2022 H1 Global Threat Analysis Report

Radware's first half of 2022 threat report reviews the most important cybersecurity events, and provides detailed insights into the attack activities for the first six months of 2022. The report leverages intelligence provided by Radware's Threat Intelligence Team, network and application-attack activity sourced from Radware's Cloud and Managed Services, Radware's Global Deception Network, and Radware's Threat Research team.

Contents

Executive Summary

The invasion of Ukraine by Russia marked the first half of 2022 and had a significant impact on cybercrime and underground hacking, with many Russian-speaking threat actors residing in both sides of the war. Patriotic hacktivism increased dramatically, while influencers inside and outside the country enticed hacktivists and vigilantes in the Western world to support their efforts. Both established and new cyber legions, took up arms in support of two factions at war, as proxies in a conflict that could go down as the first cyberwar.

Both pro-Ukrainian and pro-Russian legions aimed to disrupt and create chaos by stealing and leaking information, defacements, and Denial-of-Service (DoS) attacks. Pro-Russian attackers aimed at every organization, or government that demonstrated support for Ukraine or put sanctions against Russians. The Western world was focused mostly on Russian targets, broadly ranging from government organizations and media outlets, to local food delivery and pharmacies. No organization in the world was safe from retaliation at the time of publication. Online vigilantes and hacktivists could disrupt wider security efforts driven by nations and authorities, and introduce extreme unpredictability for intelligence services with a potential for spillover and wrongful attribution that could eventually lead to an escalation of the cyber conflict.

Being occupied in all the events and media attention stemming from the Russo-Ukrainian conflict, one could forget that there is activity also outside the war realm. The war did shift the focus and priorities of nations and some crime groups alike, but others went on with their business as usual. The first half of 2022 saw several DoS attacks, led by groups of hacktivist across the globe, and its fair share of Ransom Denial-of-Service (RDoS) attacks led by actors claiming to be Phantom Squad and REvil.

No organization in the world was safe from retaliation at the time of publication. Online vigilantes and hacktivists could disrupt wider security efforts driven by nations and authorities, and introduce extreme unpredictability for intelligence services

DDoS Attacks

In the first six months of 2022, the number of malicious events mitigated per customer grew by 203% compared to the first six months of 2021, and by 239% when compared to the last six months of 2021. Radware mitigated 60% more malicious events in the first six months of 2022, compared to the entire year of 2021. The number of blocked events per customer almost doubled each quarter in 2022.

The average number of events blocked per month for a customer was almost 1.5 times higher in the first half of 2022, compared to 2021 and 2020. The average volume blocked per customer, per month in 2022, was 3.39TB, an increase of 47% compared to 2021.

In May 2022, a global cloud service provider in the U.S. was attacked for a duration of 36 hours with a volumetric carpet bombing attack, which was peaking almost 1.5Tbps, sustaining 700+ Gbps attack rate for over eight hours, sweeping almost the whole subnet range and leveraging random destination ports. The attack represented a total volume of 2.9PB, which corresponds to

1.5 times all the information contained in all U.S. academic research libraries. Most of the attack traffic was UDP reflection and amplification.

The second quarter of 2022, was dominated by the enormous attack on a U.S. cloud service provider. In Q1, Americas and EMEA were the most attacked regions; the research and education, telecom, and healthcare repelling the most significant volumes. Media and communications fended off most of the attack attempts, followed by healthcare, technology, and finance.

Overall, Radware observed a decline in larger attack vectors in favor of smaller ones, thereby continuing a key attack trend from 2021. Larger attacks are less frequent, but they hit harder and longer when they struck. The attack vectors leveraged for volumetric and application-level attacks were similar to those leveraged in 2021.

The largest attack, mitigated in the first six months of 2022, was 1.46Tbps, and the most complex attack consisted of 38 dissimilar attack vectors.

DDoS Attack Trend Highlights

The number of malicious DDoS events per customer grew by

203%

2X

The number of blocked events per customer **nearly doubled** each quarter in 2022

The average volume blocked per customer, per month, in 2022 was

3.39TB

Log4Shell Activity

According to a report published on April 26, 2022, more than four months after the Log4Shell critical vulnerability was disclosed, there were still over 90,000 vulnerable internet-facing applications and more than 68,000 servers which were publicly exposed. The activity slowed down between February and May, but as of mid-May the activity seemed to regain importance again. Between the day of disclosure of the vulnerability and June 30, 2020, Radware cloud services had blocked over 6 million exploits.

Web Application Attacks

The number of blocked malicious web application transactions in the first half of 2022 grew by 38% compared to the first half of 2021, and surpassed the total number of malicious transactions recorded in 2020.

The most important security violation was predictable resource location attacks, which accounted for almost half of all attacks witnessed in the first half of 2022. Code injection and SQL injection were in the second and third place. These three attacks combined, were responsible for almost 75% of the total attack activity on web applications and APIs.

The most attacked industries in the first half of 2022 were retail, wholesale trade, and high tech, acccounting for over 50% of blocked web application attacks.

The top 3 security violations in the first half of 2022 were:
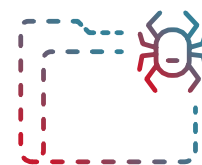
Predictable Resource Location Attacks

Code Injections

SQL Injections

Unsolicited Network Scanning and Attack Activity

The total number of unsolicited events observed by the deception network in the first half of 2022, increased by 30% compared to the number of unsolicited events registered in the last half of 2021. Almost 4.4 billion events were recorded in the first six months of 2022.

The top 10 most scanned and attacked TCP services were SSH, RDP, Redis, HTTPS, HTTP on port 80, HTTP on port 8088, Telnet, VNC, SMB and VNC-1 on port 5901. Compared to 2021, Redis scans and attacks increased significantly while VNC-1 joined the top 10 in favor of SMTP.

SIP (port 5060) was the most targeted UDP-based service in the first half of 2022 (similar to 2021). NTP, Memcached, SNMP, SSDP/UPnP, LDAP, and mDNS were the most scanned services. These protocols were also typically leveraged for DDoS amplification attacks.

CoAP, a specialized web transfer protocol (web API) for use with constrained nodes and constrained networks in the Internet of Things, entered the top 10 most scanned UDP ports for the first time.

The top usernames used during SSH account takeover attempts demonstrated that Postgres, Oracle, Git, and MySQL were the most frequently abused and sought-after credentials during the first half of 2022.

30%

The total number of unsolicited events observed by Radware in the first half of 2022 **increased by 30%** compared to the last half of 2021

Denial-Of-Service Attack Activity

In the first six months of 2022, the number of malicious events per customer, mitigated by Radware's Cloud DDoS Service, grew by 203% compared to the first six months of 2021, and by 239% compared to the last six months of 2021. The first six months of 2022 saw 60% more malicious events, compared to the whole year of 2021.

In 2022, on an average, the service blocked 12,057 malicious events per customer, per month. In 2021, this number was 4,893, and in 2020, 4,583 malicious events were blocked per customer, per month.

In comparison to years 2021 and 2020, the average number of events blocked per month for a customer was almost 1.5 times higher in the first half of 2022.

The average volume blocked per customer, per month in 2022 was 3.39TB; in 2021 it was 2.30TB, and in 2020 it was 2.34TB. This represented a 47% increase in the first half of 2022, compared to the first six months of 2021.
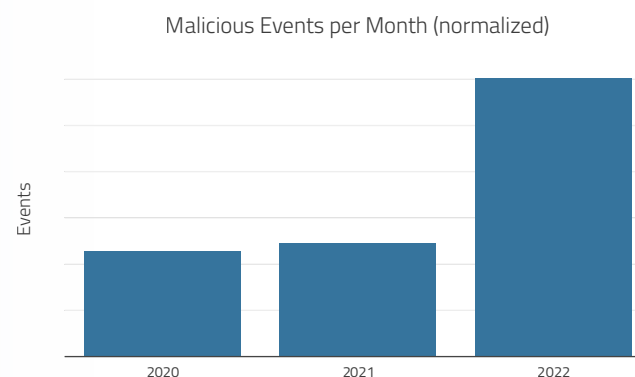
Figure 1

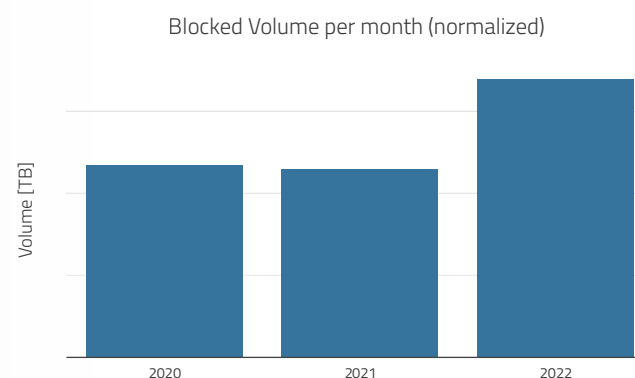Total Malicious Events Blocked per Year by Radware Cloud DDoS Service
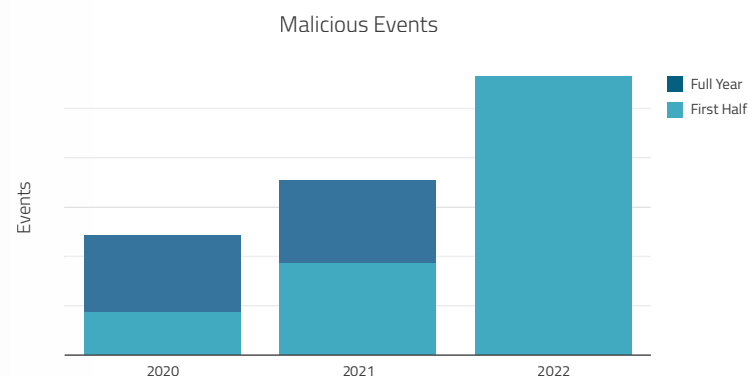
Figure 2

Average Number of Events Blocked per Customer, per Month

Figure 3

Average Volume Blocked per Customer, per Month

Malicious Events

Legend: Full Year, First Half

Malicious Events per Month (normalized)

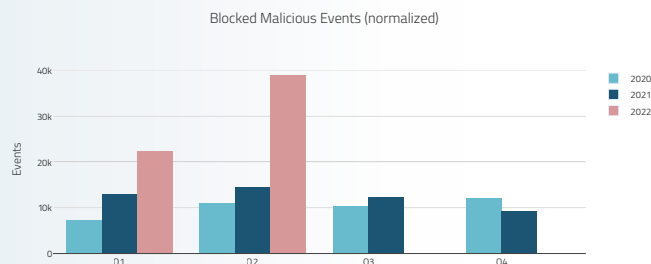Blocked Volume per month (normalized)

The number of blocked events per customer almost doubled in each quarter of 2022, compared to the previous quarter.

Compared to a very low volume in the first quarter, the second quarter of 2022 saw record-level volumes.
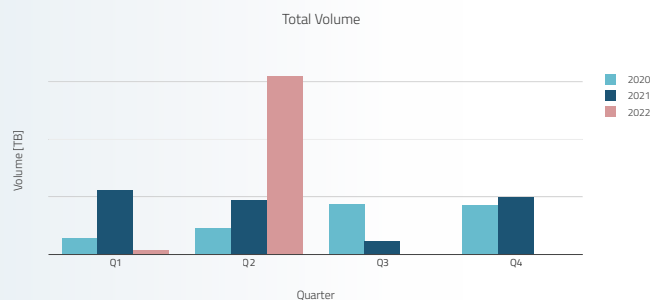
Attack Sizes

The average attack size, expressed in bits per second (bps), was considerably lower in the first half of 2022, compared to the previous years. In May, Radware mitigated an attack targeting a global cloud service provider in the U.S. The attack was volumetric and peaked at almost 1.5Tbps. The attack lasted for 36 hours, and sustained over 700 Gbps for more than eight hours. The attack represented a total volume of 2.9PB, and the largest part of this volume consisted of reflected UDP packets.

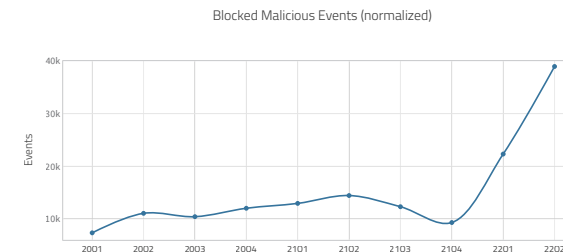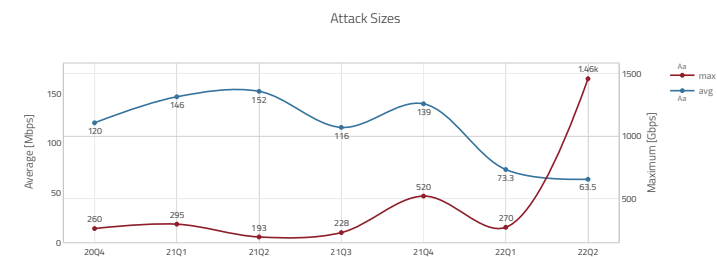**Figure 4:** Blocked Malicious Events per Customer, per Quarter

Figure 5: Evolution of Blocked Malicious Events per Customer, per Quarter

Figure 6: Total Blocked Volume per Quarter

Figure 7: Average and Maximum Attack Sizes per Quarter

Regions and Industries

The volume in the second quarter of 2022 was dominated by multiple attacks on a leading U.S. cloud service provider. The attack volumes, excluding the enormous attack, were mainly in Americas and EMEA. APAC accounted for only a smaller part of the blocked volume per customer.

In Q1 2022, research and education, telecom, and healthcare received the largest attack volumes. However, media and communication suffered the most attacks, followed by healthcare, technology, and finance.

Volumes and number of attacks do not always have to match up. UDP-based network level attacks typically account for a lot volume. TCP- (L4) and application-level attacks can seriously impact the services, but typically generate much smaller volumes. Attack volume is just one criterion to understand the attacks; the number of attacks is the second criterion that needs to be considered to have a complete picture.

In Q2 2022, service providers in U.S. dominated the attack volume, but in terms of the number of attacks per customer, communications had to fend off more attacks; a trend that started in Q1 and continued in Q2. Service providers followed media and communications in terms of attacks per customer, followed by healthcare and finance.

Figure 8

Blocked Volume per Region (Large Volumes on US Cloud Service Providers Ignored to Prevent Skewed Data)

2021 Blocked Volume (normalized)
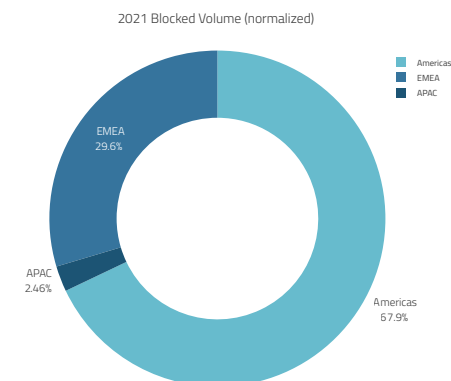
Figure 9: 2022 Q1 and Q2 Blocked Volume, Normalized per Customer

2022 Q1, Q2 Blocked Volume (normalized)
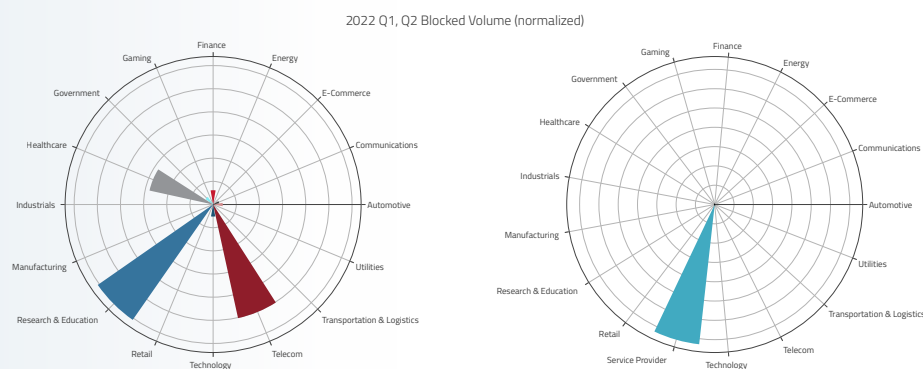
Figure 10: 2022 Q1 and Q2 Blocked Attacks, Normalized per Customer

2022 Q1, Q2 Blocked Attacks (normalized)

Attack Vectors and Applications

During the first six months of 2022, attacks smaller than 1Gbps were dominantly TCP protocol-based attacks, while the majority of the attacks above 10Gbps were UDP based.
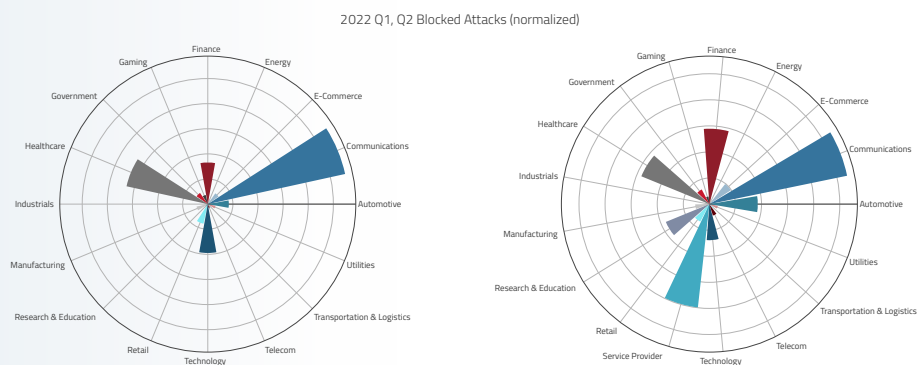
The larger the attack vector, the longer its duration will be. Attack vectors that are larger than 100Gbps had an average duration of almost 180 minutes (3 hours). For application and L4 attacks, more and smaller attack vectors were leveraged, with most TCP-based attacks below 1Gbps, leveraging vectors with an average duration of less than five minutes.

Attack vectors above 100Gbps leveraged UDP exclusively; no TCP-based attack vectors reached throughputs higher than 10Gbps.
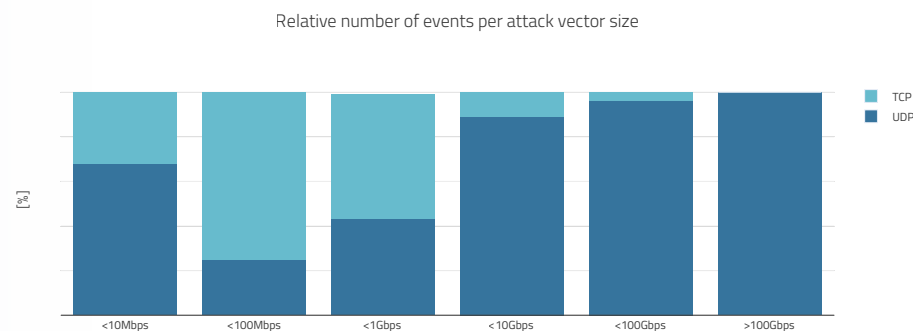
Large Attack Vectors

Radware considers attack vectors above 10Gbps to be large attack vectors. A single large attack vector would be enough to saturate many organizations headquarters and branches. Not every organization has 10GB per second internet links to provide connectivity for onsite employees to cloud-hosted applications or remote access for home workers.

Note that this section considers attack vectors. A vector is only one component of an attack. An attack consists of at least one, but typically, several attack vectors that can be active concurrently or sequentially in time.

Figure 11

TCP- vs UDP-Based Attacks per Attack Size

Relative number of events per attack vector size
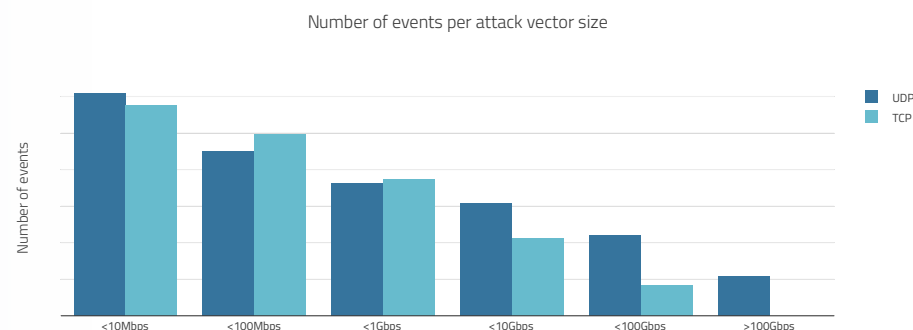
Figure 12

Average Duration per Attack Vector Size and Protocol

Average duration per attack vector size
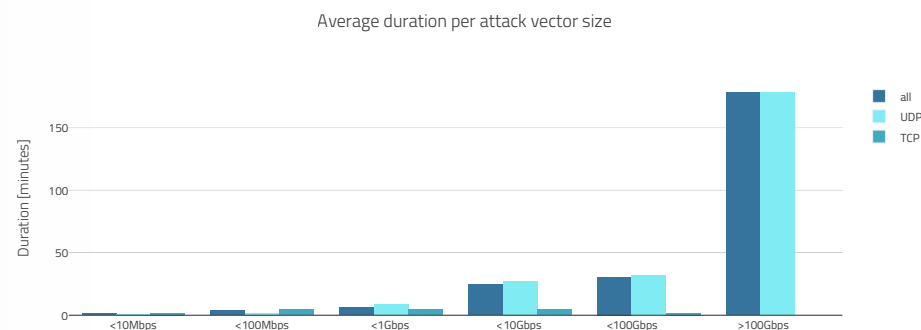
Figure 13

Number of Events per Attack Vector Size and per Protocol

Number of events per attack vector size

In 2022, the number of attack vectors, larger than 10Gbps, has declined compared to the same quarters in 2021. The large attack vectors have increased slightly between Q1 and Q2 of 2022.

Mid-Sized Attack Vectors

Vectors with throughputs between 1Gbps and 10Gbps are considered mid-sized attack vectors. A single mid-sized attack vector is enough to degrade the quality and experience of internet users and remote workers. Considering that attack traffic comes on top of legitimate traffic, attacks do not always need to reach above the total capacity of the internet connection to degrade the experience of on-premise employees and remote workers.

On average, the number of mid-sized attack vectors in the first half of 2022 was in decline compared to last year.
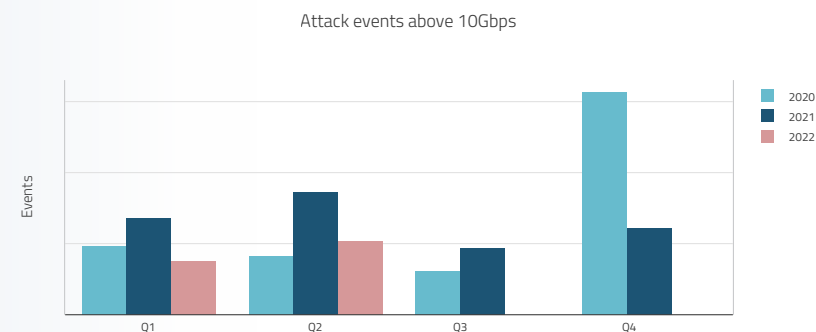
Micro Floods

Micro floods, or small-sized attack vectors, are vectors with throughputs below 1Gbps but above 10Mbps to eliminate bias from events that do not qualify as floods. Slower events could be network monitoring probes or discovery scans.

Micro floods do not necessarily impact the user experience. However, they are enough to become a nuisance when multiple floods are orchestrated that can concurrently force the owners to upgrade their internet links or infrastructure to keep a certain level of positive user experience. Micro floods are typically much harder to detect. They are at the bottom of the barrel and cannot be detected using traditional algorithms and techniques that detect larger attack vectors, based solely on thresholds.

By combining a large number of micro floods, or adding micro floods in a mix of mid and large size attack vectors, attackers can significantly increase the complexity of their attack campaigns. Attackers can make mitigation harder by forcing mitigators to constantly have to adapt their policies.

Figure 14

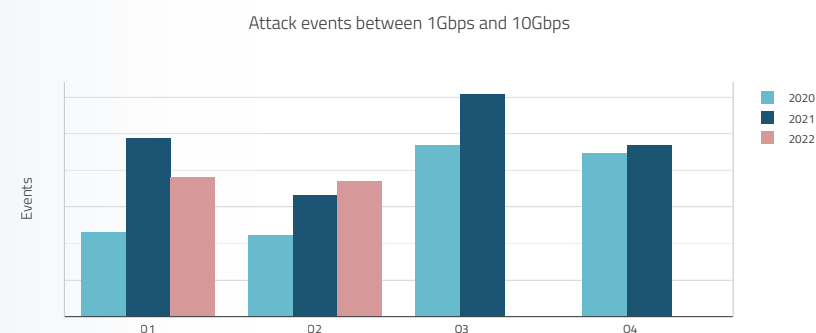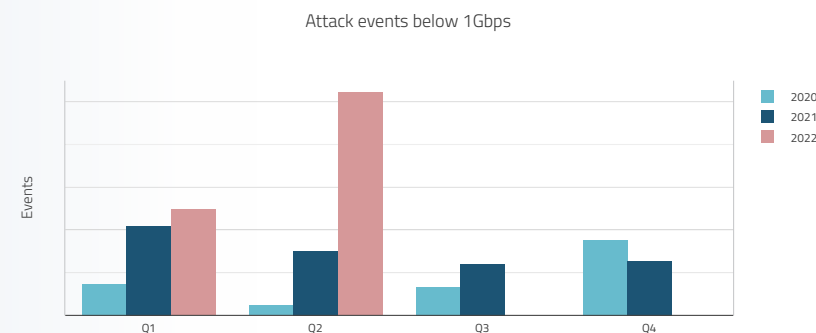Quarterly Number of Large Attacks

Attack events above 10Gbps

Figure 15

Number of Mid-Sized Attack Events by Quarter

Attack events between 1Gbps and 10Gbps

Figure 16

Number of Micro Flood Events by Quarter

Attack events below 1Gbps

In 2021, the number of micro floods had increased by 79% compared to 2020. The trend continued in 2022 and the number of micro floods has significantly increased attack vectors that are smaller than 1Gbps in Q1, and more pronounced in Q2.
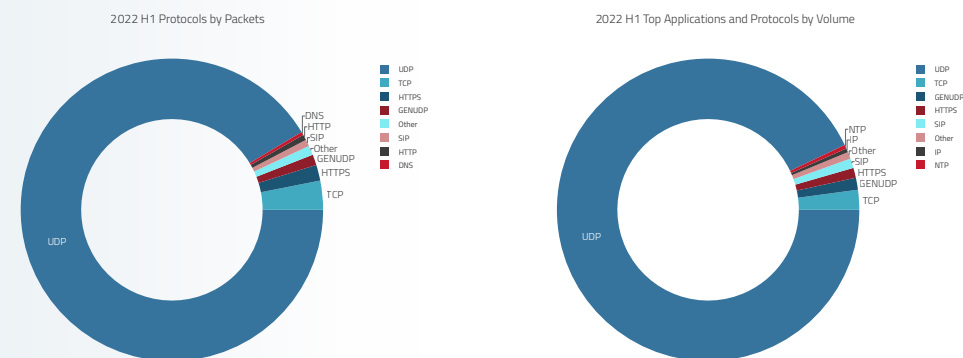
Attack Protocols and Applications

UDP is by far the most leveraged protocol in volumetric DDoS attacks. Because of its stateless character, UDP allows legitimate services to be abused, to send large volumes of unsolicited traffic to victims through reflection and amplification attacks.

HTTPS, SIP, and NTP were the most targeted applications, for targeted attacks. UDP and TCP are still the most dominant in volume while leveraged for random port attacks against networks.

In the first half of 2022, DNS amplification was the amplification attack vector that generated the most volume, with 84.5% of the total amplification volume. NTP amplification was the second most leveraged amplification attack vector, accounting for 15.5% of the volume. Smaller volumes were generated by SSDP, Memcached, CLDAP, DHCP Discover (IPv6), Chargen, ARMS, NXNS, and SNMP amplification attack vectors.

The gigantic volumetric, random port, carpet bombing attacks against a U.S. cloud service provider have significantly marked Q2, which biased the most dominant attack vector for that quarter as UDP Floods and UDP Fragmentation attacks. In Q1, the UDP Floods and Frag were present in large volumes, but TCP Out-of-State generated the most volume. In Q2, UDP Floods and Frag were followed by NTP amplification, SSDP amplification, and SYN Flood attack vectors.

Figure 17: Top Protocols Leveraged by Attacks in 2022

2022 H1 Protocols by Packets

Figure 18: Top Targeted Applications and Protocols by Volume

2022 H1 Top Applications and Protocols by Volume
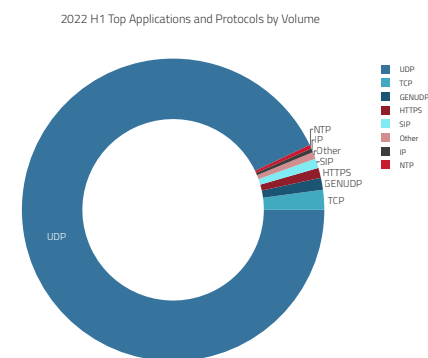
Figure 19: Top Amplification Attack Vectors by Volume

2022 H1 Amplification Attacks (normalized)
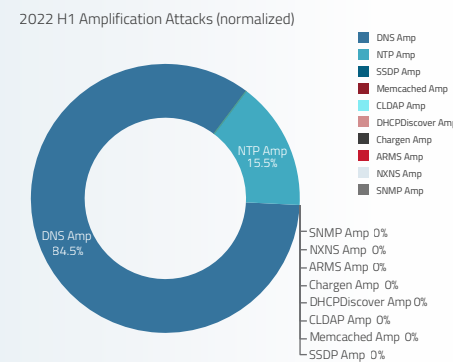
Figure 20: Top Attack Vectors by Attack Volume

H1 2022 Top Amplification Volumes (normalized)
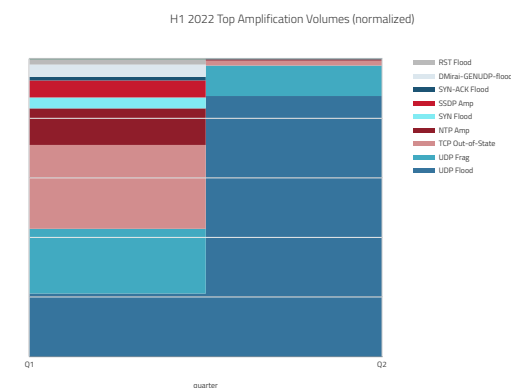
Attack Complexity

An attack is considered more sophisticated or complex when it leverages diverse attack vectors, that is, attacks that make use of multiple concurrent or attack vectors, which change over time, attempting to confuse detection and make mitigation harder. Fast shifts and high numbers of concurrent vectors are impossible to mitigate without leveraging automation.

Figure 21

Number of Dissimilar Attack Vectors per Attack, Function of Attack Size

Number of dissimilar attack vectors per attack in function of attack size (H1 2022)
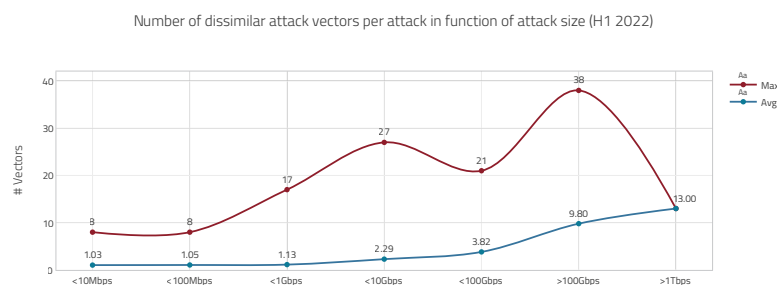
The average complexity of attacks in the first half of 2022 increased with the attack size. Since the average number of attack vectors in a single attack can impossibly be smaller than one, smaller attacks exhibit a more isolated character, as their average vectors per attack becomes closer to one. Attacks above 1Gbps average more than two dissimilar attack vectors per attack. One attack above 100Gbps had the largest complexity with 38 dissimilar attack vectors. In May, the largest attack was recorded by Radware, with 13 dissimilar attack vectors, a higher complexity than the average attack complexity of smaller attack vectors.

Record-Breaking DDoS Attacks

In April, Cloudflare detected one of the largest HTTPS DDoS attacks on record. Cloudflare announced to have blocked 15 million request per second, the HTTPS DDoS attacks originated from 6,000 unique bots that targeted a crypto launchpad. The attack lasted for 15 seconds and no actor claimed credit for it.

In May, Radware mitigated a volumetric DDoS attack that peaked at almost 1.5Tbps. While the peak attack throughput was not the highest ever recorded, unlike most DDoS record breaking attacks, with a duration of less than 60 seconds reported in the last two years. This volumetric random port attack was a carpet bombing attack that swept evenly across all IP addresses of the targeted subnet and lasted for 36 hours. The attack throughput sustained over 700Gbps for more than eight hours. The total volume generated by this attack was 2.9PB, which was 1.5 times all the information contained in all U.S. academic research libraries. The attack vectors consisted mainly of UDP reflection and amplification; a total of 38 dissimilar attack vectors were observed.

Hacktivism

Philippine Elections

On February 27, 2022, as CNN Philippines was gearing up to live stream a debate between candidates standing in the country's presidential elections, their website went down. It was the second time in two months that the site had been hit, as Peter Guest, enterprise editor for Rest of World, reported. Since June 2021, opposition politicians, independent media, and fact-checking websites in the Philippines had been hit repeatedly with DDoS attacks. CNN, major news network ABS-CBN, Rappler (the outlet founded by Maria Ressa- Nobel Peace Prize winner, 2021), and VERA Files (fact-checking organization), have all been targeted, along with the website of Vice President Leni Robredo, who was a staunch critic of the current president, Rodrigo Duterte. For the previous 10 months, the attacks had escalated in frequency and aggression, as the country moved towards the 2022 general elections. Some of the organizations had been under a constant barrage of DDoS attempts.

OpsBedil, DragonForce Malaysia vs Israel

OpIsrael is a yearly operation which targets Israelian businesses and citizens. It was almost non-existent this year due to Anonymous' focus on the Russo-Ukrainian conflict. OpsBedil, a hacktivist operation targeting Middle Eastern organizations in 2021, however, did make a return this year. OpsBedil can be considered the replacement for the now-defunct OpIsrael operations. The new OpsBedil operations were conducted by DragonForce Malaysia, and its affiliates throughout Southeast Asia, specifically Malaysia and Indonesia. The current operation, OpsBedil Reloaded, is considered as a political response to events that occurred in Israel on April 11, 2022, while hacktivists executed website defacements, sensitive data leaks, and Denial-of-Service attacks. Hacktivist campaigns, like OpsBedil, were not as notorious as OpIsrael once was, presenting a renewed level of risk for the region. Unlike Anonymous, DragonForce Malaysia, and its affiliates have the time, resource, and motivation to execute these attacks and present a moderate-level threat to Israel.

OpsPatuk, DragonForce Malaysia vs India

On June 10, 2022, Radware reported that, "DragonForce Malaysia launched a series of cyberattacks against the government of India and numerous organizations across the country". OpsPatuk is a new campaign, and like all other operations this hacktivist group runs, it is reactionary and in response to a controversial statement made by the spokesperson of Bharatiya Janata Party (BJP) condemning the Prophet Muhammad, SAW. As a result, DragonForce Malaysia, with the assistance of several other threat groups, had begun indiscriminately scanning, defacing, and launching Denial-of-Service attacks against numerous websites in India. The advanced members of this group were observed leveraging current exploits, breaching networks, and leaking data.

Ransom DoS

The first half of 2022, was marked by a significant increase in DDoS activity across the globe. Attacks have ranged from cases of hacktivism to terabit attacks in Asia and the United States. In the previous months, Ransom Denial-of-Service (RDoS) groups claimed to be Phantom Squad and REvil resurged. In May, Radware discovered several ransom demand letters from a group posing as Phantom Squad.

Figure 22

Phantom Squad 2022
Ransom Note


```
FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE
DECISION!

We are Phantom Squad

Your network will be DDoS-ed starting May 23rd if you don't pay protection
fee - 0.2 Bitcoin @

We will start by brining down your corporate DNS:

If you don't pay by May 23rd, attack will start, yours service going down
permanently price to stop will increase to 20 BTC and will go up 10 BTC for
every day of attack.

This is not a joke.
```
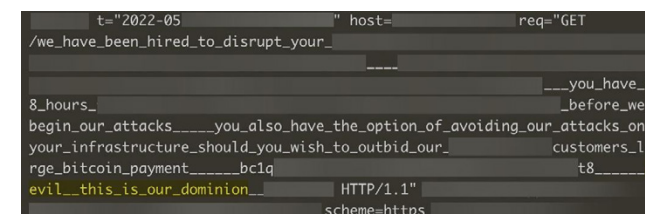
During one of the many waves of RDoS campaigns in 2021, a group claiming to be REvil (a notorious ransomware group), targeted several VoIP providers worldwide. At the time, REvil had just returned to action, followed by the Kaseya VSA ransomware attack. The RDoS campaign sparked concern as critical infrastructure was impacted, and it resulted in an industry-wide warning from Comms Council UK stating a "coordinated extortion-focused international campaign by professional cyber criminals", targeting IP-based communication services providers in October 2021. While RDoS attacks were typically considered lower tier threats they were easy to mitigate, Bandwidth.com went on record that the RDoS attacks caused a $700,000 reduction of revenue in Q3, and would end up costing them up to $12 million in actual and defamation.

During the first half of 2022, a renewed campaign of RDoS attacks by a group claiming to be REvil emerged. This time the group was not only sending warning notes for ransom before the attack starts, but also embedded the ransom note and demands within the attack payload. The attacks were high-frequency HTTPS GET request floods, lasting for several minutes, and ranging up to millions of requests per second, targeting online applications, hosts, and embedding the ransom message as a readable string in the URL.

Figure 23

REvil RDoS Note
Embedded in URL and
Recorded in Server Log
Files


```
t="2022-05            " host=            req="GET
/we_have_been_hired_to_disrupt_your_
____
                                ___you_have_4
8_hours_                              _before_we_
begin_our_attacks_____you_also_have_the_option_of_avoiding_our_attacks_on_
your_infrastructure_should_you_wish_to_outbid_our_        customers_la
rge_bitcoin_payment_____bc1q                          t8_____r
evil__this_is_our_dominion__            HTTP/1.1"
                                scheme=https
```

DDoS Attacks on Gaming

In January, APEX Legends pros went to Twitter and complained that "Ranked is unplayable due to DDoS attacks." Apex Legends, is a highly competitive game, and while the majority of the community abides by the rules, and relies on their own skill to earn victories, a percentage of players use third-party software to gain massive advantage which might include aimbots, and wallhacks in the Ranked game mode. This method includes DDoS attacks that disrupt the entire sever, effectively disconnecting all the players in a match.

On January 22, the high stakes Squidcraft Games were plagued by DDoS attacks which resulted in the elimination of Team Andorra. Twitch Rivals Squidcraft Games is a Minecraft tournament for streamers, held in a custom mode inspired by the popular TV series "The Squid Game". Over 150 participants, Twitch's most famous Spanish-speaking creators, were competing in various mini-games with direct elimination over five days. On the second day of the tournament, many Andorran streamers were eliminated after disconnecting repeatedly. NetBlocks, a group that tracks network disruptions and shutdowns, claimed in a tweet that the DDoS attack was actually targeting the competition. Unfortunately, the rest of Andorra also went down with the eliminated streamers. The internet outage lasted for over half an hour after the start of the DDoS attacks, as Andorra Telecom worked to restore service.

On March 25, a DDoS attack left 'Among Us' unplayable in North America and Europe.

Intrusions

Not all malicious events that target the internet exposed assets are DoS attacks. Network intrusion attacks consist of easy-to-execute exploits, based on known vulnerabilities, and range from scanning, using open source or commercial tools, information disclosure attempts for reconnaissance, up-to-path traversal and buffer overflow exploitation attempts, that could render a system inoperable or could provide access to sensitive information.

When considering malicious events targeting the same assets and resources, the number of recorded intrusion events is typically larger than the number of DoS attacks. However, this difference in numbers should not be interpreted as assets having to block more traffic from intrusion, than from DoS events.

The relative amount of intrusions grew from 67% in 2021 to 82% in the first half of 2022.

Figure 24

Denial-of-Service vs Intrusion Events

2022 H1 Attack Categories

Intrusions
DoS

DoS 17.9%
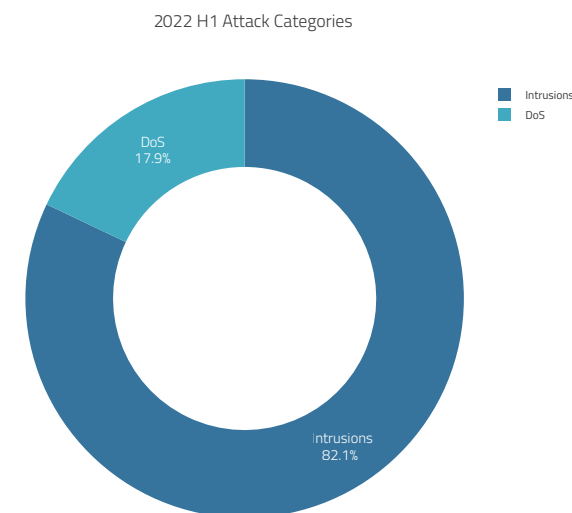
Intrusions 82.1%

Log4Shell Intrusion Activity

The December 9, 2021 publicly disclosed Log4j vulnerability took the security community by storm. A vulnerability in a pervasively used Java logging library, allowing an unauthenticated attacker to leverage publicly available exploits for Remote Command Execution (RCE), was considered as the most critical vulnerability of 2021. Some argued that it was the worst vulnerability of the decade.

According to Rezilion report on April 26, 2022, more than four months after the vulnerability was disclosed, there were still over 90,000 vulnerable internet-facing applications and more than 68,000 servers that are still publicly exposed.

The peak of the activity was on December 22, with over 90,000 exploits blocked in a single day. The activity slowed down between February and May, but by mid-May, the activity seemed to gain importance again. Between the day of disclosure of the vulnerability and June 30, 2020, Radware cloud services blocked over 6 million exploits.

As in the case of other vulnerability scanning activities, a portion of the recorded events and exploits originated from benign actors and organizations, performing internet-wide scans to assess the risk and proactively inform corporations that might not be aware of the risk. Bug bounty programs were initiated to motivate vulnerability researchers to discover vulnerable services and organizations. While the numbers were alarming, a portion of the activity could be considered non-malicious. The size of the non-malicious portion is unfortunately harder to quantify, since white, grey, and black-hat scanners, leveraged very similar attack methods. Some of the white-hat scanners were kind enough to identify themselves through web application parameters, or user agent strings, but their identifiers were inconsistent at best, and did not allow to make a complete assessment, between benign and malicious operations.

Figure 25: Daily Blocked Log4 Shell Intrusion Attempts in Radware Cloud WAF and Cloud DDoS Services

Blocked Log4shell exploits per day (a total of 6,134,647 exploits blocked)
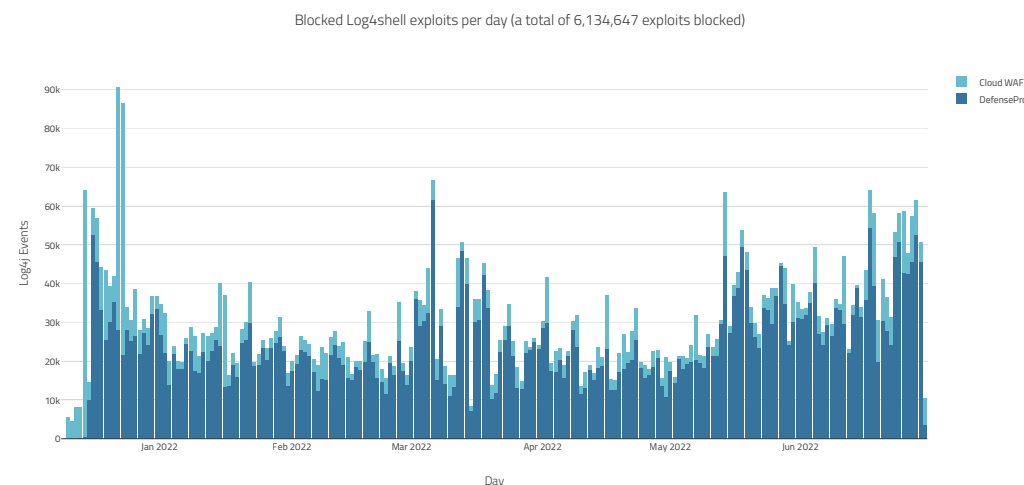
Web Application Attack Activity

The number of blocked malicious web application transactions in the first half of 2022, grew by 38% compared to the first half of 2021; it was higher than the total number of malicious transactions in 2020.

The first two quarters of 2022 followed a similar growth pattern compared to previous years. After a dip in Q4 of 2021, Q1 and Q2 of 2022 are tracking back to levels comparable to Q3 of 2021. Q2 of 2022 currently has the highest number of malicious web transactions, since January 1, 2020.

Web application transactions can be blocked by application specific, and custom rules created by the Security Operation Center (SOC). Figure 28, shows the total number of blocked transactions, and the share of those transactions, that were blocked by signature, and behavioral detection modules. Overall, 49% of malicious web transactions were detected and blocked by web application modules, based on known malicious behavior and signatures.

To eliminate potential bias introduced by application and customer specific security policies, the remainder of this section considers only the attacks detected and blocked, based on known malicious behavior, vulnerabilities, and exploits.
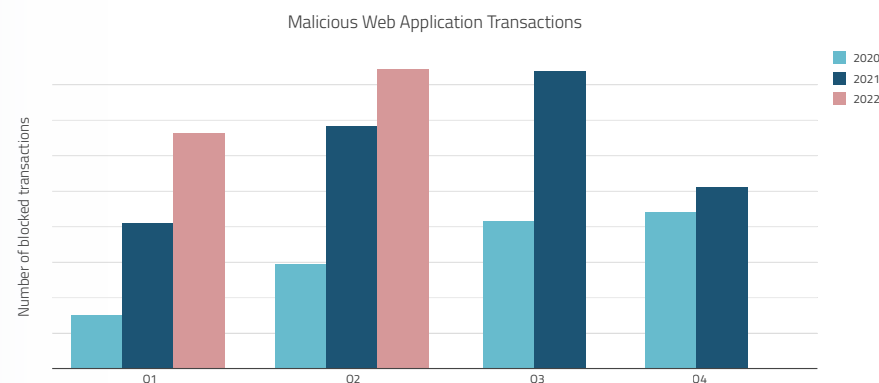
Figure 26

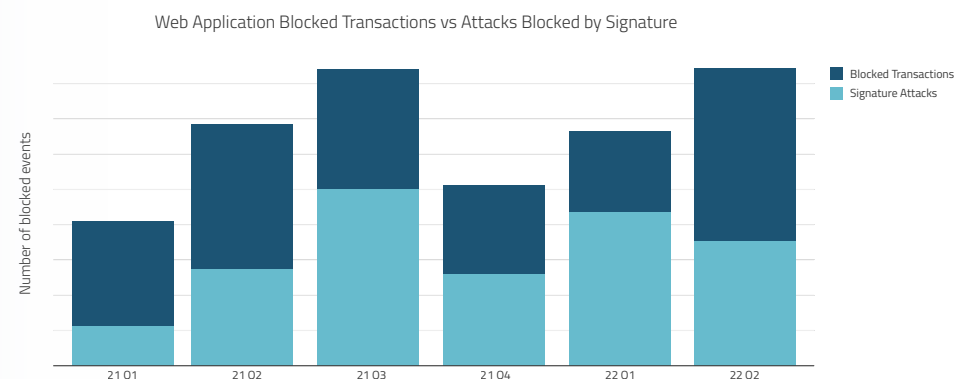Yearly Blocked Malicious Web Application Transactions
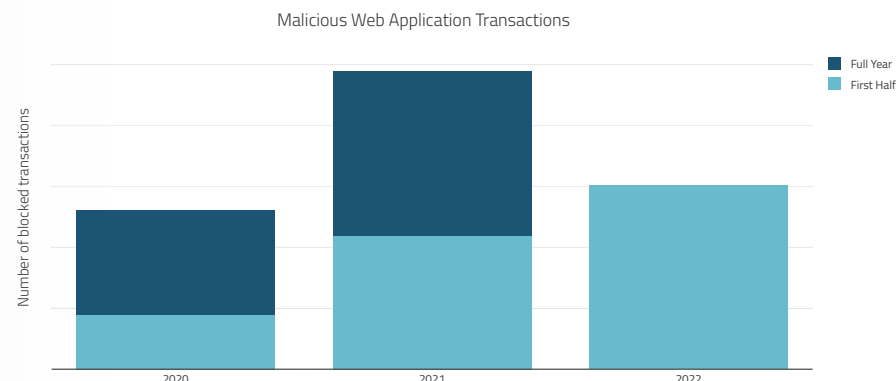
Figure 27

Quarterly Blocked Malicious Web Application Transactions

Figure 28

Web Application Transactions vs Attacks Blocked by Signature

Malicious Web Application Transactions

Malicious Web Application Transactions

Web Application Blocked Transactions vs Attacks Blocked by Signature

Security Violations

The most important security violation, Figure 29, predictable resource location attacks and Figure 30, accounted for almost half of all attacks witnessed in the first half of 2022.

Predictable resource location attacks, target hidden content and functionality of web applications. By guessing common names for directories of files, an attack may be able to access resources that were not intended to be exposed. Examples of resources that might be uncovered through Brute Force techniques include old backup and configuration files, yet to be published web application resources, and so on. Predictable resource location attempts are covered by the OWASP 2017 Top 10[1] web application security risk "Broken Access Control," was ranked 5th in 2017, and moved to first position in the 2021 OWASP Top 10 (refer to Figure 31). Code Injection and SQL Injection were in the second and third position. Combined with predictable resource location attacks, these three attacks were responsible for almost 75% of the total attack activity on web applications and APIs.

1. The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications and published by the OWASP® Foundation.
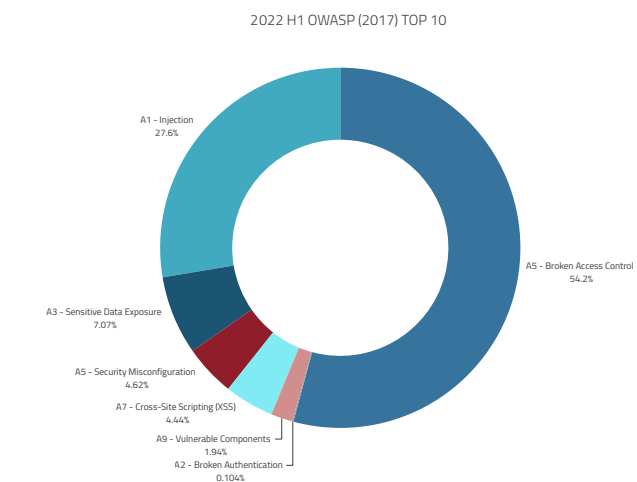
Figure 29: Top Security Violation Types

2022 H1 Top Violation Types
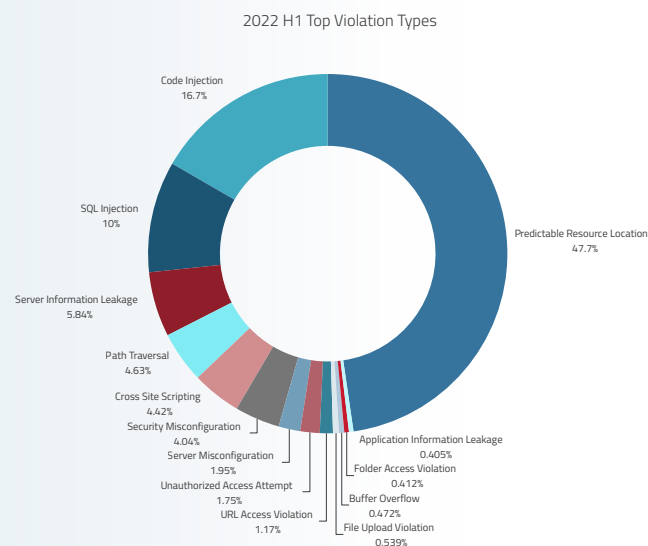
Figure 30

Violation Types
for Known Web
Application Attacks by
Quarter
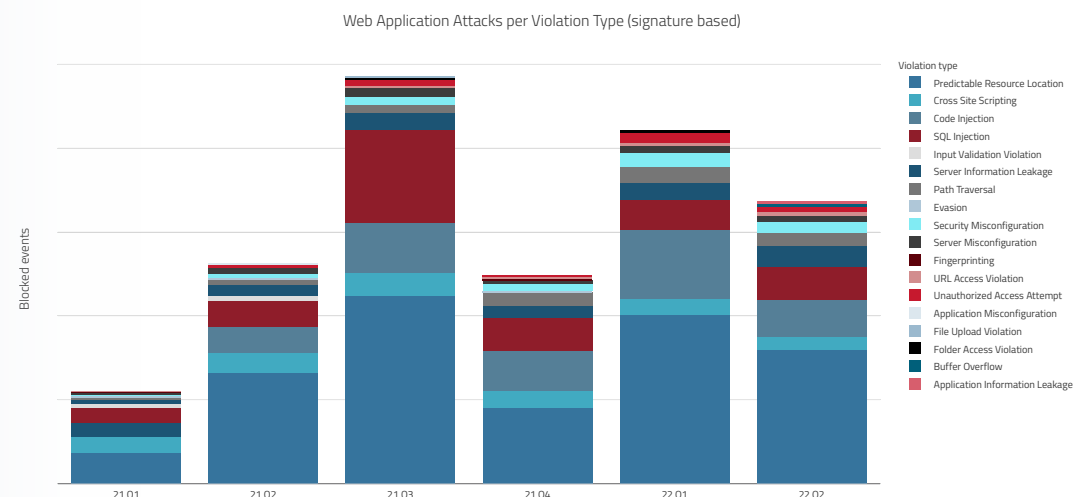
Figure 31: Blocked Security Violation by OWASP 2017 Application Security Risk


2022 H1 OWASP (2017) TOP 10

Web Application Attacks per Violation Type (signature based)

Attacking Countries

Most blocked web security events in the first half of 2022 originated from the United States and India. Russia, Italy, and the Netherlands completed the top five in the first half of 2022. It is important to note that the country where an attack originates from does not have to correspond to the nationality of the threat actor or group. Arguably, the country where the attack originates from, will most often not correspond to the home country of the threat actor. Threat actors leverage anonymizing VPNs, ToR, and compromised servers as jump hosts to perform their attacks. The originating country of an attack is chosen based on the location of the victim, or based on the country the threat actor wants to see attributed during false flag operations.

Attacked Industries

The most attacked industries in the first half of 2022, were retail, wholesale trade, and high tech, together accounting for over 50% of blocked web application attacks. Carriers were third with 13.7%, followed by SAAS providers with 7%. This was followed by e-commerce and gaming (5%), education (3.2%), healthcare (3%), manufacturing (3%), government (2.8%), banking and finance (2.7%), and so on.
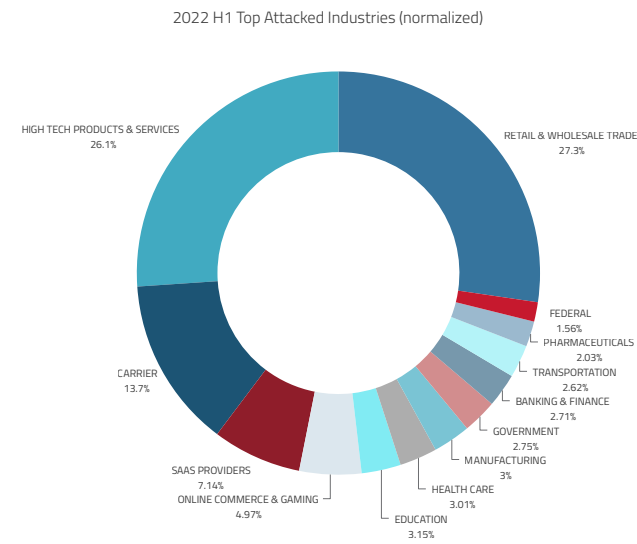
Figure 32

Top Offending Countries per Quarter

Top Attacking Countries
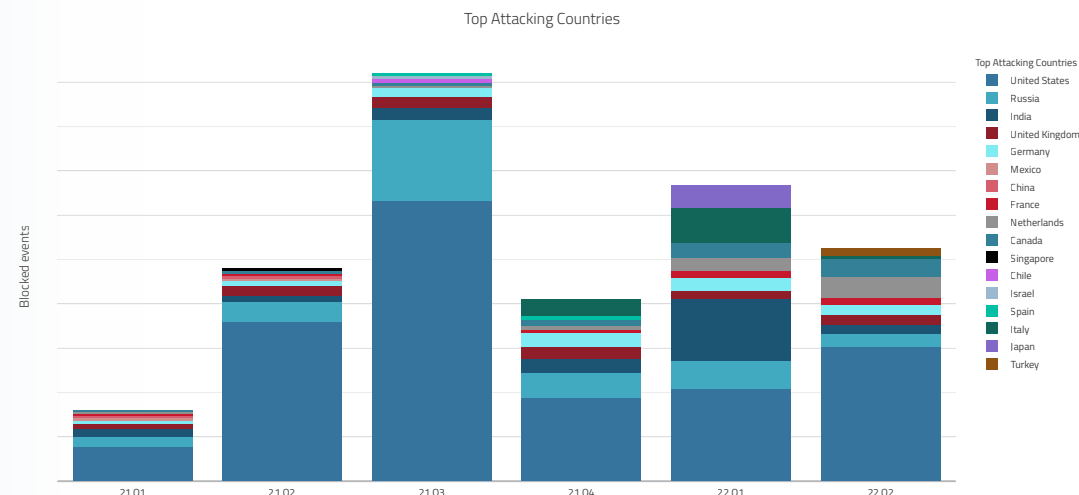
Figure 33: 2022 H1 Top Offending Countries

2022 H1 Top Attacking Countries
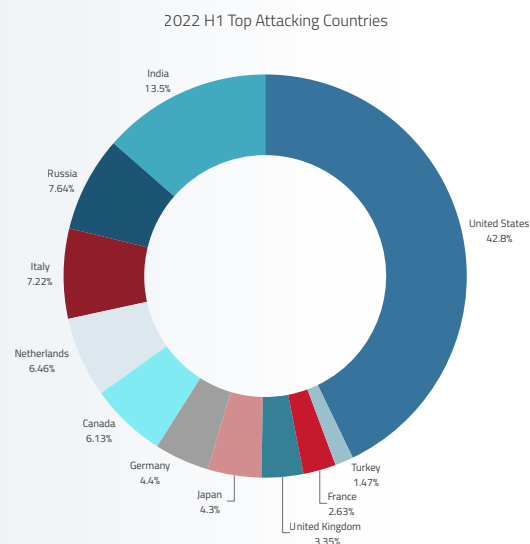
Figure 34: Web Application Attacks by Industry

2022 H1 Top Attacked Industries (normalized)

Unsolicited Network Activity

The Radware Global Deception Network consists of a wide range of globally distributed sensors that collect unsolicited traffic, and attack attempts. Unsolicited events include DDoS backscatter, spoofed[2] and non-spoofed scans, and spoofed and non-spoofed attacks.

The difference between deception network events discussed in this section and the web application and DDoS attack events in previous sections is the unsolicited nature of the event.
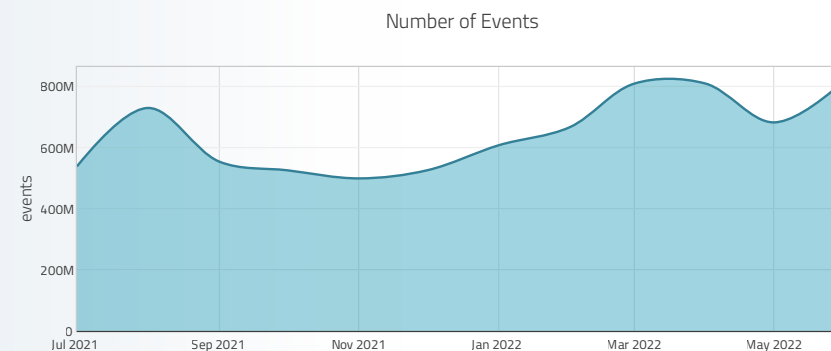
Web application and DDoS attack events were collected from services that protect actual services of organizations that are published and exposed on the internet, backed by real applications and networks. In the latter case, attackers targeted a particular organization or a known service.

Unsolicited events, as recorded by the deception network, are random acts. These scans or attacks do not target known services or a particular organization. The IP addresses of the deception network are not exposed in DNS or used to publish applications or services. No client, agent, or device has a legitimate reason to access the Radware Deception Network sensors.
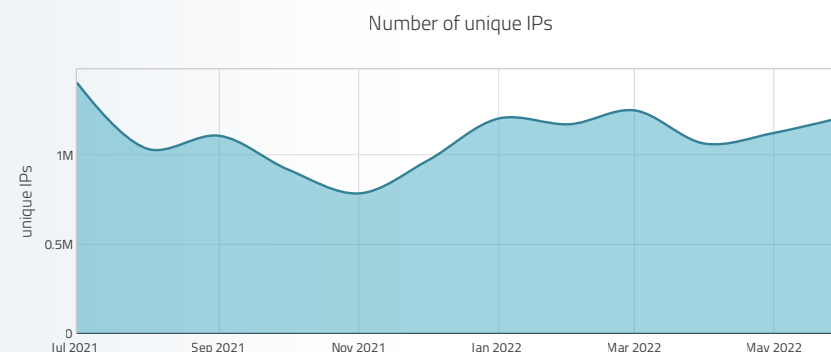
The total number of unsolicited events, registered by the deception network, in the first half of 2022 was almost 4.4 billion, 30% up from the number of unsolicited events registered, in the last half of 2021. During the first half of 2022, the number of events peaked at over 820 million events, in the month of June.

The number of unique IP addresses provide a measure for the evolution of the number of malicious hosts and devices that randomly scan the internet, and exploit known vulnerabilities. In March 2022, the number of unique IP addresses reached 1.25 million. A total of 7 million unique IPv4 addresses were recorded in the first half of 2022; an increase of 13% compared to the last half of 2021.

2. IP address spoofing or IP spoofing is the crafting of Internet Protocol (IP) packets with false source IP addresses, for the purpose of impersonating another originating computing system and geolocation. (source: Wikipedia)
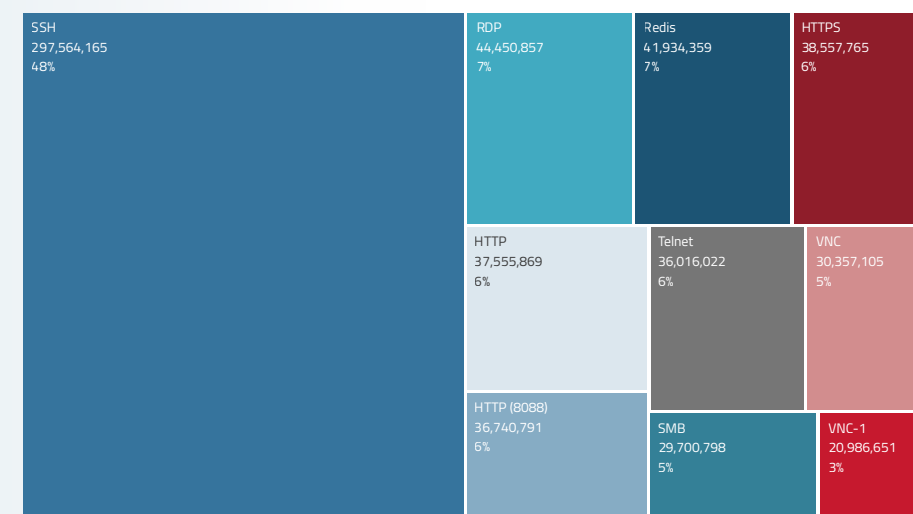
Figure 35: Number of Events per Month as Recorded by Radware's GDN

Number of Events

Figure 36: Number of Unique IPs per Month, Registered by Radware's GDN

Number of unique IPs

Most Scanned and Attacked TCP Ports

For TCP services, the top 10 most scanned and attacked services, were SSH on port 22, followed by RDP[3] on port 3389, Redis[4] on port 6379, HTTPS on port 443, HTTP on port 80, HTTP on port 8088, Telnet on port 23, VNC[5] on port 5900, SMB[6] on port 445, and VNC-1[7] on port 5901. Compared to 2021, Redis scans and attacks increased significantly, while VNC-1 joined the top 10 in favor of SMTP.

Telnet, HTTP on port 8088, and SSH remain amongst the top exploited TCP ports of 2021. These are typically abused by IoT botnets, including many of the Mirai variants, that are continuing to wreak havoc on the internet through DDoS attacks, and put IoT devices such as IP cameras, and network devices such as, routers and modems at risk. While Telnet was a Mirai favorite for a long time, the events on SSH surpassed Telnet by almost eight times. Most SSH attacks consist of account takeover, and Brute Force attempts. By leveraging default credentials or leaked credentials, attackers try to get unauthorized access to devices and systems, and either move laterally across organizations networks, abuse the resources of cloud instances for crypto mining, leverage the foothold as jump host to anonymize targeted attacks, or leverage the devices connectivity to perform DDoS attacks.

Figure 37: Top Scanned and Attacked TCP Ports

H1 2022 Top Scanned Ports - TCP

SSH 297,564,165 48%	RDP 44,450,857 7% / Redis 41,934,359 7% / HTTPS 38,557,765 6%
	HTTP 37,555,869 6% / Telnet 36,016,022 6% / VNC 30,357,105 5%
	HTTP (8088) 36,740,791 6% / SMB 29,700,798 5% / VNC-1 20,986,651 3%

---

3. Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. (source: Wikipedia).

4. Redis (port 6379) is an open source (BSD licensed), in-memory data structure store, used as a database, cache, and message broker. In July of 2021, a Remote Command Execution (RCE) vulnerability (CVE-2021-32761) was disclosed. A remote attacker can pass specially crafted data to the application, trigger integer overflow, and execute arbitrary code on the target system.

5. Virtual Network Computing (VNC) is a graphical desktop-sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It transmits the keyboard and mouse input from one computer to another, relaying the graphical-screen updates, over a network. (source: Wikipedia).

6. Server Message Block (SMB) is a communication protocol[1] that Microsoft created to provide shared access to files and printers across nodes on a network. (source: Wikipedia).

7. VNC-1 port provides desktop :1 sharing in the Virtual Network Computing (VNC) graphical desktop-sharing system.
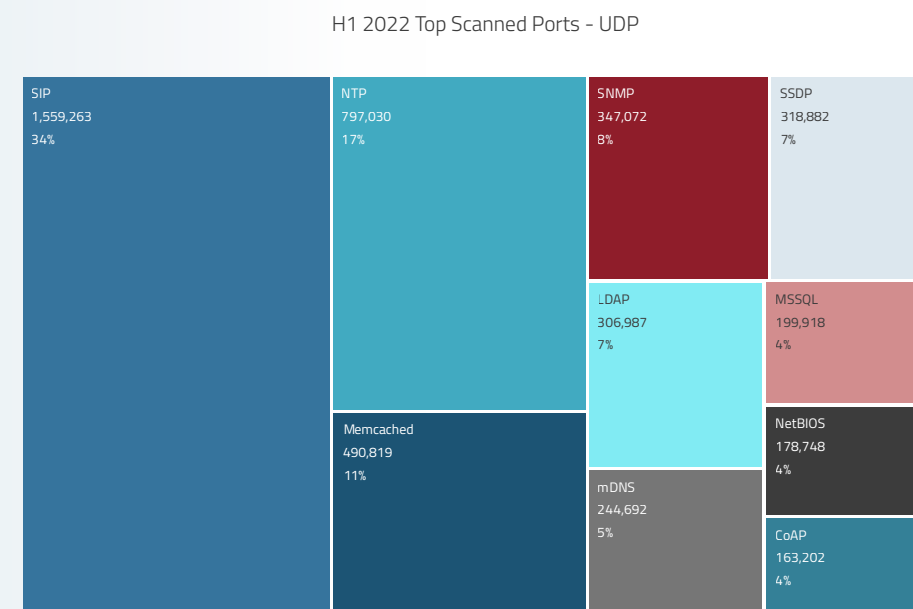
Most Scanned and Attacked UDP Ports

Like 2021, SIP (port 5060) was the most targeted UDP-based service, in the first half of 2022. Port 5060 is used by many SIP-based VoIP phones and providers. VoIP remains critical to organizations to ensure their productivity, and for this reason, it was one of the most targeted services for DDoS attacks in 2021 and 2022. Vulnerabilities, and weak or default passwords in VoIP services, allow them to be abused for initial access, spying, and moving laterally inside organizations networks.

NTP (port 123), Memcached (port 11211), SNMP (port 161), SSDP/UPnP (port 1900), LDAP (port 389), and mDNS (port 5353), are amongst the most leveraged protocols for DDoS amplification attacks. Many black and white-hat actors are continuously scanning and cataloging the internet's addressable range, to abuse for DDoS attacks (Blackhat), or assess the risk in the DDoS threat landscape (Whitehat).

MSSQL (port 1434), is used by the Microsoft SQL Server database management system monitor, and abused through remote code execution vulnerabilities, known for the W32.Spybot.Worm that spread through MSSQL Server 2000, and MSDE 2000, were a very solicited port in 2021 and 2022.

CoAP (port 5683), closes the top 10 scanned and attacked ports in 2022. Constrained Application Protocol (CoAP), is a specialized web transfer protocol (web API), used with constrained nodes and constrained networks in the Internet of Things.

Figure 38: Most Scanned and Attacked UDP Ports

H1 2022 Top Scanned Ports - UDP

SIP 1,559,263 34%	NTP 797,030 17%
	SNMP 347,072 8%
	SSDP 318,882 7%
	LDAP 306,987 7%
	MSSQL 199,918 4%
Memcached 490,819 11%	mDNS 244,692 5%
	NetBIOS 178,748 4%
	CoAP 163,202 4%

Originating Countries

In the first half of 2022, the top countries in which unsolicited network activity originated were the US, Russia, China, Netherlands, and Hong Kong. Compared to the previous year, the UK left the top five and Hong Kong joined it.

Note: The real origin of an attack can be spoofed to impersonate attacks from a different country.

Web Service Attacks

The top attacked HTTP Uniform Resource Identifiers (URI) are led by '/', the universal URI for testing the presence of a web service, and collecting information from header fields in server responses. There is a significant difference in the top targeted URIs for unsolicited events, compared to top targets in web application attacks, where services are backed by real applications. This section covers unsolicited events which means that there is no real application or service running on the web server. The top URIs need to be interpreted as the top services and applications that are targeted by actors, malicious and benign, randomly scanning the internet. Typically, a URI will conform with a known and disclosed vulnerability.

/ws/v1/cluster/app/new-application

A known vulnerability used to exploit Hadoop YARN services and schedule arbitrary workloads on Hadoop clusters [71]. An exploit seen leveraged by many cryptojacking campaigns, that try to leverage capable cloud instances of enterprises and research institutions illegitimately [72]. Was #1 exploit in 2020 [73].

/level/15/exec/-/sh/run/CR

In Aug 2002, Cisco released IOS 11.2 for Cisco routers, that offers an HTTP interface which allowed a user to execute commands directly from a URL. Attackers are still trying to find Cisco routers without authentication on the HTTP interface. Many routers have been deployed without changing default passwords or basic hardening practices, allowing for such opportunistic behavior by threat actors to bare fruits. Was #3 exploit in 2020 [73].

/v1.16/version

Used by threat actors to identify the available Docker API version through invoking a command for an old version. Used by cryptocurrency miners for abusing containers through docker API. [74]

/nice%20ports%2C/Tri%6Eity.txt%2ebak

Request for "/nice ports,/Trinity.txt.bak" is used by Nmap's service detection routine to test how a server handles escape characters within a URI.
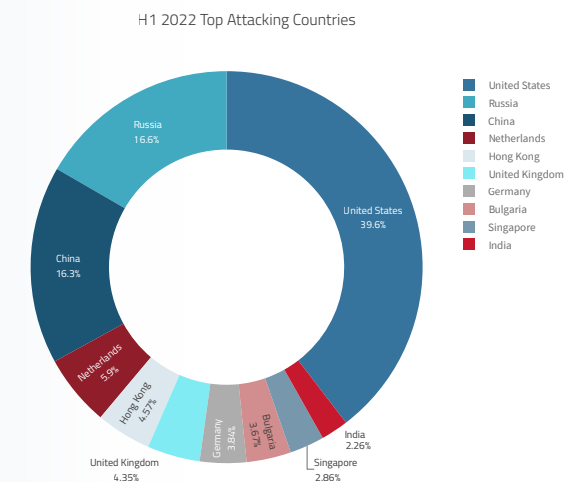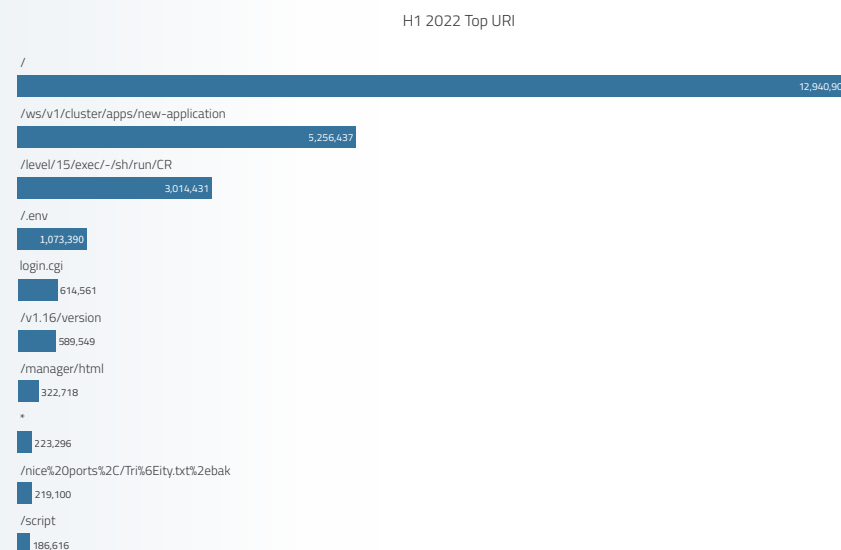
Figure 39: Top Attacking Countries

H1 2022 Top Attacking Countries

- United States
- Russia
- China
- Netherlands
- Hong Kong
- United Kingdom
- Germany
- Bulgaria
- Singapore
- India

Figure 40: Top Scanned URI

H1 2022 Top URI

URI	Count
/	12,940,902
/ws/v1/cluster/apps/new-application	5,256,437
/level/15/exec/-/sh/run/CR	3,014,431
/.env	1,073,390
login.cgi	614,561
/v1.16/version	589,549
/manager/html	322,718
*	223,296
/nice%20ports%2C/Tri%6Eity.txt%2ebak	219,100
/script	186,616

Top User Agents

In HTTP, the User-Agent string is often used for content negotiation, where the origin server selects suitable content or operating parameters for the response. For example, the User-Agent string might be used by a web server to choose variants based on the known capabilities of a particular version of client software and differentiate its interface for different user interfaces on mobile phones, tablets, and desktop browsers. The concept of content tailoring is [built into the HTTP standard](#) in RFC 1945, "for the sake of tailoring responses to avoid particular user agent limitations."

As such, the User-Agent field in a web request can be used to identify the client agent that makes the request. Some malicious actors are aware of this identifying feature being leveraged to score the legitimacy of a web request by web security modules and mask their origins by randomly generating and changing the User-Agent to known legitimate values.

Commercial and open source web service vulnerability scanning tools can be identified through their User-Agent, such as 'ZGrab', which is the application-layer network scanning component of the Zmap open source scanning tool.

Top HTTP Credentials

Not all web service vulnerabilities can be exploited without authentication. Some web services have widely used default and some have even hard-coded secrets to protect access from unauthorized users or devices. The typical weak passwords, combined in credential pairs with user admin or root, were 'admin', 'password', '123', '1234', '12345', '123456', '1234567890', and no password. These weak password permutations make up the top 10 credentials. These are universally agreed upon as the worst credentials and the most abused, because they provide a good amount of access to unauthorized devices that did not have their default credentials changed on installation.
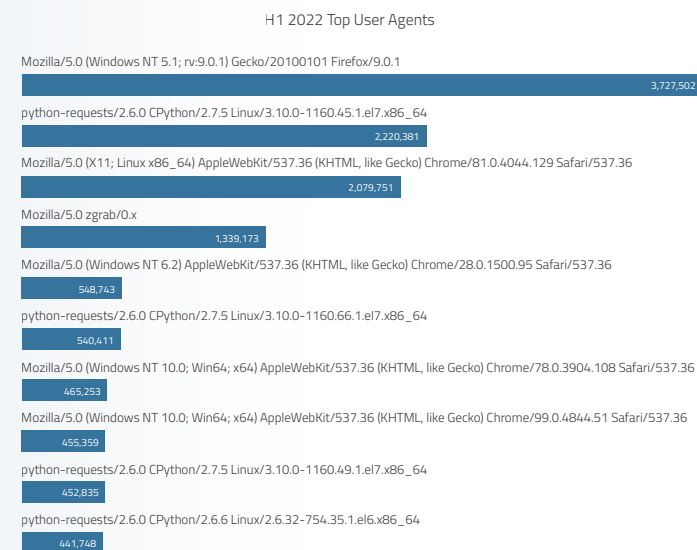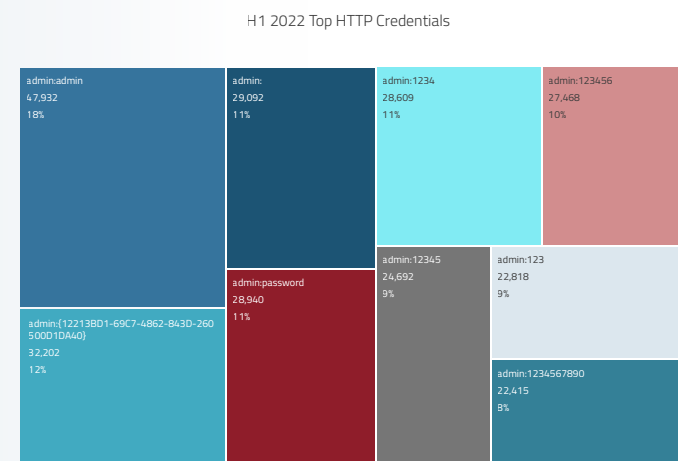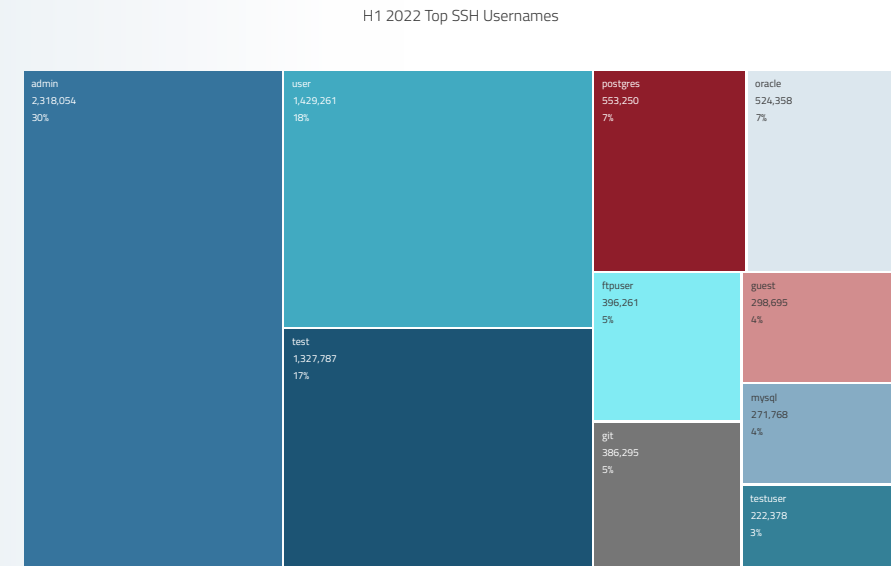
Figure 41: Top User-Agents

H1 2022 Top User Agents

Mozilla/5.0 (Windows NT 5.1; rv:9.0.1) Gecko/20100101 Firefox/9.0.1
3,727,502

python-requests/2.6.0 CPython/2.7.5 Linux/3.10.0-1160.45.1.el7.x86_64
2,220,381

Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36
2,079,751

Mozilla/5.0 zgrab/0.x
1,339,173

Mozilla/5.0 (Windows NT 6.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36
548,743

python-requests/2.6.0 CPython/2.7.5 Linux/3.10.0-1160.66.1.el7.x86_64
540,411

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
465,253

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
455,359

python-requests/2.6.0 CPython/2.7.5 Linux/3.10.0-1160.49.1.el7.x86_64
452,835

python-requests/2.6.0 CPython/2.6.6 Linux/2.6.32-754.35.1.el6.x86_64
441,748

Figure 42: Top HTTP Credentials

H1 2022 Top HTTP Credentials

admin:admin 47,932 18%
admin: 29,092 11%
admin:1234 28,609 11%
admin:123456 27,468 10%
admin:{12213BD1-69C7-4862-843D-260500D1DA40} 32,202 12%
admin:password 28,940 11%
admin:12345 24,692 9%
admin:123 22,818 9%
admin:1234567890 22,415 8%

Top SSH Usernames

The top usernames used during SSH authentication provide information on the most sought for and most likely services that are vulnerable to Brute Forcing. Amongst the top 10 are 'Postgres', 'Oracle', 'Git', and 'MySQL'.

Figure 43: Top SSH Usernames

H1 2022 Top SSH Usernames

List of Figures

Methodology and Sources

The data for DDoS events and volumes 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.

Radware's Global Deception Network provides detailed events and payload data on a wide range of attacks and serves as a basis for the "Unsolicited Network Scanning and Attack Activity" section.

The data for web application attacks was collected from blocked application security events from the Radware Cloud WAF Service. Collected events were based solely on automatically detected and known vulnerability exploits and exclude any events that might be blocked or reported by custom rules added to a web application policy by managed services and/or customers.

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.

Editors

Pascal Geenens | Director of Threat Intelligence
Daniel Smith | Head of Threat Research

Executive Sponsors

Shira Sagiv | VP Portfolio Marketing
Ron Meyran | Sr Director of Corporate Enablement

Production

Colin Beasty | Corporate Marketing Manager
Dasnet Garcia | Brand Marketing Manager
Gerri Dyrek | Director of Public Relations

radware