CCN-CERT

BP/21

Gestión de incidentes de ransomware

INFORME DE BUENAS PRÁCTICAS

ABRIL **2021**

ccn-cert centro criptológico nacional
CCN centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Centro Criptológico Nacional, 2019

Fecha de edición: abril de 2021

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Índice

1. Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN.

El **CCN-CERT** es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es **contribuir a la mejora de la ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de **conseguir un ciberespacio más seguro y confiable**, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. Alcance del incidente

Para determinar el **alcance** de un incidente en el que esté involucrado ransomware hay que recopilar:

- **Información de contexto del incidente.**
- **Información técnica sobre la infección.**
- **Información de la red en la que se ha producido la infección.**

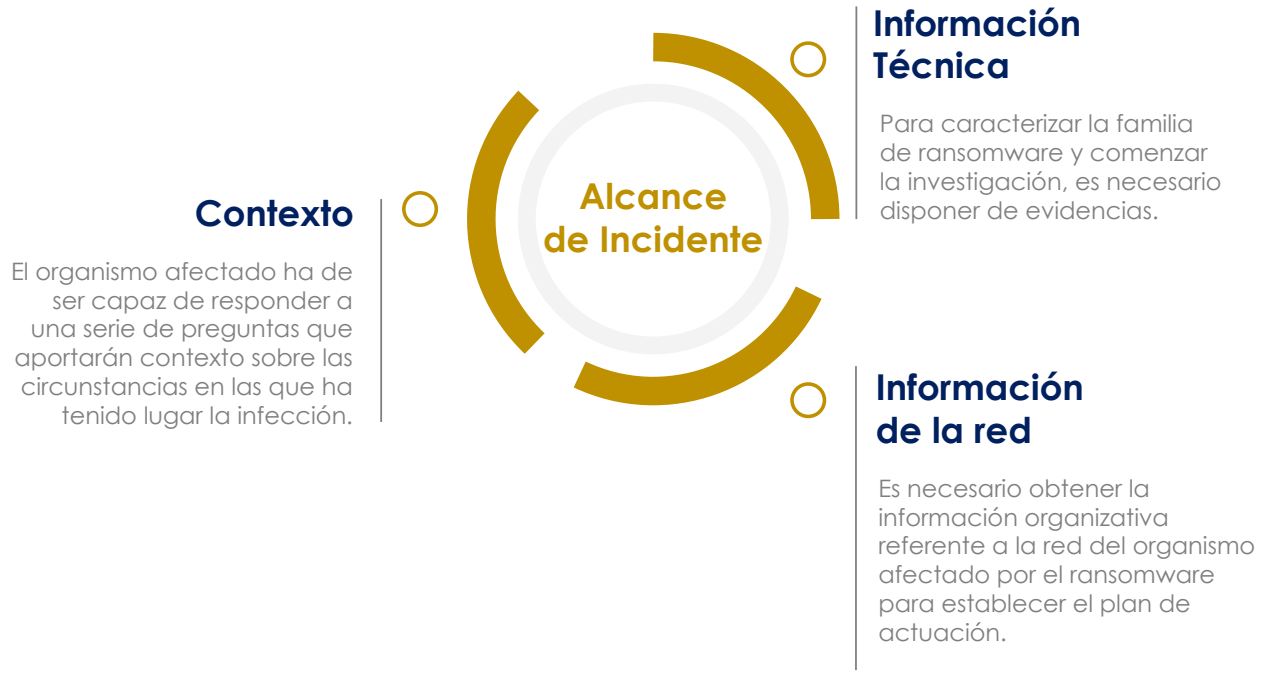


Figura 1. Alcance de incidente

2.1 Contexto del incidente

El organismo afectado ha de ser capaz de responder a las siguientes preguntas que aportarán **contexto sobre las circunstancias** en las que ha tenido lugar la infección:

¿Cuándo se produjo la infección?

¿Cómo se produjo la infección (adjunto en correo electrónico, RDP, etc.)?

¿Cuántos equipos afectados hay?

¿Se dispone de copia de seguridad de los datos cifrados?

¿Se ha realizado alguna acción de mitigación?

2.2 Información técnica sobre la infección

Además de dar respuesta a las preguntas anteriores, para caracterizar la familia de ransomware y comenzar la investigación, es necesario disponer de las siguientes **evidencias**:

Nota de rescate del ransomware.

Muestras de ficheros cifrados (no superior a 2 megas).

Muestra del ransomware, del correo de phishing, fichero ofimático o de cualquier evidencia que permita analizar el código dañino.

2.3 Información de la red

Finalmente, es necesario obtener la siguiente información organizativa referente a la red del organismo afectado por el ransomware para establecer el plan de actuación:

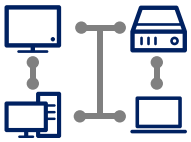


Diagrama de red

Esquema en el que aparezcan los componentes que forman la red de comunicaciones y cómo interactúan entre ellos, donde figuren routers, firewall, servidores, estaciones de trabajo y sus conexiones. En el ANEXO I se incluyen ejemplos de diagrama de red.

Listado de servidores y activos principales

Tabla donde figuren IP, dominio, nombre del equipo y ubicación. En el ANEXO II se incluye una tabla de ejemplo que puede ser utilizada.

Direccionamiento púbico, IP y dominios

Listado de direcciones y dominios expuestos a Internet.

Registros (logs)

De los sistemas de seguridad presentes en la red:

- **Antivirus, EDR**
- **Firewall, proxy, DNS, IDS/IPS**
- **Antispam, mail de cuarentena**
- **Accesos remotos (VPN, SSH, Teamwiewer, etc.)**
- **Copia de tráfico**

3. Líneas de actuación

Se trabajará en las siguientes **líneas de actuación**, definiendo un equipo que lidere cada tarea y designando a un responsable de equipo:

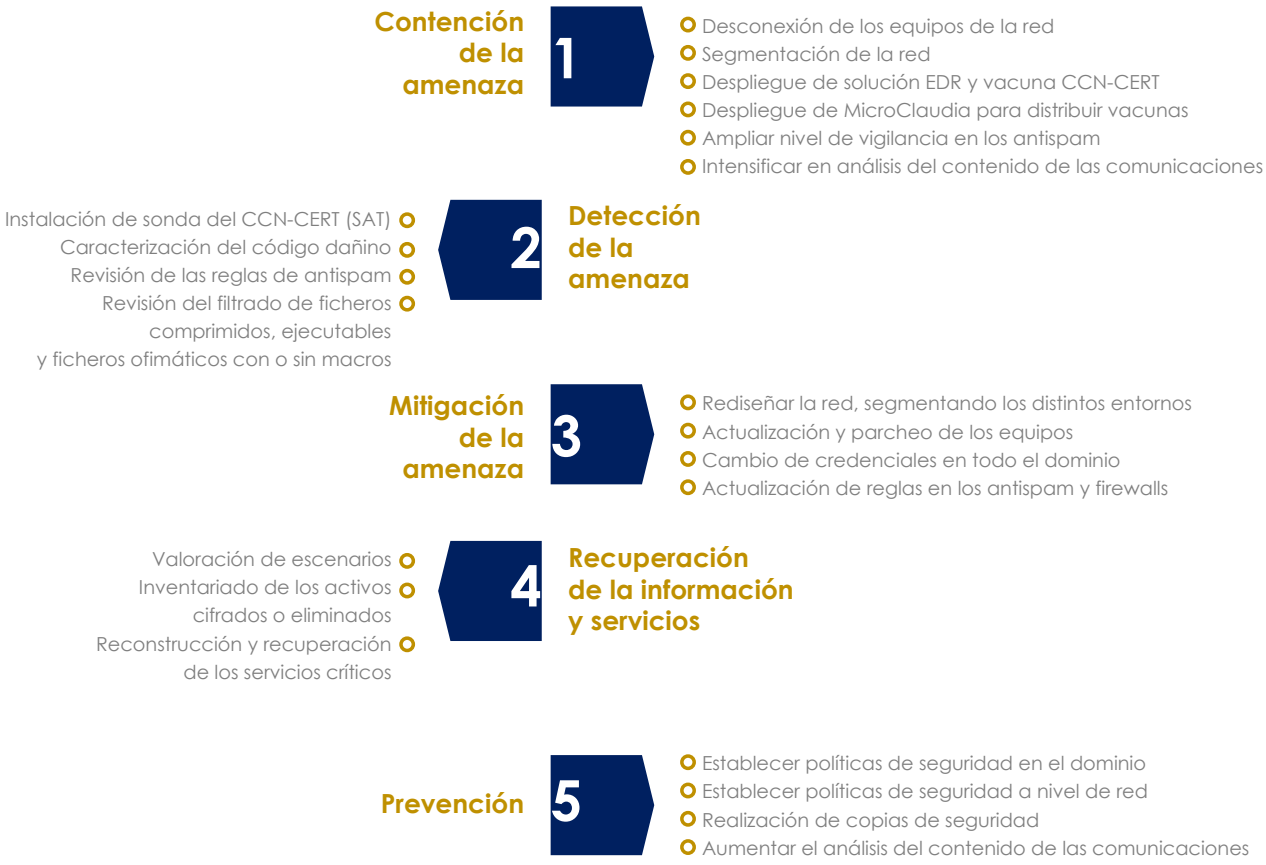
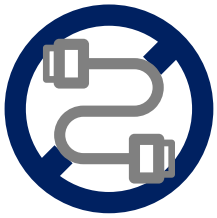


Figura 2. Líneas de actuación

3.1 Contención de la amenaza

La fase de contención es la primera que se lleva a cabo para asegurar que:

El código dañino no continúa propagándose por la red (cifrado de carpetas compartidas, movimiento lateral a equipos con visibilidad, etc.).



En el caso de que un atacante tenga acceso a la red de forma remota, ésta será interrumpida de inmediato para evitar que pueda continuar con su actividad (exfiltración de información, despliegue de puertas traseras adicionales, eliminación o destrucción de evidencias, etc.)

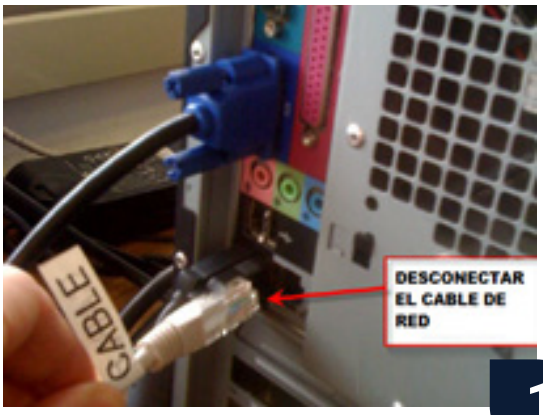
Para ello, y sobre todo en los incidentes de seguridad en los que hay un espécimen de ransomware involucrado, hay que proceder de forma inmediata, realizando las acciones que se detallan en los siguientes epígrafes.

3.1.1 Desconexión de los equipos de la red

En el momento en que se produce una infección por ransomware se comenzarán a cifrar los ficheros del equipo y los mapeados en las unidades conectadas, tanto dispositivos físicos (USB's, discos duros externos, etc.) como unidades de red.

En la gran mayoría de situaciones se es consciente de la infección cuando el ransomware ha finalizado su ejecución y todos los ficheros se han cifrado. Sin embargo, existe la posibilidad de que éste aún no haya terminado su ejecución, permitiendo en el mejor de los escenarios recuperar la clave de cifrado o evitar que más ficheros sean cifrados.

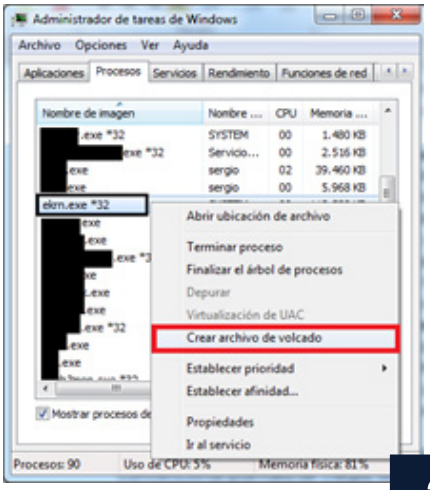
Se recomienda seguir los siguientes pasos generales en el momento de la detección de un ransomware:



1

Desconectar las unidades de red

Esto supone "tirar del cable" de red (o desactivar las interfaces inalámbricas). De este modo se podría llegar a evitar el cifrado de ficheros en unidades de red accesibles, en el caso de que el ransomware aún no hubiera finalizado su ejecución.

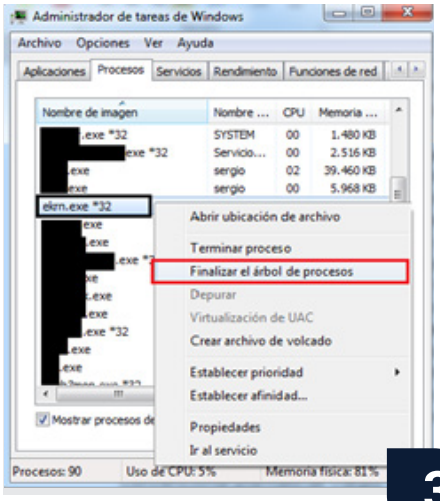


2

Comprobar si el proceso dañino aún sigue ejecutándose

Esta tarea no es sencilla en muchos casos ya que el proceso dañino podría haberse inyectado en otro legítimo o simplemente podría haber finalizado su ejecución.

Sin embargo, en caso de identificarse el proceso en cuestión (usando herramientas como Process Explorer de Sysinternals), desde el Administrador de Tareas de Windows (Taskmanager) se realizará un dump (volcado de la memoria) del proceso dañino. Para ello, hay que hacer clic derecho sobre el proceso y seleccionar la opción "Crear archivo de volcado" (se guardará en %TMP%). Una vez volcado el fichero, hay que guardarlo a buen recaudo en un sistema aislado.



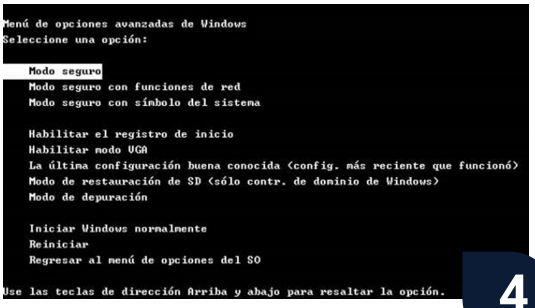
3

Finalizar la ejecución del proceso dañino

Para ello existen dos alternativas:

I. En caso de haberse identificado el proceso, simplemente bastará con parar su ejecución desde el Administrador de Tareas de Windows: clic derecho sobre el proceso y seleccionar la opción "Finalizar el árbol de procesos".

II. Si no se ha podido identificar el proceso, se recomienda apagar el equipo de manera manual e inmediata.



4

Arrancar el equipo en Modo seguro

Antes de que arranque Windows de manera convencional (pantalla de carga) se habrá de pulsar la tecla F8 para acceder al menú de arranque avanzado, desde el que se seleccionará iniciar desde "Modo Seguro". De este modo evitaremos que el ransomware vuelva a arrancar de nuevo en caso de que éste fuera persistente.

5

Realizar una copia de seguridad del equipo

Esta copia contendrá todos los ficheros cifrados y no cifrados, y deberá realizarse en un dispositivo de almacenamiento externo aislado de la red. **En caso de que no pudieran descifrarse los ficheros, es importante conservarlos** ya que en un futuro puede que se rompa el cifrado o se liberen las claves del C&C (Command and Control).

3.1.2 Segmentación de la red

Éste probablemente sea el punto fundamental que ha de llevarse a cabo.

Normalmente, el ransomware es capaz de propagarse por la red a través de unidades compartidas en el dominio. Sin embargo, las tendencias indican que en las últimas campañas en las que está involucrado ransomware también puede existir **código dañino adicional** con mayores capacidades y complejidad. Se ha observado que en algunos casos la amenaza puede escalar privilegios, moverse lateralmente por la red empleando credenciales comprometidas, arrancar equipos de la red apagados usando WoL (*Wake on Lan*), y exfiltrar información.

Los responsables de sistemas han de rediseñar la red y establecer el punto idóneo para ubicar el firewall. El cortafuegos permitirá tener visibilidad de todo el tráfico de red que pase por él, esto será especialmente útil en caso de disponer de IOC (indicadores de compromiso, por sus siglas en inglés) para localizar aquellos equipos de la red que intenten establecer comunicaciones con servidores de mando y control (C2) conocidos.

Las tendencias indican que en las últimas campañas en las que está involucrado ransomware también puede existir código dañino adicional con mayores capacidades y complejidad.

3.1.3 Despliegue de solución EDR y vacuna CCN-CERT

Para concluir la fase de contención, se recomienda desplegar una solución EDR (*Endpoint Detection and Response*) en los puntos finales, equipos cliente y servidores, para mejorar la capacidad de detección y aislamiento.

Por su parte, el CCN-CERT mediante su herramienta **MicroClaudia** distribuye vacunas específicas para cada caso de ransomware. Mediante MicroClaudia se generan actuaciones que **permiten el bloqueo inmediato de cualquier malware** relacionado con **Emotet**, **Trickbot**, **Bitpaymer**, **Ryuk** y **Sodinokibi entre otros,** de forma que se pueda detener la ejecución de los mismos en caso de que los equipos estén infectados o el código dañino intente propagarse.

3.2 Detección de la amenaza

Tras la fase de contención, se procede a **detectar qué equipos han sido afectados** por el código dañino, bien porque el atacante los hubiera utilizado para pivotar por la red o para cifrar y/o eliminar su contenido.

Durante esta fase se procede con las labores que a continuación se indican.

3.2.1 Instalación de sonda del CCN-CERT (SAT)

El CCN-CERT dispone de una sonda, Sistema de Alerta Temprana, que realiza las funciones de IDS (*Intrusion Detection System*) y que puede ser desplegada en un punto de interconexión de la red donde se tenga visibilidad de todo el tráfico entrante y saliente.

Esta sonda permite identificar si, en base a los patrones conocidos por el CCN-CERT, existe tráfico categorizado como dañino en la red, de forma que se pueda actuar de forma oportuna para localizar y neutralizar la amenaza posteriormente.

3.2.2 Instalación de MicroClaudia

El CCN-CERT pone a disposición su herramienta para distribuir vacunas específicas de cada ransomware y así evitar la ejecución de los mismos.

La herramienta se instala en los equipos finales y contiene detectores de actuación basados en la investigación de los diferentes ransomwares.

El equipo de **MicroClaudia** se encarga de **añadir nuevas vacunas a partir del análisis de muestras** que van apareciendo.

3.2.3 Caracterización del código dañino

El CCN-CERT dispone de informes de código dañino (ID) en su portal (https://ccn-cert.cni.es) relacionados con distintas familias de ransomware.

En estos informes se recopila toda la caracterización de la amenaza, incluyendo **características**, **funcionalidad**, **conectividades**, **persistencia** e **indicadores que permitan la detección**.

Existen diversas páginas que pueden ayudar a identificar la familia de ransomware implicada en el incidente. Partiendo de un fichero de muestra, las más efectivas y recomendables son:

nomoreransom.org

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

IDRansomware

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

En estas páginas se pueden **subir los ficheros cifrados** y las **notas de rescate**. De este modo, y a través del tipo de cifrado y método de rescate, se logra saber qué tipo de familia es la que ha producido la infección.

3.3 Mitigación de la amenaza

De forma paralela a la contención y detección de la amenaza, se puede llevar a cabo la fase de mitigación, consistente en neutralizar de forma efectiva el malware desplegado por el atacante. Para ello se pueden seguir los siguientes pasos:

3.3.1 Rediseñar la red segmentando los distintos entornos

En una red no segmentada es trivial para un atacante tener visibilidad de todos los activos, a pesar de disponer de distintos direccionamientos.

Una vez que el atacante obtiene credenciales de dominio, comprometiendo previamente un equipo de la red, podría empezar a moverse lateralmente, buscando qué equipos son más interesantes de cara a robar, cifrar o eliminar el contenido.

Teniendo en cuenta la naturaleza de los equipos y servidores (DMZ, LAN, DC y servidores, etc.), si la red está correctamente segmentada utilizando elementos de red como firewalls y separando los distintos entornos y direccionamientos, el potencial impacto que pudiera derivar de una infección por ransomware sería inferior respecto al caso en el que se disponga de una red plana. De hecho, la segmentación permitiría acotar y aislar los equipos afectados durante un incidente de seguridad, impidiendo que el código dañino pudiera propagarse por la red para, en última instancia, tomar el control de la misma tras el compromiso del Controlador de Dominio (DC).

Idealmente hay que ajustar las políticas del firewall siguiendo una aproximación basada en ***whitelist***, es decir, habilitando únicamente aquellas conectividades que sean imprescindibles en cada caso para el correcto funcionamiento y operación de los equipos del parque.

Idealmente hay que ajustar las políticas del firewall siguiendo una aproximación basada en *whitelist*, es decir, habilitando únicamente aquellas conectividades que sean imprescindibles en cada caso.

3.3.2 Actualización y parcheo de los equipos

En el parque de equipos suele existir un conjunto muy heterogéneo de versiones de dispositivos y sistemas operativos.

Esto implica que, en algunos casos, el nivel de parcheo no es uniforme o que ya no se dispone de soporte para las actualizaciones de seguridad.

Es **imprescindible** que periódicamente se continúe dando **soporte y mantenimiento** en forma de parches y actualizaciones a los equipos del parque.

Es imprescindible que periódicamente se continúe dando soporte y mantenimiento en forma de parches y actualizaciones a los equipos del parque.

3.3.3 Cambio de credenciales en todo el dominio

Cuando se produce una brecha en una red, normalmente a través de la explotación de una vulnerabilidad en uno de los servicios expuestos a Internet en la zona de la DMZ o infectando vía *spear-phishing* a través del correo electrónico a uno de los trabajadores, el atacante tratará de **escalar privilegios** en la máquina comprometida para hacerse con las **credenciales** del equipo y del dominio.

Acto seguido, tras un reconocimiento de la red, el atacante tratará de moverse y pivotar a nuevos equipos de la red hasta lograr obtener acceso al Controlador del Dominio (DC), desde donde tendrá todo el control de la red.

La solución pasa por **resetear las credenciales del dominio**, una vez haya sido reconstruido el DC junto con el Directorio Activo (AD). Asimismo, se han de buscar todos los usuarios de tipo administrador, de cara a identificar posibles usuarios privilegiados creados por parte del atacante.

La solución pasa por resetear las credenciales del dominio, una vez haya sido reconstruido el DC junto con el Directorio Activo (AD).

3.4 Recuperación de la información y servicios

Esta línea de acción también se puede realizar en paralelo al resto. Tras un incidente de seguridad que ha implicado el cifrado y borrado de activos, es fundamental establecer el alcance del impacto sufrido, evaluando qué información se puede recuperar y qué servicios se han visto afectados.

3.4.1 Valoración de escenarios

Es necesario realizar una **valoración del impacto producido** por el ransomware, de modo que en última instancia se pueda intentar la recuperación de los ficheros cifrados.

A continuación se listan los escenarios posibles, partiendo del más favorable al más desfavorable:

ESCENARIO {1}

Se dispone de backup completo del equipo afectado

En este escenario se procedería a desinfectar el equipo afectado para posteriormente restaurar la copia de seguridad.

ESCENARIO {2}

Existe una herramienta que permite el descifrado

Si existen herramientas públicas para restaurar los ficheros cifrados por un espécimen concreto de ransomware se hará uso de las mismas. Desafortunadamente, sólo unas pocas variantes de ransomware son descifrables, o bien porque se han obtenido todas las claves de cifrado tras la intervención del servidor C&C, o porque existe una vulnerabilidad conocida en el código dañino que permite el descifrado de los ficheros. Consultar el séptimo apartado, "Descifrado de ransomware".

ESCENARIO {3}

Se dispone de Shadow Volume Copy

Bastaría con restaurar las copias de seguridad que realiza Windows automáticamente de los ficheros, utilizando Shadow Explorer, por ejemplo. En muchos casos el ransomware imposibilitará esta acción.

ESCENARIO {4}

Se pueden recuperar los ficheros con SW forense

En ocasiones algunos programas forenses son capaces de recuperar algunos ficheros originales borrados por el ransomware.

ESCENARIO

{5}

Conservar los ficheros cifrados a buen recaudo

Es posible que en el futuro los ficheros afectados puedan ser descifrados con una herramienta específica.

BACKUP DEL EQUIPO → **DESINFECCIÓN**

Efectuar el pago por el rescate del equipo no garantiza que los atacantes envíen la utilidad y/o contraseña de descifrado, sólo premia su campaña y les motiva a seguir distribuyendo masivamente este tipo de código dañino.

3.4.2 Inventariado de los activos cifrados o eliminados

Para determinar el alcance de la infección y el impacto del incidente es necesario elaborar un **listado de los servicios afectados** en base a la información que fue cifrada o eliminada.

A continuación, se adjunta un ejemplo de tabla que puede utilizarse para el listado de los activos afectados, incluyendo el impacto:

SERVIDOR	DATOS	IMPACTO	RESULTADOS
XXXXXXXXX	Correo corporativo BBDD documentales	Sin impacto en el servidor virtual Réplicas borradas o cifradas Backup cifrado	**Recuperación completa**

3.4.3 Reconstrucción y recuperación de los servicios críticos

A continuación, se describen algunas recomendaciones de cara a la recuperación de información.

El servicio *Shadow Copy* de Windows, también conocido como **Volume Snapshot Service (VSS)**, permite hacer copias automáticas periódicas de los datos almacenados en recursos compartidos, así como unidades del equipo (sobre sistemas de ficheros NTFS). Para ello el VSS crea copias ocultas de los cambios que experimentan bloques de datos del sistema de ficheros, permitiendo así recuperar información individual (por ejemplo ficheros) en el caso de pérdida o borrado accidental. Para más información técnica sobre este sistema se recomienda la lectura *"Volume Shadow Copy"* desde la página de Microsoft.

A diferencia del sistema implementado en Windows XP[1] (restauración del sistema), el VSS mantiene *snapshots* de volúmenes del sistema; por ejemplo, de toda la unidad C. De esta forma, se protegerían no sólo los ficheros del sistema sino todos los datos contenidos en dicha unidad, incluyendo los documentos de los usuarios, ficheros de programas, etc.

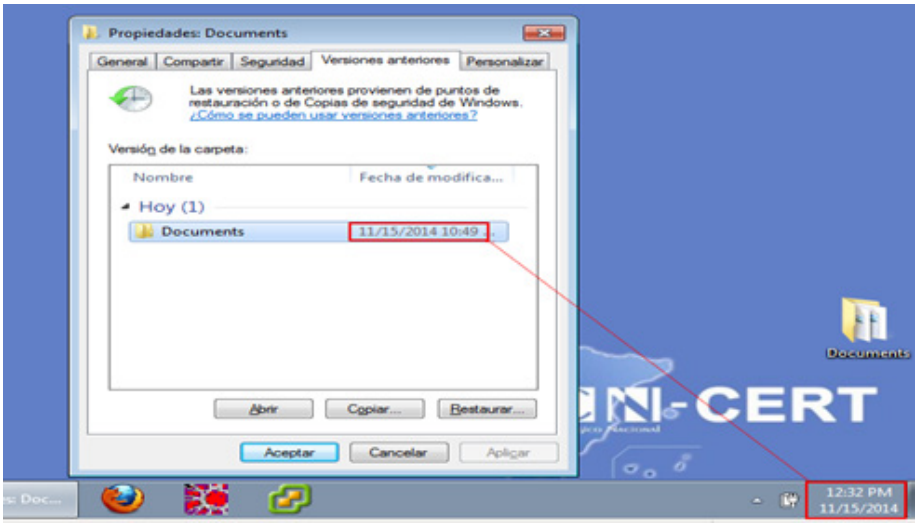
Si se cuenta con un sistema operativo Windows Vista[2] o superior, en el caso de ser víctima de un ransomware del cual sea prácticamente imposible recuperar los ficheros originales –por ejemplo, debido al sistema de cifrado utilizado–, es recomendable considerar el uso de VSS para tratar de recuperar una copia previa de los ficheros afectados (siempre y cuando la unidad VSS no se haya visto afectada).

El VSS mantiene *snapshots* de volúmenes del sistema. De esta forma, se protegerían no sólo los ficheros del sistema sino todos los datos contenidos en dicha unidad.

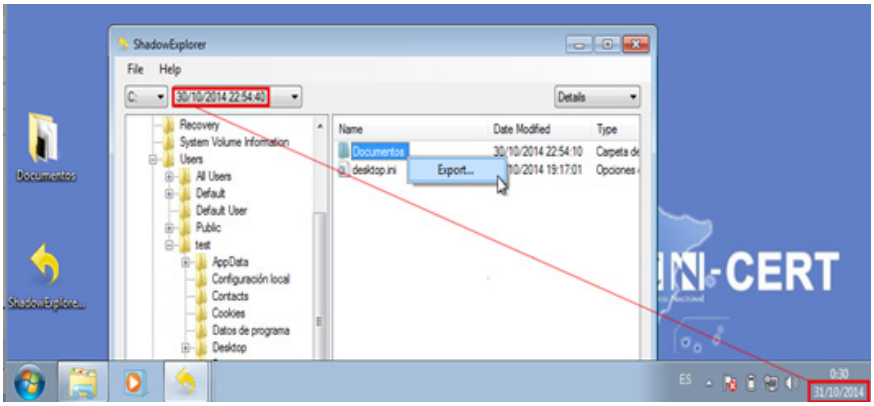
1. Sistema operativo de Microsoft Windows, lanzado en el año 2002, cuyo soporte técnico finalizó en 2014.
2. Sistema operativo de Microsoft Windows, lanzado en el año 2007, cuyo soporte técnico finalizó een 2017.

Para proceder a recuperar los ficheros de cierto directorio, únicamente es necesario acceder a las propiedades del mismo y posteriormente dirigirse a la pestaña **"Versiones Anteriores"**.

Desde esta pestaña será posible visualizar y restaurar cada una de las copias creadas por VSS sobre dicho directorio. Téngase en cuenta que el *backup* más reciente puede no coincidir (al tratarse de una versión más antigua) con la última versión del fichero original antes de verse afectado por el ransomware.



Otra alternativa para restaurar una copia creada por el VSS de los documentos es utilizar el software **Shadow Explorer**. Dicho programa presenta una interfaz muy sencilla desde la que se podrá visualizar y restaurar cada una de las copias creadas por el VSS. En la siguiente captura se ha seleccionado el *backup* más reciente, previo a la infección de cierto ransomware. Posteriormente, tras hacer botón derecho sobre el directorio seleccionado, se ha elegido la opción **"Export"**.



Cabe destacar que los *ransomware* más recientes, conscientes de este mecanismo para recuperar ficheros, implementan funcionalidades para desactivar el VSS y eliminar los puntos de restauración.

En ciertos casos, es posible descifrar los ficheros cifrados por un espécimen concreto de ransomware. Las herramientas que permiten el descifrado y restauración de los ficheros pueden aprovechar:

- **Debilidades en el algoritmo de cifrado empleado por el ransomware.**
- **Recuperación de la clave a través de la información contenida o generada por el binario (ficheros temporales, claves de registro, etc.)**
- **En ocasiones, mediante la colaboración policial e internacional, es posible tomar el control de los servidores de C&C, de los cuales se pueden extraer las claves empleadas en los procesos de cifrado.**

A continuación se listan algunas de las **herramientas** y **utilidades online existentes**, que permiten el descifrado de ciertos especímenes de ransomware ordenadas por familia:

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

Además de estos enlaces, se puede consultar:

Enlace a la solución de **Trendmicro**, para combatir un **amplio abanico** de variedades **de ransomware** (incluyendo algunas no tan conocidas).

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

Una herramienta de parte de **Emsisoft**, que **combate la infección de diversas familias de Ransomware**, también menos conocidas y algunas no incluidas en las herramientas anteriores listadas.

Enlace: https://decrypter.emsisoft.com/

En caso de que la variante que ha infectado el equipo no se encontrara listada en ninguna de las herramientas anteriores, se puede probar suerte con el buscador que ofrece **Barkly.**

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

3.5 Prevención

Las líneas de trabajo anteriores carecen de sentido si no se establecen las políticas y mecanismos de seguridad necesarios para asegurar la prevención de una nueva infección que siga patrones similares a los exhibidos en esta intrusión.

Para prevenir una futura infección que siga un *modus operandi* similar se han de establecer las siguientes pautas:

3.5.1 Establecer políticas de seguridad en el dominio

Una vez llevadas a cabo todas las tareas de desinfección y mitigación expuestas en los puntos anteriores, es necesario:

Desplegar políticas para todo el dominio, **deshabilitando la ejecución de PowerShell** en todos los equipos, permitiendo únicamente la ejecución en aquellos que por necesidad deban hacerlo. De esta manera se evita la ejecución de herramientas de post-explotación usadas por el atacante para obtener información y moverse por la red.

Asimismo, es necesario **deshabilitar la ejecución de macros** en documentos ofimáticos, que es típicamente el vector de infección que comúnmente se emplea para entrar en una red.

Para más información de cómo llevar a cabo este punto se dispone de un **Informe de Amenazas del CCN-CERT** que explica detalladamente el procedimiento:

Enlace: 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

Forzar al **empleo de contraseñas robustas** que caduquen con cierta periodicidad. Idealmente, para aquellos servicios expuestos en Internet requerir **segundo factor de autenticación**, usando para ello SMS, email, Google Authenticator, o cualquier solución que se estime oportuna.

Revisar periódicamente los usuarios con privilegios de administrador que existen en el dominio, comprobando que no existe ninguno que no esté controlado y reduciendo al máximo el nivel de acceso que tienen los usuarios. De esta forma, se evitará que tras una infección el atacante obtenga fácilmente credenciales de administración del dominio y pueda colonizar la red.

3.5.2 Establecer políticas de seguridad a nivel de red

A nivel de red es necesario establecer políticas que permitan controlar granularmente las conexiones que se pueden establecer entre los distintos puntos y equipos de la red, para ello se aconseja seguir las siguientes recomendaciones:

- **Bloquear a nivel de firewall**, preferiblemente de capa 7, todas aquellas conectividades que no sean estrictamente necesarias. Para ello se recomienda seguir una aproximación de ***whitelisting***, habilitando únicamente las conectividades imprescindibles y denegando el resto del tráfico.

- Se deberá **registrar toda la actividad** del Firewall, proxy, DNS y de cualquier elemento de seguridad o servicio en la red para analizar y monitorizar patrones anómalos:

  - **Equipos cliente que intenten acceder a otros equipos** de la organización, tales como servidores, equipos en otros segmentos, etc. a los que no debieran tener acceso.

  - **Conectividades desde y hacia Internet** por parte de los equipos de la red que empleen puertos no estándar (distintos a 53/UDP, 80/TCP, 443/TCP) y que se salgan de la *whitelist* establecida en el proxy.

  - Idealmente se deberían centralizar todos los registros y trazas en un **SIEM** de cara a llevar una **monitorización de todos los logs** desde un único punto de forma íntegra.

Para aquellos usuarios, empresas o clientes, que requieran acceso externo a la Intranet usando VPN se debería solicitar la IP de origen desde donde se vaya a establecer siempre la comunicación, siempre que sea posible, para reducir lo máximo posible la superficie de exposición. Se deben revisar con periodicidad dichos accesos para confirmar su legitimidad.

De esta forma el equipo de seguridad podrá tener **visibilidad** y **trazabilidad** de todos los eventos generados en la red, detectando en un tiempo oportuno **actividad anómala** que pudiera denotar un malfuncionamiento o una posible intrusión en la red.

3.5.3 Actuaciones en los antispam

La principal vía de entrada son correos electrónicos con contenido dañino, por ello se debe hacer especial énfasis en las reglas de detección en los antispam y contemplar la posibilidad de complementarlos con ejecución de sandbox de los ficheros adjuntos.

Los ficheros pueden contener malware, tanto si son ofimáticos como si vienen cifrados con contraseña con las habituales herramientas como ZIP y RAR. Al venir los ficheros cifrados puede que se dejen pasar sin realizar un correcto análisis de los mismos, por ello se debería extremar las precauciones con estas actuaciones o bien utilizar siempre cifrado PGP que permite cifrar cualquier tipo de información personal.

3.5.4 Realización de copias de seguridad

La realización de copias de seguridad es probablemente el punto más importante cuando se está gestionando un incidente que involucra ransomware. Es importante que estas copias de seguridad se realicen siguiendo las siguientes recomendaciones:

Copias diarias, al menos, e incrementales de los sistemas de información prioritarios para la organización.

Aislamiento de los servidores de backup, o cabinas, respecto al resto de la red, de manera que tras la infección de un equipo el malware no pueda saltar directamente a dicho servidor (se pueden usar soluciones que implementen NAC, *Network Access Control*, para ello).

Disponer de almacenamiento suficiente para mantener **más de una copia de seguridad** de un mismo activo, ya que en caso de sufrir el cifrado de la información y que ésta sea introducida en el backup, se pueda disponer de una copia anterior que no se encuentre cifrada.

Idealmente habría de **realizarse periódicamente**, cada mes, por ejemplo, una **copia de seguridad** que se encuentre físicamente aislada y desconectada de la red.

Anexo I

Ejemplos de diagrama de red:

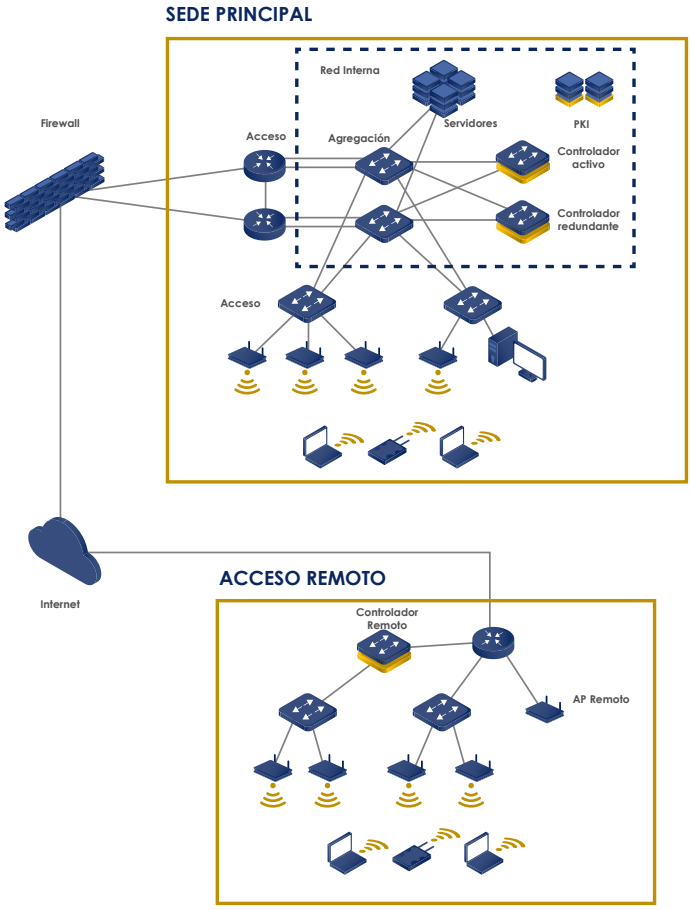


Figura 3. Diagrama de red

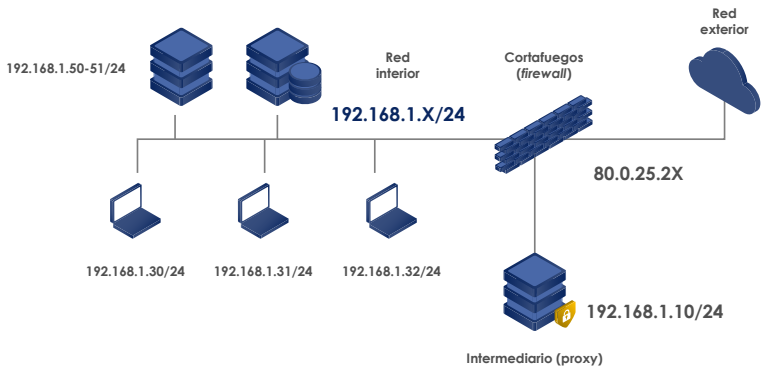


Figura 4. Diagrama de red

Anexo II

Ejemplo de Listado de servidores y activos principales:

Dispositivo	IP	Tipo	Ubicación	Observaciones
Servidor RADIUS	192.168.1.6/24	W2012	Sede Norte	Está aislado en la VLAN de GESTION
Servidor Activity Directory	192.168.1.10	W2008R2	CPD AISLADO	Pendiente de actualizar a W2016
Servidor DHCP	192.168.1.101	W2008R2	Sede Sur	Rango de IP 192.168.50 - 99
Servidor de Virtualización	192.168.102	VMWare 6.5	Sede Norte	Sin Backup

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es