

Forum:[Hack Forums](#)

Thread: [Coinminer with Bank Trojans ?](#)

UnNamedHacker - April 30, 2012, 1:02 am

Well so here it is

i've been snooping around on Coinminers Thread.

So here is what i saw .

[img]/img]

As you can see that post got deleted if you check the other pages.

So now.

If you have clicked the Scan.

Here's what it popped out.

Here's the link to the Scan Result.

Credits to the guy and Meta scan Click [HERE](#)

So i'm just wondering Why did the owner deleted post of the unencrypted bin scan and why does it have ngrbot/Zues bot and banker trojans

I'm not really good at this kind but its really suspicious too see this alot of trojans .

SO can anyone clarify this or what ?

I'm not bashing threads or something but this is just suspicious.

66754 - April 30, 2012, 1:30 am

(Apr 30, 2012 01:18 AM)BV1 ? Wrote: [CITE](#) Scans can say whatever. I scanned my Insomnia and it's said blackshades before.

I've been using the bot quite a bit myself, it's legit. It's just downloading the miner.

It's a bitcoin miner, they wouldn't generally come up as an irc bot "ngrbot"

But yes the scans can generally say what ever as i have come across a few that said pissux.trojan.

Run the miner in wireshark if you are worried.

Also could i get your bin? i wouldn't mind taking a look.

W1tch - April 30, 2012, 8:11 am

I can say that I saw that post myself. While an AV scanner getting blackshades confused with Insomnia is quite easy for an AV company to make, getting a bitcoin miner confused with Zbot is much harder.

Hunter S Thompson - April 30, 2012, 9:38 am

(Apr 30, 2012 01:18 AM)BV1 ? Wrote: [CITE](#) Scans can say whatever. I scanned my Insomnia and it's said blackshades before.

I've been using the bot quite a bit myself, it's legit. It's just downloading the miner.

Yeah, because we all know that a download function usually means that injection is present (Zbot) and that it connects to irc (NgrBot), right?

UnNamedHacker - April 30, 2012, 9:37 pm

(Apr 30, 2012 01:26 PM)BV1 ? Wrote: [\[CITE\]](#) True, I do agree

However I just don't feel a scan is enough proof to base anything off of. If a couple of skilled users want to rip the miner apart, then any information I see from there I'd take note of, but honestly, scan reports can vary way too much.

well i'm not bashing any sales or ruining sales.

but i'm just suspicious unlike you guys you have knowledge in these stuff.

but sadly i'm not so i'm asking and i'm skeptical. :)

again sorry if i ruined or bash his sales.

W1tch - May 1, 2012, 10:07 am

It downloads the miner, so the 6KB ASM file is just a freaking downloader -_- I could make one that isn't FUD in C that's about 1.5KB :/

So I guess it's downloading some dodgy stuff (still doesn't explain the detection name).

I'm with BV1's idea, and I also think that bin should be sent to an AV company, and see if they'll explain why it has that detection (I smell C/P code).

Pineapple - May 1, 2012, 10:22 am

More than willing to let a HJT guy take a look at a coinMiner bin if you don't believe it's clean from that nasty stuff. Not only is the file only 6kb (not enough to house such larger executables such as ZeuS/ngrBot) but it's just AVs being silly.

Don't worry mate, we wouldn't sell something for a higher price than other miners just to bind it with our own stuff. Also BV1's explained it pretty well on this thread for us. @Beev, thanks.

DAMD - May 1, 2012, 10:24 am

Well, looks like I'll need to be careful with what I buy around here.

#cn - May 1, 2012, 10:25 am

So Zbot and Ngrbot are somehow both contained within a 6kb file? Sure, it could download them, but it wouldn't be detected as ngrbot for that, it would be detected as a downloader. Because it downloads.

(May 1, 2012 10:07 AM)W1tch Wrote: [\[CITE\]](#) (I smell C/P code).

So I c/p'd from zbot and ngrbot and somehow used that code in the ASM bins? Are you retarded?

UnNamedHacker - May 1, 2012, 7:57 pm

(May 1, 2012 10:25 AM)#cn Wrote: [\[CITE\]](#) So Zbot and Ngrbot are somehow both contained within a 6kb file? Sure, it could download them, but it wouldn't be detected as ngrbot for that, it would be detected as a downloader. Because it downloads.

So I c/p'd from zbot and ngrbot and somehow used that code in the ASM bins? Are you retarded?

Again i'm really sorry.

about this.

i would have closed the thread but i'm not uber or leet so i cannot close it .

I posted this thread cause i was suspicious cause i'm zero to none knowledgeable in this field. So i was skeptical why this it have that kind of detections.

BV1 already explained thou. So i'm ok with it ;)