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	Distribution de malwares exploitant l'épidémie du coronavirus
Numéro de Référence	23811703/20
Risque	Important
Impact	Important

Résumé :

Vu les circonstances actuelles et la vaste médiatisation du coronavirus, plusieurs applications et sites web malveillants sont apparus. Le but est d'infecter un nombre important de victimes.

A titre d'exemple, l'application de suivi de Coronavirus « CovidLock » n'est en réalité qu'un ransomware, disponible sur le site « coronavirusapp[.] ». Ce ransomware chiffre les appareils des victimes, puis demande qu'une rançon de 100$ soit payée (en Bitcoin) dans un délai de 48 heures pour récupérer l'accès à l'appareil infectée. Les auteurs de ce ransomware avertissent les victimes que les contacts, photos et autres contenus seront supprimés d'une part et les comptes de médias sociaux seront divulgués d'autre part.

Un autre exemple d'attaques vise spécifiquement les victimes qui s'intéressent aux 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 elle installe un malware afin de compromettre les machines des victimes et partant de voler les informations confidentielles.

BlackWater est une autre variante des malwares apparus dans ce sillage. L'attaque est initiée par des e-mails de phishing contenant des pièces jointes malveillantes qui prétendent contenir des informations pertinentes sur le coronavirus (COVID-19) pour attirer les victimes. Une fois ces pièces ouvertes, le malware est installé sur l'ordinateur de la victime.

Pour contrer ce type d'attaques, il est conseillé de s'assurer que la source des applications est de confiance et que les ressources utilisées proviennent d'établissements de santé gouvernementaux ou de médias officiels.

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

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