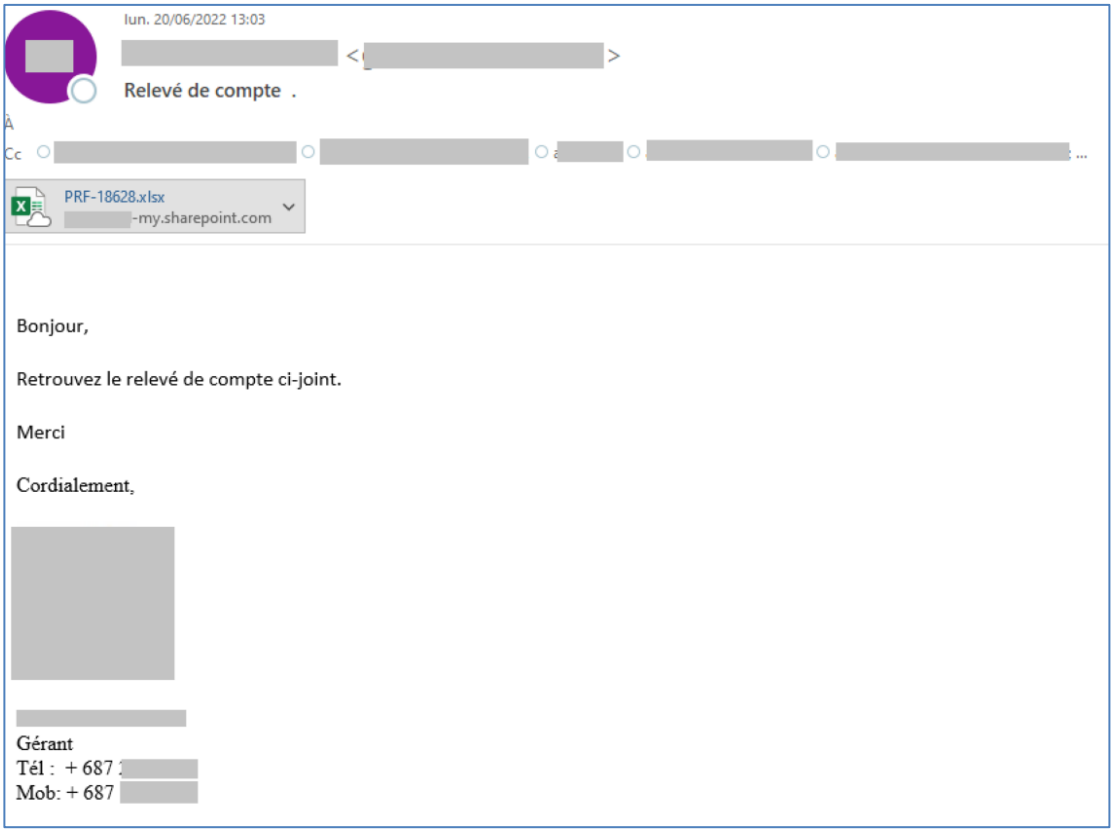
ATTAQUE DE PHISHING

Jour et heure du début	Lundi 20 juin 2022 à 13:03
Organisation	Fonds Interprofessionnel d'Assurance Formation (FIAF)
Nature de l'incident	Attaque par phishing ayant pour conséquence la compromission du compte Office 365 de l'employé.
Conséquences	Compromission du compte de l'employé et utilisation de ce compte pour envoyer des mails de phishing à ses destinataires.

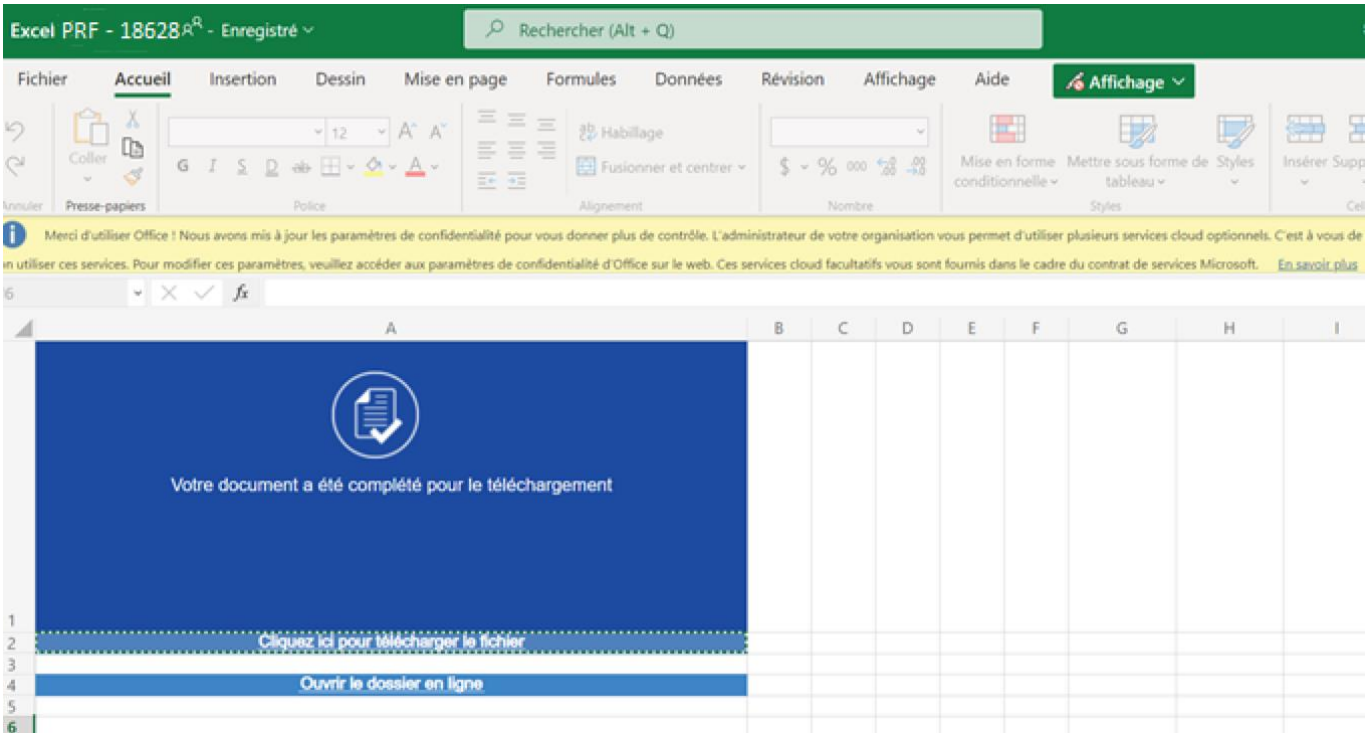
1. Déroulement de l'incident

Le lundi 20 juin 2022 à 13 :03, l'employé reçoit un mail intitulé « Relevé de compte. ». L'expéditeur de ce mail est un client basé en Nouvelle Calédonie. C'est un client usuel de la société et il n'y a rien d'inhabituel à recevoir des mails de sa part.



L'employé se dit légèrement surpris que le relevé de compte soit un document Sharepoint plutôt qu'une pièce jointe mais ouvre cependant le document.

Dans le document Excel, certaines cases affichent un message invitant à télécharger du contenu externe.



L'employé ne se souvient pas clairement des actions réalisées à partir de ce moment, mais indique l'apparition d'un pop-up invitant à entrer ses identifiants.

L'employé suspecte avoir commis une erreur, mais n'observe aucune conséquence immédiate et ne notifie pas l'événement immédiatement au prestataire informatique qui est en déplacement en métropole.

Le lendemain, l'employé est contacté par téléphone par des clients qui indiquent avoir reçu de sa part des mails suspects. L'employé contacte alors son prestataire Informatique qui confirme que le compte a été corrompu.

> « Nous avons été alertés d'une probable corruption d'un de vos comptes Microsoft en date du 21/06/2022 à 7h53. Le compte présente le rapport suivant :
>
> - Courriers suspects au cours des dernières 24 heures : 434
>
> - Nombre total de courriers sortants au cours des dernières heures : 547
>
> - Pourcentage de courriers suspects : 79 %
>
> - L'envoi de messages sortants a été restreint pour le compte d'utilisateur le 21/06/2022 à 8h00 »
>
> Le prestataire informatique

2. Actions en remédiation

Le prestataire informatique intervient le 21 juin et réalise les actions suivantes :

- Réinitialisation du mot de passe du compte
- Déconnexion forcée de toutes les sessions Office 365
- Vérification du transfert de courrier : désactivé
- Vérification des règles de boîte de réception : Suppression d'une règle douteuse sans nom.

- Déblocage du compte afin d'autoriser à nouveau l'envoi de message vers des adresses extérieures à l'organisation

En termes de communication externe, un mail est fait à la clientèle de l'entreprise pour les informer de la compromission. Par ailleurs, lors des réunions clients, une communication sur l'incident leur est faite.

Enfin, le DPO fait une déclaration à la CNIL le 21 juin.

3. Renseignements complémentaires

3.1. Gestion informatique

L'informatique est complètement externalisée à un prestataire externe. La fonction de DPO (Data Protection Officer) est aussi assurée par un prestataire externe.

3.2. Office365 et authentification forte (MFA)

La société victime utilise la suite Office365 et avait mis en place une authentification forte depuis plusieurs mois. L'authentification forte n'a cependant pas empêché la compromission du compte.

3.3. Description du mail reçu

Le mail reçu provient d'un expéditeur de confiance (client de l'entreprise) et son sujet et son contenu (logo de l'entreprise et signature du mail) sont cohérents. Il n'y a pas de faute de Français dans le mail.

Le mail ne contient pas de destinataire mais une longue liste de personnes (en tout 489 personnes dont l'employé victime) en sont en copie.

L'entête du mail ne présente aucun élément particulier et le mail respecte les règles d'authentification (DMARC=pass, DKIM=pass, SPF=pass).

3.4. Le document Excel (Sharepoint)

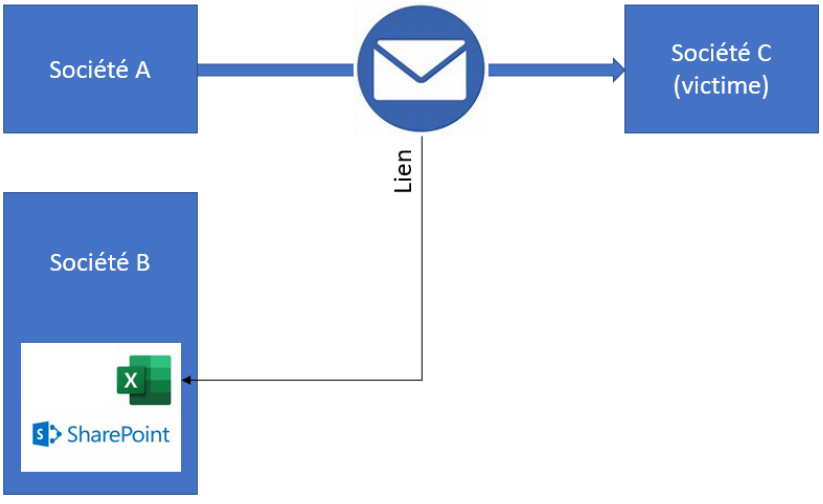
Celui-ci est accessible via le lien suivant :

https://societeB-my.sharepoint.com/:x/g/personal/societeB/EeNE5lWlhkpJkoG14GB7-IkB37eNCsEedtH8bzMTwMWpLQ

Il s'agit d'un document présent sur le Sharepoint d'une société tierce (société B). Cette société basée en Nouvelle Calédonie est aussi cliente de la société victime.

Contactée cette autre société a indiqué aussi avoir fait l'objet d'une attaque similaire quelques jours auparavant.

La société B ignorait cependant l'existence de ce document sur son Sharepoint. Elle a pu procéder à un « scan » de son Sharepoint et a identifié 2 documents Sharepoint qui ont été effacés le lundi 04 juillet.



4. Conclusion et enseignements

Cette attaque de phishing utilise la technique d'ingénierie sociale et d'usurpation d'identité : un compte de confiance (un client de l'entreprise) dont le compte est compromis est utilisé pour compromettre de nouveaux comptes.

Le mail de phishing est particulièrement réaliste car l'expéditeur du mail est donc un client de cette entreprise et le mail reprend la charte graphique du client. Il n'y a pas non plus de faute de Français qui aurait pu indiquer un risque.

Trois signaux « faibles » auraient cependant pu attirer l'attention de l'employé :

1. Le mail n'est pas ciblé vers un destinataire mais est diffusé largement (489 destinataires)
2. Le document est hébergé sur le Sharepoint d'une société tierce (société B) et non pas par celui de l'émetteur du mail.
3. Le document joint est un document Sharepoint et non une pièce jointe (point relevé par l'employé) comme habituellement avec ce client. Il est toutefois à noter que de plus en plus de sociétés utilisent Sharepoint et qu'il n'est plus rare d'avoir des liens Sharepoint dans des mails.

Une fois la compromission détectée, la société victime a réagi rapidement et a pris des actions de nature à arrêter la propagation de cette attaque (réinitialisation du compte compromis, communication à ses clients).

Il est à noter que le document Sharepoint n'a été effacé que le 04 juillet soit une quinzaine de jours après la compromission. La société B ignorait d'ailleurs l'existence de ce document.

Enseignements :

- **La formation faite aux employés pour reconnaitre des mails de phishing doit évoluer pour permettre aux employés une meilleure reconnaissance**. Les critères classiques de reconnaissance (expéditeur inconnu, adresse email incorrecte ou encore fautes d'orthographes) ne sont plus suffisants.

- Lors d'une compromission ou tentative de compromission d'un compte Office365, il est important de **« scanner » le Sharepoint pour s'assurer que des documents qui pourraient servir à propager une nouvelle attaque soient effacés**.