International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 3 Issue 5 May 2016

Steganalysis Application to Detect Image with Malicious Code

Reshma Dharman[1], Ajoy Thomas[2]
Department of Computer Science and Engineering, College of Engineering, Kallooppara[1, 2]
Reshmadharman92@gmail.com[1], ajoythomas11@rediffmail.com[2]

Abstract: *Steganographic attacks are happening repeatedly throughout different conducts. Such attacks are complicated to distinguish as it conceals presence of message itself, they are done through digital media which come out as normal such as MP3, MP4, PNG, JPEG etc. Mainly targets on the passive distribution of malevolent code by hiding in image, these sorts of attacks suggest the call for of application which can examine, discover the presence of malware in image file entering a network.*

Keywords: *Steganography, Steganalysis, Images, Malware, Statistical Steganalysis.*

1. INTRODUCTION

Steganography is utilized to camouflage even the evidence that a message is being transmitted between parties. Steganography employs cover medium, which can be an image, audio file, video file, or any other digital medium which contain noise. The message is implanted into the cover media such that it is unnoticeable to anyone viewing the cover file. In theory, the message can be discovered or derived by the intended recipient who knows that an obnubilated message subsists in the cover medium and how to derive the message. For security the message is often encrypted afore it is embedded.

While steganography deals with camouflaging information the aim of steganalysis is to become aware of and/or guess potentially concealed information from observed data with slight or no facts regarding the steganography algorithm and/or its parameters. While it is likely to propose a realistically good steganalysis method for a specific steganographic algorithm, the extensive goal is to cultivate a steganalysis framework that can function competently slightly for a set of steganography methods.

Recently a team led by Peter Gramantik discovered a backdoor on compromised site. This backdoor didn't depend on the usual form to hide its content but stored its data in EXIF headers of JPEG image. It used innocent function such as exif_read_data and preg_replace PHP is used to read the headers and execute itself. Exif_read_data read images and preg_replace to exchange the content of strings. But, preg_replace consist of a tricky option if you permit the "/e" modifier it will implement the content (eval), rather than examining/replacing. Another fact is that these compromised image load and execute properly on these sites, the attackers altered a legit, pre-existed image from the site. This inquisitive steganographic way to conceal the malware.

Another instance of such events is Stegoloader. Stegoloader could represent an emerging trend in malware DELL Secure Works Counter Threat Unit(CTU) researchers have analysed multiple variant of this malware which stealthy abducts data from compromised site. Stegoloader has modular design and employ steganography to hide its main module's code inside PNG image. Other malware families have used this technique including lurk downloader while CTU have analysed in April 2014.At end of 2014 CTU researchers also noticed the Never request version of gozi Trojan used these kind of technology to conceal information on its backup command and control server, so these examples shows that steganography are used by of malware family and in these scenario image acts as innocent but when the attack is initiated it act as an aid to malicious activities.

These images are not detected by antivirus or IDS.As former is based on virus signature and the images contain new signature for each attack detection is very difficult and later monitors on data packets. When these images are not triggered it operates as a normal image. So it bypasses as it operates as a usual image file. And both antivirus and IDS are deficient perform steganalysis. So there need of application to analyse these images and to attain hidden malicious code.

2. LITERATURE REVIEW

Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt [1] present a study carried out to compare the working of some frequent Steganographic tools distributed online. The tools that used for this study Hide and Seek, S-Tools, Stella, Hide in Picture (HIP), Revelation.

Sruthi Das and Rasmi P [2] give a brief description about steganography and its performance criteria.

Shoniwa, Geogen George [3] discusses the importance of steganalysis tool which can detect the presence of malware embedded in JPEG.

Andreas Westfeld and Andreas Pfitzmann [4] present attacks on EzStego, Jsteg, Steganos, and S-Tools going into details of each utility.

attacked where needed. Jessica Fridrich and MiroslavGoljane [5] recognize several qualitatively different approaches to practical steganalysis – visual detection, histogram analysis, RS steganalysis, universal blind detection schemes.

Sujit Prakash Gujarand C E VeniMadhavan [6] this paper proposes new procedures and technique for detection and analysis of steganographic embedded content. They discuss both statistical and pattern classificatio techniques.

Jan Kodovskýa, TomášPevnýband JessicaFridricha [7] in this paper steganalyze YASS using several recently proposed general-purpose steganalysis feature sets.

3. PROPOSED METHOD

Proposed system is a steganalysis application which can analyse image for malicious code and retrieve the embedded data. These sorts of application are crucial in a network of systems or in a targeted attack.

In this application the image will be loaded, Different steganalysis algorithm will used some of them are chi square attack, visual detection, histogram analysis to check if steganographic artifacts are present these artifacts imply the implementation of steganography. if no artifacts are discovered it implies no usage of steganographic algorithm.

As reported by Westfeld and Pfitzmann the LSBs are not random. They claim it is rare for the pixel value 2k to be equal to the frequency of pixel value 2k +1 in an image with no embedded information. The Chi-squared attack was intended to discover these nearly-equal POVs in images and based on the likelihood of embedding on how near to equal the even pixel values and their matching odd pixel values are in the image. Chi square attack were modified according to different embedding algorithm.

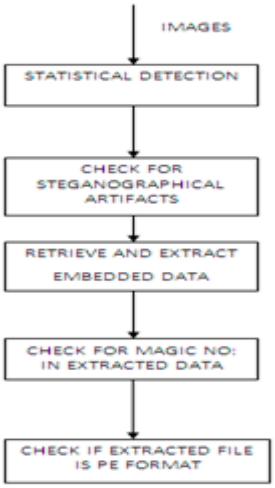

Fig. 1 Detailed Structure

In visual detection by reviewing the repetitive patterns, discovery of concealed information in stego images is possible. These recurring patterns may reveal signature of a steganography tool or concealed information. Even minor distortions can divulge the existence of concealed information.

These statistical test gives an account about statistics of image which implies whether there has been any tampering with the image. Some steganographic techniques generate exclusive and detectable artefacts. For example, Los Alamos scheme19

can be rapidly broken by examining the final row of the stego image since this row provide assistances as a side channel and contains evidence around color pairs adopted for embedding. Gifshuffle22, yields images with randomized palettes, which is also a wary and an easy-to-check artifact. S-Tools pre-process the palette and generate clusters of very near colors that are swapped for embedding.

A simple investigation of the image palette can point to the occurrence of stealthy messages. Its compared with signatures of different steganography tools which help to detect and extract hidden data. For an improved result use database which consist signature of various tools. After extraction of hidden data, the magic number of header is analysed to find the file type. Magic number is unique identification value for each file type. In this paper emphasis given on PE format such as executable. If executable or other PE format is found, Its considered as most risky.

4. CONCLUSION

Attacks through images are prevalent so to inhibit such real time attack which causes disruption in functioning, information stealing or password stealing should be prevented as Antivirus and IDS are not efficient, there is immediate need to address these type scenario, therefore, propose a solution which detect image with malicious code.

ACKNOWLEDGEMENT

We would like to thank god almighty and all the faculty members of college of engineering kallooppara.

REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt, “A Comparative Analysis of Steganographic Tools”.
[2] Sruthi Das N, Rasmi P S,” A Survey on Different Image Steganalysis Techniques”, International Journal of Modern Trends in Engineering and Research,2015.
[3] Robert T. R. Shoniwa, GeogenGeorge,” Design of Application to Detect Images Embedded with Malicious Programs”, International Journal of Science and Research (IJSR),2013.
[4] Westfeld, A. and Pfitzmann, “Attacks on Steganographic Systems”, 3rdInternational Workshop. Lecture Notes in Computer Science, Vol.1768. Springer-Verlag, Berlin Heidelberg NewYork,2000.
[5] Jessica Fridrich, MiroslavGoljan, “Practical Steganalysis of Digital Images – State of the Art”.
[6] Sujit Prakash Gujar, C E VeniMadhavan,” Measures for Classification and Detection in Steganalysis”.
[7] Jan Kodovskýa, TomášPevnýb, Jessica Fridricha,” Modern Steganalysis Can Detect YASS”.
[8] Ross J. Anderson, Fabien A.P. Petitcolas (1999)," On the Limits of Steganography,” IEEE Journal of Selected Areas in Communications, May 1998,16(4):474-481.
[9] Lakhotia, A., & Phoha, V. V. (DEPSCOR FY 09) “Obfuscation and Deobfuscation of Intent of Computer Programs”,2012.
[10] R. Chandramouli and N. Memon, "Analysis of LSB based Image Steganography Techniques", Proceedings of ICIP 2001, Thessaloniki, Greece, October 7−10, 2001.
[11] “Stegoloader”https://www.secureworks.com/research/stegoloader-a-stealthy- information-stealer.
[12] “Malware hidden inside EXIF header” https://blog.sucuri.net/2013/07/malware-hidden-inside--exif-headers.html.
[13] “Base64” https://blog.sucuri.net/tag/base64/.
[14] “Lurk” https://www.secureworks.com/research/malware-analysis- of-the-lurk-downloader