SOPHOS
Security made simple.

Novedades de Sophos Intercept X

Enero de 2018

Nueva detección de malware de aprendizaje profundo (Deep Learning)

El modelo de escaneado de archivos de aprendizaje profundo detecta nuevo malware desconocido y aplicaciones potencialmente no deseadas.

El modelo ocupa menos de 20 MB y solo requiere actualizaciones ocasionales.

Durante el entrenamiento, el modelo identifica atributos importantes automáticamente, lo que tiene como resultado un límite de decisión más preciso entre los archivos de malware y los benignos.

- **Técnicas de prevención de exploits nuevas y mejoradas**
  - **Migración de procesos maliciosos**: detecta una reflective DLL injection remota utilizada por adversarios para moverse lateralmente entre procesos que se ejecutan en el sistema.
  - **Aumento de privilegios de procesos**: evita que un proceso con privilegios limitados obtenga privilegios más altos, una táctica utilizada a menudo por un adversario activo para obtener derechos de acceso al sistema.
- **Nuevas mitigaciones de adversarios activos**
  - **Protección contra robos de credenciales**: evita el robo de contraseñas de autenticación e información de hash de la memoria, el Registro y el disco duro.
  - **Utilización de cuevas de código**: detecta la presencia de código desplegado en otra aplicaciones, utilizado a menudo para la persistencia y la elusión de antivirus.
  - **Protección de llamadas a procedimientos de aplicaciones (APC)**: detecta usos ilegítimos de las llamadas a procedimientos de aplicaciones, utilizadas a menudo como parte de la técnica de inyección de código Atom Bombing y, más recientemente, como método para propagar el gusano WannaCry y el wiper NotPetya a través de EternalBlue y DoublePulsar. Los adversarios pueden aprovechar estas llamadas para hacer que otro proceso ejecute su código.
- **Bloqueo de aplicaciones mejorado**
  - **Bloqueo del comportamiento del navegador**: Intercept X impide usos maliciosos de PowerShell desde navegadores como bloqueo de comportamiento básico.
  - **Bloqueo de aplicaciones HTA**: se aplicarán las mitigaciones de bloqueo a las aplicaciones HTML que carga el navegador como si fueran un navegador.
- **Nuevas protecciones del Registro**
  - **Protección de teclas especiales**: Intercept X impide el reemplazo del ejecutable de las teclas especiales por parte de un adversario, que suele hacerlo para lograr persistencia.
  - **Protección del comprobador de aplicaciones**: Intercept X impide el reemplazo de los DLL del comprobador de aplicaciones que permitiría al adversario burlar un antivirus y otro comportamiento normal de inicio de procesos.

Técnica detectada	Notificación al usuario	RCA	Acción del administrador necesaria	Estado de seguridad	Proceso finalizado
Robo de credenciales	SÍ	SÍ	SÍ (ALERTA)	RED:	SÍ
Cueva de código	SÍ	SÍ	NO (Evento)	VERDE	SÍ
Reflective DLL injection remota	SÍ	SÍ	SÍ (ALERTA)	RED:	SÍ
Aumento de privilegios	SÍ	SÍ	SÍ (ALERTA)	RED:	SÍ
Protección de APC	SÍ	SÍ	NO (Evento)	VERDE	SÍ
Teclas especiales	NO	NO	NO	VERDE	No disp.
Comprobador de aplicaciones	NO	NO	NO	VERDE	No disp.
Bloqueo (PowerShell del navegador)	SÍ	SÍ	NO (Evento)	VERDE	SÍ
Bloqueo (ATA desde el navegador)	SÍ	SÍ	NO (Evento)	VERDE	SÍ

Detección de malware de aprendizaje profundo

Con el nuevo modelo de aprendizaje profundo, podemos realizar una evaluación previa a la ejecución sin firmas de cualquier archivo ejecutable y determinar si se trata de malware, software potencialmente no deseado o una aplicación legítima.
En Sophos hemos aplicado un enfoque único a nuestras capacidades de aprendizaje automático de seguridad: hemos invertido de forma sustancial en la tecnología de redes neuronales profundas a expensas de métodos más frecuentes que, aunque sigan dominando la industria de la seguridad, están siendo descartados rápidamente por la comunidad de informáticos especialistas en aprendizaje automático.

Ventajas del aprendizaje profundo sobre el aprendizaje automático tradicional:

- El aprendizaje profundo identifica automáticamente lo que es importante en los datos sin procesar y, por ende, ofrece una mayor precisión.
- El aprendizaje profundo utiliza macrodatos de forma nativa, y se escala fácilmente de forma que puede "memorizar" el extenso panorama de amenazas y generalizar a partir de él para detectar nuevas amenazas.
- El aprendizaje profundo es la tendencia tecnológica dominante en inteligencia artificial, lo que significa que la estrategia de aprendizaje profundo de Sophos se beneficia de la innovación de los principales actores del sector.
- El aprendizaje profundo produce unos mejores índices de detección, menos falsos positivos y muchísimas menos huellas que otros sistemas de detección de aprendizaje automático.

¿Cómo detecta Intercept X los archivos ejecutables maliciosos?

En lugar de realizar un escaneado heurístico con firmas como hacen los antivirus tradicionales, las redes neuronales profundas pueden seleccionar los atributos de software que determinan que se corresponden de forma más exacta con el malware. El modelo de aprendizaje profundo aprende lo que debe buscar en el código, cómo eluden la detección los adversarios, cómo crean su software y cómo planea desplegarse y ejecutarse el software. Esta información se evalúa por medio de un algoritmo de aprendizaje profundo de varias fases para determinar la similitud entre el software y el malware o software potencialmente no deseado; en función de la puntuación, se clasifica como malicioso, potencialmente no deseado o legítimo. Todo esto se hace en unos 20 milisegundos con un modelo de menos de 20 MB.

¿Qué ocurre cuando se detecta un ataque?

Cuando el modelo de aprendizaje profundo detecta malware, Intercept X comprueba si se encuentra en alguna lista de supresión. Más adelante hablaremos de la supresión de falsos positivos pero, por ahora, basta con saber que la lista de supresión nos permite ejecutar un modelo sumamente agresivo para detectar malware y seguir manteniendo una tasa de detección de falsos positivos extremadamente baja. El software detectado como malicioso se pondrá en cuarentena y se iniciará un análisis de causa raíz. Si la detección no es correcta, un administrador puede liberar la muestra simplemente añadiéndola a su lista local de aplicaciones permitidas. A continuación, el endpoint mostrará un estado de seguridad verde, puesto que se ha impedido que se ejecutara el malware.

¿Qué debe hacer un administrador?

El ataque se ha detectado antes de la ejecución, pero es posible que el administrador quiera consultar el informe de RCA para determinar cómo ha llegado al dispositivo, a fin de poder tomar medidas y evitar futuras infecciones.
Si el administrador determina que la detección no es correcta, puede añadir la aplicación a la lista de aplicaciones permitidas para su sitio directamente desde el evento de detección. Así se restaurará automáticamente la aplicación donde se haya detectado en todos los dispositivos afectados y se suprimirán futuras detecciones en función del hash de archivo, el certificado de firma o el nombre y la ruta del archivo.

Supresión de falsos positivos

Se ha creado una nueva cuarentena para contener el malware detectado. Cuando se produce una detección de actividad maliciosa, se ordena a Sophos Clean que realice una eliminación dirigida del archivo y de cualquier entrada del Registro, enlace o archivo asociado. La información se pone en cuarentena, y el administrador puede liberarla directamente desde el evento de detección en Sophos Central.
Liberar malware o un archivo de una aplicación no deseada lo añadirá a la lista de aplicaciones permitidas de todo el sitio y restaurará el archivo en los endpoint afectados. Al añadir un archivo a la lista de aplicaciones permitidas, el administrador puede seleccionar la identidad del hash de archivo, el certificado de firma o el nombre y la ruta del archivo. De ahí en adelante, si se detecta este archivo, se suprimirá el bloqueo y se ejecutará de la forma prevista. Además de la lista de supresión de falsos positivos específica del cliente, Sophos mantiene una función de supresión global. La supresión de falsos positivos de Sophos se activa automáticamente cuando Live Protection está habilitado, y Sophos enviará pequeñas actualizaciones de datos al endpoint cuando esté conectado a la red. La razón por la que tenemos una función de supresión de falsos positivos global es posibilitar que el modelo de aprendizaje profundo de detección de malware y aplicaciones no deseadas sea sumamente agresivo a la hora de detectar malware. Esto nos permite disponer de un modelo de detección progresivo con una detección de falsos positivos sumamente baja.

SOPHOS

Otra enorme ventaja de ofrecer esta robusta supresión de falsos positivos es que los clientes pueden desplegar y empezar a sacar partido del aprendizaje automático sin tener que pasar por semanas de ajustes y configuraciones, que es lo habitual con muchos otros proveedores.

Prevención de robos de credenciales

Intercept X detecta cuando un proceso controlado por un adversario intenta extraer credenciales de autenticación de usuarios y administradores de un dispositivo. Un adversario que intenta robar credenciales puede atacar múltiples componentes del sistema operativo para conseguir la contraseña o las contraseñas con hash de los usuarios y los administradores del dispositivo. El adversario tiene a su disposición docenas de herramientas distintas para lograr esto, pero entre las más utilizadas se incluyen mimikatz, una herramienta de extracción de credenciales que ataca la memoria LSASS (Servicio de subsistema de autoridad de seguridad local) y hashdump, una herramienta de robo de credenciales que extrae la contraseña con hash de la base de datos SAM (Administrador de cuentas de seguridad).

¿Cómo evita Intercept X el robo de credenciales?

En lugar de dirigirse a las herramientas específicas que utilizan los adversarios (y existen muchas), Intercept X busca interacciones no autorizadas con la memoria en tiempo de ejecución LSASS, el registro de la base de datos SAM y la extracción directa de datos de credenciales del disco duro. Como técnica de prevención, hemos realizado pruebas con diversas muestras de malware y herramientas de penetración y hacking, y hemos observado que la mitigación es sumamente efectiva sin generar alertas de falsos positivos para el software legítimo que interactúa con LSASS y la base de datos SAM.

¿Qué ocurre cuando se detecta un ataque?

Cuando Intercept X detecta que un adversario intenta robar credenciales, se pone fin al proceso que realiza el ataque y se presenta una notificación al usuario final.

Esto también inicia un análisis de causa raíz y alerta al administrador de la actividad para que pueda investigarse.

El endpoint permanecerá en un estado de seguridad rojo hasta que el administrador borre la notificación de alerta después de la investigación.

¿Qué debe hacer un administrador?

El ataque se ha detectado en tiempo de ejecución y, aunque se ha puesto fin al proceso atacante, es posible que se repita la técnica de penetración inicial o que el atacante aún tenga acceso al dispositivo. La penetración en el dispositivo suele implicar un engaño al usuario final para que autorice la instalación de software malicioso, o habilitar macros u otras acciones, pero en algunos casos, la penetración no implica ninguna autorización por parte del usuario.

La detección de un ataque genera una alerta para informar al administrador de que se ha detectado un intento de robo de credenciales y que está justificada una revisión más a fondo del incidente. Para ayudar en la investigación, esta detección también solicita la generación de un informe del incidente utilizando la función de análisis de causa raíz de Intercept X.

Protección de procesos (cueva de código)

El uso de cuevas de código es una técnica utilizada por adversarios en la que estos modifican lo que probablemente es software legítimo de modo que contenga una aplicación adicional. Esta aplicación adicional se inserta en lo que se denomina cueva de código, una sección del archivo de la aplicación de destino que no utiliza el programa. Las cuevas de código existen en la mayoría de aplicaciones, y añadir código en estas secciones normalmente no altera el comportamiento de la aplicación principal. A menudo, el código de ejecución que se inserta en una cueva de código es simplemente un iniciador de shell remoto. Este suele ser muy pequeño y sencillamente concede acceso al adversario al dispositivo en que puede realizar otras acciones. Este tipo de ataque requiere que el adversario tenga establecida una presencia en el dispositivo, a fin de que pueda desplegar el software o engañar al usuario para que descargue e instale una aplicación que tiene la cueva de código ya explotada.

Una de las principales razones por las que utilizan cuevas de código los adversarios es evitar que los detecten los usuarios generales y administradores. La aplicación esperada sigue funcionando bien, pero la aplicación insertada también se está ejecutando. Si la aplicación que se ha modificado es una herramienta empresarial legítima que el administrador espera encontrar en el dispositivo, es menos probable que la considere malware

si un antivirus tradicional detecta un problema. Es posible que los administradores simplemente la añadan a la lista de exclusión al dar por supuesto que el motor antivirus ha generado un falso positivo. De esta forma, el adversario establece persistencia en el endpoint e incluso puede haber engañado al administrador para que permita la ejecución de la aplicación insertada.

¿Cómo evita Intercept X el uso de la técnica de la cueva de código?

Existe una serie de herramientas que pueden utilizar la técnica de la cueva de código para incrustar software en otra aplicación, y la mayoría de soluciones antivirus tradicionales simplemente buscan indicadores o firmas que estas herramientas dejan atrás cuando insertan código en la cueva de código. Para Intercept X, no queríamos seguir este planteamiento y, en su lugar, evaluamos las aplicaciones a fin de detectar el uso de cuevas de código. Esto se hace durante la ejecución inicial del software y, cuando detectamos la presencia de una aplicación adicional que reside en una cueva de código, finalizamos la aplicación.

¿Qué ocurre cuando se detecta un ataque?

Al detectar el uso de una cueva de código, se pone fin a la aplicación y se notifica al usuario.

Esto también inicia un análisis de causa raíz y alerta al administrador de la actividad para que pueda investigarse.

A continuación, Sophos Clean elimina el malware del dispositivo.

¿Qué debe hacer un administrador?

Al detectar el uso de una cueva de código, el administrador debe revisar el análisis de causa raíz para determinar cómo se desplegó en el dispositivo la aplicación infectada. Es posible que el adversario ya hubiera comprometido el dispositivo por otros medios y simplemente estuviera desplegando la cueva de código para garantizarse la persistencia en el dispositivo. Al bloquearse este ataque, es probable que el adversario esté buscando otras formas de ataque y persistencia. Si se ha engañado a un usuario para que descargue una aplicación con una cueva de código, es probable que el ataque se haya evitado, pero entender cómo intentó penetrar en el dispositivo ayudará a determinar qué formación se requiere o si es necesario implementar controles de políticas adicionales.

Protección de procesos (migración maliciosa – reflective DLL injection remota)

La migración de procesos es una técnica que aplica comúnmente el adversario cuando establece su presencia en un dispositivo al inicio y quiere pasar a otro proceso a fin de aumentar privilegios o hacerse con un acceso más perdurable. El adversario no quiere perder el control cuando el usuario final simplemente cierra el navegador o finaliza un proceso que se ha visto comprometido, de modo que le conviene migrarse a un proceso del sistema.

Las técnicas de migración pueden servirse de una reflective DLL injection remota. Si desea obtener más información sobre las DLL injections en general, MITRE pone a su disposición un recurso excelente. Un ataque de DLL reflectivo remoto es similar, pero es más difícil de resolver; el adversario ya ha comprometido un proceso y, a partir de ahí, manipula otro proceso para cargar archivos DLL y ejecutar código arbitrario.

¿Cómo evita Intercept X la migración maliciosa?

Intercept X supervisa la actividad de los procesos para detectar un comportamiento de asignación de memoria en un proceso remoto y la DLL injection en ese proceso. Este comportamiento no debería producirse y, cuando Intercept X lo detecta, tenemos una gran confianza en que es malicioso e indica que un adversario o script de malware se está ejecutando en el sistema comprometido.

¿Qué ocurre cuando se detecta un ataque?

Cuando Intercept X detecta que un adversario intenta migrarse a otro proceso de esta forma, se pone fin al proceso atacante y se presenta una notificación al usuario final.

Esto también inicia un análisis de causa raíz y alerta al administrador de la actividad para que pueda investigarse.

El endpoint permanecerá en un estado de seguridad rojo hasta que el administrador borre la notificación de alerta después de la investigación.

¿Qué debe hacer un administrador?

Puesto que el ataque se ha detectado en tiempo de ejecución, es posible que el adversario siga activo en el dispositivo y, aunque se ha puesto fin al proceso atacante, puede que se repita la técnica de penetración inicial o que el atacante aún tenga acceso desde otro proceso.

La detección también generará una alerta para informar al administrador de que se ha detectado una migración de procesos con inyección de DLL reflectiva remota y que está justificada una revisión más a fondo del dispositivo. Para ayudar en la investigación, este evento también solicita la generación de un informe del incidente utilizando la función de análisis de causa raíz de Intercept X.

Protección de procesos (aumento de privilegios)

Cuando un adversario consigue acceder a un sistema, normalmente no tiene el nivel de privilegios que quiere o necesita para llevar el ataque hasta el final. Existen varios métodos con los que el adversario puede aumentar sus privilegios, desde el robo de credenciales hasta la migración de procesos, pero como Intercept X cierra estas puertas, el adversario debe recurrir a otras técnicas. Una de ellas es robar el token de autenticación de un proceso de privilegios e insertarlo en otro proceso para aumentar sus privilegios.

Todos los procesos que se ejecutan en el dispositivo tienen un token de autenticación que utiliza el sistema operativo para determinar los privilegios del proceso. Con esta técnica, lo más probable es que el adversario quiera robar el token de autenticación de un proceso del sistema. Si un adversario puede robar el token de autenticación de un proceso con privilegios del sistema y utilizarlo, consigue lo que quiere sin necesidad de robar la contraseña del usuario administrador ni de migrar un proceso para conseguirla. Al aprovecharse de vulnerabilidades conocidas del kernel del sistema en dispositivos Windows no corregidos, el adversario dispone de una serie de técnicas bien documentadas para capturar un token con privilegios de un proceso y utilizarlo para sus propios propósitos. Dada la cantidad de métodos disponibles para el robo de tokens con privilegios, es probable que queden más vulnerabilidades aún desconocidas en el sistema operativo y en el kernel.

¿Cómo evita Intercept X el robo de tokens?

En lugar de intentar proteger contra las muchas vulnerabilidades conocidas que permiten el robo de tokens con privilegios, Intercept X detecta si a un proceso se le inserta un token de autenticación de privilegios con el fin de aumentar estos. Este comportamiento simplemente no lo utiliza el software legítimo y, al descubrirse, podemos estar bastante seguros de que se trata de un ataque por parte de un adversario activo. Al detectar este aumento de privilegios, Intercept X puede proteger contra esta técnica independientemente de qué vulnerabilidad, conocida o desconocida, se haya utilizado para robar el token de autenticación para empezar.

¿Qué ocurre cuando se detecta un ataque?

Se da fin al proceso y se notifica al usuario. También se inicia Sophos Clean para eliminar el malware.

Al producirse la detección, se genera un análisis de causa raíz para determinar cómo se ha iniciado el proceso atacante y qué otras cosas pueden haber ocurrido en el dispositivo que estén relacionadas con la causa raíz o el aumento detectado.

El endpoint pasa a un estado de seguridad rojo, ya que este ataque indica que es probable que un adversario se haya introducido en el dispositivo y se recomienda investigarlo.

¿Qué debe hacer un administrador?

Al igual que con las detecciones de prevención de exploits similares, los administradores deben revisar el informe de análisis de causa raíz para determinar cómo se ha desarrollado el ataque y de dónde procede.

Cuando se ha completado la investigación, el administrador puede borrar la alerta y permitir el normal funcionamiento del dispositivo.

Protección de procesos (APC malicioso en uso – AtomBombing)

AtomBombing es una técnica que utilizan los adversarios para engañar a otra aplicación a fin de que ejecute malware u otro código. La técnica es bastante compleja y nueva, e implica un uso indebido de las tablas ATOM de los sistemas operativos y las llamadas a procedimientos asincrónicos. Puede obtener más información sobre el AtomBombing aquí.

¿Cómo evita Intercept X el AtomBombing?

Intercept X busca usos indebidos de las llamadas APC. Al igual que muchos de los métodos de protección contra exploits ya disponibles en Intercept X, el producto puede supervisar la actividad de los procesos a nivel del kernel y, según nuestros conocimientos, este tipo de comportamiento nunca es benigno.

¿Qué ocurre cuando se detecta un ataque?

Se da fin a la aplicación explotadora y se notifica al usuario final.

También se inicia Sophos Central para eliminar el malware y se activa una evaluación del análisis de causa raíz para determinar cómo se ha iniciado el proceso atacante y qué otras cosas pueden estar ocurriendo.

¿Qué debe hacer un administrador?

Al igual que con las detecciones de prevención de exploits similares, los administradores deben revisar el informe de análisis de causa raíz para determinar cómo se ha iniciado el ataque y si se requieren otras acciones.

Protección del Registro (persistencia de teclas especiales)

Teclas especiales es una función de los sistemas operativos Windows. Esta función inicia una aplicación cuando el usuario pulsa la tecla Mayús cinco veces consecutivas. La aplicación que se debe iniciar está identificada en el Registro. La mayoría de aplicaciones simplemente deshabilitan esta función de Windows pero, si no lo hacen, el adversario puede aprovecharse de esta opción del Registro para iniciar el programa que quiera. Por si esto fuera poco, las teclas especiales funcionan desde la página de inicio de sesión, por lo que la aplicación se inicia con privilegios del sistema. Para realizar este cambio en el Registro, el adversario necesita obtener acceso al dispositivo o hacer que el usuario final ejecute la aplicación que quiere.

¿Cómo evita Intercept X la persistencia de teclas especiales?

Utilizar teclas especiales y otras modificaciones del Registro para establecer persistencia en un dispositivo es una técnica antigua que los hackers han utilizado durante años. Intercept X simplemente deshabilita la capacidad de cambiar el ejecutable de las teclas especiales de Windows. Esto evita que el adversario utilice la función para iniciar malware o lanzar una conexión remota al shell que por lo demás sería legítima.

¿Qué ocurre cuando se detecta un ataque?

No notificamos al usuario ni generamos una alerta cuando se modifica el registro para iniciar otra aplicación al activar las teclas especiales; simplemente garantizamos que se inicie la utilidad de Microsoft Windows autorizada.

Protección del Registro (migitación del comprobador de aplicaciones – DoubleAgent)

Esta es otra función del registro que pueden aprovechar como herramienta los adversarios. El ataque implica la modificación del registro para identificar software que debe ejecutarse siempre que se inicia una aplicación. La función de Microsoft está pensada para permitir a los desarrolladores supervisar y diagnosticar la actividad de la aplicación, pero, cuando la utiliza un adversario, normalmente es para obtener acceso al dispositivo y puede eludir las funciones de protección de la aplicación que se está ejecutando. Este ataque salió en las noticias en 2017, cuando se observó que era posible modificar el registro del software de muchos productos antivirus para ejecutar también la aplicación de un adversario. En realidad, el ataque es mucho más amplio que simplemente dirigirse a los productos antivirus; un cambio en el registro del comprobador de aplicaciones puede ser utilizado por cualquier aplicación que haya en el sistema operativo. Consulte este artículo de Sophos Naked Security para obtener más información.

¿Cómo evita Intercept X la modificación del registro?

Intercept X impondrá los DLL de Windows autorizados cuando se utilice la comprobación de aplicaciones. De esta forma, aunque el adversario consiga manipular el registro y configurarlo para que lance su ataque, la aplicación ignorará estos cambios ilegítimos en el registro.

Es importante destacar que, cuando Intercept X se despliega junto con un antivirus de la competencia, protegeremos ese producto antivirus contra ataques que utilicen la técnica DoubleAgent (comprobador de aplicaciones).

¿Qué ocurre cuando se detecta un ataque?

No notificamos al usuario final ni generamos una alerta cuando se modifica el registro para iniciar otra aplicación al activar el comprobador de aplicaciones; simplemente garantizamos que se inicie la utilidad de Microsoft Windows autorizada.

Bloqueo de procesos mejorada (navegadores y aplicaciones HTML)

Intercept X ya incluye el bloqueo de procesos, por el que se impiden diversos comportamientos maliciosos de tipos de procesos identificados. Con Intercept, hemos ampliado la función de bloqueo a fin de evitar que los navegadores web inicien PowerShell y la función de bloqueo de navegadores a aplicaciones que ejecuta el navegador (aplicaciones HTA).

¿Cómo evita Intercept X que se ejecuten aplicaciones desde el navegador?

Intercept X clasificará automáticamente una aplicación como navegador y, cuando lo haga, el bloqueo de aplicaciones clasificadas podrá impedir comportamientos maliciosos como PowerShell. El bloqueo se sirve de la capacidad de Intercept X de supervisar la actividad de la aplicación en el kernel y siempre está ejecutándose con la aplicación.

¿Qué ocurre cuando se detecta un ataque?

Cuando Intercept X detecta que una aplicación se comporta de esta forma, se le impide que lleve a cabo la actividad y se notifica al usuario.

También se genera un evento para que el administrador lo revise.

La detección de este tipo de comportamiento malicioso también solicitará la generación de un análisis de causa raíz para que lo revise el administrador.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

2017-11-30 (MP)

SOPHOS