Detection Strategy for Reflection Amplification DoS (T1498.002), Detection Strategy DET0408

Archived: 2026-04-05 13:59:07 UTC

AN1140

Outbound spoofed traffic to known amplification protocols (e.g., DNS, NTP, Memcached) combined with abnormal network traffic volume targeting remote reflectors, resulting in disproportionate traffic returned to a victim

Log Sources

Mutable Elements

Field	Description
TimeWindow	Interval for measuring sudden outbound spike or volume pattern
AmplificationProtocolPorts	List of known ports used for reflection amplification (e.g., 53/DNS, 123/NTP, 11211/Memcached)
PacketToByteRatio	Heuristic threshold where the response volume far outweighs the request volume

AN1141

Spoofed outbound packets sent to amplification services from command-line tools or scripts, combined with abnormal outbound packet volume on known reflector ports

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	auditd:SYSCALL	Execution of spoofing tools (e.g., hping3, nping, scapy) sending UDP packets to known amplifier ports
Network Traffic Flow (DC0078)	NSM:Flow	Outbound UDP floods targeting common reflection services with spoofed IP headers
Host Status (DC0018)	sar:network	Outbound network saturation with minimal process activity

Mutable Elements

Field	Description
TimeWindow	Sliding interval for detecting volumetric anomalies
AmplificationProtocolList	Which protocols to watch (e.g., DNS, NTP, SSDP, Memcached)
ExecutionToolList	Set of binaries and scripts commonly abused for spoofing/reflection

AN1142

Command-line initiated UDP traffic bursts to external reflection amplification ports using built-in scripting or binaries with network anomalies

Log Sources

Mutable Elements

Field	Description
ReflectionPorts	Ports known for reflection abuse — DNS, NTP, SSDP, Memcached
TrafficSpikeThreshold	How much deviation in outbound traffic constitutes a suspicious spike

AN1143

Cloud-hosted VM or container generates spoofed UDP requests to third-party services on known amplifier ports, with high outbound-to-inbound traffic ratios in VPC Flow Logs

Log Sources

Mutable Elements

Field	Description
EgressRulePorts	Cloud security group rules permitting UDP to reflector protocols
OutboundToInboundRatio	Ratio threshold to flag traffic as potential reflection behavior
VMInstanceTagContext	Cloud metadata that can help scope anomalous behavior to development, testing, or external-facing services

---