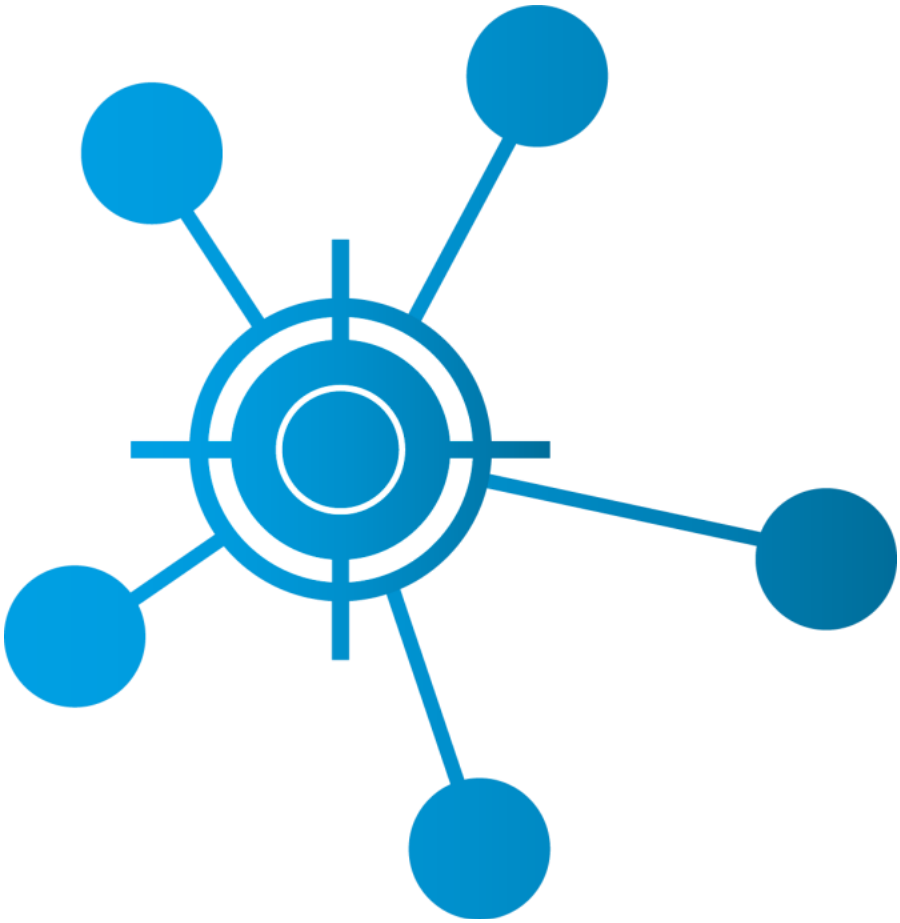
CCN-CERT IA-51/19

Prevención de la campaña de código dañino EMOTET con medidas técnicas de las guías CCN-STIC de ENS nivel ALTO



Octubre 2019

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.10.07 17:12:56 +02'00'

Fecha de Edición: octubre de 2019

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. INTRODUCCIÓN

Cada vez más a menudo se muestra que las configuraciones predeterminadas con las que cuentan los sistemas operativos y aplicaciones no sirven para frenar acciones perniciosas que afectan a los sistemas de la información. Solo configuraciones de protección consolidadas y enfocadas a la mejora en la seguridad, pueden ser capaz de frenar los vectores que actualmente emplean los atacantes y que en ocasiones pueden aprovechar funcionalidades propias de los productos.

Recientemente se ha identificado una campaña de acción por parte del código dañino EMOTET que está afectando de forma significativa a los sistemas de la información. ¿En qué consiste dicha campaña y que consideraciones son importantes para la aplicación de medidas adecuadas?

1.1 VECTOR DE ATAQUE

El código dañino EMOTET constituye una aplicación maliciosa con un vector de ataque bastante conocido y que presenta las siguientes características:

a) El punto de entrada o infección se produce mediante la ejecución de código embebido desde un documento ofimático a través de aplicaciones tales como MS Word.

b) Dicho script, inicializa un proceso de conexión contra servidores y sistemas de comando y control, existentes en Internet, que descargan un código dañino e inicializan la infección del sistema. Una vez producida la infección se lleva a cabo el cifrado del sistema, realizándose además otras acciones no autorizadas.

c) Para garantizar la fase de persistencia, el código dañino iniciará dos potenciales acciones:

   i. Alteración del sistema con elevación de privilegios.

   ii. Movimientos en la red mediante la dispersión replicándose en otros sistemas.

d) Otras acciones relacionadas con la post explotación tomando en consideración la realización de movimientos laterales, exfiltración de datos o robo de información sensible.

1.2 CONSECUENCIAS

Una vez que la acción maliciosa se ha producido, el sistema de información se ve afectado por las siguientes consecuencias:

a) El código dañino inicializa un proceso de secuestro del sistema mediante el cifrado del contenido en los sistemas de información afectados, servidores y puestos de trabajo.

b) El código dañino puede robar y exfiltrar contenido sensible de la organización tales como documentos, información de índole bancaria, credenciales y otras que pueden afectar a la integridad del sistema o perjudicar la imagen de la organización afectada.

c) Otras consecuencias tales como formar parte de una red de tipo “botnet” mediante la integración de los sistemas afectados en un sistema de mando y control para la manipulación y ejecución de acciones no autorizadas.

2. MECANISMOS DE PREVENCIÓN APLICABLES A TRAVÉS DE LOS DOCUMENTOS DE SEGURIDAD CCN-STIC PARA EL ENS EN SU CATEGORÍA ALTA

Atendiendo a la forma de actuar de este tipo de código dañino, deben tomarse en consideración todas aquellas medidas, que siendo de aplicación en los sistemas de la información, quedan recogidas en las guías técnicas de seguridad CCN-STIC que mejoran la seguridad y podrían prevenir su actuación:

a) Protección del sistema operativo.

b) Protección de productos ofimáticos.

Los puntos clave de la protección son los siguientes:

a) Ejecución de contenido activo y scripts en documentos ofimáticos.

b) Endurecimiento de las condiciones de ejecución de código en el sistema operativo.

c) Prevención frente a la alteración local del sistema operativo.

d) Bloqueo de conexiones para minimizar los movimientos laterales entre sistemas que permitan la dispersión del código dañino en la red local.

e) Otras medidas preventivas que recogidas en el ENS ayudarían a frenar el proceso de infección o mitigar la acción dañina:

   i. Implementación de una solución frente a código dañino, así como mantener actualizada la misma.

   ii. Implementación de una política consolidada de actualizaciones de seguridad del sistema operativo y aplicaciones que limite la explotación de vulnerabilidades que puede emplear un código dañino para garantizar su persistencia o llevar a cabo movimientos laterales.

Adicionalmente a estas medidas recogidas en las guías CCN-STIC aplicables sobre el ENS de nivel alto, no deben desdeñarse adicionalmente otras potenciales medidas que ofrecerían la protección adecuada:

a) Aplicar mecanismos integrales de protección Endpoint con análisis y protección frente a comportamientos dañinos que ofrezcan una medida preventiva adicional a la detección basada en firmas.

b) Aplicar mecanismos de protección en el perímetro consolidadas, con prevención frente a conexiones internas a sitios de contenido malicioso o de mando y control.

Para especificar las medidas de seguridad a tener en cuenta se ha hecho uso de las guías de seguridad definidas a continuación:

a) CCN-STIC-599A18: Dentro del citado documento se ha hecho uso de las medidas de seguridad definidas en el Anexo A dedicado al ENS y más concretamente las configuraciones aplicables a la categoría alta del ENS.

b) CCN-STIC-585: El presente informe toma como medidas de seguridad todas aquellas configuraciones implementadas por medio de la guía aplicable a Office 2013 en su configuración para un entorno de dominio dentro de la categoría alta del ENS.

2.1 PROTECCIÓN DE EJECUCIÓN DESDE DOCUMENTOS OFIMÁTICOS

En el caso de la campaña de EMOTET es punto clave como inicializador de la acción maliciosa la ejecución desde un documento ofimático mediante código embebido. Este se hecho se da habitualmente mediante la ejecución de macros, scripts, códigos de Visual Basic u otros. En este sentido un primer punto de interrupción de la aplicación dañina sería la ejecución automatizada de los mismos, siendo necesaria una actuación forzosa y voluntaria del usuario para que el contenido de un documento pueda afectar negativamente al sistema.

En este sentido cabe determinar que las plantillas de protección definidas en las guías CCN-STIC de office en su nivel alto se ha tenido en consideración dicho hecho, presentando medidas de prevención, incluso forzando que documentos no confiables como los descargados de internet o contenidos en correos electrónicos en Outlook, sean forzado a su apertura en vista protegida. Esta, aun no teniendo en consideración las otras medidas dispuestas, impedirían de forma consciente la ejecución del contenido activo dañino que es precursor del resto de acciones dañinas.

Solo una acción consciente del usuario permitiría que el código fuera ejecutado.

Las medidas de protección recogidas en la guía CCN-STIC críticas para el control del primer proceso son las siguientes:

a) Seguridad de automatización: Esta configuración de directiva controla si se pueden ejecutar macros en una aplicación de Office 2016 abierta mediante programación por otra aplicación.

   La configuración de esta directiva se establece en “Deshabilitar macros de forma predeterminada” de modo que se deshabilitan todas las macros en la aplicación abierta mediante programación.

b) Bloquear complementos web: Esta configuración de directiva permite impedir que los usuarios usen complementos web.

   La configuración de esta directiva se establece “Habilitado”, de forma que los complementos web se bloquean y se ignoran el resto de configuraciones de directiva en la carpeta Catálogos de confianza.

c) Advertencia de firma: Esta configuración de directiva controla el modo en que Outlook advierte a los usuarios acerca de mensajes con firmas digitales no válidas.

   Esta configuración se encuentra “Habilitada” y en modo “Advertir siempre sobre las firmas no válidas” lo que permite que la aplicación advierta al usuario de forma sistemática cuando intente hacer uso de un mensaje con una firma no válida.

d) Desactivar la Vista protegida para los datos adjuntos abiertos desde Outlook: Esta configuración de directiva le permite determinar si los archivos de Word de los datos adjuntos de Outlook se abrirán en la Vista protegida.

   La configuración de esta directiva se establece en “Deshabilitado” de modo que dichos archivos se abrirán siempre en el modo “Vista protegida”.

e) Establecer el comportamiento de los documentos si se producen errores durante la validación del archivo: Esta clave de directiva controla la administración de los documentos de Office cuando se produce un error en la validación de archivos.

Esta configuración se encuentra "Habilitada" y en modo "Bloquear completamente archivos", lo que impide que los usuarios puedan abrir los archivos.

f) No abrir los archivos de la zona Internet en la Vista protegida: Esta configuración de directiva le permite determinar si los archivos descargados de la zona "Internet" se abrirán en la Vista protegida.

   La configuración de esta directiva se establece en "Deshabilitado" de modo que dichos archivos se abrirán en el modo "Vista protegida".

g) No abrir los archivos de ubicaciones no seguras en la Vista protegida: Esta configuración de directiva le permite determinar si los archivos de ubicaciones no seguras se abrirán en la Vista protegida.

   La configuración de esta directiva se establece en "Deshabilitado" de modo que dichos archivos se abrirán en el modo "Vista protegida".

h) Desactivar documentos confiables: Esta configuración de directiva permite desactivar la característica "Documentos confiables". La citada característica permite a los usuarios habilitar siempre el contenido activo de documentos como macros, controles ActiveX, conexiones de datos, etc. para que no pregunten al usuario la próxima vez que abran documentos. Los documentos confiables quedan excluidos de las notificaciones de seguridad.

   Esta configuración se encuentra "Habilitada" lo que permite que los usuarios reciban una notificación de seguridad cada vez que se abre un documento que contiene contenido activo.

2.2 PREVENCIÓN DE EJECUCIÓN LOCAL Y MODIFICACIÓN DEL SISTEMA

Una vez producida la primera fase y asumiendo que el sistema haya podido conectarse a Internet, la siguiente consecuencia pasa por la descarga local de una aplicación y su ejecución. En este sentido deben tenerse en consideración dos posibles variantes:

a) Elevación de privilegios locales para una ejecución privilegiada.

b) Ejecución en el contexto de un usuario.

Para que la primera de las consecuencias puede darse, el código dañino debe haber adquirido en una otra medida privilegios administrativos sobre el sistema. Con unas medidas de seguridad adecuadas y tomando en consideración los mecanismos aplicables que recogen las guías CCN-STIC, este hecho requiere una acción consciente por parte del administrador. Esto es así puesto que la configuración del Control de Cuentas de Usuario advertirá y solicitará credenciales a un administrador para ejecutar dicha acción.

Adicionalmente el sistema tendrá implementados una serie de mecanismos adicionales que limitarán la alteración o manipulación del sistema.

Si te tiene en consideración el otro vector de acción dañina, la afectación sería menor limitándose a una acción local sobre ficheros donde el usuario tuviera permisos o bien en red, pero sin afectar al propio sistema operativo.

La fase de persistencia local del sistema nuevamente constituye como necesidad la alteración del sistema operativo para el mantenimiento de la afectación más allá del reinicio del equipo.

Las medidas de prevención recogidas en la guía de protección del sistema operativo se definen en los siguientes apartados.

2.2.1 CONTROL DE CUENTAS DE USUARIO (UAC)

El control de cuentas de usuario (UAC) fue introducido en Microsoft Windows Vista y Microsoft Windows Server 2008 como un mecanismo para limitar las acciones administrativas de aquellos usuarios que no eran conscientes del empleo de sus privilegios. UAC permite a los usuarios iniciar sesión en sus equipos con una cuenta de usuario estándar. Los procesos lanzados utilizando un token de usuario estándar pueden realizar tareas mediante los derechos de acceso concedidos a un usuario estándar. Por ejemplo, el explorador de Windows automáticamente hereda permisos de nivel de usuario estándar. Además, todos los programas que se ejecutan mediante el explorador de Windows (por ejemplo, haciendo doble clic en un acceso directo de la aplicación) también se ejecutan con el conjunto estándar de permisos de usuario. Muchas aplicaciones, incluyendo las que se incluyen con el sistema operativo, están diseñadas para funcionar de esta manera.

No obstante, otras aplicaciones, especialmente aquellas que no fueron diseñadas específicamente otorgando prioridad a la configuración de la seguridad, a menudo requieren permisos adicionales para poder ser ejecutadas con éxito. Este tipo de programas se denominan aplicaciones heredadas. Además, acciones como instalar nuevo software y realizar cambios de configuración en programas como Firewall de Windows, requieren más permisos que los que están disponibles en una cuenta de usuario estándar.

Cuando una aplicación tiene la necesidad de ejecutar con derechos de usuario más estándar, la UAC puede restaurar grupos de usuarios adicionales para el token. Esto permite al usuario tener un control explícito de programas que están haciendo cambios de nivel de sistema para su máquina. Tras la revisión de la directiva P3P de privacidad del sitio web, el usuario podrá especificar cómo desea que internet administre las cookies de dicho sitio web o si se permite o no que el sitio web almacene cookies en el equipo. Esto, se hará a través de la comparación de la directiva de privacidad del sitio con la configuración de privacidad del usuario. Para ello, el usuario deberá activar la casilla “Comparar la directiva de privacidad de las cookies con mi configuración”.

En MS Windows 10 la funcionalidad del UAC es mejorada para:

a) Permitir que un usuario con privilegios de administrador pueda configurar la experiencia UAC a través del Panel de Control.

b) Proporcionar directivas de seguridad local adicional que permitan que un administrador local cambie el comportamiento de los mensajes UAC, para administradores locales, en modo de aprobación de administrador.

c) Proporcionar directivas de seguridad local adicional que permitan que un administrador local cambie el comportamiento de los mensajes UAC para los usuarios estándar.

UAC es configurada en la categoría alta para definir el siguiente comportamiento:

a) Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador.

   Esta directiva se establece en “Pedir credenciales en el escritorio seguro” de modo que cualquier usuario administrador debe autenticarse con sus credenciales para realizar modificaciones en el Sistema Operativo.

b) Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándarPedir credenciales en el escritorio seguro.

   Esta directiva se establece en “Pedir credenciales en el escritorio seguro” de modo que cualquier usuario estándar debe autenticarse con sus credenciales para realizar modificaciones en el Sistema Operativo.

Teniendo en consideración las configuraciones anteriores cualquier intento de modificación sobre el equipo deberá estar autorizado por un usuario con privilegios.

2.2.2 SMART SCREEN

Una defensa en profundidad no debe desdeñar nunca ningún mecanismo que pueda suponer una mejora en la seguridad global. En este sentido Microsoft ha incorporado desde hace tiempo un complemento de navegación que ayuda a identificar sitios web comprometidos o empleados parapPhising o la distribución de código dañino: el filtro SmartScreen.

Asumiendo la posibilidad de que un script puedan forzar a un usuario a realizar una navegación a sitios web para la descarga de contenido, el filtro SmartScrren permitirían limitar dicha acción. Aunque esta prevención sería mucho más adecuada mediante una protección en el perímetro defensivo de la organización impidiendo acceso a URL o IP consideradas de lista negra, al menos una función activa como la de SmartScreen prevendría conexiones de navegación a sitios potencialmente peligrosos.

SmartScreen de Windows Defender proporciona mensajes de advertencia que ayudan a proteger a los usuarios contra posibles estafas de suplantación de identidad (phishing) y software malintencionado.

SmartScreen ayuda a proteger los equipos, ya que muestra una advertencia a los usuarios antes de ejecutar programas potencialmente malintencionados de Internet. Esta advertencia se presenta en un cuadro de diálogo intersticial que se muestra antes de ejecutar una aplicación descargada de Internet y que no se reconoce o se sabe que es malintencionada.

Dentro de la configuración especificada para la categoría alta se implementan medidas de seguridad dedicadas al bloqueo de ejecución de código malicioso, las cuales se definen a continuación:

a) Configurar SmartScreen de Windows Defender: Esta directiva se encuentra “Habilitada” lo que permite que SmartScreen de Windows Defender esté activado y los usuarios no podrán desactivarlo.

b) Configurar SmartScreen de Windows Defender: Esta directiva, aunque nombrada igual que la anterior se encuentra en “Habilitado” con la opción "Advertir e impedir la omisión", de modo que los cuadros de diálogo de SmartScreen no presentarán al usuario la opción de omitir la advertencia y ejecutar la aplicación. SmartScreen seguirá mostrando la advertencia cuando se intente ejecutar de nuevo la aplicación.

2.2.3 INTEGRIDAD DE FICHEROS

Por medio de la implementación de seguridad a través de los documentos de seguridad CCN-STIC en el ENS se establece como medida de seguridad la restauración de ficheros concretos del sistema en el inicio lo que permite asegurar la integridad y confiabilidad de estos, asegurando que son legítimos y que no realizan acciones no deseadas por medio de dichos ficheros.

Dentro del apartado que define esta configuración dentro de la guía de seguridad, es posible definir no solo los ficheros indicados por defecto en la directiva de grupo, si no incluir ficheros adicionales de diferentes rutas del Sistema para asegurar la integridad de los mismos. Algunos de estos ficheros pueden ser:

a) CMD.exe

b) PowerShell.exe

c) PowerShell_ISE.exe

d) WORD.exe

e) OUTLOOK.exe

3. DISPERSIÓN Y MOVIMIENTOS LATERALES

Toda vez que un sistema haya sido afectado por un código dañino, para garantizar la dispersión en una red y afectar a un número mayor de equipos, requiere la ejecución en otros sistemas. Esta acción se lleva a cabo normalmente mediante dos acciones:

a) Aprovechar debilidades de los sistemas, tales como vulnerabilidades, que permitan conexiones remotas con ejecución privilegiada.

b) Haber obtenido credenciales privilegiadas en un sistema, siendo aprovechadas para la validación en otros sistemas.

Si se produce un endurecimiento de las condiciones de uso de credenciales, los sistemas se mantienen actualizados según criterios recogidos en el propio Esquema Nacional de Seguridad y se limita las conexiones entre sistemas, dicha acción de dispersión puede quedar controlada.

La implementación de medidas tales como la protección de credenciales o la aplicación del firewall de tipo host bastión recogida en la guía prevendrían de dicha acción.

3.1 FIREWALL

Según lo definido en la norma “MP. COM. 3. PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD” Se deberá asegurar la autenticidad del otro extremo en un canal de comunicaciones antes de proceder al intercambio de datos entre los mismos. Además, deberá prevenirse ataques activos, garantizando que los mismos serán al menos detectados, permitiendo activarse los procedimientos que se hubieran previsto en el tratamiento frente a incidentes.

Para aquellos entornos con sistemas o información catalogados como de nivel alto, es recomendable el empleo de dispositivos hardware para el establecimiento y utilización de redes virtuales privadas, frente a soluciones de tipo software. Se deberá tener en consideración los productos que se encuentran certificados y acreditados.

A través de controles centralizados en plantillas de seguridad, se establecerán mecanismos que controlen el acceso y salida de información a los puestos de trabajo mediante el empleo del firewall en su modalidad avanzada. Por ello en la aplicación de seguridad base se establece una configuración base del Firewall de Windows el cual bloquea todas las conexiones entrantes que no coincidan con una regla.

Adicional a esto se especifican configuraciones para realizar una administración de este firewall de forma centralizada por medio de objetos de política de grupo y así mejorar las condiciones de seguridad en los puestos de trabajo.

3.2 AUTENTICACIÓN Y ALGORÍTMOS DE CIFRADO DÉBILES

Según lo definido en la norma "OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN" Dentro de los procesos habituales en el manejo de los sistemas de la información, el correspondiente a la autenticación, corresponde al primero a llevar a efecto. Antes de acceder a datos, gestionar recursos o tratar servicios es necesario indicar al sistema "quién eres".

El sistema de autenticación se puede traducir tecnológicamente mediante múltiples mecanismos, siendo el del empleo de una contraseña el más habitual pero no por ello el más seguro, sino todo lo contrario. Los mecanismos de autenticación se deberán adecuar en función del nivel de criticidad de la información o el servicio atendiendo lógicamente a diferentes criterios.

Según establece el propio Esquema Nacional de Seguridad, a grandes generalidades para el nivel alto, se prohíbe el uso de autenticadores basados en el empleo de claves concertadas. Se exige para ello el uso de dispositivos físicos o de biometría. Para ello deberán emplearse algoritmos acreditados por el Centro Criptológico Nacional, recogidos en la guía CCN-STIC-807 de criptología de empleo en el ENS.

Conforme a las necesidades establecidas por el Esquema Nacional de Seguridad se deberá tener también en consideración lo establecido en la guía CCN-STIC-804 para los mecanismos de autenticación y que se encuentra recogido en el punto 4.2.5.

La implementación del documento de seguridad tiene en consideración los siguientes aspectos, para el desarrollo de plantillas:

de seguridad por niveles, enfocados en los procesos de autenticación:

a) Gestión y definición de política de contraseñas.

b) Gestión y definición de política para los bloqueos de cuenta.

c) Implementación de algoritmos para el almacenamiento de contraseñas cifradas.

Dentro de las medidas de seguridad concretas que se implementan para la categoría alta se encuentran las siguientes:

a) Permitir algoritmos de criptografía compatibles con Windows NT 4.0: Esta configuración de directiva controla si el servicio de Net Logon permitirá el uso de los algoritmos de criptografía más antiguos que se usan en Windows NT 4.0. Los algoritmos de criptografía usados en Windows NT 4.0 y versiones anteriores no son tan seguros como los algoritmos más nuevos que se usan en Windows 2000 y versiones posteriores, incluida esta versión de Windows.

   La configuración de esta directiva se encuentra configurada en "Deshabilitado" de modo que Net Logon no permitirá la negociación y el uso de algoritmos de criptografía

obsoletos.

b) Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash: Atendiendo a la normativa en materia de uso de algoritmos validos se encuentra activa la función que permite emplear única y exclusivamente algoritmos compatibles con FIPS 140.

c) Seguridad de red: configurar tipos de cifrado permitidos para Kerberos: Esta directiva permite establecer los algoritmos validos para Kerberos dentro de todo el entorno de dominio asegurando de esta forma solo el uso de los algoritmos más robustos.

d) Se encuentran mejorados los procesos de gestión de ticket kerberos así como su durabilidad dentro del ámbito del dominio.

e) Seguridad de red: restringir NTLM: autenticación NTLM en este dominio: Esta configuración de directiva permite denegar o permitir la autenticación NTLM en un dominio.

   La configuración de esta directiva se establece en modo "Denegar todo", de modo que el controlador de dominio denegará todas las solicitudes de autenticación de acceso directo NTLM de sus servidores y para sus cuentas y devolverá un error de NTLM.

f) Seguridad de red: nivel de autenticación de LAN Manager: Esta configuración de seguridad determina el protocolo de autenticación desafío/respuesta que se usa para inicios de sesión de red. Esta opción afecta al nivel de protocolo de autenticación usado por los clientes, el nivel de seguridad de sesión negociado y el nivel de autenticación aceptado por los servidores

   Se configura esta directiva con el valor “Enviar solo respuesta NTLMv2 y rechazar LM y NTLM” impidiendo el uso de protocolos de autenticación vulnerables.

4. OTRAS MEDIDAS

Adicionalmente a las medidas técnicas que de forma implícita son aplicadas mediante la implantación de las guías CCN-STIC, deben tomarse también en consideración otra serie de acciones que recogen las propias guías y como recordatorio de los principios regulados en el Esquema Nacional de Seguridad.

Contar con un sistema de protección antivirus o de protección Endpoint, habiendo aplicado las medidas adecuadas y con la protección de prevención frente a comportamiento anómalos activos, prevendría la afectación en sus primeras fases.

La aplicación de procedimientos operacionales y protocolos del buen de los sistemas de la información también limitaría los perjuicios que ocasiona un código dañino.

Así, una política consolidada de no navegación, consulta de correo electrónico o apertura de documentos en servidores, limitaría la afectación sobre los servicios de la organización.

Emplear, por parte de los usuarios administradores, de cuentas estándar para tareas tales como la navegación, lectura de correos electrónico o la apertura de documento, limitaría la acción de un código dañino a una acción no privilegiada sin que esta pudiera afectar a los servicios de la organización.

Mantener una política de credenciales adecuada, segregando los roles y diferenciando el uso de las cuentas, limitará en gran medida los procesos de dispersión.

La aplicación de una política consolidada de actualización del sistema operativo y las aplicaciones reducirá drásticamente el impacto de explotación de vulnerabilidades que tiene como consecuencia la dispersión o ejecución privilegiada de contenido dañino para los sistemas.

4.1 ANTIVIRUS

Según lo definido en la norma "OP. EXP. 6. PROTECCIÓN FRENTE A CÓDIGO DAÑINO", y tal como reflejan las guías CCN-STIC, la organización deberá implementar para puestos de trabajo una solución antimalware que proteja contra código dañino. Se considerarán como tal los virus, gusanos, troyanos, programas espías y en general cualquier tipo de aplicación considerada como código dañino.

Debe tomarse en consideración que, aunque Windows 10 tenga implementada de forma predeterminada la solución Windows Defender, ésta no cubre todo el espectro de protección frente a código dañino Por ejemplo sin una solución de administración centralizada como la aportada por MS System Center 2012 Endpoint Protection o la de otros fabricantes no tendrá la visibilidad para hacer la gestión centralizada de la seguridad y gestión de incidencias demandadas por el Esquema Nacional de Seguridad.

Adicionalmente este producto en sí mismo no ofrece un mecanismo de protección con administración centralizada, objetivo fundamental de toda organización no solo para centralizar los procesos de despliegue y configuración de políticas de protección, sino de la centralización de los estados y reportes de detección y eliminación de código dañino.

Las organizaciones deberán por lo tanto proveer de otra solución frente a código dañino que ofrezca un alcance completo en la detección y eliminación de código dañino, así como atender a las recomendaciones del fabricante para su mantenimiento.

4.2 ACTUALIZACIONES DE SEGURIDAD

Según lo definido en la norma "OP. EXP. 4. MANTENIMIENTO", recogido así mismo en las guías CCN-STIC, para mantener el equipamiento físico y lógico se deberán atender a las especificaciones de los fabricantes en lo relativo a la instalación y mantenimiento de los sistemas. Se realizará un seguimiento continuo para garantizar la seguridad de los sistemas. Para ello deberá existir un procedimiento que permita analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

Adicionalmente a las actualizaciones de seguridad, debe tomar en consideración que el Sistema Operativo Windows 10 y servidores inaugura una nueva metodología basada en la revisión continua del sistema. Dicha revisión incluye nuevas funcionalidades y características al sistema. Las opciones de mantenimiento reflejan los tiempos máximos que tendrá la organización para mantener actualizado el sistema. No debe confundir no obstante dichas actualizaciones de funcionalidad con las actualizaciones tradicionales de seguridad.

Recuerde por lo tanto que deberá atender no solo a las especificaciones del fabricante en cuanto a las actualizaciones de seguridad, sino también a las actualizaciones que incluyen las mejoras de funcionalidad.

Dentro de la guía CCN-STIC de sistema operativo se incluye configuraciones para adecuar los puestos de trabajo o servidores a las diferentes ramas de actualización del sistema operativo según las necesidades de cada organización.

5. CONCLUSIONES

Tomando en consideración las medidas aplicables que recogen las guías de seguridad CCN-STIC para la categoría alta, se puede determinar que las acciones dañinas consecuencia de códigos como EMOTET pueden ser controladas, bien impidiendo su acción o bien limitando la misma. Solo acciones conscientes del usuario y degradando la seguridad existente podrían suponer un riesgo general para la organización, habiendo aplicado las medidas de protección adecuadas.

Además, debe tomarse en consideración que en general la aplicación efectiva de los principios de mínima exposición, mínimo privilegio y seguridad continua, sumada a la concienciación en materia de ciberseguridad, que quedan fielmente recogidas y son de inspiración en el Esquema Nacional de Seguridad, serían consideraciones a tomar siempre en cuenta para limitar o impedir acciones dañinas a través de campañas tales como la originada por el código EMOTET.