Octobre 2022 • VOL. 9 N° 9

ARS SOLUTIONS

PASSION AFFAIRES et technologies

PRÉSENTÉS CE MOIS-CI

« La cybersécurité est une priorité absolue pour les Bois de Plancher PG…

Nous avons à respecter des normes de sécurité rigoureuses afin d'assurer la pérennité de notre entreprise. L'expertise qu'ARS éprouve dans le domaine manufacturier et les environnements complexes nous permet d'atteindre, voire de dépasser, les exigences liées à la certification C-TPAT.

De plus, ARS est en mesure de travailler de concert avec les exigences toujours plus élevées de nos assureurs afin de respecter les critères d'admissibilités aux polices d'assurance contre les cyberrisques. Nous sentons que l'équipe est en parfaite maîtrise de notre environnement et, surtout, qu'elle comprend notre réalité de production.

ARS est donc un véritable partenaire d'affaires et nous permet de se concentrer sur la croissance de notre entreprise sans se soucier de la cybersécurité. »

Alain Bédard
Directeur de la gestion des systèmes d'information
Bois de Plancher PG

SUIVEZ-NOUS SUR NOS RÉSEAUX SOCIAUX

- ARS Solutions Affaires-TI et Cybersécurité
- ARS Solutions Affaires et Technologies
- ARS Solutions
- arssolutions89

AFFAIRES-TI

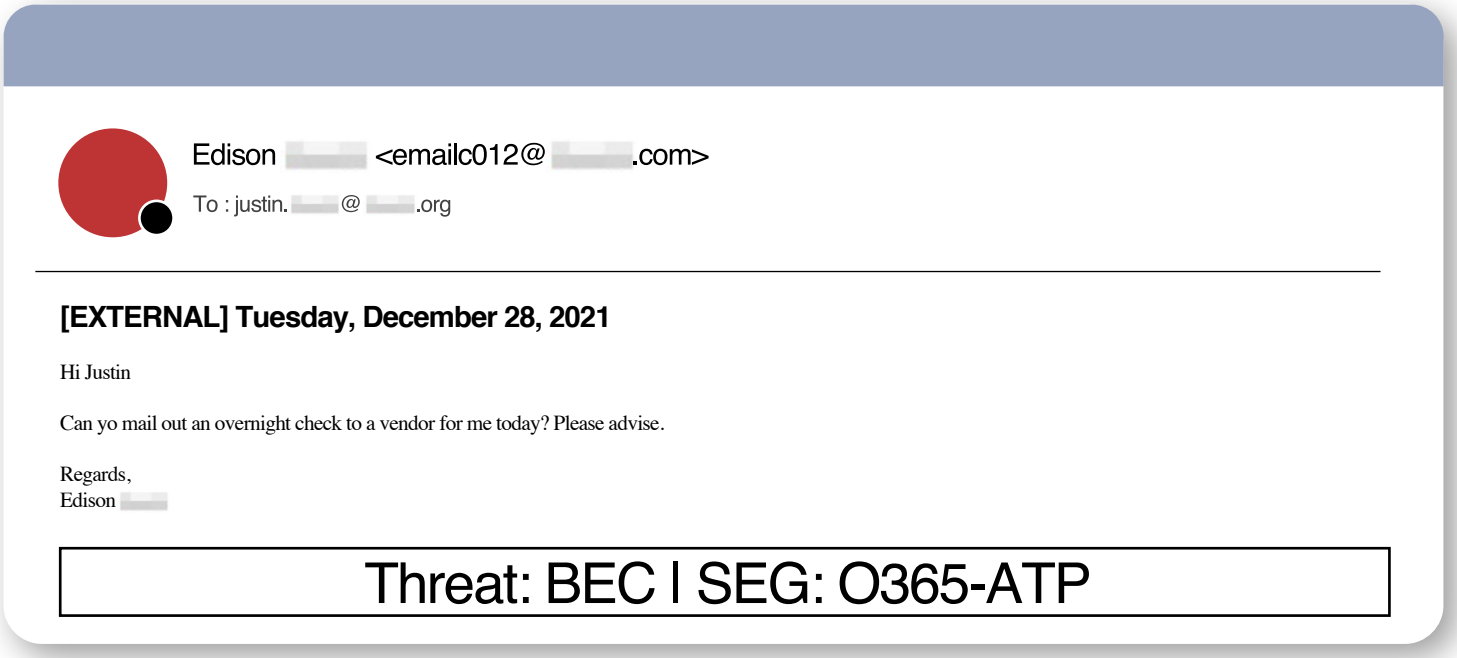
ATTAQUES PAR ÉCHANGES DE COURRIELS SANS LIEN CLIQUABLE

Bien que toute notre attention se porte sur les liens cliquables des courriels frauduleux, il existe également des **attaques par échanges de courriels sans lien cliquable**. À faire attention puisque la victime n'est pas du tout en communication avec la personne qui semble se présenter. Les tendances observées par Cofense incluent **les escroqueries de dépôt direct, la fraude par carte-cadeau et les arnaques de factures**. Ces attaques reposent uniquement sur l'interaction humaine. **Ce mois-ci, on vous présente la fraude au niveau des factures.**

SUITE PAGE 2

Il s'agit d'un vecteur d'attaque particulièrement frustrant pour de nombreuses raisons.

Premièrement, **l'attaquant peut rester à l'affût dans une boîte de réception pendant des mois avant de lancer son attaque**. Deuxièmement, comme les attaquants utilisent des règles de transfert de courriels pour créer une présence dans la boîte de réception de l'utilisateur, **la norme industrielle consistant à réinitialiser un mot de passe après une violation n'aidera pas l'attaque**, car les règles de transfert de courriels existent toujours sur le compte. Troisièmement, en détournant un fil de messagerie connu et fiable, l'attaque est ponctuelle et passe théoriquement **sur le dos de la victime potentielle**. Les attaquants iront jusqu'à **imiter la typographie, les signatures et la manière d'écrire** pour augmenter leurs chances de réussite. D'où l'importance de vérifier régulièrement vos messages reçus/ouverts, envoyés et même supprimés pour **signaler rapidement un courriel/discussion inconnu à votre partenaire TI** pour mettre fin à l'échange et trouver sa provenance pour, non seulement vous déculpabiliser, mais aussi pour assurer votre sécurité financière et celle de votre organisation.



La première étape d'une escroquerie de facture **peut commencer des semaines avant l'attaque financière**, la plupart des malfaiteurs ne sachant pas qui sera leur victime finale. Pour que son plan fonctionne, le cybercriminel doit d'abord compromettre un compte de messagerie, **par le biais d'identifiants hameçonnés ou de l'achat d'identifiants sur le Dark Web**, afin d'obtenir l'accès à un compte de messagerie.

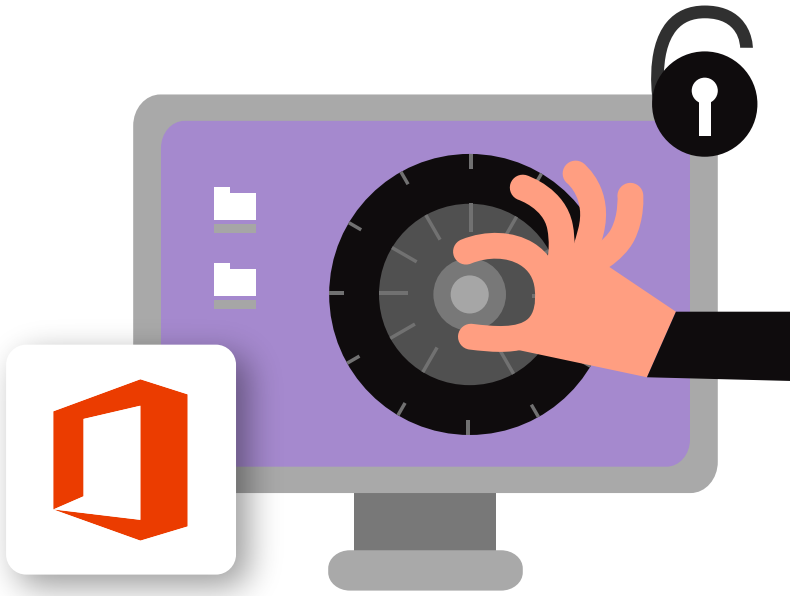
Une fois le compte compromis, les acteurs mettent en place des règles de transfert de courriels dans la boîte de réception compromise pour détourner les courriels entrants touchant de la facturation ou des bons de commande. Une fois qu'un potentiel d'attaque a été identifié, les criminels vont rapidement **falsifier des factures et détourner des fils de discussion** pour se faire passer pour le propriétaire de la facture légitime. Pour l'utilisateur qui s'est fait usurper son compte, **il y a malheureusement très peu d'éléments qu'il peut détecter comme étant malveillants dans ces attaques…**

Source : Cofense 2022 Annual State of Phishing Report

25 % DES PROFESSIONNELS DE L'INFORMATIQUE

ne savent pas ou ne pensent pas que les données de Microsoft 365 peuvent être affectées par un rançongiciel

De nombreuses organisations pensent à tort que Microsoft 365 est protégée contre les attaques par rançongiciel... 40 % des professionnels en informatique qui utilisent Microsoft 365 dans leur organisation ont admis ne pas avoir de plan de récupération.



La dernière enquête de Hornetsecurity confirme les prévisions du secteur de la cybersécurité selon lesquelles le rythme des rançongiciels s'intensifiera en 2022. Hornetsecurity **a interrogé plus de 2 000 responsables TI** pour sa dernière enquête annuelle. Parmi les résultats, près de **25 % des entreprises ont subi une attaque par rançongiciel (versus 20 % l'an dernier)**. 20 % d'entre elles se sont produites au cours des 12 derniers mois.

Les cyberattaques sont de plus en plus fréquentes

"Le rythme d'infection par rançongiciels augmente, parallèlement à une diminution **du nombre d'organisations activant la protection contre les spams et les malwares par courriel**", a déclaré Daniel Hofmann, PDG de Hornetsecurity. "Une raison que nous soupçonnons pour expliquer cette diminution est **le taux croissant d'adoption de la plateforme Microsoft 365**." **De nombreuses organisations qui ont adopté des services cloud pensent que leur fournisseur les protège contre des cyberattaques comme les rançongiciels**, a déclaré Hofmann. "Malheureusement, dans la plupart des cas, y compris pour Microsoft 365, ce n'est pas le cas", a-t-il souligné. "Et c'est à l'entreprise de sécuriser et de protéger ses propres données".

Manque généralisé de préparation des entreprises

40 % des professionnels en informatique qui utilisent Microsoft 365 dans leur organisation ont admis ne pas avoir de plan de récupération au cas où leurs données Microsoft 365 seraient compromises par un rançongiciel. "Avec l'aide de certains outils, les administrateurs TI peuvent sauvegarder leurs données Microsoft 365 en toute sécurité et se protéger contre de telles attaques", a déclaré Hofmann. Les réponses à l'enquête ont montré le **manque généralisé de préparation des entreprises**. **Cela inclut une augmentation des entreprises n'ayant pas de plan de reprise après sinistre en place**.

En 2021, 16 % des personnes interrogées ont déclaré ne pas avoir mis en place de plan de reprise après sinistre. En 2022, ce chiffre est passé à 19 %, malgré l'augmentation des attaques. L'enquête a également montré que plus de 20 % des entreprises ayant subi une attaque ont payé la rançon et/ou perdu leurs données. Les cybercriminels sont incités à mener ces attaques par rançongiciel, car ils ont de bonnes chances d'être payés.

Le "ça ne m'arrivera pas" est encore très répandu

La mentalité du "ça ne m'arrivera pas" est certainement quelque chose que Hornetsecurity continue de voir, selon Hofmann. C'est d'autant plus vrai que de plus en plus d'organisations adoptent les services en cloud. "Il existe plusieurs idées fausses lorsqu'il s'agit du cloud", mentionne Hofmann. "Les nouveaux adoptants supposent souvent que la sécurité et la protection des données sont traitées dans le cadre de leur facture mensuelle, ce qui n'est pas le cas. Nous voyons également des cas où **certaines organisations pensent que des plateformes telles que Microsoft 365 ne sont pas sensibles aux attaques par rançongiciel**. Ce qui est malheureusement faux. Dans un cas comme dans l'autre, **l'organisation s'expose à un risque énorme de perte de données**, d'atteinte à sa réputation et à tous les autres problèmes associés à une violation de la sécurité.

Selon M. Hofmann, près de 60 % des attaques de rançongiciel ont pour origine des attaques par hameçonnage.

Les fournisseurs TI spécialisés en cybersécurité peuvent offrir une **protection et une tranquillité d'esprit** considérables. Ils peuvent apporter une aide supplémentaire en proposant des **solutions éprouvées qui aident à combler les lacunes organisationnelles en matière de sécurité** pour chacun de leurs clients. Par exemple, vous avez peut-être un client dans un secteur hautement règlementé comme la finance. Fournir des services de sécurité supplémentaires à vos employés, tels que de la **formation pour les sensibiliser à la cybersécurité**, peut apporter une confiance et une protection supplémentaires à vos précieux clients.

Source : Edward Gately

BUSINESS EMAIL COMPROMISE : FRAUDE PAR CARTE-CADEAU

Le Business Email Compromise (BEC) est responsable de milliards de pertes financières auprès d'entreprises à travers le monde.

Lorsqu'il est question de fraude par carte-cadeau, **les acteurs se font passer pour le PDG ou une autorité quelconque au sein d'une entreprise et demandent à un employé d'effectuer une "tâche" ou un "achat" en leur nom**. Dans de nombreux cas, les escrocs demandent le numéro de cellulaire des employés afin de sortir la conversation de la chaîne de courriers électroniques et de la transférer vers un moyen qui n'est pas systématiquement suivi : **les SMS**. Non seulement cette méthode est plus difficile à suivre, mais le fait de disposer d'un numéro de téléphone rend l'attaque plus crédible, augmentant ainsi la probabilité que la victime potentielle croit qu'elle s'adresse réellement à un responsable.

Matt [redacted] < matt- [redacted] @att.net >

To : redacted@manufacturing

Birthday

How are you? I need a favor from you.

I'm sorry for botherinhg you with this. I need to get an Itunes gift card for my Niece. It's her birthday today and I totally forgot. I can't do this now because I'm currently out of the town with no means of getting this done. Can you get it from any store around you? I'll pay back as soon as I am back. Kindly let me know if you canhandle this. Please email me back as soon as possible.

Thank you,
Matt

Alors que **les attaques Business Email Compromise (BEC) traditionnelles utilisent les comptes bancaires des victimes**, il devient de plus en plus difficile pour les escrocs d'encaisser la totalité de leurs gains mal acquis. En effet, un faible pourcentage est prélevé sur le montant total à chaque étape, ce qui réduit considérablement les gains des malfaiteurs. En revanche, dans le cas des escroqueries aux cartes-cadeaux, **les acteurs échangent ensuite les cartes-cadeaux contre de la crypto-monnaie** pour convertir directement les cartes-cadeaux volées, en bitcoin par exemple, en quelques minutes seulement. **Les acteurs sont donc en mesure de passer sous le radar** des autorités fédérales, nationales et locales en raison de la complexité des escroqueries. En outre, les organismes de réglementation font peu pour suivre les cartes-cadeaux qui ont été volées, ce qui en fait presque le crime BEC parfait.

Source : Cofense 2022 Annual State of Phishing Report