CDNetworks

State of Web Application and API Protection 2022

Phone: +65 6908 1198 Email: Sales@cdnetworks.com

Table of Contents

Email: sales@cdnetworks.com www.cdnetworks.com

Significant Trends

Tbps-level DDoS Attacks Occur Frequently

As the Internet continues to develop, the scale of well-known botnets such as XorDDoS, Mirai, Gafgyt, Fodchas, and others is also expanding. At the same time, the scale of distributed denial-of-service (DDoS) attacks continues to escalate in frequency and intensity year over year, often reaching capacities exceeding Tbps levels. CDNetworks' security platform data in 2022 revealed that the peak of network layer DDoS attacks encountered by the CDNetworks' cloud platform reached 2.09Tbps, with Tbps-level attacks occurring eight times throughout the year.

Web Vulnerability Outbreak Continues

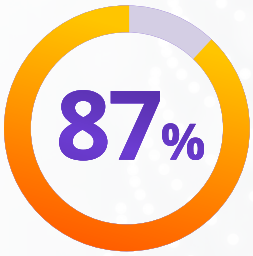
As of the end of 2022, the number of newly added vulnerabilities publicly released in 2022 and recorded in the U.S. Government's National Vulnerability Database (NVD) database is 26,431, an increase of 25.87% compared to 2021. These vulnerabilities include:

- Hot Apache Fineract path traversal vulnerability
- OpenSSL security vulnerability
- SQLite input validation error vulnerabilities
- Atlassian Bitbucket Server and Bitbucket Data Center command injection vulnerabilities
- Apache Commons BCEL buffer error vulnerabilities

It is worth noting that the Log4shell vulnerability, which was a critical-severity vulnerability, was even more insidious than first thought. After its introduction at the end of 2021, it spawned a number of variants with various vulnerabilities that continued to wreak havoc in 2022. CDNetworks' Security Platform detected a total of 27 million exploits for various variants of Log4shell vulnerabilities in 2022.

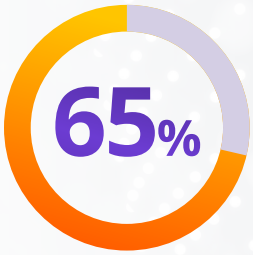
WAF Struggles to Cover Diverse Threats

The continuing digitalization evolution conducted by organizations has found their core business migrating to multiple platforms such as web, APPs, and H5. This migration relies on open Application Programming Interfaces (APIs) for flexible development. With the increasing attack surfaces of web applications, security threats such as DDoS, vulnerability



of Web-based Businesses Encountered **Two or More** Types of Threats Simultaneously

exploitation, data scraping, and business fraud are emerging, making it challenging, if not impossible, for traditional web application firewalls (WAFs) to address such diversified threats. According to CDNetworks' security platform data in 2022, 87% of web-based businesses encountered two or more threats at the same time, with 65% of web-based businesses encountering three or more simultaneous threats.



of Web-based Businesses Encountered **Three or More** Types of Threats Simultaneously

API Assets Have Become the Top Target for Malicious Attacks

In the digital era of the Internet, more and more organizations are adopting technical and economic models of APIs to remain competitive. In 2022, all API requests circulating on the CDNetworks' content delivery network (CDN) cloud platform accounted for 61.3% of the platform's total requests. The resulting API attacks have shown a significant upward trend, with the percentage of attacks against APIs exceeding 50% for the first time in 2022, reaching 58.4%.

Transportation and Information/Consulting Services Become the Hardest Hit Targets of Bot Attacks Again

Like a Phoenix rising from the ashes, the easing of COVID-19 restrictions has resurrected the tourism and travel industries and brought them back to life. The rise in tourism and travel has witnessed a surge of bot attacks on industries such as transportation and ticketing services as well as information/consulting services. According to CDNetworks' security platform data in 2022, the three industries most severely affected by bot attacks are software information services, transportation services, and information/consulting services. Bot attacks on transportation and information/consulting services industries account for as many as 25% of all bot attacks.

Web Application & API Traffic Analysis

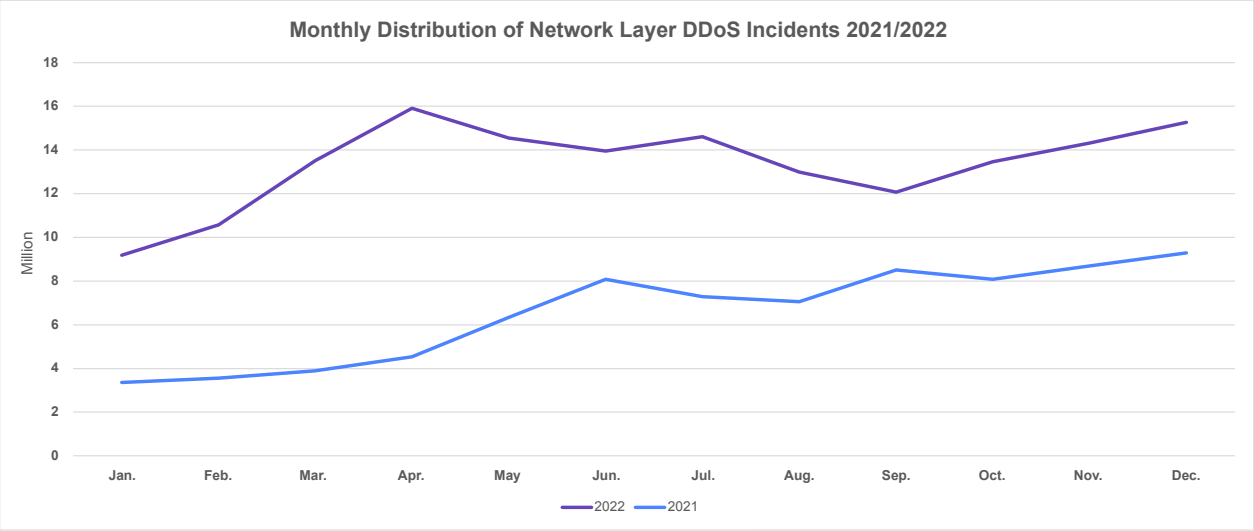
DDoS Attack Overview and Trends

DDoS Attack Peaks and Incident Numbers Hit a New High Record

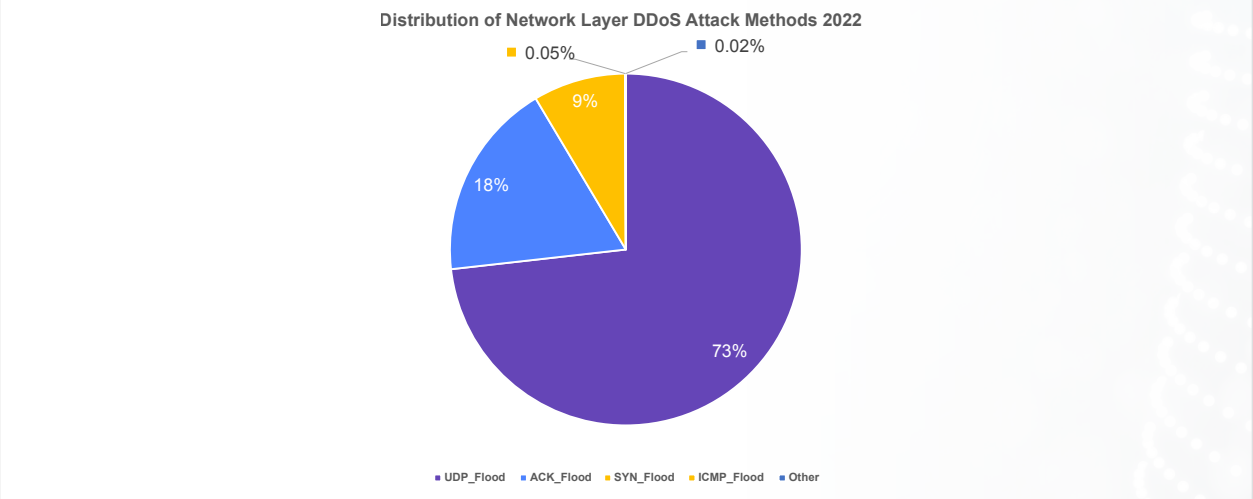
According to CDNetworks' security platform data in 2022, the number of network-layer DDoS attacks

Email: sales@cdnetworks.com www.cdnetworks.com

encountered by the CDNetworks' cloud platform peaked at 2.09 Tbps, with eight Tbps-level or higher attacks throughout the year, and the peak of application-layer DDoS attacks reached 34 M QPS. At the same time, the frequency of attacks also increased significantly. CDNetworks' security platform monitors and intercepts an average of 439,200 DDoS attack incidents per day, a year-on-year increase of 103.8%. Throughout the year, a total of 160 million network-layer and application-layer DDoS attack incidents were monitored and intercepted, a year-on-year increase of 104.59%.

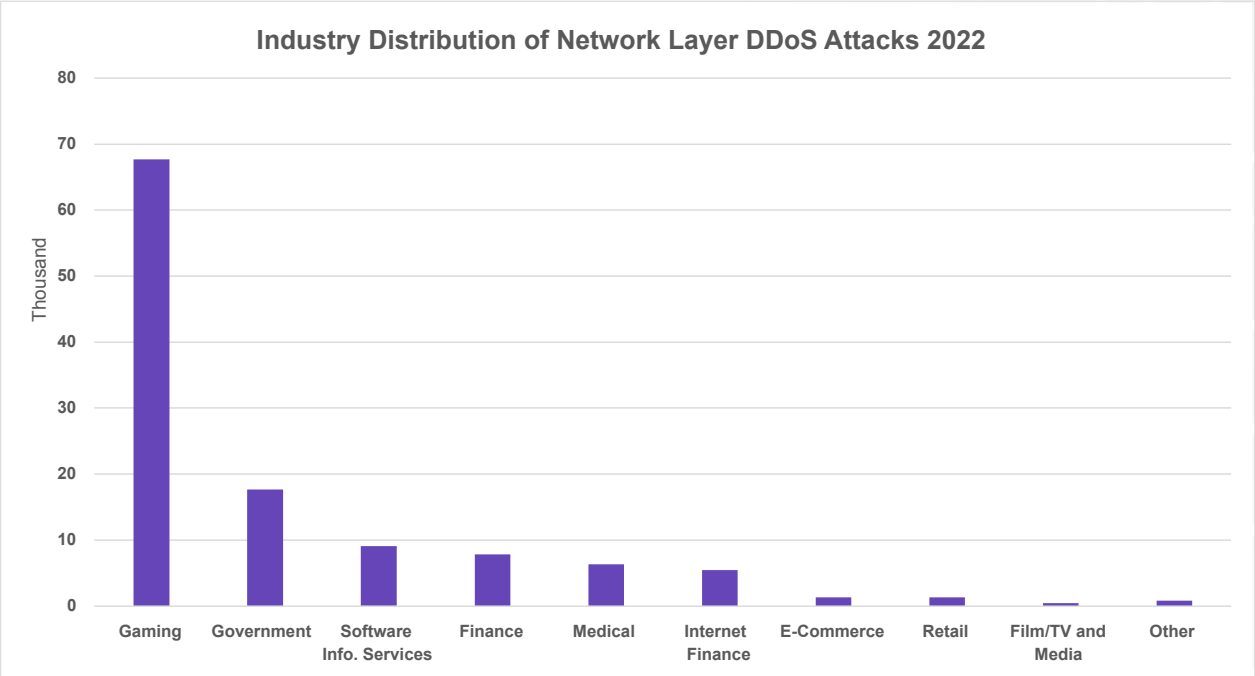


The following figure shows the distribution of top network-layer DDoS attack methods in 2022.

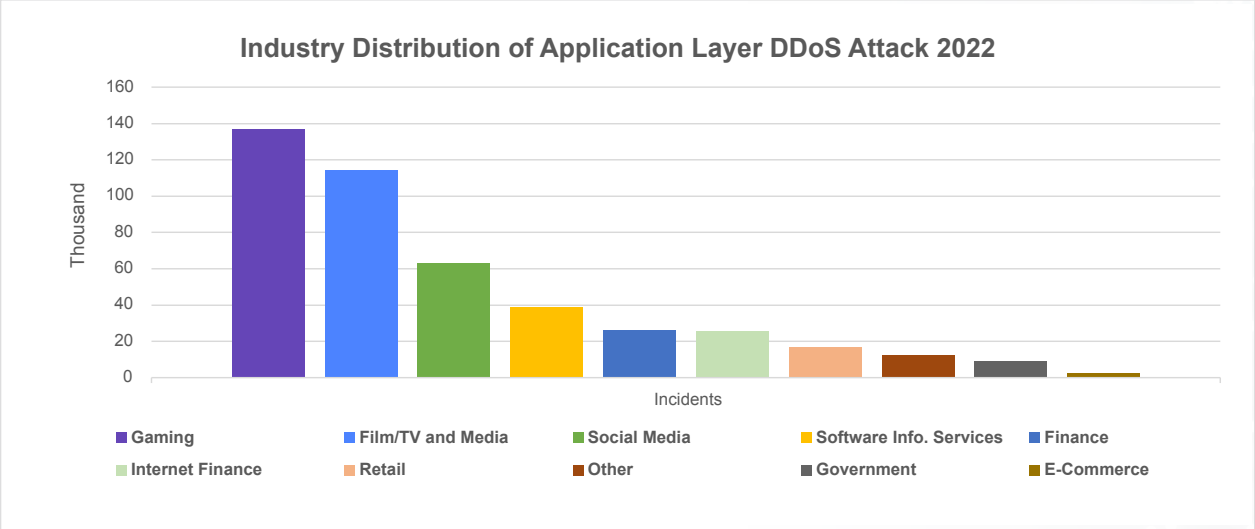


Email: sales@cdnetworks.com www.cdnetworks.com

The following figure shows the industry distribution of network-layer DDoS attacks in 2022.



The following figure shows the application-layer DDoS attacks across industries in 2022.

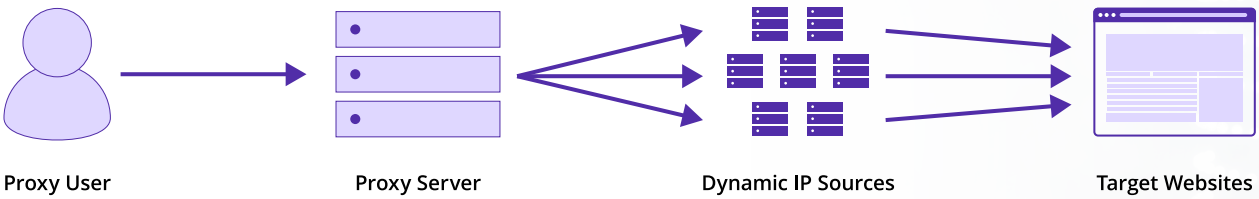


In the face of such frequent, brutal, and large-scale attacks, on-premise protection measures based on a single data center boundary are no longer able to put up a credible defense. To safeguard assets against these attacks, CDNetworks' security expert team recommends choosing cloud security service providers such as ISPs, CDNs, and cloud platforms, which have the ability to deal with large-scale attack scrubbing. In particular, some CDN platforms that provide integrated security and acceleration services can offer effective protection against large-scale DDoS attacks while ensuring positive online experiences for users and cloaking the IP address of the origin server.

Analysis of Low-Frequency Application Layer DDoS Attack Methods

By continuously tracking botnets, CDNetworks' security team found that multiple mixed botnet attacks have become the preferred mainstream attack method — and for good reason. The attack platform can quickly mobilize the resources of multiple botnets and instantly manipulate hundreds of thousands (and even more!) IP addresses of compromised devices to launch attacks. Distributed low-frequency application-layer DDoS attacks launched in this way present a considerable challenge to today's protection solutions.

Because application-layer traffic is close to an organization's business logic, DDoS attacks at the application layer can threaten the stability of both the target network and server. The attack methods and techniques used by application-layer DDoS attacks are constantly evolving and upgrading. From centralized high-frequency requests, these attacks have gradually evolved into distributed low-frequency requests. Instead of simply carrying significant malicious features in the request message, attackers often use various means to circumvent common frequency restrictions or access control policies, such as replaying legitimate request traffic, using fake search engine bot traffic, and second dialing IP addresses. Among these means, Second-Dialing IP addresses has become an important tool that is frequently used in low-frequency application-layer attacks.



The underlying idea of second dialing is to use the IP address pool management principle of broadband dial-up (PPPoE) to obtain a new IP address every time a connection disconnects and reconnects. The intent is to achieve dynamic allocation and recycling of IP addresses by managing the IP address pool. When a user needs to use an IP address, an available IP address is assigned to the user from the IP address pool. When the user has finished using that IP address, the address is recycled to the IP address pool where it can be used for the next assignment.

Using a large number of Second-Dialing IP addresses to launch attacks on legitimate and low-frequency requests of web service sites has two advantages in combating defense strategies:

1. Huge Pool of Resources: With as few as 100,000 or as many as a million Second-Dialing-IP addresses, attackers can bypass traditional frequency-based protection methods easily.
2. Hard to Distinguish: Second-Dialing IP shares the same pool as normal user sources, and the survival period of second dial IP is short. After an IP address is released, it is highly likely to be

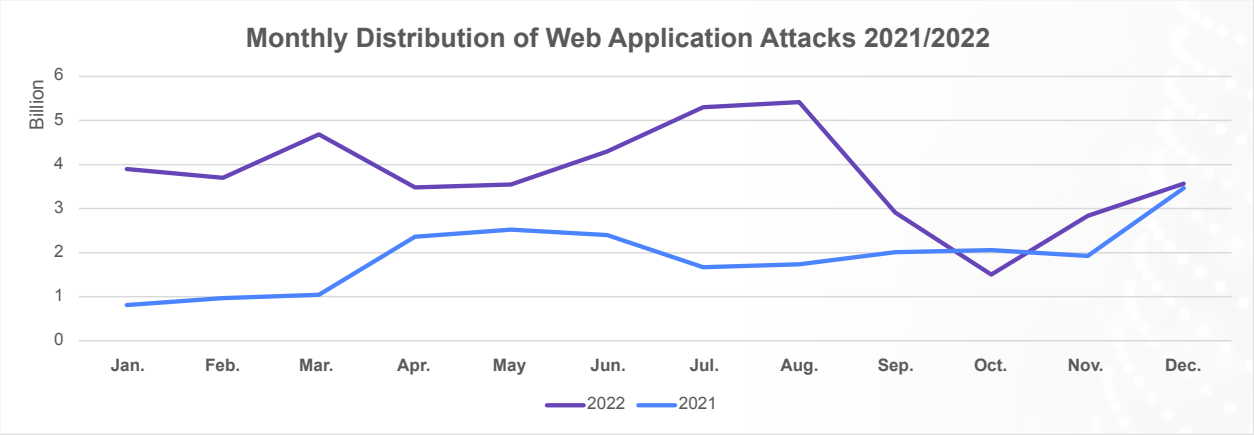
allocated to normal users. This makes it extremely difficult to distinguish between normal user IP and second dialing IP. As a result, using traditional methods to defeat such attacks, such as by accumulating IP pools, inevitably result in large numbers of false positives.

The most effective way to defend against Second-Dialing-IP is to identify risky IP addresses. The core basis for identifying risky IP addresses is rooted in determining whether an IP address is currently held by blackmail based on the factors of “blackmail usage period” and “time effectiveness of the IP address.” For “non-shared” IP addresses, such as home broadband and data center host IP addresses, it is important to determine whether the IP address is being used by the black market. For “shared” IP addresses, such as outside address of the NAT, and those used by base stations, the prevention and control threshold should be relatively lenient to account for the large number of users located behind a single IP address. However, if it can accurately determine when an IP address is being used by the black market, this information can be an important reference indicator for spotting nefarious activity. CDNetworks’ DDoS protection product teams have invested much effort in intelligence data mining, analysis, and production to form data-driven protection capabilities that can effectively mitigate all kinds of low-frequency application-layer DDoS attacks.

Web Application Attack Overview and Trends

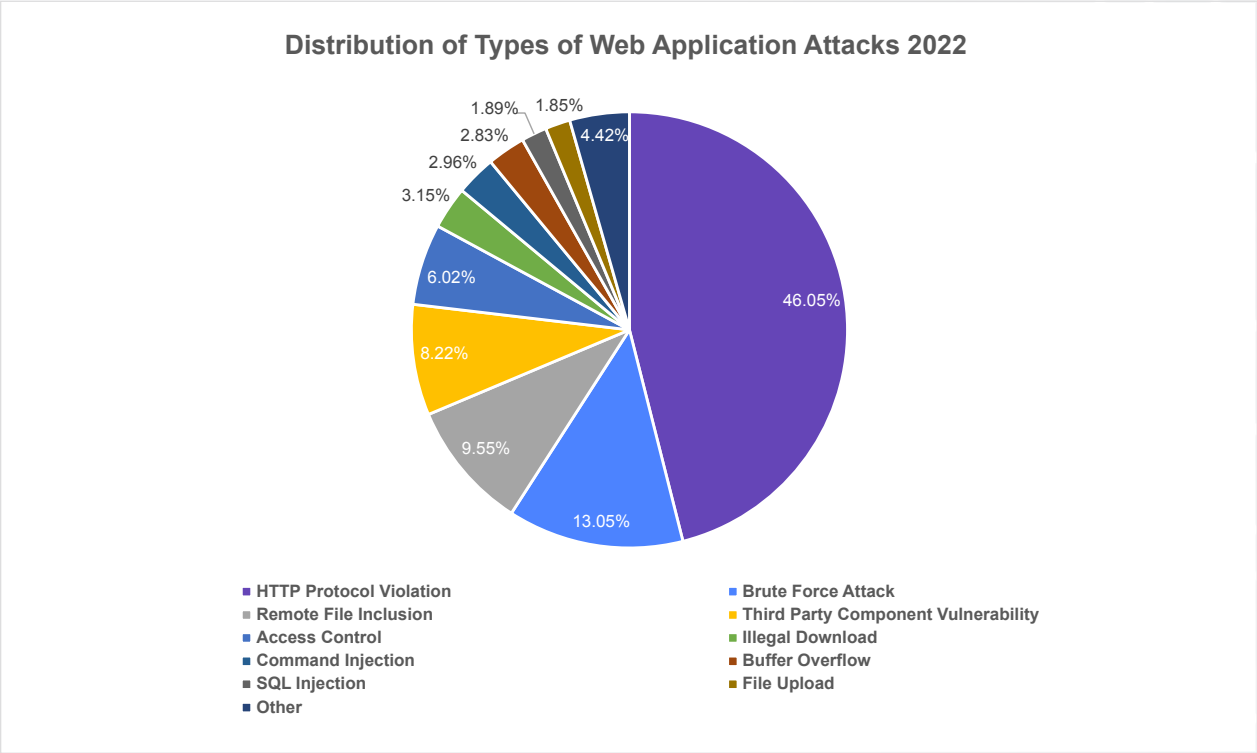
Web Application Attacks are Surging

According to statistics collected by the CDNetworks’ security platform, 45.127 billion web application attacks were detected and blocked throughout the year — an increase of 96.35% compared to the last year. Among them, the monthly distribution of web attack incidents is shown in the following figure.

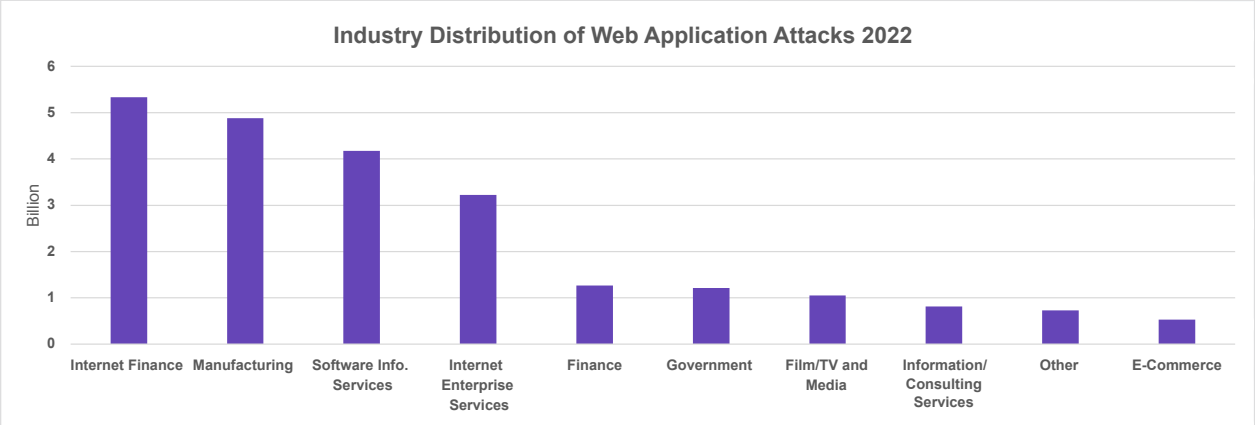


HTTP Protocol Violation, Brute Force Attacks, Remote File Inclusion, Third-party Component

vulnerability, and Access Control are the top 5 types of web-application attack.



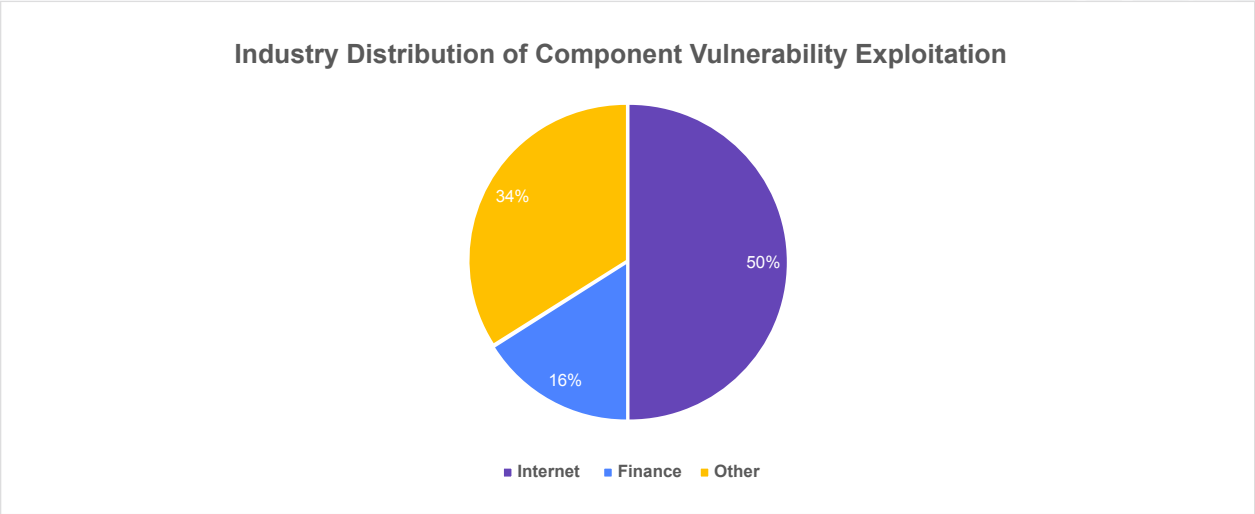
Manufacturing, Internet finance, and software information services are the main industries targeted by web application attacks.



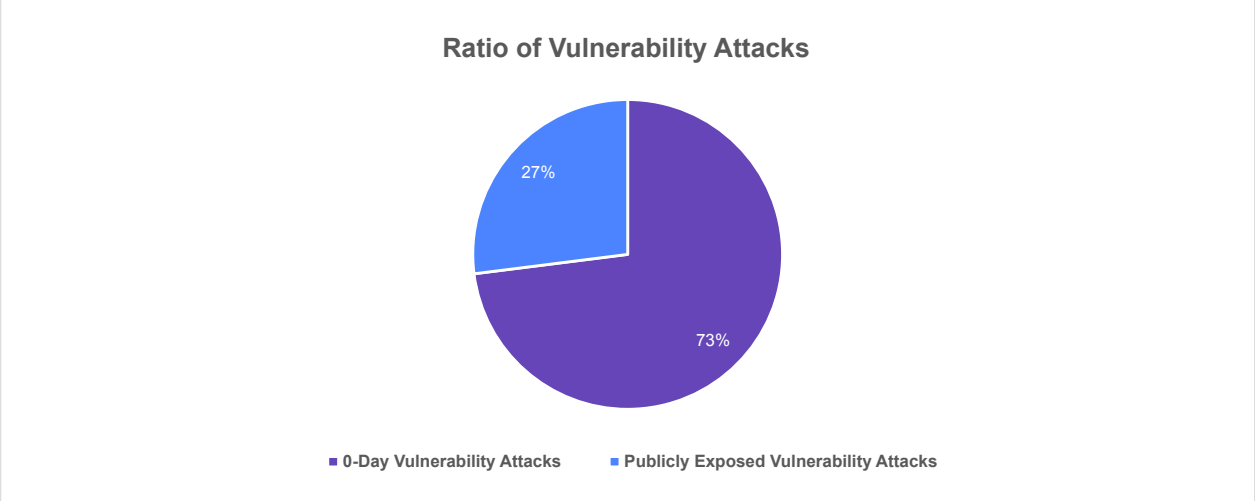
Analysis of 0-Day Vulnerability Exploitation Attacks

In 2022, the CDNetworks' Security Platform found that 66% of vulnerability exploitation attacks occurred in the Internet and financial industries. The reason for targeting these industries is due to the fact that they often hold more valuable information and assets than data associated with other industries.

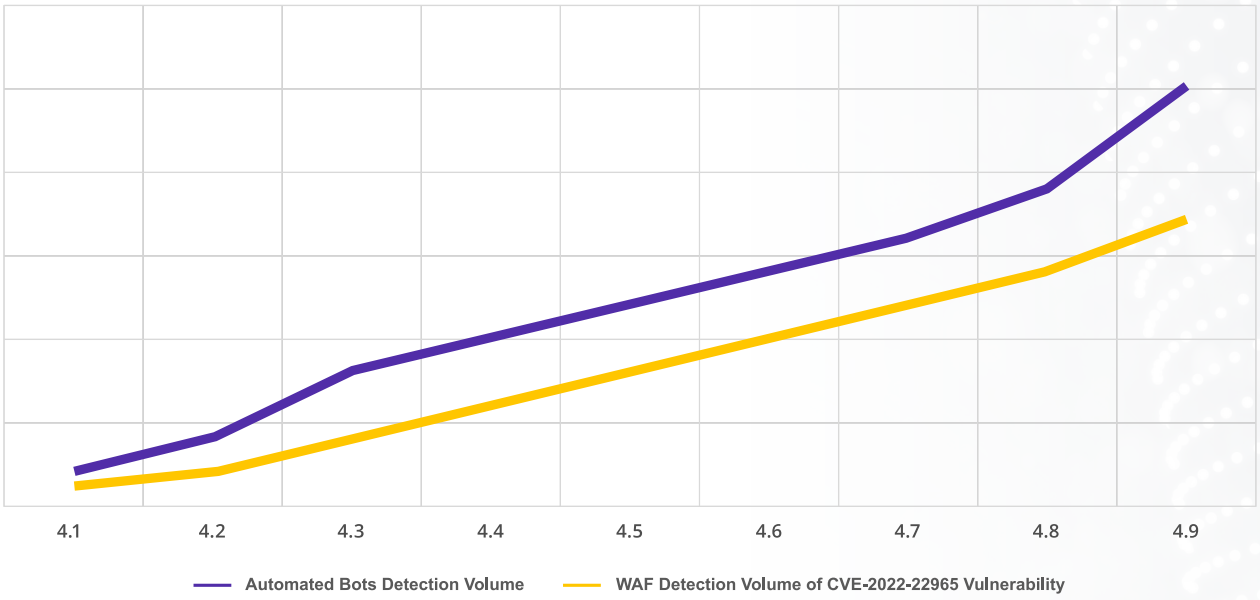
Email: sales@cdnetworks.com www.cdnetworks.com



The percentage of attack exploits for new vulnerabilities reached as high as 73%.



Before the 0-Day vulnerability was formally announced, hackers had already exploited it to their advantage. The CDNetworks' security expert team found that prior to the formal announcement about the 0-Day vulnerability, hackers had already used it to their advantage by utilizing automated programs to conduct batch sniffing to find potential attack targets quickly. One prominent example is the CVE-2022-22965 Spring Framework remote code execution vulnerability. After this vulnerability was formally announced, tracing historical attack data in the CDNetworks security platform revealed that a large number of probing requests initiated by this vulnerability had been identified by CDNetworks' Bot Shield protection products even before the vulnerability was announced publicly. By analyzing the number of WAF detections and automated bot detections corresponding to the CVE-2022-22965 vulnerability, we found two trends that have a significant positive correlation.



When examining the rate at which vulnerabilities propagate, the speed at which the Internet shares information contributes significantly to the velocity at which vulnerabilities are spread. After the official disclosure of 0-Day vulnerabilities, hackers may have already completed large-scale initial sniffing on the Internet using batch-scanning tools. As a result, WAF and other devices that have not updated their defense rules at this point place their organization's web business at extremely high risks of being compromised.

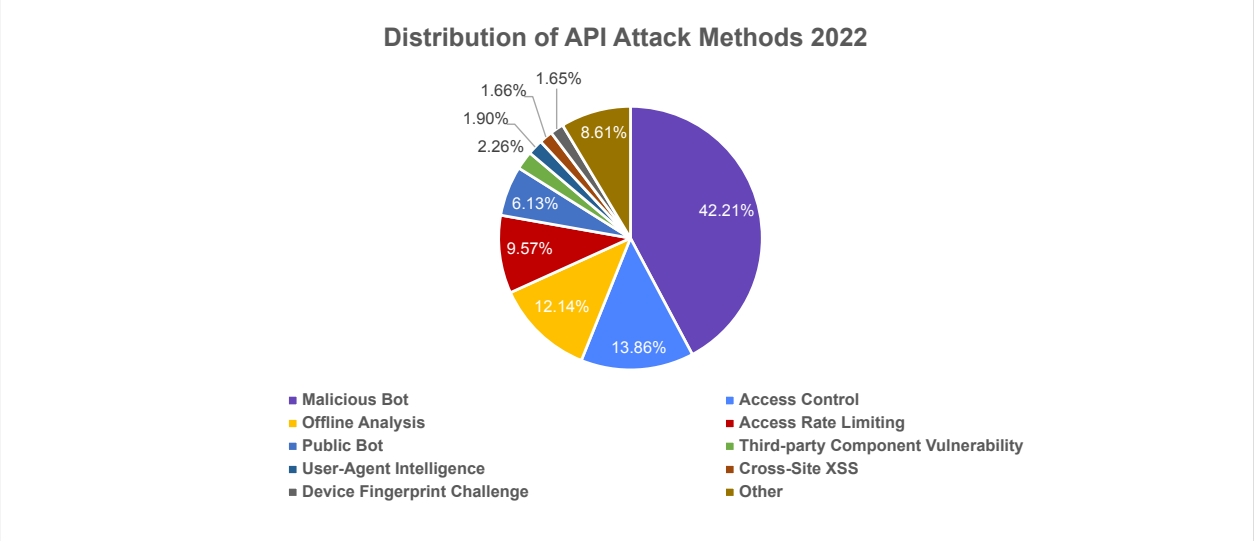
In terms of the effectiveness of responding to 0-Day vulnerabilities, traditional defense models rely on updating rule plugins on WAF devices for protection. In the face of the endless 0-Day vulnerabilities and the impact of continuous N-Day vulnerabilities, the requirements for the WAF defense capabilities are increasingly high. An organization's security operations personnel need to consider both security and service stability when making reasonable decisions about updating rule libraries. In addition, as businesses expand rapidly, their IT systems become increasingly complex, resulting in a lack of unified central management for defense systems. These challenges create potential security risks, as individual security devices become disconnected from the edge and are unable to update defense rules promptly to cope with emerging cyberthreats.

When retaining the WAF device of origin, the CDNetworks security expert team recommends combining the cloud WAF protection service with threat intelligence data from the third-party cloud security platform. In this way, organizations can respond to 0-Day vulnerabilities and establish a multi-layer defense system quickly and effectively.

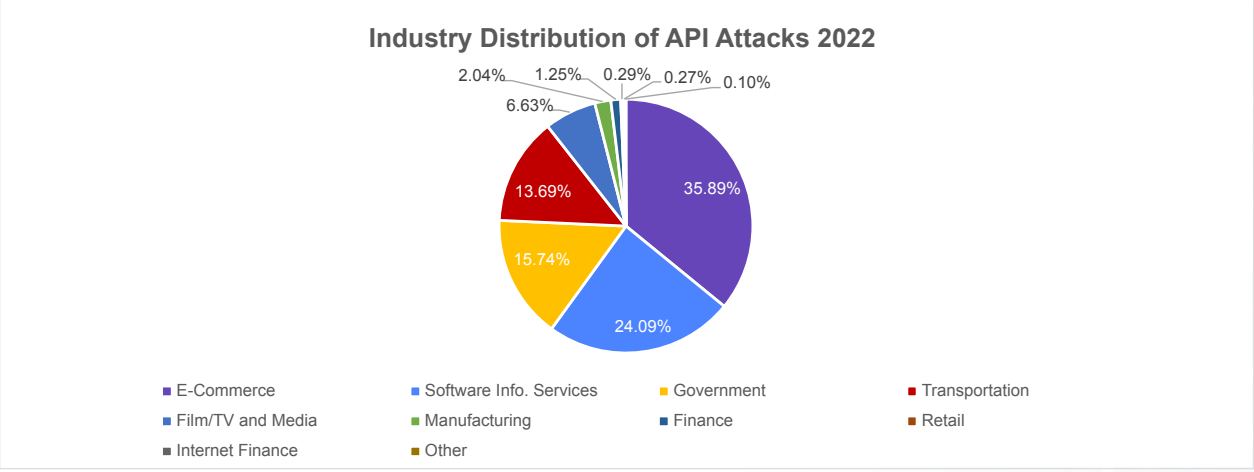
API Attack Overview and Trends

API Attack Incidents Continue to Grow at a High Speed

Throughout 2022, attacks against API businesses continued to exhibit a high-speed growth trend. As mentioned earlier, the proportion of attacks on APIs exceeded 50% for the first time, reaching 58.4% in total for the year. Compared to the first half of 2021, the attack types aimed at APIs have become increasingly fragmented, with Malicious Bots, Access Control, Offline Analysis, and Access Rate Limiting threats becoming the main types of API attacks.



In terms of industries, e-commerce (35.89%), software and information services (24.09%), government agencies (15.74%), transportation (13.69%), and film/TV and Media (6.63%) continue to rank as the top five industries impacted by API attacks.



Lack of Security Management System for API Assets is Becoming a Major Loophole

APIs act as a way to bridge different components of a software system. Attackers can access sensitive data, tamper with data, or even directly attack back-end systems through APIs, which can cause serious damage to an organization's assets and reputation. The CDNetworks' security expert team analyzed the reasons behind the rapid increase in API attacks and found the following causes.

Firstly, API attacks are cost-effective. Attackers need to find only the API interface address and, once found, can obtain data or launch attacks using simple network requests. In contrast, attacking an entire website requires attackers to possess higher technical skills and takes more time. For example, attackers can use API interfaces to obtain users' personal information, account balances, and other sensitive data, and then conduct phishing fraud or directly steal user funds. In addition, attackers can tamper with the data returned by APIs, causing damage to the organization's business, such as altering product prices, inventory information, and other information, resulting in heavy losses for the enterprise.

Secondly, companies have an unclear understanding of their API assets. This makes it difficult for companies to fully protect the security of all API assets, leaving a loophole in their business. Moreover, security threats posed by zombie and shadow APIs can expose sensitive data while residing in hidden "black holes" that may be completely unknown to operations personnel or even the company itself. It is not surprising, therefore, that security management and protection start with "known" and "visible" assets, but make it difficult, if not impossible, for operations personnel to secure forgotten and invisible assets. Because these forgotten and uncontrollable APIs are often hidden and less likely to be updated with the latest security patches, they make the perfect candidates for breaches when cybercriminals come calling.

Organizations that fail to adopt a comprehensive security policy that protects their APIs leave themselves vulnerable to cyberattacks. In June 2022, for example, Travis CI, a continuous integration development tool, suffered an API breach that allowed anyone to access the company's plaintext historical logs. The breach compromised more than 770 million pieces of user log data containing 73,000 tokens, access keys and other cloud service credentials.

API Attack Techniques Analysis

CDNetworks' security expert team analyzed and found that attackers often exploit API flaws to launch a series of destructive attacks against API businesses:

1. **Improper Identity Verification and Access Control**
   Identity verification and access control are the first line of defense for API security. If implemented improperly, attackers can bypass or break through these mechanisms to gain unauthorized access to APIs. In a well-known case, the failure of a social media platform's API to authenticate the source of API requests allowed attackers to use stolen credentials to gain unauthorized access.
2. **Theft of Sensitive Information**
   The attacker retrieves confidential information such as usernames, passwords, and API keys by searching for them in unencrypted transmissions or data storage repositories. According to APIsecurity.io, data leakage is the second biggest issue when it comes to API security risks. Some APIs expose excessive amounts of data, including users' private information and system configuration information. Attackers can use this information to launch targeted attacks. Therefore, APIs should implement the principle of least privilege, providing only the minimum amount of information needed to the applications that need the data.Attackers can also steal and modify data through insecure data storage. For example, a social media platform's API stored users' personal information without hashing or encrypting passwords, allowing attackers to directly access and steal user passwords.
3. **Brute-force Attacks and Credential Stuffing**
   An attacker can perform brute force attacks and credential stuffing by systematically checking large numbers of usernames and passwords until the right combination is found. This type of attack can exploit API weaknesses, which can lead to accounts being blocked or being completely hijacked.
4. **API Parameter Pollution**
   Attackers modify the parameters of an API to alter the results that it returns. This type of attack usually occurs in an API's query string, POST data, or HTTP header. By modifying these parameters, an attacker can bypass the API's access control or spoof the API's returned results.
5. **Replay Attack**
   An attacker may be able to bypass authentication or perform unauthorized operations by exploiting a replay attack vulnerability in the API service to repeatedly execute previous requests. For example, the attacker might repeat a previous request to execute malicious operations or steal data.

To deal with API attacks, it is key for organizations to effectively manage API security risks. At a minimum, the CDNetworks security expert team encourages organizations to adopt the following recommended security protection guidelines:

 Email: sales@cdnetworks.com www.cdnetworks.com

1. **Avoid API Security Flaws**

   Make sure API gateways and other management tools used allow you to manage closed-loop integration across the entire API lifecycle stages. This includes API planning, design, implementation, testing, release, operation, invocation, version control, and retirement.
2. **Secure Your Core Data**

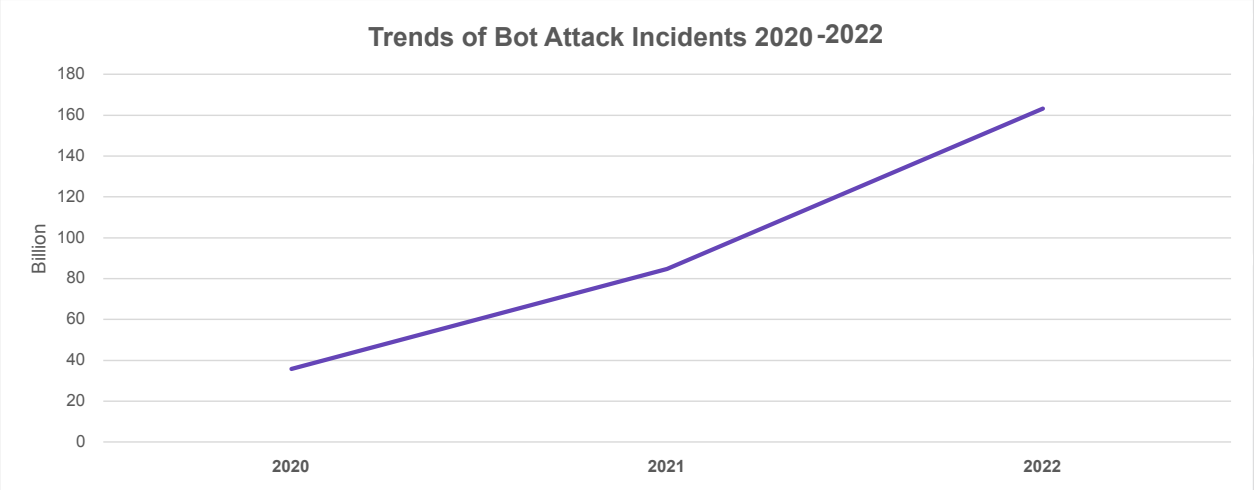
   Secure your core data through sensitive data discovery, vulnerability assessment, de-identification, auditing, data security posture operation, and other means.
3. **Protect Against Threats**

   Obtain assistance from professional API security tools or Web Application and API Protection Products (WAAP). Include protection afforded by identity verification, content inspection, traffic management, artificial intelligence (AI) business model analysis, and other methods. Together, using this approach protects APIs from abuse, unauthorized access, and denial of service attacks prompted by their own shortcomings and flaws.

Bot Attack Overview and Trends

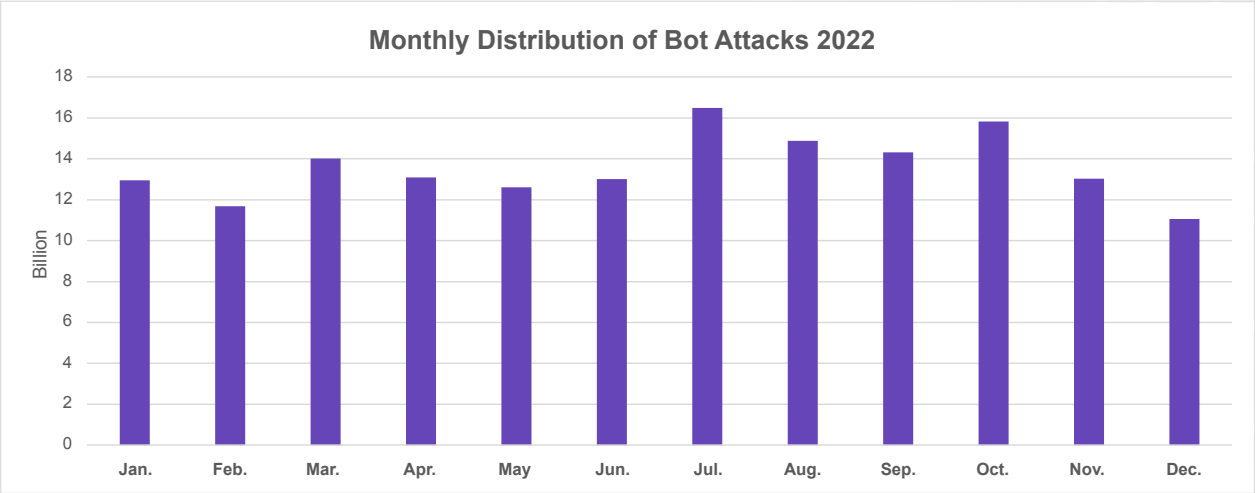
More and More Attacks are Launched from Automated Bots

The CDNetworks security platform monitored a total of 163,185 million bot attacks throughout 2022. This equates to an average of about 5,175 bot attacks per second. Compared to previous years, the number of attacks is 1.93 times higher than in 2021 and 4.55 times higher than in 2020.



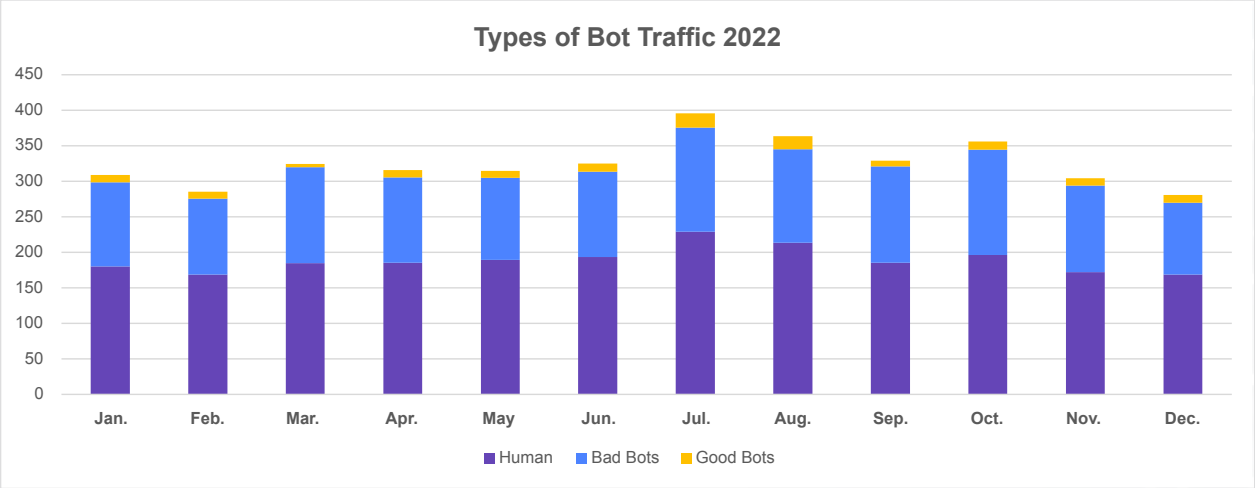
Email: sales@cdnetworks.com www.cdnetworks.com

Among them, the distribution in the number of bot attacks in 2022 is as follows.



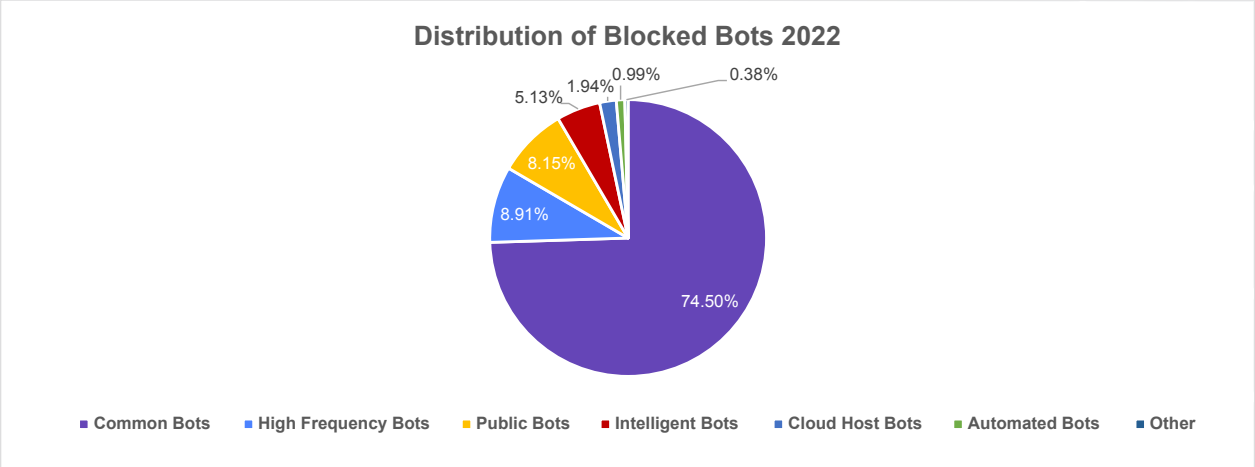
Bot traffic accounts for up to 40% of web application and API traffic

Data from CDNetworks' Security Platform 2022 shows that only about 60% of the traffic to web applications and APIs really were made by human visits. The remaining 40% is mostly bot traffic, which includes search engine bots and malicious bots. The vast majority of this traffic comes from malicious bots.



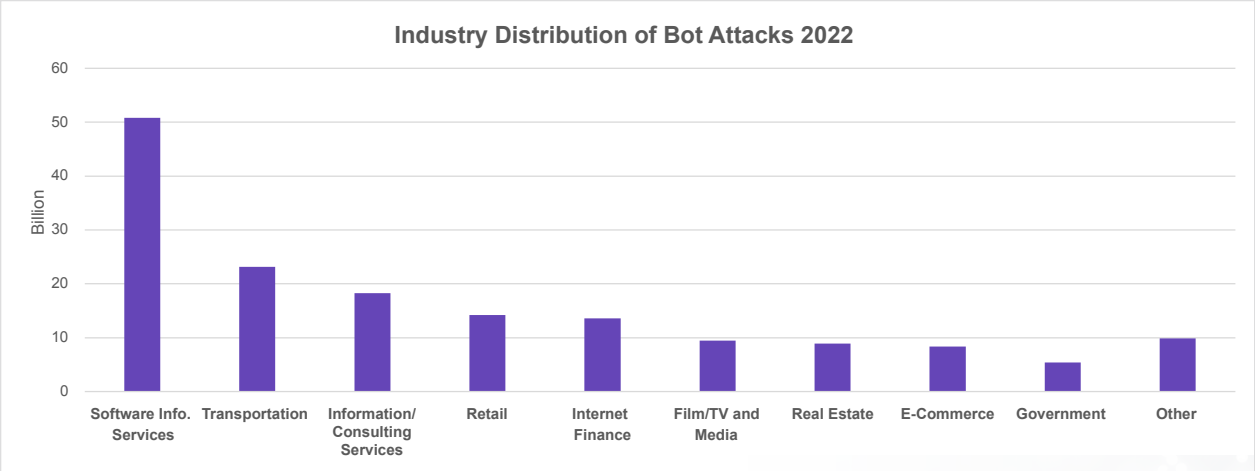
Email: sales@cdnetworks.com www.cdnetworks.com

The following figure shows the types of bot attacks.



Software Information Services, Transportation, and Informaton/Consulting Services are Three Key Industries Prone to Vulnerability

Looking at industry segments, the three industries most severely affected by bot attacks are software and information services, transportation, and information/consulting services, all of which are closely related to people's lives today. These top three industries were attacked by more than half of the total number of bot attacks.



Bot Attacks are Becoming More Insidious

After aggregating and analyzing the massive amounts of bot attack data, CDNetworks' security expert team found that bot attacks are becoming more and more insidious. For example, some malicious bots forge normal User-Agents and use automated frameworks that simulate a normal browser to launch their attacks. In addition to forging a seemingly legitimate User-Agent value, bots can disguise themselves as bona fide search engine bots to confuse fixed-rule-based detection schemes and elude the "heavy siege" of traditional protection methods.

Bot Attack Techniques Analysis

The CDNetworks' security expert team analyzes techniques used in bot attacks, and then classifies the attacks into meaningful categories such as:

Regular/Common Bots

Bots blocked by cookie/JavaScript challenges, human interaction verification, access control, and similar policies

High Frequency Bots

Bots intercepted by rate limiting policies

Known Bots

Search engine bots identified by bot intelligence

Intelligent Bots

Bots identified by fingerprint challenges, machine learning, AI analysis, and similar strategies

Cloud-Hosted Bots

Bots sent to a cloud host IP address defined in a bot intelligence library

Automation Tools Bots

Bots that involve automation tools defined in a bot intelligence library

To understand how pernicious bot attacks can be, the following table created by the CDNetworks' security expert team shows a real-world scenario suffered by an airline company in 2022. In this attack, automated and intelligent ticket-scalping bots were used to purchase as many airline tickets as possible to later resell at a high markup. The bots were based on an automated framework that allowed them to complete the entire ticketing process.

Email: sales@cdnetworks.com www.cdnetworks.com

Normal Ticket Purchasing Process	Automated Framework BOT	Note
Trip Search	Automated Trip Search	
Ticket Price Inquiry	Automated Ticket Price Inquiry	Main Targets
Account Login	Automated Login	
Edit Passenger Information	Automatically Add and Select Passengers	
Submit Order	Automatically Submit Orders	
Pay Order	Automatically Pay Order	

CDNetworks' security experts team offers the following recommendations for organizations to address in the face of ever-changing types of bot attacks.

Automated frameworks are essentially still written and maintained by humans. Due to the dual constraints of efficiency and cost, attack behavior often differs from normal human access in one or more areas. For example:

1. **User-Agent(UA)** to avoid detection and tracking, automated frameworks typically change UA values dynamically, usually by using random UA generation tools or maintaining UA lists.
2. **Access Interval:** to take advantage of the efficiency of scraping page information, the access interval of the automated framework is usually different than that of normal human access. For example, after querying air tickets, real human access usually stays on a page longer than automated access.
3. **Similar Behavior:** although the automation framework can mimic the normal human click, swipe, and other operational behavior, such behavior must be performed using recording or coding methods. Usually, multiple clients exhibit identical or similar operational behavior.
4. **Access Sequences:** due to cost and efficiency constraints, automation frameworks often present a regular access sequence when scraping page information.

Based on these differences, the following protection strategies can be used:

1. Adopt stricter verification such as CAPTCHA or direct blocking of IP addresses, UA, and other identifiers that have a history of malicious attacks based on intelligence.

2. Support dynamic detection of browser kernel and browser fingerprint using browser feature detection denies visits by bots carrying an illegal UA or associated multiple UAs.
3. Continuously use big data analysis and AI detection technology to infer and detect website access logs, identify abnormal human-like access behavior, and implement appropriate controls.
4. Consider using professional bot management services from third-party cloud security platforms. For instance, the product team of CDNetworks' bot management solution, Bot Shield, has been deeply involved in e-commerce, ticketing, aviation, fintech and other industries for many years, and has accumulated decades of experience in bot management. Bot Shield can effectively identify and prevent attacks and abuses such as content scraping, denial of inventory, brute force, malicious registration, and malicious vulnerability scanning.

Online Business Fraud Incident Analysis

The digital transformation faced by today's organizations is prompting large numbers of offline businesses to accelerate their online presence. As a result, the ability to examine website traffic patterns has become critical, and Html5 and mini-programs are becoming increasingly popular. At the same time, an organization's online business requires APIs so that data, algorithms, transactions, processes, and other business functions can be shared — making APIs key targets for cyberattacks. Cybercriminals and fraudsters often use highly personalized and automated attack techniques in large volumes, along with various device-emulating tools that falsify information, all of which contribute to the dramatic increase in online fraud risks.

CDNetworks' security expert team analyzed the 2022 CDNetworks platform traffic and found that many enterprises suffer from malicious registration, malicious login, marketing cheating, and other business fraud. As more and more enterprises conduct and promote their businesses online in today's post-pandemic era, the black market that survives by profiting from business fraud is extending its reach to various industries, especially brand retail, online e-commerce, ticketing, and finance.

These cyberthreats have become so pronounced that in 2023, the OWASP API Security Top 10 added "API8 Lack of Protection Against Automated Threats" to its list of growing API security vulnerabilities. This move indicates that threats such as data scraping and business fraud initiated by automated bots must be taken seriously by organizations.

Email: sales@cdnetworks.com www.cdnetworks.com

Fraudulent Activities are Supported by a Dark Supply Chain

The black market continues to engage in fraudulent business through a large amount of automation and process-oriented methods — actions that permeate across all online businesses. In rampant attack scenarios targeting registration, login, and marketing, the proportion of automated attacks is well over 50%. Taking the heavily affected e-commerce industry as an example, we have outlined in the following figure major attack scenarios and risk types.

Login Registration

Credential Stuffing
API Abuse
SQL Injection
XSS Vulnerability
Cookie Injection and Tampering
WebShell Upload

View Product

Content Scraping
Inventory Scraping
SQL Injection

Add to Your Cart

API Abuse
SQL Injection
XSS Vulnerability
Cookie Injection and Tampering
WebShell Upload

Place an Order

API Abuse
SQL Injection
XSS Vulnerability
Cookie Injection and Tampering
WebShell Upload

Each business process is prone to fraudulent behavior, and the black market that lurks in the background has a highly mature industrial and technological infrastructure that is prepared to scam organizations out of their revenue and data as shown in the following diagram:

Fraudulent Activity Process	Methods
Material Layer	Phone Card Sellers, Account Merchants, Bank Card Sellers, Leaked Accounts/Passwords through Interface Attacks
Platform Layer	Captcha Solving Platform, Temporary Phone Number Platform, Proxy IP Pool, Illegal Trading Platform
Tool Layer	Mobile Group Control Software, Automation Tools, and Device Modification Tools.
Implementation Layer	Credential-Stuffing, Transaction Fraud, Marketing Fraud, Scalpers Proxy Ordering, Fake Orders
Profit-making Layer	Reselling Discounted Goods, Cashing Out, Earning Commissions through Fake Orders, Stir-frying Customer Information or Credit History

To deal with highly industrialized business fraud, organizations need refined and scenario-based

risk management solutions. Currently, large enterprises in finance, e-commerce platforms, ticketing, and similar industries have their own risk control systems. The capabilities of some professional risk management and intelligence companies are also incorporated into their own risk management systems. However, many small and medium-sized enterprises do not yet have the ability and experience to deal with such threats. For these organizations, the CDNetworks' security expert team suggests seeking help from professional security companies that provide business scenario-based solutions, such as CDNetworks' risk management service.

Security Recommendation

Based on the observation of web security trends in 2022, the CDNetworks' security expert team recommends that enterprises fully integrate DDoS protection, WAF, bot management, API security, threat intelligence, and other protection capabilities to achieve full-scenario, one-stop protection for web business. Adopting such holistic solutions protects an organization's multi-channel assets and effectively responds to diverse threats.

When choosing a WAAP solution, pay special attention to the following capabilities:

- **Prioritizing CDN and cloud computing platforms with high security levels of their own**
  CDN and cloud computing platforms that serve as the critical Internet infrastructures provide high levels of security. For example, under the IT infrastructure of a hybrid cloud, the real business origin can be hidden using CDN/cloud computing and WAAP reverse proxy, thereby achieving attack surface convergence and reducing the risk of exposure.
- **Supporting complete closed-loop API asset and risk inventory, integrated management, monitoring, and response**
  With increasingly complex web security threats emerging on a near-daily basis, only end-to-end closed-loop security management can truly address the challenges posed by today's ever-emerging threats. When choosing a solution, avoid stacking web and related security products. Instead, focus on whether the product has core capabilities such as API asset and risk inventory, integrated management of security policies, and highly automated monitoring and response.
- **Combining powerful threat intelligence with Proactive AI capabilities**
  Data-driven intelligence and proactive AI-based capabilities are indispensable when it comes to addressing automated stealing of sensitive data, business fraud, and other attacks that exceed the capabilities of traditional passive protection strategies. We recommend you consider WAAP solutions that include intelligence, AI capabilities, and the ability to detect threats.

- **Providing Managed Security Services**

  Complex web security threats raise the bar with extremely high requirements that organizations must acknowledge in order to build and maintain a defense-in-depth security posture. We recommend you give preference to vendors that have a proven track record when it comes to continuous expert security operations and security managed services to realize the total protection value of WAAP solutions.

In 2022, CDNetworks has officially released its cloud-based WAAP solution. CDNetworks' WAAP is a cloud-based protection solution uniquely designed to combine the power of threat intelligence and proactive AI capabilities with managed security services. Integrated features such as DDoS Protection, Web Application Firewall (WAF), API Protection, Bot Management, and other advanced technologies empower CDNetworks' WAAP solution to mitigate a broad range of runtime attacks. Our WAAP solution offers a full range of features to deliver a comprehensive, one-stop experience that helps organizations protect web sites, applications, and APIs with more automatic and applicable measures, while ensuring top performance and reliability with unlimited scalability.

To learn more about our WAAP solutions and take advantage of a free trial offer, please contact us.