



JULY 2021

Quarterly DDoS Attack Report

Radware's Quarterly DDoS Attack Report provides an overview of attack activity witnessed during the second quarter of the 2021 calendar year. It analyzes DDoS attack activity by industry, attack vector, DDoS attack on applications, and on-premise vs. cloud.

Contents

- Overview3
- Quarterly Trends4
- Regions and Industries.....6
- Attack Vectors and Applications8
 - Amplification Attack Vectors9
 - Top Attack Vectors: HTTPS10
 - Top Attack Vectors: DNS10
 - Burst Attacks11
- RDoS Campaign12
- Hacktivist Activity13
- Vulnerability Scanning Activity.....14
- Conclusion16
- References.....18
- List of Figures18
- Methodology and Sources19



Overview

The second quarter of 2021 was characterized by renewed DDoS extortion campaigns by an actor posing as “[Fancy Lazarus](#)” [1], a hacktivist group named DragonForce Malaysia [2] targeting financial institutions based in Israel, and a rise in burst attacks on organizations in finance and technology verticals.

The average blocked volume per customer in Q2 increased by 40% compared to the same period in 2020. On average, Radware customers had to detect and block almost 4,900 malicious events and a volume of 2.3TB per month.

The average attack size in Q2 grew by over 10% compared to Q1 of 2021. The number of attacks larger than 10Gbps increased from 2.75 per 1,000 attacks to 3.32 per 1,000 attacks.

Technology, healthcare and finance industries were the most targeted, while the gaming and telecommunications industries observed the largest attack volumes in Q2.

The Americas and EMEA accounted for 80% of the attack volume, and organizations across both regions were attacked by nearly equal volumes.

Most of the attack traffic was directed at HTTP and HTTPS, with DNS, SIP, BGP, RDP and SMTP following in order. The majority of attack traffic was generated by UDP-based protocols, while the fastest attack vectors, in terms of packets per second, were TCP-based assaults.

The most-leveraged amplification attack vectors during Q2 were DNS, CLDAP, NTP and SSDP. HTTPS applications were attacked mostly by TCP-based attack vectors, while DNS services were targeted mostly by DNS Flood attacks, attempting to exhaust server-side resources.

On average, organizations blocked almost 2,000 scan events from 76 different vulnerability scanners. Eighty percent of scan events and 60% of the scanners are assumed to have acted with good intentions.



Quarterly Trends

Compared to Q2 of 2020, the average number of blocked malicious events per customer increased by over 30% to 14,500 events. The average blocked volume per customer increased by over 40% to 6.8TB. This represents a monthly average of 4,850 malicious events and a volume of 2.3TB blocked per customer during Q2 of 2021.

Compared to Q1 of 2021, the average number of events per customer in Q2 increased by 11.5% from 13,000 to 14,500. The average blocked volume per customer decreased by 28% from 8.7TB in Q1 to 6.8TB in Q2, but maintained an average volume above the maximum average of 6.4TB per customer in 2020 (see Figure 3).

FIGURE 1:
Blocked malicious events, normalized per customer

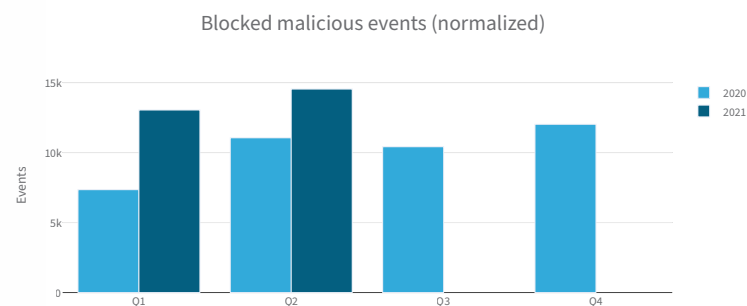


FIGURE 2:
Blocked malicious events, normalized per customer

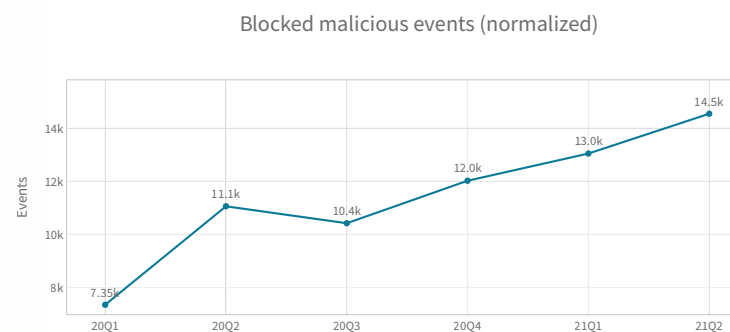


FIGURE 3:
Blocked volume in TB, normalized per customer

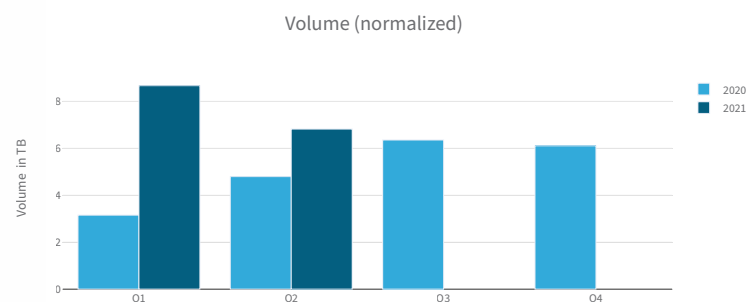
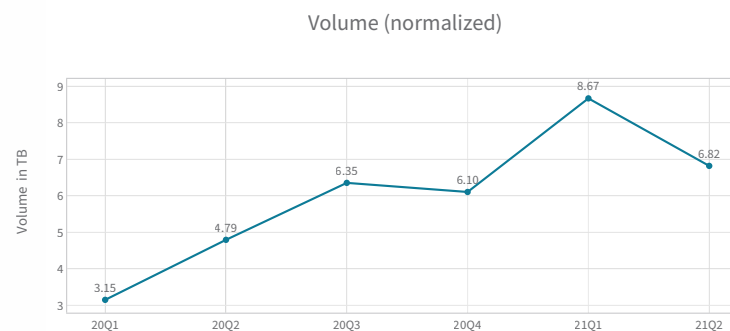


FIGURE 4:
Blocked volume in TB, normalized per customer



The average attack¹ size shows a continued, slightly slower than linear growth of 20% from 120Mbps in Q4 of 2020 to 146Mbps in Q1 of 2021 and a 11% increase to 162Mbps in Q2 of 2021. The maximum attack size shows similar but slightly faster than linear growth from 260Gbps in Q4 of 2020 to 348Gbps in Q2 of 2021.

The relative number of attacks larger than 10Gbps grew from 2.25 per 1,000 attacks in Q1 of 2021 to 3.32 per 1,000 attacks in Q2 of 2021. The number of attacks larger than 1Gbps was down from 10.7 in Q1 of 2021 to 9.22 per 1,000 attacks in Q2 of 2021. The average number of attacks per customer in Q2 of 2021 was 318, down from 382 in Q1 of 2021.

FIGURE 5:
Quarterly
average and
maximum
attack sizes

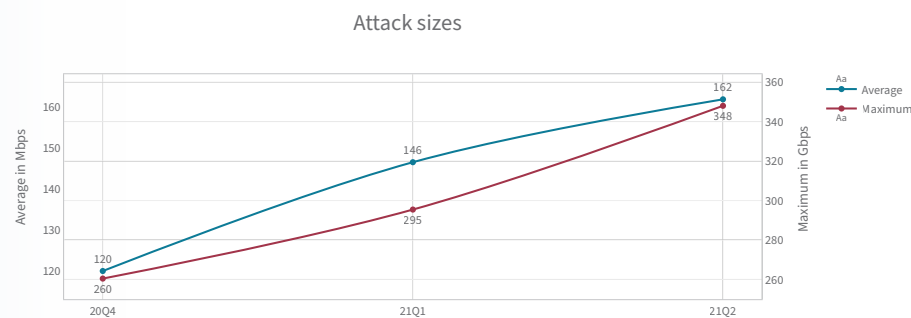


FIGURE 6:
Number of
attacks larger
than 10Gbps,
normalized per
1,000 attacks

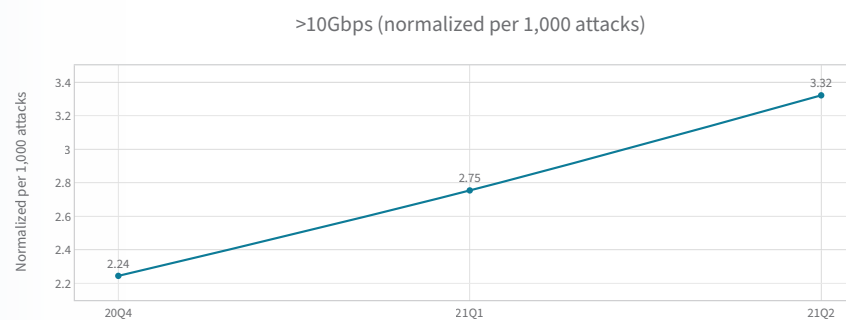


FIGURE 7:
Number of
attacks larger
than 1Gbps,
normalized per
1,000 attacks

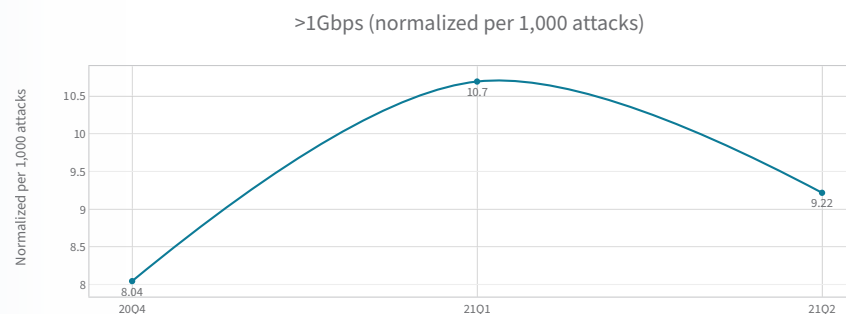
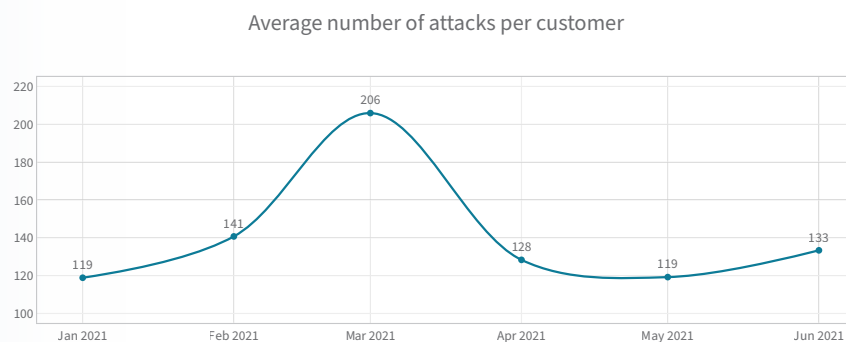


FIGURE 8:
Average number
of attacks per
customer



1. Attacks are groups of one or more malicious events, overlapping in start time and duration, all representing a common, perceived attack on a customer. Attacks consist of one to hundreds of events, depending on the complexity and duration of the attack.

Regions and Industries

The majority of the blocked volume, normalized per customer, shifted between the Americas and EMEA from quarter to quarter, but it averaged out over the first half of 2021 to equal parts of about 40% volume blocked by American and EMEA customers and about 20% of total volume in APAC customers.

FIGURE 9:
*Blocked volume
per region,
normalized per
customer*

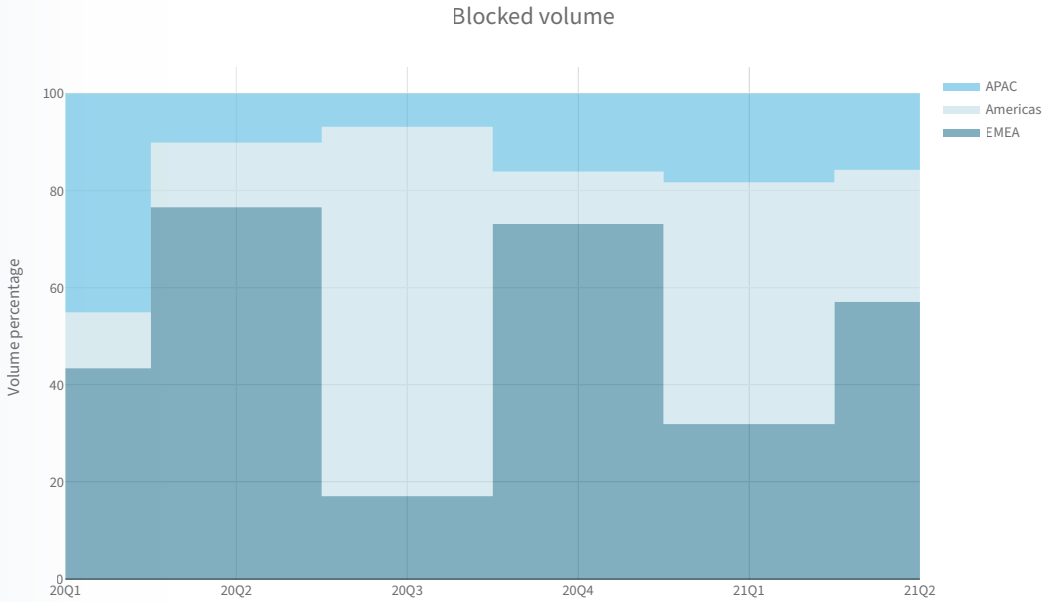
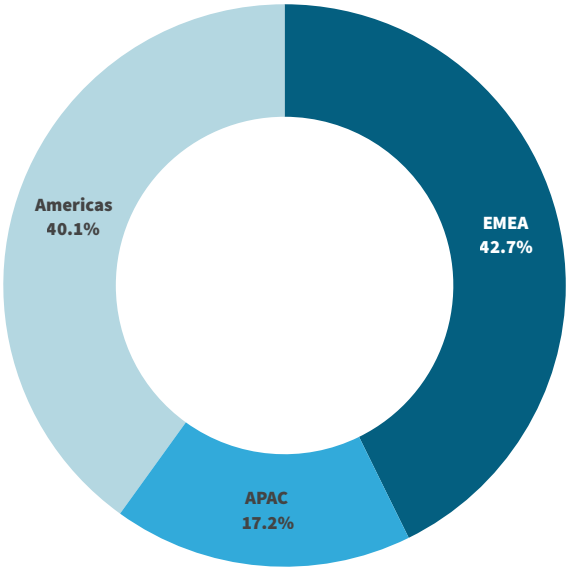


FIGURE 10:
*Blocked volume
per region
for the first
half of 2021,
normalized per
customer*

Blocked volume (normalized) in the first half of 2021



The most attacked industry in Q2 was technology, with an average of almost 3,000 attacks per customer, followed by healthcare, with 2,000 attacks per customer, and finance, with 1,350 attacks per customer. Retail, communications and telecommunications averaged between 500 and 1,000 attacks per customer. Gaming averaged a little over 400 attacks per customer, while an average of about 280 attacks targeted government and utility customers.

In terms of blocked volume, retail had to endure the highest volumes in Q2, with a 33TB average per customer. Radware mitigated 24TB on average per gaming customer, 17TB for telecommunications, 9TB for technology, 6TB for finance and 2TB for government.

FIGURE 11:
Top attacked industries in Q2 of 2021, normalized per customer

Top attacked industries (normalized) in Q2 of 2021

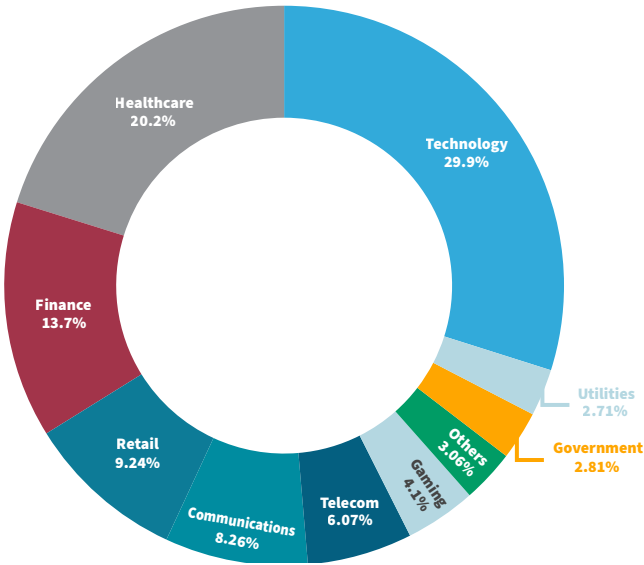
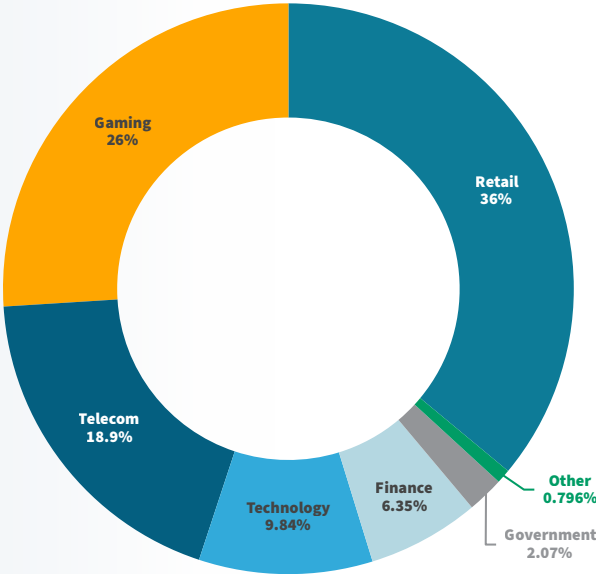
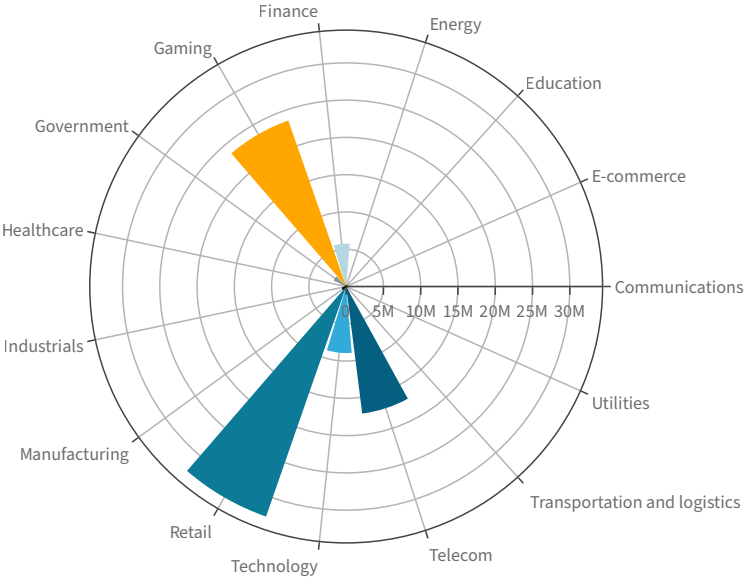


FIGURE 12:
Volume by industry for Q2 of 2021, normalized per customer

Q2 volume by industry



Q2 volume by industry



Attack Vectors and Applications

On average in Q2 of 2021, 70% of the attack volume targeted HTTP (port 80). HTTPS (port 443) and HTTP represented almost 90% of the average attack volume per customer. Other applications that were regularly targeted by large volumes included DNS, SIP, BGP, RDP and SMTP. The objective of volumetric attacks is to saturate the internet links. Even if an organization does not expose HTTP services, volumetric assaults can overrun internet pipes and network equipment.

UDP Fragment and UDP Floods, on average, accounted for over 90% of the attack volume. More specific, UDP amplification vectors such as NTP, SSDP and DNS accounted for a little over 6%. TCP out of state, typically an attack vector with higher packet rates and lower volumes considering the small packet sizes, accounted for almost 1% of the average attack volume per customer.

The fastest attack vector was DNS, with a rate of over 40 million packets per second (MPPS), followed by a SYN Flood attack vector reaching 27MPPS and a SYN-ACK Flood attack vector with a rate of 20MPPS.

FIGURE 13:
Top applications
by volume,
normalized per
customer

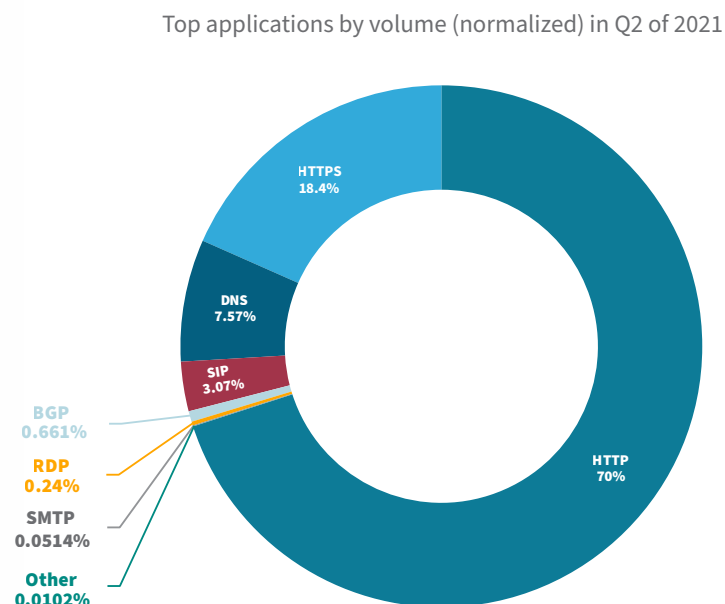
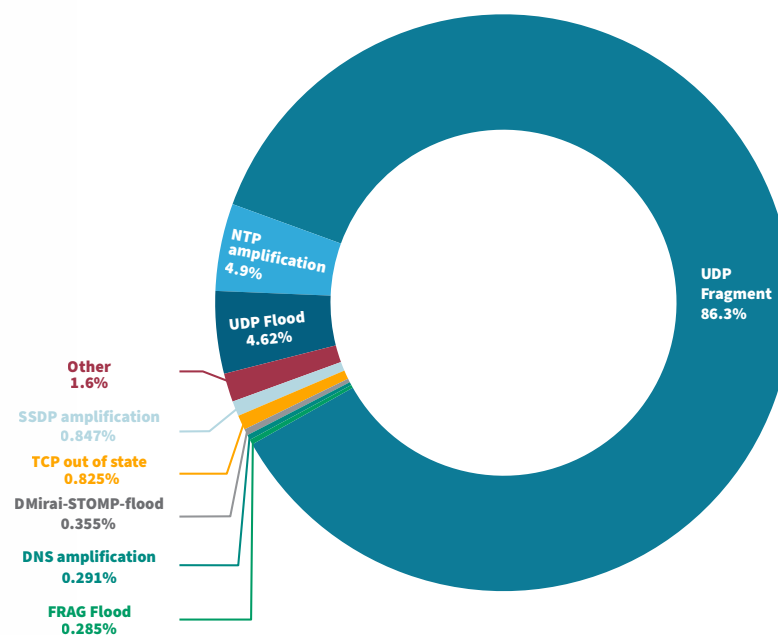


FIGURE 14:
Top attack
vectors by
volume,
normalized per
customer

Top attack vectors by volume (normalized) in Q2 of 2021



UDP is still the most leveraged protocol for DDoS attacks, which is not surprising considering UDP traffic can be easily spoofed and most of the amplification attack vectors are UDP based. TCP-based attacks represented an average of 2.36% of the attack volume per customer, and ICMP represented 0.36%.

AMPLIFICATION ATTACK VECTORS

On average, DNS and CLDAP represented more than half of the amplification attack vectors. NTP and SSDP accounted for a quarter of the amplification attack vectors targeting customers.

FIGURE 15:
Protocols
by volume,
normalized per
customer

Protocols by volume (normalized) in Q2 of 2021

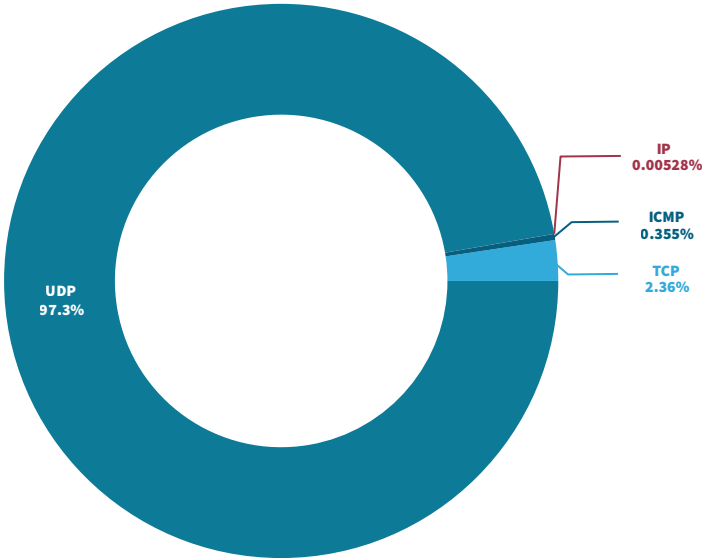
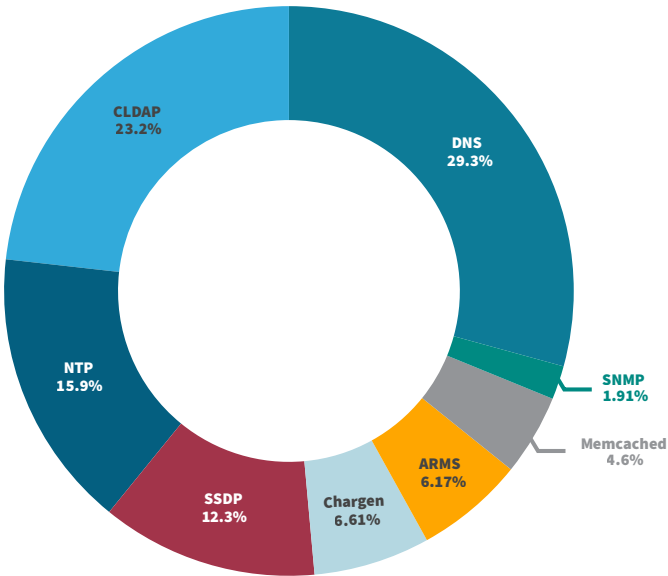


FIGURE 16:
Top
amplification
attacks,
normalized per
customer

Top amplification attacks (normalized) in Q2 of 2021



TOP ATTACK VECTORS: HTTPS

More than half of the packets targeting HTTPS applications were from TCP-based attack vectors (TCP zero seq, SYN Flood, TCP ACK zero, TCP out of state, SYN-ACK and RST Floods). About 20% of the attacks were UDP-based amplification attacks leveraging SSDP, NTP and DNS reflection and amplification services. A few customers observed TLS renegotiation attacks.

TOP ATTACK VECTORS: DNS

The majority of packets targeting DNS servers were DNS Flood attacks. A DNS Flood attack targets the DNS service in an attempt to exhaust server-side resources such as memory or CPU with application-level requests typically generated by malicious programs running on compromised devices that are part of a botnet. UDP Floods are effective at saturating internet connections in volumetric attacks. Nonetheless, only about 2.5% of the packets observed on average per customer during DNS server attacks are UDP Floods.

FIGURE 17:
Top HTTPS
attack vectors,
by packets and
normalized per
customer

Top HTTPS Floods (packets, normalized) in Q2 of 2021

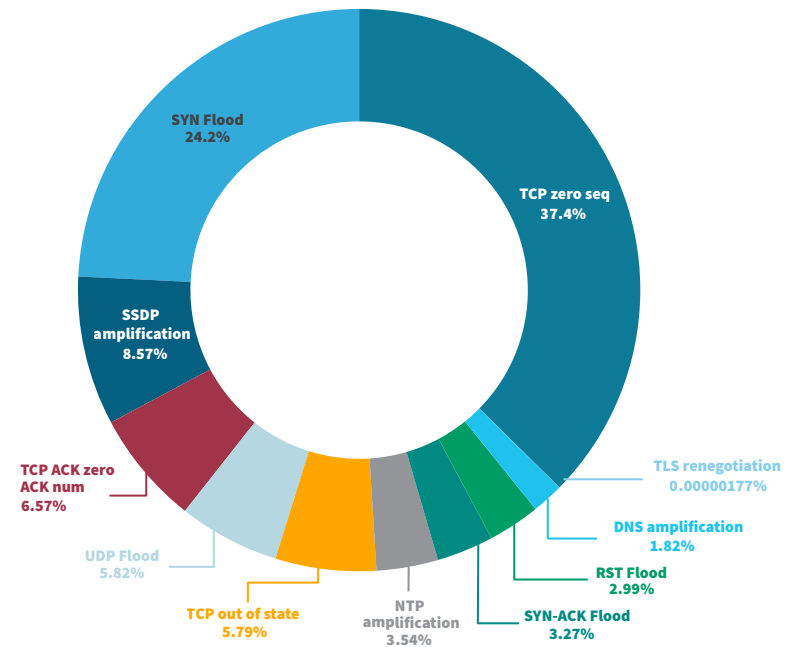
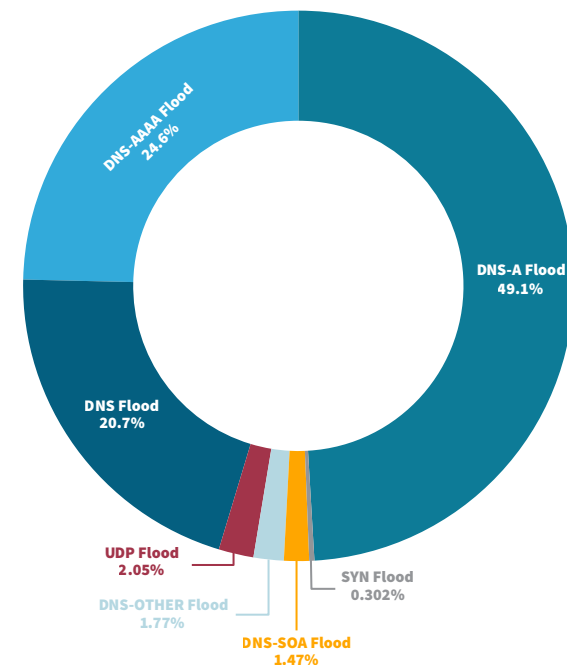


FIGURE 18:
Top DNS attack
vectors, by
packets and
normalized per
customer

Top DNS Floods (packets, normalized) in Q2 of 2021

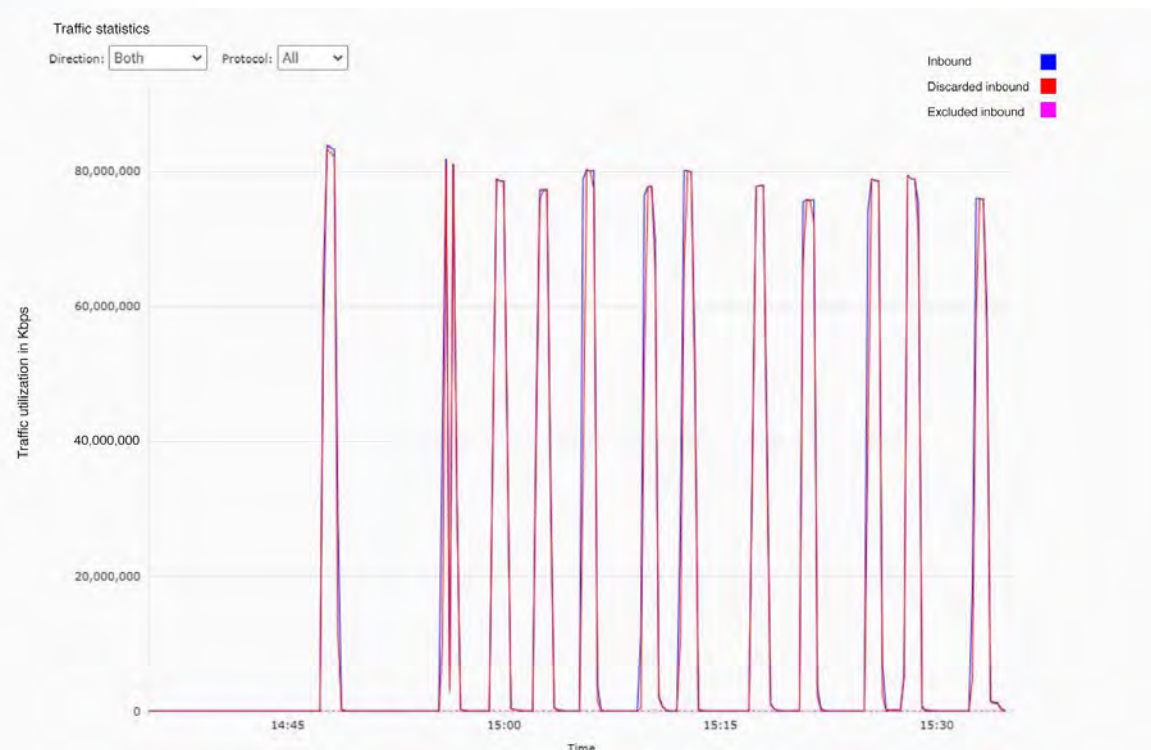


BURST ATTACKS

Common DDoS attacks come in the form of sustained, high-volume traffic floods that ramp up gradually, reach a peak, and are followed by either a slow or a sudden descent. In recent years, a new attack pattern has emerged. Burst attacks, also known as hit-and-run DDoS assaults, use repeated short bursts of high-volume attacks.

Throughout Q2 of 2021, Radware observed several burst attacks targeting customers in the finance and technology industries. These attacks were particularly aggressive in their amplitude (attack size) and frequency (number of bursts per unit of time). One sample of such an attack, included here, showed multiple, consistent 80Gbps bursts lasting two to three minutes, repeating every four minutes. This resulted in 12 attack bursts of 80Gbps within a 45-minute time frame.

FIGURE 19:
*Burst attack
against a
technology
organization
in APAC*



RDoS Campaign

Ransom denial of service (RDoS) attacks – where the victim receives a letter with a demand to pay a ransom or else become the target of a DDoS attack – have been a persistent component of the DDoS threat landscape since August of 2020. Most recently [\[1\]](#), an actor posing as “Fancy Lazarus” has demanded a payout between 0.5 and 5 bitcoins to prevent a DDoS attack against a victim’s critical assets. In early May, several internet service providers (ISPs) in Scandinavia, Western Europe and Ireland reported receiving ransom letters followed by DDoS attacks. By the end of May, Radware had numerous emergency onboardings of its cloud security services from organizations that had received these ransom letters. Most of the onboardings were new customers, while others were existing customers seeking to protect new assets. Radware did not witness “Fancy Lazarus” campaign attacks that approached their claim of 2Tbps attack power, but it has observed multivector attacks of up to 120Gbps, lasting up to 2.5 hours. The threat actor targeted only assets protected by cloud protection services leveraging hybrid or on-demand deployment models. Emergency onboarded targets leveraging always-on cloud protection deployment models did not receive follow-up attacks that could be correlated to the self-proclaimed “Fancy Lazarus” actor. Based on this analysis, Radware believes that the threat actor leveraged BGP to check for cloud protections in their targets before attempting the DDoS attacks.

FIGURE 20:
Example letter
received by a
victim of an
RDoS campaign

We are the Fancy Lazarus and we have chosen [REDACTED] as target for our next DDoS attack.

Please perform a google search to have a look at some of our previous work. Also, perform a search for "NZX DDoS" or "New Zealand Stock Exchange DDoS" in the news. You don't want to be like them, do you?

work will be subject to a DDoS attack starting in 7 days on Thursday next week. (This is not a hoax, and to prove it right now we will start a small attack on a few random IPs from your AS [REDACTED] block that will last for about 2 hours. It will not be a heavy attack, and will not cause you any damage, so don't worry at this moment. We are attacking you with 10 out of 117 of our servers, so do the math.) There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers who use online services. And worst of all you will lose Internet access in your offices too.

We will refrain from attacking your network for a small fee. The current fee is 5 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay the attack will start and the fee to stop will increase to 1 BTC and will increase by 0.5 Bitcoin for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: [REDACTED]

Once you have paid we will automatically get informed that it was your payment.

Please note that you have to make payment before the deadline or the attack WILL start!

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

Once you have paid we won't start the attack and you will never hear from us again.

Please note we will respect your privacy and reputation, so no one will find out that you have complied.

Hacktivist Activity

OpsBedil [2] is a hacktivist operation that targets a number of verticals and government agencies throughout the Middle East. It is the latest digital campaign to target the region and is being conducted by threat actors in Southeast Asia, specifically Malaysia and Indonesia. The attacks performed under OpsBedil are considered a political response to Israel's ambassador to Singapore stating in June that Israel is ready to work towards establishing ties with Southeast Asia's Muslim-majority nations. Malaysia, which is over 60% Muslim and supports Palestine, has a significant presence of hacktivist and Palestinian militants. As a result of this call to establish ties, hacktivists in the region began targeting Israeli assets in mid-June with a series of denial-of-service attacks, data leaks and defacement campaigns. The group condemns the proposal to establish ties and reiterates their ongoing support of Palestine with digital attacks.

The driving force behind OpsBedil is DragonForce Malaysia (DFM) [2], a pro-Palestinian hacktivist group located in Malaysia. DFM has also been observed working in collaboration with a number of other hacktivist groups including T3S and SBC x PANOC. DFM has their own website and forum where threat actors conduct the majority of their operational discussions. DFM also has a Telegram channel, but most of the content is repeated throughout the forum and other social media outlets. In addition to leaking content in their Telegram channel, the group posts details on Pastebin, AnonFiles and Google Drive.

FIGURE 21:
OpsBedil
advertisement



FIGURE 22:
DragonForce
Malaysia logo



Vulnerability Scanning Activity

In March, Radware issued a [threat advisory \[3\]](#) about the ProxyLogon zero-day exploits in Microsoft Exchange Server. In June, Radware published another [threat advisory \[4\]](#) about actors actively scanning for critical remote command execution (RCE) vulnerabilities in VMWare vCenter servers. In both advisories, Radware observed scanning activity in an attempt to discover exposed and vulnerable servers only a few hours after a proof of concept for the vulnerability was published. The window between public disclosure and active exploitation of vulnerabilities is shrinking fast, leaving organizations with little time to update or patch their systems.

Scanning is not limited to malicious actors. Many researchers and cyberthreat intelligence organizations continuously scan the whole internet to discover vulnerable servers to assess the risk associated with new vulnerabilities. Organizations such as Shodan, Censys and ZoomEye have turned their scanning activities into a service that allows anyone with, or even without, a subscription to query specific IPs for open ports, services and vulnerabilities or find a list of exposed servers with particular vulnerabilities.

FIGURE 23:
Scan activity,
normalized
in events per
customer

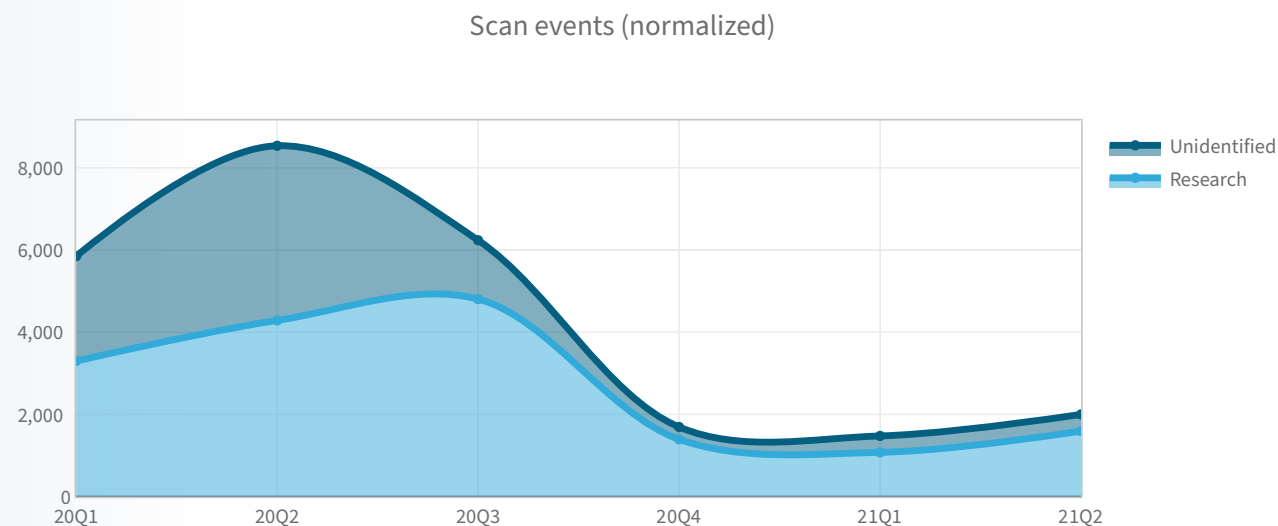
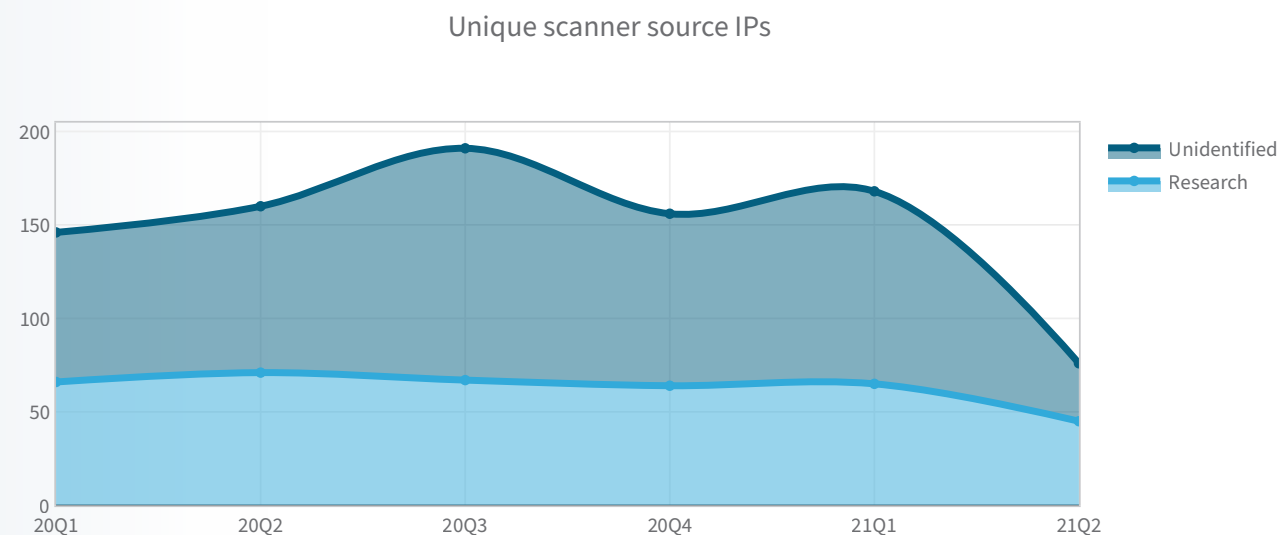


FIGURE 24:
Unique scan
sources



Vulnerability Scanning Activity (cont.)

While it can be useful for organizations to perform periodic assessments of their exposed attack surface, most prefer to keep scanners at bay and block any probes for known vulnerabilities or DDoS reflection and amplification vectors.

Based on information from our managed on-premise and cloud services, we were able to identify scanning activity directed towards customer production servers. Those scans that had good intentions and were originating from security researchers and indexing organizations that disclosed their activities were labeled as good. A portion of the scanning activity was undisclosed and was labeled as unidentified, as we do not have the information to determine the intention of the scanners.


Well-intended and disclosed scans can be identified through a DNS reverse lookup on the source IP of the scanner. If the IP has a PTR DNS record, the domain part of the hostname of the scanning server will reveal the origin of the scan.

In Q2 of 2020, scanning activity reached as high as 8,500 events per customer, of which 4,300 were identified as benign and performed by a disclosed and identified security research party. The highest number of unique scanners recorded since January of 2020 is 191. Of the 191 scanners, 67 were research scanners.

In Q2 of 2021, customers, on average, blocked almost 2,000 scan events from 76 different scanners. Eighty percent of the scan events and 60% of the scanners are assumed to have acted with good intentions. Note that this activity was observed targeting production servers; these are not honeypots designed to trick or trap vulnerability scans and exploits.

Conclusion

What an average customer witnessed per month in Q2:

4,850
Malicious events  **11.5%** compared to Q1 of 2021

2.3TB
Volume blocked  **28%** compared to Q1 of 2021

33TB on average for retail customers
24TB on average for gaming customers
18TB on average for telecom customers
9TB on average for technology customers
6TB on average for finance customers
2TB on average for government customers
<1TB on average for healthcare customers
<1TB on average for communications customers
<1TB on average for utilities customers

320
Attacks { **162Mbps** average attack size { **3** attacks >1Gbps
1 attacks >10Gbps

3,000 attacks on average for technology customers
2,000 attacks on average for healthcare customers
1,350 attacks on average for finance customers
1,000 attacks on average for retail customers
800 attacks on average for communications customers
600 attacks on average for telecom customers
400 attacks on average for gaming customers
280 attacks on average for government customers
270 times on average for utilities customers

2,000
Vulnerability
scanners blocked { **76** unique scanners
60% with good intentions

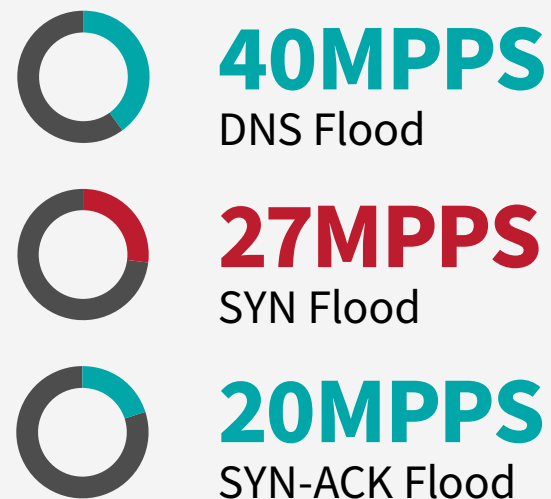
2. The probability of an attack being larger than 1Gbps was 9.22 per 1,000 in Q2, resulting in an average of $318 \times 9.22 / 1,000 = 2.932$ attacks.

3. The probability of an attack being larger than 10Gbps was 3.32 per 1,000 in Q2, resulting in an average of $318 \times 3.32 / 1,000 = 1.0558$ attacks.

The three fastest attack vectors for the quarter were:

The most leveraged amplification attack vectors were DNS, CLDAP, NTP and SSDP. HTTPS applications were attacked mostly by TCP-based attack vectors, and DNS services were primarily targeted by DNS Flood attacks, attempting to exhaust server-side resources. Radware observed several burst attacks targeting customers in the finance and technology industries. The bursts were particularly aggressive in their amplitude (attack size) and frequency (number of bursts per unit of time).

DDoS extortions have been a persistent part of the DDoS threat businesses face in all verticals since August of 2020, and Q2 of 2021 was no different, with new campaigns targeting particularly unprotected assets.



References

- [1] Radware, "Ransom DDoS Update: The Hunt For Unprotected Assets," June 11, 2021. [Online]. Available: www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/ransom-ddos-update-hunt-for-unprotected-assets.
- [2] Radware, "DragonForce Malaysia – #OpsBedil," July 13, 2021. [Online]. Available: www.radware.com/security/ddos-threats-attacks/dragonforce-malaysia-opsbedil.
- [3] Radware, "ProxyLogon: Zero-Day Exploits In Microsoft Exchange Server," March 16, 2021. [Online]. Available: www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/proxy-logon.
- [4] Radware, "Mass Scanning For VMWare vCenter RCE," June 7, 2021. [Online]. Available: www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/mass-scanning-vmware-vcenter-rce.

List of Figures

Figure 1: Blocked malicious events, normalized per customer	4	Figure 13: Top applications by volume, normalized per customer	8
Figure 2: Blocked malicious events, normalized per customer	4	Figure 14: Top attack vectors by volume, normalized per customer	8
Figure 3: Blocked volume in TB, normalized per customer	4	Figure 15: Protocols by volume, normalized per customer	9
Figure 4: Blocked volume in TB, normalized per customer	4	Figure 16: Top amplification attacks, normalized per customer	9
Figure 5: Quarterly average and maximum attack sizes	5	Figure 17: Top HTTPS attack vectors, by packets and normalized per customer	10
Figure 6: Number of attacks larger than 10Gbps, normalized per 1,000 attacks	5	Figure 18: Top DNS attack vectors, by packets and normalized per customer	10
Figure 7: Number of attacks larger than 1Gbps, normalized per 1,000 attacks	5	Figure 19: Burst attack against a technology organization in APAC	11
Figure 8: Average number of attacks per customer	5	Figure 20: Example letter received by a victim of a RDoS campaign	12
Figure 9: Blocked volume per region, normalized per customer	6	Figure 21: OpsBedil advertisement	13
Figure 10: Blocked volume per region for the first half of 2021, normalized per customer	6	Figure 22: DragonForce Malaysia logo	13
Figure 11: Top attacked industries in Q2 of 2021, normalized per customer	7	Figure 23: Scan activity, normalized in events per customer	14
Figure 12: Volume by industry for Q2 of 2021, normalized per customer	7	Figure 24: Unique scan sources	14

Methodology and Sources

The data for this report was collected from a sampled set of Radware devices deployed in Radware cloud scrubbing centers and on-premise managed devices in Radware hybrid and peak protection services.

ABOUT RADWARE

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our Security Research Center that provides a comprehensive analysis of DDoS attack tools, trends and threats. This document is provided for information purposes only.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services or processes described herein are subject to change without notice.

© 2021 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this report are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see www.radware.com/LegalNotice. All other trademarks and names are the property of their respective owners.