woanware

autorunner

Introduction

autorunner is based upon the AutoRuns tool by the Sysinternals/Microsoft gurus. It is designed to perform automated Authenticode checking for binaries designed to auto-start on a host. Its primary purpose is to aid forensic investigations.

I didn't want to write this application, it was one that I had to...software persistence is a key factor when identifying malware and I wanted AutoRuns to work. Ideally I would have just run the command line version of it and parsed the output and performed other checks on the data extracted, however, this is flawed for a number of reasons.

The key one being I can never get it to run on more than one user profile, so if I am working on a host with two user accounts, then I can extract the data from the first profile, but when run it against the second profile then it fails. Or I can reboot, remount the image, then it will load the second profile and not the first?!

The second issue that is in off-line mode it needs the user to supply the path to the user profile, which is fine for one profile, but we will work with hosts that have numerous profiles.

So autorunner is designed to work around all of these issues. It will check against all user profiles associated with the host. It will parse out LNK files to the actual binary (one level down). It allows the user to specify multiple drive mappings, so that if the forensic image contains multiple partitions you can map the original drives to mounted drives on the forensic workstation.

The application should be used against a forensic image that has been mounted using what ever method you desire.

Usage

- Mount a forensic image so that the primary Windows drive is exposed to Windows
- Extract all of the registry hives from the image to a folder, including all NTUSER.dat hives, ideally maintain the original directory structure (X-Ways will do this)
- Choose the File->Import menu item or the Import toolbar button. The Import window will be displayed
- Enter/copy and paste the path to the directory containing all of the registry hives into the Registry Path textbox
- Now add a drive mapping for each of the mounted partitions from the forensic image e.g. if there is two (one used to be C:\ and the other was E:\ for example) and after mounting to the forensic workstation they are mounted to J:\ and M:\ respectively, create a first drive mapping from C:\ to J:\ and check the “Is Windows Drive” option. Create a second mapping from E:\ to M:\
- Click OK to start the import process.

Missing files will displayed in yellow

Binaries that are not signed will be displayed in red.

Once the import process has been completed, you can use the Tools->Virus Total Check menu item to validate all of the MD5 hashes against the Virus Total (VT) website. Note that it is slow due to rate limiting against the VT API. To use the VT checking you must have a VT API key. Once you have an API key then edit the **Settings.xml** file and add it to the following area:

<ApiKey></ApiKey>

If you do not have the API key set then the menu item will be disabled.

The VT checking caches the results to a database, so in theory over time it will speed up. If you cancel the VT checking then just wait for it to finish as it will take about 20 seconds to stop.

Notes

The way that paths to binaries are stored in the registry varies wildly and autorunner attempts to deal with every case, however, there is a good chance that you will have a path that it cannot deal with. If you find such a path then send me the contents of the **File Path** column and I will add some specific parsing that will deal with it. Below is some of the different ways that paths have been expressed:

- `\??\C:\Windows\system32\Drivers\DgiVecp.sys`
- `%SystemRoot%\system32\svchost.exe -k defragsvc`
- `“C:\Program Files (x86)\GNU\GnuPG2\dirmngr.exe" --service`
- `\SystemRoot\system32\drivers\dmvsc.sys`
- `system32\drivers\drmkaud.sys`
- `C:\Windows\SysWOW64\wex4962\EMCliSrv.exe`
- `%windir%\system32\svchost.exe -k ftpsvc`
- `%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe`
- `"C:\\Program Files\\MySQL\\MySQL Server 5.5\\bin\\mysqld\" --defaults-file=\"C:\\ProgramData\\MySQL\\MySQL Server 5.5"`

The areas that autorunner parses is also limited e.g. primary logon locations e.g. registry and file system and services. The reason being is that these are the main ones and in some cases the parsing requires lookups into other areas of the registry e.g. CLSID, so I will add these in due course.

History

V0.0.4

- Added missing settings.xml file to releases. Thanks RobL
- Added error logging to the VirusTotal.NET library, outputs to the users local AppData directory for the application e.g. C:\Users\ABC\AppData\Local\woanware\virustotalchecker\Errors.txt
- Added new Updated event to the VirusTotal.NET library
- Added parsing of the AppInit_DLL keys
- Added parsing of the BHO keys
- Updated the VirusTotal.NET to v1.0.2 which should fix a number of issues including the VT checking not starting and the improvement of handling resources that don't exist. Thanks RobL

v0.0.3

- Corrected missing field from CSV export (File Version)
- Modified to clear list on each run
- Fixed issue where path replace failed due to case
- Added ability to copy entry information to clipboard
- Added ability to export a sorted and uniqued list of MD5 hashes
- Added double edit to mapping list
- Fixed error that occurred when enumerating drives that are not ready

v0.0.2

- Updated to extract ServiceDll

v0.0.1

- Initial public release