Socket-filter trigger → on-host raw-socket activity → reverse connection (T1205.002), Detection Strategy DET0162

Archived: 2026-04-05 12:48:56 UTC

AN0462

Adversary installs/uses packet-capture or raw-socket capability (WinPcap/Npcap, wpcap/packet DLLs or raw socket attach) and sets a filter. A crafted inbound packet is observed; within a short window the host process that loaded capture libraries initiates an outbound connection (e.g., reverse shell) to the packet origin.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Seconds to correlate inbound trigger → process library load/driver start → outbound connect (default 120s).
CaptureLibIndicators	DLL/driver names to match (wpcap.dll, packet.dll, npcap.sys, npf.sys) – extend for EDR drivers in your fleet.
AllowedInstallers	Signed/expected processes allowed to install/start Npcap (software distribution tools).
ReversePorts	Likely egress ports to watch after trigger (4444, 53, 80/443, 8080, high ephemeral).

AN0463

Process creates a raw/packet socket and attaches a (e)BPF filter (setsockopt SO_ATTACH_FILTER/ATTACH_BPF or bpf(BPF_PROG_LOAD)). Immediately after a matching inbound packet, the same process binds/connects outward to a remote host (reverse shell or beacon).

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	socket(AF_PACKET|AF_INET, SOCK_RAW, *), setsockopt(… SO_ATTACH_FILTER|SO_ATTACH_BPF …), bpf(cmd=BPF_PROG_LOAD), open/openat path="/dev/bpf*" (BSD/macOS-like) or setcap cap_net_raw.

Data Component	Name	Channel
Network Connection Creation (DC0082)	linux:osquery	family=AF_PACKET or protocol raw; process name not in allowlist.
Network Traffic Content (DC0085)	NSM:Flow	Rare inbound packet characteristics (ICMP/UDP/TCP to uncommon port) from src_ip followed ≤TimeWindow by outbound SF from same host to src_ip.

Mutable Elements

Field	Description
UserContext	Flag raw-socket activity outside privileged daemons (root-only by default).
MinPayloadEntropy	If using packet content (Zeek), treat high-entropy single-packet triggers as suspicious.
AFPacketAllowList	System services allowed to open AF_PACKET (dhclient, keepalived, LLDP, monitoring agents).

AN0464

Process opens /dev/bpf* (libpcap) or loads NetworkExtension filter, then after a crafted inbound packet the same process initiates an outbound connection to the trigger origin.

Log Sources

Mutable Elements

Field	Description
BPFDevicePath	Alternate BPF device paths if customized (default /dev/bpf*).
DeveloperMode	Relax thresholds on known developer tooling hosts (Xcode, instrumenting tools).
