# TTP Detail – T1189

## TTP Information

Name: Drive-by Compromise

Description: Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including:

\* A legitimate website is compromised, allowing adversaries to inject malicious code
\* Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary
\* Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008))
\* Built-in web application interfaces that allow user-controllable content are leveraged for the insertion of malicious scripts or iFrames (e.g., cross-site scripting)

Browser push notifications may also be abused by adversaries and leveraged for malicious code injection via [User Execution](https://attack.mitre.org/techniques/T1204). By clicking "allow" on browser push notifications, users may be granting a website permission to run JavaScript code on their browser.(Citation: Push notifications - viruspositive)(Citation: push notification -mcafee)(Citation: push notifications - malwarebytes)

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or a particular region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise)

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. The user may be required to assist in this process by enabling scripting, notifications, or active website components and ignoring warning dialog boxes.
3. Upon finding a vulnerable version, exploit code is delivered to the browser.
4. If exploitation is successful, the adversary will gain code execution on the user's system unless other protections are in place. In some cases, a second visit to the website after the initial scan is required before exploit code is delivered.

Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## Kill Chain Phases

**•** mitre-attack: initial-access

## Malware

* Bad Rabbit
* Bundlore
* Grandoreiro
* IcedID
* KARAE
* LoudMiner
* POORAIM
* REvil
* Snip3
* SocGholish

## APTs (Intrusion Sets)

* APT19
* APT28
* APT32
* APT37
* APT38
* Andariel
* Axiom
* BRONZE BUTLER
* CURIUM
* Daggerfly
* Dark Caracal
* Darkhotel
* Dragonfly
* Earth Lusca
* Elderwood
* Lazarus Group
* Leafminer
* Leviathan
* Machete
* Magic Hound
* Mustard Tempest
* PLATINUM
* PROMETHIUM
* Patchwork
* RTM
* Threat Group-3390
* Transparent Tribe
* Turla
* Windigo
* Windshift
* Winter Vivern