The steganography technique can hide malicious files in images on Twitter

A cybersecurity expert has made a stir in security circles by revealing a relatively detailed method of hiding up to 3MB of data inside an image on the social networking platform Twitter.

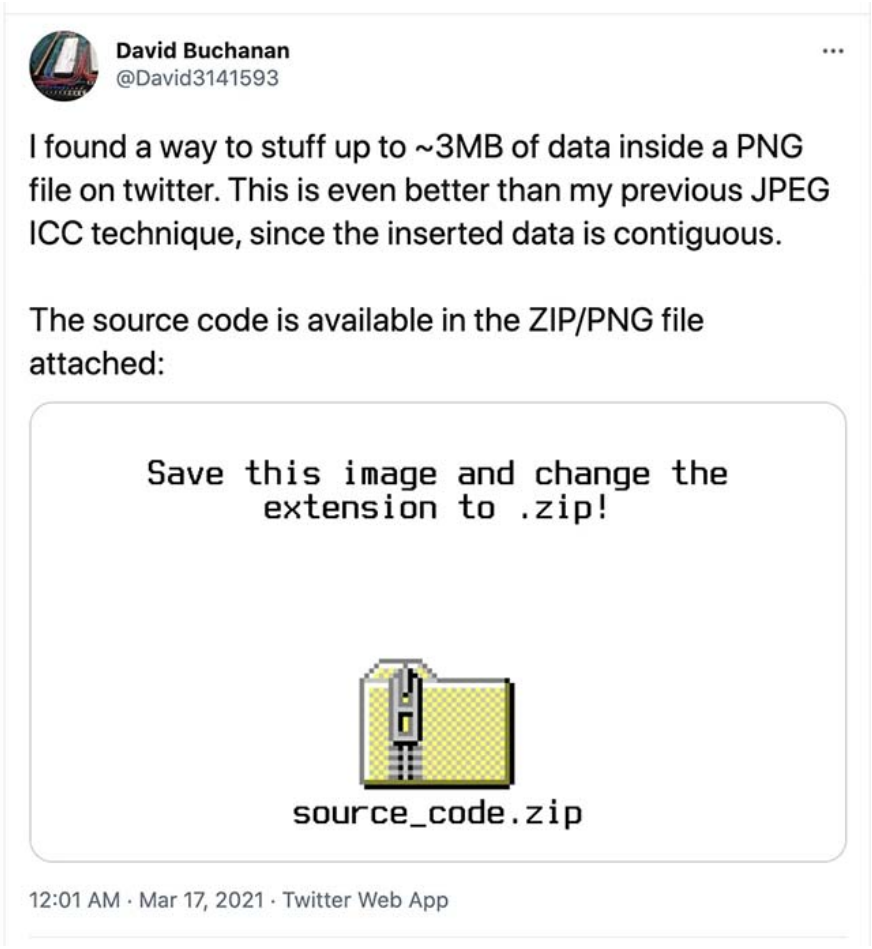
More specifically, in his testing, this researcher showed that both an MP3 audio file as well as a ZIP archive can be hidden in PNG images hosted on Twitter.

In fact, the technique of hiding non-image data in an image (steganography) is not something new. But the fact that images can be hosted on a popular platform that has an extremely large number of regular visitors like Twitter will lead to the possibility of them being abused by bad guys to commit malicious acts. is very high.

The photo can 'sing'

The discovery that attracted a lot of attention was that of a cybersecurity expert and programmer named David Buchanan. This expert used his personal Twitter account to post the information he found, including an example image with a ZIP archive and an MP3 file hidden inside.

While attached PNG files stored on Twitter represent valid images when previewed, basically just downloading and changing their file extension is enough to get more content. together from a single file.



An example image file posted by Buchanan on Twitter, which contains a ZIP file inside
The 6 KB image that David Buchanan posted in his tweet contained a full ZIP file. This ZIP file contains the source code of Buchanan's. In particular, anyone can use this source code to 'package' any content into a PNG image.

For those who prefer a slightly less 'physical' approach, Buchanan has also publicly provided the source code for creating what he calls the tweetable-polyglot-png file on GitHub.

In another example posted to Twitter, Buchanan tweeted an image that literally sounded out.

" *You just need to download this file, change the extension in the filename to .mp3, and enable it in VLC to see 'magic'. (Note: make sure you download the full resolution version of the file) , it should be 2048x2048px)* ", said the researcher.

According to analysis results, this photo is stored in Twitter image server approximately 2.5 MB in size and can be saved using the ".mp3" extension. Here is the photo access link:

`https://pbs.twimg.com/media/Ewo_O6zWUAAWizr?format=png&name=large`

Once opened, the image file, which was then converted to MP3, will begin playing Rick Astley's song Never Gonna Give You Up.

" *The new trick I discovered is that you can append the data to the end of the 'DEFLATE' stream (the part of the file that stores the compressed pixel data) and Twitter won't split it,* 'said Buchanan.

Risk of abuse by harmful agents

These coding techniques are often used by stealthy threats because they can hide malicious commands, payloads, and more in files that look normal. , such as pictures.

The fact is that Twitter may not always remove irrelevant information from an image, as Buchanan demonstrated. This opens up the potential for abuse of the threat agents.

Furthermore, another challenge poses that blocking image traffic on Twitter can interfere with legitimate activities. For example, a network administrator blocking Twitter's image domain pbs.twimg.com will also block legitimate images hosted on Twitter.

That's why Buchanan believes his technique of inserting files into PNG images may not be particularly useful to hackers. Besides, there are other more sophisticated steganography methods that can be overused.

' *I don't think this technique is particularly useful for attackers, because there are so many other existing steganography techniques that are easier to implement (and even harder to detect)* '.

However, saying so does not mean that Buchanan's PNG technique is less at risk of abuse. It can be used by malware to facilitate command and control operations from the C2 server.

" *But maybe it could be used as part of a C2 system, to distribute malicious files to infected servers* ," Buchanan added.

Likewise, for network monitoring systems, Twitter can be considered a secure server. Hence, distributing the malware over Twitter using such an image file remains a viable method of bypassing specialized security programs.

When asked if Twitter knew about the error, Buchanan said:

" *I reported my original JPEG-based trick to the people in charge of Twitter's bug bounty program, but they said it was not a security bug, so I don't bother reporting the problem. This is for them too* ".