Des malveillants derrière des images

Les applications de messagerie sont non seulement utiles pour rester en contact avec d'autres, mais elles constituent également une porte ouverte par laquelle des intrus peuvent pénétrer dans nos vies. Aujourd'hui, nous allons parler d'une nouvelle infection multifonctionnelle détectée par les experts de chez KASPERSKY Lab.
Elle s'attaque aux ordinateurs de bureau et se répand à travers Telegram de manière très ingénieuse également.

Le malware devient une image de chaton !

L'une des principales tâches des créateurs de chevaux de Troie est de persuader les utilisateurs d'exécuter les malwares. Pour ce faire, ils utilisent toute une série de techniques pour faire passer pour inoffensifs des fichiers dangereux.

En ce qui concerne cette astuce particulière, gardez à l'esprit que certaines langues s'écrivent de droite à gauche, comme l'arabe et l'hébreu, et qu'Unicode, la norme informatique et l'ensemble presque omniprésent des caractères, fournit un moyen de changer la direction des mots écrits. Si vous utilisez un caractère spécial invisible, la chaîne de lettres qui suit s'affiche automatiquement dans l'ordre inverse. C'est ce que les pirates informatiques ont exploité lors d'une attaque récente.

Supposons qu'un cybercriminel crée un fichier malveillant appelé Trojan.js. Comme vous pouvez le voir grâce à l'extension JS, il s'agit d'un fichier JavaScript, et il peut contenir n'importe quel code exécutable.

Un utilisateur prudent se méfiera automatiquement et ne l'exécutera pas. Mais l'escroc peut le renommer – par exemple : chaton_mignon*U+202E*gnp.js.

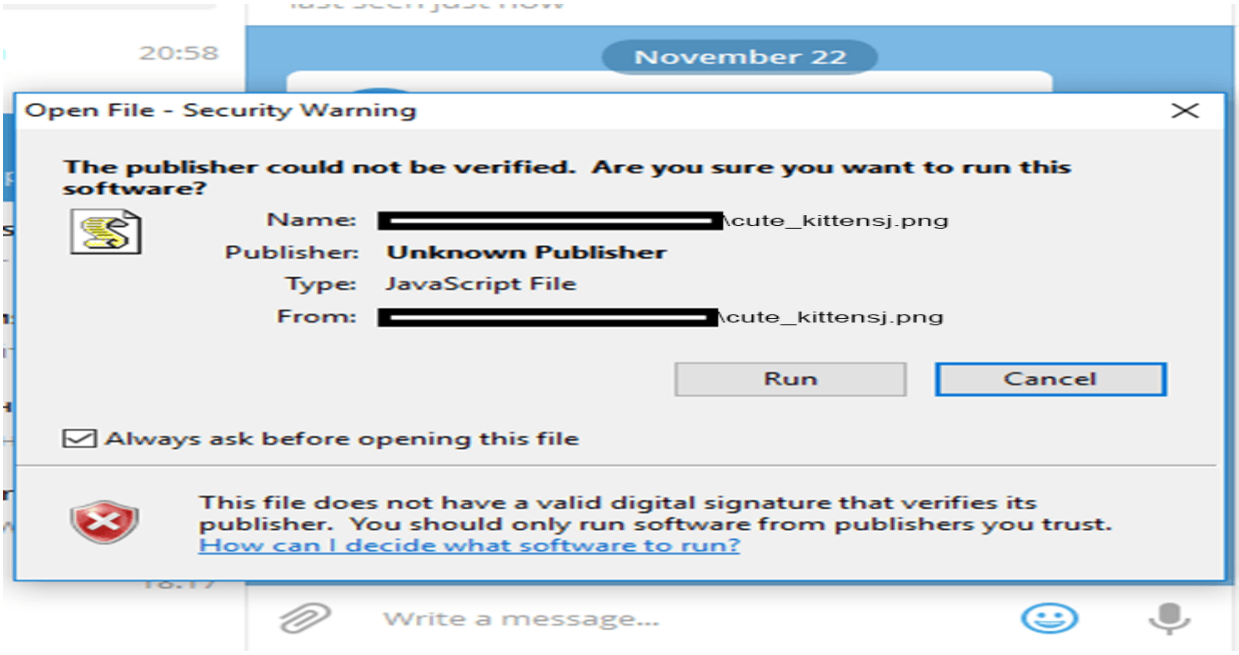
Cela semblerait encore pire à notre utilisateur… sauf qu'ici, U+202E est le caractère Unicode après lequel les lettres et les signes de ponctuation sont affichés de gauche à droite. Le nom du fichier sera par conséquent affiché comme suit : chaton_mignonsj.png**.** L'extension du fichier semble à présent être PNG ; on dirait un fichier d'image parfaitement normal, mais en réalité, il s'agit d'un cheval de Troie JavaScript.

Cette technique utilisant Unicode n'est pas nouvelle. Elle est utilisée pour masquer des pièces jointes d'e-mails et des téléchargements de fichiers depuis près d'une décennie, et de nombreux environnements se protègent déjà contre celle-ci. Mais quand Telegram a été visé pour la première fois, ça a marché. Autrement dit, Telegram a (ou plutôt avait) la vulnérabilité dite RLO, et c'est cela que nos chercheurs ont remarqué.

L'image de chaton devient un mineur ou une porte dérobée

La vulnérabilité n'a été détectée que dans le client Telegram Windows et pas dans les applications mobiles. Nos experts ont découvert non seulement son existence, mais aussi que les attaquants l'utilisaient activement. Les systèmes d'exploitation des victimes doivent les avertir s'ils sont sur le point d'exécuter un programme d'une source inconnue (ce qui doit leur mettre la puce à l'oreille), mais de nombreuses personnes cliquent sur *Exécuter* sans même regarder le message.

Si vou voyez un fenêtr comm ce ci, arrêtez-vou et réflé
Ou plutôt, arrêtez-vou tout co



Une fois lancé, le malware montre vraiment un « chaton mignon » pour éloigner toutes les suspicions. Le cheval de Troie est livré avec différents types de charge utile à exécuter en cachette, selon sa configuration.

Les plus courantes sont les mineurs cachés. Quand ils sont exécutés, l'ordinateur ralentit, surchauffe et finit généralement par s'endommager en essayant de miner des devises chiffrées pour les attaquants. L'alternative, c'est une porte dérobée qui permet aux cybercriminels de contrôler l'ordinateur à distance et de faire tout ce qu'ils veulent avec, de la suppression et l'installation de programmes à la collecte de données personnelles. Ce type d'infection peut rester caché longtemps sans que l'utilisateur ne se doute de rien.

Restez calme et continuez

Nos chercheurs ont rapidement signalé la vulnérabilité aux développeurs de Telegram qui l'ont corrigée (au grand dam des cybercriminels qui voulaient l'exploiter). Cependant, cela ne signifie certainement pas que Telegram et d'autres applications de messagerie instantanée populaires sont exempts de vulnérabilités. Celles-ci n'ont tout simplement pas encore été signalées. Ainsi, pour rester protégé contre de futurs fléaux, rappelez-vous quelques règles de sécurité simples. Celles-ci sont valables pour les médias sociaux, la messagerie instantanée et tout autre moyen de communication électronique :

- Ne téléchargez pas ou n'ouvrez pas de fichiers à partir de sources risquées. Si quelqu'un que vous ne connaissez pas vous envoie une photo, réfléchissez à deux fois avant de l'ouvrir.

- Si vous voyez un avertissement système concernant l'ouverture d'un fichier, vérifiez si la description correspond au fichier que vous êtes sur le point d'ouvrir.

- Prévenez votre prestataire en dépannage informatique à domicile le plus proche de chez vous et le plus réactif (http://MarcoServices.fr)

  Néanmoins, je ne peux que vous conseillez de prendre un bon antivirus payant ! Cela limitera beaucoup de problèmes. Dites-vous que cela n'arrive pas qu'aux autres..
  A ce jour la meilleure protection reste les produits KASPERSKY LAB, dont je dispose.