COMPX508 – Malware Analysis

Week 9

Lecture 1: Windows Registry

Vimal Kumar

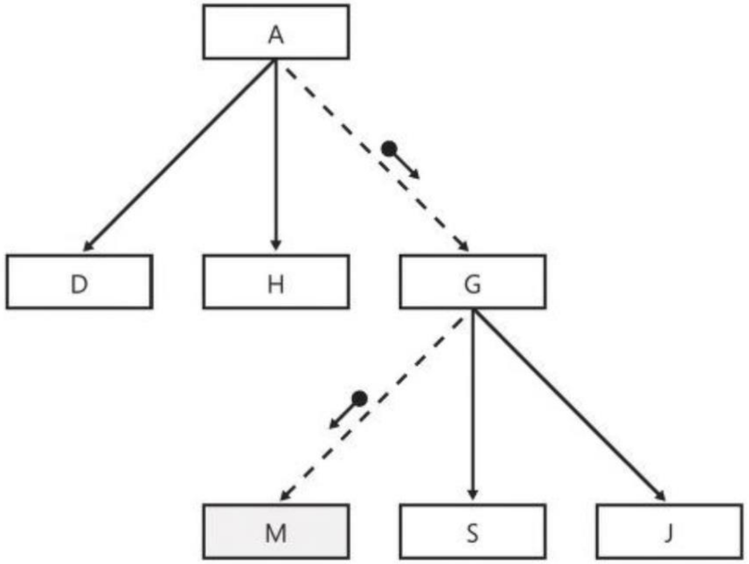
Windows Registry

- Windows stores configuration data in the registry.
- This configuration information is continually referenced during operation by Windows

- Malware often uses the registry to achieve,
  - Persistence and
  - Evasion and
  - Information hiding

Windows Registry

- The registry
  - stores information as <key, value> pairs
  - is hierarchical in nature

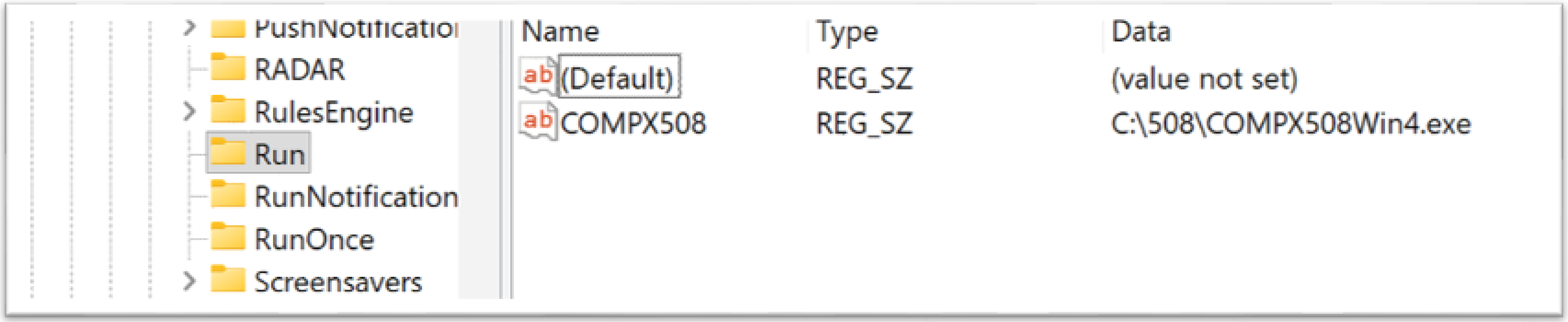


Windows Registry

- 5 Hives or root level keys

Name	Abbreviation	Contents
HKEY_CLASSES_ROOT	HKCR	Information used by programs for file association and for sharing information.
HKEY_CURRENT_USER	HKCU	Settings and configuration for the current user.
HKEY_LOCAL_MACHINE	HKLM	Settings and configuration for entire machine.
HKEY_USERS	HKU	Settings and configuration for all users on the computer; the information in HKCU is copied from this hive when the user logs in.
HKEY_CURRENT_CONFIG	HKCC	Hardware information about the PC’s resources and configuration.

Registry



Name	Type	Data
(Default)	REG_SZ	(value not set)
COMPX508	REG_SZ	C:\508\COMPX508Win4.exe

Data Types in Registry

REG_BINARY	Binary data in any form.
REG_DWORD	A 32-bit number.
REG_DWORD_LITTLE_ENDIAN	A 32-bit number in little-endian format.
REG_DWORD_BIG_ENDIAN	A 32-bit number in big-endian format.
REG_EXPAND_SZ	A null-terminated string that contains unexpanded references to environment variables (for example, "%PATH%").
REG_LINK	A null-terminated Unicode string that contains the target path of a symbolic link
REG_MULTI_SZ	A sequence of null-terminated strings, terminated by an empty string (\0).
REG_NONE	No defined value type.
REG_QWORD	A 64-bit number.
REG_QWORD_LITTLE_ENDIAN	A 64-bit number in little-endian format.
REG_SZ	A null-terminated string. This will be either a Unicode or an ANSI string, depending on whether you use the Unicode or ANSI functions.

Windows Security Identifier (SID)

- On Windows, user accounts, groups, and other security-related objects are called security principles.
  - Security Identifiers (SIDs) uniquely identify security principles.

- Example
  - S-1-5-21-2857422465-1465058494-1690550294-500

- An SID always begins with s-.
- The next number identifies the SID’s version—in this case, version 1.
- The next number indicates the identifier authority and is usually 5, which is NT Authority.
- The string of numbers up to 500 is the domain identifier,
- The rest of the SID is a relative identifier, which is the account or group.

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers

Windows Globally Unique Identifier (GUID)

- Globally unique identifiers (GUIDs) are numbers that uniquely identify objects such as computers, program components, and devices.

- An example of a GUID is {645FF040-5081-101B-9F08-00AA002F954E},

- They are 16-byte hexadecimal numbers in groups of 8, 4, 4, 4, and 12 digits.
- A dash divides each group of digits, and curly brackets enclose the whole number.

Registry related Windows API functions

- In advapi32.dll
  - advapi32.dll has many other functions as well

RegQueryInfoKey	Retrieves information about the specified registry key.
RegCreateKeyEx	Creates the specified registry key.
RegDeleteKey	Deletes a subkey and its values.
RegDeleteKeyEx	Deletes a subkey and its values from the specified platform-specific view of the
RegGetValue	Retrieves the type and data for the specified registry value.
RegDeleteValue	Removes a named value from the specified registry key.

… and many others. : see: https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-functions

Persistence and Registry

- Malware creates or modifies a key.
  - The key is set to the file path of the malware

- After a reboot
  - A part of the Windows startup process checks registry to determine what programs are to be loaded.
  - The process finds the file path to the malware and executes it.

BootExecute

- *smss.exe* launches as the first user mode process
- It calls the configuration manager subsystem and loads the permanent registry keys from the disk
- Location of the permanent keys is in the registry key

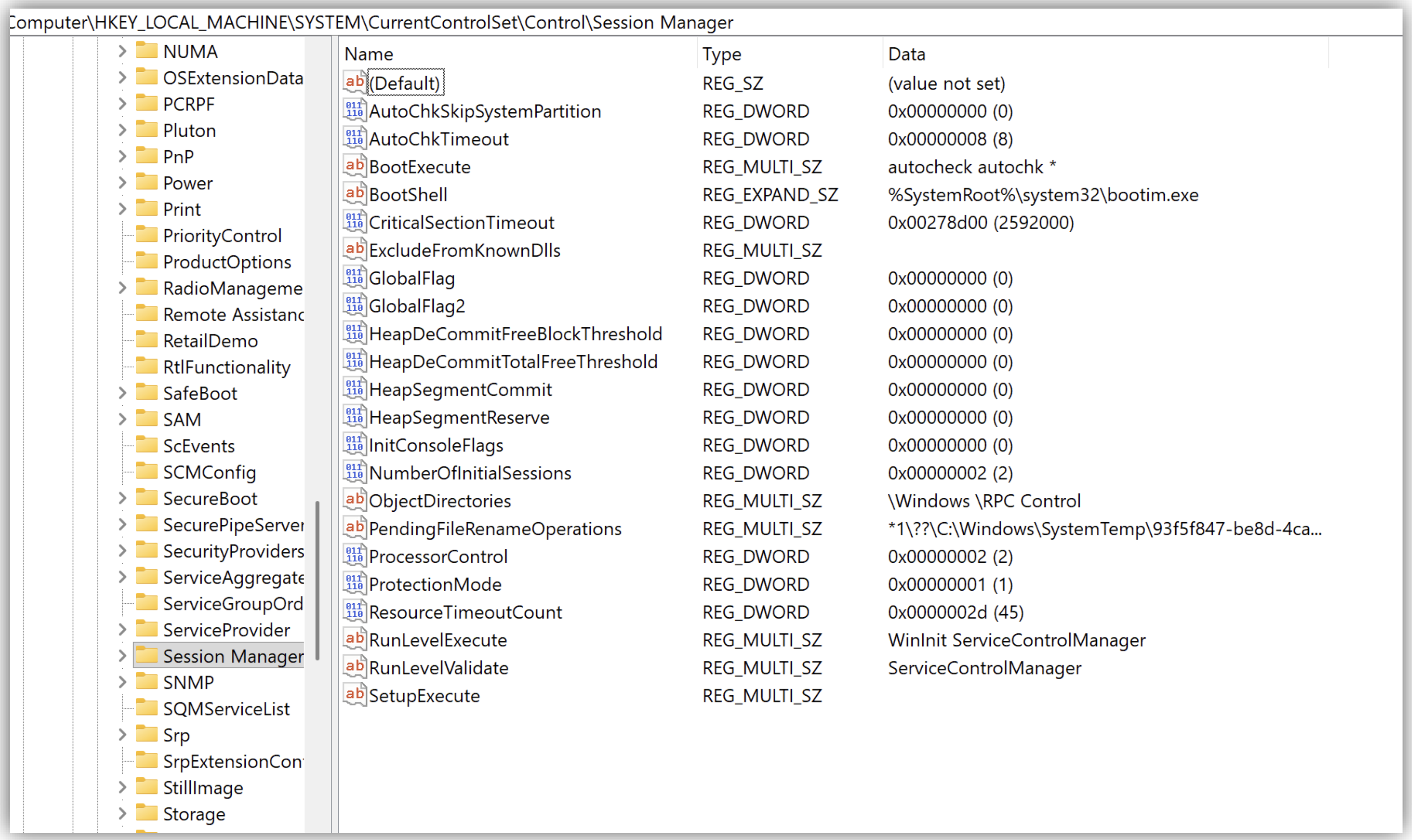
```
HKLM\SYSTEM\CurrentControlSet\Control\hivelist
```

- One of the keys that is loaded is

```
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute
```

- Windows will execute anything that is present as the value
    - The default is autocheck
    - The data type is REG_MULTI_SZ
        - Multiple strings can be added

BootExecute key



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager

- NUMA
- OSExtensionData
- PCRPF
- Pluton
- PnP
- Power
- Print
- PriorityControl
- ProductOptions
- RadioManageme
- Remote Assistanc
- RetailDemo
- RtlFunctionality
- SafeBoot
- SAM
- ScEvents
- SCMConfig
- SecureBoot
- SecurePipeServer
- SecurityProviders
- ServiceAggregate
- ServiceGroupOrd
- ServiceProvider
- Session Manager
- SNMP
- SQMServiceList
- Srp
- SrpExtensionCon
- StillImage
- Storage

Name	Type	Data
(Default)	REG_SZ	(value not set)
AutoChkSkipSystemPartition	REG_DWORD	0x00000000 (0)
AutoChkTimeout	REG_DWORD	0x00000008 (8)
BootExecute	REG_MULTI_SZ	autocheck autochk *
BootShell	REG_EXPAND_SZ	%SystemRoot%\system32\bootim.exe
CriticalSectionTimeout	REG_DWORD	0x00278d00 (2592000)
ExcludeFromKnownDlls	REG_MULTI_SZ	
GlobalFlag	REG_DWORD	0x00000000 (0)
GlobalFlag2	REG_DWORD	0x00000000 (0)
HeapDeCommitFreeBlockThreshold	REG_DWORD	0x00000000 (0)
HeapDeCommitTotalFreeThreshold	REG_DWORD	0x00000000 (0)
HeapSegmentCommit	REG_DWORD	0x00000000 (0)
HeapSegmentReserve	REG_DWORD	0x00000000 (0)
InitConsoleFlags	REG_DWORD	0x00000000 (0)
NumberOfInitialSessions	REG_DWORD	0x00000002 (2)
ObjectDirectories	REG_MULTI_SZ	\Windows \RPC Control
PendingFileRenameOperations	REG_MULTI_SZ	*1\??\C:\Windows\SystemTemp\93f5f847-be8d-4ca...
ProcessorControl	REG_DWORD	0x00000002 (2)
ProtectionMode	REG_DWORD	0x00000001 (1)
ResourceTimeoutCount	REG_DWORD	0x0000002d (45)
RunLevelExecute	REG_MULTI_SZ	WinInit ServiceControlManager
RunLevelValidate	REG_MULTI_SZ	ServiceControlManager
SetupExecute	REG_MULTI_SZ	

Services

- Windows then starts loading drivers and services
- Every device driver has a registry subkey under `HKLM\SYSTEM\CurrentControlSet\Services`
- Review the subkeys to see if any service is running from a non system directory

Winlogon

- smss.exe launches the winlogon process

- Winlogon looks for the initialization process(es) at

`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit`

- In case of an event, winlogon loads and executes the dll specified at

`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify`

- The shell key should be set to ‘explorer.exe’. The shell used by windows

`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell`

Run, RunOnce, RunOnceEx registry keys

- Cause programs to run each time the user logs in
    - RunOnce value is deleted once the program runs
        - RunOnceEx shows a dialog box while the program executes
- Value is a 260 character command
- This is the most obvious location for persistence and has been used frequently in the past
    - Sophisticated malware use this to mostly either
        - Create a lot of noise and therefore cover for other persistence techniques
        - Use this for persistence until a better persistence mechanism is found
    - This has become an obvious giveaway so usually avoided these days

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
```

Startup Keys

- Placing a malicious file under the startup directory is often used by malware authors. Any shortcut created to the location pointed by subkey Startup will launch the service during logon/reboot. Start up location is specified both at Local Machine and Current User.

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
```