

Forum:[Hack Forums](#)

Thread: [Malware Circulating on Facebook](#)

Silicon - February 7, 2014, 6:10 pm

Hey folks,

it has came to my attention that a new 'strain' of malware is going around on facebook. You'll be sent a .rar file (named as a JPEG or something like DCIM_123456.jpg.rar), inside which has a .jar file which drops an EXE from someone's dropbox (Which has since been deactivated) into C:\temp and executes it. There's some info on SomethingAwful [here](#) about it and I've tried to do my own analysis, be it limited.

The dropped executable seems to be heavily scrambled and I've not yet ascertained what it does. I've looked at it in Dependency Walker - not much shows up there. I had a look at it in PeID and here's what I've gathered. Dropped program was compiled on the 5th of February

In the strings table, it has 'mscoree' leading me to believe it's a .NET executable packed with a native crypter

Seems to do something to explorer.exe, but I can't quite work out what yet

Avast! keeps popping up warnings for me now coming from explorer.exe since my computer illiterate mother downloaded and ran the virus on my laptop. If anyone else wants to do some analysis I can give you the original .rar file and dropped .exe file, but if that's against the rules then I'll by all means not do that.

This seems to be FUD in everything including MBAM. Anyone else seen this?

Gustav - February 7, 2014, 6:16 pm

There are a lot of adware and malicious content around facebook ads. Be cautious of what you download at all times.

Jagster™ - February 7, 2014, 11:46 pm

This is not surprising, I read somewhere that the SEA (Syrian Electronic Army) was posting videos of beheadings and such which would redirect users to a site that used a working SJDB to drop executables on people.

Silicon - February 8, 2014, 4:36 am

I've done a little bit more digging, and it seems to be a background LiteCoin miner. It's trying to auto update itself periodically but Avast is blocking it - what concerns me is how it's still doing it now I seem to have got rid of it. MBAM give nothing and neither does Avast. Not sure what to do at this point.

Jagster™ - February 8, 2014, 8:26 am

Head over to the MRT section and they will remove it for you. It is most likely FUD therefore the AV's/scanners are not picking it up. They are only blocking the 'updater' because that is trying to execute a remote download, install.