it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Febrero 2018 - nº 5

Meltdown y Spectre, ¿final o principio?

Sergio Martínez, SonicWall: “Vamos a por el midmarket”

Ojo a las criptodivisas y sus problemas de seguridad

LLega BEC, ¿sabes lo que es?

Seguridad endpoint a debate con los líderes del sector

Gestión de Seguridad Corporativa

Guarda esta revista en tu equipo y ábrela con Adobe Acrobat Reader para aprovechar al máximo sus opciones de interactividad

IT Digital Security
Juan Ramón Melara
juanramon.melara@itdmgroup.es

Miguel Ángel Gómez
miguelangel.gomez@itdmgroup.es

Arancha Asenjo
arancha.asenjo@itdmgroup.es

Bárbara Madariaga
barbara.madariaga@itdmgroup.es

IT Digital Security
Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

Colaboradores
Hilda Gómez, Arantxa Herranz, Reyes Alonso
Diseño revistas digitales
Contracorriente
Diseño proyectos especiales
Eva Herrero
Producción audiovisual
Favorit Comunicación
Fotografía
Ania Lewandowska

Clara del Rey, 36 1º A
28002 Madrid
Tel. 91 601 52 92

Meltdown y Spectre, ¿final o principio?

Estrenábamos el año con la noticia de varios fallos de seguridad masivos que afectan a la mayoría de microprocesadores modernos, tanto de Intel como de AMD o ARM. Las vulnerabilidades, bautizadas como Meltdown y Spectre, han obligado a modificar no sólo los procesadores, sino los sistemas operativos, y abren la puerta a una nueva vía de ataque complicada de predecir.

Meltdown y Spectre, ¿son el principio de un nuevo tipo de ataques? El problema tiene tanto alcance que habrá una mayor concienciación por aplicar seguridad en cada proceso de creación, o por el contrario ¿son el principio de un nuevo tipo de vulnerabilidad localizada en la parte más profunda de un dispositivo? ¿un tipo de vulnerabilidad que no se puede parchear? ¿un tipo de vulnerabilidad que está en el corazón de nuestros sistemas, con acceso a todos nuestros datos más sensibles?

También dedicamos unas páginas a hablar de la seguridad de las criptomonedas y un nuevo tipo de malware que cada vez se hace más popular, el cryptojacking, cuyo objetivo es el robo de recursos de computación para minar criptomonedas sin permiso.

Hemos hablado con Sergio Martínez, el nuevo responsable de SonicWall, un fabricante que ha pasado por momentos complicados en los últimos años, que ha recuperado su capacidad de innovación, y que ahora se ha propuesto conquistar el midmarket.

El desayuno de este mes se ha dedicado a la Seguridad Endpoint y hemos tenido la suerte de contar con la flor y nata de los proveedores de soluciones para este mercado. Empresas como Kaspersky, Trend Micro, ESET, Symantec, Panda Security o Stormshield han desgranado la problemática que afecta a esta área, qué funcionalidades debe tener una solución de seguridad endpoint, si el antivirus ha muerto o qué papel juega el machine learning en la seguridad de punto final. ¡No te lo pierdas!

Insertado en el este número incluimos un especial desarrollado en colaboración con GMV y centrado en la Gestión de la Seguridad Corporativa en momentos de Transformación.

Las redes WiFi, que este año estrenarán un nuevo protocolo de seguridad, y los ataques BEC, que llegan a generar más ingresos que el ransomware, son las otras temáticas a las que hemos dedicado un espacio en ese nuevo número.

¿Te interesa la seguridad? Entonces seguro que te gusta este número de IT Digital Security.

Actualidad

No solo IT

Nuevo paradigma en la Confianza

Índice de anunciantes

Kaspersky
Panda Security
Trend Micro
Symantec
GMV
Stormshield
ESET
IT Webinars
Quest
IT Whitepapers

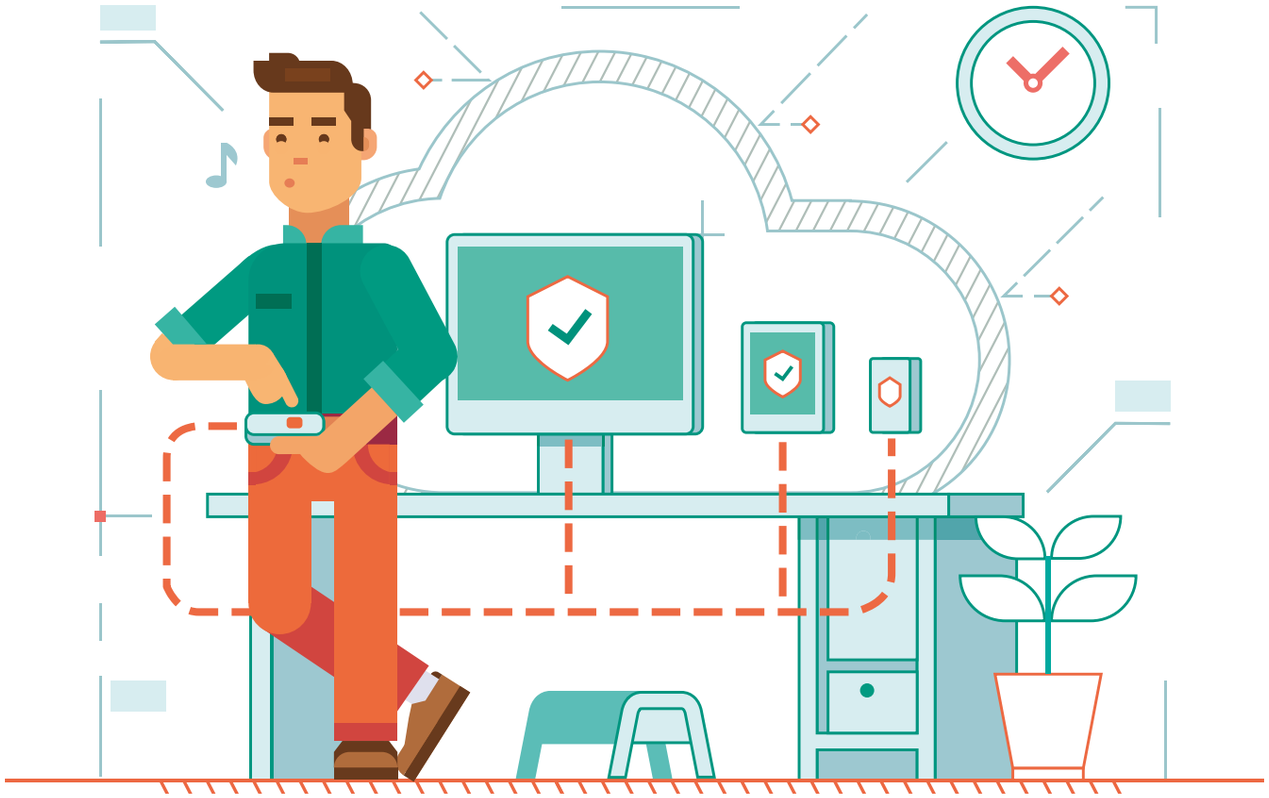
Desayunos ITDS

La Seguridad Endpoint a Debate con los líderes del sector

Especial GMV

Gestión de Seguridad Corporativa en momentos de Transformación

¿Te avisamos del próximo IT Digital Security?



Deje que fluya su creatividad. Y aleje las ciberamenazas

Kaspersky Endpoint Security Cloud.
La seguridad que necesita con la flexibilidad que desea

El 40 % de las empresas afirma que el aumento de la complejidad de su infraestructura está llevando sus presupuestos al límite. Kaspersky Endpoint Security Cloud ayuda a las pequeñas y medianas empresas a simplificar la gestión de la seguridad, sin tener que invertir en recursos o hardware adicional. Gestione la seguridad de endpoints, dispositivos móviles y servidores de archivos Mac y Windows de forma remota, desde cualquier lugar, con nuestra consola basada en la nube.

cloud.kaspersky.com

© 2017 Kaspersky Lab Iberia, España. Todos los derechos reservados. Las marcas registradas y logos son propiedad de sus respectivos dueños.

Por fin WiFi más seguras

Las redes WiFi van a ser, a partir de ahora, un poquito más seguras. La seguridad de las redes inalámbricas siempre ha estado en entredicho, y con razón, porque no es extremadamente complicado interceptar el tráfico de estas redes para conseguir información como contraseñas o datos de tarjetas de crédito. También existen programas gratuitos y extremadamente fáciles de utilizar con los que se puede acceder a la red inalámbrica del vecino; sólo hace falta tiempo para saber buscarlos.

Existe un organismo, la Wi-Fi Alliance, compuesta por decenas de empresas que buscan impulsar la adopción y evolución de las redes WiFi, que ya transportan más de la mitad del tráfico de Internet.

Esta alianza no sólo trabaja en especificaciones que sea cada vez más fáciles de desplegar y tengan mayor capacidad y mayor alcance, sino en la seguridad de las mismas. Estas especificaciones, o estándares son conocidos como 802.11, que son los referidos a las redes inalámbricas de área local

Y del mismo modo que con el correr de los años se ha pasado de los estándares WiFi a/b/g a WiFi n y, últimamente, a WiFi ac, el protocolo de seguridad ha ido avanzando, anunciándose recientemente WP3, el nuevo estándar de seguridad para redes inalámbricas.

Existen diferentes alternativas que permiten garantizar la seguridad de las rede WiFi. Lo más habitual es la utilización de protocolos de cifrado, como el WEP, el WPA o WPA2, que se encargan de cifrar la información transmitida. En el caso de WEP, utiliza un cifrado de 64bit o 128bit, pero no está recomendado porque a consecuencia de la cantidad de vulnerabilidades que presenta, es relativamente fácil para un hacker conseguir las claves de cifrado.

Las mejoras llegaron con WPA, que incluía la generación dinámica de claves de acceso. WPA2, o Wi-Fi Protected Access 2, fue ratificado en 2004, tres años después de que el protocolo anterior, WEP, fuera crackeado y, como consecuencia, demasiado inseguro para seguir utilizándolo. WPA2 es el protocolo que se está utilizando actualmente y al que le seguirá, a lo largo de este año, WPA3.

La llegada de WP3 no significa el final para el protocolo anterior. Wi-Fi Alliance continuará realizando mejoras en WP2 que aseguren una protección adecuada a los usuarios de redes inalámbricas mientras evoluciona el panorama de la seguridad. De hecho, según la organización, las aplicaciones de Wi-Fi avanzadas se basarán en WPA2 con marcos de administración protegida y las nuevas mejoras reducirán el potencial de vulnerabilidades como consecuencia de una mala configuración de

WPA2 es el protocolo de seguridad para redes WiFi que se está utilizando actualmente y al que le seguirá, a lo largo de este año, WPA3

la red, al tiempo que protegerán aún más las redes administradas con servicios de autenticación centralizados.

WiFi más segura

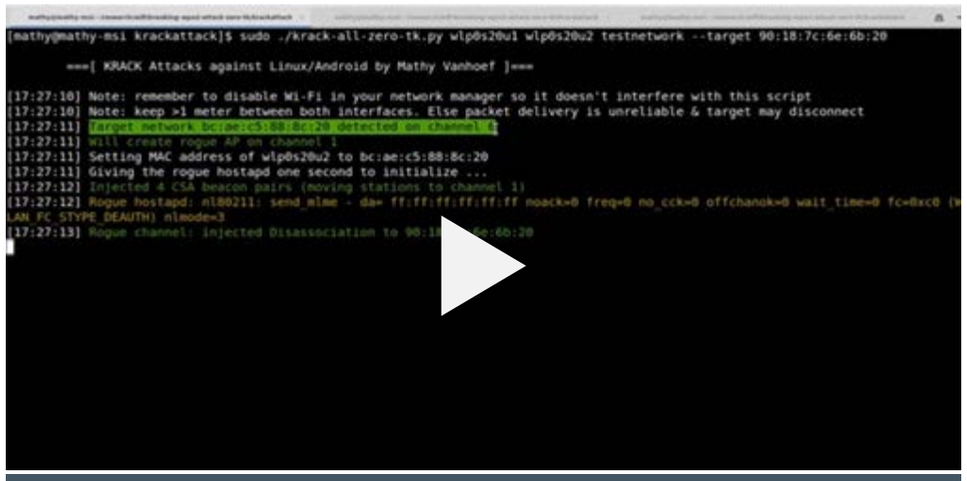
Aunque quizá lo más destacado sea la llegada de un nuevo protocolo de seguridad, la Wi-Fi Alliance anunció varias nuevas características para Wi-Fi Protected Access, que es la familia de tecnologías de seguridad Wi-Fi Certified desde hace más de una década, incluidas mejoras en la configuración, autenticación y cifrado que permiten que todos los dispositivos WiFi Certified continúen mejorando las protecciones de seguridad.

Como parte de WPA3 se esperan cuatro nuevas capacidades que se aplicarán tanto a redes Wi-Fi empresariales como personales. Dos de ellas ofrecerán protecciones robustas incluso cuando los usuarios eligen contraseñas que no cumplen con las recomendaciones, y simplificarán el proceso de configuración de seguridad para los dispositivos que tienen una interfaz de visualización limitada o nula.

Otra de las nuevas características de seguridad fortalecerá la privacidad del usuario en redes abiertas a través del cifrado de datos individualizado. Finalmente, WPA3 también contará con una suite de seguridad de 192 bits alineada con la Suite del Algoritmo de Seguridad Nacional Comercial (CNSA) que protegerá las redes gubernamentales, de defensa e industriales que tienen mayores requisitos de seguridad.

KRACK compromete WiFi

Si en 2001 el protocolo WEP era hackeado, en octubre de 2017 le llegaba el turno a WP2, lo que sig-



KRACK ATTACKS — CLICAR PARA VER EL VÍDEO

Como parte de WPA3 se esperan cuatro nuevas capacidades que se aplicarán tanto a redes Wi-Fi empresariales como personales

nifica que el protocolo que protege las redes WiFi, y que llegó al mercado en 2004, no es tan seguro desde entonces; sobre todo, y lamentablemente es lo habitual, cuando no se apliquen los parches de seguridad que reparan el fallo.

¿Te avisamos del próximo IT Digital Security?

La culpa la tiene KRACK (Key Reinstallation Attacks), que el nombre que los investigadores Mathy Vanhoef y Frans Piessens pusieron a la vulnerabilidad. Afecta a todos los routers del mundo y a cualquier red WiFi, incluyendo las de la oficina, el hogar o las públicas. A grandes rasgos, lo que hace este fallo es permitir que un ciberatacante se introduzca dentro del radio de la red inalámbrica para, una vez dentro, inyectar virus o apoderarse de contraseñas, números de tarjetas de crédito o fotos enviadas a través de internet. O lo que es lo mismo, interceptar el tráfico de esas redes inalámbricas.

La vulnerabilidad es devastadora porque se encuentra en el propio estándar, no en los dispositivos, lo que significa que cualquier implementación de WPA2 está afectada. Es decir, si tienes un dispositivo que utilice WiFi, está afectado. Además, afecta a todos los sistemas operativos (Android, Windows, iOS, macOS, Linux, OpenBSD, etc), así como al hardware de todos los fabricantes.

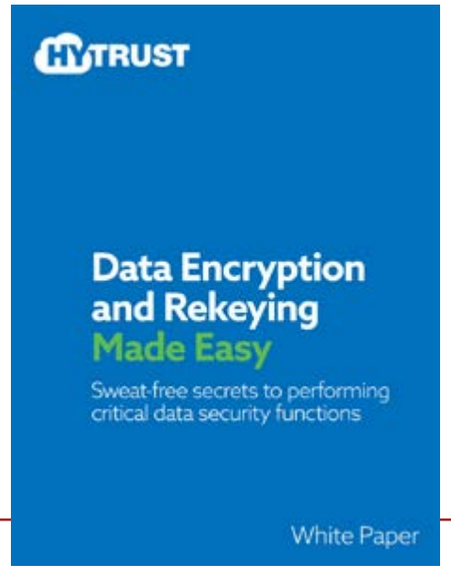
Como ya ocurría con las redes WEP, para realizar el ataque con KRACK es necesario que el ciberdelincuente esté cerca de la red a hackear. La diferencia es el alcance que tienen hoy en día las redes WiFi y que el sustituto de WP2 tarda en llegar, a lo que habrá que añadir el periodo de implementación.

Cómo protegerte de KRACK

Lo que hace KRACK es explotar un defecto en el proceso de handshake de cuatro vías entre el dispositivo de un usuario que intenta conectarse y una

HACIENDO FÁCIL EL CIFRADO Y LA ROTACIÓN DE CLAVES

El cifrado de datos es fundamental para la seguridad de las empresas modernas. Y una buena práctica relacionada con el cifrado es el llamado rekeying, que no es otra cosa que la rotación de las claves de cifrado de forma periódica y que evita, entre otras cosas, reduce el riesgo de que alguien use una clave antigua para acceder a los sistemas.



red Wi-Fi. Lo que ocurre es que lo mejor es seguir utilizando el protocolo WPA2 -y así ha ocurrido desde que se conoció el problema, porque sigue siendo la opción disponible más segura para la mayoría de las redes inalámbricas.

Entre las recomendaciones, comprobar si hay actualizaciones de seguridad para todos aquellos dispositivos susceptibles de conectarse a una red WiFi. Microsoft, por ejemplo, fue de las primeras empresas en parchear el fallo. Apple creó un parche para el exploit aplicable a iOS y MacOS, y también para su Apple Watch y Apple Tv. Aruba tiene un parche disponible para Aruba OS, Aruba Instant, Clarity Engine and other software. Cisco, Fortinet, FreeBSD Project, Intel, Linksys/Belkin, Netgear, OpenBSD, Samsung e incluso WatchGuard son algunas de las empresas que se apresuraron a proteger a sus clientes de KRACK.

Utilizar una VPN, o red privada virtual, es una buena manera de protegerse de KRACK porque cifra todo el tráfico de internet. Tambien hay que tener cuidado con los sites a los que nos conectamos, mejor los que utilicen HTTPS. Aunque no lo impide, y ya que no se puede hackerar lo que no se ve, se recomienda cambiar el nombre de la red y ocultarla, que es una opción que existe en el software de control de los routers.

También podría ser útil aplicar un filtrado MAC, que sigue siendo una de las mejores maneras de conseguir que nadie que no queramos se conecte a nuestro punto de acceso a internet. Cada dispositivo capaz de conectarse a una red (ordenador, tablet, impresora, smartphone, proyector, etc.), tiene una dirección única que se conoce como MAC, o Media Access Control. Y lo que hay que hacer es una lista de direcciones MAC que queremos que se conecten a nuestro router.

Enlaces de interés...

- Todo lo que necesitas saber sobre KRACK
- Key Reinstallation Attacks
- WiFi Alliance

Compartir en RRSS

THE RANSOMWARE X.

Mediante la integración de tecnologías de Machine Learning a sus mecanismos de detección, la solución **Trend Micro™ XGen ™ endpoint security** protege contra el ransomware y garantiza la integridad de sus datos.

El ransomware es sólo una parte del problema. Su vulnerabilidad, representada por la "X", también podría ser un ataque de tipo Zero Day, una amenaza debida al comportamiento de sus usuarios o cualquier actividad que comprometa la integridad de sus datos y de su reputación.

What's your X? Tren Micro™ XGen™ endpoint security es la solución.

#WhatsYourX

TREND MICRO™

trendmicro.es/xgen

Con Sergio Martínez, SonicWall quiere conquistar el midmarket

Rosalía Arroyo

Hace dos años que SonicWall ha tomado carrerilla, que está recuperando el tiempo perdido. A la nueva hornada de productos lanzada el pasado mes de septiembre le sigue otra en marzo de este año. Ransomware y análisis de tráfico cifrado impulsarán el mercado, con Capture convertido en motor de crecimiento de la compañía. Sergio Martínez, nuevo responsable de SonicWall para España y Portugal, llega para liderar el cambio.

Los últimos han sido años complicados para SonicWall. La compañía perdió su independencia a manos de Dell en marzo de 2012, un compromiso que apenas duró cuatro años, y desde hace dos endereza su estrategia bajo la atenta mirada de Francisco Partners y Elliot Management, las firmas de

Compartir en RRSS

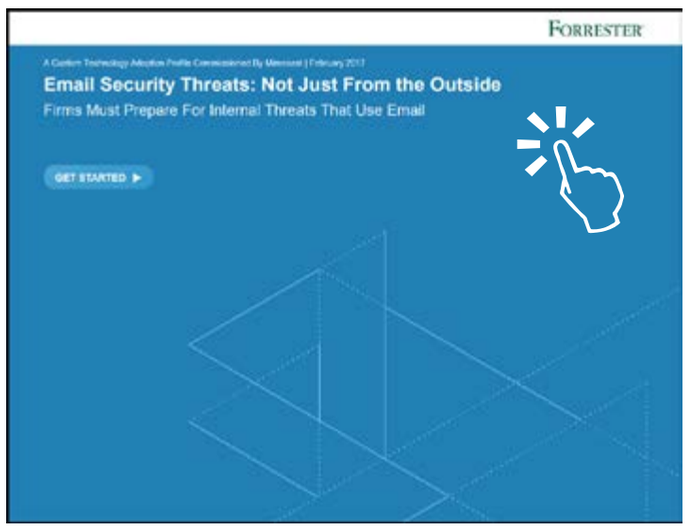
¿Te avisamos del próximo IT Digital Security?

SonicWall Capture será uno de los motores de crecimiento para la compañía este año

it whitepapers

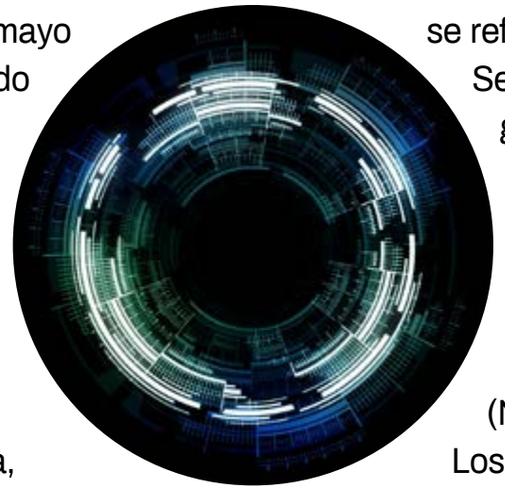
AMENAZAS
DE SEGURIDAD DEL EMAIL,
NO TODO VIENE DE FUERA

El correo electrónico sigue siendo un componente crítico de la actividad empresarial cotidiana y un canal importante a través del cual los empleados interactúan entre sí y con el mundo exterior. No es de extrañar entonces que el correo electrónico también represente una vulnerabilidad de seguridad significativa y constante para muchas empresas. Descubra la perspectiva de Forrester sobre las amenazas internas y cómo las organizaciones están respondiendo y cómo deberían responder.



capital riesgo que le compraron en mayo de 2016, y con las que ha recuperado su capacidad de innovación.

De forma que SonicWall vuelve a ser SonicWall. Atrás quedó el tiempo de Dell Security, de intentar hacerse escuchar en una empresa de talla XXL que empezó a soltar lastre tras la compra de EMC. Se recupera la independencia, la libertad, la capacidad de reacción ante un mercado, el de la seguridad, que cambia rápidamente. "El momento es el correcto para SonicWall", decía Bill Conner, CEO de SonicWall, en un vídeo publicado tras el anuncio de la separación de Dell.



Poco más de un año después de volver a tomar las riendas de su destino, SonicWall lanzaba la que aseguraba que es la mayor renovación tecnológica de la compañía. Lo hacía en septiembre del año pasado, anunciando nuevos productos y soluciones entre los que se incluyen un nuevo SonicOS 6.5 con cerca de 50 nuevas características, el nuevo firewall NSA 2650, nuevos puntos de acceso inalámbricos SonicWave 802.11ac Wave 2, un nuevo SonicWall Cloud Analytics, y la nueva versión de Secure Mobile Access OS 12.1.

El impulso continúa, porque en marzo se lanzarán nuevos productos, se potenciarán los servicios y se reforzará el canal. Nos lo ha contado Sergio Martínez, el nuevo director general de SonicWall para España y Portugal.

El mercado de firewalling se está transformando. Lleva años haciéndolo. Se pasó del firewall, tal cual, al next generation firewall (NGFW), pero eso es lo de menos. Los que nacieron arriba quieren bajar, los que nacieron abajo, quieren subir y los que no estaban, buscan su hueco con alguna adquisición. Así que tenemos a Palo Alto, Check Point, Fortinet, Sophos, Watchguard, Barracuda, Juniper, Cisco y la mismísima SonicWall moviéndose de arriba abajo. Intentando conquistar, por ahora sin demasiado éxito, un terreno mayor que el que por su naturaleza le corresponde.

Y con Sergio Martínez, SonicWall quiere crecer, no sólo en cuanto a negocio, sino en lo que respecta al tipo de empresa a la que se quiere llegar. Según Sergio Martínez el posicionamiento de SonicWall en España, bien asentado en el mundo de la pequeña y mediana empresa, no es el que la compañía tiene en el resto de Europa, "donde estamos posicionados hacia arriba, hacia el mundo enterprise"; quizá no igual que Check Point, reconoce, "pero somos una gran alternativa a Fortinet".

BILL CONNER, CEO OF SONICWALL, HABLA DE FUTURO TRAS LA SEPARACIÓN DE DELL

CLICAR PARA VER EL VÍDEO

Reforzar el canal de distribución es clave

Las claves para conseguirlo están claras: productos y canal, y ya se trabaja en ambos. La renovación de producto está en marcha, se recupera el tiempo a marchas forzadas y tras los últimos lanzamientos, veremos una nueva catarsis en apenas mes y medio -y el tema irá de redes inalámbricas.

También se trabaja con el canal. Tan sólo hay que echar un vistazo a los comunicados de prensa de la compañía de los últimos meses. Recientemente se celebraban las bodas de plata con Ingram Micro; hace unos meses se anunciaba el nuevo programa de servicios habilitados para socios; se firmaba una alianza con SentinelOne para la detección, prevención y remediación de brechas en tiempo real; y tras lanzar el SonicWall SecureFirst Partner Program en noviembre de 2016, se anunciaba el pasado mes de marzo el lanzamiento de dos iniciativas para partnes: SonicWall University y programas de marketing.

Tech Data, Esprinet, Ingram Micro e Ingecom; estos son los cuatro mayoristas de la compañía en España. SonicWall quiere reforzar el canal, pero no se trata tanto de sumar nuevos miembros como de capacitar a los que hay para que vendan a empresas más grandes. “Debemos hacer algún tipo de transformación y disponer de algún partner más preparado para otro tipo de operaciones, como en Europa”, nos cuenta Sergio Martínez.

Europa es el referente; mientras aquí “estamos muy centrados en los TZ, fuera lo que más se vende es la gama alta”. No se plantea la compañía la búsqueda de nuevos mayoristas, pero sí desarrollar este canal y buscar nuevas oportunidades.

Se apuesta por el mundo telco y de MSSP, o servicios de seguridad gestionados. “Se trata de llegar al SMB más a través de los servicios y no tanto de los productos”, explica el máximo responsable de SonicWall España. Es una tendencia mundial que las telco busquen incrementar su facturación mensual vendiendo más servicios -cada vez más sofisticados, porque el mundo de la voz murió y el mundo de los datos está cambiando.

> El pasado mes de septiembre SonicWall lanzaba la que asegura que es la mayor renovación tecnológica de la compañía

Ransomware y SSL

Ransomware y la inspección del tráfico cifrado serán dos motores que impulsarán el negocio de SonicWall este año. Lo dice Sergio Martínez, quien asegura que la lucha contra el ransomware “es uno de los fuertes” de la compañía, cuyos clientes no se vieron afectados ni por Wannacry ni por Petya.

Enlaces de interés...

- SonicWall renueva su oferta
- SonicWall anuncia su desvinculación total de Dell
- Canal de SonicWall en YouTube

Elemento clave para SonicWall es su servicio Capure Advanced Threat Protection (ATP), una sandbox basada en cloud que trabaja con múltiples motores de detección de amenazas y que, anunciado en julio de 2016 ya era capaz de detectar y detener más de 1.000 variantes únicas de malware cada día en octubre del año pasado.

Y sobre el tráfico cifrado, que ya representa el 60% del tráfico de internet mundial, se ha convertido en un gran reto desde el punto de vista de la seguridad. El tráfico cifrado, SSL/TSL, está creciendo porque mejora la privacidad de las comunicaciones y evita el espionaje. La demanda de cifrado se disparó después de destaparse el escándalo de la NSA, el espionaje internacional y masivo llevado a cabo por la Agencia de Seguridad Nacional de Estados Unidos, y otros organismos gubernamentales. Claro que cifrar el tráfico sirve a los ciberdelincuentes para expandir sus creaciones y extraer los datos robados.

Inspeccionar el tráfico cifrado no es un asunto baladí. Por un lado, porque debe hacerse manteniendo la privacidad, y por otro porque la tarea de descifrar, inspeccionar y cifrar puede ralentizar los sistemas y las comunicaciones. A estas alturas la tecnología ha evolucionado y los procesos se han simplificado mucho, pero dado que no se espera que la cantidad de tráfico cifrado vaya a descender, sino todo lo contario, ni que los ciberdelincuentes dejen de explotar una técnica que tan buenos resultados les da, la demanda de soluciones capaces de analizar lo que viaja en ese tráfico cifrado van a crecer.

Sergio Martínez, Director General de SonicWall para España y Portugal

De forma que ya lo ven. SonicWall se ha tomado muy en serio su nueva etapa. Renovación de productos, refuerzo del ecosistema de canal, e incluso incremento de la plantilla, que ha pasado de 1.300 empleados a 1.500 en poco tiempo. SonicWall avanza y en España estrena responsable para la región de Iberia, Sergio Martínez, quien asegura que el nombramiento le ha sentado “muy bien”.

Sergio Martínez Hernández es Ingeniero de Telecomunicación y MBA por el IESE, y ha trabajado en diversas compañías del sector como Techdata, Colt o Telefónica, así como consultoría y diversos startups. Sergio Martínez llega para incrementar su presencia en el canal de distribución y ayudar a los integradores de sistemas y resellers a construir nuevo negocio basado en la seguridad.

NUESTRO RETO

TU CIBERSEGURIDAD

Cada vez somos más conscientes del riesgo al que estamos expuestos. Debemos asumir que tarde o temprano vamos a ser atacados. Por lo tanto, debemos incrementar nuestros esfuerzos para minimizar el impacto de estos ataques en nuestras infraestructuras.

En GMV apostamos por una aproximación proactiva y global, abordando la ciberseguridad en todas sus formas: definiendo una estrategia operativa, protegiendo los activos, adelantándonos al atacante y restableciendo la normalidad ante ciberincidentes.

- GESTIÓN DE VULNERABILIDADES
- GESTIÓN DEL RIESGO
- CONSULTORÍA CIBERSEGURIDAD
- RESPUESTA ANTE INCIDENTES Y ANÁLISIS FORENSE
- CIBERSEGURIDAD EN CAJEROS
- TEST DE INTRUSIÓN Y ANÁLISIS DE SEGURIDAD
- FORMACIÓN Y CONCIENCIACIÓN EN SEGURIDAD
- DISEÑO Y ARQUITECTURA SEGURA
- SERVICIOS GESTIONADOS
- CLOUD SECURITY
- BIG DATA ANTIFRAUDE
- PROTECCIÓN DEL DATO

www.gmv.es marketing.TIC@gmv.com

www.facebook.com/infoGMV

@infoGMV

gmv® INNOVATING SOLUTIONS

LLega BEC, ¿sabes lo que es?

Los ataques BEC, o Business Email Compromise, se han convertido en un negocio multimillonario, superior incluso al que genera ramsonware. Las víctimas pueden ser empresas grandes y pequeñas, de cualquier vertical, y este año generará costes por valor de 9.000 millones de dólares

Hace unos meses el FBI lanzó un comunicado advirtiendo de la peligrosidad de los ataques BEC, o Business Email Compromise. Y también de lo que les está costando a las empresas, nada menos que más de cinco mil millones de dólares.

También conocidos como el Fraude al CEO, este tipo de ataques continuarán creciendo (lo han hecho un 1.300% desde 2015), evolucionando y dirigiéndose contra empresas de todos los tamaños.

Un BEC es un tipo de ataque contra altos directivos que tiene como objetivo secuestrar y controlar cuentas empresariales reales que los ciberdelincuentes pueden utilizar para interceptar o redireccionar las transacciones financieras. A diferencia de los ataques de phishing tradicionales, los BEC son dirigidos, diseñados para cada víctima. La mayoría de las ocasiones los ciberdelincuentes estudian las últimas noticias de las empresas e investigan las redes sociales de los empleados para hacer que el ataque, el señuelo, sea lo más convincente posible. Este nivel de personalización es lo que ayuda a que este tipo de estafas por correo electrónico superen los filtros de spam y otras protecciones.

Además de conseguir grandes sumas de dinero, muchos grupos de cibercriminales utilizan este método de ataque para obtener información confidencial de la empresa llevando a cabo ataques muy sigilosos y extrayendo información sensible que puede acarrear a la organización serios problemas, no solo económicos sino también de reputación.

Se calcula que ataques BEC superen los 9.000 millones de dólares en 2018, según un estudio de Trend Micro. Una cifra que está cerca de duplicar los 5.300 millones de dólares que según el FBI habían costado a las empresas este tipo de ataques hace un año. Decía entonces el FBI que los ataques BEC crecen porque “son relativamente simples”.

Compartir en RRSS

"Es muy importante que los trabajadores sean conscientes de las amenazas existentes y los trucos que utilizan los ciberdelincuentes"

Alfonso Ramírez, Director General de Kaspersky Lab Iberia

¿Por qué son tan peligrosos los ataques BEC?
"Son peligrosos porque utilizan ingeniería social para conseguir su propósito. Son dañinos porque el impacto no sólo es económico, sino que puede tener implicaciones en la situación laboral de las/los implicadas/os y eso, sin duda, es terrible. Además, tienen un enfoque de poner en duda la capacidad corporativa de proteger la infraestructura propia, de enmascararse el ataque utilizando componentes de la entidad que, por supuesto, ponen en jaque la robustez y solidez de las estrategias de protección y defensa. La pérdida de reputación e imagen pública (no sólo externa sino interna) es notable, perdiendo la credibilidad en los sistemas corporativos", asegura Ramsés Gallego, Strategist & Evangelist en la oficina del CTO en Symantec.

Para Eutimio Fernández, Director de ciberseguridad en cisco España, a pesar de la mayor popularidad de los ataques de ransomware, "la amenaza

BEC (Business Email Compromise) es actualmente -según Flashpoint, partner de inteligencia de seguridad de Cisco- el método más lucrativo y rentable para obtener mediante fraude grandes cantidades de dinero de los negocios", y añade el directivo que se trata de un vector de ataque realmente sencillo que se basa en la ingeniería social para llevar a cabo el robo, que es otra de las razones por las que este tipo de ataques se han vuelto extremadamente peligrosos.

Esto es precisamente lo que destaca José Luis Laguna, Director Técnico Fortinet Iberia, al asegura que realizar estafas a través del correo electrónico corporativo "es bastante sencillo y económico para los atacantes". Asegura el directivo que al ser un

"Realizar estafas a través del correo electrónico corporativo es bastante sencillo y económico para los atacantes"

José Luis Laguna, Director Técnico Fortinet Iberia

negocio tan rentable anima a todo tipo de ciberdelincuentes a continuar con su actividad maliciosa, y que en en la mayoría de los casos, "los ataques son tan sofisticados que el engaño se descubre cuando ya es demasiado tarde". Organizaciones de cualquier tamaño son objetivo de un ataque BEC, dice también el CTO de Fortinet Iberia.

Alfonso Ramírez, director general de Kaspersky para España y Portugal, explica sobre los ataques BEC que comienzan con el envío de un correo electrónico de phishing, muy elaborado, que parece llegar del directivo de la empresa y en el que se solicita a un empleado realizar una transferencia o movimiento bancario a una cuenta controlada por los ciberdelincuentes. "Las víctimas también pueden ser empresas que creen recibir un correo electrónico de su cliente. De esta forma, tanto los empleados de la compañía en la que la identidad del CEO ha sido suplantada como la compañía cliente que realiza la transacción, son víctimas de este nuevo fraude".

Tipos de ataques BEC

Una vez que un ciberdelincuente ha accedido al correo electrónico de un ejecutivo, una estafa de BEC usualmente toma una de las cinco formas básicas:

Fraude del CEO. Los ciberdelincuentes envían un email que parece proceder del máximo responsable de la empresa a un empleado que tenga capacidad para realizar transferencias, dándole instrucciones para que envíe fondos a una cuenta que, evidentemente, está bajo el control de los ciberdelincuentes. Es habitual que este tipo de ataques incluyan una nota en la que se advierte que la transferencia es urgente, lo que evita que el empleado tenga tiempo de verificar la orden.

Estafa de factura falsa. El ciberdelincuente bucea en la cuenta de correo de un ejecutivo hasta dar con una factura que venza pronto para después contactar con el departamento financiero y pedirles que cambien la cuenta de pago por una diferente.

Suplantación del Abogado. El ciberdelincuente se hace pasar por el bufete de abogados de una empresa y solicita una transferencia de fondos para resolver un litigio o pagar una factura vencida. Es habitual que el cibercriminal utilice este tipo de ataque para convencer a los destinatarios de que la transferencia es confidencial y sensible al tiempo, por lo que es menos probable que el empleado intente confirmar que debe hacer el envío de dinero.

Compromiso de cuenta. Similar a la estafa de la factura falsa, este tipo de ataque supone que un cibercriminal hackee la cuenta de un empleado para enviar correos a los clientes en los que se les avisa de que hubo un problema con sus pagos y necesitan reenviarlos a una cuenta diferente. Este tipo de ataques son más habituales en empresas pequeñas.

Robo de datos. La única versión de la estafa de BEC cuyo objetivo no es una transferencia de fondos directa, son los ataques que buscan el robo de datos mediante el compromiso de la cuenta de correo electrónico de un ejecutivo para solicitar que se le envíe información confidencial. A menudo estos ataques se utilizan como el punto de partida para un ciberataque más grande y dañino.

"Existen mecanismos que ayudan a garantizar la legitimidad del emisor de los correos electrónicos recibidos y enviados hacia y desde nuestra organización"

José de la Cruz, Director técnico de Trend Micro

Normalmente, los ataques BEC "están relacionados con objetivos económicos (el caso más habitual es solicitar a alguien del departamento financiero una transferencia de dinero muy urgente) y su impacto es muy alto, pues puede suponer no sólo un coste económico alto para la compañía, sino que también afectar a su reputación", añade José de la Cruz, director técnico de Trend Micro.

Lo que, en definitiva, persigue un ataque BEC es el "lucro mediante fraude", dice Eutimio Fernández. Y, al tratarse de un fraude altamente lucrativo, probablemente seguirá creciendo como vector de amenaza, tanto en grandes cuentas como en pequeñas empresas.

Siendo tan peligrosos, ¿por qué no reciben tanta atención como otros tipos de ataques? Para José de la Cruz, hay que destacar que suelen tratarse de ataques dirigidos; "esto supone que el número de ataques sea inferior a cualquier ataque masivo (ej.: ransomware). Asimismo, las empresas afectadas no suelen hacer público el ataque y sus detalles". De la misma opinión es Eutimio Fernández al asegurar que "se trata de un fraude -principalmente basado en ingeniería social- que a ninguna empresa le gusta reconocer, y por tanto no se conoce exactamente su alcance". Para José Luis Laguna, de Fortinet, "posiblemente las organizaciones no estén dando publicidad cuando son atacadas de este modo para que no afecte a su reputación corporativa", lo que hace que este tipo de ataques sea menos conocido.

Ramsés Gallego habla de visibilidad y mecanismos de protección. Siendo tan costosos, ¿por qué los ataques BEC recibe mucha menos atención que otros tipos de ataques? "Por dos motivos fundamentales: no gozan de visibilidad pública y, por ello,

"A pesar de la mayor popularidad de los ataques de ransomware, la amenaza BEC es el método más lucrativo y rentable para obtener mediante fraude grandes cantidades de dinero"

Eutimio Fernández, director de Ciberseguridad en Cisco España

BUSINESS EMAIL COMPROMISE CLICAR PARA VER EL VÍDEO

conocemos muchos menos de lo que realmente ocurren (las estadísticas, en consecuencia, no reflejan la realidad de los muchos que ocurren) y, por otra parte, las compañías no disponen de los mecanismos de detección de ese ataque que requiere de diversos controles/contramedidas para la identificación, detección y bloqueo del ataque".

¿Cómo se producen los ataques BEC?

Para poder llevar a cabo este tipo de ataques los ciberdelincuentes utilizan software malicioso para robar credenciales de correo electrónico, analizan el contenido de los correos electrónicos comprometidos y luego usan la información recopilada para, a través de técnicas de ingeniería social, sustraer el dinero de las víctimas. "Para evitar la detección del malware que utilizan para robar las credenciales, emplean herramientas llamadas Crypters que les permiten ocultar los binarios malware. También utilizan VPN para falsear sus IPs de origen y parecer que se encuentran en la red del cliente", explica el director técnico de Fortinet.

Ramsés Gallego, de Symantec, habla de ataque híbrido y asegura que tras conseguir las credenciales de acceso al correo corporativo, a la agenda de direcciones, a la estructura de los correos internos, es relativamente sencillo enviar un mensaje con la apariencia de una/un ejecutiva/o hacia alguien en su departamento "para realizar una transacción financiera 'que no se puede realizar de otra manera', 'que es crítico que se haga en este momento' o con cualquier otro sentimiento de urgencia y necesidad". Merece destacarse que el 66% de los títulos de estos mensajes -según los laboratorios de investigación en Symantec- contienen las palabras 'Petición', 'Pago, 'Urgente'... Además, una vez se tiene acceso a la plataforma de colaboración que supone el correo corporativo, se puede tener acceso a correos con facturas para pagar... en las que se puede modificar el IBAN para direccionar el pago hacia los intereses de los atacantes (y eso suele pasar altamente inadvertido). Asegura también el Strategist & Evangelist en la oficina del CTO en Symantec que se pueden generar correos que aparentan venir de una dirección conocida ya que es tremendamente sencillo modificar una letra 'L' minúscula por una 'i' mayúscula ya que en según qué tipos de letra es indistinguible; "eso permite generar dominios de Internet que pueden parecer de una compañía conocida cuando, en realidad, no lo es, sino que está creada por los atacantes para engañar".

Para José de la Cruz, un ataque BEC se divide en cuatro fases: Selección de un objetivo, Adquisición de la inteligencia, Ejecución y Conclusión. La garantía del éxito a menudo viene determinada por identificar un objetivo que proporcione una alta probabilidad de éxito; "normalmente una compañía internacional con una gran dispersión geográfica de sus empleados". En cuanto a la adquisición de inteligencia habla el CTO de Trend Micro de dos actores principales, por un lado, el usuario suplantado y por otro lado la víctima; "en esta fase se investiga el objetivo obteniendo información pública para identificar al usuario comprometido y victimas

"Los ataques BEC han evolucionado de manera exponencial, impactando -según nuestros datos- a 8.000 entidades cada mes a nivel mundial"

Ramsés Gallego, Strategist & Evangelist en la oficina del CTO en Symantec

a atacar dentro de dicha compañía. Adicionalmente se trata de buscar el método más adecuado: suplantar la identidad del objetivo mediante phising o comprometer una cuenta corporativa a través de un servicio público.

Alfonso Ramírez, de Kaspersky, señala que, aunque altos cargos y empleados suelen ser las víctimas, también "las empresas proveedoras o clientes de una organización pueden ser objeto de ingeniería social".

En cuanto a Eutimio Fernández, asegura que, en su forma más básica, una campaña BEC implica el envío de un correo electrónico (a veces usando spoofing para aparecer como si fuera de un compañero/jefe de trabajo) a los empleados de Finanzas que pueden realizar transferencias bancarias online.

Evolución de los ataques BEC

Como ocurre con casi todo, sobre todo si se trata de ciberamenazas, los ataques BEC ha evolucionado, y su evolución, dice José de la Cruz, "radica en la sofisticación de la solicitud enviada a la víctima: mejorando técnicas de phising, utilizando formatos corporativos, aprovechando vulnerabilidades en sistemas, utilizando malware para robo de credenciales, etc.".

Recuerda Jose Luis Laguna, Director Técnico Fortinet Iberia, que los ataques BEC existen desde hace tiempo en diferentes formas. Históricamente hemos visto la misma táctica utilizada contra empresas, usuarios de comercio electrónico y directores ejecutivos de empresas, entre otros. "Los atacantes perfeccionan constantemente sus técnicas y sus herramientas, pero además se asesoran con abogados, cuentan con servicios de traducción, con hackers, con expertos en ingeniería social, etc.", dice el directivo.

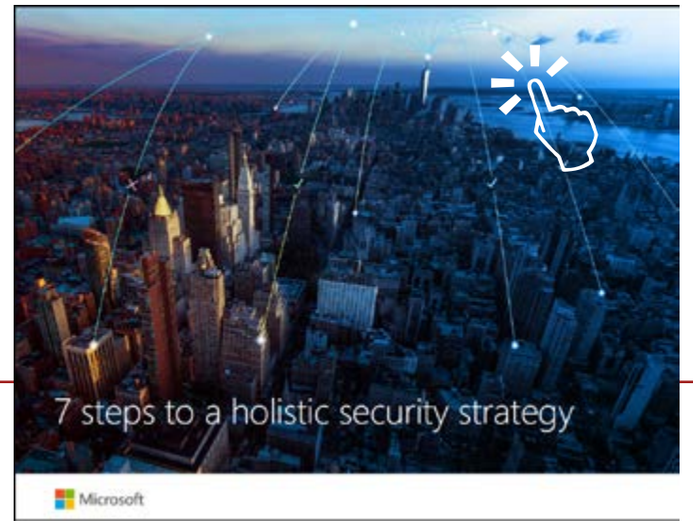
Si tomamos la evolución desde el punto de vista de costes, los informes del Internet Crime Complaint Center (IC3) -colaborador del FBI de EE.UU., del Departamento de Justicia de EE.UU., y del National White Collar Crime Center de EE.UU.- recogidos en el Informe Semestral de Seguridad 2017 de Cisco, "el fraude BEC generó unos beneficios a los ciberdelincuentes de 5.300 millones de dólares entre octubre de 2013 y diciembre de 2016, lo que implica una media de 1.700 millones de dólares anuales", dice Eutimio Fernández. En comparación, los ataques de ransomware generaron unos mil millones de dólares en 2016.

it whitepapers

SIETE PASOS
PARA UNA ESTRATEGIA
DE SEGURIDAD HOLÍSTICA

Hoy, el objetivo de los CISO es la gestión más adecuada de los riesgos para sus organizaciones. ¿El desafío? Hacer que las medidas de seguridad sean más efectivas en un contexto de escasez de personal y ciberataques en constante expansión de usuarios, dispositivos, aplicaciones, datos e infraestructura.

Este documento ofrece las pautas para generar esa estrategia, a través de siete pasos que empiezan por construir un ecosistema de aplicaciones de seguridad diseñadas para integrar...



Los ataques BEC “han evolucionado de manera exponencial”, dice Ramsés Gallego. Según datos de Symantec, este tipo de ataques han impactado a 8.000 entidades cada mes a nivel mundial y han supuesto un impacto económico de más de 4.084 millones de Euros entre Octubre de 2013 y Diciembre de 2016. “Dado que hay clara actividad criminal detrás por el beneficio económico evidente, es un ataque que continuará ocurriendo, lamentablemente”, dice Ramsés Gallego.

Cómo evitar ser víctima de un ataque BEC

Formación y concienciación es uno de elementos clave para evitar un ataque BEC, algo que en realidad sirve para casi todas las ciberamenazas que llegan a través del correo electrónico.

El director técnico de Fortinet habla además de pasarelas de correo electrónico, sistemas de prevención de intrusiones y productos antivirus como elementos que ayudan a evitar que el malware comprometa nuestro correo electrónico, así como la implementación de sistemas de autenticación fuerte para el acceso al correo electrónico.

Precisamente por eso José de la Cruz establece el correo electrónico como el elemento “donde deberemos dedicar la mayoría de nuestros esfuerzos”. Entre las recomendaciones que propone el director técnico de Trend Micro destaca la implementación de mecanismos de verificación de identidad para el correo, así como se sistemas de ciberseguridad que protejan contra el spam o las vulnerabilidades, el refuerzo de las políticas de seguridad para las contraseñas y, porque “en cualquier ataque, hay que tener en cuenta el factor humano, es importante concienciar al usuario final sobre el peligro que supone este tipo de ataques”.

Desde Kaspersky Lab recomiendan implementar una serie de medidas de seguridad capaces de proteger contra ataques BEC, como es la formación de los empleados en materia de seguridad; evitar hacer clic en enlaces o abrir documentos que parezcan sospechosos y comprobar el origen de los correos electrónicos; cambiar las contraseñas de todas las cuentas utilizadas en caso de que el sistema haya sido afectado; revisar siempre las solicitudes para cambiar los detalles de la cuenta bancaria o los métodos de pago durante las transacciones; instalar una solución de seguridad en todas las estaciones de trabajo y servidores donde sea posible y siempre implementar todas las actualizaciones.

Eutimio Fernández razona que, ya que los mensajes BEC no contienen malware o enlaces sospechosos, por lo general pueden superar la gran mayoría de herramientas de defensa frente a amenazas. “De hecho, las víctimas suelen ser grandes empresas con sólidas medidas de seguridad”, dice el responsable de ciberseguridad de Cisco. Dice también el directivo que la lucha contra el fraude BEC generalmente requiere mejoras en los procesos de negocio y en la educación de los trabajadores, formando a los empleados para identificar solicitudes fuera de lo común, como una transferencia fuera del país en una empresa que opera a nivel nacional. Las organizaciones pueden también requerir que los empleados verifiquen las transferencias electrónicas con otros empleados -quizá por teléfono- para eludir un posible email falso.

Enlaces de interés...

- BEC, una estafa de 5.000 millones de dólares
- Profundizando en el mundo del Business Email Compromise (BEC)
- Business Email Compromise, el ataque que temen todas las organizaciones
- W Guía para luchar contra los ataques BEC

BE SURE TO BE FREE

BLINDA TUS "SUPERCONFIDENCIAL"

#BlindaTuLibertad

Garantiza que lo que pasa en tu empresa se queda en la empresa.
Descubre lo último en ciberseguridad empresarial.

www.eset.es

ESET
ENJOY SAFER TECHNOLOGY™

Ojo a las criptodivisas y sus problemas de seguridad

Hablar de criptomonedas se ha puesto de moda. Invertir en ellas también. Y que los ciberdelincuentes aprovechen una nueva tecnología para explotarlas a su favor, no es de extrañar. Cryptojacking se pone de moda.

Más de la mitad de las organizaciones de todo el mundo se están viendo afectadas por el mal uso que las herramientas de minería de criptomonedas. Es lo que se conoce como cryptojacking, una nueva forma de malware que roba recursos de la máquina infectada para minar criptomonedas sin permiso. De forma que, si en un momento dado la CPU de tu equipo está trabajando al 100% de su capacidad, y la batería se agota rápidamente, puede que alguien esté utilizando tu ordenador para realizar tareas de minería de criptodivisas.

La popularidad de algunas criptomonedas, entre ellas Bitcoin o Ethereum está alimentando el interés entre los ciberdelincuentes por aprovechar la de CPU detrás de los principales sitios web y servicios de transmisión. Según el último "Índice Global de Amenazas" de Check Point, los 100 principales malware incluyen diez tipos diferentes de herramientas de minería de criptomonedas. En algunos casos, el 65% de los recursos de un sistema se están dedicando a la minería, yendo mucho más allá de los usos legítimos o legales del software.

En este caso, este tipo de ataques no están buscando robar los datos o el dinero de las víctimas, pero también impactan en las empresas. Se están detectando ataques que buscan instalar código malicioso en anuncios para instalar herramientas de minería de criptomonedas diseñadas para recolectar Monero, una criptodivisa. De forma que el usuario sólo tendría que hacer click en un pop-up y el proceso se iniciaría sin su conocimiento.

Compartir en RRSS

Cryptojacking es una nueva forma de malware que roba recursos de la máquina infectada para minar criptomonedas sin permiso

Minería de criptomonedas

Pero empecemos por el principio. ¿Cómo funcionan las criptomendas y qué es eso de minar criptomonedas? Las criptomonedas permiten a los usuarios realizar pagos de forma segura a través de internet sin tener que utilizar bancos. Nacida en 2009, Bitcoin tiene la distinción de ser la primera moneda digital; desde entonces se han creado varios centenares, 900 de ellas activas, entre las que se encuentran Ethereum, DigitalNote o PotCoin.

La existencia de las criptomonedas se basa en blockchain, o cadena de bloques, que es un libro compartido y duplicado varias veces a lo largo de una red de ordenadores, algo que garantiza su validez y la ausencia de fraude, ya que el documento se actualiza con cada operación y es distribuido y está disponible para todos los que tienen criptomonedas.

De forma que cada transacción realizada se registra en blockchain. Esta cadena de bloques está a cargo de los mineros, que usan potentes computadoras que hacen un recuento de las transacciones. Su función es actualizar esa cadena de bloques cada vez que se realiza una transacción y también garantizar la autenticidad de la información.

El valor de una criptomoneda no es fijo, sino que fluctúa en función de la demanda y la oferta. Dado que no existe un banco intermediario no existen costes y la identidad del comprador y el vendedor no se revela. Sin embargo, todas y cada una de las transacciones se hacen públicas a todas las personas en la red blockchain.

De forma que la minería de criptodivisas es el proceso por el cual se verifican las transacciones y se añaden a esa cadena de bloques, y también es la manera de crear y liberar nuevas criptomonedas. Cualquiera con acceso a internet y el hardware adecuado puede participar en la minería. El proceso de minería consiste en compilar transacciones recientes en bloques y tratar de resolver un rompecabezas computacionalmente difícil. El participante que resuelve primero el acertijo coloca el siguiente bloque en la cadena de bloques y reclama las recompensas. Y esas recompensas, que incentivan esa minería, son tanto las tarifas de transacción asociadas con las transacciones compiladas en el bloque como el bitcoin recientemente lanzado.

Y la nueva actividad de los ciberdelincuentes es buscar, o mejor dicho robar, esa recompensa. En según qué casos, cosechar bitcoins mediante minería podría ser más rentable para los ciberdelincuentes que utilizar ransomware.

Existen miles de personas buscando ganar dinero real con monedas virtuales. Hay varias

herramientas para la minería de criptomonedas como Bitcoin Miner, Multiminer, BFG Miner o EasyMiner. La mayoría de estas aplicaciones no fueron creadas para ser mal utilizadas, pero ahí han estado los chicos malos para explotarlas. Y a medida que la fiebre por las criptomonedas gana fuerza, los ciberdelincuentes dedican cada vez más atención a la minería de criptodivisas y a las herramientas que lo permiten.

Explotando las criptomonedas

De forma que los ciberdelincuentes, habida cuenta del incremento del valor de las criptomonedas, están buscando la manera de sacar partido. Una de las maneras es crear exploits de blockchain que les permitan robar fondos directamente de las carteras.

Un exploit de blockchain tiene como objetivo infectar las aplicaciones de monedero móvil y los intercambios en línea donde se almacena criptomoneda. En los últimos meses, se han viso men-

En según qué casos, cosechar bitcoins mediante minería podría ser más rentable para los ciberdelincuentes que utilizar ransomware

sajes de phishing específicos para penetrar en estos sistemas.

Pero las carteras, o wallets, no son las únicas fuentes de fondos digitales. El año pasado se produjo el aumento de la oferta de monedas inicial, un evento de financiación similar a una oferta pública inicial, pero utilizando nuevas criptomonedas. El fraude ya se vio cuando los ciberdelincuentes reemplazan la dirección de Ethereum en la plataforma de inversión de criptomonedas Enigma con su propia dirección y recaudaron 500,000 dólares en fondos de inversión que iban dirigidos para la puesta en marcha de la empresa antes de que alguien de la compañía notara el cambio. El reemplazo fue un simple ataque con contraseña que ayudó a los actores a obtener acceso al sitio web de Enigma. Aunque finalmente se recuperó el dinero, se esperan más ataques de este tipo a lo largo de 2018.

También se ha detectado un incremento de la infección de ordenadores para extraer o crear

Crypto-Mining Malware, una epidemia

El malware para minar monedas criptomonedas fue una amenaza en los primeros días de Bitcoin, cuando aún se podía generar esa moneda digital con hardware de consumo, pero esto no ha sido posible desde hace algún tiempo, el malware de criptomonedas prácticamente desapareció después de 2014. Pero en los últimos años se ha visto una afluencia masiva de nuevas monedas como Monero, Zcash y Ethereum, todas las cuales pueden extraerse provechosamente con hardware que la mayoría de la gente ya tiene.

El malware para la minería de criptomonedas ha regresado con fuerza en 2017, explica Symatnec en un post, en el que menciona a Coinhive como el más popular, junto con JSEcoin y Crypto-Loot.

En este regreso se han detectado algunas innovaciones tecnológicas notables, como ventanas "pop-under" que mantienen la minería después de haber cerrado la principal ventana del navegador y botnets que secuestran los dispositivos de Internet of Things.

En un informe del pasado mes de septiembre, IBM dijo que entre enero y julio de 2017 detectó seis veces más ataques de minería de CPU que implicaban el uso de malware para instalar herramientas virtuales de minería de divisas contra sus clientes. Las herramientas generalmente estaban incrustadas en archivos de imagen falsos que estaban alojados en servidores infiltrados que ejecutaban WordPress o Joomla. La mayoría de los ataques que IBM analizó fueron diseñados para apuntar a monedas virtuales como Monero, cuyo algoritmo CryptoNight puede ejecutarse en PC y servidores ordinarios en comparación con el hardware especializado requerido para la minería Bitcoin.

En los últimos meses se han encontrado pistas que apuntan a grupos de ciberdelincuencia organizada como Lazarus están activamente involucrados en la minería de criptomonedas. A principios de este mes, Bloomberg informó sobre un incidente en el que un grupo de Corea del Norte llamado Andariel secuestró un servidor perteneciente a una organización surcoreana y lo utilizó para extraer alrededor de 70 monedas Monero.

La amenaza ha evolucionado. En 2014 llegó a dispositivos Android con Kagecoin, un malware capaz de extraer bitcoin, litecoin y dogecoin; un troyano (RAT) njrat/NjwOrm de acceso remoto compartido en Oriente Medio fue modificado para agregar la funcionalidad de minería de bitcoin; lo mismo se hizo con una vieja Java RAT que puede explotar litecoin.

Otros conocidos malware de minería de criptomonedas son Adylkuzz, CPUMiner/EternalMiner y Linux.MulDrop.14. Todos ellos explotan vulnerabilidades conocidas: Adylkuzz aprovecha EternalBlue, el mismo fallo de seguridad que el ransomware WannaCry, mientras que CPUMiner/EternalMiner utiliza SambaCry, una vulnerabilidad en el paquete de software de interoperabilidad Samba; Linux.MulDrop.14, un troyano de Linux, se dirige a dispositivos Raspberry Pi.

CÓMO UTILIZAR LA DARK WEB PARA LA INTELIGENCIA DE AMENAZAS

Ha habido una tendencia a etiquetar la web oscura como “cualquier sitio web no indexado por Google”, pero esta definición es demasiado amplia. Es mejor pensar en términos de actividad puramente ilegal, y no hay duda de que los investigadores pueden usar la web oscura para obtener inteligencia de amenazas muy valiosa, a menudo relevante para un amplio espectro de posibles objetivos, tanto organizaciones como individuos, a los que no se puede acceder a través de la monitorización convencional.

nuevas criptomonedas. En este sentido Neptune es un kit de exploit que permite esconder cargas útiles de minería en anuncios que registran la dirección de correo electrónicos del atacante como fuente de la operación de minería antes de infectar el ordenador de la víctima.

Los navegadores también son un medio de explotar la minería de bitcoins. Algunos scripts de malware basados en navegador se ejecutan en segundo plano incluso después de que el usuario cierre su sesión de navegador, lo que podría permitir a los estafadores procesar los ciclos de las PC corporativas.

A este respecto, el navegador Opera ha sido uno de los primeros en incorporar un mecanismo que evite el cryptojacking, o el uso secreto de los dispositivos para minar criptomonedas, en su versión 50.

La herramienta anti-mining de Opera se llama NoCoin y es parte de la función de bloqueo de publicidad del navegador. Explicaba la compañía en un post que la herramienta está deshabilitada por defecto, pero que se puede activar en la página de ajustes y preferencias, y que es capaz de bloquear esos scripts de minería de criptomonedas de la misma manera que se bloquearía un pop-up de publicidad.

Según ha publicado la compañía, sin una herramienta como NoCoin, un minero de criptodivisas podría pasar desapercibido hasta que el uso de la unidad de procesamiento central (CPU) aumentara dramáticamente sin ninguna razón obvia, evitando que la víctima ejecutara sus propios programas.

Coinhive es el malware más utilizado para minar criptomonedas. Inicialmente se presentó como una forma para que los propietarios de una web ganaran dinero sin la necesidad de mostrar anuncios para obtener ingresos. Pirate Bay fue uno de los primeros en utilizar Coinhive para este propósito, pero al final se eliminó en respuesta a la protesta de los usuarios.

Coinhive proporciona a los propietarios y operadores de páginas web un código JavaScript que se inserta en la página y que utiliza la capacidad de procesamiento del ordenador de quien visita la web para minar la criptomoneda Monero sin que el usuario se dé cuenta.

> Los navegadores también son un medio de explotar la minería de bitcoins, y Opera ha sido uno de los primeros en incorporar un mecanismo que evita el cryptojacking en su versión 50

Los investigadores también han observado intentos de ocultar crypto-miners JavaScript utilizando ventanas ocultas pop-under, lo que permite a los estafadores continuar usando la CPU de la víctima incluso después de que el usuario haya navegado fuera del sitio web. Algunos criminales astutos incluso integraron scripts JavaScript para minería directamente en sus falsas pantallas de bloqueo de advertencia de seguridad del navegador.

El malware de minería a menudo explota vulnerabilidades conocidas, como el exploit EternalBlue, que se usó en el brote de ransomware WannaCry. CoinMiner, por ejemplo, utiliza Eter-

nalBlue para infectar otros puntos finales una vez que llegan a una PC en una red. Estos programas de minería pueden ser muy difíciles de detectar porque a menudo se combinan con otras técnicas, como los métodos sin archivos, o fileless, para ocultar sus pistas.

A medida que el cryptojacking despegado, también ha conseguido unificar algunas tecnologías mineras que se han estado filtrando lentamente a lo largo de los años. Coinhive incluso ha comenzado a promover un tipo de mecanismo antispam denominado Proof of Work Captcha, una idea que ha existido durante años. En lugar de verificar si un usuario es humano, esta herramienta resuelve acertijos mineros matemáticos intensivos en el procesador para hacerlo más lento y menos factible económicamente para que los spammers carguen ciertas páginas o realicen ciertas acciones en un sitio. Estos captchas resultan menos molestos para los usuarios individuales, pero gravan los procesadores de dispositivos.

Vulnerabilidades que arruinan el valor de las criptomonedas

En sus previsiones de seguridad para este año, Watchguard ya dijo que una gran vulnerabilidad arruinará el valor de una popular criptomoneda. Dos semanas después el segundo hackeo de la plataforma de bitcoins de Corea del Sur, Youbit, (anteriormente conocida como Yapizon) provocaba pérdidas millonarias entre los inversores, lo que le llevó a declararse en quiebra. La empresa, que se ha visto obligada a cerrar sus operaciones y declararse en bancarrota, no podrá devolver a los clientes más de un 75% del valor que había alcanzado su inversión.

Ethereum ya experimentó una caída de casi el 50% de su valor en 2016 cuando los hackers explotaron una vulnerabilidad en una popular aplicación de blockchain para robar más de 50 millones de dólares en criptomonedas Ethereum. Desde entonces, los programas de recompensas por búsquedas de vulnerabilidades y revisiones de código se han convertido en una parte importante del desarrollo de blockchain, pero los ataques han continuado, incluyendo uno que atacó a un popular monedero de código multifirma de Ethereum y dejó entre 100 y 500 millones de dólares en Ethereum inaccesibles de forma permanente.

En WatchGuard prevén que los hackers encontrarán una vulnerabilidad lo suficientemente grave como para eliminar por completo una popular criptomoneda socavando la confianza del público en su seguridad.

Enlaces de interés...

- Criptodivisas, el próximo gran objetivo de los hackers
- La botnet Necurs reorienta su negocio hacia las criptomonedas
- El Impacto del malware de minería de criptodivisas
- Bitcoin, las criptomonedas al asalto del Sistema Financiero Digital
- Criptodivisas, Bitcoin y seguridad

GDPR is coming.
Not sure where
to start?

Get Our Checklist >

Quest

Gestión de Seguridad Corporativa en momentos de Transformación

INNOVATING SOLUTIONS

¿Te avisamos del próximo IT User?

Febrero 2018

Gestión de Seguridad Corporativa en momentos de Transformación

Siempre se ha afirmado que una cadena es tan fuerte como su eslabón más débil. Y, aplicado a la protección, ésta es tan segura como su punto más inseguro. Por este motivo, el enfoque en toda estrategia de seguridad debe apostar por la globalidad, por proteger todos y cada uno de los elementos vulnerables de la entidad.

Y, precisamente, éste es el enfoque de Faro Security, una plataforma de BBVA desarrollada por GMV. Se trata de una solución completa para la gestión global de la seguridad física en todas sus localizaciones. Para ello, gestiona todos los elementos de seguridad y los incidentes que sucedan en las diferentes instalaciones de manera detallada, obteniendo una visión global del Estado de la Seguridad de todo el negocio. Además, planifica las actividades de los proveedores de servicios de seguridad: vigilancia, mantenimiento… para conseguir mejorar la eficiencia de los recursos y ahorrar costes.

Con esta solución, es posible mejorar los procesos de evaluación de seguridad y obtener mapas geográficos de riesgos de toda la organización. Además, con un flujo completo de información de todo lo que sucede globalmente en la compañía, ayuda mejorar la toma de decisiones.

Resumiendo, Faro Security tiene como objetivo principal la gestión de todas las actividades de un departa-

mento de seguridad, así como ayudar a establecer un modelo corporativo de procesos de seguridad, facilitando un uso más eficiente de los recursos humanos, tecnológicos y económicos.

Grosso modo, podemos definir una lista de beneficios potenciales para las compañías compuesto por elementos tales como: una mejora de la productividad en un 20%, simplificación de procesos, reducción del tiempo de gestión de incidencias, automatización de todos los informes entregados a terceros (internos y externos), disminución del tiempo dedicado al análisis de datos, automatización de informes de siniestralidad, minimizando el impacto a través de medidas preventivas, mejora de la gestión de proveedores y reducción de espacio físico para archivos e inventario.

Plataforma Faro Security

La plataforma Faro Security supone un paso adelante en la mejora de la gestión de la seguridad actual en las organizaciones.

Esta mejora se nota en diferentes líneas.

- Primero, en la recopilación de toda la información relevante ante un incidente de seguridad que pudiera derivar en un expediente. Así, se encargaría de la custodia de las evidencias (por ejemplo, imágenes captadas en una instalación que pudieran esclarecer la autoría de un robo).
- Segundo, en el mantenimiento y gestión de toda la documentación de la actividad de seguridad de la organización: planes de protección, procedimientos operativos, legislación aplicable, checklists, políticas de ciberseguridad… manteniendo un repositorio único y global, lo que elimina muchas duplicidades e incongruencias.
- Tercero, en las operaciones y mantenimiento de las instalaciones de seguridad, llevando un control pormenorizado de las incidencias, de las renovaciones de los sistemas, control de los presupuestos…
- Y cuarto, en la evaluación del desempeño de proveedores externos, en especial, en el servicio de vigilancia contratado. Este servicio acapara gran parte del presupuesto de seguridad privada y se necesita verificar que el servicio contratado es el servicio recibido.

ENTREVISTA A INÉS DÍAZ Y JAVIER ZUBIETA SOBRE FARO SECURITY

CLICAR PARA VER EL VÍDEO

Faro Security, plataforma de BBVA diseñada por GMV, es una solución completa para la gestión global de la seguridad física en todas sus localizaciones

Faro Security: Gestión de Seguridad Corporativa en momentos de Transformación

En el entorno digitalizado en el que vivimos, los problemas relativos a la seguridad se están incrementando día a día, desde los niveles más altos en el ámbito internacional hasta el individuo mismo. Las estrategias de Transformación Digital actuales están provocando que la actividad y responsabilidades de seguridad dentro de una organización se estén transformando, alineándose con el negocio, bien por necesidad, bien por evolución o madurez. La Seguridad Corporativa ha asumido esta nueva realidad, ha presentado una notoria transitoriedad hacia la implementación de nuevas medidas y debe destacar como facilitador, involucrándose en la estrategia y, por lo tanto, en las decisiones. No sólo debe proteger el negocio, sino también aportar la confianza necesaria, no sólo a los estamentos más altos de la organización, sino también al resto de partes interesadas, como clientes, accionistas o inversores, para elevar al máximo la reputación e imagen al exterior teniendo en cuenta el activo más importante de una organización, las personas.

Existe una percepción clásica de la Seguridad como un gasto y una de las formas de revertir esta situación es transformar la actividad en un proceso empresarial, como cualquier otro. Y para que esta transformación se lleve a cabo, es imprescindible GESTIONAR con amplitud de miras: riegos, cumplimiento legislativo y regulatorio, expectativas… Y para ello se necesitan metodologías y herramientas, enmarcadas en un Plan de Seguridad Integral. Sobre las metodologías, existen muchas y de gran aceptación mundial; sobre las herramientas, encontramos una situación artesanal que rara vez evoluciona a una plataforma de gestión.

Como empresa innovadora y conocedora de esta era en la que nos encontramos, GMV propone la plataforma de gestión de la seguridad corporativa Faro Security. A través de esta aplicación el proceso de seguridad se modela de forma corporativa y homogénea, buscando la estandarización, simplicidad y veracidad de la información manejada a lo largo de toda la organización y en todos los países donde tiene presencia.

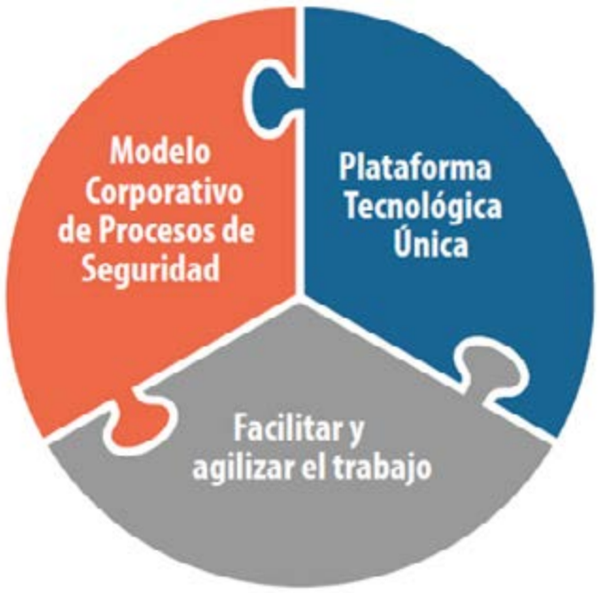
¿En qué mejora la gestión de la seguridad con Faro Security?

- En el conocimiento de qué tipo de incidente está ocurriendo, en qué lugar. Dadas las grandes automatizaciones inmersas en la propia herramienta se han optimizado los tiempos: informes en tiempo real de la información que cada usuario necesita en un momento, envío por mails a grupos de usuarios donde hay que notificar la incidencia, plantillas predefinidas, visual de mapas de riesgos…
- En la recopilación de toda la información relevante ante un incidente de seguridad que pudiera derivar en un expediente. Así, se encargaría de la custodia de las evidencias (por ejemplo, imágenes captadas en una instalación que pudieran esclarecer la autoría de un robo).
- En el mantenimiento y gestión de toda la documentación de la actividad de seguridad de la organización: planes de protección, procedimientos operativos, legislación aplicable, checklists, políticas de ciberseguridad... Manteniendo un repositorio único y global que elimina muchas duplicidades e incongruencias.
- En las operaciones y mantenimiento de las instalaciones de seguridad, llevando un control pormenorizado de las incidencias, de las renovaciones de los sistemas, control de los presupuestos...
- En la evaluación del desempeño de proveedores externos, en especial, en el servicio de vigilancia contratado. Este servicio acapara gran parte del presupuesto de seguridad privada y se necesita verificar que el servicio contratado es el servicio recibido.

BBVA gestiona su Seguridad Corporativa, una de las funciones críticas en la organización, a través de la plataforma Faro desde el año 2012. Hasta la fecha, BBVA ha desplegado la solución en 11 países y es utilizada por más de 1000 usuarios.

Por Inés Díaz Ochagavia, Banking Corporate Security en BBVA; y Javier Zubieta, Responsable de Desarrollo de Negocio de Ciberseguridad en GMV Secure e-Solutions

Gestión de Seguridad Corporativa en momentos de Transformación



Faro Security gestiona todos los elementos de seguridad y los incidentes que sucedan en las diferentes instalaciones de manera detallada, obteniendo una visión global del Estado de la Seguridad de todo el negocio en tiempo real

Faro Security está especialmente diseñada para organizaciones con múltiples localizaciones y multinacionales. La actividad de seguridad privada está fuertemente legislada en cada país, por lo que es necesario equilibrar los procesos de seguridad privada internos de una organización (lo que la organización considera que debe hacer, de una manera global) con la obligatoriedad de realizarle de una manera concreta (lo que la legislación de cada país exige que se haga).

Como decíamos, además del registro y seguimiento de todos los incidentes de seguridad, Faro Security ofrece una serie de funcionalidades que lo convierten en una potente herramienta para la gestión integral de la seguridad. Entre estas funcionalidades cabe destacar las siguientes: inventario pormenorizado de todos los dispositivos de seguridad instalados en las oficinas y edificios; planificación y seguimiento de los servicios de vigilancia, incluyendo la elaboración de presupuestos, la gestión de contratos y el seguimiento de la facturación; gestión de auditorías de seguridad en oficinas, edificios y cajeros automáticos; agenda de empresas proveedoras de seguridad y herramientas para el seguimiento y evaluación de los proveedores; gestión contable de los incidentes de seguridad; mapas de riesgo, informes de siniestralidad y cuadros de mando.

Asimismo, también incorpora un gestor documental en el que es posible almacenar toda la documentación asociada a cada incidente (denuncias, documentación del cliente, cuadres de caja...), así como fotos y vídeos relacionados con el mismo. Además, el gestor documental permite guardar cualquier tipo de do-

FARO SECURITY, GESTIÓN GLOBAL DE SEGURIDAD

CLICAR PARA VER EL VÍDEO

La solución está pensada para entidades multinacionales, de ahí que el diseño permita que la aplicación se pueda adaptar muy fácilmente a las características y necesidades de cada país

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkedIn

cumentación asociada a cada oficina y edificio, como certificados de instalación, registros de revisión, mapas o especificaciones técnicas de los dispositivos de seguridad instalados. Junto con ello, también ofrece una biblioteca digital que permite centralizar toda la documentación relacionada con la gestión de la seguridad: procedimientos y manuales internos, documentación normativa, legislación vigente...

La solución está pensada para entidades multinacionales, de ahí que el diseño permita que la aplicación se pueda adaptar muy fácilmente a las características y necesidades de cada país, manteniendo entre todos ellos una estructura común que favorece la homogeneización de los procesos de seguridad y la obtención de informes a nivel global.

Conviene señalar que, debido a su motor de perfilado y a la gestión de ámbitos de actuación que incorpora a nivel de usuario (ámbito de actuación geográfico y organizativo), puede ser utilizado por todo el personal involucrado en la seguridad, desde los vigilantes de seguridad hasta el responsable último del área de Seguridad Corporativa. De esta manera, actúa como un repositorio de información altamente detallada que es alimentada y mantenida continuamente por los diferentes grupos de usuarios. Toda esta información puede ser analizada y explotada de manera conjunta a través de diferentes informes y cuadros de mando personalizables que permiten obtener información agregada a cualquier nivel.

Por último, el diseño permite obtener en tiempo real informes y cuadros de mando a nivel mundial sin necesidad de disponer de procesos periódicos de consolidación de datos y sin que se vean afectadas las operaciones diarias realizadas desde cada uno de los países.

Enlaces relacionados

- Faro Security Solicitar una demo
- Documentación Faro Security
- Faro Security
- Faro Security, gestión global de seguridad
- GMV
- BBVA

Panda Adaptive Defense

Control y visibilidad de tus datos personales

Simplifica el cumplimiento del GDPR

Con la entrada en vigor del GDPR (General Data Protection Regulation), las empresas deberán, no solo proteger su privacidad, sino también controlar cómo se procesan, almacenan y utilizan sus datos. **Panda Adaptive Defense** y su módulo adicional **Data Control,** te ayudarán en el cumplimiento del GDPR.

Descubre y audita

Identifica a los usuarios, equipos o servidores con acceso a Información de Identificación Personal (PII) de tu empresa.

Monitoriza y detecta

Implementa medidas de acceso y operación sobre PII con la ayuda de los informes y las alertas en tiempo real.

Simplifica la gestión

Su activación es inmediata y se gestiona directamente desde la misma plataforma cloud.

Control de datos

Tu empresa tendrá un control exhaustivo de la PII ubicada en sus equipos.

Contacta con tu distribuidor habitual o llamando al 900 90 70 80

panda

pandasecurity.com/business/

La seguridad endpoint a debate con los líderes del sector

El endpoint se ha transformado, y también se ha multiplicado. Ya no sólo hablamos de un ordenador de sobremesa, hablamos de impresoras, proyectores, portátiles, tabletas, smartphones, relojes inteligentes e incluso pulseras de fitnets, por no mencionar las decenas de sensores del IoT. Todos ellos pueden ser fuente de problemas, puerta de ataques.

Las afirmaciones de que los antivirus están muertos y condenados al fracaso se han convertido en leyenda. ¿Qué hay de cierto en ello? Y además, ¿tiene el mercado realmente claro lo que es un endpoint? ¿Están seguro de poder controlar todos y cada uno de ellos? ¿qué papel juega el machine learning en una solución de seguridad enpoint?

Éstas y otras preguntas similares son las que se han planteado en un desayuno de trabajo que bajo el título “La Seguridad Endpoint a debate” ha reunido a varios expertos de seguridad, empezando por Pedro García Villacañas, director de preventa de Kaspersky Lab; José de la Cruz, Director Técnico de Trend Micro; Eduardo Sanz, Regional Manager ESET España; Ramsés Gallego, estratega y evangelista de Symantec; Raúl Pérez, Global Presales manager de Panda Security y Borja Pérez, Country Manager Stormshield Iberia.

"Ahora es económicamente viable y técnicamente posible utilizar machine learning de manera universal. Y creo que eso hay que celebrarlo"

Ramsés Gallego, estrategia y evangelista de Symantec

Arrancamos el evento hablando sobre las funcionalidades que debe tener un endpoint, que no son, ni más ni menos que las necesarias para cubrir todos los posibles vectores de ataque a los que se puede ver expuesto un endpoint, mediante una protección multicapa con distintas tecnologías de detección, aseguraba Pedro García.

La seguridad multicapa es un planteamiento general, también en Trend Micro. Y explica José de la Cruz que es necesario mantener una tecnología actualizada que combine tecnologías tradicionales con modernas "porque los atacantes utilizan métodos tradicionales y más modernos, y tenemos que ser capaces de abarcar todas las posibilidades".

Eduardo Sanz explica que en ESET se apuesta también por una seguridad multicapa, y añade que también es importante la concienciación al usuario y aportar una respuesta rápida.

"La obsesión de defender y de proteger de manera holística", es lo que para Ramsés Gallego tiene que tener una solución de seguridad endpoint. Que garantice, independientemente de los vectores de ataque que se utilicen, la protección y defensa del endpoint en sus diversas formas y variables.

LA SEGURIDAD ENDPOINT A DEBATE CON LOS LÍDERES DEL SECTOR

CLICAR PARA VER EL VÍDEO

Para Raúl Pérez la prevención es un punto clave. "Se deben utilizan todas las tecnologías posibles, desde el big data a temas holísticos, para que todos los sistemas estén protegidos".

Borja Pérez añade que un elemento clave es la concienciación del usuario y que las herramientas que pongamos para proteger los puestos de trabajo, el endpoint, deben ser lo más transparentes posibles.

Propuestas de Seguridad Endpoint

Stormshield. Stormshield Endpoint Security es un agente ligero que se instala en cualquier puesto de trabajo para monitorizar procesos a ver si son legítimos o ilegítimos. Mira las técnicas de bajo nivel de todos estos malware y sus mutaciones para detectar keylogger, escrituras en memoria que no corresponden, etc. Hasta ahora nuestra solución ha sido puramente de protección y en el roadmap se platean funcionalidades de detección y respuesta. Todo el tema forense es muy interesante, pero seguimos pensando que para una empresa lo importante es para los ataques. Borja Pérez, Country Manager de Stormshield Iberia

Panda Security. Por nuestra parte, reafirmar lo que ha comentado el laboratorio independiente de AV Comparatives: que somos la única empresa en el mundo con una detección del 100% en Zero Days, y que Gartner nos ha situado como líderes de innovación. Ahora estamos evolucionando hacia el Threat Intelligence Service, hacia plataformas de Threat Hunting Investigation con telemetría en tiempo real de millones de puestos. Raúl Pérez, Global Presales Manager de Panda Security

Symantec. No creemos en ser monolíticos. Entendemos muy bien el endpoint, pero también el Gateway, y la nube, y somos líderes en DLP y entendemos la movilidad. Se trata de una estrategia completa y simplificada que sin duda tiene en el endpoint uno de los puntos importantes que se debe hablar necesariamente con el restos de herramientas. Eso es lo que creemos y en eso es en lo que trabajamos. Ramsés Gallego, estratega y evangelista de Symantec.

Kaspersky Lab. Uno de los puntos fuertes de Kaspersky ha sido siempre la protección endpoint, pero en los últimos años el portafolio de la compañía ha cambiado drásticamente. La idea de la compañía a nivel estratégico es intentar cubrir todos los procesos en los que nos podemos ver inmersos dentro de la seguridad. La propuesta de nivel endpoint sigue siendo la misma que

venimos ofreciendo en los últimos años, y lo que empezamos a incorporar y está a punto de salir al mercado es la tecnología de DR, y por supuesto todo esto integrado en distintas áreas de threat intelligence y threat hunting que también tenemos dentro del portfolio. Pedro García Villacañas, Director Preventa de Kaspersky Labs Iberia.

Trend Micro. Nosotros en Trend Micro basamos nuestra estrategia de defensa en dos premisas. La primera sería la seguridad multicapa: incorpora todas las tecnologías que hemos venido desarrollando durante casi 30 años de historia de la compañía, y hacerlo de manera coordinada y efectiva. Y por otro lado creemos en la seguridad conectada, es decir, todos nuestros productos son capaces de proteger todos los posibles vectores de ataque, comparten la misma inteligencia desde el punto de vista de amenazas y son capaces de compartir inteligencia desde el punto de vista de compartir la información sobre un intento de ataque de Día Cero con el fin de bloquear en mi empresa ese ataque y que no se pueda propagar. Y con esto creemos que proporcionamos una seguridad completa y robusta. José de la Cruz, Director Técnico de Trend Micro.

ESET. Nosotros tenemos soluciones para endpoint, pero también podemos proteger cualquier otra plataforma dentro de la empresa, como puede ser un servidor de correo o un servidor de archivos, incluso gateways. En cuanto a endpoint, intentamos dar el máximo de seguridad posible con el menos impacto en el rendimiento del equipo; nos hemos reconvertiros y hemos pasado de ser un fabricante para convertirnos en un proveedor de seguridad y damos una serie de servicios que antes no dábamos como puede ser un servicio de threat intelligence, la inteligencia frente a amenazas, hacemos auditorías de seguridad, que da una visión más amplia al cliente del estado de seguridad de su empresa. Seguimos mejorando nuestros productos y añadiendo nuevas capas en función de las nuevas amenazas que van surgiendo. Eduardo Sanz, Regional Manager ESET España.

CÓMO GENERAR UNA POLÍTICA DE SEGURIDAD DE RED RAZONABLE

Los expertos en seguridad coinciden en que las empresas bien administradas necesitan una política de seguridad por escrito. Pero en la práctica, redactar y mantener estos documentos se atasca en un marasmo de ineficiencia burocrática y disputas inútiles interminables. El enfoque de "preguntas y respuestas" de este documento permite a las empresas plantearse generar una política de seguridad sin contar con un consultor externo y producir un documento breve, utilizable y, lo que es más importante, comprensible y en un tiempo razonable.

Impacto del BYOD

Si algo ha tenido un fuerte impacto a la hora de proteger el endpoint ha sido el famoso Bring Your Own Device (BYOD), que añadió algo de color a las empresas, y muchos quebraderos de cabeza a los responsables de TI. El BYOD no sólo añadió diversidad en cuanto a las plataformas, sino a la cantidad de dispositivos. Se pasó de contemplar un PC o impresora a tener que tener en cuenta un reloj inteligente, una pulsera de fitness, una Tablet, incluso una cafetera, como recuerda Borja Pérez.

Raúl Pérez compartió la noticia de las pulseras de ejercicio que el ejército americano repartió entre los soldados sin tener en cuenta que la información era reportada a un sitio en el que se podía ver dónde estabas los soldados del ejército americano, incluso se desvelaron bases secretas siguiendo los movimientos de tropas. "Antes había unas normas clásicas de protección del períme-

"La prevención es un punto clave. Se deben utilizan todas las tecnologías posibles, desde el big data a temas holísticos, para que todos los sistemas estén protegidos"

Raúl Pérez, Global Presales Manager de Panda Security

tro, pero ahora eso no existe y lo importante es el endpoint porque ya no hay barreras y al final todo se ejecuta en el punto final", dice el ejecutivo de Panda Security.

Para Ramsés Gallego, BYOD tiene que ser una invitación, no una imposición del empleado, y se debe enfatizar en la capacidad de proteger la información allá donde vaya.

Para Eduardo Sanz, de ESET, se está permitiendo el BYOD, o que se trabaje desde casa, y esto lo que hace es comprometer los datos de la empresa, porque no hay control de qué se está haciendo, dónde se está conectando. "Yo creo que el BYOD se puede utilizar, se ha demostrado que es muy productivo, pero tiene que haber unas políticas", dice el ejecutivo.

José de la Cruz, que reconoce encontrarse con empresas que no sólo permiten el BYOD sino que lo subvencionan, propone "dejar una pequeña porción de tu dispositivo para acceder a la información que es corporativa, y cuando salgas de aquí no vas a poder acceder".

"Next Generation Endpoint Security responde también a un Next Generation Malware, al que tenemos que hacer frente"

Pedro García Villacañas, Director Preventa de Kaspersky Lab Iberia

Coincidiendo en que hay que acomodarse a las nuevas tendencias, Pedro García Villacañas platea que las empresas integren la seguridad o la protección de estos dispositivos como un proceso más de la seguridad de la compañía, porque "de nada sirve que tengas la mejor solución de seguridad, sin después a nivel de políticas, o de concienciación del usuario, las cosas fallan".

Endpoint virtualizado

Igual que la movilidad o el BYOD ha impactado en la seguridad del endpoint, preguntamos también a nuestro grupo de expertos qué impacto ha tenido la virtualización. Para Ramsés Gallego, evangelista de Symantec, "es un reto añadido". Tampoco se le da excesiva importancia y lo considera como "un capítulo más del libro de TI. La virtualización es un entorno que requiere protección, como lo requiere la nube o la movilidad".

¿Te avisamos del próximo IT Digital Security?

Raúl Pérez, Global Presales Manager de Panda Security, coincide que la virtualizada se tiene que tratar como el resto de las máquinas de una empresa.

“Creo que la virtualización añade una capa adicional de complejidad tecnológica, pero tiene otras ventajas, porque normalmente está más controlado lo que utiliza el usuario”, dice Boroja Pérez, responsable de Stormshield Iberia, que recalca que se puede crear la falsa ilusión de que al estar virtualizado creamos que no tiene que estar protegido.

Tanto Pedro García como José de la Cruz coinciden en que es algo que hay que proteger, aplicando la solución adecuado, que sea transparente, no tenga impacto en las cargas de trabajo en ese entorno y garantizando la visibilidad y el control. Con respecto al impacto recuerda Eduardo Sanz, Regional Manager de ESET España que “hace tiempo las máquinas virtuales no se protegían por temas de rendimiento, pero ya existen soluciones que se adecúan y no requieren tanta carga dentro de la máquina como antes.

El antivirus no ha muerto

Las afirmaciones de que los antivirus están muertos y condenados al fracaso se han convertido en leyenda. Borja Pérez asegura que Stormshield siempre recomienda a los clientes que los mantengan; “no es 100% efectivo, pero hace una serie de funciones que aún son necesarias”.

Raúl Pérez, Global presales Manager de Panda Security asegura que el antivirus ha tenido que reinventarse, actualizarse, modernizarse –como la propia Panda Security, y que por eso surge el concepto de Next Generation Endpoint Security.

“El antivirus no está muerto, pero tiene que combinarse inteligentemente con técnicas avanzadas”, dice Ramsés Gallego, para quien hablar de Next Generation Endpoint significa que hay un next generation attack. Para Pedro García Villacañas, la palabra antivirus le parece obsoleta y prefiere hablar de antimalware. “Next Generation responde también a un Next Generation Malware, al que tenemos que hacer frente”, explica el ejecutivo de Kaspersky, para quien lo realmente importa dentro de las soluciones de seguridad en-

"El BYOD ha demostrado que es muy productivo, pero tiene que haber unas políticas y cierto control"

Eduardo Sanz, Regional Manager ESET España

"El endpoint es fundamental, pero no es el único vector. Hay que proteger todos porque los ciberdelincuentes diversifican en tecnología y en los vectores de ataque"

José de la Cruz, Director Técnico de Trend Micro

dpoint, es la inteligencia de amenazas que cada uno de nosotros poses.

El antivirus, o antimalware, es una capa más de protección, dice José de la Cruz, añadiendo que, aunque sea una protección poco eficaz "me está quitando mucha morralla".

Eduardo Sanz, para quien el antivirus no está muerto, explica que ESET ha ido añadiendo nuevas capas de seguridad, incluido el machine learning para identificar las muestras buenas, o malas y potencialmente indeseables. El machine learning sirve para quitar carga de trabajo. Es la opinión generalizada, a lo después se añade que no reemplaza a un técnico especializado, y que tampoco es una bala de plata.

José de la Cruz añade dos elementos imprescindibles dentro del machine learning: tiene que tener una buena base de datos detrás, "y cuando digo eso no me refiero a cantidad sino a calidad". De forma que es muy importante que el muestreo sea el adecuado.

Para Pedro García el machine learning es fundamental, aunque habla de contexto como elemento clave, ya que "tener toda esta información y toda esta inteligencia de amenazas sin contextualizad es una locura".

Dentro de Symantec el machine learning juega un papel fundamental. No sólo está implementado en la propuesta de seguridad endpoint, sino en otros doce productos más, explica Ramsés Gallego, quien añade que ahora "es económicamente viable y técnicamente posible utilizar machine learning de manera universal. Y creo que eso hay que celebrarlo".

Para Panda Security Machine Learning fue crítico, dice Raúl Pérez. La compañía se dio cuenta a primeros del 2000 que el incremento del malware exigiría el trabajo de miles de analistas para 2010, por lo que en 2002/2003 se abrió un proyecto, un motor de machine learning que, recogiendo todas las evidencias de los endpoints de manera automática, catalogara el malware con un 100% de

Compartir en RRSS

precisión. “Si enseñas bien a la máquina a hacer su trabajo y los datos son de calidad su trabajo será certero”, asegura el ejecutivo de Panda Security.

“Para nosotros machine learning es importante en otras áreas”, doce Borja Pérez, que explica que la solución endpoint de Stormshield es “determinística”; hay una serie de procesos a bajo nivel que no son legítimos, eso es lo que bloquea nuestro agente, independientemente de que sea una aplicación legitima. Lo que hace Stormshield es compartir el conocimiento que se obtiene en el endpoint con las soluciones de protección perimetral o en servicio de sandboxing. “En el endpoint no es tan crítico para nosotros el machine learning, pero sí aprovechamos ese conocimiento para alimentar otras soluciones”, concluye Borja.

Para el director preventa de Kaspersky Lab el mejor lugar para detener un ataque es el endpoint porque lo que está detrás de ese punto final es un humano. “Siempre decimos que el mejor antimalware es el que está entre la silla y el teclado”, dice Pedro García.

Raúl Pérez coincide en la opinión, asegurando que, aunque los usuarios sean cuidadosos hay que poner distintas contramedidas para evitar esos ataques. Borja Pérez habla de la “democratización” de los ataques, que hace que nadie esté a salvo, lo que impone más presión en el endpoint.

“El mejor lugar para parar un ataque es donde lo pares”, dice Ramsés Gallego, mientras que José de la Cruz dice que el endpoint es fundamental pero no es el único vector hay que proteger todos porque “los ciberdelincuentes diversifican en tecnología y en los vectores de ataque”.

El hecho de que en el endpoint es donde interactúan hombre y máquina lleva a Eduardo Sanz a hablar de métodos de protección junto con la promoción de cursos de concienciación dentro de las empresas para los empleados.

Enlaces de interés...

- Amenazas de primer nivel y su impacto en las decisiones de seguridad endpoint
- El endpoint no es el mejor lugar para detener las amenazas
- Machine Learning vs Inteligencia Artificial
- Next Generation llega al endpoint

"La virtualización puede crear la falsa ilucisión de que creamos que, al estar virtualizado, no tiene que estar protegido"

Borja Pérez, Country Manager Stormshield Iberia

Securing the Cloud Generation

The Cloud Generation is all of us, working anywhere and everywhere. We break the boundaries of desktops and data centers and embrace the mobile, social, global, crowd-sourced, always-on realities of our age.

It's a time when critical data, apps and infrastructure shift from 'behind the firewall' to 'running on the cloud'. Some of us are all in; some are only 20% there.

Yes, it's liberating. Yes, it's chaotic. And Symantec is here to help you conquer cloud chaos.

Symantec

Copyright © 2017 Symantec Corporation. All rights reserved.

Meltdown y Spectre,
¿final o principio?

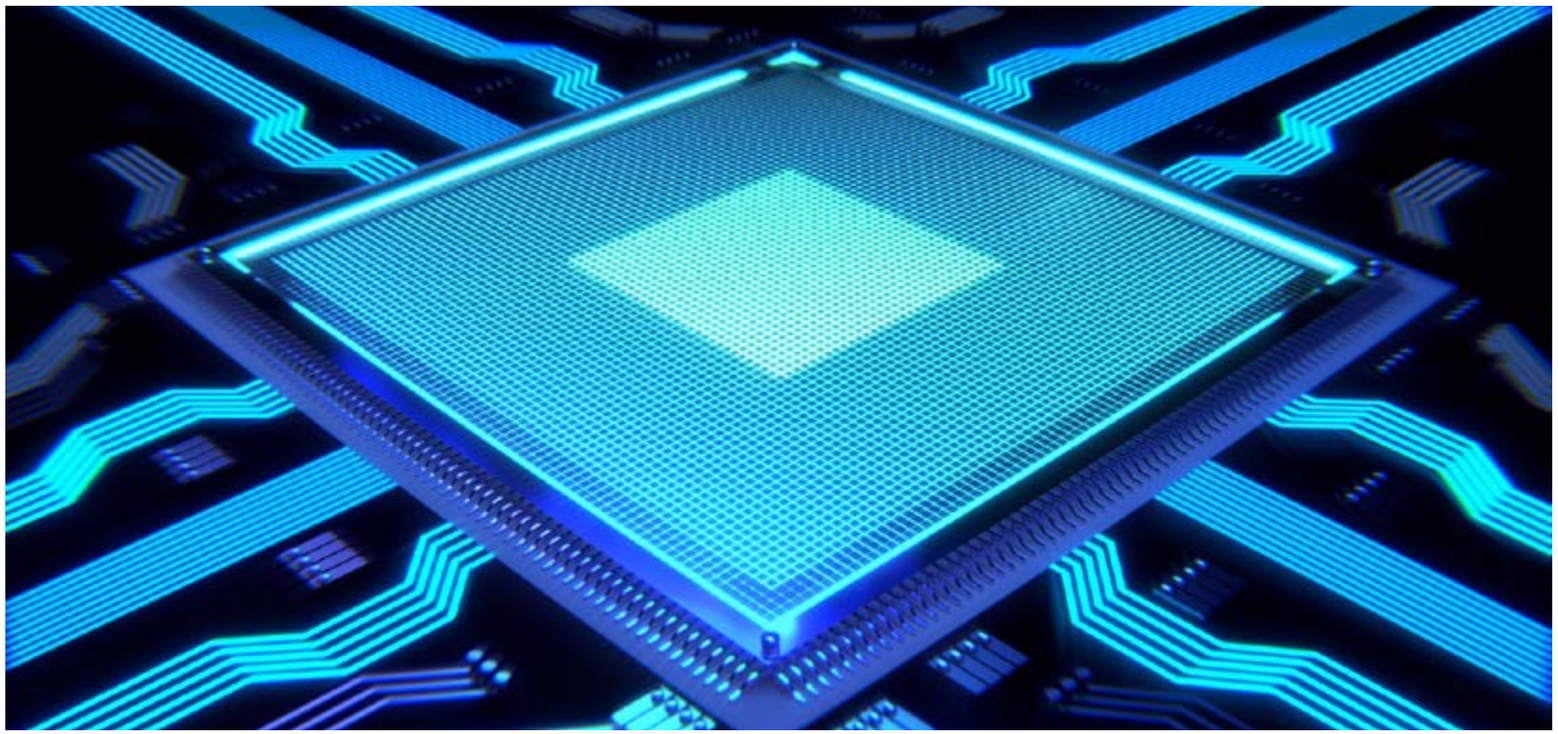
El pasado tres de enero la industria de TI se paralizó. Cuando algo verdaderamente importante ocurre, algo tan significativo como para cambiar el futuro establecido, se produce un antes y un después. Un ejemplo puede ser el de las escuchas de la NSA que salieron a la luz en junio de 2013; un escándalo que convirtió Internet en un lugar menos amigable y disparó el uso de comunicaciones cifradas para evitar espionaje. Y 2018 se ha estrenado con Meltdown y Spectre.

En 3 de enero se hacía público lo que pueden considerarse las mayores vulnerabilidades en la historia de la informática, no tanto por su complejidad –que también, sino por su alcance: la mayoría de los microprocesadores modernos. Bautizadas como Spectre y Meltdown, las vulnerabilidades fueron descubiertas unos meses antes por diferentes investigadores, quienes advirtieron a los fabricantes de chips.

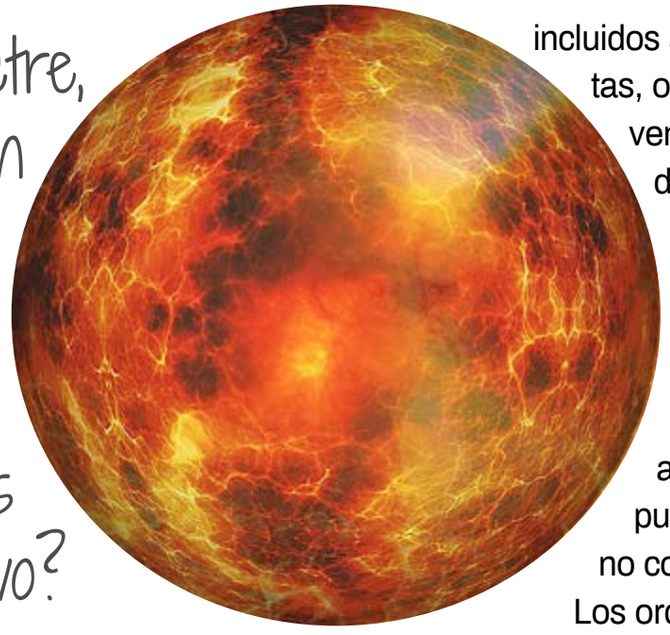
En principio, no debería ser diferente a lo que ocurre con otras muchas vulnerabilidades y parches, pero el problema es que los fallos están en el propio hardware, no en el software y afectan a los microprocesadores fabricados en los últimos 20 años. Hablamos de miles de millones de chips, de miles de empresas afectadas y la necesidad de una coordinación a gran escala que, como se ha visto en las últimas semanas, no está resultando nada fácil.

Meltdown fue descubierto e informado de forma independiente por tres equipos, incluidos Jann Horn del Proyect Zero de Google; Werner Haas y Thomas Prescher, de Cyberus Technology; y Daniel Gruss, Moritz Lipp, Stefan Mangard y Michael Schwarz, de la Universidad de Tecnología de Graz en Austria. En cuanto a Spectre, fue descubierto independientemente por dos personas, Horn y Paul Kocher, que trabajaron en colaboración con Daniel Genkin, de la Universidad de Pennsylvania y la Universidad de Maryland así como Mike Hamburg, de la firma Rambus. La suma de ambas vulnerabilidades afecta, virtualmente, a todo equipo moderno,

La suma de Meltdown y Spectre afecta, virtualmente, a todo equipo moderno, incluidos smartphones, tabletas, o PC, de cualquier vendedor, y ejecutando casi cualquier sistema operativo



Meltdonw y Spectre, ¿son principio o son final? ¿son el principio de un nuevo tipo de vulnerabilidad localizada en la parte más profunda de un dispositivo?



incluidos smartphones, tabletas, o PC, de cualquier vendedor, y ejecutando casi cualquier sistema operativo.

De forma que Meltdonw y Spectre abren la puerta a una nueva vía de ataque, y la respuesta del mercado no convence.

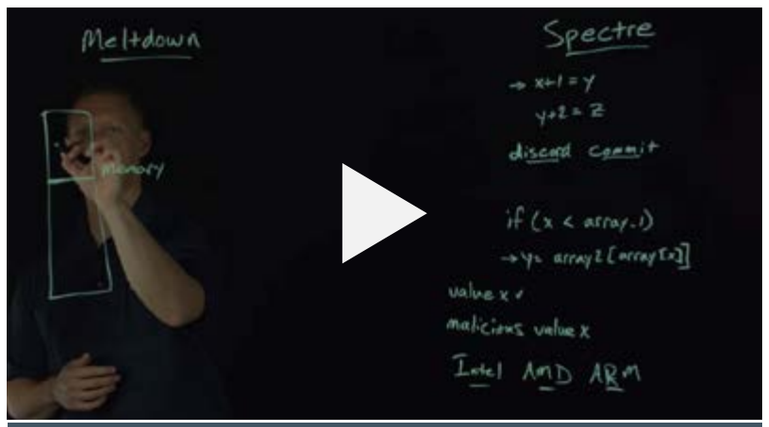
Los ordenadores actuales pueden hacer varias cosas al mismo tiempo, tener varias aplicaciones abiertas de forma simultánea. Se puede estar escuchando música mientras se navega, ver un vídeo mientras se renderiza otro, o estar escribiendo en Word mientras el sistema descarga las últimas actualizaciones y las instala. Si hablamos de la nube, se pueden estar ejecutando multitud de aplicaciones para multitud de ordenadores, y cada uno de estos procesos necesita estar aislado de los demás. Una aplicación no puede ver lo que está haciendo otra, salvo en determinadas circunstancias; de otra manera, a una aplicación maliciosa le sería muy fácil ver los datos que gestiona otra, lo que generaría un grave problema de privacidad y seguridad. De forma que las empresas que desarrollan software dedican tiempo y esfuerzo en aislar sus aplicaciones o mejor dicho, las cargas de trabajo de sus aplicaciones. Spectre y Meltdown echan por tierra ese esfuerzo, rompen ese aislamiento y lo hacen a nivel de chip.

Quizá habría que mirar unos cuantos años atrás, hacia los esfuerzos de optimización de los procesadores, para entender el problema. Una de las claves para acelerar la actividad de los procesadores es acelerar la entrada y salida, el I/O, de los datos en la memoria para su procesamiento. Es lo que se llama el rendimiento del procesador, que puede acelerarse mediante lo que se denomina ejecución especulativa: adivinar qué datos se van a recibir, y ejecutar las instrucciones en función de eso; si se acierta, se gana y se mejora el rendimiento, y si no, se descarta lo que se ha hecho sin pérdida de tiempo.

Meltdown y Spectre atacan esa ejecución especulativa, y de diferentes maneras. Meltdown es una vulnerabilidad más convencional porque es un error de más fácil reparación. Sin embargo, Spectre, cuya actualización es la que está ocasionando tantos problemas, es un fallo que afecta a todo el concepto de la ejecución especulativa y por tanto la solución pasa por un rediseño del propio procesador.

El momento de la reparación

Desde que se tuvo noticias de las vulnerabilidades, recogidas como CVE-2017-5715, CVE-2017-5753 y CVE-2017-5754, los fabricantes han estado implementando parches que los corrijan en la medida de lo posible. Sistemas operativos, navegadores y chips han sido parcheados, en la mayoría de las ocasiones sin que los usuarios tuvieran conciencia de ello, de manera tan rutinaria a como multitud de empresas, desde Microsoft, pasando por Adobe, Mozilla, Opera, Apple u Oracle, lanzan sus actualizaciones. Pero Meltdown y Spectre son especiales



EXPLICANDO LAS VULNERABILIDADES MELTDOWN Y SPECTRE

CLICAR PARA VER EL VÍDEO

CVE, la compilación de vulnerabilidades universal

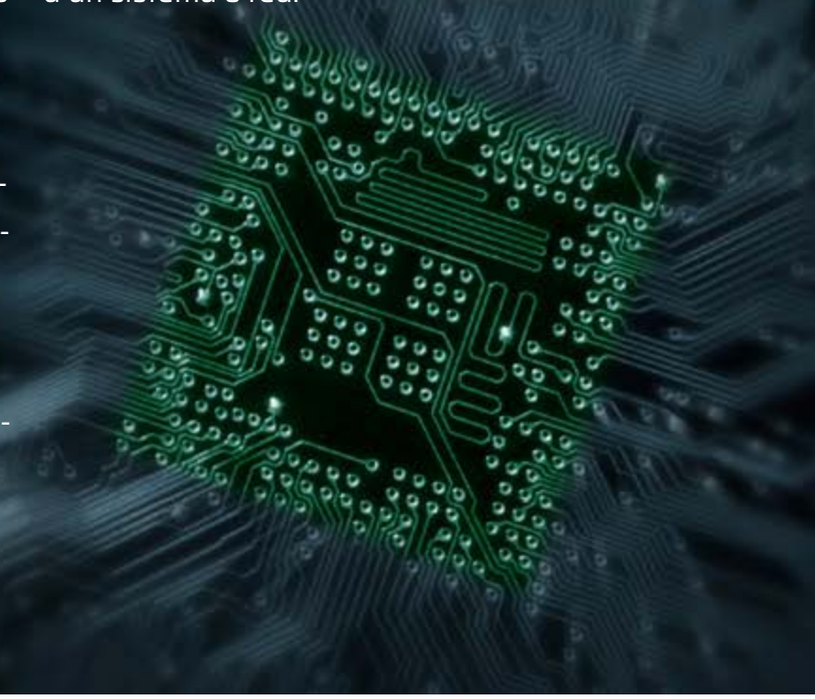
CVE, o Common Vulnerabilities and Exposures, es un programa creado en 1999 dedicado a la catalogación de vulnerabilidades cuyo objetivo es ayudar a las empresas a mejorar su seguridad, además de establecer un método común en la manera en que cada vulnerabilidad conocida es identificada.

Explica el organismo que su función es el intercambio de datos sobre vulnerabilidades, cada una de las cuales es identificada con un número, una descripción y al menos una referencia pública. Esta identificación común permite a los administradores acceder a información técnica sobre una amenaza específica.

El programa está apoyado por el US-CERT dentro del Department of Homeland Security (DHS) Office of Cybersecurity and Information Assurance (OCSIA). MITRE se encarga de mantener la Lista CVE para el beneficio de la comunidad a fin de garantizar que siga siendo un estándar abierto y gratuito, así como para proteger legalmente el uso continuo de la misma y cualquier contenido resultante por parte del gobierno, proveedores y/o usuarios. Además, MITRE ha registrado el acrónimo de CVE y el logotipo de CVE para proteger su uso único y continuo del esfuerzo de CVE en el ámbito de la ciberseguridad.

En varias ocasiones se ha planteado si este diccionario de vulnerabilidades no es una de las mejoras herramientas que puede tener un hacker a la hora de decidir qué fallo poder explotar. Sin embargo, desde la organización defienden que los beneficios que aporta CVE supera los riesgos, como el hecho de que CVE esté restringido a vulnerabilidades ya conocidas; además, a una organización le lleva más trabajo proteger sus redes y solucionar todos los agujeros de seguridad posibles de lo que le lleva a un hacker encontrar una sola vulnerabilidad, explotarla y poner en peligro la red.

Por cierto, que explica el organismo en su página web que se considera vulnerabilidad a un error en el código de software que proporcionar a un atacante acceso directo a un sistema o red. Este fallo permitiría que un atacante se convirtiera en administrador del sistema con todo tipo de privilegios. En cuanto a Exposición, es un problema de configuración del sistema o un error en el software que permite, a modo de trampolín, el acceso a un sistema o red.



y, como decíamos al comienzo, han marcado un antes y un después, haciendo que muchos vean en futuro de una manera diferente.

Y entre las previsiones, que los ataques contra el hardware, y no tanto contra el software, serán más comunes. Quizá sean más difíciles de detectar, pero una vez hecho, las posibilidades de explotar esas vulnerabilidades con éxito mejoran sustancialmente. Además, quizá no estemos hablando del futuro, sino del presente. Como ejemplo, la vulnerabilidad detectada en Intel Management Engine, una característica de administración remota de los procesadores de la compañía. Como Meltdown y Spectre, afectan a la manera en que operan los chips.

Que una vulnerabilidad afecte a una parte fundamental de un ordenador, como son los procesadores, significa que parchearlos exige de la coordinación de muchas compañías, lo que deja mucho

tiempo a los atacantes para explortarlos. Es lo que se está viendo ahora, que incluso cuando Intel y AMD son capaces de crear un parche, son los fabricantes de ordenadores y vendedores de aplicaciones quienes tienen que continuar la cadena, haciendo que dichos parches lleguen a los usuarios.

Otra cosa por la que las vulnerabilidades Meltdown y Spectre son especiales, es porque afectan directamente a la funcionalidad de los ordenadores. En algunos casos, los parches han generado un impacto en la velocidad y rendimiento de los propios procesadores. Aunque inicialmente se hablaba de un impacto del 30%, finalmente se trata de un impacto mínimo que afecta sólo a ciertos servidores que corren en la nube.

Finalmente, algo de suma importancia, hay algunas vulnerabilidades que no se pueden parchear. Lo habitual es que cuando se detecta una vulnerabilidad el fabricante responsable del producto lance un parche que solucione el fallo. Ahora, es cada vez más habitual que los fallos no puedan repararse. Un go-to-market demasiado agresivo, que no tiene en cuenta las mínimas medidas de seguridad, puede ser una de las razones. Ejemplos hay y más que habrá, sobre todo en el mundo del Internet de las Cosas (IoT), donde muchas cámaras web se han convertido en parte de la botnet Mirai.

Y para dar otra vuelta de tuerca, y darnos cuenta de cómo Meltdown y Spectre suponen un antes y un después, tener en cuenta que, si entendemos que un ordenador es un endpoint, el número y variedad de ellos se ha multiplicado. ¿No se puede considerar un coche conectado como un ordenador? ¿Y un teléfono? ¿un dispositivo médico? Meltdonw y Spectre, ¿son principio o son final? ¿son el principio de un nuevo tipo de vulnerabilidad localiza-

it whitepapers

GUÍA
PARA SOBREVIVIR
A LOS ATAQUES BEC

A diferencia de otros ciberataques, los ataques BEC, Business Email Compromise, no incorporan malware ni URL maliciosas en los emails. En cambio, aprovechan la ingeniería social. BEC ataca a personas concretas, generalmente directores financieros o personas en los departamentos de recursos humanos, finanzas o nóminas. Usando una técnica llamada “spoofing”, los ataques engañan a su gente haciéndoles creer que han recibido un correo electrónico de un jefe, compañero de trabajo, proveedor o socio.

Secure Networks, Data & Endpoints for IT,
OT, Cloud & Mobility

Smile!

You're protected

STORMSHIELD
NETWORK SECURITY

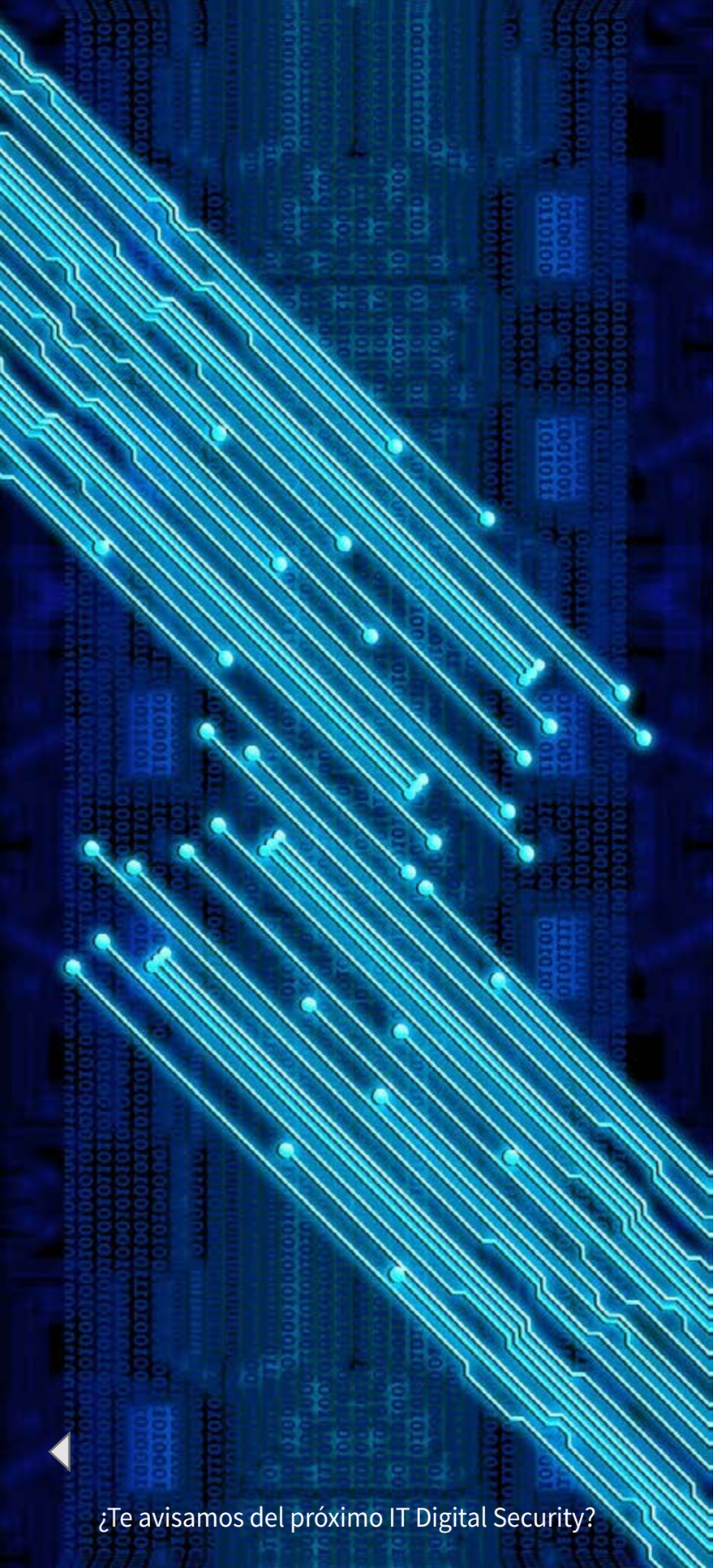
STORMSHIELD
ENDPOINT SECURITY

STORMSHIELD
DATA SECURITY

Stormshield is your trusted provider of
end-to-end security solutions and your key
supplier of peace of mind

STORMSHIELD

www.stormshield.com



Reptoline es una técnica de modificación binaria desarrollada por Google que utiliza parches de software en lugar de deshabilitar las características de la CPU afectada

da en la parte más profunda de un dispositivo? ¿un tipo de vulnerabilidad que no se puede parchear?

Meltdown vs Spectre

Meltdown y Spectre son vulnerabilidades estrechamente relacionadas que pueden explotarse de diferentes maneras para que posibles programas maliciosos puedan acceder a datos a los que no deberían poder acceder. A pesar de su similitud, tienen una serie de diferencias.

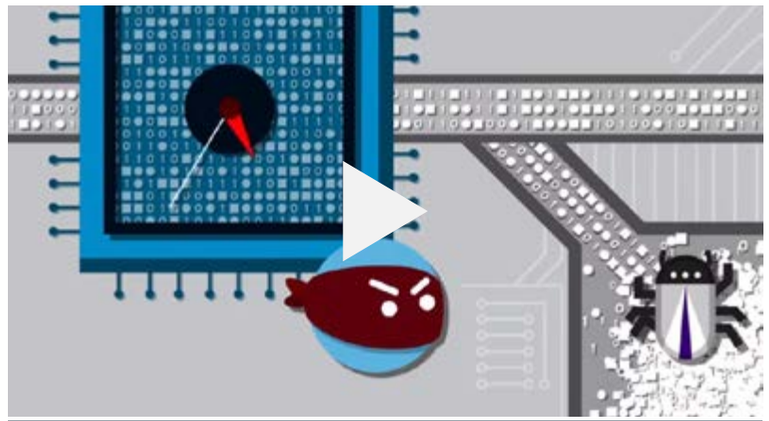
Meltdown, o CVE-2017-5754 se puede explotar para leer contenido almacenado en la memoria del kernel de un proceso de usuario sin privilegios.

Los procesadores afectados son todos los de Intel lanzados desde 1995 con excepción de los Itanium a Atom anteriores a 2013. Ningún procesador de AMD se ve afectado por esta vulnerabilidad, al contrario que algunos de ARM.

Se han lanzado parches que solucionan la vulnerabilidad para Windows y Linux. En cuanto a MacOS, ha sido parcheado desde la versión 10.12.2, el iOS desde a versión 11.2. Según Intel la vulnerabilidad de Meltdown puede ser solucionada mediante la actualización del sistema operativo sin necesidad de aplicar ninguna actualización de firmware adicional.

Decíamos antes que hay dos vulnerabilidades Spectre: CVE-2017-5753 y CVE-2017-5715. Ambas se pueden explotar para extraer información de otros procesos en ejecución en el mismo sistema. Estas vulnerabilidades afectan a procesadores de Intel, ARM y AMD.

En términos generales Spectre es más complicado de parchear que Meltdown, aunque también es más difícil de explotar. Para los expertos, explotar el fallo pasaría por utilizar JavaScript con el fil de filtrar información, claves de sesión, etc., en el navegador. Empresas como Mozilla, Google y Microsoft

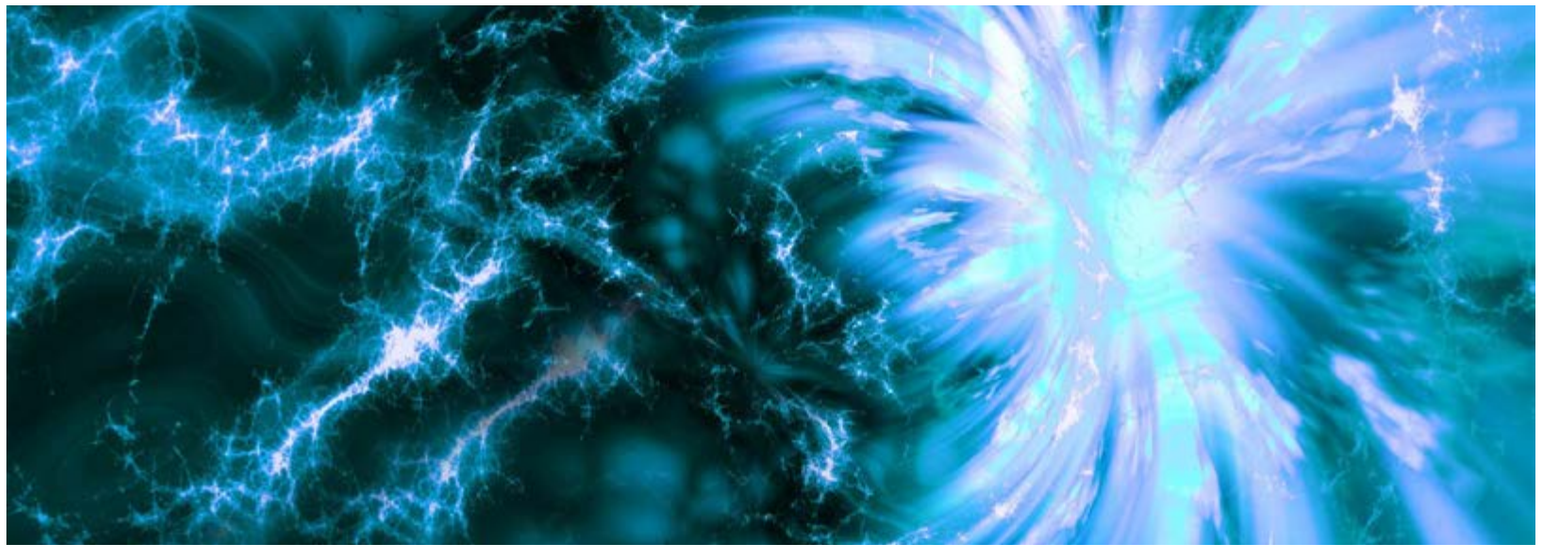


MELTDOWN Y SPECTRE EN TRES MINUTOS

CLICAR PARA VER EL VÍDEO

Cronología de un desastre

Aunque la noticia de Meltdown y Spectre se hizo pública el 3 de enero de 2018, hacía meses que se escuchaban rumores. Además, las partes implicadas ya estaban enteradas de la existencia de dos vulnerabilidades que iban a marcar un antes y un después en la historia de la informática moderna.



1/02/2017. Se asignan los números identificativos CVE-2017-5715, CVE-2017-5753 y CVE-2017-5754, que se corresponden con las vulnerabilidades Meltdown y Spectre.
01/05/2017. Aunque se desconoce la fecha exacta, sí que se tiene conocimiento de que antes de junio del año pasado los dos vectores de ataque de Spectre fueron descubiertos por investigadores del Project Zero de Google y de diferentes universidades.
01/06/2017. Los descubrimientos sobre Spectre son compartidos con Intel, AMD y ARM, los fabricantes de los procesadores afectados.
01/07/2017. También se comparte la información sobre Meltdown con Intel.
09/11/2017. Intel comparte la información sobre las vulnerabilidades con partners y otras partes interesada bajo un NDA (non-disclosure agreement).
29/11/2017. Brian Krzanich, CEO de Intel, vende 890.000 acciones de Intel por 39 millones de dólares.
13/12/2017. Apple lanza iOS 11.2, MacOS 10.13.2 y TVos 11.2. Las actualizaciones ya incorporan parches para Meltdown, pero la compañía no lo menciona hasta el 5 de enero de 2018.
15/12/2017. Amazon envía un aviso a los clientes de AWS informándoles de que habrá un reinicio programado de instancias de EC2 en torno al seis de enero de 2018. Tras ese reinicio comienzan las quejas sobre una reducción del rendimiento.
03/01/2018. Google hace públicas las vulnerabilidades asegurando que su nube yta está segura. AWS y Microsoft también publican un comunicado diciendo que sus respectivas nubes están parcheadas.
05/01/2018. Microsoft informa que su actualización de seguridad está ocasionando problemas de compatibilidad con una serie de productos antivirus. Para ayudar a prevenir errores, la compañía solo está implementando la actualización de seguridad de Windows relacionad con Meltdown en dispositivos con software AV confirmado como compatible.
09/01/2018. Microsoft detiene la actualización de PCs basados en AMD después de que estas máquinas no arrancaran tras la actualización.
10/01/2018. Microsoft comparte detalles de un potencial impacto en el rendimiento de los procesadores una vez aplicado el parche para las vulnerabilidades.
12/01/2018. Después de prometer actualizaciones de firmware para el 90% de los procesadores afectados en los últimos cinco años antes del 12 de enero, Intel lanza actualizaciones de microcódigo.
17/01/2018. Las actualizaciones de seguridad de Windows dejan a los sistemas de 32bit (x86) vulnerables a Meltdown.
18/01/2018. Microsoft reanuda el despliegue de actualizaciones para dispositivos AMD.
22/01/2018. Intel recomienda a sus clientes no aplicar actualizaciones de firmware.
30/01/2018. Microsoft lanza una actualización de emergencia para Windows que deshabilita el parche que Intel lanzó para solucionar la vulnerabilidad Spectre.

Enlaces de interés...

- Spectre
- Meltdown
- Lo que necesitas saber sobre Spectre y Meltdown
- CVE - Common Vulnerabilities and Exposures

Los códigos CVE asignados para ambas vulnerabilidades son: CVE-2017-5754 para Meltdown, y CVE-2017-5753 y CVE-2017-5715 para Spectre.

han actualizado sus navegadores para hacer este escenario exponencialmente más difícil, aunque no imposible.

Apple también ha aplicado actualizaciones en iOS 11.2.2 así como en MacOS High Sierra 10.13.2, mientras los fabricantes de procesadores actualizan los microcódigos de sus productos para evitar que Spectre sea explotado.

Reptoline, el truco de Google para parchear Spectre y Meltdown

Desde que las vulnerabilidades se hicieron públicas a principios de enero, tanto Intel como sus partners trabajaron en la implementación de los parches. No fue, ni está siendo una tarea fácil, sobre todo después de que algunos de los parches lanzados tuvieran un impacto negativo en el rendimiento de la CPU.

En todo caso Google, que fue una de las empresas que detectó los fallos, desarrolló una técnica, bautizada como Reptoline, una técnica de modificación binaria que utiliza parches de software en lugar de deshabilitar las características de la CPU afectada, por lo que, a diferencia de otras técnicas utilizadas hasta el momento, no impactaba en el rendimiento de los procesadores.

Explicaba la compañía que las secuencias de Rentoline permite aislar ramas indirectas de la ejecución especulativa, lo que permite proteger los binarios sensibles (como el sistema operativo o las implementaciones de hipervisor) de los ataques de inyección dirigido contra sus ramas indirectas. Paul Turner, ingeniero sénior de personal de infraestructura técnica en Google, dijo que el nombre de Reptoline es un acrónimo de 'return' y 'trampoline' (retorno y trampolín); es decir que se trata de un de trampolín construido utilizando operaciones de retorno, lo que asegura, de manera metafórica, que cualquier ejecución especulativa asociada rebotará interminablemente".

Google ha solicitado en diferentes ocasiones que Rentoline sea el parche implementado de manera universal. Incluso Intel reconoció que la técnica de Google podría funcionar mejor que su propio enfoque.

Compartir en RRSS

Próximos #ITWebinars

www.ittelevision.es

it televisión

El puesto de trabajo productivo:
dispositivos y tecnologías para potenciar el rendimiento

Jueves, 8 de febrero de 2018

DevOps: cómo fomentar la agilidad de tu negocio

Jueves, 1 de marzo de 2018

Gestión de vulnerabilidades

Jueves, 22 de marzo de 2018

Nuevo paradigma en la confianza

DIEGO RODRÍGUEZ ROLDÁN

DIRECTOR DE RISK ADVISORY DE DELOITTE

La labor de Diego Roldán como responsable del Centro de Innovación de Risk Advisory IT de Deloitte es aprovechar tecnologías como Blockchain, IoT, Cognitive, Big Data o Movilidad para acelerar la innovación de los clientes de la compañía.

Colaborar con direcciones técnicas y de negocio, le permite entender la innovación desde una perspectiva global que abarca tanto el nivel técnico como el valor y las oportunidades para el negocio.

Antes de formar parte en Deloite, Diego Roldán fue mentor de adventure Network, partner de KPMG España y Responsable de las operaciones, la gestión y el desarrollo de Protiviti, una firma internacional de consultoría, en España.

Desde que hace dos años, en marzo de 2016, se aprobó una directiva del SEPBLAC (Servicio de Prevención y Blanqueo de Capitales) autorizando la contratación de productos financieros de manera remota gracias a la identificación electrónica mediante el uso de nuevas tecnologías, no son pocos los avances que hemos presenciado en el área de Onboarding Digital. En este tiempo, las compañías implicadas en su desarrollo han sabido sacar el mayor partido a las distintas herramientas disponibles, combinándolas de manera que la experiencia de usuario sea cada vez más satisfactoria.

Por ejemplo, la capacidad de utilizar sistemas de reconocimiento de caracteres (OCR) para captar los datos del DNI de los solicitantes, así como la comparación biométrica en tiempo real, facilitan que la identificación del solicitante sea no sólo rápida, sino también precisa.

En este sentido, veremos muchos avances. A la implementación de la firma biométrica basada en características físicas de los individuos (huellas dactilares, retina, iris o incluso patrones faciales) que son difícilmente falsificables, o copiables, se irán añadiendo las características de comporta-

Compartir en RRSS

¿Te avisamos del próximo IT Digital Security?

A la implementación de la firma biométrica basada en características físicas de los individuos se irán añadiendo las características de comportamiento único de cada persona

miento único de cada persona, lo que significa que los sistema de autentificación no sólo reconocerán, por ejemplo, la huella dactilar de un individuo, sino también factores como la presión que suele ejercer sobre el lector, la probabilidad de que use una mano u otra según sus costumbres, el ángulo en el que normalmente apoya el dedo para que sea reconocido o el tiempo que tarda en responder a la petición de identificarse para, analizando toda esa información física y del comportamiento de usuario, reducir drásticamente, las probabilidades de error, de coacción o de un acceso fraudulento y acercarnos al fallo cero en la identificación.

Pero la tecnología no solo está revolucionando la forma de identificar a las personas. También está revolucionando, y este sí es un cambio transcendente, la forma en que confiamos entre las propias personas.

Hasta ahora, a la hora de realizar transacciones importantes, las personas no terminábamos de confiar entre nosotras y teníamos la necesidad de incluir en esas transacciones a terceras personas o entidades, normalmente, además, muy reguladas, para darnos esa confianza.

Cuando pagamos a desconocidos, lo hacemos a través de entidades financieras. Cuando compramos o vendemos una vivienda, la inscribimos en el registro de la propiedad. Las disputas y las evidencias dejamos que las valore un juez. Las transacciones importantes las hacemos delante de un notario. Pagamos las operaciones importantes “por bando” para que quede constancia. De hecho, desde que nacen, inscribimos a nuestros hijos en el registro.

NUEVE BUENAS PRÁCTICAS PARA LA SEGURIDAD DEL DIRECTORIO ACTIVO

Debido a que Active Directory (AD) es el principal directorio de autenticación y autorización para más del 90% de las empresas del mundo y alrededor de 500 millones de cuentas de usuario activas, es un objetivo común para los ciberataques. De hecho, más de 95 millones de cuentas de Directorio Activo están bajo ataque cibernético a diario.

Aunque no existe un enfoque estricto para la seguridad del AD, las organizaciones pueden tener en cuenta algunas prácticas, como las nueve que se plantean en este documento.

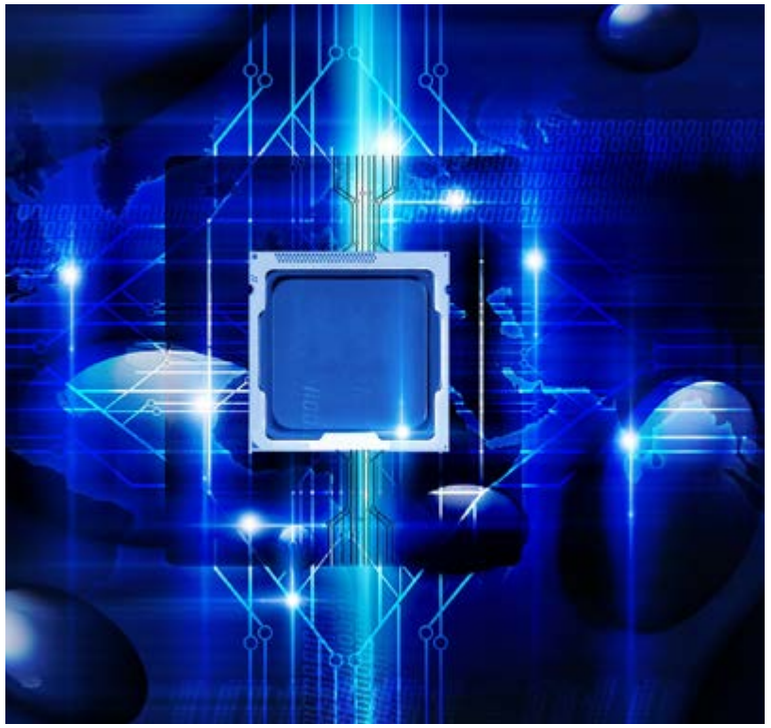
Pero este modelo también está cambiando con la tecnología blockchain. El concepto es muy sencillo, esta tecnología permite que las propias personas, independientemente de lo confiables que sean individualmente (que las habrá más y menos confiables), se den confianza entre sí como grupo sin necesidad de delegar esta confianza en ninguna persona o entidad especialmente “de fiar”, sino en la propia tecnología blockchain.

Blockchain es simplemente un archivo que todas las personas de un grupo definido comparten y en

el que lo que anota un individuo es automáticamente validado “tecnológicamente” por todo el grupo y escrito de forma “tecnológicamente” inalterable en ese archivo compartido por todos.

Esta idea sencilla revolucionará la forma en la que confiamos entre nosotros. ¿Seguiremos necesitando el registro para confiar la propiedad de nuestras casas si tenemos un registro electrónico inalterable en el que confiar? ¿Necesitaremos que alguien valide evidencias y pruebas que toda la red validó con el consenso de la mayoría y que han sido técnicamente inalterables desde que ocurrieron? Seguiremos realizando determinadas transacciones ante notarios, pero ¿lo haremos de la misma forma que hasta ahora? ¿Pagaremos por banco pudiendo pagar directamente mediante “cripto”-transacciones validadas inmediatamente por la tecnología de la propia red de individuos? ¿Confiaremos nuestra identidad, y de hecho nuestra propia existencia,

> ¿Seguiremos necesitando el registro para confiar la propiedad de nuestras casas si tenemos un registro electrónico inalterable en el que confiar?



a registros centrales cuando podemos hacer que sea el propio grupo el que de forma tecnológica, inmediata y transparente valide que somos quienes decimos que somos y que lo somos desde que nacimos?

Es evidente que seguiremos necesitando estos organismos centralizados de confianza de alguna manera, pero también lo es que cambiara la forma de utilizarlos. Y de hecho todos estos agentes ya se están adaptando para hacer posible la nueva vida digital manteniendo e incluso mejorando los niveles de garantías ofrecidos.

Las entidades financieras, pioneras en el uso de estas tecnologías, deben asegurarse de que todos sus procedimientos están alineados con los requisitos legales exigidos para su uso a la vez que aportan el máximo valor a sus clientes.

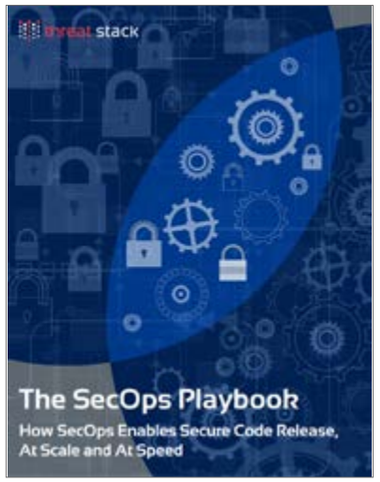
Pero esto no es fácil en el mundo digital, en el que tanto la regulación como las tecnologías y las costumbres de los usuarios cambian cada vez más rápidamente. Antes necesitábamos decenas de años para ver cambios significativos en la forma en que las personas y los mercados se relacionaban e interactuaban, pero ahora los cambios suceden cada año.

Vivimos en un mundo donde la digitalización avanza a pasos agigantados, convirtiéndose en la máxima aspiración de cualquier empresa o proceso. Es, además, una demanda cada vez más acuciante de las nuevas generaciones, aquellos que han crecido con estas tecnologías perfectamente integradas en su día a día y que quieren disfrutarlas en cualquier ámbito. Y, sobre todo, aquellos que han nacido en un entorno de cambio continuo al que están acostumbrados. Satisfacer estos requerimientos, con el mayor grado de seguridad posible, es, sin duda alguna, el motor del desarrollo futuro de estas soluciones.

En este sentido, el factor clave de éxito, dejará de ser la propia adaptación a las tecnologías actuales sino la adaptación al cambio continuo de las tecnologías, la regulación y las expectativas de un entorno en cambio constante.

Enlaces de interés...

- W Desmitificando el panorama de amenazas
- W Lagunas de conocimiento en ciberseguridad
- W ¿Qué es el blockchain?



El libro de estrategias de SecOps

Este documento explica cómo SecOps puede ayudar a que las empresas continúen lanzando código regularmente sin sacrificar la seguridad. SecOps requiere un cambio de mentalidad y cultura, y este manual describe todos los aspectos prácticos de la implementación de SecOps, incluyendo: La historia de DevOps y SecOps; ¿quién debería implementar SecOps y por qué?; los seis pasos prácticos que debes seguir para comenzar con SecOps, o los indicadores clave de rendimiento y las métricas de éxito que deberían interesarle.

Guía para encontrar la solución UBA correcta

UBA, o user behavior analytics, analiza los millones de eventos de red que sus usuarios generan todos los días para detectar credenciales comprometidas, movimientos laterales y otras actividades furtivas y maliciosas al principio de la cadena de ataques.
Pero encontrar al socio perfecto no es tan simple. Gartner predice que para 2020, menos de cinco soluciones independientes de UBA permanecerán en el mercado, y la mayoría de los proveedores se concentrarán en casos de uso y resultados específicos.

Guía para sobrevivir a los ataques BEC

A diferencia de otros ciberataques, los ataques BEC, Business Email Compromise, no incorporan malware ni URL maliciosas en los emails. En cambio, aprovechan la ingeniería social. BEC ataca a personas concretas, generalmente directores financieros o personas en los departamentos de recursos humanos, finanzas o nóminas.
Usando una técnica llamada “spoofing”, los ataques engañan a sus empleados haciéndoles creer que han recibido un correo electrónico de un jefe, compañero de trabajo, proveedor o socio.

La seguridad en un mundo de accesos remotos

Los negocios actuales, cada vez más distribuidos, no solo están incrementando las necesidades de ancho de banda, sino disolviendo los perímetros de la red, lo que a su vez incrementa las amenazas de seguridad.
Muchos ejecutivos de TI esperan que sus demandas de ancho de banda superen los 10 Gbps en 2020. Esta es solo una de las conclusiones del informe Security in a Remote Access World de iboss, que recoge que la conversación sobre empresas distribuidas va más allá del simple fortalecimiento de la infraestructura de red y un mayor y presupuesto para hardware de TI.

La Seguridad TIC a un solo clic

it Digital MEDIA GROUP
it whitepapers