

Forum:[Hack Forums](#)

Thread: [Apps for crypto wallet hacking](#)

pilona - September 29, 2024, 8:42 pm

I have had some success with hacking of crypto wallets. As you may know the wallets recovery phrase/seed phrase is not entirely random, nor are the total number of words that can be chosen from quite limited actually. 2048 English words make up the full range of words to choose from. Thus old fashion brute force may work quite well on wallets (in particular when they are open). One problem is that the software has only partially been updated over the last few years.

Here below are a few ones that I have found that are quite new/updated - and in several cases I have also used them. I would be interesting to learn the experiences of other hackers with this type of hacking apps.

The apps that I have tried so far are:

1. Crypto-Wallet-Cracker-Stealer-2024-crack (withdrawal possible) It can be downloaded from: [deleted]

or: [deleted]

2. BitcoinHunter_updated [deleted]

or: [deleted]

3. Crypto Checker all in one updated [deleted]

or [deleted]

One idea of this project is to build a "database" over working Wallet crackers. And of course to share experiences about configurations for Rypto wallet hacking.

Bastille - September 30, 2024, 1:31 am

3 tools with 2 links for each to download them.

First links are dead. Second and third allow to download two files :

- BitcoinHunter.zip
- Crypto Checker all in one_updated.zip

Both ZIP file contain the similar read_me.txt file :

Both ZIP file contain the same update.exe file :

MD5 : 40104fe031ddbbaa7846752b6e7e06d4

SHA256 : 3a794867b593dc70111214a0e2e3f684b8a01f25b82dad14573df000b243b628

Update.exe have been made with Python and converted to exe :

<https://www.virustotal.com/gui/file/3a794867b593dc70111214a0e2e3f684b8a01f25b82dad14573df000b243b628>

Looks like a cliper at first sight :

Will take a deeper look later

UPDATE _____

I used the following tool to extract the .pyc files from the update.exe file :

<https://github.com/extremecoders-re/pyinstxtractor>

Remember, we saw earlier that update.exe was made in Python and that Py2Exe was used to convert it to an exe file :

Using the strings command also gives us a hint :

Then I used decompyle3 on "clipper_ed.pyc" to read to code. You cannot read .pyc files as they are binaries files, to be able to read them you need to decompile them back to .py files. This operation is possible on high level languages, but not on lower level languages, that's why you need to use others tools such as Ghidra to decompile files to Assembly.

Here is what I was able to retrieve, and that confirms it's a BTC clipper :

I wanted to take a look at the main file called "BitcoinHunterGUI.exe", I succeeded to find with Detect It Easy that it was written in C# with .NET libraries :

However I'm not skilled enough to read the code through DnSpy, I need to improve my skills and knowledge regarding this field, if someone else want to take a look or let me know how to do it, I would be glad.

Here is the VT report of this file by the way :

<https://www.virustotal.com/gui/file/e0ae3cf680a2c57ee53367c574dda9dd7693b225e0cf9202ce29723d6f08cc32/behavior>

teeeeeekar - October 8, 2024, 2:29 pm

(Sep 30, 2024 01:31 AM)Bastille Wrote: [\[CITE\]](#) 3 tools with 2 links for each to download them.

First links are dead. Second and third allow to download two files :

- BitcoinHunter.zip
- Crypto Checker all in one_updated.zip

Both ZIP file contain the similar read_me.txt file :

Both ZIP file contain the same update.exe file :

MD5 : 40104fe031ddbbaa7846752b6e7e06d4

SHA256 : 3a794867b593dc70111214a0e2e3f684b8a01f25b82dad14573df000b243b628

Update.exe have been made with Python and converted to exe :

<https://www.virustotal.com/gui/file/3a794867b593dc70111214a0e2e3f684b8a01f25b82dad14573df000b243b628>

Looks like a cliper at first sight :

Will take a deeper look later

UPDATE _____

I used the following tool to extract the .pyc files from the update.exe file :

<https://github.com/extremecoders-re/pyinstxtractor>

Remember, we saw earlier that update.exe was made in Python and that Py2Exe was used to convert it to an exe file :

Using the strings command also gives us a hint :

Then I used decompyle3 on "clipper_ed.pyc" to read to code. You cannot read .pyc files as they are binaries files, to be able to read them you need to decompile them back to .py files. This operation is possible on high level languages, but not on lower level languages, that's why you need to use others tools such as Ghidra to decompile files to Assembly.

Here is what I was able to retrieve, and that confirms it's a BTC clipper :

I wanted to take a look at the main file called "BitcoinHunterGUI.exe", I succeeded to find with Detect It Easy that it was written in C# with .NET libraries :

However I'm not skilled enough to read the code through DnSpy, I need to improve my skills and knowledge regarding this field, if someone else want to take a look or let me know how to do it, I would be glad.

Here is the VT report of this file by the way :

<https://www.virustotal.com/gui/file/e0ae3cf680a2c57ee53367c574dda9dd7693b225e0cf9202ce29723d6f08cc32/behavior>

I think I can use your expertise on a project I have. Please PM me for more details buddy

morgane_mlr1 - December 1, 2024, 6:23 am

can i contact you on telegram pls ?

Jadzia - December 13, 2024, 7:50 am

(Sep 30, 2024 01:31 AM)Bastille Wrote: [\[CITE\]](#) 3 tools with 2 links for each to download them.

First links are dead. Second and third allow to download two files :

- BitcoinHunter.zip
- Crypto Checker all in one_updated.zip

Both ZIP file contain the similar read_me.txt file :

Both ZIP file contain the same update.exe file :

MD5 : 40104fe031ddbbaa7846752b6e7e06d4

SHA256 : 3a794867b593dc70111214a0e2e3f684b8a01f25b82dad14573df000b243b628

Update.exe have been made with Python and converted to exe :

<https://www.virustotal.com/gui/file/3a794867b593dc70111214a0e2e3f684b8a01f25b82dad14573df000b243b628>

Looks like a cliper at first sight :

Will take a deeper look later

UPDATE _____

I used the following tool to extract the .pyc files from the update.exe file :

<https://github.com/extremecoders-re/pyinstxtractor>

Remember, we saw earlier that update.exe was made in Python and that Py2Exe was used to convert it to an exe file :

Using the strings command also gives us a hint :

Then I used decompyle3 on "clipper_ed.pyc" to read to code. You cannot read .pyc files as they are binaries files, to be able to read them you need to decompile them back to .py files. This operation is possible on high level languages, but not on lower level languages, that's why you need to use others tools such as Ghidra to decompile files to Assembly.

Here is what I was able to retrieve, and that confirms it's a BTC clipper :

I wanted to take a look at the main file called "BitcoinHunterGUI.exe", I succeeded to find with Detect It Easy that it was written in C# with .NET libraries :

However I'm not skilled enough to read the code through DnSpy, I need to improve my skills and knowledge regarding this field, if someone else want to take a look or let me know how to do it, I would be glad.

Here is the VT report of this file by the way :

<https://www.virustotal.com/gui/file/e0ae3cf680a2c57ee53367c574dda9dd7693b225e0cf9202ce29723d6f08cc32/behavior>

Damn!!! I love posts like this. Awesome find. I'd love to be able to do stuff like this. I watch John Hammond tear malware apart but he just goes really fast through things.

(Dec 13, 2024 08:50 AM)Jadzia Wrote: [\[CITE\]](#) Damn!!! I love posts like this. Awesome find. I'd love to be able to do stuff like this. I watch John Hammond tear malware apart but he just goes really fast through things.

Hey buddy, thanks ! Glad to see you back on HF by the way, hope you'll stay longer this time !

Haha, then you should check my thread, a lot of examples like this :

<https://hackforums.net/showthread.php?tid=6276795>

If you have any question regarding cybersecurity, malware analysis, reverse engineering, or any technical field, feel free to open a thread I'll be glad to help you ;) my DM/Convo are also open (but I prefer if we post on HF, so we make the forum keep living !)

omegalord751 - January 3, 2025, 9:12 am

so nice hop to learn how to analyse this

SIM-5604220 - January 11, 2025, 3:40 pm

Wow awesome find!! Thanks for sharing

PopeyeToolsUK - January 12, 2025, 12:22 am

Wow find!! Thanks for sharing

Bastille - January 16, 2025, 6:09 am

(Jan 3, 2025 10:12 AM)omegalord751 Wrote: [\[CITE\]](#) so nice hop to learn how to analyse this

(Jan 11, 2025 04:40 PM)JoshuaDev Wrote: [\[CITE\]](#) Wow awesome find!! Thanks for sharing

(Jan 12, 2025 01:22 AM)PopeyeToolsUK Wrote: [\[CITE\]](#) Wow find!! Thanks for sharing

Hello guys, if you're interested by this kind of content feel free to take a look at my thread where I put every analysis : <https://hackforums.net/showthread.php?tid=6276795>

By the way, I've made a thread to motivate all of us to post every day our progresses on the hacking / cybersecurity realm, feel free to join us and participate :

<https://hackforums.net/showthread.php?tid=6288695>

Hackers - January 16, 2025, 6:12 am

[Bastille](#) you just owned this guy lol

[Tyr](#) [mention=1441945] [tbr0](#) [Klonopin](#)

Check this out lol ~ Bastille comin' in hot.

(Sep 30, 2024 01:31 AM)Bastille Wrote: [\[CITE\]](#) 3 tools with 2 links for each to download them.

First links are dead. Second and third allow to download two files :

- BitcoinHunter.zip

- Crypto Checker all in one_updated.zip

Both ZIP file contain the similar read_me.txt file :

Both ZIP file contain the same update.exe file :

MD5 : 40104fe031ddbbaa7846752b6e7e06d4

SHA256 : 3a794867b593dc70111214a0e2e3f684b8a01f25b82dad14573df000b243b628

Update.exe have been made with Python and converted to exe :

<https://www.virustotal.com/gui/file/3a794867b593dc70111214a0e2e3f684b8a01f25b82dad14573df000b243b628>

Looks like a cliper at first sight :

Will take a deeper look later

UPDATE _____

I used the following tool to extract the .pyc files from the update.exe file :

<https://github.com/extremecoders-re/pyinstxtractor>

Remember, we saw earlier that update.exe was made in Python and that Py2Exe was used to convert it to an exe file :

Using the strings command also gives us a hint :

Then I used decompyle3 on "clipper_ed.pyc" to read to code. You cannot read .pyc files as they are binaries files, to be able to read them you need to decompile them back to .py files. This operation is possible on high level languages, but not on lower level languages, that's why you need to use others tools such as Ghidra to decompile files to Assembly.

Here is what I was able to retrieve, and that confirms it's a BTC clipper :

I wanted to take a look at the main file called "BitcoinHunterGUI.exe", I succeeded to find with Detect It Easy that it was written in C# with .NET libraries :

However I'm not skilled enough to read the code through DnSpy, I need to improve my skills and knowledge regarding this field, if someone else want to take a look or let me know how to do it, I would be glad.

Here is the VT report of this file by the way :

<https://www.virustotal.com/gui/file/e0ae3cf680a2c57ee53367c574dda9dd7693b225e0cf9202ce29723d6f08cc32/behavior>

(Jan 16, 2025 07:09 AM) Bastille Wrote: [\[CITE\]](#) Hello guys, if you're interested by this kind of content feel free to take a look at my thread where I put every analysis :

<https://hackforums.net/showthread.php?tid=6276795>

By the way, I've made a thread to motivate all of us to post every day our progresses on the hacking / cybersecurity realm, feel free to join us and participate :

<https://hackforums.net/showthread.php?tid=6288695>

Bastille - January 16, 2025, 6:25 am

(Jan 16, 2025 07:12 AM) nodes Wrote: [\[CITE\]](#) [Bastille](#) you just owned this guy lol

[Tyr](#) [mention=1441945] [ttbr0](#) [Klonopin](#)

Check this out lol ~ Bastille comin' in hot.

Haha, thanks buddy, doing my best to protect HF members

(Jan 16, 2025 07:15 AM)m0hx Wrote: [\[CITE\]](#) Niceeee pls send me similar threads links I wanna attempt to analyze tooooo
Added to my todo list !

Hackers - January 16, 2025, 7:04 am

(Jan 16, 2025 07:25 AM)Bastille Wrote: [\[CITE\]](#) Haha, thanks buddy, doing my best to protect HF members

Added to my todo list !

In cases like this, it is acceptable to continue RE and pen testing on any backend server they use to distribute their payload (to HF users)? Or is that technically off limits still?

Bastille - January 16, 2025, 7:15 am

(Jan 16, 2025 08:04 AM)nodes Wrote: [\[CITE\]](#) In cases like this, it is acceptable to continue RE and pen testing on any backend server they use to distribute their payload (to HF users)? Or is that technically off limits still?

That's a good question, to be honest I do this only to reduce the risks and protect HF members, but I wasn't into something like a "hunt" or "revenge". I've never discussed about this with Omni but I don't think I should go further to avoid escalating the problem.

I just share what I find and show how I found these things (IOCs, artifacts) to help people interested in malware analysis / cybersecurity understand how to proceed. Then, other members do what they want with these info ...

Hackers - January 16, 2025, 7:24 am

(Jan 16, 2025 08:15 AM)Bastille Wrote: [\[CITE\]](#) That's a good question, to be honest I do this only to reduce the risks and protect HF members, but I wasn't into something like a "hunt" or "revenge". I've never discussed about this with Omni but I don't think I should go further to avoid escalating the problem.

I just share what I find and show how I found these things (IOCs, artifacts) to help people interested in malware analysis / cybersecurity understand how to proceed. Then, other members do what they want with these info ...

Yeah I agree with this - probably best to not encourage people to go after them, escalate it, and have the user come back with vengeance. And legally speaking, hacking a hacker is still a crime technically. They'll just call it vigilante hacking.

Makes sense , was just curious :)

ttbr0 - January 16, 2025, 9:13 pm

(Sep 30, 2024 01:31 AM)Bastille Wrote: [\[CITE\]](#) 3 tools with 2 links for each to download them.

First links are dead. Second and third allow to download two files :

- BitcoinHunter.zip
- Crypto Checker all in one_updated.zip

Both ZIP file contain the similar read_me.txt file :

Both ZIP file contain the same update.exe file :
MD5 : 40104fe031ddbbbaa7846752b6e7e06d4

SHA256 : 3a794867b593dc70111214a0e2e3f684b8a01f25b82dad14573df000b243b628

Update.exe have been made with Python and converted to exe :

<https://www.virustotal.com/gui/file/3a794867b593dc70111214a0e2e3f684b8a01f25b82dad14573df000b243b628>

Looks like a cliper at first sight :

Will take a deeper look later

UPDATE _____

I used the following tool to extract the .pyc files from the update.exe file :

<https://github.com/extremecoders-re/pyinstxtractor>

Remember, we saw earlier that update.exe was made in Python and that Py2Exe was used to convert it to an exe file :

Using the strings command also gives us a hint :

Then I used decompyle3 on "clipper_ed.pyc" to read to code. You cannot read .pyc files as they are binaries files, to be able to read them you need to decompile them back to .py files. This operation is possible on high level languages, but not on lower level languages, that's why you need to use others tools such as Ghidra to decompile files to Assembly.

Here is what I was able to retrieve, and that confirms it's a BTC clipper :

I wanted to take a look at the main file called "BitcoinHunterGUI.exe", I succeeded to find with Detect It Easy that it was written in C# with .NET libraries :

However I'm not skilled enough to read the code through DnSpy, I need to improve my skills and knowledge regarding this field, if someone else want to take a look or let me know how to do it, I would be glad.

Here is the VT report of this file by the way :

<https://www.virustotal.com/gui/file/e0ae3cf680a2c57ee53367c574dda9dd7693b225e0cf9202ce29723d6f08cc32/behavior>

excellent work! you should definitely script something up to help automate and quicken your analyses.

Bastille - January 17, 2025, 12:24 am

(Jan 16, 2025 10:13 PM)ttbr0 Wrote: [\[CITE\]](#) excellent work! you should definitely script something up to help automate and quicken your analyses.

Thanks for the proposal ! Just sent you the links, one is still working, I would definitely be interested looking at the script !