

Product

▼

Solutions

▼

Resources

▼

Open Source

▼

Enterprise

▼

Pricing

Search

Sign in

Sign up

redcanaryco / atomic-red-team

Public

Notifications

Fork

2.8k

Star

9.7k

<> Code

Issues

6

Pull requests

5

Actions

Wiki

Security

Insights

Files

f339e7d

Go to file

>

.github

>

atomic\_red\_team

▼

atomics

>

Indexes

>

T1003.001

>

T1003.002

>

T1003.003

>

T1003.004

>

T1003.005

>

T1003.006

>

T1003.007

>

T1003.008

>

T1003

>

T1006

>

T1007

>

T1010

▼

T1012

T1012.md

T1012.yaml

>

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

atomic-red-team / atomics / T1012 / T1012.md

CircleCI Atomic Red Team doc...

Generate docs from job=gener...

36d49de · 3 years ago

History

Preview

Code

Blame

63 lines (40 loc) · 3.14 KB

Raw

# 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 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> <http://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](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)

```
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\No
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Us
reg query "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\
```

Page 1 of 2

- >  T1036.006
- >  T1036
- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005

```
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObj
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\Explor
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explor
reg query HKLM\system\currentcontrolset\services /s | findstr ImagePath
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
```