

## Re: Win2k machine hacked with Serv-U FTP etc

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-05/msg00112.html>

---

- *From:* "JM" <[jm@xxxxxxxx](mailto:jm@xxxxxxxx)>
  - *Date:* Mon, 29 May 2006 15:39:58 GMT
- 

more info:

Evidently, he made a newbie decision: he told me he "might have" clicked on the app shortcut on the desktop, because he remembers a bunch of icons appearing on the desktop for a few seconds and then disappearing.

Did he execute a destructive program?

wjm

"JM" <[jm@xxxxxxxx](mailto:jm@xxxxxxxx)> wrote in message  
[news:kuEeg.33351\\$YI5.19631@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:kuEeg.33351$YI5.19631@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

My father's Win2k machine has been hacked. Saturday he called me in a panic, and when I got to his house I could see why. There were windows opened all over his desktop (I will upload screenshots to my web server if it will help), a command window starting the Serv-U FTP service and

checking

ipconfig settings, a web browser opened to his router with a service

started

on port 333, a shortcut to an app, and the 2000 services and computer mngment window.

I'm not familiar enough with 2000 to know how to investigate exactly what happened. What I'm more interested in is where to go from here. My gut tells me to immediately backup all his important files, reformat,

reinstall,

Re: Win2k machine hacked with Serv-U FTP etc

and set him up with improved security measures. I also think a call to

his

cc companies are in order, as well as changing all passwords to all accounts, websites, etc.

What were the hacker's main purpose?

Please advise me in other ways. I'm not interested in finding fault with how he had things set up, other than to learn from his mistakes. While

he's

not a computer expert, he's not a newbie either.

thank you,

wjm