

Forum:[Hack Forums](#)

Thread: [imsorri1 | UID: 4233147](#)

Harald - December 10, 2019, 12:38 am

So, Morning All.

Was just chilling drinking my coffee, till I received a random-ass PM from some user. This user is claiming I asked for an eBook? Considering, I've never asked for an eBook in my life, I found this very hard to believe, so I had to check his profile which was already looking fishy as it is, so I proceed to run a virus total scan against the sent file, you can see for your self below the results and the PM.

So be cautious dealing with this user, I will update the thread with any more reports like this.

Profile Link:

<https://hackforums.net/member.php?action=profile&uid=4233147>

Virus Total:

<https://www.virustotal.com/gui/url/c64bc5c7dbd40cefd3237db4232acff7335838ed843c335798d18f88350f408/detection>

PM Proof:

User Info:

UID: 4233147

Username(s)

imsorri1

rsx - December 10, 2019, 12:39 am

There's gotta be someone with a VM on here to test this.

I'm willing to be it's a RAT.

SIM-1729678 - December 10, 2019, 12:40 am

Nice alert. Curious if the file is actually infected.

Harald - December 10, 2019, 12:40 am

(Dec 10, 2019 01:39 AM)Nuzi Wrote: [\[CITE\]](#) There's gotta be someone with a VM on here to test this.

I'm willing to be it's a RAT.

I can send you the link, if you want?

rsx - December 10, 2019, 12:41 am

(Dec 10, 2019 01:40 AM)LiteDev Wrote: [\[CITE\]](#) I will send you the link if you want?

I don't have that type of stuff or knowledge to test it, I know there was someone on here a while ago

who used to test sus files in a VM.

Harald - December 10, 2019, 12:42 am

(Dec 10, 2019 01:41 AM)Nuzi Wrote: [\[CITE\]](#) I don't have that type of stuff or knowledge to test it, I know there was someone on here a while ago who used to test sus files in a VM.
If I get some free time, I will set up a VM and debug it.

In the meantime, if anyone wishes to take this task on, just say. I can send you the link.

rsx - December 10, 2019, 12:44 am

(Dec 10, 2019 01:42 AM)LiteDev Wrote: [\[CITE\]](#) If I get some free time, I will set up a VM and debug it.

In the meantime, if anyone wishes to take this task on, just say. I can send you the link.
Let us know what you find, his profile is for sure suspicious with an upgrade already with only 3 posts sending random links.

Harald - December 10, 2019, 12:45 am

(Dec 10, 2019 01:44 AM)Nuzi Wrote: [\[CITE\]](#) Let us know what you find, his profile is for sure suspicious with an upgrade already with only 3 posts sending random links.
Exactly, The virus scan has picked up a detection as well, which is not normal behaviour for a PDF Document.

Natas - December 10, 2019, 12:48 am

[Bastille](#) your time to shine buddy enlighten us with your knowledge buddy.

Could be false positive could be a virus I cant really tell and am not gonna test it lmao.
although im going to upload one of my ebooks and see if it shows a false positive or not because im curious
and its pretty sketchy that dude has no posts giving a ebook he had 1 thread but it got deleted and I cant see what it is
so in my opinion it is super sketchy

Harald - December 10, 2019, 12:50 am

(Dec 10, 2019 01:48 AM)Natas Wrote: [\[CITE\]](#) [Bastille](#) your time to shine buddy enlighten us with your knowledge buddy.

Could be false positive could be a virus I cant really tell and am not gonna test it lmao.
although im going to upload one of my ebooks and see if it shows a false positive or not because im curious
and its pretty sketchy that dude has no posts giving a ebook he had 1 thread but it got deleted and I cant see what it is
so in my opinion it is super sketchy
Yes, I should mention somewhere this isn't confirmed a threat. However, giving the following circumstances I'm at least 80% sure this is user is trying his luck to infect unaware users that may fall for this.

Update; <https://hackforums.net/showthread.php?tid=6031692>

Natas - December 10, 2019, 12:52 am

Also looks like it could be a lost / stolen account

Password Reset in Last Week: Yes

Last Password Change: Yesterday

crypt - December 10, 2019, 12:58 am

Give me the link, will test it.

(Dec 10, 2019 01:40 AM)ScreemS Wrote: [\[CITE\]](#) Nice alert. Curious if the file is actually infected.

(Dec 10, 2019 01:44 AM)Nuzi Wrote: [\[CITE\]](#) Let us know what you find, his profile is for sure suspicious with an upgrade already with only 3 posts sending random links.

(Dec 10, 2019 01:50 AM)LiteDev Wrote: [\[CITE\]](#) Yes, I should mention somewhere this isn't confirmed a threat. However, giving the following circumstances I'm at least 80% sure this is user is trying his luck to infect unaware users that may fall for this.

Update; <https://hackforums.net/showthread.php?tid=6031692>

(Dec 10, 2019 01:52 AM)Natas Wrote: [\[CITE\]](#) Also looks like it could be a lost / stolen account

Password Reset in Last Week: Yes

Last Password Change: Yesterday

I believe this file isn't actually a virus.

Now, I would NOT open this on a PC or disregard it because of my following statement.

But you can see: <https://hackforums.net/showthread.php?tid=6031640>

He responded to this, I'm 75% sure he's spreading a referral link rather than a virus.

Bass_Reeves - December 10, 2019, 1:34 am

Hahah, literally same thing just happened to me. Morning coffee, and everything.

Thought to myself..."not today Satan".

?

Dracaryzs - December 10, 2019, 1:35 am

It's not a RAT. It's a JavaScript Tamper Monkey script to change Bitcoin receiving address.

Bastille - December 10, 2019, 1:35 am

[Natas](#) Thanks for mentioning, old my beer

[Harald](#) Can you send me the link ?

By the way, should we move this thread to the White hat section admins ?

Edit : Get the link into the Virus Total link

Harald - December 10, 2019, 1:37 am

(Dec 10, 2019 02:35 AM)Yseurk Wrote: [\[CITE\]](#) [Natas](#) Thanks for mentioning, old my beer

[Harald](#) Can you send me the link ?

By the way, should we move this thread to the White hat section admins ?

I have provided you with the link.

SIM-1729678 - December 10, 2019, 1:42 am

(Dec 10, 2019 02:35 AM)Dracaryzs Wrote: [\[CITE\]](#) It's not a RAT. It's a JavaScript Tamper Monkey script to change Bitcoin receiving address.

You sure about this?

cryp - December 10, 2019, 1:44 am

Under closer inspection, this is not your typical "virus". It is a bitcoin address replacer for G2a. Similar to the LocalBitcoins one we saw recently which is just a tampermonkey script which replaces the payment address on payment coupled with an ebook saying the script is to trick (website) into refunding you. Ex. Timezone exploit, double spend exploit, etc.

The script is encrypted.

<https://www.blockchain.com/btc/address/3JUkCKFaBB7RjtmgnS83JmbNSvQ2AhfhWd>

His btc addy ^

Seems he just scammed someone for \$40. :(

(Dec 10, 2019 02:42 AM)ScreemS Wrote: [\[CITE\]](#) You sure about this?
I have confirmed this. Above! :)

(Dec 10, 2019 02:35 AM)Yseurk Wrote: [\[CITE\]](#) [Natas](#) Thanks for mentioning, old my beer

[Harald](#) Can you send me the link ?

By the way, should we move this thread to the White hat section admins ?

Edit : Get the link into the Virus Total link
I already did the digging. Read my post :)

Bastille - December 10, 2019, 2:05 am

(Dec 10, 2019 02:44 AM)cryp Wrote: [\[CITE\]](#) Under closer inspection, this is not your typical "virus". It is a bitcoin address replacer for G2a. Similar to the LocalBitcoins one we saw recently which is just a tampermonkey script which replaces the payment address on payment coupled with an ebook saying the script is to trick (website) into refunding you. Ex. Timezone exploit, double spend exploit, etc.

The script is encrypted.

<https://www.blockchain.com/btc/address/3JUkCKFaBB7RjtmgnS83JmbNSvQ2AhfhWd>

His btc addy ^

Seems he just scammed someone for \$40. :(

I have confirmed this. Above! :)

I already did the digging. Read my post :)
Found the same thing, don't need be worried about the PDF's file it's clean, thanks [cryp](#)

Dracaryzs - December 10, 2019, 2:18 am

(Dec 10, 2019 02:42 AM)ScreemS Wrote: [\[CITE\]](#) You sure about this?
Pretty sure. ?

Eagle 95 - December 10, 2019, 2:26 am

Thank you for reporting.

Omniscient - December 10, 2019, 9:29 am

He sent mass PM spam. Probably infected but he is closed now just for the mass PM.