

Re: Is your system Hacked/Owned

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-12/1351.html>

From: MyndPhlyp (nobody@home.com)

Date: 12/13/02

From: "MyndPhlyp" <nobody@home.com>
Date: Fri, 13 Dec 2002 11:36:06 -0500

"ferrethater" <"ferrethaterinva;lid"@aol.com> wrote in message
news:3DF87761.E3B65199@aol.com...

- > *There are a number of ways to tell if your Windows system is hacked.*
- > *IF YOU'RE THE GENERAL AVERAGE INTERNET USER, NOT RUNNING ANY FTP, PROXY,*
- > *NNTP, SMTP SERVER AND USING ONE ISP AND A MODEM, HERE ARE A FEW TIPS.*

(Interpreted as meaning "if you are a neophyte – a real novice – you are most likely gullible and will believe anything.")

- >
- > *If you're on a Windows Platform, select Start, Settings, Control*
- > *Panel, Folder Options, View and make sure you select and have a*
- > *dot in the circle where it says Show Hidden Files and Folders.*

Absolutely a proven way to tell if your system is hacked. Uh, okay ... now that I can see those Hidden Files and Folders, what exactly am I to look for?

- >
- > *Select Start, Control Panel, Network, and if you see two*
- > *AOL adapters, two TCP/IP, two dial-up adapters, two Virtual Private*
- > *Network adapters your computer has what hackers install called a*
- > *Virtual Private Network, BEWARE!*

Sounds like what network administrators in general call a Virtual Private Network, too. But it doesn't mean the workstation has been hacked. VPN's have been around for quite some time.

- >
- > *If you find your system re-boots itself from time to time, this*
- > *is another sign that an Administrator (hacker) has to update your*
- > *hacked system.*

Ah yes ... everybody is aware of the stability and reliability of Windows. This is one operating system that NEVER crashes due to poor memory handling, poorly written installation scripts, less-than-desirable-quality shareware,

comp.security.firewalls: Re: Is your system Hacked/Owned

freeware, drivers and the like, disk drives full to the brim, flaws in the original and updated code, borderline hardware failures, etc., etc., etc. Windows never crashes unless a hacker updates the system? That's good to know. I guess I won't finish writing that letter to Bill Gate\$.

- >
- > *Select Start, type regedit, select Registry, Export Registry, and in*
- > *the box type say 3-12-02.txt and say ok. Then open this file with*
- > *a text editor or word doc and you might be shocked to find what*
- > *really is installed on your system. Check the bottom of this file,*
- > *have found the hackers love to install a bunch of their crap here.*

Hmm ... so, regardless of WHAT I find at the end of the Registry dump, it was placed there by a hacker. This gets better and better by the syllable.

- >
- > *What these hackers do is disable your anti-virus program using Trojan*
- > *Horses, which makes checking for viruses or trojans useless. If running*
- > *a software*
- > *firewall, the hackers install another version of what your running*
- > *and program it so you aren't able to see their activities.*

And just how do they go about disabling the antivirus software? These days, antivirus software has the ability to detect virus-like activity in even the newest viruses and Trojans. And hackers replaced my software firewall? Doesn't sound like much of a firewall if it let that activity through in the first place.

- >
- > *Once these factors take into play, the best bet to keep the hackers*
- > *out of your system is to perform the below.*
- >
- > *My suggestion would be to keep the hard drive (send to the FBI, minus*
- > *your*
- > *personal files) or make a copy of your entire hard drive. This way if*
- > *the hackers have destroyed*
- > *other Systems, Networks or Servers using your computer, at least you*
- > *have evidence if the*
- > *FBI ever come knock on your door. The Trackers would like a copy, but*
- > *that's*
- > *another story in itself.*

Out of both sides of the mouth at the same time – I am to keep the hard drive, but send it to the FBI minus my personal files. That is a trick even I cannot do unless I figure out how to conquer this space/time continuum thing. Has anybody really been able to figure out how to have the same matter exist in two places at the same time?

- >
- > *You want to format the hard drive, install from cd-rom only and*
- > *get yourself a free port scanner. Before you go online, port scan your*

comp.security.firewalls: Re: Is your system Hacked/Owned

- > *own computer to check for any open ports, Backdoors, Trojan Horses and*
- > *Viruses.*
- > *Dis-able any Windows services your not using including Windows*
- > *file and print sharing, install an anti-virus and firewall application.*
- > *This is just for starters. You also need to secure your browser and*
- > *email application.*

So, after installing a fresh copy of the OS on a newly formatted HD, I need to check for Trojans and viruses. Oh the pain ... make it stop ... the laughter is disturbing the neighbors. And I also have to install antivirus software and a firewall application ... the same stuff that got hacked a few paragraphs ago when they broke through my software firewall and disabled my antivirus software. I guess I can forget about any factory-supplied drivers that reside on floppy disk, too. But that's okay – since I can't get my network driver installed, I don't have to worry about open ports.

- >
- > *Your system can also be running a Proxy Server, NNTP Server, SMTP*
- > *Server,*
- > *Web Server, SQL Server a Virtual Private Network and more then likely*
- > *has*
- > *a "Root Kit(s)" installed. All these factors need to be taken into*
- > *consideration.*

Do tell. By all means, spell out in no uncertain terms the exact vulnerabilities. Don't gloss over any of the details, now. All these things are found on Win95/98/ME systems, right? ROFLMAO! It hurts so much. Make it stop, please.

Oh, that was good. I haven't had a laugh like that in quite some time. My ribs are so sore that I'll have to see about getting some meds.