ICCT 2015
"The 5th International Conference on Convergence Technology 2015"

Date: June 29 – July 2, 2015
Place: Chateraise Gateaux Kingdom Sapporo Hotel, Hokkaido, Japan
Co-organized by:
- Korea Convergence Society
- Korea Institute of Science and Technology Information
- The Korean Association for Comparative Government
- The Society of Digital Policy & Management
- Convergence Society for SMB
- Kyung Hee University, Well-Dying LAB
- Korea Mobile Enterprise Promotion Association
- DAEHAN Society of Industrial Management

Sponsored by:

Korea Convergence Society
http://www.kcons.or.kr
Session 5-C (SW Visualization (SE Center))

Chair R. Young Chul Kim (Hongik Univ.)

• 13:00-14:20

Tuesday June 30, 2015

01. W-13-01_Hybrid Visual Security Analysis to Prove Vulnerability for Safety / 262
Seok Mo Kim (Dankook Univ., Korea), Sang Eun Lee (Software Engineering Center, Korea), Su Nam Jeon (Software Engineering Center, Korea), Young B. Park (Dankook Univ., Korea)

02. W-13-02_Compatibility Enhancing Agent for Managing Software Toolchain / 264
Eun Seung Lee (Dankook Univ., Korea), Young Soo Kim (Software Engineering Center, Korea), Byungho Park (Hongik Univ., Korea), Young B. Park (Dankook Univ., Korea)

03. W-13-03_A Visualized Blocking Method against a Hidden Malware in the Image / 266
Byungho Park (Ministry of National Defence, Korea), R. Young Chul Kim (Hongik Univ., Korea), Young B. Park (Dankook Univ., Korea), Daechool Shin (Korea e-Government Exp. Associations, Korea), Young Soo Kim (NIPA, Korea), Sang Eun Lee (NIPA, Korea)

04. W-13-04_A Guideline for Realization on extracting automatic size maturity level of diverse component via Source Codes / 268
Jun Sun Hwang (Hongik Univ., Korea), R. Young Chul Kim (Hongik Univ., Korea), Sang Eun Lee (NIPA, Korea)

05. W-13-05_Design of a Framework of 3D Geofence and Geocode / 270
Jun Cho (Gangneung-Wonju National Univ., Korea), Kihyun Kim (Gangneung-Wonju National Univ., Korea), Jinhyung Park (Gangneung-Wonju National Univ., Korea), Sungjin Cho (Gangneung-Wonju National Univ., Korea), Byungkook Jeon (Gangneung-Wonju National Univ., Korea), Sungkuk Cho (Gangneung-Wonju National Univ., Korea)

06. W-13-06_Design of a Temporal Geofence System / 272
Kihyun Kim (Gangneung-Wonju National Univ., Korea), Jun Cho (Gangneung-Wonju National Univ., Korea), Jinhyung Park (Gangneung-Wonju National Univ., Korea), Sungjin Cho (Gangneung-Wonju National Univ., Korea), Byungkook Jeon (Gangneung-Wonju National Univ., Korea), Sungkuk Cho (Gangneung-Wonju National Univ., Korea)

07. W-13-07_Extracting Designs via Code on Reverse Engineering / 274
Haeun Kwon (Hongik Univ., Korea), Bokyung Park (Hongik Univ., Korea), R. Young Chul Kim (Hongik Univ., Korea), Sang Eun Lee (NIPA, Korea)

08. W-13-08_Extracting performance factors against performance degradation through Code Visualization / 276
Geon-Hee Kang (Hongik Univ., Korea), R. Young Chul Kim (Hongik Univ., Korea), Sang Eun Lee (NIPA, Korea), Su Nam Jeon (NIPA, Korea)
A Visualized Blocking Method against a Hidden Malware in the Image

1 Byungho Park, 2 R. Young Chul Kim, 3 Young B. Park, 4 Daecheol Shin, 5 Young Soo Kim, 6 SangEun Lee
1, 2, 3, 4, 5 First Author, Ministry of National Defence, Seoul, Korea, sunsonbob@naver.com
2, 3, 4 Dept. of CIC, Hongik University, Sejong, Korea, bob@selab.hongik.ac.kr
3, 4 Dept. of Computer Science, Dankook University, Korea, ybpark@dankook.ac.kr
4, 5 Korea e-Government Exp. Associations, Seoul, Korea, dcschin04@nate.com
5, 6 Corresponding Author NIPA, Seoul, Korea, {ysgold, selee}@nipa.kr

Abstract In the Internet, we conveniently download the image file which doesn’t know whether it contains a malicious code or not. Moreover, the Internet Image files are passages which are easy enough to flow in a closed network, and a malicious code, which is secretly inserted into a picture file, can be performed as a malicious offensive code, that is, a hacking code with triggers such as HTML files or JS files.

So, we suggest an idea for safe use with a visualized blocking method of the image file which doesn’t know whether to contain a malicious performance code in a closed network or not.

Keywords: Code Visualization, Malicious Code, Image hacking

1. Introduction

Various information can be taken advantage of on the Internet which is conveniently used, and particularly, pictures are reused by downloading picture files on the Internet easily. They are known to have Steganography to conceal data in a picture, but generally, it does not have an offensive function[3].

This paper identifies how the images, which are created by putting a malicious performance code in the image file, are serious, and for its preparation, it examines image management schemes as far as a general management one which does not need a special control and the inside of a file in accordance with each closed network. Then it investigates the existence of a malicious hacking code, security management which can be used if it is clear, and finally, the possibility of hacking the inside of a picture. It suggests a high security management method to create and store a separate image capture file in order to fundamentally block internal hacking data which may exist by using an image capture tool if clear.

2. Main Subject

Generally, a malware refers to a software or a malicious code which is created with an incorrect purpose or a wrong intention to conduct harmful behaviors, and it also includes a script virus[2].

The following pictures show two images, a clean one and the other including a malicious code respectively.

Fig1. Original picture (smile_w-origin.jpg)
Fig2. The picture containing a hacking code (smile_w.jpg)

As seen, those two images are the same in size and quality of the picture.

<table>
<thead>
<tr>
<th>Image</th>
<th>Date</th>
<th>Size</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>smile_w.jpg</td>
<td>2015-05-17</td>
<td>10K8</td>
<td>JPG</td>
</tr>
<tr>
<td>smile_w-origin.jpg</td>
<td>2015-05-17</td>
<td>10K8</td>
<td>JPG</td>
</tr>
</tbody>
</table>

Fig3. The images are the same between the original and a hacking code

However, they are different in their internal image structures. We show the hexadata code using a hexa editor tool.
So, we suggest an idea for safe use with a visualized blocking method of the image file which doesn't know whether to contain a malicious performance code in a closed network or not. On an important network, an image management plan is performed in the following procedure:

1) A general internet network does not have a special measure.
2) An important security network visualizes a file internally and then uses an image.
3) In a security network of high level, the image file only uses the captured image using an image capture tool.

3. Conclusion

Internet Image files are passages which are easy enough to flow in a closed network, and a malicious code, which is secretly inserted into a picture file, can be performed as a malicious offensive code, that is, a hacking code with triggers such as HTML files or JS files [5].

This paper presents three methods for managing an image file as follows.

A typical internet network can be used without special measures, and an important security network can visualize a file internally to use an image. Finally, in a security network of high level, the image file only uses the captured image using an image capture tool in order to fundamentally block the flow of a malicious code in a closed network.

References