CDNetworks

State of the Web Security H1 2021

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

Table of Content

Email: info@cdnetworks.com www.cdnetworks.com

Overview

CDNetworks serves thousands of enterprises, governments, and online services by collecting and analyzing anonymized attack data, and then reporting the results in annual security reports sent to clients. These reports analyze a variety of critical indicators—including attack volume, forms of attacks, and target industries—from various perspectives.

All data used in the report is provided by the CDNetworks security platform. This platform, like the CDNetworks security services themselves, continues to evolve based on cyber-security trends indicated by the data; however, such evolutions do not affect how CDNetworks interprets or gains insight into such trends based on the data analyzed in order to understand the state of attack and possible defense mechanisms and strategies.

The report makes a comprehensive comparison of attack and defense data in 2019, 2020, and the first half of 2021 to identify and interpret attack trends.

DDoS Attacks Overview

- In H1 2021, the CDNetworks security platform detected about 30 million distributed denial of service (DDoS) attacks. This number is consistent with the same period in 2020, while the peak number of DDoS attacks experienced a slight increase.
- Traditionally, one of the hardest hit areas by cyber-attackers has been the gaming industry, which ranked first in the number and peak level of DDoS attacks in H1 2021.
- In terms of reflection-amplification attacks, the network time protocol (NTP) experienced a sudden increase in attacks that accounted for 87.55% of the attack volume.

Web Application Attacks Overview

- In H1 2021, the CDNetworks security platform monitored and blocked 10.113 billion Web application attacks. This number was 2.39 times higher than that of H1 2020 and 21.66 times higher than that of H1 2019. This increase demonstrated an overwhelming increase in Web application attacks.
- The target of Web application attacks shifted from government assets to industries such as software information services, real estate, and finance.

Email: info@cdnetworks.com www.cdnetworks.com

Bot Attacks Overview

- In H1 2021, the CDNetworks security platform monitored and blocked 34.147 billion bot attacks. This figure equated to an average of 2183.52 attacks per second, doubling the figure of previous years.
- The software-information service was the industry most affected by malicious bot attacks, followed by real estate, transportation, and e-commerce.

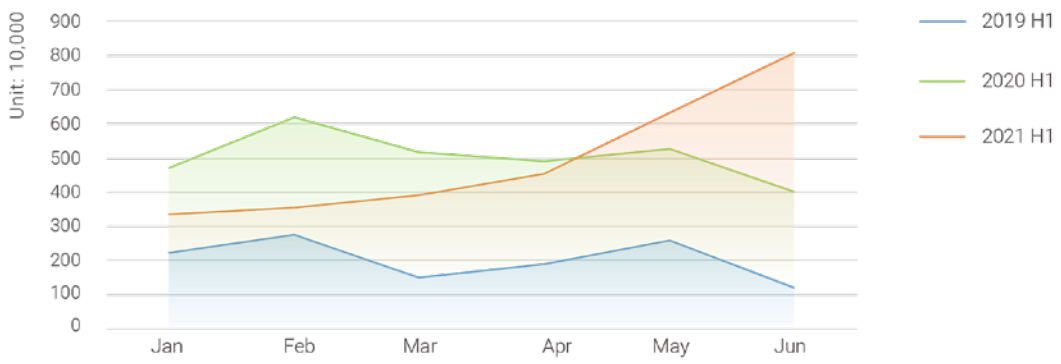
API Attack Overview and Trends in H1 2021

- In H1 2021, the CDNetworks security platform monitored and blocked 4.253 billion attacks against application programming interface (API) services. This figure was double the number for the same period in 2020, indicating a significant rise in API attacks.
- The concentration of attack methods against APIs decreased due to diversification in attack methods.
- The majority of API attacks was concentrated in the software-information services and finance industries, which accounted for 41.62% and 28.41% of attacks, respectively.

DDoS Attacks

Number of DDoS Attack Incidents Continue to Rise in H1 2021

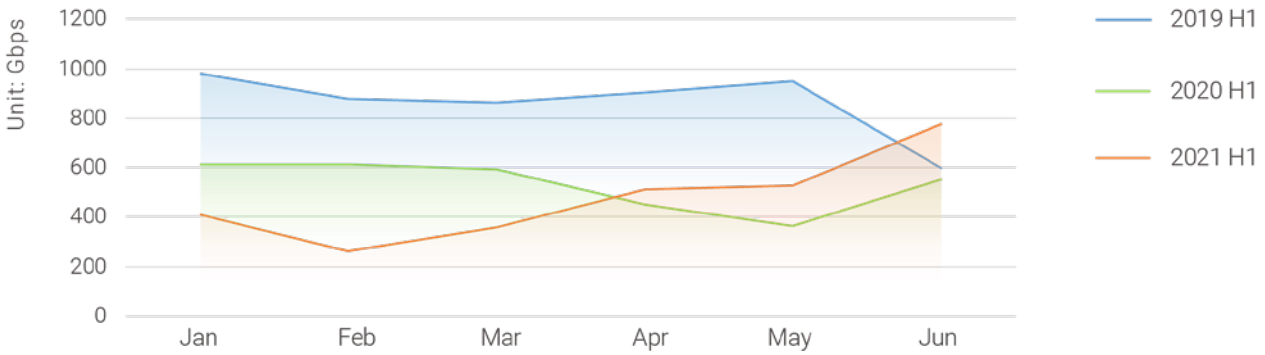
In H1 2021, the number of DDoS attacks detected by the CDNetworks security platform was consistent with the same period in 2020, albeit with a slight decrease of 1.63%. Based on the monthly trend, the number of attacks showed sustained growth in the first half of 2021, with the largest increase occurring in May and June.



DDoS Attack Event Trend of H1 2019/2020/2021

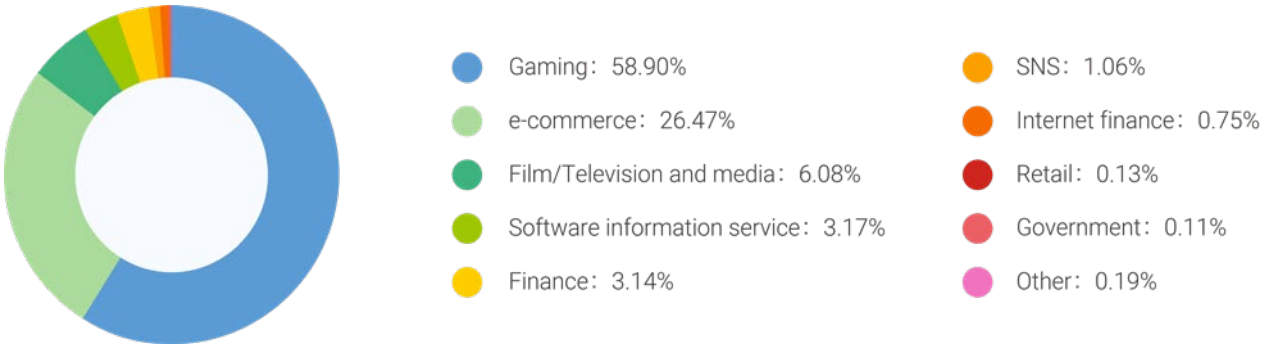
Email: info@cdnetworks.com www.cdnetworks.com

The peak level of DDoS attacks reached 774.58Gbps in June. This number was 26.62% higher than the peak of 611.73Gpbs reached in the first half of 2020, but lower than the 982.47Gpbs reported in the first half of 2019. Unlike 2019 and 2020, when DDoS attacks peaked in January, the increase in monthly DDoS attacks for 2021 began in February and peaked in June.



Monthly Distribution of DDoS Attack of H1 2019/2020/2021

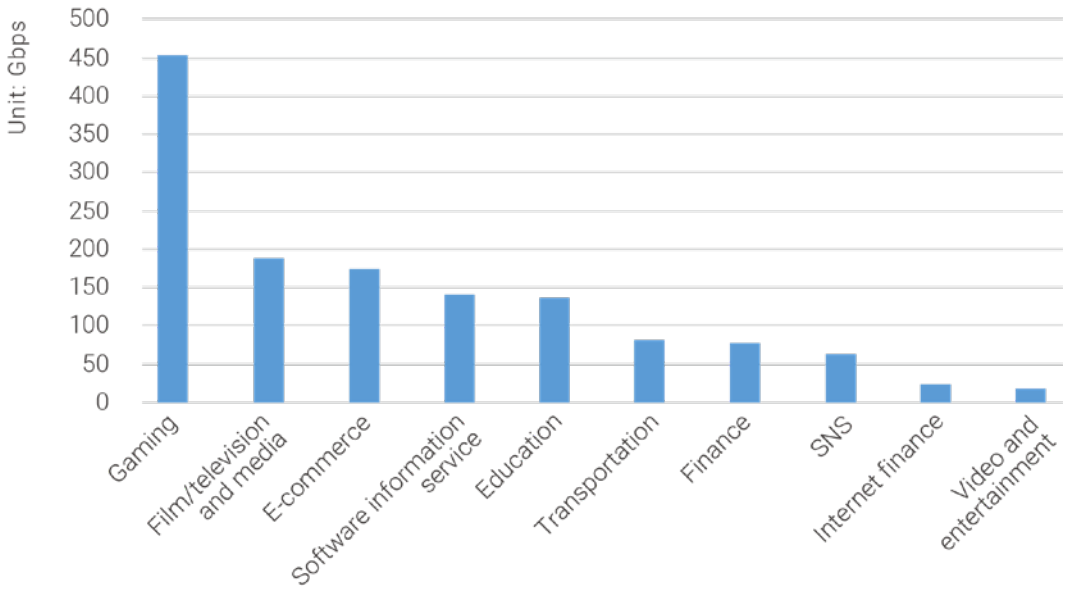
More than 80% of DDoS attacks are concentrated in the gaming and e-commerce industries



Industry Distribution of DDoS Attack of H1 2021

Gaming was the number one industry prone to DDoS attacks in H1 2021. When it comes down to numbers, DDoS accounted for 58.90% of all attacks against the gaming industry, a figure that vastly surpassed attacks against all other industries. E-commerce took second place with 26.47%. Collectively, DDoS accounted for 85% of all attacks against both industries combined. Film/television and media information came in third at 6.08%, while software-information services came in fourth at 3.17%.

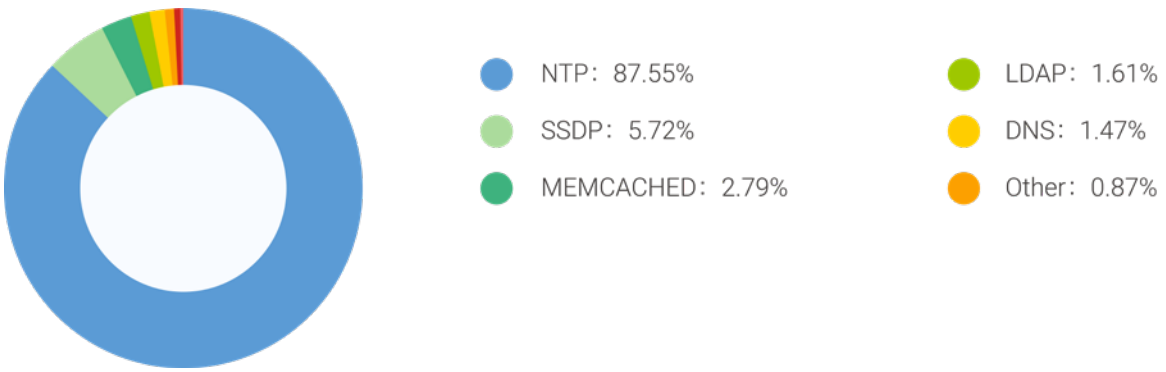
Email: info@cdnetworks.com www.cdnetworks.com



Top 10 Industries of DDoS Attack Peaks for H1 2021

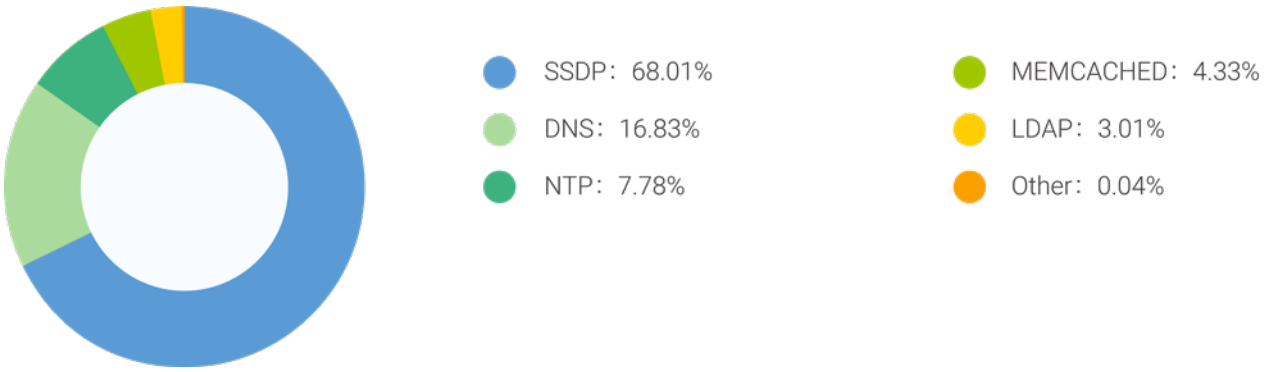
Statistics show that the top four industries targeted for DDoS hackers were gaming, film/television and media information, e-commerce, and software-information services, with peak attacks against the gaming industry surpassing 450Gbps. The number of attacks and the industry distribution of attack peaks clearly reflect an upward trend in industry-specific attack behavior.

NTP Reflection Amplification Attacks Leading the Trend



Distribution of Reflection Amplification Attack Protocol in H1 2021

Email: info@cdnetworks.com www.cdnetworks.com



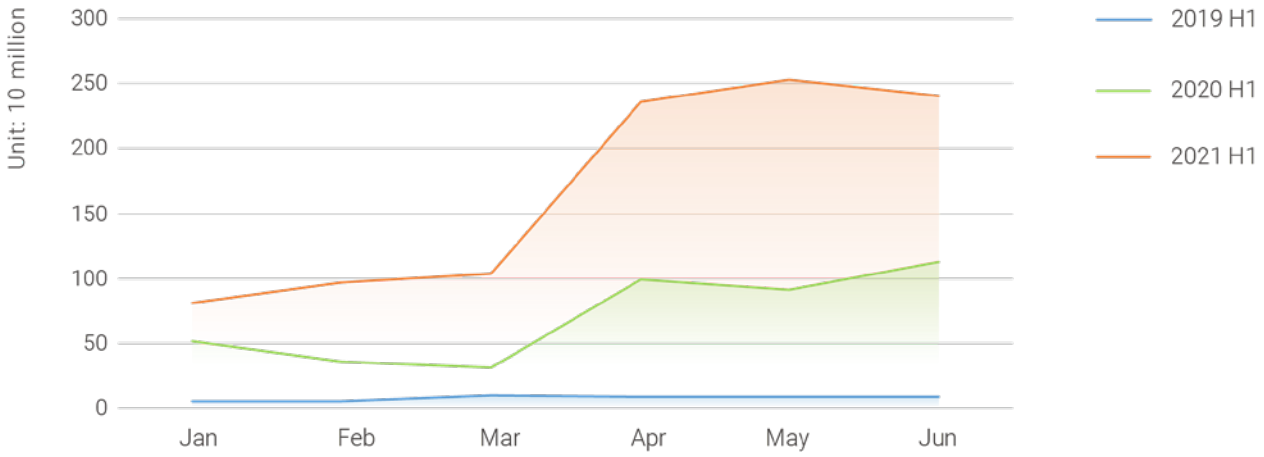
Distribution of Reflection Amplification Attack Protocol in H1 2020

Reflection-amplification attacks remain one of the most common DDoS attacks among cyber-criminals. In the first half of 2021, the mainstream protocol used with reflection-amplification attacks experienced a major reshuffle when NTP reflection-amplification attacks surpassed simple service discovery protocol (SSDP) attacks, which had been the dominant attack type in previous years. The proportion of NTP attacks versus SSDP attacks was an astonishingly high 87.55%, an increase from 7.78% for the same period last year. From these statistics, it is evident that the NTP protocol remains a popular tool of cyber-attackers, and that there are large numbers of vulnerably misconfigured NTP servers that remain exposed for attack on the public network. As proof of this trend, the proportion of SSDP attacks plummeted from 68.01% to 5.72%.

Web Application Attacks

Number of Web application attacks in the first half of the year has exceeded that the entire of 2020

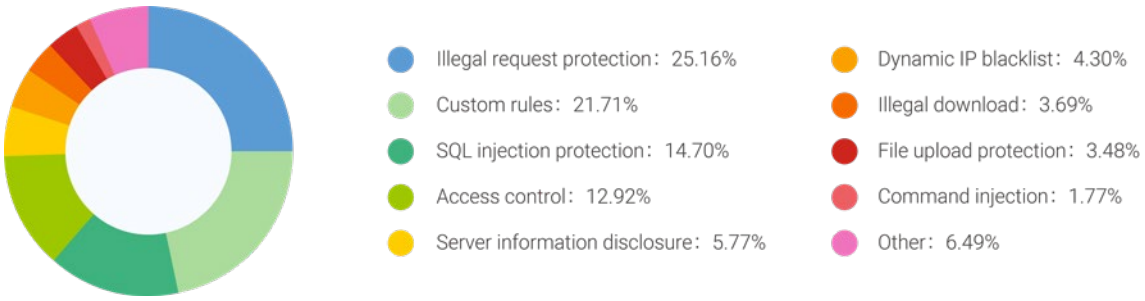
In H1 2021, the CDNetworks security platform monitored and blocked 10.113 billion Web application attacks. This figure exceeded the number of attacks for all of 2020 and showed an increase of 139.39% over the same period last year. This upsurge indicates that threats originating from Web application attacks continue to rise.



Web Attack Trend of H1 2019/2020/2021

Diversification of Web attack methods

According to the Web attack protection system powered by the CDNetworks platform, there are different ways to observe and deal with different attack methods.



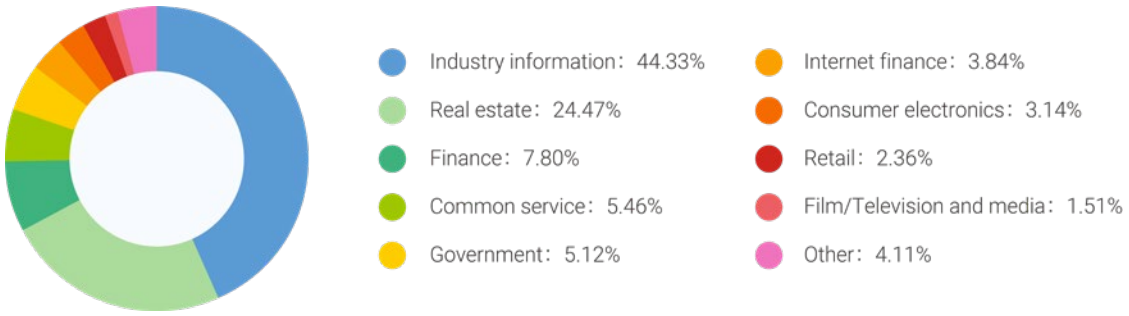
Web Attack / Defense Measure Distribution of H1 2021

As the figure above shows, the offensive and defensive ways of protecting against Web application attacks maintained a relatively scattered distribution. The top three methods are illegal request protection (25.16%), custom rules (21.71%), and SQL injection protection (14.70%). Compared with previous years, only SQL injection protection remained a preferred choice by users, while brute-force cracking protection fell out of the top 3 choices and accounted for only 0.53% of protection methods.

It is worth noting that the proportion of custom rules is much higher than before. This indicates that the use of custom rules based on business conditions and specific attack scenarios is a very effective policy against Web attacks.

As traffic from automated scanners continues to increase, the CDNetworks security platform identifies vulnerability scanners using feature analysis, behavior pattern, artificial intelligence (AI) model detection, threat intelligence, and other state-of-the-art capabilities. These resources directly filter most scanner attacks through access control (12.92%) and dynamic IP blacklist (4.30%), effectively reducing the probability of targeted attacks on specific websites while, at the same time, reducing the load imposed by automatic scanners on websites.

Software information services suffered more than 4 billion attacks



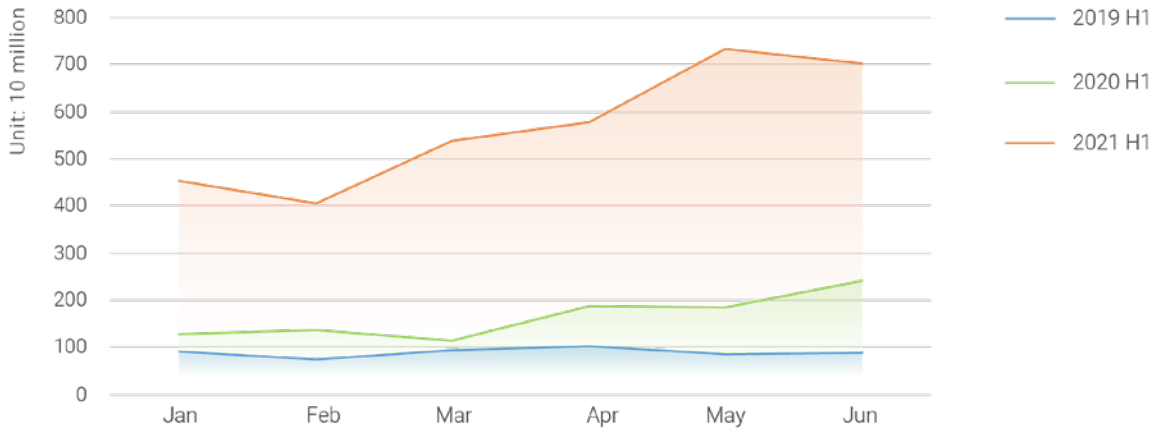
Industry Distribution of Web Application Attack in H1 2021

According to the data of H1 2021, the software-information service and real estate industry have become the industries with the most Web attacks. The two industries accounted for nearly 70% of Web application attacks in the first half of 2021, which totaled nearly 7 billion attacks. Finance (7.80%), common services (5.46%), and government agencies (5.12%) ranked third to fifth, respectively.

Email: info@cdnetworks.com www.cdnetworks.com

Bot Attacks

Malicious Bot Surged 3.29 times

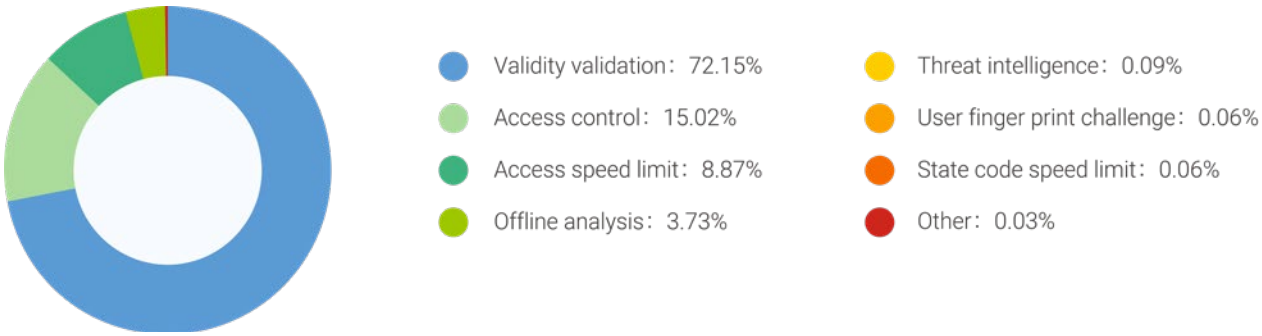


Malicious Crawler Attack Trend of H1 2019/2020/2021

In the H1 2021, the CDNetworks security platform monitored and blocked more than 34.147 billion malicious bot attacks. This number corresponds to an average of 2183.52 attacks per second, which is close to the total amount of 2020, 3.29 times that of the same period in 2020, and 6.34 times that of the same period in 2019. The trend has been doubling for consecutive years, making the security threat increasingly prominent.

Validity verification effectively blocks more than 70% of attacks

The CDNetworks platform integrates with a variety of protection algorithms to establish a protection system for malicious bot attacks. The trend of such attacks and commensurate protection results can be evaluated by examining online attack and defense data.

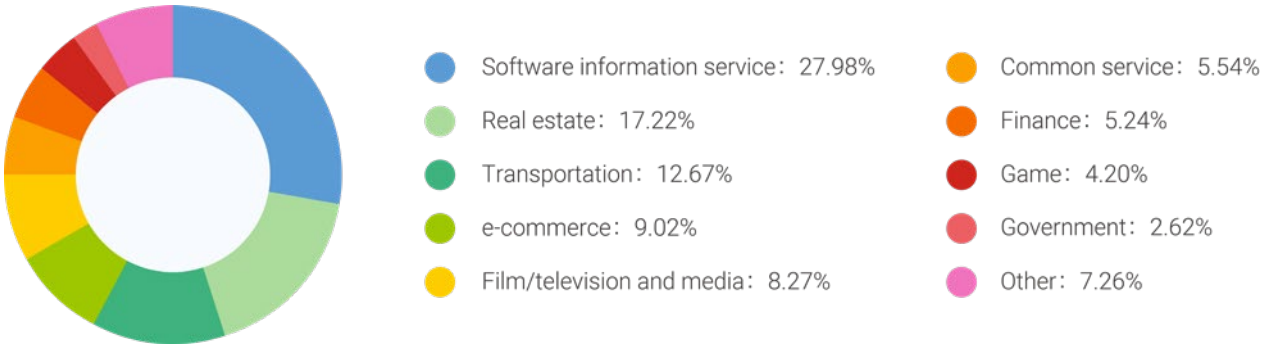


Malicious Crawler Attack / Defense Measure Distribution of H1 2021

Attack and defense data in the first half of 2021 shows that malicious bot protection methods that verify the validity of clients and their requests continue to be the most effective way of dealing with malicious bots, filtering more than 70% of attacks.

Furthermore, access control (15.02%), access speed limit (8.87%), and other means have also demonstrated significant protection capabilities.

Malicious bot attacks are scattered in the industries



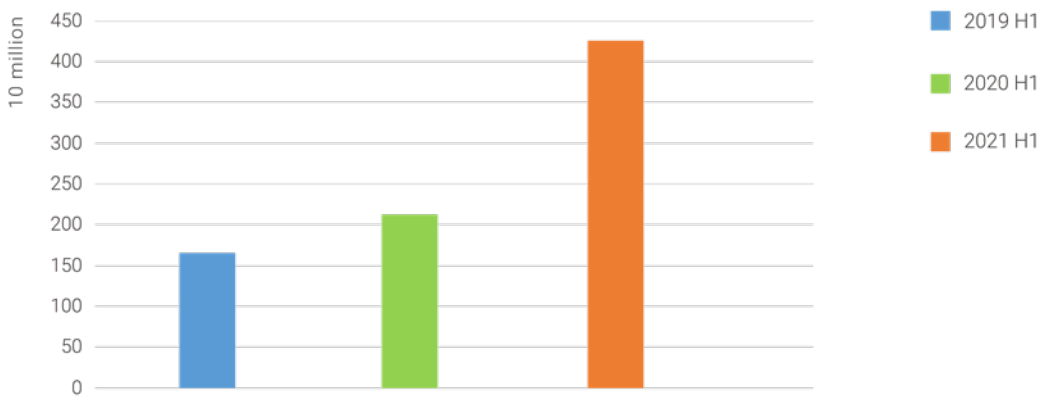
Industry Distribution of Malicious Crawler Attack in H1 2021

Among industries prone to malicious bot attacks, transportation rose from ninth place to third (2.08%) during the same period last year. This rise reflects that the transportation industry has gradually recovered from the negative impact of the COVID-19 pandemic and that bot attacks against ticket bookings have made a comeback.

API Attacks

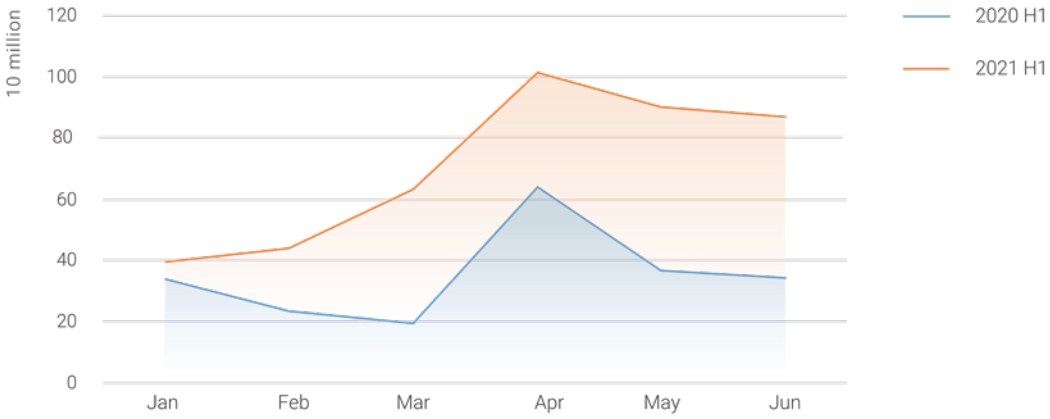
API Attacks Surged 2.01 times

Accompanied by the boom of the Internet, big data, and micro-service architecture, APIs experienced a significant growth. Although open APIs provide convenience when developing various Internet products and services, they also have become a lucrative target for cyber-criminals.



API Attacks of H1 2019/2020/2021

In H1 2021, the CDNetworks security platform monitored and blocked a total of 4.253 billion attacks against API services. This figure corresponds to an average of 271.96 attacks per second, an increase of 2.01 times that of the same period last year. The growth rate has increased with each year, indicating the disturbing security prospects faced by API services.

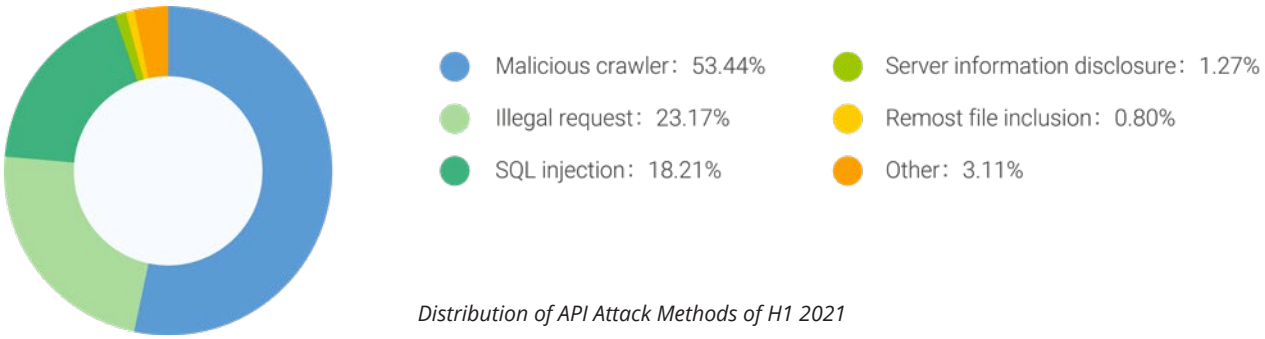


Monthly Distribution of API Business Attack in H1 2020 and H1 2021

In terms of monthly trends, API attacks in the first half of the year have been rising since January, reaching a small peak in April that is roughly similar to that of the same period in 2020.

Email: info@cdnetworks.com www.cdnetworks.com

Diversification of API attack methods

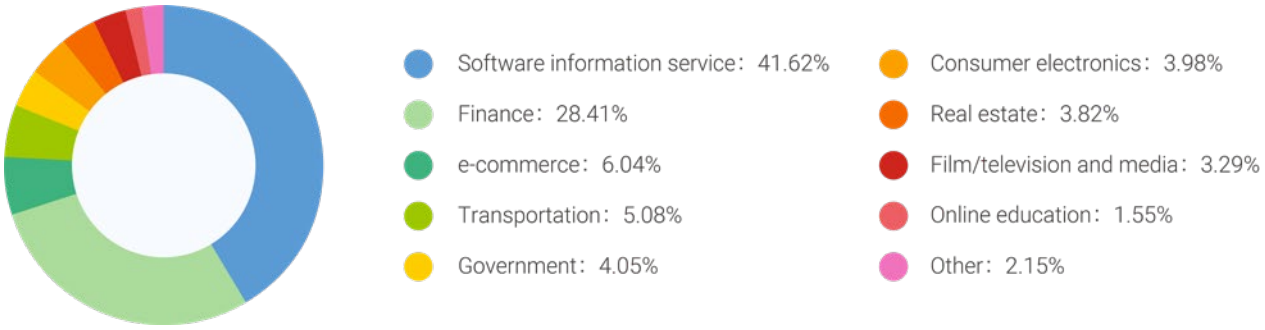


Distribution of API Attack Methods of H1 2021

When it comes to attacks against API services, malicious bots remain the most prominent attack method and are gaining momentum. In H1 2021, malicious bot attacks against API data accounted for 53.44% of the total number of attacks, down significantly from 74.82% in the same period last year.

Second place and third place were occupied by illegal request attacks (23.17%) and SQL injection attacks (18.21%), which increased significantly compared with 5.97% and 10.94% in the same period last year. Centralized distribution of attack methods has decreased, which shows that the attack methods against APIs are gradually trending toward diversified development rather than relying on a single attack method.

The software information service and the financial industry have become the hardest hit areas of API attacks



Industry Distribution of API Attack in H1 2021

In H1 2021, the software-information service industry has suffered the most API attacks, accounting for 41.62% of the total attack volume. The financial sector ranked second with 28.41%.

The proportion of API attacks suffered by these two industries reached nearly 70%, indicating the extremely grim situation in these two industries.

Government agencies that attracted the vast majority of API attacks in previous years experienced a sharp decline in attacks in the first half of 2021 to approximately 10% that of the same period last year, down from 60.94% in the first half of 2020 to 4.05 percent.

Trends and Future

Data shown in the CDNetworks security report clearly shows that attacks continue to morph, and that offensive and defensive scenarios have undergone changes to address this vulnerability evolution compared to the same period in 2019 and 2020. The security report also shows that enterprises faced with security threats to their businesses respond by constantly adjusting to the dynamics of the situation. As a result, protection concepts and strategies must keep pace with the changes in attacks in order to implement effective response.

Compared with network layer DDoS attack, application-layer attacks and business data are increasingly favored by attackers

As indicated in the CDNetworks security report, the number of Web attacks, malicious bot attacks, and API attacks have all increased exponentially. On the other hand, the growth of DDoS attacks in the network layer tended to stagnate, which shows that the attack methods aimed at the application layer and customer business are increasingly favored by cyber-criminals and are increasing proportionally. The purpose of attacks is no longer simply to render a business inaccessible, but rather to focus directly on business-related data. Once an attack succeeds, it will not only affect the business itself, but will provide monetary rewards to hackers who sell the stolen data on the dark web. Moreover, the hacked server will become a resource for future data mining and act as a foothold to infiltrate other targets within the exploited enterprise, creating more benefits for attackers and causing more long-term damage to the victimized enterprise.
When it comes to attack methods, cyberattacks have improved their ability to automate and conceal. It has become commonplace for hackers to use AI to simulate human behavior in order to bypass conventional security policies, thereby making it more difficult to detect intrusions and protect valuable assets.

Comprehensive cloud security solutions will become more popular.

To protect against cybercriminals, enterprises are forced to stay up to date with the ever-changing threat landscape. Since no individual security measure can guarantee protection against every attack, combining several layers of security, from the network layer to the application layer, has proven to be highly effective when fending off attackers. Attacks missed by a defensive measure at one layer are caught by another defensive measure at the same layer or at succeeding layers. In this way, a layered approach builds a security fortress that's intercepts sophisticated cyberthreats before they can reach core business applications and data.

Email: info@cdnetworks.com www.cdnetworks.com