# TTP Detail – T1552.001

## TTP Information

Name: Credentials In Files

Description: Adversaries may search local file systems and remote file shares for files containing insecurely stored credentials. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

It is possible to extract passwords from backups or saved virtual machines through [OS Credential Dumping](https://attack.mitre.org/techniques/T1003).(Citation: CG 2014) Passwords may also be obtained from Group Policy Preferences stored on the Windows Domain Controller.(Citation: SRD GPP)

In cloud and/or containerized environments, authenticated user and service account credentials are often stored in local configuration and credential files.(Citation: Unit 42 Hildegard Malware) They may also be found as parameters to deployment commands in container logs.(Citation: Unit 42 Unsecured Docker Daemons) In some cases, these files can be copied and reused on another machine or the contents can be read and then used to authenticate without needing to copy any files.(Citation: Specter Ops - Cloud Credential Storage)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* Agent Tesla
* Azorult
* BlackEnergy
* Emotet
* Hildegard
* Pysa
* Smoke Loader
* StrelaStealer
* TrickBot
* XTunnel
* jRAT
* pngdowner

## Tools

* AADInternals
* Empire
* LaZagne
* PoshC2
* Pupy
* QuasarRAT

## APTs (Intrusion Sets)

* APT3
* APT33
* Ember Bear
* FIN13
* Fox Kitten
* Indrik Spider
* Kimsuky
* Leafminer
* MuddyWater
* OilRig
* RedCurl
* Scattered Spider
* TA505
* TeamTNT