74 lines (31 loc) · 1.96 KB

T1552.002 - Credentials in Registry

Description from ATT&CK

> Adversaries may search the Registry on compromised systems for insecurely stored credentials. The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.
> Example commands to find Registry keys related to password information: (Citation: Pentestlab Stored Credentials)
>
> - Local Machine Hive: `reg query HKLM /f password /t REG_SZ /s`
> - Current User Hive: `reg query HKCU /f password /t REG_SZ /s`

Atomic Tests

- Atomic Test #1 - Enumeration for Credentials in Registry

- Atomic Test #2 - Enumeration for PuTTY Credentials in Registry

Atomic Test #1 - Enumeration for Credentials in Registry

Queries to enumerate for credentials in the Registry. Upon execution, any registry key containing the word "password" will be displayed.

Supported Platforms: Windows

auto_generated_guid: b6ec082c-7384-46b3-a111-9a9b8b14e5e7

Attack Commands: Run with `command_prompt`!

```
reg query HKLM /f password /t REG_SZ /s
reg query HKCU /f password /t REG_SZ /s
```

Atomic Test #2 - Enumeration for PuTTY Credentials in Registry

Queries to enumerate for PuTTY credentials in the Registry. PuTTY must be installed for this test to work. If any registry entries are found, they will be displayed.

Supported Platforms: Windows

auto_generated_guid: af197fd7-e868-448e-9bd5-05d1bcd9d9e5

Attack Commands: Run with `command_prompt`!

```
reg query HKCU\Software\SimonTatham\PuTTY\Sessions /t REG_SZ /s
```