Des malveillants de sexe, jusqu'à la publication de vous nue !

Dans cet articles nous allons voir ; des malwares se propagent par PornHub, Facebook veut vos photos intimes, un ransomware qui exigent des photos intimes de vous pour débloquer votre PC ou Tablette/Smartphone.

Des malwares se propagent par PornuHub :

Aujourd'hui, un collègue m'a transmis un article indiquant que le célèbre site de pornographie en ligne PornHub envoyait des publicités avec des malwares intégrés qui infectaient les ordinateurs des utilisateurs en se faisant passer pour des mises à jour importantes de navigateurs. L'attaque, signalée par Proofpoint, provient du groupe KovCoreG.

Vous avez peut-être le réflexe de dire, *Ça ne peut pas me concerner !* ou *Qui donc regarde du porno sur Internet ?* mais PornHub est un site très populaire, et cela rend la menace pertinente pour plus de personnes que ce que vous pouvez imaginer. Selon Alexa, il s'agit du vingtième site le plus populaire aux États-Unis et le 37e au monde. L'année dernière, 92 milliards de vidéos (le lien ne comporte pas d'images gênantes) ont été regardées sur le site.

Donc oui, ce problème pourrait être important.

Que pouvez-vous faire pour vous protéger d'attaques de ce type ?

• **Ne cliquez pas.** Je l'ai répété de nombreuses fois, mais ça vaut la peine de le répéter : si vous êtes sur un site que vous n'assumeriez pas avoir visité devant votre grand-mère, réfléchissez bien avant de cliquer sur des pubs ou de télécharger quoi que ce soit.
• **SI vous devez cliquer, vérifiez bien tous les liens.** Dans ce cas particulier, les fausses mises à jour venaient de sites qui n'avaient aucun lien

avec les développeurs de navigateurs.

• **Exécutez votre anti-virus.** Les bonnes solutions de cybersécurité ont une protection multicouches qui aide les utilisateurs à éviter les cybermenaces à différents points d'une cyberattaque.

Facebook veut des photos intimes.. :

Nous avons tous entendu parler de ces cas où un ex révèle des photos intimes en ligne sans le consentement de la personne. Même les célébrités en sont victimes, et les fuites d'images alimentent bien des tabloïdes.

Pour la plupart des utilisateurs, la publication de telles images privées ou revenge porn est une catastrophe, et certains cas de suicides ont amené ces affaires dans les médias mainstream. Il va sans dire que ces fuites représentent une grande violation de la confidentialité et ne devraient pas avoir lieu dans une société civilisée. Cependant, ce sont des choses qui arrivent.

C'est pour cela que Facebook propose une approche intéressante qui vise à prévenir la publication de photos intimes sans l'accord de leurs sujets, au moins sur Facebook ou Instagram ainsi que par Facebook Messenger. L'idée qu'a eu le réseau social et sur laquelle elle travaille avec le gouvernement australien, c'est de suggérer aux utilisateurs d'envoyer les photos qui les préoccupent à la société elle-même.

Attendez… quoi ?!

Oui, vous avez bien lu. Voici les détails : Le plan de Facebook est de chiffrer les images privées en utilisant hachage ; ainsi, si quelqu'un envoie ou publie cette image sur Facebook, Messenger ou Instagram, le service peut détecter cette image en comparant sa somme de hash à celles de la base de données de Facebook et empêcher sa transmission.

Le commissaire a la sécurité en ligne australien a déclaré à ABC News comment cela est supposé fonctionner : Facebook suggérera aux utilisateurs de lui envoyer leurs photos les plus intimes par Facebook Messenger, et ce en se les envoyant à eux-mêmes. Les images seront hachées lors de l'envoi. Ensuite, si quelqu'un essaie de publier une image avec la même valeur de hash, celle-ci ne sera visible pour personne. Facebook affirme que le chiffrage d'extrémité en extrémité utilisé sur Messenger (sur l'application mobile, pas sur les ordinateurs) assurera que les photos seront sûres car il exclut les intermédiaires et que les images elles-mêmes ne seront pas stockées, ce qui les rend immunes au vol.

Est-ce que ça marchera vraiment ?

Facebook a annoncé le programme pilote au Royaume-Uni, aux États-Unis, en Australie et au Canada, pour le moment. Nous ne savons donc pas encore à quel point il sera efficace. D'une part, il a un vrai potentiel de solution contre cette menace. De l'autre, on peut encore se demander comment s'assurer que cela ne deviendra pas un moyen de chiffrer les photos publiques de quelqu'un d'autre. Parce que le chiffrage d'extrémité à extrémité ne permet pas à Facebook de regarder les photos, il ne pourra pas utiliser des algorithmes d'apprentissage machine pour distinguer une photo de nu d'une autre, par exemple.

En outre, de nombreuses personnes sont encore inquiètes à l'idée de donner leurs photos à une tierce partie, que ce soit Facebook ou une autre entreprise, et sur la sécurité de toute technologie qu'elle ne connaît pas, en particulier s'il s'agit de Facebook où plusieurs photos d'utilisateurs privées ont déjà fait l'objet de fuites..

Y a-t-il une meilleure manière ? Pour de nombreuses personnes, oui :

1. Si vous prenez une photo nue ou potentiellement compromettante de vous-même, ce ne sont pas mes affaires. Mais il faut savoir que ce sont des cibles tentantes et qu'il vaut donc la peine de bien y réfléchir. Si les photos n'existent pas, elles ne peuvent pas fuiter.
2. Si vous prenez des photos de ce type, stockez-les hors ligne sur un dispositif de stockage chiffré.
3. Si vous voulez partager quelque chose qui peut être utilisé pour vous ridiculiser ou vous blesser en atterrissant entre de mauvaises mains (ou en cas de changement d'intentions, comme après une rupture), soyez prêt à faire face à des conséquences difficiles.
   Une fois que quelque chose est mis en ligne sur Internet, cela peut

devenir public quelle que soit la sécurité du service en ligne. Le facteur humain compte aussi, il n'existe pas de système absolument sûr.

Un Ransomware exigent des photos nues de vous :

On considère depuis un certain temps déjà les ransomwares comme un fléau d'Internet. C'est l'une des menaces virtuelles principales du XXIe siècle, et elle s'est récemment présentée sous un jour assez surprenant… Des chercheurs de MalwareHunterTeam ont découvert une nouvelle souche de ransomware appelé nRansom qui bloque les ordinateurs des victimes et, au lieu d'exiger de l'argent pour débloquer l'ordinateur, demande des photos nues de l'utilisateur.

Ce ransomware ne semble pas être un chiffreur mais un bloqueur, ce qui veut dire qu'en cas d'infection, il ne chiffre pas vos fichiers mais bloque simplement l'accès à votre ordinateur. La note de rançon qui apparaît sur l'écran informe les victimes que la seule manière d'accéder à leurs ordinateurs est d'envoyer des photos : dix photos des victimes nues.

Elle indique qu'ils vérifieront d'une certaine manière que ces photos nues appartiennent bien à la victime avant d'envoyer le code pour débloquer

l’ordinateur.

https://twitter.com/malwrhunterteam/status/910952333084971008

À ce jour, nRansom n’a été détecté que sous forme de fichier appelé nRansom.exe., ce qui signifie qu’il ne peut toucher que les utilisateurs de Windows.

Nous ne pouvons que faire des spéculations sur ce que les criminels comptent faire avec les photos qu’ils obtiendront. Ils utiliseront probablement les photos pour harceler les victimes et essayer de leur soutirer plus de photos nues ou de l’argent.

Comme toujours, nous vous recommandons de ne pas payer la rançon si votre ordinateur est infecté. Dans ce cas, le mot » payer » est aussi légitime qu’avec les rançons en argent ; les informations privées constituent un paiement au même titre que l’argent.

KASPERSKY détecte nRansom en tant que Trojan-Ransom.MSIL.Agent.zz et le neutralise immédiatement. Si le bloqueur s’est infiltré sur votre PC; vous pouvez débloquer l’ordinateur en appuyant sur Ctrl + Alt + Maj + F4 simultanément. (pour faire cette commande, vous devez être équipé d'un antivirus KASPERSKY, si pas le cas contactez-moi)

Cette technique est disponible dans toutes nos sécurités de solutions vedettes et fonctionne contre tous les bloqueurs si ceux-ci se sont infiltrés sur votre ordinateur. Cependant, si vous laissez votre solution activée, cela est très peu probable ; KASPERSKY neutralise presque toutes les sortes de ransomware avant qu’ils ne fassent quoi que ce soit, et ceux qui parviendraient à s’infiltrer malgré tout sont détectés par le System Watcher quand ils tentent de faire quelque chose de malveillant.