itTrends

La persistencia del Ransomware

Secure&IT www.secureit.es · STORMSHIELD · panda · Bitdefender · TREND MICRO · vmware · SOPHOS · SONICWALL · eset

#ITWEBINARS

La persistencia del Ransomware

6 de cada 10 organizaciones fueron víctimas de ransomware en 2019, una cifra que va en aumento año a año debido al incremento en los pagos de rescates. Más de un tercio de las organizaciones experimentaron seis o más ataques exitosos, y el 69% esperan sufrir uno este año.

Aunque inicialmente el ransomware se utilizaba de manera aleatoria, infectando usuarios a los que se pedían rescates de cientos de dólares por recuperar el control de sus ordenadores, los ataques se han hecho mucho más dirigidos y ambiciosos, llegando a colapsar empresas e incluso ciudades. Nadie está a salvo de una amenaza difícil de rastrear.

¿Cómo hacer frente a la amenaza? ¿Qué sectores están más expuestos? ¿Cómo puedes recuperarte de un ataque de ransomware? En este IT Webinars hemos reunido a un grupo de expertos para hablar de cómo hacer frente al ransomware, una de las ciberamenazas que más preocupan a los responsables de ciberseguridad de las empresas. Contamos con la participación de Panda Security, Secure&IT, Stormshield, Bitdefender, Trend Micro, VMware, Sophos, SonicWall y ESET. A continuación, puedes leer un resumen de sus intervenciones, con los puntos más destacados. También puedes pinchar en cada una de las imágenes de sus portavoces para acceder a su intervención en el webinar o ver la sesión completa aquí. ■

Si te ha gustado este artículo, compártelo

Francisco Valencia, Secure&IT

Borja Pérez, Stormshield Iberia

Alberto Tejero, Panda Security Iberia, a WatchGuard brand

Horatiu Bandoiu, Bitdefender

José de la Cruz, Trend Micro Iberia

Francisco José Verdugo, VMware

Alberto Rodas, Sophos

Sergio Martínez, SonicWall Iberia

Josep Albors, ESET España

FRANCISCO VALENCIA, DIRECTOR GENERAL, SECURE&IT

"A futuro, el ransomware va a ser muchísimo más duro de lo que es ahora"

El año pasado, el 51% de las empresas sufrieron un ataque de ransomware, y en el 73% por ciento de las ocasiones los datos acabaron siendo cifrados. De esta amenaza hablamos con Francisco Valencia, director general de Secure&IT, en la sesión online La Persistencia del Ransomware.

Asegura el directivo que las empresas tienen una falsa sensación de seguridad, que no creen que el malware les vaya a afectar, ni que vayan a sufrir un ataque. Pero lo cierto es que hay una amenaza muy clara, "hay grandísimos grupos de ciberdelincuencia organizada con distintos motivos que utilizan cientos o miles de herramientas distintas para poder lanzar sus ciberataques". El ransomware, dice Francisco Valencia, se ha convertido en el ataque más mediático, "por lo tanto genera un impacto no solamente sobre los datos que se han perdido o sobre la operación que se ha dejado hacer, sino también desde el punto de vista re-

FRANCISCO VALENCIA, DIRECTOR GENERAL, SECURE&IT

“El ransomware es un malware democrático, en el sentido que ataca a todas las empresas de todos los tamaños y todos los sectores”

putacional”. Es, además, “un tipo de malware que ataca a todas las empresas de todos los tamaños y todos los sectores”, que también se utiliza para ataques dirigidos y que genera enormes cantidades de dinero a los ciberdelincuentes que lo explotan.

“El futuro inmediato es un ransomware que va a ser muchísimo más duro de lo que es ahora”, porque si hasta ahora lo que ocurría es que se cifraban los datos, las nuevas versiones de esta lacra los roban y amenazan con hacerlos públicos si no se paga el rescate, “lo que puede tener un impacto mucho mayor”.

Asegura también Francisco Valencia que los ataques de ransomware han evolucionado hasta el punto de que ahora eliminan las copias que están en el shadow copy, son capaces de detectar y evadir técnicas de sanboxing, utilizan múltiples vectores de ataque, afectan a todos los sistemas operativos y emplean mecanismos de cifrado tremendamente avanzados.

Entre las medidas que se pueden tomar, menciona el director general de Secure&IT que el ransomware no es sólo un problema informático, sino de información, y que hay cuatro vectores fundamentales en los que la alta dirección de una empresa tiene que trabajar: cumplimiento normativo, procesos corporativos, seguridad informática y vigilancia de la seguridad.

Vea aquí la intervención de Secure&IT en La Persistencia del Ransomware

Si te ha gustado este artículo, compártelo

SECURE&IT. SEGURIDAD 360º

Secure&IT es una empresa española que cuenta con un equipo de auditores que trabajan de manera integrada en el análisis de riesgos de las empresas, siendo uno de los mayores la protección inadecuada de la información. La compañía cuenta con su propio SOC, que ha sido reconocido como CERT y que está dotado de sistemas y procesos avanzados, pudiendo monitorizar,lk vigilar, registarar, gestionar y actuar de manera inmediata ante eventos que afecten a la seguridad de la información de su empresa.

BORJA PÉREZ, DIRECTOR GENERAL, STORMSHIELD

"Es necesario entender cómo se ha producido el ataque"

El 26% por ciento de las víctimas de un ataque de ransomware en el que los datos se han cifrado, pagan el rescate. Hablamos con Borja Pérez, director general de Stormshield Iberia, en la sesión online La Persistencia del Ransomware sobre cómo ha percibido su compañía la evolución de esta amenaza, sobre la que asegura que antes de 2016 hablar de ransomware era hablar de CryptoLocker y que con Wannacry esta amenaza apareció en los medios de comunicación. Tras un descenso en 2018, "probablemente porque los cibercriminales orientaron sus esfuerzos hacia la minería de bitcoin", el ransomware no ha dejado de crecer y la nueva tendencia es no sólo cifrar los datos, sino amenazar con hacerlos públicos".

Este tipo de ataques, dice Borja Pérez, "está afectando a todos los sectores" y se producen tanto de manera masiva como más dirigidos, "un ataque más sofisticado que requiere más inversión también por parte de los delincuentes".

BORJA PÉREZ, DIRECTOR GENERAL, STORMSHIELD

"Tener nuestros datos convenientemente cifrados significa que lo que se está llevando el atacante es pura basura criptográfica, información a la que no puede acceder"

¿Cómo se puede hacer frente al ranwomware? Menciona el director general de Stormshield Iberia algunas medidas "que no son tan complicadas", como es tener un backup junto con una solución de disaster recovery, así como algunas medidas de seguridad básicas que protejan el puesto de trabajo y el perímetro, junto con una solución de cifrado de datos.

Las medidas coinciden con la propuesta de Stormshield, centrada en: Network Security, Endpoint Security y Data Security. Sobre Stormshield Endpoint Security dice Borja Pérez que es un agente ligero que se instala en los puestos y monitoriza el comportamiento de los procesos, bloqueando el que no sea legítimo –y no la aplicación para que el usuario pueda seguir trabajando. Este agente también protege las conexiones o dispositivos que se puedan conectar a él, bloqueando lo que no esté permitido por la organización. Menciona el directivo la tendencia del mercado hacia los EDR, o lo que es lo mismo, no sólo la detección, sino también la respuesta, "y entender cómo se ha producido el ataque, que debilidad ha encontrado el atacante y como lo está intentando hacer para mitigar posibles futuros ataques".

La red también es importante y es vital saber lo que está pasando en el tráfico. Sobre el cifrado dice Borja Pérez que no es una mediante anti ransomware como tal, pero que teniendo en cuenta que la tendencias de los últimos ataques de ransomware es hacer públicos datos o de robarlos, el tener nuestros datos convenientemente cifrados significa que "lo que se está llevando el atacante es pura basura criptográfica, información a la que no puede acceder".

Vea aquí la intervención de Stormshield en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

STORMSHIELD ENDPOINT SECURITY

Los ataques de hoy son cada vez más selectivos y sofisticados en un intento por eludir los sistemas de protección convencionales. Utilizan técnicas de infección avanzadas, como la explotación de vulnerabilidades desconocidas, y emplean mecanismos sofisticados para pasar desapercibidos en el sistema operativo. Las amenazas ya no se limitan a las redes: ahora se extienden a entornos sensibles o industriales donde el impacto potencial es considerable (riesgos de deterioro físico, parada de la línea de producción, etc.).

ALBERTO TEJERO, DIRECTOR GENERAL DE PANDA SECURITY IBERIA, A WATCHGUARD BRAND

"Tenemos un problema de concienciación"

Sólo el 64 por ciento de las empresas que tienen un ciberseguro están cubiertas por el ransomware, una amenaza que cada vez preocupa más a los responsables de las empresas y de la que hablamos con Alberto Tejero, director general de Panda Security Iberia, una compañía de WatchGuard, quien comienza explicándonos que los problemas de ciberseguridad se han incrementado junto con el teletrabajo, que ha tenido que adoptarse a gran escala en pocas semanas o incluso días.

Durante la sesión online La Persistencia del Ransomware, dice Alberto Tejero que el phishing es una de las maneras en las que se ha propagado el ransomware. Ha habido un incremento del número de correos enviados en los últimos tiempos, lo que ha sido aprovechado por los ciberdelincuentes para enviar mensajes maliciosos con información sobre el confinamiento y el virus.

Otra vía de propagación del ransomware ha sido a través de vulnerabilidades en el softwa-

ALBERTO TEJERO, DIRECTOR GENERAL DE PANDA SECURITY IBERIA, A WATCHGUARD BRAND

“La propuesta de Panda Security pasa por Adaptive Defense 360, una solución EDR en la que se combinan diferentes capas de seguridad”

re, algo que ya vimos en los casos de Wannacry y Petya. “Pero sobre todo hay mucho phishing”, asegura el directivo de Panda Security.

La mayor complejidad en los ataques y los mensajes de phishing cada vez más dirigidos y profesionalizados hace que “los usuarios necesiten una solución un poco más avanzada”. La propuesta de Panda Security pasa por Adaptive Defense 360, una solución EDR en la que se combinan diferentes capas de seguridad, empezando por una tecnología de firmas y heurística para la detección de ataques, “como cualquier solución de seguridad antivirus tradicional”; una segunda capa de detección contextual que permite detectar ataques sin ficheros para pasar a una tecnología antiexploit “que también nos permite detectar ataques fileless que explotan vulnerabilidades.

A estas cuatro primeras capas le siguen otras dos. Un servicio gestionado que permite clasificar todo lo que se ejecuta en las máquinas, lo que permite detener ataques en la red interna y por movimientos laterales. La solución Adaptive Defense monitoriza todos los procesos en ejecución para permitir únicamente la ejecución de los clasificados como confiables por Panda Security

Y finalmente, algo que según Tejero les diferencia: un servicio de Threat Hunting, “en el que no sólo vemos los ataques de ransomware, sino de suplantación de identidad”.

Asegura Alberto Tejero que el mercado tiene un problema de concienciación y que el mercado tiene que darse cuenta de que teletrabajar en casa y estar en una oficina “no implica los mismos procedimientos de seguridad”.

Vea aquí la intervención de Panda Security en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

PANDA SECURITY REPORT. SODINOKIBI

Este documento recoge el análisis de una muestra del Ransomware “Sodinokibi”, también conocido como REvil, que apareció a lo largo de la primera mitad de 2019 y se caracteriza por su gran capacidad de evasión y el gran número de medidas que toma para evitar ser detectado por los motores antivirus.

HORATIU BANDOIU, CHANNEL MARKETING MANAGER ESPAÑA & LATAM, BITDEFENDER

"Es importante entender que cualquier organización puede ser un blanco de los atracadores"

Los cibercriminales consiguieron cifrar datos en el 73% de los ataques de ransomware lanzados el año pasado. En la sesión online La Persistencia del Ransomware aporta Horatiu Bandoiu, Channel Marketing Manager España & LATAM de Bitdefender,otros datos del mundo de la seguridad, extraídos de una encuesta realizada en diferentes países que recoge, entre otras cosas que el 63% de los responsables de ciberseguridad considera que estamos en una ciberguerra, que el 27% de las empresas no tienen una estrategia de seguridad o que el 72% creen que hay necesidad de un tipo más diverso de habilidades en la ciberguerra.

Sobre el ransomware dice el directivo de Bitdefender que los ataques se están incrementando "pero que la protección contra ellos no ha avanzado mucho en los últimos años", a pesar de lo cual 3 de cada 5 han reforzado sus infraestructuras y están prestando atención a la formación de los empleados en ciberse-

HORATIU BANDOIU, CHANNEL MARKETING MANAGER ESPAÑA & LATAM, BITDEFENDER

“A los responsables de ciberseguridad les preocupa no sólo el impacto reputacional de un ataque de ransomware, sino las multas”

guridad, sobre todo ahora que muchos están teletrabajando. A los responsables de ciberseguridad les preocupados no sólo el impacto reputacional de un ataque, sino las multas, por lo que uno de cada seis está creando una partida presupuestaria para ello.

Tras mencionar el caso de Garmin, que el verano pasado sufrió un ataque de ransomware que dejó sin cobertura a sus clientes, dice Horatiu Bandoiu que “es importante entender que cualquier organización puede ser un blanco de los atracadores”.

Bitdefender, cuyas soluciones de seguridad han alcanzado la tercera generación, ofrece “un approach integrado” para lucha frente al ransomware. Explica el directivo de la compañía que la primera generación fue la de prevención; la segunda generación incorporó tecnología de próxima generación y EDR, “pero hemos visto que en menos de un año los atacantes ya se han adaptado”, lo que ha llevado a la compañía a adoptar una aproximación diferente, basado en ciberresiliencia, “que significa estar preparados para responder en cualquier momento en un ciclo que no acaba nunca, en el cual tienes que entender tus riesgos de seguridad, poner medidas de prevención, pero estar preparado para detectar las señales de que has sido atacado y responder, reduciendo los riesgos de seguridad”.

La clave pasa por GravityZone Enterprise, una suite completa capaz de prevenir, detectar, investigar, dar una respuesta adecuada y reforzar el sistema. Clave es también mantener una actitud ciberresiliente, lo cual significa tener capas de protección y tecnologías que buscan reducirla superficie de ataque, reforzar la capa de red “para poder identificar las técnicas de ataque, tecnologías de detección de ataques o tecnologías de detección y respuesta para una contención automática.”

Vea aquí la intervención de Bitdedfender en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

BITDEFENDER GRAVITYZONE ULTRA PLUS

Las soluciones tradicionales de detección y respuesta en los endpoints se basan únicamente en el análisis de datos de los endpoints para detectar las amenazas digitales. GravityZone Ultra Plus utiliza un modelo XDR y aplica el Machine Learning, la correlación de eventos y la inteligencia sobre amenazas a los datos recopilados desde todos los elementos de la infraestructura empresarial: endpoints (físicos o virtualizados), recursos en la nube y elementos de red.

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO, TREND MICRO

"No debemos pagar nunca el rescate"

Pagar el rescate duplica el coste de un ataque de ransomware. Sobre esta amenaza dice José de la Cruz, director técnico de Trend Micro, que es un malware como otro cualquiera que lo que hace es infectar a un usuario, propagarse de manera muy rápida y secuestrar máquinas, sistemas operativos o información, cifrando archivos y carpetas.

En la sesión online La Persistencia del Ransomware asegura también el directivo de Trend Mico que el atacante quiere obtener una rentabilidad económica y explica la evolución de la amenaza desde que apareciera hacia 1989 con el AIDS Trojan hasta nuestros días, cuando los atacantes no sólo cifran la información y piden un rescate por ella, sino que amenazan con hacerla pública si no se paga el rescate, lo que puede tener un impacto muy grande de cara a normativas como GDPR.

¿Cómo pueden afrontar las empresas la lucha contra el ransomware? Ofrece José de la Cruz una serie de recomendaciones genéricas que empiezan con que no debemos pagar nunca el rescate porque, entre otras cosas, "no tenemos ninguna certeza de que nos vayan a devolver la información, y no tenemos ninguna certeza de que, aunque hayamos pagado, no vayan a continuar extorsionándonos una y otra vez". Aislar nuestro entorno de Internet para impedir que el ataque prospere, apagar

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO, TREND MICRO

“No tenemos ninguna certeza de que, aunque hayamos pagado, no vayan a continuar extorsionando una y otra vez”

cualquier sistema prescindible, ir recuperando los servicios de manera progresiva o hacer uso de herramientas EDR y analizadores de red son otras de las recomendaciones del director técnico de Trend Micro.

A la hora de prevenir, dice José de la Cruz que es necesario tener una copia de seguridad externa, “y cuando digo externa me refiero que no estoy relacionada directamente con nuestro sistema, es decir, que el atacante no la pueda corromper y que sea robusta”. Añade el directivo la necesidad de contar con una solución de parchado de sistemas físico y virtual, como puede ser la solución de Virtual Patching de Trend Micro. “No demos acceso libre a internet, ni a usuarios ni al sistema”, recomienda José de la Cruz, añadiendo que es necesaria una formación y concienciación del usuario y una supervisión continua.

En la parte de protección contra las amenazas de seguridad, incluido el ransomware, Trend Micro cuenta con diferentes productos para cada una de las fases de un ataque: entrada, infección, ejecución y limpieza. Entre la batería de productos menciona el directivo de Trend Micro un motor antispam, protección para la navegación, un buen motor antimalware que incorpore tecnología no solo basadas en machine learning sino en análisis de comportamiento, una sandboxing y una buena tecnología de EDR para la fase de limpieza “que nos aporte visibilidad de lo que está ocurriendo”.

Para la parte de concienciación se propone PhishInsight, una herramienta gratuita que permite hacer formación a los empleados y enseñarles cómo hacer frente a un ataque de phishing, por ejemplo.

Vea aquí la intervención de Trend Micro en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

PROTECCIÓN DEL LUGAR DE TRABAJO INTERRUMPIDO POR LA PANDEMIA

En un momento en el que muchas operaciones comerciales están inmovilizadas o incluso al borde del cierre, los cibercriminales continúan prosperando. Estos ciberdelincuentes se aprovechan de la crisis actual planteando nuevas amenazas y reforzando las existentes. Incluso con menos detecciones, el ransomware sigue siendo una amenaza a medida que los cibercriminales dotan con nuevas capacidades para apuntar a objetivos más grandes.

FRANCISCO JOSÉ VERDUGO, SENIOR PARTNER SOLUTION ENGINEER, VMWARE

"Necesitamos un nuevo enfoque de seguridad que se fije más en el contexto"

El ransomware se ha convertido en una auténtica pesadilla para los responsables de ciberseguridad de las empresas. En la sesión online La Persistencia del Ransomware hablamos con Francisco José Verdugo, Senior Partner Solution Engineer de VMware, quien explica que nunca se ha tenido en cuenta sobre qué infraestructura se está ejecutando la amenaza, sobre qué usuario o dispositivo, a lo que se añade el problema de que "tenemos una cantidad ingente de vendedores de seguridad" y que siempre se ha hablado de una seguridad por capas. "La seguridad debe ser un deporte de equipo, que forme parte de la infraestructura, y que se centre en el contexto", asegura Verdugo.

Desde VMware proponen un nuevo enfoque que se fije "en quién soy, con quién me hablo, dónde me estoy ejecutando, en qué sistema operativo estoy corriendo o dónde estoy para ser capaces de detectar ya no solamente lo co-

FRANCISCO JOSÉ VERDUGO, SENIOR PARTNER SOLUTION ENGINEER, VMWARE

“Nunca se ha tenido en cuenta sobre qué infraestructura se está ejecutando la amenaza, sobre qué usuario o dispositivo”

nocido, sino también lo desconocido”, explica el directivo. A nivel de red se cuenta con NSX; en la parte de Cloud en relación con toda la parte de gobernanza con una solución que se llama Secure State; para la parte de cargas de trabajo y servidores virtuales la propuesta de VMware es vSphere; para gestionar la seguridad de los dispositivos, controlar aplicaciones y el control de identidades y de usuarios se utiliza Workspace One.

¿En qué consiste la Seguridad Intrínseca? “En dar de base esa capa de seguridad que en este caso proporciona Carbon Black, una compañía que se compró en agosto de 2019 y cuya inteligencia se está integrando en los distintos ámbitos”. Y la compra de Octarine, ¿cómo impacta en esta visión de la ciberseguridad? Explica Francisco José Verdugo que las aplicaciones de nueva generación siguen un modelo basado en contenedores donde los modelos de seguridad son muy distintos, “Octarine viene a cubrir una necesidad dentro de ese ámbito por su capacidad de proteger un entorno Kubernetes en cualquiera de las fases de vida”. Volviendo a la filosofía de una única consola, de una gestión simplificada, por lo que se opta es por integrar toda la funcionalidad de Octarine dentro de Carbon Black.

Sobre el ransomware dice el ejecutivo de VMware que “podemos decir que tenemos un cien por cien de efectividad contra él”. Propone además una serie de buenas prácticas que van desde la creación regular de copias de seguridad, aplicar los parches, utilizar antivirus de nueva generación capaz de detectar ataques que no estén en la memoria, o implementar programas de formación o concienciación.

Vea aquí la intervención de VMware en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

SEGURIDAD INSTRÍNSECA FOR DUMMIES

La seguridad intrínseca es un enfoque fundamentalmente diferente para proteger su negocio. No es un producto, una herramienta o un paquete para su organización, sino una estrategia para aprovechar su infraestructura existente y puntos de control de nuevas formas, en tiempo real, en aplicaciones, nubes y dispositivos.

ALBERTO RODAS, SALES ENGINEER MANAGER IBERIA REGION, SOPHOS

"Se necesitan herramientas de nueva generación capaces de detectar comportamiento"

El 59% de los ataques con éxito cifraron datos que estaban almacenados en la nube pública. Durante la sesión online La Persistencia del Ransomware Alberto Rodas, Sales Engineer Manager Iberia Region de Sophos, asegura que la mitad de las empresas sufren un ataque de ransomware que tiene éxito en el 73% de las ocasiones. Añade el directivo que el coste promedio de la remediación de estos ataques son unos 760 mil dólares, que afectan a todos los sectores y que se utilizan múltiples técnicas para tener éxito.

El ataque de ransomware típico acaba con el cifrado de datos, algo que a menudo ocurre durante el fin de semana o aprovechando algún festivo, y suele iniciarse con un correo o enlace malicioso que afecta a un puesto, desde el que empieza a extenderse.

Propone Alberto Rodas unas buenas prácticas contra el ransomware, empezando por contar con una buena solución de seguridad.

ALBERTO RODAS, SALES ENGINEER MANAGER IBERIA REGION, SOPHOS

“El ataque de ransomware típico acaba con el cifrado de datos, algo que a menudo ocurre durante el fin de semana”

Menciona el directivo de Sophos que muchas empresas cuentan con productos obsoletos, basados sólo en firmas y que se necesitan herramientas de nueva generación capaces de detectar comportamiento y detectar técnicas de explotación.

Se debe reducir la superficie de ataque, por lo que “si no necesito ciertos servicios, hay que quitarlos”. Una tercera buena práctica es el uso de VPN para accesos remotos de forma que nunca exponga mis sistemas a internet. El uso de autenticación multifactor es importantísimo, dice Alberto Rodas, así como prevenir los movimientos laterales.

Propone el directivo una arquitectura de red con Sophos XG Firewall y Sophos Intercept X EDR capaz de identificar todo lo que está ocurriendo en la red de la empresa, e incluso la monitorizando de aplicaciones cloud, pudiendo decir “cuáles son las permitidas y cuáles no”.

A nivel de puesto de trabajo se cuenta con Sophos Intercept X con capacidades de detección en tiempo de ejecución y control de comportamiento para detectar esa ejecución de ransomware, la propagación o el cifrado no deseado. “Pero además tenemos los servicios de detección y respuesta, donde con el módulo EDR el cliente puede realizar acciones, o hacerlas nosotros a través de Managed Threat Response, nuestro servicio de EDR gestionado”.

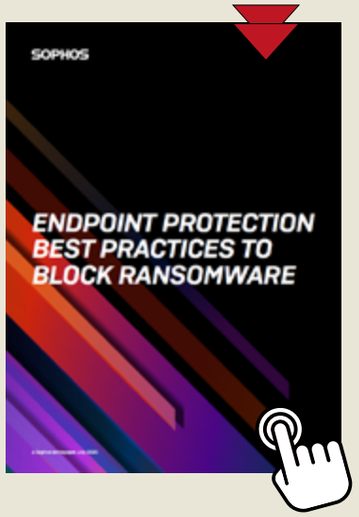
Muy interesante también la parte de Threat Hunting, un servicio en el que Sophos ha pre-establecido una serie de queries que se pueden adecuar a las necesidades de cada cliente.

Vea aquí la intervención de Sophos en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

it whitepapers

MEJORES PRÁCTICAS PARA BLOQUEAR EL RANSOWMARE



Uno de los métodos más efectivos para protegerse contra los ataques de ransomware es con una solución de protección de endpoints configurada correctamente. En este documento técnico, analizaremos cómo funcionan los ataques de ransomware, cómo se pueden detener y las mejores prácticas para configurar su solución de punto final para la protección más sólida posible.

SERGIO MARTÍNEZ, DIRECTOR GENERAL, SONICWALL IBERIA

"Hemos visto todo tipo de estrategias para conseguir ataques cada vez más dirigidos"

El 50% de los responsables de ciberseguridad está convencido de que su empresa pagaría un rescate para evitar la publicación de sus datos. Durante la sesión online La Persistencia del Ransomware hablamos con Sergio Martínez, responsable de SonicWall para la región de Iberia, sobre ransomware y lo que está ocurriendo en el mundo de la seguridad. Dice el directivo que esta pandemia ha sido una bendición para los cibercriminales, ya que "mientras que las empresas y las organizaciones tenían que dedicarse a sobrevivir, los cibercriminales han estado sacando tajada de esto".

Según los informes de SonicWall, el ransomware está creciendo globalmente. Durante la pandemia "hemos visto todo tipo de estrategias para conseguir ataques cada vez más dirigidos y sobretodo basados en ransomware", dice el directivo, explicando también que el RTDMI de la SonicWall, el algoritmo desarrollado por la compañía para realizar detecciones a nivel de sand-

SERGIO MARTÍNEZ, DIRECTOR GENERAL, SONICWALL IBERIA

“Hemos identificado una serie de productos y servicios que necesitan las empresas y hemos construido un SMB Pack para pymes”

boxing, ha detectado más de 120.000 variantes de malware nunca identificados. El informe de la compañía recoge también un crecimiento de los ataques a puertos no estándar así como de las amenazas encriptadas.

La propuesta Boundless Cybersecurity de la compañía se basa en el gap hay que entre lo que se necesita a nivel de seguridad y el presupuesto que pueden invertir las empresas para: conocer lo desconocido; tener un punto de visibilidad y control sobre lo que está sucediendo y ayudar a las empresas con estrategias y dispositivos que sean asumibles por los clientes.

“Hemos identificado una serie de productos y servicios que necesitan las empresas y hemos construido un SMB Pack para pymes”, asegura Sergio Martínez, diciendo que la idea es juntar un firewall fácil de instalar con un software para gestionarlo todo; un punto de acceso o puntos de acceso; un switch POE para dar alimentación a los puntos de acceso; seguridad para Office 365 y una antivirus de nueva generación, todo esto en una oferta basada en componentes.

Recuerda también Sergio Martínez que se ha lanzado recientemente la Generación 7 de los productos de la compañía; “se ha renovado nuestro sistema operativo y nuestro hardware”. Entre las mejoras el multiplicar el rendimiento de dispositivos “por dos, por tres, incluso por cuatro, con softwares para configurarnos en remoto”. Recientemente se han presentado los nuevos switches, que se gestionan también desde el mismo punto de gestión en la nube. La última línea de defensa es Capture Client, un antivirus basado en lo mejor del mercado “que añade nuestros algoritmos de detección de malware para tener un gran producto que dar seguridad a nuestros clientes”.

Vea aquí la intervención de SonicWall en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

INFORME SOBRE CIBERAMENAZAS 2020 DE SONICWALL

El Informe sobre Ciberamenas 2020 de SonicWall proporciona información detallada y un análisis exhaustivo del panorama de ciberamenazas. Entre los principales hallazgos del informe destaca que los ataques de ransomware dirigido están creciendo, que el cryptojacking continúa desmoronándose o que el Internet de las Cosas (IoT) es un tesoro para los ciberdelincuentes.

JOSEP ALBORS, DIRECTOR DE INVESTIGACIÓN Y CONCIENCIACIÓN, ESET ESPAÑA

"Hay que distinguir entre el ransomware genérico y el dirigido, mucho más peligroso"

El ransomware también está presente en la plataforma Android; entre los primeros ataques, uno detectado en Canadá bajo el disfraz de una aplicación de rastreo COVID-19. En la sesión online La Persistencia del Ransomware dice Josep Albors, responsable de investigación y concienciación de ESET España, que muchas personas y empresas siguen pensando en el ransomware como una amenaza que no ha variado en años. Sin embargo, "estamos hablando de una amenaza que no ha dejado de evolucionar en este tiempo y que ahora tiene muchas familias, muchas variantes y nuevas y peligrosas consecuencias", asegura el directivo explicando que en un ataque de ransomware hay varias etapas, desde la explotación o infección, que les permite colarse en la empresa, para pasar a una segunda fase en la que el ransomware hace un reconocimiento de la red empresarial para ver qué equipos o qué información es más interesante para robarla y enviarla a los servidores controlados por delincuentes. Y una fase final que es la extorsión

JOSEP ALBORS, DIRECTOR DE INVESTIGACIÓN Y CONCIENCIACIÓN, ESET ESPAÑA

“Hemos pasado de una amenaza cuyo máximo temor por parte de los usuarios era que te cifren los archivos, a una amenaza cuyo miedo actual es que los archivos sean robados y filtrados”

o filtrado de datos, lo que coloca a las empresas a un paso de incumplir normas como GDPR. “Emotet es una de las variantes que hemos visto evolucionar en base a este nuevo modelo de negocio”, dice Jose Albors.

Respecto a los vectores de ataque que utiliza el ransomware, el principal, asegura Josep Albors, es el compromiso mediante RDP, o escritorio remoto, muy explotado debido al aumento por el teletrabajo, seguido del phishing y las vulnerabilidades de software.

“Hay que distinguir entre un rasomware genérico, que una pyme podría afrontar, incluso un usuario particular, en el que hay un ataque clásico de cifrado, y los ataques dirigidos”, explica el directivo de ESET añadiendo que se ha visto un aumento muy elevado de ataques dirigidos a empresas multinacionales con una facturación muy elevada y que son víctimas de este tipo de ataques dirigidos, y algunos sectores, como la administración pública, infraestructuras sanitarias, centros de investigación o infraestructuras críticas.

Habla también Josep Albors del Ransomware como servicio, y explica que los ciberdelincuentes se dedican a crear kits de generación de ransomware para que otros delincuentes con mucho menos conocimiento técnico, o directamente sin apenas conocimiento técnico, puedan con unos cuantos clicks crear su propia amenaza y empezar a ganar dinero.

Termina el directivo de ESET ofreciendo una serie de consejos para hacer frente al ransomware: contar con una buena copia de backup; tener la información cifrada para que al usuario no le sirva de nada; y contar con una solución para la monitorización de la actividad de la red para detectar posibles amenazas.

Vea aquí la intervención de ESET en La Persistencia del Ransomware. ■

Si te ha gustado este artículo, compártelo

it whitepapers

RANSOMWARE DESDE EL PUNTO DE VISTA EMPRESARIAL

Los objetivos de este documento son explicar por qué el ransomware sigue siendo una amenaza grave para su organización, independientemente de su tamaño, y qué puede hacer su organización para reducir la exposición y el daño de los ataques de ransomware.