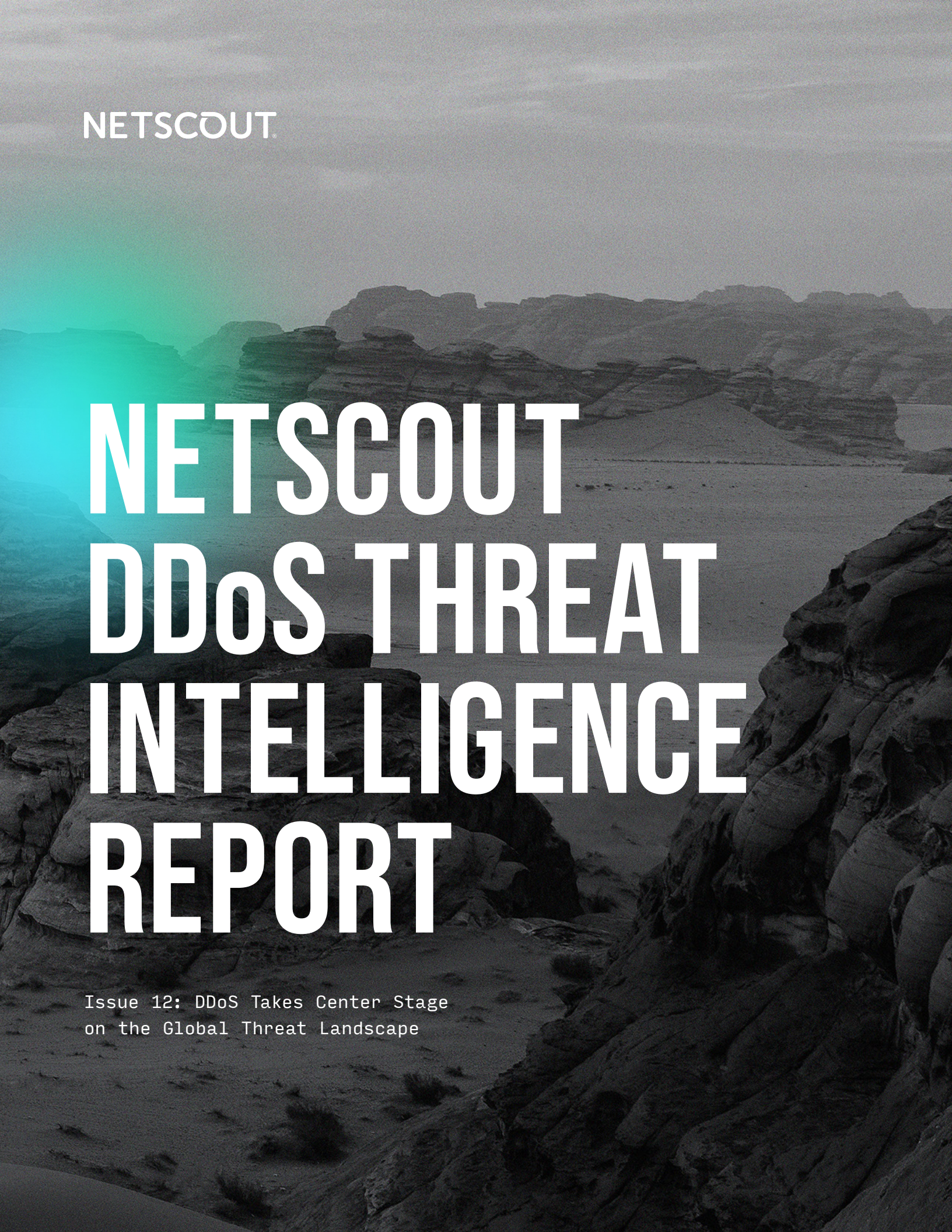


NETSCOUT DDoS THREAT INTELLIGENCE REPORT

Issue 12: DDoS Takes Center Stage on the Global Threat Landscape

DDoS Visibility

Imagine your website swamped, servers overloaded, and customers locked out—all thanks to a relentless distributed denial-of-service (DDoS) attack. This isn't a hypothetical scenario; it's a real and growing threat.

In 2023 alone, we observed: **13,142,840** DDoS attacks

This surge underscores a stark reality: Without proper DDoS protection, organizations are left scrambling in the dark, desperately trying to mitigate an attack that's already causing major damage. The repercussions of an unmitigated DDoS attack extend beyond mere inconvenience; they manifest in tangible crises. Critical hospital services, including scheduling, can grind to a halt, risking lives when seconds count. Businesses face not only significant financial hemorrhage but also erosion of customer trust that took years to build. And for network operators, the relentless barrage of DDoS threats creates a siegelike environment, with a constant state of security fatigue replacing the essential proactive stance needed to safeguard their digital assets.

Instead of playing defense at the last minute, imagine being one step ahead of attackers. With advanced DDoS protection powered by predictive and real-time threat intelligence, you can identify and prioritize threats before they impact network infrastructure. Such protection further allows organizations to react instantly and automatically mitigate attacks, minimizing downtime and disruptions. Ultimately, this allows for business continuity, ensuring customers and users have uninterrupted access to critical services. Investing in proactive DDoS protection transforms defense strategies from reactive to predictive. This frees security teams to focus on strategic initiatives, knowing they have a robust shield against online threats.

Gaining insight and visibility into the DDoS threat landscape is the first step down the road to predictive DDoS defense. Throughout this 2H 2023 DDoS Threat Intelligence Report, our ASERT team dissects trends and attack methodologies adversaries are deploying against service providers, enterprises, and end users and provides actionable recommendations on the needed steps for moving from reactive to predictive responses.

CONTENTS

All chart data derived from ATLAS

Multiple decades working with the world's largest service providers and enterprises grants NETSCOUT far-reaching visibility into the global internet, allowing us to discern the pulse of the digital world. Our capacity to monitor and respond to DDoS attacks is powered by our ATLAS telemetry platform that grants us insight into 500 terabits per second (Tbps) of network traffic. Such comprehensive coverage yields insights into a large majority of the DDoS attacks around the world (Figure 1).

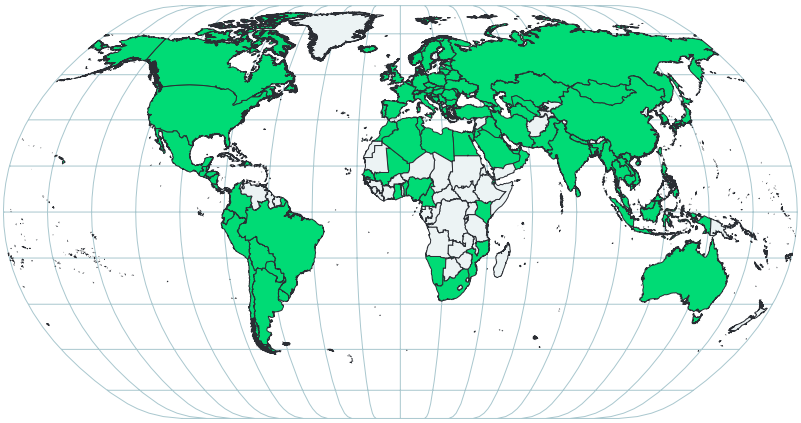


Figure 1: ATLAS Telemetry

Key Findings

Threats

The rise of tech-savvy and politically motivated DDoS hacktivism that transcends geographic borders, as exemplified by groups such as NoName057(16) and Anonymous Sudan in 2023, signifies a distinct shift in the global cybersecurity landscape. These groups demonstrate not only advanced technical prowess but also the ability to harness such skills for varied political agendas. This trend marks a new era in cyberattacks, profoundly impacting networks and organizations worldwide.

Targeting

Imagine an unseen world where a hidden epidemic of malicious activity thrives. Beneath the surface of normal internet traffic, analysis reveals a growing infection of DDoS attacks targeting authoritative and recursive Domain Name System (DNS) servers, the unsung heroes of the internet's infrastructure. From groups such as Lazarus Bear Armada (LBA) in 2019 to more successful operations run by Anonymous Sudan, DNS query floods can cause a domino effect, knocking systems offline that serve hundreds to thousands of websites. Massive industries such as gaming and gambling experience similar collateral damage when gaming servers, hosting tens of thousands of users, experience increasing waves of DDoS attacks.

Defense

A "sophistication gap" in DDoS attacks is becoming increasingly evident. On one end, advanced attackers employ custom tools and cloud infrastructure; on the other, some still use basic, often free services. This disparity demands quick and targeted responses to effectively safeguard against these evolving cyberthreats.

DDoS Threats

Active DDoS Attack Campaigns

One of the most significant shifts in the DDoS threat landscape is the continued onslaught of attacks from DDoS hacktivist groups bombarding websites and organizations around the world. Although the focus of a lot of these groups lies in EMEA due to geopolitical turmoil, the attacks absolutely reach across the world as surrounding countries and regions become invested in network infrastructure and services in affected areas. These groups require many different responses to properly defend against them, and just as doctors use precise tools to target specific illnesses, we must apply the same level of precision to DDoS threat actors. These threat actors, whether driven by money, beliefs, or politics, are experts at causing digital chaos. By keeping a close eye on them, we're better equipped to build up our defenses and keep our networks—and the organizations they support—safe and sound.

2023 was an exceptionally busy year for defenders as threat actors launched many DDoS attack campaigns against a variety of targets. NoName057(16) holds the top position with 780 targeted websites across 35 countries. EXECUTOR DDOS follows with 201 websites in 29 countries. Other notable groups include DDOS-V2, SYLHET GANG-SG, and the Russian Cyber Army Team. Anonymous Sudan ranks ninth, with 81 targeted websites in 17 countries (Figures 2 and 3).

Figure 2: Claimed DDoS Attacks by Adversary (2H 2023)

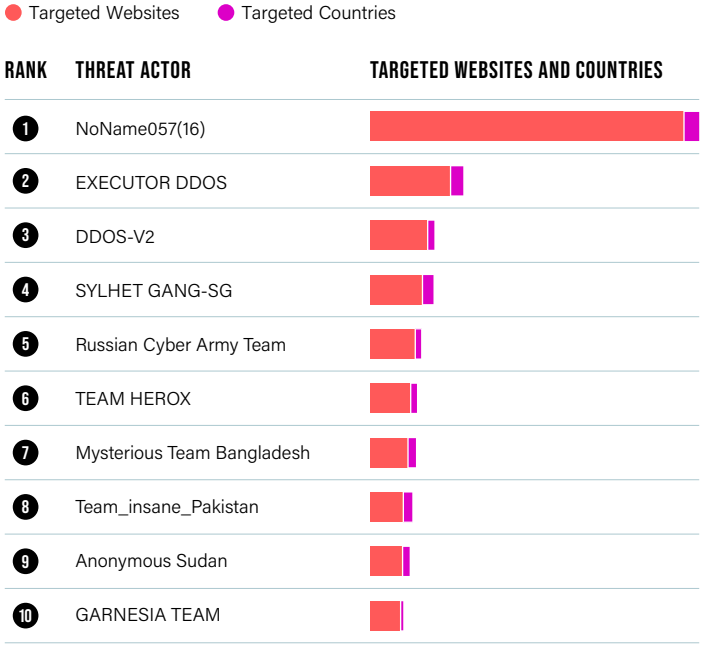
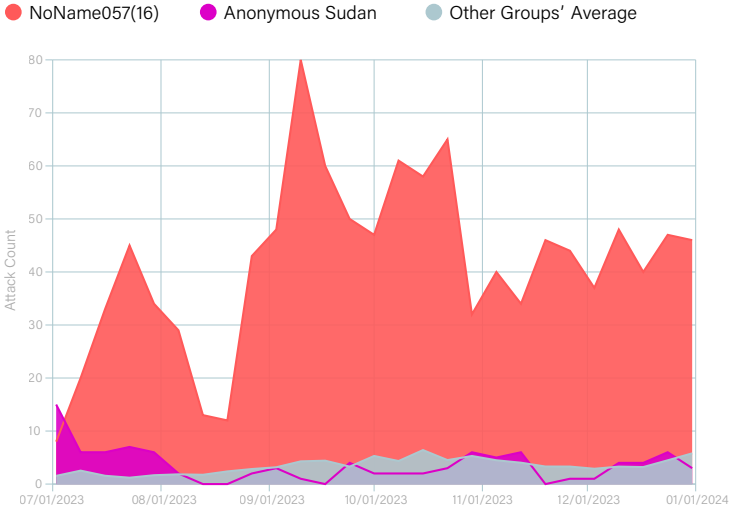


Figure 3: Claimed Threat Actor Activity Over Time (2H 2023)



In the second half of 2023, Anonymous Sudan was notably active in DDoS hacktivism, briefly outpacing NoName057(16) in terms of attacks. As of our latest review, NoName057(16) has regained its leading role, eclipsing all competitors. Meanwhile, Anonymous Sudan's activity has normalized, aligning with the general levels observed among similar groups. This fluctuation highlights the ever-changing landscape of cyberthreats, reinforcing the need for constant vigilance.

Anonymous Sudan

Anonymous Sudan has made a significant impact since its emergence in 2023. This group, with its pro-Russian leanings, has been notable for its number of attacks against a variety of targets, including major messaging platforms such as X (formerly known as Twitter) and Telegram. Interestingly, these attacks were driven by specific grievances: a push to influence Elon Musk regarding Starlink service in Sudan in the case of X, and retaliation against Telegram for suspending its primary channel.

Operating with the sophistication of a well-funded organization, Anonymous Sudan has also joined forces with the Killnet hacktivist network. Anonymous Sudan's global assaults, aligning often with Kremlin-friendly goals, strategically target high-demand services such as streaming platforms during peak usage times. Anonymous Sudan utilizes well-known DDoS attack vectors and methodologies effectively, resulting in significant impact against unprepared targets and making the group a formidable threat.

NoName057(16)

NoName057(16), a pro-Kremlin group, smashed onto the scene supporting Russia in the ongoing Russia-Ukraine conflict in early 2022. It made a name for itself with its custom malware, DDoSia, targeting NATO-aligned countries in response to perceived anti-Russia sentiments. The group's innovative use of gamification in cyberwarfare stands out, offering digital currency rewards to encourage volunteer participation in attacks. This strategy not only increases the scale of the group's operations but also showcases a unique way of mobilizing support in the digital sphere.

NoName057(16) leverages decentralized botnets and attacker infrastructure, predominantly utilizing public cloud and hosting services. This approach significantly reduces costs and risks. The group's preferred attack method, HTTPS-based application-layer DDoS, bombards sites with junk HTTPS requests, causing notable disruptions, especially in Eastern and Western European nations. In response to these evolving threats, it's imperative to adopt robust security measures.

ASERT ADVICE

To combat such threats, staying updated with real-time intelligence feeds is crucial. These feeds are vital, offering deep insights into DDoS tactics and sources of compromised traffic, and are an essential component of any robust DDoS mitigation strategy. They represent more than mere data; they are a critical line of defense in the constantly shifting landscape of cyberwarfare.

DDoS on the Geopolitical World Stage

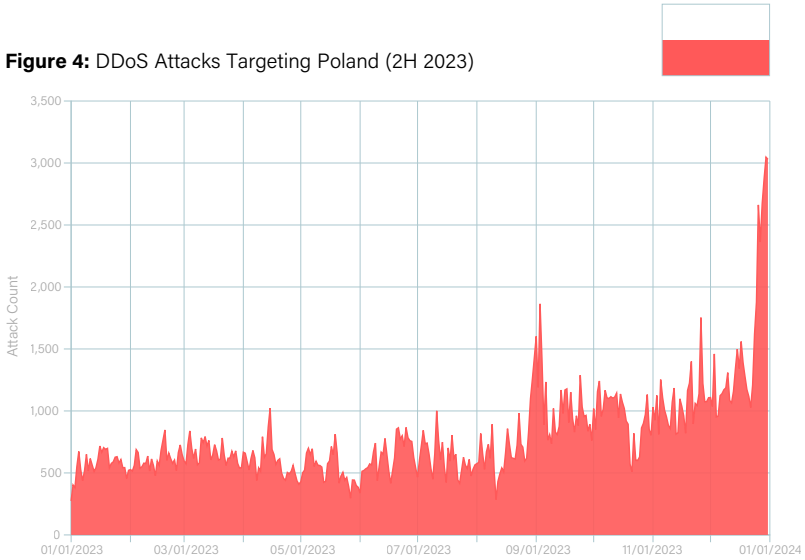
The activities of groups such as NoName057(16) and Anonymous Sudan demonstrate a growing trend in DDoS attacks driven not just by lone hackers or small collectives but also by politically motivated groups. These organizations increasingly are using DDoS as a tool to target those ideologically opposed to them, executing attacks that seamlessly transcend national borders.

Protesting with DDoS Attacks

DDoS attacks tend to escalate during periods of significant political unrest. For example, in mid-December of 2023, Peru experienced a 30 percent increase in attacks over an already-inflated doubling of attacks throughout the year. This spike came on the heels of a nationwide series of protests that coincided with the release of former Peruvian President Fujimori from prison on December 6.

In Poland, the average number of observed DDoS attacks surged at the end of 2023 to nearly quadruple the country's yearly average as it embarked on a transition of power out of the hands of the Law and Justice party, which had held power in government for the last eight years (Figure 4). Coupled with the regime change was a series of statements that reaffirmed Poland's support of Ukraine in the Russia-Ukraine conflict—a perfect storm for adversaries opposing this stance.

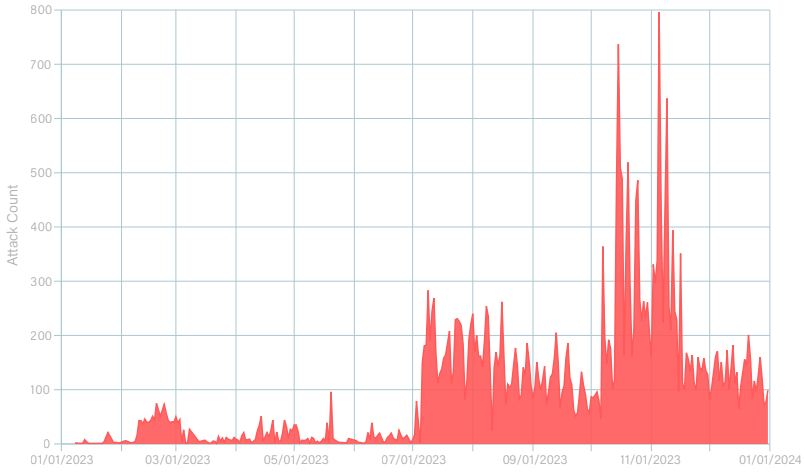
Figure 4: DDoS Attacks Targeting Poland (2H 2023)



International Conflicts Attract DDoS Attacks

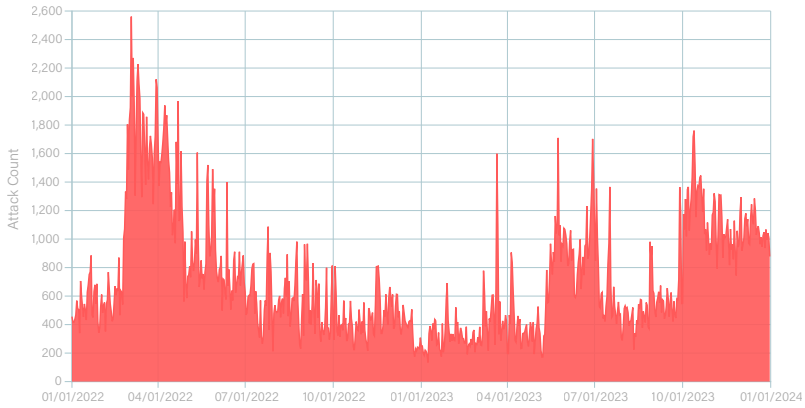
Of course, it's impossible to discuss DDoS being used in a geopolitical context without thinking of Russia and Ukraine, but more recent conflicts such as Israel and Palestine also attracted a flood of adversaries and DDoS attacks, with daily attacks increasing more than tenfold between the first and second halves of 2023 (Figures 5 and 6). Hacker groups such as NoName057(16), Anonymous Sudan, and Killnet have all taken credit for attacks launched during this time, with primary targets including communication infrastructure, hospitals, and banks. These international conflicts stand as glaring examples of how cyberattacks, particularly DDoS, have become a commonplace method for sowing chaos during significant political turmoil regardless which side of the political spectrum an adversary happens to align with.

Figure 5: DDoS Attacks Targeting Israel and Palestine — Combined (2023)



Russian-aligned hacker groups often claim to launch attacks to "punish" governments for sending aid to Ukraine. As they do so, they are more than willing to opportunistically co-opt local causes as well to justify their actions. For example, NoName056(16) launched a series of attacks on Spanish websites earlier this year. When explaining its actions, the attackers cited the Spanish government's support of Ukraine, but also claimed to support a group of Spain's firefighters that were protesting for improved benefits. Both the DDoS attack and these protests took place during an election year for Spain, demonstrating a clear willingness on the part of these hacker groups to attempt to place their thumb on the scales during election times.

Figure 6: DDoS Attacks Targeting Russia and Ukraine — Combined (2022–2023)



ASERT ADVICE

Understanding the motives behind these cyberattacks is important to comprehending their full impact. With the digital battlefield constantly evolving, it becomes increasingly critical to monitor and analyze the patterns of these disruptions to anticipate future threats and protect against them.

DDoS Targeting

Gaming Giants Experience Waves of DDoS and Triple Extortion

Politics and international conflicts are among primary motives in the DDoS threat landscape. But perhaps the most influential cause of DDoS attacks is that of gaming and the gambling associated with gaming. Our findings consistently show that the gaming sector is a prime target for these attacks, attracting a diverse range of threat actors globally.

The allure of attacking the gaming industry lies in its substantial financial value and the goal of disrupting competitors. The industry's heavy reliance on digital infrastructure and high-profile nature, often in the spotlight of media, heightens its vulnerability to DDoS attacks. A notable aspect of these attacks is their frequent occurrence during online gaming tournaments. Although these events are sometimes linked to the extensive gambling activities around them, it is the DDoS attacks themselves that pose the most significant threat. These attacks not only disrupt the gaming experience but also threaten the integrity and stability of the gaming industry's digital platforms, highlighting the critical need for robust cybersecurity measures.

In early 2023, a prominent multiplayer online gaming provider (Company A), experienced a multiphased cyberattack. The initial phase was a DDoS attack, which was more severe than any other attacks faced by the company throughout the year. This DDoS attack disrupted not only the online gaming services but also other critical operational services. Following this, Company A faced a series of additional cyberattacks (Figure 7). These culminated in a significant data breach and subsequent ransom demands, which were communicated to Company A via email.

This phenomenon is not isolated. Another notable online gaming company that operates a platform and game creation system enabling users to design, create, and play games made by others (Company B) experienced a volume of DDoS attacks nine times greater than the average seen across the global gaming industry (Figure 8). A key distinction in this scenario is the active user base participation in these DDoS attacks, despite such activities constituting serious crime in many regions, to gain competitive edges against other players. A brief internet search reveals an abundance of tools and methods specifically tailored to assist players in identifying competitors and launching basic DDoS attacks against them, which leads to Company B facing a constant onslaught of DDoS attacks.

The heightened frequency and sophistication of DDoS attacks in the gaming industry, as revealed by NETSCOUT's analysis, underscores the urgent need for robust cybersecurity measures. These attacks, targeting major online gaming companies, not only disrupt game play but also compromise critical operational and data security. Successfully defending against such attacks requires a comprehensive cybersecurity strategy involving advanced protection measures, user awareness, and industrywide collaboration to counter the growing threat. With the active participation of some users in these attacks for competitive advantage, the gaming industry faces the additional challenge of curbing the accessibility and use of DDoS tools. It is imperative that gaming companies, cybersecurity experts, and regulators unite and actively collaborate to combat the escalating threat of DDoS attacks. This concerted effort is essential not just for maintaining but also for strengthening a secure and fair gaming environment.

Figure 7: DDoS Attacks Targeting Company A (2023)

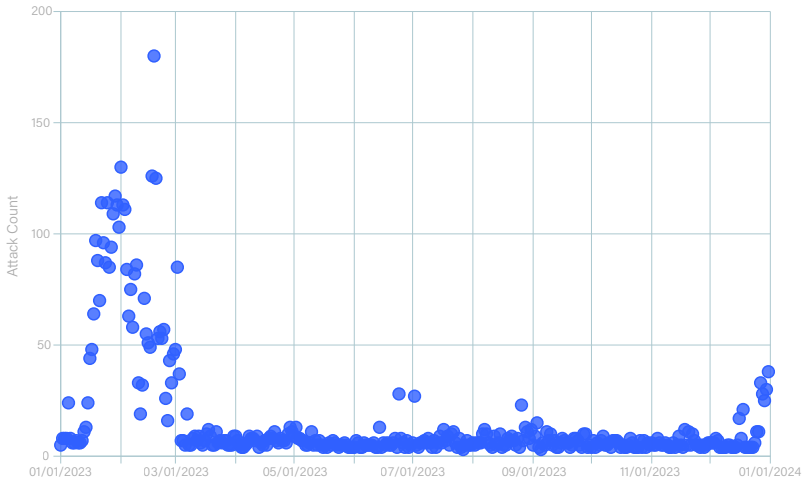
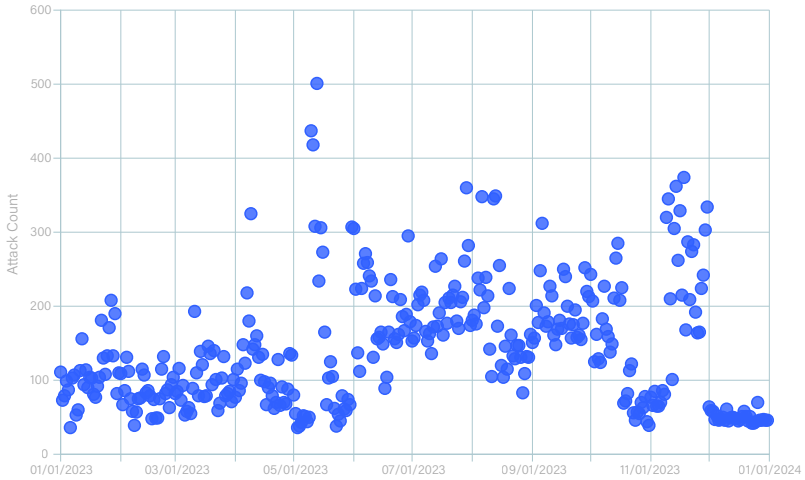


Figure 8: DDoS Attacks Targeting Company B (2023)



DDoS ATTACKS AGAINST ENTERPRISES IN THE GAMING INDUSTRY

104,216

Total attacks

DDoS ATTACKS AGAINST ENTERPRISES IN THE GAMBLING INDUSTRY

20,551

Total attacks

Industries Under Assault by DDoS Botnets

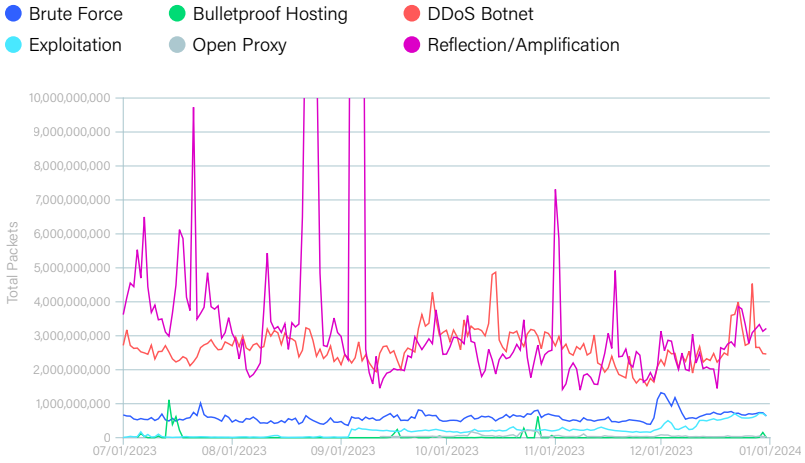
Adapting to the Changing Pulse of DDoS Threats from Reflection/Amplification Attacks to Direct-Path Attacks

Much like a doctor meticulously analyzing an echocardiogram for any signs of irregularity, NETSCOUT's ASERT team scrutinizes the data from the NETSCOUT visibility platform with equal precision. Our goal is to detect emerging or evolving DDoS threats, an integral part of maintaining the resilience of enterprises and services providers and the user experience they deliver (Figure 9). Given all the internal and external threats faced by enterprises, what is ASERT's prognosis?

Current trends indicate a gradual rise in direct-path DDoS attacks. Although the rate of reflection and amplification attacks has generally remained consistent, there were notable exceptions. Throughout the year, there were a few significant spikes in these types of attacks, with some reaching as high as 40 billion total packets in a single day (Figure 10). These intense surges predominantly targeted internet service providers (ISPs) that use enterprise in-line DDoS defense systems for data centers or specific infrastructure such as authoritative DNS servers.

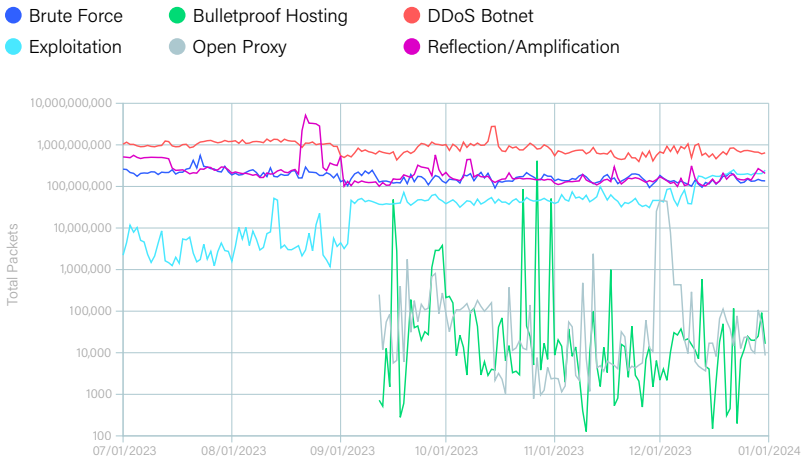
A significant development as the year ended was the marked increase in activity from a bulletproof hosting provider. This provider is known for its association with DDoS attacks executed via the DDoSia tool, linked to the Russian threat actor group NoName057(16). The variable nature of this activity suggests a strategic pattern, likely reserved for high-impact attacks that demand considerable resources.

Figure 9: Global Enterprise Threat Activity (2H 2023)



Peaks exceeding the y-axis represent data values beyond the scale shown.

Figure 10: Enterprise Threat Activity Analysis by Industry — Higher Education (2H 2023)



To delve into additional industries, see the full report.

ASERT ADVICE

Enterprises across various sectors constantly face these sophisticated cyberthreats, underscoring the need for advanced defense mechanisms and unmatched global visibility. Solutions incorporating machine learning and comprehensive threat intelligence are paramount. These systems provide robust, continuous protection, operating at the network edge to efficiently block and mitigate inbound attacks and prevent compromised internal systems from communicating with external command-and-control servers.

Employing these cutting-edge defenses enables businesses to strengthen their digital environments, ensuring operational resilience and continuity in the face of an ever-evolving spectrum of cyberthreats.

DNS and Collateral Damage

DNS Servers Under Constant Barrage of DDoS Attacks

Transitioning from adversary infrastructure to targeted infrastructure, perhaps the most critical area is that of attacks on authoritative and recursive DNS servers. Starting at the end of 2019, there's been a marked rise in DNS water torture attacks, a growing threat that targets the critical systems at the heart of the internet's control plane. DNS query floods—attacks specifically designed to overwhelm authoritative DNS servers—experienced a massive 553 percent increase from 1H 2020 to 2H 2023. Adversaries are no longer content with targeting one website or one server: They frequently go after systems that, if successfully taken down, would result in far-reaching collateral damage.

Consolidation of Web Infrastructure

When collocated domains share web infrastructure, DDoS attacks targeting one website and disrupting the underlying infrastructure diminish performance, availability, and overall reliability for all collocated websites. These adverse effects either propagate inadvertently or can be used by the attacker to conceal the real target. Investigation of attacks affecting at least one domain reveals that, on average (median) seven domains suffer collateral damage (Figure 11). The top 15 percent of attacks, in terms of web collateral damage, impact as few as 100 and as many as 100,000 or more websites.

Authoritative Nameservers in the Crosshairs

Because so many domains rely on a relatively small number of authoritative DNS servers, successful attacks become magnified in terms of impact. NETSCOUT's visibility enables observation of between 50 and 100 DNS query flood attacks against DNS infrastructure daily (Figures 12 and 13). Although over-provisioning systems and relying on a single authoritative DNS hosting provider appears to be cost-effective and a natural decision to avoid additional costs or seemingly redundant DDoS defense systems, it does not take much to recognize that devastating, multimillion query-per-second floods are no longer a rarity.

Figure 11: Web Domain Collateral Damage

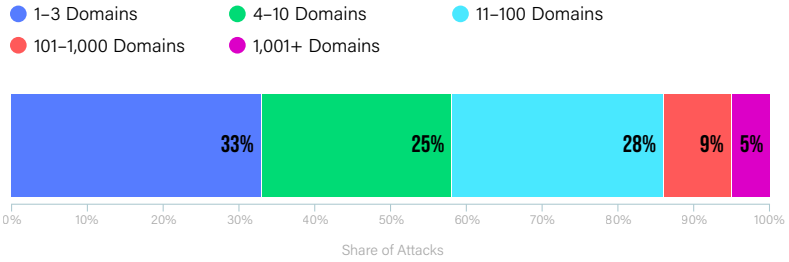


Figure 12: DNS Query Floods Targeting DNS Infrastructure (2H 2023)

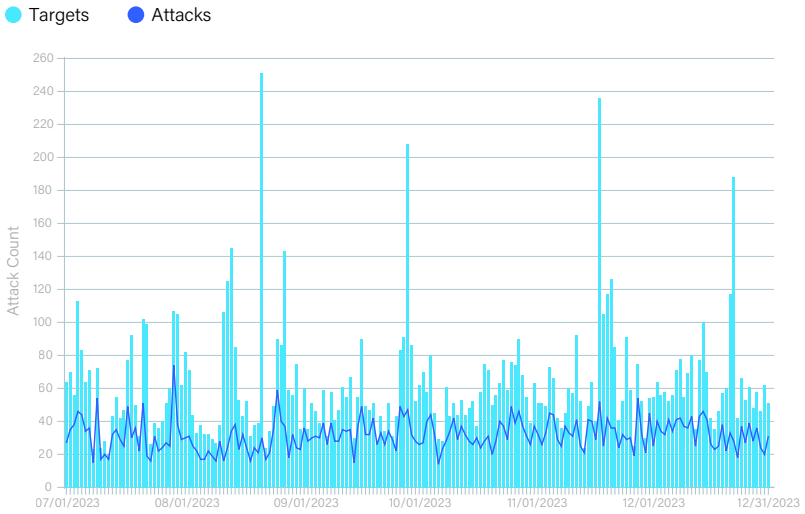
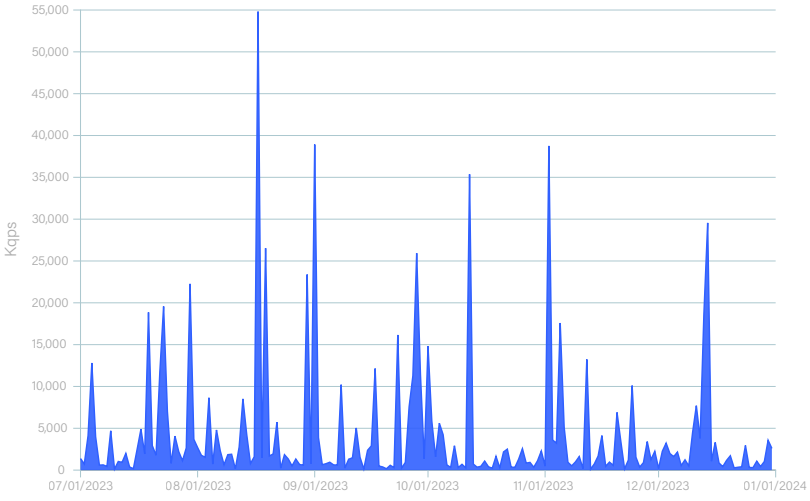


Figure 13: Peak DNS Query Floods (2H 2023)



Recursive Resolvers and the Looming Threat

We identified dozens of public resolvers that attracted a startling 50,000 DDoS attacks in 2H 2023. 83 percent of these attacks targeted prominent public resolvers, while the remaining 17 percent of attacks were scattered among the less prominent resolvers (Figure 14). Globally exposed DNS resolvers pose multifaceted risks, including susceptibility to DDoS attacks, cache poisoning, and security breaches due to their unrestricted internet access. Best practices for mitigating these dangers include restricting resolver access to authorized networks, implementing rate limiting and Domain Name System Security Extensions (DNSSEC), and regular security monitoring and updates. This approach enhances security and maintains the integrity and performance of DNS services.

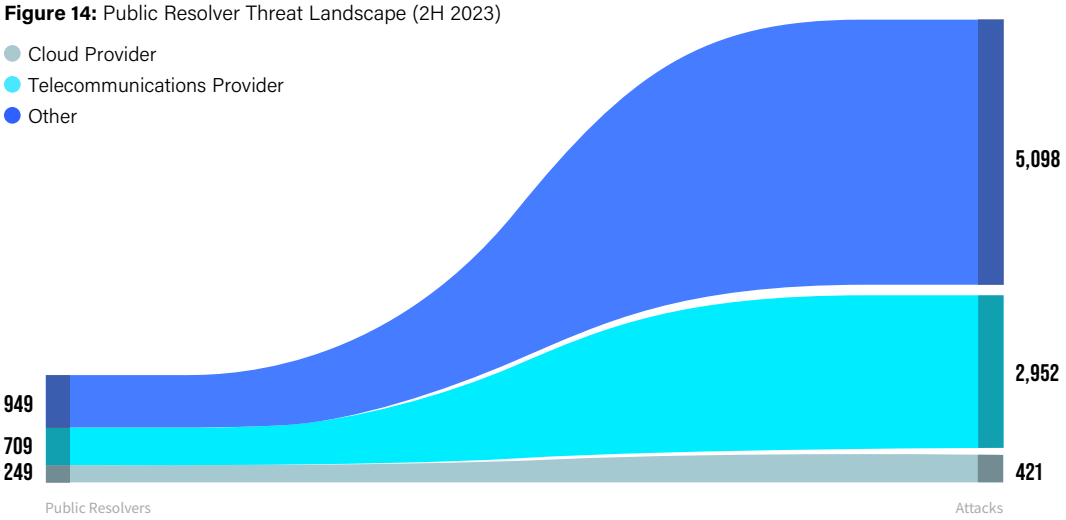
Moreover, even resolvers shielded against direct attack from external sources find themselves vulnerable to DDoS attacks from their ostensible user base. They must first defend against threats from within, such as malicious actors from inside their network boundaries, before turning their shields outward to fend off reflection/amplification attacks from outside. From experience, shielding an external resolver from DNS reflection/amplification bears a notorious challenge. The path is clear: To mitigate these risks, global exposure of DNS resolvers should be avoided at all costs, and reliance should be placed on intelligent DDoS mitigation services with proactive defense strategies and threat mitigation capabilities. The alternative means the acceptance of collateral downtime for any device legitimately configured to use the resolver in question.

ASERT ADVICE

These findings underscore the critical importance of protection for both authoritative and recursive DNS servers and demonstrate that DNS query floods composed of millions of queries per second (mqps) are a constant in the authoritative nameserver market.

Besides well-known public resolvers, there is no legitimacy in exposing a resolver globally. Doing so not only poses a significant threat of collateral downtime to the network's devices using this DNS resolver, but it also violates best common practices and good internet citizenship by hosting another piece of abusable infrastructure. Even shielding an external resolver from outside does not guarantee a nonintermittent uptime if not protected with the right assets.

Figure 14: Public Resolver Threat Landscape (2H 2023)



DDoS Defense

Intelligent DDoS Mitigation Systems Are Frontline Defense

DDoS attacks remain one of the internet's most persistent security challenges. The packet-sending capacity of just a few colluding hosts can wreak havoc on internet targets. Many wonder why ISPs can't just block bad traffic. After all, how difficult can that be? Although individual traffic flows in distributed systems might seem harmless, especially under encryption or within usage limits, disaster lurks unseen. Aggregating these seemingly innocent flows from attackers can unleash a potent assault on your target, often leaving traditional defenses powerless in its wake.

Three ways to mitigate DDoS attacks:

1. Eliminate or reduce harmful traffic early enough
2. Increase network capacity to absorb harmful traffic
3. Make targets unreachable to anonymous and remote systems entirely

   This idea finishes the job of an attack, but it also helps prevent collateral damage to systems near the target.

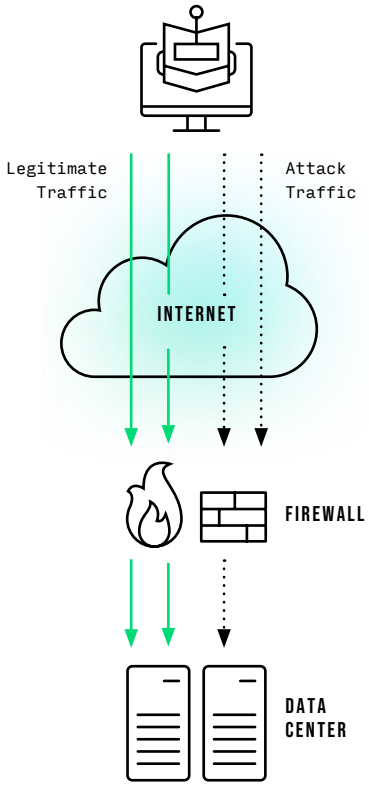


Figure 15: Front Lines of Network Defense

NETSCOUT explores how these strategies are deployed in practice, considering their effectiveness in different environments, each facing unique pressures and trade-offs. The following is intended to shed light on those trade-offs to help guide decision-making for your own DDoS mitigation thinking and strategy.

Firewalls perform "stateful inspection" to keep track of traffic to make informed decisions. However, they require memory to do this and can be overwhelmed by DDoS attacks, showing the limits of some security mechanisms (Figure 15). Many administrators have been surprised to learn that their 10Gbps connected firewall can be overwhelmed by less than 1Gbps of traffic!

Measuring Attack Volume

DDoS attacks are often "volumetric." We measure volume using metrics such as bits per second (bps) for data volume, flows per second (fps) for traffic properties, packets per second (pps) for packet size and rate, and queries per second (qps) or requests per second (rps) for application-layer attacks—depending on the type of service running.

ISP DDoS Mitigation Common Practices

ISPs can't always block bad traffic. They selectively block certain types and provide security for their infrastructure. This includes DDoS mitigation to handle customer and network demands, using strategies such as source address validation and traffic scrubbing.

Despite these efforts by ISPs, the challenge escalates as DDoS attacks evolve in complexity, presenting a myriad of forms akin to a viral fever with countless strains. So, the question arises: how do we effectively combat these multifaceted threats? NETSCOUT delves into this by examining a broad spectrum of defense tactics deployed across our total service provider visibility. The picture? A mishmash of defenses—surgical precision with intelligence mitigation systems, blunt force using Flowspec, zero-tolerance blackhole routing, and a patchwork of router access control lists (ACLs).

To further understand the nuances of DDoS mitigation, let's explore specific strategies:

SOURCE ADDRESS VALIDATION (SAV)

Around half of DDoS attacks are reflection/amplification attacks, made possible by IP spoofing. ISPs mitigate these by verifying customer traffic has valid source IP addresses. Although this is challenging, progress has been made thanks to vendor and community collaboration. Notably, we reported on a tectonic shift in attack methodology in 2022 because of this global vendor and community initiative.

REMOTE TRIGGERED BLACKHOLE FILTERING

This is a common method against denial-of-service attacks, where ISPs drop traffic based on Border Gateway Protocol (BGP) route announcements from customers. It's effective in preventing volumetric attacks from reaching customer links, at the cost of making prefixes temporarily inaccessible.

FLOW SPECIFICATION (FLOWSPEC) RULES

Flowspec enhances filtering between BGP devices, targeting specific traffic types. Widely adopted in certain networks, it presents operational challenges but offers precise control over traffic management.

INTELLIGENT DDoS MITIGATION

ISPs and specialized services use this technique to direct traffic through intelligent DDoS mitigation systems for thorough inspection and attack-traffic mitigation. This method is extremely effective, focusing on maintaining normal traffic flow while isolating and treating suspicious traffic.

CONTENT DISTRIBUTION NETWORKS (CDNs)

Utilized for hosting and distributing content globally, CDNs optimize content delivery and act as extensive load balancers. Although effective, they can be expensive for smaller-scale projects. Anycast is another load-balancing technique often used, especially in DNS services.

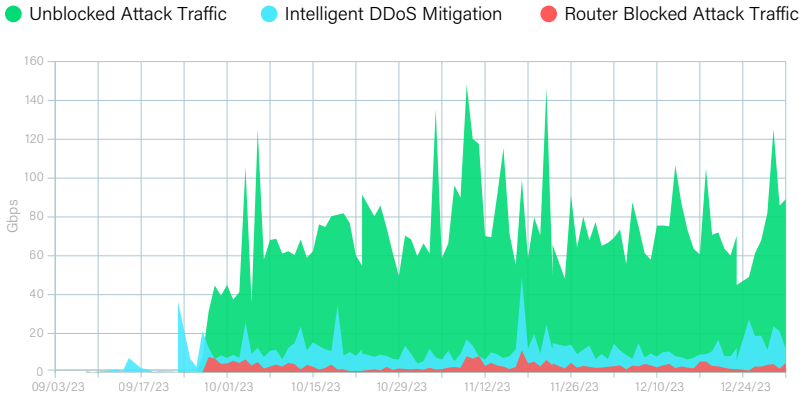
ASERT ADVICE

Mitigation is not a one-size-fits-all approach. One method is preattack intelligence and early detection, like an immune system sniffling out the bad before it spreads. That is where NETSCOUT's threat intelligence steps in, a vaccine for the digital body.

NETSCOUT's Threat Intelligence

So, how much can NETSCOUT's threat intelligence stop before it reaches critical systems? NETSCOUT's analysis demonstrates what gets blocked by an intelligent DDoS mitigation system using standard bandwidth/throughput thresholds and what could be neutralized by our intel before it cripples downstream networks.

Figure 16: A 10 Percent View of Average Attack Traffic in ISP Networks (2H 2023)



Outbound DDoS Attack Suppression

Mitigating incoming and suppressing outbound DDoS attacks is crucial for robust network operations and altruistically benefits the internet ecosystem.

Managing outgoing threats revolves around being a responsible internet citizen. Actively preventing the egress of attack traffic curbs the DDoS tax. By preventing themselves from ending up on third-party blocklists, organizations not only achieve smoother operations but also preserve the reputation of their IP address space. In the current climate of IPv4 address exhaustion, this reputation management has a ripple effect on IP address prices and facilitates lucrative reselling opportunities.

Mitigating incoming attacks is pivotal for transit providers (Figure 17). Protecting networks within their customer cone not only enhances credibility but also attracts more clients. The ability to charge a premium for DDoS mitigation services makes the acquisition of such products a self-sustaining investment.

Our statistical analysis indicates that our clients' networks encounter around 100,000 outgoing and 150,000 incoming attacks to external networks per month. Our analysis highlights a notable disparity in the attention given to suppressing outbound attacks (Figure 18). Overall, 99 percent of outgoing attacks are not suppressed. We find that only 19 out of 335 NETSCOUT customers with outbound attacks suppressed such an attack at least once. It is essential to recognize that while there rarely are valid reasons to forego suppressing outbound attacks, transit providers may receive explicit requests from clients to refrain from interfering with their network traffic.

Figure 17: Mitigation of Incoming DDoS Attacks (2H 2023)

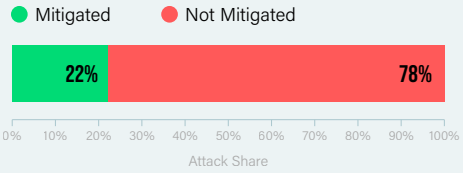
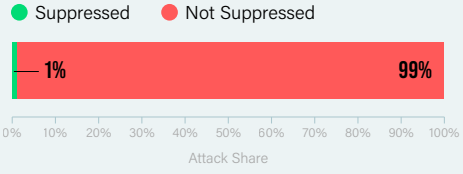


Figure 18: Suppression of Outgoing DDoS Attacks (2H 2023)



ASERT ADVICE

These patterns of suppressing—or the lack thereof—demonstrate a landscape where DDoS attack strategies are continuously advancing. In light of these findings, it is imperative for organizations to proactively reassess and enhance their security measures against outbound attacks, ensuring they stay ahead in this ever-evolving cyberthreat environment.

The Future of DDoS Defense Requires Innovation

Adversaries made a pivotal change toward application layer and direct-path attacks beginning early last year that carried through into 2023. This shift marks an increasingly volatile landscape of DDoS attacks that continue to grow in frequency. This was due to the defenders becoming more proficient in detecting and mitigating most of the more commonly used DDoS attack vectors. Also, the broader deployment of SAV led to a significant increase in direct-path DDoS attacks. This, however, resulted in the adversaries researching new DDoS attack vectors and enhancing their attack methodologies and other aspects of their repertoires to bypass the improved defenses.

Adversary advances include:

1. New and improved DDoS reflection/amplification vectors
2. Taking increased advantage of the large numbers of available abusable reflector/amplifiers to increase the total attack volume
3. Bypassing existing defenses by using service-chain attacks, employing increased use of proxies, and/or by launching internally facing DDoS attacks
4. Increased use of IPv6 attacks
5. Using machine learning/artificial intelligence to automate preattack reconnaissance and for launching multivector DDoS attacks

ASERT ADVICE

To meet these new threats, defenders are now focusing on predictive DDoS defense, DDoS suppression, and DDoS interdiction in addition to increased emphasis on IPv6 defense. Also, the introduction of federated DDoS defense systems will open new possibilities.

Defenders are now focusing on the following:

PREDICTIVE DDoS DEFENSE	▪ Tracking global malicious activity to identify potential DDoS sources ▪ Using real-time DDoS threat intelligence for early detection and mitigation
DDoS SUPPRESSION	▪ Proactively identifying and blocking abusable devices ▪ Detecting and stopping outbound DDoS attacks both to rapidly stop internally facing attacks and to stop DDoS attacks from reaching overwhelming volumes
DDoS INTERDICTION	▪ Blocking DDoS initiation traffic and DDoS command-and-control communication ▪ Encouraging deployment of anti-spoofing measures at network edges
IPv6 DEFENSE	▪ Addressing the rise in both unintentional and intentional IPv6 DDoS attacks with specialized defense strategies ▪ Applying best current practices for IPv6 to match IPv4 defense levels
FEDERATED DDoS DEFENSE	▪ Collaboration across networks for situational defense and intelligence sharing for predictive DDoS defense, DDoS suppression, and DDoS interdiction ▪ Implementing programmatically driven cooperative efforts for real-time attack mitigation

CONTRIBUTERS

Chris Conrad, *Writer*
Richard Hummel, *Writer*
Steinthor Bjarnasen, *Writer*
Roland Dobbins, *Writer*
Filippo Vitale, *Writer*
Chad Robertson, *Writer*
John Kristoff, *Writer*
Roman Lara, *Writer*
Marcin Nawrocki, *Writer*
Max Resing, *Writer*
Clark Arenberg, *Writer*
Kinjal Patel, *Contributor*

Final Thoughts

The DDoS landscape is changing fast, and staying ahead of these threats is critical to your business. 2023 has shown us the real impact of these attacks across different sectors, from political hacktivism to attacks against DNS servers resulting in widespread collateral damage and to the gaming world where every microsecond is life or death (virtually). But it's not all doom and gloom. Thanks to strong collaboration, predictive and proactive mitigations, and advanced threat intelligence, we're better equipped to face these challenges head-on.

It needs to be a top priority, as critical as day-to-day operations, to push for stronger defenses and smarter solutions together as we build a more secure digital world.

NETSCOUT®

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) protects the connected world from cyberattacks and performance disruptions through advanced network detection and response and pervasive network visibility. The data in this report is derived from NETSCOUT's ATLAS, which provides unparalleled internet visibility at a global scale collecting, analyzing, prioritizing, and disseminating data on DDoS attacks from 214 countries and territories, 456 industry verticals, and 13,005 Autonomous System Numbers (ASNs). ATLAS Intelligence Feed (AIF) continuously delivers relevant, actionable DDoS threat intelligence that is used proactively to defend against DDoS attacks and other cyber threats. That's why the world's most demanding government, enterprise, and service provider organizations rely on NETSCOUT's industry-leading Arbor Adaptive DDoS Protection solutions to protect the digital services that advance our connected world.

Visit www.netscout.com or follow @NETSCOUT on Twitter, Facebook, or LinkedIn.

SECR_001_EN-2401