

## Forum:[Hack Forums](#)

Thread: [.jpg.vbs vs .vbs](#)

**thewasp333** - November 12, 2017, 10:31 am

Hi, may you please help me out here.

I am trying to infect a pedo but I would like to know what is better to send him

a .jpg.vbs or a .vbs file, what would he open up?

thanks.

**Mr. Kim** - November 12, 2017, 10:51 am

I mean, if file extensions are off he's much more likely to open the .png.vbs

**botxfive** - November 12, 2017, 12:38 pm

crypt vbs file and bind it with some game setup

**Mr. Kim** - November 12, 2017, 12:45 pm

(Nov 12, 2017 01:38 PM)botxfive Wrote: [CITE](#) crypt vbs file and bind it with some game setup  
Lol what? This is a horrible idea. Bind it to an .exe, that will be MUCH easier to convince someone to run than a spoofed image file.

**Vuln** - November 12, 2017, 12:49 pm

OP, you're better off using a shortcut.

Step 1. Right click somewhere on your Desktop > New > Shortcut

Step 2. Enter the following text into the textbox (where "just-an-image.png" is the relative path to your payload):

PHP Code

```
<?php
```

```
%comspec% /c "start just-an-image.png"
```

Step 3. Click on Next and give the shortcut any name you want, with a file extension of your choice. "beach adventures.png" will do. Now click on Finish.

Step 4. Right click on the generated shortcut file and choose Properties.

Step 5. Select the text in the "Start in:" textbox and delete it.

Step 6. Locate the "Run:" listbox and select the "Minimized" option.

Step 7. Click on "Change Icon" and an .ico file that looks like an image.

Step 8. Press on "OK" twice and you got yourself a malicious shortcut that resembles an image. It will bypass SmartScreen by the way.

Of course there's endless of variations on this, some better than others, but this should get you started.

(Nov 12, 2017 11:51 AM)M?m?ry Wrote: [CITE](#) I mean, if file extensions are off he's much more likely to open the .png.vbs

Once the file is on his PC, sure. But getting him to download it without noticing anything will be even harder.

Mr. Kim - November 12, 2017, 1:03 pm

(Nov 12, 2017 01:49 PM)Jailbyte Wrote: [\[CITE\]](#) Once the file is on his PC, sure. But getting him to download it without noticing anything will be even harder.

I dont see how it's much easier to have him download a shortcut AND a payload the shortcut will run.

sexy\_lady.png > cool

awndibkdawpdj0awd.exe > probably gunna set off some red flags

Vuln - November 12, 2017, 1:28 pm

(Nov 12, 2017 02:03 PM)M?m?ry Wrote: [\[CITE\]](#) sexy\_lady.png > cool

awndibkdawpdj0awd.exe > probably gunna set off some red flags

There won't be a file with an .exe extension. And "awndibkdawpdj0awd" probably isn't the most believable name either.

(Nov 12, 2017 02:03 PM)M?m?ry Wrote: [\[CITE\]](#) I dont see how it's much easier to have him download a shortcut AND a payload the shortcut will run.

I personally don't mind as you can just make it look like an album for example, but if you want to then nothing is stopping you (other than your scripting knowledge) from keeping everything malicious into the shortcut itself.

More advanced example (1 file, persistent background download&execute, exception handling, SmartScreen bypass, cloned fake tooltip, FUD, character limit bypass, hidden arguments exploit and more):

Mr. Kim - November 12, 2017, 2:29 pm

(Nov 12, 2017 02:28 PM)Jailbyte Wrote: [\[CITE\]](#) There won't be a file with an .exe extension. And "awndibkdawpdj0awd" probably isn't the most believable name either.

I personally don't mind as you can just make it look like an album for example, but if you want to then nothing is stopping you (other than your scripting knowledge) from keeping everything malicious into the shortcut itself.

More advanced example (1 file, embedded download & execute script):

I suppose that's fair enough, if you wanted to get more in depth you can do a lot more with shortcuts. I assume this is being done via powershell, yes? Just passing the script to powershell.exe and throwing the -Command flag? Again, im not experienced with powershell so if I'm being a retard please let me know so I can stop being a retard ?

EDIT: I guess im a retard on the file extension thing. I just tried it and sure enough cmd gives 0 fucks about the extension as long as it's a valid PE.

thewasp333 - November 13, 2017, 4:58 am

thank you very much for the help

Vuln - November 13, 2017, 8:26 am

I noticed that I made a little mistake in my original post which I have now updated. You should add the "start" command before the payload path, otherwise the CMD window may briefly appear on the taskbar.

(Nov 12, 2017 03:29 PM)M?m?ry Wrote: [\[CITE\]](#) I suppose that's fair enough, if you wanted to get more in depth you can do a lot more with shortcuts. I assume this is being done via powershell, yes? Just passing the script to powershell.exe and throwing the -Command flag? Again, im not experienced with powershell so if I'm being a retard please let me know so I can stop being a retard ?

%comspec% is a relatively unknown environment variable that points to CMD, but PowerShell or even MSHTA are commonly used as well.

(Nov 12, 2017 03:29 PM)M?m?ry Wrote: [\[CITE\]](#) EDIT: I guess im a retard on the file extension thing. I just tried it and sure enough cmd gives 0 fucks about the extension as long as it's a valid PE. Yeah it's odd right? It's a rather big flaw that they somehow never bothered to fix.

One of the other odd exploitable flaws I discovered is the fact that both the shortcut creation wizard and Explorer's Properties window have a limit of 254 characters for a shell link's Target field, but the actual limit (e.g. when creating them with WshShell) is many times higher. This means that you can embed much larger and more advanced scripts. Among other things, this also allows you to append a bunch of spaces before your target string, to completely hide your whole script, or even to show a fake Target string. Once again, a ridiculous flaw that Microsoft never bothered to fix...

Not too long ago I had [a builder tool](#) for all of this, but I abandoned the project due to lack of time. Perhaps I'll revive it some day, but no promises.

Mr. Kim - November 13, 2017, 8:45 am

(Nov 13, 2017 09:26 AM)Jailbyte Wrote: [\[CITE\]](#) Yeah it's odd right? It's a rather big flaw that they somehow never bothered to fix.

One of the other odd exploitable flaws I discovered is the fact that both the shortcut creation wizard and Explorer's Properties window have a limit of 254 characters for a shell link's Target field, but the actual limit (e.g. when creating them with WshShell) is many times higher. This means that you can embed much larger and more advanced scripts. Among other things, this also allows you to append a bunch of spaces before your target string, to completely hide your whole script, or even to show a fake Target string. Once again, a ridiculous flaw that Microsoft never bothered to fix...

Not too long ago I had [a builder tool](#) for all of this, but I abandoned the project due to lack of time. Perhaps I'll revive it some day, but no promises.

Damn, it seems like all you need to break Windows is attempt to break Windows ?

On the point I made about powershell though, did you not use powershell for your download and execute shortcut? I suppose either vbscript or javascript could work too. Was the entire script just cmd commands? If so would you mind posting the code for the script? I'm really interested to see how that worked if it was pure batch ?

Vuln - November 13, 2017, 9:38 am

(Nov 13, 2017 09:45 AM)M?m?ry Wrote: [\[CITE\]](#) Damn, it seems like all you need to break Windows is attempt to break Windows ?

Pretty much.

(Nov 13, 2017 09:45 AM)M?m?ry Wrote: [\[CITE\]](#) On the point I made about powershell though, did

you not use powershell for your download and execute shortcut? I suppose either vbscript or javascript could work too. Was the entire script just cmd commands? If so would you mind posting the code for the script? I'm really interested to see how that worked if it was pure batch ?

I've created PowerShell scripts too yeah, but no matter what you use, the possibilities are endless. I don't have access to any code at the moment, however my favorite download&execute method was a batch script that made use of [BITS](#) through the BITSAdmin tool (installed by default on any Windows version up from XP). It allows you to create download jobs that are surprisingly silent and persistent (it's also used by Windows Update). Run it once on an offline PC and it'll finish the job a year later (or whatever moment it'll have internet access again). And all without the usual startup traces and detection rates.

**Mr. Kim** - November 13, 2017, 9:48 am

(Nov 13, 2017 10:38 AM)Jailbyte Wrote: [\[CITE\]](#) I've created PowerShell scripts too yeah, but no matter what you use, the possibilities are endless.

I don't have access to any code at the moment, however my favorite download&execute method was a batch script that made use of [BITS](#) through the BITSAdmin tool (installed by default on any Windows version up from XP). It allows you to create download jobs that are surprisingly silent and persistent (it's also used by Windows Update). Run it once on an offline PC and it'll finish the job a year later (or whatever moment it'll have internet access again). And all without the usual startup traces and detection rates.

Never knew that was a thing. I need to dig around more in C:\Windows lol, there's alot of interest utilities I never knew existed that can be easily exploited apparently. Thanks for the information dude, I really appreciate it ?

**smartpoison** - August 23, 2018, 7:13 am

Please teach me how to infect pc with this shorcut looks preety cool

**PoseidOFF** - August 24, 2018, 3:00 am

(Nov 12, 2017 11:31 AM)thewasp333 Wrote: [\[CITE\]](#) Hi, may you please help me out here.

I am trying to infect a pedo but I would like to know what is better to send him

a .jpg.vbs or a .vbs file, what would he open up?

thanks.

If you have evidence against him, you could do better if you would report him to the proper authorities.