**« Gootloader » infecte insidieusement les internautes avec des logiciels malveillants et des ransomware**

* *Campagnes ciblées détectées aux* *États-Unis, en Allemagne, en* *Corée du Sud et* *en France*
* *Bientôt en Belgique ?*

Oosterhout, 1 mars 2021 - **Une nouvelle recherche de Sophos montre comment des criminels ont transformé la méthode d’infection pour "Gootkit" malware financier en une plate-forme de livraison complexe pour un large éventail de logiciels** [**malveillants,**](http://www.sophos.com/) **y compris des ransomware. Les chercheurs de Sophos ont nommé la plate-forme de livraison , « Gootloader ». Les attaquants Gootloader atteignent leurs cibles en piratant des sites Web légitimes et en modifiant subtilement le contenu. Ainsi, les sites Web peuvent afficher un contenu différent pour chaque visiteur.**

Ces opérateurs criminels manipulent l’optimisation des moteurs de recherche (SEO) de sorte que lorsqu’une personne pose une question dans un moteur de recherche comme Google, les sites piratés apparaissent parmi les meilleurs résultats. Ce qui se passe après le clic de l’utilisateur sur un lien vers un site web piraté dépend de leur pays d’origine.

Par exemple, si un utilisateur en provenance d’un pays qui n’est pas une « cible » clique sur un site Web piraté, ces sites sont alors désignés comme bénins ou comme un faux contenu Web et rien ne se passe.

Toutefois, si les utilisateurs viennent de l’un des pays ciblés par Gootloader et cliquent sur un site web piraté, ils atterrissent sur une page comportant un faux forum de discussion sur le sujet même qu’ils ont recherché, utilisant les mêmes termes qu’ils ont tapé dans le moteur de recherche. Les faux sites web se ressemblent, qu’ils soient en anglais, allemand ou coréen.

Le faux forum de discussion comprend un message d’un « administrateur de site », avec un lien vers un téléchargement. Le téléchargement est un fichier malveillant. Si le lien est cliqué, la prochaine étape de l’infection commence.

À partir de ce moment, l’attaque procède sous couverture, via une charge malveillante à la cible en utilisant un large éventail de techniques d’évasion pour éviter la détection par des outils de sécurité.

Gootloader livre actuellement des logiciels malveillants financiers Kronos en Allemagne, ainsi qu’un outil post-exploitation appelé Cobalt Strike aux États-Unis et en Corée du Sud. Les attaquants ont également livré REvil ransomware et le cheval de Troie Gootkit lui-même comme charges utiles lors d’opérations antérieures visaient la France.

« Les développeurs derrière Gootkit semblent avoir déplacé les ressources de la livraison de leurs propres logiciels malveillants financiers pour voler des informations d’identification à la création d’une furtivité, plate-forme de livraison complexe pour toutes sortes de charges utiles, y compris REvil ransomware », a déclaré Gabor Szappanos, directeur de recherche sur les menaces à Sophos.

« Les créateurs de Gootloader utilisent un certain nombre de trucs d’ingénierie sociale qui peuvent tromper, même techniquement qualifiés, les utilisateurs de l’informatique. Heureusement, il ya quelques signes avant-coureurs que les internautes peuvent regarder. Il s’agit notamment des résultats de recherche Google qui pointent vers des sites Web pour les entreprises qui n’ont aucun lien logique avec les conseils qu’ils semblent offrir; une page qui correspond précisément aux termes de recherche utilisés dans la question initiale; et une page qui semble identique aux exemples montrés dans la recherche Sophos, avec du texte et un lien de téléchargement qui correspond également précisément aux termes de recherche utilisés dans la recherche initiale google.

**À propos de Sophos**

En tant que leader mondial en solution de cybersécurité Next-Gen, Sophos protège plus de 400 000 entreprises de toutes tailles, dans plus de 150 pays, contre les cybermenaces actuelles les plus avancées. Développées par les SophosLabs, une équipe présente dans le monde entier et spécialisée dans le renseignement sur les menaces et la science des données, les solutions Cloud-Native et basées sur l'IA de Sophos protègent les systèmes endpoint (les ordinateurs portables, les serveurs et les périphériques mobiles) ainsi que les réseaux contre les techniques de cyberattaque évolutives, notamment les ransomwares, les malwares, les exploits, l'exfiltration de données, le phishing, et bien plus encore. Sophos Central, la plateforme de management Cloud-Native, intègre l'ensemble des produits Next-Gen de Sophos, y compris la solution Intercept X endpoint et le pare-feu XG Next-Gen, via un système unique de « sécurité synchronisée » accessible via un ensemble d'API. Sophos commercialise ses produits et services exclusivement par l’intermédiaire d’un réseau mondial regroupant plus de 53 000 partenaires et fournisseurs de services gérés (MSP : Managed Service Provider). Sophos met également ses technologies commerciales innovantes à la disposition des particuliers via Sophos Home. Le siège de l’entreprise est basé à Oxford, au Royaume-Uni. Plus d'informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contact presse :**

Square Egg Communications, Sandra Van Hauwaert, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497251816.