الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ م ا م

LETTRE D'INFORMATION : BON A SAVOIR (N°37)

C'est quoi les Banking Trojans ? Comment fonctionnent-ils ?

Les Banking Trojans ne sont pas des malwares comme les autres : ce sont les plus discrets et les plus rentables, mais également les plus sophistiqués, avec des capacités d'adaptation étonnantes. Quels dommages causent-ils ? Comment fonctionnent-ils ?

Les Banking Trojans (ou chevaux de Troie bancaires) sont des logiciels malveillants particulièrement intrusifs, dont l'objectif est d'accéder illégitimement aux comptes bancaires de particuliers ou d'entreprises, afin d'en détourner de l'argent.

Les Banking Trojans les plus connus s'appellent Zeus, SpyEye, Carberp, Citadel, Hermes, Torpig, etc.

S'ils existent depuis plusieurs années, ils continuent de faire des ravages aujourd'hui, notamment parce que leur code informatique est continuellement amélioré**.** Les Banking Trojans sont donc capables de s'adapter à différents types de situation (et depuis peu aux appareils mobiles, notamment sous Android), afin d'être toujours plus efficaces et discrets dans le pillage de comptes bancaires.

Comment éviter les chevaux de Troie ?

Il est difficile de se protéger à 100% contre les chevaux de Troie, qu'ils soient bancaires ou non. Voici néanmoins quelques conseils pratiques qui assureront une sécurité minimum sur votre ordinateur :

- Effectuer les mises à jour logicielles dès qu'elles sont disponibles, et activer les mises à jour système automatiques,
- Créer un compte Utilisateur (en plus du compte Administrateur), qui sera utilisé au quotidien,
- Effectuer des scans réguliers avec le logiciel antivirus, et éventuellement des logiciels de sécurité complémentaires,
- Si possible fournir votre numéro de téléphone mobile à votre banque directement en agence, auprès de votre conseiller financier, ou sur le formulaire d'ouverture de compte,
- Régulièrement inspecter les extensions (plugins, modules complémentaires) des navigateurs web installés, et désinstaller ceux qui ne sont pas utiles.

Les Banking Trojans sont la Rolls Royce des chevaux de Troie traditionnels parce que ce sont ceux qui innovent le plus. Ils sont spécialisés dans les détournements de transactions financières et dans le pillage de comptes bancaires. Pour cela, certains embarquent des codes informatiques spécialement conçus pour des banques précises.

Comment se protéger contre les Trojans bancaires ?

Plusieurs outils aident à se protéger contre les Trojans bancaires. Pour contaminer le système, les malfaiteurs peuvent utiliser les vulnérabilités du navigateur web, des clés USB infectées, les emails en joignant des pièces jointes malveillantes.

Pour assurer la protection et l'intégrité du système d'exploitation, ainsi que pour la prévention des infections par les Trojans bancaires, il est recommandé de suivre les règles suivantes.

1. Installer toutes les mises à jour du système d'exploitation et des programmes installés sur l'ordinateur. Actualiser les navigateurs dès que c'est possible. Les malfaiteurs recherchent constamment les failles de sécurité dans les systèmes d'exploitation ou dans les applications afin d'effectuer des attaques, c'est pourquoi il est nécessaire de les mettre à jour.
2. Utiliser des mots de passe forts dont la longueur dépasse sept caractères. Ne pas utiliser comme mot de passe des mots populaires ou des combinaisons de symboles proches sur le clavier ou des combinaisons faciles à deviner (comme votre nom ou votre date de naissance). Dans ce cas, les malfaiteurs peuvent le trouver en utilisant des outils spécifiques. Un mot de passe fort doit comprendre des chiffres, des lettres majuscules et minuscules, ainsi que d'autres symboles. N'utiliser qu'un mot de passe pour un compte et le modifier périodiquement.
3. Installer un logiciel antivirus fiable, qui utilise des moyens efficaces de détection des malwares, prévoit une protection résidente et des scans périodiques du système. Le logiciel antivirus doit contrôler tous les protocoles utilisés pour la connexion Internet, les supports amovibles, la messagerie locale. Pour assurer une protection antivirus fiable, les bases virales et les composants de l'antivirus doivent être mis à jour régulièrement. Eviter d'utiliser les logiciels antivirus d'éditeurs inconnus : des logiciels malveillants sont souvent distribués sous couvert de ces applications.
4. Utiliser une protection antivirus complète, qui inclut un système de contrôle d'accès, de contrôle des mises à jour de sécurité et de mises à jour des applications installées, ainsi qu'un pare-feu.
5. Ne pas ouvrir les pièces jointes suspectes dans les emails. Une pièce jointe contenant un Trojan ou un fichier infecté par un virus ne représente aucune menace avant que le logiciel malveillant ne soit exécuté. Mais même l'analyse de la pièce jointe enregistrée sur le disque avec le scanner antivirus ne peut pas garantir la sécurité : cette menace n'a peut-être pas encore été entrée dans la base virale. C'est pourquoi il ne faut pas exécuter les fichiers reçus via email d'un expéditeur inconnu. En cas de doute, vérifier ce fichier en le téléchargeant sur l'un des serveurs de test antivirus.
6. Contrôler l'accès aux ressources Internet. L'utilisateur ne doit avoir accès qu'aux ressources locales du réseau nécessaires à son travail quotidien. Le contrôle d'accès aux ressources web permet de restreindre l'accès aux sites indésirables et d'autoriser les ressources web spécifiées dans le composant antivirus.

Les entreprises qui utilisent un système de banque en ligne doivent également protéger leurs serveurs. La meilleure approche pour les entreprises est l'utilisation de la protection complète qui permet:

- une analyse du trafic Internet avant son traitement par le navigateur ;
- d'empêcher au mieux la pénétration des virus en interdisant l'utilisation des supports amovibles et en limitant l'accès aux périphériques locaux et réseau (y compris les dossiers sur l'ordinateur local et les sites Internet) ;
- de minimiser la quantité de spam.
- Pour les entreprises à dizaines postes de travail, il est recommandé d'utiliser un système de gestion centralisée de la protection antivirus. Cela permet:

- D’installer et configurer de manière centralisée les antivirus tournant sur les postes ;
- De mettre à jour la base virale et les composants antivirus de façon centralisée
- De surveiller les événements viraux sur tous les postes en temps réel.
- L'utilisation de solutions antivirus prêtes à fonctionner (paramétrage par défaut opérationnel) est très avantageux car cela permet de :
  - minimiser le délai de déploiement du système de protection ;
  - simplifier le déploiement et la maintenance du système de protection grâce à une interface intuitive et facile à utiliser.

Le Cybersquatting

Le cybersquatting est une pratique qui consiste à déposer un nom de domaine qui contient le nom d’une marque connue pour s’assurer un trafic « illégitime ».
Le cybersquatting touche généralement les marques qui n’ont pas été assez promptes dans leur politique de dépôt et de protection de noms de domaine.
Nitendo a ainsi récupéré en octobre 2011 le nom de domaine supermario.com utilisé depuis 15 ans par un cybersquatteur.
Le cybersquatting peut également prendre la forme d’un dépôt de noms de domaines proches d’un domaine très visité en espérant récupérer des visiteurs ayant fait une erreur dans la saisie de l’adresse, on parle alors de typosquatting.
Le cybersquatting peut être considéré comme une pratique de concurrence déloyale ou de parasitisme.
Les pratiques de cybersquatting sont devenues un peu moins courantes avec le développement du cadre juridique relatif aux noms de domaines et aux procédures de résolution de conflit.

Qu’est ce que le cybersquatting et comment s’en protéger ?

Le cybersquatting, qu’est-ce que c’est ?
Si vous êtes propriétaire d’une marque, sachez que votre nom de domaine peut être utilisé par un tiers en vue d’en tirer profit ou de nuire à votre réputation. Cette pratique est d’autant plus aisée sur Internet qu’il existe une pléiade d’extensions possibles au delà des mythiques .fr .com ou .org. Apprendre à protéger votre nom de domaine est donc indispensable, mais s’il est déjà trop tard, nous allons vous expliquer quelles sont les solutions pour récupérer votre nom de domaine et lutter contre le cybersquatting (aussi connu sous le nom de cybersquattage).
Pour soulever toutes ces questions juridiques, nous avons interviewé Nameshield, le partenaire de Creads, un site de veille juridique et économique, spécialisé dans la surveillance des marques sur Internet.
Comment peut se concrétiser un cybersquatting ?
Il existe plusieurs types de cybersquatting mais les plus dangereux sont les suivants :

- Cybersquatting à l’identique sur une extension (souvent une extension pays) non enregistrée par la marque.
- Typosquatting : marque avec une faute dans le nom

- Phishing : le pirate utilise le nom de domaine typosquatté pour créer une adresse mail générique et demander aux clients de re saisir leur code.

Certains cas de cybersquatting utilisent l'image d'une marque pour rediriger les internautes vers leur propre site concurrent.
D'autres proposent des liens commerciaux sur lesquels les internautes peuvent cliquer, ce qui leur génère un revenu.
Enfin, le plus souvent, l'objectif est de se faire racheter le nom au prix fort par la marque concernée, lorsqu'il n'y a pas de cas de contrefaçon évident.

Que faire pour éviter le cybersquatting ?

Il faut savoir que les cybersquatteurs les plus avisés surveillent les dépôts de marque pour enregistrer les noms de domaine associés, c'est pour cela que la priorité est d'enregistrer le nom de domaine avant de déposer la marque.
Les recommandations d'enregistrement :

- Le .com s'il est disponible avec et sans les tirets.
- Les pays dans lesquels vous êtes ou souhaitez-vous implanter (ex : .es pour l'Espagne, .be pour la Belgique…)
- Les extensions dites à risque : .ru (Russie)/ .cn (Chine) / .de (Allemagne)
- Les nouvelles extensions qui correspondant à votre secteur d'activité (exemple : pour une plateforme e-commerce, enregistrer un .boutique et bientôt le .shop)

Comment être au courant d'un cybersquatting ?

Vous ne pouvez pas enregistrer toutes les extensions car il en existe des centaines.
Mais le premier réflexe est d'enregistrer les noms de domaine les plus pertinents avec votre marque, puis de placer une surveillance du web. Vous pouvez ainsi être alerté de tous les dépôts qui sont fait par des tiers avec votre marque au contenant exact ou approchant.
Si un cas de cybersquatting malveillant est avéré, vous aurez des solutions pour le récupérer, à étudier avec votre registrar partenaire.

Qu'est-ce que le typosquatting ?

Le typosquatting est la pratique qui consiste à acheter des versions mal orthographiées d'un nom de domaine dans le but de rediriger les utilisateurs à l'origine de ses fautes sur son propre site. Cela s'apparente à du cybersquatting.
En effet, les cybersquatteurs achètent des noms de domaine dans le but de surfer sur la popularité d'une marque ou d'une entreprise allant même jusqu'à parvenir, dans certains cas, à acheter un nom de domaine avant qu'une entreprise affiliée ne le fasse.
Mais dans le cas du typosquatting, il s'agit surtout de profiter du fait que les fautes de frappe au moment d'entrer une adresse sont nombreuses et qu'il ne faut pas risquer de perdre des clients potentiels. Si on prend l'exemple d'un site renommé qui bénéficierait de millions de visites, même s'il n'y a qu'un nombre insignifiant de personnes qui commettent des erreurs en tapant le nom du site, cela sera quand même profitable au typosquatteur.
Ce dernier est en mesure d'acheter des domaines avec des lettres manquantes, en trop etc. de cette façon, il pourrait s'approprier des noms de domaines tels que «amazone», « yahou » ou encore « googke » (ce sont des fautes que chacun de nous pourrait faire au moment d'entrer trop rapidement un nom dans une barre de recherche).

Plusieurs options sont disponibles pour les typosquatteurs disposant d'un nom de domaine : ils peuvent tout simplement utiliser le nom du site mal entré pour rediriger la personne vers le site original, ce qui constitue une pratique très utilisée par les entreprises qui ont fait la démarche d'acheter les fautes les plus récurrentes sur leur nom afin de protéger leurs arrières, de conserver leurs clients et de ne pas perdre du chiffre d'affaires. Il est également possible de faire du domaine un lien et ou une ferme de publicité afin que les utilisateurs cliquent sur le contenu et qu'ils créent du profit.

Une des problématiques que pose le typosquatting est que de plus en plus de typosquatteurs créent des sites similaires à d'autres afin de faire en sorte que l'utilisateur y laisse volontairement des informations personnelles et/ou confidentielles et pouvoir ainsi s'en servir à leur insu. Il est arrivé que des typosquatteurs ciblent des enfants en achetant des noms de domaine qu'ils ont l'habitude de visiter.

Le typosquatting n'est pas une pratique illégale à proprement parler, mais s'il est avéré que le typosquatteur utilise un nom de domaine à des fins frauduleuses ou néfastes, on peut considérer que le site va à l'encontre de la loi. Toutefois, les sites qui ne font que surfer sur les fautes de frappe et autres incompréhensions de l'utilisateur ne sont pas tous forcément hors la loi. Il faut savoir également que les entreprises peuvent se montrer aussi agressives qu'elles le souhaitent pour ce qui est du typosquatting**,** le fait que les noms possèdent plusieurs homonymes ou équivalents proches permet à l'utilisateur d'abandonner un site pour s'attaquer à un autre.

Le Typosquatting

Le Typosquatting est malheureusement une pratique relativement courante, bien connue en stratégie du Web. Voici quelques informations et astuces qui devraient vous éviter bien des ennuis !

Qu'est-ce que le Typosquatting ?

Le Typosquatting est proche de la contrefaçon de marque puisqu'il s'agit de réserver un nom de domaine extrêmement proche de celui de la marque. Les différences sont minimes, et relèvent généralement de la faute de frappe ou de la faute d'orthographe.

Ainsi, on parlera par exemple de Typosquatting pour celui qui possède le nom de domaine Gogle ou Googl ou encore Gogole, qui sont des mots ressemblant sensiblement au célèbre Google. Les célébrités sont bien souvent également victime de Typosquatting, Nicolas Sarkozy notamment en ayant fait les frais durant sa campagne présidentielle de 2012.

Pourquoi le Typosquatting ?

Le Typosquatting est généralement utilisé pour nuire à l'image d'un concurrent. Il est également possible grâce à cette technique de capter le trafic d'un site à succès, les fautes de frappe étant monnaie courante lors de la navigation sur Internet. Un internaute pourra en effet facilement se tromper et inverser des lettres, ce qui le conduirait sur un autre site !

Mais cela peut aller encore plus loin puisque le Typosquatting peut être à l'origine de détournements des correspondances vers un site officiel, ce qui peut être réellement problématique. Parfois enfin, le Typosquatting sert tout simplement à nuire à l'image de marque d'un concurrent.

Comment faire face au Typosquatting ?

Pour tenter au maximum de faire face au Typosquatting, faut tout d'abord être extrêmement vigilant au moment de la réservation de son nom de domaine. Ainsi, la première règle est de réserver le .fr et le .com, ce sont des précautions essentielles à prendre en compte. Ensuite, il faut tenter de répertorier toutes les erreurs de frappe ou d'orthographe qu'un internaute est susceptible de faire, et réserver ces noms de domaine, en les redirigeant vers le site de la marque.
Sachez enfin qu'il existe un vide juridique autour de la pratique du Typosquatting mais que si l'image de la marque est trop atteinte, le juge rend souvent un verdict favorable au plaignant.
Le Typosquatting représente bien souvent un sérieux problème pour une entreprise, d'où l'importance d'y songer dès la création du site Web en se protégeant au maximum.

Le typosquatting et le cybersquatting

Nous allons évoquer dans ce billet le *typosquatting* et le *cybersquatting*, deux techniques qui peuvent être utilisées pour tromper un internaute à des fins frauduleuses en manipulant les noms de domaine.

Rappel sur les noms de domaine

Tout ordinateur connecté à Internet possède une adresse dite « IP » (*Internet Protocol*) constituée d'une série de chiffres. Cette adresse est utilisée pour joindre un autre équipement informatique sur Internet.
Le nommage Internet consiste à associer un nom tel que *www.google.fr* à une adresse IP. Il est en effet plus simple pour un humain de retenir puis saisir un nom qu'une série de chiffres. Toutefois, votre navigateur va traduire le nom saisi en adresse IP.
Pour cela, il utilise le service DNS (*Domain Name Service*). Ce dernier fait automatiquement l'association entre un nom et une adresse IP.
L'erreur étant humaine, il peut arriver qu'un internaute fasse une faute de frappe en entrant le nom d'un site dans son navigateur. Ainsi, il peut taper « www.so**cei**tegenerale.fr » au lieu de « www.so**cie**tegenerale.fr ».
Dans certains cas, cette erreur aboutit à l'affichage d'un message d'erreur informant l'internaute que le nom saisi n'existe pas. Dans d'autres, le nom mal orthographié existe et un site est chargé par le navigateur.
Deux techniques sont couramment utilisées pour exploiter les erreurs de frappe : le typosquatting et le cybersquatting.

Qu'est-ce que le typosquatting ?

Le typosquatting est une technique consistant à acheter un nom de domaine dont l'orthographe est très proche d'un domaine existant afin de profiter des fautes de frappe des internautes pour détourner le trafic destiné au site légitime vers un autre site.
On distingue 3 grandes catégories de typosquatting :

- l'utilisation du nom du site « squatté » en l'écrivant différemment : www.societe**s**generale**s**.fr, www.societe--generale.fr... ;
- l'utilisation d'une faute d'orthographe dans le nom : www.so**ss**ietegenerale.fr, www.societege**n**nerale.fr... ;
- l'exploitation des fautes de frappe prévisibles dans le nom : www.societegenera**k**e.fr, www.s**oice**tegenerale.fr...

Qu'est-ce que le cybersquatting ?

Le cybersquatting est une technique qui consiste à déposer un nom Internet correspondant à une marque déposée en lieu et place de son propriétaire. Cela s'apparente à une usurpation d'identité.

On peut distinguer plusieurs cas de figure.

Si le nom n'existe pas encore, le cybersquatteur peut le déposer avant que le propriétaire légitime de la marque ne le fasse. Très souvent, le cybersquatteur va tenter de prendre de vitesse le dépositaire d'un nom de domaine avec une certaine extension (« .com » par exemple) en achetant avant lui le nom de la marque avec une extension différente : « .fr », « .org », et ainsi de suite.

Ont ainsi été victimes de ce type de cybersquatting :

- le site *eBay.com* : en 1999, une société française a déposé le nom *ebay.fr*
- France Télévisions : en 2001, les noms *france3.com* et *france2.com* ont été déposés par une société éditant du contenu pour adulte. Ces deux noms dirigeaient les internautes vers des sites pornographiques.

Quels sont les buts de ces deux techniques ?

Les buts de ces deux techniques sont multiples et ne sont pas tous illégaux.

Le détournement de trafic est une des principales motivations du typosquatting : le site de typosquatting présente alors une simple liste de liens publicitaires. Chaque « clic » d'un internaute sur un de ces liens rapporte quelques centimes au typosquatteur. Le typosquatteur parie sur le fait que quelques internautes cliqueront sur un lien. Quand le site typosquatté est très fréquenté, cela peut s'avérer payant à moindre coût et à moindres efforts.

Le typosquatteur peut aussi proposer des biens et services proches ou concurrents de ceux du site typosquatté, en espérant que les internautes arrivés sur son site par erreur y resteront et effectueront des transactions.

Cela représente cependant des risques pour le typosquatteur car son site peut être assimilé à de la contrefaçon ou de la concurrence déloyale.

De manière plus insidieuse, le typosquatteur tout comme le cybersquatteur peuvent espérer négocier le rachat de leur domaine par le propriétaire légitime d'une marque ou d'un site. En effet, il existe de grandes disparités juridiques entre les pays. Une procédure judiciaire visant, pour une entreprise victime de cybersquatting ou de typosquatting, à récupérer par voie de justice un domaine usurpant une de ses marques, peut se révéler longue, couteuse, et, parfois, inefficace.

Les squatteurs espèrent alors que l'entreprise va privilégier un mauvais accord (c'est-à-dire que l'entreprise paiera très cher le rachat du domaine) à un procès. Cela peut s'apparenter à une « prise d'otage » numérique ou à du racket.

Mais le typosquatting et le cybersquatting peuvent aussi avoir des objectifs nettement plus frauduleux.

Un pirate peut ainsi typosquatter le nom ou la marque d'une banque, d'un site d'e-commerce ou d'un opérateur Internet, et héberger sous ce nom une copie du site original. En résumé, le pirate peut utiliser le typosquatting et le cybersquatting pour des opérations de phishing, dans le but de rendre celui-ci plus crédible.

Beaucoup d'internautes ne vérifient malheureusement pas l'adresse d'un site de phishing. Quelques-uns, plus avertis que d'autres, prennent le temps de lire l'adresse Internet réelle vers laquelle le phishing renvoit.

Une adresse Internet (ou *URL*) trop « exotique » (utilisation d'une adresse IP, d'un site d'hébergement de pages personnelles, etc.) éveillera la méfiance de l'internaute et réduira le taux d'efficacité de l'attaque. Mais si cette URL est www.maban**quue**.com au lieu de www.maban**que**.com, une lecture trop peu attentive ne permettra pas à

l'internaute de déceler le subterfuge. Le nom ressemblant à celui du site légitime, il sera plus enclin à entrer des informations sur la page de phishing.

Que faire face à ces deux techniques ?

Au-delà des conseils qui figurent dans notre billet intitulé « Sensibilisation : le "phishing" ou hameçonnage » et qui restent entièrement applicables, la vigilance reste la meilleure façon de déceler l'emploi de typosquatting ou de cybersquatting à des fins frauduleuses.

Lorsque vous saisissez une adresse Internet dans votre navigateur, nous vous conseillons de la relire pour vous assurer qu'elle ne comporte pas d'erreur avant de taper la touche Entrée.

Les sites que vous visitez fréquemment devraient faire partie de votre liste de favoris. Cette fonctionnalité, offerte par tous les navigateurs grand public, vous permet d'organiser ces sites par rubriques et d'y accéder à chaque fois que vous le désirez par simple clic. Veuillez consulter la documentation de votre navigateur pour savoir comment utiliser cette fonctionnalité.

Lorsque vous recevez un courriel qui vous demande de cliquer sur un lien Internet, assurez-vous que le corps et le sujet du message ne comportent pas d'erreurs d'orthographe ou de grammaire flagrantes. S'il vous semble correctement rédigé, positionnez le pointeur de votre souris sur le lien proposé afin de voir l'adresse vers laquelle il mène. Celle-ci peut avoir été subrepticement définie à des fins de typosquatting et de cybersquatting.

En cas de doute, ne répondez pas au courriel et ne cliquez pas sur les liens qui peuvent vous être proposés. Ne faites pas confiance aux adresses ou numéros de téléphone de contact proposés dans le corps du message. Rendez-vous directement sur le site dont se prétend le courriel afin d'obtenir l'adresse électronique ou le numéro de téléphone du support ou du conseiller qui saura vous indiquer si le courriel est légitime ou non.

Le pharming : comment s'en protéger ?

Le terme "pharming" est issu de la contraction des mots anglais "farming" ("culture fermière" qui consiste pour les jeux en ligne à récolter de l'argent) et "phone phreaking" (piratage de lignes téléphoniques).

Un virus ("Cheval de Troie") sur votre ordinateur réussit à détourner votre connexion à la banque à distance vers un site pirate. Vous tapez une adresse correcte mais vous êtes redirigé automatiquement vers un site pirate ressemblant au vrai site. Les pirates peuvent alors récupérer toutes vos informations

Les bons réflexes anti-pharming

- Vous devez protéger votre ordinateur par un antivirus efficace, intégrant toujours les dernières mises à jour.
- Vérifiez régulièrement le certificat de sécurité (chemin d'accès différent selon votre navigateur internet) : votre banque s'appuie sur ce système (protocole de communication, généralement SSL 128 bits - Secure Socket Layer) pour coder l'ensemble des informations échangées sur le site et permettre ainsi de garantir leur confidentialité et leur intégrité.
- Vérifiez que le site est sécurisé : "https" figure dans la barre d'adresse de votre navigateur Internet et en bas d'écran figure un petit cadenas.
- Choisissez un fournisseur d'accès Internet reconnu.

- Vérifiez l'adresse de l'espace sécurisé dans la barre de navigation et assurez-vous que la session s'ouvre sur la véritable page du site.

Si un virus est détecté

- N'effectuez aucune opération de banque à distance (connexion, virement, opposition...)
- Suivez les indications de votre antivirus pour détruire le virus de votre ordinateur.
- Relancez votre antivirus pour vérifier qu'il ne reste plus aucune trace du virus et que les fichiers atteints ont bien disparu.
- Contactez le Service Relations Clientèle de la banque et demandez à votre conseiller de réinitialiser vos codes.
- Changez vos codes d'accès et mot de passe.

Phreaking : piratage téléphonique coûte 43 000€ au Conseil Départemental des Deux-Sèvres

Le piratage téléphonique, le phreaking**,** touche de nombreuses personnes, de nombreuses entreprises.

L'une de ces attaques consiste à mettre la main sur le mot de passe de gestion du standard téléphonique afin de passer des appels sur le compte de la victime. Le départemental des Deux-Sèvres vient d'en faire les frais.

5000€ pour la MJC de Nancy, 15000€ par les communes de Pessac et de Licques… la liste des entreprises et collectivités piégées par le phreaking, le piratage téléphonique ne cesse de s'allonger. Nouvelle victime en date, le conseil départemental des Deux-Sèvres qui se retrouve avec une facture salée : 43000€ d'appels téléphoniques frauduleux. Attaque malheureusement facile. Un peu de social engineering (quel type de standard utilisé), le numérique de téléphone de l'établissement et le mode d'emploi du matériel informatique utilisé pour le standard.

Le pirate n'a plus qu'à rentrer le précieux sésame pour prendre la main sur le standard. Bilan, il suffit que le malveillant commercialise dans le blackmarket cette nouvelle source et le tour est joué. Les acheteurs utilisent ensuite ce code d'accès pour enclencher des escroqueries pour des lignes surtaxées [permet de blanchir l'argent détourné par les appels frauduleux], exploité dans des cybercafés un peu partout dans le monde (Afrique, Asie, …).

Pour le département, des appels nombreux et long vers l'Afrique pour un montant de 43000 euros ! La police judiciaire de Niort est sur trois autres affaires allant de 416€ de facture à 1400 appels pour un global de 15000€.

Le phreaking peut prendre plusieurs formes, comme le cas du détournement téléphonique de la société CarGlass. Une modification permettant de lancer des appels téléphoniques malveillants sur le compte de l'entreprise connue pour ses réparations de pare-brises. L'idée des pirates, perturber par une forme de DDoS téléphonique une cible choisie.

Ce que dit la loi

Pour les pirates, la loi est claire : piratage, escroquerie, … entre 5 et 7 ans de prison et jusqu'à 350000 euros d'amende.

Pour l'entreprise impactée, il est dorénavant possible de se retourner contre le prestataire de service, l'entreprise qui a pris en charge l'installation du standard.

Une jurisprudence condamne les intégrateurs dans la mesure où ces derniers n'ont pas informé et formé leurs clients. Oublier de leur expliquer comment changer le mot de passe usine du standard ou oublier de mettre en place les patchs de sécurité devient une faute.
Un arrêt de la cour d'appel de Versailles et du tribunal de commerce de Nanterre a condamné un de ses intégrateurs pour faute par négligence. Le tribunal a obligé la société de maintenance à payer la somme volée, soit plus de 12000€ : « Il revient à l'utilisateur de gérer la sécurité de son matériel, à condition toutefois qu'il ait été informé de cette nécessité et qu'on lui ait montré comment procéder **».**