NSFOCUS Threat Intelligence

2017 Annual Cybersecurity Insights

NSFOCUS

NSFOCUS

About NSFOCUS

Founded in April 2000, NSFOCUS Information Technology Co., Ltd. (NSFOCUS) is headquartered in Beijing. With more than 40 branches and subsidiaries at home and abroad, the company provides most competitive security products and solutions for governments, carriers, and financial, energy, Internet, education, and medical sectors, ensuring customers' business continuity.

Based on years of research in security protection, NSFOCUS has set foot in intrusion detection and prevention, security assessment, security platform, remote security O&M service, and security SaaS service areas. The company provides the intrusion detection/prevention system, anti-DDoS system, remote security assessment system, and web security protection products as well as professional security operations services for customers.

NSFOCUS Information Technology Co., Ltd. started trading its shares at China's Nasdaq-style market, ChiNext, in Shenzhen on January 29, 2014, with the name of NSFOCUS and code of 300369.

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.

2017 Annual Cybersecurity Insights

NSFOCUS

Contents

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

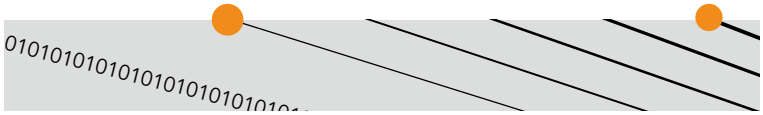
Richard ZHAO

PhD,CISSP
Chief Technology Officer
NSFOCUS

Sun Tzu, an ancient Chinese military general and strategist, said in his famous book "*The Art of War*", that "knowing yourself, and knowing the enemy, and you will never loss a battle". This principle holds true in the cyber-war too. However, as another Chinese old proverb says, "it is easier said than done". Nowadays, tons of open-source software and a wide variety of Application Programming Interfaces (APTs) exist in the information systems, making the supply chain longer and longer. In addition, a variety of micro services go live every day. In such a dynamic environment, it is a big challenge to have a clear picture of assets in your network as well as their values, security properties, logical distribution, and dependencies. While knowing yourself is already very difficult, knowing the enemy is even harder: Who are them? What are their purposes and motives? Are their attacks targeted or non-targeted? How good are the techniques used, advanced or average? What are the current tends? Which vulnerabilities and exploits are popular? What kinds of threats are behind millions of security alerts?

In theory, threat intelligence, as its name and definition suggests, is supposed to provide the way to know the ememies. Today, dozens or even hundreds of threat intelligence sources are out there, including both open-source and commercial ones. However, in reality, sometimes, it provides too much info, as tens of millions pieces of threat intelligence overwhelm the security operations as they require considerable resources to analyze and use. Yet at other times, when large or specific security events happen, it fails to provide relevant and actionable information.

After several years of practices, the security industry begins to realize that in order for it to realize its full value, threat intelligence must be put through the continuous cycle of extracting-consumption-analysis to make it more and more precise. In this cycle, the analysis phase is most crucial, as it produces new intelligence to be extracted and added to the new consumption phase. This way, the users and vendors of threat intelligence form a cyber protection ecosystem, which delivers the latest threat trend and information to all of its



members. Such a system will provide a sustainable and realistic means to know enemies.

If the Dyn attack in 2016 serves as a wake-up call about Internet of Things (IoT) threats, IoT devices have become frequent participants of cyber attacks in 2017. According to data collected by NSFOCUS Threat Intelligence (NTI), IP addresses of IoT devices used for attacks account for 12% of all malicious IP addresses. About 4.8% of all IoT devices are malicious, triple the percentage of other malicious IP addresses. Therefore, it won't be a surprise to see that as security threats from IoT devices continuously increase, the IoT threat protection capability will become an indispensable part of a security protection system.

Of more than 3.9 million attack sources we observed in 2017, about 20% are malicious IP addresses which attacked multiple targets. 0.39% of attack sources are responsible for 90% attack events. Tracking, analysis, profiling, and fighting against these repeated offenders will be the most efficient and effective way to improve the security protection solution. Likewise, covering these repeated offenders will be one of the most essential capabilities of the threat intelligence.

As indicated in our 2017 Midyear Cybersecurity Insights, we find a clear correlation between the proportion of malicious IP addresses in a country and the overall economic development level of that country. More specifically, in less developed areas, computers are more likely to become attacker-controlled hosts to attack other systems due to poor Internet security governance and less sufficient security protection which fails to keep up with the popularization speed of computers. For example, the proportion of malicious IP addresses reaches as high as 17% in Vietnam and 11% in India. Such fundamental threat statistics can serve as an important reference for User and Entity Behavior (UEBA) and other security behavior analysis when building a more intelligent security monitoring system. Meanwhile, we should be aware that as profit-driven security threats are increasingly globalized, we should take advantage of threat intelligence to achieve threat monitoring, analysis, and response from the global perspective.

In 2017, we have detected a total of 640,000 TB DoS traffic volume, an increase of 79.4% from 2016. The average peak size is 14.1 Gbps in 2017, up 39.1% over 2016. In 2017, the largest DDoS attack occurred in May, with the peak size hitting 1.4 Tbps, while it was 730 Gbps in 2016.

Reflective amplification attacks are still the dominant type in the DoS attacks. It is worthwhile to note that new deadly weapons are added to the arsenal of reflective attacks. Several days ago, GitHub, a renowned code hosting website, was hit by a DoS attack with peak traffic of 1.3 Tbps. This attack was based on the reflective DoS vulnerability contained in Memcached. According to data collected by NSFOCUS NTI, more than 100,000 Memcached servers are available on the Internet around the world. Owing to their high bandwidth and long online duration, Memcached servers are likely to be new destructive weapons of reflective DDoS attacks.

In this report, we will share some insights we have seen in 2017, hoping to help you to know a little bit more about threats we all face, and the enemies we are fighting against.

1. Geographical Distribution of Attacks

1.1 Geographical Distribution of Attack Sources

From the perspective of the absolute quantity of attack sources, China, USA, India, and certain areas in Middle East have the most attack sources.

Figure 1.1 Geographical distribution of attack sources

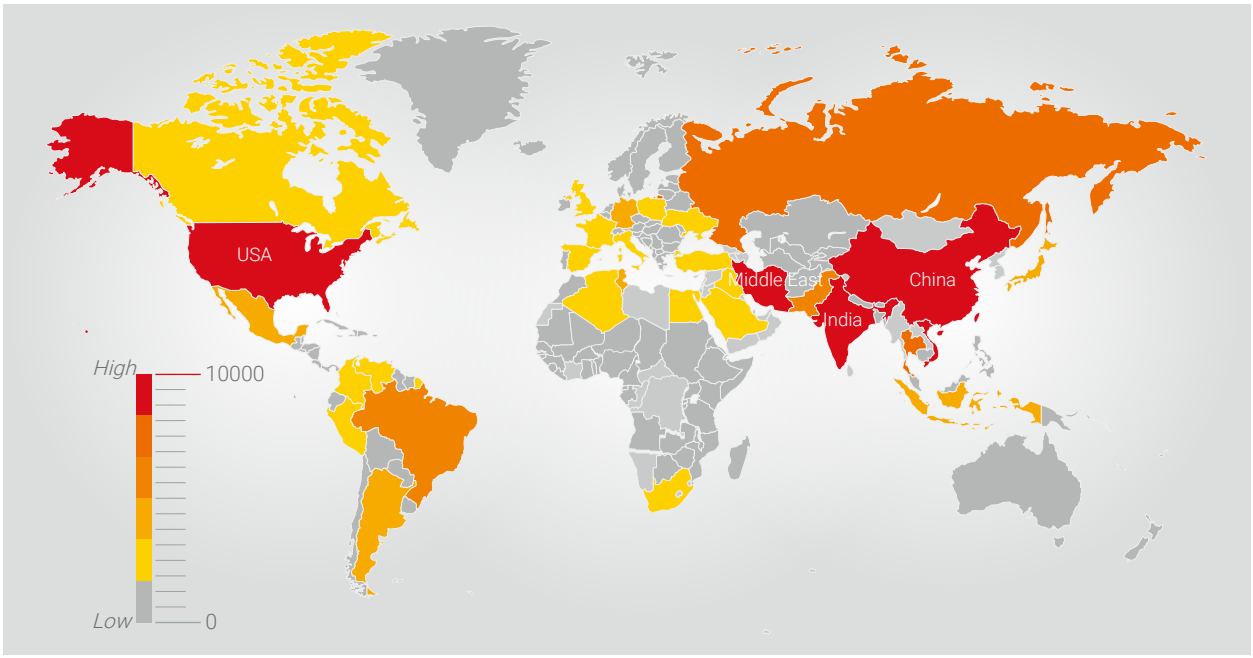
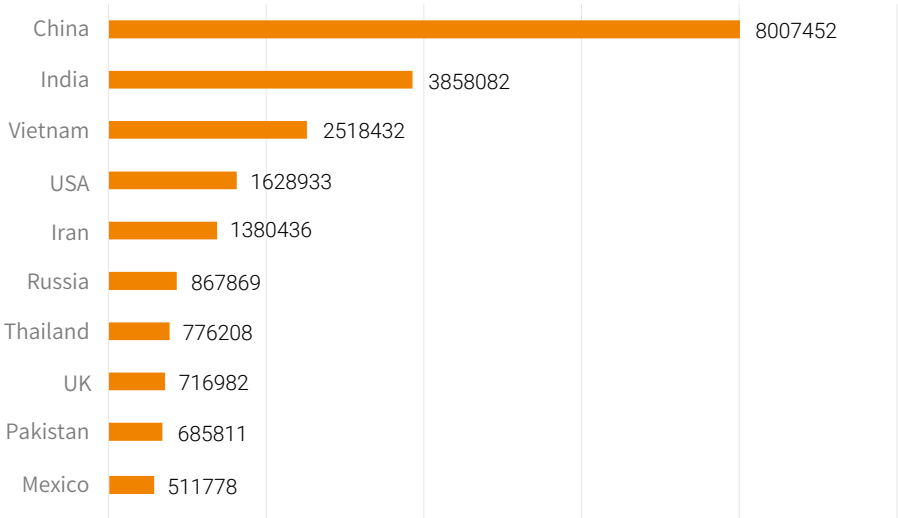
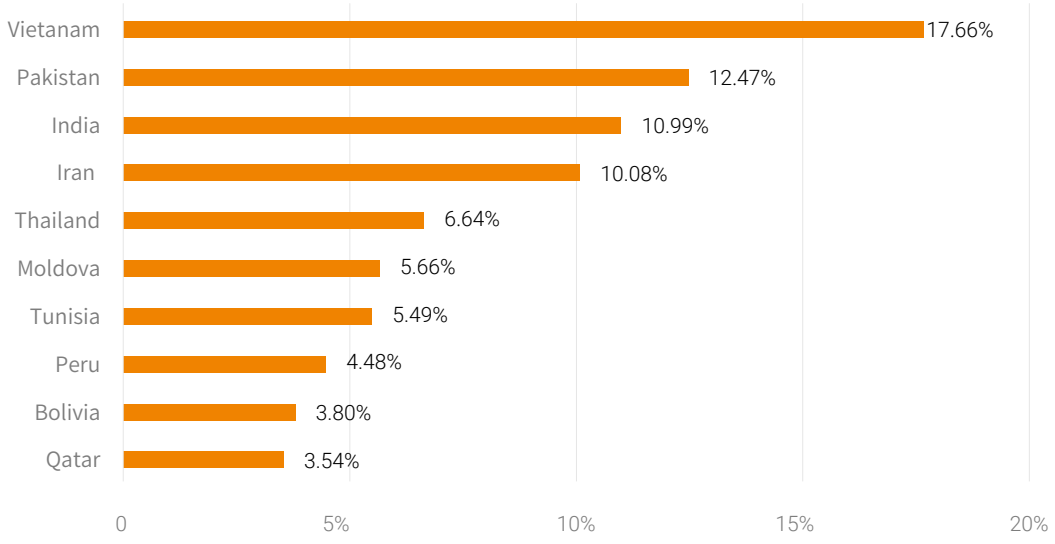


Figure 1.2 Top 10 countries by attack source count



In addition, we have calculated proportions of malicious IP addresses in different areas by collecting statistics of ASNs by geographical locations from ASN administration authorities. We find that economically underdeveloped countries or areas have a higher percentage of attack IP addresses due to relatively weak security governance, with Vietnam having the largest proportion of up to 17%. It is important to note that such a high proportion means that attacks are launched most frequently from these areas, rather than hacking groups residing there. As hackers can use all highly vulnerable devices on the Internet as attack tools without geographical limitations, it is the negligence of security governance that turn such areas to major attack sources.

Figure 1.3 Top 10 countries with most malicious IP addresses



The following table shows top 10 ASNs with the most attack sources.

Figure 1.4 Top 10 ASNs with most malicious IP addresses

ASN	Country	ASN Administration Authority	Number of Malicious IPs
AS4134	China	CHINANET-BACKBONE	2688819
AS9808	China	China Mobile Communications Corporation	1658532
AS9829	India	National Internet Backbone	1495907
AS45899	Vietnam	VNPT Corp	1478966
AS4837	China	CHINA UNICOM China169 Backbone	1302938
AS24560	India	Bharti Airtel Ltd., Telemedia Services	733811
AS45595	Pakistan	Pakistan Telecom Company Limited	633042
AS7552	Vietnam	Vietel Corporation	591468
AS56046	China	China Mobile Communications Corporation	586240
AS12880	Iran	Information Technology Company (ITC)	437364

We suggest that enterprises, based on business characteristics, filter and restrict IP addresses accessing their networks by ASN and area. Doing so will significantly reduce unnecessary attack risks, especially for high-risk areas and ASN segments.

1.2 Geographical Distribution of Victims

From the perspective of geographical distribution of attacks, the USA, China, Britain, Germany, and Japan suffered the most attacks. This demonstrates that the number of attacks against a region is positively correlated to the development level of this region. This is because the value of information assets in a region is closely associated with the development and informatization level of this region. China, USA, and European countries have a large number of high-value information assets thus surely become the most seriously hit regions.

Figure 1.5 Geographical distribution of victims

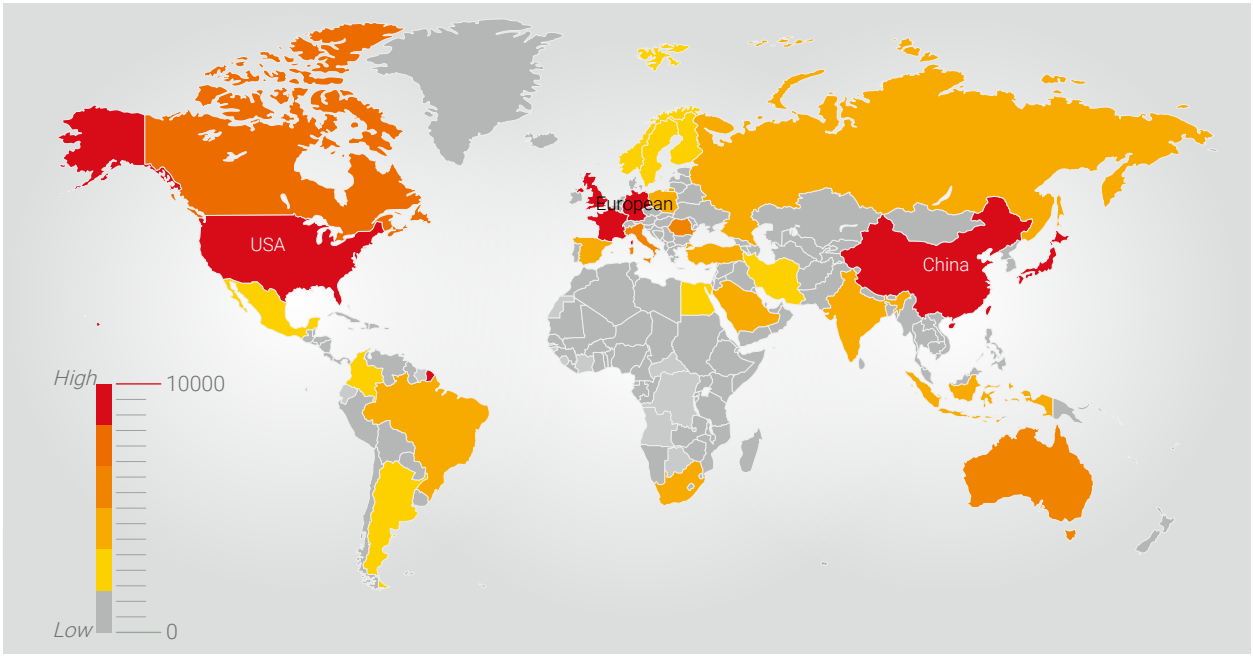
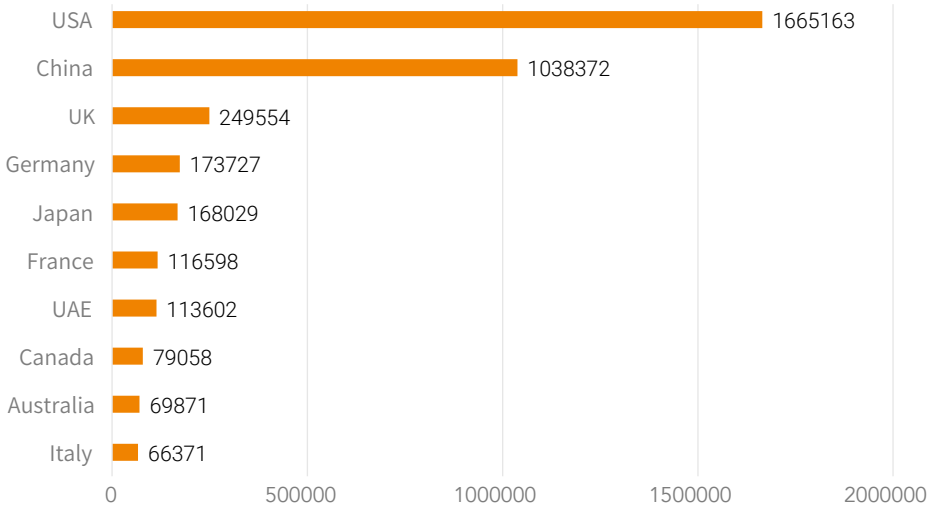


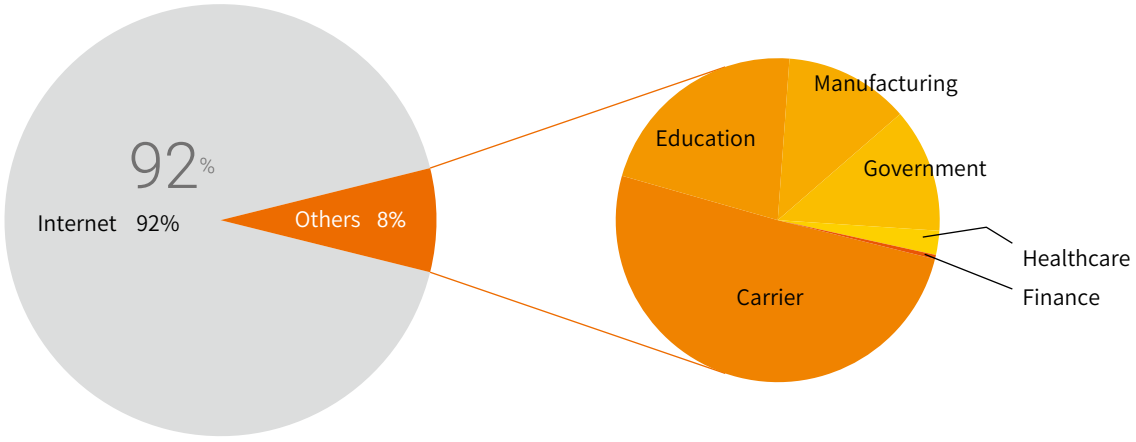
Figure 1.6 Top 10 countries with most victim IP addresses



2. Attacks Against Different Industries

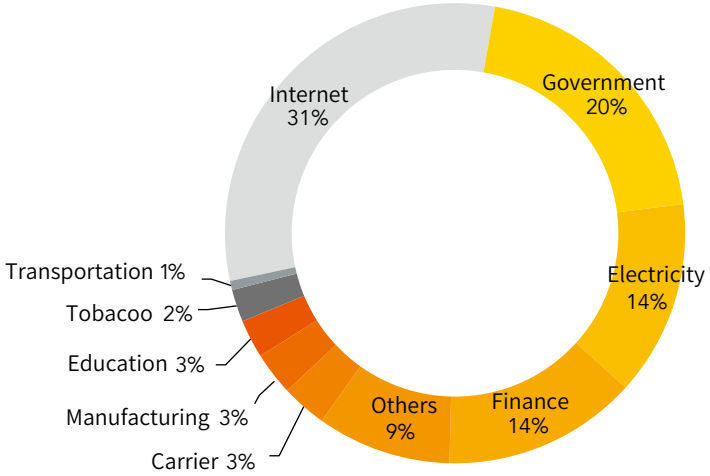
As each industry has its own business characteristics, hackers target different industries with various attack methods. Internet enterprises have complex business environments where a great deal of business is served via a web UI and complex IT architectures need to be built to provide technical support. In view of this, the Internet industry is particularly vulnerable to web attacks and system-based attacks, therefore requires a more powerful protection solution. Special attention should also be paid to the protection against web attacks for other industries, including carriers, education, manufacturing, and government.

Figure 2.1 Web attack distribution by industry



As for system-based attacks, the Internet industry is still the top target, followed by government, electricity, and financial sectors. Systems used in these sectors are often highly sensitive in nature, and therefore are consistently favored targets of hackers. Governments and the financial sector are most severely attacked by ransomware, botnets, and worm viruses. By extensively spreading malicious code through exploitation of vulnerabilities (such as improper configurations, weak passwords, and system vulnerabilities) in systems, hackers intended to cause a negative social impact and gain economic benefits.

Figure 2.2 System attack distribution by industry



Unlike web attacks, system-based attacks are more targeted and thus more efficient. Besides, complex attacks such as those from APT groups, ransomware attacks, and social engineering attacks are often seen in industries shown in the preceding chart, causing customer information leaks and monetary loss. For example, the APT-C1 organization detected by NSFOCUS this year was found to steal cryptocurrencies from customers, incurring a direct economic loss of up to $1.5 million.

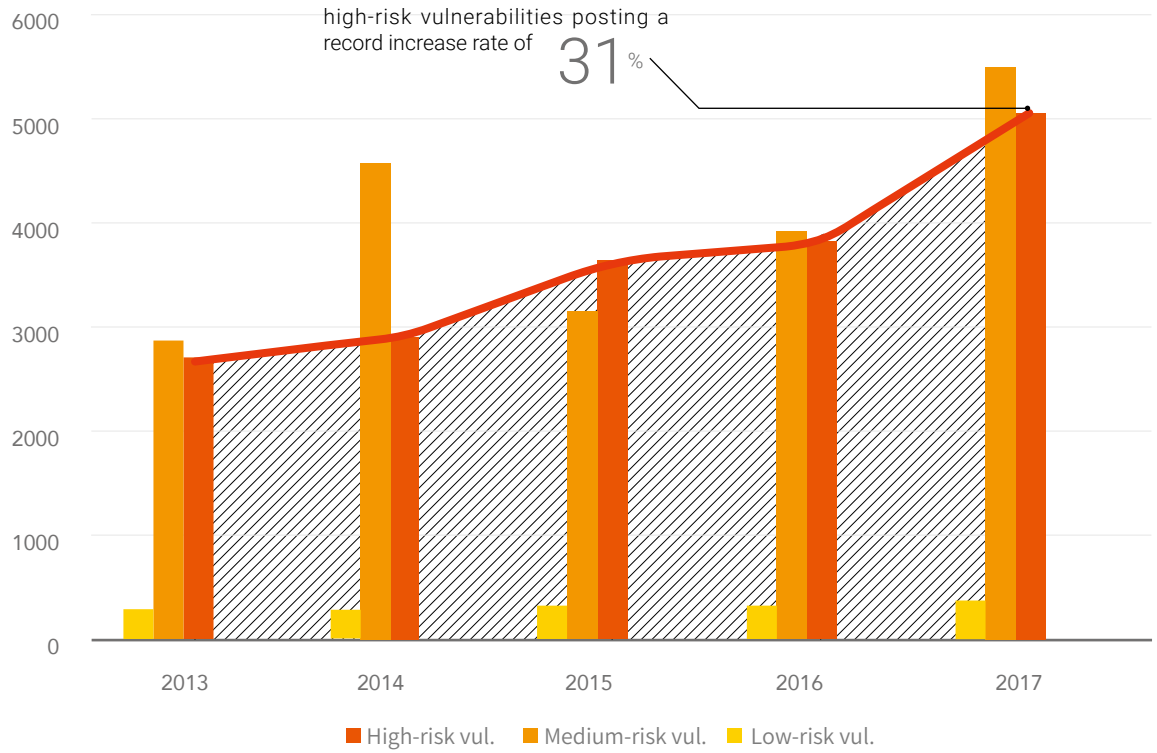
3. Changes to the Security Trend

3.1 Vulnerability Trend

3.1.1 Overall Trend

In 2017, the total number of vulnerabilities went up 28% compared with 2016, with high-risk vulnerabilities posting a record increase rate of 31%.

Figure 3.1 2013–2017 vulnerability quantity



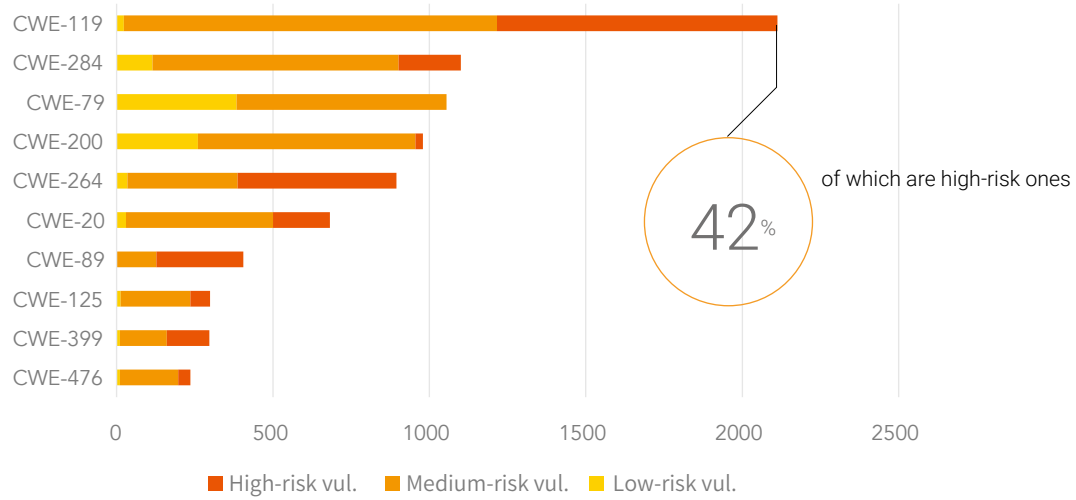
Top 10 vulnerability types by exposure count in 2017 are as follows:

- Buffer overflow (CWE-119)
- Improper access control (CWE-284)
- Cross-site scripting (CWE-79)
- Information leak (CWE-200)
- Privilege access control (CWE-264)
- Improper input validation (CWE-20)
- SQL injection (CWE-89); Out-of-bounds read (CWE-125)

- Resource management errors (CWE-399)
- NULL pointer deference (CWE-476).

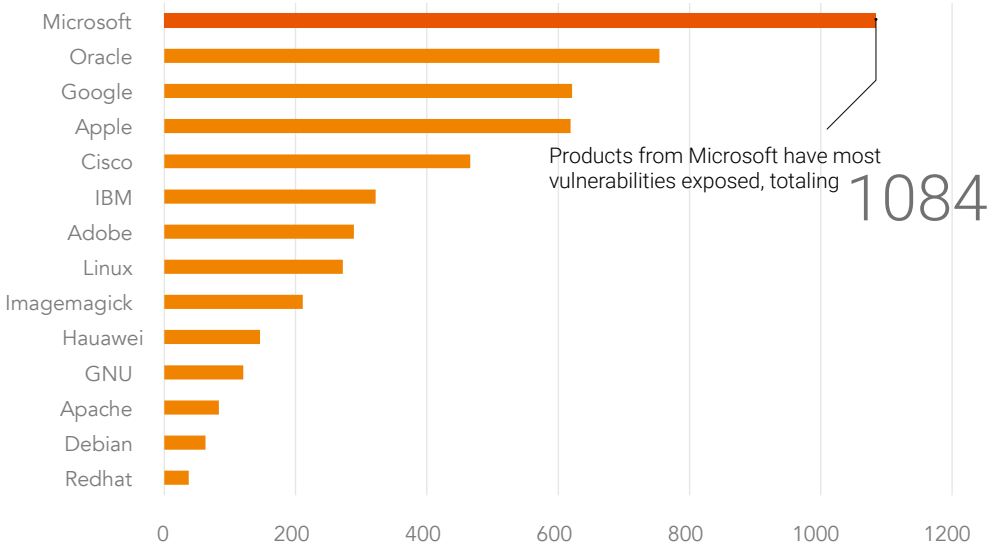
Of all preceding vulnerabilities, buffer overflow vulnerabilities account for the largest share, hitting 2112, 42% of which are high-risk ones.

Figure 3.2 2017 top 10 vulnerability types by exposure count



The following figure shows vendors with most vulnerabilities exposed. Products from Microsoft have most vulnerabilities exposed, totaling 1084.

Figure 3.3 2017 top vendors by vulnerability count

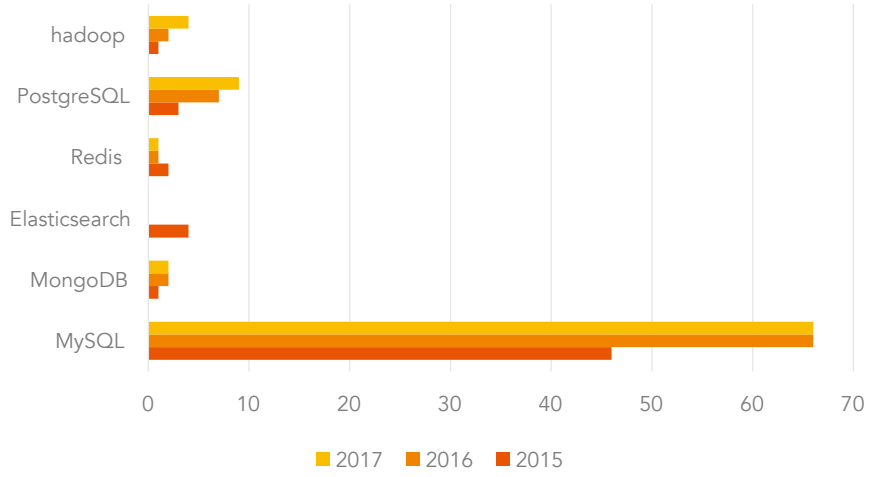


3.1.2 Topical Vulnerabilities

3.1.2.1 Database Vulnerabilities Attracting Attention

As indicated *in* *NFOCUS's 2017H1 Cybersecurity Insights*, a number of notorious database ransomware events occurred from January to February in 2017. Many databases have read-only interfaces directly exposed to the Internet and do not have complete access control policies. Anyone can take control of such a database with a weak or empty password. A database ransom attack is implemented by taking control of a database to further encrypt or damage data for the purpose of demanding ransoms from victims. Database security became a hot security issue in 2017. The following figure shows statistics of high- and medium-risk vulnerabilities in the databases attacked in 2015, 2016, and 2017.

Figure 3.4 Distribution of database vulnerabilities used for ransomware attacks



As shown in the above figure, MySQL has the most vulnerabilities exposed over the past three years and PostgreSQL has also registered a rapid increase in vulnerabilities. In contrast, MongoDB, Elasticsearch, Redis, and Hadoop are more secure, despite a moderate increase in vulnerabilities. From the database vulnerability trend, security issues of databases will definitely attract more attention from attackers. Furthermore, vulnerability exploits based database hijackings will probably emerge in the near future.

3.1.2.2 Ransomware Propagation via Vulnerability Exploitation

In 2017, ransomware is definitely a security issue that is worthy of special attention as ransomware families, including Wannacry, EternalRocks, Petya, GodenEye (NotPetya), and BadRabbit, spread wildly, causing an adverse impact and incurring a great loss of data and money t o enterprises and individuals.

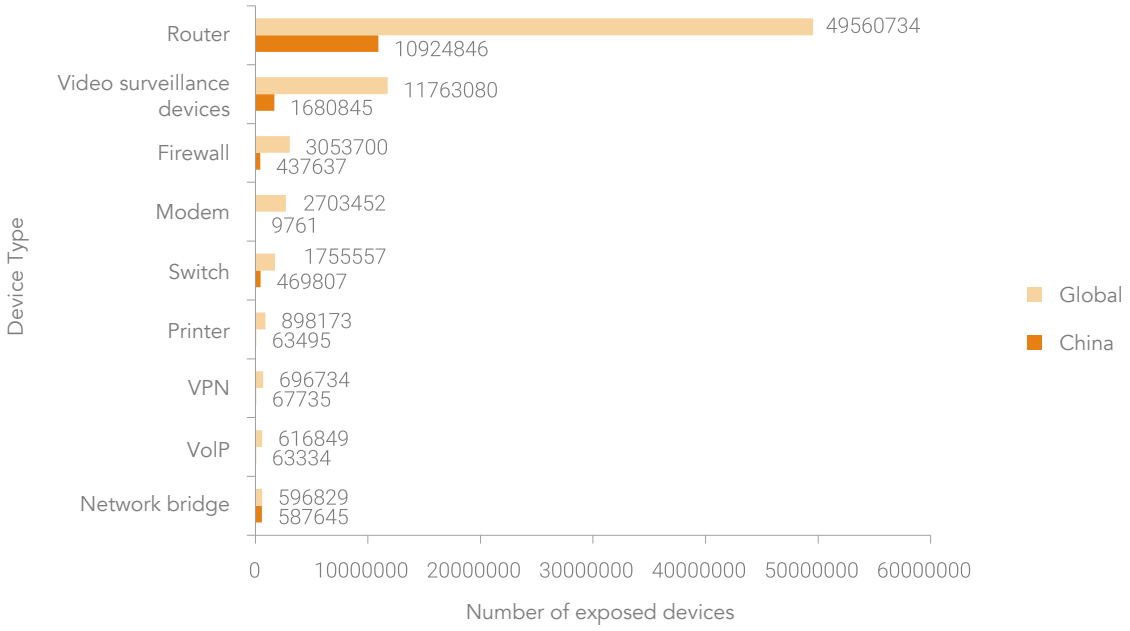
Figure 3.5 Major ransomware events in 2017

These well-known ransomware events have one thing in common: They propagate by exploiting defects in the Windows SMB service such as CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0147 which are listed in Microsoft Security Bulletin MS17-010.

3.1.2.3 Exposure of a Large Number of Vulnerabilities in IoT Devices

The Persirai botnet attracted great attention as it targeted 120,000 IP cameras by exploiting on April 26, 2017. Since then, securing IoT devices, typically web cameras and home wireless routers, had become a security focus in 2017. Globally, more than 49 million routers are exposed, which is far higher than the number of other exposed IoT devices. Over 11 million video surveillance devices are exposed, ranking second only to routers and much more than traditional network devices such as firewalls and switches. Surprisingly, more than 890,000 printers are exposed.

Figure 3.6 Exposure of IoT devices globally and in China



Cameras, routers, and wireless devices are top 3 types of IoT devices in numbers. These devices are widely distributed, but often have serious vulnerabilities due to weak security protection. We collect statistics on exposed vulnerabilities in such devices and find that the recent three years have seen a rapid increase in vulnerabilities discovered in routers, wireless devices, and video surveillance devices. As many defects exist in updates and protection mechanisms of IoT devices, we have the reason to believe that these vulnerabilities will exist for a long time. For example, we mentioned in the later part that Gafgyt took advantage a Netcore vulnerability exposed in 2014 for large-scale spread in 2017 and was frequently used to carry out malicious activities.

Figure 3.7 Trend of vulnerabilities in commonly used routers and wireless access devices in recent three years

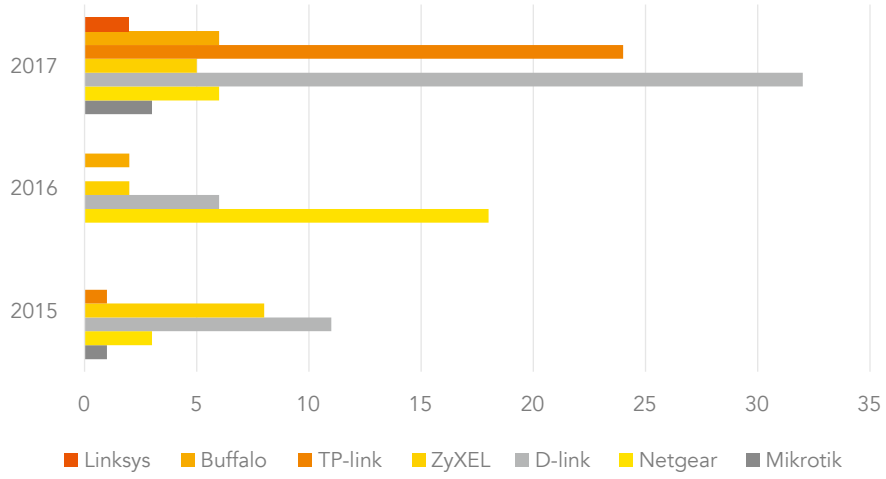
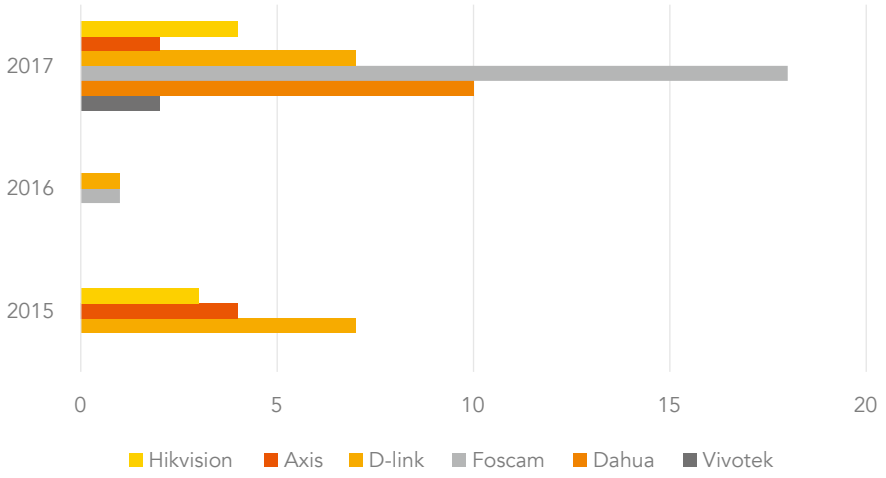


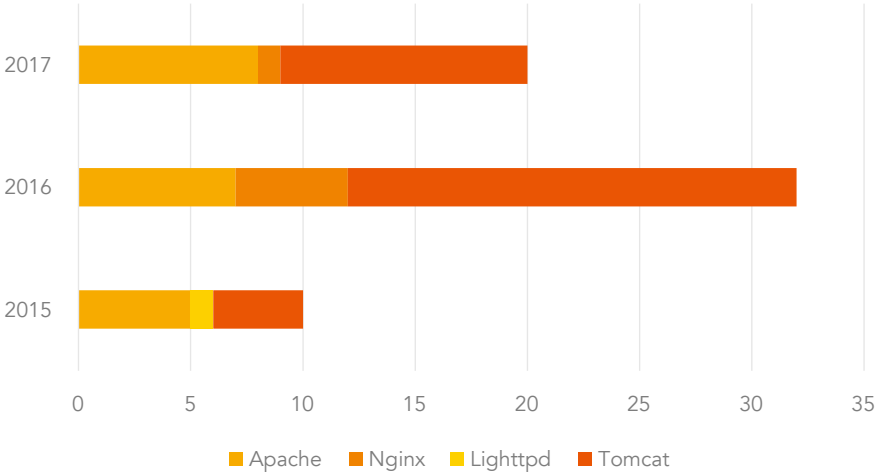
Figure 3.8 Trend of vulnerabilities of major camera vendors from 2015 to 2017



3.1.2.4 Extensive Use of Deserialization Vulnerabilities

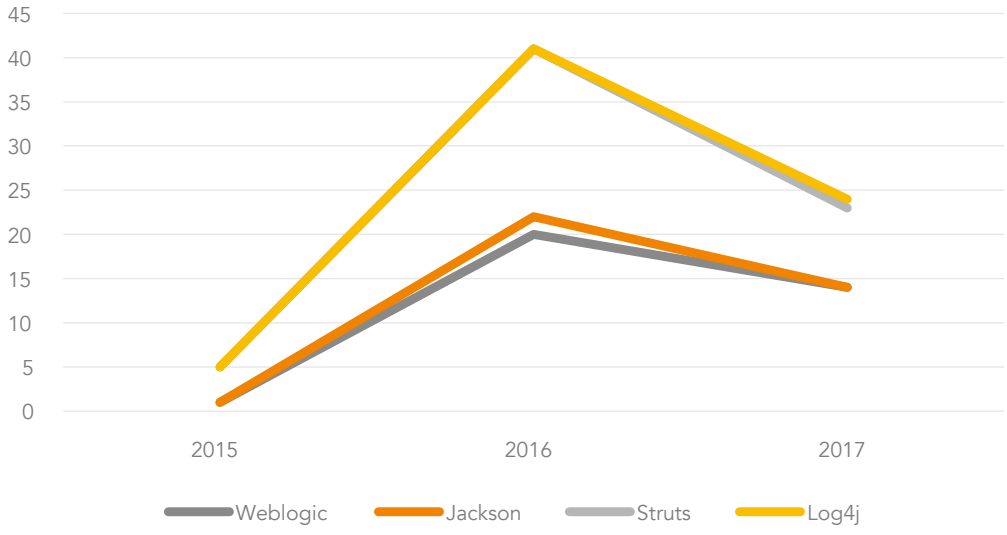
While compared with 2016, there is a moderate decrease in vulnerabilities in traditional web services due to a sharp drop in vulnerabilities in Tomcat and Nginx. The number of Apache vulnerabilities remains steady in the recent three years, despite a slight increase.

Figure 3.9 Trend of vulnerabilities in popular web servers from 2015 to 2017



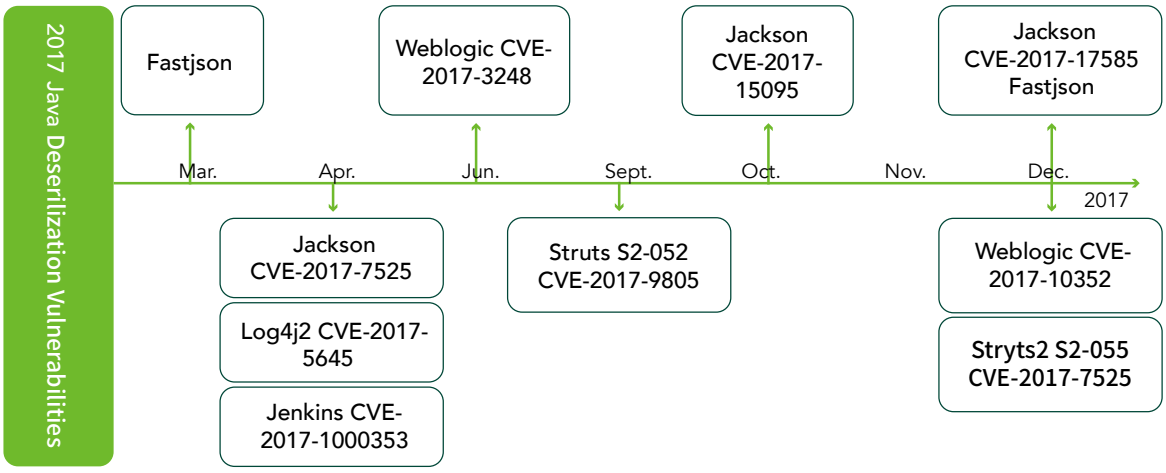
We notice that deserialization vulnerabilities see the fastest growth in attacks against web services. This kind of vulnerability began to rise substantially from 2016 and has become a preferred means of web attacks. Among top 10 web vulnerabilities revealed by OWASP in 2017, deserialization vulnerabilities ranked eighth. As far as we discover, major web programs such as WebLogic, Jackson, Struts, and Log4j contain deserialization vulnerabilities.

Figure 3.10 Deserialization vulnerability trend of common applications from 2015 to 2017



Serialization is a process of encoding data objects (for example, instantiated objects of Java, XML, and high-level programming languages) usually to facilitate communications. However, deserialization is a process of decoding the data encoded during serialization. As Java's serialization mechanism supports both serialization and deserialization of Java objects, hackers can execute many complicated commands by using Java's deserialization mechanism, inflicting great damage. This, together with its widespread application, makes Java deserialization vulnerabilities eye-catching. In 2017, NSFOCUS continued to keep a close eye on the trend of Java deserialization vulnerabilities and found that 10 of these vulnerabilities caught considerable attention of the security industry.

Figure 3.11 Deserialization vulnerabilities in web components in 2017



The main reason why deserialization vulnerabilities never cease is that vendors fail to completely fix vulnerabilities. Once a vulnerability is discovered, vendors, focusing on providing flexible and diverse functions, merely add blacklist entries concerning the vulnerable class that is invoked. Such a perfunctory effort results in the filtering mechanism being frequently bypassed. Therefore, with one vulnerability exposed, there will often come more afterwards. In this regard, we suggest that vendors take vulnerability remediation seriously by identifying the vulnerability's root cause and introducing an appropriate mechanism to prevent recurrence of similar vulnerabilities.

3.2 Attack Situation

This chapter provides a retrospective analysis of the attack situation in 2017 from perspectives of attackers, groups, sample families, and attack types. From the perspective of attackers, we find five quite active attack groups. An analysis of attack sources reveals that a large proportion of IP addresses originated attacks on multiple targets and no more than 0.5% of IP addresses were responsible for various cyberattacks. Based on our statistics on attacks in 2017, we analyze the key trends and characteristics of various attacks, namely, web attacks, DDoS attacks, and system attacks. A clear understanding about the critical security situation in 2017 can facilitate your deployment of defenses for business security and creation of a sound defense system according to the unique characteristics of your own business.

3.2.1 Active Attackers

3.2.1.1 Five Groups Active in Campaigns

We keep close tabs on more than 200 active individual attackers, attack groups, and sample families. We conduct ongoing monitoring on known indicators of compromise (IoCs) of these groups and have found that quite a few groups and sample families, including the backdoor KeyBoy, Hidden Cobra, and Carbanak, are involved in rampant malicious activities. Besides, a series of events that exploited WebLogic backdoors to plant miner viruses as well as a host of black hat search engine optimization (SEO) events also drew our attention. Of course, we also noticed reports about attacks conducted in May by hackers who disguised themselves as group APT28. Organizations like the notorious APT128 have had their attack facilities exposed, making it possible for other attackers to impersonate them.

- **WebLogic backdoors exploited to plant miner viruses**

In December 2017, NSFOCUS's emergency response team released the Security Alert Advisory on WebLogic Hosts' Infection of Miner Viruses after discovering a malicious program planted in a number of hosts running different versions of WebLogic upon receipt of reports from customers of the financial, telecom, and Internet service sectors. This malicious program was found to consume large quantities of CPU resources on hosts. We followed up with this event and tracked the spread of this backdoor program based on historical log data.

- **KeyBoy**

KeyBoy is a backdoor program that is usually delivered via vulnerabilities in the Office program. Generally, a hacker crafts a malicious Word document and then executes malicious code on target hosts by exploiting backdoors in several versions of Office (CVE-2012-0158, CVE-2015-1641, and MS12-060) before remotely downloading and installing the KeyBoy backdoor. This program was first reported by Rapid7 in June 2013 and then media reports in November 2016 disclosed activities of KeyBoy variants. According to related analysis, KeyBoy is used for planned and organized advanced persistent threat (APT) attacks. It can steal browser certificates to hide its true identity for keystroke logging and installation of interactive shells. Our ongoing monitoring of this backdoor finds that its activity intensified in June 2017, so much so that an obvious peak was formed.

- **Black Hat SEO**

In December 2017, NSFOCUS's emergency response team reported black hat SEO. This type of SEO leverages the resolution of second-level domains of high-value websites for website promotion. In the events covered by NSFOCUS, more than 50 domain names were affected and, moreover, IP addresses corresponding to these promoted domain names pointed to the same destination. According to our statistics based on continuous tracking of visits owing to black hat SEO and an overall analysis of the related data throughout 2017, this type of network traffic peaked in November and December.

- **Hidden Cobra**

Since 2009, Hidden Cobra has attacked a wide range of targets by means of data theft or direct compromise of IT systems. It has different names in reports from different research institutes, including Lazarus Group and

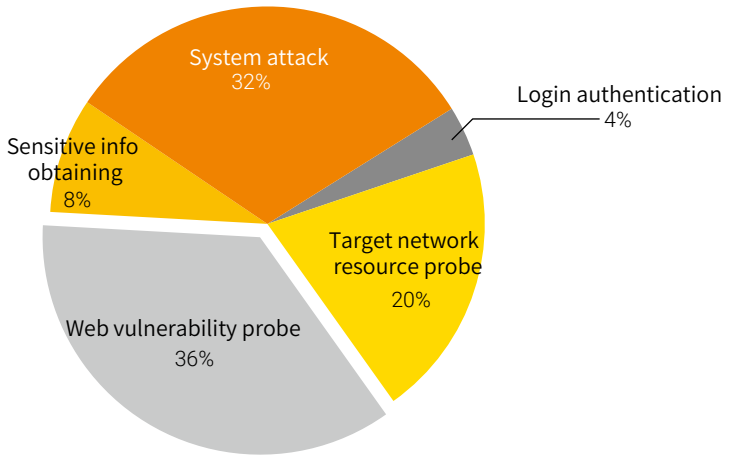
Guardians of Peace. This group has sophisticated attack capabilities and is capable of launching DDoS attacks with botnets. In addition, powered by complex, systematic attack tools and capabilities of exploiting critical CVE vulnerabilities for intrusion, it can gain control access to hosts, log keystrokes, and compromise computer system data. Security vendors, including Symantec, Fireeye, X-Force, AlienVault, and Novetta, have tracked and analyzed this group, disclosing a host of malicious samples used and attacks conducted by this group. The best-known activity attributable to Hidden Cobra was an APT attack on Sony Pictures in 2014. In the wake of this event, Novetta organized Operation Blockbuster to track and investigate this malicious actor. In 2017, US-CERT released a series of alert advisories on campaigns by this group and disclosed related technical details, including DDoS facilities and backdoor trojans it used.

- **Carbanak**

Carbanak is a backdoor program discovered and named by Kaspersky Lab in February 2015. With financial organizations as the main target, this program exploits vulnerabilities in Office programs to steal sensitive information from target hosts and then manipulates these hosts to conduct illegal transfers. It has caused an accumulated loss of $100 million, affecting more than 100 institutions.

Having a close look at their behavior patterns, we find that such groups, in active phase, initiate numerous scans and probes. Scans are performed to discover common vulnerabilities in systems. For this purpose, hackers try to find out open ports on the target network and the services running on these ports before initiating tentative attacks on different services. Such tests are often geared to web attacks (SQL injection, cross-site attacks, path traversal, and exploitation of vulnerabilities in frequently used plug-ins), system attacks (login authentication and password cracking for access to sensitive services), and attacks exploiting high-risk vulnerabilities in other common services. In fact, more often than not, administrators in organizations neglect such behaviors because this type of probe is not unusual in day-to-day operations. However, such procedural actions are valuably informative for APT groups to proceed with subsequent attacks. Therefore, it is advisable to identify such malicious IP addresses from threat intelligence so as to extract key alerts involving specific groups and sample families that deserve administrators' special attention.

Figure 3.12 APT groups' tentative actions on vulnerabilities in Internet assets

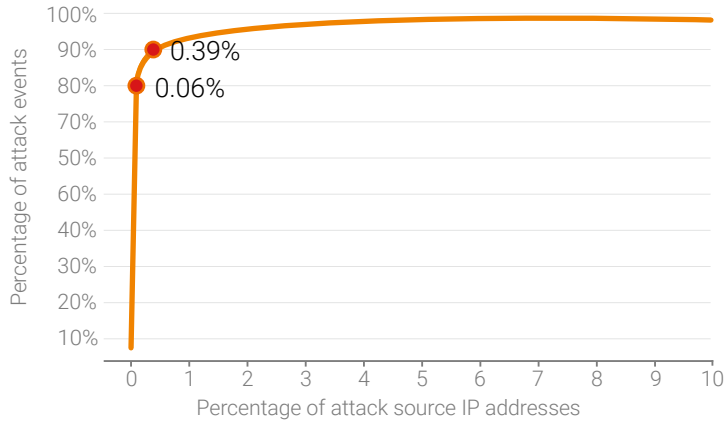


According to our observation, it is an undeniable fact that organizations are lacking in long-term systematic O&M management. For example, in an asset scan for the financial sector in October 2017, we found that, among all hosts under scanning, at least 6% were improperly configured. Some hosts were in idle state after fulfilling development and commissioning tasks but stayed online with default settings and network services available without any access control. Some exposed ports for highly sensitive services, such as remote-control services of SSH, Telnet, RDP, and VNC, to the Internet, and even worse, used weak login passwords. The remaining ones made critical data assets, including the Mongo server, Elasticsearch server, and MySQL server, publicly available without any control. All these security loopholes are like time bombs that may detonate anytime. To protect against such attacks, technology is critical, however management methodology and security awareness is also important on the other hand.

3.2.1.2 About 20% of IP Addresses Attacking More Than One Target, and 0.39% of Attack Sources Responsible for 90% of Attack Events

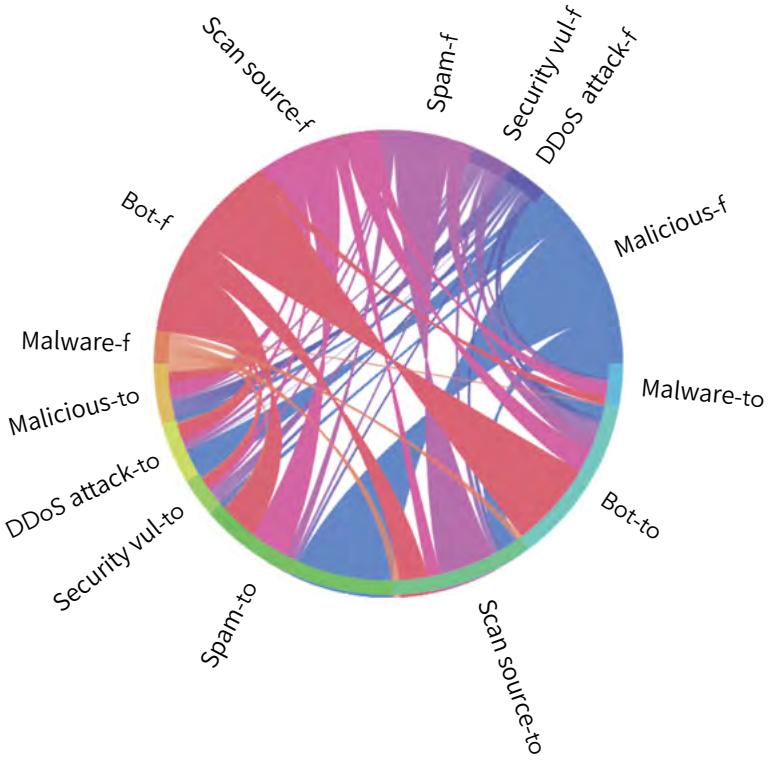
In 2017, over 3.9 million attack sources were detected during our ongoing monitoring, of which 20,511 were involved in various attacks, such as DDoS attacks, spread of botnets/trojans/worms, malicious scans, and exploitation of vulnerabilities in websites and other network services. We found that these IP addresses were "recidivists" and "rogues" in network environments as they were active in taking turns to launch different attacks against different targets. Despite the fact that they may not belong to any hacking group, these IP addresses are more possible to be controlled by hackers and become their "assets" than others due to the loose control of virtual private server (VPS) tenants and host owners on their own assets. Small as their proportion is, they have wreaked havoc on the Internet. We draw this conclusion because of the fact that, in 2017, 20% of IP addresses attacked more than one target and 0.39% of attack sources were responsible for 90% of attack events.

Figure 3.13 Most attack events initiated by a small portion of attack sources



Furthermore, we discovered that these IP addresses followed some pattern in their malicious activities. Specifically, an IP address involved in spam attacks has a 90% chance of performing malicious scans in the Internet, while bots are often associated with various attacks, most frequently malicious scans and other malicious activities such as spam and phishing.

Figure 3.14 Attack pattern of attack sources



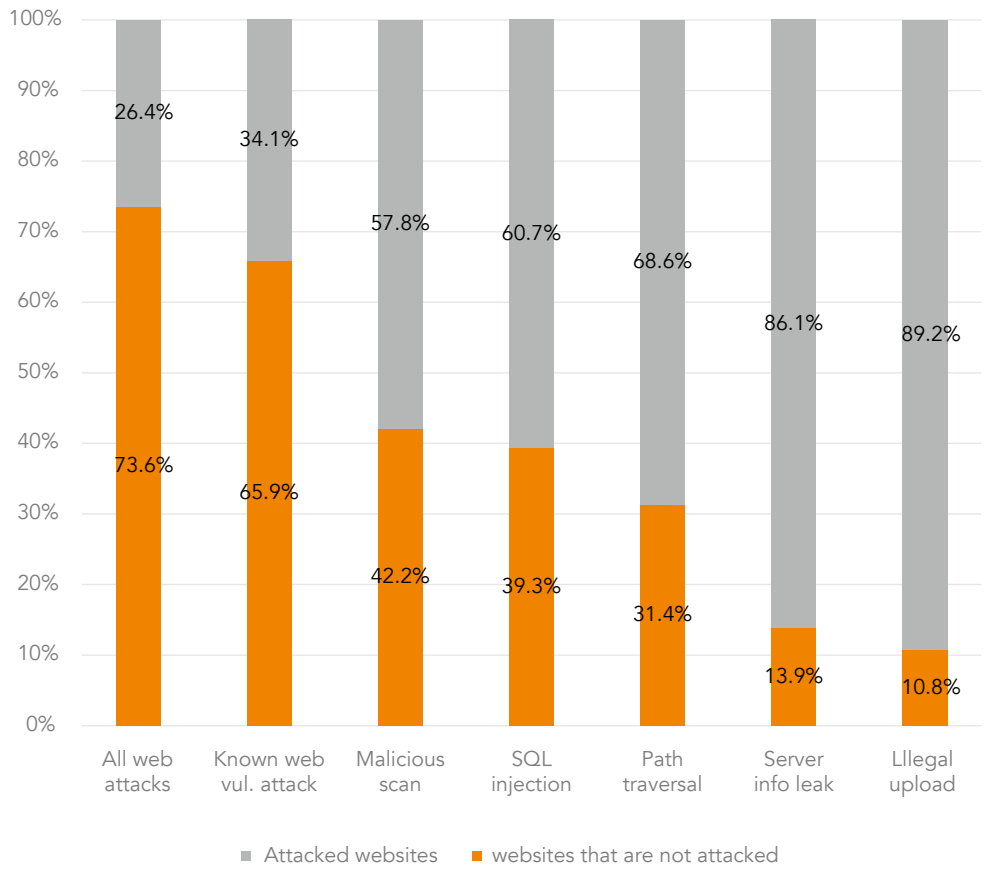
For these high-risk IP addresses, we recommend that they be blocked based on threat intelligence on IP addresses so as to effectively reduce the routine O&M workload.

3.2.2 Web Attack

3.2.2.1 76% Websites Having Been Attacked

Web attacks are a common type of attacks. In general, websites usually have the most direct assets exposed on the Internet. On various hacking technique and scripting tool forums, one of the most frequently discussed topics is web attacks. Generally, SQL injection and cross-site scripting (XSS) are easier to implement and its related techniques are more straight forward to master than attacks exploiting vulnerabilities in protocols/programs and memory leaks. We observed that 76% of websites suffered attacks at least once in 2017. Understandably, to be attacked is almost inevitable for websites that are focused on Internet services and use web as major user interfaces.

Figure 3.15 Comparison of sites that have been attacked and those not attacked

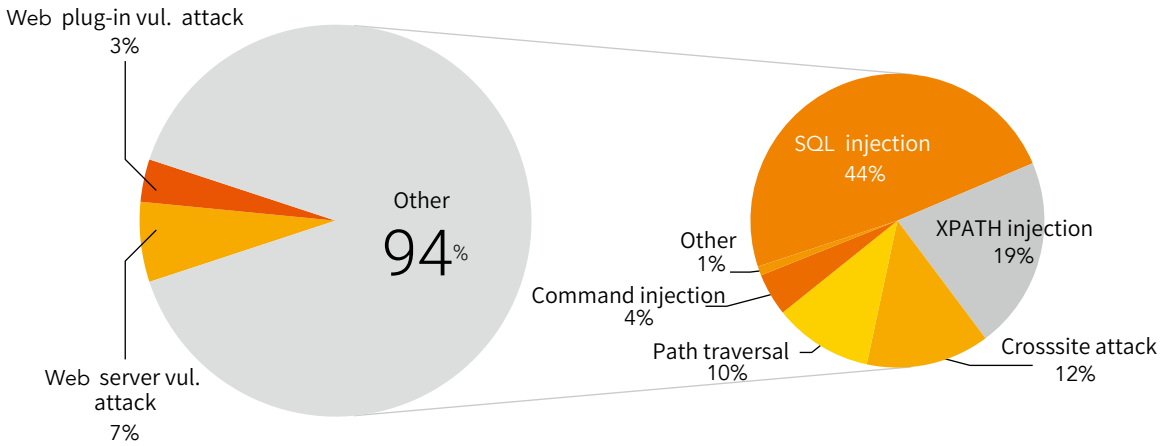


[illegible]2017[illegible]DDoS[illegible]Web[illegible]

3.2.2.2 Traditional Attack Methods Still Effective

Of all attacks against web servers, the most conventional ones, such as SQL injection, XPath injection, cross-site attacks, path traversal, and command injection, still account for more than 90%. Web attacks have become the most prevalent threat and also are easier to implement compared with other attacks. It is true that this type of attacks has been well known in recent years. Management in business environments, however, lags far behind. As a result, hackers are more than happy to use web applications as an entry to intranets. Among the seemingly never-ending attacks, traditional ones are still effective. As the most frequently seen attacks, countermeasures need to be considered carefully.

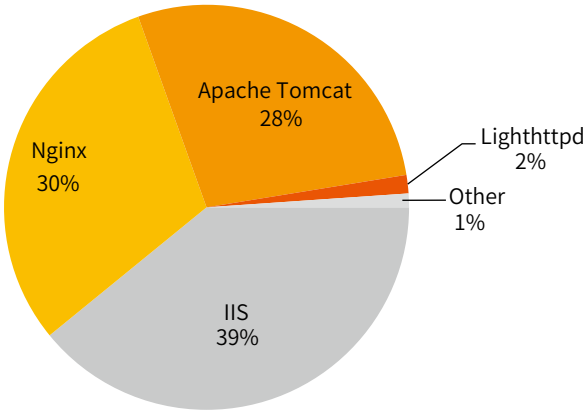
Figure 3.16 Classification of web attacks



3.2.2.3 Most Attacked Web Servers

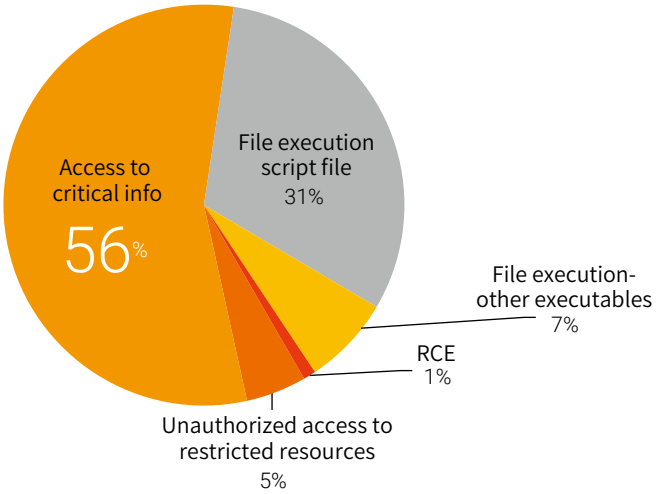
The most attacked types of web servers are Apache Tomcat, nginx, and Microsoft IIS.

Figure 3.17 Proportions of web server types attacked



Vulnerability exploitation, as an attack method, can, in most times, lead to disclosure of critical information, including directory and file enumeration, file path disclosure, disclosure of source code of website scripts, and leak of system configurations. This type of attacks accounts for 56% of all web attacks. Another significant type of attacks is file execution. Specifically, attackers exploit flaws in server programs' resolution of URLs and file names and leverage the file upload function to execute the uploaded files as scripts for the purpose of further intrusion via webshells. Besides, some attacks can allow access to restricted resources with escalated privileges so that attackers can read, download, upload files or even run executables in a restricted directory.

Figure 3.18 Distribution of vulnerabilities in web servers



It is worth noting that this trend is consistent with that mentioned in the *2017H1 Cybersecurity Insights*. Hackers, when attacking web servers, most frequently exploit very old vulnerabilities. The following table lists top 5 vulnerabilities favored by hackers.

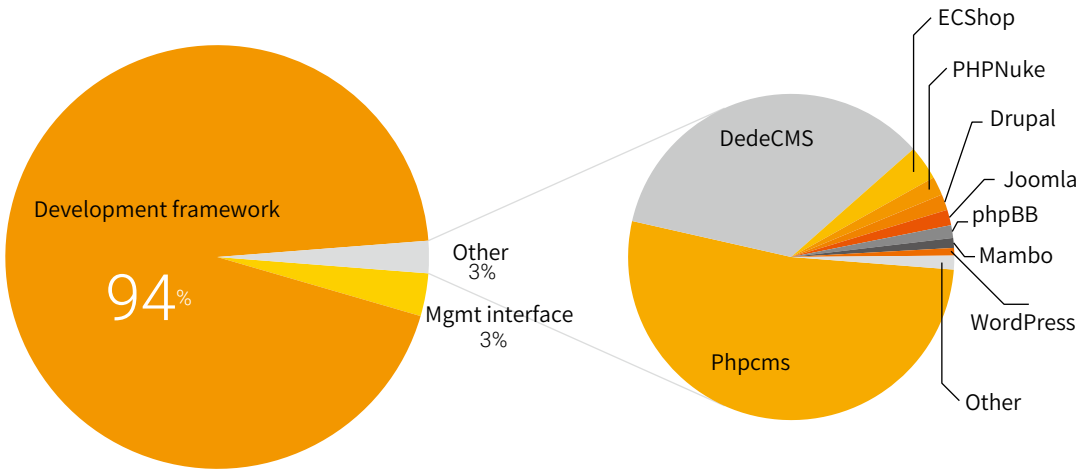
Figure 3.19 Top 5 vulnerabilities most frequently exploited in web attacks

Vulnerability Name	Vulnerability Description	Product
CVE-2008-2938	Code in Tomcat for handling requests is vulnerable when allowLinking and UTF-8 are enabled. A remote attacker could exploit this vulnerability to read arbitrary files from a server via encoded directory traversal sequences in the URI.	Apache Tomcat
CVE-1999-0253	IIS determines whether to directly display the content of a file or to execute it as a script via the extension of the file name. For ASP files, if the extension is .asp in the request, IIS can handle it properly. If a dot (.) is appended to the extension or %2e is contained, IIS does not regard it as an ASP file and so will directly display the content of this file. However, the file system ignores the dot following the file name. Therefore, it can find the correct file.	Microsoft IIS
CVE-2009-4445	This vulnerability allows upload of certain executable files.	Microsoft IIS
CVE-2009-4444	This vulnerability allows upload of certain executable files.	Microsoft IIS
CVE-2000-0886	Microsoft IIS 4.0/5.0, when handling the CGI application (.exe, .pl, .php, and so on), does not perform a proper security check of CGI file names requested by users. This may cause IIS to mistakenly open or run a file if a special character is contained in the file name.	Microsoft IIS

3.2.2.4 Most Targeted Web Frameworks

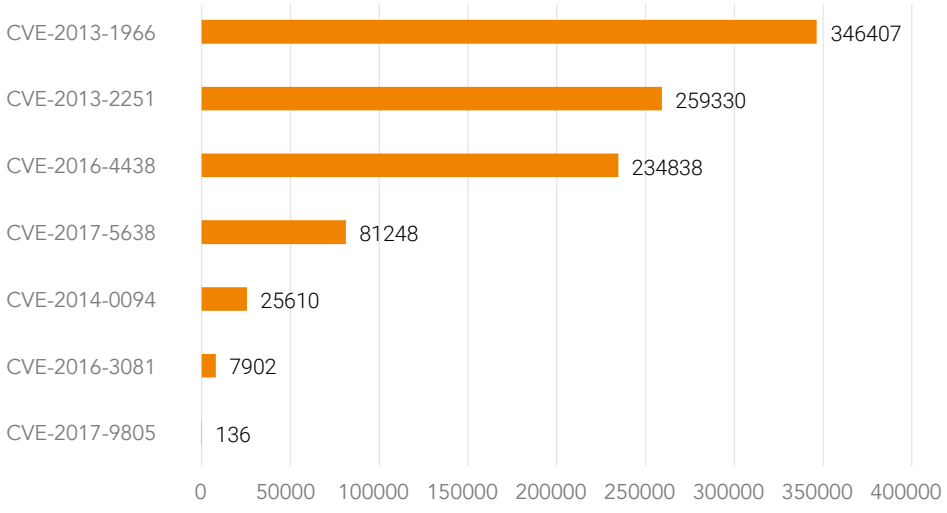
Web applications mentioned in this article include various types of software for setting up websites, such as different content management systems (CMSs) built in PHP, JSP, or ASP, and some special interfaces for management purposes, such as the famous phpMyAdmin and web access interfaces of NoSQL databases.

Figure 3.20 Most targeted web applications



A web framework is a software framework designed to support the development of web applications, including dynamic websites, web application programs, and web services. Many universal web service systems are also developed based on similar frameworks. Examples of web frameworks are Django, ThinkPHP, Apache Struts, and Spring. According to statistics, attacks targeting framework programs are most frequently seen. Struts is a typical example that attracts much attention from attackers. ThinkPHP and Spring are also attacked from time to time. The following figure shows vulnerabilities in the Struts framework that are most exploited.

Figure 3.21 Most exploited Struts vulnerabilities

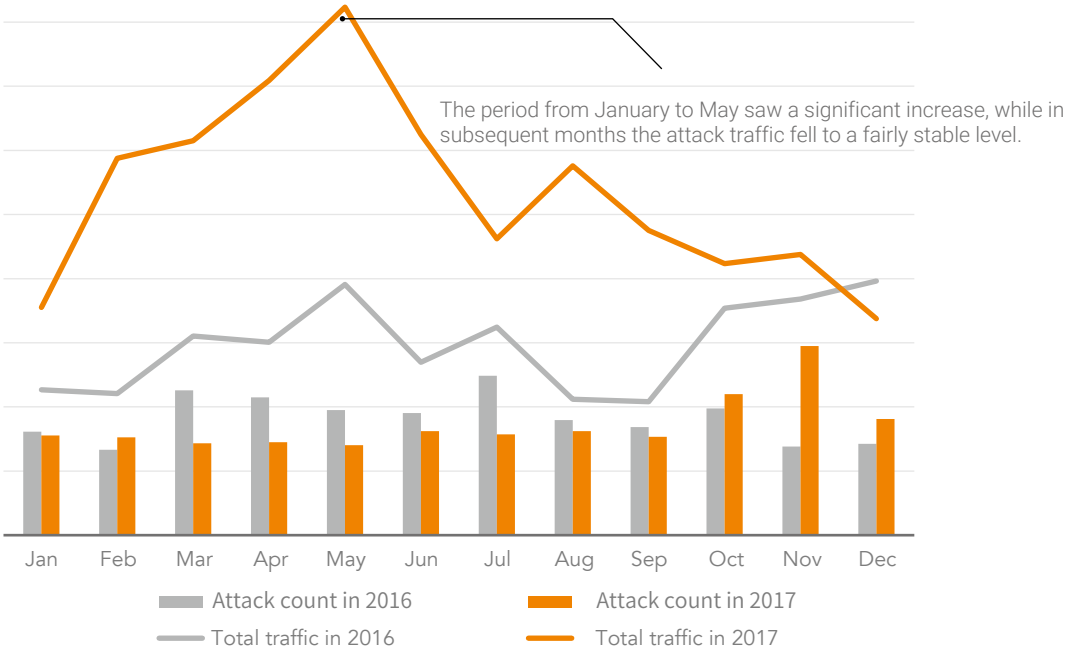


3.2.3 DDoS Attack

3.2.3.1 207,000 Attacks a Year

In 2017, the total number of attacks reached 207,000, on a par with the previous year. The total attack traffic, however, fluctuated rather obviously throughout the year. The period from January to May saw a significant increase, while in subsequent months the attack traffic fell to a fairly stable level. Compared with 2016, 2017 was still an eventful year, with the total attack traffic increasing significantly.

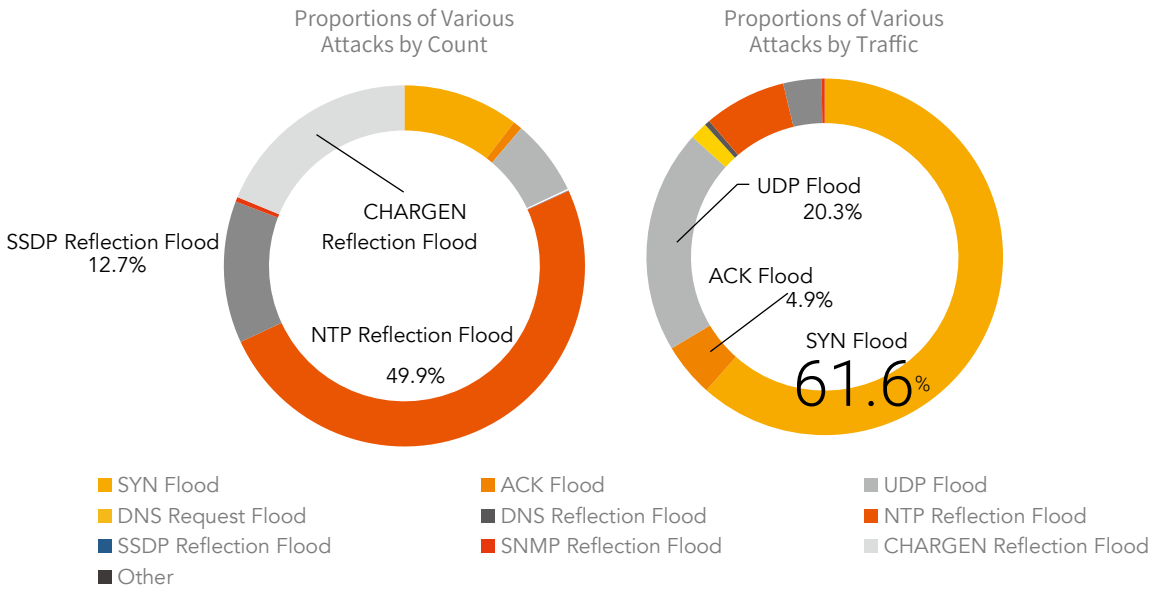
Figure 3.22 Monthly number and traffic of attacks in 2016 and 2017



Source: 2017 DDoS and Web Application Attack Situation Report, China Telecom DamDDoS Team and NSFOCUS

In terms of attack types, the most frequently seen attacks in 2017 were still reflection attacks. This is because, with these attacks, hackers can generate amplified traffic even with a limited bandwidth. In terms of the traffic, SYN flood attacks generated over 60% of traffic throughout 2017. Based on a comprehensive analysis of network environments in 2017, we believe that this was closely related to the expansion of IoT botnets. The staggering number of IoT devices that need to always stay online but with insufficient protection make them a hotbed of DDoS attacks.

Figure 3.23 DDoS attack type distribution

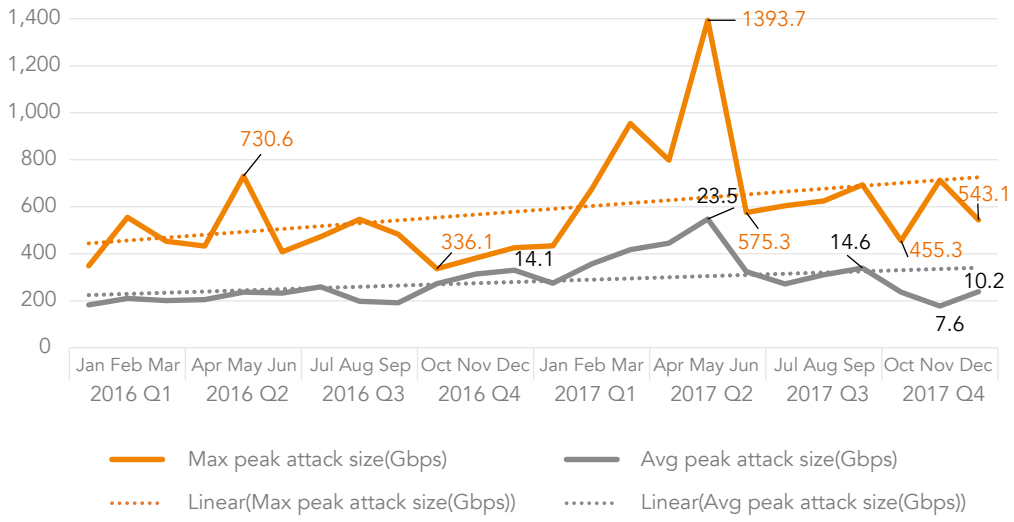


Source: 2017 DDoS and Web Application Attack Situation Report, China Telecom DamDDoS Team and NSFOCUS

3.2.3.2 Attack Size Peaking at 1.4 Tbps

It is nothing new that attack traffic keeps growing. Reports of the past two years show that each month saw attack traffic of over 100 Gbps and sometimes even over 1 Tbps. In May 2017 when DDoS attacks were most rampant, the peak traffic hit 1.4 Tbps. Such gigantic attacks have posed great challenges to protection capabilities of defenders.

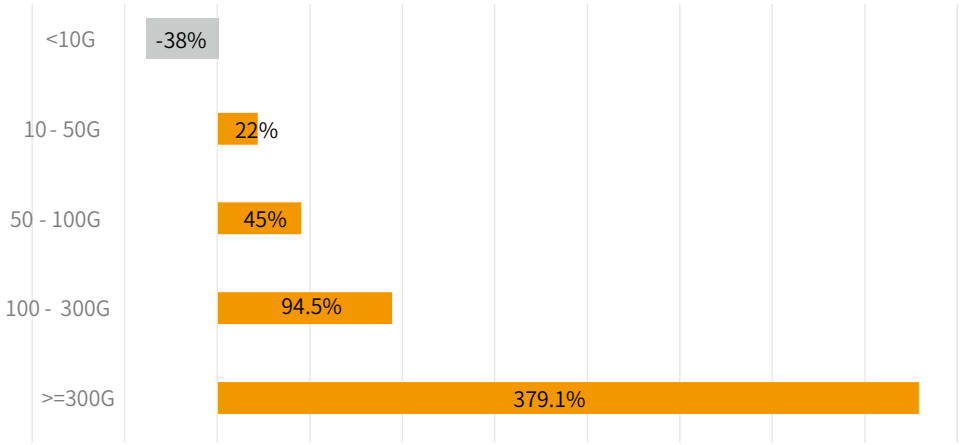
Figure 3.24 Monthly single-attack traffic peak and average attack peak



Source: 2017 DDoS and Web Application Attack Situation Report, China Telecom DamDDoS Team and NSFOCUS

In addition, from the distribution of traffic, we can find that voluminous attacks increased significantly. This was also an obvious trend in 2017.

Figure 3.25 Year-on-year increase/decrease of attacks in various peak size ranges in 2017

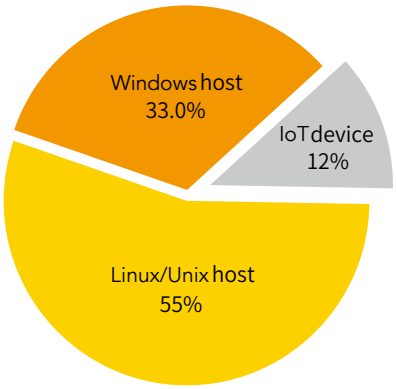


Source: 2017 DDoS and Web Application Attack Situation Report, China Telecom DamDDoS Team and NSFOCUS

3.2.3.3 12% of Attacks from IoT Devices

Of all DDoS attacks in 2017, large or small, the proportion of those originated from IoT devices was so large as not to be ignored. Arguably, IoT devices have become a category of attack sources calling for special attention. From the holistic point of view, the steady development of IoT industry makes it hardly possible for security techniques to keep up. It is foreseeable that threats posed by IoT devices will be put on the agenda of governance. As a handy tool, more and more IoT devices are expected to get involved in DDoS attacks.

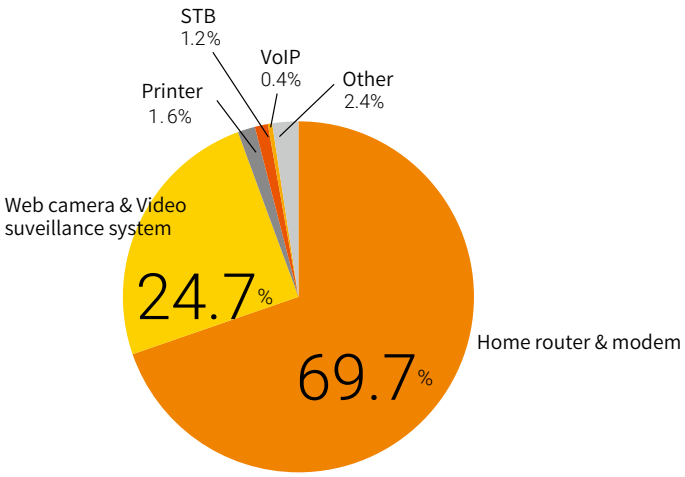
Figure 3.26 Types of devices exploited to launch DDoS attacks



Source: 2017 DDoS and Web Application Attack Situation Report, China Telecom DamDDoS Team and NSFOCUS

When we speak of IoT devices involved in DDoS attacks, routers and cameras are the major types of devices. This is consistent with the development of IoT in the past two years. A great number of routers and web cameras have been introduced into production and living environments, with no sufficient security measures enforced. We have every reason to believe that attacks leveraging the IoT will become more diverse in the future.

Figure 3.27 Types of IoT devices exploited to launch DDoS attacks



Source: 2017 DDoS and Web Application Attack Situation Report, China Telecom DamDDoS Team and NSFOCUS

According to statistics, cameras used for malicious purposes accounted for about 4.8% of all cameras, three times the proportion (1.57%) of maliciously exploited IP addresses to the total IP addresses in China. Therefore, we need to pay close attention to cameras.

3.2.3.4 Memcached-based DRDoS Attacks with Strong Attack Capabilities

At the beginning of 2018, a Memcached-based reflection denial of service (DRDoS) attack was detected, attracting wide attention from all sides. It was reported that, on February 28, 2018, the peak traffic of the Memcached-based DRDoS attack hit an astonishing 1.35 Tbps. Memcached is a high-performance open-source distributed memory object caching system. It is widely used all over the world as to improve the scalability of web applications and solve many issues related to big data caching. Memcached is an in-memory key-value store for small chunks of data and uses such data for calls to databases and APIs or page rendering. It is the key-value store that the attacker depends on for reflection attacks. In terms of amplification factors of various reflection attacks, Memcached-based attacks come top with a factor up to 51,000.

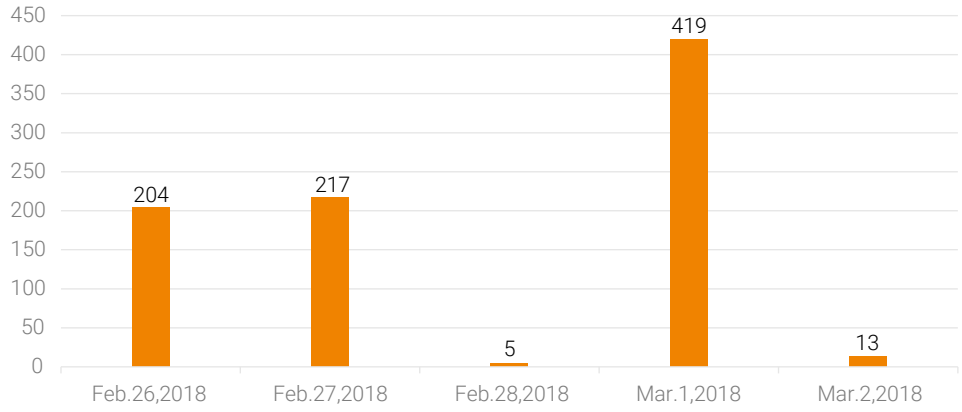
Figure 3.28 Amplification factor of each type of reflection attacks[1]

Targeted Protocol of Reflection Attacks	Bandwidth Amplification Factor
DNS	28 to 54
NTP	556.9
SNMPv2	6.3
NetBIOS	3.8
SSDP	30.8
CharGEN	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake Network Protocol	63.9
Steam Protocol	5.5
Multicast DNS (mDNS)	2 to 10
RIPv1	131.24
Portmap (RPCbind)	7 to 28
LDAP	46 to 55
CLDAP	56 to 70
TFTP	60
Memcache	10,000 to 51,000

1 https://www.us-cert.gov/ncas/alerts/TA14-017A

According to the attack monitoring data provided by the DamDDoS Team of China Telecom, 79 Memcached-based DRDoS attacks were launched globally with the peak volume of 419 TB in just five days.

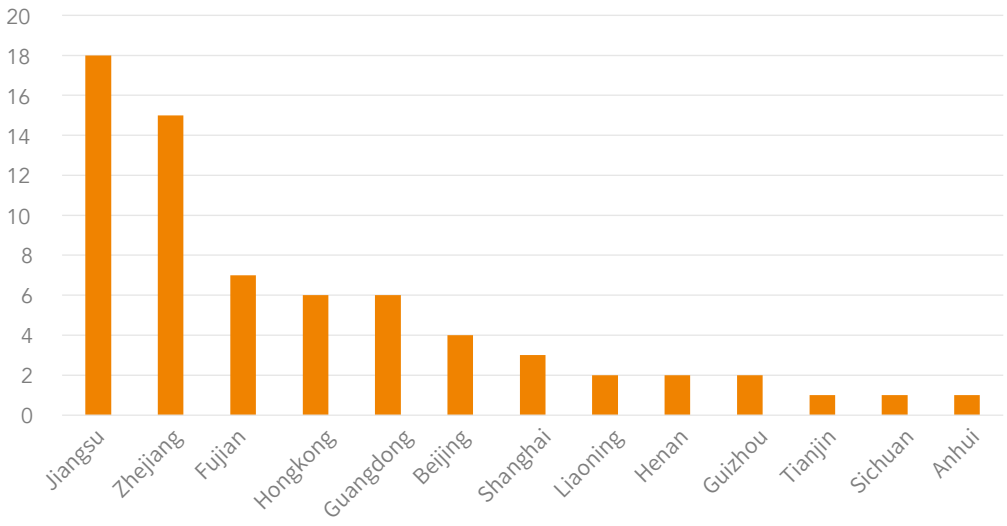
Figure 3.29 Total daily traffic of Memcached-based DRDoS attacks



Source: 2017 DDoS and Web Application Attack Situation Report, China Telecom DamDDoS Team and NSFOCUS

A total of 68 Memcached-based DRDoS attacks were detected in China, with Jiangsu and Zhejiang provinces hit hardest. Of all those attacks, the maximum single-peak size hit 505 Gbps and the longest-lasted attack occurred on March 1, lasting for 1.2 hours and contributing traffic totaling 103.8 TB.

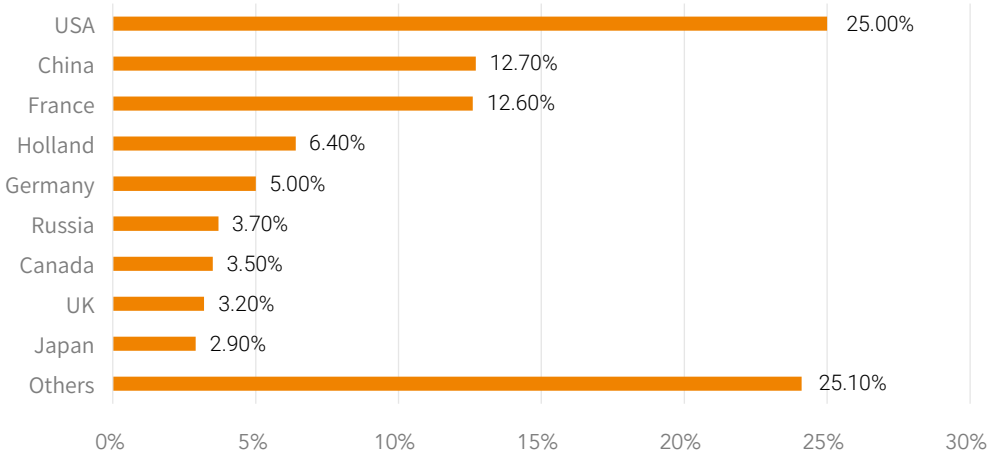
Figure 3.30 Number of Memcached-based DRDoS attacks detected in provinces and municipalities in China



Source: 2017 DDoS and Web Application Attack Situation Report, China Telecom DamDDoS Team and NSFOCUS

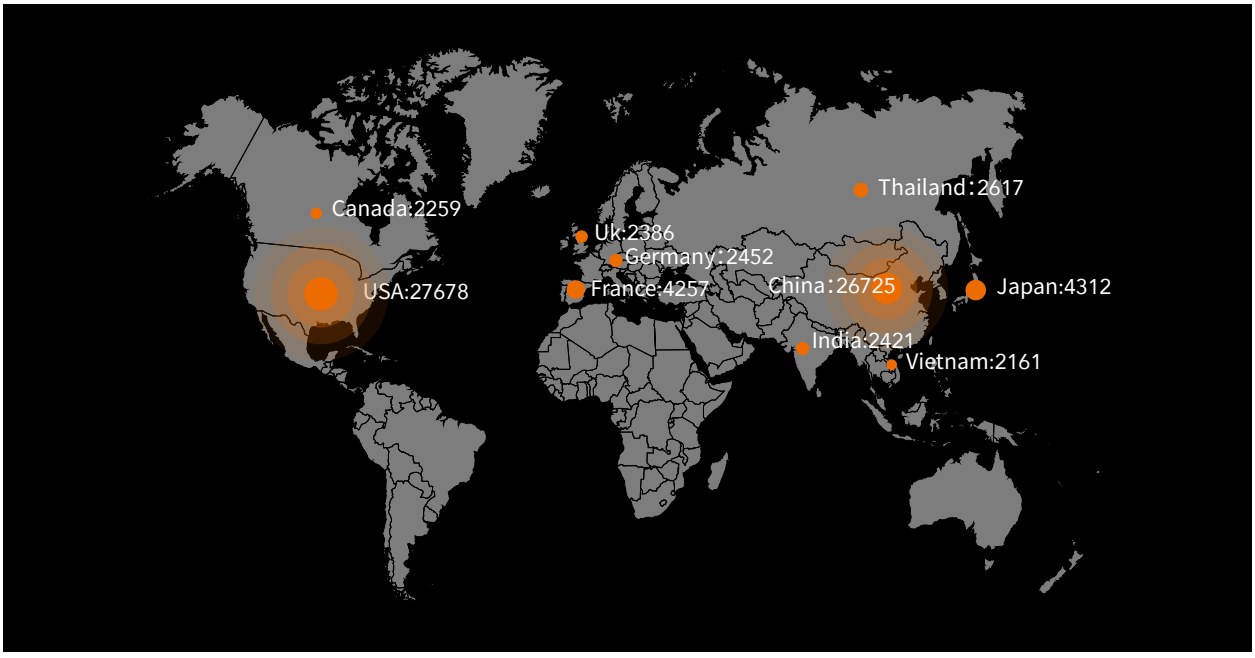
Globally, a total of 3790 Memcached servers were exploited to help with Memcached-based DRDoS attacks. Such reflection sources are distributed in 96 countries and regions across the world, a quarter of which are in the USA. China has the largest number of exploited Memcached servers which account for 12.7% of the total number with Guangdong, Beijing, and Zhejiang contributing the biggest part.

Figure 3.31 Global distribution and percentages of Memcached-based DRDoS attacks



Source: 2017 DDoS and Web Application Attack Situation Report, China Telecom DamDDoS Team and NSFOCUS

According to statistics collected by NTI, 104,506 Memcached servers are at risk of exploitation around the world. In terms of geographic distribution, USA has the most Memcached servers that can potentially be exploited, followed by China.



Source: 2017 DDoS and Web Application Attack Situation Report, China Telecom DamDDoS Team and NSFOCUS

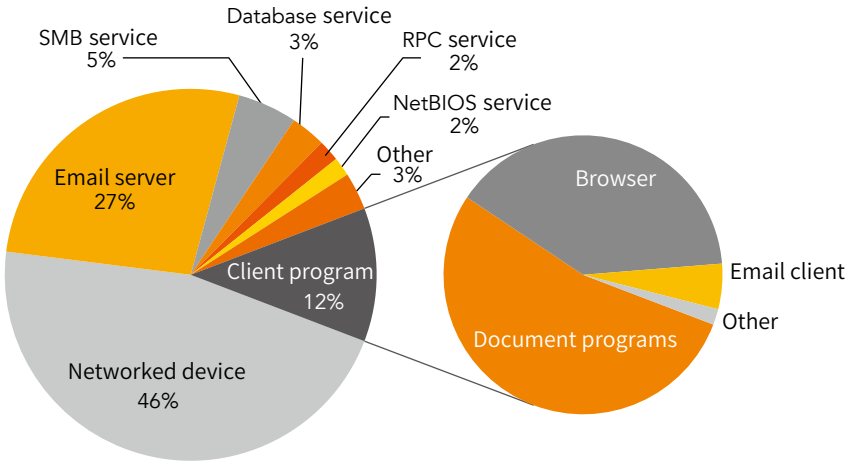
A large number of exploitable Memcached reflectors are prerequisites for super high-volume DRDoS attacks. If these Memcached servers are not patched promptly, DRDoS based on them will continue to increase and lead to a disastrous consequence.

In terms of attack impact, all Internet services are potential targets of Memcached-based DRDoS attacks. On one hand, bandwidths or services may be hit by super high-volume attacks, which would, in turn, cause the outbound bandwidth to be saturated and normal services to be unavailable. On the other hand, the internal Memcached system may be exploited by criminals to become their accomplice. We urge customers in various regions and sectors to remain highly vigilant against Memcached-based DRDoS attacks which may have a direct impact on servers or compromise information security by covering other attacks. For recommendations on protection and defense against Memcached-based DRDoS attacks, see [2]*Deep Analysis of Memcached Large DRDoS Attacks*.

3.2.4 System Attacks

According to our investigation on common network products and services, attacks targeting the server-side account for as much as 88%, while attacks targeting the client-side account for only 12%. For attacks targeting the server-side, 46% target networked devices, such as routers and printers. In addition, the proportion of attacks targeting the email server reaches 27%. Most of such attacks are launched by sending spam emails. For attacks targeting the client-side attacks, document programs, browser programs, and email client programs are the most hit ones. Document programs refer to the software for processing and reading texts and images, including Microsoft Office, Adobe Reader, and streaming media players. Browser programs include Firefox, Microsoft Edge, and Microsoft Internet Explorer, all of which are the frequent target of attackers.

Figure 3.32 Products and services targeted by system



3.2.4.1 Shadow Brokers Disclosure Leading to Many High-Risk Attack Events

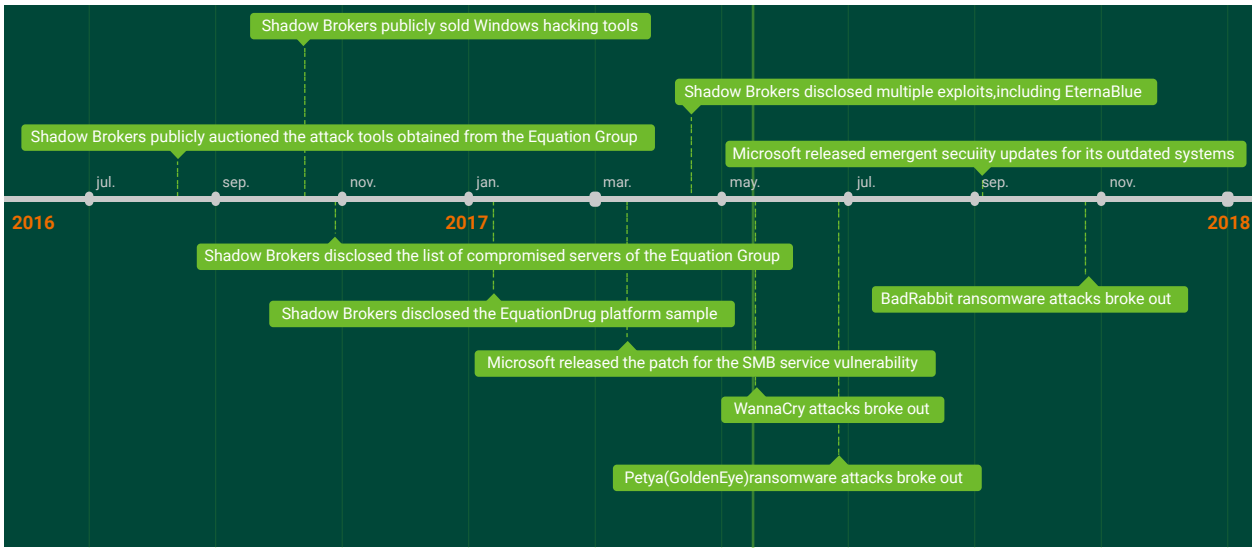
The Shadow Brokers (TSB) is a hacker group who first appeared in the summer of 2016. They published several vulnerabilities containing hacking tools from the National Security Agency (NSA), including a couple of zero-

2 http://blog.nsfocusglobal.com/categories/emergency-response/deep-analysis-of-memcached-large-drdos-attacks-china-telecom-damddos-nsfocus-jointly-released/

day exploits. Specifically, these exploits and vulnerabilities targeted enterprise firewalls, antivirus software, and Microsoft products. The Shadow Brokers originally attributed the leaks to the Equation Group threat actor, who have been tied to the NSA's Tailored Access Operations unit. A vulnerability in the Server Message Block (SMB) service contained in EternalBlue is used for the propagation of WannaCry, Petya, and BadRabbit ransomware and corresponding attacks, leading to widespread concern. Among all attacks, Shadow Brokers-related attacks make up only 3.47%, but they pose the greatest potential hazards.

- Attacks targeting the Windows SMB service account for 89.8%. The tools disclosed by the Shadow Brokers are most used for SMB exploits and attacks, including the famous EternalBlue, EternalChampion, and EternalRomance.
- The activities of the backdoor tool, Darkpulsar, make up 3%. As a simple backdoor program, Darkpulsar has relatively few functions, most of which are to execute shellcode and download DLL, paving the way for planting complicated backdoors.
- Also, there are some attacks targeting Windows RPC and RDP services. By using various tools to launch attacks, an attacker can take control of the system to implant a backdoor for further intrusion.

Figure 3.33 Significant events of Shadow Brokers

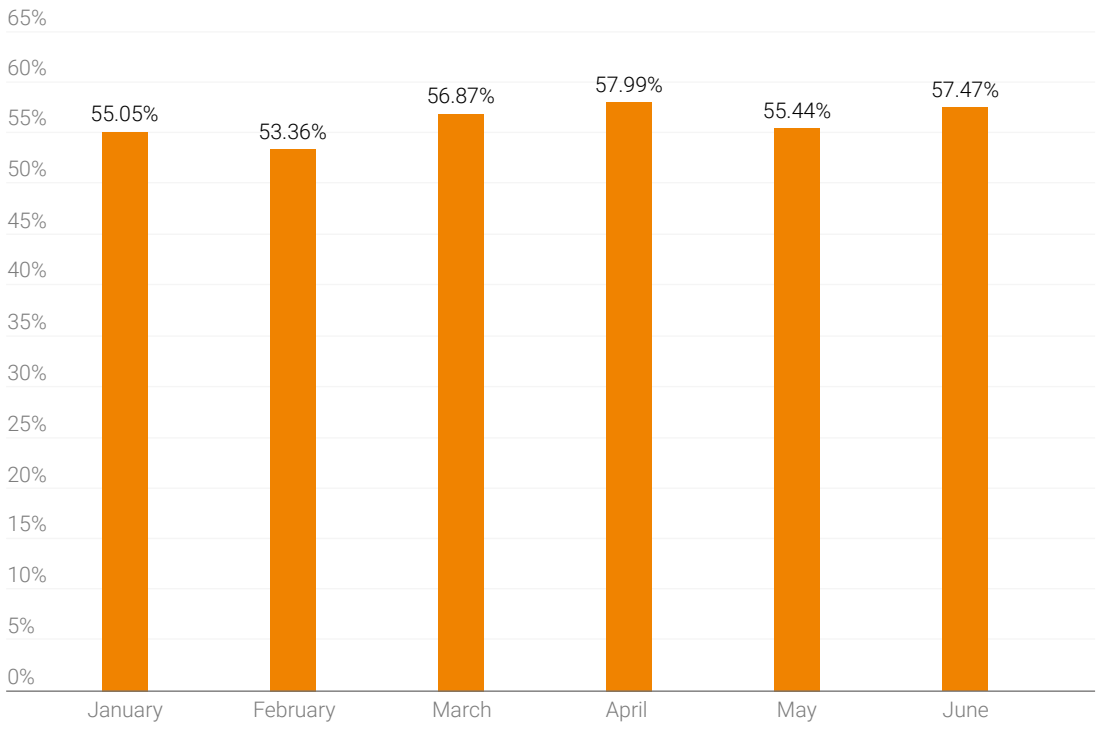


As shown in the preceding figure, from August 2016, the Shadow Brokers started to auction or sell hacking tools obtained from the Equation Group. In April 2017, they revealed a collection of exploits on the Internet. The leak includes the notorious EternalBlue, which contains an SMB vulnerability. This vulnerability has been aggressively exploited by three ransomware families, including the WannaCry ransomware in May, Petya ransomware (aka Golden Eye) ransomware in June, and BadRabbit ransomware in October. Actually, Microsoft fixed the exploited vulnerability and published related patches in the middle of March, but ransomware families could still exploit the vulnerability to spread widely till October.

3.2.4.2 Emails Becoming an Important Attack Entrance

In recent years, malicious emails have become an important infection path for various malicious codes. Malicious mails use social engineering methods to trick users into opening a malicious attachment file or clicking a malicious website link, in a bid to infect the users with various viruses (such as encrypted ransomware or trojan software), thereby causing direct economic losses. It is reported that Jaff and Locky, distributed by the notorious spam botnet Necurs, were still quite active in 2017[3] . In addition, malicious mail-based attacks against enterprises have become quite common and can bring great profits. Some attackers directly trick users into disclosing key information or performing transfer operations, resulting in serious economic losses. According to the statistics[4] , Business Email Compromise (BEC) attacks have caused greater economic losses even than ransomware.

Figure 3.34 Percentages of malicious emails in enterprise correspondence

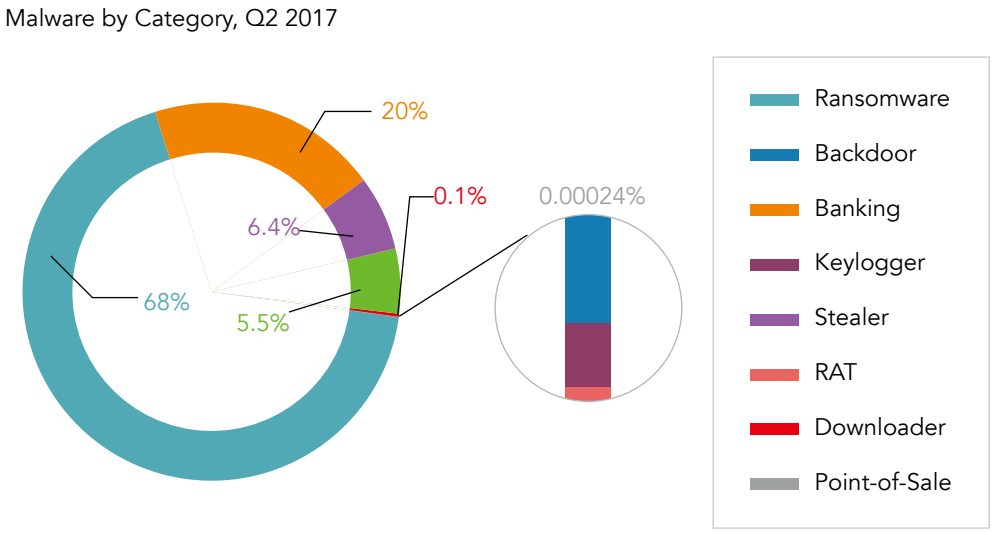


Data source: https://securelist.com/spam-and-phishing-in-q2-2017/81537/

3 Data source:https://www.bleepingcomputer.com/news/security/ransomware-was-the-most-prevalent-malware-payload-delivered-via-email-in-q2-2017/

4 Data source:https://www.nttsecurity.com/en-us/gtir-2017

Figure 3.35 Spreading of malware via malicious emails

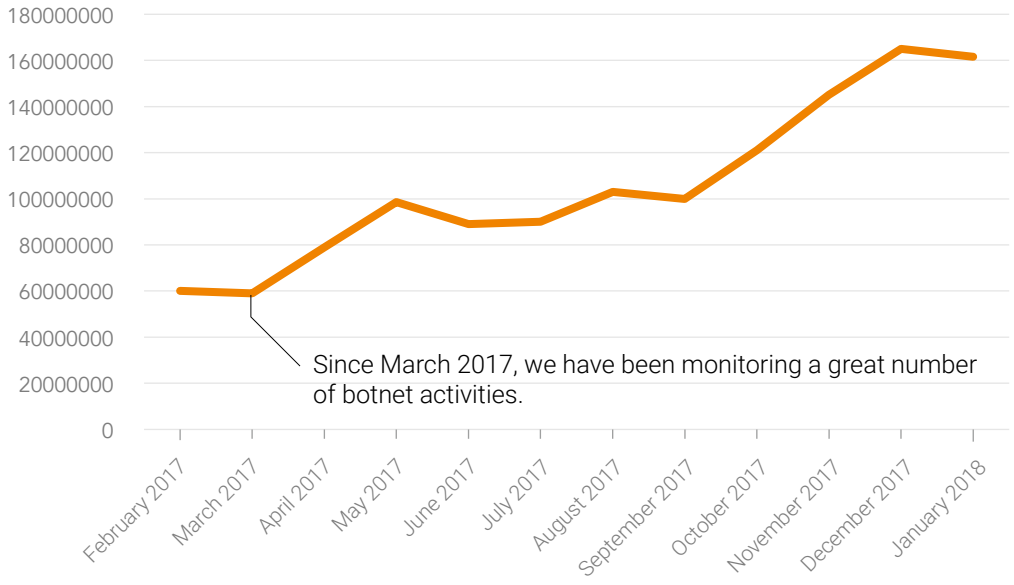


Data source: Proofpoint: https://www.bleepingcomputer.com/news/security/ransomware-was-the-most-prevalent-malware-payload-delivered-via-email-in-q2-2017/

3.2.4.3 Netcore Botnet-based Attacks Becoming Quite Frequent

Attack statistics show that the proportion of attacks targeting networked devices reaches as much as 46%, most of which targeting routers. According to our monitoring data of 2017, one botnet family was very rampant in attacks. The attacks targeted the Netcore routing device which was found to have a firmware backdoor by Trend Micro as early as in 2014. This device forcibly enables a management interface (which users cannot disable or turn off) which has a unified hardcoded password. Hackers can take control of this device as long as it is accessible. In earlier reports, it was widely believed that this vulnerability could be used to launch intermediate attacks. Only in recent attack monitoring did we find that botnet family named Gafgyt helped widely exploit this vulnerability. Since March 2017, we have been monitoring a great number of botnet activities. Such activities have continued through the end of 2017 and show no trend of slowing down.

Figure 3.36 Statistics of router backdoor-based attacks launched by Gafgyt



Gafgyt had an extensive impact on the network environment, whether in the geographical or industrial distribution aspect. It was the Netcore backdoor that the Gafgyt botnet depends on for large-scale spread. Though it has been three years since the vulnerability was published, there are still a lot of devices with this vulnerability unpatched on the Internet.

Figure 3.37 Distribution of sectors targeted by Gafgyt botnet-based attacks

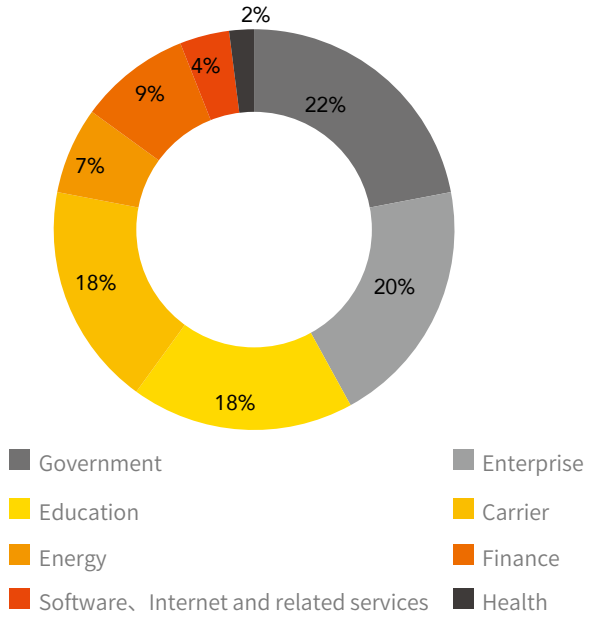
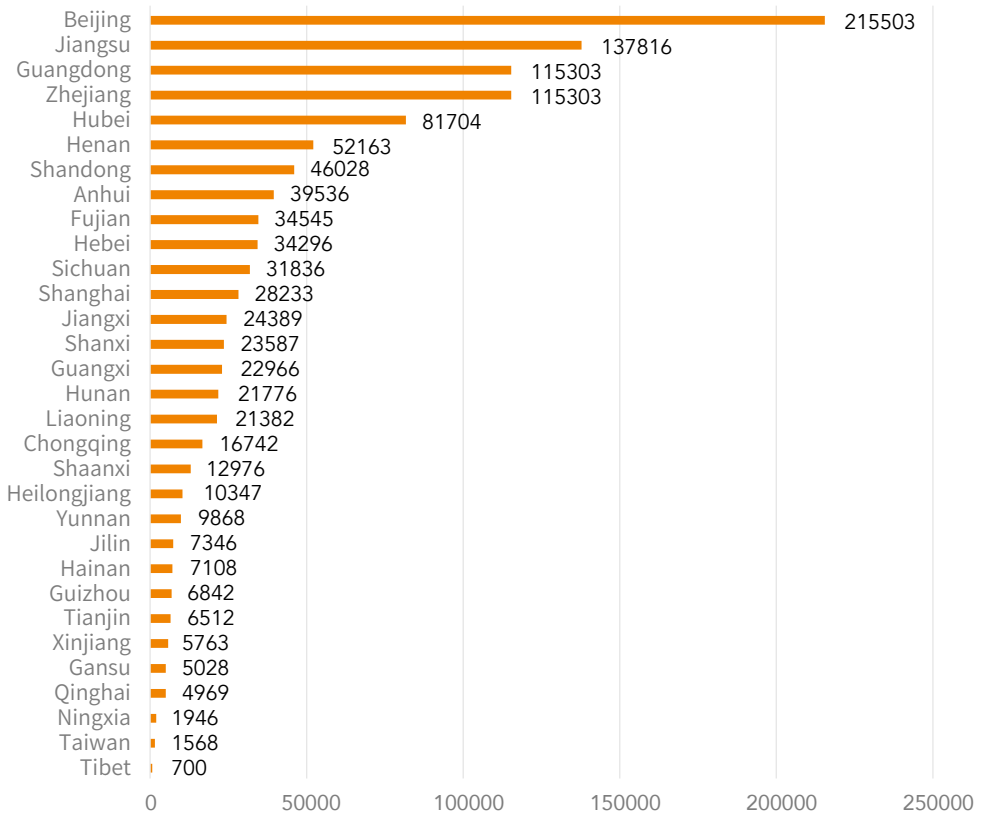


Figure 3.38 Provincial distribution of Gafgyt



We recommend that enterprises check their own assets (not limited to traditional IT assets, but also various network devices e.g. printers and smart routers) and regularly update the software. Some of these devices, as the enterprise intranet perimeter devices, should be better protected against unnecessary risks, and prevented from being compromised by botnets attacks.

3.3 Malware

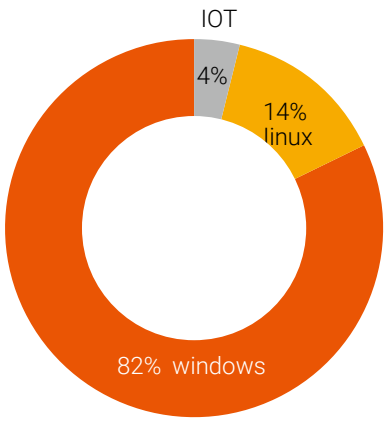
In 2017, we detected 310,620 hosts that were injected with ransomware and bot software, with attack sources from 34 countries/regions. Among various types of malware, botnets and ransomware are the most common and eye-catching.

3.3.1 Trend of Botnets

Botnets are always the hazard that cannot be overlooked in the Internet environment. As a common malicious program, botnets feature high elusiveness and share characteristics with worms and trojans. Botnets can take control of the target host by exploiting vulnerabilities, so as to steal information from the host or instruct the host to launch network attacks. Botnets pose great hazards to the controlled hosts and even the entire network environment. According to data obtained from NTI, botnets were still active in 2017, especially the second quarter that saw the most botnet activities. As for attack instructions, C&C servers of botnets, in the most active state,

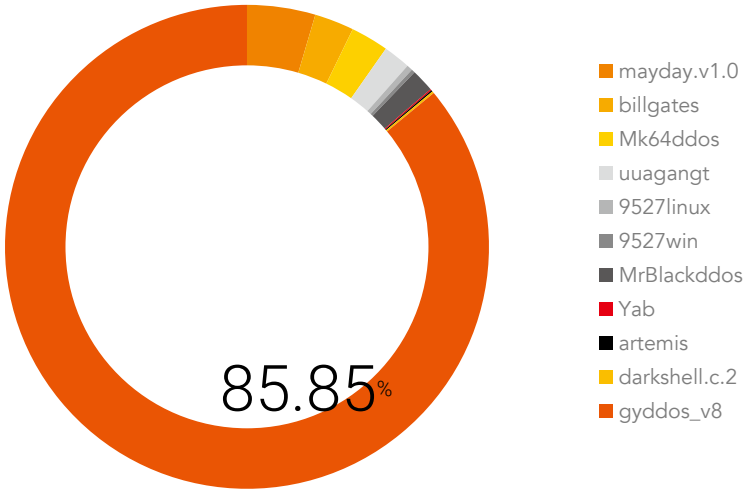
issued 5187 instructions on average each day and a single C&C server even issued 114 instructions in a day. In 2017, botnets continued to grow in both quantity and scale. The number of C&C servers steadily grew, which could be seen in August, and the number further increased 1.67% in October from the previous month. At the same time, the global number of controlled hosts experienced an intermittent growth. In August, this number tripled (320%) over the previous month. Among all botnets under our constant monitoring, at least 4% targeted IoT devices. Most botnets are still based on the Windows platform, but in recent years, with more and more IoT, smart, and mobile devices connected to the network, we expect to see an increasing number of malicious activities targeting those devices.

Figure 3.39 Distribution of platforms on which botnets run



"Ghost" is an active and influential botnet in China, which is developed based on Windows platforms. In the recent botnet activity monitoring, we saw a whirlwind of Ghost activities. This botnet family appeared very early and enjoys different variants and a quite mature commercial operation model. Therefore, attention needs to be paid and counter measures should be taken against this botnet.

Figure 3.40 Statistics of instructions of active botnet families



At present, "Ghost" has at least 10 versions, each of which has more functions than the previous version. DDoS attack techniques also get updated continuously. So far, "Ghost" is often used to launch high-volume attacks, spreads on a large scale, and supports different commercial operation models.

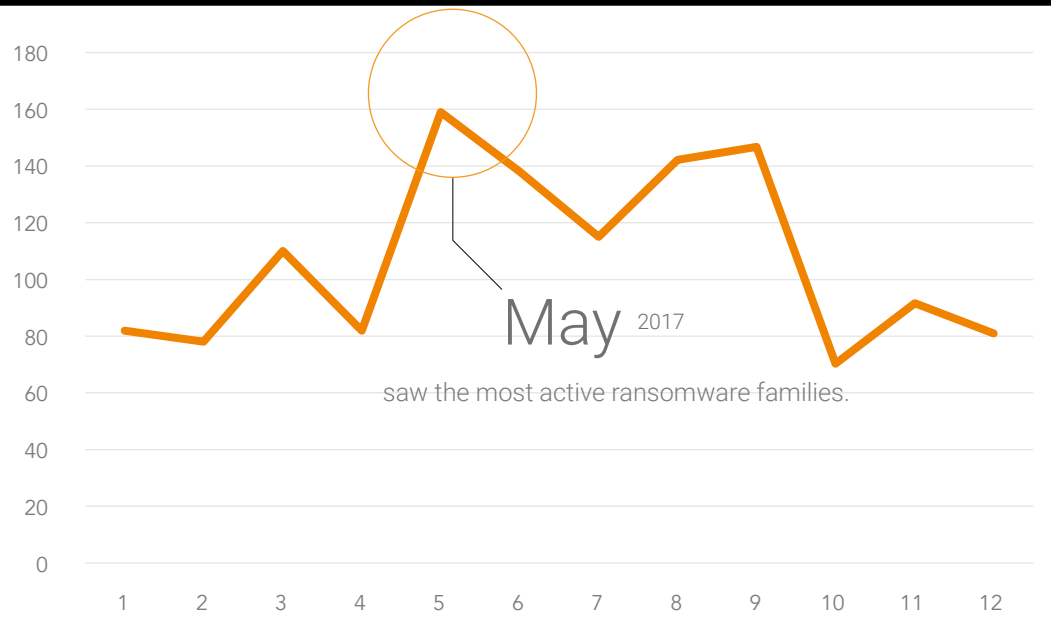
3.3.2 Trend of Ransomware

Ransomware is the most eye-catching malware in 2017.

- On May 12, 2017, the WannaCry ransomware exploited the EternalBlue vulnerability to affect over 150 countries. Infected users were asked to pay Bitcoin equivalent to $300 and the required payment would increase to the Bitcoin equivalent to $600 after 72 hours. Seven days after the victim's infection, the computer files would become encrypted permanently.
- In June 2017, the NotPetya ransomware also used EternalBlue to spread itself. It utilized a payload that modified the computer's master boot record (MBR), overwriting the Windows bootloader and then triggering a restart. On the next startup, the payload would be executed and then the system prompted a message indicating that the computer was scanning disks, while in fact the NotPetya ransomware was encrypting computer files. After the file encryption was complete, NotPetya displayed the ransom message demanding a Bitcoin payment equivalent to $300. In July 2017, the virus writer published all keys of the Petya ransomware.
- In October 2017, the BadRabbit ransomware broke out. Attackers first compromised news websites and then used these websites to launch watering hole attacks. The BadRabbit ransomware asked victims to pay 0.05 Bitcoin (equivalent to $300) within 40 hours after infection.

May 2017 saw the most active ransomware families.

Figure 3.41 the number of active ransomware families in 2017



4. Appendix

Mappings between vulnerability categories and Common Weakness Enumeration (CWE) IDs	
Targeted Protocol of Reflection Attacks	**Vulnerability Category**
CWE-119	Buffer Errors
CWE-284	Improper Access Control
CWE-79	Cross-Site Scripting (XSS)
CWE-200	Information Leak / Disclosure
CWE-264	Permissions, Privileges, and Access Control
CWE-20	Input Validation
CWE-89	SQL Injection
CWE-125	Out-of-bounds Read
CWE-399	Resource Management Errors
CWE-476	NULL Pointer Dereference

Microsoft ranked first in 2017 among all vendors for the 1084 vulnerabilities contained in its products.

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