**PNG Embedded – Malicious payload hidden in a PNG file**

One of the most complex tasks for the cybercriminals is to ensure their malicious code goes undetected by antivirus and achieves its goal. For this, they have invested a lot on more complex infection processes, going beyond the traditional phishing and using techniques where the malicious payload is hidden in encrypted files – even using a known file format. This is what we found in a new Brazilian Trojan in the wild: it tries to conceal the malicious files in a PNG image. And the attack starts with a simple phishing PDF.

**Malware distribution**

It looks like Brazilian cybercriminals follow the security news – this type of attack was publicized several months ago in the US and now they are using the same method in Brazil. The phishing aspect used in this campaign distributes a PDF attached to the email. The file is clean. The type of attack is the same as that used to distribute an executable file or a .ZIP file containing the .pdf extension in the filename.

The attached PDF contains a text commonly used in mail content, while the link (see screenshot below) directs the user to the malicious file.

Closer inspection of the PDF content reveals the malicious link as well as the URL of the tool used to generate the PDF from HTML content.

**The malicious payload**

The link prompts us to download a malicious JAR which downloads a ZIP file containing other files. Among those files we found three without any extension, but containing a PNG (Portable Network Graphics) file header – a common image format. Usually the header shows the file type that will be used in order to open the file. Something similar

to this was discovered some years ago in BMP files.

Looking at the file we can see that it is a solid color image of 63 x 48 pixels, but with a file size of 1.33 MB, which is too big for this specific image. Analyzing the binary that performs some operations on these files we identified the function that loads the PNG files to the memory:

This function is responsible for loading the PNG file to memory, decrypting and executing the extracted binary using a technique known as RunPE, where the malicious code is executed in the context of another process, in this case iexplore.exe.

From this code we could identify that the PNG file was only 179 bytes (0xB3) – the remaining content is the encrypted malicious file.

Based on this we managed to write a script to decrypt the content of the PNG files.

By giving the key that can be found in the malware code we can successfully decrypt the files.

**Conclusion**

Brazilian attacks are evolving day-by-day, becoming more complex and efficient. It is there necessary to be wary of emails from unknown sources, especially those containing links and attached files.

Since the malicious payload hosted in the PNG file cannot be executed without its launcher, it cannot be used as the main infector; that is usually delivered to your mailbox, so it has to be installed by a different module.

This technique allows the criminals to successfully hide the binary inside a file that appears to be a PNG image. It also makes the analysis process harder for antivirus companies as well as bypassing the automated process to detect malicious files on hosting servers.

The files related to this attack are detected by Kaspersky Lab products as:

**Trojan.Win32.KillAv.ovo**

**HEUR:Trojan.Win32.Generic**

**Trojan-Downloader.Win32.Banload.cxmj Trojan-Downloader.Win32.Agent.hgpf HEUR:Trojan-Downloader.Java.Generic**