proofpoint.

EBOOK

Cinq cyberattaques réelles et comment les neutraliser

Vol. 2 : attaques techniques

proofpoint.com/fr

Introduction

Les cybercriminels sont habiles et extrêmement motivés. Pourquoi ne le seraient-ils pas ? Ils évoluent dans un secteur à forte croissance où les risques sont faibles et les bénéfices si importants que la cybercriminalité devrait coûter au monde 23,8 billions de dollars par an d'ici 2027[1].

Face à de telles perspectives de profits, la créativité dont font preuve les cyberpirates semble infinie. De nouvelles campagnes de malwares, attaques de phishing et tactiques d'ingénierie sociale ingénieuses voient quotidiennement le jour, les équipes de sécurité jouant au chat et à la souris avec les cybercriminels. Bien que ces nouvelles menaces puissent sembler infiniment variées, elles présentent un certain nombre de points communs : elles sont véhiculées par la messagerie et ciblent des personnes.

Dans cette série d'eBooks, nous nous pencherons sur certaines des attaques par email les plus insidieuses actuellement en circulation. Bon nombre d'entre elles ont franchi les défenses de plusieurs outils de sécurité avant d'être détectées. Pour vous aider à comprendre pourquoi, nous analyserons chaque attaque pas à pas afin de vous montrer comment elles se sont déroulées et comment les cybercriminels ont essayé d'exploiter les vulnérabilités humaines. Nous vous expliquerons ensuite comment elles ont été neutralisées.

Dans le volume 1, nous nous sommes intéressés aux attaques ayant recours à l'ingénierie sociale. Ce volume se penche sur des attaques plus techniques.

1 Forum économique mondial, « 2023 Was a Big Year for Cybercrime – Here's How We Can Make Our Systems Safer » (2023 a été une excellente année pour les cybercriminels – voici comment renforcer la sécurité de nos systèmes), janvier 2024.

Sommaire

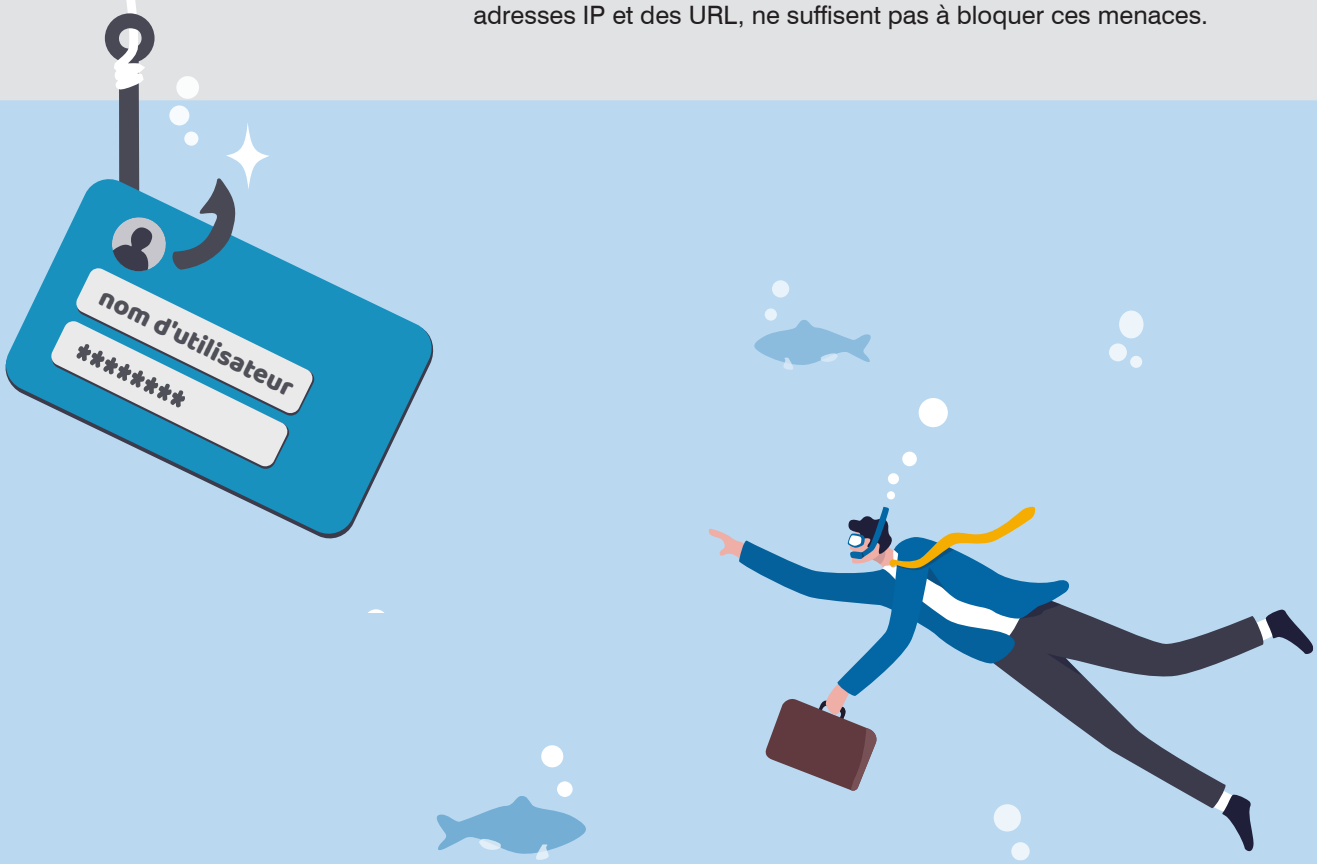
SECTION 1

Kit d'outils de phishing EvilProxy

EvilProxy est un kit d'outils de phishing conçu pour voler des identifiants de connexion utilisateur et des jetons d'authentification multifacteur (MFA).

Pour ce faire, il se place derrière une page Web légitime. Lorsque l'utilisateur se connecte à une page de phishing, une page de connexion frauduleuse ressemblant à un vrai portail de connexion et fonctionnant comme celui-ci s'affiche. EvilProxy peut ainsi capturer les identifiants de connexion de l'utilisateur et le jeton de la session d'authentification. Le cybercriminel peut alors utiliser ces informations pour contourner les protections MFA et se connecter au nom de l'utilisateur.

EvilProxy et les autres menaces contournant la MFA se multiplient, car les cybercriminels s'adaptent aux contrôles de sécurité renforcés. Les méthodes traditionnelles, comme l'analyse de la réputation des adresses IP et des URL, ne suffisent pas à bloquer ces menaces.



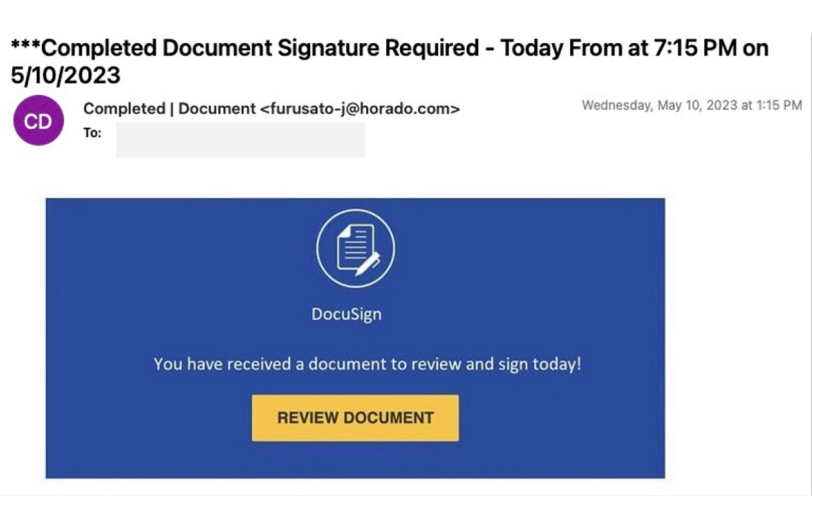
Le scénario

Au cours d'une évaluation des menaces liées à la messagerie, nous avons découvert qu'une entreprise technologique comptant 1 500 clients avait été exposée à EvilProxy. Cette menace avait échappé à un outil de protection de la messagerie existant.

Le déroulement de l'attaque

Examinons plus en détail le déroulement de l'attaque.

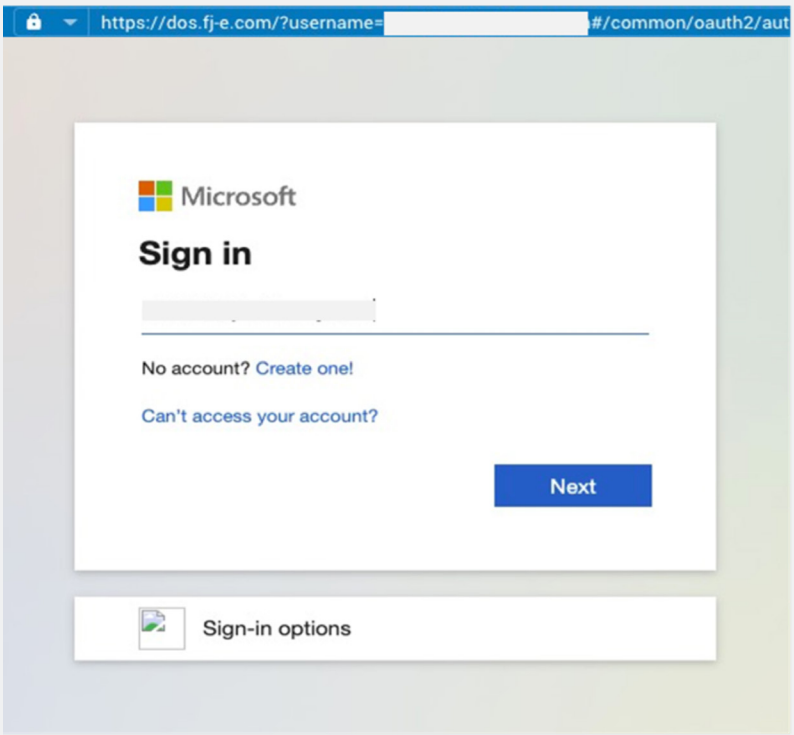
1. **Le message de leurre.** L'attaque a commencé par un email qui ressemblait à un avis DocuSign légitime. Celui-ci informait les destinataires qu'un document était prêt pour signature. Ce message en apparence inoffensif était en fait une passerelle vers une cyberattaque avancée.



L'email de leurre initial reçu par le client

2. **L'URL malveillante.** Lorsque les destinataires ont cliqué sur l'URL incorporée, ils ont été redirigés vers leur propre page de connexion Microsoft, derrière laquelle le proxy du cybercriminel avait été configuré. Avec cette page, le cybercriminel espérait inciter les utilisateurs à saisir leurs identifiants de connexion.

3. **Le framework de phishing EvilProxy.** Le framework de phishing EvilProxy était l'élément moteur de cette attaque. Les cybercriminels ont employé une technique de proxy inverse pour intercepter les tentatives de connexion des utilisateurs par le biais de leur page de connexion Microsoft. Ils ont ainsi pu extraire secrètement des codes MFA et des identifiants de connexion utilisateur.



La page de connexion Microsoft malveillante

4. **Le contournement de la vérification MFA.** Une fois en possession des codes MFA et des identifiants de connexion utilisateur, les cybercriminels ont pu accéder librement aux comptes compromis. Puisqu'ils sont parvenus à contourner la vérification MFA, ils ont pu infiltrer l'environnement de l'entreprise.

Comment Proofpoint a détecté l'attaque

Proofpoint a recours à l'apprentissage automatique avancé pour déchiffrer le contexte des messages entrants et analyser leur langage afin de détecter les menaces potentielles. Nous déterminons si un email est inoffensif, malveillant ou suspect en analysant le corps du message et le contexte. Nous examinons également les comportements d'envoi habituels de l'expéditeur. Si l'email comporte des charges virales suspectes, Proofpoint l'envoie dans un environnement sandbox en vue d'une analyse approfondie. Cela nous aide à déceler le contenu malveillant, même s'il n'a jamais été observé auparavant.

Dans ce scénario, Proofpoint a conclu que le message était suspect pour plusieurs raisons. Pour commencer, le destinataire n'avait pas l'habitude de recevoir des emails de cet expéditeur. En outre, l'expéditeur demandait au destinataire d'effectuer une action (cliquer sur l'URL). Comme nous ne pouvions pas déterminer de prime abord si l'URL était inoffensive ou malveillante, nous l'avons préventivement analysée en environnement sandbox.

En suivant l'URL, nous avons constaté qu'elle utilisait une tactique de redirection pour dissimuler sa nature malveillante. Notre moteur d'analyse des URL a découvert qu'elle menait à une page Web qui ressemblait à s'y méprendre à une page de connexion Microsoft. Au vu du comportement de cette page Web, Proofpoint a détecté un framework d'URL qui utilisait un service proxy destiné à voler les identifiants de connexion et les réponses MFA des utilisateurs en temps réel. Ces caractéristiques concordaient avec EvilProxy. En interceptant des identifiants de connexion et la réponse à un défi MFA en temps réel, les cybercriminels peuvent obtenir rapidement accès au compte d'un utilisateur même si une protection MFA est en place.

Résumé des observations de Proofpoint concernant l'email de signature électronique ayant conduit à son signalement

Détection du framework de phishing EvilProxy par Proofpoint

SECTION 2

Attaque SocGholish

Observé en circulation dès 2018, SocGholish est une variante de malware qui continue à faire des dégâts. Il utilise une grande diversité de phases, de vérifications de l'éligibilité et de routines d'obfuscation, ce qui en fait l'une des familles de malwares les plus furtives à ce jour. L'absence de détails concernant la sélection de ses cibles, sa logique de contournement et les procédures spécifiques de ses phases intermédiaires entretient le mystère qui l'entoure.

On observe quatre phases de base :

Phase 1 – Injections malveillantes
Un cybercriminel compromet un site Web légitime et injecte un script JavaScript malveillant qui établit le profil des utilisateurs dans l'objectif d'identifier des cibles à attaquer.

Phase 2 – Téléchargement de SocGholish
Si un utilisateur remplit certains critères, le script JavaScript introduit clandestinement SocGholish, qui ressemble souvent à une fausse mise à jour du navigateur. Si l'utilisateur clique dessus, SocGholish est téléchargé sur son terminal.

Phase 3 – Commande et contrôle
Le malware communique ensuite avec des proxys de commande et contrôle afin d'obtenir des instructions supplémentaires.

Phase 4 – Distribution de malwares secondaires et infection
SocGholish continue à établir le profil du terminal de l'utilisateur et effectue ensuite des appels aux serveurs de commande et contrôle pour distribuer des malwares secondaires, généralement des chevaux de Troie d'accès à distance ou des ransomwares.

Il est difficile de se défendre contre SocGholish. Cette menace est très répandue et peut échapper aux outils de protection de la messagerie les plus avancés. En 2023, au cours d'un seul mois, Proofpoint a détecté des milliers d'instances de SocGholish ayant échappé à d'autres couches de sécurité dans le monde entier.

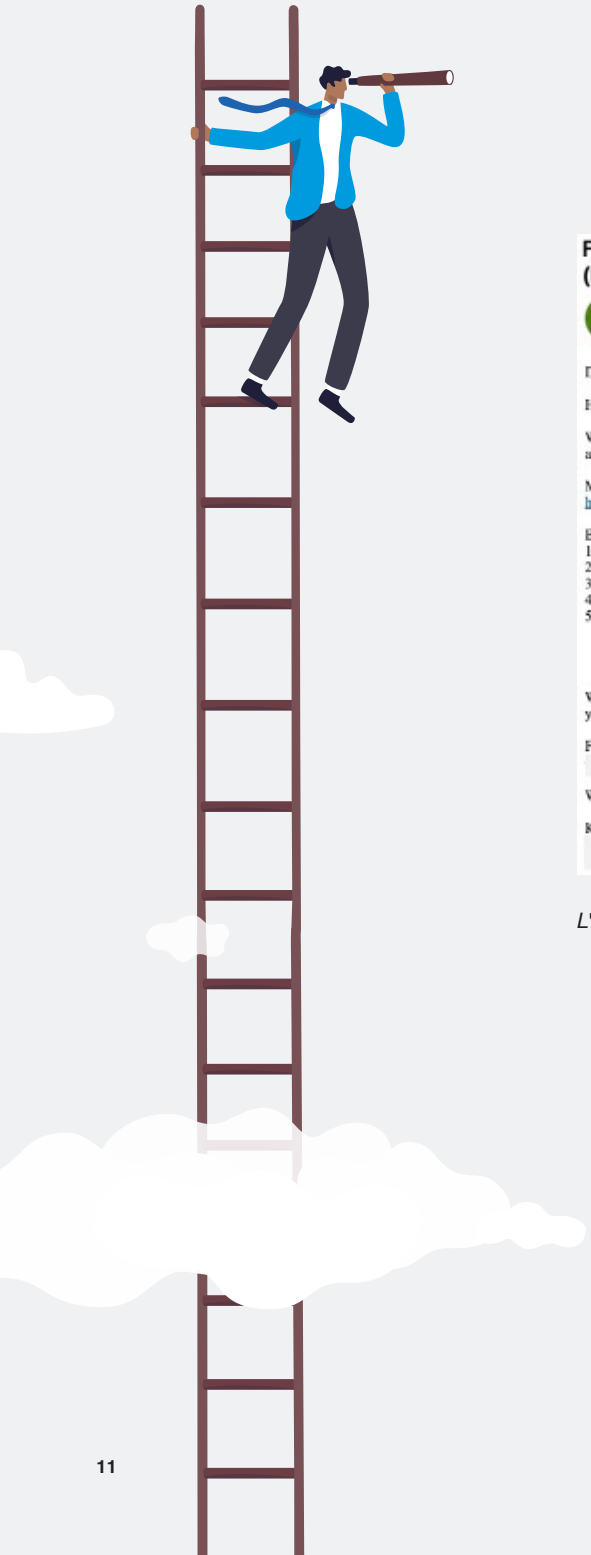
Le scénario

Au cours d'une évaluation des menaces liées à la messagerie, nous avons découvert qu'une entreprise technologique comptant 4 000 utilisateurs avait été exposée à une attaque SocGholish. Cette menace avait échappé à son précédent outil de protection de la messagerie.

Le déroulement de l'attaque

Examinons plus en détail le déroulement de l'attaque.

1. **Le message initial.** Les utilisateurs ont reçu un email les invitant à soumettre un article pour publication dans une revue spécialisée réputée. L'email en lui-même n'était pas malveillant et n'avait pas été créé par un cybercriminel. Comme toujours avec les campagnes SocGholish, le code malveillant ne s'est pas manifesté jusqu'à ce que l'utilisateur arrive sur le site Web compromis, mais légitime.



Follow up: Paper Invitation: [Environment and Social Psychology] (Indexed in Scopus) is Open for Submission

TS

To:

Thursday, June 29, 2023 at 6:05 AM

Dear

Hope this mail finds you well.

We were wondering if you have received our paper invitation for the journal *Environment and Social Psychology*. We are writing to inquire if you are interested in submitting a paper for publication in this journal.

More information can be found on the website:
https://esp.apacsci.com/index.php/esp/index

Benefits of publishing with ESP:
1.Open access (unlimited and free access for readers).
2.Indexed by the Scopus, NLB, Portico, and other databases.
3.Fast Publication combined with thorough peer review.
4.As indicated on the website, the APC of USD 1250 in 2023 applies to submitted papers.
5.We will provide discount for early bird submission:
*Early Bird Submission before July 31, 2023: 90%
*Early Bird Submission before August 31, 2023: 60%
*Early Bird Submission before September 30, 2023: 50%

We cordially invite you to submit a paper. In addition, we would appreciate it if you could recommend this journal to your colleagues. If you are interested, please kindly let us know.

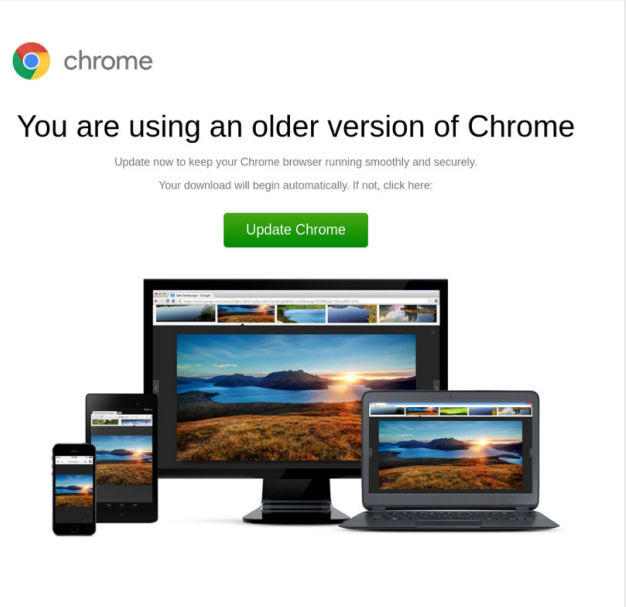
For any questions regarding technical issues or applying discount, please feel free to contact

We look forward to hearing from you.

Kind regards,

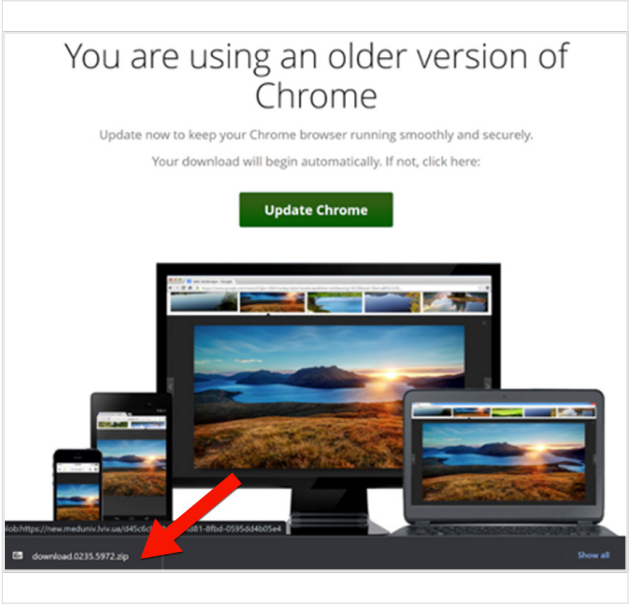
L'email initial reçu par notre client

2. **L'URL compromise.** Si l'utilisateur cliquait sur l'URL figurant dans l'email, le script JavaScript injecté à la destination commençait à établir son profil pour déterminer s'il s'agissait d'une cible à attaquer. Une fenêtre contextuelle s'affichait pour les utilisateurs pris pour cible, les informant que leur navigateur avait besoin d'être mis à jour.



La fausse demande de mise à jour du navigateur

3. **Installation de SocGholish.** Si l'utilisateur téléchargeait le pack de mise à jour, SocGholish analysait le terminal de l'utilisateur, sa configuration et les éléments auxquels il avait accès. SocGholish communiquait ensuite avec des proxys de commande et contrôle afin d'obtenir des instructions supplémentaires et de déterminer si des malwares secondaires devaient être installés.



Le fichier téléchargé lors de l'exécution de la fausse mise à jour du navigateur

Pourquoi ces menaces sont difficiles à détecter

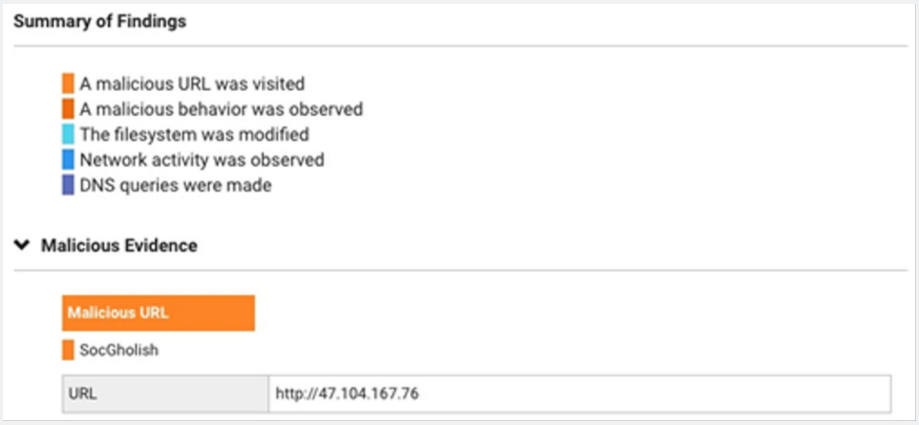
La plupart des outils de protection de la messagerie peuvent détecter les scripts JavaScript malveillants, mais SocGholish est de nature furtive. De nombreuses solutions de protection de la messagerie éprouvent des difficultés à détecter ses techniques de profilage, notamment l'inspection de l'adresse IP, du système d'exploitation, du navigateur et de la langue locale du terminal. Par ailleurs, les outils qui reposent exclusivement sur la détection des anomalies peinent à détecter les attaques telles que SocGholish, car l'email et l'URL sont tous deux légitimes.

SocGholish a également recours à des tactiques de contournement capables de détecter les environnements sandbox. Il ne se manifestera donc pas s'il détecte un environnement simulé tel que la sandbox d'un analyste des menaces. En outre, les outils de protection de la messagerie qui prétendent analyser les menaces grâce à l'IA et à l'apprentissage automatique ont également du mal à détecter SocGholish, car l'email en lui-même n'est pas malveillant. Les comportements d'envoi antérieurs ne permettraient pas non plus de l'identifier comme suspect.

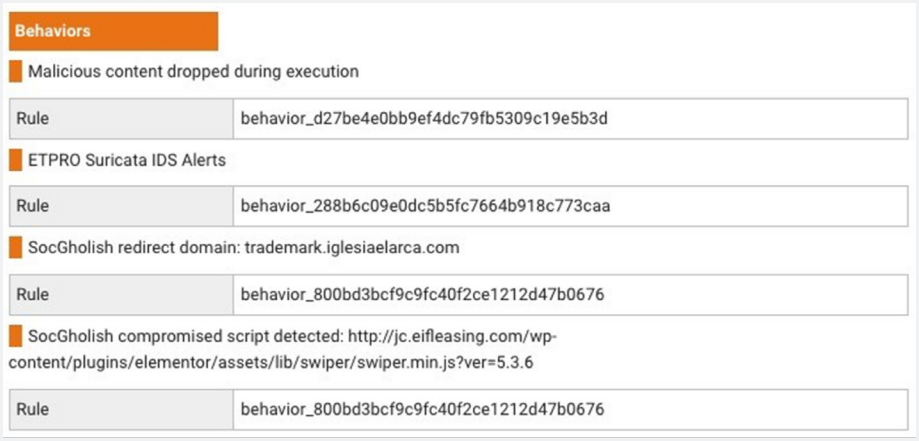
Comment Proofpoint a détecté l'attaque

Proofpoint a recours à une analyse comportementale approfondie des URL pour détecter plusieurs comportements suspects associés à SocGholish, tels que le profilage. Étant donné que nous analysons l'activité réseau, nous pouvons constater que le malware communique avec des proxys de commande et contrôle. Nous décelons également une autre tactique employée par SocGholish : la redirection vers un service DNS et l'exploitation de scripts compromis.

Dans ce scénario, Proofpoint a détecté des comportements d'envoi inhabituels. Nous avons donc analysé les URL en environnement sandbox avant que les utilisateurs ne cliquent sur des liens. Le sandboxing prédictif d'URL sélectives est une fonctionnalité distincte propre à Proofpoint. C'est l'une des raisons pour lesquelles nous sommes en mesure de détecter des menaces basées sur des URL qui n'ont encore jamais été observées auparavant.



Rapport d'investigation numérique du tableau de bord Proofpoint TAP montrant des activités qui sont le signe d'une attaque SocGholish



Rapport d'investigation numérique du tableau de bord Proofpoint TAP montrant des comportements spécifiques qui sont le signe d'une attaque SocGholish

Proofpoint priorise par ailleurs une analyse fréquente et exhaustive des URL. Le groupe cybercriminel TA569, souvent associé à SocGholish, est parvenu à conserver un contrôle sur les sites injectés. Nous avons observé des cas dans lesquels des pages Web nettoyées ont été à nouveau compromises au moyen d'attaques similaires ou différentes.

Nous analysons donc les URL en environnement sandbox de manière proactive après qu'elles ont été identifiées comme inoffensives ou nettoyées. Une surveillance continue permet de s'assurer que toute compromission potentielle est détectée rapidement.

SECTION 3

Phishing par code QR

Le phishing par code QR déplace le canal d'attaque de l'environnement de messagerie protégé vers le terminal mobile d'un utilisateur, souvent bien moins sécurisé.

Avec les codes QR, l'URL n'est pas exposée dans le corps de l'email, ce qui rend la plupart des analyses de protection de la messagerie inefficaces. Par ailleurs, le décodage des escroqueries par code QR à l'aide de la reconnaissance d'image ou de la reconnaissance optique des caractères (OCR) devient rapidement gourmand en ressources et difficile à appliquer à grande échelle.

Le scénario

Proofpoint a récemment détecté l'une de ces attaques dans une entreprise agricole comptant plus de 16 000 collaborateurs. Un cybercriminel avait créé un leurre de phishing qui semblait fournir des informations sur les salaires d'un collaborateur. Le message demandait au collaborateur de scanner un code QR avec son téléphone mobile pour accéder aux informations, plutôt que de cliquer sur un lien. Une fois le code QR scanné, un faux écran de connexion SharePoint l'incitait à renseigner ses identifiants de connexion.

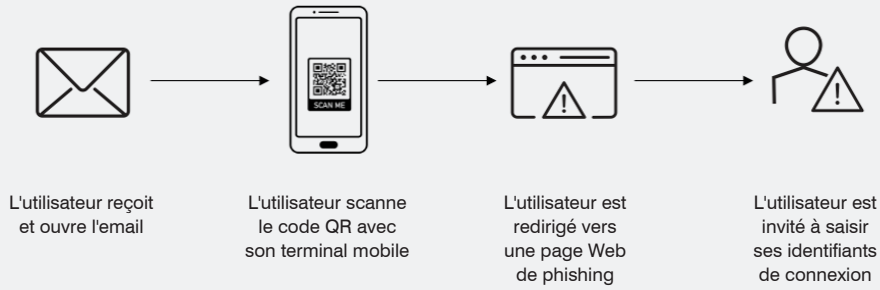
Le déroulement de l'attaque

Voici comment l'attaque s'est déroulée :

1. **Le message de leurre.** Le collaborateur a reçu un email qui semblait provenir de l'équipe RH de l'entreprise et qui prétendait contenir des informations relatives aux salaires.

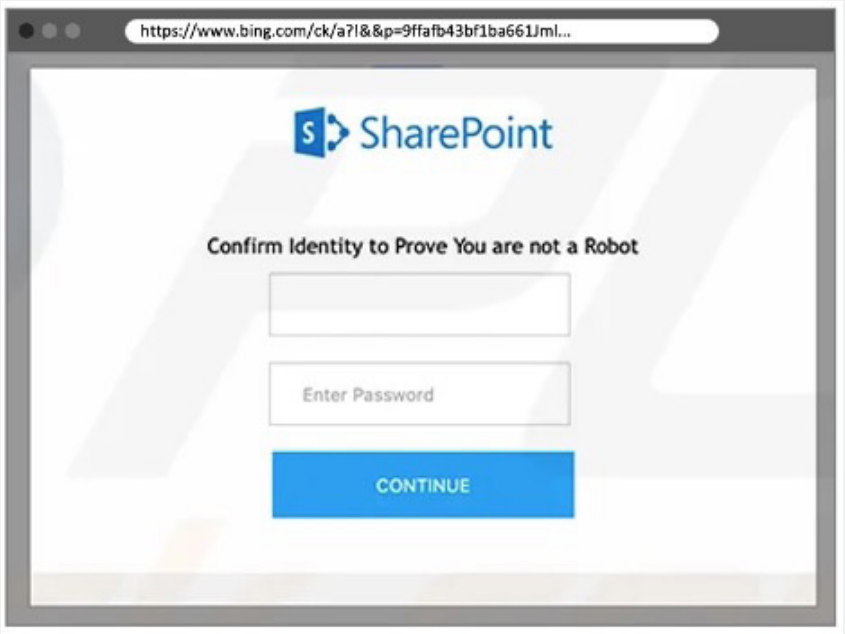
Email malveillant bloqué par Proofpoint avant qu'il ne soit distribué dans la boîte email de l'utilisateur (Remarque : pour des raisons de sécurité, nous avons remplacé le code QR malveillant par un code QR redirigeant vers le site Proofpoint.com. Le reste du message est une capture d'écran de l'original sur laquelle certaines informations ont été masquées.)

2. **Séquence d'attaque par code QR.** Le message demandait au collaborateur de scanner le code QR avec son téléphone mobile.



Séquence d'attaque type par code QR

3. **Leurre de phishing SharePoint.** Une fois l'URL décodée par le collaborateur, un faux écran de connexion SharePoint l'incitait à saisir ses identifiants de connexion.

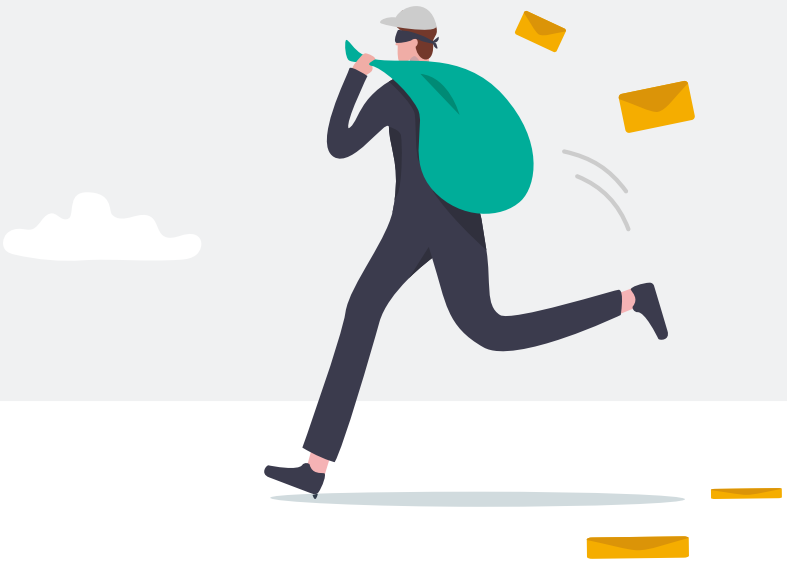


Code QR décodé redirigeant l'utilisateur vers une page de phishing SharePoint

Pourquoi ces menaces sont difficiles à détecter

Pour commencer, une URL de phishing incorporée à un code QR n'est pas facile à extraire et à analyser. Pour ne rien arranger, les codes QR sont aujourd'hui omniprésents. La plupart des signatures d'emails inoffensives contiennent des logos, des liens vers des pages de réseaux sociaux incorporés à des images et même des codes QR redirigeant vers des sites Web légitimes. La présence d'un code QR n'est donc pas un signe certain d'attaque de phishing.

Bien souvent, les outils de sécurité essaient de bloquer ces menaces en se focalisant exclusivement sur des comportements d'envoi inhabituels. Toutefois, ceux-ci ne constituent pas une base suffisamment solide pour condamner un message et peuvent entraîner la classification incorrecte d'un message inoffensif comme dangereux. C'est souvent le cas avec les outils de protection de la messagerie qui essaient de neutraliser les menaces après la remise.



Comment Proofpoint a détecté l'attaque

Proofpoint utilise une combinaison avancée de signaux et de couches d'analyse pour faire la différence entre les codes QR piégés et inoffensifs. Nous analysons les éléments suivants :

- L'expéditeur
- Les comportements de l'expéditeur
- La relation entre l'expéditeur et le destinataire en fonction des communications précédentes

Tous ces indices nous aident à identifier les expéditeurs suspects et à déterminer si leur comportement s'écarte d'un profil établi. Dans cet exemple, nos systèmes n'avaient encore jamais observé cet expéditeur communiquer avec cette entreprise ou ce destinataire.

Signaux utilisés par Proofpoint pour identifier le message comme une menace

Toutefois, nous ne nous basons pas uniquement sur les comportements d'envoi inhabituels. Pour réduire le nombre de faux positifs, nous combinons de nombreux autres signaux afin d'extraire la nature et les métonymies du contenu de l'email. (Une métonymie est une figure de style consistant à utiliser un mot ou une phrase pour représenter autre chose, par exemple « la Couronne » pour désigner la monarchie britannique. Ce type d'analyse nous aide à déduire l'intention d'un expéditeur quels que soient les mots employés.)

Nous inspectons l'historique des emails de l'expéditeur et procédons à une analyse linguistique et sémantique du corps du message. Grâce à cette approche, nous avons identifié un langage indiquant que l'email demandait au destinataire d'effectuer une action (ici, scanner un code QR avec son terminal mobile).

Outre une analyse comportementale et du langage, nous avons également détecté des tactiques d'imposture dans les en-têtes du message.
Les cybercriminels essaient souvent d'usurper l'identité d'entités fiables ou d'autres collaborateurs pour inspirer confiance. Dans ce scénario, les cybercriminels ont créé les en-têtes de l'email de manière à ce que celui-ci semble provenir du service RH et de paie de l'employeur.

Nous sommes également allés plus loin en analysant le code QR. Grâce aux technologies OCR et de reconnaissance d'image de nos moteurs de détection, nous avons analysé et neutralisé les URL malveillantes dissimulées au sein du code QR lui-même. Nous extrayons les URL et le texte pour nous assurer que les messages qui doivent être distribués le sont et que ceux qui ne doivent pas l'être sont bloqués ou corrigés.

SECTION 4

Manipulation de l'authentification multifacteur

La manipulation de l'authentification multifacteur (MFA) représente une menace majeure pour les plates-formes cloud. Il s'agit d'une technique sophistiquée dans le cadre de laquelle les cybercriminels appliquent leur propre méthode MFA à un compte cloud compromis.

Plusieurs options s'offrent aux cyberpirates qui souhaitent contourner la MFA. Ils peuvent notamment lancer une attaque de type adversary-in-the-middle (AiTM) : le cybercriminel insère un serveur proxy entre la victime et le site Web auquel elle tente de se connecter. Le cyberpirate peut ainsi voler le mot de passe de l'utilisateur ainsi que le cookie de session.

Rien n'indique à l'utilisateur qu'il a été attaqué ; il a l'impression de s'être connecté à son compte comme d'habitude. Pourtant, les cybercriminels ont ce dont ils ont besoin pour s'implanter durablement. Ils peuvent donc conserver un accès même si les identifiants de connexion MFA volés sont révoqués ou considérés comme invalides.

Les attaques de manipulation de la MFA sont déployées après une prise de contrôle de comptes cloud (ATO). Malheureusement, les attaques ATO sont très courantes. En 2023, les chercheurs spécialisés en menaces de Proofpoint ont découvert que presque toutes les entreprises (96 %) étaient ciblées par des attaques cloud. De plus, 60 % d'entre elles ont subi une compromission et la prise de contrôle d'au moins un compte.

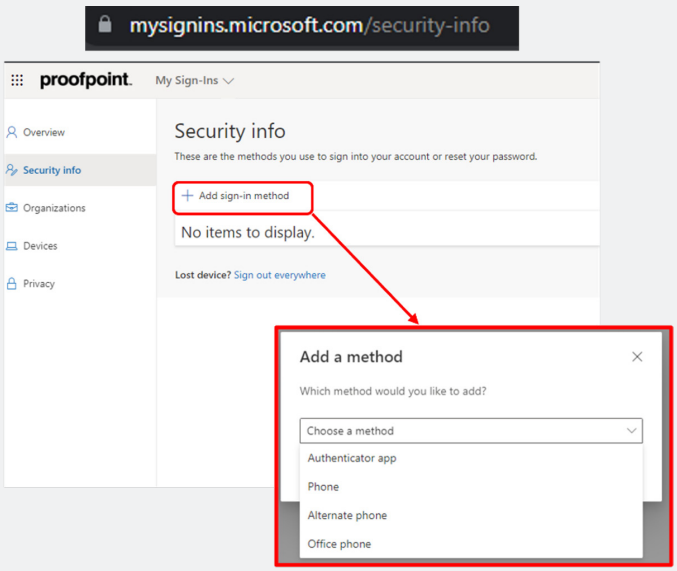
Le scénario

Proofpoint a intercepté une série d'attaques de manipulation de la MFA visant une importante société du secteur immobilier. Dans un cas, les cybercriminels ont utilisé une attaque AiTM pour voler les identifiants de connexion du contrôleur financier de l'entreprise ainsi que le cookie de session. Ils se sont ensuite connectés au compte professionnel de cet utilisateur et ont généré 27 activités d'accès non autorisé.

Le déroulement de l'attaque

Examinons plus en détail le déroulement de l'attaque.

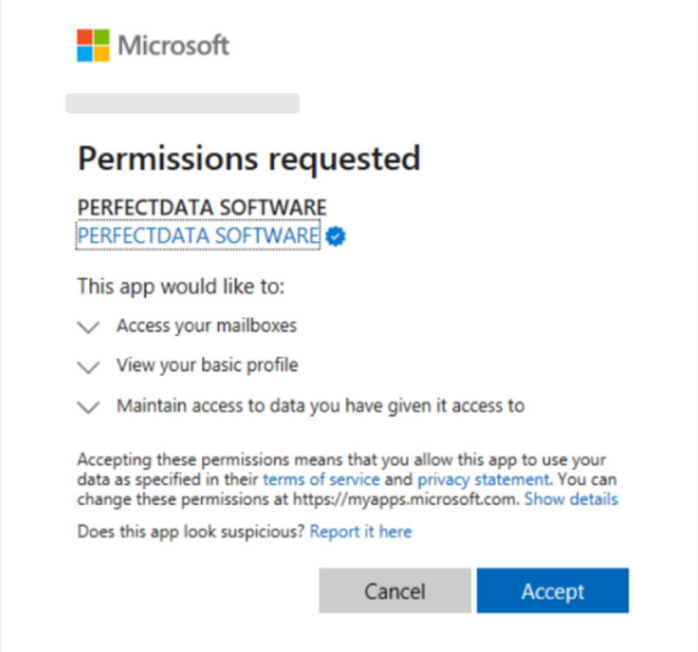
1. **Implantation sur le système.** Les cybercriminels ont utilisé l'application native « Mes connexions » pour ajouter leurs propres méthodes MFA afin de compromettre des comptes Microsoft 365. Nous avons constaté que les cybercriminels avaient enregistré leur propre application d'authentification avec notification et code. Cet enregistrement est intervenu juste après qu'ils ont obtenu un accès au compte piraté dans le cadre de l'exécution d'une attaque automatisée. Cela leur a permis de s'implanter durablement dans l'environnement cloud ciblé.



Flux type de manipulation de la MFA utilisant l'application « Mes connexions » de Microsoft

2. **Combinaison de plusieurs tactiques d'attaque.** Les cybercriminels ont adopté une approche très sophistiquée. Ils ont combiné manipulation de la MFA et exploitation des applications OAuth. Pour faire simple, on parle d'exploitation d'OAuth lorsqu'un cybercriminel utilise une application tierce pour voler des données, propager des malwares ou semer le chaos.
3. **Établissement d'un accès persistant.** Les cybercriminels ont également recours à une application exploitée pour conserver un accès même après que leur accès initial à un compte compromis a été révoqué. Dans ce scénario, les cyberpirates ont demandé des autorisations pour l'application en apparence inoffensive « PERFECTDATA SOFTWARE » pour établir un accès persistant au compte de l'utilisateur et aux systèmes, ainsi qu'aux ressources et applications. Voici les autorisations que les cybercriminels ont demandées pour cette application :
    - Accès complet et permanent à la boîte email de l'utilisateur
    - Accès hors ligne aux données
    - Accès au profil de l'utilisateur

Si ces autorisations avaient été octroyées, les cyberpirates auraient été libres de voler des données sensibles en continu. Il leur aurait ainsi été facile de distribuer des menaces à des comptes utilisateur internes ou externes.



La demande d'autorisations pour l'application « PERFECTDATA SOFTWARE », qui montre l'étendue de ces autorisations

Pourquoi ces menaces sont difficiles à détecter

Ces attaques en plusieurs étapes exploitent des fonctionnalités cloud légitimes. En outre, elles se fondent parfaitement avec les activités habituelles. C'est la raison pour laquelle elles échappent souvent aux mesures de sécurité traditionnelles. Les autres fournisseurs, qui se concentrent sur des événements isolés, peinent à établir des liens.

Comment Proofpoint a détecté l'attaque

Proofpoint a utilisé plusieurs stratégies pour déterminer comment les cybercriminels se sont infiltrés et ce qu'ils ont fait après la compromission. Ces stratégies comprenaient l'utilisation d'informations de threat intelligence internes ainsi que l'analyse du comportement des utilisateurs et des entités (UEBA).

Les étapes suivantes ont consisté à automatiser la correction des sessions malveillantes et à révoquer l'application PERFECTDATA SOFTWARE exploitée. Cela a permis à l'équipe de sécurité de l'entreprise du secteur immobilier de prendre immédiatement des mesures correctives.

Les chercheurs spécialisés en menaces cloud de Proofpoint ont également conseillé l'entreprise pendant qu'ils analysaient cet incident. Ils se sont assurés que toutes les méthodes MFA contrôlées par le cybercriminel avaient été supprimées pour de bon, afin de réduire les risques à l'avenir.

Détails de l'application tierce révoquée

SECTION 5

Attaque multicouche par code QR

En général, lors d'une attaque par code QR, un code QR malveillant est directement incorporé dans un email. Mais récemment, les cybercriminels ont imaginé une nouvelle variante sophistiquée. Lors de ces attaques multicouches, le code QR malveillant est dissimulé dans ce qui semble être une pièce jointe inoffensive au format PDF.

Pour ralentir la détection automatisée et perturber les outils traditionnels de protection de la messagerie, les cyberpirates ont recours à des tactiques de contournement telles que l'ajout d'un CAPTCHA sur la page de renvoi. Les outils de détection traditionnels basés sur l'analyse de la réputation des URL ont donc de plus en plus de mal à identifier ces menaces.

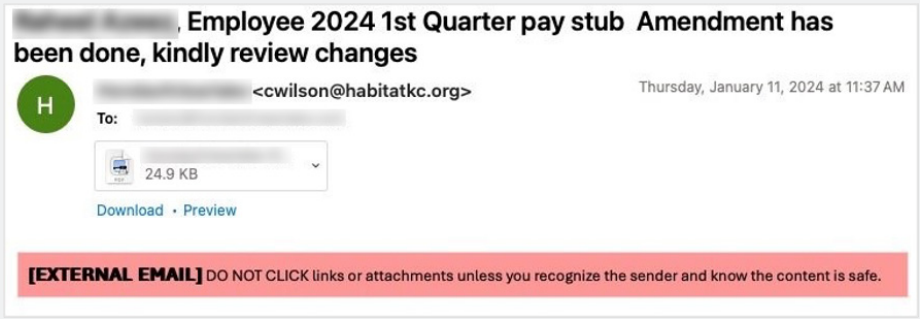
Le scénario

Proofpoint a récemment détecté l'une de ces menaces alors qu'il réalisait une évaluation des menaces dans une entreprise automobile américaine comptant 11 000 collaborateurs. Les outils de sécurité existants de l'entreprise — une solution de protection de la messagerie basée sur une API et sa sécurité native — se targuaient de disposer de fonctionnalités d'analyse des codes QR. Pourtant, ils ont classifié l'email comme inoffensif et l'ont distribué à l'utilisateur final.

La menace – Comment l'attaque s'est-elle déroulée ?

Examinons plus en détail le déroulement de l'attaque.

1. **Leurre.** L'email était conçu pour paraître légitime et jouait sur l'urgence de la période de déclaration fiscale. Il incitait le destinataire à ouvrir une pièce jointe au format PDF.

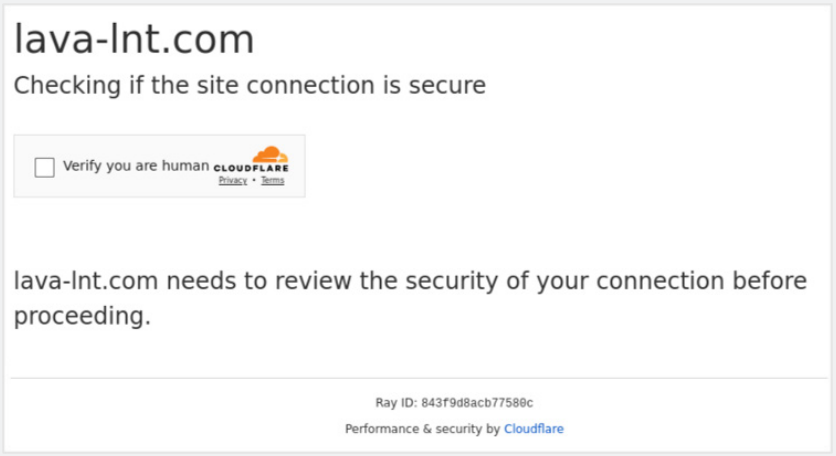


L'email initial reçu par l'utilisateur final

2. **Code QR malveillant incorporé dans le PDF.** Contrairement à de précédentes attaques par code QR, l'URL malveillante utilisée dans cette attaque n'était pas directement visible dans l'email. Elle était dissimulée dans le PDF joint. Compte tenu de l'omniprésence des codes QR, le destinataire n'aurait pas forcément trouvé cela suspect.

Le PDF joint avec le code QR incorporé (masqué)

3. **CAPTCHA Cloudflare.** Le cybercriminel a ajouté une couche de leurre supplémentaire. Il a utilisé un CAPTCHA Cloudflare sur la page de renvoi de l'URL du code QR pour dissimuler davantage la menace sous-jacente. Cette étape avait pour but de contourner les outils de détection qui s'appuient exclusivement sur l'analyse de la réputation des URL.



CAPTCHA Cloudflare sur la page de renvoi de l'URL du code QR

4. **Phishing d'identifiants de connexion.** Une fois le CAPTCHA résolu, le code QR malveillant menait à une page de renvoi de phishing destinée à voler des identifiants de connexion utilisateur. Le vol d'identifiants de connexion utilisateur peut permettre à un cyberpirate d'accéder au compte d'un utilisateur pour propager des attaques en interne. Le cybercriminel peut également utiliser ces identifiants en externe pour piéger des partenaires ou des fournisseurs, par exemple pour compromettre des comptes fournisseurs.

Pourquoi ces menaces sont difficiles à détecter

L'utilisation de la reconnaissance optique des caractères (OCR) ou d'autres techniques d'analyse des codes QR joue un rôle essentiel dans la défense contre les menaces basées sur des codes QR. Toutefois, l'analyse des codes QR n'est pas le seul mécanisme employé pour extraire l'URL dissimulée. Il ne s'agit pas d'un mécanisme de détection permettant de distinguer les codes QR légitimes des codes QR malveillants.

De nombreux outils, y compris les solutions de protection de la messagerie utilisées par l'entreprise automobile, prétendent inspecter les codes QR et extraire l'URL à des fins d'analyse. Ils ne sont cependant pas capables d'analyser les URL au sein d'une image incorporée dans une pièce jointe.

Comment Proofpoint a détecté cette attaque

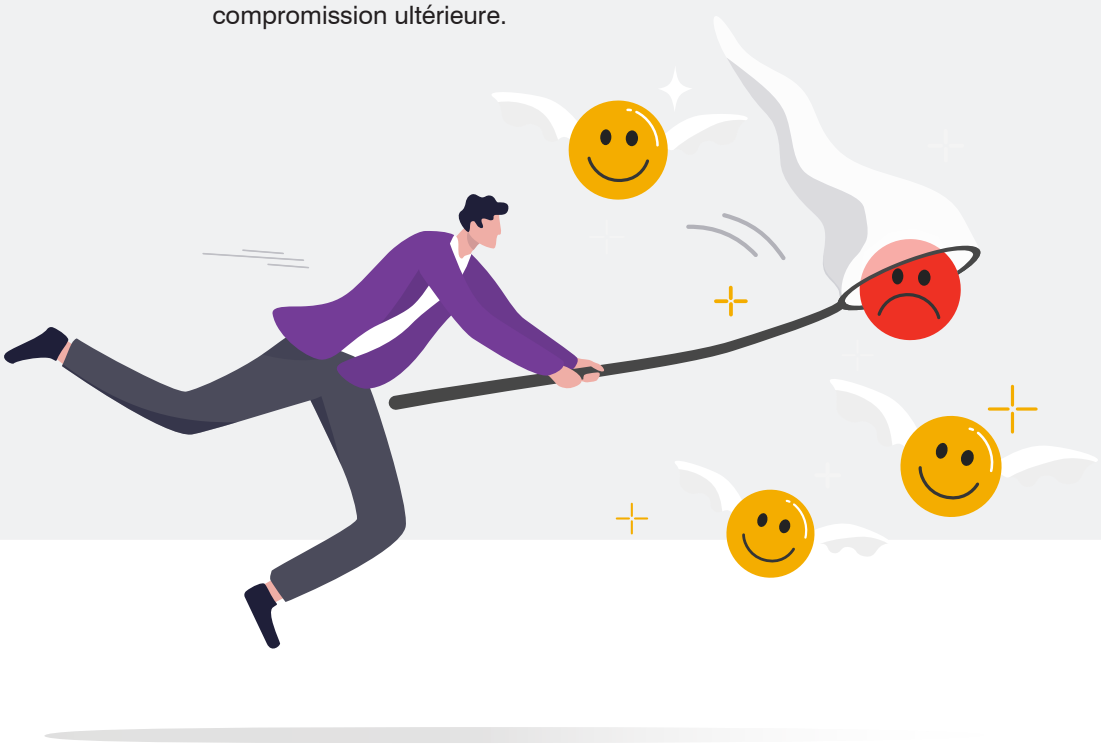
Rares sont les outils permettant de procéder à une analyse approfondie des URL à la même échelle que Proofpoint. Nous combinons l'analyse des codes QR à une pile de détection multicouche, qui a recours à des technologies d'IA et d'apprentissage automatique avancées. Comme nous analysons à la fois l'URL et son comportement, nous sommes en mesure de comprendre le contexte des emails et de détecter des menaces avancées basées sur des URL qui échappent aux autres outils.

Voici ce que nous avons utilisé pour détecter et neutraliser cette menace :

Analyse des codes QR. Proofpoint a utilisé l'analyse des codes QR pour convertir des images dans un format lisible par machine. Nous avons ainsi pu extraire l'URL dissimulée pour procéder à une analyse plus poussée. Notre technologie d'analyse des codes QR prend en charge les fichiers PDF, le corps des emails, les images, les fichiers Microsoft Word et bien d'autres éléments.

Indicateurs comportementaux. Proofpoint a analysé le comportement de l'utilisateur, le contexte de l'email et la nature thématique du message. Nous avons détecté des schémas indiquant qu'il était très probable que l'email soit malveillant.

Sandboxing d'URL. Lorsque l'URL est extraite au sein d'un environnement sandbox, Proofpoint peut analyser les éléments visuels, les schémas de redirection, les processus des endpoints, l'activité réseau, les appels DNS et les processus de processeur et de mémoire. Nous pouvons également détecter les tactiques de contournement des mesures antifraude telles que les CAPTCHA. Même si l'URL semble inoffensive, malgré l'observation d'indicateurs comportementaux associés à une activité malveillante, nous continuons à la surveiller et à l'analyser afin de détecter toute compromission ultérieure.



SECTION 6

Conclusion

Toutes ces escroqueries ne font que souligner le besoin critique de mesures de cybersécurité robustes et multicouches.

Pour garder une longueur d'avance sur les menaces en constante évolution telles que celles-ci, vous devez adopter une approche complète de la protection contre les menaces qui ciblent vos collaborateurs :

- **Détectez les menaces avant la remise.** Le seul moyen de protéger les utilisateurs est de bloquer les messages malveillants avant leur remise. D'après les recherches menées par Proofpoint, un utilisateur sur sept clique sur un email dans la minute. Optez pour un outil qui allie algorithmes d'apprentissage automatique et threat intelligence avancée pour identifier et bloquer les menaces avancées.
- **Formez vos utilisateurs.** Vos collaborateurs, sous-traitants et partenaires constituent votre première ligne de défense. Assurez-vous qu'ils bénéficient de formations de sensibilisation à la sécurité informatique pour tous les types d'attaques. Rappelez-leur de signaler rapidement tout comportement inhabituel.
- **Réalisez des audits de sécurité réguliers.** Les audits peuvent vous aider à identifier les vulnérabilités potentielles au sein de votre environnement. Ce faisant, assurez-vous de rechercher les irrégularités dans vos configurations et vos journaux d'accès.
- **Configurez votre système afin qu'il détecte les erreurs de configuration.** En plus de rechercher les erreurs de configuration, n'oubliez pas d'activer la correction automatique. Vous pourrez ainsi détecter les modifications non autorisées et les corriger rapidement, ce qui empêchera les cybercriminels de s'implanter durablement dans votre entreprise.
- **Élaborez un plan de réponse aux incidents.** Identifiez plusieurs scénarios d'attaque. Déterminez ensuite comment vous analyserez et corrigerez les incidents. Assurez-vous de tester l'efficacité réelle de votre plan en effectuant régulièrement des exercices de simulation.

Étapes suivantes

Plus que jamais, il est important de protéger votre entreprise contre les menaces email en plein essor. Vous devez adopter une approche proactive pour protéger votre entreprise, vos collaborateurs et vos clients contre les attaques avancées telles que les ransomwares, les menaces BEC et le phishing d'identifiants de connexion.

L'évaluation rapide des risques liés à la messagerie proposée par Proofpoint vous offre une visibilité et des informations complètes sur votre vulnérabilité aux attaques. Elle vous aide à identifier les personnes ciblées par des menaces email au sein de votre entreprise.

N'attendez pas qu'il soit trop tard pour tester la sécurité de votre messagerie. Contactez Proofpoint pour bénéficier d'une **évaluation gratuite des risques liés à la messagerie**.

EN SAVOIR PLUS

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

À PROPOS DE PROOFPOINT

Proofpoint, Inc. 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 85 % des entreprises de l'index Fortune 100, 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.

0503-007-03-01 08/24