No.61
February 2023

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/ SPONSORED**

Intelligence-Driven DDoS Defence

Sponsored by NETSCOUT

- No-one knows more about DDoS threats than NETSCOUT. With the company's latest threat report highlighting a growing threat from Direct Path and multi-vector DDoS attacks, telcos, ISPs and their customers need to be able to automatically block these threats.
- The Arbor Sentinel is a key element of NETSCOUT's Arbor 'Adaptive DDoS Defense'. Driven by Arbor's ATLAS Intelligence Feed (AIF), Sentinel orchestrates multi-vector mitigation across routers, scrubbing centres and inter-provider messaging. It dynamically selects optimal mitigations for each attack vector.

22 years after the company was founded, and 6 years after NETSCOUT acquired it, the 'Arbor' product line still leads the market in DDoS protection. Competitors routinely cite differentiators, revenue growth, and reasons why they are winning this or that type of deal. But none would claim to be outperforming NETSCOUT in DDoS protection revenues.

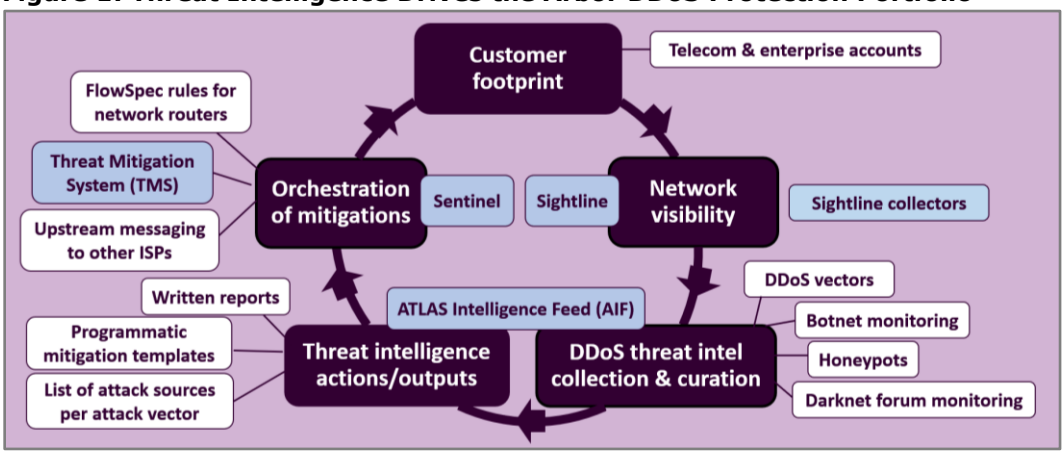
The Arbor portfolio still leads in the all-important telco and ISP market segment.

The Arbor portfolio still leads in the telco and ISP space as well. It is used by around 500 customers in this all-important market segment – all-important because telcos and ISPs see so many more DDoS attacks and attack vectors than any other type of organization which drives the ability to differentiate through threat intelligence.

Drawing on the latest NETSCOUT DDoS Threat Intelligence Report, this HardenStance Briefing on the evolution of NETSCOUT Arbor's portfolio comprises three sections:

1. **Threat intel founded on unique visibility** – what the global footprint of Arbor solutions enables in terms of visibility into the Internet and DDoS threat activity.
2. **Constantly evolving DDoS threat vectors** – the latest in DDoS threat actor tactics, techniques and procedures (TTPs) that NETSCOUT has publicly reported on.
3. **DDoS suppression and per vector mitigation** – how NETSCOUT's threat intelligence-driven Arbor portfolio enables telco and ISP defenders to dynamically deploy optimal mitigation techniques against each DDoS threat vector it detects.

Figure 1: Threat Intelligence Drives the Arbor DDoS Protection Portfolio



Source: HardenStance

Threat Intel Founded on Unique Network Visibility

The sheer scale and breadth of its customer footprint among leading telcos and ISPs is the foundation of NETSCOUT's continued competitiveness. Beyond the low-hanging fruit of simple incumbency like robust financial performance and account relationships – which is easily wiped out in the high-tech sector with a new market transition – NETSCOUT's Arbor footprint in telcos, ISPs and Virtual Private Server (VPS) providers yields something much more important for sustainable differentiation. That 'something' is unique depth and breadth of visibility into the DDoS threat landscape, which is itself a key factor that drives market transitions in DDoS protection.

The aggregate DDoS threat data yielded by the global Arbor account footprint, together with enrichment with other data sources, is what NETSCOUT calls ATLAS. The curation and classification of the ATLAS data to render it actionable in customer environments is overseen by ASERT. This is the company's security research and response team, which has more than 80 aggregate years of experience in hands-on DDoS mitigation.

However important it is, visibility is just a foundational platform for differentiating through threat intelligence.

Visibility into Attacks in 190 Countries

Leveraging the Arbor portfolio, as well as automated reconnaissance tools, ASERT pulls anonymised metadata from many of the world's largest telco and ISP networks. This is the biggest contributor to providing ASERT with unparalleled visibility into DDoS attacks in 190 out of 198 countries in the world. ASERT sees these attacks against 550 of the 950 types of business organization defined by the North American Industry Classification System (NIACS). It observes 50,000 out of the world's 90,000 active Autonomous System Numbers (ASNs) used by telcos and ISPs to control routing within and between their networks. In the first half of 2022, ASERT's global honeypot network saw more than 67 million connections from 608,000 unique IP addresses, spanning 13,000 ASNs, 30,000 organizations, and 165 countries.

Private and public threat intel sources, sinkholes, botnet monitoring, darknet forum monitoring, and honeypots are added into the mix of ATLAS data inputs. This data is continuously analysed using machine learning techniques as well as human curation. The results of this analysis are automatically distributed to all Arbor DDoS protection products via the ATLAS Threat Intelligence Feed (AIF). This arms them with the latest DDoS threat intelligence and drives automated attack mitigation.

NETSCOUT is Currently Seeing 36,000 DDoS Attack Alerts Per Day

Many DDoS protection vendors don't serve the telco and ISP market at all. Of those that do, many are only ever deployed at an endpoint or in front of a website. These vendors are typically not monitoring the entire telco or ISP traffic stream. Hence they are only seeing a subset of all the DDoS threats arising around the world at any one time. This is important because while the vast majority of DDoS attacks can't be seen at enterprise customer endpoints, they can be seen within telco and ISP traffic. As a result, some DDoS protection vendors cite seeing DDoS attacks in the several thousand or tens of thousands a year. Due to the breadth and scale of its Arbor product's deployments in the telco and ISP market, NETSCOUT sees 36,000 alerts or events per day.

A lot of the delta between what NETSCOUT and many other DDoS vendors can see is accounted for by their worldwide Arbor deployments and the visibility that provides into telco and ISP networks that deliver services to many different industry segments (e.g. financial services, insurance, medicine, e-commerce, government, utilities, education, on-line gaming, and other mission-critical infrastructure). This generates more granular insight into what adversaries are doing. NETSCOUT gains insight into what infrastructure these adversaries are using, how they're using that infrastructure to attack customers, what new attack vectors are being used in general and what new tactics, techniques and procedures (TTPs) are being used to disrupt a particular industry segment.

Constantly Evolving DDoS Threat Vectors

One of the critical aspects of the threat landscape shared in NETSCOUT's latest DDoS Threat Intelligence report is the latest trends in DDoS threat actor TTPs. These are the latest observed behaviours that characterize a wide variety of well-established DDoS threat activity. They cover things like very low-cost 'DDoS as a Service' websites as well as the bundling of DDoS attacks into triple extortion attacks that combine DDoS with a ransom demand and/or threats to leak sensitive data.

The key takeaways from the report in terms of the latest threat actor TTPs are captured below, then described in more detail.

1 Direct Path attacks are overtaking reflection/amplification as the most popular DDoS attack vector.

Direct Path attacks are overtaking reflection/ amplification as the most popular DDoS attack vector.

2 DDoS attacks are increasingly botnet-driven, multi-vector, and dynamically managed and adjusted in real time.

3 Greater use of DDoS attacks by nation state threat actors (as well as their supporters and opponents) is increasing the risk to organizations that their supply chain partners will suffer damaging outages arising from global political flashpoints.

With the Resurgence of Direct Path Attacks…

The first recorded reflection/amplification attack was in 1997. That was the first time someone managed to trick benign but abusable intermediary devices into sending large responses to a targeted IP address (thereby obscuring the ultimate source IPs of the attack infrastructure).

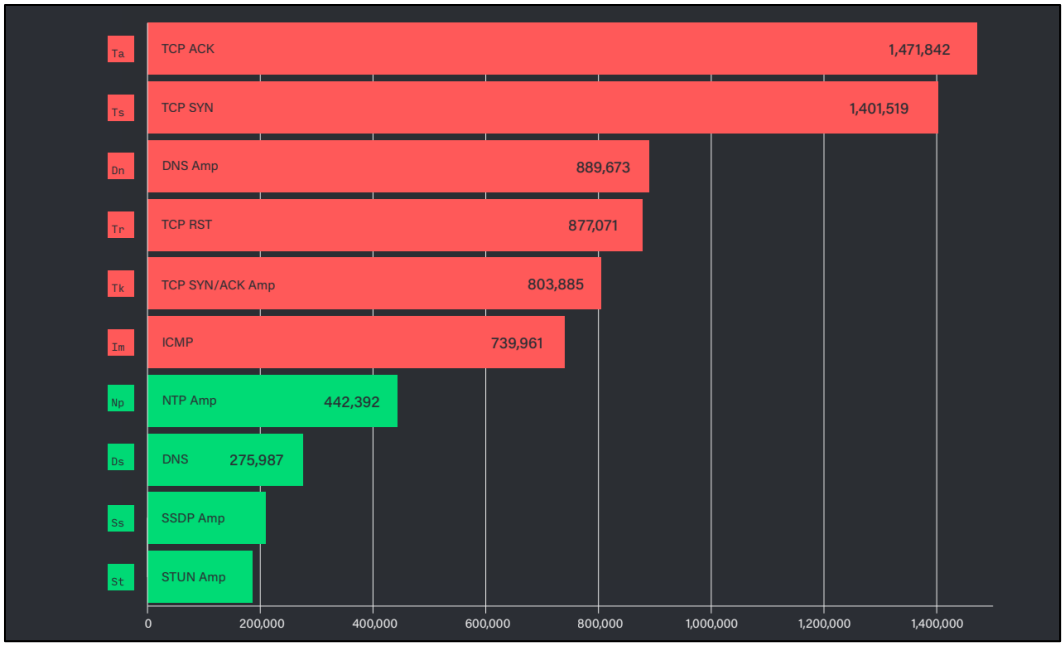
That milestone fundamentally altered the DDoS threat landscape because, until then, it had only seen Direct Path attacks sourced directly from the attack infrastructure, which does not spoof the source address. The benefit of reflection was amplification — the volume of DDoS traffic was amplified many times over when doing reflection. By contrast, direct attacks had to generate the full volume of the attack bandwidth using only the attacking sources which therefore resulted in smaller sized attacks.

Reflection/amplification attacks went on to dominate the DDoS threat landscape, especially with the additional boost provided to their weaponization by DDoS-for-hire services from 2013 onwards. Rather than focusing on where an attack is coming from and how it reaches its target, in more recent years the emphasis shifted to segmenting the market according to what an attack looks like when it reaches its target – in other words prioritizing the distinction between volumetric attacks (sending large volumes of messages to a target) and application layer attacks (targeting vulnerabilities in application servers).

…the Pendulum is Swinging Away from Reflection/Amplification

The latest threat report states that the key trend in terms of the number of attacks is how the pendulum is swinging away from reflection/amplification and back again towards Direct Path attacks. ASERT first identified this in 2021 when the number of DNS amplification and Connection-less Lightweight Directory Access Protocol (CLDAP) amplification attacks dropped fully 32% and 64% respectively compared to 2020.

Figure 2: Top 10 DDoS Attack Vectors by Count



Source: NETSCOUT Threat Report, 1H 2022

Telco and ISP DDoS protection teams have been leaders in accelerating deployment of anti-spoofing or source address validation (SAV).

For the first half of 2022, **Figure 2** now shows that three Direct Path attacks - TCP Acknowledgement (TCP ACK); TCP Synchronization (TCP SYN) and TCP Reset (TCP RST) – have risen to become the number one, two and four most common DDoS threat vectors being observed via the Arbor portfolio. The number of TCP ACK and TCP SYN attacks was up 11% and 20% respectively compared to the second half of 2021. The number of DNS amplification attacks was down 31%. Whereas ASERT ranked it as the single most common attack vector in 2020, **Figure 2** shows DNS amplification down to third spot in the first half of 2022.

Ironically, this resurgence in Direct Path attacks is partially due to great work by information security professionals. Telco and ISP DDoS protection teams have led the way in accelerating the deployment of anti-spoofing or source address validation (SAV) solutions at customer edge sites over the last couple of years. As highlighted by the marked drop in DNS reflection attacks, this effort has significantly reduced the number of networks that are available for reflection/amplification attacks.

Botnet-Driven Threat Innovation

A shift in defender tactics as with the accelerated roll-out of SAV invariably drives threat actors to adjust their TTPs. And this is exactly what the ASERT reports with the resurgence in Direct Path attacks. DDoS threat actors are having to invest in more sophisticated botnets for launching Direct Path attacks, as well as employing open proxies to reflect those attacks towards their intended targets, thereby hiding the actual IP addresses of the attack infrastructure. As shown, with a reflection/amplification attack, the power of the amplification factor means you don't need a big or sophisticated botnet to launch it. Without that amplification factor, success with Direct Path attacks requires more pervasive botnet infrastructure. ASERT tracks around 400,000 infected devices that are enslaved by botnets. It estimates at least 60 variants of the MIRAI botnet malware are available now for attackers to use.

This doesn't mean reflection/amplification attacks pose any less of a threat; it just means they currently account for a smaller share of all DDoS threats. In terms of the ongoing threat they pose, consider the TP240 PhoneHome reflection/amplification attack. This was discovered in February 2022 when a spike in DDoS traffic was seen sourced from UDP port 10074 targeting ISPs and other organizations. This vector recorded the largest amplification factor in history, with a packet amplification ratio of 4 billion to 1.

Attacks are Increasingly Managed and Adjusted in Real Time

In recent years, most DDoS attacks have become highly automated. A threat actor simply has to push a button and the attack programme runs from beginning to end. This is still true today. ASERT nevertheless reports an acceleration in the number of what it calls "Adaptive" DDoS attacks. These are "hands-on keyboard" style attacks. While this term usually refers to lateral movement within a breached organization it's used here to refer to the way that DDoS threat actors are increasingly adjusting attack vectors dynamically, often in real time. This can be in the context of weaknesses the attack is able to identify in the target organization or in its mitigation capabilities. Or it can be in the context of opportunities they spot to leverage vulnerable or exposed infrastructure in the attack path between a potential source and the target entity.

ASERT reports increasing instances of attackers carrying out advanced reconnaissance of target networks and continuous attack efficacy monitoring.

ASERT reports increasing instances of attackers carrying out advanced reconnaissance of target networks, continuous attack efficacy monitoring, and rapid changing of attack vectors to counter mitigations. Threat actors will also locate attack assets – for example, bots or reflectors/amplifiers – that are sited topologically adjacent to the target. By sourcing the attack traffic from nearby, attackers can minimize the number of administrative boundaries the attack traffic crosses. This assures more attack bandwidth per source as well as fewer opportunities for the attack to be detected and mitigated.

A Marked Acceleration in Multi-Vector Attacks

Traditional single vector reflection/amplification attacks - especially volumetric attacks – are relatively easy for telcos, ISPs and other organizations to block. Hence, leveraging investments in botnets and other attack tooling, threat actors are increasingly using coordinated multi vector attacks. They are mixing and matching volumetric and application layer vectors, Direct Path and reflection/amplification vectors, one after the other or concurrently. Some of these comprise more than ten unique vectors. A common pattern consists of mundane vectors being used as a smokescreen to smuggle in an application layer vector undetected. The hands-on overseeing of an attack as it progresses in this way allows real time launching of new vectors that are tailored to overcoming the defences that the initial one or two vectors may be unable to get past.

Persistence and Churn in Abusable Infrastructure

The H1 2022 report shares details about the arsenal of abusable infrastructure that is available to DDoS threat actors now. For example, 5.5 million distinct adversary IP addresses attacked NETSCOUT customers in the first half of 2022, although most attacks originated from a small minority of them. ASERT is confident that the 5.5 million were not spoofed, implying that a lot of infrastructure is at the disposal of adversaries. The team nevertheless assesses "with very high confidence" that more than 80% of all DDoS attack traffic originates from a relatively small number of confirmed IP addresses. This suggests that a lot of adversary infrastructure is also highly re-usable.

Multiple Players Report Strong Growth in Multi-Vector DDoS Attacks

Other DDoS protection providers besides NETSCOUT report seeing similar trends with respect to the strong growth in multi-vector attacks. In one case, Neustar reported in its 2021 Threat Report that almost half the DDoS attacks it saw were multi-vector attacks - 37% comprised two or three vectors and 9% comprised four or more. In another, Lumen Technologies has recently taken to sharing the mix of single and multi-vector DDoS attacks that it sees across its networks on a quarterly basis. During the 12 months spanning Q4 2021 and Q3 2022, Lumen reports that multi vector attacks increased their share of the total DDoS attacks it saw from 35% to 40%.

The greatest number of abusable amplifiers out there according to the 1H 2022 report are SIP (4.1 million), NTP (2.5 million) and TFTP (2.2 million). Consistent with the defender community's efforts to roll out SAV, DNS amplifiers (at just 1.6 million) have dropped a long way down the rankings from second a couple of years ago to sixth.

The data also shows that while there are still millions of reflectors/amplifiers out there, ASERT estimates that only 8.5% - 12.5% are being abused at any one time today. Moreover, ASERT knows which ones they are. That's valuable insight because it allows the list of malicious IP addresses in the AIF – and that customers therefore need to block – to be narrowed down from several million to a few hundred thousand. It's worth noting again here that these curated lists are arrived at via NETSCOUT's extensive footprint of Arbor products in the telco and ISP space. They are also being constantly refreshed to reflect daily churn among those devices that are currently being abused.

ASERT estimates that only 8.5% - 12.5% of reflectors/ amplifiers are being abused at any one time today.

Geopolitical Trends are Making Things Worse, Not Better

The use of DDoS attacks in geopolitical conflicts isn't new but has certainly ramped up during 2022. The most striking impacts seen have revolved around Russia's invasion of Ukraine. Apart from the inevitable increase in DDoS attacks on those two countries themselves, other countries were also drawn into the cyber realm of the conflict. Ireland suffered a big spike in DDoS attacks when, in order to avoid Russian attacks, Ukraine offloaded a lot of its critical infrastructure onto public cloud servers based in Ireland.

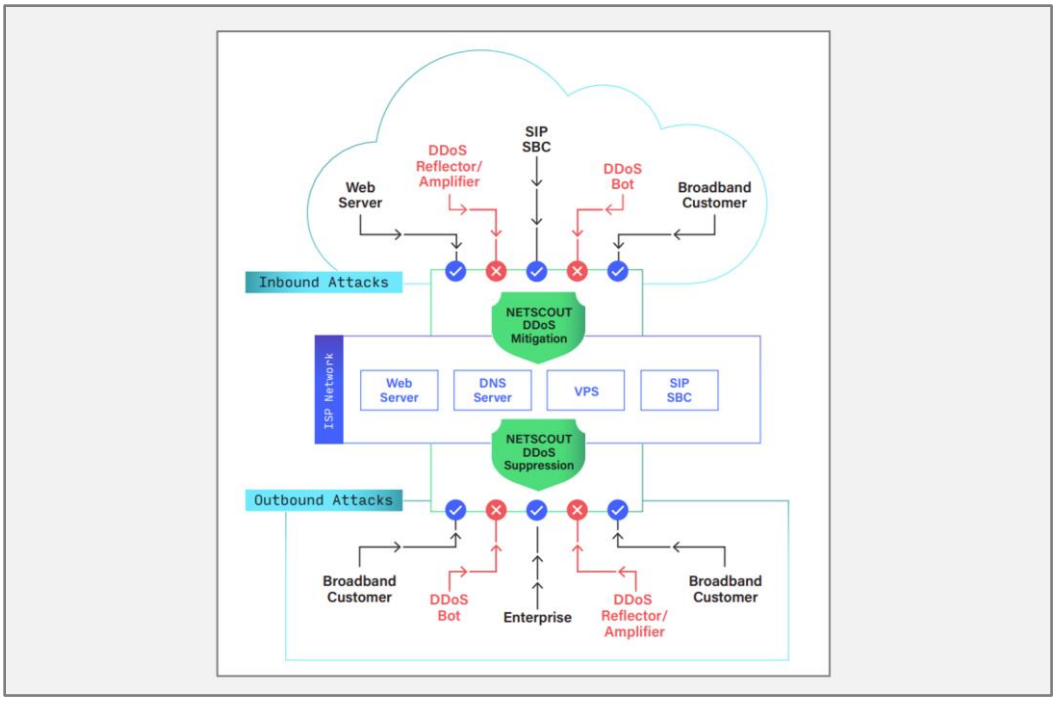
Finland also saw a major spike soon after the country's leaders began discussing making a commitment to joining NATO. What's key to understanding the implications of this is that they extend way beyond the target countries themselves. Committed threat actors are increasingly performing extensive pre-attack reconnaissance to identify key elements in the service delivery chains of their targets. This heightens the vulnerability to DDoS attack disruption of all manner of businesses all over the world – many of which have little or nothing directly to do with the countries or organization targeted.

DDoS Suppression and Per-Vector Mitigation

Ultimately, DDoS protection solutions are always evaluated against two critical metrics: how good are they at stopping DDoS attacks? And how cost effective are they? Neither metric is static. They both evolve with changes in the threat landscape; with the roadmaps of DDoS protection vendors themselves; and with the roadmaps of other players in the DDoS protection ecosystem, like router vendors.

If a vendor roadmap doesn't adapt to changes in the threat landscape, then what worked well a year ago might not work quite so well now. It might work even less well a year from now. Consistent with this, NETSCOUT's value proposition has evolved from simple 'DDoS mitigation', which is starting to have a bit of a 'legacy' ring to it now. These days, as shown in **Figure 3** overleaf, NETSCOUT's value proposition is framed as enabling DDoS 'suppression' as well as orchestrated DDoS mitigation per threat vector.

Figure 3: DDoS Suppression and Mitigation in the Arbor Solution



Source: NETSCOUT

DDoS suppression is proactive, stopping abusable devices from attacking you before they get the chance to even try.

DDoS suppression is depicted in **Figure 3**. The emphasis on this is fairly recent, reflecting the growing scale and sophistication of botnets, the rise in Direct Path attacks and the increased risk this poses from both outbound (from a customer endpoint out to the Internet) and cross-bound (customer endpoint to customer endpoint) attacks. Malicious traffic coming into a telco or ISP network across their peering/transit pipes can certainly trigger a network or service outage. But the same is also true of rogue devices within their own or their customer's network filling up their pipes with outbound or cross-bound traffic. Moreover this is a risk that is liable to accelerate with the growth in insecure and un-securable IoT devices expected to be connected to high-speed 5G networks. Many of these simple, even 'dumb', IoT 'things' are also not equipped to leverage some of the protections that Carried Grade Network Address Translation (CGNAT) offers more traditional southbound endpoints against DDoS traffic.

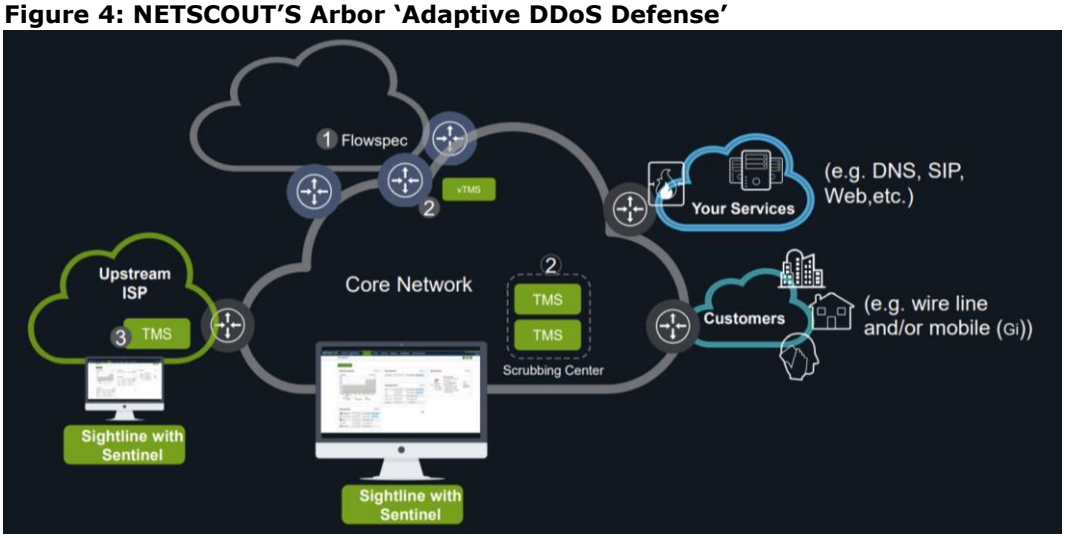
DDoS Suppression is Proactive where DDoS Mitigation is Reactive

DDoS mitigation is inherently reactive. It deals with an attack once it gets to you. In contrast, DDoS suppression is proactive. It stops abusable devices from attacking you before they get the chance to try. NETSCOUT's Arbor solution leverages the curated lists of abusable botnet and reflector/amplifier devices that ASERT is constantly scanning for and updating to carry out DDoS suppression in one of two ways:

- The rogue devices themselves can be remediated by the owners of those devices.
- Alternatively, an Arbor customer's access control lists can be updated to block the device from being able to access their network.

Customers can also share feedback on those lists so that they can be better tailored to individual customers and help enhance the signal-to-noise ratio for all customers.

Figure 4: NETSCOUT'S Arbor 'Adaptive DDoS Defense'



Source: NETSCOUT

Orchestrated Multi-Vector Mitigation via Sentinel

The core of NETSCOUT's Arbor 'Adaptive DDoS Defense' portfolio revolves around three main products. As shown in **Figure 4**, the first two are the Arbor Sightline and Threat Mitigation System (TMS) products that have driven the company's market leadership from when it was first founded up until the present day. Sightline provides the visibility into customer networks, serving as the customer's management interface and providing data to ATLAS. TMS is the intelligent in-line DDoS 'scrubbing centre', removing malicious traffic from streams that are sent to it, while forwarding legitimate traffic on to its intended destination.

Sightline and TMS are fundamental to the portfolio but it's the third of the core products whose value is most accentuated by the latest DDoS threat intelligence trends.

Arbor Sightline and TMS are fundamental to the portfolio but it's the third of the core products whose value is most enhanced by the latest DDoS threat intelligence trends. This third product is the Arbor Sentinel mitigation orchestration platform. First announced in January 2020, Sentinel adds a layer of orchestrated multi-vector mitigation, making it key to the portfolio's mitigation efficacy as well as cost efficiency in a changing DDoS threat landscape. Sentinel orchestrates the mitigation of attacks by dynamically selecting from among the three mitigation tools and platforms listed below:

1. **Generating a Flowspec rule to block an attack in the router infrastructure**: The extent to which a telco or ISP can use this lowest cost option will vary according to the capabilities of a company's router infrastructure. At minimum, any telco or ISP router should be able to handle significant volumes of rudimentary reflection/amplification vectors. Some router vendors either have or will have more advanced DDoS filtering capabilities than that.
2. **Sending traffic to the Threat Mitigation System (TMS):** More sophisticated Direct Path attacks typically need to go to TMS for packet-based defence. In some cases that will involve active authentication of the sender to determine whether the traffic is malicious. You can't just block a TCP SYN vector at the edge in response to a TCP SYN flood because that risks taking down the Internet for all users.
3. **Using Inter-Provider Signaling:** A telco or ISP can leverage Arbor's proprietary Inter-Provider signaling to request upstream mitigations for threats that they believe peers that are also using Arbor products may not be aware of yet. Due in part to the "chicken and egg" issue which has delayed adoption of communications technologies dating back to the original telephone itself, adoption of this inter-telco messaging capability is still in its infancy. It nevertheless has potential to be a valuable addition to defensive options as telco and ISP customers become more familiar with it.

Sentinel orchestrates the response of a telco, ISP or other customer to the huge variety of simple, complex, as well as highly complex, DDoS threats across these three mitigation options. Importantly, customers can choose a level of automation of these responses according to their own capabilities and preferences. The approach is designed to directly mirror the real-time dynamism of advanced threat actor behaviours in the way they dynamically adjust attack vectors by mitigating them just as dynamically. Sentinel dynamically selects different mitigations for different threat vectors. For example, it can block the first two of three vectors with a FlowSpec rule for the router infrastructure and send the third to TMS. If available, it can also send an Inter-Provider signal to an upstream peer using Arbor with attack vector information for mitigation.

Sentinel can also mitigate more optimally at a granular, per packet level, within a single vector.

Mitigation Per Vector or Per Packet

Sentinel can also mitigate more optimally at a granular, per packet level, within a single vector. Take an example of an NTP reflection/amplification attack, a common volumetric attack that uses datagram fragmentation to break packets up into smaller fragments. Most routers are able to block the initial NTP packet in this attack whereas they typically can't differentiate the other two or three fragmented packets. So within this one vector, Sentinel can use the lower cost router infrastructure to reduce the attack volume by around a third, and send the rest for TMS to mitigate. Using Sentinel to orchestrate mitigations within, as well as between different threat vectors, in this way drives both security efficacy and cost efficiency.

How effectively you close the loop in cyber threat intelligence comes down to how well integrated your threat intelligence people, processes and technology are and how good they are at pushing high-fidelity intelligence outputs into customer environments. In the Arbor solution, traditional written DDoS threat advisories are, of course, regularly pushed to customers and partners. In today's highly dynamic environment, however, the largest part of the value arises from the product portfolio's continuous responses to the AIF. These are constantly triggering automated countermeasures that detect and block the latest threats without a customer having to do anything. AIF mitigation templates can also be spun up in JSON and pushed programmatically directly to the Sightline management console. Customers can then run these mitigations exactly as they are or with additional customization. ■

About NETSCOUT

NETSCOUT is a leading provider of service assurance, DDoS protection, cyber security, and business analytics solutions to the world's largest and most innovative service providers, enterprises and government agencies. Via its acquisition of Arbor Networks, NETSCOUT provides industry leading DDoS attack research and Adaptive DDoS Defense solutions. NETSCOUT's Arbor Sightline, Threat Mitigation System and Sentinel products are backed by the continuous global DDoS threat intelligence of ATLAS and ASERT. The solution provides network operators the ability to:

- Gain pervasive network visibility via the combination of highly scalable IP Flow analysis and deep packet inspection.
- Automatically detect multi-vector DDoS attacks using patented ML-based network behaviour analysis, DPI, and unmatched global DDoS threat intelligence.
- Intelligently orchestrate multiple methods of attack mitigation using existing network infrastructure, dedicated, intelligent DDoS mitigation systems and inter-provider communication.

For more information on NETSCOUT's Arbor DDoS attack protection solution visit: https://www.netscout.com/solutions/service-provider-ddos-protection

To obtain a copy of the referenced or latest NETSCOUT DDoS Threat Intelligence report visit: https://www.netscout.com/threatreport

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, MEF OASIS, ETSI and TM Forum. www.hardenstance.com.

To receive an email notification whenever HardenStance releases new reports in the public domain, register here (there are only four fields): Registration Link

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.