Malware Dropped Through a ZPAQ Archive

isc.sans.edu/diary/Malware Dropped Through a ZPAQ Archive/30366/

Published: 2023-11-01
Last Updated: 2023-11-01 06:33:33 UTC
by Xavier Mertens (Version: 1)
0 comment(s)

Did you ever seen ZPAQ archives? This morning, my honeypot captured a phishing attempt which lured the potential victim to open a "ZPAQ" archive. This is not a common file format. This could be used by the attacker to bypass classic security controles. What Wikiepadia

says about ZPAQ:

ZPAQ is an open source command line archiver for Windows and Linux. It uses a journaling or append-only format which can be rolled back to an earlier state to retrieve older versions of files and directories. It supports fast incremental update by adding only files whose last-modified date has changed since the previous update. It compresses using deduplication and several algorithms (LZ77, BWT, and context mixing) depending on the data type and the selected compression level. To preserve forward and backward compatibility between versions as the compression algorithm is improved, it stores the decompression algorithm in the archive.

The file was called "Purchase Order pdf.zpaq" (SHA256:1c33eef0d22dc54bb2a41af485070612cd4579529e31b63be2141c4be9183eb6[1]). The fact that the archive is using an "exotic" compress algorithm, the VT score is null! I tried the classic tools on a stock Windows operating systems, including 7Zip and no one was able to decompress the archive. This is a strange because it reduces the number of potential victims! On Windows, you can use PeaZip[2].

On my REMnux sandbox, I had to install 'zpaq' to process the file:

```
remnux@remnux:/MalwareZoo/20231101$ zpaq x Purchase\ Order\ pdf.zpaq
zpaq v7.15 journaling archiver, compiled Mar 22 2020
Purchase Order pdf.zpaq: 1 versions, 1 files, 3 fragments, 0.006140 MB
Extracting 1000.000000 MB in 1 files -threads 2
[1..3] -> 160908
> Zfaggccwnm.exe
0.385 seconds (all OK)
```

You can see that the same technique as describe in one of my last diary[3] is used: the PE file is pretty big (1GB) to defeat more security controls.

The malware (SHA256:d15eaee1ad4cadfeada118324f7bd65f546940cb23808142de1157373ee35389) and is unknown on VT. It's a .Net executable. I had a quick look and it downloads an obfuscated payload from hxxps://www[.]mediafire[.]com/file/vgvujtm9ke2lj1c/Gnwwcgocwzl[.]wav/file. I started to debug the .Net file to understand the obfuscation used and the purpose of the wav file (probaly the real malware) but it seems to not work in my lab. If you have more details, feel free to share!

[1] https://www.virustotal.com/gui/file/1c33eef0d22dc54bb2a41af485070612cd4579529e31b63be2141c4be9183eb6
[2] https://peazip.github.io
[3] https://isc.sans.edu/diary/Size%20Matters%20for%20Many%20Security%20Controls/30352

Xavier Mertens (@xme)
Xameco
Senior ISC Handler - Freelance Cyber Security Consultant
PGP Key

Keywords: Archive Malware ZPAQ
0 comment(s)

Comments

Login here to join the discussion.

Top of page
×

Diary Archives