Usurpation d’identité procédure

Connexion Exchange

Vérification que le même mail a été envoyé à d’autres utilisateur > phishing

Connexion aux centre d’administration O365

Déconnexion et reset du mot de passe > garder les informations

Connexion à ENTRA

Vérification des journaux de connexion

Vérifier dans les journaux les connexions interactives suspectes (depuis l'étranger, IP …)

Dans applications

On peut voir certaines application suspectes comme Perfectdata software > on peut voir les privilèges graph accordés.

Des concentrement utilisateurs peuvent être donnés > cliquer sur afficher les autorisation octroyées.

Masquer la visibilité de l’application

Application > application d’entreprise > Permettre aux utilisateurs la connexion & décocher toutes les case pour empêcher la propagation

Supprimer l’application et si impossible > script en Shell

Mise en place de la MFA dans l’ancienne interface

Utilisateur > MFA par utilisateur > activer et appliquer

Configuration avec l’utilisateur

Déconnexion des appareil mobile depuis l’OWA

Suppression des règles de courrier suspectes

Désactiver le SMTP authentifié

Sur le poste > analyse anti-virus

Revision #1
Created 25 November 2024 12:52:05 by Johann
Updated 25 November 2024 12:54:34 by Johann