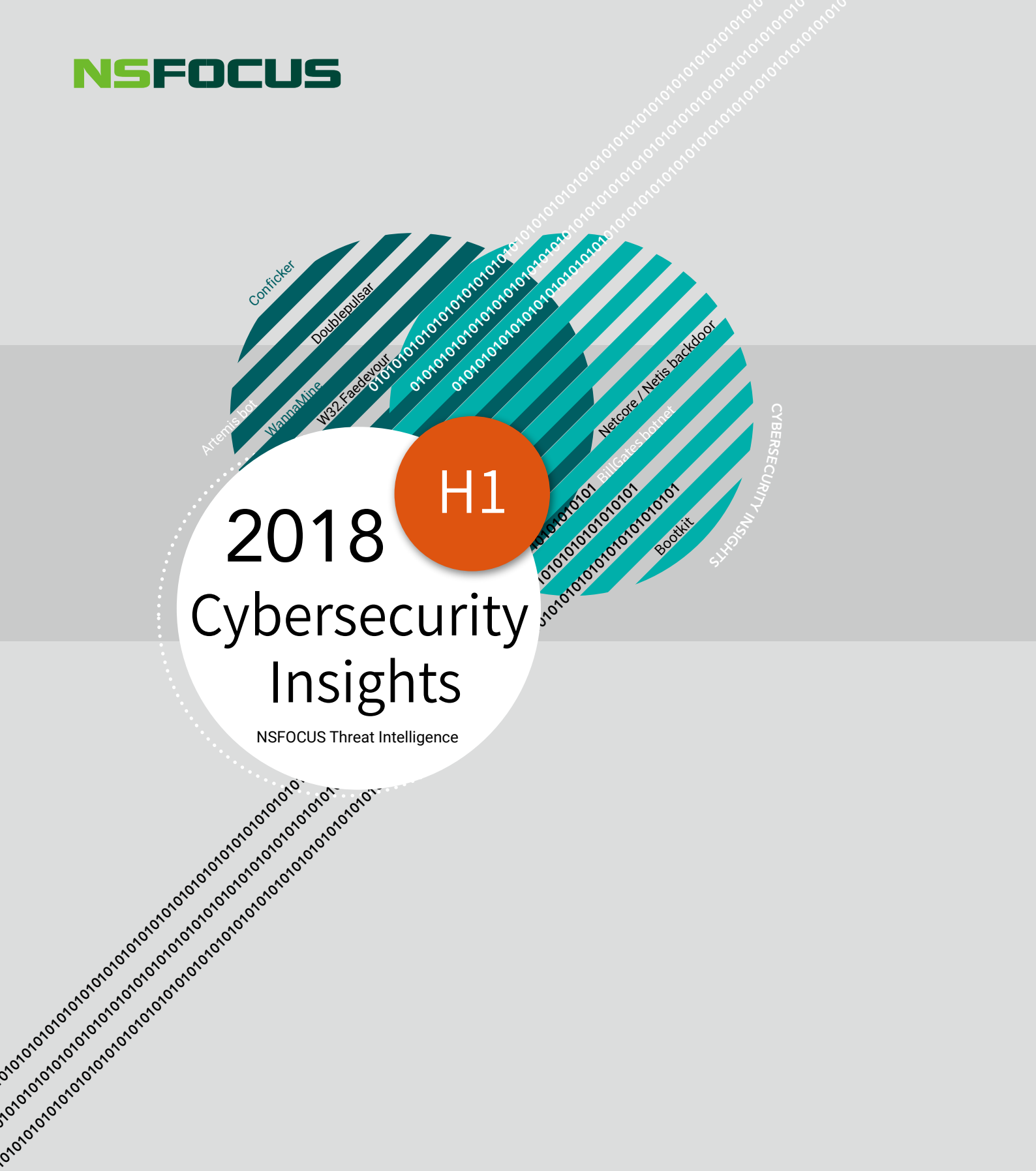
NSFOCUS



H1

2018 Cybersecurity Insights

NSFOCUS Threat Intelligence

NSFOCUS

About NSFOCUS

NSFOCUS is an iconic internet and application security company with over 18 years of proven industry experience. Today, we are operating globally with 2000+ employees at two headquarters in Beijing, China and 40+ offices worldwide including the IBD HQ in Santa Clara, CA, USA. NSFOCUS protects four of the ten largest global telecommunications companies and four of the five largest global financial institutions.

With its multi-tenant and distributed cloud security platform, NSFOCUS effectively moves security into the internet backbone by: operating in data centers around the world, enabling organizations to fully leverage the promise of cloud computing, providing unparalleled and uncompromising protection and performance, and empowering our partners to provide better security as a service in a smart and simple way. NSFOCUS delivers holistic, carrier-grade, hybrid DDoS and web security powered by industry leading threat intelligence.

Special Statement

All data for analysis is anonymized and no customer information appears in this report to avoid information disclosure by negligence on our part.

NSFOCUS Threat Intelligence

Catalogue

NSFOCUS Threat Intelligence (NTI)

NSFOCUS Threat Intelligence center (NTI) is a professional security research organization set up by NSFOCUS for implementing the intelligent security 2.0 strategy, improving the cybersecurity ecosystem, promoting applications of threat intelligence, and enhancing customers' capabilities of defending against various attacks. Thanks to the company's competent security teams and powerful security research capabilities, NTI is able to continuously observe and analyze the global cybersecurity threats and landscape. With a focus on the capabilities and key techniques for threat intelligence production, operations, and applications, NTI has launched a threat intelligence platform and a series of next-generation security products that incorporate threat intelligence. By delivering actionable intelligence data, expert intelligence services, and efficient threat protection, NTI can help users better understand and address various cyber threats.

Executive Summary

Of more than 27 million attack source IP addresses detected by us in the first half of 2018, 25% have been linked to repeated attacks. We call these sources "recidivists".

In recent years, security events have frequently made headlines around the world. Personal information disclosure, bank deposit stealing, and IoT device exploitation events always catch people's eye. In terms of public concern, Baidu Index reveals that the average number of overall daily searches for such keywords as "personal information disclosure" and "hacker" has been fluctuating at a high level in the past two years. This indicates that cybersecurity and information security are no longer just a technical issue, but one that affects people's livelihood.

In the meantime, security vendors' perspective is also changing, slowly but steadily. Take the RSA Conference as an example. The theme was "Connect to Protect" for 2016, "Power of Opportunity" for 2017, and "Now Matters" for 2018. The keyword also changed from "threat intelligence" and "artificial intelligence" in previous years to this year's "emergency response" and "threat hunter". All these convey a message that security vendors no longer content themselves with advocacy of some ideas and concepts, but have unanimously agreed on collaborative defense and silo breakdown. With years of technical accumulation, they are mature enough to focus their attention on the effect of implementation and the timeliness of response, with an eye to turning from reactive to proactive in combating cyberattacks.

Vulnerability discovery, exploitation, and emergency response are the areas where the offensive and defensive sides fight most fiercely. Attackers try to win battles by employing different ruses. The past year saw a series of events that was characterized by the EternalBlue exploit used in ransomware, such as the notorious WannaCry, and in cryptocurrency miners like WannaMine and Smominru. Attack targets and methods keep changing, but the pursuit for financial gains never changes. Rapidity is the essence of war. Cybersecurity warfare is hard to win in that it is difficult for the defensive side to rapidly grasp the situation, expand the arsenal,

and get fully prepared when the conditions are favorable to the offensive side. Sun Tzu said, "If you know the enemy and know yourself, your victory will not stand in doubt; if you know Heaven and know Earth, you may make your victory complete." The essence of threat intelligence is "knowing". From data to information to knowledge, security vendors, through years of practice, have built up the capability of extracting authentic information from massive attack data, basic data, and external intelligence to profile individual attackers in a multidimensional manner. Moreover, they can find the common characteristics of and associations between attacker groups. Through these efforts, a deep perception system of the cyberspace comes into being.

According to observations from the NSFOCUS Threat Intelligence center (NTI), nearly 20% of attack source IP addresses have initiated more than one type of attacks, which is similar to the situation in the first half of 2017. The change of attack types coincides with the characteristic of the kill chain where attacks gradually escalate, as demonstrated in 50% of web attackers who would try to launch more sophisticated exploitation attacks after initial campaigns. Quite a large proportion of botnet hosts show symptoms of worms. In other words, they, after being infected, continue to scan other hosts and exploit vulnerabilities, thus rapidly expanding the botnet by infecting more devices. In addition, an attack resource may be repeatedly used for multiple purposes. For example, 44% of malicious scan sources are found to send spam later. This, on the one hand, indicates that attackers are sensitive to the attack cost and so try to exploit bots to the maximum extent possible, and on the other hand, tells us that the cost of time and effect of scale are also top concerns of attackers.

In terms of attack traffic, the number of active malware variants, such as cryptocurrency miners, worms, and Trojans, dropped or fluctuated at a low level from late February to early March. This somewhat indicates that most attackers being monitored were Chinese because this period coincided with the Chinese Spring Festival holiday. At the same time, the temporary stagnancy of the Bitcoin market seems not to affect attackers' preference to profiteering from cryptocurrency. Cryptomining programs have become increasingly active since the Chinese Spring Festival. Among all cryptomining worms, WannaMine, a Monero cryptocurrency miner, is especially active and accounts for more than 70% of cryptomining activities. According to research conducted by Palo Alto Networks[1], Monero is the cryptocurrency most favored by malware authors and 5% of Monero

1 https://researchcenter.paloaltonetworks.com/2018/06/unit42-rise-cryptocurrency-miners/

coins have been mined via malware.

Of more than 27 million attack source IP addresses detected by us in the first half of 2018, 25% have been linked to repeated attacks. We call these sources "recidivists". "Recidivists" are responsible for 40% of attacks, most of which are botnet activities and DDoS attacks. This phenomenon may be attributable to two factors:

1. attack resources are reused
2. security posture of extensive IP infrastructures exposed on the Internet has not been improved over a long period of time, making them an easy target for various attackers.

Vulnerabilities disclosed in the first half of 2018 were mostly medium-risk ones, while the proportion of both high-risk and low-risk ones dropped a bit from a year earlier. It is worth noting that most of the vulnerabilities that are easily accessible and exploitable but hazardous are found in products from several mobile device or gateway vendors. Mobile devices and gateways are widely used globally. Once exploited, they can and will cause a devastating impact.

Cyberspace is constructed by software developers across the world, so to speak. Software development processes increasingly rely on collaboration between worldwide developers. From such collaboration comes all kinds of software development infrastructure such as package managers, version managers, and code sharing and hosting platforms. According to our observations, code sharing and hosting platforms like Pastebin and GitHub have become the hotbed of malware. Many malicious executables are uploaded, after being Base64-encoded, to these platforms that often use HTTPS globally, making it especially difficult to detect malware through traffic analysis. At the same time, they are found to be related to a great number of information disclosure events, such as disclosure of developers' code snippets, user names and passwords of email accounts, and database structures.

1 Insights into Threats

1.1 19.3% of Attack Sources Initiating More Than One Type of Attacks

From the geographic distribution of attack source IP addresses in China, Beijing, Jiangsu, Zhejiang, Shandong, and Guangdong are the top 5 provinces/municipalities home to the largest number of malicious IP addresses in China. Globally, China and the USA are still the two countries with the largest number of attack sources. The distribution of attack victims is a bit different from that of attack sources. In China, victims are mostly found in the southeast coastal area. In the world, Southeast Asia and Europe are also frequently targeted besides China and the USA. Where economic activities are booming, users are most likely to be attacked. This reflects attackers' never-ending pursuit of money and fame.

Figure 1-1 National distribution of attack sources and targets in China (in thousands)

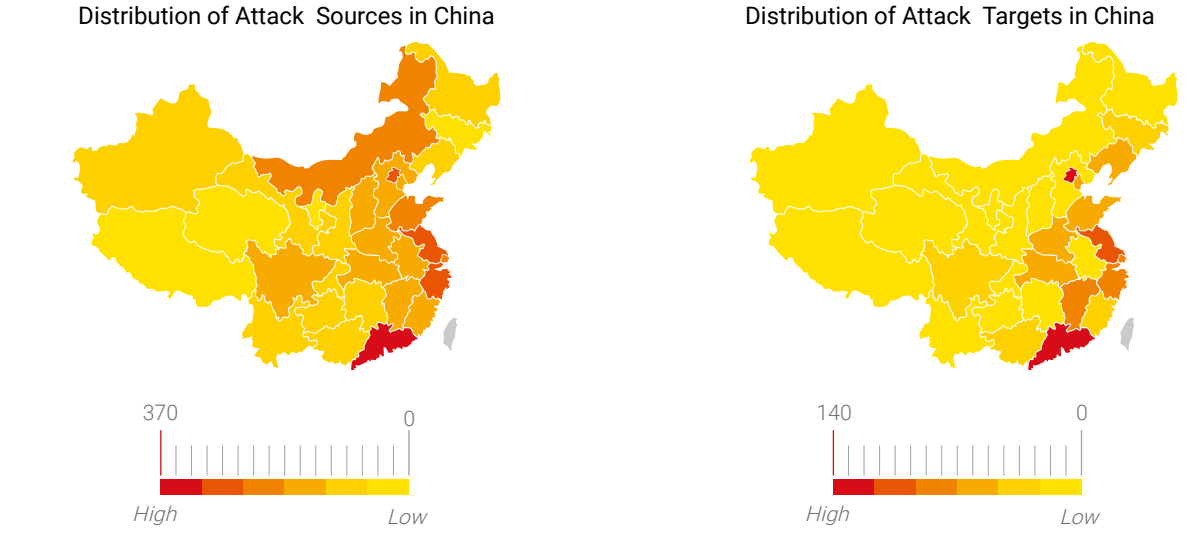
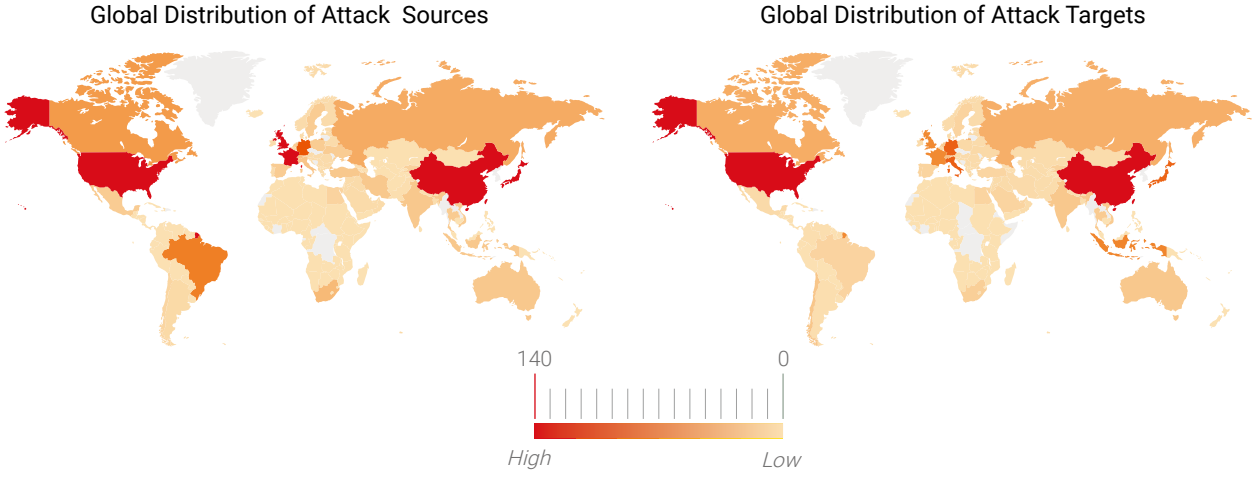
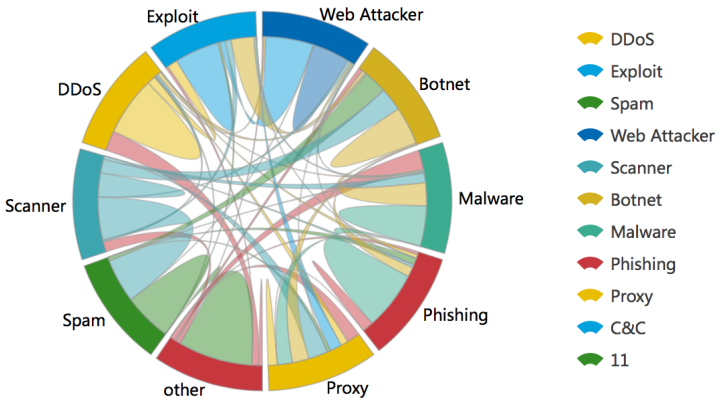


Figure 1-2 Global distribution of attack sources and targets (in thousands)



From behaviors of specific attack sources, about 19.3% of malicious IP addresses have launched more than one type of attacks.

Figure 1-3 Malicious IP addresses used for multiple purposes



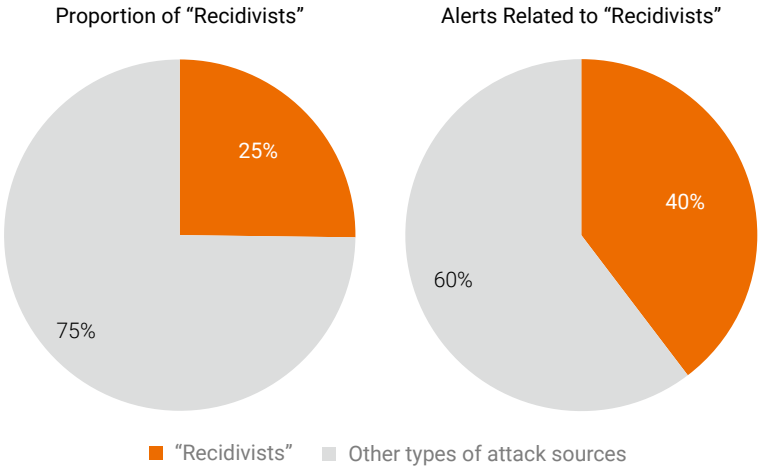
According to our observations, behaviors of attack sources change with time and follow some patterns:

- DDoS attack sources are not often seen in other types of attacks. 61% of DDoS attack sources have launched only DDoS attacks over a long period of time. This is closely related with the technical characteristics of DDoS attacks. Common DDoS attack resources include reflectors and controlled hosts or devices, whose IP addresses or IP address ranges are relatively fixed. However, we also notice that about 9% of DDoS attack sources launch exploit attacks later.
- Host resources used in exploits have a 24% chance of being flagged as bots later. We believe that a large proportion of bots are constantly and frequently used for vulnerability scanning and exploitation.
- Malicious scan sources have a 44% chance of becoming spam sources in future. Malicious scan and spam attacks both need large quantities of hosts or IP addresses. Therefore, the same batch of resources may be used for these two purposes at the same time.
- Web attack sources have a 50% chance of attempting more sophisticated exploit operations. Most attackers are not equipped with sophisticated security knowledge and skills. What they can do is use ready-made tools and scripts to cast as wide a net as possible for vulnerable hosts. Web attacks are a less complicated type of attack. In most occurrences, they are the first attempt before a real attack against servers. Specifically, attackers gain low-level privileges or obtain sensitive information via web vulnerabilities and then, based on intelligence previously collected, further exploit vulnerabilities for more targeted penetration and exploits.
- 20% of host resources used as proxies will be used for malicious scans later. Some of these hosts are likely to be most frequently used or even owned by hackers. While hackers use hosts as traffic proxies to hide their real identities, they just as easily use such hosts for simple reconnaissance before attacks.

1.2 "Recidivist" Attack Sources

Among more than 27 million attack sources detected by NSFOCUS in the first half of 2018, the proportion of "recidivist" attackers was too large to ignore. Recidivists here refer to attack sources found to be repeatedly linked with malicious behaviors. The large proportion of recidivists indicates that it is a common practice among attackers to reuse attack resources. Of all the detected attack sources, 25% were responsible for 40% of attack events. This implies that "recidivists" are more threatening than other attack sources and should be given greater attention.

Figure 1-4 Number of "recidivists" and proportion of alerts related to "recidivists"



China, the USA, and Russia are home to the most "recidivists". In terms of the number of attack targets, Canada and many European countries follow China and the USA, which are still the most targeted by attackers. As for China, "recidivists" are mostly distributed in coastal cities and populous provinces, with economically developed regions as most favored targets.

Figure 1-5 Global distribution of "recidivists" and their targets (in millions)

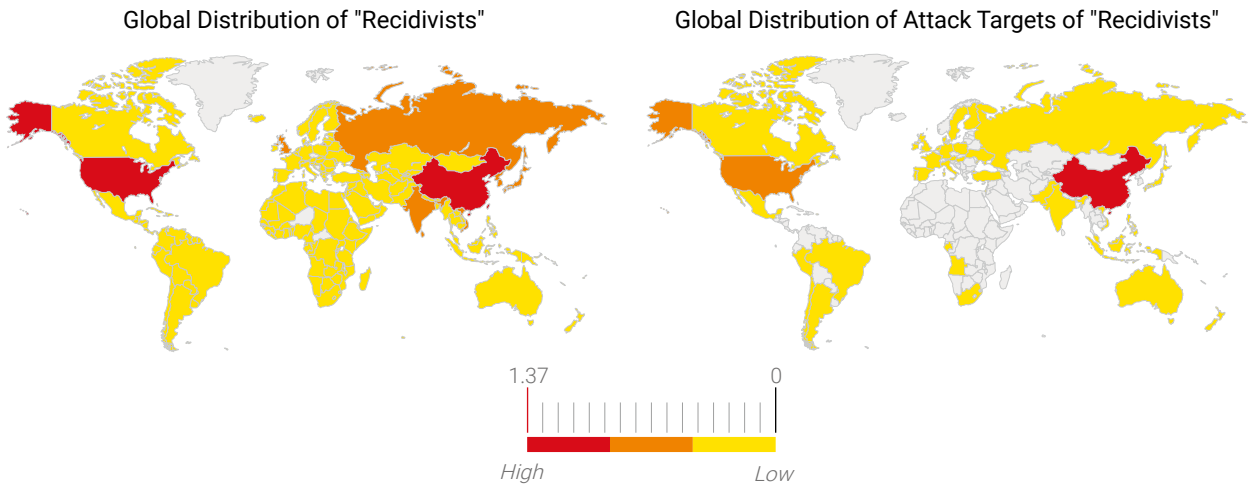


Figure 1-6 National distribution of attackers in China

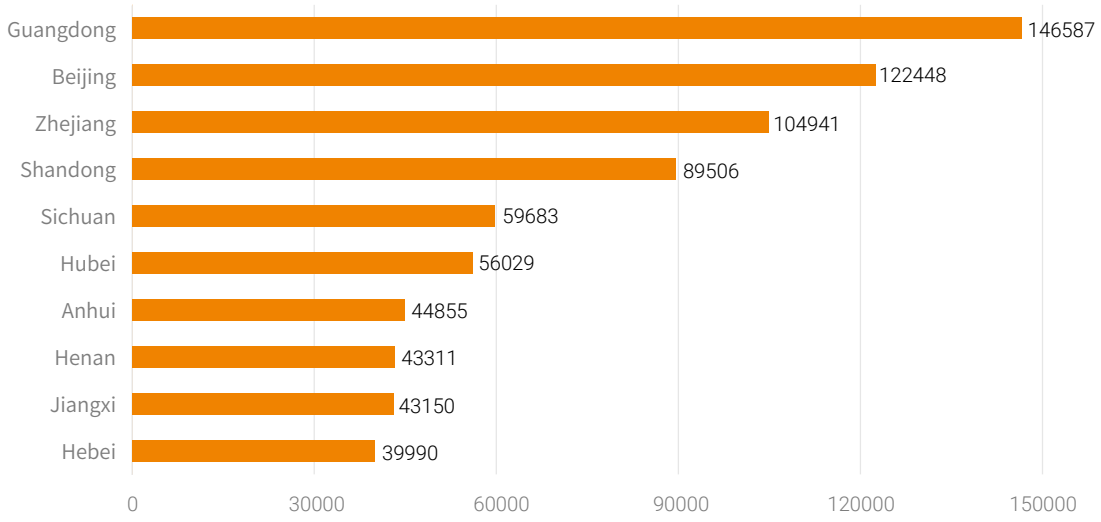


Figure 1-7 National distribution of attack targets in China

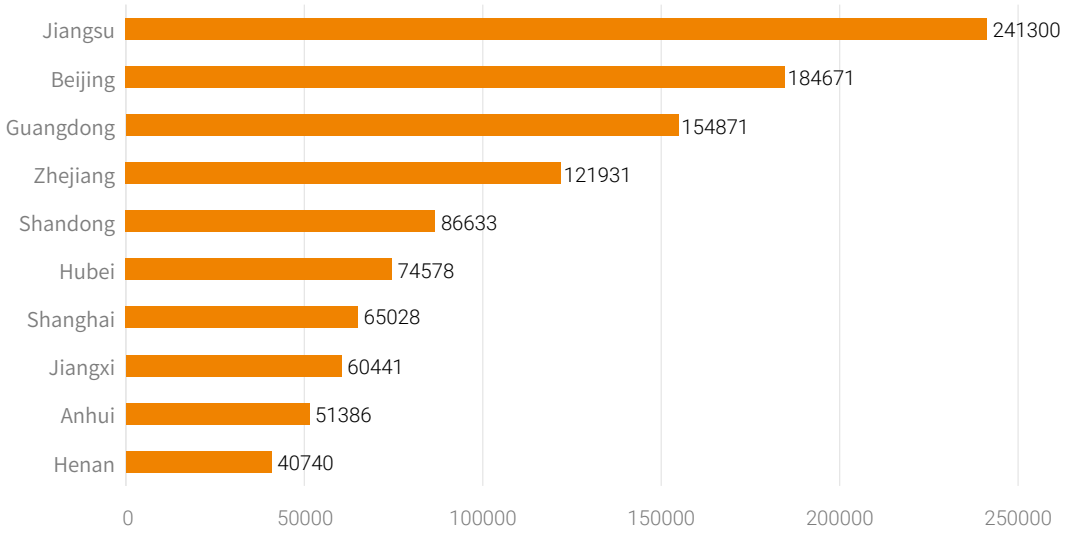


Figure 1-8 Major types of attacks launched by "recidivists"

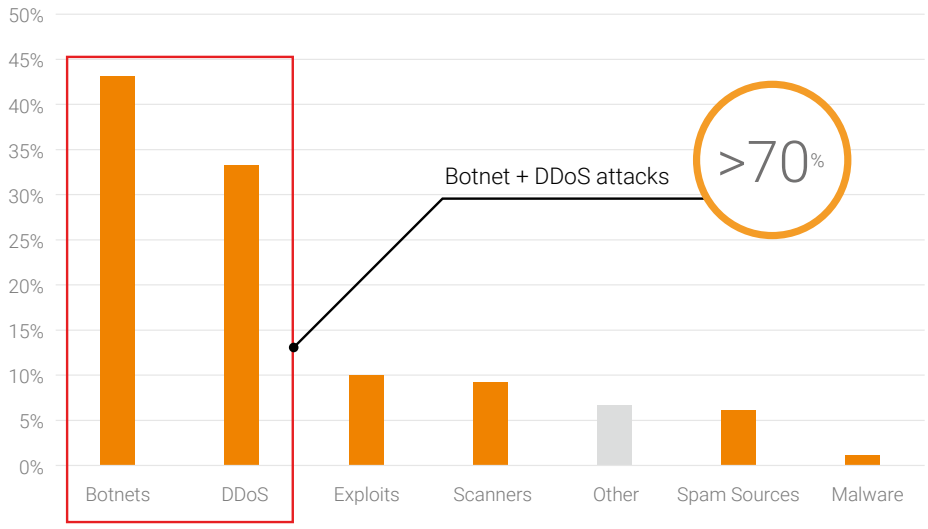
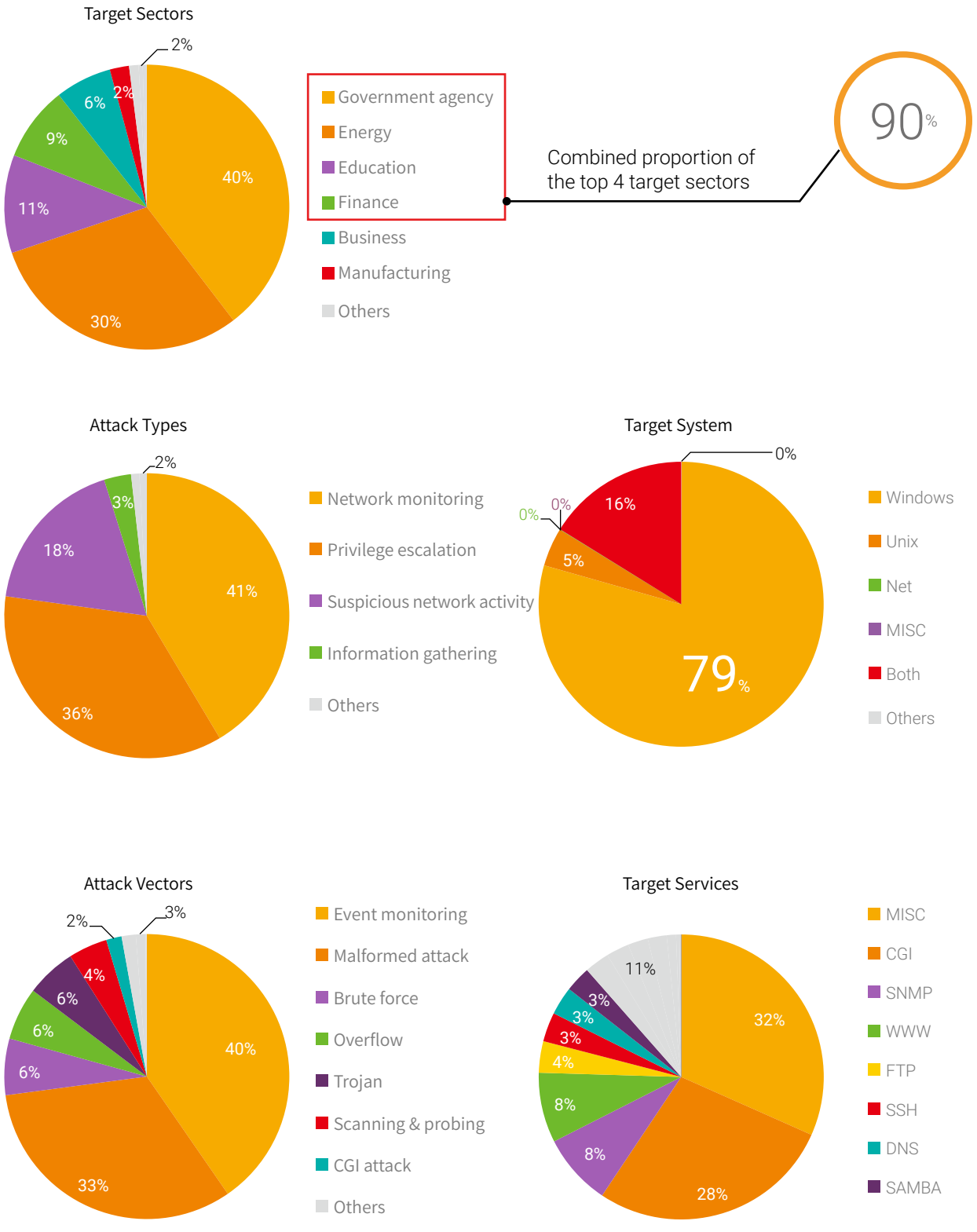


Figure 1-8 shows major types of attacks launched by "recidivists". These attacks account for more than 90% of the total. Obviously, botnets and DDoS attacks see the most frequent involvement of "recidivists", taking up over 70%.

"Recidivists" follow some patterns when launching attacks:

- Attackers usually prioritize their attack targets and methods based on their understanding of the characteristics of each sector and the operators' weaknesses. As for "recidivists", government agencies, energy, education, and finance sectors are most favored targets, suffering 90% of attacks, owing to the large volume of business, extensive distribution, and more sensitive data.
- Every cyberattack is launched via a point of entry. Attackers may first discover vulnerabilities or open services through unauthorized scans. They may also collect data by means of social engineering or use publicly available data or phishing emails to obtain more information before choosing an appropriate target. Network monitoring, privilege escalation, and suspicious activities account for 95% of all "recidivist" attacks. This means that hackers have done a lot of work in reconnaissance and intrusion phases.
- Compared with other operating systems, Windows is obviously favored by hackers, suffering 75% of "recidivist" attacks. From the attack types, while promptly fixing security issues in operating systems is a priority, efforts should be revved up to standardize administrators' security-related operations.
- Top 5 attack vectors contributed 91% of "recidivist" attacks. Event monitoring and malformed attacks are most frequently used, found in 73% of "recidivist" attacks. The malformed attack is conducted by sending malformed packets to a target system, causing the machine to spend an unusually long time parsing such packets, report errors, or even crash. A large number of such packets will pose a serious threat to the target machine. Brute-force cracking is another commonly used method. It consists of an attacker trying many passwords one by one with the hope of eventually guessing correctly. This method seems inefficient, but can be very effective by creating a weak password dictionary, which facilitates password cracking.

Figure 1-9 "Recidivist" profiling



1.3 Security Threats and Events Being Frequently Reported

In early June 2018, AcFun suffered a serious information disclosure breach, affecting tens of millions of users and becoming a newsmaker that caused widespread concern across China. This is another example of the virtual cyberspace sounding the alarm with a real-world consequence for information security management. In the Internet, the offensive and defensive sides never stop fighting. In addition to traditional methods of using techniques to implement attacks, attackers may collude with insiders for gradual penetration. However, due to the lack of cohesive monitoring & detection measures and analysis methods, many administrators are unable to see this battle and, thus, unaware of what is happening, until the breach comes to light. Therefore, it is especially important to establish security monitoring and management systems for different business assets and risk levels with multiple levels of granularity. For some sensitive resources, profiling should be conducted around key behavioral characteristics to dig out potential risks.

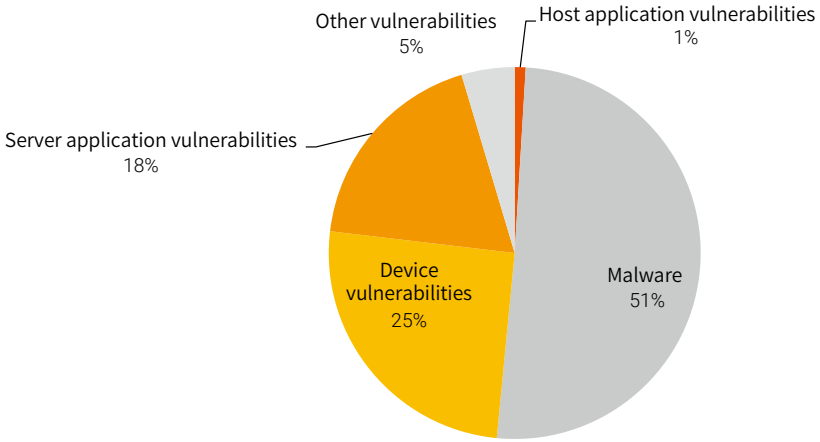
NSFOCUS Threat Intelligence center (NTI) routinely tracks activity of known hacker groups and events (including advanced persistent threats (APTs). Some of our NTI analysis may be useful for proactive threat mitigation. For example, while monitoring based on key indicators of compromise (IoCs), we found some suspicious traffic that indicated risks to some of our customers. Based on IoCs most frequently found in our traffic monitoring, we list here related events or organizations, with the hope of informing security professionals who are working to enhance the security of their networks:

- **Unauthorized access to Hadoop YARN.** In May 2017, NTI detected a number of attacks against Hadoop YARN. In these attacks, hackers directly called the REST API of the Hadoop YARN cluster without authentication to perform arbitrary command execution. These attacks were eventually used for cryptomining. Based on IoCs, we conducted ongoing monitoring of attackers involved in these events. As of June 2018, attacks against Hadoop YARN were still frequently detected.
- **Cryptominer targeting WebLogic hosts.** In December 2017, NTI detected a series of automated attacks launched by exploiting the WebLogic deserialization vulnerability (CVE-2017-3248). After being infected, a cryptominer was installed on a WebLogic host and would proceed to consume large amounts of host resources. After developing an attack profile, we monitored WebLogic hosts for such events based on IoCs. In the first half of 2018, malicious exploit and malware delivery were still frequently seen for the purpose of cryptomining via WebLogic hosts.
- **Operation Cobalt Kitty.** This is a series of attacks reported by the security company Cybereason. These attacks are directed at Asia, with the goal of compromising businesses to steal their mission-critical data. These attacks all share the same tactics, techniques & procedures (TTPS). Cybereason dubbed the operation "Cobalt Kitty" in May 2017 and released their resulting analysis. According to our monitoring, the first half of 2018 still saw similar IoCs in some networks, which may be connected with the original threat actor.

1.4 Malware Activities Still Rampant, with Cryptominers Standing Out as a New Source of Infection

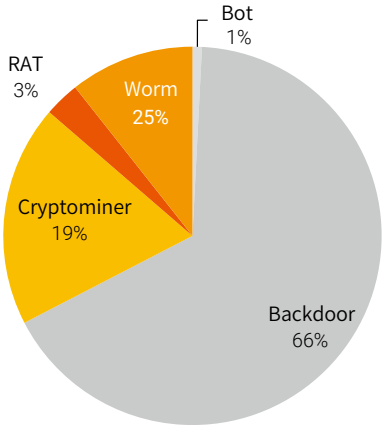
Overall, vulnerability exploitation still accounts for a large proportion of attack traffic. Exploits against servers make up 18%, while those against host applications make up 1%. It is worth noting that malware activities are extremely rampant this year according to our observations. Through monitoring of malicious network behaviors, we detected various activities linked to cryptominers, worms, Trojans, botnets, and backdoor programs.

Figure 1-10 Distribution of malicious activity types



In terms of activity, backdoors, cryptominers, worms, remote access Trojans (RATs), and botnets are top 5 malware types. Cryptominers are a type of malware that has stolen the limelight this year. In recent years, people from all walks of life have shown a keen interest in Bitcoins, Monero, and other cryptocurrency, hence the booming business there. We have found that various malicious cryptominers, represented by WannaMine, have started to be spread extensively.

Figure 1-11 Distribution of malware types



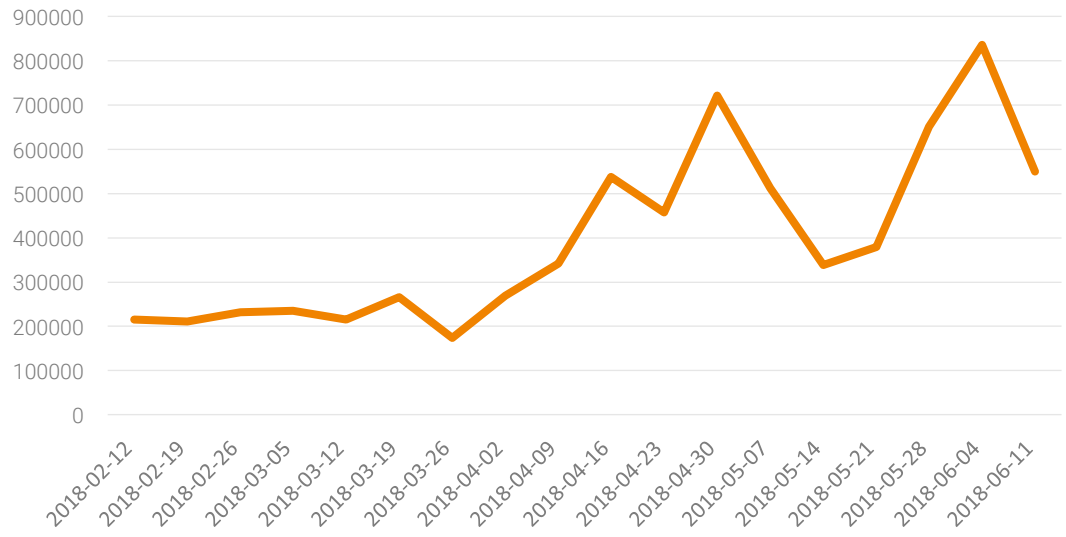
Moreover, in the first half of 2018, some malware families and variants spread vigorously. We strongly recommend administrators be aware of this activity and check their networks and systems as soon as possible. As there is no uniform standard for classification of viruses and as viruses are not generally designed using coding best practices, they tend to be tailored and spliced according to vendors' actual needs and habits. As a result, a virus classified as a Trojan is likely to have characteristics of a worm, and a backdoor may have characteristics of a Trojan. Based on an intuitive understanding from studying hundreds of malicious samples, we roughly classify viruses according to the essential nature or functionality of code as follows:

- Worms are characterized by the large-scale self-propagating capability;
- Trojans take information theft and other complicated actions like remote control as their core functionality;
- Bot programs are characterized by construction of botnets from computer clusters for large-scale hacking activities (such as DDoS attacks and cryptomining);
- Backdoors and Trojans are much alike, but the former are mostly used to provide a persistent entrance for further attacks.

Active Cryptominers

The first half of 2018 witnessed cryptominers becoming increasingly active. Since the end of March, the number of cryptomining activities has risen sharply compared to the beginning of the year.

Figure 1-12 Monitoring of cryptomining activities

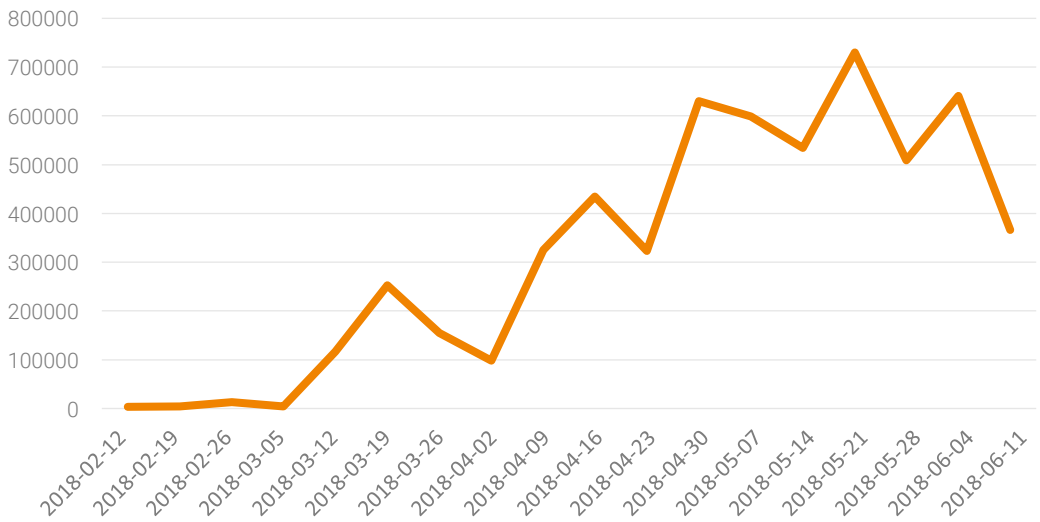


Among all cryptominers, WannaMine was the most active, responsible for more than 70% of all detected cryptomining activities. This virus was first detected at the beginning of 2018 by CrowdStrike and was named so because it is spread via the EternalBlue vulnerability like the notorious WannaCry.

Active Worm Viruses

Worms were nearly dormant in February, but became increasingly active from March to June. Although their activity fluctuated up and down, the general trend was on the rise.

Figure 1-13 Worm activity monitoring



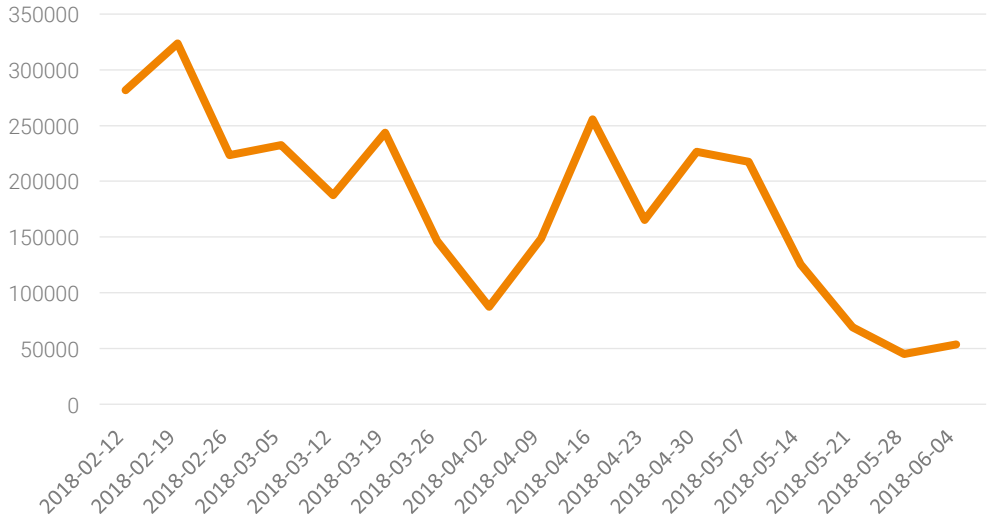
According to our observations, as many as 28 worm viruses have remained active for a long time and most of them were first discovered more than five years ago. This indicates how capable these viruses are of propagating and evolving and how difficult it is to remove them completely from a network. This year, the following two worms are found to be most active:

- **W32.Faedevour.** This is a worm that opens a backdoor and steals information from the compromised computer. According to our statistics, the W32.Faedevour family tops the list of worms due to its fast propagation and spreading.
- **Conficker.** Also known as Downup, Downandup, Downadup, and Kido, it is a computer worm that was first detected in October 2008 to target the Microsoft Windows operating system. After extracting the virus family's interaction patterns, we monitored the worm continuously and found that it had never ceased propagating and spreading and, in fact, its traces of activity are still here on the Internet in the first half of 2018. However, it is also possible that other virus families used Conflicker's communication mechanism for spreading, resulting in similar traffic.

Active Trojans

During the first six months of 2018, Trojans were a bit less active. Moreover, we discovered fewer new Trojan variants than botnets and worms over this period. This is probably linked with the proliferation of networked hosts and IoT devices in part due to the reduction of hardware costs in recent years. As a result, large quantities of malicious code can be rapidly spread very easily across the new and insecure systems online. Amid this trend, heavyweight Trojans with complicated functions lag behind botnets and cryptominers that are easier to develop and evolve.

Figure 1-14 Trojan activity monitoring

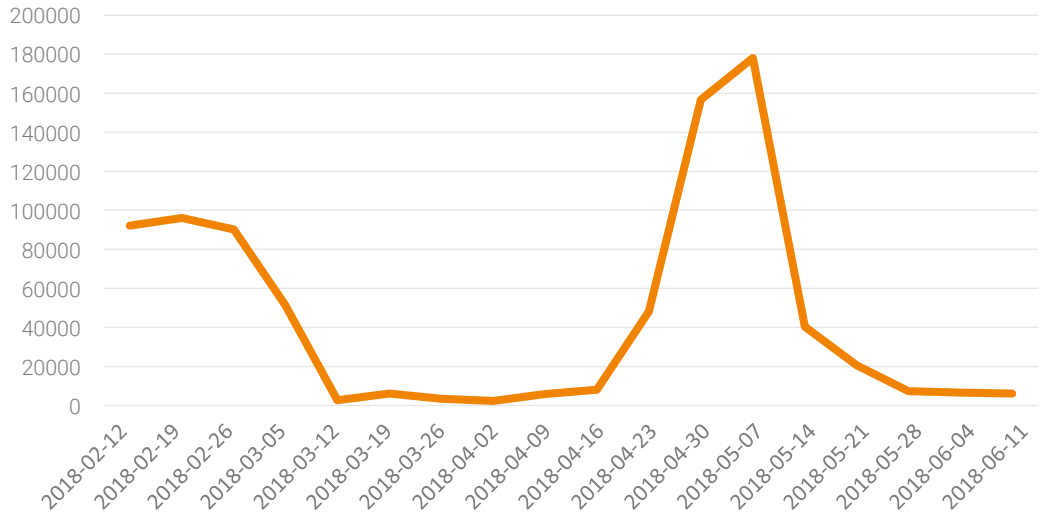


Still, we found more than 30 active Trojan families. Needless to say, these programs are very harmful. This year, the most active Trojan is Bootkit, which had infected millions of computers when first discovered in early 2015. With the Rootkit + Boot capability, this Trojan directly infects the boot sectors of a hard drive and is very hard to remove even if the hard drive is reformatted. In the first half of 2018, Bootkit was still active. Security professionals are advised to monitor and review their environments for potential incursion.

Active Bot Programs

The activity of botnets seems to be connected with that of backdoors. In early May, both bot programs and backdoors saw spikes in activity in the first half of 2018.

Figure 1-15 Botnet activity monitoring



Unlike worms and Trojans, currently active bot programs are either new virus families or variants of existing families, both with the core functionality and application remaining unchanged; that is, channeling a volumetric flood of DDoS traffic. Just as NSFOCUS's *2017 Botnet Trend Report* [2] points out, these programs keep evolving and upgrading and can provide more stable DDoS attack capabilities, generate increasingly large traffic, and make botnets reusable. From botnet infection to malware sale then to Botnet as a Service (BaaS), an entire black industrial chain has come into being. Our monitoring in the first half of 2018 found the following active families:

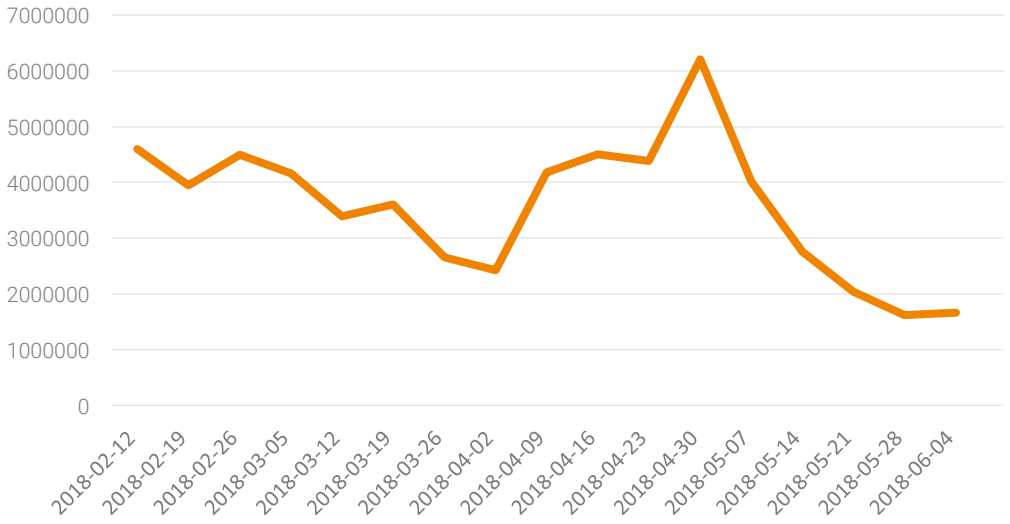
- **BillGates botnet.** This is a widely used bot program discovered and named in 2016. This program aims to set up botnets for volumetric DDoS attacks.
- **Artemis botnet.** Discovered and disclosed in 2015, this botnet is still widely used for DDoS attacks.

2 https://nsfocusglobal.com/2017-botnet-trend-report/

Active Backdoor Programs

Backdoor programs open backdoors on devices, usually routers. In the first half of 2018, backdoor activity remained at high levels and then peaked in May before falling to more nominal levels.

Figure 1-16 Backdoor activity monitoring



Backdoors are common malicious programs that can provide remote control access solely through default login interfaces of Internet of Things (IoT) devices. In the most frequent 20+ backdoor programs, five are related to accessing routers. The high activity of backdoor programs should remind device and network administrators that it is critical to upgrade devices and check their configurations regularly. Following are two backdoor applications that deserve much attention:

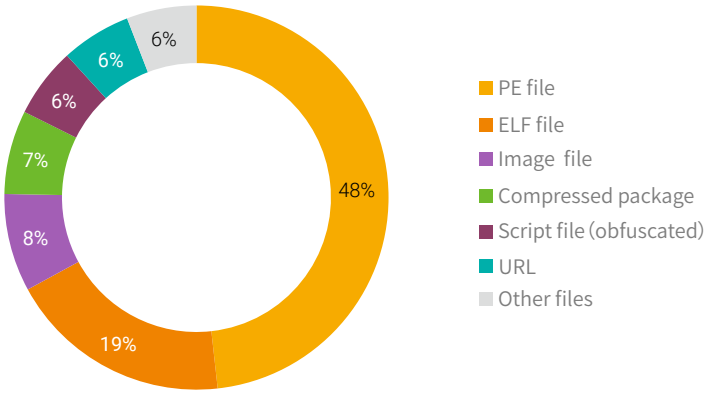
- **Netcore/Netis router backdoor.** In the *2017 Cybersecurity Insights*, we pointed out that the Gafgyt bot family was rather rampant, with the backdoor in the Netcore router (which was disclosed and fixed early in 2014) as the main target. Even now, it is still frequently detected, as active as it was at the end of 2017.
- **DoublePulsar backdoor.** Compared with the Netcore backdoor, DoublePulsar features more sophisticated techniques. The NSA hacking tools disclosed by Shadow Brokers in 2017 exploited this backdoor, which was later widely spread and seriously impacting the Internet. This backdoor was frequently spotted in our daily monitoring over the first half of 2018.

1.5 Abuse of Code Sharing Platforms like Pastebin Getting Worse

Pastebin and GitHub are two popular code sharing and hosting platforms. Malware tends to leverage them to spread key information. In the first half of 2018, we found that more and more malware families were following suit. NTI's monitoring of multiple code sharing and hosting platforms finds the abuse of such platforms an increasingly serious threat.

Take Pastebin for example. To store non-text data on this platform, some users encode binary data with the Base64 scheme before uploading it to Pastebin. According to our observation, the Base64-encoded text uploaded each day carries a variety of files or text, as shown in the following figure.

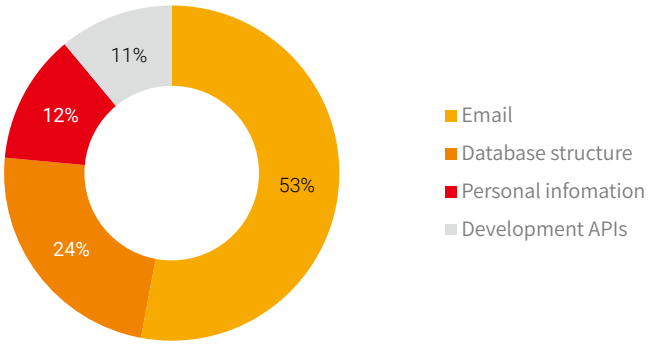
Figure 1-17 Distribution of Base64-encoded data types



Through analysis, we believe that most executables uploaded are malware and find that some URLs and IP addresses are listed in our NTI Command & Control (C&C) server database. Ironically, such code sharing and hosting platforms are well reputed. They use HTTPS encryption throughout the communication, so security products can only detect threats on the device side, thus significantly weakening the security defense mechanism. To bypass monitoring of in-platform code and text, attackers take to other encoding methods or use other encryption algorithms on the basis of Base64 encoding, making the governance of public platforms an even harder task.

There are other types of abuse that cannot be neglected. Every day, a large number of email addresses and passwords are uploaded to Pastebin as part of code development. Some developers even upload code snippets to the platform, which include database structures and API keys.

Figure 1-18 Distribution of disclosed data types



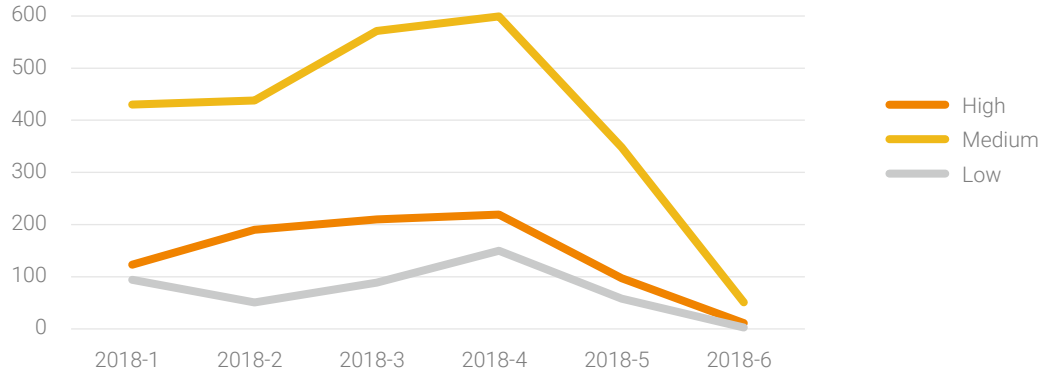
Such types of basic information from software development are crucial to business security. Attackers regularly try to forage valuable information from code sharing and hosting platforms during the information collection stage before actual intrusion. Such information, once exploited, will pose a serious threat to business continuity.

2 Insights into Vulnerabilities

2.1 More Medium-Risk Vulnerabilities Exposed Due to Permission Control Issues

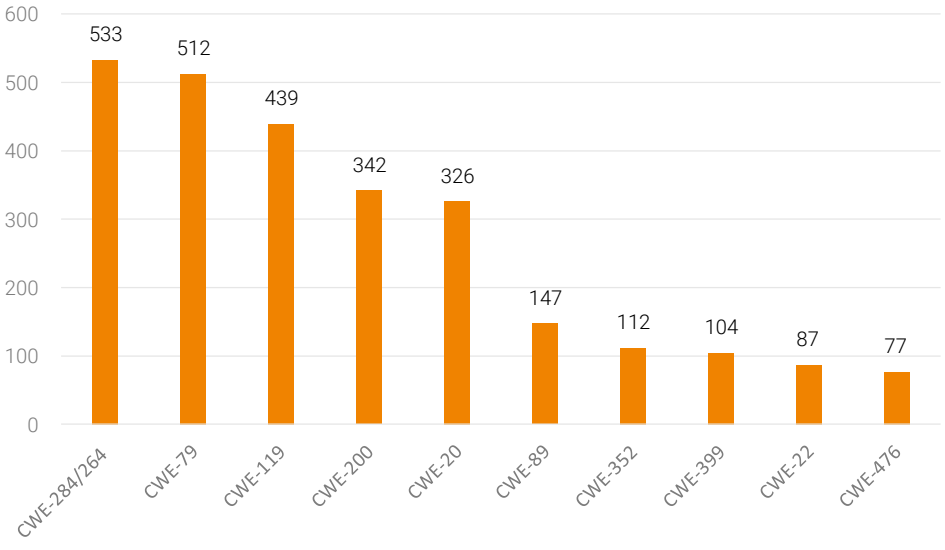
By June 19, 2018, a total of 3731 vulnerabilities identified with CVE IDs have been disclosed on the official National Vulnerability Database (NVD) website, of which 850 were high-risk, 2437 were medium-risk, and 445 were low-risk. Compared with the same period last year, this year sees a smaller number of vulnerabilities, with an increase in the proportion of medium-risk ones but a corresponding decrease in high-risk and low-risk ones.

Figure 2-1 Monthly number of vulnerabilities exposed



Medium-risk vulnerabilities have quite a big impact on the integrity of system information and the availability of system functions yet are very difficult to exploit. If proof of concept (PoC) code or tools are available, exploiting these vulnerabilities will cause extensive damage.

Figure 2-2 Distribution of different types of vulnerabilities



As shown in the preceding figure, the top 10 vulnerability types are as follows:

- **CWE-284/264 (privilege control):** This kind of vulnerabilities is the most frequently exposed. Vulnerabilities, mostly medium-risk, like out-of-bounds access and privilege escalation, have a close connection with specific business functions. High-risk vulnerabilities, however, mainly exist in operating systems of servers, applications like databases, and some open-source content management systems.
- **CWE-79 (cross-website scripting vulnerabilities):** This kind of vulnerabilities ranks second in terms of exposure. There are numerous such vulnerabilities that are especially common in various website building systems and are almost impossible to effectively protect against. Such vulnerabilities, if exploited independently, may pose minor threats, but when combined with other vulnerabilities, may contribute to a complicated attack through which attackers can gain system privileges.
- **CWE-119 (out-of-bounds memory operation):** By exploiting these kind of vulnerabilities, hackers can obtain privileges for executing arbitrary code, causing the system to crash at times. In the first half of 2018, among these vulnerabilities, 216 are high-risk and 217 are medium-risk. The top 3 products that are most susceptible to these high-risk vulnerabilities are browsers and Microsoft Office software, including Microsoft Edge, Internet Explorer, and Office Word.
- **CWE-200 (information exposure):** Hackers could exploit such vulnerabilities to cause disclosure of sensitive information. Also, these vulnerabilities could circumvent privilege controls in some device firmware, causing the devices to be compromised. The information disclosure vulnerability assigned CVE-2018-10106 in the D-Link device firmware is such an example. In terms of the vulnerability distribution, Windows Server 2016 tops the list of vulnerable products.
- **CWE-20 (improper input validation):** Via malformed input, hackers can cause programs to behave abnormally, allowing taking control of, stealing information from, and taking down devices as well as achieving other malicious purposes. In the first half of 2018, 61 vulnerabilities of this kind were found high-risk.
- **CWE-89 (SQL injection):** SQL injection is now a very conventional attack in which an attacker submits carefully crafted SQL statements to the system, tricking it into executing them while bypassing the system's protection mechanisms. This kind of attack is usually used against applications like web pages and tend to cause quite a great damage.
- **CWE-352 (cross-site request forgery):** Cross-site request forgery (CSRF) is a common attack method used to pass traffic from a malicious website to a target website within the tabs of a web browser. In the first half of 2018, 112 CSRF vulnerabilities were assigned CVE IDs.
- **CWE-399 (improper memory resource management):** This category is inclusive of a wide spectrum of vulnerabilities as memory resource mismanagement may cause serious consequences. For example, improper system-level management behaviors like memory allocation and release and object destroying can lead to arbitrary code execution and denial of service.
- **CWE-22 (path traversal):** By exploiting this kind of vulnerability, an attacker, via crafted input, could access all or part of files or directories that are outside of the restricted directory.
- **CWE-476 (NULL pointer dereference):** Like out-of-bounds memory operations and improper resource management, this kind of vulnerability could cause a system crash or code execution.

2.2 Device Vulnerabilities Looming Large

Vulnerabilities in devices are especially severe when viewed from such angels as ease of resource acquisition, vulnerability exploitation, and damage to the system after successful exploitation. This is because device resources, which are available in large quantities, are easy to obtain due to poor protection. Vulnerabilities in devices are usually not difficult to exploit and once successfully exploited, they could allow attackers to gain high system privileges of devices. Thus, these vulnerabilities inevitably find great favor with attackers. In view of the severity of the vulnerability situation, security vendors and cybersecurity professionals should pay great attention to these vulnerabilities and explore related defense techniques as well as solutions to address them. The following table lists device vulnerabilities disclosed in the first half of 2018. We can see that vulnerabilities that are easy to obtain, exploit and could cause great damage mainly exist in products from four vendors of mobile devices or network gateways.

Table 2-1 List of device vulnerabilities disclosed In the first half of 2018

Vendor	Product/Firmware	Major High-Risk Vulnerability
D-Link	DSL-3782 DIR-629 DSL-2640U DIR-880L	CVE-2018-10746 CVE-2018-10747 CVE-2018-10748 CVE-2018-10749 CVE-2018-10996 CVE-2018-5371 CVE-2018-6530 CVE-2018-8941
Mitel	ST14.2	CVE-2018-5779 CVE-2018-5780 CVE-2018-5781 CVE-2018-5782
Qualcomm	SD 850 SDM 660 SD 845	CVE-2018-3589 CVE-2018-3590 CVE-2018-3591 CVE-2018-3592 CVE-2018-3593 CVE-2018-3594
Cisco	D9800 FTD RV132W Secure Access Control System IOS XE ...	CVE-2018-0099 CVE-2018-0101 CVE-2018-0125 CVE-2018-0147 CVE-2018-0150 CVE-2018-0151 CVE-2018-0152 CVE-2018-0171 CVE-2018-0238 CVE-2018-0253 CVE-2018-0258

In addition to the vulnerabilities listed above, there are still numerous ones that have not yet been assigned CVE IDs or pose low-risk threats. In the first half of 2018, we released analysis reports or threat advisories regarding the following vulnerabilities:

- Vulnerability in Schneider Pelco Sarix Professional cameras
- 0-day vulnerability in DrayTek routers
- Multiple vulnerabilities exploited for spread of VPNFilter malware

In the *2017 IoT Security Report*[3], we summarized botnets and worms that targeted various types of new devices. We also pointed out that IoT threats and protection against them is no longer an abstract concept to the general public, but has galvanized public concern since the massive propagation of Mirai in 2016. In 2017, we observed that a variety of malicious programs such as Rowdy, DarkCat, and Gafgyt constantly evolved, with a focus alternating between routers, cameras, and TV set-top boxes (STB). It is worth noting that these devices are massively deployed globally, stay permanently online, and usually have generic hardware modules and firmware embedded in them. All of these device characteristics encourage the propagation of malware.

2.3 Lack of Governance on Code Management Infrastructure

As early as 1983, Ken Thompson, in his Turing-Award-winning paper *Reflections on Trusting Trust*, demonstrated how to embed backdoor code into compilers to affect the programs generated by the compilers. In 2015, the XcodeGhost malware turned this experiment into reality. Up until then, the software development process increasingly depended on the concerted efforts of developers from all over the world. At the same time, all kinds of software development infrastructure such as package managers, version control tools, and code sharing & hosting platforms came into being. The formation and proliferation of such infrastructure surely make developers more productive, but bring some security issues as well.

If an attacker successfully injects any code at all, it's pretty much game over. [4]

The security team of npm, a well-known package manager for JavaScript, released a report[5] in May, saying that they removed a package masquerading as a cookie parser which allowed an attacker to inject and execute arbitrary code in the server. Objectively speaking, other package management tools are also exposed to this kind of attack risk. However, npm's widespread application and overly complicated dependencies make it an easy target.

Figure 2-3 Dependence between malicious modules

```
mailparser
└── http-fetch-cookies
    └── express-cookies
        └──getcookies
```

In June 2018, Git, a code version control tool, was reported to contain a remote code execution vulnerability (CVE-2018-11235). The root cause was not sufficient validation for the submodule's folder name during the execution of the **git clone** command. Thus, once a user runs the **git clone –recurse-submodules** command, an attacker could create a repository containing a malicious "**.gitmodules**" file to achieve arbitrary code execution. Other Git-based version control tools such as SourceTree are also affected by this vulnerability.

3 https://nsfocusglobal.com/2017-annual-iot-cybersecurity-report/

4 https://developers.google.com/web/fundamentals/security/csp/

5 https://blog.npmjs.org/post/173526807575/reported-malicious-module-getcookies

3 Insights into Malicious Traffic

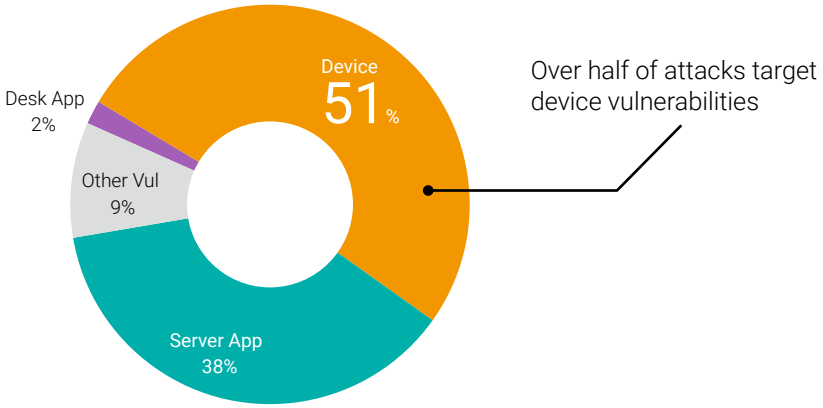
3.1 Vulnerability-based Attacks

Key findings:

- Among all attacks based on vulnerabilities, those exploiting device vulnerabilities account for more than 50%.
- Router vulnerabilities are still overlooked by security governance personnel.
- Windows servers, Java application servers, Apache servers, email servers, and DNS servers are at high risk as targets of vulnerability-based attacks. Therefore, special attention should be given to protection against vulnerabilities in such servers.
- Probe-based scanning never ceases on the network. Therefore, once vulnerable devices are exposed, they are likely to be compromised in a very short time.
- Vulnerabilities in desktop apps are usually exploited during phishing and spam attacks. Individual users should be vigilant against those attacks.

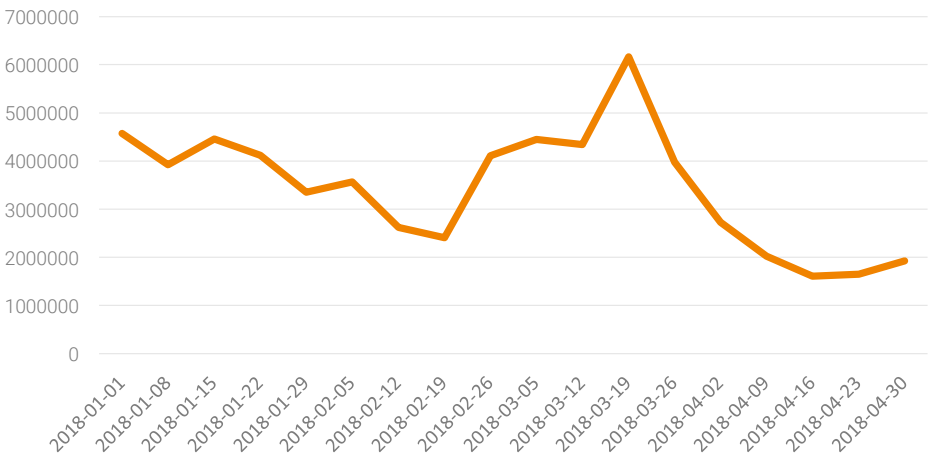
Here we classify vulnerabilities into server vulnerabilities, desktop application vulnerabilities, and device vulnerabilities in terms of the host environment and business scenario where vulnerabilities exist. Server vulnerabilities mainly reside in servers' system services and commonly used programs such as email services, HTTP services, and website scripting language parsing services, which provide or support network management and business functions. Desktop applications primarily provide document- & multimedia-related, and host management functions. Among commonly used applications are various clients (such as browsers and email clients), antivirus software, Microsoft Office software, Adobe Flash player, and PDF readers. Vulnerabilities in these types of software are frequently exploited. Very often, they are used with malware which usually spreads through a malicious mail or web page, enticing a user to execute the malware and, thus infecting the target host. Device vulnerabilities are a special new type of vulnerabilities. Mobile terminals and IoT devices are typical examples of such devices and they pose a new type of threat.

Figure 3-1 Distribution of vulnerability-based attacks by exploitation type



As shown in the preceding figure, attacks based on device vulnerabilities account for more than 50% of the total number of attacks, surpassing attacks exploiting server vulnerabilities which had been the dominant attack form over past years. This is mainly due to the dramatic increase in networked devices such as smart routers. As indicated in our *2017 IoT Security Report*[6] security issues have not been given serious consideration during the design of smart devices. As a result, as these types of devices are widely deployed, a lot of high-risk devices flood into the market and then are rarely updated or maintained. We find that, even though vendors have discovered device vulnerabilities or have provided upgrades, patches or fixes for those devices, an alarming number of devices are still vulnerable. This can be attributed to the poor design of device upgrade and maintenance mechanisms. After all, unlike traditional PCs, smart devices have no complicated built-in applications, and thus are incapable of providing various effective detection and defense services or automatic maintenance services. This makes it easy for attackers, using low cost and simple techniques, to attack such devices with a high rate of success.

Figure 3-2 Trend of router vulnerability exploits



6 https://nsfocusglobal.com/2017-annual-iot-cybersecurity-report/

In the first half of 2018, attacks based on router vulnerabilities are less effectively curbed than other types of attack traffic. This reflects that these types of vulnerabilities have not been given due attention for a long time. According to our monitoring data, the following vulnerabilities are most frequently exploited by hackers for attacks:

- Netcore/Netis router backdoor vulnerability
- TP-Link wireless router HTTP/TFTP backdoor vulnerability
- ASUS WRT firmware backdoor command execution vulnerability (CVE-2014-9583)
- D-Link router User-Agent backdoor vulnerability (CVE-2013-6026)
- Motorola wireless router WR850G authentication bypass vulnerability (CVE-2004-1550)
- Linksys WRT54G wireless router apply.cgi overflow remote security vulnerability (CVE-2005-2799)
- Cisco IOS router denial-of-service vulnerability
- Huawei HG532 router remote command execution vulnerability (CVE-2017-17215)
- HP/H3C and Huawei switch/router SNMP access sensitive information disclosure vulnerability (CVE-2012-3268)

As for server vulnerabilities, Windows servers receive the most attacks, closely followed by servers from Oracle. Counting WebLogic servers together with other Java application servers, we find that up to 27% of Java application servers are attacked. Apache servers, email servers, and DNS servers are easy targets on which related services are frequently probed and attacked. Among all attacks against servers, about 5% are probe-based scans in which hackers check for vulnerabilities with automatic scan tools and a large amount of code for known vulnerability exploitation. Once vulnerabilities are discovered, hackers promptly take advantage of them to compromise the server. Therefore, sever administrators should perform vulnerability scans and make sure to upgrade related devices and services on a regular basis. Vulnerabilities that were disclosed previously should be fixed as soon as possible. Typically, server vulnerabilities are frequently exploited in April to June, base on the approximately 200,000 attacks are detected every day during that period.

Figure 3-3 Distribution of vulnerabilities in server services

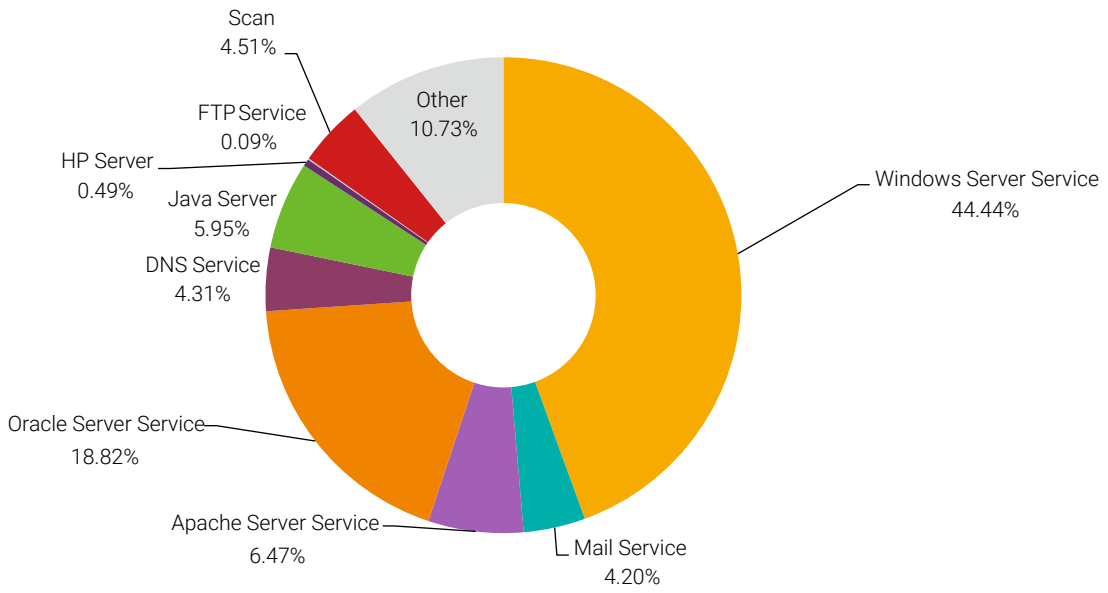
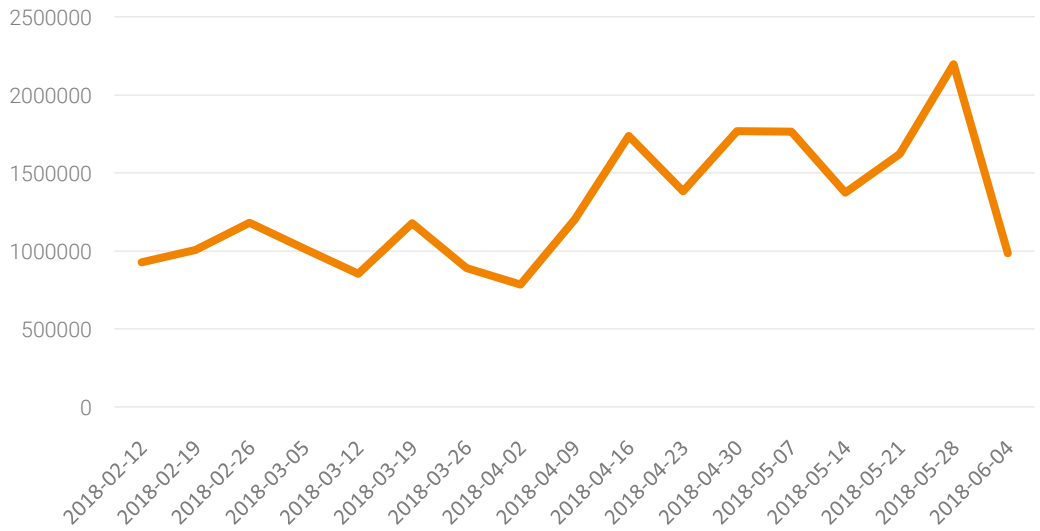


Figure 3-4 Trend of server vulnerability exploits



Attacks based on vulnerabilities in desktop applications mainly target individual users, of which some are administrators of core assets. A typical attack flow includes:

- The hacker delivers a malicious program by sending a phishing email that contains a malicious link or attachment.
- When a user is tricked into clicking the malicious link or attachment, the malicious program will be downloaded and to exploit the vulnerability in a related program, finally infecting the user's machine and causing information disclosure.

As shown in the following figure, vulnerabilities in browsers, applications on Apple hosts, Microsoft Office software, PDF readers, and Adobe Flash Player are most favored by attackers.

Figure 3-5 Distribution of desktop application vulnerability exploits

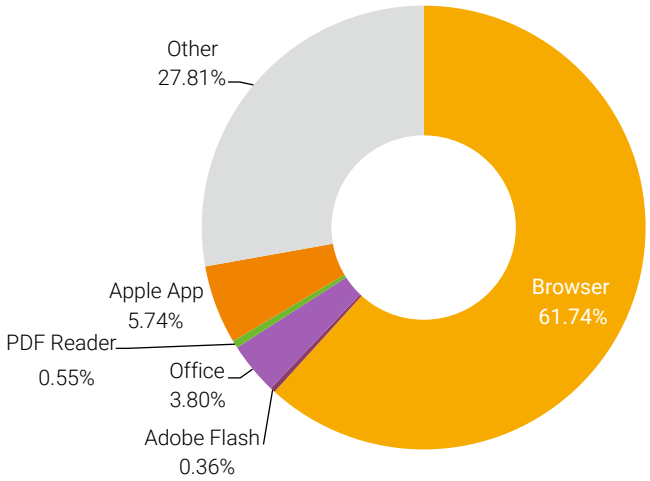
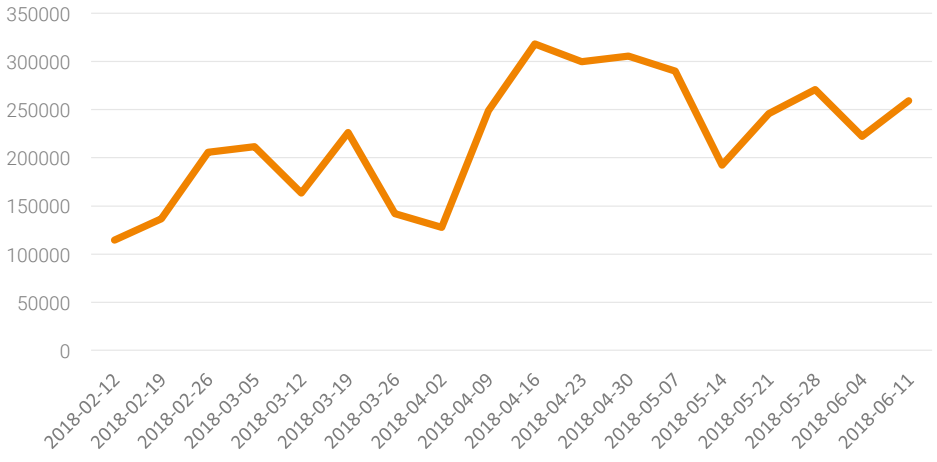


Figure 3-6 shows the trend of desktop application vulnerability exploits. As shown in Figure 3-4 and Figure 3-6, we can see that such vulnerabilities have a similar exploitation trend as server vulnerabilities, especially in April when both kinds saw an upward trend. In the first half of 2018, the number of desktop application vulnerability exploits peaked in April. This reflects that frequent vulnerability exposures entice attackers to test their abilities. Also, we can see the time from vulnerability/PoC announcement to vulnerability exploitation is becoming increasingly shorter. This is evident in Drupal monitoring data from early April which shows that it took only six days from PoC announcement on April 13 to detection of a large number of attacks on April 18. Compared with server vulnerabilities, desktop application vulnerabilities began to show an upward trend after April and were still active in June. It should be noted that desktop application vulnerabilities are less targeted than server vulnerabilities on average, with about 40,000 attacks occurring each day during peak times.

Figure 3-6 Trend of desktop application vulnerability exploits



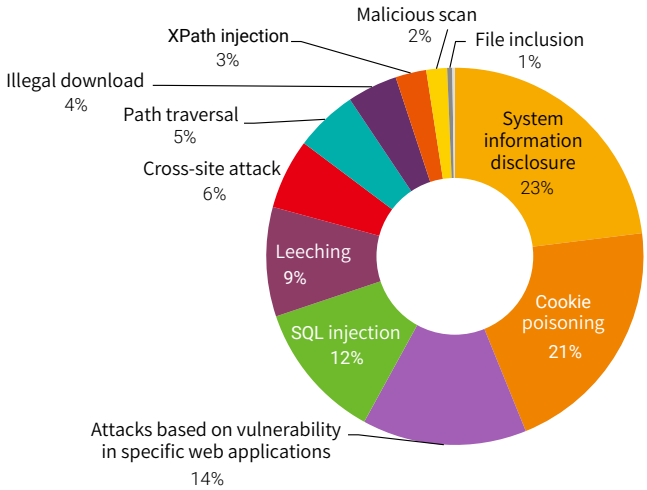
3.2 Website-Targeting Attacks

Key findings:

- Among website security events that occur frequently, traditional attacks account for a large proportion and still deserve great attention.
- Vulnerabilities in Struts frameworks are still frequently exploited by hackers.
- As the website vulnerability exploit cycle is significantly shortened, web masters should upgrade websites more frequently.
- Deploying a WAF is mandatory in this day and age.

Traditionally, users tend to focus on new and complicated vulnerabilities as well as vulnerabilities with a broad influence. Actually, during daily business operations, users inevitably face various probes ranging from simple scans to insidious attacks with an extremely high degree of concealment. Proportionally, besides high-risk vulnerabilities, emerging vulnerabilities also have an adverse impact on assets. As far as website management is concerned, traditional attacks can be very annoying. For example, SQL injection attacks and cookie poisoning keep pestering websites all the year round.

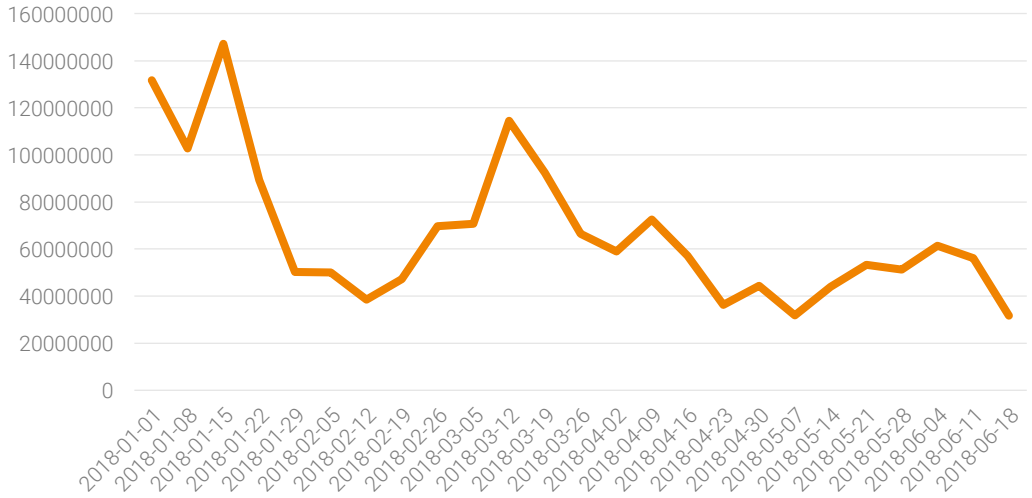
Figure 3-7 Distribution of website-targeting attacks



Many administrators are inundated by alerts from attacks shown in the preceding figure and do not take them seriously. However, it is not unusual for these seemingly common behaviors to escalate into real attacks. Observing cyberattack monitoring data, we believe that traditional attacks must be taken seriously.

According to monitoring data in the first half of 2018, attacks were more frequently seen in January, but experienced a fall in February, and then got a rebound in March before returning to the previous levels in April to June, fluctuating around the average value.

Figure 3-8 Trend of web attacks



Among web vulnerabilities, deserialization vulnerabilities (a way for applications to accept untrusted data) are easily usable and remotely exploitable, and therefore find special favor with hackers who most frequently target Struts 2 frameworks, WebLogic servers, and JBoss servers.

Struts frameworks are preferred targets of attackers. Most vulnerabilities in Struts frameworks are typical deserialization vulnerabilities. Our *2017 Annual Deserialization Vulnerability Report*[7] shows how vendors deal with deserialization vulnerabilities, revealing a vicious cycle of fixing, bypassing, refixing, and re-bypassing. Making the 2017 OWASP Top 10 list, such vulnerabilities are extremely valuable for attackers because they are easy to exploit and a successful exploitation allows attackers to obtain higher privileges. In the first half of 2018, although Struts announced two vulnerabilities (S2-055/S2-056), the most frequently exploited vulnerabilities are ones that have received much attention in the past years:

- **CVE-2017-5638:** In early 2017, this remote code execution vulnerability was reported to exist in the Jakarta Multipart parser plug-in in Apache Struts2. An attacker could exploit this vulnerability to launch a remote attack by setting the filename field in the Content-Disposition header or setting the Content-Length field to a length over 2 GB to trigger an exception and execute the OGNL expression in the filename field.
- **CVE-2014-0094:** This vulnerability exists in the ParametersInterceptor class in Apache Struts 2 2.3.16 and earlier versions. A remote attacker could exploit this vulnerability to manipulate the loader of this class by using the "class" parameter passed to the getClass method. This vulnerability, though discovered years ago, is frequently tried or exploited now by hackers with occasional success.
- **CVE-2017-9805:** On September 5, 2017, Apache Struts released the latest security advisory to reveal that a high-risk vulnerability (CVE-2017-9805 (S2-052)) exists in the REST plug-in in Apache Struts 2.5.x and some versions in the range from 2.x to 2.5.x. The cause of this vulnerability is that the REST plug-

7 http://www.nsfocus.com.cn/content/details_62_2694.html

in uses XStreamHandler to deserialize XStream instances without any kind of filtering, thus allowing arbitrary code execution.

Now there are new active vulnerabilities exposed in websites:

- **CVE-2018-7600:** Drupal released an advisory on a remote execution vulnerability in the Drupal kernel (SA-CORE-2018-002/CVE-2018-7600) on March 28, 2018, and then announced two vulnerabilities, one cross-site scripting vulnerability and one high-risk code execution vulnerability (SA-CORE-2018-004/CVE-2018-7602). During the following months, attacks against Drupal were frequently launched on the Internet. In May, NSFOCUS Threat Intelligence (NTI) made an elaborate analysis[8] of the spreading infection of cryptominers exploiting vulnerabilities in Drupal. We observed that it was only a few hours from vulnerability exposure to effective exploit attacks, which poses a greater challenge for traditional protection and upgrade policies.
- **CVE-2018-1273:** A remote code execution vulnerability (CVE-2018-1273) was exposed in Spring Data Commons in April, which allows an attacker, via a SPEL expression that contains malicious code, to launch a remote code execution attack so as to gain server control privileges.

8 http://blog.nsfocusglobal.com/threats/vulnerability-analysis/drupal-remote-code-execution-vulnerability-analysis/

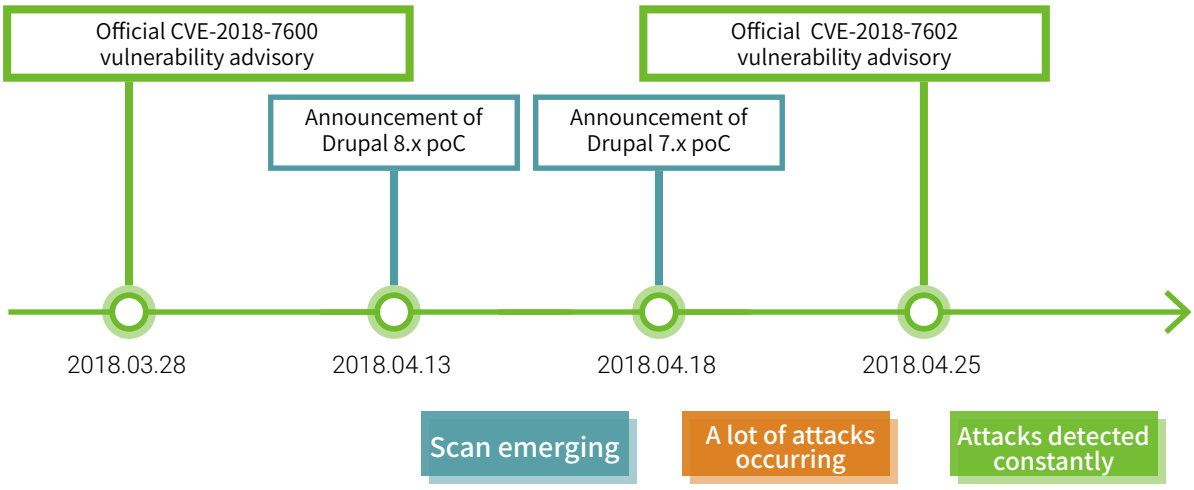
We issued an analysis report[9] for the CVE-2018-7600 vulnerability at the end of March to present the whole timeline from vulnerability announcement to the actual detection of attacks. Since this vulnerability was announced, we have detected at least three types of attacks and exploits (cryptomining, remote control, and WebShell) which spread rapidly. Later, we analyzed several IP addresses with most frequent attack behaviors and discovered that these IP addresses had made a wide range of attack attempts by exploiting other vulnerabilities (such as WebLogic deserialization vulnerability and Struts 2 vulnerabilities) besides the CVE-2018-7600 vulnerability. Therefore, we believe that such IP addresses, instead of targeting specific objects, are implementing numerous valuable vulnerability exploitation methods. They then hunt for targets extensively by using search engines and automatic scanning tools in a bid to gain more website privileges in a broader sphere.

Here is a summary of distinguishing features for recent website-targeting attacks to which attention should be given:

- The time from the announcement of vulnerability details to the emergence of effective attacks has become such a short period that defenders hardly have time to make a response. The analysis of the emergence response for the CVE-2018-7600 vulnerability shows that attacks were performed just hours after this vulnerability is announced.
- Hackers attempt to compromise as many hosts as possible. Shortly after vulnerabilities are announced, hackers complete exploit development rapidly and hunt for vulnerable hosts throughout the Internet. Obviously, each vulnerable website is at risk of compromise. Therefore, administrators should pay significant attention to vulnerabilities in websites and upgrade websites to fix such vulnerabilities as quickly as possible.

A properly configured and deployed web application firewall (WAF) is a key defense against web application attacks. A WAF that is certified to mitigate the OWASP Top 10 will greatly reduce the ability of attackers to exploit vulnerabilities between patch and upgrade cycles.

Figure 3-9 Drupal vulnerability lifecycle



9 http://blog.nsfocusglobal.com/categories/research/drupal-code-execution-vulnerability-analysis/

3.3 DDoS Attacks

Key findings:

- Common SYN attacks, common UDP attacks, NTP reflection attacks, and SSDP reflection attacks are dominant attack forms in the first half of 2018.
- Hackers' capability of launching volumetric attacks keeps growing at a high speed and there is no sign of stopping growing.
- In the first half of 2018, the amount of DDoS traffic seen in the network environments in China is suppressed somewhat due to the government's traffic governance for major events.

Among more than 20 types of DDoS attacks detected by us, four types, i.e., SYN flood attack, UDP flood attack, NTP reflection attack, and SSDP reflection attack, hold dominant positions whether in terms of the attack count or attack traffic.

Figure 3-10 Percentages of DDoS attacks by count and traffic

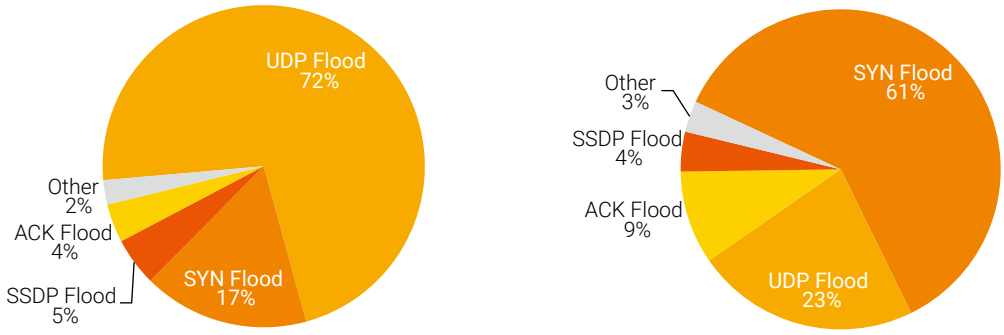
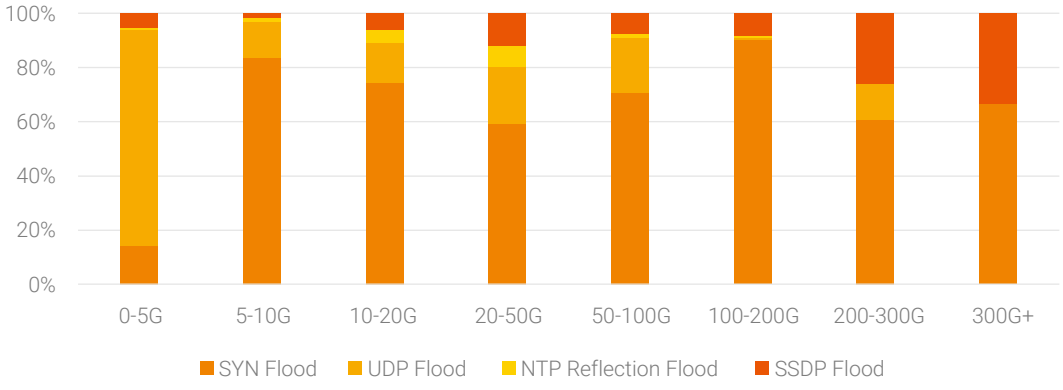
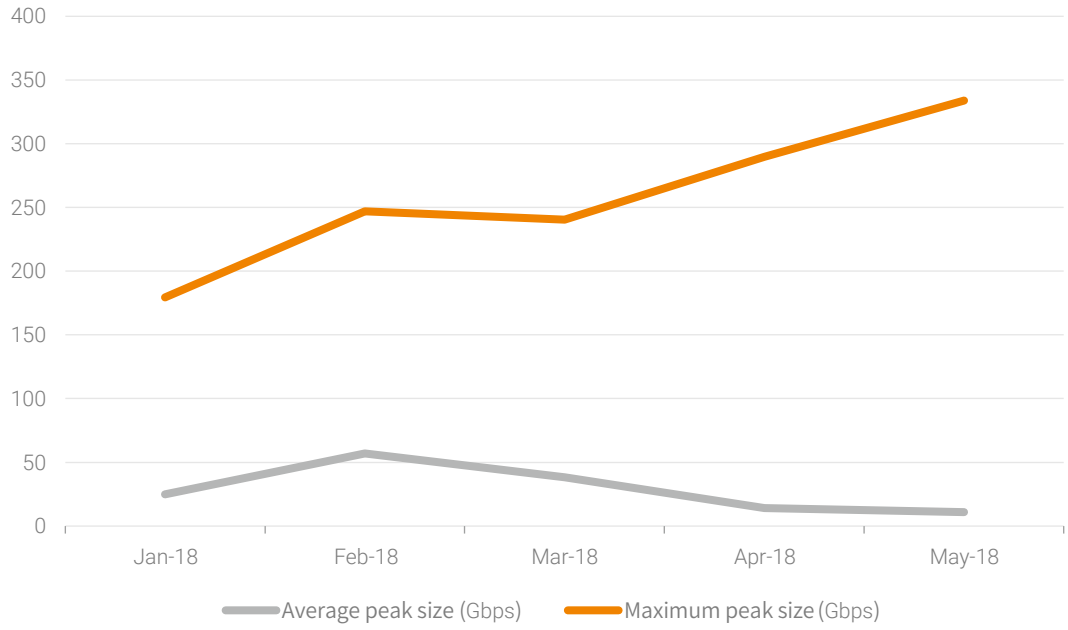


Figure 3-11 Traffic distribution of DDoS attacks



Two different types of attacks dominate in the angle of the attack count and attack traffic. In the former perspective, UDP flood attacks are the major form. In the latter perspective, SYN flood attacks dominate. In terms of traffic, UDP attacks produce small traffic, while SYN attacks usually generate medium-sized and large traffic.

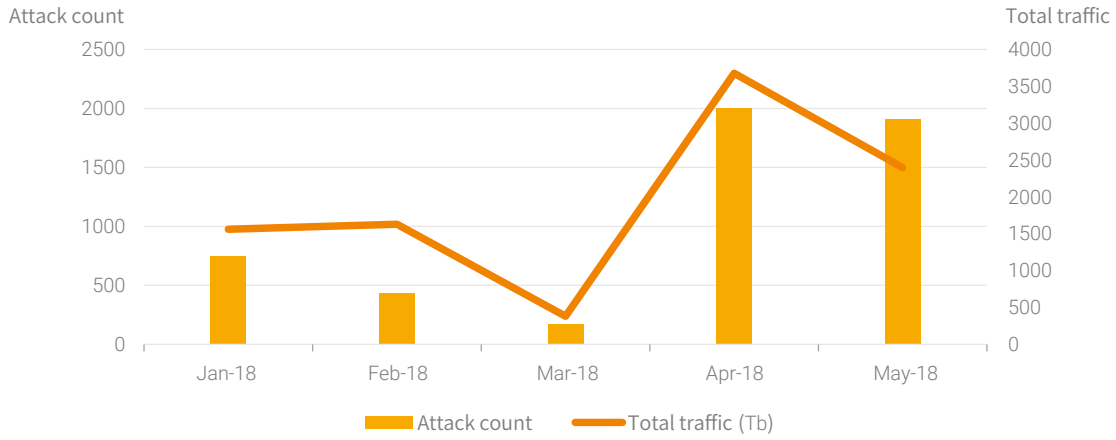
Figure 3-12 Trend of peak sizes



In terms of peak traffic, hackers' attack capability is still on the rise and there is no sign of slowdown in growth. DDoS traffic remains a great scourge on the Internet. Arguably, most hackers are capable of causing gigantic amounts of traffic and their capability is growing rapidly, which is a great challenge to defenders and security governance personnel.

In contrast, the average peak size remains stable around the baseline of about 50 Gbps. Of course, it is difficult for most enterprises providing Internet services to deal with such DDoS traffic size.

Figure 3-13 Monthly trend of DDoS attacks by count and total traffic



The total DDoS traffic and attack count remained stable in the first two months of 2018. Then there was a fall after March, but both surged from April until the end of May. Unlike other threats, DDoS attacks do not undergo a complete overhaul in their working principles. Typically, the offensive side and defensive side fiercely compete on resources and efficiency, instead of scrambling to make radical technical changes. We find that DDoS attack traffic drops sharply when the government exercises security governance during major events both physical and cyber. In particular, the cracking of major DDoS cases can be a very effective deterrent for cybersecurity criminals[10] .

10 https://www.jianshu.com/p/2a47a9116cad

4 Conclusions

Going into H2 2018 we predict the following:

- Malicious IPs will continue to launch multiple attack types. This makes sense as it increases the utility and efficiency of botnets (especially monetized ones).
- "Recidivist" attackers will increase. This also makes sense as the number of infected bots still increase over time. What makes them difficult to identify are dynamic IP address changes. Work needs to be done to better fingerprint devices for identification of malicious devices regardless of their IP address.
- Web attacks, scanners and spammers will be prominent companions to DDoS attacks. These are still the easiest and most popular attack types.
- Government & education, infrastructure and finance will continue to be primary targets. They contain the most coveted data and resources.
- More medium and high level vulnerabilities provide increased attack surfaces. These in turn will give rise to PoC/exploit code becoming available for a good percentage of those vulnerabilities.
- Time between release of vulnerability and available PoC will continue to decrease, especially for recurring or non-eradicated vulnerability types. This could mean that organizations may not be able to patch quickly enough before breach.
- Cryptominers are here to stay. Criminals are always looking for the fast easy money. You cannot get any easier than deploying cryptominers using botnets for hire across the internet.

One would hope the opposite of the above will occur. Unfortunately, vulnerabilities continue to be discovered with each passing day and the need to exploit those found for gain will always be present. Attackers prefer to reuse tactics and exploits so patching regularly is key.

However, regular patching of applications and systems are not enough to combat attackers due to practical considerations such as the time and resources needed to patch large numbers of systems. Proactive security monitoring to identify indicators of attack and compromise as they arise as well as deploying technologies like WAF to protect against application attacks between patch cycles are key to defending against attacks between patch cycles.

NSFOCUS

Over years, NSFOCUS has been committed to defense researches in the cybersecurity realm, providing most competitive security products and solutions for governments, carriers, and financial, energy, Internet, education, and medical sectors, ensuring customers' business continuity. To these customers, NSFOCUS lives up to the reputation of a trustworthy expert.

www.nsfocusglobal.com