# TTP Detail – T1016.001

## TTP Information

Name: Internet Connection Discovery

Description: Adversaries may check for Internet connectivity on compromised systems. This may be performed during automated discovery and can be accomplished in numerous ways such as using [Ping](https://attack.mitre.org/software/S0097), <code>tracert</code>, and GET requests to websites.

Adversaries may use the results and responses from these requests to determine if the system is capable of communicating with their C2 servers before attempting to connect to them. The results may also be used to identify routes, redirectors, and proxy servers.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* DarkTortilla
* GoldFinder
* More\_eggs
* NKAbuse
* Neoichor
* QakBot
* QuietSieve
* Rising Sun
* SUGARUSH
* SysUpdate
* Woody RAT

## APTs (Intrusion Sets)

* APT29
* FIN13
* FIN8
* Gamaredon Group
* HAFNIUM
* HEXANE
* Lotus Blossom
* Magic Hound
* TA2541
* Turla
* Volt Typhoon