ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

NOTE D'INFORMATION

Titre	Ransomware se présente comme application de suivi du coronavirus
Numéro de Référence	23811703/20
Risque	Important
Impact	Important

Résumé :

Vu les circonstances actuelles, et vu la vaste médiatisation du coronavirus, plusieurs applications et sites web malveillants ont apparu exploitant le thème de coronavirus afin d'infecter un nombre important de victimes.

Une nouvelle application de suivi de Coronavirus, CovidLock qui est en réalité un ransomware, disponible sur le site coronavirusapp [.], invite les victimes à lui attribuer l'accessibilité et les autorisations de verrouillage sur leurs appareils. Par conséquence, le ransomware chiffre les appareils des victimes, puis demande qu'une rançon de 100$ soit payée (en Bitcoin) dans un délais de 48 heures pour récupérer l'accès à l'appareil. De plus, les auteurs de ce ransomware avertissent les victimes que les contacts, photos et autres contenus seront supprimés et les comptes de médias sociaux seront divulgués.

Un autre exemple d'attaques vise spécifiquement les victimes qui recherchent des présentations cartographiques de la propagation de coronavirus sur Internet. Un utilisateur peut télécharger et exécuter une application malveillante qui montre une carte de propagation de la maladie, mais en arrière-plan installe un malware afin de compromettre les machines des victimes et voler leurs informations confidentielles.

BlackWater est une autre variante de malware qui profite de l'épidémie du coronavirus. L'attaque est initiée par des e-mails de phishing contenant des pièces jointes malveillantes qui prétendent être des informations sur le coronavirus (COVID-19) pour attirer les victimes. Une fois ouvertes, le malware extrait un document Word Microsoft Office permettant l'exécution et l'installation du malware sur l'ordinateur de la victime.

Pour contrer ce type d'attaques, il est conseillé aux utilisateurs de s'assurer qu'ils ne téléchargent que des applications de confiance, n'utilisent que les ressources des gouvernements et des établissements de santé concernant le coronavirus.

Référence :

- https://www.androidauthority.com/covidlock-coronavirus-ransomware-1093465/
- https://www.scmagazine.com/home/security-news/cybercrime/foreign-apt-groups-use-coronavirus-phishing-lures-to-drop-rat-malware/
- https://thehackernews.com/2020/03/coronavirus-maps-covid-19.html
- https://www.bleepingcomputer.com/news/security/blackwater-malware-abuses-cloudflare-workers-for-c2-communication/

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma