Trois histoires vrais de vies inquiétées par du piratage informatique ciblé

Trois histoires vrais de vies inquiétées par du piratage informatique ciblé

L'expérience le prouve : même les vieux habitués d'Internet n'arrivent pas toujours à se protéger des piratages ciblés. Étant donné que notre vie quotidienne devient de plus en plus connectée à Internet et à d'autres réseaux, la sécurité en ligne s'est convertie comme un besoin impératif.

La plupart d'entre nous ont un email, un compte sur les réseaux sociaux et une banque en ligne. On commande sur le web, et utilisons notre mobile pour nous connecter à Internet (par exemple, dans les solutions de l'authentification à deux facteurs) et pour d'autres choses tout aussi importantes. Malheureusement, aucun de ces systèmes n'est 100% sûr.
Plus nous interagissons en ligne et plus nous devenons les cibles de hackers sournois. Les spécialistes en sécurité appellent ce phénomène « la surface d'attaque ». Plus la surface est grande et plus l'attaque est facile à réaliser. Si vous jetez un coup d'œil à ces trois histoires qui ont eu lieu ces trois dernières années, vous comprendrez parfaitement le fonctionnement de cette attaque.

1. Comment détourner un compte : faut-il le pirater ou simplement passer un coup de fil ?

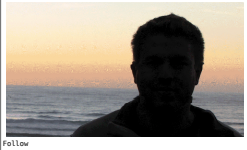
Un des outils les plus puissants utilisés par les hackers est le « piratage humain » ou l'ingénierie sociale. Le 26 février dernier, le rédacteur en chef de Fusion Kevin Roose, a voulu vérifier s'il était aussi puissant qu'il n'y paraissait. Jessica Clark, ingénieure sociale spécialisée en piratage informatique et l'expert en sécurité Dan Tentler ont tout deux accepté ce défi.
Jessica avait parié qu'elle pouvait pirater la boîte mail de Kévin rien qu'avec un email, et sans grande difficulté elle y est arrivé. Tout d'abord, l'équipe de Jessica a dressé un profil de 13 pages qui définissait quel genre d'homme il était, ses goûts, etc, provenant de données collectées de diverses sources publiques.
Après avoir préparé le terrain, Jessica a piraté le numéro mobile de Kévin et appelé sa compagnie de téléphone. Pour rendre la situation encore plus réelle, elle ajouta un fond sonore d'un bébé en train de pleurer.
Jessica se présenta comme étant la femme de Roose. L'excuse inventée par cette dernière fut qu'elle et son « mari » devaient faire un prêt, mais qu'elle avait oublié l'email qu'ils utilisaient en commun, en se faisant passer pour une mère de famille désespérée et fragile. Accompagnée des cris du bébé, Jessica ne mit pas longtemps à convaincre le service technique de réinitialiser le mot de passe du mail et ainsi d'y avoir pleinement accès.
Dan Tentler a accompli cette tâche avec l'aide de l'hameçonnage. Tout d'abord, il avait remarqué que Kevin possédait un blog sur Squarespace et lui envoya un faux email officiel depuis la plateforme, dans lequel les administrateurs de Squarespace demandaient aux utilisateurs de mettre à jour le certificat SSL (Secure Sockets Layer) pour des questions de « sécurité », permettant ainsi à Tentler d'accéder à l'ordinateur de Kévin. Dan créa de nombreux faux pop-up demandant à Roose des informations bien spécifiques et le tour était joué.
Tentler réussit à obtenir l'accès à ses données bancaires, son email, ses identifiants sur les sites web, ainsi que ses données de cartes de crédit, son numéro de sécurité sociale. De l'écran de son ordinateur, il capturait des photos toutes les deux minutes et ce pendant 48h.
View image on Twitter

Follow

Kaspersky Lab
@kaspersky
What is phishing and why should you care? Find outhttps://kas.pr/6bpe #iteducation #itsec
8:05 PM – 11 Dec 2015
•
•
1717 Retweets
•
77 likes

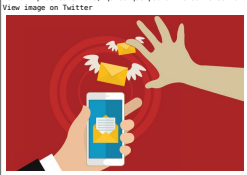
2. Comment détourner de l'argent à un ingénieur informatique en moins d'une nuit

Au printemps 2015, le développeur de logiciels Partap Davis a perdu 3000$. Durant une nuit, en seulement quelques heures, un hacker inconnu a obtenu l'accès de ses comptes mail, son numéro de téléphone et son Twitter. Le coupable a contourné habilement le système de l'authentification à deux facteurs et littéralement vidé le portefeuille des bitcoins de Partap. Comme vous devez sans doute l'imaginer, Davis a passé une mauvaise journée le lendemain.
Il est important de noter que Partap est une pointure concernant l'usage d'Internet : il choisit toujours des mots de passe fiables et ne clique jamais sur des liens malveillants. Son email est protégé avec le système d'authentification à deux facteurs de Google, ce qui veut dire que lorsqu'il se connecte depuis un nouvel ordinateur, il doit taper les six numéros envoyés sur son mobile.



Follow

The Verge
@verge
Anatomy of a hack: a step-by-step account of an overnight digital heist http://www.theverge.com/a/anatomy-of-a-hack …
4:02 PM – 4 Mar 2015
•
•
6969 Retweets
•
7171 likes
Davis gardait ses économies sur trois portefeuilles Bitcoin, protégés par un autre service d'authentification à deux facteurs, conçu par l'application mobile Authy. Même si Davis utilisait toutes ces mesures de sécurité prévoyantes, ça ne l'a pas empêché de se faire pirater.
Suite à cet incident, Davis était très en colère et a passé plusieurs semaines à la recherche du coupable. Il a également contacté et mobilisé des journalistes de The Verge pour l'enquête. Tous ensemble, ils sont parvenus à trouver comment le piratage avait été exécuté. Davis utilisait comme mail principal l'adresse suivante : Patrap@mail. Tous les mails furent envoyés à une adresse Gmail plus difficile à mémoriser (étant donné que Patrap@gmail était déjà utilisé).
Pendant plusieurs mois, quiconque pouvait ensuite se rendre sur la page Hackforum et acheter un script spécial afin d'obtenir les mots de passe qui se trouvaient dans la boite mail. Apparemment, le script était utilisé pour contourner l'authentification à deux facteurs et changer le mot de passe de Davis.
View image on Twitter



Follow

Kaspersky Lab
@kaspersky
Unfortunately two-factor authentication can't save you from#banking Trojans https://kas.pr/S4jV #mobile
4:40 PM – 11 Mar 2016
•
•
2828 Retweets
•
1515 likes
Ensuite, l'hacker a fait une demande de nouveau mot de passe depuis le compte de Davis et demandé au service client de transférer les appels entrants à un numéro de Long Beach (ville en Californie). Une fois le mail de confirmation reçu, le service technique a donné le contrôle des appels à l'hacker. Avec une telle technique, il n'était pas bien difficile de contourner l'authentification à deux facteurs de Google et avoir accès au compte Gmail de Davis.
Pour surmonter cet obstacle, l'hacker a tout simplement réinitialisé l'application sur son téléphone en utilisant une adresse mail.com et une nouvelle confirmation de code, envoyée de nouveau via un appel vocal. Une fois que l'hacker mit la main sur toutes les mesures de sécurité, il changea les mots de passe des portefeuilles Bitcoin de Davis, en utilisant Authy et l'adresse email .com afin de lui détourner de l'argent.
L'argent des deux autres comptes est resté intact, l'un des services interdisant le retrait des fonds 48h après le changement du mot de passe, et l'autre demandant une copie du permis de conduire de Davis, que l'hacker n'avait pas en sa possession.

3. La menace rôde sur nos vies

Comme l'a écrit le journal Fusion en octobre 2015, la vie de la famille Straters s'est retrouvée anéantie à cause d'une pizza. Il y a plusieurs années, des cafés et restaurants locaux se sont installés sur leur arrière-cour, les envahissant de pizzas, tartes et toute sorte de nourriture.
Peu de temps après, des camions de remorquage ont déboulé munis de grandes quantités de sable et de gravier, tout un chantier s'était installé sans aucune autorisation au préalable. Malheureusement, il ne s'agissait que de la partie visible de l'iceberg comparé au cauchemar des trois années suivantes.
Follow

Techmeme @Techmeme
How the Strater family endured 3 years of online harassment, hacked accounts, and swatting http://fusion.net/story/212802/haunted-by-hackers-a-suburban-familys-digital-ghost-story/ …http://www.techmeme.com/151025/p4##a151025p4 …
6:36 PM – 25 Oct 2015

Haunted by hackers: A suburban family's digital ghost story
A suburban Illinois family has had their lives ruined by hackers.
fusion.net
•
•
88 Retweets
•
66 likes
Paul Strater, ingénieur du son pour une chaine de télé locale et sa femme, Amy Strater, ancienne directrice générale d'un hôpital, ont été tout deux victimes d'un hacker inconnu ou de tout un groupe. Il s'avérait que leur fils Blair était en contact avec un groupe de cybercriminels. Les autorités ont reçu des menaces de bombe signées du nom du couple. Les hackers ont utilisé le compte d'Amy pour publier une attaque planifiée dans une école primaire, dans lequel figurait ce commentaire « Je tirerai sur votre école ». La police faisait des visites régulières à leur domicile, n'améliorant en rien les relations du couple avec leur voisinage, qui à force se demandait ce qu'il se passait.
Les hackers ont même réussi à pirater le compte officiel de Tesla Motors et posté un message qui encourageait les fans de la page à appeler les Strater, en échange de gagner une voiture Tesla. Les Strater « croulaient sous les appels téléphoniques », environ cinq par minute, provenant des « admirateurs » de Tesla, désireux de gagner la voiture. Un jour, un homme s'est même présenté au domicile des Strater en demandant aux propriétaires d'ouvrir leur garage, prétendant qu'ils cachaient la Tesla à l'intérieur.
Follow

r00t @rootworx
Again, There is no free car, I did not hack Elon Musk or Tesla's Twitter account. A Finnish child is having fun at your (and my) expense.
12:51 AM – 26 Apr 2015
•
•
1414 Retweets
•
1818 likes
Paul tenta de démanteler le groupe d'hackers en changeant tous les mots de passe de ses comptes et en donnant l'ordre aux patrons des restaurants locaux de ne rien dévoiler sur leur adresse. Il contacta également le Département de Police d'Oswego en leur demandant de vérifier à l'avance si une urgence était bien réelle, avant d'envoyer des renforts. En conséquence de tous ces problèmes, Paul et Amy finirent par divorcer.
Les attaques ont continué par la suite. Les réseaux sociaux d'Amy ont été piratés et utilisés pour publier toute une série de revendications racistes, ce qui a causé la perte de son emploi. Elle fut licenciée malgré avoir dit à ses supérieurs qu'elle et sa famille étaient les victimes de hackers et que leur vie s'était transformée en un véritable cauchemar.
Amy réussit à temps à reprendre le contrôle de son LinkedIn et à supprimer son compte Twitter. Malheureusement, elle était incapable de retrouver un travail dans sa branche à cause de ce qui s'était passé. Elle fut contrainte de travailler chez Uber pour arrondir ses fins de mois, mais disposait de ressources insuffisantes pour payer son loyer.
« Avant, lorsqu'on tapait son nom sur Google, on pouvait voir ses nombreux articles scientifiques et son travail admirable » a déclaré son fils Blair au journal Fusion. « Désormais, on ne voit plus que des hackers, hackers, hackers ».
De nombreuses personnes ont critiqué Blair Strater pour avoir été impliqué lui-même dans de nombreux réseaux de cybercriminels, où il n'arrivait pas à se faire d'amis. Dans le cas précis de la famille Strater, les parents de Blair ont payé pour les « crimes » de leur fils, alors qu'eux n'avaient absolument rien à voir avec les hackers.
Article original de Kate Kochetkova

Denis JACOPINI ne peut que vous recommander d'être prudent.
Si vous désirez être sensibilisé aux risques d'arnaques et de piratages afin d'en être protégés, n'hésitez pas à nous contacter, nous pouvons animer conférences, formations auprès des équipes dirigeantes et opérationnelles.
La sécurité informatique et la sécurité de vos données est plus devenu une affaire de Qualité (QSE) plutôt qu'un problème traité par des informaticiens.
Vous souhaitez être aidé ? Contactez-nous

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Comment pirater, détourner de l’argent et rendre la vie de quelqu’un impossible sur Internet : trois histoires inquiétantes de piratages ciblés. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.