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. **Ensure that the image is mounted writeable, so that the writes are cached and the original image is not affected. This is so the application can take ownership of the files where necessary to ensure that everything is accessible to retrieve the file attributes**
- 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 and binaries that are not signed will be displayed in red