

The image shows a file explorer window with a search bar at the top containing the text 'f339e7d'. Below the search bar is a list of files and folders. The 'atomics' folder is expanded, showing a list of subfolders. The subfolders are: 'Indexes', 'T1003.001', 'T1003.002', 'T1003.003', 'T1003.004', 'T1003.005', 'T1003.006', 'T1003.007', 'T1003.008', 'T1003', 'T1006', 'T1007', 'T1010', 'T1012', 'T1014', 'T1016', 'T1018', 'T1020', 'T1021.001', 'T1021.002', 'T1021.003', 'T1021.006', 'T1027.001', 'T1027.002', 'T1027.004', 'T1027', 'T1030', 'T1033', 'T1036.003', 'T1036.004', 'T1036.005', 'T1036.006', and 'T1036'.

atomic-red-team / atomics / T1547.004 / T1547.004.md

Atomic Red Team doc generat... Generated docs from job=generate-d... 819934c · 2 years ago History

PreviewCodeBlame139 lines (70 loc) · 4.68 KB

RawCopyDownloadMenu

T1547.004 - Winlogon Helper DLL

Description from ATT&CK

Adversaries may abuse features of Winlogon to execute DLLs and/or executables when a user logs in. Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl-Alt-Delete. Registry entries in `HKLM\Software[\Wow6432Node\]\Microsoft\Windows NT\CurrentVersion\Winlogon\` and `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\` are used to manage additional helper programs and functionalities that support Winlogon.(Citation: Cylance Reg Persistence Sept 2013)

Malicious modifications to these Registry keys may cause Winlogon to load and execute malicious DLLs and/or executables. Specifically, the following subkeys have been known to be possibly vulnerable to abuse: (Citation: Cylance Reg Persistence Sept 2013)

- Winlogon\Notify - points to notification package DLLs that handle Winlogon events
- Winlogon\Userinit - points to userinit.exe, the user initialization program executed when a user logs on
- Winlogon\Shell - points to explorer.exe, the system shell executed when a user logs on

Adversaries may take advantage of these features to repeatedly execute malicious code and establish persistence.







Atomic Tests

- [Atomic Test #1 - Winlogon Shell Key Persistence - PowerShell](#)
- [Atomic Test #2 - Winlogon Userinit Key Persistence - PowerShell](#)
- [Atomic Test #3 - Winlogon Notify Key Logon Persistence - PowerShell](#)

Atomic Test #1 - Winlogon Shell Key Persistence - PowerShell

PowerShell code to set Winlogon shell key to execute a binary at logon along with explorer.exe.

Upon successful execution, PowerShell will modify a registry value to execute cmd.exe upon logon/logoff.

- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005
- >  T1039
- >  T1040

Supported Platforms: Windows

auto_generated_guid: bf9f9d65-ee4d-4c3e-a843-777d04f19c38

Inputs:

Name	Description	Type	Default Value
binary_to_execute	Path of binary to execute	Path	C:\Windows\System32\cmd.exe

Attack Commands: Run with powershell !

```
Set-ItemProperty "HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Win
```

Cleanup Commands:

```
Remove-ItemProperty -Path "HKCU:\Software\Microsoft\Windows NT\CurrentVe
```

Atomic Test #2 - Winlogon Userinit Key Persistence - PowerShell

PowerShell code to set Winlogon userinit key to execute a binary at logon along with userinit.exe.

Upon successful execution, PowerShell will modify a registry value to execute cmd.exe upon logon/logoff.

Supported Platforms: Windows

auto_generated_guid: fb32c935-ee2e-454b-8fa3-1c46b42e8dfb

Inputs:

Name	Description	Type	Default Value
binary_to_execute	Path of binary to execute	Path	C:\Windows\System32\cmd.exe

Attack Commands: Run with powershell !

```
Set-ItemProperty "HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Win
```

Cleanup Commands:

```
Remove-ItemProperty -Path "HKCU:\Software\Microsoft\Windows NT\CurrentVe
```

Atomic Test #3 - Winlogon Notify Key Logon Persistence - PowerShell

PowerShell code to set Winlogon Notify key to execute a notification package DLL at logon.

Upon successful execution, PowerShell will modify a registry value to execute atomicNotificationPackage.dll upon logon/logoff.

Supported Platforms: Windows

auto_generated_guid: d40da266-e073-4e5a-bb8b-2b385023e5f9

Inputs:

Name	Description	Type	Default Value
binary_to_execute	Path of notification package to execute	Path	C:\Windows\Temp\atomicNotificationPacka

Attack Commands: Run with powershell!

```
New-Item "HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\No
Set-ItemProperty "HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Win
```

Cleanup Commands:

```
Remove-Item "HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
```