

Forum:[Hack Forums](#)

Thread: [My Observation: Byte Crypter - Be Careful, crypts are binded with downloader](#)

sbuzza - December 12, 2013, 7:59 am

Edited the title to show that this is my observation and findings, and true from my belief.

Disclaimer: This is true based on my findings as of 12/12/2013. The crypter may get updated to alter or remove this functionality.

Summary: Byte Crypter binds a downloader with the files it crypts, that downloads a BitCoin miner from

`http : // www . diablo3keygen . net / crvbox . exe` after 20 minutes of file execution.

Details: So I recently bought Byte Crypter (<https://hackforums.net/showthread.php?tid=3463236>). Crypted my RAT server file. Byte Crypter made it FUD, which is good. I update a bunch of my slaves with this crypted file, and they all connected back to me good. After a while I noticed a bunch of them had the same vbc error showing up on their screen. So I got a little suspicious, as to what was happening. It had to be either my RAT (but that has never shown this issue before) or the Byte Crypter which was a new entity in my setup. To get to the bottom of this:

1. I work for a place that has a lot of machines lying around. I picked two of them and set them up with brand new OS (lets call them Machine1 and Machine2).
2. Checked to make sure nothing was installed on the startup of these machines.
3. I then created a .net app that just shows a MessageBox with foo in it. (lets call it MyApp.exe). its code is just `MessageBox.Show("foo");`
4. Then crypted MyApp.exe with Byte Crypter (lets call this crypted file MyAppCrypted.exe).
5. Ran MyApp.exe on Machine1, and my MyAppCrypted.exe on Machine2. Both showed the messagebox with foo, which I closed.
6. Checked startup of both and both were clean.
7. Came 30 minutes later, and Machine1 still had nothing installed in the startup, but Machine2 had something setup in the startup, that could not be disabled
8. cleaned both machines again to new OS and this time repeated the same thing, but kept fiddler running
9. Came 30 minutes later, and Machine1 showed no fiddler activity, but Machine2 had downloaded a file from `http : // www . diablo3keygen . net / crvbox . exe`
10. Checked the size of crvbox.exe and it was 241kb
11. Checked the size of crvbox.exe next day, and now it was 299kb. so this file is actively getting updated as well to be the newest or fuddest.

Sent a Pm to Mark, the seller of Byte Crypter and he says his crypter is clean and its either my foo app that is downloading the miner or my internet connection is doing that. To check that I tried the same experiment on a machine at home (a different internet connection) and same results as before. So blaming this on `MessageBox.Show("foo")`, or internet connection or Microsoft having built this into their OS is a far fetched thing than the crypter actually being bugged to download the miner. Do as you please with this information.

BoomShot - December 12, 2013, 8:03 am

You're going to need to actually provide evidence of this accusation regarding his product being backdoored.

Treeple - December 12, 2013, 8:04 am

Wow this is a serious thing I must admit! However I think this thread belongs in the marketplace discussion forum.

Thx for the share though!

Cletus Kasady - December 12, 2013, 8:06 am

You're going to need actual proof like pictures or if you can decode it, a story isn't going to cut it.

sbuzza - December 12, 2013, 8:06 am

If you are a customer of Byte Crypter than you can experiment for yourself. My job was to inform the public of what I found. I am not sure what proof/evidence you are seeking. If you do experiment, remember the downloader kicks in 20 minutes after the crypted file execution. Get fiddler to see it go for the miner file. It is likely that the file itself will be deleted when the owner/seller of Byte see this.

BTW the Byte Crypter TOS say we cant run the crypted files in a VM or SandBoxie. Makes me think why that is. Makes sense to not allow to run Crypter in VM, but crypted files in VM can only be disallowed if they are scared we will be able to do such tests to find out the truth. Just saying. Don't take my word for it. Do your due diligence.

BoomShot - December 12, 2013, 8:10 am

It's not a matter of being incapable of performing the necessary task, it's the fact that you're making a very serious accusation towards another member's product without the proper evidence to back up the claim. So it appears to just be sales bashing, but if you can prove it then it's a very serious issue that must be looked into it and handled appropriately.

Bull™ - December 12, 2013, 8:11 am

I am the son in law of barak Obama, Just trying to make a stroy like you but think I am not good as you .

241kb miner, I Cant belive it,Cause the miner will download more then 1 exe and 3 dl.

Post some real proofs before open your fucking mouth.

sbuzza - December 12, 2013, 8:13 am

tell me how you want me to prove it? fiddler picture?

I am not sure how to prove a binded downloader downloading stuff!!

BoomShot - December 12, 2013, 8:31 am

(Dec 12, 2013 09:13 AM)sbuzza Wrote: [\[CITE\]](#) tell me how you want me to prove it? fiddler picture?

I am not sure how to prove a binded downloader downloading stuff!!

If you can prove it with screen shots, then go for it.

You could simply record it. Regardless, there needs to be evidence.

Royal ! - December 12, 2013, 8:42 am

Stop Spreading this fake Bullshit Regarding my Product. It is Online Now Since November 2011 And i am Earning more then enough from it each Month, Earning such amounts which are not even in your Range of thoughts, So I don't need to backdoor any shit or do any miner thing with it. Furthermore, I have Lots of other people using Byte Crypter and you are NOT the only one who used Byte. And Not a single other person reported any such issue to Me. Further, I Don't allow to use Byte Crypter in Vm's and Sandboxes Because Idiots like you Have like 5-7 Sample Collecting

AV's installed on your VM's and you fucktards Totally FUCK the crypter By running crypted files in VM's with your various Sample Collecting AV's installed there. And Just to let you know furthermore, Many Other Crypter Owners and Sellers I am not taking names of Cos I don't want to spoil my friendship with them, they Also DO NOT allow to use their Product in VM's . Does that make them suspicious as well? ???

Your Account from Byte Crypter is Banned.

And now you Can FUCK OFF and create more bullshit about Byte. IDGAF about it.

BoomShot - December 12, 2013, 8:47 am

(Dec 12, 2013 09:42 AM)Mark ! Wrote: [\[CITE\]](#) Stop Spreading this fake Bullshit Regarding my Product. It is Online Now Since November 2011 And i am Earning more then enough from it each Month, Earning such amounts which are not even in your Range of thoughts, So I don't need to backdoor any shit or do any miner thing with it. Furthermore, I have Lots of other people using Byte Crypter and you are NOT the only one who used Byte. And None a single other person reported any such issue to Me. Further, I Don't allow to use Byte Crypter in Vm's and Sandboxes Because Idiots like you Have like 5-7 Sample Collecting AV's installed on your VM's and you fucktards Totally FUCK the crypter By running crypted files in VM's with your various Sample Collecting AV's installed there. And Just to let you know furthermore, Many Other Crypter Owners and Sellers I am not taking names of Cos I don't want to spoil my friendship with them, they Also DO NOT allow to use their Product in VM's . Does that make them suspicious as well? ???

Your Account from Byte Crypter is Banned.

And now you Can FUCK OFF and create more bullshit about Byte. IDGAF about it.

There's nothing wrong with disallowing the use of virtual machines when it comes to the product, I'm the same way and I know many others are as well.

Mace - December 12, 2013, 8:47 am

Sbuzza you didn't proof anything, my guess would be your a kid spreading false rumors about bytecrypter.

Royal ! - December 12, 2013, 8:48 am

(Dec 12, 2013 09:47 AM)BoomShotKapow Wrote: [\[CITE\]](#) There's nothing wrong with disallowing the use of virtual machines when it comes to the product, I'm the same way and I know many others are as well.

I Did not said "ALL". I said "Various". Ok thank you for clarifying yourself.

sbuzza - December 12, 2013, 9:05 am

Thanks for banning my Byte Crypter account, which is fine since I wasn't going to use a backdoor-ed product anyway.

As for the proof... I provided my observations and findings and made it clear that that is what they were. If you are Byte Crypter customer, and wish to do due diligence, feel free to test it yourself as appropriate. As for not allowing the use of VMs because the VMs may have file collection AVs, then guess what that is exactly the setup on the slave machines where your crypted server files are run... the slave machines have lots of varieties of AVs that collect... so not allowing the crypted file (not talking about the crypter itself) to run on the cryptee's VM doesn't make it anymore safer than the same crypted file being run all over the place on different slave machines.

BoomShot - December 12, 2013, 9:07 am

(Dec 12, 2013 10:05 AM)sbuzza Wrote: [\[CITE\]](#) Thanks for banning my Byte Crypter account, which

is fine since I wasn't going to use a backdoor-ed product anyway.

As for the proof... I provided my observations and findings and made it clear that that is what they were. If you are Byte Crypter customer, and wish to do due diligence, feel free to test it yourself as appropriate. As for not allowing the use of VMs because the VMs may have file collection AVs, then guess what that is exactly the setup on the slave machines where your crypted server files are run... the slave machines have lots of varieties of AVs that collect... so not allowing the crypted file (not talking about the crypter itself) doesn't make it anymore safer than the same crypted file being run all over the place on different slave machines.

This is why you're banned, you're making accusations that you can't even back up with evidence.

Until there's proof, no one will listen to your story and take it seriously.

Bat™ - December 12, 2013, 10:26 am

Guys do your crypt right now OTHERWISE HE'LL UPDATE IT AND REMOVE IT FROM THE SOFTWARE and you would have no evidence left against him.

I believe you should have a backup of that crypted file from BYTE Crypter or anyone who has previous files should submit it to MRT Team to check if its backdoored or not.

Good thing you did bro, but it needs some proof to backup all that you have said. It's a good thing that people are really coming out against these cunts and not caring about the rep but the community. :)

(Dec 12, 2013 09:42 AM)Mark ! Wrote: [\[CITE\]](#) Stop Spreading this fake Bullshit Regarding my Product. It is Online Now Since November 2011 And i am Earning more then enough from it each Month, Earning such amounts which are not even in your Range of thoughts, So I don't need to backdoor any shit or do any miner thing with it. Furthermore, I have Lots of other people using Byte Crypter and you are NOT the only one who used Byte. And Not a single other person reported any such issue to Me. Further, I Don't allow to use Byte Crypter in Vm's and Sandboxes Because Idiots like you Have like 5-7 Sample Collecting AV's installed on your VM's and you fucktards Totally FUCK the crypter By running crypted files in VM's with your various Sample Collecting AV's installed there. And Just to let you know furthermore, Many Other Crypter Owners and Sellers I am not taking names of Cos I don't want to spoil my friendship with them, they Also DO NOT allow to use their Product in VM's . Does that make them suspicious as well? ???

Your Account from Byte Crypter is Banned.

And now you Can FUCK OFF and create more bullshit about Byte. IDGAF about it.
I really like how rude you are to others. You said all the "goody-goody" things about your crypter which are totally FAR AWAY from this discussions.

This makes me think that it is indeed backdoored.

@OT send the files to KFC watermelon :)

sbuzza - December 12, 2013, 10:54 am

(Dec 12, 2013 11:17 AM)KFC Watermelon Wrote: [\[CITE\]](#) Send me a crypted file and I will test these claims.

sending you link to the crypted MyAppCrypted.exe file via pm... which should bring up dialogbox foo, and then 20 minutes later download the file I mentioned, or atleast try to download it... might fail to download if the file has been removed from that place

Bat™ - December 12, 2013, 10:59 am

(Dec 12, 2013 11:54 AM)sbuzza Wrote: [\[CITE\]](#) sending you link to the crypted MyAppCrypted.exe file via pm... which should bring up dialogbox foo, and then 20 minutes later download the file I mentioned, or atleast try to download it... might fail to download if the file has been removed from that place

I went to that dl you posted, it has been removed by Mark! lol.

sbuzza - December 12, 2013, 11:02 am

(Dec 12, 2013 11:59 AM)Bat™ Wrote: [\[CITE\]](#) I went to that dl you posted, it has been removed by Mark! lol. Off course it has been. Why would it not be. However to anyone who wants to try, I can provide the crypted My Simple foo dialog app, and you can use any network/http sniffer to see the downloader binded by Byte going for that file after some delay (in my tests the delay was 20 minutes, but may be random depending on what it was set in the downloader)

Bat™ - December 12, 2013, 11:09 am

(Dec 12, 2013 12:02 PM)sbuzza Wrote: [\[CITE\]](#) Off course it has been. Why would it not be. However to anyone who wants to try, I can provide the crypted My Simple foo dialog app, and you can use any network/http sniffer to see the downloader binded by Byte going for that file after some delay (in my tests the delay was 20 minutes, but may be random depending on what it was set in the downloader)

Send to me via PM ? Will report results after checking the file. Also I would like Byte Crypter customers to come up and send their file samples (they created before 12/13/2013) to MRT team if they really have backdoored their crypter. If you wish you can send them to me also via PM :)

NOTE : Do not get scared by Mark's neg's. This kid wouldn't be able to do anything if we talk via PM's. If you post it in public, he might ban you account. So be careful :)

J?ck - December 12, 2013, 11:11 am

No pcaps? No screenshots? Yeah, we need more than that.

sbuzza - December 12, 2013, 11:35 am

Bat I sent you via PM the file link of my foo dialog app crypted by Byte. Thanks.

stefsot - December 12, 2013, 12:24 pm

(Dec 12, 2013 12:20 PM)KFC Watermelon Wrote: [\[CITE\]](#) I got OPs file and will provide a complete analysis.

Our only option is to wait for the result.

We shall see.

x64 - December 12, 2013, 12:47 pm

(Dec 12, 2013 01:24 PM)stefsot Wrote: [\[CITE\]](#) Our only option is to wait for the result.

We shall see.

Indeed, I'm really intrested if this story is true or not. We shall see.

Post ss's please.

TreeChar - December 12, 2013, 1:03 pm

WinUpdate.exe is the default process name of crypted file.

I own byte crypter and have tested it twice after i saw this thread.

I got nothing on the freshly installed OS.

Looks clean to me.

sbuzza - December 12, 2013, 1:21 pm

TreeChar, If you are using the same crypter as was there this morning, wait for 20 mins after executing the crypted file and look in fiddler to see any attempt to download another exe. There is a delay execution. the additional file it was downloading 20 mins after execution has since been taken offline, so you will not see anything happen anymore, but will see the ping to try and download the file from <http://www.diablo3keygen.net/crvbox.exe>

(Dec 12, 2013 02:03 PM)TreeChar Wrote: [\[CITE\]](#) WinUpdate.exe is the default process name of crypted file.

I own byte crypter and have tested it twice after i saw this thread.

I got nothing on the freshly installed OS.

Looks clean to me. Just FYI: When crypting, I did not select the Install options in Byte Crypter.

TreeChar - December 12, 2013, 1:33 pm

(Dec 12, 2013 02:21 PM)sbuzza Wrote: [\[CITE\]](#) TreeChar, If you are using the same crypter as was there this morning, wait for 20 mins after executing the crypted file and look in fiddler to see any attempt to download another exe. There is a delay execution. the additional file it was downloading 20 mins after execution has since been taken offline, so you will not see anything happen anymore, but will see the ping to try and download the file from <http://www.diablo3keygen.net/crvbox.exe>

Just FYI: When crypting, I did not select the Install options in Byte Crypter.

No Connection over there,

been 1 hr file is running, Crypted yesterday.

I also got an av with firewall, if there was any connection then It must have catch it.

(Dec 12, 2013 02:23 PM)KFC Watermelon Wrote: [\[CITE\]](#) I can't find anything to support Mark! being the owner of this site, other than I believe he is from India, and the site is hosted in India.

Mark had an us verified business paypal where i payed,

From that I Can say he is from US.

and I believe mark crypter is clean, am using from few weeks.

Cause if it was binded with the story made by OP then all the crypter users along with me have been infected Cause all test there crypted file in the main os only.

I am with mark, op is making stories here, or used the download/execute option from the crypter by mistake.

AffProfit - December 12, 2013, 3:08 pm

(Dec 12, 2013 09:11 AM)Bull™ Wrote: [\[CITE\]](#) I am the son in low of barak Obama, Just trying to make a stroy like you but think I am not good as you .

241kb miner, I Cant belive it,Cause the miner will download more then 1 exe and 3 dl.

Post some real proofs before open your fucking mouth.

Learn to know how to spell your father in laws name, mr son in low or barak Obama.

kalandershihabrocker - December 13, 2013, 5:23 am

(Dec 12, 2013 02:48 PM)KFC Watermelon Wrote: [\[CITE\]](#) I have nothing against Mark, at all, and a lot of my customers use his crypter and say it's great. However, I do believe he has a PayPal holder. I'm 90% sure he is from India, or at least a foreign country, as English is not his primary language.

Yes, he's Indian. He also has a chevrolet Beat as his car. Saw him post this somewhere.

Qmz_ - December 13, 2013, 3:40 pm

(Dec 12, 2013 09:11 AM)Bull™ Wrote: [\[CITE\]](#) 241kb miner, I Cant belive it,Cause the miner will

download more then 1 exe and 3 dl.

Actually my older miner(no external files like dll etc.) which is coded in C++, has nice size of 204kb, and it doesn't download or drop files. It works with GPU+CPU. :)

Hyphyxo - December 13, 2013, 7:09 pm

p.sure <http://www.diablo3keygen.net/> is owned by man_of_my_word and all his fanboys all up in this thread.

/thread cy@

G33K - January 1, 2024, 9:44 pm

Anyone know where i can getr the link to thios crypter i payedd lifetime opackage and he always mailed me link but now its impossible to get a hand of this...