OUCH! Avril 2023

SANS SECURITY AWARENESS

OUCH!

Votre bulletin mensuel sur la sensibilisation à la sécurité

Scareware : Une histoire

Attention ! Votre ordinateur est infecté par le rançongiciel Black Basta. Appelez ce numéro de téléphone immédiatement pour réparer votre ordinateur ! - *Si vous voyiez cet avertissement apparaître sur votre ordinateur, appelleriez-vous le numéro de téléphone ?*

L'attaque

Après trente ans de travail acharné, Déborah avait économisé suffisamment d'argent pour prendre sa retraite avec son mari. Désireuse de passer en revue ses comptes de retraite, elle a tapé le nom de sa banque dans son navigateur. Ce qu'elle n'a pas réalisé, c'est qu'elle avait mal tapé le nom de la banque, ce qui l'a conduite sur un autre site Web qui a immédiatement affiché une bannière d'avertissement effrayante affirmant que son ordinateur était infecté et lui demandant d'appeler immédiatement le support technique. La bannière d'avertissement était très professionnelle. Il indiquait le logiciel malveillant qui avait infecté son ordinateur, comportait le logo officiel de l'entreprise et fournissait un numéro d'urgence à appeler.

Déborah a immédiatement appelé le numéro, qui a été répondu par un agent d'assistance apparemment professionnel. L'agent lui a expliqué que son ordinateur était effectivement infecté et qu'il fallait y accéder pour le réparer. Elle devait aller sur un site Web spécifique, télécharger leur logiciel de sécurité, puis l'installer. Elle a fait ce qu'on lui a demandé et l'agent d'assistance l'a informée qu'ils avaient accès à son ordinateur, après quoi ils ont commencé à le fouiller.

Ils ont rapidement confirmé ses pires craintes : non seulement son ordinateur était infecté, mais il s'est avéré que son compte bancaire avait été piraté. Heureusement, l'entreprise d'assistance technique était en contact direct avec sa banque, qui l'a rapidement transférée vers un agent anti-fraude. L'agent de fraude a confirmé que son compte était effectivement compromis et qu'il était utilisé pour transférer des fonds frauduleux. Ils lui ont dit de transférer immédiatement tout son argent sur un autre compte bancaire pour le protéger. Déborah a fait ce qu'on lui a demandé. Ils l'ont ensuite informée que son compte de retraite était également compromis. Heureusement, ils avaient aussi un partenariat avec l'agence gouvernementale des impôts. Elle a ensuite été mise en relation avec un agent du gouvernement qui lui a expliqué que pour sécuriser son compte de retraite, elle devait encaisser ses économies et les transférer sur un autre compte avant que les criminels ne puissent accéder à l'intégralité de ses fonds. Elle l'a fait. La nuit a été longue et terriblement émouvante, mais Déborah était heureuse d'avoir non seulement réparé son ordinateur, mais aussi économisé tout son argent en le transférant sur de nouveaux comptes sûrs. Elle s'est couchée épuisée.

Le lendemain matin, elle s'est connectée à son nouveau compte bancaire pour accéder à ses comptes d'épargne et de retraite récemment transférés, mais tout l'argent avait disparu. Dans la panique, elle a appelé le numéro d'assistance technique qu'elle avait appelé hier. Il n'y a pas eu de réponse. Elle a vite compris que toutes ses économies avaient disparu. Elle venait de donner tout son argent.

Comment éviter que cela ne vous arrive

Les cybercriminels ont appris que le moyen le plus simple d'infecter votre ordinateur ou de vous voler votre argent est de le demander. Les scarewares sont un moyen courant d'y parvenir : ils vous font croire que votre ordinateur est infecté alors qu'il ne l'est pas. Ils vous poussent ensuite à prendre des mesures hâtives afin de pouvoir profiter de vous. Cette histoire est basée sur des événements réels qui sont arrivés à des personnes réelles. L'ordinateur de Déborah n'a jamais été infecté, elle a plutôt visité par accident le mauvais site web. L'entreprise d'assistance technique n'était pas une vraie entreprise, mais une équipe de cybercriminels à l'autre bout du monde. Même la fraude bancaire et les agents gouvernementaux n'étaient que des membres différents de la même équipe de cybercriminels. Une fois que les cybercriminels vous auront eu au téléphone, ils feront tout leur possible pour gagner de l'argent. Comment pouvez-vous vous protéger ?

- Etre méfiant est votre meilleure défense. Chaque fois que quelqu'un essaie de vous pousser à entreprendre une action, il peut s'agir d'une attaque. Plus vous avez une impression d'urgence, plus vous avez de chance que ce soit une arnaque.
- Aucune entreprise légitime ne vous demandera jamais votre mot de passe. Aucune banque ne va vous demander de déplacer votre argent.
- N'utilisez jamais les informations de contact fournies dans une alerte ou une fenêtre pop-up. Si vous voulez vérifier la légitimité d'une alerte, utilisez toujours des méthodes de contact que vous connaissez déjà, comme les numéros de téléphone figurant sur vos relevés bancaires ou vos cartes de crédit, ou utilisez des liens mis en signet dans votre navigateur.

Si vous pensez que vous ou une personne qui vous est chère avez été victimes d'une escroquerie financière, signalez-le immédiatement aux services de police et à votre banque. Plus tôt vous le signalerez, plus vous aurez de chances de récupérer votre argent.

Ressources

Ingénierie sociale : https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Navigateurs : https://www.sans.org/newsletters/ouch/browsers
Les déclencheurs émotionnels :
https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Les attaques par hameçonnage deviennent de plus en plus travaillées :
https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Traduit pour la communauté par : Juliette Busson