radware

Report

2022 Global Threat Analysis Report

Radware's 2022 Global Threat Analysis Report reviews the year's most important cybersecurity events and provides detailed insights into the attack activity of 2022. The report leverages intelligence provided by Radware's Threat Intelligence Team, and network and application attack activity sourced from Radware's Cloud and Managed Services, Global Deception Network and Threat Research team.

Contents

Executive Summary

During 2022, cybersecurity threats continued to evolve and become more sophisticated. Ransomware continued to be a major issue, with many organizations falling victim to these attacks. Cybercriminals increasingly targeted cloud infrastructure and remote workers. Social engineering attacks, such as phishing and business email compromise (BEC) scams, remained popular among attackers. Additionally, a number of high-profile data breaches resulted in the loss of sensitive personal and financial information. In response to these threats, organizations and governments stepped up their efforts to improve cybersecurity and protect against attacks.

Distributed Denial of Service (DDoS) attacks have been a common and growing threat for many years, causing significant disruption to organizations. In 2022, DDoS attacks continued to be a major issue. The cyber landscape was marked by a sharp increase in malicious activities and DDoS attacks, particularly targeting organizations in the financial, healthcare, and technology sectors. Radware's Cloud DDoS Service recorded a 233% growth in blocked malicious events compared to the previous year, with the number of DDoS attacks growing by 150%. The total attack volume reached 4.44PB, a 32% increase from 2021. The largest recorded attack in 2022 was 1.46Tbps, a staggering 2.8 times larger than the largest attack recorded in 2021.

The frequency of attacks also saw a significant uptick, with organizations mitigating an average of 29.3 attacks per day in Q4 of 2022, a 3.5x increase compared to the previous year. EMEA was the most targeted region, with over half of all attacks aimed at organizations located in the region. The financial sector bore the brunt of the attacks globally, accounting for 52.6% of the overall attack activity. The technology sector also saw a significant share of attacks at 20.3%, with healthcare third at 10.5%.

DDoS Attack Trend Highlights

Number of malicious events **blocked by Radware's Cloud DDoS Service**

↑233%

1.5x

The number of **DDoS attacks grew by 150%**

Total attack volume in 2022

4.44PB

An increase of 32% compared to 2021

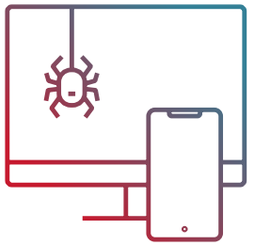
The Americas saw a substantial increase in malicious activities, with a 328% growth in blocked malicious events and a 212% increase in DDoS attacks compared to 2021. The largest attack recorded in 2022 in this region was 1.46Tbps, 6.8 times larger than the largest attack of 214Gbps recorded in 2021. The finance and healthcare sectors were the most targeted, with 31.5% and 23.9% of the overall attack activity, respectively.

In contrast, the EMEA region saw a decrease in attack volume of 44%. However, the frequency of attacks increased with organizations mitigating an average of 45 attacks per day in Q4 of 2022, a 4x increase compared to the previous year. The financial sector continued to be the most targeted, with 70.6% of the attack activity, followed by the technology sector at 16%.

The increase in cyberattacks in 2022 can be attributed to a number of geopolitical events that took place during the year. The ongoing tensions between major world powers led to an increase in state-sponsored cyberattacks and espionage activities. Additionally, the ongoing global shift towards digitalization and remote work due to the pandemic created new vulnerabilities for attackers to exploit.

Web application and API attacks grew exponentially throughout 2022, resulting in an increase of 128% compared to 2021, a significantly faster growth compared to the 88% growth in 2021. Predictable resource location attacks targeting the hidden content and functionality of web applications accounted for almost half of attack activity in 2022. Code injection and SQL injection attacks represented more than a quarter of web application attacks. Retail & wholesale trade, high tech and carriers represented 60% of all blocked web application attacks.

Overall, the threat landscape in 2022 was a complex and rapidly evolving one, requiring organizations to have a comprehensive security strategy in place to protect against the wide range of threats they faced.



Web application and API attacks grew exponentially throughout 2022, resulting in an increase of 128% compared to 2021, a significantly faster growth compared to 88% growth in 2021

Denial-of-Service Attack Activity

The total number of malicious events blocked by Radware's Cloud DDoS Service in 2022 grew by 233%, compared to 2021. The number of DDoS attacks grew by 150%. The total attack volume in 2022 was 4.44PB, an increase of 32% compared to 2021. The largest attack recorded in 2022 was 1.46Tbps, 2.8 times compared to the largest attack of 520Gbps in 2021.

Attack Trends

Throughout the year, the number of DDoS attacks per customer kept increasing every quarter, from less than 1,000 attacks per quarter in Q4 of 2021 to over 2,500 attacks per customer in Q4 of 2022. By the end of 2022, the average number of attacks mitigated per customer increased by over three times. For comparison, in 2021 the average number of attacks per customer in Q4 of 2020 was slightly higher than the number of attacks in Q4 of 2021. The busiest quarter of 2021 (Q2) saw a rise of almost 50% in the average number of attacks per customer.

The trend for the number of attacks to increase is significant and concerning. To put this in perspective, the number of attacks a customer witnessed per day at the end of 2021 was 8.4[1], compared to 29.3 attacks on average per day by the end of 2022, a 3.5x increase.

The attack volume per customer did not grow at the same rate as the number of attacks. The average total attack volume per customer in 2022 was 15TB, a modest increase of 14.3% compared to 2021.

Figure 1: Malicious events, DDoS attacks, volume and largest attack 2022 vs 2021

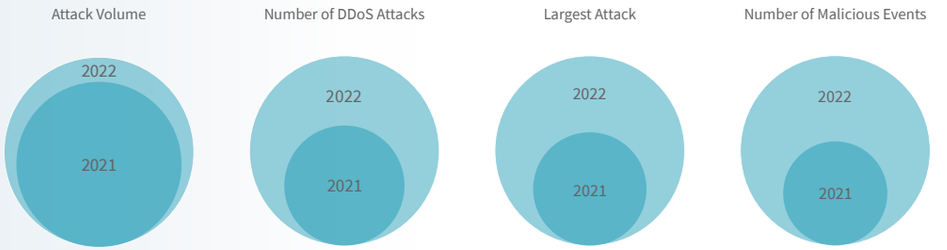


Figure 2

Number of attacks per quarter, normalized per customer

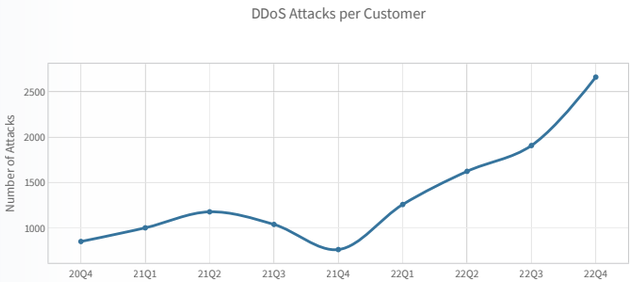
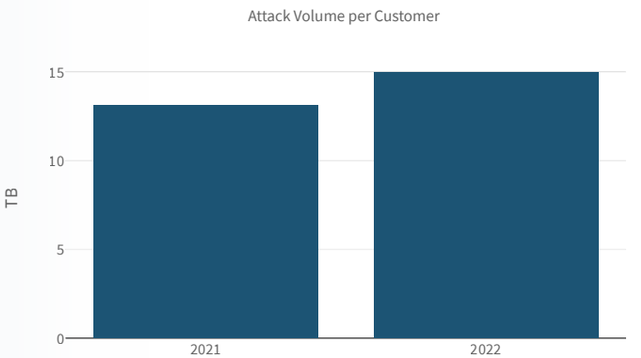


Figure 3

Yearly attack volume per customer



1. To calculate the average number of attacks per day, the average number of attacks per quarter is divided by 91 (number of days in a quarter for 2 x 30 + 1 x 31)

Attack Sizes

To compare the characteristics of attacks recorded in 2022 and 2021, these were divided into buckets by attack size bracket. An upper and lower attack size defines each bracket and the attacks in the bucket.

Compared to 2021, in 2022 there was a significant increase in the number of attacks below 10Gbps, and a moderate but not insignificant increase in attacks above 250Gbps. The average size of attacks above 500Gbps was significantly larger in 2022.

Attacks in 2022 were pushed out from the center to both ends of the attack size spectrum. The increase in attacks was most significant at the lower end of the attack size spectrum. In the center of the attack size spectrum, there was a moderate decrease in attacks, while the higher end of the spectrum showed a moderate increase.

On average, smaller attacks tend to be shorter. Attacks below 1Gbps last on average 4 minutes, while attacks between 50 and 100Gbps last on average 8.67 hours. The longest attacks seem to gather between 100 and 250Gbps, where on average the attacks lasted 66 hours, or 2.75 days.

While the increase in the higher end of the attack size spectrum was less significant, the attacks did hit significantly harder compared to the biggest attacks in 2021.

Figure 4: Number of attacks by attack size bracket

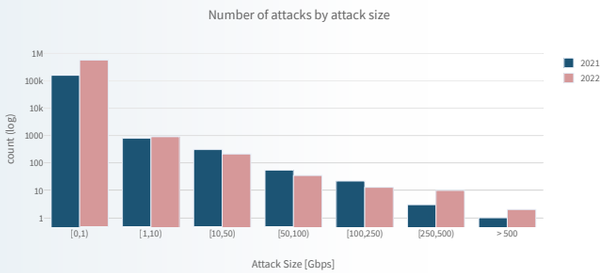
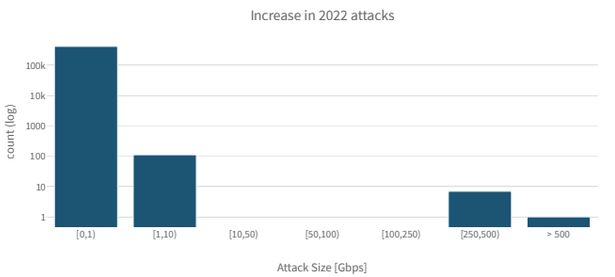


Figure 5: Change in number of attacks per attack size bracket for 2022 compared to 2021



The longest attacks seem to gather between 100 and 250Gbps, where **on average the attacks lasted 66 hours, or 2.75 days**

Figure 6: Average attack duration per attack size

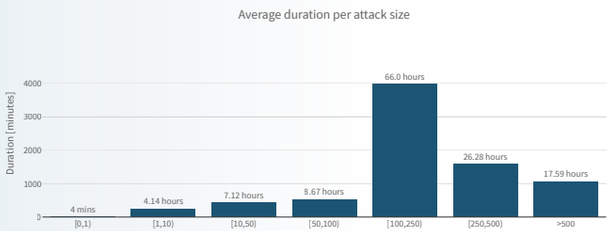
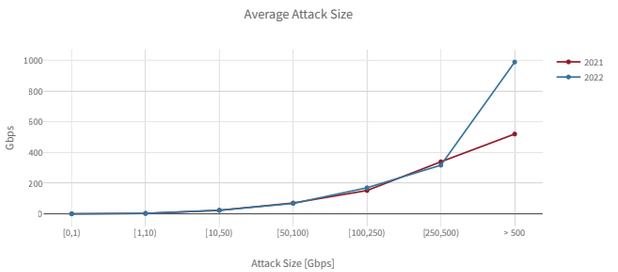


Figure 7: Average attack size per size bracket



Regions and Industries

In 2022, more than half of the attacks targeted organizations in EMEA. The Americas accounted for 35% of the attacks while 7.11% of the attacks targeted APAC organizations.

The most significant attack volumes targeted customers in the Americas, accounting for 84% of the total attack volume. EMEA customers, representing more than half of the number of attacks, accounted for 15.2% of the total attack volume.

Finance was the most attacked industry in 2022, with 52.6% of the overall attack activity and a frequency of attacks growing a modest 2.4% compared to 2021. Technology represented 20.3% of the overall attack activity and suffered nearly the same number of attacks (+0.5%) compared to 2021. Healthcare was the third most attacked industry with 10.5% of attacks and was slightly more frequently the target of attackers (+1%) compared to 2021. Other industries under attack in 2022 included communications (4.47%), government (3.9%) and research & education (2.28%).

Industrials were attacked 72% more often in 2022 compared to 2021. Energy and research & education were the second and third most significant growth industries when comparing attacks in 2022 to 2021.

Figure 8:

Blocked attacks per region for 2022

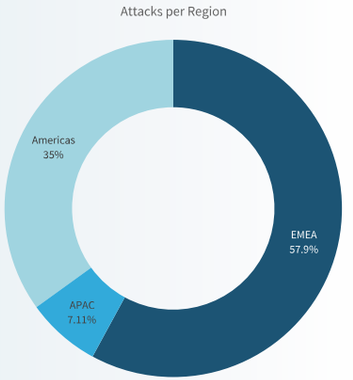


Figure 9:

Blocked attack volume per region for 2022

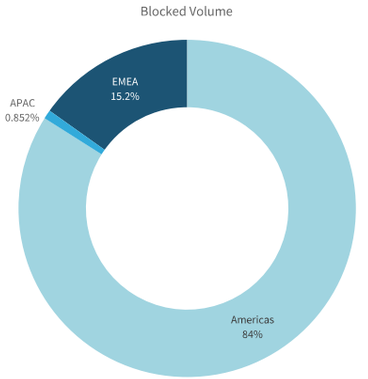


Figure 10:

Most attacked industries in 2022

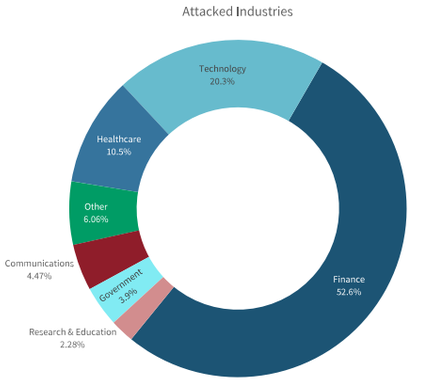
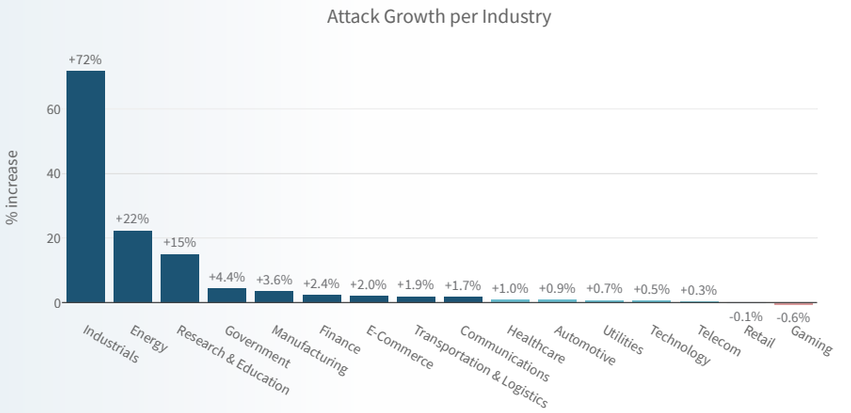


Figure 11: Attack growth per industry in 2022, compared to 2021



Finance was the most attacked industry in 2022, with 52.6% of the overall attack activity and a frequency of attacks growing 2.4% compared to 2021

The Americas

In 2022, the number of malicious events targeting customers in the Americas blocked by Radware's Cloud DDoS Service grew by 328%, compared to 2021. The number of DDoS attacks grew by 212%. The total attack volume in 2022 increased by 110% compared to 2021. The largest attack recorded in 2022 was 1.46Tbps, 6.8 times greater than the largest 2021 attack of 214Gbps.

The average number of attacks per customer in the Americas ended 2021 with 603 attacks per quarter and grew steeply to 1,420 attacks in Q1 of 2022. The number of attacks per customer peaked at 2,142 per quarter in Q3 and ended with 1,831 attacks per customer per quarter in Q4 of 2022. On average, organizations located in the Americas mitigated 20.1 attacks per day[2] in Q4 of 2022, a 3x increase compared to 6.6 attacks per day in Q4 of 2021.

The average yearly attack volume blocked by Americas organizations increased by 88.1% in 2022 to an average of 34.44TB per customer.

Figure 12: Malicious events, DDoS attacks, attack volume and largest attack 2022 vs 2021, The Americas

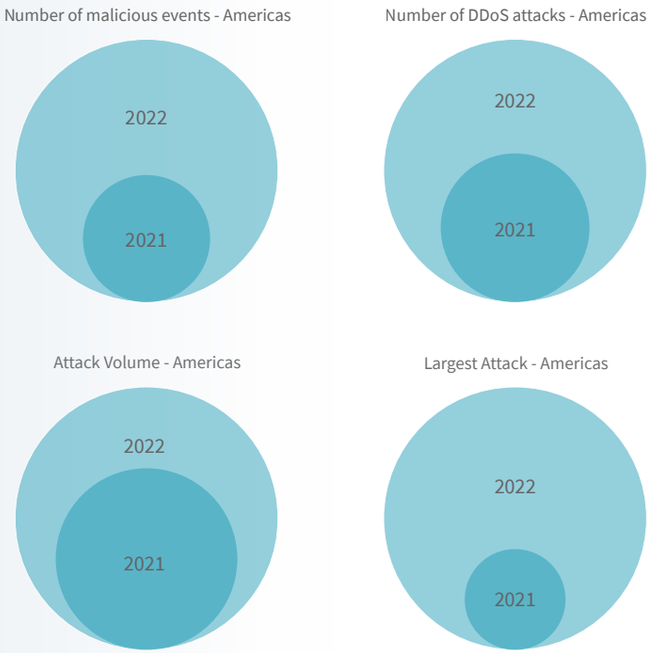
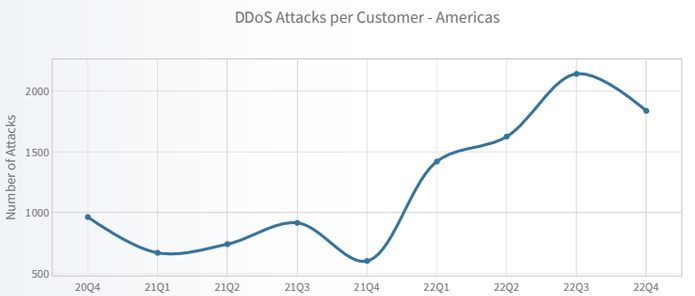


Figure 13: Average number of attacks per Americas organization, per quarter



The number of DDoS attacks grew by 212%. The total attack volume in 2022 increased by 110% compared to 2021. **The largest attack recorded in 2022 was 1.46Tbps**, 6.8 times greater than the largest 2021 attack of 214Gbps

2. To calculate the average number of attacks per day, the average number of attacks per quarter is divided by 91 (number of days in a quarter for 2 x 30 + 1 x 31)

Finance was the most attacked industry in the Americas in 2022, with 31.5% of attack activity, and the frequency of attacks growing in line with global growth of 2.4% compared to 2021. Healthcare represented 23.9% of the attack activity, a slight increase of 1.7% compared to 2021. Technology was the third most attacked industry in the Americas with 17.2% of the attacks, slightly more frequently the target of attackers (+1.5%) compared to 2021. Other industries attacked in the Americas in 2022 included communications (12.3%), research & education (4.41%) and government (2.75%).

Industrials were attacked 72% more often in 2022 compared to 2021. Research & education and government were the second and third most significant growth industries when comparing attacks in 2022 to 2021.

Figure 14:

Average yearly attack volume for Americas organizations

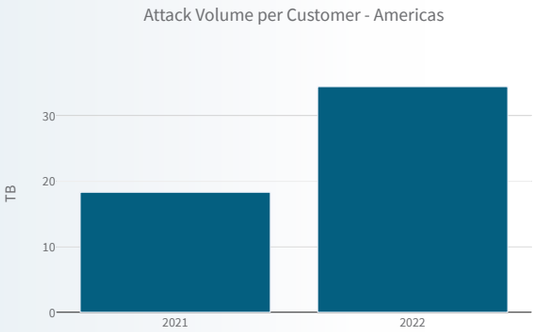


Figure 15:

Most attacked industries in the Americas in 2022

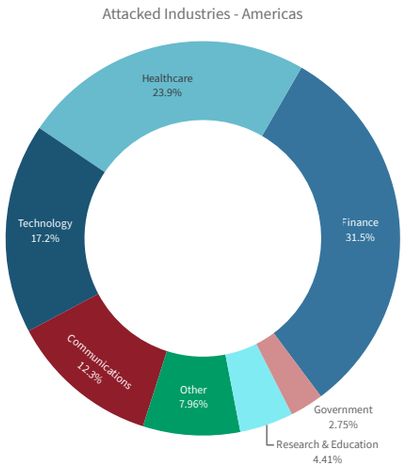
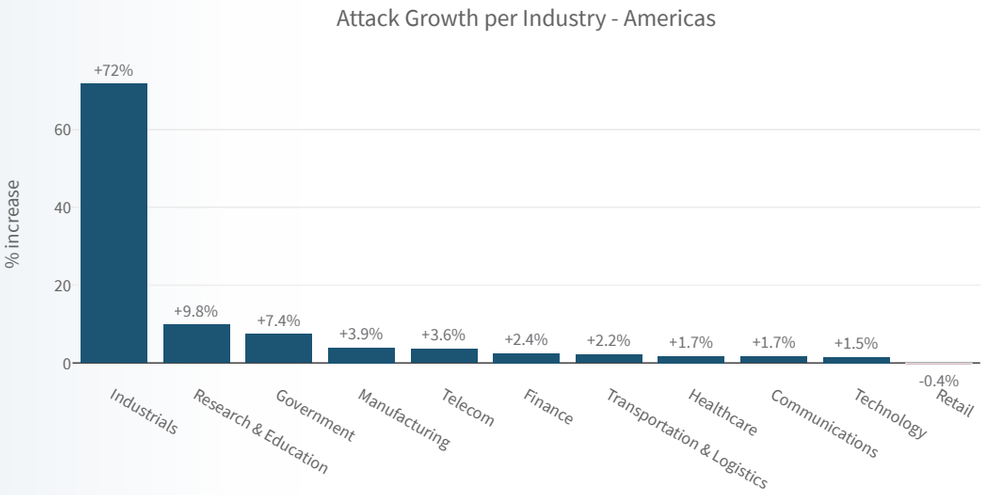


Figure 16: Attack growth per industry in the Americas in 2022, compared to 2021



Europe, Middle East and Africa

In 2022, the number of malicious events targeting EMEA customers blocked by Radware's Cloud DDoS Service grew by 158%, compared to 2021. The number of DDoS attacks grew by 140%. The total attack volume in 2022 decreased by 44% compared to 2021. The largest attack recorded in 2022 was 518.7Gbps, similar in size to the largest 2021 attack of 519.6Gbps.

The average number of attacks per customer in EMEA almost tripled between the first and last quarter of the year. In Q4 of 2021, EMEA organizations mitigated on average 1,029 attacks or 11.3 attacks per day[3]. In Q4 of 2022, EMEA organizations mitigated on average 4,093 attacks, or 45 attacks per day, a 4x increase compared to Q4 of 2021.

In 2022, the average yearly attack volume blocked by organizations in EMEA decreased by 49.5% to an average of 6.50TB per customer.

Figure 17: Malicious events, DDoS attacks, attack volume and largest attack 2022 vs 2021, EMEA

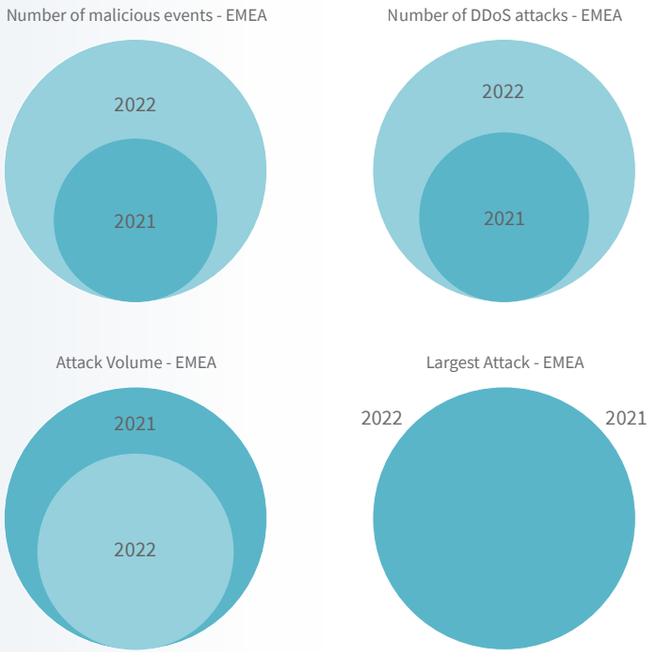
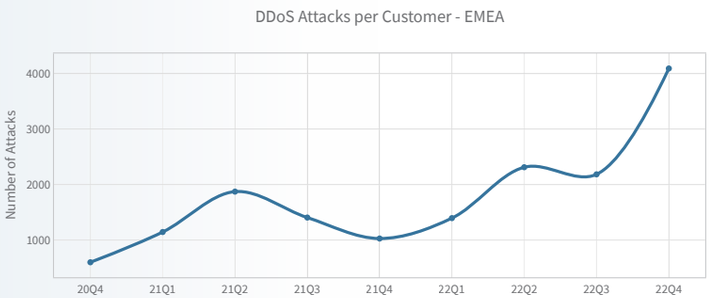


Figure 18: Average number of attacks per EMEA organization, per quarter



In 2022, the number of **DDoS attacks targeting EMEA organizations grew by 140%.** In Q4 of 2022, EMEA organizations blocked on average 45 attacks per day, a 4x increase compared to Q4 of 2021

3. To calculate the average number of attacks per day, the average number of attacks per quarter is divided by 91 (number of days in a quarter for 2 x 30 + 1 x 31)

In 2022, finance was the most attacked industry in EMEA with 70.6% of the attack activity. This represents a 2.6% rise year-over-year, a slightly faster growth compared to the global rate of 2.4%. Technology represented 16% of the attack activity, a slight decrease of 0.1% compared to 2021. Government was the third most attacked industry in EMEA with 4.09% of the attacks and the fastest growing industry with 11% more attacks compared to 2021. Other notable industries in 2022 included healthcare (3.32%), research & education (1.28%) and telecom (1.13%). E-commerce and healthcare were the second and third most significant growth industries when comparing attacks in 2022 to 2021.

Figure 19: Average yearly attack volume for EMEA organizations

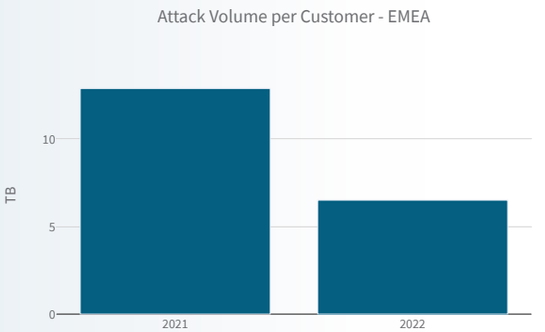


Figure 20: Most attacked industries in EMEA in 2022

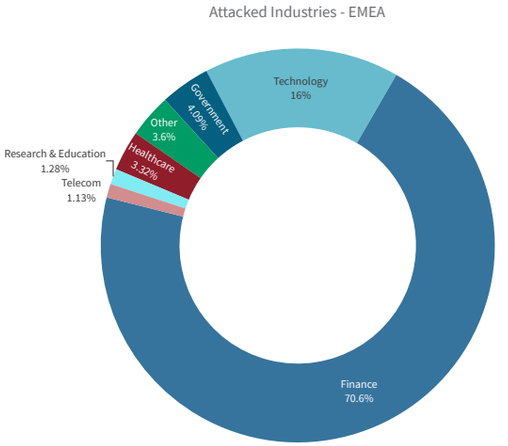
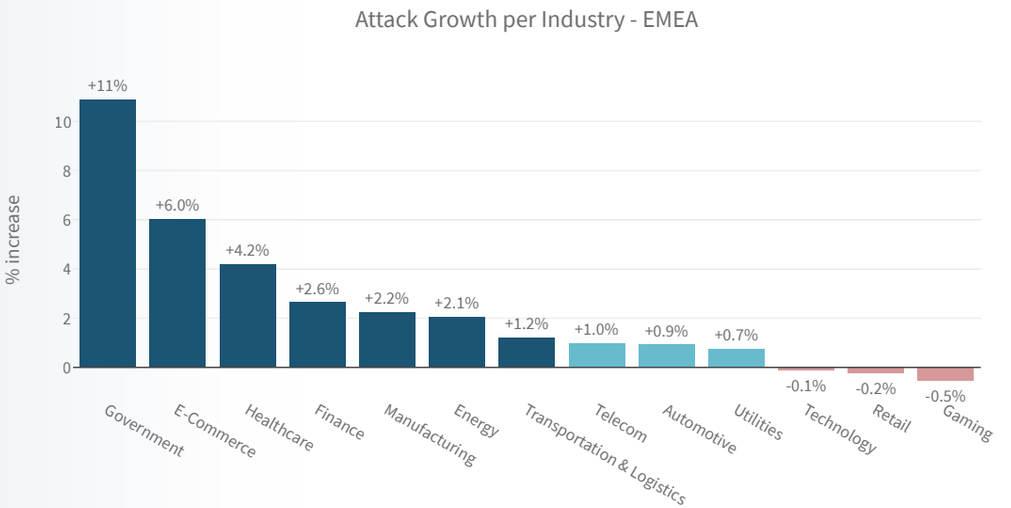


Figure 21: Attack growth per industry in EMEA in 2022 compared to 2021



Asia Pacific (APAC)

In 2022, the number of malicious events targeting APAC customers blocked by Radware's Cloud DDoS Service grew by 207% compared to 2021. The number of DDoS attacks grew by 51%. The largest attack recorded in 2022 was 74.1Gbps, a third the size of the largest attack of 228Gbps in 2021.

The average number of attacks per APAC organization started 2022 slightly above Q4 of 2021. The average number reached a minimum of 215 attacks per quarter in Q2 and swiftly rose to an average of 1,110 attacks per organization in Q4 of 2022. In Q4 of 2021, APAC organizations mitigated on average 405 attacks, or 4.5 attacks per day[4]. In Q4 of 2022, APAC organizations mitigated on average 1,110 attacks, or 12.2 attacks per day, a 2.7x increase compared to Q4 of 2021.

Figure 22: Malicious events, DDoS attacks and largest attack 2022 vs 2021, APAC

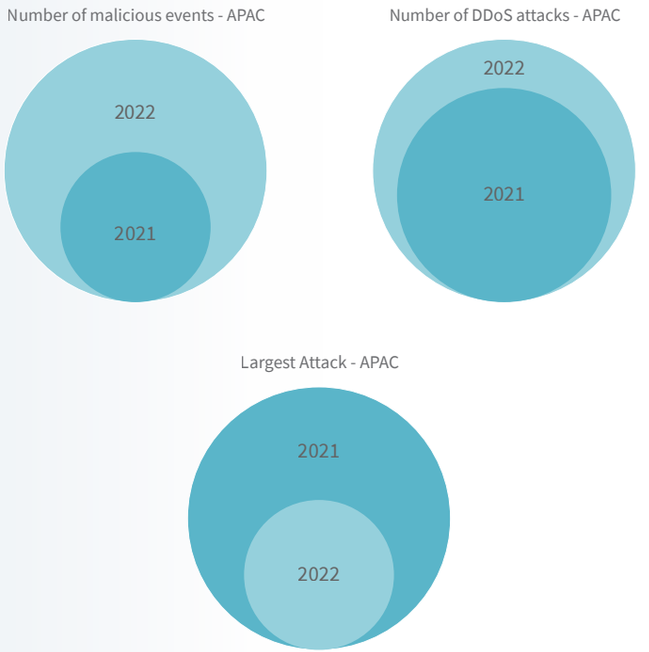
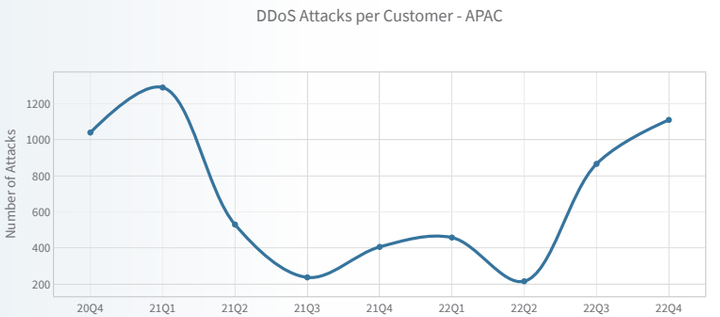


Figure 23: Average number of attacks per APAC organization, per quarter



In 2022, the number of DDoS attacks targeting APAC organizations grew by 51%. **In Q4 of 2022, organizations in APAC mitigated on average 12.2 attacks per day, a 2.7x increase compared to Q4 of 2021**

4. To calculate the average number of attacks per day, the average number of attacks per quarter is divided by 91 (number of days in a quarter for 2 x 30 + 1 x 31)

Technology was the most attacked industry in APAC in 2022, with 70.2% of the APAC attack activity representing a growth of 9.9% year-over-year, a significantly faster growth compared to the global 0.5%. Finance represented 9.35% of the attack activity, a slight decrease of 0.4% compared to 2021. Government was the third most attacked industry in APAC with 7.92% of attacks, slightly up by 0.4% compared to 2021. Other industries attacked in 2022 included retail (3.46%), healthcare (2.61%) and communications (2.3%).

In 2022, APAC organizations in the manufacturing and technology industries were attacked 10% more often compared to 2021. Communications and retail were the third and fourth most significant growth industries when comparing attacks in 2022 to those in 2021.

Figure 25:

Most attacked industries in APAC in 2022

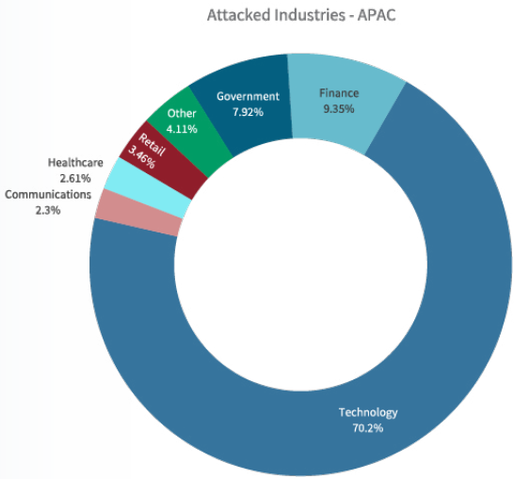
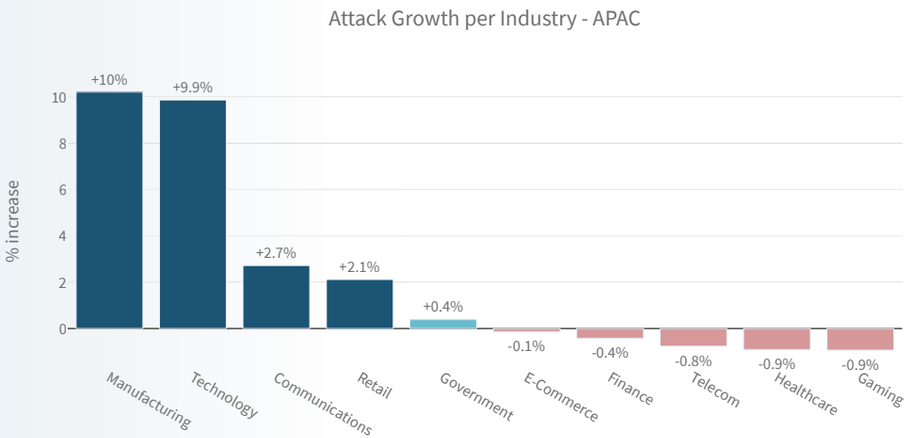


Figure 26: Attack growth per industry in APAC in 2022, compared to 2021



Attack Protocols and Applications

User Datagram Protocol (UDP) is by far the most leveraged protocol in 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. TCP SYN and out-of-state packets can be leveraged for volumetric attacks, but TCP is typically the most used protocol for exhausting resources on devices and servers.

HTTP, DNS, HTTPS and NTP were the most targeted applications. Online applications were the most obvious targets for attacks in 2022, representing 62.5% of the targeted applications. DNS represented 26.4% of the targeted applications, unsurprising because DNS is an important way of targeting online applications. If the name of a web resource cannot be resolved to an IP address through DNS, the resource will be inaccessible and appear offline even though the service is available and able to process new requests and transactions.

By a significant margin, the top attack vector was UDP flood (78.1%), followed by UDP fragment flood (5.73%). TCP attacks through several variations of flag attacks completed the vectors above 1% comprising TCP SYN (5.53%), TCP Out-of-State (5.27%), TCP SYN-ACK (2.27%) and TCP RST (1.59%) floods.

Attackers leverage amplification services that are publicly exposed on the internet. If it's UDP and it is exposed to the internet, it can be weaponized for DDoS amplification attacks. The motivation to weaponize a specific protocol depends on the amplification factor (AF) – the ratio between the size of the request and the reply – and the number of available or exposed services on the internet. A higher AF means a more efficient attack. More exposed services represent a larger total aggregate bandwidth and a higher diversity in source IPs in the attack traffic, making detection (a little) harder.

Figure 27: Protocols leveraged by attacks in 2022

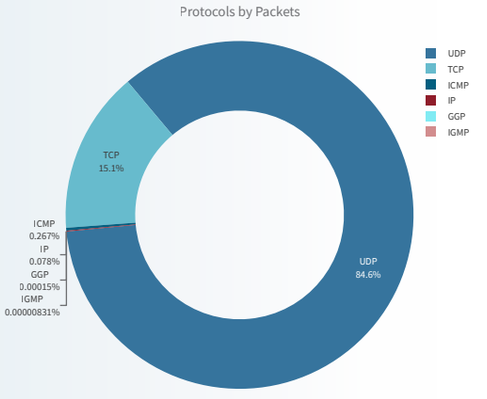


Figure 28: Top targeted applications by volume

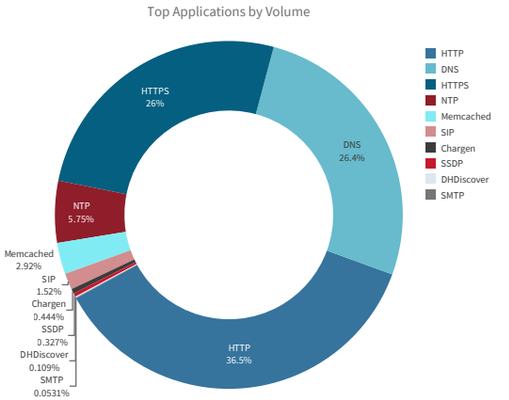
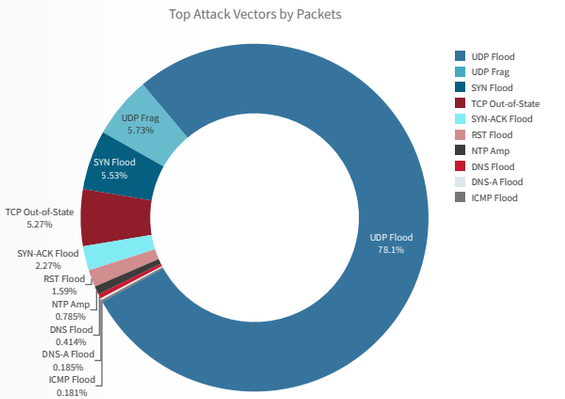


Figure 29: Top attack vectors by packets



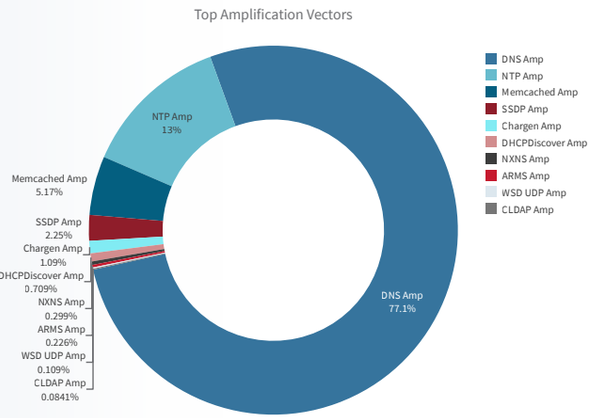
Some of the most important and top amplification vectors and their associated maximum amplification factor are listed in Table 1.

DNS amplification was the amplification attack vector that generated the most volume in 2022, representing 77.1% of the total amplification volume. NTP amplification was the second most abused amplification attack vector, accounting for 13% of the volume. Smaller volumes were generated by Memcached, SSDP, Chargen, DHCP Discover (IPv6), NXNS, ARMS, WSD and CLDAP.

Table 1: DDoS amplification attack vectors

Amplification Vector	Amplification Factor	Port
NTP	500x	UDP/123
DNS	160x	UDP/53
SSDP	30x	UDP/1900
Memcached	50,000x	UDP/11211
Chargen	1,000x	UDP/19
ARMS	30x	UDP/3283
CLDAP	50x	UDP/398
DHCPDiscover	25x	UDP/37810
SNMP	880x	UDP/161
RDP	80x	UDP/3389
CoAP	30x	UDP/5683
mDNS	5x	UDP/5353
WSD	500x	UDP/3702, TCP/3702
Plex (PMSSDP)	5x	UDP/32410

Figure 30: Top amplification attack vectors



HTTPS Attack Vectors

HTTPS is still a crucial port for online web applications and services. Even with QUIC (a UDP-based protocol) gaining traction, the most obvious way to impact web applications and APIs is by targeting TCP port 443. UDP floods are the number one attack vector leveraged against HTTPS services. While this might seem odd since HTTPS is TCP-based, there is good reason to expect UDP floods. When the objective of an attacker is to flood the service and saturate the internet connection, UDP is the preferred protocol as it can leverage multiple amplification services to generate high-bandwidth attacks.

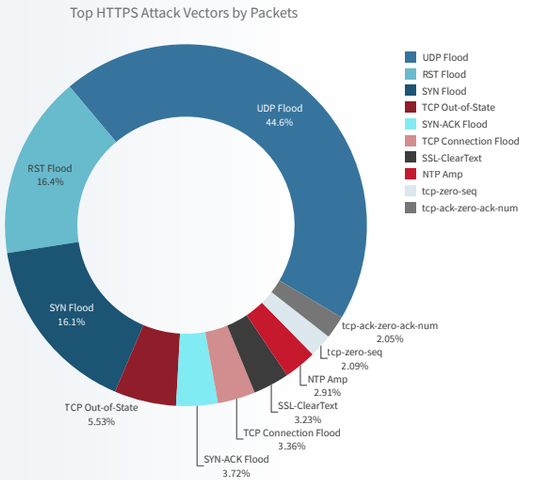
When targeting the web server itself, attackers will typically resort to TCP-based attack vectors such as RST, SYN, SYN-ACK, Out-of-State TCP floods, or even TCP connection floods that send clear text (HTTP) to a service expecting encrypted communications.

HTTP Attack Vectors

While most internet communications used by B2B and e-commerce are encrypted, there is still a plethora of internet devices that expose unencrypted HTTP services on the internet. Referred to as IoT (Internet of Things), these consist of modems, routers, and IP cameras. These typically unmanaged devices are left exposed by unaware home users or businesses and are targeted by attackers for all kinds of malicious activities, including exploiting compromised devices in large-scale botnets to conduct highly distributed denial-of-service attacks.

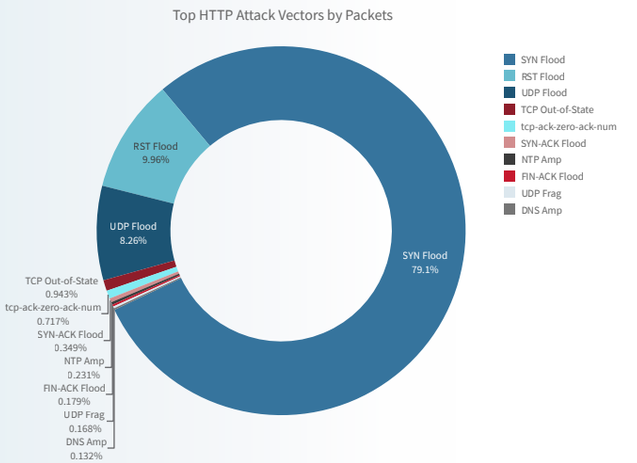
While HTTP on port 80 should no longer be used in mission critical environments, there is still a good amount of DDoS activity targeting it. In 2022, the most common attack vectors included different types of TCP flag attacks such as SYN, RST, SYN-ACK, FIN-ACK, and Out-of-State floods, but also amplified UDP-based floods.

Figure 31: Top attack vectors targeting HTTPS



HTTPS services were **predominantly targeted by UDP Floods**

Figure 32: Top attack vectors targeting HTTP



HTTP services were **most targeted by TCP SYN floods**

DNS Attack Vectors

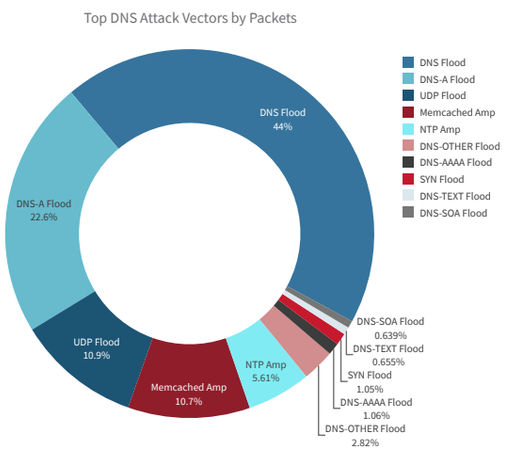
The Domain Name System (DNS) is the forgotten cornerstone of the internet. DNS is responsible for resolving hostnames into IP addresses. If DNS fails, the online applications, services, and third-party web APIs many applications depend on become unavailable. While the root servers of the hierarchical DNS infrastructure can resist most attacks, the authoritative servers can be the subject of denial-of-service attacks. Taking out the authoritative DNS server of a domain will disable name resolution for the domain and result in inaccessible applications and services for that domain. In some attacks, the recursive caching DNS servers can be leveraged to amplify attacks against the authoritative domain servers, such as Pseudo Random Subdomain (PRSD) floods, also known as the 'DNS water torture' attack.

Besides online web applications and APIs, DNS is one of the services most targeted by DDoS attackers. DNS uses both TCP and UDP; TCP for zone transfers between servers and UDP for name resolution and querying servers for different types of records. The most common DNS record types are A, AAAA, CNAME, MX and TXT. A DNS A record provides the translation from a hostname to an IPv4 address. A DNS AAAA record provides the translation of a hostname to an IPv6 address. The DNS CNAME (Canonical Name) record can be used as a hostname alias and points to the original hostname in the same or another domain or subdomain, but does not translate to an IP address. The DNS Mail Exchanger (MX) record points to the SMTP email servers for the domain. The DNS text (TXT) record is a freeform record that can resolve to any configured string. Some spam prevention systems, such as the Sender Policy Framework (SPF), rely on TXT records to verify ownership of a domain.

It should be clear that DNS is both essential for ensuring the good working of the internet and critical for keeping businesses online. As such, DNS provides an interesting target for attackers attempting to disrupt online businesses.

Since DNS is UDP-based and unauthenticated, it can be leveraged as a DDoS amplification service (see earlier discussion on page 14). Any type of query resulting in large responses is preferred for amplification attacks. Considering that DNS primarily uses UDP for the client side, UDP floods and UDP amplification attacks such as NTP amplification or DNS amplification will be the most effective way to disrupt service to clients.

Figure 33: Top attack vectors targeting DNS



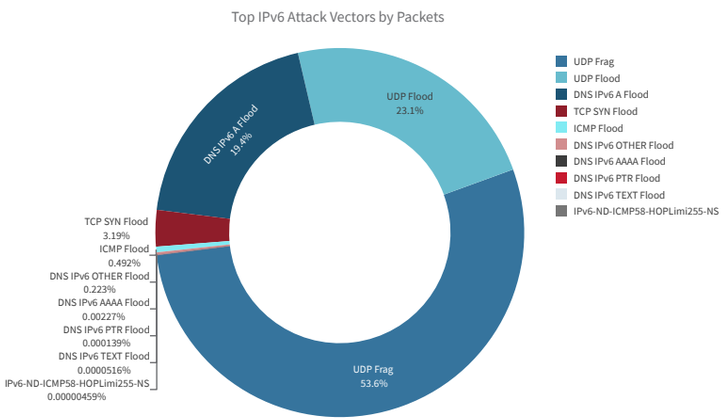
The Domain Name System (DNS) is the forgotten cornerstone of the internet. Taking out the DNS server of a domain will result in inaccessible applications and services for that domain

IPv6 Attack Vectors

While IPv6 attack vectors represent less than 1% of the total attack activity in Radware's Cloud DDoS Service, it's still worth understanding the top attack vectors targeting IPv6-based protocols and applications.

As with its IPv4 counterpart, IPv6 is mainly leveraged in UDP and UDP fragmentation floods. The number one application targeted with IPv6 is DNS through several types of query floods. New IPv6 protocol features are also subject of attacks, such as IPv6 Neighbor Discovery ICMP floods.

Figure 34: Top IPv6 attack vectors



Attack Vector Characterization

A DDoS attack consists of one or more attack vectors. Attack vectors can change during an attack, increasing its complexity. In this section individual attack vectors are analyzed to understand and characterize the nature of the DDoS attack threat landscape.

To compare the size evolution, attack vectors are split into three categories based on their attack size, expressed in bits per second. Small attacks are those below 1Gbps, while large attacks are those above 100Gbps. By normalizing the number of vectors in each size category against 2020, their relative vector size evolution can be compared.

The number of attack vectors below 1Gbps increased faster than exponentially year-on-year, from just below 2x in 2021 to over 5x in 2022. The number of attack vectors above 100Gbps increased almost 3x in 2021 and kept increasing, albeit at a slower than linear rate, to a 3.75x increase in 2022 compared to 2020. The number of mid-sized attack vectors, between 1Gbps and 100Gbps, remained relatively unchanged over time, with a 1.31x increase in 2021 and ending with 1.29x increase in 2022 compared to 2020.

The average duration of an attack vector varies with the attack bandwidth (bits per second) and the throughput (packets per second). The longest attack vectors were also the biggest attack vectors in terms of bandwidth and throughput. On average, UDP attack vectors above 100Gbps lasted 147 minutes or about 2.5 hours. In contrast, attacks above 100Gbps, consisting of an average of 9.32 vectors per attack (see below), lasted on average between 18 and 66 hours (see Figure 6).

Figure 35: Relative attack vector size evolution

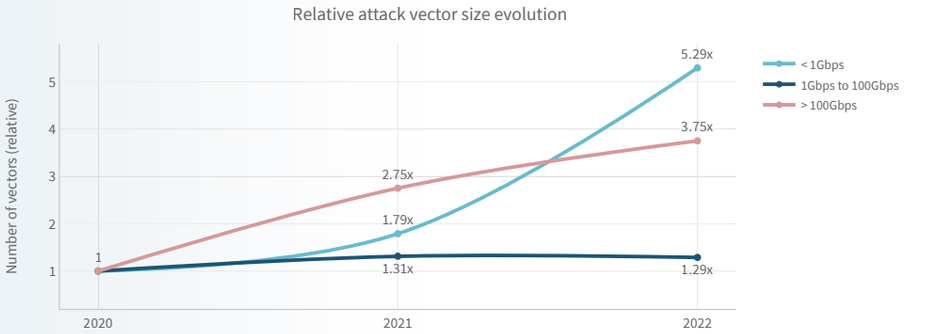


Figure 36: Average attack vector duration for TCP and UDP as a function of its bandwidth

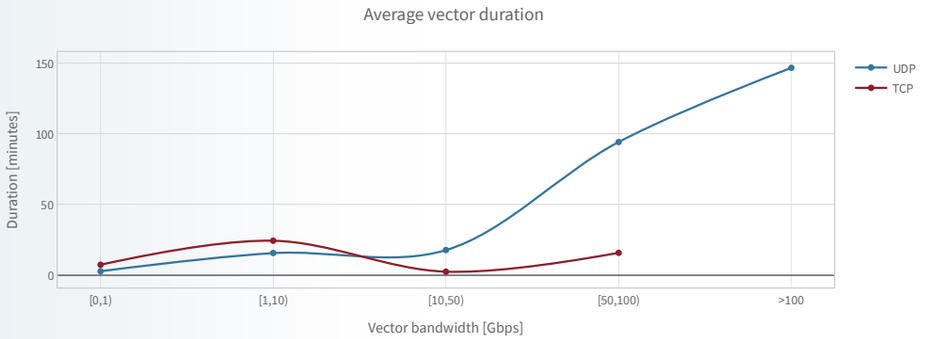
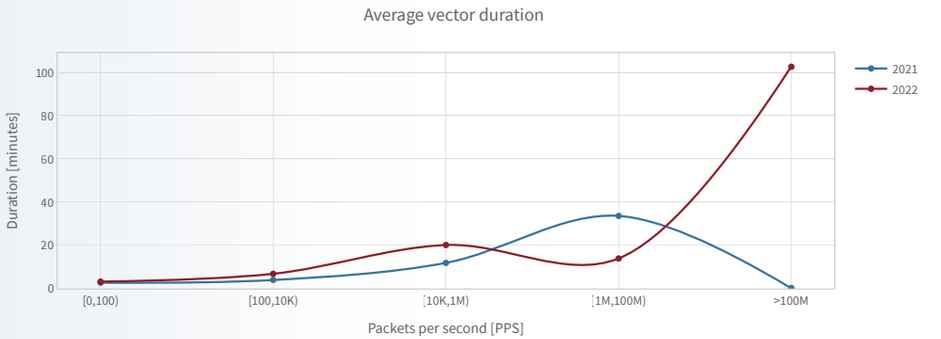


Figure 37: Average attack vector duration for TCP and UDP as a function of its packet rate



The attack bandwidth is governed by the packet rate and the size of the packets. Average packet size is an important metric to maximize the impact of an attack depending on the resources available to the attackers or the victims. Attacks will typically favor larger packets to increase the bandwidth of the attack when packet rates are constrained by the available processing resources. When attempting to exhaust the processing resources of network components and servers, the packet rate will be the most effective tactic. Consequently, bandwidth can be reduced by leveraging smaller packets without impacting the effectiveness of the attack.

Figure 38: Average attack vector packet size for TCP and UDP as a function of its bandwidth

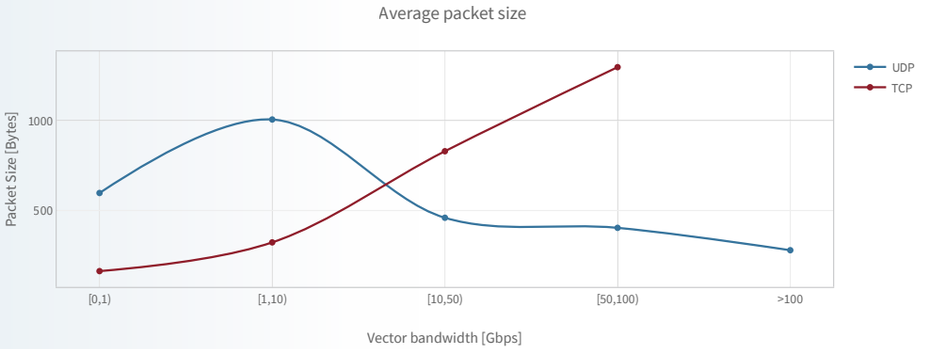
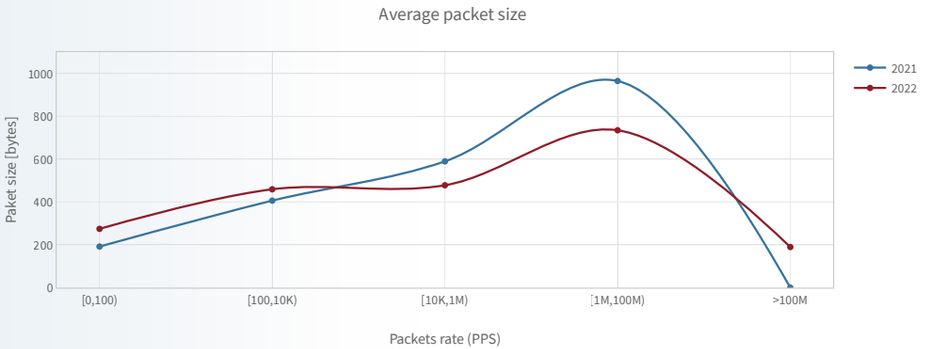


Figure 39: Average attack vector packet size for TCP and UDP as a function of its packet rate



Attack Complexity

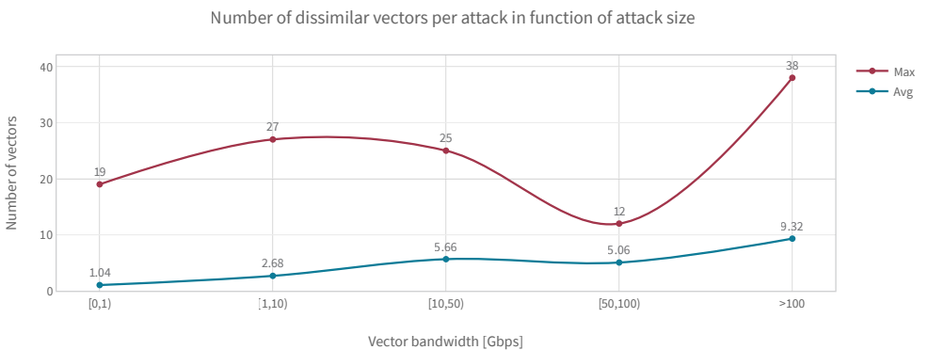
While a single attack vector can be devastating, attackers will typically leverage multiple and dissimilar vectors to increase the impact and confuse detection to make attack mitigation harder. When attackers leverage multiple amplification servers and protocols, a single attack will consist of several dissimilar concurrent attack vectors. Attackers will also change attack vectors over time to evade mitigation by manually crafted access control lists. While changing attack vectors is typically not sufficient to evade automated DDoS mitigation services, it can still be effective against targets that have inadequate DDoS protection in place.

An attack is considered more sophisticated or complex when it leverages a greater number of dissimilar attack vectors. Attacks that make use of multiple concurrent or changing attack vectors will make mitigation harder. Fast shifts and high numbers of concurrent vectors are impossible to mitigate without automated mitigation solutions.

The average complexity of attacks in 2022 increased along with the attack size. Since the average number of attack vectors in a single attack can't be smaller than one, smaller attacks exhibit a more isolated character as their average vectors per attack becomes closer to this number. Attacks above 1Gbps on average had more than two dissimilar attack vectors per attack which doubled in number for attacks above 10Gbps. Attacks above 100Gbps had on average more than nine dissimilar attack vectors with the most complex attacks leveraging 38 dissimilar attack vectors.

Attacks above 1Gbps on average had more than two dissimilar attack vectors per attack which doubled in number for attacks above 10Gbps. Attacks above 100Gbps had on average more than nine dissimilar attack vectors with **the most complex attacks leveraging 38 dissimilar attack vectors**

Figure 40: Number of dissimilar attack vectors per attack as a function of attack size



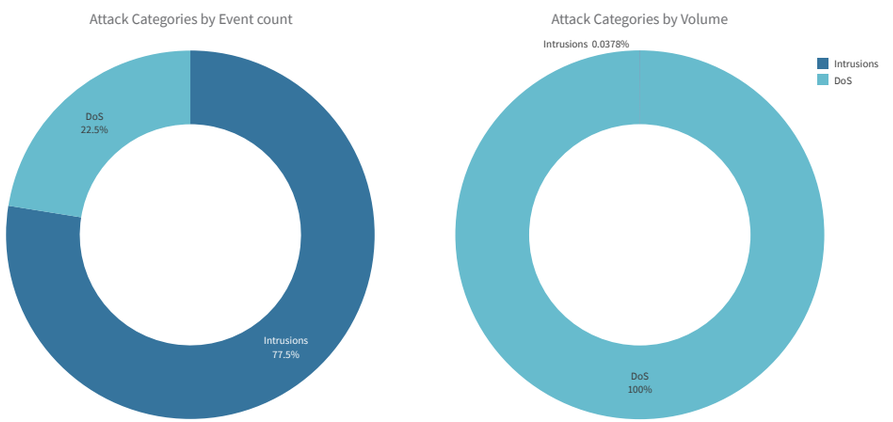
Network Scanning and Exploit Activity

Not all malicious events targeting exposed internet assets are DoS attacks. Network intrusion attacks consist of easy-to-execute exploits based on known vulnerabilities. These range from scanning using open-source or commercial tools to information disclosure attempts for reconnaissance, as well as path traversal and buffer overflow exploitation attempts that could render a system inoperable or allow access to systems and 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. This difference in numbers should not be interpreted as assets having to block more traffic from intrusions than from DoS events. Intrusions are typically smaller, consisting of one or few packets, compared to DoS events where a single event can consist of millions of packets and significant attack volume.

The number of intrusions in 2022 accounted for over two thirds of all blocked malicious events. In terms of volume, however, intrusions represented less than 0.04% of the total blocked attack volume.

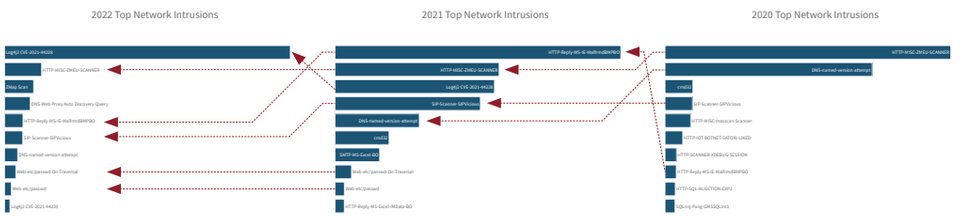
Figure 41: Malicious events by attack category



Unsurprisingly, the number one most blocked exploit in 2022 was Log4Shell. Disclosed by the end of 2021, Log4Shell took the internet by storm and exploit activity grew to the number three most exploited vulnerability of 2021 within weeks. Log4Shell exploit activity remained a constant throughout 2022.

The top 10 intrusions in 2022 had a good amount of overlap with those of 2021 and even 2020. For example, the most blocked intrusion of 2020, ZmEu vulnerability scans, only dropped to the second most blocked intrusion in 2021 where it remained throughout 2022.

Figure 42: 2020 vs 2021 vs 2022 Top Network Intrusions



SIP[5] scanning leveraging a tool named SIPVicious was another strong performer across all three years. SIPVicious is a set of open-source security tools used to audit SIP-based Voice-over-IP (VoIP) systems. It allows discovery of SIP servers, enumeration of SIP extensions, and password brute-forcing and scanning for known vulnerabilities. SIP scanning activity was the fourth most blocked intrusion in 2020 and 2021 and took a solid sixth place in 2022. The Malformed BMP file buffer overflow vulnerability in Microsoft Internet Explorer moved from an 8th place in 2020 to the most blocked intrusion in 2021, before declining to a respectful 5th place in 2022. See Appendix A for a detailed description of the top network intrusions.

5. SIP, or Session Initiation Protocol, is a protocol that can be used to set up and take down VoIP calls and can also be used to send multimedia messages over the Internet using PCs and mobile devices.

Log4Shell

The December 9 2021 publicly disclosed log4j vulnerability attracted huge attention across the security community. A vulnerability in a commonly used Java logging library, this allowed an unauthenticated attacker to leverage publicly available exploits for remote command execution (RCE). This was the most critical vulnerability of 2021, and some even argued it was the worst vulnerability of the decade.

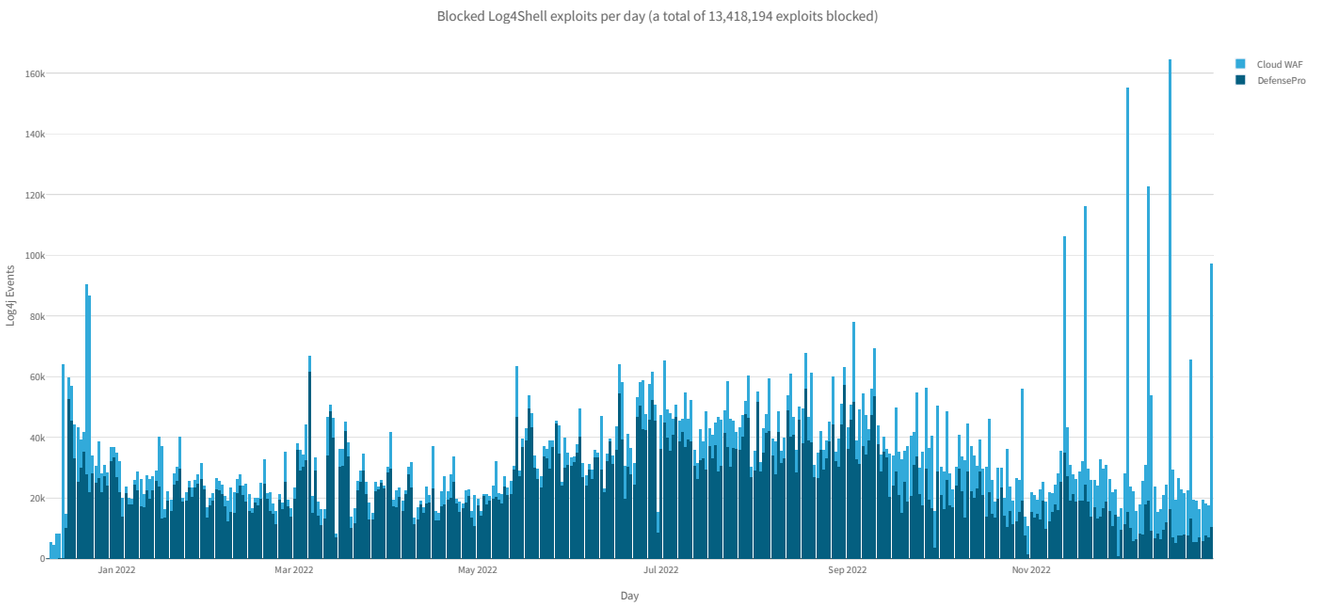
While Radware assessed the vulnerability to be easy to exploit, we also noted that performing remote command execution was a more involved process and harder to achieve. The remote command would need to be executed in the security context of the logging application, which according to best practice should run as a limited user. However, immediate action was required to close the vulnerability in applications, systems and devices across the globe. The vulnerability could still allow attackers to escalate privileges on compromised systems, move laterally across the network, and access backend databases and information stores accessible by the application.

Scanning and exploit activity was detected and blocked by the Radware Cloud WAF Service as early as December 9, 6pm UTC, only hours after disclosure of the vulnerability. By December 10, scanning and exploit activity ran to several thousands of events per day.

By December 15, a good amount of clear-text activity was blocked by freshly created and deployed Log4Shell signatures in Radware's network level DefensePro devices. Exploits leveraging encrypted transport and targeting web applications were detected and blocked by the WAF AppWall. AppWall detected Log4Shell exploits at day one without requiring specific signatures because the exploit was only possible by using a URI to a secondary server detected as a Server-Side Request Forgery (CSRF) violation.

Peaks of several tens of thousands of exploits per day were not exceptional. By the end of 2022, **a total of almost 13.5 million Log4Shell exploit attempts were blocked by Radware Cloud services**

Figure 43: Daily blocked Log4Shell activity in Radware Cloud WAF and Cloud DDoS Services



Log4Shell exploits were a constant in 2022. Peaks of several tens of thousands of exploits per day were not exceptional. By the end of 2022, a total of almost 13.5 million Log4Shell exploit attempts were blocked by Radware Cloud services.

As is the case with all vulnerability scanning activity, a portion of the recorded events and exploits originate from benign actors and organizations performing internet-wide scans to assess risks organizations might not be aware of. Bug bounty programs were initiated to motivate vulnerability researchers to discover vulnerable services and organizations. While the numbers are alarming, a portion of the activity can be considered non-malicious. The size of that non-malicious portion is unfortunately harder to quantify since white, grey and black hat scanners all use 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 do not allow us to distinguish between benign and malicious operations.

Web Application Attack Activity

The total number of web application transactions blocked by the Radware Cloud WAF service grew 128% from 2021 to 2022, faster compared to the 88% growth between 2020 and 2021.

During the first three quarters of 2021, the number of blocked transactions steadily increased. In Q4 the number decreased but was still above the quarterly levels recorded in 2020. The activity in every quarter of 2021 was above the activity in all quarters of 2020. In 2022, we saw an acceleration of this growth trend every quarter. Web application and online API attacks are growing exponentially.

Web application transactions can be blocked by application-specific custom rules created by the security operation center (SOC), or by automated detection based on signature rules and behavioral algorithms. The remainder of this section will consider only transactions blocked by signature and behavioral rules. This makes it possible to understand threats independent of the specificities of protected applications while eliminating the potential bias of customer-specific security policies. Figure 46 shows the total number of blocked transactions and the share of transactions that were blocked by signature and behavioral detection modules. In 2022, 50% of the blocked web transactions were based on known malicious behavior.

Figure 44

Yearly Blocked Web Application Transactions

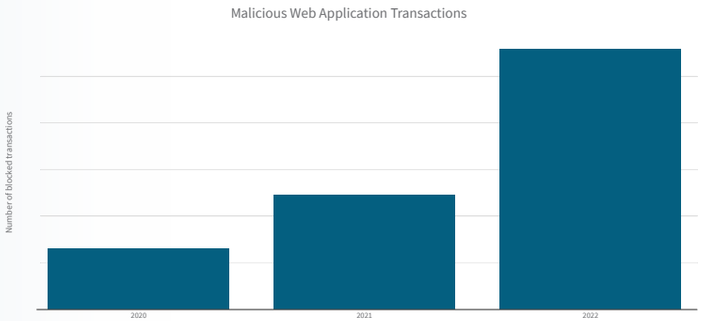


Figure 45

Quarterly Blocked Web Application Transactions

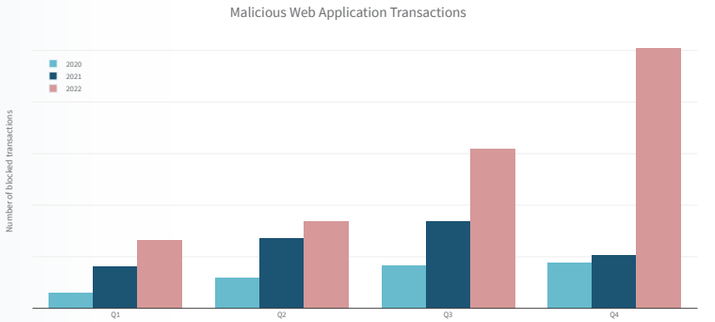
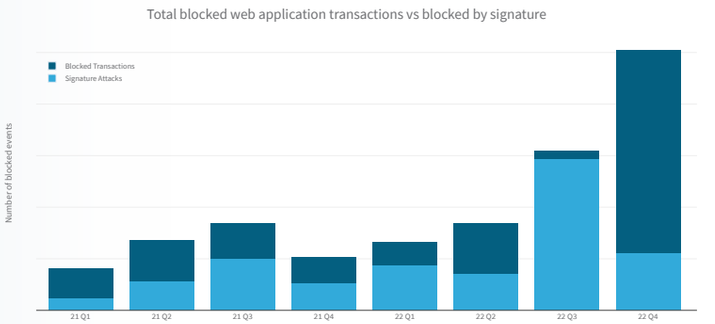


Figure 46

Total blocked web application transactions vs transactions blocked by signature

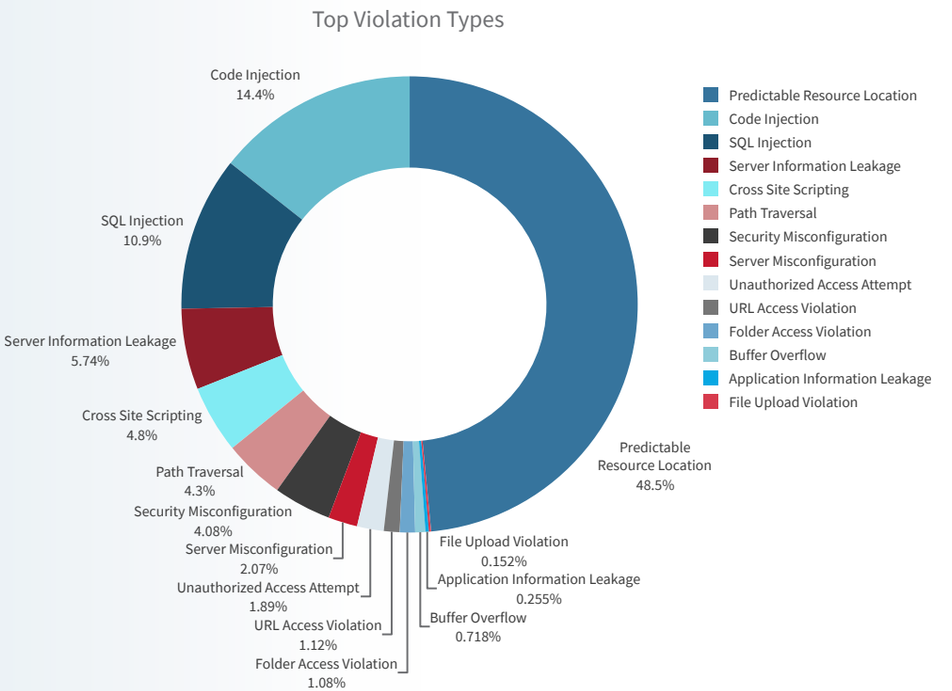


Security Violations

The most important security violation – predictable resource location attacks featured in Figure 47 – accounted for almost half of all attacks witnessed in 2022. Predictable resource location attacks target the hidden content and functionality of web applications. By guessing common names for directories or files, an attack may be able to access resources that were unintentionally exposed. Examples of resources that might be uncovered through guessing techniques include backup data, configuration files with insufficient access permissions, and yet-to-be-published, forgotten, or outdated elements of a web application. Predictable resource location attempts cover several top web application security risks in the OWASP 2021 Top 10[6], but the #1 and most important risk is 'A01 Broken Access Control'.

Code and SQL injection attacks represent more than one quarter of all web application attacks. The earlier discussed Log4Shell exploit, leveraged by most of the Java based online applications, contributed significantly to the number of code injections blocked in 2022. Together with Cross Site Scripting, Code and SQL Injection were the top three attack vectors most often used by criminals against online web applications and APIs.

Figure 47: Top security violation types



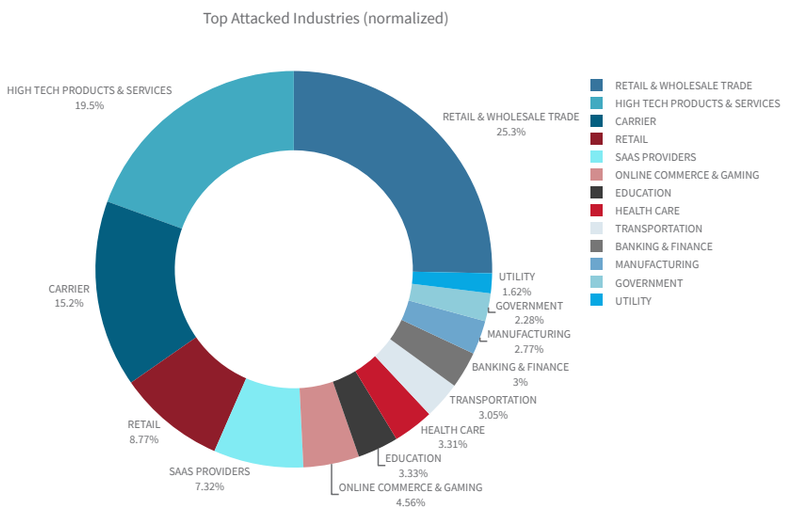
6. The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications and is published by the OWASP® Foundation.

Attacked Industries

The most attacked industries in 2022 were retail & wholesale trade (25.3%), high tech (19.5%), and carriers (15.2%), together accounting for 60% of blocked web application attacks.

The most attacked industries in 2022 were **retail & wholesale trade (25.3%), high tech (19.5%), and carriers (15.2%)**, together accounting for 60% of blocked web application attacks

Figure 48: Web application attacks by industry

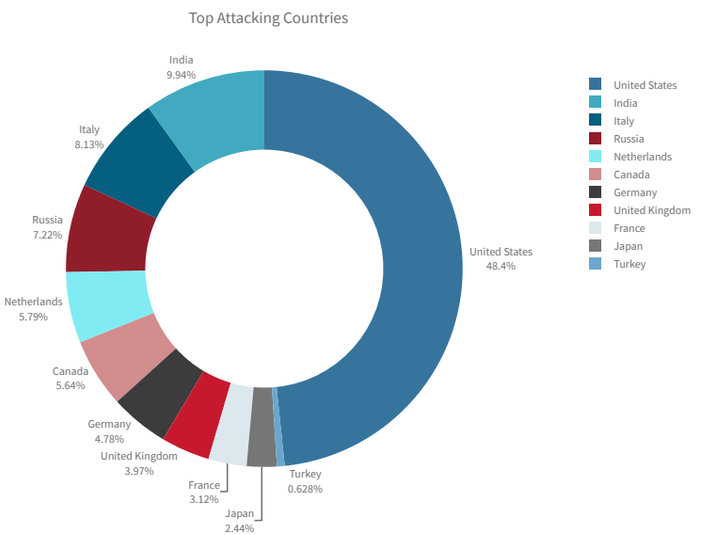


Attacking Countries

Most blocked web security events originated from the United States (48.4%). India, Italy, Russia, and the Netherlands completed the top five in 2022, not far ahead of Canada, Germany, the United Kingdom, France, and Japan.

It is important to note that the country where an attack originates does not necessarily correspond to the nationality of the threat actor. Often, the country where the attack originates will not be the home country of the threat actor. Threat actors leverage anonymizing VPNs, dark net routers and compromised systems as jump hosts to perform attacks. The originating country of an attack will sometimes be chosen based on the location of the target or the nation the threat actor wants to see attributed during false flag operations.

Figure 49: Top attacking countries in 2022



Unsolicited Network Activity

The Radware Global Deception Network (GDN) consists of a network of globally-distributed sensors that collect data on unsolicited traffic and attack attempts. Unsolicited events include DDoS backscatter and spoofed and non-spoofed scans and exploits.

The major difference between the GDN events discussed in this section and the web application and DDoS attack events in previous sections, is the unsolicited nature of the events. Web application and DDoS attack events were collected from real-world services accessible via the internet. In the latter case, attackers are targeting a particular organization or a specific application or service. By contrast, the unsolicited events recorded by the GDN are random acts. The scans or attacks are not targeting known services or a particular organization. The IP addresses of the sensors in the GDN are not published in DNS and do not provide accessible applications or services. No client, agent or device has a legitimate reason to reach a Radware GDN sensor.

In 2022, the Deception Network collected a total of 2.65 billion unsolicited events, an average of 7.3 million events per day. Compared to 2021, the total number of events in 2022 decreased slightly by 8.21%.

The number of unique IP addresses provides a measure for the evolution of the number of malicious hosts and devices randomly scanning the internet and exploiting known vulnerabilities. In 2022, the deception network registered an average of 52,860 unique IPs per day. A total of 12.75 million unique IPv4 addresses were recorded in 2022, representing 0.34% of the 3.7 billion IPv4 addresses available for non-reserved use on the internet. In other words, one in every 290 potential devices on the internet was caught doing something unexpected in the deception network.

Figure 50: The number of events per month recorded by Radware's GDN

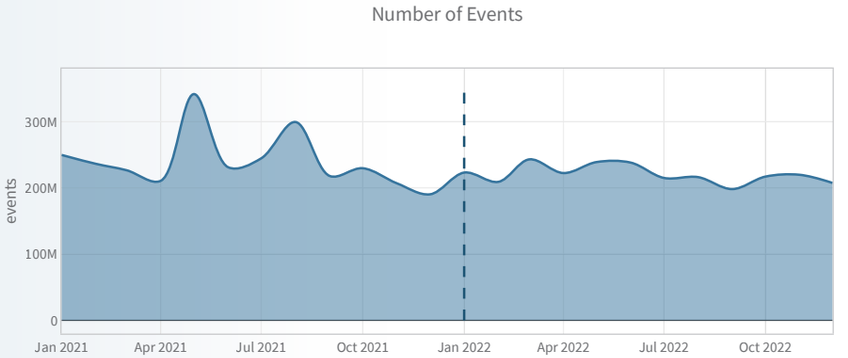
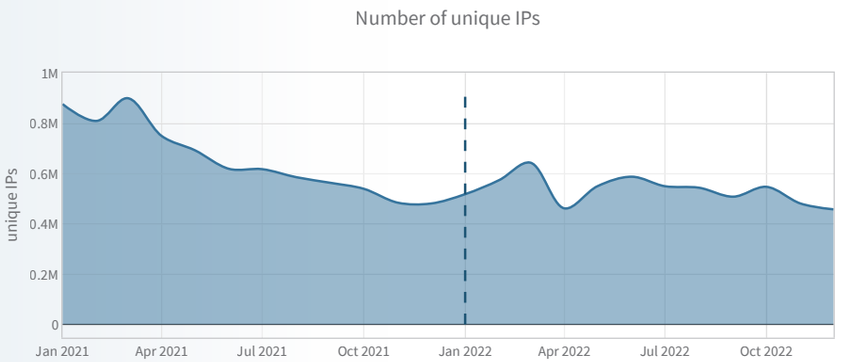


Figure 51: The number of unique IPs per month registered by Radware's GDN



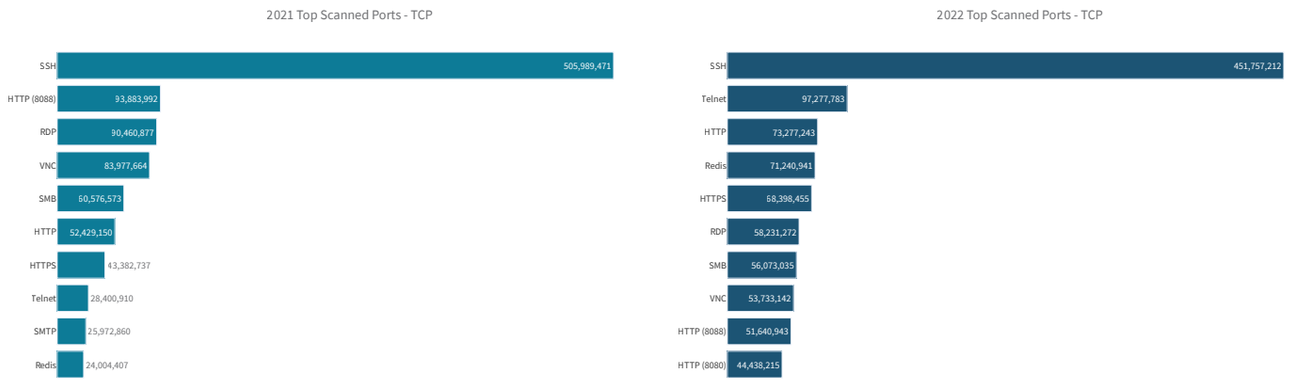
Most Scanned and Attacked TCP Ports

For TCP services, the most attacked service was SSH on port 22, followed by Telnet and HTTP. The top 10 is completed by Redis, HTTPS, RDP, SMB and VNC, followed by two popular IP camera web UI ports, 8088 and 8080.

While Telnet was a favorite of the Mirai botnet for a long time, the number of access attempts on SSH surpassed Telnet by a good margin. SSH attacks are leveraged in account takeover and brute force attempts. Leveraging default credentials or leaked credentials, attackers try to get unauthorized access to devices and systems to move laterally across organizations' networks, abuse the resources of cloud instances for cryptomining, leverage the foothold as a jump host to anonymize targeted attacks, plant cryptolocking malware for ransomware campaigns, or hijack the devices' connectivity to perform DDoS attacks.

Redis (port 6379) is an open-source (BSD licensed) in-memory data structure store used as a database, cache and message broker. In March, the Muhstik malware gang was actively targeting and exploiting a Lua sandbox escape vulnerability in Redis, tracked as CVE-2022-0543, after the release of a proof-of-concept exploit. In December, a previously undocumented Golang-based malware, dubbed Redigo, was targeting Redis servers aiming to take control of systems vulnerable to CVE-2022-0543, most likely to build a botnet. The malware mimicked the Redis protocol to communicate with its command & control (C2) infrastructure. The objective of the botnet and the attackers remains unknown.

Figure 52: Top scanned and attacked TCP ports, 2021 vs 2022



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. RDP is still a regularly exposed remote access protocol in remote location for industrial control systems (ICS) and became more exposed as people worked remotely during the COVID pandemic. RDP is one of the favorite initial attack vectors leveraged by Initial Access Brokers (IAB), who purchase and exploit leaked accounts from underground forums to gain access to organizations, subsequently installing cryptolocking ransom malware.

Server Message Block (SMB) is a popular file and printer sharing protocol leveraged by Microsoft in Windows and many Linux implementations through Samba or the more recent ksmbd kernel service. In December, a critical vulnerability with a CVSS score of 10 was disclosed that could enable remote attackers to execute arbitrary code on Linux servers exposing the SMB protocol from Linux servers with ksmbd enabled.

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.

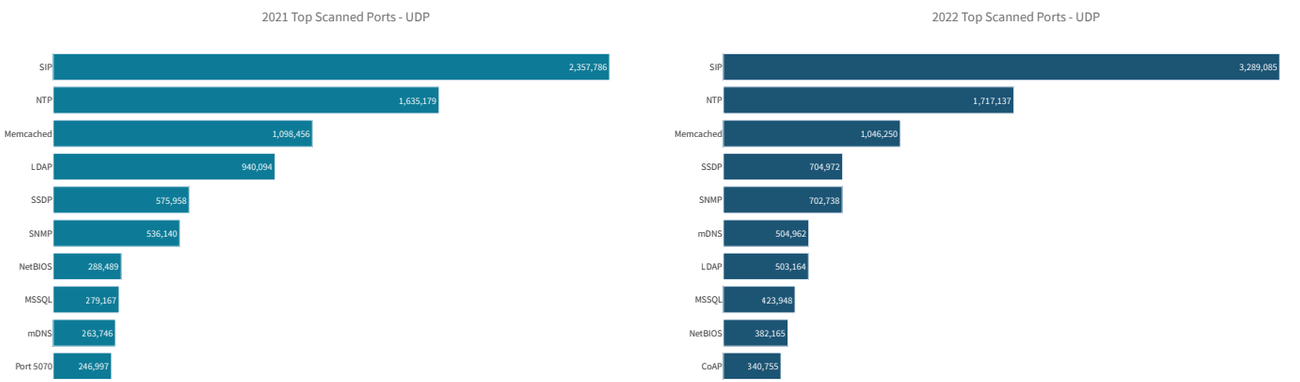
Most Scanned and Attacked UDP Ports

With the exception of LDAP moving down a few positions in the top ten, the top eight most scanned and attacked UDP ports remained identical between 2021 and 2022. SIP (port 5060) was again the most targeted UDP-based service in 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 also made the charts as one of the most targeted services for DDoS attacks in 2021. Vulnerabilities and weak or default passwords in VoIP services allow attackers to abuse them for initial access, spying, and moving laterally inside organizations' networks.

NTP (port 123), Memcached (port 11211), SSDP/UPnP (port 1900), SNMP (port 161), mDNS (port 5353), and LDAP (port 389) are among the most abused 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 (black hat) or assess the risk in the DDoS threat landscape (white hat).

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

Figure 53: Top scanned and attacked UDP ports, 2021 vs 2022



CoAP (port 5683) is a new addition to this year's top 10 most scanned and attacked UDP ports. Constrained Application Protocol (CoAP) is a specialized Internet application protocol for constrained devices, as defined in RFC 7252. CoAP is designed for use between devices on the same constrained network (e.g., low-power, lossy networks), between devices and general nodes on the internet, and between devices on different constrained networks connected via the internet. CoAP is also one of the most popular services targeted by attackers in DDoS amplification attacks.

NetBIOS (port 137) defines a software interface and a naming convention. NetBIOS includes a name service, often called WINS on Microsoft Windows operating systems. The NetBIOS name service is only needed within local networks and

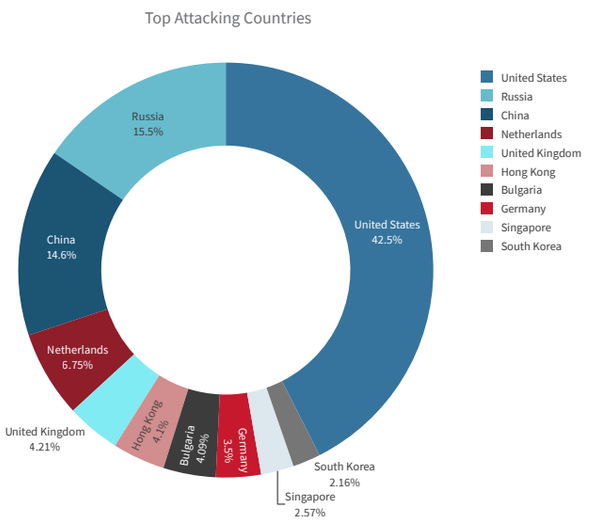
NTP (port 123), Memcached (port 11211), SSDP/UPnP (port 1900), SNMP (port 161), mDNS (port 5353), and LDAP (port 389) **are among the most abused protocols for DDoS amplification attacks**

with systems prior to Microsoft Windows 2000 which require name resolution through WINS. Otherwise, internet name resolution is done via DNS. Openly accessible NetBIOS name services can be abused for DDoS reflection attacks against third parties. Furthermore, they allow potential attackers to gather information on the server or network for the preparation of further attacks.

Attacking Countries

The top countries from which unsolicited network activity originated in 2022 were the United States, Russia, China, the Netherlands, and the United Kingdom. However, as mentioned earlier, the real origin of an attack can be spoofed to impersonate attacks from a different country.

Figure 54: Top attacking countries

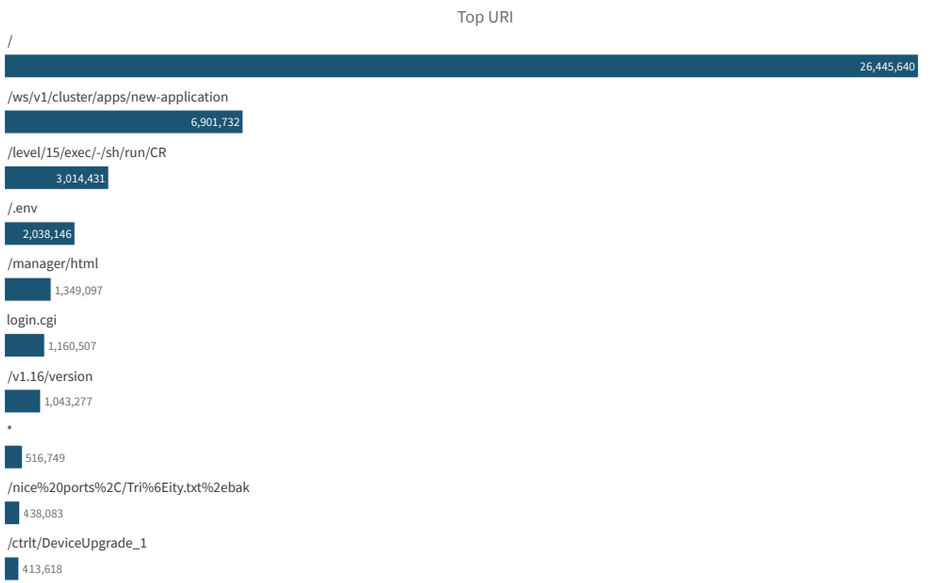


The top countries from which unsolicited network activity originated in 2022 were the **United States, Russia, China, the Netherlands, and the United Kingdom**

Web Service Exploits

The top attacked HTTP Uniform Resource Identifiers (URI) were 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 the top targets in web application attacks where services are supporting real applications. This section covers unsolicited events, meaning 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 that are randomly scanning and exploiting the internet. Typically, a URI will conform with a known and disclosed vulnerability.

Figure 55: Top scanned URI



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

A known vulnerability used to exploit Hadoop YARN services and schedule arbitrary workloads on Hadoop clusters. An exploit abused by many cryptojacking campaigns that try to leverage the cloud instances of enterprises and research institutions illegitimately. Was #2 in 2021.

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

In Aug 2002 Cisco released IOS 11.2 for Cisco routers that offered an HTTP interface allowing a user to execute commands directly from a URL. Today, 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 such opportunistic behavior by threat actors to bear fruit. Was #5 in 2021.

/manager/html

Apache Tomcat Manager Application Upload Authenticated Code Execution vulnerability. This module can be used to execute a payload on Apache Tomcat servers that have an exposed 'manager' application. The payload is uploaded as a WAR archive containing a JSP application using a POST request against the /manager/html/upload component. Was #4 in 2021.

/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 the Docker API. Was #6 in 2021.

/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. Was #10 in 2021.

/ctrlt/DeviceUpgrade_1

Huawei HG532 routers Remote Code Execution vulnerability, CVE-2017-17215.

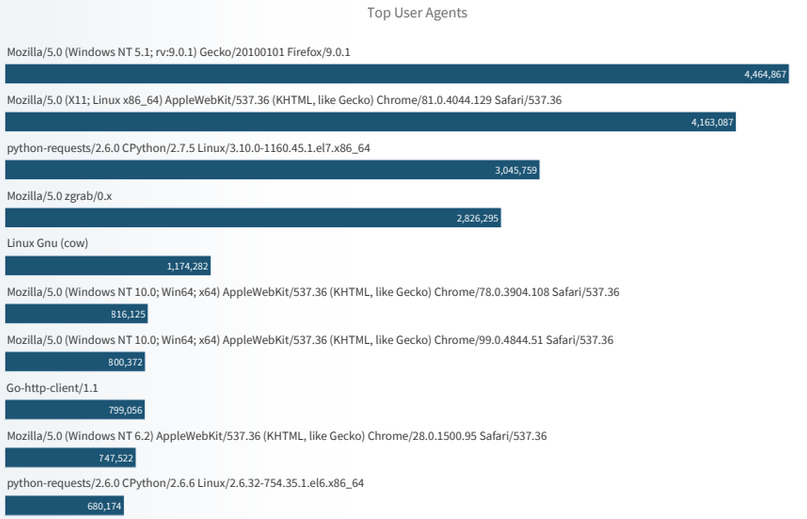
Top User Agents

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 to differentiate its interface for smartphones or desktop browsers. The concept of content tailoring is built into the HTTP standard in RFC1945.

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 used to score the legitimacy of a web request by web security modules. This causes them to 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', the application-layer network scanning component of the Zmap open-source scanning tool.

Figure 56: Top user agents

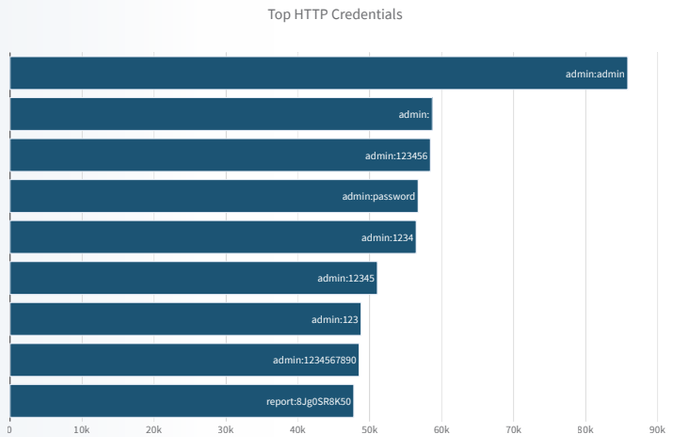


Top HTTP Credentials

Not all web service vulnerabilities can be exploited without authenticating. Some web services have widely used defaults and some even have hard-coded secrets to protect access from unauthorized users or devices. Typically, weak passwords are combined in credential pairs such as 'admin', 'password', '1234567890', or no password. These weak password permutations make up nine of the top 10 credentials. These are universally agreed to be the worst credentials and are abused because they provide access to devices that did not have their default credentials changed during installation.

The credential 'report:8Jg0SR8K50' is hard-coded in digital video recorders (DVRs) from vendor LILIN and was publicly disclosed in March 2020. DVRs are ubiquitous in the IoT landscape, as are the security cameras that feed them.

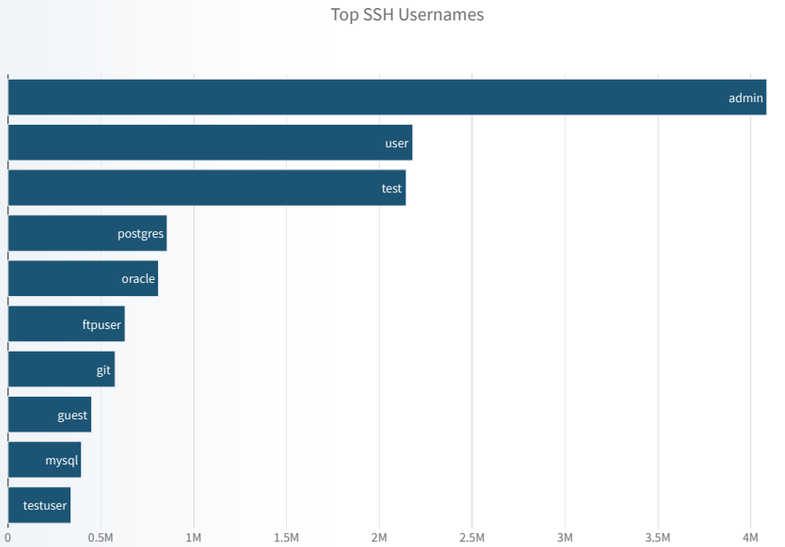
Figure 57: Top HTTP credentials



Top SSH Usernames

The top usernames used during SSH authentication give an indication of the services most vulnerable to brute forcing. Amongst the top 10 are ‘postgres’, ‘oracle’, ‘ftpuser’, ‘git’, and ‘mysql’. The others are the most leveraged usernames by administrators for default accounts, for example, ‘admin’, ‘user’, ‘test’, ‘guest’, and ‘testuser’.

Figure 58: Top SSH usernames



Appendix A

Radware ID	Classification	CVE
Log4j2 CVE-2021-44228	**RCE**	**CVE-2021-44228**
Log4j remote code execution vulnerability, also known as Log4Shell – A JNDI Injection vulnerability has been reported in the JndiManager class of Apache Log4j. This vulnerability is due to improper handling of a logged error. A remote, unauthenticated attacker who can control log messages or log message parameters can exploit this vulnerability by sending a specially crafted parameter to the target application. Successful exploitation results in the target server retrieving a potentially malicious serialized object from an attacker-controlled server which may lead to the execution of arbitrary code in the security context of the affected server.		
SIP-Scanner-SIPVicious	**Scanning**	**--**
SIPVicious is a SIP information gathering and scanning tool. It detects SIP devices, identifies active extensions on a PBX, and the existence of known vulnerabilities.		
HTTP-Reply-MS-IE-MalfrmdBMPBO	**Buffer Overflow**	**CVE-2004-0566**
Microsoft Internet Explorer Malformed BMP File Buffer Overflow – A vulnerability in the Microsoft Internet Explorer application that could allow a malicious website to execute arbitrary code when a specially crafted BMP file is loaded.		
HTTP-MISC-ZMEU-SCANNER	**Scanning**	**--**
ZmEu is a vulnerability scanner which searches for web servers that are vulnerable to attacks. It also attempts to guess passwords through brute force methods which may lead to DoS.		
DNS-named-version-attempt	**Information disclosure**	**--**
IQUERY version on named – The Bind named DNS service is vulnerable to an information disclosure attack allowing an attacker to determine if the server supports IQUERY requests. The information disclosed contains server version information.		
Web-etc/passwd-Dir-Traversal	**Information disclosure**	**CVE-2021-41733**
'../../etc/passwd' file access with Directory Traversal – Various web servers may be vulnerable to an information disclosure attack that occurs when the webserver is misconfigured or contains coding errors that allow access to sensitive files. A recently discovered vulnerability in Apache HTTP Server (CVE-2021-41733) started being actively exploited in the wild in October 2021. This vulnerability was introduced in a recent version of Apache (2.4.49). Users running older versions of Apache are not currently affected. The fix for CVE-2021-41733 in 2.4.50 was found to be insufficient, leading to a second, new vulnerability (CVE-2021-42013) that Apache is now reporting. As a result, version 2.4.51 was released to fully address the issue.		

List of Figures

Tables

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 (GDN) 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

Ron Meyran | Sr Director of Corporate Enablement
Deborah Myers | Sr Director of Corporate Marketing

Production

Gerri Dyrek | Director of Public Relations
Jeffrey Komanetsky | Content Development Manager