03

Adversaries Evolve and Innovate Attack Methods and Vectors

Adversaries constantly innovate and explore new and more powerful DDoS attack vectors, evidenced by the creation of new ones every year. As DDoS defenses become more precise and effective, attackers continue to find ways to bypass those defenses with new DDoS attack vectors and methodology.

Reflection/amplification vectors, wherein a device or service on the internet is tricked into sending large responses to a spoofed source IP address, are the most common form of new DDoS attack vectors (despite them becoming less effective). This kind of attack often takes the form of UDP-based service with no authentication, which sends large replies when a specific spoofed trigger packet is received. Some TCP services also can be used for this purpose; however, this is less common because doing so usually requires a three-way, nonspoofed handshake before responding.

When a new DDoS vector is adopted by the attackers, it is heavily used at the outset, but use will taper off as compromised devices and services get patched, resulting in the number of potential reflectors decreasing. This was the case with Memcached, which saw large initial attacks using tens of thousands of devices to launch the attacks, as well as with the recent TP240 PhoneHome vector, which has the largest amplification factor on record. The number of vulnerable devices rapidly declined for both, and the subsequent number of attacks in the wild corresponded to that decrease in abusable devices. However, it's not just new vectors that demand attention. In many cases, older vectors are rediscovered, creating surges in their use. For instance, there was a marked increase in Memcached attacks in Q2 2022, with nearly 50 percent more attacks month over month than occurred in Q1 2022.

Because adversaries continually adapt and change, security practitioners must also adapt their thinking, understanding, and defenses to combat the innovation by using DDoS suppression and threat intelligence. Although this isn't an easy task, NETSCOUT makes the endeavor a little more bearable by providing semiannual updates about the DDoS threat landscape. Following is a comprehensive overview of trends and outliers in DDoS attack vectors, as well as some adversary methodology.

KEY FINDINGS

1. TCP-based flood attacks (SYN, ACK, RST) remain the most used attack vector (~46 percent of all attacks) in 1H 2022.

2. DNS water-torture attacks accelerated into 2022, with a 46 percent increase in attacks primarily using UDP query floods.

3. Carpet-bombing attacks experienced a decline toward the latter half of 2021 but experienced a big comeback by the end of Q2 2022.

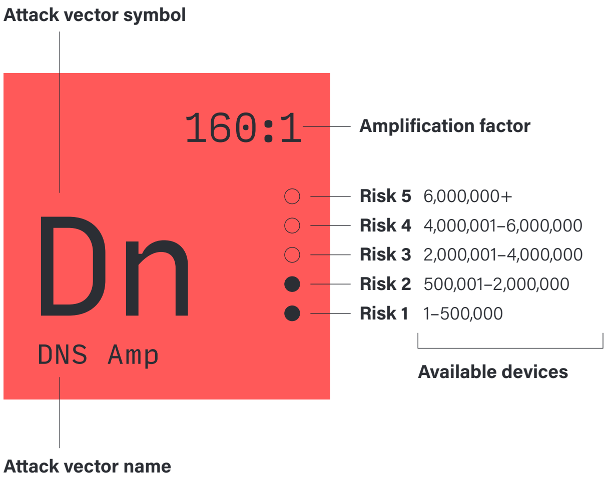
Periodic Table of Attack Vectors

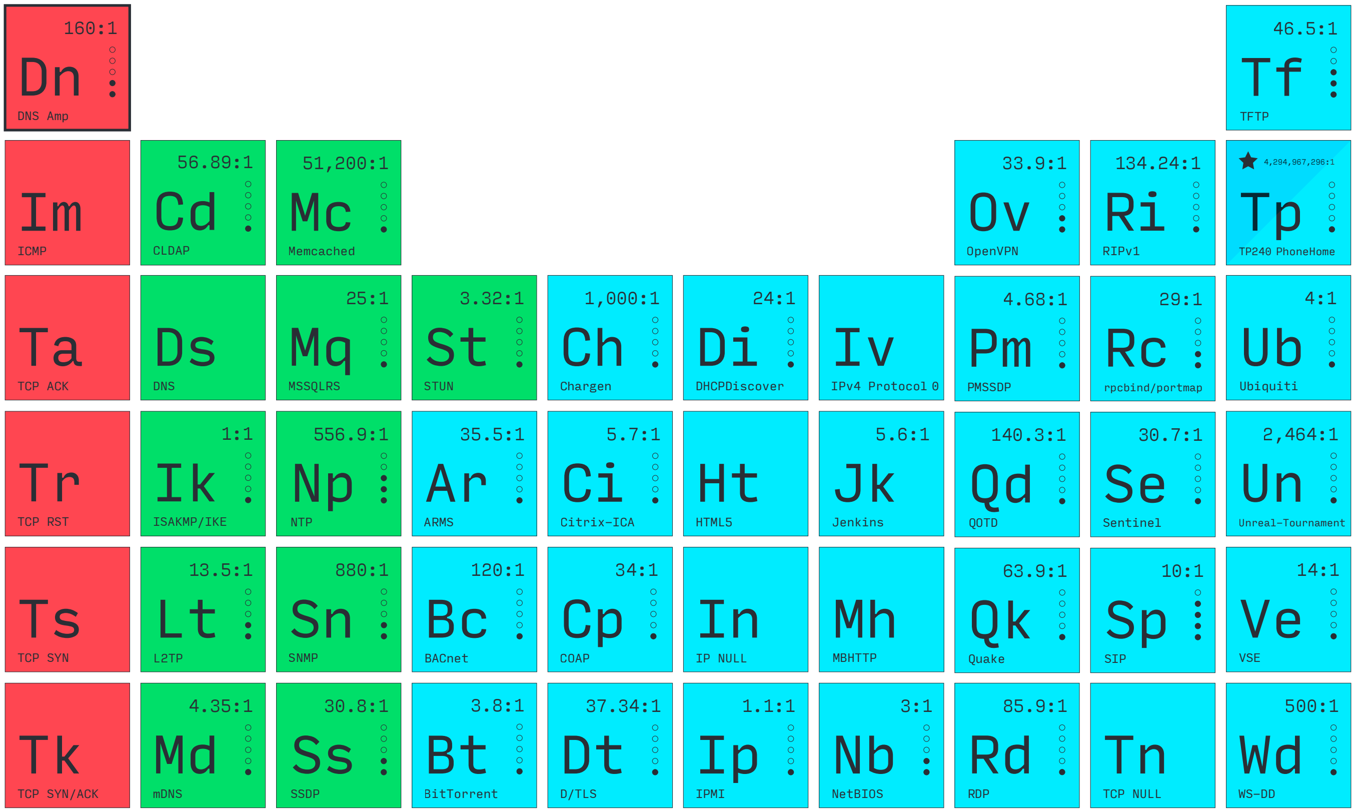
VIEW LIVE INTERACTIVE PERIODIC TABLE

DNS Amplification

A DNS reflection/amplification DDoS attack is a common two-step DDoS attack in which the attacker manipulates open DNS servers.

NUMBER OF ATTACKS	927,366
AVAILABLE DEVICES	1,617,024





🟥 160:1 Dn ○○○●● DNS Amp									🟦 46.5:1 Tf ○○●●● TFTP
🟥 Im ICMP	🟩 56.89:1 Cd ○○○○● CLDAP	🟩 51,200:1 Mc ○○○○● Memcached					🟦 33.9:1 Ov ○○○●● OpenVPN	🟦 134.24:1 Ri ○○○○● RIPv1	🟦 ★ 4,294,967,296:1 Tp ○○○○● TP240 PhoneHome
🟥 Ta TCP ACK	🟩 Ds DNS	🟩 25:1 Mq ○○○○● MSSQLRS	🟩 3.32:1 St ○○○○● STUN	🟦 1,000:1 Ch ○○○○● Chargen	🟦 24:1 Di ○○○○● DHCPDiscover	🟦 Iv IPv4 Protocol 0	🟦 4.68:1 Pm ○○○○● PMSSDP	🟦 29:1 Rc ○○○●● rpcbind/portmap	🟦 4:1 Ub ○○○○● Ubiquiti
🟥 Tr TCP RST	🟩 1:1 Ik ○○○○● ISAKMP/IKE	🟩 556.9:1 Np ○○○●● NTP	🟦 35.5:1 Ar ○○○○● ARMS	🟦 5.7:1 Ci ○○○○● Citrix-ICA	🟦 Ht HTML5	🟦 5.6:1 Jk Jenkins	🟦 140.3:1 Qd ○○○○● QOTD	🟦 30.7:1 Se ○○○○● Sentinel	🟦 2,464:1 Un ○○○○● Unreal-Tournament
🟥 Ts TCP SYN	🟩 13.5:1 Lt ○○○●● L2TP	🟩 880:1 Sn ○○○●● SNMP	🟦 120:1 Bc ○○○○● BACnet	🟦 34:1 Cp ○○○○● COAP	🟦 In IP NULL	🟦 Mh MBHTTP	🟦 63.9:1 Qk ○○○○● Quake	🟦 10:1 Sp ○○●●● SIP	🟦 14:1 Ve ○○○○● VSE
🟥 Tk TCP SYN/ACK	🟩 4.35:1 Md ○○○○● mDNS	🟩 30.8:1 Ss ○○○●● SSDP	🟦 3.8:1 Bt ○○○○● BitTorrent	🟦 37.34:1 Dt ○○○○● D/TLS	🟦 1.1:1 Ip ○○○○● IPMI	🟦 3:1 Nb ○○○●● NetBIOS	🟦 85.9:1 Rd ○○○○● RDP	🟦 Tn TCP NULL	🟦 500:1 Wd ○○○○● WS-DD

🟥 500,000+ Attacks 🟩 50,001–500,000 Attacks 🟦 0–50,000 Attacks

DDoS Attack Vector Analysis

Following a trend that started in early 2021, TCP flooding attacks (ACK, SYN, RST) remain the most commonly used attack vector (46 percent). When combined with ICMP flooding attacks (9 percent), these attacks overtake the more traditional reflection/amplification attacks, which total 45 percent. Out of those, DNS amplification constitutes 11 percent, TCP amplification (TCP SYN/ACK) follows at 10 percent, and NTP amplification makes up 5 percent. The remaining 19 percent of attacks are then split among the more exotic reflection/amplification vectors. Notably, these more exotic vectors are not part of the free tier of DDoS attacks offered by booter/stresser services.

46%

of attacks are TCP flooding attacks (ACK, SYN, RST), remaining the most commonly used attack vector.

Top 10 DDoS Attack Vectors by Count 1H2022

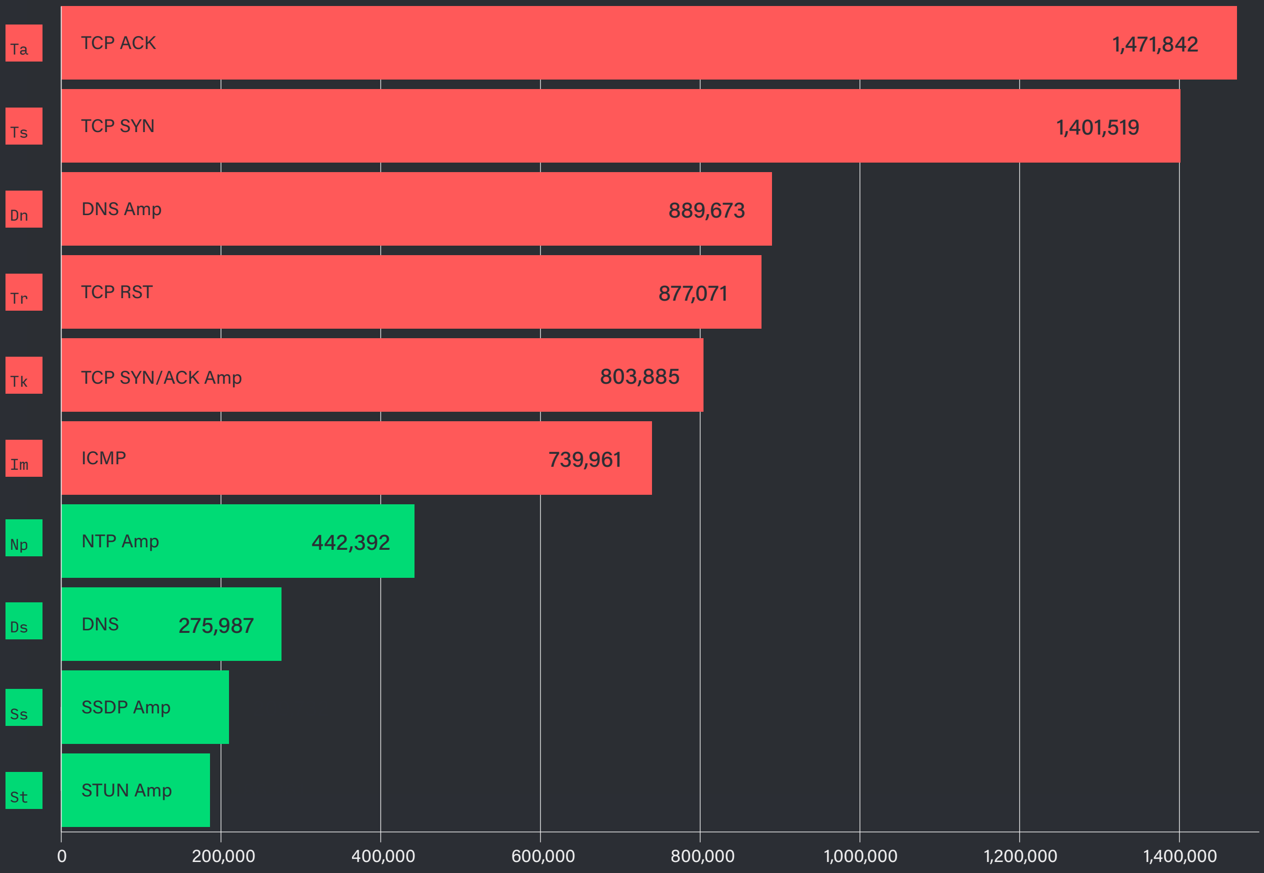


Figure 1: Top 10 DDoS Attack Vectors by Count 1H2022 (Data: ATLAS)

Abusable Devices and Amplifiers

Looking at the availability of abusable devices, the greatest number of amplifiers are SIP (4.1 million), NTP (2.5 million) and TFTP (2.2 million). DNS reflectors come in at sixth place (1.4 million). Rewind two years, and DNS took second or third place on the list, hitting more than 2.3 million abusable devices. The decrease in available DNS amplifiers and the push to implement source address validation (SAV) to stop spoofing are having a significant impact on DNS amplification attacks: They were down 21 percent from 1H 2021 to 2H 2021 and another 31 percent from 2H 2021 to 1H 2022. Overall, this almost 50 percent reduction in total DNS amplification attacks has had a significant impact on the entire DDoS threat landscape. In this vacuum, TCP-based attacks continue to increase.

-31% Dn

Decrease in DNS amplification attacks from 2H 2021 to 1H 2022. This almost 50% reduction in total DNS amplification attacks has had significant impact on the entire DDoS threat landscape.

Top 10 Available Reflector Amplifiers

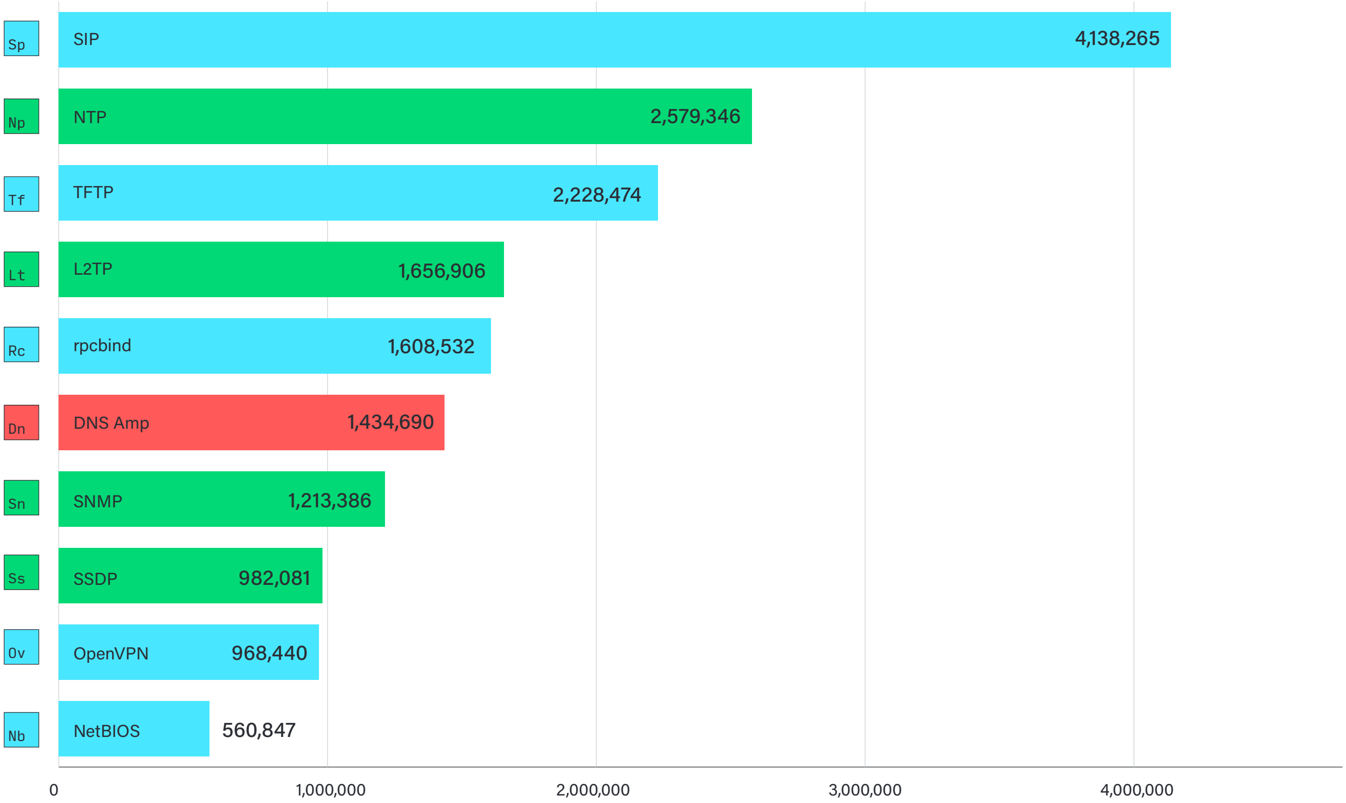


Figure 2: Top 10 Available Reflector Amplifiers (Data: ATLAS)

Tp

TP240 PhoneHome

TP240 PhoneHome

The TP240 PhoneHome reflection/amplification DDoS vector discovered in early 2022 is new to the periodic table. This vector has the largest amplification factor in history, with a record-setting packet amplification ratio of 4,294,967,296:1. This was made possible by a bug-testing facility in Mitel PBX software that allowed anyone on the internet to send spoofed UDP packets to the testing facility. This resulted in a flood of outbound packets being sent to victims.

In 1H 2022, there were approximately 4,000 attacks seen in the wild. This vector had the potential to wreak havoc that was, fortunately, avoided thanks to a swift and urgent response from Mitel to eradicate the abusable nature of this service—something NETSCOUT played an important role in facilitating. In fact, monthly attack numbers illustrate the effectiveness of those efforts:

TP240 PhoneHome Attack Timeline 1H 2022

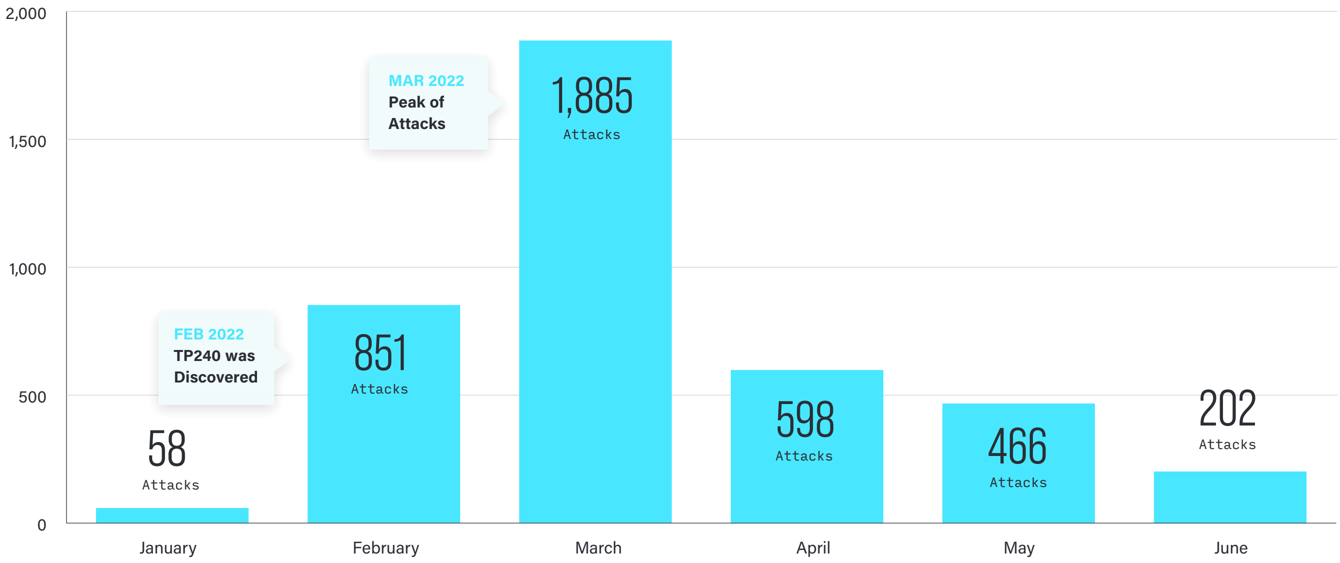


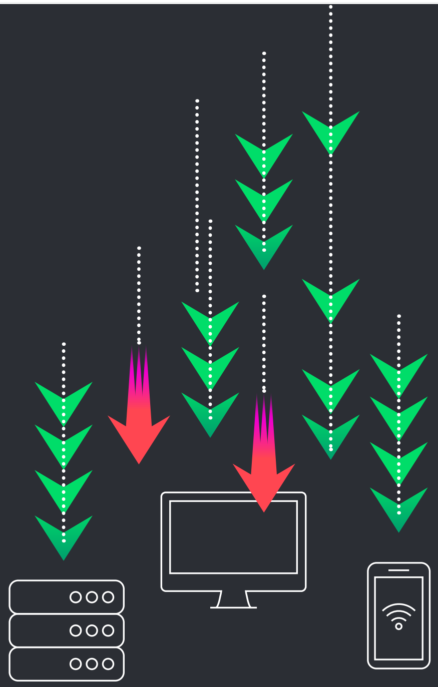
Figure 3: TP240/Mitel Attack Timeline (Data: ATLAS)

TP240 PhoneHome has the largest amplification factor in history, with a record-setting packet amplification ratio of

4,294,967,296:1

ADVERSARY METHODOLOGY

Carpet-Bombing Attacks



Carpet-bombing attacks, one of the more commonly seen methodologies, occur when an adversary spreads the attack across entire subnets or Classless Inter-Domain Routing (CIDR) blocks rather than targeting a single target or host.

Because many DDoS mitigation systems focus on individual IP addresses as opposed to entire subnets, these attacks often fly under the radar. Likewise, by attacking the subnet where the target resides, there is a greater chance of taking down other systems and services used by the victim, creating a ripple effect of collateral damage.

Carpet-bombing appears to follow the same trend line across much of the DDoS threat landscape. In many areas globally, we saw a decrease in attacks during 2H 2021 that coincided with the decrease in carpet-bombing attacks. Then, we saw a major increase in attacks right around mid-February and subsequently saw an increase in carpet-bombing attacks as well.

Carpet Bombing Attack Timeline

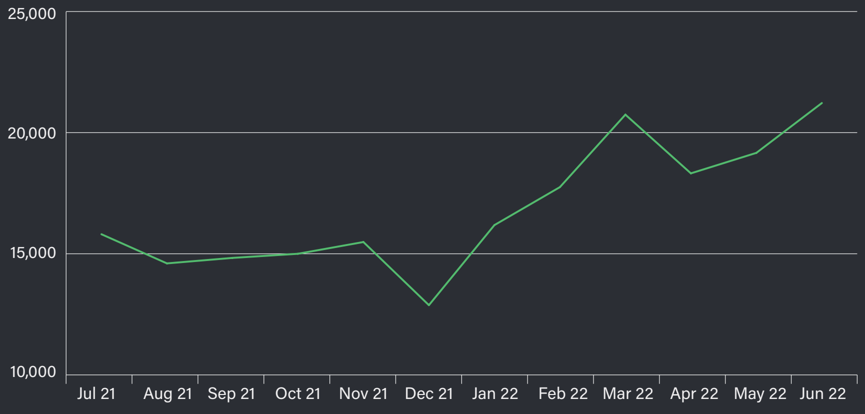


Figure 4: Carpet Bombing Attack Timeline 2H 2021 – 1H 2022 (Data: ATLAS)

The attack vectors used in carpet-bombing attacks also follow the same pattern as the global attack landscape, with a large portion including generic UDP flooding (44 percent) in multivector attacks, followed by DNS amplification (15 percent), TCP flooding (14 percent), TCP amplification (4 percent) and the remaining UDP reflection/amplification vectors (23 percent).

ATTACK VECTORS USED IN CARPET-BOMBING ATTACKS

44%	UDP Flooding
15%	DNS Amplification
14%	TCP Flooding
4%	TCP Amplification
23%	All other vectors

ADVERSARY METHODOLOGY

Application Layer Attacks + DNS Water Torture

DNS attacks targeting application-layer services, commonly known as DNS water torture, occur when an attack targets a web service designed to receive certain types of incoming traffic.

Adversaries can overwhelm the application by sending legitimate transactions that use up abnormally high resources, including CPU, bandwidth, state tables, and other resources that the application requires for normal operations. As such, these attacks can be highly effective, requiring fewer resources on the attacker side for a greater impact.

NETSCOUT has observed a startling increase in application-layer attacks in which adversaries use DNS water torture to overwhelm DNS servers with high volumes of bogus domain requests. Since 1H 2021, there has been an increase in DNS water-torture attacks, including a 46 percent increase from 2H 2021, when the entire DDoS landscape experienced an overall decline in attacks.

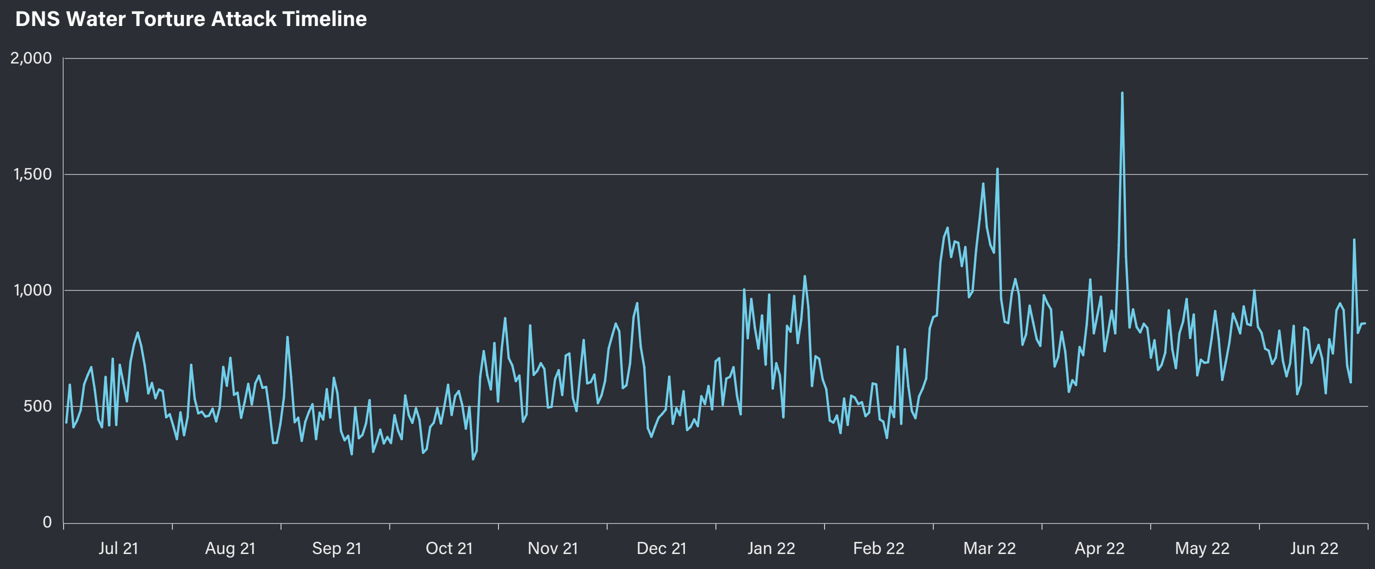
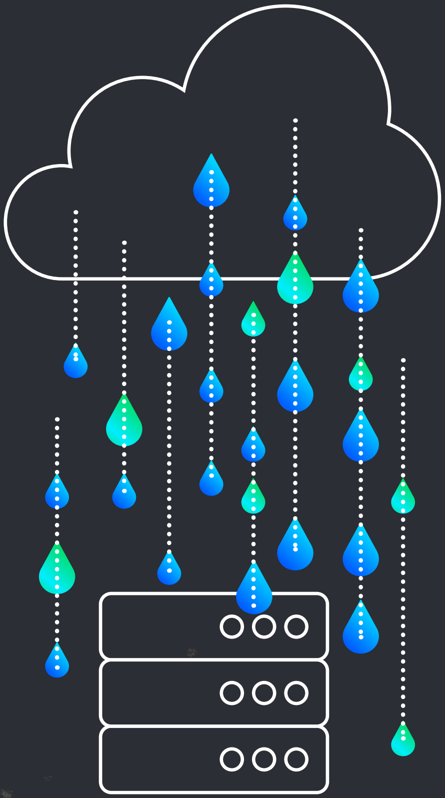


Figure 5: DNS Water Torture Attack Timeline 2H 2021–1H 2022 (Data: ATLAS)

DNS WATER TORTURE ATTACK COUNT

1H 2021	2H 2021	1H 2022
102,412	112,373	157,494



Breaking down these attacks by vector, it's apparent that attackers are relying more heavily on brute-force DNS UDP query flooding, because this vector type makes up nearly 75 percent of all DNS water-torture attacks. Although the vast majority of attacks use UDP protocol, TCP attacks associated with this attack methodology started to trend up in 2022. This trend may relate to the forced use of TCP protocol from anti-spoofing techniques designed to mitigate DNS query flooding. Alternatively, the increase could mean adversaries are using TCP-based attacks from the start. Fortunately for team defense, these particular types of TCP attacks often are not spoofed and have the potential to burn adversary infrastructure quickly.

Due to the increased focus on implementing SAV across the internet, it has become more difficult to launch spoofed DDoS attacks, and that includes both volumetric and reflection/amplification attacks. This has forced attackers to instead use bots to launch direct attacks. As such, attackers must use devices with real-source IP addresses at the risk that they'll be blacklisted and unusable for further attacks. In turn, this increases the number of application-layer attacks, which are both more powerful and easier to launch using advanced botnets.

In most cases, application-layer attacks are accompanied by more mundane DDoS attacks that act as interference or a smokescreen to successfully smuggle application-layer attacks—which are harder to mitigate via first-line defense. The three primary vectors used in conjunction with the DNS water-torture method are UDP flooding (34 percent), TCP flooding (18 percent), and DNS amplification (9 percent).

Adversary Infrastructure

Direct flooding and application-layer DDoS attacks are becoming more popular as anti-spoofing efforts increase globally and make it more difficult for spoofed packets to travel across the internet.

As part of DDoS adversary infrastructure research, NETSCOUT's ATLAS Security Engineering and Response Team (ASERT) is keeping track of the group of devices that professional attackers utilize to launch attacks. In 1H 2022, we confirmed that the most frequently used infrastructures remain relatively constant over time.

Minor changes occur when devices become useless for attackers as well as when new, compromised devices are added to the group. However, using our algorithm and visibility, we can assess with very high confidence that greater than 80 percent of all attack traffic we see originates from a relatively small number of confirmed IP addresses. The fact that there is such a high degree of reusability for adversary infrastructure is concerning, and security practitioners should take steps to obtain deep insight into network traffic to detect, identify, and eliminate the threat of repeat offenders—a process NETSCOUT already uses to secure our customers against these threats.

Adversary Infrastructure: Persistent IPs

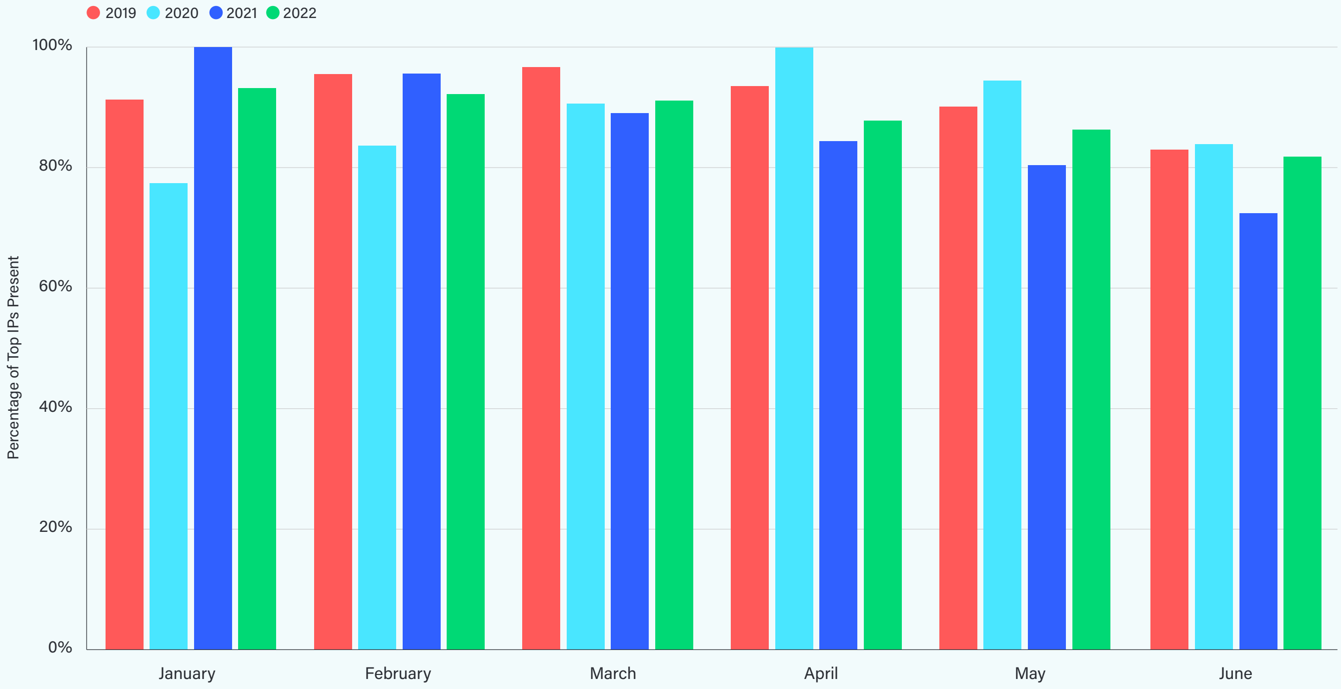


Figure 6: Adversary Infrastructure: Persistent IPs (Data: ATLAS)

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

Steinthor Bjarneson
AUTHOR

Filippo Vitale
AUTHOR

Richard Hummel
EDITOR

NETSCOUT

SECR_044_EN-2201 09/2022