Fiche réflexe

Compte M365 non privilégié compromis par hameçonnage
« *X a partagé un fichier avec vous* »

Objectif : Garantir une réaction rapide lorsqu'un compte Microsoft 365 compromis procède à un envoi massif d'e-mails incitant les destinataires à ouvrir un fichier partagé via OneDrive. À l'ouverture du document, la victime est redirigée vers une fausse page d'authentification Microsoft 365 destinée à collecter ses identifiants, entraînant la compromission de nouveaux comptes et la propagation exponentielle de l'attaque selon ce même mode opératoire.

Acteur : Administrateur du Tenant M365

Penser à conserver l'original des preuves (emails, fichier créé, logs...) pour les transmettre à Breizh Cyber à des fins d'investigations.

Etape 1	Désactiver le compte compromis ;
Etape 2	Forcer la déconnexion du compte sur l'ensemble des appareils ;
Etape 3	Réinitialiser le mot de passe avec un mot de passe fort et unique, sur un périphérique de confiance ;
Etape 4	Activer l'authentification multifacteurs ;
Etape 5	Faire une copie locale du fichier déposé dans l'espace OneDrive pour conservation des preuves et supprimer immédiatement ce fichier partagé ;
Etape 6	Contrôler et supprimer toutes les règles de messagerie suspectes ;
Etape 7	Contrôler les applications tierces installées sur le client de messagerie ;
Etape 8	Réactiver le compte de l'utilisateur ;
Etape 9	Communiquer en interne pour identifier d'autres comptes compromis ; Si la licence le permet, consulter l'audit des fichiers ouverts via Purview->Audit pour identifier les comptes ayant eu accès au fichier malveillant. Renouveler les étapes 1 à 8 sur les comptes identifiés.
Etape 10	Extraire les logs EntraID (Audit, Sign-In) ;
Etape 11	Déclarer l'incident auprès de Breizh Cyber via le formulaire suivant : https://breizhcyber.bzh/declarer-un-incident/ ou contacter Breizh Cyber au 0800 200 008.