# TTP Detail – T1211

## TTP Information

Name: Exploitation for Defense Evasion

Description: Adversaries may exploit a system or application vulnerability to bypass security features. Exploitation of a vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Vulnerabilities may exist in defensive security software that can be used to disable or circumvent them.

Adversaries may have prior knowledge through reconnaissance that security software exists within an environment or they may perform checks during or shortly after the system is compromised for [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001). The security software will likely be targeted directly for exploitation. There are examples of antivirus software being targeted by persistent threat groups to avoid detection.

There have also been examples of vulnerabilities in public cloud infrastructure of SaaS applications that may bypass defense boundaries (Citation: Salesforce zero-day in facebook phishing attack), evade security logs (Citation: Bypassing CloudTrail in AWS Service Catalog), or deploy hidden infrastructure.(Citation: GhostToken GCP flaw)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## APTs (Intrusion Sets)

* APT28
* Velvet Ant