# TTP Detail – T1040

## TTP Information

Name: Network Sniffing

Description: Adversaries may passively sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data.

Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol. Techniques for name service resolution poisoning, such as [LLMNR/NBT-NS Poisoning and SMB Relay](https://attack.mitre.org/techniques/T1557/001), can also be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary.

Network sniffing may reveal configuration details, such as running services, version numbers, and other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for subsequent [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and/or [Defense Evasion](https://attack.mitre.org/tactics/TA0005) activities. Adversaries may likely also utilize network sniffing during [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) (AiTM) to passively gain additional knowledge about the environment.

In cloud-based environments, adversaries may still be able to use traffic mirroring services to sniff network traffic from virtual machines. 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) Often, much of this traffic will be in cleartext due to the use of TLS termination at the load balancer level to reduce the strain of encrypting and decrypting traffic.(Citation: Rhino Security Labs AWS VPC Traffic Mirroring)(Citation: SpecterOps AWS Traffic Mirroring) The adversary can then use exfiltration techniques such as Transfer Data to Cloud Account in order to access the sniffed traffic.(Citation: Rhino Security Labs AWS VPC Traffic Mirroring)

On network devices, adversaries may perform network captures using [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `monitor capture`.(Citation: US-CERT-TA18-106A)(Citation: capture\_embedded\_packet\_on\_software)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: discovery

## Malware

* Emotet
* FoggyWeb
* J-magic
* JumbledPath
* Line Dancer
* MESSAGETAP
* Penquin
* Regin
* VersaMem
* cd00r

## Tools

* Empire
* Impacket
* NBTscan
* PoshC2
* Responder

## APTs (Intrusion Sets)

* APT28
* APT33
* DarkVishnya
* Kimsuky
* Salt Typhoon
* Sandworm Team
* Velvet Ant