Tencent Cloud EdgeOne Platform

Tencent Cloud 2024 DDoS and Application Security Threat Trend Report

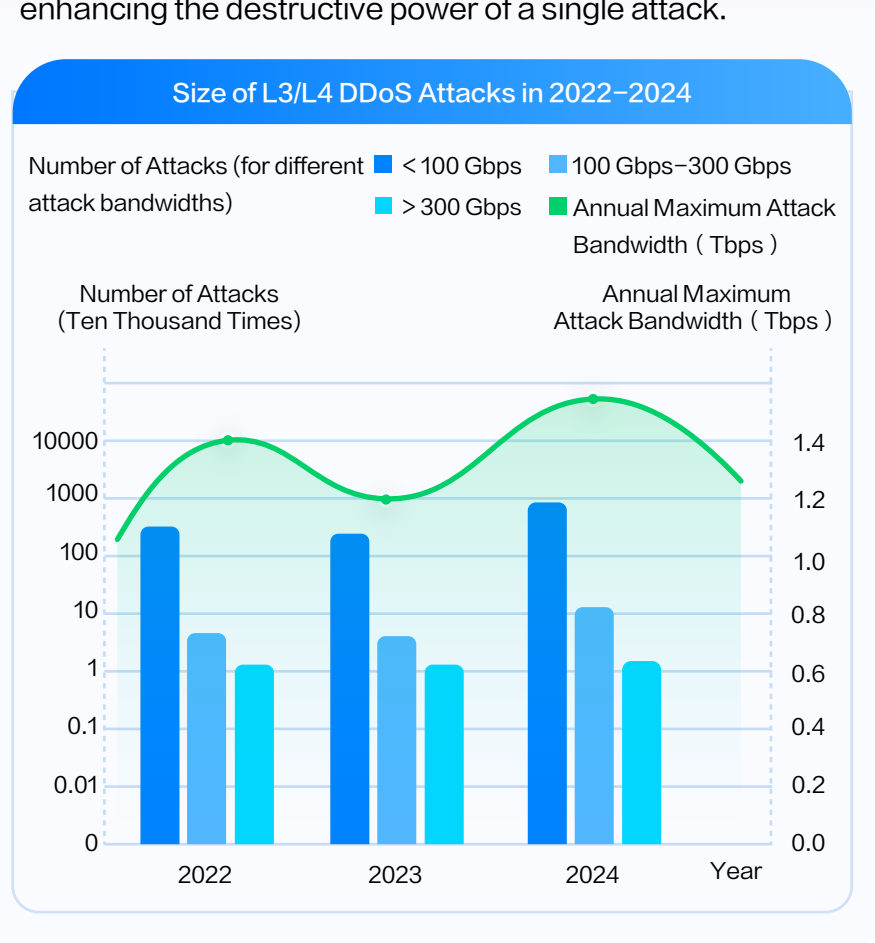
In 2024, the threats facing the cybersecurity field continue to evolve, and the means of attack have become more diverse and complex. Based on a large amount of data from Tencent Cloud's entire network, we have comprehensively analyzed the trends of cyber attacks over the past year. In this article, we will elaborate on the major cyberattack trends, sources of attacks, and the security situation in various industries in 2024, and put forward corresponding protection recommendations based on Tencent Cloud EdgeOne's protection practices to help customers effectively identify potential risks and respond to these threats.

PART1 Network Layer (L3/L4) DDoS Attacks

Attack Trends: Normalization of Small-Scale Attacks, Significant Increase in the Size of Very Large Attacks

DDoS attacks continue to show strong growth in 2024. The number of volumetric DDoS attacks increased by 144% year-on-year, with the number of small-scale attacks less than 100 Gbps surging by 146% year-on-year. Attackers are more inclined to consume defense resources through low-intensity sustained attacks, a strategy that puts tremendous pressure on enterprises with weaker protection capabilities. Meanwhile, the number of mega-attacks larger than 300 Gbps increased by 73% year-on-year, and the peak traffic volume exceeded 1.5 Tbps during the year, indicating that attackers continued to invest more in enhancing the destructive power of a single attack.

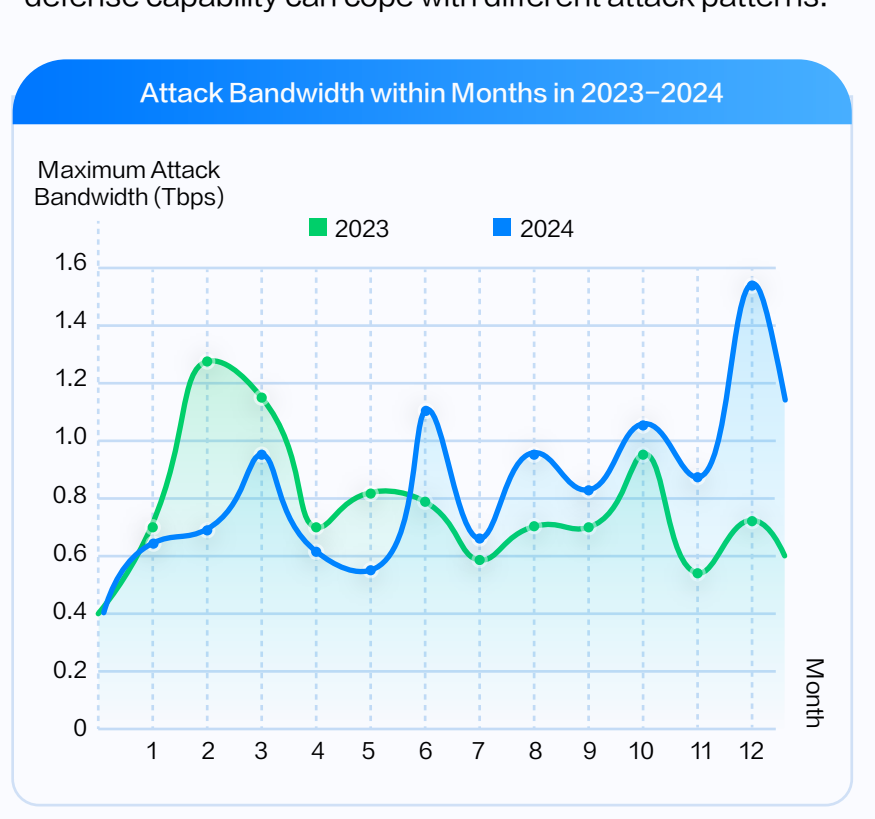
Size of L3/L4 DDoS Attacks in 2022-2024



High Attack Period: Holidays Become the Period of Concentration of Attacks

Monthly peak attack data shows that the scale of attack bandwidth in December 2024 hit a record high, with a 115% year-on-year increase. In addition, the maximum attack bandwidth in June, August, and October also exceeded 1 Tbps, focusing on key business cycles such as e-commerce promotions, summer traffic peaks, and year-end settlement periods. This trend shows that attackers are increasingly focusing on utilizing holidays and peak business periods to launch attacks. Therefore, enterprises need to pay more attention to the protection of DDoS attacks during these periods to ensure that the defense capability can cope with different attack patterns.

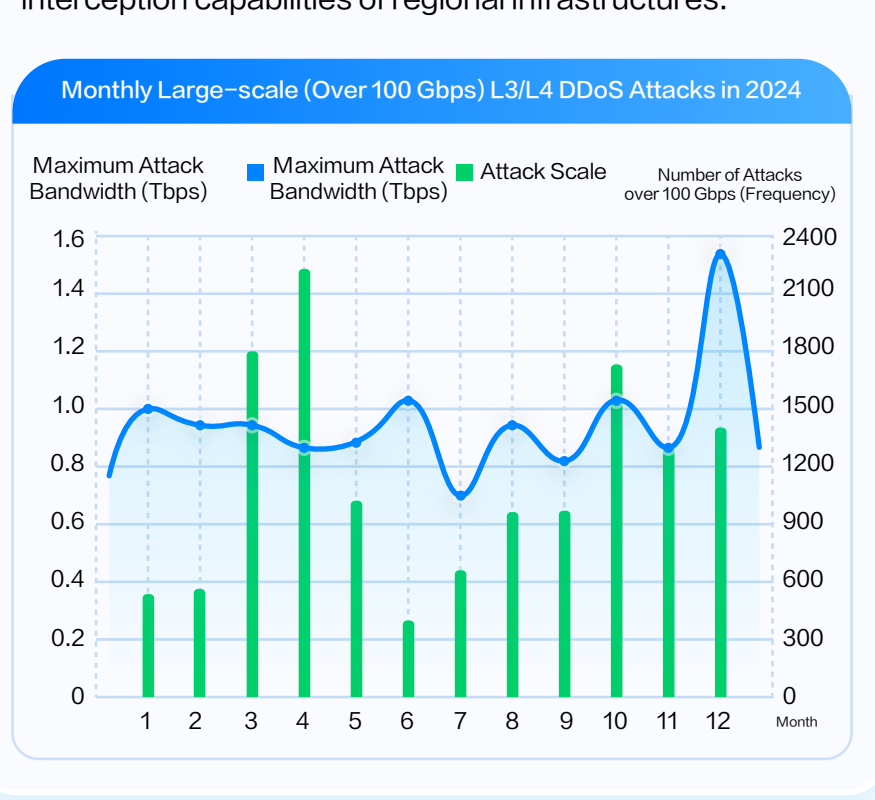
Attack Bandwidth within Months in 2023-2024



Attacks show pulse-type intensive outbreaks, and the risk of cross-regional coordinated attacks increases

In September and December 2024, global attack traffic showed a "short burst" pattern worldwide, with a significant increase in attack density compared to the rest of the year. Localized businesses, especially those in Europe, the United States and Southeast Asia, have become the main targets of attacks, and global multi-region coordinated attacks have become a significant trend. Globalization and transnational business should strengthen the localized interception capabilities of regional infrastructures.

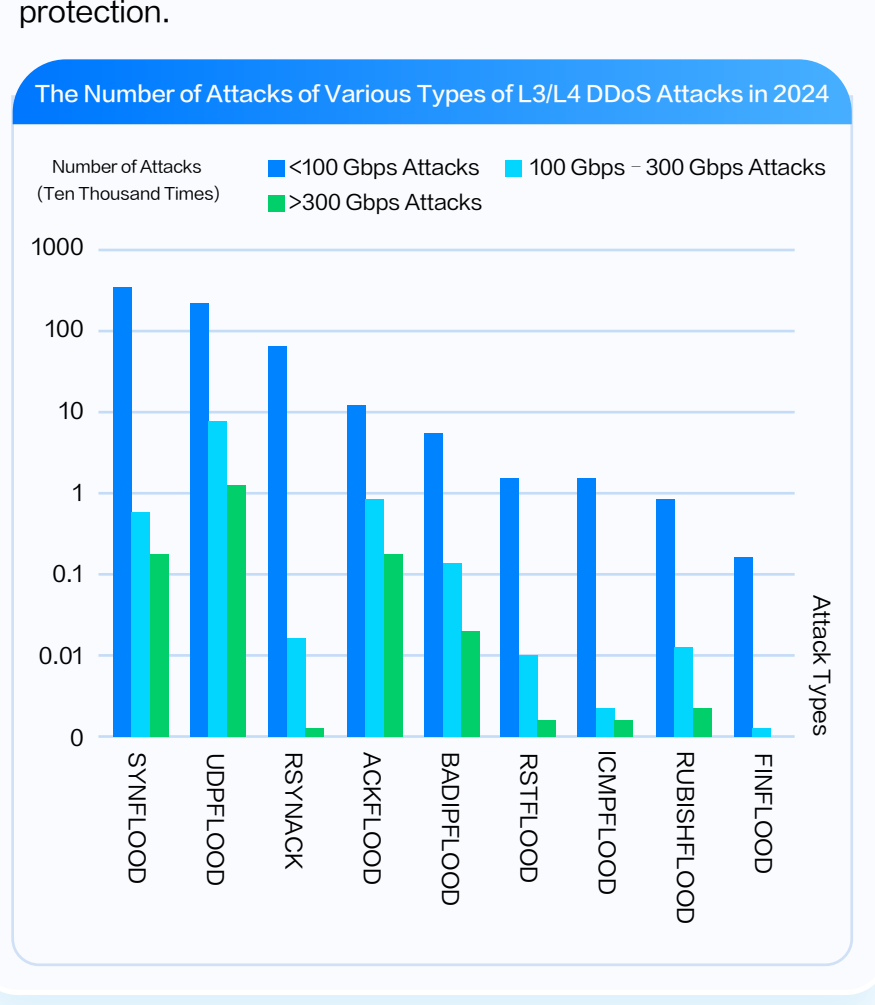
Monthly Large-scale (Over 100 Gbps) L3/L4 DDoS Attacks in 2024



Attack Strategy: Deep Exploitation of Protocol Vulnerabilities

In terms of the distribution of attack types, SYN Flood attacks still dominate low-cost attacks, especially in the scale of less than 100 Gbps with 58%. On the other hand, UDP Flood dominated the medium-sized attacks, accounting for 91% of the 100-300 Gbps attacks and 69% of the attacks larger than 300 Gbps. Exploitation of traditional protocol vulnerabilities is still the main form of attacks, and protection against reflection attacks is still the core requirement for Internet services to deal with DDoS protection.

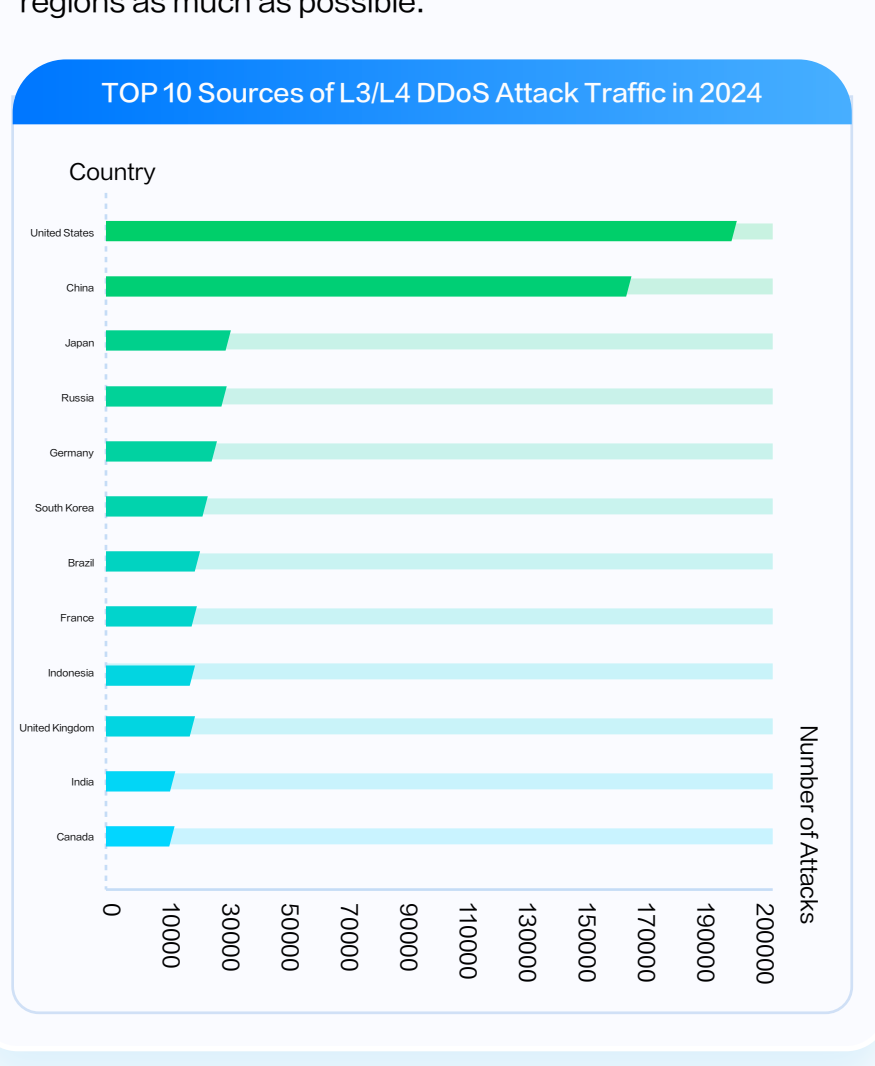
The Number of Attacks of Various Types of L3/L4 DDoS Attacks in 2024



Geographic Analysis of Attack Sources

In 2024, attack traffic primarily originates from regions such as the U.S. and China, where exposed infrastructure (e.g., un-hardened reflection sources) is often exploited by attackers as a staging ground for reflection attacks. Although the attack traffic in these regions is larger, it does not mean that the attacks come directly from these regions. Enterprises should strengthen infrastructure protection, especially to prevent common reflection protocols (e.g., DNS, NTP, etc.) from being abused, take measures to close unnecessary ports, harden service authentication, and deploy necessary traffic filtering policies to reduce the risk of Internet services becoming the source of reflection attacks. Meanwhile, for globally deployed application services, it is recommended to adopt a distributed access architecture and protection mechanism, and localize traffic processing to isolate the risk of attacks between different regions as much as possible.

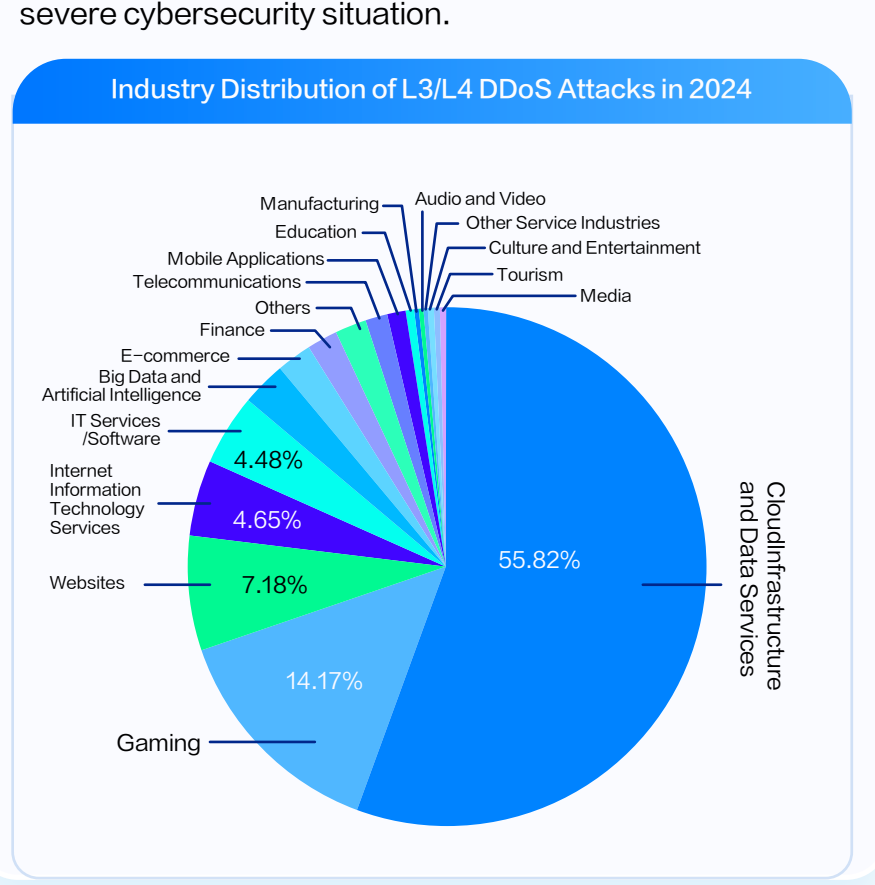
TOP 10 Sources of L3/L4 DDoS Attack Traffic in 2024



Cloud Infrastructure and Data Services Industry Takes the Biggest Hit

The cloud infrastructure and data services industry has become a major target for attacks. According to the latest data, the cloud infrastructure and data services sector has been attacked more than 60,000 times across all industries, far more than any other industry. As organizations increasingly migrate their business to the cloud, the security of cloud infrastructure and data services is particularly important. Attackers are aiming not only to access sensitive data, but also to affect the operations and reputation of organizations through attacks on cloud infrastructure and data services. Therefore, cloud service providers and users must strengthen security measures and improve their ability to recognize and respond to potential threats in order to cope with the increasingly severe cybersecurity situation.

Industry Distribution of L3/L4 DDoS Attacks in 2024

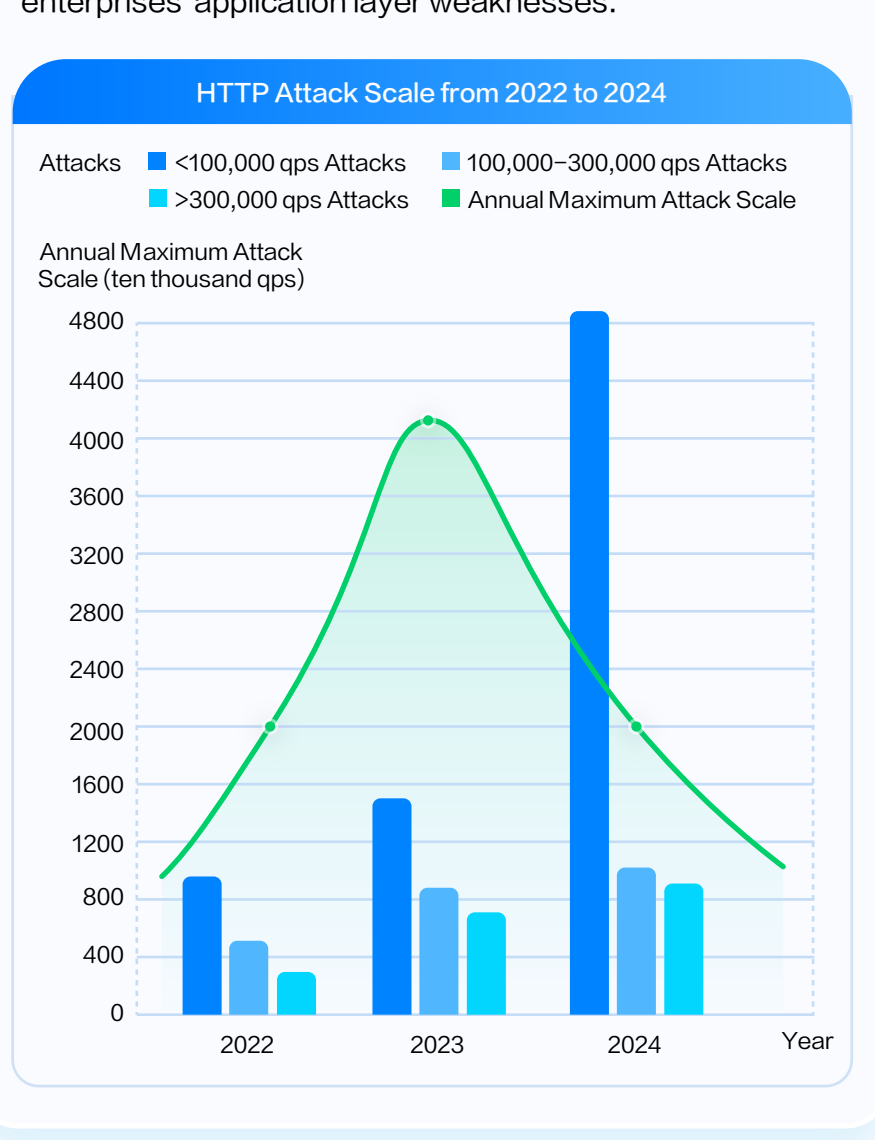


PART2 HTTP/S Attacks

HTTP/S DDoS Attacks Explode in Volume, Mega Attacks Remain at High Frequency

In 2024, HTTP/S DDoS attacks are showing more sophisticated attack patterns. The number of small-scale HTTP/S attacks of less than 100,000 QPS increased by 491% year-on-year; the number of mega-attacks of more than 300,000 QPS increased by 187%, and the annual peak value exceeded 2 million QPS. Attackers are focusing on hitting the application layer weaknesses of the enterprises through the tactic of "massive low-intensity probing + intermittent high-pressure breakthrough". Attackers are using the strategy of "massive low-intensity probes + intermittent high-pressure breaches" to focus on hitting enterprises' application layer weaknesses.

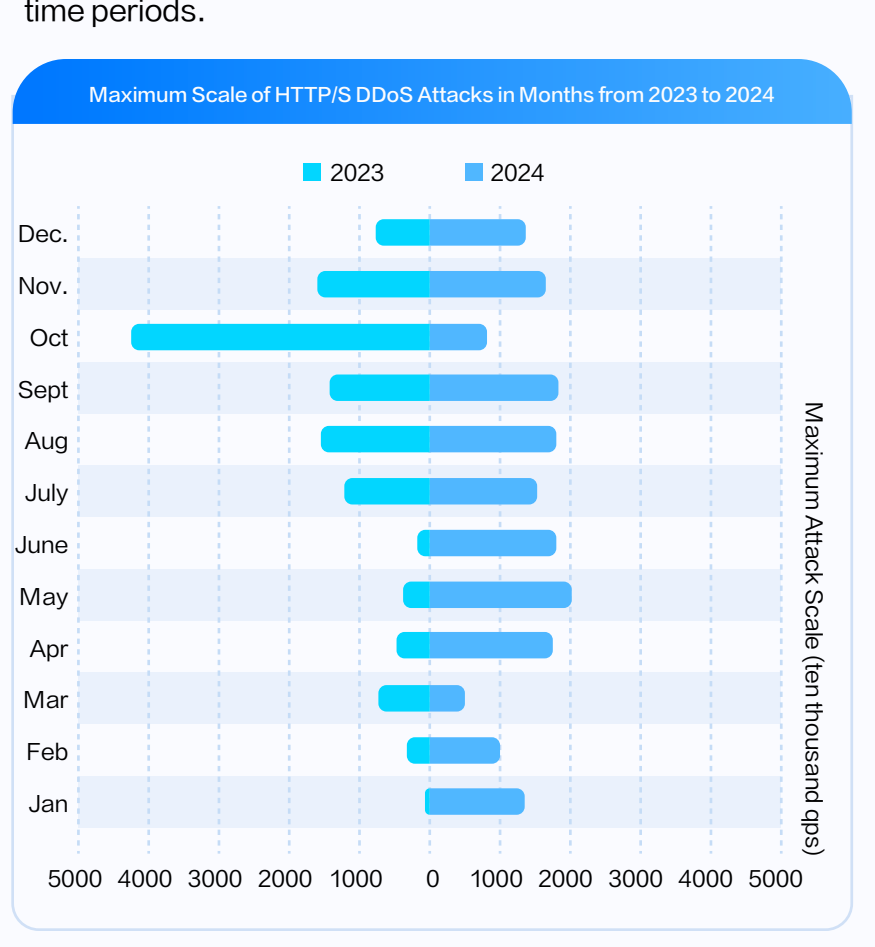
HTTP Attack Scale from 2022 to 2024



High Attack Periods: Peak Business Hours Continue to Be the Hardest Hits

In 2024, May, September and December became the main peak periods for HTTP/S attacks, especially during the e-commerce promotion, summer traffic peak and year-end settlement period, where attackers take up a large amount of server resources through high-frequency requests, resulting in huge pressure on application systems. E-commerce, finance and other industries need to pay special attention to the protection strategy for these time periods.

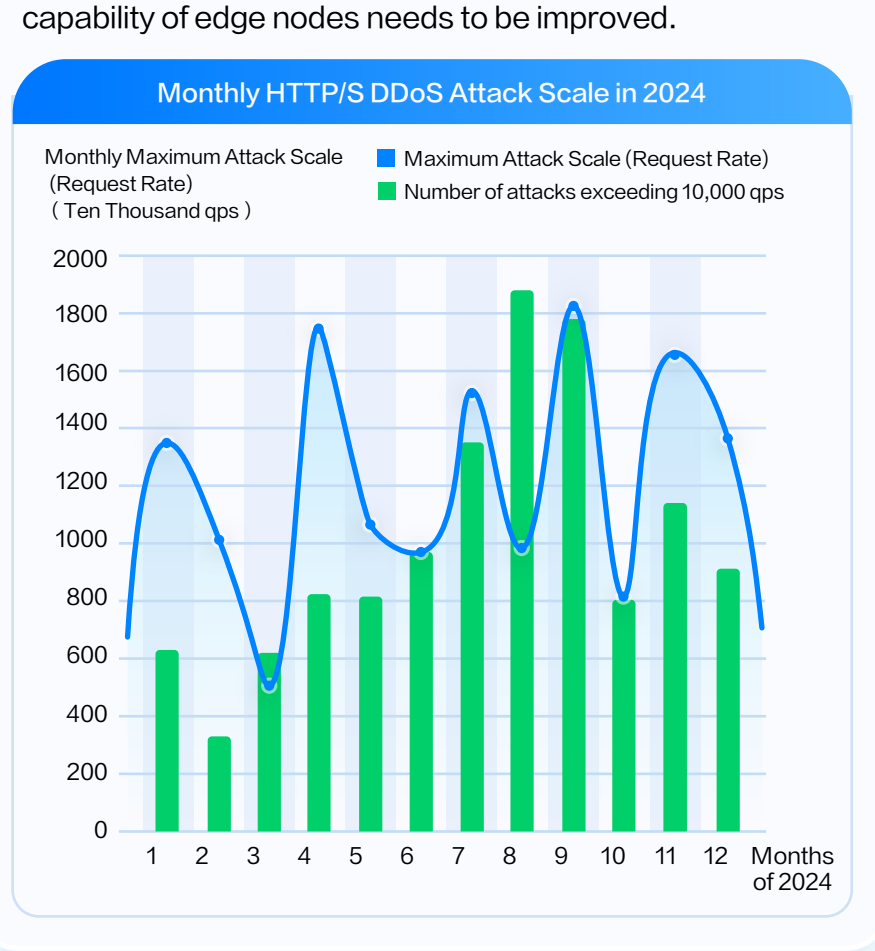
Maximum Scale of HTTP/S DDoS Attacks in Months from 2023 to 2024



Global Attacks Surge, Increased Demand for Cross-Domain Collaborative Protection

Global HTTP/S attacks saw a 254% increase in September, with more than 60% of attacks in Europe and the United States. This pattern of "cross-domain attacks" indicates that globalized businesses are facing more severe security challenges, and the protection capability of edge nodes needs to be improved.

Monthly HTTP/S DDoS Attack Scale in 2024

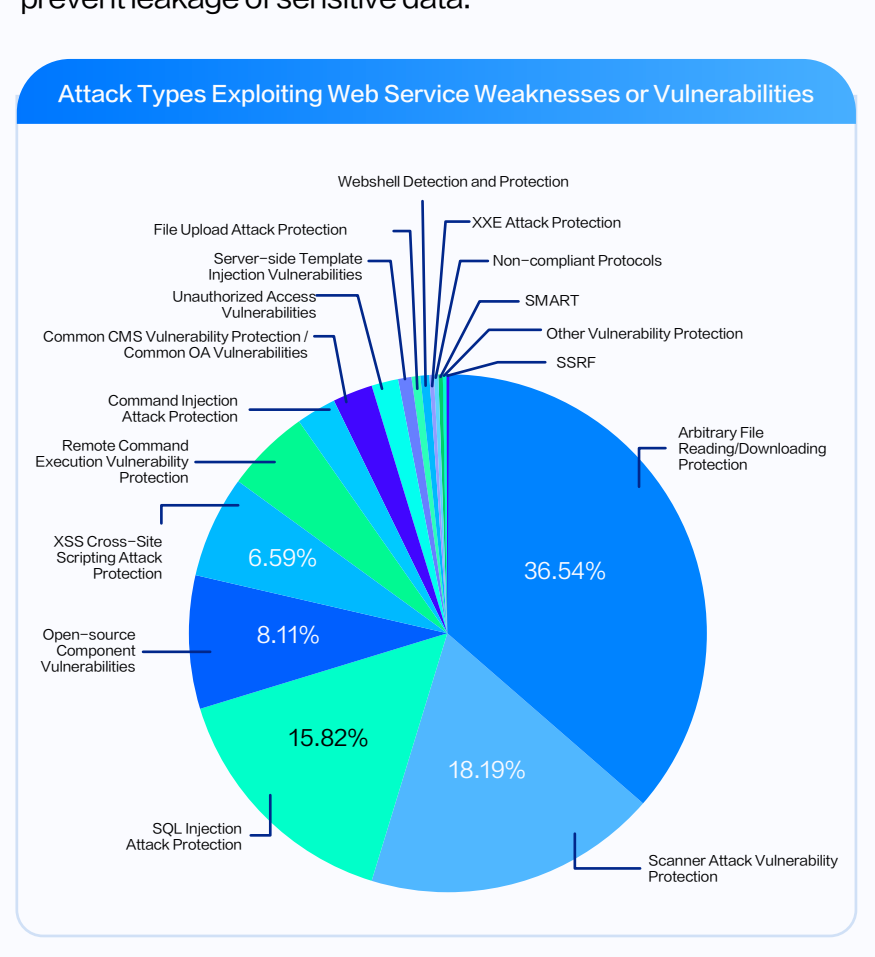


PART3 Attacks that Exploit Vulnerabilities and Application Weaknesses

Arbitrary File Read Vulnerabilities and Vulnerability Scanners Remain the Biggest Threats

In 2024, vulnerability exploitation attacks will continue to show a high incidence trend, with the total number of high-risk vulnerability attacks exceeding 1.7 billion, of which 36.5% are arbitrary file reading/downloading vulnerabilities, far exceeding the traditional types of attacks such as SQL injection and scanner attacks. Attackers are more and more inclined to scan for vulnerabilities and try to infiltrate through the attack vectors of "low technical threshold" such as configuration errors and privilege loopholes. Enterprises need to strengthen privilege control and directory access control to prevent leakage of sensitive data.

Attack Types Exploiting Web Service Weaknesses or Vulnerabilities



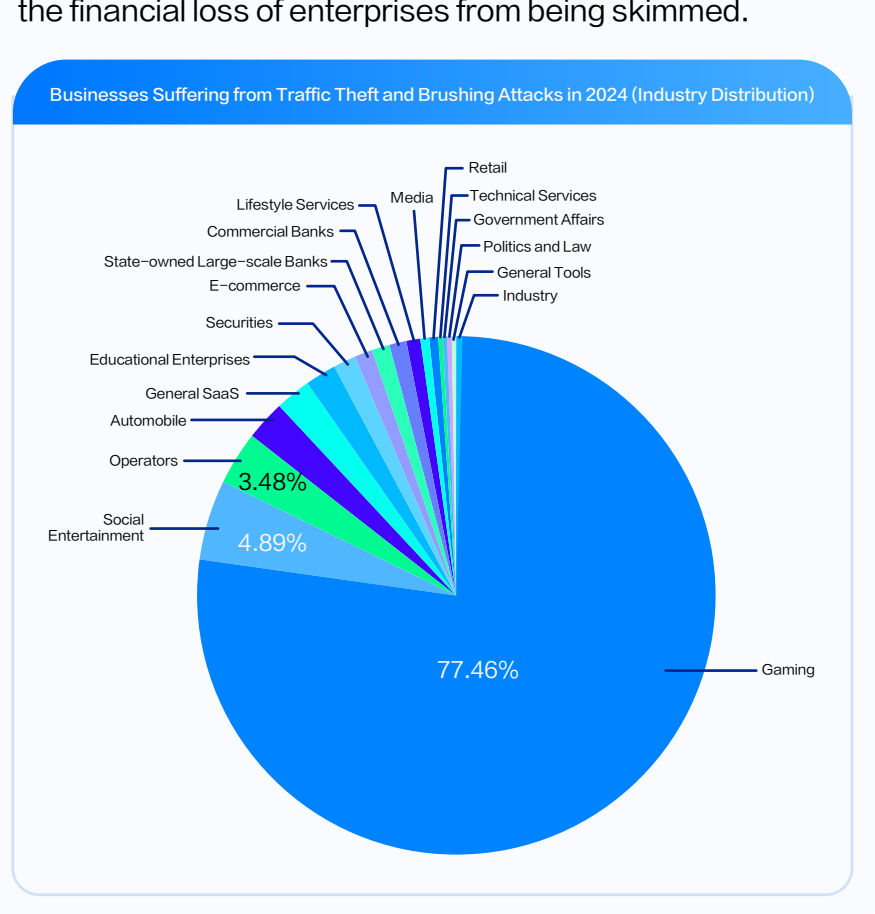
PART4 New Threat Trend: Bandwidth Theft Attacks

In 2024, download bandwidth theft attacks are becoming a new security threat trend, especially in industries such as e-commerce, cloud storage, and online streaming media.EdgeOne can help enterprises effectively respond to traffic theft attacks, which frequently initiate false download requests through malicious scripts or simulated user behavior, consuming bandwidth resources and resulting in inaccessibility to normal users or degradation of platform performance. Attackers utilize platform resources to cause economic loss or business interruption, posing a serious threat to enterprises.

Single Quarter Traffic Piracy Scale Surpasses 2 PB, Game Industry Accounts for More Than 70% of the Total

From September to December 2024, the size of traffic theft attacks exceeded 2 PB (including intercepted, ungenerated stolen traffic). The gaming industry accounted for 77% of this. The fourth quarter saw a 134% YoY increase in stolen traffic compared to the previous quarter. Attackers generate huge traffic bills by repeatedly downloading game update packages, images and other static resources, which seriously affects the bandwidth cost and system resources of enterprises. Especially in the gaming industry, game installation and update package files are generally large, making them the main target of traffic theft. EdgeOne provides free traffic anti-skimming function for all platform businesses, significantly reducing the financial loss of enterprises from being skimmed.

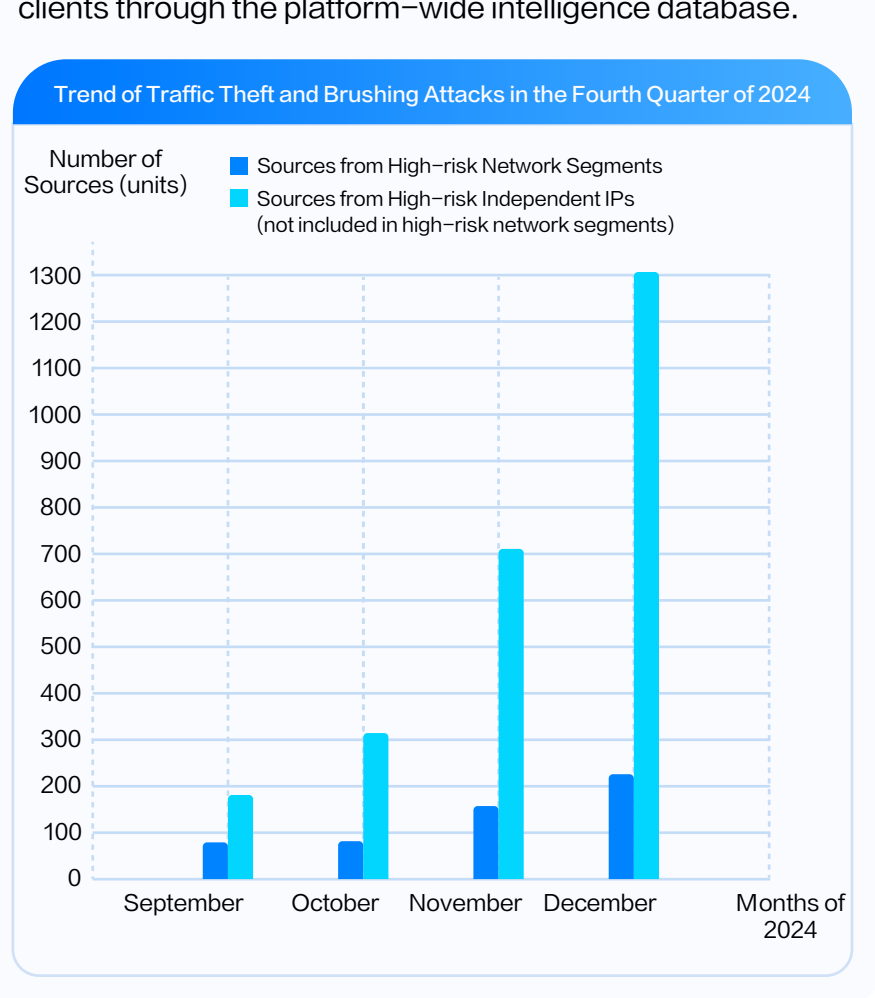
Businesses Suffering from Traffic Theft and Brushing Attacks in 2024 (Industry Distribution)



Difficulty of IP Tracing for Traffic Scraping Attacks Increases, Involving Over 47,000 IPs in a Single Quarter

In the fourth quarter of 2024, traffic theft attacks involved more than 47,000 IPs, up 367% from September. Among them, 87% of the attack traffic sources have more decentralized attributed network segments, indicating that the attackers are abusing through a distributed, low-intensity approach to circumvent detection. Traditional IP blacklisting mechanisms can no longer cope with this complex attack pattern. In order to improve the protection effect, enterprises need to accurately identify abnormal traffic and strengthen prevention by combining multi-dimensional risk control methods such as device fingerprinting and user behavior analysis, etc. EdgeOne effectively protects the static content of enterprise and personal sites by automating the identification and interception of the source of theft and the fingerprints of clients through the platform-wide intelligence database.

Trend of Traffic Theft and Brushing Attacks in the Fourth Quarter of 2024



PART5 Application Layer HTTPS Attack Cases

A live streaming service platform provides a global live streaming service, which is accessed by users through multiple endpoints (e.g., applets, APPs, Web, etc.).2024 The platform suffered a large-scale application-layer DDoS attack, which employed sophisticated tactics, in which the attacker invested a large amount of resources, and implemented a variety of highly stealthy attack methods.2025 The attack was carried out by an attacker with the help of the Bot network:

- The attack came from a real Bot network with JavaScript execution capabilities that were able to bypass basic JavaScript challenge mechanisms;
- The attack has a very high rate of concurrent requests and the source of the attack is widely distributed;
- Attackers customize clients that closely resemble business endpoints and forge similar JA3 fingerprints;
- Using a new type of HTTP2 protocol vulnerability to continuously launch attacks and consume platform resources.

This type of application layer attack combines a variety of threat mechanisms, and the attacker not only deeply customizes the clients and requests, but also launches a large-scale distributed attack through the Bot network, which reduces the request frequency of a single client. Since traditional IP frequency limiting and header feature filtering cannot effectively identify and distinguish such attacks, the new hybrid attacks pose a new challenge to the enterprise protection system.

It is expected that such attacks will gradually increase in the next 1-2 years. We recommend that Internet services, especially financial, gaming, e-commerce, retail and Internet SaaS services, upgrade their security protection baseline to address this new threat trend:

- Use distributed edge security mechanisms with more adequate protection resources (e.g., Tencent Cloud EdgeOne) to cope with larger-scale DDoS attacks;
- Deploying security solutions at the outermost perimeter of the network to better apply new TLS fingerprint ing and client fingerprinting technol ogies to efficiently identify the source of attacks;
- Frequency limiting mechanisms based on multiple statistical indicators to mitigate overall availability risks;
- Establishing a positive protection mechanism that analyzes client fingerprints and request characteristics during non-attack periods and dynamically whitens them to establish a security trust baseline;
- Using a clustering analysis strategy to aggregate and analyze metrics such as TLS fingerprints and HTTP headers to improve protection efficiency.

With powerful protection capabilities, Tencent Cloud EdgeOne helps global enterprises deal with a wide range of complex network security threats and safeguard the security of Internet services.

Co-produced by Tencent Security and Tencent Cloud EdgeOne team