Detect Forced SMB/WebDAV Authentication via lure files and outbound NTLM, Detection Strategy DET0022

Archived: 2026-04-05 18:29:28 UTC

AN0065

Adversary stages a lure that references a remote resource (e.g., LNK/SCF/Office template). When the user opens/renders the file or a shell enumerates icons, the host automatically attempts SMB or WebDAV authentication to the attacker host. The chain is: (1) lure file is created or modified in a user-exposed location → (2) user or system accesses the lure → (3) host makes outbound NTLM (SMB 139/445 or WebDAV over 80/443) to an untrusted destination → (4) repeated attempts from multiple users/hosts or from privileged workstations.

Log Sources

Mutable Elements

Field	Description
UserLocations	Folders where lures are most effective (Desktop, Public, Downloads, Temp, Cache, Start Menu, Startup). Adjust to enterprise layout.
LureExtensions	File types commonly abused (.lnk, .scf, .url, .doc/.xls/.ppt/.pdf/.html). Extend for your tooling and languages.
UntrustedCIDR/DNS	Org-specific list of external/unknown networks or domains; used to suppress sanctioned file servers and WebDAV gateways.
TimeWindow	Correlation horizon (e.g., 15–30 minutes) between file access and outbound NTLM attempt.
WorkstationZones	Asset/zone tags that distinguish workstations from servers; helps flag workstation→workstation SMB, which is often abnormal.
OfficeTemplatePaths	Paths to Office templates to catch template injection references and abnormal loads.