Week 8: Using Forensic tools

> Author: Nguyen Anh Khoa
>
> Instructor: Dang Dinh Phuong

Update 1: 29 July 2019, add PCHunter and PowerTool. I tried to run a demo of HideToolZ but to no avail, the driver cannot be loaded so it fail hiding the process.

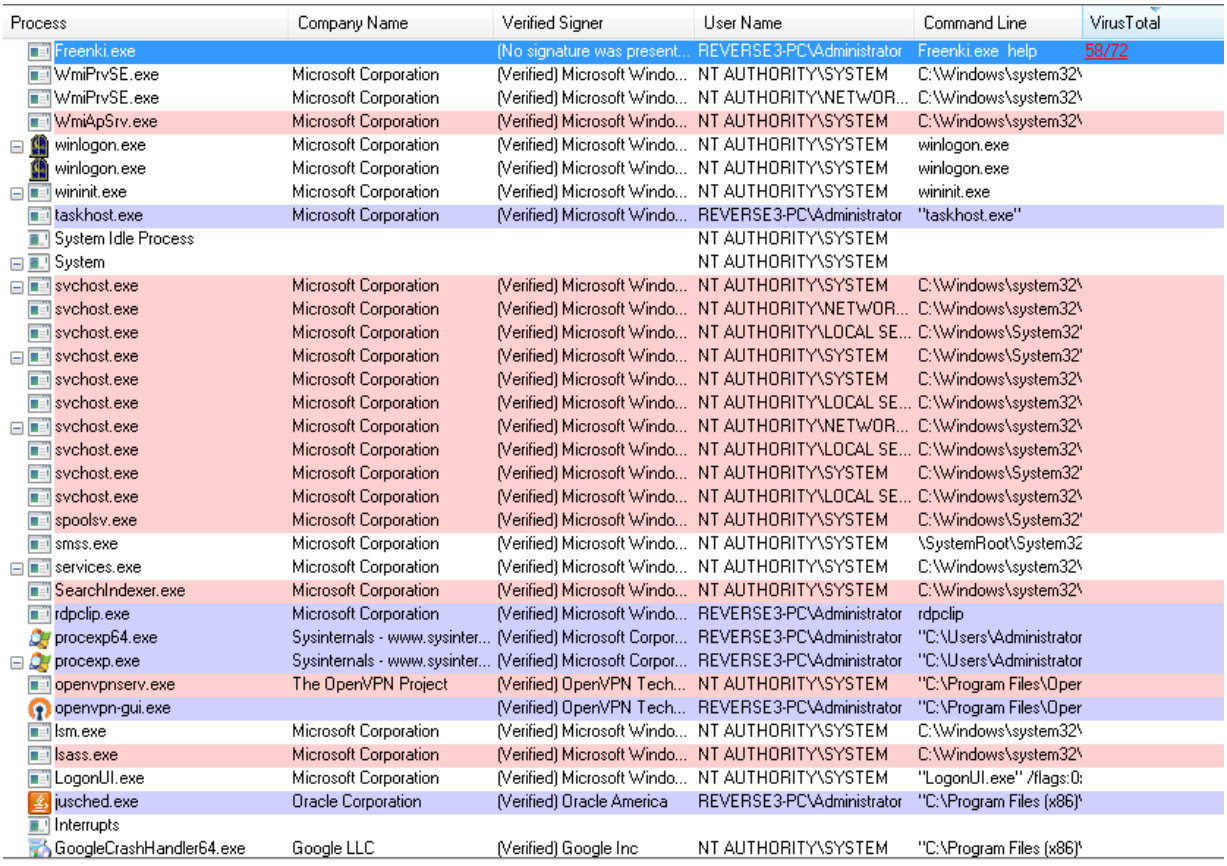
In this last week of internship, I learned about using tools to inspect, find, and removing malware. The suit of programs mostly are from SysInternal, and can be downloaded online for free on microsoft.

Process Explorer

> Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

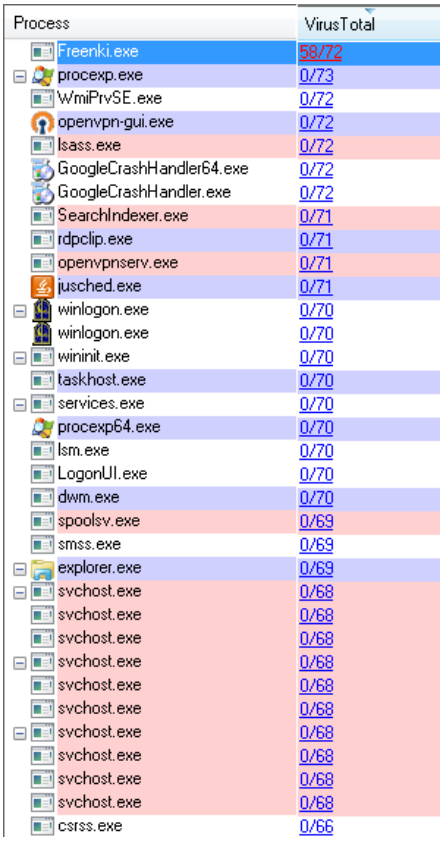
This program lists process running and updates every interval (1s, 5s, ...). Using this program, we can find processes running on our system, checking the verification of the process. If a process is not signed, it could be a warning. The interface is simple, we have processes listed as tree on the left, clicking on one of them will provide details in the box below. To the right of the process's name are information to that process. We can see the PID, Description, Verified Signer, User Name invoke the process, Command Line given to it when run, and network in out.

Right-clicking on a process will provide us many options like kill, restart, and suspend. We can create a dump of a process by using `Create Dump` option, which then ask for a minidump or a fulldump, these will come in handy when we need to inspect the process memory. We can `Debug` the process, which will open a windows for us to choose debugger, Visual Studio, or manually choose the debugging engines. And we can also check virus total for the file of the process. Process explorer will send the file hash to the server, if it is a known malware, the result will be like below.



Process	Company Name	Verified Signer	User Name	Command Line	VirusTotal
Freenki.exe		(No signature was present...	REVERSE3-PC\Administrator	Freenki.exe help	58/72
WmiPrvSE.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	C:\Windows\system32\	
WmiPrvSE.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\NETWOR...	C:\Windows\system32\	
WmiApSrv.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	C:\Windows\system32\	
winlogon.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	winlogon.exe	
winlogon.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	winlogon.exe	
wininit.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	wininit.exe	
taskhost.exe	Microsoft Corporation	(Verified) Microsoft Windo...	REVERSE3-PC\Administrator	"taskhost.exe"	
System Idle Process			NT AUTHORITY\SYSTEM		
System			NT AUTHORITY\SYSTEM		
svchost.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	C:\Windows\system32\	
svchost.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\NETWOR...	C:\Windows\system32\	
svchost.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\LOCAL SE...	C:\Windows\System32'	
svchost.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	C:\Windows\System32'	
svchost.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	C:\Windows\system32\	
svchost.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\LOCAL SE...	C:\Windows\system32\	
svchost.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\NETWOR...	C:\Windows\system32\	
svchost.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\LOCAL SE...	C:\Windows\system32\	
svchost.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	C:\Windows\System32'	
svchost.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\LOCAL SE...	C:\Windows\system32\	
spoolsv.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	C:\Windows\System32'	
smss.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	\SystemRoot\System32	
services.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	C:\Windows\system32\	
SearchIndexer.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	C:\Windows\system32\	
rdpclip.exe	Microsoft Corporation	(Verified) Microsoft Windo...	REVERSE3-PC\Administrator	rdpclip	
procexp64.exe	Sysinternals - www.sysinter...	(Verified) Microsoft Corpor...	REVERSE3-PC\Administrator	"C:\Users\Administrator	
procexp.exe	Sysinternals - www.sysinter...	(Verified) Microsoft Corpor...	REVERSE3-PC\Administrator	"C:\Users\Administrator	
openvpnserv.exe	The OpenVPN Project	(Verified) OpenVPN Tech...	NT AUTHORITY\SYSTEM	"C:\Program Files\Oper	
openvpn-gui.exe		(Verified) OpenVPN Tech...	REVERSE3-PC\Administrator	"C:\Program Files\Oper	
lsm.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	C:\Windows\system32\	
lsass.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	C:\Windows\system32\	
LogonUI.exe	Microsoft Corporation	(Verified) Microsoft Windo...	NT AUTHORITY\SYSTEM	"LogonUI.exe" /flags:0:	
jusched.exe	Oracle Corporation	(Verified) Oracle America	REVERSE3-PC\Administrator	"C:\Program Files (x86)\	
Interrupts					
GoogleCrashHandler64.exe	Google LLC	(Verified) Google Inc	NT AUTHORITY\SYSTEM	"C:\Program Files (x86)\	

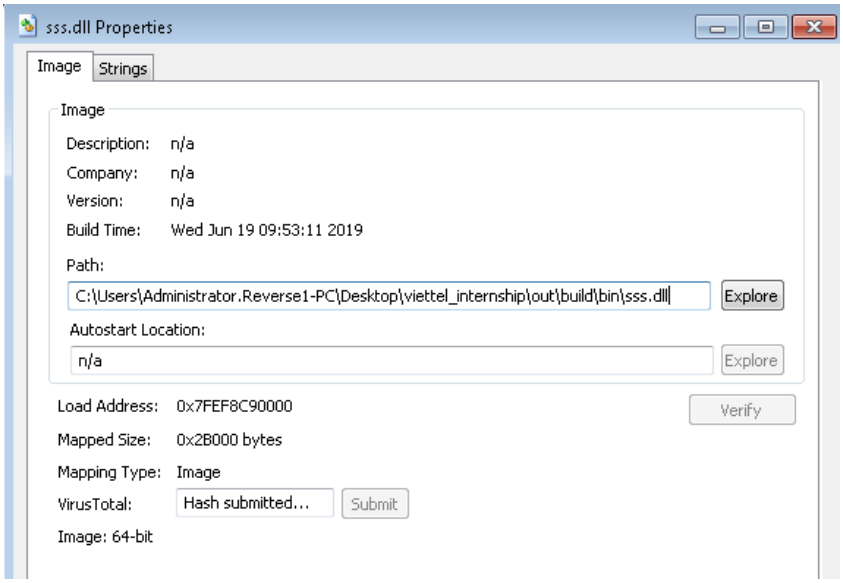
We can see that Freenki.exe does not have a valid signature, and Virus Total check shows a 58/72 virus engines detecting the malware. If we click `Options -> VirusTotal.com -> Check VirusTotal.com` it will send all running process to VirusTotal. The result:

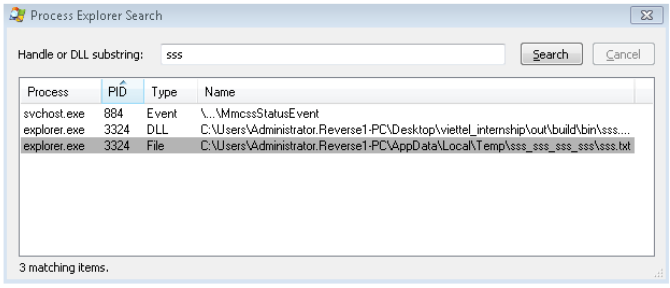


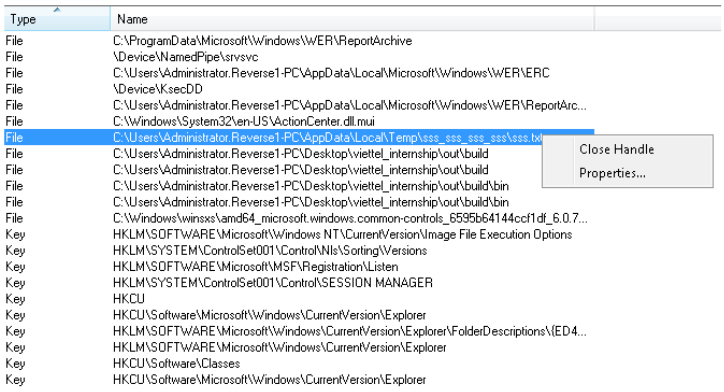
Process	VirusTotal
Freenki.exe	58/72
procexp.exe	0/73
WmiPrvSE.exe	0/72
openvpn-gui.exe	0/72
lsass.exe	0/72
GoogleCrashHandler64.exe	0/72
GoogleCrashHandler.exe	0/72
SearchIndexer.exe	0/71
rdpclip.exe	0/71
openvpnserv.exe	0/71
jusched.exe	0/71
winlogon.exe	0/70
winlogon.exe	0/70
wininit.exe	0/70
taskhost.exe	0/70
services.exe	0/70
procexp64.exe	0/70
lsm.exe	0/70
LogonUI.exe	0/70
dwm.exe	0/70
spoolsv.exe	0/69
smss.exe	0/69
explorer.exe	0/69
svchost.exe	0/68
svchost.exe	0/68
svchost.exe	0/68
svchost.exe	0/68
svchost.exe	0/68
svchost.exe	0/68
svchost.exe	0/68
svchost.exe	0/68
svchost.exe	0/68
svchost.exe	0/68
csrss.exe	0/66

Now we know that Freenki.exe is a malware, we can kill it, or suspend it by right clicking on the process, and choose Kill Process/Suspend.

If somehow the malware is not a process, but a dll injected to the process, or more stealth, a thread injected and run inside a process? Using the old malware that inject the dll in Explorer I created in week 3 exercise. sss.dll is listed in the dll section, there is no Company Name, no signature, and VirusTotal check shows `Unknown`. This dll looks suspicious. If this is a injected dll, we can find the find by right clicking on the dll file, a choose properties. The path to the dll can be found. We can check the thread of the host application `Explorer.exe`. At this time, we can kill the running thread, however we have not unload the dll. Process Explorer cannot unload the library, so restarting the process will clear these library. Supposed we know the dll name, we can search for opening `Handle` by `Ctrl+F` and type in the search box. With sss as our dll name, we also find the `file Handle` and close the handle.

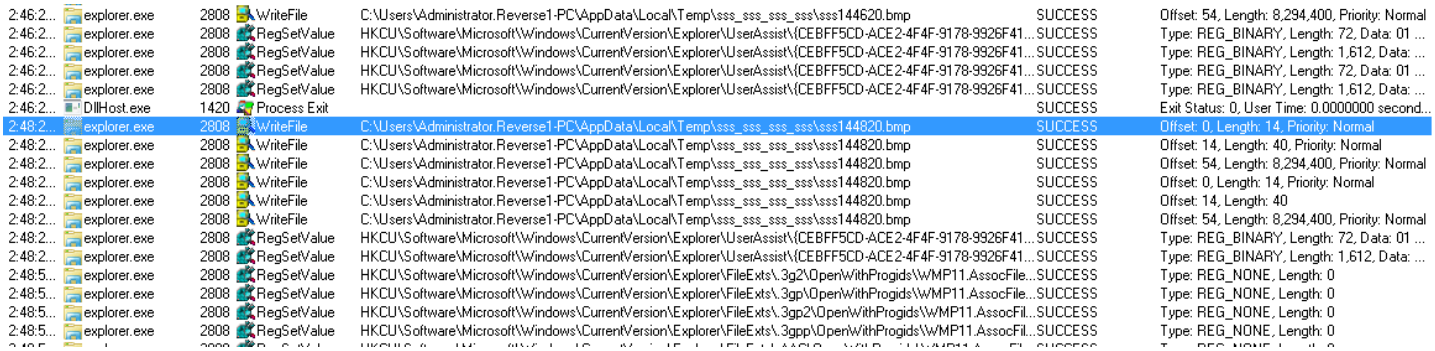






Process Monitor

Now after we have found the malware, we may not want to kill it instantly but want monitor the internet traffic, files read write, registry read write. We will open Process monitor. By default, process monitor will list everything, but we can change the filter. So this application works best only if we know, or suspect, some processes is doing bad behavior.



If we filter only WriteFile

2:46:2...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss144620.bmp	SUCCESS
2:46:2...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss144620.bmp	SUCCESS
2:46:2...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss144620.bmp	SUCCESS
2:48:2...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss144820.bmp	SUCCESS
2:48:2...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss144820.bmp	SUCCESS
2:48:2...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss144820.bmp	SUCCESS
2:48:2...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss144820.bmp	SUCCESS
2:48:2...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss144820.bmp	SUCCESS
2:48:2...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss144820.bmp	SUCCESS
2:49:4...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:4...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:4...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:4...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:4...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:4...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:4...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:4...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:49:5...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS
2:50:0...	explorer.exe	2808	WriteFile	C:\Users\Administrator.Reverse1-PC\AppData\Local\Temp\sss_sss_sss_sss\sss.txt	SUCCESS

TCP View

Process monitor is good for events and stuff, but everything together is a mess. We can use TCP View to simplify the internet connection. TCPView has two options, `address resolve` and `show unconnected endpoint`. If our malware is connecting outside, we can turn off `unconnected endpoint` to see only connecting ones. And turn off `address resolve` to find the ip address. And yes we can end the process, or close the internet handle. After we have identify the connection, we can use other tools (Wireshark) to inspect the request. This application works best if there is no other network, or we can filter out clean processes.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
svchost.exe	304	TCP	192.168.113.104	3389	192.168.110.28	55351	ESTABLISHED	315	195,015	844	72,796
Freenki.exe	1060	TCP	192.168.113.104	1119	206.189.148.40	80	ESTABLISHED	3	1,020	3	2,196

Autoruns

When we hunt a malware, we should definitely look out for autoruns. Autoruns are executable that will run on system log on. Like our `Freenki.exe` inject it self as a key to run automatically after a user logs on. With autoruns, we can inspect those registry keys, folders that contains autoruns application.

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				7/14/2009 11:49 AM	
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	11/20/2010 4:46 PM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				6/24/2019 5:39 PM	
SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America	c:\program files (x86)\common files\java\java update\jusched.exe	4/2/2019 1:25 PM	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2/13/2019 11:36 AM	
OPENVPN-GUI		(Verified) OpenVPN Technologies	c:\program files\openvpn\bin\openvpn-gui.exe	3/19/1925 1:45 AM	
Windscribe			File not found: C:\Program Files (x86)\Windscribe\Windscribe.exe		
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				6/18/2019 9:50 AM	
Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files (x86)\google\chrome\application\75.0.3770.142\installer\chrmstp.exe	7/12/2019 12:00 PM	
n/a	Microsoft .NET IE SECURITY REGISTRATI...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	6/4/2009 10:59 AM	
OpenVPN Setup			File not found: reg		
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				6/18/2019 9:50 AM	
n/a	Microsoft .NET IE SECURITY REGISTRATI...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	9/29/2010 10:53 AM	
HKLM\SOFTWARE\Classes\Protocols\Filter				7/14/2009 11:53 AM	
application/octet-stream	Microsoft .NET Runtime Execution Engine	(Verified) Microsoft Corporation	c:\windows\system32\mscoree.dll	3/5/2010 10:05 AM	
application/x-complus	Microsoft .NET Runtime Execution Engine	(Verified) Microsoft Corporation	c:\windows\system32\mscoree.dll	3/5/2010 10:05 AM	
application/x-msdownload	Microsoft .NET Runtime Execution Engine	(Verified) Microsoft Corporation	c:\windows\system32\mscoree.dll	3/5/2010 10:05 AM	
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers				6/19/2019 2:24 PM	
WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winrar\rarext.dll	4/28/2019 3:03 AM	
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers				6/19/2019 2:24 PM	
WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winrar\rarext.dll	4/28/2019 3:03 AM	
HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers				6/19/2019 2:24 PM	
WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winrar\rarext.dll	4/28/2019 3:03 AM	
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				6/24/2019 5:39 PM	
Java(tm) Plug-In 2 SSV Hel...	Java(TM) Platform SE binary	(Verified) Oracle America	c:\program files\java\jre1.8.0_211\bin\jp2ssv.dll	4/2/2019 11:35 AM	
Java(tm) Plug-In SSV Helper	Java(TM) Platform SE binary	(Verified) Oracle America	c:\program files\java\jre1.8.0_211\bin\ssv.dll	4/2/2019 11:41 AM	
Task Scheduler					
\GoogleUpdateTaskMachi...	Google Installer	(Verified) Google Inc	c:\program files (x86)\google\update\googleupdate.exe	4/22/2017 8:31 AM	
\GoogleUpdateTaskMachi...	Google Installer	(Verified) Google Inc	c:\program files (x86)\google\update\googleupdate.exe	4/22/2017 8:31 AM	
\Microsoft\VisualStudio\U...	Visual Studio Background Download	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft visual studio\installer\resources\app\servicehub\ser...	6/7/2019 3:19 AM	
\npcapwatchdog			c:\program files\npcap\checkstatus.bat	5/1/2019 12:59 AM	
HKLM\System\CurrentControlSet\Services				7/24/2019 1:53 PM	
clr_optimization_v2.0.5072...	Microsoft .NET Framework NGEN	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework\v2.0.50727\mscorsvw.exe	6/4/2009 12:25 PM	
clr_optimization_v2.0.5072...	Microsoft .NET Framework NGEN	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework64\v2.0.50727\mscorsvw.exe	6/4/2009 10:59 AM	
clr_optimization_v4.0.3031...	Microsoft .NET Framework NGEN	(Verified) Microsoft Dynamic Code P...	c:\windows\microsoft.net\framework\v4.0.30319\mscorsvw.exe	3/27/2018 2:58 AM	
clr_optimization_v4.0.3031...	Microsoft .NET Framework NGEN	(Verified) Microsoft Dynamic Code P...	c:\windows\microsoft.net\framework64\v4.0.30319\mscorsvw.exe	3/27/2018 3:08 AM	
FontCache3.0.0.0	Optimizes performance of Windows Present...	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework64\v3.0\wpf\presentationfontcache.exe	9/29/2010 2:36 PM	
GoogleChromeElevationSe...	Google Chrome	(Verified) Google LLC	c:\program files (x86)\google\chrome\application\75.0.3770.142\elevation_service....	7/12/2019 12:00 PM	
gupdate	Keeps your Google software up to date. If thi...	(Verified) Google Inc	c:\program files (x86)\google\update\googleupdate.exe	4/22/2017 8:31 AM	
gupdatem	Keeps your Google software up to date. If thi...	(Verified) Google Inc	c:\program files (x86)\google\update\googleupdate.exe	4/22/2017 8:31 AM	
idsvc	Securely enables the creation, management,...	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework64\v3.0\windows communication foundation\in...	9/29/2010 2:25 PM	
MozillaMaintenance	The Mozilla Maintenance Service ensures th...	(Verified) Mozilla Corporation	c:\program files (x86)\mozilla maintenance service\maintenanceservice.exe	6/18/2019 11:19 AM	
OpenVPNService		(Not verified)	c:\program files\openvpn\bin\openvpnserv2.exe	11/25/2016 2:43 PM	
OpenVPNServiceInteractive	OpenVPN Service	(Verified) OpenVPN Technologies	c:\program files\openvpn\bin\openvpnserv.exe	1/2/1970 7:24 PM	
OpenVPNServiceLegacy	OpenVPN Service	(Verified) OpenVPN Technologies	c:\program files\openvpn\bin\openvpnserv.exe	1/2/1970 7:24 PM	
VSStandardCollectorServic...	Visual Studio Data Collection Service. When...	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft visual studio\shared\common\diagnosticshub.collect...	5/1/2019 1:11 PM	
HKLM\System\CurrentControlSet\Services				7/24/2019 1:53 PM	
npcap	Npcap Packet Driver (NPCAP)	(Verified) Insecure.Com LLC	c:\windows\system32\drivers\npcap.sys	3/13/2018 10:14 PM	

After `Freenki.exe` injection:

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				7/14/2009 11:49 AM	
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	11/20/2010 4:46 PM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				6/24/2019 5:39 PM	
SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America	c:\program files (x86)\common files\java\java update\jusched.exe	4/2/2019 1:25 PM	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				7/24/2019 3:00 PM	
OPENVPN-GUI		(Verified) OpenVPN Technologies	c:\program files\openvpn\bin\openvpn-gui.exe	3/19/1925 1:45 AM	
runsample			c:\users\administrator.reverse1-pc\desktop\freenki.exe	5/14/2017 2:29 PM	
Windscribe			File not found: C:\Program Files (x86)\Windscribe\Windscribe.exe		
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				6/18/2019 9:50 AM	
Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files (x86)\google\chrome\application\75.0.3770.142\installer\chrmstp.exe	7/12/2019 12:00 PM	
n/a	Microsoft .NET IE SECURITY REGISTRATI...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	6/4/2009 10:59 AM	
OpenVPN Setup			File not found: reg		
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				6/18/2019 9:50 AM	
n/a	Microsoft .NET IE SECURITY REGISTRATI...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	9/29/2010 10:53 AM	
HKLM\SOFTWARE\Classes\Protocols\Filter				7/14/2009 11:53 AM	
application/octet-stream	Microsoft .NET Runtime Execution Engine	(Verified) Microsoft Corporation	c:\windows\system32\mscoree.dll	3/5/2010 10:05 AM	
application/x-complus	Microsoft .NET Runtime Execution Engine	(Verified) Microsoft Corporation	c:\windows\system32\mscoree.dll	3/5/2010 10:05 AM	
application/x-msdownload	Microsoft .NET Runtime Execution Engine	(Verified) Microsoft Corporation	c:\windows\system32\mscoree.dll	3/5/2010 10:05 AM	
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers				6/19/2019 2:24 PM	
WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winrar\rarext.dll	4/28/2019 3:03 AM	
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers				6/19/2019 2:24 PM	
WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winrar\rarext.dll	4/28/2019 3:03 AM	
HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers				6/19/2019 2:24 PM	
WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winrar\rarext.dll	4/28/2019 3:03 AM	
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				6/24/2019 5:39 PM	
Java(tm) Plug-In 2 SSV Hel...	Java(TM) Platform SE binary	(Verified) Oracle America	c:\program files\java\jre1.8.0_211\bin\jp2ssv.dll	4/2/2019 11:35 AM	
Java(tm) Plug-In SSV Helper	Java(TM) Platform SE binary	(Verified) Oracle America	c:\program files\java\jre1.8.0_211\bin\ssv.dll	4/2/2019 11:41 AM	
Task Scheduler					
\GoogleUpdateTaskMachi...	Google Installer	(Verified) Google Inc	c:\program files (x86)\google\update\googleupdate.exe	4/22/2017 8:31 AM	
\GoogleUpdateTaskMachi...	Google Installer	(Verified) Google Inc	c:\program files (x86)\google\update\googleupdate.exe	4/22/2017 8:31 AM	
\Microsoft\VisualStudio\U...	Visual Studio Background Download	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft visual studio\installer\resources\app\servicehub\ser...	6/7/2019 3:19 AM	
\npcapwatchdog			c:\program files\npcap\checkstatus.bat	5/1/2019 12:59 AM	
HKLM\System\CurrentControlSet\Services				7/24/2019 1:53 PM	
clr_optimization_v2.0.5072...	Microsoft .NET Framework NGEN	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework\v2.0.50727\mscorsvw.exe	6/4/2009 12:25 PM	
clr_optimization_v2.0.5072...	Microsoft .NET Framework NGEN	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework64\v2.0.50727\mscorsvw.exe	6/4/2009 10:59 AM	
clr_optimization_v4.0.3031...	Microsoft .NET Framework NGEN	(Verified) Microsoft Dynamic Code P...	c:\windows\microsoft.net\framework\v4.0.30319\mscorsvw.exe	3/27/2018 2:58 AM	
clr_optimization_v4.0.3031...	Microsoft .NET Framework NGEN	(Verified) Microsoft Dynamic Code P...	c:\windows\microsoft.net\framework64\v4.0.30319\mscorsvw.exe	3/27/2018 3:08 AM	
FontCache3.0.0.0	Optimizes performance of Windows Present...	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework64\v3.0\wpf\presentationfontcache.exe	9/29/2010 2:36 PM	
GoogleChromeElevationSe...	Google Chrome	(Verified) Google LLC	c:\program files (x86)\google\chrome\application\75.0.3770.142\elevation_service....	7/12/2019 12:00 PM	
gupdate	Keeps your Google software up to date. If thi...	(Verified) Google Inc	c:\program files (x86)\google\update\googleupdate.exe	4/22/2017 8:31 AM	
gupdatem	Keeps your Google software up to date. If thi...	(Verified) Google Inc	c:\program files (x86)\google\update\googleupdate.exe	4/22/2017 8:31 AM	
idsvc	Securely enables the creation, management,...	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework64\v3.0\windows communication foundation\in...	9/29/2010 2:25 PM	
MozillaMaintenance	The Mozilla Maintenance Service ensures th...	(Verified) Mozilla Corporation	c:\program files (x86)\mozilla maintenance service\maintenanceservice.exe	6/18/2019 11:19 AM	
OpenVPNService		(Not Verified)	c:\program files\openvpn\bin\openvpnserv2.exe	11/25/2016 2:43 PM	
OpenVPNServiceInteractive	OpenVPN Service	(Verified) OpenVPN Technologies	c:\program files\openvpn\bin\openvpnserv.exe	1/2/1970 7:24 PM	
OpenVPNServiceLegacy	OpenVPN Service	(Verified) OpenVPN Technologies	c:\program files\openvpn\bin\openvpnserv.exe	1/2/1970 7:24 PM	
VSStandardCollectorServic...	Visual Studio Data Collection Service. When...	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft visual studio\shared\common\diagnosticshub.collect...	5/1/2019 1:11 PM	
HKLM\System\CurrentControlSet\Services				7/24/2019 1:53 PM	

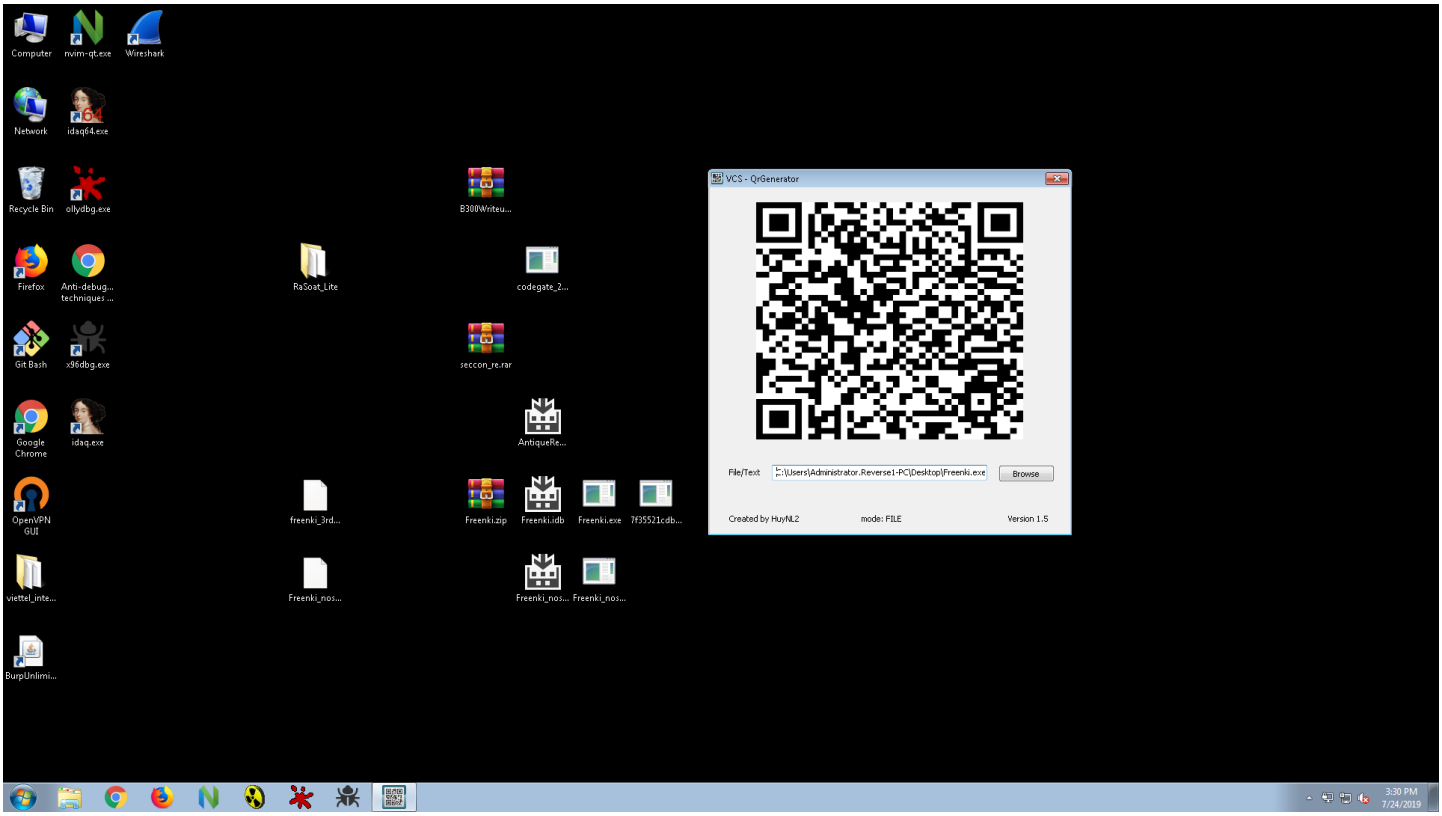
Again we can check virus total. Autoruns `Options -> Hide VirusToal Clean Entries` is a big help for us to whitelist others processes. We can enable this by enable VirusTotal for every file. After that, rescan and we can focus more on the suspicious file.

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				7/24/2019 3:00 PM	
runsample			c:\users\administrator.reverse1-pc\desktop\freenki.exe	5/14/2017 2:29 PM	58/72
Windscribe			File not found: C:\Program Files (x86)\Windscribe\Windscribe.exe		
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				6/18/2019 9:50 AM	
OpenVPN Setup			File not found: reg		
HKLM\System\CurrentControlSet\Services				7/24/2019 1:53 PM	
VGPU			File not found: System32\drivers\rdvgkmd.sys		
WMI Database Entries					
BVTConsumer			File not found: KernCap.vbs		

And deleting the entry file can't be more simpler.

QrCode

This is a application for a no internet connection machine. Sometimes machine comes with no outside internet to prevent infiltration or secret data stealing. If this is the case, the VirusTotal check is unable. But we can still, hash the file and send to VirusTotal, using this application, we can hash the file by dropping to the window. The application will draw a QrCode, which opens a link to VirusTotal check.



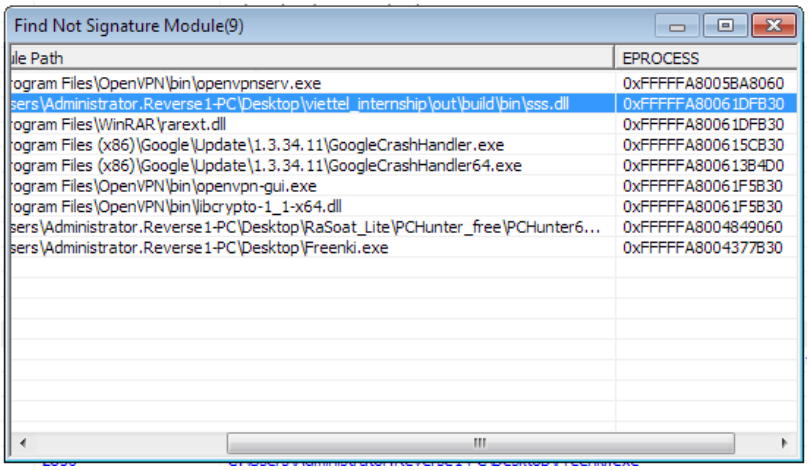
The result above will resolve to:
https://www.virustotal.com/#/file/7f35521cdbaa4e86143656ff9c52cef8d1e5e5f8245860c205364138f82c54df.

```
from pyzbar.pyzbar import decode
from PIL import Image

print(decode(Image.open('qrcode.png')))

# [Decoded(data=b'https://www.virustotal.com/#/file/7f35521cdbaa4e86143656ff9c52cef8d1e5e5f8245860c205364138f82c54df', ty
```

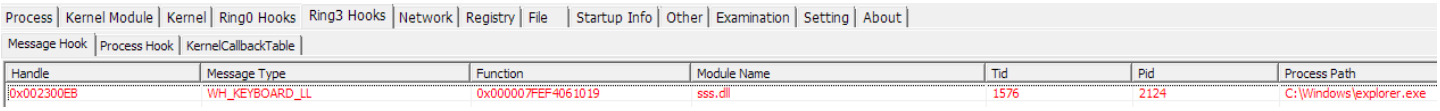
PCHunter

This is a program that is commonly used to detect applications, processes in kernel level. It was first named xuetr, but later renamed to PCHunter. The current program is still being updated and avaible on their website. Upon opening the program, we see a list of process. Different to aforementioned programs, PCHunter has a `EPROCESS` field. In short, `EPROCESS` is a process representation, like PEB, in the Kernel Mode, the struct is here.

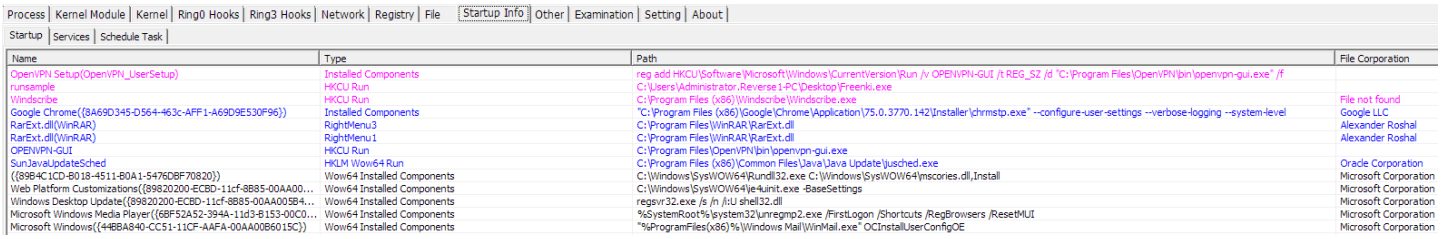
Right click on one process, and choose `Find Unsigned Module`, the program will open and search for unsigned modules. In the screenshot below, we can see that our `sss.dll` and `Freenki.exe` are both listed with their EPROCESS addresses.



We can inspect Ring0 Hooks, and Ring3 Hooks. In Ring3 Hook, we can see our `sss.dll` is hooking `WH_KEYBOARD_LL`, we can right click and disable hooking.



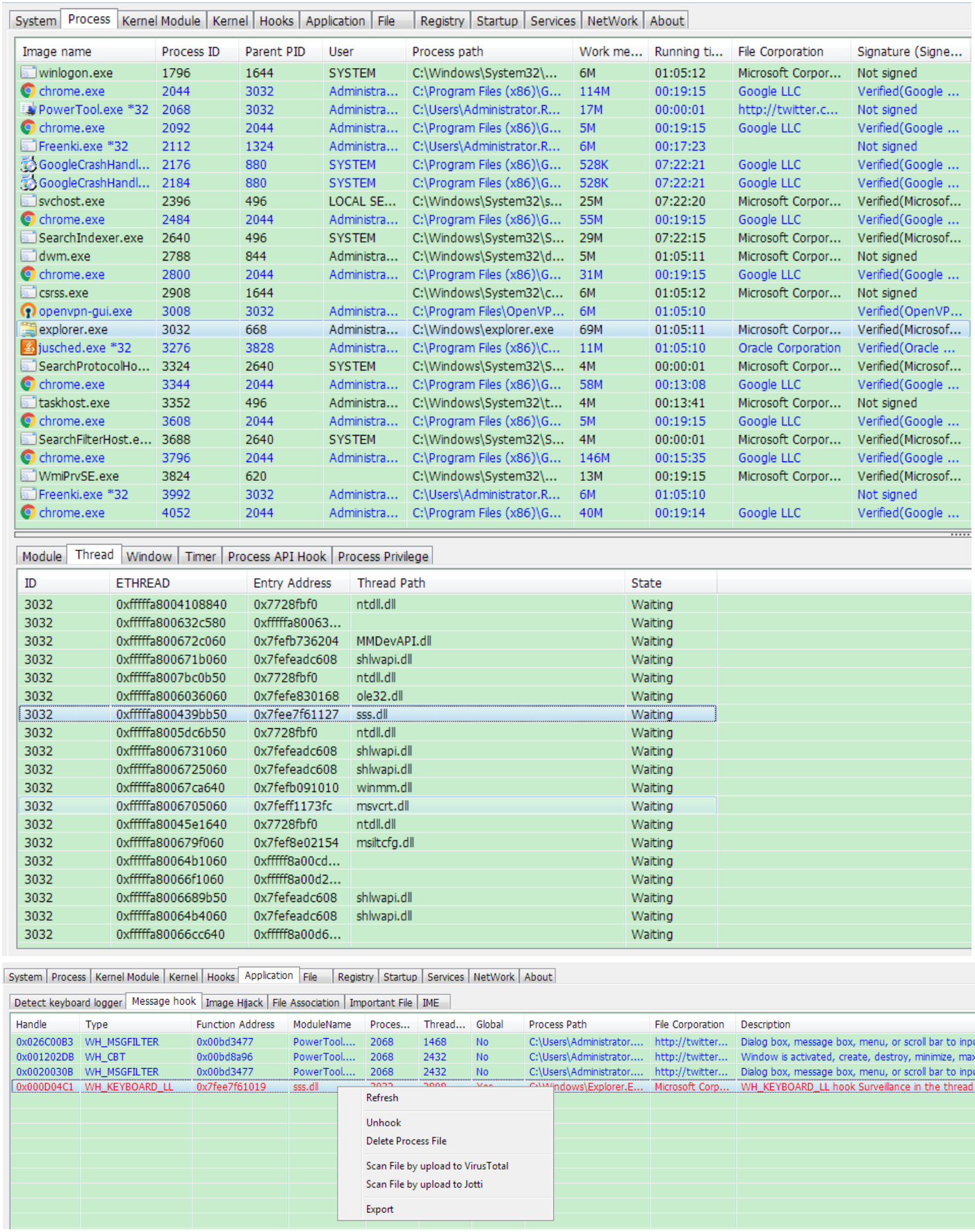
PCHunter also has Network inspection, and Registry file tree, Startup Info. In Startup Info, we can right click and choose to `Verify All Startup Signature`. After, we can right click and choose to delete `startup` or `startup and file` of any startup entry.

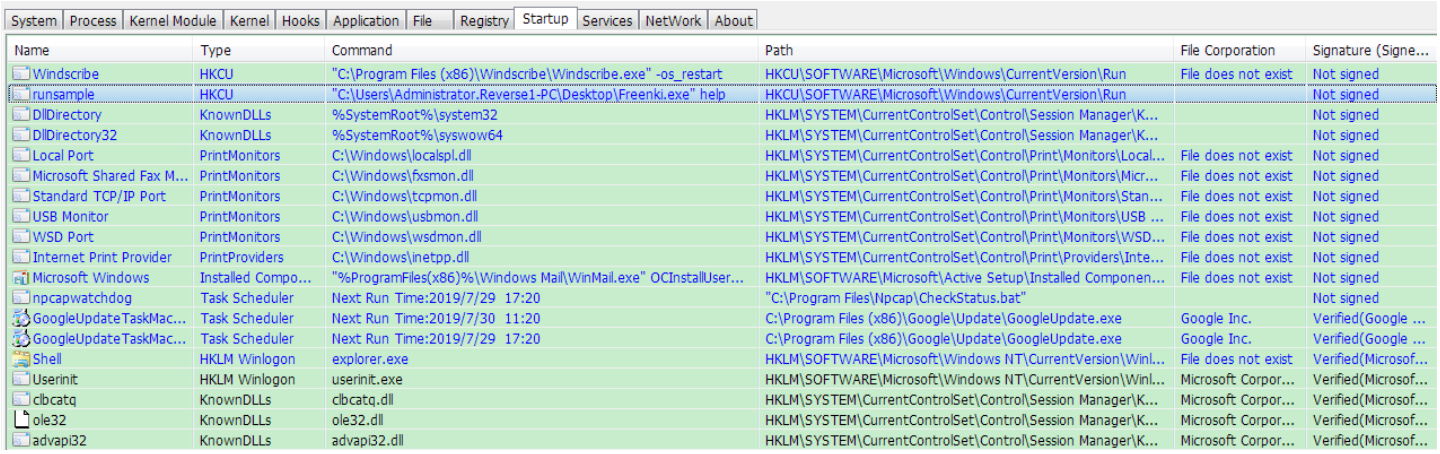


PCHunter is a kernel mode analysis tool, we can kill, force kill, unload any process/library. Which is why it could cause harm to the system. This tool should be used with care, and before using the tool on a client machine, ask for permission first.

PowerTool

I cannot find a trusted source for PowerTool, but someone posted the files on github/repoool/powertool. PowerTool is a kernel mode analysis tool like PCHunter, the interface is quite alike to previous programs. We can inspect processes, processes' modules, processes' threads, application message hook, kernel hook, startup entries, and network activities. We can also stop threads, and unhook. This program can also verify all processes' signature and scan file upload to virus total.


System
Process
Kernel Module
Kernel
Hooks
Application
File
Registry
Startup
Services
NetWork
About
Image name
Process ID
Parent PID
User
Process path
Work me...
Running ti...
File Corporation
Signature (Signe...
winlogon.exe 1796 1644 SYSTEM C:\Windows\System32\... 6M 01:05:12 Microsoft Corpor... Not signed
chrome.exe 2044 3032 Administra... C:\Program Files (x86)\G... 114M 00:19:15 Google LLC Verified(Google ...
PowerTool.exe *32 2068 3032 Administra... C:\Users\Administrator.R... 17M 00:00:01 http://twitter.c... Not signed
chrome.exe 2092 2044 Administra... C:\Program Files (x86)\G... 5M 00:19:15 Google LLC Verified(Google ...
Freenki.exe *32 2112 1324 Administra... C:\Users\Administrator.R... 6M 00:17:23 Not signed
GoogleCrashHandl... 2176 880 SYSTEM C:\Program Files (x86)\G... 528K 07:22:21 Google LLC Verified(Google ...
GoogleCrashHandl... 2184 880 SYSTEM C:\Program Files (x86)\G... 528K 07:22:21 Google LLC Verified(Google ...
svchost.exe 2396 496 LOCAL SE... C:\Windows\System32\s... 25M 07:22:20 Microsoft Corpor... Verified(Microsof...
chrome.exe 2484 2044 Administra... C:\Program Files (x86)\G... 55M 00:19:15 Google LLC Verified(Google ...
SearchIndexer.exe 2640 496 SYSTEM C:\Windows\System32\S... 29M 07:22:15 Microsoft Corpor... Verified(Microsof...
dwm.exe 2788 844 Administra... C:\Windows\System32\d... 5M 01:05:11 Microsoft Corpor... Not signed
chrome.exe 2800 2044 Administra... C:\Program Files (x86)\G... 31M 00:19:15 Google LLC Verified(Google ...
csrss.exe 2908 1644 C:\Windows\System32\c... 6M 01:05:12 Microsoft Corpor... Not signed
openvpn-gui.exe 3008 3032 Administra... C:\Program Files\OpenVP... 6M 01:05:10 Verified(OpenVP...
explorer.exe 3032 668 Administra... C:\Windows\explorer.exe 69M 01:05:11 Microsoft Corpor... Verified(Microsof...
jusched.exe *32 3276 3828 Administra... C:\Program Files (x86)\C... 11M 01:05:10 Oracle Corporation Verified(Oracle ...
SearchProtocolHo... 3324 2640 SYSTEM C:\Windows\System32\S... 4M 00:00:01 Microsoft Corpor... Verified(Microsof...
chrome.exe 3344 2044 Administra... C:\Program Files (x86)\G... 58M 00:13:08 Google LLC Verified(Google ...
taskhost.exe 3352 496 Administra... C:\Windows\System32\t... 4M 00:13:41 Microsoft Corpor... Not signed
chrome.exe 3608 2044 Administra... C:\Program Files (x86)\G... 5M 00:19:15 Google LLC Verified(Google ...
SearchFilterHost.e... 3688 2640 SYSTEM C:\Windows\System32\S... 4M 00:00:01 Microsoft Corpor... Verified(Microsof...
chrome.exe 3796 2044 Administra... C:\Program Files (x86)\G... 146M 00:15:35 Google LLC Verified(Google ...
WmiPrvSE.exe 3824 620 C:\Windows\System32\... 13M 00:19:15 Microsoft Corpor... Verified(Microsof...
Freenki.exe *32 3992 3032 Administra... C:\Users\Administrator.R... 6M 01:05:10 Not signed
chrome.exe 4052 2044 Administra... C:\Program Files (x86)\G... 40M 00:19:14 Google LLC Verified(Google ...
Module
Thread
Window
Timer
Process API Hook
Process Privilege
ID
ETHREAD
Entry Address
Thread Path
State
3032 0xffffffa8004108840 0x7728fbf0 ntdll.dll Waiting
3032 0xffffffa800632c580 0xffffffa80063... Waiting
3032 0xffffffa800672c060 0x7fefb736204 MMDevAPI.dll Waiting
3032 0xffffffa800671b060 0x7fefeadc608 shlwapi.dll Waiting
3032 0xffffffa8007bc0b50 0x7728fbf0 ntdll.dll Waiting
3032 0xffffffa8006036060 0x7fefe830168 ole32.dll Waiting
3032 0xffffffa800439bb50 0x7fee7f61127 sss.dll Waiting
3032 0xffffffa8005dc6b50 0x7728fbf0 ntdll.dll Waiting
3032 0xffffffa8006731060 0x7fefeadc608 shlwapi.dll Waiting
3032 0xffffffa8006725060 0x7fefeadc608 shlwapi.dll Waiting
3032 0xffffffa80067ca640 0x7fefb091010 winmm.dll Waiting
3032 0xffffffa8006705060 0x7feff1173fc msvcrt.dll Waiting
3032 0xffffffa80045e1640 0x7728fbf0 ntdll.dll Waiting
3032 0xffffffa800679f060 0x7fef8e02154 msiltcfg.dll Waiting
3032 0xffffffa80064b1060 0xfffff8a00cd... Waiting
3032 0xffffffa80066f1060 0xfffff8a00d2... Waiting
3032 0xffffffa8006689b50 0x7fefeadc608 shlwapi.dll Waiting
3032 0xffffffa80064b4060 0x7fefeadc608 shlwapi.dll Waiting
3032 0xffffffa80066cc640 0xfffff8a00d6... Waiting
System
Process
Kernel Module
Kernel
Hooks
Application
File
Registry
Startup
Services
NetWork
About
Detect keyboard logger
Message hook
Image Hijack
File Association
Important File
IME
Handle
Type
Function Address
ModuleName
Proces...
Thread...
Global
Process Path
File Corporation
Description
0x026C00B3 WH_MSGFILTER 0x00bd3477 PowerTool.... 2068 1468 No C:\Users\Administrator.... http://twitter... Dialog box, message box, menu, or scroll bar to input...
0x001202DB WH_CBT 0x00bd8a96 PowerTool.... 2068 2432 No C:\Users\Administrator.... http://twitter... Window is activated, create, destroy, minimize, maxi...
0x0020030B WH_MSGFILTER 0x00bd3477 PowerTool.... 2068 2432 No C:\Users\Administrator.... http://twitter... Dialog box, message box, menu, or scroll bar to input...
0x000D04C1 WH_KEYBOARD_LL 0x7fee7f61019 sss.dll Microsoft Corp... WH_KEYBOARD_LL hook Surveillance in the thread i...
Refresh
Unhook
Delete Process File
Scan File by upload to VirusTotal
Scan File by upload to Jotti
Export



Name	Type	Command	Path	File Corporation	Signature (Signe...
Windscribe	HKCU	"C:\Program Files (x86)\Windscribe\Windscribe.exe" -os_restart	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	File does not exist	Not signed
runsample	HKCU	"C:\Users\Administrator.Reverse1-PC\Desktop\Freenki.exe" help	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		Not signed
DllDirectory	KnownDLLs	%SystemRoot%\system32	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\K...		Not signed
DllDirectory32	KnownDLLs	%SystemRoot%\syswow64	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\K...		Not signed
Local Port	PrintMonitors	C:\Windows\localspl.dll	HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors\Local...	File does not exist	Not signed
Microsoft Shared Fax M...	PrintMonitors	C:\Windows\fxsmon.dll	HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors\Micr...	File does not exist	Not signed
Standard TCP/IP Port	PrintMonitors	C:\Windows\tcpmon.dll	HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors\Stan...	File does not exist	Not signed
USB Monitor	PrintMonitors	C:\Windows\usbmon.dll	HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors\USB ...	File does not exist	Not signed
WSD Port	PrintMonitors	C:\Windows\wsdmon.dll	HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors\WSD...	File does not exist	Not signed
Internet Print Provider	PrintProviders	C:\Windows\inetpp.dll	HKLM\SYSTEM\CurrentControlSet\Control\Print\Providers\Inte...	File does not exist	Not signed
Microsoft Windows	Installed Compo...	"%ProgramFiles(x86)%\Windows Mail\WinMail.exe" OCInstallUser...	HKLM\SOFTWARE\Microsoft\Active Setup\Installed Componen...	File does not exist	Not signed
npcapwatchdog	Task Scheduler	Next Run Time:2019/7/29 17:20	"C:\Program Files\Npcap\CheckStatus.bat"		Not signed
GoogleUpdateTaskMac...	Task Scheduler	Next Run Time:2019/7/30 11:20	C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	Google Inc.	Verified(Google ...
GoogleUpdateTaskMac...	Task Scheduler	Next Run Time:2019/7/29 17:20	C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	Google Inc.	Verified(Google ...
Shell	HKLM Winlogon	explorer.exe	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winl...	File does not exist	Verified(Microsof...
Userinit	HKLM Winlogon	userinit.exe	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winl...	Microsoft Corpor...	Verified(Microsof...
clbcatq	KnownDLLs	clbcatq.dll	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\K...	Microsoft Corpor...	Verified(Microsof...
ole32	KnownDLLs	ole32.dll	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\K...	Microsoft Corpor...	Verified(Microsof...
advapi32	KnownDLLs	advapi32.dll	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\K...	Microsoft Corpor...	Verified(Microsof...

And again, we should take into consideration using these tools as it could cause harm to the client machine.

Summary

The above are some tools that malware analysis frequently use to monitor the computer and look for bad files. These tools are simple, easy to use, but a good user is a user with experience. One must know what bad files do to detect them quickly and counter them with ease. After the malware sample is taken, the next step is to remove it, safely, and learn about it by reversing.