Une fois rentré, il rebondit

Phase 3 sur 4. La phase la plus longue. La plus visible si on sait regarder.

Propagation

Mouvement latéral. Escalade de privilèges. Ciblage des sauvegardes. Plusieurs semaines, parfois mois.

1 Mouvement latéral

Il utilise le compte compromis pour se connecter aux serveurs de fichiers, AD, sauvegardes.

2 Escalade de privilèges

Il essaie de devenir admin du domaine. Quand il y arrive, il peut tout faire.

3 Persistance

Comptes cachés, scripts au démarrage, backdoors. Il peut revenir même après reset MDP.

4 Ciblage sauvegardes

Sa cible n°1 une fois admin. S'il les chiffre aussi, vous payez la rançon.

Supervision vs Journalisation

Supervision

Contrôle temps réel. Quand un seuil est franchi (élévation privilège, scan interne), alerte immédiate.

Journalisation

Stockage historique. Analyse a posteriori. Identifie les causes profondes après incident.

> **Sans supervision, l'attaque démarre en silence et dure des mois. Sans journalisation, on rouvre les mêmes portes.**

3 moyens de couper

EDR centralisé

Détecte les mouvements latéraux. Pas un antivirus — un EDR/XDR moderne.

Segmentation VLAN

Entre postes utilisateurs et serveurs critiques.

Sauvegardes immutables

Hors site, hors domaine. Que le hacker ne peut pas chiffrer.

R.I.P. en 4 phases

Une attaque cyber suit un parcours prévisible. À chaque étape, il existe un moyen de la couper.

R

Reconnaissance

Limiter expo · monitoring leaks

I

Intrusion

MFA · EDR · patch mensuel

P

Propagation

Vous êtes ici

†

Impact

Sauvegardes testées · plan crise

La semaine prochaine
Le RIP final

Comment ça finit quand on n'a rien coupé avant. Et comment ne **jamais en arriver là**.

Et concrètement chez vous ?

Diagnostic 2h sur place sans engagement

Tél +41 78 811 92 21

Email eric.darien@abaxinfo.com

Web diagnostic.abaxinfo.com