Agir contre une attaque par hameçonnage

*Fiche à l'attention des **responsables de la sécurité des systèmes d'information***

Objectifs de l'attaque

Récupérer des informations sensibles pour accéder à des comptes (messagerie, administration, etc…) et qui serviront à des fins illégales (spam, intrusion, fraude, etc…)

La technique de **l'hameçonnage** (phishing) consiste à usurper l'identité d'un tiers légitime dans le but d'obtenir des informations sensibles. Elle est basée sur l'utilisation de la messagerie électronique, de SMS et des portails Web. Une fiche de sensibilisation est disponible sur le portail **cybermalveillance.gouv.fr** .

Mesures de détection

Surveiller l'espace de quarantaine de la messagerie qui peut permettre d'identifier des campagnes de pourriels en cours

Mettre en place un module sur le client de messagerie permettant de remonter les courriels suspects au responsable sécurité (avec l'entête et tous les éléments nécessaires)

Surveiller les logs du proxy (blocage urlhaus, téléchargements suspects, url complexe accédée sans aucun referer...)

Surveiller les connexions d'adresse IP étrangères et les tentatives de force brute sur le webmail (analyser les logs permettant d'identifier l'utilisateur ciblé pour vérifier avec lui s'il n'a pas été victime d'un phishing)

Surveiller quotidiennement les flux anormaux de réception et d'envoi de courriels, par exemple le « top 20 » des courriels les plus diffusés en réception et en émission, les stats de supervision de la congestion de la file d'attente et les stats DMARC (usurpation du nom de domaine)

Surveiller si l'IP du service d'émission de courriels (smtp sortant) n'est pas black-listée en utilisant le protocole DNS (Black Listing) (DNSBL.net par exemple)

Mesures de réaction

● Comptes de messagerie ●

Désactivation des comptes compromis puis changement des mots de passe

Désactivation temporaire du webmail si tous les comptes compromis ne sont pas identifiés

Vérifier qu'aucune redirection (ou script de redirection) n'a été paramétré

● *Au niveau de la réception (MX)* ●

Filtrer les éléments (atypiques ou uniques) susceptibles de pouvoir être bloqués (corp: uri, ip / entetes: useragent, from, ip émettrice, header spécifique)

Analyser le contenu des courriels **et mettre en place des règles de scoring** basée sur des mots clés

● *Au niveau de l'émission (SMTP)* ●

Bloquer l'émission de messages vers l'attaquant (from & reply to)

● *Au niveau Proxy* ●

Bloquer les tentatives d'accès HOST/IP (la résolution IP de l'host) identifiée comme malveillante (action réalisée sur les flux http & https)

Bloquer les URLs contenant des éléments atypiques (chemin, argument, nom de la page...) (action possible que sur les flux non chiffrés => http)

● *Organisation* ●

Informer les utilisateurs d'une campagne en cours

Si l'attaque provient d'une adresse mail qui semble légitime, **informer l'organisation concernée**