# TTP Detail – T1020.001

## TTP Information

Name: Traffic Duplication

Description: Adversaries may leverage traffic mirroring in order to automate data exfiltration over compromised infrastructure. Traffic mirroring is a native feature for some devices, often used for network analysis. For example, devices may be configured to forward network traffic to one or more destinations for analysis by a network analyzer or other monitoring device. (Citation: Cisco Traffic Mirroring)(Citation: Juniper Traffic Mirroring)

Adversaries may abuse traffic mirroring to mirror or redirect network traffic through other infrastructure they control. Malicious modifications to network devices to enable traffic redirection may be possible through [ROMMONkit](https://attack.mitre.org/techniques/T1542/004) or [Patch System Image](https://attack.mitre.org/techniques/T1601/001).(Citation: US-CERT-TA18-106A)(Citation: Cisco Blog Legacy Device Attacks)

Many cloud-based environments also support traffic mirroring. For example, AWS Traffic Mirroring, GCP Packet Mirroring, and Azure vTap allow users to define specified instances to collect traffic from and specified targets to send collected traffic to.(Citation: AWS Traffic Mirroring)(Citation: GCP Packet Mirroring)(Citation: Azure Virtual Network TAP)

Adversaries may use traffic duplication in conjunction with [Network Sniffing](https://attack.mitre.org/techniques/T1040), [Input Capture](https://attack.mitre.org/techniques/T1056), or [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) depending on the goals and objectives of the adversary.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: exfiltration