



DDoS In a Pandemic

Tony Scheid

Senior Sales Engineer

Agenda

- Key Findings
- Global Attack Trends
- Regional Breakdowns
- BotNet Analysis
- Conclusion
- Questions (and Free Stuff)



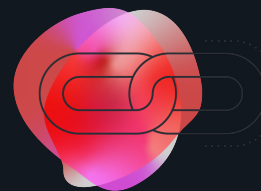
NETSCOUT[®]

Key Findings

Key Findings H1 2021



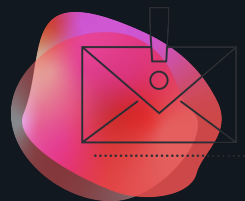
7 Vectors in 7 Months



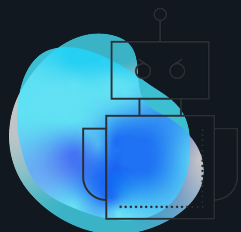
Connectivity Supply Chain Under Attack



Adaptive DDoS Attacks



ISPs Face DDoS Extortion



Botnet Snapshot



Triple Threat: A Ransomware Trifecta



Key Findings H1 2021

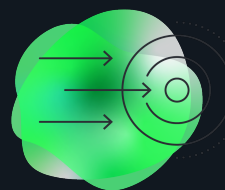


7 Vectors in 7 Months

- Threat Actors weaponize at least 7 new attack vectors based upon abusable Open source and commercial UDP services and Applications
- The number of multi-vector attacks has soared, with one attack against a German organization seeing 31 attack vectors – resulting in greater risk to organizations



Key Findings H1 2021

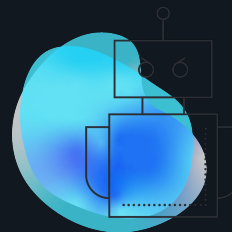


Adaptive DDoS Attacks

- Adversaries develop new techniques to evade traditional defences
- Threat Actors can now customise their Attacks to evade traditional Cloud Based and On Premises defences
- Attackers perform significant reconnaissance prior to launching attacks



Key Findings H1 2021

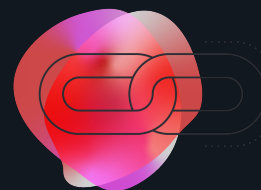


Botnet Snapshot

- Bolstered by previous years of attacks, Botnet propagation increases based upon weaponization of new attack vectors
- Botnets are responsible for ~2.8M DDoS Attacks in H1 2021
- 3 Large BotNets emerged in 2021



Key Findings H1 2021



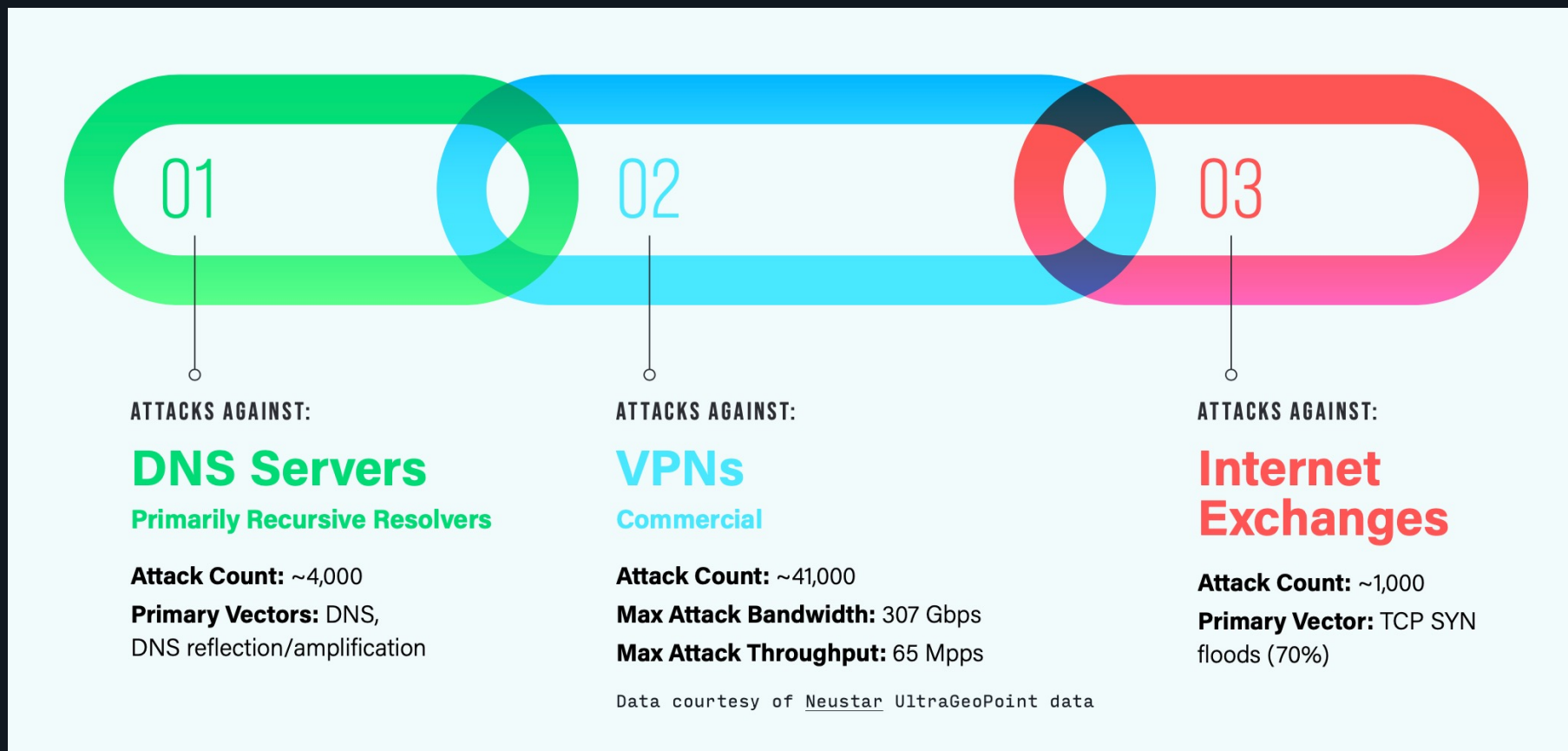
Connectivity Supply Chain Under Attack

- The Global Connectivity Supply Chain is constantly under attack, concentrated attacks against vital infrastructure such as DNS Servers, VPN Concentrators and services as well as Internet Exchanges
- Attacks against vital infrastructure continue to cause collateral damage that affects a huge array of entities on both Wired and Wireless networks beyond the initial target.
 - Think of Netflix, Webex & Zoom
- LBA Often Targeted Corporate VPN Infrastructure to prevent Users accessing Corporate services, or prevent Security Staff from responding to attacks

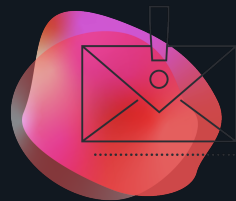


Connectivity Supply Chain Under Attack

DNS Servers, Internet Exchanges, & VPN Concentrators



Key Findings H1 2021



ISPs Face DDoS Extortion

- Threat actors launched the self-dubbed Fancy Lazarus DDoS extortion campaign primarily against authoritative DNS Servers for ISP's
- Lazarus Bear Armada (LBA) DDoS extortion continued to target victims across multiple industries



Key Findings H1 & H2 2021



Triple Threat: A Ransomware Trifecta

- Ransomware gangs added Triple extortion attacks to their offerings
Combining File Encryption, Data Theft and DDoS attacks
- 3 Major Campaigns throughout 2021:
 - Lazarus Bear Amada – Targets multiple Verticals
 - Mostly R/A different vectors
 - Fancy Lazarus – Targets ISP Authoritative DNS
 - Mostly DNS R/A & DNS “Water Torture”
 - Threat Actors masquerading as REvil - Attacks against High Profile VOIP Providers
 - Reported loss of revenue of \$9-\$12M
- Leak Site often used to prove Data Theft

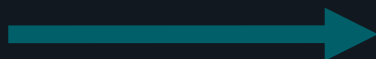


What is Triple Extortion?

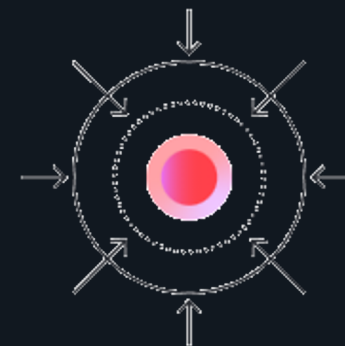
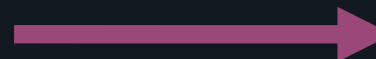
Ransom + Theft + DDoS



Encrypt



Data Theft



DDoS Extortion

Ransomware is big business.

\$100,000,000

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



Key Findings H2 2021



The Triple Threat



The Rise of Server-Class Botnet Armies



Flood of Attacks



DDoS-For-Hire Free-for-All



DDoS As a Homing Missile



The Intersection of Encryption, State, and DDoS Defense

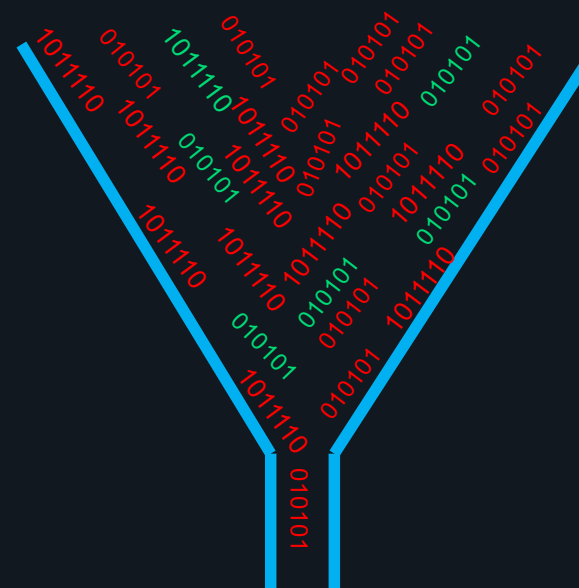


Key Findings H2 2021



Flood of Attacks

- Adversaries bombard organisations with floods of TCP and UDP targeted direct path (non spoofed) attacks
- TCP Based attacks surpassed some Reflection Amplification
- 32% Decrease in DNS Amplification Attacks, which represented 14% decline from H1 2021
- 64% Decrease in CLDAP Based Attacks



Key Findings H2 2021



DDoS As a Homing Missile

- Attackers Zeroed in on a Number of specific industries
 - VOIP Providers (93% increase)
 - Electronic Computer Manufacturing (162% increase)
 - Computer Storage Device Manufacturing (263% increase)
 - Software Publishers (606% increase)
 - Insurance Agencies/Brokers (257% increase)
 - Colleges/Universities/Professional Schools (102% increase)



Key Findings H2 2021



The Rise of Server-Class Botnet Armies



Meris

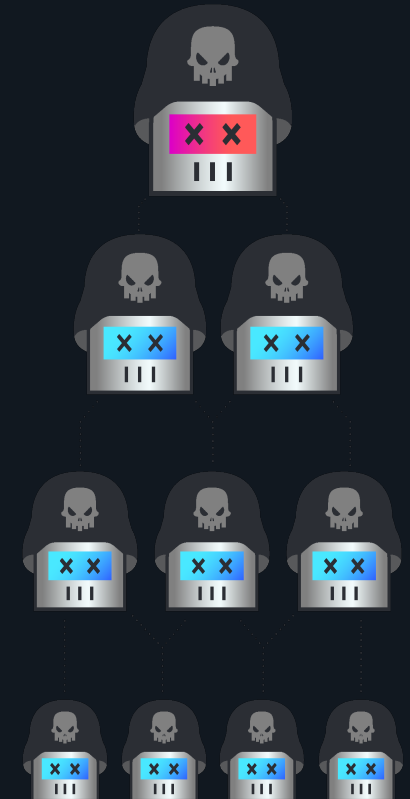
- Compromised MikroTik Routers used to launch application layer attacks with high requests-per-second (RPS).

Dvinis

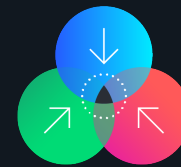
- Secondary botnet using compromised MikroTik routers to similarly launch very high RPS attacks

GitMirai

- Leveraging a Gitlab vulnerability, Mirai enslaved Git servers to participate in a very high-powered server-class botnet.



Key Findings H2 2021



The Intersection of Encryption, State, and DDoS Defense

- High Volume Application Layer Attacks observed
- Attacks launched via the Meris and Dvinis Router Based Botnets
- Attacks up to 17M Requests per Second (Mrps) Reported



Key Findings H2 2021



DDoS-For-Hire Free-for-All

Purchase

PICK YOUR OPTIONS

The maximum duration your attacks will have:
(828) Second(s)

How many stress tests you can have simultaneously:
(5) Concurrent(s)

The duration of your subscription:
(2) Month(s)

API ACCESS

Yes

Price: \$245.94

ORDER

- Custom configurations allow adversaries to heavily tailor their attack to a target of their choosing.
- **FREE** test attacks eliminate the barrier to entry
- Combining the total attack count listed in 19 of hundreds of platforms, adversaries claim to have launched more than **10,000,000 DDoS attacks**, with more than **400,000 registered users**.



Global Attack Trends

Global Statistics H1 2021

5.4M

DDoS ATTACKS IN 1H 2021

Attackers launched a record-breaking number of attacks in 1H 2021, an 11 percent increase year over year.

+106%

MULTIVECTOR ATTACKS

On average, multivector attacks using 20-plus vectors spiked by 106 percent, including a record-breaking 31-vector attack on an organization in Germany.

200K

BOTS DRIVE 2.8M DDoS ATTACKS

Tracking global botnet clusters and density zones shines a light on how malicious adversaries abuse these botnets to launch DDoS attacks.



Global Statistics H2 2021

9.7M

DDoS ATTACKS IN 2021

A 3% decline from 2020, but a 14% increase over 2019

\$9-\$12M

IN POTENTIAL REVENUE LOSS

From DDoS extortion of VoIP providers

Free!

THE BARRIER TO ENTRY FOR DDoS ATTACKS IS NONEXISTENT

The most prominent DDoS-for-hire services provide DDoS attacks ranging from no cost to greater than \$6,500 for terabit-class attacks



Max Counts in 1H 2021

Frequency, Bandwidth, and Throughput

Total: 5,351,930

11% increase in 1H 2021 compared with 1H 2020

Max: 1.5 Tbps

169% increase in 1H 2021 compared with 1H 2020

Max: 675 Mpps

16.17% increase in 1H 2021 compared with 1H 2020



DDoS Global Attack Trends H2 2021

- DNS Amplification (-32%)
- CLDAP Amplification (-64%)

Global Stats: Number of Attacks

4,406,713

14% decrease from 2H 2020

Largest Attack

612 Gbps*

14% increase from 2H 2020

Fastest Attack

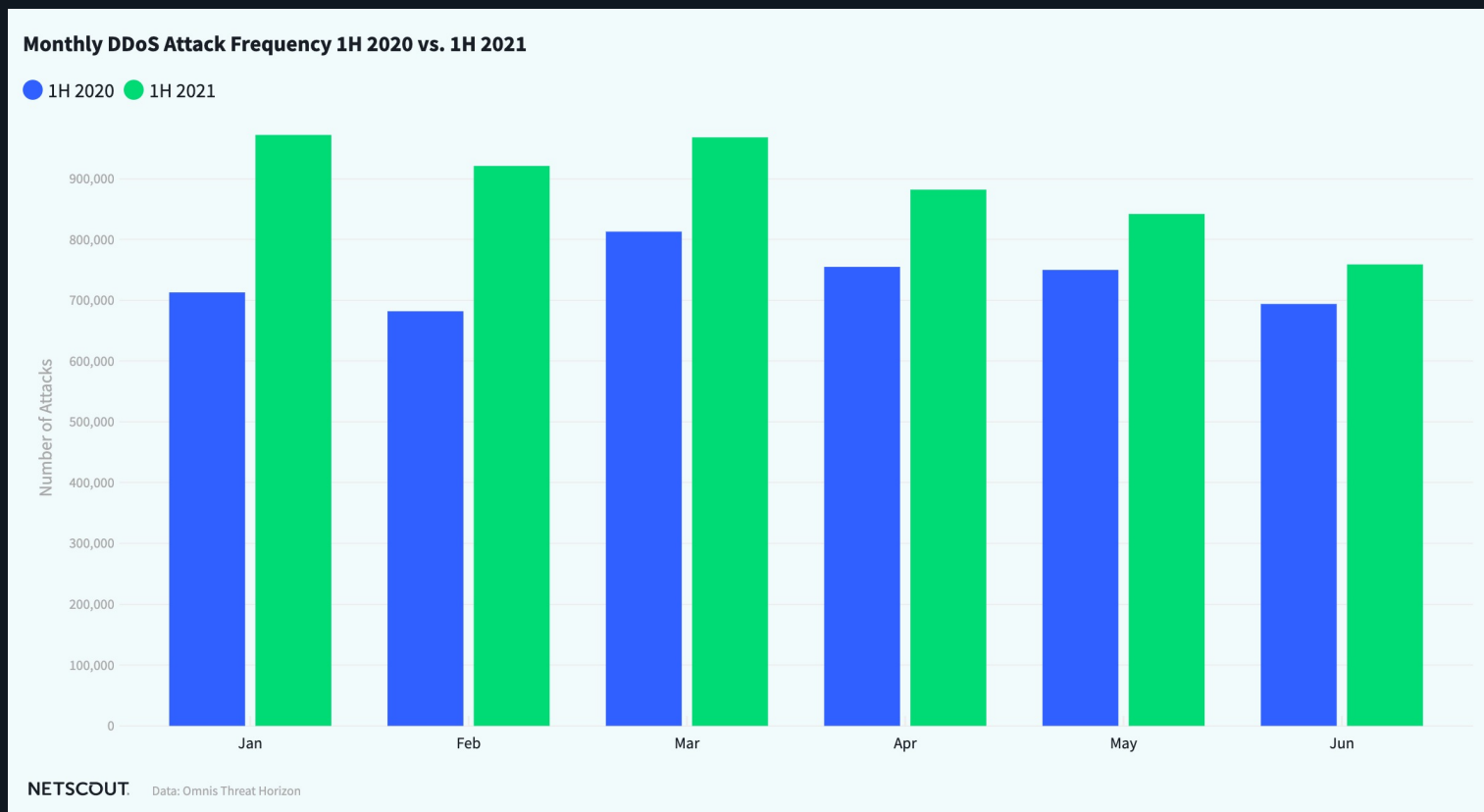
453 Mpps

107% increase from 2H 2020



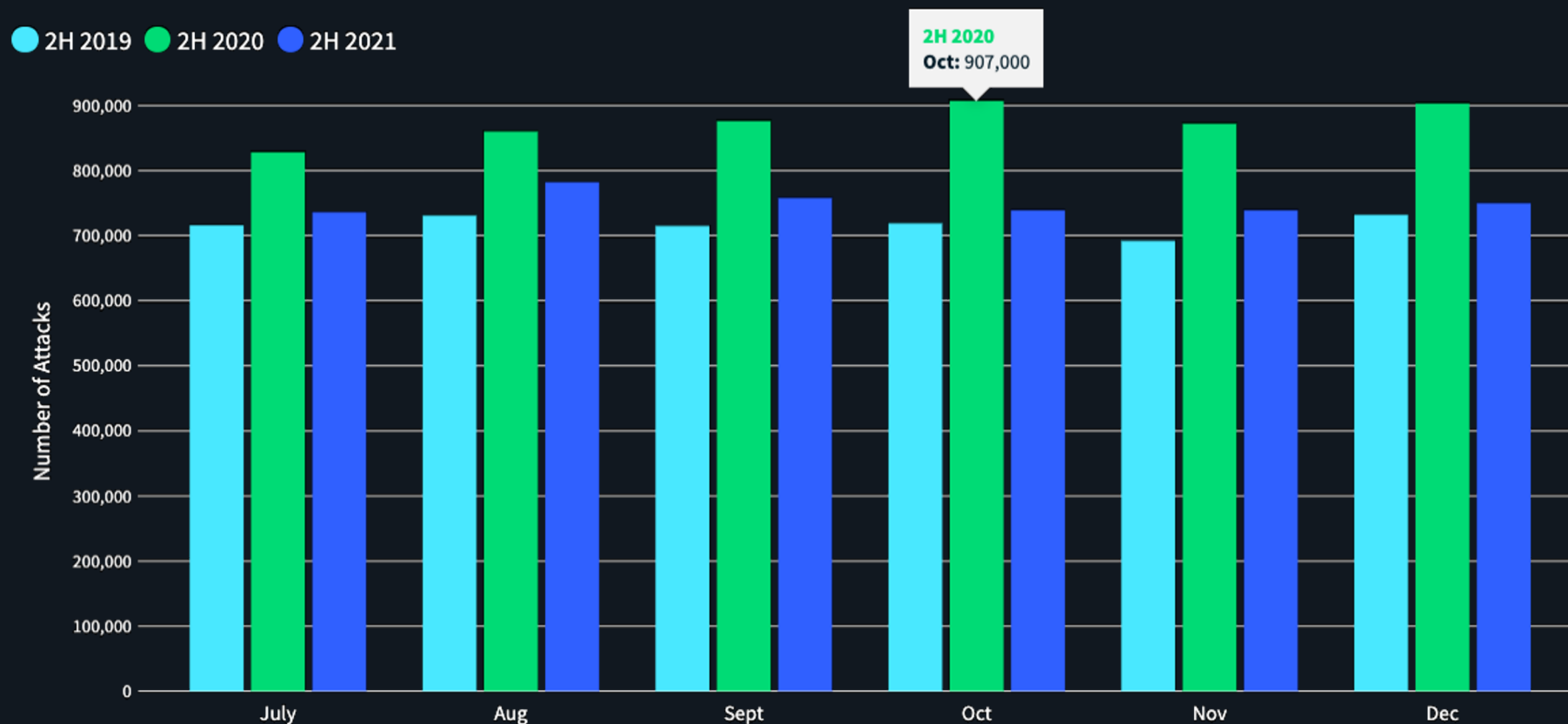
Month over Month Attack Frequency H1

The long tail of COVID-19 continues to influence attacks

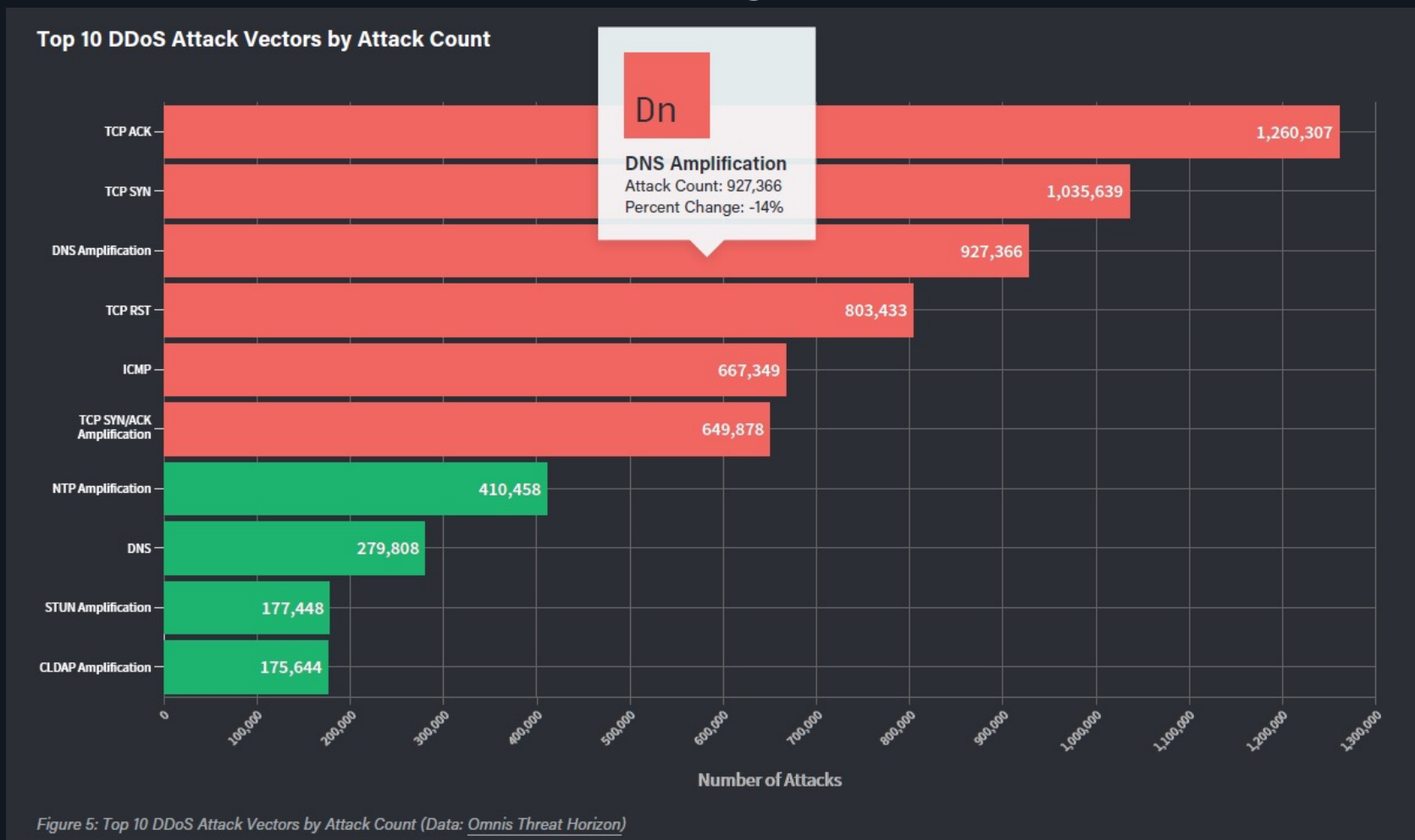


Month over Month Attack Frequency H2

Monthly Attacks from 2H 2019 to 2H 2021



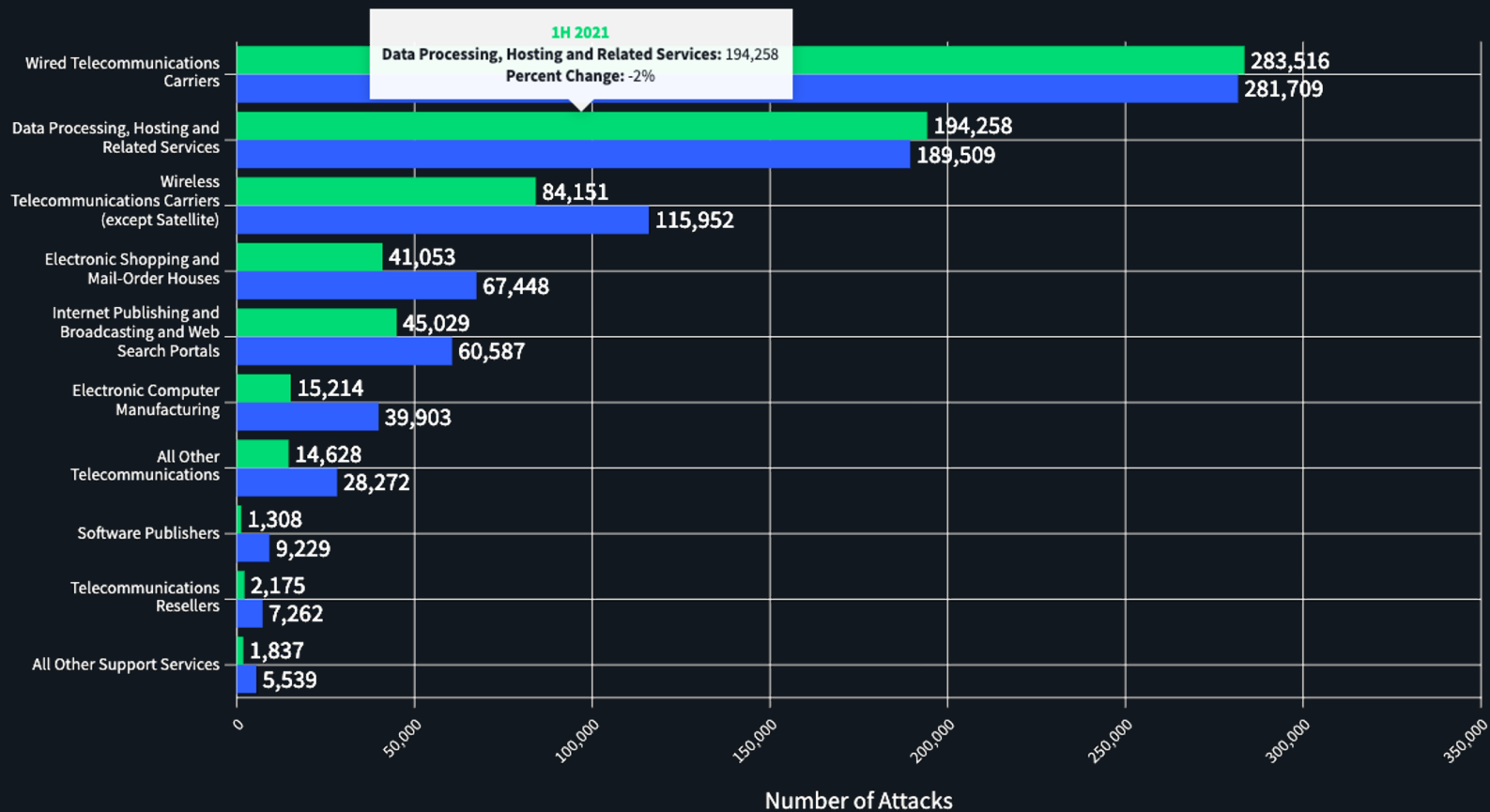
Top 10 Attack Vectors by Attack Count



Industry Spotlights


Top 10 Vertical Industry Targets 1H 2021 vs. 2H 2021

● 1H 2021 ● 2H 2021



Normalization of Terabit-Class Attacks H1 2021

Despite the large bandwidth, these attacks leverage well-understood DDoS attack vectors and often result in little to no impact to the target.

Terabit-Class Attacks					
ATTACK SIZE	LOCATION		MONTH	TARGET	VECTORS USED
1 Tbps		Hong Kong	Late May 2021	Mobile ISP	DNS, DNS reflection/amplification, SSDP reflection/amplification
1.5 Tbps		British Virgin Islands	Late May 2021	Enterprise	DNS, CLDAP reflection/amplification
1.5 Tbps		Germany	Mid June 2021	ISP	DNS, CLDAP reflection/amplification

NETSCOUT Data: Omnis Threat Horizon



Regional DDoS Attack Statistics

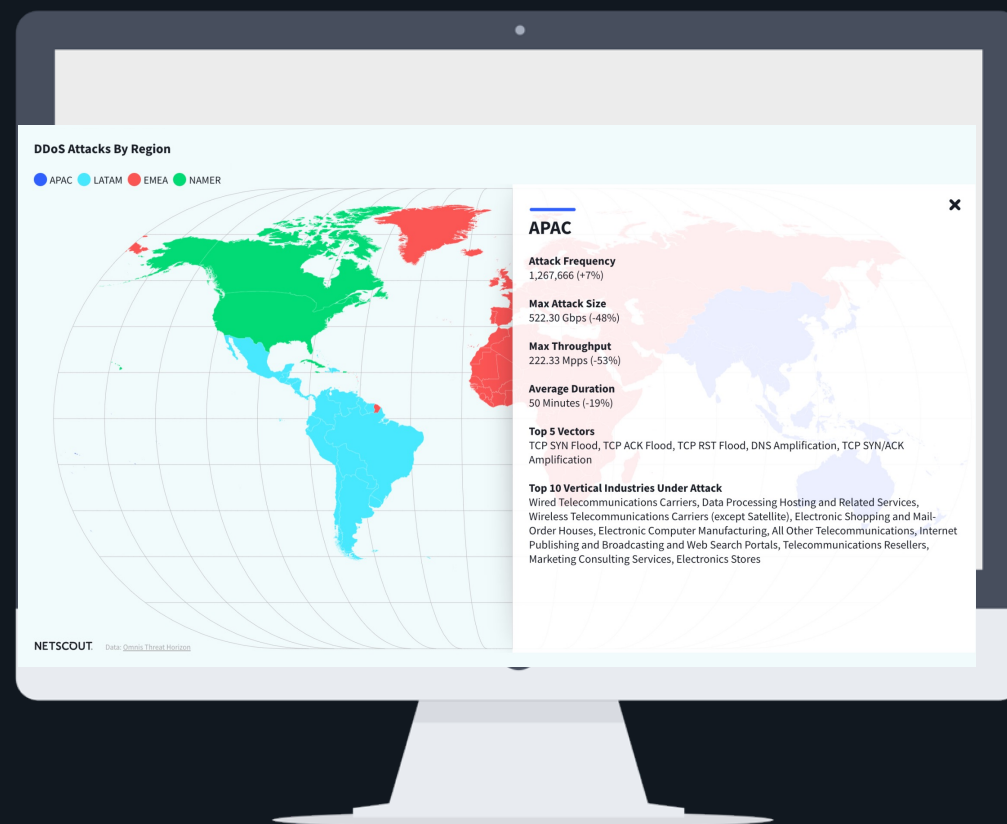
Regional Attack Trends – 1H 2021

- NAMER
 - 1,262,467 Attacks – 10% increase
 - ~630 Gbps Max Bandwidth – 47% increase
- LATAM
 - 555,039 Attacks – 39% increase
 - ~1.3 Tbps Max Bandwidth – 256% increase
 - ~675 Mpps Max Throughput – 479% increase
- EMEA
 - 2,004,044 Attacks – 25% increase
 - ~1.5 Tbps Max Bandwidth – 167% increase
- APAC
 - 1,186,398 Attacks - 2% decrease
 - ~1 Tbps Max Bandwidth – 192% increase



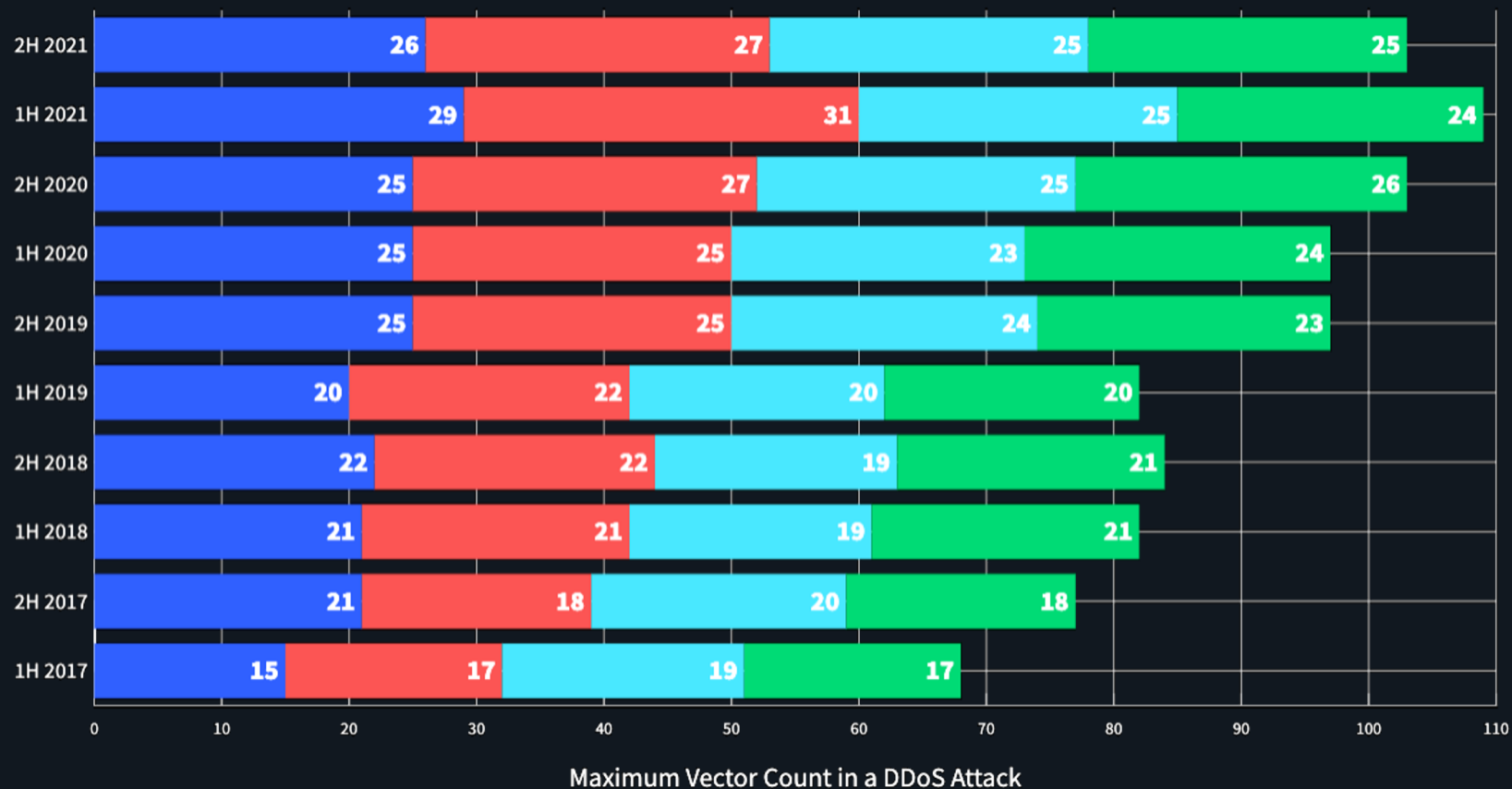
Regional Attack Trends – 2H 2021

- NAMER
 - -24% Frequency
- LATAM
 - -2% Frequency
- EMEA
 - -20% Frequency
- APAC
 - +7% Frequency
 - Likely related to geo-political events



Multi-Vector Attacks by Region

● APAC ● EMEA ● LATAM ● NAMER



BotNet Analysis

Mēris

Botnet Snapshot

First Seen:

June 2021

Current Nodes: ~2,000

Peak Active: ~4,800

Attacks: ~4,000

Max Attack Size: ~337 Gbps

Average Size: ~7 Gbps

- Uses HTTP-Pipelining
- High-powered MikroTik routers
- Launched Notable attacks against websites
- Approximately 17M request-per-second peak



Dvinis

Botnet Snapshot

First Seen:

September 2021

Current Nodes: ~24,000

Peak Active Nodes: ~24,000

Attacks: ~29,000

Max Attack Size: ~463 Gbps

Average Size: ~3 Gbps

- High-powered MikroTik routers
- **585%** Increase in botted nodes since we started tracking



GitMirai

Botnet Snapshot

First Seen:

November 2021

Current Nodes: ~3,800

Peak Active Nodes: ~3,800

Attacks: ~16,000

Max Attack Size: ~694 Gbps

Average Size: ~5.4 Gbps

- Exploits CVE-2021-22205 to compromise GitLab servers
- Incorporated the exploit into a Mirai code branch
- Capable of launching very high throughput attacks



Conclusion

Conclusion – DDoS in a Pandemic

- 2021 – fewer number of attacks compared to 2020 albeit a ~14% growth over 2019
- H2 2021 saw a drop in Attack Numbers compared to H1
 - Relaxation of Covid restrictions / Return to the office ???
- Attackers are leveraging new methodologies (TLS) with High Powered Router and Server Botnets
- Slight Decrease in the use of Reflection Amplification Attacks

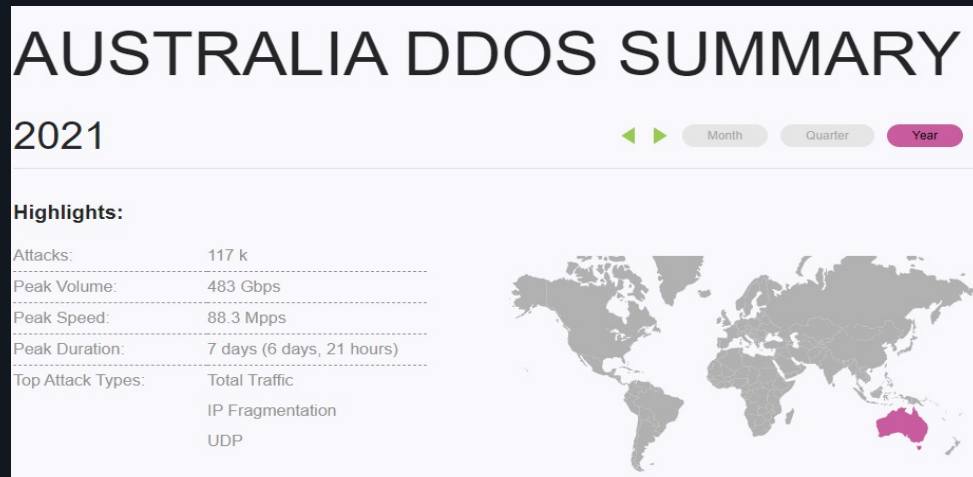


Conclusion – DDoS in a Pandemic

- Statistically attack numbers were lower
- Nothing has Changed Significantly – DDoS is here to stay



Questions (and Free Stuff)



<https://horizon.netscout.com/>



<https://netscout.com/threatreport>

NETSCOUT's ASERT Cybersecurity Blog

Stay up to date with NETSCOUT's ATLAS Security Engineering and Response Team (ASERT) research.

Subscribe to the Blog

<https://netscout.com/asert>

