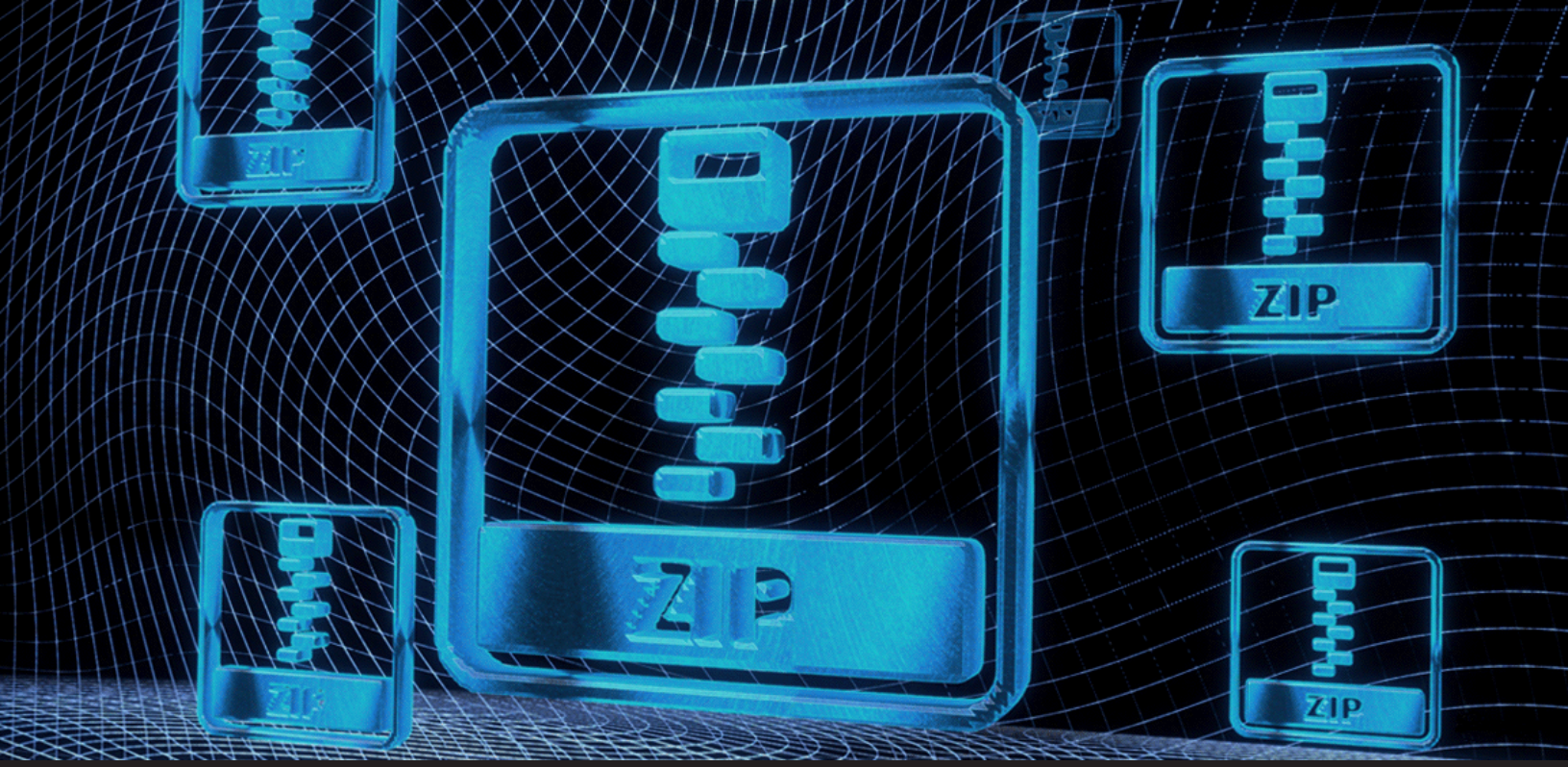


Why You Should Never Use the Native .Zip Crypto in Windows

Devolutions

IS THERE ANY WAY TO CRACK A PASSWORD-PROTECTED ZIP FILE?

When working in IT security, there are some questions that keep coming up, and I thought this one deserved to be answered once and for all: Is there any way to crack a password-protected zip file?

I understand how much we all want to be absolutely certain and reassured that our files will not be cracked — not now, not ever! For some time now, the .zip format has provided encryption as an added feature. But the type of encryption it offers depends on the program you use to create and open the zip file.

One of the .zip password protection algorithms is called ZipCrypto. ZipCrypto is supported natively on Windows, but it should never be used because it is completely broken, flawed, and relatively easy to crack. All hackers need to know is 12 bytes of plain text and where it is located in the zip (which can be easily found) in order to quickly decrypt the entire content of the archive. To give you an idea, on most laptops, it would usually takes less than a minute to decrypt the entire content of a zip file.

Exploiting ZipCrypto

Exploiting ZipCrypto through a widely known plain text attack is straightforward and doesn't require sophisticated technical skills. Although I will walk you through the steps, I am obviously not doing so to help go out and hack someone. I simply want to show you how basic and easy this exploit really is.

Requirements

- Download bkcrack from GitHub
- Download encrypted.zip
- (Optional) Download plain.zip

Opening the zip file reveals an XML file called SomeXmlFile.xml.

Usually, XML files contain the following header at the beginning:

```
<?xml version="1.0" encoding="UTF-8"?>
```

Steps

The procedure itself is quite simple:

1. Create a file named **plain.txt**.

2. Add the following text to **plain.txt**: <?xml version="1.0" encoding="UTF-8"?>

3. Zip the file and call it **encrypted.zip**. Do not use a password and use the same compression algorithm as the encrypted archive. (If you wish, you can download **plain.zip** using the link supplied above, which already has the **plain.txt** file in it.)

4. Feed both files to bkcrack using the following command line:

```
bkcrack -C encrypted.zip -c SomeXmlFile.xml  -P plain.zip -p plain.txt
```

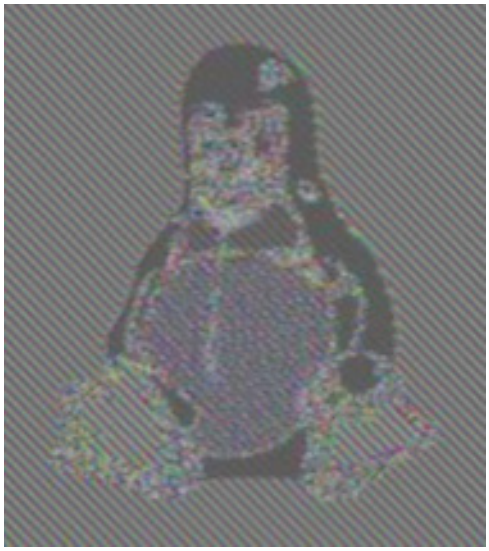
The final tool output should look like this:

```
Generated 4194304 Z values.
[11:58:53] Z reduction using 30 bytes of known plaintext
100.0 % (30 / 30)
260948 values remaining.
[11:58:54] Attack on 260948 Z values at index
7 88.3 % (230335 / 260948)
[12:01:52] Keys
c072e51c a36b7996 b6f8d312
```

Once the keys have been obtained, any files in the zip can be deciphered using the following command line:

```
bkcrack -C encrypted.zip -c Tux_ecb.jpg -k c072e51c a36b7996 b6f8d312 -d Tux_ecb.jpg
```

This example extracted the Tux_ecb.jpg file. The resulting image should look like this:



Congratulations, you have successfully decrypted the zip file!

Additionally

We included multiple files in the encrypted.zip (MIT License, HTML file), so that you can practice and go off the beaten track!

AES-256

By now you're probably wondering: If you should never use ZipCrypto, then what is the alternative? Well, we strongly recommend AES-256, which is the industry standard for zip encryption and has been proven to be quite strong and safe. Unfortunately, Windows does not have native support for this. However, most third-party archivers such as 7Zip, Winrar, and Winzip support it.