UNIVERSIDAD CATÓLICA de Colombia

GUÍA DE HARDENING PARA ELEVAR LOS NIVELES DE SEGURIDAD Y MINIMIZAR LOS RIESGOS DEL TELETRABAJO

CAMILO ALEJANDRO IBAÑEZ NARANJO
LUIS FELIPE RODRIGUEZ VARON

UNIVERSIDAD CATÓLICA DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ D.C
2020

UNIVERSIDAD CATÓLICA de Colombia

PALABRAS CLAVES

Ciberseguridad; Threat Intelligence; Teletrabajo; Adversarios; Phishing; BYOD (Bring Your Own Device).

UNIVERSIDAD CATÓLICA de Colombia

CONTENIDO

Resumen 5
Introducción **6**
Propósito y alcance 6
Público 6
Recomendaciones de seguridad para el teletrabajador **7**
Acceso Inicial 8
Spearphishing **9**
1. Indicadores que pueden ayudar a identificar con éxito un ataque **9**
2. Prácticas de seguridad **10**
2.1. Aplicación de parches y actualizaciones 10
2.2. Configure las funciones de seguridad en el cliente de correo 10
2.3. Otras Recomendaciones 10
Drive-by Compromise **11**
1. Identifique sitios web falsos **11**
2. Seguridad en navegadores **12**
2.1. Microsoft Edge 12-13
2.2. Google Chrome 14-15
2.3. Mozilla Firefox 16-17
3. Recomendaciones **18**
Replication Through Removable Media **19**
1. Prácticas de seguridad **19**
1.1. Mitigue el riesgo de infección 19
1.2. Deshabilitar ejecución automática 20
1.3. Cifrado de dispositivos 21-22
2. Recomendaciones **23**
Recomendaciones adicionales para el teletrabajador **24**
Recomendaciones de seguridad para el área de tecnología **25**
Ejecución **26**
Command and Scripting Interpreter **27**
1. Prácticas de seguridad **27**
1.1. Mitigue la ejecución de comandos 27
1.2. Detección 27
2. Protección de los activos de información contra ataques de PowerShell 28
2.1. Actualice Microsoft PowerShell V7.0.3 o superior 28
2.2. Use el modo de lenguaje restringido 28
2.3. Detección por regla sigma 28
3. Deshabilitar Windows Command Shell a través del registro 29
4. Regla sigma Visual Basic 30
5. Uso de firmas digitales para proteger 31
5.1. Crear una plantilla de certificado 31
5.2. Crear un certificado de firma 31
5.3. Firma de Scripts 32
Scheduled task/job 33
1. Prácticas de seguridad 33
1.1. Mitigue la ejecución de Programación de tareas 33
1.2. Detección 33
2. Configure las opciones de seguridad de las tareas programadas 34
2.1. Controlador de dominio 34
2.2. Aumentar la prioridad de programación a los administradores 35
2.3. Habilitar protección LSA 35
Malicious file **36**
1. Prácticas de seguridad **36**
1.1. Mitigue la ejecución de archivos maliciosos 36
1.2. Detección 36
2. Configure reglas de reducción de superficie de ataque **37-38**
Referencias **39**

RESUMEN

Para muchas organizaciones, sus empleados utilizan tecnologías de teletrabajo empresarial o acceso remoto para realizar trabajos desde ubicaciones externas. Todos los componentes de estas tecnologías, incluidos los dispositivos cliente emitidos por la organización y dispositivos BYOD, deben protegerse contra las amenazas de ciberseguridad.

Esta publicación proporciona información sobre las consideraciones de seguridad como respuesta a el análisis realizado de Threat Intelligence, los cuales revelaron como diferentes grupos de amenazas utilizan las técnicas de Spearphishing, Drive-by Compromise y Replication Through Removable Media como vector de ataque para comprometer a un usuario de teletrabajo de una entidad financiera. Al mismo tiempo, esta publicación destaca las recomendaciones de seguridad para las tácticas de **Ejecución** después del compromiso del **Acceso Inicial**.

INTRODUCCIÓN

Propósito y alcance

El propósito y alcance de este documento es ayudar a las organizaciones financieras a disminuir los riesgos vinculados a diversos grupos de amenazas y que buscan como objetivo comprometer a un usuario en teletrabajo.

El documento enfatiza la importancia del conocimiento de los usuarios de teletrabajo sobre Ingeniería Social, así como las recomendaciones de seguridad que deben tener en cuenta para no ser víctima de algún ciberdelincuente por **Acceso Inicial**.

Este documento proporciona de igual forma, recomendaciones de seguridad sobre como bloquear y mitigar el cumplimiento del objetivo del ciberdelincuente paras las técnicas de **Ejecución** analizadas en la **Threat Intelligence**.

Público

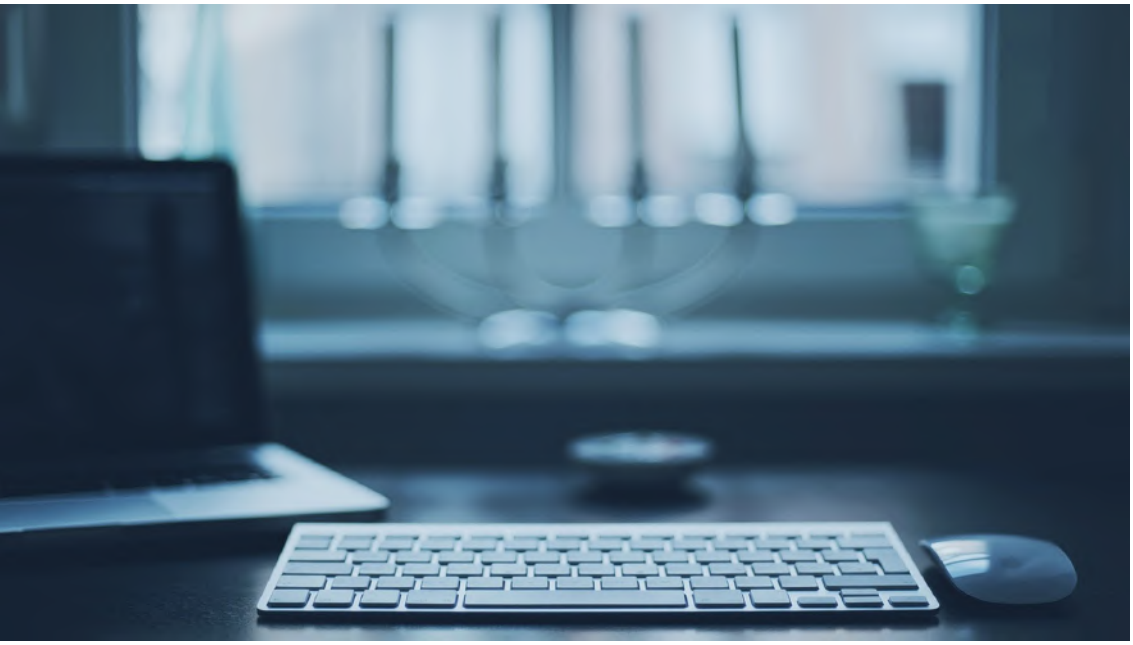
Este documento está dirigido a dos tipos de personas en una entidad financiera, a los oficiales de seguridad que son los responsables de los aspectos técnicos, infraestructura, y soluciones de aseguramiento en accesos remotos, y para los usuarios finales que laboran desde la casa quienes son los más vulnerables a sufrir un ataque externo por un adversario.

RECOMENDACIONES DE SEGURIDAD PARA USUARIO EN TELETRABAJO

El siguiente contenido de esta sección resalta las recomendaciones de seguridad enfocadas especialmente al usuario que labora desde casa, este contenido le dice al teletrabajador que medidas y pasos debe adoptar para prevenir y mejorar su seguridad en su dispositivo BYOD en un ambiente fuera de la empresa. En esta sección se expone las medidas contra el **Spearphishing**, **Drive-by Compromise** y **Replication Through Removable Media** que, de acuerdo al análisis de Threat Intelligence, son los mas utilizados por los adversarios para ingresar a sus dispositivos con propósitos maliciosos.

ACCESO INICIAL

"Any sufficiently advanced technology is indistinguishable from magic."
Arthur C. Clarke, Profiles of the Future: An Inquiry Into the Limits of the Possible



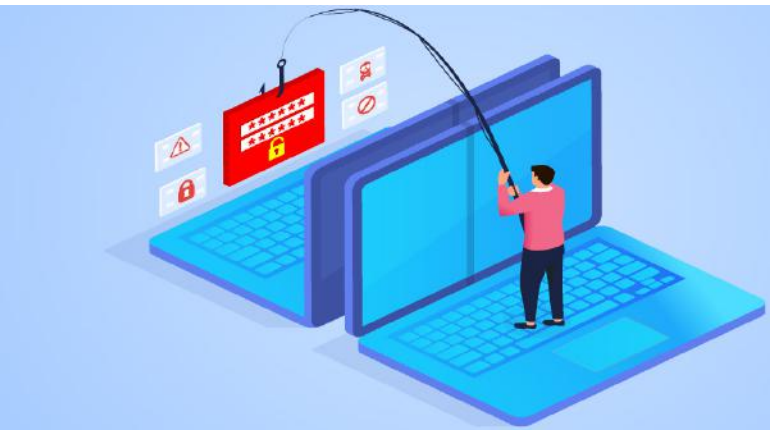
SPEARPHISHING

1. Indicadores que pueden ayudar a identificar con éxito un ataque

El Spearphishing es una estafa por correo electrónico dirigida a una persona, organización o empresa específica. aunque a menudo tienen la intención de robar datos con fines maliciosos, los ciberdelincuentes también pueden intentar instalar malware en la computadora de un usuario objetivo.

A continuación presentamos algunas recomendaciones de seguridad que un usuario de teletrabajo debe tener en cuenta para identificar y minimizar un ataque de Spearphishing.

- Verifiqué la dirección de correo electrónico real del remitente, está se puede revelar colocando el puntero del mouse sobre el nombre del remitente revelando la dirección real de donde proviene el correo.
- Verifique la autenticidad, la autenticidad de un correo electrónico se puede verificar leyendo detenidamente la dirección de correo electrónico y asegurándose de que sea legítima (es decir, **gmail.com** en lugar de **gmaill.com**).
- Identifique los enlaces ocultos, al pasar el cursor sobre imágenes o textos brevemente se mostrará el URL y a dónde conducen los enlaces.
- Sin trazabilidad de correos electrónicos. ¿El remitente se ha puesto en contacto antes? ¿El correo electrónico proviene de una dirección interna? ¿Hay algo fuera de lo común? Por lo general, los atacantes intentarán que el objetivo cometa una acción mediante un sentido de urgencia, es decir, para hacer clic en un enlace o para iniciar una transferencia financiera.



- Hacer una llamada telefónica, no dude en llamar al remitente para confirmar la legitimidad del correo electrónico y la información solicitada.
- Lea y verifique, lea el contenido del correo electrónico con atención. Si es de alguien con quien ha estado enviando correos electrónicos antes, vea si el estilo y el tono le son familiares. Si el correo electrónico tiene una firma, verifique que las firmas coincidan.
- Tenga en cuenta que ninguna institución financiera, ni un proveedor de servicios le pediría nunca a sus clientes que revelaran información personal por correo electrónico.

1. Spearphishing a law enforcement and cross-industry perspective, European Cybercrime centre, Europol EC3 2019

Otros tipos de phishing incluyen:

• Smishing ("SMS Phishing") implica que un usuario abre un SMS o mensaje de texto malicioso en un dispositivo móvil.
• Vishing involucra a un actor de amenazas cibernéticas que intenta recopilar información a través de teléfonos de Voz sobre IP (VoIP).
• Whaling es un intento de spearphishing dirigido a un alto ejecutivo u otro objetivo de alto perfil.

2. Prácticas de seguridad

2.1. Aplicación de parches y actualizaciones

- Instale un software de antivirus/antimalware que ponga en cuarentena automáticamente los archivos sospechosos y manténgalo actualizado.
- Actualice sus dispositivos conectados a internet, si su proveedor de software le notifica que hay una nueva actualización, hágalo de inmediato. La mayoría de los sistemas de software incluyen actualizaciones de software de seguridad que deberían ayudarlo a protegerse de ataques comunes. Siempre que sea posible, habilite las actualizaciones automáticas de software.
- Asegúrese de que este utilizando la última versión de la aplicación de cliente de correo.
- Si utiliza cliente de correo web, mantener el navegador actualizado.
- No ejecutar una versión segura de un cliente de correo puede reducir el resto de medidas de seguridad y comprometer el equipo a un ciberataque.

2.2. Configure las funciones de seguridad en el cliente de correo

- Desactive la descarga y el procesamiento de contenido activo. (Macros, Adobe Flash, Javaapplets y JavaScript.)
- Desactive la vista previa automática de mensajes.
- Desactive la apertura automática de mensajes.
- Desactive la carga automática de imágenes en mensajes.
- Habilite las funciones anti-spam y anti-phishing, si están disponibles. Estas características suelen tener una configuración predeterminada, por lo que puede ser beneficioso desde una perspectiva de seguridad establecerlos en un nivel superior

2. Guidelines on Electronic Mail Security, NIST Special Publication 800-45, Versión 2.

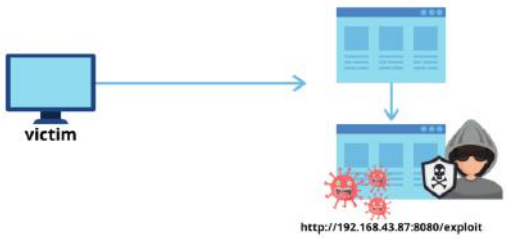
2.3. Otras recomendaciones

- No se apresure a enviar información solo porque la otra persona le dice que es urgente, confirme la urgencia de la información primero, realice una llamada
- No dude sólo porque el remitente parece saber mucho sobre usted, recuerde que estos atacantes realizan primero un seguimiento de su objetivo, recopilando la mayor información posible para que este genere confianza a la victima.
- No confíe en los detalles proporcionados por el remitente cuando los consulte.
- No siga las instrucciones sobre cómo ver un correo electrónico que aparece dentro del correo electrónico mismo.
- No abra correos electrónicos sospechosos ni haga clic en enlaces desconocidos. La forma más sencilla de comprobar un enlace es colocando el mouse sobre él. Esto permite que el verdadero destino del enlace aparezca en la esquina inferior izquierda de la ventana de su navegador o junto al puntero del mouse en Microsoft Outlook.
- No tenga miedo de obtener una segunda opinión, si no esta seguro de la procedencia del correo, pregunte.

DRIVE-BY COMPROMISE

1. Identifique sitios web falsos

Drive-by Compromise requiere la implementación de algunas estrategias y técnicas, generalmente el atacante identifica los tipos de sitios web que la víctima visita con frecuencia. Luego, el atacante inyecta un script malicioso que generalmente redirige a la página web maliciosa y el navegador de la víctima se conecta a la máquina del atacante.



Ataque de pozo de agua: Es un ataque basado en estrategias, en el que intentamos obtener acceso a una organización a través de empleados débiles.

3. Drive-by Compromise (t1189), Cyberwarfare labs.

Este tipo de ataque dirigido se conoce como un **compromiso web estratégico** o u**n ataque de pozo de agua.**

Los sitios web falsificados se ven casi idénticos a los legítimos. Dichos sitios web suelen presentar mensajes de alerta y enlaces maliciosos, los sitios web bancarios falsificados implementan ventanas emergente que le solicita que ingrese sus credenciales bancarias.

Principales recomendaciones para indentificar en sitio web falso:

- Preste mucha atención a la URL, Recuerde, el nombre de dominio real aparece justo antes del TLD (por ejemplo **.com/ .edu/**)
- Compruebe los indicadores de seguridad de la conexión, ingrese a URLs que implementen conexiones seguras HTTPS
- Busque sellos de confianza, los sellos de confianza se colocan comúnmente en las páginas de inicio, las páginas de inicio de sesión y las páginas de pago. Son inmediatamente reconocibles y recuerdan a los visitantes que están seguros en esta página.
- Identifique si el sitio web presenta mensajes de alerta, estos sueles ser utilizados con el fin de que el usuario de clic e infectar el equipo.

- Tenga en cuenta que los sitios web bancarios no habilitan ventanas emergentes, estas se utilizan comúnmente para recopilar información confidencial suya. No haga clic en ellos y evite enviar datos personales en dichas ventanas.
- Identifique el diseño del sitio web, tenga cuidado con los sitios web que tienen fallas en su diseño o errores de ortografía y gramática,

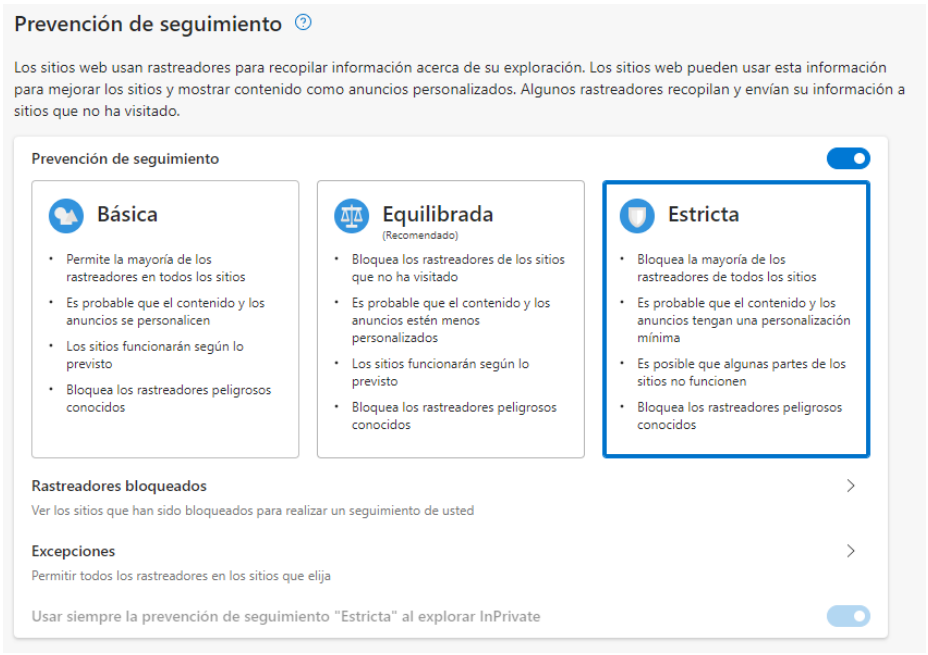
1. Spearphishing a law enforcement and cross-industry perspective, European Cybercrime centre, Europol EC3 2019

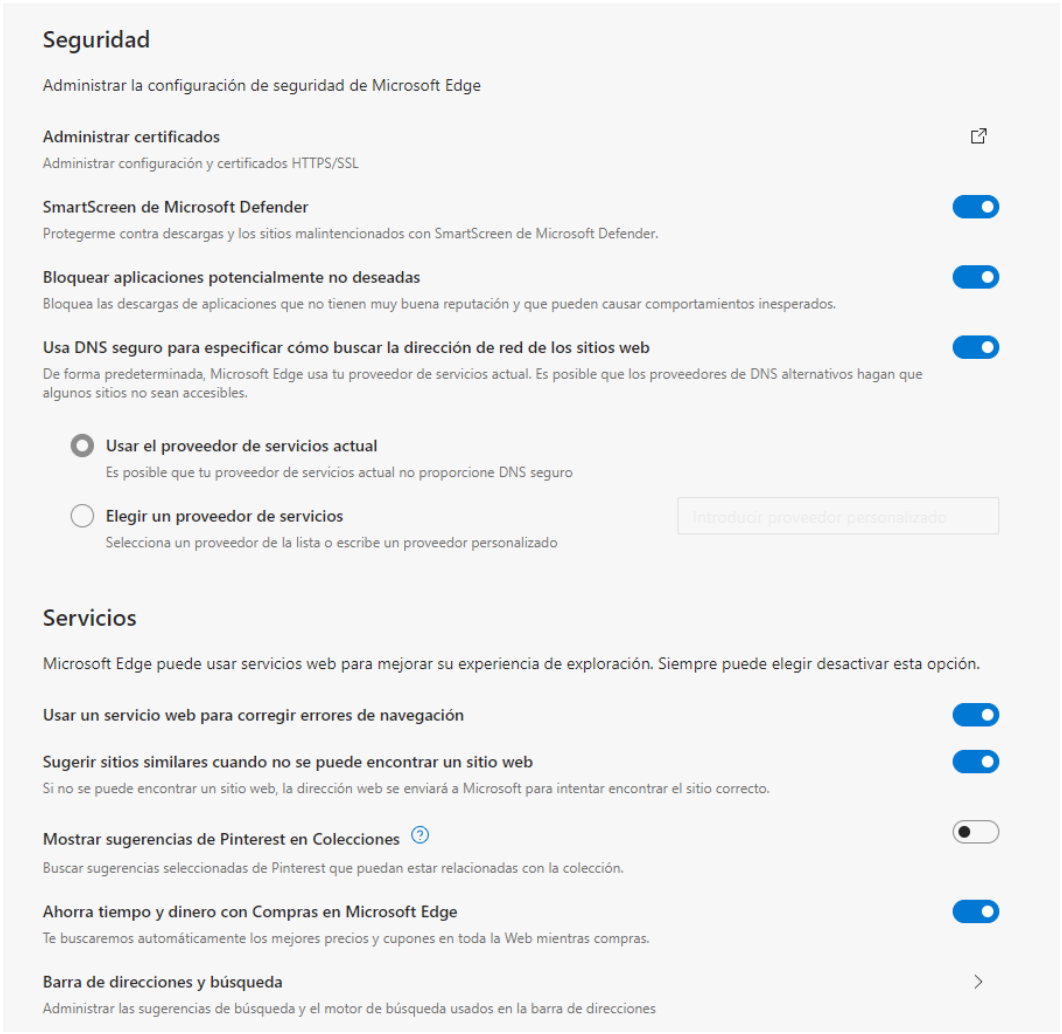
2. Seguridad en navegadores

Para ayudarle a proteger el navegador. a continuación le presentaremos algunas de las características más importantes de configuración segura que puede aplicar.

2.1. Microsoft Edge

Puede acceder a la configuración de privacidad de Microsoft Edge abriendo el navegador, haciendo clic en los puntos suspensivos (...) y luego viendo la configuración "Avanzada". Una vez allí, desplácese hacia abajo para encontrar la configuración de "Privacidad y servicios".

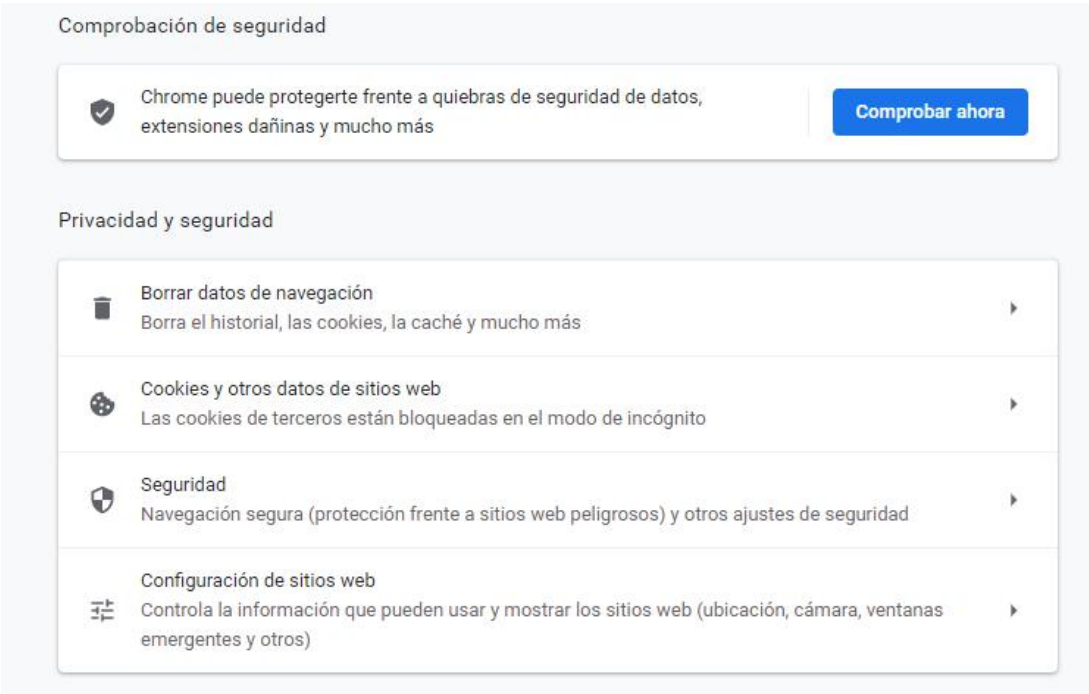


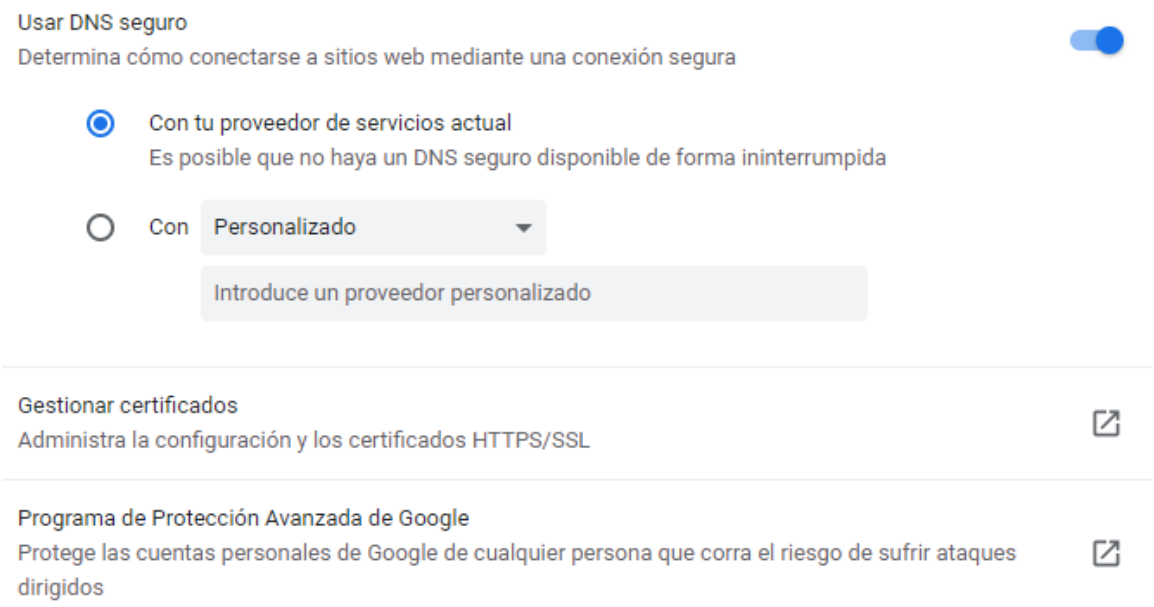


4. Top 12 Tips For Safer Browsing On The Internet, Cybercrime Magazine.

2.2. Google Chrome

Para Chrome, abra el navegador, haga clic en los puntos suspensivos verticales en la esquina superior derecha y luego vaya a la configuración. Desplácese hacia abajo hasta encontrar la configuración "Avanzada" en la parte inferior. Haga clic en él y encontrará la configuración de "Privacidad y seguridad" de Chrome. Puede acceder a la configuración de privacidad de Microsoft Edge abriendo el navegador, haciendo clic en los puntos suspensivos (...) y luego viendo la configuración "Avanzada". Una vez allí, desplácese hacia abajo para encontrar la configuración de "Privacidad y seguridad".





Navegación segura

Protección mejorada
Protección más rápida y proactiva frente a descargas, extensiones y sitios web peligrosos. Te advierte sobre robos de contraseñas. Necesita enviar datos de navegación a Google.

- Predice y te advierte de eventos peligrosos antes de que se produzcan
- Te protege en Chrome y puede usarse para mejorar tu seguridad en otras aplicaciones de Google cuando has iniciado sesión
- Mejora tu seguridad y la de todos los usuarios en la Web
- Te avisa si tus contraseñas se ven expuestas en una quiebra de seguridad de datos
- Envía URL a Navegación segura para que las compruebe. También envía una muestra pequeña de páginas, descargas, actividad de las extensiones e información del sistema para contribuir a detectar nuevas amenazas. Cuando inicias sesión, vincula estos datos a tu cuenta de Google de forma temporal para protegerte en las aplicaciones de Google.

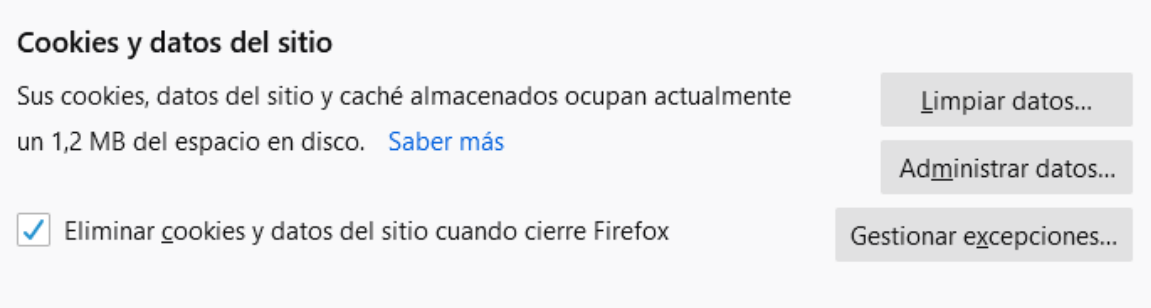
Protección estándar
Protección estándar frente a descargas, extensiones y sitios web que son peligrosos.

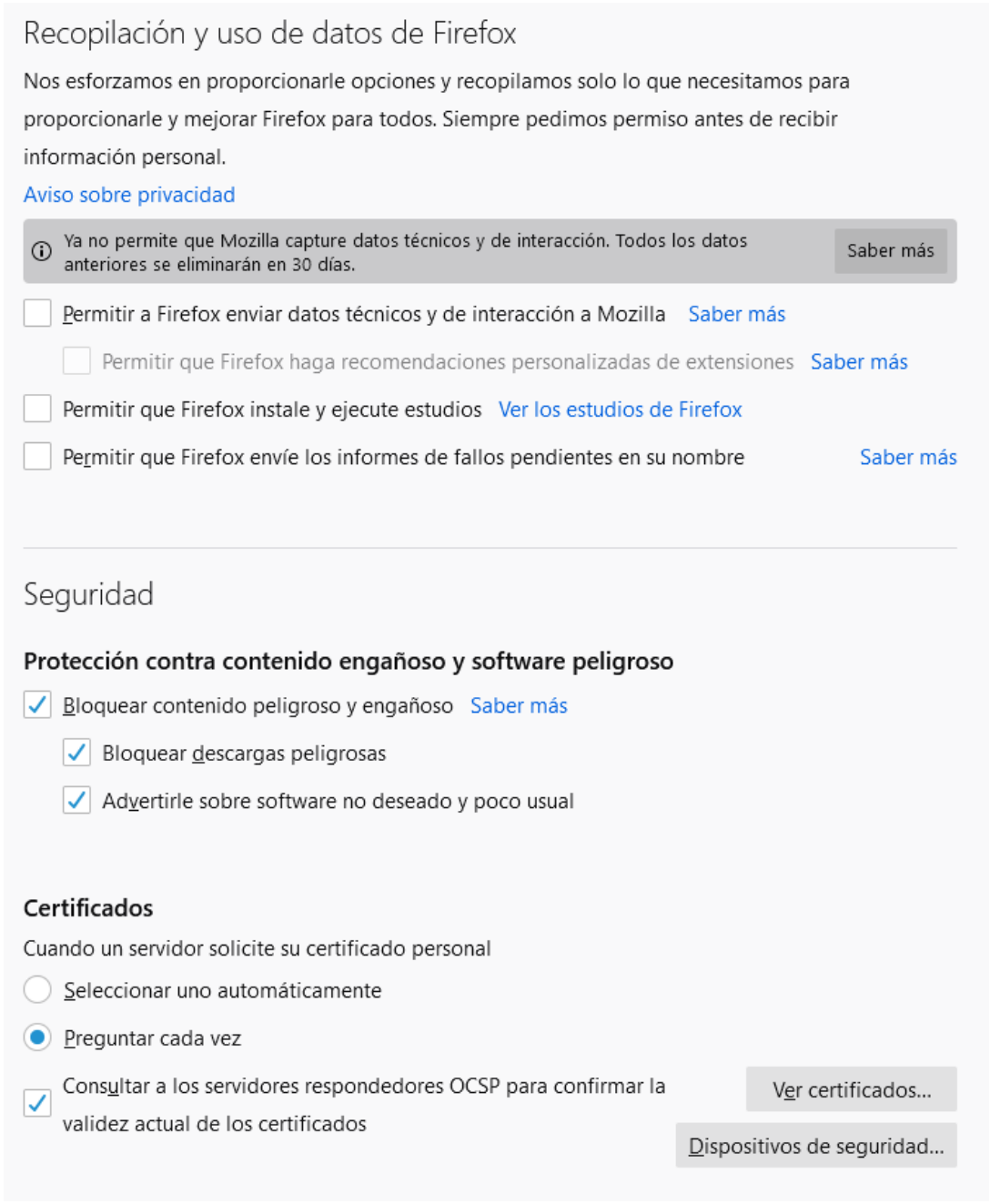
Sin protección (no recomendado)
No te protege frente a descargas, extensiones ni sitios web peligrosos. Seguirás disfrutando de protección con la función Navegación segura, si está disponible, en otros servicios de Google, como Gmail y la Búsqueda.

4. Top 12 Tips For Safer Browsing On The Internet, Cybercrime Magazine.

2.3. Mozilla Firefox

Para Firefox, abra el navegador y luego haga clic en el botón de menú en la esquina superior derecha. Luego haga clic en Opciones. Debería encontrarse en el menú de opciones ahora, así que desplácese hacia abajo y busque "Privacidad & Seguridad".





4. Top 12 Tips For Safer Browsing On The Internet, Cybercrime Magazine.

3. Recomendaciones

Verifique la procedencia del sitio Web

Siempre vale la pena investigar un poco sobre una empresa para comprobar si tiene buena reputación y si es quien dice ser. Existe una buena posibilidad de que si un sitio ha defraudado a personas en el pasado, las víctimas se conecten a Internet para compartir su experiencia y advertir a otros usuarios que eviten el sitio. Si hay muchas opiniones negativas de los clientes, es una buena indicación de que debe mantenerse alejado del sitio en cuestión.

Compruebe quién es el propietario del sitio web

Todos los dominios deberán registrar su dirección web, por lo que vale la pena hacer una búsqueda de WHOIS para ver quién es el propietario del sitio web. Este es un servicio gratuito y le permitirá verificar quién es el propietario del sitio web cuando se creó y proporcionará los datos de contacto del propietario del sitio.

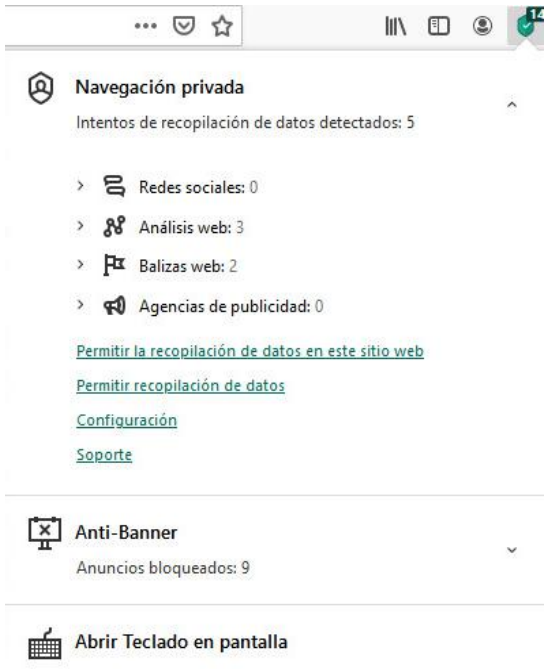
Utilice Métodos de pago confiables

Los sitios web legítimos siempre aceptarán tarjetas de crédito como método de pago o pueden utilizar un portal como PayPal para transacciones en línea. Si la única opción de pago proporcionada en un sitio web es a través de una transferencia bancaria, entonces deberían sonar las alarmas. Los sitios de buena reputación nunca pedirán a los consumidores que paguen con este método. Esto indica que ningún banco ha proporcionado servicios de tarjeta de crédito para el sitio web y lo más probable es que se trate de un estafador.

Evalué el contenido dentro de un sitio

Los errores de ortografía simples, el inglés roto, los errores gramaticales o las imágenes de baja resolución deben actuar como una señal de alerta de que estás en un sitio de phishing y debes irte de inmediato.

- Evite los sitios web cuestionables.
- Aumente la configuración de seguridad de su navegador.
- Solo descargue software de sitios en los que confíe. Evalúe cuidadosamente el software gratuito y las aplicaciones para compartir archivos antes de descargarlos. Actualice su sistema operativo con regularidad.
- Escriba una URL confiable para el sitio de una empresa en la barra de direcciones de su navegador para evitar los enlaces en un correo electrónico o mensaje instantáneo.
- Nunca haga clic en enlaces publicitarios.
- Utilice un navegador que le permita bloquear las ventanas emergentes.
- Si algo importante realmente necesita su atención, su banco lo alertará cuando acceda a su cuenta en línea.
- Permita que el antivirus se integre al navegador para que gestione su seguridad.



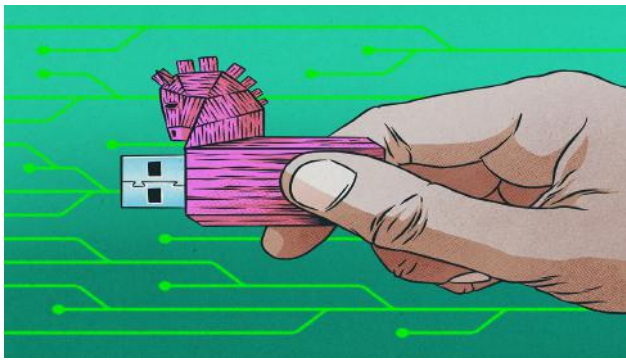
REPLICATION THROUGH REMOVABLE MEDIA

1. Prácticas de seguridad

1.1. Mitigue el riesgo de infección.

Mitigación	Descripción
Antivirus/ Antimalware	Instale soluciones antivirus en su equipo que escanee activamente en busca de malware cuando se conecte cualquier tipo de medio o dispositivo extraíble.
Deshabilitar funciones automáticas	Desactive la Ejecución automática y Reproducción automática de los medios extraíbles. **1.2.**
Actualizaciones y parches	Habilite las actualizaciones automáticas, mantenga actualizado las bases de datos de virus así como el sistema operativo de su equipo. La mayoría de los sistemas de software incluyen actualizaciones de software de seguridad que deberían ayudarlo a protegerse de ataques comunes. Siempre que sea posible, habilite las actualizaciones automáticas de software.
Cifre sus dispositivos extraíbles	Busque la oportunidad de cifrar sus dispositivos o información almacenada. **1.3.**

Los atacantes pueden propagar su programa malicioso infectando los medios extraíbles (unidad USB). Un atacante puede tomar ventaja de Autorun (explotar la vulnerabilidad en la ejecución automática) para infectar otros sistemas de forma automática, cuando los medios infectados está conectado a la misma.



Esta técnica generalmente implica copiar archivos o modificar los archivos existentes almacenados en los medios extraíbles. Una vez que el malware copia el archivo malicioso en un medio extraíble, puede usar varios trucos para hacer que ese archivo parezca un archivo legítimo y engañar al usuario para que lo ejecute cuando el USB esté conectado a un sistema diferente.

5. Risk Management for Replication Devices, NISTIR 8023.

1.2. Deshabilitar ejecución automática

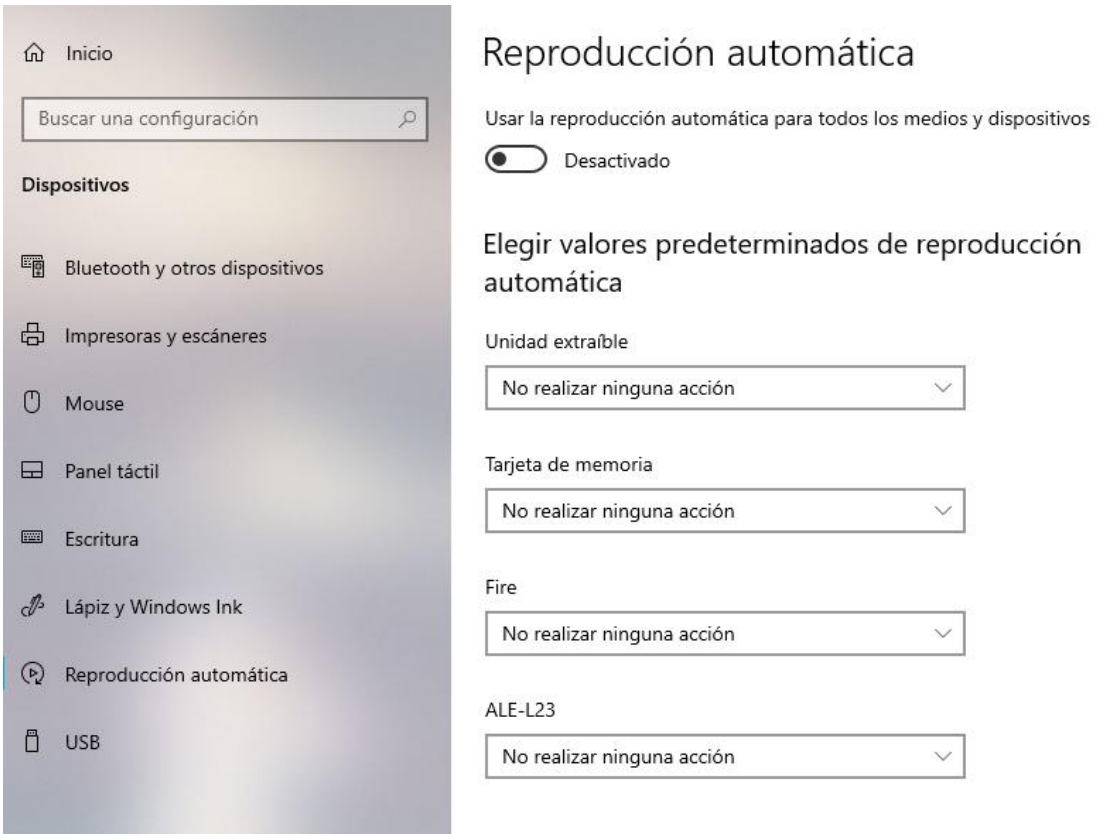
La función de ejecución automática hace que los medios extraíbles, como CD, DVD y unidades USB, se abran automáticamente cuando se insertan en una unidad. Al deshabilitar la ejecución automática, puede evitar que el código malicioso de una unidad USB infectada se abra automáticamente.

A continuación resaltamos la información sobre cómo habilitar, deshabilitar y configurar la reproducción automática en Windows 10.

1. Abra el menú Inicio. Haga clic en Configuración y luego en Dispositivos.

2. Haga clic en Reproducción automática en la parte inferior izquierda de la pantalla. A continuación, active o desactive la opción Usar reproducción automática para todos los medios y dispositivos.

3. En Elegir valores predeterminados de reproducción automática, configure la acción predeterminada para la reproducción automática al conectar cada tipo de medio o dispositivo.



1.3. Cifrado de dispositivos

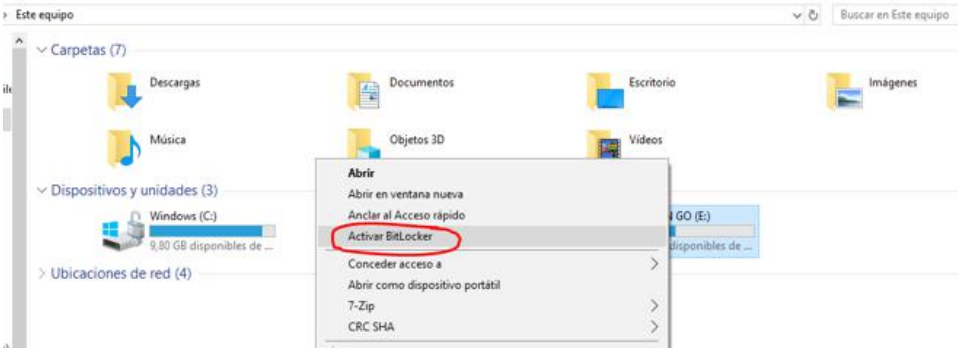
Cifrar una unidad extraíble, como una memoria USB, no lleva mucho tiempo. Una vez que finaliza el proceso de cifrado, cada vez que conecta su dispositivo a una computadora con Windows, el Explorador de archivos muestra el dispositivo con un icono de candado, que indica que el dispositivo está cifrado. Para acceder a su contenido, debe ingresar la contraseña establecida durante el proceso de cifrado.

En sistemas operativos Windows (ediciones Education, Pro y Enterprise) disponemos de la herramienta "BitLocker". Se trata de una herramienta desarrollada por Microsoft que suele venir preinstalada en casi todas las versiones de su sistema operativo.

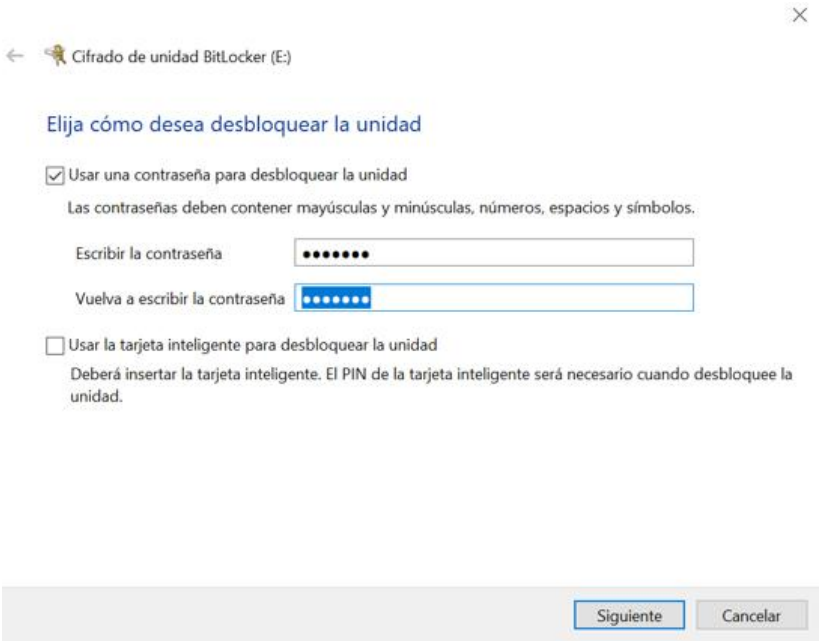
A continuación resaltamos la información sobre cómo utilizar la herramienta de BitLocker de Windows para cifrar sus unidades y dispositivos.

Paso 1. Abra el explorador de archivos. Haga clic en Este equipo.

Paso 2. Haga clic derecho sobre el dispositivo y/o unidad que desea proteger y elija la opción Activar BitLocker para iniciar el proceso.

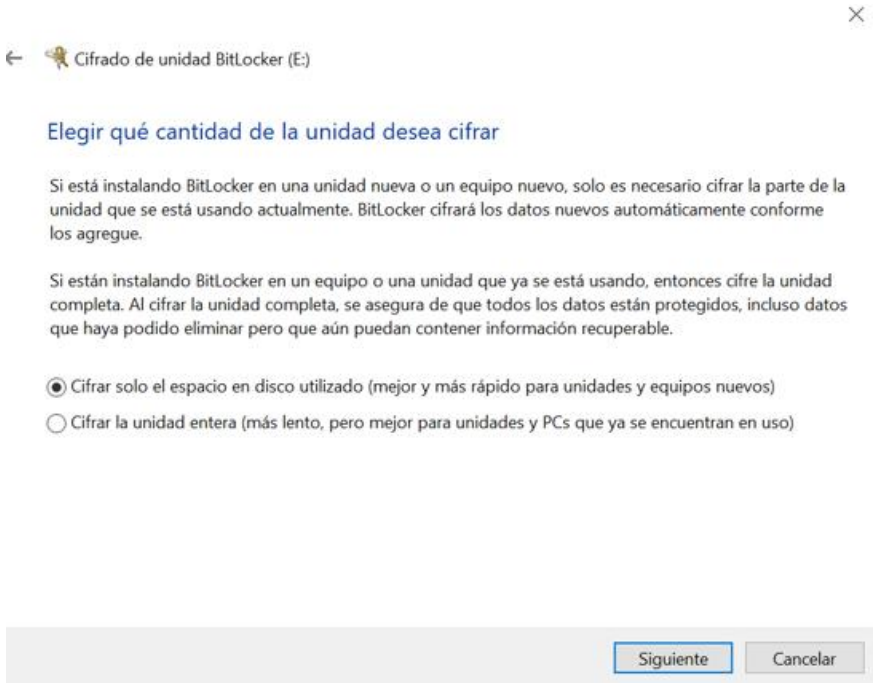


Paso 3. Haga clic en la opción "Usar una contraseña para desbloquear la unidad", y a continuación, escribir la contraseña que utilizarás para el cifrado.

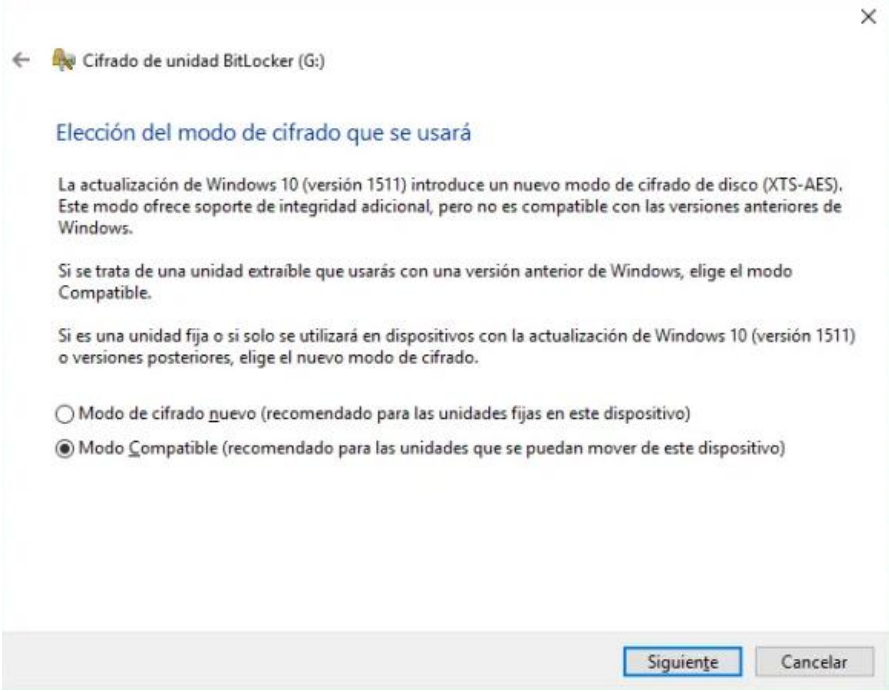


Paso 4. Luego de que Windows generar una clave de recuperación para el supuesto caso tiene la opción de elegir entre dos opciones de cifrado. Uno rápido que cifra solo el espacio utilizado y otro más lento que cifra por completo la memoria USB. La diferencia es que la segunda opción cifrará también los datos que pueda haber borrado, pero que aún podrían ser recuperados.

Elija la opción que prefiera y pulse "Siguiente".



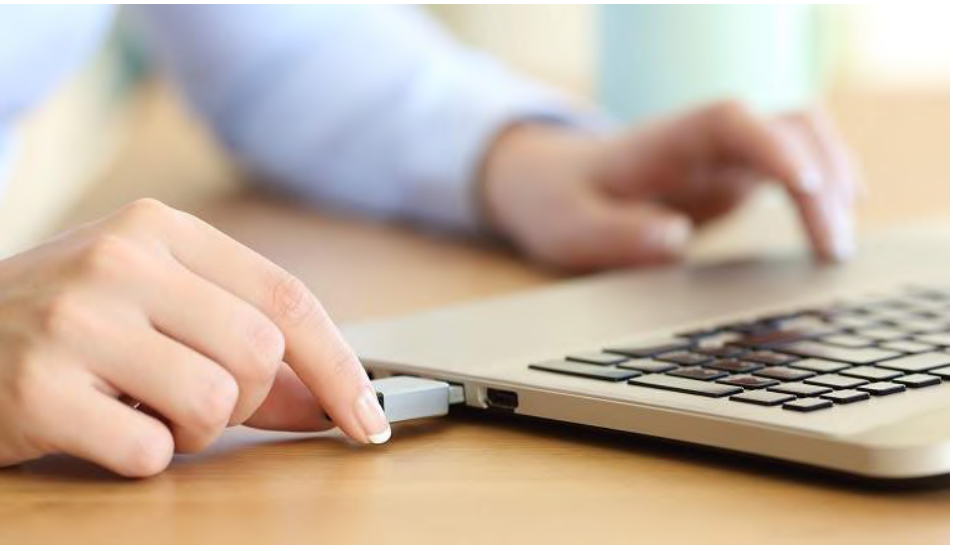
Paso 5. Haga clic en la opción "Modo Compatible" y siguiente, a continuación pulse sobre el botón "Iniciar Cifrado" para comenzar el proceso de cifrado de la unidad.



2. Recomendaciones

- Limite el uso de todos los dispositivos de medios extraíbles excepto cuando estén específicamente autorizados.
- Aplicar protección con contraseña. Para salvaguardar la información confidencial y restringir el acceso, todos los medios extraíbles deben protegerse con contraseñas seguras.
- Cifre la información almacenada en medios extraíbles. Si se requiere el uso de medios extraíbles, la información de todos los dispositivos debe estar cifrada. El nivel de cifrado dependerá de la sensibilidad de la información almacenada en el dispositivo.
- Nunca copie archivos en medios extraíbles a menos que sea necesario o haya sido autorizado.
- Escanee todos los medios en busca de malware. Los medios extraíbles deben analizarse minuciosamente en busca de malware antes de que se utilicen o se reciban de cualquier otra organización.
- Nunca deje medios extraíbles por ahí. Ciérrelo de forma segura cuando no esté en uso.
- Desactive Bluetooth, Wi-Fi y otros servicios cuando no los esté usando.
- Nunca intente acceder a archivos desde cualquier medio extraíble que pueda haber encontrado. Puede contener un virus que infecte los sistemas informáticos con malware.
- Cuando utilice Bluetooth, configúrelo en el modo "no detectable" para ocultar el dispositivo de los dispositivos no autenticados.
- Informe los dispositivos faltantes de inmediato, para que se puedan borrar todos los datos.
- Realice y mantenga copias de seguridad de los medios y de sus archivos con frecuencia.
- Utilice Office365 OneDrive u otro servicio de copia de seguridad en la nube para almacenar y acceder a los datos de forma segura. Esto también protege contra la posible pérdida de datos cuando se pierde un dispositivo extraíble.

6. Using Caution with USB Drives, Cybersecurity & Infrastructure Security Agency.



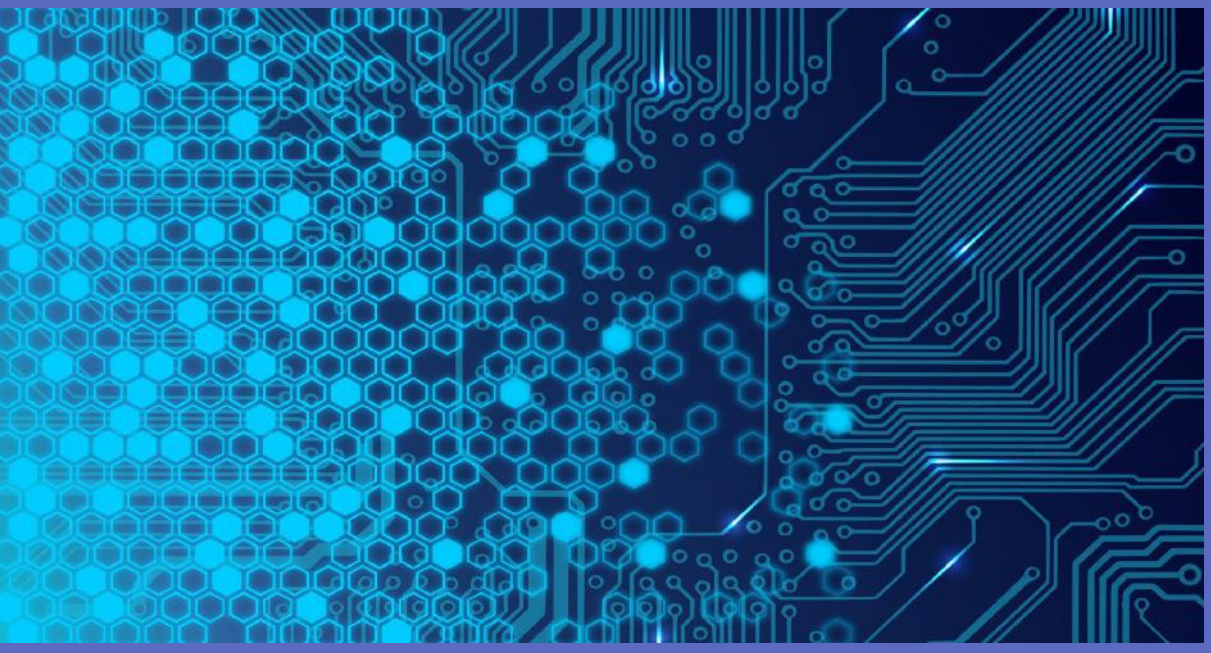
RECOMENDACIONES ADICIONALES PARA EL TELETRABADOR

- Cambie la clave constantemente del acceso al wifi de su hogar, y evite conectarse a redes inalámbricas vecinas que estén abiertas, te pueden robar información sensible de la empresa o persona.
- Si en su dispositivo BYOD contiene información sensible he importante del trabajo, realice copias de seguridad de manera periódica haciendo uso de medios de almacenamientos externos entregados por la misma organización o empresa para evitar robo o alteración de la información.
- Evite enviar información sensible o confidencial de la organización y/o empresa por medios que no son autorizados como otros correos de dominios gratuitos, redes sociales, servidores de almacenamientos en la nube, etc.
- Es importante que cada vez que no utilice su dispositivo BYOD en el hogar o en lugares públicos, cierre siempre la sesión.
- No instale programas de fuentes desconocidas o extensiones de los navegadores, ya que los malware se camuflan por estos softwares descargables causando daños en su dispositivo o robando información sensible.
- Conozca las políticas de teletrabajo de su organización. Esto incluye cuándo y dónde es aceptable trabajar fuera de la oficina, así como las medidas de seguridad o las mejores prácticas.
- Creé contraseñas seguras. Asegúrese de que incluyan una combinación de letras mayúsculas y minúsculas, números y símbolos. Hágalos lo suficientemente difíciles como para que nadie pueda adivinarlos.
- No comparta contraseñas en línea. Si debe compartir la información de inicio de sesión con un compañero de trabajo, llámelo con los detalles en lugar de enviarlo por correo electrónico, mensaje de texto o mensaje instantáneo.
- Utilice la autenticación de dos factores. Aunque puede ser un inconveniente, la autenticación de dos factores, si está disponible, proporciona una capa adicional de seguridad para evitar que los piratas informáticos accedan a las cuentas.

RECOMENDACIONES DE SEGURIDAD PARA EL ÁREA DE TECNOLOGÍA

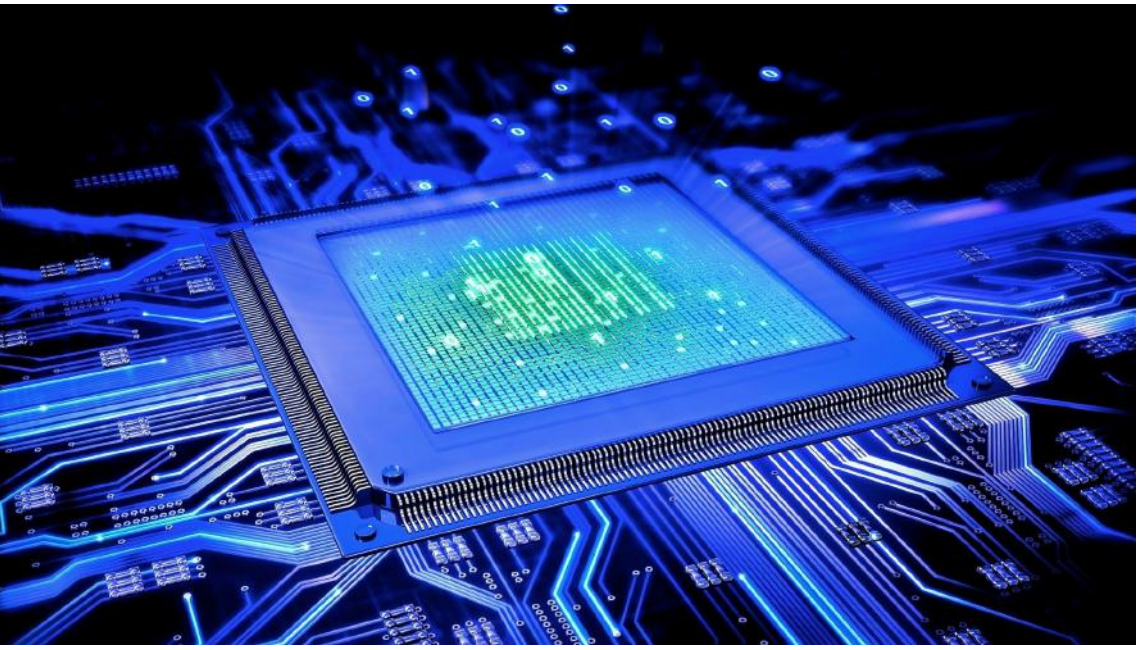
En la siguiente sección del contenido, se resaltarán las recomendaciones de seguridad para las técnicas más utilizadas de la Threat Intelligence después de haber un compromiso en el acceso inicial del teletrabajador.

Tenga en cuenta que en el siguiente contenido, se presentan algunas de muchas recomendaciones que se pueden aplicar para las técnicas descritas en la táctica de **Ejecución**, y que el oficial de seguridad de la organización será el principal responsable de los aspectos técnicos de la preparación, organización y aseguramiento de las demás tácticas descritas en la Threat Intelligence.



EJECUCIÓN

"If we continue to develop our technology without wisdom or prudence, our servant may prove to be our executioner". O*mar Bradley*



COMMAND AND SCRIPTING INTERPRETER

1. Prácticas de seguridad

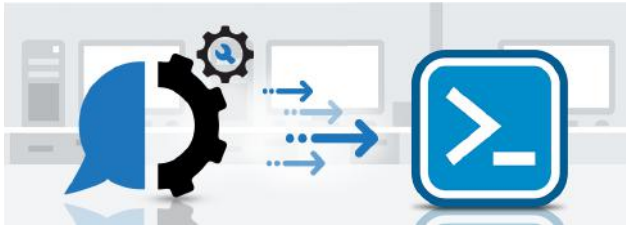
1.1. Mitigue la ejecución de comandos

Mitigación	Descripción
Antivirus/ Antimalware	Instale soluciones antivirus en todos los equipos corporativos, y programe escaneos diariamente en busca de malware. Mantenga la base de virus actualizada.
Firma de código	Solo permita la ejecución de scripts firmados. 2.3.
Deshabilitar o quitar función o programa	Deshabilite o elimine cualquier intérprete o shells innecesarios o no utilizados.
Gestión de cuentas privilegiadas	Restrinja la política de ejecución de PowerShell a los administradores.
Restringir el contenido basado en la web	Instale extensiones de bloqueo de scripts, estas pueden ayudar a prevenir la ejecución de scripts y archivos HTA que pueden usarse comúnmente durante el proceso de explotación. Instale bloqueadores de anuncios en los equipos del usuario.

7. Command and Scripting Interpreter, Mitre att&ck.

1.2. Detección

Las actividades de la línea de comandos y de secuencias de comandos se pueden capturar mediante el registro adecuado de la ejecución del proceso con argumentos de la línea de comandos. Esta información puede ser útil para obtener información adicional sobre las acciones de los adversarios a través de cómo utilizan procesos nativos o herramientas personalizadas.



- Supervise los procesos y los argumentos de la línea de comandos para la ejecución del script y el comportamiento posterior.
- Supervise la carga de módulos asociados con idiomas específicos.
- Restringa la secuencia de comandos para usuarios normales.

2. Protección de los activos de información contra ataques de PowerShell

2.1. Actualice a Microsoft PowerShell v7.0.3 o superior

PowerShell v7.0.3 ofrece mejores capacidades de registro e incorpora funciones de seguridad mejoradas para administrar ciberataques. Ejemplos incluyen:

Interfaz de exploración antimalware (AMSI)
Registro de bloques de scripts
Transcripción

2.2. Use el modo de lenguaje restringido

Una forma de defenderse de los ataques de PowerShell es limitar los diferentes tipos de comandos ejecutados con sesiones de PowerShell.

El uso y la aplicación del modo de lenguaje restringido (CLM) ayuda a evitar que los actores malintencionados ejecuten scripts fabricados como Invoke-Mimikatz.

2.3. Detección por regla sigma

La siguiente regla Sigma se puede utilizar para detectar la recopilación de información del sistema mediante el cmdlet Get-WmiObject de PowerShell:

```
título: SystemInformationDiscoveryviaPowerShellCmdlet
estado: experimental
descripción: DetectstheattempttogathersysteminformationusingGet-
WmiObjectcmdletofPowerShell.Thistechniqueiscommonlyutilizedfordiscovery.
autor: PicusSecurity
referencias:
- https: //attack.mitre.org/techniques/T1047/
- https: //attack.mitre.org/techniques/T1086/
- https: //attack.mitre.org/techniques/T1082/
- https: //attack.mitre.org/tactics/TA0002/
- https: //attack.mitre.org/tactics/TA0007/
fuente de registro:
    producto: windows
    servicio: security
    definición1: 'Requirements: Group Policy : Computer Configuration\Windows Settings\Security
Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process
Creation'
   definición2: 'Requirements: Group Policy : Computer Configuration\ Administrative Templates\
System\ Audit Process Creation\ Include Command Line'
detección:
   selección:
      EventID: 4688
      NewProcessName: '*\powershell.exe'
      ProcessCommandLine: '*wmi* *Win32_ComputerSystem*'
   condición: falsos selection
positivos:
   - Legitimate administrative activities
nivel: medium
etiquetas:
   - attack.execution
   - attack.discovery
   - attack.t1047
   - attack.t1086
   - attack.t1082
   - attack.ta0002
   - attack.ta0007
```

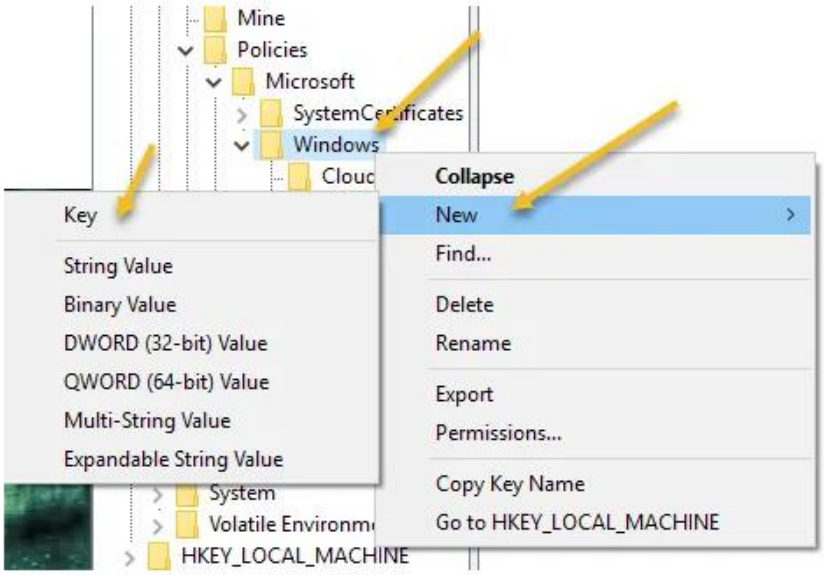
8. Mitre att&ck T1059 Command Line Interface, Picus Security Company.

3. Deshabilitar Windows Command Shell a través del registro

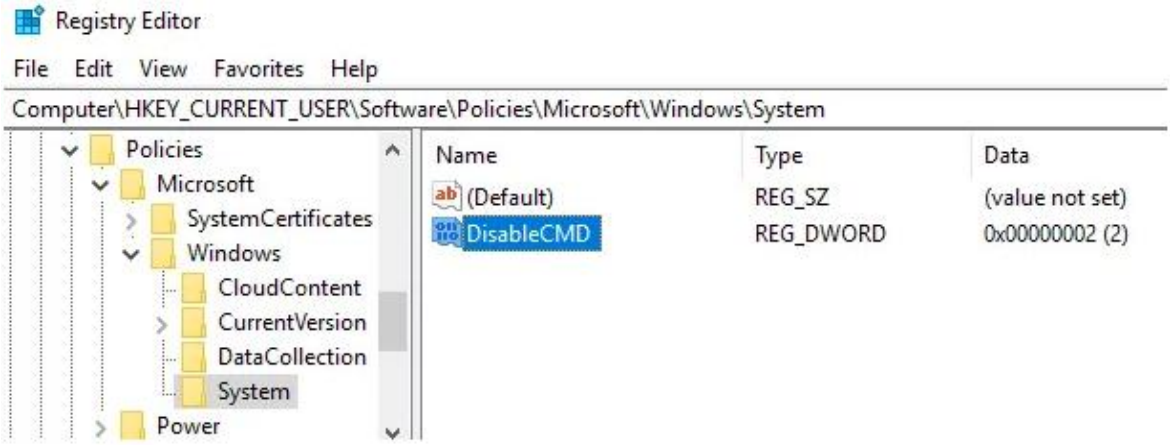
Abra el editor de registro haciendo clic en Inicio y escribiendo regedit . Navegue a la siguiente ruta:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows

Cree una nueva clave para Sistema, selecciónelo y luego haga clic con el botón derecho en el panel de la derecha y elija Nuevo - Valor DWORD (32 bits).



Asigné el nombre al valor Ej: DisableCMD. El valor de 0 habilitará el símbolo del sistema y un valor de 1 deshabilitará el símbolo del sistema y evitará que se ejecuten los scripts.



4. Regla sigma Visual Basic

La siguiente regla Sigma se puede utilizar para detectar archivos DLL de WMI cargados a través de macros VBA en archivos de Word, Excel, PowerPoint y Outlook:

```
title: Windows Mangement Instrumentation DLL Loaded Via Microsoft Word
id: a457f232-7df9-491d-898f-b5aabd2cbe2f
status: experimental
description: Detects DLL's Loaded Via Word Containing VBA Macros
Executing WMI Commands
author: Michael R. (@nahamike01)
date: 2019/12/26
tags:
    - attack.execution
    - attack.t1047

    - attack.t1059.005
logsource:
    category: image_load
    product: windows
detection:
    selection:
        Image:
            - '*\winword.exe'
            - '*\powerpnt.exe'
            - '*\excel.exe'
            - '*\outlook.exe'
        ImageLoaded:
            - '*\wmiutils.dll'
            - '*\wbemcomn.dll'
            - '*\wbemprox.dll'
            - '*\wbemdisp.dll'
            - '*\wbemsvc.dll'
    condition: selection
falsepositives:
    - Possible. Requires further testing.
level: high
```

9. Mitre att&ck T1064 Scripting, Picus Security Company.

5. Uso de firmas digitales para proteger

5.1. Crear una plantilla de certificado

Primero, vaya al **Panel de control** y luego a **Herramientas administrativas** > **Autoridad de certificación**. Haga clic con el botón derecho en **Plantillas de certificado** y haga clic en **Administrar**. Debería ver una lista de plantillas integradas disponibles para su uso. Haga clic derecho en **Firma de código** y seleccione **Plantilla duplicada**.

Configure las propiedades de la nueva plantilla. En la pestaña **General**, podrá establecer el nombre de la plantilla. En la pestaña **Compatibilidad**, podrá configurar la Autoridad de certificación y el Destinatario del certificado. En la pestaña **Criptografía**, puede configurar los detalles del algoritmo criptográfico utilizado, como Proveedor criptográfico, Nombre del algoritmo, Tamaño de clave y más.

Y en la pestaña **Seguridad**, puede configurar qué usuarios o grupos pueden crear certificados de firma de código. Los usuarios que pueden crear certificados de firma de código deben obtener permisos de **Inscripción** y **Lectura**.

Si ya tiene una plantilla de certificado configurada, simplemente puede importarla para usarla.

```
ldifde -i -k -f TEMPLATE_FILE
```

De vuelta en **Herramientas administrativas** > **Autoridad de certificación**, haga clic derecho en **Plantillas de certificad**o y luego vaya a **Nuevo** > **Plantilla de certificado para emitir.**

5.2. Crear un certificado de firma

En una máquina de desarrollo, ahora puede crear un certificado de firma de código. Primero, abra Microsoft Management Console (mmc.msc). Luego, vaya a **Archivo** > **Agregar o quitar complemento**. En el menú **Complementos disponibles**, seleccione **Certificados** y haga clic en **Agregar**, luego **Aceptar.**

En la ventana original, haga clic derecho en **Personal**, seleccione **Todas las tareas** > **Solicitar nuevo certificado,** Marque el certificado correspondiente y haga clic en **Inscribirse**. Se creará un certificado de firma de código.

Puede importar un certificado para usar ejecutando este comando.

```
Import-Certificate -FilePath "CERT_TO_IMPORT" -CertStoreLocation cert:CERT_LOCATION
```

También puede exportar un certificado de un almacén de certificados a un archivo.

```
$cert = Get-ChildItem -Path cert:CERT_LOCATION
Export-Certificate -Cert $cert -FilePath FILE_PATH
```

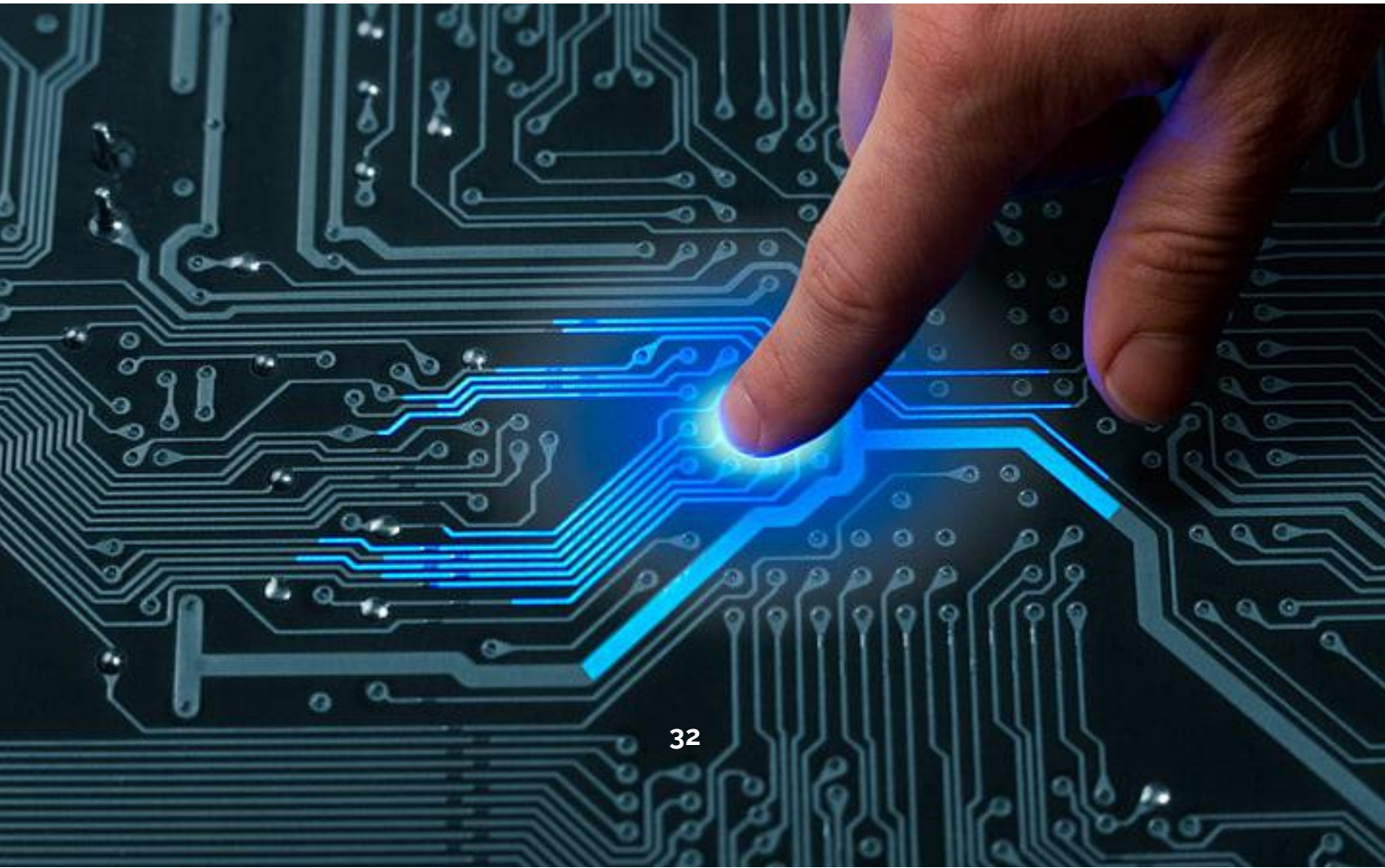
5.3. Firma de Scripts

Ahora puede firmar un script con el certificado de firma de código! Estos comandos recuperarán un certificado de firma de código y lo usarán para firmar los scripts.

```
$cert=Get-ChildItem -Path Cert:CERT_LOCATION -CodeSigningCert
Set-AuthenticodeSignature -FilePath SCRIPT_PATH -Certificate $cert
```

Ahora puede ejecutar su script firmado.

```
SCRIPT_PATH
```



SCHEDULED TASK/JOB

1. Prácticas de seguridad

1.1. Mitigue la ejecución de Programación de tareas

Mitigación	Descripción
Kit de Herramienta PowerSploit	Implemente un kit de herramientas como PowerSploit que se pueden usar para explorar sistemas en busca de debilidades de permisos en tareas programadas que podrían usarse para escalar privilegios.
Configuración del sistema operativo	Configure las opciones de las tareas programadas para forzar la ejecución de las tareas en el contexto de la cuenta autenticada en lugar de permitir que se ejecuten como SISTEMA. **2.1**
Gestión de cuentas privilegiadas	Configure la opción Aumentar la prioridad de programación para permitir solo al grupo de administradores los derechos para programar un proceso de prioridad. **2.2**
Gestión de cuentas de usuario	Limite los privilegios de las cuentas de usuario y corrija los vectores de escalamiento de privilegios para que solo los administradores autorizados puedan crear tareas programadas en sistemas remotos.

10. Scheduled Task/Job, Mitre att&ck.

1.2. Detección

Supervise la creación de tareas programadas desde utilidades comunes mediante la invocación de la línea de comandos. Se pueden crear tareas legítimas programadas durante la instalación de nuevo software o mediante funciones de administración del sistema. Busque cambios en las tareas que no se correlacionen con software conocido, ciclos de parche, etc.

La ejecución de programas sospechosos a través de tareas programadas puede aparecer como procesos atípicos que no se han visto antes cuando se comparan con datos históricos. Los datos y los eventos no deben verse de forma aislada, sino como parte de una cadena de comportamiento que podría conducir a otras actividades, como las conexiones de red realizadas para el mando y control, el aprendizaje de detalles sobre el entorno a través del descubrimiento y el movimiento lateral.

2. Configure las opciones de seguridad de las tareas programadas

2.1. Controlador de Dominio

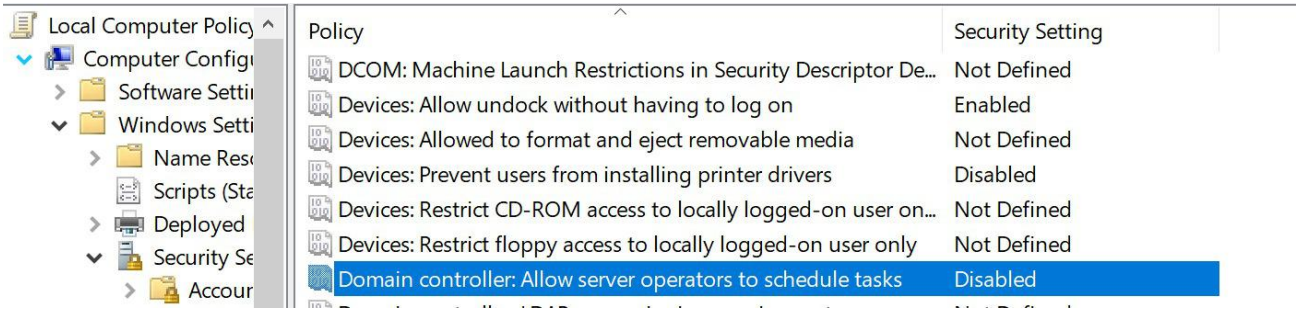
La configuración "Controlador de dominio: permite que los operadores del servidor programen tareas" determina si las tareas programadas deben ejecutarse en el contexto de la cuenta autenticada en lugar de permitir que se ejecuten como SISTEMA. La desactivación de esta configuración afecta solo la capacidad de programar trabajos usando el comando AT y no afecta las tareas configuradas usando el Programador de tareas.

Entonces, si aún no lo ha hecho, se recomienda configurar el siguiente valor usando el registro. Establezca el siguiente valor de registro en 0:

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl
```

Si la clave SubmitControl no estaba creada en el equipo, se recomienda agregarla. Para hacerlo, vaya al subárbol del registro: **HKEY_LOCAL_MACHINE** luego a la ruta del registro: **\System\CurrentControlSet\Control\LSA**. Agregue el nombre del valor **SubmitControl** como un valor **REG_DWORD** de 0.

Si necesita configurar esto a través de la Política de grupo, vaya a **Configuración del equipo** > **Políticas** > **Configuración de Windows** > **Configuración de seguridad** > **Políticas locales**. En Opciones de seguridad, establezca "Controlador de dominio: permitir que los operadores del servidor programen tareas" como deshabilitado.



Si la clave SubmitControl no estaba creada en el equipo, se recomienda agregarla. Para hacerlo, vaya al subárbol del registro: **HKEY_LOCAL_MACHINE** luego a la ruta del registro: **\System\CurrentControlSet\Control\LSA**. Agregue el nombre del valor **SubmitControl** como un valor **REG_DWORD** de 0.

Si necesita configurar esto a través de la Política de grupo, vaya a **Configuración del equipo** > **Políticas** > **Configuración de Windows** > **Configuración de seguridad** > **Políticas locales**. En Opciones de seguridad, establezca "Controlador de dominio: permitir que los operadores del servidor programen tareas" como deshabilitado.

11. Domain controller: Allow server operators to schedule tasks, Microsoft.

2.2. Aumentar la prioridad de programación a los administradores

Esto se puede configurar a través de GPO: **Configuración del equipo** > **Políticas** > **Configuración de Windows** > **Configuración de seguridad** > **Políticas locales** > **Asignación de derechos de usuario:** Aumente la prioridad de programación.

Se aplica a: Windows Vista, Windows Server 2008, Windows 7, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2012, Windows 8.

Específicamente, esta configuración de seguridad determina qué cuentas pueden usar un proceso con acceso de propiedad de escritura a otro proceso para aumentar la prioridad de ejecución que se asigna al otro proceso. Un usuario con este privilegio puede cambiar la prioridad de programación de un proceso a través de la interfaz de usuario del Administrador de tareas.

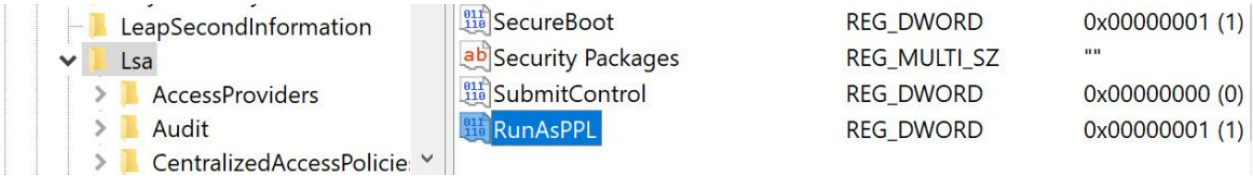
12. Increase scheduling priority, Microsoft.

2.3. Habilitar la protección LSA

En el panel izquierdo del Editor del registro, expanda **HKEY_LOCAL MACHINE** > **Sistema** > **CurrentControl** > **Control** > **Lsa**. En el panel derecho, haga clic con el botón derecho en un área de espacio vacío y seleccione "**Nuevo Valor DWORD (32 bits)**" en el menú.

En el cuadro de nuevo valor, escriba "**RunAsPPL**" y presione enter. Ahora haga doble clic en el nuevo valor **RunAsPPL**. En el cuadro Información del valor, escriba "**1**" y presione "**Aceptar**".

Cierre el Editor del Registro y reinicie el equipo.



Los atacantes a menudo apuntan a este proceso para recolectar credenciales utilizando herramientas como Mimikatz y realizar ataques de paso del hash. Si tiene complementos en su entorno, es posible que deba establecer el valor en "auditoría" antes de habilitarlo por completo para probar el impacto en su red.

Microsoft comparte la configuración adicional para la protección LSA de valor auditoria en el siguiente link:

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn408187(v=ws.11)

MALICIOUS FILE

1. Prácticas de seguridad

1.1. Mitigue la ejecución de archivos maliciosos

Mitigación	Descripción
Prevención de ejecución	Bloqueé la ejecución de código en un sistema a través del control de aplicaciones y/o bloqueo de scripts.
Entrenamiento de usuario	Utilice la formación de los usuarios como una forma de concienciar sobre las técnicas habituales de phishing y spearphishing y cómo generar sospechas de posibles eventos maliciosos.
Gestión de extensiones	Determine qué extensiones de archivo se están cargando. Asegúrese de que solo se puedan cargar las extensiones necesarias y que solo se autorice una cantidad limitada de tipos de archivo.
Reglas del Firewall	Agregue reglas de firewall que eviten que los servidores web establezcan nuevas conexiones a sitios web externos ayudará a evitar vulnerabilidades de inclusión de archivos remotos.

13. User Execution: Malicious File, Mitre att&ck.

1.2. Detección

Supervise la ejecución y los argumentos de la línea de comandos de las aplicaciones que un adversario puede utilizar para obtener acceso inicial que requiera la interacción del usuario. Esto incluye aplicaciones de compresión, como las de archivos zip, que se pueden utilizar para Desofuscar/Decodificar archivos o información en cargas útiles.

El antivirus puede detectar potencialmente documentos y archivos maliciosos que se descargan y ejecutan en la computadora del usuario. La detección de puntos finales o la detección de red pueden detectar potencialmente eventos maliciosos una vez que se abre el archivo (como un documento de Microsoft Word o PDF que se conecta a Internet o genera powershell.exe).

2. Configure reglas de reducción de superficie de ataque

Las siguiente sección describe cada una de las 15 reglas de reducción de la superficie de ataque, si requiere detallar la configuración para cada regla, se anexa el link de Microsoft para su consulta.

Esta tabla muestra sus GUID correspondientes, que usa si está configurando las reglas con la directiva de grupo o PowerShell.

Nombre de la regla	GUID	Exclusiones de archivos y carpetas	SO mínimo compatible
Bloquear el contenido ejecutable del cliente de correo electrónico y el correo web	BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior
Bloquear todas las aplicaciones de Office para que no creen procesos secundarios	D4F940AB-401B-4EFC-AADC-AD5F3C50688A	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior
Impedir que las aplicaciones de Office creen contenido ejecutable	3B576869-A4EC-4529-8536-B80A7769E899	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior
Impedir que las aplicaciones de Office inyecten código en otros procesos	75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior
Bloquear JavaScript o VBScript para que no inicien contenido ejecutable descargado	D3E037E1-3EB8-44C8-A917-57927947596D	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior
Bloquear la ejecución de scripts potencialmente ofuscados	5BEB7EFE-FD9A-4556-801D-275E5FFC04CC	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior
Bloquear llamadas a la API de Win32 desde macros de Office	92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior
Bloquear la ejecución de archivos ejecutables a menos que cumplan con un criterio de prevalencia, edad o lista de confianza	01443614-cd74-433a-b99e-2ecdc07bfc25	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior
Utilice protección avanzada contra ransomware	c1db55ab-c21a-4637-bb3f-a12568109d35	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior

Nombre de la regla	GUID	Exclusiones de archivos y carpetas	SO mínimo compatible
Bloquear el robo de credenciales del subsistema de autoridad de seguridad local de Windows (lsass.exe)	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior.
Bloquear las creaciones de procesos que se originan a partir de comandos PSExec y WMI	d1e49aac-8f56-4280-b9ba-993a6d77406c	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior.
Bloquear procesos no confiables y sin firmar que se ejecutan desde USB	b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior.
Impedir que la aplicación de comunicación de Office cree procesos secundarios	26190899-1602-49e8-8b27-eb1d0a1ce869	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior.
Impedir que Adobe Reader cree procesos secundarios	7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c	Soportado	Windows 10, versión 1709 (RS3, compilación 16299) o superior.
Bloquear la persistencia a través de la suscripción a eventos de WMI	e6db77e5-3df2-4cf1-b95a-636979351e5b	No soportado	Windows 10, versión 1903 (compilación 18362) o superior.

14. Reduce attack surfaces with attack surface reduction rules, Microsoft.

REFERENCIAS

1. Spearphishing a law enforcement and cross-industry perspective, European Cybercrime, Europol EC3 2019.

2. Guidelines on Electronic Mail Security, NIST Special Publication 800-45, Versión 2. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-45ver2.pdf

3. Drive-by Compromise (t1189), Cyberwarfare labs. https://blog.cyberwarfare.live/drive-by-compromiset1189/

4. Top 12 Tips For Safer Browsing On The Internet, Cybercrime Magazine. https://cybersecurityventures.com/12-tips-for-safer-browsing/

5. Risk Management for Replication Devices, NISTIR 8023. https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8023.pdf

6. Using Caution with USB Drives, Cybersecurity & Infrastructure Security Agency. https://us-cert.cisa.gov/ncas/tips/ST08-001

7. Command and Scripting Interpreter, Mitre att&ck. https://attack.mitre.org/techniques/T1059/

8. Mitre att&ck T1059 Command Line Interface, Picus Security Company. https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1059-command-line-interface

9. Mitre att&ck T1064 Scripting, Picus Security Company. https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1064-scripting

10. Scheduled Task/Job, Mitre att&ck. https://attack.mitre.org/techniques/T1053/

11. Domain controller: Allow server operators to schedule tasks, Microsoft. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj852168(v=ws.11)?redirectedfrom=MSDN

12. Increase scheduling priority, Microsoft. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn221960(v=ws.11)?redirectedfrom=MSDN

13. User Execution: Malicious File, Mitre att&ck. https://attack.mitre.org/techniques/T1204/002/

14. Reduce attack surfaces with attack surface reduction rules, Microsoft. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction#block-untrusted-and-unsigned-processes-that-run-from-usb

CONTACT

UNIVERSIDAD CATÓLICA DE COLOMBIA
FACULTAD DE INGENIERÍA

lfrodriguez59@ucatolica.edu.co
caibanez67@ucatolica.edu.co