# TTP Detail – T1555.003

## TTP Information

Name: Credentials from Web Browsers

Description: Adversaries may acquire credentials from web browsers by reading files specific to the target browser.(Citation: Talos Olympic Destroyer 2018) Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers.

For example, on Windows systems, encrypted credentials may be obtained from Google Chrome by reading a database file, <code>AppData\Local\Google\Chrome\User Data\Default\Login Data</code> and executing a SQL query: <code>SELECT action\_url, username\_value, password\_value FROM logins;</code>. The plaintext password can then be obtained by passing the encrypted credentials to the Windows API function <code>CryptUnprotectData</code>, which uses the victim’s cached logon credentials as the decryption key.(Citation: Microsoft CryptUnprotectData April 2018)

Adversaries have executed similar procedures for common web browsers such as FireFox, Safari, Edge, etc.(Citation: Proofpoint Vega Credential Stealer May 2018)(Citation: FireEye HawkEye Malware July 2017) Windows stores Internet Explorer and Microsoft Edge credentials in Credential Lockers managed by the [Windows Credential Manager](https://attack.mitre.org/techniques/T1555/004).

Adversaries may also acquire credentials by searching web browser process memory for patterns that commonly match credentials.(Citation: GitHub Mimikittenz July 2016)

After acquiring credentials from web browsers, adversaries may attempt to recycle the credentials across different systems and/or accounts in order to expand access. This can result in significantly furthering an adversary's objective in cases where credentials gained from web browsers overlap with privileged accounts (e.g. domain administrator).

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* Agent Tesla
* Azorult
* BLUELIGHT
* Backdoor.Oldrea
* BlackEnergy
* Carberp
* ChChes
* Chaes
* CookieMiner
* CosmicDuke
* Crimson
* Emotet
* Grandoreiro
* H1N1
* Javali
* KGH\_SPY
* KONNI
* KeyBoy
* Lizar
* Lokibot
* Lumma Stealer
* Machete
* Manjusaka
* Melcoz
* MgBot
* Mispadu
* NETWIRE
* OLDBAIT
* Olympic Destroyer
* PLEAD
* PinchDuke
* PoetRAT
* Prikormka
* Proton
* QakBot
* ROKRAT
* Raccoon Stealer
* RainyDay
* RedLeaves
* SUGARDUMP
* Smoke Loader
* TRANSLATEXT
* TSCookie
* TrickBot
* Trojan.Karagany
* Unknown Logger
* WarzoneRAT
* XAgentOSX
* XLoader
* Zebrocy
* jRAT
* njRAT

## Tools

* Empire
* Imminent Monitor
* LaZagne
* Mimikatz
* Pupy
* QuasarRAT
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT3
* APT33
* APT37
* APT41
* APT42
* Ajax Security Team
* FIN6
* HEXANE
* Inception
* Kimsuky
* LAPSUS$
* Leafminer
* Malteiro
* Molerats
* MuddyWater
* OilRig
* Patchwork
* RedCurl
* Sandworm Team
* Stealth Falcon
* TA505
* Volt Typhoon
* ZIRCONIUM