CCN-CERT

BP/21

Gestion des incidents liés aux ransomwares

RAPPORT DE LES MEILLEURES PRACTIQUES

AVRIL **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Centre National de Cryptologie, 2019

Date de sortie: mayo de 2021

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.

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 et 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. L'étendue de l'incident

Pour déterminer la **portée d'un** incident impliquant un ransomware, il est nécessaire de collecter :

- **Informations de base sur l'incident.**
- **Informations techniques sur l'infection.**
- **Informations sur le réseau où l'infection s'est produite.**

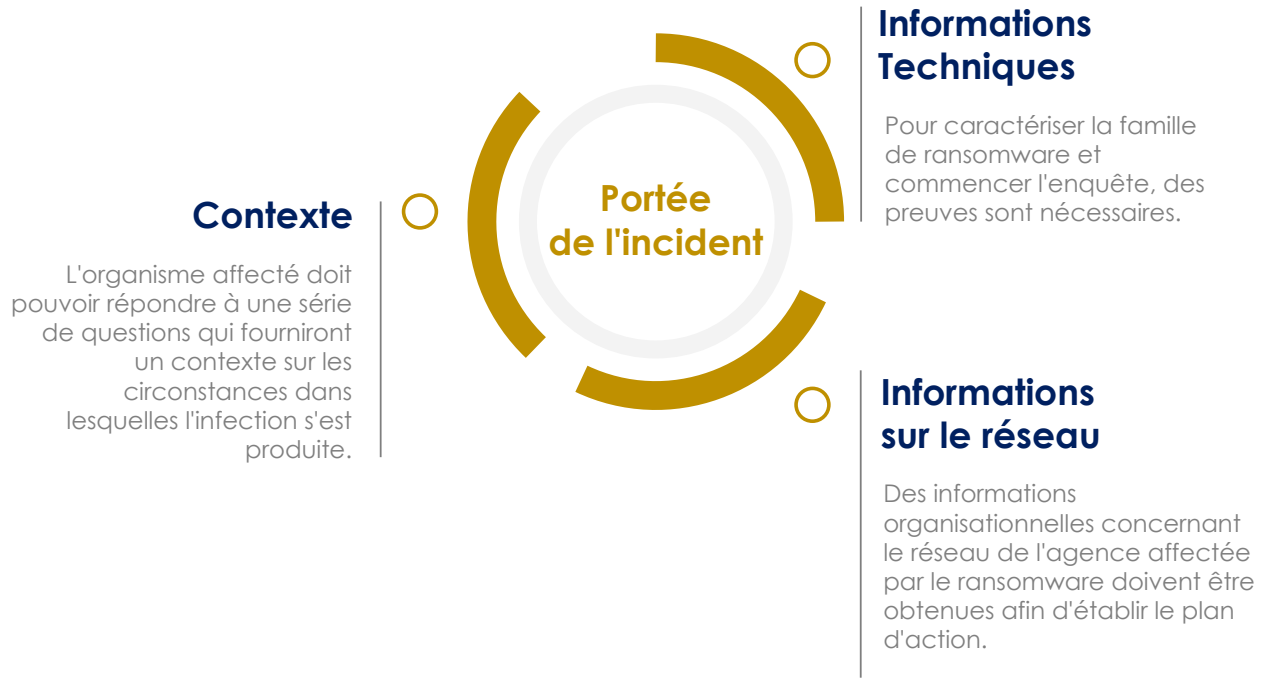


Figure 1. L'étendue de l'incident

2.1 Contexte de l'incident

L'organisme affecté doit pouvoir répondre aux questions suivantes qui fourniront un **contexte sur les circonstances** dans lesquelles l'infection s'est produite:

Quand l'infection s'est-elle produite?

Comment l'infection s'est-elle produite (pièce jointe d'un courriel, RDP, etc.)?

Combien d'équipes sont concernées?

Une sauvegarde des données cryptées est-elle disponible?

Des mesures d'atténuation ont-elles été prises?

2.2 Des informations techniques sur l'infection

En plus de répondre aux questions ci-dessus, pour caractériser la famille des ransomwares et commencer la recherche, les **éléments** suivants sont nécessaires:

Note de rançon d'un ransomware.

Echantillons de fichiers cryptés (pas plus de 2 mégaoctets).

Echantillon du ransomware, email de phishing, fichier bureautique ou tout élément permettant d'analyser le code malveillant.

2.3 Informations sur le réseau

Enfin, il est nécessaire d'obtenir les informations organisationnelles suivantes concernant le réseau de l'organisation touchée par le ransomware afin d'établir le plan d'action:

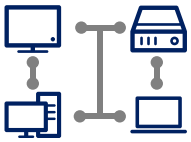


Diagramme de réseau

Diagramme montrant les composants qui constituent le réseau de communication et la manière dont ils interagissent entre eux, notamment les routeurs, les pare-feu, les serveurs, les postes de travail et leurs connexions. Des exemples de diagrammes de réseau sont inclus dans l'ANNEXE I.

Liste des serveurs et des principaux actifs

Tableau indiquant l'IP, le domaine, le nom de l'équipement et la localisation. Un exemple de tableau qui peut être utilisé est inclus dans l'ANNEXE II.

Adressage public, IP et domaines

Liste des adresses et des domaines exposés à l'Internet.

Les journaux

Des systèmes de sécurité présents sur le réseau:

- **o Antivirus, EDR**
- **o Pare-feu, proxy, DNS, IDS/IPS**
- **o Antispam, quarantaine de courrier**
- **o Accès à distance (VPN, SSH, Teamwiewer, etc.)**
- **o Copie du trafic**

3. Lignes directrices

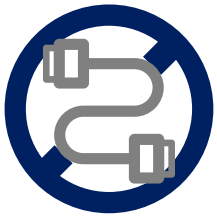
Nous allons travailler sur les **lignes d'action** suivantes, en définissant une équipe pour mener chaque tâche et en désignant un chef d'équipe :

Figure 2. Lignes d'action

3.1 Endiguement des menaces

La phase de confinement est la première phase qui est effectuée pour s'assurer que:

Le code malveillant ne continue pas à se propager sur le réseau (cryptage des dossiers partagés, déplacement latéral vers des ordinateurs à visibilité, etc.)



Dans l'éventualité où un attaquant obtiendrait un accès à distance au réseau, celui-ci serait immédiatement fermé pour empêcher toute activité ultérieure (exfiltration d'informations, déploiement de portes dérobées supplémentaires, suppression ou destruction de preuves, etc.)

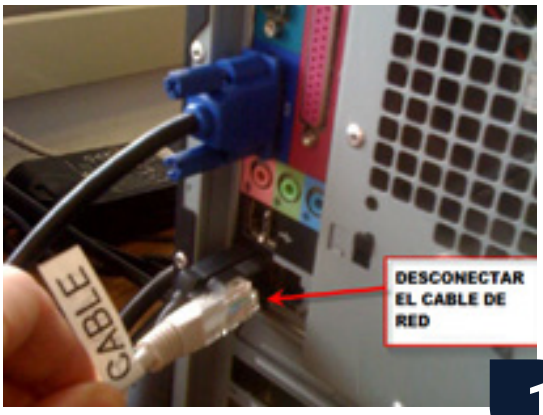
Pour ce faire, et notamment dans les incidents de sécurité dans lesquels un spécimen de ransomware est impliqué, il est nécessaire de procéder immédiatement, en effectuant les actions détaillées dans les sections suivantes.

3.1.1 Déconnecter l'équipement du réseau

Lorsqu'une infection par un ransomware se produit, les fichiers de l'ordinateur et ceux stockés sur les lecteurs connectés, qu'il s'agisse de périphériques physiques (USB, disques durs externes, etc.) ou de lecteurs réseau, commencent à être chiffrés.

Dans la grande majorité des cas, vous vous rendez compte de l'infection lorsque le ransomware a fini de s'exécuter et que tous les fichiers ont été chiffrés. Toutefois, il est possible que le ransomware n'ait pas encore fini de s'exécuter, ce qui permet, dans le meilleur des cas, de récupérer la clé de chiffrement ou d'empêcher le chiffrement d'autres fichiers.

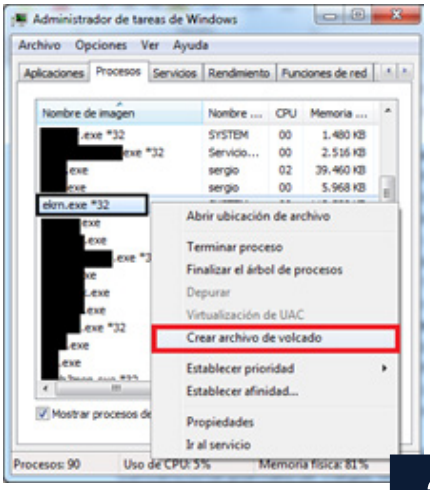
Les étapes générales suivantes sont recommandées pour la détection des ransomwares:



1

Déconnectez les lecteurs réseau

Cela signifie "tirer le câble réseau" (ou désactiver les interfaces sans fil). Cela peut empêcher le cryptage des fichiers sur les lecteurs réseau accessibles si le ransomware n'a pas encore fini de s'exécuter.

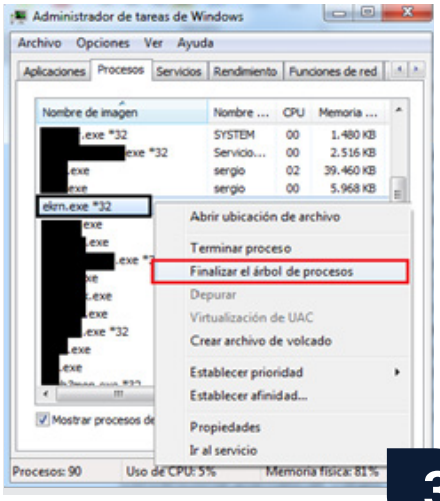


2

Vérifiez si le processus malveillant est toujours en cours

Cette tâche n'est pas facile dans de nombreux cas, car le processus malveillant peut s'être injecté dans un processus légitime ou avoir simplement terminé son exécution.

Toutefois, si le processus en question est identifié (à l'aide d'outils tels que Process Explorer de Sysinternals), une vidange du processus nuisible sera effectuée à partir du gestionnaire des tâches de Windows. Pour ce faire, faites un clic droit sur le processus et sélectionnez l'option "Créer un fichier de vidage" (il sera enregistré dans %TMP%). Une fois que le fichier a été vidé, il doit être stocké en toute sécurité sur un système isolé.



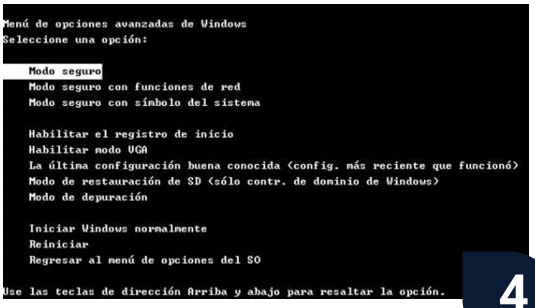
3

Terminer l'exécution du processus nuisible

Il existe deux possibilités pour cela:

I. Si le processus a été identifié, il suffit d'arrêter son exécution à partir du Gestionnaire des tâches de Windows : faites un clic droit sur le processus et sélectionnez l'option "Terminer l'arborescence du processus".

II. Si le processus n'a pas pu être identifié, il est recommandé d'arrêter l'équipement manuellement et immédiatement.



4

Démarrez l'ordinateur en mode sans échec

Avant que Windows ne démarre de manière classique (écran de chargement), appuyez sur la touche F8 pour accéder au menu de démarrage avancé, dans lequel vous pouvez sélectionner le "Mode sans échec". Cela empêchera le ransomware de redémarrer à nouveau s'il est persistant.

5

Sauvegardez votre ordinateur

Cette copie contiendra tous les fichiers cryptés et non cryptés, et doit être effectuée sur un dispositif de stockage externe isolé du réseau. **Dans le cas où les fichiers ne peuvent pas être décryptés, il est important de les conserver car le cryptage** peut être cassé ou les clés C&C peuvent être libérées à l'avenir.

3.1.2 Segmentation du réseau

C'est probablement le point le plus fondamental à souligner.

En général, les rançongiciels peuvent se propager sur le réseau par le biais des lecteurs partagés du domaine. Cependant, les tendances indiquent que dans les récentes campagnes impliquant des ransomwares, il peut également y avoir un **code malveillant supplémentaire** avec des capacités et une complexité plus grandes. Il a été observé que, dans certains cas, la menace peut élever les privilèges, se déplacer latéralement sur le réseau en utilisant des informations d'identification compromises, démarrer des ordinateurs hors du réseau en utilisant WoL (*Wake on Lan*) et exfiltrer des informations.

Les gestionnaires de systèmes doivent redessiner le réseau et déterminer le point idéal pour installer le pare-feu. Le pare-feu permettra de voir tout le trafic réseau qui le traverse, ce qui sera particulièrement utile en cas de présence d'IOC (indicators of compromise, pour son acronyme en anglais) pour localiser les ordinateurs du réseau qui tentent d'établir des communications avec des serveurs de commande et de contrôle (C2) connus.

Les tendances indiquent que dans les récentes campagnes impliquant des ransomwares, il peut également y avoir un code malveillant supplémentaire avec des capacités et une complexité plus grandes.

3.1.3 Déploiement d'une solution d'EDR et d'un vaccin pour le CCN-CERT

Pour conclure la phase de confinement, il est recommandé de déployer une solution EDR (*Endpoint Detection and Response*) sur les terminaux, les machines clientes et les serveurs, afin d'améliorer les capacités de détection et d'isolation.

De son côté, le CCN-CERT distribue des vaccins spécifiques pour chaque cas de ransomware via son outil **MicroClaudia**. MicroClaudia génère des actions qui **permettent le blocage immédiat de tout logiciel malveillant** lié à **Emotet**, **Trickbot**, **Bitpaymer**, **Ryuk** et **Sodinokibi** afin que leur exécution puisse être arrêtée au cas où les ordinateurs seraient infectés ou que le code nuisible tenterait de se propager.

3.2 Détection des menaces

Après la phase de confinement, nous procédons à la d**étection des ordinateurs qui ont été affectés** par le code malveillant, soit parce que l'attaquant les a utilisés pour pivoter dans le réseau, soit pour chiffrer et/ou supprimer leur contenu.

Au cours de cette phase, les tâches suivantes sont effectuées.

3.2.1 Installation de la sonde CCN-CERT (SAT)

Le CCN-CERT dispose d'une sonde, Early Warning System, qui remplit les fonctions d'un IDS (*Intrusion Detection System*) et peut être déployée à un point d'interconnexion du réseau où il y a une visibilité de tout le trafic entrant et sortant.

Cette sonde permet d'identifier si, sur la base des modèles connus par le CCN-CERT, il y a du trafic catégorisé comme nuisible dans le réseau, de sorte qu'il puisse agir en temps utile pour localiser et neutraliser la menace ultérieurement.

3.2.2 MicroClaudia installation

Le CCN-CERT met à disposition son outil pour distribuer des vaccins spécifiques à chaque ransomware et ainsi empêcher l'exécution de ce dernier.

L'outil est installé dans les ordinateurs finaux et contient des détecteurs d'actions basés sur la recherche des différents ransomwares.

L'équipe de **MicroClaudia** ajoute de **nouveaux vaccins sur la base de l'analyse d'échantillons émergents**.

3.2.3 Caractérisation du code nuisible

Le CCN-CERT dispose de rapports de codes nuisibles (ID) sur son portail (https://ccn-cert.cni.es) liés à différentes familles de ransomware.

Ces rapports compilent toute la caractérisation de la menace, y compris les **caractéristiques**, la **fonctionnalité**, la **connectivité**, la **persistance et les indicateurs** qui **permettent la détection**.

Il existe plusieurs pages qui peuvent aider à identifier la famille de ransomware impliquée dans l'incident, à partir d'un exemple de fichier, les plus efficaces et recommandées sont:

nomoreransom.org

Lien: https://www.nomoreransom.or/crypto-sheriff.php

IDRansomware

Lien: https://id-ransomware.malwarehunterteam.com

Des **fichiers cryptés** et **des notes de rançon** peuvent être téléchargés sur ces pages. De cette façon, et grâce au type de cryptage et à la méthode du ransomware, il est possible de savoir quel type de famille est responsable de l'infection.

3.3 Atténuation des menaces

Parallèlement au confinement et à la détection de la menace, il est possible de procéder à la phase d'atténuation, qui consiste à neutraliser efficacement le logiciel malveillant déployé par l'attaquant. Pour ce faire, les étapes suivantes peuvent être suivies:

3.3.1 Reconcevoir le réseau en segmentant les différents environnements

Dans un réseau non segmenté, il est trivial pour un attaquant d'avoir une visibilité sur tous les actifs, même s'ils ont des adresses différentes.

Une fois que l'attaquant a obtenu les informations d'identification du domaine, en compromettant préalablement un ordinateur du réseau, il peut commencer à se déplacer latéralement, à la recherche des ordinateurs les plus intéressants pour voler, crypter ou supprimer du contenu.

Compte tenu de la nature des ordinateurs et des serveurs (DMZ, LAN, DC et serveurs, etc.), si le réseau est correctement segmenté à l'aide d'éléments de réseau tels que des pare-feu et en séparant les différents environnements et l'adressage, l'impact potentiel qui pourrait résulter d'une infection par ransomware serait plus faible que dans le cas d'un réseau plat. En fait, la segmentation permettrait de délimiter et d'isoler les ordinateurs affectés lors d'un incident de sécurité, ce qui empêcherait le code malveillant de se propager dans le réseau et d'en prendre finalement le contrôle après la compromission du contrôleur de domaine (DC).

Idéalement, les politiques de pare-feu devraient être ajustées selon une approche basée sur une ***liste blanche***, c'est-à-dire en autorisant uniquement les connectivités qui sont essentielles dans chaque cas pour le bon fonctionnement et l'exploitation des équipements du parc.

Idéalement, les politiques de pare-feu devraient être ajustées selon une approche basée sur une *liste blanche*, c'est-à-dire en autorisant uniquement les connectivités qui sont essentielles dans chaque cas.

3.3.2 La mise à jour et la correction des équipements

Le parc d'équipements comporte souvent un ensemble très hétérogène de versions de dispositifs et de systèmes d'exploitation.

Cela signifie que, dans certains cas, le niveau des correctifs n'est pas uniforme ou que la prise en charge des mises à jour de sécurité n'est plus disponible.

Il est **essentiel** que le **support et la maintenance sous** forme de correctifs et de mises à jour continuent d'être fournis périodiquement aux équipements du parc.

Il est essentiel que le support et la maintenance sous forme de correctifs et de mises à jour continuent d'être fournis périodiquement aux équipements du parc.

3.3.3 Changement d'habilitation à l'échelle du domaine

Lorsqu'une brèche se produit dans un réseau, généralement par l'exploitation d'une vulnérabilité dans l'un des services exposés à Internet dans la zone DMZ ou par le *spear-phishing* d'un des travailleurs par courrier électronique, l'attaquant tentera d'**escalader les privilèges** sur la machine compromise pour obtenir les **informations d'identification** de l'ordinateur et du domaine.

Ensuite, après une reconnaissance du réseau, l'attaquant tentera de se déplacer et de pivoter vers de nouveaux ordinateurs sur le réseau jusqu'à ce qu'il parvienne à accéder au contrôleur de domaine (DC), d'où il aura le contrôle total du réseau.

La solution consiste à **réinitialiser les informations d'identification du domaine**, une fois que le DC a été reconstruit avec l'Active Directory (AD). De plus, tous les utilisateurs administrateurs doivent être recherchés, afin d'identifier les éventuels utilisateurs privilégiés créés par l'attaquant.

La solution consiste à réinitialiser les informations d'identification du domaine, une fois que le DC a été reconstruit avec l'Active Directory (AD).

3.4 Recherche d'informations et services

Cette ligne d'action peut également être menée en parallèle avec le reste. Après un incident de sécurité ayant entraîné le cryptage et la suppression de biens, il est essentiel d'établir l'étendue de l'impact subi, en évaluant quelles informations peuvent être récupérées et quels services ont été affectés.

3.4.1 Évaluation du scénario

Une **évaluation de l'impact** du ransomware doit être effectuée afin de pouvoir tenter de récupérer les fichiers cryptés.

Les scénarios possibles sont énumérés ci-dessous, en commençant par le plus favorable au plus défavorable:

SCÉNARIO {1}

Une sauvegarde complète de l'ordinateur affecté est disponible

Dans ce scénario, l'ordinateur affecté serait désinfecté, puis la sauvegarde serait restaurée.

SCÉNARIO {2}

Il existe un outil qui permet le décryptage

Si des outils publics sont disponibles pour restaurer les fichiers chiffrés par un spécimen particulier de ransomware, ils seront utilisés. Malheureusement, seules quelques variantes de ransomware sont décryptables, soit parce que toutes les clés de chiffrement ont été obtenues après l'intervention du serveur C&C, soit parce qu'il existe une vulnérabilité connue dans le code malveillant qui permet de décrypter les fichiers. Voir la septième section, "Décryptage des ransomwares".

SCÉNARIO {3}

La copie de volume fantôme est disponible

Il suffirait de restaurer les copies de sauvegarde que Windows fait automatiquement des fichiers, en utilisant Shadow Explorer, par exemple. Dans de nombreux cas, le ransomware rendra cette action impossible.

SCÉNARIO {4}

Les fichiers peuvent être récupérés avec SW forensics

Parfois, certains programmes d'expertise sont capables de récupérer certains des fichiers originaux supprimés par le ransomware.

SCÉNARIO

{5}

Garder les fichiers cryptés en toute sécurité

Il est possible qu'à l'avenir les fichiers affectés puissent être décryptés avec un outil spécifique.

SAUVEGARDE DES ÉQUIPEMENTS → **DISINFECTION**

Le paiement de la rançon ne garantit pas que les attaquants enverront l'utilitaire de décryptage et/ou le mot de passe, il ne fait que récompenser leur campagne et les motiver à poursuivre la diffusion massive de ce type de code malveillant.

3.4.2 L'inventaire des biens cryptés ou supprimés

Pour déterminer la portée de l'infection et l'impact de l'incident, il est nécessaire de dresser la **liste des services affectés** en fonction des informations qui ont été cryptées ou supprimées.

Vous trouverez ci-dessous un exemple de tableau qui peut être utilisé pour dresser la liste des biens affectés, y compris l'impact:

SERVER	DONNÉES	IMPACT	RÉSULTATS
XXXXXXXXX	Courrier de l'entreprise Bases de données documentaires	Aucun impact sur le serveur virtuel Répliques supprimées ou cryptées Sauvegarde cryptée	**Récupération complète**

3.4.3 Reconstruction et rétablissement des services essentiels

Quelques recommandations pour la recherche d'informations sont décrites ci-dessous.

Le service Windows *Shadow Copy*, également connu sous le nom de **Volume Snapshot Service (VSS)**, vous permet d'effectuer des copies périodiques automatiques des données stockées sur les ressources partagées, ainsi que sur les disques d'ordinateur (sur les systèmes de fichiers NTFS). À cette fin, VSS crée des copies cachées des modifications des blocs de données dans le système de fichiers, ce qui permet de récupérer des informations individuelles (par exemple, des fichiers) en cas de perte ou de suppression accidentelle. Pour plus d'informations techniques sur ce système, nous vous recommandons de lire "*Volume Shadow Copy*" sur le site de Microsoft.

Contrairement au système mis en place dans Windows XP[1] (restauration du système), le VSS maintient des *instantanés* des volumes du système, par exemple, le lecteur C entier. De cette façon, non seulement les fichiers système mais aussi toutes les données contenues sur ce disque, y compris les documents de l'utilisateur, les fichiers de programme, etc. seraient protégés.

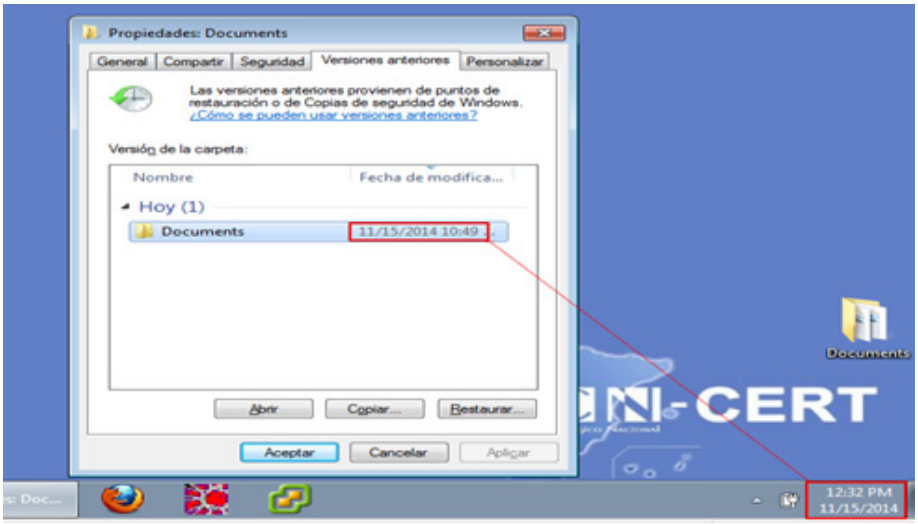
Si vous avez un système d'exploitation Windows Vista[2] ou supérieur, dans le cas où vous êtes victime d'un ransomware dont il est pratiquement impossible de récupérer les fichiers originaux - par exemple, en raison du système de cryptage utilisé -, il est conseillé d'envisager d'utiliser VSS pour essayer de récupérer une copie antérieure des fichiers affectés (tant que le lecteur VSS n'a pas été affecté).

Le VSS maintient des instantanés des volumes du système, par exemple, le lecteur C entier. De cette façon, non seulement les fichiers système mais aussi toutes les données contenues sur ce disque.

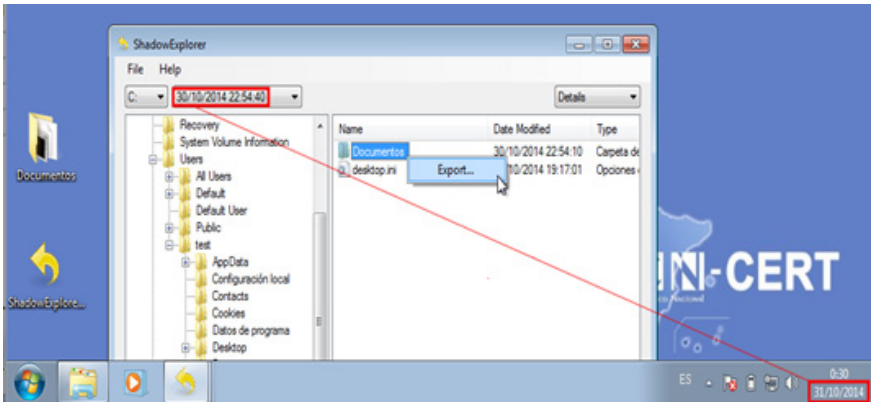
1. Système d'exploitation Microsoft Windows, sorti en 2002, dont le support a pris fin en 2014.
2. Système d'exploitation Microsoft Windows, sorti en 2007, dont le support a pris fin en 2017.

Pour procéder à la récupération des fichiers d'un certain répertoire, il suffit d'accéder à ses propriétés puis d'aller dans l'onglet "**Versions précédentes**".

A partir de cet onglet, il sera possible de visualiser et de restaurer chacune des copies créées par VSS sur ce répertoire. N'oubliez pas que la *sauvegarde* la plus récente peut ne pas correspondre (puisqu'il s'agit d'une version plus ancienne) à la dernière version du fichier original avant d'être affecté par le ransomware.



Une autre alternative pour restaurer une copie créée par le VSS des documents est d'utiliser le logiciel **Shadow Explorer**. Ce programme possède une interface très simple à partir de laquelle vous pouvez visualiser et restaurer chacune des copies créées par le VSS. Dans la capture d'écran suivante, la *sauvegarde* la plus récente, avant l'infection d'un certain ransomware, a été sélectionnée. Ensuite, après un clic droit sur le répertoire sélectionné, l'option "**Exporter**" a été sélectionnée.



Il est à noter que les *ransomwares* les plus récents, conscients de ce mécanisme de récupération des fichiers, mettent en œuvre des fonctionnalités permettant de désactiver le VSS et de supprimer les points de restauration.

Dans certains cas, il est possible de décrypter les fichiers chiffrés par un spécimen particulier de ransomware. Les outils qui permettent le décryptage et la restauration des fichiers peuvent en tirer parti:

- **Faiblesses de l'algorithme de cryptage utilisé par le ransomware.**
- **Récupération des clés à travers les informations contenues ou générées par le binaire (fichiers temporaires, clés de registre, etc.).**
- **Parfois, grâce à la collaboration de la police et de la communauté internationale, il est possible de prendre le contrôle de serveurs C&C, à partir desquels les clés utilisées dans les processus de cryptage peuvent être extraites.**

Vous trouverez ci-dessous une liste des **outils** et **utilitaires** en ligne existants, qui permettent de décrypter certains spécimens de ransomware, classés par famille:

Ransonware	Outil	Web
AlcatrazLocker	Outil Avast	https://files.avast.com/files/decryptor/avast_decryptor_alcatrazlocker.exe
Apocalypse	Outil Avast	https://files.avast.com/files/decryptor/avast_decryptor_apocalypse.exe
Bad Block	Outil Avast	https://files.avast.com/files/decryptor/avast_decryptor_badblock.exe
Bandarchor	Outil Kaspersky	https://support.kaspersky.com/sp/viruses/disinfection/10556
Bart	Outil Avast	https://files.avast.com/files/decryptor/avast_decryptor_bart.exe
Cryptodefense	Outil Emsisoft	https://decrypter.emsisoft.com/cryptodefense
Cryptolocker	-	http://www.decryptcryptolocker.com
CryptXXX v3	Outil Kaspersky	https://support.kaspersky.com/mx/8547
Crysis	-	https://files.avast.com/files/decryptor/avast_decryptor_crysis.exe
DMAlocker	Outil Emsisoft	https://decrypter.emsisoft.com/dmalocker
Globe	Outil Avast	https://files.avast.com/files/decryptor/avast_decryptor_globe.exe
JigSaw	Outil Avast	https://files.avast.com/files/decryptor/avast_decryptor_jigsaw.exe
Legion	Outil AVG	http://files-download.avg.com/util/avgrem/avg_decryptor_Legion.exe
Locky	Outil Emsisoft	https://decrypter.emsisoft.com/autolocky
Petya	Bleepingcomputer Tool	http://download.bleepingcomputer.com/fabian-wosar/Petyaextractor.zip
SFZLocker	-	https://www.avg.com/es-es/ransomware-decryption-tools#szflocker
Teslacrypt	Outil Eset	https://download.eset.com/special/ESETTeslaCryptDecryptor.exe
Torrentlocker	Bleepingcomputer Tool	http://download.bleepingcomputer.com/Nathan/TorrentUnlocker.exe
Zerolocker	Outil Vinsula	http://vinsula.com/security-tools/unlock-zerolocker/

En plus de ces liens, vous pouvez consulter:

Lien vers la solution de **Trendmicro**, pour lutter contre un **large éventail** de souches de **ransomware** (y compris certaines moins connues)

Lien: https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor

Un outil d'**Emsisoft**, qui **combat l'infection de plusieurs familles de Ransomware**, également moins connues et certaines non incluses dans les outils précédents listés

Lien: https://decrypter.emsisoft.com/

Si la variante qui a infecté votre ordinateur n'est répertoriée dans aucun des outils ci-dessus, vous pouvez tenter votre chance avec le moteur de recherche proposé par **Barkly.**

Lien: https://www.barkly.com/ransomware-recovery-decryption-tools-search

3.5 Prévention

Les lignes de travail ci-dessus n'ont aucun sens si les politiques et les mécanismes de sécurité nécessaires ne sont pas établis pour assurer la prévention d'une nouvelle infection qui suit des schémas similaires à ceux présentés dans cette intrusion.

Pour prévenir toute infection future suivant un *modus operandi* similaire, il convient d'établir les lignes directrices suivantes:

3.5.1 Établir des politiques de sécurité de domaine

Une fois que toutes les tâches de désinfection et d'atténuation décrites dans les points précédents ont été effectuées, il est nécessaire:

Déployez des stratégies pour l'ensemble du domaine, en **désactivant l'exécution de PowerShell** sur tous les ordinateurs et en ne l'autorisant que sur ceux qui doivent nécessairement le faire. Cela empêche l'exécution des outils de post-exploitation utilisés par l'attaquant pour obtenir des informations et se déplacer sur le réseau.

Il est également nécessaire de **désactiver l'exécution des macros** dans les documents bureautiques, qui est généralement le vecteur d'infection utilisé pour pénétrer dans un réseau.

Pour plus d'informations sur la manière d'effectuer ce point, il existe un **rapport sur les menaces de CCN-CERT** qui explique la procédure en détail:

Lien: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4171-ccn-cert-ia-52-19-implementacion-segura-de-microsoft-windows-office-frente-a-la-campana-emotet/file.html

Imposez l'utilisation de **mots de passe forts** qui expirent périodiquement. Idéalement, pour les services exposés sur Internet, exigez un **deuxième facteur d'authentification**, en utilisant le SMS, le courriel, Google Authenticator, ou toute autre solution jugée appropriée.

Passez périodiquement en revue les utilisateurs ayant des privilèges d'administrateur qui existent dans le domaine, en vérifiant qu'il n'y en a aucun qui ne soit pas contrôlé et en réduisant autant que possible le niveau d'accès des utilisateurs. Cela empêchera l'attaquant d'obtenir facilement les informations d'identification de l'administration du domaine et de coloniser le réseau après une infection.

3.5.2 Établir des politiques de sécurité au niveau du réseau

Au niveau du réseau il est nécessaire d'établir des politiques qui permettent un contrôle granulaire des connexions qui peuvent être établies entre les différents points et ordinateurs du réseau, pour cela il est conseillé de suivre les recommandations suivantes:

- **Bloquez au niveau du pare-feu**, de préférence la couche 7, toutes les connectivités qui ne sont pas strictement nécessaires. Pour ce faire, il est recommandé de suivre une approche de ***liste blanche***, en n'autorisant que les connectivités essentielles et en refusant le reste du trafic.

- **Toute activité** du pare-feu, du proxy, du DNS et de tout élément ou service de sécurité sur le réseau doit être **enregistrée** afin d'analyser et de surveiller les schémas anormaux:

  - **Ordinateurs clients qui tentent d'accéder à d'autres ordinateurs** de l'organisation, tels que des serveurs, des ordinateurs d'autres segments, etc. auxquels ils ne devraient pas avoir accès.

  - **Connectivité vers et depuis Internet** par des ordinateurs du réseau utilisant des ports non standard (autres que 53/UDP, 80/TCP, 443/TCP) et en dehors de la *liste blanche* définie dans le proxy.

  - Idéalement, tous les journaux et traces devraient être centralisés dans un **SIEM** afin de **surveiller tous les *journaux*** à partir d'un point unique et de manière intégrale.

Pour les utilisateurs, les entreprises ou les clients qui ont besoin d'un accès externe à l'Intranet en utilisant un VPN, l'IP source à partir de laquelle la communication doit être établie doit toujours être demandée, dans la mesure du possible, afin de réduire au maximum la surface d'exposition. Ces accès doivent être vérifiés périodiquement pour confirmer leur légitimité.

De cette façon, l'équipe de sécurité peut avoir une **visibilité** et **une traçabilité** de tous les événements générés dans le réseau, en détectant en temps utile les **activités anormales** qui pourraient dénoter un dysfonctionnement ou une éventuelle intrusion dans le réseau.

3.5.3 Performance anti-spam

Les courriels au contenu malveillant constituent la principale porte d'entrée. Il convient donc d'accorder une attention particulière aux règles de détection des antispam et d'envisager la possibilité de les compléter par l'exécution des pièces jointes en sandbox.

Les fichiers peuvent contenir des logiciels malveillants, qu'il s'agisse de fichiers bureautiques ou de fichiers cryptés par un mot de passe avec les outils habituels tels que ZIP et RAR. Comme les fichiers sont cryptés, ils peuvent être laissés passer sans être correctement analysés. Vous devez donc être extrêmement prudent avec ces actions ou essayer de toujours utiliser le cryptage PGP car il s'agirait d'un cryptage personnel.

3.5.4 Faire des dossiers

La sauvegarde est probablement le point le plus important dans la gestion d'un incident impliquant un ransomware. Il est important que ces sauvegardes soient effectuées conformément aux recommandations suivantes:

Au moins des **copies quotidiennes** et incrémentielles des systèmes d'information prioritaires de l'organisation.

Isolation des serveurs ou armoires de sauvegarde par rapport au reste du réseau, afin qu'après l'infection d'un ordinateur, le logiciel malveillant ne puisse pas accéder directement à ce serveur (les solutions qui mettent en œuvre le NAC, *Network Access Control*, peuvent être utilisées à cette fin).

Disposer d'une capacité de stockage suffisante pour conserver **plus d'une copie de sauvegarde** d'un même bien, car dans le cas où les informations sont cryptées et sont introduites dans la sauvegarde, une copie antérieure non cryptée peut être disponible.

Idéalement, une **sauvegarde** isolée physiquement et déconnectée du réseau devrait être **effectuée périodiquement**, tous les mois par exemple.

Annexe I

Exemples de diagramme de réseau:

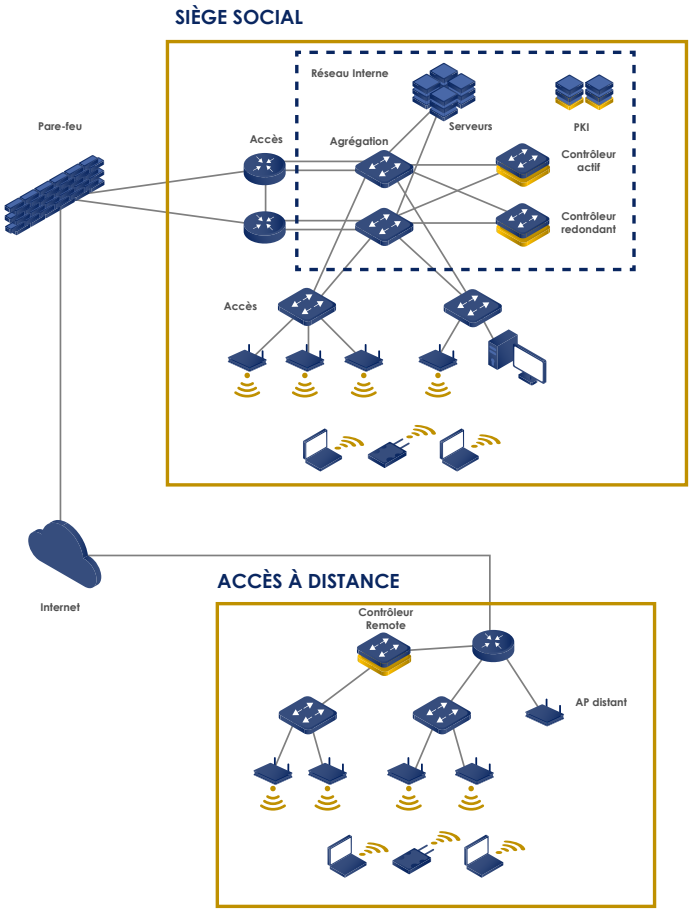


Figure 3. Diagramme de réseau

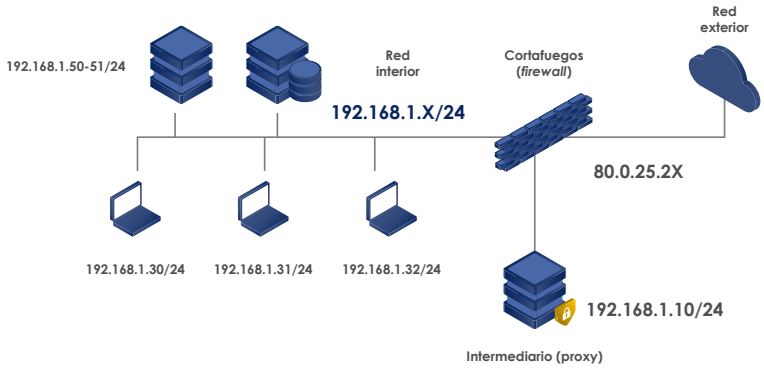


Figure 4. Diagramme de réseau

Annexe II

Exemple de liste de serveurs et d'actifs principaux:

Dispositif	IP	Type	Localisation	Observations
Serveur RADIUS	192.168.1.6/24	W2012	Siège Nord	Vous êtes isolé dans le VLAN MANAGEMENT
Serveur d'annuaire d'activité	192.168.1.10	W2008R2	DPC ISOLÉ	En attente de mise à niveau vers W2016
Serveur DHCP	192.168.1.101	W2008R2	Siège Sud	Plage IP 192.168.50 - 99
Serveur de virtualisation	192.168.102	VMWare 6.5	Siège Nord	Pas de sauvegarde

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es