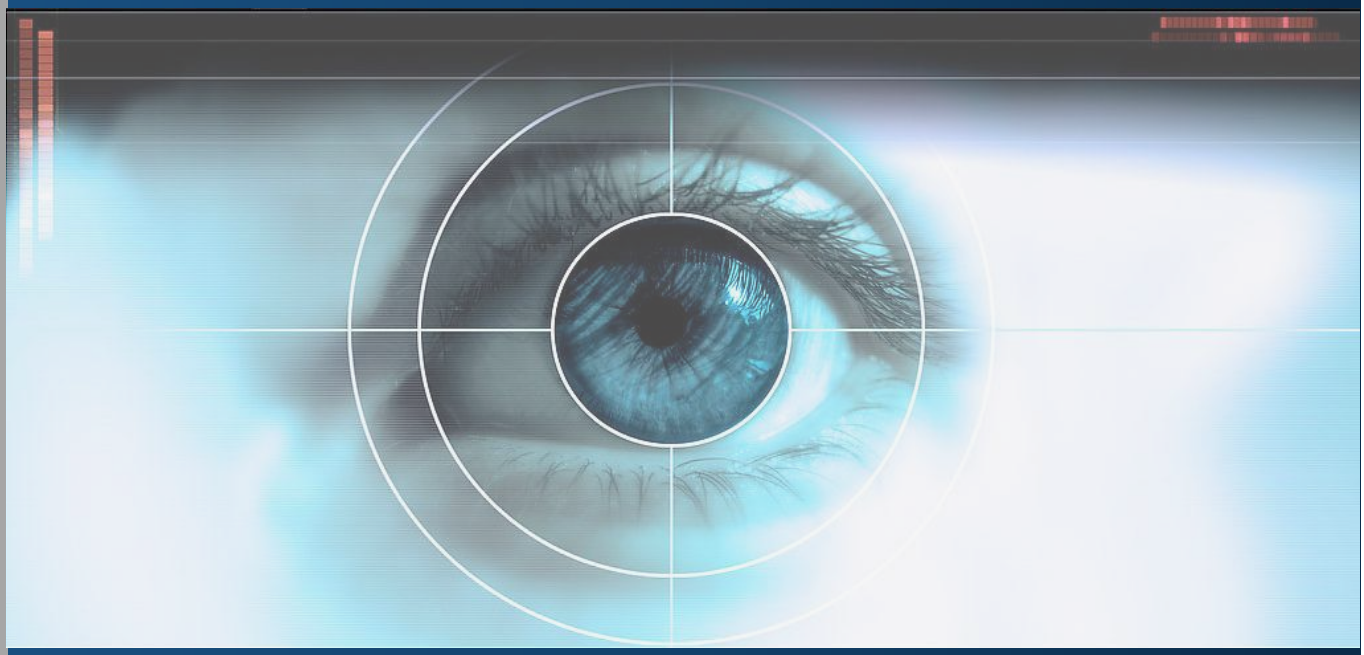
ANTIY



Review of the Year of 2014, the Moment of Network Security

——The annual report of network security in 2014

Security Research and Emergency Response Center of Antiy Labs

Contents

1 Prologue

The year of 2014 was full of noises and unusual incidents in terms of network security, which makes us feel that those lengthy statistics numbers exported from the malware backend systems cannot represent this magnificent and changeable age. Therefore, we decided to review the whole year by some immature words and diagrams.

Antiy still updated the Malware Wanted Poker with security threat theme as our gifts in the beginning of 2014. We chose APT (Advanced Persistent Threat) as the Red Joker, which means it is the most serious security threat; we made the Malware/Other as the Black Joker, which is the prediction of security threat trend. The word Malware/Other is made by ourselves according to the malware nomenclature.

2 APT

"Is the APT getting less and less attention", this question was asked several times after our technical lectures by the audiences and media. And our answer to it is as follows: when the threat have bored the media, it's time for it to behave normal, instead of emergency research, which means it starts to approach more and more people.

From the time the word APT was created from the office of USA Eighth Air Force wing during the year of 2005 and 2006, APT has been 8 years old and got too much interpretation. The spark of APT started in 2011 and 2012, which is the result of some new product solutions have getting mature and been focused by the industry.

From this point, when we were still paying attention to the influence of the rapid expansion of Trojan amount, we have been left behind.

Speaking of APT of 2014, the public would pay more attention to the incident of Sony Pictures Entertainment, which resulted from the film of *The Interview*. But from another point of view, when the attack starts with blackmail warning and ends with damaging the hardware data, is it still a kind of APT? As Michael questioning whether Stuxnet is APT or Cyberware at *Why Stuxnet*

Isn't APT, the incident of Sony might also be a kind of warlike operations with less brilliant techniques.

However, APT incidents still get lots of attention. There are 33 APT attack incidents during the whole year of 2014, among which Regin and Epic Turla are the incidents that attacked the largest numbers of countries and organizations. Regin is a set of advanced invisible malware with brilliant concealing methods and uses P2P technology to send instructions and steal information. We truly see the artistic attack methods and equipment system.

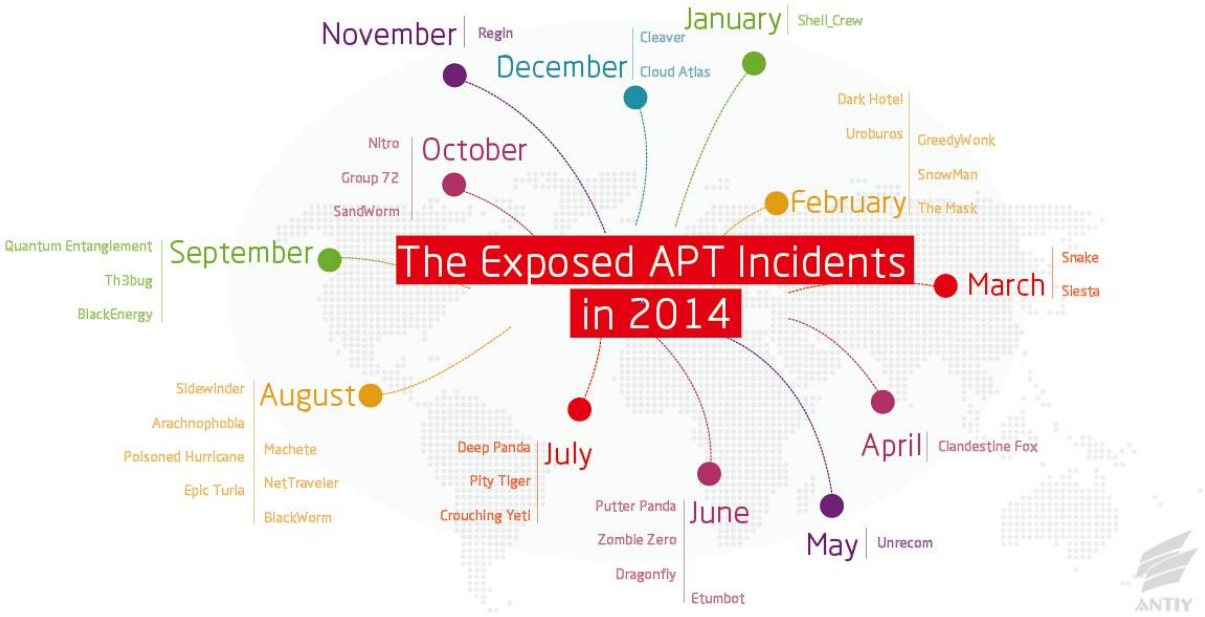


Figure 1 The exposed APT incidents in 2014

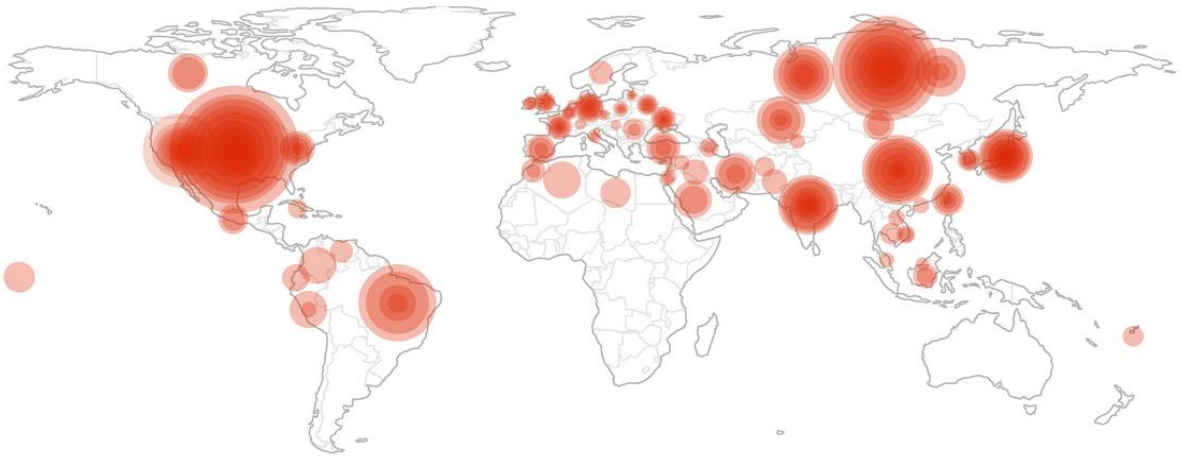


Figure 2 The attacked countries of the exposed APT incidents in 2014

The exposed APT incidents in 2014 have attacked nearly one hundred countries, among which the most attacked countries are America, Russia, China and Japan. The attacked industries include energy, finance, medical and health, media and electric communication, public administration, security and defense, transportation and so on.

3 Severe vulnerabilities

The most severe vulnerability for the past three years, Heartbleed, occurred on April 7, 2014. It exists in the OpenSSL. The attacker can use it to read the 64k data from the OpenSSL server memory with vulnerability, which serves as a way for attackers to access the following sensitive information, such as accounts, passwords, personal information, the certificates and private keys. As OpenSSL is widely used, the vulnerability has affected several large-sized Internet vendors, including Google, Facebook, Yahoo and BAT, as well as various network service vendors and organizations, such as online banks, online payment and email.

The vulnerability has existed in OpenSSL for two years, which was found by Neel Mehta (the Google researcher) and the researcher of Codenomicon (Network Security Company). They informed OpenSSL to fix the vulnerability. The new version OpenSSL 1.0.1g has been released when the public announcement was published. Meanwhile, Google has fixed it earlier than the industry. The network attackers started to access the data in a crazy way after it was released.

Someone made jokes that the price of hard disk got higher in order to store the data obtained by Heartbleed. Though it was exaggerated, the usage value is remarkable. When we review these incidents, we found that the cutting-edge companies released POC irresponsibly, such as Codenomicon, which is the important reason of Malware/Other.

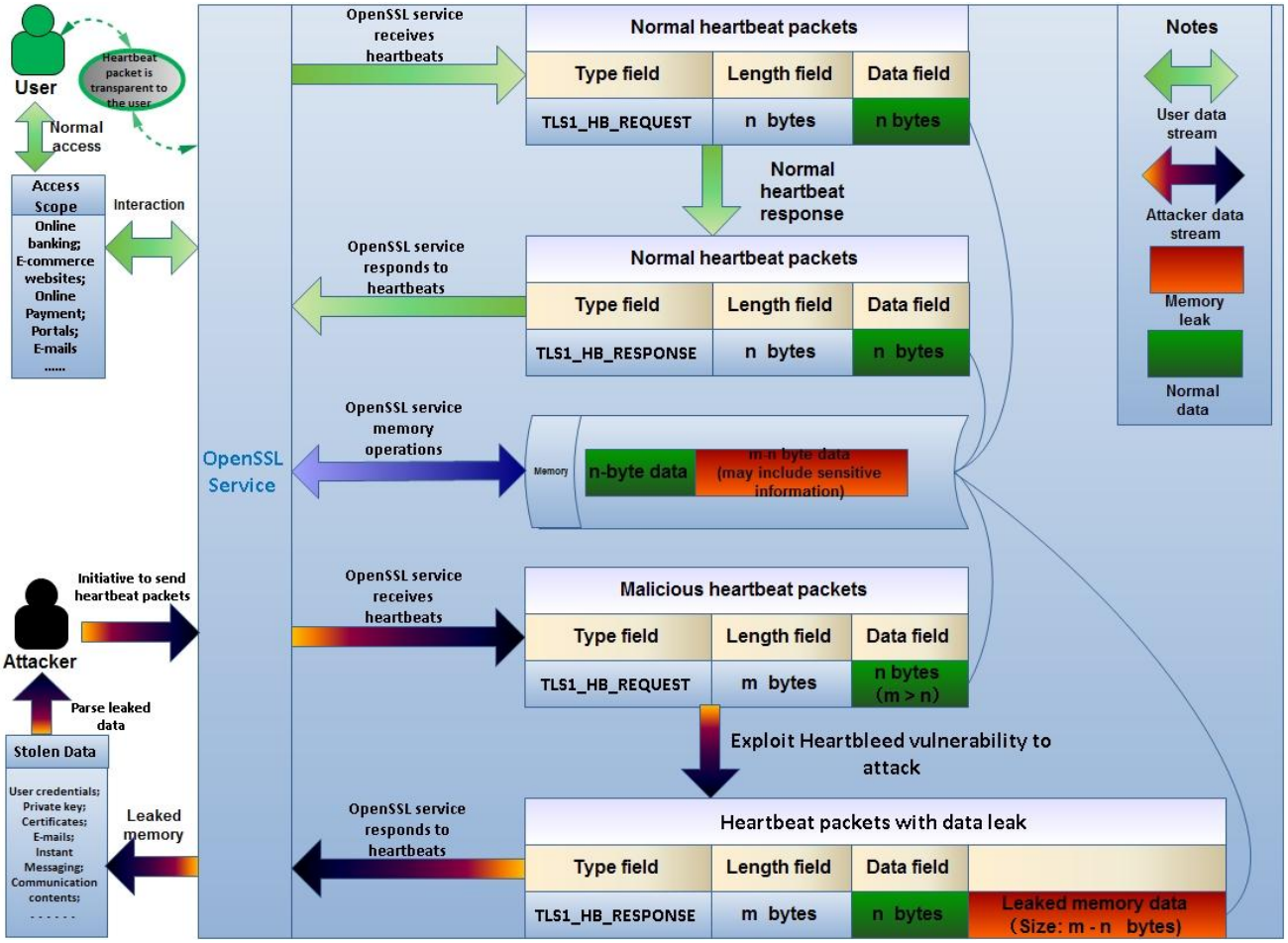


Figure 3 The schematics of Heartbleed

*Note: Figure 3 is quoted from*http://www.antiy.com/response/heartbleed_faq.html.

The more severe vulnerability, Bash Shellshock, was exposed in September. Due to the wider existence of GNU, it has threatened not only the server system, but also the network security equipment, including network devices, exchange devices and firewalls, as well as the custom systems using Linux. It is found that it has existed nearly 20 years. The other fatal problem is: it's impossible to realize complete position fixing as GNU Bash is widely spread; moreover, the flexible grammar of Bash results in the extremely complexity of the analysis program. Therefore, there

were new problems occurred after each patch released, which resulted in a series of Bash vulnerabilities.

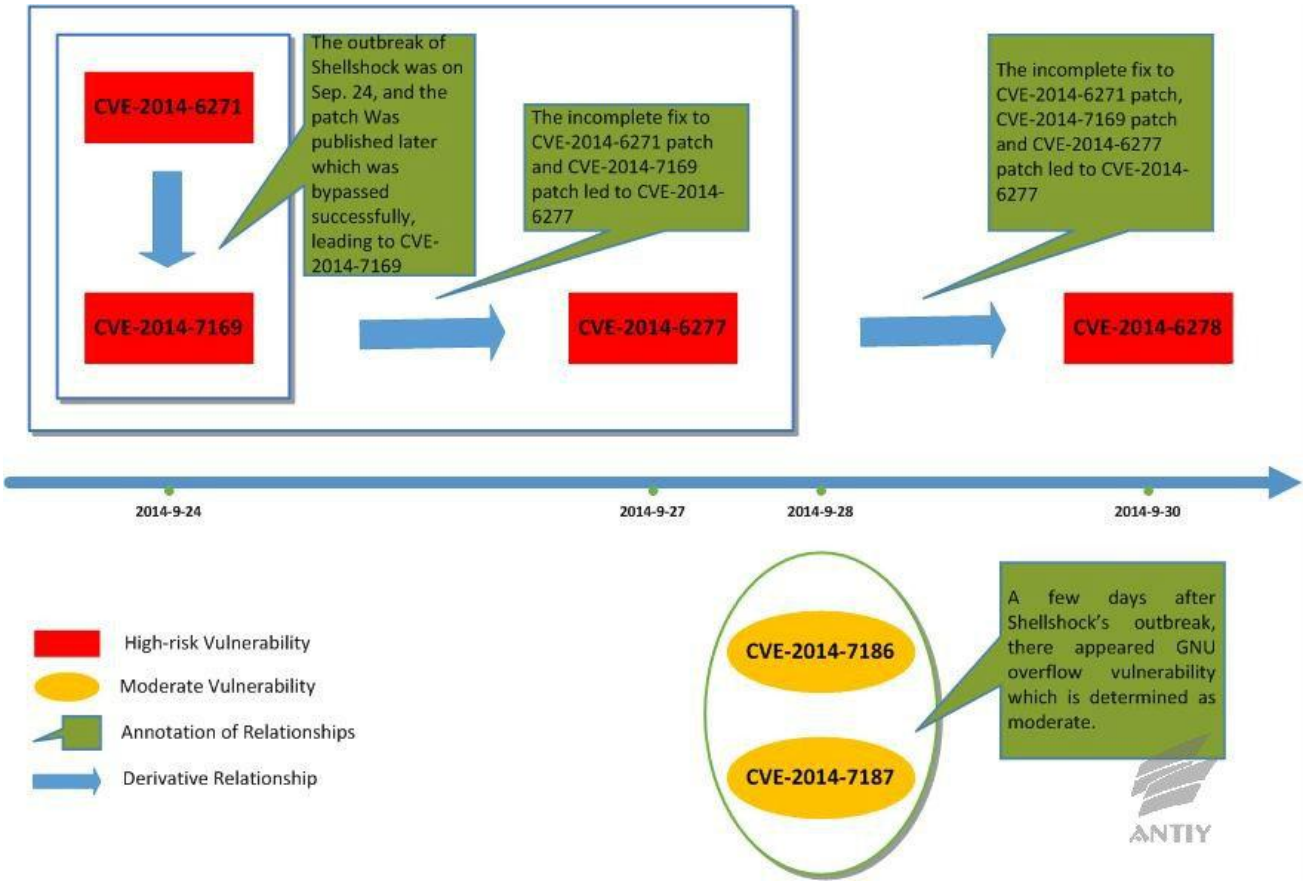


Figure 4 The revealing of Bash and its iterative fixing

Note: Figure 4 is quoted from http://www.antiy.com/response/The_Association_Threat_Evolution_of_Bash_and_the_Current_Status_of_Malware_in_UNIX-like_Systems.html.

Then, a continuing DDoS attack has affected the operation of domestic DNS system. The majority of nodes that launched the attack are the online intelligent devices, such as cameras. After analyzing the relevant botnet, we found that it accessed large amounts of nodes by using Bash vulnerability.

In fact, we also found the existence of Bash vulnerability on some domestic operation systems. As for the domestic operation system field that depending on the open systems, the pseudo closed source system poses more threats than the open software.

In addition, as the basic protocol of security certification and encrypted communication, HTTPS has been repeatedly mentioned in this year. There were problems in the SSL realization of Microsoft Server, and several online banks have exposed incorrect code realization.

4 The generalization and distribution of security threats

Except for the vulnerabilities of the following familiar systems, such as Windows, Linux, Unix, iOS, Android, with the development of smart home and wearable hardware, the threats are evolving, too.

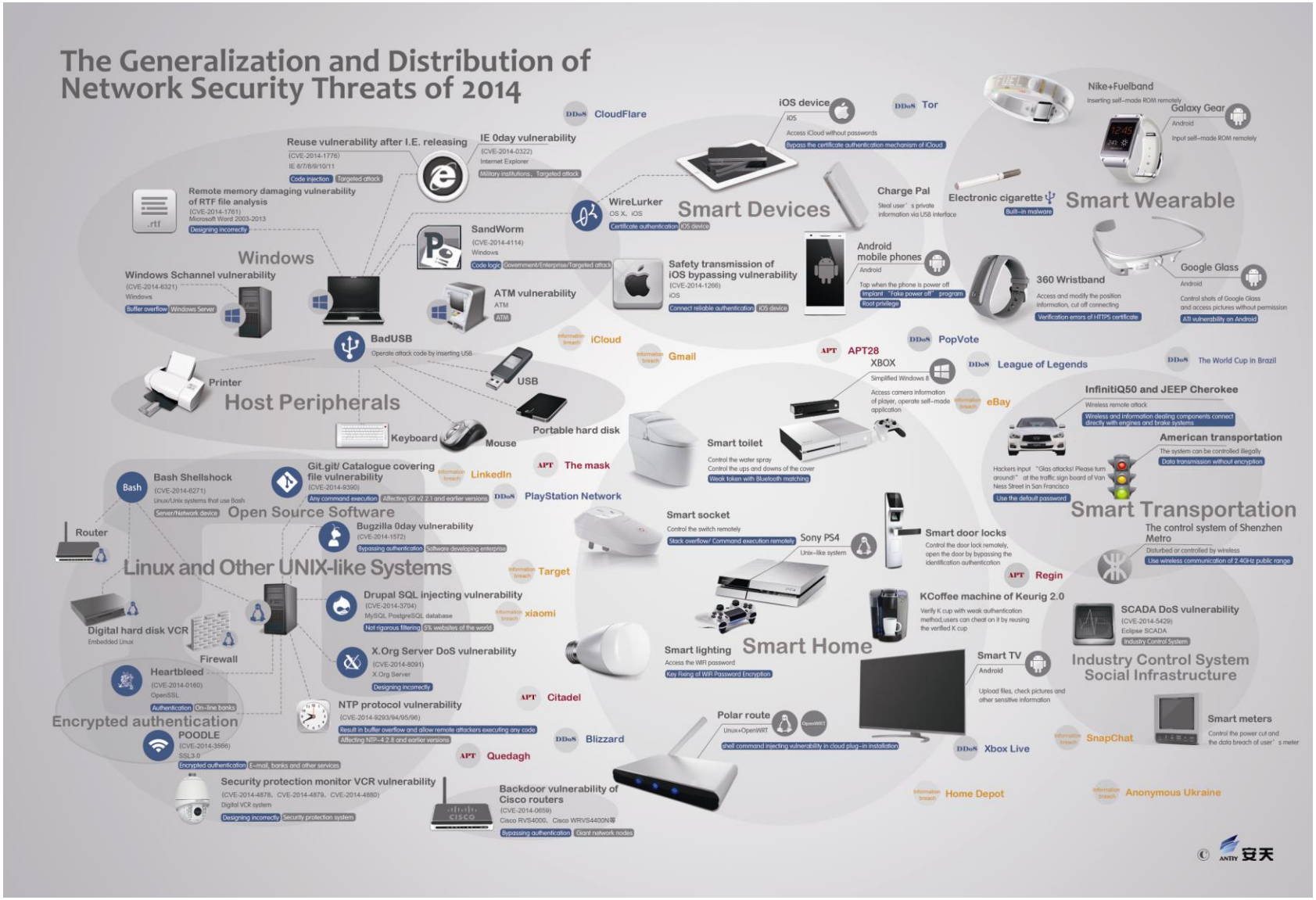


Figure 5 The generalization and distribution of security threats of 2014

5 Data breach

The series of data breach incidents in 2012 have brought great influence, while the problem is still severe in 2014. Some of the leaked data came from dragging the library, while some others from hit the library. The "12306 Hit the Library Incident" made people believe that few data integrations and backend data breach would cause some social panic.

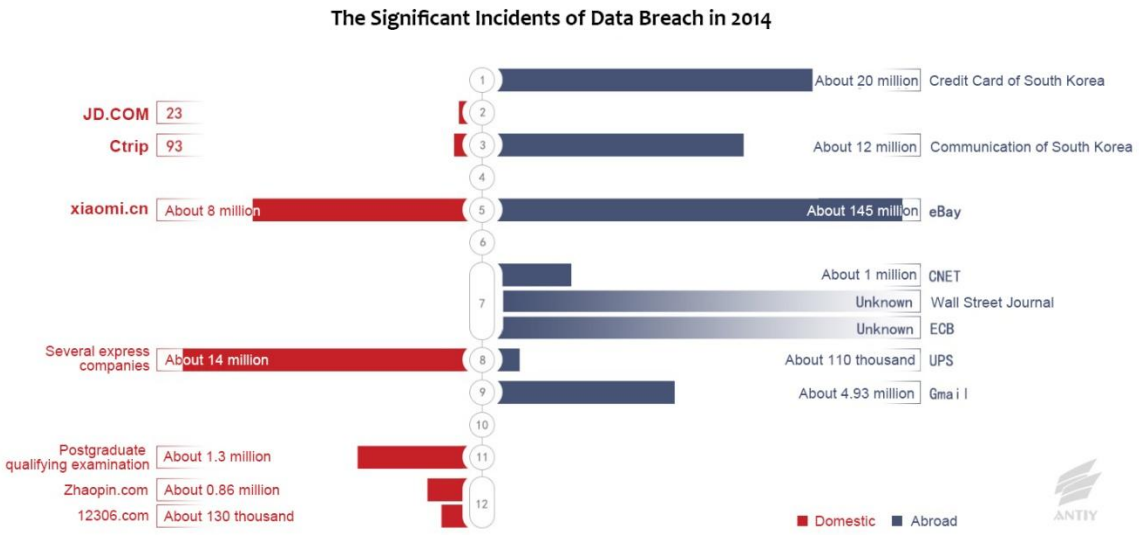


Figure 6 The significant incidents of data breach in 2014

We have made statistics about the breach data in the "12306 Hit the Library Incident", which indicates that the website service still need to lead users to practice more powerful password strategies, especially using separated passwords for important websites.

	Password	Numbers of users	Percentage
1	123456	392	0.30%
2	a123456	281	0.21%
3	123456a	165	0.13%
4	5201314	161	0.12%
5	111111	157	0.12%

Table 1 The TOP5 order from the leaked data of 12306

	Amount(with repetition)	Percentage	Amount (without repetition)	Percentage
Numbers of passwords	131653	100.00%	117808	89.48%

With special characters	177	0.13%	154	0.12%
Users with absolute numerical passwords	35572	27.02%	30456	23.13%
Users with absolute letter passwords	7161	5.44%	6004	4.56%
Users with absolute lower-case letter passwords	6947	5.28%	5797	4.40%
Users with absolute capital letter passwords	62	0.05%	61	0.05%
capital letter + number	395	0.30%	383	0.29%
lower-case letter + number	87664	66.59%	80133	60.87%
Mix of capital letter and lower-case letter + number	237	0.18%	228	0.17%
Password with birth day (such as 19810101)	3400	2.58%	1725	1.31%
Using birth day as password (such as 19810101)	2326	1.77%	3322	2.52%
Password with birth day – Not self-birthday (such as 19810101)	11368	8.63%	10269	7.80%
Password without birthday	114559	87.02%	102889	78.15%
The user name and the password are the same (the same data)	1733	1.32%	1712	1.30%
The user name and the password are the same (Not the same data)	1769	1.34%	1746	1.33%
Password with user name (the same data)	832	0.63%	820	0.62%

Table 2 The statistic of password using habits of the leaked data of 12306 website

6 Malware on PC platform

We have analyzed on the rapid explosive growth of malware from 2006 to 2012 in *The Association and Inevitability of Trojan Avalanche and APT*. The trend currently shows great changes. In terms of the black sample amounts, our sample database has added 30 million Hash in 2014, but the growth rate has slowed down considerably.

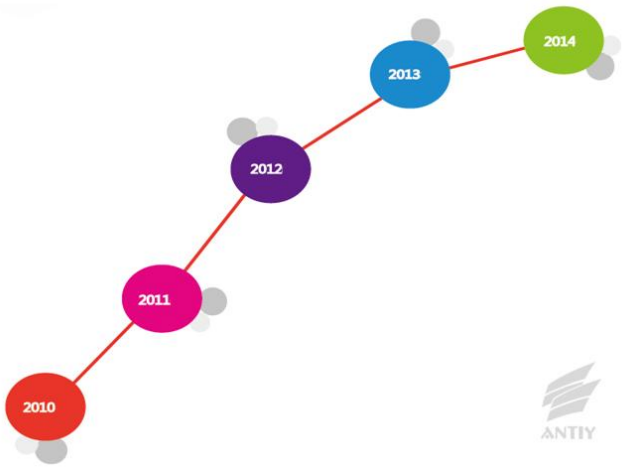


Figure 7 The trend of increasing amounts of malware in the past 5 years

In the following ranking list, Trojan/Win32.AntiFW got the first place. This family occurred in February 2014 with the goal of obtaining economic benefits, which has the following potential threats: installing advertisement software, blocking browsers, modifying the home page of browser, customizing search settings and so on.

There are 5 similar advertisement software families with the same goals of obtaining economic interests in the top 10 list, namely DomaIQ, Lollipop, Morstar, AdLoad and MultiPlug. Except for GrayWare[AdWare]/Win32.AdLoad, most of them were the newly occurred families.

In the list, there were no newly occurred infective malware. Sality and Virut still got top places in the infective virus ranking list; meanwhile, Nimnul still existed. In the TOP10 list, the last place is Zbot family, which propagated by emails and still existed during the year of 2014.

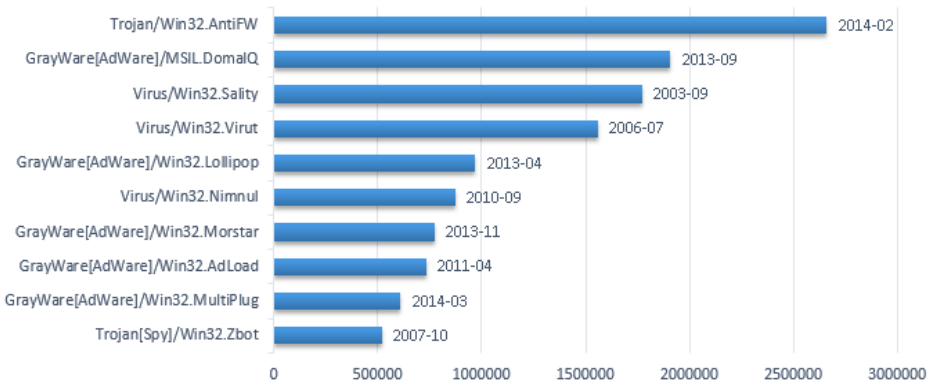


Figure 8 The ranking list of malware amounts on PC platform in 2014

In the following ranking list, the advertisement behavior with the goal of obtaining benefits got the first place again; the amount of downloading behaviors was pretty big due to its strong concealment and practicability; the backdoor malware with remote control behaviors ranked the third.

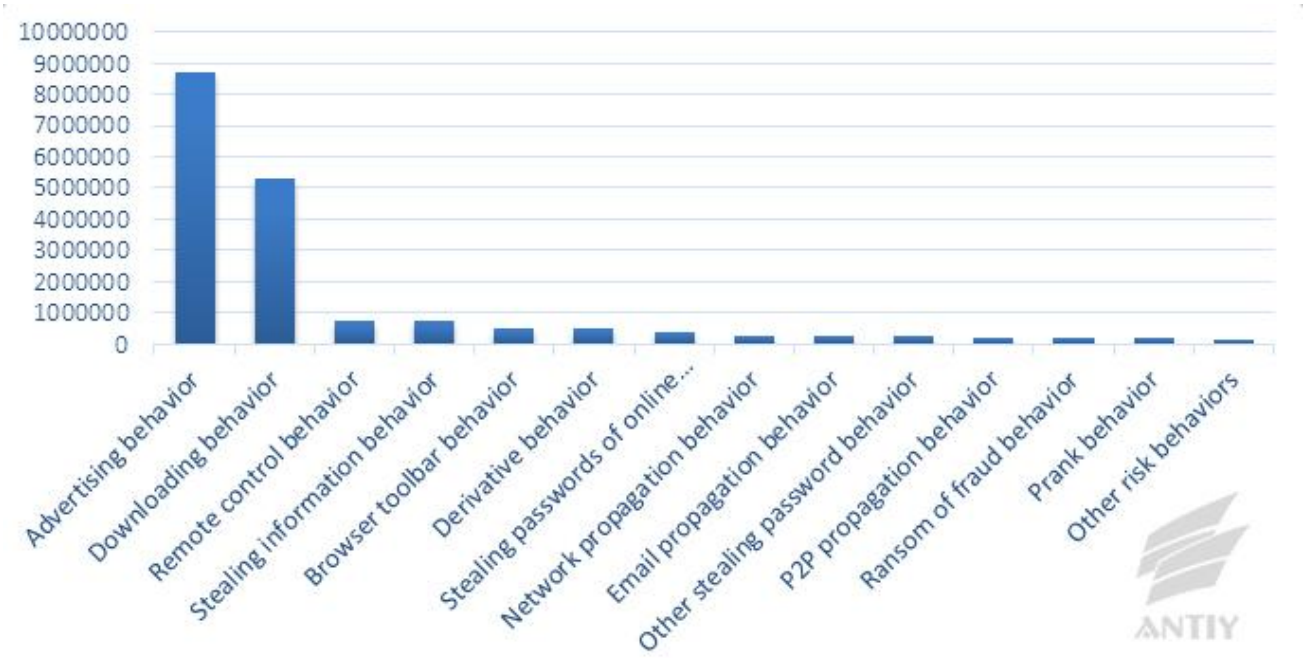


Figure 9 The ranking list of malware behaviors on PC platform in 2014

7 The statistics of malware on mobile platform

The trend of increasing amounts of malware on mobile platform in 2014 slows down slightly, the sample amount has exceeded 0.8 million.

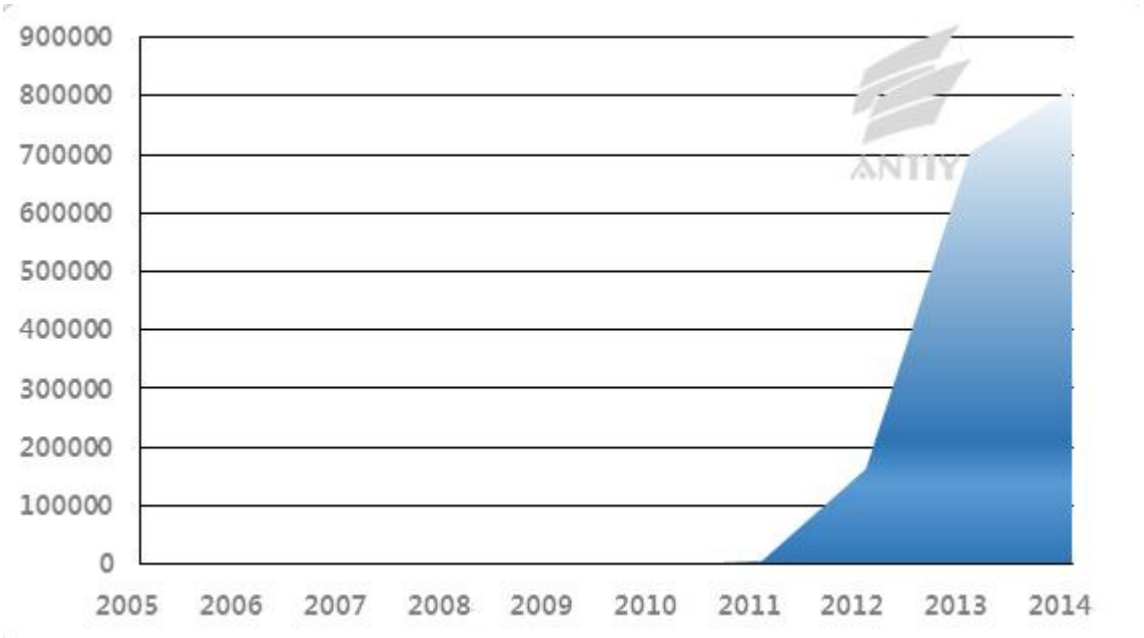


Figure 10 The trends of malware on mobile platform from 2005 to 2014

The malware can be classified into the follow 8 categories according to behavior attribution: malicious charging, fee consumption, system damaging, stealing private, rogue behaviors, remote control, fraud and malicious propagation.

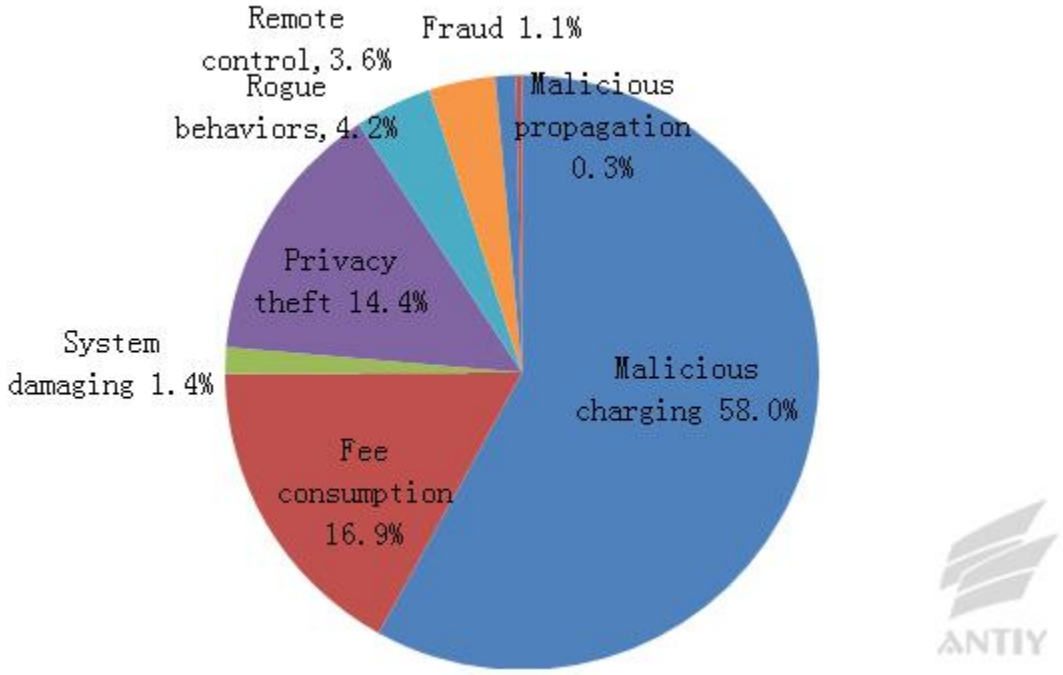


Figure 11 The statistics of behavior attributions of the number of malware on mobile platform in

2014

According to the monthly statistics of the number of malware propagation incidents on mobile platform in 2014, the number is nearly 12 million, which is the highest; while the number in December is the lowest. From this figure, we can see that there are downtrends in both the first half and the second half of the year.

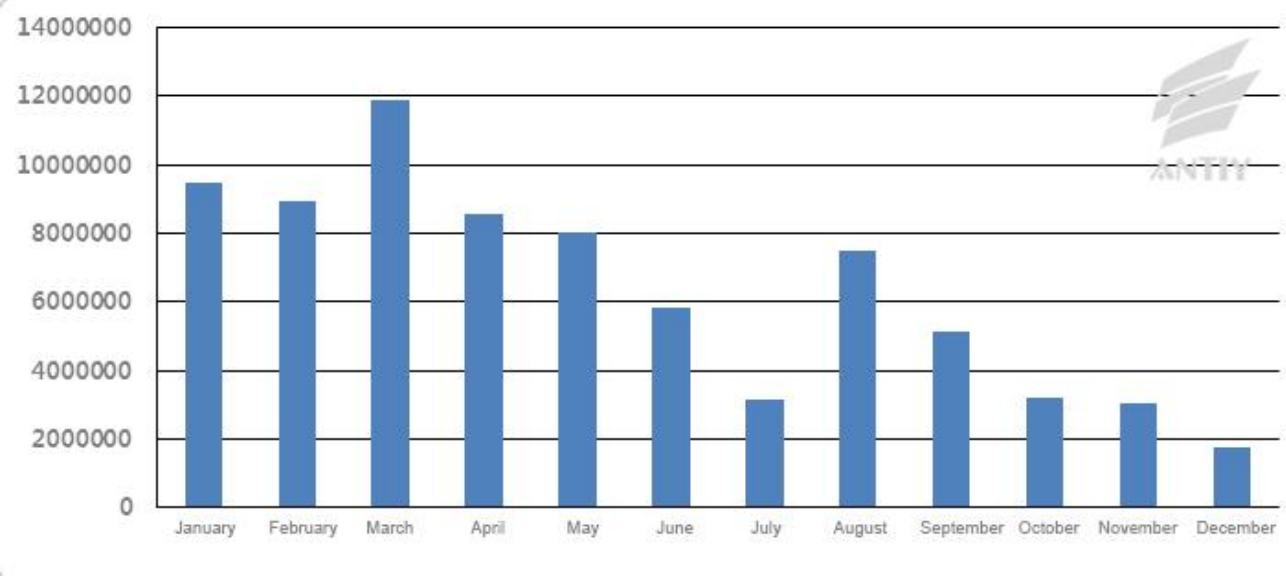


Figure 12 The monthly statistics of the number of malware propagation incidents on mobile platform in 2014

From the monthly statistics of the malware propagation domains and number of IP on mobile platform in 2014, we can see using domain accesses is the choice for most malware propagations.

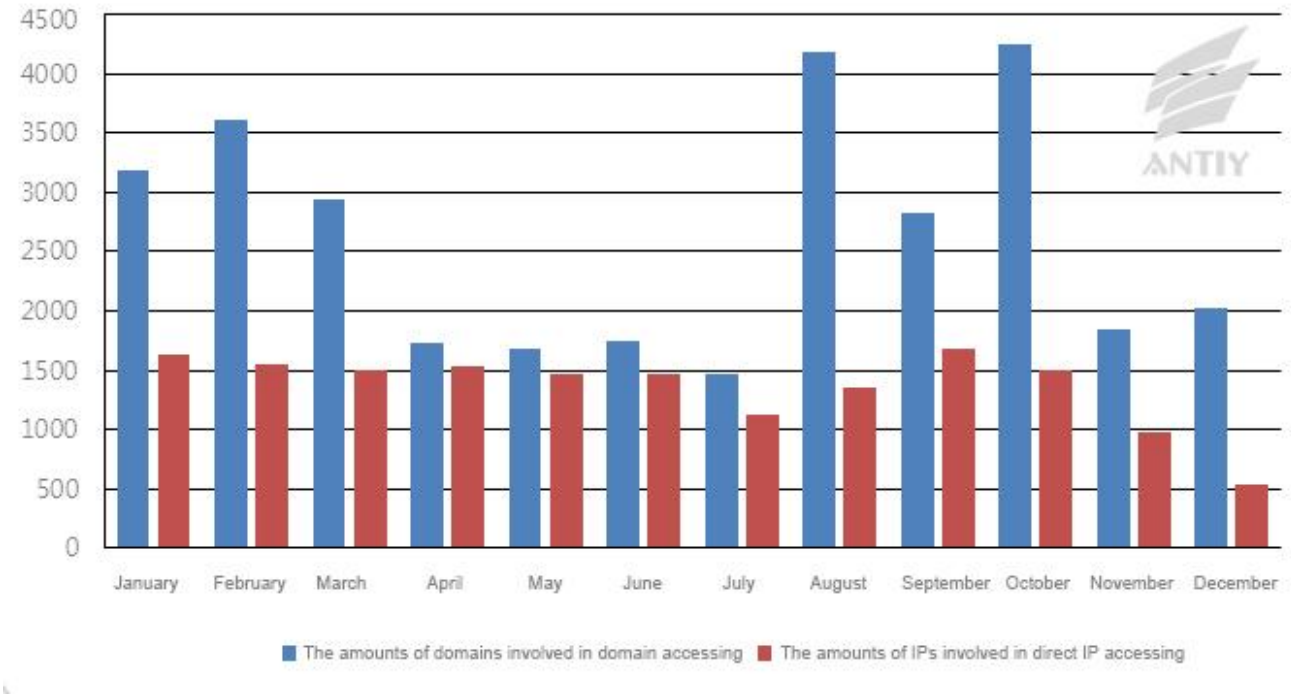


Figure 13 The monthly statistics of the malware propagation domains and number of IP on mobile platform in 2014

8 Some thinking in this era

The era of Malware/Other breaks our illusions, such as the so-called open source security legend. When few people insist on open source security still stick to the view that "open source means the whole world produce a system together, while close source refers to several people doing the same", the effect of community weakness that brought by the imbalance of security capability is being highlighted. Heartbleed shows the result of black light in OpenSSL, and reminds the industry that these are the security profession, study capability and security cost that we need to integrate to reach safety. On the other hand, the safety survey actions against open source after Heartbleed can be regarded as a compensation of the disaster. The action got a review from the whole domain threats for the open source system. And Wirelurker also made the security mythology of iOS being dashed.

The key vulnerabilities showed the powerful energy again in 2014, which made the comparison of vulnerability amounts and the discussion of which system is more secure lose the meanings completely. The key vulnerabilities brought too much uncertainty and contingency to both the attackers and the defenders. The gap of information attack and defense capability might be leveled by a key vulnerability in a moment.

This era might be blind. We tend to transfer our focus fully to the new threats when they are under reinforcement, instead of analyzing what we have and our basis which are of the same significance. For instance, in the case of Heartbleed, the thoughtful question is that the researchers found that the HTTPS usage ratio of domestic websites is pretty low, while many websites still adopt HTTP, and the security arrangement is only the hash computed by order. In fact, this is the gap between China and the developed countries in terms of basic security awareness and capability.

It is still popular to condemn both by speech and writing about the three traditional ways: firewalls, antivirus and patching. The denouncement is used to support finding a new security mode or thought. But in fact, the real situation of more and more Chinese governments and enterprise customers is: lots of firewalls are shelved and have never been installed after the purchase; the virus database of the intranet antivirus product is upgraded once for several months or half a year; and patching is regarded as the dangerous move that might affect the business

stability. Is the current security issue resulting from the useless of the three traditional ways or the lack of real attention and valid usage?

We have lots of lessons to catch up from the Internet security service specification to the IT governance capability. We did not establish the firm system that can transfer our insights to examine the new threats. Instead, we need to confront both new and old challenges simultaneously. If we ignore this situation, we would breed unrealistic miscarriage of justice, especially starting to worship and look forward to the "Perpetual Motion Machine" to change the security situation, while forgetting that the security nature is the endless fight and improvement.

This era might also be apathetic, the Bash vulnerability that is more severe than Heartbleed did not get more attention from the domestic media, and the reason was many people thought Heartbleed did not have too much influence. When the memory data of some mainstream websites were being accessed with T as measurement, we cannot imagine what a greater impact is. Would only the network outage of large areas or exposure of large amount of backend data account for significant impact? This is an extremely under-developed security criterion; and the mindset can make people be positive about the dangerous situation.

The reason of threat generalization is the great development of information, which makes it become ubiquitous; in addition, more and more traps, hidden troubles and incorrect thoughts continue to be inherited, which is the development land for Malware/Other; the second reason is the universalness of attack capability, as is said in *The State of Incident Response* by Bruce Schneier, "the ongoing and significant trend is that more and more tactical behaviors are applied to the wide network space", which provides tools for accelerating Malware/Other; and the flourish of underground dark industry also becomes the continuous power of Malware/Other.

This era makes many people conceive the preset plot of command economy. The fear of security has resulted in the resurface of the view: no security, no more development. This point of view ignored the rigidity of demands.

Many people in this era would think of *Out of Control* written by Kevin Kelly. One of my respected teachers told me that there are two books on his desk, one is *Out of Control*, and the other is *The Road Ahead* from Bill Gates; and he said that the anxiety and fear brought by the former book are

far better than the wish brought by the latter. But with a second thought, all the giant technical improvement in the history brought great anxiety to people, such as the steam engine, electric machine, atomic energy, gene technology and so on. There were used for damaging, crimes and wars, but they made the world more civilized, developed and beautiful.

The existence value of security is to protect the application value instead of neither making limitations against it, nor fettering the development. Today, although we are confronting various security crises and the associated anxiety about future, we still believe that only development and improvement are the most important security.

Security engineers should be doers instead of predictors. Maybe this choice is more suitable for era of social instability.

Appendix 1: About Antiy Labs

Antiy Labs is a professional next-generation security-testing engine R&D enterprise. Antiy's engines provide the ability to detect various viruses and malware for network security products and mobile devices. They are used by more than ten well known security vendors. Antiy's engines are embedded in tens of thousands of firewalls and tens of millions of mobile phones all over the world. Antiy Labs is awarded the "Best Protection" prize by AV-TEST in 2013. Based on engines, sandboxes and background systems, Antiy Labs will continue to provide traffic-based anti-APT solutions for enterprises.

For more information about antivirus engines, please refer to: http://www.antiy.com

http://www.antiy.net

For more information about antivirus engines, please refer to: http://www.antiy.cn

Appendix 2: Incident logs

Time	Version	Updated content
2014-12-25 13:58	V1.0	Writing
2015-01-15 16:53	V1.1	Modifying data and diagrams
2015-01-18 14:11	V1.2	Modifying words
2015-01-29 10:21	V1.3	Proofreading