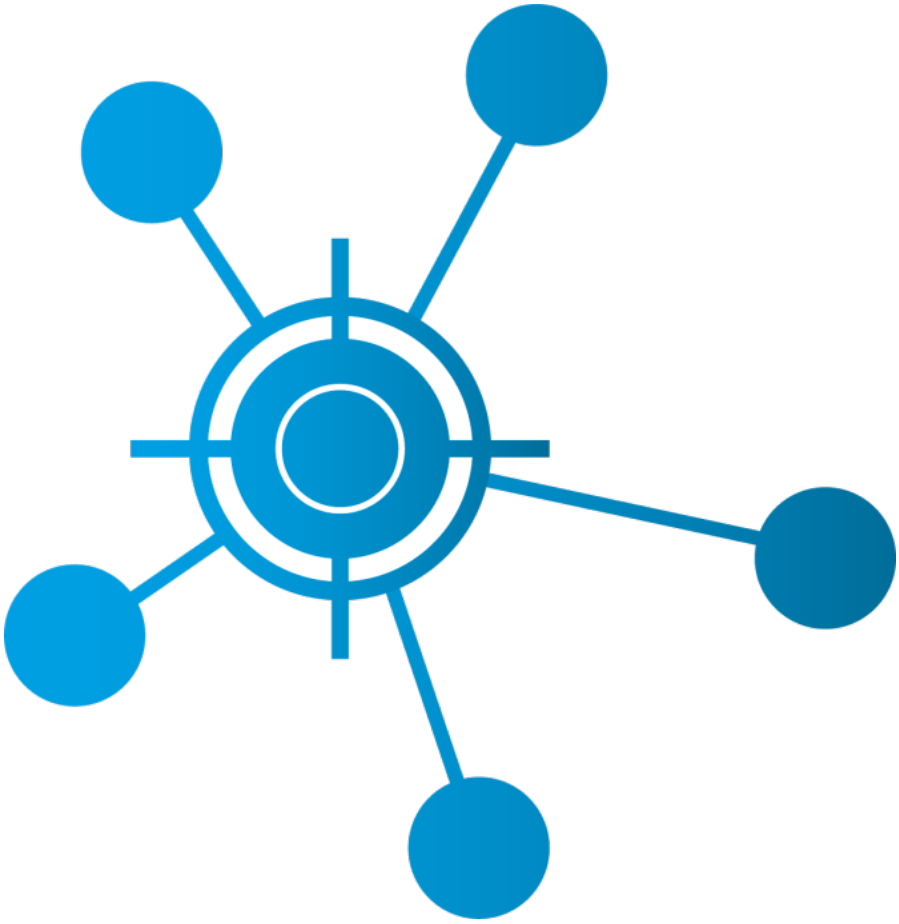
CCN-CERT IA-76/19

Medidas de actuación frente al código dañino EMOTET



Diciembre 2019

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Fecha de Edición: enero de 2020

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL 4

2. INTRODUCCIÓN 5

3. MÉTODOS DE PREVENCIÓN 7

3.1 CORREO ELECTRÓNICO 7

3.2 MICROSOFT WORD 8

3.3 SISTEMA OPERATIVO 9

3.4 ARQUITECTURA DE RED 9

4. DETECCIÓN DE LA AMENAZA 10

5. MÉTODOS DE DESINFECCIÓN 12

6. RECOMENDACIONES 13

7. CONCLUSIONES 14

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, 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. INTRODUCCIÓN

El código dañino conocido como Emotet lleva en activo, aunque con ciertas interrupciones desde 2014, utilizando diferentes métodos para conseguir infectar equipos que utilizan Sistemas Operativos (SO) de Microsoft Windows.

Durante su periodo de operación, a principios de 2017, su funcionalidad principal evolucionó, pasando de ser un troyano bancario a un distribuidor de otras amenazas como Trickbot, el cual es otro código dañino que, aunque también se distribuye de forma independiente, es muy común encontrarlo como parte de una infección de Emotet. TrickBot no comparte relación con el código fuente de Emotet, pero normalmente es utilizado como carga para realizar un desplazamiento lateral y distribuir, a su vez, otras piezas de código dañino como el *ransomware* Ryuk.

El proceso de infección de Emotet comienza con la llegada de un correo electrónico que podría parecer legítimo a primera vista, al estar escrito en el mismo idioma del receptor usualmente y pretendiendo ser enviado por una dirección que resulta familiar, incitando a la apertura de un documento ofimático que es recibido como fichero adjunto o con un enlace para descargarlo de Internet.

Tras abrir este documento, en caso de encontrarse activadas la vista protegida y el aviso de macros, al hacer *click* para editar y activarlas o, en caso contrario, simplemente abriéndolo, se ejecutan macros con código *Visual Basic For Aplication* (VBA) que se encargan de crear un proceso PowerShell para descarga de Internet el binario de Emotet, tratándose usualmente de sitios que utilizan el CMS Wordpress y han sido comprometidos para alojarlo. Éste se copia y ejecuta desde la carpeta del usuario e inicia el proceso de persistencia.

Una vez ejecutado en el sistema, el binario de Emotet intenta obtener persistencia para ejecutarse siempre que se inicie el sistema. La técnica utilizada varía en función del nivel de privilegios con el que se ejecute:

- Si la muestra se ejecuta con privilegios de Administrador, crea un servicio en el SO para arrancar con el inicio del sistema y se copia en las carpetas de instalación de Windows System32 o SysWOW64, en función de si se trata de un sistema de 32 o 64 bits. De esta forma el binario se ejecutaría sin importar el usuario que inicie el sistema.
- En caso contrario, utiliza la clave *Run* del registro de Windows para el usuario y copia el binario a la carpeta %LOCALAPPDATA%.

Tras obtener persistencia, el código dañino está preparado para conectar con sus servidores de mando y control para descargar código dañino adicional.

Por un lado, Emotet posee módulos propios para realizar acciones como robo de credenciales almacenadas en navegadores web (basado en la utilidad *WebBrowserPassView*) y clientes de correo (basado en la utilidad *Mail PassView*), propagación en la red mediante el protocolo SMB y credenciales obtenidas de la memoria del usuario infectado, haciendo fuerza bruta con un listado de contraseñas para los usuarios de las máquinas objetivo, robo de contactos de la cuenta de Outlook o envío de SPAM desde el propio equipo víctima para continuar propagándose.

Adicionalmente, Emotet despliega, en función de la ubicación y campaña, diferentes códigos dañinos como, por ejemplo, Trickbot. Este código dañino es completamente independiente de Emotet y posee sus propios mecanismos de persistencia, movimiento lateral mediante módulos y capacidad de despliegue de otros códigos dañinos, en concreto dispone de las siguientes acciones:

- Módulo de gusano SMB (worm.dll y spreader.dll) que hace uso del *exploit EternalBlue* (CVE-2017-0144 / MS17-010) para propagarse e intentar aumentar los privilegios a nivel del sistema.
- Módulo para extracción de credenciales RDP (pwgrab32.dll).
- Módulos para obtener información o realizar acciones que resulten interesantes para los atacantes como sceenlocker.dll, systeminfo.dll o vncsrv.dll.

En los casos de campañas de Trickbot distribuidas por Emotet es usual encontrar como carga útil el *ransomware* Ryuk, el cual cifra todos los ficheros de la máquina víctima. Esta carga, normalmente es distribuida de forma semiautomática o manual y es común ver el uso de puertas traseras como *Empire Powershell* o *Cobalt Strike* que los atacantes utilizan gracias al uso de la información obtenida a través de los códigos dañinos descritos.

A continuación, se puede observar el proceso completo de infección.

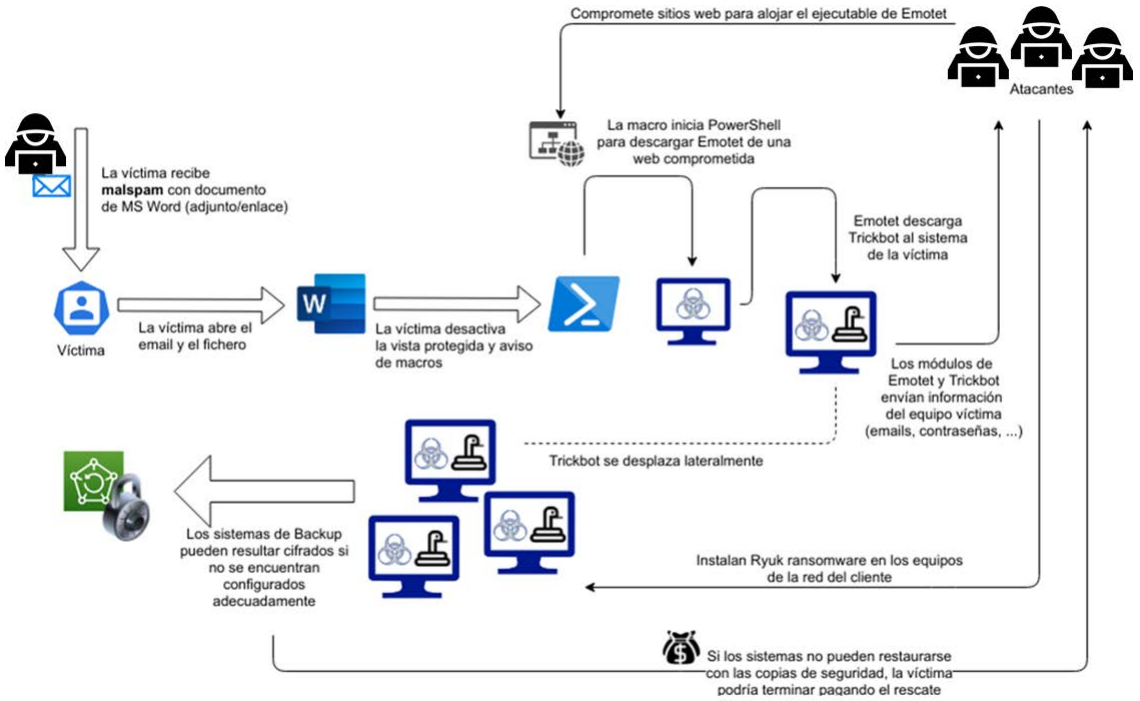


Ilustración 1. Gráfico que ilustra el proceso de infección de Emotet

Para más información técnica sobre estas amenazas pueden consultarse los informes de código dañino publicados por el CCN-CERT:

- CCN-CERT ID-23/19 Emotet[1].
- CCN-CERT ID-24/19 TrickBot[2].
- CCN-CERT ID-26/19 Ryuk[3].

3. MÉTODOS DE PREVENCIÓN

Atendiendo al comportamiento de este tipo de código dañino, debe tomarse especial atención en todas aquellas medidas que puedan mejorar la seguridad y que podrían prevenir su actuación, en todos los niveles a los que pueda producirse.

3.1 CORREO ELECTRÓNICO

En cuanto al correo electrónico, se deben de bloquear aquellos que contengan enlaces dañinos conocidos, como los que pueden obtenerse de repositorios como por

[1] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4183-ccn-cert-id-23-19-emotet/file.html
[2] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4189-ccn-cert-id-24-19-trickbot/file.html
[3] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4217-ccn-cert-id-26-19-ryuk-1/file.html

ejemplo el de *URLhaus*[4]. Haciendo uso de los listados *SURBL* y *Spamhaus DBL* de esta plataforma, deberían filtrarse todos aquellos correos electrónicos que contengan un enlace a un dominio listado en ellos o bloquear su acceso a nivel de red. El procedimiento para incluir estos listados dependerá de la solución que se tenga instalada. También habrá que tener en cuenta que, al tratarse de repositorios mantenidos por la comunidad, pueden darse casos de falsos positivos. Por otro lado, se debería controlar la recepción de correos electrónicos con documentos ofimáticos que contengan macros VBA.

Cualquier documento que sea abierto desde el correo electrónico Outlook debería abrirse en el modo Vista Protegida y, aunque el documento incite a desactivarla, no hacerlo nunca.

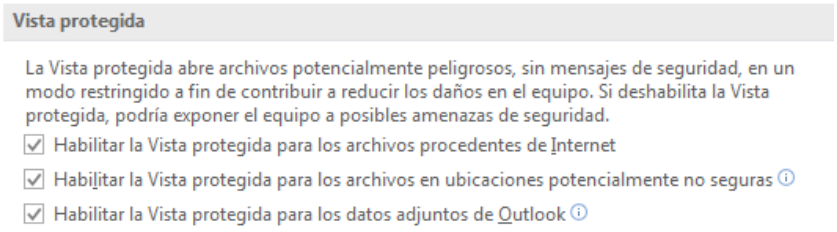


Ilustración 2. Configuración de vista protegida para documentos adjuntos de MS Outlook

No obstante, para más información técnica y recomendaciones para la protección del correo electrónico, se puede consultar la Guía de CCN-CERT IA-52/19 - Implementación Segura de Microsoft Windows/Office frente a la Campaña EMOTET[5].

3.2 MICROSOFT WORD

Para prevenir la ejecución del código VBA, se deberían deshabilitar por defecto la ejecución de macros en documentos ofimáticos y no permitir su ejecución mediante la opción “Habilitar contenido”.

[4] https://urlhaus.abuse.ch/
[5] 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

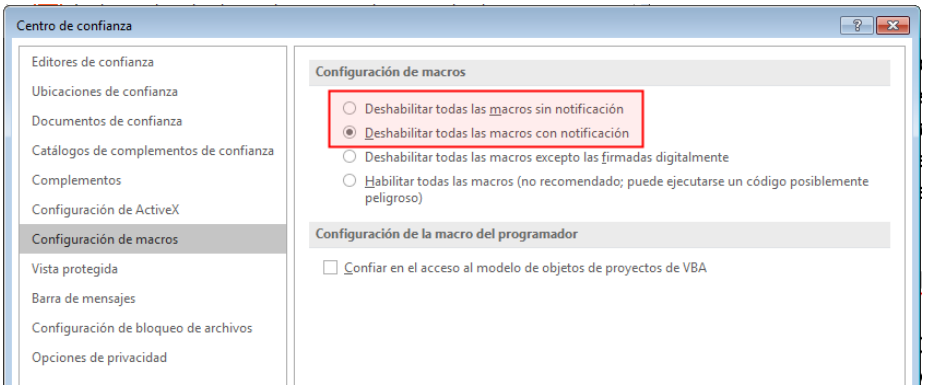


Ilustración 3. Configuración de macros en MS Word

3.3 SISTEMA OPERATIVO

A nivel de SO, se deberían aplicar políticas de seguridad que endurezcan las condiciones de ejecución de código procedente de fuentes desconocidas o que adviertan al usuario de la peligrosidad de sus acciones. A no ser que sea exclusivamente necesario, tampoco debería permitirse la ejecución de PowerShell en los equipos. Además, se debería comprobar que los sistemas estén parcheados frente a *exploits* como *EternalBlue* (CVE-2017-0144) y *BlueKeep* (CVE-2019-0708) implementando una política consolidada de actualizaciones de seguridad del SO y aplicaciones.

En cualquier caso, es también muy recomendable aplicar mecanismos integrales de protección de tipo Endpoint (EDR) con análisis y protección frente a comportamientos dañinos que ofrezcan una medida preventiva adicional a la detección basada en firmas de los motores antivirus convencionales.

Se debería prestar especial atención al acceso a los Controladores del Dominio corporativo y proveerlos de mecanismos para poder detectar los indicadores aquí descritos.

3.4 ARQUITECTURA DE RED

Como norma general, la arquitectura de red de la organización debería estar correctamente segmentada y disponer de los mecanismos necesarios para poder filtrar el acceso a sitios y direcciones de Internet. Además, todos los sistemas deberían de estar integrados en un sistema de log (SIEM) para poder correlacionar la actividad que ocurre en los equipos de la organización.

Por último, para más información sobre medidas adicionales que tomar, puede consultarse la Guía de CCN-CERT IA-51/19 - Prevención de la campaña de código dañino EMOTET con medidas técnicas de las guías CCN-STIC de ENS nivel ALTO[6].

4. DETECCIÓN DE LA AMENAZA

Para la detección de un sistema comprometido por el código dañino Emotet, se debe tener en cuenta los dos posibles escenarios, dependiendo de los privilegios de ejecución:

- El código dañino se ha ejecutado con privilegios de administrador.
- El código dañino se ha ejecutado con privilegios de usuario estándar.

En el escenario de ejecución con privilegios de administrador, el código dañino crea una copia de sí mismo a la carpeta "%WINDIR%\System32" (32-bit) o "%WINDIR%\SysWOW64" (64-bit), dependiendo de la arquitectura del Sistema Operativo, el nombre fichero del código dañino en su nueva localización es diferente para cada equipo, por lo cual será necesario conocer cuáles son los ficheros frecuentes contenidos en esas carpetas.

Puesto que todos los ficheros ejecutables alojados en estas carpetas son ficheros propios del SO y son bien conocidos y debería ser trivial localizar el binario del código dañino.

En este caso, para que el código dañino se pueda ejecutar de forma automática tras un reinicio de la máquina, éste crea un nuevo servicio dentro del Sistema Operativo con el mismo nombre con el que se copió en alguno de los directorios descritos en el anterior párrafo.

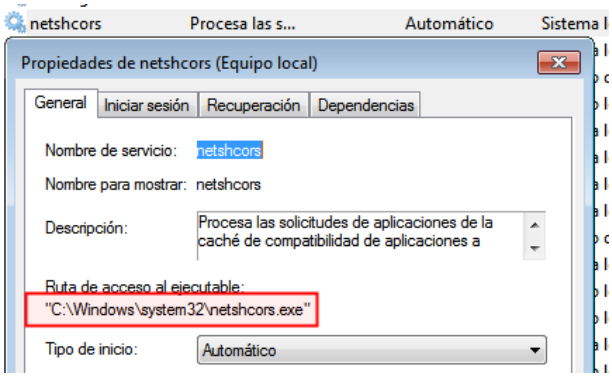


Ilustración 4. Servicio creado por Emotet cuando se ejecuta como usuario administrador.

[6] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4119-ccn-cert-ia-51-19-prevencion-de-la-campana-de-codigo-danino-emotet-con-medidas-tecnicas-de-las-guias-ccn-stic-de-ens-nivel-alto-1/file.html

En el escenario de ejecución con privilegios de usuario estándar, al igual que en el anterior escenario, el código dañino se copia a sí mismo en una nueva localización, "%LOCALAPPDATA%\<NOMBRE_ALEATORIO>". El nombre del ejecutable es diferente para cada equipo y coincide con el nombre de la carpeta donde se ha copiado.

En este caso, para que el código dañino se pueda ejecutar de forma automática para dicho usuario tras cada reinicio, se crea un nuevo valor para la clave de registro "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", donde el nombre asignado a este nuevo valor coincide con nombre del fichero dañino sin la extensión y el campo "Datos" contiene la ruta hasta el fichero dañino.

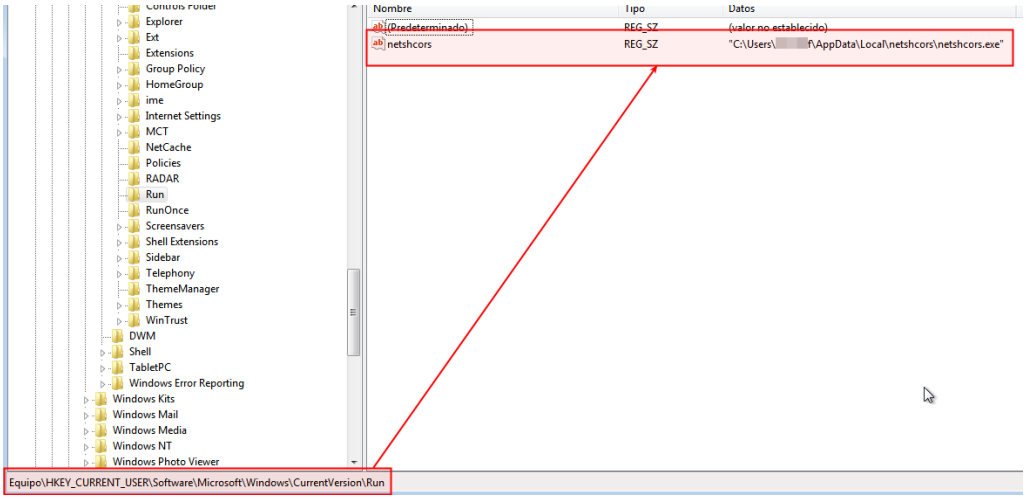


Ilustración 5. Clave de registro creada por Emotet cuando se ejecuta como usuario estándar.

A nivel de red, se debe prestar especial atención a conexiones http (no https) sospechosas a los puertos 443, 447 y 449, que son los más utilizados por este código dañino.

Si la infección ha proseguido, o la máquina ha sido comprometida por desplazamiento lateral, se pueden haber descargado al equipo otros códigos dañinos adicionales como Trickbot. Tal y como puede consultarse en el documento CCN-CERT ID-24/19 TrickBot, adquiere persistencia mediante una tarea programada por lo que se debería comprobar la existencia de ésta, que seguramente apunte a un binario en la ruta %APPDATA% en la que suele instalarse.

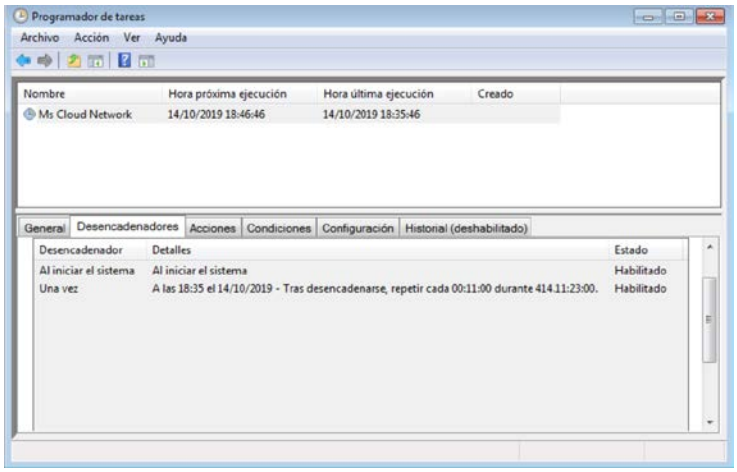


Ilustración 6. Tarea programada creada por Trickbot

También, puede darse el caso de que Trickbot haya conseguido descargar al sistema otro código dañino como el *ransomware* Ryuk. Si éste ha llegado a ejecutarse, será evidente puesto que aparecerán ficheros con su extensión y nota de rescate.

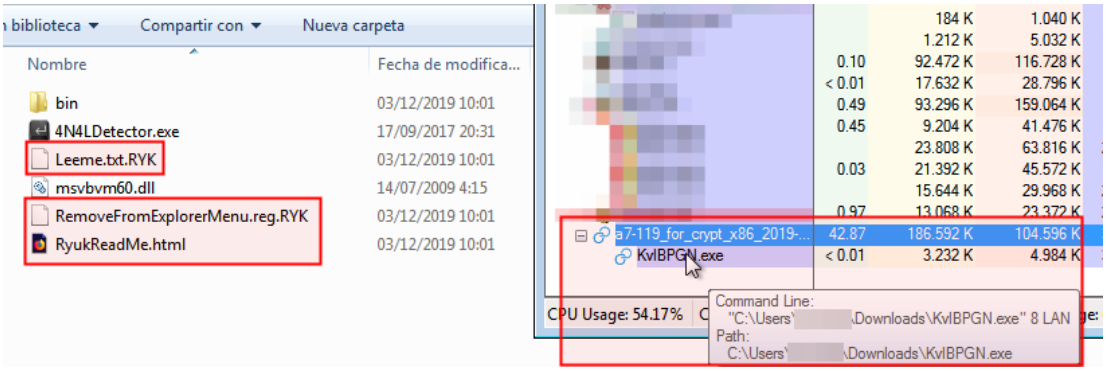


Ilustración 7. Ficheros creados en equipo infectado por Ryuk y ejecución en curso observada en Process Explorer

5. MÉTODOS DE DESINFECCIÓN

Para realizar la completa desinfección de una campaña de Emotet es necesario, en primer lugar, identificar la fase en la que se encuentra y características de la infección.

La recepción o incluso apertura del documento, no conlleva a una infección si no se ha llegado a ejecutar el código de las macros. Igualmente, si el código de las macros se ha ejecutado y PowerShell ha intentado descargar un fichero de las URL configuradas, pero estas se encontraban caídas o bloqueado su acceso en el proxy de la compañía, la infección no debería de haber proseguido, por lo que bastaría con eliminar el documento y correo.

Para comprobar si el binario Emotet se ha llegado a ejecutar con permisos de administrador, hay que comprobar la existencia de un servicio asociado a un ejecutable de las carpetas indicadas que no sea ninguno de los legítimos de Windows, para lo cual se debería de contar con un listado de ellos obtenido de una instalación

limpia. Esta comprobación puede realizarse mediante programación o, de forma manual en el apartado de propiedades del servicio, yendo a la pestaña "General" y, en la opción "Ruta de acceso al ejecutable:", se encontrará la ruta de instalación.

En caso de no haberse ejecutado con permisos de administrador, hay que localizar la clave de registro descrita en el apartado anterior. Mediante una cuenta de administrador, deberían comprobarse todos los árboles de registro de la clave HKEY_USERS, que contiene la configuración de cada uno para comprobar si existe dicha entrada en alguno de ellos. En caso de encontrar una entrada que coincida con el patrón, se debe desinfectar la ruta a la que apunte dicha clave.

Idealmente, este proceso debería realizarse arrancando el equipo en modo seguro y desconectado de la red para evitar ejecuciones adicionales del código dañino en caso de haber obtenido persistencia o haberse ejecutado mediante movimiento lateral.

En caso de que la infección haya proseguido, descargando al equipo otros códigos dañinos adicionales como Trickbot o éste se ha propagado de forma lateral por la red, se debería comprobar la existencia de la tarea programada descrita en el apartado anterior y proceder a su eliminación, además de la del binario en la ruta de %APPDATA% en la que se instala.

Si Trickbot ha conseguido descargar al sistema otro código dañino como el *ransomware* Ryuk, se pueden dar dos casos, puesto que se han observado muestras que no adquieren persistencia, como la descrita en el documento CCN-CERT ID-26/19 Ryuk, por lo que para desinfectar bastaría con reiniciar el equipo en las condiciones descritas y eliminar el binario. En el caso de muestras que tienen persistencia, ésta suele ser mediante la misma clave de registro que Emotet, por lo que debería ser fácil de localizar.

De esta forma se procederá a la eliminación de los códigos dañinos del equipo, eliminando siempre primero el método de persistencia, si lo hubiera y, a continuación, borrando los ficheros identificados.

6. RECOMENDACIONES

Como norma general, se proveen una serie de recomendaciones generales que se deberían siempre de tener en cuenta para evitar cualquier tipo de compromiso de los sistemas:

- Mantener los Sistemas Operativos, el software de ofimática y el resto de software instalado en los equipos actualizados con los últimos parches de seguridad.
- Mantener los sistemas de antivirus actualizados con las últimas firmas disponibles.

- Evitar el uso de software que no disponga de soporte oficial.
- Deshabilitar el uso de macros en ficheros ofimáticos y mantener siempre que se desconfíe de su origen la vista protegida activada.
- Evitar o restringir los permisos administrativos cuando sea posible.
- Aislar los equipos infectados con código dañino.
- Aplicar políticas de backup, considerando respaldos fuera de línea y copias diarias, entre otras medidas.
- Forzar al empleo de contraseñas robustas.
- Deshabilitar la ejecución de macros en documentos office.
- Usar una política de *whitelisting para las conexiones al exterior.*
- Deshabilitar la ejecución de PowerShell, siempre que no sea necesario.
- Limitar el uso de cuentas con privilegios elevados, la activación del uso de escritorios remotos, el almacenamiento de contraseñas en formato de texto plano y, revisar el acceso y permisos de directorios compartidos.
- Aplicar políticas de red, como segmentación de red entre otras.
- Uso de vacunas como EMOTET-STOPPER[7] elaborada por el CCN.

Para más recomendaciones y mecanismos de protección frente a infecciones de este tipo de códigos dañinos, se puede consultar la guía de CCN-CERT IA-11/18 - Medidas de seguridad contra ransomware[8].

7. CONCLUSIONES

Teniendo en cuenta las medidas aplicables, se puede determinar que las acciones dañinas derivadas de la ejecución del código dañino EMOTET y sus módulos o familias que pueda distribuir pueden ser controladas, impidiendo su acción o, al menos, limitándola. De esta forma, para acometer estas medidas se deben aplicar las recomendaciones mencionadas en este documento, así como las indicadas en los documentos que se hacen referencia, como por ejemplo: ampliando y actualizando los recurso tecnológicos, invirtiendo en formación y concienciación, aplicando políticas de seguridad (infraestructura, accesos físicos, contraseñas, backups, auditorias, etc.) y asignando personal dedicado, entre otras medidas.

[7] http://ccn-cert.net/emotet2019
[8] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html