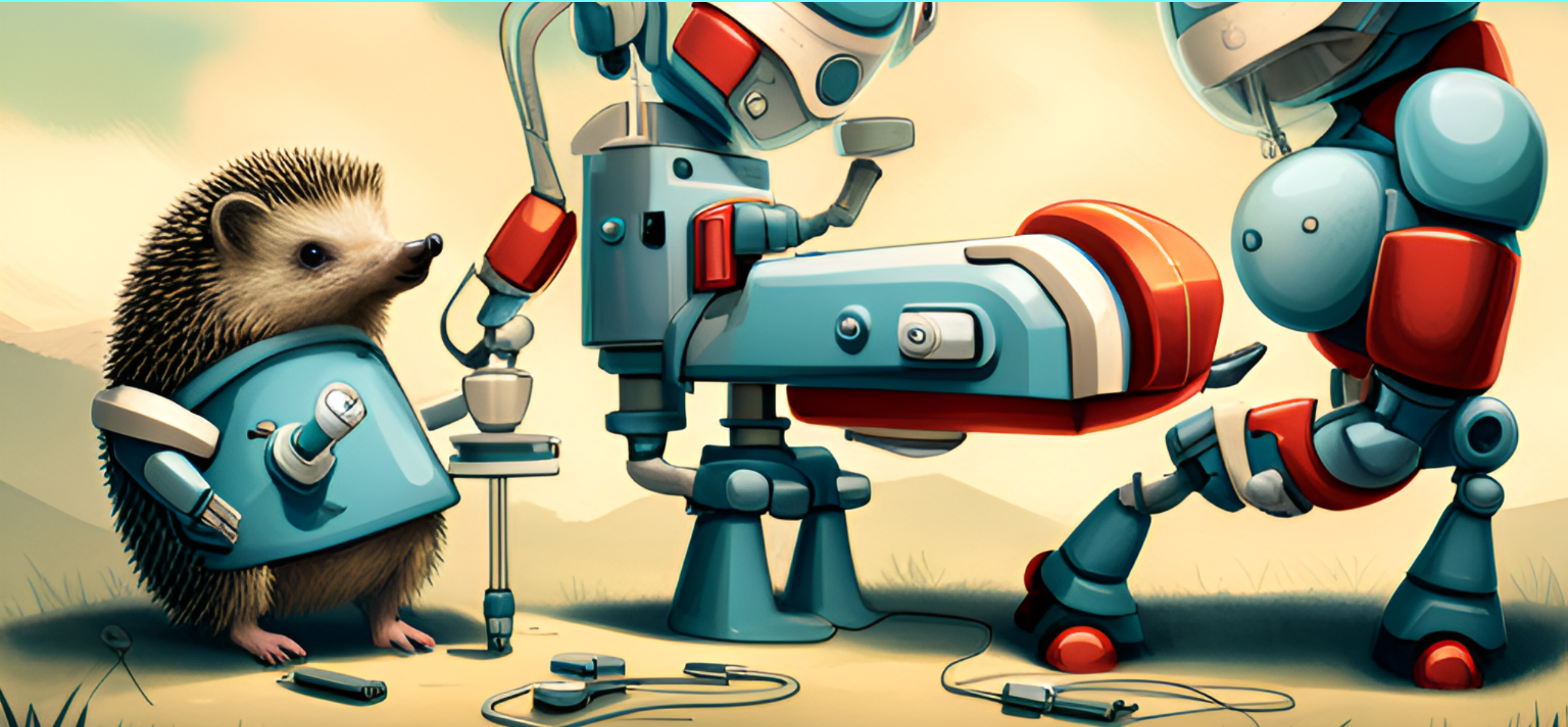
Auto Start Extensibility Points



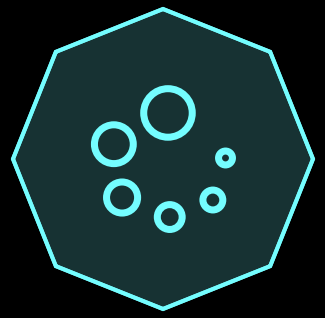
Auto Start Extensibility Points (ASEPs)

ASEPs are places that allow a program to run automatically, without user interaction

Types of ASEPs

SYSTEM PERSISTENCE MECHANISMS

- mechanisms by Windows that are meant to run user programs



PROGRAM LOADER ABUSE

- abusing the Windows loader process

APPLICATION ABUSE

- abusing extensions of legitimate programs

SYSTEM BEHAVIOR ABUSE

- Windows features

Reference: Daniel Uroz, Ricardo J. Rodríguez , Characteristics and detectability of Windows auto-start extensibility points in memory forensics, Digital Investigation, Volume 28, Supplement, 2019, Pages S95-S104, ISSN 1742-2876

System Persistence Mechanisms

RUN KEYS

- Run
- RunOnce
- RunOnceEx

STARTUP FOLDER

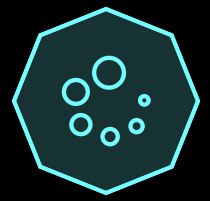
- Microsoft\Windows\Start Menu\Programs\Startup

SCHEDULED TASKS

- periodic execution of programs via Windows Task Scheduler
- every task has XML file in %Systemroot%\System32\Tasks

SERVICES

- background programs with no user interaction
- managed by Service Control Manager (SCM)



Program Loader Abuse

IMAGE FILE EXECUTION OPTIONS (IFEO)

- feature to launch programs with debugger
- malware can register as debugger

EXTENSION HIJACKING

- change default program associated with extension

SHORTCUTS MANIPULATION

- modify shortcuts to also launch malware

COM HIJACKING

- modify path of associated COM object DLLs to malware DLL

SHIM DATABASES

- apply program patches before execution
- databases stored in C:\Windows\AppPatch

Application Abuse

TROJANIZED SYSTEM BINARIES

- modification of legitimate binary, e.g., by inserting code

OFFICE ADD-INS

- extend MS Office applications

BROWSER HELPER OBJECTS (BHO)

- plugins for Internet Explorer
- only < Windows 11

System Behavior Abuse

WINLOGON

- can change desktop and file manager (explorer.exe)
- can change system program after login (userinit.exe)
- can change Winlogon notification package (DLL)

DLL HIJACKING

- abuse Windows' DLL search order so that malware DLL is loaded

APPINIT DLLS

- load DLL into address space of every application with user interface
- But: disabled if secure boot is enabled (>= Win 8)

ACTIVE SETUP

- Windows feature
- can launch programs when user signs in

ASEP Examination Tools

SYSINTERNALS AUTORUNS

- dynamic malware analysis

WINESAP (VOLATILITY PLUGIN)

- forensic investigations

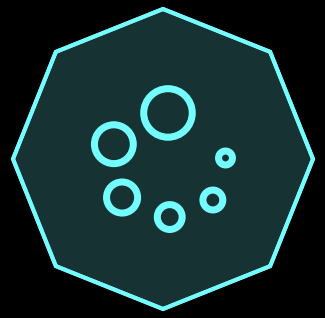
FARBAR RECOVERY SCAN TOOL (FRST)

- system disinfection

Types of ASEPs

SYSTEM PERSISTENCE MECHANISMS

- Run keys
- startup folders
- scheduled tasks
- services



PROGRAM LOADER ABUSE

- Image file execution options
- extension hijacking
- shortcut manipulation
- COM hijacking
- Shim databases

APPLICATION ABUSE

- trojanized system binaries
- Office add-ins
- browser helper objects

SYSTEM BEHAVIOR ABUSE

- Winlogon
- DLL hijacking
- AppInitsDLLs
- Active Setup