

Forum:[Hack Forums](#)

Thread: [Run an .exe that is encoded in a jpeg image \(Windows\)](#)

HCauldfield - September 11, 2024, 6:04 am

I have an image with an .exe inside, my goal is to achieve that when the image is opened or a rar is decompressed (Any action) the executable starts.

Delfin - September 11, 2024, 6:11 am

Vulnerabilities that allow you to run payloads upon opening an image file are few and far between. Maybe you'll find an answer, but you'll most likely have to find a different route to deploy your payload. You could try using a .LNK shortcut to download a payload? You could disguise it as an image but people might still realize.

HCauldfield - September 11, 2024, 6:21 am

(Sep 11, 2024 06:11 AM)Delfin Wrote: [\[CITE\]](#) Vulnerabilities that allow you to run payloads upon opening an image file are few and far between. Maybe you'll find an answer, but you'll most likely have to find a different route to deploy your payload. You could try using a .LNK shortcut to download a payload? You could disguise it as an image but people might still realize.

From what I've been able to read on the forum looking for information on the subject, infecting through an image is not a good idea, the tricks used are not very subtle. It's better to look for another way.

Delfin - September 11, 2024, 6:30 am

(Sep 11, 2024 06:21 AM)HCauldfield Wrote: [\[CITE\]](#) From what I've been able to read on the forum looking for information on the subject, infecting through an image is not a good idea, the tricks used are not very subtle. It's better to look for another way.

Yeah, there's definitely better ways. You could use malicious excel macros, malicious .MSI installer files, malicious batch scripts, etc. Depends entirely on your targets really

YolidPop - September 11, 2024, 7:25 am

(Sep 11, 2024 06:30 AM)Delfin Wrote: [\[CITE\]](#) Yeah, there's definitely better ways. You could use malicious excel macros, malicious .MSI installer files, malicious batch scripts, etc. Depends entirely on your targets really

Please bro ... Macro is not a good idea now because of the mark of the web. Macro is dead.

Delfin - September 11, 2024, 7:38 am

(Sep 11, 2024 07:25 AM)YolidPop Wrote: [\[CITE\]](#) Please bro ... Macro is not a good idea now because of the mark of the web. Macro is dead.

Loads of other options, and still a better method than trying to use images to deploy payloads lmao

DramaKing - September 12, 2024, 3:54 am

(Sep 11, 2024 07:25 AM)YolidPop Wrote: [\[CITE\]](#) Please bro ... Macro is not a good idea now because of the mark of the web. Macro is dead.

It's not a good idea because macros are disabled in any version of Office updated within the last several years.

(Sep 11, 2024 06:04 AM)HCauldfield Wrote: [\[CITE\]](#) I have an image with an .exe inside, my goal is to achieve that when the image is opened or a rar is decompressed (Any action) the executable starts.

If you somehow stuffed an exe into an image, the image would be invalid. There's the WebP exploit that you could try to execute code (no PoC). Using a WinRAR SFX archive with a custom icon and an image can look fairly convincing. You could also try [this WinRAR exploit](#). It uses crafted ZIP files in WinRAR , but good luck.

Ghandi090909 - September 14, 2024, 2:14 am

U used a crypter? (Sep 11, 2024 06:04 AM)HCauldfield Wrote: [\[CITE\]](#) I have an image with an .exe inside, my goal is to achieve that when the image is opened or a rar is decompressed (Any action) the executable starts.

DramaKing - September 14, 2024, 6:44 am

(Sep 14, 2024 02:14 AM)Ghandi090909 Wrote: [\[CITE\]](#) U used a crypter?
Totally missing the point here.

Ivanov_1 - September 15, 2024, 8:39 am

When you do some searching about the possibility of the jpg+exe success everything you will find would have the .sfx/.rar or server.jpg.exe (hiding extensions).

Still the real extension will be shown,and therefore make it harder for evasion/suspicion.