Communiqué de presse

Dans des versions piratées de Windows 10, un Trojan stealer vole de la crypto-monnaie. Il infiltre le PC via la partition système EFI.

Le 15 juin 2023

Doctor Web a détecté un Trojan stealer dans un certain nombre de versions non officielles de Windows 10, que les attaquants ont distribuées via un tracker torrent. Nommée Trojan.Clipper.231, cette application malveillante remplace les adresses des portefeuilles crypto dans le presse-papiers par des adresses indiquées par les pirates. À l'heure actuelle, à l'aide de ce malware, les attaquants ont réussi à voler de la crypto-monnaie pour un montant équivalent à environ 19 000 $.

Fin mai 2023, un client a contacté Doctor Web car il soupçonnait que son ordinateur, tournant sous Windows 10, était infecté. L'analyse menée par nos spécialistes a confirmé la présence de chevaux de Troie dans le système : le stealer **Trojan.Clipper.231** et les applications malveillantes **Trojan.MulDrop22.7578** et **Trojan.Inject4.57873** ayant assuré son lancement. Le laboratoire de Doctor Web a localisé avec succès toutes ces menaces et a réussi à les neutraliser.

Dans le même temps, il s'est avéré que le système d'exploitation cible était une version non officielle et que des logiciels malveillants y étaient initialement intégrés. Une enquête plus approfondie a révélé plusieurs de ces versions de Windows infectées :

- Windows 10 Pro 22H2 19045.2728 + Office 2021 x64 by BoJlIIIebnik RU.iso
- Windows 10 Pro 22H2 19045.2846 + Office 2021 x64 by BoJlIIIebnik RU.iso
- Windows 10 Pro 22H2 19045.2846 x64 by BoJlIIIebnik RU.iso
- Windows 10 Pro 22H2 19045.2913 + Office 2021 x64 by BoJlIIIebnik [RU, EN].iso
- Windows 10 Pro 22H2 19045.2913 x64 by BoJlIIIebnik [RU, EN].iso

Tous les builds étaient disponibles en téléchargement sur un tracker torrent, mais il ne peut pas être exclu que les attaquants utilisent d'autres sites pour distribuer des images infectées du système.

Les programmes malveillants dans ces assemblages se trouvent dans le répertoire système :

- \Windows\Installer\iscsicli.exe (**Trojan.MulDrop22.7578**)
- \Windows\Installer\recovery.exe (**Trojan.Inject4.57873**)
- \Windows\Installer\kd_08_5e78.dll (**Trojan.Clipper.231**)

L'initialisation du stealer se fait en plusieurs étapes. D'abord, le planificateur système est utilisé pour lancer le programme malveillant **Trojan.MulDrop22.7578**:

```
%SystemDrive%\Windows\Installer\iscsicli.exe
```

Doctor Web France – Cécile Chastanet-Responsable communication. c.chastanet@drweb.com

Son objectif est de monter la partition système EFI sur le disque M:\, d'y copier deux autres composants puis de supprimer les fichiers originaux du Trojan du disque C:\, ensuite, il doit lancer **Trojan.Inject4.57873** et démonter la partition EFI.

A son tour, **Trojan.Inject4.57873** utilisant la technique Process Hollowing, infiltre **Trojan.Clipper.231** dans le processus système %WINDIR%\\System32\\Lsaiso.exe, ensuite, le stealer se met à fonctionner.

Après avoir obtenu le contrôle, **Trojan.Clipper.231** commence à suivre le presse-papiers et remplace les adresses copiées des portefeuilles crypto par des adresses indiquées par les pirates. Le malware agit avec un certain nombre de restrictions. Tout d'abord, il ne commence à remplacer que s'il existe le fichier système %WINDIR%\\INF\\scunown.inf. Deuxièmement, le cheval de Troie vérifie les processus actifs. S'il détecte les processus d'un certain nombre d'applications qui sont dangereuses pour lui, il ne falsifie pas les adresses de portefeuille crypto.

L'infiltration de logiciels malveillants dans la partition système EFI des ordinateurs en tant que vecteur d'attaque est encore très rare. Par conséquent, le cas identifié est d'un grand intérêt pour les spécialistes de la sécurité informatique.

Selon les calculs de nos analystes, au moment de la publication de la news, les pirates ayant utilisé le stealer **Trojan.Clipper.231** ont volé 0.73406362 BTC et 0.07964773 ETH, ce qui équivaut à peu près à un montant de18 976 $.

Doctor Web recommande aux utilisateurs de télécharger uniquement des images ISO originales des systèmes d'exploitation et uniquement à partir de sources fiables, telles que les sites Web des éditeurs. Dr.Web Antivirus détecte et neutralise **Trojan.Clipper.231** ainsi que les applications malveillantes associées, de sorte que ces chevaux de Troie ne présentent pas de danger pour nos utilisateurs si leur antivirus est bien à jour et qu'aucune fonctionnalité importante n'est désactivée.

En savoir plus sur **Trojan.Clipper.231**

En savoir plus sur **Trojan.MulDrop22.7578**

En savoir plus sur **Trojan.Inject4.57873**

Indicateurs de compromission