NETSCOUT

ISSUE 11

NETSCOUT DDoS Threat Intelligence Report

Complete Network Visibility Enables Total Network Control

CONTENTS

You were not in control; you had no visibility...

Alain Prost, Formula 1 World Champion

You can't win 51 Grand Prix victories without visibility. Alain Prost needed it on the racetrack, and it's the cornerstone of internet security today. As internet connectivity becomes more complex and more vital for organizations around the globe, the NETSCOUT Visibility Without Borders® platform enables us to see around corners with unparalleled insight into attacker behavior.

Our role is to ensure your critical infrastructure is available and resilient—protecting everything from mass and individual communications to economic activity, news, education, utilities, and national security. Preparation is key to successful Adaptive DDoS defense, and our visibility not only provides insight into the minute-zero attacks but also tells you what to expect next with attacks that have yet to even be deployed on the internet.

It's that unprecedented level of visibility into all stages of Distributed Denial of Service (DDoS) attacks that allows us to peer into the future in our role as Guardians of the Connected World and empower our customers to take control.

Key Findings

Internet Traffic Growth and Visibility Accelerating

Accelerating at amazing speeds, the growth of the internet necessitates increased visibility. And NETSCOUT's commitment to worldwide visibility granted us insights into an average of 424Tbps of internet peering traffic in 1H 2023, a 5.7 percent increase over the 401Tbps reported at the end of 2022. The internet's rapid growth unfortunately experienced drag—a reduction in capabilities because of an increase in DDoS attacks. For example, we witnessed a nearly 500 percent growth in HTTP/S application-layer and 17 percent increase DNS reflection/amplification attack volumes in 1H 2023.

The Power of Persistence

The majority of observed application-layer, reflection/amplification, and direct-path volumetric DDoS attack traffic share a near-universal characteristic: a significant degree of attack source persistence. NETSCOUT's ASERT Team identified DDoS reflectors/amplifiers, DDoS botnet nodes, and DDoS attack generators exhibit an average churn rate of only 10 percent over a two-week interval from their inception. In practical terms, this means that 90 percent of verified DDoS attack sources can be proactively blocked for as much as two weeks after initial discovery.

DDoS Attack Infrastructure Telemetry

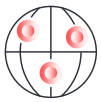
ASERT examined several different types of abusable infrastructure leveraged in DDoS attacks worldwide—DDoS botnets, open proxies, The Onion Router (Tor) nodes, and attacker-friendly networks commonly referred to as bulletproof hosting providers. In 1H 2023, we observed open proxies consistently leveraged in HTTP/S application-layer DDoS attacks primarily directed toward the higher education and national government sectors, whereas DDoS botnets frequently target state and local governments.

Adversary Discovery Lifecycle

The unmatched breadth and depth of our data horizon allows us to identify the exact point in time when new DDoS attack vectors are discovered, tested, optimized, first utilized by adaptive attackers, and eventually weaponized in DDoS-for-hire services. This DDoS Threat Intelligence Report covers the evolution of the Apple remote management system (ARMS), TP240, and Service Location Protocol (SLP) DDoS attack vectors from inception to weaponization.

Carpet-Bombing and DNS Water Torture Attacks Increase Pace

Domain Name System (DNS) water torture DDoS attacks have been steadily rising in prevalence—with a sharp increase observed in June 2023. At the same time, carpet-bombing attacks continue to rise, and our new research demonstrates that most carpet-bombing attacks are univector rather than multivector, with DNS reflection/amplification being the most prevalent attack type, followed by Session Traversal Utilities for Nat (STUN) reflection/amplification.



World Events Fuel DDoS Attack Campaigns

Since the initiation of ground operations in the Russia/Ukraine conflict, ideologically motivated DDoS attacks targeting the United States, Ukraine, Finland, Sweden, Russia, and other countries have remained constant. Last year, Finland experienced a wave of DDoS attacks before and immediately after its NATO acceptance. Sweden has experienced a similar onslaught as that country's bid to join NATO moves forward. But it's not just politics: A wave of DDoS attacks hammered wireless telecommunications, no doubt a result of 5G wireless connectivity expanding at a staggering rate and subscribers opting to use 5G as their primary internet connection.

Internet Traffic and Slipstreamed Threats

Global Internet Traffic Visibility

We are committed to true global visibility and tracking the growing DDoS problem with insight into more than 500 contributing networks—with more networks being added weekly. NETSCOUT's intelligence from these internet service providers (ISPs) provide a holistic and nuanced perspective on the good and bad of the vast, interconnected digital universe. This macro view of the internet's transit traffic yields many unique insights. We extracted findings from an average of 424Tbps of total internet peering traffic during the first half of 2023 (Figure 1)—a 5.74 percent increase over 2H 2022.

The constant expansion in internet visibility becomes critical as the internet grows—one organization reported a 21 percent growth in international internet peering traffic at the end of 2022—and the visibility gained is essential to developing attack mitigation strategies, because more than 75 percent of these networks see dozens or even hundreds of incoming DDoS attacks every day (Figure 2).

Figure 1: Global Average Internet Traffic Volume

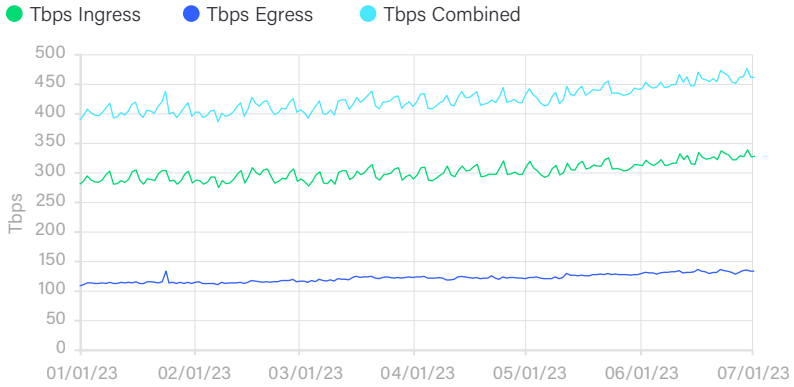
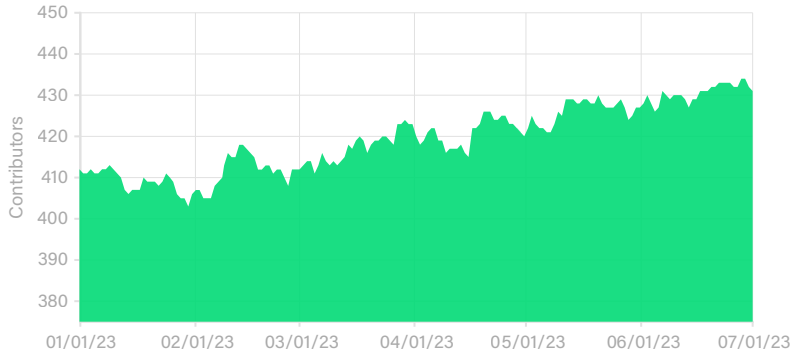
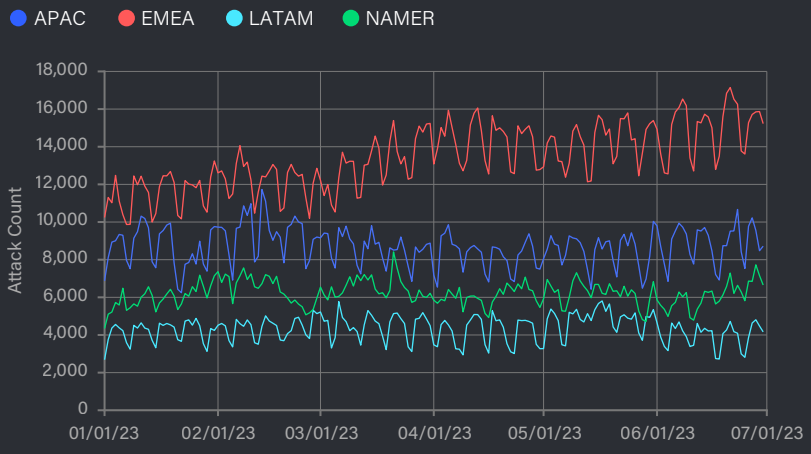


Figure 2: Contributing ISP Networks



The Undercurrent of Malicious Traffic

Figure 3: Regional DDoS Attack Counts

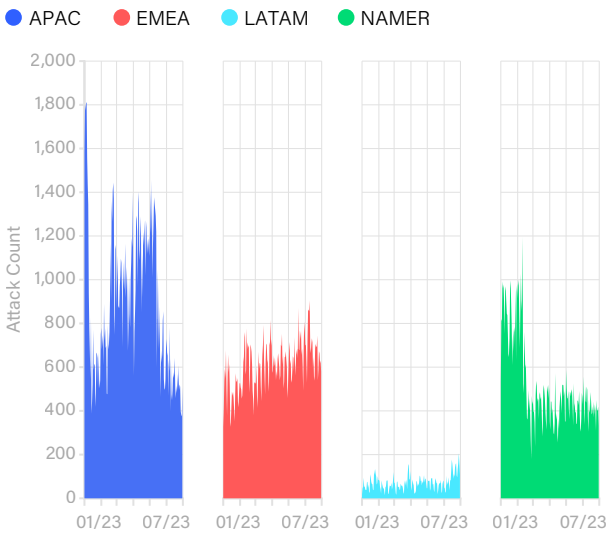


In racing, drivers often use a technique called slipstreaming, drafting directly behind another car to increase speed. Like slipstreaming, adversaries use the resources of others to steal "speed" to the detriment of others. Unfortunately, the theft never ends, and ISP networks always bear the cost. In the first half of 2023, NETSCOUT observed a staggering total of ~7.9 million DDoS attacks, representing a 31 percent increase year over year. This represents an unbelievable 44 thousand DDoS attacks per day (Figure 3).

The growth in attacks implies this malicious traffic is ever-present. To illustrate how this attack traffic is always present, we dive into HTTP/S and DNS below (Figures 4 and 5).

HTTP/S Application-Layer Attacks

Figure 4: Total HTTP/S Application-Layer Attacks



MITIGATED HTTP/S APPLICATION-LAYER ATTACKS IH 2023

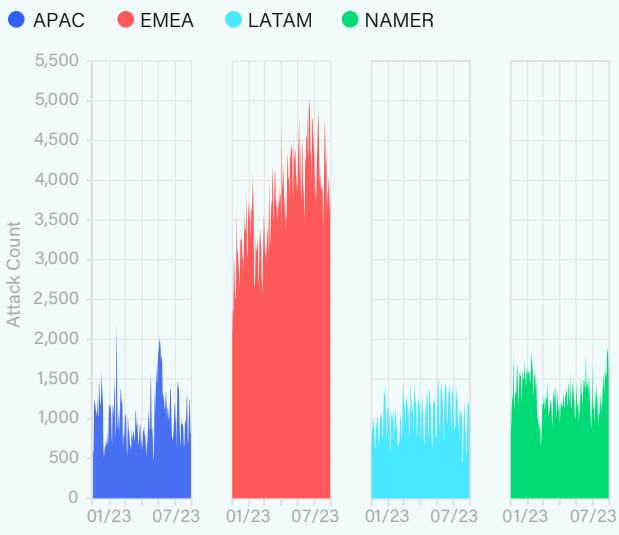
- APAC 1%
- EMEA 37%
- LATAM 10%
- NAMER 35%

TOP 5 INDUSTRIES TARGETED BY HTTP/S APPLICATION-LAYER ATTACKS

1. Wired Telecommunications Carriers 159,701
2. Data Processing Hosting and Related Services 48,227
3. Wireless Telecommunications Carriers (except Satellite) 34,791
4. Electronic Computer Manufacturing 17,020
5. Internet Publishing and Broadcasting 11,208

DNS Amplification Attacks

Figure 5: Total DNS Amplification Attacks



MITIGATED DNS AMPLIFICATION ATTACKS IH 2023

- APAC 10%
- EMEA 35%
- LATAM 25%
- NAMER 37%

EMEA was the No. 1 targeted region

TOP 5 INDUSTRIES TARGETED BY DNS AMPLIFICATION ATTACKS

1. Wired Telecommunications Carriers 480,905
2. Wireless Telecommunications Carriers (except Satellite) 187,700
3. Data Processing Hosting and Related Services 83,359
4. Satellite Telecommunications 16,598
5. All Other Telecommunications 16,348

The Power of Persistence

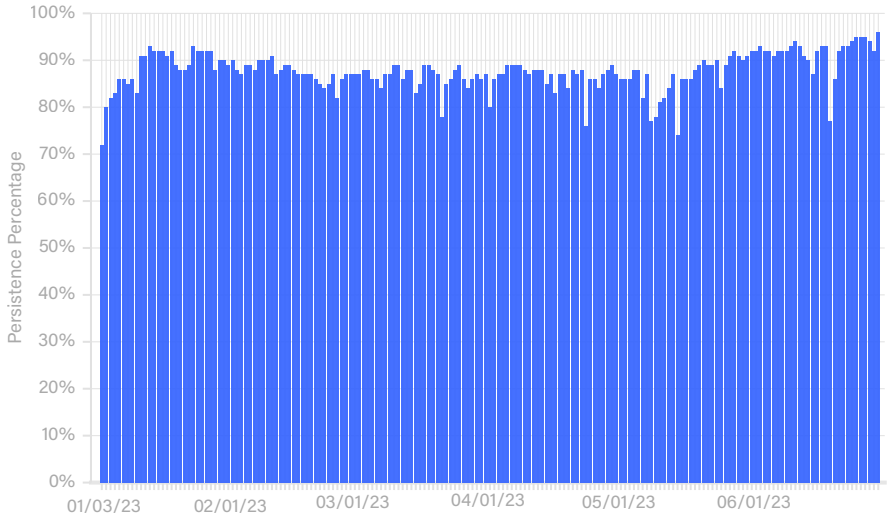
Formula 1 tracks remain the same, every race, every year, with only variables in weather, visibility, and road conditions. That persistence enables drivers to prepare and build confidence in their ability. The same persistence is true in the infrastructure abused by adversaries to launch DDoS attacks—from reflectors/amplifiers to DDoS botnets and even lists of open proxies conscripted into attack tools. Despite the fact there are hundreds of millions of abusable internet-connected devices an adversary can leverage to launch DDoS attacks, ASERT confirmed that a relatively small number of nodes are involved in a disproportionate number of DDoS attacks and contribute significantly to attack impact.

Persistent Attacker-Abused Infrastructure

Every day, NETSCOUT enterprise customers face security events from millions of attacker-abused and/or owned network-connected devices. We can identify persistent infrastructure leveraged by these relentless attackers by analyzing countermeasure behavioral heuristics.

During the first half of 2023, the top 5 percent of persistent attack sources' IP addresses revealed that ~90 percent of the IPs maintained a constant presence within any given two-week interval (Figure 6).

Figure 6: Top 5 Percent of Persistent Attackers



Within the same context of a dynamic two-week moving window, we determined that approximately half of the attack sources identified and blocked by our enterprise solutions corresponded to persistent attackers.

Based on comparative analysis, fully one-third of persistent attack sources remain unidentified by conventional threat intelligence feeds and methodologies. NETSCOUT's unique breadth and depth of insight into the global DDoS threat landscape allows us to determine that blocking only 5 percent of persistent attack sources would result in a significant reduction in attack impact.

VALIDATED ATTACK SOURCES BASED ON THREE CHARACTERISTICS

1. Daily persistence over time
2. Volume of attack traffic directed towards NETSCOUT customers
3. Number of customers targeted by the same persistent infrastructure

TOP 5 SOURCE COUNTRIES


United States
26.5%


Brazil
10.3%


India
6.9%


China
6.7%


Netherlands
3.2%

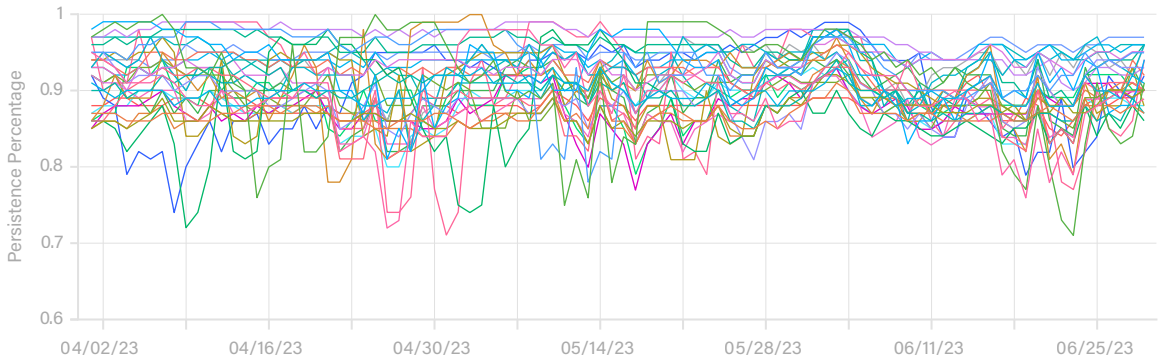
Known DDoS Sources

In addition to persistent attackers, NETSCOUT's visibility provides a unique perspective into known DDoS sources used in reflection/amplification and botnet attacks. A high day-to-day persistence implies the attacker infrastructure NETSCOUT knew about yesterday is the same participating in today's DDoS activity (in other words, known DDoS sources).

Figure 7 illustrates the degree of persistence exhibited by abusable reflectors/amplifiers and DDoS-capable botnets from April to June 2023. Our research revealed that these attack sources have an average of 10 percent churn. We also discovered that many of the IPs churning from day-to-day are responsible for a large amount of impact against our customers. This means that while there is a high degree of persistence in reusable adversary-abused infrastructure, it is equally imperative to have an always-updated list of new IPs to account for the high-impact sources evolving near-daily. NETSCOUT's ATLAS Intelligence Feed (AIF) includes a daily list of both the persistent and new infrastructure to provide full-scope coverage on DDoS attacks sourced from these IPs.

Figure 7: DDoS Attack Types

Reflector/Amplifier and DDoS Botnets Feeds



Bulletproof Hosting (BPH) Providers

Bulletproof hosting (BPH) providers pose a unique and challenging threat. Their activity is often disguised under a veil of legitimacy; however, due to their willful neglect of community norms, their illicit activities often evade normal responses such as takedown requests. Furthermore, inaction by their peers and upstream providers prolongs abusive behavior, often across the course of many years, resulting in BPH providers becoming emboldened by the internet community's lack of response. This allows BPH providers to refine and enhance their methods unencumbered while incident responders must search for ways to track and mitigate their behavior. Many of the most notorious threats to internet safety and stability previously have found safe havens at BPH providers, but this strategy is becoming less tenable as we uncover and provide defensive recommendations to our customers and the world.

As described in our recent blog focused on bulletproof hosting providers, we classify them as belonging to one of three categories: malicious, abusive, or controversial.

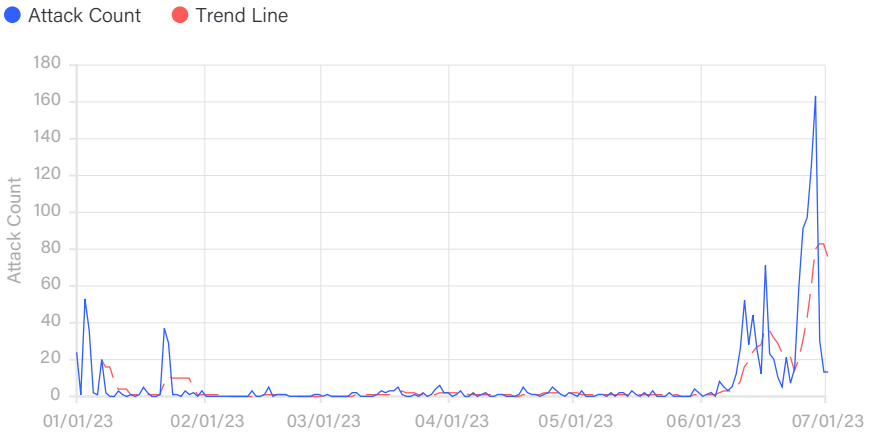
We focus our examination on the malicious and abusive categories of two well-known BPH providers. We refer to these BPH providers as Provider X and Provider Y. Provider X operates its own autonomous system (AS) and has dozens of small Internet Protocol version 4 (IPv4) prefixes it announces into the global BGP routing table. In total, Provider X announces less than a /16 of IPv4 address space. This is not a lot of addresses. However, when we consider the frequency of attacks involving this provider (Figure 8 on the following page), it becomes apparent Provider X is a significant source of attacks.

THREE TYPES OF BPH PROVIDERS

1. **MALICIOUS**
   Practically no legitimate or lawful activity
2. **ABUSIVE**
   Significantly uncooperative, unresponsive, or unwanted activity
3. **CONTROVERSIAL**
   Legal, but often condemned for unwanted material or activity

Most of these attacks are sourced from Provider X to other networks. Compared with a university of a similar network size, Provider X exhibits a greater number of attacks originating from its network than it should.

Figure 8: BPH-X Attacks and Trend Line Per Day



BPH-X TARGETED COUNTRIES


Ukraine
1,024 Attacks


Singapore
62 Attacks


United States
51 Attacks


Russia
40 Attacks


Netherlands
27 Attacks

To further classify suspicious traffic sourced from this provider, we analyzed the outbound packet size distribution (Figure 9). Typical traffic patterns would exhibit either consistency on one end or a sinusoidal curve of varied packet sizes over time. Instead, we see packet sizes polarized at both ends simultaneously. In normal traffic, it is extremely rare for large packets to trail immediately behind small packets. This suggests that the network in question is atypical and likely used for a limited subset of specialized applications such as scanning and malicious content hosting.

By way of contrast, Provider Y has been known to provide internet transit for other bulletproof hosters, acting as their upstream ISP. Provider Y announces only one-fourth the IPv4 address space that Provider X does, but the number of attacks we see on our customer networks involving Provider Y are more than double Provider X's, and the attacks in and out are closer to being symmetrical (Figure 10). Because of the nature of these types of services, it's highly probable they are enabling malicious activity to (command and control, exfiltration, and so forth) and from (exploitation, scanning, brute-forcing) this network, resulting in a higher degree of symmetry of inbound/outbound traffic. In contrast, Provider X is the source of a great deal of aggressive and abusive internet scanning.

Figure 9: Packet Size Distribution

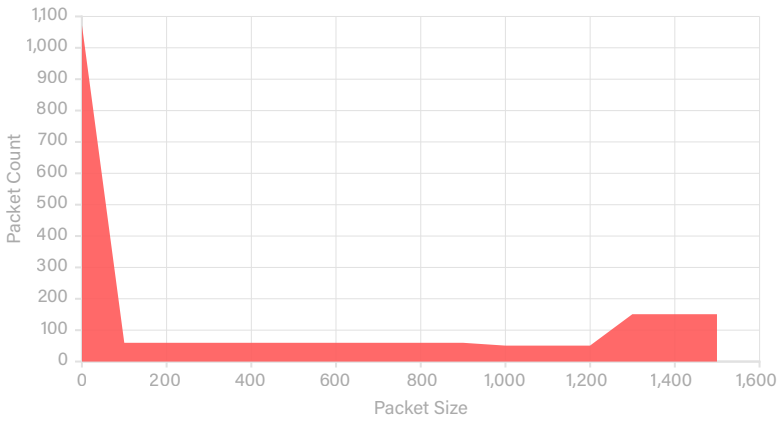
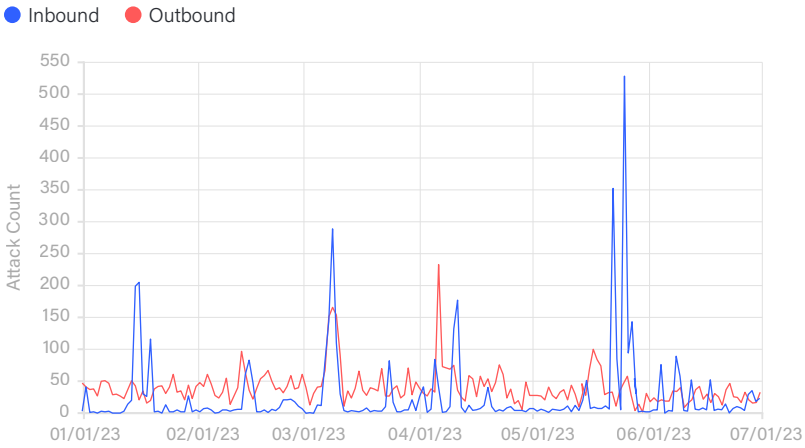


Figure 10: BPH-Y Inbound and Outbound Attacks Per Day



DDoS Vector Discovery and Attack Enablers

Increasingly, adversaries are creating their own and/or abusing different types of infrastructure as platforms to conduct reconnaissance and launch attacks. The following analysis highlights how some of that abusable infrastructure is leveraged in attacks and how adversaries discover new DDoS attack vectors and methodologies.

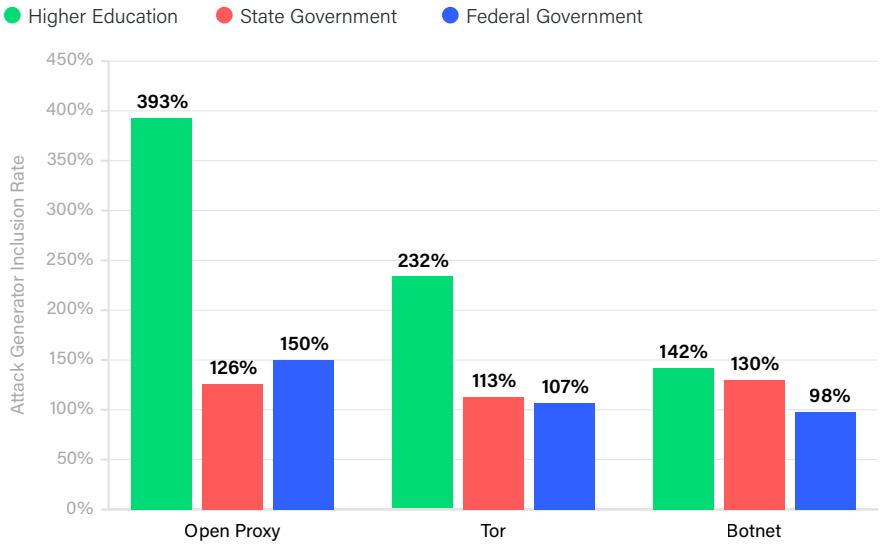
Dissecting Adversary Attack Generators

Threat actors are now relying more on DDoS-capable botnets, Tor nodes, and open proxy servers to generate and obfuscate the actual sources of direct-path DDoS attacks. As a result of the great rebalancing described in our 2H 2022 DDoS Threat Intelligence Report—we have seen a renewed emphasis on direct-path attacks and a transition from a nearly decade-long stint of reflection/amplification preeminence.

Although reflection/amplification attacks remain the primary DDoS attack methodology used to target service provider properties and infrastructure, botnets, open proxies, and Tor nodes are employed primarily in attacks directed toward enterprises and other types of endpoint networks.

All three types of attack sources display disproportionately high rates of activity in security events targeting institutions of higher education and data-hosting services (Figure 11). The Y-axis in the figure below represents the percentage above observed baselines (proxies, Tor nodes, and botnet nodes) in comparison to other types of hosts. DDoS botnets frequently are used in attacks targeting state and local governments, whereas open proxies have seen disproportionate use in attacks against federal/national governments. Proxy use against federal/national governments is notable because proxies are a favorite tool of ideologically motivated adversaries such as Killnet for launching application-layer DDoS attacks against web servers and online portals.

Figure 11: Industries Impacted by Attack Generators



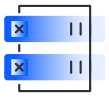
ATTACKS TARGETING ISPs 1H 2023

TOR NODES

30
Daily Alerts

OPEN PROXIES

30
Daily Alerts



BOTNET NODES

730
Daily Alerts

INDUSTRY TOP TARGETS

1. **HIGHER EDUCATION**
   Frequent use of open proxy, botnet and Tor
2. **STATE GOVERNMENT**
   Frequent use of DDoS botnet attacks
3. **FEDERAL GOVERNMENT**
   Frequent use of open proxies

A Vector is Born

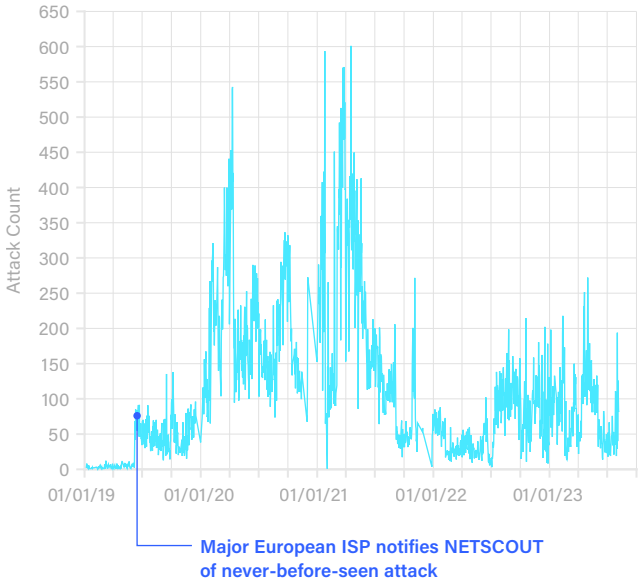
Like defense in traditional warfare, the protection of digital assets during cyberwarfare is significantly enhanced by early warnings combined with top-notch visibility. NETSCOUT's unmatched ability to observe emerging DDoS vectors is of the utmost importance in safeguarding global networks. This level of visibility allows us to identify adversary attempts to exploit abusable hosts and services to launch DDoS attacks.

ARMS Reflection/Amplification

In mid-2019, NETSCOUT received notification of significant DDoS attack traffic sourced from UDP/3283, a previously unused and unknown attack vector. ASERT researchers immediately began reverse-engineering the attack. Within four days, NETSCOUT had successfully replicated this never-before-seen reflection/amplification DDoS attack, which leveraged unpatched systems running ARMS. Our testing revealed a substantial amplification ratio of 35.5:1.

NETSCOUT then created surgical deny lists of abused ARMS reflectors/amplifiers, published customer and public advisories on mitigating this new DDoS attack vector, and worked with the vendor on mitigation/remediation recommendations. At discovery, there were a total of 54,000 abusable nodes on the public internet, and today that number is ~6,000 thanks to in part to NETSCOUT visibility, remediation guidance to network operators, education efforts, and patching by Apple. This early identification of a new DDoS vector allowed us to publish mitigation recommendations before adversary activity became commonplace in early 2020 (Figure 12).

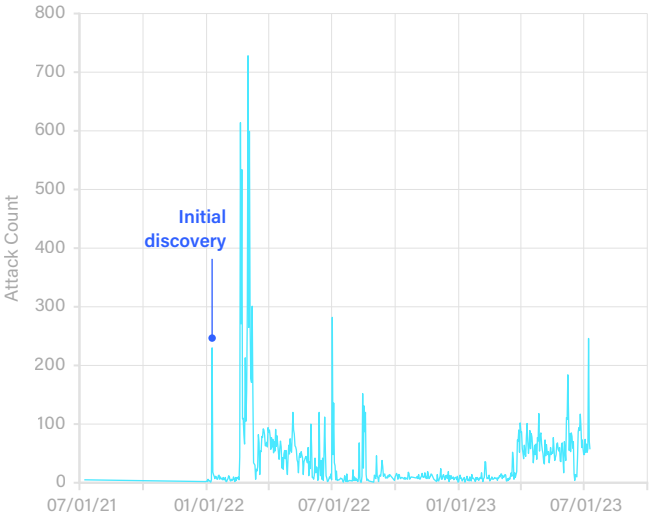
Figure 12: ARMS Related Activity



TP240 Phone Home
Reflection/Amplification

But this was not just lightning in a jar. Beginning in January 2022, NETSCOUT observed probes targeting services running on UDP/10074 (Figure 13). Concurrently, NETSCOUT, via partnerships with global network operators, vendors, and research teams, began investigations into a potential new DDoS attack vector dubbed TP240 Phone Home. ASERT discovered that this vector had an astonishing potential amplification ratio of 4,294,967,296:1—capable of generating more than 53 million packets per second. NETSCOUT initially identified more than 5,000 abusable nodes on the public internet. Today that number is fewer than ~2,800, due in part to NETSCOUT's visibility, remediation, and public education efforts.

Figure 13: TP240 Related Activity

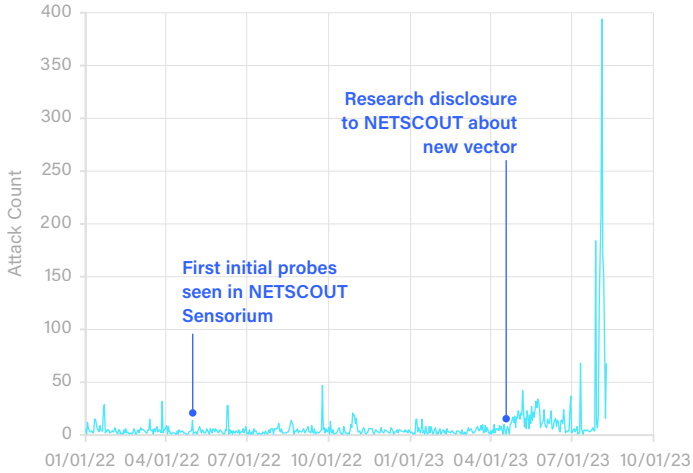


S1

SLP Reflection/Amplification

Most recently, NETSCOUT witnessed the emergence of a new vector with the greatest lead time yet. We discovered the activity in 1H 2023, but after investigating traffic in our global honeypot network found that adversaries started probing UDP/427 in September of 2022 (Figure 14). These early probes originated from a security researcher looking into vulnerabilities in the SLP protocol. In April of 2023, ASERT characterized and provided mitigation recommendations and surgical deny lists for this new DDoS attack vector, which is capable of amplifying traffic at a ratio of 2200:1 with proper priming. At discovery, NETSCOUT identified more than 40,000 abusable reflectors/amplifiers on the public internet. Today, that number is ~38,000 and declining. NETSCOUT mitigation and remediation guidance has minimized this vector's effectiveness, ensuring customers are proactively protected against SLP reflection/amplification attacks.

Figure 14: SLP Related Activity

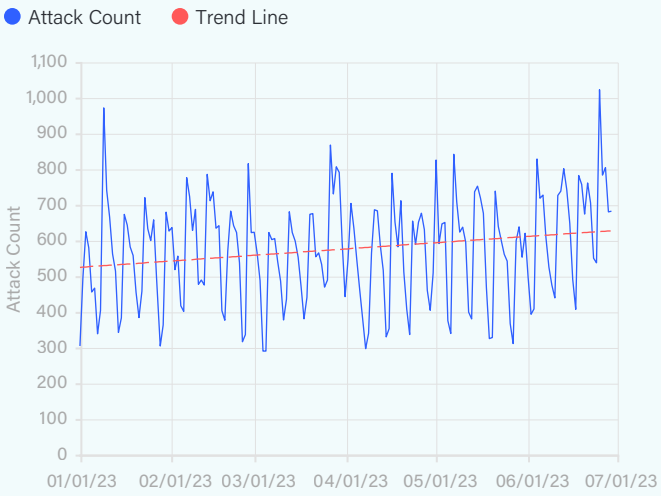


Revealing Adversary Methodology

In addition to using a multitude of DDoS attack vectors, threat actors also employ various attack methodologies against targeted organizations. For example, DNS query floods were first observed in the wild in 1997, but since that time they have evolved, with varieties of DNS water torture attacks (floods of DNS queries for nonexistent records) becoming commonplace. When carpet-bombing attacks—in which entire networks are targeted instead of just specific hosts on those networks—first debuted in 2017, ASERT researchers quickly issued mitigation guidance to customers and the operational community.

Carpet-Bombing Deep Dive

Figure 15: Daily Carpet-Bombing Attacks (1H 2023)



A sudden resurgence in carpet-bombing attacks prompted our researchers to investigate this tactic, and since the first week of 2023, we observed a 55 percent increase in daily carpet-bombing attacks, from an average of 468 per day to 724 per day (Figure 15).

It should be noted that these figures are conservative and are based on high-impact attacks on ISP networks. Given the nature of these attacks—adversaries intentionally spreading traffic to multiple hosts, thus decreasing bandwidth rates and avoiding traffic threshold alerts—it is highly plausible these numbers are an order of magnitude lower than the actual number of carpet-bombing attacks present on the internet.

Carpet-Bombing Attacks: A Breakdown

ATTACK METRICS

88 Average Attacked IPs + Prefix	**841** Maximum Attacked IPs + Prefix
118 Average Attacking Source IPs + Prefix	**1,257** Maximum Attacking Source IPs + Prefix
18.5 Average Attack Duration (Minutes)	**2,949** Maximum Attack Duration (Minutes)

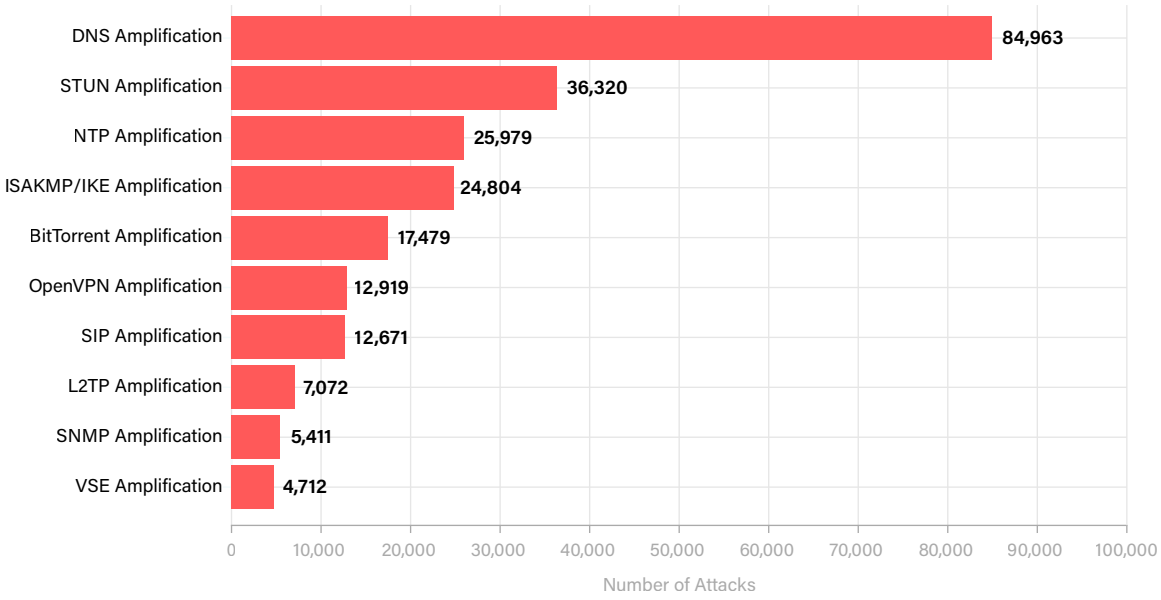
TOP 5

TARGETED COUNTRIES	SOURCE COUNTRIES
1 United States	1 United States
2 Brazil	2 Netherlands
3 Spain	3 Great Britain
4 Japan	4 Germany
5 Italy	5 France

Because carpet-bombing attacks are designed to target a broad network footprint, it is no surprise that wired and wireless telecommunications and cloud hosting providers bear the brunt of these attacks as they spread across their networks. Most of the reflectors/amplifiers used to launch these attacks are sourced from the very same networks they target.

DNS amplification features most prominently in carpet-bombing attacks, but perhaps slightly more surprising is that STUN amplification is a close second (Figure 16). That is, until we realized that STUN is necessary for Webtrp-based VoIP and video communications leveraged by services such as FaceTime, Skype, and Teams. This means that, like DNS responses, it cannot be filtered wholesale at the network edge. Previously, carpet-bombing attacks were almost always univector UDP reflection/amplification attacks. In the last 18 months, however, we have observed an uptick in the use of TCP reflection/amplification with carpet-bombing attacks.

Figure 16: Top 10 Vectors: Carpet-Bombing DDoS Attacks (1H 2023)



DNS Query (Water Torture) Flood Deep Dive

The Domain Name System, or DNS, which serves as the internet's address book, mapping (mostly) human-friendly names into IP addresses so that devices, applications, and services know where to send packets. Since 1997, attackers have been launching attacks against DNS servers to disrupt applications and devices.

After all, if the name of a website, online game service, or streaming video provider can't be resolved, the effect is the same as if the actual service itself has been successfully attacked. This is also the case with key enterprise properties such as corporate web servers, collaboration services, and VPN concentrators: If an enterprise's authoritative DNS servers are successfully disrupted, the entire organization is, for all practical purposes, unreachable. Unfortunately, many organizations fail to include DNS servers in their DDoS defense plans.

DNS Attack Analysis

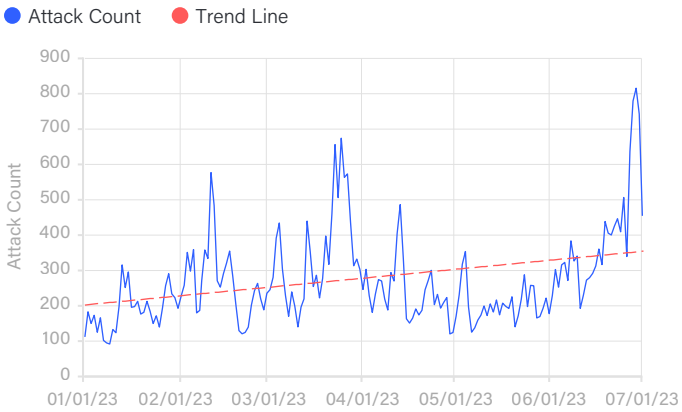
DNS water torture attacks rose from an average of 144 daily attacks at the start of 2023 to 611 at the end of June, marking a nearly 353 percent increase in only six months. The highest-impact attack involved ~89.4 million queries per second (mqps), a 51.1 percent increase in attack impact over the same period in 2022.

A decrease took place at the start of 2023, but our observations indicate that these attacks were once again on the rise toward the end of 1H 2023 (Figure 17). This indicates that although variability in attacker motivations leads to some seasonal variations in targeting, DNS water torture attacks inevitably climb back up and continue to remain high-impact attacks that are highly disruptive to organizations unprepared to defend their DNS infrastructure.

Given the diversity of attacked industries, it appears that both ideologically motivated threat actors and DDoS extortionists intent on monetary gain attack DNS servers to cause disruption to the online properties and activities of organizations in their crosshairs.

Worse, the increasing prevalence of well-known open DNS recursive services as sources in these attacks is concerning and may indicate that adversaries are intentionally trying to smuggle traffic past network operators responsible for securing DNS resources. Not only does that present more sophisticated adversaries, but DNS water torture attacks reflected through these services are more challenging for defenders to mitigate due to the intermingling of attack traffic with genuine DNS queries originating from legitimate sources. It is imperative that organizations ensure their authoritative and recursive DNS infrastructure is included in DDoS defense plans and reviewed regularly.

Figure 17: DNS Water-Torture Attacks Per Day



DNS Attacks: A Breakdown

TOP 5 TARGETED COUNTRIES

1. United States
2. Morocco
3. Turkey
4. South Africa
5. Argentina

On a regional basis, EMEA received most attacks, with North America and Asia-Pacific in second and third place, respectively.

TOP 5 TARGETED INDUSTRIES

1. Wired Telecomm
2. Wireless Telecomm
3. Data Processing Hosting and Related Services
4. Electronic Shopping and Mail-Order Houses
5. Insurance Agencies and Brokerages

The wireline and wireless broadband access ISP/cloud/VPS/hosting/colocation, and insurance sectors were especially hard-hit by DNS water torture attacks during the first six months of 2023.

Geopolitical and Technology Impact in DDoS

Everything from vectors to infrastructure and methodology play a part in the remaining analysis contained in our report as we examine how geopolitical influences continue to play a dominant role in the DDoS threat landscape—followed closely by changes in the technology arena.

Geopolitics in the Cyber Arena

Figure 18: Swedish Attacks and Trend Line Per Day

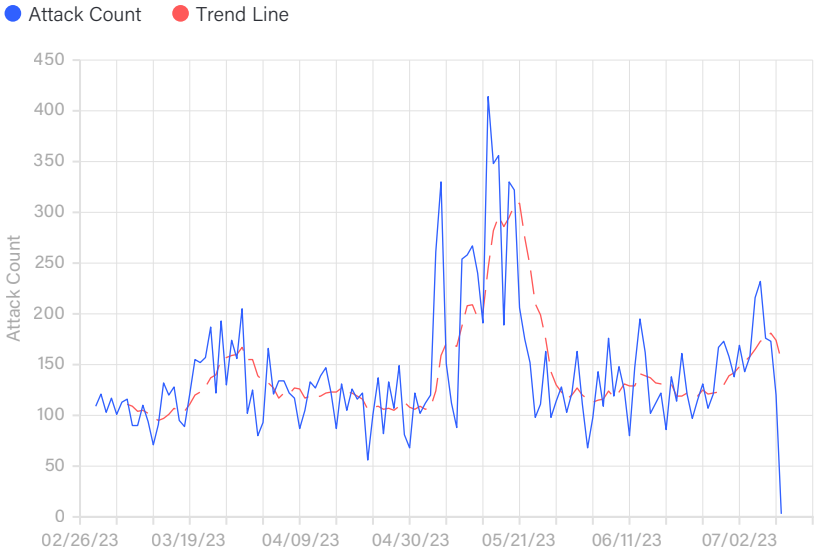
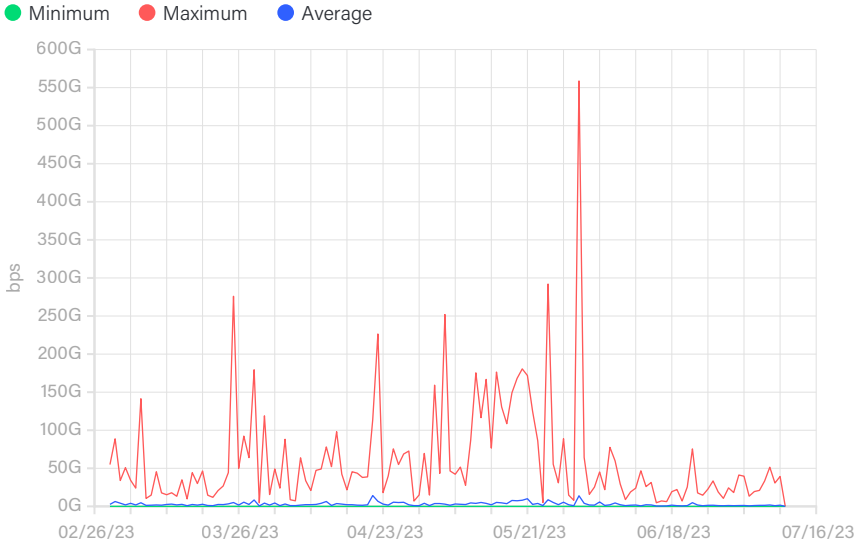


Figure 19: Swedish Attacks Per Day



Last year in our threat report and in several blogs published since, we detailed the presence of DDoS attacks related to ongoing geopolitical and ideological conflicts. Specifically, we know that pro-Russian aligned hacktivists targeted Finland in its bid to join NATO. These attacks had ramifications for Turkey and Hungary as the two countries finally approved Finland's application. Fast-forward to June 2023, and Sweden is on the verge of joining NATO amidst a significant rise in DDoS attacks coinciding with major political dynamics.

On May 3, it was reported that the Swedish parliament website had been the target of a highly disruptive DDoS attack. Sure enough, our global visibility revealed a significant increase in attacks against the country coinciding with the timeline played out in the political theater (Figure 18).

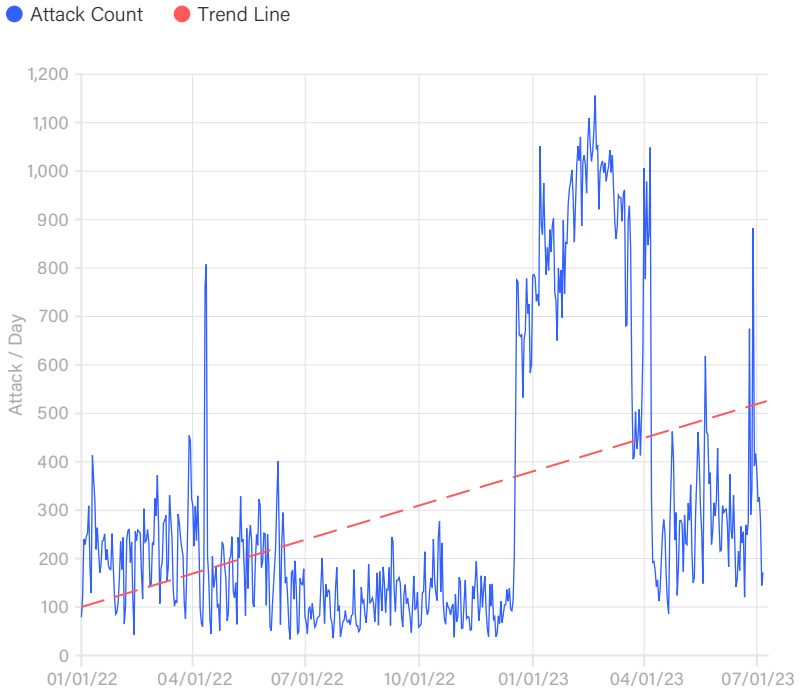
These attacks culminated with a DDoS attack of more than 500Gbps (Figure 19) before finally subsiding in June to a more usual daily attack frequency. It is expected that DDoS attacks targeting Sweden will increase yet again as the ratification of Sweden's bid to join NATO progresses through the political process.

Wireless Advancements Impacts DDoS Landscape

In the first half of 2023, NETSCOUT observed a sharp increase in DDoS attacks against multiple wireless telecommunications providers in APAC (Figure 20). This is a global trend we observed at the end of 2022, with a 79 percent increase in attacks targeted at wireless telecommunications providers. This trend isn't surprising, given the number of commercial 5G networks being deployed globally. According to Analysis Mason's 5G deployment tracker report, there were more than 16 5G networks already deployed or set to launch in 2023.

Although we cannot confirm all these networks were deployed, at least one service provider in the region expanded significant 5G offerings accounting for much of the increase in 2023. The root cause of this shift is almost certainly tied to many former broadband access users moving to 5G fixed wireless access, including gamers shifting their network access. Historically, most attacks in service provider networks have correlated back to gaming in some fashion, prompting a shift in this attack activity to the wireless space.

Figure 20: APAC Daily Attacks: Wireless Telecommunications



Conclusion

Visibility has become an even more important defensive tool for leveling the playing field. Enzo Ferrari said it best: "What's behind you doesn't matter." That is, learn from the past, but look to the future. Lean into visibility to peer around those tight corners to see what's ahead and know where the adversary is headed. Traditionally, the costs of DDoS attacks have been in the attacker's favor. However, when we detect their early actions, such as scanning or trying to use new attack methods, we stop them immediately. By limiting their resources and pushing them to use only one method, we reduce their opportunities to exploit vulnerabilities. By imposing artificial scarcity of resources and forcing attackers into unidimensional methodologies, we help to reduce adversary options for exploitation. This is possible only with our visibility.

Learn from what we see in the NETSCOUT Visibility Without Borders® platform and leverage Arbor Adaptive DDoS protection technology to take control of your future and join NETSCOUT as Guardians of the Connected World®

CONTRIBUTORS

Richard Hummel
Writer

John Kristoff
Writer

Roland Dobbins
Writer

Clark Arenberg
Writer

Chris Conrad
Writer

Kinjal Patel
Writer

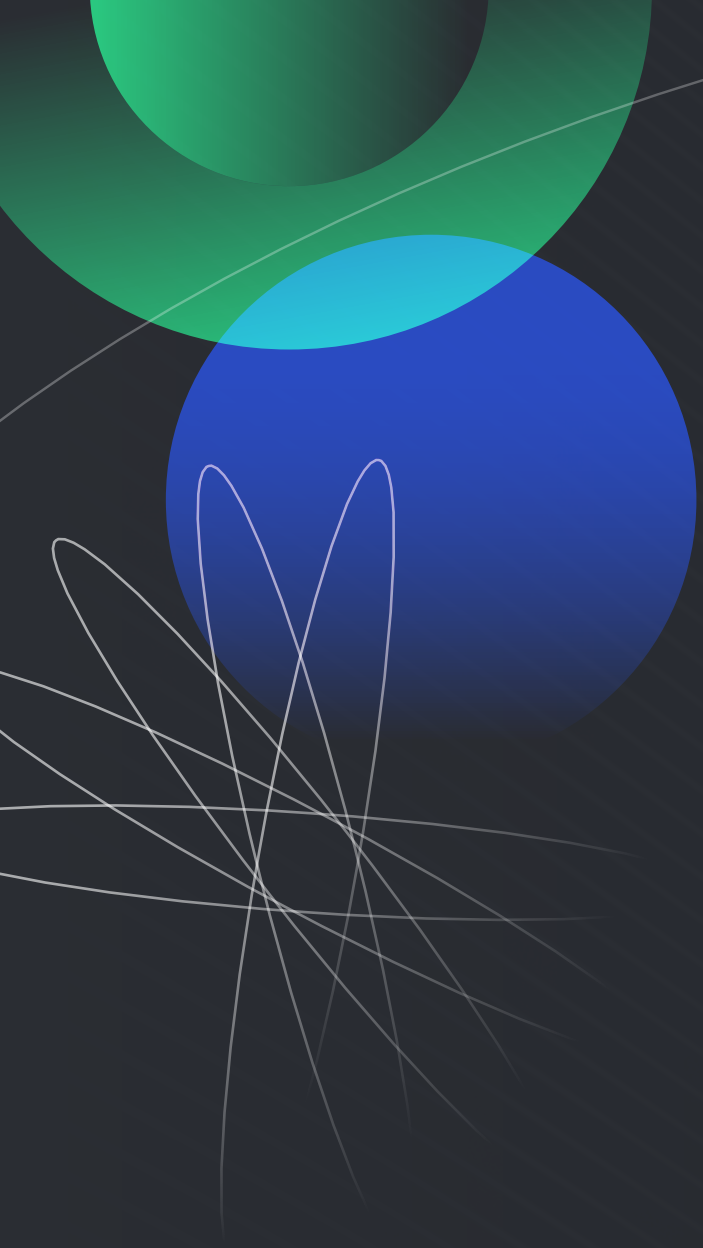
Filippo Vitale
Writer

Max Resing
Writer

Chad Robertson
Writer

Steinthor Bjarnasen
Writer

Roman Lara
Writer



NETSCOUT SYSTEMS, INC.® (NASDAQ: NTCT) delivers multi-purpose, real-time visibility, troubleshooting and protection wherever your technology infrastructure and business applications reside. NETSCOUT Smart Data gives technology and business teams the next-generation level of visibility to see the full range of performance, availability and security risks, earlier and with more precision, to resolve problems faster. That's why the world's most demanding government, enterprise and service provider organizations rely on NETSCOUT solutions to assure and protect the digital services which advance our connected world.

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

NETSCOUT®

SECR_001_EN-2302