# TTP Detail – T1203

## TTP Information

Name: Exploitation for Client Execution

Description: Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility.

Several types exist:

### Browser-based Exploitation

Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed.

### Office Applications

Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run.

### Common Third-party Applications

Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Agent Tesla
* Bankshot
* Cobalt Strike
* DealersChoice
* EvilBunny
* HAWKBALL
* InvisiMole
* Ramsay
* SUPERNOVA
* SpeakUp
* VersaMem
* Woody RAT
* XLoader
* Xbash

## APTs (Intrusion Sets)

* APT12
* APT28
* APT29
* APT3
* APT32
* APT33
* APT37
* APT41
* Andariel
* Aoqin Dragon
* Axiom
* BITTER
* BRONZE BUTLER
* BlackTech
* Cobalt Group
* Confucius
* Darkhotel
* Dragonfly
* EXOTIC LILY
* Elderwood
* Ember Bear
* Higaisa
* Inception
* Lazarus Group
* Leviathan
* MuddyWater
* Mustang Panda
* OilRig
* Patchwork
* Saint Bear
* Sandworm Team
* Sea Turtle
* Sidewinder
* TA459
* The White Company
* Threat Group-3390
* Tonto Team
* Transparent Tribe
* Tropic Trooper
* admin@338