

Forum: [Hack Forums](#)

Thread: [\[SOLVED\]](#)

BLKLXVESMATTER! - September 8, 2016, 7:47 pm

[illegible]

?Creative - September 8, 2016, 7:49 pm

Well i wouldnt be shocked, <https://hackforums.net/trustscan.php?uid=1313225>

you haven't enabled 2fa which i recommend doing because if you lose your account and you didnt have it enabled the account gets closed.

?Synapse - September 8, 2016, 7:49 pm

Nothing you can prove for sure unfortunately as anyone can rep anyone without a reason. What if the RATTter possibly repped those two users to frame them?

Target™ - September 8, 2016, 7:50 pm

why don't you delete that first post?

SIM-2502833 - September 8, 2016, 7:51 pm

What member downloaded the file? May I have the file? We can find who did this.

Steve - September 8, 2016, 7:54 pm

Maybe you should give yourself a vacation ban until this gets sorted out. Sorry this happened to you, thanks for the warning.

BLKLXVESMATTER! - September 8, 2016, 7:56 pm

(Sep 8, 2016 07:51 PM)MrMcShroom Wrote: [\[CITE\]](#) What member downloaded the file? May I have the file? We can find who did this.

I will PM you the file.

(Sep 8, 2016 07:49 PM)?Creative Wrote: [\[CITE\]](#) Well i wouldnt be shocked,

<https://hackforums.net/trustscan.php?uid=1313225>

you haven't enabled 2fa which i recommend doing because if you lose your account and you didnt have it enabled the account gets closed.

I've added 2fa now, thanks for the reminder.

I'll try find proof to link it to those guys.

Codefuser - September 8, 2016, 8:06 pm

(Sep 8, 2016 07:51 PM)MrMcShroom Wrote: [\[CITE\]](#) What member downloaded the file? May I have the file? We can find who did this.

Download it from Hybrid-Analysis ?

Edit: nvm sample not shared. OP PM me also please.

BLKLXVESMATTER! - September 8, 2016, 8:20 pm

(Sep 8, 2016 08:06 PM)Codefuser Wrote: [\[CITE\]](#) Download it from Hybrid-Analysis ?

Edit: nvm sample not shared. OP PM me also please.
I've sent you a PM.

MasterCurser - September 8, 2016, 8:21 pm

This could be a perfect way to frame someone. Not saying that you are but could.

Both the other users that you are accusing have such low rep. (curious)

Gary - September 8, 2016, 8:26 pm

If they logged inTo your account check your IP logins lol. There's no way a login isn't logged on it

BLKLXVESMATTER! - September 8, 2016, 8:27 pm

(Sep 8, 2016 08:21 PM)MasterCurser Wrote: [\[CITE\]](#) This could be a perfect way to frame someone. Not saying that you are but could.

Both the other users that you are accusing have such low rep. (curious)

I agree, it's just a big feeling I have it's those two... The Roy Wood\$ guy is the guy who posted on the thread saying "Downloaded, works fine thanks" or whatever and the person who got the rep about \$850 btc...

MasterCurser - September 8, 2016, 8:33 pm

(Sep 8, 2016 08:27 PM)Sup? Wrote: [\[CITE\]](#) I agree, it's just a big feeling I have it's those two... The Roy Wood\$ guy is the guy who posted on the thread saying "Downloaded, works fine thanks" or whatever and the person who got the rep about \$850 btc...

Could very easily be them. Or if someone was actually thinking and wanted to frame you and Roy Wood\$. That would be interesting. lol

Just post the trust scan of Roy Wood\$ too - <https://hackforums.net/trustscan.php?uid=596576>

No need to even doubt you after that.

BLKLXVESMATTER! - September 8, 2016, 8:46 pm

(Sep 8, 2016 08:33 PM)MasterCurser Wrote: [\[CITE\]](#) Could very easily be them. Or if someone was actually thinking and wanted to frame you and Roy Wood\$. That would be interesting. lol

Just post the trust scan of Roy Wood\$ too - <https://hackforums.net/trustscan.php?uid=596576>

No need to even doubt you after that.

It's probably a shared account stolen from the HF database leak from long ago.

Codefuser - September 8, 2016, 8:50 pm

Scan of the archive:

<https://www.virustotal.com/en/file/0c4b8dcd0c98b99bc3f75724a0155f22251a0c1c4e8eb491441054f265a686ff/analysis/1473392005/>

iLCH+v4 (11).exe appears to be clean.

iLCH+v4.exe is protected with confuserex 1.9

Will update more

BLKLXVESMATTER! - September 8, 2016, 8:53 pm

(Sep 8, 2016 08:26 PM)Gary. Wrote: [\[CITE\]](#) If they logged inTo your account check your IP logins lol.

There's no way a login isn't logged on it

Literally only my IP's showing up. Which I think they used the RAT on my pc while I was out or asleep to post it. They tried and changed my password a moment ago, but all my shit's secure now.

Stashyy - September 8, 2016, 9:17 pm

(Sep 8, 2016 08:53 PM)Sup? Wrote: [\[CITE\]](#) Literally only my IP's showing up. Which I think they used the RAT on my pc while I was out or asleep to post it. They tried and changed my password a moment ago, but all my shit's secure now.

Strange but they could of possibly done that easily using some features on mainly every rat. Just make sure that you get your PC checked out etc.

BLKLXVESMATTER! - September 8, 2016, 9:51 pm

(Sep 8, 2016 09:17 PM)Stashy Wrote: [\[CITE\]](#) Strange but they could of possibly done that easily using some features on mainly every rat. Just make sure that you get your PC checked out etc.

Yeah, hopefully I've secured everything alright. I'll be reverse engineering the files from tomorrow, I'll find the culprit with his pants down.

Bluffer - September 8, 2016, 10:09 pm

I hope you can secure your account dude, might be a good idea to self ban yourself until you can figure this one out... also get 2FA if you don't have it yet!

Mali - September 8, 2016, 11:14 pm

PM me the file, I'll analyze it. And find out exactly what it contains and report back to ya fam. For now. I'd suggest running a Malwarebytes scan, and possibly checking your APPDATA and TEMP folders.

Be sure to run a Netstat as well, to see if any connections pop up.

Codefuser - September 9, 2016, 12:52 am

This is an analysis of the file the user sent to me. The file is the payload that infected OP. Surprisingly, it is poorly designed and named itself "svhost.exe".

Hybrid Analysis:

<https://www.hybrid-analysis.com/sample/f4d516d65fc242cd5affe0f2da8ac6eb28a437f406b44390977d4d656be3edae?environmentId=100>

Process: svhost.exe

Startup key: HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows with the key "Load"

File location: %TEMP%\yeee\ewww.exe

OP should download and install Process Hacker, kill the process svhost.exe (NOT SVCHOST!) and remove the key using regedit. Not sure about the damage done and the information stolen.

Mr. Robot - September 9, 2016, 1:16 am

Just for anyone wondering, you can use my little trick to view that thread title.

Go the the page, then view the source - you will see

"Junk-JUNK: iLCH v4 Cracked [All Cod Tool] DO NOT DOWNLOAD (IM COMPROMISED)"

Not able to check the file myself right now, does anyone have a DNS entry on it?

Scanning both exes

iLCH v4.exe

<https://www.virustotal.com/en/file/91ccb8062ee90158f728d0c1593f7e3358f0fe8a7a1bb3da386e3f991b3c2acf/analysis/1473409379/>

iLCHv4 11.exe

<https://www.virustotal.com/en/file/34c39730c7d7625460904f79215093958f592aebb1889a5a569fadc81de0c480/analysis/1473409280/>

You can see the original file here

Code

http://webcache.googleusercontent.com/search?q=cache:YabhUZU_xSoJ:hackforums.net/printthread.php%3Ftid%3D5399301+&cd=5&hl=en&ct=clnk&gl=nz&client=firefox-b

Mali - September 9, 2016, 1:19 am

(Sep 9, 2016 12:52 AM)Codefuser Wrote: [\[CITE\]](#) This is an analysis of the file the user sent to me. The file is the payload that infected OP. Surprisingly, it is poorly designed and named itself "svhost.exe".

Hybrid Analysis:

<https://www.hybrid-analysis.com/sample/f4d516d65fc242cd5affe0f2da8ac6eb28a437f406b44390977d4d656be3edae?environmentId=100>

Process: svhost.exe

Startup key: HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows with the key "Load"

File location: %TEMP%\yeee\ewww.exe

OP should download and install Process Hacker, kill the process svhost.exe (NOT SVCHOST!) and remove the key using regedit. Not sure about the damage done and the information stolen. Hit me with the file. I'm going to tear into it and do some extensive anal probing.

Codefuser - September 9, 2016, 1:21 am

(Sep 9, 2016 01:16 AM)Mr. Robot Wrote: [\[CITE\]](#) Just for anyone wondering, you can use my little trick to view that thread title.

Go to the page, then view the source - you will see

"Junk-JUNK: iLCH v4 Cracked [All Cod Tool] DO NOT DOWNLOAD (IM COMPROMISED)"

Not able to check the file myself right now, does anyone have a DNS entry on it?

Check the hybrid-analysis above. You can sign up and download the file that infected OP. Gunna PM you the file

@Mali just sign up and download from hybrid. I uploaded there for a reason.

Mali - September 9, 2016, 1:25 am

(Sep 9, 2016 01:21 AM)Codefuser Wrote: [\[CITE\]](#) Check the hybrid-analysis above. You can sign up and download the file that infected OP. Gunna PM you the file

@Mali just sign up and download from hybrid. I uploaded there for a reason.

Thats fine fam. Thanks for the information on how to obtain the file. I'll post back with my results.

Mr. Robot - September 9, 2016, 1:29 am

(Sep 9, 2016 01:21 AM)Codefuser Wrote: [\[CITE\]](#) Check the hybrid-analysis above. You can sign up and download the file that infected OP. Gunna PM you the file

@Mali just sign up and download from hybrid. I uploaded there for a reason.

Trying to remember that boss ass site that would run it in a virtual environment nice and easy - it was better than hybrid but I can't remember the fucking site name.'

Oh it was <https://malwr.com/> but they are down

Mali - September 9, 2016, 1:33 am

(Sep 9, 2016 01:29 AM)Mr. Robot Wrote: [\[CITE\]](#) Trying to remember that boss ass site that would run it in a virtual environment nice and easy - it was better than hybrid but I can't remember the fucking site name.'

Oh it was <https://malwr.com/> but they are down

Anubis used to. However I don't think they do anymore.

BLKLXVESMATTER! - September 9, 2016, 1:38 am

i think problem has been solved thanks anyways guys

Mr. Robot - September 9, 2016, 2:04 am

I downloaded the file hosted at Mega on the original thread and the hash is different than the file OP sent the other user.

<https://www.virustotal.com/en/file/ed2ab45787b7c7ef8e856366ac29c0faa80ba774ff055b2d87f7de0ac82d3d75/analysis/1473411810/>

(Sep 8, 2016 08:50 PM)Codefuser Wrote: [\[CITE\]](#) Scan of the archive:

<https://www.virustotal.com/en/file/0c4b8dcd0c98b99bc3f75724a0155f22251a0c1c4e8eb491441054f265a686ff/analysis/1473392005/>

iLCH+v4 (11).exe appears to be clean.

iLCH+v4.exe is protected with confuserex 1.9

Will update more

That sha and file name doesn't match the original file on that thread.

<https://www.virustotal.com/en/file/ed2ab45787b7c7ef8e856366ac29c0faa80ba774ff055b2d87f7de0ac82d3d75/analysis/1473411810/>

Original file

Code

http://webcache.googleusercontent.com/search?q=cache:YabhUZU_xSoJ:hackforums.net/printthread.php%3Ftid%3D5399301+&cd=5&hl=en&ct=clnk&gl=nz&client=firefox-b

SIM-2502833 - September 9, 2016, 6:07 am

Also, to clarify, the chances of this actually being solved, or the OP being compromised are about equal, hopefully someone notices this.

(Sep 9, 2016 02:04 AM)Mr. Robot Wrote: [\[CITE\]](#) I downloaded the file hosted at Mega on the original thread and the hash is different than the file OP sent the other user.

<https://www.virustotal.com/en/file/ed2ab45787b7c7ef8e856366ac29c0faa80ba774ff055b2d87f7de0ac82d3d75/analysis/1473411810/>

That sha and file name doesn't match the original file on that thread.

<https://www.virustotal.com/en/file/ed2ab45787b7c7ef8e856366ac29c0faa80ba774ff055b2d87f7de0ac82d3d75/analysis/1473411810/>

Original file

Code

http://webcache.googleusercontent.com/search?q=cache:YabhUZU_xSoJ:hackforums.net/printthread.php%3Ftid%3D5399301+&cd=5&hl=en&ct=clnk&gl=nz&client=firefox-bDownloaded the original file, doing a hybrid scam, we'll see pretty quick if it's a different file, and that would be fishy af.

Codefuser - September 9, 2016, 8:54 am

(Sep 9, 2016 02:04 AM)Mr. Robot Wrote: [\[CITE\]](#) I downloaded the file hosted at Mega on the original thread and the hash is different than the file OP sent the other user.

<https://www.virustotal.com/en/file/ed2ab45787b7c7ef8e856366ac29c0faa80ba774ff055b2d87f7de0ac82d3d75/analysis/1473411810/>

That sha and file name doesn't match the original file on that thread.

<https://www.virustotal.com/en/file/ed2ab45787b7c7ef8e856366ac29c0faa80ba774ff055b2d87f7de0ac82d3d75/analysis/1473411810/>

Original file

Code

http://webcache.googleusercontent.com/search?q=cache:YabhUZU_xSoJ:hackforums.net/printthread.php%3Ftid%3D5399301+&cd=5&hl=en&ct=clnk&gl=nz&client=firefox-b
I have 2 files. That file is the original file that infected OP.

BLKLXVESMATTER! - September 9, 2016, 9:21 am

so was anyone able to trace this?

Mr. Robot - September 9, 2016, 6:04 pm

(Sep 9, 2016 08:54 AM)Codefuser Wrote: [\[CITE\]](#) I have 2 files. That file is the original file that infected OP.

If that's the case, why do they have different shas ?

Codefuser - September 9, 2016, 8:19 pm

(Sep 9, 2016 06:04 PM)Mr. Robot Wrote: [\[CITE\]](#) If that's the case, why do they have different shas ?
Because the file uploaded in the link is a different file.

So the file I sent to you is what infected OP.

After that, OP's account is used to post another file (the one you got).

Hammer prod - September 9, 2016, 10:57 pm

Hooe rhis is legit solved, will suck if not solved

Sup_Compromised - *September 12, 2016, 2:43 am*

Fuck sake... The fucker got my account closed!?

Wow.. I'm so pissed. 4 years on here down the drain.... Hopefully Omni can like, merge the posts etc to this account or uncloze it.