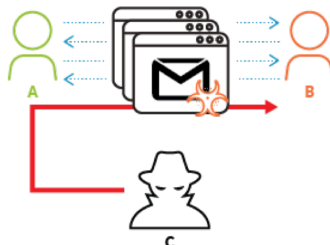
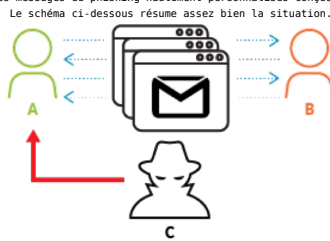


Des chercheurs découvrent une campagne de phishing durant laquelle des conversations authentiques sont détournées, pour diffuser des malwares

x	Des chercheurs découvrent une campagne de phishing durant laquelle des conversations authentiques sont détournées, pour diffuser des malwares
---	---

En mai 2017, l'unité 42 de Palo Alto Networks a identifié une campagne d'hameçonnage limitée baptisée FreeMilk qui a visé différents individus et entités à travers le monde. L'acteur de la menace a exploité la vulnérabilité d'exécution de code à distance CTP-2017-0199 Microsoft Word Office / WordPad avec un contenu soigneusement conçu pour chaque destinataire cible. Les chercheurs de Palo Alto ont expliqué que leur analyse a révélé que les courriels utilisés pendant la campagne portaient sur de multiples comptes de messagerie compromis liés à un domaine légitime en Asie du Nord-Est. « Nous croyons que l'acteur de la menace a détourné une conversation en cours existante et légitime et s'est posé par la suite comme l'expéditeur légitime afin d'envoyer des courriels malveillants de phishing aux destinataires. »

En clair, les chercheurs ont fait valoir que des hackers ont été en mesure d'intercepter des conversations légitimes par courrier électronique entre les individus et les ont détournées. L'objectif était de diffuser des logiciels malveillants vers les réseaux d'entreprise en utilisant des messages de phishing hautement personnalisés conçus pour ressembler à des communications avec l'interlocuteur d'origine.



Source : Palo Alto
Conversation détournée pour diffuser des logiciels malveillants

Des attaques utilisant cette technique ont permis d'infiltrer plusieurs réseaux, y compris ceux d'une banque du Moyen-Orient, des entreprises européennes de services relatifs à la propriété intellectuelle, une organisation sportive internationale et des « individus ayant des liens indirects avec un pays de l'Asie du Nord-Est. »

Les chercheurs de Palo Alto ont expliqué qu'en cas de succès, le document malveillant télécharge deux charges utiles malveillantes : PooMilk et Freenki. [lire la suite]

QUE PROPOSE LE NET EXPERT, (EXPERT INFORMATIQUE ASSERMÉNTÉ) :

- SENSIBILISATIONS / FORMATIONS (n° formateur)
 - + RECHERCHE DE PREUVES
- EXPERTISES & AUDITS (certifié ISO 27005)
 - NOTRE MÉTIER :
 - SENSIBILISATION / FORMATIONS :
 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

FORMATIONS EN CYBERCRIMINALITÉ, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, suivez nos formations ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettrons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

EXPERTISES TECHNIQUES : Dans le but de prouver un dysfonctionnement, de déposer ou vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : Des chercheurs découvrent une campagne de phishing durant laquelle des conversations authentiques sont détournées, pour diffuser des malwares