UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00124

STEGANOGRAPHY ON TWITTER USING PNG FILES

DATE ISSUED: 22nd March 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A researcher has discovered a novel method using steganography techniques to hide ZIP and MP3 files within PNG files on popular social media platform - Twitter.

BREAKDOWN

Attaching source code to a PNG file by exploiting Twitters' methods for filtering out excess data on PNG uploads by utilising the DEFLATE stream inside IDAT of the file means that the image file still meets requirements and will not be re-encoded. There are a number of conditions that must be met to achieve this feat including the ability to compress the image file well with a colour palette of at least 257 unique colours to avoid optimisation (re-encoding) by Twitter if the image is less that 680x680 in resolution. The total output size of the attached file must not exceed 5MB, otherwise Twitter will convert the PNG to a JPEG – again re-encoding the image. In one scenario, the researcher entreated Twitter users to download the image and save it with a .mp3 extension, followed by instructions to open a media player for a surprise, and was surprised by how many took him up on the offer – highlighting the ease of exploitation if this were a legitimate attack scenario.

REMEDIATION STEPS

- Educate users on the dangers of social media and how to remain vigilant when using such platforms.
- Remove users' ability to access social media sites on company owned devices unless it is a part of their normal work duties.
- Ensure you have a robust acceptable use and social media policy in place to guide user behaviour.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/researcher-hides-files-in-png-twitter/164881/
Bleeping Computer https://www.bleepingcomputer.com/news/security/twitter-images-can-be-abused-to-hide-zip-mp3-files-heres-how/