



Nouvelles formes d'attaques informatiques | Le Net Expert Informatique

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p>  <p>vous informe...</p>	<h2>Nouvelles formes d'attaques informatiques</h2>
--	--

Sévissant depuis l'année dernière, ce malware de nouvelle génération combine techniques informatiques sophistiquées, ingénierie sociale et intervention humaine pour que la fraude soit effective. Nom de code : Dyre Wolf

Entre 500 000 et 1,5 million de dollars par attaque. Tel est le butin ramassé lors de l'attaque réalisée à l'aide du malware Dyre qui sévit depuis le mois d'octobre dernier. Mais les criminels derrière ce programme ont récemment franchi une nouvelle étape qui permet au programme de retrouver une nouvelle jeunesse, au grand dam des entreprises qui en sont victimes.

L'attaque se déroule en plusieurs étapes. Dans un premier temps, des utilisateurs reçoivent un mail contenant une pièce jointe, elle-même infectée par le logiciel Upatre. Le but de ce logiciel est uniquement de permettre le téléchargement de Dyre, un programme beaucoup plus dangereux. Lorsque Dyre est téléchargé, il va essayer de se répandre le plus largement possible chez les autres employés de l'entreprise ou les amis de la personne infectée au travers du programme de messagerie Outlook. En parallèle, le logiciel va surveiller le travail de la personne infectée et attendre qu'elle se connecte à un parmi des centaines de sites bancaires que le malicieux est programmé pour surveiller.

Le voleur au bout du fil

Et c'est là que cela devient tout à fait nouveau. Lors de la tentative de connexion au site, Dyre va afficher un message indiquant que la connexion et le compte posent un problème et va inviter la personne à contacter un numéro de téléphone. Précisons que ceci se passe indépendamment du navigateur utilisé : Chrome, Firefox ou Internet Explorer. En effet, les trois navigateurs ont été usurpés.

En composant le numéro de téléphone, la victime ne va pas tomber sur un centre d'appel mais sur une vraie personne qui va se proposer de « l'aider » à régler son problème. Cette personne en apparence tout à fait bien intentionnée va donc vous demander des informations sur votre compte et pendant que vous discutez avec elle, elle procédera à un transfert de fonds depuis le compte bancaire de l'entreprise vers les propres comptes des criminels. « L'intervention d'un opérateur au téléphone en direct est unique », précise Caleb Barlow, vice-président d'IBM.

Et un petit DDOS pour bien masquer le tout

Enfin, simultanément au transfert de fonds, le site web de l'entreprise qui vient d'être pillée va être victime d'une attaque en DDOS. Le but de cette attaque est de détourner l'attention des services IT et de sécurité qui seront trop occupés à endiguer cette attaque pour s'occuper d'une escroquerie financière, du moins dans les premiers jours.

On le voit : l'imagination des cybercriminels est débordante. Comme à l'habitude, IBM répète une série de conseils, notamment de ne jamais fournir des informations bancaires à quiconque, les « vraies » banques ne demandant jamais ce type d'informations.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source :

<http://www.mag-securis.com/news/articletype/articleview/articleid/34604/dyre-wolf-nouvelle-etape-dans-la-cybercriminalite.aspx>

Par Raphaël Stencher