# TTP Detail – T1217

## TTP Information

Name: Browser Information Discovery

Description: Adversaries may enumerate information about browsers to learn more about compromised environments. Data saved by browsers (such as bookmarks, accounts, and browsing history) may reveal a variety of personal information about users (e.g., banking sites, relationships/interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.(Citation: Kaspersky Autofill)

Browser information may also highlight additional targets after an adversary has access to valid credentials, especially [Credentials In Files](https://attack.mitre.org/techniques/T1552/001) associated with logins cached by a browser.

Specific storage locations vary based on platform and/or application, but browser information is typically stored in local files and databases (e.g., `%APPDATA%/Google/Chrome`).(Citation: Chrome Roaming Profiles)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Calisto
* Cuckoo Stealer
* DarkWatchman
* Dtrack
* LightSpy
* Lizar
* Lumma Stealer
* Machete
* Mafalda
* Mispadu
* MobileOrder
* PowerLess
* SUGARDUMP
* Troll Stealer

## Tools

* Empire

## APTs (Intrusion Sets)

* APT38
* Chimera
* Fox Kitten
* Moonstone Sleet
* Scattered Spider
* Volt Typhoon