# TTP Detail – T1014

## TTP Information

Name: Rootkit

Description: Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Rootkits are programs that hide the existence of malware by intercepting/hooking and modifying operating system API calls that supply system information. (Citation: Symantec Windows Rootkits)

Rootkits or rootkit enabling functionality may reside at the user or kernel level in the operating system or lower, to include a hypervisor, Master Boot Record, or [System Firmware](https://attack.mitre.org/techniques/T1542/001). (Citation: Wikipedia Rootkit) Rootkits have been seen for Windows, Linux, and Mac OS X systems. (Citation: CrowdStrike Linux Rootkit) (Citation: BlackHat Mac OSX Rootkit)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* COATHANGER
* Carberp
* Caterpillar WebShell
* Drovorub
* Ebury
* HIDEDRV
* Hacking Team UEFI Rootkit
* HiddenWasp
* Hikit
* Hildegard
* Line Dancer
* LoJax
* PoisonIvy
* Ramsay
* Skidmap
* Stuxnet
* Umbreon
* Uroburos
* WarzoneRAT
* Winnti for Linux
* Zeroaccess

## Tools

* HTRAN

## APTs (Intrusion Sets)

* APT28
* APT41
* Rocke
* TeamTNT
* Winnti Group