网宿科技
WANGSU.COM

2020

CHINA INTERNET SECURITY REPORT

Table of Content

Chapter I Overview

- The 2020 China Internet Security Report is jointly created by Wangsu and Digital World Consulting. The report analyses the quantity, type, source and industry distribution of various attacks.

- From the annual data, the outbreak of COVID-19 pandemic in 2020 led to significant impact on the trend of network attacks, and the dynamic trend of related data is consistent with the development of the epidemic.

1.1. DDoS Attack Overview and Trends in 2020

In 2020, the number of DDoS attacks monitored and intercepted by the Wangsu security platform increased by 78.79% compared with the same period last year, but the scale of the attacks have decreased, and the annual attack trend matched the development of the epidemic.

- Retail and the gaming industry remain the main targets of DDoS attacks, they ranked among the top 3 industries in terms of the number of attacks and the peak value of attacks.
- Driven by the pandemic, the online education industry has ushered in explosive growth with online classes. This has also attracted the interest from illicit parties, and the online education industry has become the third industry with the highest peak of attack.
- The SSDP protocol associated with IoT and smart devices has become the most commonly used protocol for attackers to launch DDoS reflection amplification attacks.

1.2. Web Application Attack

- In 2020, the number of Web application attacks monitored and intercepted by the Wangsu security platform soared to 9.524 billion, 7.4 times that in 2019. Among them, the number of attacks in the first half of the year was nine times that of the same period last year.
- In terms of the attack methods, SQL injection and brute force cracking are still the major avenues of attack, and they have long been ranked the top two attack methods.
- Both the half year and annual data indicate that government agencies are the main targets of Web application attacks, and the security outlook appears grim.

1.3. Malicious Crawler Attack

- In 2020, the Wangsu security platform monitored and intercepted a total of 35.854 billion crawler attacks, with an average of 1134 attacks per second, three times the number of attacks in 2019.
- In terms of the distribution of attack sources, 90% of the traffic of malicious crawlers comes from within China, and the number of attacks from overseas decreased compared with the same period last year, mainly in South Korea, the United Kingdom, the United States and other countries.
- Among the domestic malicious crawler requests, Jiangsu, Zhejiang and Guangdong provinces are the most prominent sources.
- Electronic manufacturing and software information services are the industries most attacked by malicious crawlers, followed by film and television media information, e-commerce and games.

1.4. API Attack Overview and API Attack Overview and Trends in 2020

- In 2020, the Wangsu security platform monitored and intercepted a total of 4.732 billion attacks against API services, 1.56 times the number in the same period in 2019, showing a significant increase.
- Malicious crawler is the main attack method in API attacks, accounting for 76.39% of the total attacks, which is the same as that of 77.85% in 2019， followed by illegal requests, SQL injection and brute force cracking. Compared with the proportion of SQL injection in 2019, the proportion of SQL injection has increased significantly, while brute force cracking has declined.
- More than half of the API attacks are concentrated in the government and e-commerce industries, accounting for 32.79% and 21.16%, respectively.

1.5. Enterprise Host Security Enterprise Host Security Overview and Trends in 2020

- Among the host open ports, management ports such as port 22 and port 3389 are the main targets of hackers. According to the annual data, the two accounted for 46% of the attack volume.
- High-risk vulnerability attacks increasingly tend to take advantage of simple vulnerabilities, unauthorized access, remote code execution vulnerabilities, with increased degree of automation and tool integration.
- The security baseline test shows that the overall security awareness of enterprise users is still lacking, and only a small number of users will reinforce their non-compliance security items.
- Compared with 2019, the number of abnormal login IPs from within China increased significantly in 2020, which is related to global political trends and the government's tightening of the use of overseas IPs.

Chapter II
Interpretation of DDoS Attack Data

2.1. Number of DDoS Attack Events Continue to Rise While the Attack Peak Saw an Overall Decrease

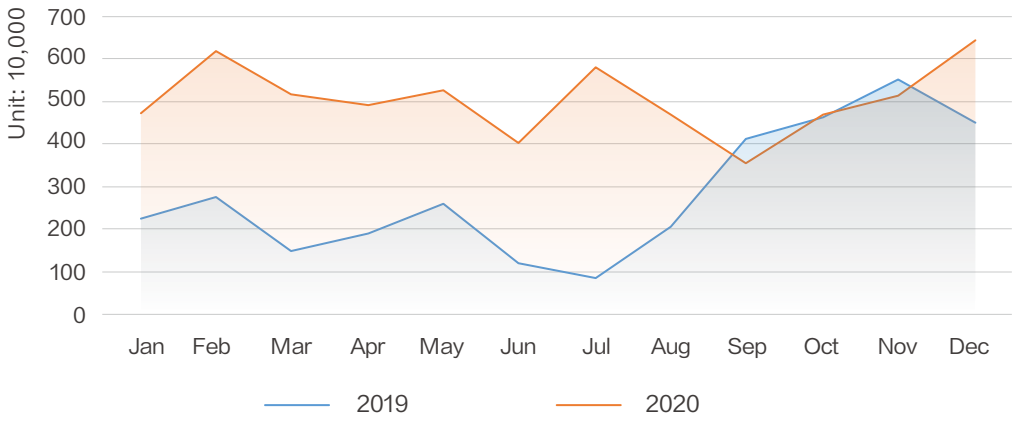

Figure 2-1 Annual DDos Attack Trend of 2019 and 2020

In 2020, the number of DDoS attacks detected by the Wangsu security platform maintained an increase compared with previous years, with an increase of 78.79% over the same period last year, an increase of 53% compared with 25.76% in 2019, and a marked increase in the growth rate.

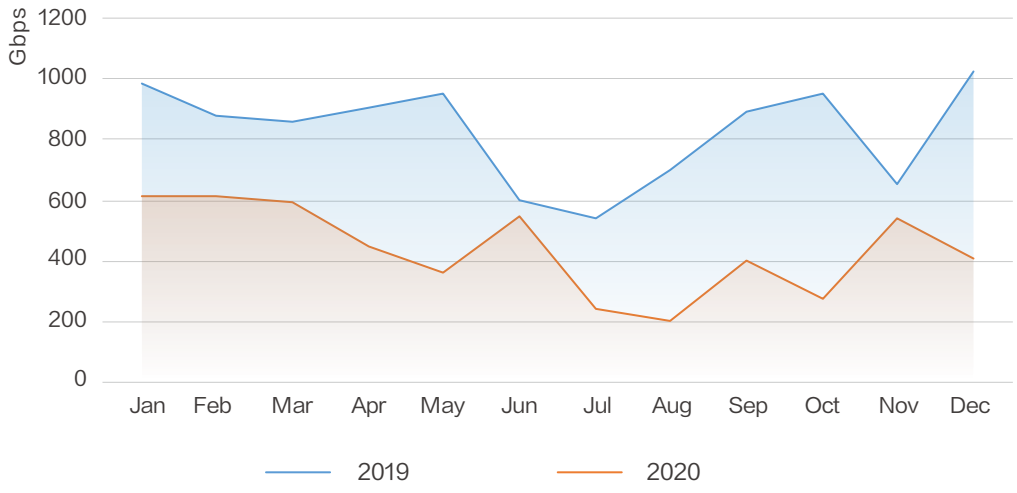

Figure 2-2 Monthly Distribution of Peak DDoS Attacks in 2019 and 2020

The scale of DDoS attacks declined in 2020, and the peak value of attacks in each month was lower than that in the same period last year.

There are two reasons behind the increase in number of DDoS attacks and the decrease in peak of attacks: on the one hand, due to the outbreak of the COVID-19 pandemic in the first half of 2020 and the continued spread of the virus overseas in the second half of 2020, the operations and production of global enterprises were affected, some "easy targets" were offline, thus the number of attack sources available to attackers decreased, resulting in a decrease in attack traffic.

On the other hand, in the first half of 2020, under the influence of COVID-19, online education and telecommuting saw rapid growth, and a large amount of capital poured in this sector. Many companies focused their IT investment on meeting the requirements of rapid business growth, and network security was unable to keep up with this growth. At the same time, the user traffic of business such as online education and telecommuting has taken up a lot of bandwidth resources, which are highly vulnerable to low-intensity attacks, thus attackers no longer need to launch high-traffic attacks to achieve their goals.

2.2. 90% of DDoS Attacks Focused on Video Entertainment, Retail, and the Gaming Industry

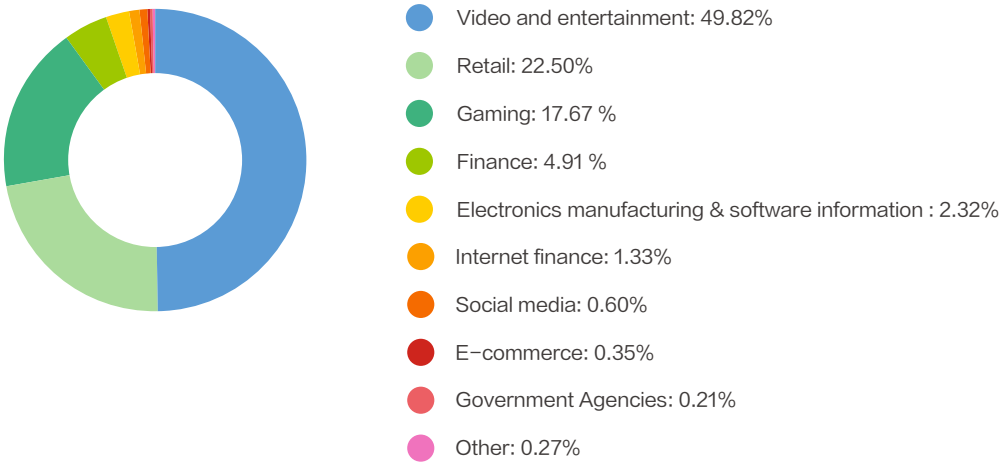

Figure 2-3 Industry Distribution of DDoS Attack Events in 2020

According to statistics on the distribution of DDoS attacks in various industries, the top three are video and entertainment (49.82%), retail (22.50%) and gaming (17.67%) accounted for nearly 90% of the attacks. The retail and gaming industries have also been the hardest hit by DDoS attacks in previous years, while video and entertainment attracted about half of the DDoS attacks in 2020. Due to the pandemic, offline activities are limited, various cloud entertainment demand of users have taken a higher priority for many companies, video and entertainment sectors are less affected, and even ushered in favorable development opportunities.

2.3. Significant impact of the pandemic on DDoS attack peaks for various industries

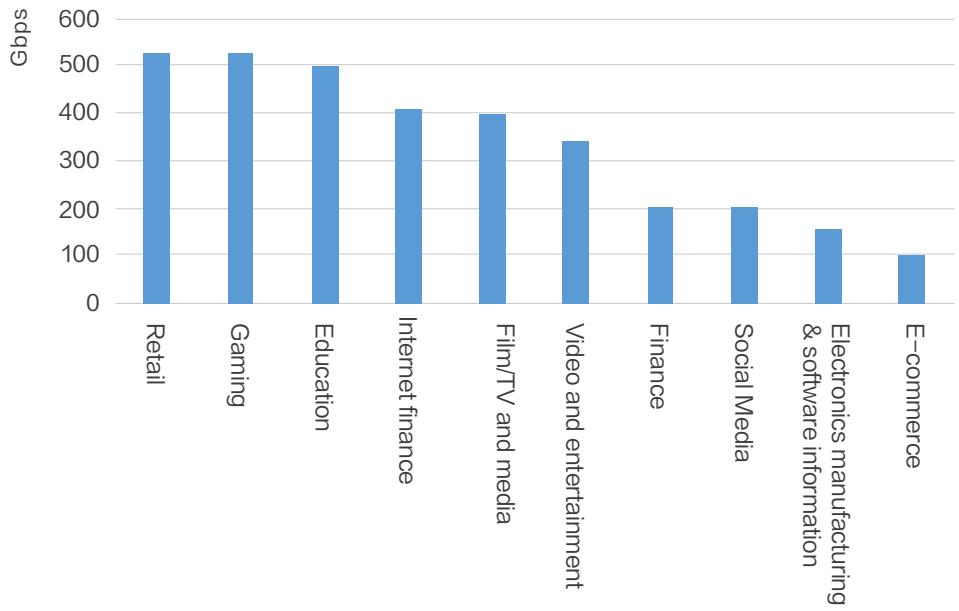

Figure 2-4 Top 10 Industries by DDoS Attack Peaks in 2020

From the peak of attacks on various industries, the retail, gaming and education industries all peaked at more than 7500 Gbps, and all occurred in the first half of the year.

In 2020, affected by COVID, the online education industry ushered in explosive growth, followed by DDoS attacks seeking to exploit the education industry. Although less intense than some other industries, but the education industry saw some large scale individual attacks. It can be predicted that in the post-COVID era, the online education business model will remain popular, driving changes in the education ecosystem, and eventually will attract more capital and service providers. Driven by profit, attacks may increase in the education industry.

2.4. Hackers Often Use IoT Devices to Initiate Reflection Amplification Attacks

Among various DDoS attacks, the reflection amplification attack only requires very little bandwidth, which can generate hundreds or even tens of thousands of times the traffic to the target. This type of attack is low in cost and high in attack power, but difficult to trace back to its source, making it a hacker favorite. Based on the data from the Wangsu security platform, the reflection amplification attack remains one of the commonly used attack methods, and a large number of reflection amplification attack requests have been captured throughout the year.

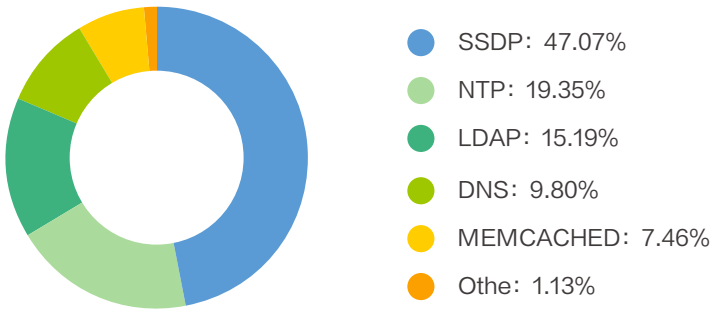

Figure 2-5 Distribution of Reflection Amplification Attack Protocol in 2020

Judging from the reflection amplification attack requests captured by the Wangsu security platform in 2020, SSDP reflection amplification (47.07%) is still the preferred method by perpetrators. SSDP protocol is mainly used for sensing home routers, webcams, printers, smart home appliances and other IoT devices. It can be predicted that with the rapid growth and adoption of IoT and smart devices, DDoS reflection amplification attacks using smart devices will become more prevalent.

Compared with the first half of the year, the obvious emerging trend is the LDAP reflection amplification attack (5.19%). The number of attacks in the second half of the year has increased nearly 30 times compared with the first half of the year. The proportion of Memcached reflection amplification attacks used by attackers is also increasing due to their amplification in tens of thousands of units.

Chapter III Interpretation of Web Application Attack Data

3.1. Explosive Escalation in Web Application Attacks, an Equivalent of 7.4 Times the Amount of Attacks in 2019

In 2020, the Wangsu security platform monitored and intercepted 9.524 billion Web application attacks, 7.4 times that of 2019, and the number of attacks saw explosive growth. The number of attacks in the first half of the year was nine times that of the same period in 2019.

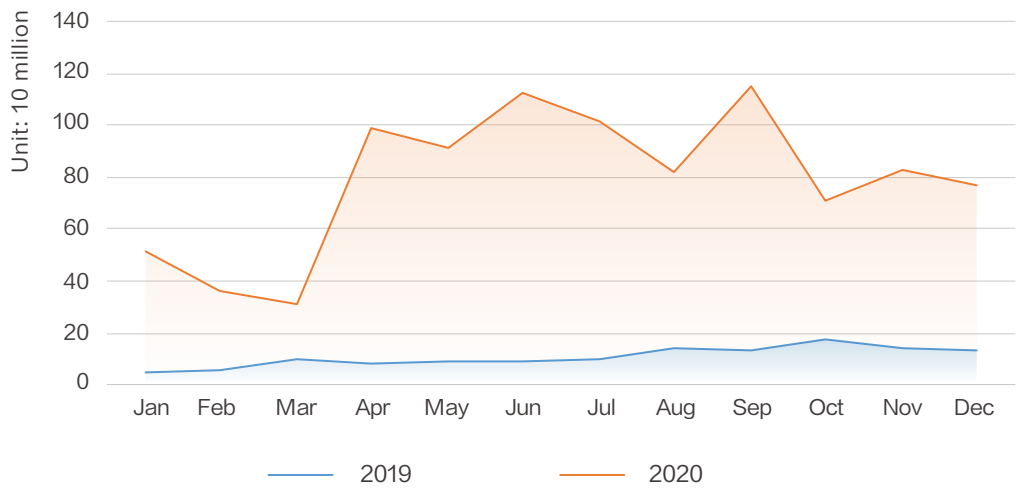

Figure 3-2 Web Application Attack Overview and Trends in 2019 and 2020

By analyzing the trend of the number of Web application attacks in 2020, it is remarkable to see that the changing trend of attack volume is consistent with the recovery of social activities and normal life. After the pandemic was initially brought under control in March 2020, the number of attacks also skyrocketed

In line with the explosive growth of Web attacks, the number of global sensitive data breaches continued to propagate at a high frequency in 2020, and the scale and impact have increased significantly. With the acceleration of digital transformation in various industries, the value of data is becoming more prominent. We can foresee that attacks targeting sensitive data will continue to grow in the future, which will inevitably require various industries to strengthen the protection of related business systems.

3.2. SQL Injection and Brute Force Cracking Attacks Consecutively Ranking Amongst the Top 3 Type of Attacks

According to the Web attack protection system powered by the Wangsu security platform, there are different ways to deal with different attack methods, which can reflect the distribution of Web application attacks.

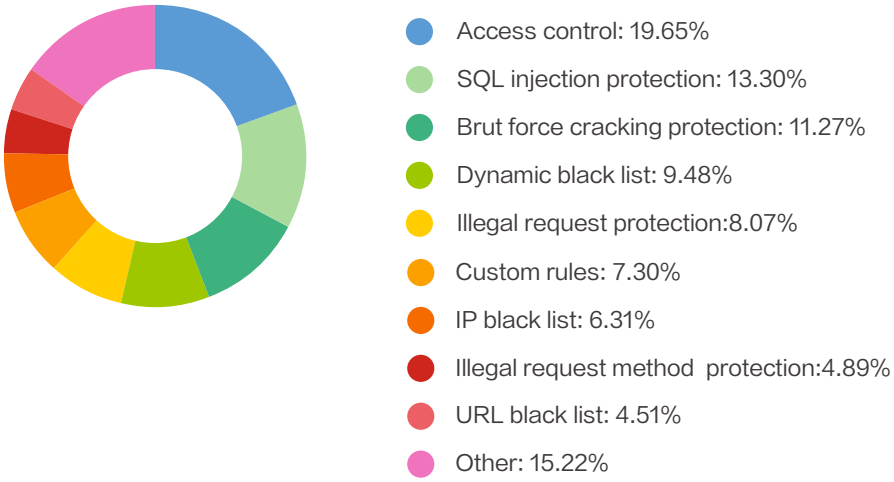

Figure 3-2 Web Attack and Protection Distribution in 2020

In general, the distribution of offensive and defensive means of Web application attacks is relatively uniform. SQL injection (13.30%) and brute force cracking (11.27%) remained within top 3 methods in recent years and are high-frequency attacks.

The Wangsu security platform has identified that more than 90% of Web attack traffic comes from automated scanners. Once the scanner sniffed out the vulnerability of the website, the attacker then launches an attack against the vulnerability. Websites that are scanned with a large number of vulnerabilities are more likely to be targeted by attackers.

The Wangsu security platform identifies Web scanners by analyzing the characteristics of attack sources, behavior pattern recognition, AI model detection, and threat intelligence, while directly filtering out a large number of attacks by means of access control (19.65%) and dynamic IP blacklist (9.48%), which can effectively reduce the probability of targeted attacks on websites and reduce the load pressure of automated scanners on websites.

3.3. Web Attack Sources are Concentrating Towards Domestic Locations

According to the analysis of the geographical location of attacking IPs, the source of global attacks in 2020 is mainly concentrated in mainland China, accounting for as high as 86.7% of all the attacks. Compared with 2019,attacks originating from mainland china accounted for just over half the attacks recorded. It can be seen that the trend of the concentration of attack sources to mainland China is significant.

This trend can be attributed to more stringent access control of overseas IP in recent years. With the increase in overseas proxy costs, attackers tend to use overseas IPs as the source of control. With only a small amount of origin IP, they can send attack instructions to a large number of domestic attack machines, which can launch direct attacks domestically, thus increasing the difficulty of tracking and reduced costs top the attacker.

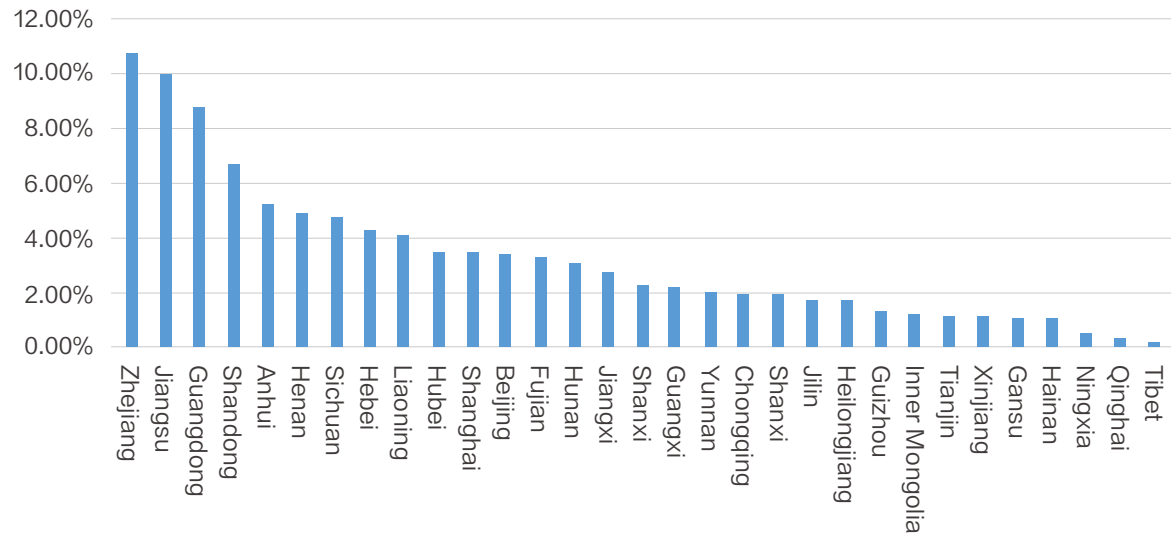

Figure 3-3 Distribution of Web Attack Sources from Mainland China in 2020

Further analysis of the sources of attack in mainland China shows that the top three regions remain to be Zhejiang, Jiangsu and Guangdong provinces, accounting for 10.75%, 9.91% and 8.71%, respectively. Due to the relatively better developed economy, these three provinces have extensive IT resources for attackers to make use of.

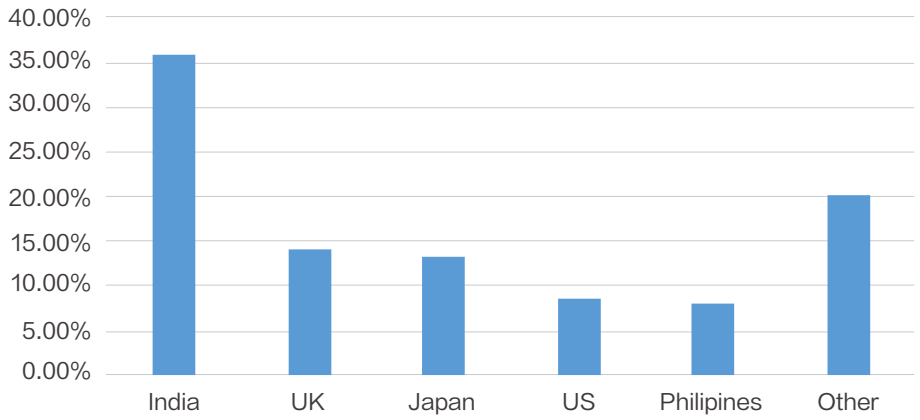

Figure 3-4 Distribution of Web Attack Sources from Overseas in 2020

According to statistics on the sources of overseas attacks, India, UK and Japan ranked in the top three, accounting for 35.86%, 14.08% and 13.26%, respectively.

3.4. Web Application Attacks are Prevalent in Various Industries

According to the statistics of the industries suffering from Web attacks, it can be easily seen that the distribution is relatively uniform. Taking the number one position, government agency accounts for only 6.36%, and the difference between each is only about 1% from retail in the second place to the gaming industry at the eighty place, indicating that Web attacks have penetrated into all industries.

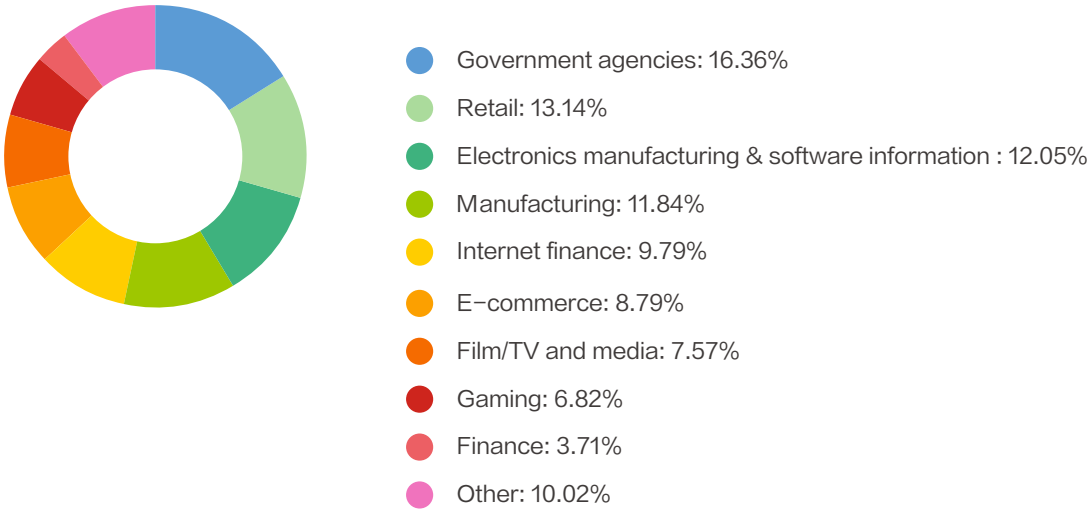

Figure 3-5 Distribution of Web Attack by Industry in 2020

Compared with the data of 2019, the ranking of government agencies has risen from the second to the first place. Combined with the fact that the number of Web attacks in 2020 is 7.4 times that in 2019, it is obvious that government agencies are under great pressure of attack. With the government affairs migration to the cloud, and comprehensively promoting the national government affairs service "one-net access" at an accelerated pace, the massive data of citizens and enterprises stored on the government platform has been coveted by hackers.

Chapter IV Interpretation of Malicious Crawler Attack Data

4.1. On Average 1,134 Crawler Attacks Occur for Every Second

In 2020, the Wangsu security platform monitored and intercepted a total of 358.54 billion crawler attacks, an average of 1133.81 attacks per second, triple the figure in 2019.

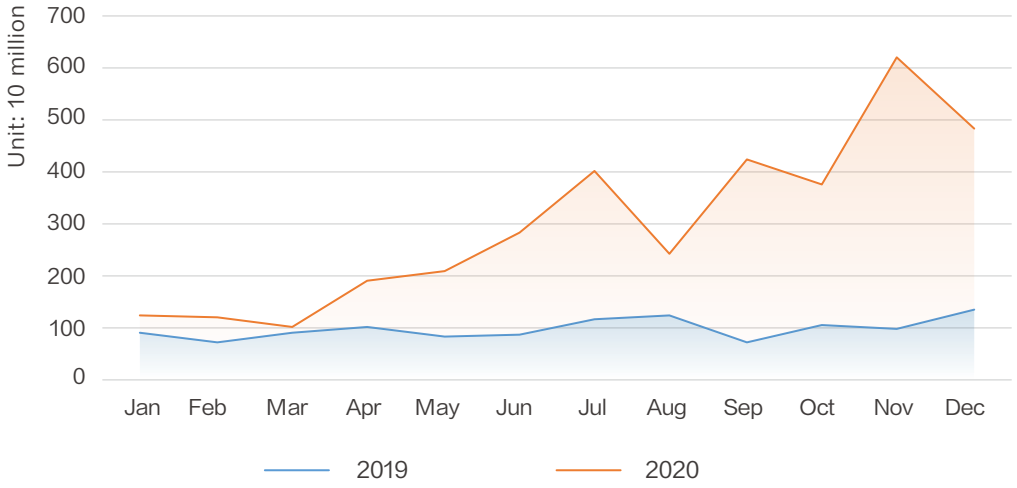

Figure 4-1 Trend of Malicious Crawler Attacks in 2019 and 2020

Based on the trend in 2020, malicious crawler attacks have soared since March. The emergence of this turning point is almost synchronized with the gradual progress of the resumption of production and work.

4.2. Significant Decrease in Crawler Attacks from Abroad

According to the distribution of source IP monitored and intercepted by the Wangsu security platform, more than 90% of malicious crawler attacks in 2020 came from domestic locations, while attacks from overseas accounted for only 9.99%, down by more than 25% from 35.28% in 2019.

Figure 4-2 Distribution of Global Sources of Malicious Crawler Attacks in 2020

The large-scale decline in overseas crawler attack data is affected by many factors, such as the COVID-19 pandemic, changes in international relations, stricter information control and so on. Affected by COVID-19, international relations, policies and regulations, industries such as purchasing agents and overseas shopping have been greatly impacted. The circulation cycle of many commodities has been extended, and goods often are unable to clear customs. The demand for data analysis of overseas merchants has decreased. Crawler attacks originating overseas have correspondingly decreased. At the same time, the state control of proxy software is more stringent, the speed and stability of overseas proxies are reduced, and the risk of being banned, have greatly increasing the cost of using overseas proxies for crawlers.

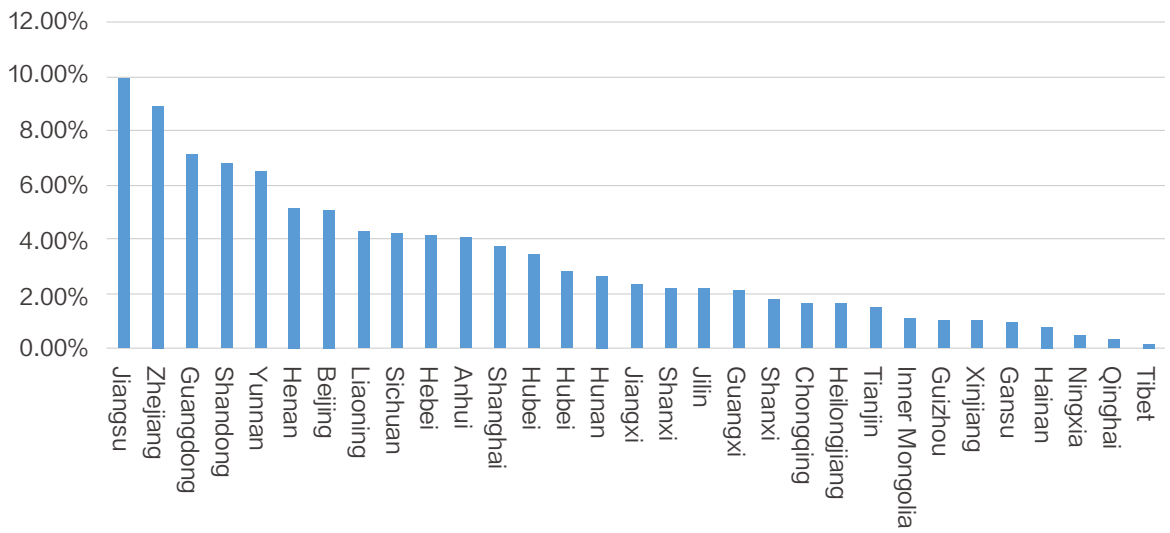

Figure 4-3 Distribution of Malicious Crawler Attack Sources from Mainland China in 2020

According to the domestic attack data, there are more than 7 million crawler attack source IPs from Jiangsu province (9.92%), followed by Zhejiang (8.97%), Guangdong (7.15%) and Shandong (6.83%) provinces with more than 5 million crawler attack source IPs.

4.3. Electronics Manufacturing and Software Information Service Among the Most Targeted Industries of Crawler Attacks

In terms of industry distribution, continuing the trend in the first half of 2020, the electronic manufacturing and software information services industry continued to occupy the first place, becoming the industry with the most serious malicious crawler attacks in the year (23.87%). This was followed by film/television and media (13.26%), e-commerce (12.46%), gaming (11.05%), retail (9.64%), transportation (8.98%), etc., each accounting for approximately 10%.

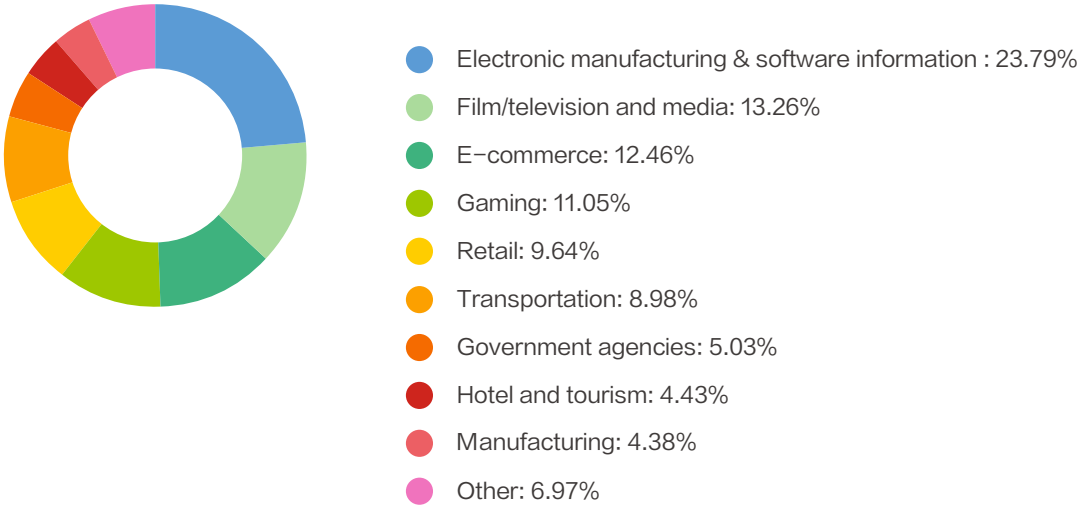

Figure 4-4 Distribution of Malicious Crawler Attack by Industry in 2020

Crawler attacks are closely related to economic interests, and the intensity of crawler attacks in various industries is in direct correlation with the development of the industry. The more prosperous the industry is, the more frequent the related crawler attacks are. At the same time, the attack intensity also has a lot to do with the value of public information data in the target industry and its anti-crawler capabilities.

Compared with previous years, the number of crawler attacks in the transportation industry decreased significantly from January to April 2020. The period from January to April of previous years is the peak period for returning home, travel and going back to work. In a short period of time, the country is faced with hundreds of millions of people moving to their destinations, train tickets and air tickets are in extreme demand, and ticket crawlers are popular at this time of the year. Affected by the pandemic in 2020, provinces and cities implemented strict traffic control and home isolation measures, restricting most of the movement of people, tourism, travel and other transportation-related industries where business saw a dramatic decrease, related crawlers also became much less useful.

However, according to the annual data, the number of malicious crawler attacks against the transportation industry is 2.16 times that of 2019, indicating that ticket crawler attacks have recovered rapidly and even doubled after the pandemic has been brought under control and travel restrictions lifted.

Chapter V
Interpretation of API Attack Data

5.1. 4.7 Billion API Attacks Recorded in 2020, an 56% Increase

Driven by the magnificent trend of the Internet and big data, APIs are widely used. Although open APIs are convenient as a data transmission and transfer channel for the development of various Internet products, they are also very easily attacked. In recent years, a number of data security incidents related to APIs have been reported at home and abroad, which have seriously infringed the legitimate rights and interests of various enterprises and users. China's communications, finance, transportation and other industries have issued relevant normative documents related to API security.

In 2020, the Wangsu security platform monitored and intercepted a total of 4.732 billion attacks against API services, a 56.03% increase over the same period in 2019. Significant increase in the number of attacks reflected the dire situation of API services.

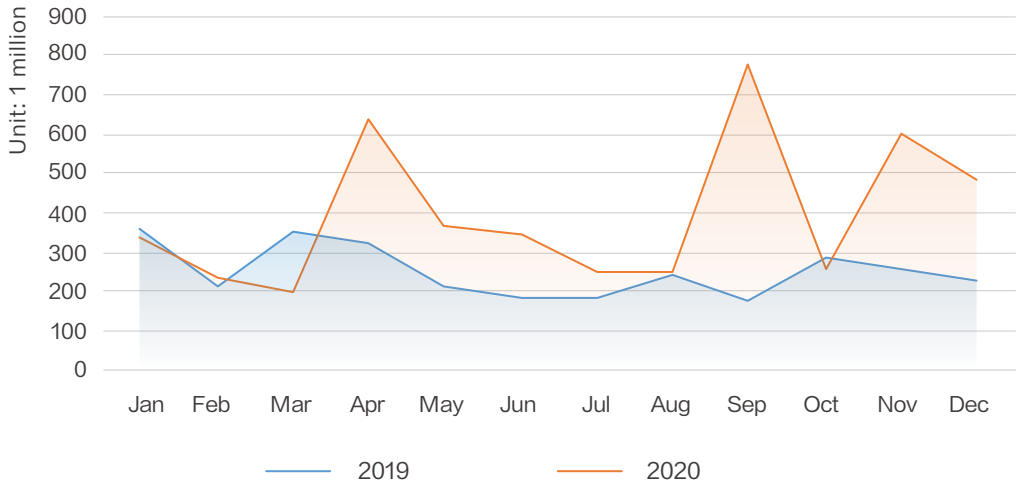

Figure 5-1 Trend of API Attacks in 2019 and 2020

As shown in the figure, API attacks soared in March-April, August-September and October-November 2020. Among them, the growth from March to April is also speculated to be related to the resumption of work and production.

5.2. Malicious Crawler Attacks Account for 70% of Recorded Attacks, Remains to be a Major API Attack Type

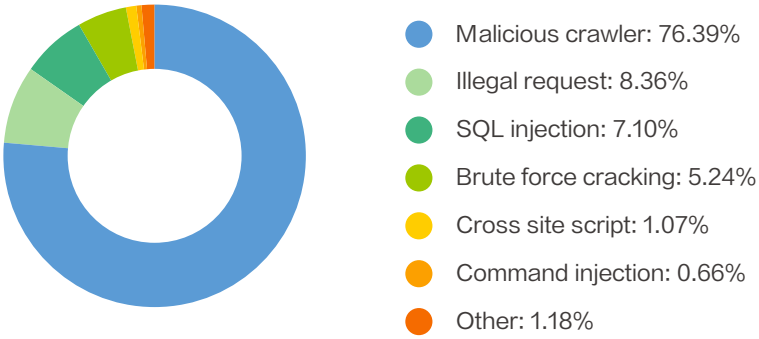

Figure 5-2 Distribution of API Attack Method in 2020

Malicious crawlers (76.39%) account for the overwhelming majority of attacks on API services, dominating the list of attacks, and the proportion is roughly the same as in 2019. Malicious crawlers may constantly attack various unprotected and valuable API interfaces opened by enterprises, in order to destroy, profits from, steal information and achieve other illicit goals.

The second and third places were illegal request (8.36%) and SQL injection (7.10%). The ranking of brute force cracking fell from second (2019) to fourth, and the proportion also dropped from 8.76% to 5.24%.

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

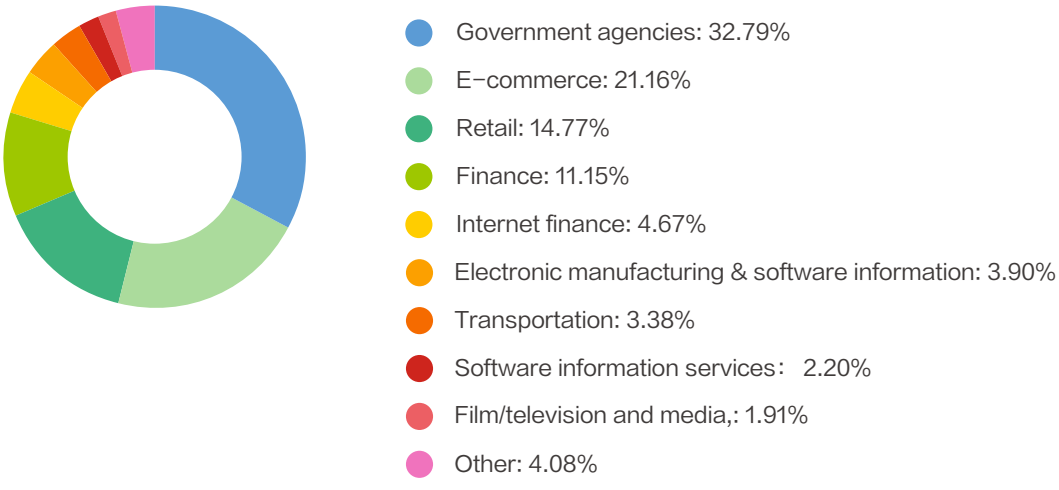

Figure 5-3 Distribution of API Attack by Industry in 2020

In 2020, government agencies still suffered the most API attacks, accounting for 32.79%. Attacks on government agencies were mainly concentrated in the first half of the year: in the first half of the year, attacks on government agencies accounted for more than 60%, reaching 60.94%.

E-commerce (21.16%) rose to second place. The changes matched people's way of life during the pandemic. Particularly in the first half of 2020, government agencies and e-commerce have taken more than 85% of API attacks, which was closely related to the fact that government information release and online shopping played an important role in people's daily life during the pandemic.

The transportation industry, which ranked second with nearly 30% in 2019, fell significantly in 2020, accounting for only 3.38%, driven down to the seventh place by the pandemic.

Chapter VI
Interpretation of Host Security Data

6.1. Over 90% of Enterprise Host are Deployed with Linux

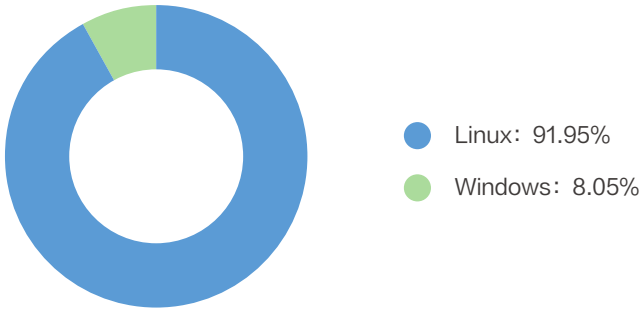

Figure 6-1 Distribution of Enterprise Server System in 2020

Windows and Linux are the mainstream systems used by enterprise hosts. According to the Wangsu security platform, 91.95% of enterprise hosts use the Linux system and 8.05% use the Windows system. Compared with 2019, the proportion of Linux has increased even further.

The Linux system offers better compatibility and stability and lower resource consumption, hence it is more suitable for mass automation management.

6.2. Over 40% Enterprise Hosts Use Container Technology

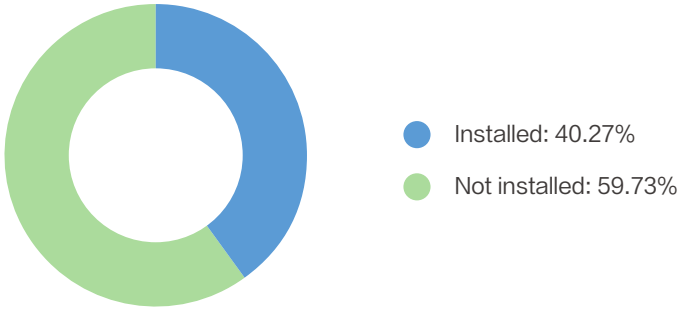

Figure 6-2 Enterprise Host Container Installation in 2020

The Wangsu security platform detected that 40.27% of the enterprise hosts had installed container-related software. As a virtualization technology, containerscan enable the deployment and operation of applications regardless of whether the server has deployed the operating system and dependent environment required by the application, thus greatly improving release and deployment efficiency. The utilization of container technology has increased rapidly in China in recent years, but compared with container utilization outside of China

6.3. Approximately 50% of Attacks Targeted Management Interfaces

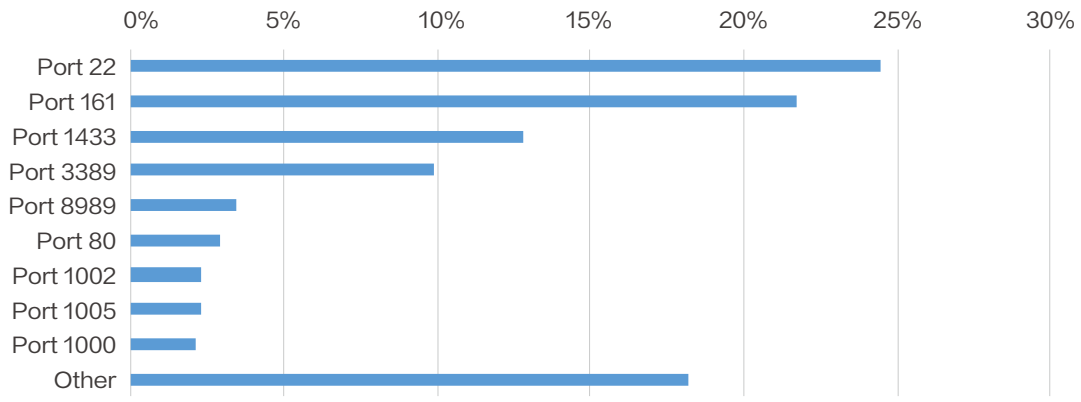

Figure 6-3 Proportion Distribution of Attacks on Host Open Ports in 2020

Based on the analysis of the port attack data collected by the Wangsu probe, the number of attacks on ports 22, 161, 1433 and 3389 is the largest, and the main attack method for these ports is brute force cracking. Brute force cracking attack is simple to execute, highly automated, and generally requires a large number of attempts to attack successfully, hence it is far ahead in the number of attacks.

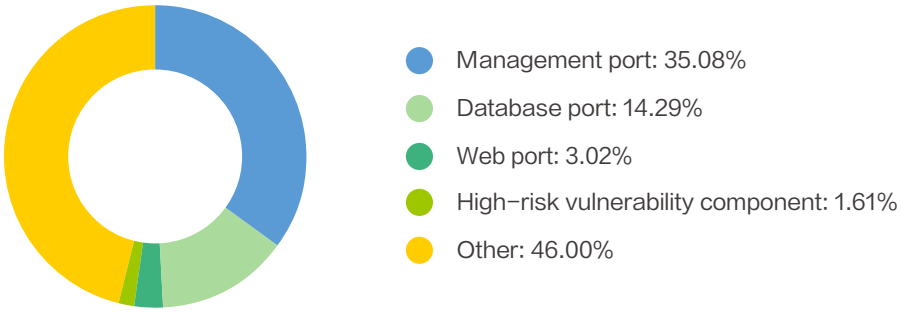

Figure 6-4 Proportion Distribution of Attacks on Various Host Open Ports in 2020

According to the type of ports attacked, the management port was attacked the most, accounting for 46.00%. Followed by database port (14.29%), Web port (3.02%) and high-risk vulnerability component port (1.61%). The simpler the attack method, the higher the degree of automation, and the more direct access to the port, the more favored by hackers.

6.4. Critical Vulnerability Attacks Utilized Simple Vulnerabilities

Top 10 high-risk vulnerabilities captured by the Wangsu host platform in 2020

No.1 Fastjson remote code execution vulnerability
No.2 Elasticsearch unauthorized access vulnerability
No.3 JMX remote command execution vulnerability
No.4 Apache Strut2 remote code execution vulnerability (S2-059/CVE-2019-0230)
No.5 Spark remote code execution vulnerability (CVE-2020-9480)
No.6 Druid remote code execution vulnerability
No.7 Docker Remote API unauthorized access vulnerability
No.8 Apache Flink Web Dashboard remote code execution vulnerability
No.9 Apache Tomcat AJP protocol file read and inclusion vulnerability（CVE-2020-1938)
No.10 Apache Tomcat remote code execution vulnerability（CVE-2017-12615)

According to the popular application and component vulnerability data collected by the Wangsu Host probe, combined with the intrusion traceability analysis, it is found that the high-risk vulnerability of the application layer components has become an important avenue of host intrusion. Compared with operating system vulnerabilities, application layer components are more exposed on the Internet, they can be directly attacked remotely, and there are more remote execution vulnerabilities than operating systems. Compared with Web business application vulnerabilities, component vulnerabilities are more common and widely used, and attackers are not required to explore vulnerabilities against Web business applications. Component vulnerabilities combined with automation tools can easily form illicit tool chains such as automatic "easy target" control and automated mining.

High-risk vulnerability attacks are increasing in the direction of the use of simple vulnerabilities, and the degree of automation and tool integration of unauthorized access and remote code execution vulnerabilities are getting significantly higher.

6.5. Enterprise Users Continue to Underestimate the Importance of Security Awareness

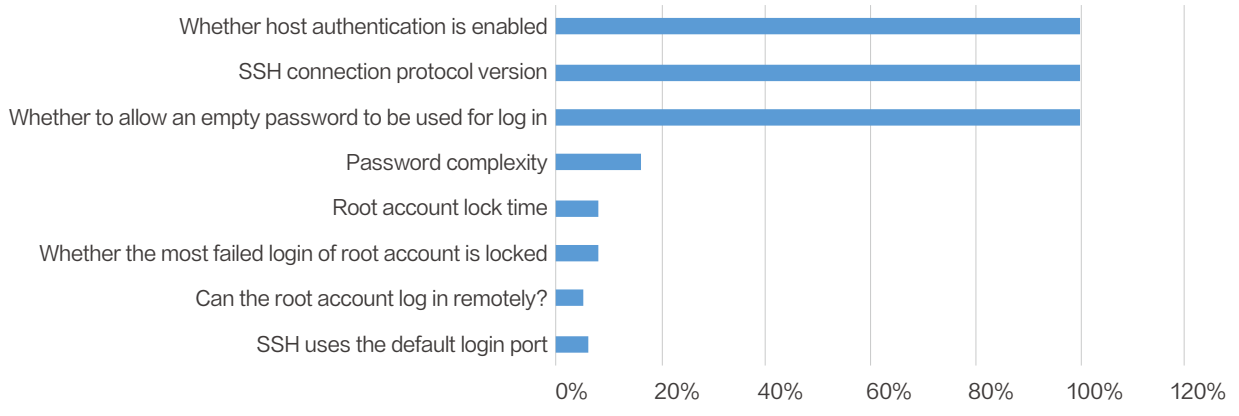

Figure 6-5 Compliance Rate of Some Core Configuration Items of Host Security Baseline Test in 2020

Based on the degree of risk, after sampling and analyzing the core configuration items of the host security baseline, the Wangsu security platform finds that users have hardly modified the default security configuration of the operating system, and the distribution of compliance items and non-compliance items are almost the same as the default configuration of the operating system. For the insecure configuration that operates the default settings of the system, such as whether the root account allows remote login, whether SSH uses the default login port, and so on, only a small number of users have carried out security enhancement.

At present, the demand for security consolidation mainly comes from the security consolidation regulations of network security level protection, rather than from the real-world internalized security awareness. Most administrators are still willing to risk a certain amount of security for the sake of convenience. At the same time, the difficulty of asset management is also an important cause. Many hosts are not included in the management scope of security personnel, and some ownerless hosts and test hosts are usually used as an avenue of intrusion.

6.6. The Number of Abnormal Login IP from Within the Country Leaped to The First Place

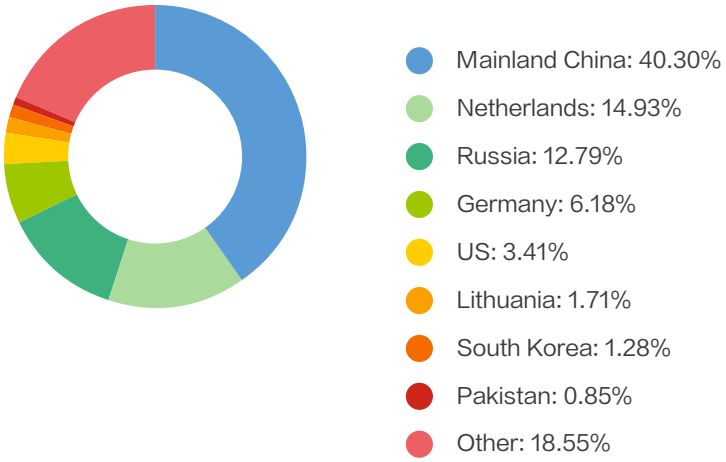

Figure 6-6 Distribution of Abnormal Login IPs in 2020

Compared with 2019, the proportion of domestic login IPs in abnormal login alert IPs has increased significantly. With the change of international relations and national policy, the cost of overseas proxies are increasing. And in recent years, the use of overseas IP as a stepping stone is no longer allowed, these factors lead to a significant increase in the proportion of domestic IP attacks.

6.7. Tempering with Scheduled Tasks is the most Frequently Used Method for Host Intrusion

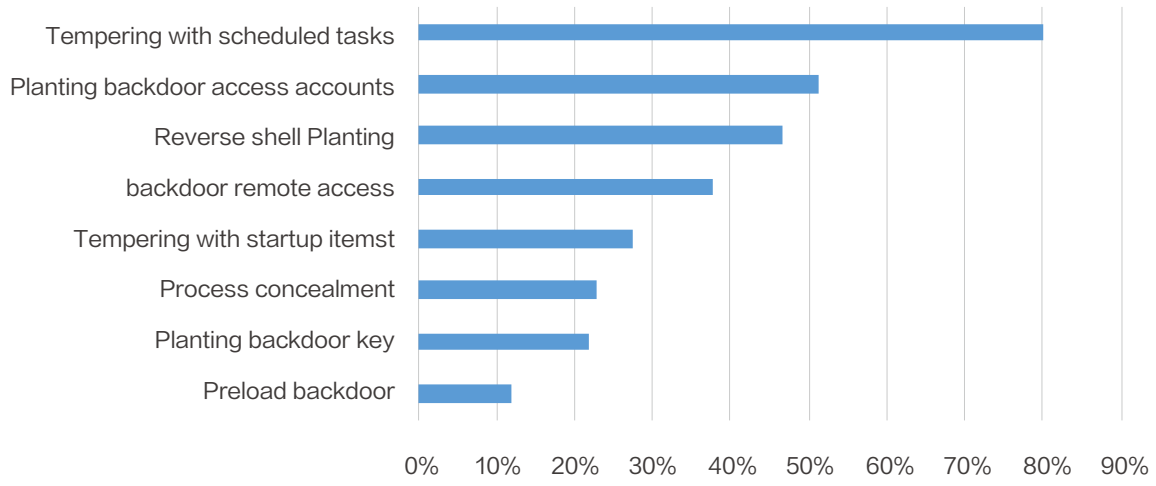

Figure 6-7 Detection Rate of Persistent Host Intrusion Methods in the First Half of 2020

Persistence is almost a critical part of host intrusion. After hacking, the persistent operation of malicious processes is usually ensured by means of modifying scheduled tasks (80.04%) and startup items(27.62%), and control are maintained by planting backdoor accounts (51.42%) and backdoor processes (37.70%). Many intrusions leave multiple backdoor channels - backdoor accounts, processes, and keys implemented at the same time. The most widespread persistent intrusions offer powerful concealment, which requires enterprises to improve their ability of investigation and analysis in order to avoid future hacker intrusions through backdoors.

Chapter VII Insight and Recommendations on Future Trends

The only constant in the world is change itself, this is especially true in the network security industry. Network threats and attacks are constantly changing, and new characteristics are reflected in each stage. Therefore, when planning and operating online businesses, we must fully consider the security risks caused various potential network security threats.

Based on the operational experience of the Wangsu security platform, we believe that network security will face the following trends in the future:

I. Comprehensive Cloud Security Solutions Becoming a Critical Requirements of Enterprises.

From data captured by the Wangsu security platform and the attacks reported in the industry, the current attack methods are gradually showing a trend of integration, and the threat faced by enterprises will not be limited to a single DDoS attack or Web application attack, but usually a comprehensive attack mix, leveraging a variety of attack methods to achieve the purpose of shutting down services of the target or stealing sensitive data.

At the same time, with the development of cloud native architectures, more enterprises are switching to cloud native services to establish their business in order to improve business agility. Cloud native solutions rely heavily on containers, micro-services, APIs and other technologies, which not only brings convenience to enterprise business, but also introduces some new risks, such as image security risks brought by container environment, API abuse and attacks, as well as other risks, which easily introduces vulnerability risks to enterprises business.

In the face of this attack trend and business development trend, the demand of enterprises has gradually developed from a single anti-DDoS, WAF and other requirements to a comprehensive cloud security solution, which is easier to use, operate and maintain cloud security production and services. For example, enterprises can carry out comprehensive report content viewing, configuration adjustment and distribution of various security events in an integrated portal system. This will greatly improve the response speed and efficiency to security events, and further reduce the impact of attacks.

Gartner has put forward the WAAP (Web application and API protection) solution in recent years, which is also a comprehensive solution that integrates various functions such as DDoS protection, Web application attack protection, crawler management, API protection etc. From which we can also see that Gartner also believes that what the enterprise industry needs is a comprehensive solution, this trend is consistent with the insights reflected by the Wangsu platform.

The security acceleration solution of Wangsu can not only provide cloud security services such as DDoS protection, Web application protection and malicious crawler protection for enterprises, but also provide network-wide acceleration features. Regardless of being attacked or not, it can provide maximum availability guarantee for the business of the enterprise. At the same time, the HIDS product can provide enterprises with vulnerability detection, attack alerts and other functions on the host and container side, which forms a more complete protection system along with cloud security.

II. SASE Is an Imminent Trend with Gradual Deployment

In 2020, under the influence of COVID-19, the demand for telecommuting has experienced exponential growth around the world. After this major test of hardship for enterprises, telecommuting is no longer a "Plan B", but has become a necessary choice, which objectively greatly promotes telecommuting as the new norm for any global enterprise.

In addition to the driving factors of the pandemic, new enterprise collaboration models, such as remote team collaboration and external partner collaboration, are also accelerating the application and popularization of telecommuting. However, for most enterprises, although the traditional telecommuting tools represented by VPN did address the needs of employees, but also exposed a large number of efficiency and security issues.

VPN gateways exposing ports in the public network that are easy targets for attackers, and be easily shut down through DDoS and other methods. At the same time, in recent years, vendors of VPN systems have been exposed to overlook vulnerabilities, which also brings great risks to the usage, operation and maintenance of such systems.
In addition, due to the fixed deployment location of VPN gateways, the access quality issues caused by cross-network access will significantly affect the user experience and office efficiency. Many enterprises have to find additional acceleration systems for VPN systems to improve their availability. More and more enterprises are beginning to realize beginning to realize that they need a more secure and efficient comprehensive solution to ensure the smooth progress of their business.

The Secure Access Service proposed by Gartner is an ideal model to meet the require-ments of this scenario. SASE integrated Edge (SASE) various networks and security solutions, such as SD-WAN, zero trust, security, etc. addressing remote access, mobile office and other scenarios, thus ensuring employees' normal access to the company's office resources in different scenarios and ensuring the security of the entire intranet. At present, more and more security vendors are attempting to launch similar solutions to promote the adoption of SASE, and there will be great admirable in this field in the future.

As the second largest CDN vendor in the world, Wansu has a inherent advantage in the field of SASE solutions. Currently, thanks to the existing SD-WAN products and resourc-es, Wangsu has launched SecureLink based on the concept of zero trust. In addition to the requirements of ensuring branch access and telecommuting, it provides enterprises with secure and efficient remote access solutions by building identity management, access management, IPS, DLP and other functions on devices and edge nodes.

Copyright information