WinPatrol

By Russ McRee – ISSA member, Puget Sound (Seattle), WA, USA chapter

Prerequisites

Windows 98/2000/XP/Vista 32 & 64 bit

Similar Projects

ESET SysInspector beta[1]
Sysinternals Process Monitor and Process Explorer[2]

There are those occasions when one takes certain tools that they have always used for granted. Such is the case for me and WinPatrol.[3] I shall now make amends. I have long used Bill Pytlovany's tool for both an added layer of personal awareness and as a first layer of behavior analysis in my virtual machine malware testing sandboxes. Because, with remarkable ease of installation and use, it just works, there is not necessarily a great deal of deeply technical guidance to provide regarding WinPatrol.

Given some of the rabbit holes we have gone down in previous months' columns, not doing so here may come as some relief. We can instead revel in the fundamental pleasure of a tool that is easy to use and of great benefit. Quite simply, WinPatrol is one of those tools that everyone running a Windows operating system should use. There is a free version that functions fully and provides ample host monitoring, but those choosing to do so can purchase an enhanced version for a reasonable fee. As *toolsmith's* mission is the discussion of freely available and/or open source tools, I only tested the free version for this month's column; but should you choose to upgrade, you will have access to the WinPatrol PLUS Knowledgebase, real-time infiltration detection, and the detection of newly created undocumented or hidden registry startup keys.

Further, you will be supporting future WinPatrol development and anti-malware research.

Aside from my firm belief that there is no reason not to run WinPatrol, I can, with great pleasure, say that Bill Pytlovany has long been one of the rare few developers who flatly refuses to bundle any sort of unwanted software with his free offering in order to drive revenue. I feel this is so significant that I can not help but share a bit of that discussion. Thanks to Alex Eckelberry of Sunbelt for pointing this out.

Bill said "I crunched the numbers and sure enough the revenue I could receive by including the toolbar would be huge. My overhead is low and the free version of WinPatrol has many thousand downloads even on the slowest day. If I chose to include the Ask.com tool bar I could probably retire comfortably by the end of the year. Unfortunately, a number of people think I'm a really good guy and I respect their opinion. For the last ten years WinPatrol has had a flawless reputation. I know myself, I really hate companies that install additional software that I didn't ask for. It's not only rude, it's just wrong."[4]

It is rare that a lasting integrity, born of a belief that reputation is inherent to a good product, can be discussed with confidence regarding a tool like WinPatrol. Alas, these views are born only of personal opinion and experience with the tool, but I can not help but pull for a good guy and good offering.

Installation

Installation is as simple as downloading `wpsetup.exe` and following the default installer process.

Usage

Normal running system

WinPatrol will drop Scotty in your *systray* and run on startup by default. You will note a small black dog in a blue transparent bubble; that is Scotty and he is on patrol. He even barks when some overreaching or busy software is trying to make changes on your system. I know, I know, we are big, bad security professionals, and a corny little barking dog on your system is not exactly cool, but the alternative is much worse. In testing a variety of AV solutions, I have had Scotty give me an immediate heads up, while any number of antivirus products sat there with that dull, blank non-reaction we all know and love, as this bot and that Trojan happily polluted my sandbox. It is the simple things.

The version I tested – 14.0.2007.1 – now offers enhanced keystroke logger protections in addition to all its other long-standing functionality. Bill feels strongly about this issue as well, noting that "use of key logger spyware is despicable." Please refer to his blog[5] for more.

1 http://www.eset.com/esibeta

2 http://technet.microsoft.com/en-us/sysinternals/default.aspx

3 http://winpatrol.com

4 http://billpstudios.blogspot.com/2008/01/would-you-like-toolbar-with-your.html

5 http://billpstudios.blogspot.com/2008/01/winpatrol-14-enhances-keylogging.html

Double clicking Scotty will pull up a simple tabbed interface that will give you ample information regarding your system's current state, including *Startup Programs, Delayed Start, IE Helpers, Scheduled Tasks, Services, Active Tasks, Cookies, File Types, Hidden Files, Options,* and *Plus*, should you choose to upgrade.

The benefit of all these features in a single view is obvious as opposed to pulling up `services.msc`, `regedit.exe`, *msconfig*, and *Scheduled Tasks* individually.

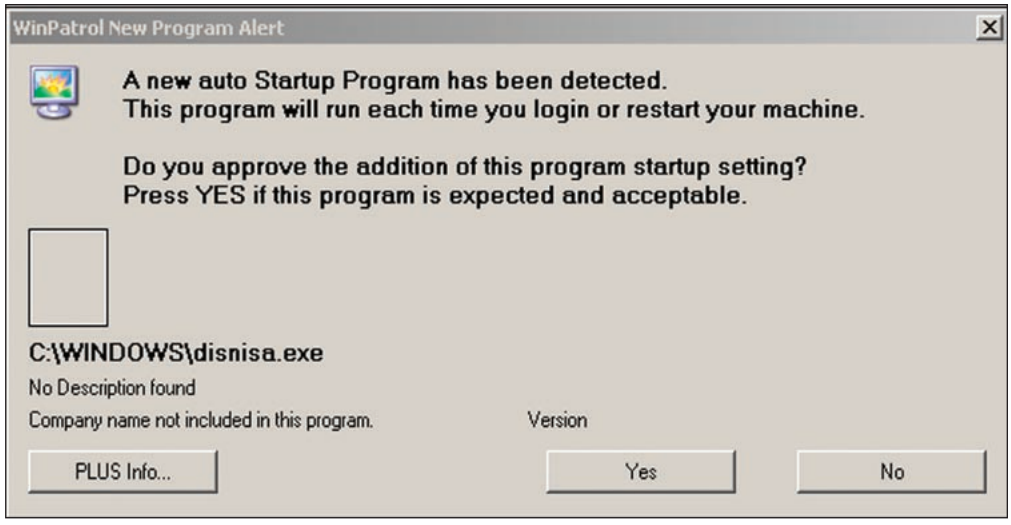

Figure 1 – WinPatrol New Program Alert

Startup Programs discloses the obvious; but when bad juju attempts to sneak on your system, one of the first things it will likely do is stick itself in the registry under HKLM_RUN or HKCU_RUN. WinPatrol will enumerate all existing entries and monitor for changes going forward. Hidden Files are an added bonus, as the sneaky, rat #$#%@^&s writing malware will likely try to avoid the obvious, and hide from visible APIs. WinPatrol will immediately reveal all legitimate hidden files, but you may well see something that does not belong there and have the option to attempt to delete it right from the WinPatrol GUI.

The other place malware sometimes likes to show itself is as a service. WinPatrol will neatly summarize all running services in the Services tab, and offer the company responsible for its creation in your immediate view. Thus, if you see an oddly named or uncommon service with no associated company name, you may have an issue. Active Tasks will show you running processes, like an improved version of Task Manager. We will run through some of these use scenarios in more detail in the next section.

For the performance conscious, Delayed Start will "greatly improve your system startup time. There may be some programs which you do want to keep running but do not need to launch immediately on boot up. Delayed Startup allows you to specify the time to wait before launching programs which may typically run instantly when you boot, slowing down initialization."[6]

If you like the idea of easily managing cookies as part of your privacy practices, WinPatrol's Cookies tab offers you the option to keep only the cookies that you find useful and remove the ones you do not. You will see what cookies are being stored by your browser and easily review their contents. You can then determine where those cookies came from and what data is being stored about you. Scotty will step right up and remove the cookies you do not want. You can even use the cookie filter list to specify a list of cookies that you would prefer to remove automatically, without any further interaction. This feature makes it easy to manage your browser's cookies by designating cookie names you know you will never want.[7] File Types will monitor for file association changes and IE Helpers will keep an eye on unwanted browser helper objects.

Malware infected system

When I am investigating malware behavior, I always have Scotty on guard. For this exercise I used one of the many Storm-distributed binaries, in particular, one of the Happy New Year 2008 ecards. While pretending I was one of the kabillions of victims of these social engineering ploys, I promptly infected myself with `happy2008.exe`, which copies itself to C:\WINDOWS as `disnisa.exe`. I know this because Scotty said so – Figure 1.

Once prompted, the wise user would obviously choose *No*, but as I intended to prove value in our experiment, I selected *Yes*.

Soon thereafter, I took a look in WinPatrol's Active Tasks tab. Uh-oh, there is `disnisa.exe` – Figure 2.

You can use *Kill Tas*k in this view to stop any questionable processes.

A quick look in Startup Programs also reveals `disnisa.exe`, and again you can opt to remove or disable any unwanted startup programs in this view – Figure 3.

You can quickly see where WinPatrol is not only of benefit for user protection, but also for study and analysis.

Benefits and drawbacks

WinPatrol is easy to install, easy to use, and always looking out for your best interests. Again, if you are running Windows, put Scotty the Windows Watchdog to good use. There are no drawbacks to using WinPatrol, unless you prefer to avoid knowing what kind of evil may come your way.

6 http://www.winpatrol.com/support/delay.html

7 http://www.winpatrol.com/support/cookies.html

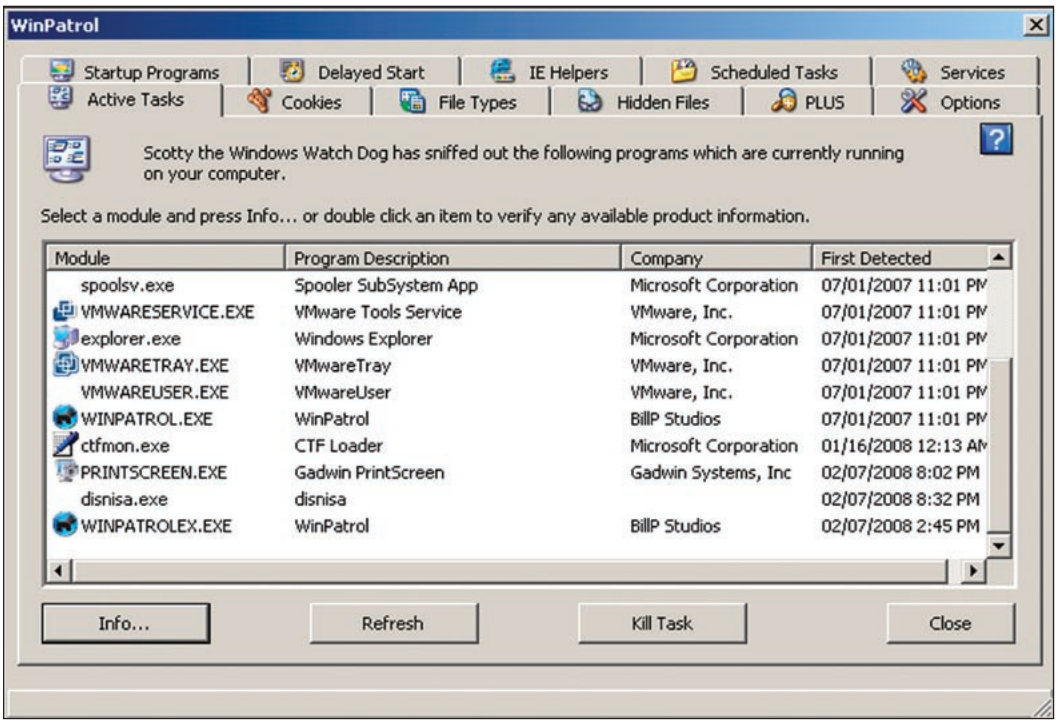

Figure 2 – Scotty spots a bad running process

In conclusion

In reaching out to Bill to discuss WinPatrol, he was kind and timely with his responses. It occurred to me from my notes that the following excerpt might best summarize what WinPatrol is really all about.

"One of the primary motivations behind WinPatrol is to make it a program that I would use myself. That means it must be robust enough not to interfere with what I'm doing. To maintain performance I've focused more on detection than on analyzing what might be happening. It's a trade off but has paid off. My best example is when MSBlaster was introduced through a hole in Windows. Out of the blue, WinPatrol users got an alert letting them know something had been installed on their system. It took a few days before I could tell users what MSBlaster was and how it worked, but WinPatrol users knew immediately it wasn't something they wanted and were able to remove it. During the first days of distribution any of the programs that used signature files were useless."

Any questions? ;-)

Use WinPatrol in good stead, knowing Scotty's got your back. Cheers, until next month.

Acknowledgments

Bill Pytlovany, for his years of hard work and dedication. Alex Eckelberry, for reminding me to not take the simple pleasures for granted.

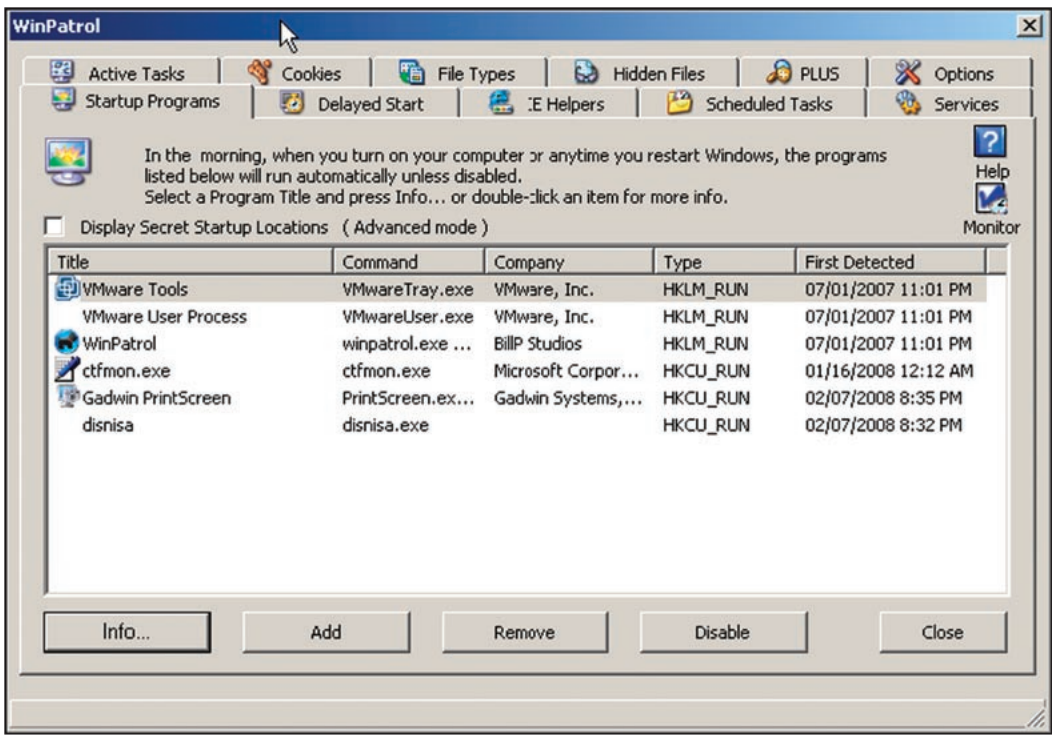

Figure 3 – Remove or disable unwanted startup programs

About the Author

Russ McRee, GCIH, GCFA, CISSP, is a security analyst working in the Seattle area. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ@holisticinfosec.org.