A Response to the Threat of Stegware

L. Lin, A. Martin, W. Chen, Seth Pierre, Y. Guan and J. Newman

Stegware refers to software, programs or apps that allow insertion of malware into a digital file, such as an image or video, using steganography techniques. Although it has been in action for around 15 years, "steganography" and "stegware" have recently just attracted the attention of law enforcement agencies as the use of stegware appears to be rising [1]. This technique has been used for international economic espionage [2], tracking of photos shared by users on social media platforms [3], and industrial and governmental espionage by hacker groups using PNG images to hide malicious code [4].

The war between the stegware and steganalysis tools is a typical cat-and-mouse game. Although many up-to-date steganalysis tools claim their abilities to prevent steganography by utilizing the most advanced detection algorithms from the academic worlds, such as [5], these tools focus mainly on one or two embedding algorithms and lack support to detect a wide range of stego objects. The capability of these current tools to prevent a stegware attack has never been tested.

In this research, we collect more than 70 stego apps and image steganography software and 10 of the most popular steganalysis tools. We propose a strategy to defend real-world attacks from stegware by combining functions from on-line steganalysis tools and algorithms from recent academic discoveries. We believe this will significantly increase the chance of identifying the threat from stegware by identifying files that have the potential to contain malicious code. Our team is working to develop a prototype of such a comprehensive steganalysis tool that provides user-friendly software for non-experts such digital evidence practitioners. We also summarized the characteristics of the code for many stego apps by reverse engineering and program analysis. The coding characteristics reflect their core embedding algorithms and encryption techniques, allowing us to classify the intent of the app as stegware even before installing it on a mobile phone. Our automatic tool to analyze app code can detect most Android stego apps that implement common spatial domain and frequency domain embedding algorithms with more than 95% accuracy.

To our knowledge, this is the first study to evaluate the performance of most recent steganalysis tools in detecting a large set of stegware. The results will provide valuable guidance to the forensic communities to develop more powerful steg analyzers.

References

1. Stegware–the latest trend in cybercrime, SIMARGL website. Link here.
2. Former GE Engineerand Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets, U.S. Department of Justice, April 2019. Link here.
3. Facebook Embeds 'HiddenCodes' To Track Who Sees And Shares Your Photos, Forbes, July 2019. Link here.
4. Ocean Lotus APT Uses Steganography to Shroud Payloads, ThreatPost, April 2019. Link here.
5. Steganography analysis tool, an online free tool developed by McAfee, Link here.