.

!

Looking to enhance your organizational cyber-resilience and shine a light over potential DDoS protection gaps?

Contact a member of the MazeBolt team