Caught A Virus?

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

If you've let your guard down--or even if you haven't--it can be hard to tell if your PC is infected. Here's what to do if you suspect the worst.

Heard this one before? You must run antivirus software and keep it up to date or else your PC will get infected, you'll lose all your data, and you'll incur the wrath of every e-mail buddy you unknowingly infect because of your carelessness.

You know they're right. Yet for one reason or another, you're not running antivirus software, or you are but it's not up to date. Maybe you turned off your virus scanner because it conflicted with another program. Maybe you got tired of upgrading after you bought Norton Antivirus 2001, 2002, and 2003. Or maybe your annual subscription of virus definitions recently expired, and you've put off renewing.

It happens. It's nothing to be ashamed of. But chances are, either you're infected right now, as we speak, or you will be very soon.

For a few days in late January, the Netsky.p worm was infecting about 2,500 PCs a day. Meanwhile the MySQL bot infected approximately 100 systems a minute (albeit not necessarily desktop PCs). As David Perry, global director of education for security software provider Trend Micro, puts it, "an unprotected [Windows] computer will become owned by a bot within 14 minutes."

Today's viruses, worms, and so-called bots--which turn your PC into a zombie that does the hacker's bidding (such as mass-mailing spam)--aren't going to announce their presence. Real viruses aren't like the ones in Hollywood movies that melt down whole networks in seconds and destroy alien spacecraft. They operate in the background, quietly altering data, stealing private operations, or using your PC for their own illegal ends. This makes them hard to spot if you're not well protected.

Is Your PC "Owned?"

I should start by saying that not every system oddity is due to a virus, worm, or bot. Is your system slowing down? Is your hard drive filling up rapidly? Are programs crashing without warning? These symptoms are more likely caused by Windows, or badly written legitimate programs, rather than malware. After all, people who write malware want to hide their program's presence. People who write commercial software put icons all over your desktop. Who's going to work harder to go unnoticed?

Other indicators that may, in fact, indicate that there's nothing that you need to worry about, include:

* An automated e-mail telling you that you're sending out infected mail. E-mail viruses and worms typically come from faked addresses.
* A frantic note from a friend saying they've been infected, and therefore so have you. This is likely a hoax. It's especially suspicious if the note tells you the virus can't be detected but you can get rid of it by deleting one simple file. Don't be fooled--and don't delete that file.

I'm not saying that you should ignore such warnings. Copy the subject line or a snippet from the body of the e-mail and plug it into your favorite search engine to see if other people have received the same note. A security site may have already pegged it as a hoax.

Sniffing Out an Infection

There are signs that indicate that your PC is actually infected. A lot of network activity coming from your system (when you're not actually using Internet) can be a good indicator that something is amiss. A good software firewall, such as ZoneAlarm, will ask your permission before letting anything leave your PC, and will give you enough information to help you judge if the outgoing data is legitimate. By the way, the firewall that comes with Windows, even the improved version in XP Service Pack 2, lacks this capability.

To put a network status light in your system tray, follow these steps: In Windows XP, choose Start, Control Panel, Network Connections, right-click the network connection you want to monitor, choose Properties, check "Show icon in notification area when connected," and click OK.

If you're interested in being a PC detective, you can sniff around further for malware. By hitting Ctrl-Alt-Delete in Windows, you'll bring up the Task Manager, which will show you the various processes your system is running. Most, if not all, are legit, but if you see a file name that looks suspicious, type it into a search engine and find out what it is.

Want another place to look? In Windows XP, click Start, Run, type "services.msc" in the box, and press Enter. You'll see detailed descriptions of the services Windows is running. Something look weird? Check with your search engine.

Finally, you can do more detective work by selecting Start, Run, and typing "msconfig" in the box. With this tool you not only see the services running, but also the programs that your system is launching at startup. Again, check for anything weird.

If any of these tools won't run--or if your security software won't run--that in itself is a good sign your computer is infected. Some viruses intentionally disable such programs as a way to protect themselves.

What to Do Next

Once you're fairly sure your system is infected, don't panic. There are steps you can take to assess the damage, depending on your current level of protection.

* If you don't have any antivirus software on your system (shame on you), or if the software has stopped working, stay online and go for a free scan at one of several Web sites. There's McAfee FreeScan, Symantec Security Check, and Trend Micro's HouseCall. If one doesn't find anything, try two. In fact, running a free online virus scan is a good way to double-check the work of your own local antivirus program. When you're done, buy or download a real antivirus program.
* If you have antivirus software, but it isn't active, get offline, unplug wires-- whatever it takes to stop your computer from communicating via the Internet. Then, promptly perform a scan with the installed software.
* If nothing seems to be working, do more research on the Web. There are several online virus libraries where you can find out about known viruses. These sites often provide instructions for removing viruses--if manual removal is possible--or a free removal tool if it isn't. Check out GriSOFT's Virus Encyclopedia, Eset's Virus Descriptions, McAffee's Virus Glossary, Symantec's Virus Encyclopedia, or Trend Micro's Virus Encyclopedia.

A Microgram of Prevention

Assuming your system is now clean, you need to make sure it stays that way. Preventing a breach of your computer's security is far more effective than cleaning up the mess afterwards. Start with a good security program, such Trend Micro's PC-Cillin, which you can buy for $50.

Don't want to shell out any money? You can cobble together security through free downloads, such as AVG Anti-Virus Free Edition, ZoneAlarm (a personal firewall), and Ad-Aware SE (an antispyware tool).

Just make sure you keep all security software up to date. The bad guys constantly try out new ways to fool security programs. Any security tool without regular, easy (if not automatic) updates isn't worth your money or your time.

Speaking of updating, the same goes for Windows. Use Windows Update (it's right there on your Start Menu) to make sure you're getting all of the high priority updates. If you run Windows XP, make sure to get the Service Pack 2 update. To find out if you already have it, right-click My Computer, and select Properties. Under the General tab, under System, it should say "Service Pack 2."

Here are a few more pointers for a virus-free life:

* Be careful with e-mail. Set your e-mail software security settings to high. Don't open messages with generic-sounding subjects that don't apply specifically to you from people you don't know. Don't open an attachment unless you're expecting it.
* If you have broadband Internet access, such as DSL or cable, get a router, even if you only have one PC. A router adds an extra layer of protection because your PC is not connecting directly with the Internet.
* Check your Internet ports. These doorways between your computer and the Internet can be open, in which case your PC is very vulnerable; closed, but still somewhat vulnerable; or stealthed (or hidden), which is safest. Visit Gibson Research's Web site and run the free ShieldsUP test to see your ports' status. If some ports show up as closed--or worse yet, open--check your router's documentation to find out how to hide them.