

NETSCOUT®



5th Anniversary DDoS Threat Intelligence Report

UNVEILING THE NEW THREAT LANDSCAPE

FINDINGS FROM 2ND HALF 2022



The rising tide of DDoS attacks threaten organizations worldwide that deliver critical access and services. This tide brings new threats, evolving tactics, and a doubling-down on adversary methodologies to launch hybrid application-layer and botnet-based direct-path DDoS attacks.

CONTENTS

- 2 Key Findings**
- 3 NETSCOUT Visibility**
- 4 DDoS Attack Timeline**
- 5 Worldwide Internet Visibility**
- 5 Visibility Is the Key to Successful DDoS Defense**
- 8 DDoS Botnet Impact**
- 9 DDoS Attack Vectors and Methodology in Focus**
- 11 Dissecting a DDoS Attack**
- 12 DDoS Attack Motivations**
- 14 Conclusion**

From our first Worldwide Infrastructure Security Report (WISR) in 2005 to our 5th Anniversary DDoS Threat Intelligence Report today, we have witnessed a tenfold increase in DDoS attacks. These attacks evolved from simple denial-of-service to dynamic distributed denial-of-service where attacks evolve and adapt to counter network defenders. This is unfolding while adversaries continue to expand and launch new botnets to devastating effect, creating a shifting paradigm with direct-path attacks at the center. Complex multi-vector attacks and more sophisticated adversary methodologies have become commonplace, highlighting the need for intensive scrutiny of the threat landscape and an ever-evolving defense-in-depth positioning to weather the onslaught of attacks that include carpet-bombing to application-layer and state-exhaustion attacks.

These attacks have a very real impact as reported by our customers, the largest service providers and enterprises in the world. We continue to invest heavily in research and development of our Visibility Without Borders® ATLAS platform, as we have done for over the last two decades. ATLAS is the key to understanding these threats, learning from them, and positioning organizations to mitigate these attacks. It is also the fuel that powers this DDoS Threat Intelligence Report, enabling global DDoS awareness and defense. We would like to thank our customers for supporting and joining us in this mission, as Guardians of the Connected World.

A handwritten signature in black ink that reads "Anil Singhal".

ANIL SINGHAL, CEO, NETSCOUT

Key Findings



Scaling Internet Traffic to Infinity and Beyond

NETSCOUT's ATLAS platform has visibility into an average of 401 Tbps of internet traffic, a staggering aggregate average of 34.6 exabits per day and greater than 50 percent of estimated international transit capacity. Meanwhile, the peak sum of DDoS alert traffic in one day reached as high as 436 petabits and more than 75 trillion packets in the second half of 2022; a global surge in bandwidth/throughput in July drastically increased these benchmarks, with service providers scrubbing a large percentage of malicious traffic, especially high-severity alerts. At the same time, enterprises eliminated an additional daily aggregate average of 2.5 petabits of unwanted traffic.



Bad Bots in Business

Threaded throughout the massive amounts of aggregate bandwidth and throughput is a dangerous trend that started in 2021, in which bots feature more prominently in attacks, accelerating the throughput rates at an astonishing pace. Separated by a growing margin, direct-path bot attacks dominate the top of the attack toolkit, resulting in millions of bots launching hundreds of thousands of attacks on enterprises and service providers alike, many of which caused significant disruptions.



Rising Tides in Attack Methodology

From TCP direct-path attack vectors to carpet-bombing and application-layer attacks against DNS servers and websites, adversaries accelerated their adoption of attack targets and techniques, resulting in huge increases in the second half of 2022.



Dissecting an Adaptive DDoS Attack

What may seem mundane is actually incredibly complex. DDoS attacks span countries, networks, and techniques like water finding a path through any available means. A single attack can span dozens of countries and networks. As one attack against the energy sector illustrates, organizations must adopt new strategies such as adaptive DDoS defense to combat the growing complexity.



DDoS Attack Motivations Know No Bounds

From nihilism to extortionism, adversaries leverage DDoS attacks to incite fear, cause mayhem, and cash out. Organizations experienced a veritable smorgasbord of DDoS attack motivations in 2022 stemming from events in late February as websites were taken offline just prior to the Russia-Ukraine war. Those events created a cascade of attacks against dozens of countries and industries that continue to this day. National security and government, manufacturing, wireless telecommunications, and even the optics industry experienced these diverse motivations in the DDoS threat landscape.



NETSCOUT

VISION

The visibility NETSCOUT gains from our ATLAS platform spans the entire globe, with historical data over multiple decades, to bring trends and real-time analytics to the research team and our [Threat Horizon Portal](#).

The following statistics reveal the depth of our visibility across the global internet:

500+

INTERNET SERVICE PROVIDERS (ISPs)

More than two decades of working with more than 500 internet service providers (ISPs) has allowed us to build a sensor network that spans more than 50 percent of the world's largest networks.

93/Day

COUNTRIES & TERRITORIES

ATLAS collects DDoS attack statistics from an average of 93 countries every day—effectively half of the world.

+807%

INCREASE IN DDoS ATTACKS OVER TIME

ATLAS data reveals that DDoS attacks are one of the most frequent cybersecurity threats facing organizations today. They jumped from hundreds to thousands between 2005 and 2013 and increased 807 percent from ~325,000 in Q1 2013 to ~2.9 million in Q1 2022.

~13M

CURRENT DDoS ATTACKS

DDoS attacks nearly reached a plateau of 13 million for 2022—a new high water mark for attack frequency—all while adversaries become more adept at evading defense and traditional DDoS mitigation.

TCP

DIRECT-PATH ATTACK PREVALENCE

From 2006 to 2021, volumetric attacks reigned supreme, with DNS amplification at the forefront. It was in early 2021 when we detected a tectonic shift in preference by adversaries to TCP-based, direct-path attacks—a move that carries throughout 2022 and one that organizations and enterprises must address to protect stateful devices and downstream customers.

ATTACK DURATION BREAKDOWN

Over the past four years, more than 4 million DDoS attacks lasted longer than one hour and a quarter of those lasted more than 12 hours, underscoring the importance of having adaptive DDoS solutions that can simultaneously handle short-lived and long-lived attacks.

Attack Duration Breakdown (2019–2022)

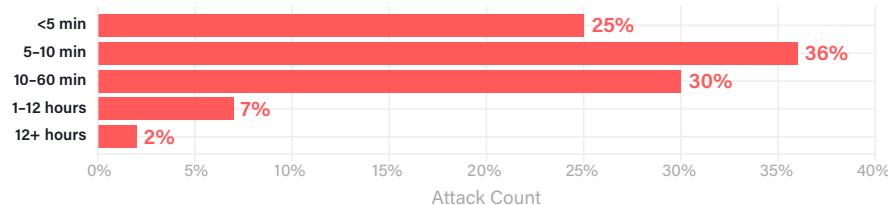


Figure 1: Attack Duration Breakdown (2019–2022) (Data: ATLAS)

MULTI-VECTOR ATTACK BREAKDOWN

Multi-vector attacks made up more than 40 percent of all DDoS attacks with 29 percent between 2 and 5 vectors, 8 percent between 6 and 10, and 3 percent leveraging more than 11 vectors in a single attack. This equates to more than 250,000 DDoS attacks using more than 10 vectors in a single attack, once again illustrating the importance of adaptive DDoS practices.

Multi-Vector Attack Breakdown

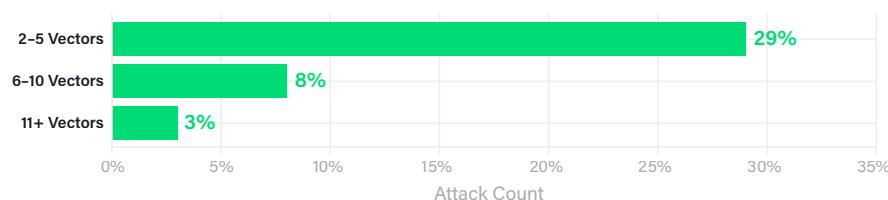
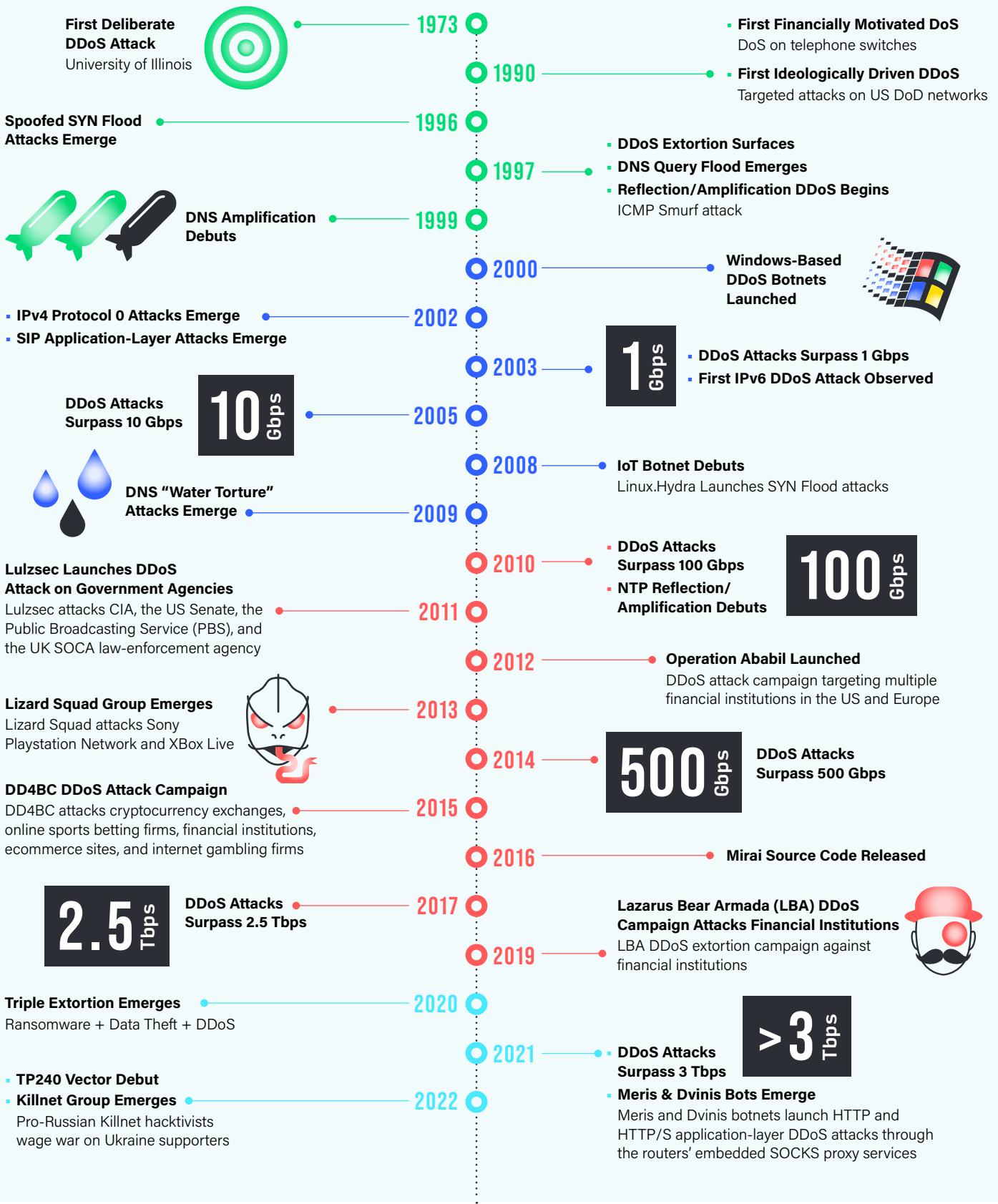


Figure 2: Multi-Vector Attack Breakdown (Data: ATLAS)

DDoS Attack Timeline



Worldwide Internet Visibility

Global visibility is key to assessing the DDoS threat landscape. Without visibility, it would be extremely difficult to create a timeline of history, identify trends, and adequately prepare for and defend against network-based attacks such as DDoS. Our global sensor network gives NETSCOUT incredible visibility into the networks around the world, allowing us to see a staggering 401+ Tbps average of internet traffic (Figure 3)—an estimated 50 percent of international transit capacity. That is 3 petabytes or 24.06 petabits of transit per minute!

Daily Average Tbps In/Out

● In ● Out

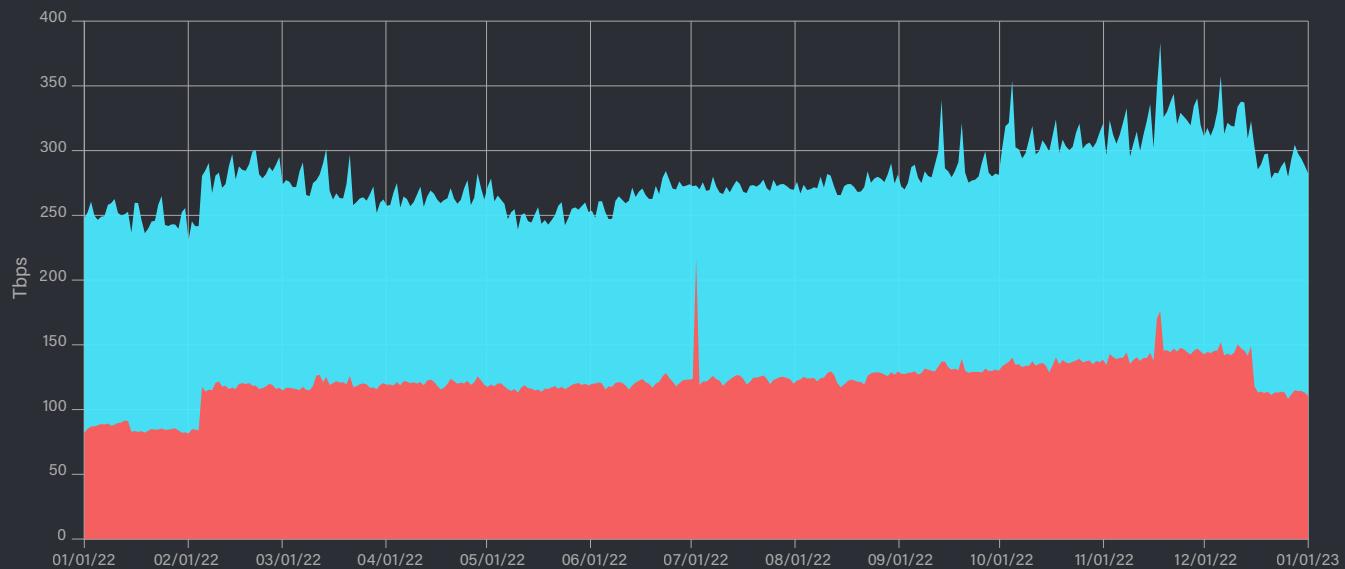


Figure 3: Daily Average Tbps In/Out (Data: ATLAS)

Visibility Is the Key to Successful DDoS Defense

Internet Service Providers (ISPs)

Global insights from just shy of 13 million attacks in 2022 allow us to precisely detect and pinpoint DDoS-related traffic.

39.13 Tbps

Cumulative peak for one hour

This metaphorical “needle in the haystack” peaks at a cumulative maximum for one hour of 39.13 Tbps on April 17, 2022.

389.57 Tbps

Aggregate peak for one day

The aggregate peak for one day occurred on November 30, 2022, with a cumulative maximum of 389.57 Tbps (44,497 DDoS attacks contributed to this cumulative value).

Examining our global telemetry revealed that approximately 25 percent of all our customer alerts move into active mitigation (Figure 4). ISPs must prioritize what alerts and traffic to mitigate while balancing between cost, capacity, and service disruption for customers. This translates to many attacks not receiving mitigation as the provider absorbs the attack across its network footprint and focuses on the most impactful attacks likely to disrupt the largest number of networks and customer services.

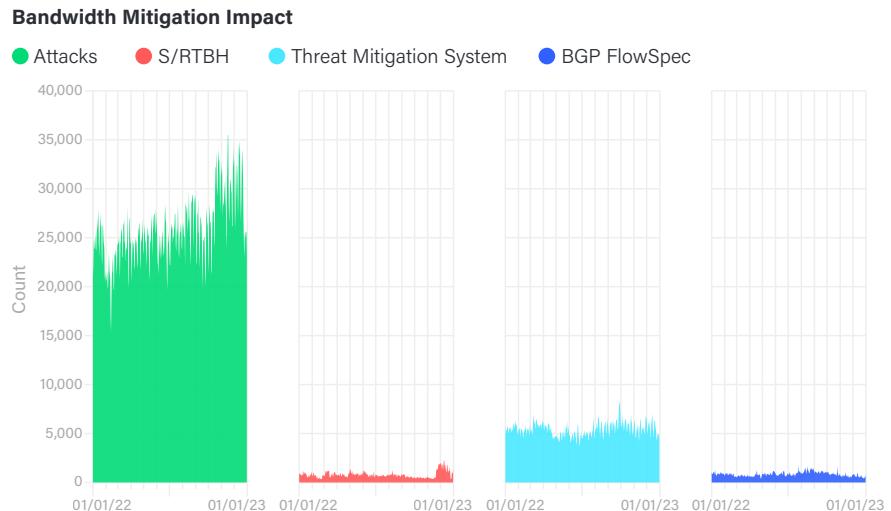


Figure 4: Bandwidth Mitigation Impact (Data: ATLAS)

Bandwidth Mitigation Impact

● Sum Bandwidth ● Sum Bandwidth Mitigated

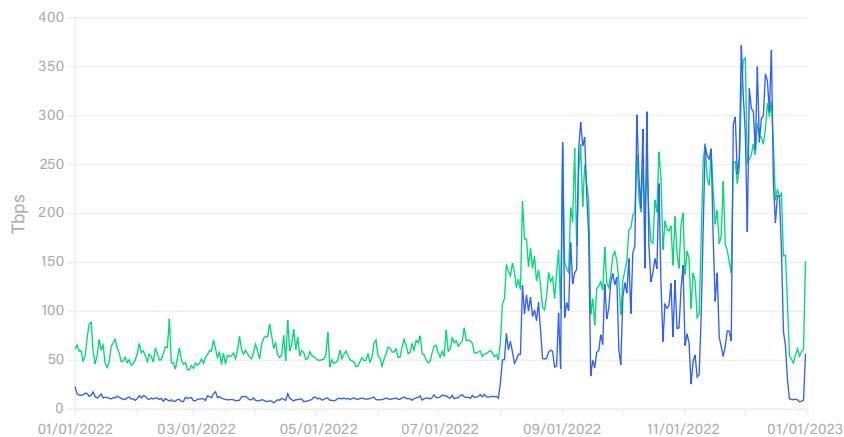


Figure 5: Bandwidth Mitigation Impact (Data: ATLAS)

Throughput Mitigation Impact

● Sum Throughput ● Sum Throughput Mitigated

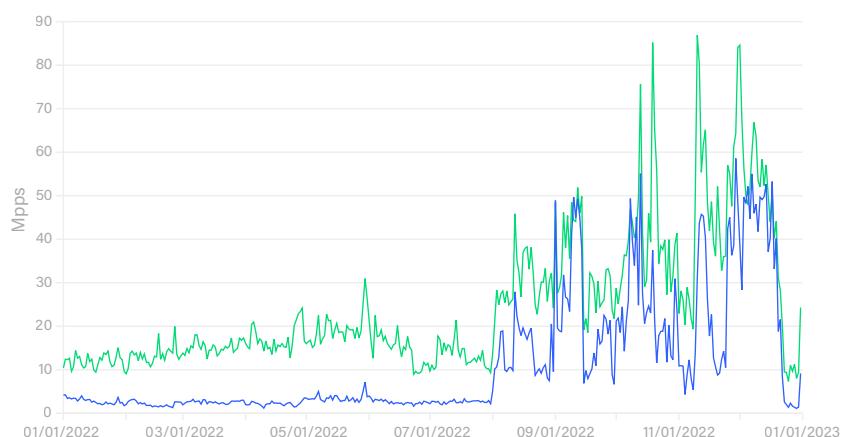


Figure 6: Throughput Mitigation Impact (Data: ATLAS)

However, a smaller number of mitigations compared with alerts does not tell the whole story. When looking at the bandwidth (Figure 5) and throughput (Figure 6) of the alert traffic, we see an entirely different metric play out. Our analysis reveals that approximately 25 percent of normal baseline traffic is mitigated due to some alert threshold established by our customers, but when impact bandwidth and throughput reaches higher severity, ISPs drop 80 to 100 percent of the attack traffic. At times, the use of BGP FlowSpec will even exceed the 100 percent mitigation threshold as entire ports and protocols get dropped in routing.

The previous graphs tell a particularly important truth. Not all alert traffic will be mitigated by the ISP networks. This is especially true when the impact of alerts is lower in severity. As previously discussed, ISPs must balance cost, capacity, and providing services to consumers. Thus, enterprises and downstream consumers should consider investing in on-premises or hybrid DDoS mitigation solutions to bolster their defensive posture.

Enterprise

With 13 million attacks in the ISP networks, we turned our attention to the enterprise, where we gathered data from one-fifth of our enterprise customers and found more than 3,500 events per day or 145 per hour. These events stemmed from high-impact traffic tripping predefined thresholds, creating a denial-of-service (DoS) alert. Not all of these alerts are DDoS attacks; high-throughput scanning also can trip these thresholds. Nonetheless, these events along with GeoIP blocks, application-layer attacks, and inbound brute-forcing/exploitation resulted in traffic being dropped to downstream users on these networks.

The following ATLAS statistics highlight the amount of mitigated anomalous traffic in enterprise environments every day:

3.5 Petabits

Mitigated bits daily

Average amount of daily bytes equating to approximately 3.5 petabits of data, the equivalent of almost 2,000 days (about five-and-a-half years) of 4K streaming video

2.5T

Packets daily

2.5 trillion packets (the DeLorean only needed 1.21 trillion watts to time travel!)

3.2 Tbps

Traffic daily

A daily aggregate of about 3.2 Tbps of traffic (consider the largest single attack recorded now is 3.4 Tbps)

Contrary to the 25 percent mitigation ratio for ISPs, nearly every alert in the enterprise environment resulted in application of preconfigured countermeasures, a large majority of which are GeoIP blocking (Figure 7).

Many of our enterprise customers rely on GeoIP blocking configurations to stop unwanted traffic from entering their networks. At least a third of our customers utilize some form of GeoIP blocking or policing, and one-quarter of those deployments always have at least one country in a blocking configuration. In contrast, the remainder have an average of 70 countries blocked, suggesting heavy restrictions on inbound traffic.

Based on our analysis of attack origination, these country restrictions block a substantial portion of malicious traffic in the DDoS threat space.

Enterprise Alerts

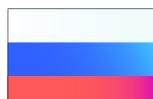
● Enterprise Alerts ● Countermeasures Applied



Figure 7: Enterprise Alerts (Data: ATLAS)

The top five countries with heavy restrictions on inbound traffic include:

1 RUSSIA



2 CHINA



3 UNITED STATES



4 NORTH KOREA



5 AFGHANISTAN



DDoS Botnet Impact

Threaded through all the statistics about network bandwidth, throughput, and attack frequency is the continuing driver of direct-path, botnet-sourced attacks. This is even more relevant for the enterprise statistics, because enterprises tend to receive the largest portion of bot-based attacks. A large majority of direct-path attacks come from DDoS botnets such as Mirai, Satori, and even lists of proxy servers leveraged by groups such as Killnet.

In 2022, NETSCOUT tracked approximately 1.35 million bots from malware families such as Mirai, Meris, and Dvinis. The analysis covers attack statistics for enterprises and ISPs and identifies the countries and industries targeted. The scale of attacks on the enterprise (Figure 8) illustrates the dominance of bot attacks against enterprises as opposed to ISPs (Figure 9).

Enterprise: Bot-Sourced Attacks

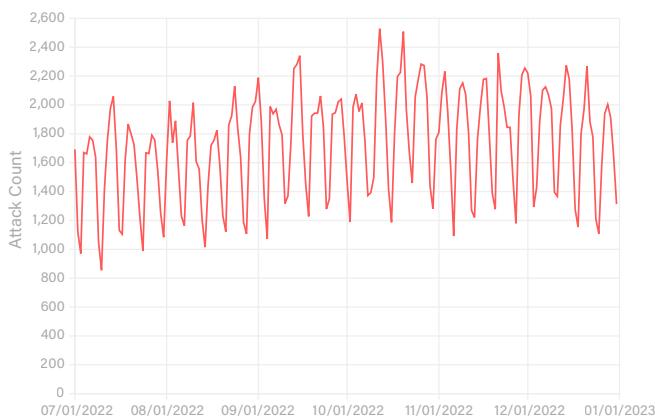


Figure 8: Enterprise: Bot-Sourced Attacks (Data: ATLAS)

Service Provider: Bot-Sourced Attacks

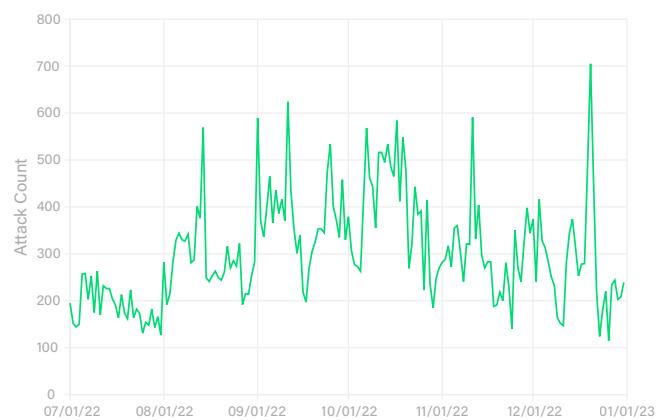


Figure 9: Service Provider: Bot-Sourced Attacks (Data: ATLAS)

Enterprise

SECURITY-RELATED ALERTS

350,000+

AVERAGE IMPACT PER BOT NODE

~5 Gbps

TOP ATTACK SOURCE COUNTRIES



China

TOP ATTACK TARGET COUNTRIES



United States

TOP TARGETED INDUSTRIES

Federal/state/regional government organizations
and banking-related companies

Internet Service Providers (ISPs)

ATTACKS IN ISP NETWORKS

~60,000

TOP ATTACK SOURCE COUNTRIES



United States



China



South Korea

TOP ATTACK TARGET COUNTRIES



South Korea



United States



Italy

BOTNET-SOURCED ATTACKS INVOLVED

TCP SYN floods and reflection/amplification attacks

DDoS Attack Vectors and Methodology in Focus

Direct-path and volumetric DDoS Attacks are equally responsible for causing mayhem on the global stage, but it is more than just one or the other. To understand the impact, we must further break these attacks down into their parts. First, we look at the continuing trend of TCP-based attacks. The top five vectors clearly illustrate the preference of adversaries in 2022 with four out of the five including an overwhelming majority of TCP-based attacks.

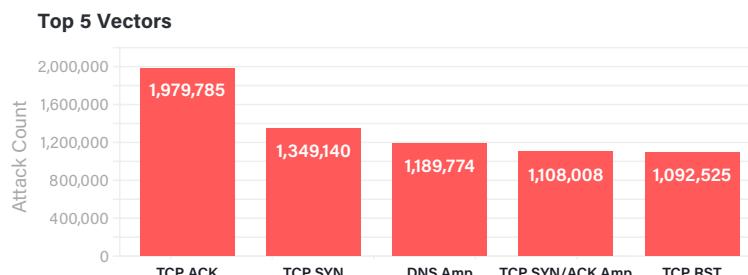


Figure 10: Top 5 Vectors (Data: ATLAS)

Inside these vectors, we next look at the types of attacks.

For this we break it down into four distinct categories:

1 HTTP and HTTPS Application-Layer Attacks

HTTP and HTTPS Application-Layer Attacks

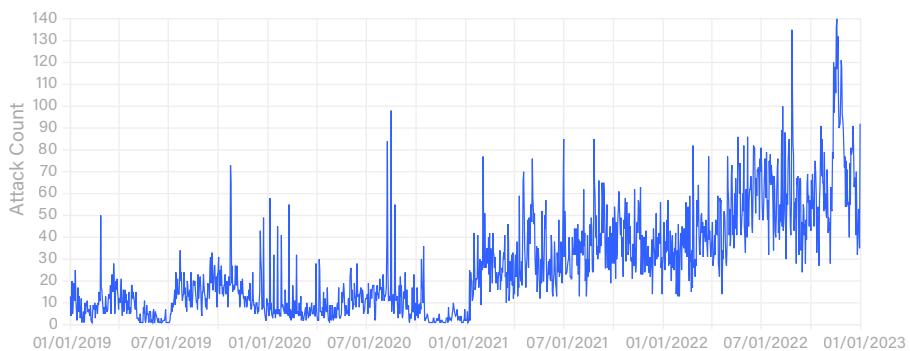


Figure 11: HTTP and HTTPS Application-Layer Attacks (Data: ATLAS)

Today, there are more than one billion websites on the internet, and it should come as no surprise that websites are often the target of DDoS attacks. We witnessed how devastating these types of attacks can be with the events preceding the Russo-Ukrainian conflict knocking out key financial, government, and media sites prior to ground forces invading. Based on a sampling of our data set, we witnessed a 487 percent increase in HTTP/HTTPS attacks since 2019 (Figure 11).

2 Direct-Path DDoS Attacks

Reflection/Amplification vs. Direct-Path Attacks

● Reflection/Amplification Attacks ● Direct-Path Attacks

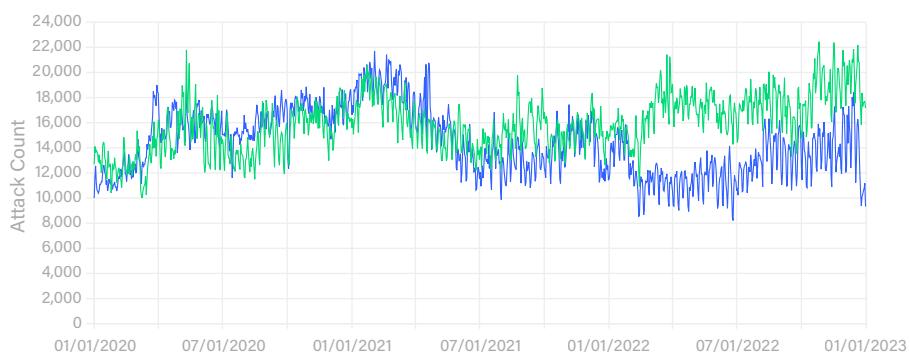


Figure 12: Reflection/Amplification vs. Direct-Path Attacks (Data: ATLAS)

Several times we have noted adversary preference for TCP-based direct-path attacks—and for good reason. These attacks are growing at an alarming rate and often are harder to mitigate than reflection/amplification attacks, which can be mitigated with BGP Flowspec or other well-established countermeasures. While reflection/amplification attacks declined 18 percent since 2020, direct-path attacks climbed 18 percent over three years, creating a difference of nearly 2 million attacks between them (Figure 12).

3 Carpet-Bombing Attacks

Carpet-bombing DDoS attacks target entire IP address ranges rather than a single host. These attacks are intended to evade common DDoS detection mechanism. This trend started in November 2021 and really accelerated in August 2022. Daily attacks using this method rose from an average of 670 in 2021 to an average of 1,134 in 2022, a 69 percent increase. Comparing the first half of 2022 with the second provides an even greater increase of 110 percent in this methodology being leveraged by adversaries (Figure 13). A brief segue into industries targeted with this method revealed most attacks were against ISP networks.

Carpet-Bombing Attacks

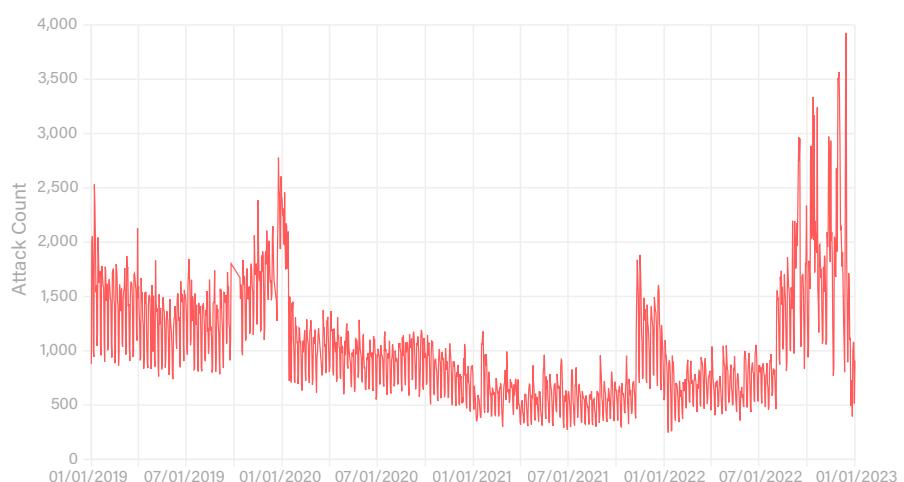


Figure 13: Carpet-Bombing Attacks (Data: ATLAS)

4 DNS Query Flood (DNS Water-Torture) Attacks

A form of application-layer attack, DNS query floods have more than tripled since they really became weaponized in 2019, a 243 percent increase in adoption of this attack technique (Figure 14). The average daily attack count for 2022 is approximately 850 attacks, a 67 percent increase over the 522 average in 2021.

DNS Query Flood (DNS Water-Torture) Attacks

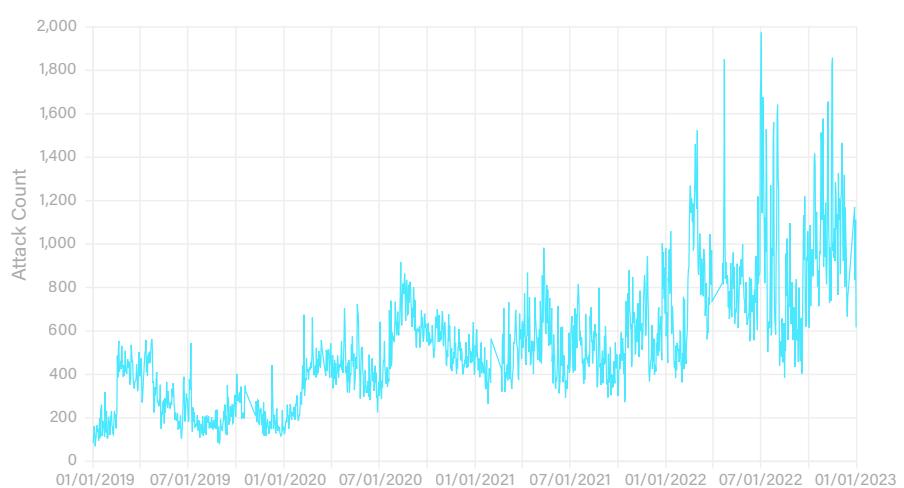


Figure 14: DNS Query Flood (DNS Water-Torture) Attacks (Data: ATLAS)

Further sub-divided into regions, the following increases in this attack technique indicate adversaries are using it everywhere:



APAC



EMEA

+108%

Increase in daily average

+131%

Increase in daily average



LATAM

+15%

Increase in daily average



NAMER

+41%

Increase in daily average

Most attacks of this nature affect ISPs, however in the second half of 2022, adversaries used this tactic to target both the national security and commercial banking sectors in North America (NAMER) and Europe, the Middle East, and Africa (EMEA). There is a high degree of certainty that these attacks are almost exclusively related to the ongoing conflict between Russia and Ukraine.

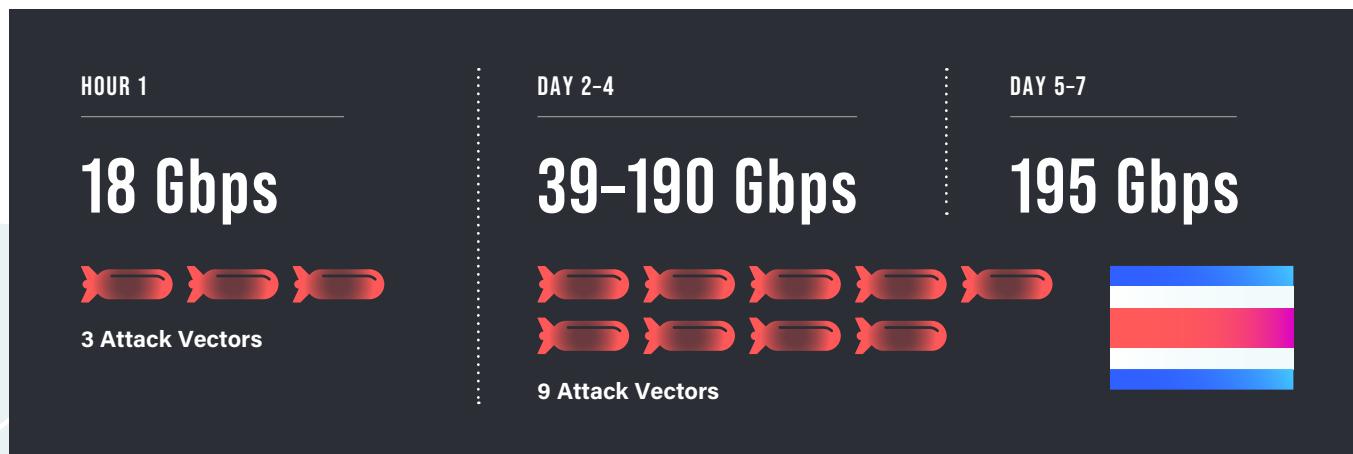
Dissecting a DDoS Attack

What does a DDoS attack look like when dissected in detail?
The following attack analysis shows how much variation
is present throughout an attack or alert.

On December 26, 2021, an attack targeting an energy company in Costa Rica began—an attack that would usher in the new year as it spanned an entire week with multiple vectors, hundreds of attack sources, at least 10 countries of origin, and more than 35 networks spanning the globe.

The initial attack contained only a handful of attacking IP addresses. As time passed, this climbed and peaked at 111, including several aggregate CIDR blocks, up to a /15 (source IP address aggregation occurs when the source IPs become distributed enough to warrant consolidation.) By Day 6, the number of source CIDRs fell to half before climbing to nearly 100 IP addresses by the end of the attack.

The adversary started by using three different attack vectors, and by the midway point of the attack had increased it to nine different attack vectors spanning both volumetric (UDP-based reflection/amplification) and direct-path TCP-based vectors.



In addition to the changing vectors, the attack originated from more than 200 TCP/UDP ports while targeting more than 300 TCP/UDP ports. The variability in ports brings with it some challenges in that much of the traffic would not be mitigated using flowspec rules. Further, typical UDP-based countermeasures would also be ineffective against the direct-path TCP-based attacks. While geo-based blocking could help with mitigation, the adversary may have had lists of reflectors/amplifiers or botted nodes in additional countries with which to launch attacks, potentially rendering any geographical countermeasures less effective.

Due to the ever-shifting, complex nature of attacks, a comprehensive, hybrid approach with NETSCOUT's adaptive DDoS defense is critical. This approach marries traditional defense and mitigation with threat intelligence-driven countermeasures and ultimately DDoS suppression to cut off attacks at the source.

DDoS Attack Motivations

Having stripped a DDoS attack down to its individual components, we now examine the motivations behind it. These range from online gaming-related grudges to acts that are political in nature, and unfortunately, not every attack has an explanation. Take, for instance, the following attacks against industries spanning the gamut.



Optical Instrument and Lens Manufacturing

In the second half of 2022, a barrage of DDoS attacks hammered the optical instrument and lens manufacturing sector, resulting in a 14,137 percent increase in attacks against this industry in EMEA (Figure 15). The attacks almost exclusively targeted one major optics distributor, with more than 6,000 attacks over a four-month period ranging from 1 Mbps and 1.6 Kpps to 260 Gbps and 42 Mpps. Thorough research failed to discover any significant cause for this sustained DDoS activity. These attacks demonstrate that no one and nothing is off limits to adversaries in an increasingly connected digital world.

Optical Instrument and Lens Manufacturing

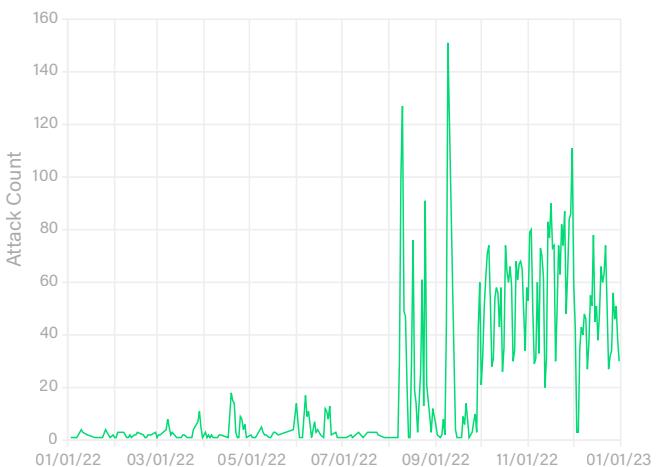


Figure 15: Optical Instrument and Lens Manufacturing (Data: ATLAS)



Wireless Telecommunications

The growth of subscribers and 5G wireless to the home, for both mobile and Internet of Things (IoT) devices, has grown at an incredible pace from 12.6 million in 2019 to a projected 1.6 billion by the end of 2023, a staggering 12,720 percent increase. This growth brings with it a vibrant playground for adversaries to conscript 5G-connected devices into attacks. It also presents an opportunity for attacks to target more types of devices and network access points than ever before.

Although not as impressive in growth, DDoS attacks on the wireless telecommunications industry has grown 79 percent since 2020 (Figure 16), which equates to 20 percent of all DDoS attacks on any industry and second only to attacks on Wired Telecommunications carriers. With 80 to 90 percent of all DDoS attacks sourced from and directed at devices on wireline networks, the increases in attacks on wireless coincide with the continued adoption of 5G to the home. Historically, these attacks are motivated by the gaming industry or underground gambling associated with esports.

Wireless Telecommunications

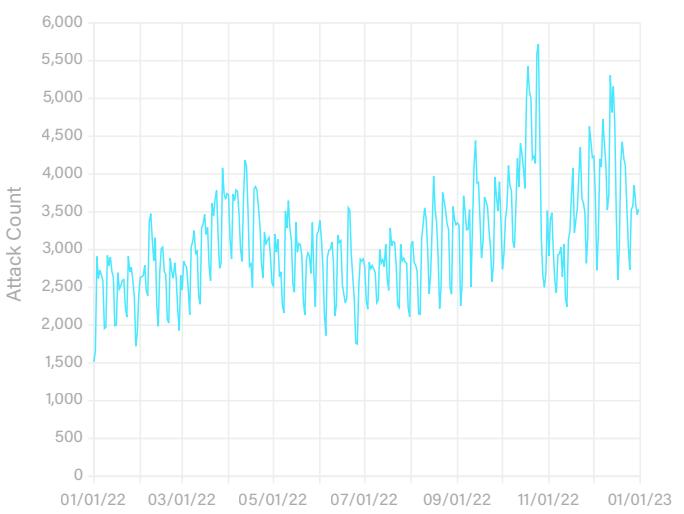


Figure 16: Wireless Telecommunications (Data: ATLAS)



Manufacturing

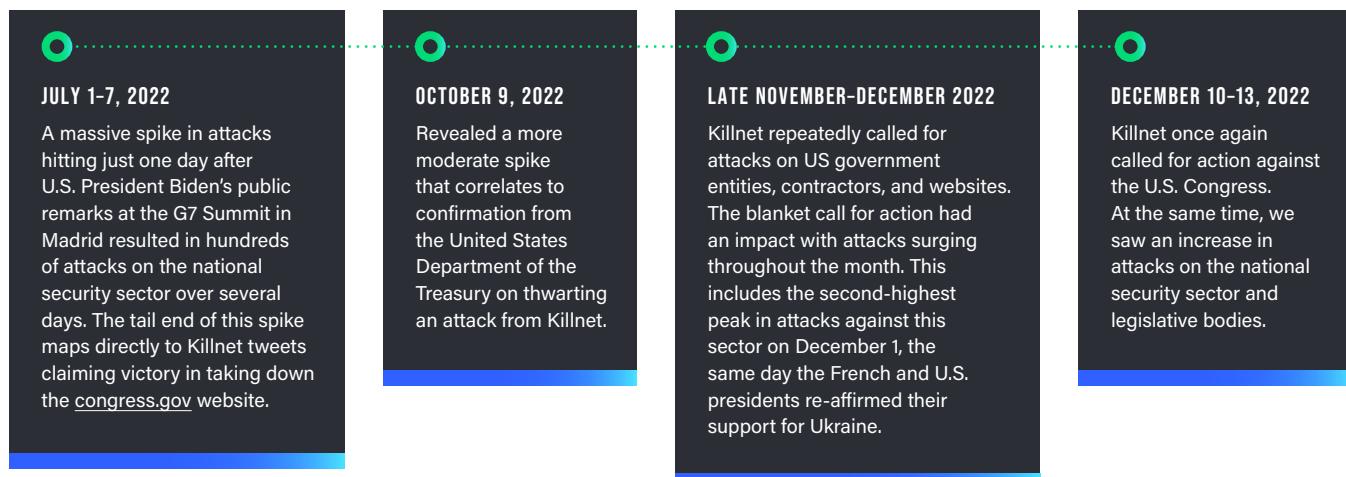
Between January and April 2022, we observed a massive application-layer attack launched against a large manufacturer. Beginning on January 7, countermeasures blocking malformed packets and abuse of Transport Layer Security (TLS) connections dropped an average of more than 950 billion packets per day over a four-month sustained period (Figure 17). For comparison, prior months often saw that amount of blocking over a week's time period. Certainly not coincidentally, the manufacturing organization experienced a ransomware attack that culminated in halting production over this same period. Given the combination of DDoS attacks and ransomware, the adversary likely attempted to extort the victim for monetary gain.



Government and National Security

The second half of 2022 brought with it a massive 16,815 percent increase in attacks against national security sector in the United States (Figure 18). Analysis of the spikes in DDoS attacks overwhelmingly pointed to the pro-Russia Killnet group as the responsible party for launching a barrage of attacks on government organizations and websites because of the country's continued support for Ukraine. Although many of these targeted entities do not directly fall under national security, we know from prior investigation that Killnet prefers a sledgehammer over precision strikes. This results in a lot of collateral damage, with the actual claims of victory coming only after "something" goes down from the bludgeoning.

National Security vs. Killnet Timeline



Application-Layer DDoS Attacks

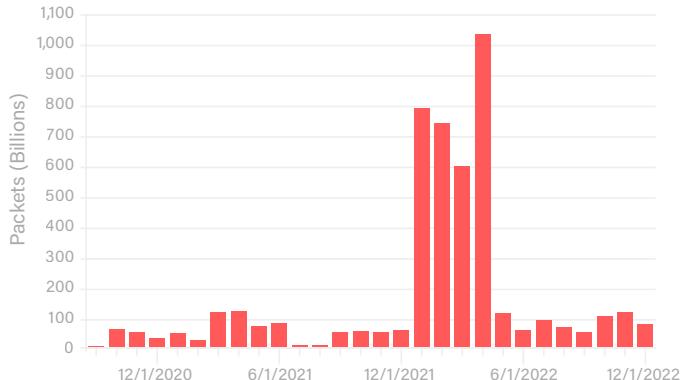


Figure 17: Application-Layer DDoS Attacks (Data: ATLAS)

Government and National Security

● Sum of Legislative Bodies ● Sum of National Security

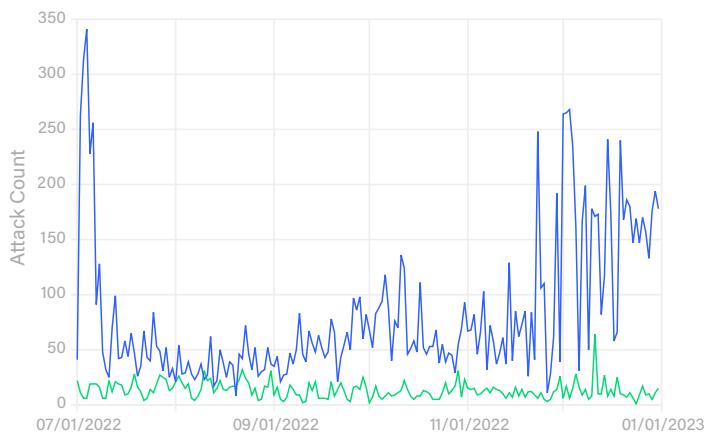
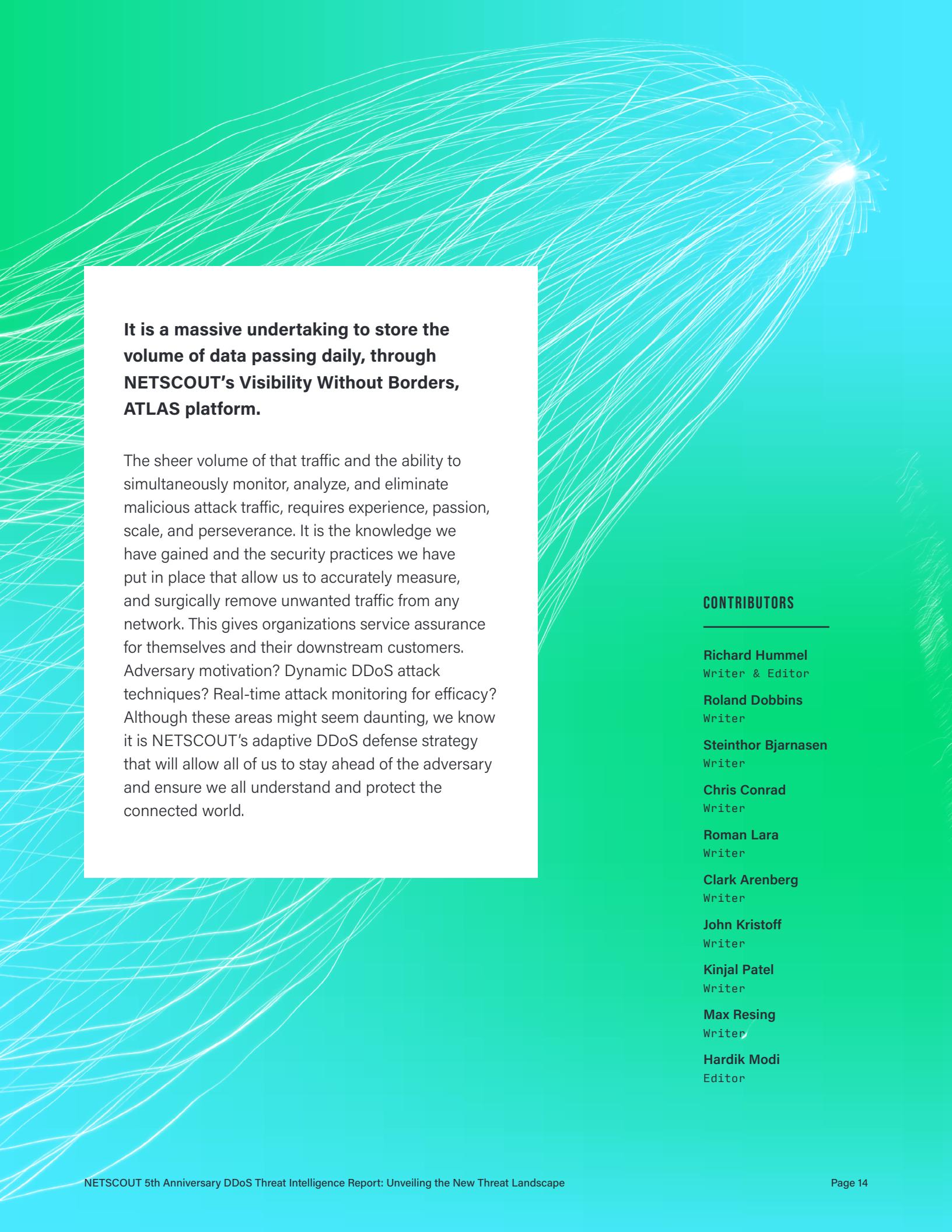


Figure 18: Government and National Security (Data: ATLAS)



It is a massive undertaking to store the volume of data passing daily, through NETSCOUT's Visibility Without Borders, ATLAS platform.

The sheer volume of that traffic and the ability to simultaneously monitor, analyze, and eliminate malicious attack traffic, requires experience, passion, scale, and perseverance. It is the knowledge we have gained and the security practices we have put in place that allow us to accurately measure, and surgically remove unwanted traffic from any network. This gives organizations service assurance for themselves and their downstream customers. Adversary motivation? Dynamic DDoS attack techniques? Real-time attack monitoring for efficacy? Although these areas might seem daunting, we know it is NETSCOUT's adaptive DDoS defense strategy that will allow all of us to stay ahead of the adversary and ensure we all understand and protect the connected world.

CONTRIBUTORS

Richard Hummel
Writer & Editor

Roland Dobbins
Writer

Steinþor Bjarnasen
Writer

Chris Conrad
Writer

Roman Lara
Writer

Clark Arenberg
Writer

John Kristoff
Writer

Kinjal Patel
Writer

Max Resing
Writer

Hardik Modi
Editor

NETSCOUT®

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) helps assure digital business services against security, availability, and performance disruptions. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility and insights customers need to accelerate and secure their digital transformation. Our Omnis™ cybersecurity advanced threat detection and response platform offers comprehensive network visibility, threat detection, highly contextual investigation, and automated mitigation at the network edge. NETSCOUT nGenius™ service assurance solutions provide real-time, contextual analysis of service, network, and application performance. And Arbor Smart DDoS Protection by NETSCOUT products help protect against attacks that threaten availability and advanced threats that infiltrate networks to steal critical business assets.

To learn more about improving service, network, and application performance in physical or virtual data centers or in the cloud, and how NETSCOUT's security and performance solutions can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT on [Twitter](#), [Facebook](#), or [LinkedIn](#).

©2023 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor, ATLAS, Cyber Threat Horizon, InfiniStream, nGenius, nGeniusONE, and Omnis are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.