# TTP Detail – T1102

## TTP Information

Name: Web Service

Description: Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites, cloud services, 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, Microsoft, or Twitter, makes it easier for adversaries to hide in expected noise.(Citation: Broadcom BirdyClient Microsoft Graph API 2024) Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Use of Web services 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

* BADHATCH
* Bazar
* BoomBox
* Bumblebee
* CHIMNEYSWEEP
* Carbon
* CharmPower
* DarkTortilla
* Doki
* DropBook
* GuLoader
* Hildegard
* Latrodectus
* NETWIRE
* Nightdoor
* Raspberry Robin
* SMOKEDHAM
* SharpStage
* ShrinkLocker
* Sibot
* Snip3
* SocGholish
* WhisperGate

## Tools

* Brute Ratel C4
* ngrok

## APTs (Intrusion Sets)

* APT32
* APT42
* EXOTIC LILY
* FIN6
* FIN8
* Fox Kitten
* Gamaredon Group
* Inception
* LazyScripter
* Mustang Panda
* RedCurl
* Rocke
* TeamTNT
* Turla