

Forum:[Hack Forums](#)

Thread: [Bitcoin stealer](#)

peniel666 - July 28, 2024, 10:35 am

Download:

[deleted]

Bastille - July 28, 2024, 11:14 am

Well, well, well

Bitcoin.exe :

<https://www.virustotal.com/gui/file/b26cffc869d48ca11fedf05913da0c7e6188918d42d909ca7d7bb49715948130?nocache=1>

Quite good to be honest, only 9/71 and not detected by most used AV. At this moment Windows Defender was like this : ???

Bitcoin.exe dropped many files :

One of these is :

<https://www.virustotal.com/gui/file/4e72ca1baee2c7c0f50a42614d101159a9c653a8d6f7498f7bf9d7026c24c187/detection>

This file is present in the Startup folder, here we have our persistent artifact.

There is a lot to say on it, I'll continue tomorrow

At least OP didn't lied, it's a Bitcoin Stealer, but for him.

Skorp - July 28, 2024, 11:37 am

(Jul 28, 2024 11:14 AM)Bastille Wrote: [\[CITE\]](#) Well, well, well

Bitcoin.exe :

<https://www.virustotal.com/gui/file/b26cffc869d48ca11fedf05913da0c7e6188918d42d909ca7d7bb49715948130?nocache=1>

Quite good to be honest, only 9/71 and not detected by most used AV. At this moment Windows Defender was like this : ???

Bitcoin.exe dropped many files :

One of these is :

<https://www.virustotal.com/gui/file/4e72ca1baee2c7c0f50a42614d101159a9c653a8d6f7498f7bf9d7026c24c187/detection>

This file is present in the Startup folder, here we have our persistent artifact.

There is a lot to say on it, I'll continue tomorrow

At least OP didn't lie, it's a Bitcoin Stealer, but for him.

A 1 poster that immediately posts a download on blackhat software will highly likely be infected during my time on here. It's so obvious sometimes haha. Good stuff though for looking out for the community!!! ?

Btw anytime you see a caxidl.exe , the malware will install itself in the system32 directory. At least he renamed the main exe bitcoin.exe, looks totally legit never knew bitcoin had an app x'D

Bastille - July 28, 2024, 10:24 pm

(Jul 28, 2024 11:37 AM)Skorp Wrote: [\[CITE\]](#) A 1 poster that immediately posts a download on blackhat software will highly likely be infected during my time on here. It's so obvious sometimes haha. Good stuff though for looking out for the community!!! ?

Btw anytime you see a caxidl.exe , the malware will install itself in the system32 directory. At least he renamed the main exe bitcoin.exe, looks totally legit never knew bitcoin had an app x'D
Haha yeah really obvious

Thanks ! I like conducting those analysis, aside of protecting members, that allows me to practice and learn, and I'm also planning to make a thread with all of them so people who are interested in malware analysis will have a bunch of examples on HF.

I didn't know this file, thanks for the heads up :)