SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]

AÑO 01 EDICIÓN 2.96

WWW.COREONEIT.COM
@COREONEIT

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

¿QUÉ ES EL SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]?

Es una combinación de información de amenazas existentes en la red con el análisis e inteligencia del grupo de especialistas de CORE ONE IT, quienes analizan exhaustivamente todo tipo de amenazas informáticas y desarrollan una serie de recomendaciones adaptadas a cada tipo de cliente.

ALCANCE

Se personaliza de acuerdo al tipo de infraestructura y entorno de red del cliente basado en los tipos de dispositivos, modelos y fabricantes, con el fin de recibir solo información relevante y que pudiera afectar de manera directa o indirecta, la continuidad del negocio.

DEFINICIONES

•Riesgo: Probabilidad que una amenaza particular explote una vulnerabilidad particular de un sistema.

•Amenaza: Es la causa potencial de un incidente no deseado, el cual puede resultar en un daño a un sistema de información u organización.

•Ataque: Acción de tratar de traspasar controles de seguridad en un sistema. Un ataque puede ser activo, resultando en la modificación de datos, o pasivo, resultando en la divulgación de información. El hecho de que un ataque sea realizado no significa que será exitoso, el grado de éxito depende de la vulnerabilidad del sistema o actividad y de la eficiencia de las medidas existentes.

•Vulnerabilidad: Debilidad en los procedimientos de seguridad de un sistema, en el diseño del sistema, en la implementación, en los controles internos, y que puede ser explotada para violar la política de seguridad del sistema.

•API: Interfaz de Programación de Aplicaciones (Application Programming Interface, por sus siglas en inglés). Conjunto de subrutinas, funciones y procedimientos de una biblioteca para ser utilizado por otro software.

•Malware: también llamado badware, código maligno, software malicioso, software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

•Ransomware: Es un tipo especial de malware que amenaza con destruir los documentos y otros archivos de las víctimas.

•Troyano: Software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo.

•ISP: Proveedor de servicios de Internet (Internet Service Provider, por sus siglas en inglés).

•Keylogger: Software de vigilancia, el cual cuenta con la capacidad de grabar cada tecla pulsada en el sistema en un archivo, usualmente cifrado.

•BSOD: Blue Screen Of Death, “pantalla azul de la muerte”; se refiere a la pantalla mostrada por el sistema operativo de Windows cuando éste no puede recuperarse de un error del sistema.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

¿HAS RECIBIDO UN CORREO DEL BANCO SOBRE UNA NUEVA NORMATIVA EUROPEA PARA LA SEGURIDAD? NO LO ABRAS, ES UNA ESTAFA.LINUX MÁS SEGURO

Cuando navegamos por Internet podemos toparnos con muchos problemas de seguridad. Muchos tipos de malware que pueden comprometer nuestro sistema. Pero si hablamos de una amenaza que está cada vez más presente es lo que se conoce como Phishing. Como sabemos, es el tipo de ataque por el que un ciberdelincuente busca robar las credenciales y contraseñas de los usuarios. Lo podemos recibir por correo electrónico, SMS, redes sociales… Hoy vamos a hacernos eco de una nueva amenaza de este tipo que se hace pasar por un banco alertando a los usuarios de que deben actualizar sus cuentas.

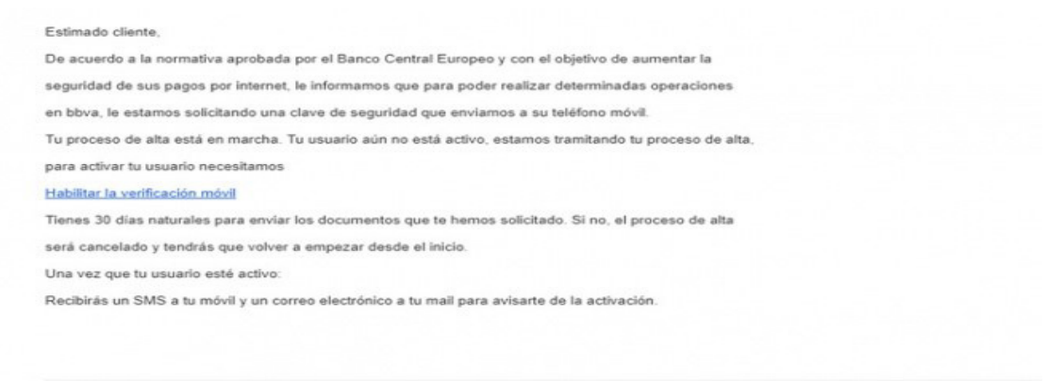
Un nuevo ataque Phishing pide activar la cuenta del banco

Hay que mencionar que con el paso del tiempo los ciberdelincuentes perfeccionan sus técnicas. Podemos encontrarnos con mensajes de este tipo escritos mal, faltas de ortografía o malas traducciones. Sin embargo cada vez parecen más "reales". En el ejemplo que ponemos, incluso agregan una imagen del banco.

En este caso el cebo que utilizan es hacer creer a los usuarios que tienen que activar su usuario del banco para adaptarse a la nueva normativa aprobada por el Banco Central Europeo. Todo ello con el objetivo de mejorar la seguridad de sus cuentas y de esta forma poder pagar por Internet sin comprometer sus datos.

Claro, los usuarios valoran mucho su seguridad. Pueden alertarse y creer que necesitan activar su usuario o configurarlo para no tener problemas de seguridad. Esto puede hacer que entren en el link donde les lleva a la supuesta página para activar su usuario y tener todo en orden.

Lógicamente al hacer clic en ese enlace lleva a una web controlada por los ciberdelincuentes. Lo que buscan es hacerse con las credenciales de acceso.



Estimado cliente,

De acuerdo a la normativa aprobada por el Banco Central Europeo y con el objetivo de aumentar la seguridad de sus pagos por internet, le informamos que para poder realizar determinadas operaciones en bbva, le estamos solicitando una clave de seguridad que enviamos a su teléfono móvil.

Tu proceso de alta está en marcha. Tu usuario aún no está activo, estamos tramitando tu proceso de alta, para activar tu usuario necesitamos

Habilitar la verificación móvil

Tienes 30 días naturales para enviar los documentos que te hemos solicitado. Si no, el proceso de alta será cancelado y tendrás que volver a empezar desde el inicio.

Una vez que tu usuario esté activo:

Recibirás un SMS a tu móvil y un correo electrónico a tu mail para avisarte de la activación.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Como vemos en la imagen de arriba, indican que el proceso de alta está en marcha pero aún no está activo. Piden verificar la cuenta para poder enviar un código por SMS para mejorar la seguridad del usuario. Además, informan de que hay 30 días naturales de tiempo para poder enviar todos los documentos que piden. Una vez pase ese tiempo, en caso de no enviarlos habría que reiniciar todo el proceso de nuevo.

FUENTES:

Javier Jiménez. (2019). ¿Has recibido un correo del banco sobre una nueva normativa europea para la seguridad? No lo abras, es una estafa. 12 abril, 2019 , de Redes@Zone Sitio web: https://www.redeszone.net/2019/04/12/ataque-phishing-pide-activar-cuenta-bancaria/

VULNERABILIDAD DÍA CERO EN ENRUTADORES TP-LINK EXPONE LOS DISPOSITIVOS A CIBERATAQUES

Hace poco hemos hablado de lo importante que era mantener correctamente protegidos estos servicios, recomendando su desactivación en caso de no utilizarlos. En este artículo, os vamos a hablar de una amenaza que se ha detectado en Internet. Se sirve de servicios SSH de equipos Linux que no están protegidos de forma correcta. El nombre de la amenaza es GoScanSSH y se encuentra en pleno proceso de expansión.

Acorde a los expertos de la escuela de hackers éticos, después de que ambos modelos de enrutador fueron analizados se descubrió que las vulnerabilidades se encuentran vinculadas al panel de control web utilizado para configurar el enrutador. “Los controles que se encuentran en la interfaz web realmente no protegen al enrutador ‘real’, lo que hace las cosas mucho más fáciles para los hackers”, agregaron los expertos.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Uno de los posibles vectores de ataque puede ser cuando un usuario envía solicitudes ping, a continuación se mostrará un mensaje en la consola del dispositivo referente al código nativo compilado al binario del firmware. Después de realizar una serie de pasos (realmente complejos) es posible generar las condiciones adecuadas para un ataque de desbordamiento de búfer. "Sin entrar en detalles, esta es una vulnerabilidad de desbordamiento de búfer clásica", mencionaron los investigadores.

Acorde a los especialistas de la escuela de hackers éticos, las actualizaciones de TP-Link fueron lanzadas desde mediados del mes de marzo y aplican para los dos modelos de enrutador vulnerables. Los usuarios de TL-WR940N deberán actualizar a TL-WR940Nv3; por otra parte, los usuarios de TL-WR940Nv3 deberán actualizar a TL-WR941NDv6.

Los investigadores sostienen que la mayoría de los fabricantes de estos dispositivos firman contratos de outsourcing con desarrolladores de firmware de bajo costo, inseguro y sin controles de calidad. Por si fuera poco, esta clase de desarrolladores no lanza actualizaciones de software con regularidad, o no las lanza en absoluto.

Dos modelos de enrutadores TP-Link están expuestos a la explotación de una vulnerabilidad día cero que permite a los usuarios maliciosos tomar control de los dispositivos, reportan especialistas de la escuela de hackers éticos del Instituto Internacional de Seguridad Cibernética (IICS).

"Hemos descubierto una vulnerabilidad día cero que compromete el funcionamiento del dispositivo, exponiéndolo a ataques remotos", menciona Grzegroz Wypych, especialista en ciberseguridad. La compañía ha reportado que los modelos de enrutadores comprometidos han sido descontinuados, no obstante, buscando en línea aún se pueden encontrar estos dispositivos disponibles para su compra.

TAJMAHAL – EL AVANZADO SPYWARE DESARROLLADO POR HACKERS DESCONOCIDOS

Especialistas del curso de ethical hacking del Instituto Internacional de Seguridad Cibernética (IICS) reportan el hallazgo de una variante de software modular y adaptable con una amplia variedad de complementos diseñados para realizar diversas tareas de espionaje cibernético.

Un grupo de investigadores de una firma de ciberseguridad descubrió este spyware, afirmando que todo el marco de trabajo comprende no sólo las características intrínsecas de un software espía (como registro de golpes en el teclado y capturas de pantalla), sino que además incluye funciones no asociadas a este tipo de desarrollos.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Acorde a los especialistas del curso de ethical hacking, el spyware TajMahal (bautizado así por los investigadores) es capaz de interceptar documentos en espera de ser impresos, dar seguimiento a archivos de interés para el atacante y extracción automática de archivos seleccionados al conectar una unidad de almacenamiento externo. Por si no fuese suficiente, los investigadores afirmaron que este spyware no parece tener relación alguna con ningún grupo conocido de cibercriminales vinculados con algún gobierno.

"Este es un desarrollo altamente complejo. TajMahal es extremadamente raro, además de ser muy avanzado y sofisticado", mencionan los investigadores. "El spyware tiene un código completamente nuevo, no parece estar relacionado con algún otro software espía desarrollado en el pasado".

Acorde a los especialistas del curso de ethical hacking, el spyware fue detectado por primera vez a mediados del 2018, en un país de Asia central cuyo nombre no ha sido revelado por motivos de seguridad. Debido a que se trata de un desarrollo altamente sofisticado, los investigadores no descartan que haya atacado en otras ubicaciones.

Después de las primeras investigaciones los expertos concluyeron que los atacantes comienzan el ataque implantando un programa de backdoor en las computadoras comprometidas. Este programa usará PowerShell para permitir que los atacantes se conecten a un servidor de comando y control, además los hackers plantarán la carga útil más importante de TajMahal, identificada como Yokohama.
Este componente muestra una versatilidad sorprendente, mencionaron los especialistas. Gracias a Yokohama, los atacantes pueden conectar una USB a una computadora infectada, escanear su contenido y enviar un listado a su servidor de comando y control, desde donde los atacantes pueden seleccionar los archivos que desean extraer del sistema comprometido. El spyware también cuenta con algunos módulos para comprometer archivos de otras formas.

FUENTES:

Raúl Gonzales. (2019). VULNERABILIDAD DÍA CERO EN ENRUTADORES TP-LINK EXPONE LOS DISPOSITIVOS A CIBERATAQUES. APRIL 9,2019, de Noticias de Seguridad Informática Sitio web: https://noticiasseguridad.com/vulnerabilidades/vulnerabilidad-dia-cero-en-enrutadores-tp-link-expone-los-dispositivos-a-ciberataques/

DRAGONBLOOD, CONJUNTO DE VULNERABILIDADES QUE AFECTAN EL ESTÁNDAR WIFI WPA3.

Especialistas del curso de seguridad informática del Instituto Internacional de Seguridad Cibernética (IICS) reportan el hallazgo de un conjunto de vulnerabilidades, bautizado como DragonBlood, que afectan el estándar de autenticación y seguridad de conexión WiFi WPA3, el más reciente lanzamiento de WiFi Alliance.

De ser explotadas, estas vulnerabilidades podrían permitir que un atacante ubicado dentro del rango de alcance de una señal WiFi pueda obtener la contraseña de la red o infiltrarse en los sistemas de las potenciales víctimas.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Acorde a los especialistas del curso de seguridad informática, DragonBlood consiste en cinco distintas vulnerabilidades:

- ***Una vulnerabilidad de ataques de denegación de servicio (DoS)***
- ***Dos errores de fuga de información de canales laterales***
- ***Dos errores que permiten ataques de degradación***

Aunque el ataque DoS no ha sido considerado altamente riesgoso, pues sólo es funcional en puntos de acceso compatibles con WPA3, las otras cuatro vulnerabilidades descubiertas pueden ser utilizadas para recuperar información sensible del usuario, como las contraseñas. Estos cuatro ataques explotan fallas en el diseño del intercambio de claves Dragonfly en el estándar WPA3, mecanismo utilizado para la autenticación de un enrutador o punto de acceso.

En el ataque de degradación, los hackers pueden forzar que una red WiFi WPA3 utilice sistemas de intercambio de claves antiguos y menos seguros; gracias a esto, los atacantes pueden recuperar las contraseñas explotando vulnerabilidades antiguas.

Por otra parte, en los ataques de fuga de información de canal lateral las redes con soporte para WiFi WPA3 pueden engañar a un dispositivo para forzarlo a usar algoritmos menos seguros, por lo que se filtrarán pequeñas cantidades de información sobre la contraseña de la red; al repetir este proceso las veces necesarias se puede recuperar la contraseña de una red WiFi por completo.

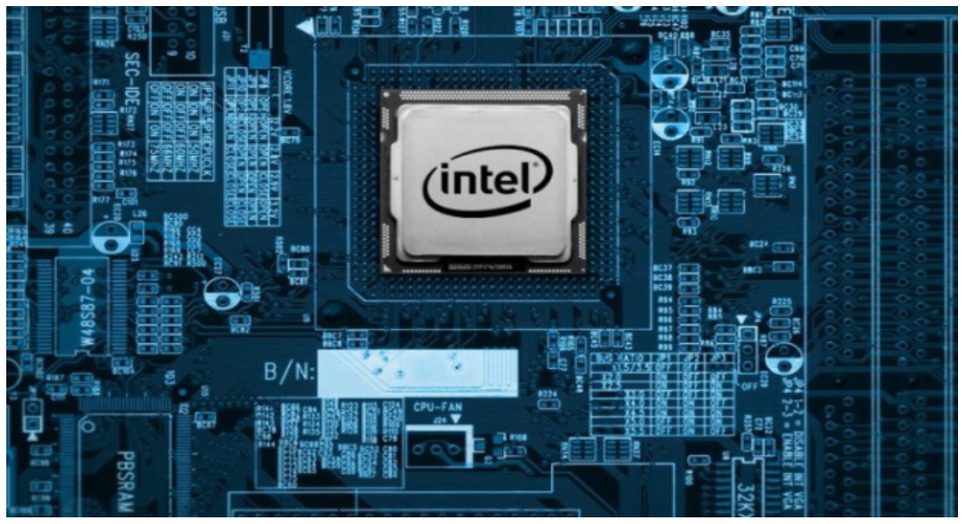
Acorde a los especialistas del curso de seguridad informática, el conjunto de vulnerabilidades DragonBlood también impacta al Protocolo de Autenticación Extensible (EAP-pwd), admitido en los estándares WPA y WPA2. "Esta vulnerabilidad permite a los hackers hacerse pasar por cualquier usuario y, por lo tanto, acceder a la red WiFi, sin saber la contraseña del usuario legítimo". Poco después de recibir el reporte sobre las vulnerabilidades, WiFi Alliance anunció que las correcciones para estas vulnerabilidades estarían disponibles a la brevedad. "Todos estos problemas son solucionables empleando actualizaciones de software, no hace falta corregir los dispositivos", mencionó WiFi Alliance en un comunicado.

FUENTES:

Fernando Márquez. (2019). TAJMAHAL – EL AVANZADO SPYWARE DESARROLLADO POR HACKERS DESCONOCIDOS. APRIL 10, 2019, de Noticias de Seguridad Informática Sitio web: https://noticiasseguridad.com/malware-virus/tajmahal-el-avanzado-spyware-desarrollado-por-hackers-desconocidos/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDADES CRÍTICAS EN MEDIA SDK Y MINI PC DE INTEL.



Acorde a especialistas del curso de seguridad informática del Instituto Internacional de Seguridad Cibernética (IICS), Intel ha lanzado parches de actualización para corregir dos vulnerabilidades críticas en su kit de desarrollo de software (SDK) Intel Media, además de la mini PC, Intel NUC.

Las actualizaciones, lanzadas el martes pasado, se enfocan en cuatro vulnerabilidades presentes en los productos mencionados. Acorde a los especialistas del curso de seguridad informática, la falla más crítica se encuentra en Intel Media SDK, y podría permitir que un hacker malicioso con autenticación obtenga una escalada de privilegios.

Media SDK es un paquete de desarrollo de software que permite a los desarrolladores trabajar con características de aceleración de medios en las plataformas Intel, incluyendo el procesamiento de foto y video. La vulnerabilidad presente en Media SDK (rastreada como CVE-2018-18094) recibió un puntaje de 7.8/10 en la escala del Common Vulnerability Scoring System (CVSS), lo que la convierte en una vulnerabilidad crítica.

La vulnerabilidad existe debido a permisos de directorio incorrectos en el instalador de Media SDK, pues conceden al usuario autenticado la posibilidad de habilitar una escalada de privilegios mediante un acceso local. Intel recomienda a sus usuarios actualizar lo antes posible a la cersión 2018 R2.1 o posteriores. Las actualizaciones están disponibles en la plataforma oficial de la compañía, mencionan los especialistas del curso de seguridad informática.

Otra vulnerabilidad crítica está presente en Intel Next Unit of Computing (Intel NUC), un kit de mini PC con capacidad de procesamiento, almacenamiento y memoria para aplicaciones como señalización digital, centros de medios, etc.

Esta vulnerabilidad (CVE-2019-0163) ha recibido un puntaje de 7.5/10 en CVSS, por lo que califica como de alta severidad. Este error existe debido a una validación de entrada insuficiente en el firmware del sistema de NUC, lo que permitiría realizar diversas acciones maliciosas como escalada de privilegios, denegación de servicio y filtración de información del sistema comprometido.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Además de lanzar las correcciones para estas vulnerabilidades, Intel también corrigió un error que permitiría una escalada de privilegios en Graphic Performance Analyzer de Linux, además de un error de filtrado de información en algunos modelos de microprocesadores.

FUENTES:

Noticias de Seguridad Informatica. (2019). VULNERABILIDADES CRÍTICAS EN MEDIA SDK Y MINI PC DE INTEL. Abril 2019, de Intel Sitio web: https://noticiasseguridad.com/vulnerabilidades/vulnerabilidades-criticas-en-media-sdk-y-mini-pc-de-intel/

MICROSOFT PAGÓ MÁS DE 2 MDD EN SU PROGRAMA DE RECOMPENSAS POR VULNERABILIDADES EN 2018.

Acorde a los autores del libro Cómo convertirse en hacker ético, Microsoft pagó más de 2 millones de dólares a los expertos en seguridad que participaron en su programa de recompensa por vulnerabilidades durante 2018. Expertos del Instituto Internacional de Seguridad Cibernética (IICS) reportan que los planes de la compañía de software se enfocan en extender este programa de recompensas implementando una serie de mejoras que contribuirán de forma significativa a la comunidad de la ciberseguridad.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Esta expansión comenzará con los programas Cloud, Windows y Azure DevOps, que otorgarán recompensas al finalizar la reproducción y evaluación de cada envío en lugar de esperar hasta que se haya determinado una solución final.

Acorde a los autores de Cómo convertirse en hacker ético, reduciendo el tiempo desde la presentación hasta la determinación de las recompensas, Microsoft ayudará a los investigadores a obtener ganancias en tiempos más reducidos, lo que debería alentarlos a seguir trabajando en el área del hacking ético; esta medida podría incluso contribuir a sumar más investigadores a esta causa.

La compañía anunció una serie de medidas que incluyen:

- *Incremento en recompensas por vulnerabilidades en Github*
- *Participación de la Unión Europea en el financiamiento del programa, con el fin de mejorar el software de código abierto*
- *Lanzamiento de un programa de recompensas por errores en impresoras HP*

Los autores de Cómo convertirse en hacker ético mencionan que Microsoft también ha formado una alianza con HackerOne, plataforma que se encargará del procesamiento de los pagos de recompensas, haciendo este proceso realmente eficiente. Esta plataforma de seguridad, operada por hackers altamente capacitados, también incluirá nuevas opciones de pago, incluyendo transferencias bancarias en más de 30 diferentes divisas, y pagos a través de PayPal.

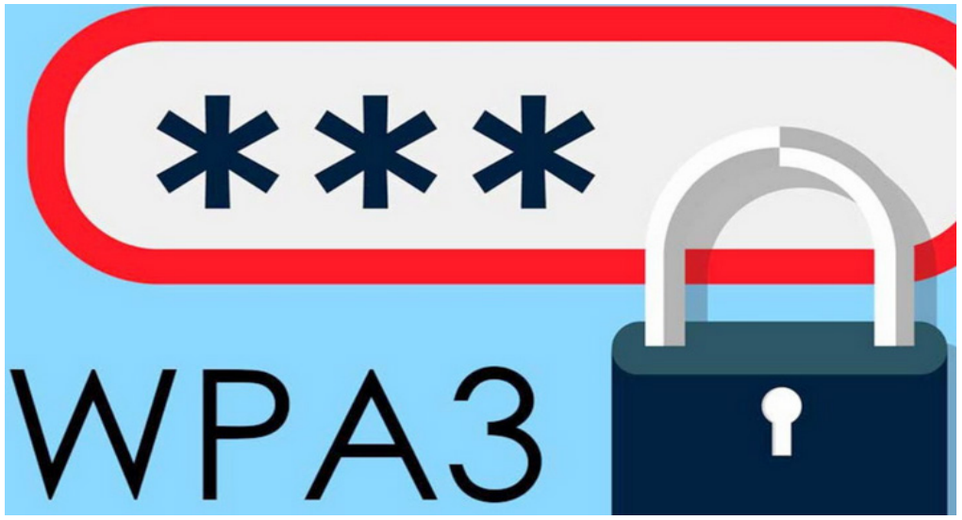
Microsoft también incrementará los pagos por recompensas. Por ejemplo, la recompensa de Windows Insider Preview incrementará de 15 mil a 50 mil dólares; por otra parte, Cloud Bounty para Azure y Office 365, incrementará de 15 mil a 20 mil dólares.

FUENTES:

Noticia de Seguridad Informatica. (2019). MICROSOFT PAGÓ MÁS DE 2 MDD EN SU PROGRAMA DE RECOMPENSAS POR VULNERABILIDADES EN 2018. Abril 2019, de GITHUB, HACKING ÉTICO, MICROSOFT, Sitio web: https://noticiasseguridad.com/seguridad-informatica/microsoft-pago-mas-de-2-mdd-en-su-programa-de-recompensas-por-vulnerabilidades-en-2018/

FALLOS GRAVES EN WPA3 PERMITEN ACCESO A REDES Y HACKEO DE CONTRASEÑAS WI-FI

Un grupo de investigadores ha encontrado fallos graves en WPA3, la nueva generación de la tecnología Wi-Fi Protected Access destinada a añadir mayor seguridad en el acceso y transferencia de datos en redes personales y profesionales, que usen la principal norma mundial para conectividad inalámbrica.



Ha pasado casi un año desde el anuncio de WPA3 y aún con un despliegue mínimo llegan malas noticias para toda la industria y los usuarios, ya que una investigación conocida como DragonBlood ha descubierto que se pueden hackear las contraseñas Wi-Fi establecidas bajo esta norma e incluso, acceder a redes inalámbricas de terceros sin conocer las contraseñas.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Nada es invulnerable y aunque WPA3 es una mejora enorme frente a anteriores versiones del estándar, la investigación plantea serias preocupaciones del futuro de la seguridad inalámbrica, particularmente entre dispositivos de Internet de las Cosas de bajo coste que van a llegar por miles de millones en los próximos años y que será más costoso parchear.

Las vulnerabilidades descubiertas podrían permitir a los atacantes hackear contraseñas de la red Wi-Fi de una manera similar a como se hacía con WPA2, aprovechando el periodo de transición entre las normas.

Dos de ellos son ataques de canal lateral basados en vulnerabilidades CVE-2019-9494 y CVE-2019-9494 contra el método de codificación de contraseñas. También se ha documentado un ataque de denegación de servicio que puede iniciarse sobrecargando un punto de acceso inalámbrico, omitiendo el mecanismo anti-obstrucción de SAE que se suponía evitaría los ataques DoS.

Como prueba de concepto, los investigadores han publicado cuatro herramientas separadas en GitHub que pueden usarse para probar las vulnerabilidades:

- *Dragondrain*
- *Dragontime*
- *Dragonforce*
- *Dragonslayer*

Los investigadores entregaron la documentación a la Wi-Fi Alliance, la organización sin fines de lucro que certifica los estándares y productos de Wi-Fi. La misma ha reconocido los fallos y dice estar trabajando con los proveedores para parchear los dispositivos con certificación WPA3 existentes a base de actualizaciones del firmware.

Lo peor del asunto es que los investigadores han criticado la especificación WPA3 en su totalidad y el proceso que llevó a su formalización por parte del grupo responsable. "A la luz de nuestra investigación y los ataques exitosos, creemos que WPA3 no cumple con los estándares de un protocolo de seguridad moderno", describen los autores, investigadores de varias universitarias.

Nos las prometíamos muy felices con WPA3 y las mejoras que de seguridad que incorpora, pero esta investigación muestra fallos en el mismo diseño de la norma. Un grave problema teniendo en cuenta los 9.000 millones de dispositivos que se calculan se conectan bajo redes inalámbricas Wi-Fi. Lo único positivo es que la nueva norma apenas está extendida y aunque no puedan solucionarse completamente por residir en su mismo diseño, al menos podrá mitigarse. Siendo realistas y según la investigación, WPA4 no tardará en desarrollarse.

FUENTES:

Juan Ranchal. (2019). Fallos graves en WPA3 permiten acceso a redes y hackeo de contraseñas Wi-Fi. 15 de abril de 2019, de Muy Seguridad Sitio web: https://www.muyseguridad.net/2019/04/12/fallos-graves-en-wpa3/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

ATAQUE DE RANSOMWARE PARALIZA LOS SISTEMAS EN CAROLINA DEL SUR, E.U.

Un ataque de ransomware forzó el cierre de todas las operaciones informáticas de la ciudad de Greenville, Carolina del Sur, E.U. Acorde a reportes de especialistas del curso de informática forense del Instituto Internacional de Seguridad Cibernética, el ataque obligó a las autoridades a cerrar la mayoría de sus servidores.

Funcionarios de Greenville, en conjunto con profesionales del resto de E.U. comenzaron una labor conjunta para detener la infección, así como para determinar quiénes son los posibles autores del ataque.

"Se trata de un ataque de ransomware", mencionó un portavoz de la ciudad". "Los autores del ataque nos exigieron un rescate, pero eso es todo lo que puedo decir por el momento", concluyó el funcionario, no sin antes agregar que los equipos de TI del gobierno están haciendo todo lo posible por rehabilitar todos los servicios afectados cuanto antes.

Acorde a los expertos del curso de informática forense los sistemas de comunicación de la policía y los servicios de emergencia funciona de manera regular, puesto que se encuentran en servidores separados del resto.

Los reportes dicen que la infección fue detectada inicialmente por un miembro del departamento de policía de Greenville, quien se puso en contacto con el área de tecnología del gobierno de la ciudad. Posteriormente, los funcionarios decidieron cerrar el sistema para comenzar el proceso de recuperación.

Las operaciones del gobierno de Greenville se están llevando a cabo de forma regular, salvo algunas excepciones; "las funciones del gobierno de Greenville son llevadas a cabo por personas, no sólo por máquinas", declaró un funcionario de la ciudad.

Variantes de ransomware de este tipo han sido detectadas recientemente en diversas partes del mundo. Hace un par de semanas, la compañía Norsk Hydro fue impactada por un ataque de ransomware que obligó a suspender algunos sistemas de la compañía manufacturera de aluminio.

El ransomware es una de las amenazas cibernéticas que más han crecido recientemente, afirman los expertos del curso de informática forense; esta variante de malware cifra los archivos de la víctima para después exigir un pago a cambio de desbloquear los archivos infectados.

FUENTES:

Noticias de seguridad informática. (2019). Ataque de ransomware paraliza los sistemas en Carolina del Sur, E.U.. 15 de abril de 2019, de Noticias de seguridad informática Sitio web: https://noticiasseguridad.com/hacking-incidentes/ata-