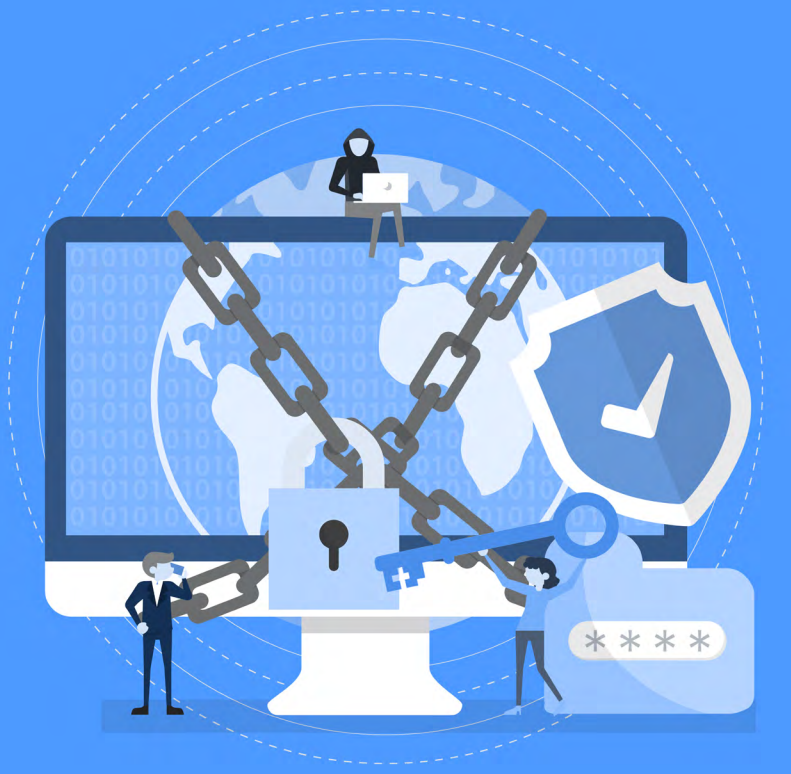
CCN-CERT

BP/04



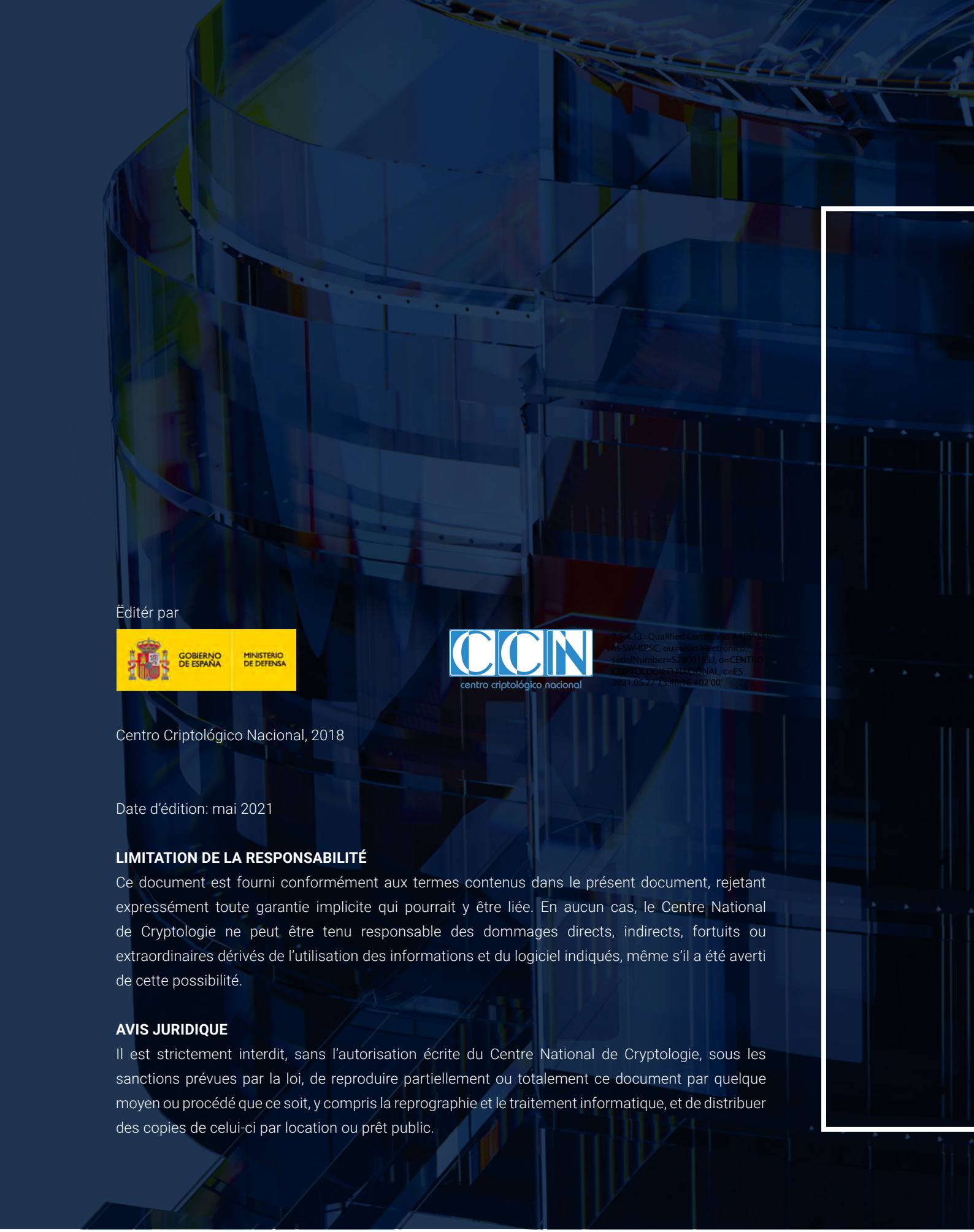
Ransomware

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
2021.05.27 13:48:16 +02'00'

Date d'édition: mai 2021

Index

Index

1. À propos du CCN-CERT, certificat gouvernemental national

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie, CCN, rattaché au Centre national de renseignement, CNI

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie, CCN, rattaché au Centre national de renseignement, CNI. 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 CNI, le RD 421/2004 réglementant le CCN est dans le RD 3/2010, du 8 janvier, réglementant le schéma de sécurité nationale (ENS), modifié par le RD 951/2015 du 23 octobre.

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 faire face activement aux cybermenaces, y compris la coordination au niveau public de l'État des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

F de la loi 11/2002) et des informations sensibles, défendre le patrimoine technologique de l'Espagne, former du personnel spécialisé, appliquer des politiques et des procédures de sécurité et utiliser et développer les technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du **secteur public**, le CCN-CERT est chargé de la gestion des cyber-incidents affectant tout organisme ou entreprise publique. Dans le cas des **opérateurs critiques du secteur public**, la gestion des cyberincidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

2. Introduction

La famille des codes malveillants connue sous le nom de "ransomware" est la menace la plus répondue et la plus nuisible, avec une grande évolution ces dernières années.

Vers 2012, les premières variantes ont été découvertes, dont l'objectif principal était de verrouiller l'ordinateur infecté. Des années plus tard, les ransomwares ont évolué vers ce que l'on appelle aujourd'hui des "crypteurs" de fichiers. Le scénario s'est aggravé en 2015-2016 lorsque les RaaS (Ransomware as a Service), services proposés par les cybercriminels pour concevoir facilement ce type de malware en échange d'un pourcentage des bénéfices potentiels de la campagne, ont proliféré.

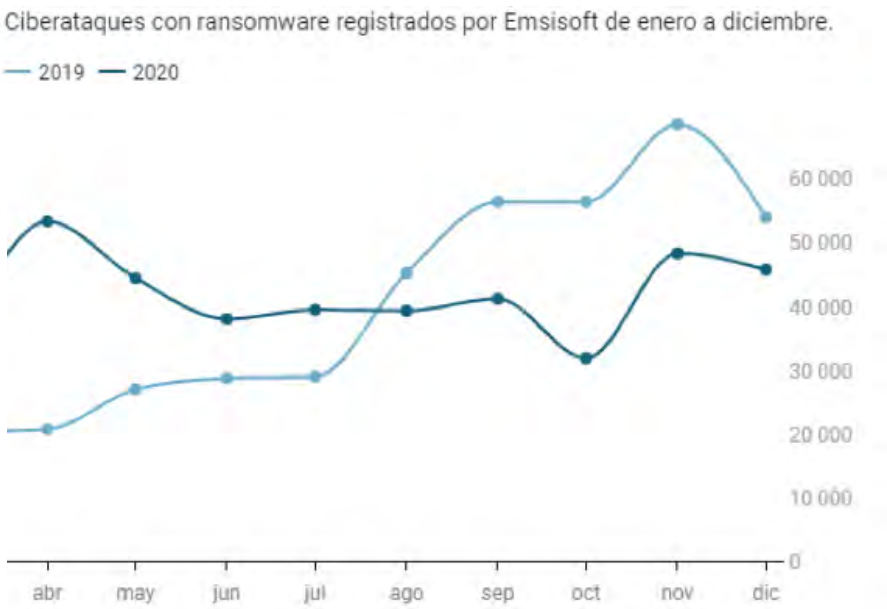
Au cours de la période allant de 2019 à 2020, une nette augmentation des cyberattaques a pu être observée, lorsque la pandémie a commencé à se diffuser dans le monde et que les gouvernements de différents pays ont décrété des confinements.

Selon Emsisoft[1], le nombre total d'attaques par ransomware a augmenté de 12,39 % en 2020 par rapport à l'année précédente. En janvier 2020, les incidents liés aux ransomwares ont augmenté de 59,84 % par rapport au même mois de l'année précédente. En février, les attaques avec ce type de code ont augmenté de 137,17 %. Mais ce n'est qu'en avril que la croissance record a été enregistrée : 156,55%. À partir de mai, la croissance s'est ralentie. Ce mois-là, il a augmenté de 64,36% par rapport au même mois de mai de l'année précédente, et en été, la différence a oscillé autour de 30%. Le second semestre 2020 a enregistré moins d'incidents que durant la même période en 2019.

En novembre 2020, environ 25 groupes de ransomware différents ont été signalés comme étant actifs.

Le nombre total d'attaques par ransomware a augmenté de 12,39 % en 2020 par rapport à l'année précédente

1. https://www.businessinsider.es/grafico-ensena-como-pandemia-ha-disparado-ciberataques-834287.



[Figure 1] Ciberataques con ransomware registrados por Emisoft

Des rapports tels que celui de Cognyte[2] affirment que les trois familles de ransomware les plus actives au niveau mondial en 2020 étaient Ryuk, Maze et REvil/Sodinokibi. En outre, selon un autre rapport réalisé par Palo Alto Networks, les cybercriminels[3] exploitant des attaques par ransomware ont collecté plus que jamais au cours de la même année.

Dans les cyberattaques de type "ransomware", les cybercriminels[4] utilisent un code malveillant qui crypte les données et les systèmes informatiques, puis exigent une rançon de leurs victimes si elles veulent revenir à la normale. Il convient de noter que les criminels s'en prennent de plus en plus à des cibles plus vulnérables, comme les organismes de santé, et qu'ils ont mis au point des stratégies plus agressives pour forcer le paiement de rançons.

Dans les cyberattaques de type "ransomware", les cybercriminels utilisent un code malveillant qui crypte les données et les systèmes informatiques, puis exigent une rançon de leurs victimes si elles veulent revenir à la normale

2. Voir : https://www.cognyte.com/blog/what-you-need-to-know-about-the-top-4-global-ransomware-vulnerabilities-and-how-to-stay-protected/
3. Voir : https://unit42.paloaltonetworks.com/ransomware-threat-report-highlights/
4. Voir : https://www.businessinsider.es/pagos-rescate-ransomware-triplicaron-durante-pandemia-833859

Le mode de paiement est resté inchangé au fil des ans, les crypto-monnaies (dans la plupart des cas, le bitcoin) étant utilisées en raison de leur caractère anonyme.

Dans un monde où la plupart des sources de cybersécurité s'attendent à ce que les cybermenaces continuent à augmenter, il est important de savoir comment se défendre.

Ce guide présente les mesures applicables à ces phases.

Moins quatre phases distinctes de cyberattaque qui doivent être abordées :

1. **La prévention**
2. **Détection**
3. **Réponse**
4. **Remédier à l'attaque**

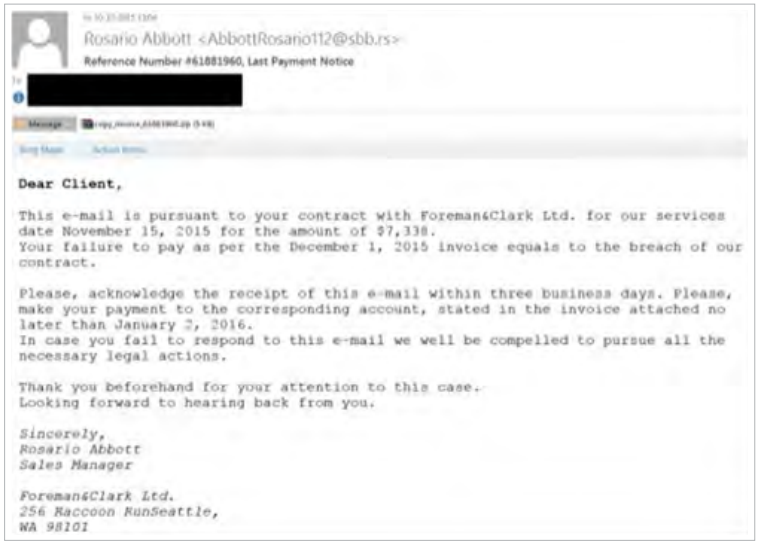
3. Les vecteurs d'infection

Pour prévenir les infections, il est préférable de connaître les moyens d'entrée de la menace, ainsi que ses mécanismes de propagation. Cependant, après une infection, il n'est pas toujours possible de déterminer l'origine ou les causes exactes.

Les mécanismes et les possibilités d'infection sont variés, et il est important de connaître les vecteurs les plus courants. Dans certains cas, le code nuisible peut rester latent dans le système pendant un certain temps et se manifester à la suite d'une action spécifique ou de la détermination d'une date précise, ce qui rend difficile de préciser le moment exacte de l'infection.

3.1 Phishing par e-mail

Bien qu'en diminution (dans le cas des ransomwares), l'utilisation d'emails frauduleux (p hishing) est encore très présente au quotidien.



Rosario Abbott <AbbottRosario112@sbb.rs>

Reference Number #61881960, Last Payment Notice

To: [redacted]

Dear Client,

This e-mail is pursuant to your contract with Foreman&Clark Ltd. for our services date November 15, 2015 for the amount of $7,338.
Your failure to pay as per the December 1, 2015 invoice equals to the breach of our contract.

Please, acknowledge the receipt of this e-mail within three business days. Please, make your payment to the corresponding account, stated in the invoice attached no later than January 3, 2016.
In case you fail to respond to this e-mail we well be compelled to pursue all the necessary legal actions.

Thank you beforehand for your attention to this case.
Looking forward to hearing back from you.

Sincerely,
Rosario Abbott
Sales Manager

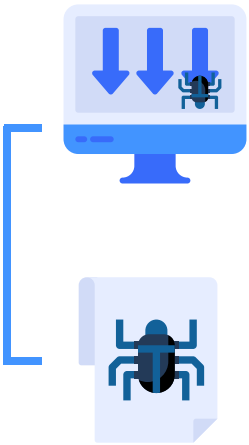
Foreman&Clark Ltd.
256 Raccoon RunSeattle,
WA 98101

[Figure 2] Courriel frauduleux utilisé par TeslaCrypt

Ce type d'e-mail s'appuie sur ce que l'on appelle l'ingénierie sociale (la manipulation de personnes dans le but de leur faire accomplir une série de tâches à la convenance du manipulateur) pour amener l'utilisateur à exécuter un fichier apparemment inoffensif.

Il existe deux formes typiques d'infection, soit par un lien vers une page frauduleuse, qui dissimule le code malveillant dans une application apparemment légitime, soit par un fichier spécialement manipulé joint au message électronique.

Formes typiques d'infection



Via web link

Par pièce jointe

3.2 Via web link

Ce type d'infection consiste à diriger la victime vers un site web qui peut être légitime, mais que les cybercriminels ont modifié au préalable, ou bien il peut s'agir d'une copie quasi identique qui ne se distingue pas de la version légitime.

Dans les deux cas, la victime télécharge ou exécute (consciemment ou inconsciemment) une ¬application qui, bien qu'elle ne semble pas suspecte au premier abord, cache le code malveillant.

3.3 Par pièce jointe

Dans ce cas, le message électronique lui-même transporte un fichier sémantiquement lié au texte du message et, sous un prétexte quelconque (faux rapport bancaire, formulaires, images, curriculum vitae, etc.), invite et amène la victime à l'ouvrir, opération qui déclenche l'exécution du code malveillant.

Pour plus d'informations sur la manière de prévenir ces formes d'infection, il est conseillé de consulter le rapport BP-02-16 Good Practices in Electronic Mail

3.4 Browsing web. Kits d'exploitation web

Vous pouvez également trouver ce que l'on appelle des kits d'exploitation Web : un mode d'infection plus subtil et transparent qui tire parti d'une vulnérabilité connue du navigateur ou d'un plugin installé pour exécuter un code malveillant.

La transparence de cette méthode réside dans le fait que les responsables des campagnes de ransomware prennent d'abord le contrôle du serveurs légitimes pour compromettre les pages qu'ils proposent, notamment les contenus malveillants qui exploitent les faiblesses des navigateurs. De cette façon, ils font en sorte que le navigateur de l'utilisateur télécharge un code binaire qui ¬est immédiatement exécuté, lançant ainsi le processus d'infection.

Web : Un mode d'infection plus subtil et transparent qui tire parti d'une vulnérabilité connue du navigateur ou d'un plugin installé pour exécuter un code malveillant

Pour éviter ce type d'infection, la seule chose à faire est d'utiliser la version la plus récente du navigateur et de ses extensions. En principe, il est conseillé de bloquer tous les composants qui ne sont pas strictement nécessaires. Parmi les plugins les plus couramment utilisés figurent Flash Player, Java et Silverlight.

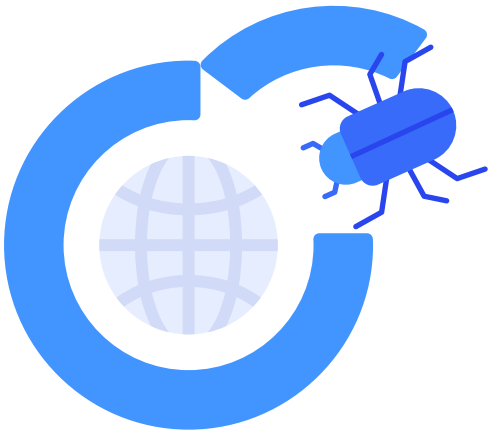
L'un des principaux problèmes des plugins est qu'ils augmentent considérablement l'exposition à certains types d'attaques pendant la navigation sur le web. Certains de ces plugins contiennent un grand nombre de vulnérabilités critiques qui permettent aux attaquants d'exécuter un code sur l'ordinateur du victime.

Il suffit à l'utilisateur de cliquer ou de naviguer sur une page malveillante pour que son ordinateur soit compromis (sans même télécharger ou interagir avec la page en question). La plupart des navigateurs vous permettent d'activer ou de désactiver les composants installés. L'activation des plugins, tels que Flash et Java, de manière temporaire et contrôlée par l'utilisateur peut être une bonne option.

Il est également conseillé d'utiliser des modules complémentaires spécifiques pour bloquer l'ouverture des pop-ups[5], des iframes, l'exécution du code JavaScript et des publicités (Ads). Tous ces mécanismes peuvent être utilisés pour forcer le navigateur à charger des pages, qui peuvent être compromises, ou pour exécuter un code nuisible.

Pour plus d'informations sur la manière de prévenir ces formes d'infection, il est conseillé de consulter le rapport BP-06-16 Good Practices in Web Browsers

Pour éviter ce type d'infection, la seule chose à faire est d'utiliser la version la plus récente du navigateur et de ses extensions



5. Voir : http://es.ccm.net/faq/9996-bloquear-ventanas-emergentes-de-publicidad-pop-ups

3.5 Attaques par RDP

Conscients du changement de scénario dû à la pandémie de COVID 19, qui a obligé les employés à effectuer une grande partie de leur travail à distance, les cybercriminels - en particulier les opérateurs de ransomware - tentent d'exploiter les nouvelles opportunités pour augmenter leurs profits[6].

RDP est devenu un vecteur d'attaque populaire ces dernières années, notamment parmi les opérateurs de ransomware, qui utilisent ce protocole pour accéder aux machines de l'infrastructure et de se diffuser ensuite.

Les attaquants, à l'aide d'outils automatisés, recherchent les ordinateurs qui ont ce service exposé à l'Internet. Ensuite, à l'aide d'une attaque par force brute (c'est-à-dire en essayant toutes les combinaisons alphanumériques possibles) ou d'une attaque par dictionnaire (gros fichiers composés des utilisateurs et des mots de passe les plus courantes utilisés sur Internet), ils tentent d'accéder à l'ordinateur.

C'est pourquoi il est essentiel de s'assurer que les combinaisons du nom d'utilisateur et des mots de passe utilisées pour accéder aux services sont solides.

RDP est devenu un vecteur d'attaque populaire ces dernières années, notamment parmi les opérateurs de ransomware

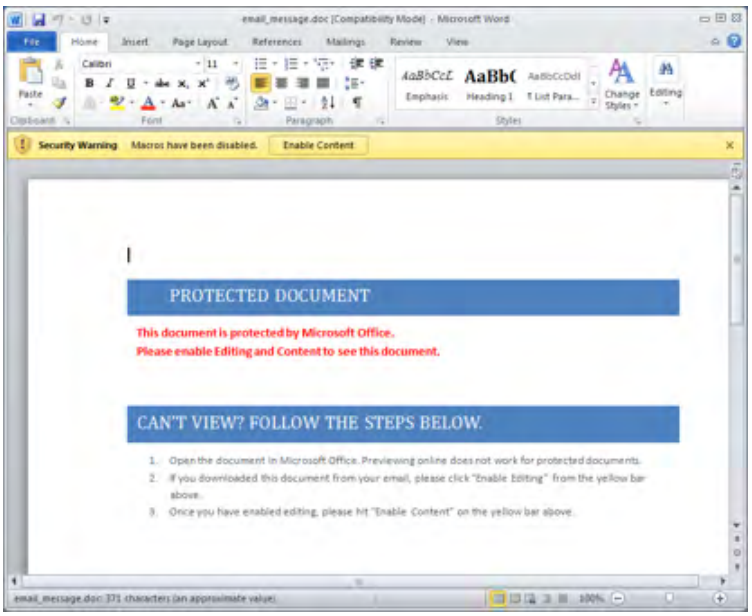
6. https://www.welivesecurity.com/la-es/2020/06/29/crecieron-ataques-fuerza-bruta-dirigidos-rdp-durante-pandemia/

3.6 Attaques sans interaction avec l'utilisateur

Face à un scénario où de plus en plus d'utilisateurs sont informés sur les attaques informatiques et les méthodes d'infection les plus fréquentes (en bref, plus sensibilisés à la sécurité informatique), les créateurs du logiciels malveillants (en général) adaptent leurs méthodes afin de diffuser le plus possible leurs exécutables malveillants.

Cette évolution s'est traduite par la diffusion des documents bureautiques malveillantes, dont le contenu semble à première vue illisible ou protégé. Il est à noter que pour pouvoir lire le document, il faut activer des macros, après quoi le code malveillant est exécuté.

[Figure 3]
Exemple d'un document malveillant prétendument protégé



Cependant, depuis fin 2017, des méthodes ont commencé à être utilisées où l'ingénierie sociale n'était plus nécessaire, puisque l'interaction avec l'utilisateur est éliminée. Un exemple est l'utilisation d'exploits (programmes qui profitent d'une insécurité pour exécuter un code arbitraire) dans des documents bureautiques qui sont exécutés par simple ouverture, sans qu'il soit nécessaire d'activer des macros. Ce type d'attaque est très dangereux car le besoin d'interaction est nul, car ils ne montrent généralement aucune alerte ou fenêtre, ce qui rend difficile la détermination du moment où l'infection a eu lieu.

3.7 Via d'autres logiciels malveillants

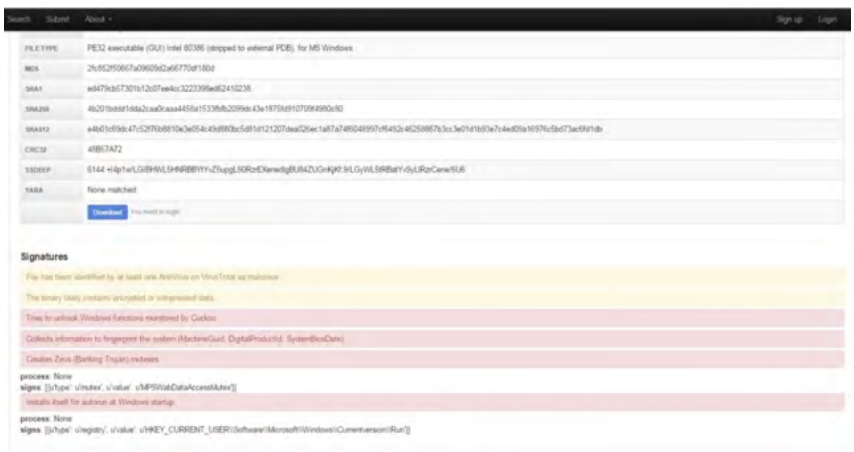
Il est assez fréquent que les logiciels malveillants s'introduisent dans l'ordinateur par l'intermédiaire d'autres logiciels malveillants préalablement installés

De tels cas peuvent se produire, par exemple, avec la famille de virus connus sous le nom de chevaux de Troie, qui donnent à l'attaquant le contrôle total du système, les téléchargeurs dont le seul but est de télécharger d'avantage des logiciels malveillantes, ou les backdoors, c'est-à-dire les portes dérobées qui sont laissées ouvertes sur l'ordinateur infecté dans le but de s'y introduire directement à l'avenir.

Dans le même temps, il est très fréquent que des programmes destinés à pirater des logiciels commerciaux soient infectés. Au premier abord, il peut sembler que ces programmes remplissent correctement leur fonction, mais c'est dans ces cas-là que les logiciels malveillants groupés peuvent ne pas être détectés, car le logiciel parvient en fait à fonctionner et à infecter le système en même temps.

Dans ce cas, une analyse plus approfondie du dossier est nécessaire. Il existe des services web qui analysent gratuitement un document suspect avec différents logiciels antivirus, comme http://www.novirusthanks.org/.

De même et pour un examen encore plus approfondi, il est possible d'utiliser le service de https://malwr.com/ dont la technologie met en œuvre un Sandbox avec Cuckoo (machine virtuelle) où l'échantillon est exécuté et analysé en détail (fichiers créés, logs modifiés, connexions, appels système, captures d'écran...), pour offrir des résultats beaucoup plus complets et approfondis.



[Figure 4]
Exemple d'analyse effectuée par "*malwr*"

4. Disinfection

4.1 Premières étapes

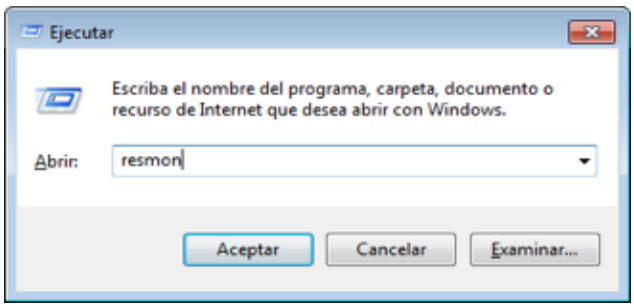
La première chose à faire si une infection est détectée est de déconnecter l'ordinateur du réseau, car le cryptage nécessite généralement la puissance de calcul de l'ordinateur infecté pour fonctionner. Cette procédure a plusieurs objectifs :

- **Empêcher le cryptage d'atteindre le contenu des lecteurs du réseau accessibles depuis l'ordinateur infecté.**

- **Empêchez les codes malveillants d'entrer en contact avec votre serveur de commande et de contrôle.**

L'analyse des processus en cours d'exécution sur l'ordinateur n'est généralement pas d'une grande aide pour diagnostiquer ce qui se passe, car dans la plupart des cas, les ransomwares sont généralement déguisés sous l'apparence d'un processus légitime tel que "explorer.exe". Si vous identifiez le processus qui accède massivement au disque, vous devez agir sur lui en le terminant[7].

Pour aider à identifier le processus nuisible, vous pouvez utiliser l'outil Windows Resource Monitor. Pour y accéder, il suffit d'exécuter "resmon" (touche Windows + r).

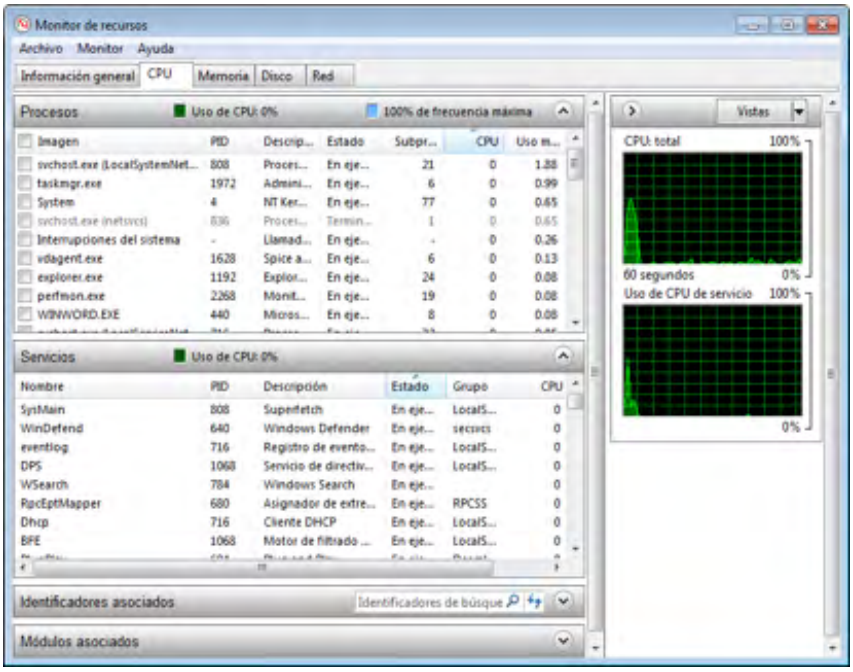


[Figure 5]
Fenêtre de commande "execute"

7. Fermez les processus avec le Gestionnaire des tâches, voir https://support.microsoft.com/es-es/kb/2499971.

Étant donné que l'opération de cryptage des fichiers nécessite du temps de traitement et un accès au disque, ces caractéristiques peuvent être utilisées pour identifier le processus ou l'application qui effectue l'attaque. Pour ce faire, il convient de prêter attention aux éléments suivants :

- **Processus d'application qui ne sont pas réellement en cours d'exécution :** si vous voyez un processus portant le nom d'une application dans la liste des processus, comme "notepad.exe" ou "calc.exe", par exemple, et que l'application n'est pas réellement ouverte, il s'agit très probablement d'un processus malveillant déguisé en application inoffensive.
- **Identifier les processus répétés avec un PID différent[8]:** si des processus portant le même nom apparaissent plusieurs fois, ils peuvent être identifiés par leur PID. Tous ces processus doivent dépendre de celui d'origine et faire partie de votre arbre de processus. S'il y en a un en dehors de cet arbre, il s'agit probablement d'un processus nuisible.
- **Processus avec un grand nombre de fichiers ouverts ou avec une utilisation excessive du CPU ou du disque :** le processus de cryptage est coûteux en termes de consommation de ressources, de sorte que le processus d'attaque utilisera une grande quantité de ressources, en particulier le CPU et l'accès au disque.



[Figure 6]
Image du moniteur
de ressources dans Windows 7

8. PID, "Process ID" : est un numéro d'identification unique qui représente chaque processus en cours. Voir https://www.computerhope.com/jargon/p/pid.htm

4.2 Identifier les ransomwares

Il est important de savoir quelle variante de ransomware a infecté les ordinateurs concernés. Pour ce faire, vous pouvez utiliser l'un des services suivants : **NoMoreRansom** ou **IDRansomware**.

Sur ces pages web, vous pouvez télécharger des fichiers et identifier à quelle famille appartient le code malveillant qui a infecté votre ordinateur et crypté vos fichiers. Dans ce cas, l'attaquant peut être identifié en fournissant un fichier crypté ou en envoyant le fichier contenant les instructions de rançon. Ces deux éléments sont suffisamment éclairants pour savoir s'il s'agit d'un attaquant connu.

Le fait de savoir quelle famille a attaqué les systèmes permet d'effectuer une recherche sur les détails et le comportement de ce code malveillant, et d'obtenir des informations précieuses (comme l'existence ou non d'un outil de décryptage et de récupération des fichiers).

.

4.3 Aspects à prendre en compte

4.3.1 La météo

Certaines variétés de ransomware utilisent le temps écoulé après l'infection comme facteur de pression pour obliger la victime à payer la rançon.

Il est préférable de profiter de cette période pour contacter les experts en cybersécurité et les autorités afin d'obtenir le plus d'informations possible sur des infections similaires et des conseils sur la marche à suivre dans de tels cas.

4.3.2 Suppression du code nuisible

En général, l'objectif principal d'un ransomware n'est pas de persister sur l'ordinateur infecté, car la demande de rançon elle-même révèle sa présence.

C'est pourquoi, dans la plupart des cas, leur suppression peut être simple et il existe généralement des outils de désinfection, spécialement développés à cet effet, mis à la disposition des victimes afin qu'elles puissent supprimer le code malveillant de l'appareil attaqué.

.

4.3.3 Récupération de fichiers

Une fois que le ransomware qui a infecté votre ordinateur a été identifié, vous pouvez consulter des sites Internet qui indiquent si la récupération (décryptage) des fichiers détournés est possible ou non à ce moment-là.

Si une telle récupération est possible, c'est grâce aux outils développés par des organisations aussi variées que Kaspersky[9], Intel Security, McAfee, Panda Security, Sophos, HitMan, des sociétés de lutte contre les logiciels malveillants, divers centres d'intervention connus sous le nom de CERT[10], des équipes de recherche telles que NoMoreRansom[11], des agences nationales et internationales d'application de la loi, des forums spécialisés tels que bleepingcomputer[12] et des chercheurs et analystes en sécurité, qui publient les clés maîtresses publiquement et de manière altruiste, parmi beaucoup d'autres.

9. Voir : http://www.kaspersky.es/
10. Voir : https://searchdatacenter.techtarget.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia#
11. Voir : https://www.nomoreransom.org/index.html
12. Voir : http://www.bleepingcomputer.com/

Il existe un utilitaire fréquemment mise à jour qui compile des informations sur toutes les familles de ransomware connues (outils de récupération, dates d'apparition, etc.). Il est recommandé de le consulter si vous avez été victime d'une infection, afin de connaître les informations disponibles sur l'attaque et, si nécessaire, d'obtenir un outil de récupération. Cet outil se trouve sur le lien suivant :

https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml

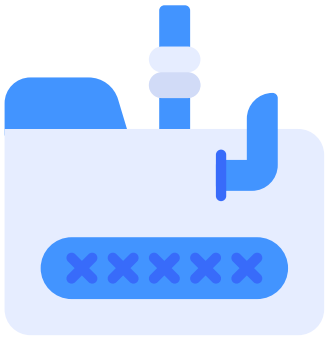
En outre, il est essentiel de consulter le document intitulé "CCN-CERT IA-11-18 Ransomware Security Measures", qui énumère de nombreuses autres ressources pour faciliter la récupération des fichiers, entre autres :

- http://files-download.avg.com/util/avgrem/avg_decryptor_Legion.exe
- https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor
- https://www.mcafee.com/us/downloads/free-tools/index.aspx
- https://decrypter.emsisoft.com/

Il est important de mentionner que si aucun outil de décryptage n'est disponible, il est déconseillé de payer, car cela ne fait qu'inciter les cybercriminels à continuer à créer des campagnes de ransomware.

En outre, le paiement de la rançon ne garantit pas la récupération des fichiers. Il existe des campagnes qui proposent non seulement de véritables outils de décryptage, mais qui sauvegardent également les données de la carte de crédit utilisée. Des pages TOR frauduleuses (liens anonymes où les paiements de rançon sont généralement effectués) ont également été détectées. Selon Symantec 2017, une entreprise sur cinq n'a pas réussi à récupérer ses fichiers après avoir effectué le paiement.

Paiement de la rançon ne garantit pas la récupération des fichiers



4.4 Atténuer les effets de l'infection

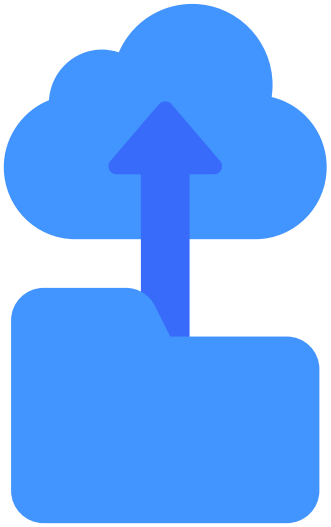
L'atténuation des effets de l'infection doit être comprise comme les actions qui permettent à la victime de réduire les effets de l'infection, en l'occurrence le nombre de fichiers cryptés, ou qui rendent possible une récupération totale ou partielle de l'infection.

Une fois que l'infection a eu lieu et que les fichiers ont été cryptés, ils peuvent être récupérés par différents moyens :

- Utilisation d'un outil de décryptage spécifique (section 4.3.3).
- Grâce à la restauration du système, qui vous permet de récupérer les fichiers cryptés.

Il existe plusieurs solutions pour une telle restauration :

- Si l'ordinateur infecté fonctionne sous Windows 7 ou une version antérieure, il existe une option préventive permettant d'activer et d'utiliser les "Shadow Copies".[13]
- Sur les systèmes Windows après la version 7, il est possible d'utiliser l'option Historique des fichiers.[14]
- Pour tout type de système d'exploitation et d'infrastructure, il est toujours possible d'utiliser des outils de sauvegarde.



13. Voir : https://www.welivesecurity.com/la-es/2017/09/26/shadow-copies-backup-windows-ransomware/
14. Voir : https://support.microsoft.com/en-us/help/17128/windows-8-file-history

5. Bonnes pratiques

Voici les principales mesures à prendre pour prévenir, détecter ou atténuer partiellement l'action des ransomwares :

1. **Conservez des copies de sauvegarde régulières** de toutes les données importantes. Il est nécessaire de conserver ces copies isolées et sans connectivité avec d'autres systèmes, évitant ainsi l'accès depuis des ordinateurs infectés.

2. **Maintenez le système à jour** avec les derniers correctifs de sécurité, tant pour le système d'exploitation que pour tout logiciel installé.

3. **Politiques BYOD (Bring Your Own Device).** Il est de plus en plus fréquent que les entreprises adoptent ce type de politique, qui permet aux travailleurs d'utiliser leurs appareils électroniques comme moyen de travail au sein de l'organisation. Ces appareils sont un vecteur potentiel d'infection et c'est pourquoi il est essentiel de définir des règles de sécurité.

4. **Mots de passe sécurisés**. Comme nous l'avons mentionné, l'attaque de services visibles depuis l'Internet avec des identifiants d'accès faibles (mots de passe non sécurisés) est une procédure de plus en plus courante.

5. **Maintenir une première ligne de défense avec les dernières signatures de code nuisible** (antivirus), en plus d'avoir une **configuration correcte des pare-feu** au niveau des applications (sur la base de listes blanches d'applications autorisées).

6. Mettez en **place des systèmes anti-spam au niveau du courrier électronique** et fixez un niveau de filtrage élevé. Cela réduit les risques d'infection par des campagnes de ransomware par courrier électronique de masse.

7. **Établissez des politiques de sécurité sur le système** pour empêcher l'exécution de fichiers provenant de répertoires couramment utilisés par les ransomwares (App Data, Local App Data, etc.). Des outils tels que AppLocker, Cryptoprevent ou CryptoLocker Prevention Kit vous permettent de créer facilement de telles politiques.

8. **Bloquez le trafic lié aux domaines et aux serveurs C2** à l'aide d'un IDS/IPS, empêchant ainsi la communication entre le code malveillant et le serveur de commande et de contrôle.

9. **N'utilisez pas de comptes dotés de privilèges d'administrateur**, ce qui réduit l'impact potentiel des ransomwares.

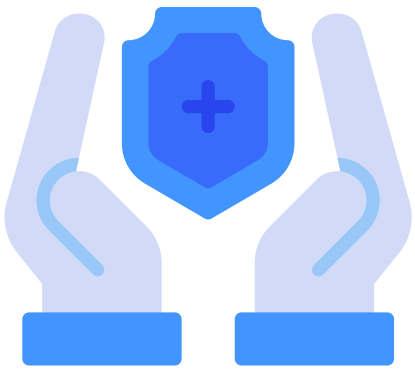
10. **Maintenir des listes de contrôle d'accès** pour les lecteurs mappés du réseau. En cas d'infection, le cryptage se produit sur tous les lecteurs réseau mappés de la machine victime. La restriction des privilèges d'écriture sur le réseau atténuera partiellement l'impact.

11. Nous recommandons **l'utilisation de bloqueurs de Javascript** pour le navigateur, comme "Privacy Manager", qui empêche l'exécution de tous ces scripts qui peuvent causer des dommages à notre ordinateur. Cela réduit les risques d'infection à partir du Web (Web Exploit Kits).

12. **Afficher les extensions des types de fichiers connus**, afin d'identifier les éventuels fichiers exécutables qui pourraient se faire passer pour un autre type de fichier.

13. En outre, il est recommandé **d'installer l'outil "Anti Ransom"**, qui tentera de bloquer le processus de cryptage d'un ransomware (en surveillant les "fichiers miel"). En outre, cette application effectue un vidage de la mémoire du code malveillant au moment de son exécution, dans lequel on peut espérer trouver la clé de cryptage utilisée.

14. Enfin, **l'utilisation de machines virtuelles** permet d'éviter l'infection par un ransomware dans un pourcentage élevé de cas. En raison des techniques d'anti-débogage et d'anti-virtualisation couramment présentes dans ce type de code malveillant, il a été démontré que dans un environnement virtualisé, son action ne se matérialise pas.



6. Sensibilisation

La sécurité d'une organisation repose, dans une large mesure et d'une manière ou d'une autre, sur les utilisateurs. Les sensibiliser aux menaces du monde numérique est une tâche essentielle qui doit être entreprise.

Il est de la plus haute importance que les personnes qui travaillent avec des ordinateurs connaissent les différentes techniques utilisées par les cybercriminels pour s'attaquer aux systèmes informatiques, qu'elles soient capables de les détecter et de les éviter afin de réduire le nombre d'infections.

Comme indiqué plus haut, de nombreuses stratégies utilisées par les attaquants font appel au facteur humain, notamment à l'ingénierie sociale, par exemple dans le cas d'e-mails frauduleux (phishing) ou de l'activation de macros dans un document bureautique infecté. Par conséquent, la sensibilisation des utilisateurs réduit considérablement le risque d'attaques.

On a également observé comment les cybercriminels ont pris conscience de la formation croissante de ces derniers et, par conséquent, ont utilisé des méthodes dans lesquelles l'interaction des personnes n'est pas nécessaire.

C'est un signe que le monde de la sécurité informatique est toujours en mouvement, et pour cette raison il est nécessaire que la formation du personnel d'une entreprise soit continue dans le temps et avec une certaine fréquence pour se tenir au courant des nouvelles menaces qui apparaissent jour après jour.

La sensibilisation à la composante humaine peut réduire considérablement le risque lié à la saisie de courriels, de documents et de tout autre téléchargement dans le système. Décrire la facilité avec laquelle nombre de ces attaques sont menées est l'un des meilleurs moyens de sensibiliser l'utilisateur aux conséquences d'une mauvaise utilisation des ressources du système.

Décrire la facilité avec laquelle nombre de ces attaques sont menées est l'un des meilleurs moyens de sensibiliser l'utilisateur aux conséquences d'une mauvaise utilisation des ressources du système

7. Copies de l'ombre

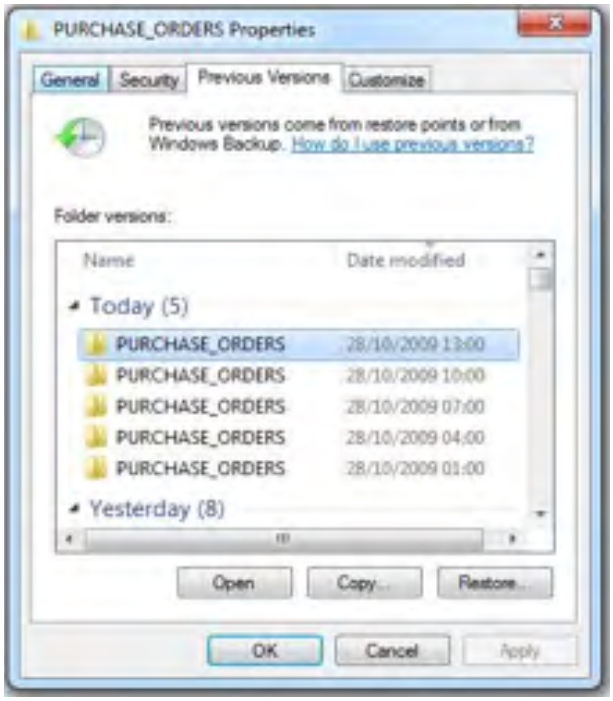
7.1 Systèmes d'exploitation Windows antérieurs à Windows 8

Dans les systèmes d'exploitation allant de Windows XP à Windows 7, tous deux inclus, une technologie appelée **Shadow Copies** est disponible, qui permet à l'utilisateur de faire, manuellement ou automatiquement, des copies des fichiers stockés sur l'ordinateur, même s'ils sont en cours d'utilisation. Ces copies sont réalisées afin de pouvoir les restaurer ultérieurement si un incident le rend nécessaire.

Il s'agit d'une mesure préventive facile à mettre en œuvre et qui ne nécessite pas de logiciel supplémentaire. Cependant, ce n'est pas une solution valable contre tous les types de ransomware ; par exemple, "CryLocker" et "CryptoWall" suppriment explicitement ces fichiers de restauration. Toutefois, il peut être utile dans le cas d'une infection par un ransomware qui ne modifie pas les **Shadow Copies**. Ils sont activés comme suit :

La technologie Shadow Copies permet à l'utilisateur de faire des copies manuelles ou automatiques des fichiers stockés sur l'ordinateur, même lorsqu'ils sont utilisés

1. À partir de **Démarrer**, le **Panneau de configuration** s'ouvre.
2. Vous accédez au **système**.
3. Sous Système, allez dans la section **Protection du système**.
4. Dans la section **Protection Settings** (Paramètres de protection), sélectionnez les lecteurs dont vous voulez faire des **Shadow Copies**.
5. Enfin, vous choisissez **Créer**.



[Figure 7] Copies fantômes dans Windows 7

Dans les cas où l'infection n'a pas affecté les *copies d'ombre*, l'effet de l'infection peut être combattu en restaurant ces copies sur un ordinateur préalablement désinfecté sans traces du code malveillant. Pour ce faire, suivez les instructions ci-dessous :

- Dans le menu **Protection du système** (après les étapes 1, 2 et 3 de sa création), choisissez l'option **Restauration du système**.
- Vous sélectionnez ensuite le **point de restauration** auquel vous souhaitez **revenir**.
- Elle est **confirmée** et attend l'achèvement du **processus de restauration**.

Pour plus d'informations sur l'utilisation des **Shadow Copies**, veuillez consulter l'article[15] de Microsoft sur ce service.

15. https://technet.microsoft.com/en-us/library/ee923636(v=ws.10).aspx

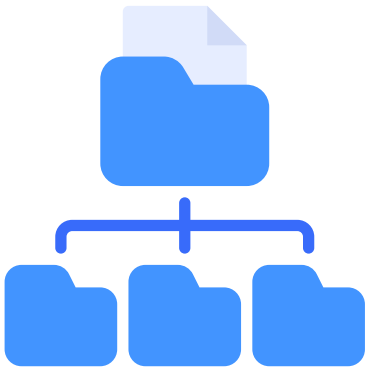
7.2 Systèmes d'exploitation Windows 8 ou ultérieurs

À partir de Windows 8, la fonctionnalité qui vous permet de faire différentes copies de fichiers s'appelle **Historique des fichiers** et consiste à stocker des sauvegardes **sur un support amovible**[16], ce qui constitue une grande différence par rapport à la même fonctionnalité dans les versions précédentes des systèmes d'exploitation Windows. En plus de cela, il est également possible d'activer les ***Shadow Copies*** mentionnées ci-dessus.

Avant d'utiliser l'**historique des fichiers**, il est nécessaire de choisir où les sauvegardes seront effectuées. Pour ce faire, vous pouvez sélectionner un **support amovible** tel qu'un disque externe ou une clé USB connectés à l'ordinateur, ou même un disque accessible sur le même réseau local auquel l'ordinateur est connecté.

Notez que l'**historique des fichiers ne copie que** les fichiers stockés dans les dossiers Documents, Musique, Images, Vidéos et Bureau, ainsi que les fichiers stockés sur ***OneDrive*** pour un accès hors ligne sur votre ordinateur.

File History permet de faire différentes copies des fichiers, en stockant les sauvegardes sur un support amovible



16. Voir : http://www.howtogeek.com/74623/how-to-use-the-new-file-history-feature-in-windows-8/

7.3 Backup generique

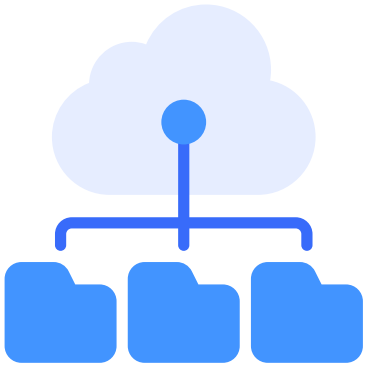
La mesure la plus efficace contre les ransomwares est de toujours avoir plusieurs copies de sauvegarde de tous les fichiers importants. L'extorsion ne se produit que lorsque l'attaquant du ransomware a réussi à crypter des **fichiers uniques et irrécupérables** et qu'il n'y a pas d'autre choix que de payer la rançon si vous voulez les récupérer. Il est essentiel de disposer d'au moins une **sauvegarde** de tous les fichiers importantes, afin de pouvoir s'appuyer sur cette sauvegarde en cas de besoin.

Les politiques de sauvegarde recommandent de toujours disposer de trois copies complètes et à jour, déposées en trois endroits différents et géographiquement distants, ainsi que d'être stockées sur deux types de supports différents et, surtout, d'**être toutes en dehors du réseau**. Par exemple, une possibilité, bien que ce ne soit pas la meilleure, serait d'utiliser simultanément votre propre ordinateur, un service de stockage en nuage et un support amovible.

Les sauvegardes doivent protéger à la fois leur **intégrité** et leur **confidentialité**, il est donc recommandé de les **chiffrer et de les signer de manière cryptographique**, en particulier si elles sont destinées à être stockées dans le nuage.

.

La mesure la plus efficace contre les ransomwares est de toujours avoir plusieurs copies de sauvegarde de tous les fichiers importants



Vous trouverez ci-dessous un certain nombre d'applications open source qui vous permettent d'effectuer des sauvegardes de manière efficace.

- **Amanda**[17]. Il s'agit d'un outil multiplateforme (Windows, Linux, macOS) qui vous permet de faire des copies sur des disques magnétiques, des bandes, des dispositifs optiques (DVD) et des systèmes de stockage en nuage.

- **BackupPC**[18]. Il s'agit d'un outil disponible pour Windows et Linux qui vous permet de faire des copies de sauvegarde de grandes quantités de données, en utilisant la compression de fichiers pour réduire la taille des informations à sauvegarder, ce qui réduit les coûts..

- **Bacula**[19]. C'est l'une des suites les plus utilisées dans l'environnement professionnel pour effectuer des sauvegardes. Il est disponible pour les environnements Windows, Linux et macOS.

- **FreeFileSync**[20]. Il s'agit d'un outil de synchronisation de dossiers qui vous permet de faire des copies de sauvegarde à la fois des ordinateurs locaux et des lecteurs du réseau. Ses fonctions les plus utiles sont l'automatisation des tâches, la création de rapports d'erreur détaillés et la possibilité d'utiliser des noms de chemin longs. Il est disponible pour Linux, Windows et macOS.

- **UrBackup**[21]**.** Cet outil vous permet d'effectuer des copies de sauvegarde en arrière-plan, pendant que vous travaillez, afin de ne pas interférer avec le travail de l'utilisateur. C'est un outil rapide et efficace, qui vous permet en même temps de faire des copies de sauvegarde sur Internet. Disponible pour Windows et Linux.

17. Voir : http://www.amanda.org/
18. Voir : https://backuppc.github.io/backuppc/
19. Voir : http://blog.bacula.org/
20. Voir : http://www.freefilesync.org/
21. Voir : http://www.urbackup.org/

7.4 Macro locking

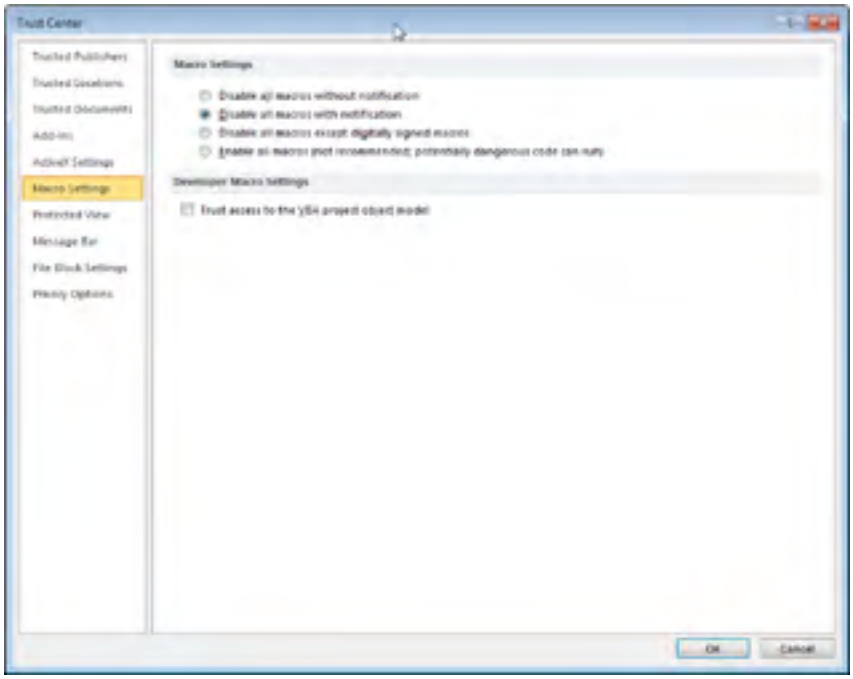
Depuis l'arrivée de la suite MS Office 2007, les documents se terminant par *.docx, .xlsx* et *.pptx* ne contiennent pas de macros[22], seulement ceux se terminant par "*.m*"[23], les macros sont désactivées par défaut. Il est préférable de travailler dans un environnement où les macros ne sont pas nécessaires.

Pour vous assurer que les macros sont désactivées[24], vous pouvez procéder comme suit

1. Sélectionnez l'onglet **Fichier** (MS Office 2013-2010) ou le **bouton Microsoft Office** (MS Office 2007).
2. Sélectionnez **Options** (MS Office 2013-2010), **Excel/ Word/... Options** (MS Office 2007).
3. Sélectionnez **Centre de confiance**, puis sélectionnez **Paramètres** du centre de confiance.
4. Sélectionnez **Macro Setup**.
5. Sélectionnez **"Désactiver toutes les macros sans notification"**.
6. **Acceptez**.
7. **Quittez** le programme et **redémarrez-le** pour vérifier la configuration choisie

22. Voir : https://support.microsoft.com/es-es/office/inicio-r%C3%A1pido-crear-una-macro-741130ca-080d-49f5-9471-1e5fb3d581a8
23. Voir : https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/
24. Voir : https://support.office.com/es-es/article/Habilitar-o-deshabilitar-macros-en-documentos-de-Office-7b4fdd2e-174f-47e2-9611-9efe4f860b12

[Figure 8]
Blocage des macros dans Microsoft Office



Si l'exécution du code VBA (macros) est nécessaire, il est recommandé de choisir l'option "**Désactiver toutes les macros avec notification**", afin de pouvoir examiner leur comportement a priori à l'aide d'outils tels que **OfficeMalScanner**. Si des macros sont nécessaires, la meilleure option est "**Désactiver toutes les macros, sauf les macros à signature numérique**".

Sur Internet, il existe des services qui permettent d'analyser le contenu de n'importe quel fichier[25], mais il y en a aussi d'autres qui se spécialisent dans l'analyse des macros nuisibles incluses dans les documents PDF, Word, Excel et PowerPoint. Dans tous les cas, il faut tenir compte du fait que lors de l'analyse du fichier, on perd le contrôle exclusif du fichier, il faut donc tenir compte du fait qu'il a **été rendu public**.

Certains de ces services sont les suivants :

- **Général** (http://www.document-analyzer.net/).
- **Doc** (https://malwaretracker.com/doc.php).
- **PDF** (https://malwaretracker.com/pdf.php).

25. Par exemple, voir https://www.virustotal.com/es/

7.5 La configuration correcte des comptes d'utilisateurs et de leurs autorisations

Tout système d'exploitation multi-utilisateurs (Windows en est un) doit suivre une politique d'autorisation aussi restrictive que possible, afin que les utilisateurs n'aient accès qu'aux ressources et fonctionnalités nécessaires à leur travail.

C'est ce que l'on appelle le ***"moindre privilège"*** et qui doit être appliqué dans tous les scénarios. Une mise en œuvre correcte de la politique de permissions peut empêcher qu'un utilisateur puisse infecter tout un réseau en cas de propagation d'un ransomware.

Vous trouverez ci-dessous une série d'adresses contenant des instructions sur la manière de gérer correctement les autorisations des utilisateurs sur des machines équipées de différentes versions du système d'exploitation Windows :

- **Windows 7:** http://www.welivesecurity.com/la-es/2015/05/22/como-administrar-permisos-usuarios-grupos-usuarios-windows-7/
- **Windows 10:** https://channel9.msdn.com/Blogs/MVP-LATAM/Administra-tus-cuentas-de-usuario-en-Windows-10

7.6 Les pots de miel ou les systèmes de piégeage

L'une des phases de tout processus de défense contre une attaque est la détection de l'attaque. En général, plus vite on sait que le système est attaqué, plus vite il pourra réagir en l'arrêtant ou en atténuant ses effets.

L'un des moyens de détecter les infections par ransomware consiste à installer un système de pot de miel[26], sur la machine, qui agit comme un leurre qui trahit la présence du code malveillant.

La mesure consiste à créer un dossier contenant divers fichiers attrayants pour le code malveillant, mais qui ne sont pas ceux utilisés par les utilisateurs de cette machine. Les actions sur ce dossier sont surveillées en temps réel, de sorte que lorsque le ransomware y accède pour les crypter, sa présence est détectée et il est arrêté.

Une des limites de cette mesure est qu'elle ne détecte pas les actions du code malveillant avant qu'il n'accède aux fichiers leurres et ne crypte une partie du système. Comme le contenu du dossier ne représente pas un pourcentage significatif de la totalité des fichiers, sa sensibilité dans la détection de l'attaque peut ne pas être élevée. Vous trouverez un exemple d'un tel outil à l'adresse suivante : http://www.security-projects.com/?Anti_Ransom

Si une infection est détectée, le programme affiche une alerte indiquant quel processus est en train de modifier l'un des fichiers appâts et offre la possibilité de mettre fin à ce processus ou de le laisser continuer.

[Figure 9] Anti-Ransomware

26. Voir : https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/

7.7 Une navigation sûre

L'une des méthodes d'infection les plus courantes utilisées par les ransomwares est l'exploitation des vulnérabilités des navigateurs web. Pour ce faire, on utilise des **kits d'exploitation**,[27] qui sont des programmes conçus pour exploiter les vulnérabilités connues des applications afin de prendre le contrôle total du système attaqué..

Cependantn'est pas la seule méthode d'infection liée aux navigateurs web, vous pouvez également utiliser le p hishing ou toute autre méthode qui se termine par l'exécution d'un code malveillant sur l'ordinateur de la victime (clés USB annoncées, données ou trouvées, pps à la mode, services web, etc.).

Pour se protéger de ce type d'attaque, la recommandation de base est de maintenir à jour à la fois le navigateur web et les extensions ou modules complémentaires qui y sont installés. De cette façon, toutes les corrections connues auront été appliquées au navigateur, ce qui réduira le nombre et l'étendue des points faibles que l'attaquant peut utiliser (**surface d'exposition**).

En outre, il est recommandé de faire usage d'extensions ou de compléments du navigateur web dont le but est d'accroître la sécurité de ceux-ci. Les extensions recommandées sont celles qui bloquent l'ouverture des fenêtres pop-up, comme **AdBlock**[28] (Google Chrome et Mozilla Firefox), qui empêcheraient le chargement de pages non demandées par l'utilisateur ou connues pour être nuisibles. En complément, pour éviter l'apparition de fenêtres pop-up, vous pouvez ajouter le plugin **PopUp Blocker**.

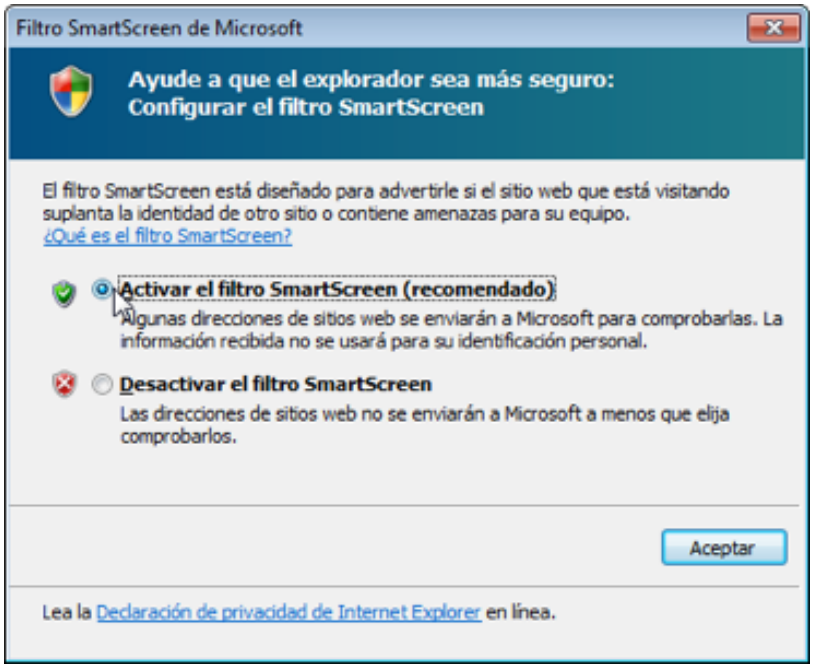
Il est également recommandé d'utiliser des extensions pour se protéger contre le p hishing (qui sont incluses dans les principaux navigateurs) et d'autres menaces, comme l'extension **Avast Online Security** pour Google Chrome.

L'une des méthodes d'infection les plus courantes utilisées par les ransomwaresest l'exploitation des vulnérabilités des navigateurs Web, àaide dekits d'exploitation

27. Voir : https://www.eset.com/bo/empresas/compania/kit-de-exploits-que-son-y-como-protegerse-de-ellos/
28. Voir : https://getadblock.com/

Si vous utilisez d'autres navigateurs qui n'autorisent pas ce type d'extensions, comme Internet Explorer, vous pouvez utiliser des outils tels que le filtre **SmartScreen**, qui indique si la page à laquelle vous accédez est légitime ou si elle se fait passer pour une autre. Pour activer ce filtre, sélectionnez l'onglet **Sécurité Filtre SmartScreen Activer le filtre.**

[Figure 10]
Blocage des macros dans Microsoft Office



Une mesure plus radicale, mais très efficace, consiste à désactiver l'exécution de **JavaScript**[29], pour qu'il ne soit activé que sur les sites Web de confiance. L'exécution de ce type de code est dangereuse car elle peut permettre l'activation automatique d'un code malveillant qui télécharge et exécute un ransomware sur la machine.

La désactivation de JavaScript peut être réalisée dans les paramètres du navigateur web lui-même ou en utilisant des extensions telles que **NoScript** (FireFox) et **ScriptSafe** (Chrome). Cette mesure, efficace pour empêcher l'exécution de codes nuisibles, est la plus intrusive pour l'utilisateur et peut causer des problèmes avec certains de vos sites web habituels, en les empêchant de s'afficher comme ils le devraient ou en éliminant certaines fonctionnalités.

Parmi ces fonctionnalités figurent certains plugins, la visualisation de données, les présentations web, les moteurs de recherche et les éléments graphiques en général. La désactivation de JavaScript donne donc un aspect beaucoup plus plat au site Web.

29. Voir : https://developer.mozilla.org/es/docs/Learn/JavaScript/First_steps/What_is_JavaScript

7.8 Extensions de fichiers connues

L'occultation est une technique de tromperie largement utilisée par les logiciels malveillants en général et par le p hishing en particulier. L'idée est de cacher un fichier exécutable, sous l'apparence d'un autre non exécutable et apparemment inoffensif.

Pour la commodité de l'utilisateur, dans les systèmes d'exploitation actuels, les extensions de fichier les plus courantes sont omises du nom de fichier et leur icône est choisie pour être la plus représentative de ce type de fichier.

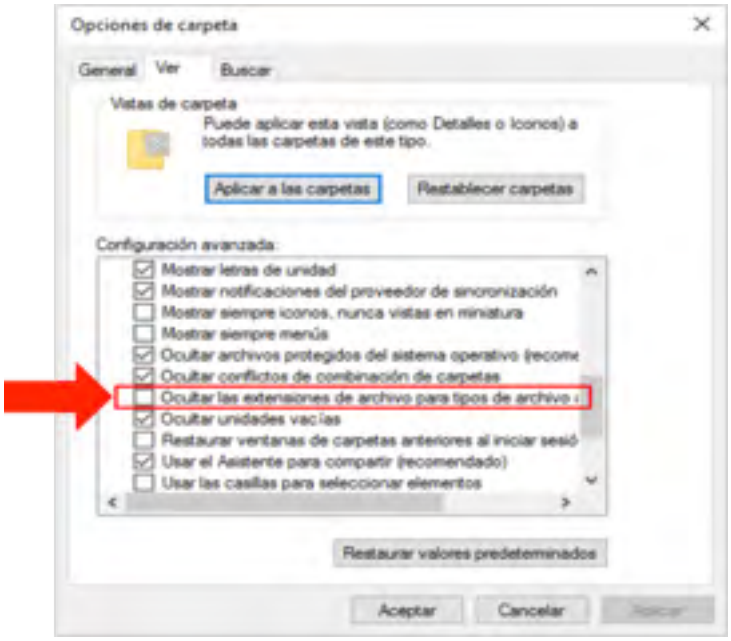
Ce comportement peut être utilisé pour faire croire à l'utilisateur qu'un fichier est autre chose que ce qu'il est réellement ; par exemple, un processus exécutable pourrait prétendre être une image en ayant un nom se terminant par "*.jpg*", mais être en réalité un fichier se terminant par "*.jpg.exe*" qui est quelque chose de complètement différent. En activant l'option de masquage des extensions connues, l'utilisateur ne verra pas qu'il s'agit d'un exécutable et non d'une image.

Pour afficher les extensions cachées, vous devez accéder aux options du dossier dans l'Explorateur Windows. Le moyen le plus simple est de choisir, à partir de la barre d'outils de n'importe quelle fenêtre de l'Explorateur, l'option **Options des dossiers** dans le menu **Affichage**. Une fois dans les options du dossier, dans la section Affichage, l'option **Masquer les extensions des fichiers connus** doit être décochée.

Une autre façon d'abuser de ce comportement consiste à créer des raccourcis dont l'icône est modifiée pour faire croire à l'utilisateur qu'il s'agit d'un type de fichier connu. Pour distinguer un fichier d'un raccourci, il suffit de regarder le coin inférieur gauche de l'icône qui, s'il s'agit d'un raccourci, affichera un indicateur en forme de flèche et ne devrait pas être utilisé à moins que vous ne soyez sûr de sa provenance.

L'occultation est une technique de tromperie largement utilisée par les logiciels malveillants en général et par le phishing en particulier

[Figure 11]
Option permettant de ne pas masquer les extensions connues



7.9 Applocker

AppLocker[30] est une application introduite dans Windows Server 2008 R2 et Windows 7 qui étend ses fonctions de contrôle des applications et ses politiques d'exécution.

Cet outil permet de créer des règles basées sur les attributs des fichiers (nom, signature numérique, etc.) pour contrôler l'accès aux logiciels installés sur l'ordinateur. Ce contrôle permet, parmi de nombreuses options, de bloquer l'accès à un programme ou à un service particulier. Des informations détaillées sur AppLocker sont disponibles sur le lien suivant :
https://technet.microsoft.com/es-es/library/mt431725(v=vs.85).aspx6

30. Voir : https://msdn.microsoft.com/es-es/library/ee424367(v=ws.11).aspx

7.10 Politiques BYOD

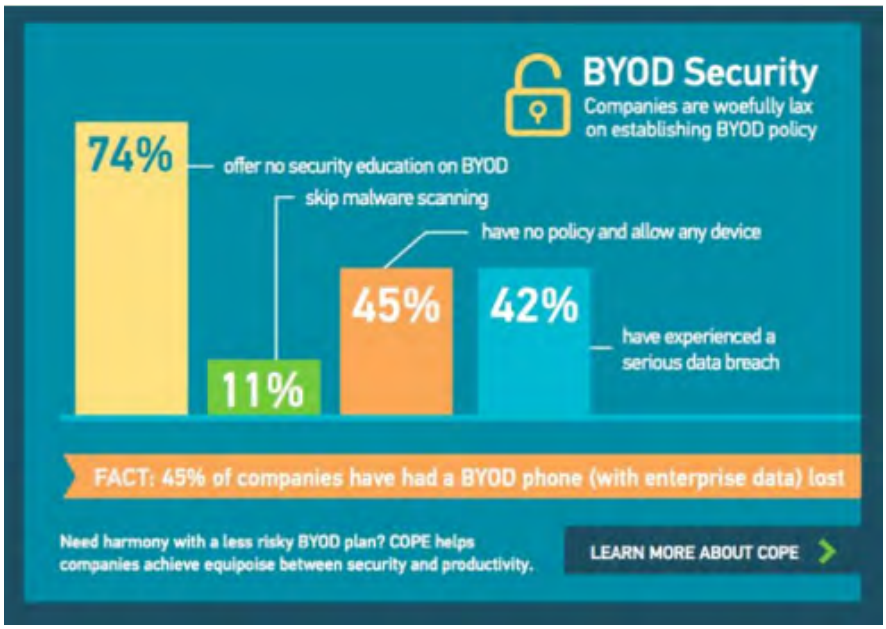
À mesure que le BYOD se développe (pas moins de 74 % des organisations ont mis en place de telles politiques ou prévoient de le faire à l'avenir), les employeurs ou les responsables d'organisations doivent s'assurer que leurs employés et l'entreprise elle-même sont correctement protégés contre les nouveaux risques auxquels ils s'exposent.

Ces risques peuvent comprendre :

- Perte d'informations sur les clients ou les entreprises.
- Accès non autorisé au réseau de l'entreprise.
- Infections par des logiciels malveillants.

Avec l'expansion du BYOD, les employeurs ou les responsables d'organisations doivent s'assurer que leurs employés et l'entreprise elle-même sont protégés de manière adéquate contre les nouveaux risques auxquels ils sont exposés

[Figure 12] Statistiques sur les politiques dérivées de la mise en œuvre du BYOD



Voici quelques recommandations pour atténuer les risques autant que possible :

1. Veillez à ce que les appareils ne soient pas déverrouillés sans saisir un code PIN, un motif ou un mot de passe. Cela semble être une évidence, mais plus de 30 % des utilisateurs ne mettent pas en place de protection d'accès sur leur appareil parce que c'est plus compliqué.
2. Surveillez les connexions effectuées, notamment au niveau des points d'accès Wi-Fi, qui doivent être correctement configurés et toujours protégés par un mot de passe. D'autres contrôles peuvent également être mis en œuvre, comme le contrôle d'accès par liste blanche ou le filtrage MAC.
3. Des sauvegardes régulières.
4. Il est intéressant de disposer de services tels que "Find my device", mis en œuvre par de nombreux smartphones Android, qui peuvent être localisés (même sans avoir de GPS activé) par le biais du compte Google associé, donnant même lieu à la possibilité de supprimer les informations si nécessaire..
5. Les données relatives à l'entreprise ne doivent jamais être stockées sur des appareils destinés à être utilisés en dehors de l'entreprise.
6. Disposer d'un antivirus spécifique pour les appareils mobiles ou les tablettes.
7. Il existe de nombreuses applications commerciales qui analysent le système à la recherche de codes malveillants et qui offrent une protection supplémentaire contre les menaces les plus courantes. Bien que le fait de disposer de ce type de logiciel ne garantisse pas que vous soyez à l'abri des attaques, il s'agit d'une mesure essentielle..
8. Comme nous l'avons déjà mentionné, il convient d'utiliser un logiciel qui offre un MDM, tel que Docker ou Sandbox. L'équipe informatique doit évaluer les différentes possibilités et les examiner en profondeur pour choisir la meilleure option.

Pour plus d'informations, vous pouvez consulter le guide CCN sur la sécurité d'Android Guide CCN-STIC 453C.

7.11 Mots de passe sécurisés

Comme nous l'avons mentionné, il est important de disposer d'identifiants d'accès robustes aux services déployés par l'organisation. également essentiel de veiller à ne jamais utiliser des utilisateurs et des mots de passe qui sont déjà configurés par défaut ; vous devez les réinitialiser. Voici quelques conseils pour choisir un mot de passe sûr :

- **Utilisez une combinaison de caractères alphanumériques : il est impératif que les mots de passe ne se limitent pas à une séquence de lettres ou de chiffres uniquement.**
- **Utilisez des mots de passe différents pour chaque service.**
- **La longueur ne doit pas être inférieure à 12 caractères.**
- **Utilisation de symboles pour rendre la force brute plus difficile, ainsi que l'alternance de majuscules et de minuscules.**

Idéalement, le mot de passe doit être aléatoire. Vous pouvez tester la robustesse de la séquence choisie dans des services web tels que http://password-checker.online-domain-tools.com/ où vous pouvez estimer la difficulté pour un attaquant de la deviner par force brute ou par attaque par dictionnaire (il est recommandé d'utiliser un mot de passe similaire et non le mot de passe final).

En suivant ces étapes, on peut atténuer considérablement les attaques contre des services tels que le RDP mentionné plus haut.

> **Il est important de disposer d'identifiants d'accès robustes aux services déployés par l'organisation**

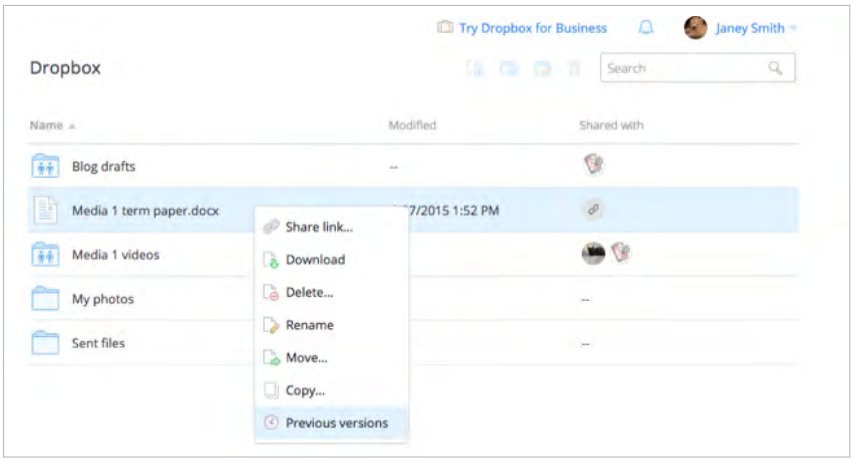
7.12 Récupération de fichiers via le stockage en nuage

Depuis quelque temps, il est très courant d'utiliser des[31] **services de synchronisation de fichiers**[32] ou de stockage en nuage.

Lorsque vous avez synchronisé le contenu d'un dossier local avec un autre dans le nuage, les deux emplacements contiennent les mêmes fichiers. Si un ordinateur local est attaqué par un agent ransomware, les copies locales seront cryptées et, par la suite, le système de synchronisation copiera ces mêmes fichiers sur le nuage, en supprimant les précédents, de sorte que les copies sur le nuage finiront également par être cryptées.

Cependant, la suppression de fichiers est une action apparente dans nombre de ces services de stockage en nuage, car il s'agit en réalité d'un système de fichiers à contrôle de version[33].

[Figure 13]
Contrôle de version dans Dropbox



31. Voir : https://support.microsoft.com/es-es/office/v%C3%ADdeo-%C2%BFqu%C3%A9-es-la-sincronizaci%C3%B3n-de-archivos-7b265f0e-2e36-478a-8857-7026b9ec831c
32. Voir : https://azure.microsoft.com/es-es/overview/what-is-cloud-storage/
33. Voir : https://www.techopedia.com/definition/1861/versioning-file-system

Dans ces systèmes, les fichiers supprimés ne sont pas réellement supprimés, mais sont stockés en tant que version antérieure qui reste accessible à l'administrateur du service en nuage

Dans ce cas, selon la politique du fournisseur de services, il est parfois possible de supprimer les versions cryptées (détournées) du nuage et de récupérer les versions précédentes des mêmes fichiers.

Dropbox[34] et **Google Drive**[35] offrent tous deux des possibilités à cet égard. Vous devez donc toujours envisager la possibilité de restaurer ce que vous aviez synchronisé dans le nuage. Évidemment, l'opération de restauration doit être effectuée après que l'ordinateur affecté ait été complètement nettoyé.

7.13 Quand tout semble perdu

Une fois que le système a été infecté et que le ransomware a réussi à crypter l'ensemble du système de fichiers accessible, il se peut qu'en consultant les forums spécialisés, il n'existe pas d'antidote permettant de récupérer les informations. Dans ce cas, il **n'est pas conseillé de procéder à la suppression des fichiers concernés**.

Le fait qu'un outil permettant de décrypter les fichiers détournés n'existe pas pour le moment ne signifie pas qu'il ne pourra pas exister dans un avenir proche. Dans ce cas, il est préférable de ne pas détruire la seule copie existante des fichiers, même si elle est cryptée avec une clé qui n'est pas disponible à ce moment-là.

Le plus recommandé est :

1. **Copiez tous les fichiers cryptés sur un disque externe vide.**
2. **Nettoyez et désinfectez le matériel infecté.**
3. **Sécurisez une copie de sauvegarde des fichiers cryptés jusqu'à ce qu'un moyen de récupérer ces fichiers soit connu.**

34. Voir : https://www.dropbox.com/help/11
35. Voir : https://support.google.com/docs/answer/190843?hl=es

8. Conclusion

Lorsqu'il s'agit d'assurer la sécurité d'un système informatique, il est nécessaire d'appliquer toutes les mesures disponibles et, si possible, de les organiser en couches afin de rendre difficile la réussite de toute attaque.

De plus, une détection rapide de l'infection peut l'arrêter, en limitant le nombre de fichiers affectés. À ce stade, l'ordinateur est entièrement nettoyé et l'on tente de récupérer les fichiers qui ont été affectés.

Le risque réel d'un ransomware étant qu'il détourne **la seule copie disponible d'un fichier**, toute la résilience du système dépend du maintien de **sauvegardes** correctement **mises à jour, cryptées** et **signées, hors** de portée **(hors ligne)** de votre ordinateur. Une bonne sauvegarde des fichiers importants fait d'une attaque par ransomware une nuisance plutôt qu'une catastrophe. Enfin, pour vous tenir au courant des mesures de sécurité contre les ransomwares, nous vous recommandons de lire le rapport sur les menaces IA-11/18 de CCN-CERT.

Lorsqu'il s'agit d'assurer la sécurité d'un système informatique, il est nécessaire d'appliquer toutes les mesures disponibles et, si possible, de les organiser en couches afin de rendre difficile la réussite de toute attaque

9. Décalogue de sécurité de base

Ce Décalogue des bonnes pratiques a pour but de jeter les bases des mesures de sécurité contre les ransomwares

1. Informer et sensibiliser tous les utilisateurs aux risques et aux menaces que représentent les ransomwares, afin que leur état de conscience, leur vigilance et leur formation réduisent les possibilités d'infection.
2. Maintenir un système de sauvegarde à jour des systèmes locaux et des sites distants. Si possible, au moins deux sauvegardes doivent être conservées dans des endroits différents et déconnectées du système.
3. Désactiver les macros dans les documents Microsoft Office et autres applications similaires.
4. Désactivez Windows Script Host pour empêcher l'exécution de scripts sur le système. Pour ce faire, vous pouvez suivre les étapes décrites dans le lien suivant de Microsoft : https://technet.microsoft.com/es-es/library/ee198684.aspx
5. Suivez les recommandations publiées sur la protection du courrier électronique. (voir le guide CCN-CERT BP-02/16)
6. Complétez votre antivirus et votre pare-feu personnels avec des programmes tels que Applocker (blocage de l'exécution des programmes) et EMET (détection et blocage des techniques d'exploitation).
7. Maintenez un comportement de navigation sécurisé, en utilisant des outils et des extensions de navigateur web entièrement mis à jour qui contribuent à empêcher l'exécution de code non autorisé dans le navigateur web. (voir le guide CCN-CERT BP-06/16)
8. Activez l'affichage des extensions de fichiers pour empêcher l'exécution d'un code malveillant déguisé en fichier légitime non exécutable.
9. Configurez l'UAC (User Access Control) de Windows de manière aussi restrictive que possible, en demandant toujours une confirmation pour l'exécution des processus qui nécessitent des privilèges élevés.
10. Maintenez le système d'exploitation et toutes les solutions de sécurité à jour, ainsi que le pare-feu personnel activé. N'utilisez pas les utilisateurs et les mots de passe par défaut.

CCN
centro criptológico nacional

CCN-CERT
centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es


ccn-cert
centro criptológico nacional
CCN
centro criptológico nacional