CDNetworks

State of Web Security H1 2022

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

Table of Contents

Preface 4

About This Report 5

Key Findings 5

Unrelenting DDoS Attacks 5

Significant Increase in Supply Chain Attacks 5

Attackers Launching Greater Numbers of Automated, Intelligent Attacks 6

Explosive Growth of API Security Threats Making Business Logic More Vulnerable 6

Large-scale Telecommuting Exposed Many Security Issues 6

Interpreting of DDoS Attack Data 7

Significant Increase in Attack Volume with Attack Intensity Reaching an All-time High 7

Peak of Internet Access In-sync with Peak of DDoS Attacks 8

75% of Attack Traffic Comes from UDP Attacks That Produce Reflection Amplification 9

Gaming Remains a Major Target of DDoS 10

Interpreting of Web Application Attack Data 11

Web Application Attack Growth Slowing Down 11

Violation of HTTP Protocol Becoming the Preferred Choice of Attack 11

The Internet Finance Industry Has Become the Top Target 12

Interpreting of Malicious Bot Attack Data 13

Attack Volume of Bots Doubled in Consecutive Years. 13

Threat of Meticulously Disguised Intelligent Bots on the Rise 14

More Than Half of Bot Tools Use the Chrome Kernel 15

Hardest Hit Areas: Software Information Services, Transportation, Retail Industry 15

Illicit Perpetrators Have Made Extensive Use of Meticulously Disguised Bots for Business Fraud 16

Interpreting API Attack Data 17

Extremely Significant Risk of Malicious Use of API Parameters 17

Hardest Hit Areas: E-Commerce, Film/TV and Media Information, Transportation Industry 19

Interpreting of Enterprise Telecommuting Security Data 19

BYOD with Weak Security Measures Account for Nearly 30% of All Scenarios 20

End-users Continue to Underestimate the Importance of Security Awareness 20

Email: sales@cdnetworks.com www.cdnetworks.com

Phishing and Vulnerability Exploitation Provide Critical Means of Network Attack 21
Instant Messaging Ranks First in Causes of Corporate Data Breach 22
Be Vigilant Against Covert Attacks Behind Abnormal Behaviors Such as Unauthorized Access and IP Scanning 22

Interpreting Host Security Data 23
Most High-risk Vulnerabilities are Associated with Open-source Ecosystem Components..... 23
Proportion of Fileless Processes Greatly Increased Among All Abnormal Processes..... 24
More than 80% of Intrusions Leveraged Timed Task Implementation to Maintain Permissions..... 25

Insight and Recommendations for Future Trends..... 26

 Email: sales@cdnetworks.com www.cdnetworks.com

Preface

In 2022, the perfect storm created by international conflicts and the COVID-19 pandemic gave rise to an escalation in global cyberspace attacks. To date, large-scale targeted cyberattacks continue to increase unabated. The 2022 Global Risks Report, released by the World Economic Forum in early 2022, listed the rise of cybersecurity risks as one of the major risks facing the world in 2022.

It comes as no surprise, then, that data security and compliance have become one of the top network security concerns in the first half of this year. Driving this concern is the large number of data breaches that occurred in H1 2022, which impacted organizations around the world. To address this concern, many countries and regions are improving their data security policies and regulations, personal information protection, key information infrastructure protection, and supply chain security.

As a global-leading CDN (Content Delivery Network) and Edge Service provider, CDNetworks pays close attention to global internet security dynamics in its ongoing efforts to explore network security defense technology and improve its security defense capabilities. To that end, CDNetworks shares its findings in its annual State of Web Security, which has been published continuously since 2016.

This report is based on the network attacks and events monitored by the CDNetworks' security platform in H1 2022. The findings in this report are complemented with CDNetworks Security Lab's extensive network attack and defense experience. Together, this information is intended to provide enterprises with unique insights and suggestions about current network defense technologies, network systems, data security, compliance, security management, and other relevant information that can help industries cope with the increasingly high number of incidents of network security threats by leveraging our unparalleled expertise.

Email: sales@cdnetworks.com www.cdnetworks.com

About This Report

All data used in the report is provided by the CDNetworks' security platform and is subject to change, as CDNetworks' security services and customer types continue to evolve with future trends. Although these changes may impact trends indicated by the data, they do not affect how CDNetworks interprets or gains insight into security trends, as well as the dynamics of security attacks and defenses and our analysis of them.

The report makes a comprehensive comparison of the attack and defense data in 2022 and H1 2021, including the same period of previous years, to interpret and identify attack trends.

Key Findings

Unrelenting DDoS Attacks

In the first half of 2022, the CDNetworks' security platform monitored on a daily basis 429,000 Distributed Denial of Service (DDoS) traffic attacks at the network layer and 1,170 DDoS Challenge Collapsar (CC) attacks at the application layer. In terms of intensity, the network-layer attacks successfully blocked by the CDNetworks' security platform reached a peak of 2.09 TBPS, while the peak of application-layer attacks reached a global record of 34.7 million RPS. Combined with the current updated peak records of DDoS attacks in the industry, the order of magnitude of 2TBPS at the network layer and 30 million RPS at the application layer is more of a frequent occurrence than an exception. Greater DDoS attack intensity calls for an increase in countermeasures.

Significant Increase in Supply Chain Attacks

During the statistical period covered by this report, the number of web attacks that exploited third-party component vulnerabilities reached 6.2 times that of the same period in 2021. Moreover, the ranking of web attacks jumped from 12th place to 3rd on the list of monitored web attacks. Nearly all of the high-risk vulnerabilities come from open-source third-party components, such as the vulnerability in Apache Log4j2, which allows an attacker to execute code on a remote server. With increasing dependency on third-party open-source components, attacks against hardware and software that rely on these components within the enterprise are expected to rise with broad and far-reaching impact.

Attackers Launching Greater Numbers of Automated, Intelligent Attacks

The number of automated bot attacks detected by the CDNetworks' security platform in H1 2022 more than doubled compared with the same period in 2021. This trend shows no signs of slowing down, as it continues to double in 2022, as spam registration, batch login, database breach, and other bot malware continue to put organizations at risk. Even more disturbing, the number of intelligent bots disguised as legitimate applications increased 3.5 times. Intelligent bots bring greater challenges to man-machine identification methods used to deter such attacks.

Explosive Growth of API Security Threats Making Business Logic More Vulnerable

As a special web service that generates enormous amounts of data, application programming interfaces (APIs) have become a key target of network attacks, and a major avenue of data breaches, in today's API-driven economy. In H1 2022, the attack volume against APIs continued to grow rapidly, increasing by approximately 1.7 times compared with the same period last year. Most attacks were concentrated in E-Commerce, Film/TV and Media Information, Transportation, Software Information Services, and Government Agencies.

Unlike traditional web services, a large number of API attacks targeted vulnerabilities in the design of API services to facilitate unauthorized access, particularly with malicious request parameters. These types of attacks are often difficult to identify with traditional web-protection rules, and must be protected by professional API security monitoring and management solutions.

Large-scale Telecommuting Exposed Many Security Issues

The long-term global impact of COVID-19 has led organizations to accept remote work and cloud-based applications as a viable alternative to the traditional on-premise business model. Nearly 89% of enterprise users who utilize CDNetworks' security services have used remote-access technology, with Bring Your Own Devices (BYODs) accounting for nearly 30% of remote-access use cases.
The widespread adoption of large-scale telecommuting has exposed a number of security issues, such as:

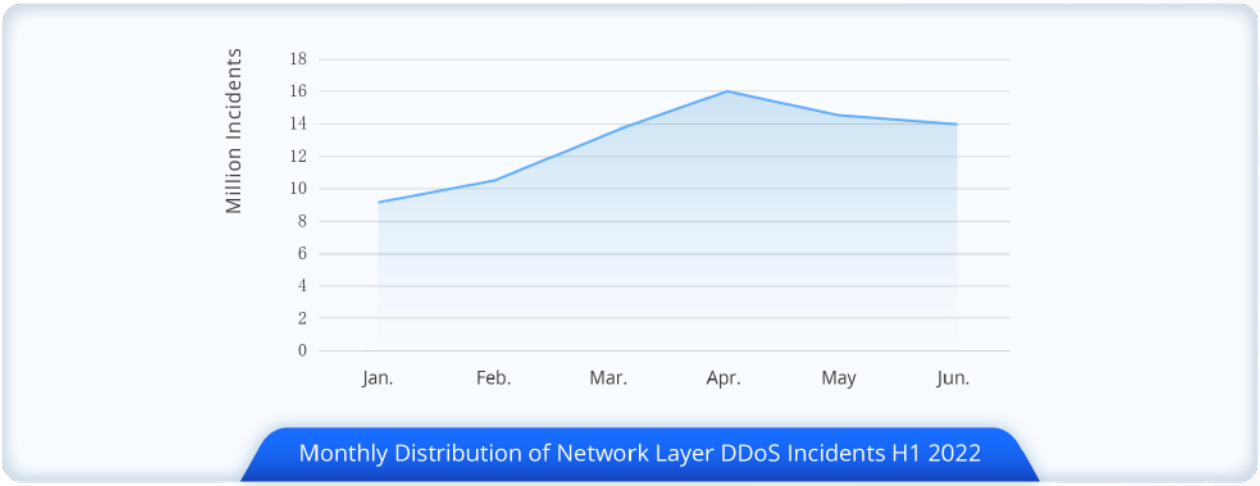
Email: sales@cdnetworks.com www.cdnetworks.com

- Inadequate security awareness by end users about their BYODs, which lowers an organization's security posture
- Intranet applications that are easily captured by phishing, vulnerability exploitation, credential theft, and other threats
- Internal data is breached using tools such as instant messaging and e-mail
- The alarming increase in Advanced Persistent Threat (APT) attacks against office networks

Interpreting of DDoS Attack Data

Significant Increase in Attack Volume with Attack Intensity Reaching an All-time High

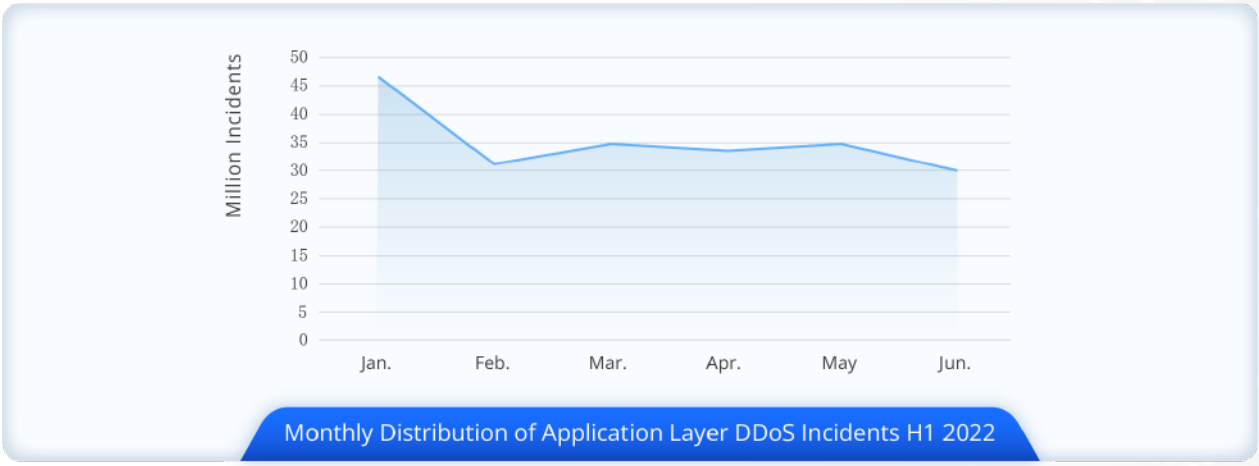
In the first half of 2022, the CDNetworks' security platform monitored and blocked an average of 429,000 network-layer DDoS attacks per day, a substantial increase of 161.02% over the same period last year. The platform also monitored and blocked 1,170 application-layer DDoS attacks per day, and blocked 12,100 application-layer DDoS attack requests every second.



Monthly Distribution of Network Layer DDoS Incidents H1 2022

Examining the monthly distribution of attacks, one can see that DDoS attacks at the network layer increased gradually from January to April, and then decreased slightly, while application-layer DDoS attacks peaked at 46,700 in January, and then fell to a range between 30,000 and 35,000 in the following five months.

Email: sales@cdnetworks.com www.cdnetworks.com

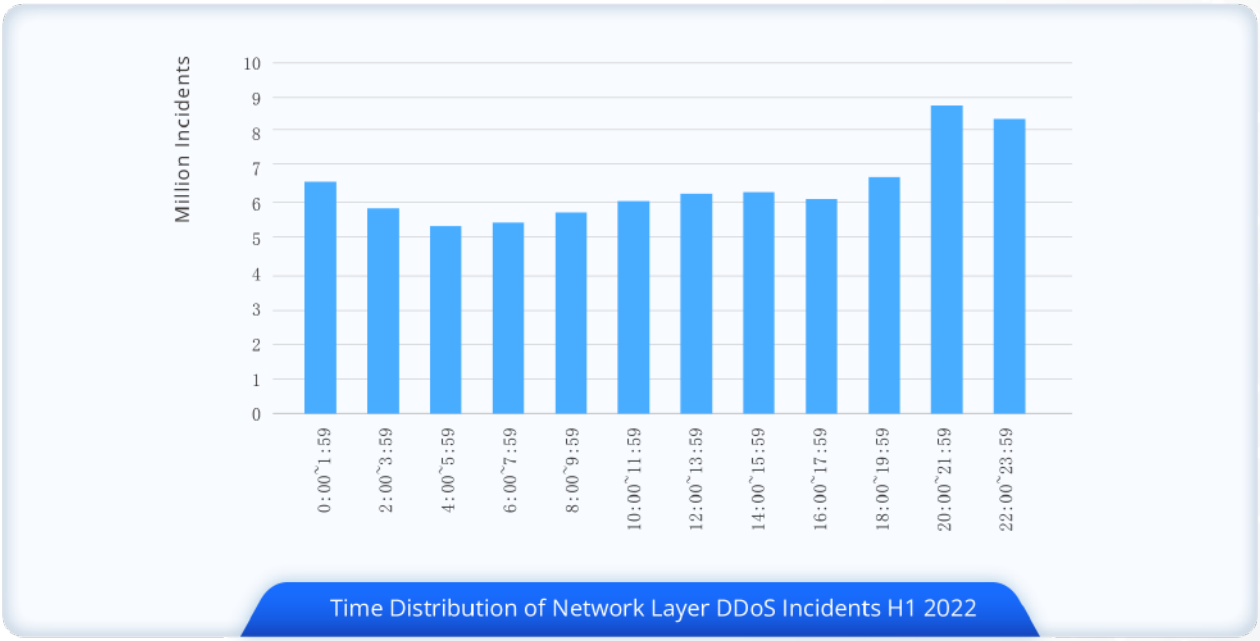


Monthly Distribution of Application Layer DDoS Incidents H1 2022

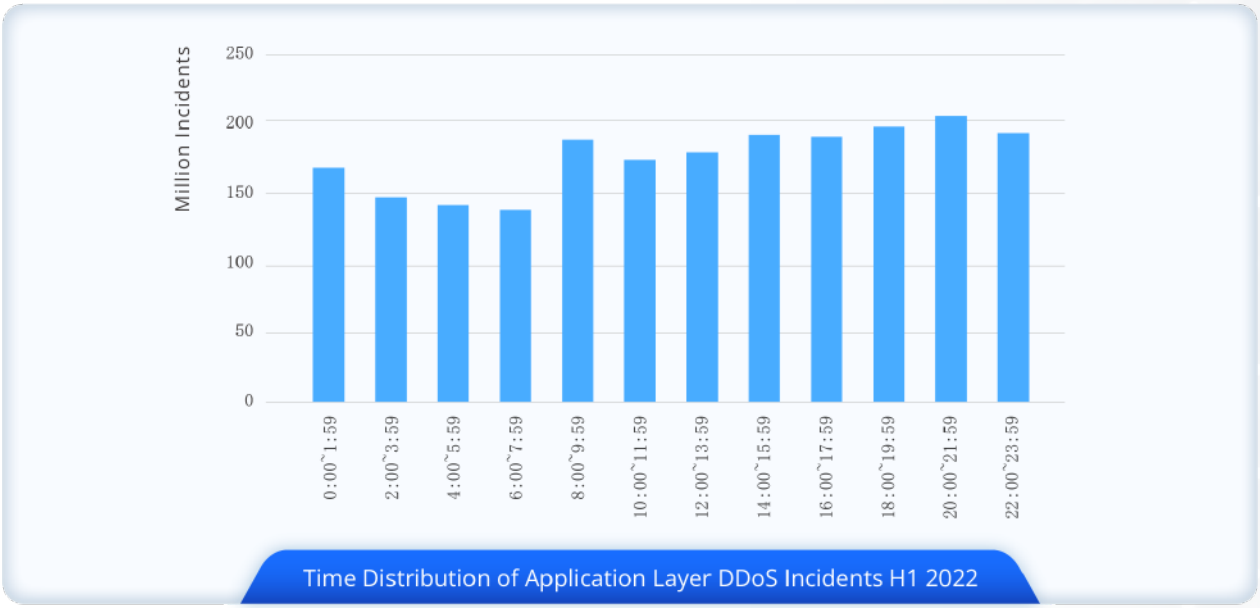
In terms of attack scale, both network-layer and application-layer attacks reached record highs in the first half of the year. On January 16, the CDNetworks 'security platform encountered and purged a record level of traffic DDoS attacks, with a peak of 2.09 TBPS. On April 24, the platform successfully defended against application-layer DDoS attacks, with a peak of 34.7 million RPS. This record number of L7 DDoS attacks surpassed the previous world record for such incidents.

Peak of Internet Access In-sync with Peak of DDoS Attacks

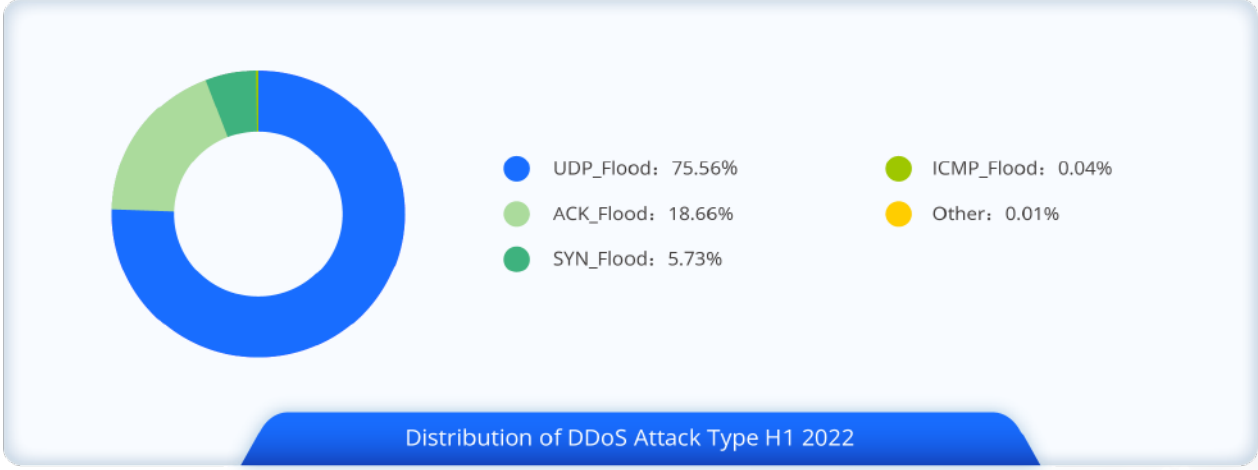
Analysis of DDoS attacks at both the network and application layers show that they follow a pattern where attack volume decreased in the early morning, picked up during the day, and reached a peak from 20:00 to 22:00 in the evening. This shows that, in order to maximize damage, attackers launched their attacks based on the peaks and valleys of network usage.



Time Distribution of Network Layer DDoS Incidents H1 2022



75% of Attack Traffic Comes from UDP Attacks That Produce Reflection Amplification

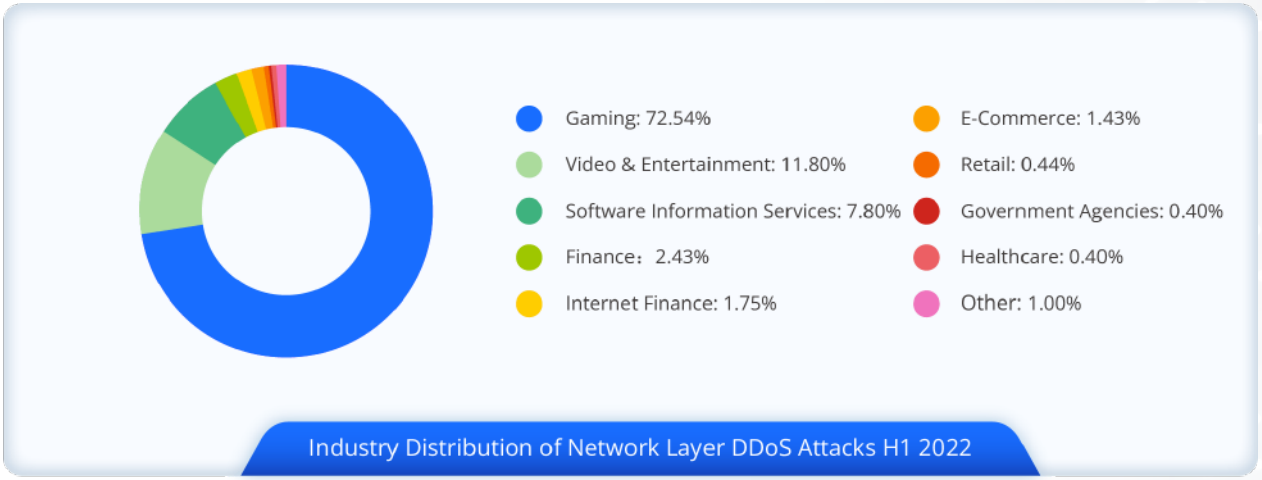


In terms of attack methods, 75.56% of the traffic in network-layer attacks comes from UDP_flood attacks, followed by ACK_flood attacks (18.66%) and SYN_flood attacks (5.73%).
Currently, the most popular choice of UDP_flood attacks are reflection-amplification attacks, which can cause significant damage at low cost to the hacker.

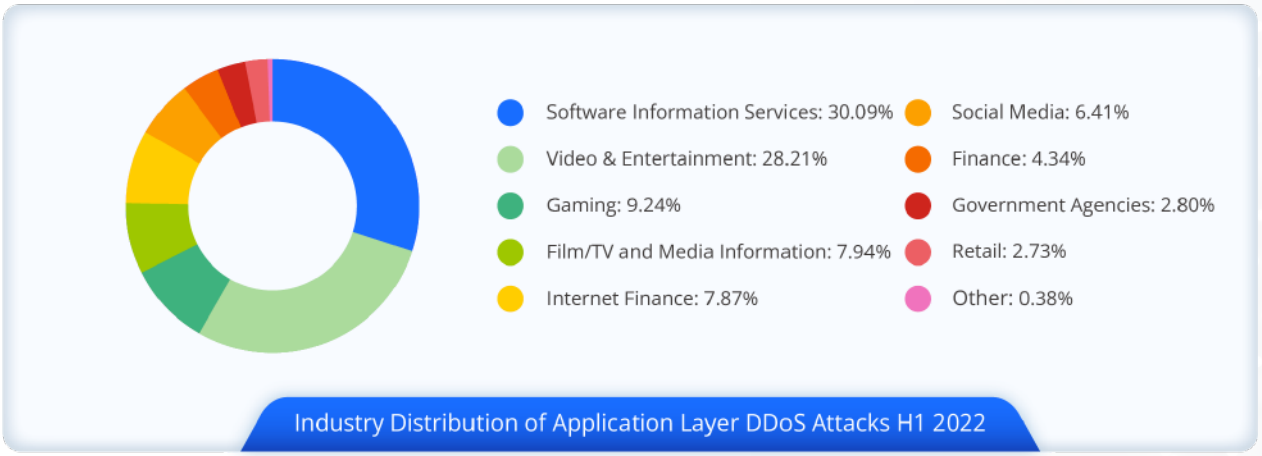
Network Time Protocol (NTP), Simple Service Discovery Protocol (SSDP), and Memcache accounted for over 90% of all reflection-amplification attacks captured by the CDNetworks' security platform in the first half of 2022.

Gaming Remains a Major Target of DDoS

In H1 2002, the Gaming industry continues to suffer from virulent and unrelenting DDoS attacks. Network-layer attacks targeting gaming accounted for 72.5% of the total number of attacks, an increase of 13% over the same period last year. At the same time, application-layer DDoS attacks of the gaming industry also ranked in the top three of industry distribution of application layer Attacks.



Industry Distribution of Network Layer DDoS Attacks H1 2022



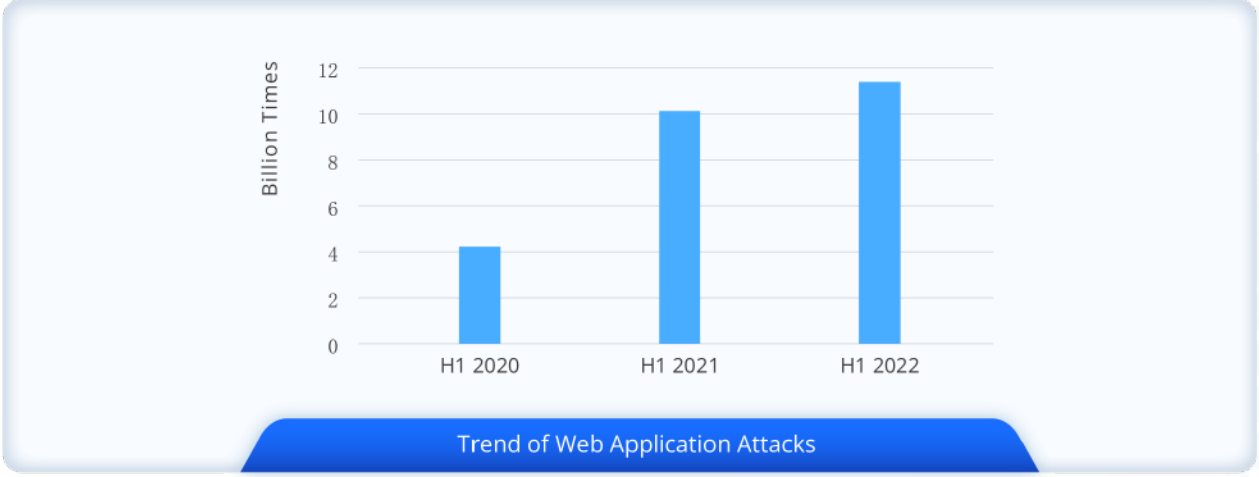
Industry Distribution of Application Layer DDoS Attacks H1 2022

With intense competition and high revenue that is inherent in the gaming business, DDoS attacks can paralyze a gaming business at little cost to the originator of the attack. The significant losses in revenue and reputation resulting from these DDoS attacks make the gaming industry one or the hardest hit areas. Historically, DDoS attacks in January against game application download markets, a critical segment of the gaming industry, peak at 2.09 TBPS.

Compared with network-layer attacks, the target industries of application-layer attacks are more evenly distributed and dispersed, with the hardest hit sectors, Software Information Services and Video and Entertainment industries, accounting for roughly 30% of all attacks — far less than the number of network-layer attacks in the game industry.

Interpreting of Web Application Attack Data

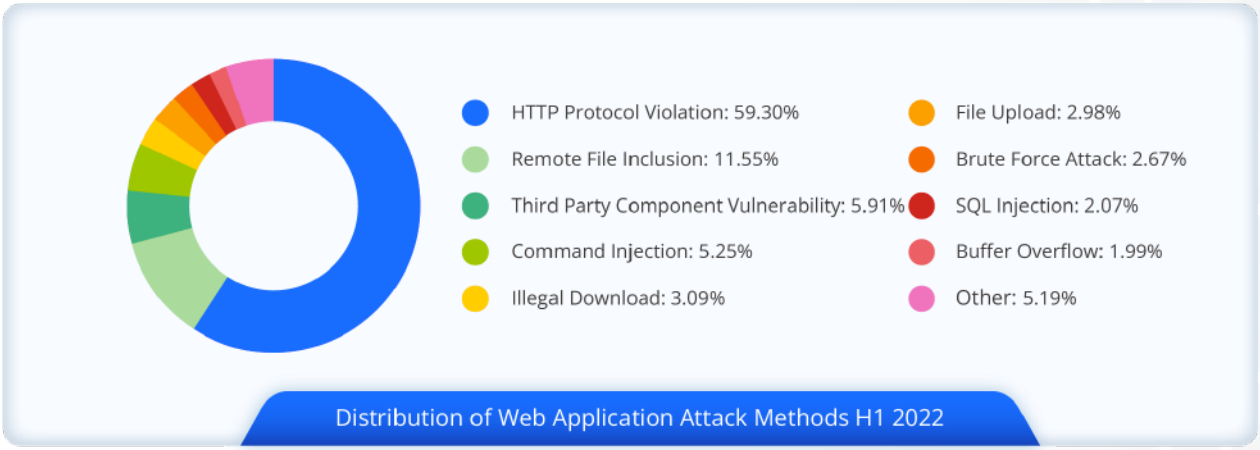
Web Application Attack Growth Slowing Down



In H1 2022, the CDNetworks' security platform monitored and blocked 62.8875 million web application attacks per day, a slight increase of 12.56% compared with H1 2021. With this increase, a slowdown in growth has also been evidenced.

Violation of HTTP Protocol Becoming the Preferred Choice of Attack

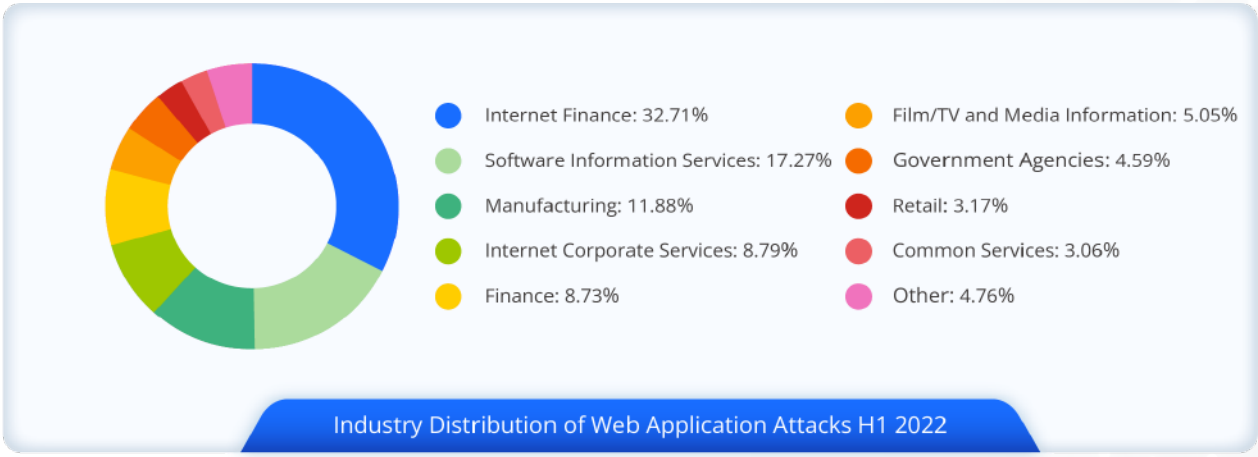
Based on the analysis of web-application attacks, the proportion of HTTP protocol violations has risen sharply. They now account for an overwhelming 59.30% of all web-application attacks, an increase of roughly 25% over the same period last year.



Ranking second and third are remote file attacks (11.55%) and third-party component vulnerability attacks (5.91%). Both of these attack methods increased significantly in ranking, and are now ranked 10th and 12th compared to the same period last year.

As enterprises increase dependence on third-party open-source components driven by digital transformation initiatives, attacks against third-party components continue to rise. A large number of third-party components are utilized in commercial applications and businesses developed within the enterprise. The vulnerabilities in any lower-level components can have a devastating impact that reenforces the saying “one successful attack damages many.”

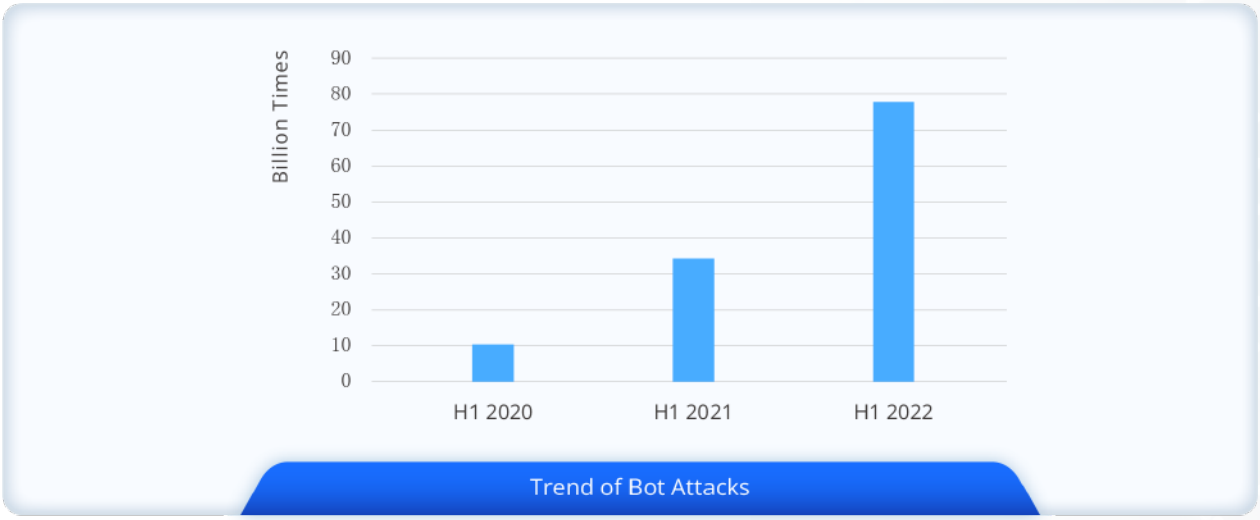
The Internet Finance Industry Has Become the Top Target



From the perspective of target industries, the Internet Finance industry (32.17%) jumped to the top of web-application attacks in the first half of 2022, with 3.678 billion attacks — a year-on-year increase of nearly 9 times. The number of attacks against Manufacturing (11.88%) soared 29-fold year-on-year in the first half of 2021, ranking third in all industries. The Software and Information Service industry, which occupied first place for consecutive years (17.27%), saw a sharp decline in the number of attacks during the period, falling to second place.

Interpreting of Malicious Bot Attack Data

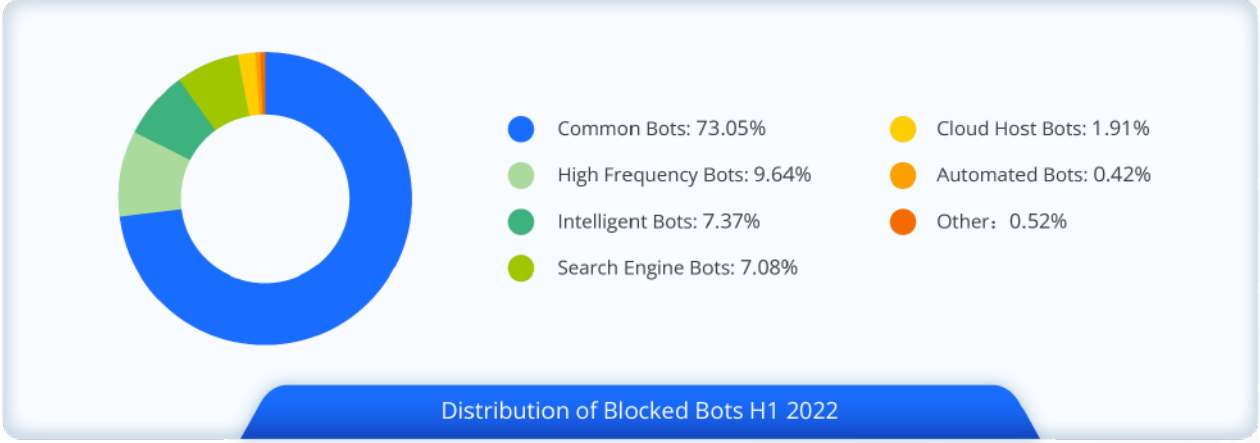
Attack Volume of Bots Doubled in Consecutive Years.



In H1 2022, the CDNetworks' security platform monitored and blocked a total of 77.366 billion bot attacks, an average of 4947 attacks per second. This number is 2.27 times the number in H1 2021 and 7.46 times the value in H1 2020.

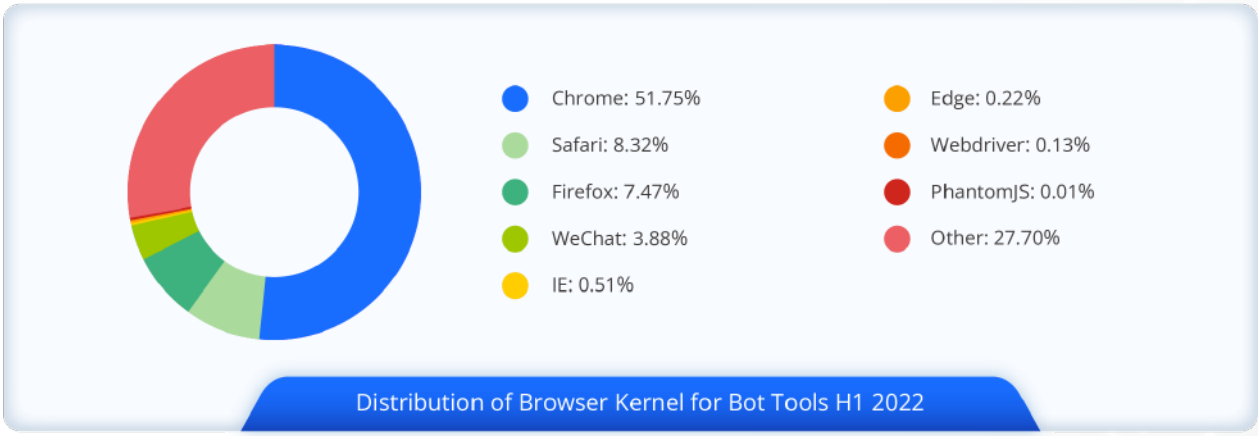
Email: sales@cdnetworks.com www.cdnetworks.com

Threat of Meticulously Disguised Intelligent Bots on the Rise



Distribution of Blocked Bots H1 2022

The types of bots captured by the CDNetworks' security platform in the first half of 2022 show that the relatively simple conventional bots remain the most predominant, accounting for 73.05% — a slight decrease of 4% compared with the same period last year. At the same time, the number of intelligent bots, which mimic human-access behavior, increased by 348.17% compared with the same period last year and accounted for 7.37% of all bot attacks — from 3.73% in 2021. Trends show that threats from undetected and increasingly intelligent bots is on the rise. Especially disturbing is the fact that bots have been evolving and becoming better adapted to copying real-world access behaviors.



Distribution of Browser Kernel for Bot Tools H1 2022

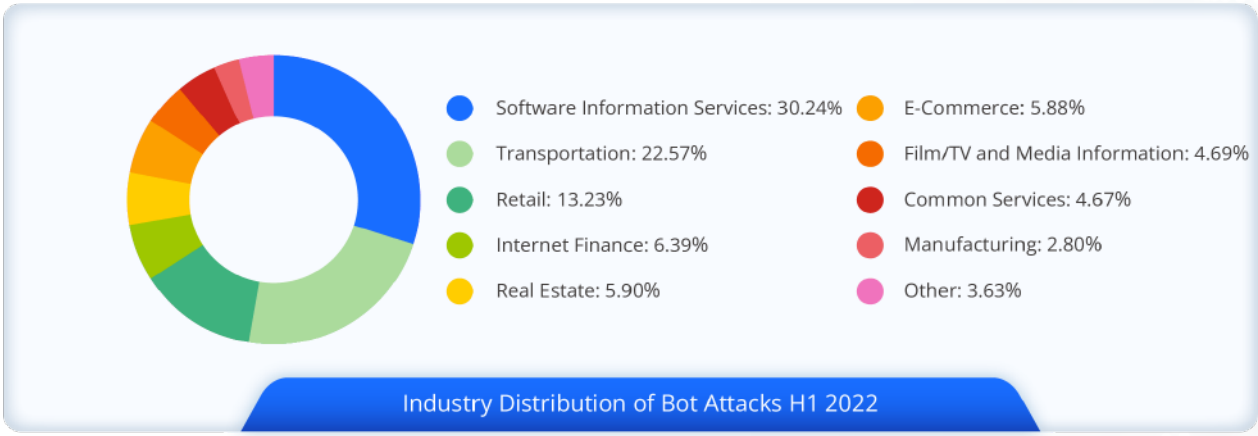
More Than Half of Bot Tools Use the Chrome Kernel

The evolution of improved attack and defense measures prompted bot tools to conceal their true identity. This cloaking has reached a point where malicious bots can disguise themselves as legitimate browser behavior and mimic the behavior of real users.

By analyzing browser kernels for bot tools monitored by the CDNetworks' security platform, the platform found that the Chrome family remains the preferred choice for bot attacks. Accordingly, bot tools developed with the Chrome kernel account for 51.75%.

Safari and Firefox kernels ranked second and third, accounting for 8.32% and 7.47%, respectively. With the high-frequency usage of applications such as blog and Mini Programs (also known as Mini-apps on mobile devices), the WeChat mobile application kernel ranks fourth and accounts for 3.88% of all bot attacks.

Hardest Hit Areas: Software Information Services, Transportation, Retail Industry



In H1 2022, the target industry distribution of malicious bot attacks continued to show a relatively scattered scenario, with relatively low concentration. Software Information Services (30.24%), Transportation (22.57%) and Retail (13.23%) remained the hardest hit areas by bot attacks. The Internet Finance industry, which exchanges significant amounts of high-value information, such as funds and wealth-management products in online business, has risen sharply, from 10th place in the same period last year to 4th place today.

Illicit Perpetrators Have Made Extensive Use of Meticulously Disguised Bots for Business Fraud.

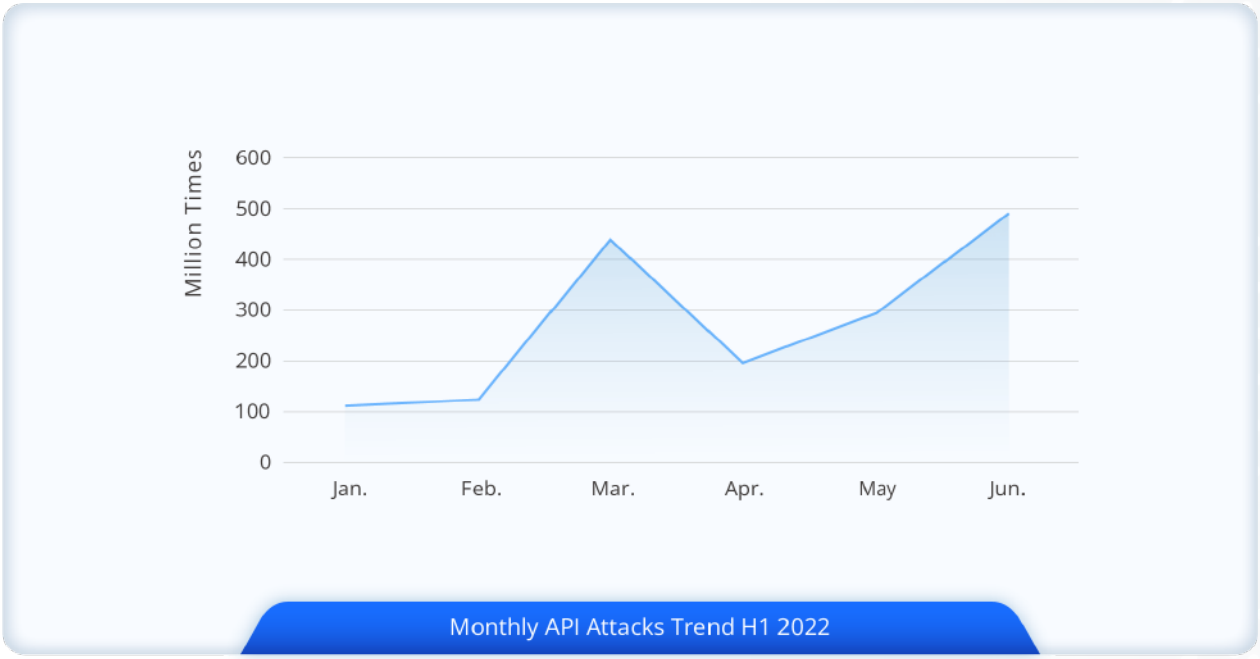
The influence that COVID-19 has had after 2020 has prompted a large number of offline businesses to accelerate their migration to online platforms, especially in the areas of finance and marketing. This migration has not gone unnoticed by attackers, who have taken advantage of this opportunity by using highly anthropomorphic bots to create bogus identities and accounts in order to commit click farming, deal spamming, and other fraudulent automated batch-driven business activities. Business fraud has evolved into a complex industry chain, which requires greater requirements for risk management that can identify known and unknown automated attacks from legitimate business activities.

In the first half of 2022, a variety of business risk management scenarios were monitored by the CDNetworks' security platform. Among them, the most common risk types associated with registration are spam registration (42.84%) and traffic fraud (32.65%). For logins, risk behaviors such as bulk login (53.41%), remote login (15.88%), and database breach (9.12%) were detected. For marketing, the most prominent risk was system cheating for profit (67.49%).

Interpreting API Attack Data

In today's API-driven economy, enterprise online businesses often use large numbers of APIs to share data, algorithms, transactions, and processes, and perform business functions. Given their rise in significance, APIs have become a key target for network attacks.

In the first half of 2022, attacks against API services continued to show rapid growth. The CDNetworks' security platform monitored and blocked 9.0865 million average daily attacks against API services, a 168.80% increase over the same period in 2021.



Monthly API Attacks Trend H1 2022

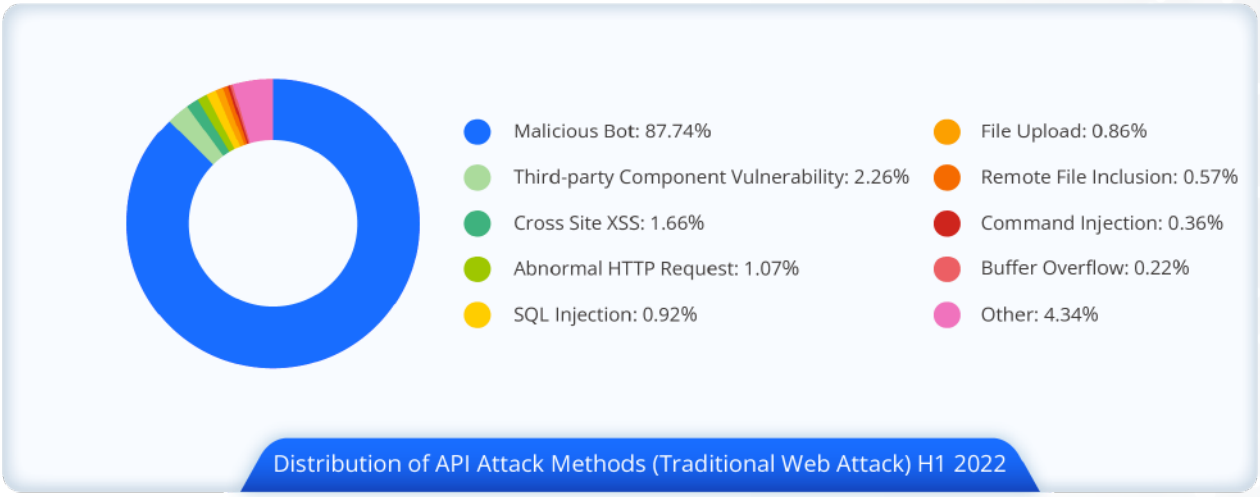
In terms of the monthly attack trend, the data show that API attacks peaked in March and June in the first half of the year.

Extremely Significant Risk of Malicious Use of API Parameters

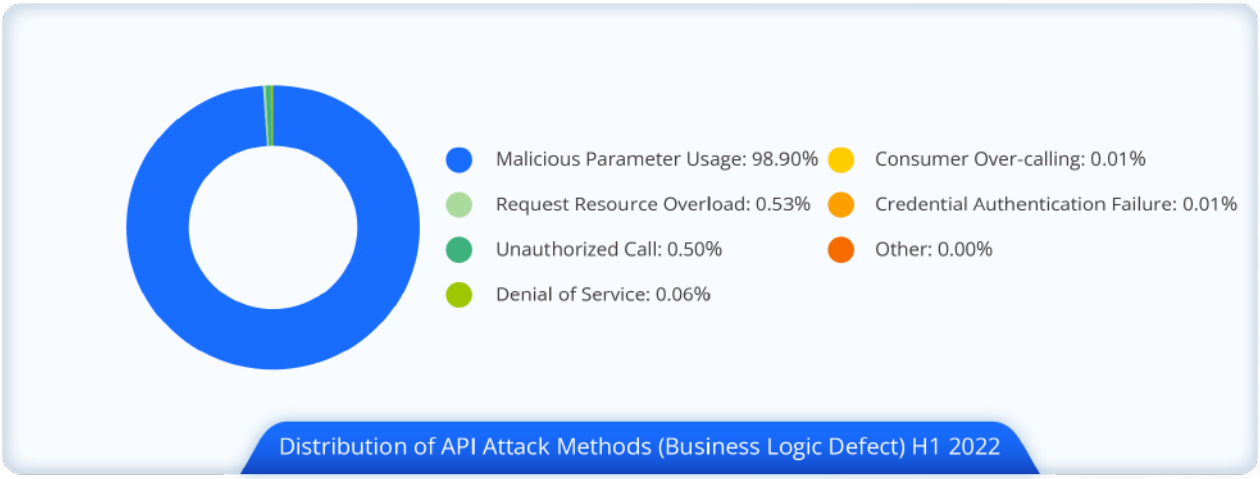
The CDNetworks' security platform has observed two major types of attacks against API services. One is the traditional web attack. Because APIs support web services, and considering that many API calls consist of high-value dynamic data, APIs have become popular targets for web attacks. This type of attack often has malicious characteristics that are distinctive from normal API requests.

Email: sales@cdnetworks.com www.cdnetworks.com

The other type of attack takes advantage of the shortcomings inherent in APIs without presenting malicious characteristics. Rather, it uses “logic defects” within APIs to facilitate unauthorized access. This type of attack is often difficult to identify with traditional web-protection rules, and requires professional API security monitoring and management countermeasures.



Distribution of API Attack Methods (Traditional Web Attack) H1 2022

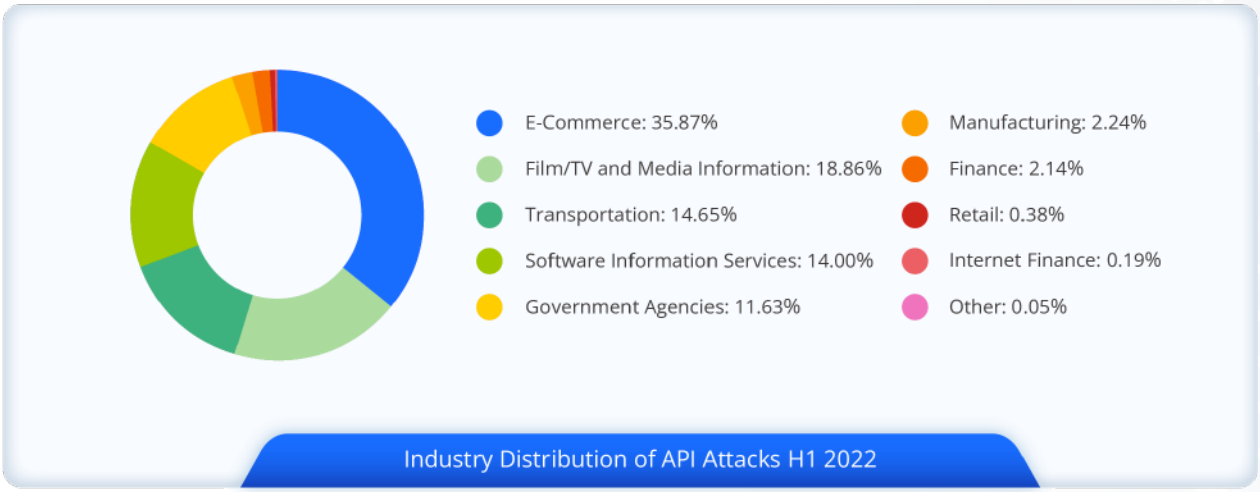


Distribution of API Attack Methods (Business Logic Defect) H1 2022

Analyzing API attacks blocked by the CDNetworks’ security platform shows that traditional web attacks against API services began the first half of this year and continues to grow. Currently, they account for the vast majority of the 87.7% of all API attacks. This figure is a significant increase compared with 53.44% of web attacks against APIs last year.

The major avenue of attacks against API business logic is malicious use of API request parameters, which accounts for 98.9% of all API incidents. If an API service is not sufficiently strict with the parameters it sends to an endpoint to modify a response, attackers can easily build malicious request parameters that mimic legitimate parameters in order to create high-efficiency attacks at a low cost to the cyber criminals.

Hardest Hit Areas: E-Commerce, Film/TV and Media Information, Transportation Industry



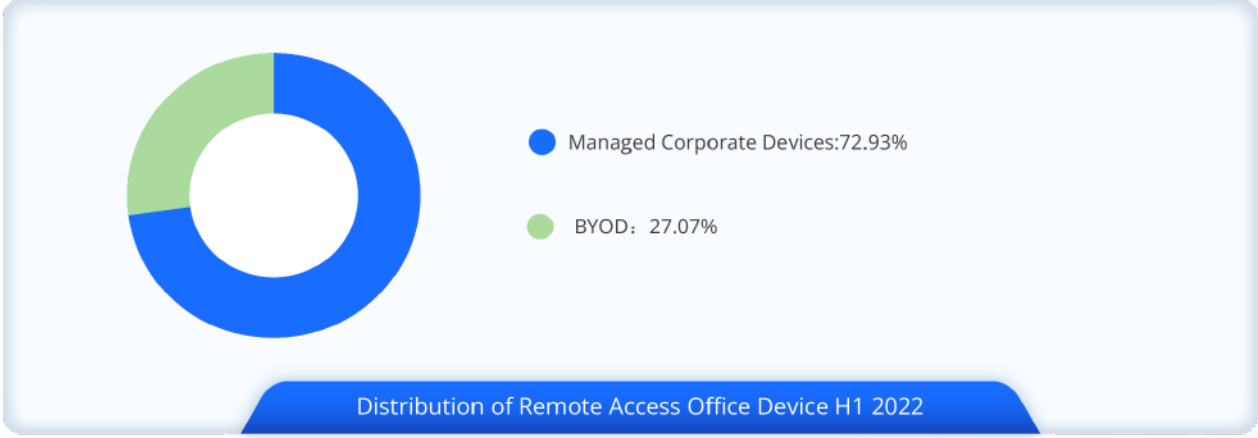
Industry Distribution of API Attacks H1 2022

When it comes to identifying target industries prone to API attacks, the E-Commerce industry, which is rich in goods and user privacy information, has become the biggest target, accounting for 35.87% of all attacks aimed at API services. Industries that came in second place to fifth place were Film/TV and Media Information industry (18.86%), Transportation industry (14.65%), Software Information Service industry (14.00%), and Government Agencies (11.63%). These five industries comprise 95% of all API attacks.

Interpreting of Enterprise Telecommuting Security Data

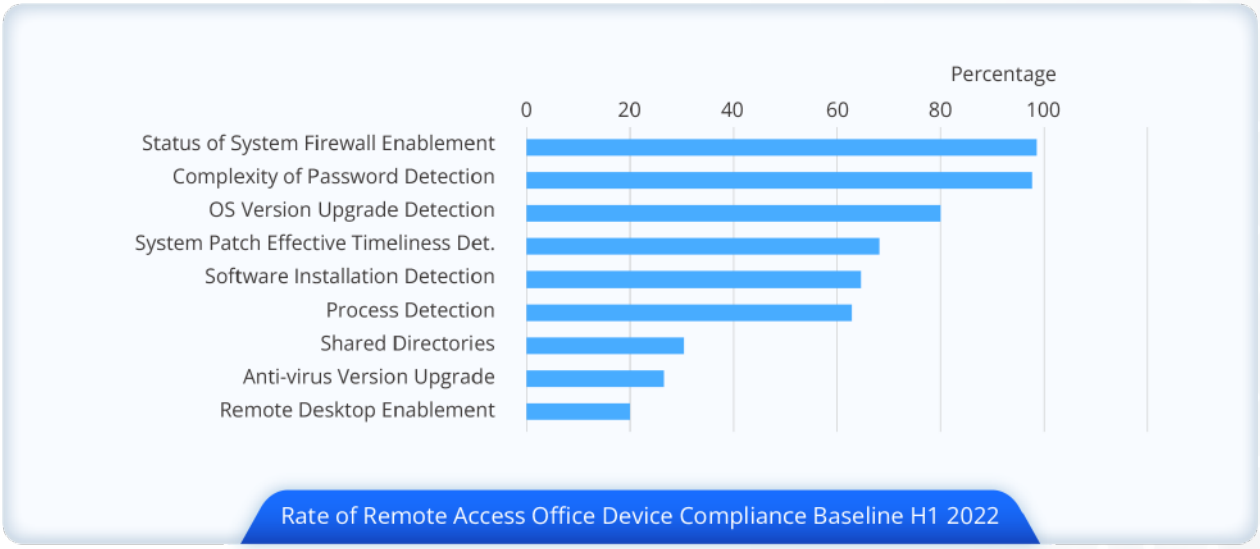
Since 2020, COVID-19 has been the catalyst for spurring the global demand for telecommuting. Among the enterprise users of CDNetworks' services, nearly 89% leveraged remote-access technologies to access corporate office intranet through external network devices. The large-scale adoption of telecommuting has also exposed several security issues.

BYOD with Weak Security Measures Account for Nearly 30% of All Scenarios



Analyzing the types of remote-access devices used by CDNetworks' enterprise users, the proportion of BYOD has reached 27.07% and continues to rise. Compared with centrally managed corporate devices, BYOD generally lacks a clear security management policy and suffers from security measures that are often weak, making them vulnerable to targeted hacking attacks.

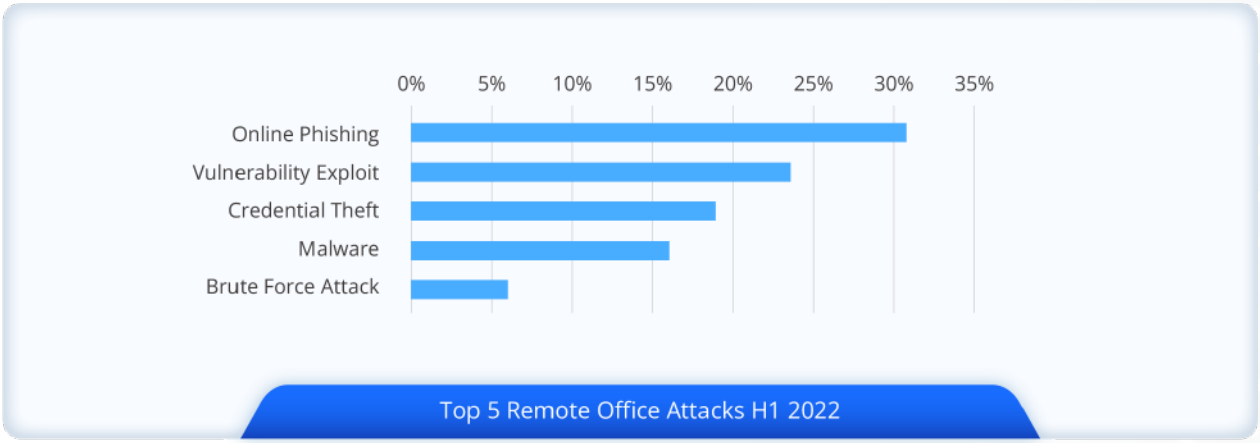
End-users Continue to Underestimate the Importance of Security Awareness



By monitoring core factors in the security baseline of user devices, it was found that most end-users seldom optimize the original security configuration of their device's operating system. The two factors with which most end-users comply are enabling the operating system firewall (99.21%) and making passwords sufficiently complex (98.3%).

The three factors with the lowest compliance are specifying whether remote desktops are enabled (20.14%), making sure devices have the latest anti-virus software installed (26.7%), and deciding whether to use a shared directory (30.61%). To make connectivity easy for end-users, most administrators do not issue mandatory specifications for these three factors and most end-users do not take the initiative to optimize their devices, resulting in security risks.

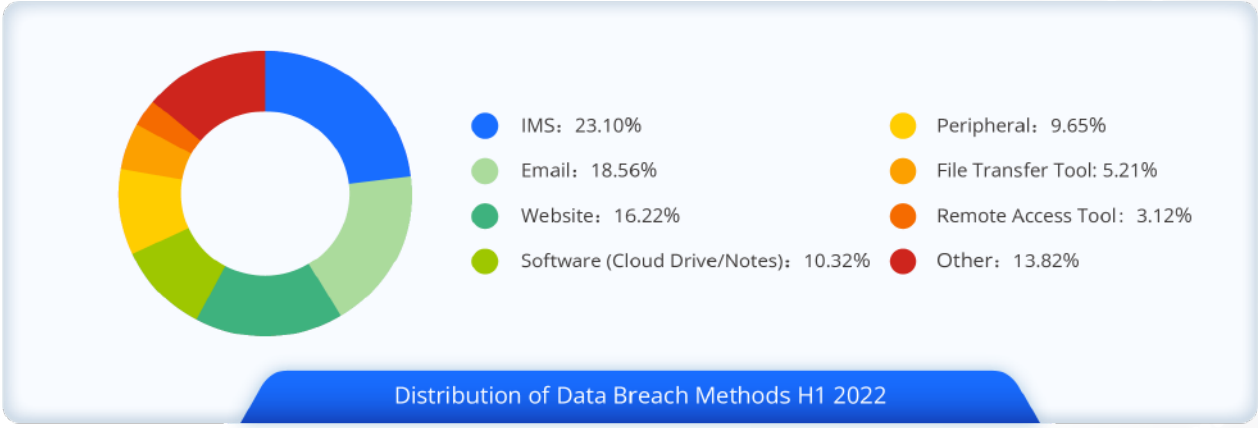
Phishing and Vulnerability Exploitation Provide Critical Means of Network Attack



Hackers often utilize indirect devices as a springboard to attack applications in the office network. And why not? After all, many web applications have not been upgraded from HTTP protocol to HTTPS, and the system vulnerabilities intrinsic to nearly all applications have not been fixed. This means that once hackers gain access to an intranet, they can easily breach intranet applications.

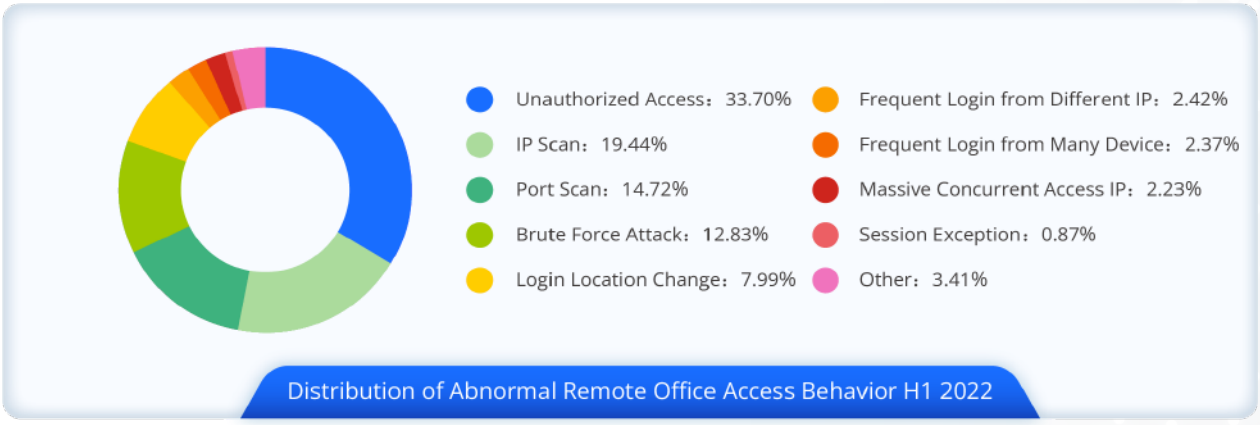
When discussing attacks against office networks, phishing email is the most common means of attack. Vulnerability exploitation, credential acquisition, malware, and brute force cracking are also major attacks that require countermeasures.

Instant Messaging Ranks First in Causes of Corporate Data Breach



Internal data breaches have become an urgent security threat for enterprises. The Internet not only improves employee' work efficiency, but also makes it easy for employees to disclose corporate data, whether intentional or accidental, through a variety of ways. Among the avenues of data breaches, the top three are instant messaging (23.1%), e-mail (18.56%), and websites (16.22%).

Be Vigilant Against Covert Attacks Behind Abnormal Behaviors Such as Unauthorized Access and IP Scanning



With the exponential growth of telecommuting, APT attacks against office networks continue to rise. As an organized, targeted, and persistent threat, APT attacks remain undetected on a targeted

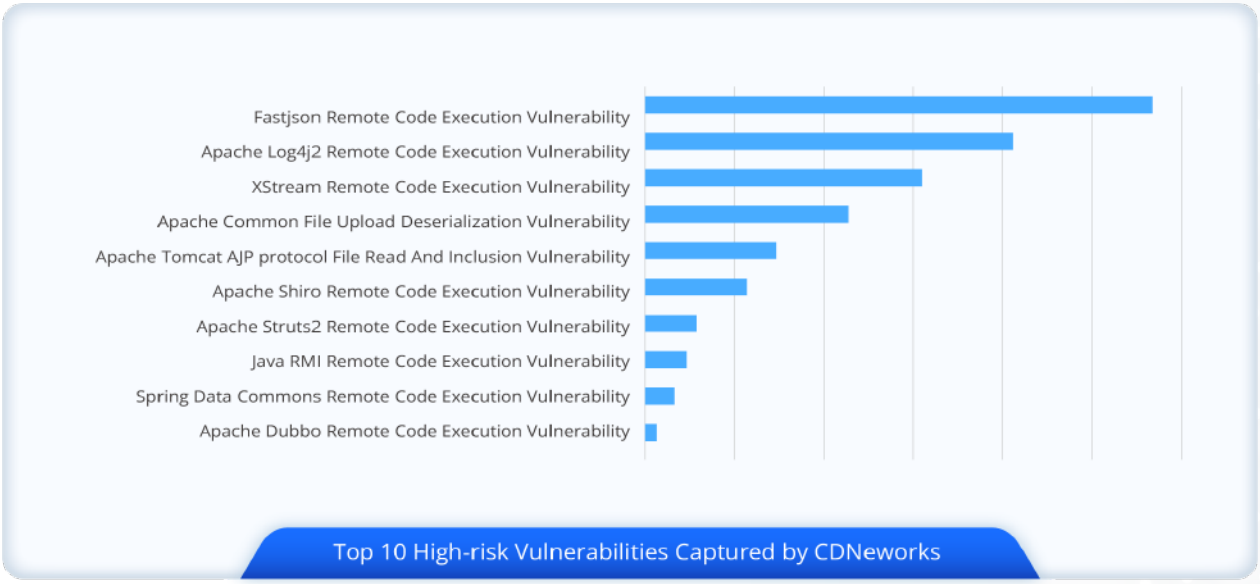
network for a significant period of time. After gaining and maintaining unauthorized access to the targeted network, the intruder monitors, blocks, and relays information and sensitive data to the hacker. APT attacks often bypass traditional network defenses.

Although they are hidden, they can still be identified by their abnormal behavior or by analyzing abnormal traffic patterns using CDNetworks' Enterprise Secure Access, a Zero Trust solution.

Analyzing abnormal access behavior with the CDNetworks' ESA found that gaining unauthorized access to targeted systems and applications was the most frequently used method (33.70%) for APT attacks. In order to detect and assess targeted corporate networks, attackers adopt methods such as IP scans (19.44%) and port scans (14.72%), which rank second and third, respectively.

Interpreting Host Security Data

Most High-risk Vulnerabilities are Associated with Open-source Ecosystem Components.



Top 10 High-risk Vulnerabilities Captured by CDNeworks

The high-risk vulnerabilities favored by attackers focus on weaknesses in applications and components. Intruders focus on these components because they reside and operate in an environment that is easier for hackers to access compared to operating systems.

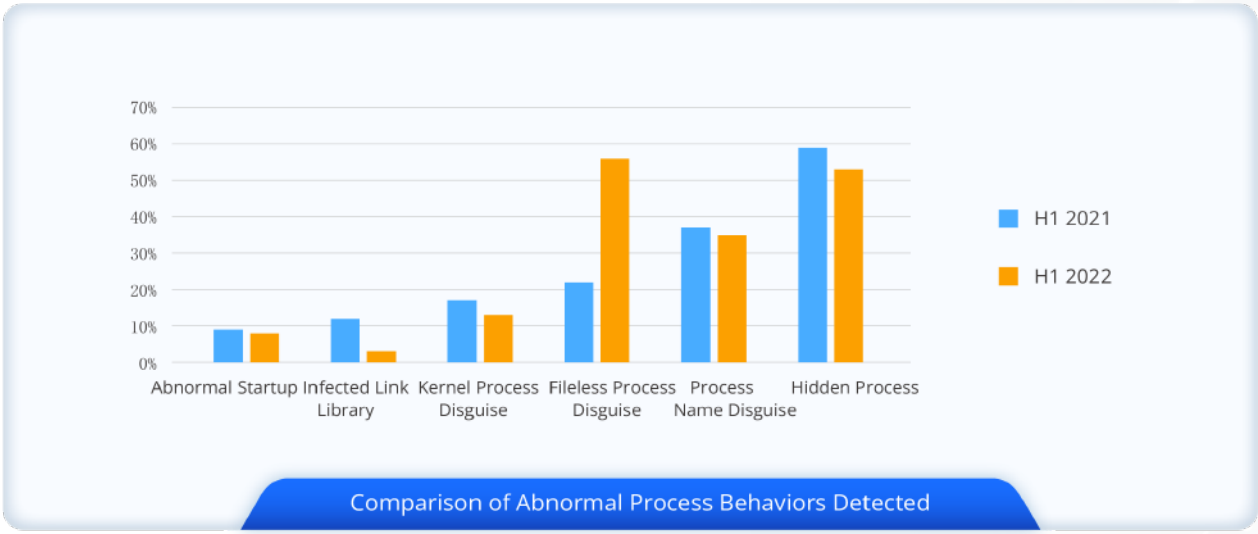
Among the high-risk vulnerabilities captured by the CDNetworks' security platform in H1 2022, open-source ecosystem components accounted for a high proportion of all vulnerabilities. Among them,

Email: sales@cdnetworks.com www.cdnetworks.com

the most prominent is the Fastjson remote code execution vulnerability. As a commonly used basic library of the Java ecosystem, Fastjson vulnerabilities were exposed in May of this year, and data shows that its impact to date has been extensive.

In second place is the ongoing Apache Log4j2 vulnerability, which emerged at the end of last year. Its incident numbers remained among the top two high-risk vulnerabilities in H1 2022, which indicates that this vulnerability remains widespread in hosts and is having a lasting impact.

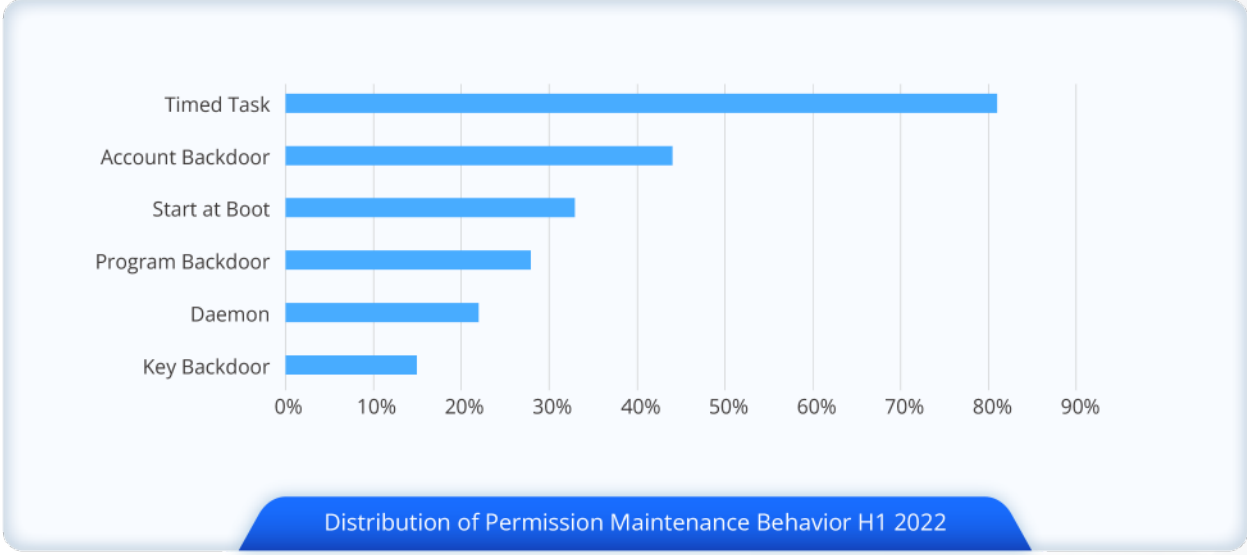
Proportion of Fileless Processes Greatly Increased Among All Abnormal Processes



By identifying irregular data processing, the CDNetworks' Host Probe shows that the proportion of hidden processes, disguised process names, and other abnormal processes decreased slightly. In addition, the proportion of fileless infections increased significantly compared with all abnormal processes. At its peak, fileless infections reached 56.44%, an increase of 33.86% over the same period last year.

Fileless infections can avoid detection by security software because the software cannot capture the contents of the process files to match them with virus feature libraries. Typically, there are two ways to create a fileless infection. One way is by generating executable virus files from other processes, and then deleting the virus files immediately after the processes are pulled. The other way creates a fileless process directly in memory through mem_fd calls. Both methods can render traditional anti-virus software impotent when it comes to identifying any virus files, which makes it difficult for security researchers to analyze these types of intrusions.

More than 80% of Intrusions Leveraged Timed Task Implementation to Maintain Permissions



Distribution of Permission Maintenance Behavior H1 2022

Permission maintenance is targeted in more than 95% of host intrusions. Among the permission maintenance behaviors identified by the CDNetworks' Host Probe in H12 2022, timed tasks, backdoor accounts, and boot startup ranked in the top three, accounting for 81.29%, 44.13%, and 33.46% of attacks, respectively.

Maliciously timed tasks are usually implemented in the form of scripts that execute Trojans, malicious instructions, and other malware. Compared with traditional PC viruses, server host viruses are more likely to use timed tasks to maintain permissions. Since server hosts rarely are rebooted, timed tasks have proven to be more efficient than boot configurations (which ranked third) in gaining unauthorized access to systems and applications.

Insight and Recommendations for Future Trends

- Based on the analysis and industry observation of the CDNetworks' security platform in H1 2022, security threat trends can be summarized in the following way:

- The risk of data breaches continues to escalate. As digital transformation becomes more widely adopted, the value of data continues to rise. Accordingly, increasing amounts of data and devices are exposed to the network, facing the dual threat of external attacks and internal breaches. From these observations, one can extrapolate that risks to data security will continue to rise as the scale of data breaches continues to escalate. On the other hand, the introduction of Network Security Law, Data Security Law, Personal Information Protection Law, and other laws and regulations are aiding enterprises with their compliance management for regulating data-processing activities and ensuring data security.

- API security threats continue to rise at an alarming rate, and the security challenges they present exceed those of traditional webpages. APIs are involved in many of these scenarios. Given the frequent iterations of APIs and the chasm that often exists between business and security, it is not uncommon for API services to have varying degrees of security defects — even when those APIs come from the same organization. In particular, design vulnerabilities found in API parameters are commonly used by attackers to steal data en masse. Rule-based web protection no longer offers the capabilities and assurances that it once did in combatting today's complex and virulent cyberthreats.

- Supply chain attacks against open-source ecosystems will continue to run rampant. Modern software remains highly dependent on shared open-source software ecosystems, yet the security issues of these third-party software applications and components are frequently ignored by security teams, primarily because they are difficult to find and difficult to trace. Unfortunately, the damage wrought by infected applications and components is almost always devastating. For this reason, supply chain attacks aimed at open-source ecosystem security vulnerabilities are increasingly favored by attackers. The statistics in this report show this trend to some extent: Specifically, statistics indicate that the number of web attacks against third-party component vulnerabilities has increased significantly. Nearly all high-risk vulnerabilities aimed at host systems come from open-source components. Such is the case with Apache Log4j2, which continues to damage business revenues and reputations since its detection at the end of 2021 due to the widespread use of Log4j and Java.

Email: sales@cdnetworks.com www.cdnetworks.com

- The establishment of extensive enterprise defense systems based on Secure Access Service Edge (SASE) has gradually become the trend for enterprises to adopt when securing information systems. SASE is a security model that addresses security by acknowledging the shift from datacenters to cloud and mobile platforms. Specifically, SASE converges network and security functionality in a model where user and resource identities determine access decisions instead of physical data centers. This migration promulgates more stringent requirements for all aspects of security technology. In terms of hardware, SASE calls for a comprehensive endpoint environment that is aware of the devices within the environment and manages their security. In terms of networks, the requirements for device access control and network access control are more stringent and precise. With applications and data, SASE focuses on data breach protection and network threat analysis, while security operations focus on abnormal behavior detection and unified security policy management. In this way, SASE eliminates the cost and effort to maintain a complex and disparate infrastructure composed of point solutions, enforces an optimal security posture that reduces risks for breach and data loss, enables secure work from anywhere, and improves access to applications on premises and in the cloud.

As online enterprises shift their business to clouds, containers, and APIs, the notion of using security tools that focus on points or lines is no longer a viable option. What is needed are security solutions that address cloud and remote platforms in a comprehensive and systematic security architecture. Only then can the continuous evolution of network security risks be addressed effectively. By focusing on cloud security, corporate security, and security services, along with driving cutting-edge concepts and technologies such as Web Application and API Protection (WAAP), zero trust, SASE, artificial intelligence, big data, and other forward-thinking concepts and technologies, CDNetworks has created extensive defense capabilities for enterprise users. Our capabilities cover the gamut from host layer and network layer to application layer, data layer, and business layer. They even push the security boundary to the user layer, forming an integrated security system whose elements work in concert to deliver a holistic approach to current and evolving cyberthreats.

Going forward, CDNetworks remains dedicated to providing unparalleled security solutions. With that pledge comes our commitment to continue leveraging our expertise in technological innovation and services to promote additional collaboration, make the most of upstream and downstream security technologies to capitalize on the benefits of both, and elevate existing security systems present within today's enterprises by realizing the power of SASE-integrated security services. By completely rethinking network and security architecture in hybrid and remote environments, CDNetworks predicts that SASE technology and security will continue to improve and become more refined in the years to come.

 Email: sales@cdnetworks.com www.cdnetworks.com