

---

Subject: vbrkmtzd.exe?

Posted by [z310](#) on Thu, 27 Jan 2005 02:31:40 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

This is new to me, and Google showed no results.

If anybody want's it I zipped it, and will send it via AIM.

---

---

Subject: vbrkmtzd.exe?

Posted by [Majiin Vegeta](#) on Thu, 27 Jan 2005 02:41:50 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

mostlikly a botnet

check your firewall for outgoing connections and block it

had something similar

also check mscongif(in run > msconfig > startup)

find that .exe name and uncheck it from starting up

and find it and delete it

---

---

Subject: vbrkmtzd.exe?

Posted by [z310](#) on Thu, 27 Jan 2005 02:43:27 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Erm, alright... would explain why the connection has been so laggy. Thnx, Ill also delete the .zip file.

---

---

Subject: vbrkmtzd.exe?

Posted by [Majiin Vegeta](#) on Thu, 27 Jan 2005 02:48:15 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

search around for other unknown startup files.. these things recreate the .exe under another random filename they can be real bastards to get rid of

update virus scanners et.c and scan really good now

---

---

Subject: vbrkmtzd.exe?

Posted by [z310](#) on Thu, 27 Jan 2005 02:59:15 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Thnx man

I quarintined it, should be no problems O\_o

<3 Security Task Manager

---

---

Subject: vbrkmtdz.exe?

Posted by [IRON FART](#) on Thu, 27 Jan 2005 03:36:18 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Delete it, then if it reappears after a few seconds it may be a legit file (restored by Windows File Protection - WFP).

The odd filename makes me think that it could be spyware/adware.

---

---

Subject: vbrkmtdz.exe?

Posted by [genetix](#) on Thu, 27 Jan 2005 04:41:59 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

make sure and disable the windows file restore function before you delete it. Then if it isn't a system tool it doesn't have a chance of coming back. Keep a zip copy just incase.

I would also recomend searching that .exe name on syntemantec(I know its spelt wrong)

---

---

Subject: vbrkmtdz.exe?

Posted by [IRON FART](#) on Thu, 27 Jan 2005 05:43:28 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Symantec

<http://www.symantec.com>

---

---

Subject: vbrkmtdz.exe?

Posted by [exnyte](#) on Thu, 27 Jan 2005 06:58:05 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

IRON-FARTDelete it, then if it reappears after a few seconds it may be a legit file (restored by Windows File Protection - WFP).

The odd filename makes me think that it could be spyware/adware.

If it reappears after killing the task doesn't make it a legit file. There may be other processes running that will replace the process if it finds it's not running. Best to just search for any and all

---

unknown files running and kill/delete them. If it was something you needed, you can always get it back.

---

---

Subject: vbrkmtdz.exe?

Posted by [Xtrm2Matt](#) on Thu, 27 Jan 2005 07:49:40 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

By the size of it, it looks like a mIRC-Based botnet script. It's most likely using the WinRAR .EXE thingy for that kind of size.

Most botnets using C++ are 250kb and under. (Do not argue with me)

---

---

Subject: vbrkmtdz.exe?

Posted by [Opalkilla](#) on Thu, 27 Jan 2005 21:54:40 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

If you have Norton Antivirus, use the "Submit to Symantec" feature to prevent further infections of other users.

---

---

Subject: vbrkmtdz.exe?

Posted by [Beanyhead](#) on Thu, 27 Jan 2005 21:59:06 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

If it was a legit windows file google would return some results

---

---

Subject: vbrkmtdz.exe?

Posted by [z310](#) on Thu, 27 Jan 2005 23:27:23 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Im going to restore my sys later today, incase of anything I missed

Thnx guys, that was alot of help.

---