CDNetworks

State of the Web Security 2020

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

Table of Content

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

Preface

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 for clients. The reports analyze volume, forms, industries, and other critical indicators from various perspectives. From this analysis, we can assess the impact that the Coronavirus disease (COVID-19) has on cyber-attacks.

This report describes the impact of the COVID-19 pandemic on cyber-attacks. The information in this report is organized according to the following four attack vectors:

- DDoS
- Web application attacks
- Bot attacks
- API attacks

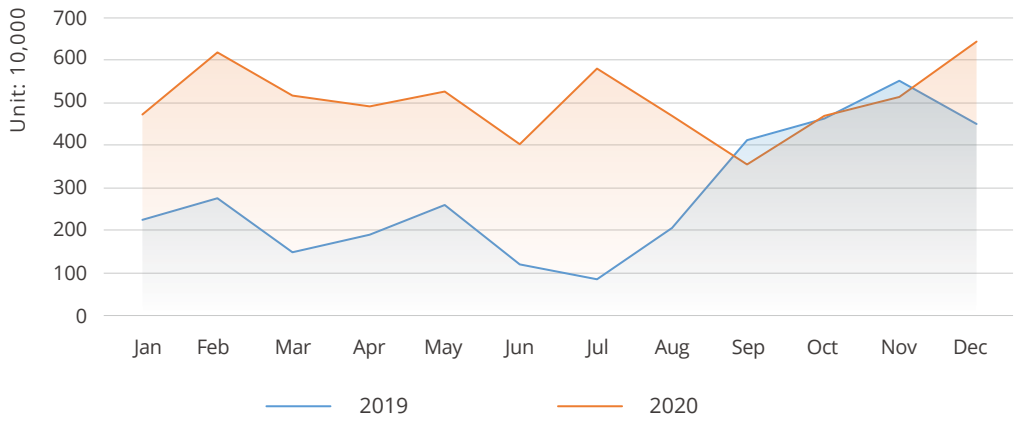
Email: info@cdnetworks.com www.cdnetworks.com

DDoS Attacks

Distributed Denial of Service (DDoS) attacks attempt to slow down or take down sites and businesses. To achieve this goal, DDoS attacks generate excessive bogus traffic that overwhelms servers with spurious packets, thereby preventing legitimate traffic from passing through.
During 2020, the CDNetworks cloud security platform reported an increase in the number of DDoS incidents. Compared with 2019, the DDoS attacks we monitored and blocked rose by over 78.79%, marking a significant and disturbing growth rate. The size of these DDoS attacks, however, declined noticeably.

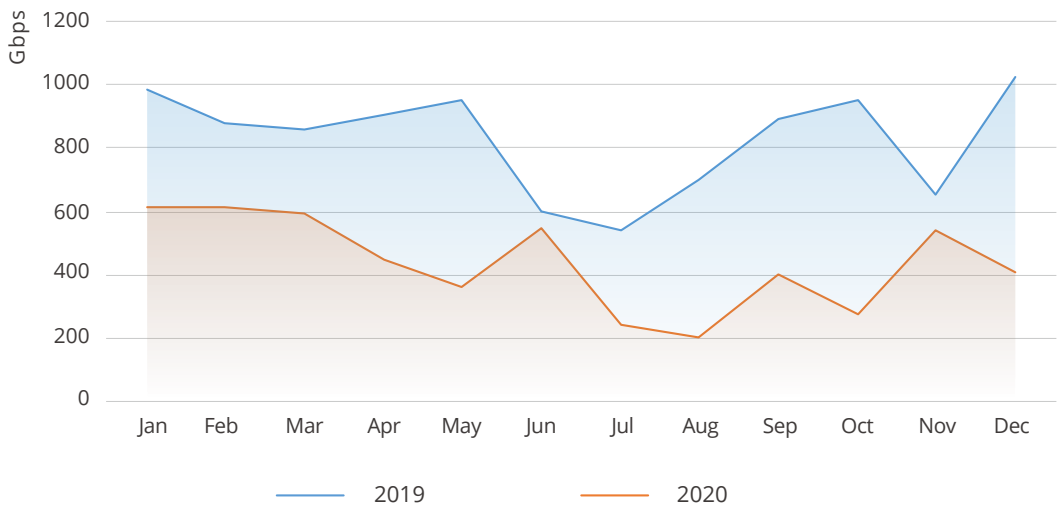
- The retail and gaming industries remain the main target of DDoS attacks. They also ranked among the top 3 industries in terms of the number and peak size of DDoS attacks.
- Following closely is the online education industry. With COVID-19 forcing places of learning to migrate from on-premise teaching to virtual environments, the exponential growth of the online education industry has gained the attention of hackers. Today, online education has become the third-largest industry when it comes to the peak size of DDoS attacks.

Number of DDoS Attack Incidents Continue to Rise Compared with 2019



Annual DDos Attack Trend of 2019 and 2020

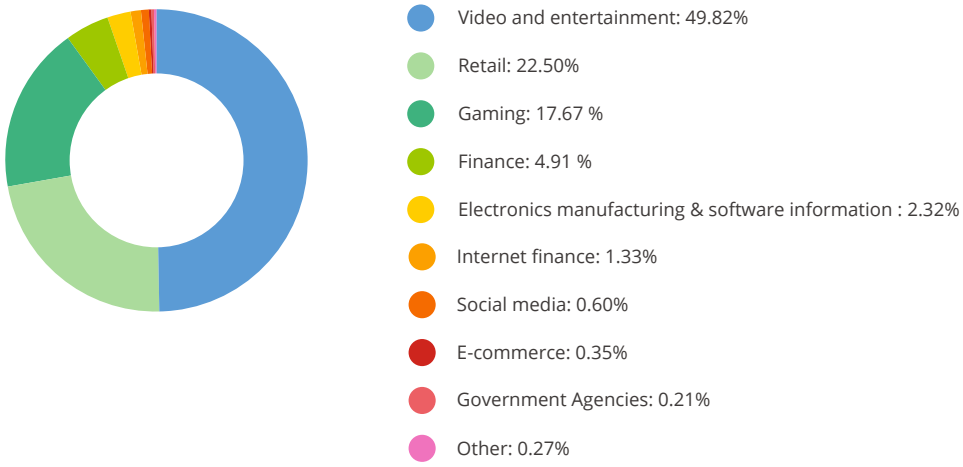
Email: info@cdnetworks.com www.cdnetworks.com



Monthly Distribution of Peak DDoS Attacks in 2019 and 2020

By comparison, peak of DDoS attacks fell in 2020, with the attack peak for each month coming in lower than in 2019.

Video, Retail, and Gaming Suffered the Most DDoS Attacks



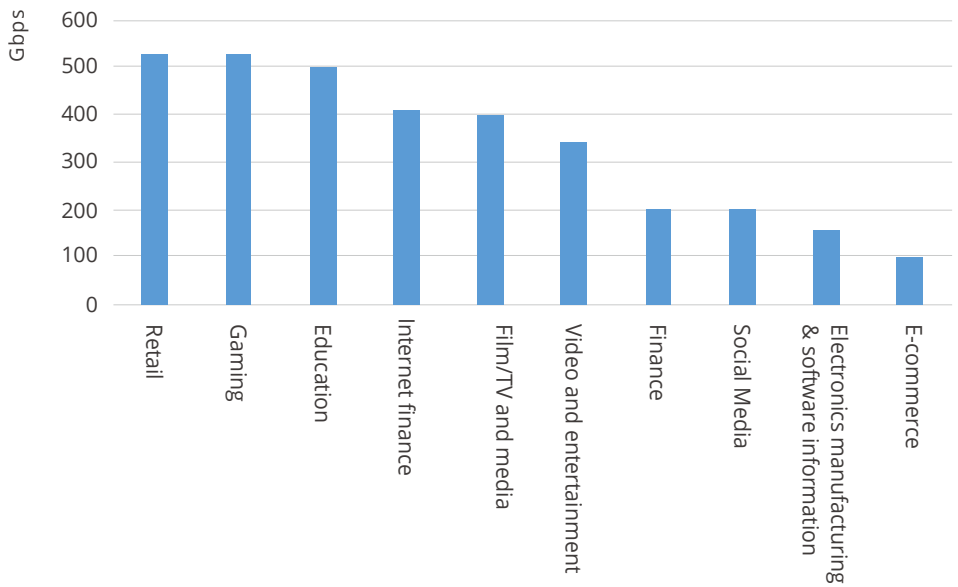
Industry Distribution of DDoS Attack Events in 2020

According to statistics that monitor DDoS attacks across industries, the top three victimized industries are video and entertainment (49.82%), retail (22.50%), and gaming (17.67%). Collectively, these industries account for nearly 90% of all DDoS attacks. The video and entertainment industries in particular accounted for about half of all DDoS attacks in 2020.

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

The COVID-19 pandemic has led video and entertainment industries to adopt cloud-based offerings. As these offerings gained traction, their popularity was quickly followed by cyber-criminals intent on stealing sensitive data for fraudulent purposes.

DDoS Attacks in Various Industries Experienced Significant Impact from the Pandemic



Top 10 Industries by DDoS Attack Peaks in 2020

The DDoS peak for the retail, gaming, and education industries reached its high point in H1, 2020, where such attacks surpassed 500 Gbps per second.

Hackers Often Use IoT Devices to Initiate Reflection Amplification Attacks

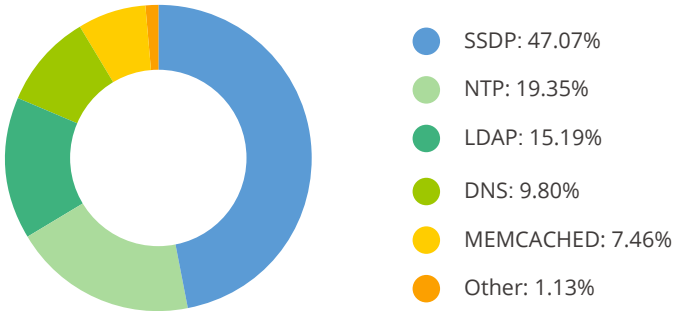
A reflection attack is a type of DDoS attack that uses the User Datagram Protocol (UDP). Instead of attacking a target directly, cyber-criminals use public servers to spoof the victim's IP address in order to send a request for information to the victim using UDP. The servers assume that the request came from the victim, answer the request, and send responses to the victim's IP address. All of these responses collect at the victim servers, clogging the servers' Internet connectivity.

This type of attack is a favorite of cyber-criminals because it is relatively inexpensive to initiate, extremely crippling to its victims, and difficult to trace back to its source. Based on data collected by the CDNetworks security platform, reflection amplification attacks remain one of the commonly used attack methods, with a significant number of reflection amplification attack requests detected throughout the year.

Reflection attacks are commonly used for IoT smart devices, such as sensing home routers, webcams, printers, smart appliances and other IoT devices.

Extrapolating reflection amplification attack request data detected by the CDNetworks security platform in 2020 shows that the Simple Service Discovery Protocol (SSDP) protocol is involved in nearly half (47.07%) of all DDoS reflection amplification attacks, as shown in the following figure. By exploiting the vulnerabilities of the SSDP protocol, either the communication channel of the victimized server will be clogged with garbage, or the server will drown as it tries to process a blitz of SSDP responses.

Given the rapid growth and adoption of IoT and smart devices, DDoS reflection amplification attacks against smart devices will become even more widespread.



Distribution of Reflection Amplification Attack Protocol in 2020

Compared with H1, 2020, the clearly emerging trend in reflection amplification attacks is the Lightweight Directory Access Protocol (LDAP) reflection amplification attack (15.19%). The number of LDAP attack in H2 increased nearly 30 times compared with H1, 2020.

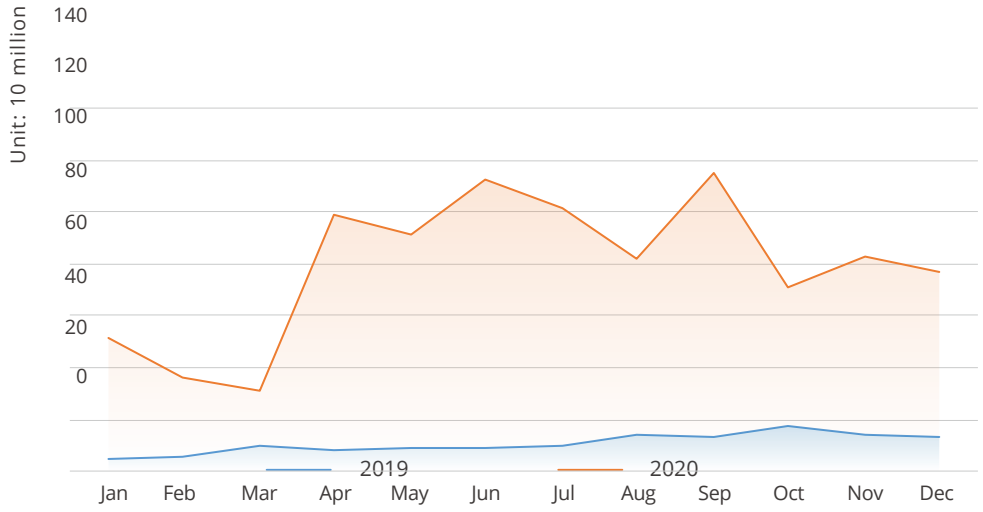
Web Application Attacks

In 2020, the CDNetworks security platform monitored and intercepted 9.524 billion web-application attacks, a number that is 7.4 times higher than in 2019.

- SQL injection and brute force, which have long been ranked as the top two attack methods, remain the major web-application attacks.
- Government agencies are the main targets of web application attacks, and the security outlook for the future looks grim.

Web Application Attacks Surged 7.4 Times

In 2020, the CDNetworks security platform monitored and intercepted 9.524 billion Web application attacks, 7.4 times more than in 2019.

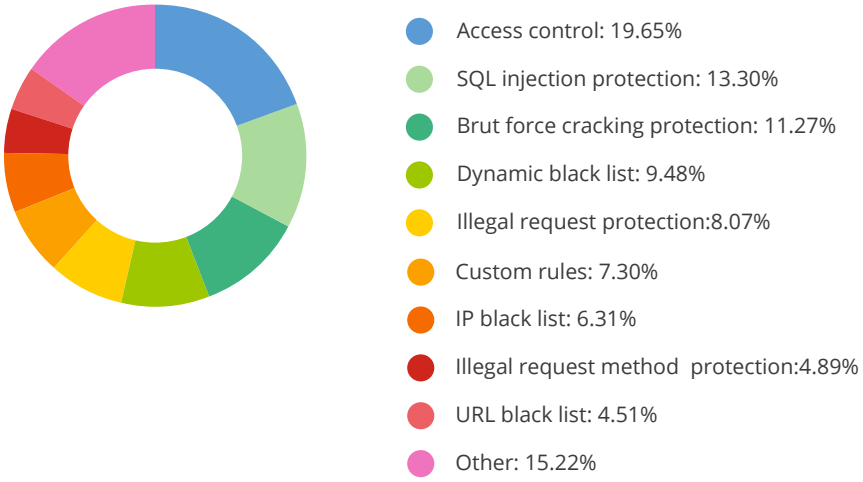


Web Application Attack Overview and Trends in 2019 and 2020

SQL Injection and Brute Force Attacks

The Web Application Firewall (WAF) powered by the CDNetworks security platform identified various techniques used to limit or prevent cyber-attacks. There are different ways to prevent different attacks, which can reflect the distribution of Web application attacks.

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

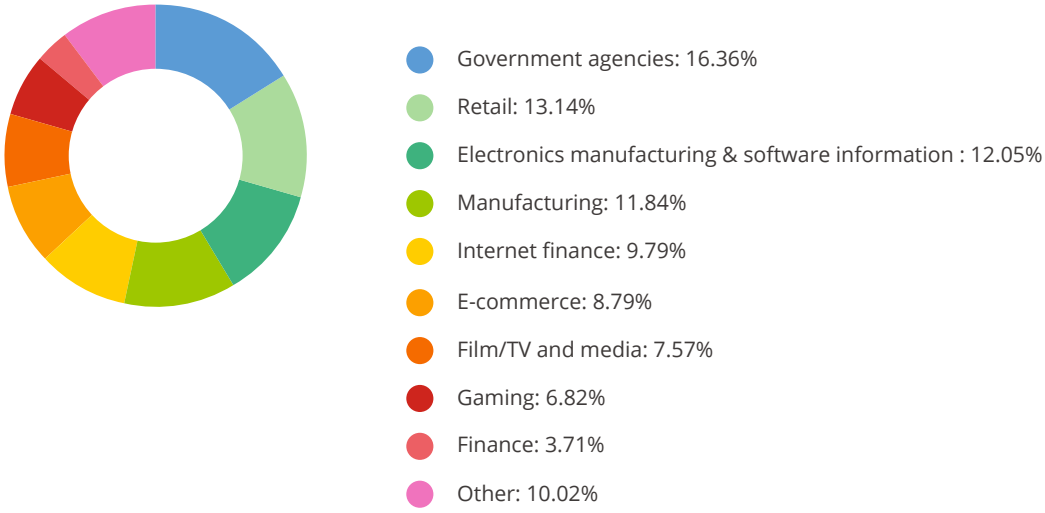


Web Attack and Protection Distribution in 2020

Access Control exploits (19.65%) became the Top 1 attack method in 2020. Not far behind were SQL injection protection (13.30%) and brute force cracking protection (11.27%) techniques.

Web Application Attacks are Prevalent in Various Industries

Statistics reported by the CDNetworks security platform show that web attacks across industries is relatively uniform. The biggest change in 2020 occurred with government agencies, whose ranking catapulted from second place to first on the list of web-application attacks compared to data collected in 2019.



Distribution of Web Attack by Industry in 2020

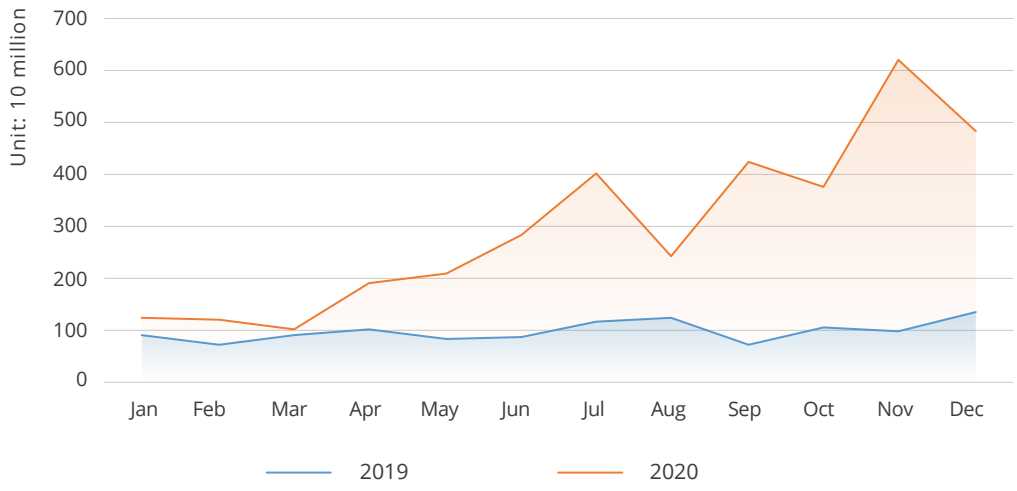
Email: info@cdnetworks.com www.cdnetworks.com

Bot Attacks

Bot attacks are automated requests that abuse or exploit site resources by scraping data, guessing passwords, stealing credit-card numbers, generating fake accounts, and more. Bot attacks typically focus on vulnerable industries, especially gaming, e-commerce, media and entertainment, where the value of the data and other resources can be extracted and abused.

In 2020, the CDNetworks security platform monitored and blocked a total of 35.854 billion bot attacks. The average number of occurrences was a staggering 1134 attacks per second, three times the number of attacks in 2019.

Bot Attacks Nearly Tripled in 2020

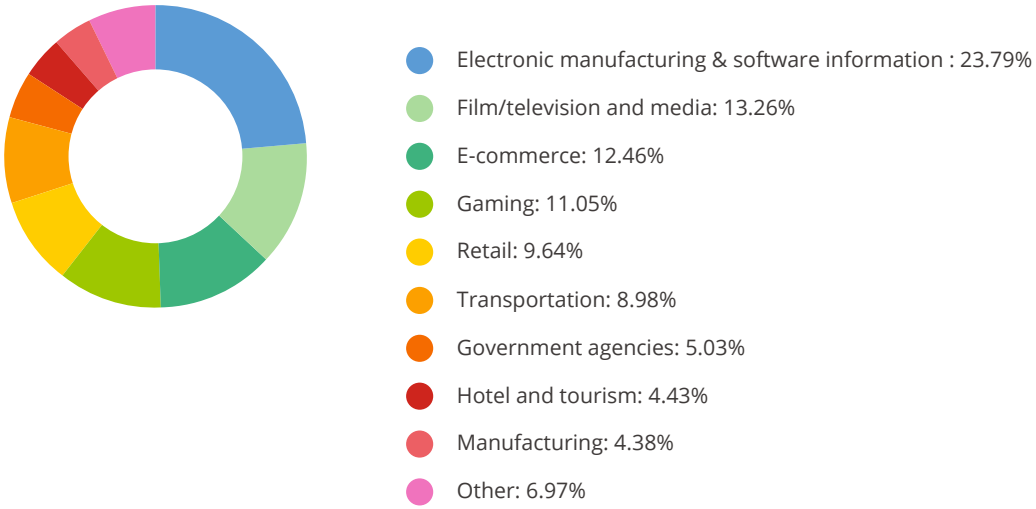


Trend of Malicious Crawler Attacks in 2019 and 2020

Tourism Saw a Decline in Bot Attacks

Continuing the trend in H1, 2020, the electronic manufacturing and software information services industry led the pack as the industry with the most serious malicious bot attacks (23.87%). Following behind were film and television media (13.26%), e-commerce (12.46%), gaming (11.05%), retail (9.64%), and transportation (8.98%).

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



Distribution of Malicious Crawler Attack by Industry in 2020

Bot attacks are closely related to economic interests: the more prosperous an industry, the more frequent the bot attacks against that industry. The intensity of bot attacks also depends on the value of the sensitive information collected by a target industry and that industry's anti-bot capabilities.

API Attacks

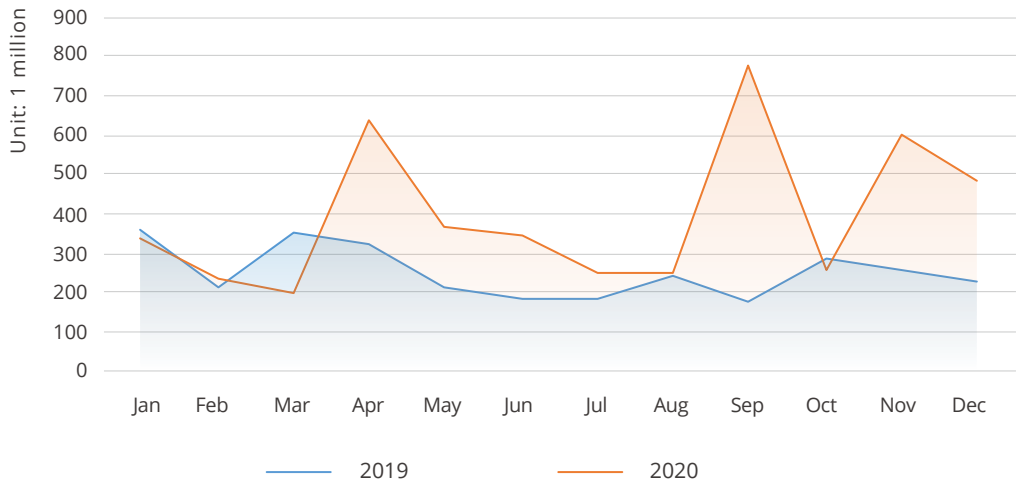
In 2020, the CDNetworks security platform monitored and blocked a total of 4.732 billion attacks against API services, 1.56 times as many as in 2019, showing a significant increase.

- Malicious bots were the main attack method in API attacks, accounting for 76.39% of the total attacks. This figure is close to the 77.85% registered in 2019. Following behind malicious bots are illegal requests, SQL injection, and brute force attacks. Compared to 2019, the proportion of SQL injection attacks in 2020 increased significantly, while brute force attacks declined.
- More than half of the API attacks were directed against the government (32.79%) and e-commerce industries (21.16%).

4.7 Billion API Attacks Recorded in 2020, an 56% Increase

Open APIs are publicly available application programming interface that provides developers with programmatic access to a proprietary software application or web service. Typically, when an API is exposed to the public, it provides direct access to large amounts of data while bypassing browser precautions, making them susceptible to DDoS attacks.

In 2020, the CDNetworks security platform monitored and intercepted 4.732 billion attacks against API services, a 56.03% increase over the same period in 2019. This significant increase exposed the vulnerabilities of API services to being hacked.



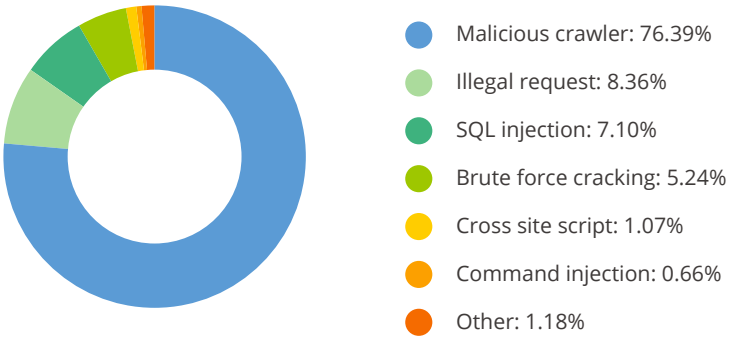
Trend of API Attacks in 2019 and 2020

Malicious Bots Remain the Major Attack Type

A bot is a small piece of software that automates web requests. Bots conduct certain tasks that had been performed by humans. Because they are automated, bots operate much faster than humans.

A bot can be used in helpful or malicious ways. A malicious bot is used by cyber criminals to steal data, break into user accounts, submit junk data via online forms, infect computers with malware, and perform other harmful activities. In 2020, malicious bots (76.39%) accounted for the overwhelming majority of attacks on API services, with a proportion roughly the same as in 2019.

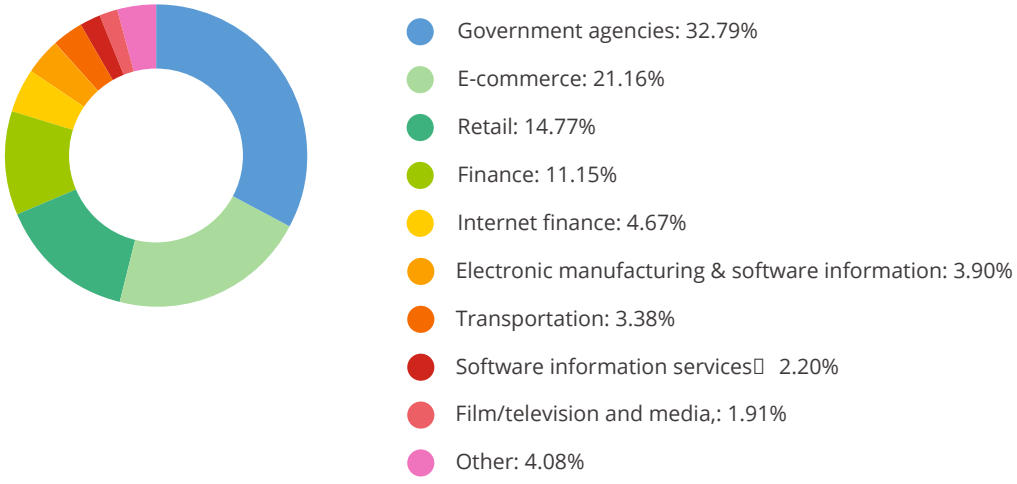
Email: info@cdnetworks.com www.cdnetworks.com



Trend of API Attacks in 2019 and 2020

Lagging behind malicious bots were illegal request (8.36%) and SQL injection (7.10%) attacks. Brute force attacks fell from second place (2019) to fourth, with the proportion also dropping from 8.76% to 5.24%.

Over 50% of Attacks Targeted Government Agencies and E-commerce



Distribution of API Attack by Industry in 2020

In 2020, government agencies continued to encounter the majority (32.79%) of API attacks. E-commerce (21.16%) moved into second place — a rise that can be directly tied to changes in people's way of life during the COVID-19 pandemic. The transportation industry, which ranked second with nearly 30% in 2019, fell significantly in 2020, accounting for only 3.38% and dropping to seventh place due to COVID-19.

Trend and Future

Year after year, breaches continue to rise across all attack types and vectors. Data generated by the CDNetworks security platform shows an ominous trend where DDoS attacks have become amplified. Instead of single types of DDoS attacks, cyber-criminals are now integrating a combination of attack types into formidable threat. This means that targeted industries will be forced to contend with increasingly complex and virulent threats that leverage a combination of attack methods.

In the face of this menacing trend, standard current best practices are shifting away from solutions that focus on single attack types and moving toward comprehensive cloud security solutions that are scalable, easy to operate and manage, and provide comprehensive reporting content viewing, configuration adjustment, and distribution of security events in one portal system. This approach identifies and neutralizes attacks quickly to eliminate or minimize their impact.

Artificial Intelligence (AI) will also play a major role in cybersecurity. One reason AI has attracted interest, for enterprises and cyber-criminals alike, is because it can discover patterns in big data. Hackers can use machine learning to learn database rules and protection strategies of a target in order to detect vulnerabilities in a network or system. Cloud security vendors, on the other hand, can use AI to enforce automated policy learning, entity behavior analysis, attack source tracing, and security detection. Intelligent confrontation will be the battlefield for cloud security in the near future.

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