● ALERTE — URGENT

Campagne de phishing massive ciblant les sociétés utilisatrices de Microsoft 365 au Sénégal

La semaine dernière a été particulièrement chargée pour nos équipes : audit, conseil et accompagnement cyber de plusieurs clients et partenaires victimes d'une vague d'attaques de phishing. Point commun entre toutes les victimes identifiées : ce sont des sociétés utilisatrices de Microsoft 365.

CIBLE	VECTEUR	IMPACT
Entreprises sous Microsoft 365	Lien de partage SharePoint piégé	Vol de session & propagation

01 Mode opératoire

Le mode opératoire est bien connu. Il se déroule en plusieurs étapes, chacune visant à prendre le contrôle du compte tout en restant invisible pour l'utilisateur légitime.

1. **Le mail d'hameçonnage**
   La victime reçoit un e-mail contextualisé contenant un fichier partagé via SharePoint : facture, documents comptables, preuves d'audit, contrats…

2. **Le vol de la session**
   Lorsque la victime mord à l'hameçon et ouvre le lien, on lui demande de s'authentifier, puis de valider le second facteur, et enfin d'accorder une délégation OAuth2. L'attaquant récupère ainsi une session valide à la place de l'utilisateur légitime.

3. **La dissimulation**
   Une règle de suppression automatique des messages reçus est créée, afin que l'utilisateur légitime ne reçoive pas les alertes par e-mail.

4. **La propagation**
   Le même procédé est ensuite utilisé contre l'ensemble des contacts de la victime, placés en copie cachée (Cci) — et qui deviennent à leur tour victimes du phishing.

Pourquoi c'est dangereux : l'authentification multifacteur (MFA) ne suffit pas ici. En accordant la délégation OAuth2, la victime donne elle-même à l'attaquant un accès valide à sa messagerie.

02 Mesures de remédiation

Si votre organisation est touchée, voici les premières actions à mener sans attendre :

Bloquer

Suspendre temporairement l'envoi de courriers pour toutes les adresses identifiées comme compromises.

Réinitialiser

Réinitialiser l'ensemble des mots de passe et révoquer toutes les sessions en cours.

Rétablir

Réactiver l'envoi des e-mails une fois les comptes assainis.

Prévenir

Contacter l'ensemble des destinataires (en Cci) pour leur signaler l'incident.

Ne pas cliquer

Ne pas réutiliser le mail contenant le lien malveillant, toujours actif : une simple capture d'écran suffit pour le signaler.

Sensibiliser

Sensibiliser l'ensemble des collaborateurs de l'entreprise à ce type d'attaque.

Surveiller

Surveiller via le SOC les journaux (logs) et tout comportement anormal de la messagerie de l'ensemble des utilisateurs.