

Forum:[Hack Forums](#)

Thread: [Might have my Pendrive infected with virus](#)

Narvikz - June 3, 2014, 7:36 am

This never happened to me but I don't get what's actually happening here.

[img]http://s28.postimg.org/3y3tf7w6l/image.png[/img]

All the hidden files were made system files. This is my android SD card content.

Pastebin of the script it is running:

<http://pastebin.com/aWCyczkp>

Aura - June 3, 2014, 7:40 am

This is the content of an SD card ?

Trying to access Pastebin to see the script right now.

Narvikz - June 3, 2014, 7:44 am

(Jun 3, 2014 07:40 AM)Aur? Wrote: [\[CITE\]](#) This is the content of an SD card ?

Trying to access Pastebin to see the script right now.

Yea, this is odd and started happening today afternoon (which means now). I accessed it fine at the morning.

Aura - June 3, 2014, 7:46 am

(Jun 3, 2014 07:44 AM)ThatGuyPT Wrote: [\[CITE\]](#) Yea, this is odd and started happening today afternoon (which means now). I accessed it fine at the morning.

Looks like a crypted VBscript.

Like the function name is crypted and so is the methods and variables.

If you run Windows XP, Windows Vista or Windows 7, I would definitively get both your SD card and your system checked by the MRT.

Narvikz - June 3, 2014, 7:48 am

(Jun 3, 2014 07:46 AM)Aur? Wrote: [\[CITE\]](#) Looks like a crypted VBscript.

Like the function name is crypted and so is the methods and variables.

If you run Windows XP, Windows Vista or Windows 7, I would definitively get both your SD card and your system checked by the MRT.

I delete the shortcuts and they are recreated, I think it's this school computer. And I have accessed HF on it. It probably has a rootkit since it's hidden from everywhere (task manager, msconfig and such)

DpzFAsq4UEK8 - June 3, 2014, 7:50 am

First of all, do not open any of those shortcuts.

This VBS script is malicious. Here's it deobfuscated: <http://pastebin.com/F4T4NKmm>

Looks like it is a very simple RAT which allows executing commands and downloading other crap.

Your computer has been most likely infected with a worm that has USB spreading feature. Have you got a Skype or Jabber where I can contact you?