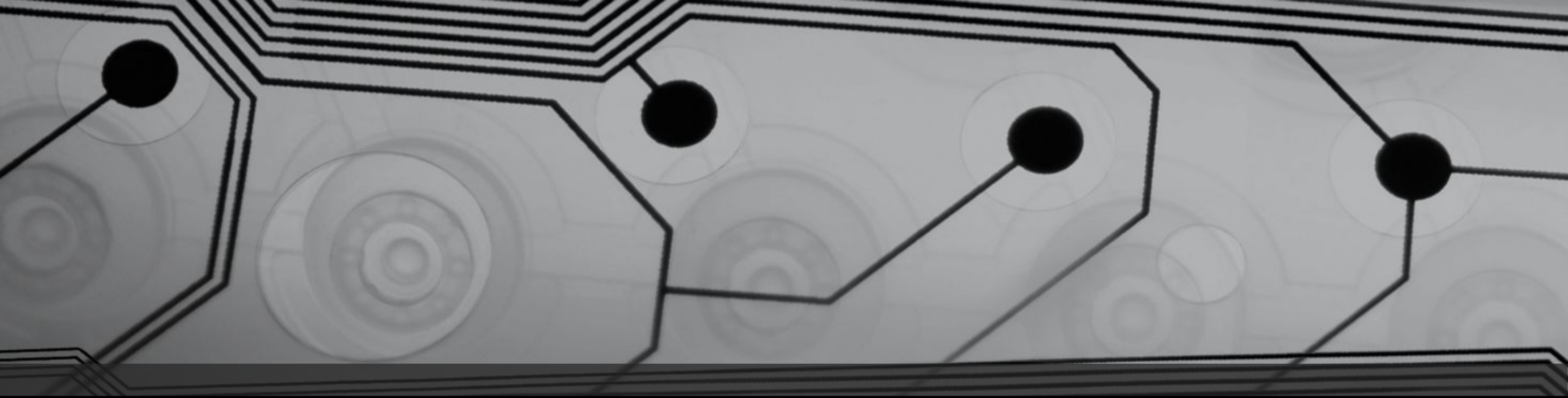


DIGITAL DEAD DROPS: Glimpses into Steganography

Presented by: Rebecca Gonzalez and Alex Jeong

Why Steganography

- Interesting History
  - According to the historian Herodotus, Histiaeus (a tyrant and ruler of Miletus in the late 6th century BCE) shaved the head of one of his servants and tattooed a message onto their scalp. After the servant's hair grew back and they reached the message recipient, the receiver shaved the servant's scalp again to read the message.
  - The first formally recorded use of the term was in 1499 by Johannes Trithemius in his disquisition on cryptography and steganography, The Steganographia, itself disguised as a book about magic.
- Modern Uses
  - Thanks to AI, steganography is becoming more and more prevalent in cyberattacks. AI is now able to create things such as perfectly secure steganography (an algorithm that conceals information so well that it is considered completely undetectable) and language models steganography (LLMs have mastered "encoded reasoning" which allows LLMs to embed intermediate reasoning steps within generated text that is undecipherable by humans)
- A Growing and Challenging Threat
  - It's intriguing and has the potential to be especially dangerous

DEMONSTRATION OUTLINE & SUMMARY

- Alex reads slides 1-7 (first half of presentation until demo)
- (Time Permitting - may have to condense)
    - Alex hides a .txt message in a .wav file using WavSteg and uploads file to Google Drive.
    - Rebecca downloads .wav file from Google Drive and using WavSteg, recovers the hidden message.
    - Rebecca then uploads a .txt file that has a message hidden using StegSnow.
    - Alex downloads .txt file and uses StegSnow to reveal Rebecca's hidden message to the class
- Rebecca finishes slides and answers any technical questions the class might have.

MITIGATION STRATEGIES

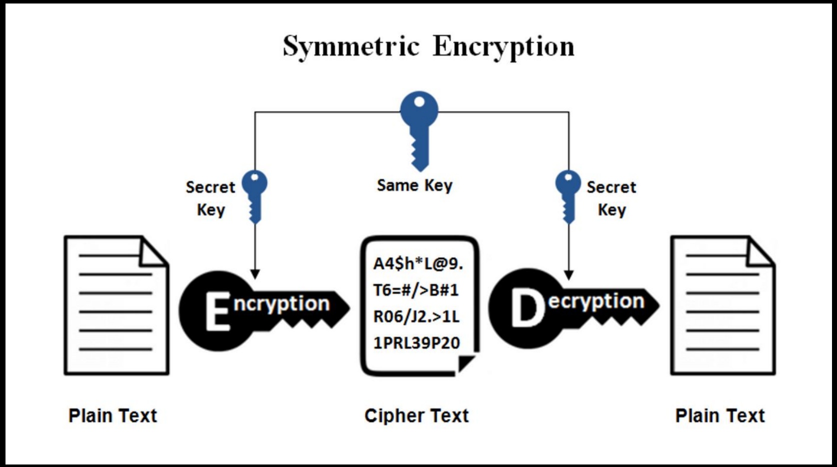
- A well equipped anti-virus/malware detection system may be helpful after the file has already been downloaded, but ultimately the best mitigation strategy is end user training.
    - Don’t download things from untrusted sources
    - Keep an eye on file sizes - be wary of files that are unusually large
    - Stay up-to-date on patches and updates.

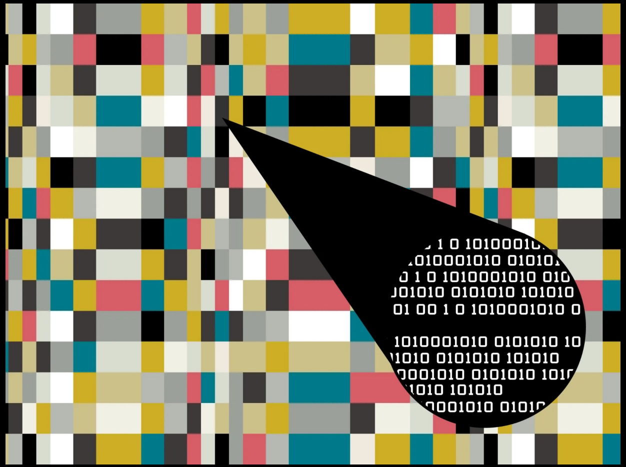
What is Steganography?

- Derives from the Greek words, “steganos” which, means hidden or covered and “graphein” means to write or express by written characters.

- It is a method of concealing secret information within (or on top of) seemingly ordinary media with the intent of avoiding detection or scrutiny.

Cryptography vs Steganography





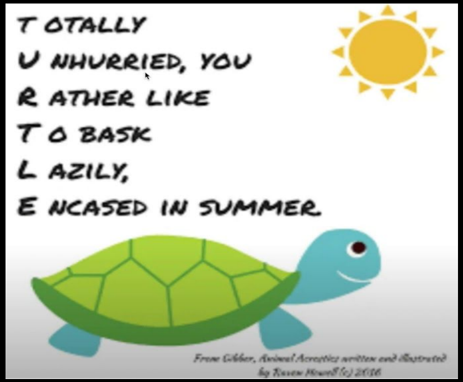
Means “Hidden Writing”	Means “Covered Writing”
Data is altered	Structure of data is (usually) unaltered
Confidentiality, Authentication, Integrity, and Non-Repudiation principles	Confidentiality & Authentication principles
information is visible	information is not visible
The main goal of cryptography is to keep the contents of the message secret from unauthorized access.	The goal of steganography is to make the information invisible to anyone who doesn’t know where to look or what to look for

Types of Steganography

Image	concealing data by using an image as a cover
Audio	hiding data in sound
Text	hiding data in text
Video	embedding data into video file
Network	concealing data by using a network protocol (TCP, UDP, ICMP, IP, etc.)

Steganography in the Real World

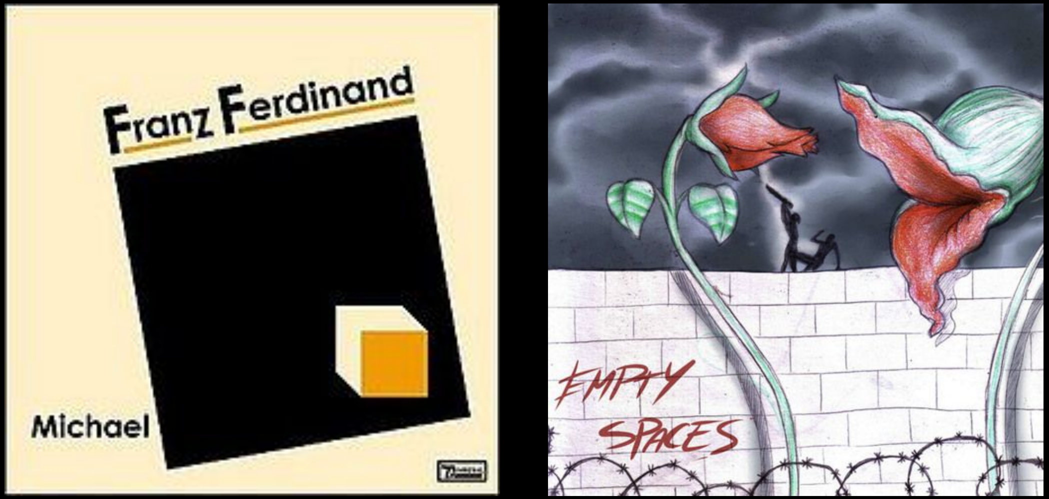
Invisible Ink



T OTALLY
U NHURRIED, YOU
R ATHER LIKE
T O BASK
L AZILY,
E NCASED IN SUMMER

From Gibber, Animal Acrostics written and illustrated by Raven Howell (c) 2016

Acrostic



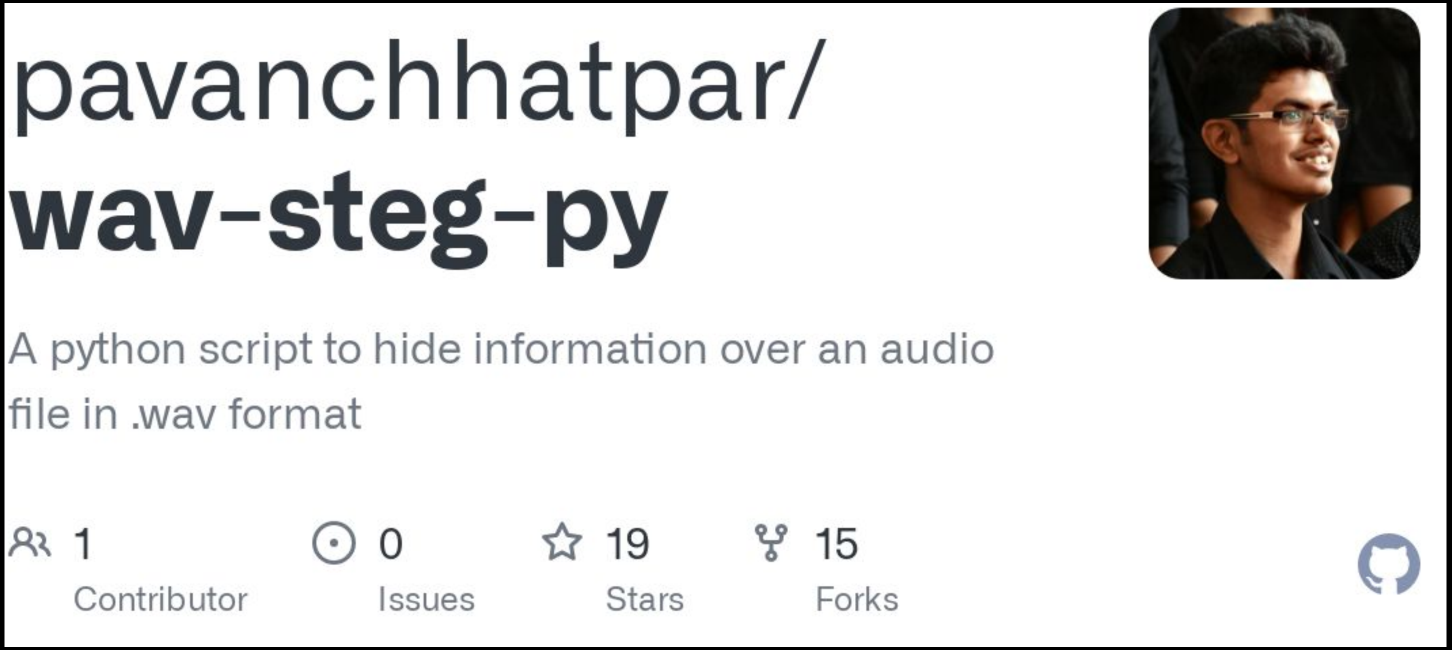
Backmasking

LIVE DEMO

Tools being demonstrated today:

WavSteg

Special Thanks To….



pavanchhatpar/
wav-steg-py

A python script to hide information over an audio file in .wav format

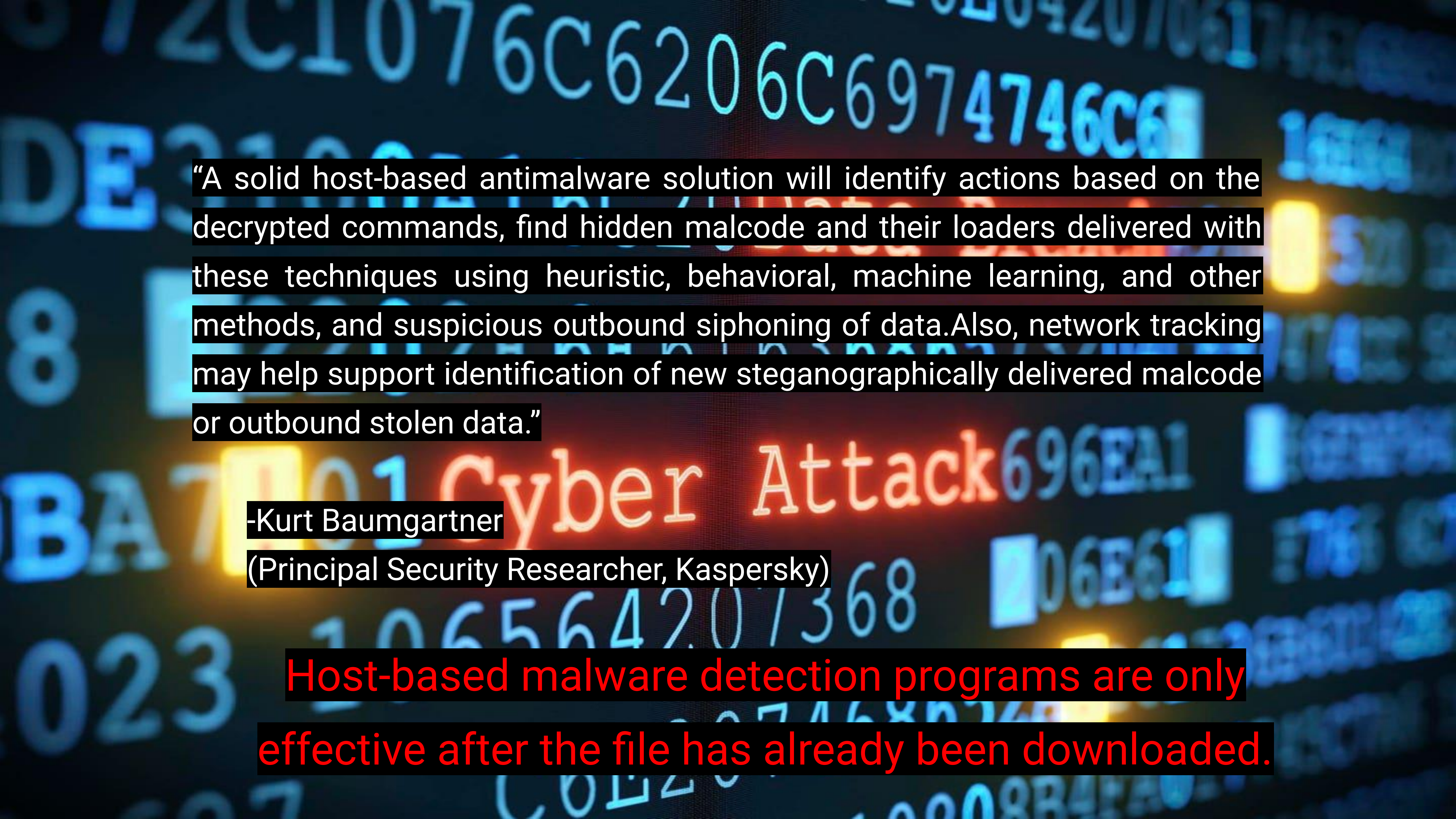
1 Contributor
0 Issues
19 Stars
15 Forks

KALI
BY OFFENSIVE SECURITY

python™

Protecting Against Steganographic Attacks

…is kind of tricky.



> “A solid host-based antimalware solution will identify actions based on the decrypted commands, find hidden malcode and their loaders delivered with these techniques using heuristic, behavioral, machine learning, and other methods, and suspicious outbound siphoning of data.Also, network tracking may help support identification of new steganographically delivered malcode or outbound stolen data.”

-Kurt Baumgartner
(Principal Security Researcher, Kaspersky)

Host-based malware detection programs are only effective after the file has already been downloaded.

- Educate yourself and others - be wary of files that are unusually large
- Stay up-to-date on patches and security updates
- Don’t download things from untrusted websites

RESOURCES

Arntz, Pieter. “Explained: Steganography.” *Malwarebytes*, 19 Aug. 2022, www.malwarebytes.com/blog/news/2022/08/explained-steganography.

CISOMAG. “How to Prevent Steganography Attacks.” *CISO MAG | Cyber Security Magazine*, 22 Feb. 2022, cisomag.com/how-to-prevent-steganography-attacks/.

Dickson, Ben. “Language Models Can Use Steganography to Hide Their Reasoning, Study Finds.” *VentureBeat*, 9 Nov. 2023, venturebeat.com/ai/language-models-can-use-steganography-to-hide-their-reasoning-study-finds/.

Imaizumi, Shoko, and Kei Ozawa. “Palette-Based Image Steganography for High-Capacity Embedding.” *Bull. Soc. Photogr. Imag. Japan*, vol. 25, no. 1, 2015, pp. 7–11, www.spij.jp/wp-content/uploads/2019/02/BSPIJ25_007.pdf.

Kwann, Mathew. “The SNOW Home Page.” *Darkside.com.au*, 20 June 2013, darkside.com.au/snow/. Accessed 12 Nov. 2023.

Loeffler, John. “New Encryption Method Uses AI-Generated Content to Hide Info in Plain Sight.” *Interestingengineering.com*, 8 Mar. 2023, interestingengineering.com/innovation/new-steganographic-encryption-method-developed.

Simplilearn. “What Is Steganography? Types, Techniques, Examples & Applications | Simplilearn.” *Simplilearn.com*, 25 Oct. 2021, www.simplilearn.com/what-is-steganography-article.

Stanger, James. “The Ancient Practice of Steganography: What Is It, How Is It Used and Why Do Cybersecurity Pros Need to Understand It.” *CompTIA*, 6 July 2020, www.comptia.org/blog/what-is-steganography.