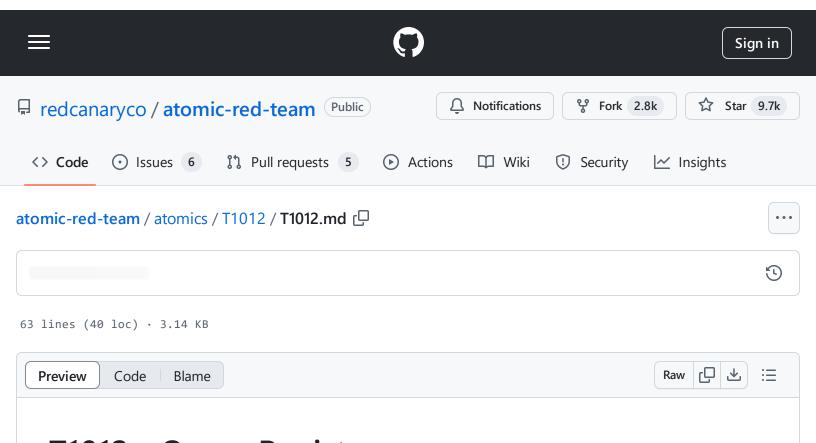
atomic-red-team/atomics/T1012/T1012.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 19:01 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1012/T1012.md



T1012 - Query Registry

Description from ATT&CK

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry) Information can easily be queried using the Reg utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from Query Registry during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Atomic Tests

Atomic Test #1 - Query Registry

atomic-red-team/atomics/T1012/T1012.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 19:01 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1012/T1012.md

Atomic Test #1 - Query Registry

Query Windows Registry. Upon successful execution, cmd.exe will perform multiple reg queries. Some will succeed and others will fail (dependent upon OS). References: https://blog.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search-order https://blog.cylance.com/windows-registry-persistence-part-1-introduction-attack-phases-and-windows-services https://www.handgrep.se/repository/cheatsheets/postexploitation/WindowsPost-Exploitation.pdf https://www.offensive-security.com/wp-content/uploads/2015/04/wp.Registry_Quick_Find_Chart.en_us.pdf

Supported Platforms: Windows

auto_generated_guid: 8f7578c4-9863-4d83-875c-a565573bbdf0

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

```
ſĠ
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows"
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify"
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit"
reg query "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\\Shell"
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\\Shell"
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLow
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
reg query HKLM\system\currentcontrolset\services /s | findstr ImagePath 2>nul | fi
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
```