

Wargames MY 2020 write-up

Category: Steganography

Challenge Name: nuisance

Introduction

In this challenge we are given a file named nuisance.arc. A very uncommon file extension indeed.

Tools used

1. [Google](#) (our best friend)
2. [FreeArc](#)
3. [An online palm to bmp converter](#)

Google > Decompress > Convert > Flag

“When you don’t know something, just google it”. This is the first action we did, which was very useful at almost all time.

(The above statement will works on most country)

The screenshot shows a Google search for ".arc file". The search bar at the top contains ".arc file" and the search button is visible. Below the search bar, the results are displayed. The first result is from fileinfo.com, titled "ARC File Extension - What is an .arc file and how do I open it?". It describes an ARC file as a backup file created by Norton software products, such as Norton 360 and Norton Online Backup. The format is listed as Binary. To the right of the search results, there is a knowledge panel for "ARC" (File format). It includes a description: "ARC is a lossless data compression and archival format by System Enhancement Associates. The file format and the program were both called ARC. The format is known as the subject of controversy in the 1980s, part of important debates over what would later be known as open formats. Wikipedia". It also lists the type of format as "Data compression" and the developer as "System Enhancement Associates". Below the knowledge panel, there is a section "People also search for" with icons for ZIP, PDF, STL, ARJ, and LHA. At the bottom of the search results, there is a link to the Wikipedia page for "ARC (file format)".

After knowing it's a compressed file, we searched for the decompressing software.

Which, to our surprise, is easily found. So we stumbled upon FreeArc, downloaded it and installed it.

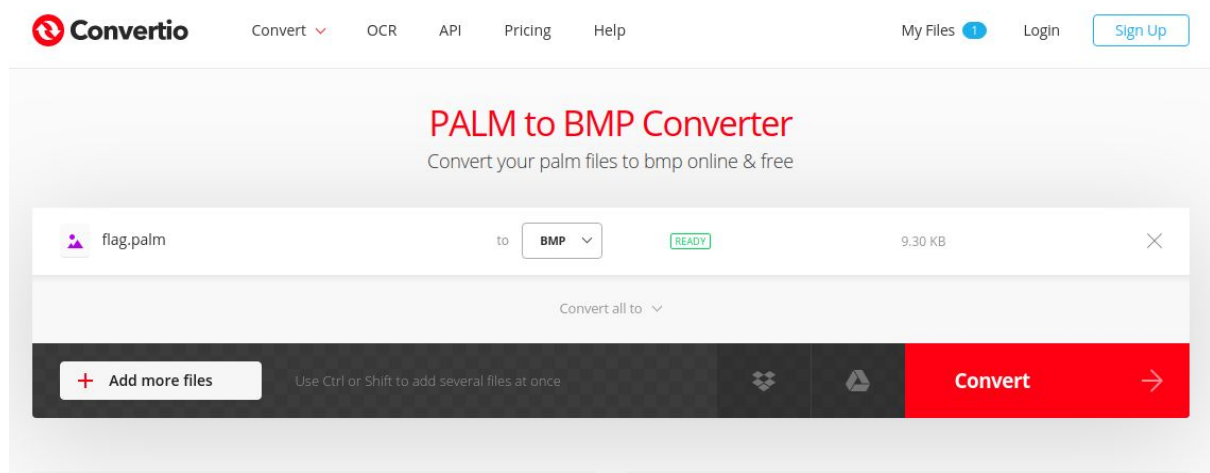
The screenshot shows the SourceForge project page for FreeArc. The page has a dark header with the SourceForge logo and navigation links for "Open Source Software", "Business Software", and "Resources". The project name "FreeArc" is prominently displayed, along with its status "Beta" and the developers "bulatz, markshevchenko". Below the project name, there are statistics: "17 Reviews" (represented by stars), "Downloads: 866 This Week", and "Last Update: 2013-04-03". A large green "Download" button is visible, along with "Get Updates" and "Share This" buttons. The page also lists supported operating systems: "Windows", "BSD", and "Linux". At the bottom, there is a tabbed interface with "Summary" selected, showing a description of FreeArc: "FreeArc combines best 7-zip and RAR features: auto-selected LZMA/PPMD/Multimedia compression, 1gb dictionary, exe/dict/delta data filters, updatable solid archives, SFXes, recovery record, AES+Twofish+Serpent encryption, Linux support and much more...". There is also a section for "Project Samples".

Decompress the file and we get flag.palm.

```
FreeArc 0.51 unpacker. Extracting archive: nuisance.arc
Extracting flag.palm (9520 bytes)
All OK
nkzlx@nkzlx-Nitro-AN515-52:~/Nkzlx_projects/ctf/wargames2
total 24K
drwxrwxr-x  2 nkzlx nkzlx 4.0K Dec  6 21:13 .
drwxrwxr-x 10 nkzlx nkzlx 4.0K Dec  6 01:07 ..
-rw-rw-r--  1 nkzlx nkzlx 3.1K Dec  5 17:48 nuisance.arc
-rw-----  1 nkzlx nkzlx 9.3K Dec  4 19:08 flag.palm
nkzlx@nkzlx-Nitro-AN515-52:~/Nkzlx_projects/ctf/wargames2
```

Next, we googled again and we know that .palm file can be converted into image files.

Let's find an online converter and do the job for us!



And... this is the result of the .bmp file!

wgmy{c6a9f61e26a8be4d4f856ab326d729dd}