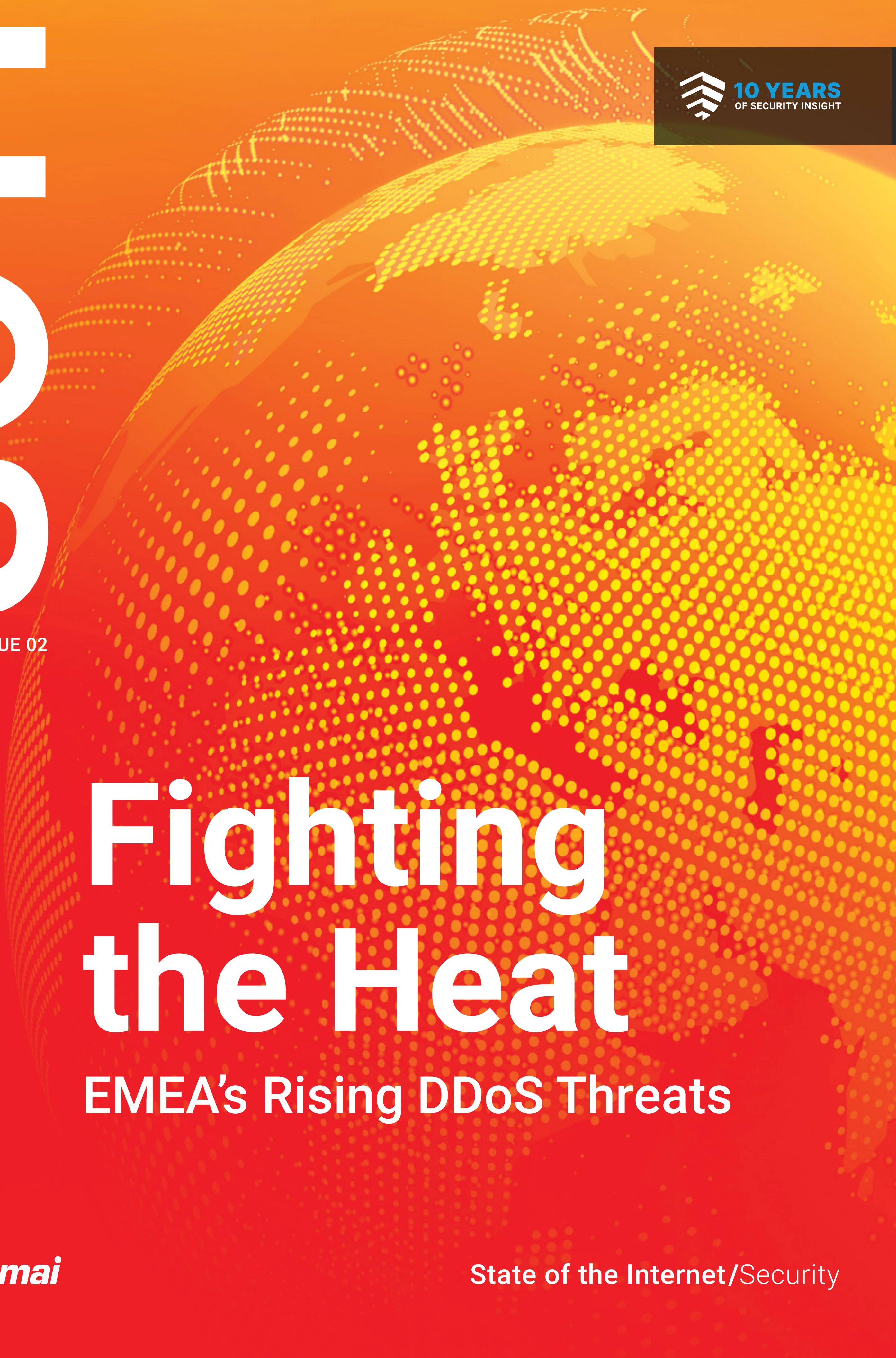


SOTI

V10 ISSUE 02

10 YEARS
OF SECURITY INSIGHT

Fighting the Heat

EMEA's Rising DDoS Threats

Akamai

State of the Internet/Security

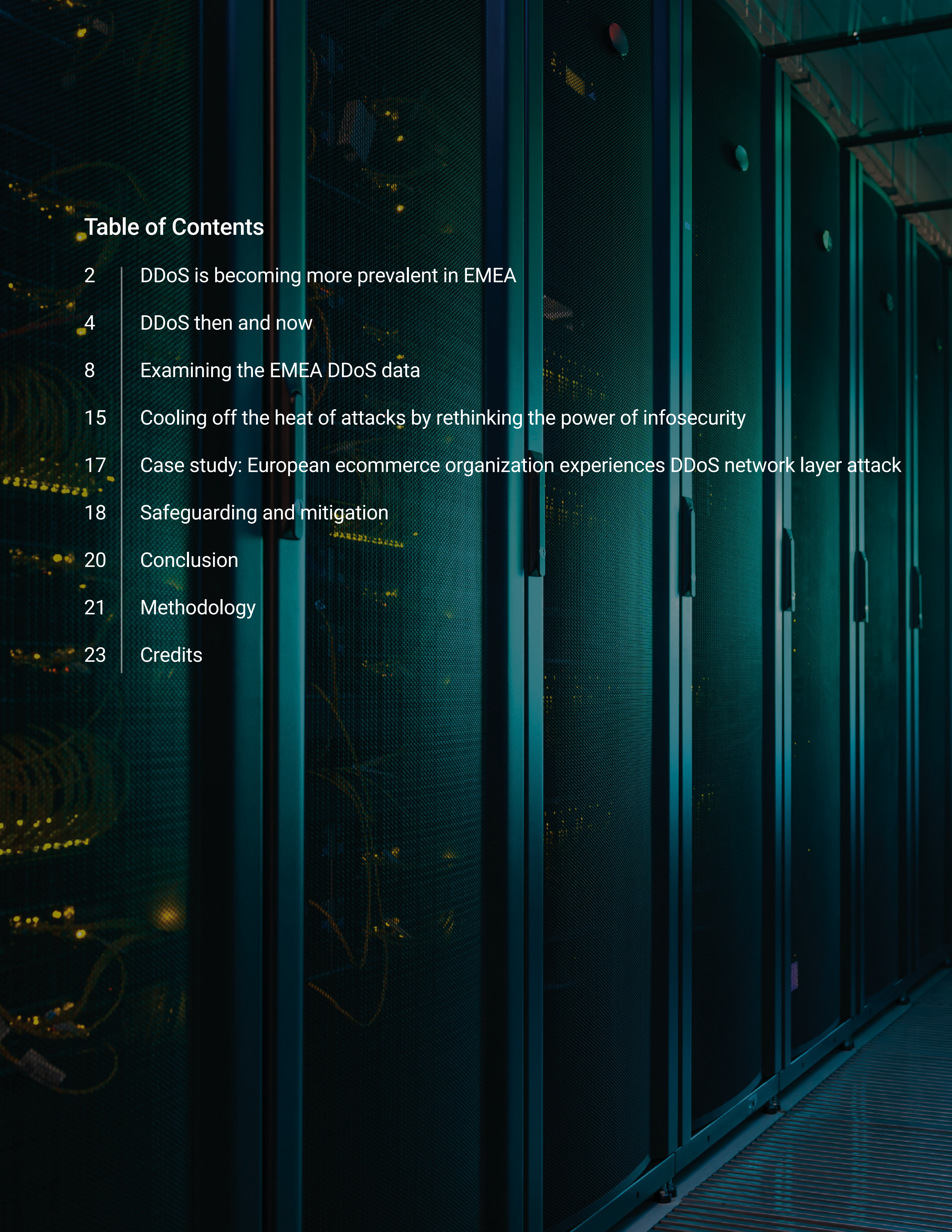


Table of Contents

2 DDoS is becoming more prevalent in EMEA

4 DDoS then and now

8 Examining the EMEA DDoS data

15 Cooling off the heat of attacks by rethinking the power of infosecurity

17 Case study: European ecommerce organization experiences DDoS network layer attack

18 Safeguarding and mitigation

20 Conclusion

21 Methodology

23 Credits

DDoS is becoming more prevalent in EMEA

Distributed Denial-of-Service (DDoS) attacks are surging in global volume and growing in sophistication. This surge is especially apparent in Europe, the Middle East, and Africa (EMEA), where Akamai researchers observed a dramatic upward shift in the rate of growth of DDoS attacks; in fact, the rate of DDoS attacks in the region is increasing even more rapidly than in other regions. DDoS attacks affect targets with unwanted malicious traffic and hinder the operations of networks and websites in EMEA.

Our conjecture is that much of this regional shift is due to geopolitical tension — such as nation-state activities and hacktivism in response to ongoing wars, including the Russia-Ukraine and Israel-Hamas wars. And upcoming high-profile events and elections in Europe are likely to elevate the risk of DDoS attacks even further. While the magnitude of EMEA DDoS events is quite large and growing, we've also witnessed a rise in both the number of DDoS attack vectors employed by cybercriminals and the length of those attacks.

In this State of the Internet (SOTI) report, we examine the nature and frequency of DDoS attacks in the EMEA region and explore some of the top verticals impacted by them, including financial services, commerce, and healthcare. We also take a closer look at new EMEA legislation designed to strengthen protection against the rise of cybersecurity threats in the region, and we provide mitigation and safeguarding techniques that work together to fight the increasing heat of EMEA's rising DDoS threats.

Key insights of the report

- Akamai researchers observed that the number of DDoS attack events in EMEA has been continuously rising, with higher peaks, since the beginning of 2019.

- More than one-third of all DDoS attack events globally are in the EMEA region.

- The complexity and severity of DDoS attacks in the EMEA region have been transformed by geopolitical motives, such as hacktivism, with the potential for life-threatening consequences.

- Of all the DDoS attack types, the DNS DDoS are among the most prevalent, according to Akamai research. Specifically, we observed the NXDOMAIN (nonexistent domain) vector, also known as the Pseudo-Random Subdomain vector, flooding DNS nameservers with requests for nonexistent domains.

- More than one-third of DDoS events used multiple attack vectors — as many as 12 — to increase success.

- In EMEA, the vertical with the highest number of Layer 3 and Layer 4 attacks is financial services; for Layer 7 attacks, it's commerce.

- EMEA governments and nations have been rethinking the power of infosecurity by enacting new legislative measures, such as NIS2 and DORA, to help positively influence IT and cybersecurity strategies, including better resilience and protection against DDoS.

DDoS then and now

DDoS attacks, whether deployed by individuals or botnets, flood servers with requests and overwhelm them with traffic, which leads to the hosted services and sites being unavailable for users and visitors.

DDoS attacks have evolved from the period in which open-source tools were used by threat actors to conduct them. For this group, motivation was often simplistic — perhaps they were dissatisfied with the newest game feature, hoping to gain a competitive edge, or just looking for sport. In general, this group of threat actors did not dominate the attack landscape with trends of targeting critical infrastructure or hospitals, nor with aiming to severely damage networks or endanger human life.

Hacktivism changed the landscape dramatically, both in terms of the threat actors' identities and their motivation. While some hacktivist attacks may have only limited or nuisance-level impact, others target commercial industry for significant financial gain and may cause service outages that last for days. Attacks can have potentially life-threatening consequences, as seen in some healthcare center attacks.

The ability to conduct DDoS attacks has become simpler over the past few years, with the emergence of services such as DDoS booter services, that allow even the most unsophisticated adversary to launch an attack with just a click of a button and for a nominal fee — sometimes as low as €10. These simple attack launches then lead to a plethora of traffic, which forces entire websites and networks offline, harming businesses both financially and operationally and depriving customers and users of crucial services.

Zooming in with the geopolitical lens

DDoS is a popular tool of politically motivated hacktivists and nation-state–sponsored attackers alike. For example, in the ongoing cyber war between Ukrainian and Russian actors, DDoS incidents play a significant role, as hacktivists have found these low-cost attacks to be quite effective.

In early 2022, Akamai began to support the Ukraine government in the fight against cyber warfare by defending 20 different government entity web resources. This included the URL president.gov.ua, which had been the most attacked site and was observed to have high-volume DDoS peaking at 1 million malicious requests per second.

Hacktivists like Anonymous Sudan, NoName057(16), and Killnet have been making headlines since Russia invaded Ukraine in February 2022. Killnet was the first of these groups to emerge, and began activity sometime around October 2021 by offering DDoS-for-hire services. Killnet has attacked government agencies, the healthcare industry, media companies, and others they consider to be allies of Ukraine.

NoName057(16) is believed by many threat researchers to support Russia and has been observed widely using HTTP-based (Layer 7) DDoS attacks. In early 2023, the pro-Russian group Anonymous Sudan began using DDoS attacks against entities in Denmark, Sweden, the United States, and other countries. In June 2023, many threat actor groups, including ReVIL, Killnet, and Anonymous Sudan, turned their attention to critical banking infrastructure, leveraging the chaos brought on by the Russia-Ukraine war.

More recently, Anonymous Sudan claimed responsibility for the attack on France's Telegram messaging app as part of the unprecedented DDoS attack on the country's state inter-ministerial network, causing the disruption of more than 17,000 IP addresses and devices and 300+ domains. It is believed that this attack on French government websites and services was likely in response to the February 26, 2024, announcement made by French President Emmanuel Macron about the possibility of sending French troops to Ukraine.

The conflict between Ukraine and Russia isn't the only battle that is causing a surge of DDoS attacks in EMEA. The Israel-Hamas war has led to increased attacks as well. Anonymous Sudan has claimed responsibility for DDoS attacks on Mossad, Israel's national intelligence agency, as well as on the Israeli prime minister's website and Facebook accounts and on pro-Israeli sites connected to the escalation of conflict in the Red Sea. NoName057(16) has also attacked Israeli websites in response to this conflict.

Tripling up

Historically, ransomware attacks encrypted a victim's data, making it unusable unless a ransom was paid. Double extortion attacks came next; they increased the damage to victims, with criminals making a copy of the victim's data before encrypting their network, and threatening to publish or sell it unless the ransom was paid. A third attack type — triple extortion — emerged soon after. In these attacks, the threat actor uses DDoS to hinder the victim's business in addition to the other two tactics. These triple extortion attacks are often referred to as Ransom DDoS, or RDDoS.

DDoS is a common element in extortion attacks, either as a smokescreen to distract infosecurity teams while the hackers try to intrude the systems, or to increase the pressure on the victim. Using multiple attack vectors increases the chances that a victim will pay a demanded ransom. One of the first recorded triple extortion attacks occurred in a Finnish psychotherapy clinic, Vastaamo, in October 2020 and occurred as Europe was hurrying to find ways to better share health data across the European Union.

Healthcare continues to be a main target for threat actors that use triple extortion attacks. One example is the ransomware group NoEscape, which emerged last year from the defunct Russian-speaking group Avaddon and targets healthcare organizations. And some cybersecurity firms are already preparing for more groups to target healthcare in the future.

Also, the Russia-based ransomware group LockBit was said to have run the world's biggest and most harmful ransomware operation as of February 2024, triggering destruction that cost billions of euros. Europol and Eurojust teamed up to coordinate an international task force known as Operation Cronos to take down LockBit. Operation Cronos included arrests, warrants, indictments, and the confiscation of 34 servers in EMEA, Australia, and the United States. LockBit was known for experimenting with new methods for pressuring victims into paying ransoms, such as RDDoS.

Although there are other well-known groups using RDDoS such as Darkside, Lazarus, AvosLocker, and BlackCat, the impact of Operation Cronos against LockBit is significant because it's the first time that cyber law enforcement has been effective to this degree. The scope and scale of this takedown included the dismantling and taking complete control of a large ransomware group's infrastructure while it was still operational.

Hacking back: Using DDoS to fight DDoS

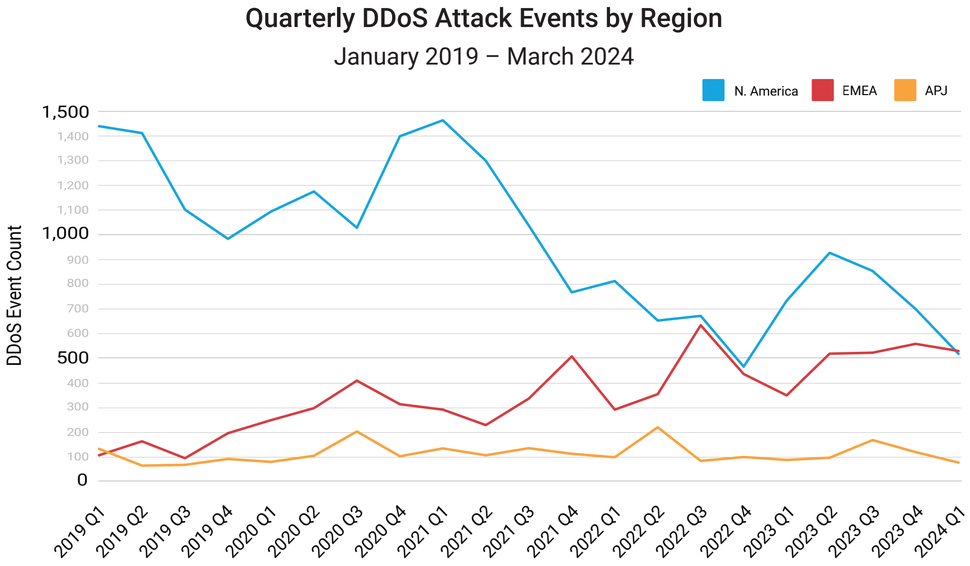
The concept of hacking back with offensive cyberattacks against cybercriminals has been a subject of debate for years. This strategy is thought of as either "a good offense is a good defense" (in the sense that it can protect companies from international threats) or is thought to set a dangerous precedent by allowing cybersecurity companies to launch DDoS attacks around the world and potentially destabilize state relations and escalate diplomatic tensions. Furthermore, regulatory ambiguities concerning counter cyberattacks, such as DDoS, raise highly complex legal questions.

As we know, LockBit used DDoS as part of their triple extortion attacks. Ironically, their use of this method was partly influenced by a DDoS attack that experienced themselves. The cybersecurity company Entrust was added to LockBit's list of victims in July 2022. In response, Entrust launched a DDoS counterattack that effectively crippled the darknet systems LockBit used to publish stolen data.

Counterattacks are also being used as a warfare tactic by some nation-states. Ukraine has been recruiting volunteers as part of an "IT army" of hackers from around the world that works to defend networks by hacking back; it's considered the first of its kind.

Examining the EMEA DDoS data

DDoS attack events have been on the rise globally, and this is especially true in the EMEA region. Akamai researchers have analyzed regional DDoS data and are seeing EMEA's DDoS attack event numbers moving at a steadier incline than any other region's numbers, including North America's, which leads overall (Figures 1a and 1b).


Quarterly DDoS Attack Events by Region

January 2019 – March 2024

Fig. 1a: EMEA's DDoS attack event numbers are increasing more steadily than any other region's numbers, including North America's

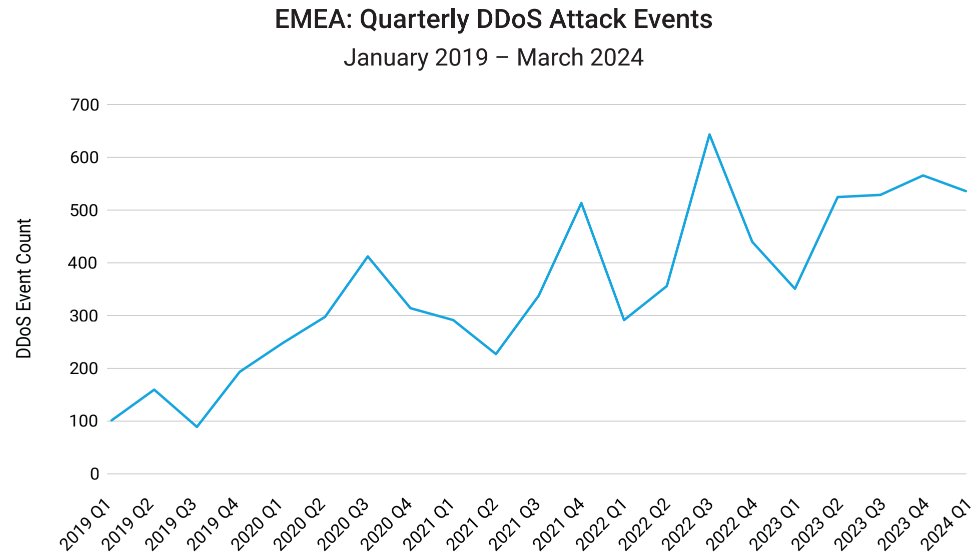


Fig. 1b: The growth of DDoS attacks in the EMEA region

Within the EMEA region, the United Kingdom (26%), Saudi Arabia (22.3%), and Germany (9.1%) lead the way for countries with the highest number of attack events. Also, Akamai's findings show that more than one-third of all DDoS attack events globally are in the EMEA region (Figure 2).

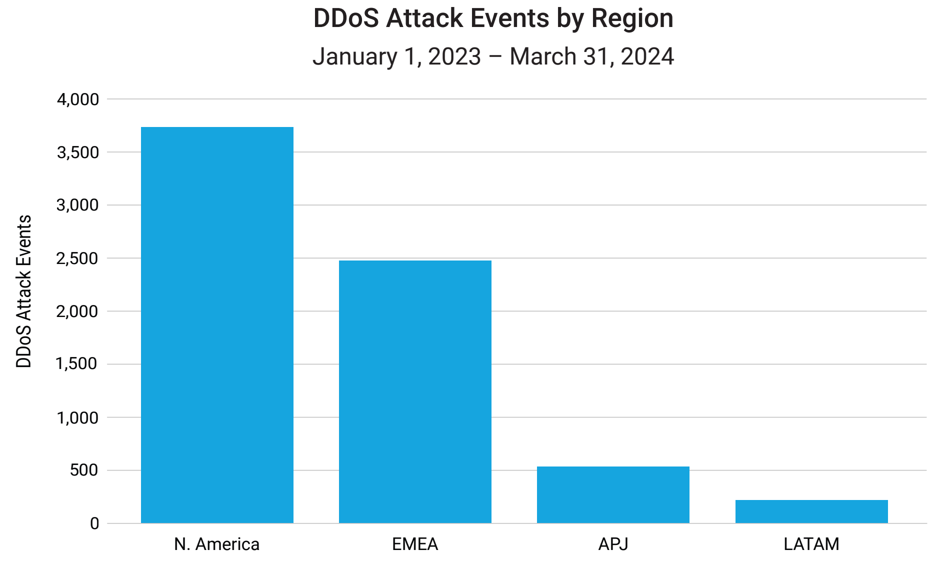


Fig. 2: The number of EMEA DDoS attacks climbed to nearly 2,500 from the beginning of 2023 to the first quarter of 2024 — more than three times as many as in the Asia-Pacific and Japan (APJ) and Latin America (LATAM) regions combined

In the financial services vertical, EMEA is the region with the most amount of DDoS Layers 3 and 4 attack event traffic (Figure 3). As mentioned earlier, Russian hacktivist groups declared their intention to launch DDoS attacks on the European banking system, and we surmise that the main reason for the rise in DDoS attack events in the financial services industry is this geopolitical hacktivism.

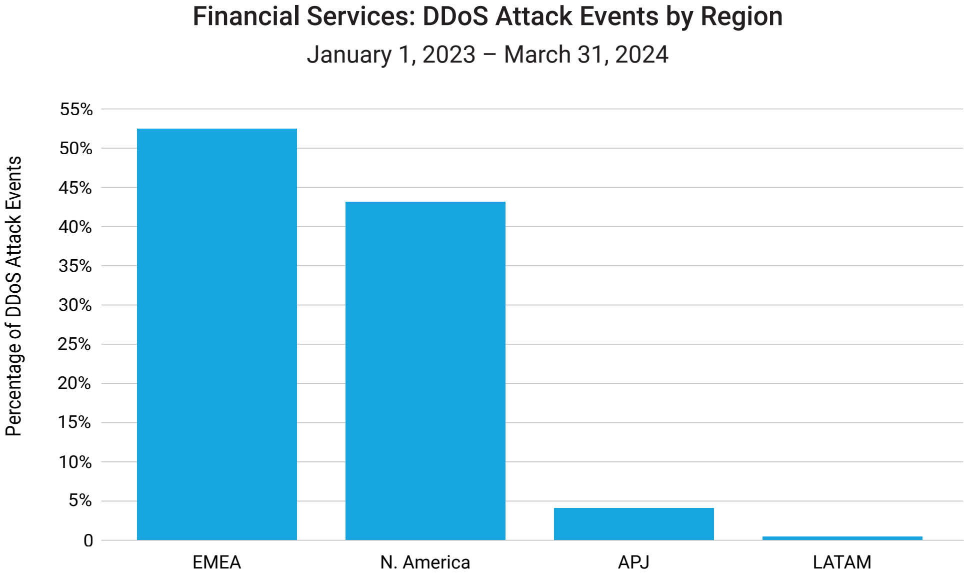
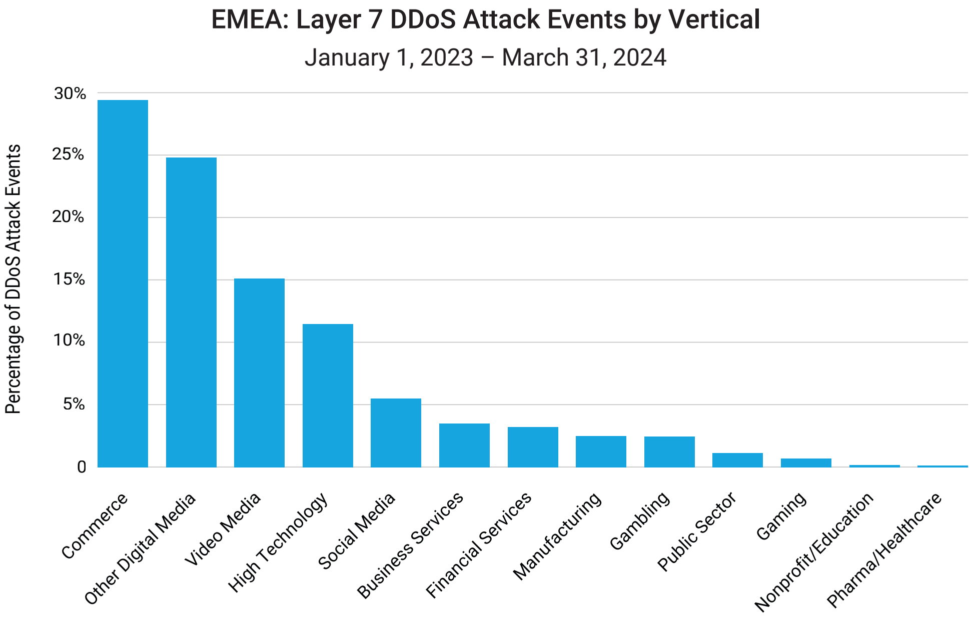


Fig. 3: EMEA experienced 52.5% of the regional DDoS Layers 3 and 4 attack event traffic in the financial services vertical

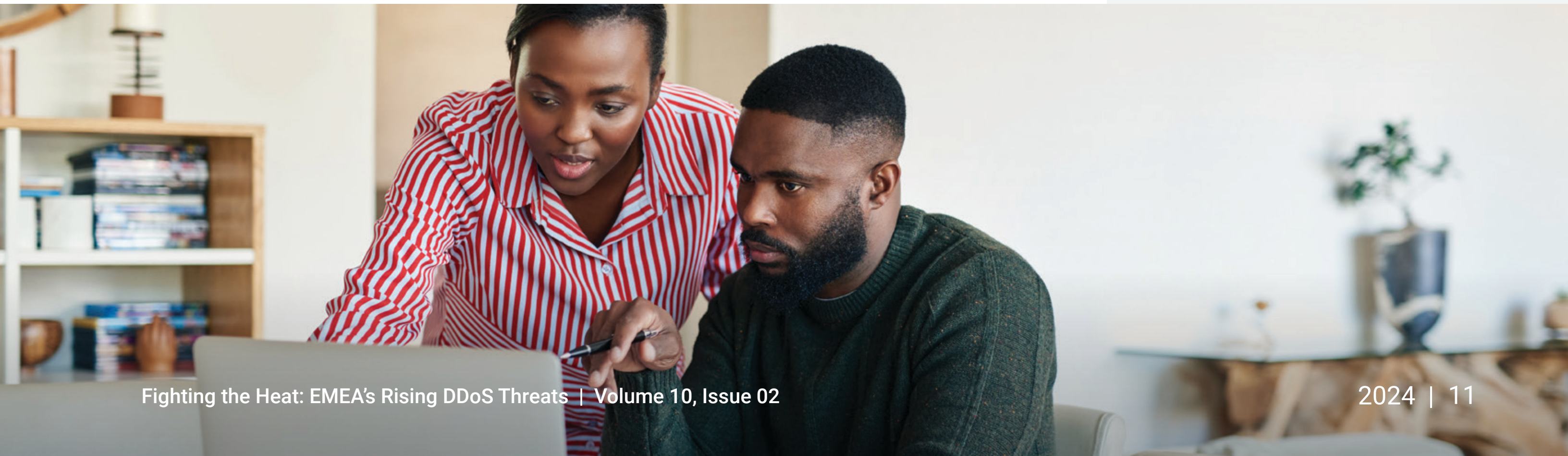
In addition to Layer 3 and 4 attacks, financial services applications are plagued by Layer 7 DDoS attacks. But the commerce vertical is seeing the largest increase in Layer 7 DDoS attacks in EMEA, experiencing almost 30% of all attacks in the region (Figure 4).


EMEA: Layer 7 DDoS Attack Events by Vertical

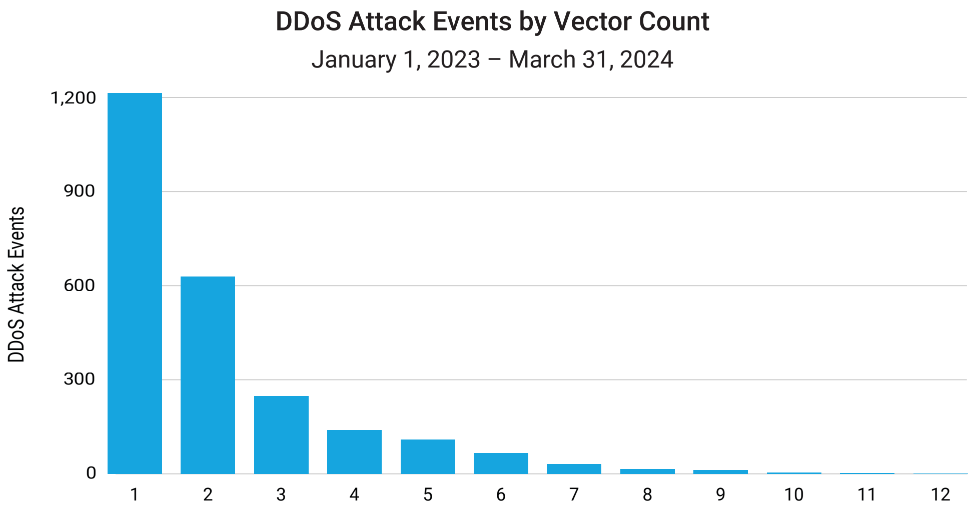
January 1, 2023 – March 31, 2024

Fig. 4: The commerce vertical experiences 29.4% of the regional DDoS Layers 7 attack event traffic in EMEA

It is possible that application-layer DDoS attacks, like those that employ HTTP flooding, may be highest in the commerce vertical because of the significant revenue disruption opportunity these attacks offer to threat actors. These types of attacks are especially crippling for commerce organizations because they can make an online store inaccessible or a reservation system unavailable, leading to a significant revenue loss for the victim company. Additionally, they may be deployed as a distraction tactic to consume incident response resources, while attackers aim to steal lucrative customer data (such as payment card information) from other areas in the victim's network.

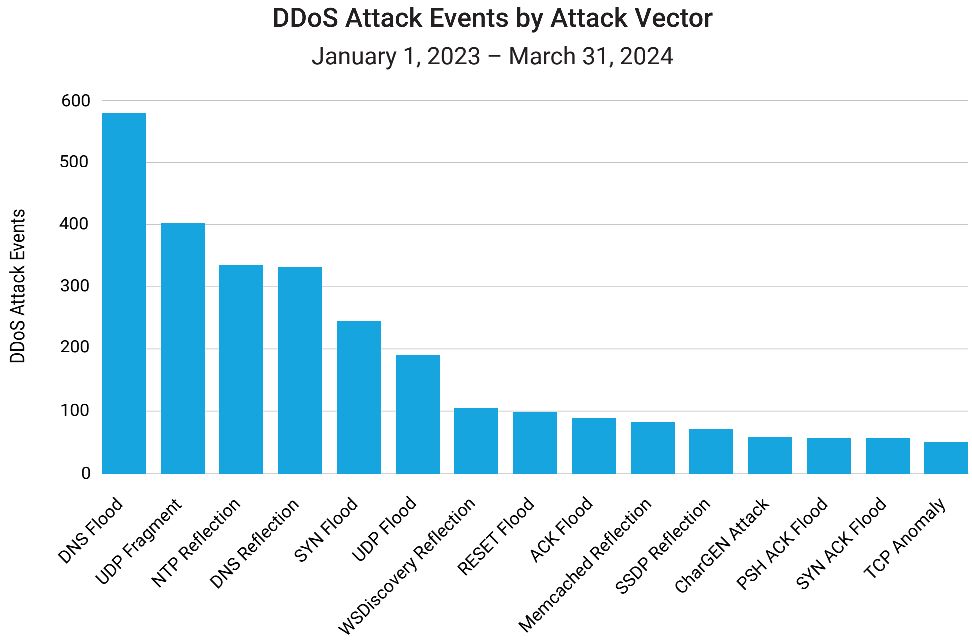


While DDoS attack event numbers have been on the rise, we have also observed that the number of vectors used to deploy DDoS attacks has increased sharply (Figure 5a). Those attack types include DNS Flood, UDP Fragment, and NTP Reflection (Figure 5b). Attacks have also been lasting longer.


DDoS Attack Events by Vector Count

January 1, 2023 – March 31, 2024

Fig. 5a: The number of vectors used to deploy DDoS attacks has increased sharply


DDoS Attack Events by Attack Vector

January 1, 2023 – March 31, 2024

Fig. 5b: EMEA's DDoS attack types include DNS Flood, UDP Fragment, and NTP Reflection

Prolonged attacks hinder productivity and the ability of operations to preserve continuity when other threats are found and responsive action is needed. DDoS techniques involving longer-lasting attacks and the use of more DDoS attack vectors are effective strategies for attackers, allowing them to better achieve resource exhaustion and overwhelm businesses' network security teams.

The newly trending DDoS target: DNS

Of all the DDoS attack types, those targeting the Domain Name System (DNS) are among the most prevalent (Figure 6). DNS is a popular target for DDoS attacks because of the impact malicious traffic can have on this critical and foundational service. A successful DNS attack has the potential to literally erase a company's presence on the internet.

What is a DNS DDoS attack?

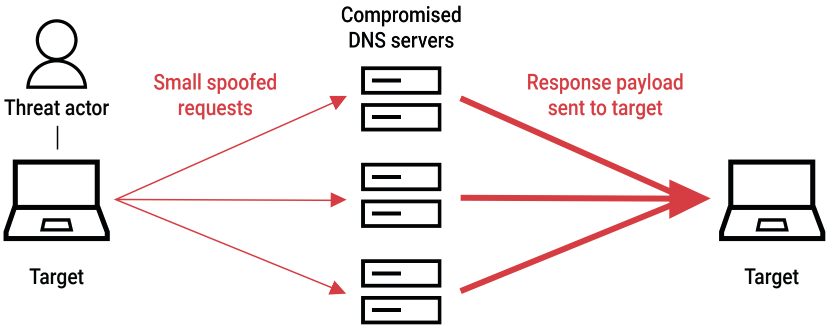


Fig. 6: A DNS DDoS attack compromises DNS servers with spoofed requests, causing an overwhelming response of payloads to the target

Specifically, the NXDOMAIN (nonexistent domain) attacks, also called Pseudo-Random Subdomain (PRSD) or DNS Water Torture attacks, have been observed flooding DNS infrastructure with requests for nonexistent domains. This type of attack aims to get to the origin name servers and cause high load on the systems — processing a request for a nonexistent domain is an involved task that consumes many processing cycles, ultimately exhausting the systems' ability to respond. We have seen many short attacks of this type, which typically are used to probe the victim's DNS infrastructure setup, only to return later with a refined attack in full force. According to research findings from our top 50 financial customers using Akamai Edge DNS, requests toward nonexistent domains made up almost 60% of their internet traffic in March 2024 (Figure 7).

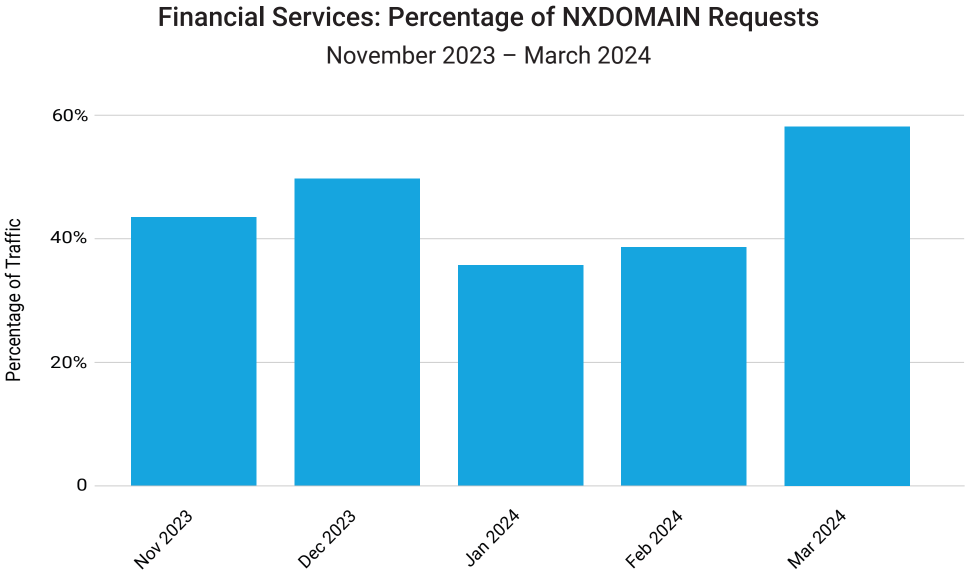


Fig. 7: Since the end of 2023, NXDOMAIN requests hit a peak in March 2024 with 58%

DNS Flood attacks are one of two main groups of DNS DDoS attacks. The other is DNS amplification attacks, which includes reflection attacks, and involves the spoofing of IP addresses created by the attacker to send a substantial number of DNS requests in an attempt to cripple the targeted machine's resources. Another incentive for the attacker to select DNS DDoS is the ease of execution since most of the traffic runs over User Datagram Protocol (UDP), which allows for spoofed IPs.

Cooling off the heat of attacks by rethinking the power of infosecurity

To combat and prevent the rise of cybersecurity threats (including DDoS) in the region, EMEA governments and nations have been rethinking the power of infosecurity. The changing landscape includes the new Network and Information Systems (NIS2) Directive and the Digital Operational Resilience Act (DORA) among other new legislative measures (e.g., the General Data Protection Regulation [GDPR], the Cyber Resilience Act [CRA], the European Programme for Critical Infrastructure Protection, etc.).

It's crucial for businesses to implement robust security measures and routinely evaluate their applications and networks to avoid and mitigate cyberattacks. This is especially important to protect against DDoS attacks since they do not allow much reaction time. Additionally, DDoS attacks tend to target less well-protected entities, which attackers identify through precise reconnaissance and testing. It is, therefore, important for organizations to establish efficient security procedures, as well as to have available business continuity and disaster recovery plans. Combined, the new legislative measures and directives may provide some safety guardrails for organizations.

The NIS2 Directive, which was adopted in December 2022 and repeals and replaces NIS1, aims to expand, strengthen, and harmonize implementation of the European Union's existing cybersecurity framework to respond to increased exposure of Europe to cyberthreats. EU member states have until October 17, 2024, to transpose the directive.

Procedures for the management of vendors, such as third parties, are also important. DORA is focused on EU financial services regulation and will be applicable starting January 17, 2025. In addition to promoting cyber resilience and helping EU entities in financial services deal with cybersecurity incidents, DORA provides guidance for third-party vendor management procedures. This assists financial entities by assuring that the information and communications technology (ICT) providers they contract with will comply with the appropriate information security standards. These are key components in DORA's five pillars model, which is designed to enhance cyber resilience for entities in financial services. The five pillars are risk management, incident reporting, digital operational resiliency testing, ICT third-party risk, and information and intelligence sharing.

Both NIS2 and DORA include guidance on strategies that leverage Zero Trust as a method of resilience. Trust and availability are crucial, especially in the online universe, and a DDoS attack can critically erode trust. Therefore, it is important that businesses follow appropriate safeguarding procedures, such as basic cyber hygiene. This concept includes the use of Zero Trust principles, which enact a more granular, context-aware access control mechanism that continuously verifies identity, device posture, and user behavior before granting access to sensitive resources. Additionally, the concept of least privilege is a key part of Zero Trust security practices and segments those users approved for access. Zero Trust solutions also help protect critical assets of organizations from RDDoS.

In addition to DDoS-related legislation, it is also important for organizations to be familiar with other existing legislation in the EMEA region that aims to tackle cyberthreats. For example, the European Union's new CRA targets software and hardware vulnerabilities that attackers increasingly leverage to infiltrate organizations and launch ransomware attacks. Also, the GDPR created obligations for all organizations that deal with personal data connected to European businesses and customers.

And outside the European Union, other countries are creating and enforcing their own controls. Saudi Arabia's National Cybersecurity Authority has introduced data protection laws similar to the GDPR, and Interpol's Africa Cybercrime Operations Desk has established programs such as the Africa Cyber Surge.

Case study: European ecommerce organization experiences DDoS network layer attack

Maintaining website uptime and resiliency is critical for any ecommerce organization to drive top-line revenue. That's why protecting web-facing assets and applications against DDoS attacks to prevent events that impact their business — and customers — is top of mind for security leaders. But what if the underlying infrastructure or the back-end systems that enable the order lifecycle were disrupted or taken offline completely? It's one thing for a customer to place an order, but if the order cannot be processed or fulfilled, successful operation could grind to a halt. That's what happened to an ecommerce organization in Europe when a network layer DDoS attack successfully targeted services within the data center where insufficient controls were in place.

Many threat actors commonly launch attack campaigns on weekends and holidays when fewer security personnel and incident response resources are available to remediate a threat. In the case of this European ecommerce organization, the DDoS attackers used a combination of SYN and UDP Flood attack vectors to target the organization's data center on a Friday afternoon and take down vulnerable corporate resources like company email. This prevented the transmission of important data to other parts of the organization, including fulfillment warehouses.

As a result, the logistics infrastructure was unable to operate and process any orders that were received from the ecommerce platform even though the logistics infrastructure itself was not impacted. Because the organization was unable to defend against the sustained level of volumetric DDoS attacks, Akamai was brought in to assist with an emergency integration to protect the retailer's corporate data centers. Within 24 hours, the customer was on the Akamai Prolexic platform and its connectivity to critical corporate services was restored.

The bottom line: Ecommerce organizations need to have a holistic approach to DDoS attacks that includes mitigation of Layer 7 (application) attacks and Layer 3 (network) and Layer 4 (transport) assaults to prevent downtime and to ensure resiliency across the entire order lifecycle.

Safeguarding and mitigation

Now that we've discussed the top DDoS trends and legislation in EMEA and provided some examples of attacks, let's look at what you can do to protect your organization. In addition to following the legislative measures mentioned earlier, including NIS2, DORA, GDPR, and CRA, and employing Zero Trust solutions, Akamai researchers recommend three actionable strategies to help combat the evolving DDoS landscape.

1. **Proactively prepare with a DDoS protection posture for your digital assets.** This includes:
   - Ensuring that mitigation controls are in place for all exposed IP addresses and critical subnets
   - Deploying DDoS security controls in an in-line protection posture
   - Ensuring that incident response plans and teams are up to date and designated
   - Backing up your on-prem DDoS protection with a hybrid protection platform to defend against attacks that overload on-prem appliances
   - Setting up proactive security controls through a network cloud firewall, as well as a web application firewall
   - Configuring rate limiting
   - Caching content on a CDN
   - Using a Security Operations Command Center team to ease the pressure on critical in-house resources

2. **Shield your DNS infrastructure.** If an entity's DNS falls, so does the entity's presence. A traditional DNS firewall may not provide adequate protection if the setup is managing zones both on-premises and in the cloud. In this case, a hybrid platform might be the optimal solution. Generally, to achieve a sufficient DDoS security posture, any traffic from the internet to your network should be scrutinized, and attack traffic mitigated and filtered out before it reaches your actual applications, APIs, and infrastructure, including your DNS.

3. **Don't rely on solutions that are "good enough."** It may seem simpler to use only the bare minimum protections based on requirements and budget. However, companies often find that this initial "savings" leads to a later loss that incurs more expenses and damages that drastically outweigh the pros of the original plan. It is, therefore, important to stress test your defenses from the perspectives of both best practices and technical solutions. This testing should include incident documentation, processes, runbooks, and more, to ensure that your solutions provide a robust level of cybersecurity.

Conclusion

The nature and impact of DDoS attacks have undergone significant transformations by becoming increasingly severe and complex.

The EMEA region has been particularly affected by this escalating DDoS landscape. Governments, financial services, commerce, and healthcare industries have all experienced a heightened number of these types of attacks. This regional shift can be attributed, in part, to the ongoing geopolitical tensions and conflicts in the EMEA area, which have fueled a rise in hacktivism and its associated DDoS activities.

Furthermore, the upcoming high-profile events and elections in Europe, including the European Parliament elections, the UK elections, and the Summer Olympic Games in France, are likely to elevate the risk of DDoS attacks even further. These events, which hold significant political and economic importance, may serve as prime motivations for malicious actors who seek to disrupt and influence proceedings through the use of DDoS tactics.

EMEA's legislators have been rethinking the power of infosecurity and enhancing security measures with new directives and regulations. Generally, businesses and organizations that abide by these regulations and have protective measures in place are less likely to be seen by cybercriminals as easy prey. DDoS attackers tend to aim at vulnerable targets that are not well protected, and threat actors are continuously conducting reconnaissance to discover which targets are easiest to exploit with DDoS. Because of the multitude of DDoS attack vectors and the many available paths among network, transport, and application layers, it is crucial to use a combination of solutions to provide full protection against DDoS. This kind of defense is essential for the best chance of success in fighting the heat of EMEA's rising DDoS threats.

Methodology

DDoS (Layers 3 and 4)

Akamai Prolexic Routed defends organizations against DDoS attacks by stopping the attacks and other unwanted or malicious traffic before they reach applications, data centers, and cloud and hybrid internet-facing infrastructure (public or private), including all ports and protocols. Experts in the Akamai Security Operations Command Center (SOCC) tailor proactive mitigation controls to detect and stop attacks instantly, and conduct live analysis of the remaining traffic to determine further mitigation as needed. These mitigated attacks are organized and grouped into attack events, and all the associated data is recorded by the SOCC to be analyzed.

This data in this report covered the 15-month period from January 1, 2023, to March 31, 2024, unless otherwise stated.

DDoS (Layer 7)

This data describes application-layer alerts on traffic seen through our web application firewall (WAF). The Layer 7 DDoS alerts are triggered when we detect volumetric anomalies in the number of requests to a protected website, application, or API. These alerts can be triggered by both malicious and benign requests. Typically, the requests themselves are benign, but the high volume of requests indicates malicious intent. The alerts do not indicate the successfulness of an attack. Although these products allow a high level of customization, we collected the data for this report in a manner that does not consider custom configurations of the protected properties.

The data was drawn from an internal tool for analysis of security events detected on Akamai Connected Cloud, a network of approximately 340,000 servers in more than 4,000 locations on nearly 1,300 networks in 130+ countries. Our security teams use this data, measured in petabytes per month, to research attacks, flag malicious behavior, and feed additional intelligence into Akamai's solutions.

This data in this report covered the 15-month period from January 1, 2023, to March 31, 2024.

DDoS (NXDOMAIN)

This data describes traffic seen through our edge network for 50 of our top financial services customers. The requests aimed toward NXDOMAINs are tracked and documented. These requests can be made with either malicious or benign intentions. In general, an increase in NXDOMAIN requests seen within a specific time frame and/or geography indicates malicious behavior. Our security teams use this data to research attacks, flag malicious behavior, and feed additional intelligence into Akamai's solutions.

This data covered the five-month period from November 2023 to March 2024.

Credits

Editorial and writing

Lance Rhodes – Editor in Chief
Susan McReynolds – Case Study Writer
Maria Vlasak – Copy Editing

Review and subject matter contribution

Christian Borggreen
Cheryl Chiodi
Sven Dummer
Jim Gilbert
Mitch Mayne
Richard Meeus
Craig Sparling
Carley Thornell

Data analysis

Chelsea Tuttle

Promotional materials

Annie Brunholzl

Marketing and publishing

Georgina Morales Hampe
Emily Spinks

More State of the Internet/Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet/Security reports. **akamai.com/soti**

More Akamai threat research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. **akamai.com/security-research**

Access data from this report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided that Akamai is duly credited as a source and the Akamai logo is retained. **akamai.com/sotidata**

More on Akamai solutions

To learn more information on Akamai solutions for DDoS attacks, visit our **Prolexic solutions** and **App and API Security** pages.

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn.
Published 06/24.