

AU-DELÀ DU PHISHING

EXPLICATION - LA MENACE CROISSANTE DE LA FRAUDE D'OPÉRATIONS BANCAIRES SUR L'INTERNET

Les opérations bancaires sur l'Internet sont maintenant un produit grand-public qui est exigé comme service essentiel par de nombreux clients des banques. De plus en plus on compte sur le côté pratique et la facilité d'utilisation des services bancaires sur l'Internet dans la vie quotidienne. De plus en plus, la qualité du service bancaire sur l'Internet peut affecter le niveau général de la satisfaction et de la fidélité des clients de la banque.

Ironiquement, la disponibilité et la popularité croissantes des opérations bancaires sur l'Internet deviennent le plus grand défi à leur viabilité et développement continu. Les fraudeurs sont attirés par le potentiel énorme pour le vol en ligne et constituent des menaces de plus en plus sophistiquées et efficaces à la sécurité des transactions des clients effectuées sur l'Internet.

Le Phishing

Beaucoup de publicité existe sur les attaques 'phishing' - les tentatives par des fraudeurs de capturer et enregistrer les détails de la sécurité des clients, pour les utiliser plus tard pour commettre la fraude. Les attaques de phishing ont connu un niveau élevé de succès, en exploitant l'assurance des banques dans l'identification simple du client par ids, mots de passe et autre informations secrètes. Maintenant, les attaques de phishing sont devenues mondaines et banales - la plupart des clients sont au courant d'une pléthore d'emails plus ou moins crédible, lui demandant de 'confirmer vos détails de sécurité'.

Le résultat, comme toujours, est que le monde continue à tourner. Les banques ont commencé à traiter la menace de phishing en augmentant la sécurité de leurs systèmes, en adoptant la prétendue 'authentification à deux voies', qui exige de leur clients d'utiliser un lecteur de cartes à puce ou un autre appareil d'authentification pour accéder au service. Cependant, les fraudeurs sophistiqués ont toujours une longueur d'avance, et ont maintenant évolué dans la menace d'attaques bien au-delà du phishing.

Au delà du Phishing – Man in the Middle (MitM)

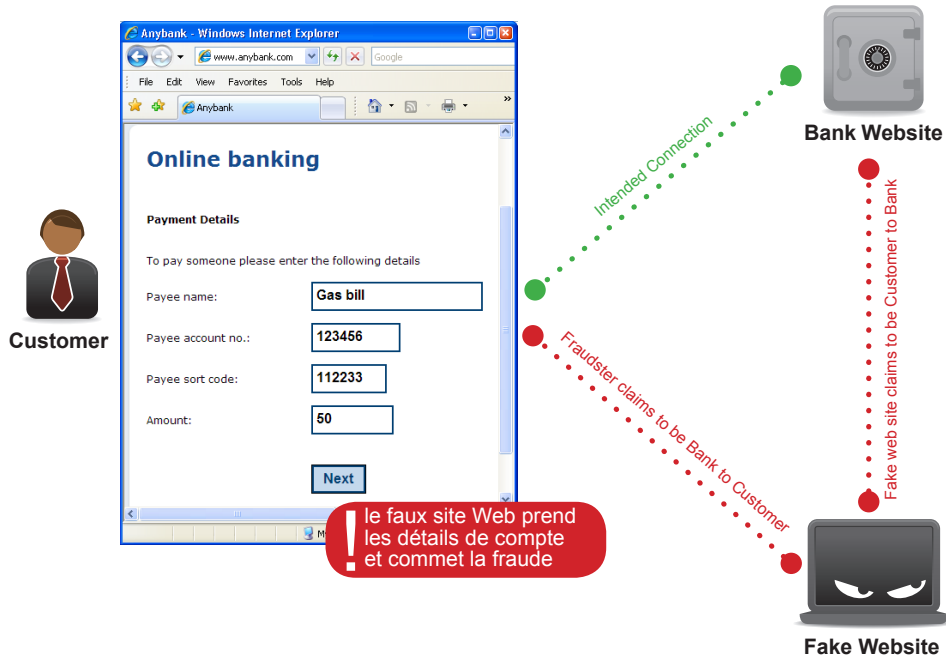
Une menace récente et rapidement croissante pour la sécurité d'opérations bancaires en ligne est l'attaque prétendue "man in the middle" (MitM). Cette technique de fraude a été adoptée pour éviter des mesures de sécurité récemment déployées par les banques, telles que l'authentification mutuelle. Tandis que l'attaque de MitM exige une approche plus sophistiquée que le 'phishing', cette technique a été déjà souvent employée par des criminels et a été responsable de grandes quantités de fraudes. Maintenant, il y a des kits fournis par l'Internet, qui permettent à des fraudeurs relativement peu qualifiés de monter des attaques apparemment sophistiquées.

L'attaque MitM implique typiquement que le fraudeur contraint le client de la banque de visiter un faux site Web. Ceci est généralement réalisé en envoyant un email, imitant ceux d'une banque, qui demande au client de cliquer sur un lien fourni, censé être le site Web de la banque. D'autres approches implique de modifier le raccordement internet des clients, de sorte que lorsqu'ils essayent de visiter le site Web correct, ils sont en fait reliés au faux.

À l'utilisateur, le site Web semblera identique au site Web normal de la banque. Il peut même être crypté ainsi le client verra le symbole prévu (le cadenas) dans leur navigateur. Cependant, les détails écrits iront au faux site Web de la banque,

Entre 2005 et 2007, **Nordea** était la cible d'une attaque sophistiquée de malware, qui a causé **des pertes de plus de \$1.000.000**. Le logiciel a enregistré les détails du compte de l'utilisateur et les a envoyés aux fraudeurs, censés être basé en Russie. Les fraudeurs ont fait une série de petits transferts, afin d'éviter les mesures de détection de fraude de la banque.

Man in the Middle



En 2006 les clients d'affaires de Citibank ont été visés par une attaque 'man in the middle'. Un email a demandé à des clients de confirmer leur adresse, déclarant qu'une activité suspecte a été détectée. Le site a demandé des détails de compte, y compris le mot de passe jetable de la marque délivré aux clients. S'ils étaient incorrects, le client serait invité à les ressaisir.

pas au vrai. Quand ces détails sont reçus, le logiciel spécial se reliera au vrai site Web de la banque, identifie le client et fait les transactions frauduleuses. Puisque le faux site Web a tous les détails que le client donnerait normalement, la banque ne peut pas faire la différence entre le vrai client et le fraudeur. Puisque la correspondance vers la banque se produit juste après que le client ait introduit ses détails de compte, n'importe quel mot de passe sera toujours valide. Si la banque a mis en application l'authentification mutuelle, le faux site Web recevra la réponse correcte de la banque, telle que des images ou des réponses aux questions secrètes, et les renvoie au client. Le client verra la réponse prévue et ainsi enverra les détails de compte désirées par le fraudeur. Tandis que le client et la banque croient qu'ils communiquent directement, en fait le fraudeur est libre de regarder et modifier n'importe quelle partie d'information transmise.

Cependant, les clients de banque perspicaces peuvent identifier les faux sites, puisque leur adresse peut être incorrecte. Tandis que certains sont cryptés, l'inspection attentive de la certification de site Web peut prouver que le site n'appartient pas vraiment à qui il prétend. En outre, alors que les fraudeurs peuvent essayer de se relier au site Web de la banque à partir d'un ordinateur dans le même pays que le client, les systèmes de détection de fraude bancaire pourraient relever des caractéristiques suspectes.

Encore pire – 'Man in the Browser' (MitB)

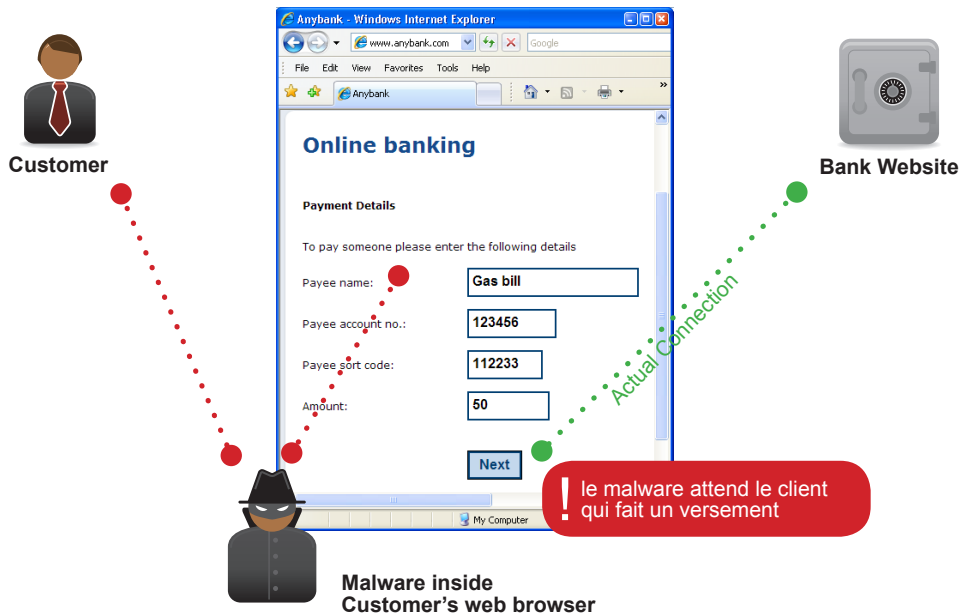
Pour ces raisons, les fraudeurs ont maintenant développé une variante plus sophistiquée de MitM – l'attaque 'man in the browser' (MitB). Au lieu d'intervenir entre l'ordinateur du client et le site Web de la banque, les interceptions de MitB agissent entre le client et son navigateur.

Une attaque de MitB est conçue en installant un logiciel malveillant (malware) sur l'ordinateur du client. Ceci peut se produire lorsqu'un client ouvre un attachement d'email ou télécharge un dossier d'un site Web. Visiter un site Web, ou lire un email, peut être suffisant pour qu'un fraudeur puisse installer le malware sans permission du client. Dans certains cas les criminels ont trébuché des sites Web légitimes existants, de sorte qu'ils infectent leurs visiteurs.

Le client est peu susceptible de noter que quelque chose est différent. Pas moins de 80% de nouveau malware est non détecté par les logiciels d'anti-virus. L'enchaînement normal reste inchangé, mais le malware

En 2007, ABN AMRO était la victime d'une attaque malware-basée sur leur service bancaire en ligne. Un email a été envoyé à des clients, prétendant être de la banque elle-même, qui contenait un attachement. Quand le client visite leur site d'opérations bancaires, ils seront envoyés au faux site qui rassemble les détails de la compte. Quoique ABN AMRO ait déployé l'authentification à deux voies basée sur un lecteur de cartes à puce, les fraudeurs pouvaient placer des transactions pendant que le mot de passe jetable était encore valide.

Man in the Browser

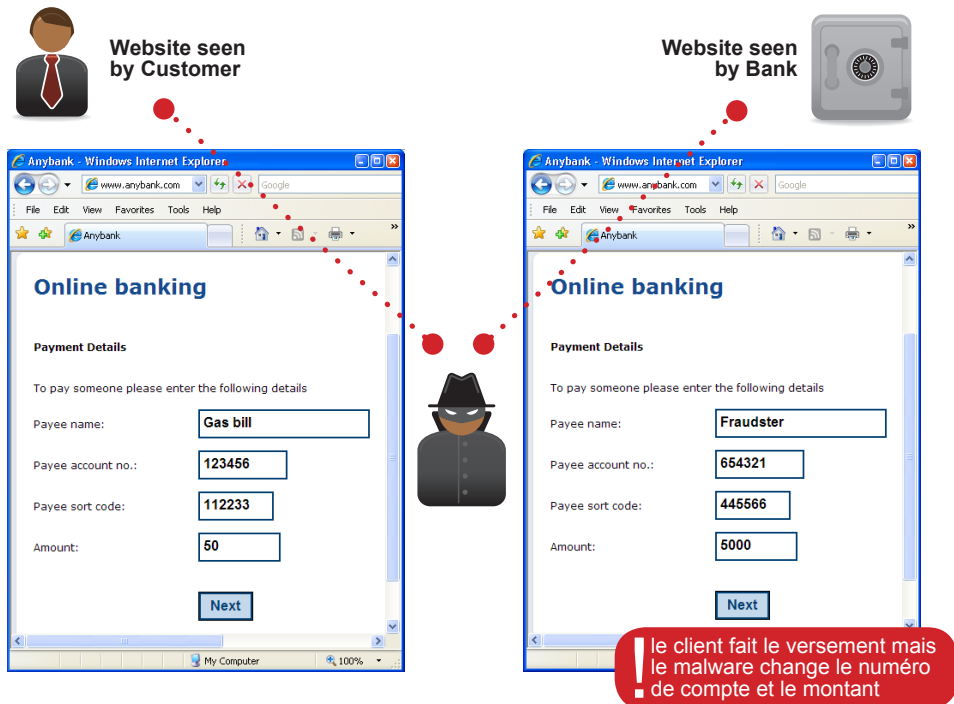


En janvier 2008, le **SilentBanker Trojan** a visé plus de **400 banques** dans le monde, comprenant les Etats-Unis, France, Espagne, Irlande, R-U, Finlande, Turquie. Le malware est capable d'exécuter **une attaque 'MitB'** et inclut un mécanisme automatique de mises à jour pour prolonger la liste de cibles.

identifiera quand le client visite le site Web de la banque. Puis, le malware peut librement changer la page Web pendant qu'il est montré au client, et modifier les demandes envoyées de nouveau à la banque.

Par exemple, si le client fait un versement, le malware pourrait changer le numéro de compte de destination vers celui du fraudeur, et de plus, augmenter le montant. De même, une fois que la banque confirme que le versement est effectué, le malware changera ce qui est montré au client, pour qu'il pense que la transaction désirée a été exécutée.

Man in the Browser



Les paquets génériques de malware disponibles permettent à des fraudeurs de configurer facilement le logiciel pour attaquer certaines banques en particulier. Le dossier de configuration est téléchargé à partir d'un site Web, ainsi il peut être rapidement mis à jour pour ajouter de nouvelles banques ou pour s'adapter aux

changements de la structure de site Web. Un tel paquet, connu sous le nom de SilentBanker, peut monter des attaques sur plus de 400 sites Web de banque différents dans le monde entier, ayant des dispositifs spécifiquement conçus pour éviter l'authentification à deux voies. SilentBanker est non seulement capable d'attaques classiques MitM, mais il est également capable d'attaque MitB.

Il est encore plus difficile de se défendre contre une attaque de MitB que contre une attaque MitM. Puisque le raccordement de réseau n'est pas interféré, l'adresse et le certificat de site Web seront corrects. Des systèmes de détection de fraude sont également entravés par le fait que, du point de vue de la banque, le client les visite à partir de son ordinateur normal et emploie son raccordement habituel d'Internet. Comme avec MitM, parce que les attaques de MitB se produisent en temps réel, la marque de sécurité et l'authentification mutuelle peuvent être évitées. Puisque le fraudeur a le contrôle total de l'ordinateur du client, les mécanismes de sécurité biométriques sont également inefficaces.

Alors, où les banques vont-elles?

Bref, les attaques MitM et MitB sont une menace sérieuse et croissante aux opérations bancaires en ligne. Ils fonctionnent en amenant les clients à croire qu'ils communiquent directement avec leur banque, alors qu'en fait un fraudeur est en train de regarder et modifier l'information envoyée et reçue. Puisque les attaques fonctionnent en temps réel, des techniques standard de sécurité, telles que les tokens, les mots de passe jetable, l'authentification mutuelle et la biométrie peuvent tous être déviés. Que peuvent faire les banques pour parer à ces dernières menaces ?

La réponse se situe dans l'authentification complète de chaque transaction, non seulement l'identité du client mais également les détails de la transaction à effectuer doit être authentifiée par le client. Ceci, en même temps que l'authentification deux-facteur (en utilisant un lecteur de cartes à puce ou un autre appareil d'authentification), fournit une défense beaucoup plus robuste. Le client doit vérifier que tous les détails de chaque transaction sont corrects, incluant par exemple le nom de bénéficiaire, numéro de compte et montant, avant qu'elle puisse être exécutée.

Un certain nombre de banques ont récemment fourni des lecteurs de cartes à puce à leurs clients pour mettre en application l'authentification à deux voies et pour se protéger contre des attaques phishing. Cet appareil peut également être utilisé pour l'authentification de chaque transaction. Cependant, les détails de transaction doivent être manuellement ressaisis par client (avec seulement des clefs numériques disponibles). Ceci réduit considérablement ce qui peut être authentifié, et augmente ainsi la vulnérabilité. En outre, exiger des clients de ressaisir tous les détails significatifs de transaction augment la risque d'erreur et diminue la facilité d'emploi.

Une méthode plus utilisable et plus souple pour une authentification plus sûre peut être trouvée dans les solutions telles que le cryptogramme visuel de la société Cronto. Cronto propose des applications dédiées aux transactions en ligne basées sur une signature visuelle via la caméra du téléphone mobile ou une clé optique spécialisée de l'utilisateur. Ceci enlève le besoin d'appareils difficiles à utiliser et la nouvelle saisie des codes générés ou des détails de transaction. La capacité plus grande permet à plus de détails de transaction d'être authentifiés, et ceux-ci peuvent être changés rapidement, en réponse à l'adaptation dans le comportement criminel.

"A new form of man-in-the-middle attack, called **"man-in-the-browser"** has surfaced. These attacks can bypass current browser security mechanisms to read, insert, and modify transaction data... So, what should enterprises do to protect themselves against this new threat? ... A longer-term solution lies in **transaction verification**.

Organizations that do business online should re-evaluate their solution road maps and incorporate transaction verification as a core component of their overall security strategy."

Forrester Research, 2007