2016

China Internet Security Report

February 7, 2017

Abstract

Personal Security

- In 2016, 360 Internet Security Center intercepted a total of 190 million new malware samples on PCs. Racketeer virus went viral twice in China, attacking at least 4.97 million user computers nationwide. A survey reveals that 42.6% of the victims were unaware of the causes of the infections. In 2017 the number of infections is expected to grow 10 times, and attacks using embedded Trojan will break out again.
- In 2016, 360 Internet Security Center intercepted a total of 14,033,000 new malware samples on the Android platform, with tariff-consuming programs taking up 74.2%. Just like PCs, ransomware started to break out on mobile phones. Throughout the year, 360 intercepted 170,000 new ransomware samples on mobile phones, attacking 1.70 million mobile phones.
- In 2016, 360 Internet Security Center intercepted a total of 1969,000 new phishing sites, and 27.95 billion phishing attacks. Among the new phishing sites, 19.0% were built after websites were hacked.
- In 2016, 360 Internet Security Center intercepted a total of 38.51 billion crank calls, mainly including advertising and telemarketing scams. Phone scams took up 56.7%, mainly from real estate and wealth management institutions. People harassed were mainly from developed regions like Guangdong, Beijing and Shanghai.
- Advertising took up the largest percentage among phone scams on fixed telephones, while real estate agencies accounted for the largest percentage among phone scams on mobile phones. Phone numbers and times of interceptions suggest that most crank calls were dialed with a handful of numbers. 0.4% of frequently intercepted numbers (intercepted more than 30,000 times) took up 31.5% in the total number of interceptions. Crank calls were made not merely during the day; from 20:00 to 24:00, 55.8% of users were harassed, and even 29.8% were harassed from 0:00 to 6:00.
- Telemarketing scams are an important type of crank calls; financial planning and impersonation are the most common types of fraud, and they are also easiest to cause victims heavy losses. The success rate of telemarketing scams is about 0.1%, with the figure for those made with mobile phones being the highest, 0.28%. 66.8% of scam calls are made with long-distance calls. The lifecycle of telemarketing scams averages 57.6 days, and the cycle of continuous activeness is some 7.6 days.
- In 2016, 360 Internet Security Center intercepted a total of approximately 17.35 billion spam messages, with numbers starting with 106 accounting for 70.0%. Commercial promotion SMS took up 92.2%, followed by 4.2% of illegal SMS, and there were 2.8% typical SMS scams. An in-depth analysis of the content of SMS scams tells us that most are impersonation-type fraud, and the swindlers mainly impersonate banks, e-commerce stores and telecom operators.
- Among spam messages sent using pseudo base-stations, advertising messages took up 41.3%,

illegal messages 33.8%, and SMS scams 24.0%. It can be seen that pseudo base-stations have become a technical tool for crimes. In particular, with SMS scams, many messages sent via pseudo base-stations pretend to be sent by service numbers of banks or telecom operators.

- 99.99% of current Android phones have security vulnerabilities. By comparing the update status of users' mobile phone systems, Android's official update status and mobile phone makers' update status, we find that it is mobile phone makers generally unable to update their custom Android system in sync with Android's official version that leads to customers' delay in updating their mobile phones.

- In 2016, 110.360.cn received a total of 20,623 tip-offs against Internet fraud filed by users around China, involving a total amount of more than RMB195 million, which translated into a loss of RMB9,471 per victim. Fraud part-time jobs are the most frequently tipped off form of fraud, while financial planning is the type of fraud that involves the largest amount of money. 56.0% of victims voluntarily transferred money to swindlers. Those born in the '90s constituted the largest group of victims. The number of victims declined as age grows, but the amounts of money tricked went up.

- Smartcams are used widely. Due to the great gap among participants in the industry, smartcams entail a lot of security risks, mainly including: disclosure of user privacy, unencrypted transmission, lack of man-machine recognition mechanism, lateral control of most smart devices, lack of, hardening at the client side, code flaws, opened hardware debugging interfaces, lack of programs launching protection, and lack of remote update mechanism.

- Drawing upon its years' experience in Internet security and automobile security research, as well as the security conditions of the automobile company, 360 compiled a best practice guide fit for information security development at domestic automakers with reference to the *Modern Automotive Information Security Best Practices of the US Department of Transportation*, elaborating on lifecycle security methods, to guide enterprises to effectively carry out information security ecosystem construction.

Enterprise Security

- In 2016, webscan.360.cn detected a total of 917,000 websites with vulnerabilities; 140,000 of them had high-risk vulnerabilities, taking up 7.1% in the total number of websites scanned. loudong.360.cn included 37,188 vulnerabilities, involving 30,329 websites, with high-risk vulnerabilities accounting for 50.6%. According to a sampling survey on website vulnerabilities put on the record, the average repair rate of vulnerabilities is only 42.9%.

- wangzhan.360.cn intercepted a total of 1.71 billion website vulnerabilities attacks, on average 5,344,000 attacks per day. 66.9% of victims' IP addresses come from Mainland China, mainly Beijing, Zhejiang and Sichuan. Attackers' IP addresses are also mainly from the mainland, mainly Jiangsu, Beijing and Henan.

- In May 2016, 360 Internet Security Center conducted data analysis of 2015 DDoS attacks. It was found the Internet around the world suffered 27,489,410 DDoS attacks; as many as

776,095 websites were attacked. Sampling analysis of traffic over one month shows that nearly one fourth (23%) of websites are unable to escape from the lethal impact of DDoS attacks, and they stand little chances of revival.

- DDoS attacks are launched mainly by controlled botnets. Around the world excluding China, Venezuela and the U.S. are the primary sources of botnet attacks. In China, attacks come largely from Guangdong, Zhejiang and Henan.
- In 2016, 360 Threat Intelligence Center detected 5.12 million scanning source IP addresses worldwide, and detected a cumulative of 164 million scanning events. For network scanning against China, the scanning source IP addresses were mainly from the U.S., Russia and Brazil. The three most scanned IP ports were #23, #2323 and #1433. Scanning of the IoT devices is a type of new scanning that rose rapidly in 2016 and has gone rampant. The most typical case is the infamous Mirai, which was responsible for both the Dyn DNS outage in both the U.S. and Germany.
- On average, an enterprise user in China receives more than 20 million spam mails per day, taking up 69.8% in the total number of mails received by it. On average, domestic businesses encounter some 10,000 suspected mailbox theft attacks every day. After a mailbox is stolen, abnormal occurrences follow, like tampered password, sending outbound spam mails, and sending fraud mails inside. Use of weak passwords by users is the primary reason of mailbox theft.
- To enterprise users, internal phishing mails are the most dangerous phishing mails. Attackers pose as system administrators to send mails, and trick enterprise users to log on phishing sites on the ground of mailbox upgrade and email outage, thereby swindling information of enterprise staff like accounts, passwords, names and positions.
- Not all network attacks are perceived by enterprises themselves. In 2016, among the more than 500 network security emergency response incidents that 360Cert took part in handling, only 4.7% of attacks were discovered by the enterprises through in-house security inspection; 26.8% were spotted by the enterprises only after significant intrusions or economic losses occurred; 68.5% of attacks were not perceived by the enterprises themselves, and they did not find out they had been attacked until they were informed by the regulators or competent authorities, or they saw media coverage.
- In 2016, 360 Threat Intelligence Center detected 36 domestic and overseas APT organizations launching attacks on targets located in China. There are nearly 200 domestic organizations that are targets of suspected APT attacks. Colleges and universities take up the largest percentage, 40.0%, followed by enterprises (25.0%), governments and non-profit institutions (18.3%).
- APT attacks' impacts are most noteworthy in three fields: destruction of industrial systems, crimes in financial systems, and geopolitical impacts. In the next few years, APT attacks will show the following four trends: cyberspace will become a new battlefield for the world's big powers, destructive attacks on infrastructure will become increasingly active, there will be a remarkable increase in attacks on particular individuals' mobile devices, and Belt & Road and military-civilian integration will be the focus of attacks.

- Given the current APT monitoring and defense technology system, there are still many blind zones in enterprises' network security construction. Meanwhile, capability security vendors are still severely in short supply in China. Data-driven, coordinated in-depth defense system will become the main method of APT detection and defense in the future.
- Industrial Internet security involves three domains: industrial control, Internet and information security. We are faced by dual challenges in both traditional network security and industrial security. On the attack front, in 2016, attacks on industrial systems got increasingly frequent around the world, with growing diversity in attack means. On the defense front, industrial systems in China generally have security vulnerabilities. With significant limitations, security policies put forward by NIST SP 800-82 and IEC62443 cannot accommodate the rapid development of industrial Internet.

Network Threats

- In 2016, Internet fraud largely showed the following notable characteristics: SIM cards became a new target for theft; short URL and Micro cloud sharing links were used to jump to phishing sites; false part-time jobs on well-known recruitment sites and voice platforms were used for swindling; personal information was used for accurate fraud; fraud got increasingly specialized, and there were more and more flawless deceptions; vulnerabilities of new services and unpopular services were used for swindling; cloud disk and synchronization software were used to steal information.
- According to the research conducted by 360 Internet Security Center on Internet vulnerabilities since 2016, the main characteristics include: Firstly, leak of personal information from websites has become a booster for Internet fraud; the leak of personal information is mainly caused by hackers' illegal intrusion by utilizing websites' security vulnerabilities and the illegal selling by the internal staff of the websites. Secondly, in the financial industry, threats of website vulnerabilities have become more complicated. Apart from traditional financial fields such as banking and insurance, many high-risk vulnerabilities have appeared in emerging fields such as third-party payment and Internet P2P. Thirdly, website vulnerabilities are used for embedded Trojan attacks, which shows a trend of rampancy. Fourthly, vulnerabilities exposed when smart hardware accesses the Internet are easy targets for hackers, and the security hazards also cannot be neglected.
- The theme of 2016 China Internet Security Conference was "Collaborating to Build a Community of Security + Fate". The purpose was to show that the industry had come to realize that as high-level threats occur frequently, individual enterprises or products cannot do when it comes to security protection. In the "Internet+" era, both security technology and security industry require collaboration, which is both an essential and inevitable trend. Specifically, collaboration at least involves the following three aspects: data collaboration, industry collaboration and intelligence collaboration. At the conference, we identified four main development trends of Internet security: Collaboration will become a new trend in the security industry; controllable industrial Internet security has drawn great attention again; growing importance is attached to big data analysis technology in the field of security; security talents cultivation has gradually become a focus of attention in the industry.

Security Trend

- The year 2016 marked technology transformation in the field of network security. In particular, first of all, the primary characteristic of website security protection is the shift from single-point defense relying on individual devices and technologies to multi-point security defense. The traditional pyramid-style layered combating can no longer suit the current security situation. Secondly, website security model innovation represented by All-testing is an improvement and upgrade from the prior non-profit open vulnerability-solicitation model. Thirdly, collaboration innovation featuring "end + cloud" application awareness provides a new idea and direction for enhancing Web application security, especially RASP technology. Fourthly, new trend of threats represented by Internet open data mining will become a new trend of research on Web security technology in 2017 and beyond.
- In August 2016, an artificial intelligence machine contest was held in the field of security, and after that a man-machine contest was held, drawing great attention in the field of security. As a result, people now have a new understanding of the application of artificial intelligence technology in the field of security and network attack and defense. The high-profile security contests are machine contest CGC and DEF CON CTF finals in which the winner system from CGC took part in for the first time. Although CGC winner Mayhem system came out last in DEF CON CTF finals, , it led the two human teams at the end of the second day during the match.,. Furthermore, according to the feedback from the human teams after the contest, Mayhem system generated effective attacks on vulnerabilities that human beings find it hard to harness. CGC has opened up a new era for the application of artificial intelligence in the field of security. In the next few years, it is believed that we will see more new application of auto systems and the combination of auto systems and human beings in the field of security.
- Collaboration is a silver bullet for information security, and an inevitable product of the contradiction and predicament faced in network security. Collaboration capability can be divided into three basic aspects: data collaboration, industry collaboration and intelligence collaboration.
- The development of industrial Internet security technology involves change of concepts in many aspects. In particular, it is necessary to introduce the technical idea of data-driven security, and utilize threat intelligence technology to establish a new internal threat warning system and emergency response mechanism. Based on 360's security practices, we put forward PC4R, an adaptive protection architecture used to guide the daily operation of industrial Internet information security. The architecture consists of six closed-loop steps: information perception, data collection, transformation and analysis, information integration, cognitive prediction and response decision.

Policies & Regulations

- Policies and regulations concerning network security introduced by China from 2016 through January 2017 include the followings: Outline of China's 13th Five-year Plan, Outline of the

National Informatization Development Strategies, Regulations on the Protection of Minors from the Internet (exposure draft), Network Security Law, National Cyberspace Security Strategy, Three-year Action Plan for Major Projects of Information Infrastructure, Planning on the Big Data Industry, and Opinions on Promoting the Healthy and Orderly Development of Mobile Internet.

- This report examines policies and legal documents released in 2016 (inclusive of January 2017), so as to interpret more clearly China's policies for regulating, constraining, guiding and promoting players in the network security industry. Furthermore, in light of the hot issues of concern in the industry, the report focuses on the areas of key information infrastructure, security vulnerability protection, personal information protection, responsibilities and obligations of operators and regulators, cultivation of teenagers' security awareness, security audit regulation, and cyberspace sovereignty. It expounds the characteristics and law of main policies and regulations issued in 2016, and the impacts that they will have on the network security industry and trends.

Key words: malware, ransomware, phishing sites, crank calls, telemarketing scams, SMS scams, pseudo base-station, Android system, Internet fraud, smartcams, IoV, website vulnerabilities, DDoS attacks, email security, emergency response, APT, industrial Internet, China Internet Security Conference, artificial intelligence, network security regulations analysis