radware

Report

2023 H1 Global Threat Analysis Report

The 2023 H1 Global Threat Analysis Report explores changes in today's threat landscape as cybercriminals shift their attention from network DDoS attacks to more sophisticated, application-level Web DDoS attacks. Discover the latest targets, tactics and motivations so you can proactively protect your organization.

Contents

Executive Summary

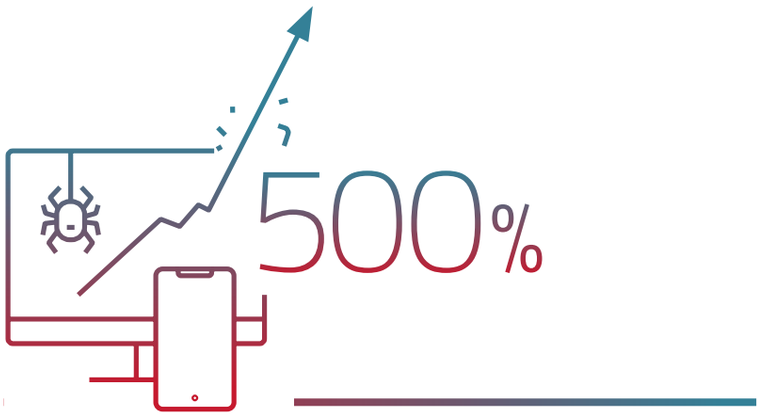
The cybersecurity landscape continued to rapidly evolve in the first half of 2023 (H1), when we observed a significant shift in Denial-of-Service (DoS) attack patterns. Increasingly, DoS attacks are progressing to layer 7 (L7), targeting not just the online applications and their APIs but also essential infrastructure such as the Domain Name System (DNS).

We noted a considerable surge in DNS query floods during H1 2023. Furthermore, Web Distributed Denial-of-Service (Web DDoS) attacks have become more sophisticated, utilizing high Request Per Second (RPS) traffic while randomizing multiple elements of the request to create seemingly legitimate traffic. This tactic has found favor with numerous hacktivist groups, including Anonymous Sudan and NoName057(16).

Hacktivists constitute a major part of the L7 DDoS problem. The effectiveness of these attacks has been significantly amplified by the use of patriotic volunteers in crowdsourced botnets or by providing them with custom attack tools and detailed tutorials on how to execute such attacks.

Network-layer attacks are better understood, and arguably easier to detect and mitigate compared to the new generation of HTTPS Floods organizations are facing in 2023. Since HTTPS Floods have been around for a few years, they are sometimes considered old news. However, the volume and intensity of the new generation of HTTPS Floods has increased dramatically while the sophistication and viciousness of attackers continue to grow. That is why we like to refer to these new-generation HTTPS Floods as Web DDoS attacks.

There's a discernible trend among malicious actors transitioning to cloud-based operations. By switching from compromised IoT devices to much more scalable and cost-effective cloud services providing high-speed internet connectivity, they can now orchestrate a limited number of very powerful



While in 2022 we observed a near linear growth per quarter, **in H1 2023 the number of malicious web application transactions skyrocketed by 500%**

nodes within their control. The advantages are considerable: they maintain control over their servers, suffer no loss from device reboots, and run a lower risk of detection by security researchers. Utilizing bulletproof hosting and proxy services that provide frequently rotating residential IP addresses creates the perfect platform to launch high-frequency, sophisticated attacks such as Web DDoS.

While the total number of DDoS events decreased by 33% compared to the first half of 2022 and the average attack volume per customer per month declined by 70%, the number of malicious web application transactions skyrocketed by 500%. In 2022 we observed a near linear growth in the number of malicious web transactions per quarter; in H1 2023 this growth accelerated exponentially. While the number of DDoS events in H1 2023 was below the number for H1 2022, it surpassed the total for the whole of 2021.

The narrative for 2023 is clear: as attackers ascend the network stack, they're increasingly targeting online applications and their infrastructure. Global DDoS activity hasn't reduced compared to 2022, but we observed a sizable proportion of network DDoS attacks shifting to more sophisticated application-level Web DDoS attacks. The task for organizations going forward is to proactively adapt to these evolving cyberthreats.

We noted a **considerable surge in DNS query floods during H1 2023.** Furthermore, Web Distributed Denial-of-Service **(Web DDoS) attacks have become more sophisticated**, utilizing high Request Per Second (RPS) traffic while randomizing multiple elements of the request to create seemingly legitimate traffic

Network-level DDoS Attack Activity

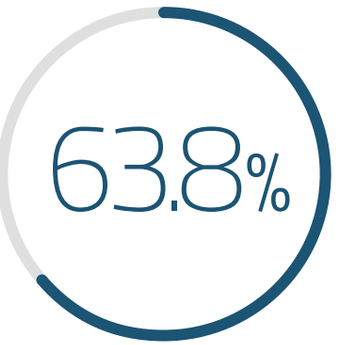
In H1 2023, UDP was the most abused protocol for volumetric network DDoS attacks, accounting for 63.8% of the total attack volume. TCP Out-of-State attacks followed with nearly 20%. DNS amplification produced the highest volume of amplification attacks at 61.6%. Resource exhaustion attacks, which exploit vulnerabilities in system resources and are characterized by high packet rates but low traffic volume, were also common. Attack vector distribution by packet rate showed a preference for TCP flag floods and DNS-A query floods in resource exhaustion attacks.

Compared with earlier years, the number of mid-sized attacks is growing very slowly. The number of small attack vectors is growing, but not as fast as last year. Large attack vectors in H1 2023 demonstrated a very steep growth compared to 2022.

In 2021 and most of 2022, less than 1% of all attack vectors were DNS Flood vectors, but this ratio doubled to almost 1.8% by Q2 2023. DNS Floods—application-layer attacks that overload a server's capacity to manage DNS requests—have also increased in scale since Q4 2022, with the largest attack in Q2 2023 reaching a rate of 1.29 million DNS queries per second. Despite this, the traffic volume of these attacks remained under the 1Gbps threshold as they aimed to overload servers rather than saturate internet connections. The most common DNS query used in DNS Floods in H1 2023 was the regular hostname to IPv4 query, accounting for 76.5% of all DNS Floods, followed by MX, TEXT, OTHER, and AAAA queries.

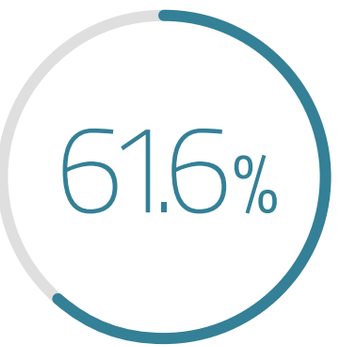
In terms of global DDoS events, the EMEA region (Europe, the Middle East and Africa), accounted for 66.2% of the attacks blocked in H1. Conversely, the Americas (North, Central, and South America) blocked a smaller number, 24.9%, but interestingly faced an almost equal attack volume to EMEA. This indicates that the threat level in the Americas is on par with EMEA, despite fewer blocked attacks. The APAC region (Asia and the Pacific) blocked 8.98% of DDoS events and faced approximately 5% of the global attack volume.

Network Level DDoS Attack Trends



UDP represented 63.8% of volumetric network DDoS attacks

TCP Out-of-State attacks represented roughly 20% of volumetric network DDoS attacks



DNS amplification produced the highest volume of amplification attacks at 61.6%

Estonia, Poland, Spain, the United Kingdom, and the Netherlands in the EMEA region, and the United States in the Americas, all emerged as major targets of DDoS attacks, suggesting continued focus by attackers on these countries.

To tackle DDoS threats, a global, decentralized approach is needed, preferably eliminating threats closer to their source. This reduces the malicious traffic burden on the larger internet infrastructure. Scrubbing centers, designed to filter out malicious traffic and ensure only legitimate data reaches its intended destination, play a pivotal role in this process. Distributed worldwide, these centers provide global DDoS protection, maintaining service continuity even during an attack. Interestingly, Ashburn (United States) handled nearly half of the total global malicious traffic. Frankfurt (Germany) blocked 20% of the attack volume, while London (United Kingdom) handled 10%. Together, Dallas and San Jose (United States) accounted for 12% of blocked global attack volume, demonstrating the importance of each scrubbing center in mitigating global DDoS threats.

In H1 2023, DDoS attack volume distribution across industries was unevenly distributed, with the research and education sectors bearing almost a third of the attacks. Service providers faced close to 20%, while the technology sector accounted for 11.6%. Gaming and telecom were also frequently targeted, representing respectively 7.1% and 5.61% of total attacks. Compared to 2022, the gaming industry saw attack volume surge by almost 20%, with industries such as manufacturing, energy, and retail also experiencing increases. However, e-commerce, communications, telecom, utilities, and service providers observed a slight decrease. The number of attacks increased most in utilities (+18%), telecom (+3.1%), and energy (+2.7%), while there were slight reductions in the retail, transportation, finance, communications, and manufacturing sectors.

1.29M

DNS Floods have also increased in scale since Q4 2022, with **the largest attack in Q2 2023 reaching a rate of 1.29 million DNS queries per second**

DDoS Attack Volume by Industry

20%
Service providers

7.1%
Gaming

11.6%
Tech

5.61%
Telecom

Hacktivism

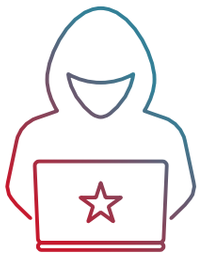
On the hacktivist front, NoName057(16) proved to be the biggest threat for western countries supporting Ukraine in the war with Russia.

Meanwhile, Anonymous Sudan, a new but fast-growing actor, became "the hacktivist with too many causes". Anonymous Sudan profiled itself as a pro-Muslim hacktivist group, joined pro-Kremlin hacktivist campaigns, ran several ransom DDoS campaigns, and became a politically driven hacktivist when a conflict broke out in Sudan in April 2023 between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF).

The Killnet group, meanwhile, under-delivered on its promises and its attack activity was nowhere near the level witnessed in 2022. However, on the media front, Killnet leader Killmilk increased his presence and reach as the most influential personality in the pro-Russian hacktivist scene.

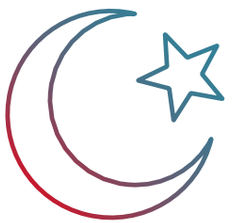
Hacktivist campaigns against India have escalated, fueled by social media initiatives such as "Islamophobia_in_India" and "SaveIndianMuslims" which spread disinformation. Starting with a series of attacks in 2022 led by DragonForce Malaysia, numerous ideologically aligned groups have since taken up the banner. A group named Team Insane PK, notable for its international cyberattacks, revived the anti-India campaign in early 2023. Concurrently, Mysterious Team Bangladesh initiated "Operation Payback" in response to Indian cyber activities against various countries. In parallel, other hacktivist groups from multiple countries initiated campaigns against India based on perceived social injustices toward Indian Muslims. However, pro-Indian hacktivist groups have emerged to counter these attacks, including Anonymous India, Mariana's Web, and Kerala Cyber Xtractors. These evolving campaigns and responses highlight a complex and globally interconnected landscape of cyber-activism surrounding India.

Key Trends in Hacktivism



Biggest worry for western countries supporting Ukraine
NoName057(16)

Anonymous Sudan found motivation in religion, politics and money



Killnet leader **Killmilk** became the most influential pro-Russian hacktivist

Web Application Attack Activity

In H1 2023, the most significant security violation was predictable resource location attacks, accounting for a major portion of the total attack count. These attacks aim to uncover hidden web application resources by guessing common names for directories or files. Following this, SQL and code injection attacks were the second and third most common. Together, these three types of attacks accounted for 64% of the total attack activity on web applications and APIs. In Q2 2023, SQL injection attacks increased significantly, reaching almost the same frequency as predictable resource location attacks.

The majority of blocked web security events originated from the United States, with Germany, Russia, the United Kingdom and Italy completing the top five. While the United States has consistently dominated the attack landscape, it's crucial to note that the origin country doesn't necessarily reflect the nationality of the threat actors. Often, actors use cloud-hosted servers, VPNs, proxies, and compromised servers to conceal their real origins. The country from which an attack originates is usually chosen based on the victim's location to avoid potential geo-blocking or to misdirect attribution during false flag operations.

The retail industry was the most targeted by web application attacks, accounting for 35.5% of all attacks. Carriers and SAAS providers followed as the second and third most attacked industries, representing 10.6% and 8.08% of web application attacks, respectively. The transportation sector (5.12%), government entities (5%), educational institutions (4.77%), utility providers (4.65%), and healthcare sector (3.3%) also experienced significant web application attacks.

64%

Combined web app and API attack activity from **predictable resource location attacks, SQL injection attacks and code injection attacks**

Industry Share of Web Application Attacks

35% Retail

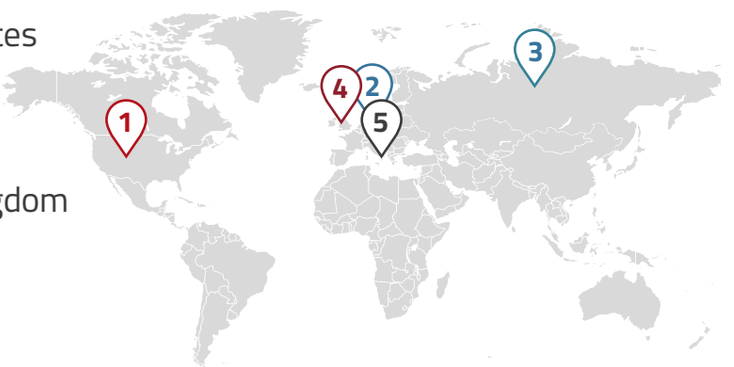
5.12% Transportation

10.6% Carriers

8.08% SaaS providers

Most Blocked Web Security Events

1. United States
2. Germany
3. Russia
4. United Kingdom
5. Italy



Unsolicited Network Activity

In H1 2023, Radware's Global Deception Network (GDN), which collects unsolicited events or random scans and attacks that don't target known services or organizations, recorded a substantial rise in such activities. The network collected a total of 2.05 billion unsolicited events, representing a marked increase compared to the total 2.65 billion events gathered in all of 2022. On average, the network recorded 11.3 million events per day, an increase of 55% compared to the previous year. There was also a 15% increase in unique IPs per day, with an average of 60,775 recorded in H1 2023 compared to 52,860 in 2022. Although the number of malicious devices on the internet increased only slightly, their activities became significantly more aggressive.

The most attacked TCP service was SSH, followed by Telnet and VNC. Other frequently targeted services included HTTP, Redis, HTTPS, SMB, TR-069, RDP, and the popular IP camera web UI port, 8080. TR-069 emerged as a new entry in the top ten for H1 2023, a prominent protocol from the Mirai era that re-entered the global scanning activity six years after its first major exploit.

Most of the scanned and exploited UDP ports were also among the top contenders in 2022. LDAP, which had been in the top ten, was replaced by OpenVPN in the tenth spot. CoAP, which had secured tenth place in 2022, was also displaced during H1 2023. SIP (port 5060) was again the most targeted UDP-based service in H1 2023.

The United States was the top country of origin for unsolicited network activity, accounting for 41.2% of all activity in H1 2023. This is almost identical to 2022 when it accounted for 42.5% of all such activity. The Netherlands rose from the fourth position in 2022 to the second in H1 2023, accounting for 16.5% of activity. China remained in the third spot, while Russia dropped from second in 2022 to fourth in H1 2023. The United Kingdom held steady in the fifth position. However, again it's important to note that the apparent origin of an attack doesn't necessarily reflect the true location of the attacker, as locations can be spoofed to make it seem as if attacks are originating from different countries.

Many web service vulnerabilities exploited common weak password combinations or hard-coded credentials to gain unauthorized access. The majority of the top 10 abused credentials were simplistic and widely used defaults such as "admin", "password", and "1234567890", often remaining unchanged from the default settings during device installation. A standout in this list was "report:8Jg0SR8K50", a hard-coded credential found in digital video recorders (DVRs) from the manufacturer LILIN. This vulnerability was publicly disclosed in March 2020 and is notable due to the ubiquity of DVRs and associated security cameras in the Internet of Things (IoT) landscape.

2.05B

Unsolicited events collected by Radware's Global Deception Network (GDN)

11.3M

Events tracked per day up 55% from 2022

↑15%

Increase in **unique IPs per day**

Denial-of-Service Attack Activity

In H1 2023, the number of DDoS events per customer blocked by Radware's Cloud DDoS Protection Service decreased by 33% compared to H1 2022 but grew by 103% compared to H1 2021. The H1 period of 2023 represented 32% of the DDoS events observed in 2022 and saw 7% more events compared to 2021.

In H1 2023, on average, the service blocked 6,271 DDoS events per customer, per month. In 2022, the service blocked 10,266 events per customer, per month. In 2021, the number of events per customer per month was 4,258. The average number of events blocked per month for a customer decreased by 39% compared to 2022 but increased by 47% compared to 2021.

Figure 1: Evolution of blocked DDoS events per quarter over time

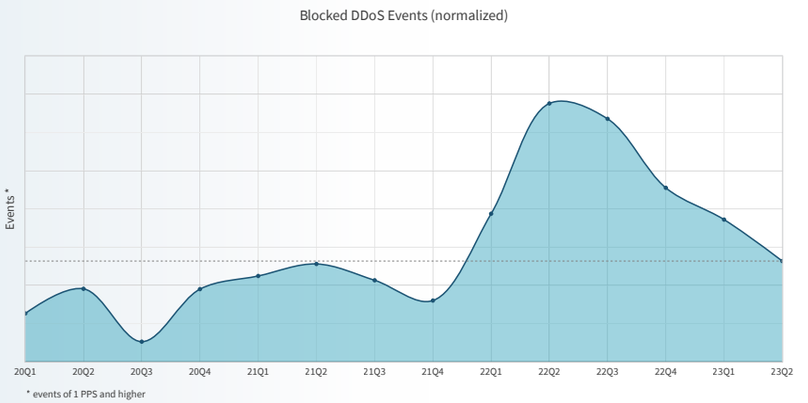
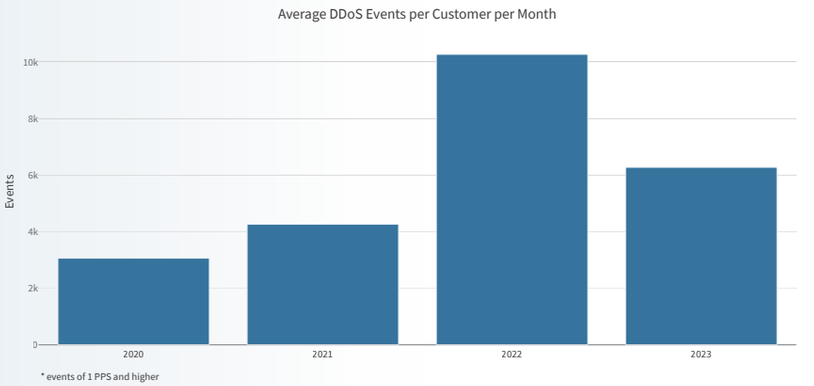


Figure 2: Average number of DDoS events blocked per customer per month



Regions and Industries

Regions

The EMEA region blocked 66.2% of global DDoS events. The Americas, while accounting for a lower 24.9% of blocked DDoS events, saw a similar attack volume compared to EMEA, 47.4% and 47.7%, respectively. This suggests that while the number of blocked attacks may be lower, the actual threat level in the Americas is comparable to EMEA.

The APAC region blocked 8.98% of DDoS events and faced about 5% of the global attack volume. Although these figures are lower than the other regions, they still represent a significant burden.

Organizations based in Estonia, Poland, Spain, the United Kingdom and the Netherlands experienced the highest attack volumes, indicating that organizations in these countries have the highest probability to be hit by volumetric DDoS attacks.

Despite EMEA's overall effectiveness in blocking a large proportion of DDoS events, the attack volume in these countries suggests that as attackers continue to focus on this type of attack they remain an area of concern.

On the other side of the Atlantic, the United States emerged as another hotspot for DDoS attacks. The attack volume in the United States was just behind that of the top five European countries. This aligns with the data indicating that the Americas region faced a similar attack volume as the EMEA region despite blocking fewer attacks.

Addressing DDoS attacks effectively necessitates a worldwide, decentralized strategy. The best method to mitigate distributed threats is by eliminating them as close to their source as possible, significantly reducing the strain of malicious traffic on the wider internet infrastructure.

Figure 3

Blocked DDoS events per region

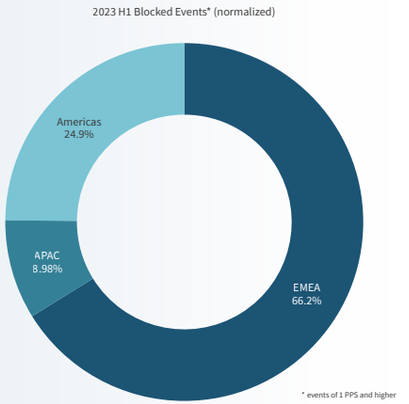


Figure 4

Blocked DDoS volume per region

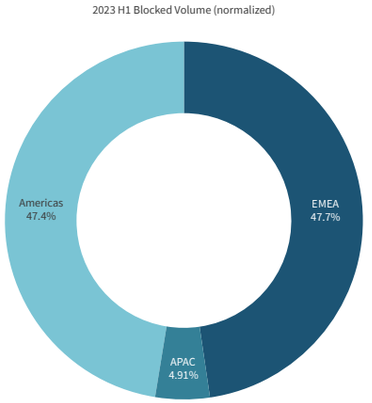
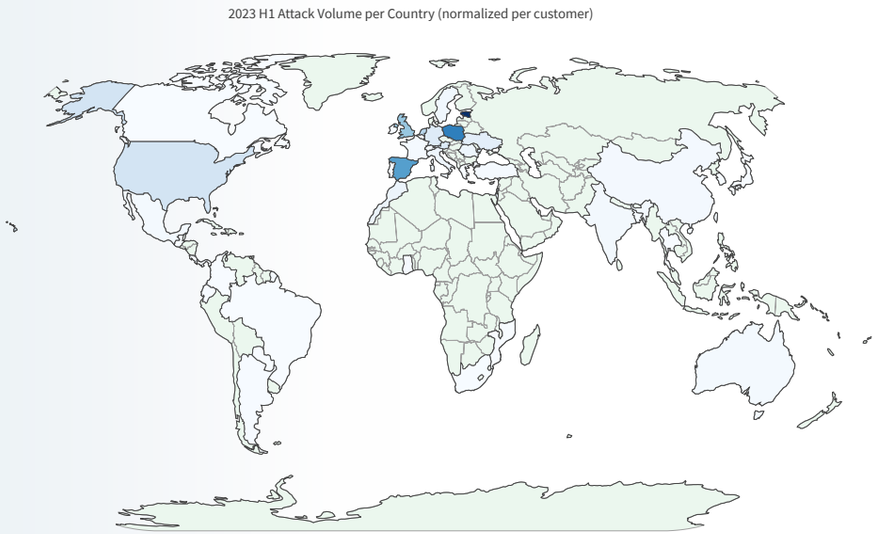


Figure 5: World map of DDoS attack volume per country



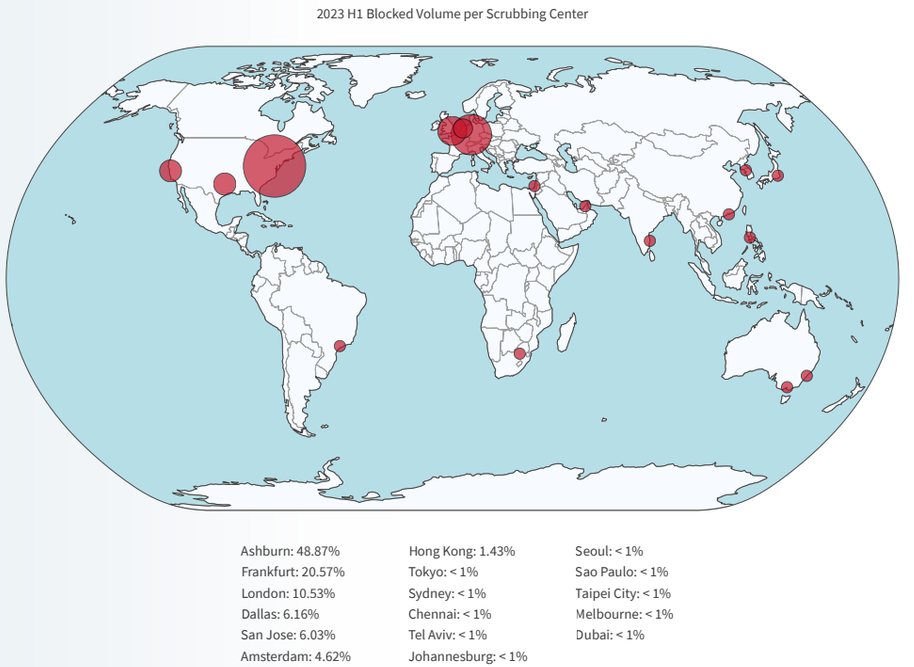
A scrubbing center is a data cleansing facility designed to help organizations protect their data and infrastructure from DDoS attacks. When incoming network traffic is directed through a scrubbing center, the role of the center is to "scrub" the data, that is to filter out malicious traffic and allow only legitimate traffic to be routed through the Cloud DDoS Protection Service backbone to its intended destination. This process involves the separation of clean data, which is allowed to reach the target server, from the "dirty" or harmful data, which is dropped.

Scrubbing centers should be distributed across the world to provide global DDoS protection and ensure uninterrupted service, even when an attack is underway. The quantity of attack volume intercepted by a scrubbing center offers a reliable indication of the origin of the hostile traffic.

Ashburn (United States) handled nearly 50% of the total global malicious traffic. Frankfurt (Germany) accounted for 20% of the attack volume while London (United Kingdom) consumed 10% of the global attack volume.

In the United States, the cities of Dallas and San Jose jointly accounted for 12% of the total global attack volume blocking. This diverse geographical distribution underlines the critical role of each scrubbing center in the collective fight against DDoS threats.

Figure 6: Blocked DDoS attack volume by scrubbing center



Industries

In H1 2023, certain industries faced a disproportionate share of the total DDoS attack volume. Notably, organizations within research and education bore the brunt with nearly a third of the total attack volume directed at them.

Service providers also faced considerable volumes, with almost 20% of the total attack volume aimed at their operations. Meanwhile, the technology sector experienced 11.6% of the total volume.

Other notable industries that found themselves frequent targets of these attacks included the gaming industry, with a 7.1% share of the attack volume, and the telecom industry, which accounted for 5.6% of the total.

Compared to 2022, during H1 2023 organizations in the gaming industry faced almost 20% more attack volume. Other significant growth industries in terms of attack volume were manufacturing (+14%), energy (+12%), industrials (+9.6%) and retail (+7.1%). Organizations in e-commerce, communications, telecom and utilities as well as service providers saw a slight (less than 1%) decrease in attack volumes during H1 2023 compared to 2022.

Figure 7

Blocked DDoS volume per industry

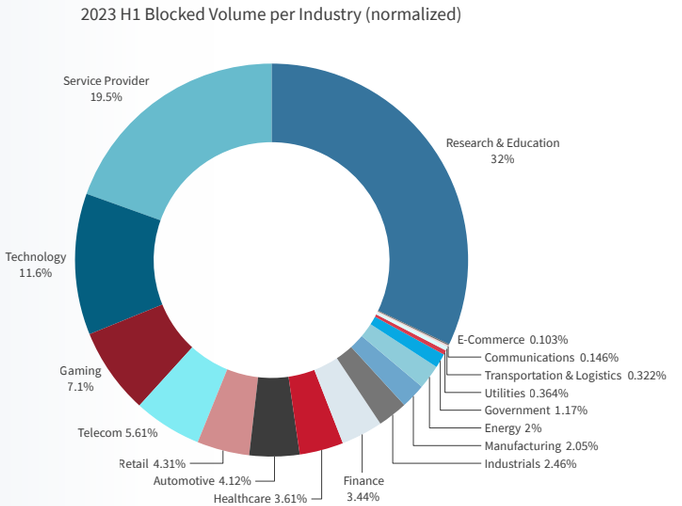
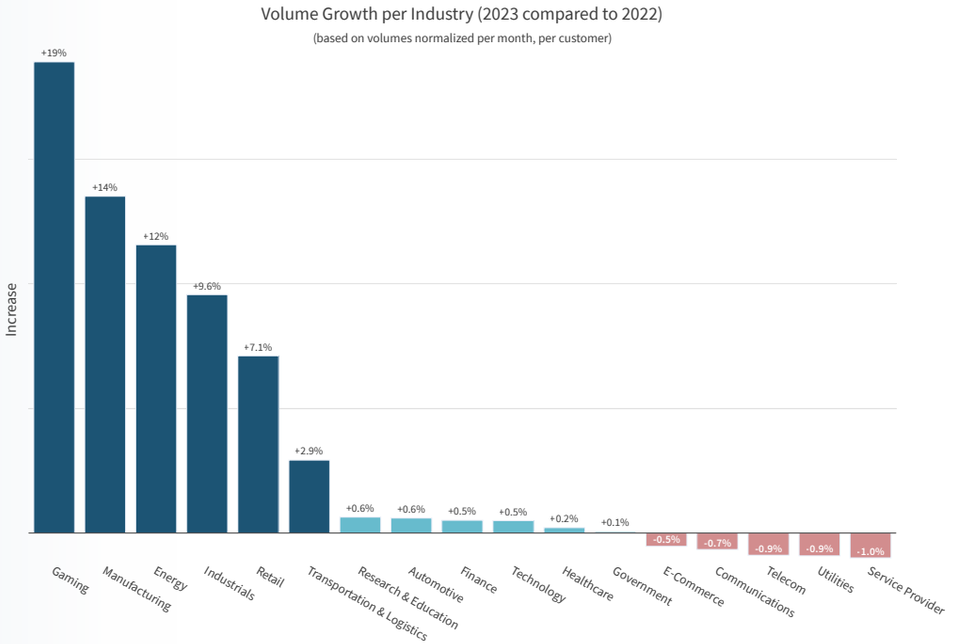


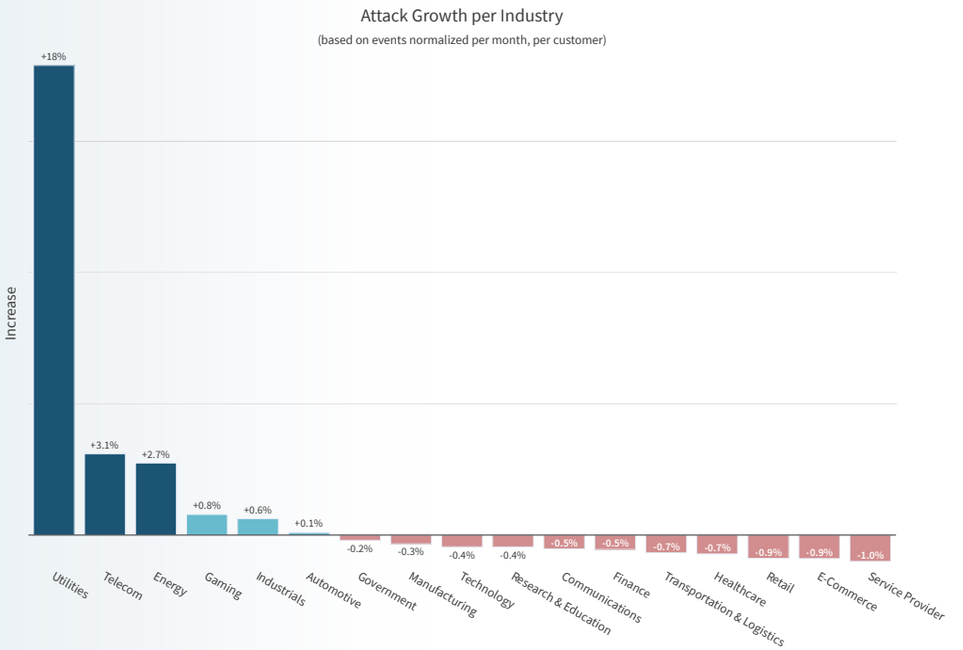
Figure 8

Growth of attack DDoS volume per industry from 2022 to H1 2023



In terms of DDoS attack events, utility organizations saw the largest increase (18%), followed by telecom organizations (+3.1%) and organizations in the energy industry (+2.7%). While the attack volumes targeting organizations in the retail, transportation and logistics, finance, communications and manufacturing industries increased in H1 2023, the number of attack events shrank slightly (between 0.3 and 1%).

Figure 9: Growth in the number of DDoS attack events between 2022 and H1 2023 by industry

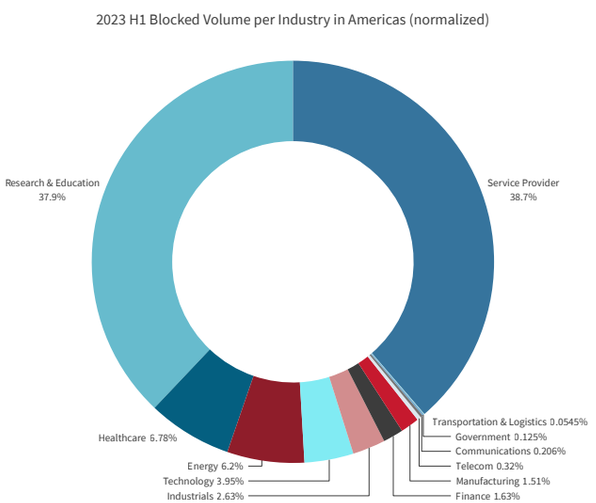


The Americas (North, Central, and South America)

In H1 2023, service providers and research and education organizations were the main targets, constituting 38.7% and 37.9% of the total DDoS attack volume respectively. This indicates a significant cyberthreat focus on these sectors in the Americas.

Further down the list, healthcare organizations were subjected to 6.8% of the attack volume. Energy companies experienced a slightly lower proportion of attacks, receiving 6.2% of the total volume. Technology organizations, while also significantly affected, saw a smaller proportion of the overall attack volume at 3.95%.

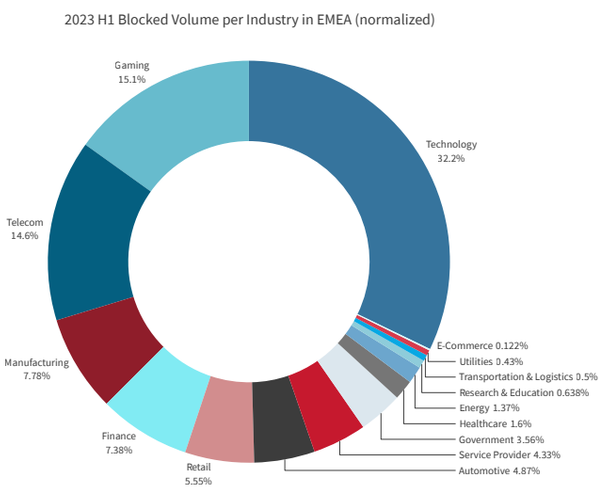
Figure 10: Blocked DDoS volume per Americas industry



EMEA (Europe, Middle East and Africa)

In the EMEA region, the distribution of DDoS attack volume during H1 2023 showed a broader spread across various industries. The technology sector was the most affected, accounting for 32.2% of the attack volume. This was followed by the gaming industry (15.1%), telecom (14.6%), manufacturing (7.78%), finance (7.38%), and retail (5.55%).

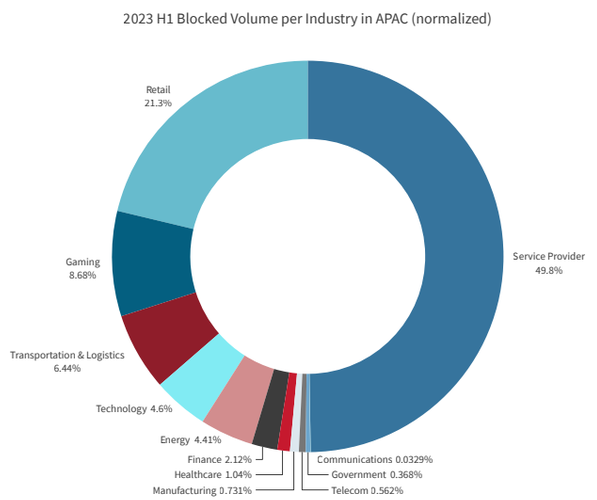
Figure 11: Blocked DDoS volume per industry in EMEA



Asia Pacific (APAC)

In the APAC region, service providers bore the brunt of DDoS attacks during H1 2023, with 50% of the total attack volume targeting this sector. The retail industry faced a significant proportion of the remaining volume, accounting for 21.3%, followed by the gaming industry at 8.68%, and transportation and logistics at 6.44%.

Figure 12: Blocked DDoS volume per industry in APAC



Attack Protocols

In 2023, UDP was again the most leveraged protocol for volumetric network DDoS attacks. UDP and UDP Fragment floods represented 63.8% of the total attack volume in H1 2023. TCP Out-of-State attacks represented almost 20% of the attack volume.

Volumetric network DoS attacks aim to saturate the connectivity of organizations or services by flooding the network with more traffic than it can handle. The use of UDP Floods in volumetric attacks is reflected in the attack vector distribution per vector size in Figure 14.

Attackers leverage reflection and amplification services that are publicly exposed on the internet. If it's UDP and is exposed to the internet, it can be weaponized for DDoS attacks. By reflecting malicious packets from legitimate services on the internet, the attackers hide the origin of their attacks while making them more resistant to simple mitigations such as IP blocklisting. Another motivation to weaponize specific protocols is amplification. Certain protocols are preferred as they provide more amplification. 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 will cause attackers to gravitate to vulnerable protocols and services. 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 harder.

Figure 13: Protocols leveraged by volumetric network attacks

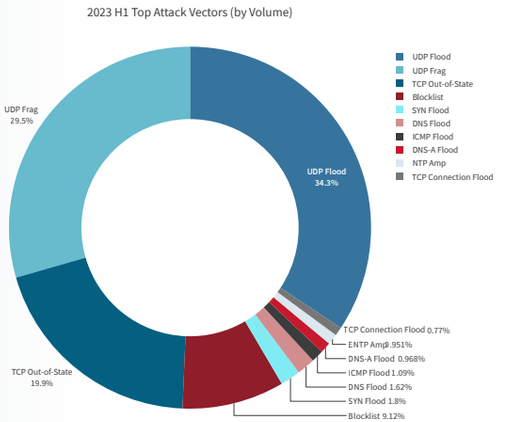
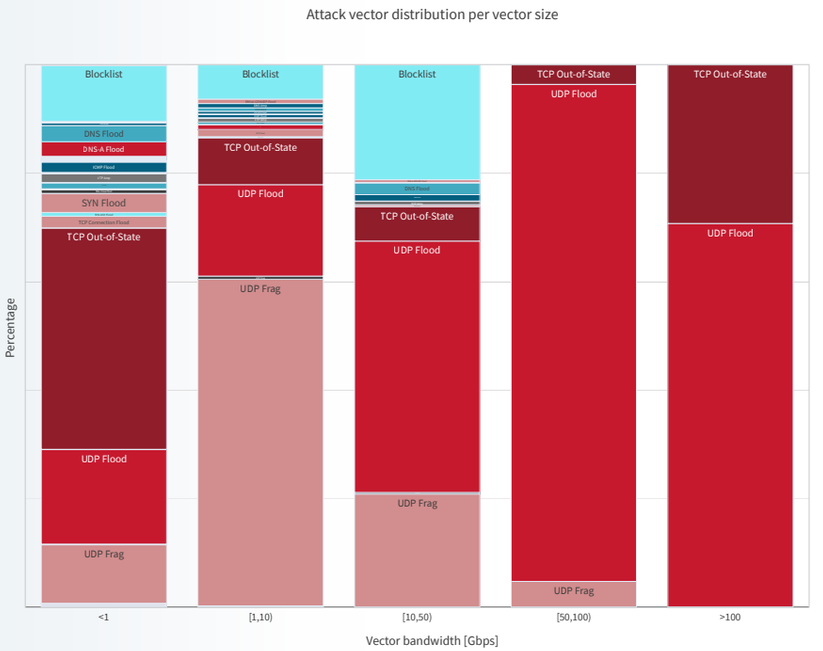


Figure 14: DDoS attack vector distribution per vector size



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

DNS amplification was the amplification attack vector that generated the most volume in H1 2023, representing 61.6% of the total amplification volume. NTP amplification was the second most abused amplification attack vector, accounting for 34.1% of the volume. Smaller volumes were generated by SSDP, ARMS, Memcached, DHCP Discover (IPv6), Chargen, CLDAP, SNMP and COAP.

In addition to volumetric attacks, attackers also leverage resource exhaustion attacks. Unlike volumetric attacks, these do not rely on volume but rather on packet rates. Resource exhaustion attacks are designed to exploit vulnerabilities in system resources, such as memory, computing power, or even specific application resources. These types of attacks are characterized by a high packet rate, where a large number of small packets are sent to overwhelm specific elements of a network's infrastructure. As a consequence, the traffic volume associated with resource exhaustion attacks is typically limited.

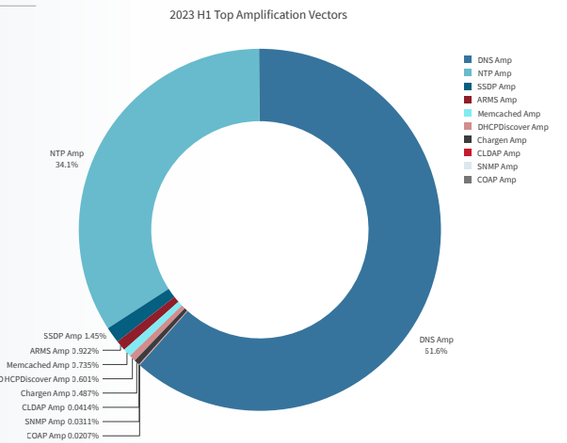
Even if the overall network bandwidth isn't overloaded, these attacks can render targeted systems unresponsive by causing server processes to consume too much CPU or memory, by filling up connection tables, or by filling up disk space or database connections.

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 15

Top DDoS amplification attack vectors



In H1 2023, 29.4% of all blocked packets originated from UDP floods. UDP floods are also responsible for most of the volume. Generating a large volume requires high packet rates. The maximum size of an internet packet is limited to less than 1500 bytes. To saturate high bandwidth connections with terabit per second attacks, attackers need to leverage high packet rates to reach such high traffic levels.

TCP Out-of-State (20%) and TCP SYN Flood (13.7%) attacks are resource exhaustion attacks, as are TCP RST (5.4%) and DNS-A (4.91%) Floods. While representing only about 5% of the malicious packets blocked in H1 2023, DNS query floods can cause disruption to the network infrastructure of organizations. It's a tactic that has been used more often by attackers in the last few months (see DNS Floods, page 20).

The attack vector distribution by packet rate demonstrates attackers' preference for TCP flag floods such as SYN, SYN-ACK, RST floods and TCP Out-of-State floods in all attack vectors with higher packet rates, including the highest packet rate attack vectors generating more than 1 million PPS. DNS-A query floods were typically leveraged in attack vectors between 10,000 and 1 million PPS. Other DNS query floods, such as AAAA, SOA and OTHER queries, are more significant for attack vectors between 100 and 1,000 PPS.

Figure 16

Top DDoS amplification attack vectors

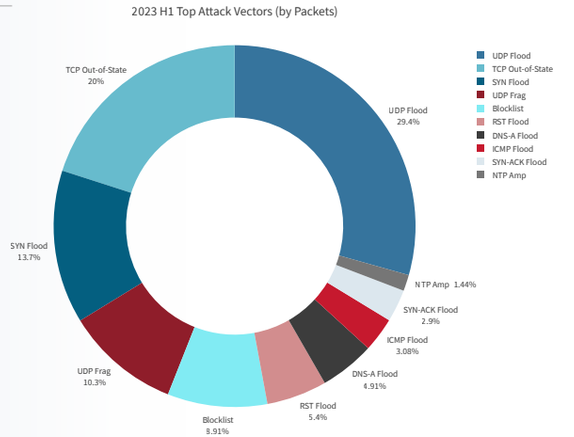
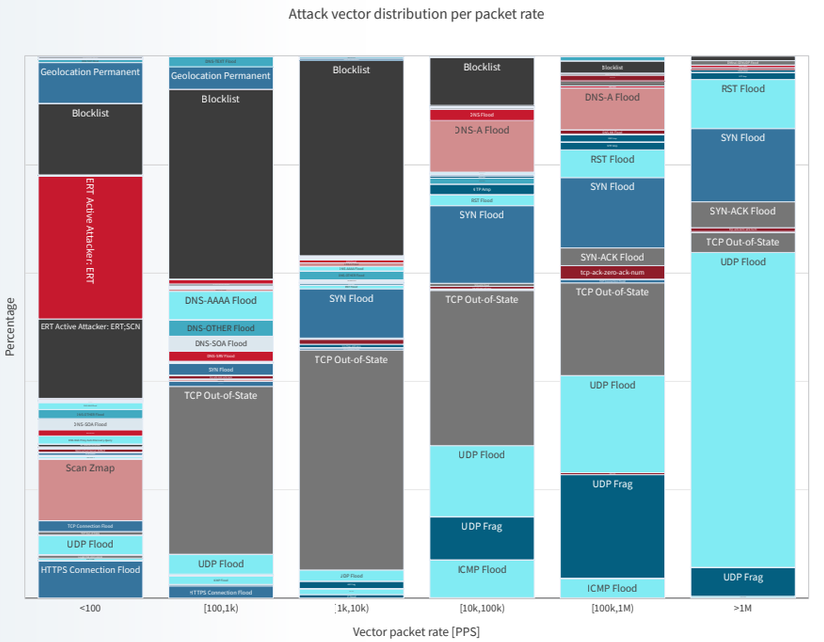


Figure 17: DDoS attack vector distribution by packet rate



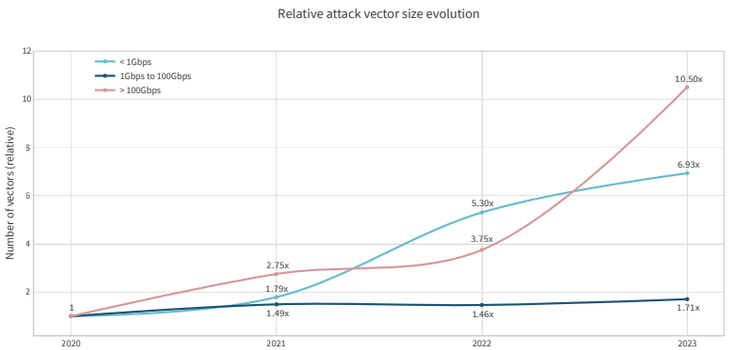
Attack Vector Characterization

A DDoS attack campaign consists of one or more attack vectors running simultaneously or sequentially over the time of the attack. In this section, individual attack vectors are analyzed to understand and characterize the nature of the DDoS attack threat landscape during H1 2023.

To compare the size evolution, attack vectors are divided 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 the number of vectors in 2020, the relative vector size evolution over time can be compared. For H2 2023, we assume an equal volume of attack vectors in the second half compared to the first half.

Figure 18

Relative DDoS attack vector size evolution



Compared to earlier years, the relative number of mid-sized attacks grew very slowly. The number of small attack vectors grew, but not as fast as their growth last year. In contrast, large attack vectors in H1 2023 demonstrated a very steep growth compared to last year.

In conclusion, H1 2023 can be characterized as a period in which attack sizes rapidly grew larger.

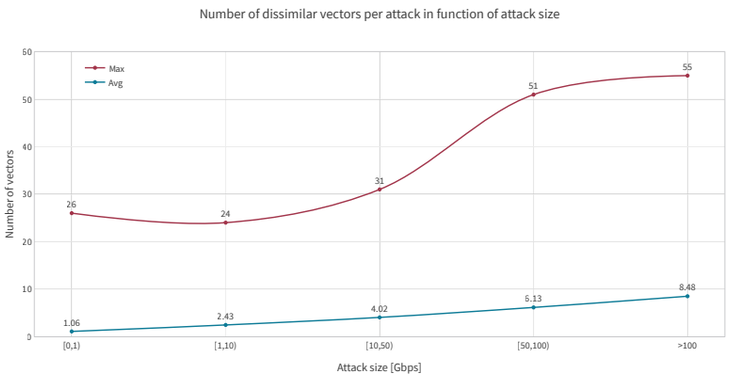
Attack Complexity

While a single attack vector can be devastating, attackers will often leverage multiple and dissimilar vectors to increase the impact, confuse detection and 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 using manually crafted access control lists. While changing attack vectors is usually 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 using multiple concurrent or changing attack vectors are harder to mitigate. Fast shifts and high numbers of concurrent vectors are impossible to mitigate without automated mitigation solutions.

Figure 19

Number of dissimilar DDoS attack vectors per attack as a function of attack size



The average complexity of attacks in H1 2023 increased with attack size. Since the average number of attack vectors in a single attack can't be smaller than one, smaller attacks exhibited a more isolated character as their average vectors per attack came closer to this number. Attacks above 1Gbps on average had more than two dissimilar attack vectors per attack, which almost doubled in number for attacks above 10Gbps. Attacks above 100Gbps had on average more than eight dissimilar attack vectors with the most complex attacks leveraging 55 dissimilar attack vectors.

Application-layer Attacks

DNS Floods

The digital era has catalyzed rapid growth in online commercial activities, making e-commerce and online platforms a vital component of the global economy. However, this technological advancement is not without its vulnerabilities. A crucial and ubiquitous part of this digital ecosystem is DNS, which acts as the internet's phonebook, translating human-readable domain names into their underlying IP addresses. When a DNS service is subjected to a cyberattack, such as denial-of-service or distributed denial-of-service, the disruption caused can be catastrophic for businesses.

DNS denial-of-service attacks come in various forms, each with unique techniques and impacts. Here are the most common attack types:

DNS Amplification Attack

This is a type of network-level, reflection-based, volumetric DDoS attack where the attacker crafts a DNS query packet with a forged source IP address (the victim's). It sends it to a legitimate open DNS resolver which subsequently replies to the victim with a large amount of data. The goal is to overwhelm the victim's network with traffic.

DNS Flood Attack

A DNS Flood is a type of application-layer DDoS attack that seeks to overload a DNS server with a high volume of requests until it becomes unresponsive. The requests appear legitimate, making it difficult to filter out malicious traffic.

DNS NXDOMAIN Attack

In this type of DNS Flood attack the attacker sends a high volume of requests for non-existent or invalid domains, resulting in DNS recursion and NXDOMAIN (nonexistent domain) responses. The server must work hard to try and resolve these spurious requests, thereby consuming valuable resources instead of processing legitimate requests. When a DNS server is under NXDOMAIN attack, the cache of the DNS server will be flooded with NXDOMAIN results, forcing the server to resolve legitimate requests repeatedly instead of fetching the answer from its cache.

Phantom Domain Attack

This attack involves the attacker setting up one or more phantom domains that do not respond to DNS queries and sending requests to the victim's DNS server to resolve the phantom domains. The victim's DNS server gets overwhelmed when it tries to resolve the phantom domains through non-responsive servers. This causes the recursive server to spend valuable resources waiting for responses that will never come.

Pseudo Random Subdomain (PRSD) Attack

Also known as water torture attacks, this attack is similar to the DNS NXDOMAIN attack. The attacker sends a massive number of requests for non-existent subdomains of a valid and existing domain through different recursive resolvers. This causes the authoritative server to consume resources trying to resolve these non-existent subdomains, eventually leading to a denial of service.

In each case, the attacker's objective is to disrupt the DNS service and make the websites and online services that rely on it inaccessible. These attacks exploit different aspects of the DNS protocol, making them challenging to defend against and highlighting the importance of implementing robust DNS security measures.

DNS amplification attacks are discussed in the Attack Protocols section (page 16). This section analyzes DNS Flood attacks or L7 DNS query flood attacks that aim to overwhelm a DNS server with a high volume of illegitimate requests.

By determining the proportion of DNS Flood attack events or vectors directed specifically at DNS services in relation to the overall event count, we can gauge the progression of DNS Floods over time, irrespective of the total activity or number of customers protected by the Cloud DDoS Protection service.

Throughout 2021 and most of 2022, fewer than nine out of every 1,000 attack vectors was a DNS Flood vector. However, from Q4 of 2022, we noted a marked increase in the proportion of attacks featuring a DNS Flood vector. The ratio experienced a twofold surge, rising to almost 18 attacks per 1,000 in Q2 2023.

The area chart depicted in Figure 21 traces the development of the count of DNS Flood attack vectors according to each query type. A description of the key DNS record types can be found in Appendix A: Common DNS Record Types. The total number of DNS Floods mitigated each month corroborates the escalating trend discerned in the previous DNS Flood attack ratio. From September 2022 onwards, the monthly number of DNS Floods consistently surpassed the figures recorded in the preceding months.

DNS Floods are application-layer assaults with the objective of compromising the server's capability to manage valid DNS requests. The pace of these requests determines the total effect on the server. The blue trajectory in Figure 22's chart illustrates the highest DNS query rate detected each quarter, denoted in queries per second (QPS). Aside from a notable DNS Flood attack in Q1 2021, which peaked at 1.59 million QPS, the DNS Floods since Q4 2022 were

Figure 20: DNS Flood attack vector ratio evolution over time

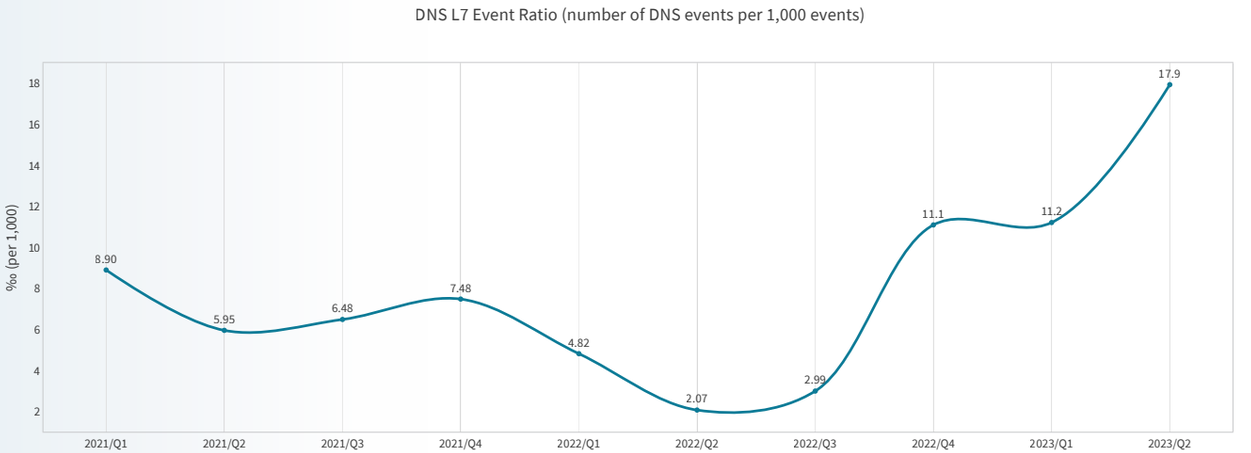
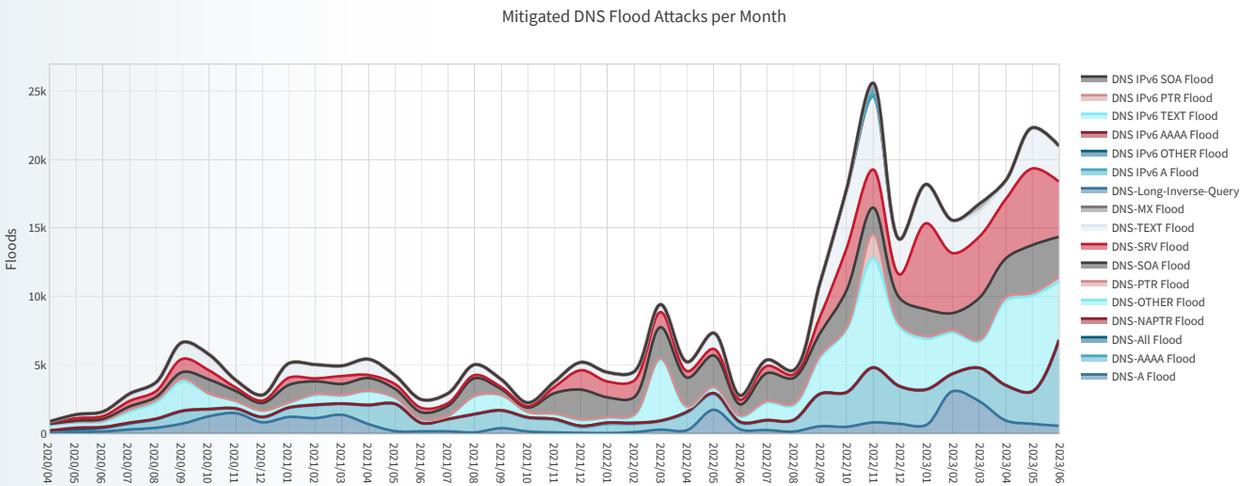


Figure 21: Number of DNS Floods per month



significantly larger in scale compared to previous quarters. The largest DNS Flood in the past two years was observed in Q2 2023, registering an attack rate of 1.29 million DNS queries per second.

The red trajectory in Figure 22's chart demonstrates the peak traffic of the most significant DNS Flood each quarter. The traffic rate shows a consistent pattern aligning with the maximum query rate. It is important to understand that application-level attacks focus on overloading the server, which does not necessarily equate to a traffic volume high enough to saturate the server's internet connection. The red line emphasizes this point; considering that the most substantial DNS Flood recorded a traffic volume of less than 1.3Gbps, all the DNS Floods monitored over the past two years remained under the 1Gbps threshold.

The most prevalent DNS query leveraged in DNS Floods in H1 2023 was the regular hostname to IPv4 query, accounting for 76.5% of all DNS Floods. The second most used was the MX query with 6.14%, followed by the TEXT (5.56%) and OTHER (4.89%) queries. The hostname to IPv6 address resolution query, AAAA, was the fifth most leveraged query type and represented 3.79% of all DNS query floods.

Figure 22: Queries per second and bandwidth consumption by DNS Floods

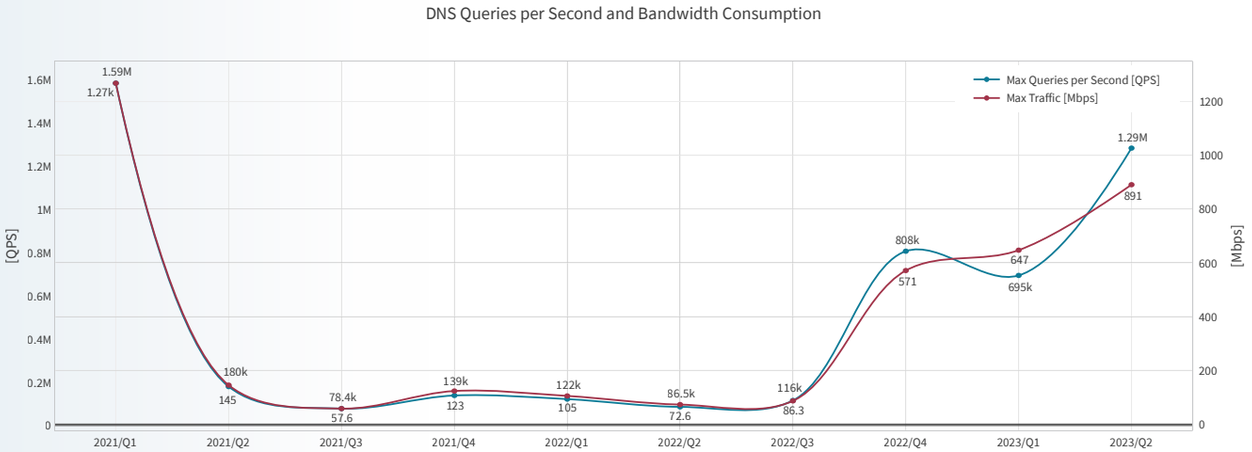
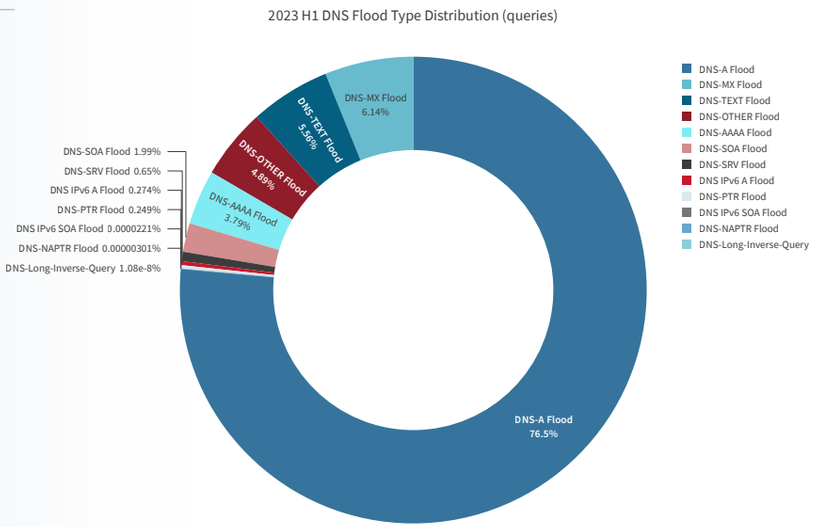


Figure 23

DNS Flood type distribution in H1 2023



Web DDoS

Network-layer attacks are better understood and arguably easier to detect and mitigate compared to the new generation of HTTPS Floods organizations are facing in 2023. Since HTTPS Floods have been around for a few years, they are sometimes considered old news. However, the volume and intensity of the new generation of HTTPS Floods has increased dramatically, and the sophistication introduced by attackers is growing quickly and viciously. That is why we like to refer to these new-generation HTTPS Floods as Web DDoS attacks.

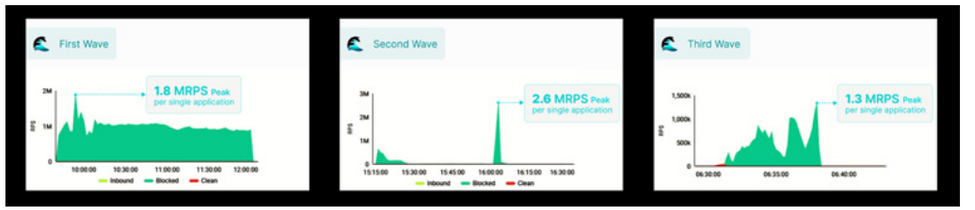
A 2.8 million RPS Web DDoS Attack

As an example, one of our customers became the target of a Web DDoS attack consisting of multiple attack waves and alternating attack vectors. One of the most threatening attack vectors was a Web DDoS attack vector that performed 2.8 million seemingly legitimate encrypted web application requests per second. Radware's new Web DDoS Protection service was able to eliminate the threat and handle the attacks, ensuring the customer's online applications remained available and uninterrupted.

The campaign, which lasted a total of four days, targeted multiple customer applications and consisted of three significant attack waves. The waves lasted for 2.5, 1.5 and 0.5 hours, respectively. The cumulative attack duration across all applications amounted to 20 hours.

Figure 24: Three Web DDoS attack waves spread over four days

Figure 25: DDoS attack wave detail per single targeted application



The attack originated from a large-scale anonymizing proxy network spanning multiple countries, including, among others, Sweden, the United States, Denmark, Morocco, Poland and Italy. Approximately 30,000 unique source IPs participated in the attack. Before being proxied through the anonymizing proxies, the attack traffic was generated from an attack infrastructure consisting of several public cloud-hosted servers.

The attackers employed various methods to increase the impact of their attacks and evade regular security measures, including:

- Encrypted requests (HTTPS)
- HTTP GET requests designed to appear legitimate
- Techniques that included HTTP/2 multiplexing for improved effectiveness
- Alteration of request patterns at different stages of the attack

It's important to note that, despite these changing tactics, Radware's algorithm swiftly detected and updated security measures in real time.

Figure 26: Samples of crafted HTTP GET requests disguised as legitimate web requests

Network Scanning and Exploit Activity

Not all malicious events that target internet-exposed 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, information disclosure attempts for reconnaissance, and path traversal and buffer overflow exploitation attempts designed to render a system inoperable or provide access to sensitive information.

In H1 2023, half of the attack events were DoS attacks and 22% were network intrusion attacks. 27.4% of the blocked attacks were identified as known culprits in the Radware active attackers threat intelligence feed. The ERT Active Attackers Feed (EAAF) is a feed comprising devices found to be actively scanning or randomly exploiting the internet which were caught in the Radware Global Deception Network or GDN. See Unsolicited Network Activity section (page 43) for more information on the GDN and the type of activity caught in our honeypots.

The information disclosure exploit (DNS-named-version-attempt) is used by malicious actors to identify the version of the Bind-named[1] DNS service. This is the first period in which this DNS server information disclosure exploit has led the charts and it does so with three times as many attempts as the runner up.

Half of the top ten network intrusions were related to known log4j exploits. The December 2021 publicly disclosed log4j vulnerability, dubbed Log4Shell, attracted huge attention across the security community. This vulnerability in a commonly used Java logging library allowed an unauthenticated attacker to leverage publicly available exploit tools for remote command execution (RCE). Log4shell was the most critical vulnerability of 2021, and some even argued it was the worst vulnerability of the decade.

1. BIND is a suite of software for interacting with the Domain Name System. Its most prominent component, named, performs both of the main DNS server roles, acting as an authoritative name server for DNS zones and as a recursive resolver in the network (source: Wikipedia).

Figure 27

Attack categories by event count

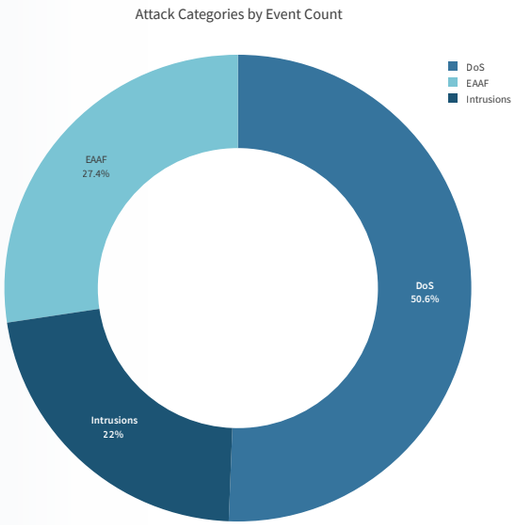
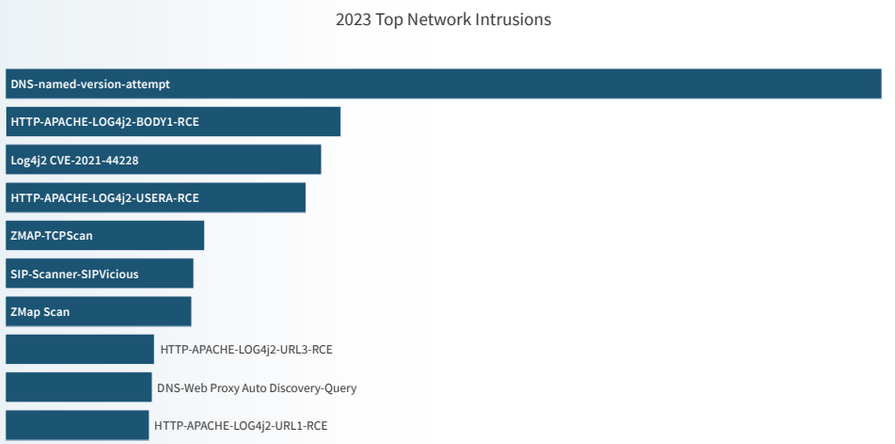


Figure 28: H1 2023 top network intrusions (see Appendix B: Radware Network Intrusion Signatures)



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 easily extract confidential information such as cloud secrets and API keys or to escalate privileges on compromised systems, move laterally across the network, and access backend databases and information stores accessible by the application.

Positions five to seven in the top 10 network intrusions were taken up by the scanning tools ZMap and SIPVicious. 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. SIPVicious, 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, and password brute-forcing and scanning for known vulnerabilities.

In ninth position we find another DNS information disclosure attempt, DNS Web Proxy Auto Discovery Query. The Web Proxy Auto Discovery (WPAD) Protocol is a method used by clients to locate the URL of a configuration file using DHCP or DNS discovery methods. Once detection and download of the configuration file is complete, it can be executed to determine the proxy for a specified URL.

The information disclosure exploit (DNS-named-version-attempt) is used by malicious actors to identify the version of the Bind-named DNS service. **This is the first period in which this DNS server information disclosure exploit has led the charts and it does so with three times as many attempts as the runner up**

Hacktivism

Hacktivism is a complex phenomenon that can be motivated by various factors, including religious and political beliefs. While hacktivists may have different motivations and methods, they all share a desire to use technology to advance their cause and to challenge those they believe are acting against it.

Hacktivists use a variety of tactics to achieve their goals, and the specific tactics they use depend on their motivations and the resources they have at their disposal. Their methods are constantly evolving as new technologies and platforms emerge. While some tactics may be illegal or unethical, hacktivists argue that they use their skills to promote social or political change and hold powerful organizations and governments accountable for their actions.

Some common tactics used by hacktivists include DoS attacks, website defacements, data breaches and media publicity campaigns.

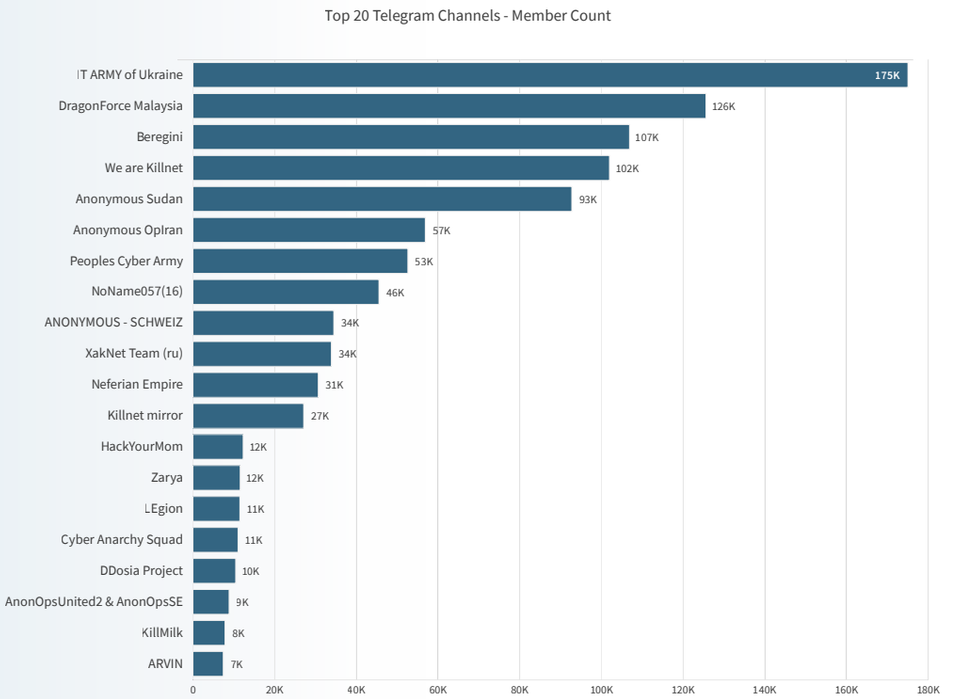
Patriotic Hacktivists

Shortly after the start of the invasion of Ukraine, the vice prime minister of Ukraine, Mykhailo Fedorov, announced the creation of a volunteer cyber army to fight Russian propaganda and protect the interests of Ukraine in cyberspace. The IT Army of Ukraine mainly coordinates its efforts via Telegram and Twitter. The IT Army of Ukraine Telegram channel gathered over 175 thousand members in a little over a year. It became one of Telegram's largest active hacker channels, surpassing by a good margin the DragonForce Malaysia channel known to be one of the largest and most social hacktivist groups before the invasion.

The emergence of pro-Russian hacktivists was a reaction to the Western cyber response countering Russia's invasion of Ukraine. Western hackers volunteering for the IT Army of Ukraine started conducting attacks against Russian targets, joined by factions of Anonymous under their battle tag #OpRussia, on the first day following the invasion. As a reaction, several opposing groups formed, amongst them a faction of Anonymous calling itself "Anonymous Russia." Soon a cluster of pro-Russian hacktivist allies and affiliates started to form around a group called Killnet. After little

Figure 29

Top 20 hacktivist Telegram channels monitored by Radware Research (ranked by member count)



more than a year, the Killnet Telegram groups generated a following that matched DragonForce Malaysia but were still only two thirds of the following generated by the IT Army of Ukraine in the same timeframe. Other notable pro-Russian hacktivist groups generated much lower followings compared to the largest groups.

NoName057(16), a pro-Russian hacktivist group that does not want to be associated with Killnet, generated a respectable following of over 46,000 members and its DDosia volunteer botnet project generated 10,000 members. Killnet cluster members such as XakNet Team and Zarya respectively generated 34,000 and 12,000 members. The leader of Killnet, Killmilk, was able to create a following of 8,000 members on his personal Telegram channel.

Killnet, one of the authors behind several highly visible and impactful campaigns in 2022, was relatively quiet in terms of actual DDoS campaigns in H1 2023. However, Killmilk, the media savvy leader of Killnet, was able to make headlines on several occasions by authoring highly visible statements on a new world order, attempts to establish a private military cyber company named Black Skills, and a cooperation between REvil, Anonymous Sudan and Killnet designed to take down the European financial system. None of the projects announced by Killmilk came to fruition. Killnet has a habit of starting new endeavors that bleed out and leave little but hot air in their wake.

Religious Hacktivism

Politically driven patriotic hacktivists have been a growing presence since the start of the war in Ukraine. By contrast, the threat from religious hacktivists continues on a path established over several years. A new group called Anonymous Sudan made a lot of headlines in H1 2023 when its attacks aligned (possibly coincidentally although the relationship is open to debate) with pro-Russian hacktivists. Anonymous Sudan, is an allegedly Sudan-based pro-Muslim hacktivist group that was announced as a Killnet cluster member by Killmilk after the group attacked Sweden and Denmark for the burning of the Quran outside the Turkish embassy in Stockholm by the Danish-Swedish right-wing activist Rasmus Paludan.

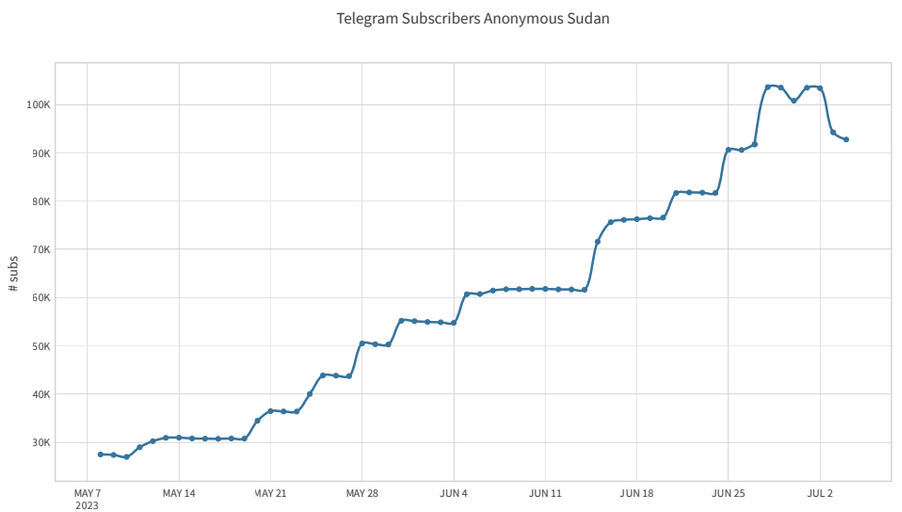
There is still a lot of controversy and confusion surrounding Anonymous Sudan as a religiously-driven and Sudan based activist group. In a report following the DDoS campaigns that targeted Swedish and Danish websites in February 2023, the security firm Truesec concluded that Anonymous Sudan is a false flag operation by the Russian government, leveraged as an information operation to harm and complicate Sweden's NATO application. After targeting Sweden and Denmark, the pro-Islamic group put its crosshairs on French airports, education, healthcare and government websites in response to a cartoon of the Prophet Muhammed published by the French magazine Charly Hebdo several years ago.

Pro-Islamic hacktivist crews Team insane pk, Eagle Cyber, and Mysterious Team targeted Australia because an Australian fashion label featured models wearing designs with "Allah walks with me" inscribed on them in Arabic. Subsequently, Anonymous Sudan joined the #OpAustralia campaign and started targeting Australian businesses and government websites with DDoS attacks.

More recently the group ventured in politically driven campaigns against countries that mocked the power struggle that broke out in April 2023 in Sudan between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF). In the final few weeks of H1 2023, Anonymous Sudan turned to Ransom DDoS, asking for millions of dollars in ransom from high profile organizations including

Microsoft. Microsoft later reported that Azure and Office Cloud services had been affected by the attacks of an unspecified hacker group. The report demonstrates the effectiveness and capabilities of a group such as Anonymous Sudan and emphasizes the need not to take the threat from hacktivists for granted.

Figure 30: Anonymous Sudan Telegram subscribers



In Q2 2023, Anonymous Sudan was able to more than triple its Telegram subscriber count from less than 30,000 subscribers to more than 90,000, peaking above 100,000 subscribers at the end of June. The attention they got from their highly visible attack campaigns and their early inclusion as an official member of the Killnet cluster all contributed to their rapid growth.

Hacktivist campaigns targeting India have been on the rise in H1 2023, mostly due to negative sentiments spread through social media campaigns such as "Islamophobia_in_India" and "SaveIndianMuslims." These campaigns often involve the sharing of fake content by people in India and abroad who have strong ideological biases.

In 2022, India was targeted by a series of hacktivist incidents that lasted for two months. These campaigns were initiated by a prominent hacktivist group called DragonForce Malaysia, under the campaign OpsPatuk. Many other hacktivists who shared the same ideology also participated. The campaign continued under the name OpIndia after DragonForce Malaysia distanced itself from OpsPatuk in June 2022.

Throughout 2022, intermittent hacktivist attacks against Indian entities continued. Then, in February 2023 a group called Team Insane PK restarted the OpIndia campaign on Kashmir Solidarity Day. They launched cyberattacks and leaked documents from the Indian government and private organizations. Since then, they have collaborated with other anti-India hacktivists.

Team Insane PK is operated by a group of individuals. Two of them are known as Mr Insane and HOAX1337. Besides targeting India, they have also attacked websites in other countries such as the Philippines, Sweden, Afghanistan, Russia, Dominican Republic, Indonesia and Brazil. Interestingly, they have also targeted government websites in Pakistan, using religious reasons to justify their attacks.

In March 2023, another hacktivist group called Mysterious Team Bangladesh started a campaign named "Operation Payback." They launched multiple cyberattacks against Indian websites and publicized their actions on social media and internet messaging channels. This campaign was a response to Indian hacktivists targeting websites in Pakistan, Bangladesh, Indonesia and Malaysia.

Mysterious Team Bangladesh also leaked files from past security breaches. These files included various identification documents such as Aadhaar cards, PAN cards, passports, old bank statements, invoices, checkbooks and scanned payment cards. Most of the leaked documents were outdated, but some were still valid. The group has a history of conducting pro-Islamic hacktivist campaigns against several countries. They claim to have been active since 2012 and have been involved in previous campaigns including OpIndia, OpsPatuk and OpIsrael. Other hacktivist groups that supported

these campaigns included Ganosec Team, Hacktivist of Garuda, Khalifah Cyber Crew and Eagle Cyber Crew.

In March 2023, during Ramadan, Eagle Cyber Crew and eight other groups from Malaysia, Bangladesh, Pakistan, Indonesia, Yemen, Vietnam, Sudan and Palestine launched a campaign called #opsjentik. These groups believe that Indian Muslims are victims of social injustice which justifies conducting cyberattacks against India. They were also involved in the OpIsrael campaign.

Eagle Cyber Crew, claiming to be from Malaysia, created its Telegram channel in December 2022. They identified themselves as part of the "Army of Mahdi" and the "Anti Dajjal Community," referring to figures from Islamic scripture.

On April 19, 2023, Eagle Cyber Crew, along with other hacktivist groups including 4-EXPLOITATION, Khalifah Cyber Crew and Tiger Cyber Crew, started a campaign called OpAbabeel. This campaign was in response to Indian hacktivists leaking data of Muslim citizens. They used tactics including DDoS attacks, web defacement and selling compromised Indian databases. However, the data samples they shared were actually from a 2020 leak by another threat actor. In this campaign, their main targets were Indian government entities, the judiciary and educational institutes. They also targeted companies in Mexico, the United States, Ghana and Cyprus.

Pro-Islamic hacktivist crews Team insane pk, Eagle Cyber, and Mysterious Team targeted Australia because an Australian fashion label featured models wearing designs with "Allah walks with me" inscribed on them in Arabic

Another campaign called OpIndia2.0 was initiated by Indonesian hacktivist groups VulzSec and Hacktivist of Garuda on April 20, 2023. This campaign was retaliation against attacks on Indonesian government sites by Indian sympathizers. They planned to launch DDoS attacks on 54 entities, mainly the government websites of different Indian states. However, they stopped the campaign when approached by a pro-Indian hacktivist group called Kerala Cyber Xtractors. Other groups like Ganosec Team and Team Insane PK continued their attacks despite this truce.

On April 26, 2023, pro-Islamic groups started another campaign called #OpIndia23. This ongoing campaign aims to protest against perceived injustice and prejudice against Indian Muslims. Various hacktivist groups, including Mysterious Silent Force, DragonForce Malaysia, Mysterious Team Bangladesh, Pakistan Cyber Hunters, AnonGhost and others, are involved in this campaign. They claimed to compromise the government websites of Kerala, Rajasthan, Maharashtra, and Jammu and Kashmir, as well as leak related data.

In retaliation for attacks on Indian infrastructure, a few Indian-sympathizing hacktivists emerged from the shadows. They publicized their claims of DDoS attacks against organizations from Bangladesh, Indonesia, Malaysia and Pakistan on social media and Telegram channels. Among many such small factions, the following groups led coordinated waves of attacks: Anonymous India, Mariana's Web, Team UCC Operation, Indian Cyber Mafia, Indian Cyber Force, Team 1-4-1 and Kerala Cyber Xtractors.

Most Targeted Countries

Most of the claimed DDoS attacks in H1 2023 targeted India, United States, Israel, Ukraine and Poland, in that order. India was a constant target for the same pro-Islamic actors that moved focus to Israel and Australia for #OpIsrael and #OpAustralia. Poland was the fifth most targeted country because of its ongoing support for Ukraine which displeases pro-Russian hacktivists.

Figure 32 demonstrates that the activity by hacktivists is a global threat. Organizations across the globe, willing or not, are now in the crosshairs of hacktivists. There are exceptions such as Alaska, the North and South Poles and parts of Africa, Latin America and Asia.

Figure 31

Number of DDoS attacks claimed per country

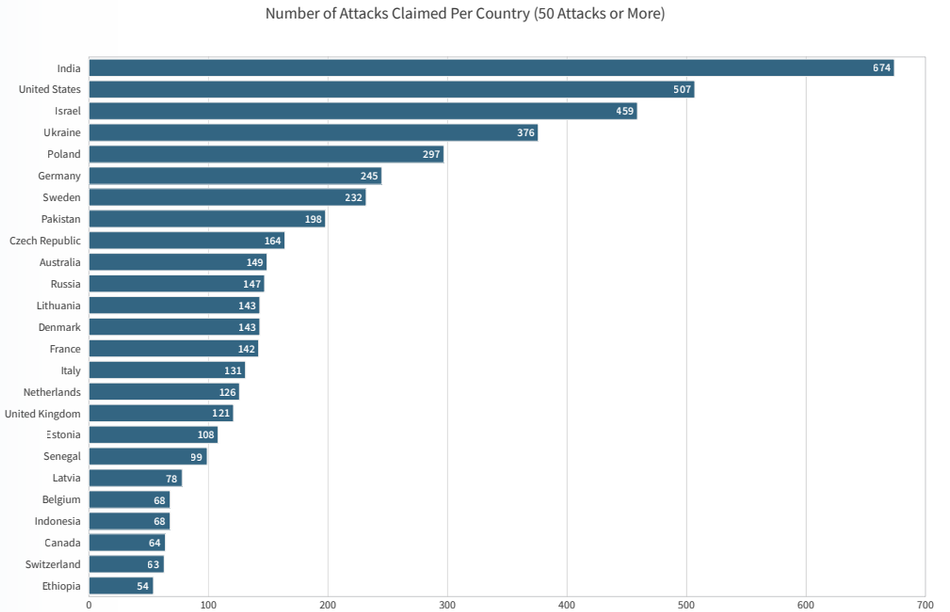


Figure 32

World heatmap of claimed DDoS attacks

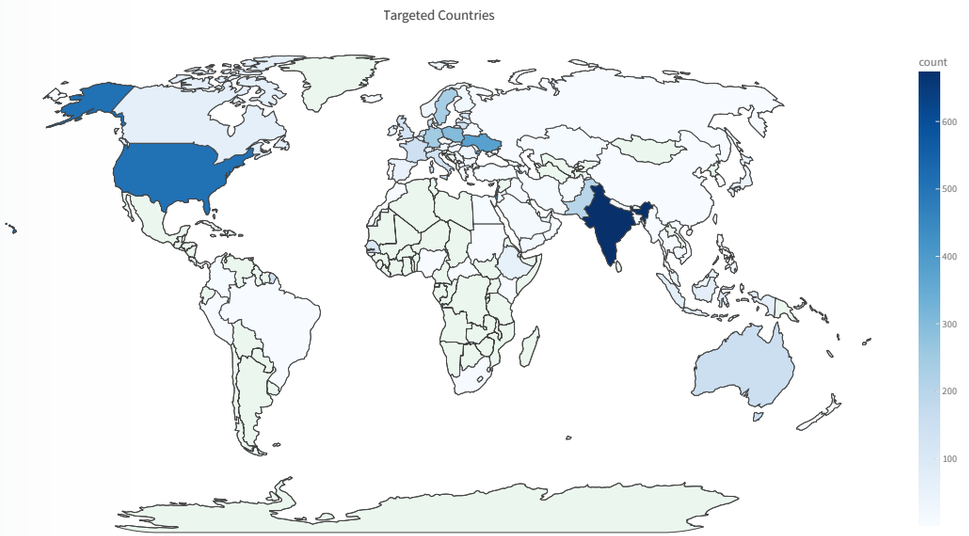
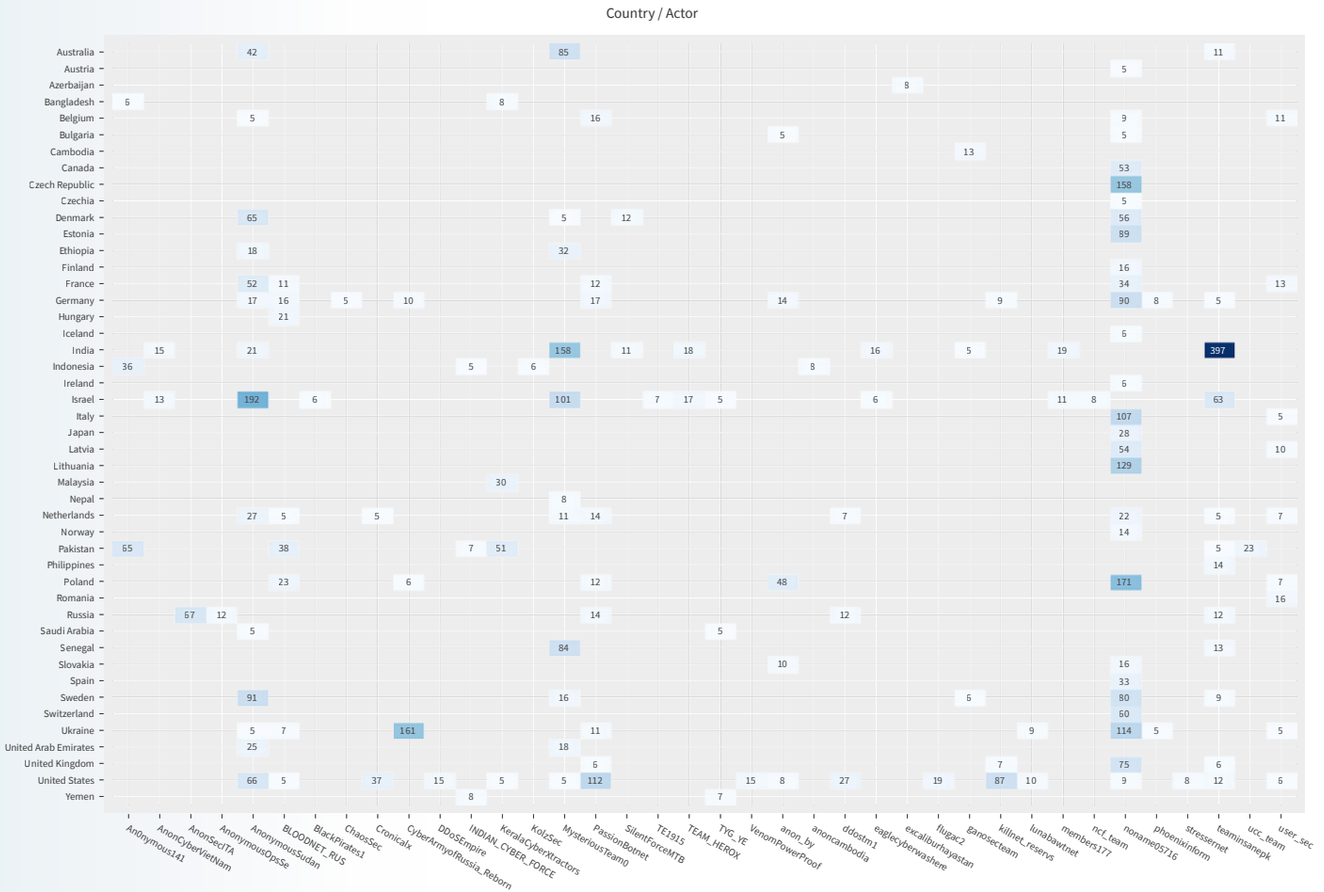


Figure 33 shows the frequency of claimed attacks by country and Telegram Channel. Several pro-Islamic hacktivist groups, including Mysterious Team, Anonymous Sudan, Team Insane PK, Anon Cyber Vietnam, Eagle Cyber, Nigeria Cyber Force, and Ganosec Team, targeted Israel, India and Australia. Meanwhile, Poland was targeted by pro-Russian hacktivist groups NoName057(16) and Anonymous Russia.

From the countries that NoName057(16) targeted, it is evident that this group focuses on Western countries that demonstrate support for Ukraine in its conflict with Russia. On the other hand, Mysterious Team, Team Insane PK, and Eagle Cyber were primarily motivated by religion and mostly targeted Israel and India.

Anonymous Sudan was active in many countries, but predominantly attacked Israel, Sweden, the United States, Denmark, France and Australia.

Figure 33: DDoS attacks claimed per actor by country (>5 attacks claimed)



Most Targeted Website Categories

Government, business/economy and travel websites were the most targeted categories, followed by those involved in financial services, health/medicine, society, news/media, education and the military.

Business/economy, government, travel and finance websites were the primary targets for NoName057(16). Government was also the most attacked category for Team Insane PK and Mysterious Team. Anonymous Sudan has an outspoken preference for health/medicine and travel websites.

Note that travel includes websites for airports and seaports, two categories that were often targeted by hacktivists.

Figure 34: Top website categories targeted globally

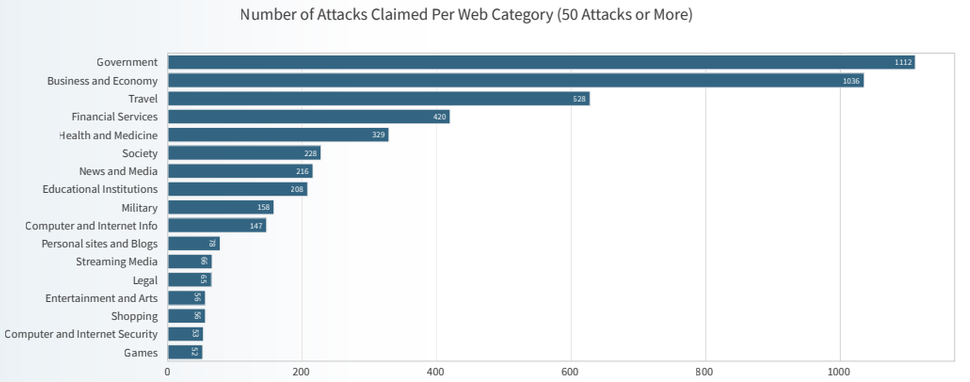
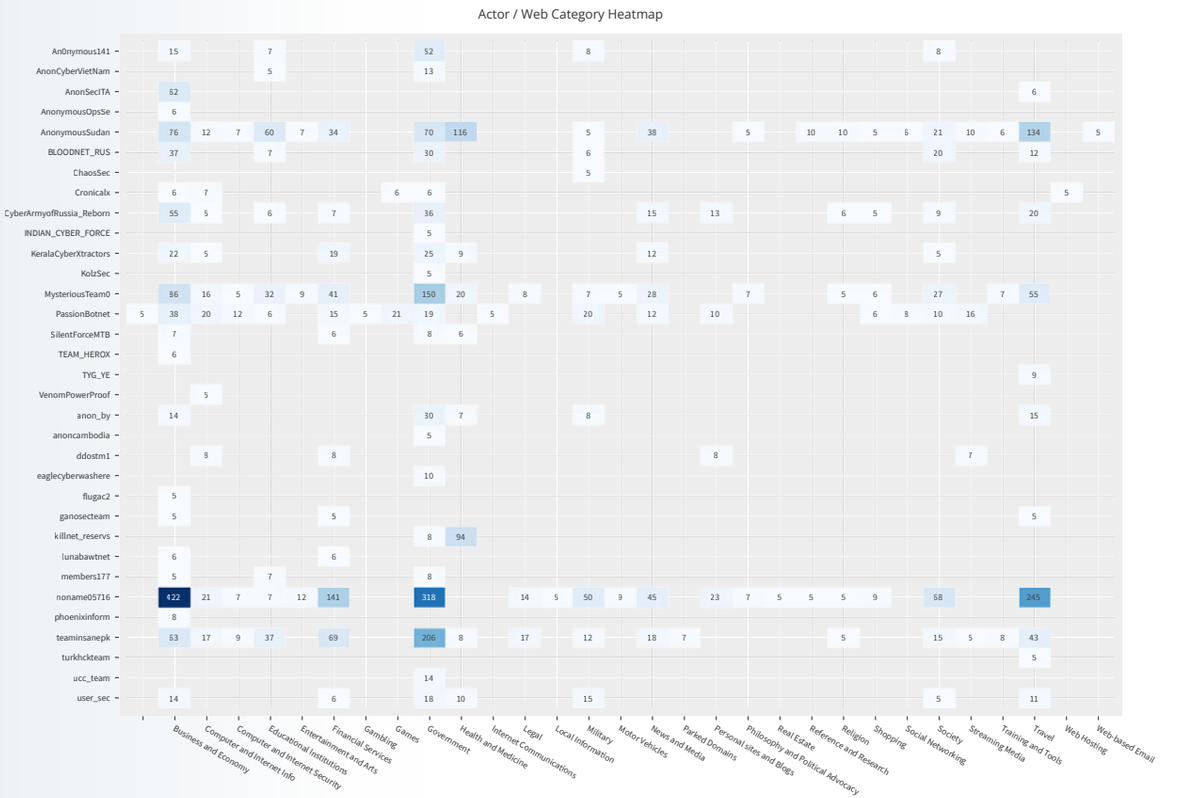


Figure 35: Number of DDoS attacks claimed by website category (> 5 attacks claimed)



Top Claiming Actors

With more than double the number of DDoS attacks claimed than the runner-up, NoName057(16) was by far the most active hacker group on Telegram. Anonymous Sudan was in second place by a significant margin to like-minded groups Team Insane PK and Mysterious Team in third and fourth place. Passion Botnet was in fifth place with almost half the latter's attacks, followed by the Cyber Army of Russia and Bloodnet in sixth and seventh place. Killnet took eighth place, with less than a tenth of the attacks claimed by NoName057(16).

Note that throughout the analysis only the first claim is assumed to be genuine. That means that the first actor claiming an attack will be attributed that attack rather than any subsequent actors. For example, Sharp3377 and Team Herox almost exclusively repost DDoS attack claims, something also seen with NoName057(16), Mysterious Team and Anonymous Sudan. However, in the latter three cases, the number of original posts far surpassed the number of reposted claims. Killnet_reservs (Killnet) meanwhile, reposted twice as many claimed attacks versus original claims.

Figure 36: Top claiming actors (50 DDoS attacks or more)

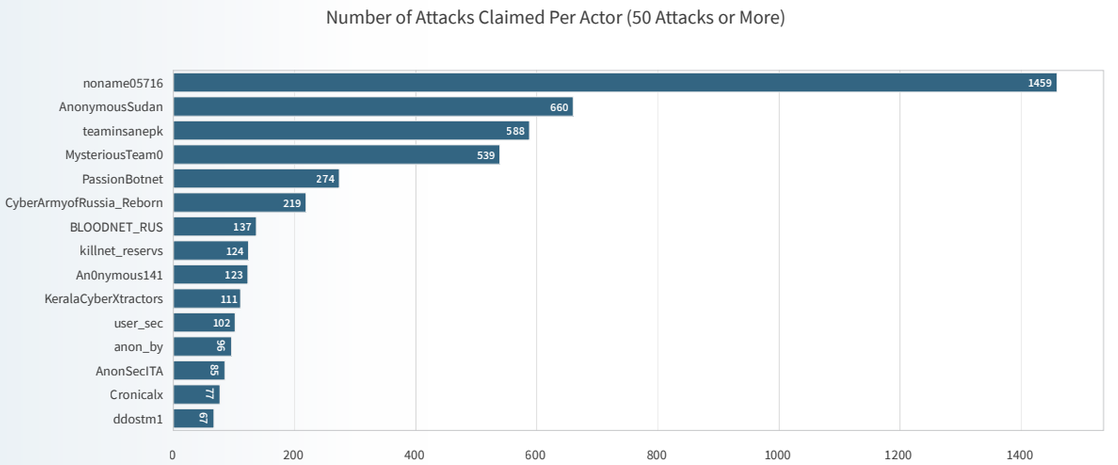
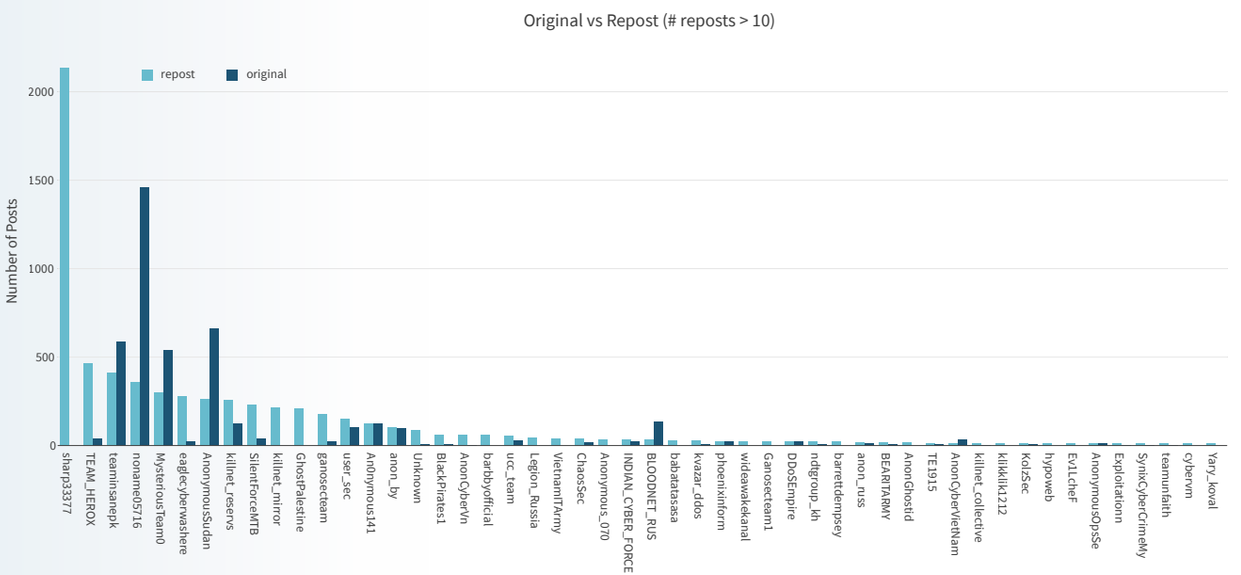


Figure 37: Number of reposts vs original claimed DDoS attacks per Telegram channel



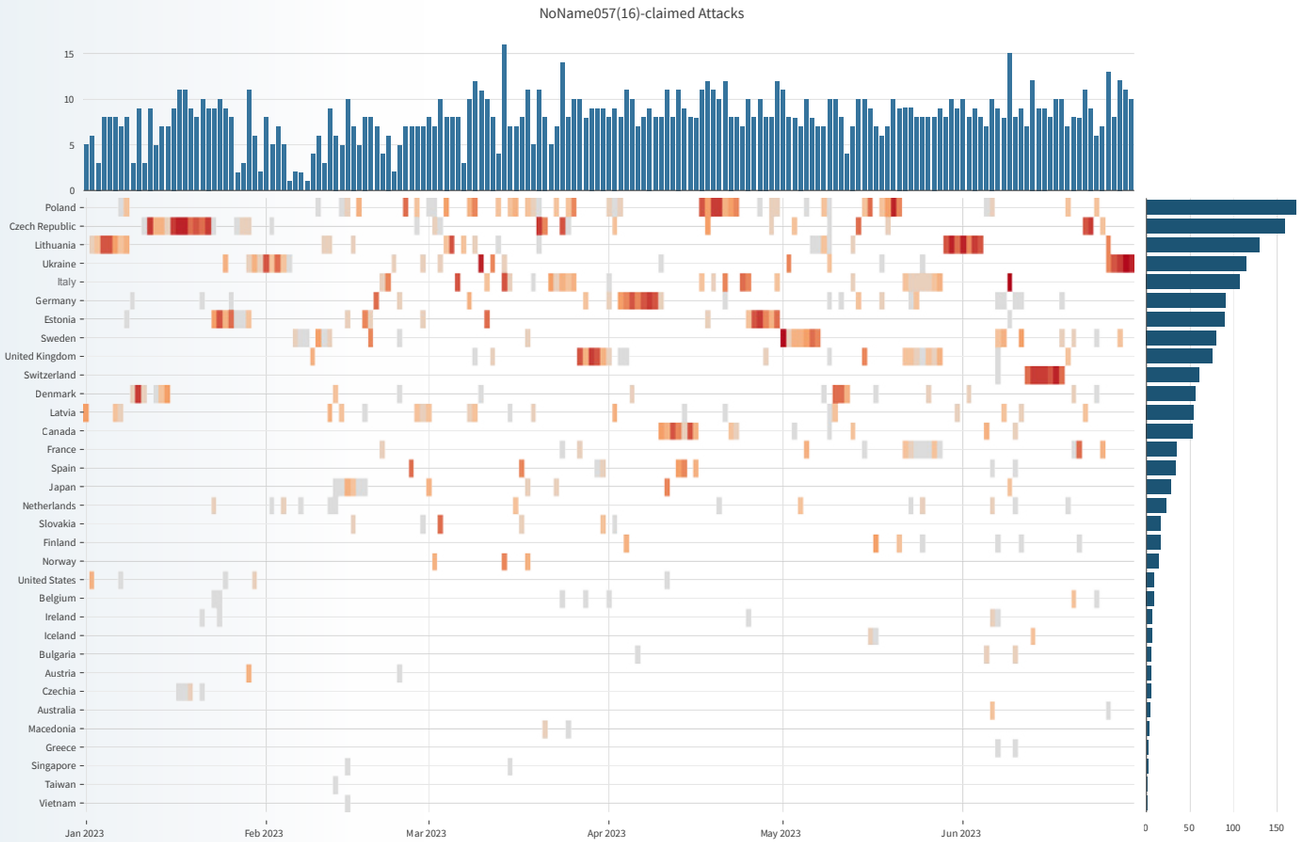
NoName057(16)

NoName057(16), by far the most active of the pro-Russian hacktivists, claimed more than 170 attacks targeting Poland. Czechia, Lithuania, Ukraine and Italy were also countries heavily targeted by NoName057(16) in H1 2023. NoName057(16) was also the only actor that claimed at least one attack per day between January 1, 2023 and June 30, 2023, with up to 15 DDoS attacks on some days. This feat was only possible by leveraging automation—in this case using project DDoSia. DDoSia is a volunteer, crowdsourced DDoS botnet that performs Web DDoS attacks around the clock on a curated list of websites updated daily by the NoName057(16) leadership team.

Anonymous Sudan

The security community is divided on the motivations behind the attacks claimed by Anonymous Sudan. Whether the group is a religious hacktivist, a Russian black flag operation, or a politically driven hacktivist, there is no doubt that the group was a problem for many organizations around the globe. Anonymous Sudan relies on an infrastructure that allows large-scale Web DDoS attacks to be performed and was more recently seen leveraging DDoS-for-Hire infrastructure as part of what appeared to be a marketing stunt. Anonymous Sudan is like a confused rebel with too many causes. One minute it wants to be a religious hacktivist, the next it

Figure 38: DDoS attacks claimed by NoName057(16) per country over time



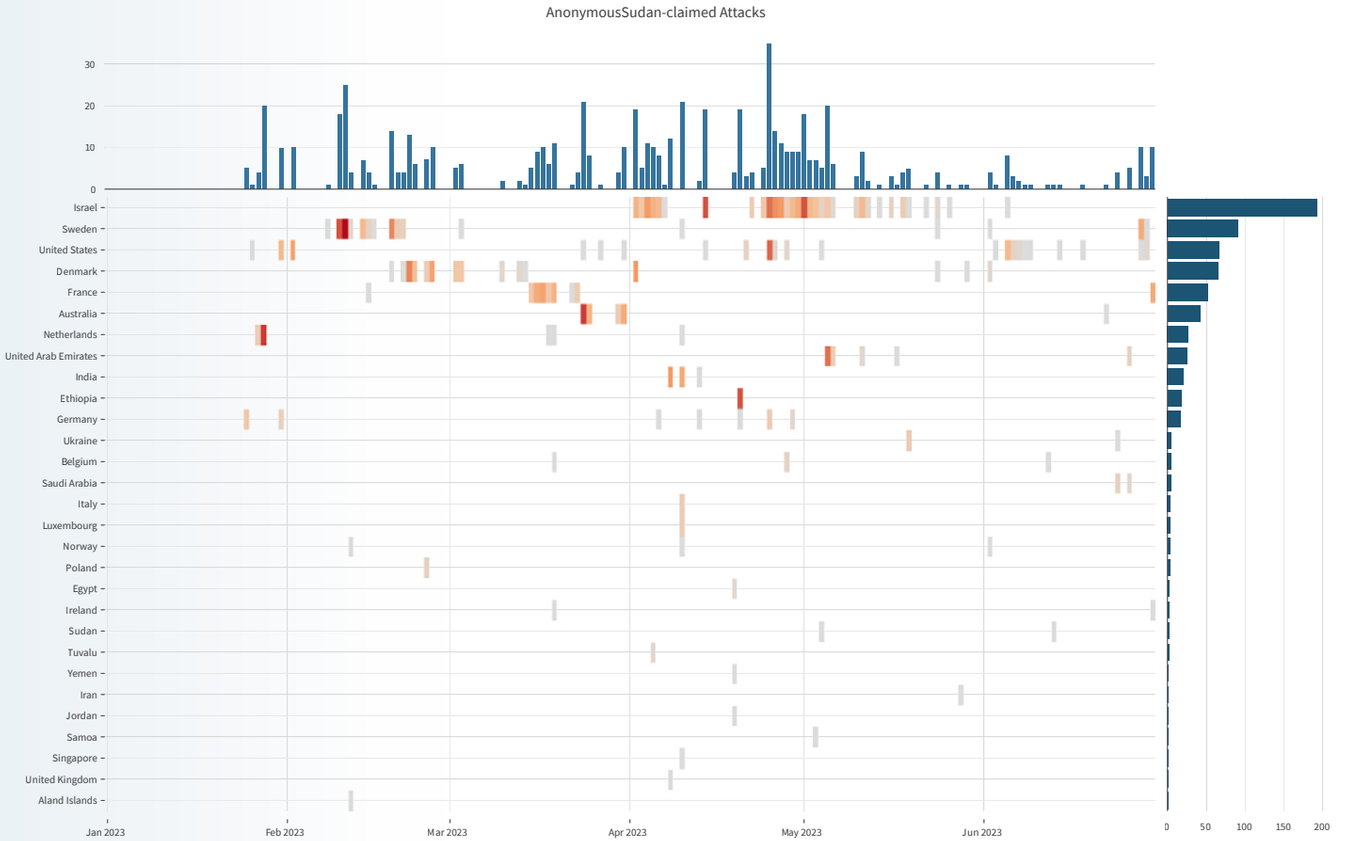
engages in Ransom DDoS and promotes DDoS-as-Service platforms, then it profiles itself as a political hacktivist.

Anonymous Sudan struck first in Germany on January 25, 2023, targeting the Bundesnachrichtendienst Federal Intelligence Service and several airports followed by more airports and healthcare institutions in the Netherlands. It attracted more headlines after campaigns targeting Sweden and Denmark in February 2023, after which the group was "knighted" a Killnet cluster member by Sir Killmilk himself.

The most attacked country by Anonymous Sudan, however, was Israel with 192 claimed attacks. Sweden was next with 91, followed by the United States, Denmark, France, Australia, the Netherlands, the United Arab Emirates, India, Ethiopia and Germany. The remaining countries had five or fewer claimed attacks.

The attack activity over time by Anonymous Sudan suggests a manually operated attack infrastructure.

Figure 39: DDoS Attacks claimed by Anonymous Sudan per country over time



Passion Botnet

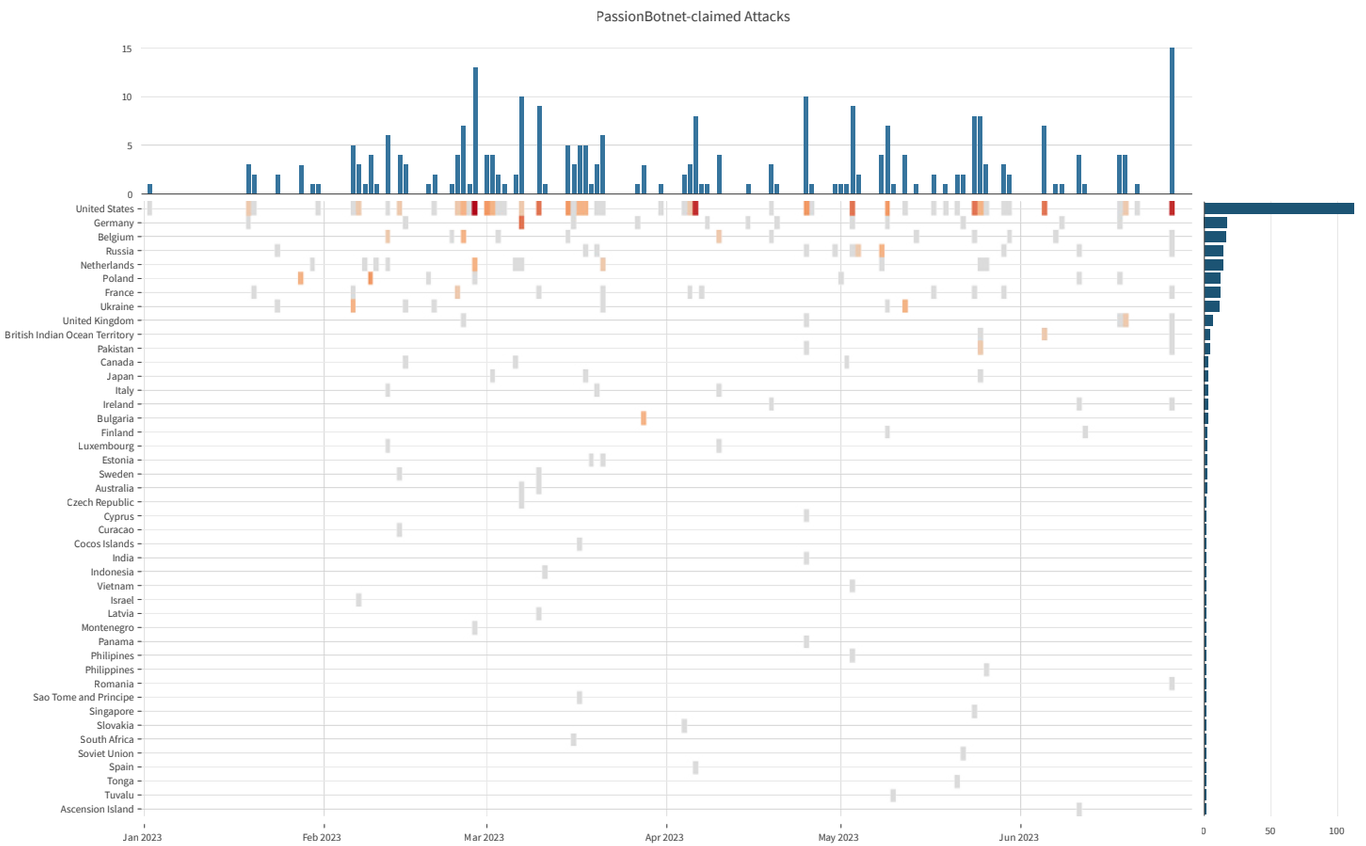
The origins of the Passion group remain unknown, but they have made their presence felt since the beginning of 2023. The group, affiliated with Killnet and Anonymous Russia, has been associated with web defacement and denial-of-service attacks targeting individuals and organizations unsympathetic to the Russian invasion of Ukraine. Passion has a strong online presence through its Telegram channels dating back to March 2022. Other hacktivist groups, such as Anonymous Russia, MIRAI, Venom, and Killnet have also promoted Passion.

The Passion group's tactics, techniques and procedures (TTPs) resemble those of the other hacktivist groups involved in the Russo-Ukrainian conflict. In H1 2023, however, Passion group began offering DDoS-as-a-Service attacks to pro-Russian hacktivists. The Passion Botnet was leveraged during the attacks on January 27, 2023, targeting medical institutions in the USA, Portugal, Spain, Germany, Poland, Finland, Norway, Netherlands and the United Kingdom as retaliation for sending tanks in support of Ukraine.

Because of its use of DDoS attacks to promote its DDoS-for-Hire services, the global spread of claimed Passion Botnet attacks was very evenly distributed with the exception of the United States against which Passion Group claimed 112 attacks. The targets claimed by Passion botnet are typically highly visible and well known targets such as Spotify, Netflix, Kaspersky, Twitch, Twitter and Nasa. The better known the target, the better the promotion for its services.

The group has been associated with attacks **targeting individuals and organizations unsympathetic to the Russian invasion of Ukraine**

Figure 40: DDoS Attacks claimed by Passion group per country over time



DDoS Tactics and Techniques

NoName057(16) – Reconnaissance

NoName057(16) operates a crowd-sourced botnet called Project DDoSia. That means the group provides client software (a bot) to its volunteers who download and run the software on their PC or cloud-rented hosts. The client software communicates with a command and control (C2) server. This is very aligned with IoT DDoS botnets with the difference that instead of being installed on compromised IoT devices it is installed on home PCs, mobile phones and cloud servers by volunteers. To make it more interesting, NoName057(16) provides financial incentives for those performing the most attacks.

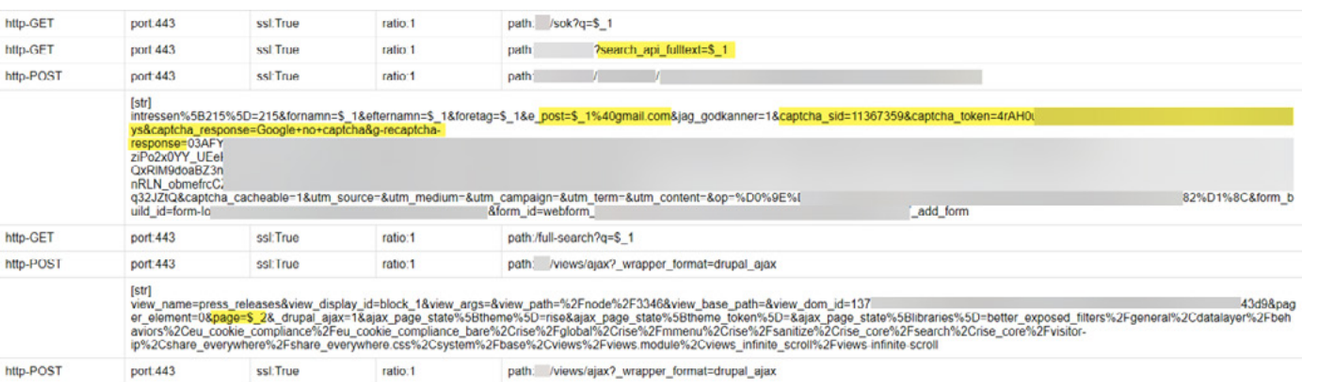
The group's admins update the list of targets on a daily basis and distribute them through a C2 server. The bots download the list of new targets and start executing attacks until the bot is either stopped or a new list of targets is provided. So far, this suggests nothing unusual about the attack technique.

However, what is new about NoName057(16) DDoSia attacks is that the group admins perform reconnaissance before staging their attack vectors. They investigate the target website and identify the most resource-intensive parts of the site. Pages which have a search function or provide a form to fill in are typical candidates. NoName057(16) records all the variables used by GET and POST requests for those pages, including any cookies and potential captcha keys and then crafts specific web requests with placeholders for random data to be leveraged as attack vectors.

When a bot receives the attack vectors, it will craft the GET or POST requests that contain legitimate parameters, arguments and cookies, and will randomize the data passed through the arguments for each request. The randomization of the data takes into account the type of data the application expects, for example for a phone number field the bot will generate a 7-12 digit random number. For email fields the bot will generate a random 10-15 alphanumeric sequence and append "@gmail.com" to it. The resulting request from the bot will look like a legitimate web page request or form post. Even a Web Application Firewall (WAF) or the application itself will not be able to detect any anomalies because the variable names will correspond to the names used by the web application and the contents of the variable will be within the bounds set by the application. The only difference between this and real requests is that the data will be completely random and would be recognized by a human operator as garbage.

All the volunteers that run a bot submit these legitimate looking requests as fast as their resources allow. This will create a lot of stress on the back end of the application, such as the database used for search queries and for storing the data of form posts. Also, after the attack, the person processing posted forms will have a nice surprise consisting of millions of new information requests of which only a small fraction will be legitimate requests. NoName057(16) is growing its following, but as of today we estimate their active volunteers to average somewhere in the low thousands.

Figure 41: Example of attack vectors targeting a single website captured from DDoSia C2 servers at any moment in time



The botnet does not generate millions of RPS, but because of the reconnaissance step, the attacks are still able to target the most important parts of a web application or API. In many cases, mere hundreds of RPS are enough to create issues in the back end infrastructure of the application.

The botnet is not perfect. Instead of using anonymizing proxies it relies instead on the volunteers running the bot to create a VPN tunnel to conceal its origins. This means that most requests from a single bot will originate from the same source IP and isolating the IP addresses performing several hundreds of requests per second will in most cases mitigate at least part of the attack. If the bot had leveraged per request anonymous HTTPS proxies, the requests would originate from tens of thousands of IPs and it would become much harder to correlate the hundreds of requests per second to a single source IP. The bot is written in Go and leverages the net/http Go package, which is reflected in the user-agent of the requests.

Anonymous Sudan – Cloud VPS and Anonymous Proxies

Anonymous Sudan leverages highly capable cloud-rented virtual private servers to create a bot infrastructure that is centrally orchestrated. During the attacks on Denmark, for example, Anonymous Sudan used 61 very capable cloud servers hosted in the IBM/Softlayer Cloud. Those 61 servers generated HTTPS request floods at very high rates in the range of 800,000 to 2 million RPS. To conceal its infrastructure and to make detection harder, the group leverages proxy and SOCKS servers to hide behind and change those proxies randomly for each request. There are several services that provide 100-200,000 anonymous proxies of which 10 to 20% of the IP addresses rotate on a daily basis. This results in high-scale encrypted HTTPS attacks seeming to originate from several hundreds of thousands of IPs. The attacks last anything from a couple of minutes to several hours.

Note that much larger hyperscale RPS HTTPS attacks have been recorded in the past by Google, Akamai and Cloudflare. The last was reported by Cloudflare in February 2023 and reached 71 million requests per second. However, these hyperscale attacks only lasted from a few seconds up to five minutes. The Anonymous Sudan attacks we observed were no higher than 1.8 million RPS, but the attack sustained a high RPS count for several hours.

Anonymous Sudan also leverages UDP and SYN floods to alternate its HTTPS attack waves. The floods originate from about 10,000 unique source IPs with UDP floods reaching up to 600Gbps. The HTTPS connection floods also leverage HTTP/1.1 connection pipelining and HTTP/2 multiplexing and use a CDN cut-through technique by appending "?<random-junk>" to each request.

The SOCKS network leveraged for HTTPS attacks is probably also used for direct path UDP and SYN floods. Some of the HTTPS proxies are running Squid in a forward proxy configuration on Ubuntu servers while some SOCKS services are compromised Mikrotik routers with SOCKS enabled.

Web Application Attack Activity

In H1 2023, the number of blocked malicious web application transactions grew by a staggering 500% compared to the first half of 2022. The high number of malicious web transactions underscores the earlier statement that DDoS attacks are moving to the application layer.

Compared to last year, malicious web transactions grew 366% in Q1 2023 and even faster in Q2 at 605%.

While in 2022 we observed a near linear growth in the number of malicious web transactions per quarter, in H1 2023 this accelerated to an exponential growth.

Targeted malicious web application attacks can be blocked by application-specific and custom rules, learned by inspecting the application and tuned by the Security Operations Center (SOC). The chart in Figure 45 shows that the share of targeted malicious transactions blocked by signature and behavioral detection modules remained mostly unchanged in the last three quarters. However, the bulk of malicious web transactions blocked were unsolicited and random attacks, not specifically targeting the application or a known web application exploit or vulnerability.

The remainder of this section considers attacks detected and blocked based on known malicious behavior, vulnerabilities, and exploits.

While in 2022 we observed a near linear growth in the number of malicious web transactions per quarter, **in H1 2023 this accelerated to an exponential growth**

Figure 42: Yearly blocked malicious web application transactions

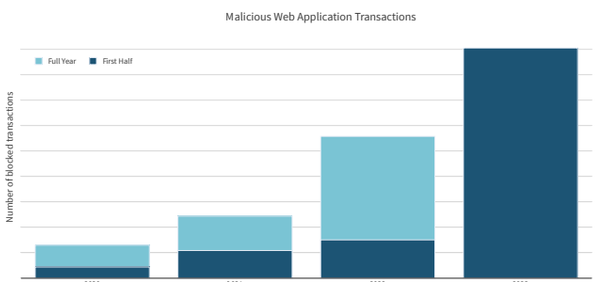


Figure 43: Quarterly blocked malicious web application transactions

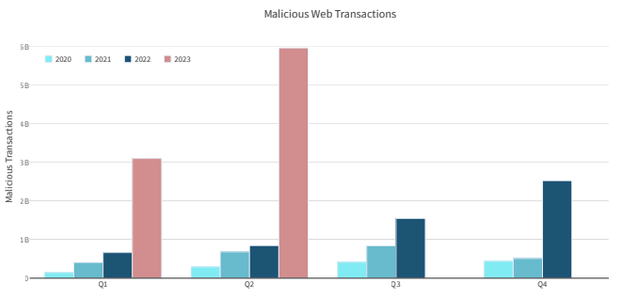


Figure 44: Blocked malicious web application transactions growth evolution

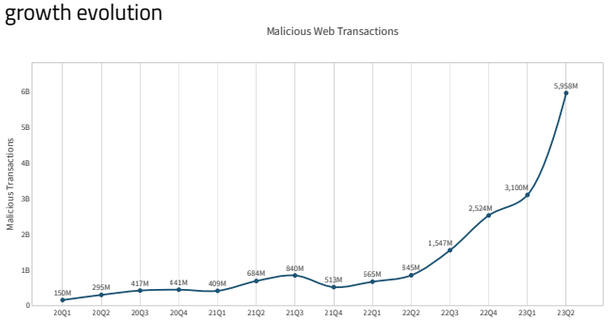
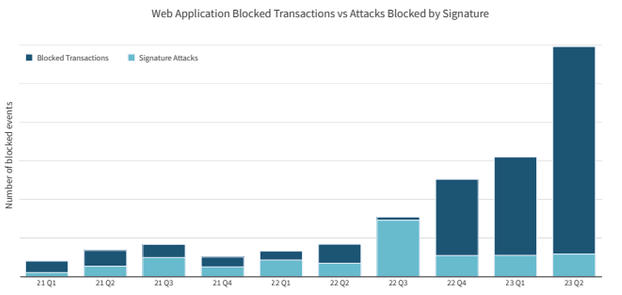


Figure 45: Web application transactions vs attacks blocked by signature



Security Violations

The most important security violation for H1 2023 (Figure 46), predictable resource location attacks, has always accounted for a significant part of the total attack count. Predictable resource location attacks target hidden content and functionality of web applications. By guessing common names for directories of files, an attack may be able to access resources that were not intended to be exposed. Examples of resources that might be uncovered through brute force techniques include old backup and configuration files and yet-to-be-published web application resources. SQL and code Injection were, respectively, in second and third position. Combined with predictable resource location attacks, these three web application attacks were responsible for 64% of the total attack activity on web applications and APIs.

In Q2 2023 (Figure 47), SQL injections became more prominent and for the first time were leveraged for attacks almost as often as predictable resource location.

Figure 46

Top security violation types for H1 2023

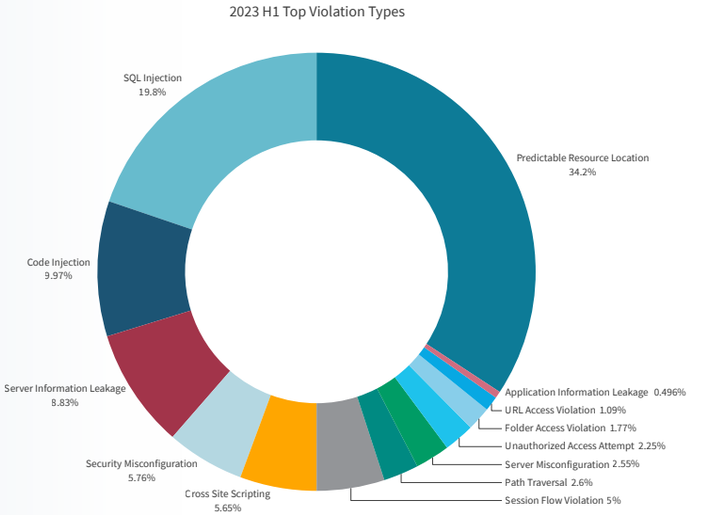
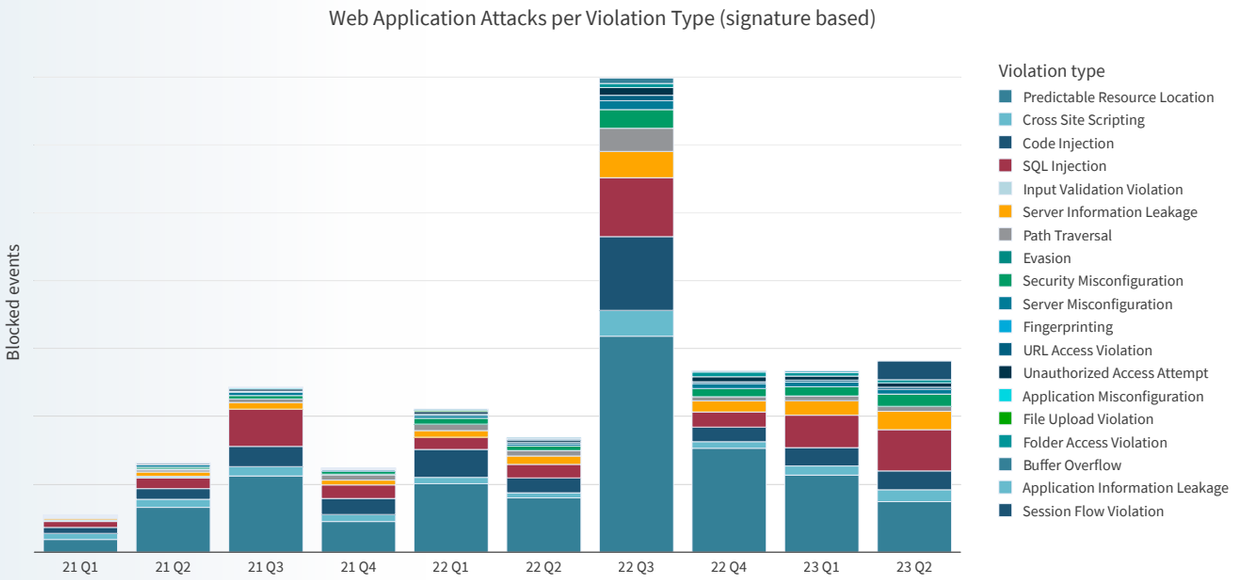


Figure 47: Evolution of violation types over time



Attacking Countries

Most blocked web security events in H1 2023 originated from the United States with Germany, Russia, United Kingdom and Italy completing the top five. The United States has dominated the attack scene and has consistently taken the number one spot in most quarters (Figure 49). It is important, however, to note that the country where an attack originates from does not have to correspond to the nationality of the threat actor or group. Arguably, the country where the attack originates will most often not be the home country of the threat actor. Threat actors leverage public cloud-hosted servers, anonymizing VPNs and proxies, the Tor network, and compromised servers as jump hosts to conceal the real origin of their attacks. The originating country of an attack is typically chosen based on the location of the victim to circumvent potential geo-based blocking. It can also be based on the country the threat actor wants to see attributed during false flag operations.

Figure 48

H1 2023 top attacking countries

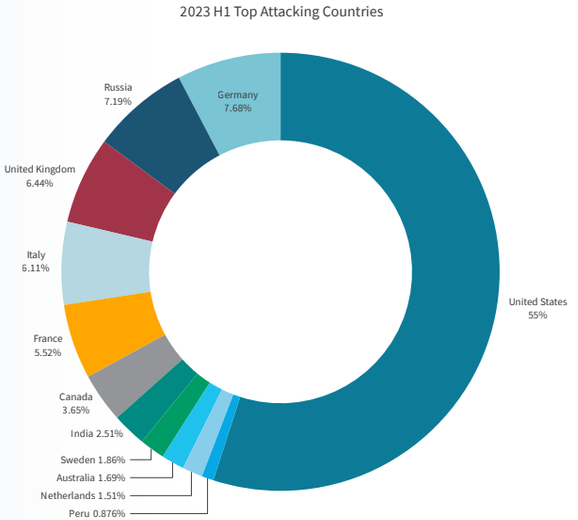
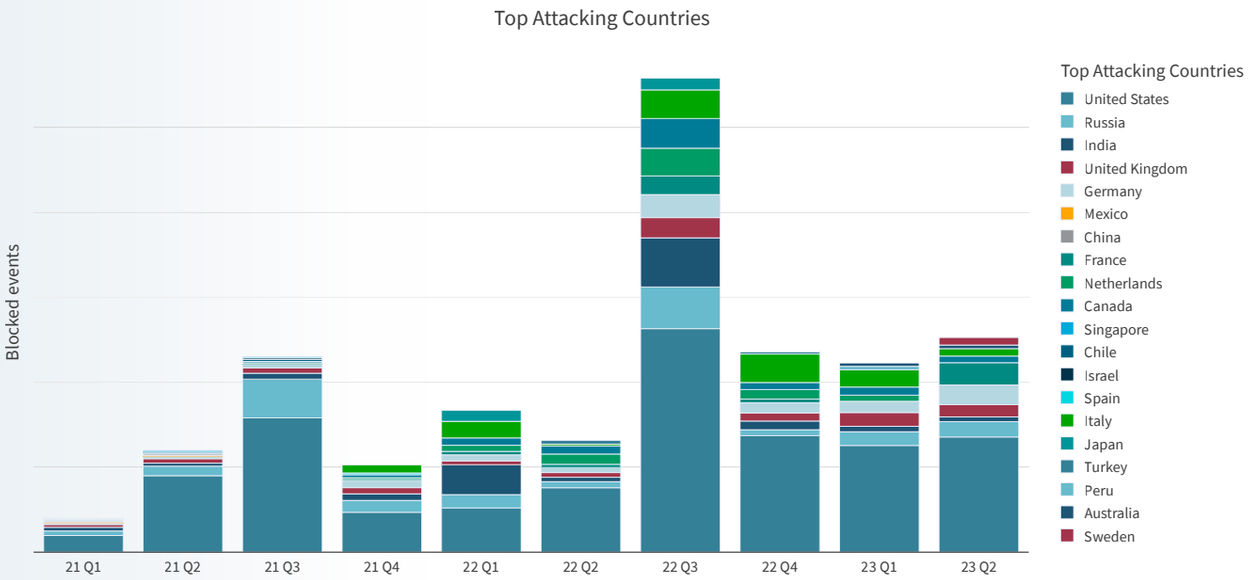


Figure 49: Top attacking countries over time

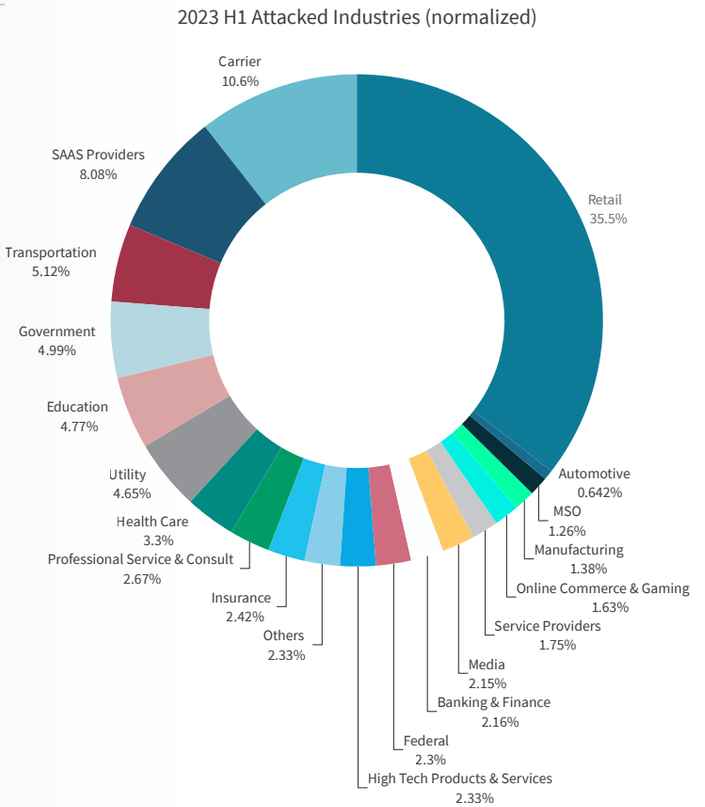


Attacked Industries

The most attacked industry in H1 2023 was retail, accounting for 35.5% of web application attacks. Carriers and SAAS providers were in second and third place, respectively representing 10.6% and 8.08% of web application attacks. Transportation was fourth (5.12%), followed by government (5%), education (4.77%), utility (4.65%) and health care (3.3%).

Figure 50

Web application attacks by industry



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[2] 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 were 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 were 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.

2. IP address spoofing is the crafting of Internet Protocol (IP) packets with false source IP addresses for the purpose of impersonating another originating computing system and geolocation.

In H1 2023, the GDN collected a total of 2.05 billion unsolicited events. This represents a significant increase compared to the total 2.65 billion unsolicited events collected in the full year 2022. The network collected an average of 11.3 million events per day. Compared to 2022, the average events per day increased by 55%.

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 H1 2023, the deception network registered an average of 60,775 unique IPs per day. This was an increase of 15% compared to 2022, which had an average of 52,860 unique IPs per day.

While the total number of events per day grew significantly (55%) in H1 2023, the number of unique IPs per day increased only slightly (15%). In conclusion, the number of malicious devices on the internet increased slightly, but their actions became much more aggressive compared to earlier years.

Figure 51: Number of events per month recorded by Radware's GDN

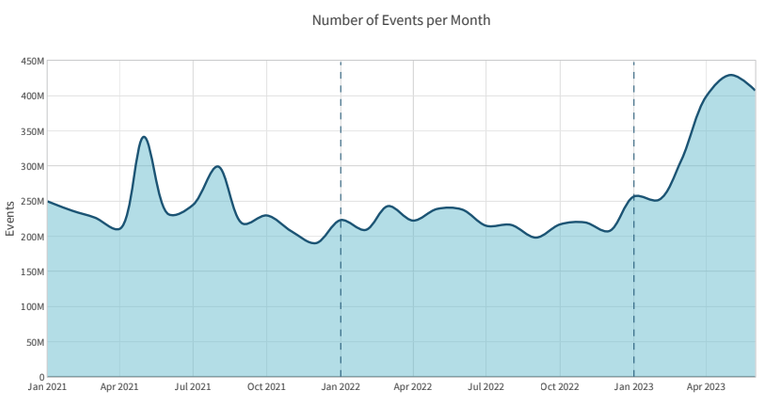
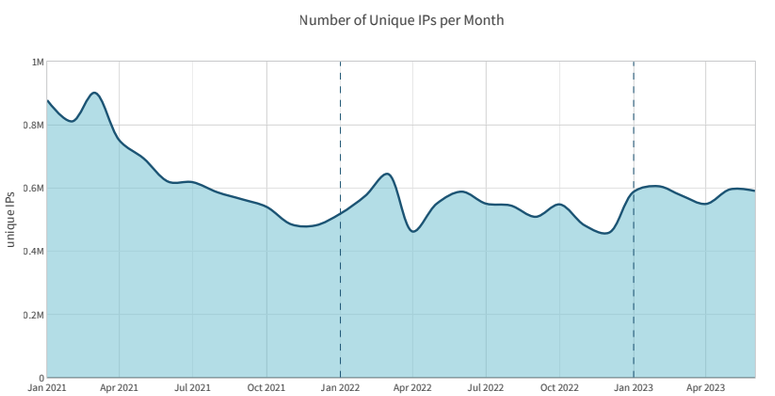


Figure 52: Number of unique IP addresses per month recorded by Radware's GDN



Most Scanned and Attacked TCP Ports

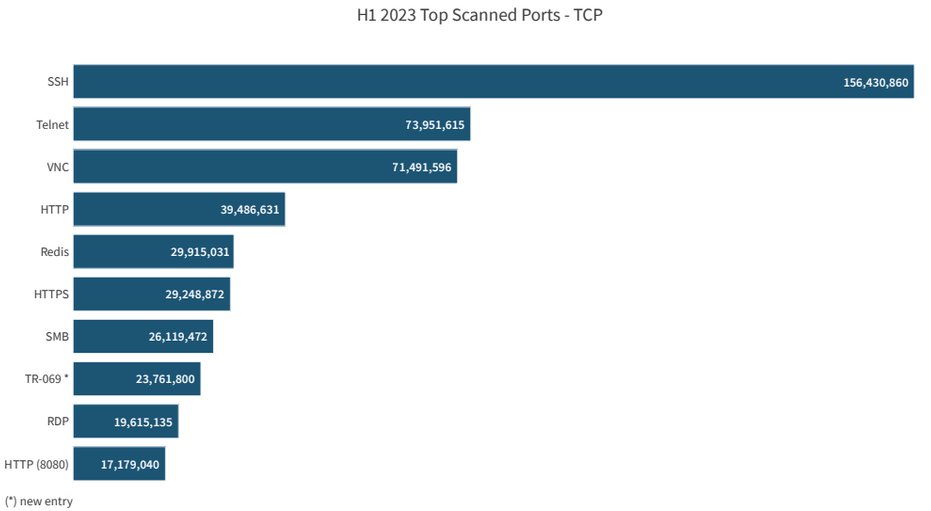
For TCP services, the most attacked service was SSH on port 22, followed by Telnet and VNC. The top 10 was completed by HTTP, Redis, HTTPS, SMB, TR-069 and RDP, followed by the popular IP camera web UI port 8080. TR-069 was a new entry in the top ten for H1 2023 compared to 2022. Leaving the top ten in H1 2023 was HTTP port 8088, another popular IP camera web UI port.

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 or leaked credentials, attackers try to gain unauthorized access to devices and systems to move laterally across organizations' networks. This is used for abuse of cloud instances for cryptomining, as a jump host to anonymize targeted attacks, to plant cryptolocking malware during ransomware campaigns, and to hijack device connectivity to perform DDoS attacks.

Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the Remote Frame Buffer (RFB) protocol 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. In 2022, VNC took the eighth spot on the top ten most scanned ports. This year VNC scans were even more prominent, moving VNC up to the third most scanned TCP port in H1 2023.

Redis (TCP port 6379) is an open source (BSD licensed) in-memory data structure store used as a database, cache and message broker. In March 2022, the Muhstik malware gang started actively targeting and exploiting a Lua sandbox escape vulnerability in Redis (CVE-2022-0543) after the release of a proof-of-concept exploit. In December 2022, a previously undocumented Golang-based malware, dubbed Redigo, targeted Redis servers to take control of systems with this vulnerability, most likely to build a botnet. The malware mimicked the Redis protocol to communicate with its command & control (C2) infrastructure. In 2022, Redis took fourth place, just behind HTTP. In H1 2023,

Figure 53: Top scanned and exploited TCP ports



both HTTP and Redis were surpassed by VNC, with each dropping down one place.

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 2022, 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 on Linux servers with ksmbd enabled. SMB remained in seventh place in the top ten for H1 2023, unchanged from 2022.

Technical Report 069 (TR-069) is a technical specification of the Broadband Forum that defines an application-layer protocol for the remote management and provisioning of customer premises equipment (CPE) connected to an IP network. TR-069 uses the CPE WAN Management Protocol (CWMP) which provides support functions for auto-configuration, software or firmware

image management, software module management, status and performance management, and diagnostics. The CPE WAN Management Protocol is a bidirectional SOAP- and HTTP-based protocol, which provides communication between a CPE and Automatic Configuration Servers (ACS). The protocol addresses the growing number of different internet access devices such as modems, routers, and gateways as well as end user devices such as set-top boxes and VoIP phones. TR-069 was one of the most targeted IoT protocols back in 2016 when Daniel Kaye, also known as "BestBuy" and "Spiderman", adapted Mirai to exploit vulnerabilities in routers exposing TR-069 on their WAN interfaces.

Remote Desktop Protocol (RDP) was eclipsed by SMB and moved down from sixth place in 2022 to ninth place in H1 2023. RDP is a proprietary protocol developed by Microsoft which provides users with a graphical interface to connect to other computers over a network connection. RDP is still a regularly exposed remote access protocol in remote locations used by industrial control systems (ICS) and became more exposed as people worked from home 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 install cryptolocking ransom malware.

SSH attacks are leveraged in account takeover and brute force attempts. **Leveraging default or leaked credentials, attackers try to gain unauthorized access to devices and systems and abuse them for cryptomining, as a jump host to anonymize targeted attacks, to plant cryptolocking malware during ransomware campaigns, and to hijack device connectivity to perform DDoS attacks**

Most Scanned and Attacked UDP Ports

Most of the scanned and exploited UDP ports during H1 2023 were the same as the top scanned UDP ports in 2022. The exception was LDAP which left the top 10 in favor of HTTP, and CoAP, which took tenth place in 2022, replaced during H1 2023 by OpenVPN in the same spot.

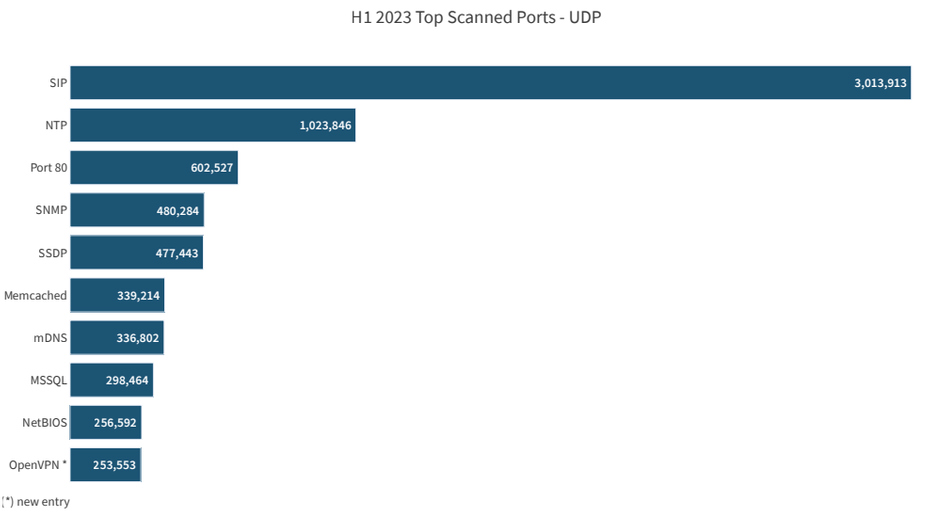
SIP (UDP port 5060) was again the most targeted UDP-based service in H1 2023. Port 5060 is used by many SIP-based VoIP phones and providers. VoIP remains critical to organizations and for this reason it also made the charts as one of the most targeted services for DDoS attacks in 2021. Vulnerabilities and weak or default passwords in VoIP services allow attackers to abuse them for initial access, spying, and moving laterally inside organizations' networks.

NTP (UDP port 123), SNMP (UDP port 161), SSDP/UPnP (UDP port 1900), Memcached (UDP port 11211) and mDNS (UDP port 5353), 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 (UDP 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, 2022 and also H1 2023.

NetBIOS (UDP 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 needed only within local networks and for 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.

Figure 54: Top scanned and exploited UDP ports



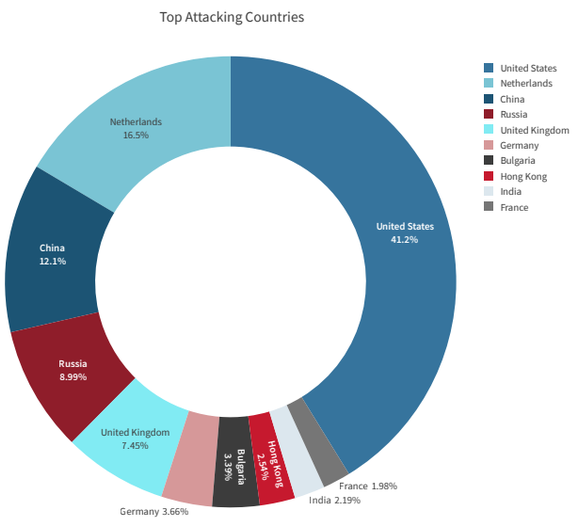
OpenVPN (UDP port 1194) is a virtual private network (VPN) system that implements techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations providing remote access for clients. It makes extensive use of the OpenSSL encryption library as well as the TLS protocol and contains many security and control features. It uses a custom security protocol that utilizes SSL/TLS for key exchange and is capable of traversing network address translators (NATs) and firewalls. OpenVPN has been ported and embedded in many router firmware platforms including DD-WRT which has an OpenVPN server function.

Attacking Countries

The United States was the country from which the most unsolicited network activity originated during H1 2023. The United States was also the number one in 2022 with 42.5% of all activity and remained so with 41.2% of all activity in H1 2023. The Netherlands moved from fourth spot in 2022 to second place in H1 2023 with 16.5%. China remained in the third spot in H1 2023 while Russia moved from second in 2022 to fourth position in H1 2023. The United Kingdom remained unchanged in fifth place. That said, as discussed earlier, the origin of an attack often does not align with the home country of the attacker and can be spoofed to impersonate a different country.

The real origin of an attack often does not align with the home country of the attacker and can be spoofed to impersonate a different country

Figure 55: Top attacking countries

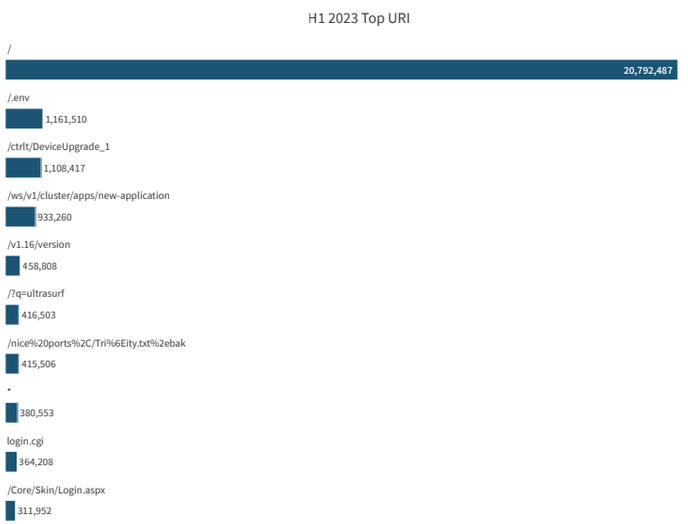


Web Service Exploits

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 targeted server and the IP address of the targeted server is not published in DNS or referred by any services on the Internet. The top URIs should 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 56

Top scanned URIs



Most important and known vulnerabilities based on top scanned URIs are listed in the following table:

/.env

A predictable resource location access exploit attempting to find configuration information of the service in the hidden file ".env". Moved from a fourth spot in 2022 to second place in H1 2023.

/ctrlt/DeviceUpgrade_1

Huawei HG532 routers Remote Code Execution vulnerability, CVE-2017-17215. Moved from tenth place in 2022 to third place in H1 2023.

/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 illegitimately leverage the cloud instances of enterprises and research institutions. This was the second most exploited URI in 2022 but moved down to third place in H1 2023.

/v1.16/version

Used by threat actors to identify the available Docker API version by invoking a command for an old version. Used by cryptocurrency miners for abusing containers through the Docker API. This was in seventh place in 2022 but moved to fifth place in H1 2023.

/q=ultrasurf

UltraSurf is a freeware internet censorship circumvention product created by UltraReach internet Corporation. The software bypasses internet censorship and firewalls using an HTTP proxy server, employing encryption to ensure privacy. The software works by creating an encrypted HTTP tunnel between the user's computer and a central pool of proxy servers, enabling users to bypass firewalls and censorship. UltraReach hosts all of its own servers. The software makes use of sophisticated proprietary anti-blocking technology to overcome filtering and censorship online. The tool was originally designed for internet users in mainland China, where the internet is heavily censored and Internet activities are monitored. With the advent of Ultrasurf and other circumvention tools, these internet users are provided a lifeline to access and share information freely. After nearly two decades of development, the technology has proven extremely resilient and adaptable in the face of increasingly advanced censorship techniques and aggressive blocking. Its success in helping internet users in China to surf the web in freedom has attracted the attention of internet users beyond China's borders. Today, Ultrareach has millions of users from over 180 countries. Radware assumes that "/q=ultrasurf" is leveraged in attempts to identify the locations and addresses of Ultrareach proxies. Ultrasfurf is a new entry in the top scanned URI list.

/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.

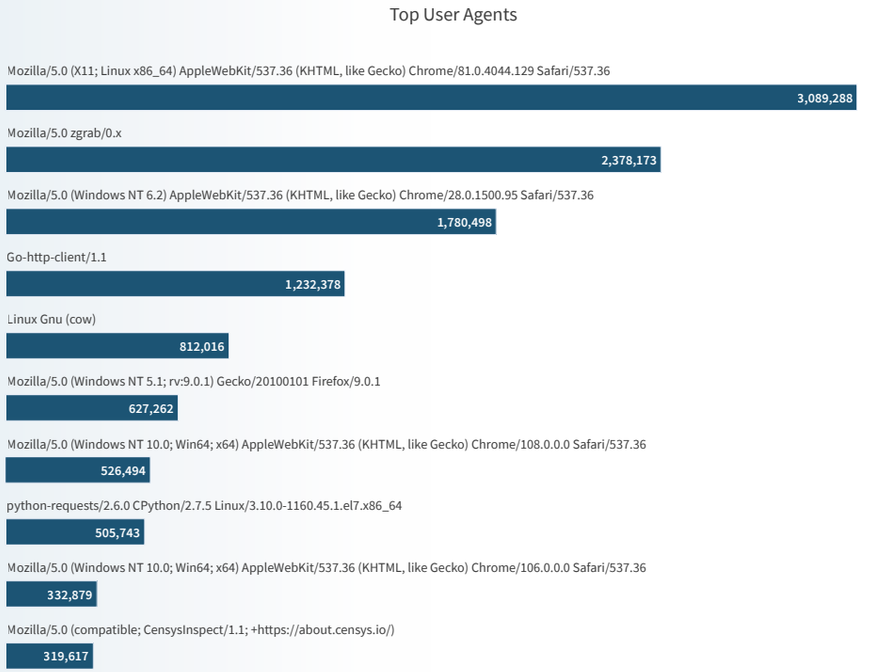
Top User Agents

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 and programming language implementations can be identified through their user agent. For example, zgrab is the application-layer network scanning component of the Zmap open source scanning tool and “Go-http-client” is the default user agent header when using the Golang net/http package.

Figure 57: Top user agents

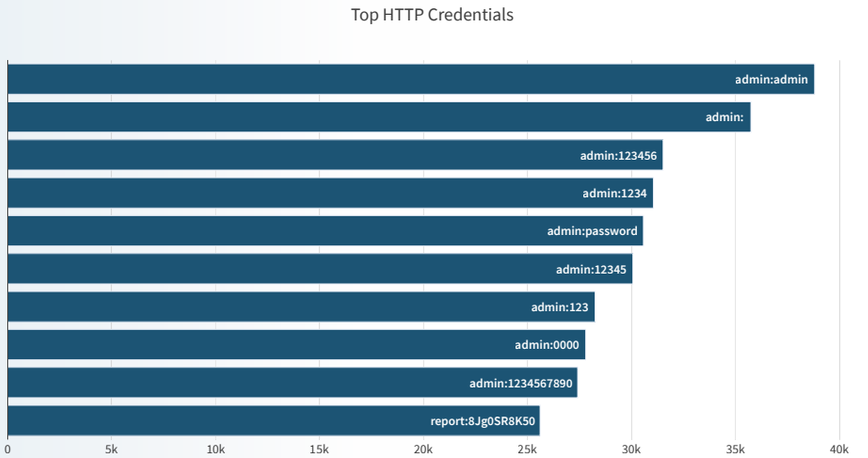


Top HTTP Credentials

Not all web service vulnerabilities can be exploited without authentication. Some web services embed 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 have not had 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.

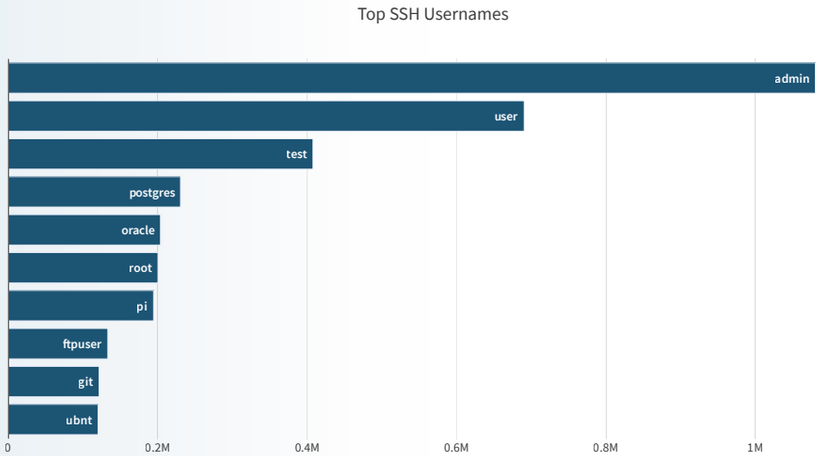
Figure 58: Top HTTP credentials



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”, “root”, “pi” (Raspberry Pi default username) and “ubnt” (Ubuntu default username). The others are the most leveraged usernames by administrators or default accounts, for example, “admin”, “user”, and “test”. Appendix A

Figure 59: Top SSH usernames



Appendices

Appendix A: Common DNS Record Types

A	The address mapping record, also known as a DNS host record, stores a hostname and its corresponding IPv4 address.
AAAA	The IP Version 6 address record stores a hostname and its corresponding IPv6 address.
CNAME	The canonical name record is used to alias a hostname to another hostname. When a DNS client requests a record that contains a CNAME, which points to another hostname, the DNS resolution process is repeated with the new hostname.
MX	The mail exchanger record specifies an SMTP email server for the domain.
NS	The name server record specifies that a DNS Zone, such as "example.com," is delegated to a specific authoritative name server and provides the address of that name server.
PTR	The reverse-lookup pointer record provides the IP address of a hostname (reverse DNS lookup).
SRV	The service location record is like the MX record but for other services.
TXT	The text record can contain arbitrary information and typically carries machine-readable data such as opportunistic encryption, sender policy framework (SPF), DKIM, DMARC, etc.
SOA	The Start of Authority record appears at the beginning of a DNS zone file and indicates the authoritative name server for the current DNS zone, contact details of the domain administrator, domain file version number, and information on how frequently DNS information for this zone should be refreshed.
NAPTR	The Naming Authority Pointer records map domain names to URIs (uniform resource identifiers) and other resources. NAPTR records are commonly used for applications in internet telephony.

Appendix B: Radware Network Intrusion Signatures

Radware ID	Classification	CVE
DNS-named-version-attempt	Information disclosure	—
Attempt to query version on named – The Bind named DNS service is vulnerable to an information disclosure attack allowing an attacker to determine if the server supports information query requests. The information disclosed contains server version information.		
HTTP-APACHE-LOG4j2-BODY1-RCE	RCE	CVE-2021-44228
Log4j remote code execution vulnerability, also known as Log4Shell – A JNDI Injection vulnerability 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 a server controlled by the attacker which may lead to the execution of arbitrary code in the security context of the affected server.		
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.		
HTTP-APACHE-LOG4j2-USERA-RCE	DoS	CVE 2021-45105
Apache Log4j DoS – An uncontrolled recursion vulnerability has been reported in the StrSubstitutor class of Apache Log4j. This vulnerability is due to improper handling of logged messages when the logging configuration uses a non-default Pattern Layout with a Context Map Lookup, Map Lookup, or Structured Data Lookup. A remote attacker who can control an item in the Thread Context Map or a MapMessage or StructuredDataMessage can exploit this vulnerability by sending a specially crafted parameter to the target application. Successful exploitation could result in a denial-of-service condition due to a crash of the Log4j service.		
ZMAP-TCPScan	Scanning	--
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-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.		
ZMAP Scan	Scanning	--
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.		

Radware ID	Classification	CVE
HTTP-APACHE-LOG4j2-URL3-RCE	RCE	CVE-2021-44228

Apache Log4j JndiManager JNDI Injection - A JNDI Injection vulnerability has been reported in the JndiManager class of Apache Log4j. This vulnerability is due to improper handling of logged error messages. 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 under the security context of the affected server.

DNS-Web Proxy Auto Discovery-Query	Information Disclosure	--

DNS Web Proxy Auto Discovery Query - A DNS information disclosure attempt. The Web Proxy Auto-Discovery (WPAD) Protocol is a method used by clients to locate the URL of a configuration file using DHCP or DNS discovery methods. Once detection and download of the configuration file is complete, it can be executed to determine the proxy for a specified URL.

HTTP-APACHE-LOG4j2-URL1-RCE	RCE	CVE-2021-44228

Apache Log4j JndiManager JNDI Injection - A JNDI Injection vulnerability has been reported in the JndiManager class of Apache Log4j. This vulnerability is due to improper handling of logged error messages. 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 under the security context of the affected server.

HTTP-APACHE-LOG4j2-URL5-RCE	RCE	CVE-2021-44228

Apache Log4j JndiManager JNDI Injection - A JNDI Injection vulnerability has been reported in the JndiManager class of Apache Log4j. This vulnerability is due to improper handling of logged error messages. 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 under the security context of the affected server.

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. Note that attack events and blocked events are considered the same for the purpose of this report. All blocked volume is considered attack volume. 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, which corresponds to 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 (page 43).

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.

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
Daniel Smith | Head of Threat Research

Executive Sponsors

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

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.

RW-396 | 22 Aug 2023