

Drive by download attack Using a png image

Contents

- About drive by download attack using a png image
- Why this method
- PNG file structure
- Demo
- The embedding script
- Mitigation

About drive by download attack using a png image

A method to hide an html page + malicious javascript inside a png file then uploading it to legitimate website. User loads the png file into the browser and javascript is executed.

Why this method

- Can be used for redirection to malware infected site using a png file
- Malicious javascript inside the png not detected by the security products

PNG file structure

- PNG files consist of a PNG signature followed by several FourCC chunks. FourCC stands for Four Character Code. FourCC chunks are used in several multimedia formats including audio and video
- The PNG signature is a fixed sequence of 8 bytes: 89 50 4e 47 0d 0a 1a 0a

```
00000000 89 50 4e 47 0d 0a 1a 0a 00 00 0d 49 48 44 52 |.PNG.....IHDR|
00000010 00 00 02 5a 00 00 02 59 08 06 00 00 00 71 cf 9b |...Z...Y.....q..|
00000020 44 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 |D....sBIT....|.d|
```

PNG file structure

- Each chunk consists of four parts:
- Length: 4 byte unsigned integer indicating the size of only the chunk's data field.
- Chunk Type 4 byte FourCC code. Some chunk types are IHDR, IDAT, IEND, etc.
- Chunk Data Variable length data.
- CRC 4 byte CRC value generated from the chunk type and the chunk data, but not including the length.

PNG Header

IHDR

IDAT chunk

IDAT chunk

IDAT chunk

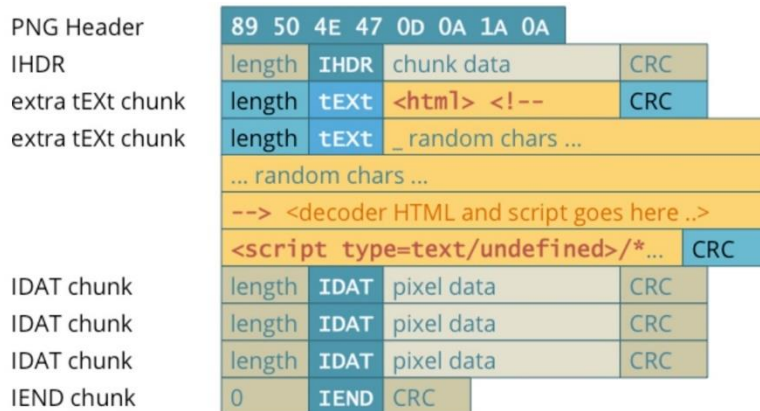
IEND chunk

89 50 4E 47 0D 0A 1A 0A			
length	IHDR	chunk data	CRC
length	IDAT	pixel data	CRC
length	IDAT	pixel data	CRC
length	IDAT	pixel data	CRC
0	IEND	CRC	

PNG file structure

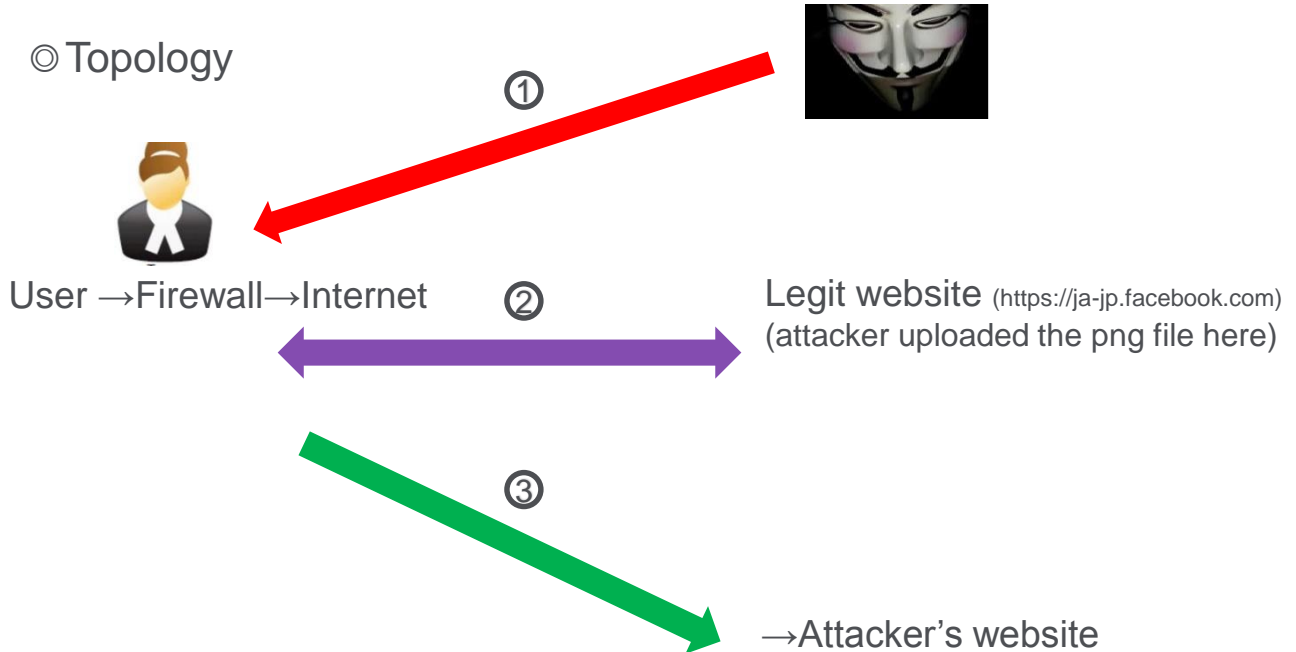
© Adding extra content in PNG files:

PNG provides informational chunks such as tEXt chunks that may be used to contain image metadata. We can insert tEXt chunks immediately after the IHDR chunk.



Demo: Email Phishing as an attack vector

© Topology



Demo: Email Phishing as an attack vector

- ① Attacker initiates the attack by sending a phishing email

宛先 KZK90RTAM@yahoo.co.jp

Hello Bob,

Check out my new photo!

<https://ja-jp.facebook.com/nicepic/posts/NicePic>



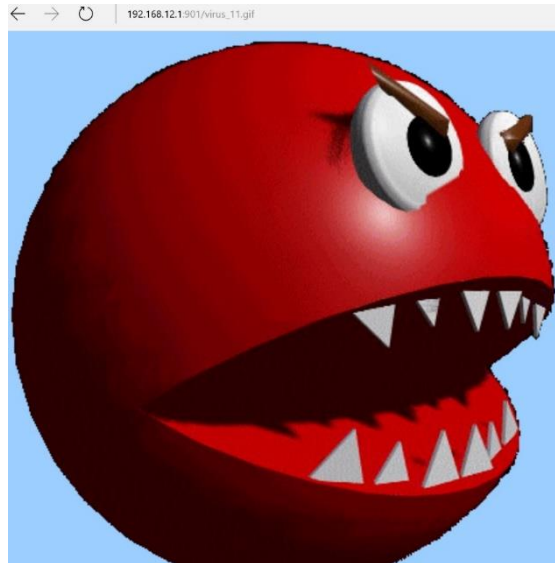
- ② User interacts with the email and loads the bad file into the browser (Edge,IE)



**Loading
Please Wait**

Demo: Email Phishing as an attack vector

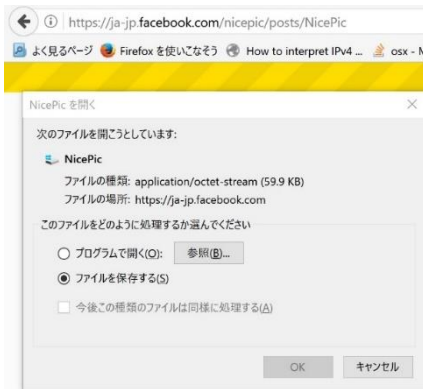
③ User is being redirected to the attacker malicious -> System compromised



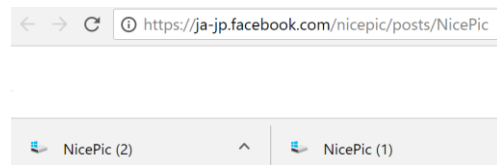
Demo: Email Phishing as an attack vector

◎ Note:

- Only Edge and IE browsers are affected.
- The attack does not affect Chrome, Firefox, Safari browsers.






【Firefox】



【Chrome】

The embedding script

- Three files required for the script to function: CRC32.pm(checksum calculation), PNGDATA.pm (png structure processing), png_with_html.pl (main script)
- Detailed comments in every file
- CRC32.pm 
CRC32.pm
- PNGDATA.pm 
PNGDATA.pm
- png_with_html.pl (rename it to .pl) 
png_with_html.pl
- Usage: # perl png_with_html.pl <html source> <png source> <output>
Example: perl png_with_html.pl Loader.html OK.png NicePic

Mitigation

- Use a threat isolation solution like Fireglass (<https://fire.glass/>)
- Do not not click links or download files even if they come from seemingly “trustworthy” sources
- Use common sense and critical eye when reviewing emails
- Do not set the default browser for viewing email to Edge or IE