radware | PRESIDIO®

2021 – 2022 Global Threat Analysis Report Executive Summary

Radware's 2021 threat report reviews the year's most important cyber security events and provides detailed insights into the attack activity of 2021. The report leverages intelligence provided by Radware's Threat Intelligence Team and network and application attack activity sourced from Radware's Cloud and Managed Services, Radware's Global Deception Network and Radware's Threat Research team.

DDOS ATTACKS

The Radware Cloud DDoS Service mitigated an average of 1,591 attacks per day. The total number of attacks mitigated in 2021 was 580,766. Most distributed denial-of-service (DDoS) activity was concentrated throughout the middle of the year. In the first two weeks of June 2021, the average number of attacks per day was significantly higher and reached a maximum of 9,824 attacks on July 10, 2021. The first half of 2021 had an increasing trend, while the second half had a decreasing trend. The number of attacks mitigated in the first half was almost equal to the number of attacks mitigated in the second half.

The number of blocked malicious events per customer grew 37% from 2020 to 2021. The average attack volume per customer grew 26%. On average, each customer blocked 6.49TB of volume. A DDoS attack in 2021 represented an average volume of 5.69 GB. The largest attack was recorded in Q4 and had a size of 520Gbps.

While less common, several terabit-level attacks were reported in 2021 by large-scale cloud providers. Microsoft Azure reported the largest DDoS attack ever recorded in Q4, with a size of 3.47Tbps. In the same quarter, Microsoft experienced two more attacks above 2.5Tbps.

As businesses migrate critical resources and applications to the public cloud, attackers will have to adapt their tactics and techniques to match the scale of public cloud providers. Enterprises should not immediately be alarmed by these reports of huge attacks. However, they do need to be aware that DDoS attacks are a part of their threat landscape, irrespective of their geography or industry. As such, DDoS mitigation should be part of the protective measures companies implement whenever using or exposing services and applications to the internet.

As bandwidths and resources increase for legitimate businesses, they also increase for threat actors. It is only fair to assume that bad actors can scale as fast and high as their targets. Services hosted in the public cloud will need to consider cloud-scale attacks.

Multiterabit attacks are not necessarily more effective or dangerous than several 100Gbps attacks. In the first few weeks of 2022, during the Twitch Rivals SquidCraft Games event hosted in Andorra, a DDoS attack no larger than 100Gbps interrupted the connectivity of the entire country for hours on end. The attack was performed by an individual or group targeting the event by leveraging a paid subscription to a DDoS-for-hire service.

More concerning is the trend of micro floods and application-level attacks. We noted a slight decline (5%) in the number of large attacks, above 10Gbps, between 2020 and 2021 (see the section “Large Attack Vectors” in “Attack Vectors and Applications”), while attacks smaller than 1Gbps increased by almost 80% (see the section “Micro Floods” in “Attack Vectors and Applications”). Micro floods and slower attacks, such as application-layer attacks, can go undetected and consume resources. Organizations are at risk of having to constantly increase infrastructure resources, such as bandwidth, network and server processing, until the service becomes cost prohibitive. Application-layer attacks typically require more resources to detect them than their network-layer flood counterparts do.

GEOGRAPHIES AND INDUSTRIES

Europe, the Middle East, and Africa (EMEA) and the Americas both blocked 40% of the attack volume in 2021, while the Asia Pacific region blocked 20%. The top attacked industries in 2021 were gaming, retail, government, healthcare, technology and finance. Customers in online commerce and gaming, retail and technology witnessed the largest increase in DoS events and attack volume. Customers in government, healthcare and research and education saw the biggest increase in attack volume. The volume per DoS event for research and education, government and retail saw a severalfold increase between 2020 and 2021. This increase could be indicative of a change in tactics: attacks that were previously random are now being used as part of more targeted and organized campaigns.

ATTACK VECTORS

Radware recorded a slight decline (5%) in the number of attack vectors larger than 10Gbps, but an increase in mid-sized attack vectors of 39% and a steep increase of 79% in the number of micro floods in 2021 compared to 2020.

On average, customers were targeted by 10.8 attack vectors above 1Gbps for every 1,000 attack vectors in Q1 of 2021. This number dropped to 4.93 in Q4 of 2021. Customers found 3.31 attack vectors above 10Gbps per 1,000 attack vectors in Q2 of 2021. Out of every 3,000 attack vectors targeting a customer, fewer than one was above 100Gbps.

In 2021, the most-often-leveraged amplification protocols were NTP, DNS and SSDP. NTP is also the second top-scanned UDP port in Radware's Global Deception Network. Memcached, LDAP, SSDP, SNMP and mDNS, all popular DDoS reflection and amplification protocols, are in the top 10 most-scanned UDP ports recorded by the deception network.

The diversity in leveraged attack vectors decreases as the size of the attack vector increases. The average packet size increases with the size of the attack vector. The average attack vector duration also increases as attack vectors become larger and range from a few minutes for micro floods to one hour for attack vectors over 100Gbps. Consequently, the larger attack vectors are also responsible for the largest mitigated volumes in 2021.

Ninety-six percent of the attack vectors recorded in 2021 were smaller than 10Mbps, while the volume generated by those attack vectors represented only 0.3% of the total attack volume in 2021. Sixty percent of the attack volume in 2021 was generated by attack vectors with sizes between 10Gbps and 100Gbps. Attack vectors above 100Mbps represented only 0.8% of all attack vectors recorded in 2021.

TCP attack vectors with throughputs below 10Mbps generated the largest volumes on average and had the longest durations, while UDP attacks were responsible for the highest throughputs and longest durations with attack vectors above 10Mbps. TCP attack vectors were responsible for the highest packet rates and were surpassed in packet rate only by UDP attack vectors for attack vectors larger than 100Gbps.

The average complexity of attacks increased with the size of the attack. The largest number of attack vectors in a single attack was 21 and was an attack between 10Gbps and 100Gbps. Attacks between 10Gbps and 100Gbps had an average duration of 8.72 hours. Attacks below 1Gbps lasted less than an hour, on average.

INTRUSION ATTACKS

Network intrusion attacks consist of easy-to-execute exploits based on known vulnerabilities and range from scanning using open source or commercial tools, information disclosure attempts for reconnaissance, up to path traversal and buffer overflow exploitation attempts that could render a system inoperable or could provide access to sensitive information.

DoS events accounted for one-third of all blocked events in 2021, while intrusions represented two-thirds.

Most of the intrusion activity in 2021 consisted of SIP scanning. The second-most-blocked exploits in 2021 were attempts to exploit a file buffer overflow in Microsoft Internet Explorer through a malformed BMP, a vulnerability that was published in 2004. The third-most-blocked intrusions were Brute Force attempts over SSH.

Log4Shell, arguably the most critical vulnerability of 2021, took the security community by storm in December. Our cloud services detected and blocked more than 800,000 Log4Shell exploits in December and recorded peaks of over 90,000 exploits per day.

WEB APPLICATION ATTACKS

The number of blocked malicious web application requests grew 88% from 2020 to 2021.

Predictable resource location attacks accounted for almost half of all attacks. In terms of the 2017 OWASP Top 10 application security risks,[1] broken access control and injection attacks represented three-quarters of all attacks recorded in 2021.

Most attacks originated in the United States and Russia, followed by India, the United Kingdom and Germany. The country in which an attack originates typically does not correspond to the nationality of the threat actor or group. The originating country of the attack will be chosen by the threat actor based on the location of the victim or the country the threat actor wants to see attributed during false flag operations.

The 2021 attack activity was dispersed across an array of industries, with no one vertical standing out. The most attacked industries were banking and finance and SaaS providers, followed by retail and high-tech industries. Manufacturing, government, carrier, transportation, online commerce and gaming, and research and education all had notable levels of activity.

UNSOLICITED NETWORK SCANNING AND ATTACK ACTIVITY

The Radware Global Deception Network registered a total of 2.9 billion unsolicited network events and peaked at almost 10 million events in a single day.

A total of 5.7 million unique IPs were recorded in 2021. This represents 0.15% of the available public IPv4 addresses on the internet. The number of unique IPs provides a good measure for the number of malicious hosts and devices involved in scanning and malicious activity on the internet.

SSH was the target of half of all unsolicited TCP activity, followed by IP cams, RDP, VNC and SMB, and only then followed by the most pervasive web application protocols HTTP and HTTPS. Just 2% of the total activity, but still a notable 24 million events, was targeting Redis, an open source, in-memory data structure store used as a database, cache, and message broker for which a remote code execution vulnerability (CVE-2021-32761) was disclosed in July 2021. This allowed an attacker to execute arbitrary code on the target system.

The SIP protocol, used by many VoIP phones and providers, was the most targeted UDP-based service in 2021. VoIP remains critical to organizations to ensure their productivity, and it also made the list of most-targeted services for DDoS attacks in 2021. Vulnerabilities and weak or default passwords in VoIP services allow these to be abused for initial access, spying and moving laterally inside organizations' networks.

NTP, Memcached, LDAP, SSDP/UPnP, SNMP and mDNS were among the most-leveraged protocols for DDoS amplification attacks and comprised over 60% of all unsolicited network activity. These services are continuously scanned and meticulously cataloged by black hat threat actors to abuse for DDoS attacks, and white hat actors assess the risk in the DDoS threat landscape.

The United States was the top attacking country in 2021, generating more than a third of all unsolicited network activity, closely followed by Russia and China, which both were good for about one-fifth of the total activity.

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

Apache Hadoop YARN was the most eagerly scanned and exploited online service, followed by platforms, routers and Docker APIs powered by Java Enterprise Edition.

Eight out of the top 10 abused credentials leveraged for account takeover (ATO) attempts in online services consisted of the typical weak passwords “admin”, “pass”, “password”, “123456”, “1234”, “1111”, “1234” and empty password, all combined with usernames “admin” or “root”. Almost one-tenth of all the credentials used during online service attacks consisted of “root:icatch99”, a hardcoded credential in digital video recorders (DVRs) from vendor LILIN that was publicly disclosed in March 2020 [1]. DVRs are still ubiquitous in the IoT threat landscape, as are the security cameras that feed them.

The credentials “8hYTSUFk:8hYTSUFk” represented 11% of all abused credentials during online service attacks. The exact origins of the credentials are still a bit of a mystery. They were used in an example for passing authentication arguments to a generic web API interaction and exploration module written in Node called Yiff Rewrite [2], an extended wrapper based on the furry API wrapper. The string was also discovered in several malware binaries.

The top usernames leveraged during SSH Brute Force ATO attempts were unsurprisingly “admin”, “user” and “test”. Among the top 10 are also “postgres”, “oracle” and “git”, exposing the most sought for and most likely targeted services for ATO.