# TTP Detail – T1552.002

## TTP Information

Name: Credentials in Registry

Description: 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: <code>reg query HKLM /f password /t REG\_SZ /s</code>
\* Current User Hive: <code>reg query HKCU /f password /t REG\_SZ /s</code>

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* Agent Tesla
* IceApple
* StrelaStealer
* TrickBot
* Valak

## Tools

* PowerSploit
* Reg

## APTs (Intrusion Sets)

* APT32
* RedCurl