Dynamic Analysis Considerations

Tyler Hudak
INCIDENT RESPONDER

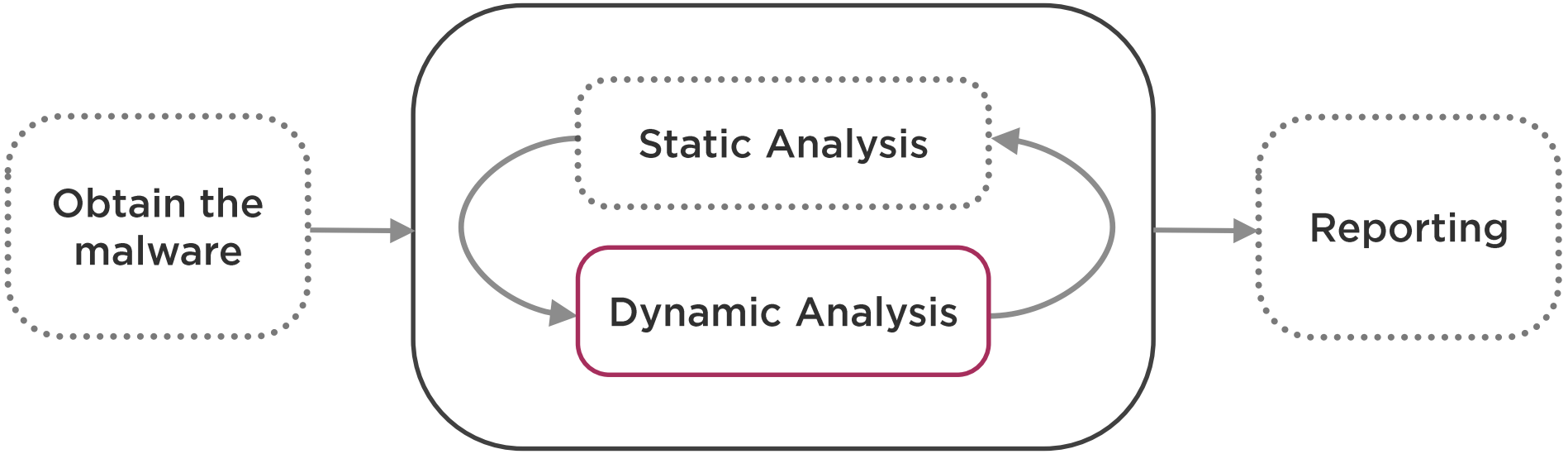
@secshoggoth

Overview

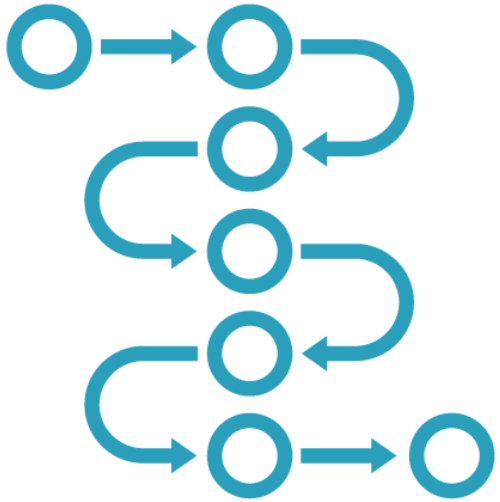
How to focus dynamic analysis

OS and malware considerations

Malware Analysis Process



Dynamic Analysis



Behavior monitoring

Tools run at same time

Single execution of malware

Focus Your Analysis

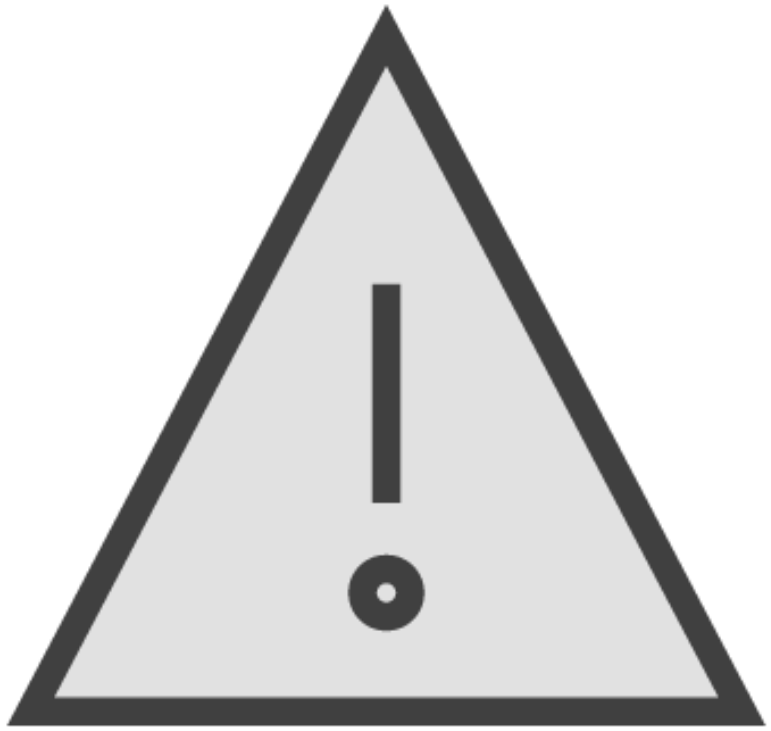
File system modifications?

Registry modifications?

What network traffic is generated?

How does the malware auto-start?

Does it launch any other processes?

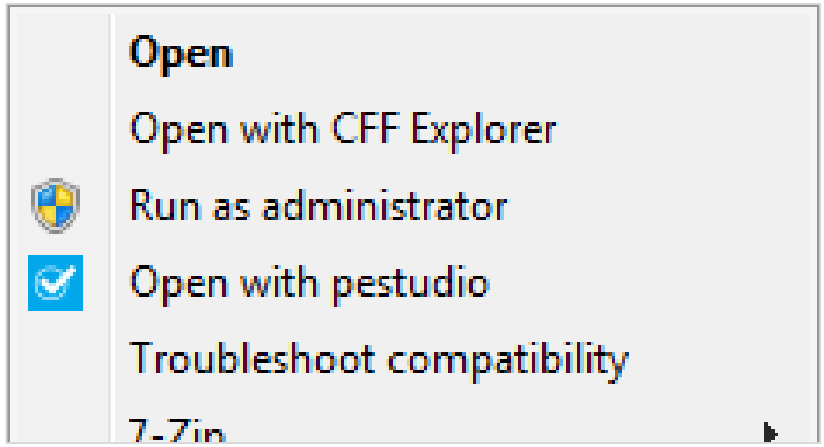


Malware will be executed!

Host-only networking

No shares mapped to important folders

User Access Control (UAC)

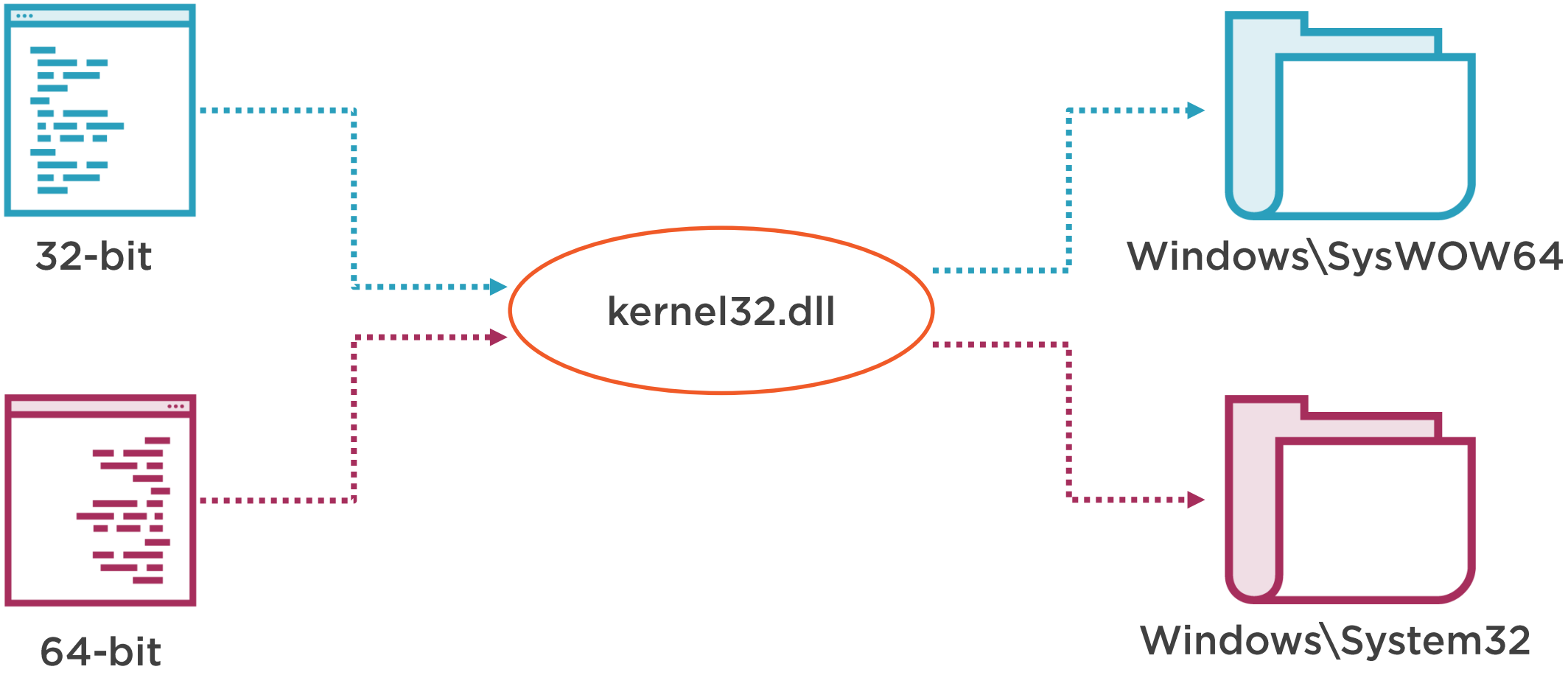


Run tools with full admin privileges

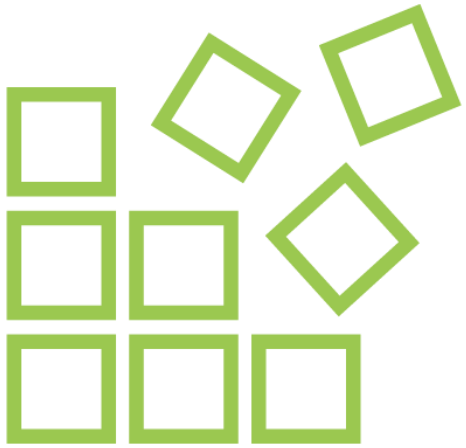
Malware privileges depend on what you are simulating

32-bit Programs on 32-bit Windows

32-bit Programs on 64-bit Windows



Malware Persistence



Registry

Keys that will auto-start programs on boot or logon

DLL Search Order

Takes advantage of the order in which DLLs are loaded

Registry Persistence

HKLM HKCU	\Software\Microsoft\Windows\CurrentVersion\Run
	\Software\Microsoft\Windows\CurrentVersion\RunOnce
	\Software\Microsoft\Windows\CurrentVersion\RunServices
	\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
	\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
	\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs

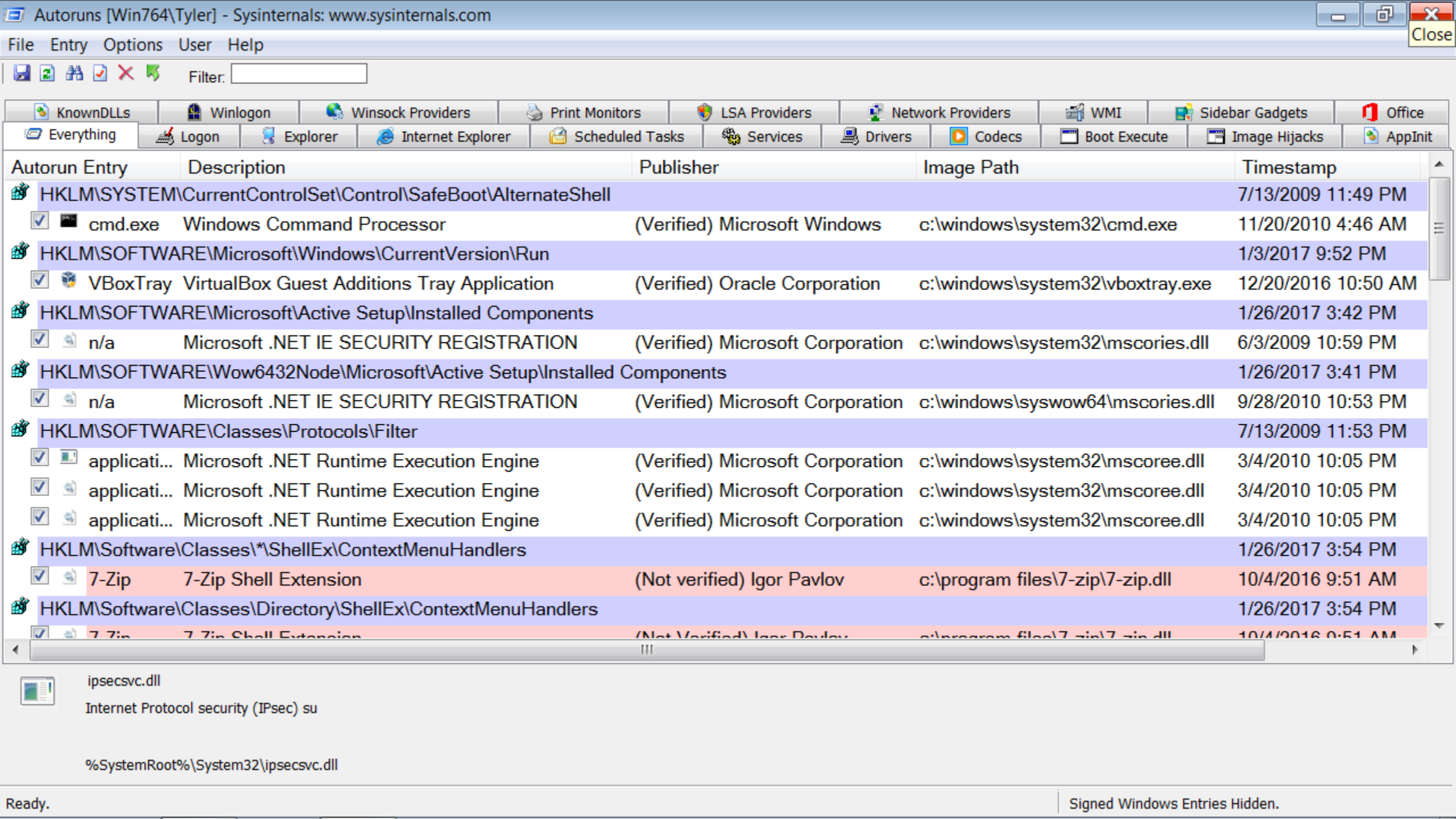
Autoruns

Shows many persistence locations

VirusTotal Integration

Shows code signed entries

https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx


Autoruns [Win764\Tyler] - Sysinternals: www.sysinternals.com
Close
File Entry Options User Help
Filter:
KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit
Autorun Entry Description Publisher Image Path Timestamp
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell 7/13/2009 11:49 PM
cmd.exe Windows Command Processor (Verified) Microsoft Windows c:\windows\system32\cmd.exe 11/20/2010 4:46 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 1/3/2017 9:52 PM
VBoxTray VirtualBox Guest Additions Tray Application (Verified) Oracle Corporation c:\windows\system32\vboxtray.exe 12/20/2016 10:50 AM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components 1/26/2017 3:42 PM
n/a Microsoft .NET IE SECURITY REGISTRATION (Verified) Microsoft Corporation c:\windows\system32\mscories.dll 6/3/2009 10:59 PM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components 1/26/2017 3:41 PM
n/a Microsoft .NET IE SECURITY REGISTRATION (Verified) Microsoft Corporation c:\windows\syswow64\mscories.dll 9/28/2010 10:53 PM
HKLM\SOFTWARE\Classes\Protocols\Filter 7/13/2009 11:53 PM
applicati... Microsoft .NET Runtime Execution Engine (Verified) Microsoft Corporation c:\windows\system32\mscoree.dll 3/4/2010 10:05 PM
applicati... Microsoft .NET Runtime Execution Engine (Verified) Microsoft Corporation c:\windows\system32\mscoree.dll 3/4/2010 10:05 PM
applicati... Microsoft .NET Runtime Execution Engine (Verified) Microsoft Corporation c:\windows\system32\mscoree.dll 3/4/2010 10:05 PM
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers 1/26/2017 3:54 PM
7-Zip 7-Zip Shell Extension (Not verified) Igor Pavlov c:\program files\7-zip\7-zip.dll 10/4/2016 9:51 AM
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers 1/26/2017 3:54 PM
ipsecsvc.dll
Internet Protocol security (IPsec) su
%SystemRoot%\System32\ipsecsvc.dll
Ready.
Signed Windows Entries Hidden.

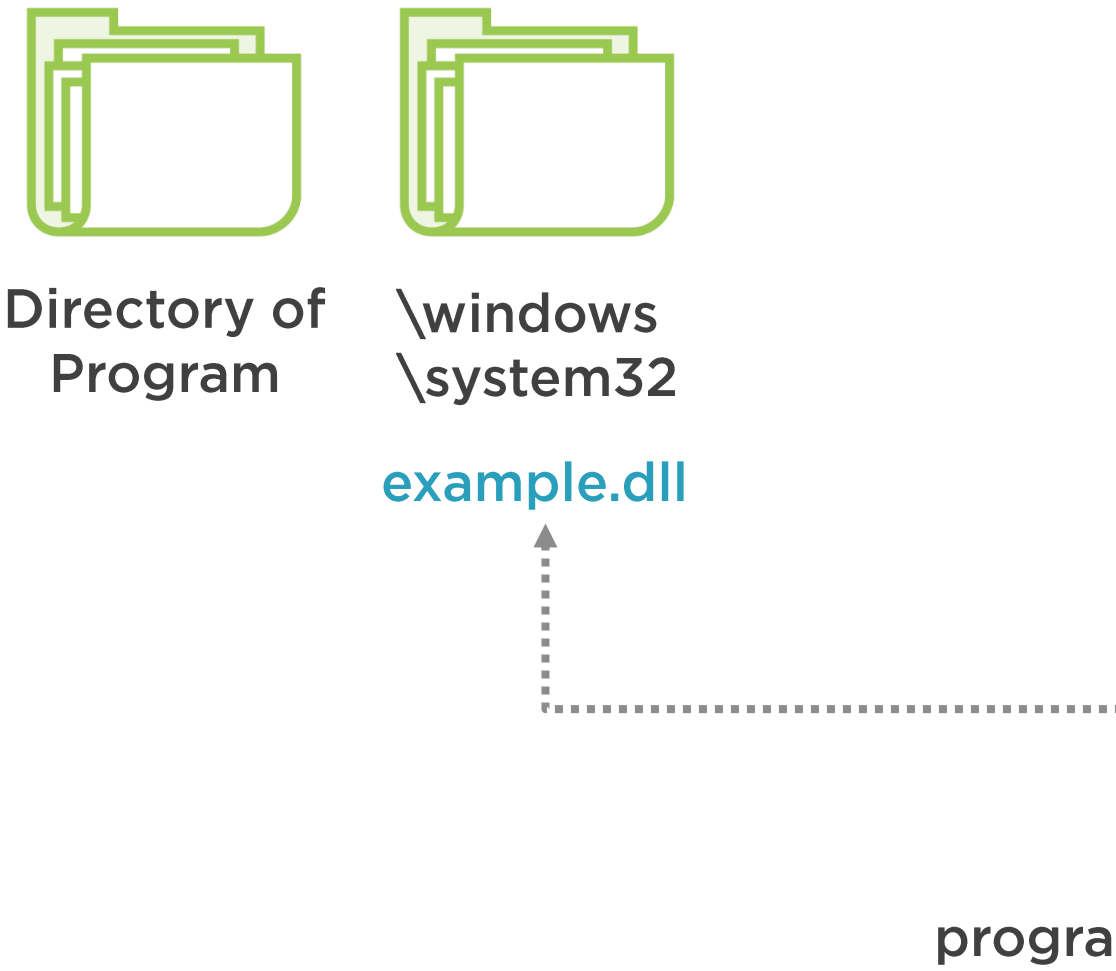
DLL Search Order

Directory of Program

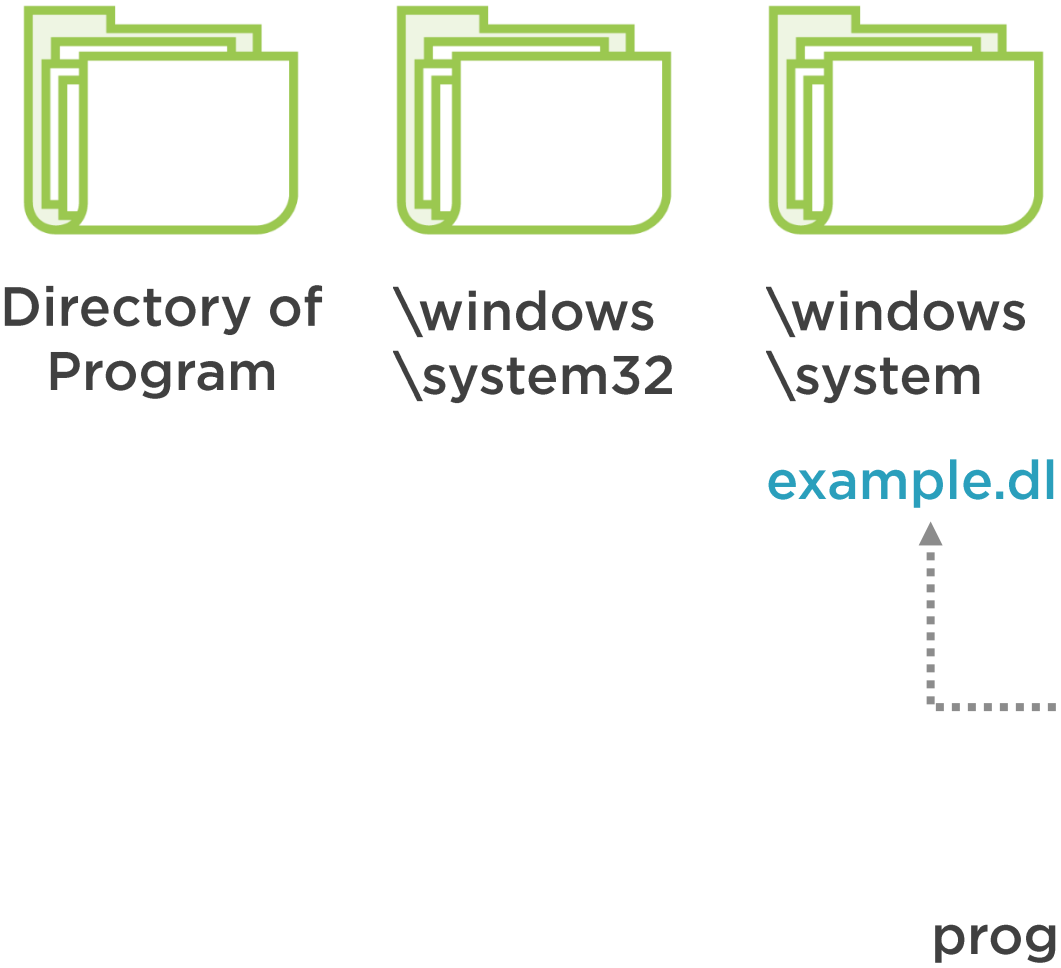
example.dll

program.exe

DLL Search Order



DLL Search Order



DLL Search Order

Directory of Program

\windows \system32

\windows \system

\windows

example.dll

program.exe

DLL Search Order

Directory of Program

\windows \system32

\windows \system

\windows

Current Directory

example.dll

program.exe

DLL Search Order

Directory of Program

\windows \system32

\windows \system

\windows

Current Directory

%PATH%

example.dll

program.exe

DLL Search Order

Directory of Program

example.dll

\windows \system32

\windows \system

\windows

Current Directory

%PATH%

example.dll

program.exe

Summary

Focus your investigation

Be careful!

Understand how the tools will behave

- UAC
- 32 vs. 64 bit

Malware persistence