Ne laissez pas les cybercriminels transformer la panique en profit

Nos amis de Recorded Future ont confirmé l'enregistrement de milliers de faux sites Web liés au coronavirus. Ne vous méprenez pas : ces domaines sont utilisés pour hameçonner vos informations ou infecter les réseaux informatiques avec des logiciels malveillants.

En exploitant les peurs actuelles dues à l'épidémie mondiale de COVID-19, les criminels misent sur le fait que des employés naïfs cliqueront sans réfléchir sur les liens en rapport avec le coronavirus. Le risque de menace est encore exacerbé par les centaines de milliers d'employés travaillant désormais depuis chez eux à travers le monde.

Dans sa synthèse hebdomadaire, le centre VTRAC (Verizon Threat Research Advisory Center) a rendu compte de nombreux évènements liés à la sécurité, notamment le déploiement de correctifs pour plus de 116 produits Microsoft, ainsi que différentes attaques APT menées par de multiples acteurs.

Que font-ils ?
Parmi les nombreuses organisations ayant émis des avertissements, la FTC (Federal Trade Commission) a publié une note alertant les consommateurs de la recrudescence des emails, messages texte et appels téléphoniques frauduleux dont l'émetteur affirme travailler pour un CDC (centre américain de contrôle et de prévention des maladies). Ces sites Web proposent un « remède » au virus sous la forme de médicaments, de vaccins et de kits de test.

Selon l'agence sanitaire de l'ONU, des criminels tentent également de se faire passer pour des représentants de l'OMS afin de commettre différentes escroqueries, notamment des piratages de compte, de fausses demandes de dons et des campagnes de propagation de logiciels malveillants.

KrebsonSecurity a révélé qu'un tableau de bord interactif des infections et des décès liés au coronavirus élaboré par l'Université Johns Hopkins est employé par des sites Web malveillants afin de diffuser des programmes malveillants.

Comment s'y prennent-ils ?
Même avant la crise du COVID-19, l'hameçonnage constituait une technique prisée et efficace pour les pirates. Cette méthode consiste à dérober vos identifiants de connexion pour obtenir des informations sensibles, souvent via un email contenant un lien vers un faux site Web identique à une page de connexion d'un fournisseur de messagerie cloud.
Selon de rapport d'enquête complet sur le piratage de données (DBIR) 2019 de Verizon, près d'un tiers des piratages ont fait appel à une attaque d'hameçonnage, le principal mode d'attaque utilisé lors des piratages réussis.

Lorsque des attaquants s'en prennent à vous, ils savent que votre entreprise a mis en place des protocoles de sécurité. C'est pourquoi ils se voient obligés de prendre différentes mesures avant d'obtenir gain de cause.
Le DBIR ajoute que 28 % des 2 000 piratages ont impliqué une infraction de programmes

malveillants (généralement transmis par email), tandis que 29 % ont nécessité l'emploi d'identifiants de connexion volés, ces deux méthodes recourant fréquemment à des attaques d'hameçonnage.

Que puis-je faire ?

Pour éviter tout risque, si vous détectez des messages provenant de domaines liés au coronavirus, ne cliquez pas sur les pièces jointes et contentez-vous de les supprimer. Méfiez-vous des sites Web qui appellent à des dons, proposent des conseils et des produits médicaux, et offrent des recommandations liées aux marchés financiers. En bref, ne vous laissez pas appâter par les liens issus de sources inconnues.

Si un message provenant d'une organisation familière (banque, hôpital, etc.) rend état d'un problème important ou urgent, contactez l'expéditeur par un autre moyen officiel. Il va sans dire que vous devez tenir à jour la sécurité de votre système et chiffrer ou protéger par mot de passe vos informations sensibles. Si vous télétravaillez, assurez-vous que votre VPN emploie une authentification à deux facteurs afin de sécuriser votre connexion réseau.