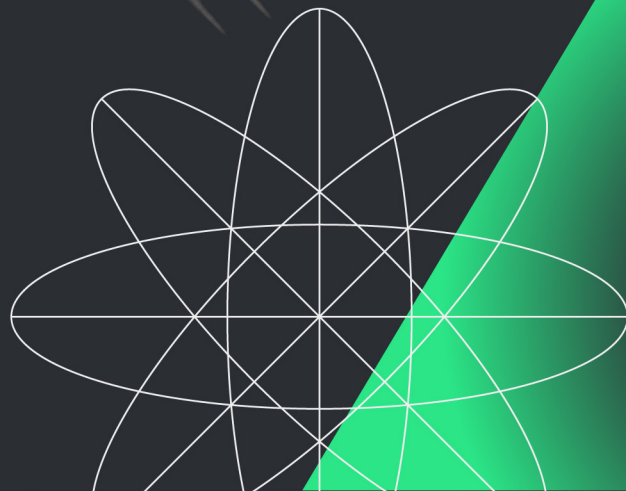


02

Adaptive DDoS Attacks and Learning How to Suppress Them



NETSCOUT®

Adaptive DDoS Attacks

Since the onset of the COVID-19 pandemic, network operators worldwide have rallied to upgrade network infrastructure to accommodate increases in demand for bandwidth and throughput driven by remote work and education.

In many cases, this resulted in service providers accelerating timelines for 5G and other high-bandwidth access technologies, following the example of companies in the energy, public utilities, manufacturing, logistics, environmental, and governmental sectors, which already had embraced remote monitoring and machine-to-machine (M2M) communications across broadband internet links.

The constant evolution of the internet and global network topology has forced adversaries and defenders to adapt. Changes in attack vectors and methodology allow DDoS attackers to circumvent defenses and countermeasures. Meanwhile, security practitioners face a constant battle of adapting their own defense posture to mitigate this evolving threat.

1H2022 INDUSTRY ATTACKS



20,633

Attacks against
Education Organizations



1,340

Attacks against Utilities




3,617

Attacks against
Executive and Legislative
Government Entities

Carrier Grade Network Address Translation (CG-NAT)

One such defensive measure inadvertently used by security practitioners is CG-NAT. Although CG-NAT systems are not explicitly intended to be network security elements, they do provide southbound devices with basic protection against unsolicited internet traffic. Unfortunately, many of these newer online devices and services utilize protocols that don't work well when sited behind NATs, thereby exposing them to the internet without intervening protection. Additionally, poor security defaults such as hardcoded administrative credentials and remotely exploitable software vulnerabilities increase the number of automated IoT-type systems being compromised and subsumed into DDoS-capable botnets. Thus, additional security and defenses measures are needed to thwart DDoS attacks.

5.5M 

distinct adversary IPs attacking NETSCOUT customers in the first half of 2022. We believe these were not spoofed, meaning adversaries have a lot of infrastructure at their disposal.

DDoS Defenses

DDoS defenses traditionally have been focused on protecting internet properties and networks by implementing attack detection, classification, traceback, and mitigation technologies at points of topological convergence for inbound network traffic. This typically is accomplished by deploying defensive measures immediately northbound of protected assets on directly connected networks. Source-address validation (SAV), for example, has a very positive impact in reducing prominent vectors such as DNS amplification as they become ineffective (Figure 1).

DNS Amplification Attacks

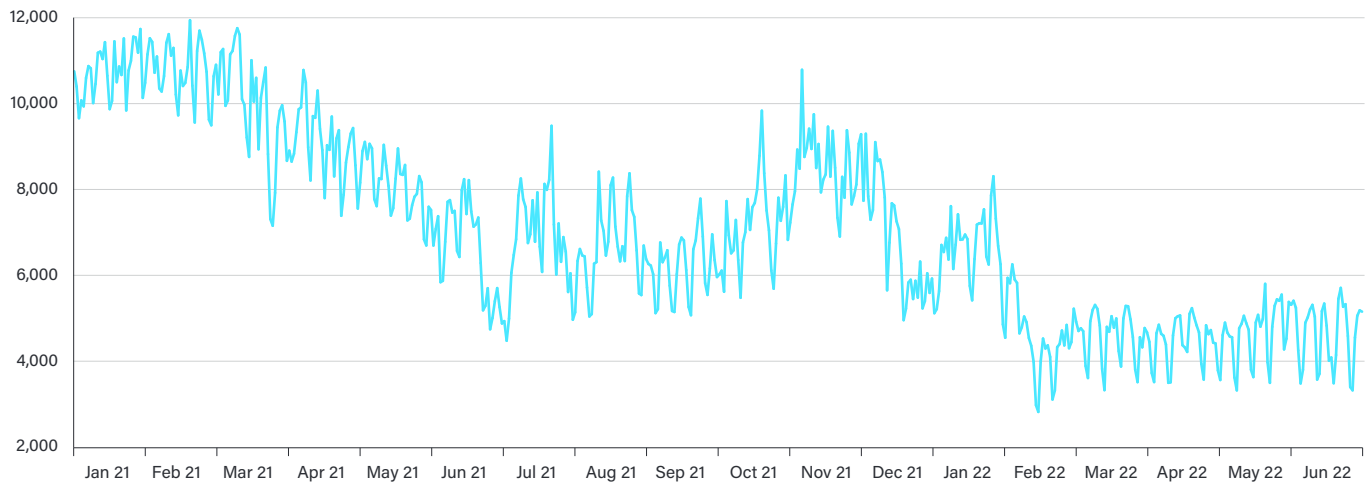


Figure 1: DNS Amplification Attacks (Data: ATLAS)

This approach has worked well to defend targeted organizations and networks from inbound DDoS attacks; however, outbound and cross-bound DDoS attacks can be just as devastating and disruptive as inbound attacks. Compromised workstations, IoT devices, and high-capacity servers have been subsumed into botnets and used by attackers to launch DDoS attacks, and the resulting traffic generated by these systems has significantly impacted production services for the enterprise and service provider networks. Because of adversary innovation and adaption, defenders must change their way of thinking and in turn adapt to the threat landscape.

NETSCOUT collected information on more than

500,000+

compromised devices infected with IoT malware capable of launching DDoS Attacks.

What is Adaptive DDoS?

Adaptive DDoS Attacks

- 1 Advanced reconnaissance of target networks
- 2 Continuous attack efficacy monitoring
- 3 Quickly changing attack vectors to counter mitigations
- 4 Using topologically adjacent attack infrastructure
- 5 Continuous attacker innovation and vector weaponization

Adaptive DDoS Defense

- 1 Intelligence DDoS Detection, Classification, Traceback, and Mitigation
- 2 Ability to detect and mitigate minute-zero attacks
- 3 Enhanced anomaly-detection technology, dynamic traffic analysis and classification
- 4 Curated threat intelligence, dynamic vector identification
- 5 Pre-attack adversary infrastructure identification

In an adaptive DDoS attack, adversaries perform extensive pre-attack reconnaissance to identify specific elements of the service delivery chain to target. Increasingly, adversaries are making use of botnet nodes and reflectors/amplifiers that are topologically adjacent to the target, a phenomenon we recently observed with botnets launching attacks against Ukraine. This, in turn, minimizes the number of administrative boundaries that DDoS attack traffic must traverse, often resulting in fewer opportunities to detect and mitigate the attack.

The combination of increases in available per-node bandwidth and throughput, increasing populations of abusable devices not sited behind NATs, and adaptive DDoS defense techniques creates a massive threat to network operators—especially when they are required to support more of these devices at higher speeds to meet customer demand. As such, it is imperative that network operators move from a default posture of DDoS mitigation to a new paradigm of DDoS suppression.

DDoS Suppression Systems

By implementing adaptive DDoS defenses at all edges of their networks, including directly within peering and customer aggregation points of presence (PoPs), network operators can suppress DDoS attack traffic as it ingresses at multiple points across the entire network edge—or before it ever converges into a large-scale attack. By implementing edge-based attack detection, intelligent DDoS mitigation, and network infrastructure-based mitigation techniques at all network ingress points, operators can implement adaptive DDoS suppression systems that scale to counter DDoS attack capacity and adversary innovation.

One method of DDoS suppression NETSCOUT uses to secure customer's edges is pushing threat intelligence-derived attack infrastructure (Figure 2) as a feed that can predefine what IP addresses or CIDRs an adversary might use to launch an attack. Thus, when an attack using the identified infrastructure begins, we can immediately and quickly start blocking before any additional routing decisions, countermeasures, or manual analysis is required, nullifying the attack before it ever reaches critical mass.

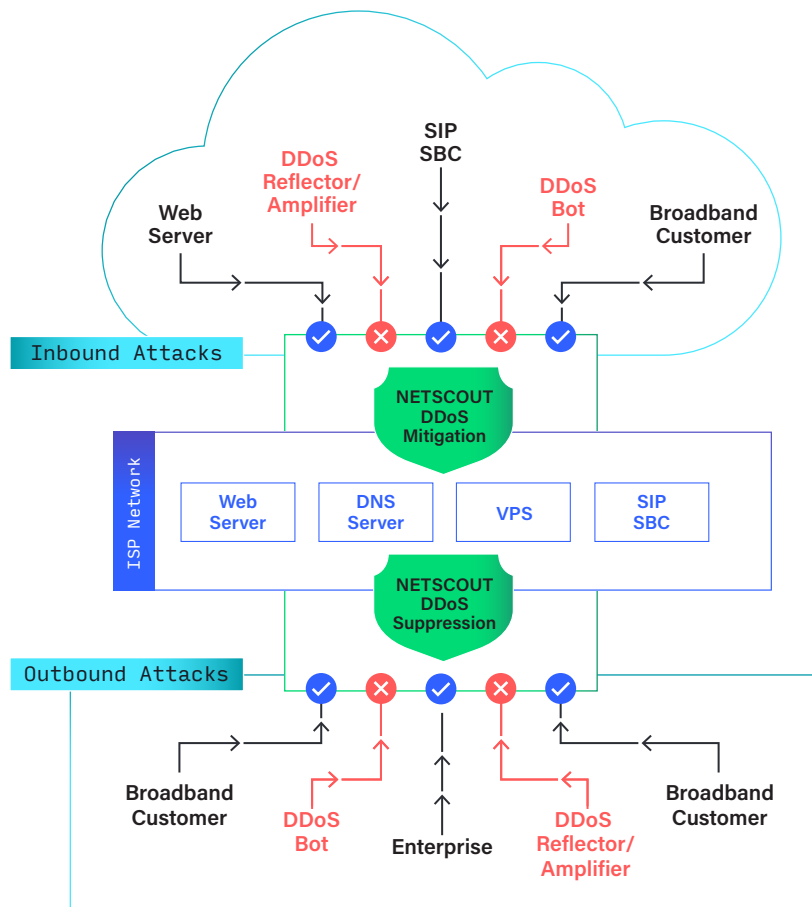


Figure 2: DDoS Suppression and Mitigation

Conclusion

The operational community has successfully suppressed spoofed attack initiator traffic, resulting in demonstrable decreases in reflection/amplification DDoS attacks when compared with direct-path attacks. The next logical step is to extend this paradigm into adaptive DDoS suppression across the network edge to further build a safer, more resilient internet for all.

EXPLORE MORE OF THE 1H2022 DDoS THREAT INTELLIGENCE REPORT

For more expert insight in DDoS global and regional attack statistics, botnet activity, attack vectors and DDoS is used in geopolitical conflicts, revisit the NETSCOUT 1H 2022 DDoS Threat Intelligence Report landing page.

[VISIT THE SITE](#)

ABOUT 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](#).

CONTRIBUTORS

Roland Dobbins
AUTHOR

Richard Hummel
EDITOR

NETSCOUT®

©2022 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.