The NirSoft Collection

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

Join the Discussion
Connect

Prerequisites

NirSoft

Windows OS

Virtualized or disposable Windows instance for testing

I'm writing part of this on the plane flying back from the ISSA International Conference, having presented "Incident Response in Increasingly Complex Environments." First, the conference was an unbridled success; hats off to Kate Kapeneaux and team for putting together a great event. Additionally, it was a privilege to present for and meet those of you who attended in Atlanta.

Discussing the likes of incident response and malware analysis always leads to me to thinking about the number of tools I have yet to discuss as toolsmith topics. Some of the NirSoft[1] utilities have been on that list for quite a while. I was reminded of the fact that I've been negligent in discussing them when one of my analysts broke out CurrPorts to find a fake malicious process I'd seeded on a server as part of PCI DSS-related incident response drill. We conduct such drills quarterly; they keep your teams tight and practiced, and they make auditors really happy. Ping me for feedback if you'd like to discuss suggested methodology.

NirSoft offers many tools, not all serve security practitioners in any particular fashion, but there is a select list that is quite useful. I would describe these utilities as most useful for a jump kit or dedicated malware analysis workstation. When you need to deploy quickly, consider pre-staging some of these utilities on a tools server for remote response, or on portable media for those of you who conduct more onsite incident response.

I'm in the midst of defining a package of all the tools I recommend for these occasions, based on *toolsmith* research and real-world use – the "can't live without" list, if you will. I really don't want to maintain a LiveCD/USB or the like, but a package list, along with pointers for use is long overdue...stay tuned. These NirSoft utilities will definitely be part of the recommended jump kit list.

That said, for this month, we'll discuss CurrPorts with IPNetInfo, OpenedFilesView, WhatInStartup, and a few possible uses for NirCmd.

1 http://www.nirsoft.net.

I used a variety of malware samples to create scenarios for testing these utilities, all of which are part of a sample collection (MalCol[2]) mentioned on OffensiveComputing.net. As always, I'd be negligent if I didn't say, this is a significant collection of malware samples; exercise extreme caution and analyze only in a controlled lab environment.

One attribute specific to these NirSoft utilities is that they don't need to be installed (just run them), they have no dependencies that aren't typical to most Windows systems, and x64 support is available as well.

Also note that NirSoft utilities are included in the "Windows side" of the Helix distribution in the \IR\nirsoft directory, including various password and browser-specific tools.

CurrPorts with IPNetInfo

You can certainly use CurrPorts by itself, but when configured to work with IPNetInfo, you gain additionally useful information regarding destination IP addresses.

To learn more about the remote IP address displayed in CurrPorts, you can utilize IPNetInfo as follows to easily view IP address information via WHOIS:

- Run the latest version of IPNetInfo utility.
- Select the desired connections, and then choose "IPNetInfo" from the File menu (or click Ctrl+I).
- IPNetInfo will retrieve information about remote IP addresses of the selected connections.

Before I infected my virtual machine with `Backdoor.Win32.Agent.adqt` (MD5: 6DBA44B457414593A858A3520A2F2278), I took a screenshot of CurrPorts running on the system to exemplify a baseline (Figure 1). The baseline step is always useful when conducting malware analysis in isolation, but may not serve you all that well when you're responding to a system that has already been infected. That said, CurrPorts will likely present you with fairly obvious suspicious processes.

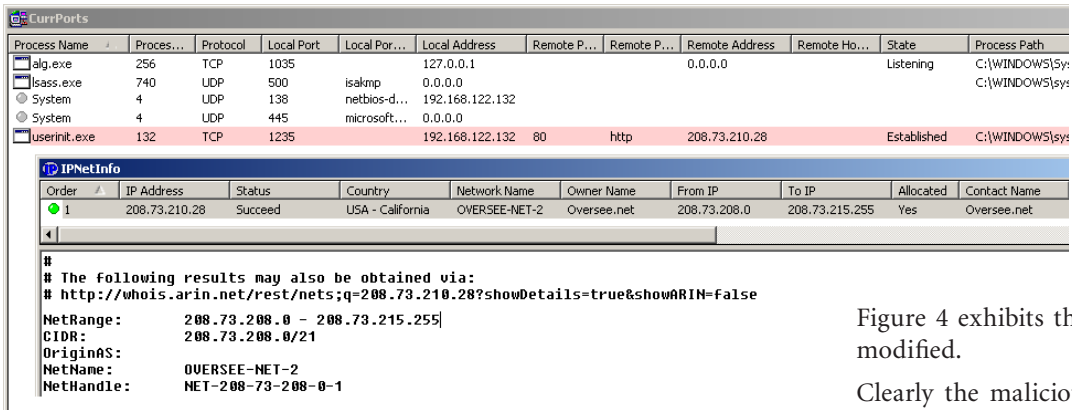
2 http://rapidshare.com/files/397723192/MalCol.rar.

CurrPorts

Process Name	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote P...	Remote P...	Remote Address	Remote Ho...	State	Process Path
alg.exe	256	TCP	1035		127.0.0.1			0.0.0.0		Listening	C:\WINDOWS\System
lsass.exe	740	UDP	500	isakmp	0.0.0.0						C:\WINDOWS\system
lsass.exe	740	UDP	4500		0.0.0.0						C:\WINDOWS\system
svchost.exe	996	TCP	135	epmap	0.0.0.0			0.0.0.0		Listening	C:\WINDOWS\system
svchost.exe	1092	UDP	123	ntp	192.168.122.132						C:\WINDOWS\system
svchost.exe	1092	UDP	123	ntp	127.0.0.1						C:\WINDOWS\system
svchost.exe	1252	UDP	1900		192.168.122.132						C:\WINDOWS\system
svchost.exe	1252	UDP	1900		127.0.0.1						C:\WINDOWS\system
System	4	TCP	445	microsoft...	0.0.0.0			0.0.0.0		Listening	
System	4	TCP	139	netbios-ssn	192.168.122.132			0.0.0.0		Listening	
System	4	UDP	137	netbios-ns	192.168.122.132						
System	4	UDP	138	netbios-d...	192.168.122.132						
System	4	UDP	445	microsoft...	0.0.0.0						

Figure 1 – CurrPorts baseline pre-infection

Figure 2 – CurrPorts and IPNetInfo after infection



After executing the malicious binary, CurrPorts immediately presented conclusive evidence of the process and connection spawned (Figure 2). First, `userinit.exe` was written to `C:\WINDOWS\system32`. The `userinit.exe` process then made an immediate connection to 208.73.210.28; a right-click with IPNetInfo selected resulted in all the details needed to identify and mitigate the problematic system compromise.

A little Internet research on the hash reveals ThreatExpert feedback,[3] and the IP address has definitely been tagged as a "bad host" by project Honey Pot.[4]

You can take additional action via CurrPorts. If you wish to *Close Selected TCP Connections* or *Kill Processes Of Selected Ports*, again, a simple right-click and select is all you need. As is consistent with NirSoft utilities you can opt to create an HTML report of either the selected process or all items visible to the CurrPorts UI.

OpenedFilesView

The OpenedFilesView UI is a bit busier than CurrPorts and will be useful to those of you who know what to expect in the way of open or locked files on a given Windows system.

As done with CurrPorts, I snapped a baseline view of my lab virtual machine (see Figure 3). OpenedFilesView is best sorted by Created Time or Modified Time as this will alert you to system changes as they occur.

Sticking solely with MAC-times analysis we see that only four files have been modified as of 9/26/10. I then executed `Backdoor.Win32.Poison.apec`[5] (MD5: CB702C3319A27E792B84846D3D6C61AD).

Figure 4 exhibits the resulting opened files as modified.

Clearly the malicious binary has invoked Internet Explorer as we see changes to `index.dat`. A quick review of C:\Documents and Settings\...\Cookies\ shows two cookies written to the system dated 9/26/10 for globo.com. Again, a bit of search engine research via site:threatexpert.com globo.com will reveal endless hits on various malicious behavior associated with globo.com, with particular emphasis on Brazilian malware.

WhatInStartup

This utility really couldn't be more simple but is ideal for both live incident response and malware analysis as malicious processes often set themselves up to load automatically when Windows starts.

Figure 5 shows a startup files baseline for my malware analysis VM.

I chose a rogue AV sample to make use of WhatInStartup; specifically, `Trojan.Win32.FraudPack.amgz` (MD5: 59C0E80D7F9705D10DA91E01B2763E9A[6]).

Once executed SE2010 wrote and entry to `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`.

Security Essentials 2010 is classic rogue AV. Pervasive, annoying, and fraudulent, it will not leave you alone once installed. Send us your credit card number immediately to license your version of Security Essentials 2010 so we can clean your system right away! Um, yeah, no thanks.

3 http://www.threatexpert.com/report.aspx?md5=6dba44b457414593a858a3520a2f2278.

4 http://www.projecthoneypot.org/ip_208.73.210.28.

5 http://www.threatexpert.com/report.aspx?md5=cb702c3319a27e792b84846d3d6c61ad.

6 http://www.virustotal.com/file-scan/report.html?id=15b579f79e9f0a7b31fc1b5e6cff38b8c490612c7c16eebae9252b1b98dfd6a5-1271766329.

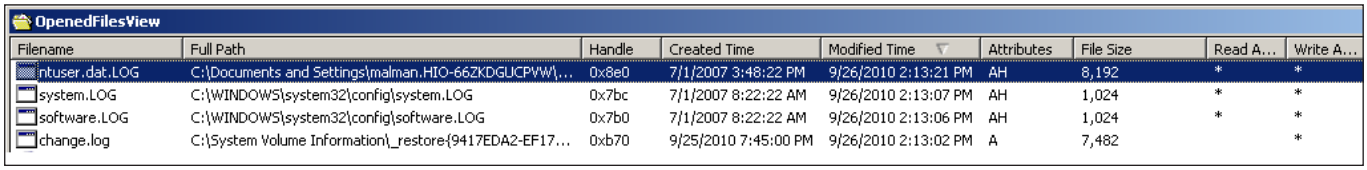


Figure 3 – OpenedFilesView pre-infection

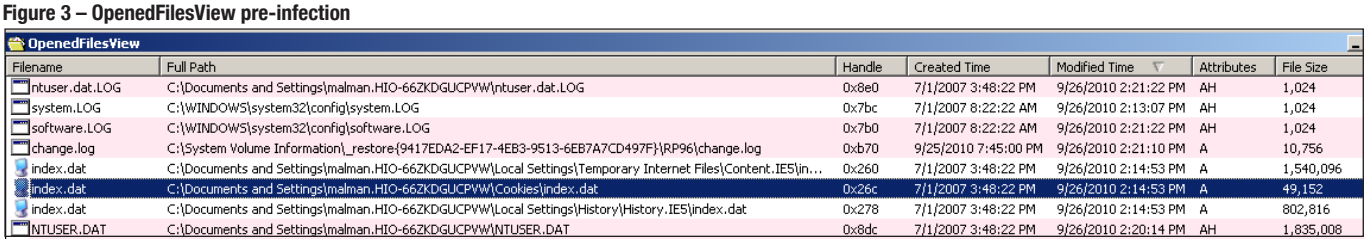
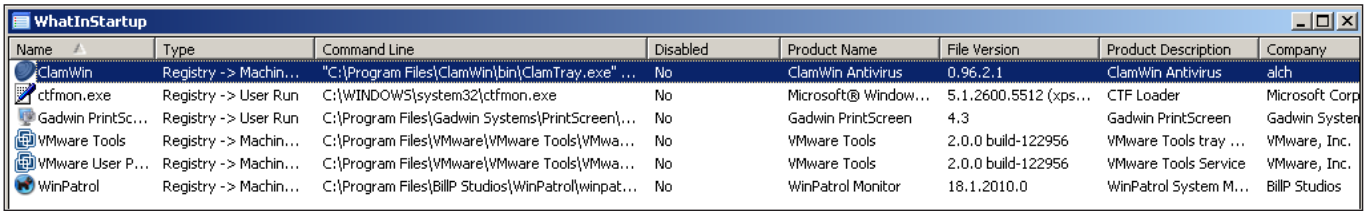


Figure 4 – OpenedFilesView after Win32.Poison infection

Figure 5 – WhatInStartup before infection



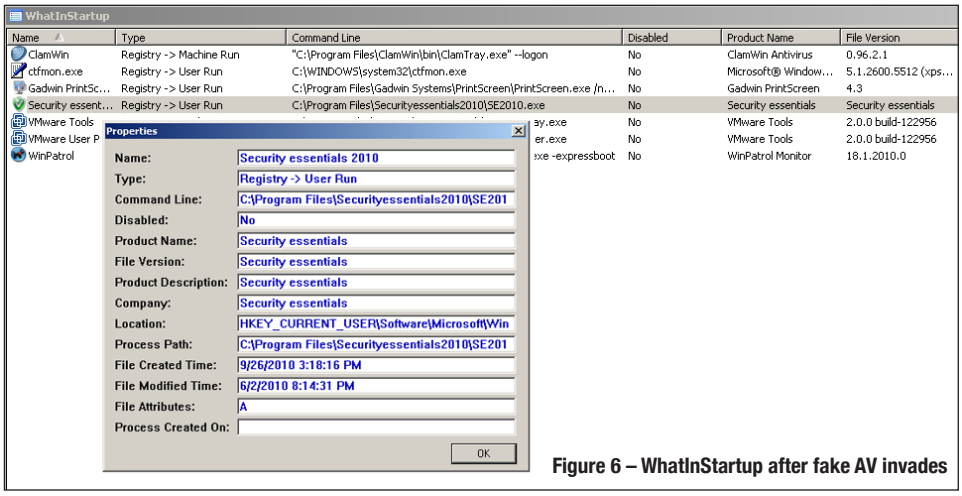


Figure 6 – WhatInStartup after fake AV invades

Figure 7 cracks me up: Critical Vulnerables Found! OMG!

You can disable or delete selected startup items via right-click context menu choices and pull reports for items of interest as with all other NirSoft utilities.

NirCmd

Finally, NirCmd is more of a general utility than a security-centric tool, but you may find it useful for any number of scenarios.

As an incident responder attending to a compromised system, you may find said system in an unstable state where `explorer.exe` may be hung or altogether useless if malware-mangled. If you can execute CTRL-ALT-DEL you can opt to use NirCmd from the run option via Task Manager.

`Executing`

`nircmd.exe regedit "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run"` will pull up regedit and point you to whatever evil may have been written as a value.

Perhaps you wish to kill the process that you noted as set to initialize on Windows startup as seen in the above mentioned registry key.

As an arbitrary reference, `nircmd.exe killprocess malware.exe` will shut down the process you choose to kill.

Maybe there's a critical service installed on the system under investigation such as an antivirus or HIDS service that has been stopped by a malicious process. Assuming said service has not been circumvented, you could opt to run nircmd service `start|stop|restart YourService`.

You'll find that you can do a few more things with NirCmd than indicated in the help menu; experiment to find additionally useful capabilities. Multiple clipboard options are at your beck and call for dumping content to text files or reading in file and folder paths.

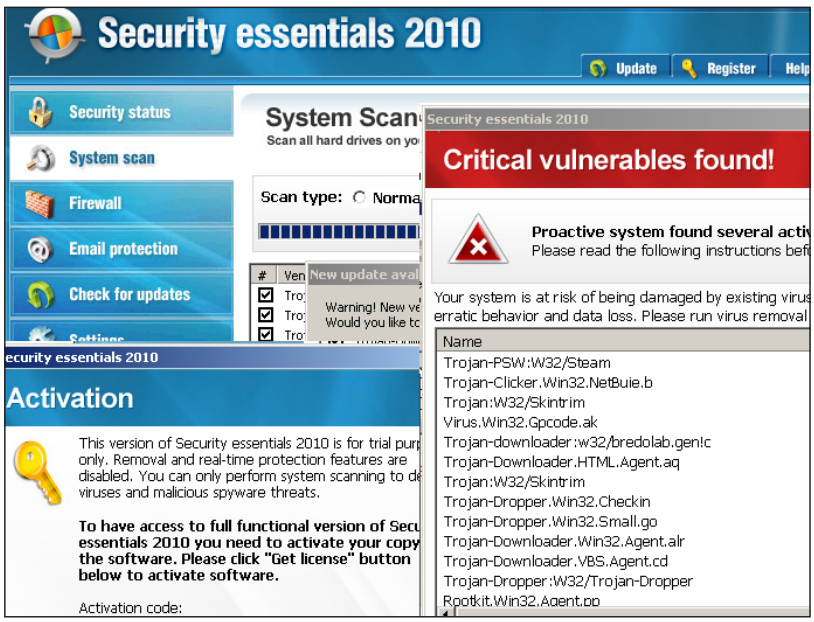


Figure 7 – Critical Vulnerables Found!

In conclusion

The NirSoft collection is obviously really useful: light, quick, easy to use and interpret. Stick these utilities on a USB stick, burn them to a CD, or populate them to a directory on your incident response server or malware analysis workstation; they'll be useful no matter how you choose to use them.

Cheers…until next month.

About the Author

Russ McRee, GCIH, GCFA, GPEN, CISSP, is team leader and senior security analyst for Microsoft's Online Services Security Incident Management team. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ@holisticinfosec.org.