



CODING HORROR

programming and human factors
by Jeff Atwood

Jun 15, 2007

How to Clean Up a Windows Spyware Infestation

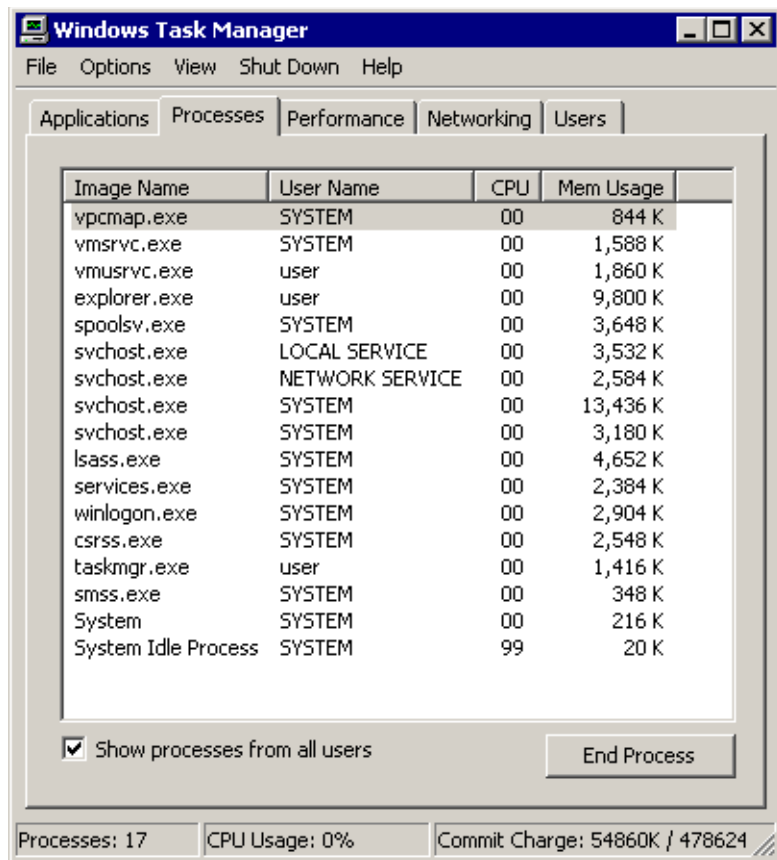
I recently upgraded my [dedicated racing simulation PC](#), so I was forced to re-install Windows XP SP2, along with all the games. As I was downloading the no-cd patches for the [various racing sims](#) I own, I was suddenly and inexplicably deluged with popups, icons, and unwanted software installations. I got that sinking feeling: I had become the unfortunate victim of a **spyware infestation**.

Of course, this is *completely my own fault* for browsing the web using the 2004-era web browser included with a default install of Windows XP Service Pack 2. If I was thinking rationally, I would have downloaded [Firefox](#) first, or at least connected to Windows Update to get the latest patches, *before* venturing on to the open internet. But I figured I'd save myself that work, and just pop into a few specific web sites for a few quick downloads. Couldn't hurt, right? Let my mistake be a lesson to everyone reading this: **never browse the web without the very latest version of your preferred web browser**. Intentionally choosing to browse the web with a three year old browser, as I did, is an incredibly dangerous thing to do.

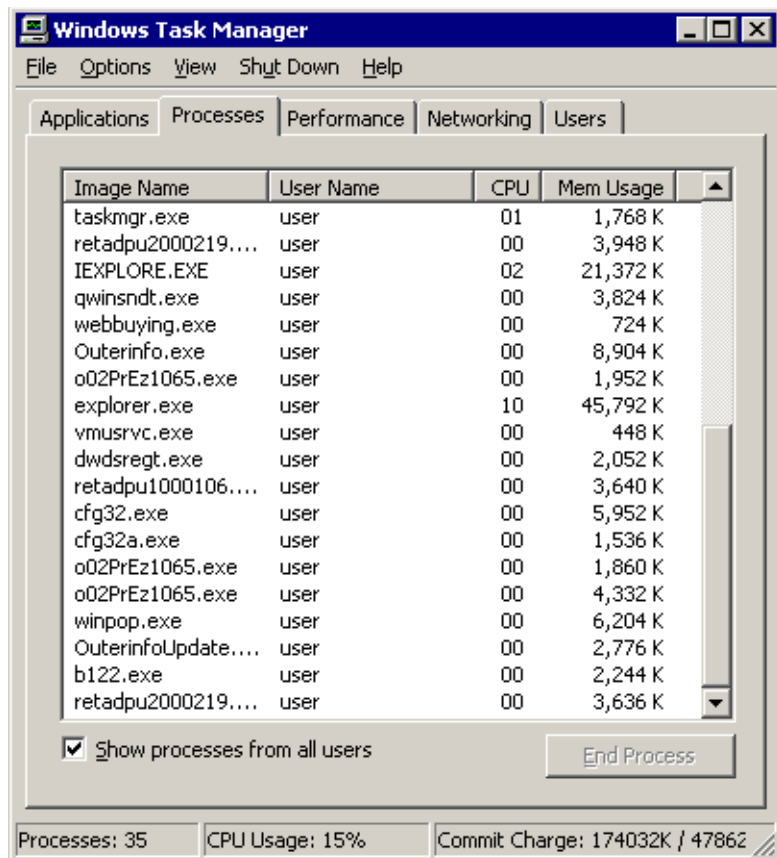
The consequences in this case are fairly minimal since this isn't even my secondary machine-- it's a special-purpose PC dedicated to gaming. Reinstalling the operating system is no big deal. But it's still an inconvenient timesink, and in any case, the spyware infestation has to be dealt with because it causes serious performance problems and will even interrupt gameplay with incessant popups.

The two most common sites for no-cd patches are [MegaGames](#) and GameCopyWorld. In case you're wondering, yes, I do own all my games. I download no-cd patches for convenience's sake; I consider them a privilege of ownership for knowledgeable, ethical PC gamers. I figured the infection came from one of these sites. So I set up a [honeypot virtual machine](#) under [Virtual PC 2007](#), using the ancient, original 2001 release of Windows XP and the classic [Devil's Own key](#), and began testing.

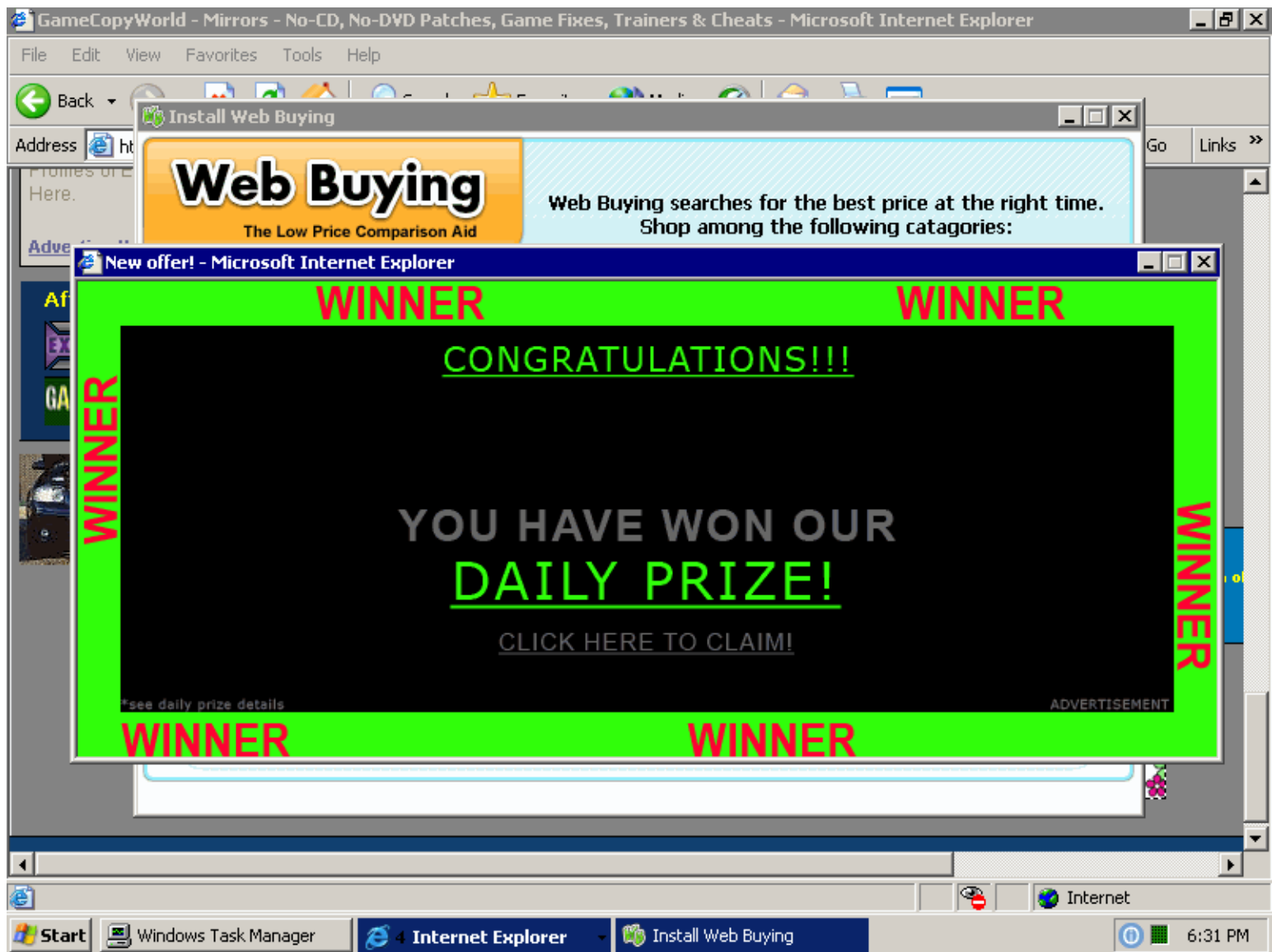
Here's a shot of Task Manager at the desktop, after installing the necessary virtual machine additions. This is a completely plain vanilla, clean Windows XP installation: no service packs, no updates, no nothing. This system is connected to the internet, but it's not as dangerous as it sounds. Because it's behind a NAT router that blocks all incoming connections, there's no way it can get *passively* infected. I let it connect to the internet and quiesce at the desktop for about an hour, just to prove my point. **No passive infections occurred behind a NAT router**, even for this woefully out of date September 2001 era install of Windows XP.



Now we're leaving passivity behind, and unwisely **browsing the open internet with the unpatched, six year old original version of Internet Explorer 6.0**. [Danger, Will Robinson!](#) I left Task Manager running as I browsed to MegaGames, downloaded a no-cd patch, and... nothing. I then visited GameCopyWorld, downloaded a no-cd patch, and... all of a sudden, it's crystal clear who the culprit is. Check out Task Manager now:



This comes as a shock to me, because GameCopyWorld is recommended often in gaming forums. I consider(ed) it a reputable web site. I've never had a problem with the site before, because I usually surf with the latest updates. But the unpatched browser spyware infestation from visiting GCW-- **just from visiting the web pages, even if you don't download a single thing**-- is nearly immediate and completely devastating. The virtual machine desktop, after a few scant minutes, tells the story:



It isn't pretty, and let me tell you, **I have a new degree of sympathy for the poor users who become the unfortunate victims of spyware infestations.** The machine becomes borderline unusable, between...

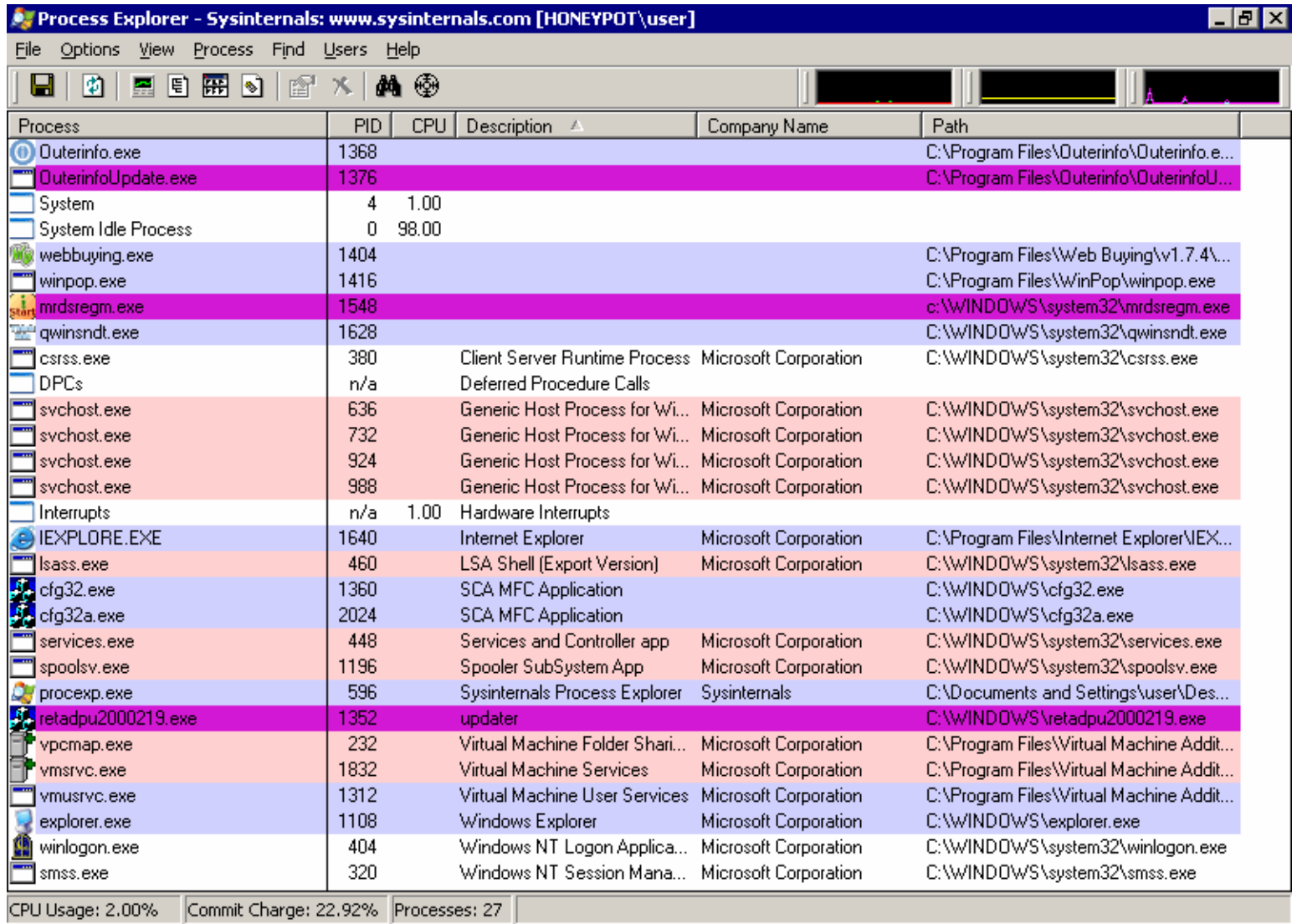
- new icons that magically appear on your desktop
- full-screen popups that occur every two minutes
- dialog boxes that offer to "install antivirus software" with only an OK button
- system performance degradation from all those spyware background processes

... it's a wonder people don't just give up on computing altogether. Once the door is open, it seems the entire neighborhood of malware, spyware, and adware vendors take up residence in your machine. There should be a special circle of hell reserved for companies who make money doing this to people.

At first, I was mad at myself for letting this happen. I should know better, and I *do* know better. Then I channeled that anger into action: **this is my machine, and I'll be damned if I will stand for any slimy, unwanted malware, adware, or spyware that takes up residence on it.** I resolved to clean up my own machine and fix the mess I made. It's easier than you might think, and I'll show you exactly how I did it.

Our first order of business is to **stop any spyware that's currently running.** You'll need something a bit more heavy-duty than mere Task Manager-- get Sysinternals' [Process Explorer](#). Download it, run it,

and sort the process list by Company Name.

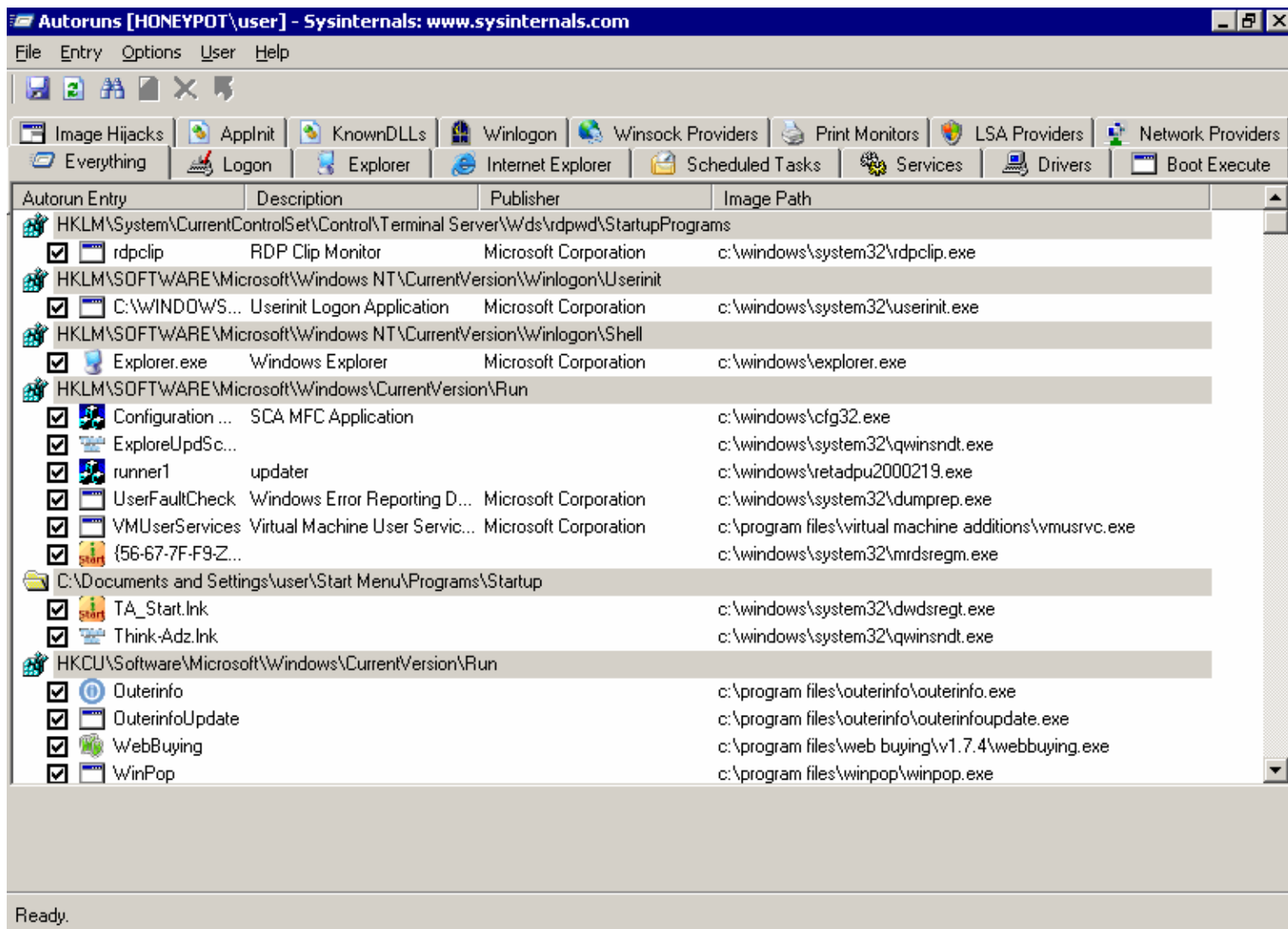


Process	PID	CPU	Description	Company Name	Path
Duterinfo.exe	1368				C:\Program Files\Duterinfo\Duterinfo.e...
DuterinfoUpdate.exe	1376				C:\Program Files\Duterinfo\DuterinfoU...
System	4	1.00			
System Idle Process	0	98.00			
webbuying.exe	1404				C:\Program Files\Web Buying\v1.7.4\...
winpop.exe	1416				C:\Program Files\WinPop\winpop.exe
mrdssregm.exe	1548				c:\WINDOWS\system32\mrdssregm.exe
qwinsndt.exe	1628				C:\WINDOWS\system32\qwinsndt.exe
csrss.exe	380		Client Server Runtime Process	Microsoft Corporation	C:\WINDOWS\system32\csrss.exe
DPCs	n/a		Deferred Procedure Calls		
svchost.exe	636		Generic Host Process for Wi...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe
svchost.exe	732		Generic Host Process for Wi...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe
svchost.exe	924		Generic Host Process for Wi...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe
svchost.exe	988		Generic Host Process for Wi...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe
Interrupts	n/a	1.00	Hardware Interrupts		
IEXPLORE.EXE	1640		Internet Explorer	Microsoft Corporation	C:\Program Files\Internet Explorer\IEX...
lsass.exe	460		LSA Shell (Export Version)	Microsoft Corporation	C:\WINDOWS\system32\lsass.exe
cfg32.exe	1360		SCA MFC Application		C:\WINDOWS\cfg32.exe
cfg32a.exe	2024		SCA MFC Application		C:\WINDOWS\cfg32a.exe
services.exe	448		Services and Controller app	Microsoft Corporation	C:\WINDOWS\system32\services.exe
spoolsv.exe	1196		Spooler SubSystem App	Microsoft Corporation	C:\WINDOWS\system32\spoolsv.exe
proccxp.exe	596		Sysinternals Process Explorer	Sysinternals	C:\Documents and Settings\user\Des...
retadpu2000219.exe	1352		updater		C:\WINDOWS\retadpu2000219.exe
vpcmap.exe	232		Virtual Machine Folder Shari...	Microsoft Corporation	C:\Program Files\Virtual Machine Addit...
vmssvc.exe	1832		Virtual Machine Services	Microsoft Corporation	C:\Program Files\Virtual Machine Addit...
vmusrvc.exe	1312		Virtual Machine User Services	Microsoft Corporation	C:\Program Files\Virtual Machine Addit...
explorer.exe	1108		Windows Explorer	Microsoft Corporation	C:\WINDOWS\explorer.exe
winlogon.exe	404		Windows NT Logon Applica...	Microsoft Corporation	C:\WINDOWS\system32\winlogon.exe
smss.exe	320		Windows NT Session Mana...	Microsoft Corporation	C:\WINDOWS\system32\smss.exe

CPU Usage: 2.00% Commit Charge: 22.92% Processes: 27

Kill any processes that don't have a Company Name (with the exception of DPCs, Interrupts, System, and System Idle Process). Right-click the processes and select Kill, or select them and press the Delete key. You can use my initial screenshot of Task Manager, at the top of this post, as a reference for what *should* be running in a clean Windows XP installation. But there's usually no need to be that specific; unless it has a Company Name you recognize, it's highly likely to be a rogue application and should be terminated.

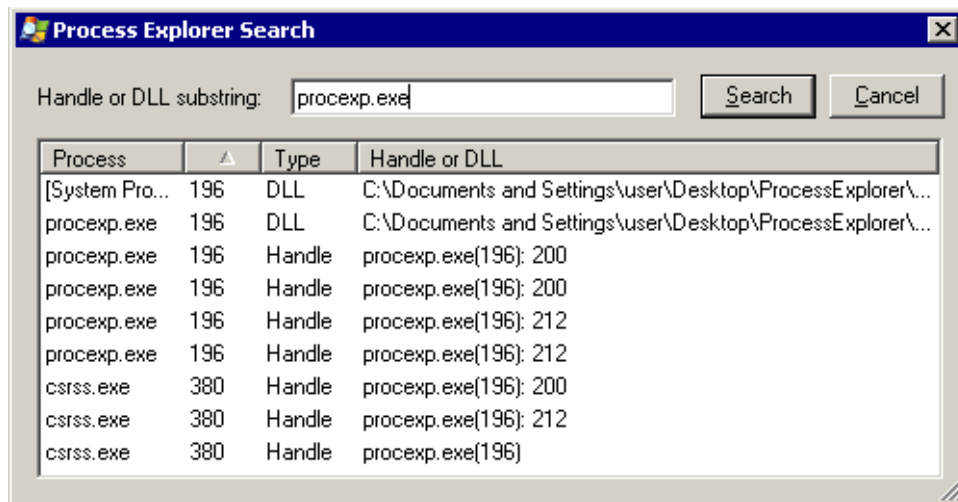
Stopping the running spyware is only half the battle. Now we need to **stop the spyware from restarting the next time we boot the system**. [Msconfig](#) is a partial solution, but again we need something more powerful than what is provided out of the box. Namely, SysInternals' [AutoRuns utility](#). Download it, run it, and start browsing through the list that appears:



As you can see, there's a bunch of spyware, malware, adware, and god knows what else gunking up the works-- all from visiting a *single* website! **Scroll through the list, all the way to the bottom, scanning for blank Publishers, or any Publisher you don't recognize. If you see anything that's suspect, delete it!** In a default Windows install, 99.5% of the entries will have "Microsoft Corporation" as the Publisher. Any *reputable* vendor will have no problem attaching their name to their work, so it's generally only the blank entries you need to worry about.

Now **reboot the system**. We've removed most of the spyware infestation, but there's a certain much more virulent class of spyware that can survive this treatment. We'll deal with them next.

After rebooting, check Process Explorer and Autoruns for anything suspicious, exactly as we did before. The first thing I noticed that "came back" in Autoruns was a suspicious driver, core.sys, that didn't have a Publisher. I used **the powerful Find | Find Handle or DLL menu in Process Explorer** to locate any active references to this file.



Unfortunately I didn't capture the right screenshot at the time, so I'm showing a generic search result above. Anyway, there was exactly one open handle to the core.sys file. I selected the result, which highlights the corresponding handle in the lower pane of the Process Explorer view. Right-click the handle entry in the lower pane and click "Close Handle".

Type	△	Name
File		C:\System Volume Information_restore{969DEF20-3A10-4964-AEC0-5
File		\Device\Tcp
File		C:\WINDOWS\system32\config\SECURITY.LOG
File		C:\pagefile.sys
File		\Device\Tcp
File		C:\WINDOWS\system32\drivers\core.cache.dsk
File		\Device\Tcp
File		C:\WINDOWS\system32\drivers\core.sys
File		\Device\Tcp
File		\Device\Tcp
File		C:\WINDOWS\system32\config\SAM.LOG
File		\Device\Tcp

Close Handle
Properties...

After I closed the handle, I could physically delete the rogue core.sys file from the filesystem, along with the Autoruns entry for it. Problem solved!

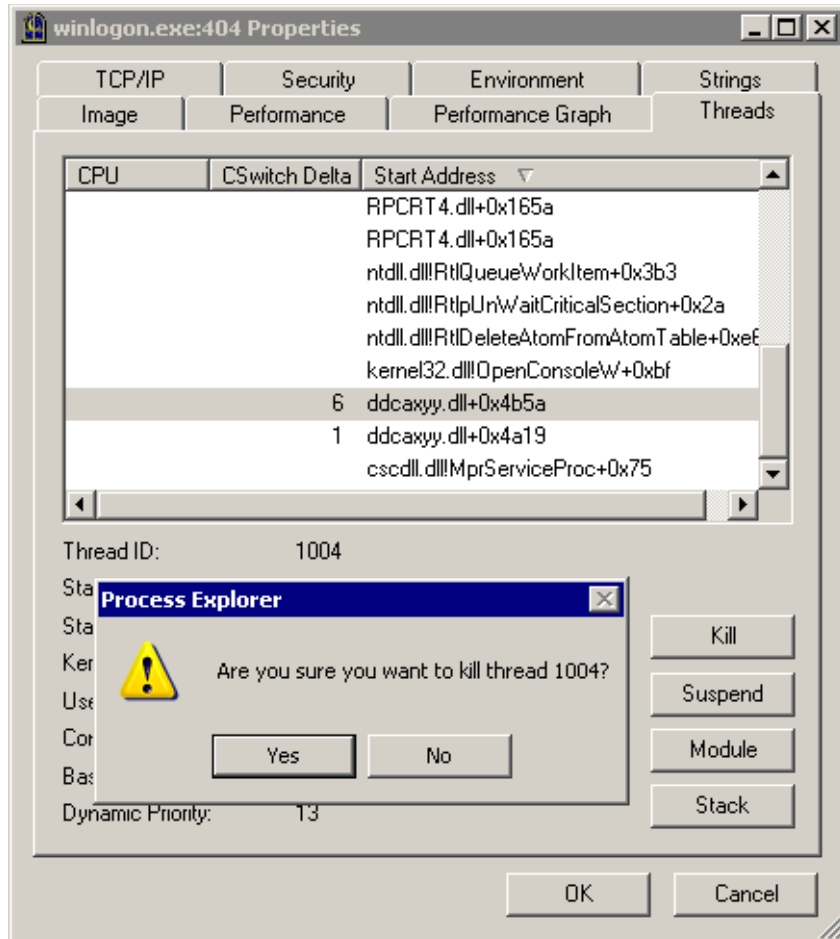
The other item that reappeared in Autoruns after the reboot was an **oddly named DLL file with hooks into Winlogon and Explorer**. In addition to the suspicious name, each entry carries the tell-tale sign of the missing Publisher value:

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks				
<input checked="" type="checkbox"/>	ddcaxyy.dll			c:\windows\system32\ddcaxyy.dll
<input checked="" type="checkbox"/>	shell32.dll	Windows Shel...	Microsoft Corporation	c:\windows\system32\shell32.dll
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				
<input checked="" type="checkbox"/>	{8A61098D-61...			c:\windows\system32\ddcaxyy.dll
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify				
<input checked="" type="checkbox"/>	crypt32chain	Crypto API32	Microsoft Corporation	c:\windows\system32\crypt32.dll
<input checked="" type="checkbox"/>	cryptnet	Crypto Networ...	Microsoft Corporation	c:\windows\system32\cryptnet.dll
<input checked="" type="checkbox"/>	cscdll	Offline Networ...	Microsoft Corporation	c:\windows\system32\cscdll.dll
<input checked="" type="checkbox"/>	ddcaxyy			c:\windows\system32\ddcaxyy.dll
<input checked="" type="checkbox"/>	ScCertProp	Common DLL ...	Microsoft Corporation	c:\windows\system32\wlnotify.dll

Delete the entries in Autoruns all you want; they'll keep coming back when you press F5 to refresh. This rogue, randomly named DLL continually monitors to make sure its ugly little hooks are in place. The nasty thing about processes attached to [Winlogon](#) is that they're very difficult to kill or remove. We can kill

Explorer, but **killing Winlogon is not an option**; it's the root process of Windows, so shutting it down causes the OS to restart. It's a difficult [catch-22](#).

But we're smarter than the malware vendors. Fire up Process Explorer and use the Find | Find Handle or DLL menu to locate all the instances of this DLL by name. (See, I told you this option was powerful.) Kill any open handles to this file that you find, exactly as we did before. But you'll need to go one step further. We know from the Autoruns that this DLL is likely to be attached to the Explorer and Winlogon processes, but let the find results be your guide. Double-click on any processes you found that reference this DLL. **In the process properties dialog, select the Threads tab. Scroll through the threads and kill every one that has the rogue DLL loaded.**



Once you've killed all the threads, you can finally delete the entries in Autoruns without them coming back. Reboot, and your machine is now completely free of spyware. **I count 17 entries in Task Manager, exactly the same number as when I originally started.**

Of course, the smartest thing to do is **not to get infected with spyware, malware, or adware in the first place**. I can't emphasize this enough: *always browse with the latest patches for your preferred web browser*. But if you do happen to get infected, at least now you have the tools and knowledge to banish these evildoers from your machine forever.

Update: If you're worried about spyware, malware, and adware, you should strongly consider [not running as an Administrator](#).

Posted by Jeff Atwood

« [Incremental Feature Search in Applications](#)

[Escaping From Gilligan's Island](#) »

Comments

After carrying out the above steps, your system is clean in the sense that it isn't actively running adware/malware/spyware any more. However you should still run Ad-Aware, Spybot, and/or HijackThis to get rid of any spoor left behind by the adware. Things like orphaned files, tracking cookies, obsolete registry entries, and so forth.

http://www.lavasoftusa.com/products/ad_aware_free.php

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

<http://www.spywareinfo.com/~merijn/programs.php#hijackthis>

Microsoft also has a malicious software removal tool which is freely downloadable:

<http://www.microsoft.com/security/malwareremove/default.msp>

Jeff Atwood on June 17, 2007 11:46 AM

With all due respect and without trying to sound noobish, wouldn't it have been better if I had left the job to a combination of Spybot SD, Ad-Aware and HijackThis instead of rummaging through tons of process threads and startup entries and then deleting them. These can do the job pretty efficiently with HJT being the best choice for getting rid of BHOs.

There is no doubt this post is a highly knowledgeable one considering that it delves deep into the manipulation of things at the process and registry level, places about which people are either totally unaware or even if they are in the know, they choose not to fix what ain't broken. From the sole viewpoint of academic interest, this is an excellent post. But if I wanted to do the job faster and more efficiently, I would have rather gone for the above mentioned tools.

anomit on June 17, 2007 11:47 AM

Very helpful, thanks. Spybot SD isn't as powerful as this.

Another recommendation would be to have Firefox with the NoScript addon. It disables all scripts on pages, and has a whitelist function. After installing it I've received alot less adware.

Cheers.

Jaan on June 17, 2007 11:54 AM

I would also consider running RootKitRevealer from sysinternals for those extra sneaky spyware that don't even show up in ProcessExplorer.

<http://www.microsoft.com/technet/sysinternals/utilities/RootkitRevealer.msp>

Haacked on June 17, 2007 11:55 AM

These can do the job pretty efficiently with HJT being the best choice for getting rid of BHOs

Both Ad-Aware and Spybot *FAILED* to remove the multiple winlogon infections, including Virtumonde. They were the first thing I tried! After that I figured, the heck with it, I can do it better myself.

Those programs are good for cleaning up leftover files on disk and miscellaneous registry keys *after* the steps I outlined above.

Jeff Atwood on June 17, 2007 11:58 AM

Thanks for the explanation of the latter-stage removal, thread killing, etc.

It just boggles the mind that a user application could put this much debris in the system directories (I'm assuming that you were browsing as an unprivileged user.) Not to be naive or a troll, but honestly, what the hell were they thinking when they expanded IE into something so complex with such loose security? With all the convoluted access control that Windows offers, the OS app vendor couldn't or wouldn't obviate this problem during the design phase; it's pathetic.

In a related exercise, try downloading a Firefox installer as Administrator on Windows 2003 Server. The combination of Mozilla's random download mirrors and IE's twitchy security model make it improbable you'll ever get the installer downloaded. So even if you want to use a browser that is unlikely to run with elevated privileges, you can't get it because the existing browser knows what's best for you, security-wise.

There's a balance between protecting the user and giving them enough control to make the system usable. The problem here is lack of visibility and choice - in the former case you have software that installs without giving you any notice or choice, in the latter you have plenty of alerts, but very little choice because the alerts appear after the browser has interfered with your request.

Why the OS installer decides (again, without giving me a choice) that I need a graphical desktop environment, a media player, and a browser more complex than lynx on a headless server mounted in a rack in a datacenter is a separate question that nobody has satisfactorily answered (Microsoft is the major culprit, but not the only one.) I think you're on the right track with virtualization.

Bob on June 17, 2007 12:04 PM

obligatory Linux post:

I really doubt the average user could do all that. It would be much easier to just use a user-friendly Linux distribution like Ubuntu (after getting a knowledgeable friend to do the initial setup of course).

James Justin Harrell on June 17, 2007 12:19 PM

or ditch Windows and switch to Linux or Mac. problem solved.

Jack on June 17, 2007 12:25 PM

It's amazing how something as small as this gets overlooked by so many blogs and self-help articles out there. Ad/Spyware is one of the biggest problems plaguing the general computing world today! :(

Thanks for the steps and the programs Jeff! I'll use this guide if (keep my fingers crossed) I ever get infected with those things! :)

Aditya Mukherjee on June 17, 2007 12:33 PM

or ditch Windows and switch to Linux or Mac. problem solved

Well, except for the fact that the excellent PC racing simulators I referenced in the very first paragraph-- the entire reason this machine exists-- don't run on Linux or Mac. :)

Jeff Atwood on June 17, 2007 12:38 PM

Perhaps I'm a little biased, and perhaps I should ignore the trolls, but I don't see too many Racing sim titles on Mac:

<http://www.apple.com/games/>

or on Ubuntu:

http://doc.gwos.org/index.php/Simulation_Games

Jim on June 17, 2007 12:39 PM

What about....

- * attaching to Internet Explorer [start page, search address, plugin, toolbar...]
- * changing proxy settings
- * editing the hosts file

Admittedly you did a very thorough job, but there's so many places things can get that I will never trust a machine as clean once it has anything on it.

Nick on June 17, 2007 12:46 PM

I think you are wrong here in 2 points:

1: if there was a process running as an administrator your system is corrupt. (regardless of what your process list says) either look for the names of the programs and find antispyware/antivirus/antiwhatever software. if every program could get identified and removed, your system is restored. if you don't know what the program does you just can't only remove them because you don't know where the program writes something into.

2: your company name search pattern is too vague. there will be good software without and there will be bad software with a company name.

hacktick on June 17, 2007 12:54 PM

So, you cleaned an infestation without resorting to cleaners? You know your way around a computer? Feeling "all high and mighty, eh?"

I did once, too, until I met my first rootkit. One of my production servers on a remote data server was "infected" with a pirate FTP server and numerous little applications to administer and protect it. On top of them all was a damned little tool called "Hacker Defender", a rootkit based tool that can hide processes, directories, files and even ports at the kernel level.

There was 5 or 6 processes that were hidden by HD and Process Explorer did not even see them. I had to use a special tool to even be aware of them. And what's more, most of those hidden processes, when killed, took the system down with them, as well. A remote server crashing and restarting itself? Fun.

So, don't become over-confident on your abilities and tools. Be like the Zen and add the Rootkit Unhooker to that toolkit (<http://rkunhooker1.narod.ru/>)

Ishmaeel on June 17, 2007 12:55 PM

what a nice *nix fanbase you have jeff. :)

Sad that no-cd patches is important. This is a typical example on how the fight against pirated software do more harm to those who buy the software. The ones that wanted a pirated version would probably get it anyway.

Maybe IE had some security breaks, but it should not be possible for IE to act as an administrator. No software is perfect, no operating system is perfect, and for sure no human is perfect.

Compared to Unix, Windows never seemed to be designed for the net; you could maybe say that Windows had the network as a feature.

Where a windows commercial would go "Use this software to go on the internet", you could say that with a *nix machine you already where a part of the net and was forced to think of security.

I am by no means a security expert, but I can say it has been healthy for me installing linux distributions after several years as a Microsoft developer.

Peter Palludan on June 18, 2007 2:06 AM

autoruns + processxp indeed.

My gf had a root-kit on her computer, nobody realized it who had worked on it before. She was just randomly getting pop-ups and nothing was running. Rootkit revealer, also from sysinternals is also a

nice program to run. finds most of them.

apeinago on June 18, 2007 2:32 AM

On the interminable linux point:

I've seen what end-users do with linux. They'll happily just run, as root (either directly or via sudo) any random .rpm or .deb they think has The Coolest Thing (say, oh, "EverythingYouNeedForBery!!! OMGITZKOOL !!! JustLikeVistaOnlyLinux!!!!InOneFile!!!.rpm" - I exaggerate, but only a little.).

If lthat/i contains a rootkit, they've just screwed themselves as well as anyone running Windows running a random .exe.

The problem is not so much the OS (not to let MS off the hook - various versions of IE 7, for instance, would run 3rd party code from a popup ad even if you clicked the close icon on the IE window frame, nothing inside the popup - that's just intolerable), as users.

Users are lazy and clueless, and will happily disregard your security infrastructure if there's any way for them to do so, if they think it'll make their lives temporarily easier, or faster.

MS has done pretty well at preventing attacks that laren't due to the user/i, these days, with XP SP2+ or Vista. Nothing can save the user from user stupidity.

(Vista UAC helps, but just today, somewhere else, I saw someone say "first thing, turn UAC off!" ... I suppose the only way people are going to be satisfied is if the default install simply installs a fast virtual machine and that's all you ever run, to just reinstall it whenever necessary.)

Sigivald on June 18, 2007 2:42 AM

And they say Linux isn't ready for the desktop...

Christoffer Hammarstrm on June 18, 2007 3:15 AM

If it's just a gaming rig, don't connect it to the internet (ignore if you're playing networked games!). Download your no_cd hacks on a fully patched PC (or a Mac or Linux box).

Adrian M on June 18, 2007 3:27 AM

Hurray for Norton Ghost and the 10 minute rebuild. I dont bother with anti-virus/anti-spyware eating my resources - just keep your eyes on your CPU/network usage, and when ready nuke it!

Do this to XP every 3 months or so anyway - fast and clean windows.

mafro on June 18, 2007 3:39 AM

I wonder how long it takes for the spyware/adware people (slime?) to start setting "Microsoft Corporation" as the publisher.

Hrm...is the publisher a cryptographically signed field?

Neil on June 18, 2007 3:49 AM

hi jeff

There isd a nice bit of software that allows you to not need to get a no-CD crack for your own software try Alcohol 120%, allows you to backup the cd /dvd then run the disk in a virtual drive, what i do as some online games think the no cd crack is a cheat.

AlBear on June 18, 2007 3:52 AM

Perhaps the reason that the freeware tools you used completely failed was that they are increasingly really pretty (comparatively) useless..

<http://www.av-comparatives.org/>

This doesn't include the freeware stuff, but I did see a comparison in one of the PC mags some months ago (something similar to PC World) that did, and it found the freeware tools only had a detection rate of around 55%.. They were compared to McAfee which at the time showed a 97% removal rate. Now, if you look at the above link you'll find that McAfee has a pretty poor showing when compared to a few of the winners (in order - G-Data AVK (Anti-Virus Kit), Avira AntiVirus, NOD32, and iirc the next one was Sytmantec)..

To me, this suggests that these winning entries (Avira did especially well at heuristics - detecting stuff for which no product has signatures for) are waaaay ahead of the trusted freeware alternatives.

That said, you want good protection, pay or pirate..

Al Binewski on June 18, 2007 4:06 AM

A machine which was infected by a virus, trojan or any other badware must be cleaned from scratch - burn the data to DVD, and scrub the rest.

Rootkits are very challenging to detect - to take no risk, set up the system from ground off.

For your gaming machine your actions taken may be ok - but if it was a machine used for business i could never sleep well again, if the machine is not purified to the very last bit.

Of course, the saved data must be analyzed by a number of virus-scanners before being used again.

Paranoia is useful even for non-paranoids :-)

toettoe on June 18, 2007 4:10 AM

When it comes to malware removal, I really like a combination of safe mode and AVG Anti-Spyware/AVG Anti-Virus. When preventing malware, safe browsing habits and a secure browser are tops. And you always need a good firewall when connected to the Internet.

My system of monthly full scans using AVG's products and weekly quick scans using the same programs (both using up-to-date definitions), Firefox, safe browsing habits, and a firewall (in my case, ZoneAlarm), I haven't had any malware worse than a tracking cookie (which isn't a program or application anyway, at least to my knowledge).

In fact, I even carry a CD with the installation files for the free versions of AVG, the latest Firefox, and ZoneAlarm with my computer. I've set up systems for friends that have these, and I haven't been asked to fix a spyware problem since then.

Thomas on June 18, 2007 4:22 AM

+10 for SysInternals RootKit Revealer

I recently had my very first virus in all of 15+ years of computing. There is a mechanism where by which the rootkit installs itself as a service in the registry (HKLM\System\CurrentControlSet\Services\...). It doesn't appear in the task manager, nor could I find it in Process Explorer. The rootkit will actually prevent you from modifying the registry entry either via RegEdit, Win32 API, or Native NT functions. The rootkit in turn, makes sure that a browser helper object is always loaded. Of course I couldn't delete the .sys or .dll files, they were locked and/or the rootkit installed hooks preventing the files deletion.

The only way to clear this infection is to mount the HD onto another machine and remove offending files, or, what I did in the end, create a BartPE windows "live" cd and delete the files that way. Then after booting off the HD, the service wasn't being loaded, and I could repair the registry.

Jeff, I really recommend you run RKR.

Damian on June 18, 2007 4:25 AM

Run IE in a sandbox. Sandboxie.com has a free tool and it's better than running a VM because it tells you which files and processes have been touched in a virtual HD. Plus it's lightweight and runs fast.

Abdu on June 18, 2007 4:57 AM

"I have been running Windows XP without any firewall or antivirus applications for years with no virus or spy/adware infections. It often makes me wonder how I seem like the only person who manages to do that..."

Me too... same wonder.

Jasmine on June 18, 2007 5:04 AM

your demonstrations was another great suggestion,
browse the internet from a virtual pc.

jg on June 18, 2007 5:26 AM

First: Jeff, thanks for the article. It does resemble Russinovich's presentation, but since his is video and yours is text, I find this more valuable. Good job - now I can paste a link rather than giving a 20 minute demonstration!

To some of the extra-paranoid folks who're head-desking and shouting reformat and reinstall: *you are right* - they *are* out to get you! But different situations have different security needs. If the system is used to manipulate highly valuable data (like your bank account, or your connection to the company VPN), then yeah. Reformat, reinstall. But Jeff was at pains to note that this is only a gaming system, so he was happy once the system stopped *acting* infected. Me, I might have done a little packet sniffing to be sure, but again, Jeff's choices are based on his own perception of risk level. Not all systems need to be run as if they were full of Top Secret data!

(If Helen Keller gets a virus that presents no symptoms at all, is she actually sick?)

To those of you suggesting all sorts of antimalware tools: run nonadmin, stay patched (and actually reboot when the OS tells you to, m'kay?), turn on the Windows Firewall, pay attention to what you are allowing whenever the 'OK' button pops up. Skipping these measures and running a ton of antimalware tools slows down your system and leaves you fighting fires constantly. Scan your system with a reputable antimalware scanner weekly or so. You'll be surprised how secure the OS is once you start using it properly!

quux on June 18, 2007 5:45 AM

and after all that effort you still can't trust that installation again.
You are much better off reinstalling from scratch and this time, install all patches and don't run as administrator.

Jesse on June 18, 2007 5:49 AM

I would also compare listening pids to tasklist, and msconfig to rule out ms processes if your going thru all the trouble of checking processes.

Anonymous Coward on June 18, 2007 5:53 AM

The Unix root user security model is not what makes Unix secure. A limited user account might have saved your system data. That's not much use when user data is the important data anyway. System data is cheap to restore: the system disk comes on its own CD with a new computer.

On a multiuser system limited users are vital. I maintain several Unix servers and see user accounts get hijacked every now and then due to bad passwords, insecure web sites, ssh keys hijacked from a home machine, etc. Users are limited to damaging their own accounts, so long as the systems are kept up to date.

There are privilege escalation attacks available against unpatched systems, and those `_do_` get tried. I live in fear of zero-days, of course. That would mean a wipe and restore from tape.

I wouldn't trust a manual clean up like you've just done. As other users have pointed out, root kits are easy. Root kit revealers are not nearly as reliable as virus scanners, which are themselves not especially reliable. If you've got a root kit, your machine can be re-hijacked at any time to send spam or whatever, just by the bad guy connecting in.

Linux or Macs are one kind of solution, as others have pointed out. I've seen too many Unix security incidents to consider them any sort of ecosystem solution -- if everybody adopted Linux, we'd be exactly where we are with Windows, once all the bad guys began writing their tools for it.

My own belief is that things are as good right now as they are going to get. There is no technical solution to the problem of software security bugs. If we ever want to end the spam, the identity theft, and the viruses, we're going to have to do it with international legislation and international enforcement. Doesn't seem likely to me.

Joel Eidsath on June 18, 2007 6:09 AM

I also get no-cd patches and other goodies from gamecopyworld.

I've been doing this for some years and always found the process tedious (if you have some games and don't want to "filter" before downloading, that's an awful lot of links to click on)

As some kind of a programmer (at least that's what i do for a living), i quickly hacked together a lil' perl script that does "automatic downloading" of all files related to the games i own.

The big advantage is I only need one click to check if there's any new (updated ?) no-cd/trainer/savegame/gameguide/etc... for any game of my collection and to download it.

It was really an easy thing to do and a big time savior...

...

So what made me post this is how somebody like you could possibly go through the hassle of doing it manually...

I mean you could've submitted the task of writing this script as a substitute to "FizzBuzz" in you interviews ;)

billy on June 18, 2007 6:11 AM

Friends don't let friends use IE :) It's a massive front door for every piece of malware that dubious parties want to install remotely on your PC. I never use IE to visit any unknown or untrusted site, and the first thing I do with it on a new computer is, invariably, downloading Firefox.

CleverShark on June 18, 2007 6:12 AM

I've used these tools often to remove spy/adware as well. My friend's PC recently had a particularly nasty piece of adware which wouldn't leave without hacking it away from Safe Mode.

I have been running Windows XP without any firewall or antivirus applications for years with no virus or spy/adware infections. It often makes me wonder how I seem like the only person who manages to do that... and yes, I do browse the net, download um.. "Linux distros" and... the usual suspects, so the PC is used for a lot of things.

Jani on June 18, 2007 6:22 AM

Interesting your "completely my own fault" comment. I have done the same thing ... I preach security all day long at my job and on my own time to friends and family. But then ... for some reason ... I forget my own advice and don't patch, or post personal info somewhere, or something. I guess its human nature sometimes to "just get the job done" and feel sick with all the dumb precautions. Can't the world just be free of bandits?

James Risto on June 18, 2007 6:24 AM

This reminds me of a video (or was it a series of screenshots? Whatever it was i'd love to find it again if anyone else remembers) of a virtual machine after bonzi-buddy was installed on it.

Anyone else remember this?

koenocphi on June 18, 2007 6:30 AM

Block startup leechers, or at least get warning:

<http://www.mlin.net/StartupMonitor.shtml>

landmn on June 18, 2007 6:39 AM

<http://housecall.trendmicro.com>

I use the above whenever I wonder about the state of my WinXP partition.

BTW- it bugs me to no end when people think that *nix boxes are only saf(ER) because fewer use them. It has much more to do with native userspace security and the bleedingly fast development curve.

"Linux and Apple boxes are safer because no one uses them" -Bah! Microsoft propaganda...

Sorry- but I've been meaning to rant on that for a while now. Most of the people I hear say that in real life are too clueless to understand the concepts anyway, so I just keep it to myself.. I'm glad it came up here amongst this audience.

Petskull on June 18, 2007 6:47 AM

A few other suggestions (for when you just can't nuke the box).

Use "Verify Signatures" + "Hide Signed Microsoft Entries" if (when!) you're using Autoruns.

Instead of killing the threads with the dlls loaded, suspend them. You'll be able to remove the files/registry entries and reboot without the malicious code replacing them since it won't be re-run by any logoff/shutdown hooks.

The Recovery console almost guarantees success if you're intimately familiar with Windows.

A port scan from "the outside" (and an IP Bridge you can watch network traffic on) can go a long way to having confidence the box is clean(ish).

mostly anonymoose on June 18, 2007 6:48 AM

Have you asked GameCopyWorld to 'splain themselves? If you can get to GCW via a Google search, have you notified Google?

David A. Lessnau on June 18, 2007 6:56 AM

Jeff,

Fantastic (and timely) article, this is exactly the level of detail I needed. I have just managed to clean 2 bad infestations which where proving particularly resilient, but thanks to your thread killing advice it all didn't end in tears, a full rebuild of this ugly sucker would have taken days to weeks to have back in shape. Many many thanks

cl3ft

cl3ft on June 18, 2007 7:06 AM

Windows is in desparate need of a robust package system.

Problems

- inability to install multiple copies of the same program
- problems removing old applications cleanly
- conflicts between installed programs
- no way of specifying an applications interactions with the system and other programs
- no enforcement mechanism for declared interactions
- compromised applications typically have access far beyond their needs

Implementation

- each application must provide a manifest documenting all possible interactions
- the application would explicitly document its dependencies
- the administrator chooses whether to activate an application, possibly with additional restrictions
- the user may be enabled to activate applications as well but this is an explicit process
- the application interacts with the system through a layer that restricts what the app can do
- when a violation is detected, the application is halted and flagged
- the wrapper layer provides a view of the filesystem that only includes areas it needs to see
- the wrapper layer can restrict access to the file types declared in the manifest
- developer tools should help autogenerate the manifests and packages

Benefits

- solves much of the configuration decay issues that Windows has
- the manifest driven wrapper layer helps to control compromised executables
- malware (and any application) is easily uninstalled
- you can run multiple versions of the same program (e.g. Word)
- easier to run programs remotely, or from removable media

Notes

- SoftGrid, et al, is a step in this general direction
- Unix world have various parts and techniques (packages, chroot, executable bit, privilege separation, etc)
- no complete or consistent system applied to all apps though

Grant on June 18, 2007 7:09 AM

It's been my experience that System Restore can be pretty evil, and cause the reinstallation of viruses and malware once you've cleaned them up. Of course it's entirely possible that such cases are do to multiple malware installations.

If you encounter a rash of malware you can't get rid of, try turning off system restore, that may solve the "recurring infection" problem.

CleverShark on June 18, 2007 7:20 AM

"MS has done pretty well at preventing attacks that aren't due to the user, these days, with XP SP2+ or

Vista. Nothing can save the user from user stupidity."

Oh come on. Vista still gladly gives you administrator rights by default, and the "notifications" you get before messing up your system come in the form of a rather innocuous alert box that doesn't even require you to type anything more than the enter key to dismiss.

It's not a robust mechanism, but it does allow Microsoft to say "well, we warned you so it's your own fault". It won't do a great job protecting anyone except the Microsoft Corporation.

CleverShark on June 18, 2007 7:25 AM

My recipe: Disable java, javascript and active-x.

Problem solved.

No need for spyware searchers, AV or other "security" packages that attempts to detect a threat retroactively.

Of course, in theory a security hole could exist in the jpg rendering engine (and such has been found before), but most (if not near-all) holes seem to hit the script engines and active-xs.

Or just leave the admin account alone until needed. (Ironically... Game copy protection checks rely on admin rights to install their drivers, which is probably why MS started distributing some of the copy protection engines as part of the standard OS installation)

--

Rune

Rune on June 18, 2007 7:28 AM

Uhm, Grant: You can already run multiple versions of Word. Word 2003 can co-exist with Word 2007... User settings are stored separately and they are by default installed to separate folders.

Rune on June 18, 2007 7:32 AM

Wow, these posts sure do demonstrate the level of superstition around malware. The typical user machine that is loaded with malare can be cleaned by hand, as Jeff demonstrates, and as I've done numerous times. You can even get away with not using the tools he suggested and going straight to safe mode, regedit, and unlinking the DLLs from the Command Prompt.

It's entirely possible and has always worked just as well as SpyBot or AdAware did for me. People seem to think that these tools implement some magical techniques, but really they are just doing exactly what Jeff outlined above, but automatically. No tricks, no industrial-strength algorithms, just killing processes, removing files, and removing registry entries.

John C on June 18, 2007 7:35 AM

But an Apple Mac or an easy install like Ubuntu or Mandriva

David Ginger on June 18, 2007 7:50 AM

Jeff, it's often amusing when someone of your stature gets "bitten". A few months ago I think you went on about how you didn't need anti-virus software and intimated that it was really necessary only for users who hadn't quite arrived.

At any rate, after Windows 3.11 it seems that it became the norm for vendors to write files to my PC at will, usually without my consent or prior knowledge. Software connects back to the vendor with no action taken on my part.

Until laws are passed that make it a crime for anyone to put software on my PC without my consent, we will be in the prevent mode that is illustrated here, which makes it clear that most users should not browse the web at all -- it is too dangerous.

You also should mention some of the tools at grc.com.

Steve on June 18, 2007 7:50 AM

Thanks, excellent post. I'm gonna save a copy of this post as reference.

Fred on June 18, 2007 7:59 AM

This EXACT same thing happened to me even with what I thought was the latest of everything. The kicker was I didn't have my antivirus' active scanner running. I'll never do that again.

The funny thing is I never had trouble with GameCopyWorld before and now I go there and get popups and wierdness even through all of the protection.

Now I go there using Firefox with all of the scripting disabled. :) Moral of the story, use protection when venturing into possibly infected 'websites'.

Josh K. on June 18, 2007 8:00 AM

- 1) Always run as a Limited User.
- 2) Gaming, sports, gambling, music/lyrics, and porn sites can never be trusted.
- 3) If you need to go to the types of sites listed under #2 above, always do so using Virtual PC or VmWare and throw away any changes to the virtual hard disk when you are done.

4) Ignore the Linux and Mac trolls. Using tip #1 above levels the playing field. The Linux and Mac folks will have their comeuppance anyway on the day that people actually start USING those operating systems. ;)

Matt on June 18, 2007 8:12 AM

Couldn't you have just done a 'System Restore' instead of all that work?

Andrew Davey on June 18, 2007 8:14 AM

I won't get into the whole Mac-vs-Linux-vs-Win argument, we're talking about specialized software/hardware that only run on win. What the hell is wrong with IE that it installs software without user notification? The fact that this is the REQUIRED browser for federal employees should make all taxpayers very very nervous.

A virtual machine might be a good way to handle doing the regular restores of a stable base system every few months.

rev_matt_y on June 18, 2007 8:18 AM

Also it's a simple possibility to check what was changed in your system. Use a scan tool like systracer (<http://www.blueproject.ro/systracer>) from time to time, and see which files or registry entries are newly added.

steven on June 18, 2007 8:25 AM

ThanQ very much for this useful article.

Jonathan Orlev on June 18, 2007 8:46 AM

Heres how i clean a scumware laden windows install:

backup docs

format c:

Patch immediately

Install firefox and anti-spyware measures

create a ghost dvd

I used to have to clean this junk of computers daily... its just not worth the hassle if you have all the stuff you need to reinstall. No matter how deep you go, there is a chance you missed something that can bring it all back in no time. I say nuke it and start over.

forrest on June 18, 2007 8:46 AM

AVG Avast are two exceptional, FREE antivirus applications. I highly recommend either one to any person using an expired antivirus application.

For detecting malware, I recommend AVG Anti-spyware, A-squared Free, A-squared HiJackFree, HiJackThis, AdAware.

I also recommend using CrapCleaner to remove temporary data from your machine, like temporary files, browser data, etc. It also has a registry cleaner that is most exceptional.

yessir on June 18, 2007 8:58 AM

Great post! And the follow-up about root-kit monitor was important as well. This stuff can get really nasty- I've read an article where the author was able to hide malware in EEPROM chips on the motherboard or graphics card. It's designed to mimic most of the original functionality of the chip, but when the OS tries to load the driver the malware gets run instead. And, it could in some instances be run on the gpu. This means that even a complete re-format of the hard drive would not be enough to remove it.

Joel Coehoorn on June 18, 2007 9:02 AM

Although this is an interesting article, it in no way can deal with modern malware. Most modern malware incorporates kernel-mode rootkits, which can (and do) easily hide from tools like Rootkit Revealer. Your only chance is to detect them without booting the infected OS - you need a boot CD and knowledge about how things get hidden in the registry and file system. Some malware hides on the hard drive not in common files, but in alternate data streams, slack space, boot sectors, etc., and are not found by tools running in the OS itself. Someone mentioned Hacker Defender, which is an ancient rootkit, and easily detected/removed now. Source code is readily for HackerDefender and many other rootkits, and all of these are weak compared to modern standards.

It seems a lot of people on here think removing malware is easy to do by hand, which is false. It is easy to find **some** malware, and sometimes you can remove it by hand, but the point of a rootkit is that the OS will never tell you about the files, registry locations, etc. that contain the malware.

System Restore does not remove malware, since it does not fix the registry back to a previous state, nor does it remove files that contain malware. It merely tries to restore driver settings AFAIK, and things in start locations in the registry will reinstall themselves.

Running in a VMWare session is also insecure. It is possible for malware to escape to the host system, as shown by research at IntelGuardians. In short, VMWare does host-guest communication through a channel they created, and reverse-engineers have shown how to subvert this to do malware transfer. I don't know if there are exploits in the wild yet, but you can bet there will be.

I'd be willing to bet that your article above only removed obvious, older, sloppy malware. There are

most likely things still on your PC that are hidden much better.

Protocol for many secure places is that once a machine has been exposed to possible infection, it gets wiped and rebuilt. Very secure places scrap the machine completely after any possible infection.

In short, if you got a modern infection, odds are that the above methods would not even detect it. Unfortunately in many cases you'll spend less time formatting and reinstalling your apps than trying to ferret out all the places things can hide.

For info, read www.rootkit.org.

Chris Lomont
www.lomont.org

Chris Lomont on June 18, 2007 9:11 AM

Links do not work for Sysinternals utils. Here are the correct ones (ddl)
Autoruns: <http://download.sysinternals.com/Files/Autoruns.zip>
Process Explorer: <http://www.sysinternals.com/Files/ProcessExplorerNt.zip>
Above links are for NT os, search softpedia for others.
Cheers.

Jaan on June 18, 2007 9:23 AM

David L: good idea. I should report GCW to google, as they are *clearly* hosting malware.

Chris: I hear what you're saying, but I don't like making decisions based on fear of undetectable unknowns. And for a standalone gaming rig, probably not worth it...

Jeff Atwood on June 18, 2007 9:30 AM

On an XP reload, NEVER connect to the 'net or surf without at A BARE MINIMUM turning the Windows Firewall on and applying ALL updates and patches.

<http://autopatcher.com> gets you all the post-SP2 patches in one download. Keep it around on CD or a thumb drive, and fully patch your stuff BEFORE connecting.

Also, for those of you who think Firefox = automatic security on XP, read this:
<http://www.firefoxmyths.com>

mechmike on June 18, 2007 9:49 AM

Wow, you can do all that, or you can just not use Windows and never have to deal with scumware again. The choice was pretty simple for me :)

Matt on June 18, 2007 9:55 AM

It's not even necessarily GCW's direct fault - a banner ad could've done it, or one of their mirrors could've been compromised. It seems kind of silly for such a popular site to deliberately push malware, although I guess NoCDs and trainers are in kind of a shady area.

Still their fault for not taking care of it even if it's not intentional, of course.

cdr on June 18, 2007 9:55 AM

Just had to say thank you very much for publishing this article. I'm a long time lurker, and I keep coming back here because with every single post I learn something.

DrHogie on June 18, 2007 10:13 AM

I am reposting the hook on qt3 with a link, hope you don't mind.

stroker on June 18, 2007 10:54 AM

I've had this very problem *tonight* - apart from this ddcaxy.dll thing you also had, I also had some wierd rootkit thing.

I've just spent the last 6 hours recovering the machine. I was going to use procps like you but couldn't find it so used the trial version of Kaspersky (www.kaspersky.com) instead. After many safe boots I managed to get rid of everything except for the damn rootkit which had winlogon hooked.

I eventually booted into the Recovery Console on the XP disk and just del'd the thing from the DOS prompt. Done.

Gotta recommend Kaspersky though:- looks like a nice solid, honest product that seems to do the job very well. I'll keep it around for the trial period and buy it if it works out.

But, #\$\$^^\$^~hell, 6 hours of lost time just because my son visited some kids gaming website? What sort of damn'd operating system is this pile of junk?

JM on June 18, 2007 10:55 AM

I don't get why people run windows. Its crap. Don't run it. You'll get screwed multiple times from multiple directions. The evidence is overwhelming. Just say no. Don't say nobody ever told you. You will eventually get hosed.

Separatist on June 18, 2007 11:07 AM

hey, great article, seems like finally i managed to remove one malware: apple's quicktime from autorun.

could not do it using msconfig even after disabling a specific service relevant to it.

yeah the only apple software on my precious pc (except for the safari beta which is utter crap and not because of the fonts) and this one has to be malware.

...don't tell me anything that will not let itself removed from startup using the normal msconfig practice isn't malware!!!

other than this, ive never had problems with virii or anything.

thanks again. i hope it will not come back.

cmon_ on June 18, 2007 11:11 AM

(just to be more clear, uninstallation of the crap (quicktime) is sadly not an option)

cmon_ on June 18, 2007 11:12 AM

"I don't get why people run windows. Its crap. Don't run it. You'll get screwed multiple times from multiple directions. The evidence is overwhelming. Just say no. Don't say nobody ever told you. You will eventually get hosed."

And before you get hosed, you just might see some network benefits from to sticking with the market leader.

Daniel Pritchett on June 18, 2007 11:26 AM

Excellent guide on how to fix a shafted machine, a while back I got infected by an IRC bot, thanks to a vulnerability in VNC, which took me ages to fix, going through similar processes to what you have detailed above.

Thankfully I traced their ip address and the IRC host, and had them taken down, but not before I'd pulled out an awful lot of my hair.

To those who keep recommending Linux/Macs, how many racing simulation games for this system do you think your beloved OS supports? Clearly a windows machine is the only thing that's going to do the job.

poots on June 18, 2007 11:45 AM

@cmon_

Are you talking about qttask.exe? If so, that can easily be disabled through QuickTime. If you're like me

and you don't like QuickTime then there's always QuickTimeAlternave (and RealAlternative). Those will let you play MOV and HDMOV files in Media Player Classic which I much prefer over QuickTime anyway, as well as have proper plugins/settings for your browser(s).

Domenic on June 18, 2007 11:46 AM

Instead of hunting nocd patches on lousy sites how about dumping your games into iso files and mount them with programs like daemon tools when you feel like sitting behind the wheel?

10 on June 18, 2007 11:49 AM

The first order of buisness, before killing a spyware process is to look where it is located and to erase it once the process is killed. this is an almost sure way to make sure it won't come back.

ShooshX on June 18, 2007 11:50 AM

A couple things to note, a very nice article. The only thing I would add would be IceSword, excellent program from finding "hidden" processes. The other thing to note is, regardless of the OS this can happen, the only reason it doesn't happen on other OS's, is simply market share. On top of that, this was a base install of a 5-6 year old OS, to expect it to preform fine is foolish, no patches were done on it. If this were a fully updated version of XP, running a virus scan, I think the results would be different. In fact, that would be a wonderful thing to try. If I had the time I may just do that.

Luke on June 18, 2007 11:53 AM

I LOVE YOU. i was near reformatting my computer becuase i could not do anything about it, no matter where i looked. And then luck had it that i saw your post on iGoogle. Thank YOU!!!!!!!!!!

Zach Al-Nasser on June 18, 2007 12:03 PM

cmon_:

I don't know what version you were trying to get rid of, but there's an option in quicktime's prefs to remove the autorun. ;)

Araemo on June 18, 2007 12:17 PM

NO, NO, NO!

Like the other rootkit people have mentioned - you CANNOT clean an infected system from within itself. If you've got a rootkit, you're *fucked*.

Rootkits load themselves into the kernel and *modify* it. Yes, simply they can just hide processes from task manager (though there are other ways of doing this). But there's no reason why, if a rootkit get onto your system before you start running process explorer or rootkit revealer, it couldn't hide itself from those either. Or even if it gets on after.

After you've been hit with any malware that's been able to run as administrator, you *cannot* trust anything that system tells your, or anything that any program that runs on that system tells you. You either need to go one level higher - to the hypervisor if it's a VM and fix from there, or you need to boot from known safe media (CD-ROM) and replace *all* files containing executable code - exes, dlls, etc... and start again from there.

Do not try to clean a system that's been infected from that same system. It's not worth it.

Save your data elsewhere (take off), wipe the system (nuke the site from orbit), and start again - it's the *only* way to be sure.

Adam on June 18, 2007 12:20 PM

ditch Windows and switch to Linux or Mac. problem solved
Of course if everyone did this, then it wouldn't be long before they had problems too

Red on June 18, 2007 12:23 PM

Thank you so much for this post. I call myselef an advanced user of Windows, I've been a coder for years and consider myself security-savvy... but a piece of spyware my 12 year old picked up recently has been driving me nuts. I've gone though these steps and still am fighting this thing. Reading this convinced me to rebuild the system and take any admin rights away from the li'l shaver.

To all of y'all who said to switch to Ubuntu or MacIntosh... yes, you are correct, you don't pick this crud up with those very fine OS's. I run them too, but our gaming system ... and also the .NET dev work I do gotta be Windows. Changing OS's is not like changing socks.

Nat on June 18, 2007 1:00 PM

Thanks for posting this great stuff.

How do I handle the situation when two processes or DLLs, A and B, keep monitoring when the other is killed and re-creating/re-launching each other? I can't kill them both simultaneously .. or can I?

Gregory on June 18, 2007 1:03 PM

This kind of stuff drove me to mac.

D on June 18, 2007 1:07 PM

Hi Jeff, why is "Company Name" such a good indicator of a product's spamminess? Can't spyware makers just put "Microsoft Corp" into those fields?

(The only Windows application development I've done has been in IIS, so I'm pretty ignorant.)

jacob on June 18, 2007 1:08 PM

Wish I had known about all this back when I got nailed a year ago. Took me a week to get everything sufficiently scrubbed.

Question about relying on the "missing publisher" to identify malicious processes. Isn't it possible for these processes to just give themselves an identity of "Microsoft Corporation" or something?

Mark on June 18, 2007 1:14 PM

Jeff,

Another free program that's worth a mention: Spyware Terminator.

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

It will effectively remove spyware, adware, trojans, keyloggers, home page hijackers and other malware threats. It is easy to use, requires minimal PC resources and has ultra fast scanning speed.

David Brabant on June 18, 2007 1:17 PM

Yes, you all are correct on saying that the only way to make sure all spyware/whatever is gone is to reformat. But, some nicely written malware requires a low-level format, or use of Dban. I like the scope of this article and what it covered, it did an excellent job of providing an alternative to reformatting.

Luke on June 18, 2007 1:21 PM

I'll reiterate the best piece of advice given thus far: format and reinstall. Its the only way to know.

Dave on June 18, 2007 1:23 PM

@Separatist:

I run windows because I have a large number of programs that are windows only. I'd rather not mess with incomplete interpreters (WINE) and the like.

If I could run these programs outside of windows, then I would switch. I really don't like the look and feel of MacOS. So, that switch would probably be to a popular Linux Distro.

@Jeff:

Nice article. I will definitely look into those tools. I usually reformat a computer that I find to be riddle with malware (and may continue to do so), but those tools could really help if reformat is not available.

Sean on June 18, 2007 1:28 PM

Fantastic post Jeff!

Mike on June 18, 2007 1:33 PM

It's just outrageous that Microsoft's OS/browser security was so terrible for so long. I guess they've gotten their act together with Vista, but the internet will remain polluted with botnets and malware for years to come.

Jeff, just curious, have you ever used OS X or Linux enough to really get a sense of them? Would you ever switch if you weren't a Windows Developer?

BTW, I met Woody Pewitt of Microsoft at a Rails Meetup and he had a huge Coding Horror sticker on his laptop :)

Nathan Bowers on June 18, 2007 1:34 PM

Jeff,

2 quick notes, as obvious as this may sound, login on to safe mode would've helped you get rid of most of those process with a simple registry edit, and running ad-aware /Spybot

secondly, you could've simply used a live cd to get rid of the infected files, I've had to do that to remove a rootkit.

Gotta love Linux Live CDs

Eilrama on June 18, 2007 1:38 PM

As someone who is a contractor in a large company (hence no admin access), can I say this article was a life-saver!

I got infected by spyware somehow (I haven't done anything dodgy, but it must have got in some how) and was dreading calling IT to ask them to log in as an administrator so I could run spybot as admin.

This article helped me whack the files myself!

You can't imagine how grateful I am!

Anonymous (for good reason) on June 18, 2007 1:42 PM

What are the results if you're not running as administrator?

Trying it in the VM now. So far so good. I don't see any change in Task Manager with multiple GCW browser windows open.

I agree this is a logical thing to do, but not on a dedicated gaming system.

I lost my enthusiasm for limited user accounts when Microsoft didn't have the guts to make standard users (instead of administrators) the default-- as they absolutely should have-- in Windows Vista. I swore they would. Instead we got hybrid administrator weirdness and the "Cancel or Allow". Sigh. I guess that's another thing we can sacrifice at the altar of backwards compatibility.

Jeff Atwood on June 18, 2007 1:51 PM

Jeff,

As interesting and complete as this was, isn't it an awfully lot like Mark Russinovich's presentation entitled: "Enterprise Malware Solutions"?

Considering your background, I'd be willing to accept that you came to the same conclusion independently. However, if that presentation was your source, you should really give credit where it's due.

Long-time reader, first-time commenter,

-Jeff

Jeff on June 18, 2007 1:54 PM

As interesting and complete as this was, isn't it an awfully lot like Mark Russinovich's presentation entitled: "Enterprise Malware Solutions"?

I've never seen this presentation. But any comparison between me and Mark Russinovich is a tremendous compliment. Mark is the real deal; without his tools, none of this would be possible.

I have the utmost respect for Mark and you can rest assured I'd never copy his work. What I did, I did on my own with a few Google searches.. and I posted it largely because the Google results weren't very good, and I felt I could provide a better resource for the next poor souls to have the same problem I did.

Plus, have you *met* Mark Russinovich? He's like 6 foot 3 and literally could be a male model. Between his encyclopedic, world-renowned guru-level knowledge of every part of Windows, and his unnatural good looks, he makes the rest of us geeks look like.. well, the geeks that we are. :) He's a fantastically nice guy, too.

Jeff Atwood on June 19, 2007 2:01 AM

Great article, and great explanations. Of course there is no perfect place ! If you like other operating systems, good for you I say. I have run everything over the past 30 years, nothing compares with Windows, nothing. All one has to do is look at the take up rate of Windows and it's easy to see that it is the easiest and most popular, and as a result the best target for the pirates to attack, as they are likely to get a return on their investment....and they do, because it all comes down to the user and their inability to detect and defend against them. The average user is not very knowledgeable about computers and just wants to download or buy something, and they get caught. Articles like this will help those people a little more each time and by the time the next generation comes along, they will begin to win against the pirates. Nothing is easy or free !

Kingsmeadow on June 19, 2007 2:20 AM

[More comments»](#)

Post a comment

To comment, please [sign in](#) using TypePad, Twitter, Facebook or OpenID.