Machine Translated by Google

Quarkslab

AU-DELÀ DE LA BOÎTE DE RÉCEPTION : GUIDE PRATIQUE DU CLOUD À L'INTENTION DU RSSI TACTIQUES DE PHISHING BASÉES SUR ET LA NOUVELLE CHAÎNE D'ENNUI DU PHISHING

JUIN 2025

Machine Translated by Google

RÉSUMÉ EXÉCUTIF

Le courrier électronique reste la principale porte d'entrée des attaquants modernes :

Ampleur de la menace : L'hameçonnage représente déjà 1,2 % du trafic mondial de courriels, soit environ 3,4 milliards de messages par jour. Même avec un taux de clic moyen de « seulement » 3 %, cela représente plus de 100 millions d'opportunités de compromission quotidiennes.

Impact sur l'activité : 91 % des incidents de sécurité majeurs commencent encore par un seul courriel malveillant.

Trois instantanés du monde réel qui sont passés inaperçus passerelles au cours des 12 derniers mois :

1. Des collecteurs d'identifiants Microsoft 365 qui reproduisent à la perfection le flux de connexion natif, attirant les utilisateurs vers les écrans « Suivant » et « Mot de passe » hébergés sur des serveurs de l'attaquant.

2. Notifications de faux documents DocuSign
   Exploiter la notoriété de la marque : bannières, boutons et pieds de page sont si bien clonés que même le personnel formé les reconnaît au premier coup d'œil.

3. La campagne de faux CAPTCHA de Blind Eagle , se faisant passer pour Google reCAPTCHA mais déposant discrètement une charge utile PowerShell lorsque l'utilisateur suit les frappes de touches de « vérification » à l'écran.

Pourquoi ces e-mails parviennent à vos utilisateurs :

Abus de réputation du cloud : les attaquants se cachent derrière des domaines Microsoft Azure, Cloudflare Worker ou Google qui héritent de certificats de confiance ; l'abus de Cloudflare à lui seul a augmenté de 198 % en 2024.

L'authentification multifacteur n'est plus une solution miracle : les kits Browser-in-the-Browser et Adversary-in-the-Middle renvoient une session de connexion en direct aux attaquants, contournant les jetons 2FA de manière transparente.

Escalade en cas de compromission de messagerie professionnelle (BEC) : Une fois qu'une boîte mail est compromise, les attaquants répondent depuis le compte réel pour contourner les contrôles internes et effacer les signaux d'alerte classiques.

Implications pour les RSSI

La frontière est passée du filtrage périmétrique aux frontières de confiance humaine et aux chaînes d'approvisionnement cloud.

Les contrôles traditionnels (passerelles de messagerie sécurisées, formation des utilisateurs) doivent désormais être renforcés par une simulation continue d'adversaires, une surveillance de l'infrastructure et une analyse comportementale.

La validation indépendante par une équipe rouge est le moyen le plus rapide de découvrir quels chemins trompeurs atteignent encore votre conseil d'administration, vos équipes financières ou DevOps avant que les criminels ne le fassent.

NOTE BRÈVE :

L'unité de sécurité offensive de Quarkslab réalise des exercices complets de phishing et de tests d'intrusion dans le cloud pour les entreprises du Fortune 500/CAC 40 et les clients du secteur des infrastructures critiques. Si les scénarios décrits ci-dessus vous semblent trop réalistes, notre équipe est à votre disposition pour évaluer votre niveau d'exposition et adapter vos défenses en conséquence.

Machine Translated by Google

TABLE DES MATIÈRES

Machine Translated by Google

INTRODUCTION

En 2025, le phishing reste la forme de cyberattaque la plus répandue au monde. En effet, 1,2 % du trafic mondial de courriels est constitué de tentatives de phishing, soit 3,4 milliards de courriels par jour. Pourtant, seul un faible pourcentage d'entre eux aboutit à une compromission, puisque « seulement » 3 % des employés cliqueraient sur un lien malveillant. Or, lorsqu'ils cliquent, les conséquences peuvent être désastreuses pour leur entreprise. 91 % des cyberattaques débutent par l'envoi d'un courriel malveillant à une cible.
Compte tenu de cela, on comprend aisément pourquoi le phishing reste l'un des vecteurs d'accès initiaux préférés des acteurs malveillants.

Plongeons-nous dans une exploration technique des tactiques de phishing modernes, des simples pages HTML aux techniques avancées de contournement de l'authentification multifacteur, en analysant l'infrastructure et les méthodes de diffusion utilisées par les phishingers en 2025.

Machine Translated by Google

1. TECHNIQUES DE PHISHING AVANCÉES

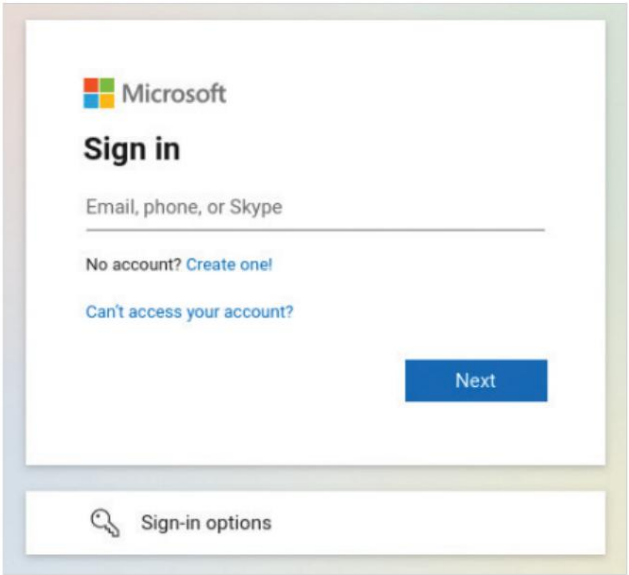
Mettez-vous à la place d'un attaquant. Vous voulez compromettre une organisation, que feriez-vous ? Du phishing, bien sûr. Après tout, c'est la voie de la moindre résistance, mais comment ?
Dans cette section, nous examinerons différentes approches utilisées dans les campagnes d'hameçonnage pour récupérer les identifiants ou même les sessions des victimes. Chacune de ces méthodes présente des avantages et des inconvénients.

LA MÉTHODE CLASSIQUE

PAGE HTML

Mentionner la page de phishing HTML classique parmi les techniques de phishing avancées peut paraître étrange, mais c'est probablement la plus répandue. Cette méthode consiste à créer une page HTML imitant l'apparence d'un site web légitime.
Par exemple, Microsoft étant l'entreprise la plus usurpée dans les campagnes d'hameçonnage, les auteurs de ces attaques copient souvent sa page de connexion afin de voler les identifiants de leurs victimes.

Le pirate n'a besoin que d'une page identique à l'originale, ce qui lui permet de supprimer ou de désactiver les éléments superflus. Dans l'exemple ci-dessus, tous les boutons sauf « Suivant » peuvent être désactivés. Il en va de même pour les liens.

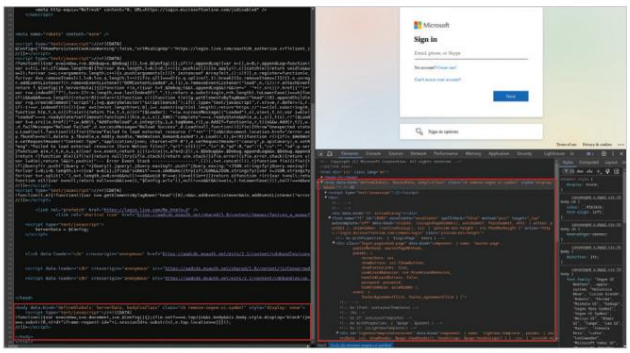


page de connexion Microsoft

REDIRECTIONS PERSONNALISÉES

Une autre option consiste à rediriger l'utilisateur vers une fausse page d'erreur lorsqu'il clique sur un bouton indésirable. Essayez de provoquer des erreurs sur le site légitime et copiez son design. N'oubliez pas d'adapter le texte pour qu'il corresponde à la nouvelle page d'erreur.

Puisque nous souhaitons uniquement conserver l'apparence, il est nécessaire de supprimer tous les scripts JavaScript, car ils pourraient envoyer des requêtes HTTP au site web d'origine et lui donner ainsi l'opportunité de détecter notre page de phishing. Attention cependant : de nos jours, les sites web sont générés dynamiquement dans votre navigateur. Il est donc conseillé de n'afficher la page souhaitée qu'une fois celle-ci entièrement chargée. Comme le montre la capture d'écran, le code source (à gauche) et la page chargée (à droite) ont des corps différents.

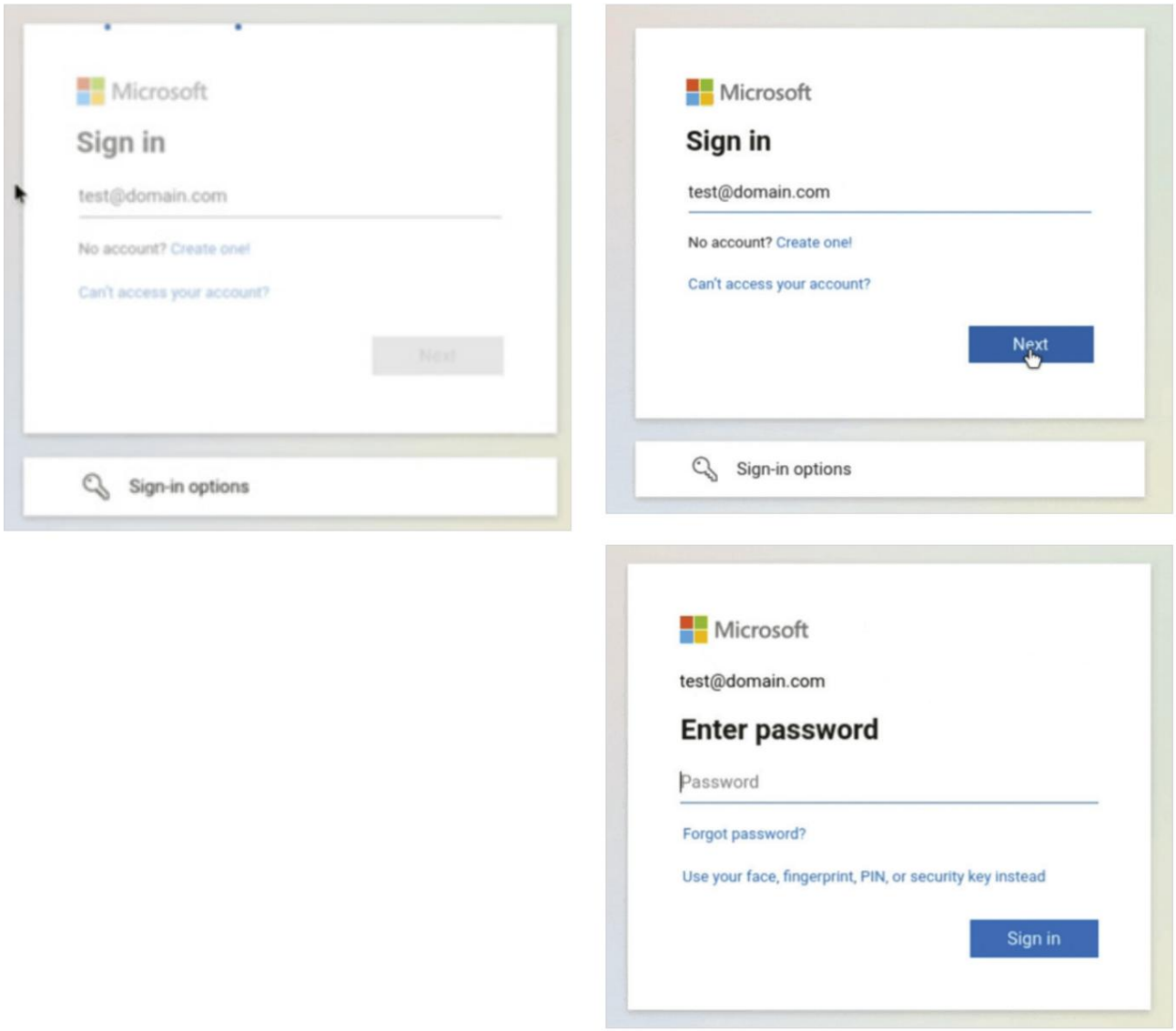


Différence dans <body> avant et après le chargement de la page

Machine Translated by Google

Sur les pages comportant plusieurs étapes, comme celles de Microsoft, il peut être judicieux de conserver certains effets d'animation pour rendre la page plus crédible aux yeux de la victime. Dans l'exemple, on voit une capture d'écran avec des points, puis la page demande le mot de passe de l'utilisateur. Le maintien de ces effets peut contribuer à réduire la vigilance des utilisateurs, car ils leur donnent l'impression que leur messagerie est réellement vérifiée.

familles



Transition entre l'invite de courriel et de mot de passe

Une fois que la victime a envoyé ses identifiants, redirigez-la vers un site web légitime ou affichez une page d'erreur.

AUCUN RETOUR EN ARRIÈRE

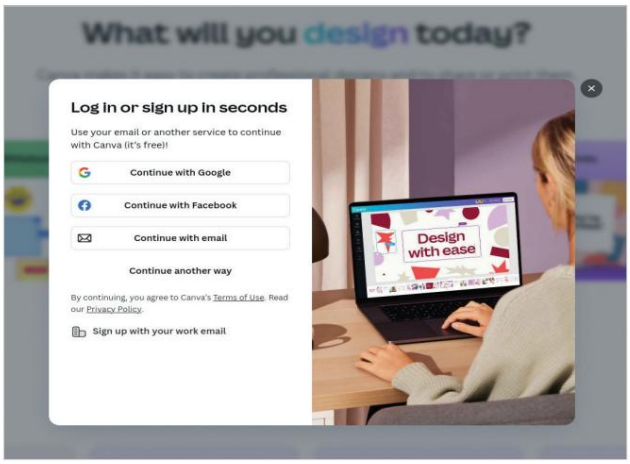
Au lieu d'envoyer le formulaire via une requête POST, utilisez JavaScript avec fetch() ou ajax, puis redirigez l'utilisateur.
Cela les empêchera d'utiliser le bouton Retour pour revenir à notre page d'hameçonnage.

Machine Translated by Google

LA MÉTHODE DÉLICATE

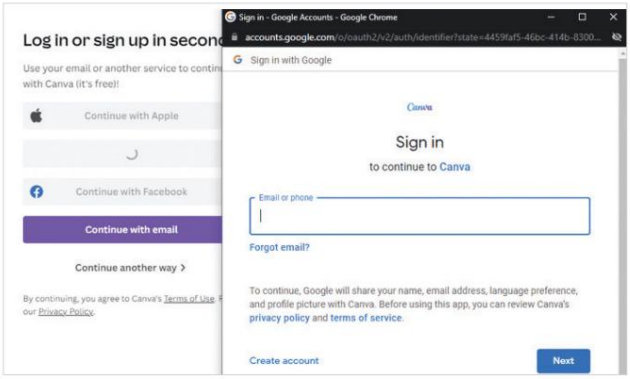
NAVIGATEUR DANS LE NAVIGATEUR

En 2022, un chercheur en sécurité nommé mr.d0x (@mrd0x) Il a introduit une technique appelée « attaque du navigateur dans le navigateur » (BITB). Son point de départ était une question simple : comment rendre le conseil « Vérifiez l'URL » moins fiable ? En effet, l'URL est souvent un excellent indicateur de la légitimité d'un site web, car elle ne peut être falsifiée. De plus, de nombreux sites web offrent aux utilisateurs la possibilité de s'authentifier auprès d'un tiers de confiance comme Microsoft, Apple, Google ou encore GitHub.



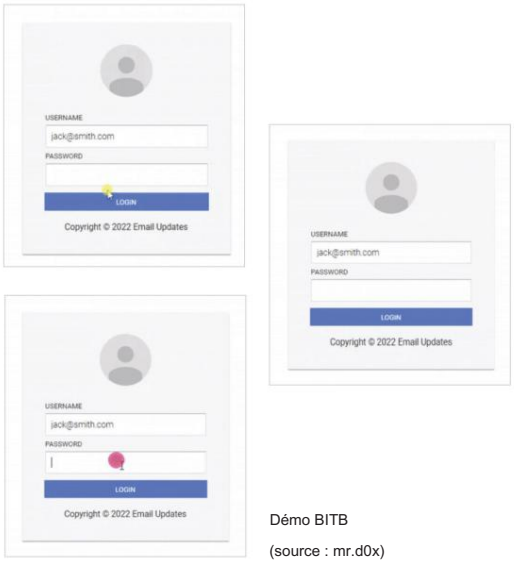
Plusieurs authentificateurs tiers sur la page de connexion de Canva

Cliquer sur « Continuer avec Google », par exemple, fait apparaître une fenêtre contextuelle vous demandant de vous connecter avec votre compte Google. compte.



Fenêtre contextuelle de connexion avec Google (source : mr.d0x)

Et c'est là que réside le piège. Le pirate peut reproduire ce comportement en utilisant uniquement HTML, CSS et JavaScript. Nous pourrions améliorer la page de phishing HTML classique en déplaçant le processus de connexion de notre domaine inhabituel vers une fausse page de navigateur avec une URL apparemment légitime. Cette fausse fenêtre de navigateur est une iframe que l'on peut déplacer et déposer comme une véritable fenêtre, ce qui la rend encore plus réaliste. Cela permet de créer un prétexte sans rapport avec les identifiants que l'on souhaite récupérer, simplement en ajoutant un bouton « Se connecter avec X ».



Démo BITB (source : mr.d0x)

Des modèles Windows et MacOS sont disponibles chez Dépôt de mr.d0x . Il a même créé des thèmes clairs et sombres pour les deux systèmes d'exploitation, qui pouvaient être affichés selon les préférences de la victime.

PLUS QU'UN FAUX NAVIGATEUR

La première preuve de concept réalisée par mr.d0x montre l'ouverture d'un faux navigateur, mais nous pouvons développer cette idée.
Un pirate informatique pourrait inciter un utilisateur à saisir ses identifiants dans un faux client VPN SSL comme FortiClient, par exemple.

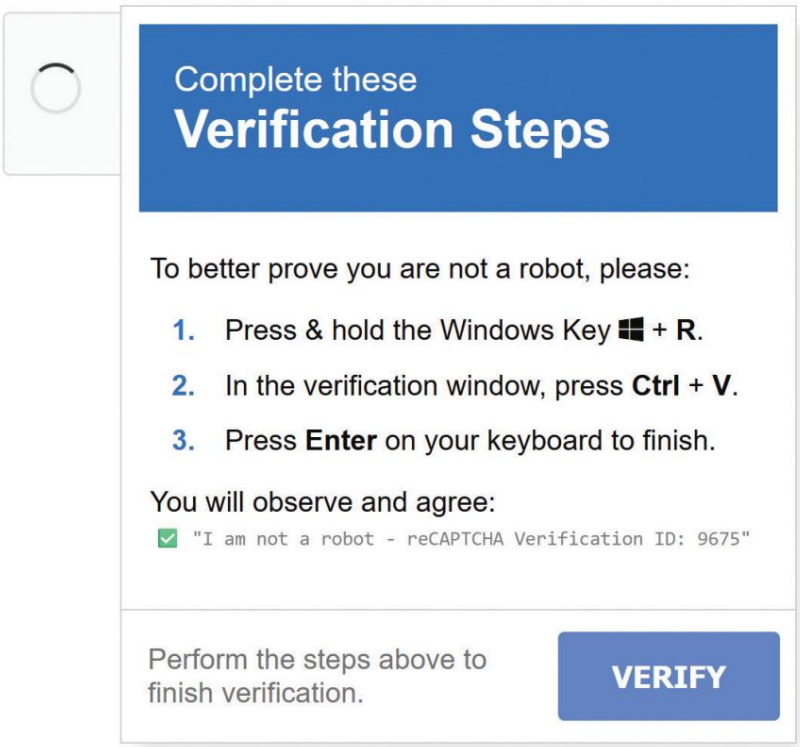
Machine Translated by Google

FAUX CAPTCHA

Un groupe APT appelé Blind Eagle (APT-C-36) a utilisé une technique de phishing ingénieuse. Cette technique d'hameçonnage tente de déployer un logiciel malveillant. Elle se fait passer pour un faux test Google reCAPTCHA de vérification humaine. Cependant, au lieu de simplement cocher une case ou de sélectionner des carrés là où un élément apparaît, elle demande aux utilisateurs d'effectuer une combinaison de touches.

Il repose sur le fait que la victime ignore les raccourcis clavier qu'elle utilise. En coulisses, un script remplit les champs requis.

Le presse-papiers de la victime contient une commande PowerShell. La victime suivra les instructions et ouvrira un menu « Exécuter ». Ils colleront ensuite le code malveillant et l'exécuteront, croyant avoir réussi le test CAPTCHA. John Hammond (@_JohnHammond) Il a republié une preuve de concept basée sur cette technique d'hameçonnage que l'on peut trouver dans son dépôt. Sa version semble plus crédible que celle de Blind Eagle. De plus, il a ajouté un fichier HTA factice qui exécute le code malveillant et affiche un faux message d'erreur pour paraître moins suspect.



Faux défi reCAPTCHA
(source : JohnHammond)

MÉTHODE D'EXÉCUTION

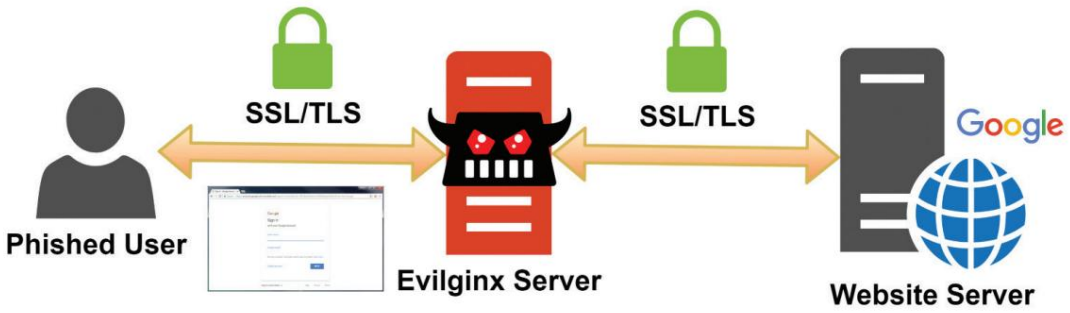
JH utilise mshta pour l'exécution, mais comme nous lançons une commande arbitraire, nous pouvons choisir le programme que nous voulons pour exécuter notre charge utile. Il s'agit en fait d'une exécution de commande à distance ; la seule limite est votre imagination (et le risque de détection).

Machine Translated by Google

LA MÉTHODE PARESSEUSE

L'ATTAQUANT AU MILIEU

Qualifier cette technique de « paresseuse » est probablement trompeur, mais elle exige moins de compétences en programmation. Permettez-nous de vous présenter la technique appelée « Attaque du milieu » ou AITM. Le concept est très similaire à celui des attaques de l'homme du milieu (MITM). L'objectif est de se positionner entre… la victime (ou client) et le serveur, agissant comme un proxy inverse.
Le pirate configure son serveur pour envoyer une requête au site web légitime lorsqu'un client se connecte et lui renvoyer la réponse. Ce processus est totalement transparent pour la victime.



Hameçonnage transparent avec un proxy inverse (source : mrgretzky)

Nous n'aurons pas besoin d'écrire de code HTML ni CSS, car la page sera renvoyée par le site web légitime et chargée par le navigateur de la victime. Pour ce faire, nous devons remplacer dynamiquement chaque domaine que nous souhaitons faire transiter par un proxy dans les requêtes envoyées par le client. Nous pourrions utiliser Evilginx 3.0, développé par Kuba Gretzky (@mrgretzky), Il s'agit d'un outil de phishing AITM. Le plus intéressant, comme indiqué dans le dépôt Evilginx, est qu'il permet de capturer non seulement les identifiants, mais aussi les sessions (cookies, jetons, etc.), contournant ainsi l'authentification multifacteur.

Interface de ligne de commande Evilginx 3.3

Machine Translated by Google

L'utilisation d'Evilginx est relativement simple, et la documentation complète est disponible ici. Voici un bref récapitulatif. Nous déployons le binaire Go compilé statiquement sur un hôte exposé sur Internet. Nous créons des enregistrements DNS pour faire pointer notre domaine de phishing vers notre instance Evilginx, qui servira de serveur web et DNS. Enfin, nous configurons Evilginx à l'aide d'un fichier de configuration dans lequel nous spécifions les domaines, les interfaces d'écoute, etc. (cette configuration est également possible via la ligne de commande). Voilà pour la partie réseau. Il nous faut maintenant créer des « phishlets », c'est-à-dire des fichiers de configuration permettant de cibler des sites web spécifiques afin d'obtenir des liens de phishing.

à envoyer à notre victime.

Les Phishlets sont écrits en YAML et définissent comment l'inverse

Un proxy doit agir pour une cible spécifique. Par exemple, on peut spécifier les domaines à proxyfier à l'aide de la directive ` proxy_hosts` . On peut également effectuer des remplacements de chaînes à la volée grâce aux ` sub_filters`. Les identifiants et les sessions à capturer sont définis respectivement dans les directives `auth_tokens` et `credentials` en spécifiant l'expression régulière à rechercher. Le format phishlet est décrit en détail ici.

Modlishka est un autre outil qui remplit la même fonction et fonctionne de la même manière (proxy inverse) . un outil créé par Piotr Duszyński (@drk1wi). Cependant, cet outil n'est pas maintenu aussi fréquemment qu'Evilginx. De plus, il ne permet pas de capturer facilement les sessions authentifiées autrement que par des cookies, comme par exemple avec un jeton JWT. Il est toutefois possible de contourner ce problème en développant son propre plugin pour Modlishka en Go.

```
± % sudo ./dist/proxy -target login.microsoftonline.com -proxyDomain login.macrosoftonline.com
[Thu Nov  7 10:37:06 2024]  INF  Enabling plugin: autocert v0.1
[Thu Nov  7 10:37:06 2024]  INF  Autocert plugin: Auto-generating login.macrosoftonline.com domain TLS certificate
[Thu Nov  7 10:37:06 2024]  INF  Enabling plugin: control_panel v0.1
[Thu Nov  7 10:37:06 2024]  INF  Enabling plugin: hijack v0.1
[Thu Nov  7 10:37:06 2024]  INF  Enabling plugin: template v0.1
[Thu Nov  7 10:37:06 2024]  INF  Control Panel: SayHello2Modlishka handler registered
[Thu Nov  7 10:37:06 2024]  INF  Control Panel URL: login.macrosoftonline.com/SayHello2Modlishka
[Thu Nov  7 10:37:06 2024]  INF

 _______           __ __ __          __      __
|   |   |.-----.--|  |  |__|.-----.|  |--.|  |--.---.-.
|       ||  _  |  _  |  |  ||__ --||     ||    <|  _  |
|__|_|__||_____|_____|__|__||_____||__|__||__|__|___._|

>>>> "Modlishka" Reverse Proxy started - v.1.1 <<<<
Author: Piotr Duszynski @drk1wi

Listening on [127.0.0.1:443]
Proxying HTTPS [login.microsoftonline.com] via [https://login.macrosoftonline.com]
Listening on [127.0.0.1:80]
Proxying HTTP [login.microsoftonline.com] via [http://login.macrosoftonline.com]
```

Informations de démarrage Modlishka

RÉPONSE SÉLECTIONNÉE

Grâce aux phishlets, nous pouvons utiliser la directive js_inject qui indique au proxy inverse d'ajouter du JavaScript personnalisé à la réponse renvoyée. Pouvoir exécuter du JavaScript dans le navigateur de la victime est un atout considérable : les possibilités sont nombreuses, allant de la modification du style à l'enregistrement des frappes au clavier, et bien plus encore.

Machine Translated by Google

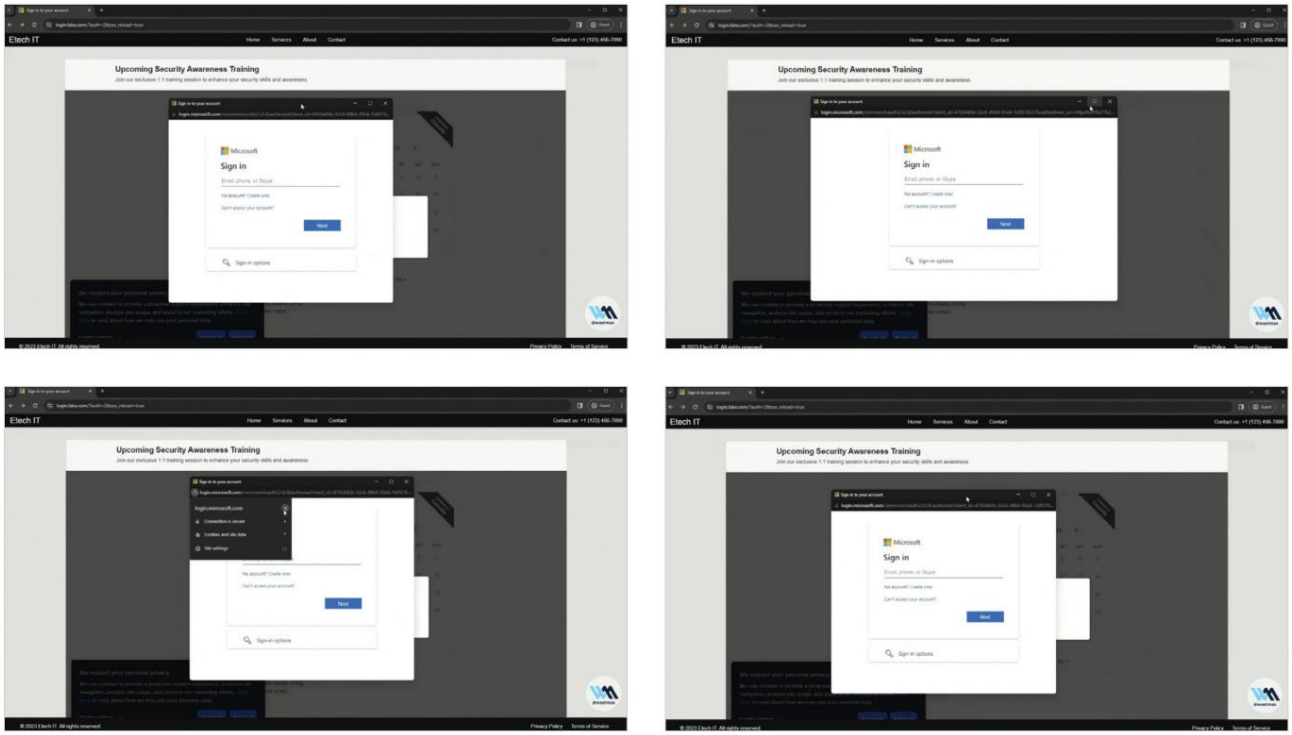
LA MÉTHODE HYBRIDE

SANS CADRE
NAVIGATEUR DANS LE NAVIGATEUR

Nous avons déjà vu plusieurs techniques efficaces, mais présentant des inconvénients. Combiner ces techniques en une technique « hybride » peut en accroître l'efficacité et même contourner certains indicateurs de phishing (IoP). Prenons l'exemple de « Frameless BITB », une technique utilisant une fausse fenêtre de navigateur contenant une véritable page d'authentification proxyfiée. Elle a été développée par Wael Masri (@waelmas01). L'idée derrière cet outil est simple : utiliser la technique BITB avec une fausse URL tout en intégrant une véritable page d'authentification.

BITB utilise des iframes pour charger la page de phishing, mais cette technique est détectée et bloquée par Microsoft, Google et d'autres grands acteurs du web. Pour contourner ce problème, l'effet BITB est obtenu en remplaçant les éléments de la page d'authentification originale par du code HTML personnalisé. Ainsi, il n'est plus nécessaire d'insérer la page dans une iframe : la magie du CSS suffit. Au final, l'utilisateur interagit avec notre page, qui semble s'exécuter en arrière-plan via une URL différente, et affiche la page d'authentification originale, relayée par Evilginx, avec d'importantes modifications de style, comme l'insertion de la fausse URL dans la fenêtre.

Ces éléments renforcent la confiance de l'utilisateur dans notre page d'hameçonnage, lui donnant l'impression que l'ensemble du processus est légitime.



BITB sans cadre en action (source : Wael Masri)

Une vidéo complète Une vidéo illustrant l'attaque et expliquant son fonctionnement est disponible sur YouTube. De plus, toutes les étapes pour reproduire cette preuve de concept sont décrites dans le dépôt de Wael.

BITB TOUT

Cette preuve de concept démontre la possibilité de créer un compte BIBT à partir de la page de connexion de Microsoft. Toutefois, cela est possible avec n'importe quelle autre entreprise. Un travail de développement des modèles adéquats est nécessaire.

Machine Translated by Google

LA MÉTHODE LOURDE

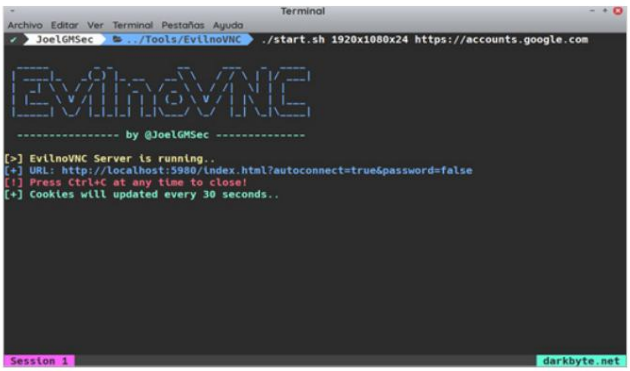
NoVNC

Dans cette section, nous allons examiner certaines techniques de phishing avancées. Pourquoi les qualifions-nous d'avancées ? Tout simplement parce qu'elles nécessitent davantage de ressources de la part de l'attaquant. Jusqu'à présent, nous avons vu des techniques qui chargent des pages de phishing dans le navigateur de la victime, lui laissant ainsi le soin d'effectuer la majeure partie du travail. Nous allons maintenant aborder des techniques qui nous obligent à charger nous-mêmes les pages et à les afficher aux victimes.

Une technique consiste à utiliser noVNC. Ceci a été détaillé par mr.d0x (@mrd0x), Il s'agit du même chercheur en sécurité à l'origine de la technique BITB. Mais selon lui, cette technique avait déjà été mentionnée dans cet article. Dans les deux cas, le concept reste le même : héberger un navigateur web en mode kiosque et en donner l'accès via VNC web.

Puisque la victime utilise notre navigateur pour s'authentifier, l'authentification à deux facteurs est contournée car nous pouvons réutiliser sa session en récupérant le profil du navigateur. Il est important de noter que vous accordez un accès VNC à votre instance ; la victime pourrait donc tenter de sortir du mode kiosque et accéder à d'autres parties de la machine distante. Pour éviter cela, il est nécessaire de renforcer au maximum la sécurité du protocole VNC.

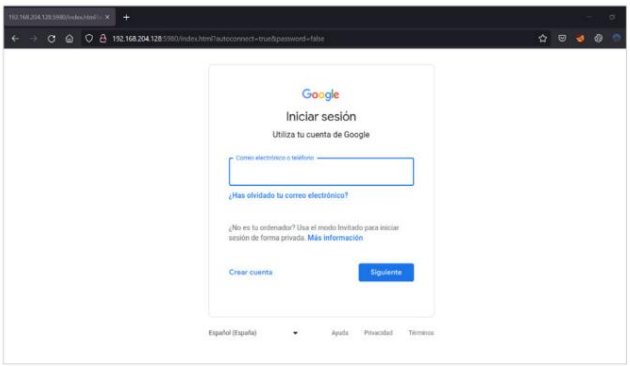
Un excellent projet nommé EvilnoVNC répond aux points mentionnés. Développé par Joel Gamez Molina (@JoelGMSec), Conçu par un expert en cybersécurité (Red Team), cet outil utilise des conteneurs Docker pour isoler le navigateur et limiter les risques de fuite de code. Ce projet a été présenté lors de nombreuses conférences. Joel l'a rendu extrêmement simple d'utilisation : pour tenter de pirater un compte Google, par exemple, exécutez la commande ci-dessous.



EvilnoVNC en cours d'exécution (source : JoelGMSec)

Voilà. Il se chargera de créer le conteneur, d'ouvrir la page web souhaitée dans un navigateur en mode kiosque et même d'adapter la résolution au navigateur de la victime si l'option dynamique est choisie au lieu de 1920x1080x24.

Le profil de la victime est enregistré dans le dossier « Téléchargements », ce qui permet de l'importer dans votre navigateur et de naviguer sur le site web avec la session authentifiée fraîchement piratée.



Vue de la victime lors de l'accès à la page d'hameçonnage (source : JoelGMSec)

RESTER CONNECTÉ

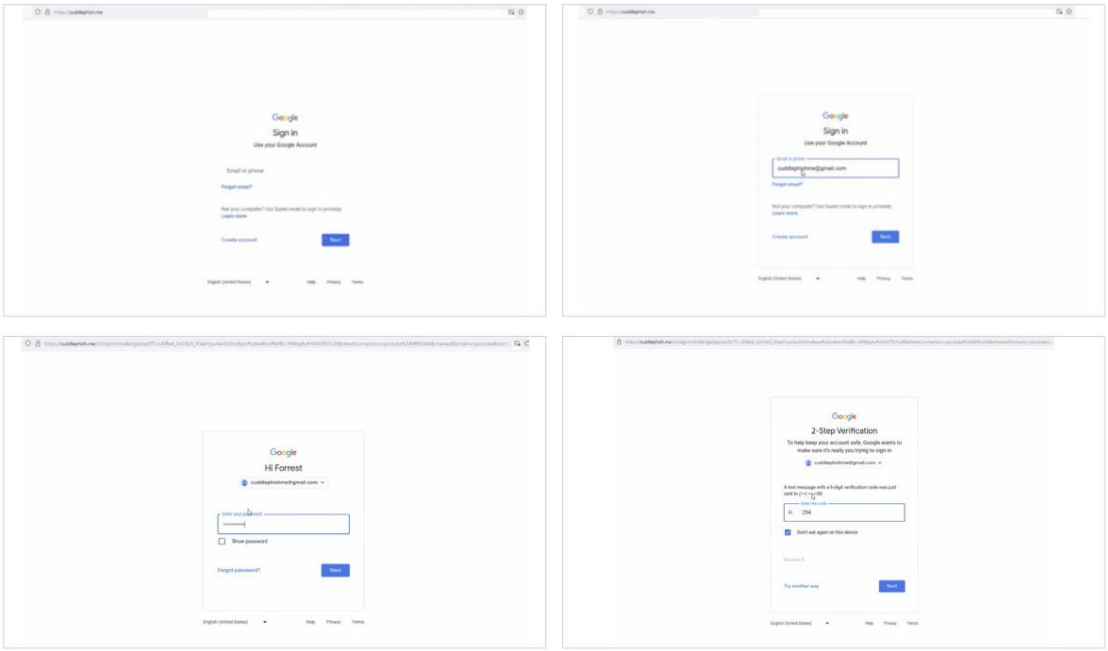
Comme Joel l'indique dans son article de blog, certains cookies de session ne peuvent pas être réutilisés dans un autre navigateur par simple importation. C'est le cas, par exemple, des cookies de Google et de Microsoft. Il est donc nécessaire de maintenir la session active et de ne pas fermer EvilnoVNC.

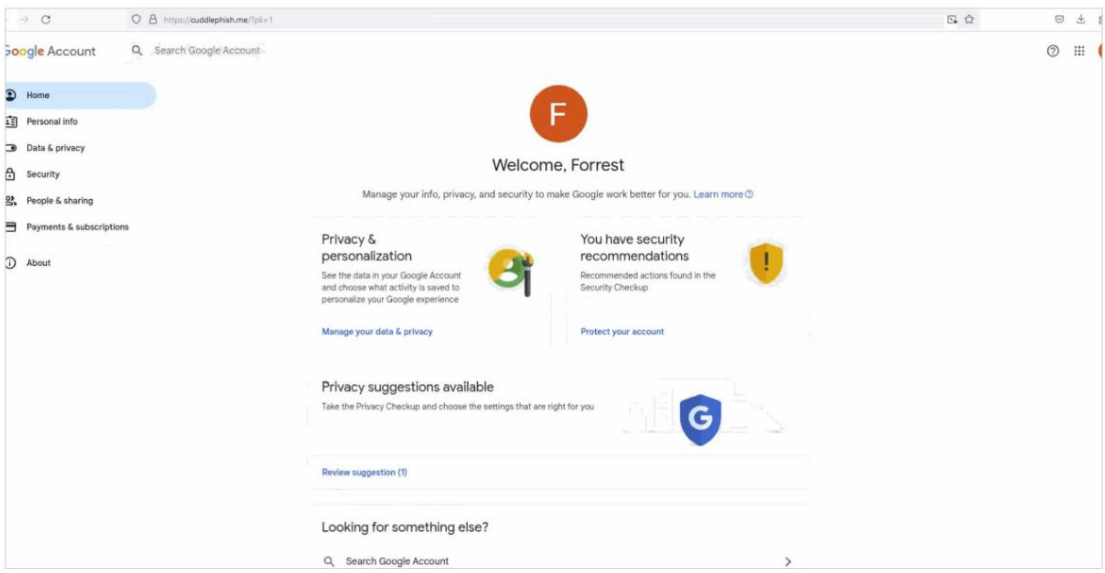
Machine Translated by Google

WebRTC

La catégorie des attaques les plus dangereuses inclut les attaques de phishing, souvent qualifiées d'attaques « navigateur au milieu » (BITM). Après avoir placé un navigateur à l'intérieur d'un autre (BITB), puis nous-mêmes entre le client et le site web (AITM), nous plaçons maintenant un navigateur entre le client et le site web (BITM) que nous tentons d'hameçonner. Mais comment procéder sans donner à la victime accès à la machine distante ? La réponse est simple : en diffusant le contenu du navigateur. La cible n'a pas besoin d'interagir directement avec le navigateur ; nous, si. En effet, les actions de la cible sont reproduites dans le navigateur contrôlé, ce qui nous confère un contrôle bien plus précis sur les entrées de l'utilisateur.

Un outil exceptionnel créé par Forrest Kasler (@FKasler) et nommé CuddlePhish permet de réaliser précisément cette attaque.
Il utilise WebRTC, une technologie conçue spécifiquement pour des fonctionnalités telles que le partage d'écran. Le navigateur s'exécute au sein de Xvfb (X virtual framebuffer), un serveur X11 souvent utilisé pour les tests clients, et est contrôlé par Puppeteer. De cette manière, les actions effectuées par la cible sont relayées vers le navigateur de l'attaquant, donnant l'illusion que la page web affichée est la véritable page web.



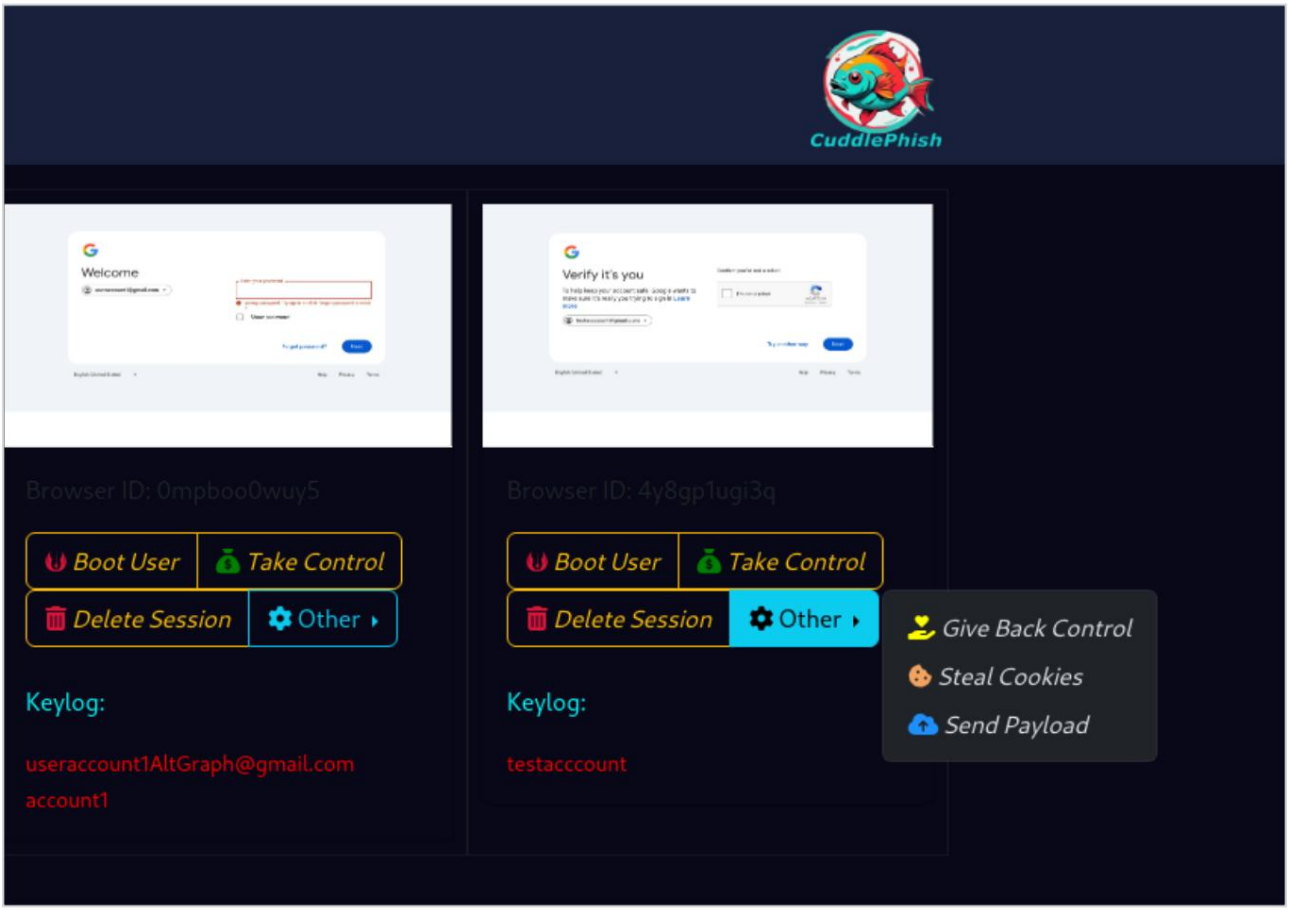


CuddlePhish en action (source : FKasler)

Machine Translated by Google

CuddlePhish possède une section d'administration permettant d'effectuer diverses actions concernant la session. Le pirate peut rediriger l'utilisateur vers une autre page, prendre le contrôle du navigateur, redonner le contrôle à la victime et même…

Une fois la cible authentifiée, l'attaquant récupère les cookies. La fonction « Envoyer une charge utile » est pratique car elle force le téléchargement d'un fichier arbitraire choisi par l'attaquant dans le navigateur de la victime.



Panneau d'administration CuddlePhish

UN REFUGE ÉPOUSTOUFLANT

Comme l'indique Forrest dans son article de blog (et dans la section Dépannage du dépôt Git), certains réseaux peuvent ne plus autoriser STUN en raison des restrictions NAT. Pour contourner ce problème, il est possible de déployer ou de gérer un serveur TURN, de le lier au port 443 et d'ajouter TLS via coTURN. Par défaut, il acceptera les requêtes STUN et TURN ; si STUN est bloqué, CuddlePhish utilisera TURN.

Machine Translated by Google

COMPARAISON

Nous avons vu de nombreuses techniques pouvant être utilisées pour hameçonner des cibles. Chacune de ces techniques présente des avantages, mais aussi des inconvénients. Dans cette section, nous examinerons leurs points forts et leurs points faibles selon plusieurs critères :

- Indépendance du système : Capacité à fonctionner de manière transparente sur tous les principaux systèmes d'exploitation (Windows, MacOS, Linux), quelle que soit la plateforme cible.
- Évolutif : La capacité d'évaluer simultanément de nombreuses cibles tout en maintenant une utilisation efficace des ressources, évitant ainsi les problèmes de ciblage. augmentation exponentielle des besoins en calcul ou en infrastructure.
- Contournement de l'authentification à deux facteurs : possibilité de contourner les mécanismes d'authentification multifacteurs, notamment les notifications push et la vérification par SMS. codes et jetons basés sur une application d'authentification.
- Réaliste : La capacité d'imiter des services et des interfaces utilisateur légitimes, en éliminant les indicateurs familiers souvent enseignés à cibles.
- Compatibilité mobile : Capacité à maintenir l'intégralité des fonctionnalités lors de l'accès via des appareils mobiles.

PAGE HTML

- Avantages : Le HTML est compatible avec tous les navigateurs et systèmes d'exploitation, tandis que le serveur reste léger, même pour un grand nombre de cibles. Nous conservons un contrôle total sur les éléments visuels, permettant une reproduction parfaite de l'application cible légitime et une grande flexibilité sur tous les appareils. Il n'y a pas de connexion directe entre le serveur de phishing et l'application légitime, ce qui réduit le risque de déclenchement.

une détection.

- Inconvénients : Il ne peut pas gérer les mécanismes d'authentification à deux facteurs car il Le site ne communique pas avec le service légitime. Certains indices sont révélateurs, comme une URL qui ne correspond pas au site web officiel, un élément souvent recherché par les personnes visées. Il est également important de rappeler que la création et la maintenance d'une page d'apparence soignée prennent du temps, car elle est susceptible d'évoluer.

NAVIGATEUR DANS LE NAVIGATEUR

- Avantages : Le réalisme est bien supérieur à celui d'une simple page HTML, car nous pouvons falsifier l'intégralité de la barre d'adresse. L'attention de l'utilisateur est ainsi détournée de la page principale vers la fenêtre du navigateur simulée. Les besoins en ressources et en infrastructure sont faibles, les identifiants de journalisation étant les mêmes que pour la page HTML, ce qui facilite la gestion simultanée d'un grand nombre de cibles.
- Inconvénients : Cette approche ne peut pas gérer les mécanismes d'authentification à deux facteurs, car elle ne communique pas avec le service légitime distant. Le style des fenêtres peut varier d'un système d'exploitation à l'autre, et même au sein d'un même système comme Linux, différents styles peuvent exister selon le gestionnaire de bureau et son thème. Cette méthode n'est pas prise en charge sur les appareils mobiles, qui n'utilisent pas de fenêtres.

FAUX CAPTCHA

- Avantages : Un simple serveur HTTP et une page HTML suffisent pour mettre en œuvre cette technique. Cette méthode permet d'exécuter une commande à distance sur le serveur distant.

cible.

- Inconvénients : Cette méthode ne fonctionne actuellement que sous Windows en raison de la combinaison de touches, ce qui la rend spécifique à cette plateforme. Bien qu'il n'existe pas de contournement direct de l'authentification à deux facteurs, un attaquant pourrait utiliser l'exécution de code à distance pour voler une session. Le CAPTCHA affiché à la cible est inhabituel ; aucun défi de ce type n'existe, ce qui augmente les risques de détection si l'utilisateur en est conscient.

Machine Translated by Google

L'ATTAQUANT AU MILIEU

• Avantages : Aucune mise à jour n'est nécessaire pour implémenter cette fonctionnalité. Cette technique est efficace car elle agit comme un proxy inverse entre la victime et l'application distante. Les exigences en ressources et en infrastructure sont également faibles, puisqu'un seul serveur suffit.
peut gérer un grand nombre de cibles. Il fonctionne sur n'importe quel appareil, le rendant totalement indépendant de toute plateforme. En étant situé au centre, tout le trafic passe par le un attaquant, qui peut relayer les phases d'authentification à deux facteurs et Capture de sessions, contournant ainsi cette mesure de sécurité.

• Inconvénients : Les utilisateurs avancés peuvent faire la différence entre un Un domaine légitime et un autre utilisé par un hameçonneur.

BITB SANS CADRE

• Avantages : Cette technique représente une amélioration par rapport à la méthode classique. La méthode BITB, dont elle conserve tous les avantages.
Un avantage supplémentaire par rapport à la méthode originale est la possibilité de contourner l'authentification à deux facteurs.

• Inconvénients : Cette technique présente les mêmes inconvénients que la L'original. Le style de la fenêtre peut ne pas correspondre à la cible. cet environnement est donc un indicateur de phishing.
Cette technique est réservée aux ordinateurs de bureau car les appareils mobiles Ces appareils n'utilisent pas Windows.

noVNC

• Avantages : La victime s'authentifie directement sur le compte du fraudeur. le navigateur via leur propre navigateur, stockant la session sur le du côté de l'attaquant. Cette méthode fonctionne sur n'importe quel appareil, car elle peut Adapter la résolution du navigateur avant d'afficher la page.
Cela s'applique également aux appareils mobiles.

• Inconvénients : Cette technique permet à l'utilisateur d'accéder non seulement au navigateur, mais aussi à l'ensemble de la machine si celle-ci n'est pas suffisamment sécurisée. durci, augmentant le risque de compromission si l'utilisateur trouve une percée. Comme cela nécessite un accès complet au machine, une seule cible peut être hameçonnée par instance, ce qui signifie que les besoins en ressources augmentent rapidement Le nombre de cibles augmente. L'URL sera différente de l'originale, constituant ainsi un indicateur de phishing connu des utilisateurs avertis. victimes.

WebRTC

• Avantages : La victime s'authentifie directement sur le compte du fraudeur. Navigateur via un flux vidéo. Cela permet de contourner l'authentification à deux facteurs. puisque la session est stockée dans le navigateur de l'attaquant.
Les appareils peuvent être pris en charge, y compris les appareils mobiles.

• Inconvénients : Des problèmes d'affichage peuvent survenir en cas de connexion lente, rendant la page web suspecte en raison de son flou.
L'apparence est incorrecte. L'URL ne correspond pas au domaine d'origine.
Bien que cette méthode soit évolutive, les besoins en ressources augmentera rapidement à mesure qu'il générera un conteneurisé Instance de navigateur par victime.

RÉSUMÉ

MÉTHODE	SYSTÈME INDÉPENDANT	ÉVOLUTIF	CONTOURNEMENT DE L'AUTORISATION À DOUBLE FACULTATION	RÉALISTE	MOBILE COMPATIBLE
page HTML	✅	✅	❌	⚠️ (URL incorrecte)	✅
Navigateur dans le navigateur	⚠️ (Incohérence de style de fenêtre)	✅	❌	✅	❌
Faux CAPTCHA	❌	✅	⚠️ (Exécution de la commande)	❌	❌
Attaquant au milieu	✅	✅	✅	⚠️ (URL incorrecte)	✅
BITB sans cadre	⚠️ (Incohérence de style de fenêtre)	✅	✅	✅	❌
noVNC	✅	❌	✅	⚠️ (URL incorrecte)	✅
WebRTC	✅	⚠️ (Tampon de trame virtuel)	✅	⚠️ (URL incorrecte)	✅

Pleinement: ✅ Partiellement: ⚠️ Pas: ❌

Machine Translated by Google

2. INFRASTRUCTURE DE PHISHING

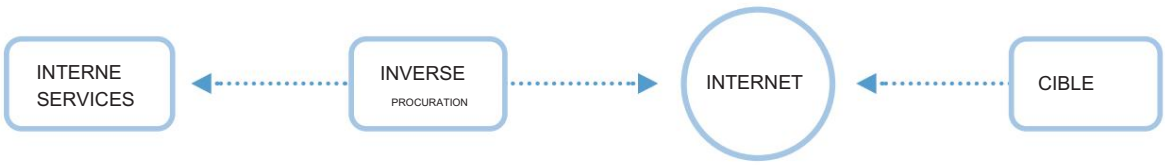
Lorsqu'un pêcheur prend la mer, il a besoin d'un bateau fiable et robuste pour mener à bien sa mission. Il en va de même pour un pirate informatique qui lance une opération : il a besoin d'une infrastructure solide adaptée à ses besoins. Dans cette section, nous examinerons quels sont ces besoins et comment y répondre.

HÉBERGEMENT

Pour mener une campagne de phishing, il suffit généralement d'un simple VPS dans le cloud, avec des spécifications techniques minimales comme 1 vCPU et 2 Go de RAM. Une adresse IP publique à laquelle les cibles peuvent se connecter est également nécessaire. C'est presque tout ce qu'il faut pour exécuter les techniques mentionnées. Cependant, pour une approche plus rigoureuse, où chaque service est séparé et où les données sensibles sont gérées de manière appropriée, l'architecture de l'infrastructure peut être différente.

Premièrement, comme mentionné précédemment, nous traiterons des données sensibles telles que cookies de session valides ou identifiants en clair. Pour réduire

Compte tenu du risque de compromission de ces données par une tierce personne, il est essentiel de les stocker non pas sur le VPS, mais sur une machine dont vous avez un accès complet. Même si ce serveur est sécurisé, il reste exposé sur Internet et peut potentiellement être compromis par des vulnérabilités non connues du public, entraînant ainsi de graves fuites d'informations.
La bonne pratique consisterait à configurer un proxy inverse exposé qui redirigerait les requêtes vers les services internes sur site.
Ces services locaux sont souvent composés d'un outil de phishing, d'un serveur SMTP et d'autres applications utiles que nous détaillerons plus loin.



Proxy inverse exposé uniquement

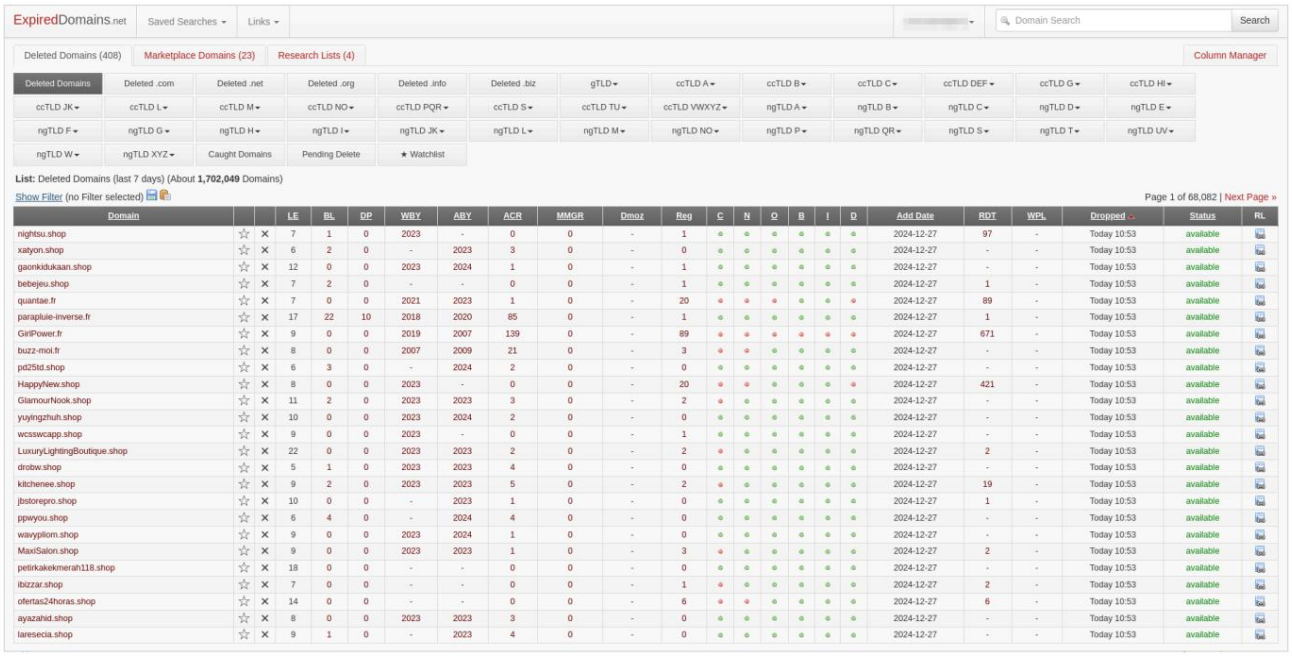
Ensuite, il faut choisir un ou plusieurs noms de domaine correspondant au prétexte. Plusieurs options s'offrent à vous : enregistrer un nouveau domaine, récupérer un domaine expiré ou utiliser des domaines de confiance.
Enregistrer un nouveau domaine correspondant parfaitement au prétexte, incitant les victimes à mordre à l'hameçon sans le moindre doute, peut sembler tentant. Attention cependant : l'ancienneté d'un domaine est un facteur clé pour la détection du phishing. Les domaines récents, enregistrés peu de fois et n'ayant pas encore été repérés sur Internet, peuvent rendre votre tentative de phishing plus suspecte. Les domaines ont besoin de temps et de requêtes pour être catégorisés.
Une bonne catégorisation de vos domaines réduira les risques d'être considéré comme un spam ou bloqué par les serveurs proxy de votre entreprise. Voici une liste pour vérifier la catégorisation de votre domaine :

- Centre de sécurité des sites Trend Micro
- Recherche de filtre Web | FortiGuard
- Filtrage d'URL Palo Alto Networks - Tester un site
- Symantec Sitereview
- URL de vérification McAfee
- Centre de réputation IP et de domaine Talos
- Rapport de transparence de Google

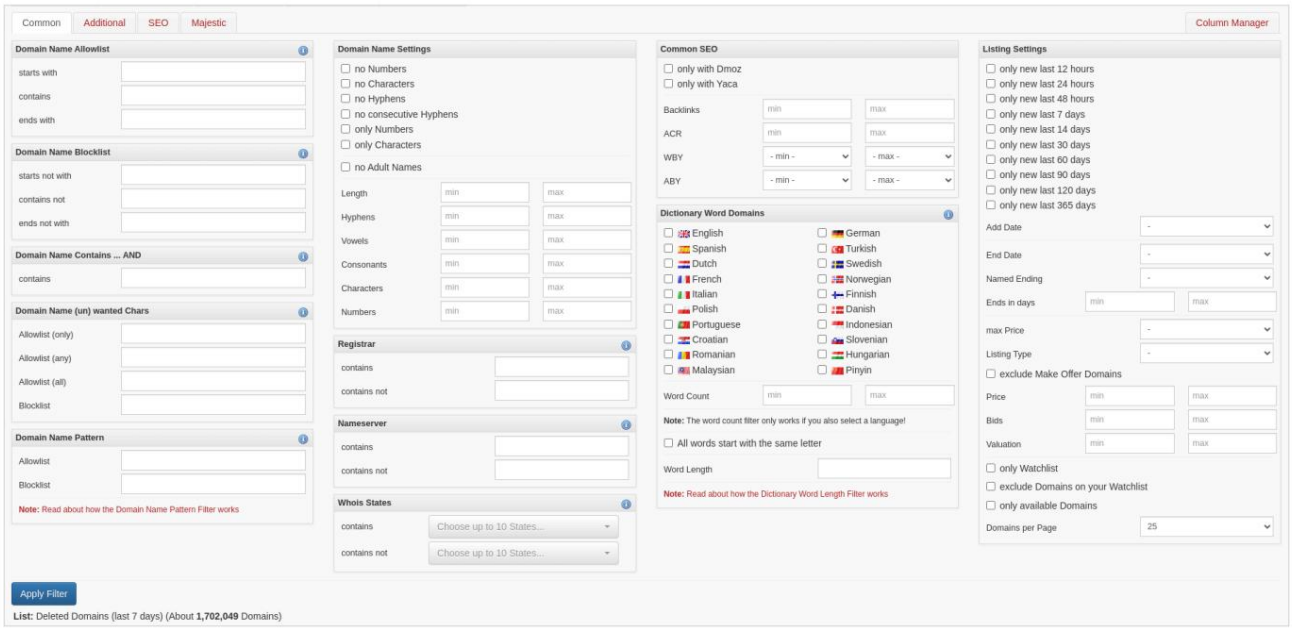
Machine Translated by Google

Si vous souhaitez éviter l'étape de la catégorisation, vous pouvez enregistrer un domaine expiré déjà catégorisé. Le meilleur moyen de trouver un tel domaine est d'utiliser Expired-Domains.net. Ce site web répertorie tous les domaines expirés et vous permet de les rechercher à l'aide de filtres avancés. Vous pouvez

Vous pouvez même créer une liste de surveillance avec des critères spécifiques et recevoir des alertes par e-mail lorsqu'un domaine expire. N'oubliez pas de vérifier la réputation du domaine car certains peuvent déjà l'être catégorisé comme « domaine d'hameçonnage ».



page principale d'ExpiredDomains.net

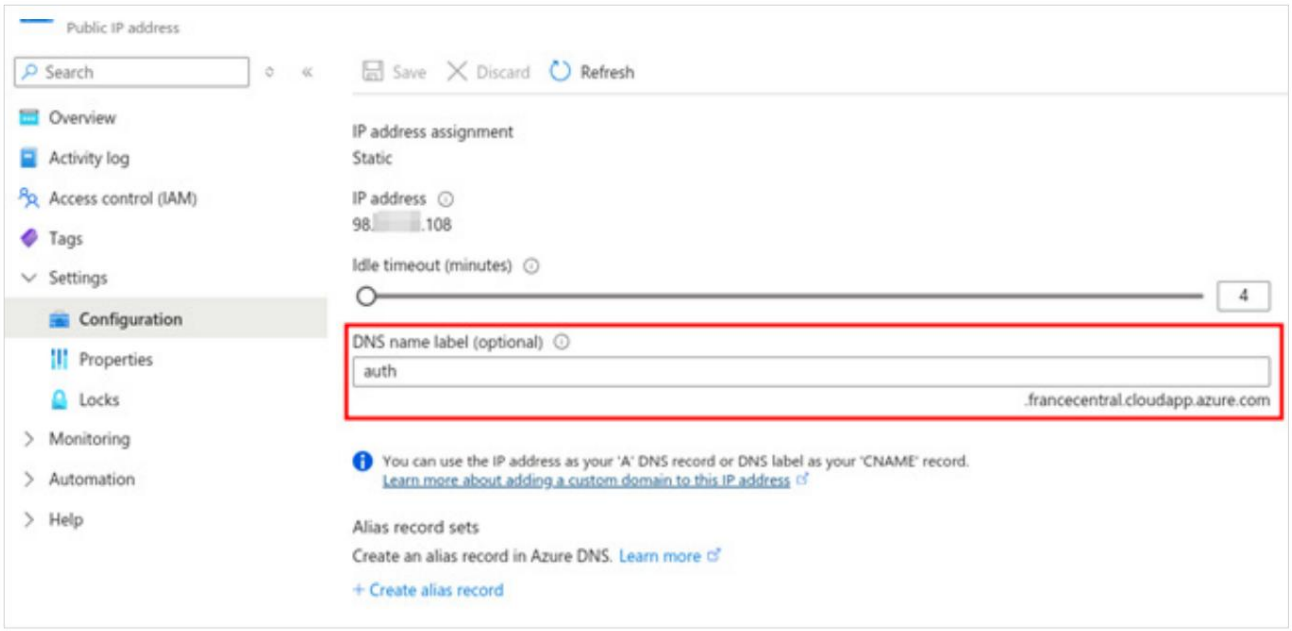


Recherche avancée par filtre sur ExpiredDomains.net

Machine Translated by Google

Vous ne trouvez pas de nom de domaine expiré de qualité ou vous rencontrez des difficultés pour catégoriser votre nouveau domaine ? Empruntons un domaine de confiance. Le principe est simple : utiliser les services cloud pour obtenir un nom de domaine. En effet, la création d'une machine virtuelle sur Azure, par exemple, génère également une adresse IP publique. Azure vous permet de définir une adresse IP publique.

Nous avons ajouté un sous-domaine personnalisé à l'un de leurs domaines. Ci-dessous, nous avons choisi d'ajouter « auth » comme sous-domaine, afin d'inciter une victime à divulguer ses identifiants Azure dans le cadre d'une arnaque.



Configuration du nom DNS pour une adresse IP publique dans Azure

Le résultat final est que vous disposez d'un sous-domaine auth.francecentral.cloudapp.azure.com qui pointe vers votre machine virtuelle.

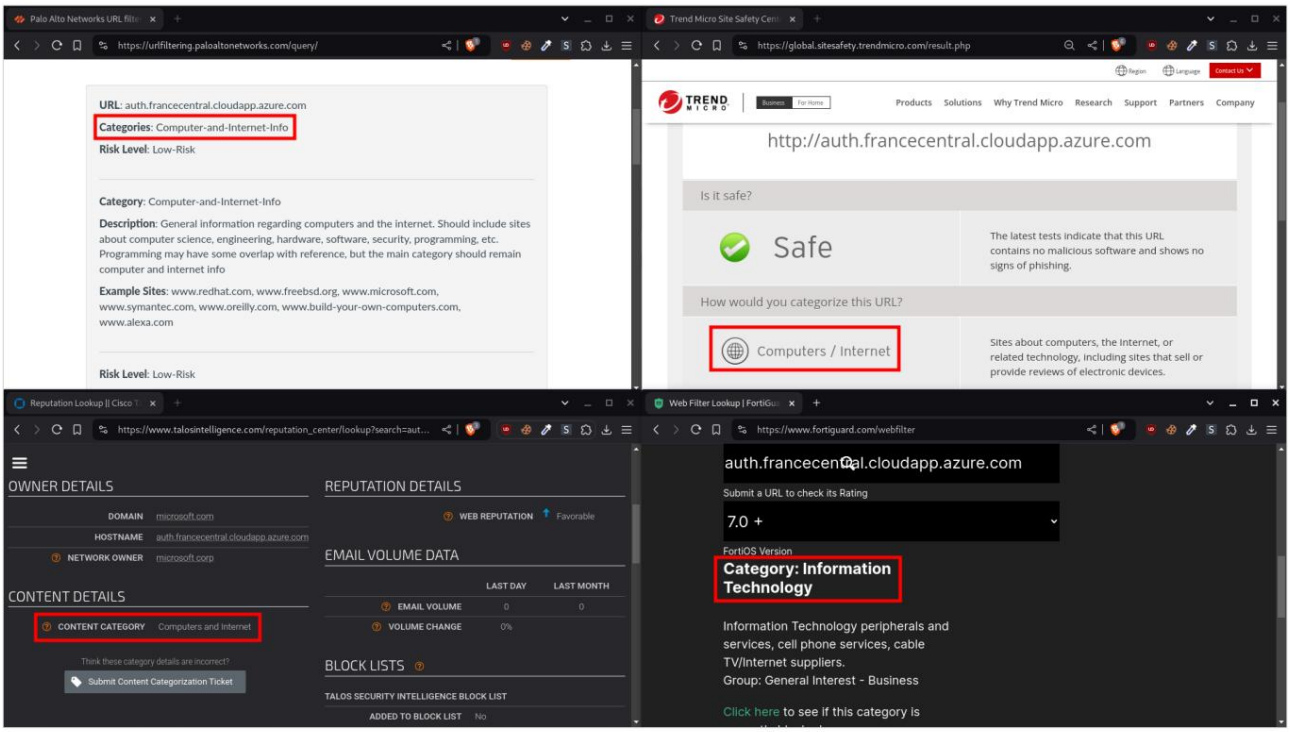
```
-<%>- dig auth.francecentral.cloudapp.azure.com

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> auth.francecentral.cloudapp.azure.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13583
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6da57f65fc3695fa01000000676e8e91699bf3bf0182bea8 (good)
;; QUESTION SECTION:
;auth.francecentral.cloudapp.azure.com. IN A

;; ANSWER SECTION:
auth.francecentral.cloudapp.azure.com. 10 IN A  98.    .108

;; Query time: 20 msec
;; SERVER: 100.100.100.100#53(100.100.100.100) (UDP)
;; WHEN: Fri Dec 27 12:25:05 CET 2024
;; MSG SIZE  rcvd: 110
```

Résolution DNS vers la machine virtuelle du phishing

Machine Translated by Google

Parallèlement, ce sous-domaine bénéficie de la réputation du nom de domaine Microsoft Azure. Il satisfait à tous les critères de vérification que nous avons effectués à l'aide de la liste fournie ci-dessus.

Bien entendu, d'autres grands fournisseurs de services cloud tels qu'Amazon Web Services (AWS) et Google Cloud Platform (GCP) peuvent être utilisés pour obtenir les mêmes résultats.



Bonne catégorisation et bonne réputation lors de plusieurs vérifications

MAUVAIS CODE PUNY

Punycode est une technique utilisée depuis longtemps pour tromper les humains en leur présentant une URL très similaire à l'originale.
Par exemple, un pirate pourrait enregistrer le domaine apple.com, qui ressemble trait pour trait à apple.com. Si vous ne l'avez pas remarqué, toutes les lettres composant le mot « apple » ont été remplacées par des caractères Unicode similaires. Cependant, votre navigateur affichera plutôt xn--80ak6aa92e.com dans la barre d'adresse. De nos jours, cette technique est également détectée par les fournisseurs de messagerie, et les courriels entrants sont presque systématiquement signalés comme indésirables.

Machine Translated by Google

ORCHESTRATION

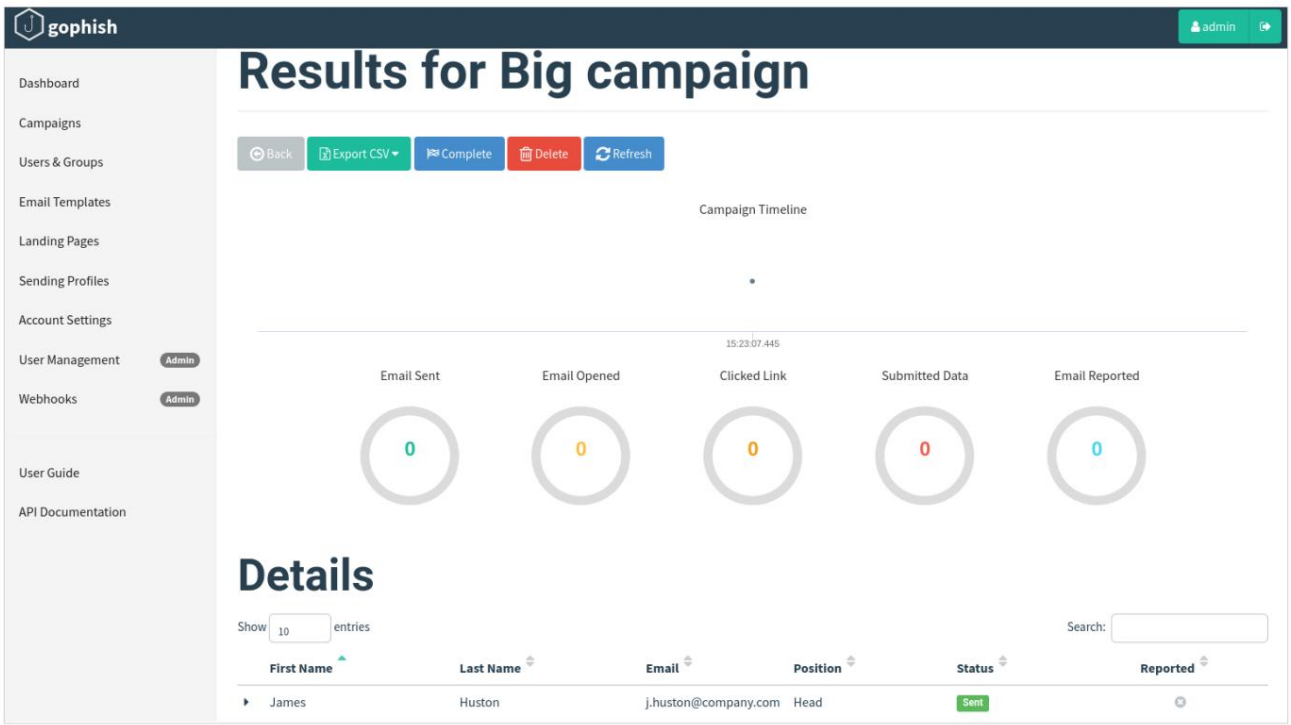
L'orchestration est ici définie comme la coordination entre différents éléments pour produire l'effet désiré. On peut considérer l'orchestration comme le cerveau de l'infrastructure, le point central. Bien qu'il n'existe pas d'outils parfaits pour remplir ce rôle, j'ai trouvé Gophish Gophish se présente comme le candidat idéal. Il se décrit comme « une boîte à outils de phishing open source conçue pour les entreprises et les testeurs d'intrusion ». En effet, il possède plusieurs fonctionnalités intéressantes et est facile à déployer, ce qui en fait le tableau de bord du phishing.

Gophish vous permet de gérer plusieurs campagnes simultanément. Chaque campagne correspond à un ensemble de configurations comprenant les données de lancement, l'URL de phishing, le groupe cible et d'autres informations. Concrètement, vous pouvez créer des groupes de personnes définis par leur nom, prénom, adresse e-mail et fonction, puis les affecter à vos campagnes.

Vous pouvez également configurer des « profils d'envoi », qui correspondent à des identités utilisées comme expéditeurs dans vos campagnes. Le champ « De » peut être personnalisé selon votre message. Les profils d'envoi vous permettent de vous connecter à un relais ou un serveur SMTP à l'aide d'identifiants (ou de manière anonyme) et de l'utiliser pour envoyer des e-mails.
Une fonctionnalité intéressante est la possibilité de vérifier si la campagne fonctionnera correctement en envoyant un e-mail de test.

Gophish permet de créer des modèles d'e-mails et de pages de destination directement dans le navigateur, puis de les importer. Il est possible d'utiliser des champs vides, comme le nom ou l'adresse e-mail du destinataire, pour rendre les e-mails personnalisés plus convaincants. La page de destination peut être vide et son URL peut être spécifiée lors de la création du modèle d'e-mail.

Ainsi, Gophish peut être utilisé pour envoyer et suivre les résultats d'une campagne tout en employant d'autres techniques de phishing.



Bonne catégorisation et bonne réputation lors de plusieurs vérifications

Le processus typique de création d'une campagne de phishing est le suivant : 1. Ajouter ou importer des groupes de cibles ; 2. Créer ou importer un modèle d'e-mail ; 3. Créer une page de destination (s'applique uniquement à la campagne classique). Page HTML) 4. Créez un profil d'envoi et testez l'envoi d'un e-mail. 5. Créez et planifiez une campagne. 6. Réalisez le profit.

INTÉGRATION SANS EFFECTIF

Kuba Gretzky a créé une version dérivée de Gophish qui s'intègre à son outil Evilginx. Cela permet aux auteurs d'attaques de phishing de profiter du contournement de l'authentification à deux facteurs offert par Evilginx, tout en conservant les fonctionnalités de gestion et de suivi des campagnes de Gophish. Il est même possible d'utiliser les espaces réservés présents dans le modèle Gophish avec la fonctionnalité js_inject d'Evilginx , qui permet d'injecter du JavaScript personnalisé dans les réponses du proxy.

Machine Translated by Google

PROTECTION

Mettre en place une infrastructure derrière un proxy inverse est un bon point de départ, mais insuffisant. Il est nécessaire de la renforcer. L'objectif est de contrôler au maximum les visiteurs de vos pages d'hameçonnage, car le lien figurera dans l'e-mail envoyé à votre cible. Avant d'atteindre le destinataire, ce lien sera analysé à plusieurs reprises par différents mécanismes de détection, tels que les environnements de test (sandboxes), qui tentent d'intercepter les e-mails indésirables avant qu'ils n'arrivent dans la boîte de réception.

Un hameçonneur peut employer les mêmes méthodes qu'un site web légitime pour protéger sa page contre les robots et les accès indésirables.

Une protection élémentaire pouvant être mise en œuvre au niveau du proxy inverse consiste à établir une liste blanche des visiteurs en fonction de leur agent utilisateur et de leur adresse IP. Ceci peut être réalisé grâce à la configuration Nginx.

Vous pouvez effectuer une correspondance (insensible à la casse) sur l'opérateur Nous `~*` user-agent, comme dans l'exemple ci-dessous. Cela bloquera pouvons bloquer tout visiteur dont l'agent utilisateur contient « googlebot », « curl » ou « python ». À l'inverse, nous pouvons autoriser uniquement certains agents utilisateurs identifiés comme étant ceux utilisés par la cible. Dans l'exemple ci-dessous, si la cible n'utilise ni Firefox, ni Chrome, ni Safari, elle sera bloquée.

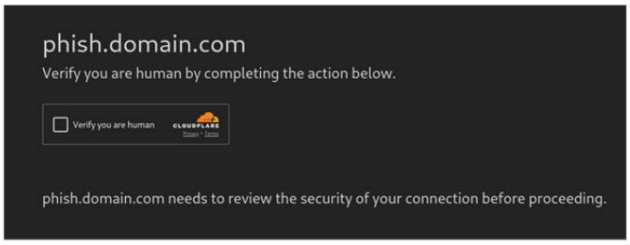
```
emplacement / {
    # si contient l'un des éléments suivants, bloquer
    si ($http_user_agent ~* «googlebot|curl|python») {
        retour 403 ;
    }

    # Si ne contient pas l'un des éléments suivants, bloquer
    si ($http_user_agent !~* «gecko|chrome|applewebkit») {
        retour 403 ;
    }
}
```

Pour autoriser ou bloquer les requêtes provenant d'adresses IP spécifiques, nous pouvons utiliser le module ngx_http_access_module de Nginx. Par exemple, si vous souhaitez autoriser uniquement les connexions provenant de France, vous pouvez ajouter cette liste à votre configuration Nginx comme indiqué ci-dessous.

```
emplacement / {
    autoriser 1.179.112.0/20 ;
    autoriser 2.3.0.0/16 ;
    autoriser 2.4.0.0/14 ;
    [...]
    nier tout ;
}
```

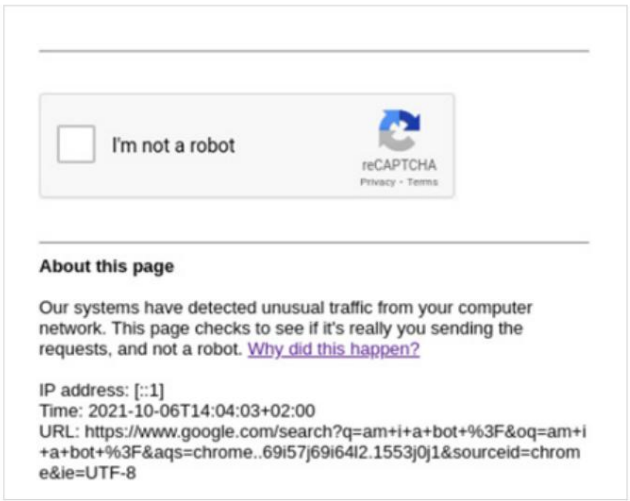
Machine Translated by Google

Ces protections sont très rudimentaires, car elles peuvent être facilement contournées en modifiant l'agent utilisateur et en utilisant un proxy pour les requêtes. Pour les améliorer, nous pouvons faire appel à des fournisseurs externes afin de lutter contre les bots. Par exemple, un pirate peut utiliser Cloudflare comme façade de sa page. Une offre gratuite propose d'excellentes fonctionnalités telles qu'un certificat SSL (plus fiable que Let's Encrypt, souvent détourné), un pare-feu applicatif web et une protection simple contre les bots. En activant le « Mode Attaque », Cloudflare affiche une page d'avertissement avec sa solution alternative de CAPTCHA Turnstile, obligeant l'utilisateur à résoudre le problème avant de poursuivre.



Page Web protégée par le « Mode Attaque »

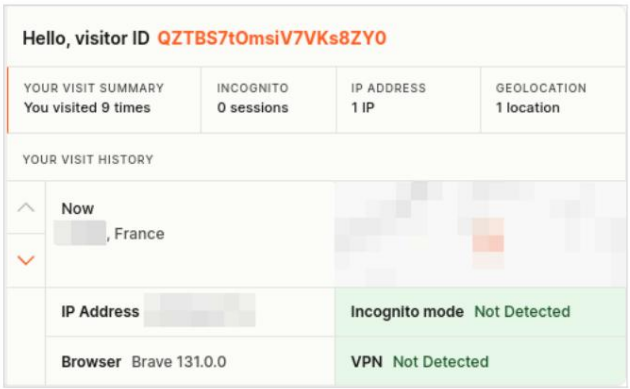
Une autre option consiste à utiliser Google reCAPTCHA et à créer votre propre page qui redirigera l'utilisateur vers la page finale s'il réussit le test. Une bonne approche consiste à imiter la fameuse page « Trafic inhabituel » de Google. Les utilisateurs connaissent peut-être déjà cette page simple qui apparaît parfois, ce qui renforce leur confiance dans l'appât.



Fausse page de trafic inhabituel de Google

Si, en tant que pirate informatique, nous suivons cette voie et commençons à construire notre propre mécanisme de redirection pour permettre à des utilisateurs spécifiques d'accéder à la page, nous n'aurons aucune limite en termes de granularité. Par exemple, nous pourrions autoriser la cible à accéder à la page de phishing une seule fois, toute tentative ultérieure étant bloquée. Ou, sans être aussi restrictif, autoriser l'accès à la page uniquement aux visiteurs identifiés qui ne sont pas des robots. Une solution consiste à utiliser

Empreinte digitale, Un script collecte des indicateurs et les évalue à l'aide de « Signaux intelligents ». Ainsi, nous pourrions autoriser l'accès à la page au premier visiteur humain, en associant l'identifiant généré par Fingerprint à un identifiant unique inséré dans l'URL. Un autre visiteur tentant d'accéder à la même URL serait bloqué, car les deux identifiants ne correspondraient pas.



Identifiant unique généré par empreinte digitale

SIGNALISATION INTELLIGENTE

Fingerprint ne se contente pas d'attribuer un identifiant unique ou de détecter les robots ; il analyse également les données du navigateur afin d'établir un profil précis du visiteur. De cette manière, Fingerprint peut détecter plusieurs informations pertinentes permettant de déterminer si un visiteur constitue ou non une cible légitime.

- Machine virtuelle
- Appareil Android émulé
- Mode navigation privée
- Usurpation d'agent utilisateur

Machine Translated by Google

3. MODES DE LIVRAISON

Maintenant que nous avons vu comment un pirate informatique peut mettre en place et sécuriser son infrastructure, examinons de plus près comment il parvient à introduire des courriels malveillants dans la boîte de réception de sa cible. Cette section détaillera les différentes méthodes utilisées par un pirate informatique pour envoyer des courriels d'hameçonnage convaincants, incitant la cible à cliquer sur le lien et à se faire piéger.

EXPÉDITEUR

Bien sûr, un pirate informatique pourrait consacrer du temps à configurer un serveur SMTP, à renforcer sa sécurité et à gagner la confiance des internautes. Cependant, cette approche est chronophage et peut parfois échouer. Pour contourner les filtres de réputation et garantir une délivrabilité optimale, les attaquants se tournent souvent vers des solutions éprouvées, déjà en place et opérationnelles.

Pourquoi s'embêter à configurer un serveur relais SMTP alors qu'il en existe tant d'autres disponibles sur Internet ? L'une des raisons pourrait être d'usurper le domaine cible. Cette stratégie consiste à s'approprier le domaine cible si certains enregistrements DNS sont manquants. Spoofy est un excellent outil pour détecter ce type de configuration erronée. Il vérifie les enregistrements DNS et vous indique si un domaine est vulnérable à l'usurpation d'identité en fonction des réponses. Vous pouvez également consulter ce tableau. Il est important de savoir si un domaine est falsifiable. Si c'est le cas, il y a de fortes chances que votre courriel malveillant arrive dans la boîte de réception de la victime si vous l'envoyez en prétendant provenir du même domaine.

```
└> ./spoofy.py -d visualstudio.com
[*] Domain: visualstudio.com
[*] Is subdomain: False
[*] DNS Server: 1.1.1.1
[*] SPF record: v=spf1 -all
[*] SPF all record: -all
[*] SPF DNS query count: 0
[?] No DMARC record found.
[+] Spoofing possible for visualstudio.com.
```

Domaine vulnérable identifié par Spoofy

Autrement, nous pourrions exploiter certains serveurs ouverts ou SMTP disponibles sur Internet. C'est précisément ce que font les auteurs de phishing. Ils profitent du fait que les serveurs peuvent être mal configurés, sans authentification adéquate par exemple, pour mener leurs campagnes. Il est important de noter que ces serveurs peuvent avoir déjà été utilisés lors de campagnes précédentes, ce qui peut nuire à leur réputation.

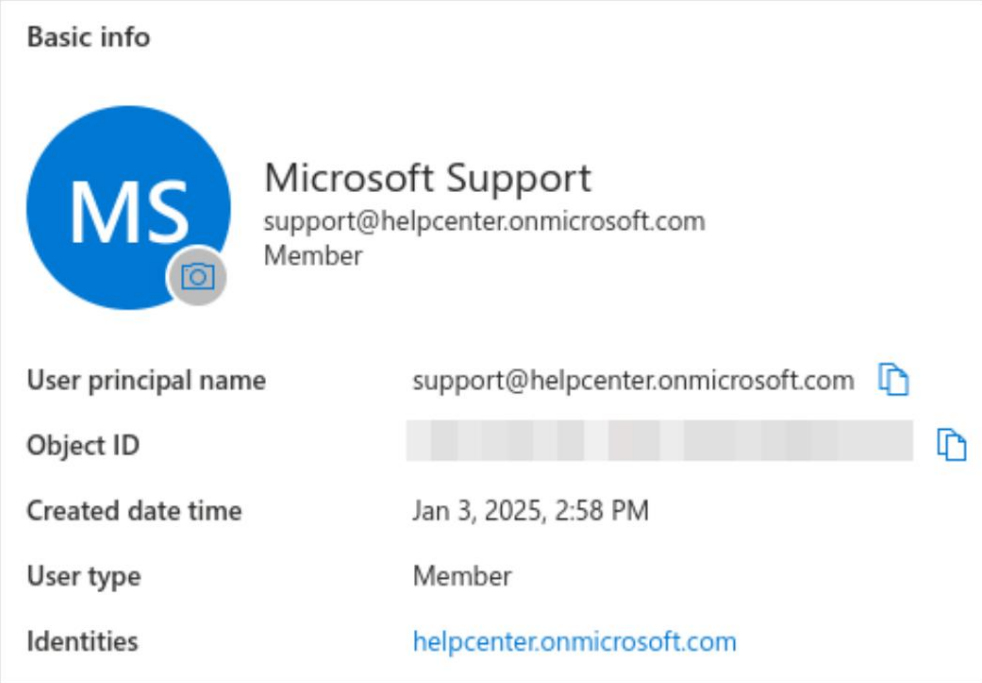
Pour surmonter ce problème, nous pouvons nous tourner vers des services de marketing et d'envoi de courriels tiers tels que Mailchimp. Mailjet ou SendGrid. Ces plateformes sont souvent détournées car elles fournissent une infrastructure d'envoi fiable que les auteurs d'hameçonnage peuvent associer à leurs propres domaines soigneusement sélectionnés. De plus, ces services offrent des fonctionnalités utiles aux attaquants, comme la possibilité de vérifier la bonne réception des e-mails. La plupart des services d'envoi d'e-mails tiers proposent une formule gratuite permettant d'envoyer des milliers d'e-mails par mois. Vous trouverez à droite un tableau comparatif des formules gratuites :

PLATE-FORME	COURRIELS PAR JOUR	COURRIELS PAR MOIS	NOMBRE DE CONTACTS
SendGrid	100	3000	∞
Mailjet	200	6000	1500
Mailchimp	500	1000	500
Brevo	∞	9000	2000
Expéditeur	∞	15000	2500

Machine Translated by Google

Les fournisseurs de services cloud sont devenus un vecteur privilégié pour les auteurs d'hameçonnage, car ils proposent des services de messagerie électronique reposant sur des infrastructures de confiance. Par exemple, Microsoft Entra ID (Azure) fournit des domaines au format <tenant>.onmicrosoft.com, ce qui peut s'avérer particulièrement efficace pour l'ingénierie sociale.
Comme ces courriels proviennent de l'infrastructure de Microsoft, ils paraissent automatiquement plus fiables et sont plus

Ce type de courriel a de fortes chances d'atterrir dans la boîte de réception. Lorsqu'un domaine Microsoft figure dans l'adresse de l'expéditeur, les destinataires sont plus enclins à baisser leur garde et à faire confiance au contenu. Nous pourrions, par exemple, nous faire passer pour l'équipe de support Microsoft en créant le compte « helpcenter » et en nous nommant « support », ce qui amènerait notre cible à croire qu'il s'agit d'un courriel officiel.



faux compte de support Microsoft

Vous souhaitez encore plus de sécurité ? L'usurpation d'identité par courriel professionnel (BEC) pousse le phishing à un tout autre niveau. Au lieu de créer de faux comptes ou d'usurper des identités, les phishing utilisent l'accès à des comptes de messagerie d'entreprise légitimes qu'ils ont déjà compromis par phishing ou attaques par force brute. Utilisés pour du phishing interne, ces courriels sont assurés d'atteindre votre boîte de réception avec un niveau de confiance extrêmement élevé. Même lorsqu'ils ciblent des utilisateurs externes, ces comptes compromis bénéficient de la réputation établie de l'entreprise, de ses relations existantes et de son nom de domaine légitime, garantissant ainsi que leurs courriels parviendront à destination.

Bien que ce ne soit pas un phénomène nouveau, l'utilisation abusive des formulaires de contact refait surface et est plus répandue que jamais. Les auteurs d'hameçonnage exploitent ces formulaires de deux manières : soit lors de l'envoi du formulaire, l'adresse électronique indiquée reçoit une copie du message, soit le message n'est reçu que par l'entreprise ciblée. Dans les deux cas, l'attaquant détourne un service légitime pour envoyer des liens malveillants à ses victimes.

Il est intéressant de noter que les chances que le message soit délivré sont très élevées, et il n'y a probablement aucune limite au nombre de messages que le fraudeur souhaite envoyer.

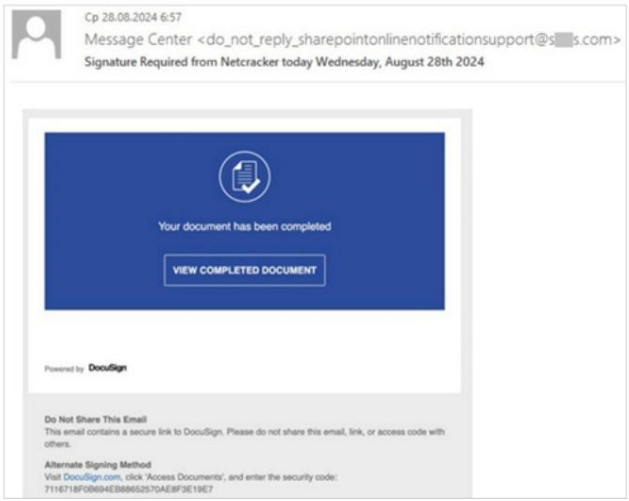
PIRATAGE À PIRATAGE

Pour un pirate informatique souhaitant atteindre son objectif, une approche furtive consiste à cibler d'abord une personne plus vulnérable et moins vigilante. Ensuite, en utilisant le compte de la victime, il peut atteindre des cibles plus conscientes des attaques externes, mais qui ne se méfient pas des courriels provenant de leurs collègues. Ce qui rend cette technique particulièrement dangereuse, c'est le nombre d'indicateurs de phishing qu'elle permet de dissimuler, à condition que le prétexte ne soit pas trompeur.

Machine Translated by Google

APPARENCE DES E-MAILS

Nous avons vu comment acheminer l'e-mail jusqu'à sa cible et comment maximiser ses chances d'arriver dans sa boîte de réception plutôt que dans le dossier spam. Si la cible n'a pas remarqué l'expéditeur ou est convaincue de sa légitimité, il faut maintenant la convaincre par l'apparence même de l'e-mail. Nous devrons exploiter plusieurs biais cognitifs pour l'inciter à continuer de croire à l'authenticité de l'expéditeur.



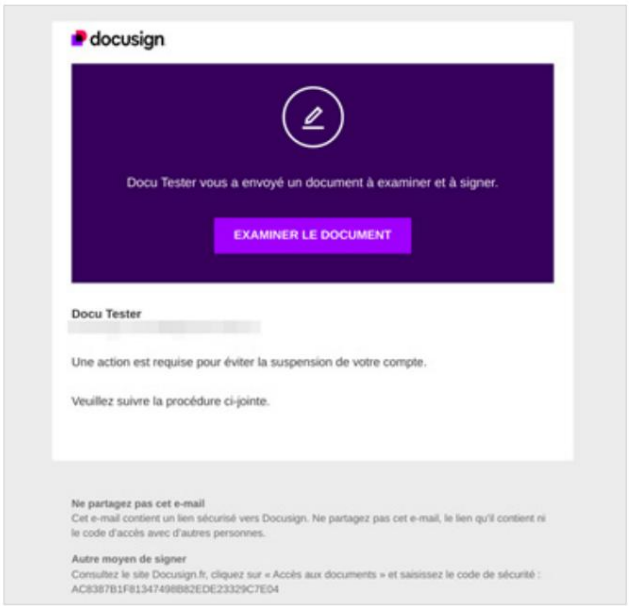
Courriel d'hameçonnage imitant DocuSign (source : Kaspersky)

Un pirate informatique copiera la mise en page de l'e-mail pour exploiter la « familiarité visuelle ». En tant qu'êtres humains, nous sommes sensibles à l'« effet de simple exposition », un biais qui explique notre préférence naturelle pour ce que nous avons déjà vu. Les attaquants s'appuient naturellement sur cet effet lors de la conception de leurs e-mails, car il déclenche automatiquement une première réaction positive de la part de la cible. La mise en page peut comprendre un logo, un titre, un sous-titre, du texte, des images et un pied de page. Ce sont des éléments courants présents dans la plupart des e-mails automatisés, comme ceux envoyés par Microsoft ou DocuSign. Récemment, ce dernier a été utilisé dans de nombreuses campagnes de phishing thématiques, reproduisant le même e-mail lorsqu'une personne partage un document.

toi.

L'usurpation d'identité de marque consiste à reproduire certains schémas et détails souvent observés et reconnus par la victime potentielle. Les auteurs d'hameçonnage exploitent ce biais de constance en répondant aux attentes que la cible a développées au fil du temps. Par exemple, la capture d'écran ci-dessus d'un courriel d'hameçonnage reprend certains éléments clés du courriel ci-dessous, qui est un courriel légitime reçu de DocuSign (les éléments graphiques ont été récemment mis à jour). La structure est identique : une icône centrée dans une bannière colorée avec une invitation à…

On peut prendre un clic droit et afficher un bouton, puis en dessous l'expéditeur du document et son message, et enfin un pied de page classique avec des informations et des instructions.



Courriel original de DocuSign

Logo HTML

Les images, et notamment les logos d'entreprise, sont utilisées pour imiter les marques et renforcer la crédibilité des e-mails. Cependant, la plupart des clients de messagerie bloquent le contenu distant ou les images encodées en base64. Une solution pour contourner cette restriction et conserver les avantages des images consiste à recréer le logo uniquement en utilisant HTML et CSS. Par exemple, ce gist Il est possible de l'utiliser pour créer un logo Microsoft. Il convient de tenir compte de la compatibilité CSS entre les différents fournisseurs et clients de messagerie ; il est donc toujours conseillé de vérifier le rendu dans un environnement identique à celui de la cible.

Machine Translated by Google

Notre perception de la légitimité d'un courriel peut être influencée par un biais d'autorité, car nous avons tendance à moins remettre en question les figures d'autorité. En règle générale, un courriel provenant d'un responsable ou d'une personne équivalente, portant la même signature que le courriel original, paraîtra plus convaincant et laissera moins de place au doute quant à la légitimité de l'action. Ce même phénomène peut se produire lorsqu'un pseudo-administrateur informatique vous demande de « changer votre mot de passe conformément à la nouvelle politique », car cette demande est présentée comme une mesure de « sécurité » et vous êtes censé vous y conformer.

Enfin, les auteurs de phishing tenteront d'exercer une pression pour obtenir une réponse plus rapide, réduisant ainsi votre temps de réflexion et pouvant vous amener à agir de manière imprévue. C'est ce qu'on appelle le « biais d'urgence ». Bien que ce biais soit

Souvent exprimé par écrit sous forme de prétexte, le prétexte peut être renforcé par des éléments visuels. Par exemple, reprenons l'exemple du faux administrateur informatique : le courriel contient des instructions précises, une date limite et des conséquences en cas de non-exécution. Tous ces éléments sont mis en évidence en gras ou en couleur. Le choix de la police est également crucial pour attirer l'attention. Voici un exemple simple de prétexte, avec des éléments mis en évidence, exploitant le biais d'urgence :

Dear [Employee Name],

Our security monitoring system has detected that your current password does not comply with the new enhanced password policy being implemented across all company systems.

Your account access will be **automatically suspended** if no action is taken before **20th January 2025**.

To maintain uninterrupted access to company resources, please update your password immediately by following the usual procedure described below:

1. Login on the company **portal**
2. Enter the new password
3. Click update button
4. Wait for confirmation message (important !)

For your information, the Updated Password Policy requirements are the following:

- Minimum *14 characters*
- At least *1 lower and 1 capital letter* required
- At least *1 number* required
- At least *1 special character* required
- Must not match previous 5 passwords

This is part of our ongoing security enhancement initiative outlined in Policy Document SEC-2025-01.

IT Security Team
Information Technology Department
Company Name
Reference: SEC-UPD-25-1103

Courriel d'hameçonnage exploitant plusieurs biais

Machine Translated by Google

LIEN

Le lien est le dernier élément qui doit être soigneusement conçu. Dans cette section, nous explorerons différentes techniques utilisées par les auteurs de phishing pour rendre leurs liens malveillants plus crédibles et contourner les mesures de sécurité telles que les filtres anti-spam.

Les raccourcisseurs d'URL sont des services qui transforment une URL longue en une version plus courte. Initialement conçus pour faciliter le partage de liens, notamment sur les plateformes à limite de caractères, ils sont aujourd'hui fréquemment utilisés à des fins d'hameçonnage. Parmi les raccourcisseurs d'URL populaires proposant une formule gratuite, on peut citer Bitly. T.ly, Rebrandly (ou version gratuite), Court.io, Cutt.ly.

Ces services offrent plusieurs avantages clés pour les campagnes d'hameçonnage. Le principal atout réside dans la possibilité d'utiliser des domaines de confiance bénéficiant d'une excellente réputation (testée à l'aide des outils de catégorisation mentionnés précédemment) tout en conservant des URL courtes et claires. De nombreux services proposent également des options de personnalisation des sous-domaines et des chemins d'accès, permettant ainsi aux auteurs d'hameçonnage de créer des liens parfaitement en phase avec leur prétexte, tels que :

- https://bit.ly/office-365-sign-in
- https://t.ly/account-microsoftonline-com
- https://rebrand.ly/login-microsoftonline-com
- https://microsoftonline.short.gy/login
- https://cutt.ly/sign-in-to-continue

L'association d'un nom de domaine réputé et d'un chemin d'accès soigneusement conçu rend ces URL raccourcies particulièrement efficaces dans les campagnes d'hameçonnage. Lorsqu'une cible voit un nom de domaine raccourci familier suivi de mots-clés pertinents, elle sera plus encline à faire confiance au lien.

Les vulnérabilités de type Cross-Site Scripting (XSS) et Open Redirect représentent une opportunité majeure pour les auteurs d'hameçonnage. Ces vulnérabilités surviennent lorsqu'un site web accepte, sans validation adéquate, une entrée utilisateur spécifiant une URL de redirection. Les attaquants exploitent ces failles pour rendre leurs liens malveillants plus crédibles en utilisant des domaines de confiance.

Cette technique est particulièrement efficace car le domaine initial est légitime et digne de confiance, ce qui procure immédiatement un sentiment de sécurité à la victime. La redirection s'effectue automatiquement, ne laissant que peu de temps aux utilisateurs pour remarquer le changement de domaine, car ils sont transférés sans transition vers le site malveillant. La plupart des utilisateurs ont pris l'habitude de ne vérifier que le début d'une URL pour en vérifier la légitimité, ce qui rend les redirections ouvertes particulièrement trompeuses.

Prenons un exemple concret. Le chercheur en sécurité Jip (@jipisback) partagé récemment sur X Voici une méthode pour détourner la fonction de redirection de YouTube. Voici les étapes décrites dans l'article :

1. Trouvez une vidéo YouTube dont la description contient des liens externes.
2. Copiez l'URL de redirection, qui devrait ressembler à ceci : https://www.youtube.com/redirect?event=video_description&redir_token=TOKEN&q=URL&v=VIDEO_ID
3. Modifiez le paramètre q pour qu'il pointe vers votre site.
4. Profit

Nous avons créé un exemple qui redirige vers le site web de Quarkslab : lien

```
https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbmhkMT-luUmZ4VVhPMk84TXdjTDN1NEFaVFhnZ3xBQ3Jtc0tsRkdrdlR5djhhSk1Uc3JxcFUzcXpETzkxT-2dUWnFIOGp-sYmExR3lDWHB6Q0ZMNFVhblILYnM2WERDbFpOSDNmZmdkTkVBa0VFQnh-sM2taWDZSMVlaUEJyZTZaY1JxaGpDMk1kdTk2X2IzNIIIcHZ2Yw&q=https%253A%252F%252Fwww%252Equarkslab%252Ecom%252Fpentest%252Dproactive%252Dthreat%252Dmitigation%252F
```

CHAÎNE DE REDIRECTION

Lors de l'exploitation de vulnérabilités de redirection ouverte, utilisez un raccourcisseur d'URL comme destination de redirection plutôt que votre véritable domaine d'hameçonnage. Cette technique présente deux avantages clés : elle empêche l'application vulnérable d'enregistrer votre véritable domaine d'hameçonnage et elle ajoute une couche d'obfuscation supplémentaire, rendant la détection de l'hameçonnage plus difficile pour les utilisateurs.

Machine Translated by Google

Les fournisseurs de services cloud offrent aux attaquants un moyen efficace de créer des URL d'apparence légitime, capables de contourner les solutions de sécurité et de tromper même les utilisateurs les plus vigilants face au phishing. Ces plateformes proposent des domaines de confiance bénéficiant de la réputation des grandes entreprises technologiques. Le tableau ci-dessous présente une liste non exhaustive de services pouvant être utilisés à des fins malveillantes.

à des fins telles que l'hameçonnage.

Provider	Service	Domain Format	Use Case
Microsoft Azure	Virtual Machines	`[custom].[region].cloudapp.azure.com`	Host phishing infrastructure with custom subdomain
	App Service	`[appname].azurewebsites.net`	Deploy full web applications with Microsoft domain
	Blob Storage	`[accountname].blob.core.windows.net`	Host static phishing pages
	Azure Front Door	`[name].azurefd.net`	CDN with SSL for phishing content
	Azure Functions	`[appname].azurewebsites.net/api/[function]`	Serverless redirectors or API endpoints
	Microsoft 365	`[tenant].onmicrosoft.com`	Send phishing emails from Microsoft domains
Amazon AWS	EC2	`ec2-[IP-with-dashes].compute-1.amazonaws.com`	Host phishing infrastructure
	S3 Buckets	`[bucketname].s3.amazonaws.com`	Host static phishing content
	CloudFront	`[distribution-id].cloudfront.net`	CDN with SSL certificates
	Lambda URL	`[id].lambda-url.[region].on.aws`	Serverless functions as redirectors
Google Cloud	App Engine	`[project-id].appspot.com`	Deploy full web applications
	Cloud Storage	`storage.googleapis.com/[bucket]`	Host static phishing content
Cloudflare	Pages	`[project].pages.dev`	Host static phishing sites
	Workers	`[subdomain].[worker-name].workers.dev`	Serverless functions for redirects

Les domaines fournis par le cloud sont devenus des outils de phishing parfaits, utilisant des marques de confiance comme Microsoft, Amazon et Google qui passent facilement les contrôles de sécurité. Ces domaines sont dotés de certificats SSL fiables et les solutions de sécurité les bloquent rarement car ils hébergent du trafic professionnel légitime. Ils sont généralement classés comme « Professionnels ».

Il est préférable de parler de « technologie » plutôt que de « suspect ». Bien que les fournisseurs de services cloud tentent de prévenir les abus en fermant les sites suspects, les attaquants peuvent souvent agir sans être détectés suffisamment longtemps pour mener à bien leurs campagnes.

Par exemple, un domaine comme auth.francecentral.cloudapp.
Le site azure.com (mentionné précédemment dans la section Hébergement) doit réussir tous les contrôles de sécurité tout en paraissant légitime aux utilisateurs qui reconnaissent « Azure » comme un produit Microsoft.

Machine Translated by Google

CONCLUSION

CONCLUSION TECHNIQUE

Le paysage du phishing a considérablement évolué, passant des simples pages HTML à des techniques avancées telles que le Browser-in-The-Browser (BITB), l'Attacker-in-The-Middle (AITM) et les approches basées sur WebRTC. Certaines méthodes sont même combinées pour créer des techniques plus puissantes, comme le BITB sans cadre. Ces méthodes témoignent d'une sophistication croissante dans le contournement de l'authentification multifacteurs et la création d'expériences utilisateur convaincantes.

Parallèlement, les améliorations apportées à l'infrastructure, tirant parti des domaines des fournisseurs de services cloud et des méthodes de distribution sophistiquées, rendent les courriels malveillants de plus en plus difficiles à détecter. En 2024, selon Fortra, On a constaté une augmentation de 104 % des abus liés à Cloudflare Workers et de 198 % pour Cloudflare Pages. L'entreprise est consciente de ces abus et s'efforce d'y remédier au plus vite.

Avec l'émergence de l'IA, les attaquants disposent d'outils toujours plus performants pour concevoir des campagnes toujours plus convaincantes. Cependant, cette technologie peut également être utilisée par les équipes de défense pour détecter les tentatives d'hameçonnage en identifiant des indicateurs subtils qui pourraient échapper à l'œil humain.

Une défense efficace contre le phishing nécessite une approche multicouche combinant contrôles techniques et vigilance humaine.
Les organisations doivent mettre en œuvre un filtrage avancé des courriels, une protection des terminaux et une surveillance du réseau, tout en tenant les équipes de sécurité et les employés informés des nouvelles techniques d'hameçonnage.

Machine Translated by Google

CONCLUSION STRATÉGIQUE POUR LE RSSI

L'hameçonnage a évolué, passant de simples liens falsifiés à des chaînes d'attaque hybrides hébergées dans le cloud, qui combinent ingénierie sociale, imitation parfaite de marques et contournement de l'authentification multifacteur en temps réel. Les attaquants exploitent trois failles systémiques :

1. L'omniprésence du courrier électronique : chaque employé en possède un, chaque partenaire s'y fie et chaque attaquant sait que les défenseurs doivent rester vigilants. livrer le courrier légitime.
2. Reconnaissance humaine de schémas : des logos de confiance, un langage urgent ou un nom d'hôte cloud familier court-circuitent l'examen rationnel.
3. Angles morts des piles modernes : les jetons SaaS, la confiance entre locataires et les portées d'API trop permissives restent largement non testés dans les manuels de réponse aux incidents de nombreuses organisations.

PRIORITÉS ACTIONNABLES POUR LES RSSI

IMMÉDIAT (0-90 JOURS)	MOYEN (90-180 JOURS)	STRATÉGIQUE (6-18 MOIS)
• Renforcer l'authentification des courriels (DMARC p=rejet, MTA-STS) et bloquer les domaines nouvellement enregistrés. • Règles relatives aux boîtes aux lettres pour les instruments et transmission des alertes.	• Mener une simulation d'attaque ciblée (équipe rouge) Campagne d'hameçonnage testant explicitement les vecteurs de contournement de l'authentification multifacteur et d'abus de domaine cloud. • Étendre la détection SOC au Cloud Flare Workers, sites Azure *.cloudapp et autres refuges de réputation.	• Intégrer l'émulation continue des adversaires dans les indicateurs de cyber-résilience. • Aligner la tolérance au risque du conseil d'administration sur les données issues d'attaques réalistes des simulations plutôt que des statistiques génériques.

POURQUOI UN ADVERSAIRE EXTERNE LA SIMULATION EST IMPORTANTE

Les équipes internes excellent dans la maintenance et l'optimisation des contrôles ; elles disposent rarement des ressources nécessaires pour innover au rythme de l'écosystème criminel. Un partenaire spécialisé qui recherche, met en œuvre et déploie de manière éthique des techniques de pointe (BITB, streaming noVNC, usurpation d'identité inter-cloud) fournit des informations factuelles sur :

- Quels dirigeants ou processus métiers se laissent encore séduire par des clones haute fidélité ?
- Dans quelle mesure votre SOC détecte les détournements de session et les déplacements latéraux Jetons SaaS et enregistrements d'applications frauduleuses.
- La maturité de vos procédures de remédiation lorsque L'attaquant possède déjà un domaine cloud de confiance.

CONCLUSION

Pendant le temps qu'il vous a fallu pour lire cette page, plus de six millions de courriels d'hameçonnage ont été envoyés. La question n'est pas de savoir si l'un d'eux parviendra à contourner votre système de sécurité, mais ce qui se passe une fois à destination. Faire appel à une équipe d'experts en sécurité informatique indépendante, telle que…

Quarkslab garantit que la première attaque de phishing sophistiquée visant votre environnement sera un exercice, et non une intrusion. Parlons de la manière dont nous pouvons tirer les leçons d'aujourd'hui pour bâtir la résilience de demain.

Machine Translated by Google

DÉFENSE INNOVANTE
POUR DES MENACES EN CONSTANTE ÉVOLUTION

Société française de cybersécurité fondée en 2011 par Fred Raynal

14 ans de R&D, d'audit et de conseil

Publications dans les principaux médias événementiels et techniques (SSTIC, DIVERS, CVE et plus encore)

Plus de 300 conférences

Plus de 200 articles de blog
Plus de 50 articles académiques

Plus de 20 articles divers

30 rapports publics
Plus de 70 CVE

Notre portefeuille de services et de produits

Des renseignements exploitables en matière de cybersécurité, alimentés par la R&D et l'innovation, pour garder une longueur d'avance sur les menaces émergentes.

Évaluation approfondie de la sécurité pour renforcer les défenses et protéger les actifs critiques contre les attaques

Protection logicielle complète pour sécuriser votre code, vos données et vos secrets sur les appareils périphériques.

Machine Translated by Google

Quarkslab

Contactez-nous et suivez-nous