Journal of Engineering Science and Technology Review 6 (3) (2013) 146- 152

JOURNAL OF
Engineering Science
and Technology Review

www.jestr.org

Research Article

The Inside of Information Security Industry in the Perspective of Hackers and Economics

Cong Gao*, Jianfeng Ma, Jingjing Guo, Liang Zhang and Xindi Ma

Shaanxi Key Laboratory of Network and System Security, School of Computer, Xidian University, Xi'an, 710071- China

Received 12 May 2013; Accepted 28 November 2013

Abstract

Nowadays, the rapid development of the Internet has given rise to a global murky underground business, which is called the hacker economy industry. Numerous individuals and companies have become victims of the industry. In essence, the leakage of user information which facilitates the operation of the industry is the chief culprit. Hackers all over the world have invented hundreds and thousands of sophisticated schemes to obtain user information. Once user information is obtained, a full utilization of it will be performed by hackers until ultimately, the value of it is drained out. In order to present a general picture of the hacker economy industry, we in this paper perform a detailed analysis of websites, malware, hackers, and users. In addition, we elaborate the operations and the structure of the hacker economy industry. Lastly, we point out the direction of possible countermeasures for guarding user information which facilitates a further in-depth study and present a case study to illustrate our work.

Keywords: Hackers, Personal Information, Privacy, Security, Web Sites

1. Introduction

December, 2011, a text file with 6.43 million user information, including user name, password, and e-mail, all in clear text leaked on the Internet. The sensitive information originally belongs to CSDN.net (Chinese Software Developer Network,) and undoubtedly, was supposed to be kept confidential. Founded in 1999, CSDN is the largest online Chinese IT technology community in the world, currently owning more than 18 million registered users.

After CSDN.net, similar security breaches followed in Tianya, Mop, Kaixin001 and other leading Internet companies in China. The series of incidents aroused a hacking scare that has prompted most netizens to change their passwords. Internet security company Qihu 360's surveillance data showed the wave of password exposure has affected "hundreds of millions". This marked the biggest outbreak of data leakage in the history of China's Internet. Meanwhile, since users tend to use the same password for multiple accounts, hackers try to login other websites with the obtained user names and passwords. In this way, the leakage of user data will certainly initialize a domino effect, opening the door for more widespread cyber security incidents. A domino effect would occur as one site's password file falls prey to hacker who then uses it to infiltrate other systems, potentially revealing additional password files that could lead to the failure of other systems [1]. The leakage of private information does harm to each individual concerned not only in terms of material loss but also of spiritual well-being. Understandably, victims in such situations usually tend to be overwhelmed and frustrated.

During February 2011 to March 2012, there was a spate of data breaching incidents, with the range and size of victims being rarely seen in history. In February 2011, HBgary, the well-known information security enterprise, was hacked. Greg Hoglund, CEO of HBGary, admitted that lackluster security at his company played a central role in the breach that led to the release of some 50,000 company emails [2]. In April 2011, Epsilon, the world's largest permission-based e-mail service provider, was hacked. The incident resulted in a leakage of customer names and their e-mail addresses. At least 38 large enterprises were involved and millions of their customers' e-mail information was exposed in the breach [3]. After Epsilon, Sony was also confronted with a serious leakage of user information. Due to the compromise of its PlayStation Network, more than 75 million PSN user information was stolen. Details including names, passwords, addresses, and purchase histories were exposed by the mega hack. Whether credit card details were compromised is not yet confirmed but very much under suspicion from the public [4]. In March 2012, credit and debit card processor Global Payments was hit by a security breach that put some 50,000 cardholders at risk. Thus it can be seen that data breaching has been a disaster for both companies and users. Indeed, it has already become a global issue. We present in this paper a general picture of the hacker economy industry. We present the distribution of criminal activities among ten countries in 2008 and 2009 based on a technical report [5] released by Symantec Corporation. The detailed data is illustrated in Table I.

The remainder of this paper is structured as follows: Section 2 presents a classification of websites and the notion of malware, further exploring three types of malware. Section 3 introduces three kinds of hackers. Section 4 shows

* E-mail address: glidergao@gmail.com

the operation and hierarchy of the hacker economy industry, together with a general frame of countermeasures. Section 5 presents a case study. Section 6 concludes.

Table I: Distribution of Criminal Activities

Overall rank		Percentage		
2009	2008	Country	2009	2008
1	1	United States	19	23
2	2	China	8	9
3	5	Brazil	6	4
4	3	Germany	5	6
5	11	India	4	3
6	4	UK	3	5
7	12	Russia	3	2
8	10	Poland	3	3
9	7	Italy	3	3
10	6	Spain	3	4

2. Websites and Malware

Judged from whether a website proactively attacks its visitors in nature, websites can be divided into two classes: malicious and unmalicious.

2.1 Malicious Sites

There are basically two kinds of malicious sites: attack site and phishing site. They are both illegitimate and of different focuses. The former intends to install something in user computers, while the latter tries to steal user's information directly. Generally, the accomplishment of both objectives largely relies on the weak vigilance of users and poor anti-virus protection in their computers. For ordinary users, the anti-virus protection of a computer is of great importance. In [6], the authors presented three anti-malware techniques: scanner/unpacker, static analysis, and dynamic analysis. The counterparts of the above three methods used by malware are packers, polymorphism, and metamorphism, respectively. The malware is mainly infected through the Internet, such as browsers, web mail sites, instant-messaging software, and file sharing.

For the sake of convenience, we make the following premises: 1) Users are unconscious of unusual phenomena (e.g. slow Internet connection speeds, strange changes in system settings, abnormal functioning of application software, etc) appeared in their computers; 2) There are no anti-virus mechanisms in user computers or the actual effectiveness of existing anti-virus protection is far from satisfaction.

An attack site is specifically built for the purpose of attacking with its target set on visitors' computers. There are many sorts of attack sites on the Internet. We concentrate only on those which make every effort to deliver malicious software to your computer system. In the remainder of this paper, we call malicious software "malware" for short, which is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network.

Many works have contributed to the classification of malware. In [7], the authors chose five specific types of malware to conduct their research. They are Trojans, Spyware, Backdoors, Worms, and Undecided. In this paper, we mainly concern three types of malware: Adware, Spyware, and Trojan, arranged in ascending order in relation to the degree of harmfulness.

Adware reflects its pursuit of economic benefits by automatically rendering advertisements without the permission of users. It functions in the form of a pop-up or other forms of advertising. The existence of adware does not always affect the operating status of computer systems. When the advertising is in progress, the system will be dragged. Whereas no advertising proceeds, the system runs as usual. For ordinary users, the existence of most adware can easily be noticed, but the uninstall can hardly be done. Generally speaking, adware frequently makes pop-ups, consumes system resources, embeds icons in browsers, etc. It is more annoying than harmful by itself.

Spyware, in contrast to adware, collects and sends information via the Internet without users' knowledge. It quietly runs in the background and never clearly exhibits its existence. By monitoring the system, spyware surreptitiously gathers almost all of the information flowing in it, including user names, passwords, bank accounts, etc. Moreover, the collected data will be sent to a mysterious e-mail address. To some extent, its stealthy feature enables it to stay away from the observation of users. However, because of its persistent surveillance on the system, spyware constantly slows down the system being monitored. Theoretically, it is likely that some seriously security-sensitive users might be aware of the abnormalities and make a further investigation. In practice, due to the rapid development of hardware technology and the universal high-performance computers, the chances are slim to none.

Trojan comes with a client and a server, whereas adware and spyware always appear in a form of stand-alone application. A complete Trojan consists of two parts: server (victim) and client (attacker). Victim is referred to a system with Trojan server-side program installed. Attacker is referred to a system with Trojan client-side program installed. The communication between client and server facilitates hackers to gain remote access and full control of the victim system. Undoubtedly, the relative complex constitution makes Trojan more intricate and powerful than the former two.

Generally, there is no communication between victim systems and hackers for either adware or spyware; even though spyware sends information, there is no feedback instruction from hackers. Nevertheless, the essence of Trojan is order and response. Once the server-side program is initialized successfully, hackers are able to make contact with it using the client-side program. Then, client issues an order, server executes it and responds. As the operations in victim system are performed directly by the attacker, Trojan, on the one hand, is much harder to be perceived by users than adware; and on the other hand, unlike spyware, Trojan remains inertia when there are no orders to be carried out. We depict the main differences of the three types of malware in Table II.

As its name implies, the trick of a phishing site is much like fishing in real life. Elaborately created by hackers, phishing sites are designed to scam users into entering personal information by masquerading as genuine sites such as banks, online payment services. Once deployed, they just wait for careless visitors. The technique of phishing sites is typically performed by spam emails. Once the links contained in spam are clicked, users will be directed to a fake site which appears almost identical to the genuine one. During the input process, private information like passwords

and credit card details are obtained without the victim's awareness. Then, a transaction or money transfer is conducted by hackers immediately based on the obtained information, causing the victim significant financial losses. Unlike attack sites, phishing sites acquire user information directly, without any malware installation. According the data illustrated in Table I, we have that the origin of phishing activities is located mostly in the US, Southern Asia and Eastern Europe.

Table II: Comparison of Maleware

	Adware	**Spyware**	**Trojan**
Structure	Stand-alone	Stand-alone	Client/Server
User Awareness	Easy	Hard	Difficult
Activity	Frequently	Constantly	Irregularly
Data Theft	No	Yes	Yes
Communication	None	Uni-direction	Bi-direction
Harmfulness	Slight	Serious	Severe

2.2 Unmalicious Sites

In order to obtain user information, rather than creating their own malicious sites against individual users, hackers can also attack innocent third-party sites on the Internet. In general, these sites are legitimate and focused on providing information and services of various areas which people can get access to either for free or by payment. Technically, information and services can be provided through two ways: interactive and non-interactive. Non-interactive sites just display certain information on the screen without requiring any input from users, such as news sites, archive sites, mirror sites. Namely, users merely "read". Interactive sites like social networking sites, electronic commerce sites and gaming sites, etc, however, do often rack their brains to obtain as much user information as possible for a further development of their business. That is, users not only "read", but also "write". Due to the characteristics of the above two type of sites, our attention is drawn by the interactive sites. We will introduce and discuss four major types of interactive sites which are of great interest to the hackers. They are Electronic Commerce, Gaming, Community, and Web Mail.

Electronic Commerce. Recent years have witnessed a rapid development of online commerce activities: stock trading, banking, home shopping, ticket/hotel booking and almost every imaginable service. When you are conducting transactions, information like debit card, credit card is stored on the sites. Once hackers obtained the information, they could directly blackmail the victim site and make certain demands. This is usually referred to as ransom scam. In practice, due to the risk of contact, hackers usually prefer a money transfer, a transaction or just selling the information on the black market without touching the valuable data.

Gaming. The same with electronic commerce, financial elements are also abounded in the thriving online gaming industry. Fascinating settings and cool experience of the games tempt increasingly more people spend money on it. In order to gain certain privileges in the games, people cannot help buying various virtual properties which bring more fun to the players. Besides those operations done in the case of electronic commerce, hackers can also sell virtual properties like World of Warcraft credentials in the gaming world. This, however, for some people, could be more frustrating than naked money stealing in electronic commerce because of the time and energy which he invested in the gaming world.

Community. Community sites serve as a platform where friends or people with similar interests can communicate with each other. There are many kinds of community sites, such as forum sites, social networking sites, blog and micro-blog sites. Usually, users are linked up by private messages or public message boards. Recent years, social networking sites are booming all over the world. Besides the communicating function which ordinary people use in everyday life, social networking sites also facilitate the knowledge sharing in scientific field [8].

Generally, once these sites are compromised by hackers, users will suffer social engineering tricks in the forms of masquerading chatting and messages. Let us take a compromised social networking site for example. Hackers may masquerade as a legitimate user to defraud other users' information, to ask them run a certain malware (e.g. a Trojan) which is subtly disguised as an attractive application; or to send them messages containing a link to a malicious site. These are generally referred to as targeted phishing. Since people are usually not alert to friends or acquaintances, such masquerading could lead to unpredictable consequences.

Web Mail. For an individual user, websites which provide e-mail service always store user information like user names, passwords, contact lists, mails, etc. In case of a complete compromise in which all the information is stolen, the seriousness of a large scale masquerading could be no less than that of the case of the social networking site previously mentioned. Fortunately, this kind of complete compromise is not common for e-mail service providers. However, even partial information could be taken advantage of. Suppose now that a shoddy hacker merely obtained all user names of a web mail site, without one single password or any other information. Then, he/she can do three things: 1) Earnestly apply some password guessing mechanisms or just a brute-force attack with all the user names hoping to discover more information which might contributes to a further in-depth penetration (e.g. the emails of the staff might contain more internal information about the website). 2) Accurately pour spam to these real e-mail addresses instead of enormous lists of potential addresses, many of which are artificially fabricated and do not truly exist. These are generally labeled as untargeted phishing. 3) Simply sell the e-mail addresses obtained for profit.

In practice, 1) and 2) could be performed in parallel. Hackers always prefer performing a thorough exploitation of the obtained information by means of 1) and 2), and this process can last for months or even years until ultimately, the value of the original data is drained out. Then, the data become useless and are prepared to be sold, namely 3). As long as the data are not openly and freely available, with high probability, the buyer of this "useless" data will repeat the process again, so on ad infinitum.

3. The Hackers

Literatures have proposed many different schemes to classify hackers. We shall not enumerate them here. The community of hackers is divided into three main types separated by motivation [9]. The first class is good hackers who voluntarily share security weaknesses in a computer system or network in a way that will allow the system owners to fix the breach, instead of taking malicious advantage of it. The second class is bad hackers who hack for notoriety, namely, they hack in pursuit of fame and the

accolades of their cohort. The third group of hackers is greedy and they are driven by nothing but profits.

In order to gain a better understanding of the hacker economy industry, we draw on some fundamental notions of ecology and further divide greedy hackers into three categories.

3.1 Apex Predators

Apex predators reside at the top of the hacker economy industry and play a crucial role in maintaining its normal operation. They are familiar with all kinds of popular computer systems on the market, specialized in discovering the vulnerabilities of websites and operating systems, proficient in malware manufacturing, and so on. Generally, they spend a lot of time dealing with technical issues and do not have sufficient time to directly make use of the exploits and malware they created. Thus, they sell the exploits and malware for profit. Occasionally, they directly attack some websites in order to obtain user information which will lead to more penetrations. In the hacker economy, these valuable commodities dominate the market and can only be provided by apex predators. Hence, it is not hard to see that apex predators, who are knowledge-intensive participators, could gain the maximum profit. Undoubtedly, they are the dominators and driving force of the hacker economy industry, and naturally, small in number.

3.2 Skilled Hunters

Conventionally, skilled hunters are the buyers of exploits and malware, since they themselves, are not capable of creating these commodities. They are experienced in building attack sites with malware planted in or just phishing sites. Because they have relatively more time than apex predators do, they often initialize various attacks on appropriate websites with the bought exploits. In most cases, they are desperately in pursuit of user information, since user information means potential profit and opportunities to expand their business. Generally, skilled hunters could obtain moderate profit in the hacker economy industry. Because less expertise than apex predators is required, the number of skilled hunters is medium.

3.3 Inferior Scavengers

Inferior scavengers rely on advertising for profit, mainly in the form of e-mail. Most inferior scavengers have little professional knowledge. They merely purchase data containing e-mail addresses from skilled hunters or even apex predators. When Internet aggressively creates novel business schemes, spam become a by-product of this creation. As of August 2010, the amount of spam was estimated to be around 200 billion per day [10]. More than 97% of all emails sent over the net are unwanted, according to a Microsoft security report [11]. As a globally recognized problem, spam is low in cost, high in profit, subtle in concealment. Moreover, it is also a medium for untargeted phishing. Due to the low technique content and the minimum profit, inferior scavengers are the last gainer of the hacker economy industry and large in number.

4. The Hacker Economy Industry

4.1 Operations

An overview of the sophisticated operations of the hacker economy industry is shown in Fig.1. There are four areas: hackers, user computer, malicious sites, and unmalicious sites. Hackers and users are denoted by circles. User computer, malicious sites, and unmalicious sites are bounded by dotted lines. A dash dotted arrow represents sensitive user information and its flow direction. A solid line arrow stands for actions or results. Users are directly suffering from information stealing, malware installation, adware advertising, targeted/untargeted phishing, spamming, many of which could cause financial losses. Moreover, the user computer might be used for launching DDoS attacks. In general, hackers are able to obtain user information from phishing sites, spyware, Trojan, and unmalicious sites.

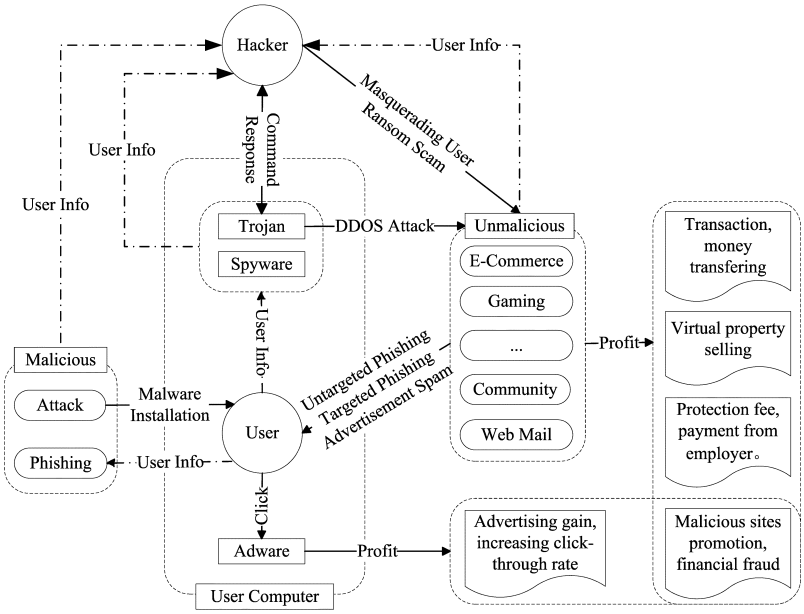

Fig. 1. Operations of Hacker Economy

Profit can be made in many ways. One approach taken by hackers is ransom scam. Demands for payment to stop DoS attacks or refrain from publishing stolen data on the Internet are often made against companies. Ransom scam is

risky, since it is based on a direct financial contact between hackers and victims. There is a variant of ransom scam, in which hackers launch DoS attacks against a website A, and get paid from an employer B, where A and B are competitors. In order to completely avoid risks of direct contact with victims, hackers usually prefer to sell malware, exploits, and stolen data on the black market. Nowadays, more and more malware such as adware, spyware, and Trojan programs are sophisticatedly manufactured with a profit motive in mind, the prices of which are proportional to the functionality and complexity. In most cases, malware are targeted at personal users, while exploits often aim to companies. The creation of exploits is based on vulnerabilities. Both security engineers and hackers are able to detect hidden flaws of an existing system, but the consequences will be entirely different. The former will notify the company which produced the system, so that patches or security updates can be promptly made. The latter, however, will take advantage of the vulnerability for exploit creation. Undoubtedly, zero-day exploits are of the most value. Stolen data, which is another commodity, usually contain sensitive information such as trade secrets, credit and debit card numbers, user names, passwords, e-mail addresses and phone numbers. As is shown in Fig. 1, the leakage of user information is the primary loss suffered by users, together with the consequent economic losses. Hackers could easily make profit through transaction, money transferring, virtual property selling, financial fraud, malicious sites promotion, advertising, etc.

4.2 Hierarchy

Fig.2 illustrates a structure similar to the pyramid showing relationships among hackers and users. From the top down to the bottom, the number of members at each layer increases. The bottom of the pyramid represents users, which is the only prey to all the three kinds of greedy hackers in the hacker economy industry; and undoubtedly, the number of users is much larger than the sum of all the above layers added together. Each layer can make profit from all layers below it. As far as each hacker is concerned, the one in the lower layer makes less profit than those above him. Apex predators not only dominate the operation of the industry, but also control the future direction of development. To some extent, skilled hunters and inferior scavengers are just followers of apex predators. As all industries need pillars, this industry is no exception. It is obvious that the whole industry is based on users, so the pillar of the hacker economy industry is the user information.

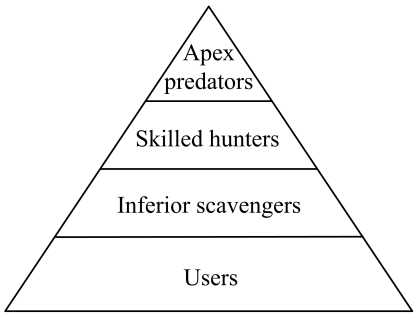

Fig. 2. Hierarchy of Hacker Economy

4.3 Countermeasures

As illustrated in Fig.3, the link between hackers and users can be established through three ways. Under the premises made in Section Malicious Sites, hackers could easily obtain user information by building malicious sites or delivering malware to user computers. If we make the opposite assumption, namely 1) users are conscious of unusual phenomenon appeared in their computers, and 2) there are several anti-virus mechanisms in user computers and the actual effectiveness of existing anti-virus protection is excellent. As a result, hackers will have to directly attack unmalicious sites in order to obtain user information. Now, if we make assumption 3), unmalicious sites are well protected and user information will never be stolen by hackers. Then, there is no link between users and hackers. Namely, users are in isolation from hackers. However, it is hard to coordinate unmalicious sites, security software manufactures, users and law enforcement. Unmalicious sites cannot guarantee to be able to resist the attacks from hackers. Security software cannot absolutely safe-guard a computer system. Users suffer from lacking of professional knowledge and negligence. The existing legal provisions are not sufficient and the law enforcement is facing a lot of technical difficulties.

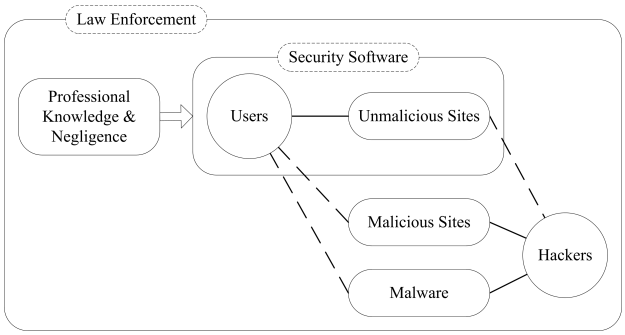

Fig. 3. Links Between Hackers and Users

5. Case Study

5.1 The Case Study Context

In order to illustrate our work, we present a case study in this section. The countermeasures mentioned above are based on the following three assumptions:

1) users are conscious of unusual phenomenon appeared in their computers, 2) there are several anti-virus mechanisms in user computers and the actual effectiveness of existing anti-virus protection is excellent, and 3) unmalicious sites are well protected and user information will never be stolen by hackers.

Since we cannot influence the unmalicious sites on the Internet, our case study is concerning the former two assumptions. The case study is carried out in a computer room of Xidian University. We chose 40 computers and divided them into four groups: GA, GB, GC, and GD. Each group consists of 10 computers. On the computers in GA and GB, we installed two kinds of anti-virus software which have good reputation. While on the computers in GC and GD, we checked the existing applications and uninstalled any security-related software. The students who came to this computer room are randomly chosen to use the computers in the above four groups. However, a half of the chosen students are educated with professional knowledge and given a check list to improve their consciousness of unusual phenomena appeared in a computer. We divided these students into two equal groups: SA and SB. For another half of the chosen students, we did nothing but divided into two equal groups: SC and SD. Before we started our experiment,

we checked the 40 computers thoroughly in order to make sure that there is no malware. The computers in GA, GB, GC, and GD are used by students in SA, SC, SB, and SD, respectively. The four combinations denoted by E1, E2, E3, and E4 are depicted in Table III.

Table III: Combinations of Users and Computers

E1	GA–protected SA – educated
E2	GB – protected SC – not educated
E3	GC – not protected SB - educated
E4	GD – not protected SD – not educated

5.2 Experimental Results and Analysis

The whole experiment lasted three months. The total number of students in SA, SB, SC, and SD is 3821. The average numbers of Adware, Spyware, and Trojan per PC are illustrated in Fig. 4, Fig. 5, and Fig. 6, respectively. The overall trends of the curves of E1, E2, E3, and E4 are the same. The combination E1 shows the best performance concerning three malware, while the combination E4 shows the worst performance. The performance of combination E2 and E3 are between E1 and E4. Moreover, the curves of E2 and E3 are close to each other. This indicates that a combination of a student who is not educated and a protected computer shows similar result with a combination of a student who is educated and a computer which is not protected. In a word, the best situation is that a protected computer is used by an educated student.

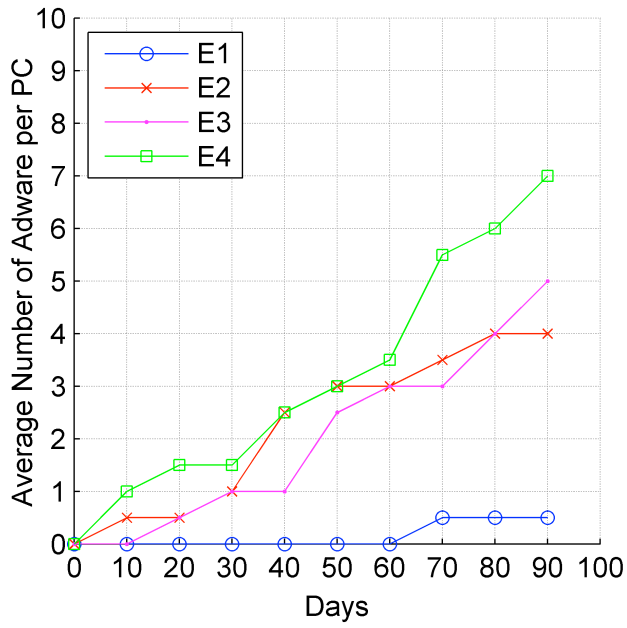

Fig. 4. Average Number of Adware per PC

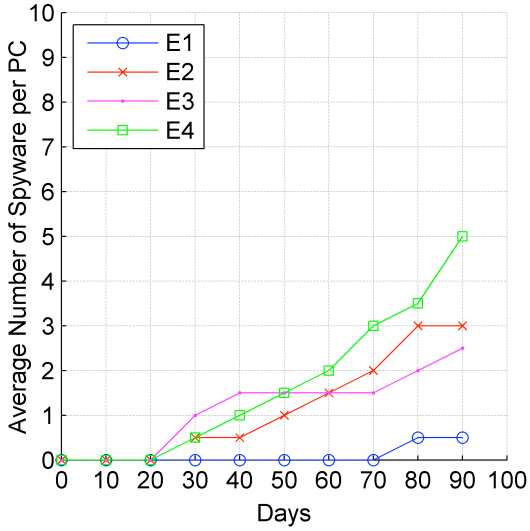

Fig. 5. Average Number of Spyware per PC

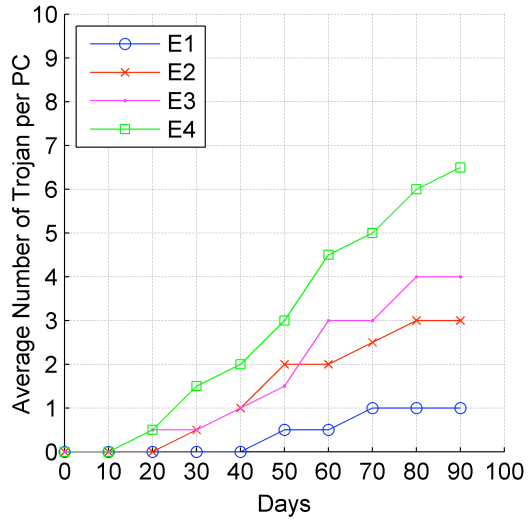

Fig. 6. Average Number of Trojan per PC

6. Conclusion

Concerning the contents considered in this paper, we come to the following conclusion. User information is leaked either through unmalicious sties or the vulnerabilities of user system. The security of user computers guarantees that user information cannot be obtained by malicious sites or malware. Similarly, the security of unmalicious sites ensures that user information cannot be obtained directly by hackers. As shown in Fig. 3, once these two conditions are achieved, users will be completely isolated from hackers. With the absence of user information, the scale of hacker economy industry will shrink dramatically. Nevertheless, there does not yet exist—and probably never will—a universally practical solution that can protect user information in all possible contexts. The pursuit of guarding user information, still a long way to go, deserves more efforts both technically and legally.

Acknowledgment

This work is supported by the Key Program of NSFC-Guangdong Union Foundation under Grant No. U1135002; Major national S&T program under Grant No.

2011ZX03005-002; National Natural Science Foundation of China under Grant No. 60872041, 61072066; and the Fundamental Research Funds for the Central Universities under Grant No. JY10000903001, JY10000901034.

References

1. B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Communications of the ACM*, 47(4), , 2004, pp. 75-78.
2. B. Donohue, "HBGary CEO Speaks Out On Anonymous Hack," Threat Post, 23, Mar. 2011; Available: http://threatpost.com/en_us/blogs/hbgary-ceo-speaks-out-anonymous-hack-032311
3. K. J. Higgins, "Attackers Steal Major Retailers', Financial Firms' Customer Email Data," Dark Reading, 4 Apr. 2011; Available: http://www.darkreading.com/database-security/167901020/security/attacks-breaches/229400828/attackers-steal-major-retailers-financial-firms-customer-email-data.html
4. E. Peralta, "In Hack, PlayStation Users' Credit Card Data Might Have Been Compromised," NPR, 26 Apr. 2011; Available: http://www.npr.org/blogs/thetwo-way/2011/04/26/135747338/sony-says-playstation-users-credit-card-data-might-have-been-compromised
5. M. Fossi, D. Turner, E. Johnson, T. Mack, T. Adams, J. Blackbird, S. Entwise, B. Graveland, D. McKinney, J. Mulcahy, C. Wueest, In: Symantec Global Internet Security Threat Report. Trends for 2009. Technical Report, Symantec Corporation, Cupertino, 2010.
6. O'Kane, Philip, Sakir Sezer, and Kieran McLaughlin. "Obfuscation: The hidden malware." *Security & Privacy, IEEE 9.5*, 2011, pp. 41-47.
7. Raftopoulos, Elias, and Xenofontas Dimitropoulos. Technical report: Shedding light on data correlation during network forensics analysis. Technical Report 346, 2012.
8. Lei G, Xin G. Social Network Analysis on Knowledge Sharing of Scientific Groups. *Journal of System and Management Sciences*, 2011, 1(3), pp.65-73.
9. P. T. Leeson and C. J. Coyne, "The economics of computer hacking," *Journal of Law, Economics and Policy*, 1(2), 2005, pp. 511-532.
10. J. Halliday, "Email spam level bounces back after record low," The Guardian, 10 Jan. 2011; Available: http://www.guardian.co.uk/technology/2011/jan/10/email-spam-record-activity
11. D. Waters, "Spam overwhelms e-mail messages," BBC News, 8 Apr. 2009; Available: http://news.bbc.co.uk/2/hi/technology/7988579.stm