

Forum:[Hack Forums](#)

Thread: [\[NEW\] Demon-606 13lackWorm PYTHON SOURCE CODE](#)

tanmay606 - December 5, 2014, 3:33 am

[+] Hello try my worm-script i name it [Demon-606 13lack Worm]

[!] you can full edit it ! :D

image link : goo.gl/v3TsKO

1. inject its code in all files in current directory
2. has two options [inject] and [corrupt].

inject => simple inject code in all files in current dir.

corrupt => inject code and corrupt all files in current dir.

[++] just try it and please tell me in comment you like it or not [++]

pastebin link => goo.gl/Ht0d1A

#13lackDeMOn ? ?

Ju1c3b0x - March 5, 2015, 12:05 pm

Code if(files.split('.')[1] in files_ext_to_infect):

```
    if(signature.decode('base64') in files):
```

```
        pass
```

```
    else:
```

```
        vul_files.append(files)
```

```
    del files
```

```
else:
```

```
    pass
```

```
    del files
```

```
except:
```

```
    pass
```

```
    del files
```

Hope you don't mind. I'm reading over your code to learn. I have a few questions.

why are you decoding the signature and checking to see if its already in the file? Is it to make sure its not going over the files constantly? And why decode it first?

And why multiple attempts at del the files? Is this to ensure they get deleted? And does that mean the .append makes a copy of the file?

MR.FREE - March 5, 2015, 1:45 pm

(Mar 5, 2015 01:05 PM)Ju1c3b0x Wrote: [\[CITE\]](#) Code if(files.split('.')[1] in files_ext_to_infect):

```
    if(signature.decode('base64') in files):
```

```
        pass
```

```
    else:
```

```
        vul_files.append(files)
```

```
del files
else:
    pass
del files
except:
    pass
del files
```

Hope you don't mind. I'm reading over your code to learn. I have a few questions.

why are you decoding the signature and checking to see if its already in the file? Is it to make sure its not going over the files constantly? And why decode it first?

And why multiple attempts at del the files? Is this to ensure they get deleted? And does that mean the .append makes a copy of the file? According to OP's neg rep, he steals source code and posts it as his own. So I doubt you'll get an answer.

Edit: After looking at the code OP deff wrote this.

Ive barely skimmed the script but, this is another proof of concept script, it does absolutely nothing, at most it would seed what pretty much amounts to a string into 'X' files and then does nothing else. It almost looks like he ripped off someones word-press eval vulnerability.

Where is the rest of the script, or is that all you got?

Assuming that what ever you posted above is the same as <http://pastebin.com/ZznhyHmY>

everydayguy - March 6, 2015, 12:06 am

^ Clearly, MR. FREE, you shouldn't be posting about code, this is super basic. No offense, buddy - but you're off the hook by a lot and that misleads others. (Your need to feed your self-importance hunger by posting about stuff you wish you'd understand makes others lose time. Not cool, bra.) (Nothing personal, I don't know you. But misleading others is not beneficial to anybody)

Decodes a base64 string which assumingly is an exploit and then writes it to the files.

Code > I decide my life is short so #yolo (<https://www.youtube.com/watch?v=Ewf6HDtFUbw>) <- OP.

> I decide I can just paste code at the end of the files and it'll execute whenever I open them

> I write this script and make sure my name is mlg_noScope_xXxHackerXx_momgetdecamera

> I publish it so other skids who're learning python can say they have a 0day

^ The writer's mind.

I have an one-liner reverse TCP shell spawner in one line too. (Literally base64 decode to a socket which connects back to my IP, which then loads a stager).

Pretty good example:

<https://www.phillips321.co.uk/2013/10/22/one-line-python-meterpreter-reverse-shell/>

Except this thing decodes to:

```
Code ,./~!@#$$%^&*())_+{}[]:;<,.!~!@#$$%^&*())_+{}[]:;<,.!~!@#$$%^&*())_+{}[]:;<
Which does...nothing. Whoever wrote this code is a retard.
```

To give you some more insight:

Binding files doesn't work this way. The PE format (I don't know a lot, but I can tell you what to google) must be well understood to be tampered with. Some links to help you with that:

<https://msdn.microsoft.com/en-us/magazine/cc301805.aspx>

<http://www.rohitab.com/discuss/topic/29972-simple-file-binder/>

MR.FREE - March 6, 2015, 1:07 pm

(Mar 6, 2015 01:06 AM)everydayguy Wrote: [\[CITE\]](#) ^ Clearly, MR. FREE, you shouldn't be posting about code

Decodes a base64 string which assumingly is an exploit and then writes it to the files.

Which does...nothing. Whoever wrote this code is a retard. Before I get started. #worm

Lol what fuckin planet are you from?

How did you write a wall of text and not say anything more then I said in my first post.

It's really cool you could google a reason to encode python stings. OP said "[NEW] Demon-606 13lackWorm PYTHON SOURCE CODE", that implies it should spread and execute itself with no interdiction.

you said

(Mar 6, 2015 01:06 AM)everydayguy Wrote: [\[CITE\]](#) which assumingly is an exploit and then writes it to the files. So please, show me the one liner(the exploit) that you would write and spread to a .txt, png, exe, html, zip, etc to make this thing work like a "WORM"...

Dude this is the python section, we write code around here. We don't just run programs and think were Ub3r l33t. Look at my profile, all my posts are in the python section. All my rep is from the python section, lol get bent. And keep this half assed garbage off the sub-section, posting altered broken code from other people is a sin around here.

Anybody that programs tools/malware, would tell you this isn't a real script. Show me that script running and spreading like a "Worm" and I will Blow "averageguys"(your) mom. LOL Op I would give you +1 if you could Google and find an exploit that could make that script actually work.

I say proof of concept cause op attempts to check for seed in files, if seed not in file, write a decoded base64 string.

lol that is very little concept. Let me know If I need to dumb down what im saying OP, I can make it simpler.

<http://pastebin.com/ZznhyHmY>

Edit:

(Mar 6, 2015 01:06 AM)everydayguy Wrote: [\[CITE\]](#) ^ Clearly, MR. FREE, you shouldn't be posting about code

No offense, buddy - but you're off the hook by a lot and that misleads others.

Since I am misleading people, you should hurrying up and post the one liner you Googled. Don't edit the actual function of the code, just base.encode(64).oneline and run. Let us know how far the script gets.

When you find that miracle one liner that would make this script work, let me know, i'll write you a real spreader that actually executes the seed, if the signature isn't detected in memory.