# TTP Detail – T1091

## TTP Information

Name: Replication Through Removable Media

Description: Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.

Mobile devices may also be used to infect PCs with malware if connected via USB.(Citation: Exploiting Smartphone USB ) This infection may be achieved using devices (Android, iOS, etc.) and, in some instances, USB charging cables.(Citation: Windows Malware Infecting Android)(Citation: iPhone Charging Cable Hack) For example, when a smartphone is connected to a system, it may appear to be mounted similar to a USB-connected disk drive. If malware that is compatible with the connected system is on the mobile device, the malware could infect the machine (especially if Autorun features are enabled).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: lateral-movement

**•** mitre-attack: initial-access

## Malware

* ANDROMEDA
* Agent.btz
* CHOPSTICK
* Conficker
* Crimson
* DustySky
* Flame
* H1N1
* QakBot
* Ramsay
* Raspberry Robin
* SHIPSHAPE
* Stuxnet
* USBStealer
* USBferry
* Unknown Logger
* Ursnif
* njRAT

## APTs (Intrusion Sets)

* APT28
* Aoqin Dragon
* Darkhotel
* FIN7
* LuminousMoth
* Mustang Panda
* Tropic Trooper