SSI Project Proposal - G1

Steganography & Stegomalware Lab

Group members: Adam Gershenson Nogueira, Carlos Rafael Barbosa Madaleno, Diogo Costa Pinto and Ismael Medeiros Moniz

1. Subject

Our mini-project proposal involves developing an interactive learning approach to digital steganography, steganalysis and CDR (Content Disarm and Reconstruction), also known as file sanitization. Besides giving the users hands-on experience with detecting and applying steganography to files, we want to introduce them to stegomalware as malware payloads hidden via steganography and how these payloads can be:

- extracted and activated by a malicious program;
- prevented with CDR-like techniques;

2. Purpose and comparison with existing resources

While steganography is a relatively niche area of cybersecurity, due to security by obscurity getting less attention nowadays, it has been around since ancient times in physical formats: writing with invisible ink, between the lines of text or music sheets, etc.. Even social steganography is a thing in communities suffering from censorship that have to resort to hiding the true meaning of their messages in banal concepts, for example, the watermelon as a symbol of Palestine.

We believe steganography to be an interesting concept in digital media as well, especially in circumstances where cryptographed content would arouse suspicion or be outright forbidden in certain countries. Hiding cryptographed material in certain image formats for example even has the additional nicety of the payload being hard to distinguish from the uniformly distributed noise in the image data. Steganography practices can also be used for many malicious purposes, which is why we also believe it is important to discuss appropriate detection and prevention mechanisms.

There exist many resources relating to steganography, but not many interactive-format learning resources that discuss both the crafting and the detection of steganographed content, as well as extraction and activation mechanisms for the payload. We believe this is the gap our proposal would fit.

3. Lab plan

The lab plan can be subdivided into roughly 3 tasks. In the first task, we would see the user interact with an image file and examine its binary contents in detail with the aid of tools such as exiftool, binwalk, etc.. With careful inspection it can be seen that the image is in fact composed of two images. The user would then extract the hidden image from the file. This would serve as a gentle introduction to both the structure of image file formats and how they can be inspected for steganography.

In a second task, we would familiarize the reader with the concept of stegomalware as a malware payload transmission mechanism. This task essentially involves two smaller parts:

- Hiding the malware inside an inconspicuous file, such as an image or a document;
- Crafting a simple extractor program living inside the target that would be able to receive the file and execute the malware;

It is worthy of note that the initial mechanism to place the extractor inside the target does not concern the reader. We are only interested in the hiding and extracting of malicious payloads part of the process. As such, we would provide the user with:

- The “malware”: really just a simple script with debugging output, i.e. “You have been hacked”
- Two containers they have full access to. One of the containers would serve the stegomalware, the other container would simulate the victim’s computer and here an appropriately disguised extractor would run the malicious payload. For example, why not craft an extractor named “imv” replacing the well-known image viewing utility in opening the stegomalware?

Finally, we would introduce the readers to CDR practices and other detection methods. These practices are often used in enterprise environments to protect against stegomalware, where human error is a great cause of breaches (downloading weird files…). They do not rely on malware detection: they simply validate the files against the templates and policies provided by the file type vendors. Since few non-proprietary tools exist for CDR implementation, we would be more interested in giving the reader hands-on experience with the following detection methods:

- Comparison with original carrier, which is trivial
- Noise-floor consistency analysis (frequently tools modify the noise-floor (LSB) of the images to embed content)
- Format analysis

4. Tools

Although plenty of fancy steganography tools and analysis suites exist, we wish to actually give users a thorough understanding of what is happening under the hood. As such, whenever possible, we opt for lower-level tools (all open-source) such as:

- Steghide

- hexdump
- exiftool
- bitwalk
- file

For the lab setup, we will be relying on containerization with Docker. It is also expected that the users have some knowledge in languages such as Python and bash scripting.

5. Conclusion and learning results

As a result of completing our lab, we expect readers to have a grasp on file formats, steganography, steganalysis and stegomalware. We think it will amount to a valuable learning experience, mainly due to its historical significance in physical media and current significance in malware transmission. We also hope that these techniques will help spur creativity in the minds of future cybersecurity specialists and allow them to see the craftiness attackers and defenders can achieve.