COMPTE RENDU D'INCIDENT
GROUPE CONFLUENT

APICEM SARL
Développement et exploitation des outils APICRYPT®
sous le contrôle de l'association APICEM
www.apicrypt.org

3, Route de Bergues
CS 20 007
F-59412 COUDEKERQUE Cedex 2
Tél. +33(0)3 28 63 00 65
mail : infoapicrypt@apicrypt.org

SARL au capital de 8 000 € - RCS DUNKERQUE 439 752 353

TABLE DES MATIERES

1 OBJET

L'objet du présent document est de présenter le compte rendu détaillé de l'incident dénommé « Campagne de Phishing[1] du Groupe Confluent ».

2 INTRODUCTION

Le 26 juin 2019, nous vous avons adressé une information importante concernant une attaque informatique ciblant le Groupe Confluent de Nantes.

Nous tenons aujourd'hui à vous apporter, en toute transparence, des éléments complémentaires au sujet de cette attaque et notamment vous faire part des mesures qu'il convient de prendre.

3 GENESE DE L'INCIDENT :

La cyberattaque ciblant le Groupe Confluent a eu pour effet la compromission d'un certain nombre de comptes de messageries internes du Groupe Confluent.

Cette compromission aura permis à l'attaquant, non identifié à l'heure actuelle, de prendre le contrôle total de plusieurs boîtes de messagerie du Groupe Confluent et d'envoyer plusieurs campagnes massives d'email de Phishing.

La première campagne massive d'email s'est produite le 14 mai 2019.

L'APICEM a détecté, a posteriori, un volume inhabituel de messages en provenance d'une adresse email du Groupe Confluent et à destination de plusieurs centaines d'utilisateurs APICRYPT.

L'APICEM, suspectant un Spam, a pris contact avec le Groupe Confluent afin de rappeler la charte d'utilisation de la messagerie APICRYPT.

Le Groupe confluent s'est engagé à respecter et faire respecter cette charte par ses utilisateurs.

Le 18 juin 2019, l'APICEM a détecté, à nouveau, un volume inhabituel de messages en provenance d'une adresse email du Groupe Confluent destinés à plusieurs centaines d'utilisateurs APICRYPT.

L'APICEM suspectant un Spam et donc une récidive de la part d'un utilisateur du Groupe Confluent a pris, une fois encore, contact avec le Groupe Confluent afin de les en informer et de les mettre en demeure de respecter et faire respecter la charte d'utilisation de la messagerie APICRYPT. Le Groupe Confluent s'y est, à nouveau, engagé.

Le 24 juin, une adresse email du Groupe Confluent émettait, une nouvelle fois, un email à destination de plusieurs centaines d'utilisateurs APICRYPT.

La Direction de l'APICEM prend alors contact avec la Direction des Systèmes d'Information (DSI) du Groupe Confluent afin de trouver une solution à ce problème récurrent.

C'est à cette occasion que le Groupe Confluent informe l'APICEM de la survenue d'une attaque informatique sur ses systèmes. L'attaque aurait débuté avant la première campagne d'emails non désirés du 14 mai.

Le 25 juin 2019, compte tenu de la gravité de l'incident et du nombre d'utilisateurs de la messagerie APICRYPT concernés, l'APICEM prend la décision d'activer sa cellule de crise.

[1] Cf. Article 5 - Informations complémentaires

À cette occasion, l'APICEM prend la décision :

- De mettre en œuvre une mesure de filtrage et de contrôle des flux de messagerie du Groupe Confluent ;
- De procéder à une déclaration d'incident de sécurité informatique sur le portail https://signalement.social-sante.gouv.fr ;
- D'adresser à ses utilisateurs impactés une communication urgente visant à les informer de l'incident en cours et des mesures à prendre ;
- De coordonner ses actions avec la DSI du Groupe Confluent.

Le même jour, la DSI du Groupe Confluent faisait part à l'APICEM des mesures mises en œuvre sur leur système de messagerie visant à circonvenir les attaques. L'APICEM décide néanmoins de maintenir sa mesure de surveillance jusqu'à la semaine suivante.

Le 3 juillet, la DSI du Groupe Confluent informe l'APICEM que la situation est stabilisée.

Le 5 juillet, en l'absence de nouveau email frauduleux, la cellule de crise de l'APICEM décide de lever la mesure de surveillance des flux du Groupe Confluent.

Cette action de contrôle, plusieurs heures de vérification manuelle par jour, était réalisée par un technicien APICRYPT et représentait un coût quotidien important que l'APICEM ne pouvait maintenir sur le long terme.

Le 9 juillet, l'APICEM détecte à nouveau un envoi massif d'emails destinés à 3 500 utilisateurs APICRYPT. Les ¾ de ces correspondances seront néanmoins stoppés par la direction technique de l'APICEM avant de parvenir aux destinataires.

La mesure de surveillance des flux est immédiatement remise en œuvre le 9 juillet par l'APICEM et la coordination étroite avec la DSI du Groupe Confluent est relancée.

L'APICEM informe alors le Groupe Confluent qu'une solution doit être trouvée rapidement si possible avec l'aide d'un intervenant tiers.

Le Groupe Confluent fait intervenir son prestataire informatique qui prendra contact avec l'APICEM, le 10 juillet, afin de l'informer de la décision du Groupe Confluent de couper les accès de messagerie externes du Groupe Confluent. Cette mesure permet de stopper immédiatement l'attaque et toute tentative ultérieure.

Le 12 juillet, en l'absence d'équipe dédiée des pouvoirs publics, et de moyens, autant humains que réglementaires, pour procéder à un audit du Groupe Confluent, la cellule de crise de l'APICEM prend la décision d'agréer le plan d'action du Groupe Confluent et de lever la mesure de filtrage des flux. Les mesures correctives prises pour circonvenir l'attaque semblent, en effet, adéquates d'un point de vue technique et chronologique.

La cellule de crise de l'APICEM est clôturée le 18 juillet. Le RSSI de l'APICEM poursuivra, en revanche, la coordination avec la DSI du Groupe Confluent jusqu'à la fin de l'exécution du plan d'action correctif.

4 ASSISTANCE AUX UTILISATEURS :

Pour l'APICEM, il s'est agi de trouver une solution pour assister et protéger les utilisateurs, destinataires du message de Phishing, et en particulier ceux qui auraient ouvert le message et cliqué sur le lien contenu dans celui-ci.

Bien que l'attaque sur le Groupe Confluent semble exclusivement destinée au piratage des comptes email du Groupe Confluent, nous ne pouvons avoir la certitude que dans certains cas cette attaque ne se traduit pas par l'installation d'un virus sur le poste des destinataires.

La mission de la cellule cyber de l'ASIP Santé est en revanche limitée à l'accompagnement des structures de santé dans la résolution d'incidents de sécurité conformément au décret n° 2016-1214 du 12 septembre 2016.

L'accompagnement des éditeurs de logiciels ainsi que l'audit des structures de santé ne font pas partie des attributions de la cellule cyber.

Concernant les utilisateurs destinataires de ces messages frauduleux, nos recommandations sont les suivantes :

- Si vous n'avez pas ouvert le lien se trouvant dans le message :
  - Vous pouvez supprimer ce message de votre boîte de réception puis de votre corbeille.
- Si vous avez ouvert le lien se trouvant dans le message :
  - Vous pouvez lancer une analyse antivirale si vous disposez d'un logiciel antivirus ou faire intervenir votre prestataire informatique pour que celui-ci puisse lancer une analyse antivirale.
- Si vous avez ouvert le lien se trouvant dans le message et renseigné des identifiants :
  - Vous devez changer ces identifiants (renouvellement du mot de passe) et vous pouvez lancer une analyse antivirale si vous disposez d'un logiciel antivirus ou faire intervenir votre prestataire informatique pour que celui-ci puisse lancer une analyse antivirale.

En cas de difficulté, nous vous invitons à contacter :

- Le service informatique du Groupe Confluent par mail : informatique.du.confluent@groupeconfluent.fr

  Ou
- L'assistance téléphonique de l'APICEM qui se tient à votre disposition de du lundi au vendredi de 8h à 19h et le samedi de 9h à 12h (hors jours fériés) au +33 (0)3 28 63 00 65.

5 INFORMATIONS COMPLEMENTAIRES :

Le Phishing (ou encore hameçonnage) est une technique dite de "social engineering" ayant pour but de dérober à des individus leurs identifiants de connexion et mots de passe ou leurs numéros de carte bancaire. Le Phishing est considéré comme une forme de Spam.

Dans la pratique, vous recevez un email de votre banque, d'un fournisseur d'accès internet, ou de la direction des services informatiques vous demandant de mettre à jour vos informations bancaires ou vos identifiants de connexion. Cet email comporte un lien vous dirigeant vers une page à l'aspect sécurisé, identique à celles que vous avez déjà vues maintes fois. On vous demande alors de confirmer vos informations personnelles (identifiant, n° de compte bancaire, mot de passe, etc.) perdues suite à une erreur interne ou pour d'autres raisons... Il est alors trop tard, les pirates ont vos données ! Une fois vos identifiants de comptes et mots de passe en pochent, les malfaiteurs n'auront plus qu'à se servir ou à les revendre.

Dans le cadre de l'attaque du Groupe Confluent, certains utilisateurs du Groupe Confluent ont reçu sur leur adresse de messagerie interne un email prétextant la saturation de la boîte email de l'utilisateur et l'invitant à se connecter à son compte pour modifier ses paramètres.

Quelques dizaines d'utilisateurs se sont fait prendre au piège et ont donné leurs identifiants de compte de messagerie. Les pirates ont alors pu exploiter les boîtes aux lettres des utilisateurs et leur carnet d'adresses pour propager l'attaque à d'autres adresses email tel que des adresses de l'Espace de confiance MSSanté, des adresses APICRYPT, mais aussi des adresses de messagerie non dédiée aux échanges en santé.