



Sauver les partenaires des escroqueries par usurpation d'identité

PreCrime Brand

Situation

La compromission et l'usurpation d'identité des e-mails professionnels représentent les coûts les plus importants encourus par les organisations pour la cybercriminalité. Des pertes supérieures à 2 milliards de dollars par an sont encourues en raison de cette méthode d'attaque qui est beaucoup plus courante et coûteuse que les méthodes les plus fréquemment discutées telles que les ransomwares ou le vol d'informations d'identification.

Régulièrement, les clients et partenaires de Signify étaient la cible d'attaques d'usurpation d'identité et de compromission des e-mails professionnels, entraînant parfois des pertes de centaines de milliers de dollars. L'équipe de sécurité veut reprendre le contrôle, cesser d'être victime de cybercriminalité et commencer à protéger son public de manière proactive.

Impact

Signify est le leader mondial de l'éclairage. Ils fournissent aux clients professionnels et aux consommateurs des produits, systèmes et services de qualité. Leurs innovations contribuent à un monde plus sûr, plus intelligent et plus durable.

Signify a demandé à Bfore.Ai d'appliquer la technologie PreCrime pour la protection de sa marque. Visant à couvrir leurs 50 marques pour identifier les menaces émergentes et arrêter les criminels avant que quiconque ne devienne une victime.

Résumé

- Régulièrement, les clients et partenaires de Signify étaient la cible d'attaques d'usurpation d'identité et de compromission des e-mails professionnels
- Signify a demandé à Bfore.Ai d'appliquer la technologie PreCrime pour la protection de sa marque
- Bfore.Ai fournit un service de protection des actifs numériques de marque entièrement géré
- Au cours des 6 premiers mois, 41 vecteurs de menace ont été prédits et supprimés de manière proactive. Aucune victime signalée.
- Des économies de 12 millions de dollars ont été réalisées grâce à la détection précoce des menaces en évitant les gestes commerciaux coûteux et les procédures judiciaires.

A propos de Bfore.Ai

La première solution de sécurité réellement prédictive. Nous aidons les organisations à prévenir les intrusions et l'exfiltration de données en prédisant les vecteurs d'attaques futures, les informations sont utilisées dans #PreCrime for Network - intelligence prédictive des cybermenaces pour mettre à niveau les solutions de sécurité existantes (pare-feu, résolveurs DNS, filtres anti-hameçonnage, proxies, etc.)

Points clés à retenir

50 marques protégées à travers le monde

Notification jusqu'à 72 heures plus tôt par rapport aux solutions existantes

95 % des contre-mesures réalisées en moins de 24 heures

Aucune victime

12 millions de dollars en ROSI (retour sur investissement de sécurité) estimé

<0,05 % de faux positifs

Comment ça marche

Signify a implémenté PreCrime via une API certifiée sur sa Threat Intelligence Platform. Leur architecture de sécurité avancée permet aux analystes des menaces de pousser les indicateurs vers les terminaux (résolveurs DNS, pare-feu, pare-feu d'application Web, etc.) et de surveiller les hits qui indiqueraient une attaque émergente.

Bfore.Ai fournit un service de protection des actifs numériques de marque entièrement géré, en exécutant PreCrime Brand et en envoyant un nombre minimum d'alertes, avec près de zéro faux positifs, directement à l'équipe de renseignement sur les menaces. La perturbation du réseau des domaines malveillants et les suppressions ultérieures sont mises en œuvre pour arrêter l'attaque avant qu'elle ne commence.

Clients protégés et économies importantes réalisées

Au cours des 6 premiers mois, 41 vecteurs de menace ont été prédits et supprimés de manière proactive. Aucune victime signalée.

Des économies de 12 M\$ ont été économisées, en évitant les gestes commerciaux coûteux, les poursuites judiciaires, l'impact sur la réputation et en optimisant la gestion du temps de remédiation et post-mortem.

La technologie PreCrime aide désormais l'équipe Signify Threat Intelligence à assurer la sécurité de l'organisation et de ses parties prenantes en continuant à identifier les menaces émergentes et à appliquer des contre-mesures pour éviter les victimes.

Bfore.ai est l'outil parfait pour aider toute équipe de renseignement sur les cybermenaces à prédire le crime avant qu'il ne se produise. Superbe détection de l'infrastructure d'attaque de l'acteur de la menace. Mais en plus de la détection, bfore.ai fournit les outils pour lutter contre le crime avec atténuation et suppression des actifs de l'acteur de la menace.

Kobe S. Head of Cyber Threat Intelligence

Contact Us Now

FR +33 7823 62484

sales@bfore.ai

<https://bfore.ai>

Distribué en France par :

AMC SOFT

1, PI Paul Verlaine

92100 Boulogne - Billancourt FRANCE.

<https://amcsoft.fr>

contact@amcsoft.fr

Tel : +33680741316

"PreCrime, c'est comme les prévisions météo mais pour la cybersécurité"

Luigi Lenguito - BforeAi CEO