MAZEBOLT

DDoS Threat Landscape Report

Q4 2024 Review

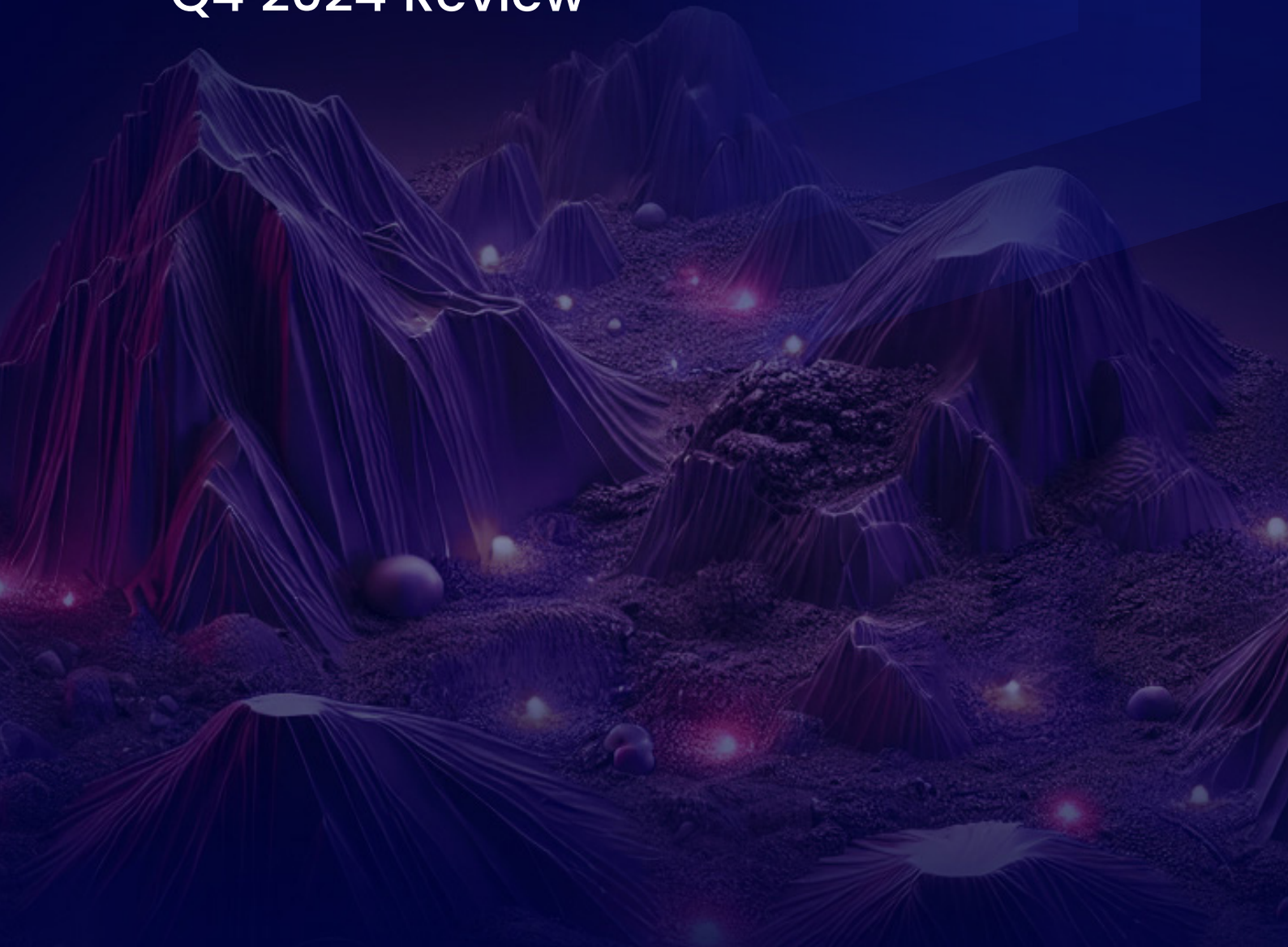


Table of Contents

Executive Summary	3
DDoS Attacks on Critical Services	4
Retailers Lost Revenues	5
Political Hacktivism and State Actors	6
Matrix Botnet Highlights Increased IoT Risk	8
Rise in Telecom and Internet Infrastructure Attacks	9
Drill-Down: Top DDoS Threats in Q4 2024	10
About MazeBolt	11

Executive Summary

The final quarter of 2024 saw an 83% increase year-over-year (YoY) in the number of DDoS attacks, according to a recent Cloudflare report. Looking back on the year as a whole, the number of DDoS attacks surged by 53%.

Some of the most notable DDoS news and attack trends in Q4 2024 included:

- **During the holiday season, there was a series of DDoS attacks on critical infrastructure:** The week of Christmas saw large-scale DDoS attacks on government websites and critical infrastructure.
- **Retailers lost revenue due to damaging downtime:** DDoS downtime in the holiday shopping season represented a significant loss for retailers this quarter – as consumers faced with the downtime of ecommerce sites quickly looked elsewhere, in their scramble to buy holiday gifts.
- **Political hacktivism was behind many large-scale attacks:** Sharp increases in politically motivated DDoS activity were seen during Q4 in response to significant political events, such as the US presidential elections.

This year, the number of DDoS attacks surged by 53%.

- **The Matrix botnet highlighted increased IoT risk:** Matrix emerged as a significant cyber threat actor in November. Primarily by leveraging Mirai malware, Matrix orchestrated widespread DDoS attacks by exploiting misconfigurations and vulnerabilities in Internet of Things (IoT) devices.
- **Telecom and Internet infrastructure attacks increased:** Q4 saw a rise in the number of DDoS attacks on telecom companies and Internet infrastructure.

DDoS Attacks on Critical Services

Alongside the holiday spirit and festive decorations, this year the week of Christmas was marked by a series of high-profile DDoS attacks on government offices, financial organizations, and other critical services. The most striking examples include:

Cyberattack on Italy's Foreign Ministry, Airports Claimed by Pro-Russian Hacker Group – Approximately ten official websites in Italy were disabled by this DDoS attack.

Ukraine's Intelligence Disrupts Lukoil Services with Cyberattack– Lukoil customers could not make payments at gas stations via the mobile application.

Internet Sites of Several French Cities Hit by Cyberattacks – Hackers used DDoS attacks to protest French support for Ukraine.

Mizuho Bank and Resona Bank May Have Been Hit by Cyberattack – Two of the largest banks in Japan were attacked, impacting the availability of online banking services.

NIPOST's Website Down, Suffers DDoS Attack – The Nigerian Postal Service's site went down.

Retailers Lost Revenues

The holiday shopping season in Q4 comes together with a significant increase in consumer spend. For cybercriminals, it's the busiest time of the year. While e-commerce platforms gear up for the surge in online traffic, hackers are gearing up to launch some of their most disruptive attacks.

One of the biggest threats to business continuity during this period is DDoS, which can bring even the most robust online systems to their knees - resulting in significant financial losses, reputational damage, and operational chaos. This year's attacks during the holiday season leveraged advanced tactics with an increase in DDoS-for-hire operations, the assembly of extensive DDoS botnets by script kiddies, and the bypass of Content Delivery Network (CDN) protections.

Financial losses due to damaging DDoS downtime tend to be much steeper during the holiday season, due to:

- **Lost sales and customers:** When the website is down, customers are likely to switch to a competing company since competition is so harsh. During the holiday season, many purchases are urgent, and a site being unavailable due to DDoS downtime can translate to direct loss of sales. More worryingly, being unavailable tends to hurt long-term customer relationships.
- **High recovery costs:** DDoS attacks often leave behind more than just downtime. They can cause systems to malfunction, corrupt data, and force organizations to perform costly forensics and recovery operations. For many businesses, the recovery costs after an attack can be higher than the initial financial impact of the downtime.
- **Reputational damage:** In an age where customer trust is everything, a DDoS attack that brings business to a halt during the holidays can do permanent harm to a brand's reputation. Customers expect seamless online shopping experiences, and failing to deliver on that expectation can hurt long-term growth.

Financial losses due to damaging DDoS downtime tend to be much steeper during the holiday season.

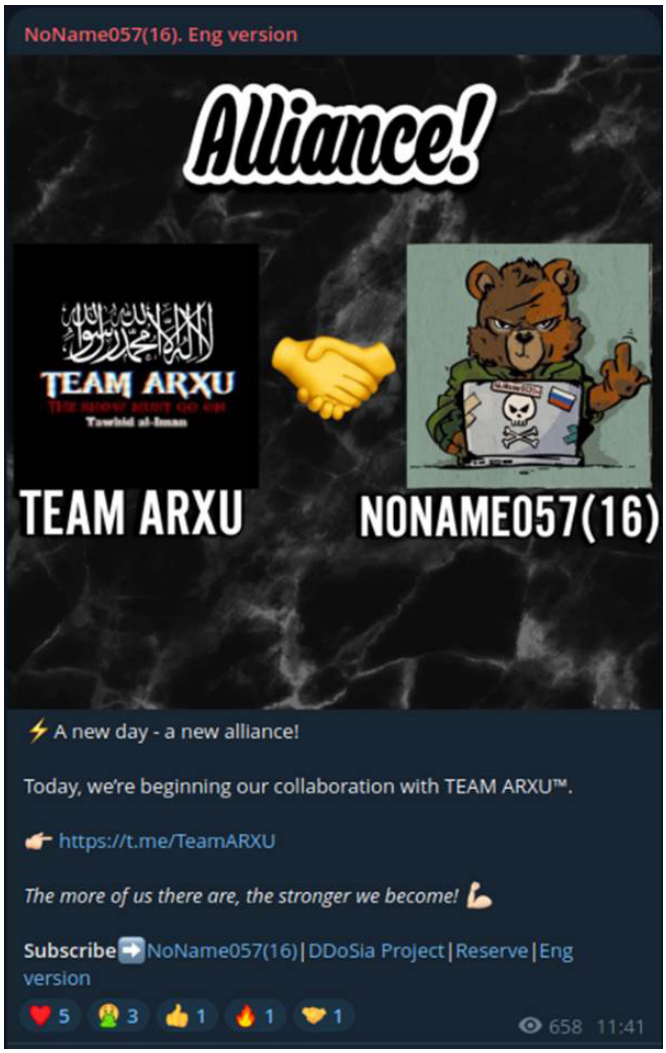
Political Hacktivism and State Actors

A sharp increase in politically motivated DDoS attack activity was seen in several contexts:

In Response to Political Events

Geopolitical tensions in regions including Russia and Ukraine, the Middle East, and China and Taiwan continued to contribute to the surge in DDoS attacks globally. Hacktivists frequently targeted government websites or critical infrastructure, including financial institutions, following political events. These attacks typically aimed to destabilize economies or disrupt financial support for the opposing side of a conflict.

Note that the hacktivist group NoName057 underwent a striking transformation this year, from functioning as a solitary actor to being a leader of a cooperative network. By leveraging strategic alliances, NoName057 has been able to increase its operational capacity – coordinating attacks, sharing intelligence, and pooling resources with like-minded hacktivist and cybercriminal groups. This new mode of operation represents a worrisome trend, as it allows hacktivist groups to amplify their power and ideological impact .

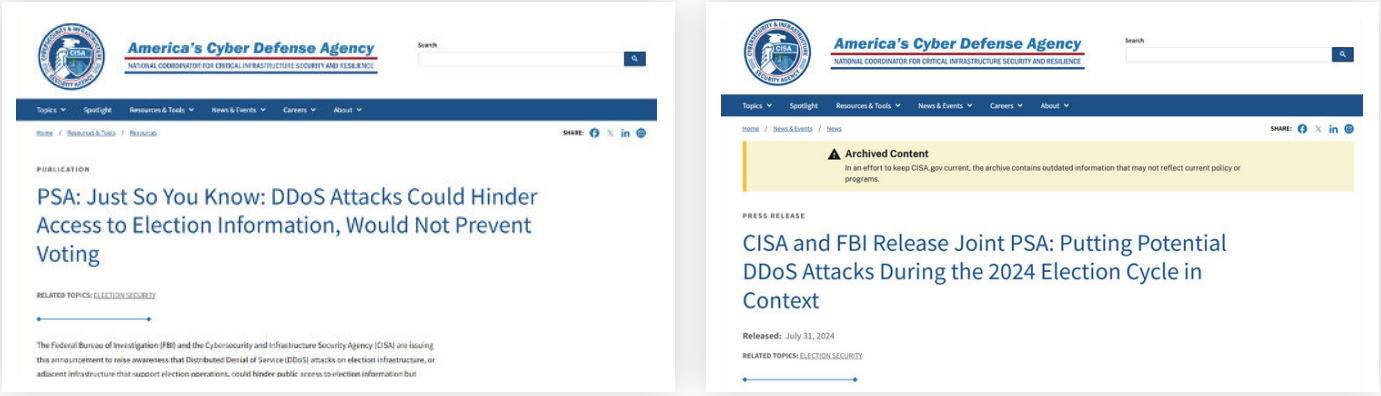


NoName057 Announces New Alliance
Source: Radware

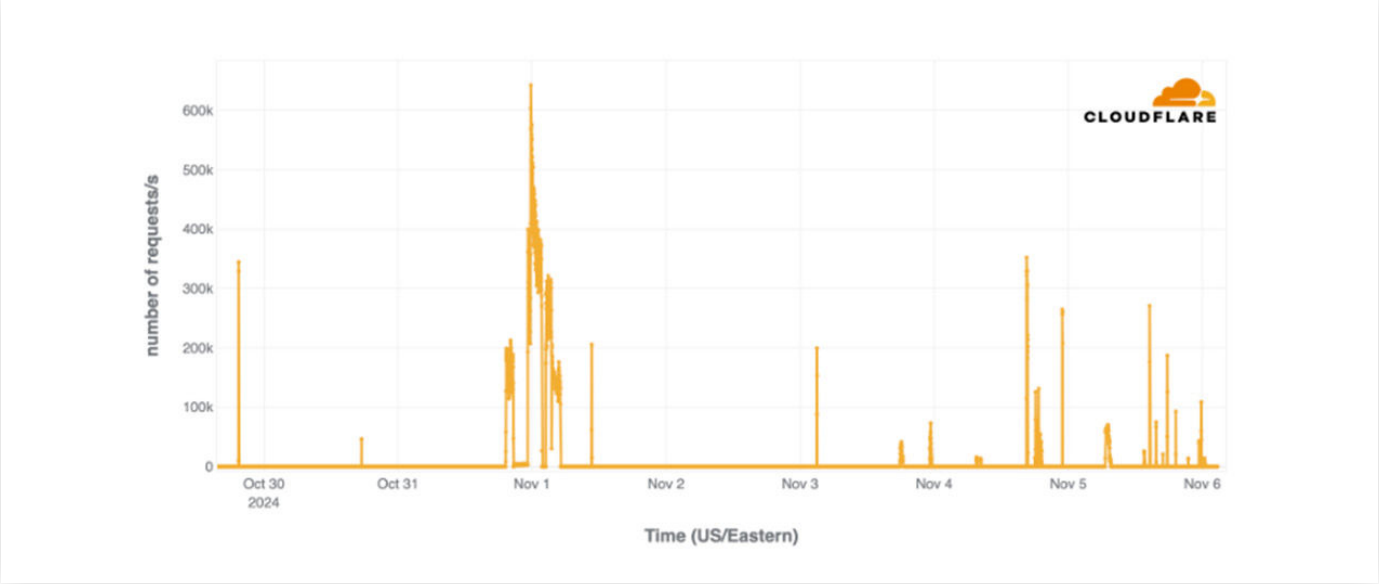
Politically motivated DDoS attacks typically aimed to destabilize economies or disrupt financial support for the opposing side of a conflict.

During Electoral Cycles

The impact of DDoS on election-related processes was significant throughout the year, with voting websites and systems serving as the primary targets as hackers attempted to impede voter access. Earlier in 2024, we saw surges of DDoS activity around events such as the presidential elections in Taiwan in January and the EU parliamentary elections in June. In Q4, this pattern repeated itself. For example, there was an uptick in DDoS attacks – some of which were significant, but none of which caused disruption – immediately prior to the US presidential elections.



CISA and FBI Relate to Potential DDoS Attacks on Elections (Source: America's Cyber Defense Agency)



Application-layer DDoS Attacks Target a U.S. Election-related Campaign Website, Oct. 29 to Nov. 6 (Source: Cloudflare)

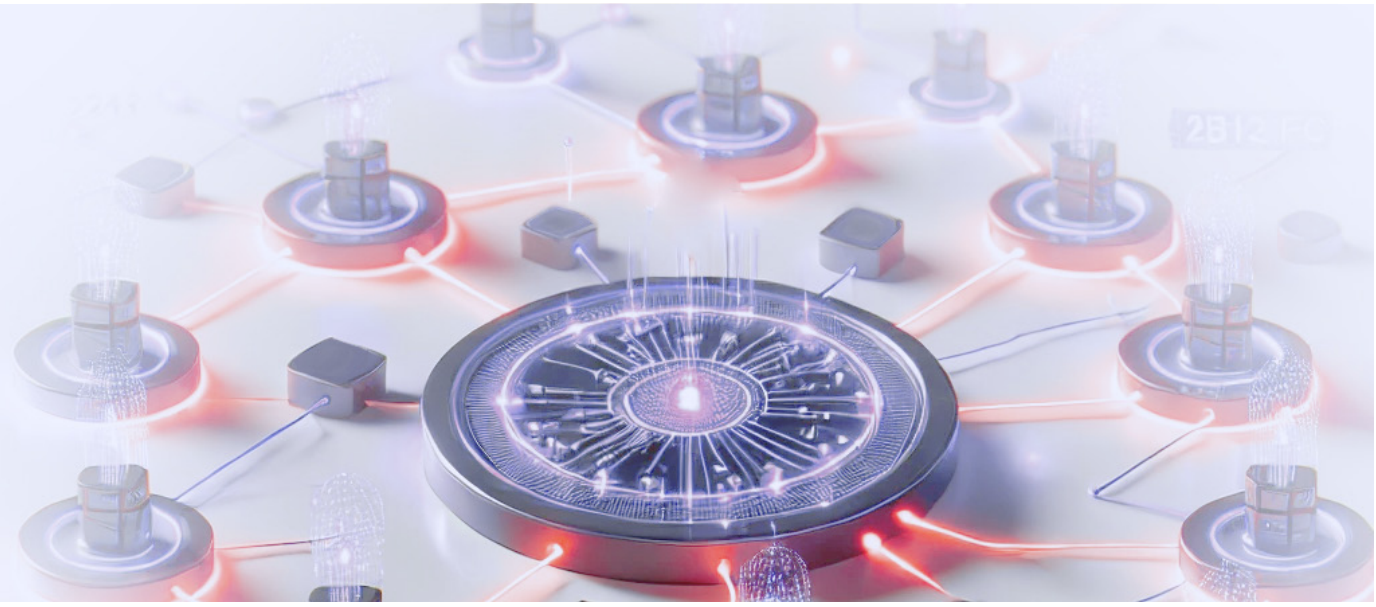
Matrix Botnet Highlights Increased IoT Risk

In November, Matrix emerged as a significant cyber threat actor. Matrix orchestrates widespread DDoS attacks by exploiting misconfigurations and vulnerabilities in Internet of Things (IoT) devices. Primarily leveraging Mirai malware, the widespread campaign creates a botnet using public scripts and brute-force attacks, and by exploiting weak credentials in IoT devices to compromise devices such as IP cameras, DVRs, routers, and telecom equipment. The fact that Matrix focuses on IoT devices highlights the growing concern over IoT device security.

Matrix orchestrates widespread DDoS attacks by exploiting misconfigurations and vulnerabilities in IoT devices.

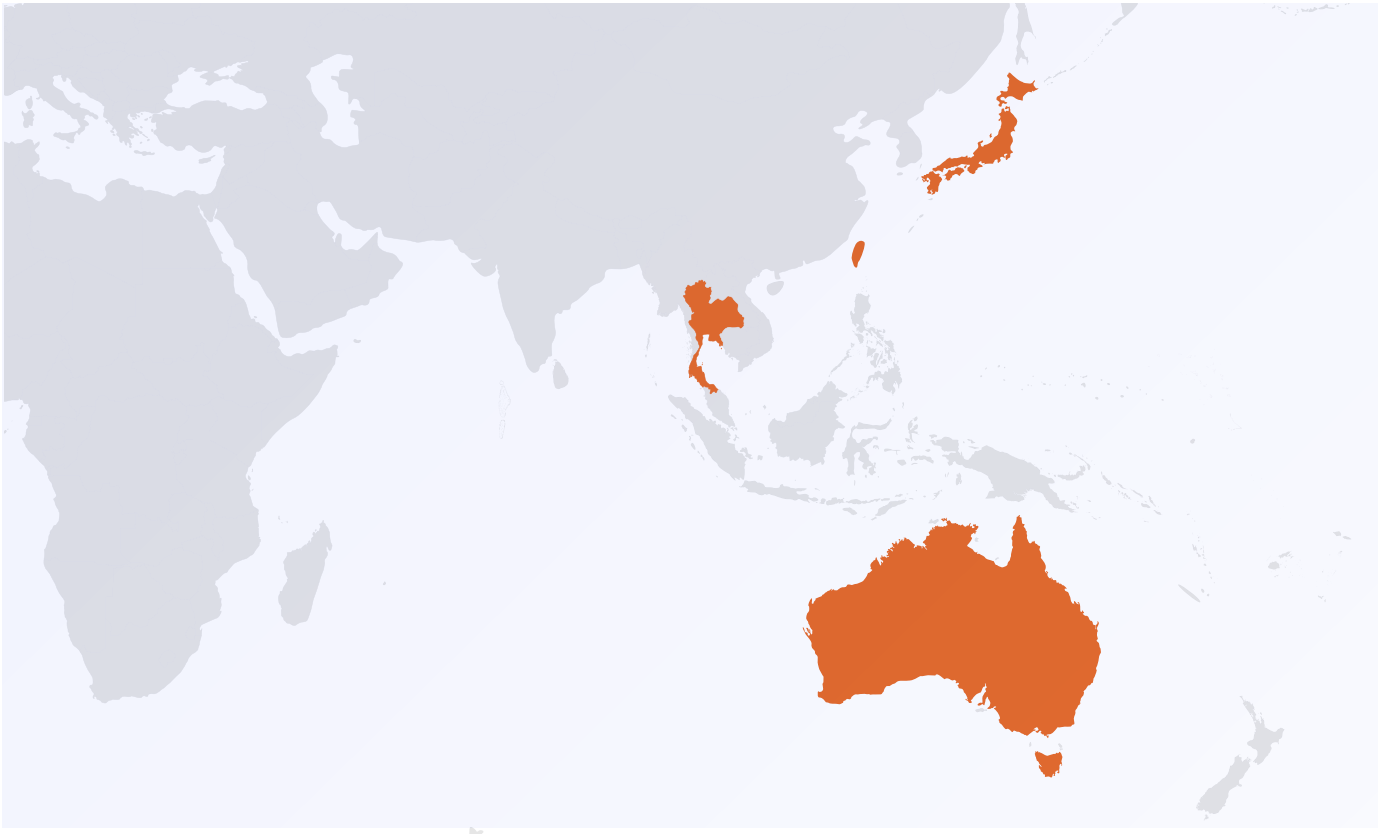
IoT devices often have persistent vulnerabilities stemming from inadequate security measures such as outdated firmware or default and poorly configured credentials. Exploiting IoT devices in DDoS attacks causes large-scale disruption globally – taking down targeted services as well as posing broader risks both to critical infrastructure and to the public safety.

IoT botnets are a growing threat that exploits two main security issues: First, the enormous number of IoT devices accessible over public Internet; and second, the fact that security considerations typically are an afterthought when it comes to IoT device architecture.



Rise in Telecom and Internet Infrastructure Attacks

Q4 saw an increase in the number of DDoS attacks on telecom companies and Internet infrastructure, particularly in the Asia-Pacific region. These attacks didn't necessarily make the headlines, but researchers identified a surge in DDoS activity taking place in the APAC region - specifically in Japan, Thailand, Australia, and Taiwan.



Researchers Note Rising Attacks in APAC on Telecom & Internet Infrastructure

As a case in point, the largest DDoS attack on record took place during the week of Halloween, on October 29 – when a 5.6 Tbps UDP DDoS attack launched by a Mirai-variant botnet targeted an Internet service provider (ISP) from Eastern Asia.

Drill-Down:
Top DDoS Threats in Q4 2024

October 2024

Date	Location	Vertical	Targets	Attacker	Headline
Oct. 7 & 8	Belgium	Government	Municipalities and Ports	NoName057	Link
Oct. 9	United States	Nonprofits	Internet Archive	SN_BLACKMETA	Link
Oct. 14	Latvia	Media	Novaya Gazeta Europe	North Korean Hackers	Link
Oct. 15	Japan	Government	Liberal Democratic Party and Local Government Websites	NoName057 and Cyber Army of Russia	Link
Oct. 18	Cyprus	Banking, Transportation, and Critical Infrastructure	Hermes Airport; Bank of Cyprus; Cyprus Electricity Authority, (EAC); Cyprus Telecommunications Authority (CYTA); Fuel Company EKO Cyprus Limited	LulzSec Black	Link
Oct. 29	Israel	Financial Services	SHVA	N/A	Link
Oct. 30	United Kingdom	Government	Burnley Council	N/A	Link
Oct. 31	Russia	Banking	Four Banks of the Russian Federation Located in Crimea	Main Intelligence Directorate (GUR) of the Ministry of Defense of Ukraine	Link

November 2024

Date	Location	Vertical	Targets	Attacker	Headline
Nov. 1	United Kingdom	Government	Portsmouth City Council in Hampshire	NoName057	Link
Nov. 5	South Korea	Government	Defense Ministry	N/A	Link
Nov. 10	Israel	Financial Services	Hyp's CreditGuard	Iran-linked Hacker Group	Link
Nov. 5	Singapore	Healthcare	Hospitals and Polyclinics	N/A	Link
Nov. 26	Global	IoT Devices	Cloud Service Providers (CSPs) and Smaller Enterprises in IoT-heavy Regions like China and Japan	Matrix	Link

December 2024

Date	Location	Vertical	Targets	Attacker	Headline
Dec. 3 & 5	Germany	Software Services	Encrypted Email Service Tuta	N/A	Link
Dec. 5	Russia	Banking	Gazprombank	Cyber Specialists from Ukraine's Military Intelligence (HUR)	Link
Dec. 7	France	Government	50 Attacks on Government Offices, Municipalities, and Private Organizations (including AXA)	Holy League, a Broad Alliance of Pro-Russian and Pro-Palestinian Hacker Groups	Link

Date	Location	Vertical	Targets	Attacker	Headline
Dec. 9	Australia	Government, Transportation, and Financial Services	Over 60 attacks on Australian Government Institutions, Transportation, Financial, Legal, Educational, and Insurance Sectors	Pro-Russian Groups, including NoName057, the Cyber Army of Russia Reborn, and Z-Pentest	Link
Dec. 26	Japan	Transportation	Japan Airlines	N/A	Link
Dec. 27	Japan	Banking	MUFG Bank	N/A	Link
Dec. 28	Italy	Government	Ministry of Foreign Affairs, the Turin Transport Group, and the Linate and Malpensa Airports	NoName057	Link
Dec. 30	Japan	Banking	Resona Bank, Mizuho Bank	N/A	Link
Dec 30	Russia	Oil	Lukoil Oil, Evotor Smart Terminals and Digital Goods Labeling System Chestny Znak	Defense Intelligence of Ukraine (DIU)	Link

About MazeBolt

MazeBolt RADAR™ is a patented solution addressing the highly vulnerable DDoS protection market. Without affecting online services, through ongoing nondisruptive DDoS attack simulations, RADAR continuously identifies and enables remediation of DDoS vulnerabilities that lead to damaging downtime. Global enterprises trust RADAR to proactively prevent damaging attacks, eliminating reliance on reactive manual responses or SLA guarantees. With its unique technology, RADAR provides unparalleled visibility into defense configurations, empowering organizations to prevent attacks entirely and maintain uninterrupted business continuity. Learn more at www.mazebolt.com

MAZEBOLT