VEILLE TECHNOLOGIQUE • SÉCURISATION D'ACTIVE DIRECTORY — FICHE 3

Le ransomware PAYLOAD paralyse un domaine via GPO sans chiffrer

Date de la veille : 21 septembre 2026

L'analyse publiée par Kaspersky en septembre 2026 revient sur une attaque marquante survenue en avril contre un parc Windows. Après être entré via un VPN FortiGate grâce à un compte compromis sans MFA, l'attaquant a obtenu les droits d'administrateur du domaine et créé une simple GPO malveillante nommée **PAYLOAD**, liée à la racine de l'annuaire.

La particularité de cet incident est qu'aucun malware ni logiciel de chiffrement n'a été déposé sur les postes clients. Au redémarrage, la stratégie de groupe a suffi à afficher la demande de rançon, bloquer le compte administrateur local et désactiver le pare-feu Windows, tandis que les données étaient exfiltrées depuis les serveurs de fichiers.

Cet incident montre que les GPO sont devenues une arme redoutable pour les cybercriminels : comme il s'agit d'une fonction légitime d'Active Directory, les EDR classiques ne détectent rien. La parade passe avant tout par le **MFA** sur les accès distants, la séparation des droits de gestion des GPO et la surveillance des modifications dans `SYSVOL` (événements 5136 à 5141).

SOURCES

- Kaspersky (Securelist) — *PAYLOAD ransomware attacks through Active Directory GPO* (21 sept. 2026)
- Help Net Security — *Sophos Active Adversary Report 2026* (27 fév. 2026)