SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]

AÑO 02 EDICIÓN 3.04

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"

PREOCUPA A DIRECTIVOS LA CIBERSEGURIDAD¿CUÁNTOS TIPOS DE HACKERS EXISTEN? LAS TRES CLASES DE PIRATAS INFORMÁTICOS

Existen tres clases de piratas informáticos. Y no todos son el típico perfil de cibercriminal ladrón de datos.

Según su propio diccionario, un hacker "es todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo", y fuera del ámbito informático se le llama 'hacker' a toda persona que implementa soluciones para cualquier sistema, sea informático o no, de manera que éste pueda emplearse de formas no pensadas por quienes crearon dichos sistemas. Así mismo, en la era actual 3.0 el término hacker se asocia a toda persona que manipula o que posee conocimientos prácticos que modifican los usos de las cosas, de modo que éstas puedan emplearse para fines no previstos en su origen.

Para el público generalista, mencionarla evoca a alguien que usa su PC para entrar en un sitio sin autorización y cometer actos fraudulentos. Pero en realidad existen varias clases de hackers en el mundo -no hay que confundir el término 'hacker' con el término 'pirata informático'-, tres para ser más exactos, y os las vamos a describir para que veáis porque hacerse hacker de guante blanco es una de las profesiones con más futuro por lo demandados que son sus servicios.

Los hackers con sentido ético, en este grupo se engloban tanto los investigadores de seguridad como aquellos que rompen sistemas por razones no maliciosas para probar sus propios códigos de seguridad, o para demostrar a un cliente o en una empresa en la que trabajan que el software y los protocolos no son seguros. Son los que notifican a las compañías si ven vulnerabilidades aprovechables, y a cambio se les puede pagar de 500 a 100.000 dólares incluso, dependiendo de la importancia del problema, de la posible brecha en potencia y del renombre de la compañía.

Hackers de Sombrero Negro / Black hats Hackers

Considerados directamente como criminales y ejemplificando todo lo negativo en que solemos pensar al leer el término 'hacker', un black hat es un hacker que "viola la seguridad de un dispositivo para poco menos que provecho personal y de mala fe". Hablamos de los que hacen los virus malware, ransomware, todo el SPAM que recibimos en el correo, las brechas de seguridad dentro de las grandes empresas, etc, para entrar, modificar o destrozar datos según les convengan. Y también para robar datos de usuarios y venderlos a quien pague más.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Hackers de Sombrero Gris / Grey hats hackers

A medio camino entre uno y otro bando, los hackers en la zona gris pueden ser tanto contratistas de Defensa como individuos anónimos o grupos de estos que hackean un sistema o toda una compañía y después les comunican lo que han hecho y cómo podrían arreglar sus fallos de seguridad. Su ambigüedad estriba en que venden la información que han obtenido, pero lo hacen por el bien del público. Aunque existen gobiernos que pagan por estos datos y las herramientas de hackeo y no los usan para tapar agujeros de seguridad, sino a su favor para espiar a potencias enemigas.

FUENTES:

Cesar Otero (2019). Preocupa a directivos la ciberseguridad ,07 de junio de 2019, de AS.com de Torreón, Sitio Web: https://as.com/meristation/2019/06/06/betech/1559858238_866290.html

EL PELIGRO DE CONECTARLO TODO: UNA CIUDAD LLEVA UN MES «HACKEADA» POR UN PELIGROSO «RANSOMWARE»

«La ciudad de Baltimore actualmente no puede enviar o recibir correos electrónicos. Si necesita asistencia, llame al departamento con el que desee contactar». Este es el mensaje que aparece en la página web oficial de la ciudad más poblada del estado de Maryland (EE.UU.). Baltimore lleva desde el pasado 7 de mayo bloqueada. Toda su Red está en mano de «hackers».

Puede parecer surrealista pero no lo es. La ciudad de Atlanta fue «hackeada» en 2018. Ahora, le ha tocado a Baltimore. Está en manos de los ciberdelincuentes que se han hecho con el control absoluto de la ciudad mediante un ataque «ransomware» conocido como RobbinHood. Aunque poco a poco la ciudad va recobrando la normalidad, la realidad es que, a día de hoy, sigue estando secuestrada. Y lo peor es el coste que le está acarreando solucionar esta brecha de ciberseguridad: de momento lleva gastados más de 18 millones de dólares (16 millones de euros), según recoge « Ars Technica».

La ciudad informó el 7 de mayo de sus primeros problemas con la Red. El email de los servicios del gobierno municipal estaba fuera de servicio. Las líneas telefónicas de atención al cliente tampoco funcionaban. Los 10.000 funcionarios de la ciudad no podían trabajar ni atender a los ciudadanos, a quienes les era imposible pagar sus facturas online. Lo que comenzó siendo un habitual fallo de Red se convirtió en un secuestro en toda regla. Solo los servicios esenciales, como la policía, bomberos o el de salud, no se han visto afectados.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

La causa de todos estos problemas es una variedad relativamente nueva de «malware» llamado RobbinHood. Al igual que otros programas de «ransomware», este virus informático cifra los sistemas, bloqueándolos totalmente. Los ciberdelincuentes se hacen con el control de la Red e impiden que pueda usarse, exigiendo un rescate. Tras recibir el dinero, ofrecerían la clave del descifrado.

El chantaje es el proceder habitual de este tipo de ataques. Sin embargo, los expertos en seguridad informática aconsejan no pagar nunca ya que, aunque la víctima desembolse el dinero, normalmente sigue sin recuperar la información. De hecho, según un estudio realizado en 2016 por Kaspersky Lab, aproximadamente una de cada cinco víctimas de «ransomware» que pagan a sus atacantes, no pueden recuperar sus datos.

La nota de rescate exigía el pago de 3 Bitcoins (unos 22.000 dólares; 19.500 euros) para desbloquear cada ordenador, o 13 Bitcoins (99.000 dólares; 88.000 euros) para liberar la ciudad entera.

Según la prensa del país, cuatro días después del ataque, el coste del rescate ascendía a 10.000 dólares al día (8.800 euros). Los «hackers» aseguraban que pasados los 10 días sería imposible recuperar los datos. Sin embargo, el alcalde, Bernard C. Jack Young, se ha mantenido firme en no pagar el rescate.

«Sé que muchos residentes han dicho que deberíamos haber pagado pero tanto el FBI como el Servicio Secreto nos aconsejaron que no», informa el alcalde, que añade que «esa no es la forma en que operamos. No recompensaremos el comportamiento criminal». De hecho, pagar no es garantía de nada. Los ciberdelincuentes pueden dejar «malware» distribuido o «puertas traseras» para volver al ataque en un futuro.

Tres semanas después del ataque inicial, Baltimore sigue sin poder mandar correos electrónicos ni procesar gran parte de los pagos. Desde este martes, sin embargo, los ciudadanos pueden ya pagar sus facturas de agua. La ciudad intenta, poco a poco, volver a la normalidad.

«Estamos en el proceso de restaurar el correo electrónico y el acceso a los ordenadores de los empleados de la ciudad». Aunque Bernard C. Jack Young no ha dado detalles de los pasos que la Oficina de Tecnología de la Información de la Ciudad de Baltimore (BCIT) está siguiendo, sí ha dicho que «se implementó con éxito un piloto y estamos implementando esa solución en toda la ciudad». La recuperación sigue en sus primeras etapas.

«Ars Technica» informa que la ciudad se ha gastado más de un millón de dólares en hardware nuevo comprado a la compañía Dell.«Y mediante un contrato de personal provisional, la ciudad ha comenzado a traer trabajadores temporales para ayudar en la limpieza de 'malware'»

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Los responsables estiman que el coste del «hackeo» asciende a unos 10 millones de dólares (casi 9 millones de euros), sin tener en cuenta los otros 8 millones de dólares (7 millones de euros) que la ciudad ha perdido por su inactividad este tiempo.

El director de finanzas de la ciudad, Henry Raymond, ha calificado el estado actual de los sistemas de «no ideal, pero manejable»: se han restaurado algunos correos electrónicos y servicios telefónicos, y muchos sistemas se han mantenido. Pero los sistemas de procesamiento de pagos y otras herramientas utilizadas para manejar las transacciones de la ciudad aún están pendientes.

Cómo y quién ha realizado este ataque podría saberse tras meses de investigación. Pero, de momento, poco se sabe. Según « The New York Times», RobbinHood consiguió entrar en los sistemas gracias a EnternalBlue, la misma vulnerabilidad de la que se aprovechó WannaCry, el «ramsonware» que afectó a más 360.000 equipos de 180 países diferentes en el año 2017.

Una vez más, se evidencia la importancia de aplicar los parches de seguridad, que para EternalBlue existe desde abril de 2017.

FUENTES:

Ana Martínez (2019). El peligro de conectarlo todo: una ciudad lleva un mes «hackeada» por un peligroso «ransomware» ,07 de junio de 2019, de abc Redes , Sitio Web:
https://www.abc.es/tecnologia/redes/abci-baltimore-ciudad-lleva-hackeada-peligroso-ransomware-robbinhood-201906070334_noticia.html-y-los-hackers-prefieren-recompensas-en-bitcoin/

CISCO INDUSTRIAL NETWORK DIRECTOR ENCONTRÓ QUE CONTENÍA ERRORES DE SEGURIDAD IMPORTANTES

Cisco ha identificado tres errores de seguridad en el software Industrial Network Director (IND). En una serie de avisos de seguridad publicados el miércoles, Cisco abordó estas fallas principales presentes en IND. Una de estas fallas fue una vulnerabilidad de ejecución remota de código (RCE) de "alta severidad" que podría permitir a los actores de amenazas ejecutar código arbitrario con privilegios elevados. Cisco IND es un software diseñado para administrar redes industriales y ayuda a monitorear dispositivos automatizados en una red industrial.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Puntos clave:
** La falla RCE, designada como CVE-2019-1861, tuvo una puntuación CVSS de 7.2. La falla fue el resultado de un problema de validación de archivos en IND. En una advertencia, Cisco menciona que un atacante podría explotar esta falla al autenticarse en un sistema afectado utilizando privilegios de administrador y posteriormente cargar archivos arbitrarios.*

** Las otras dos fallas identificadas por Cisco son una falla almacenada de scripts entre sitios (XSS) y una vulnerabilidad de falsificación de solicitud entre sitios (CSRF). Si bien la falla XSS permite que los atacantes envíen solicitudes maliciosas, la vulnerabilidad CSRF permite que cualquier persona realice acciones arbitrarias en los sistemas afectados.*

** Cisco ha lanzado actualizaciones de software para la falla RCE. Sin embargo, los defectos de XSS y CSRF aún no se han reparado.*

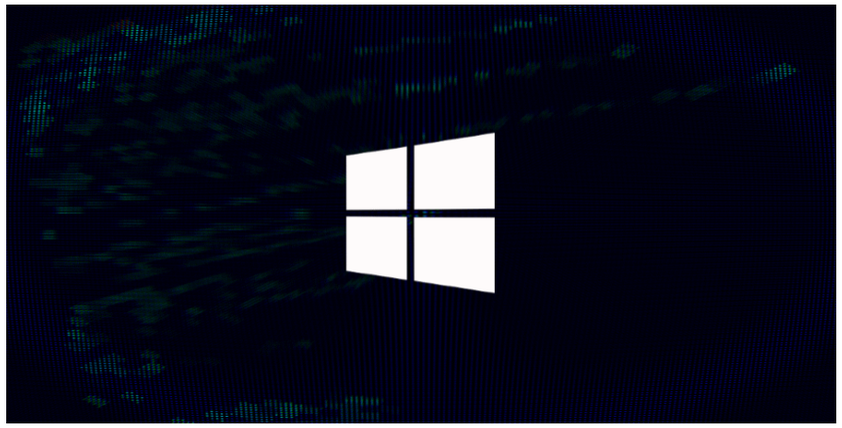
Vale la pena señalar:

Además de abordar las fallas de IND, Cisco también ha lanzado actualizaciones de seguridad para varios productos que tenían agujeros de seguridad. Los productos parcheados son Cisco Unified Communications Manager IM y Servicio de Presencia, Cisco TelePresence Video Communication Server, Cisco Expressway Series, Cisco Enterprise Chat and Email Center, Cisco Unified Computing System, Cisco IOS XR y Cisco Webex Meetings Server.

FUENTES:

Stewart, Ryan. (2019). *Cisco Industrial Network Director found containing major security bugs*. Junio 6, de Cyware. Sitio web: https://cyware.com/news/cisco-industrial-network-director-found-containing-major-security-bugs-b7c63b70 20190320-ip-phone-csrf

NO MÁS ZERO-DAY: ERROR DE WINDOWS OBTIENE UNA SOLUCIÓN



0patch ha lanzado una micro parche interino para el peligroso error LPE de SandboxEscaper, mientras esperamos el parche oficial de Microsoft.

El error de día cero de escalada de privilegios (LPE) local en el Programador de tareas de Microsoft, divulgado por SandboxEscaper en Twitter a fines de mayo para hacer público un exploit que funciona completamente, ahora tiene una microparca. El arreglo provisional, de 0patch, se emitió el martes para abordar la vulnerabilidad. El error permitiría LPE a través de la importación de tareas heredadas de otros sistemas a la utilidad Programador de tareas.

Mitja Kolsek, cofundador de 0patch y CEO de Arcos Security, es, en muchos aspectos, un defecto típico de LPE; permite que un usuario con pocos privilegios en la computadora modifique arbitrariamente cualquier archivo, incluidos los ejecutables del sistema.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

“Dado que estos se ejecutan en un contexto de alto privilegio, el código del atacante puede ejecutarse y, por ejemplo, promover al atacante a administrador local u obtener una persistencia encubierta en la computadora”, dijo Kolsek.

Sin embargo, hay más que eso. Si bien la explotación exitosa requiere que el atacante debe conocer un nombre de usuario y una contraseña válidos en la computadora de destino (que requiera un reconocimiento o la adivinación afortunada de las credenciales de un usuario de dominio de Windows), el ataque le da acceso adverso a archivos altamente privilegiados que generalmente solo son SISTEMA y TrustedInstaller tener la propiedad sobre. Los investigadores le dijeron a Threatpost que, de manera realista, podría estar encadenado con explotaciones comparativamente más comunes y baratas para el acceso remoto, lo que lo convierte en un defecto potencialmente muy peligroso.

El microparche aborda el problema cortando una llamada a procedimiento remoto (RPC) llamada “SchRpcSetSecurity”. El exploit original funciona al realizar una llamada RPC a “SchRpcRegisterTask”, que está expuesta por el servicio Programador de tareas. Sin embargo, al ajustar esta función para frustrar la explotación, 0patch descubrió que se realiza una llamada a la “SchRpcSetSecurity” también expuesta, si la llamada original a “SchRpcRegisterTask” falla, lo cual SandboxEscaper utiliza como un tipo de mecanismo de respaldo para garantizar el éxito del exploit.

La microparche está disponible solo para máquinas con Windows 10, pero hay una razón para ello.

“Aunque Windows 8 aún contiene esta vulnerabilidad, la explotación mediante la técnica descrita públicamente se limita a los archivos donde el usuario actual tiene acceso de escritura, en nuestras pruebas”, dijo Kolsek. “Como tal, el impacto en los sistemas Windows 8 que utilizan la técnica utilizada por el exploit público parece ser insignificante. No hemos podido demostrar la vulnerabilidad en los sistemas Windows 7 “.

El exploit para la falla fue el primero en una serie de exploits recientes de SandboxEscaper, quien dijo que le gustaría vender este tipo de armas por $ 60,000 a compradores no occidentales (hasta el momento de esta publicación, el código de exploit ha sido eliminado de Github). Poco después de hacer pública la explotación de BearLPE, lanzó tres más y una vulnerabilidad para un error de Windows Internet Explorer. De estos, 0patch solo está trabajando en una solución.

“‘ Angrypolarbearbug2 “no es un día, ya que se solucionó en mayo de 2019 Windows Updates”, dijo un portavoz por correo electrónico. “InstallerBypass: no pudimos reproducirlo y no conocemos a nadie que tenga éxito (podría ser realmente difícil de reproducir o depender de algunos factores externos que no estaban presentes en nuestro entorno de prueba); y “sandboxescape” pudimos reproducirlo, pero no lo consideramos un error suficientemente crítico para la microparca “.

El cuarto es un error de bypass que 0patch pudo verificar y está analizando la micropatching. Es un bypass para un parche publicado anteriormente que trata un defecto de sobrescritura de privilegios, sobrescritura de permisos de Windows (CVE-2019-0841). El error existe porque el Servicio de implementación de Windows AppX (AppXSVC) maneja incorrectamente los enlaces duros.

SandboxEscaper tiene un historial de lanzamiento de Windows totalmente funcional de día cero. En agosto pasado, debutó con otra falla del Programador de tareas en Twitter, que fue rápidamente explotada en la naturaleza en una campaña de espionaje solo dos días después de la divulgación.

FUENTES

Seals, Tara. (2019).Zero-Day No More: Windows Bug Gets a Fix. Junio 4, de Threatpost Sitio web: https://threatpost.com/zero-day-sandboxescaper-windows-fix/145337/