



מעבדה 1



CSRP

DFIR

מבוא ל-DFIR

איתור תכניות Startup

- עמוד 1 -

כל הזכויות שמורות © סיבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

נושאי המעבדה

השיגו ראיות בנוגע לגבי התוכניות המופעלות בעת הפעלת המחשב שלך.

זמן מוערך

10-15 דקות.

סביבת המעבדה

- Windows ○
- Sysinternals ○

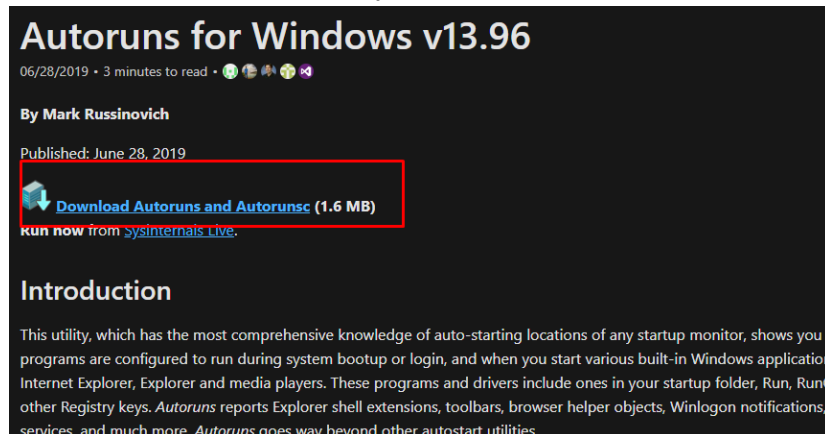
נסו למצוא ראיות של תכניות מתמשכות באמצעות היישום Autoruns הכלול בערכת הכלים של Sysinternals.

1 הורידו והתיקנו Autoruns מהקישור הבא:

<https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>

פתרון:

שימו לב: אתם לא חייבים בהכרח להתקין Autoruns. אפשר להריץ את הקובץ בר הביצוע ישירות על ידי לחיצה כפולה על הקישור Run now.



Autoruns מחלקת את הצפייה לכרטיסיות רבות. השתמש בברטיסיית Everything כדי לבצע חיפוש בסיסי.

2 השתמשו ב-Autoruns כדי למצוא תכניות המסומנות לביצוע, אך אינן מותקנות עוד.

פתרון:

אם תכנית נרשמה ב-registry לביצוע בזמן הפעלה, אבל נמחקה מבלי לנקות את ה-key, המחשב עדיין ינסה לבצע אותה.

ב-Autoruns, תכניות כאלו יסומנו בצהוב.

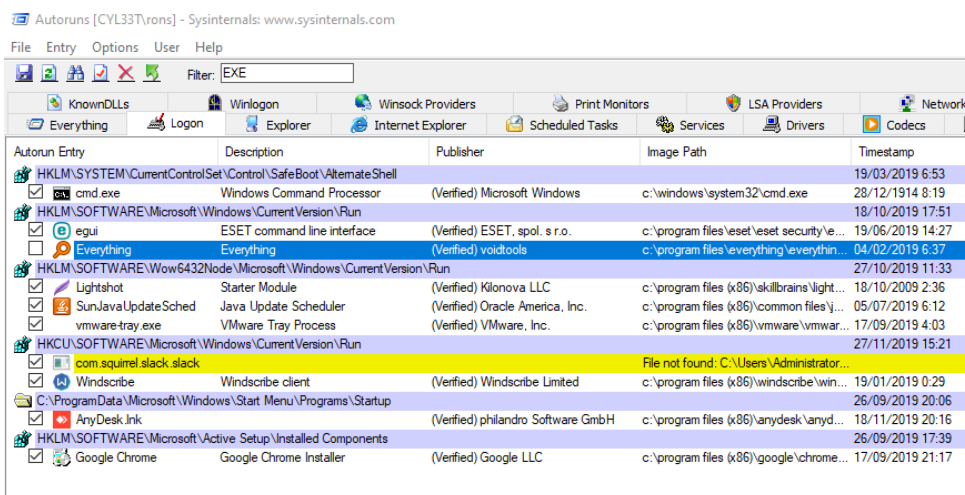
Autoun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell	Control\SafeBoot\AlternateShell	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	19/03/2019 6:53	
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	28/12/1914 8:19	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Windows\CurrentVersion\Run	(Verified) Microsoft Corporation	c:\program files\eset\eset security\esetcmd.exe	18/10/2019 17:51	
esetcmd.exe	ESET command line interface	(Verified) ESET, spol. s r.o.	c:\program files\eset\eset security\esetcmd.exe	19/05/2019 14:27	
Everything	Everything	(Verified) voidtools	c:\program files\everything\everything.exe	04/02/2019 6:37	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	Microsoft\Windows\CurrentVersion\Run	(Verified) Microsoft Corporation	c:\program files\lightshot\lightshot.exe	27/10/2019 11:33	
Lightshot	Starter Module	(Verified) Kionova LLC	c:\program files (x86)\allibrans\lightshot.exe	18/10/2009 2:36	
SunJavaUpdateSch	Java Update Scheduler	(Verified) Oracle America, Inc.	c:\program files (x86)\common files\java\bin\jusched.exe	05/07/2019 6:12	
vmware-tray.exe	VMware Tray Process	(Verified) VMware, Inc.	c:\program files (x86)\vmware\vmtoolsd\vmware-tray.exe	17/09/2019 4:03	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Microsoft\Windows\CurrentVersion\Run	(Verified) Microsoft Corporation	c:\program files (x86)\windscribe\windscribe-client.exe	27/11/2019 15:21	
com.aquamel.alack.alack	com.aquamel.alack.alack	(Verified) Windscribe Limited	File not found. C:\Users\Administrator\AppData\Local\Microsoft\Windows\Start Menu\Programs\Status\com.aquamel.alack.alack	19/01/2019 0:29	
WindowsUpdate	WindowsUpdate	(Verified) Windscribe Limited	c:\program files (x86)\windscribe\windscribe-client.exe	19/01/2019 0:29	
Microsoft\Windows\Start Menu\Programs\Status	Microsoft\Windows\Start Menu\Programs\Status	(Verified) Windscribe Limited	c:\program files (x86)\windscribe\windscribe-client.exe	19/01/2019 0:29	
AnyDesk Ink	AnyDesk Ink	(Verified) phildand Software GmbH	c:\program files (x86)\anydesk\anydesk-ink.exe	18/11/2019 20:16	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Microsoft\Windows\CurrentVersion\Run	(Verified) Google LLC	c:\program files (x86)\google\chrome\chrome.exe	26/09/2019 17:39	
Google Chrome	Google Chrome	(Verified) Google LLC	c:\program files (x86)\google\chrome\chrome.exe	17/09/2019 21:17	
Task Scheduler	Task Scheduler	(Verified) Adobe Inc.	c:\program files (x86)\common files\adobe\adobeupdate\adobeupdate.exe	24/07/2019 10:52	
Adobe Acrobat Update	Adobe Reader and Acrobat Manager	(Verified) Adobe Inc.	c:\program files (x86)\common files\adobe\adobeupdate\adobeupdate.exe	24/07/2019 10:52	
Google Update Task.Ms	Google Update Task.Ms	(Verified) Microsoft Corporation	File not found. C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	06/12/2019 1:39	
Google Update Task.Ms	Google Update Task.Ms	(Verified) Microsoft Corporation	File not found. C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	06/12/2019 1:39	
Microsoft Office Office	Microsoft Office Click-to-Run Client	(Verified) Microsoft Corporation	c:\program files\common files\microsoft\office\15\osppres.exe	06/12/2019 1:39	
Microsoft Office Office	Microsoft Office Click-to-Run Client	(Verified) Microsoft Corporation	c:\program files\common files\microsoft\office\15\osppres.exe	06/12/2019 1:39	
Microsoft Office Office	Microsoft Office SDX Helper	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\office\15\osppres.exe	06/12/2019 1:14	
Microsoft Office Office	Microsoft Office SDX Helper	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\office\15\osppres.exe	06/12/2019 1:14	
Microsoft Office Office	Background task for Office fighting s...	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\office\15\osppres.exe	06/12/2019 1:15	
Microsoft Office Office	Background task for Office fighting s...	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\office\15\osppres.exe	06/12/2019 1:15	
Microsoft Office Office	Office Telemetry Dashboard Agent (D...	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\office\15\osppres.exe	05/11/2019 15:40	
Microsoft Office Office	Office Telemetry Dashboard Agent (D...	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\office\15\osppres.exe	05/11/2019 15:40	
Microsoft\VisualStudio\15.0\Visual Studio Background Download	Visual Studio Background Download	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\visualstudio\15.0\backgrounddownload\backgrounddownload.exe	29/03/1905 19:43	
Microsoft\Windows\Wl	Microsoft Malware Protection Comm...	(Not Verified) Microsoft Corporation	c:\programdata\microsoft\windows d... \backgrounddownload\backgrounddownload.exe	28/07/1993 11:02	
Microsoft\Windows\Wl	Microsoft Malware Protection Comm...	(Not Verified) Microsoft Corporation	c:\programdata\microsoft\windows d... \backgrounddownload\backgrounddownload.exe	28/07/1993 11:02	
Microsoft\Windows\Wl	Microsoft Malware Protection Comm...	(Not Verified) Microsoft Corporation	c:\programdata\microsoft\windows d... \backgrounddownload\backgrounddownload.exe	28/07/1993 11:02	
Microsoft\Windows\Wl	Microsoft Malware Protection Comm...	(Not Verified) Microsoft Corporation	c:\programdata\microsoft\windows d... \backgrounddownload\backgrounddownload.exe	28/07/1993 11:02	
OneDrive Standalone Updater	Standalone Updater	(Verified) Microsoft Corporation	c:\users\roni\appdata\local\microso...	13/09/2019 2:30	
OneDrive Standalone Updater	Standalone Updater	(Verified) Microsoft Corporation	c:\users\roni\appdata\local\microso...	13/09/2019 2:30	

שימו לב: שהתכניות שמוצגות בדוגמה יכולות להשתנות בין תלמיד ותלמיד.

3 מצאו registry keys שמאחסנים מיקומי startup (לפחות שלושה keys).
פתרון:

ב-Autoruns, היבנסו לתיקיית Logon שמראה רשימה של כל התכניות שיופעלו על ידי שירות ה-Logon.

שימו לב: שצריך לעשות זאת כדי לסנן את הפלט. פעלות (Triggers) אחרות יכולות לגרום לתכניות לרוץ באופן אוטומטי.



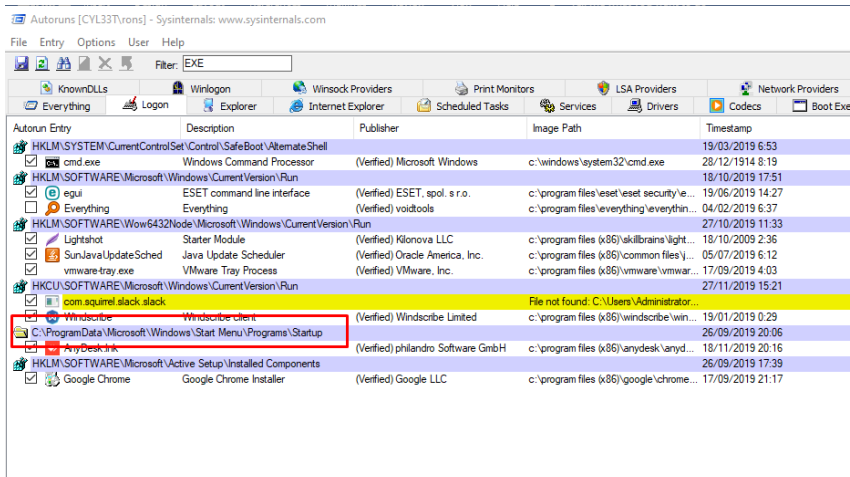
Registry keys נפוצים הנמצאים בכל מחשב כוללים:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

שימו לב: שה-keys יכולים להשתנות, תלוי באיזו גרסת מערכת הפעלה משתמשים.

4 מצאו תיקיות במיקומי ה-startup.
פתרון:

כרטיסיית ה-Logon מכילה מידע אודות תכניות שיופעלו על ידי שירות ה-logon. במקרה זה, שימו לב לתיקיות.

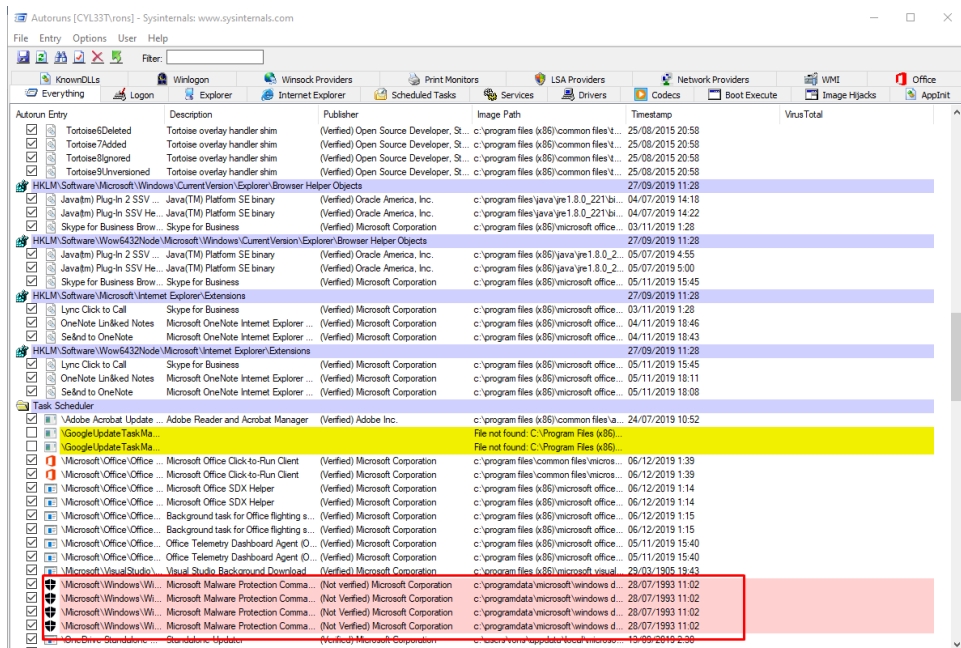


רוב הגרסאות של Windows כוללות:

- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
- C:\Users\JohnD\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

5 בדוקו אם "Not Verified" מופיע בטור ה-Publisher של יישום כלשהו. פתרון:

ב-Autoruns, תוכנות המתויגות כ-"Not Verified" יופיעו באדום. אלו יישומי תוכנה עבורם ה-publisher לא ידוע.



למרות שתוכנה שלא אומתה אינה בהכרח זדונית, יש לבדוק אותה בכל זאת.