Informe sobre inteligencia para la detección de amenazas

Panorama de amenazas de 2020

Descubra qué amenazas eludieron el perímetro

VMware Threat Analysis Unit

vmware®

Informe sobre inteligencia para la detección de amenazas

Panorama de amenazas de 2020

Resumen ejecutivo

Las vulneraciones de seguridad forman parte de la realidad actual. Los atacantes sofisticados son demasiado numerosos y obstinados como para que las defensas perimetrales puedan atraparlos. Les resulta relativamente fácil aprovecharse de las vulnerabilidades del perímetro de la red o engañar a un usuario para que les dé acceso a su dispositivo. Una vez salvados estos obstáculos, los atacantes pueden quedarse al acecho durante días, semanas o meses hasta que llega el momento oportuno para introducirse en sistemas más importantes, ejecutar una carga útil malintencionada y lograr su objetivo, sea el que sea. La cuestión no es si un ataque tendrá éxito, sino cuándo. Las organizaciones saldrán mejor paradas con un equipo de seguridad que centre sus esfuerzos en evitar la propagación de los ataques después de que se produzca la vulneración que con un equipo que intente evitar todos los ataques.

Los datos lo corroboran.

El siguiente informe de VMware Threat Analysis Unit es un resumen de los principales datos y conclusiones recabados entre julio y diciembre de 2020. En él se señalan las amenazas que eludieron las defensas perimetrales y que los sensores de VMware colocados dentro del perímetro lograron identificar.

Las conclusiones son muy claras: a pesar de haber desplegado un regimiento de defensas perimetrales, hay ciberdelincuentes operando en la red. Esta investigación nos muestra claramente cómo los atacantes eluden la detección perimetral e infectan los sistemas para después intentar propagarse lateralmente por la red a fin de lograr su objetivo. Sabiendo esto, los directores de seguridad de la información y los equipos de seguridad de la red pueden obtener información esencial sobre cómo hacer frente a estas amenazas, evitar que se propaguen e impedir que causen daños cuando ya han entrado en la red.

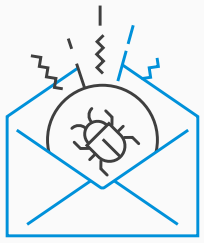
El análisis contiene

Telemetría de elementos de NSX Advanced Threat Analyzer, un entorno de pruebas específico para aislar e inspeccionar programas maliciosos que simula un host completo.

Telemetría de red de NSX Advanced Threat Prevention, que incluye análisis del tráfico de red y detección y prevención de intrusiones.

Otros análisis de amenazas detallados de ataques que tuvieron lugar en la segunda mitad de 2020.

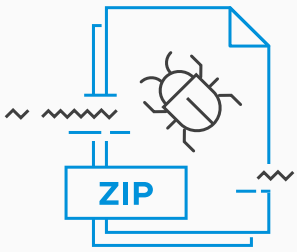
Información clave



EL CORREO ELECTRÓNICO SIGUE SIENDO EL VECTOR DE ATAQUE MÁS HABITUAL PARA OBTENER EL ACCESO INICIAL, Y MÁS DEL 4 % DE LOS MENSAJES DE EMPRESAS ANALIZADOS CONTENÍAN ALGÚN COMPONENTE MALICIOSO

Información

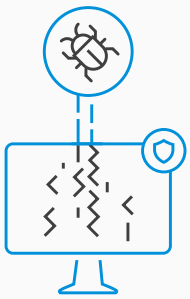
Los remitentes de correo electrónico malicioso son incansables y muy listos. Ingenian constantemente formas nuevas, o al menos diferentes, de engañar y atacar. La carga útil maliciosa que se detecta en los ataques por correo electrónico cambia a menudo, pero la gran mayoría de los ciberdelincuentes usan sobre todo tres estrategias básicas: archivos adjuntos maliciosos, enlaces a páginas web maliciosas y cebos para que se realicen transacciones. Las soluciones de seguridad del perímetro, como las herramientas antivirus, contra programas maliciosos y contra ataques de suplantación de identidad, son ineficaces frente a las amenazas sofisticadas por correo electrónico. Los agentes malintencionados van a seguir usando el correo electrónico como vector de ataque.



MÁS DE LA MITAD DE LOS ELEMENTOS MALICIOSOS ANALIZADOS SE DISTRIBUYERON EN UN ARCHIVO ZIP

Información

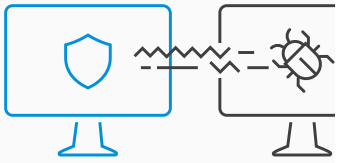
Los atacantes aumentaron enormemente sus operaciones a través de campañas de correo electrónico utilizando archivos ZIP adjuntos con contenido malicioso. Saben que las herramientas tradicionales de entorno pruebas no tienen la capacidad de analizar archivos raros y extraños, por lo que son en su mayoría ineficaces para detectar amenazas. Muchas soluciones de seguridad tratan los archivos ZIP protegidos con contraseña como si fueran archivos cifrados y no los inspeccionan. Se necesita una herramienta de entorno de pruebas moderna que identifique estas amenazas y pueda analizar el mayor número de tipos de archivos posible.



LA TÁCTICA DE MITRE ATT&CK® MÁS UTILIZADA POR LOS PROGRAMAS MALICIOSOS ES LA DE EVASIÓN DE LAS DEFENSAS, SEGUIDA POR LA EJECUCIÓN Y LA DETECCIÓN

Información

La primera línea de acción de los atacantes consiste en eludir la detección. Cuando consiguen esto, es esencial que se hagan persistentes en un entorno mediante la ejecución de elementos maliciosos. Una vez que son persistentes, empieza la detección de los procesos del sistema y los recursos de la red. Cuando los atacantes ponen en peligro un recurso de una red, ese dispositivo no suele ser su destino final. Todas estas tácticas tuvieron lugar detrás del cortafuegos, es decir, estas amenazas ya habían eludido los controles de seguridad del perímetro.

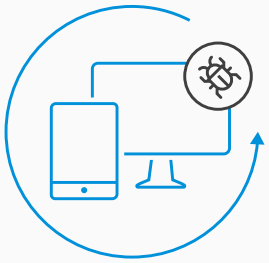


MÁS DE LA MITAD DE LAS ANOMALÍAS DE RED DETECTADAS SON DE SEÑALIZACIÓN INUSUAL, SEGUIDAS POR LAS CONEXIONES EN PUERTOS SOSPECHOSOS Y LAS CONEXIONES ANÓMALAS ENTRE DOS HOSTS

Información

La señalización inusual constituye una prueba clara y emite constantemente una señal para el objetivo deseado. La mayoría de las comunicaciones con una baliza no se cifran y los atacantes cada vez se aprovechan más de este hecho para usarlas como puerta de enlace al interior del centro de datos de una organización. La detección e identificación de la señalización anómala es un método eficaz para detectar y prevenir amenazas que los equipos de seguridad de las empresas pueden utilizar.

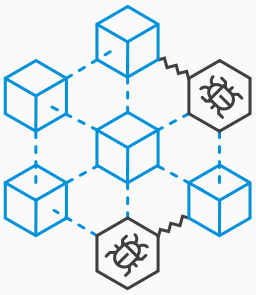
Información clave



MÁS DEL 60 % DE LAS INCIDENCIAS DE SEGURIDAD DE MANDO Y CONTROL TIENEN RELACIÓN CON UNA APLICACIÓN DE CONTROL REMOTO COMERCIAL

Información

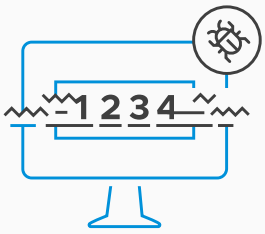
Los atacantes saben esconderse a plena luz del día. El uso de herramientas de gestión habituales para comunicarse con un atacante les permite ocultar sus transmisiones entre el tráfico legítimo. El problema es que cuando se hace explotar un programa malicioso, este se conecta tanto con sitios perjudiciales como con sitios legítimos. El programa puede hacer muchas cosas que no tienen nada que ver con su tráfico malicioso, con la actividad de mando y control, ataque o exfiltración. Por ejemplo, puede conectarse con un sitio web conocido para comprobar la conectividad a Internet o con servidores de correo legítimos para enviar correo no deseado. Si todos los destinos se clasifican como maliciosos, los conjuntos de aprendizaje se contaminarán considerablemente. Para etiquetar con precisión la actividad de las amenazas y determinar qué actividades son conexiones de mando y control, cuáles son conexiones de desplazamiento lateral, cuáles son ataques y cuáles son ruido, se necesitan algoritmos de aprendizaje automático.



EN UNA RED CORPORATIVA, LOS EVENTOS ASOCIADOS A ACTIVIDAD DE MINERÍA DE CRIPTOMONEDAS REPRESENTAN UN 25 % DE LAS AMENAZAS CONOCIDAS

Información

Existen riesgos potenciales claros cuando un programa malicioso de minería de criptomonedas pone la red en peligro. No solo están en juego los datos o la propiedad intelectual. Muchas amenazas a la seguridad atacan los recursos de la red para obtener beneficios ilegítimos. Los delincuentes podrían «aterrizar y expandirse», es decir, instalar un primer conjunto de programas maliciosos y hacer que el canal de mando y control esté operativo y, posteriormente, descargar programas maliciosos más agresivos. También podrían vender los sistemas atacados a otros delincuentes que tengan otros objetivos.



LA MALA PRÁCTICA DE SEGURIDAD MÁS COMÚN CONSTATADA ES EL USO DE CONTRASEÑAS DE TEXTO SIN CIFRAR

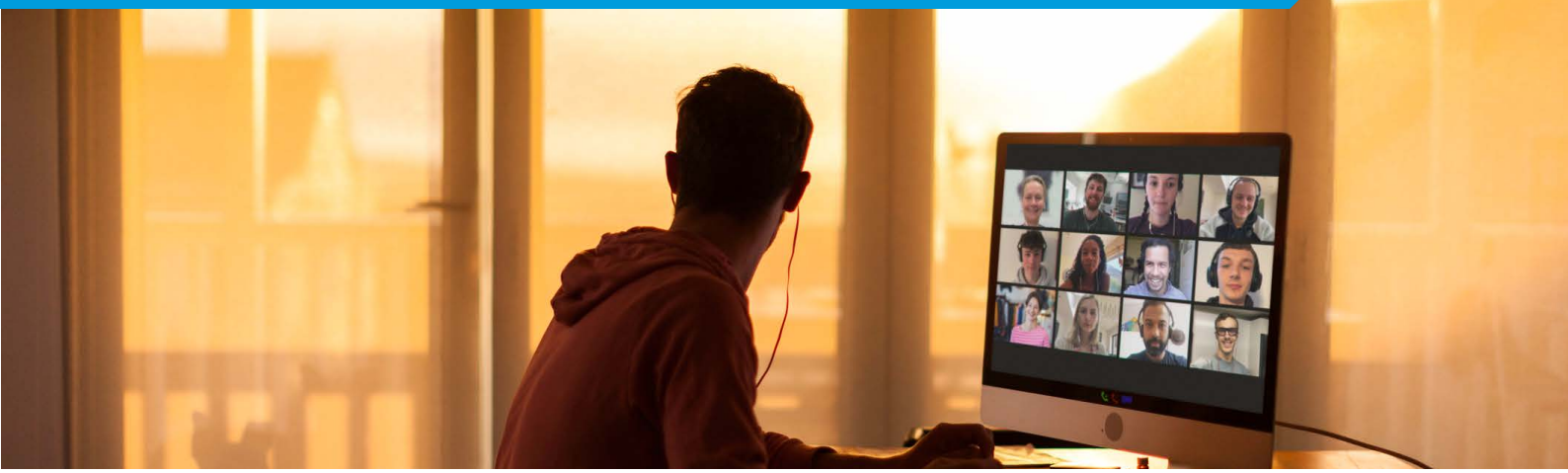
Información

Evitar estas incidencias de seguridad es sencillo. La transmisión de contraseñas de texto sin cifrar a través de la red puede proporcionar a los atacantes muchas facilidades y permitirles desplazarse lateralmente y exfiltrar datos.

MÁS DEL 75 % DE LOS EVENTOS DE DESPLAZAMIENTO LATERAL IDENTIFICADOS SE LLEVARON A CABO CON EL RDP, A MENUDO UTILIZANDO CREDENCIALES ROBADAS PARA INICIAR SESIÓN EN OTROS HOSTS DE LA RED

Información

Existen varias maneras de propagarse lateralmente, pero la técnica más común sigue siendo el inicio de sesión en hosts mediante el protocolo de escritorio remoto (RDP) utilizando contraseñas de texto sin cifrar a través de la red (vea la cifra anterior), cuentas válidas o credenciales obtenidas por la fuerza. Cuando los atacantes ponen en peligro un recurso de una red, ese dispositivo no suele ser su destino final. Para lograr su objetivo, los atacantes suelen acceder ilegalmente a un servidor web, el dispositivo de un empleado o alguna otra ubicación. A continuación, se desplazan lateralmente por la red desde el dispositivo vulnerado inicial para llegar a su objetivo. La vulneración inicial raras veces causa daños graves. Si los equipos de seguridad detectan el desplazamiento lateral antes de que los atacantes lleguen a sus objetivos, pueden impedirles que accedan a datos confidenciales. Los equipos de seguridad de las empresas pueden recurrir a la inteligencia artificial (IA) y al aprendizaje automático para detectar conexiones anómalas mediante el RDP.



Introducción

Nuestra forma de trabajar cambió en 2020 de formas que eran inimaginables. La pandemia mundial de COVID-19 y sus repercusiones económicas han separado a los usuarios de la seguridad que proporcionan las defensas perimetrales. Muchos empezaron a trabajar desde casa y a acceder a los sistemas esenciales de las empresas a través de conexiones VPN o directamente a plataformas de software como servicio (SaaS) y otras aplicaciones de nube.

Los atacantes aprovecharon inmediatamente esta situación y la ansiedad generada por la pandemia como desencadenantes de ataques de ingeniería social. Los ataques se han centrado cada vez más en la distribución de programas de secuestro, dirigidos sobre todo a víctimas importantes. Además, han vuelto a aparecer ataques que habían caído en desuso, dirigidos probablemente a ordenadores con un mantenimiento deficiente.

El principal problema que representan estos hosts vulnerables, a pesar de que no están en las instalaciones físicas de una organización, es que pueden proporcionar acceso a cuentas y hosts con mayores privilegios de las redes corporativas, así como a centros de datos empresariales. En algunos casos, los atacantes utilizan los dispositivos ya vulnerados de los usuarios para acceder a controladoras de dominio de Windows que, posteriormente, se usan como mecanismo muy eficaz para distribuir componentes de programas de secuestro por la red. Además, la pandemia ha impulsado el uso de la infraestructura de escritorios virtuales (VDI), el protocolo de escritorio remoto (RDP) y el escritorio como servicio (DaaS). Todo esto crea una combinación nueva de tráfico de aplicaciones y de usuarios en el centro de datos.

Ante estos cambios, es esencial que los equipos de seguridad de las empresas extiendan las funciones de detección y prevención de amenazas más allá del cortafuegos para proteger todo el tráfico este-oeste.

La información siguiente se obtuvo a partir de los datos recogidos entre julio y diciembre de 2020 mediante sensores de VMware distribuidos por redes empresariales muy diversas. Las redes tenían distintos tamaños y pertenecían a muchos sectores empresariales diferentes. Los sensores de VMware se instalan casi siempre tras los cortafuegos perimetrales y en el centro de datos, y proporcionan información exclusiva sobre ataques que ya han vulnerado las defensas perimetrales. Se trata de ataques muy escurridizos, sofisticados y específicos que tratan de propagar cargas útiles maliciosas para exfiltrar datos.

Telemetría de elementos

El entorno de pruebas de red constituye un entorno de aislamiento e inspección único que simula un host completo con CPU, memoria del sistema y todos los dispositivos de entrada y salida. Funciona interactuando con los programas maliciosos para analizar comportamientos de forma segura y analiza los elementos de programas maliciosos que eluden el perímetro y atraviesan el centro de datos. Durante el periodo de seis meses, el producto Advanced Threat Prevention (ATP) de la solución NSX Service-defined Firewall (SDFW) obtuvo información valiosa sobre la forma en que los elementos trataban de introducirse en los terminales.

Hay tres clases de elementos: benignos, sospechosos y maliciosos. Los benignos son elementos que no suponen una amenaza activa, como documentos, archivos ejecutables o bibliotecas. Los elementos sospechosos suponen en su mayoría un riesgo bajo, pero no se deben pasar por alto porque su naturaleza puede cambiar con solo pulsar un botón o introducir una actualización. Los elementos maliciosos son los componentes más agresivos y destructivos. Se suelen distribuir mediante un proceso de varios pasos cuyo objetivo es confundir a los sistemas de detección y ocultar acciones maliciosas entre el ruido de fondo de los eventos de la red.

El porcentaje de incidencias de estas clases de elementos permaneció relativamente constante durante los seis meses de investigación. Como se ve en la figura de la derecha, el porcentaje de elementos maliciosos detectados está en torno al 0,1 %.

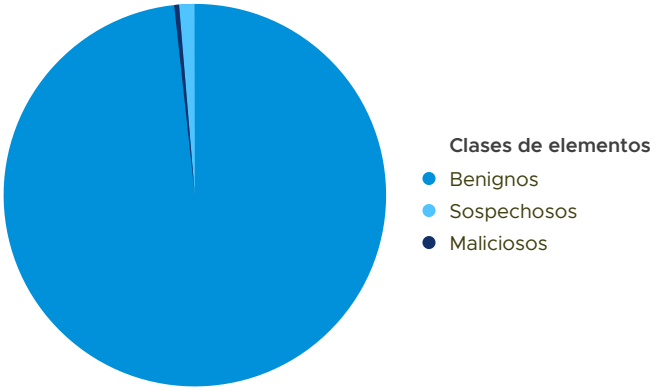


FIGURA 1: PORCENTAJES DE ELEMENTOS BENIGNOS, SOSPECHOSOS Y MALICIOSOS EN TODO EL PERIODO DE LA INVESTIGACIÓN.

El análisis de los tipos de archivos más habituales observados muestra una clara diferencia entre los elementos benignos y los maliciosos. Los benignos son en su mayoría tipos de archivos que se conocen a la perfección, como los archivos PDF que se muestran en la figura 2. Por su parte, los elementos maliciosos suelen ser distintos tipos de archivos más raros y extraños, como los archivos ISO9660 y ACE de la figura 3.

El uso de tipos de archivos poco comunes para distribuir elementos maliciosos se debe, en parte, al deseo de ocultar contenido en paquetes difíciles de analizar. Otras veces se usan para aprovechar defectos de seguridad del software anticuado y sin los parches necesarios que se utiliza para gestionar esos tipos de archivos.

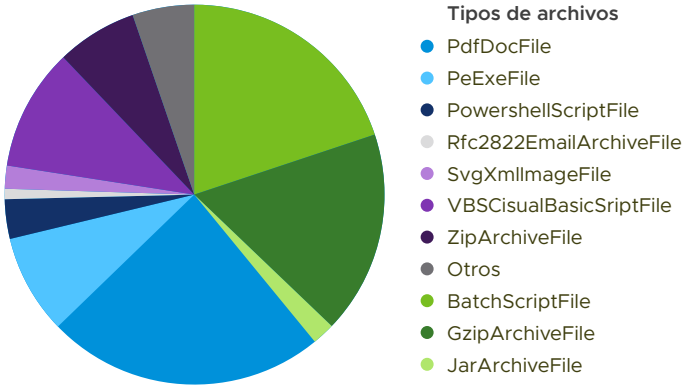


FIGURA 2: TIPOS DE ARCHIVOS MÁS OBSERVADOS EN LOS ELEMENTOS BENIGNOS.

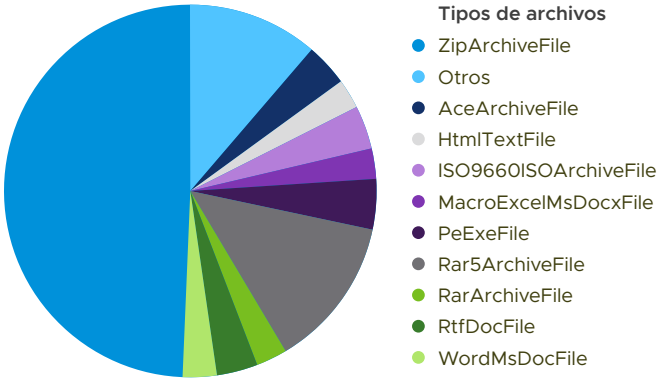


FIGURA 3: TIPOS DE ARCHIVOS MÁS COMUNES EN LOS ELEMENTOS MALICIOSOS.

El gráfico de la figura 4 muestra el porcentaje de elementos maliciosos observados durante el periodo analizado. En todo el periodo, el porcentaje de elementos maliciosos observados es de menos del 0,5 %, excepto en dos picos que se dieron en junio y noviembre. El primer pico, en junio, representa una campaña de correo no deseado malicioso que distribuía el programa de secuestro Avaddon. El atacante utilizó archivos ZIP que contenían archivos de JavaScript maliciosos. Los archivos de JavaScript maliciosos inician un comando de PowerShell que recupera y ejecuta la carga útil del programa de secuestro. El segundo pico, en noviembre, se debió a una campaña de correo no deseado malicioso llevada a cabo por la botnet Phorpiex. El atacante distribuyó archivos ZIP que contenían archivos ejecutables maliciosos que descargaban y ejecutaban el programa malicioso BitRansomware [1].

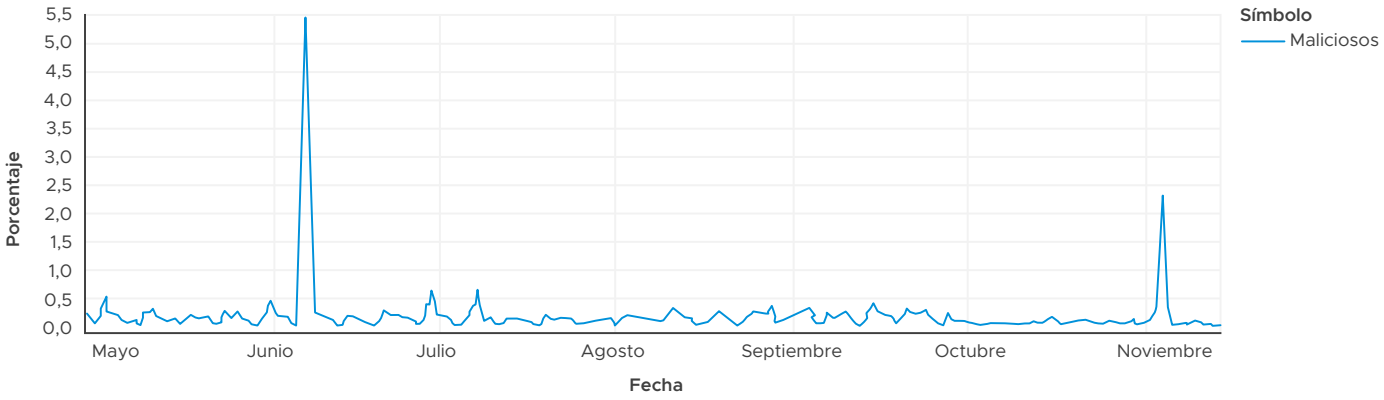


FIGURA 4: PORCENTAJE DE ELEMENTOS MALICIOSOS OBSERVADOS DURANTE EL PERIODO.

Para entender mejor cómo utilizan los atacantes distintos vectores de distribución, analizamos los índices de incidencia de archivos maliciosos y sospechosos de cada vector de distribución a partir de los datos de telemetría que generaron organizaciones en EE. UU. y EMEA en todo el periodo, como se ve en la figura 5. Los datos indican que el vector más utilizado para distribuir programas maliciosos es el correo electrónico, cuyo índice de incidencia de elementos maliciosos es de cerca del 4 %. Esto no es de extrañar. El correo electrónico sigue siendo el mecanismo de comunicación más común de las organizaciones y, por lo tanto, puede dar lugar a índices de infección más altos que otros vectores. Por otra parte, el protocolo SMB muestra el índice más alto de incidencia de archivos sospechosos en todos los vectores: más del 3 % de los archivos transferidos mediante SMB se etiquetaron como sospechosos. La investigación indica que la casi todos esos archivos son herramientas de gestión de TI, como scripts por lotes, que los servicios de TI comparten mediante SMB para actualizar Windows. Sabemos que los atacantes ya habían utilizado los dos tipos de archivos para distribuir programas maliciosos, por lo que estos tipos de archivos se etiquetan como sospechosos.

Teniendo en cuenta lo expuesto en la introducción de este informe, las amenazas distribuidas a través de los vectores indicados más abajo se detectaron detrás del cortafuegos perimetral. Es probable que los índices de infección se redujeran si a los controles perimetrales se les añadiera un entorno de pruebas de red para inspeccionar los elementos.

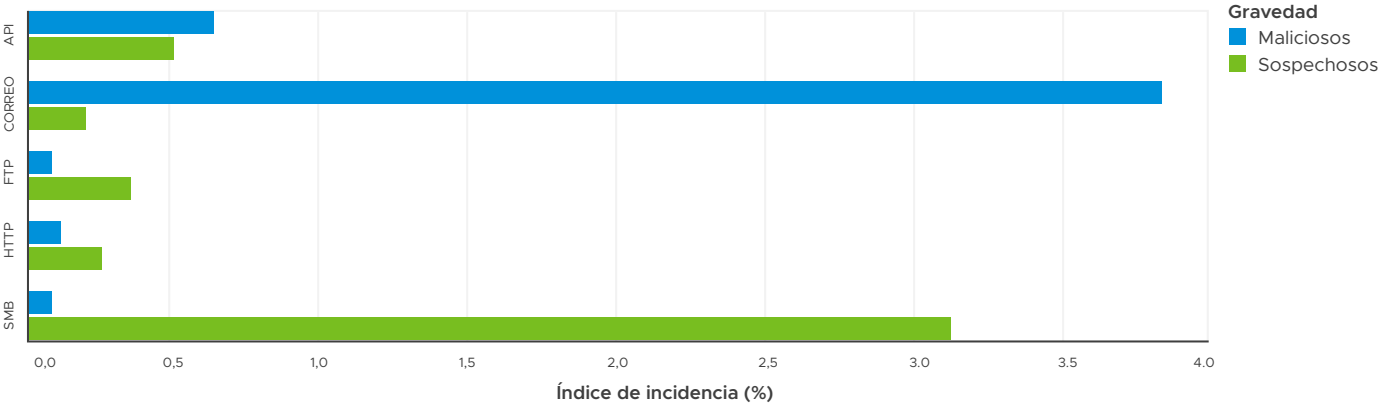
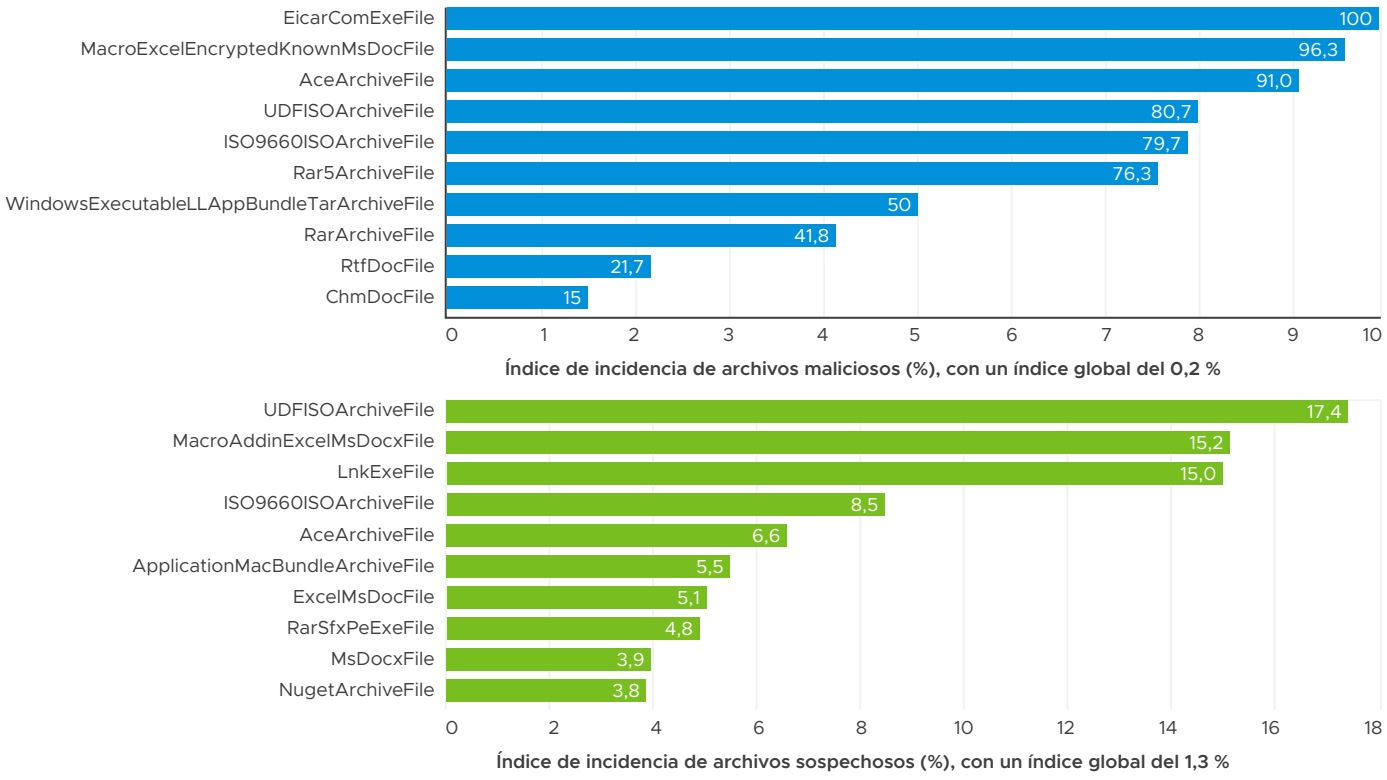


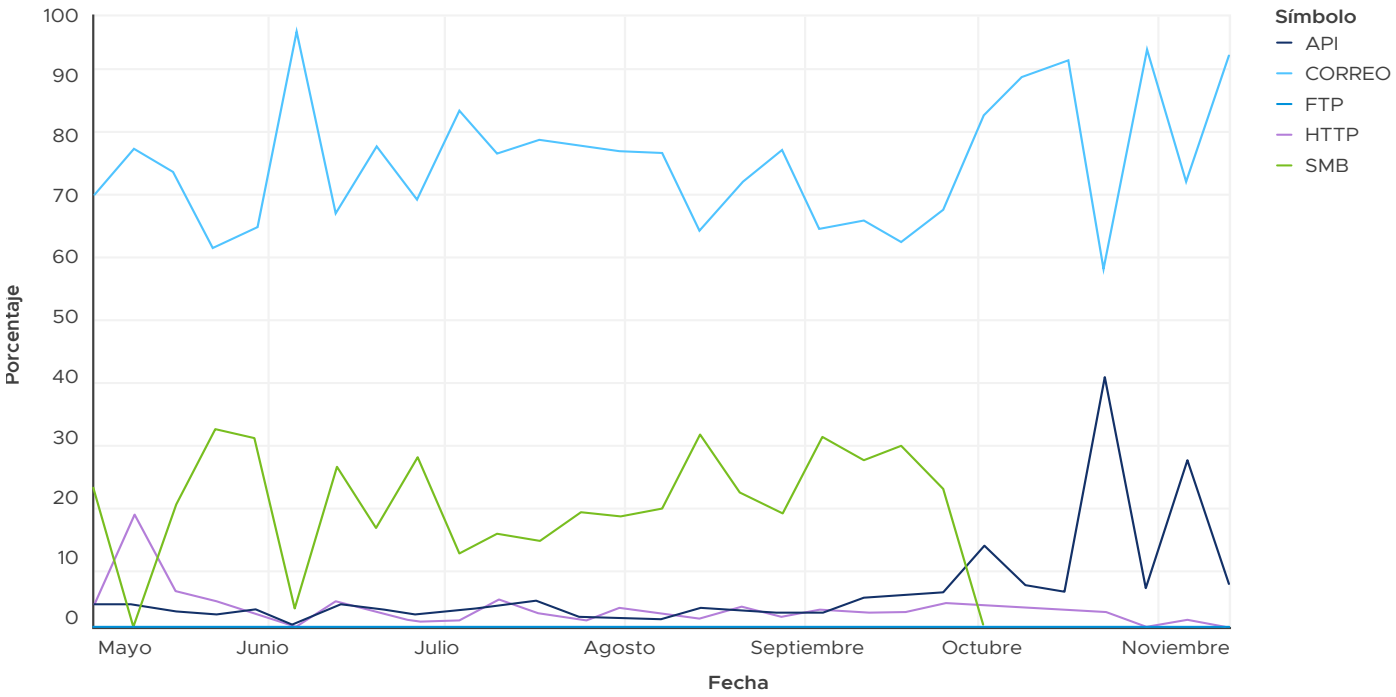
FIGURA 5: PORCENTAJES DE ELEMENTOS MALICIOSOS Y SOSPECHOSOS POR VECTOR DE DISTRIBUCIÓN EN TODO EL PERIODO.

El índice global de incidencia de elementos sospechosos de todos los tipos de archivos fue de en torno al 1,3 % durante el periodo. En el gráfico inferior de la figura 6 se enumeran los principales tipos de archivos con los índices de incidencia de sospecha más altos. El primer puesto lo ocupa el tipo de archivo de imagen con formato de disco universal (UDF), que se denomina UDFISOArchiveFile en el gráfico y tiene un índice de incidencia de sospecha de hasta el 17,4 %. Cabe señalar que este tipo de archivo tiene el cuarto índice de incidencia más alto entre los archivos maliciosos, como se ve en el gráfico anterior. Por tanto, es normal que tenga un índice de incidencia de sospecha alto. De la misma forma, otros tipos de archivos enumerados en el gráfico superior también aparecen en el inferior. El tipo de archivo MacroAddinExcelsDocxFile ocupa el segundo lugar en el gráfico, con un índice de incidencia de sospecha del 15,2 %. Es bien sabido que los atacantes utilizan con mucha frecuencia macros maliciosas integradas en archivos de Microsoft Excel para propagar programas maliciosos, tal y como se observó con la campaña Emotet a finales de 2020 [3]. Por otra parte, las macros se usan a menudo en aplicaciones legítimas. Esas macros suelen mostrar características parecidas a las de las macros maliciosas, por ejemplo, la macro se ejecuta automáticamente al abrir un archivo de Excel y se hace ininteligible para que el código VBA no se pueda copiar ni modificar. Esto explica en gran medida el alto índice de incidencia de sospecha.

Los índices de incidencia y los tipos de archivos de los elementos benignos y maliciosos son sumamente distintos. Dados estos altos índices de incidencia, es muy aconsejable implementar un entorno de pruebas de red para inspeccionar los archivos adjuntos del correo electrónico o crear reglas de correo electrónico para poner en cuarentena los tipos de archivo MacroExcelEncryptedKnownMSDocFile y AceArchiveFiles.



El gráfico siguiente, en la figura 7, muestra las tendencias en el tiempo de los elementos maliciosos observados por vector de distribución durante el periodo de investigación. Casi todos los elementos maliciosos que se observan en la telemetría se distribuyen por correo electrónico, lo que indica que los correos electrónicos de suplantación de identidad son el método que más utilizan los atacantes para distribuir elementos maliciosos. En ocasiones, los picos que se observan en las líneas de los vectores de distribución representan campañas en las que se usa el vector de distribución en cuestión. Por ejemplo, el pico que se observa en el vector de distribución por correo electrónico en junio representa la campaña de correo no deseado malicioso que distribuyó el programa de secuestro Avaddon.



El gráfico de la figura 8 muestra las tendencias en el tiempo de los elementos maliciosos observados por tipo de archivo. Se ven los cinco principales tipos de archivos que utilizaron los atacantes para distribuir elementos maliciosos durante el periodo analizado. La telemetría indica que, durante el análisis, la mayor parte de los elementos maliciosos se distribuyeron como archivos ZIP, que fueron los archivos que se utilizaron en varias campañas de correo electrónico.

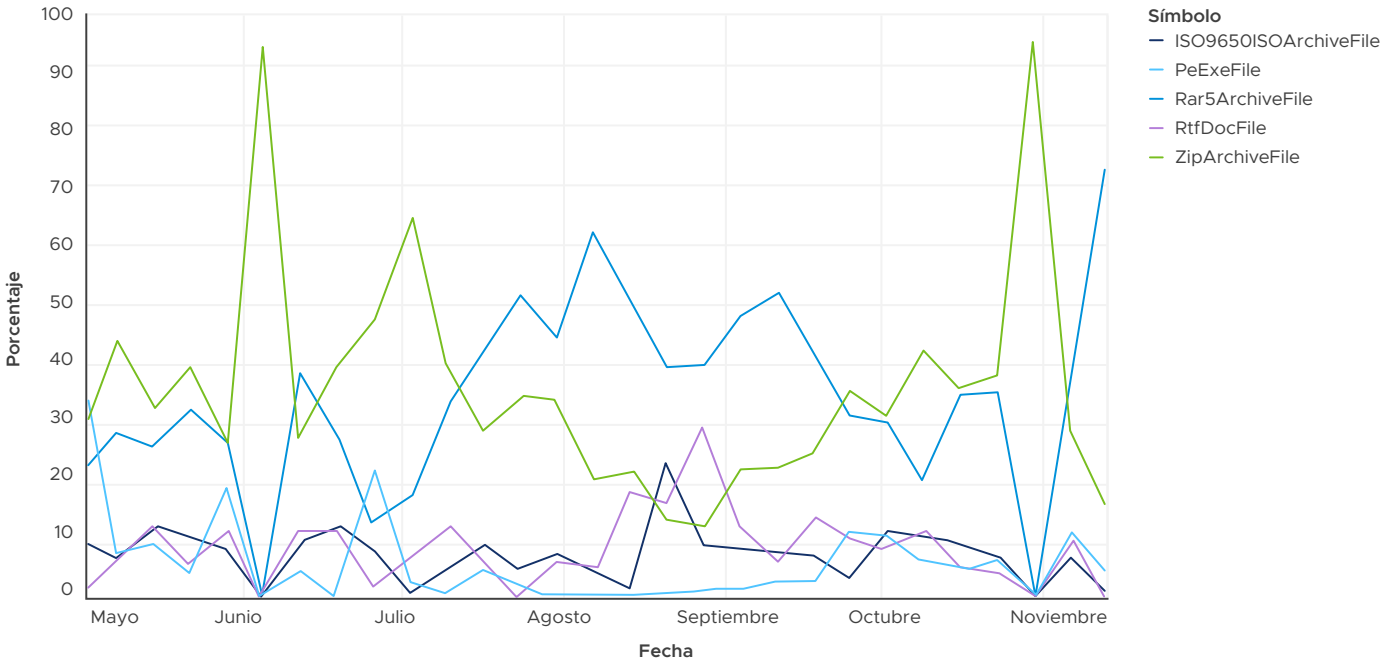


FIGURA 8: LOS CINCO TIPOS DE ARCHIVOS MALICIOSOS MÁS FRECUENTES DURANTE EL PERIODO ANALIZADO.

Si bien los vectores de distribución y los tipos de archivos son importantes a la hora de evaluar el riesgo asociado a elementos concretos, también es importante observar el comportamiento asociado a los elementos y los ataques.

Las figuras 9 y 10 muestran las tácticas y técnicas de MITRE ATT&CK® más utilizadas durante el periodo. Como se ve en la figura 9, la táctica TA0005: Evasión de defensas es la más utilizada por los programas maliciosos, seguida por las tácticas TA0002: Ejecución y TA0007: Detección. En la campaña Emotet que se analizó recientemente [3], el programa malicioso utilizó casi todas las tácticas del gráfico. El programa malicioso trata de eludir la detección (TA0005: Evasión de defensas) generando procesos de PowerShell y modificando archivos en el directorio del sistema de Microsoft Windows del ordenador de la víctima. Además, el programa malicioso introduce un archivo ejecutable (TA0002: Ejecución) y enumera los procesos en ejecución (TA0007: Detección) para ejecutar código que no es de confianza en procesos de Microsoft Office (una vez más, TA0002: Ejecución).

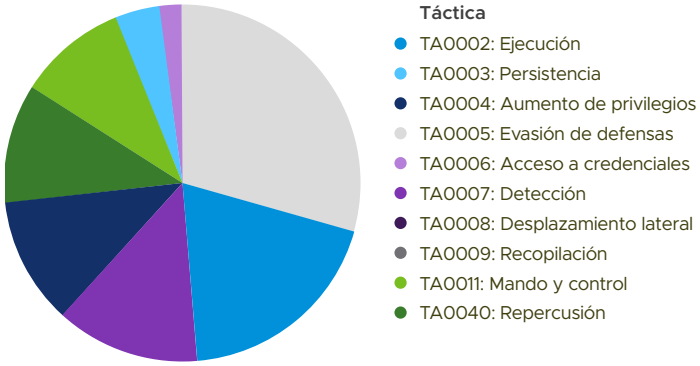


FIGURA 9: PRINCIPALES TÉCNICAS DE MITRE ATT&CK EN TODO EL PERIODO.

La figura 10 muestra las 20 técnicas más utilizadas en el mismo periodo. La más habitual es la técnica T1071: Protocolo de capa de aplicación estándar. Esta técnica tiene relación con actividades de red como la descarga de archivos desde una ubicación remota o la conexión con servidores de mando y control. Es muy común en ataques en los que se usa la carga útil inicial para realizar otras actividades maliciosas. La segunda técnica más habitual consiste en utilizar Instrumental de administración de Windows (WMI, denominada T1047: Instrumental de administración de Windows en el gráfico) como vector de ataque. Los atacantes pueden usar WMI para invocar procesos de PowerShell (T1086: PowerShell) como se vio en los ataques de Emotet [3]. Según un informe publicado en 2019 [4], casi el 50 % de los procesos de PowerShell maliciosos se iniciaron mediante WMI, y otro 40 % se invocaron directamente mediante cmd.exe (T1059: Interfaz de línea de comandos).

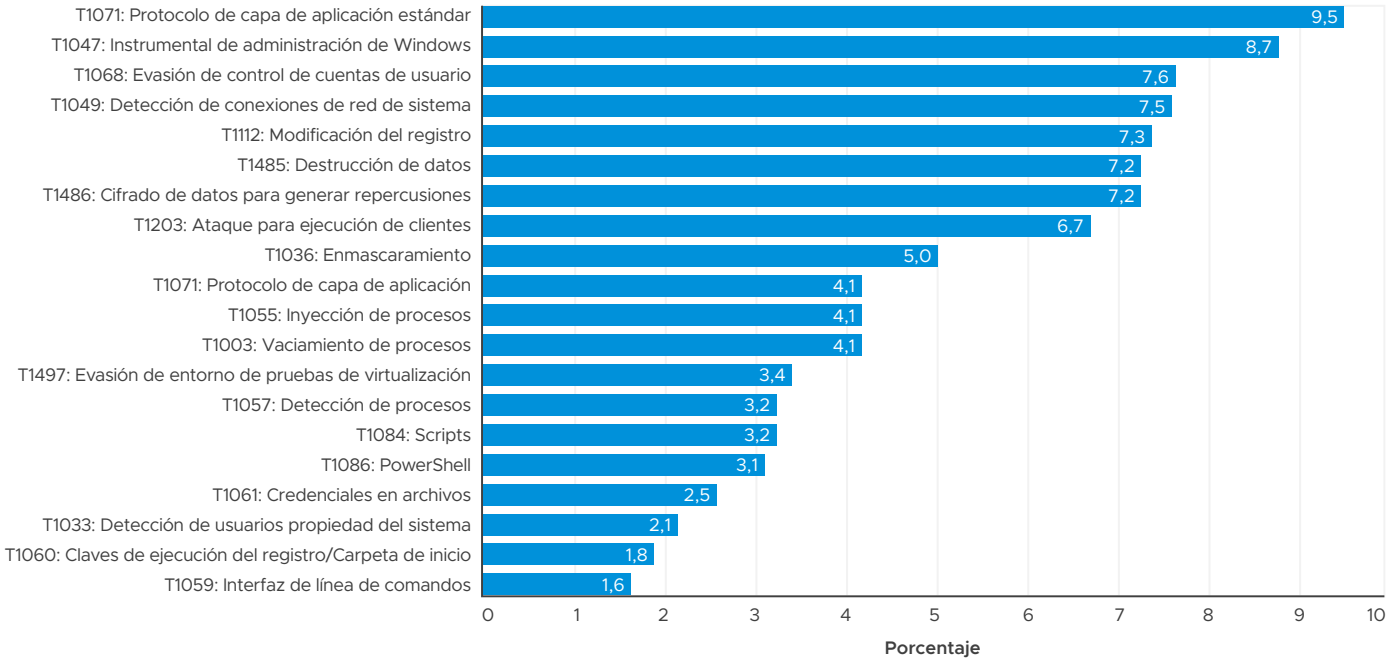


FIGURA 10: PORCENTAJE DE INCIDENCIA DE LAS PRINCIPALES TÉCNICAS DE MITRE ATT&CK EN TODO EL PERIODO. TÉCNICAS TOTALES ESTUDIADAS: 68.

Telemetría de red

El análisis de la telemetría nos permite entender mejor el panorama de la amenazas actual. El producto ATP que forma parte de NSX Service-defined Firewall (SDFW) tiene muchas funciones de detección gracias a un sistema de detección o prevención de intrusiones (IDS o IPS) totalmente distribuido y al análisis del tráfico de red basado en el comportamiento, que contribuye a obtener información muy fiable sobre las amenazas que entran en la red o se desplazan por ella.

En distintas clases de amenazas, el análisis destaca los tres tipos de eventos más frecuentes de cada clase. Los datos muestran una cantidad de ruido de fondo absoluta en forma de señalización (legítima o no) y malas prácticas de seguridad como protocolos de red sin cifrar.

Los 3 principales eventos de interacción de red anómala

Más del 50 % de las anomalías que detectaron los sensores de VMware eran actividades de señalización inusuales (vea la tabla 1), es decir, las redes corporativas supervisadas contienen dispositivos que se ponen en contacto con terminales externos o con otros dispositivos habitualmente, tanto por motivos legítimos como a consecuencia de alguna infección. Las conexiones en puertos sospechosos ocupan el segundo puesto, ya que son el distintivo de intentos de acceso no autorizado a los recursos corporativos. En el tercer puesto están las conexiones anómalas entre dos hosts. Estos eventos se producen, por ejemplo, cuando un host empieza a acceder a un servicio en un host al que nunca ha accedido anteriormente.

ANOMALÍA	PORCENTAJE
Actividad de señalización inusual	58,8 %
Conexión en un puerto sospechoso	22,9 %
Conexión anómala entre dos hosts	8 %
Otras	10,3 %

TABLA 1
CASI EL 60 % DE LAS ANOMALÍAS DETECTADAS EN LAS REDES CORPORATIVAS SON ALGÚN TIPO DE SEÑALIZACIÓN. SIN EMBARGO, PARA DISTINGUIR LAS MALICIOSAS DE LAS BENIGNAS SE NECESITA INTELIGENCIA SOFISTICADA PARA LA DETECCIÓN DE AMENAZAS.

Las 3 principales amenazas de mando y control

En esta clase de evento se incluyen todas las detecciones de red que impliquen un protocolo de comunicación (o terminales) que se pueda identificar como participante en actividad sospechosa con un nivel de precisión suficiente. Como se ve en la tabla 2, más del 60 % del total de eventos tiene relación con una aplicación comercial de «control remoto» que suelen usar los atacantes. Esto se vio en la primera mitad de 2020, por ejemplo, en algunas campañas que tenían como tema el COVID-19 y en las que se utilizaban macros de Excel XL4. El segundo puesto lo ocupa una herramienta de prueba de lápiz/ataque que también usan a menudo los atacantes sofisticados (TA505). En el último puesto están los terminales que se conectan con servidores de mando y control para descargar cargas útiles adicionales.

AMENAZA	PORCENTAJE
Aplicación comercial de control remoto	65,2 %
Herramienta de prueba de lápiz/ataque	15,3 %
Terminales que se conectan con servidores de mando y control	9,1 %
Otras	10,4 %

TABLA 2
MUCHAS HERRAMIENTAS DE SEGURIDAD SON UTILIZADAS TANTO POR LOS ATACANTES COMO POR LOS USUARIOS LEGÍTIMOS. POR LO TANTO, PARA EVALUAR SUS EFECTOS EN LA RED DE UNA ORGANIZACIÓN, ES NECESARIO ENTENDER EL CONTEXTO DE ESTAS DETECCIONES.

Las 3 principales clases de amenazas conocidas

En la tabla 3 se enumeran otras clase de amenazas, aparte de las de «mando y control» que se detectan mediante firmas no probabilísticas o detectores que no utilizan el aprendizaje automático. Las tres principales clases son infracciones de algún tipo: malas prácticas de seguridad, infracciones de políticas y actividad de minería de criptomonedas. Las demás clases de amenazas, incluidas en «Otras», están por debajo del umbral del 10 %.

Los ataques de minería de criptomonedas pueden agotar los recursos de la red. Afectan a servidores o escritorios y pueden tener efectos negativos en la productividad y los costes de la nube de una organización. En una red corporativa, los eventos asociados a actividad de minería de criptomonedas pueden representar un 25 % de las amenazas totales.

CLASE DE AMENAZA	PORCENTAJE
Minería de criptomonedas	24,8 %
Mala práctica de seguridad	20,2 %
Infracción de políticas	17,8 %
Otras	37,2 %

TABLA 3
CLASES DE AMENAZAS CONOCIDAS.

Las 3 principales amenazas de malas prácticas de seguridad

Las malas prácticas de seguridad más comunes tienen que ver con la ausencia de un cifrado adecuado (vea la tabla 4). La más frecuente es la adopción de servidores y clientes de correo electrónico confiando en la transmisión de contraseñas de texto sin cifrar, seguida por el mismo tipo de problema con FTP. La autenticación básica de HTTP, un tipo de autenticación de HTTP que utiliza contraseñas de texto sin cifrar, ocupa el tercer puesto entre las malas prácticas de seguridad.

La solución más sencilla consiste en eliminar el uso de todas las credenciales de texto sin cifrar.

.

AMENAZA	PORCENTAJE
Transmisión de contraseñas de texto sin cifrar a través de POP3/SMTP	49,3 %
Transmisión de contraseñas de texto sin cifrar a través de FTP	20,6 %
Autenticación básica de HTTP	15,7 %
Otras	14,4 %

TABLA 4
LOS SERVICIOS DE SU RED, ¿SIGUEN PRÁCTICAS RECOMENDADAS? EL 90 % DE LOS EVENTOS ASOCIADOS A MALAS PRÁCTICAS TIENEN RELACIÓN CON EL USO DE CREDENCIALES DE TEXTO SIN CIFRAR.

Las 3 principales amenazas de infracciones de políticas

Las infracciones de políticas más frecuentes tienen relación con el uso del protocolo BitTorrent, que se usa sobre todo para compartir archivos, en una empresa o con la carga de clientes de juegos. La tercera infracción de políticas (DNS mediante HTTPS) puede ser un efecto secundario de activar esta función de forma predeterminada en los navegadores web en las empresas. Muchas de las demás infracciones de políticas, que están en la categoría «Otras» de la tabla 5, tienen relación con el tráfico de las VPN, que se usa a menudo para eludir los cortafuegos corporativos y acceder a datos confidenciales.

Estas infracciones de políticas pueden dar lugar a actividad maliciosa, suelen afectar a la productividad y pueden generar infracciones de los derechos de autor.

AMENAZA	PORCENTAJE
Cliente de juegos	35,4 %
uTorrent	26,9 %
DNS mediante HTTPS	13,6 %
Otras	24,1 %

TABLA 5
LAS INFRACCIONES DE POLÍTICAS DE RED PUEDEN GENERAR CIENTOS DE MILES DE EVENTOS EN LA RED CORPORATIVA. LAS DE BITTORRENT Y DE CLIENTE DE JUEGOS PUEDEN REPRESENTAR MÁS DEL 50 % DE LAS INFRACCIONES DE POLÍTICAS EN LAS REDES CORPORATIVAS.

Las 3 principales técnicas de desplazamiento lateral

Aunque no tiene relación con ninguna amenaza ni clase de amenaza concreta, a continuación se muestra el análisis de todos los eventos de red que utilizan una de las tácticas de MITRE ATT&CK® más dañinas en el contexto de la seguridad de red, TA0008: Desplazamiento lateral. Como se muestra en la tabla 6, si bien se determinó que la mayoría de los eventos de red utilizaron RDP para iniciar sesión en otros hosts posiblemente con credenciales robadas, más del 10 % de las detecciones tenían relación con el ataque «Pass the Hash», una técnica utilizada para sortear los mecanismos de autenticación estándar que exigen una contraseña de texto sin cifrar confiando en credenciales robadas (se suelen obtener accediendo directamente a la memoria del sistema). Llama la atención que la vulneración de servicios remotos mediante el ataque ETERNALBLUE u otros ataques basados en SMB está al final de la lista con un 2 %.

AMENAZA	PORCENTAJE
T1076: Protocolo de escritorio remoto	76,5 %
T1075: Ataque «Pass the Hash»	12,7 %
T1210: Ataques a los servicios remotos	2 %
Otras	8,8 %

TABLA 6
EXISTEN VARIAS FORMAS DE DESPLAZARSE LATERALMENTE, PERO LA TÉCNICA MÁS HABITUAL SIGUE SIENDO EL INICIO DE SESIÓN EN HOSTS A TRAVÉS DE RDP UTILIZANDO CUENTAS VÁLIDAS O CREDENCIALES OBTENIDAS POR LA FUERZA.

Responda a las amenazas de evasión de la seguridad con las soluciones de VMware

Los comportamientos de estas amenazas pueden resumirse así.

NSX SERVICE-DEFINED FIREWALL CON ADVANCED THREAT PREVENTION (ATP) DE VMWARE PUEDE IMPEDIR EL ACCESO INICIAL MEDIANTE LA DETECCIÓN DE ELEMENTOS Y ENLACES MALICIOSOS QUE TRATAN DE ENGAÑAR A LOS USUARIOS. LAS FUNCIONES DE NIVEL EMPRESARIAL DE VMWARE PARA ANALIZAR ARCHIVOS UTILIZAN DEEP CONTENT INSPECTION PARA DETECTAR LAS AMENAZAS AVANZADAS QUE PERSISTEN, AUMENTAN SUS PROPIOS PRIVILEGIOS Y ELUDEN LA DETECCIÓN. EL ANÁLISIS DEL TRÁFICO DE RED UTILIZA CONOCIMIENTOS PROFUNDOS SOBRE LOS COMPORTAMIENTOS MALICIOSOS PARA DISTINGUIR LAS ANOMALÍAS BENIGNAS DEL DESPLAZAMIENTO LATERAL MALICIOSO, LAS DETECCIONES DE CUENTAS Y LAS TÉCNICAS DE FUERZA BRUTA. EL ANÁLISIS DEL TRÁFICO DE RED Y EL IDS O IPS FUNCIONAN CONJUNTAMENTE CON EL FIN DE DETECTAR LOS PROTOCOLOS UTILIZADOS PARA COMUNICARSE Y EXFILTRAR DATOS, Y ACTUAR COMO CORRESPONDA.

En lugar de solo tratar de detener lo inevitable con dispositivos de hardware físicos en el perímetro, los equipos de seguridad de las empresas deben centrarse también en impedir el desplazamiento lateral una vez que los atacantes cometen la vulneración inicial. Para ello es necesario cambiar radicalmente el enfoque de la seguridad mediante operaciones de seguridad este-oeste según las necesidades.

VMware NSX Advanced Threat Prevention (ATP) para *NSX Service-defined Firewall* (SDFW) proporciona el más amplio conjunto de funciones para la detección de amenazas con un IDS o IPS y el análisis del tráfico de red basado en el comportamiento. Incluye también *VMware NSX Advanced Threat Analyzer*™, un producto de entorno de pruebas basado en una tecnología de simulación de sistemas completos que ofrece visibilidad de todas las acciones de los programas maliciosos. VMware NSX se ha diseñado específicamente para proteger el tráfico del centro de datos mediante la información más precisa del sector sobre amenazas avanzadas.

- El análisis del tráfico de red aplica aprendizaje automático sin supervisión al tráfico de red para detectar anomalías de protocolos y de tráfico. También utiliza aprendizaje automático supervisado para crear automáticamente clasificadores que reconozcan los comportamientos de red maliciosos y programas maliciosos desconocidos.
- NSX utiliza la IA con las muestras de comportamientos y programas maliciosos que recopilan los sensores en toda la red global de inteligencia para la detección de amenazas de NSX para crear y aplicar automáticamente nuevas firmas de IDS o IPS en todos los sensores de NSX a nivel de dispositivo.
- El producto patentado NSX Advanced Threat Analyzer analiza todos los comportamientos integrados en un archivo o una dirección URL para determinar sin son maliciosos. NSX Advanced Threat Analyzer detecta todas las instrucciones que ejecuta un programa, así como todo el contenido de la memoria y toda la actividad del sistema operativo.

Conclusión

Está claro que hay atacantes que eluden el perímetro. El análisis indica que los atacantes usan técnicas de evasión avanzadas para eludir los controles de seguridad y, una vez dentro de la red, pueden desplazarse y pasar desapercibidos hasta lograr su objetivo, ya sea este robar información o causar daños. Los equipos de seguridad de las empresas necesitan un nuevo método de protección de usuarios, aplicaciones, datos y sistemas mediante operaciones de seguridad este-oeste según las necesidades.

Las soluciones de seguridad de VMware NSX proporcionan la visibilidad que se necesita para detectar amenazas en la red y los mecanismos para detener su propagación y limitar sus daños. Como parte integrante de la arquitectura de confianza cero de VMware, *NSX SDFW* con funciones de *protección contra amenazas avanzada* junto con la visibilidad y detección en el host que proporciona *VMware Carbon Black EDR* representan una opción única para implementar una solución de seguridad exhaustiva con visibilidad y controles de aplicación detallada para hacer frente a las amenazas que eluden el perímetro.

Otros análisis de amenazas detallados

VMware Threat Analysis Unit (TAU) ha llevado a cabo varios análisis de amenazas detallados. Los resultados de análisis siguientes se han hecho públicos en entradas de blog y presentaciones en conferencias.

Cómo controlar las vulnerabilidades de la cadena de suministro con una arquitectura de confianza cero
A la luz de la vulneración de SolarWinds, este análisis ayuda a los clientes que puedan tener preguntas sobre cómo una arquitectura de confianza cero (ZTA) puede ser un enfoque eficaz para limitar las consecuencias de los ataques de este tipo.

Conocer bien la vulneración de SolarWinds y sus repercusiones es un trabajo en curso. Se irá obteniendo más información con el análisis de los elementos y la telemetría.

Para obtener más información, puede consultar «Replantéese su situación de seguridad a raíz de la vulneración de los sistemas de SolarWinds» (*https://www.vmware.com/es/security/solarwinds-breach.html?src=WWW_US_HPHA_SolarWindsBreach_SiteLink*).

Evolución del uso de las macros de Microsoft Excel 4.0 como armas
VMware TAU ha observado varias olas de ataques en los que se usaban macros de XL4 para poner a los hosts en peligro. Estas macros son cada vez más populares entre los atacantes mientras los proveedores de seguridad se esfuerzan por detectarlos adecuadamente.

Esta técnica utiliza de forma indebida una función legítima de Microsoft Excel y no depende de ninguna vulnerabilidad ni ningún ataque. Bloquear estos archivos no es una solución viable en muchas empresas. Las firmas para identificar estas muestras deben ser muy precisas y no activarse en los archivos que utilizan la función de forma legítima.

Esta función lleva 30 años disponible, pero los atacantes no la han descubierto y explotado masivamente hasta el año 2020. Por lo tanto, muchos proveedores de seguridad no tienen en la actualidad mecanismos de detección que se activen en estas muestras. Crear firmas fiables para este tipo de ataque no es tarea fácil. Tras supervisar y seguir esta técnica durante seis meses, el análisis indica que hay miles de muestras que la utilizan. Interceptar esas muestras ha proporcionado datos muy útiles para elaborar estadísticas, identificar tendencias, encontrar valores atípicos y hacer el seguimiento de campañas. De esta forma, las muestras se pueden agrupar en distintas olas, que muestran claramente la evolución de esta técnica en el tiempo y cómo se ha hecho más sofisticada y elusiva.

Puesto que las macros de XL4 son en cierta medida un «territorio inexplorado», los autores de programas maliciosos introducen nuevos engaños periódicamente, que amplían el alcance de esta técnica, y buscan formas de eludir la detección y de hacer que su código sea ininteligible. Estos atacantes recurren a técnicas para eludir los análisis de entorno de pruebas automatizados y la detección basada en firmas, así como los análisis prácticos que llevan a cabo los analistas de programas maliciosos y los profesionales de ingeniería inversa. Como ya se ha mencionado, estas técnicas parecen surgir en oleadas y en cada fase se introducen engaños nuevos basados en la ola o el clúster anterior. Las distintas olas y clústeres se describen detalladamente en una serie de entradas de blog, en las que se desglosa cada nueva técnica detectada y se explica su importancia.

Los resultados de esta investigación se presentaron en la conferencia Virus Bulletin (VB2020) en octubre de 2020.

Puede consultar la entrada de blog original en este enlace: *https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/*.

Puede consultar una entrada de blog al respecto en este otro enlace: *https://blogs.vmware.com/networkvirtualization/2020/10/evolution-of-excel-4-0-macro-weaponization-continued.html/*

El engaño de una amenaza: El programa de secuestro Ryuk Ransomware ataca al sector sanitario

En octubre de 2020, la agencia estadounidense de ciberseguridad y seguridad de infraestructuras (CISA) publicó una advertencia sobre posibles ataques de programas de secuestro contra el sector sanitario. Este informe causó preocupación porque los recursos de los hospitales y otros centros sanitarios se encontraban colapsados como consecuencia de la pandemia. Por lo tanto, un ataque de programas de secuestro, además de dañar la infraestructura de los proveedores de servicios de salud, podría poner en peligro las vidas de los pacientes.

La advertencia describe minuciosamente las tácticas, las técnicas y los procedimientos utilizados por los atacantes. El ataque utiliza varios componentes de programa malicioso, como TrickBot, BazarLoader, Ryuk y Cobalt Strike, para vulnerar las redes, crear cabezas de puente y, posteriormente, desplazarse lateralmente. De esta forma, finalmente se puede llevar a cabo con éxito un ataque de programa de secuestro.

El programa de secuestro Ryuk adopta un enfoque selectivo y se dirige a empresas, hospitales y organismos de la administración pública concretos para solicitarles un rescate altísimo si quieren recuperar sus datos. Ryuk usa AES-256 como algoritmo de cifrado simétrico y RSA 4096 como algoritmo asimétrico. En casi todos los casos, los pasos iniciales son ataques de ingeniería social que engañan a los usuarios para que descarguen y ejecuten aplicaciones de descarga (TrickBot y BazarLoader) que, a su vez, descargan el programa de secuestro (Ryuk).

Se analizaron en profundidad tanto los distintos componentes del programa malicioso como el rastro asociado a sus acciones que quedó en la red. Los resultados muestran una estructura de ataque formada por aplicaciones de descarga que utilizan una larga cadena de ejecución con distintos elementos, como archivos DLL y scripts de PowerShell para distribuir la carga útil del programa de secuestro.

Puede consultar más información sobre esta amenaza en esta entrada de blog: *https://blogs.vmware.com/networkvirtualization/2020/11/ryuk-ransomware-targets-health-care-industry.html/*

Ciberamenazas y actualizaciones de programas maliciosos en torno a la COVID-19

VMware TAU abordó los ataques en relación con la COVID-19 en dos análisis distintos. En los dos casos, el análisis muestra ataques de ingeniería social que sacaba partido al estado de ansiedad creado por la pandemia.

Sin lugar a dudas, los atacantes han estado muy activos durante esta pandemia mundial. Sin embargo, la investigación inicial realizada en mayo [5] indicó que su forma de operar no es novedosa: utilizan archivos adjuntos de correo electrónico como método de infección inicial para, finalmente, distribuir programas espía o de interceptación de información. Los atacantes utilizan archivos de almacenamiento con frecuencia porque ofrecen una capa de protección ligera contra soluciones de seguridad heredadas o neutralizadas incapaces de extraer formatos de almacenamiento no muy utilizados y procesar su contenido correctamente.

La mayoría de los programas de interceptación de información siguen un modelo de «programa malicioso como servicio» y se venden a precios muy asequibles en mercados clandestinos. Como consecuencia, el principal factor diferenciador de las distintas campañas acaba siendo la configuración del programa malicioso en lugar del código en sí. Lo que cambia constantemente con el tiempo es el empaquetador encargado de que el programa malicioso pase desapercibido durante el mayor tiempo posible. Las últimas iteraciones han estado distribuyendo cargas útiles descargadas desde plataformas de hosts públicos, como el servicio de almacenamiento en línea de Google Drive™ o Microsoft OneDrive, con lo que el tráfico de red resultante es difícil de identificar y bloquear.

Si se comparan con los ataques centrados en programas de interceptación de información registrados en mayo [5], las amenazas de los meses siguientes han sido más sofisticadas, como el troyano de acceso remoto modular NanoCore y la tristemente famosa Emotet [6]. En la campaña en torno a la COVID-19 de Emotet, la banda Emotet utilizó los metadatos de descripción de un objeto de formulario para ocultar una cadena de scripts de PowerShell maliciosa. La cadena de infección general es parecida a la de otras campañas de Emotet conocidas [3], pero el análisis muestra también algunos trucos distintos en esta variante, como el uso indebido de un control de marco en lugar de un objeto de varias páginas para almacenar la cadena de scripts de PowerShell, y el uso del cmdlet Invoke-Item para ejecutar la carga útil de Emotet en lugar de llamar al método de creación de la clase win32_process.

Mientras dure la pandemia, cabe esperar que los atacantes, incluida la banda Emotet, siga explotando el tema de la COVID-19 y modificando sus tácticas, técnicas y procedimientos para lanzar nuevos ataques.

Puede consultar más información en esta entrada de blog: *https://blogs.vmware.com/networkvirtualization/2020/11/covid-19-cyberthreat-and-malware-updates.html/*

Esa entrada de blog es la continuación de un análisis anterior, que puede consultar en este enlace: *https://www.lastline.com/labsblog/infostealers-weaponizing-covid-19/*

Venza a los ataques de Emotet con protección contra programas maliciosos basada en el comportamiento

La comunidad de la seguridad disfrutó de unos meses de silencio de Emotet, una amenaza avanzada y evasiva que se inició en febrero de 2020. Este silencio se rompió cuando VMware TAU observó una nueva e importante campaña de Emotet. Lo que llamó la atención de VMware TAU fue que, en su conjunto, la comunidad de la seguridad sigue sin tener capacidad para detectar y evitar Emotet eficazmente, aunque hizo su primera aparición ya en 2014.

En los ataques que se describen en este documento, Emotet utilizó con éxito varias técnicas para maximizar su índice de infección. Como es habitual en los ataques de Emotet típicos, el proceso de infección empieza con una campaña de correo no deseado que consta de mensajes de suplantación de identidad con documentos de Word adjuntos que se utilizan como armas. Nuestros hallazgos muestran que las técnicas de evasión utilizadas en los ataques, como macros de VBA ininteligibles y el uso de controles de formulario como la descripción de varias páginas para ocultar un script de PowerShell malicioso, han sido muy eficaces a la hora de eludir la detección basada en firmas. Esto representa grandes desafíos para los controles de seguridad tradicionales que dependen en gran medida de las firmas para detectar amenazas. Por su parte, enfoques basados en el comportamiento como la solución de entorno de pruebas de nueva generación con IA de VMware demuestran ser muy eficaces para detener ataques del tipo de los que utilizan las técnicas mencionadas.

Puede consultar la información detallada de esta investigación en este enlace: *https://blogs.vmware.com/networkvirtualization/2020/11/defeat-emotet-attacks-with-behavior-based-malware-protection.html/*

VelvetSweatshop: Las contraseñas predeterminadas todavía pueden marcar la diferencia

Durante los meses de octubre y noviembre de 2020, VMware TAU observó un pico en la detección de archivos de Excel cifrados. En general, los documentos de Office se pueden proteger mediante contraseña utilizando un mecanismo de cifrado de claves simétricas con una contraseña que es la clave para cifrar y descifrar el archivo

Los autores de programas maliciosos utilizan esta clave como técnica de evasión adicional para que los motores de análisis de antivirus no detecten el código malicioso. El problema radica en el inconveniente de que un archivo cifrado precisa que la posible víctima introduzca una contraseña (esta se suele incluir en el correo electrónico no deseado o de suplantación de identidad al que se adjunta el archivo cifrado). Esto hace que el correo electrónico y el archivo adjunto sean muy sospechosos y, en consecuencia, es menos probable que la víctima objetivo abra el archivo adjunto malicioso cifrado.

Sin embargo, los atacantes están usando una función de Excel poco conocida que descifra automáticamente una hoja de cálculo cifrada sin solicitar la contraseña si la contraseña de cifrado es VelvetSweatShop, que es la clave de descifrado predeterminada almacenada en el código de programa de Excel. Es un buen truco que los atacantes pueden utilizar para cifrar archivos de Excel maliciosos y así eludir los sistemas de detección de análisis estáticos, a la vez eliminan la necesidad de que la posible víctima introduzca una contraseña.

La clave de descifrado integrada de Excel no es ningún secreto, es muy conocida desde hace años. Con todo, ver que se sigue usando mucho y activamente nos hizo dudar de la eficacia de los motores de análisis de antivirus modernos a la hora de detectar archivos de Excel maliciosos cifrados.

Se realizaron varias pruebas para determinar cómo cambia la eficacia de los motores de análisis antivirus existentes cuando los archivos de Excel se cifran, cuando se elimina el cifrado y cuando se usa otro nivel de cifrado. Los resultados fueron un tanto sorprendentes. A pesar de que el uso de la clave predeterminada es una técnica de evasión conocida, sigue siendo muy efectiva, sobre todo cuando se usa el cifrado AES-256.

Puede consultar la información detallada del análisis en esta entrada de blog: *https://blogs.vmware.com/networkvirtualization/2020/11/velvetsweatshop-when-default-passwords-can-still-make-a-difference.html/*

Programa de secuestro Snake dirigido

Durante el mes de junio de 2020, VMware TAU detectó un programa malicioso sofisticado y específico de la familia de programas de secuestro Snake. El programa malicioso está escrito en lenguaje Go y es muy ininteligible. Las cadenas codificadas de forma rígida están cifradas, el código fuente es ininteligible y el programa de secuestro trata de detener los antivirus, las herramientas de seguridad de terminales, y los componentes de supervisión y correlación.

El programa de secuestro Snake se distribuye mediante una campaña centrada y específica dirigida exclusivamente a las redes empresariales. Esta familia de programas de secuestro está vinculada a Irán e históricamente ha atacado infraestructuras esenciales, como los sistemas SCADA e ICS. Más recientemente, el programa malicioso se ha dirigido contra organizaciones del sector sanitario.

El programa de secuestro de este análisis se dirigió concretamente contra la red corporativa de un fabricante de automóviles japonés. El programa de secuestro parece tener los servidores como objetivos principales, porque tiene lógica para comprobar el tipo de host que va a infectar, y trata de detener muchos servicios y procesos específicos de los servidores.

Puede consultar la información detallada del análisis en este informe: *https://blogs.vmware.com/networkvirtualization/files/2020/11/Targeted-Snake- Ransomware.pdf*

El programa BitRansomware de la botnet Phorpiex ataca a universidades de Asia y el Pacífico

BitRansomware (también denominado DCryptSoft o Readme) apareció en julio de 2020 y es, como su nombre indica, un programa de secuestro. Inicialmente se dirigía a usuarios de habla inglesa, pero recientemente ha atacado en la región de Asia y el Pacífico, centrándose sobre todo en universidades de Japón y Hong Kong.

Al igual que el ataque del programa de secuestro Nemty que se conoció el año pasado [7], el ataque de BitRansomware se distribuyó a través de una masiva campaña de correo electrónico llevada a cabo por la botnet Phorpiex. La campaña de correo no deseado malicioso distribuía gran cantidad de archivos comprimidos ZIP que contenían programas de descarga de secuestro en ejecutables maliciosos.

Como muestra el análisis, el atacante utilizó diversas técnicas para maximizar el índice de infección del ataque. El ataque empezaba con una campaña de correo no deseado y, si se activaba el archivo adjunto, descargaba y mostraba una imagen en la pantalla de la víctima a la vez que descargaba también la variante de Phorpiex desde uno de sus hosts de mando y control. Una vez que se ejecutaba, la carga útil de Phorpiex introducía la copia de BitRansomware definitiva que obtenía de un servidor de mando y control.

Puede consultar la información detallada del análisis en este informe: *https://blogs.vmware.com/networkvirtualization/threat-intelligence/*

Bibliografía

1. J. Zhang y S. Ortolani, «Phorpiex-Powered BitRansomware Targets APAC Universities», VMware, 10/12/2020. [En línea]. Disponible en: https://blogs.vmware.com/networkvirtualization/2020/12/phorpiex-powered-bitransomware-targets-apac-universities.html/.
2. J. Zhang y S. Ortolani, «VelvetSweatshop: Default Passwords Can Still Make a Difference», VMware, 19-11-2020. [En línea]. Disponible en: https://blogs.vmware.com/networkvirtualization/2020/11/velvetsweatshop-when-default-passwords-can-still-make-a-difference.html/.
3. J. Zhang, «Defeat Emotet Attacks with Behavior-Based Malware Protection», VMware, 5-11-2020. [En línea]. Disponible en: https://blogs.vmware.com/networkvirtualization/2020/11/defeat-emotet-attacks-with-behavior-based-malware-protection.html/.
4. Symantec Security Response, «Living off the Land: Attackers Leverage Legitimate Tools for Malicious Ends», Broadcom, 24-12-2019. [En línea]. Disponible en: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/living-land-legitimate-tools-malicious.
5. S. Sarkar, J. Zhang y S. Ortolani, «InfoStealers Weaponizing COVID-19», Lastline (ahora parte de VMware), 11-5-2020. [En línea]. Disponible en: https://www.lastline.com/labsblog/infostealers-weaponizing-covid-19/.
6. J. Zhang, S. Sarkar y S. Ortolani, «COVID-19 Cyberthreats and Malware Updates», VMware, 9-11-2020. [En línea]. Disponible en: https://blogs.vmware.com/networkvirtualization/2020/11/covid-19-cyberthreat-and-malware-updates.html/.
7. J. Zhang y S. Ortolani, «Nemty Ransomware Scaling UP: APAC Mailboxes Swarmed by Dual Downloaders», Lastline (ahora parte de VMware), 18-2-2020. [En línea]. Disponible en: https://www.lastline.com/labsblog/nemty-ransomware-scaling-up-apac-mailboxes-swarmed-dual-downloaders/.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
C/ Rafael Botí, 26 - 2.ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.es