2020 Rapport sur les menaces ciblant le secteur des assurances et des services financiers

INTRODUCTION

La pandémie mondiale a contraint de nombreuses compagnies d'assurance et entreprises de services financiers à accélérer leur transformation numérique. Ces efforts ont porté leurs fruits : parcours client à distance plus rationalisé, infrastructure évolutive permettant de s'adapter au périmètre en pleine expansion et ajustements visant à répondre aux besoins de conformité et de communication en perpétuelle évolution. Si tous ces changements aident les banquiers, les conseillers en gestion du patrimoine, les traders et les agents à appréhender les marchés et à gérer les flux financiers, ils offrent également plus d'opportunités aux cybercriminels.

Les cybercriminels profitent de la moindre crise sociétale, et la pandémie de COVID-19 ne fait pas exception à la règle. À mesure que le secteur des assurances et des services financiers s'étend au-delà du périmètre réseau, les cybercriminels suivent le mouvement. De plus, les menaces ne se contentent pas de se déplacer : elles changent de forme et de cibles. Chacun de vos collaborateurs représente un niveau de sécurité ou un risque de conformité différent, en fonction des données auxquelles il a accès et de la façon dont il utilise les technologies pour exercer son métier.

Pour aider les responsables du secteur des assurances et des services financiers à mieux comprendre l'évolution du paysage des menaces, nous avons analysé une année de données, en nous concentrant sur le premier semestre 2020. L'équipe Proofpoint de recherche sur les cybermenaces a étudié des milliers de menaces parmi des millions de messages. Ce rapport présente nos conclusions, étayées par des données et des exemples concrets visant à mettre en lumière les menaces qui ciblent le secteur des assurances et des services financiers.

Public et objectif

Ce rapport est destiné aux dirigeants et aux responsables de la sécurité de compagnies d'assurance et d'entreprises de services financiers. Il a pour objectif de les aider à réduire les risques qui pèsent sur les données personnelles, les données financières, la propriété intellectuelle, les informations non publiques et les écosystèmes tiers du secteur des assurances et des services financiers, ainsi que les risques de fraude. Ce rapport vise également à sensibiliser les collaborateurs des compagnies d'assurance et des entreprises de services financiers afin de renforcer la sécurité et la protection des données.

Méthodologie de recherche

Dans le cadre de ces recherches, nous avons analysé une combinaison de données Proofpoint concernant divers cybercriminels, campagnes, attaques par piratage de la messagerie en entreprise (BEC, Business Email Compromise) et VAP (Very Attacked People™, ou personnes très attaquées) au cours du quatrième trimestre 2019 et du premier semestre 2020. Dans certains cas, nous avons utilisé des informations libres d'accès pour étudier les problématiques de sécurité qui nous intéressent, mais qui ne sont pas directement représentées dans les données recueillies par Proofpoint.

Sommaire

Résumé

Le secteur des assurances et des services financiers demeure une cible attrayante pour les cybercriminels, que leurs motivations soient fiduciaires, hacktivistes ou terroristes. Voici les principaux points à retenir de ce rapport :

Les personnes, et non les technologies, sont le principal vecteur d'attaque.

Selon les données de threat intelligence de Proofpoint, plus de 96 % des attaques débutent par le recours à l'ingénierie sociale, au pretexting, au phishing ou aux menaces internes, alors que de nombreuses entreprises dépensent la majeure partie de leur budget dans des solutions technologiques.

Grâce à une analyse des indicateurs de compromission et des tactiques, techniques et procédures réalisée par Proofpoint, il est possible de dresser une liste des VAP afin de personnaliser la fiabilité de la sécurité en fonction de ces menaces ciblées.

Les cybercriminels s'adaptent rapidement aux changements de circonstances.

Le rapport 2020 sur les compromissions de données de Verizon révèle que les attaques cloud ont doublé l'année dernière. Cette hausse s'inscrit dans la lignée de la généralisation du télétravail.

Les cybercriminels ciblant le secteur des services financiers adoptent des stratégies sophistiquées, se montrent méthodiques dans leur utilisation des tactiques et connaissent bien leurs victimes.

Au-delà du second niveau, les entreprises ont un contrôle limité sur les risques liés à la chaîne logistique.

La chaîne logistique des services financiers est plus volatile d'un point de vue économique que celle de n'importe quel autre secteur, car elle inclut des bourses, des banques de règlement, des chambres de compensation et des banques centrales d'envergure internationale.

Ayez conscience des nuances des exigences de sécurité relatives à la chaîne logistique. Abaisser les exigences internes de votre entreprise pour forcer la conformité aux mesures de sécurité spécifiques aux fournisseurs de premier et de second niveau peut créer des failles de sécurité pour le fournisseur concerné ou l'empêcher de remplir correctement sa mission auprès de votre entreprise.

Chaque segment du secteur présente des nuances propres à son paysage des menaces.

Les données de threat intelligence de Proofpoint et des rapports indépendants mettent en lumière les variations des indicateurs de compromission et des tactiques, techniques et procédures employées dans chaque segment du secteur, afin que les dispositifs de défense puissent être personnalisés en fonction du segment concerné.

Les cryptomonnaies sont en plein essor.

L'Office of the Comptroller of the Currency (OCC) a récemment publié un communiqué autorisant les établissements bancaires à conserver les clés numériques des portefeuilles de cryptomonnaie.

Si les banques sont autorisées à conserver légalement des ressources numériques pour leurs clients, les responsabilités légales et les risques de cybersécurité associés aux cryptomonnaies leur sont transférés.

Indicateurs de menace et de sécurité propres au secteur des assurances et des services financiers

Le secteur des services financiers possède plusieurs caractéristiques semi-uniques aussi attirantes pour les cybercriminels que le miel pour les abeilles :

ENJEUX IMPORTANTS

Le retour sur investissement en cas de compromission d'une entreprise de services financiers est plus élevé que dans les autres secteurs, car c'est là que se trouve l'argent.

FORT IMPACT

Toutes les compromissions, quelle que soit leur envergure, sont susceptibles de faire la une des médias et d'influer sur la réaction du marché. Par effet ricochet, elles peuvent en outre s'étendre des entreprises aux économies mondiales.

RÉGLEMENTATIONS SPÉCIFIQUES

Les entreprises du secteur devant respecter des procédures et processus réglementaires bien définis, les missions de reconnaissance menées par les cybercriminels auprès de leurs cibles s'en trouvent simplifiées.

TECHNOLOGIES D'ANCIENNE GÉNÉRATION

Étroitement liés à l'ancienneté des systèmes informatiques, les risques de sécurité sont créés par l'arrêt du support assuré par le fabricant, l'accumulation de systèmes propriétaires au fil des fusions et acquisitions, des systèmes jugés « trop critiques pour être mis à jour » ou la perte d'expertise dans les technologies d'ancienne génération.

INFRASTRUCTURE COMPLEXE

Le secteur fait l'objet de nombreuses fusions et acquisitions, ce qui accroît la complexité et l'opacité. Les intégrations fragiles entre des systèmes disparates créent une infrastructure fragmentée, ce qui multiplie les vulnérabilités et augmente la pression exercée sur les ressources de défense et de surveillance de la sécurité.

TECHNOLOGIES CLOUD / DE CONTENEURS

La migration des applications d'ancienne génération vers le cloud (ou des conteneurs) peut entraîner l'exposition de vulnérabilités inconnues auparavant ou l'introduction de nouvelles vulnérabilités dues au modèle de déploiement. Le recours à de nouveaux fournisseurs SaaS pour se décharger de systèmes non critiques peut créer une nouvelle surface d'attaque sur laquelle la gestion des incidents est fortement limitée.

AUTOMATISATION OMNIPRÉSENTE

Les compagnies d'assurance et les entreprises de services financiers se tournent vers l'automatisation pour réduire les coûts et moderniser les systèmes d'ancienne génération. Toutefois, la banalisation de l'automatisation les fragilise lorsqu'elles sont dépendantes de systèmes d'ancienne génération, qu'elles adoptent une nouvelle logique métier complexe ou qu'elles utilisent des méthodes non documentées.

Le secteur des assurances et des services financiers présente certaines statistiques qui lui sont propres en ce qui concerne la prévention, les menaces émergentes et les attaques persistantes :

Formations de sensibilisation à la sécurité

Les collaborateurs des compagnies d'assurance et des entreprises de services financiers sont légèrement plus conscients des menaces internes et des risques liés à l'authentification des comptes que ceux des autres secteurs.

- Les services financiers ont enregistré un taux d'échec de 20 %, légèrement inférieur à la moyenne globale de 22 %.
- Ils ont obtenu de meilleurs résultats dans les catégories « Identification et prévention des menaces internes » et « Authentification des comptes ».
- Ils ont enregistré de moins bons résultats uniquemetn dans les catégories « Protection contre les risques physiques » et « Prévention des attaques de ransomwares ».

Menaces véhiculées par email

Les entreprises ont reçu davantage d'URL dangereuses que de pièces jointes malveillantes.

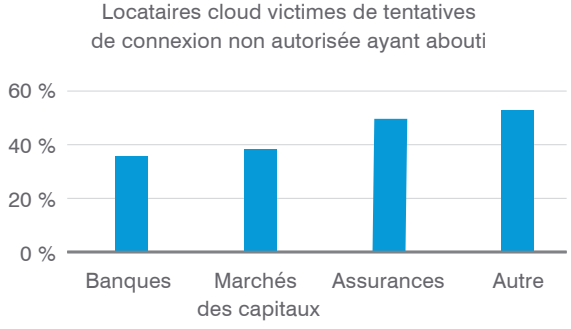
- 82 % des messages malveillants envoyés à des entreprises de services financiers contenaient des URL.
- 72 % des attaques reposaient sur des malwares.

Accès au cloud

Les tactiques d'ingénierie sociale visant à obtenir l'accès au cloud ont enregistré un *taux de succès spectaculaire de 75 %*, tandis que les attaques par force brute ne sont parvenues à leurs fins que dans environ 9,7 % des cas. Les attaques centrées sur les personnes présentent clairement le retour sur investissement le plus prometteur pour les cybercriminels.

Les compagnies d'assurance ont subi davantage de tentatives de connexion non autorisée ayant abouti que les banques et les marchés des capitaux.

- 72 % d'entre elles ont été la cible d'attaques par force brute, mais seulement 7 % ont été compromises à l'aide d'une telle méthode.
- 28 % ont été ciblées par des techniques d'ingénierie sociale. 21 % ont été compromises à l'aide d'une méthode de phishing.



Prévention des fuites de données et menaces internes

Chaque segment du secteur des assurances et des services financiers présente son propre risque de menaces internes. Selon une étude sur les incidents internes menée entre 1996 et 2018, les banques étaient de loin le secteur le plus vulnérable[1].

Segment	Groupe(s)	Risque(s) de menaces internes	Nombre d'incidents internes[2]
Banques	Épargne, crédit, finances	Données personnelles, prise de contrôle de comptes	190
Marchés des capitaux	Banques d'investissement, gestion des actifs	Propriété intellectuelle, fusions et acquisitions, délit d'initié	aucune donnée disponible
Assurances	Courtage, biens immobiliers et sinistres	Données personnelles, fraude aux assurances	14
Écosystème	Bourses, banques de règlement, données des marchés, cloud/SaaS, chaîne logistique	Lutte contre le blanchiment, contreparties, SWIFT, chambres de compensation automatisée (CCA), manipulation des marchés	33

Tactiques, techniques et procédures employées dans les attaques d'origine interne ciblant le secteur des services financiers

Entre 2005 et 2012, le CERT, en collaboration avec le ministère américain de la Sécurité intérieure et l'United States Secret Service (USSS), a mené des recherches sur les incidents d'origine interne afin de répondre à la question suivante : « Quels précurseurs techniques et comportementaux de fraude interne peut-on observer dans le secteur financier, et quelles stratégies de prévention doivent être envisagées pour y remédier ? »[3].
Voici les principales conclusions de ces recherches :

Les attaques discrètes et lentes ont fait plus de dégâts et ont échappé plus longtemps à la détection.

Les solutions technologiques basées sur la détection des anomalies se sont non seulement avérées inefficaces, mais aussi contreproductives, car ces activités malveillantes à long terme sont devenues partie intégrante du quotidien des utilisateurs.

Les moyens déployés par les cybercriminels n'étaient pas sophistiqués sur le plan technique.

Ce manque de sophistication signifie que les données des sondes existantes peuvent alimenter un programme de gestion des menaces internes. Bien entendu, le secret réside dans l'analyse comportementale.

En termes de dégâts et de durée, les fraudes commises par les cadres se distinguent nettement de celles commises par les collaborateurs aux échelons inférieurs.

Les cadres ont la possibilité de modifier les processus métier, parfois en manipulant des collaborateurs subordonnés, à des fins lucratives. Parmi les collaborateurs aux échelons inférieurs, ce sont généralement des représentants du service client qui modifient des comptes ou détournent des données personnelles à leur avantage.

La plupart des incidents ont été détectés à la suite d'un audit, d'une plainte d'un client ou d'un signalement par un collègue.

Il s'agit là d'un constat important : si les compromissions externes sèment des anomalies sur leur passage, les menaces internes se nourrissent quant à elles du ressenti, des motivations et de l'état d'esprit des utilisateurs, ce qui complique leur détection par des technologies.

Le loup dans la bergerie

Il arrive que ce soit l'entreprise chargée de détecter et d'analyser les menaces internes qui en soit justement victime. En 2019, un ancien examinateur de la conformité des valeurs mobilières de la SEC a été accusé d'avoir accédé à des informations concernant une enquête en cours dans une société de capitaux privés et de s'en être servi pour être nommé au poste de directeur de la conformité dans cette même société[4]. Le fait que l'individu occupait – et ait décroché – un poste de conformité n'est pas seulement ironique : il montre également que les menaces internes ne connaissent aucune limite en termes de moralité.

[1] Miller et Trotman (2018), « *Insider Threats in Finance and Insurance (Part 4 of 9: Insider Threats Across Industry Sectors)* » (Les menaces internes dans le secteur de la finance et des assurances – Partie 4 sur 9 de l'analyse des menaces internes par secteur d'activité), SEI de l'université Carnegie Mellon

[2] Ibid

[3] Cummings, Lewellen, McIntire, Moore et Trzeciak (2012), « *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector* » (Étude sur les menaces internes : cyberactivité illicite impliquant une fraude dans le secteur des services financiers aux États-Unis), SEI de l'université Carnegie Mellon, Direction des sciences et technologies du ministère américain de la Sécurité intérieure, USSS et Insider Threat Center du CERT

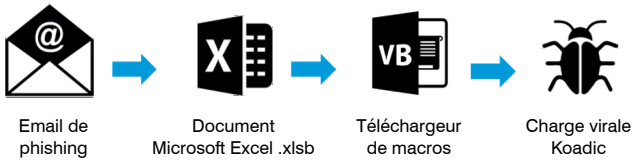
[4] Godoy et Lorenzo (2019), « *Ex-SEC Compliance Expert Denies Pilfering Info For PE Firm* » (Un ancien expert en conformité de la SEC nie le vol d'informations pour un fonds de placement privé), Law360

Tactiques prédominantes dans les attaques ciblant le secteur des assurances et des services financiers

Les données de threat intelligence de Proofpoint montrent la progression de plusieurs tactiques spécifiques utilisées par les cybercriminels :

Manipulation du code VBA (VBA stomping)

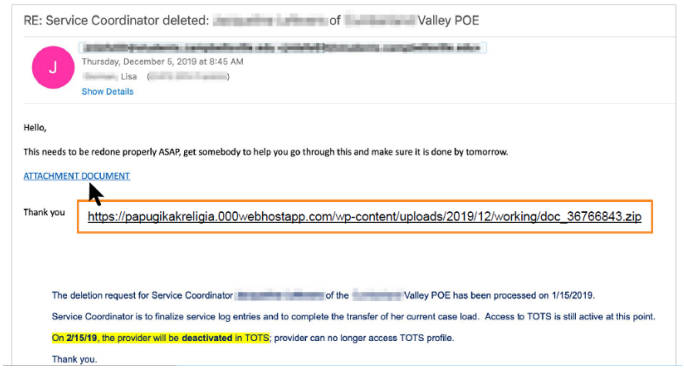
Cette technique basée sur des pièces jointes malveillantes présente aux moteurs d'analyse de sécurité un code VBA (exécutable) différent de celui qui est réellement exécuté, ce qui permet de contourner de nombreux outils de détection basés sur les signatures et les analyses heuristiques.



Piratage de fils de discussion

Ce type d'attaque BEC fait de nombreuses victimes en injectant le contenu de faux emails (p. ex. des URL malveillantes) dans un fil de discussion existant. Les utilisateurs font généralement confiance aux fils de discussion existants, ce qui les rend plus enclins à les ouvrir et à cliquer sur des liens.

Une autre tactique consiste à incorporer des URL malveillantes dans la section reprenant l'email d'origine, généralement exclue de l'analyse de la plupart des outils de protection de la messagerie, ce qui permet à nouveau de contourner de nombreux outils de détection basés sur les analyses heuristiques.


RE: Service Coordinator deleted: [redacted] of [redacted] Valley POE

J

Thursday, December 5, 2019 at 8:45 AM

[redacted], Lisa ([redacted])

Show Details

Hello,

This needs to be redone properly ASAP, get somebody to help you go through this and make sure it is done by tomorrow.

ATTACHMENT DOCUMENT

Thank you https://papugikakreligia.000webhostapp.com/wp-content/uploads/2019/12/working/doc_36766843.zip

The deletion request for Service Coordinator [redacted] of the [redacted] Valley POE has been processed on 1/15/2019.

Service Coordinator is to finalize service log entries and to complete the transfer of her current case load. Access to TOTS is still active at this point.

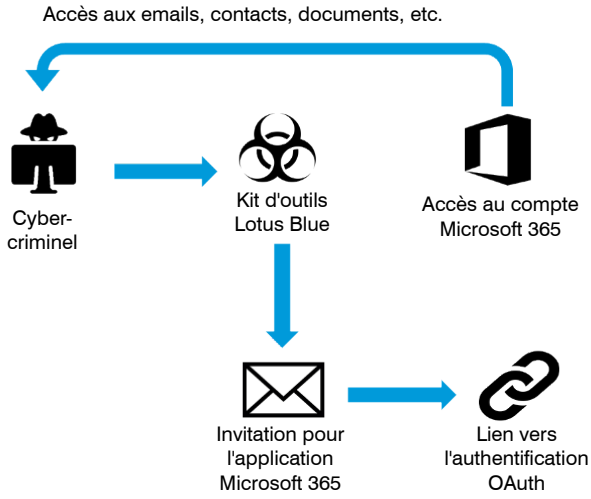
On 2/15/19, the provider will be deactivated in TOTS; provider can no longer access TOTS profile.

Thank you.

Dans le cas d'Emotet, le malware le plus prolifique de ces deux dernières années, les cybercriminels ont automatisé le processus de création de modèles afin d'appliquer cette technique à très grande échelle, ce qui, en temps normal, nécessiterait une analyse et une personnalisation directes par les cyberpirates eux-mêmes.

Authentification tierce piégée

Cette technique de prise de contrôle de comptes procède à une altération DNS classique pour inciter les utilisateurs à accorder des autorisations de jeton basées sur SAML aux applications cloud d'un collaborateur (p. ex. Microsoft 365 ou Google Workspace). Elle débute généralement par une attaque BEC, pour se transformer rapidement en compromission de comptes de messagerie (EAC, Email Account Compromise). Grâce à l'accès au compte de messagerie d'un utilisateur, la réinitialisation des mots de passe d'autres applications devient possible, ce qui permet de prendre le contrôle de ces comptes.



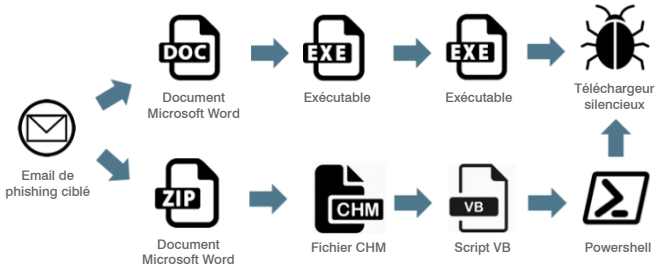
Si ce type de prise de contrôle de comptes est plus dangereux que les autres, c'est parce qu'une fois que des autorisations ont été accordées à un compte, modifier votre mot de passe ou appliquer une authentification à plusieurs facteurs ne sert plus à rien. Le seul moyen de révoquer l'accès d'un cybercriminel est de supprimer explicitement les autorisations de jeton, un processus dont la plupart des utilisateurs ignorent tout.

Attaque multicouche par partage de fichiers

Cette technique utilise un document hébergé contenant plusieurs couches d'URL pointant vers d'autres documents hébergés sur de nombreux sites de partage de fichiers différents, qui finissent par mener à une charge virale truffée de malwares.

La prévalence croissante des partages de fichiers dans le cloud (et de l'authentification tierce) dans le secteur des services financiers a renforcé l'utilisation de cette technique.

Par exemple, une charge virale (un script VB qui charge Ursnif, un cheval de Troie bancaire incorporé) est protégée par un mot de passe (chiffrée) qui figure dans le corps du message.



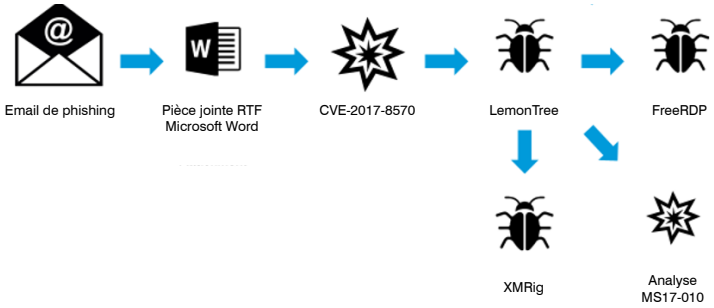
D'un côté, l'ajout d'étapes, consistant par exemple à contraindre la cible à saisir un mot de passe, semble contre-intuitif, car plus il y a d'étapes à suivre, plus il y a de chances que le collaborateur visé passe à côté de quelque chose ou abandonne avant la fin.

D'un autre côté, cette méthode empêche l'analyse de la pièce jointe. Les solutions ont donc dû mettre en œuvre des techniques reposant soit sur un dictionnaire régulièrement mis à jour de mots de passe courants (les cybercriminels font en sorte d'utiliser des mots de passe simples pour les raisons susmentionnées et n'en changent pas à chaque campagne), soit sur l'analyse du corps des messages (ce qui s'avère complexe à grande échelle).

Il arrive que le mot de passe se présente sous forme d'image plutôt que de texte. Dans ce cas, la technique d'analyse des mots de passe texte mentionnée ci-dessus s'avère inefficace.

Attaque exploitant les ressources locales (sans fichier/serveur)

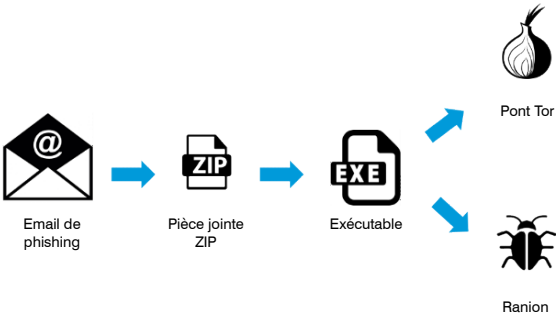
Cette technique d'attaque tire parti des fonctionnalités existantes du système d'exploitation de la cible (par exemple, PowerShell) pour exécuter sa charge virale. La charge virale en elle-même n'est pas binaire. Elle peut donc échapper aux méthodes de détection basées sur les signatures et les analyses heuristiques.



Ransomware-as-a-Service (RaaS)

Les plates-formes RaaS se sont généralisées, comme de nombreuses autres plates-formes d'attaque.

Les fournisseurs de plates-formes RaaS, qui prenaient auparavant une commission sur la rançon perçue, sont passés à un service d'abonnement. Non seulement cela confère au RaaS plus d'attrait que les autres plates-formes d'attaque, mais les fournisseurs se dégagent également de toute culpabilité directe dans les actes criminels. (Imaginez les poursuites qui seraient engagées à l'encontre des fabricants d'armes s'ils prenaient une commission sur chaque balle tirée.)



Les itérations récentes de ce service incluent l'installation automatique de clients Tor sur les ordinateurs des victimes, ce qui facilite le paiement de la rançon.

État des lieux du secteur des services financiers

Banques

C'est dans le secteur bancaire que l'on observe le plus d'innovation et de progrès ces dernières années, de l'essor des transactions mobiles aux services pilotés par des interfaces de programmation d'applications (API), en passant par l'utilisation du traitement basé sur l'intelligence artificielle. Toute nouvelle technologie s'accompagne de méthodes d'attaque inédites. En revanche, les motivations et les cibles des cybercriminels visant le secteur bancaire restent les mêmes. Accenture estime le risque de perte à 347 milliards de dollars dans le secteur bancaire[5].

FOCUS SUR LE SECTEUR BANCAIRE	
VAP :	**Phishing de grande ampleur** : • Équipes technologiques • Dirigeants **Attaques BEC :** • Responsables des relations • Relations avec les investisseurs / Conseillers financiers • Développement des activités
Cibles :	• Clients (direct) • Collaborateurs (direct) • Clients (indirect) : effectifs ayant accès aux données/systèmes des clients • Collaborateurs (indirect) : effectifs ayant accès aux données/systèmes des ressources humaines (RH)
Objectifs :	• Pertes financières pour les clients

Banques : attaques ciblées

Les données de threat intelligence de Proofpoint ont permis d'identifier des attaques ciblant une fonction ou une entreprise particulière du secteur bancaire. Les cybercriminels à l'origine de ces attaques ont donc un objectif précis, qui passe par une mission de reconnaissance auprès de l'entreprise visée.

Grand établissement bancaire

Commentaires des analystes : Un établissement bancaire du classement Fortune 100 a reçu 12 messages (100 %) utilisant une nouvelle technique WhiteShadow[6] pour déployer un ensemble de malwares inconnus. Cette observation est intéressante pour plusieurs raisons.

Le fait que les malwares ne soient pas identifiés pourrait indiquer que l'établissement fait office de cobaye avant le déploiement d'une attaque systémique de plus grande ampleur.

WhiteShadow sert souvent à déployer Crimson, un cheval de Troie d'accès à distance (RAT) identifié pour la première fois en 2016 comme charge virale employée par un groupe de cyberpirates parrainé par le Pakistan et baptisé « Transparent Tribe »[7]. Depuis lors, le RAT Crimson a été utilisé par un grand nombre de cybercriminels, mais l'équipe de threat intelligence de Proofpoint a reçu plusieurs demandes de la part d'établissements bancaires souhaitant savoir s'il pouvait toujours s'agir d'une activité commanditée par un État.

Le fait que la technique WhiteShadow ait injecté d'autres malwares en plus de Crimson à partir d'une infrastructure qui n'était pas explicitement liée au réseau pakistanais tend à corroborer l'idée d'une adoption généralisée de cette technique et des charges virales associées.

Coopérative de crédit : attaque contre la chaîne logistique

Commentaires des analystes : Une coopérative de crédit a reçu 67 messages (87 %), également envoyés à plusieurs cabinets comptables de la région. Toute relation entre la coopération de crédit et ces cabinets peut être le signe d'une attaque par canal auxiliaire ou contre la chaîne logistique.

La charge virale prévue de GuLoader QuasarRAT est plutôt quelconque, mais elle est représentative de l'évolution considérable des tactiques, techniques et procédures observée dans le paysage des menaces ces deux dernières années, qui a simplement pour but d'aider les cybercriminels à mettre le pied dans une entreprise afin d'y déployer d'autres charges virales. Qui plus est, QuasarRAT, en tant que malware open source, permet aux cyberpirates sophistiqués de brouiller les pistes. Par exemple, si un cybercriminel parvient à s'implanter sur un système au moyen d'un logiciel générique/courant, il sera bien plus difficile de déterminer qui a lancé l'attaque. En cas de compromission réussie, cette technique permet au cybercriminel de déployer une charge virale supplémentaire après avoir mené une mission de reconnaissance.

[5] Accenture (2020), « *The State of Cybercrime in Banking and Capital Markets* » (L'état de la cybercriminalité dans le secteur bancaire et des marchés des capitaux)

[6] https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

[7] https://www.proofpoint.com/us/threat-insight/post/Operation-Transparent-Tribe

Banques : tendances et analyse des menaces

Sur une période de six mois, du quatrième trimestre 2019 au deuxième trimestre 2020, l'équipe de threat intelligence de Proofpoint a effectué le suivi des menaces représentées sur la figure 1, qui ne cessent de cibler le secteur bancaire.

Virement bancaire

Commentaires des analystes : Les banques commerciales reçoivent quasiment deux fois plus de messages que le deuxième secteur le plus touché, même si les sociétés d'investissements financiers, les entreprises de services de transactions financières et les acteurs de l'écosystème financier en reçoivent tous. Le volume de messages est réparti de façon assez uniforme entre un grand nombre d'établissements et de régions, plutôt que d'être largement concentré sur un établissement et une poignée d'entreprises similaires. Le leurre simule un transfert d'argent via Western Union dans le but d'injecter un RAT. Pour ce faire, il recourt à un message dont l'objet a trait à la conformité.

Autres campagnes notables

Bot TeamViewer (MINEBRIDGE) | Documents Word | « Candidature Indeed : Guichetier à temps plein »
Cette campagne cible essentiellement le secteur des services financiers avec un leurre imitant la réponse d'une fausse entreprise de recrutement à une candidature pour un poste de guichetier à temps plein.

GuLoader / Parallax « warii » | Pièces jointes | « MAJ Code Banques »
Ces messages présentent des pièces jointes Microsoft Office contenant des macros qui, dès lors qu'elles sont activées, téléchargent et exécutent GuLoader qui, à son tour, télécharge et installe Parallax. Les cibles principales étaient des établissements bancaires et des entreprises de services.

jSocket « 88.150.189[.]98 » | URL | « Déclaration d'impôt »
Ces messages contiennent des URL pointant vers un fichier Java compressé. Ils ont presque tous été envoyés à un établissement bancaire.

Get2 / SDBbot | Documents Excel
Ces emails contiennent des pièces jointes Microsoft Excel incluant des macros qui, si elles sont activées, exécutent une DLL incorporée (malware chargeur « Get2 »). Get2 télécharge SDBbot et un malware inconnu. Les cibles principales étaient des établissements bancaires. 76 % des messages de cette campagne ont été envoyés à des entreprises de services financiers. Cette campagne a ciblé des établissements bancaires en décembre 2018 et en janvier 2019. Les établissements bancaires ont continué à être fréquemment visés.

URL | Documents Word | PDF
Les États-Unis sont ciblés par des emails contenant des URL, des documents Word ou des PDF. Les PDF usurpent l'identité de nombreuses banques du classement Fortune 100. Cette campagne passe par l'envoi à des entreprises de services financiers d'un faux avis de paiement prétendant provenir d'une société de vente au détail.

CobInt | Groupe Cobalt | URL
Les messages contiennent des liens vers un fichier PDF hébergé sur Microsoft OneDrive. Le PDF inclut des liens de téléchargement du fichier « Documents.rtf ». Ce document contient des exploits qui, s'ils parviennent à leurs fins, téléchargent CobInt. Aux États-Unis, plusieurs collaborateurs ont été victimes du malware CobInt, qui fait partie des familles des portes dérobées (backdoors) et des téléchargeurs. Cette attaque a été lancée par un groupe cybercriminel sous surveillance, qui cible principalement les banques et les établissements de crédit, ainsi que le secteur des médias et du divertissement. Dans ce cas, plus de 50 % des emails ont été envoyés à des collaborateurs d'entreprises de services financiers, ce qui en fait le secteur le plus exposé.

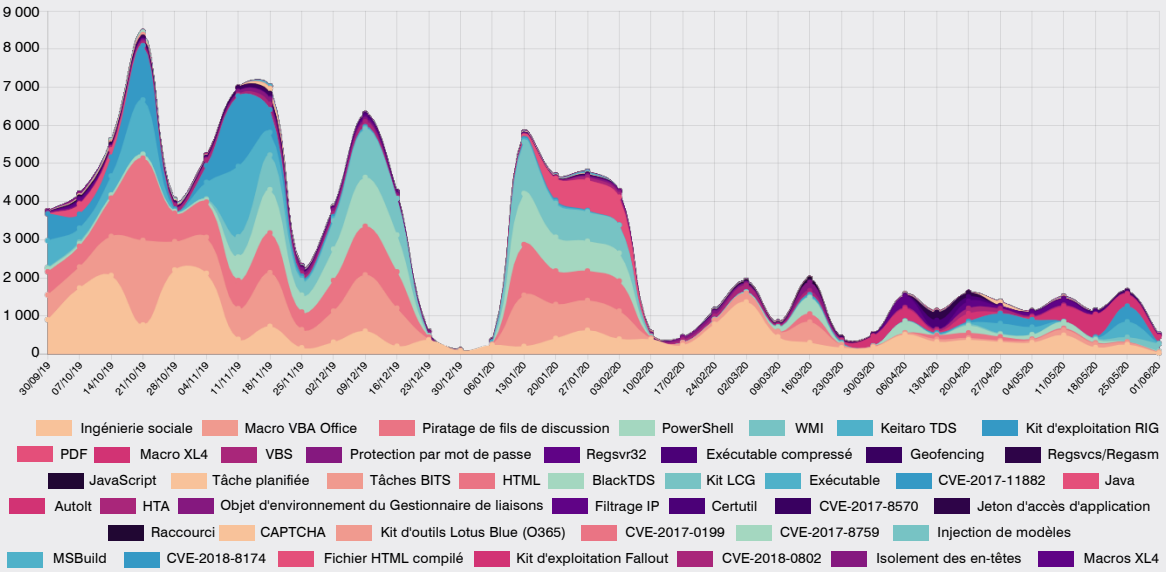


Figure 1. Caisses d'épargne – Exploits ciblés (source : Proofpoint)

Marchés des capitaux

Accenture estime le risque de pertes dues aux cyberattaques à 47 milliards de dollars dans le secteur des marchés des capitaux[8].

FOCUS SUR LE SECTEUR DES MARCHÉS DES CAPITAUX	
VAP :	**Phishing de grande ampleur** : • Équipes technologiques • Dirigeants/associés directeurs **Attaques BEC ciblées :** • Conseillers et analystes financiers • Gestionnaires de fonds/de portefeuille • Directeurs de la recherche
Cibles :	• Argent / Ressources (direct) : effectifs ayant accès aux ressources • Clients (indirect) : effectifs ayant accès aux données/systèmes des clients
Objectifs :	• Perturbation du secteur • Perturbation des marchés/activités économiques

Marchés des capitaux : attaques ciblées

Les données de threat intelligence de Proofpoint ont permis d'identifier des attaques ciblant une fonction ou une entreprise particulière du secteur des marchés des capitaux. Les cybercriminels à l'origine de ces attaques ont donc un objectif précis, qui passe par une mission de reconnaissance auprès de l'entreprise visée.

Les charges virales dissimulées pourraient avoir une longueur d'avance

Bien que ces attaques utilisent des leurres sans prétention, tels que des factures d'expédition, des liens de suivi de colis et des messages des impôts, la charge virale repose sur l'exécution de Node.js. Node.js est une plate-forme d'exécution populaire sur les serveurs et les hôtes web. En toute logique, la charge virale ne devrait donc pas s'exécuter lorsqu'elle est téléchargée sur un endpoint local.

Il est intéressant de constater que plusieurs cadres de développement d'applications déploient Node.js en local[9]. Bien que la majorité des applications financières conçues sur ces plates-formes soient axées sur la cryptomonnaie, il existe plusieurs applications libres et open source pour le suivi des marchés boursiers, l'analyse des données financières et le libre-échange (probablement utilisées par les entreprises de courtage ciblées)[10].

Marchés des capitaux : tendances et analyse des menaces

Les investissements financiers sont le secteur le plus ciblé. Ils reçoivent 31 % des messages et comptent pour 23 % des victimes. Notez qu'il existe un chevauchement avec les banques commerciales.

Sur une période de six mois, du quatrième trimestre 2019 au deuxième trimestre 2020, l'équipe de threat intelligence de Proofpoint a effectué un suivi des menaces représentées sur la figure 2, qui ne cessent de cibler le secteur des marchés des capitaux.

[8] Accenture (2020), « *The State of Cybercrime in Banking and Capital Markets* » (L'état de la cybercriminalité dans le secteur bancaire et des marchés des capitaux)

[9] https://brainhub.eu/blog/javascript-frameworks-for-desktop-apps/

[10] https://www.electronjs.org/apps?category=finance

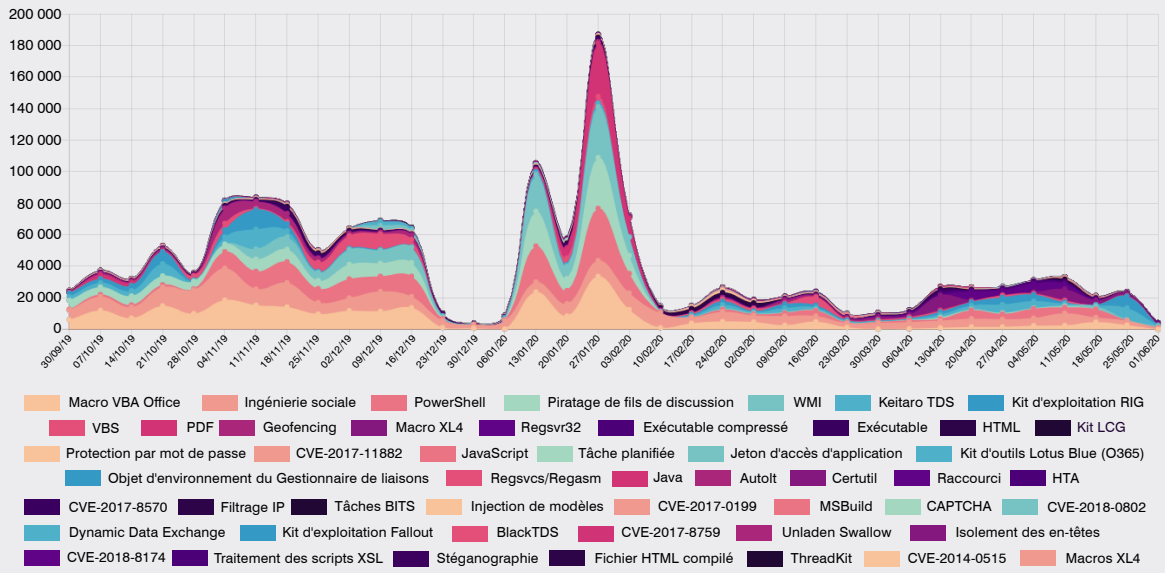


Figure 2. Courtage de valeurs mobilières – Exploits ciblés (source : Proofpoint)

Tendance d'attaque propre à la région

Commentaires des analystes : Si l'on s'intéresse aux 20 premières banques d'investissement mondiales, bien qu'elles aient leur siège aux États-Unis et qu'il serait logique qu'une majorité de collaborateurs soient basés à Londres ou à New York, la quasi-totalité de leurs 50 principaux VAP sont situés à Singapour, en Chine ou au Japon.

Cela peut s'expliquer par l'augmentation du nombre de nouvelles recrues basées en Asie-Pacifique afin de répondre au regain d'intérêt pour les investissements observé dans cette région. « Les banques constatent que des entreprises détenues par l'État chinois ont joué un rôle majeur dans les négociations en 2020 et recrutent massivement afin de maintenir à flot les activités des marchés des capitaux[11]. »

Autres campagnes notables

QuasarRAT | HTML | « Avis de correspondance avec les impôts »

Les emails ayant pour ligne d'objet « Avis de correspondance avec les impôts » contiennent une pièce jointe HTML compressée. Cette pièce jointe, si elle est ouverte, injecte un document Word incorporé, qui utilise des macros pour télécharger un script VB, lequel télécharge à son tour QuasarRAT. Cette campagne ciblait uniquement les marchés des capitaux (investissements et valeurs mobilières).

Assurances

Les assurances sont considérées comme un segment du secteur des services financiers, car elles reposent sur une gestion fiduciaire de fonds qui doivent être mis à disposition en cas de sinistre. Ce segment est toutefois très différent des autres, car les principaux risques auxquels il est exposé découlent d'événement externes.

Compte tenu de la profusion d'objectifs malveillants potentiels, il est important d'accorder autant d'attention à l'identité des collaborateurs ciblés au sein de votre entreprise qu'aux raisons pour lesquelles ils sont visés.

FOCUS SUR LE SECTEUR DES ASSURANCES

VAP :	**Phishing de grande ampleur** : • Équipes technologiques • Dirigeants • RH / Recruteurs **Attaques BEC ciblées :** • Agents d'assurance / Responsables de compte • Responsables de programmes/plans (plans de retraite, avantages sociaux, etc.)

En outre, les données de threat intelligence de Proofpoint montrent que le segment des assurances a enregistré plus de tentatives de connexion non autorisée aux locataires cloud ayant abouti que les établissements bancaires et les marchés des capitaux.

Cela peut s'expliquer par le fait que les compagnies d'assurance utilisent davantage de technologies de Big Data et d'intelligence artificielle[12], qui ne sont économiques que si elles sont déployées dans le cloud[13]. Cela pourrait aussi être dû à l'optimisation continue des coûts des opérations grâce à l'automatisation des processus robotiques, à l'externalisation des opérations de routine ou à la migration des données et opérations vers le cloud[14].

[11] Chatterjee et Murdoch (2020), « *Exclusive: Bank of America to hire 50 bankers for Asia dealmaking team in 2020—sources* » (Exclusif : Bank of America va recruter 50 banquiers pour son équipe de négociation en Asie en 2020 – Sources), Reuters

[12] Oliver (2019), « *Insurance sector prepares for disruption* » (Le secteur des assurances se prépare à des perturbations), Financial Times

[13] Thomson (2020), « *Are Insurers' Confidence in their Cyber Defense Exposing Them to Revenue Losses?* » (La confiance des assureurs en leur cyberdéfense les expose-t-elle à des pertes de revenus ?), Accenture

[14] Deloitte (2020), « *Deloitte Insights—2020 Insurance Outlook* » (Deloitte Insights – États des lieux des assurances en 2020)

Assurances : attaques ciblées

Les données de threat intelligence de Proofpoint ont permis d'identifier des attaques ciblant une fonction ou une entreprise particulière du secteur des assurances. Les cybercriminels à l'origine de ces attaques ont donc un objectif précis, qui passe par une mission de reconnaissance auprès de l'entreprise visée.

La franchise TrickBot

Commentaires des analystes : En règle générale, plus l'ampleur d'une campagne est importante en termes de volume global de messages et de nombre de destinataires, moins cette campagne est susceptible d'être ciblée. Dans le secteur des assurances, nous observons des concentrations très élevées de catégories de victimes au sein d'une seule campagne.

Dans ce cas, 21 entreprises destinataires sur 26 (81 %) sont affiliées à une assurance, tandis que 96 % des messages ont été envoyés à une compagnie d'assurance. La majorité des messages sont envoyés à une compagnie d'assurance spécifique. Mais ce n'est pas un hasard si 25 autres entreprises ayant reçu moins de messages appartiennent toutes au même secteur. En général, la répartition des secteurs destinataires est plus diversifiée, mais les assurances représentent habituellement environ 10 à 13 % des cas, là où les secteurs les plus ciblés ne reçoivent que 16 à 18 % des messages.

La charge virale du malware est l'un des chevaux de Troie bancaires les plus médiatisés. Les opérateurs exécutent leur botnet sur la base d'un modèle d'affiliation. Pour comprendre comment ces tactiques, techniques et procédures se sont banalisées, observons le fonctionnement de cette menace. Un cybercriminel devient un client des opérateurs de TrickBot. On lui attribue alors un paramètre « group tag », ici « yas24 », où le code à trois lettres désigne la campagne/le sous-groupe/l'affilié à l'origine de l'infection. Le nombre a tendance à être itératif, étant donné que le groupe continue à distribuer le malware.

Assurances : tendances et analyse des menaces

Sur une période de six mois, du quatrième trimestre 2019 au deuxième trimestre 2020, l'équipe de threat intelligence de Proofpoint a effectué un suivi des menaces représentées sur la figure 3, qui ne cessent de cibler le secteur des assurances.

AZORult | « daffy »

Les emails ayant pour ligne d'objet « Rapport de courrier de support@WellsFargo.com » contiennent une pièce jointe Microsoft Word intitulée « bon de commande nl5753637.doc » et exploitant la vulnérabilité CVE-2017-8570. Si elle est ouverte, la pièce jointe télécharge et exécute AZORult (« daffy.exe »). Le secteur des assurances reçoit 85 % des messages, alors qu'il ne représente que 18 % des clients suivis par notre équipe dans le cadre de cette campagne.

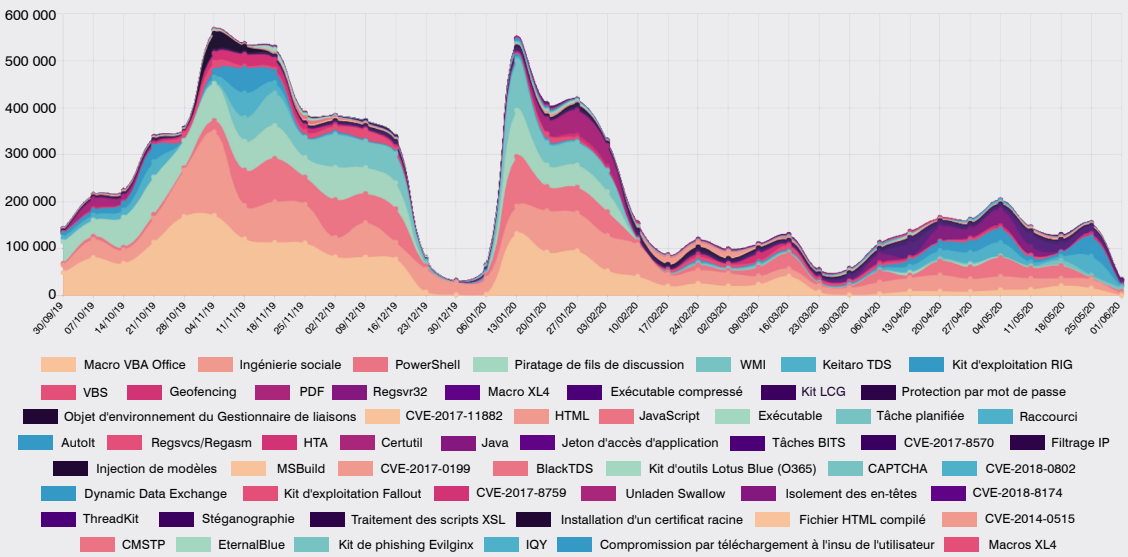


Figure 3. Assurances – Exploits ciblés (source : Proofpoint)

Conclusions et recommandations

Dans le secteur des assurances et des services financiers, la cybersécurité doit prendre en compte non seulement les surfaces d'attaque externes, mais aussi les failles de sécurité créées par les efforts internes d'optimisation des processus et technologies. Les attaques d'aujourd'hui ciblent les personnes, pas seulement les technologies. Elles exploitent le « facteur humain » du secteur des assurances et des services financiers tel qu'on le connaît actuellement : le désir d'aider les clients à atteindre leurs objectifs et de devenir un moteur d'opportunité. La pandémie mondiale a contraint de nombreuses compagnies d'assurance et entreprises de services financiers à accélérer leur transformation numérique pour améliorer leur gestion de la relation client sur l'ensemble des canaux, ainsi que faciliter la vente et la mise à disposition de solutions. Il n'a jamais été aussi difficile ni aussi important pour les entreprises de préserver la sécurité et la conformité des informations, tout en essayant de protéger et d'accroître la productivité des collaborateurs en télétravail. Les menaces et les risques de conformité qui pèsent aujourd'hui sur les compagnies d'assurance et les entreprises de services financiers nécessitent l'adoption d'une nouvelle approche centrée sur les personnes.

Voici nos recommandations pour les compagnies d'assurance et les entreprises de services financiers :

- **Adoptez une approche de la sécurité centrée sur les personnes.** Les cybercriminels ne voient pas le monde en termes de topologie réseau. Ils ciblent les personnes. Déployez une solution qui vous permettra d'identifier les personnes de votre entreprise qui sont ciblées et les méthodes utilisées à cette fin, ainsi que de déterminer si elles ont cliqué sur un lien malveillant. Tenez compte du risque individuel que chaque utilisateur représente. Une solution centrée sur les personnes vous indiquera comment vos utilisateurs sont ciblés, à quelles données ils ont accès et s'ils sont susceptibles de tomber dans les pièges tendus par les cybercriminels.
- **Utilisez les données de votre programme centré sur les personnes pour planifier et financer vos programmes de sécurité.** Ces données vous aideront à expliquer vos priorités à la direction et au conseil d'administration et à leur présenter des programmes permettant de réduire les risques auxquels est confrontée l'entreprise. Elles vous permettront également d'expliquer aux collaborateurs les raisons de la mise en place de votre programme et leur donneront les moyens de se protéger, eux et l'entreprise.
- **Formez les utilisateurs à repérer et à signaler les emails malveillants.** Une formation et des simulations d'attaques régulières peuvent réduire les risques de deux façons. D'abord, elles apportent aux utilisateurs les connaissances nécessaires pour bloquer un grand nombre d'attaques. Ensuite, elles permettent d'identifier les utilisateurs particulièrement vulnérables. Les simulations les plus efficaces imitent les techniques d'attaque du monde réel. Optez pour une solution qui tient compte des tendances actuelles des attaques ciblant le secteur des assurances et des services financiers, et qui intègre les informations de threat intelligence les plus récentes. Lorsque les utilisateurs signalent des emails suspects, l'automatisation permet de vérifier et de neutraliser les véritables menaces.
- **En parallèle, partez du principe que les utilisateurs cliqueront inévitablement sur un lien.** Les cybercriminels trouveront toujours de nouvelles techniques pour exploiter la nature humaine. Trouvez une solution qui repère et bloque les emails entrants malveillants ciblant les utilisateurs avant qu'ils n'atteignent la boîte de réception. Neutralisez les menaces extérieures qui utilisent votre nom de domaine pour cibler vos clients. Une solution de prévention des fuites de données (DLP) efficace permet de garantir la protection et la disponibilité des données. Optez pour une solution capable de classer avec précision les informations sensibles et critiques, ainsi que de garantir qu'elles sont consultées par les personnes autorisées.
- **Mettez en place un dispositif de défense robuste contre les attaques BEC.** Les outils de sécurité traditionnels peinent parfois à détecter les emails d'imposteurs. Investissez dans une solution capable de gérer les emails au moyen de règles personnalisées de mise en quarantaine et de blocage. Dans la mesure où les cybercriminels ont parfois recours à des comptes compromis pour leurrer des utilisateurs au sein de la même entreprise, votre solution doit analyser tant les emails externes qu'internes. Déployez l'authentification DMARC (Domain-based Message Authentication, Reporting and Conformance) afin de bloquer les emails usurpés avant que les collaborateurs et les associés soient victimes d'une escroquerie.
- **Adoptez une approche Zero Trust de l'accès à distance.** Les compagnies d'assurance et les entreprises de services financiers n'ont jamais stocké et traité autant de données. Leur présence numérique est plus étendue. Leur personnel est plus dispersé. Du pain béni pour les cybercriminels. En outre, les technologies VPN traditionnelles ne sont plus à la hauteur. Investissez dans une solution Zero Trust capable de mettre vos collaborateurs, associés et clients en relation avec votre centre de données et le cloud rapidement et en toute sécurité.
- **Isolez les sites Web et URL à risque.** Empêchez le contenu Web à risque d'entrer en contact avec votre environnement. La technologie d'isolement du Web peut évaluer les pages suspectes et les URL non vérifiées dans un conteneur protégé, au sein du navigateur habituel de l'utilisateur. Cette approche peut constituer une protection critique pour les comptes de messagerie partagés, qui sont difficiles à sécuriser au moyen de l'authentification à plusieurs facteurs. Cette même technologie peut isoler la navigation Web personnelle et les services de messagerie Web des utilisateurs, ce qui leur garantit liberté et confidentialité sans mettre en danger l'entreprise.

- **Sécurisez Microsoft 365 et les autres plates-formes cloud.** Face à la migration d'un nombre croissant de données et d'applications du secteur des assurances et des services financiers vers le cloud, vous avez besoin d'une visibilité en temps réel sur les activités dans le cloud. Une solution CASB (Cloud Access Security Broker) peut vous aider à analyser et à neutraliser rapidement les violations potentielles des règles de messagerie dans le cloud afin d'assurer la continuité des services.
- **Identifiez et neutralisez les menaces internes.** Protégez-vous contre les fuites de données, le sabotage et les atteintes à la marque dus à la malveillance, à la négligence ou à la compromission des utilisateurs internes. Adoptez une solution de gestion des menaces internes qui met en corrélation les activités et les mouvements de données pour vous aider à faire le lien entre le comportement et les intentions des utilisateurs. Aidez les équipes de sécurité à identifier les risques liés aux utilisateurs, à détecter et à contrer les compromissions de données d'origine interne, ainsi qu'à accélérer la réponse aux incidents.
- **Réduisez les risques de conformité.** Les réglementations de conformité applicables au secteur des assurances et des services financiers ne cessent d'évoluer. Les entreprises sont soumises à davantage d'audits et à des amendes plus élevées, et doivent assurer la conformité aux réglementations de leurs associés. Optez pour une solution d'archivage et de conformité capable de détecter et de stopper rapidement les fuites de données d'origine interne, qu'elles soient délibérées ou accidentelles. Identifiez et éliminez les pratiques métier frauduleuses, telles que les fraudes à la facturation et les pots-de-vin.
- **Collaborez avec un fournisseur spécialisé dans la threat intelligence.** Pour faire face aux attaques extrêmement ciblées, vous avez besoin d'informations de threat intelligence avancées sur les menaces. Tirez parti d'une solution combinant des techniques statiques et dynamiques de détection des nouvelles caractéristiques des attaques (c'est-à-dire leurs outils, tactiques et cibles), et qui soit en mesure d'en tirer les enseignements nécessaires.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0400-003-01-01 1/21