Anti-phishing/cybersécurité

Fournir une solution anti-phishing sur mesure

Le *phishing* dans le secteur des transports et de la livraison a augmenté de façon exponentielle pendant la pandémie de COVID-19, les entreprises et leurs consommateurs étant ciblés par une série d'escroqueries sophistiquées. Andreas Juchli explique comment l'approche sur mesure de Novagraaf en matière de protection des marques en ligne a pu aider une grande marque internationale de messagerie et de logistique à défendre son entreprise et ses clients contre la fraude en ligne et les atteintes par *phishing*.

Alors que les entreprises et les consommateurs ont été de plus en plus nombreux à se connecter en ligne pour commander des biens et faire appel à des services pendant la pandémie de COVID-19, le risque de *phishing*, fraude et autres formes d'atteinte à la marque en ligne a également augmenté. Des fausses alertes par courriel à la tromperie par le biais d'applications non autorisées, de nouvelles menaces numériques de plus en plus sophistiquées ont un impact sur chaque point de contact de la chaîne de valeur en ligne, y compris le secteur de la livraison.

Étude de cas : Les avantages en bref

Grâce à notre solution de cybersécurité sur mesure, Novagraaf a pu réduire de près de 70% l'efficacité des attaques de *phishing* pour une grande marque internationale de logistique.

Nos actions ont également eu pour avantages :

- une diminution des notifications frauduleuses par le biais de la création d'un support client dédié ;
- une authentification et, par conséquent, un paiement plus rapide des factures légitimes ;
- une mise en place d'un système de sécurisation accrue des actifs numériques ; et
- un détournement de l'attention de l'escroc vers des marques de tiers.

Notre solution sur mesure implique :

- la surveillance proactive des publicités payantes sur les réseaux sociaux ;
- la surveillance continue des enregistrements de noms de domaine et des *phishtanks* (répertoires d'escroqueries par *phishing*) ; et
- la création et la gestion d'une adresse mail de *phishing* à laquelle le public peut signaler directement les infractions.

L'entreprise : Un géant dans son secteur

L'entreprise en question est une marque de logistique mondialement connue, qui est malheureusement la cible de multiples escroqueries.

Chaque jour, des milliers de consommateurs sont visés par de faux courriels se présentant comme provenant de cette entreprise, leur demandant de cliquer sur des liens pour recevoir des informations sur un colis en attente ou de télécharger une fausse application pour mieux suivre leur parcours. La sophistication de l'atteinte a induit en erreur de nombreux destinataires d'e-mails les incitant à saisir leurs données personnelles et, dans de nombreux cas, à effectuer un paiement pour garantir la livraison d'un faux colis. Beaucoup d'autres consommateurs ont immédiatement transmis ces courriels à l'entreprise de livraison pour vérifier l'origine du courriel. Cette dernière a alors pu vérifier l'authenticité avant d'agir à l'encontre de la centaine d'e-mails reçus par le service clients.

Un tel volume d'e-mails peut poser des problèmes à toute entreprise, car elle oblige les destinataires à vérifier chaque alerte pour reconnaître sa légitimité ou non, ce qui demande beaucoup de temps et de ressources en interne. Les consommateurs anxieux exigent une réponse rapide, auquel cas cela peut entraîner des réactions négatives de la part des clients. Plus généralement, une communication pourtant légitime est également susceptible d'être considérée avec scepticisme par les clients et leurs consommateurs, car la marque commence à être associée à un volume élevé de spams. Il était clair pour le titulaire de la marque que le problème devait être résolu.

Novagraaf
A NovumIP Company

Le défi : de nouvelles solutions numériques pour les nouvelles menaces numériques

Les services de protection des marques en ligne se sont traditionnellement concentrés sur l'identification et le retrait des produits ou contenus illicites en ligne, par exemple en se concentrant sur les enregistrements de noms de domaine non autorisés ou les sites similaires frauduleux. Bien que ces services aient toujours un rôle essentiel à jouer, Novagraaf a compris que dans ce cas, ces sociétés avaient également besoin d'une solution de protection des marques qui l'aiderait à gérer et traiter le volume élevé des alertes de consommateurs.

En outre, l'analyse des médias sociaux a permis d'identifier l'activité des escrocs sur Facebook, Instagram et les applications spécifiques à la Chine telles que WeChat, Weibo et RedBubble. Comme c'est toujours le cas avec les escroqueries en ligne, il faut une application multiple et persistante pour endiguer de telles activités. Au fil du temps, les cybercriminels peuvent abandonner leur stratégie consistant à créer des faux profils sur les réseaux sociaux ou des sites Web qui se font passer pour une entreprise, par exemple.

Mais plutôt que de cesser complètement, ils se tournent généralement vers des pages génériques qui mentionnent la marque dans un message ("*scamposts*") et nécessitent donc de la publicité pour attirer l'attention des consommateurs. En adaptant nos recherches, nous avons pu faire en sorte que nos services de surveillance numérique incluent également ces nouvelles escroqueries, même si leur créateur n'a pas utilisé le nom de la marque comme mot clé, mais a plutôt utilisé son logo dans un post, par exemple.

Nous avons également cherché des moyens de soulager la charge pour l'entreprise de la marque lorsqu'il s'agit d'informer les consommateurs. Les principaux facteurs stratégiques étaient :

- agir rapidement contre les escroqueries une fois signalées, réduisant ainsi leur efficacité, plutôt que d'attendre que le titulaire de la marque identifie les escroqueries potentielles et nous les transmettent ; et
- soumettre les courriels comme preuve aux fournisseurs d'accès à Internet (FAI) qui doit être informés de la fermeture des serveurs de messagerie utilisés pour envoyer les spams. Les FAI n'accepteront pas les e-mails transférés par un tiers comme preuve valable en raison du fait qu'ils soient modifiables. Les courriels doivent être soumis sous forme de fichiers numériques pour être analysés.

La solution : Un service sur mesure

À la suite de notre analyse, nous avons mis en place un service de surveillance spécifiquement axé sur l'usurpation d'identité de marque en ligne et une boîte mail *anti-phishing* que nous gérons pour le compte des clients.

La surveillance des noms de domaine a rapidement donné les premiers résultats. Des enregistrements de noms de domaine suspects ont été identifiés, ajoutés à notre système de gestion des atteintes à la marque et de réactions immédiates lorsque des signes de comportement malveillant sont détectés.

La surveillance des médias sociaux a facilité la détection des activités non autorisées, y compris les publicités payantes, grâce aux outils disponibles (comme l'outil Commerce & Ads IP de Facebook).

La création **d'une boîte mail *anti-phishing*** permet de garantir que nos équipes soient directement alertées des arnaques et menaces détectées. Des mécanismes de signalement automatisés ont été mis en place, y compris auprès des différents FAI.

En outre :

- Les arnaques sur les réseaux sociaux utilisant la marque ont disparu après plus d'un an de surveillance et de démantèlement incessants.
- En nous transmettant les attaques par *phishing* et autres problèmes de propriété intellectuelle via une boîte mail dédiée, le personnel et l'assistance clientèle peuvent alors se concentrer sur les besoins réels des clients.
- Le montant des factures impayées a également été réduit, puisque nous transmettons tout "contenu suspect" réellement légitime aux départements correspondants qui peuvent alors aborder directement le problème avec le client.
- La sécurisation des noms de domaine et sites web des entreprises a été améliorée, et les profils des médias sociaux sont soumis à des processus de vérification pour garantir la cohérence et la fiabilité de la marque.
- Dans l'ensemble, notre approche solide et concluante a également permis de réduire le nombre d'activités de *phishing* et de fraude, les escrocs se tournant vers des cibles plus "faciles" et moins réactives.

Lorsqu'il s'agit de protéger une marque en ligne, il n'existe pas de solution universelle, car chaque titulaire de marque ainsi que ses clients peuvent être approchés de différentes manières. C'est la raison pour laquelle il est important de travailler avec un prestataire spécialisé qui non seulement comprend les défis en ligne auxquels les entreprises sont confrontées, mais qui est aussi suffisamment souple pour adapter ses solutions à leurs besoins exacts. Pour savoir comment Novagraaf peut vous aider à protéger votre marque et vos clients en ligne, contactez-nous brandprotection@novagraaf.com.

Novagraaf
A NovumIP Company