Indian Journal of Science and Technology, Vol 8(26), DOI: 10.17485/ijst/2015/v8i26/84140, October 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Study on a Method Protecting a Secure Network against a Hidden Malicious Code in the Image

Byungho Park[1*], Dukyun Kim[1] and Daecheol Shin[2]

[1]Ministry of National Defense, Seoul 140 – 701, Korea; sunsonbob@naver.com
[2]Korea e-Government Exp Associations, Seoul 121 – 915, Korea

Abstract

On the Web, internet sources not only read and view but also are saved in the computer. In addition, we conveniently download the image file which doesn't know whether it contains a malicious code or not. Moreover, the Internet Image files are the passages which are easy enough to flow in a closed network, but 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 executable JavaScript code. So, we suggest an algorithm for safe use with a blocking method of the image file which doesn't know whether to contain a malicious performance code in a closed network or not.

Keywords: Closed Network, Image Hacking, Malicious Code, Steganography, Stegosploit

1. Introduction

The Internet is often called as the Information Ocean or the Information Treasure because there is something that we want to find such as cute figures, documents, etc. Also, the Internet sources not only read and view on the Internet, but also save your computer. Various informations can be taken advantage of on the Internet which is conveniently used and particularly, pictures can be reused by downloading picture files on the Internet easily in order to detect an internal network from the Internet even though we use a firewall but an image file is made through the firewall without doubt in Figure 1.

Is an image file secure? By Park B [1, 5], an image file also can be used as a hacking file. The normal looking images could hack your computers as seen in Figure 2, a photo of a cute cat needs to be treated carefully before you click on the image to view - it might hack a victim's machine. Especially, an image hacking method is called Stegosploit where the next generation cyber attacks could be made through the Internet images to embed a malware in an image[3].

Recently, hacking methods changed from digital destruction to physical destruction, and the stuxnet is a good sample. Additionally, in case of Korea, in Dec. 2014, Korea Hydro-Atomic power was hacked by North Korea[2]. The hacker insists that the residents should leave there.

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.

In this paper, we suggest an algorithm in order to fundamentally block internal hacking data which may exist by using an image capture tool if clear. This paper is organized as follows, Chapter 2 refers to Steganography vs. Stegosploit, Chapter 3 shows Stegosploit, Chapter 4 suggests a new algorithm for detecting Stegosploit and Chapter 5 is Conclusion.

* Author for correspondence

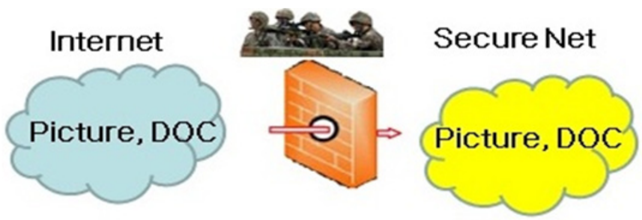

Figure 1. The Internet Image files are the passages which are easy enough to flow in a closed network.

Figure 2. Example of Cute cat figure which contains malicious code[2].

2. Steganography (Hidden Message) vs. Stegosploit (Image Hacking)

What is different between steganography and image hacking? In this paper, image hacking is regarded the same as stegosploit which has been used by Shah to demonstrate the technique during a talk titled, "Stegosploit: Hacking with Pictures", he gave on Thursday at the Amsterdam hacking conference Hack in the Box[1].

2.1 Steganography

It is known that Steganography can convey a hidden message in a picture, but generally, it does not have an offensive function[5]. Until now, Steganography has been used to communicate secretly with each other by disguising a message in a way that anyone intercepting the communication will not realize its true purpose[1]. By Wiki's Steganography[6], it is the practice of concealing a file, a message, an image, or a video within another file, message, image, or video. The word of steganography combines the Greek words Steganos, meaning "covered, concealed, or protected", and graphein meaning "writing". The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages - no matter how unbreakable - arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent as well as concealing the contents of the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside a transport layer, such as a document a file, an image file, a program or a protocol.

2.2 Stegosploit

The next generation cyber attacks could be made through the Internet images using a Stegosploit tool which allows hackers to embed a malware in an image[2]. Stegosploit is the result of a malicious exploitation code hidden within pixels of the image carrying it. The image, however, is a multi format container, which also contains the code required to decode the steganographically encoded pixels to execute the exploitation. A single file can be rendered as a perfectly valid HTML file, executed as a perfectly valid Javascript file, and displayed as a perfectly valid image, all at the same time. Therefore, the exploitation delivery happens through the transmission of pure images. No known means of malware detection have been able to successfully identify these images[1].

2.3 Summary for Steganography vs. Stegosploit

In Chapter 2, we discussed between Steganography and Stegosploit. Generally speaking, Steganography and stegosploit are the same image files, but Steganography is a just hidden massage method by way Stegosploit is a kind of malware[1, 4]. So, a malware refers to 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.

The next chapter will show the image hacking called Stegosploit.

3. Example of Stegosploit

3.1 Making the Stegosploit

Shah's image hacking method[1, 3] can execute in HTML 5 Canvas element whereas our image hacking method can execute a general HTML web browser, and we simply introduce an image hacking file as follows:

- First, program it by python - Open file (in image).
- Second, add a malware code - Javascript file.
- Third, make a simple HTML code.
- Last, just upload web browser. - HTML code.

The following Figure 3 shows how to make image hacking (Stegosploit).

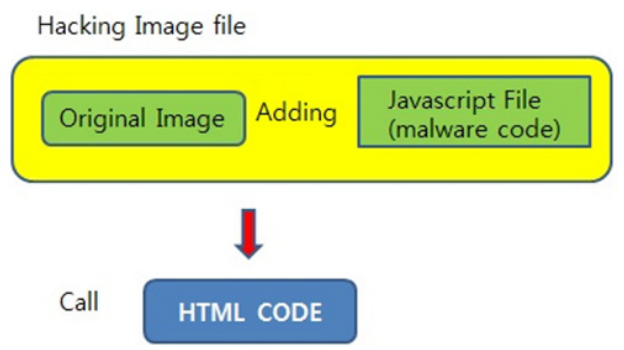

Figure 3. How to make Stegosploit (Image hacking file).

3.2 Example of Stegosploit (Image Hacking)

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

Figure 4. The ordinary original picture (smile_w-orign.jpg).

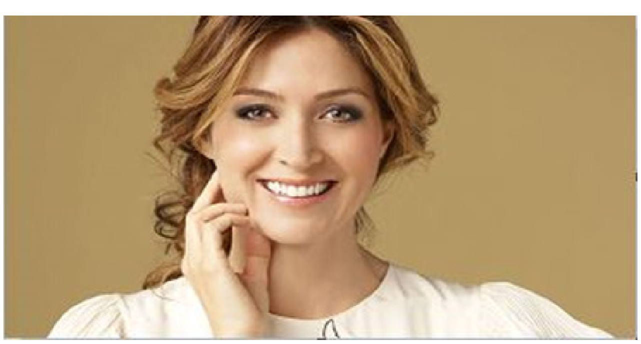

Figure 5. The picture containing a hacking code (smile_w.jpg).

Figure 4 shows the ordinary original picture (smile_w-orign.jpg), but Figure 5 (smile_w.jpg) merely shows the same as Figure 4.

Additionally, those two images are the same in size and quality of the picture in Figure 6.

Figure 6. The images are the same between the original and a hacking code.

However, they are different in their internal image structure, and we show the hexadata code using a hexa editor tool.

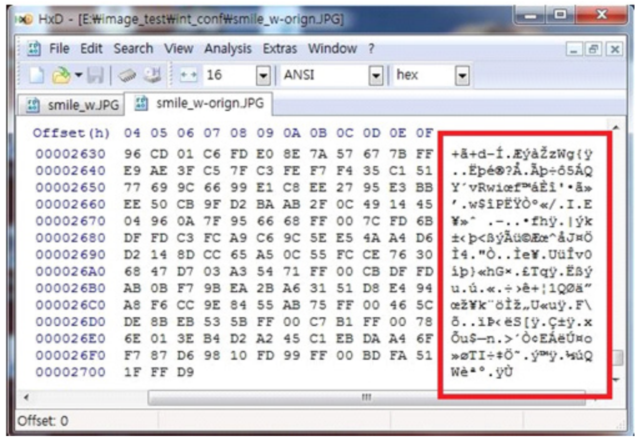

Figure 7. Hexadecimal without a malicious code (smile_w-orign.jpg).

In Figure 7, smile_w-orign.jpg file does not contain a malicious code using a hexadecimal tool, but in Figure 8, smile_w.jpg file contains a malicious code.

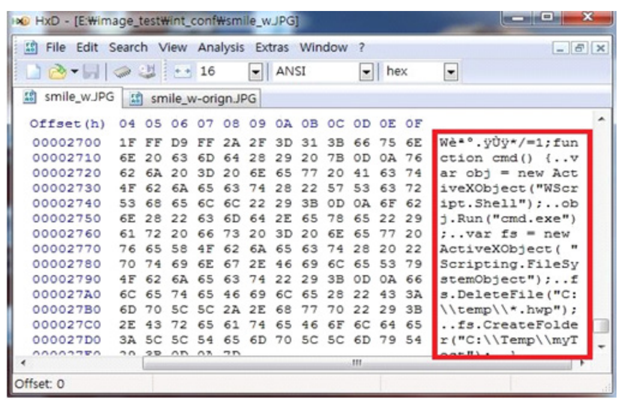

Figure 8. A file containing a malicious code (smile_w.jpg).

In Figure 9, we show the result to exploit the malicious code such as creating a new folder, deleting the hwp files, and executing CMD. Also, in Figure 10, we checked the malicious image with the vaccine program for a detection virus or a malicious code, but they were not detected.

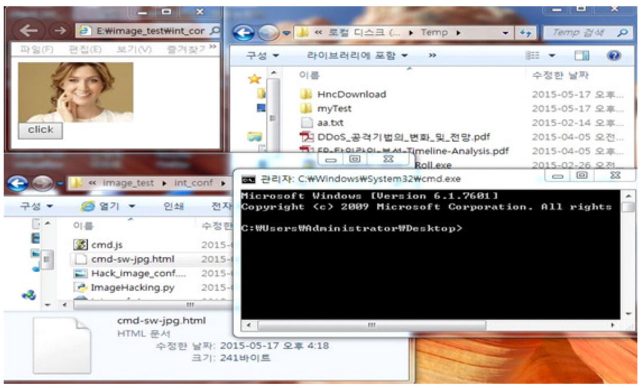

Figure 9. A performed figure (smile_w.jpg).

Figure 10. A figure undetected by vaccines (pills).

4. Detection Method against Stegosploit

4.1 Detection Algorithm

It is necessary to distinguish a normal image from a malicious image file in order to protect a closed network. Which features does a malicious image file include? Obviously, there exists a magic divider to know an image from a malicious code in the file.

We suggest an idea for safe use with a blocking method of the image file which doesn't know whether to contain a malicious performance code in a closed network or not. The following steps show our detection algorithm:

- Read an image file
- Search for Magic number in an image file

ex. In case of Bmp file, "0x42 and 0x4D" means specified BMP file.

- Find "/*" and "*/"

It means to execute as a commet, so this part isn't executed.

- Additionly, exist a code which is malicious code.
- Then, this image file can be decided as a malicious file.

5. Conclusion

The Internet Image files are the 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.

This paper suggested a new algorithm for detecting a malicious code in an image, and especially, the image hacking method is called Stegosploit which the next generation cyber attacks could be made through the Internet images to embed a malware in an image.

6. References

1. Stegosploit: Hacking with Pictures. HITB Sec Conference; Amsterdam; Netherlands: 2015. Available from: https://conference.hitb.org/hitbsecconf2015ams/sessions/stegosploit-hacking-with-pictures/
2. Available from: http://news.chosun.com/site/data/html_dir/2015/03/17/2015031702158.html
3. Available from: http://www.techworm.net/2015/06/spreading-malware-through-images-with-stegosploit-tool.html
4. How to hack a computer using just an image: The hacker news. 2015. Available from: http://www.thehackernews.com/2015/06/Stegosploit-malware.html
5. Park B, Kim RY, Park Y, Shin D, Kim Y, Lee S. A visualized blocking method against a hidden malware in the image. The 5th International Conference on Convergence Technology; Sapporo; Japan: 2015; 5(1):276–7.
6. Available from: https://en.wikipedia.org/wiki/Steganography
7. Cho S, Jeong Y. Introduction to python hacking. Freelec. 2014. p.138–43.