4.4

Tuesday, September 26, 2023 7:10 PM

Compromised host pings another host
periodically

may indicate a trap
when corresponding pings fail
this can trigger malicious
process

DLP can deny offending users access
to original file

encrypt file in place

quarantine

blocking file = no copying

blackholes - locations in net that
discard/drop incoming/out messages

blackholes locations

discard/drop incoming/out messages

without noti source

isolate attacker

Sinkhole routing - DOS traffic flooding

IP routes to another for anal

segmentation

honeynet = segmentation

Sandbox = isolation

Applocker - Windows protection against

unwanted software and helps w/

Standardization