Les chercheurs d'ESET, 1er éditeur Européen de solutions de sécurité, ont découvert une famille de malwares de type cheval de Troie, jusqu'alors inconnue, qui se répand via des torrents malveillants et qui utilise plusieurs ruses pour voler autant de cryptomonnaie que possible auprès de ses victimes, tout en échappant à la détection. ESET a nommé la menace KryptoCibule, et selon la télémétrie d'ESET, le malware semble cibler principalement des utilisateurs en République tchèque et en Slovaquie.

Ce malware est une triple menace en ce qui concerne les cryptomonnaies. Il utilise les ressources de la victime pour miner des cryptomonnaies, tente de détourner des transactions en remplaçant les adresses des portefeuilles dans le presse-papiers, et exfiltre des fichiers liés aux cryptomonnaies, tout en déployant de multiples techniques pour éviter d'être détecté. KryptoCibule utilise largement le réseau Tor et le protocole BitTorrent dans son infrastructure de communication.

« Le malware, tel qu'il a été développé, utilise des logiciels légitimes. Certains d'entre eux, tels que Tor et le client de torrents Transmission, sont fournis avec le programme d'installation ; d'autres sont téléchargés au moment de l'exécution, notamment les serveurs Apache httpd et SFTP Buru, » explique Matthieu Faou, le chercheur d'ESET qui a découvert la nouvelle famille de malwares.

ESET a identifié plusieurs versions de KryptoCibule, qui sont encore actives, ce qui nous a permis de retracer leurs débuts à décembre 2018. De nouvelles fonctionnalités ont été régulièrement ajoutées au malware au cours de sa constante évolution.

La plupart des victimes sont situées en République tchèque et en Slovaquie, ce qui reflète la base d'utilisateurs du site qui héberge les torrents infectés. Presque tous les torrents malveillants étaient disponibles sur uloz.to, un site de partage de fichiers très populaire dans les deux pays. KryptoCibule recherche également spécifiquement la présence des produits de sécurité pour terminaux : ESET, Avast et AVG. ESET a son siège en Slovaquie, tandis que les deux autres sont détenus par Avast, dont le siège est situé en République tchèque.

« KryptoCibule possède trois composants qui exploitent les hôtes infectés afin d'obtenir de la cryptomonnaie : chiffrement, détournement du presse-papiers et exfiltration de fichiers, » poursuit M. Faou. « On peut supposer que les opérateurs du malware ont réussi à gagner plus d'argent en volant des portefeuilles et en extrayant des cryptomonnaies que ce que nous avons trouvé dans les portefeuilles utilisés par le composant de détournement du presse-papiers. À lui seul, le revenu généré par ce composant ne semble pas suffisant pour justifier l'effort de développement observé. » Pour plus de détails techniques sur KryptoCibule, lisez l'article « KryptoCibule: The multitasking multicurrencycryptostealer » sur WeLiveSecurity. Suivez l'actualité d'ESET Research sur Twitter.

Composants et outils de KryptoCibule

file:///C:/Users/HP/AppData/Local/Temp/msohtmlclip1/01/clip_image001.png" />

Darina SANTAMARIA - 06 61 08 42 45 - darina.j@eset-nod32.fr

À propos d'ESET

Spécialisé dans la conception et le développement de logiciels de sécurité pour les entreprises et le grand public, ESET est aujourd'hui le 1er éditeur de l'Union européenne en matière de sécurité des endpoints. Pionnier en matière de détection proactive, ESET a été désigné pour la 2ème année consécutive, unique Challenger dans le Gartner Magic Quadrant 2019*, « Endpoint Protection » après avoir été évalué sur sa performance et sur la qualité de sa vision dans le domaine de la protection des Endpoints. À ce jour, l'antivirus ESET NOD32 détient le record mondial de récompenses décernées par le laboratoire indépendant Virus Bulletin depuis 1998. La technologie ESET protège aujourd'hui plus d'un milliard d'internautes. *Source : Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, PrateekBhajanka, Paul Webber, August 20, 2019.

Pour plus d'informations : www.eset.com/fr/ Blog : www.welivesecurity.com/fr/