网宿科技 | 网宿安全

2021

CHINA INTERNET SECURITY REPORT

Preface

With the polarized ideological and globalized economic development，international competition has extended to the cyberspace, frequent large-scale targeted network attacks towards the industry chain and government agencies ensued as a result. Adding to this plight, the COVID pandemic also exacerbated this fragile network security landscape.

A number of large-scale blackmail attacks, data breaches and supply chain attacks shocked the world in 2021. For example, CNA Financial, the largest insurance company in the United States, suffered a security loophole blackmail attack, paying a ransom of $40 million two weeks later to restore file access. Global social media platforms including Facebook and LinkedIn were exposed one after another to large-scale data breaches involving hundreds of millions of users; and at the end of the year, an Apache Log4j2 vulnerability known as a "nuclear bomb level" threat was exposed, triggering a global software supply chain security disaster.

Network security has become a major issue in the digital age. In 2021, China successively promulgated a series of network security laws and regulations, including the Data Security Law, the Key Information Infrastructure Security Protection Regulations, the Network Product Security Vulnerability Management Regulations, and the Personal Information Protection Law, which raised data security to the national security level and laid a legislative foundation for enterprises and organizations in data processing and network security. China's data industry has entered a new era in which there are explicit laws to abide by and to follow.

As the world's leading information infrastructure platform service provider and intelligent edge security leader, Wangsu pays close attention to global Internet security dynamics, actively explores network security defense technology, and continues to improve its security defense capability. Wangsu's annual China Internet Security Report has been released continuously since 2016.

In this report, based on the network attacks and events monitored by the Wangsu security platform in 2021, and complemented with Wangsu Security Lab’s extensive network attack and defense experience, we aim to provide enterprises with insights and suggestions regarding network defense technology, network system, data security, compliance, security management and other aspects of relevant information, helping industries deal with the increasingly high incidence of network security threats.

Table of Content

Table of Content

Chapter I. Overview

- This report will interpret various types of attacks in terms of their volume, type, source and industry distribution.
- All data used in the report are provided by the Wangsu security platform, which is subject to change as Wangsu security services and customer types evolve with future trends. Although 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 dynamics 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 2020 and 2021 to interpret and determine the attack trend.
- This report made a major discover on the continuous high incidence of application layer attacks, especially the explosive growth of attacks against API services, and supply chain vulnerabilities also demonstrated a significant impact.

1.1.DDoS attack overview and trends in 2021

- In 2021, the number of DDoS attacks detected by the Wangsu security platform at the network layer and application layer increased by about 60%. The peak bandwidth of DDoS attacks increased significantly.
- One of the traditionally hardest-hit area is the game industry, ranked first in the number and peak level of DDoS attacks in 2021.

1.2. Web application attack overview and trends in 2021

- In 2021, the Wangsu security platform monitored and intercepted 22.982 billion Web application attacks, 2.41 times that of 2020, demonstrating an overwhelming increase in web application attacks.
- The distribution of Web application attack mode is relatively scattered, with illegal request and SQL injection being the most commonly used means for attackers.
- The focus of Web application attacks is also widely distributed. In addition to government agencies, software information services, real estate, finance and other industries have also become major targets of Web attacks.

1.3. Malicious crawler attack overview and trends in 2021

- In 2021, the Wangsu security platform monitored and intercepted a total of 84.771 billion crawler attacks, an average of 2183.52 attacks per second, doubling the figure of the previous year.
- In terms of attack sources distribution, the proportion of overseas attack sources has increased significantly, 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 retail.

1.4. API attack overview and trends in 2021

- In 2021, the Wangsu security platform monitored and intercepted approximately 15 billion attacks against API services, a 3-fold increase over 2020, undoubtedly an explosive growth.
- Malicious crawler remains the main attack method against APIs, accounting for about 50% of all the recorded attacks, but it has decreased compared with the same period last year, and the trend of one dominant attack method tends to weaken.
- Nearly 70% of API attacks are concentrated in the retail and financial industries, accounting for 34.99% and 31.27%, respectively.

1.5. Host security overview and trends in 2021

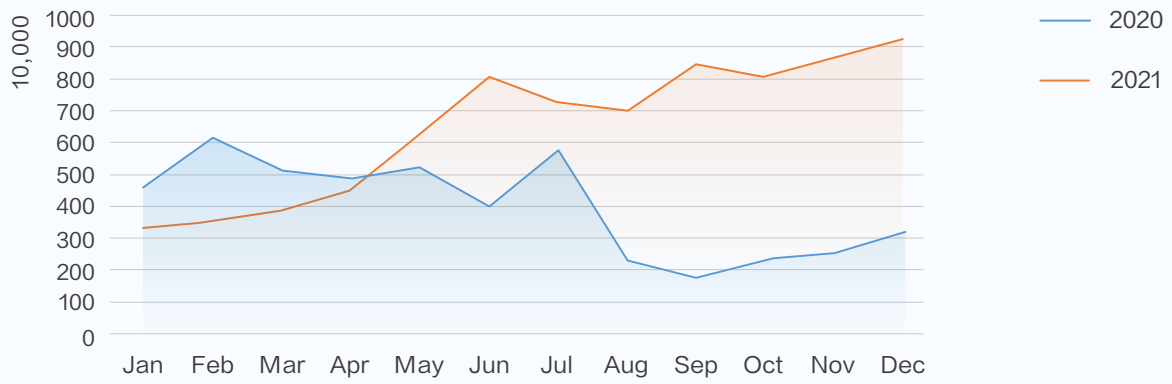
- Wangsu discovered in 2021 that over 60% of enterprise hosts have leveraged container technology, it can be predicted that increasing democratization of common container security requirements will ensue.
- As a result of regular network attack and defense drills, enterprises have significantly improved 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. The number of DDoS attacks saw continued rise and remained at a high level all the way throughout the year.

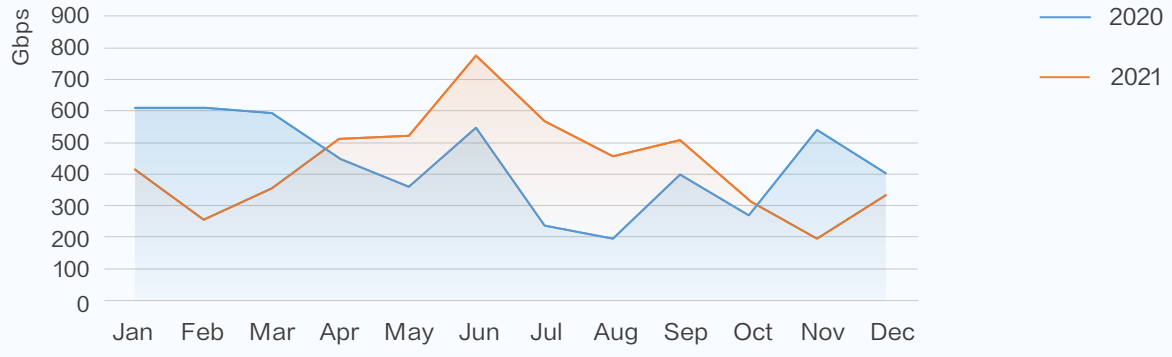
In 2021, the Wangsu security platform monitored and intercepted a daily average of 215,500 network layer DDoS attacks, an increase of 62.96% over the same period last year, and the platform blocked 1.49 billion application layer DDoS attack requests per day, an increase of 61.39% over the same period last year.

2-1 Monthly Distribution of Network Layer DDoS Attacks 2020/2021



Based on the monthly trend, the number of network layer DDoS attacks showed a sustained growth momentum in 2021, with the largest increase experienced from April to June,.

2-2 Monthly Distribution of Peak Network Layer DDoS Attacks 2020 / 2021



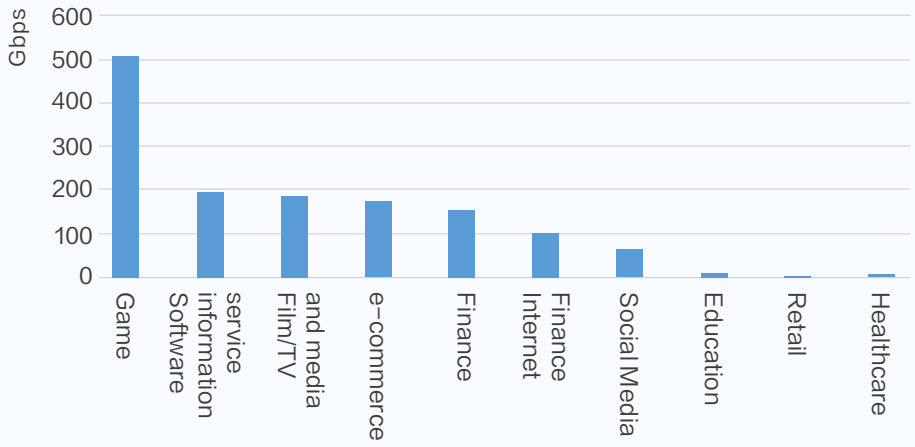
The peak of DDoS attack bandwidth in 2021 occurred in June, reaching 774.58Gbps, which was 26.42% higher than the peak of 611.73Gpbs in 2020. This peak also occurred in a different month from that of previous years, with attacks peaking in January in the past, while this year's monthly attacks began to rise in February and peaked in June.

It is worth mentioning that in January 2022, the Wangsu security platform experienced an ultra-high-traffic DDoS attack with a peak bandwidth of 2.09Tbps and managed to successfully defended against this, while scale of attack scale reached an all-time high.

2.2. Nearly 70% of DDoS attacks targeted game and e-commerce industries.

2-3 Industry Distribution of DDoS Attacks 2021

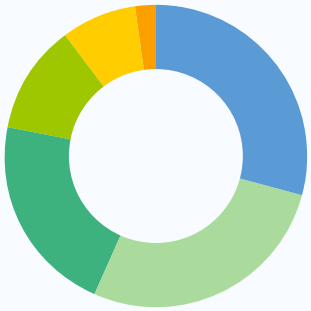
In terms of industry distribution of DDoS attacks, the game industry suffered the largest number of DDoS attacks in 2021, accounting for 50.53%, surpassing all other industries. E-commerce occupies the second place with 16.25%. Both industries combined accounted for almost 70% of the attacks. The third and fourth places are software information service (11.09%) and education industry (6.26%).



2-4 Top 10 Industries of DDoS Attack Peak 2021

According to the statistics of the peak bandwidth of attacks suffered by various industries, the game, software information services, film/television and media information, e-commerce industries are the top four targets, with peak attacks of the game industry surpassing 508Gbps. Under the influence of the "study load reduction" policy of the education industry, the business scale and investment of online education have both declined in 2021, and the scale of attacks has also declined accordingly. The number of DDoS attacks and the industry distribution of attack peaks reflected a trend of industry cross-over attack behavior.

2.3. NTP reflection amplification attacks leading the trend



2-5 Distribution of Reflection Amplification Protocol Attacks 2021

As a type of DDoS attack with great attack power at low cost, reflection amplification attack is favored by attackers. Based on the analysis of the reflection amplification attack requests captured by the Wangsu security platform in 2021, it is found that SSDP, NTP, Memcache, DNS and LADP are still the five most active reflection attack protocols.

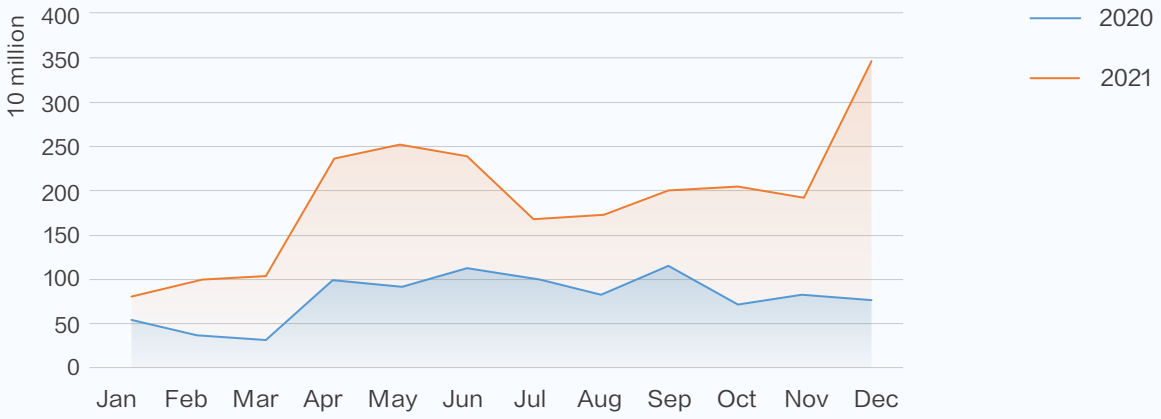
But unlike the previous year, NTP reflection amplification attack has sprung up, surpassing the previously dominant SSDP protocol and leaping to the first place. NTP (Network Time Protocol) is when attackers make use of the publicly accessible NTP server and the UDP protocol to send data without prior connection to launch a large traffic attack on the target site server. The rise in activity of NTP reflection amplification attacks indicates that there are a large number of improperly configured NTP servers exposed on the public network and exploited by hackers.

Chapter III. Interpretation of Web Application Attack Data

3.1. Web application attack volume doubles year-on-year

In 2021, the Wangsu security platform monitored and intercepted a total of 229.83 billion Web application attacks, exceeding the number of attacks for 2020, an increase of 141.30% over the same period last year and showing a doubling trend, indicating that the threat of such attacks continues to rise.

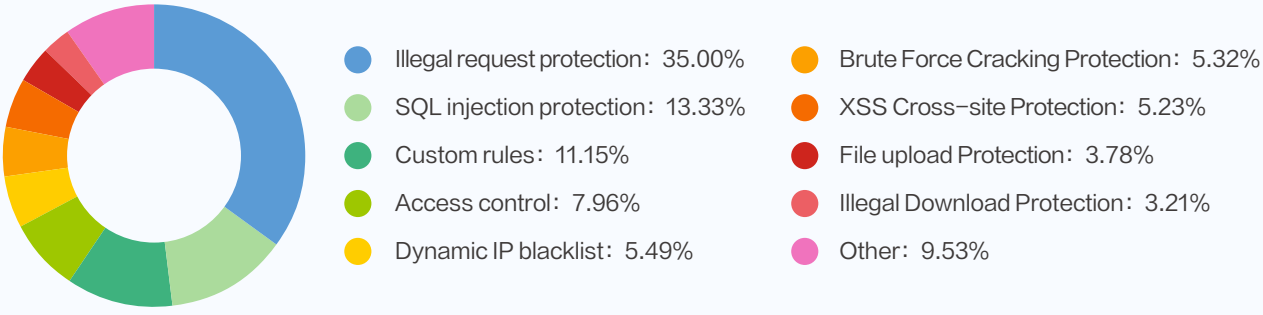
3-1 Trend of Web Application Attacks in 2020 and 2021



Web application attacks double year-on-year and increase in the value of enterprise data assets, high incidence of Web vulnerabilities, and an increase in attacks launched for political purposes in the current global political landscape, all these factors have contributed to the sustained and rapid growth of Web application attacks. From the perspective of attack behavior, the main target of Web application attack is to steal data. with the implementation of relevant laws and regulations such as the Data Security Law and personal Information Protection Law in 2021, if enterprises or organizations fail to establish an effective line of defense for network security, they will face not only the economic risk of data breach, but also legal ramifications.

3.2. Diversification of web attack methods

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



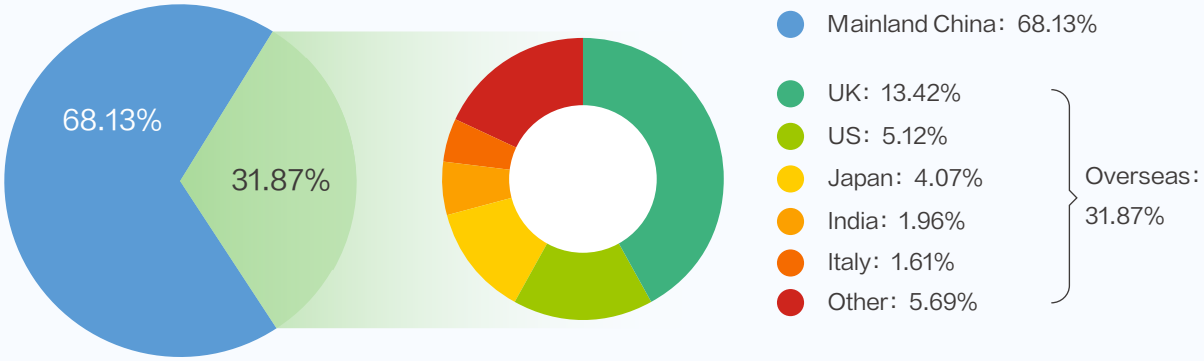
3-2 Distribution of offensive and defensive means of Web applications 2021

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 method protection (35.00%), SQL injection protection (13.33%), and custom rules (11.15%).

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

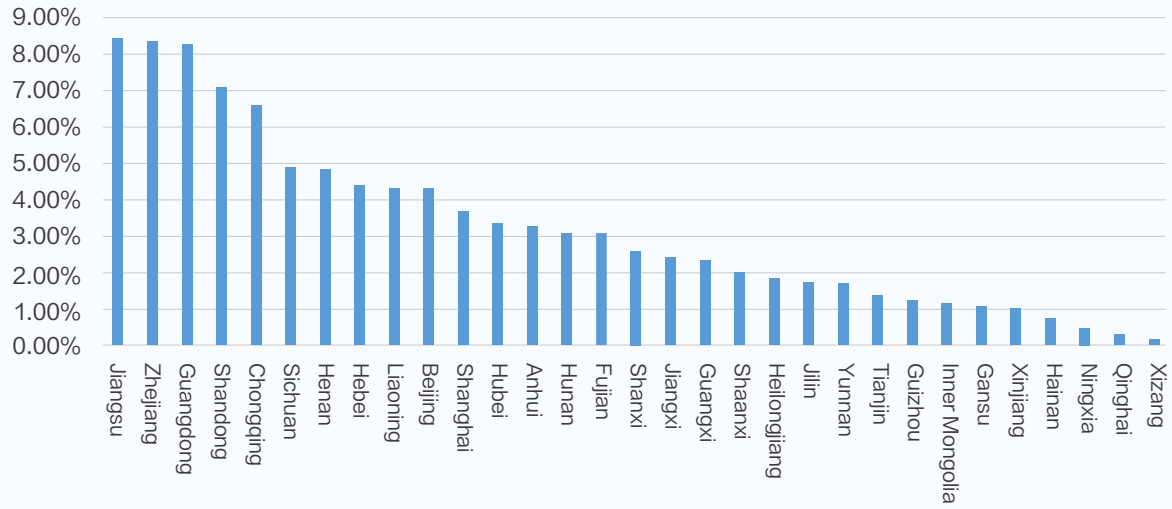
With increasing attacks from automated scanners. The Wangsu security platform identifies web scanners through attack source feature analysis, behavior pattern recognition, etc., and can directly filter out most of the scanner attacks through illegal request method protection, access control (7.96%), dynamic IP blacklist (5.49%), 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. Significant increase of attacks from overseas



3-3 Global Source Distribution of Web Application attacks 2021

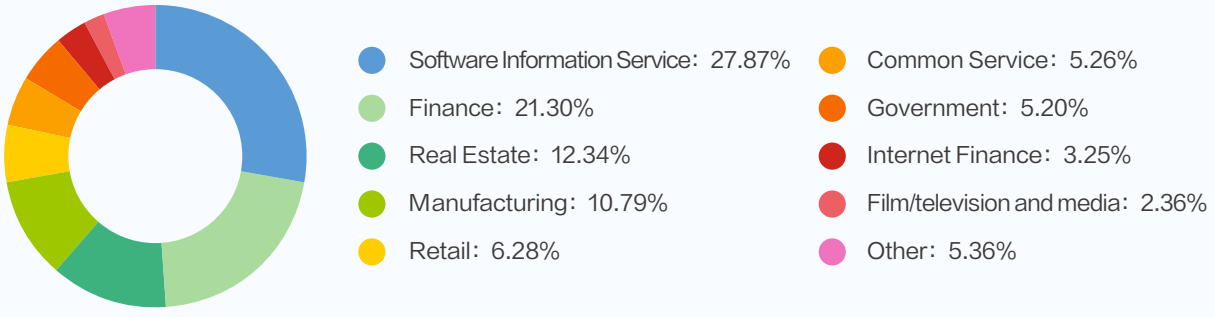
Through the statistics of the geographical location of attacking IP, it is found that the number of IP attacks by Web applications from s in 2021 soared by 357.16% compared with the same period in 2020, and the proportion of global attack sources also increased from 13.30% in 2020 to 31.87%, an increase of about 19%. The sharp rise in overseas Web attacks is speculated to be related to the increasingly tense geopolitical situation all over the globe.



3-4 Distribution of Attack Sources of Web Applications from Mainland China 2021

Statistics on the distribution of attack sources in Chinese mainland provinces show that the top 15 provinces accounted for more than 75% of attack sources in 2021. Jiangsu, Zhejiang and Guangdong are still the top three sources of attack in China, accounting for 10.64%, 8.62% and 7.77%, 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 6 billion attacks.



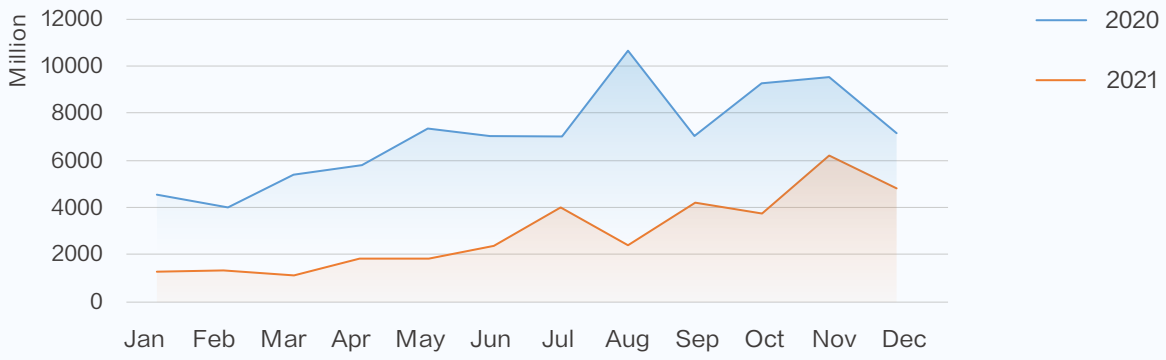
3-5 Industry Distribution of Web Application attacks 2021

According to the attack data in 2021, software information services and finance have become the industries with the largest number of Web application attacks, with nearly 11.2 billion Web attacks against them, accounting for almost half the amount of attacks in 2021. Real estate (12.34%), manufacturing (10.79%) and retail (6.28%) ranked third, fourth and fifth, respectively.

Chapter IV.
Interpretation of Malicious Crawler Attack Data

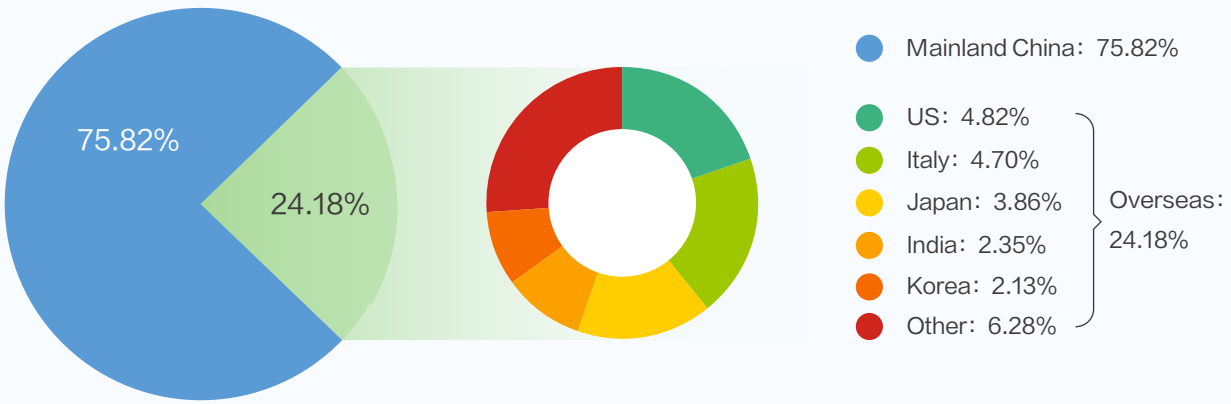
4.1. On average 2688 crawler attacks occur for every second, doubling for consecutive years

4-1 Malicious crawler attack trand of 2020/2021



n 2021, the Wangsu security platform monitored and intercepted a total of 847.71 billion crawler attacks, an average of 2688 attacks per second, surpassing the record of 2020 by 236%. The attack volume of malicious crawlers has doubled in the last three consecutive years, posing an increasingly significant security threat.

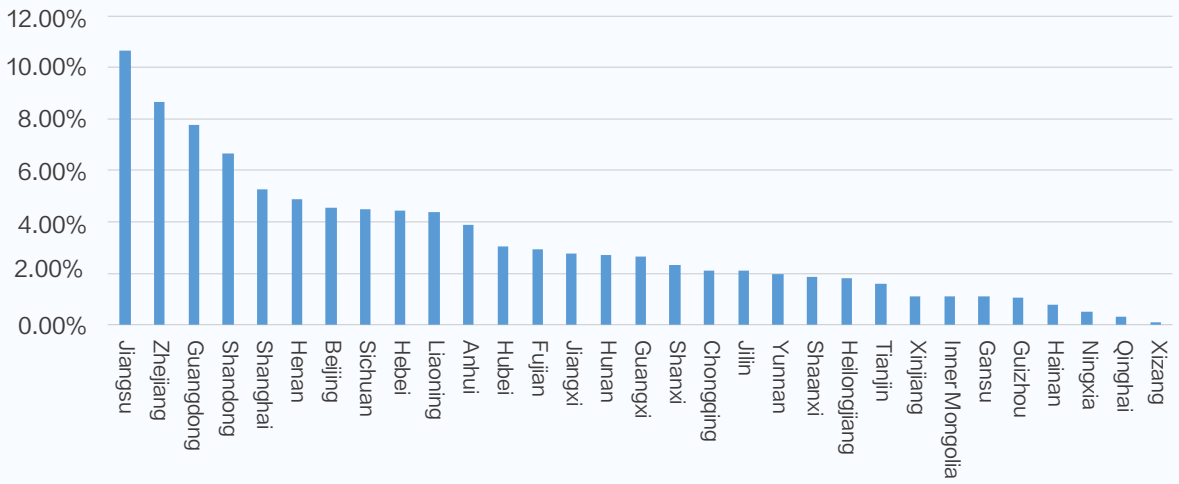
4.2. Significant rebound in proportion of overseas attack sources of malicious crawlers



4-2 Global malicious crawler attack source distribution 2021

According to the distribution of source IPs monitored and intercepted by the Wangsu security platform, more than 70% of malicious crawler attacks in 2021 came from domestic locations, The proportion of overseas attack sources increased to 24.18% from 7.08% in the same period last year.

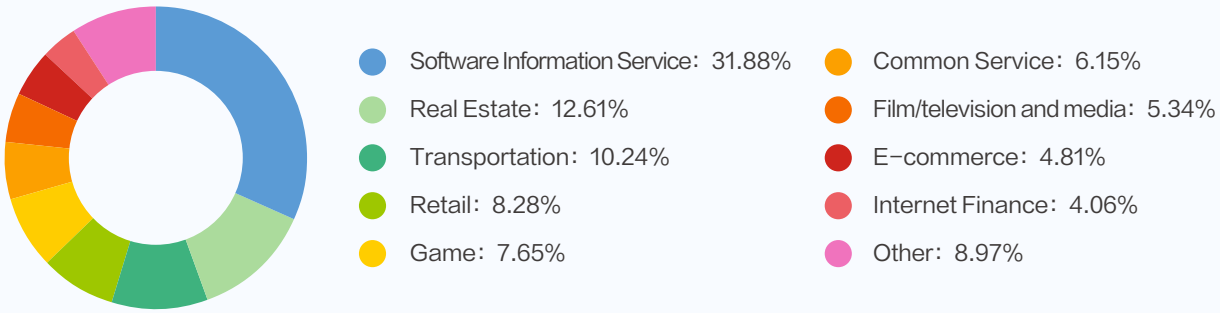
The proportion of overseas attack sources has increased significantly, which is speculated to be related to the recovery of purchasing agents and overseas shopping industry. The recovery in purchasing agents, overseas online shopping and other industries, and the rebound in demand for overseas merchants to crawl competitors' goods, prices and other information for sales strategy analysis are evident.



4-3 Malicious Cralwer Attack Source Distribution of Mainland China 2021

The number of malicious crawler attacks in Jiangsu, Zhejiang and Guangdong was 10.64%, 8.63% and 7.77% 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.

4.3. Malicious crawler attacks are scattered in the industries



4-4 Inidustry Distribution of Malicious Crawler Attack 2021

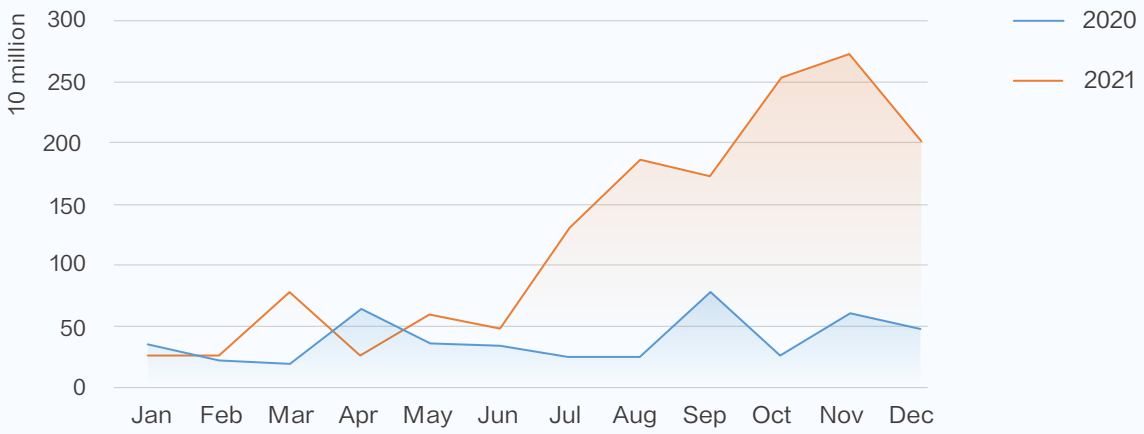
The industry distribution of malicious crawler attacks shows a trend of low concentration and are more evenly spread. The most attacked industry was the software information service industry (31.88%), followed by the real estate industry (12.61%), transportation (10.24%), retail (8.28%) and game (7.65%) ranked third to fifth respectively.

Among them, the ranking of transportation returned to the top three from the sixth place in 2020, 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. API threat outbreak with number of attacks increased by more than 200% over 2020.

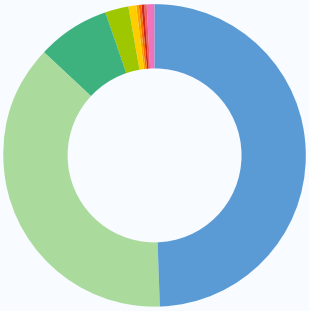
5–1 API Attack Trend of 2020 and 2021



In 2021, the Wangsu security platform monitored and intercepted 14.798 billion attacks against API services, averaging 469 attacks per second, a 3-fold increase over 2020, undoubtedly an explosive growth. In particular, in the second half of 2021, the number of attacks jumped sharply.

Under the background of digital transformation, more APIs are opened to enterprises, and the risks they are facing are getting increasingly higher. API business has gradually become the target of many hackers.

5.2. Diversification of API attack methods



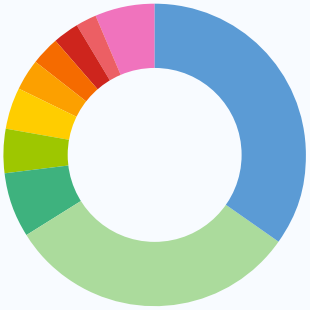
- Malicious Bot：49.49%
- Illegal Request：37.66%
- Brute Force Cracking：7.72%
- SQL Injection：2.50%
- File Upload：0.88%
- Remost File Inclusion：0.33%
- Cross Site Script：0.28%
- Threat Intellifence：0.22%
- Third-party Component：0.18%
- Other：0.73%

5-2 Distribution of API attack methods 2021

In the attacks against API service, malicious crawler remained the most proponent attack method. In terms of API attack data in 2021, malicious crawler attacks accounted for 49.49% of the total number of attacks, down significantly from the same period last year.

The second and third places were illegal request (37.66%) and brute force cracking (7.72%). Among them, brute force cracking is mostly used for account APIs, which seriously threatens the security of personal assets. In general, the types of attacks against API services tend to be diversified.

5.3. The retail industry and the financial industry have become the hardest hit areas of API attacks.



- Retail：34.99%
- Finance：31.27%
- Software Information Service：6.98%
- Real Estate：4.62%
- Government：4.53%
- E-commerce：3.44%
- Transportation：2.91%
- Film/television and media：2.72%
- Internet Finance：2.35%
- Other：6.20%

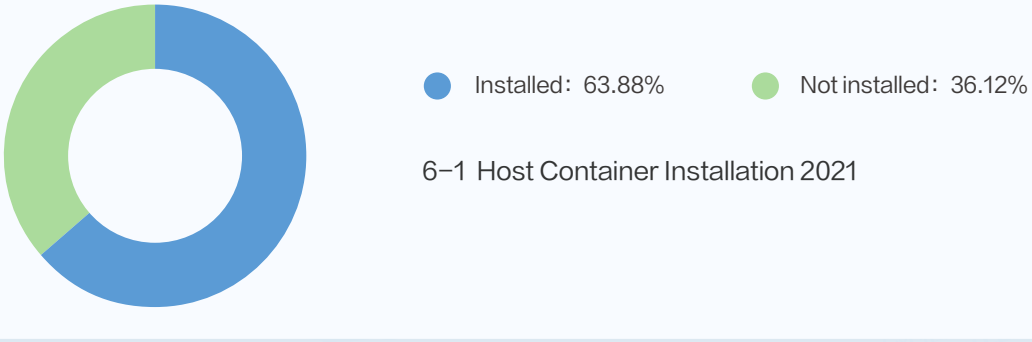
5-3 Industry Distribution of API Attack 2021

In 2021, the retail industry has suffered the most API attacks, accounting for 34.99% of the total attack volume. The financial sector ranked second with 31.27%.

The retail and financial industries have accounted for nearly 70% of API attacks, indicating that these two industries with intensive digital transformation are also the first to bear the brunt of API attacks. There has been a small increase in the proportion of transportation, which is directly related to the increase in cross-regional and cross-border passenger flow brought about by the alleviation of the pandemic compared with 2020.

Chapter VI. Interpretation of Host Security Data

6.1. Sharp increase in application of container technology

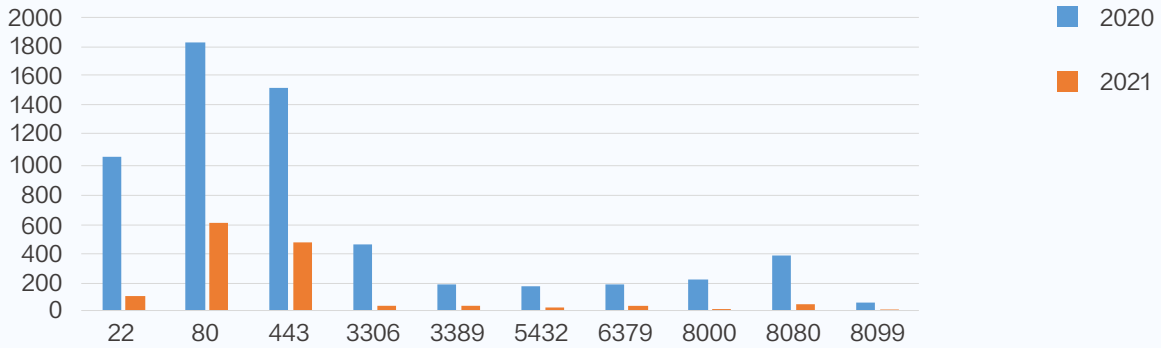


6-1 Host Container Installation 2021

Wangsu security probe detection has found that 63.88% of enterprise hosts have installed container-related software, an increase of approximately 24%. It can be predicted that the demand for container security will be increasing 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 2020 and 2021



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 2021 compared with 2020.

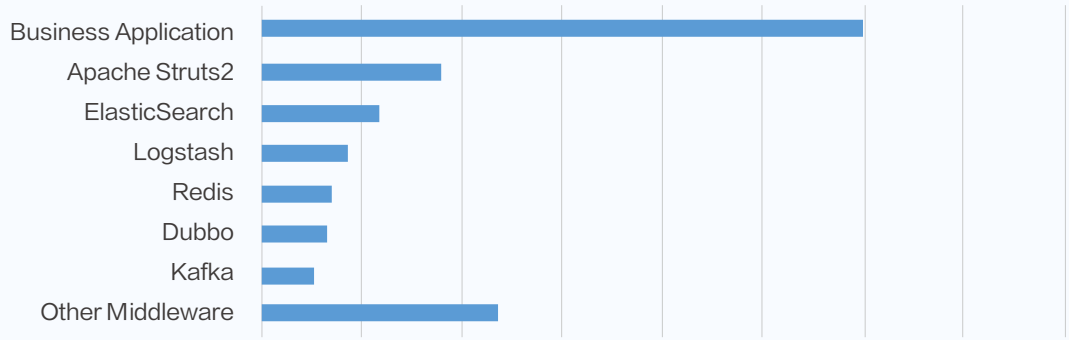
The decline in the number of public network open ports is mainly due to regular network attack and defense drills, which effectively improves the standard of the use of management ports. After the attack and defense drills, the number of open ports in the public network is still kept at a low figure, indicating that the attack and defense drills can improve enterprise security management and security awareness, and port management is also more normalized, resulting in a substantial reduction in scope of attack.

6.3. Log4j2 vulnerability is the "Nuke" of all attacks

6-3 Top 10 high-risk Vulnerabilities Captured by the WANGSU Security Platform 2021

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.

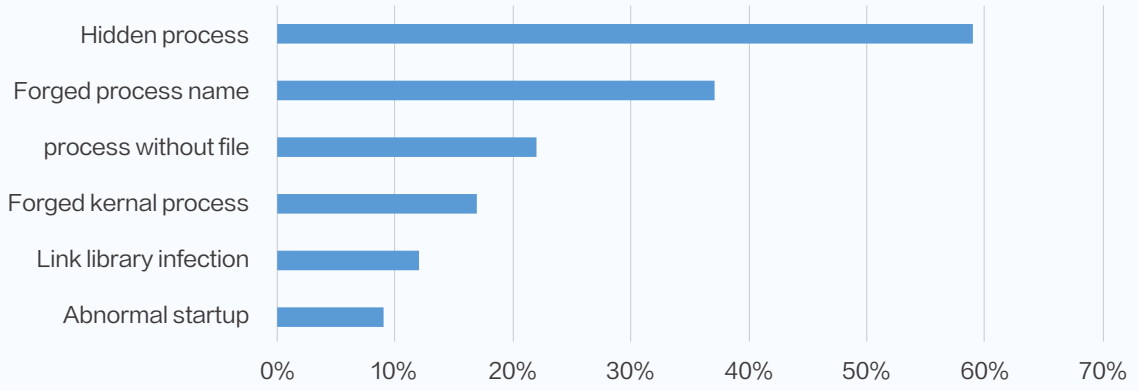
It is worth noting that the impact of the Apache Log4j2 remote code execution vulnerability (CVE-2021-44832) is enormous. As of December 31, 2021, which is the end of the statistical cycle of this report, only two weeks after the vulnerability was published, the number of intrusions exceeded the total number of intrusions caused by the 2nd-9th high-risk vulnerabilities combined. And the way of exploiting the Log4j2 vulnerabilities is still changing, and the updated official releases continued to face new bypass methods. The vulnerability information needs to be tracked continuously in order to accurately grasp the range of assets that may be affected by it.



6-4 Middleware affected by Log4j2 in 2021

Using the asset collection module of the Wangsu host probe to analyze the influence surface caused by the middleware affected by Log4j2 remote code execution vulnerabilities, it is found that Log4j2 components are widely used in business applications, and the range of hosts affected is the widest; Log4j2 is also common in Struts2, ElasticSearch, Logstash, Redis, Dubbo, Kafka and other popular middleware, and the total number of hosts affected by these middleware accounts for 36.13%.

6.4. Process concealment makes it difficult for manual Intrusion Detection



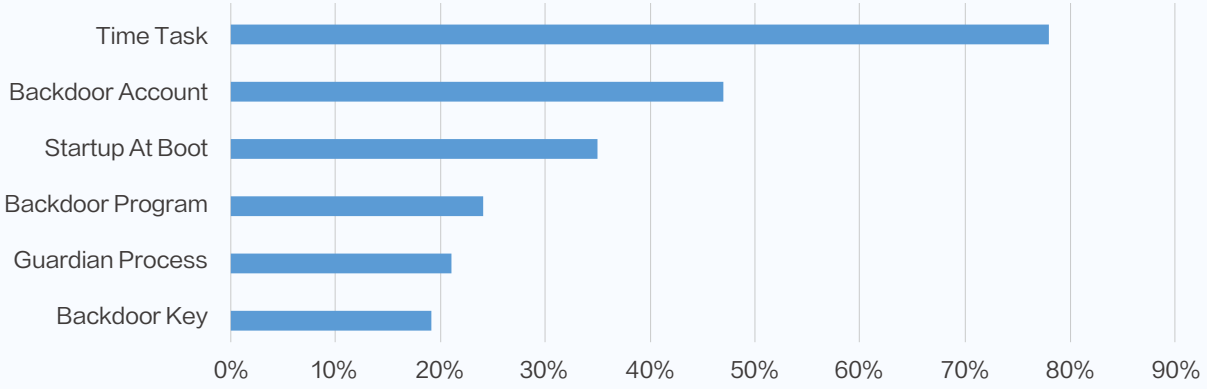
6-5 Detection Rate of Abnormal Behavior in Process 2021

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. The Wangsu host probe has detected this technology in more than 50% of intrusions. Process concealment technology can make it impossible for emergency responders to discover malicious processes and increase the difficulty of intrusion analysis.

Behaviors such as no file process, abnormal startup mode, and link library infection account for 10% to 30% of intrusions. These technologies are able to avoid the detection of security software, so that the security software can not analyses the contents of the process files and were unable match with the virus feature library.

6.5. More than 70% of intrusions leveraged timed task implementation to maintain permissions.



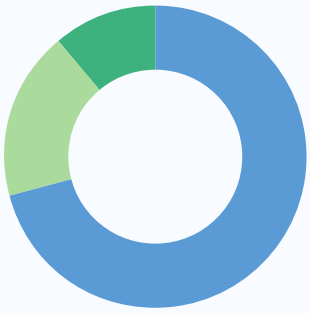
6-6 Detection Rate of Permission Sustainment Behavior 2021

Through the detection and analysis of the malicious behavior identified by the Wangsu host probe, the permission sustainment attack method is used in 95% of the intrusions. Among them, the proportion of malicious scripts and programs running through timed tasks is the most prominent, as high as 78.12%, followed by backdoor account (46.58%) and boot (35.35%).

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. Rootkit with strong compatibility and little impact on the system is favored by attackers

Rootkit is the most powerful malware 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.



6-7 Distribution of Rootkit Types 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 70.87%, followed by preloading link library (18.08%) and LKM kernel module loading (11.05%).

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. Common executable files, such as ps, top, and sshd, can be replaced to hide the process, as well as for other purposes such as backdoors.

Although the LKM kernel Rootkit is highly concealed and powerful, it can flexibly hide processes, networks, Rootkit itself and files. However, 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

Network Threats and Attacks are Constantly Changing 。As can be seen from the content presented in this report, the offensive and defensive dynamics shown in the data of 2021 indicated some different characteristics compared with 2020. It can be seen that when enterprises are building a network security defense system, they need to adjust their protection mindset and strategies at all times in accordance with the developing trend of attack technology in order to effectively defend against attacks.

I. With Aggravated Risks of the Software Supply Chain, an Urgent Need Arose for Enterprises to Establish Effective Countermeasures

According to the statistics of the Wangsu security platform during the reporting period, the intrusion events caused by the Log4j2 vulnerabilities sweeping the world have accounted for nearly half of the total number of host security intrusion events, and the attack targets include open source software that relies on this component and software platforms developed within the enterprise.

As an open source tool used by a large number of business frameworks, the harm of Apache Log4j2 vulnerabilities can be said to be the "nuke" of attacks. Soon after the vulnerability was exposed, the exploitation of the vulnerability spread widely online, causing a large-scale intrusion. So far, the impact of the vulnerability is still brewing, and the negative impact is expected to continue for the foreseeable future.

Sonatype, the world's largest repository provider of open source components, calculated in its 2021 State of the Software Supply Chain Report that software supply chain attacks in the world increased by 650% in 2021. Gartner also predicts that 45% of global companies will suffer software supply chain attacks by 2025, a threefold increase from 2021. Modern enterprise software is mostly in hybrid code. Due to the open sharing of open source software, many organizations use high-quality and free open source components as part their software products. With the digital transformation of global industries, enterprises are increasingly dependent on open source software. Any vulnerabilities in any lower-level open source component will have an extensive impact of attacking one entity and causing damage to many.

How should enterprises effectively deal with the massive security risks caused by vulnerabilities in the open source software supply chain? The Wangsu security lab recommends a combination of solutions for protection with comprehensive means. At the initial stage of vulnerability exposure, asset collection and vulnerability detection can be carried out through host security products to quickly locate software vulnerabilities and promote vulnerability application upgrades at the earliest opportunity; at the same time, virtual patches provided by Web application protection products are used to intercept attacks and exploits aimed at this vulnerability. In the stage of application development, software component analysis (SCA) technology can be used to strengthen security control before the application is launched, so as to prevent the application from going live with shortcomings.

II. Data Arose to the Height of National Strategy, and the Risk of API Data Security is Prominent, it is Urgent to Strengthen Comprehensive Prevention and Control

The business security threats identified in our 2021 H1 report continued to escalate and continued for the rest of 2021. Among them, the explosive increase in API attacks is particularly striking, with an increase of more than 200% compared with 2020. The main goal of attackers is to obtain enterprise data. In the API economy, the number of APIs saw explosive growth. The API access environment is becoming more open, and the value of data transferred through APIs is also rising, which drives the trend of API attacks higher.

By opening APIs to partners and customers, more enterprises and organizations share data, algorithms, transactions, processes and other business functions with the business ecosystem to explore new sources of value generation and build new core competencies. For example, the "open bank" strategy of the banking industry is a typical case of opening up the interface of financial services to various industries and promoting the transformation of the industry. However, open APIs also increased the risk of data privacy and security, which is directly reflected by the high number of API attacks in the financial industry.

Furthermore, there is a widespread misalignment between the fast-growing API business and the weak API protection and control mechanism among enterprises. Only relying on rule-based application vulnerability protection, it has been unable to deal with attackers launching attacks on normal business interfaces or forgotten zombie APIs by means of excessive request and unauthorized access, so as to achieve the purpose of stealing or tampering with data at scale.

Coupled with the successive promulgation of the Data Security Law and the Personal Information Protection Law in 2021, it has become a legal obligation for enterprises to take necessary measures to protect data security and personal privacy information. The Wangsu Security Lab recommends that enterprises adopt advanced API protection products that can automatically discover API, leverage API access behavior detection features, and support API lifecycle management, which will help to eliminate hidden dangers of zombie APIs, prevent unauthorized calls and excessive calls, and ultimately ensure data security. On this basis, it is recommended to select vendors that support WAAP (cloud Web applications and API protection) solutions, combined with Web application firewall, DDoS protection, and crawler management capabilities to establish a comprehensive defense capability against API attacks, Web application attacks, etc.

The Wangsu WAAP solution provides extensive insight into user scenarios, integrates DDoS cloud cluster, WAF, BotGuard and API security and management capabilities to achieve full-stack coordination and unified management based on a globally distributed platform, and provides advanced WAAP services from a user perspective by combining business flow analysis, AI models, illicit activity intelligence, vulnerability threat intelligence, and marketing risk control model.

III. Enterprises Accelerate the Shift to Zero Trust, Driving the Need for Secure Seamless Integration and SASE

TAs the world entered the third year of the COVID-19 pandemic, and enterprises have been intensifying their practice in telecommuting, business on the cloud, attack defense etc. More enterprises realized that the traditional network security protection boundary continued to disintegrate, and shifted their wait-and-see attitude towards the current popular Zero Trust protection technology, starting with gradually replacing VPNs with ZTNA (zero-trust network access), formulating strategies and time tables, and transforming to a new generation of network security model.

In the process of upgrading security protection technology, the complexity of aligning with different suppliers, policies and consoles places pressure on the implementation of enterprise security technology. It will gradually become a trend for enterprises to integrate suppliers and seamlessly integrate policies and consoles. Gartner predicts that by 2024, 30% of enterprises will adopt cloud based SWG (secure Web gateway), CASB (cloud access security broker), ZTNA and FWaaS (firewall as a service) capabilities, up from less than 5% in 2020.

After undertaking the integration of security functions, the next step is to complete the integration of WAN functions, which achieves the goal of SASE (secure access service edge), which is the integration of WAN functions and comprehensive network security functions.

As a next-generation network security model gaining increasing interest from the security industry, SASE can empower infrastructure, operations and security teams to provide extensive network and network security services in a consistent and integrated manner, supporting digital business transformation, edge computing and mobile office requirements. Observing this market trend, network security vendors are accelerating their deployment in SASE by releasing various solutions. The key to its competitiveness is whether it can support the functions of the above key components of SASE more completely and maturely.

As an intelligent edge security leader, in October 2021, Wangsu innovatively proposed a SASE implementation model based on the capability framework of "3+X". The "3" is composed of security capability, network capability and edge computing capability, and "X" refers to the open platform.

3

Network Capability: Global POP Nodes, SD-WAN

Security Capability: WAAP, ZTNA, FwaaS, DNS Security, Security Services

Edge Computing Capability: 2800+ Nodes, Continued iteration of Edge Host, Edge Container, Edge Functions

After nearly six months of development, the capabilities of "3+X" continues to evolve:

In terms of security capability, following the release of Wangsu's ZTNA (Zero Trust Network Access) SecureLink product in February 2021, Wangsu further upgraded its product capabilities to establish a **"3+1" security access system**, that is, "3" trusted principles of trusted identity, trusted device and trusted behavior, in combination with "1" platform of security capabilities built from the aspects of encrypted transmission, edge protection and application concealment. Ensuring that remote or local office workers may access corporate resources with peace of mind.

Subsequently, revolving around the basis of extensive DDoS protection, cloud WAF and Bot protection capabilities, Wangsu also launched its **API security and management product**, based on API business characteristics, providing automated API discovery, API lifecycle management and continuous security detection capabilities, forming a closed loop of management-protection-analysis services, and completing the final puzzle piece for WAAP (cloud Web application and API protection) capabilities. At this point, **Wangsu has become fully capable with WAAP, ZTNA, FwaaS, DNS security capabilities, as well as a number of mature security expert services.**

In terms of network and edge computing capabilities, the high-speed network (SD-WAN) between 2800+ edge nodes around the world not only effectively ensures the last kilometer access experience of end users and the experience of returning to the data center (including cloud platform), but also created a new generation of CDN programmability to transfer the business logic originally handled by the origin site to the CDN edge nodes. Wangsu supports users to combine various personalized edge business like building blocks to rapidly complete the global deployment of new applications or services, greatly shortening the development cycle, and further reduced the load on the origin site.

In the future, based on the three capabilities of continuous evolution, Wangsu security will further expand it's open ecosystem, make use of the massive data of the network to open up cloud security threat information, and combined with upstream and downstream security technologies and the existing security defense systems of enterprises to form a three-dimensional protection mechanism, to achieve the goal of integrated SASE security service, and maintain network security with all stakeholders.

Copyright information