# TTP Detail – T1102.001

## TTP Information

Name: Dead Drop Resolver

Description: Adversaries may use an existing, legitimate external Web service to host information that points to additional command and control (C2) infrastructure. Adversaries may post content, known as a dead drop resolver, on Web services with embedded (and often obfuscated/encoded) domains or IP addresses. Once infected, victims will reach out to and be redirected by these resolvers.

Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Use of a dead drop resolver may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: command-and-control

## Malware

* Astaroth
* BADNEWS
* BLACKCOFFEE
* CharmPower
* Grandoreiro
* Javali
* KEYPLUG
* Metamorfo
* MiniDuke
* PlugX
* PolyglotDuke
* RTM
* TRANSLATEXT
* Xbash

## APTs (Intrusion Sets)

* APT41
* BRONZE BUTLER
* Kimsuky
* Patchwork
* RTM
* Rocke