International Journal of Security and Its Applications
Vol. 10, No. 6 (2016) pp.181-192
http://dx.doi.org/10.14257/ijsia.2016.10.6.18

Forensic Analysis of MERS Smishing Hacking Attacks and Prevention

Soon-ho Moon[1], Dea-woo Park[2]

[1, 2]*Department of Convergence Technology, Hoseo Graduate School of Venture*,
[1]*nanmoonsh@naver.com* ,
[2*]*Corresponding Author : prof_pdw@naver.com*,

Abstract

In June 2015, Smishing text and malicious code designed to take advantage of the confusion caused by the Middle East Respiratory Syndrome(MERS-coV) appeared. The Korea Internet & Security Agency(KISA), says recent MERS-related information is used for Smishing text messages with the malicious code disguised as a document being circulated via e-mail attachments. Because the infection following attached e-mails intends to remotely control the system of the infected PC, there is a possibility to cause that further damage may result. This study aims to analyze the Smishing text and malware contents, and the form of hacking attacks taking used to take advantage of the confusion caused by MERS.

Keywords*: hacking, forensic, smishing*

1. Introduction

After a 60-year-old man visited a Middle Eastern country and returned to Korea, he was diagnosed as a MERS patient on May 20, 2015, and contributed to spreading the disease rapidly. As of July 6, 2015, 33 deaths from MERS were reported, and people, fearing infection by the spreading disease, began to refrain social activities [1].

Korea is a strong country in terms of Internet services. Use of smartphones on the Internet in Korea marks the highest level in the world. However, the side effect of the cyber world is the propagation of phishing, pharming and smishing [2].

Smishing is based on text messages. The principle of damage resulting from smishing incidents is described below. A hacker sends messages in SMS(Short Message Service) to a targeted user. As soon as the targeted user clicks the attached link, it causes the application with malicious code to be downloaded. The hacker distributes malicious code like Trojan horse to targeted user's smartphone while the user is not aware of it. The hacker then acquires text messages, reception alarm, camera, phone numbers, financial information, and personal information in the smartphone through the malicious code or malicious application, while controlling the functions of the smartphone. The hacker masquerades as the targeted user to use user's personal information to cause financial damages through banking approval. A smishing attack for inducing installation and execution of a malicious application(masquerading APP Store) through SMS. Victims of the attack are installed with the malicious application 'APP Store'. The victims are displayed with a message "Error: installation fails. Because the file is corrupt, you cannot use it. Check it in the homepage". When the victims click the link connected with the URL, the message that asks deletion of the application is displayed. In this case, although any one of Ok and Cancel is pressed, the malicious function is executed. The text message sent to the victims is then sent to the hacker to conduct hacking [3].

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2016 SERSC

Therefore, execution of smishing contributes to automatically installing malicious code in user's smartphone so that hacking attack including information stealing and deletion can operate by means of SMS. When the application is further executed in user's smarphone, a false text message is displayed as if the application is corrupt to show a plurality of messages, and as if the user deletes the corrupt files in person. However, the real malicious application is not deleted, but continues to operate through the device manger to attempt stealing mobile phone user's personal information and banking details [3].

Taking advantage of social confusion caused by epidemics, for example, MERS, hackers steal information through smishing hacking attacks against smartphones in a social engineering [4] method, targeting people's uneasiness, and threatening financial damages.

This study aims to describe smishing hacking attacks that take advantage of the confusion caused by the current spread of MERS in Korea. The details, analysis of, and actions against the attacks, that is, the MERS Smishing in the cyber world are described.

In this study, analyzed details of MERS Smishing attacks are provided to generate a forensic investigation report which provides a legal basis and study, using e-mails and smartphone forensic evidence, on how MERS Smishing hacking attaches may be prevented. The result of this study will provide essential technical data for people's cyber safety, and to prevent loss and damage.

2. Related Studies

2.1 Smishing Attack

Smishing is short for SMS, and Phishing is a means of sending text messages to a user to trick the user in a social engineering manner. When the user clicks the application link URL(Uniform Resource Locator) included in the text message, a malicious code is automatically installed on the user's device to steal the user's personal information or banking information while the user is not aware of the taking. The attacker who steals the user's banking information causes financial transactions to result in damages, for example, by making small amount payments or financial transfers from the user's account [5].

Table 1. illustrates smishing attacks of which the percentage is more than 9%, among spam text messages, including URLs, sourced from the data for the first quarter of 2015, by KISA(Korea Internet & Security Agency) [6].

Table 1. Smishing attack ratio among spam text messages (including URLs) in first quarter of 2015

	JAN.	FEB.	MAR.	Total
SPAM SMS (including URL)	3,074,071	3,068,611	1,279,974	7,422,656
Smishing	120,597	570,291	13,293	704,181
Percent(%)	3.92	18.58	1.04	9.49

Copyright ⓒ 2016 SERSC

2.2 Forensic Investigation Technology

Forensic is defined as “forensic science” or “forensic justice”, originated from “of a forum or by a forum”, meaning “legal” or “of a court” [7].

Although the main stream of forensic investigation technology is based on hair, fingerprint, DNA and sperm collection, the digital forensic investigation technology is now main stream, thanks to current developments in IT technology and a changing information-intensive society. Digital forensics refers to submitting digital data to legislative institutions by using forensic investigation tools and equipment or analyzing facts if various digital devices including computers, smartphones or mobile phones are used in crimes [8].

Although digital forensic investigation is generally carried out, it may be slightly different, depending on involved institutions or incidents. Digital data are easily copied, fabricated, forged and deleted. In courts, there is an issue related to truthfulness of digital evidence because it can be easily modified and forged. Digital forensic investigators must be able to prove that there is no defect or failing, for example, forgery or change [9].

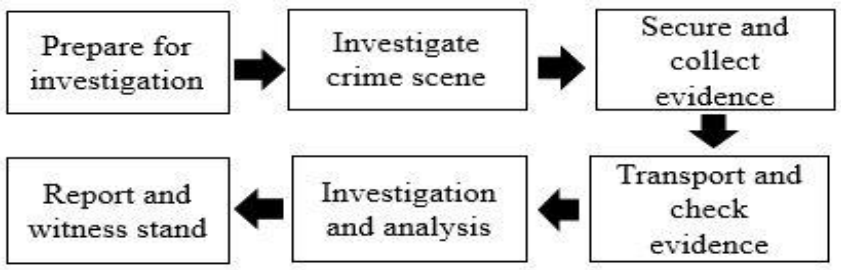

Figure 3. Model for digital forensic investigation

An exemplary smishing attack by smartphones(Sample Figure 1) is to send a text message to trick a victim in a social engineering technique, for example, winners for gift, hot issues in the society, or mobile wedding invitation cards to guide the victim to click the included URL. The damage may be caused by just one unconscious click. While more and more people use smartphones, more caution is therefore required to avoid smishing attacks.

Figure 1. Exemplary text for smishing attack (content: MERS, Please check soon. http://mrrs-cov.xxx , MERS patients grant application guidance. Message Size 1KB. Download)

While recent smishing attacks are evolving, the most smishing attacks were made under disguise of public institutions to instruct something compulsory, accounting for 58%. The text messages under disguise of public institutions citing legal articles make victims mistake they are from public institutions.

Copyright ⓒ 2016 SERSC

2.3 Smishing and Hacking Attack

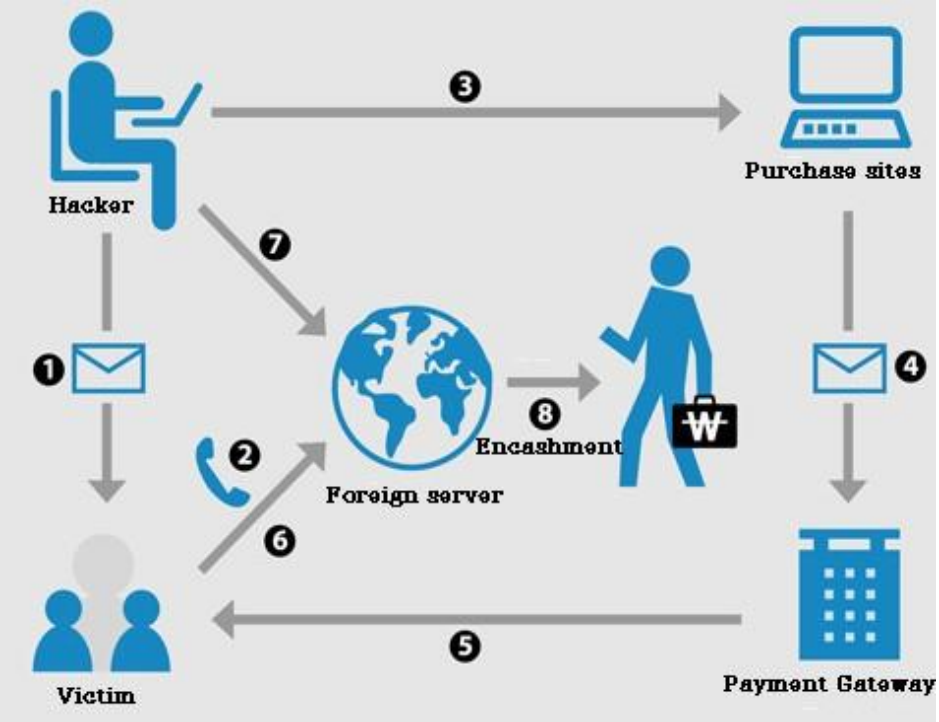

Figure 2. Smishing generation structure[10]

Smishing is a social engineering hacking attack as shown in Figure 3 and described as follows[10]: ① A malicious app producer sends a text message for installing the malicious app to specific users on the basis of personal information collected in advance => ② The victim unconsciously clicks the URL included in the text message to install hacker's app and result in infection with malicious app => ③ The hacker steals information from the victim's terminal infected with the malicious app to send it to foreign servers => ④ The hacker carries out small amount payment for services in Internet purchase sites, for example, game sites => ⑤ A numeral text for approving the user identity is sent to the victim's mobile phone through a payment agency from the purchase site => ⑥ The mobile phone is operated not to show the received numeral text by the malicious app installed in advance => ⑦ The mobile phone is operated not to show the received numeral text by the malicious app installed in advance => ⑧ The malicious app sends a text message for the approval number to the foreign server by stealth => ⑨ The hacker intercepts the approval number collected by the server to carry out normal purchase process => ⑩ The hacker illegally encash the acquired cyber money to make unfair profits.

3. Analysis of MERS Smishing Attack

The following illustrates the contents of MERS Smishing hacking attacks taking advantage of the cited MERS during to its propagation in June 2015 in Korea.

Copyright ⓒ 2016 SERSC

3.1 MERS Smishing Attack through e-mail

Figure 4. E-mail file taking advantage of MERS (content: Here is a MERS hospital and patient list. Check it now MERS hospital and patient list docx.exe)

As shown in Figure 4, hackers used the social engineering technique, for example, “Here is a MERS hospital and patient list” or “MERS, check it now”, to send e-mails to a plurality of random people. The attack file attached to the e-mails was an MS Word .exe file, named as “MERS hospital and patient list.docx.exe".

Curious and concerned users receiving the e-mails check the e-mail would click the attacked file which automatically downloaded the malicious code. If their PC was then infected with the malicious code, the hackers could remotely control the PC.

Figure 5 shows an analysis of MERS Smishing through e-mail. The attacker can remotely control victim’s computer with the malicious code, steal and send personal information, and capture financial information while the victim is unaware of the theft. If their PC is infected with the malicious code, the hackers can remotely control the PC.

Copyright ⓒ 2016 SERSC

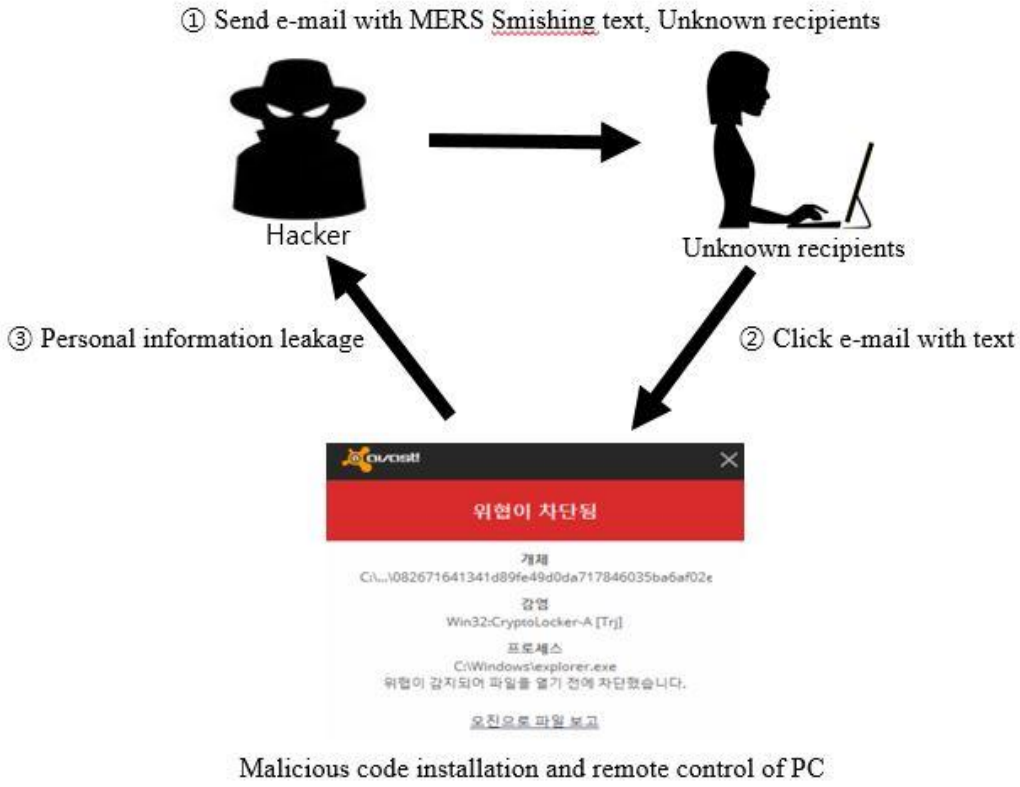

Figure 5. Flow chart for MERS Smishing through e-mail

3.2 MERS Smishing through Smartphone

Hackers use their smartphones to masquerade as an acquaintance and send the MERS Smishing text shown in Figure 6 randomly to a plurality of unspecified people. The smartphone users get curious about the smishing text and may click the link included in the MERS text immediately to which then installs a malicious app. The malicious code is then used to steal personal information and information for financial transactions from the victim's smartphone.

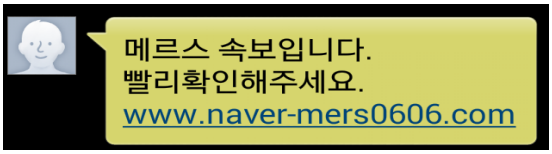

Figure 6. MERS text smishing in smartphone (Breaking news about MERS. Check it now. www.naver-mers0606.com)

Hackers use smartphone user's personal and banking information they stole from the victims to do financial damages by stealth, or control victim's smartphone to steal.

Figure 6 shows the MERS-related smishing attack text sent as an e-mail by way of smartphones. MERS text smishing attacks also show how MERS Smishing by uses social engineering methods.

Copyright ⓒ 2016 SERSC

3.3 Countermeasures against MERS Smishing Attack

When a smishing text is sent to a smartphone or e-mail address, communication service providers or security service providers collect the text to analyze and verify it through the smishing countermeasure system and the malicious app as shown in Figure 7.

For subsequent measures, the Internet Crime Investigation Center of KISA sends an emergency statement, for example, a request for blocking the malicious app, to each communication service provider, to public institutions and enterprises to business and other so that they can take measures to prevent damage and loss.

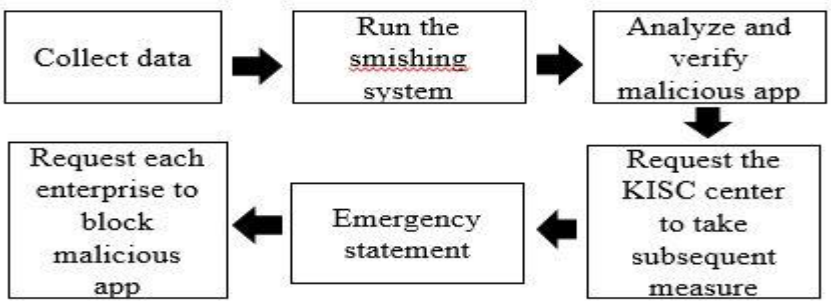

Figure 7. Flow Chart for Tackling MERS Smishing Attack

4. Forensic Analysis of MERS Smishing Attack

4.1 Forensic Investigation about MERS Smishing Attack through e-mail

Forensic investigation of MERS Smishing attacks through e-mail mail includes the acquisition and analysis of evidence, including e-mail senders and recipients, time of sending and receiving and details of the mail. The forensic investigation tool, Encase6 Enterprise, is used to analyze the MERS Smishing attacks through e-mail.

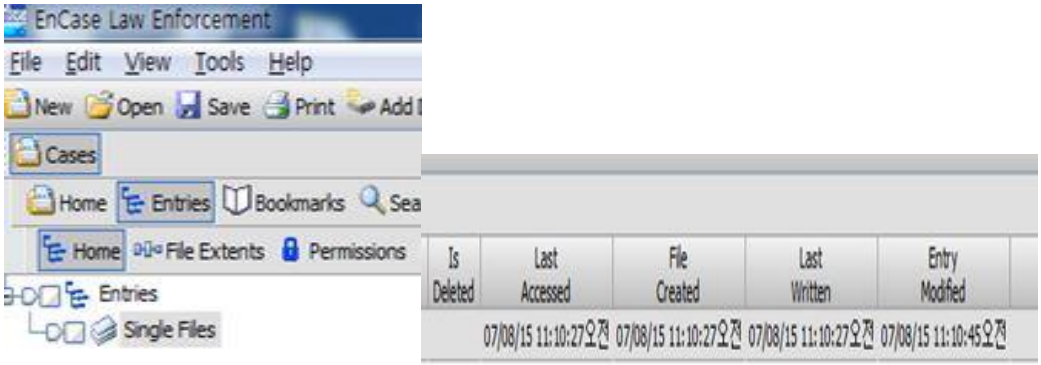

Figure 8. Analysis of malicious code in MERS e-mail by Encase

■ Analysis system :
Processor-Intel (R) Core (TM) i3 CPU,
RAM-4 GB,
OS-Microsoft Widows 7 - 32bit,
HDD-Samsung HD502IH (500 GB)
■ Forensic investigation tool :
Encase6 Enterprise

Copyright ⓒ 2016 SERSC

4.2 MERS Smishing Forensic Investigation by Smartphone

The tool Oxygen 2014 was used for forensic analysis of MERS Smishing attacks in Android smartphones to extract information for logical and forensic analysis.

Forensic evidence data were extracted from the Android operation system which is Samsung mobile phone Galaxy Note 2. The system backup was carried out in a PC through smartphone synchronization.

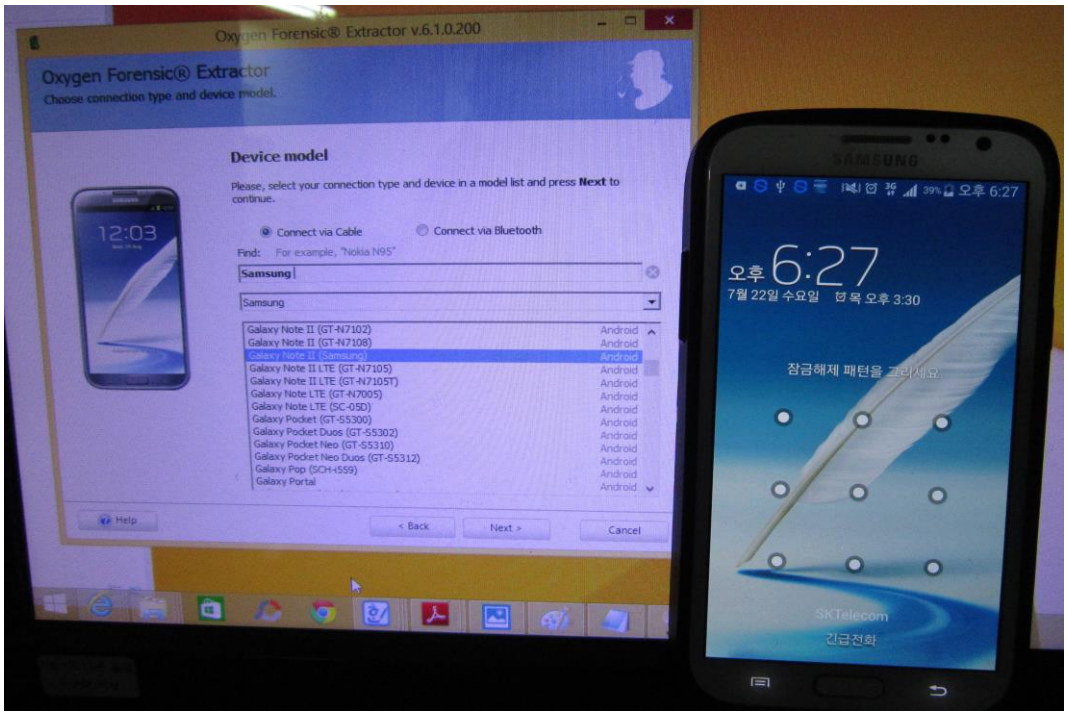

Figure 9. Proving and analyzing forensic evidence integrity by using Oxygen Forensic Suite 2014

Figure 9 shows a photograph of a screen with smartphone time and background to show the date and time for proving integrity while transferring the MERS text collected from Galaxy Note 2 to a PC. This is because the Korea Standard Time is used for all smartphone time background screens. The environment used for forensic investigation of MERS Smishing attacks through smartphones is described below.

■ Smart Phone :
Samsung Galaxy Note 2,
■ Communication program:
Samsung Kies
■ Analysis System :
Processor-Intel (R) Core (TM) i7-2630QM CPU,
RAM-8 GB,
OS-Microsoft Widows 7, 64bit,
HDD-Samsung HD502IH (500 GB)
■ Forensic Investigation tool:
Oxygen Forensic Suite 2014

 Copyright ⓒ 2016 SERSC

4.3 Making Forensic Investigation Report

After collecting evidence through forensic investigation of MERS Smishing attacks, it is necessary to make a forensic investigation report as investigation data, to be used as an evidence of the attack in a court of law.

<Form No.4>

Digital forensic

Forensic Investigation Report

● Date of investigation: JUL. 22, 2015 ● Institution: Seoul Metropolitan Police Agency ● Investigator: Senior Policeman Moon Soon-Ho (check)

1. Information about Investigation

Date of receipt	Support No.	Management No.	Date of Analysis	Place of Analysis
JUN. 8, 2015	2015 Support No.3	2015 Evidence No.3-5	JUN. 8, 2015 ~ JUL. 22, 2015	Forensic Research Center for Hacking Attacks, Hoseo Graduate School of Venture

2. Information for Investigation

Manufacturer	Model	Operating System	Serial No.	Storage Capacity	Routing
Samsung	Galaxy Note 2	Android 2.3	353930052548857	32G	X

3. Data Extraction Method for Investigation and Forensic State

Forensic extraction	● SYN / ○ JTAG / ○ Revolving
Forensic state	○ Normal / ● Partial (part) deletion / ○ Initialization / ○ Micro 3D

4. Forensic Investigation Tool

Forensic investigation tool	● Oxygen / ○ FTK imger / ○ UFED / ● Encase
Other analysis tool	Samsung Mobile Kies V2.0
Evidence collection	MERS Smishing e-mail and text was acquired and analyzed. The smartphone tools for forensic investigation Oxygen Forensic Suite 2014 and Encase6 were used for imaging work.

5. Proving Originality

Original Hash value	d3d2232f2b083c799ee33cdf8a204c5b
Copied Hash value	d3d2232f2b083c799ee33cdf8a204c5b

Figure 10. Forensic Investigation Report for Smishing Attacks through Smartphone

Figure 10 shows the report on analysis of text messages and e-mails, and the results of the forensic investigation of MERS Smishing attacks for this study by using the forensic investigation tools and devices. When a forensic investigation report is made, it is necessary to print and submit it for an evidence in a court.

Copyright ⓒ 2016 SERSC

For proving originality and integrity of the evidence data in forensic investigation of MERS Smishing attack, the values from Hash function were extracted to compare the values from the Hash function with the evidence data copy in order to prove the integrity of original data, and to show that the digital evidence was not falsified and fabricated. This is done to prove they are the same values.

5. MERS Smishing Prevention

The KISA has built and operated a smishing action system since January, 2014, to tackle smishing attacks. In addition, the KISA has various technical methods, for example, engaging more individuals in the service to block text by stolen telephone numbers in an effort to prevent hackers from using the telephone numbers of public institutions and enterprises; essential installation of the smishing blocking app when releasing all smartphones by Korean smartphone manufacturers; and the registration system of text service providers through the Internet by revising the Telecommunications Business Act.

Figure 11. Smartphone Environment Setup–security (content: Unknown source - Deselect, Check before app installation - Select)

For preventing MERS Smishing attacks and avoiding damages by the attacks, ① deselect the item " Unknown sender" in the smartphone security setting (Android OS) and select OK before app installation as shown in Figure 11. ② Do not click the URL included in a SMS sent by unknown sender. ③ Install a mobile vaccine provided by a public institution, carry out regular precise inspection and update. ④ Set the limit of small amount payment through a smartphone as a minimum amount (call the customer center of each communication service provider to change the limit with call center staff members). ⑤ Be sure to download and install apps from a known, formal market.

Smishing attacks can be avoided by checking e-mail senders or updating the latest versions of vaccines.

 Copyright ⓒ 2016 SERSC

It is necessary that the government, communication service providers, and financial institutions establish schemes for ensuring budgets and providing teams for positive public relations, as well as prevention plans so that smartphone users can avoid smishing hacking attacks

6. Conclusion

Smishing hacking attacks using a typical social issue as a basis for the attacks. This study aims to analyze MERS Smishing attacks through e-mails and smartphones, extract forensic investigation data to be used as an evidence for smishing attacks in a court, and to compare Hash function values to prove originality and integrity, and to establish and verify evidence.

As preventive steps, smartphone users should not be curious about texts sent by unknown senders or click links (URL) attached to unknown text messages. Users are advised to establish a Not to Allow gate for "app sent by unknown sender" on the smartphone.

It is necessary to further analyze MERS Smishing attacks in iPhones and to study how best to tackle the attacks.

Acknowledgments

"This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) Funded by the Ministry of Education in 2016"(No. 2013R1A1A2010118).

References

[1] Korea Centers for Disease Control and Prevention 15.07.06 09:00 government figures http://www.mers.go.kr/mers/html/jsp/Menu_B/content_B1.jsp?cid=26740, (2015) July.

[2] Dea-woo Park, "Forensic Analysis of Smishing Hacking Attack in Smartphone", INFORMATION, vol. 7, no. 11(B), (2014) November, pp. 5683-5688.

[3] In-woo Park, Dea-woo Park, "A Study of Intrusion Security Research and Smishing Hacking Attack on a Smartphone", Journal of the Korea Institute of Information and Communication Engineering, vol. 17, vo. 11, (2013) November, pp. 2588-2594.

[4] Soon-ho Moon, Dea-woo Park, "Study on MERS Smishing Hacking Attack for Forensic Analysis and Blocking ", Asia Workshop on Information Commuincation Engineering , (2015) August, pp.75-78.

[5] In-woo Park, Dea-woo Park, "A study of Intrusion Security Research and Smishing Hacking Attack on a SmartPhone", The Korean Society of Computer And Information vol. 17, no. 11, (2013). November, pp. 2588-2594.

[6] Korea Internet and Security Agency 2015 the first quarter, Smishing analysis, http://www.krcert.or.kr/kor/data/reportView.jsp?p_bulletin_writing_sequence=22685#none, (2015) July.

[7] Gyu-an Lee, Dea-woo Park, Cheong-shim Ko, "Digital Forensic", GSintervision, Seoul, South Korea, (2012) April.

[8] Phil-Joo Moon, "On the Availabiltiy of Anti-Forensic Tools for Androdid Smartphones", The Journal of the Korea Institute of Electronic Communication Science, vol. 8, no.6, (2013) June, pp. 856-857.

[9] Kyung-Bae Yoon, Woo-Sung Chun, Dea-Woo Park, "Forensic Evidence of Search and Seized Android and Windows Mobile Smart Phone" The Korean Society of Computer and Information, vol. 17, no. 2, (2013) February, pp. 328-330.

[10] Dea-Woo Park, Analysis of Mobile Smishing Hacking Trends and Security Measures, Journal of the Korea Institute of Information and Communication Engineering, vol. 19, no. 11, (2015) November, pp. 2615~2622.

Copyright ⓒ 2016 SERSC

Authors

Soon-ho Moon : he is a Policeman of Seoul Metropolitan Police Agency, South Korea. Mr. Moon received the B.S. degree in Police Administration from the Seoul Degital University in 2013. And he received the M.S. degree in Inforamtion Protection from the Sejong Cyber University Graduate School in 2015. And he He is currently enrolled in Hoseo Graduate School of Venture, Korea being in a PhD. His research interests are Digaital Forensic, Hacking, Smishing, e-Discovery, Information Protection, Cyber Law, Big-Data and Network security.

Dea-woo Park : he is an Associate Professor at Hoseo University

in South Korea. Professor Park research of the Hacking Forensic, Information Technology Communication in Lab at Hoseo Graduate School, Professor Park received the B.S. degree in computer science from the Soongsil University in 1995. And he received the M.S. degree in 1998. He received the Ph.D. degree from the computer science department of the Soongsil University in 2004. He has also been appointed, Secretary General of Forum of National CyberSecurity Policy, and Chair of Korea Information Security Forum. Professor Park has been appointed Vice-Chairman of Korea Institute of Information Security & Cryptology, Korea Information and Communications Society, Korea Digital Forensic Society

Copyright ⓒ 2016 SERSC