# TTP Detail – T1584.008

## TTP Information

Name: Network Devices

Description: Adversaries may compromise third-party network devices that can be used during targeting. Network devices, such as small office/home office (SOHO) routers, may be compromised where the adversary's ultimate goal is not [Initial Access](https://attack.mitre.org/tactics/TA0001) to that environment -- instead leveraging these devices to support additional targeting.

Once an adversary has control, compromised network devices can be used to launch additional operations, such as hosting payloads for [Phishing](https://attack.mitre.org/techniques/T1566) campaigns (i.e., [Link Target](https://attack.mitre.org/techniques/T1608/005)) or enabling the required access to execute [Content Injection](https://attack.mitre.org/techniques/T1659) operations. Adversaries may also be able to harvest reusable credentials (i.e., [Valid Accounts](https://attack.mitre.org/techniques/T1078)) from compromised network devices.

Adversaries often target Internet-facing edge devices and related network appliances that specifically do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar)

Compromised network devices may be used to support subsequent [Command and Control](https://attack.mitre.org/tactics/TA0011) activity, such as [Hide Infrastructure](https://attack.mitre.org/techniques/T1665) through an established [Proxy](https://attack.mitre.org/techniques/T1090) and/or [Botnet](https://attack.mitre.org/techniques/T1584/005) network.(Citation: Justice GRU 2024)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: resource-development

## APTs (Intrusion Sets)

* APT28
* Leviathan
* Volt Typhoon
* ZIRCONIUM