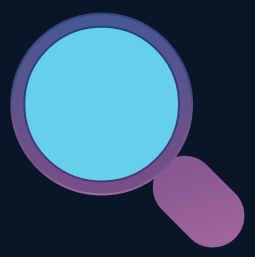

Avant de vous attaquer, il passe 1 à 3 semaines à vous observer

Phase 1 sur 4. La phase silencieuse. La plus longue à comprendre a posteriori.

Reconnaissance

Phase silencieuse. Aucun pop-up. Aucune alerte. Le hacker cartographie pendant que vous travaillez.

5 angles d'observation

Tout est public. Tout est gratuit. Tout est automatisable.

1 **Votre site web**

Liste des collaborateurs, sous-domaines oubliés, technologies utilisées, versions exposées.

2 **Vos profils LinkedIn**

DAF, RH, IT, nouvelles recrues. Croisé avec des bases publiques pour obtenir leurs emails.

3 **Vos ports ouverts**

Scan complet de votre IP publique. Ports 22, 80, 443, 3389. Bannières d'identification.

4 Vos fuites passées

Bases de credentials volés (Collection #1, breaches récents). Si un collaborateur a réutilisé un MDP, il le sait.

5 Vos sous-traitants

Le maillon faible. Un fournisseur compromis avec vos accès = supply chain attack.

> **Vous ne voyez rien. C'est la phase la plus silencieuse — et la plus longue à reconstituer a posteriori.**

3 moyens de couper

Une attaque qui n'arrive pas à passer la phase R coûte 0 € à votre PME.

Limiter l'exposition

Sous-domaines, équipe, ports inutiles fermés.

Monitoring des leaks

Surveillance bases de credentials volés pour vos emails pro.

Sensibilisation

Tout ce qu'on publie sur LinkedIn renseigne un attaquant.

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

Vous êtes ici

I

Intrusion

MFA · EDR · patch mensuel

P

Propagation

EDR centralisé · segmentation

†

Impact

Sauvegardes testées · plan crise

La semaine prochaine
Phase 2 — Intrusion

Par où le hacker rentre vraiment dans votre système. Les **4 voies d'entrée** qu'on retrouve dans 9 attaques sur 10.

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