Ce malware use d'une tactique imparable pour se répandre

Sécurité : *Le malware STRRAT, basé sur Java, crée une porte dérobée dans les ordinateurs infectées, mais distrait les victimes en agissant comme un rançongiciel. Une tactique insolite mais payante.*

Par Danny Palmer | Modifié le lundi 24 mai 2021 à 17:48

Une campagne massive de phishing distribue ce qui ressemble à une attaque trojan malware (cheval de Troie) qui crée un accès simulé dans les systèmes Windows pour voler les noms d'utilisateur, les mots de passe et autres données personnelles des victimes. Celle-ci repose sur une tentative de distraction mise en place pour dissimuler le fait que l'ordinateur a été compromis par un cheval de Troie à distance - une forme de malware très furtive, contrairement à une attaque de ransomware bien plus flagrante.

Dans le cadre du processus d'infection, le malware ajoute une extension de nom de fichier .crimson aux fichiers afin de faire passer l'attaque pour un ransomware - bien qu'aucun fichier ne soit réellement crypté.

Selon des chercheurs en cybersécurité de Microsoft, la dernière version du malware STRRAT, basé sur Java, est diffusée par le biais de courrier électronique, qui utilise des comptes de messagerie pour distribuer des messages prétendant être liés à des paiements, accompagnés d'une image se présentant comme une pièce jointe qui semble contenir des informations sur le transfert supposé. Le hacker dispose ensuite du contrôle total de l'ordinateur de la victime lorsque celle ci ouvre la pièce jointe.

Les boîtes mails infectés

Il est probable que cette campagne malveillante - ou d'autres campagnes de phishing similaires - soit toujours active, les cybercriminels poursuivant leurs tentatives de diffusion du malware STRRAT sur de nombreux appareils. Étant donné que le malware est capable d'accéder aux noms d'utilisateur et aux mots de passe, il est possible que toute personne dont le système est infecté voie son compte de messagerie utilisé de manière abusive par les hackers dans le but de propager STRRAT avec de nouveaux e-mails de phishing.

Comme ce malware repose sur des e-mails de phishing, il est possible de prendre des mesures pour éviter d'être touché. Il faut se méfier des messages inattendus ou inhabituels - en particulier ceux qui semblent offrir une incitation financière - et faire preuve de prudence lorsqu'il s'agit d'ouvrir des courriels et des pièces jointes provenant d'adresses électroniques étranges ou inconnues.

L'utilisation d'un logiciel antivirus pour détecter et identifier les menaces peut également contribuer à empêcher les courriels malveillants d'atterrir dans les boîtes de réception, éliminant ainsi le risque que quelqu'un ouvre le message et clique sur le lien malveillant.

Source : ZDNet.com

A lire aussi :
Apple s'inquiète de la quantité de malwares sur les Mac
La cybersécurité s'impose comme la raison principale pour laquelle Apple doit garder l'iPhone, l'iPad et ses autres...

Sujet: *Cyberattaque* *Cybercriminalité* *Cybersécurité* *Données privées* *Gestion de données* *Protection des données* *Ransomware* *Logiciels* *Malware*

Par Danny Palmer | Modifié le lundi 24 mai 2021 à 17:48