Beyond good ol’ Run key, Part 114

hexacorn.com/blog/2019/09/07/beyond-good-ol-run-key-part-114

September 7, 2019 *in Anti-Forensics, Autostart (Persistence)*

Ability to extend AutoPlay functionality with dedicated handlers is well-known and documented. The Registry key shown below is where these get added:

> HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\AutoplayHandlers\Handlers\

Instead of describing this persistence mechanism in detail, I will focus on a slightly different aspect.

Lots of software out there registers their own “personalized” handlers. While such software may no longer be used today too frequently it still comes pre-installed on many laptops and workstations.

One could modify these existing handlers to redirect them to a malicious component. How to find these? There are at least two ways. Use a predefined list, or enumerate all handlers and find these that point to handlers that reside within Program File directory (with an exclusion for Media Player).

The second task is trivial, and the first task is not too difficult either. Looking at installers of media burning software one can quickly find a lot of candidates:

- AntsDVDDVDMovieOnArrival
- ASHAshampoo_Burning_Studio_12BURNONARRIVAL
- ASHAshampoo_Burning_Studio_12COPYONARRIVAL
- ASHAshampoo_Burning_Studio_12RIPONARRIVAL
- ASHAshampoo_Burning_Studio_2013BURNONARRIVAL
- ASHAshampoo_Burning_Studio_2013COPYONARRIVAL
- ASHAshampoo_Burning_Studio_2013RIPONARRIVAL
- ASHAshampoo_Burning_Studio_6_FREEBURNONARRIVAL
- ASHAshampoo_Burning_Studio_6_FREECOPYONARRIVAL
- ASHAshampoo_Burning_Studio_6_FREERIPONARRIVAL
- AVSCaptureVideoCameraArrival
- BBShowPictureEventHandler
- BlindWriteAutoplay_741406
- BurnAware
- CCShowPicturesOnArrival
- CDBurnerXP
- CopyToDVDAutoplay_741406
- daccdrip
- DVDClonerBackupDVDMovieOnArrival
- dvdXsoftRipDVDMovieOnArrival
- ExsateDVCLHandler
- ExsateVideoExpressHandler
- HeliconBurnerOnArrival
- HMMAddToDatabaseHandler
- HMMMTPHandler
- HMMPlayHandler
- HMMRipAudioCDHandler

- JoyceCD
- LightImageResizerAutoplay_741406
- MagicBurnStudioOpenHandler
- MPCPlayBluRayOnArrival
- MPCPlayCDAudioOnArrival
- MPCPlayDVDMovieOnArrival
- MPCPlayMusicFilesOnArrival
- MPCPlayVideoFilesOnArrival
- P2GCDBurningOnArrival
- P2GDVDBurningOnArrival
- PicsPrintAutoplay
- PIETransfer
- PlayWithBlazeDVD
- PlayWithDVDXPlayer
- Power2GoPlayCDAudioOnArrival
- PrintstationPrint
- PStarterBlankCDArrival
- PStarterDVDBurningOnArrival
- PStarterMixedCDArrival
- PStarterMusicFilesArrival
- PStarterPicturesArrival
- PStarterVideoFilesArrival
- S4BCaptureVideoCameraArrival
- SpybotScanFiles\
- VCUPlayDVDMovieOnArrival
- VMP1PlayBluRayMovieOnArrival
- VMP1PlayDVDMovieOnArrival
- VMP1PlayMusicFilesOnArrival
- VMP1PlayVideoFilesOnArrival

Of course, such persistence method could be only used as a Plan B. After all, who is still burning CDs today…