网宿科技
WANGSU.COM

2021 H1

CHINA INTERNET SECURITY REPORT

Table of Content

Chapter I. Overview

- This report sets out to interpret in detail the source, methods and industry distribution of various attacks.
- All data used in the report are provided by the Wangsu security platform, which is subject to change as Wangsu security services evolve with future adjustments, these changes will have a certain impact on the trend indicated by the data, however this will not affect how we interpret or gain insight of the security trend from these data, where we may gain extensive understanding of the situation of security attack and defense, and enhance our perceived notion of security attack and defense.
- The report makes a comprehensive comparison of the attack and defense data in 2019, 2020 and the first half of 2021 to interpret and determine the attack trend.
- The most noteworthy finding in this report is that the number of Web attacks and malicious crawler attacks has doubled in consecutive years, indicating that application layer attacks and attacks against customer business itself have shown a growing trend.

1.1.DDoS attack overview and trends in H1 2021

- In the first half of 2021, the Wangsu security platform detected nearly 30 million DDoS attacks, which is consistent with the same period in 2020, while the peak of DDoS attacks has experienced a slight increase.
- One of the traditionally hardest-hit area is the game industry, ranked first in the number and peak level of DDoS attacks in the first half of 2021.
- In terms of reflection amplification attacks, NTP protocol attacks saw a sudden rise, accounting for 87.55% of the attack volume.

1.2.Web application attack overview and trends in H1 2021

- In the first half of 2021, the Wangsu security platform monitored and intercepted 10.113 billion Web application attacks, 2.39 times that of H1 2020, and 21.66 times that of H1 2019, demonstrating an overwhelming increase in web application attacks.
- The target of Web application attacks have shift from government assets to other industries such as software information services, real estate, and finance.

1.3.Malicious crawler attack overview and trends in H1 2021

- In H1 2021, the Wangsu security platform monitored and intercepted a total of 34.147 billion crawler attacks, an average of 2183.52 attacks per second, doubling the figure of previous years.
- In terms of attack sources distribution, the proportion of overseas attack sources has increased slightly, which is speculated to be related to the recovery of purchasing agents and overseas shopping industry as countries are recovering from the impact of COVID.
- Software information service is the industry most effected by malicious crawler attacks, followed by real estate, transportation and e-commerce.

1.4. API attack overview and trends in H1 2021

- In the first half of 2021, the Wangsu security platform monitored and intercepted a total of 4.253 billion attacks against API services, double the number in the same period in 2020, indicating a significant increase of this attack type.
- The concentration of attack methods against APIs have decreased, establishing a trend of diversification in attack methods.
- The vast majority of API attacks are concentrated in the software information services and finance industries, accounting for 41.62% and 28.41%, respectively.

1.5.Host security overview and trends in H1 2021

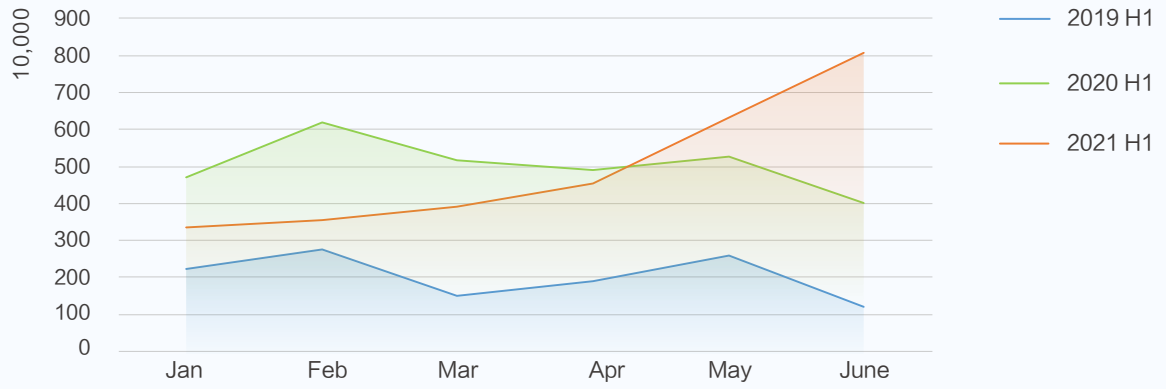
- Wangsu discovered in the first half of 2021 that over half of the enterprise hosts have leveraged container technology, which will lead to increasing democratization of common container security requirements.
- As a result of regular network attack and defense drills, enterprises have significantly improved the standardization of port management, and the number of public network open ports has dropped significantly.
- Attackers utilized a large number of hidden processes, camouflaged malicious timed tasks, Rootkit and other techniques to avoid abnormal behavior detection, obscuring the host security threat, which requires more powerful host intrusion detection capabilities.

Chapter II. Interpretation of DDoS Attack Data

2.1.Interpretation of DDoS attacks

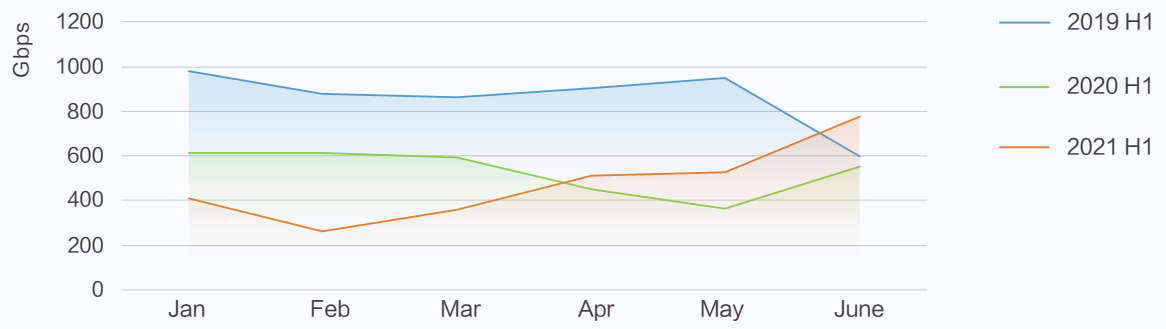
In the first half of 2021, the Wangsu security platform detected similar amount of DDoS attacks consistent with the same period in 2020 while experiencing a slight decrease of 1.63%. Based on the monthly trend, the number of attacks showed a sustained growth momentum in the first half of 2021, with the largest increase in May and June.

2-1 DDoS attack event trend of H1 2019/2020/2021

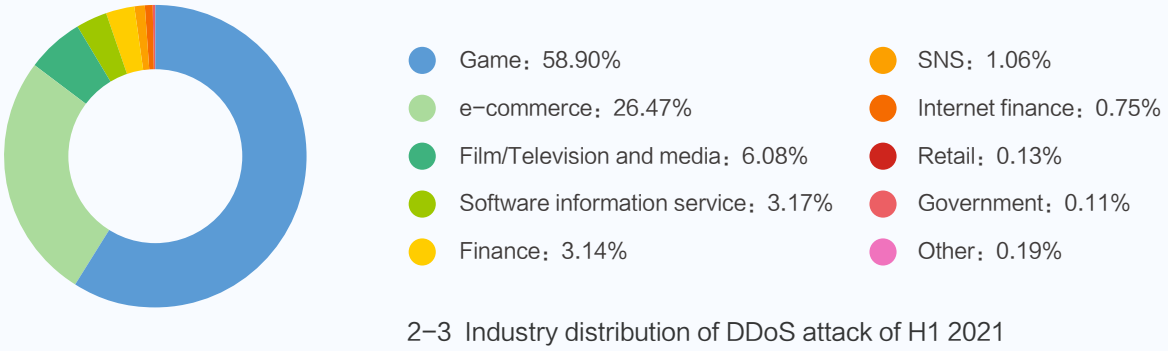


The peak of DDoS attacks in the first half of 2021 occurred in June, reaching 774.58Gbps, which was 26.62% higher than the peak of 611.73Gpbs in the first half of 2020 and lower than that of 982.47Gpbs in the first half of 2019. This year's peak also occurred in a different month from that of previous years, with attacks peaking in January in the first half of both 2019 and 2020, while this year's monthly attack peak began in February and peaked in June.

2-2 Monthly distribution of DDoS attack of H1 2019/2020/2021

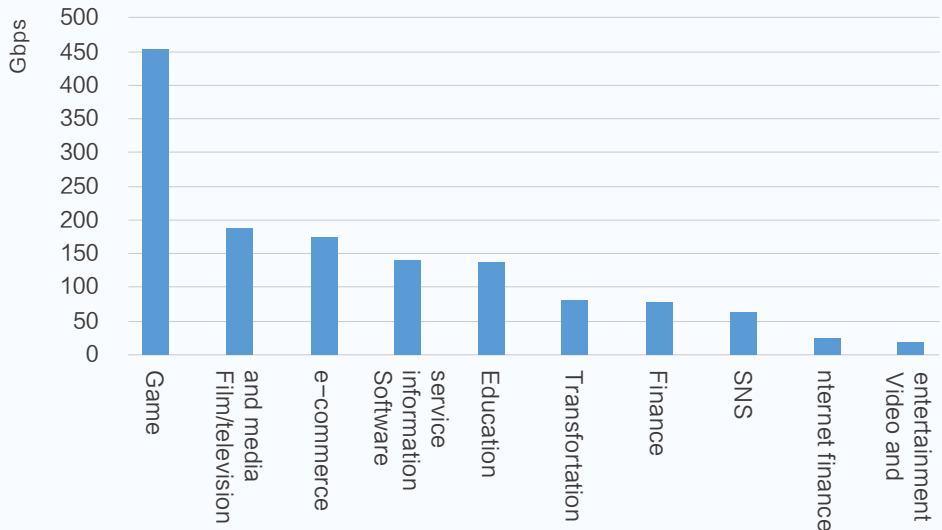


2.2. More than 80% of DDoS attacks are concentrated in the game and e-commerce industries



2-3 Industry distribution of DDoS attack of H1 2021

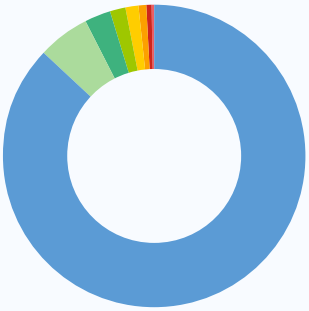
In terms of industry distribution of DDoS attacks, the game industry suffered the largest number of DDoS attacks in the first half of 2020, accounting for 58.90%, surpassing all other industries. E-commerce occupies the second place with 26.47%. Both industries combined accounted for 85% of the attacks. The third and fourth places were film/television and media information (6.08%) and software information services (3.17%).



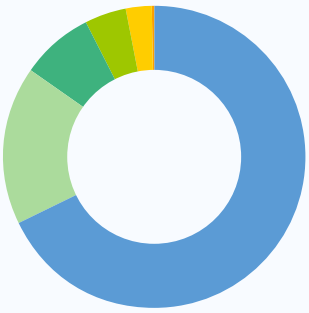
2-4 Top 10 industries of DDoS attack peaks for H1 2021

According to the statistics of the peak attacks suffered by various industries, the game, film/television and media information, e-commerce and software information services industries are the top four targets, with peak attacks of the game industry surpassing 450Gbps. The number of attacks and the industry distribution of attack peaks reflected a trend of industry-specific attack behavior.

2.3. NTP reflection amplification attacks leading the trend



2-5 Distribution of reflection amplification attack protocol in H1 2021



2-6 Figure 3-5 Distribution of reflection amplification attack protocol in H1 2021

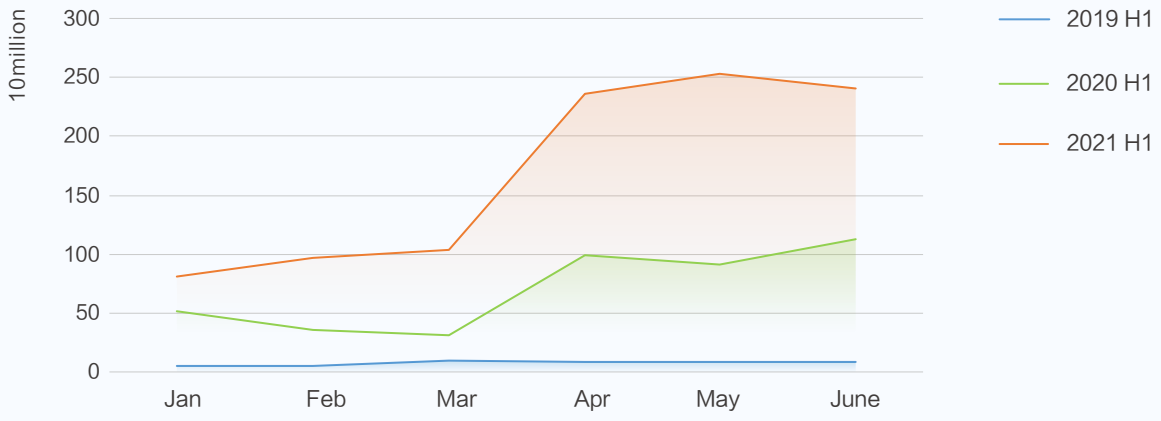
Reflection amplification attack remains as one of the most commonly used DDoS attacks for attackers, but in the first half of this year, the mainstream protocol of reflection amplification attack experienced a major reshuffle. NTP reflection amplification attacks sprang up, surpassing SSDP protocol attacks, which was the dominant attack type in previous years, and the proportion soared to an astonishing 87.55% from 7.78% in the same period last year. It is evident that the NTP protocol is widely used in attacks, and that there remains a large number of misconfigured NTP servers still exposed on the public network and can be used by hackers for attacks. The proportion of SSDP attacks plummeted from 68.01% to 50.72%.

Chapter III. Interpretation of Web Application Attack Data

3.1. The number of Web application attacks in the first half of the year has exceeded that of last year

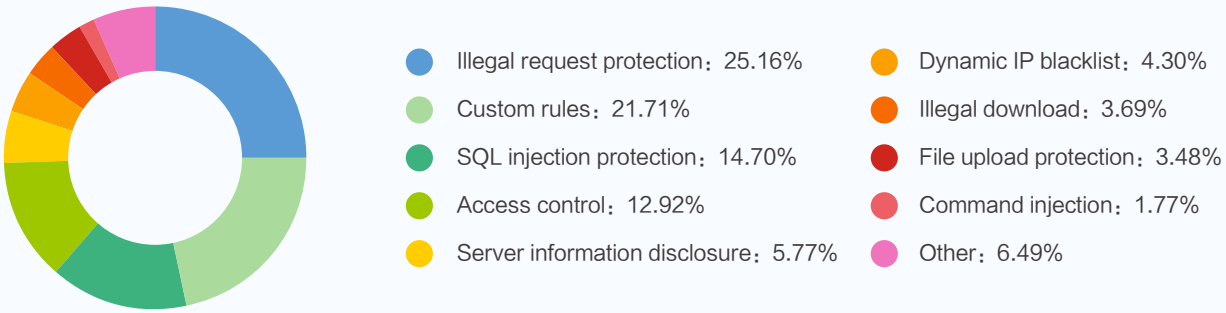
In the first half of 2021, the Wangsu security platform monitored and intercepted a total of 10.113 billion Web application attacks, exceeding the number of attacks for the entire year of 2020, an increase of 139.39% over the same period last year and showing a doubling trend, indicating that the threat of such attacks continues to rise.

3-1 Web attack trend of H1 2019/2020/2021



3.2. Diversification of Web attack methods

According to the Web attack protection system powered by the Wangsu platform, there are different ways to deal with different attack methods, it can also be clearly observed the distribution of attack methods.



3-2 Web attack/defense measure distribution of H1 2021

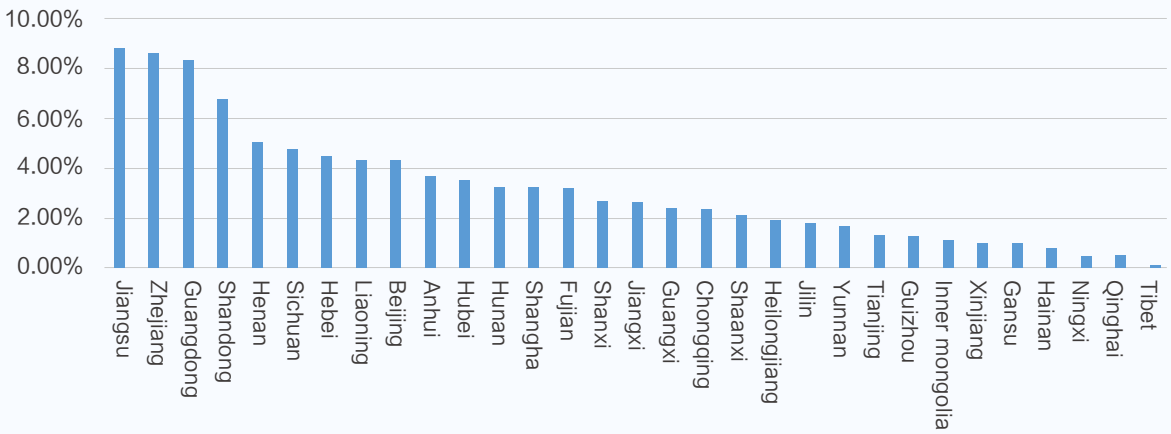
As can be seen from the above figure, the offensive and defensive means of Web application attacks maintained a relatively scattered distribution. The top three are illegal request protection (25.16%), custom rules (21.71%) and SQL injection protection (14.70%). Compared with previous years, only SQL injection protection remained a preferred choice by users, while brute force cracking protection have fallen out of the top 3, accounting for only 0.53%.

It is worth noting that the proportion of customer-defined rules is much higher than before, indicating that with Web attack protection, creating specific protection rules based on customers' own business conditions and specific attack scenarios is also a very effective measure.

With increasing traffic from automated scanners. The Wangsu security platform identifies web scanners through attack source feature analysis, behavior pattern recognition, AI model detection, threat intelligence, etc., and can directly filter out most of the scanner attacks through access control (12.92%), dynamic IP blacklist (4.30%), etc., effectively reducing the probability of targeted attacks on specific websites. At the same time, reducing the load pressure of the automatic scanners on websites.

3.3. Overseas attacks increasing in proportion

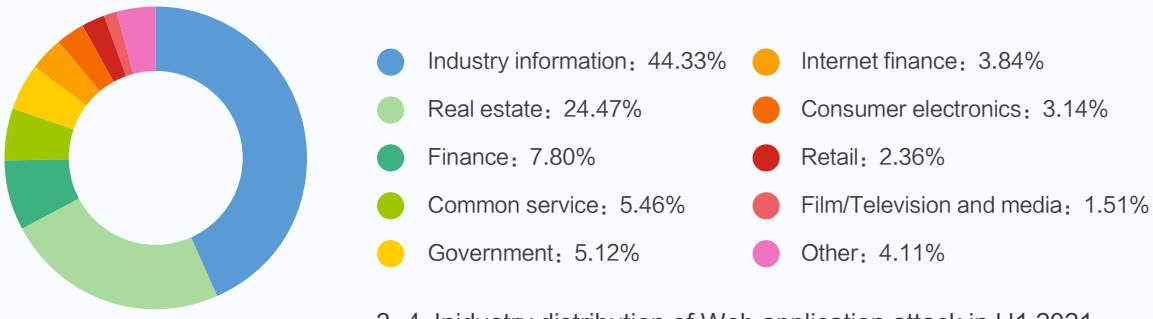
Through the analysis of the geographical location of attack IPs, it is found that 64.98% of the global attack sources came from Chinese mainland in the first half of 2021, while those from abroad accounted for 35.02%, an increase of nearly 26 percentage points over the same period last year.



3-3 Web attack source distribution of mainland China in H1 2021

Statistics on the distribution of attack sources in Chinese mainland provinces show that provinces in TOP15 accounted for more than 75% of attack sources in the first half of 2021. Jiangsu, Zhejiang and Guangdong are still the top three sources of attack in China, accounting for 8.95%, 8.78% and 8.46%, respectively. These three economically developed provinces have occupied the top three sources of domestic attacks in the past two years due to their better developed IT resources.

3.4. Software information services suffered more than 4 billion attacks



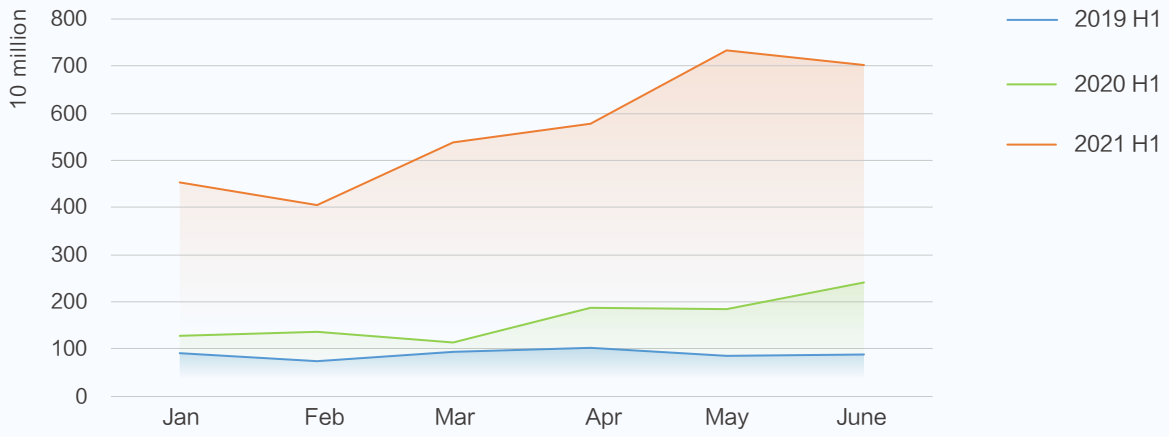
3-4 Inidustry distribution of Web application attack in H1 2021

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

Chapter IV. Interpretation of Malicious Crawler Attack Data

4.1. The attack volume of malicious crawlers has doubled in consecutive years

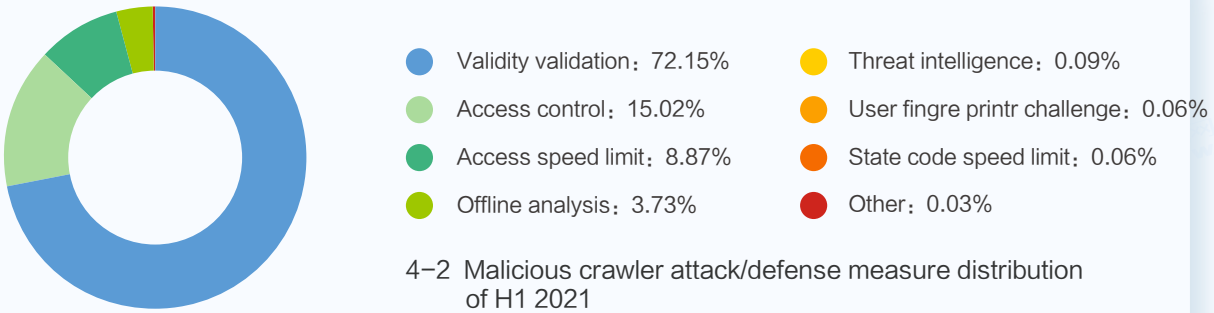
4-1 Malicious crawler attack trand of H1 2019/2020/2021



In the first half of 2021, the Wangsu security platform monitored and intercepted more than 34.147 billion malicious crawler attacks, with an average of 2183.52 attacks per second, which is close to the total amount of the previous year, 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, and the security threat is becoming increasingly prominent.

4.2. Validity verification effectively intercepts more than 70% of attacks

The Wangsu platform is integrated with a variety of protection algorithms to establish a protection system for malicious crawlers, and the trend of attack methods and protection results can be evaluated from the online attack and defense data.

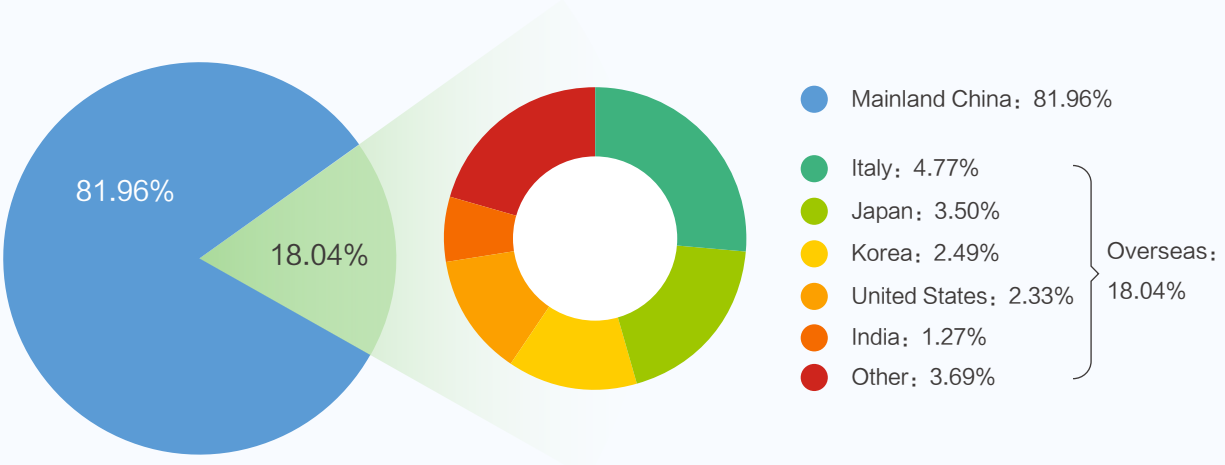


4-2 Malicious crawler attack/defense measure distribution of H1 2021

From the attack and defense data in the first half of 2021, it can be seen that various malicious crawler protection methods using the validity verification of clients and their requests are still the most effective means to deal with malicious crawlers, which can filter out more than 70% of attacks.

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

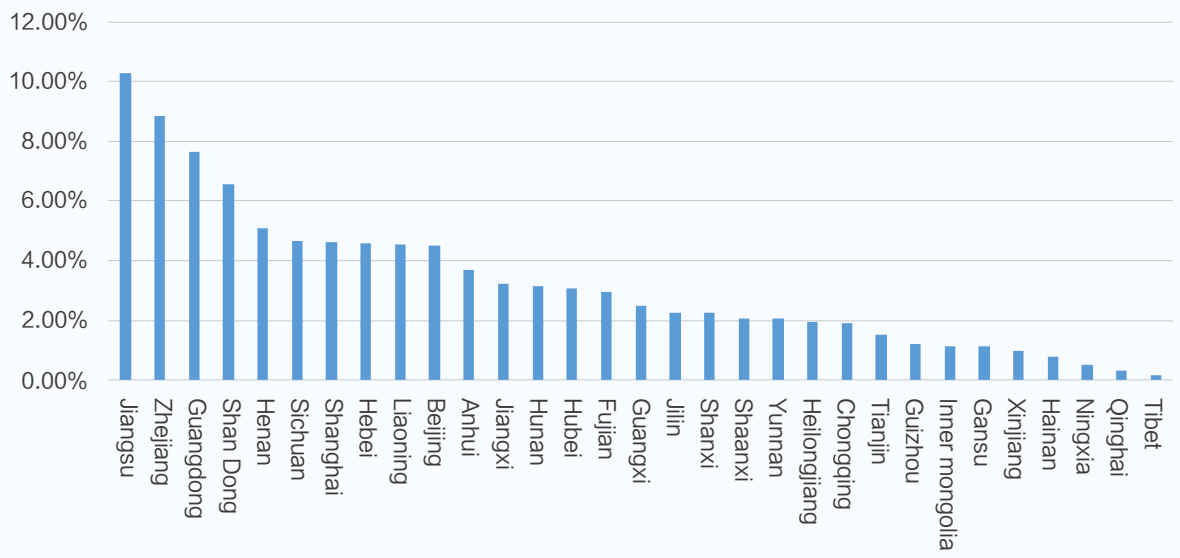
4.3. Slight rebound in proportion of overseas attack sources of malicious crawlers



4-3 Global malicious crawler aattack source distribution of H1 2021

According to the distribution of source IPs monitored and intercepted by the Wangsu security platform, more than 80% of malicious crawler attacks in H1 2021 came from domestic locations, The proportion of overseas attack sources increased to 18.04% from 7.08% in the same period last year.

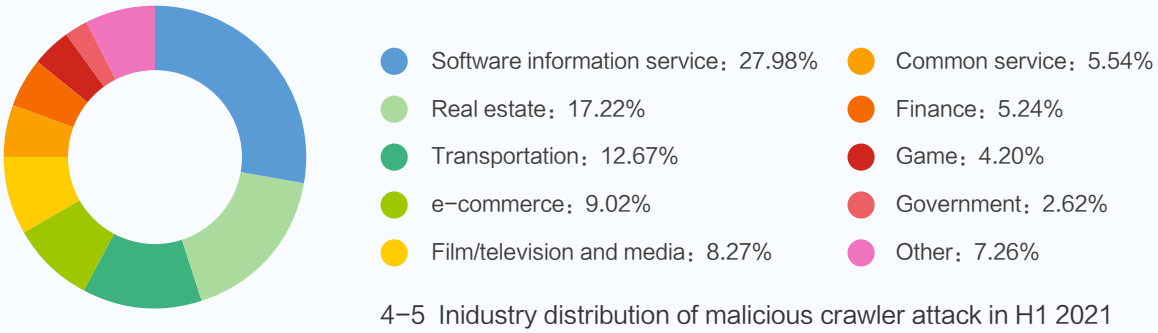
The increase in the proportion of overseas sources of attack may be related to the stabilization of the COVID-19 pandemic, the recovery in purchasing agents, overseas online shopping and other industries, and the rebound in demand for overseas merchants to crawl competitors' goods, prices and other information for sales strategy analysis.



4-4 Malicious cralwer attack source distribution of mainland China in H1 2021

The number of malicious crawler attacks in Jiangsu, Zhejiang and Guangdong was 10.29%, 8.83% and 7.65% respectively, making them the three provinces with the largest number of sources. Overall, the distribution of domestic attack sources tends to be more evenly distributed than in the same period in previous years, which can be tracked to the improvement of local IDC, network, cloud computing and other IT infrastructure construction, and the narrowing of inter-regional gaps in server and IP resources.

4.4. Malicious crawler attacks are scattered in the industries



4-5 Inidustry distribution of malicious crawler attack in H1 2021

The industry distribution of malicious crawler attacks shows a trend of low concentration and are more evenly spread. The software information services industry, which suffered the most attacks (27.98%), accounted for less than 30%. The second to fifth places were real estate (17.22%), transportation (12.67%), e-commerce (9.02%) and film/television media information (8.27%).

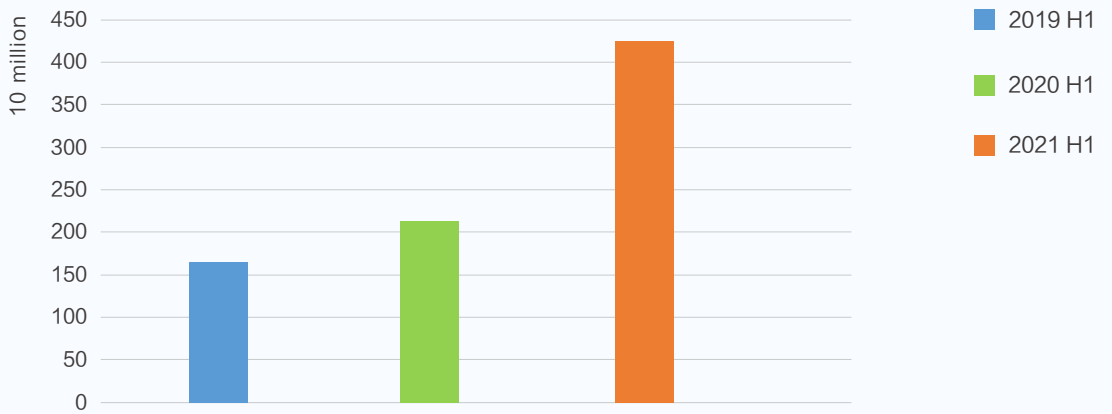
Among them, the ranking of transportation returned to the top three from the ninth (2.08%) in the same period last year, reflecting that the transportation industry has gradually recovered from the negative impact of the COVID pandemic, and ticket booking crawlers have made a comeback.

Chapter V. Interpretation of API Attack Data

5.1. In the first half of 2020, there were an average of 272 attacks against API services per second

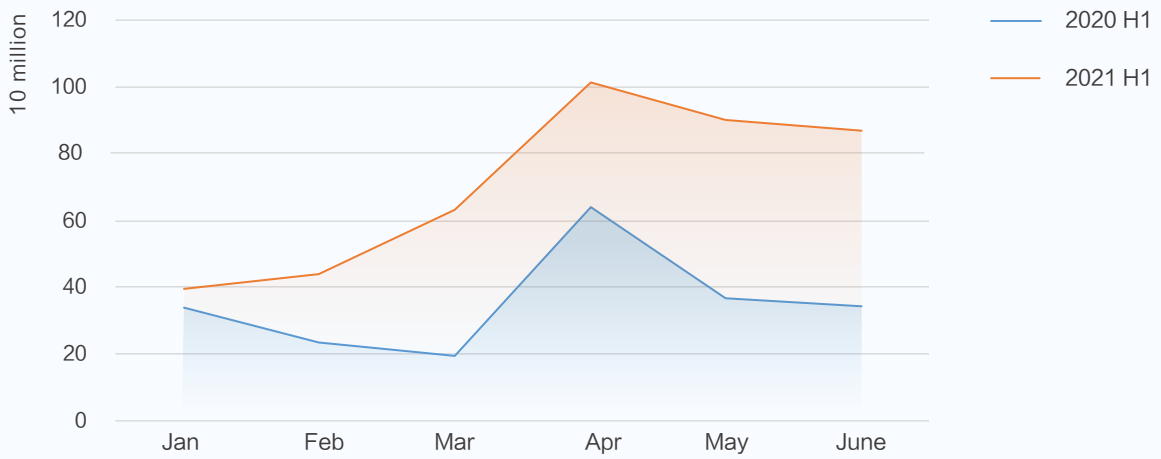
Accompanied by the boom of Internet, big data and micro-service architecture, APIs have experienced a significant growth. Although open API provides convenience for the development of various Internet products and services, it is also a lucrative target.

5-1 API attacks of H1 2019/2020/2021



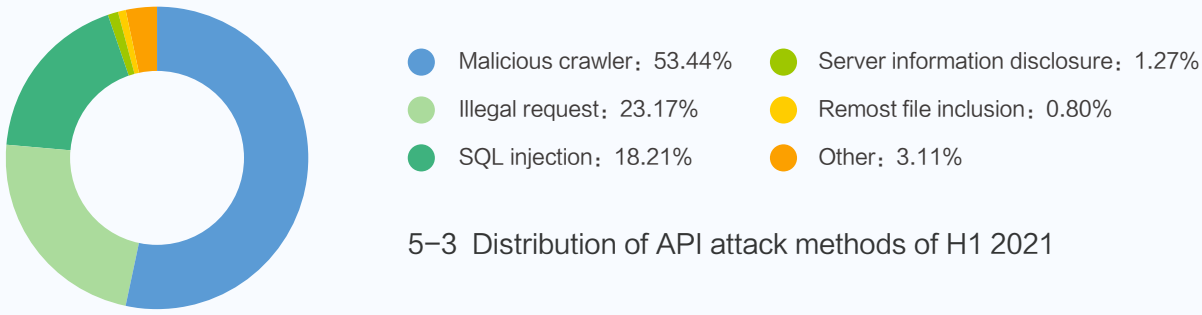
In the first half of 2021, the Wangsu security platform monitored and intercepted a total of 4.253 billion attacks against API services, with an average of 271.96 attacks per second, which has reached 2.01 times that of the same period last year, and the growth rate has increased with every passing year, indicating the severe security prospects faced by API services.

5-2 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, roughly similar to that of the same period in 2020.

5.2. Diversification of API attack methods

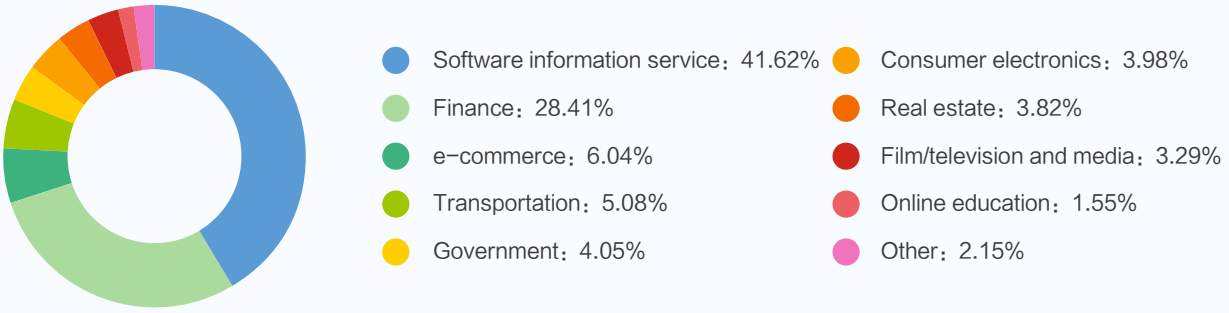


5-3 Distribution of API attack methods of H1 2021

In the attacks against API service, malicious crawler is the most proponent attack method, and this trend is developing with sustained momentum. In terms of API attack data in the first half of 2021, malicious crawler attacks accounted for 53.44% of the total number of attacks, down significantly from 74.82% in the same period last year.

The second and third places were illegal request (23.17%) and SQL injection (18.21%), which increased significantly compared with 5.97% and 10.94% in the same period last year. The centralization of the distribution of attack methods have decreased, which shows that the attack methods against API are gradually showing a trend of diversified development, rather than relying on only one attack method.

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



5-4 Industry distribution of API attack in H1 2021

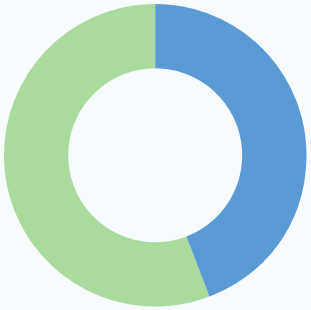
In the first half of 2021, the software information service industry has suffered the most API attacks, accounting for 41.62% of the total attack volume. The financial sector ranked second with 28.41%.

The proportion of API attacks suffered by these two industries reached nearly 70%, indicating the extremely grim attack 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 this year to approximately 10% that of the same period last year, down from 60.94% in the first half of 2020 to 4.05 per cent.

Chapter VI. Interpretation of Host Security Data

6.1. More than half of the enterprise hosts have adopted container technology

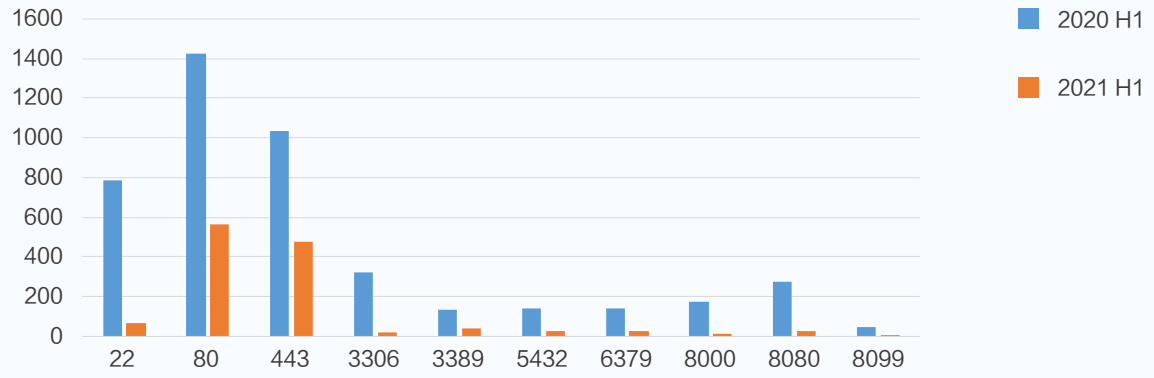


6-1 Host container installation of H1 2021

The Wangsu host security probe has discovered that 55.73% of the enterprise hosts have installed container-related software, an increase of 15.46% compared with the end of last year, indicating a relatively rapid growth rate. It can be predicted that the demand for container security will grow further in the future.

6.2. The number of open ports in the public network has decreased significantly, narrowing the breadth of attacks.

6-2 Comparison of the number of public network open ports between H1 2020 and H12021



Based on the analysis of the public network open ports collected by the Wangsu host probe, it is found that the number of public network open ports decreased significantly in the first half of 2021 compared with the same period in 2020.

Among them, management ports (such as port 22 and 3389), database ports (such as port 3306 and 5432 ports) and test ports (such as port 8000 and 8099) have decreased by approximately 90%. Formal business ports (such as port 80 and 443) have also decreased by more than 50%.

The decline in the number of open ports in public network is mainly due to regular network attack and defense drills, which effectively improved the standardization of customer management ports in the Wangsu security platform, and changes the fact that business departments did not use ports strictly in accordance with security specifications in the past. As a result, management ports and temporary test ports are often used as entry points for hackers, which greatly reduced the attack breadth.

6.3. Most of the high-risk vulnerabilities are general component vulnerabilities related to Web applications

Top 10 high-risk vulnerabilities captured by the Wangsu security platform in the first half of 2021

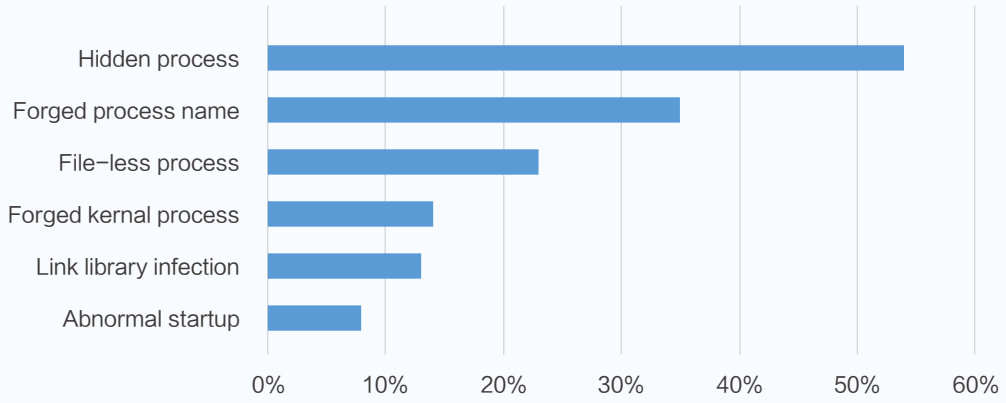
No.1	Fastjson remote code execution vulnerability
No.2	Multiple deserialization vulnerabilities in Stream
No.3	Vulnerabilities in Apache Tomcat AJP protocol files reading and inclusion
No.4	Multiple deserialization vulnerabilities in Apache Commons FileUpload
No.5	Apache Shiro remote code execution vulnerability
No.6	Apache Struts2 remote code execution vulnerability
No.7	JMX remote code execution vulnerability
No.8	Druid remote code execution vulnerability
No.9	Spark remote code execution vulnerability
No.10	Apache Flink Web Dashboard remote code execution vulnerability

Most of the high-risk vulnerabilities are application and component vulnerabilities, particularly for Web application related common components. Application component vulnerabilities have a more accessible execution environment than operating system vulnerabilities and are more versatile than business vulnerabilities.

Usually, illicit parties will choose vulnerabilities with a large number of users and simple and stable exploiting conditions to develop automated tools to profit from bot control and automated mining at a lower cost.

In addition, from the perspective of vulnerability distribution, open-source components are more favored by security researchers. Because it is easier to obtain source code and analysis environment, open-source software often exposes more vulnerabilities than commercial software. However, this does not imply that commercial software is more secure than open-source software. on the contrary, the open-source software community often can find vulnerabilities faster, which is beneficial for enterprises to shore up vulnerabilities in time, while commercial software has more potential vulnerabilities that have not been discovered.

6.4. Significant aggravation in the challenge of detecting abnormal host processes



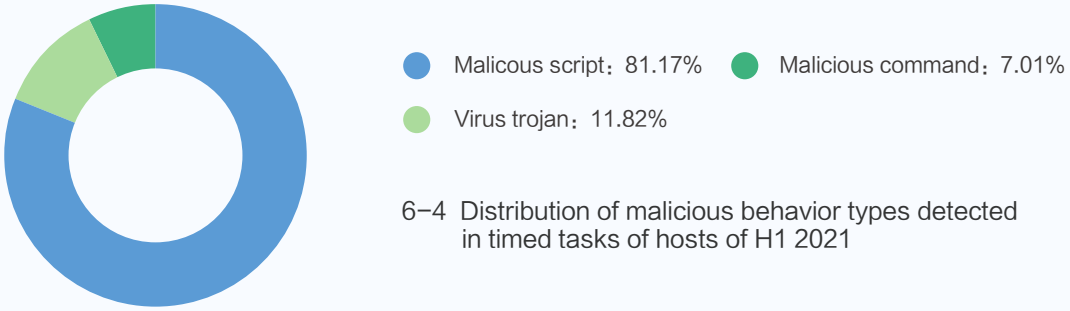
6-3 Detection rate of common abnormal process types of H1 2021

From the abnormal process data identified by the Wangsu host probe, we can deduce that the abnormal processes on the host often various techniques in evading detection or interfere with security software detection and manual intrusion analysis.

Among the means of evading detection, hidden processes are the most commonly used, and the Wangsu host probe has detected this technology in more than 50% of intrusions. Hiding processes prevents malicious processes from showing up in the process list.

Forged process names, which ranks second in detection rate, is also a common practice for attackers to evade intrusion detection and troubleshooting. By displaying a false process name such as common system process name or kernel process name, the illicit process is often difficult to identify. Link library infection and abnormal startup mode use legitimate processes to load malicious code to bypass the detection of antivirus software.

6.5. Camouflaged malicious timed tasks is also a common technique for attackers to evade detection



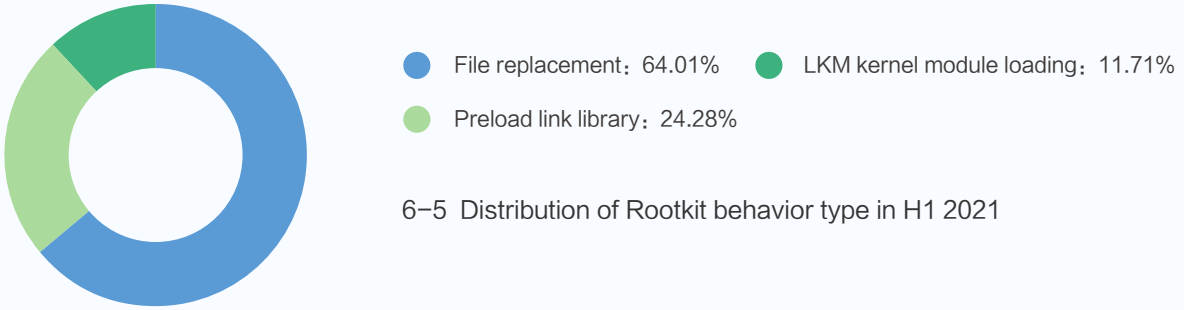
6-4 Distribution of malicious behavior types detected in timed tasks of hosts of H1 2021

Through studying and analysis of malicious timed tasks identified by the Wangsu host probe, among the malicious behaviors encapsulated by the timed tasks, the proportion of malicious scripts detected is as high as 81.17%. Followed by virus Trojan (11.82%), malicious instructions (7.01%).

Malicious timed tasks are usually implemented in the form of malicious scripts to perform malicious actions, such as executing virus Trojans, malicious instructions, and so on. In the form of malicious scripts, attackers can easily disguise malicious timed tasks as the paths of legitimate programs to avoid detection. In addition, malicious scripts can also encapsulate all kinds of malicious behaviors together to reduce the amount of scheduled task configuration and improve the configuration efficiency of attackers.

6.6. The most covert high-risk threat: Rootkit behavior with little impact on the system becomes mainstream.

Rootkit is the most powerful malware technology with concealment capabilities, which can gain root access and completely control the target operating system and its underlying hardware. Attackers often use Rootkit technology to hide their own or specific files, processes and network connections and other information for long-term evasion of intrusion detection in the target system, posing a great threat to security.



6-5 Distribution of Rootkit behavior type in H1 2021

Based on the analysis of the Rootkit behavior identified by the Wangsu host probe, it is found that the proportion of application-level Rootkit for file replacement is the highest, reaching 64.01%, followed by preloading link library (24.28%) and LKM kernel module loading (11.71%).

The practice of file replacement often has little impact on the system and is easier to integrate into the automated process, hence it is most favored by attackers. Although the loading of LKM kernel module is difficult to detect and eliminate, it has the inherent issue of kernel compatibility and the risk of damaging system stability, therefore it only accounts for a relatively low proportion of such attacks. At present, it has become a mainstream method for illicit parties to profit by implanting mining Trojans after invading a host. This approach requires a stable system to continuously reap benefits. Therefore, illicit parties often attempt to avoid actions that will cause damage to the system, with a stable system environment, it is often difficult for users to detect such intrusion.

Chapter VII. Insight and Recommendations on Future Trends

As can be seen from the report, network threats and attacks are constantly changing, and the data and offensive and defensive scenarios shown in the security report at this stage have undergone some new changes compared with the same period in 2019 and 2020. On this aspect, it can also be seen that when considering the security threats faced by their own businesses, enterprises often must constantly adjust to the dynamics of the situation, and the protection concept and strategies must keep up with the changes in attacks in order to implement effective response

I. The business security threat continues to escalate, the means of attack become more covert, and the security defense urgently needs to be integrated and extensively deployed.

As indicated in this report, **Web attacks, malicious crawler attacks and API attacks** have all increased exponentially in quantity. 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 attackers, as well as increasing in proportion**. The purpose of attack is no longer simply to make the customer's business inaccessible, but to more directly focus on the customer's business-related data, etc., once successful, it will not only affect the customer's business itself, the leaked data will also become a means of profit, or the captured server will become a resource for mining or attacking other targets, thus creating more benefits for attackers and causing more long-term damage to the victim enterprise.

At the same time, as more enterprises adopt cloud native architectures to build business, the operating environment of business applications is also changing. Technologies such as containers and micro-services that cloud native relies on not only improve the agility of the business, but also introduce new security risks, such as container escape risk, image security risk, etc., which can also directly damage business operation and cause business data theft.

In terms of attack methods, hacker attacks have shown the characteristics of improved automation and concealment. It is common to use AI to simulate human behavior to bypass conventional security rules, thus the difficulty of intrusion detection and protection is increasing.

With this trend, **when providing online services, enterprises must carefully consider comprehensive security protection solutions from the network layer to the application layer** to establish extensive defensive measures to ensure that after one layer of security measures are breached, there are multiple extra layers to intercept further threats and prevent attackers from accessing core business applications and data, to ultimately prevent any losses.

The WAAP (Web Application & API Protection) solution proposed by Gartner in recent years is a comprehensive solution that integrates the four core capabilities of Web application firewall, DDoS protection, crawler management and API protection. Gartner predicts that by 2026, 40% of organizations will adopt advanced API protection and Web application security capabilities as the basis for selecting WAAP service providers.

Gartner's view that comprehensive solutions will become the trend of enterprise security requirements coincides with Wangsu's sentiment on the same subject. The **security acceleration solution** provided by Wangsu empower customers with cloud security services such as DDoS protection, WEB application protection and malicious crawler protection, but also provide customers with network-wide acceleration features to maximize the availability of their business.

In addition to the distributed cloud security protection network, Wangsu also provides host security and container security products, and provides customers with high-precision vulnerability detection, intrusion detection, attack alerts and other capabilities based on massive big data samples and AI engine **on the host and container side**, which can form a more extensive protection system with cloud security. At the same time, the comprehensive customer service system and security operation and maintenance team will carefully monitor the customer's business state under changing attack techniques, respond to the new attack methods, and ensure the effectiveness of the protection strategy, ensuring the smooth operation of the customer's business.

II. With increasing demand for SASE, accelerate the implementation of next generation security model.

Driven by the COVID pandemic, the digital transformation of global enterprises has accelerated, giving birth to a large number of new applications such as telecommuting, coupled with the general trend of wide spread of technologies such as hybrid cloud, multi-cloud architecture, big data, Internet of things, edge computing, etc., which makes the enterprise IT architecture evolve from an IDC-centric star structure to a decentralized mesh structure. Any user, any device, can access enterprise applications located on IDC and the cloud at any location. The traditional boundary of the internal and external networks of the enterprise has been broken, greatly increasing opportunities for attacks.

The traditional intranet traffic, that is, the default and trusted boundary trust model and boundary security protection approach, have been unable to adapt to the new enterprise IT architecture, exposing significant security vulnerabilities. For example, once the VPN gateway connecting the internal network and the external network is breached, there is little to none adequate security measure to prevent the attack from reaching the enterprise digital assets.

With the accelerated failure of traditional boundary security, there is an urgent need for enterprises to build a new network security system integrated with digital services. The SASE (secure access service edge) model proposed by Gartner has become a technology trend attracting increasing attention from enterprises. SASE integrates WAN capabilities with comprehensive network security capabilities to achieve a fundamental transformation of the core of the security architecture from a data center to an identity-based approach.

In its latest report, Gartner predicts that by 2024, 30% of enterprises will adopt cloud based SWG, CASB, ZTNA and branch FWaaS capabilities from the same vendor, up from less than 5% in 2020. By 2025, at least 60% of companies will have clear strategies and timetables for SASE adoption, including users, branch offices, and edge access, up from 10% in 2020.

Observing this market trend, more network security vendors are accelerating their deployment in SASE by releasing various solutions. The key components SASE include SD-WAN, ZTNA (zero trust network access), SWG (secure Web gateway), FWaaS (firewall as a service), etc. with recent developments in the industry, the technology is on a continues pace to reach maturity.

As a world leading cloud distribution and edge computing company, Wangsu has an inherent advantage in the field of SASE solutions. Wangsu has proposed a 3+X capabilities framework for the implementation of SASE.

3

Edge Computing Capability:

2800+ nodes, edge host, edge container, edge function capability iterations

Security Capability:

WAAP, ZTNA, FwaaS, DNS security, security

X

Open platform

- Open network
- Open security capability
- Open edge capability
- Open security capability access

The “3” represents network capabilities, security capabilities, and edge computing capabilities. In terms of network capabilities, based on the 2800 + global nodes and the high-speed network (SD-WAN) between nodes, Wangsu provides a last-kilometer access experience for end users and the experience of connecting back to the data center (including cloud platform). For security capabilities, with the launch of zero-trust based SecureLink in February this year, Wangsu has successfully established WAAP, ZTNA, FwaaS, DNS security capabilities, and mature security services. In terms of edge computing capabilities, Wangsu’s edge computing platform offers a wide range of applications and mature operation systems in audio and video, Web and vertical application scenarios. In the coming future, Wangsu’s edge security capabilities will also be enhanced with our extensive experience in edge computing.

“X” refers to our open platform. The open platform will open up network capabilities and enable security software and hardware through SD-WAN and POP node resources to provide the optimal full-link experience; open edge capabilities, through open container platforms, provide a third-party operating environment to enable distributed services with professional security capabilities; open security capabilities leverage globally distributed security infrastructure to realize cloud network collaboration with security hardware and data centers. Wangsu will leverage cloud security threat information and intelligence, create comprehensive protection measures with peers and customers. With openly aligned security capabilities, users may access trusted devices, trusted connections and trusted behavior capabilities on the zero-trust framework. Wangsu plans to leverage open security capabilities to connect partners throughout the process to provide enterprises with integrated zero trust SASE services.

Copyright information