Traffic Signaling: Socket Filters, Sub-technique T1205.002 - Enterprise

Archived: 2026-04-05 17:54:50 UTC

Adversaries may attach filters to a network socket to monitor then activate backdoors used for persistence or command and control. With elevated permissions, adversaries can use features such as the `libpcap` library to open sockets and install filters to allow or disallow certain types of data to come through the socket. The filter may apply to all traffic passing through the specified network interface (or every interface if not specified). When the network interface receives a packet matching the filter criteria, additional actions can be triggered on the host, such as activation of a reverse shell.

To establish a connection, an adversary sends a crafted packet to the targeted host that matches the installed filter criteria.[1] Adversaries have used these socket filters to trigger the installation of implants, conduct ping backs, and to invoke command shells. Communication with these socket filters may also be used in conjunction with Protocol Tunneling.[2][3]

Filters can be installed on any Unix-like platform with `libpcap` installed or on Windows hosts using `Winpcap`. Adversaries may use either `libpcap` with `pcap_setfilter` or the standard library function `setsockopt` with `SO_ATTACH_FILTER` options. Since the socket connection is not active until the packet is received, this behavior may be difficult to detect due to the lack of activity on a host, low CPU overhead, and limited visibility into raw socket usage.

Source: https://attack.mitre.org/techniques/T1205/002