WHITE PAPER

vade

Spear Phishing

Les attaques ciblées
qui visent votre entreprise

Table des matières

Qu'est-ce que le spear phishing ?

Le spear phishing est une technique d'ingénierie sociale. Il prend la forme d'un email malveillant dont l'auteur prétend être quelqu'un qu'il n'est pas afin de pousser le destinataire à effectuer une action bien précise, généralement de nature financière. Bien souvent, le hacker se fait passer pour une connaissance de la victime, comme un collègue, un supérieur, un client ou un fournisseur.

Des stratégies plus ou moins sophistiquées

Pour faire croire aux destinataires que leurs emails viennent d'un expéditeur de confiance utilisant une adresse légitime, les hackers utilisent une technique dite d'usurpation.

Ils ont ainsi principalement recours à trois techniques :

- **Usurpation du nom affiché** – Le hacker usurpe le nom de l'expéditeur, mais pas son adresse email. Cette technique est efficace, car une majorité des utilisateurs font immédiatement confiance à l'expéditeur en voyant son seul nom. Par ailleurs, de nombreux clients de messagerie, en particulier sur appareils mobiles, n'affichent que le nom de l'expéditeur, sans son adresse email.

- **Usurpation du domaine** – Cette technique est plus sophistiquée que l'usurpation du nom affiché, mais aussi plus facile à détecter grâce aux protocoles SPF (Secure Policy Framework), DMARC (Domain Message Authentication Reporting) et DKIM (Domain Keys Identified Email). Le hacker peut ici spécifier l'adresse email à usurper. Lorsque cette adresse est la copie exacte de celle d'un expéditeur de confiance, les utilisateurs ont peu de chances de se rendre compte de la supercherie.

- **Usurpation par voisin proche** – Les adresses forgées selon cette technique sont très proches de l'adresse d'origine. Auparavant, ces tentatives d'usurpation étaient relativement évidentes, avec des adresses comme mlcrosoft.com au lieu de microsoft.com. Elles sont aujourd'hui plus sophistiquées et difficiles à repérer (user@mycompanyltd.com au lieu de user@mycompany.com, par exemple). Ces modifications subtiles peuvent être extrêmement difficiles à repérer pour les professionnels qui traitent leurs emails très rapidement, en particulier lorsqu'ils sont urgents. De plus, les protocoles DMARC et SPF sont inutiles dans ce cas de figure, car ils ne protègent que les domaines exacts.

$1.7 milliard

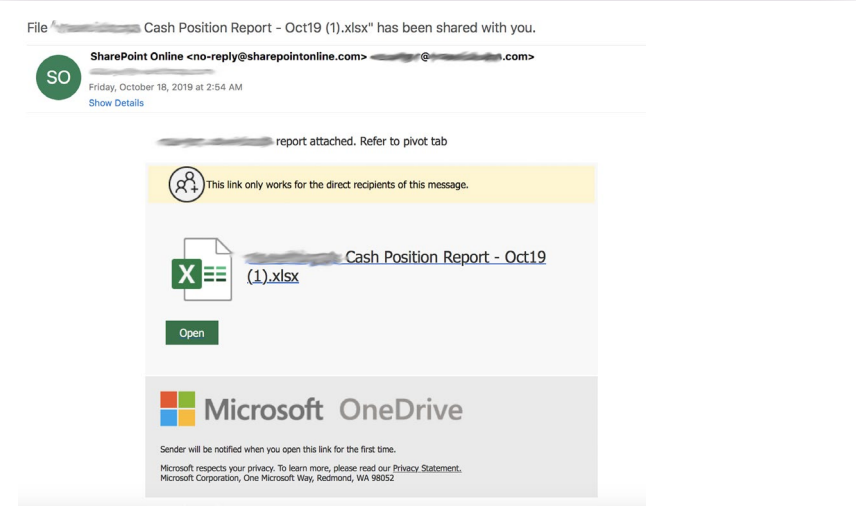
Le spear phishing a coûté aux entreprises américaines 1,7 milliard de dollars en 2018 – **FBI Internet Crime Report 2019**

Phishing et spear phishing

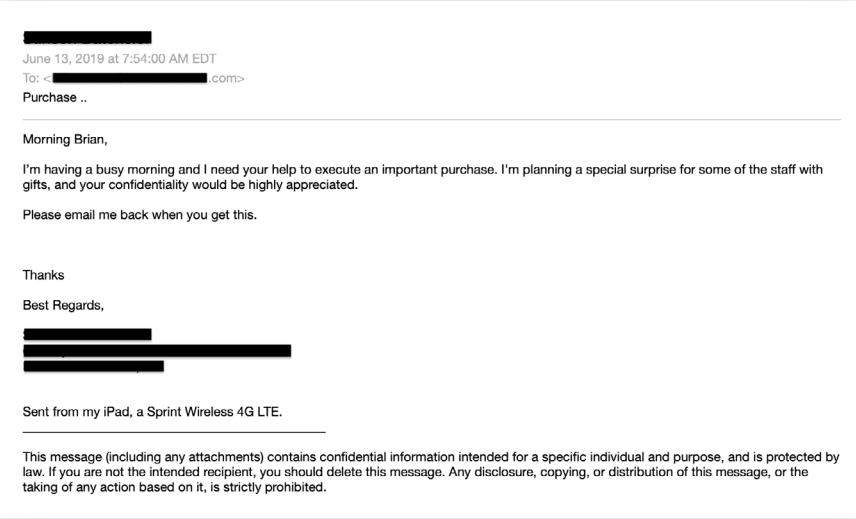
Les attaques de spear phishing et de phishing s'appuient toutes deux sur l'usurpation d'identité pour atteindre leur objectif.

Leur différence réside dans le fait que :

- Les emails de **phishing** semblent eux provenir de marques



- Les emails de **spear phishing** semblent provenir de personnes



À la différence du phishing, le spear phishing cible une personne bien précise, n'inclut pas de liens ou de pièces jointes et formule généralement une demande de virement, de cartes cadeaux ou de modifications de coordonnées bancaires, plutôt que d'identifiants de compte.

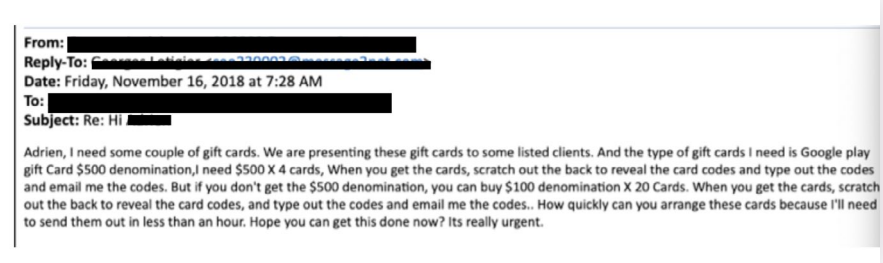
52%

Le phishing et l'ingénierie sociale au sens large ont représenté 52 % des cyberattaques visant les PME en 2018 – **Keeper & Ponemon, 2019 Global State of Cybersecurity in SMB**

Exemples d'emails de spear phishing

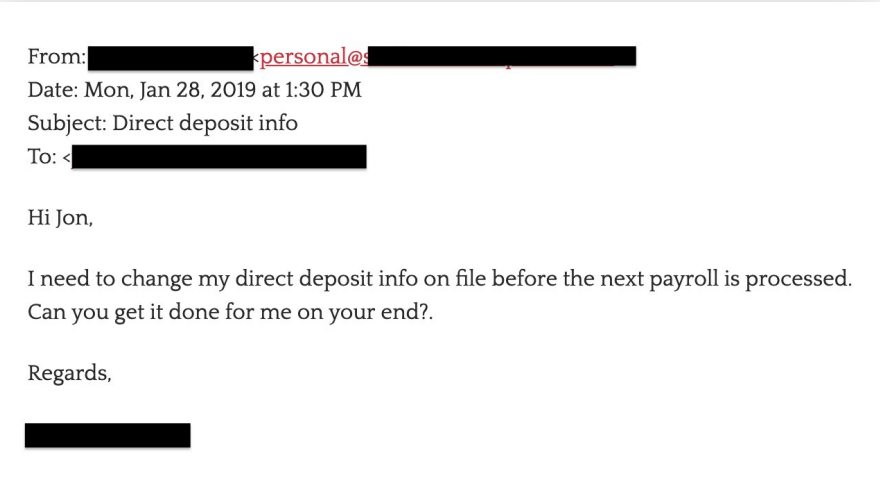
Les hackers disposent d'un vaste arsenal permettant de tromper les utilisateurs pour qu'ils dévoilent des données sensibles et des identifiants. Pour autant, ils ont souvent recours aux mêmes stratégies bien huilées..

Demandes de cartes cadeaux – Le hacker se fait passer pour un dirigeant et demande à un employé d'acheter des cartes cadeaux, puis de lui envoyer les codes figurant au verso. Bien souvent, le hacker expliquera qu'il est en réunion ou loin du bureau. Cette précision renforce la crédibilité de l'utilisation d'une adresse email personnelle, associée à un domaine Gmail ou Yahoo, par exemple.


From: [redacted]
Reply-To: [redacted]
Date: Friday, November 16, 2018 at 7:28 AM
To: [redacted]
Subject: Re: Hi [redacted]

Adrien, I need some couple of gift cards. We are presenting these gift cards to some listed clients. And the type of gift cards I need is Google play gift Card $500 denomination,I need $500 X 4 cards, When you get the cards, scratch out the back to reveal the card codes and type out the codes and email me the codes. But if you don't get the $500 denomination, you can buy $100 denomination X 20 Cards. When you get the cards, scratch out the back to reveal the card codes, and type out the codes and email me the codes.. How quickly can you arrange these cards because I'll need to send them out in less than an hour. Hope you can get this done now? Its really urgent.

Fraude au dépôt direct – Dans l'une des versions de ce scam, un hacker se fait passer par un employé et demande à un membre du service des RH de changer les coordonnées bancaires utilisées pour le paiement de son salaire. Dans une autre version, le hacker se fait passer pour un fournisseur et explique à un membre de la comptabilité que le compte bancaire et le numéro de routage du compte de l'entreprise ont changé et que les nouveaux paiements doivent utiliser un autre compte.


From: [redacted] <personal@[redacted]
Date: Mon, Jan 28, 2019 at 1:30 PM
Subject: Direct deposit info
To: <[redacted]

Hi Jon,

I need to change my direct deposit info on file before the next payroll is processed. Can you get it done for me on your end?.

Regards,

[redacted]

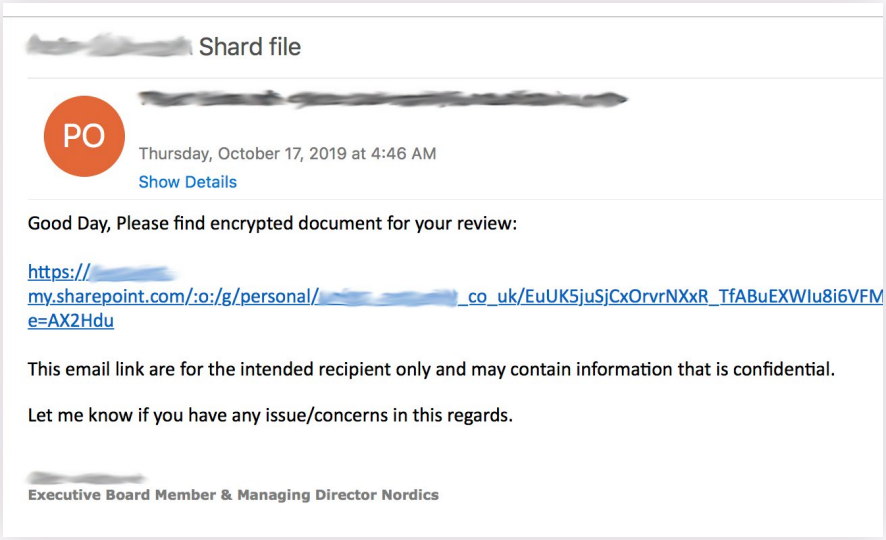
Spear phishing visant le formulaire W-2 – Un hacker se fait passer pour un dirigeant et demande à un membre des RH de lui communiquer les formulaires W-2 des employés, utilisés aux États-Unis pour déclarer les revenus et les déductions fiscales. La période des déclarations fiscales est particulièrement éprouvante pour les services de comptabilité et des RH. La pression et les délais les rendent plus vulnérables à de telles attaques.

Demande de virement – Aussi connue sous le nom d'attaque Business Email Compromise (BEC), cette stratégie de spear phishing est la plus coûteuse. Un hacker se fait passer pour un haut dirigeant et demande le versement de fonds par virement. Dans de nombreux cas médiatisés, les entreprises n'ont pas réalisé que des millions de dollars s'étaient évaporés vers des comptes bancaires frauduleux.

Attaques en plusieurs phases – Cette stratégie est souvent utilisée pour pirater des comptes Microsoft 365. Les attaques en plusieurs phases commencent par un email de phishing, puis se transforment en spear phishing. Un hacker envoie un email de phishing à un employé en se faisant passer pour Microsoft. La victime lui donne sans le savoir ses identifiants Microsoft 365 via une page frauduleuse. Armé de ces informations, le hacker pénètre dans l'écosystème Microsoft 365 de l'entreprise et y lance des attaques de spear phishing en utilisant des adresses email légitimes.

20,000

Plus de 20 000 personnes ont été victimes d'attaques BEC aux États-Unis en 2018 – **FBI**


[redacted] Shard file

PO [redacted]

Thursday, October 17, 2019 at 4:46 AM

Show Details

Good Day, Please find encrypted document for your review:

https://[redacted] my.sharepoint.com/:o:/g/personal/[redacted]_co_uk/EuUK5juSjCxOrvrNXxR_TfABuEXWIu8i6VFM e=AX2Hdu

This email link are for the intended recipient only and may contain information that is confidential.

Let me know if you have any issue/concerns in this regards.

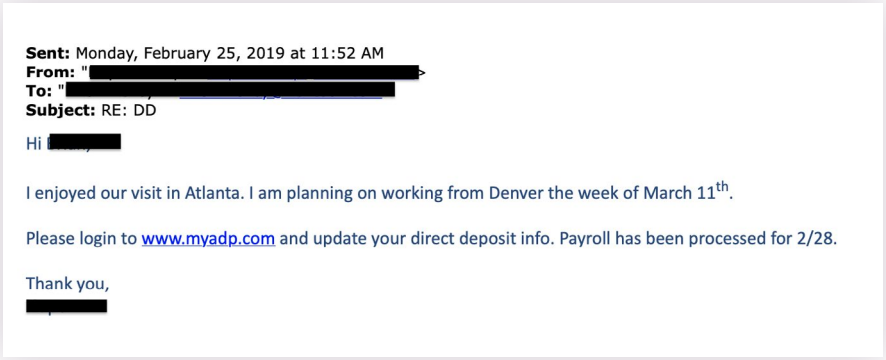
[redacted]

Executive Board Member & Managing Director Nordics

Techniques de spear phishing

Un email de spear phishing, composé uniquement de texte et envoyé à une seule personne, peut sembler bien simpliste à première vue, mais il s'appuie en réalité sur des techniques d'ingénierie sociale et de manipulation psychologique redoutablement efficaces. En voici quelques exemples :

Pretexting – Les hackers préparent leurs victimes en commençant par leur envoyer un email amical et en faisant la conversation, que ce soit pour leur demander comment se sont passées leurs vacances ou pour les féliciter de leur promotion. La victime baisse ainsi sa garde et est plus à même d'écouter la demande du hacker, qui peut ne venir qu'au bout de plusieurs emails.



Sent: Monday, February 25, 2019 at 11:52 AM
From: "[redacted]"
To: "[redacted]"
Subject: RE: DD

Hi [redacted]

I enjoyed our visit in Atlanta. I am planning on working from Denver the week of March 11th.

Please login to www.myadp.com and update your direct deposit info. Payroll has been processed for 2/28.

Thank you,
[redacted]

Demandes urgentes – Les hackers parviennent souvent à convaincre leurs victimes qu'elles n'ont que quelques heures, voire quelques minutes, pour effectuer un virement, modifier des coordonnées bancaires ou acheter des cartes cadeaux pour les clients.

GL

[redacted] <president.[redacted].com>
To: [redacted]
Monday, May 6, 2019 at 12:35 PM
Hide Details

I have important request i need you to handle immediately. Kindly confirm your availability.

Regards.

Sent from my Verizon 4G LTE Droid - please excuse any brevity or typos

Envoi d'emails via mobile – Les hackers se faisant passer pour des dirigeants affirment souvent ne pas être au bureau, voire être à l'étranger, et avoir besoin de l'aide de la victime en urgence. L'ajout de la mention « Envoyé depuis mon iPad, iPhone ou appareil Android » permet de renforcer la crédibilité de cette affirmation et d'excuser les erreurs éventuelles de l'email, notamment les fautes d'orthographe. Elle justifie également l'utilisation d'une adresse personnelle, par exemple d'une adresse Gmail.

Prévention du spear phishing

The absence of URLs and attachments makes spear phishing extremely difficult to detect. Traditional email filters use outdated methods to block threats, and most are ineffective in the fight against spear phishing. Optimal spear phishing protection requires advanced methods.

Traditional email defense

Reputation – La détection basée sur la réputation bloque les expéditeurs malveillants connus (adresse IP) et les URL de phishing. Un filtre basé sur ce système bloque les expéditeurs malveillants connus, mais laisse passer les nouvelles menaces.

Signature (Fingerprint) – La détection des menaces basée sur la signature bloque les menaces disposant d'une signature connue, par exemple un code de malware.

Sandboxing – Le sandboxing envoie les emails suspects dans un environnement contrôlé pour les analyser. Il est inefficace contre le spear phishing, car ce type d'email n'inclut ni pièce jointe ni lien.

Passerelles de messagerie sécurisées – Secure email gateways (SEG) ont recours à la fois à l'analyse de la réputation et de la signature. Elles se trouvent en dehors d'Microsoft 365 : Exchange Online Protection (EOP) est donc désactivée. Elles sont également impuissantes contre les attaques lancées depuis l'intérieur.

8%

La sécurité de l'email native d'Office 365 propose une précision totale de seulement 8 % – **SE Labs**

Défense proactive

Avec la défense proactive, l'intelligence artificielle (IA), via l'association de modèles d'apprentissage automatique supervisé et non supervisé, identifie les signes difficiles à détecter du spear phishing:

Apprentissage supervisé – Les algorithmes sont entraînés, à l'aide d'emails malveillants et légitimes, à reconnaître les caractéristiques spécifiques des emails de spear phishing, telles que les signatures des appareils mobiles et les adresses email de domaines.

Apprentissage non supervisé – Dans ce type de modèle, le traitement du langage naturel et la détection non supervisée des anomalies travaillent ensemble à la reconnaissance des schémas abusifs des emails de spear phishing, notamment le sentiment d'urgence, les mots-clés indiquant des demandes financières et les adresses email ne correspondant à aucun expéditeur du modèle d'entité de l'entreprise.

Retours des utilisateurs – Les utilisateurs peuvent signaler les emails de phishing à l'équipe chargée des opérations de sécurité (SOC) qui les analysent et améliorent ainsi les algorithmes.

En savoir plus

vadesecure.com/en/spear-phishing

vadesecure.com/en/resources?topic=Spear+Phishing

Vade for M365

Notre technologie anti spear phishing basée sur l'IA propose des bannières personnalisables permettant d'alerter les utilisateurs d'Microsoft 365 de tentatives d'usurpations potentielles.

DEMANDEZ UNE DÉMO

À propos de Vade

Notre mission?. Protéger les emails du monde entier des menaces les plus sophistiquées. Que ce soit pour assurer la protection des particuliers via les plus grands FAI ou les entreprises via nos partenaires MSP, nos solutions de sécurité de l'email basées sur l'IA sont conçues pour détecter l'indétectable.

- 1 milliard de boîtes mails protégées
- 100 milliards d'emails analysés / jour
- 1,400+ partenaires dans le monde
- Renouvellement annuel de 95%
- 15 brevets internationaux actifs

En savoir plus
www.vadesecure.com

@vadesecure