

Forum:[Hack Forums](#)

Thread: [About Jpeg](#)

greghoglund1204 - December 18, 2019, 12:05 am

Hi, I heard that the jpeg file can be used as a virus to infect windows 7 OS. So is it really possible? What kinds of tricks are used here and how to prevent this from happening? ?

CyberStrike - December 18, 2019, 2:00 am

Sources/References? No I don't want to read "my friend who is a blackhat hacker who hacked the NSA told me so, he is smart." Because "My friend says JPEG is not a polyglot". Actual sources, links, research papers, etc.

(I think that people need to honestly research how images become malicious)

greghoglund1204 - December 18, 2019, 3:14 am

This is just my curiosity. I thought that only exe files can contain malicious code. But someone says even jpg files can be used to carry malicious code too. So I wanted to confirm this is true or false. So CyberStrike, Is it really possible in modern Os?

CyberStrike - December 18, 2019, 4:20 am

(Dec 18, 2019 04:14 AM)greghoglund1204 Wrote: [\[CITE\]](#) This is just my curiosity. I thought that only exe files can contain malicious code. But someone says even jpg files can be used to carry malicious code too. So I wanted to confirm this is true or false. So CyberStrike, Is it really possible in modern Os?

This is something which is discussed at length here and it seems that no one really reads, searches or learns. Then we will have the person who wants to do some extension spoofing, nothing like using what 2005 tactics in 2019 stay current people.

<https://security.stackexchange.com/quest...attachment>
<https://warroom.rsmus.com/bmp-x86-polyglot/>

<https://hackforums.net/showthread.php?tid=583947>
<https://hackforums.net/showthread.php?tid=5886482>

There are many more such threads, just now I am being lazy and don't feel like doing all the work.

greghoglund1204 - December 18, 2019, 5:45 am

Thank you for your kindness, CyberStrike! The URLs you provided to me are all about bmp files. What I'd like to know is about jpegs. In 2004, there was a big impact on jpeg format(windows xp), and this problem is solved in Windows 7. That problem was: there was a problem in GDIPLUS.dll, and this caused "buffer overflow". After googling for a while, I noticed that gdiplus.dll and some other dlls still have some problems. (I think there are some problems in decoding jpeg file) But I can not find out. Would you please give me some clues? Thanks in advance.

CyberStrike - December 18, 2019, 11:29 am

(Dec 18, 2019 06:45 AM)greghoglund1204 Wrote: [\[CITE\]](#) Thank you for your kindness, CyberStrike! The URLs you provided to me are all about bmp files. What I'd like to know is about jpegs. In 2004, there was a big impact on jpeg format(windows xp), and this problem is solved in Windows 7. That

problem was: there was a problem in GDIPLUS.dll, and this caused "buffer overflow". After googling for a while, I noticed that gdiplus.dll and some other dlls still have some problems. (I think there are some problems in decoding jpeg file) But I can not find out. Would you please give me some clues? Thanks in advance.

Awesome that you denoted some issue, why not go and get a VM for free from Microsoft and go figure it out using a debugger? Perhaps you can stumble on something new. I will tell you now that I have only seen JavaScript used in jpeg headers, but once again it's worth you doing some research.

Perhaps someone else will chime in and provide you more information other than the common tools already running about so you may weaponize JPEG's in a way to get execution on a remote/local machine be it code execution or whatever. Please keep us up to date with your research.

greghoglund1204 - December 18, 2019, 5:37 pm

Ok, could you explain about javascript code injection in detail? Is this method still used in modern OS?