ISSUE 7: FINDINGS FROM 1H 2021

NETSCOUT THREAT INTELLIGENCE REPORT

NETSCOUT

The Long Tail of Attacker Innovation

NETSCOUT Omnis Threat Horizon

If you are looking for real-time data on global DDoS attacks, Omnis Threat Horizon is an invaluable (and free) tool.

Today's cyberthreat landscape is constantly evolving, requiring visibility into malicious threats. True situational awareness requires a global view beyond your organizational perspective. NETSCOUT Omnis Threat Horizon is a free tool composed of highly curated, real-time global threat data presented in a way that allows you to understand how it impacts your organization.

INTERACTIVE VISUALS

View any chart in this report as an interactive visualization by clicking the associated **"View Live Chart"** button.

Contents

01 Executive Summary

The COVID-19 pandemic essentially handed threat actors the keys to an all-you-can-eat buffet of malicious opportunities that triggered an enormous and extended upswing in attacker innovation—and it isn't going away anytime soon.

NETSCOUT's ATLAS Security Engineering and Response Team (ASERT) expects this long tail of attacker innovation to last well into 2021, further fueling a growing cybersecurity crisis that broadly impacts organizations across the public and private sectors, from governments to corporate behemoths.

According to ATLAS data, adversaries launched approximately 5.4 million distributed denial-of-service (DDoS) attacks in the first half of 2021, an 11 percent increase from the same period in 2020. Although attack counts abated slightly from May to June, this level of activity still puts the world on track to hit close to a record-breaking 11 million DDoS attacks in 2021. And all the while, cybercriminals are stoking the innovation machine.

Key Findings

01

7 Attack Vectors in 7 Months

Threat actors exploited or weaponized at least seven of the newer reflection/amplification DDoS attack vectors within the past seven months, igniting an explosion of new attack vectors that exploit abusable commercial and open-source User Datagram Protocol (UDP) services and applications.

Meanwhile, the number of vectors used in multivector DDoS attacks has soared, with a record-setting 31 attack vectors deployed in a single attack against one German organization. The result: Greater risk for organizations.

02

Adaptive DDoS Attacks

Adversaries developed new DDoS attack techniques designed to evade traditional defenses. Using adaptive DDoS principles, threat actors now can customize each attack to bypass both cloud-based and on-premises static DDoS defenses.

Adaptive DDoS attackers perform significant pre-attack research and reconnaissance to identify areas within service delivery chains that are vulnerable to specific types of attacks. Armed with this intelligence, they then launch a single, orchestrated onslaught of attack vectors perfectly calibrated to take down a target.

03

Connectivity Supply Chain Under Attack

The global connectivity supply chain is increasingly under attack as cybercriminals concentrate their activities on vital components of internet operations, such as DNS servers, virtual private network (VPN) concentrators and services, and internet exchanges.

These services and infrastructure elements are vital gateways to online life; successful attacks against them can cause a cascade of collateral damage that affects a huge array of entities, from banks and retailers to wired and wireless service providers—not to mention myriad individual users.

04

Triple Extortion: A Ransomware Trifecta

Ransomware gangs added triple extortion attacks to their service offerings. By combining file encryption, data theft, and DDoS attacks, threat actors have hit a ransomware trifecta designed to increase the possibility of payment.

05

ISPs Face DDoS Extortion Attacks

Threat actors launched the self-dubbed Fancy Lazarus DDoS extortion campaign that primarily targets authoritative DNS servers for internet service providers (ISPs). Meanwhile, the more broadly based Lazarus Bear Armada (LBA) DDoS extortion campaign continues to target victims across a range of industries.

06

Botnet Exposé

Against the backdrop of surging DDoS attack numbers from previous years bolstered by newly weaponized attack vectors, botnets continued their steadfast propagation and contribution to the larger DDoS threat landscape.

We've tracked botnet clusters and high-density attack-source zones around the world to showcase how malicious adversaries abused these botnets to participate in more than 2.8 million DDoS attacks in the first half of 2021 alone.

Adversaries thrive on constant innovation.

Attacks will only grow more complex, and threat actors will continue to discover and weaponize new attack vectors designed to exploit the vulnerabilities found in our digital world. It is imperative that defenders and security professionals remain vigilant in their efforts to protect the critical infrastructure that drives the modern digital economy.

NUMBER OF ATTACKS 1H 2021:

5,351,930

02

DDoS Global Attack Trends

Threat actor innovation tends to be methodical, as adversaries wring a full measure of value from every opportunity before changing tactics or targets. However, the unprecedented opportunities triggered by the COVID-19 pandemic have presented adversaries with an embarrassment of potential riches, so a much longer cycle of innovation seems likely.

Case in point: Bad actors launched approximately 5.4 million DDoS attacks in 1H 2021—yet another record-breaking number. In particular, attackers launched unprecedented numbers of DDoS attacks in the first quarter, boosting attack frequency by 20 percent over the same time period in 2020. Meanwhile, adversaries discovered or weaponized seven UDP reflection/amplification DDoS attack vectors and developed adaptive multivector attacks specifically tailored to exploit vulnerabilities of their targets. Vital components of the connectivity supply chain came under increased attack, while ransomware gangs added triple-extortion DDoS tactics to their repertoire and the Fancy Lazarus DDoS extortion campaign kicked into high gear.

EVEN INNOVATION ISN'T ALWAYS A GOOD THING.

Global Stats: Number of Attacks

5,351,930

Percent Change: +11%
Average Attack Duration: 50 minutes (+31%)

Largest Attack

1.5 Tbps

Percent Change: +169%
Date: June 18
Target: German ISP
Vectors Used: DNS reflection/amplification

Fastest Attack

675 Mpps

Percent Change: +16.17%
Date: March 22
Target: Brazilian wireline broadband internet user (likely related to online gaming)
Vectors Used: DNS reflection/amplification, TCP ACK flood, TCP RST flood, and TCP SYN/ACK reflection/amplification

Percentage changes based on 1H 2021 compared with 1H 2020

After an astonishingly busy first quarter of DDoS attack activity, things calmed down slightly in the second quarter of 2021. Unfortunately, "calmed down" is a relative term. Think of a toddler throwing a full-blown temper tantrum versus one whining constantly and loudly. One is certainly calmer, but neither scenario could be called great. Although attack frequency has dropped, we are still well above the numbers that were considered normal prior to the onset of the COVID-19 pandemic.

Monthly DDoS Attack Frequency 1H 2020 vs. 1H 2021

VIEW LIVE CHART

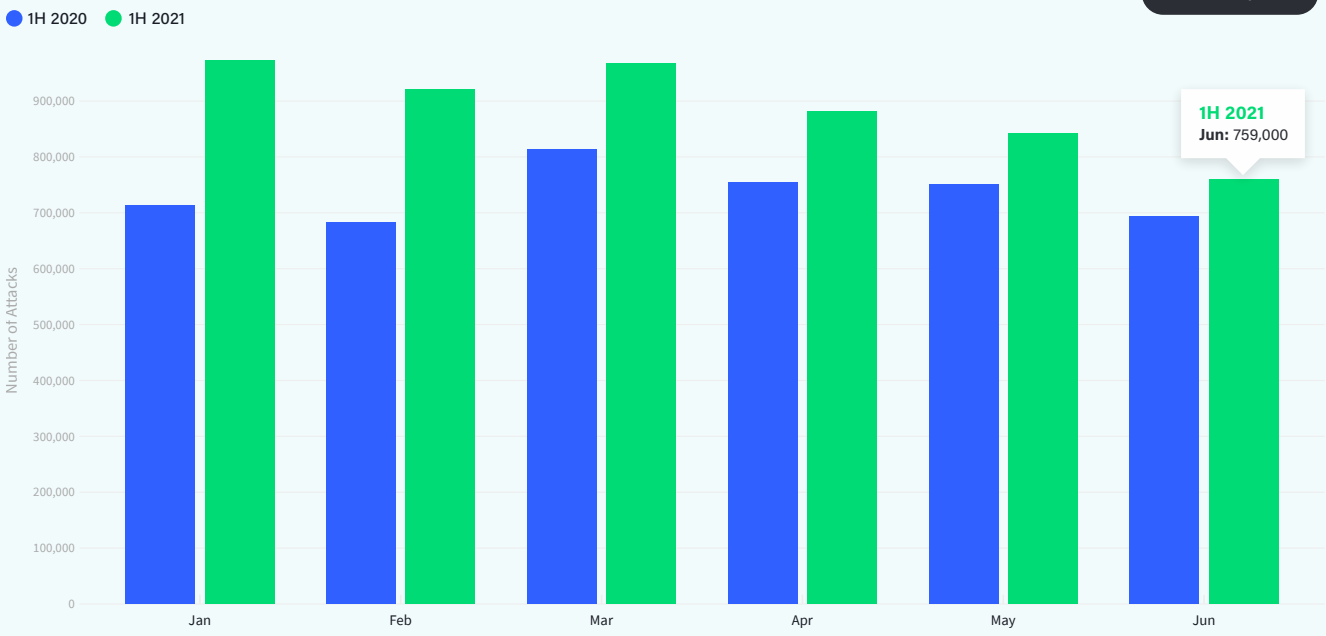


Figure 1: Monthly DDoS Attack Frequency 1H 2020 vs. 1H 2021 (Data: Omnis Threat Horizon)

The Normalization of Terabit-Class Attacks

In the first half of 2021, we witnessed at least three terabit-class attacks.*

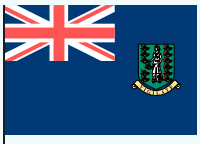
GERMANY

Attack Size
1.5 Tbps

Month
Mid June 2021

Target
ISP

Vectors Used
DNS, CLDAP reflection/amplification



BRITISH VIRGIN ISLANDS

Attack Size
1.5 Tbps

Month
Late May 2021

Target
Enterprise

Vectors Used
DNS, CLDAP reflection/amplification

HONG KONG

Attack Size
1 Tbps

Month
Late May 2021

Target
Mobile ISP

Vectors Used
DNS, DNS reflection/amplification, SSDP reflection/amplification

This was the largest attack in terms of bandwidth we observed in 1H 2021.

Despite the fact that the DDoS attack vectors leveraged in these attacks are all commonplace in the modern threat landscape, it's important to remember that quantity has a quality all its own. The good news is that organizations with up-to-date DDoS defense plans, including sufficient organic mitigation capacity and/or partnerships with skilled commercial DDoS mitigation service providers, can maintain availability even in the face of these outsized attacks on their availability.

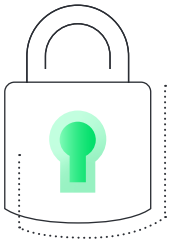
Data: Omnis Threat Horizon / Table modified from previous version for accuracy

Triple Extortion

A little bit of ransomware, a little bit of DDoS extortion, and a whole lot of trouble.

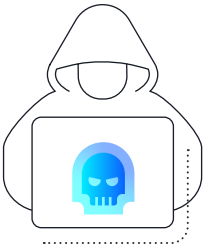
From adding new weapons to their ransomware-as-a-service (RaaS) portfolio to offering payment portals and support centers for victims, ransomware gangs are laser-focused on parting unsecured organizations from their money.

HERE'S HOW IT WORKS:



Data Encryption

This is the bedrock ransomware ploy: Cybercriminals breach a network and encrypt valuable data, blocking it (and sometimes the entire system) from the victim organization. The attackers then demand payment in return for a decryption key.

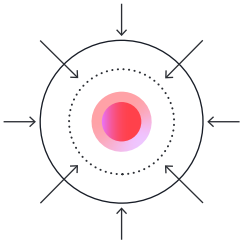


Data Theft

With the double-extortion play, cybercriminals quietly remove data before locking the victim out and then threaten to publicly expose and/or sell the stolen data unless paid. This makes it harder for victims to ignore ransomware threats, because even those who can restore data via backups remain at risk of data exposure.

Ransomware gangs known to use double extortion:

- Maze
- Sodinokibi
- DoppelPaymer
- Nemty
- Nefilim
- CLOP
- Sekhmet



DDoS Attacks

To pull off triple extortion attacks, RaaS operators add DDoS attacks (commonly used as a stand-alone extortion method) to their list of services, to be launched after steps one and two. This further ratchets up the pressure on the victim in a couple of ways: First, it emphasizes the seriousness of the adversary. And second, maintaining availability adds yet another stressor to a security team already dealing with the first two events.

Ransomware families known to use triple extortion:

- SunCrypt
- Ragnor Locker
- Avaddon
- Darkside

Ransomware is big business.

$100,000,000

One ransomware group's collection in ransom payments in 1H 2021

According to Coveware

BIG PROFITS =

more money to pay for more-expensive attack tools such as single zero-day vulnerabilities

RANSOMWARE IS A GLOBAL CRISIS.

- Attacks affect not only companies but also governments, schools, and public infrastructure.
- Global coalition Ransomware Task Force (RTF) has called ransomware "a serious national security threat and public health and safety concern."
- Heads of state are getting involved, with U.S. President Biden pressuring Russia's President Putin to shut down ransomware groups.

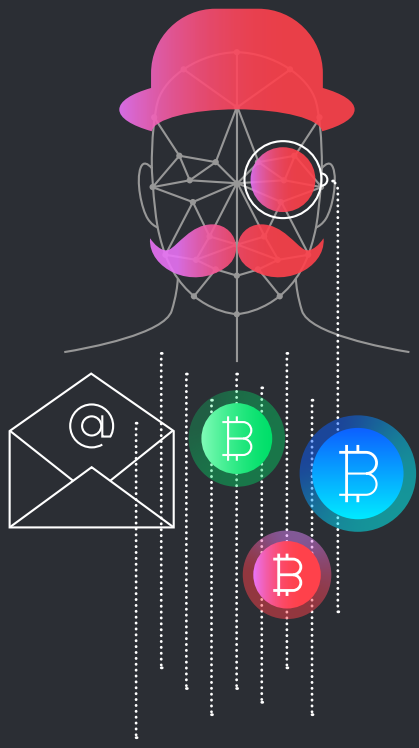
FIGHTING BACK IS A GLOBAL EFFORT.

- The White House in July announced a flurry of new federal programs to fight ransomware.
- In April, the RTF released key recommendations designed to combat ransomware.
- Interpol has called for a global coalition of police and partners to work together.

Despite these recent global efforts, we still face a massive uphill climb to make even a small dent in ransomware activity.

DDoS Extortion

DDoS extortion attacks continue to threaten organizations of all sizes and across multiple industries. As the Lazarus Bear Armada DDoS extortion campaign demonstrated, these adversaries are both persistent and adaptive, deploying new attack methodologies against an ever-expanding target set.



While the LBA DDoS extortion campaign continues to target a range of organizations, a new DDoS extortion campaign has been launched by a threat actor known as Fancy Lazarus. Despite the—dare we say it?—*fanciful* similarities between the *noms de criminel* of these threat actors, there are some key differentiators.

KEY DIFFERENCES

- Based on NETSCOUT's observations, the Fancy Lazarus campaign primarily targets ISPs (although some organizations have recently reported expanded targeting)—and more specifically, the authoritative DNS servers operated by those ISPs—whereas LBA targets a wide range of industries and service delivery elements.

- Unlike with the LBA campaign, NETSCOUT has not observed Fancy Lazarus conduct detailed pre-attack reconnaissance or adapt attack methodologies to the specifics of the targeted organizations.

- Attack vectors used by Fancy Lazarus center around DNS reflection/amplification, DNS "water torture" attacks, and TCP reflection/amplification. LBA typically leads with DNS reflection/amplification combined with at least one other reflection/amplification vector and will often use multiple additional vectors when persistently attacking a given target.

As these high-profile DDoS extortion campaigns continue and new ones emerge, successfully mitigating DDoS extortion attacks has become a high priority for enterprises and service providers alike. The most recent NETSCOUT *Worldwide Infrastructure Security Report* (WISR) reported a 125 percent increase in DDoS extortion attacks, while survey respondents listed such attacks as a primary concern, second only to ransomware.

+125%

Increase in DDoS extortion attacks as reported by the Worldwide Infrastructure Security Report (WISR)

We spoke with Carlos Morales, chief technology officer of security solutions at NETSCOUT partner Neustar, about attack trends observed by Neustar security operations center (SOC) DDoS mitigation specialists.

SOC STATS

- More than 35 customers reported receiving a DDoS extortion demand, coupled with a DDoS attack, primarily from either the LBA or Fancy Lazarus attack campaigns. Although this number may seem low at first glance, the SOC suspects that the likely prevalence of DDoS extortion attempts was significantly higher. However, not every targeted organization is willing to disclose that it's been on the receiving end of such attacks.

- More than 50 percent of targeted organizations were in the financial industry, which aligns with a primary target base of the LBA campaign.

- Throughout 2021, Neustar has performed emergency onboarding of one or more new DDoS mitigation service customers each month due to the increased prevalence of DDoS extortion attacks.

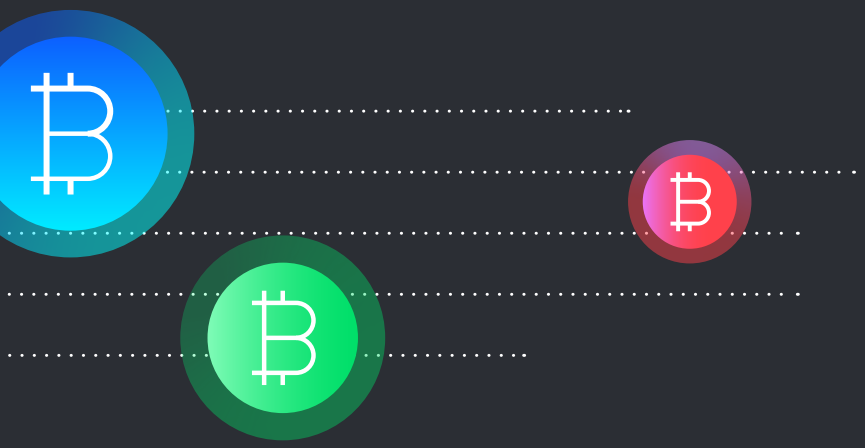
- A growing number of organizations indicate that Fancy Lazarus is on the warpath, targeting growing numbers of network operators. This tallies with observed increases in DDoS attacks directed toward authoritative DNS servers, one of the hallmarks of the Fancy Lazarus DDoS extortion campaign.

50%

Of targeted organizations were in the financial industry

INDUSTRIES REPORTING ATTACKS

- Shipping/Logistics
- Manufacturing
- Healthcare
- Energy, Media/Entertainment
- ISPs
- Hosting Providers
- Technology
- Gambling
- Retail



Connectivity Supply Chain

Although we generally think of threat actors targeting specific entities—enterprises, service providers, public sector organizations—that's not the entirety of the bad-guy sphere of interest. Cybercriminals increasingly are attacking components that make the internet tick. Unlike internet-based technologies such as cloud hosting or software as a service, these technologies allow things such as cloud computing to function over the internet. Think of it as a supply chain for connectivity.

We analyzed three key areas of what we'd classify as the connectivity supply chain and identified attacks against them.

ATTACKS AGAINST:

DNS Servers

Primarily Recursive Resolvers

Attack Count: ~4,000

Primary Vectors: DNS, DNS reflection/amplification

ATTACKS AGAINST:

VPNs

Commercial

Attack Count: ~41,000

Max Attack Bandwidth: 307 Gbps

Max Attack Throughput: 65 Mpps

Data courtesy of Neustar UltraGeoPoint data

ATTACKS AGAINST:

Internet Exchanges

Attack Count: ~1,000

Primary Vector: TCP SYN floods (70%)

LBA TARGETS:

LBA often targeted corporate VPNs to disconnect users from their organizations' online assets or prevent security teams from responding to attacks. We directly observed this tactic on multiple occasions where "vpn" was part of the targeted entity, but it's highly plausible it happened many more times where organizations practiced good OPSEC and renamed VPN nodes to something nondescript.

The most important aspect of attacks on these areas is the collateral damage inflicted.

Even if the attack does not take the component fully offline, these services represent hundreds of thousands, if not millions, of consumers, and are the gateways to everything we do online. Take one down, and you impact a huge array of people, organizations, and service providers.

Thankfully, these services are usually heavily defended, and attacks often bounce off the protection in place. We see this with the Fancy Lazarus campaign when it targets authoritative DNS servers used by ISPs. But despite the current success in defending these services, it's important to note that attackers often attempt to take down targets that could cause extensive collateral damage. This underscores the importance of constant vigilance, because it takes only one attacker innovation to change the game.

Vertical Industries

The top 10 vertical industries under attack in the first half of 2021 clearly illustrate the long pandemic tail of attack targets and methods.

Sectors such as broadband and wireless communications companies will always remain atop the target list, with attackers taking aim at both subscribers and the operational infrastructure of the companies themselves. In particular, attacks on online gaming—a hugely popular target—impact broadband, wireless, and cable internet companies (see Industry Spotlight: Online Gaming). These sectors also serve as ancillary targets, with threat actors increasingly attacking upstream and downstream connectivity providers to take down their real objective: a subscriber.

Meanwhile, the threat actors behind the Fancy Lazarus DDoS extortion campaign have focused almost exclusively on ISPs. We also note the continued popularity of the online services that businesses and consumers relied on to survive the pandemic. The sectors that contain cloud providers, Netflix, Zoom, and online shopping all experienced significant attention from cybercriminals.

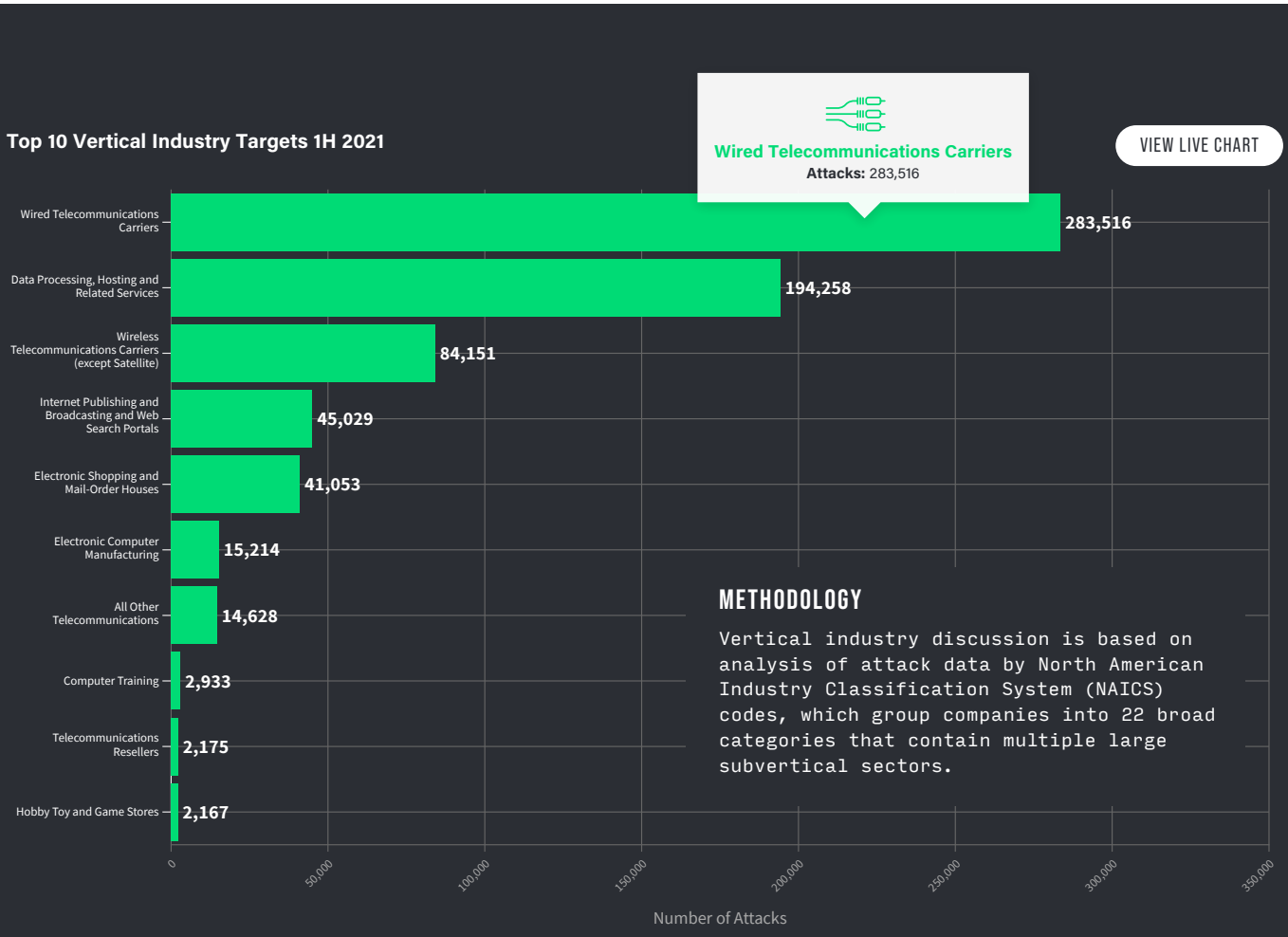


Figure 2: Top 10 Vertical Industry Targets 1H 2021 (Data: Omnis Threat Horizon)

INDUSTRY SPOTLIGHT

Online Gaming

Online gaming has always been rife with related DDoS attack activity, but the explosive growth of gaming during the pandemic added even more fuel to the fire. After all, DDoS-for-hire services are both easy to find and ridiculously cheap. And although online gaming platforms do receive a portion of the attacks, the brunt are aimed directly at gamers—and, by extension, their broadband access providers.

Online Gaming DDoS Attacks by Connection Type

VIEW LIVE CHART

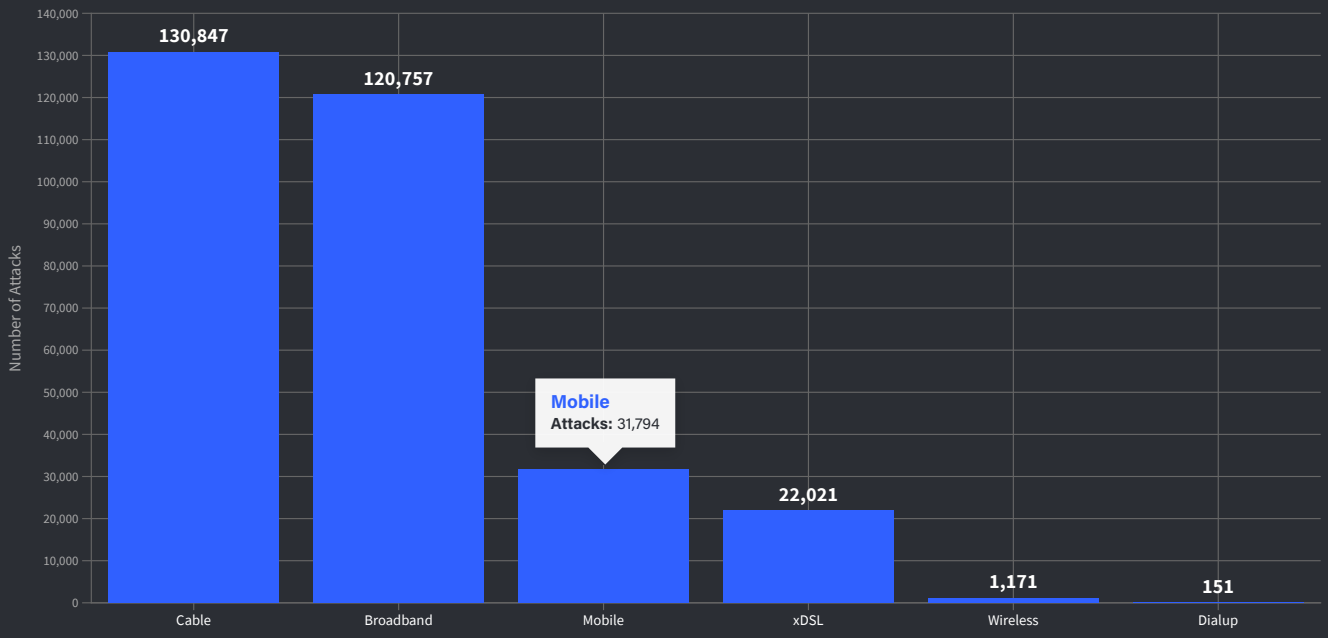


Figure 3: Online Gaming DDoS Attacks by Connection Type (Data: Omnis Threat Horizon)

VPNs Under Attack

Online game streamers know they have arrived when companies ask them to advertise their VPNs. But these days, VPNs themselves are targets. By focusing on a VPN node that may be in use by hundreds, if not thousands, of users worldwide, adversaries can inflict much higher collateral damage. Even worse, threat actors can mine those nodes for individual IP addresses. Because commercial VPNs make the list of VPN exit nodes public, it doesn't take much work for adversaries to find a slew of potential targets.

~41,000

Attacks on commercial VPNs in 1H 2021 (data courtesy of Neustar UltraGeoPoint data)

A New Era: Persistent Personal DDoS Attacks

Online gaming has always been a significant target for DDoS attacks: Common gaming industry practices such as peer-to-peer gaming session management and player-to-player voice chat give even moderately skilled miscreants the means to discover the IP addresses of their fellow players and target them with DDoS attacks. Unfortunately, those DDoS attacks often end up affecting large swathes of the ISP's adjacent customer base along with the target. For large broadband operators, the collateral damage can involve internet outages that affect thousands of users.

Now, however, DDoS-for-hire companies have taken it a step further. Security researchers and gamers on online gaming forums make note of easy-to-use solutions that allow pinpoint attacks by mapping gamer tags—players' online user names—to IP addresses. That gives malicious gamers enough data to launch DDoS attacks that knock their unsuspecting prey out of gaming sessions, disrupt their internet connectivity, and often cause collateral impact to uninvolved customers of the associated ISP.

Some of these tools are linked into associated online databases that store gamer tags along with the associated IP address(es). Malicious gamers use these information repositories to mercilessly persecute targeted gamers, in many cases not only preventing them from playing online but also disrupting their household internet access for extended periods of time.

Even worse, shady organizations now play both sides of the fence. These same services also sell purported delisting services to gamers whose gamer tags and IP addresses have been made public. Needless to say, these services provide no guarantee of success. And it takes little time for another malicious actor to flag that same gamer and relist the information with that same gamer tag database.

Those organizations also offer paid VPN services that they claim will shield gamers from DDoS attacks by hiding IP addresses. In reality, attackers can apply the same tools used to find ISP-supplied IP addresses to the task of finding the VPN-supplied IP address, which means that the VPN services offer no protection from further targeted DDoS attacks.

With these quasilegal services simultaneously empowering malicious actors while exploiting desperate targeted gamers, it's apparent that we've entered the era of the persistent personal DDoS attack. Now more than ever, it's important for broadband access ISPs to tap into top security services and edge-to-edge DDoS defense solutions to protect their users and their networks from the scourge of individualized DDoS-fueled persecution (see How Can You Protect Yourself?).

Inevitably, these attacks affect more than gamers. Targeting local networks and VPNs will almost always inflict collateral damage on innocent bystanders, making these attacks a concern for every single person on the internet.

INDUSTRY SPOTLIGHT

Commercial Banks and Payment Card Processors

DDoS attack activity in the payment card processing sector provides a useful barometer for shifting trends in adversary tactics. As threat actors adopt more complex attack techniques, we see a shift in how attack vectors are being used.

A Little Background

- There were 19 percent more TCP-based flood attacks than reflection/amplification attacks in 1H 2021.
- After two years atop the attack vector list, DNS reflection/amplification ceded first place to TCP ACK flood attacks.

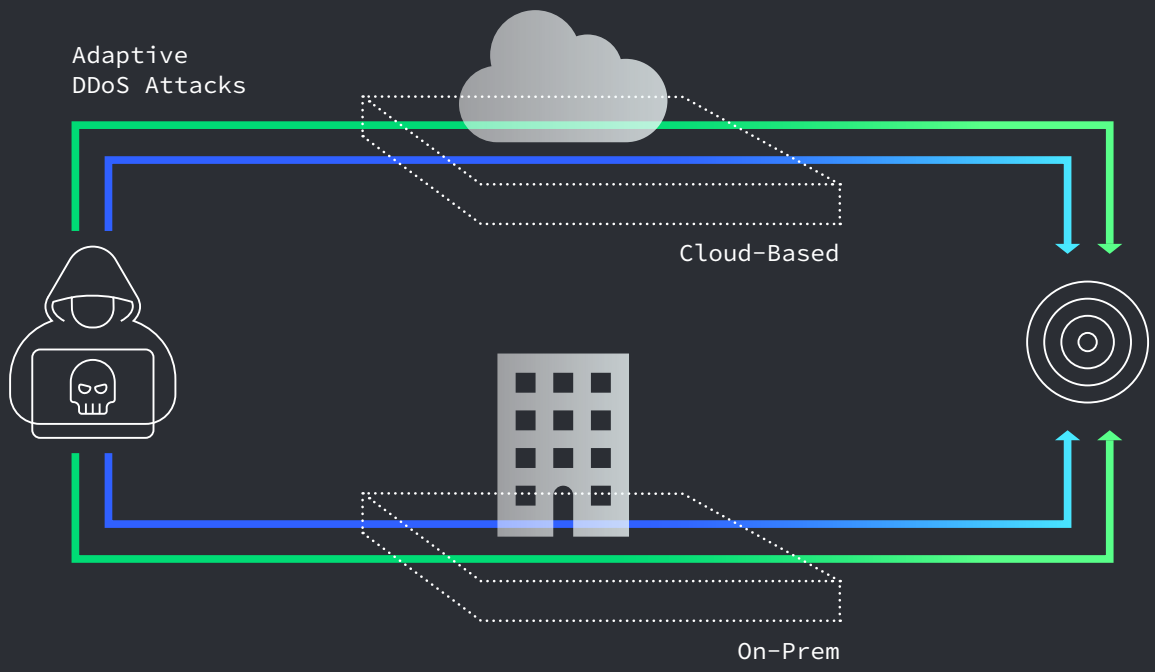
Which brings us back to the financial sector, a vertical that experienced significant increases in TCP ACK flood attacks. Many of these attacks targeted prominent payment card processing services. Attackers launched specifically chosen attack types designed to overwhelm multiple layers of both cloud-based and on-premises DDoS defenses. The result? Outages and downtime for the institutional customers of these services—and, by extension, their end customers. (It should be noted that TCP ACK floods against game developers also spiked, because many popular game developer SDKs use TCP-based connections.)

COMMERCIAL BANKS + PAYMENT CARD PROCESSORS

Attack Count	Max Bandwidth	Max Throughput
7,000+	162 Gbps	102 Mpps

Layers of DDoS Attacks

In one instance, we witnessed adversaries using well-known reflection/amplification vectors to overcome one layer of protection, followed by TCP ACK flood attacks that overwhelmed secondary defenses. In another incident, we saw this exact scenario repeated, only in reverse. Clearly, attackers are doing their homework to thoroughly understand their target's DDoS mitigation defenses before attacking. These attacks illustrate the adaptive nature of skilled adversaries: By adjusting to changes in security postures while monitoring the efficacy of their attacks, threat actors can adapt to successful defensive efforts by changing attack vectors and targets on the fly.



At more than 7,000 attacks in 1H 2021, the activity against commercial banks and payment card processing services may seem small compared with overall numbers. However, several of these attacks were successful and negatively impacted both the targeted organizations and downstream consumers attempting to use credit cards.

Given the fact that credit card processors can service as many as 5,000 transactions per second, even a few minutes of downtime can result in millions of dollars in lost revenues, not to mention negative brand impact and broad-based customer churn.

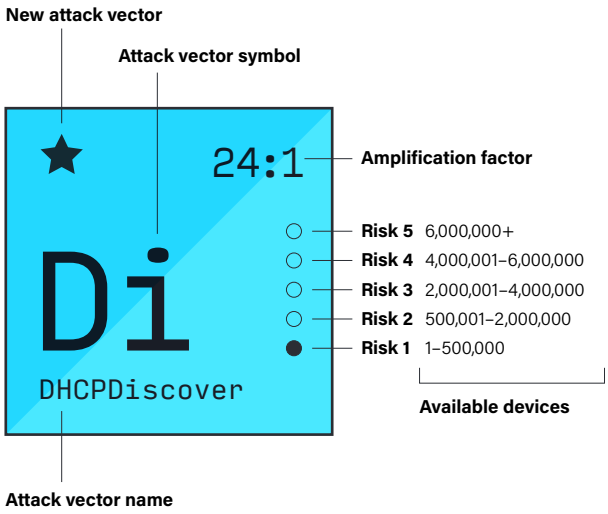
DDoS Attack Vectors

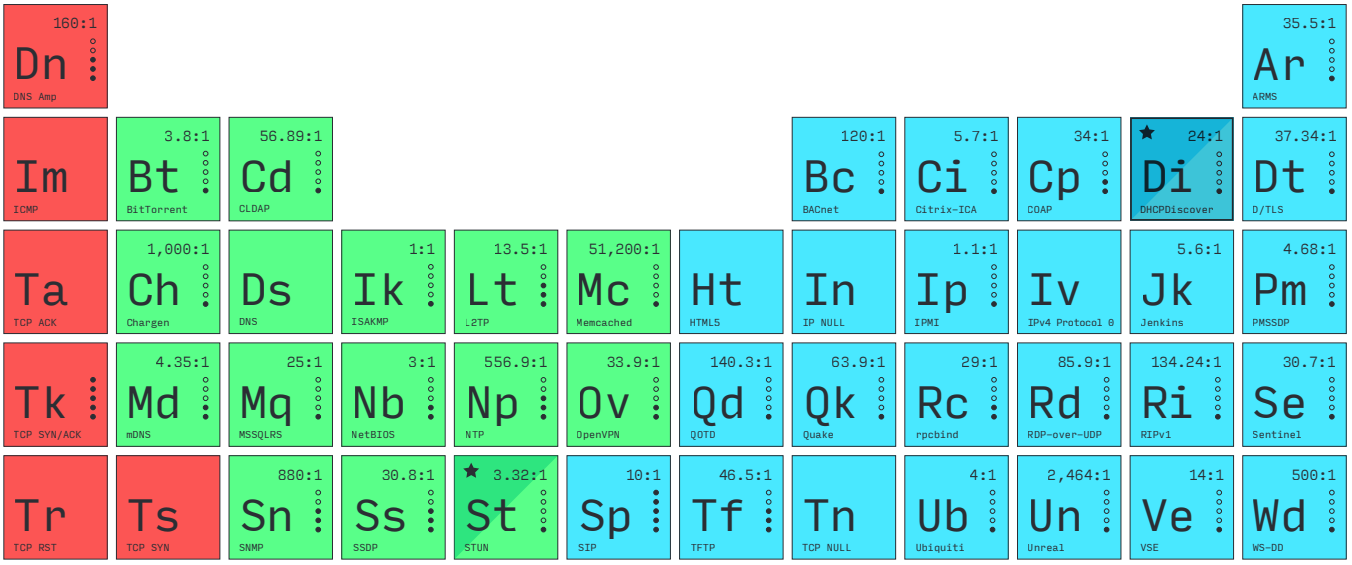
VIEW LIVE INTERACTIVE PERIODIC TABLE

DHCPDiscover

This UDP reflection/amplification attack leverages abusable, misconfigured networked DVRs, surveillance cameras, and other embedded devices to consume link bandwidth and block the ability of targeted systems to respond to network traffic.

NUMBER OF ATTACKS	797
AVAILABLE DEVICES	133,853





- 500,000+ Attacks
- 50,001–500,000 Attacks
- 0–50,000 Attacks

Abusable open-source and commercial applications and services utilizing UDP and TCP remain valuable assets for attackers. We saw a sharp uptick in new reflection/amplification DDoS attack vectors that adversaries used to power a new wave of attacks.

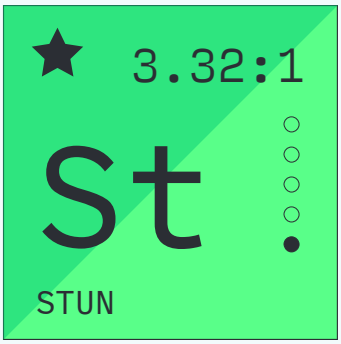
HERE'S A RUNDOWN OF THE LATEST ATTACK VECTORS AND METHODOLOGIES:

Methodology

TsuNAME Zone Cyclic Dependency-Induced Recursive DNS Query Cascade

TsuNAME is a sabotage-based DDoS attack methodology that targets authoritative DNS servers. This rather complex attack scenario involves the deliberate misconfiguration of NS records in multiple DNS domains registered by the attackers with a targeted authoritative DNS hosting service, such that the NS records for each domain pathologically refer to one another in what is termed a "zone cyclic dependency." The attackers would also be required to identify and leverage significant numbers of abusable open DNS recursive servers and/or DNS forwarders incapable of detecting and caching responses for cyclical zone dependencies.

Once attackers have successfully registered the sabotaged domains and provisioned the poisoned zone files on the targeted authoritative DNS hosting service, they can subsequently launch a classic reflected DNS query flood for the NS record. This induces the previously identified population of abusable open DNS recursors/forwarders to oscillate between the looped NS records, thereby generating endless cascades of recursive DNS queries directed toward the authoritative DNS server(s) in question. The resultant recursive DNS query cascade constitutes a DDoS attack against the targeted authoritative DNS server(s), thus having a negative impact on the availability of the targeted authoritative DNS hosting service.



Attack Vector

Session Traversal Utilities for NAT (STUN) Reflection/Amplification

STUN is a protocol used to effectuate mappings between "inside" and "outside" IP addresses and protocol ports for hosts situated behind NAT installations. It is utilized by various services such as Session Initiation Protocol (SIP), Interactive Connectivity Establishment (ICE), and Traversal Using Relays around NAT (TURN). STUN may be configured to operate over both TCP and UDP transports.

STUN services listening on UDP/3478, UDP/8088, and UDP/37833 may be abused to launch UDP reflection/amplification attacks with an average amplification ratio of 2.32:1. The amplified attack traffic consists of nonfragmented UDP packets sourced from any of the three listed UDP ports and directed toward the destination IP address(es) and UDP port(s) of the attacker's choice. The amplified attack packets range from 48 bytes (the vast majority of attack traffic) to 1,452 bytes in length. To date, 75,556 abusable STUN servers have been identified.

Attack Vector

DHCPDiscover Reflection/Amplification

DHCPDiscover, a UDP-based JSON protocol used to manage networked digital video recorders (DVRs), can be abused to launch UDP reflection/amplification attacks when an internet-exposed DVR lacks any form of authentication for the service. Unfortunately, many of these DVR variants by default do not include such authentication. When these devices are exposed to the public internet—typically via static NAT mapping—the DHCPDiscover service may be abused to launch UDP reflection/amplification attacks with an amplification ratio of ~23.15:1–25.68:1.

Top DDoS Vectors by Attack Count

After two years heading the attack vector list, DNS reflection/amplification ceded first place to TCP ACK flood attacks.

Although new reflection/amplification attack vectors are frequently discovered and used, we observed 19 percent more TCP-based flooding attacks than reflection/amplification attacks in 1H 2021. That said, there is a lot of overlap as adversaries mix and match vectors to launch complex multivector attacks.

3,848,855 Reflection/amplification attacks in 1H 2021

4,569,151 Non-reflection/amplification attacks in 1H 2021

19% Difference

Top 10 DDoS Attack Vectors by Attack Count

VIEW LIVE CHART

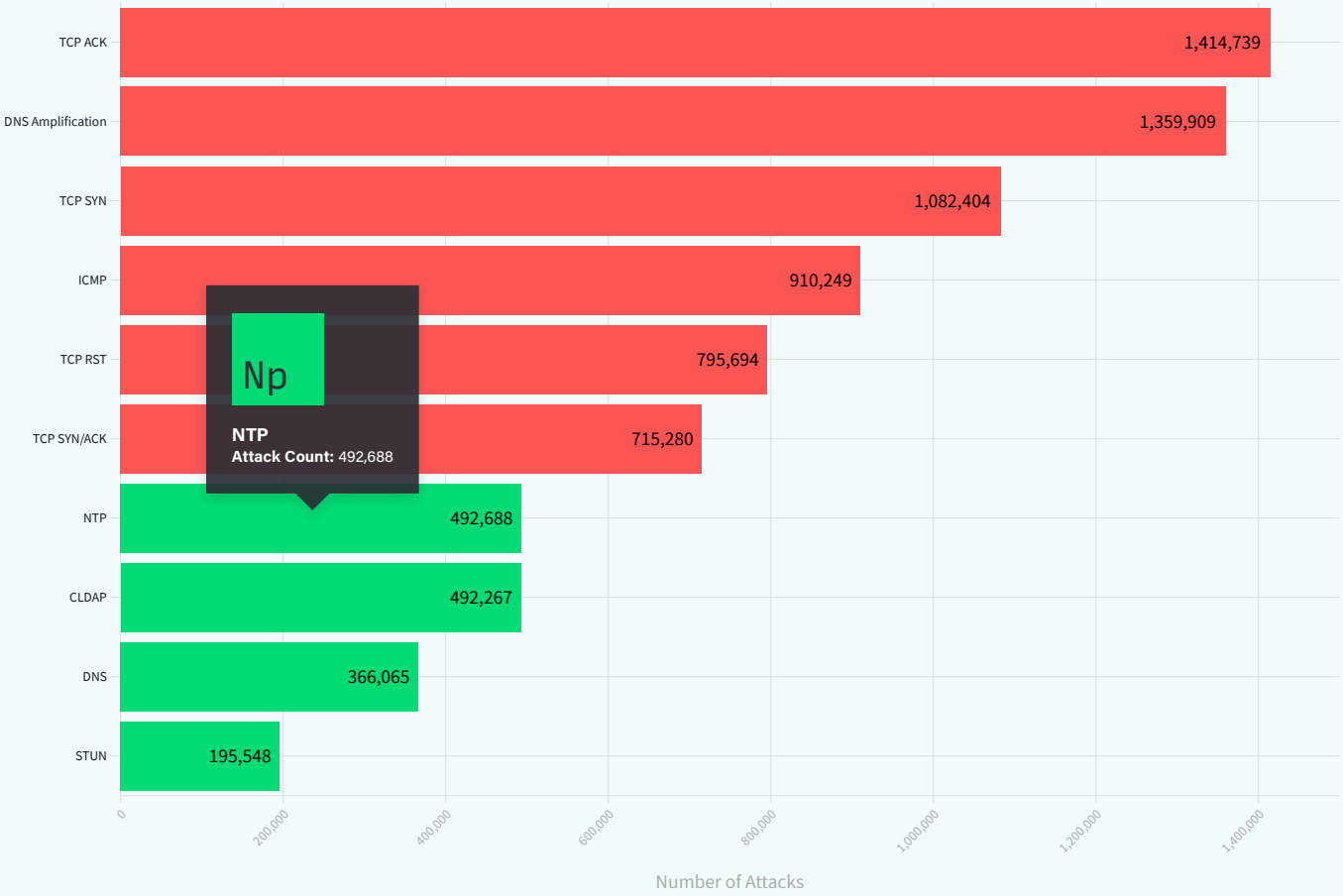


Figure 4: Top 10 DDoS Attack Vectors by Attack Count (Data: Omnis Threat Horizon)

Reflector/Amplifier Vector Distribution and Density

Adversaries continually find ways to adapt and add new tools to their repertoire.

One method is to abuse legitimate devices and protocols on the internet to reflect and amplify traffic. These operators find vulnerable devices by scanning the entire internet with probe packets to elicit an amplified response and then storing that IP address into a database they will use for attacks. To combat this ever-increasing abuse, NETSCOUT conducts internet-wide scans to identify the same devices. However, we take it a step further and correlate any matches to actual DDoS attacks in the wild. This list of IP addresses of recently observed attacks (ROAs) helps our customers shut down reflection/amplification attacks and protect themselves from a vast array of abused devices.

As part of this project, we assess the origin of these reflectors/amplifiers and use the density of these clusters to score various parts of the internet. For 1H 2021, we evaluated all of the unique devices vulnerable to abuse to illustrate key density zones. We then plotted the ROAs over time to show just how adversaries abuse these devices. Many of these devices belong to oblivious consumers—for example, woefully vulnerable Internet of Things (IoT) devices on home networks, such as routers, digital video recorders, and closed-circuit TV cameras.

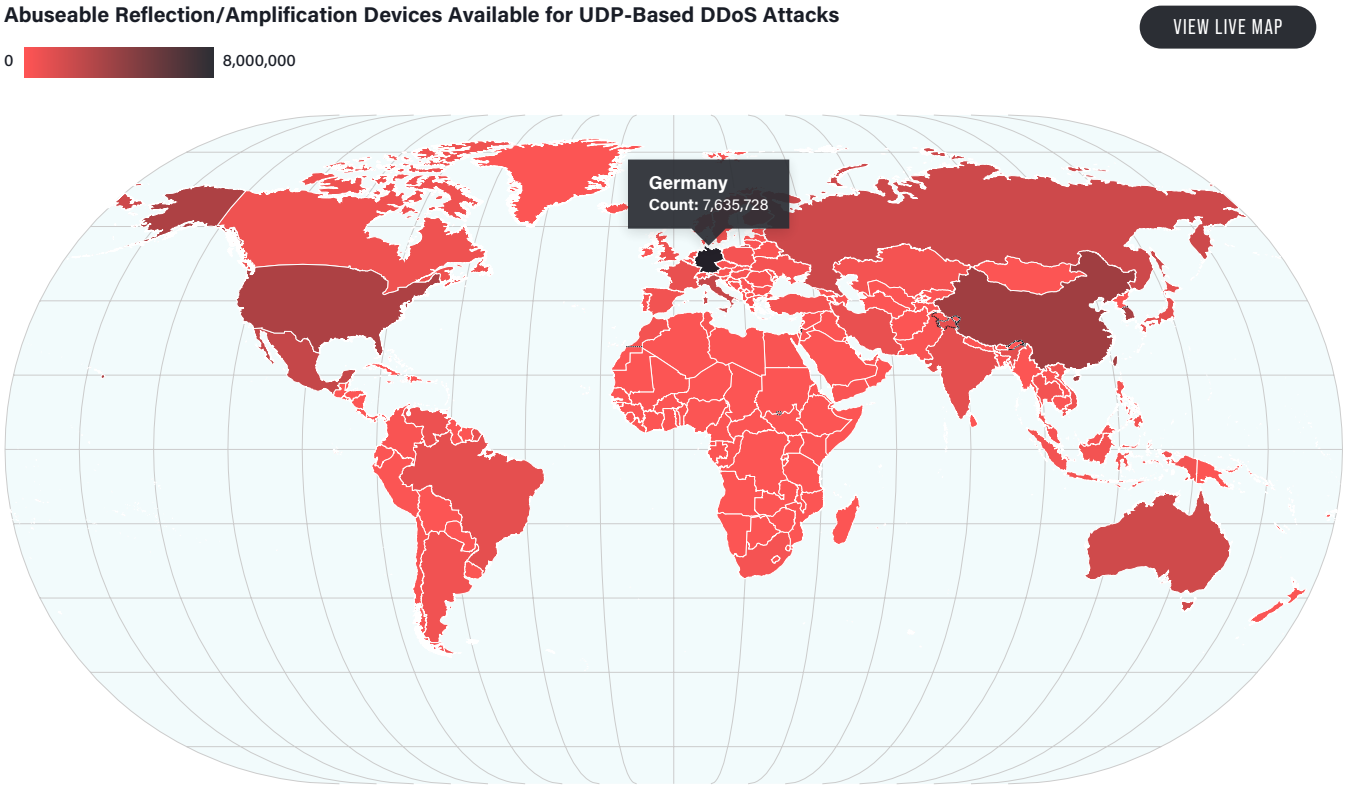


Figure 5: Abuseable Reflection/Amplification Devices Available for UDP-Based DDoS Attacks (Data: Omnis Threat Horizon)

Multivector Attacks and the Whole Kitchen Sink

There's a case to be made that DDoS attack vectors are the vampires of the threat landscape—they never die. And as adversaries constantly find and monetize new vulnerabilities, the portfolio of available vectors never stops expanding.

The always-efficient cybercrime community has made full use of this wealth to craft increasingly complex 15-plus vector attacks. We recently started calling the chart-toppers omnivector attacks, because adversaries are using all or most of the known or available DDoS attack vectors in such attacks.

Case in point: the largest multivector attack in 2020 used 26 vectors. In the first half of 2021 alone, black hats have already launched 15 attacks ranging between 27 and 31 vectors. And while 15- to 20-vector attacks show respectable growth, the real expansion hits for attacks between 22 to 26 vectors, which demonstrated growth ranging from 176 percent to 371 percent.

Percent Change in Multivector Attacks

VIEW LIVE CHART

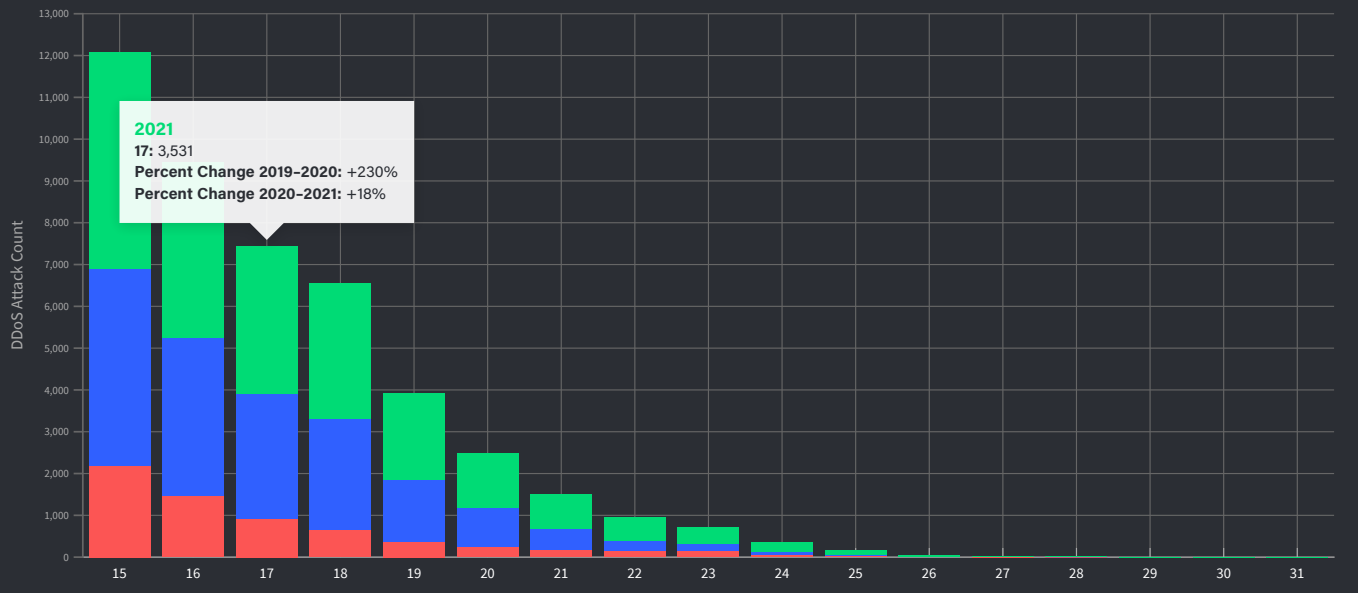


Figure 6: Percent Change in Multivector Attacks (Data: Omnis Threat Horizon)
Note: 2020–2021 percent change only accounts for first half of 2021 / 2019–2020 percent change accounts for entire year

How can you protect yourself?

As with so many other aspects of the human condition, the 80/20 rule—also known as the Pareto Principle after its famous expositor, the economist Vilfredo Pareto—applies not only to economics but also to internet security in general and DDoS defense in particular.

For approximately 80 percent of attacks, organizations that have implemented the relevant industry best current practices (BCPs) will be able to maintain availability in the face of DDoS attacks with little or no ad hoc reaction measures. The remaining 20 percent of attacks will require defenders to optimize defenses based on factors such as attacker behavior and vector selection. Even then, the time and effort expended in preparation require defenders to react in a situationally appropriate manner, maximizing the resiliency of their online properties and thwarting attackers.

NETSCOUT recommends the following actions to ensure that network operators and enterprises have maximized their ability to defend against DDoS attack.

01

Mind Your BCPs

Organizations with business-critical public-facing internet properties should implement all relevant network infrastructure, architectural, and operational BCPs, including situationally specific network access policies that permit internet traffic only via required IP protocols and ports. Deconflate internet access network traffic to and from internal organizational personnel from that of public-facing internet properties and ensure that it is served via separate upstream internet transit links.

02

Document Infrastructure Changes

Implement situationally appropriate DDoS defenses for all public-facing internet properties and supporting infrastructure, including regular testing to ensure that any changes to organization's servers, services, and applications are incorporated into the DDoS defense plan. Combine organic, on-site intelligent DDoS mitigation capabilities with cloud- or transit-based upstream DDoS mitigation services to ensure maximal responsiveness and flexibility during an attack.

03

Test, Test, Test

To optimize DDoS protection, organizations operating mission-critical public-facing internet properties and/or infrastructure must include all servers, services, applications, datastores, and infrastructure elements in recurring, realistic tests of the organization's DDoS mitigation plan. In many instances, we have encountered situations in which obvious elements such as public-facing web servers were adequately protected while authoritative DNS servers, application servers, and other critical service delivery elements were neglected, thus leaving them vulnerable to attack.

04

Custom-Tailor Countermeasures

Customize the specifics of countermeasure selection, tuning, and deployment based on the particulars of individual networks and resources.

By adhering to BCP measures and implementing these recommendations, any organization will be well positioned to successfully defend its online properties against DDoS attacks, whether those attacks fall into the 80 percent or the 20 percent of the Pareto equation.

03

DDoS Regional Attack Trends

The long tail of COVID-19-driven attack activity is generally reflected across regional statistics, with significant increases in both attack frequency and duration that reflect the growth of complex, multivector attacks.

Indeed, EMEA experienced a 31-vector attack, the largest multivector attack yet seen. Aside from perennial chart toppers such as wired and wireless telecommunications, attackers continued to target key online industries such as cloud providers, online shopping, and streaming video and conference services, which all experienced increased attacks.

Key Findings

01

Attack Frequency

Another six months of disproportionately strong growth in attack frequency, with Latin America (LATAM) showing a whopping 39 percent growth rate compared with 1H 2020. This is striking, considering that LATAM already showed 50 percent growth over the course of 2020.

Indeed, LATAM showed disproportionate growth across all categories for the second report in a row, likely reflecting significant political and ideologically motivated activity in the region.

02

Multivector Attacks

Adversaries continued to launch increasing numbers of complex multivector attacks, with EMEA and APAC recording a new high-water mark in terms of vectors used in a single attack. Multivector attacks in EMEA, which recorded the 31-vector attack, grew by 29 percent compared with the same period in 2020.

Even more telling, the use of 20-plus vector attacks skyrocketed. Whereas the largest multivector attack in 2020 clocked in with 26 attacks, the first half of 2021 went well beyond, with 15 attacks ranging from 27 to 31 vectors.

03

Attack Size

Three of the four regions experienced terabit-class attacks ranging from 1 Tbps to 1.5 Tbps. As a result, we saw significant percent increases in max attack size year over year.

04

Attack Throughput

Regional attacks exhibited considerable variability in throughput; LATAM and APAC both saw throughput increase as attackers pumped up the packets per second in an effort to overwhelm network resources and applications. North America and EMEA, on the other hand, saw throughput numbers sink.

05

Attack Duration

Attack durations increased across all regions, with significant growth in EMEA and APAC. This bucks the trend of the last 18 months toward shorter attacks and is a direct result of the proliferation of adaptive DDoS attack tactics.

31

Max number of vectors seen in a single attack (target was Germany)

+479%

Increase in throughput in Latin America

DDoS Attacks by Region

NAMER LATAM EMEA APAC

VIEW LIVE MAP

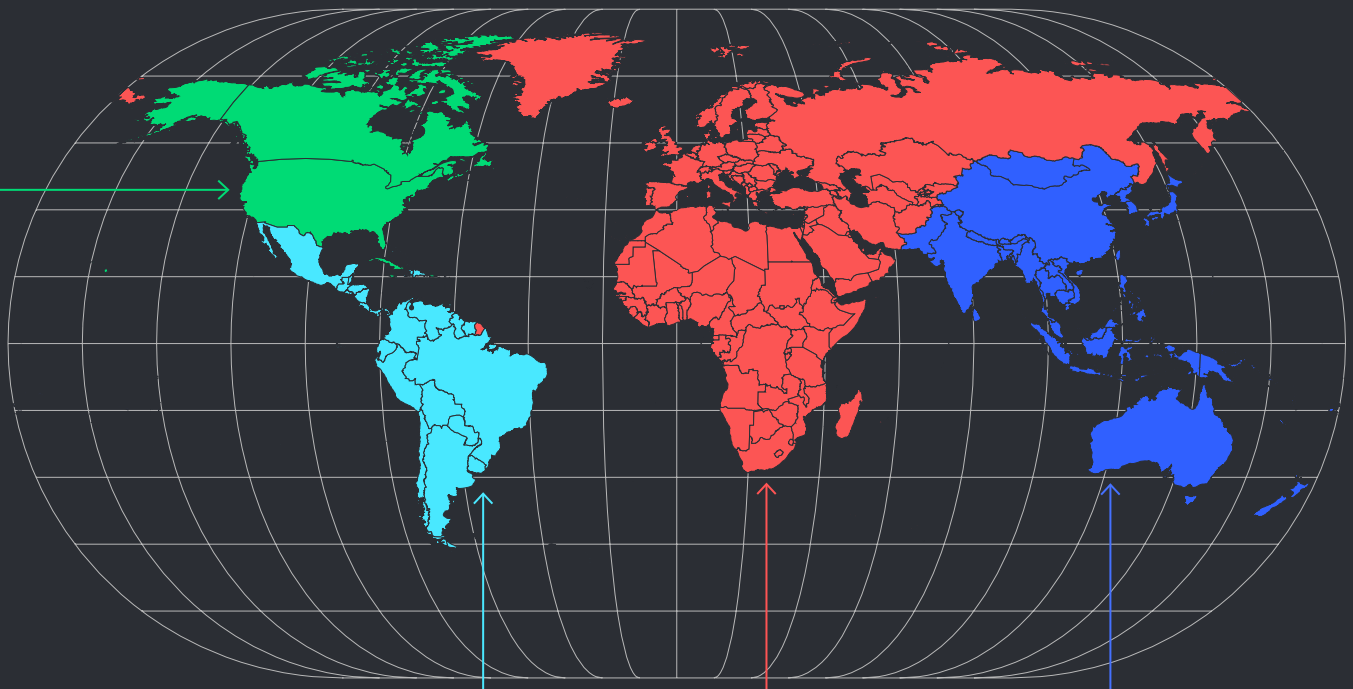


Figure 7: DDoS Attacks by Region (Data: Omnis Threat Horizon)

NAMER

Attack Frequency
1,262,467 (+10%)

Max Attack Size
629.46 Gbps (+47%)

Max Throughput
252.34 Mpps (-36%)

Average Duration
40 minutes (+8%)

Top 5 Vectors
- DNS amplification
- ICMP flood
- TCP SYN flood
- TCP ACK flood
- CLDAP amplification

LATAM

Attack Frequency
555,039 (+39%)

Max Attack Size
1.3 Tbps (+256%)

Max Throughput
675.35 Mpps (+479%)

Average Duration
63 Minutes (+2%)

Top 5 Vectors
- DNS amplification
- TCP ACK flood
- TCP RST flood
- ICMP flood
- TCP SYN/ACK amplification

EMEA

Attack Frequency
2,004,044 (+25%)

Max Attack Size
1.5 Tbps (+167%)

Max Throughput
270.50 Mpps (-5%)

Average Duration
47 Minutes (+35%)

Top 5 Vectors
- TCP ACK flood
- DNS amplification
- ICMP flood
- TCP SYN flood
- TCP RST flood

APAC

Attack Frequency
1,186,398 (-2%)

Max Attack Size
1 Tbps (+192%)

Max Throughput
471.20 Mpps (+16%)

Average Duration
62 Minutes (+55%)

Top 5 Vectors
- TCP SYN flood
- TCP ACK flood
- ICMP flood
- DNS amplification
- TCP RST

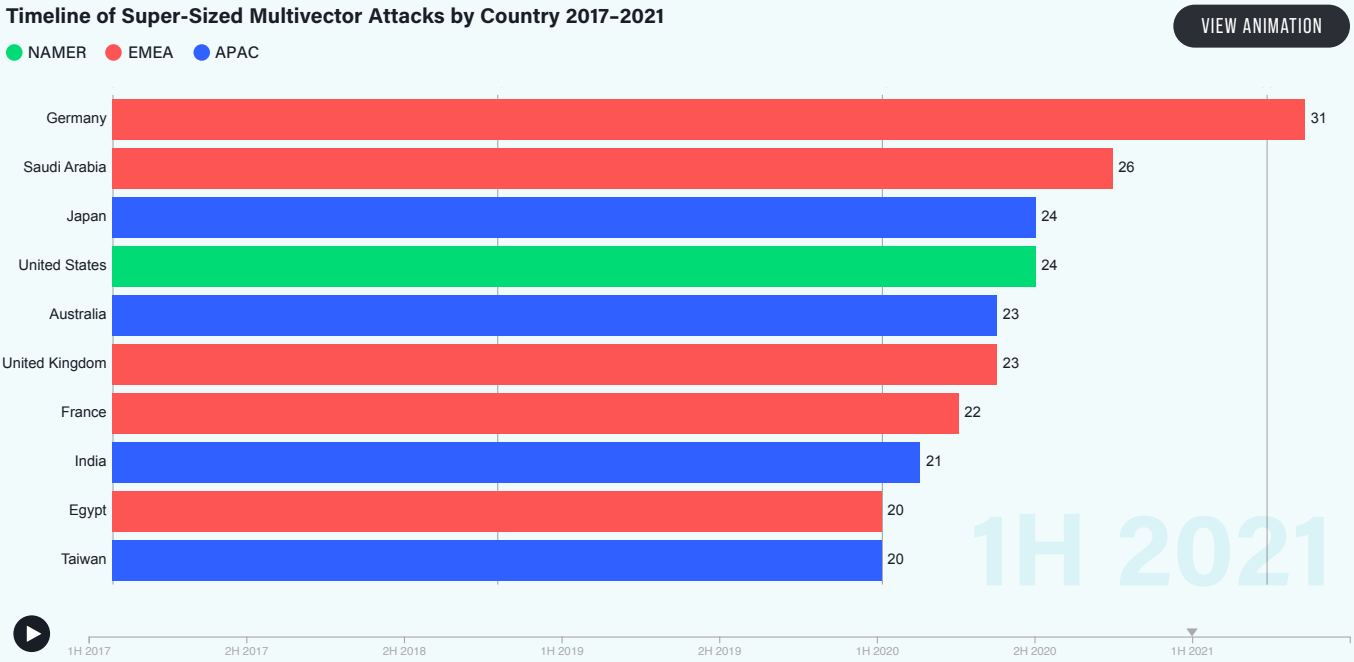


Figure 8: Timeline of Super-Sized Multivector Attacks by Country 2017–2021 (Data: Omnis Threat Horizon)

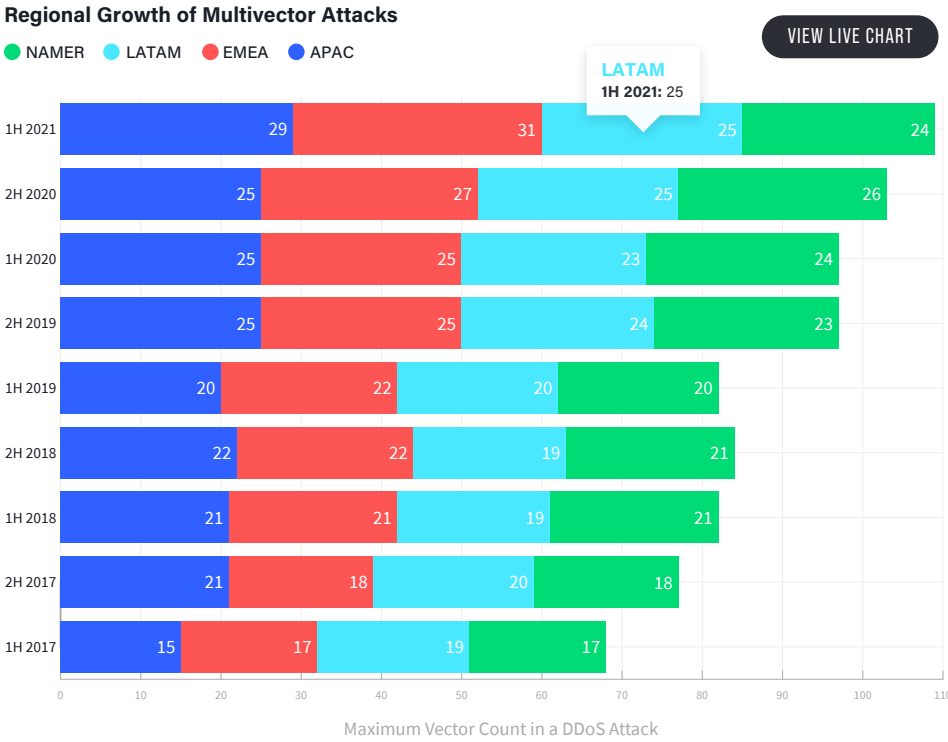


Figure 9: Regional Growth of Multivector Attacks (Data: Omnis Threat Horizon)

COUNTRY SNAPSHOTS

Read detailed DDoS attack stats for 10 countries across the global threat landscape.

LEARN MORE

Peak DDoS

For the past several reports, we've analyzed the effect DDoS traffic has on global infrastructure. Given the record-breaking DDoS attack activity seen in the first half of 2021, we can expect to see some impactful peak spikes of aggregated DDoS traffic.

By digging into the details of global DDoS traffic by region, we were able to associate some of these aggregate traffic-per-minute spikes with actual events to illustrate the real-life impact of DDoS traffic. This provides a clearer understanding of how global campaigns and disparate attacks working in concert negatively impact a network or individual entities within that network.

Spotlight on Brazil and Angola

Brazil

March 10, 2021

THE ATTACK

Nearly 50 local telecommunications providers in Brazil experienced attacks within a one- to three-minute window. The bulk of the attacks started simultaneously, suggesting that this was a coordinated, multitarget onslaught. Most of the attacks were less than 7 Gbps in size, with one exception reaching 221 Gbps in size. Attackers continued to launch successive attacks against the same targets for more than an hour.

THE PEAK DDOS SPIKE

At one point during the attack campaign, nearly 2 Tbps of aggregate DDoS traffic transited local ISPs in one minute, likely affecting significant amounts of bystander traffic in addition to the direct impact on the intended targets.

Angola

March 19, 2021

THE ATTACK

Over the course of six minutes, 81 separate DDoS attacks were launched against companies within the Internet Publishing and Broadcasting sector, primarily targeting a local TV provider in Angola. These short-lived attacks averaged 7 minutes per attack, with durations ranging from 2 minutes to 19 minutes.

THE PEAK DDOS SPIKE

The TV provider experienced approximately 1.4 Tbps of peak DDoS attack traffic over a one-minute time span.

04

IoT

Botnets may be old news, but their ability to harness legions of vulnerable IoT devices for DDoS attacks constitutes a clear and present danger. Although other vectors have emerged, botnets have traditionally been major contributors to the DDoS landscape. To understand the DDoS landscape, you need a deeper sense of the botnets behind the action.

Well-known IoT botnets, such as Gafgyt and Mirai, continue to pose a serious threat, contributing to more than half of the total number of DDoS attacks we saw in the 1H 2021. Our honeypot networks report some big numbers when it comes to vulnerable IoT devices being subsumed into botnets, and we wanted to get a clearer picture of botnet origins to educate and inform the world about their usage and distribution. By using our unique visibility of the DDoS attack landscape to identify botnets actively attacking customers, we can provide more granular detail about attack origins—and ultimately, help companies shut down DDoS botnet activity.

MIRAI

Mirai is still the predominant DDoS bot in circulation.

- 180,000+ malware samples in 1H 2021, with a significant surge in mid-March
- Mirai makes up nearly two-thirds of all linux-based malware samples collected during the same time period
- Second-place Gafgyt shows only about 50,000 malware samples—a clear indication of the preferred IoT DDoS bots used by adversaries

REVERSINGLABS

Botnet Exposé

The NETSCOUT honeypot network combines low- and medium-interactivity nodes with a global network of passive listeners. Leveraging data from NETSCOUT and a new sharing partner, GreyNoise, we collected observations on more than 1 million botted nodes worldwide. (A botted node consists of devices/systems that have been compromised by malicious bot software.) We then correlated the list of nodes with our global DDoS attack telemetry to identify bots actively contributing to DDoS attacks. Over the course of six months, we found approximately 200,000 botted nodes that participated in roughly 2.8 million DDoS attacks globally.

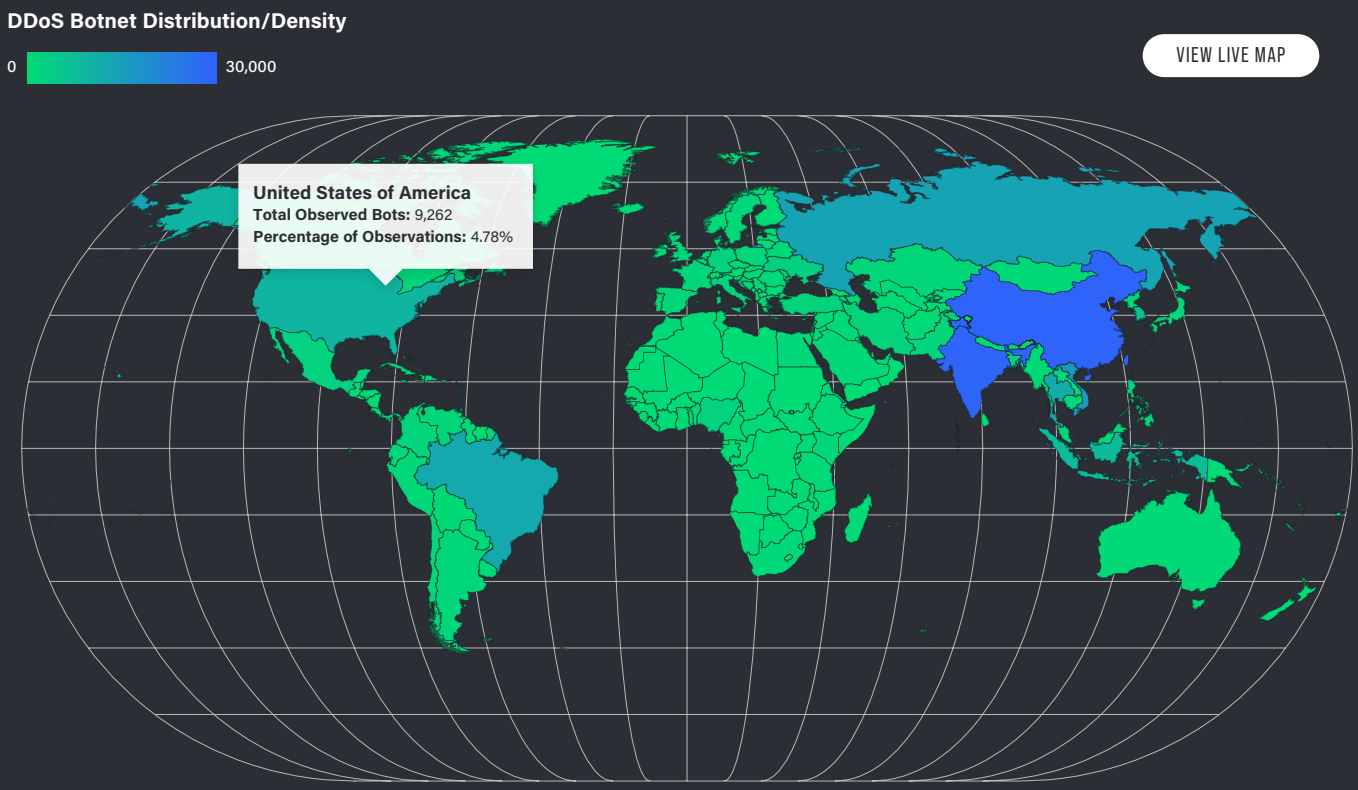


Figure 10: DDoS Botnet Distribution/Density (Data: Courtesy of NETSCOUT Partner GreyNoise)

In the first six months of 2021, the honeypot networks observed more than a million unique IP addresses across 202 countries. Leveraging only the IPs also observed in DDoS attacks, we took a closer look at the three countries with the most DDoS botnet nodes: China, India, and Vietnam.

The goal of this research is to help network operators and security professionals understand the flow of internet traffic from botted nodes in country origins as well as how bots in these countries propagate, so they can better defend and protect networks and devices. In addition to looking at the total dispersion of all bots geographically, we also dive into the top three, showcasing how bots propagate and where the botted nodes are concentrated down to how many classless interdomain routing (CIDR) addresses the bulk of the DDoS attack traffic emerged from in 1H 2021.

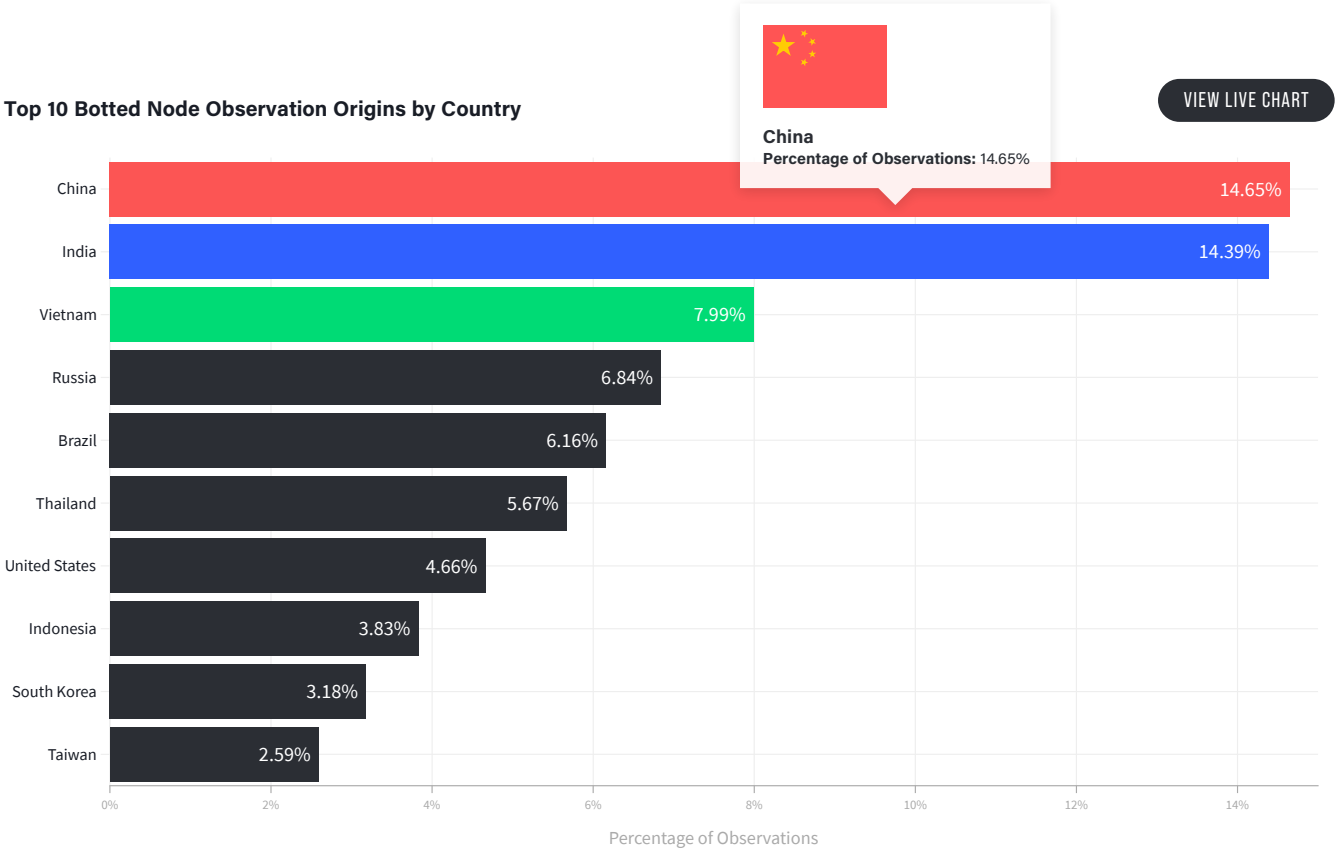


Figure 11: Top 10 Botted Node Observation Origins by Country (Data: Courtesy of NETSCOUT Partner GreyNoise)

China

Honeypot Observations 1H 2021

2,000,000+

Unique Credential Sets

147,290

Top Botnet

Mirai

Autonomous System Numbers (ASN)

- 56.72 percent botted nodes reside inside of two ASNs
- One ASN had three IP addresses that contributed to 36.53 percent of all observed botted node traffic
- 54.88 percent of that ASN's traffic originated from 23 IP addresses in a /16 CIDR block

TOP 5 USER/PASS	MIRAI VARIANTS	TOP 5 EXPLOITS	TOP 5 EXPLOITS EDB-ID
root/vizxv	IZ1H9	Huawei Router HG532 Arbitrary Command Execution	EDB-ID: 43414
admin/admin	OWARI	Hadoop YARN ResourceManager Command Execution	EDB-ID: 45025
root/root	KYTON	Realtek SDK Miniigd UPnP SOAP Command Execution	EDB-ID: 37169
guest/12345	JOSHO	Laravel 8.4.2 debug mode Remote Code Execution	EDB-ID: 49424
root/xc3511	ZHTRAP	ZeroShell 3.9.0 'cgi-bin/kerbynet' Remote Root Command Injection	EDB-ID: 49096

Table 1: China Botnet Snapshot (Data: Omnis Threat Horizon)

India

Honeypot Observations 1H 2021

340,000+

Unique Credential Sets

71,131

Top Botnet

Mirai

Autonomous System Numbers (ASN)

- 20.37 percent of botted nodes reside inside of three ASNs
- One ASN had one IP address that contributed to 36.53 percent of all observed botted node traffic
- 62.93 percent of all botted node traffic from one ASN came from a single IP address

TOP 5 USER/PASS	MIRAI VARIANTS	TOP 5 EXPLOITS	TOP 5 EXPLOITS EDB-ID
guest/12345	PEDO	Huawei Router HG532 Arbitrary Command Execution	EDB-ID: 43414
hikvision/hikvision	ZHTRAP	Realtek SDK Miniigd UPnP SOAP Command Execution	EDB-ID: 37169
admin/4321	KURC	Hadoop YARN ResourceManager Command Execution	EDB-ID: 45025
root/xc3511	OSHO	GPON Routers Authentication Bypass/Command Injection	EDB-ID: 44576
admin/admin	KYTON	Laravel 8.4.2 debug mode Remote Code Execution	EDB-ID: 49424

Table 2: India Botnet Snapshot (Data: Omnis Threat Horizon)

Vietnam

Honeypot Observations 1H 2021

300,000+

Unique Credential Sets

23,051

Emerging Botnet

MikroTik router username and password combination

- MikroTik-related passwords accounted for 12.56 percent of all user/pass observations originating from Vietnam
- Suggests targeting of a profiled set of devices

Autonomous System Numbers (ASN)

- 89.18 percent of botted nodes reside inside of four ASNs
- Top two ASNs contribute to 59.45 percent of all tracked botted nodes
- In one ASN, three IP addresses contributed to 26.46 percent of all botted node traffic

MIKROTIK USER/PASS OBSERVATIONS

- `MikroTik:`
- `MikroTik:1`
- `MikroTik:11`
- `MikroTik:1122`
- `MikroTik:123`
- `MikroTik:1234`
- `MikroTik:12345`
- `MikroTik:123456`
- `MikroTik:1234567`
- `MikroTik:12345678`
- `MikroTik:123456789`
- `MikroTik:admin`
- `MikroTik:admin1`
- `MikroTik:admin123`
- `MikroTik:password`
- `MikroTik:qwerty`
- `MikroTik:test`

TOP 5 USER/PASS	MIRAI VARIANTS	TOP 5 EXPLOITS	TOP 5 EXPLOITS EDB-ID
guest/12345	SWZNL	Huawei Router HG532 Arbitrary Command Execution	EDB-ID: 43414
admin/admin	ARMDS	Realtek SDK Miniigd UPnP SOAP Command Execution	EDB-ID: 37169
default/default	SORA	Hadoop YARN ResourceManager Command Execution	EDB-ID: 45025
admin/4321	PMVFX	GPON Routers Authentication Bypass/Command Injection	EDB-ID: 44576
root/root	JOSHO	Laravel 8.4.2 debug mode Remote Code Execution	EDB-ID: 49424

Table 3: Vietnam Botnet Snapshot (Data: Omnis Threat Horizon)

Source Device Operating System Profiles

The botnets we track typically have a common device profile; from that profile, we see the following operating systems on the bots attempting to propagate. The top three operating system profiles were Windows 7/8, Linux 2.2-3x, and Linux 2.4x. Users and network operators can employ this information to determine what kind of devices are resident on their network and match those devices against commonly used username and password combinations to ensure they aren't susceptible to brute-forcing attempts.

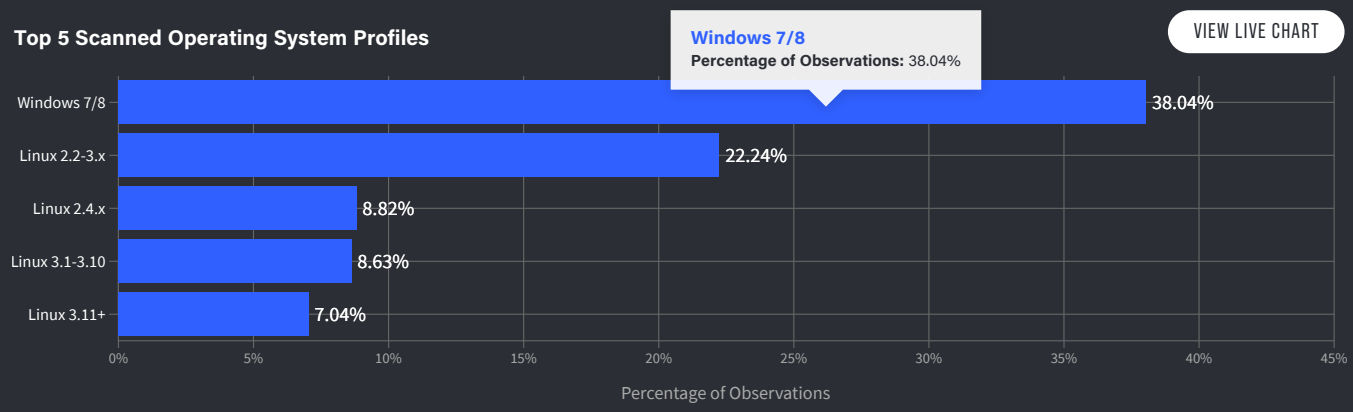


Figure 12: Top 5 Scanned Operating System Profiles (Data: Courtesy of NETSCOUT Partner GreyNoise)

Source Network Provider Classifications

In addition to understanding the device profile and operating system type, we were able to break down the network types to better show where these botted nodes reside. Note the low percentage of observations from business or education networks. This is probably due to more stringent control over what devices are allowed on the network in these institutions. The top three source network profiles were ISP, mobile, and hosting, where device control is nearly nonexistent. That lack of control means that those ISP and mobile numbers really represent compromised subscribers.

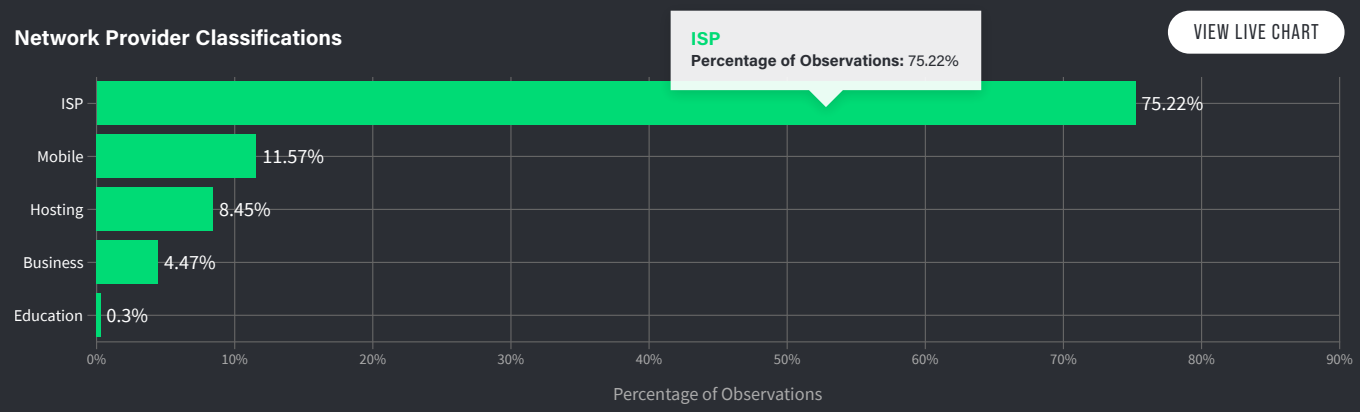


Figure 13: Network Provider Classifications (Data: Courtesy of NETSCOUT Partner GreyNoise)

Botnet Propagation

Botnets propagate via a variety of methods, including brute-forcing, exploitation, and lateral network movement. Based on data from GreyNoise, the top five exploitation behaviors observed on these botted nodes, which also contributed to DDoS attacks, were the following.

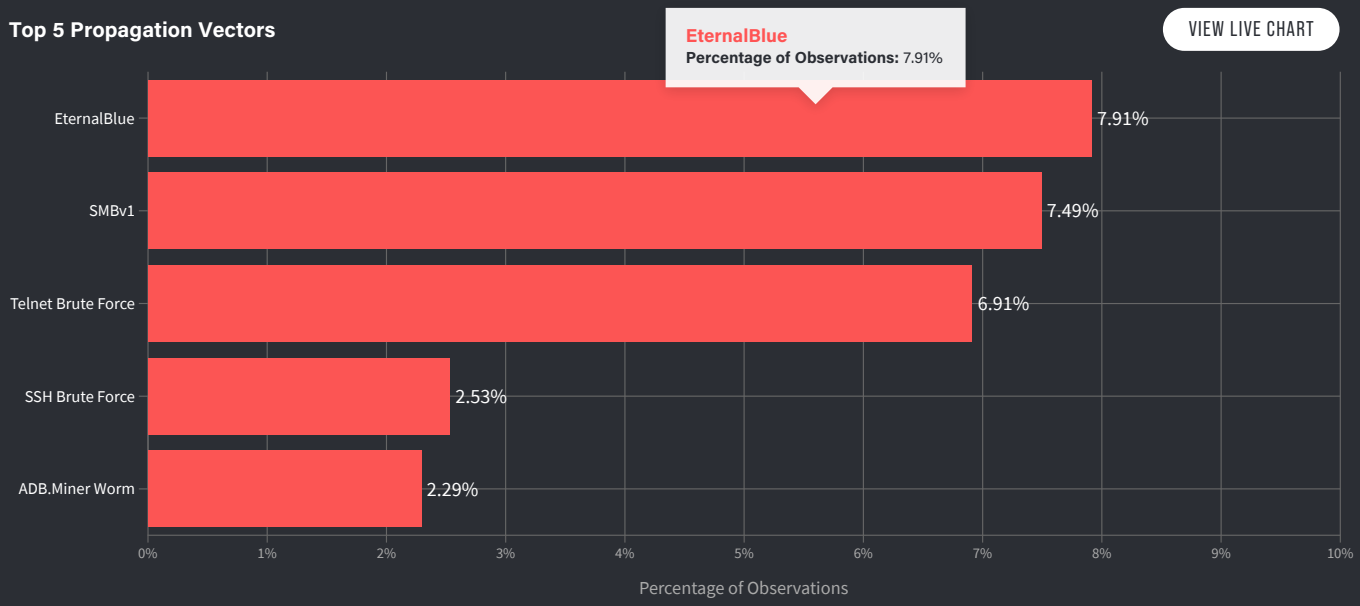


Figure 13: Top 5 Propagation Vectors (Data: Courtesy of NETSCOUT Partner GreyNoise)

05 Conclusion

The long tail of cybercrime innovation swept through the lockdown days of the COVID-19 pandemic to infiltrate the bulk of 2021. Seven emergent attack vectors in seven months represents a much faster discover-and-weaponize rate than we usually see. Meanwhile, threat actors discovered ever-more-ingenious ways to part organizations from their money, such as the advent of triple extortion ransomware and DDoS extortion campaigns.

Although the vulnerabilities introduced by the global shift to online work and play are admittedly an outlier event, the avidity of the threat actors' response should serve as a clarion call for an integrated global response to what many cyber experts believe is a national security risk. The U.S. Government Accountability Office (GAO) recently issued a report that highlights "the pressing need to strengthen federal cybersecurity and IT management," with a recommendation to urgently address high-risk areas, such as by actually creating a comprehensive federal cybersecurity strategy.

As noted in our research into attacks on the connectivity supply chain, the information and communication technology supply chains also represent risks, a fact also called out by the GAO. In the wake of events such as the Colonial Pipeline ransomware attack and the Solarwinds hack, it's clear that enterprise and service provider cybersecurity is increasingly intertwined with that of the public sector and what we consider critical infrastructure. As the danger posed by cybercrime rises to the level at which heads of state get involved, it's clearly past time for a concerted global effort to combat the crisis. Although the genie likely never will be returned to the bottle, world leaders need to do a better job of corralling such activity.

A note from the editors

Given the ongoing surge in DDoS attack activity, we fully expected that our "up and to the right" mantra would prove correct for the first half of 2021 with a record-setting 5.4 million attacks.

The world recently witnessed record-setting performances and athletics with the Tokyo Olympics, but such records in the DDoS world represent a shift in polarity and not something we ever want to achieve. Like elite athletes or smart entrepreneurs, threat actors know they must continually push beyond the expected and known. Innovation in the threat landscape happens swiftly—and when it comes to parting unsecured organizations from their money, those innovations never stop.

But the sea change wrought by the COVID-19 pandemic means that we're now in uncharted territory. The breadth and depth of opportunities to exploit the increasing online dependence of organizations in every sector of human activity triggered a long tail of attacker innovation that continued well into 2021, culminating in the mainstreaming of complex, adaptive DDoS attack methodologies that can pose significant challenges to defenders.

These threat actors use adaptive DDoS attack techniques to custom-build attacks that attempt to evade the specific DDoS defenses of a target, both cloud-based and on premises. We see cybercriminals increasingly target the global connectivity supply chain by attacking vital components of internet operations, such as DNS servers, VPN concentrators, and internet exchanges. Meanwhile, ransomware gangs hit a perfect trifecta with triple extortion attacks that combine data encryption, data theft, and DDoS attacks. Throw in DDoS extortion, and both these types of campaigns continue to wreak havoc around the world. This year, we saw the self-dubbed "Fancy Lazarus" campaign surface, while the adversaries behind the existing Lazarus Bear Armada remain active. Industries such as broadband and wireless communications companies continue to remain top targets, particularly as attacks on online gaming—a perennial top target—affect broadband, wireless, and cable internet companies.

We have long held that vigilance and ongoing adherence to best current practices, when exercised appropriately, serve to protect against a plethora of threats. Starting with and building on these practices will help organizations construct a strong foundation for cybersecurity. But as threat landscape activity continues to move up and to the right, enterprises need to move beyond today's status quo in order to survive. All organizations, regardless of size, industry, or location, need to pick up the baton of security and run the race together to defeat our enemies—cybercriminals.

RICHARD HUMMEL AND CAROL HILDEBRAND, EDITORS

Contributors

Richard Hummel
Carol Hildebrand
Hardik Modi
Roland Dobbins
Steinthor Bjarnson
Chris Conrad
Jon Belanger

Partners

REVERSINGLABS
neustar
GREYNOISE

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.

NETSCOUT

SECR_001_EN-2102 09/2021