

Golon-A, administrator profile installed

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-09/2977.html>

From: Jojo (*Walkstwice_at_yahoo.com*)

Date: 09/21/03

Date: Sun, 21 Sep 2003 11:48:39 -0700

I recently got rid of (I hope) a new trojan, Golon-A (logon.exe). But I'm still having problems with z.exe, even though I've gotten rid of it (I hope). I'm missing half the driver files, dll, etc. I'm going to completely re-install very soon... No choice. But I've also had a lot of settings changed. And found a lot of evidence of remote use of my machine.

I spent the night at my girlfriend's on Wednesday, came home after work on Thursday & found that my browser had been used to surf with. History was full of some nasty sites under the Wednesday heading. I'd deleted everything else before I left, so that was the only day in history.

There was a new entry in the windows/profiles folder: administrator/Vorlagen. I don't know how long this has been going on, my system (Windows 98 2nd edition) has been running VERY poorly for quite a while. I'd run a lot of utilities to clean my system, which would help for awhile, then bam, it'd start all over. The only way I could surf, was with java & activeX disabled (they're enabled now & I don't like it!). I wouldn't have investigated file by file if Zone Alarm hadn't asked permission for logon.exe to act as a server... That was just last week.

What brings me here, is that when I go to windows update, even with X & java enabled, I get a message saying I have X disabled, and that I don't have administrator access rights to update!! I got the same thing last week, before I found z.exe. It's gone now, but the settings that Vorlagen entered are still in effect (he's from Germany, according to some logs I found).

How can I correct this?

Thanks for any help.