DOI 10.15302/J-SSCAE-2016.06.017

Current Cybersecurity Situation and Emergency Response of Cybersecurity

Liu Xinran[1], Li Baisong[2], Chang Anqi[2], Lu Hui[3], Tian Zhihong[4]

1. National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China
2. Antiy Labs, Harbin 150000, China
3. Institute of Microelectronics, Chinese Academy of Sciences, Beijing 100029, China
4. Institute of Computer Application, China Academy of Engineering Physics, Mianyang 621900, Sichuan, China

Abstract: Based on the current situation and the emergence of recent cybersecurity threats, this article presents cybersecurity features to tackle such threats. Updated attack methods, enhanced attack technology, and an expanded attack scope have changed emergency management. The core technology and security assurance in the existing emergency management mechanisms are relatively backward. Learning from conventional emergency response systems for improving the current emergency technical measures becomes a significant part of cybersecurity. In this paper, the authors propose a multilinkage elimination method that can mobilize system strength and protect the system and mechanism against cybersecurity threats.
Keywords: cybersecurity; threat; information security; emergency response; emergency response system

1 Introduction

With the continuous development of information technology, cybersecurity is facing many challenges, and companies are gradually paying more attention to cybersecurity. Therefore, works related to emergency response are critical. The situation of cybersecurity emergency has changed in recent times, and the current scope of emergency not only includes the network but also important information content. With the evolution of threats, cybersecurity emergency is facing many challenges.

Overall, the emergency management organizations of cybersecurity incidents include national government and nongovernment organizations as well as local nongovernment organizations. Emergency response systems are beginning to be established at the lower level, for example, emergency response centers regarding security vendors, Internet companies, and e-businesses. Nevertheless, the new generation of cybersecurity threats spread very rapidly, with a wide area of attack; the threat coverage is beyond our imagination, affecting mobiles, personal computers (PCs), websites, applications, and social media. The occurrence of unexpected events results in increased trials and difficulties in works related to emergency response.

Cybersecurity issues have become more prominent in the 21st century, and the occurrence of threat activities has become more frequent, for example, the massive distributed denial of service (DDoS) on Yahoo in 2000, Code Red and DDoS on global root domain servers in 2001, SQL Slammer in 2003, Sasser in 2014, Nimaya in 2006, Stuxnet in 2010 [1], advanced persistent threat-threat on Cobalt Strike (APT-TOCS) [2], Hacking Team breaches, commercial mobile phone Trojans (such as Biige in 2015), and the increasingly active ransomware in 2016. All these issues encompass the types of information security events and demonstrate the following features.

1.1 Organization and benefit of attacks

Cyberattacks not only aim to demonstrate the unmatched skills of attackers but also embody a kind of commercial purpose

Received date: 8 October 2016; **revised date:** 20 October 2016
Corresponding author: Liu Xinran, National Computer Network Emergency Response Technical Team/Coordination Center of China, Researcher. Major research fields include network and information security, distributed computing etc. E-mail: lxr@cert.org.cn
Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)
Chinese version: Strategic Study of CAE 2016, 18 (6): 083–088
Cited item: Liu Xinran et al. Current Cybersecurity Situation and Emergency Response of Cybersecurity. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.017

to obtain economic benefits through organized groups. Attackers are straightforward about their actions, and their organization significantly enhances their ability to destroy various sites and information systems. Moreover, economic benefits-based objects further enlarge the harm caused by cyberattacks.

1.2 Evolution of attacking methods

Conventional attacks usually employed rootkit, virus infection, and other means; however, new ideas, technologies, and methods of cyberattacks, including phishing, social engineering, driven-by download, zero-day, and redirections, are emerging continuously. These constantly emerging newer attacks have increased the difficulty of analysis and technical disposal of cybersecurity and information security incidents.

1.3 Tools and platforms of attacking technologies

When it comes to conventional advanced persistent threats (APTs), we will associate with elite operation teams, the infrastructure for attacks, zero-day vulnerability discovering teams, and malicious code writing teams. However, in APT-TOCS events, attackers remotely control a target host by relying on an automated attack testing platform of Cobalt Strike to provide a new attacking vector to countries and organizations with limited technical capacity and resources. This approach reduces the attack costs; however, the highly stereotyped attacks lack distinctive genetic characteristics, and hence become more difficult to trace. This further complicates the implementation of effective emergency response.

1.4 Spread of attacking targets

In addition to conventional websites and information systems, domain name systems, e-mail systems, industrial control systems, personal terminals, smart phones, and wireless networks have all become the targets of cyberattacks. In addition to the well-known vulnerabilities of Windows, Linux, Unix, iOS, and Android operating systems and application software, security threats have spread to areas such as smart cars, smart homes, wearable devices, and smart cities.

2 Management status and problems of emergency response

Since information technology has penetrated into the aspects of government management, business operation, and the life of the masses, its yearly development has become an important basis for normal social operations. The failure of information systems to solve problems will directly affect the normal functioning of social management and services.

2.1 Complex environment both at the local and global levels

In recent years, there have been complicated and profound changes in the world. The international financial crisis of 2008 continues to significantly impact the world. The world economy is slowly recovering, and the development of differentiation, the pattern of international investment and trade, multilateral investment, and trade regulations require significant adjustment; further, the development of countries is facing grim problems. China's top-level strategy of the Belt and Road Initiative fully relies on the existing bilateral and multilateral mechanisms of China's partner countries, and actively develops economic cooperation partnership with these countries based on the existing and effective regional cooperation platform [3]. International economies and trade strategies are intertwined, and the application level of the Internet has increased; this reflects fierce international cooperation and enhanced cyberforce when countries are working together.

2.2 Shortage of core technology and equipment

The rate of adoption of foreign technologies and products by domestic networks and information systems including the information systems of prominent departments is high. However, many problems still exist: the technical level and supply infrastructure do not match, and a significant gap exists between domestic and foreign capabilities. For example, the United States has a strong technical force, including monitoring systems for hardware production and manufacture, operating systems, and the market share of chips across the world; thus, its ability to obtain information is unmatched.

2.3 Relatively backward information security level

In China, the overall information security level is relatively backward. Although local governments at all levels have begun to realize the importance of information security, problems still exist in the implementation of specific tasks, such as slow emergency response and incomplete implementation of national requirements. In addition, there are inadequate talent and investment in this field. The independent monitoring data from the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) shows that there were more than 105 000 Trojans and botnets at the control side in 2015. They controlled more than 19.78 million hosts in China, and malicious programs forwarded more than 660 000 emails to users. Personal information disclosure is frequent. Thus, vulnerabilities of network equipment security show significant risks; moreover, they are showing an increasing trend [2].

In 2014, China established the Office of the Central Leading Group for Cyberspace Affairs, which is in charge of coordinat-

ing major issues of cybersecurity and informatization. The State Council restructured the Cyberspace Administration of China and authorized it to be responsible for nationwide administration of Internet information and supervision of law enforcement. On April 19, 2016, President Xi Jinping held a symposium on cybersecurity and informatization to explore the measures and methods to implement cybersecurity [4] and emphasized the importance of the work regarding cybersecurity and informatization during the 13th Five-Year Plan period. During the investigation of old industrial bases in the northeast, President Xi Jinping visited Antiy Technology Co. Ltd., in Harbin, demonstrating that China has ascribed immense importance to cybersecurity.

The data breaches caused by cyberattacks in the last year remain rampant. Moreover, a complete chain of interests was formed based on the information leakage, and the breached information can be used in gang swindle, phishing, or precision marketing. Among the information leakages caused by malicious code, the XcodeGhost [5] event is notable. Up to September 20, 2015, the cumulative statistic shows that 692 infected applications, including WeChat, Didi Taxi, NetEase Cloud Music, and other popular applications, have been confirmed [6]. This event adopts a method of unofficial supply chain infection, which can reflect the deficiencies in the research and development of China's Internet companies and security awareness.

Currently, in China, the emergency management of information security has made definite progress; however, the emergency plan is still deficient considering the overall situation. It lacks practicability and maneuverability in practical applications. Apart from China, other major Internet or network-developed countries have developed national cybersecurity strategies [7]. National cybersecurity strategies are frequently introduced, mainly owing to the rapid development and popularization of the Internet, and governments, key infrastructure, businesses, and citizens are heavily dependent on the reliable function of networks. Cybersecurity problems could seriously endanger the operation of government and enterprises and significantly affect social life. It can be concluded that cybersecurity is the lifeline of a country's prosperity and development. The reasonable setting up of an emergency response system for information security and the maximal reduction of the negative impact of information security events by using limited input will become an urgent challenge.

In the aspect of emergency response systems of cybersecurity, China has initially formed a national emergency response system for cybersecurity, which is under the leadership of the Ministry of Industry and Information Technology, considering the CNCERT/CC as the core, based on the various Internet backbone enterprises, and supported by emergency service support units [8].

With the economic development, China has made a preliminary attempt at formulating laws and regulations on information security; however, there is still scope for improvement compared to developed countries. The complexity and cross-region characteristics of the Internet require the emergency response for cybersecurity incidents to be collaborative for multiple departments and units; this requires all the departments and emergency response organizations to integrate their respective merits and identify a leading department of emergency response based on the roles of their departments in the emergency response. The leading department is responsible for guiding the work related to the entire emergency response. Nonstandard cyber behavior is the most important factor among cybersecurity risk causes. However, only relying on cracking down on cybercrime and illegal behavior to solve the cybersecurity problems is not adequate. It is necessary to fully utilize the strategic pass of cybersecurity supervision and to fully utilize administrative measures. Currently, the entire emergency response system of cybersecurity has many problems, such as time lag, doubts regarding its effective implementation, insufficient operability of emergency plans, lack of linkage between various emergency departments, lack of emergency drills, professional skills, and overdependence on national emergency platform [9,10].

3 References of emergency response of cybersecurity in conventional fields

The emergency response systems in conventional fields include emergency response systems for enterprise production safety accidents, public disaster safety accidents, and conventional safety events in the field of public health. The relevant laws, regulations, and related operational techniques have been established in various fields and have achieved some technological innovation. The security in the conventional fields includes the security of the construction of an emergency system for national public infrastructure under a real environment, and the key aspects of cybersecurity defense are computer viruses and hacker crimes. In addition to protecting the equipment and system security, data security should also be protected. Fast, efficient, and comprehensive response should be considered in cybersecurity and other fields. Starting from the development of cybersecurity emergency response systems in conventional fields, China should sum up the advanced experiences for the development of emergency organization mechanisms, command systems, and rescue teams, and utilize these experiences as guides to construct cybersecurity emergency response systems at the high level (national institutions), middle level (Internet data center, content distribution network, e-businesses, and industry executives), and low level (netizens) to establish an emergency system for cybersecurity.

The following systems should be established in the construction of cybersecurity emergency response systems: ① organization mechanisms referring to a command and management department for national cybersecurity emergencies and corresponding emergency institutions in provinces, municipalities,

autonomous regions, and localities. ② Command systems including emergency and communication command systems at different levels; systems for monitoring, prevention, and early warnings; information sharing mechanism, incident reporting mechanism, and notification mechanism. ③ Professional rescue teams including national, provincial, and institutional emergency teams. The analysis on these four types of emergency systems is shown in Table 1.

4 Measures

In summary, under the current grim cybersecurity situation and increasing cybersecurity threats, the emergency response system faces significant challenges during its steady construction. The strengthening and improving of the emergency response system to solve the challenges of cybersecurity is critical and urgent.

As the targets of emergency response to cybersecurity in recent times have changed, and objects requiring emergency response have increased, the system and multilateral cooperation require redeployment to eliminate threats in a timely manner and prevent their adverse impact by guaranteeing the safety of system and mechanism. As such, the following conclusions can be drawn.

4.1 Assist with defense in cybersecurity incidents; urgent and fast control with focus on service in peacetime

During cybersecurity incidents, assistance should be provided to defense systems and services. That is, emergency response systems should consider securing the safe operation of military network as priority to assist the military network in planning and cutting off the public Internet network when necessary. Urgent and fast control is required in the event of large-scale attacks. The spreading of events, understanding of the development trends, estimation of the scope, and formulation of emergency response measures should be finished in the shortest possible time to mitigate the loss. Further, the focus should be on service during peacetime; emergency response should ensure Internet security and a timely response to the general cybersecurity events during peacetime.

4.2 Perform systematic confrontation during emergency response

Multidimensional systems including legal systems, mechanisms, personnel, capital, technology, and other aspects should be established, and the state apparatus should be utilized to implement cybersecurity emergency. The goal of the emergency response is not only limited to the determination of the source of harmful foreign speeches but also to deter a large number of people from attempting attacks to achieve the aim of reduction in the macro index.

4.3 Clarify the responsibilities and obligations of cybersecurity and information security

Each entity in real space has its own rights and obligations,

Table 1. Analysis on four types of conventional emergency systems.

Emergency system	Notification mechanism	Nature of the accident	Command system
Public health emergency	• Notification contents: the spread scope of events and protection measures, etc. • Notification objects: government departments at all levels, medical institutions, and individuals	Generally, the spread scope is wide; it is necessary to mobilize throughout the country; and it can easily cause panic	National, provincial, and local emergency command platforms
Fire emergency	• Notification contents: the spread scope of events and incurred losses, etc. • Notification objects: the whole society	Generally, the spread scope is small, and regional event types vary	Only provincial and local emergency command platforms
Electric power emergency	• Notification contents: the spread scope of events and time of eliminating electricity interruptions, etc. • Notification objects: government departments at all levels as well as individuals	The spread scope is wide and mainly causes economic losses	• Building a system of prevention, prediction, monitoring, and early warnings • Emergency information command system
Nuclear safety emergency	• Notification contents: the spread scope of events, incurred losses, and influence scope, etc. • Notification objects: all levels of government departments, medical institutions, and individuals	The spread scope is small but the impacted time is long; and will be harmful to the environment and public health	• Establishing a national nuclear emergency command center • Nuclear emergency command centers exist in provinces and regions where nuclear power plants are located

as does the cyberspace. Every entity should strive to maintain the normal operation of cyberspace. In addition, each network entity has the right to require countries to provide a normal and safe cyberspace, and its duty is to maintain cyberspace security.

The legislation for cybersecurtiy and information security must clarify the legal responsibility of behaviors that endanger the safety of state and public networks and provide legal conditions for the investigation of offenders. First, in the case of illegal acts, it will accordingly regulate the civil, administrative, and criminal liabilities to clarify their corresponding responsibilities. Second, the cohesion among civil, administrative, and criminal liabilities should be handled appropriately. Illegal behavior that does not yet constitute a crime shall bear civil or administrative liability according to the law. Third, a transfer system should be established. Destructive behaviors that already constitute a crime should be transferred to judicial organs to provide criminal sanctions, thus avoiding the substitution of fines for criminal punishment. Finally, all the network operators have the duty to maintain user information security, and whoever fails to fulfill their obligation to protect the cybersecurity and information security shall bear the corresponding legal responsibilities.

4.4 Improve organization system and strengthen the emergency rescue system for cybersecurity

An emergency response agency should be established and should be led by the Office of the Central Leading Group for Cyberspace Affairs. This is an emergency command agency and will be used by the central government to handle particularly serious emergency public events. It can guide, coordinate, and uniformly supervise emergencies in network infrastructures, emergencies in public infrastructure information systems, emergencies in the cyber information management, and other works regarding cybersecurity emergencies. An emergency response linkage mechanism among the different networks, systems, and departments should also be established to properly integrate the functions of various emergency management departments.

4.5 Implement the administrative executive capability and law enforcement power in terms of mechanism

First, website owners should be forced to hire security personnel (such as a chief security officer; CSO) and install safety equipment. The CSO should have relevant qualifications, undergo professional training at the relevant training organizations for safety during an emergency, and provide official proof of competence.

Second, unified hosting sites for country prefix websites, such as .gov and .edu, should be established. A considerable amount of traffic data should be centralized. This facilitates safety testing.

4.6 Transform the “emergency response after incidents” to “emergency response in and before incidents”

First, it is necessary to issue probes during peacetime, monitor key objectives when abnormal situations are detected, and analyze source IP. It is also important to query the QSO log from the operators and build a honey pot target. When attackers attack the honey pot, it not only records the detailed process but also counters the attack by using loopholes.

Second, in addition to monitoring network devices, QQ, Taobao, WooYun, and other commonly used applications should also be monitored to collect data and discover abnormal phenomenon as much as possible to determine identifiable information and capital chain of the attackers, and to share information with the stakeholders in a timely manner.

4.7 Carry out regular national cybersecurity emergency drills

Internet is a high military and civilian integration environment. Thus, although it is better to insist on prioritizing both military and civilian concerns, it is also better to coordinate the requirements of peacetime and wartime. To achieve the goal of “defense assistance during wartime, focusing on the service in peacetime, and rapid emergency control,” it is essential to reinforce emergency drills to ensure that the cyberspace security system can operate efficiently in an emergency state. Additionally, it is important to formulate a scientific, effective, and rapid response emergency mechanism to ensure stable operation of the crucial information systems. Accordingly, work groups for national, provincial, and municipal cybersecurity emergency drills should be established to formulate the cybersecurity rules, schedule the security investigation, and eliminate the cybersecurity risks in a timely manner. The formulation and implementation of contingency plans for all the levels of cybersecurity incidents can facilitate in the reporting of cybersecurity incidents in a timely and accurate manner.

5 Conclusions

This paper introduced and detailed the severity of the current cybersecurity situation and importance of emergency response work in the context of the Internet. We analyzed the main source of the threats and characteristics of the attack patterns. In addition, we summarized the management situation and problems in the current cybersecurity emergency response, and listed the measures to be adopted. As shown, the current cyberattack methods are constantly being updated compared with the previous types of attacks. Thus, the works related to emergency response

should be adjusted and improved in a timely manner to cope with various threats.

References

[1] National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC). Siemens announced to repair the vulnerability utilized by Stuxnet worm [EB/OL]. (2012-7-25) [2016-10-8]. http://www.cert.org.cn/publish/main/98/2012/20120725152801904458081/20120725152801904458081_.html. Chinese.

[2] National Computer Network Emergency Response Technical Team/Coordination Center of China. China Internet network security report of 2015 [R]. Beijing: Posts & Telecom Press, 2016. Chinese.

[3] Chu Y, Gao Y. Three issues on the strategic orientation of China "One Belt One Road" [J]. International Economic Review, 2015 (2): 12–13. Chinese.

[4] Xinhua News Agency. A speech by Chinese President Xi Jinping at the symposium on network security and informatization work [J]. China Information Security, 2016 (5): 22–31. Chinese.

[5] National Computer Network Emergency Response Technical Team/Coordination Center of China. Alert about unofficial apple XCODE contain malicious code [EB/OL]. (2015-9-30) [2016-10-8]. http://www.cert.org.cn/publish/main/12/2015/20150914152821158428128/20150914152821158428128_.html. Chinese.

[6] Computer Emergency Response Team of Antiy. Analysis and review of Xcode unofficial supply chain pollution incident (XcodeGhost) [EB/OL]. (2015-9-30) [2016-10-8]. http://www.antiy.com/response/xcodeghost.html. Chinese.

[7] Yuan C Y, Du Y J, Zhou W, et al. US "national network emergency response plan" and its reference significance [J]. Secrecy Science and Technology, 2012 (5): 35–37. Chinese.

[8] Liu Y L. Network and information security emergency response system construction of China [J]. Energy Technology and Management, 2012 (3): 164–165. Chinese.

[9] Research group of network security. Problems and solutions of network security emergency response system in China [J]. E-Government, 2014, 139 (7): 20–25. Chinese.

[10] Xie X H. Construction of emergency mobilization information management capabilities based on cyberspace [J]. National Defense Science & Technology, 2015, 36 (1): 55–57. Chinese.