# TTP Detail – T1505.003

## TTP Information

Name: Web Shell

Description: Adversaries may backdoor web servers with web shells to establish persistent access to systems. A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to access the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server.(Citation: volexity\_0day\_sophos\_FW)

In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (e.g. [China Chopper](https://attack.mitre.org/software/S0020) Web shell client).(Citation: Lee 2013)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

## Malware

* ASPXSpy
* BUSHWALK
* China Chopper
* FRAMESTING
* GLASSTOKEN
* LIGHTWIRE
* Line Runner
* Neo-reGeorg
* OwaAuth
* P.A.S. Webshell
* PULSECHECK
* RAPIDPULSE
* SEASHARPEE
* SLIGHTPULSE
* STEADYPULSE
* SUPERNOVA
* SnappyTCP
* WIREFIRE
* reGeorg

## APTs (Intrusion Sets)

* APT28
* APT29
* APT32
* APT38
* APT39
* APT5
* Agrius
* BackdoorDiplomacy
* BlackByte
* CURIUM
* Deep Panda
* Dragonfly
* Ember Bear
* FIN13
* Fox Kitten
* GALLIUM
* HAFNIUM
* Kimsuky
* Leviathan
* Magic Hound
* Moses Staff
* OilRig
* Sandworm Team
* Sea Turtle
* Threat Group-3390
* Tonto Team
* Tropic Trooper
* Volatile Cedar
* Volt Typhoon