# How to inventory Windows installed software

Jonathan Risto

December 2016

GIAC (GAWN Gold, GCIH Gold, GSLC Gold, GLEG Gold, GWAPT Gold, GCCC Gold, GSNA Gold, GPEN, GCFA, GSEC, GCPM)

# Objective

- Importance of a software inventory
- Why is this such a problem to collect
- Where is this information stored
- Methods to collect the information
- Scripting for speed and accuracy
- Conclusion

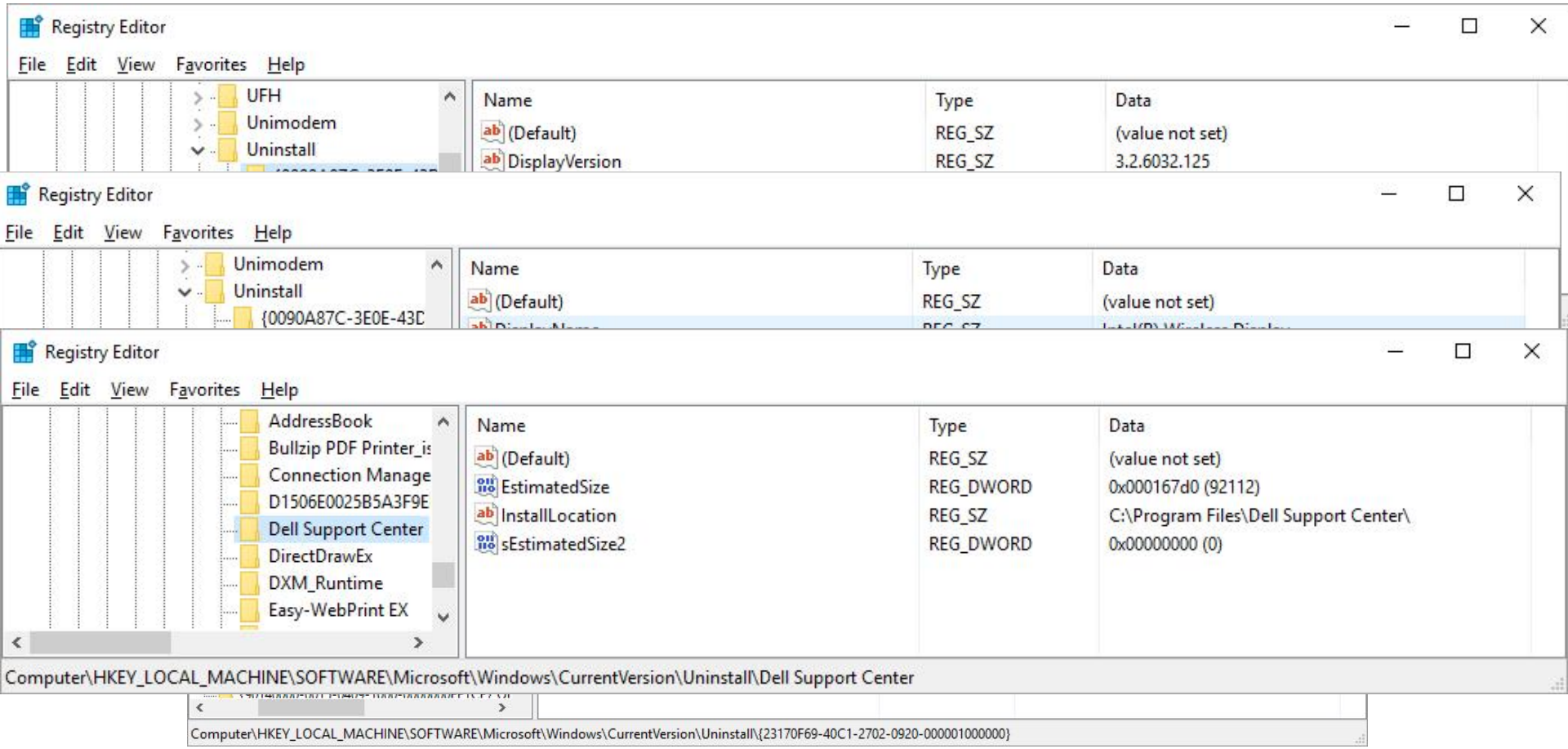
# Control 2 of the 20 Critical Controls

- The second item of the 20 CSC is software inventory
- Without a software inventory
  - Cannot know vulnerabilities
  - Cannot keep systems updated
  - Cannot validate authorized software

# Where can we find it?

- Windows does not have just one location to register an installed program
- Example registry key locations include:
  - *'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\'*
  - *'HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\'*
- No single query can return the required information

# Collection problems



# Available tools for collection

- Commercial tools
  - E.g. Tripwire, Software Inspector, Nessus
- Free tools
  - E.g. OCS inventory, PsInfo
- Built-in tools
  - E.g. WMIC, PowerShell

# PsInfo

- PsInfo is a Microsoft Sysinternals tool that can collect local or remote system information
- Version 1.77 used in paper
- Run from command line

  *psinfo.exe -s applications*

# PsInfo output example

Command Prompt

```
c:\Temp>psinfo -s application

PsInfo v1.78 - Local and remote system information viewer
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for \\JONATHAN-PC:

Applications:
Adobe AIR 22.0.0.153
Adobe AIR 22.0.0.153
Adobe Acrobat Reader DC 15.020.20039
Adobe Community Help 3.4.980
Adobe Community Help 3.4.980
Adobe Content Viewer 1.4.0
Adobe Content Viewer 1.4.0
Adobe Digital Editions 3.0 3.0.1
Adobe Download Assistant 1.0.6
Adobe Download Assistant 1.0.6
Adobe Flash Player 21 NPAPI 21.0.0.213
Adobe Flash Player 23 PPAPI 23.0.0.185
```

# WMIC

- Windows Management Instrumentation Command-line
- Permits access to query and change system functionality
- To collect inventory information

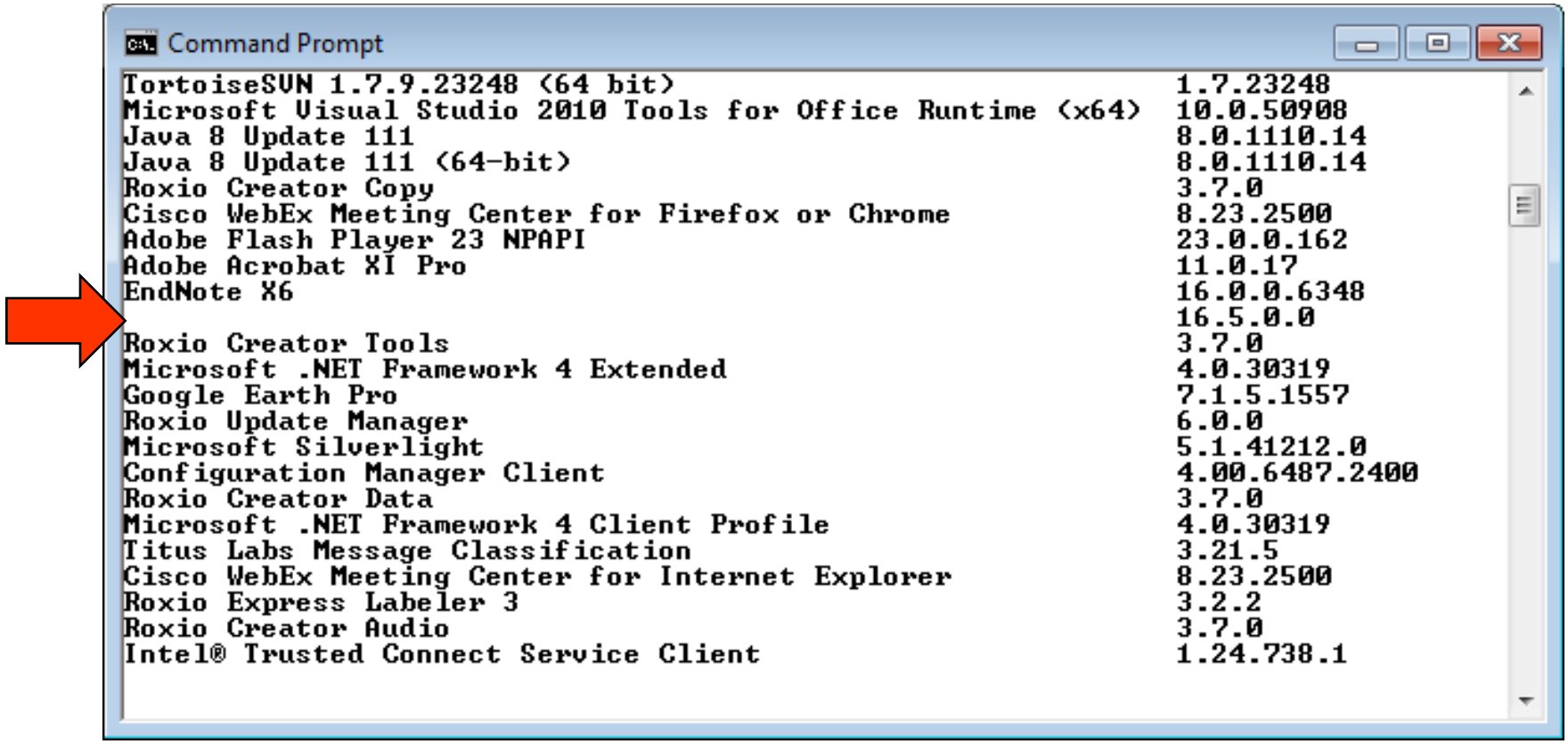
  *wmic product get name,version*

# WMIC example

Command Prompt

```
C:\Users\Jonathan>wmic product get name,version
Name                                                                  Version
Garmin MapSource                                                      6.15.11
Citrix Online Launcher                                                1.0.408
Grammarly for Microsoft® Office Suite                                 6.5.43
PxMergeModule                                                         1.00.0000
Microsoft Application Error Reporting                                 12.0.6015.5000
Microsoft Office OneNote MUI (English) 2010                           14.0.7015.1000
Microsoft Office Office 32-bit Components 2010                        14.0.7015.1000
Microsoft Office Shared 32-bit MUI (English) 2010                     14.0.7015.1000
Microsoft Office InfoPath MUI (English) 2010                          14.0.7015.1000
Microsoft Office Visio MUI (English) 2010                             14.0.7015.1000
Microsoft Office Project MUI (English) 2010                           14.0.7015.1000
Microsoft Office Access MUI (English) 2010                            14.0.7015.1000
Microsoft Office Shared Setup Metadata MUI (English) 2010             14.0.7015.1000
Microsoft Office Excel MUI (English) 2010                             14.0.7015.1000
Microsoft Office Access Setup Metadata MUI (English) 2010             14.0.7015.1000
Microsoft Office PowerPoint MUI (English) 2010                        14.0.7015.1000
Microsoft Office Publisher MUI (English) 2010                         14.0.7015.1000
Microsoft Office Outlook MUI (English) 2010                           14.0.7015.1000
Microsoft Office Groove MUI (English) 2010                            14.0.7015.1000
Microsoft Office Word MUI (English) 2010                              14.0.7015.1000
Microsoft Office Proofing (English) 2010                              14.0.7015.1000
Microsoft Office Shared MUI (English) 2010                            14.0.7015.1000
Microsoft Office Proof (English) 2010                                 14.0.7015.1000
```

# WMIC output issues



# PowerShell

- Uses the *OpenSubKey* and *GetValue* cmdlets within PowerShell
- Accesses the following registry locations and iterates through each subkey
  - *SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall* ,
  - *SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall*

# Scripting it all together

- Running commands on individual systems is tedious at best
  - Summer student project ☺
- However, scripts provide a quicker means to accomplish the tasks
- Two primary methods to create Windows scripts
  - Batch scripting
  - PowerShell

# Scripts within the paper

- Scripts examples include:
  - Batch file for PsInfo and WMIC collection
  - PowerShell script for PS commands
- All query for IP address to inventory
- Some checking is performed for valid data types and entry
- Output stored in text file for archiving and future reference

# Conclusion

- 3 methods discussed in paper
  - Scripts provided automate the process
- Increases visibility and understanding of the network
- Major first step to remediation