NETSCOUT DDoS THREAT INTELLIGENCE REPORT

Issue 13: An Era of DDoS Hacktivism

NETSCOUT.

Introduction

NETSCOUT's 1H 2024 report delivers critical intelligence essential for both daily network operations and high-level strategic decision-making.

This report underscores the growing complexity of DDoS threats, including a notable increase in both attack frequency and sophistication. For instance, the emergence of advanced botnets such as Zergeca and DDoSia, which now employ sophisticated techniques such as DNS-over-HTTP/S for C2 operations, highlights the evolving nature of these threats.

These insights provide a clear roadmap for network operations teams to fine-tune real-time detection and mitigation strategies, ensuring they stay ahead of these evolving threats. Additionally, the report presents a compelling case for investment in advanced DDoS protection systems, especially given the documented surge in targeted attacks on critical infrastructure sectors, including banking and public utilities. Leveraging this actionable intelligence, organizations can bridge the gap between operational readiness and strategic cybersecurity investments, ensuring their digital assets are well-protected against the increasingly sophisticated landscape of DDoS threats.

Contents

All chart data derived from ATLAS.

Key Findings

DDoS Attacks Experienced Surge in Frequency

Application-layer attacks surged by 43 percent in the first half of the year, surpassing the 30 percent increase in volumetric attacks, particularly in Europe and the Middle East. This escalation, driven largely by hacktivist activities targeting global organizations and industries, has not only increased the strain on networks worldwide but also led to more sophisticated attacks. Adversaries are increasingly leveraging resilient, takedown-resistant networks, such as those provided by nuisance networks and bulletproof hosting providers. Our findings show that more than 75 percent of newly established networks are involved in distributed denial-of-service (DDoS) activities within just 42 days of coming online, reflecting the rapid mobilization and integration of any network into the broader attack landscape.

Evolving Capabilities of DDoS-Capable Botnets

ASERT observed a 50 percent growth of bot-infected devices with the emergence of the Zergeca botnet and the continued evolution of the DDoSia botnet used by NoName057(16). These botnets incorporate advanced technologies such as DNS over HTTPS (DoH) for command-and-control (C2) and coordinated DDoS attacks targeting multiple entities, making detection and mitigation more challenging. The trend of implementing a distributed botnet C2 infrastructure, leveraging bots as control nodes, further complicates defense efforts because it's not just the inbound DDoS activity but also the outbound activity of bot-infected systems that need to be triaged and blocked.

Escalating Threats to Critical Infrastructure

Critical infrastructure sectors, particularly banking, financial services, and public utilities, experienced a 55 percent increase over four years. These sectors face frequent and intense multivector attacks, receiving substantial attack traffic.

DDoS Threats

DDoS Attack Classifications

DDoS attacks are intended to disrupt availability, often leading to widespread confusion, operational disruption, and heightened concern. The motivations for these attacks are endless, and although there are many variations of vectors and methodologies, there is an overall DDoS taxonomy grouping the vectors together. Two primary groupings for these attacks are application-layer attacks and volumetric attacks.

APPLICATION-LAYER ATTACKS

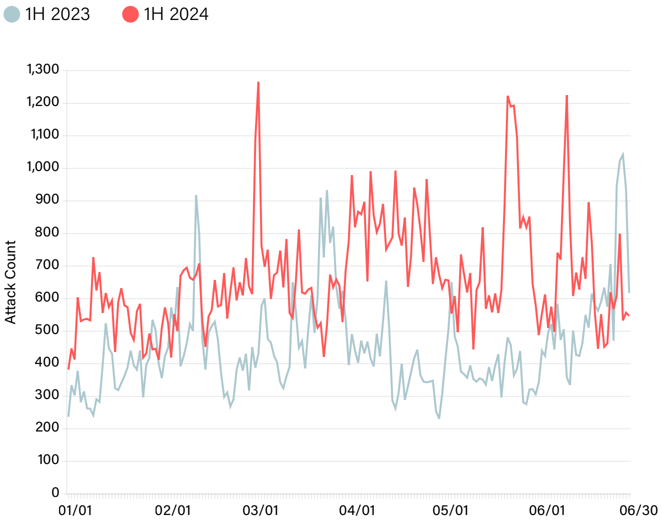
Application-layer attacks target specific implementation details of a protocol or service, causing resource exhaustion.

Common application-layer attacks include HTTP/S GET or POST floods, and domain name system (DNS) query floods. Application-layer attacks often have a smaller network footprint but are more noticeable in service-specific metrics. These attacks can be especially costly with autoscaling features of cloud resident services and require more-sophisticated defense capabilities. Typical constraints are server metrics such as CPU cycles or concurrent transactions.

Notorious threat actors such as NoName057(16) are increasingly focused on application-layer attacks, particularly HTTP/S GET and POST floods, leading to a 43 percent rise compared with 1H 2023 (Figure 1).

These hacktivist groups tend to target specific industries and countries making statements about or giving support to their perceived enemies on the world stage of politics, but they often pick the specific victims arbitrarily. This means that although we can track the overall trends and expectations of a group to go after a country or industry, it's nearly impossible to predict ahead of time which websites or individual network resources may be targeted.

Figure 1: Application-Layer DDoS Attacks 1H 2023 vs. 1H 2024



+43%

Increase in application-layer attacks compared to 1H 2023 (thanks to threat actors such as NoName057(16))

VOLUMETRIC ATTACKS

A volumetric attack aims to completely saturate the network capacity of the target, negating an endpoint's ability to send or receive legitimate traffic, causing packets to be buffered and dropped. These attacks are categorized into two main types.

1 Reflection/Amplification Volumetric Attacks

Reflection/amplification volumetric attacks leverage hundreds of thousands of unknowing users' systems to reflect and amplify massive amounts of internet traffic toward the target. Attackers exploit vulnerabilities in various protocols and services, such as DNS, network time protocol (NTP), or simple service discovery protocol (SSDP), to amplify the amount of data being sent to the target. These attacks are particularly dangerous because they generate traffic volumes that far exceed the capabilities of the original attacking machines, making these attacks highly effective at overwhelming targets.

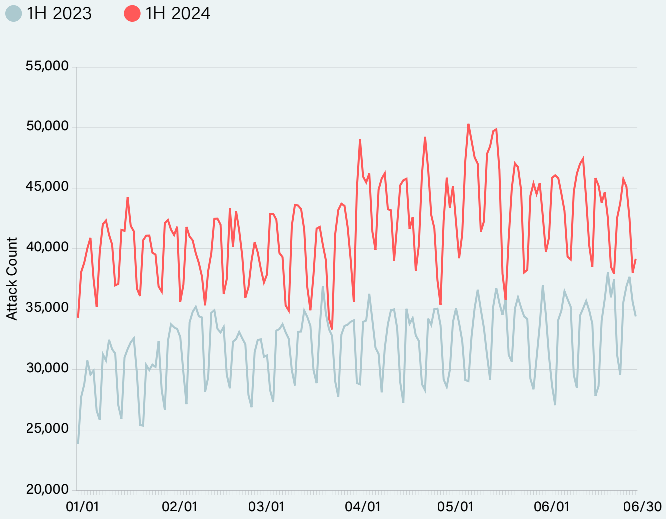
2 Direct-Path Volumetric Attacks

Direct-path volumetric attacks involve sending traffic directly from the attacking systems to the target without the use of intermediaries. These attacks often rely on a botnet of compromised devices to generate a high volume of traffic. Although direct-path volumetric attacks might not benefit from amplification, they can still be highly effective, especially when the botnet size is large and the attack is well-coordinated.

Both types of volumetric attacks risk exceeding the limits of infrastructure along the way to the target—often resulting in collateral damage that can be just as devastating as the attack itself. The primary bottleneck in these attacks is bandwidth and throughput.

During 1H 2024, the number of observed volumetric DDoS attacks increased by 30 percent compared with 1H 2023 and account for most of the ~41,000 DDoS attacks NETSCOUT's ASERT team observes every day (Figure 2). These attacks have become increasingly complex, with attackers using advanced amplification techniques to leverage abusable characteristics of multiple protocols and services.

Figure 2: Volumetric DDoS Attacks 1H 2023 vs. 1H 2024



A More Cohesive DDoS Attack Harness

As we observe the tens of thousands of DDoS attacks every day, trends emerge in the types of infrastructure and their relationship with each other. Some of these relationships surface as we monitor the sources of disruptive online activities such as DDoS attacks, credential-stuffing, invasive scans, brute-forcing activity, exploitation, and malware distribution. However, we recently started seeing DDoS attacks emerge from multiple "nuisance networks" at the same time. These nuisance networks have a business model that revolves around resiliency, anonymity, and freedom to do whatever one desires on the internet.

There are dozens of these network providers, but the following analysis focuses on six of them that we see consistently attack our customer base (Figure 3). In the first half of 2024, approximately 5 percent of observed DDoS attacks on our customers (approximately 2,000 attacks per day) involved at least one of these networks.

Furthermore, half of these incidents involved multiple attack sources located on a single nuisance network, indicating cohesion within the networks. There is a 65 percent likelihood of organizations being targeted by attack sources located on multiple nuisance networks, versus a 35 percent chance involving attack sources located on a single nuisance network.

Tracking this cohesion enables us to identify collaborative attack infrastructures and coordinated threats. During 1H 2024, we observed ~50,000 distinct attack sources located on five of the top six nuisance networks.

~50,000

Distinct nuisance traffic sources reported in 1H 2024

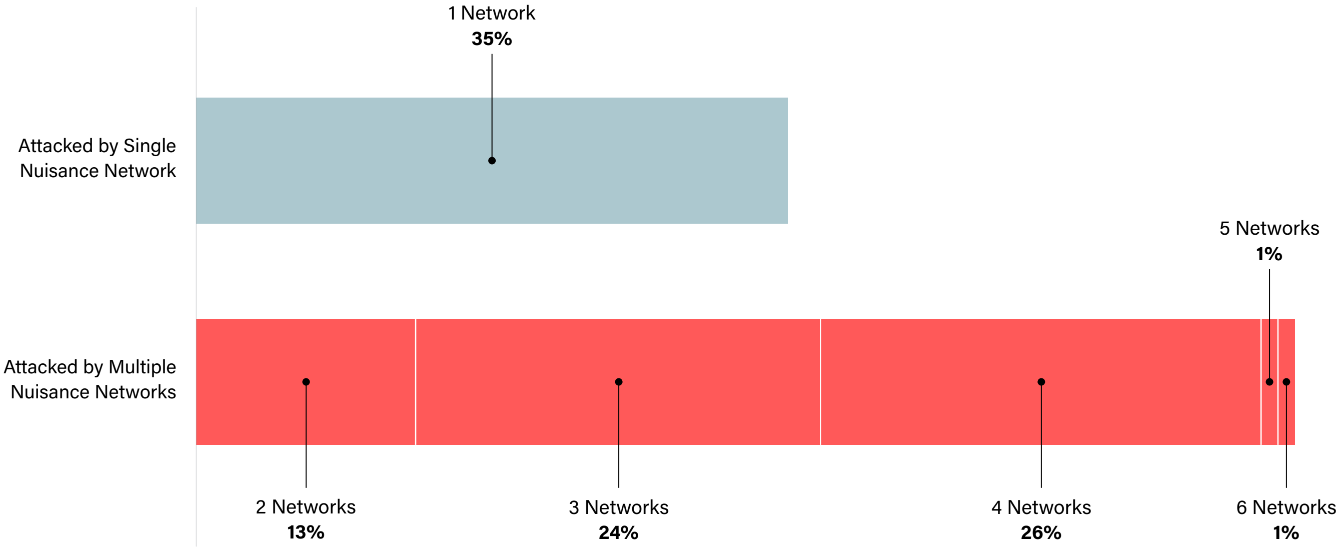


Figure 3: Coordinated DDoS Attacks from Nuisance Networks (1H 2024)

Evolving Capabilities of DDoS-Capable Botnets

The nuisance networks discussed above can facilitate all kinds of attacks—from volumetric to DDoS-capable botnets and even direct-path query floods on critical infrastructure. Botnets sourced from these networks are increasingly common, likely due to their resiliency and the unwillingness of the providers to shut down malicious services running on their networks. Part of this trend to use these less-than-legitimate networks tracks back to advancements in defensive capabilities and anti-spoofing efforts making reflection/amplification less effective.

Adversaries are forced to adapt to the changes in security posture to succeed in launching effective DDoS attacks. In the first half of 2024, there was a significant surge in compromised, botted devices globally, with ASERT observing a nearly 50 percent increase in the numbers of these attack assets in the Asia-Pacific region over the past six months.

While compromised devices act as the operational components of a botnet, the C2 infrastructure serves as its core orchestrator. ASERT's monitoring of DDoS-capable botnet C2 revealed disruptive changes in the threat landscape and an overall decline in total numbers of distinct C2 hosts during 1H 2024 (Figure 4). The reason for the disruption is unknown currently, but in the past, this often meant some coordinated form of botnet takedown, adversaries shifting to new providers, or operations shifting gears.

A new entrant into the DDoS scene is the Zergeca botnet—an entirely new DDoS-capable botnet family coded in the Go programming language. This botnet distinguishes itself by utilizing encrypted DoH via the parallel OpenNIC DNS infrastructure for name resolution of its C2 infrastructure, making identification of botnet nodes more challenging for defenders. Another increasingly prevalent Mirai DDoS botnet variant known as "Aterna" or "CatDDoS" also employs the OpenNIC DNS infrastructure to obfuscate DNS queries related to its C2 infrastructure.

Further innovation by adversaries includes the notorious DDoSia botnet, a federated botnet developed and operated by the hacktivist group NoName057(16). The infrastructure used by the botnet is outsourced to the community, allowing anyone to provide resources. NoName057(16) incentivizes contribution with its own cryptocurrency.

ASERT also observed increased use of active botnet nodes as C2 infrastructure. In some cases, unpatched or misconfigured C2 nodes are compromised and leveraged as attack nodes; in others, botnet operators intentionally make use of dual-purpose nodes to obfuscate the C2 infrastructure and achieve a higher degree of resiliency (Figure 5).

Figure 4: C2 Hosts vs. Infected Hosts (1H 2024)

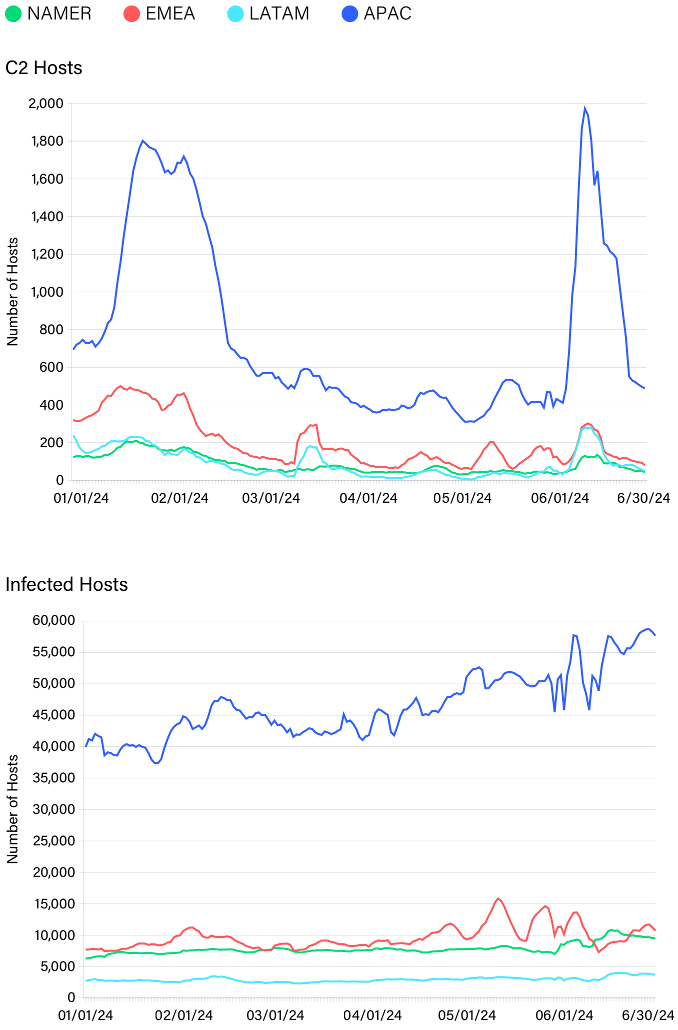
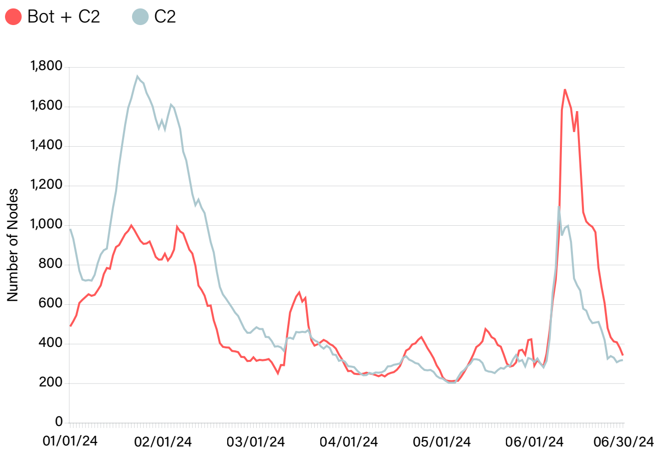


Figure 5: C2 Acting as Zombie Host (1H 2024)



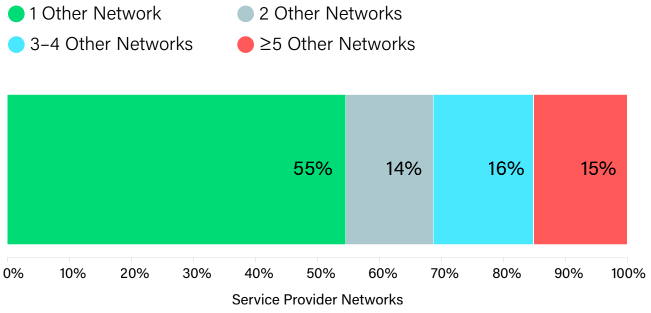
End-to-End DDoS Attack Visibility

All the observations of attack infrastructure and botnet emergence are possible only because of our ATLAS visibility platform, which allows us to see DDoS attacks from networks near the attack's source, along the transit path, and at the target network. This affords us unique insight and positioning to observe trends, detect DDoS attacks, analyze adversary infrastructure, and ultimately aid in defense of our customers' networks.

Our extended traceback abilities allow us to observe attack traffic as it traverses multiple intermediate networks, which is crucial for identifying and tracking both spoofed direct-path attacks and the spoofed attack initiator traffic used to induce reflection/amplification attacks. Among attacks transiting multiple service providers, half were observed by at least one other service provider network, while the remainder were observed by at least two or more (Figure 6). Notably, during 1H 2024, 11 large-scale DDoS attacks were observed by more than 20 service provider networks.

Comprehensive end-to-end visibility enables precise identification and neutralization of threat actors and their infrastructure. Even if attack traffic does not reach its target, we can infer the complete attack profile, thereby better preparing for future threats.

Figure 6: DDoS Attack Visibility Across Multiple Networks (1H 2024)



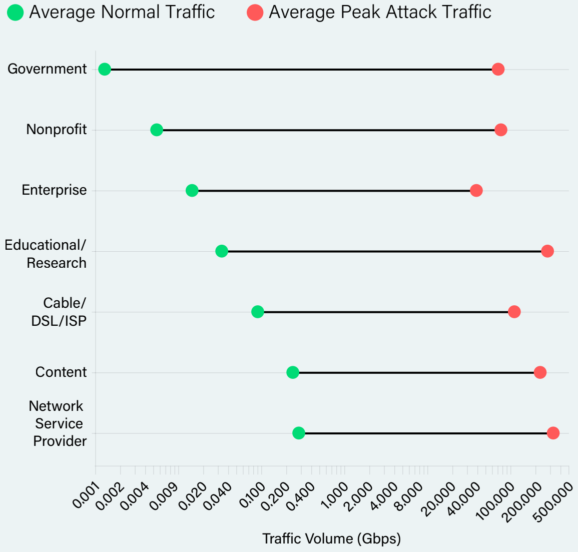
Understanding DDoS Attack Dynamics

NETSCOUT monitors attacks both globally and locally per network to identify global attack trends and provide optimal protection tailored to each network's specific context.

We first determined the global aggregated DDoS attack impact via large-scale analysis of concurrent DDoS attacks. During the first half of 2024, this averaged out to 1,900 attacks, with a total volume of approximately 3.2Tbps and 595.6Mpps, at any given point in time.

Local investigations of the aggregated attack impact per network type revealed that networks with typically lower traffic loads (such as government or nonprofit organizations) report peak attack volumes on the same scale as those experienced by high-traffic networks (such as content and service providers) (Figure 7). This indicates that the relative surge in traffic during attacks is significantly higher for lower-traffic networks (≥4 orders of magnitude) compared with high-traffic networks (3 orders of magnitude). These attack dynamics clearly demonstrate that all network types require substantial mitigation capacities to ensure robust protection.

Figure 7: DDoS Attack Intensity: High vs. Low Traffic Networks (1H 2024)



DDoS Targets

Escalating Threats to Critical Infrastructure

Service availability in critical industries such as banking, financial services, government, and public utilities is of paramount importance. Disruptions in these sectors can have wide-reaching consequences for both civilian populations and national security. Given our assessment that all network types can come under significant traffic load from DDoS attacks, it is crucial to understand the specific trends affecting these industries.

Recently, we highlighted the activities of geopolitically motivated hacktivists and their coordinated DDoS attack efforts (Figure 8). These threat actors have increasingly expanded their focus to include more specific critical infrastructure targets, resulting in a marked increase in the frequency and intensity of daily attacks. Particularly concerning is the surge in attacks against banking and financial services, government institutions, and public utilities such as energy providers. These attacks, which can sometimes escalate by an order of magnitude, pose a significant threat by disrupting vital civilian services in countries that oppose the hacktivists' ideologies.

NETSCOUT's insights into these attacks reveal that an average enterprise in these critical sectors faces attacks delivering up to 1Gbps and more than 330kpps of attack traffic that was not mitigated by an upstream service provider or cloud scrubbing center (Figure 9). The attacks include more than just DDoS, requiring defenders to be prepared for complex, multifront confrontations.

Although many smaller attacks, such as those around 1Gbps, often bypass detection and mitigation by upstream providers due to being below configured thresholds, they can still severely impact enterprises. In some cases, attacks volumes can reach more than 100Gbps, requiring upstream providers to mitigate the attack.

Figure 8: Hacktivist Attack Claims by Industry (1H 2024)

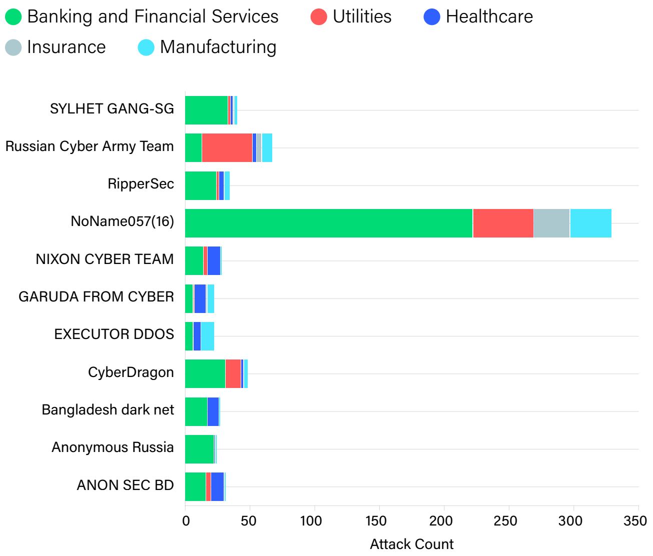
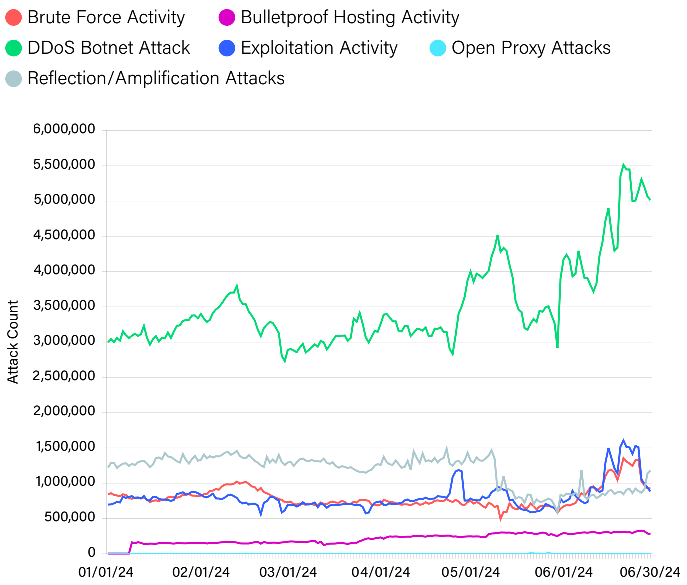


Figure 9: Global Threat Activity: Targeting Critical Sectors (1H 2024)



DDoS Threats in Emerging Networks

As these threats to critical infrastructure intensify, it is important to understand the broader context in which they occur. One aspect is the evolution of the internet itself, which introduces new vulnerabilities and potential attack vectors. In addition to the ever-present DDoS attacks against existing networks, NETSCOUT finds the emergence of new networks and the assignment of autonomous system numbers (ASNs) play a pivotal role. It is important for organizations to plan for DDoS protection when splitting off a portion of a network to a new ASN rather than assume automatic protections from upstream service providers.

Every day, new networks such as hosting providers and startup companies make their debut on the internet. One key indicator of this growth is the assignment of new ASNs and their corresponding Border Gateway Protocol (BGP) announcements into the global internet routing table (Figure 10). Our particular interest lies in the threat activity associated with new ASNs. Specifically, we examine how quickly new ASNs encounter DDoS attacks and whether they participate in DDoS attacks.

Five regional internet registries (RIRs) assign ASNs to networks or local registries. In the first half of 2024, more than 3,100 new ASNs were assigned. The RIPE region (primarily covers Europe, the Middle East, and parts of Central Asia geographically) led with slightly more than one-third of all new assignments, while AFRINIC (covers Africa geographically) had the fewest, with under 100 new assignments. However, assignments only tell part of the story. One-third of newly assigned ASNs were seen originating routes in the first half of 2024.

The average time for newly assigned ASNs to originate routes is roughly 40 days. How soon do new ASNs appear in our DDoS attack telemetry? To answer this, we looked at the cumulative distribution function (CDF) of DDoS attacks and emergent ASNs (Figure 11).

On average, it takes 42 days after announcement before a new network experiences its first DDoS attack. Some networks are attacked almost immediately, while others may not see attacks for several months. Nevertheless, the majority—approximately 75 percent—of new route-originating ASNs in the first half of 2024 were involved in DDoS attacks, either as targets or as participating sources. The mean time until a new network becomes a source in attacks is even shorter.

Figure 10: New ASNs in the Routing Table (1H 2024)

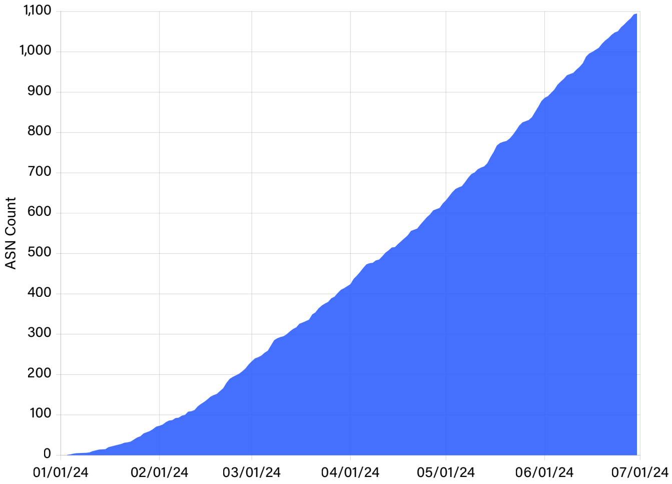
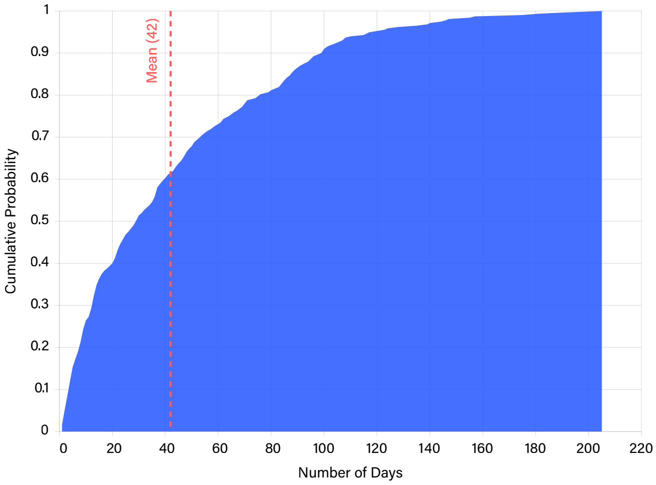


Figure 11: Days from New Route-Originating ASN to Target of an Attack (1H 2024)



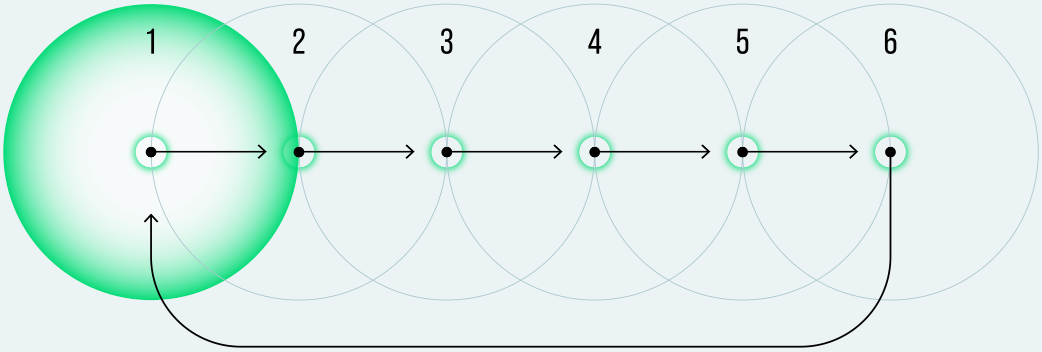
42

Days on average before a new network experiences its first DDoS attack

DDoS Defense

Surviving DDoS Attacks: Strategies and Best Practices

Adversaries abound, threats continue to grow, and networks go through trial by fire way too soon, but all is not lost. It is our belief that a well-prepared network can withstand any DDoS attack. Achieving this state requires the right equipment, planning, testing, training, and continuous improvement. A general state of preparedness for any threat, DDoS included, can be achieved by following NIST guidelines.



SIX PHASES OF INCIDENT RESPONSE

Phase 1

Preparation

Prep the network, create tools, test tools, prep procedures, train team, and practice.

We believe preparation is the most crucial step, because it involves not just implementing the technology needed to detect and mitigate DDoS attacks but also providing the necessary training to operate these tools with high confidence.

Phase 2

Detection

How do you know about the attack? What tools can you use? What's your process for communication?

Phase 3

Classification

What kind of attack is it?

Phase 4

Traceback

Where is the attack coming from? Where and how is it affecting the network?

Phase 5

Reaction

What options do you have to remedy? Which option is the best under the circumstances?

Phase 6

Postmortem

What was done? Can anything be done to prevent it? How can it be less painful in the future?

Typically, we see DDoS attacks as external threats, but we've seen adversaries launch internally facing DDoS attacks, effectively bypassing traditional DDoS defense solutions. In addition to tracking inbound DDoS attack vectors and rates, however, it becomes equally important to track any outbound C2 communications to known DDoS botnet nodes and subsequently to identify when any internally infected bot nodes begin launching high volumes of traffic outbound.

The following steps are methods for enhancing detection for both inbound and outbound DDoS attacks.

1

Track and block malicious traffic

Monitor for specific patterns that trigger amplified traffic, and use threat intelligence feeds to identify and block traffic from known bot nodes and C2 communications.

2

Rate-limit unwanted traffic

Implement rate limiting on uncommon applications and services to detect and prevent abuse of these protocols as a preemptive countermeasure.

3

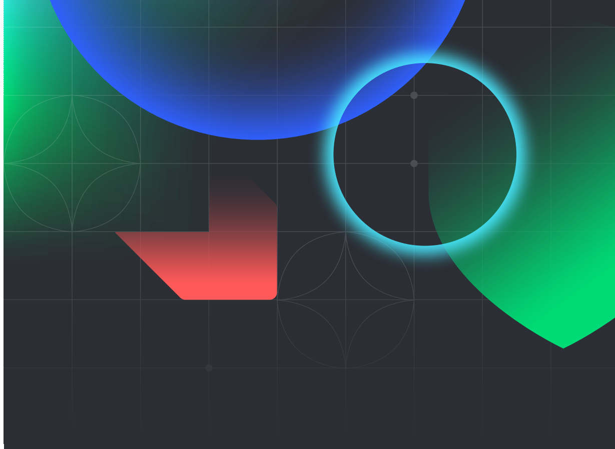
Apply internal and external detections

Use both external-facing detections and internal monitoring to identify outbound DDoS attacks and compromised systems.

4

Utilize filter lists and patch management

Employ reputation databases and custom filters, and ensure that all on-net devices are updated and patched to minimize vulnerabilities, investigate irregularities, and regulate traffic flow effectively.



Final Thoughts

Today's connected world has a pressing need for comprehensive detection and mitigation strategies that address the complexities of modern DDoS threats, even as adversaries indiscriminately pummel organizations of all types. The rapid evolution of attack tactics, especially among emergent ASNs, demands continuous monitoring and adaption. Threat intelligence is a cornerstone in defending against DDoS attacks. It provides the insights necessary to anticipate and counteract malicious activity. By implementing robust security measures, leveraging threat intelligence, and fostering collaboration among sectors, organizations can enhance their resilience against the growing threat landscape.

Contributors

Chris Conrad, Writer
Steinthor Bjarnasen, Writer
John Kristoff, Writer
Marcin Nawrocki, Writer
Kinjal Patel, Writer
Max Resing, Writer
Clark Arenberg, Writer
Roland Dobbins, Writer
Richard Hummel, Editor

netscout.com/threatreport

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 216 countries and territories, 470 industry verticals, and 14,394 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 netscout.com or follow @NETSCOUT on X, Facebook, or LinkedIn.

NETSCOUT®

©2024 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, and the NETSCOUT logo are registered trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. All other brands and product names and registered and unregistered trademarks are the sole property of their respective owners.