

Les nouvelles techniques des pirates pour piller les distributeurs de billets



Les nouvelles
techniques
des pirates
pour piller
les
distributeurs
de billets

Phishing, hacking, infections « fileless », prise de contrôle à distance. Les braqueurs de banque utilisent des méthodes de plus en plus sophistiquées, presque invisibles, pour mettre la main sur le pacolet des banques.

Quand on pense à des braqueurs de banque, on s'imagine la plupart du temps une bande de malfrats cagoulés et armés jusqu'aux dents, fonçant sur les agences en voiture-bélier. Mais la réalité est bien différente de nos jours. C'est souvent à coup d'ordinateurs et de codes malveillants que les braqueurs du XXI^e siècle mettent la main sur le liquide des distributeurs, et cela avec un degré de technicité de plus en plus impressionnant.

D'après un rapport que vient de publier l'agence Europol, les premiers malwares qui ont permis de vider des guichets automatiques datent de 2009. Ils s'appellent Skimer, Ploutus ou Padkin-Tyupkin, et nécessitent d'accéder physiquement à l'intérieur de ces machines. Pour cela, les pirates s'appuient soit sur un complice de la banque, soit sur un jeu de clés. En effet, il arrive que les distributeurs ne soient protégés qu'avec de simples verrous de type boîte aux lettres !



Figure 4. How a typical physical ATM malware attack is carried out

A l'intérieur du distributeur se trouve généralement un PC sous Windows XP que les pirates infectent avec une porte dérobée. Celle-ci est installée directement depuis un CD ou une clé USB au niveau de XFS (Extension for Financial Services), un *middleware* qui permet de gérer l'interaction entre les différents éléments logiciels et matériels du distributeur: clavier, lecteur de carte, cassettes d'argent, processeur de chiffrement, etc.

Des mules pour récupérer le magot

L'infection nécessite habituellement un démarrage sous Linux. Puis les pirates repassent la machine sous Windows XP et referment les ouvertures physiques. Toute cette opération prend moins de 10 minutes. En apparence, tout fonctionne de nouveau comme avant. En réalité, la porte dérobée permet à des mules d'entrer des commandes secrètes par le clavier numérique et d'éjecter l'argent. Voici une démonstration réalisée en 2014 par les chercheurs de GData...[Lire la suite]

http://www.youtube.com/embed/rZ8_tbtNtUE

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

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

FORMATIONS EN CYBERCRIMINALITÉ, RGPD ET DPQ : 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 ;

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 ;

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 ;

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 accompagnerons 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))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation n° 03107 010 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : *Les nouvelles techniques des pirates pour piller les distributeurs de billets*