# TTP Detail – T1583.008

## TTP Information

Name: Malvertising

Description: Adversaries may purchase online advertisements that can be abused to distribute malware to victims. Ads can be purchased to plant as well as favorably position artifacts in specific locations online, such as prominently placed within search engine results. These ads may make it more difficult for users to distinguish between actual search results and advertisements.(Citation: spamhaus-malvertising) Purchased ads may also target specific audiences using the advertising network’s capabilities, potentially further taking advantage of the trust inherently given to search engines and popular websites.   
  
Adversaries may purchase ads and other resources to help distribute artifacts containing malicious code to victims. Purchased ads may attempt to impersonate or spoof well-known brands. For example, these spoofed ads may trick victims into clicking the ad which could then send them to a malicious domain that may be a clone of official websites containing trojanized versions of the advertised software.(Citation: Masquerads-Guardio)(Citation: FBI-search) Adversary’s efforts to create malicious domains and purchase advertisements may also be automated at scale to better resist cleanup efforts.(Citation: sentinelone-malvertising)   
  
Malvertising may be used to support [Drive-by Target](https://attack.mitre.org/techniques/T1608/004) and [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), potentially requiring limited interaction from the user if the ad contains code/exploits that infect the target system's web browser.(Citation: BBC-malvertising)  
  
Adversaries may also employ several techniques to evade detection by the advertising network. For example, adversaries may dynamically route ad clicks to send automated crawler/policy enforcer traffic to benign sites while validating potential targets then sending victims referred from real ad clicks to malicious pages. This infection vector may therefore remain hidden from the ad network as well as any visitor not reaching the malicious sites with a valid identifier from clicking on the advertisement.(Citation: Masquerads-Guardio) Other tricks, such as intentional typos to avoid brand reputation monitoring, may also be used to evade automated detection.(Citation: spamhaus-malvertising)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: resource-development

## Malware

* Raspberry Robin

## APTs (Intrusion Sets)

* Mustard Tempest