Veille technologique

Dans cette veille, nous allons voire les dernières techniques utilisées par les cybercriminels pour tromper les utilisateurs et voler leurs informations sensibles. Le phishing est une forme d'attaque Dans en ligne qui vise à obtenir des informations confidentielles telles que des mots de passe, des numéros de carte de crédit ou des informations personnelles en se faisant passer pour une entité de confiance.

Une nouvelle version du logiciel malveillant Rhadamanthys, appelée Rhadamanthys 5.0, est en cours de déploiement contre les entreprises pétrolières et gazières.

Ces attaques utilisent un fichier PDF qui se font passer pour des communications provenant ‘d’organisation officielles’ pour tromper leurs cibles

Les attaques de phishing utilisent des lignes d'objet provocantes telles que "Notification : Incident impliquant votre véhicule" ou "Attention requise : Collision de votre véhicule".

Les e-mails de phishing sont soigneusement conçus pour cibler les émotions des destinataires. Chaque e-mail est différent, mais ils ont tous pour objectif de notifier un employé d'un incident de voiture par le biais d'une notification de l'employeur, de possibles actions légales ou même d'un avis de contact avec les forces de l'ordre.

Rhadamanthys 5.0 a été lancée peu de temps après la désactivation de LockBit en février.

La dernière version de Rhadamanthys, la version 5.0, a été mise à jour en 2024 avec des améliorations de ses capacités d'évasion et de vol de données.

Bien que les cibles soient les secteurs pétroliers et gaziers, la campagne pourrait être adaptée à d'autres secteurs si les acteurs malveillants décidaient de changer de cible.

Il est important de rester vigilant lors des transactions en ligne et de ne pas divulguer de mots de passe, de numéros de carte de crédit ou d'autres informations personnelles en réponse à des e-mails suspects.

Sources

https://www.darkreading.com/cyberattacks-data-breaches/oil-gas-sector-falling-for-fake-vehicle-incident-email-lure

https://thehackernews.com/2024/04/new-phishing-campaign-targets-oil-gas.html