

Re: Reporting Hackers

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-03/1972.html

From: Shenan Stanley (*newshelper_at_gmail.com*)

Date: 03/25/05

Date: Thu, 24 Mar 2005 23:53:11 -0600

drive55 wrote:

> *WinXPHome/SP2 (NIS/NAV 2004) – A few days ago, in a span of a little
> over forty–eight hours, there were seventeen attempts to place a
> Trojan Horse on my computer. The attacks all came from the same IP
> address (Charter Communications, St. Louis area). Since Charter is my
> ISP, they will investigate possible abuse from a customer in the same
> system. I filled out two abuse report forms with the relevant
> information – log excerpts, etc. Today I received an e–mail from
> Charter stating that my computer may be infected with a virus and
> that service may be suspended if the situation persists. Their
> recommendation is to apply their 3 Steps to Internet Security (which
> I already do) and to download their High–Speed Security Suite (which
> I'm not going to do). I'm contacting my ISP in the morning; but in
> the meantime, has anyone had a similar experience ? I think the whole
> episode is ridiculous, especially since I have automatic updates and
> run LiveUpdate Express and a virus scan daily. Also, can an ISP even
> determine if my computer's infected or is this a result of my
> reporting an obvious abuse ? Sorry for the long post.*

Just because you have patched and keep your antivirus up to date does not mean you are safe.

What ports are opened in your NIS configuration?

Have you now, since Charter gave you the warning, done a full virus/trojan scan with an application (AV) other than the one you had installed? (Some online free ones are available – see tip 9.)

What about Spyware – what applications do you use to not only scan for, but immunize against spyware/adware? (Many free ones are available, see tip 10.)

Have you patched the programs OTHER than Windows XP/Norton using their manufacturer web support pages? What about hardware drivers? (See tip 8 for advice on this.)

Do you keep regular backups so that you can restore your system in case of catastrophic failure – no matter the cause? (See tip 6 for information on system restore as well as Windows Backup.)

Have you gone through your Control Panel --> Add/Remove Programs list to uninstall any unknown/unused applications? (See tip 7 for help doing just

that.)

Have you checked your startup items using msconfig or msinfo32 for unneeded/unknown startup items and remedied them? (See tip 13 for help on identifying the good vs. bad startups.)

Is your computer protected with decent passwords? (See tip 4 for information on good password basics..)

Microsoft has these suggestions for Protecting your computer from the various "bad things" that could happen to you/it:

Protect your PC

<http://www.microsoft.com/security/protect/>

Although those tips are fantastic, there are many things you should know above and beyond what is there as well as other methods and applications you can use to protect yourself. Below I have detailed out many steps that can not only help you cleanup a problem PC but keep it clean and secure as well as running at its top performance mark.

I know this list can seem intimidating – it is quite long and a lot to take in for a novice – but I assure you that one trip through this list and you will understand your computer and the options available to you for protecting your data much better and that the next time you review these steps, the time it takes will be greatly reduced.

Let's take the cleanup of your computer step-by-step. Yes, it will take up some of your time – but consider what you use your computer for and how much you would dislike it if all of your stuff on your computer went away because you did not "feel like" performing some simple maintenance tasks – think of it like changing the oil in your car, changing the air filter on your home A/C unit, paying your bills on time, etc.

Let's go through some maintenance first that should only have to be done once (mostly):

Tip (1):

Locate all of the software (the installation media – CDs, etc) that you have installed on your computer. Collect these CDs into a single pile and locate the original installation media (CDs, disks) in a central and safe place along with their CD keys and such. Make backups of these installation media sets using your favorite copying method (CD Burner and application, Disk copier, etc.) You'll be glad to know that if you have a CD burner, you may be able to use a free application to make a duplicate copy of your CDs. One such application is ISORecorder:

ISORecorder home page (with general instructions on use):

<http://isorecorder.alexfeinman.com/isorecorder.htm>

Pre-SP2 version:

<http://isorecorder.alexfeinman.com/IsoRecorder/download.asp>

Post-SP2 beta version:

<http://isorecorder.alexfeinman.com/download/ISORecorderV2B2.zip>

More full function applications (free) for CD/DVD burning would be:

DeepBurner Free

<http://www.deepburner.com/>

CDBurnerXP Pro

<http://www.cdburnerxp.se/>

Another Option would be to search the web with Pricewatch.com or Dealsites.net and find deals on Nero and/or Roxio.

Tip (2):

Empty your Internet Explorer Temporary Internet Files and make sure the maximum size for this is small enough not to cause trouble in the future.

Empty your Temporary Internet Files and shrink the size it stores to a size between 128MB and 512MB..

- Open ONE copy of Internet Explorer.
- Select TOOLS -> Internet Options.
- Under the General tab in the "Temporary Internet Files" section, do the following:
 - Click on "Delete Cookies" (click OK)
 - Click on "Settings" and change the "Amount of disk space to use:" to something between 128MB and 512MB. (Betting it is MUCH larger right now.)
 - Click OK.
 - Click on "Delete Files" and select to "Delete all offline contents" (the checkbox) and click OK. (If you had a LOT, this could take 2-10 minutes or more.)
- Once it is done, click OK, close Internet Explorer, re-open Internet Explorer.

Tip (3):

If things are running a bit slow or you have an older system (1.5GHz or less and 256MB RAM or less) then you may want to look into tweaking the performance a bit by turning off some of the memory using Windows XP "prettifications". The fastest method is:

Control Panel --> System --> Advanced tab --> Performance section, Settings button. Then choose "adjust for best performance" and you now have a Windows 2000/98 look which turned off many of the annoying "prettifications" in one swift action. You can play with the last three checkboxes to get more of an XP look without many of the other annoyances. You could also grab and install/mess with one (or more) of the Microsoft Powertoys - TweakUI in particular:

<http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.msp>

Tip (4):

Understanding what a good password might be is vital to your personal and system security. You may not need to password your home computer, as you may have it in a locked area (your home) where no one else has access to it. Remember, however, that locked area is unlocked when you access the Internet unless you are taking proper precautions. Also, you aren't always "in that locked area" when using your computer online – meaning you likely have usernames and passwords associated with web sites and the likes that you would prefer other people do not discover/use. This is why you should understand and utilize good passwords.

Good passwords are those that meet these general rules (mileage may vary):

Passwords should contain at least six characters, and the character string should contain at least three of these four character types:

- uppercase letters
- lowercase letters
- numerals
- nonalphanumeric characters (e.g., *, %, &, !)

Passwords should not contain your name/logon name. Passwords should be unique to you and easy to remember. One method many people are using today is to make up a phrase that describes a point in their life and then turning that phrase into their password by using only certain letters out of each word in that phrase. It's much better than using your birthday month/year or your anniversary in a pure sense. For example, let's say my phrase is:

"Moved to new home in 2004"

I could come up with this password from that:

"Mv2n3whmN04"

The password tip is in the "one time" section, but I highly recommend you periodically change your passwords. The suggested time varies, but I will throw out a "once in every 3 to 6 months for every account you have."

Tip (5):

This tip is also "questionable" in the "one time" section. However, if properly setup, this one can be pretty well ignored for most people after the initial "fiddle-with" time.

Why you should use a computer firewall..

<http://www.microsoft.com/athome/security/viruses/fwbenefits.mspx>

You should, in some way, use a firewall. Hardware (like a nice Cable Modem/DSL router) or software is up to you. Many use both of these. The simplest one to use is the hardware one, as most people don't do anything they need to configure their NAT device for and those who do certainly will not mind fiddling with the equipment to

make things work for them. Next in the line of "simplicity" would have to be the built-in Windows Firewall of Windows XP. In SP2 it is turned on by default. It is not difficult to turn on in any case, however:

Enable/Disable the Internet Connection Firewall (Pre-SP2):

<http://support.microsoft.com/kb/283673>

More information on the Internet Connection Firewall (Pre-SP2):

<http://support.microsoft.com/kb/320855>

Post-SP2 Windows Firewall Information/guidance:

<http://snipurl.com/atal>

The trouble with the Windows Firewall is that it only keeps things out. Truthfully, for most people who maintain their system in other ways, this is MORE than sufficient. However, you may feel otherwise. If you want to know when one of your applications is trying to obtain access to the outside world so you can stop it, then you will have to install a third-party application and configure/maintain it. I have compiled a list with links of some of the better known/free firewalls you can choose from:

ZoneAlarm (Free and up)

<http://snipurl.com/6ohg>

Kerio Personal Firewall (KPF) (Free and up)

http://www.kerio.com/kpf_download.html

Outpost Firewall from Agnitum (Free and up)

<http://www.agnitum.com/download/>

Sygate Personal Firewall (Free and up)

http://smb.sygate.com/buy/download_buy.htm

Symantec's Norton Personal Firewall (~\$25 and up)

<http://www.symantec.com/sabu/nis/npf/>

BlackICE PC Protection (\$39.95 and up)

<http://blackice.iss.net/>

Perhaps you can find the right firewall for your situation in that list and set it up/configure it. Every firewall MAY require some maintenance. Essentially checking for patches or upgrades (this goes for hardware and software solutions) is the extent of this maintenance – but you may also have to configure your firewall to allow some traffic depending on your needs. Also, don't stack these things. Running more than one firewall will not make you safer – it would likely (in fact) negate some protection you gleaned from one or the other firewalls you run.

Now that you have some of the more basic (one-time) things down.. Let's go through some of the steps you should take periodically to maintain a healthy and stable windows computer. If you have not done some of these things in the past, they may seem tedious at first – however, they will become routine and some can even be automatically scheduled.

Tip (6):

The system restore feature is a new one – first appearing in Windows ME and then sticking around for Windows XP. It is a VERY useful feature – if you keep it maintained and use it to your advantage. However, remember that the system restore pretty much tells you in the name what it protects – "system" files. Your documents, your pictures, your stuff is NOT system files – so you should also look into some backup solution.

I'll mainly work around Windows XP, as that is what the bulk of this document is about. I will, however, point out a single place for you poor souls still stuck in Windows ME where you can get information on maintaining your system right now:

Windows ME Computer Health:

<http://www.microsoft.com/windowsME/using/computerhealth/articles/>

Pay close attention to the sections:

(in order)

- Clean up your hard disk
- Check for errors by running ScanDisk
- Defragment your hard disk
- Roll back the clock with System Restore

Now back to the point at hand – maintaining your system restore in Windows XP SHOULD be automatic – but I have seen the automatic go wrong too many times not to suggest the following.. Whenever you think about it (after doing a once-over on your machine once a month or so would be optimal) – clear out your System Restore and create a manual restoration point. Why? Too many times have I seen the system restore files go corrupt or get a virus in them, meaning you could not or did not want to restore from them. By clearing it out periodically you help prevent any corruption from happening and you make sure you have at least one good "snapshot".

(This, of course, will erase any previous restore point you have.)

– Turn off System Restore.

<http://support.microsoft.com/kb/310405>

– Reboot.

– Turn on System Restore.

<http://support.microsoft.com/kb/310405>

– Make a Manual Restoration Point.

<http://snipurl.com/68nx>

That covers your system files, but doesn't do anything for the files that you are REALLY worried about – yours! For that you need to look into backups. You can either manually copy your important files, folders, documents, spreadsheets, emails, contacts, pictures, drawings and so on to an external location (CD/DV – any disk of some sort, etc) or you can use the backup tool that comes with Windows XP:

How To Use Backup to Back Up Files and Folders on Your Computer
<http://support.microsoft.com/kb/308422>

Yes – you still need some sort of external media to store the results on, but you could schedule the backup to occur when you are not around, then burn the resultant data onto CD or DVD or something when you are (while you do other things!)

Tip (7):

You should sometimes look through the list of applications that are installed on your computer. The list MIGHT surprise you. There are more than likely things in there you KNOW you never use – so why have them there? There may even be things you KNOW you did not install and certainly do not use (maybe don't WANT to use.)

This web site should help you get started at looking through this list:

How to Uninstall Programs
<http://snipurl.com/8v6b>

A word of warning – Do NOT uninstall anything you think you MIGHT need in the future unless you have completed Tip (1) and have the installation media and proper keys for use backed up somewhere safe!

Tip (8):

Patches and Updates!

This one cannot be stressed enough. It is SO simple, yet so neglected by many people. It is especially simple for the critical Windows patches! Microsoft put in an AUTOMATED feature for you to utilize so that you do NOT have to worry yourself about the patching of the Operating System:

How to configure and use Automatic Updates in Windows XP
<http://support.microsoft.com/kb/306525>

However, not everyone wants to be a slave to "automation", and that is fine – as long as you are willing to do things manually. Admittedly, I prefer this method on some of my more critical systems.

Windows Update
<http://windowsupdate.microsoft.com/>

Go there and scan your machine for updates. Always get the critical ones as you see them. Write down the KB##### or Q##### you see when

selecting the updates and if you have trouble over the next few days, go into your control panel (Add/Remove Programs), match up the latest numbers you downloaded recently (since you started noticing an issue) and uninstall them. If there was more than one (usually is), uninstall them one by one – with a few hours of use in between, to see if the problem returns. Yes – the process is not perfect (updating) and can cause trouble like I mentioned – but as you can see, the solution isn't that bad – and is MUCH better than the alternatives.

Windows is not the only product you likely have on your PC. The manufacturers of the other products usually have updates as well. New versions of almost everything come out all the time – some are free, some are pay – some you can only download if you are registered – but it is best to check. Just go to their web pages and look under their support and download sections. For example, for Microsoft Office update, you should visit:

Microsoft Office Updates
<http://office.microsoft.com/>
(and select "downloads")

You also have hardware on your machine that requires drivers to interface with the operating system. You have a video card that allows you to see on your screen, a sound card that allows you to hear your PC's sound output and so on. Visit those manufacturer web sites for the latest downloadable drivers for your hardware/operating system. Always (IMO) get the manufacturers' hardware driver over any Microsoft offers. On the Windows Update site I mentioned earlier, I suggest NOT getting their hardware drivers – no matter how tempting. First – how do you know what hardware you have in your computer? Invoice or if it is up and working now – take inventory:

Belarc Advisor
http://belarc.com/free_download.html

EVEREST Home Edition
<http://www.lavalys.com/products/download.php?pid=1&lang=en>

Once you know what you have, what next? Go get the latest driver for your hardware/OS from the manufacturer's web page. For example, let's say you have an NVidia chipset video card or ATI video card, perhaps a Creative Labs sound card or C-Media chipset sound card...

NVidia Video Card Drivers
<http://www.nvidia.com/content/drivers/drivers.asp>

ATI Video Card Drivers
<http://www.atitech.com/support/driver.html>

Creative Labs Sound Device
<http://us.creative.com/support/downloads/>

C–Media Sound Device

http://www.cmedia.com.tw/e_download_01.htm

Then install these drivers. Updated drivers are usually more stable and may provide extra benefits/features that you really wished you had before.

As for Service Pack 2 (SP2) for Windows XP, Microsoft has made this particular patch available in a number of ways. First, there is the Windows Update web page above. Then there is a direct download site and finally, you can order the FREE CD from Microsoft.

Direct Download of Service Pack 2 (SP2) for Windows XP

<http://snipurl.com/8bqy>

Order the Free Windows XP SP2 CD

<http://snipurl.com/8umo>

Tip (9):

What about the dreaded word in the computer world, VIRUS?

Well, there are many products to choose from that will help you prevent infections from these horrid little applications. Many are FREE to the home user. Which one you choose is a matter of taste, really. I wouldn't list one here I had not personally used – and they all work. Many people have emotional attachments or performance issues with one or another AntiVirus software. Try some out, read reviews and decide for yourself which you like more:

avast! (Free and up)

<http://www.avast.com/>

AVG Anti–Virus System (Free and up)

<http://www.grisoft.com/>

AntiVir (Free and up)

<http://www.free-av.com/>

RAV AntiVirus Online Virus Scan (Free!)

<http://www.ravantivirus.com/scan/>

Symantec (Norton) AntiVirus (~\$11 and up)

http://www.symantec.com/nav/nav_9xnt/

Kaspersky Anti–Virus (~\$49.95 and up)

<http://www.kaspersky.com/products.html>

Panda Antivirus Titanium (~\$39.95 and up)

<http://www.pandasoftware.com/>

(Free Online Scanner: <http://www.pandasoftware.com/activescan/>)

McAfee VirusScan (~\$11 and up)

<http://www.mcafee.com/>

Trend Micro (~\$49.95 and up)

<http://www.trendmicro.com/en/home/us/personal.htm>

(Free Online Scanner:

http://housecall.trendmicro.com/housecall/start_corp.asp)

Untested (by me):

eTrust EZ Antivirus (\$29.95 and up)

<https://www2.my-etrust.com/commerce/buy.it.cfm>

Most of them have automatic update capabilities. You will have to look into the features of the one you choose. Whatever one you finally settle with – be SURE to keep it updated (I recommend at least daily) and perform a full scan periodically (yes, it protects you actively, but a full scan once a month at 4AM probably won't bother you.)

Tip (10):

The most rampant infestation at the current time concerns SPYWARE/ADWARE.

I hate this stuff. It has no purpose. I have seen people try to justify it over and over – it's worthless. It slows down your PC, it can send your private information to people you'll never meet and did I mention, it's worthless. You need to eliminate it from your machine.

If you use P2P software, this COULD make that stop working. Find some decent software to do the same thing – what you are currently using is crap.

Anyway – there is no one software that cleans and immunizes you against everything. Antivirus software – you only needed one. Firewall, you only needed one. AntiSpyware – you may need several. I have a list and I recommend you use at least the first 5. I know that sounds like a lot, and you may be saying "But you said earlier that I should clean my system, now you are telling me to install more software – 5 pieces in fact!" Okay, I get your point, but please consider that this stuff has prevented the install of the latest service pack for some people, it has the potential to slow and crater your PC, it can send your private information around the world to people you do not know – it is all around BAD.

First – make sure you have NOT installed "Rogue AntiSpyware". There are people out there who created AntiSpyware products that actually install spyware of their own! You need to avoid these:

Rogue/Suspect Anti-Spyware Products & Web Sites

http://www.spywarewarrior.com/rogue_anti-spyware.htm

Also, you can always visit this site..

<http://mvps.org/winhelp2002/unwanted.htm>

For more updated information.

Then, my suggestion again is that you at least install the first five of these: (Install, Run, Update, Scan with..)

Lavasoft AdAware (Free and up)

<http://www.lavasoft.de/support/download/>

(How-to: <http://snipurl.com/atdn>)

Spybot Search and Destroy (Free!)

<http://www.safer-networking.net/en/download/index.html>

(How-to: <http://snipurl.com/atdk>)

Bazooka Adware and Spyware Scanner (Free!)

<http://www.kephyr.com/spywarescanner/>

(How-to: <http://snipurl.com/ate3>)

SpywareBlaster (Free!)

<http://www.javacoolsoftware.com/sbdownload.html>

(How-to: <http://snipurl.com/ate6>)

IE-SPYAD (Free!)

<https://netfiles.uiuc.edu/ehowes/www/resource.htm>

(How-to: <http://snipurl.com/ate7>)

CWShredder (Free!)

http://www.softbasket.com/download/s_8114.shtml

Hijack This! (Free)

<http://mjc1.com/mirror/hjt/>

(Tutorial: <http://hjt.wizardsofwebsites.com/>)

ToolbarCop (Free!)

<http://windowsxp.mvps.org/toolbarcop.htm>

Browser Security Tests

<http://www.jasons-toolbox.com/BrowserSecurity/>

Popup Tester

<http://www.popupstest.com/>

The Cleaner (49.95 and up)

<http://www.moosoft.com/>

If used properly, you should have a malware free system now. The last two of the first five I suggest you install are immunization applications. None of these programs (in these editions) run in the background unless you TELL them to. The space they take up and how easy they are to use greatly makes up for any inconvenience you may be feeling.

Unfortunately, although that will lessen your popups on the Internet/while you are online, it won't eliminate them. I have looked at a lot of options, seen a lot of them used in production with people who seem to attract popups

like a plague, and I only have a few other suggestions that should help.

This

one ends up serving double duty (search engine and popup stopper in one):

The Google Toolbar (Free!)

<http://toolbar.google.com/>

Yeah – it adds a bar to your Internet Explorer – but it's a useful one. You can search from there anytime with one of the best search engines on the planet (IMO.) And the fact it stops most popups – wow – BONUS! If you don't like that suggestion, then I am just going to say you go to www.google.com and search for other options.

Please notice that Windows XP SP2 does help stop popups as well.

Another option is to use an alternative Web browser. I suggest "Mozilla Firefox", as it has some great features and is very easy to use:

Mozilla Firefox

<http://www.mozilla.org/products/firefox/>

One more suggestion is to disable your Windows Messenger service. This service is not used frequently (if at all) by the normal home user and in cooperation with a good firewall, is generally unnecessary. Microsoft has instructions on how to do this for Windows XP here:

<http://www.microsoft.com/windowsxp/pro/using/howto/communicate/stopspam.asp>

So your machine is pretty clean and up to date now. If you use the sections above as a guide, it should stay that way as well! There are still a few more

little things you can do to keep your machine running in top shape.

Tip (11):

You should periodically check your hard drive(s) for errors and defragment them. Only defragment after you have cleaned up your machine of outside parasites and never defragment as a solution to a quirkiness in your system. It may help speed up your system, but it should be clean before you do this.

How to use Disk Cleanup

<http://support.microsoft.com/?kbid=310312>

How to scan your disks for errors

<http://support.microsoft.com/?kbid=315265>

How to Defragment your hard drives

<http://support.microsoft.com/?kbid=314848>

I would personally perform the above steps at least once every three months. For most people this should be sufficient, but if the difference you notice

afterwards is greater than you think it should be, lessen the time in between its schedule.. If the difference you notice is negligible, you can increase the time.

Tip (12):

SPAM! JUNK MAIL!

This one can get annoying, just like the rest. You get 50 emails in one sitting and 2 of them you wanted. NICE! (Not.) What can you do? Well, although there are services out there to help you, some email servers/services that actually do lower your spam with features built into their servers – I still like the methods that let you be the end–decision maker on what is spam and what is not. I have two products to suggest to you, look at them and see if either of them suite your needs. Again, if they don't, Google is free and available for your perusal.

SpamBayes (Free!)

<http://spambayes.sourceforge.net/>

Spamihilator (Free!)

<http://www.spamihilator.com/>

As I said, those are not your only options, but are reliable ones I have seen function for hundreds+ people.

Tip (13):

ADVANCED TIP! Only do this once you are comfortable under the hood of your computer!

There are lots of services on your PC that are probably turned on by default you don't use. Why have them on? Check out these web pages to see what all of the services you might find on your computer are and set them according to

your personal needs. Be CAREFUL what you set to manual, and take heed and write down as you change things! Also, don't expect a large performance increase or anything – especially on today's 2+ GHz machines, however – I look

at each service you set to manual as one less service you have to worry about

someone exploiting. A year ago, I would have thought the Windows Messenger service to be pretty safe, now I recommend (with addition of a firewall) that most home users disable it! Yeah – this is another one you have to work for, but your computer may speed up and/or be more secure because you took the time. And if you document what you do as you do it, next time, it goes MUCH faster! (or if you have to go back and re–enable things..)

Task List Programs

http://www.answerthatwork.com/Tasklist_pages/tasklist.htm

Black Viper's Service List and Opinions (XP)

<http://www.blackviper.com/WinXP/servicecfg.htm>

Processes in Windows NT/2000/XP

<http://www.reger24.de/prozesse/>

There are also applications that AREN'T services that startup when you start up the computer/logon. One of the better description on how to handle these I have found here:

Startups

http://www.pacs-portal.co.uk/startup_content.php

If you follow the advice laid out above (and do some of your own research as well, so you understand what you are doing) – your computer will stay fairly stable and secure and you will have a more trouble-free system.

--

<- Shenan ->

--

The information is provided "as is", it is suggested you research for yourself before you take any advice - you are the one ultimately responsible for your actions/problems/solutions. Know what you are getting into before you jump in with both feet.