AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Les malwares LokiBot et NanoCore

Contenu

I. Contexte

Une campagne de spam en cours a été détectée, chaque spam contient des pièces jointes d'images de disque ISO qui dissimulent divers chevaux de Troie voleurs d'informations, notamment LokiBot et NanoCore. Les chercheurs ont déclaré avoir découvert pour la première fois les e-mails de spam créés par des hackers en avril 2019. Les spams envoyés aux victimes prétendent être un message générique concernant une facture ou une annonce pour la victime incluant un fichier ISO en pièce jointe. En réalité, la pièce jointe contient différentes charges malveillantes, notamment les chevaux de Troie d'accès distant LokiBot et NanoCore.

II. Fonctionnement

La campagne actuelle a débuté en avril 2019 avec un message générique concernant une facture. Il ne semble pas être ciblé contre des individus ou des entreprises spécifiques. Toutefois, si le courrier électronique parvient à la boîte de réception de l'utilisateur, l'avantage est du côté des attaquants. Cette pratique peut être courante car les fichiers ISO et emails sont souvent ajoutés à la liste blanche dans les moteurs d'analyse. De plus, si la cible ne la reconnaît pas comme suspecte et clique sur la pièce jointe, de nombreux systèmes d'exploitation détectent et montent automatiquement l'image ou ouvrent le mail.

Jusqu'à présent, les chercheurs ont détecté une dizaine de variantes dans la campagne en cours, utilisant différentes images ISO et emails. Le contenu a presque toujours été LokiBot ou NanoCore. Les fichiers d'image ISO sont conçus pour contenir tout le contenu d'un disque optique. En tant que tels, les fichiers légitimes ont tendance à avoir une taille de 100 Mo ou plus. C'est l'un des premiers indices détectés par les chercheurs tous les fichiers ISO observés étaient dans la plage de taille de 1 Mo à 2 Mo, ce qui est une taille de fichier inhabituelle pour les fichiers image.

LokiBot

Le cheval de Troie LokiBot, par exemple, est un voleur d'informations connu pour son apparence commune à divers types de pièces jointes. Cette campagne particulière revendique une version légèrement modifiée de LokiBot: par exemple, le malware a une nouvelle fonction «IsDebuggerPresent ()» pour déterminer s'il est chargé dans un débogueur (programme informatique utilisé pour tester et déboguer d'autres programmes); ainsi qu'une technique anti-VM commune, qui mesure la différence de temps de calcul entre deux processus (CloseHandle () et GetProcessHeap ()) afin de détecter s'il s'exécute dans une machine virtuelle (le temps différent serait plus grand dans le cas d'une machine virtuelle).

Une fois que le cheval de Troie a infecté le système, il interroge plus de 25 navigateurs Web différents pour dérober diverses informations de navigation, vérifie la présence de serveurs Web ou de serveurs de messagerie sur des ordinateurs et localise les informations d'identification de 15 clients de messagerie et de transfert de fichiers différents. En outre, le logiciel malveillant recherche la présence d'outils d'administration à distance populaires tels que Secure Shell (SSH) ou RDP (Remote Desktop Protocol).

NanoCore

Le second malware répandu dans la campagne est le cheval de Troie d'accès distant NanoCore, un cheval de Troie modulaire qui peut être modifié pour inclure des plug-ins supplémentaires, augmentant ses fonctionnalités et ses performances en fonction des besoins de l'utilisateur.

Une fois le cheval de Troie déployé, il capture un ensemble d'informations sur la machine victime, notamment: les données du presse-papiers et surveillance des frappes au clavier, collecte des données sur les fichiers de documents sur le système et connexion à un serveur FTP pour télécharger les données volées du système

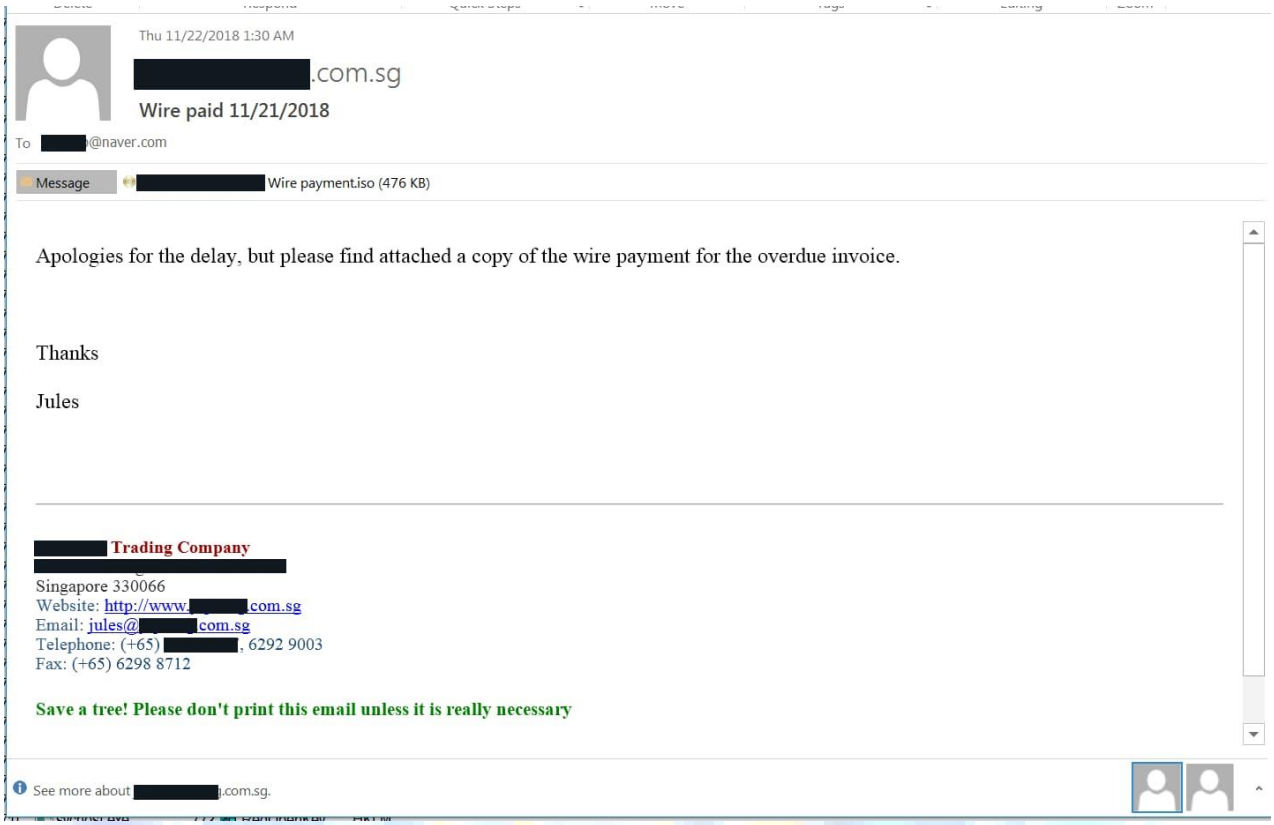
III. Comment se protéger ?

L'utilisation continue d'anciens logiciels malveillants et la réutilisation d'anciennes méthodes de distribution indique que les utilisateurs n'apprennent toujours pas à détecter les spams et les courriels de phishing, ni à utiliser des outils anti-malware adéquats pour les bloquer. Nous recommandons les mesures de sécurité ci-après :

- Faire attention lors de la navigation sur Internet, ainsi que lors du téléchargement et de l'installation de logiciels.
- S'assurer de toujours d'analyser soigneusement chaque pièce jointe reçue. Si le fichier ou le lien ne semble pas pertinent ou si l'expéditeur semble suspect ou inconnu, s'abstenir de toute action.
- Il est également extrêmement important d'avoir une suite antivirus/anti-logiciel espion de bonne réputation installée et en cours d'exécution, car de tels outils sont très susceptibles de détecter et d'éliminer les logiciels malveillants avant infection. Si vous pensez que votre ordinateur est déjà infecté, nous vous recommandons d'effectuer un scan à l'aide d'un antivirus pour éliminer automatiquement les logiciels malveillants infiltrés.
- Garder à jour les systèmes et appliquer les patches de sécurité publiés par les éditeurs des solutions et services exposés sur Internet.

IV. Annexe

Email infecté



Thu 11/22/2018 1:30 AM

[redacted].com.sg

Wire paid 11/21/2018

To [redacted]@naver.com

Message [redacted] Wire payment.iso (476 KB)

Apologies for the delay, but please find attached a copy of the wire payment for the overdue invoice.

Thanks

Jules

[redacted] **Trading Company**

[redacted]

Singapore 330066

Website: http://www.[redacted].com.sg

Email: jules@[redacted].com.sg

Telephone: (+65) [redacted], 6292 9003

Fax: (+65) 6298 8712

Save a tree! Please don't print this email unless it is really necessary

See more about [redacted].com.sg.