NSFOCUS

平安金融安全研究院
PingAn Academy of Financial Security

2017 Fintech Security Analysis Report

NSFOCUS Technologies, Inc.

hereinafter referred to as NSFOCUS. Founded in Beijing in April 2000, the company has more than 40 branches and subsidiaries at home and abroad, providing most competitive security products and solutions for various sectors, ensuring customers' business continuity. NSFOCUS Threat Intelligence center (NTI) is a professional threat intelligence security center that is built for cyberspace security ecosystem development and threat intelligence applications.

平安金融安全研究院
PingAn Academy of Financial Security

Ping An Financial Security Research Institute

As the industry's first comprehensive organization engaging in financial security research and innovation founded by Ping An Technology, a wholly funded subsidiary of Ping An Group, it provides robust technical support for financial security of Ping An Group, the related sector, and the country and makes technical contributions to information security development and business security risk control of financial institutions, fintech security assurance, and national financial security in the Internet era. This organization is committed to pushing and promoting China's scientific and technological advances in the financial security area and creating a well-recognized financial security brand.

2017 Questionnaire on the Security Status of China's Fintech Enterprises

In this report, a portion of data is sourced from a questionnaire which was jointly launched by NSFOCUS and Ping An Financial Security Research Institute. A total of 1591 copies of the questionnaire were sent out to the following personnel from the security and financial sectors:

- Security architects, security consultants, and security engineers, with a combined percentage of 40.3%
- Security development personnel and operation and maintenance (O&M) personnel, which make up a total of 15.7%
- Chief executive officers, chief information officers, information security officers, heads of the IT departments, and heads of business departments

Contents

1 Executive Summary

On August 22, 2017, the World Economic Forum released Beyond Fintech: A Pragmatic Assessment of Disruptive Potential in Financial Services[1] . This report covers interviews on hundreds of experts from financial and technology realms and is intended to explore the implications of innovation to the global financial ecosystem. The report identifies eight forces that can drive Fintech innovation and their disruptive potential. In addition, it presents future innovative models and paths for seven major financial areas, including payment, lending, wealth management, insurance, and digital banking, which are under the obvious impact of Fintech. Finally, it points out the risks to and potential end states of financial institutions in each area. In recent years, thanks to the development of advanced computer technologies, such as cloud computing, big data, artificial intelligence, and blockchain, financial services are becoming increasingly diverse, convenient, and intelligent. Fintech is growing at a high speed, and so are technological transformation and innovation. Now people have seen the emergence of Fintech 3.0.

In this bustling world, people come and go, with the same thing in mind: interest. And cybercriminals are no exception. While Fintech has become a mainstay for financial products, cybercriminals are constantly diversifying their attack targets and approaches in a bid to cash in on their operations more easily. On the one hand, attackers keep penetrating into the Fintech system, from network services and financial services to core business data and users' properties and privacy. They are no longer content to compromise the availability of financial systems, but are more inclined to directly gain profits from the sale of data and transfer of assets. On the other hand, they are not limited to traditional attacks on information systems, but resort to a roundabout way of infiltration by colluding with insiders for the ultimate end of selling stolen data. A security survey report released by Loudhouse reveals that 35% of employees will sell sensitive data, such as company patents, financial records, and customer credit card details, if the price is right. This finding indirectly corroborates the view that personnel security should receive the same attention as cybersecurity, business security, and data security.

For attackers taking Fintech as the target, profit is their major pursuit. For Fintech security practitioners, in contrast to the traditional protection revolving around vulnerabilities and detection points, a more practical approach is to perform a reverse analysis from the profit generator before deploying their own defense systems.

1 *Beyond Fintech: A Pragmatic Assessment of Disruptive Potential in Financial Services*, World Economic Forum, August 2017.

Current Security Posture

1. Fintech has been largely incorporated into the Internet. 83.5% of institutions or enterprises provide services over the Internet. In the financial sector, about 60% of institutions use various cloud services, most of which are private clouds. Besides, over 20% of institutions use public clouds or hybrid clouds. Financial institutions, when using clouds, are most concerned about access control besides data and privacy protection.

2. 40% of financial institutions can complete the handling of a security event within one day, 40% can do that within a week, and the remaining 20% need more than a week. In addition, nearly half of these organizations spend more than a week fixing a vulnerability.

3. Responses to the questionnaire show that most security events can be ascribed to the lack of security awareness and insufficient input to the operation and maintenance (O&M). This is maybe the root cause of various security management issues. The lack of basic security awareness leads naturally to insufficient input to security and deficient security management systems, which give rise to problems on data security and privacy protection.

4. As for security, Fintech practitioners are most concerned about data security and privacy protection. In the meanwhile, regulatory compliance is also an important consideration for enterprises. But it is worth noting that security measures are a holistic project instead of a single solution to one problem in an aspect or area. Security requires planning from various aspects, including development, management, and O&M. It cannot be thoroughly addressed with only one device or one preventive maintenance inspection (PMI). To better ensure data protection and privacy, a supporting management process and protection solution are required to complete the solution.

5. The most demanded security services include security consultancy, security O&M, and emergency response. From questionnaire responses, we find that the financial sector is lacking in the knowledge and experience of security management and has much to do in security training and talent recruitment.

6. We observe that enterprises begin to pay attention to information security. In addition, most enterprises (71.3%) will increase the budget allocation for security, but only a small portion (21%) of enterprises plan to expand their security teams. Drivers of these moves taken by enterprises include the rapid growth of Internet services, increasingly complicated enterprise business, constant emergence of new techniques, and the gloomier threat landscape. To protect their own business, enterprises need support in both techniques and personnel. Most of them, however, are still inclined to outsource such services in order to alleviate their own burden of management and planning.

Security Situation

1. Compared with 2016, the year 2017 witnessed DDoS attacks at an even larger scale, with the total traffic volume hitting 640,000 TB, up 79.4%. A single-attack traffic peak reached , 1.4 Tbps nearly double that in 2016.

2. In 2017, botnets continued to grow in both quantity and scale. The number of command and control (C&C) servers steadily grew, which could be obviously felt 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%) compared with the previous month.

3. Cyberextortion occurred from time to time, including Opicarus 2017 events that were launched via ransomware, endangering the website security of lots of financial institutions and leading to disclosure of sensitive data.

4. MySQL was found to have the most vulnerabilities. The past three years saw quite a rapid growth in the number of vulnerabilities in MySQL and PostgreSQL.

5. According to statistics, among all attacks targeting web applications, those on frameworks, such as Struts and ThinkPHP, took up a whopping proportion of 54%, and those on plug-ins, such as ImageMgick, accounted for 39%. In contrast, attacks on specific CMS programs were seldom seen.

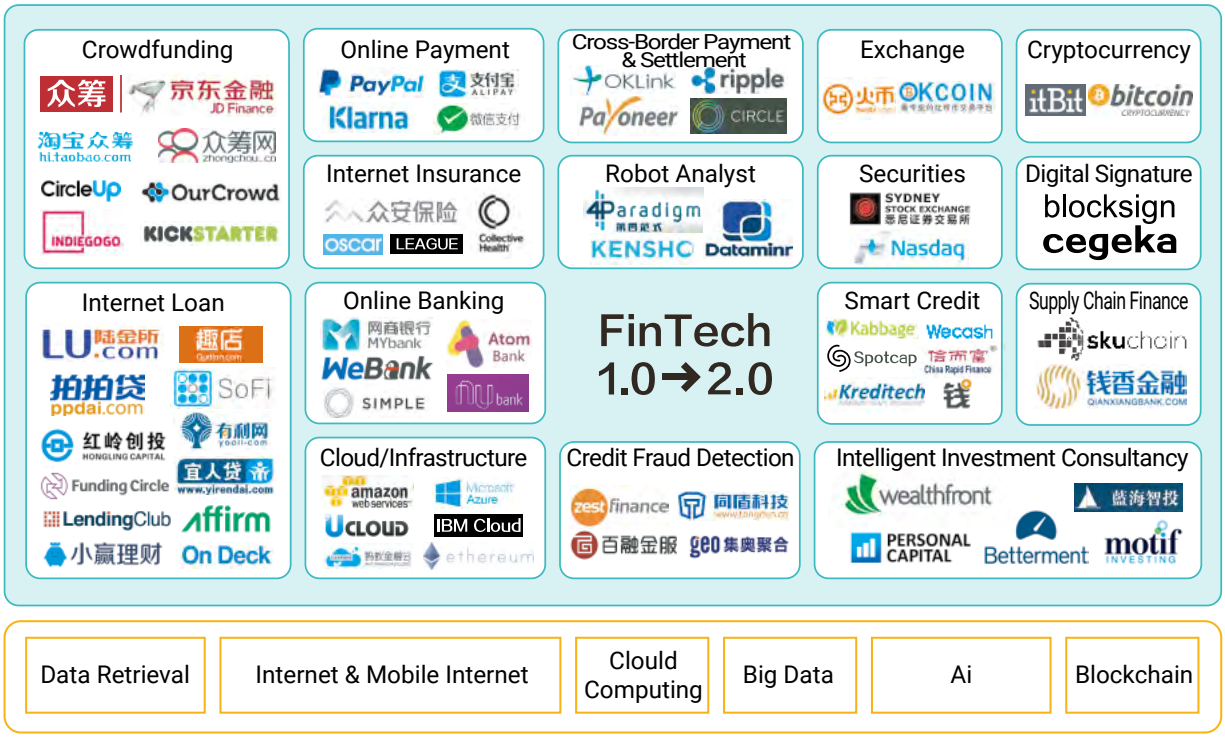
This report, based on related enterprise data, industry reports, and security analysis reports, analyzes the security status of the financial sector from the perspective of the Internet, with unique characteristics of the sector taken into account. In this report, we give a brief account of the development history and trend of Fintech, with a focus on typical cybersecurity threats, data security threats, and business security threats. By virtue of security cases and on the basis of the 2017 Questionnaire on the Security Status of China's Fintech Enterprises, we illustrate the current security posture of Fintech institutions and the security trend that they should be aware of. Financial organizations must attach great importance to security if they want to develop continuously and robustly. NSFOCUS and Ping An Financial Security Research Institute, as writers of this report, hope that this report can be informative for financial institutions and conducive to the healthy development of the financial sector in China.

2 Development of Fintech

Traditional financial activities are conducted around only savings, loans, and settlements. Obviously, conventional financial institutions are having difficulty coping with the fierce competition in today's market. The development of the Internet gives rise to Internet finance, where a financial institution sets up an online business platform to collect user information and handle transactions over the Internet. Traditional finance plus technology is version 1.0 of Fintech, which then evolves to the 2.0 version to emphasize services, in an attempt to push innovation in ways of offering financial services through changes in the underlying technology, to reshape the generation and pricing models of financial products, and to significantly improve the asset allocation efficiency. Typical applications of Fintech 2.0 include intelligent investment consultancy, intelligent credit, and supply chain finance. With the constant development of Fintech comes more and more security threats, and hence frequent security events that have caused huge losses and great negative impacts to the business. Fintech security will be a top concern in the era of Fintech 3.0.

Fintech covers a variety of fields and has a wide range of applications. Big data, artificial intelligence (AI), blockchain, and cloud computing, are core techniques of Fintech, making financial services more efficient and intelligent, as proved in many different scenarios.

Figure 2-1 Usage of Fintech[2]



Fintech, by nature, is innovative, which is beneficial to the industry, economy, and livelihood. But finance, lifted steadily by the technology, may crash and burn with a stronger, broader impact, and at a higher speed. Therefore, it is important to guide and regulate its development. A series of Fintech regulatory documents have been released around the world, including the USA, UK, and EU, to achieve balance between development and security. In China, the government has also accelerated setup of finance regulatory agencies and development of relevant laws and regulations. For example, the People's Bank of China has set up the FinTech Commission to strengthen research planning and overall coordination for Fintech. In other words, with an open attitude toward the development of Fintech, watchdogs from various countries are paying more and more attention to Fintech risks. It is projected that China's watchdogs will take more proactive supervisory measures.

2 *Financial Technology*, Zhou Wei, Zhan Jian, and Liang Guozhong, August 2017

3 Website Security Threats

The development of Fintech has become a major driver for the expansion of financial services. Unfortunately, it also exposes financial services to more threats. The *2017 Annual Cybercrime Report*[3] points out that "…cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind." According to this report, by the end of 2021, cybercrime damages will cost the world USD $6 trillion, up from USD $3 trillion in 2015. As we all know, finance is one of China's key sectors needing better cybersecurity. Owing to its unique nature, financial institutions are always the top target of cybercrime. In the following sections, we use several major security events affecting the financial sector in 2017 as examples to show how much damage and loss security threats can cause.

3.1 DDoS Attack

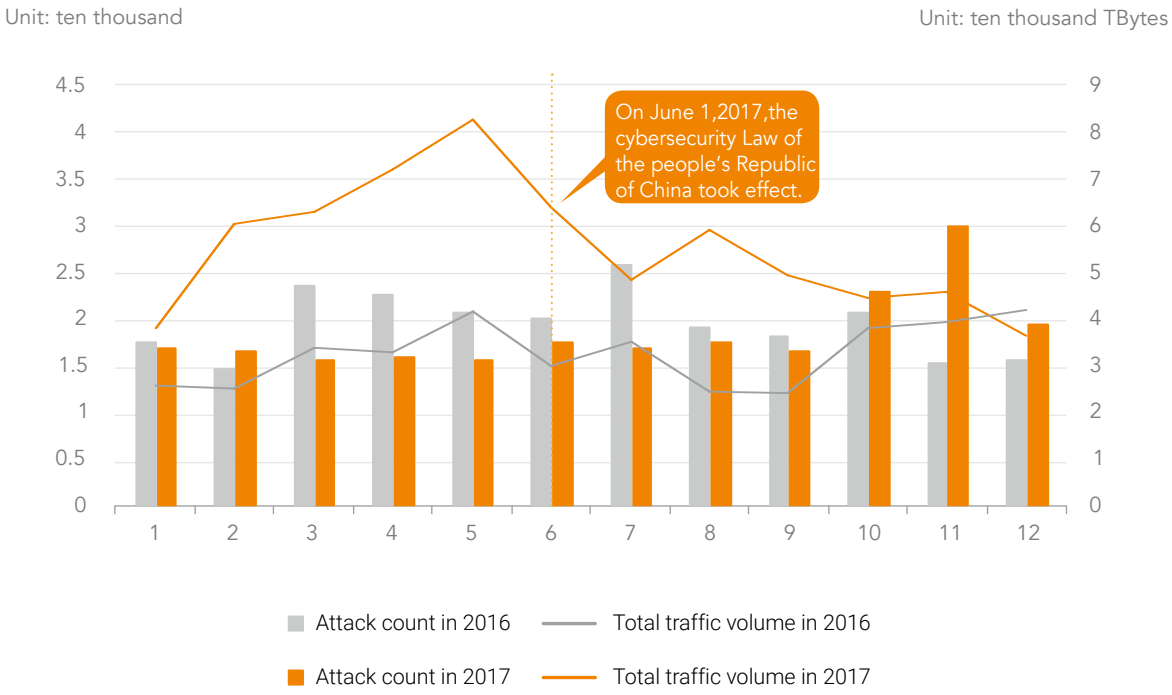
The distributed denial-of-service (DDoS) attack is a cyberattack that leverages the client/server architecture to turn many computers into an attack platform, making it possible for the attacker to flood one or more targets from many different sources. This will multiply the effect of DoS attacks.

Attacks Still Frequent, Totaling 207,000 a Year

In 2017, the total number of attacks reached 207,000, on a par with the previous year. The amount of traffic per attack, 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 amount of attack traffic increasing significantly.

3 Cybercrime damages are predicted to cost the world $6 trillion annually by 2021, PR Newswire, October 19, 2017.

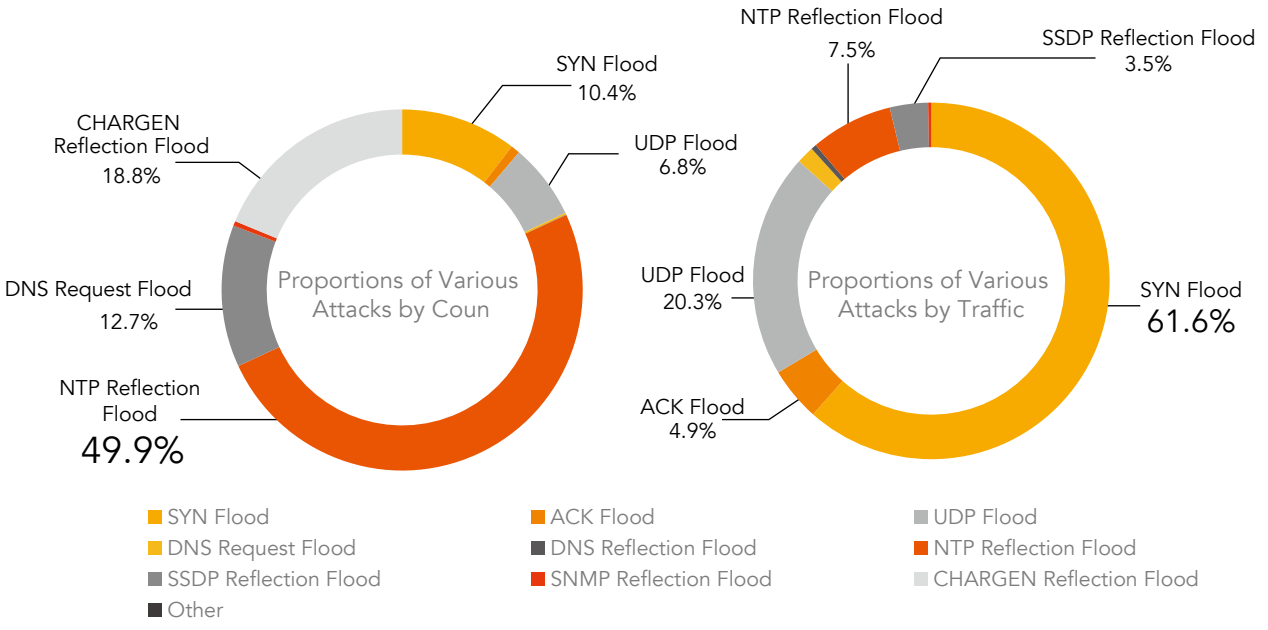
Figure 3-1 Monthly number and traffic of attacks in 2016 and 2017[4]



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

4 Figure 3-1 to Figure 3-5 and Figure 5-1 are sourced from the "2017 DDoS and Web Application Attack Situation Report", China Telecom YunDi Team and NSFOCUS (to be released).

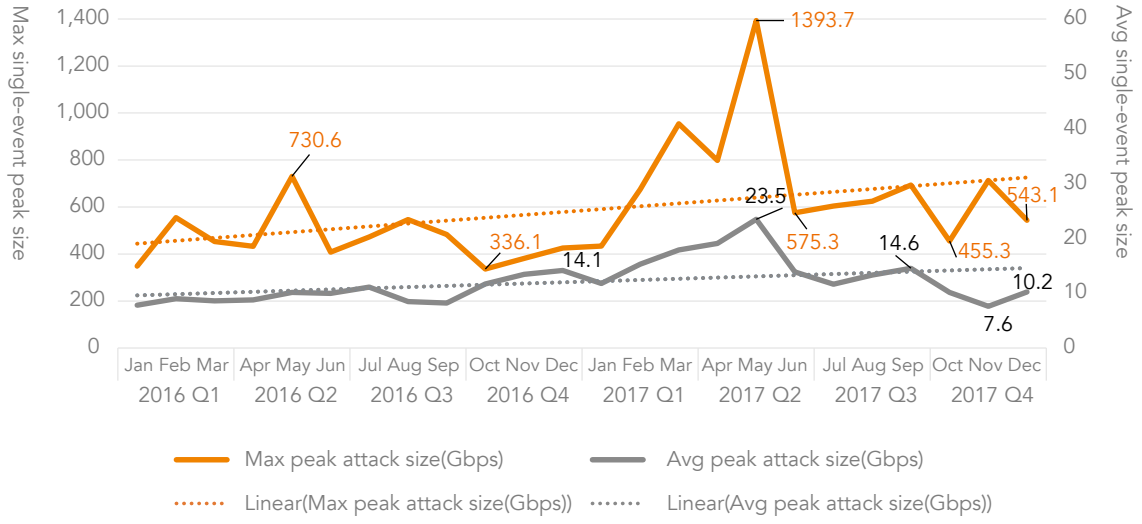
Figure 3-2 Distribution of various DDoS attacks



Traffic Hitting a Record High, Peaking at 1.4 Tbps

It is no surprise that attack traffic keeps growing. Reports from the past two years show that each month saw attacks with 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 keep challenging the protection capabilities of defenders.

Figure 3-3 Distribution of DDoS attack traffic

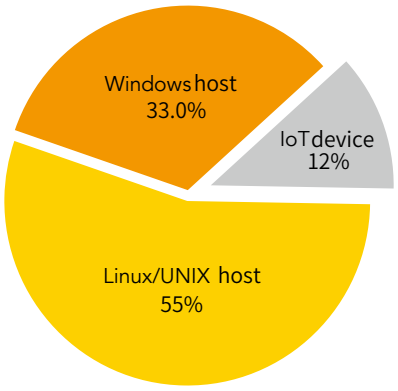


In addition, from the distribution of traffic, we see that voluminous attacks increased significantly. This was also an obvious trend in 2017.

Attacks from IoT Devices Accounting for 12%

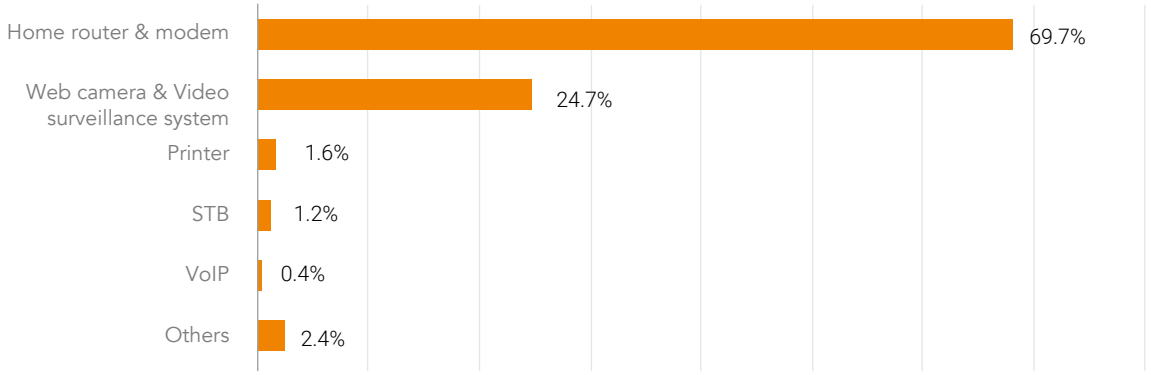
Of all DDoS attacks in 2017, whether they were large or small, the proportion of those originated from IoT devices was so large as not to be ignored. Arguably, IoT devices have become a category of attack sources calling for special attention. From the holistic point of view, the robust development of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

Figure 3-4 Types of devices used as DDoS attack sources



When we speak of IoT devices involved in DDoS attacks, routers and cameras are the major types of such 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 home environments, with no sufficient security measures deployed. We have every reason to believe that attacks leveraging the IoT will be in more diverse forms. According to statistics, IP cameras used maliciously accounted for about 4.8% of all IP cameras deployed, that is three times the proportion (1.57%) of all maliciously exploited IP addresses to the total IP addresses used in China. Therefore, special attention should be paid to cameras.

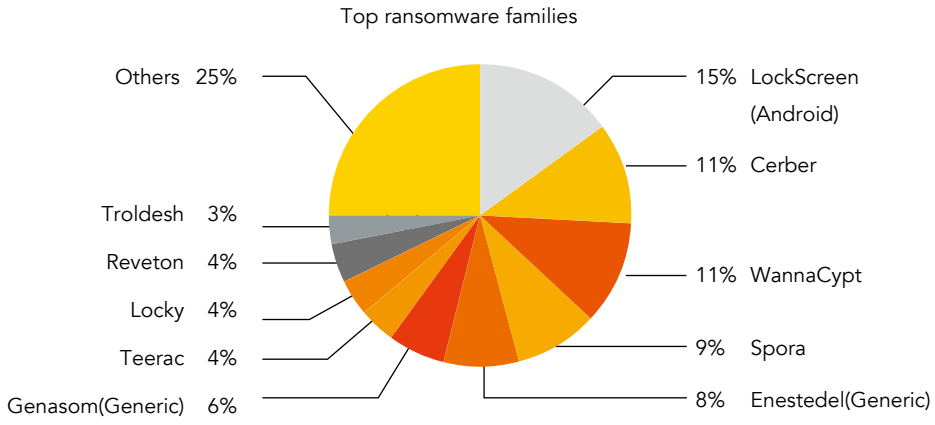
Figure 3-5 Types of IoT devices used as DDoS attack sources



3.2 Cyberextortion

Cyberextortion is a crime involving an attack or threat of attack against an enterprise, coupled with a demand for money to avert or stop the attack. In recent years, however, cybercriminals have developed ransomware that encrypts the victim's data. The attacker then demands ransom from the victim before offering the decryption key. In 2017, major ransomware such as LockScreen, Cerber, and WannaCrypt was responsible for the most attack events. WannaCrypt infections swept across the globe, subjecting nearly 100 countries to massive cyberattacks. For those attacks, the attacker, by exploiting the MS17-010 vulnerability, sent crafted packets to port 445 on users' machines, causing remote code execution. As a result, many files in the victims' computers were encrypted and the victims were asked to pay bitcoins for decryption of such files.

Figure 3-6 Most popular ransomware families in the first half of 2017 [5]



Top ransomware families and top 5 ransomware in top 5 countries,January to June 2017

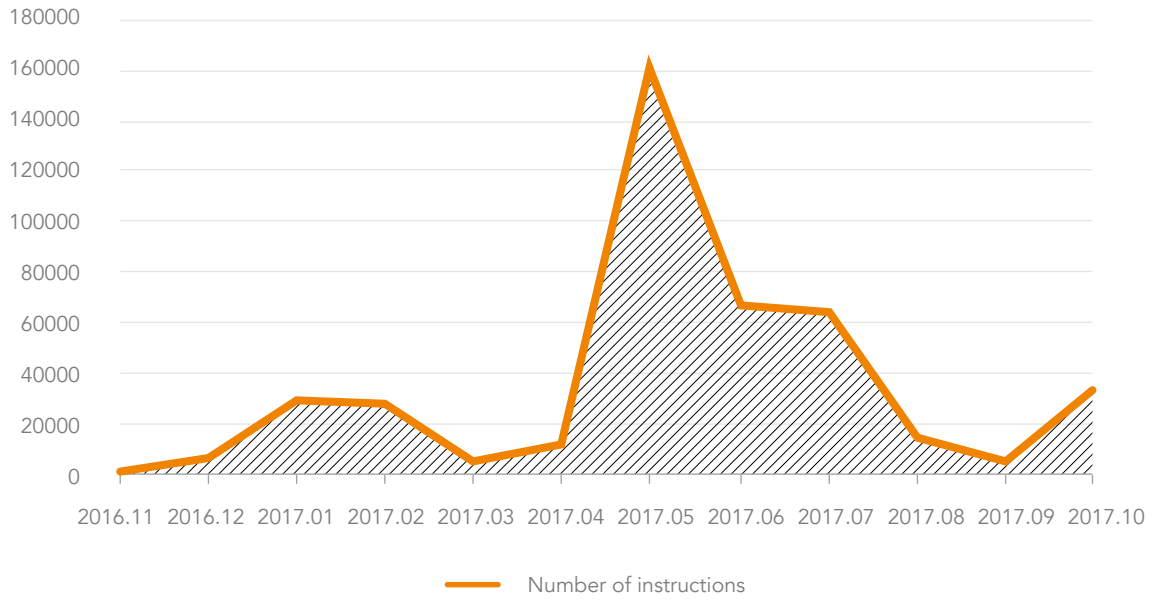
In June 2017, Anonymous and Armada Collective resurfaced again to direct a series of events against enterprises, including many financial institutions, sending ransom emails to ask for money. Anonymous launched a campaign coded "Opicarus2017" against over 140 financial institutions, including the People's Bank of China and Hong Kong Monetary Authority, demanding them to pay 10 Bitcoins (about RMB 530,000, USD $84K) as the protection fee. Nowadays, cyberextortion against Internet services has become a new trend of cyberattacks, with 4000 attacks a day on average.

3.3 Botnet

According to data obtained from NSFOCUS Threat Intelligence (NTI), botnets were still rather active in 2017, especially the second quarter which saw the most botnet activities. As for attack instructions, Command & Control (C&C) servers of botnets, in the most active period, issued 5187 instructions on average each day and a single C&C server even issued 114 instructions in a day.

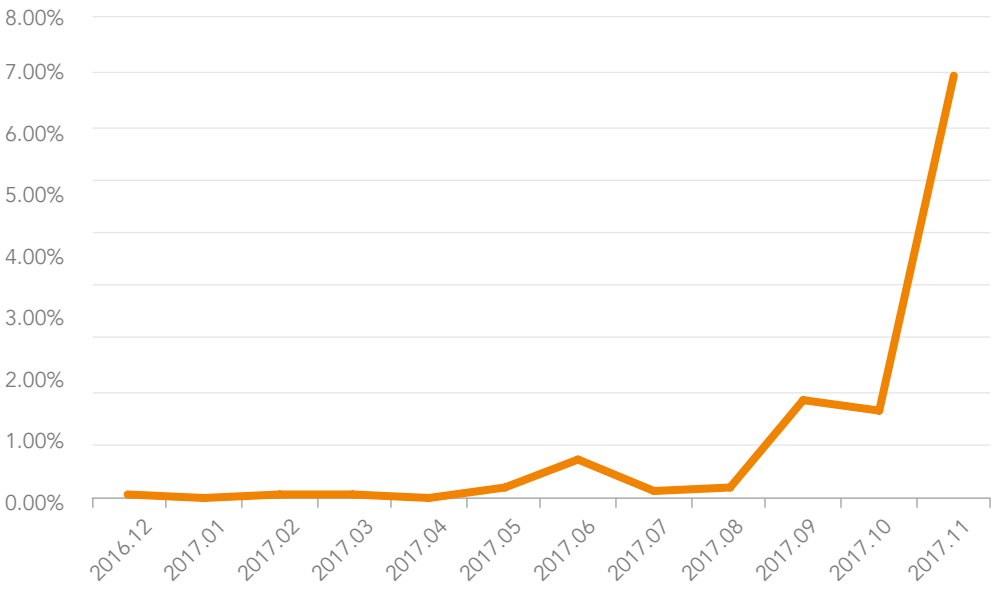
5 Ransomware FAQ, Microsoft.

Figure 3-7 Monthly number of attack instructions issued by C&C servers



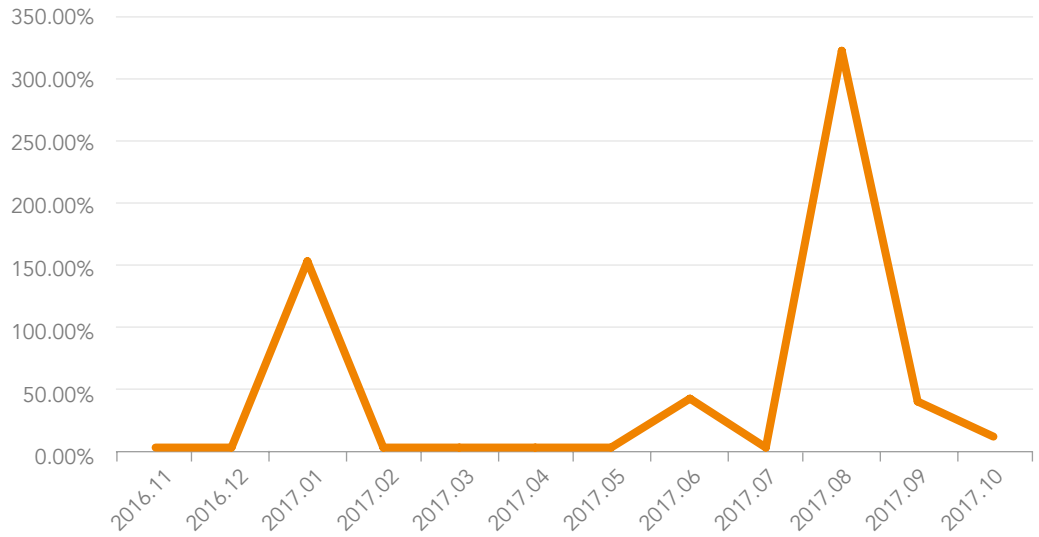
In 2017, botnets continued to grow in both quantity and scale. The number of C&C servers also steadily grew, which could be obviously felt in August, and the number further increased 1.67% in October from the previous month. At the same time, the global number of controlled hosts experienced an intermittent growth. In August, this number tripled (320%) compared with the previous month possibly due to the wide spread of WireX malware on Android devices[6].

Figure 3-8 Monthly growth rate of C&C servers



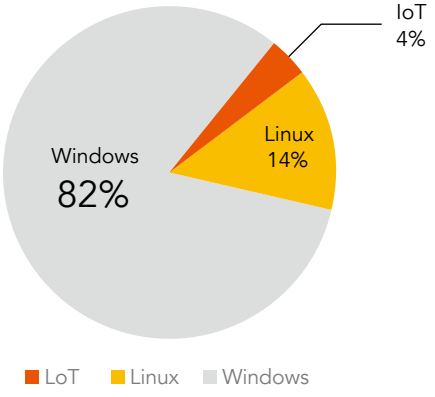
6 NSFOCUS Global IP Reputation Analysis Report Sept 2017

Figure 3-9 Monthly growth rate of controlled hosts



The power of IoT, smart, and mobile devices can now be felt in protection against botnet attacks. Among all botnets under our constant monitoring, at least 4% of the samples were IoT devices. It is true that 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, there will be an increasing number of malicious malware targeting IoT, smart, and mobile devices.

Figure 3-10 Distribution of botnets on different platforms



PCs can be compromised via emails, watering hole websites, or malicious code injected in software installation packages. For IoT devices, a simple scan is enough to enable hackers to capture a great number of vulnerable devices. The television set-top box (STB) worm detected by NTI in October 2017 and dubbed Rowdy was delivered over the Internet in China by exploiting vulnerabilities in STBs[7] . Moreover, NSFOCUS noticed some botnet families that target Android devices. Typical examples of such include Dendroid, FlexiSpy, and GMbot. Obviously, botnets, no matter which platform they are on, are a serious threat to the Internet.

7 Technical Analysis Report on Rowdy, a New Type of IoT Malware Exploiting STBs, NSFOCUS blog

As we mentioned earlier, attackers keep expanding the scale of botnets by compromising more and more devices making attacks more effective. Vulnerabilities in IoT devices make these devices ideal tools for DDoS attacks. However, avaricious hackers are far more ambitious than that. According to our observation, some botnets work across platforms. Characterized by self-replication, these botnets can also plant malware of the corresponding platform based on the device type infected to effectively take control of the devices, thus ensuring a more extensive impact. Following are some typical botnets with the cross-platform delivery capability.

Table 3-1 Botnet platforms

Botnet Family	Platform
Rowdy	Linux (x86/x86_64, ARM, ARM 4, ARM 7, MIPS, MPSL, and so on)
Mirai	Windows and Linux (ARM, EABI 4, MIPS, MIPS-I, PowerPC or Cisco 4500, Renesas SH, SPARC, and Intel 80386)
Gafgyt.bax	Linux (x86/x86_64, ARM, MIPS, PowerPC, SuperH, and Motorola 68000)
Darkshell	Windows and Linux (x86)
jRAT (remote control)	Relying on Java to spread across platforms, including Windows, Linux, macOS, and FreeBSD

From the programming languages of botnets, we can also see this cross-platform trend. C language and scripting languages have good cross-platform capabilities. Whether on an ARM embedded system or Linux or Windows, they can deliver good adaptability. Botnet malware developed in such a language is therefore able to run and spread across platforms.

Table 3-2 Programming languages of botnets

Botnet Family	Programming Language
Rowdy	C++
Gyddos	C++
LuaBot	Lua
Aldi_bot	Delphi
yi2.0	E language

Besides, scripting languages are easy to learn and use. A new botnet program can be written with this language quite efficiently. Easy to construct and promising to make quick money, botnets are attracting more and more hackers, posing an increasing big threat to the network. In September 2017, numerous websites found their web pages containing JavaScript code for mining Bitcoins. Once a user visits such a website, the JavaScript code will automatically run to mine cryptocurrency by using large quantities of resources on the user's computer, causing it to stop responding[8] . In fact, crypto-miners are the next up and coming botnet programs.

2017 is a year witnessing the widespread infection of botnet programs, including several large-scale crypto-miner botnets/malware such as Bondnet, Adylkuzz, and EvilJS. Among all crypto- miner botnets, quite a large proportion is from China. Finance, telecom, and Internet are among the sectors suffering related security events. At the end of December 2017, a security firm warned that "the famous news activation tool KMSpico containing mining malware". NSFOCUS experts analyzed and found that the original version of the tool did not contain any

8 "2017 Annual Internet Security Report", Tencent PC Manager, January 17, 2018.

miner malware. As a matter of fact, the hacker leverages search engine rankings to craft web pages that look exactly like those of KMSpico, and then plants various malicious programs, including miners, into these pages to entice users to download. Once users download such programs, the hacker can steal their privacy or use their computer resources to mine cryptocurrency for monetary gains[9] .

3.4 APT Attacks

An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by one or more persons targeting a specific entity. An APT usually targets either a specific organization or country for business or political motives. APT processes require a high degree of covertness over a long period of time.

Previous monitoring shows that most APT attacks, including Stuxnet attacks against Iran and attacks against Belarus's Military News Agency, are intended to meet political demands. Over time, the APT concept and related techniques become well known to the cybersecurity industry, and therefore confrontation at various levels grows increasingly complex. The exposure of the hacking arsenal of the United States National Security Agency (NSA) and the Center for Cyber Intelligence (CCI) under Central Intelligence Agency (CIA) by the Equation Group in 2017 provides a great number of weapons for the entire underground industry chain, making it possible for more organizations and individuals to launch advanced attacks with more mature techniques. Compared with common attack means, APT attacks are more difficult to perform and cost more. Apart from state-sponsored attacks among governments, most APT attacks, driven by great benefits, set sights on the financial sector. In 2017, NSFOCUS discovered a typical APT attack against new services in the financial sector, in which the overseas attack organization APT-C1 uses the "Internet finance thief" malware to hit an Internet finance platform in China, stealing digital assets of this platform.

Like other industries, the financial sector is also undergoing technical innovations and upgrade which bring more convenience as well as more potential risks. However, the financial sector has assets of more direct value than other industries. Therefore, the financial sector needs to maintain high vigilance against APT risks.

9 Activation Tool KMSpico Contains Miner Virus, NSFOCUS Blog.

4 Data Security Threats

In recent years, massive data breach events have skyrocketed, with the number of large scale breaches in the first 11 months of 2017 going up by 10%[10] over the entirety of 2016. In September, Equifax, a renowned US credit reporting agency, revealed that it was hit by a hacker and information of 143 million users was leaked[11] . In November, Uber, a technology & transportation company, found that it suffered a massive data breach event in 2016 in which information of 57 million passengers and drivers was stolen by hackers. In addition to government agencies and financial institutions, data breach attacks are also extending the reach to third-party contractors, data integrators, security vendors, and solution providers. Going forward, more and more enterprises and individuals will be at risk of data breach.

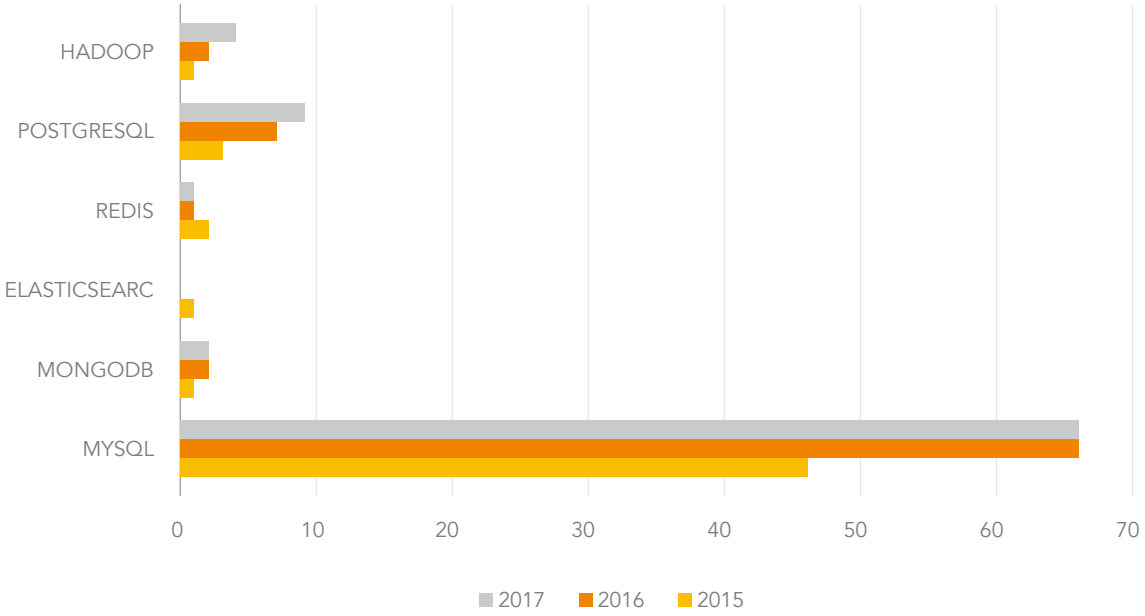
10 "The 10 Biggest Data Breaches Of 2017, CRN, December 2017".
11 "An Offensive Defense: Lessons from the Equifax Breach"

4.1 Database Vulnerability Exploitation

Many databases have read-only interfaces directly exposed to the Internet while not having complete access control policies. Anyone can take control of such a database usually with weak or empty password. A database ransom attack is implemented by taking control of a database by hacking means to encrypt or damage data for the purpose of demanding ransoms from victims.

Database security became a topical security issue in 2017. The following figure shows statistics of high and medium-risk vulnerabilities in attacked databases in 2015, 2016, and 2017.

Figure 4-1 Statistics of high and medium-risk vulnerabilities



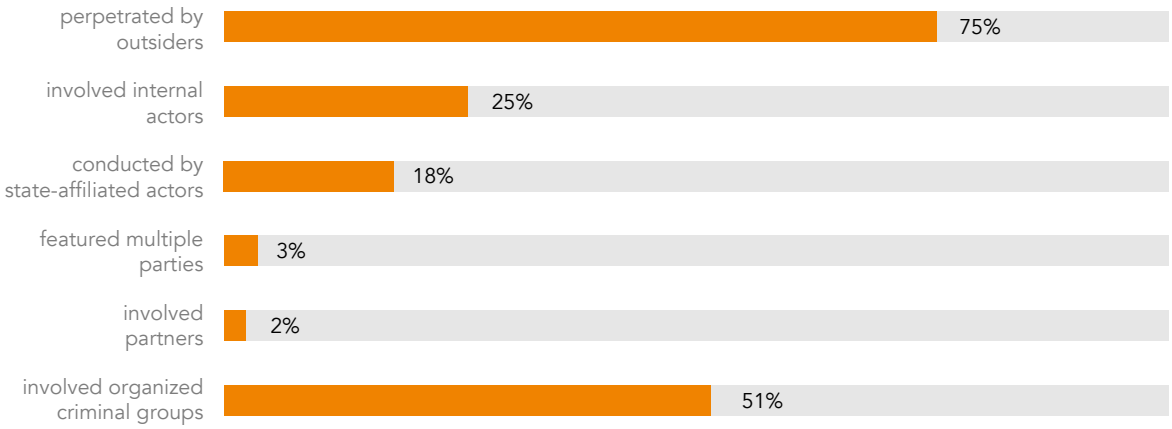
As shown in the preceding figure, MySQL has most vulnerabilities exposed over the past three years and apart from MySQL, PostgreSQL has also registered a rapid increase in vulnerabilities. In contrast, MongoDB, Elasticsearch, Redis, and Hadoop are more secure, despite a moderate increase in vulnerabilities.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

4.2 Data Sale by Insiders

The report[12] jointly released by Identity Theft Resource Center and CyberScout estimated that the number of data breaches could reach 1500 in 2017, up 37% from 1093 in 2016. A security survey report[13] released by Loudhouse reveals that 35% of employees will sell sensitive data, such as company patents, financial records, and customer credit card details, if the price is right.

In June 2017, Verizon confirmed a leak of data of 6 million users and said that the leak was caused by an employee of one of the company's vendors who accidentally allowed external access to information put in a cloud storage area. In the same year, Verizon released a data breach survey report which claims that 25% of data breach events were caused by insiders. Therefore, the financial sector, as easy targets for information leak events, should improve security measures to protect sensitive information, enhance internal security management, and set up necessary constraint and control mechanisms.

Figure 4-2 Data breach causes [14]



12 "At Mid-Year, U.S. Data Breaches Increase at Record Pace", CyberScout, July 18, 2017
13 What's your employees' price?", clearswift.
14 "Mitigate the cyber risks with the Verizon 2017 Data Breach Investigations Report.", Verizon.

4.3 Cloud Data Theft

It is estimated that the private cloud market in China has reached approximately RMB 42.5 billion in 2017 and will hit RMB 76.24[15] billion in 2020. Our questionnaire-based survey revealed that 60% of Chinese financial institutions have introduced various cloud services, of which most deploy private clouds and over 20% use public clouds or hybrid clouds. What the financial sector cares most about is data and privacy protection and business access control after cloud services are deployed.

Figure 4-3 Proportions of enterprises adopting cloud computing services

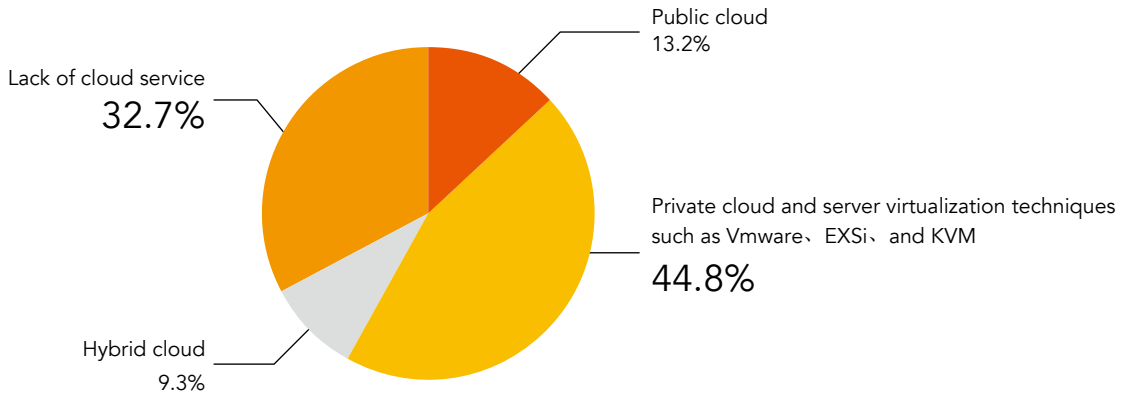
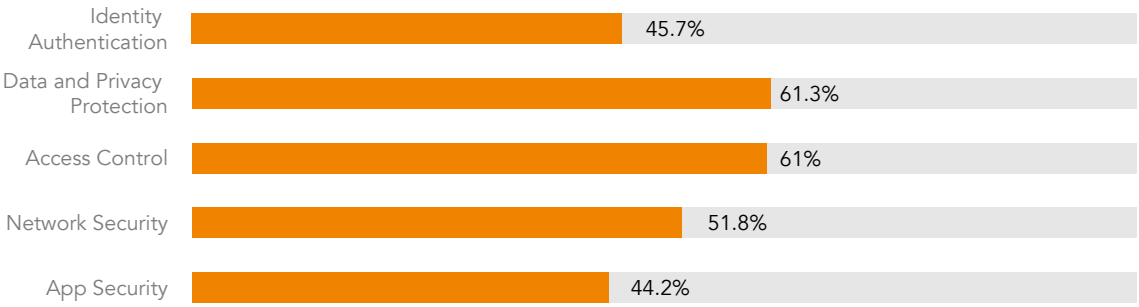


Figure 4-4 Security risks facing cloud computing services



Personal data and privacy protection is not only security requirements of enterprises, but also an increasingly major concern of state regulators. For example, the European Union (EU) has issued the General Data Protection Regulation which shall come into effect from May 25, 2018. This regulation states that EU shall enhance privacy protection for all individuals, put more efforts for privacy protection in the Internet of Things (IoT), and streamline data protection management. Recently, China has issued the *Cybersecurity Law of the People's Republic of China* and is developing the *Personal Information Protection Act*, both of which reflect state regulators' emphasis on data and privacy protection.

15 "*Analysis on Current Situation and Development Trend of China's Private Cloud Market Over 2018-2024*", Zhiyan Consulting Group, November 2017

5 Business Security Threats

Business security threats arise from several factors such as use of insecure functions or protocols, integration of a defective software development kit, web plug-in, and server utility, or logical flaws in the business process.

According to statistics of this questionnaire, Fintech has been largely incorporated into the Internet. 83.5% of institutions or enterprises provide services over the Internet. When it comes to security risks, financial enterprises and institutions pay close attention to the following aspects:

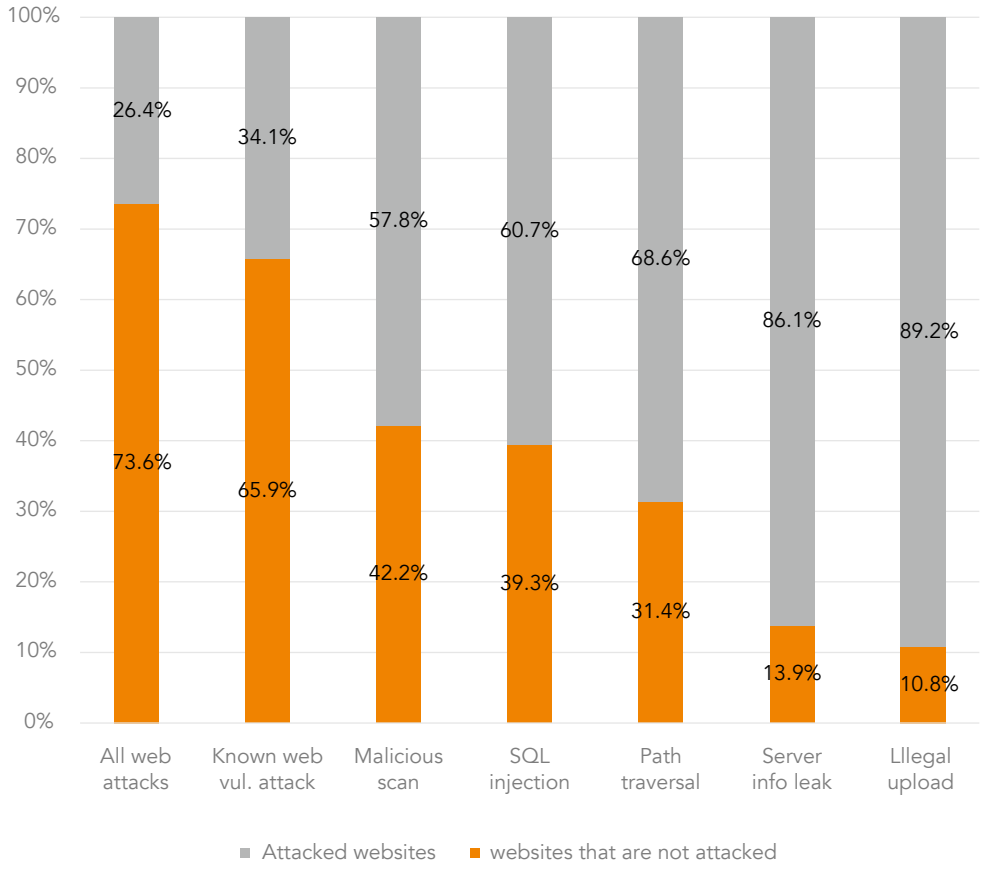
- Whether their assets contain vulnerabilities.
- Whether their proprietary assets have high-risk ports and services opened.
- Whether information leak risks exist.

By reference to the business development of the financial sector, this chapter introduces web attacks, threats faced by banks' ATMs and SWIFT systems, financial fraud threats, mobile payment threats, and blockchain security threats.

5.1 Web Attacks and Code Defects

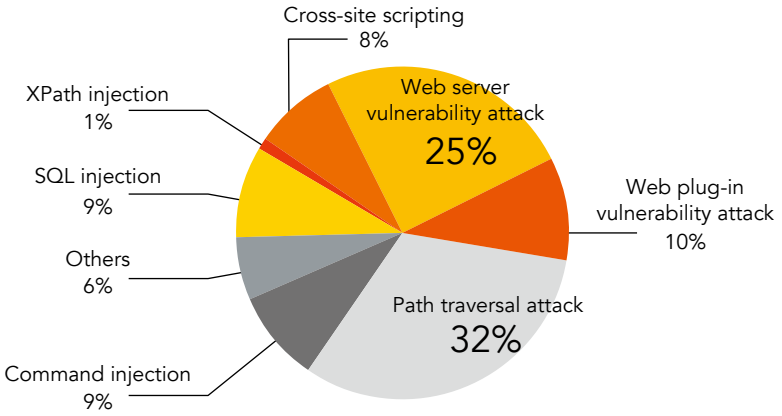
Web attacks are a common type of attacks. According to NSFOCUS's protection statistics, 73.6% of websites suffered web attacks of different sizes and 65.9% were hit by attacks that are based on vulnerabilities of a specific program.

Figure 5-1 Percentage of different types of web attacks



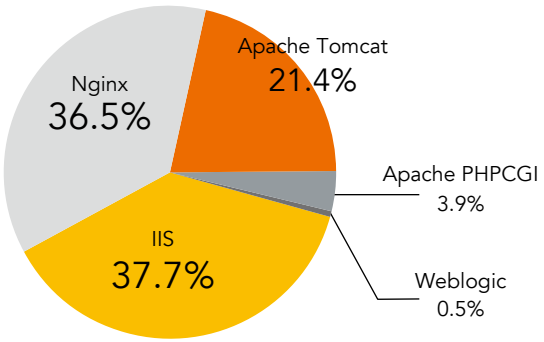
Of attacks against web servers in the financial sector, common attacks such as SQL injection, XPath injection, cross-site attacks, path traversal, and command injection account for more than 60%. Web attacks have become a basic attack means and are easier to implement compared with other attacks. In addition, attacks against specific web plug-ins and server programs make up a relatively high percentage. In view of this, enterprises should regularly conduct system maintenance and upgrade related server applications.

Figure 5-2 Classification of web attacks



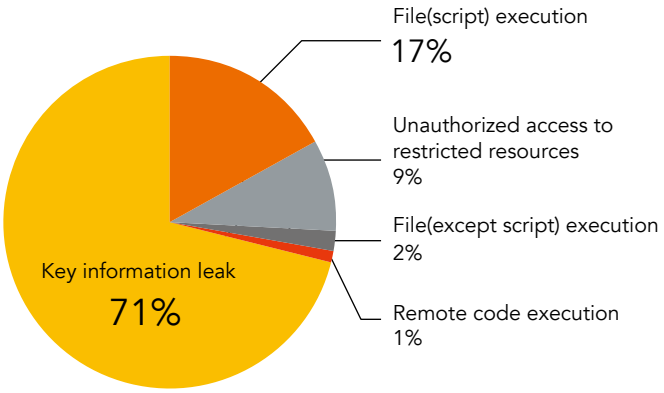
In terms of the server type, nginx, IIS, and Tomcat servers used in the financial sector were most severely attacked. Enterprises using such servers should deploy comprehensive protection measures.

Figure 5-3 Distribution of web attacks by server type



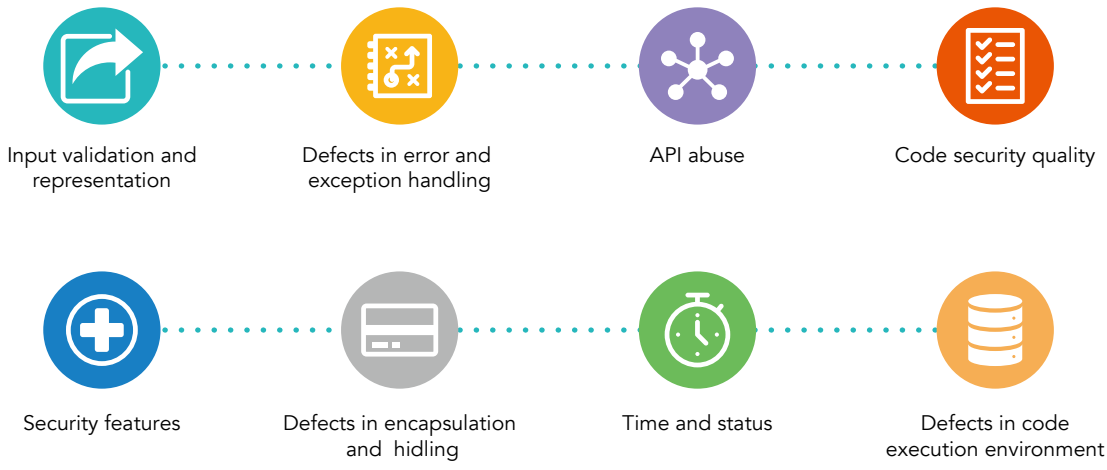
Generally, attacks against server systems in the financial sector are launched by exploiting key information (such as the storage location of files in a disk of the server and system version) leak vulnerabilities. Those vulnerabilities are caused by improper server software configurations which provide various data required for further intrusions. In addition, file execution vulnerabilities caused by improper file type filtering are a common type of vulnerabilities. Such vulnerabilities can lead to more serious damage by allowing hackers to obtain a high-privilege webshell for privilege escalation.

Figure 5-4 Distribution of vulnerabilities in web servers that are most frequently exploited



Defects in code are the major cause of the year-on-year increase of web attacks. According to the official description of Fortify, code defects are divided into the following categories in terms of the defect cause, exploitation possibility, and security issues.

Figure 5-5 Classification of common code defects



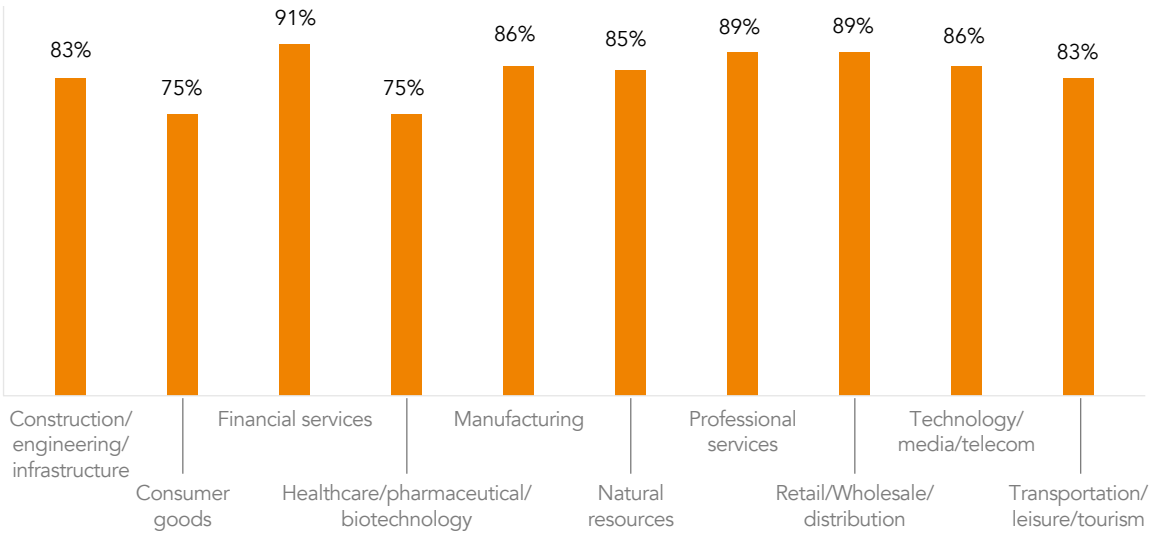
The survey shows that only 32.9% of organizations employ Security Development Lifecycle (SDL) management during information system development for the financial sector. Also, these organizations are found to devote most security management efforts to the operations and maintenance, go-live, and testing phases, without security considerations in the requirement, design, and encoding phases.

5.2 Business Fraud

With rapid development of consumer finance, all financial institutions face a serious issue—fraud. According to the *Global Fraud & Risk Report* [16] (*10th Annual Edition 2017/18*), 86% of interviewed enterprises in China said that they suffered fraud in 2017. This figure is a little higher than the global average, 84%.

The China Finance Anti-Fraud Technique Application Report [17] notes that compared with the same period of 2016, rejected transactions in the financial sector went up 40% and botnet attacks increased by 180% in the first quarter of 2017. It is expected that online payment fraud events will incur an economic loss of $25.6 billion in 2020 and data breach events will result in a global economic loss up to $2.1 trillion in 2019. Financial frauds feature mobility, a high degree of concealment, and increasing systematization. Such illegal activities can be conducted via various means to target various business phases. New Fintech firms are becoming new favorites of fraudsters.

Figure 5-6 Distribution of fraud events by industry[18]



5.3 ATM Attacks and SWIFT Attacks

In 2017, there emerged a new form of cyberattacks against ATMs of banks, that is, malicious attack began to be launched with infrared plug-in card slot holders. It is reported that plug-in card slot holders are a kind of ultrathin mini devices using short-distance infrared communication techniques. Such a device, featuring a simple structure, is hidden in a slot of an ATM to capture data concerning private credit cards and debit cards and store it in an embedded flash memory before transmitting it, via an antenna, to a mini camera hidden outside the ATM. There is a high possibility that such collected bank card data is used to forge credit cards or debit cards in order to steal users' money.

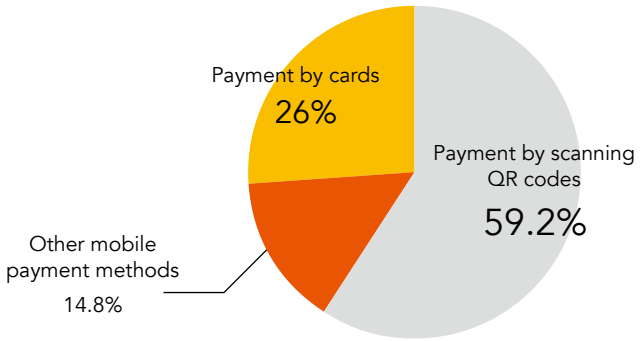
16 "Global Fraud & Risk Report", Kroll.
17 "China Finance Anti-Fraud Technique Application Report", Zero One Think-Tank, Maxent, August 2017
18 See 16th footnote

In October 2017, Taiwan Far East Bank lost $60 million in the wake of an SWIFT event, which was finally reduced to $500,000 after the police recovered most of the money. However, NIC Asia Bank was not so lucky as a similar SWIFT event in the same period incurred a loss of $5 million to it. This is not the first time that banking institutions are hit by hackers, so we can infer that banking institutions do not pay so much attention to those recurring security events as to deploy effective security measures. In view of this, we can see that information security management is not a matter of luck and the right way to lower risks is building a sound security management system and setting up an experienced security team.

5.4 Security of Mobile Payment

The *2017 Mobile Payment User Survey Report* [19] indicates that 59.0% of users are worried about mobile payment security. Also, this report reveals that 77.1% and 70.2% of users respectively regard personal privacy leaks and security risks as prime concerns when using biometrics for identity authentication of mobile payment and transaction verification.

Figure 5-7 Payment methods [20]



The *2017 Mobile Internet Payment Security Survey Report* points out that mobile payment users have the following major risky behaviors:

- Scan QR code casually.
- Fail to cancel the binding of bank cards when uninstalling mobile apps.
- Fill out real payment information.
- Click links included in SMS and emails without thinking twice.
- Install unknown executables that appear unexpectedly.

This report also indicates that more than 60% of respondents have insecure behaviors which may pose security threats to personal information or payment accounts. For these reasons, mobile payment users should be on high alert to guard against various payment risks at all times.

19 "2017 Mobile Payment User Survey Report", Payment & Clearing Association of China, January 2, 2018.
20 "2017 Mobile Internet Payment Security Survey Report", China UnionPay, January 17, 2018.

5.5 Blockchain Security

A blockchain is a distributed ledger system that records online transactions. This open technology overcomes time and space limitations in traditional transactions by allowing transactions to be dealt with anytime, anywhere. Therefore, it is believed that the blockchain technology has a bright future in a variety of fields such as finance, credit checking, IoT, economic and trade settlements, and asset management. As the blockchain technology is included by the State Council in China's 13th Five-Year Plan[21] in 2017, the market capitalization of China's crypto currencies has increased by 30 times.

The *Distributed Ledger Technology & Cybersecurity* report analyzes the blockchain technology and its challenges such as key management, privacy, and smart contract. This report points out that though this technology follows the same security principles as traditional systems, it still presents new challenges such as consensus hijacking and smart contract management.

While the blockchain technology has constantly been studied and applied, it is threatened by security risks in technical and application aspects. Security awareness and defense measures should be improved to protect consensus mechanisms and prevent private key theft. In February 2018, 132 investors filed a lawsuit against Japan’s cryptocurrency exchange Coincheck, demanding a compensation of 228 million Yen (about 2 million US dollars) as this exchange's $525 million worth of NEM coins was stolen, following a major hacking attack against it in late January. Some investors believe that this attack event is due to the exchange’s negligence in security measures [22].

21 "What’s the future of blockchain in China?", World Economic Forum, January 1, 2018.
22 132 investors filed a lawsuit against Japan’s cryptocurrency exchange Coincheck, demanding a compensation of 4 million dollars, Leiphone net, March 2, 2018.

6 Conclusion and Outlook

6.1 Conclusion

Fintech is an innovative finance business model in which scientific forces significantly promote development of financial business, increasing its inclusiveness, convenience, differentiation, and flexibility. Looking back on the human history, scientific technologies are a double-edged sword which brings both innovation and destruction. Special sectors like finance must be on high alert to guard against security risks at any time. At the National Finance Work Conference held in 2017, president Xi Jinping particularly stressed that risk aversion and control is a top priority of the financial sector. Therefore, institutions adopting the innovative Fintech model must attach great importance to security risks that are inherent in financial techniques and brought by their applications.

Based on latest cases and ample sources of intelligence, this report analyzes the present situation and trend of security threats faced by Fintech from aspects of network, data, and business. Apart from analysis of traditional threats brought by DDoS, web attacks, and database vulnerability exploits, this report highlights security threats posed by new techniques such as mobile Internet, cloud computing, and blockchain. Through analysis, we conclude that to maintain a sustained and sound development, Fintech firms should take security issues seriously and increase the overall security capability from aspects of security awareness education, security devices and services, security talents and security budget.

6.2 Outlook

As indicated at the National Finance Work Conference held in 2017, all financial services should be brought into regulation. Therefore, financial institutions must strictly follow national regulation requirements of Fintech development and application, instead of merely pursuing innovations. As mentioned above, Fintech faces both traditional and emerging cybersecurity threats. Considering the range and extent of damage resulting from these risks and the status quo of response and protection of financial institutions, we suggest that financial institutions should pay attention to the following aspects:

- **New regulation and compliance requirements**

  Measure the existing risk control capability to determine which risks can be prevented and which are beyond control.

- **Employee security training**

  Increase the security awareness of employees, develop a more comprehensive security specification, and conduct training on awareness and skills concerning security deployment and management

- **Risks arising from introduction of new techniques**

  Deal with security risks brought by IoT, blockchain, and mobile payment.

- **Development security management**

  Systematically identify and eliminate information security risks arising from insufficient knowledge and skills of staff, development environments, and business logic.

- **High-risk cyber attacks**

  Deal with potential security threats such as DDoS attacks, web attacks, organized APT attacks, fraud, and ransomware attacks.

- **Data security**

  Strictly follow both domestic and overseas data and privacy security regulations, enhance enterprise data protection, and prevent data sale risks.