# TTP Detail – T1554

## TTP Information

Name: Compromise Host Software Binary

Description: Adversaries may modify host software binaries to establish persistent access to systems. Software binaries/executables provide a wide range of system commands or services, programs, and libraries. Common software binaries are SSH clients, FTP clients, email clients, web browsers, and many other user or server applications.  
  
Adversaries may establish persistence though modifications to host software binaries. For example, an adversary may replace or otherwise infect a legitimate application binary (or support files) with a backdoor. Since these binaries may be routinely executed by applications or the user, the adversary can leverage this for persistent access to the host. An adversary may also modify a software binary such as an SSH client in order to persistently collect credentials during logins (i.e., [Modify Authentication Process](https://attack.mitre.org/techniques/T1556)).(Citation: Google Cloud Mandiant UNC3886 2024)  
  
An adversary may also modify an existing binary by patching in malicious functionality (e.g., IAT Hooking/Entry point patching)(Citation: Unit42 Banking Trojans Hooking 2022) prior to the binary’s legitimate execution. For example, an adversary may modify the entry point of a binary to point to malicious code patched in by the adversary before resuming normal execution flow.(Citation: ESET FontOnLake Analysis 2021)  
  
After modifying a binary, an adversary may attempt to [Impair Defenses](https://attack.mitre.org/techniques/T1562) by preventing it from updating (e.g., via the `yum-versionlock` command or `versionlock.list` file in Linux systems that use the yum package manager).(Citation: Google Cloud Mandiant UNC3886 2024)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

## Malware

* BFG Agonizer
* BOLDMOVE
* BUSHWALK
* Bonadan
* Ebury
* FRAMESTING
* Industroyer
* Kessel
* Kobalos
* LIGHTWIRE
* LITTLELAMB.WOOLTEA
* SLOWPULSE
* ThiefQuest
* WARPWIRE
* WIREFIRE
* XCSSET

## APTs (Intrusion Sets)

* APT5