# TTP Detail – T1555

## TTP Information

Name: Credentials from Password Stores

Description: Adversaries may search for common password storage locations to obtain user credentials.(Citation: F-Secure The Dukes) Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* Agent Tesla
* Astaroth
* Carberp
* CosmicDuke
* DarkGate
* KGH\_SPY
* Lokibot
* Manjusaka
* Matryoshka
* MgBot
* Mispadu
* NETWIRE
* OLDBAIT
* PLEAD
* PinchDuke
* Prikormka
* XLoader

## Tools

* LaZagne
* Mimikatz
* PoshC2
* Pupy
* QuasarRAT

## APTs (Intrusion Sets)

* APT33
* APT39
* APT41
* Evilnum
* FIN6
* HEXANE
* Leafminer
* Malteiro
* MuddyWater
* OilRig
* Stealth Falcon
* Volt Typhoon