radware

2024 Global Threat Analysis Report

Executive Summary

Analysis of the most significant cybersecurity events and trends of 2023

Executive Summary

Geopolitical tensions and conflicts drove changes to the threat landscape in 2023. Trends included a cyber-era version of Cold War spy campaigns from the 1900s combined with unsettled activists—driven by ideology, religion, and politics—running cyber operations and online campaigns.

New hacktivist tactics that first saw daylight in 2022 after Russia invaded Ukraine spread further and even accelerated in 2023. Unexperienced hacktivists turned into experienced threat actors and launched more sophisticated threats to organizations, independent of industry or geography. As the war and sanctions continue to put financial pressure and trading limitations on Russia, many threat actors that started out of ideology turned into financially driven threat actors offering hacking, malware and DDoS-as-a-service. The Russian-speaking threat landscape expanded. Russian actors, well aware of their opportunities in the current geopolitical environment, have long known that they had free rein as long as they did not target organizations in Russia or its close allies. The conflict and sanctions only reinforced this unwritten policy. With almost two years of illegal denial of service, breaching and defacement activity left unprosecuted, the message is clear: the threshold into a life of cybercrime has reached a new low in the former socialist republic.

Advancements in technology caused a shift in the sophistication and breadth of the threat landscape. Generative artificial intelligence (AI) made its first strides and was received with a broad and warm adoption by businesses and end-users alike. Generative pre-trained transformers (GPTs) and large language models (LLMs) took the world by storm, and every organization started to rethink their roadmaps, marking strategies and processes, all centered around generative artificial intelligence (AI). The widespread adoption and unmistakable benefits in productivity enhancement has not escaped cybercriminals. Through current generations of GPT and Gemini, many low-

Evolving Threat Landscape

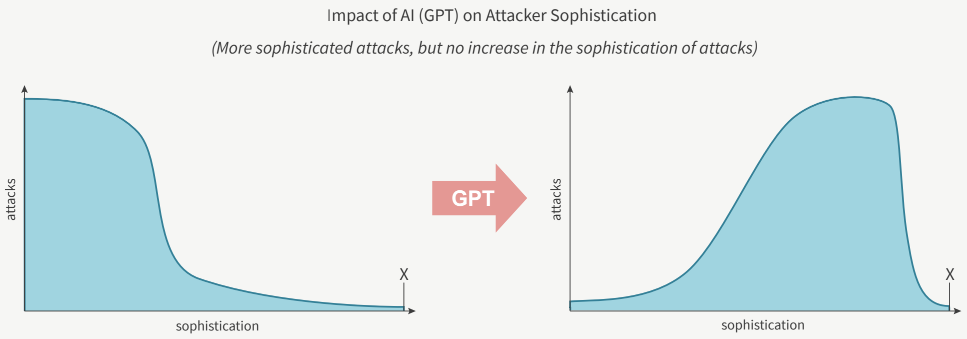
Hacktivists

More experienced.
More emboldened.

Artificial Intelligence

Generative AI is now mainstream.

Figure 1: Impact of GPT on attacker sophistication



sophistication threat actors were able to reach new levels of sophistication while highly sophisticated threat actors could leverage generative AI to scale up their attack campaign and cast wider nets than before. This new threat landscape is one of more sophisticated threats, but not one where the level of sophistication is higher than what we currently witness.

Critical vulnerabilities were common in 2024, and there was a rising trend of zero days exploited in the wild. Fortra GoAnywhere, Barracuda Email Security Gateway, Progress Moveit, VMWare, Microsoft Windows and Office, the WebP image format, Apple iOS and iPadOS, Atlassian Confluence, Citrix Netscaler ADC and gateways, and Cisco IOS XE make up just the top ten products exploited in zero-day attacks in 2023. Zero days were used in everything from commercial spyware products and cyber espionage campaigns to data extortion and ransomware attacks. In November, Michael Duffy, the Associate Director for Capacity Building in Cybersecurity at the Cybersecurity and Infrastructure Security Agency (CISA), warned attendees at the Imagine Nation ELC conference that the agency has noticed a "really high increase in zero-day activity, exploits that we're seeing across the globe, really affecting the federal government networks." Jared Semrau, Mandiant Intelligence's Senior Manager of Vulnerability and Exploitation, said 2023 is on track to be the highest year on record for zero days in their data. Don't expect this trend to slow down in 2024. Assisted by generative AI and who knows what new improved AI technology 2024 will bring, threat actors are better equipped than ever to accelerate their hunt for zero days—but so are security researchers. And with that knowledge, we come full circle in the arms race between good and bad actors. AI might force us to adapt and change the way we approach threats and threat actors, but cybersecurity will not be fundamentally different in the future than it was in past.

What's Motivating Hacktivists?

Ideology

Politics

Religion

Generative AI on the Rise

Many low-sophistication threat actors were able to reach **new levels of sophistication** while highly sophisticated threat actors could leverage generative AI to **scale up their attack campaigns**

Network-level Attacks in 2023

The number of DDoS attacks per customer grew by 94% in 2023 compared to 2022, building on the previous year's growth of 99%. The number of attacks per customer has been trending at an average rate of 106 attacks per month or 3.48 attacks per day since Q1 2021. In Q1 of 2023, a typical Radware customer had to fend off an average of 49 attacks per day.

The attack volume per customer increased 48% in 2023 compared to 2022. In 2023, we observed 63% more attacks with traffic below 1Gbps, 177% more attacks peaking between 100Gbps and 250Gbps, and an increase of 150% in large attacks peaking above 500Gbps.

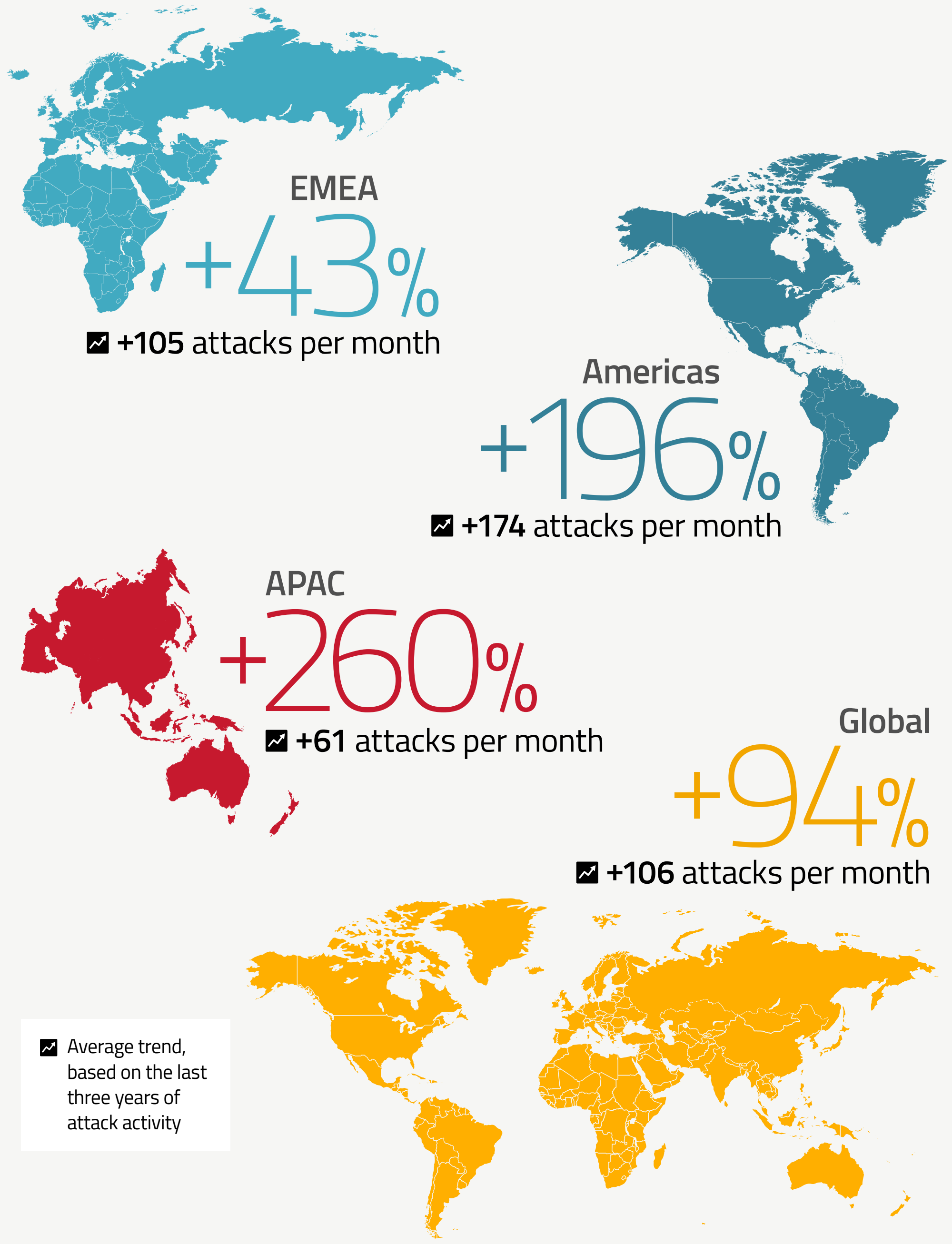
The Americas were targeted by almost half of all global DDoS attacks. The EMEA region, accounting for 39% of the DDoS attacks, had to mitigate 65% of the global DDoS attack volume. The APAC region accounted for almost 12% of global DDoS attacks.

Scrubbing centers located in EMEA blocked 60% of the total attack volume, while scrubbing centers in the Americas blocked 34% and scrubbing centers in APAC blocked almost 6%.

The average number of DDoS attacks targeting customers in the Americas grew significantly by 196% in 2023 compared to 2022. That's on top of the 157% growth seen in the region from 2021 to 2022. Attacks targeting the Americas are trending with an average increase of 174 attacks per month or 5.72 attacks per day—faster than the global average of 3.48 attacks per day.

The average number of DDoS attacks targeting customers in the EMEA region grew by 43% in 2023 compared to a growth of 107% in 2022. In the EMEA region, attacks are trending with an average increase of 105 attacks per month or 3.44 attacks per day. This is almost on par with the global average of 3.48 attacks per day.

Rise in DDoS attacks per Customer in 2023



The number of DDoS attacks targeting customers in the APAC region increased by a staggering 260% in 2023 compared to 2022. In 2022, the number of attacks per customer was on par with 2021. The number of attacks per customer in the APAC region is trending with an average increase of 61 attacks per month or 2.0 attacks per day—slower than the global average of 3.48 attacks per day.

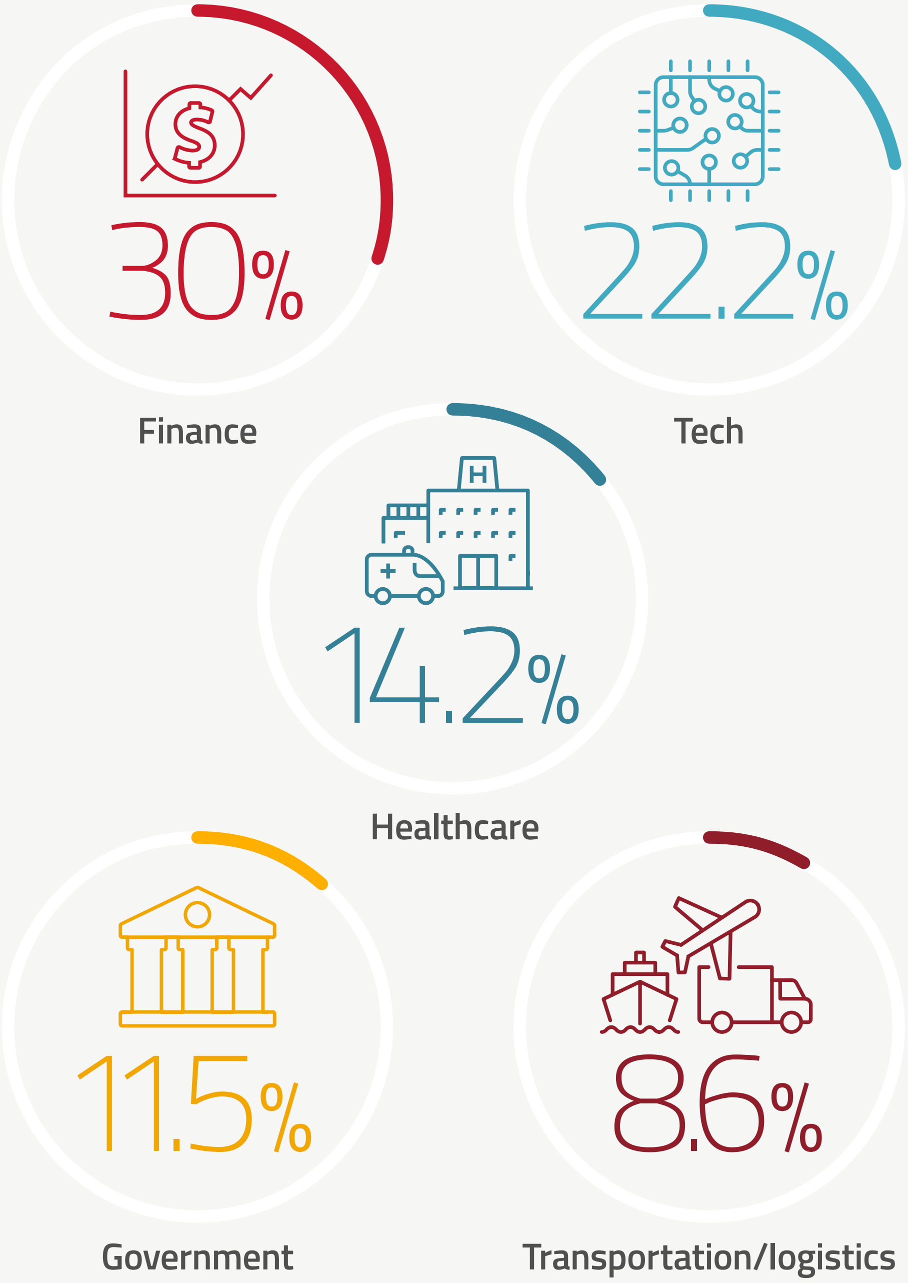
Finance organizations experienced almost 30% of global attack activity, while organizations in the technology industry faced 22.2% of all DDoS attacks. Other notable industries include healthcare (14.2%), government (11.5%), transportation and logistics (8.64%), and gaming (3.09%).

Compared to 2022, organizations in transportation and logistics faced 36% more attacks in 2023, while organizations in the utilities industry faced 23% more attacks. Other notable industries with considerable growth in the number of attacks in 2023 include energy (10%), gaming (8.9%), government (5.5%) and manufacturing (5.2%). Only a limited number of industries had a decrease in attack activity compared to last year. Organizations in the communications industry had a reduction of 0.5% in attack activity, service providers had a reduction of 0.6% and e-commerce had a reduction of 0.8%—all less than a 1% reduction based on the average number of attacks per customer per industry.

Finance (25.8%) and healthcare (24.1%) institutions accounted for almost half of the attack activity in the Americas region. Organizations in technology and the transportation and logistics industry mitigated 17% and 14.5% of the attacks, respectively, in the region. Government institutions represent almost 8% of the total attack activity of the region.

Finance was the most attacked industry in the EMEA region in 2023, accounting for 41.4% of all attacks in the region. Technology organizations and government institutions mitigated 18.2% and 14.6% of the attack activity, respectively, in the region. Other notable industries include

Global DDoS Attacks by Industry



utilities (6.27%), healthcare (4.86%) and gaming (4.75%), while a combination of remaining industries had to fend off 9.9% of the attack activity in the region.

In the APAC region, technology organizations were targeted by more than half (57.6%) of the overall attack activity in the region. Government institutions (17%) and gaming organizations (10.9%) had to endure a significant amount of the attacks. Finance (4.64%), service providers (2.87%) and healthcare (2.68%) were other notable industries that accounted for a fair amount of attack activity in the region. All other industries combined represented 4.06% of the attacks in the APAC region.

DNS and HTTPS form the cornerstone of online applications and APIs, and attackers had a clear mission in 2023: hit where it hurts the most. DNS, by far, was the most targeted application protocol, followed by HTTPS.

Application-layer DNS attacks leveraging pseudo-random subdomain (PRSD) attacks, also known as DNS water torture, were the most common attacks in 2023. Almost 95% of the attacks targeting DNS services leveraged DNS-A query floods.

NTP amplification generated the most volume in 2023, representing almost half of the global attack volume. DNS amplification was the most leveraged amplification attack vector and represented over 65% of all the amplification attack vectors observed in 2023.

Almost half of the attack vectors targeting finance applications were encrypted web attacks. In healthcare organizations, most of the network-level attack activity consisted of TCP attack vectors targeting network devices through random destination ports and carpet bombing attacks, as well as attacks targeting DNS services. The most aggressive attacks organizations in the government industry had to fend off were DNS-A query floods.

Attackers had a clear mission in 2023: hit where it hurts the most. DNS, by far, was the most targeted application protocol, followed by HTTPS

Application-level Attacks in 2023

The total malicious web application and API transactions increased by 171% in 2023 compared to 2022—a major increase compared to the 128% increase in 2022. A significant part of this increase in activity is caused by layer 7 (L7) encrypted web application attacks or Web DDoS attacks. During the first half of 2023 we noticed a large increase in web application DDoS. This trend has not slowed down and has even accelerated towards the end of the year.

Globally, throughout 2023, we observed a continuous and significant increase in DNS query flood attack vectors. DNS query flood vectors increased from fewer than nine out of every 1,000 attack vectors before Q4 2022 to 28 out of every 1,000 in Q4 of 2023—more than threefold increase in the ratio of L7 DNS attacks across all attack vectors by the end of 2023. DNS query floods do not generate large traffic volumes. The largest DNS query flood attack vector was observed in Q3 2023. It peaked at a maximum rate of 2.15 million QPS and generated a traffic volume peaking at only 1.52 Gbps.

Predictable resource location attacks, code injection and SQL injection combined were responsible for 62% of the total attack activity on web applications and APIs. Compared to 2022, predictable resource location was less prominent, but the top four violations remain predictable resource locations, code injection, SQL injection and server information leakage. Retail (36.7%) and transportation (18.6%) were the most attacked industries by web application and API attacks. Software as a service (8.4%), carrier (8.1%), utility (4.4%), healthcare (4.2%), education (4%), ISP (3.5%), insurance (3.4%) and government (3%) together with retail and transportation represent the top ten most attacked industries of 2023 by web application and API attacks.

Organizations in research and education (31.5%), telecom (24.9%), technology (18.7%), finance (9.53%) and healthcare (6.02%) were most

12.9M

Bad bot activity is growing in an average of 393 million transactions per month or **12.9 million transactions per day**

171% Increase in total malicious web application and API transactions in 2023

3X Global increase in layer 7 DNS attacks

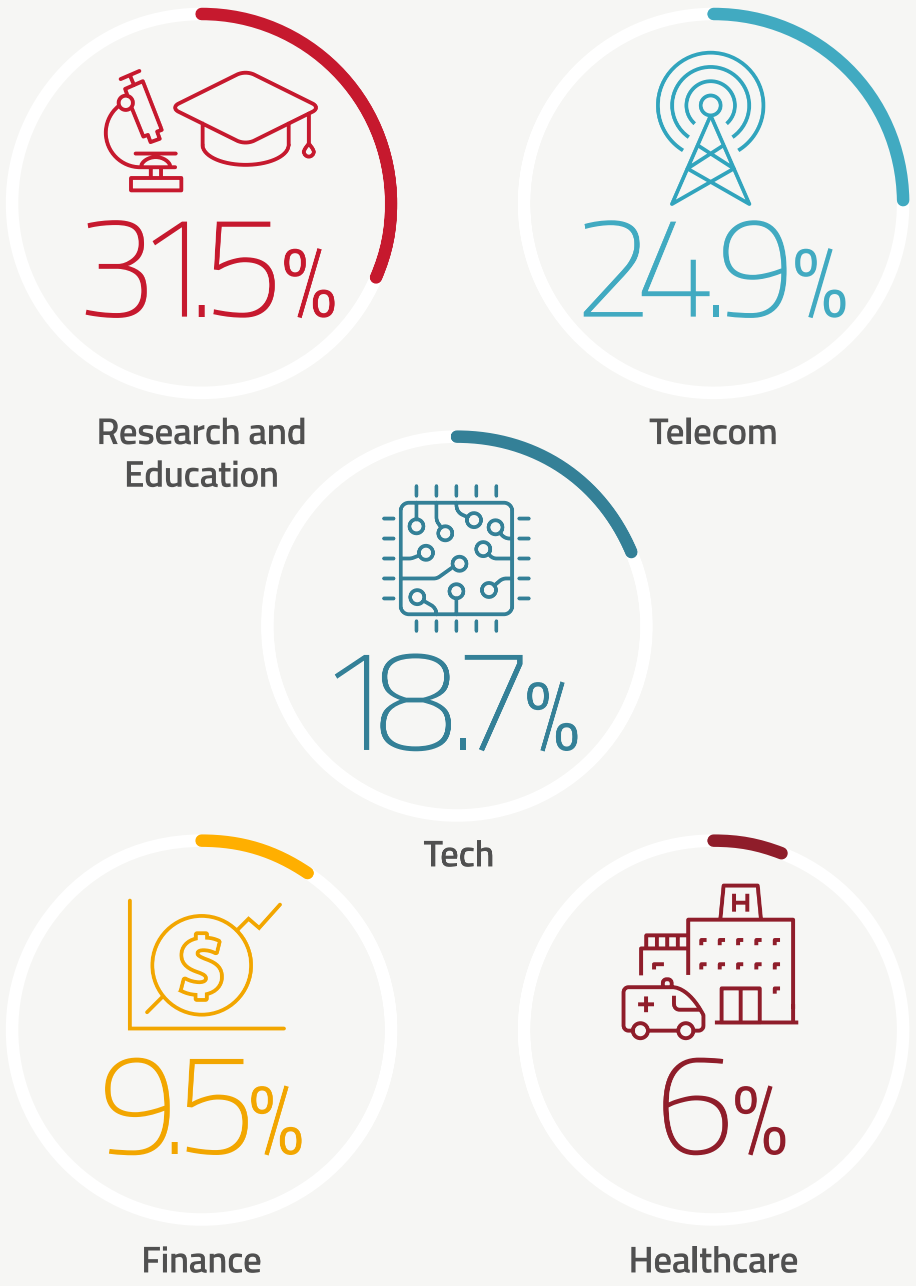
2.15M QPS in largest DNS flood attack

1.52Gbps Peak traffic value of same DNS flood attack targeted by DNS flood attacks. Technology organizations observed 73.2% of all malicious DNS queries while finance and government had to manage 10.8% and 5.45% of all malicious DNS queries, respectively. Finance had to manage the most significant DNS query flood attack, peaking at 2.15 million QPS. A telecom customer managed the second most significant attack, which peaked at 1.29 million QPS, while one government customer managed an attack peaking at 830,000 QPS.

After a year of staggering growth in 2022, the number of bad bot transactions detected per year slightly regressed by 9% in 2023 compared to 2022. The number of detected bad bot transactions per quarter, however, demonstrates a growing trend. Bad bot activity is growing an average of 393 million transactions per month or 12.9 million transactions per day. The most targeted region in 2023 was North America, which observed a growing trend across the year starting at 54.8 million transactions per day and reaching almost 110 million transactions on average per day during the last quarter. The number of bad bot transactions in the EMEA region peaked at 37.2 million transactions per day in Q3. The CALA region started the year with almost 46 million transactions per day and observed a downward trend toward the end of the year, ending the last quarter of the year with an average of 27 million transactions per day. The APAC region started with 27.4 million transactions per day and peaked in Q3 with almost 50 million transactions per day.

The retail and entertainment industry saw their online applications increasingly assaulted by bad bots across the year. Media observed a reduction in the second quarter and then remained stable for the rest of the year. Banking applications were most attacked during Q2 while travel applications had the worst period of the year in Q3.

DNS Flood Attacks by Industry



Hacktivist Activity

In the first half of 2023, threat actors claimed 5,606 attacks on Telegram. During the second half, this number increased with 24% to 6,971 claimed DDoS attacks. Some of the more noticeable actors became less prominent in the second half, but the overall trend of hacktivist-driven DDoS activity increased in the second half and reached a record level of 2,034 claims in October 2023. This record can be attributed to the global hacktivist activity following the conflict between Israel and Hamas.

Israel was the most targeted country by hacktivists. During the first half of 2023 it became the target of renewed attention for the yearly #OpIsrael Anonymous campaign. In the second half, it became the target of pro-Palestinian hacktivists and supporters after the conflict with Hamas started October 7. Israel was followed closely by India and the United States. India has been continuously targeted by different hacktivists in the region with multiple religious and political views and incidents in the media. A bit further out, Ukraine and Poland closed out the top five. They are the two most targeted countries related to the ongoing war fought on the territory of Ukraine with the Russian invaders. Poland, a direct neighbor of Ukraine, provides a lot of support and assistance to Ukraine. It should not come as a surprise that they got most of the attention from the pro-Russian patriotic hacktivists.

With 3,391 claimed DDoS attacks, NoName057(16) was by far the most active hacker group on Telegram in 2023. Executor DDoS v2, a DDoS-for-hire that performs DDoS attacks for a living, was in second place with less than one-fourth of the claimed DDoS attacks by NoName057(16). Hacktivist groups Mysterious Team, Anonymous Sudan, Team Insane Pakistan and the Cyber Army of Russia completed the top five most active hacktivists on Telegram in 2023.

Globally, the most targeted web category was government with 2,694 claimed attacks. Business and economy and travel websites were second and third, respectively, with notably less attacks. Financial services,

6,971 DDoS attacks claimed on Telegram in H2

↑ 24% Increase in claimed attacks over H1

Most Targeted Countries by Hacktivists

#1 Israel

1,480 claimed attacks

#2 India

#3 United States

#4 Ukraine

#5 Poland

educational institutions and news and media websites close the top six web categories with 500 claimed attacks or more in 2023.

NoName057(16) is probably the most organized and disciplined pro-Russian hacktivist group on the global threat scene. NoName057(16) was observed attacking multiple targets and sometimes multiple countries every day of 2023. The number of subscribers to NoName's Telegram channel has been steadily growing since May 2023 with an average of 80.3 new subscribers per day.

The Czech Republic was targeted the most by NoName057(16), accounting for 395 attacks in 2023. Czech Republic is closely followed by Poland with 353 attacks by NoName057(16). Lithuania, Germany and Italy completed the top five most targeted countries by NoName057(16).

NoName057(16) primarily targeted government websites (25.3%), travel websites (23.8%), business websites (19.2%) and websites providing financial services (19.2%).

The Cyber Army of Russia Reborn, describing itself as the "People's Cyber Army," caught our attention for its dedicated targeting of Ukraine. While Cyber Army of Russia did claim DDoS attacks on other countries, 341 out of a total of 481 attacks in 2023 were targeting Ukrainian websites. Poland, the second most targeted by Cyber Army of Russia, was targeted only 19 times. While on some days the Cyber Army of Russia would target up to a dozen websites, most days it focused on one or two Ukrainian targets.

In September 2023, Telegram banned Anonymous Sudan's main Telegram channel, which at that time gathered over 120,000 subscribers. Anonymous Sudan was not able to recover their original channel and came back a few days later with a new Telegram channel, @xAnonymousSudan. The switch to a new maiden channel caused Anonymous Sudan to lose 120,000 subscribers in a single day and it was only able to recover one-third (40,000) of the subscribers by the year's end.

KillNet, one of the most prominent pro-Russian patriotic hacktivist groups in 2022 was not very active in claiming DDoS attacks in 2023. The group came under increased scrutiny in November after the Russian news site Gazeta.ru claimed to reveal the identity of KillMilk. On December 7, 2023, KillMilk announced his retirement on his Telegram channel, stating they will be "moving to a new stage of development under the auspices of a new team."

#OpIsrael was the most mentioned hashtag in 2023. #OpIsrael was mentioned in 5,918 posts on Telegram. #OpIndia took a considerable second place with 4,308 mentions. Jointly, #OpIsrael and #OpIndia represent more than half of the operation tags in 2023. Other notable countries in operations were France, the United States, Canada, Japan, Ukraine, Italy and UK.

#OpIndia exhibited two bumps, one in the March-April timeframe and one in September-November timeframe—both closely related to the #OpIsrael campaign increases. There is also a noticeable overlap in hacktivist groups between the two operations.

In the second half of 2023, we observed more hacktivist groups starting to create alliances, some temporarily under joint attack campaigns and #Op battle tags, others more lasting.

Network Scanning and Exploit Activity in 2023

DNS-named-version-attempt, an information disclosure exploit used by malicious actors to identify the version of the Bind named DNS service, is leading the intrusion charts in 2023 by a wide margin. Six of the top 10 network intrusions in 2023 were known Log4j exploits. The December 2021 publicly disclosed Log4j vulnerability, dubbed Log4Shell, still attracts huge attention across the attacker community.

The second spot in the top 10 network intrusions is taken up by the ZMAP scanning tool. ZMap is a free and open-source security scanner that was developed as a faster alternative to Nmap. ZMap was designed for information security research and can be used for both white hat and black hat purposes. The tool is able to discover vulnerabilities and their impact and detect affected IoT devices.

SIP, the voice-over-IP (VoIP) Session Initiation Protocol, took two spots in the network intrusion top 10. The sixth spot is taken by SIPSAK. Also known as the SIP Swiss Army Knife, SIPSAK is a SIP stress and diagnostics utility that is used by developers and administrators to run simple tests on SIP applications and devices. SIPVicious, the tenth most detected intrusion in 2023, on the other hand, 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, password brute-forcing and scanning for known vulnerabilities in SIP services.

The December 9, 2021, a publicly disclosed Log4j vulnerability attracted a significant amount of attention across the security community. A vulnerability in a commonly used Java logging library allowed unauthenticated attackers to leverage publicly available exploits for remote command execution (RCE). Since its public disclosure, the exploit was detected and blocked more than 30 million times in the Radware cloud. Looking at the activity over time, it appears that exploits became more frequent in the second half of 2023, albeit slightly. The Log4shell vulnerability is a good reminder that threat actors are not only leveraging the most recent vulnerabilities, but they're also very successful at leveraging exploits for vulnerabilities that are several years old.

Log4j exploits

make up 6 of the top 10 network intrusions in 2023

30M Times that the Radware Cloud detected and blocked the Log4j exploit

The Log4shell vulnerability is a good reminder that threat actors are not only leveraging the most recent vulnerabilities, but they're also very successful at leveraging exploits for vulnerabilities that are several years old

Unsolicited Network Activity in 2023

The Radware Global Deception Network collected a total of 4.4 billion unsolicited events in 2023. This represents a 65% increase compared to the 2.6 billion events collected in 2022. The network collected an average of 12.1 million events per day in 2023, compared to 7.1 million events per day in 2022. In 2023, the deception network registered an average of 580,054 unique IPs per month, a slight increase compared to 2022 but less than in 2021.

For TCP services, the most attacked service in 2023 was SSH on port 22, followed by VNC and Telnet. The top 10 was completed by HTTP, HTTPS, Redis, RDP, SMB, TR-069 (port 7547) and HTTP port 8080, a popular IP camera web UI port. TR-069 was a new entry in the top 10 for 2023 compared to 2022.

The top scanned and exploited UDP ports in 2023 were SIP, NTP, SSDP, SNMP, Memcached, mDNS, port 80, MSSQL, IPSec (IKE) and BitTorrent P2P. Most of the scanned and exploited ports were similar to the top scanned UDP ports in 2022. The exceptions were LDAP, NetBIOS and CoAP, which left the top 10 in favor of UDP port 80, IPSec (IKE) and BitTorrent P2P.

The United States was the country from which the most unsolicited network activity originated during 2023. It was also number one in 2022 with 42.5% of all activity and remained so with 45% of the activity in 2023. The Netherlands moved from fourth spot in 2022 to second place in 2023 with 11.2%. China remained in the third spot in 2023 while the United Kingdom traded places with Russia.

The most exploited account takeover (ATO) credentials were weak passwords combined with the username "admin," for example: "admin:admin," "admin:password," "admin:1234567890," "admin: ." These weak password permutations make up nine of the top 10 tested credentials. The exact same nine made up the top 10 in 2022, only in a slightly different order. Tenth place in 2023 was taken by "report:8Jg0SR8K50," a hard coded user and password in digital video recorders (DVRs) from vendor LILIN, a vulnerability that was publicly disclosed in March 2020.

The top usernames used during attempts to compromise SSH services included "postgres," "oracle," "ftpuser," "git" and "pi" (Raspberry Pi default username).

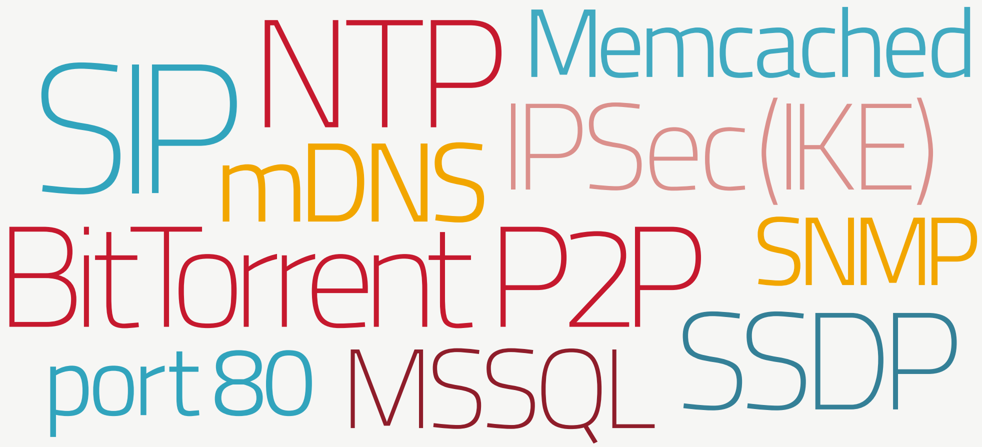
2023 Radware Global Deception Network

↑ 4.4 Billion unsolicited events collected

↑ 12.1 Million events per day

↑ 580,054 unique IPs per month

Top Scanned and Exploited UDP Ports in 2023



Methodology and Sources

The data for DDoS events and volumes was collected from Radware devices deployed in Radware cloud scrubbing centers and on-premises managed devices in Radware hybrid and peak protection services, jointly denoted as **Radware's Cloud DDoS Protection Service**. Note that attack events and blocked events are considered the same for the purpose of this report. All blocked volume is considered attack volume. An attack is a collection of several related attack vectors targeting the same customer and overlapping in time. Events correspond to attack vectors. Attack vectors consist of one or more packets. All packets of an attack vector generate a certain volume expressed in bytes. The volume generated by an attack vector is referred to as the blocked volume for that attack vector, which corresponds to the attack volume for that vector. The attack volume of all attack vectors part of the same attack correspond to that attack's attack volume.

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 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.

Web DDoS attack details were collected from the **Web DDoS Protection Service**. For 2023, only a sample of attacks was available.

Hacktivists openly publicize their actions on social media and public Telegram channels to gain media attention and raise awareness. They do not operate covertly or evade the media, but instead reveal the names and resources of their targets and attempt to take credit for their attacks. Hacktivists utilize website monitoring tools to demonstrate the impact of their denial-of-service attacks on online resources and frequently share links to reports from online web monitoring tools in their messages. Through tracking and analyzing messages from several active hacktivist groups on Telegram, the Radware Threat Intelligence team assessed the global DDoS activity conducted by hacktivists.

Editors

Pascal Geenens | Director of Threat Intelligence
Arik Atar | Senior Threat Intelligence Researcher

Executive Sponsors

Shira Sagiv | VP Portfolio Marketing
Deborah Myers | Senior Director of Corporate Marketing
Ron Meyran | Senior Director of Corporate Enablement

Production

Kimberly Burzynski | Sr. Marketing Communication Manager
Jeffrey Komanetsky | Content Development Manager

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.