Forensic APT Downgrade Part 1

28 juin 202527 JUILLET

Shutlock2025

Créé par : JOL

Logo

Forensic APT Part 1

Raisonner sur la pertinence du scénario APT & le vecteur d'attaque

1. Vecteur initial : hameçonnage social / événementiel
   L'adresse Proton est masquée derrière une invitation à un spectacle – technique classique de spear-phishing culturel. Le courriel contient/renvoie vers le script tirage_aux_sorts.sh, que la victime enregistre puis exécute.

2. Dropper & persistance
   Le script écrit (ou remplace) le fragment /etc/apt/apt.conf.d/50appstream.
   Pourquoi APT ? — en plaçant des directives Acquire:: truquées, l'agent force APT à récupérer ultérieurement un paquet ou une archive factice signée par l'attaquant. Rien n'est lancé immédiatement : le code reste dormant, attendant la prochaine mise à jour pour s'implanter discrètement (typique d'un APT qui recherche persistance basse visibilité).

3. Charge utile différée
   Les entrées icons-128x128@2.tar / icons-64x64@2.tar servent d'identifiants « courriels » uniquement pour contourner des parseurs et n'ont aucune légitimité dans une conf APT ; elles redirigeront vers un dépôt tiers au moment voulu.

4. Indicateurs d'attaque & attribution

   - Proton Mail → chiffrement, anonymat
   - Adresse "star_wars_official" → thème du leurre (spectacle / théâtre)
   - Altération d'APT : signature d'un malware déjà référencé dans divers rapports (modus operandi identique : agent dormant inséré via configuration APT ou PAM, puis payload lors d'une mise à jour).

En résumé, tout converge :

- Fichier malveillant (dropper) → écrit/altère configuration APT → déclenche infection différée lors d'une future mise-à-jour automatique, le tout introduit par un phishing culturel émanant de star_wars_official@proton.me.

Ces quatre indicateurs fournissent la chaîne complète : point de contact → vecteur → dropper → persistance.