FICHE REFLEXE PHISHING

CELLULE SOC

Août 2024

Version	Date	Propriétaire	Rédacteur / Autorité
1.0	XX/08/2024	Cellule SOC	Nicolas Clerbout
Finale			

Table des matières

1 – Récupération de mail suspect

Il existe plusieurs sources possibles de signalement de mails suspects. Parmi celles-ci, on trouve notamment les suivantes.

Veille informationnelle.

Les différentes procédures de veille, menées notamment par l'équipe d'Analyse de la Menace Cyber, peuvent mettre en lumière des campagnes de phishing en cours menant à la détection de mails suspects.

Alertes des outils de sécurité.

Les différents outils de sécurité peuvent avoir été préalablement configurés pour repérer les campagnes de phishing déjà connues à travers d'indicateurs dont on surveille proactivement la présence. Des alertes sont alors créées dans les outils de surveillance tels que le SIEM (*Security Information and Event Management*) ou l'EDR (*Endpoint Detection and Response*).

Signalement direct par l'utilisateur.

Une autre source très commune dans la détection de campagne de phishing est le signalement par un ou plusieurs utilisateurs de mails ayant provoqué leur méfiance.

Il faut dans le cas de ce type de source noter les points suivants :

- Pour une meilleure efficacité, il est nécessaire que les utilisateurs aient été sensibilisés aux risques associés au phishing, à la nécessité de faire ce type de signalement et aux canaux de communication adéquats pour le faire ;
- Comme les utilisateurs ne sont a priori pas des experts du phishing, il peut y avoir une part non négligeable de faux positifs en particulier dus à la confusion entre simple spam commercial et mails effectivement malveillants.

2 – Analyse du mail suspect

Analyse visuelle du mail

A ce premier stade d'analyse, il n'y a **pas d'interaction** avec le mail : c'est une phase limitée à l'observation.

Remarque : On peut réaliser tout ou partie de cette analyse visuelle sur le mail tel qu'il apparaît dans le client email, ou sur sa version brute. Pour cela on utilise la fonctionnalité « `Voir l'original` » (le nom de la fonctionnalité peut varier d'un client email à l'autre).

Dans l'analyse purement visuelle, il s'agit de relever les éléments suivants :

- Quel est le nom d'expéditeur affiché ? Quelle est l'adresse mail de l'expéditeur ? Y a-t-il une incongruence entre les deux ?

Exemple d'incongruence : le nom affiché est « ups.france » mais le nom de domaine dans l'adresse mail est clairement différent.

- Quels sont les destinataires visibles ?
- A quelles date et heure le mail a-t-il été reçu ?
- Quel est l'intitulé (sujet) du mail ?
- Y-a-t-il une pièce jointe ?

Corps du mail

- Le corps du mail présente-t-il uniquement du texte, ou y-a-t-il des éléments visibles de formatage html ?
    - Liens, images, etc.
- Observer le texte :
    - Y-a-t-il des fautes grossières de grammaire ou d'orthographe ?
    - Y-a-t-il des tournures étranges de phrase ?
    - Y-a-t-il une injonction à réaliser une action de la part du destinataire (cliquer sur un lien, ouvrir une pièce jointe, etc.)

- Le texte tente-t-il de provoquer un sentiment d'urgence ou d'autres émotions pour pousser le destinataire à réaliser une action ?

Dans cet exemple, le mail n'est évidemment pas du texte brut et il s'agit en fait d'une unique image à laquelle un lien est attaché. A noter dans la capture d'écran précédente le sujet du mail cherchant à provoquer un sentiment d'urgence (« ou [la commande] sera annulée »).

A ce stade, on doit avoir un certain nombre d'éléments préliminaires qui permettent de décider les étapes suivantes. On doit pouvoir notamment déterminer si on a affaire à un spam ou à un mail de phishing potentiel. Par exemple :

- Grande liste de destinataires + pas d'incohérence dans les noms de domaine et/ou pas de lien à cliquer ni de pièce jointe + message à caractère publicitaire : on est très probablement face à un spam (indésirable mais non dangereux) ;
- Texte tentant de manipuler les émotions pour cliquer ou télécharger quelque chose + tournures et orthographe défaillantes + incohérences dans les noms de domaine : on est très probablement face à une tentative de phishing.

N.B. : parfois il n'est pas facile de faire immédiatement la différence. Les autres phases d'analyse ci-dessous servent alors à reconnaître la nature malveillante ou simplement indésirable du mail.

Analyse des en-têtes du mail

Pour cette phase d'analyse, on travaille sur le message « brut » via l'option « `Voir l'original` » ou « `Voir le code source` ». On peut réaliser cette analyse manuellement ou en utilisant un outil tel que MXToolBox (https://mxtoolbox.com/) ou PhishTool. L'utilisation d'un environnement de Sandbox est recommandée.

Principaux éléments à étudier :

« `From` »	Contient l'adresse mail de l'expéditeur
« `X-Originating-IP` » (ou à défaut « `Received` »)	Contient l'adresse IP de l'expéditeur
« `Delivered To` »	Contient les adresses des destinataires. Penser à vérifier la présence de champs tels que « `CC` » ou « `BCC` » pour les destinataires en copie
« `Reply-To` » et/ou « `Return-Path` »	Adresses email qui seront utilisées pour répondre au mail analysé
« `Date` »	Date et heure
« `Authentication-Results` »	Contient les résultats des vérifications SPF et DKIM avec les valeurs `dkim=…` et `spf=…` Contient aussi le nom de domaine de l'expéditeur avec la valeur `smtp.mailfrom=…` (ou `header.from=…`)
« `Content-Type` »	Indique par exemple si le mail contient du code html. En cas de présence de pièce jointe, ce champ indiquera également le nom de la pièce jointe et on trouvera également le champ « Content-Disposition: attachment »

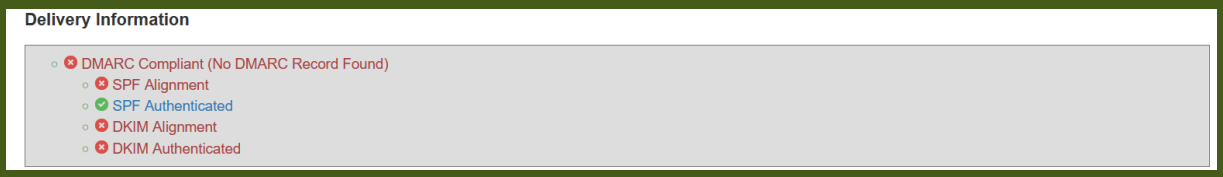
Rappels :

SPF = *Sender Policy Framework* ; standard utilisé pour vérifier qu'un serveur mail est effectivement autorisé à envoyer un mail pour un domaine donné.

DKIM = *DomainKeys Identified Mail* ; utilisé également pour l'authentification des mails y compris lors d'une chaîne de « forwarding ».

Le standard DMARC (*Domain-Based Message Authentication, Reporting and Conformance*) est utilisé pour contraster les résultats de SPF et DKIM

avec le contenu du mail. La plupart des outils d'analyse d'en-têtes ont comme fonctionnalité de contrôler le résultat DMARC :



Exemple avec MXToolBox

Analyse d'une url

Pour cette partie, il est nécessaire d'utiliser un environnement de Sandbox adapté. De plus, il faut éviter de cliquer sur les liens.

On commence toujours par simplement placer le curseur sur un lien pour voir l'url visée s'afficher (généralement en bas de la fenêtre). Dans un deuxième temps on peut **copier** l'url pour mener les investigations décrites ci-dessous.

Si l'url est raccourcie (« `bit.ly` », « `tiny.url` » et autres) : Il faut dans ce cas utiliser un outil pour découvrir premièrement la vraie url cachée derrière cette forme raccourcie. Un exemple d'outil en ligne pour cela : https://unshorten.it.

Ensuite, on peut utiliser différents outils de CTI (*Cyber Threat Intelligence* : Recherches sur les Menaces Cyber) pour vérifier la réputation et la dangerosité de l'url à étudier :

- https://urlscan.io : présenté comme « une sandbox pour le web », cet outil scanne et analyse les sites web.
- https://urlhaus.abuse.ch : une base de données d'url utilisées pour la diffusion de malwares.
- https://talosintelligence.com/reputation_center : un outil de recherche pour vérifier entre autres choses la réputation des url.

Analyse d'une pièce jointe

Pour cette analyse, il est également nécessaire de travailler dans un environnement de Sandbox.

L'analyse statique consiste à rassembler autant d'informations que possible sur la pièce jointe sans déclencher de potentielle charge malveillante (donc, en particulier, sans ouvrir la pièce jointe). On travaille quand même en Sandbox pour pallier un éventuel déclenchement accidentel.

L'analyse dynamique consiste à déclencher volontairement une potentielle charge malveillante pour en observer les effets en direct. Il est évident qu'il faut travailler dans un environnement nettement séparé du reste du Système d'Information (SI) de l'entreprise. A noter qu'il existe des solutions comme https://any.run pour réaliser ce genre d'analyse dynamique.

Analyse Statique

On peut au minimum récupérer le hash de la pièce jointe et effectuer une recherche CTI sur des plateformes comme le Talos Intelligence Reputation Center ou VirusTotal (https://virustotal.com).

Ces plateformes proposent souvent des rapports librement accessibles sur les fichiers identifiés comme malveillants.

Remarque : on peut également chercher à débusquer la charge malveillante d'une pièce jointe (avec des outils comme la suite `Oledump`, la commande `strings`, etc.). On peut travailler à la rendre lisible si nécessaire (déobfuscation) et analyser le code.

Analyse dynamique

Il s'agit de déclencher la charge potentiellement malveillante volontairement et dans un environnement correctement séparé du reste du SI.

On observe alors les effets du fichier, par exemple via des outils de capture de trafic réseau comme Wireshark ou de monitoring de l'activité du système.

Comme déjà évoqué, il existe par ailleurs des plateformes comme Any Run ou Hybrid Analysis (https://www.hybrid-analysis.com) qui proposent de réaliser ce genre d'analyse dynamique, et ont souvent une fonctionnalité de préparation d'un rapport sur les activités observées.

3 – Réponse et remédiation

Analyser l'impact d'une campagne de phishing

Le but est de déterminer à quel point la campagne de phishing s'est étendue (qui a été ciblé), à quel point elle a été efficace (combien de pièces jointes et url malveillantes ont été ouvertes) et quelles sont les conséquences néfastes (à quel point un utilisateur peut être compromis).

Les investigations décrites dans la section précédente ont permis de rassembler un certain nombre d'IoCs (*Indicator of Compromission*) :

- Adresses mail ;
- Noms de domaines et adresses IPs ;
- URLs ;
- Noms de fichiers et hash ;
- Etc.

On peut utiliser ces indicateurs et les différents outils de sécurité pour comprendre l'étendue de la campagne de phishing :

- SIEM :
  - Mails provenant d'adresses suspectes ; pièces jointes et url ;
  - Connexions vers URLs et IPs malveillantes.

  Les sources principales à surveiller sont les logs du serveur mail et les logs de surveillance de connexions réseau : pare-feu, proxy, IDS/IPS (*Intrusion Detection System*/*Intrusion Prevention System*)

- EDR :
  - Téléchargement et/ou exécution de fichiers suspects ;

    Création de nouveaux fichiers et processus, détection de hashs.

  On peut se reporter à la fiche réflexe sur la détection de binaires malveillants sous Wazuh.

Dans chaque cas, on relève les actifs impactés et notamment les machines (noms d'hôtes, IPs internes) et les comptes utilisateurs.

Si le cas se présente, on peut déterminer le niveau de compromission en étudiant les actifs concernés de manière plus approfondie en analysant notamment :

- Capture de trafic réseau ;
- Dump de la RAM ;
- Clonage des disque durs ;

Actions à mener pour écarter la menace

En cas de compromission avérée il faut immédiatement escalader à l'équipe de Réponse à Incident qui appliquera les plans d'actions pertinents, incluant notamment :

- Isoler les machines affectées du réseau,
- Invalider les tokens d'identification et réinitialiser les mots de passe,
- Supprimer les fichiers malveillants et leurs effets sur les machines infectées.

Dans tous les cas il faudra communiquer sur l'incident et appliquer certaines actions techniques pour réduire proactivement le risque de compromission future.

Communication :

- Informer les utilisateurs impactés : pour expliquer les risques et surtout rappeler les bonnes pratiques à appliquer (envoyer les documents de prévention liés au phishing) ;
- Rédiger un rapport d'incident ;
- Mettre à jour la documentation et notamment la base de données d'IoCs ;
- Contacter les équipes techniques pertinentes pour appliquer les mesures techniques que l'analyste ne peut pas mettre en place lui-même.

Mesures techniques :

- Mettre à jour les listes noires des différents équipements réseau (pare-feu, proxy, IDS/IPS, filtres DNS…) pour empêcher les connexions vers les IPs et URLs malveillantes ;
- Mettre à jour la *liste noire du serveur mail* pour filtrer / supprimer les mails provenant des adresses malveillantes identifiées ou contenant les URLs et pièces jointes identifiées ;
- Mettre à jour les équipements de sécurité des terminaux (antivirus, etc) pour détecter les fichiers malveillants identifiés.

Enfin, il faudra sans doute participer à l'organisation et la tenue d'événements de sensibilisation qui auront été planifiés après cette alerte.