USENIX Security '24 Artifact Appendix: The Imitation Game: Exploring Brand Impersonation Attacks on Social Media Platforms

Bhupendra Acharya
CISPA

Dario Lazzaro
University of Genoa

Efrén López-Morales
Texas A&M University-Corpus Christi

Adam Oest
PayPal Inc.

Muhammad Saad
PayPal Inc.

Antonio Emanuele Cinà
University of Genoa

Lea Schönherr
CISPA

Thorsten Holz
CISPA

A Artifact Appendix

This document is submitted for the artifact review for USENIX'24 AEC. In this research, we analyze the top 10,000 Tranco-ranked domains for impersonated social media profiles on four major platforms: X, Instagram, Telegram, and YouTube. Due to the nature of our study, it is not feasible to reproduce or provide a functional aspect of the experiment. Instead, we ask for an evaluation of the artifact presented to encourage further exploration of this attack by the research and security communities. Thus, for artifact evaluation, we do not provide any running to-dos for the researcher. Instead, the focus will be on validating three aspects of the research design and analysis: i) The data collection module, squatting analysis, and disclosure to social media; ii) The posts and image clustering logic; and iii) The experiment conducted to proactively find impersonating accounts on social media platforms.

As a reference to the artifact, we ask the researcher to refer to the public GitHub page, with the commit https://github.com/CISPA-SysSec/brand_impersonation/tree/6c58e42b1ab30f6c475f5b1b0648777daea65cbb that contains the code and experiment.

A.1 Abstract

Please visit the GitHub repository provided to view the available artifacts.

A.2 Description & Requirements

Please note we are not requesting for functional or reproducible badge. Thus, as stated we only ask the researcher to only perform artifacts being available.

A.2.1 Security, privacy, and ethical concerns

There are no security, privacy, or ethical concerns on accessing the GitHub repo.

A.2.2 How to access

Please visit the GitHub repo as provided for access the code and experiment.

A.2.3 Hardware dependencies

Not hardware-specific.

A.2.4 Software dependencies

The current setup was tested with Python 3.9.9; the respective version is expected.

A.2.5 Benchmarks

Not applicable.

A.3 Set-up

Please follow the following steps as part of the setup.

- Perform a git clone to set the repository by running the command in the terminal "'git clone https://github.com/CISPA-SysSec/brand_impersonation.git".
- The "readme.md" file provided on the repository provides guide to the three main components which contains additional guides on each of the components.
- As part of the data access and storage, we simply ask researchers to use their own API keys and MongoDB database installation for data storage.

A.3.1 Installation

For installation, we ask for two main setups.

- Perform a git clone as directed in subsection A.3.

- The code provides "Pipfile" which contains all the dependencies for installation. You are welcome to choose the choice of virtual env such as "pipenv" or others and run the installations. An example command, "pipenv install ." installs all the dependencies after the virtual environment is set up.

A.3.2 Basic Test

After the initial setup (see subsection A.3) and installation (see subsubsection A.3.1) as guided, this allows the researcher to further test the feature on data collection as stated in the readme file of data collection https://github.com/CISPA-SysSec/brand_impersonation/tree/6c58e42b1ab30f6c475f5b1b0648777daea65cbb.

A.4 Version

Based on the LaTeX template for Artifact Evaluation V20231005. Submission, reviewing and badging methodology followed for the evaluation of this artifact can be found at https://github.com/CISPA-SysSec/brand_impersonation/tree/6c58e42b1ab30f6c475f5b1b0648777daea65cbb.