SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]

AÑO 02 EDICIÓN 3.1

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"

HACKERS ACCEDEN A SISTEMAS CONFIDENCIALES DE STACK OVERFLOW

Stack Overflow acaba de anunciar que ha sido víctima de un ataque de hacking que ha brindado a los actores de amenazas acceso a los sistemas de producción de esta plataforma, reportan expertos del curso de ciberseguridad del IICS. Por ahora, en el sitio web sólo se ha publicado un mensaje de seguridad respecto a "cierto acceso a la producción" ocurrido hace algunos días.

A pesar de que aún no está claro cómo es que los hackers pudieron acceder a las redes de Stack Overflow, los desarrolladores han decidido lanzar actualizaciones para todas las posibles vulnerabilidades que los atacantes pudieran haber explotado.

Acorde a los expertos, el incidente fue detectado por los mismos desarrolladores de Stack Overflow; después de una investigación interna, la plataforma concluyó que los datos de los usuarios no han sido comprometidos: "Más información será revelada al concluir nuestra investigación; lo más importante para nosotros es la seguridad de la información de nuestros clientes", menciona un comunicado de la plataforma.

"A pesar de que nuestras bases de datos no se han visto afectadas, identificamos algunas solicitudes web privilegiadas realizadas por los operadores del ataque gracias a las que pudieron haber obtenido direcciones IP, direcciones email o nombres de una reducida cantidad de usuarios. Continuaremos realizando monitoreos de seguridad en nuestros sistemas", menciona la alerta de seguridad.

Expertos del curso de ciberseguridad afirman que el incidente ocurrió el pasado 5 de mayo debido a un error en la plataforma que permitió a los atacantes iniciar sesión a nivel de desarrollo, además de aumentar el acceso en la versión de producción de stackoverflow.com.

Stack Overflow comenzó sus actividades en línea en 2008, operando como un sitio web de preguntas y respuestas en temas relacionados con la programación; para 2019, la plataforma ya contaba con más de 10 millones de usuarios, acorde a los expertos del curso de ciberseguridad.

Acorde a expertos del Instituto Internacional de Seguridad Cibernética (IICS), Stack Overflow es una fuente confiable en temas relacionados con la comunidad de desarrolladores de software, pues más de 50 millones de consultas son realizadas mensualmente.

FUENTES:

Noticias de seguridad Informatica. (2019). Hackers acceden a sistemas confidenciales de Stack Overflow. Mayo 17, de Ciberseguridad Sitio web: https://noticiasseguridad.com/hacking-incidentes/hackers-acceden-a-sistemas-confidenciales-de-stack-overflow/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

HACKERS ENVIADOS A PRISIÓN POR ROBAR MÁS DE 2MDD EN CRIPTOMONEDA CON SIM HIJACKING

Acorde a especialistas del curso de seguridad web del IICS, un grupo de hackers conocido como "The Community" ha sido acusado por las autoridades de E.U. por presuntamente haber realizado un fraude conocido como "secuestro de tarjeta SIM", en complicidad con tres empleados de una compañía de telefonía móvil.

Los seis integrantes del grupo de hackers habrían participado en robo de identidad de los clientes de la compañía telefónica, abusando de la información robada para extraer criptomonedas (variante de ataque también conocida como intercambio de SIM).

"El secuestro o intercambio de tarjeta SIM es una variante de fraude de identidad que explota un punto frágil en ciberseguridad, los números de teléfono móvil", explican los especialistas del curso de seguridad web.

Los atacantes toman el control del número telefónico de las víctimas para redirigir el tráfico generado por llamadas, mensajes SMS, etc, a través de dispositivos bajo control de los hackers. Un empleado de soporte de la compañía telefónica fue engañado para que transfiriera el número telefónico de la víctima a una nueva tarjeta SIM en propiedad de los hackers.

Los hackers empleaban esta tarjeta SIM para generar un punto de acceso a las cuentas en línea de la víctima (email, almacenamiento en la nube, carteras de criptomoneda, etc), mencionan los especialistas del curso de seguridad web.

Después de secuestrar el número telefónico de la víctima, los hackers tomaron control de las carteras en de criptomoneda de la víctima, robando alrededor de 2.5 millones de dólares. Además, tres empleados de la compañía fueron señalados como cómplices del grupo de hackers.

Según las leyes estadounidenses, los acusados enfrentan una condena de hasta 20 años de cárcel por conspiración para cometer fraude electrónico, mencionan especialistas del Instituto Internacional de Seguridad Cibernética (IICS).

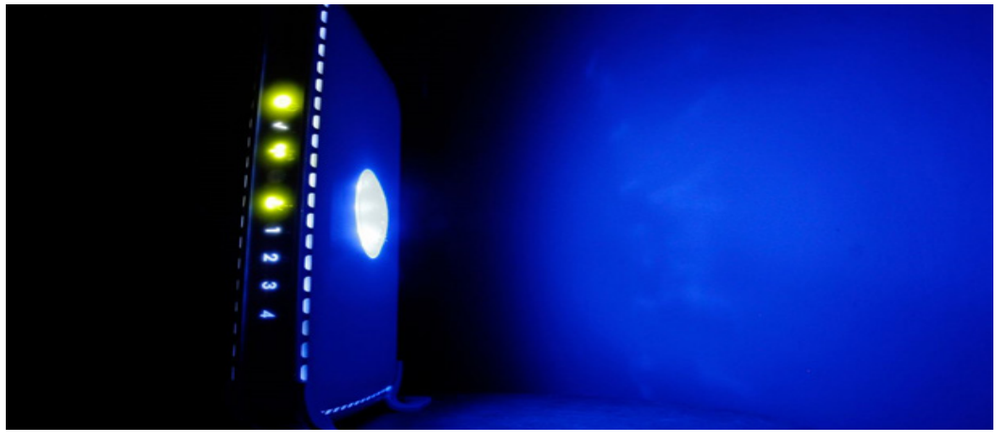
Los hackers y los ex empleados de la compañía telefónica, de entre 19 y 28 años, aún se encuentran a la espera de que comience el juicio que decidirá su futuro.

FUENTES:

Noticias de Seguridad Informatica. (2019). Hackers enviados a prisión por robar más de 2MDD en criptomoneda con SIM hijacking. Mayo 13, de Ciberseguridad Sitio web: https://noticiasseguridad.com/hacking-incidentes/hackers-enviados-a-prision-por-robar-mas-de-2mdd-en-criptomoneda-con-sim-hijacking/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

EU Y EUROPA DESMANTELAN RED DE MALWARE QUE DEJÓ PÉRDIDAS POR 100 MDD



Diez personas, entre ellas cinco prófugos rusos, han sido acusadas por una ola de ataques que infectaron a miles de computadoras en todo el mundo y provocaron pérdidas de más de 100 millones de dólares, informaron el jueves autoridades estadounidenses y europeas.

Los virus cibernéticos permitieron a criminales en Europa del Este infiltrar computadoras y retirar dinero de las cuentas bancarias de las víctimas, y el asalto afectó a compañías e instituciones de todo tipo en Estados Unidos.

Entre ellas había un bufete de abogados de Washington, una iglesia de Texas, una mueblería de California, un casino de Mississippi y una compañía de asfaltado de Pensilvania.

Varios de los procesados serán enjuiciados en Europa, y cinco son rusos que están prófugos. Un onceavo miembro del complot fue extraditado a Estados Unidos desde Bulgaria en el 2016 y el mes pasado se declaró culpable en un caso relacionado en un tribunal en Pittsburgh, donde el caso más reciente fue introducido.

Si bien el Departamento de Justicia de Estados Unidos ha iniciado múltiples procesos por ataques con malware en años recientes, este caso se destaca por el grado de cooperación internacional que conllevó, explicó Scott Brady, fiscal federal en Pittsburgh.

Las autoridades estadounidenses no pidieron de inmediato la extradición de los 10 acusados. La extradición es un proceso engorroso que puede tardar años, incluso en países que cuentan con ese tipo de tratado con Estados Unidos. En lugar de ellos, compartieron las evidencias con sus contrapartes europeos de tal manera que permitieron a las autoridades de Ucrania, Moldavia y Georgia iniciar procesos en los países donde viven los señalados.

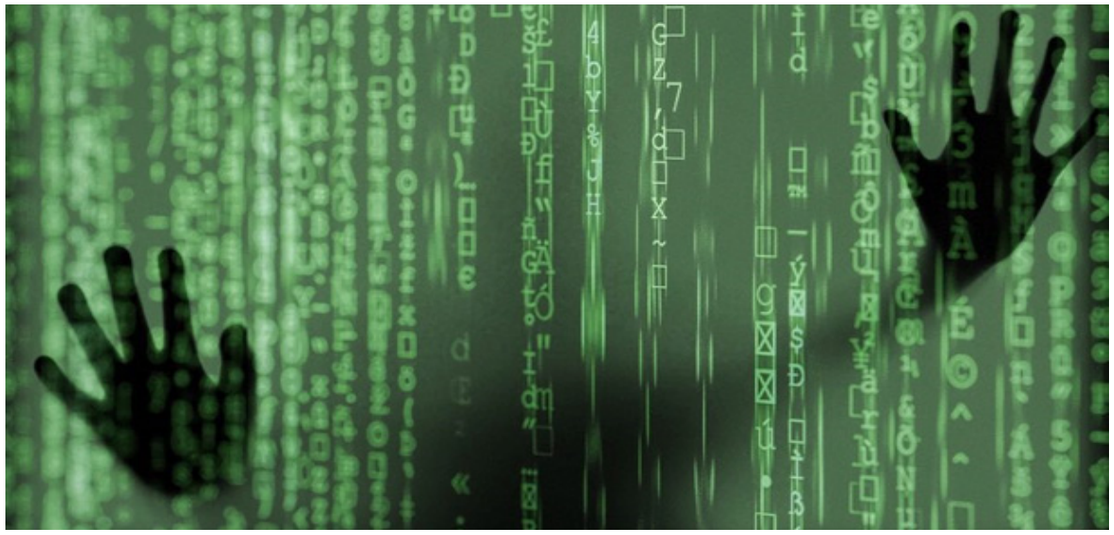
“Es un cambio del paradigma en cuanto a la manera de procesar a cibercriminales”, dijo Brady en entrevista con AP antes de una conferencia de prensa en La Haya con representantes de seis países.

FUENTES:

AP TECH (2019). EU y Europa desmantelan red de malware que dejó pérdidas por 100 mdd ,16 de mayo de 2019, de El Financiero, Sitio Web: https://www.elfinanciero.com.mx/tech/eu-y-europa-desmantelan-red-de-malware-que-dejo-perdidas-por-100-mdd

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

ESTUDIO REVELA QUE ATAQUES RANSOMWARE AUMENTARON UN 90% ESTE AÑO Y LOS HACKERS PREFIEREN RECOMPENSAS EN BITCOIN



Proveedores de ciberseguridad admiten que le pagan a los hackers para recuperar los datos secuestrados por ataques de ransomware. El estudio encontró que la principal criptomoneda entre estos atacantes es Bitcoin.

Un estudio de ProPublica encontró que la mayoría de las compañías proveedoras de soluciones de ransomware les pagan a los hackers para deshacerse de ellos.

Un ransomware o «secuestro de datos«, es un tipo de programa maligno que restringe el acceso a determinadas partes o archivos del sistema operativo infectado. A cambio de quitar esta restricción, el atacante o hacker solicita una recompensa al usuario.

Recientemente, los expertos en seguridad de Coveware señalaron que la actividad de ransomware crece semanalmente. Como resultado, las compañías, que sólo quieren seguir adelante, terminan por pagar el rescate de sus datos.

Según Coveware, los ataques de ransomware aumentaron en el primer trimestre de 2019:

En el primer trimestre de 2019, el rescate promedio aumentó en un 89%, a USD $12.762, en comparación con USD $6.733 en el cuarto trimestre de 2018. El aumento del rescate refleja el aumento de las infecciones de los tipos de ransomware más costosos como Ryuk, Bitpaymer e Iencrypt. Estos tipos de ransomware se utilizan predominantemente en ataques dirigidos a objetivos específicos de empresas más grandes.

Fraude de las empresas de ciberseguridad

Sin embargo, una vez que los hackers encriptan un equipo infectado, la verdadera pregunta es cómo desbloquear los datos. ProPublica descubrió que muchas empresas de recuperación de datos simplemente pagan el rescate y luego cobran una prima por «las molestias causadas«. Es decir, estas empresas cobran por aplicar «tecnología de primera» para desencriptar los datos, pero en realidad solo pagan al atacante para obtenerlos.

Un ejemplo de esto es Proven Data, que prometió ayudar a las víctimas de ransomware desbloqueando sus datos con la «última tecnología«, según los correos electrónicos de la empresa y sus antiguos clientes. En cambio, según Storfer y una declaración jurada del FBI obtenida por ProPublica, obtuvo herramientas de descifrado de los ciberataque pagando rescates.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Otra empresa estadounidense, MonsterCloud, con sede en Florida, también profesa utilizar sus propios métodos de recuperación de datos. Sin embargo, en su lugar, paga los rescates. De acuerdo con ProPublica, a veces la empresa ni siquiera informa a las víctimas, entre las que se cuentan agencias policiales locales.

Ambas empresas, además, tienen otras características en común. Primero, ambas cobran a las víctimas honorarios sustanciales adicionales a la cantidad que pagan por el rescate. También ofrecen otros servicios, como el «sellado de brechas para proteger contra futuros ataques«. Asimismo, ambas empresas han utilizado pseudónimos para sus trabajadores, en lugar de nombres reales, para comunicarse con las víctimas.

El Ransomware está empeorando
Después de que la Fiscalía General de los Estados Unidos rastreara y acusara a dos hackers iraníes por liberar un programa de rescate llamado SamSam, las autoridades esperaban que la prevalencia de los ataques disminuyera. En cambio, aumentó considerablemente, superando los niveles de 2018 considerablemente.

Muchos creen que la razón es porque el software de rescate es muy lucrativo. Los hackers pueden lanzar un ataque y luego, cuando las víctimas lo descubren, negocian brevemente con empresas como MonsterCloud y otras para desbloquear los ordenadores. Sin embargo, muchas de estas compañías ofrecen métodos de recuperación y muchos investigadores de seguridad trabajan en métodos gratuitos. Por ejemplo, muchos han generado soluciones para uno de los ransomware más popular: WannaCry, que afecta al sistema operativo Windows.

Desafortunadamente, los hacks están empeorando y el software necesario se está volviendo más complejo.

La empresa de soluciones, Coveware admite abiertamente que negocia con estafadores. Para ellos, el pago de la recompensa es uno de los métodos más sencillos para recuperar datos. Sin embargo, lo preocupante es que estos esfuerzos están financiando inadvertidamente el terrorismo. Además, según señalan, cada vez es más difícil descifrar los ordenadores pirateados, gracias a las nuevas versiones del ransomware. Por lo que el tiempo de inactividad se ha incrementado.

De acuerdo con un estudio de Coveware, en el primer trimestre de 2019 el «tiempo medio de inactividad aumentó, de 6,2 días en el cuarto trimestre de 2018, a 7,3 días«.

Pérdidas significativas
Para cualquier gran empresa el tiempo de inactividad puede ser crucial. Además de que el tiempo de inactividad se incrementa, también hay que considerar que en muchos casos los ransomware tienen unas tasas de pérdida de datos relativamente altas. Entre 10-20% para las variaciones del tipo de ransomware Hermes, por ejemplo.

El aumento del tiempo de inactividad también responde a la frecuencia de los ataques. En muchos casos, los sistemas de copia de seguridad se borran o cifran como parte del ataque. Una característica que indica que la naturaleza de estos ataques es cada vez más personalizada.

Mientras tanto, los costos estimados de pérdida de una empresa por el tiempo de inactividad por cada ataque de rescate también ascendieron. En promedio, las empresas pueden perder USD $ 65.645 por el tiempo de inactividad de un ataque.

Los costos de los tiempos de inactividad se vuelven particularmente agudos para las compañías que carecen de seguro cibernético y/o de seguro de interrupción de negocios. Sin embargo Coveware admite que estas estimaciones tienen muchas variables como el rubro de la empresa y su ubicación geográfica, por lo que sus estimaciones pueden no ser precisas.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Bitcoin es la principal en el pago de ransomware
En su estudio, Coveware también descubrió que Bitcoin sigue siendo la criptomoneda más común para los pagos de rescate de datos secuestrados. Asimismo, para las víctimas generalmente el pago con criptomonedas genera conflictos, y por lo tanto, también para los atacantes.

Para muchos usuarios, estos métodos de pago son peligrosos y existen quienes piensan que se tratan de grupos terroristas. En opinión del CEO de Coveware, Bill Siegel, la recuperación media en los casos de ransomware no es realmente una negociación con «terroristas«. La empresa incluso, con el tiempo, ha logrado desarrollar tácticas rescate en base a los «patrones» de ataques y los perfiles de los atacantes. Esto en función de desarrollar estrategias de negociación en nombre de sus clientes.

En cuanto a las criptomonedas, opinión del grupo, es poco probable que los hackers de ransomware cambien a Bitcoin en un futuro cercano. En especial porque han ganado terreno en perfeccionar las técnicas con las que adquieren y manejan esta moneda. Esto se pone de manifiesto por la facilidad con la que los actores de la amenaza «mezclan» Bitcoin o cambian la criptomoneda por otras monedas de privacidad, como Dash o Monero.

Un tipo de cibersecuestro popular conocido como Gandcrab acepta pagos en Dash o Bitcoin, asegura Coveware. Sin embargo, a las víctimas de este ransomware que pagan con Bitcoin se les cobra un 10% más debido a los costes de «mezcla» en los que incurren los actores de la amenaza para anonimizar los bitcoins después del pago. Esto incluye «esconder» los bitcoins transfiriéndolos a diferentes billeteras y cambiándolos por otras monedas hasta que la los bitcoins iniciales resulten irrastreables.

Si bien el envío de unos cuantos miles de bitcoins a una dirección extraña podría no encajar bien con muchas víctimas, sigue pareciendo la mejor manera de reducir los tiempos de inactividad. Después de todo, implica un gasto a la empresa y es culpa de los proveedores de ciberseguridad el detectar el ransomware en primer lugar. Su tarea es finalmente proteger y prevenir contra estos ataques y no dejar los datos a vulnerabilidad de atacantes.

FUENTES:

Hannah Estefanía Pérez (2019). Estudio revela que ataques ransomware aumentaron un 90% este año y los hackers prefieren recompensas en Bitcoin,17 de mayo de 2019, de Diario Bitcoin, Sitio Web:
https://www.diariobitcoin.com/index.php/2019/05/17/estudio-revela-que-ataques-ransomware-aumentaron-un-90-este-ano-y-los-hackers-prefieren-recompensas-en-bitcoin/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

MICROSOFT LANZA ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP POR SEVERA VULNERABILIDAD

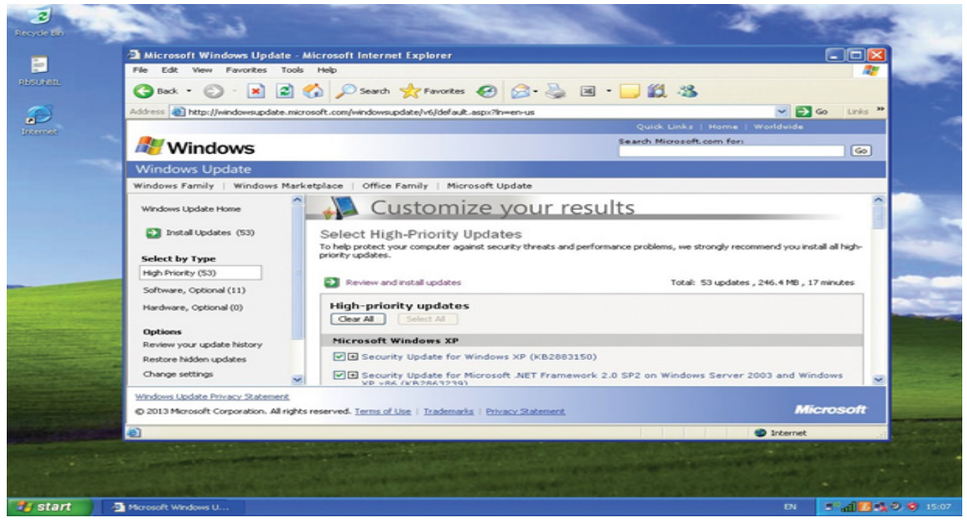
El éxito de Windows XP es un arma de doble filo: el costo de dominar el mundo de los PCs de escritorio por años es grande, considerando que muchos todavía usan dicho sistema en sus equipos. Microsoft no le entrega soporte de actualizaciones desde hace cinco años -por razones obvias- pero el veto se ha vuelto a levantar, y por un problema grave: un severo bug que podría replicarse tan fácilmente como Wannacry.

Los detalles de dicha vulnerabilidad aún son vagos, y desde Microsoft sólo se limitaron a mencionar que afecta a la funcionalidad sobre la que está sustentada el Protocolo de Escritorio Remoto (RDP, por sus siglas en inglés). Aclarando, el Escritorio Remoto como aplicación no es en sí mismo vulnerable, sino que la funcionalidad que lo sustenta lo es.

Además, dicha vulnerabilidad es pre-autenticación y no requiere interacción humana, lo que la hace susceptible a gusanos de rápida propagación. En resumen: un exploit podría usar el protocolo para propagarse de equipo a equipo, y ejecutar ataques RCE, o de ejecución remota de código, en miles de computadores que todavía usan el eterno sistema operativo.

Cómo actualizar Windows XP

¿Qué hago si todavía tengo Windows XP y simplemente no puedo hacer un upgrade? Windows Update, o al menos la funcionalidad automática, ya fue descontinuada en Windows XP, por lo que los usuarios de dicho sistema -o de Windows Server 2003, que también fue descontinuado y es vulnerable- deben descargar la actualización correspondiente a su versión del sistema operativo, y luego instalarla siguiendo las instrucciones en pantalla.



Otros sistemas operativos como Windows 7, Windows Server 2008 y 2008 R2 también son vulnerables -por poseer una implementación similar de Remote Desktop- pero todavía no son descontinuados, por lo que, si tienen activado Windows Update y sus actualizaciones de seguridad al día, deberían estar protegidos.

Los usuarios de Windows 8 en adelante no poseen la vulnerabilidad, por lo tanto, no necesitan parcharla.

FUENTES:

Gutiérrez, Norman (17 de Mayo 2019). Microsoft lanza actualización de seguridad para Windows XP por severa vulnerabilidad. Recuperado de: https://www.fayerwayer.com/2019/05/windows-xp-actualizacion/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDADES DE EJECUCIÓN REMOTA DE CÓDIGO DE CISCO PRIME INFRASTRUCTURE Y EVOLVED PROGRAMMABLE NETWORK MANAGER

Criticidad: Crítica
Impacto: Ejecución de código
Vulnerabilidad:
Ejecución: Remota
Plataforma(s) Afectada(s):
Estas vulnerabilidades afectan las versiones de software de Cisco PI anteriores a 3.4.1, 3.5 y 3.6, y las versiones de EPN Manager anteriores a 3.0.1.
Referencia: CVE-2019-1821, CVE-2019-1822, CVE-2019-1823
Descripción:
Las múltiples vulnerabilidades en la interfaz de administración basada en web de Cisco Prime Infrastructure (PI) y Cisco Evolved Programmable Network (EPN) Manager podrían permitirle a un atacante remoto obtener la capacidad de ejecutar código arbitrario con privilegios elevados en el sistema operativo subyacente.

Uno de estos problemas, CVE-2019-1821, puede ser explotado por un atacante no autenticado que tiene acceso de red a la interfaz administrativa afectada.

El segundo y tercer problema, CVE-2019-1822 y CVE-2019-1823, requieren que un atacante tenga credenciales válidas para autenticarse en la interfaz administrativa afectada.

Estas vulnerabilidades existen porque el software valida incorrectamente la entrada proporcionada por el usuario. Un atacante podría explotar estas vulnerabilidades cargando un archivo malicioso en la interfaz web administrativa. Una explotación exitosa podría permitir al atacante ejecutar código con privilegios de nivel de raíz en el sistema operativo subyacente.

Cisco ha lanzado actualizaciones de software que abordan estas vulnerabilidades. No hay soluciones que aborden estas vulnerabilidades.

FUENTES:

Vulnerabilidades de ejecución remota de código de Cisco Prime Infrastructure y Evolved Programmable Network Manager
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-pi-rce

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD DE DIVULGACIÓN DE INFORMACIÓN DE CLAVES SSH DEL SOFTWARE CISCO NX-OS

Criticidad: Media
Impacto: Acceso no autorizado
Vulnerabilidad:
Ejecución: Local
Plataforma(s) Afectada(s):

Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco NX-OS:

- Nexus 3000 Series Switches
- Interruptores de plataforma Nexus 3500
- Interruptores de plataforma Nexus 3600
- Interruptores de plataforma Nexus 5500
- Interruptores de plataforma Nexus 5600
- Nexus 6000 Series Switches
- Nexus 9000 Series Switches en modo NX-OS independiente
- Plataforma de conmutación Nexus 9500 serie R

Referencia: CVE-2019-1731
Descripción:
Una vulnerabilidad en la funcionalidad de administración de claves CLI SSH del software Cisco NX-OS podría permitir que un atacante local autenticado exponga la clave SSH privada de un usuario a todos los usuarios autenticados en el dispositivo de destino. El atacante debe autenticarse con credenciales de dispositivo de administrador válidas.

La vulnerabilidad se debe a un manejo de errores incompleto si se produce un tipo de error específico durante la exportación de la clave SSH. Un atacante podría aprovechar esta vulnerabilidad al autenticarse en el dispositivo e ingresar un comando creado en la CLI. Una explotación exitosa podría permitir al atacante exponer la clave SSH privada de un usuario. Además, un tipo de error similar en la importación de la clave SSH podría hacer que la clave privada SSH protegida por contraseña se importara involuntariamente.

Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. No hay soluciones que aborden esta vulnerabilidad.

FUENTES:

Vulnerabilidad de divulgación de información de claves SSH del software Cisco NX-OS
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-ssh-info

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

¡ACTUALIZA WHATSAPP YA! CON UNA LLAMADA PUEDEN ACCEDER A TU TELÉFONO

El lunes 13 de mayo, Facebook reveló que un "actor cibernético avanzado" ha estado espiando a algunos usuarios de su popular aplicación de mensajería WhatsApp, gracias a una vulnerabilidad día cero, que permitía a los ciberdelincuentes instalar silenciosamente software espía, simplemente llamando al teléfono de la víctima.

La vulnerabilidad ya está solucionada, lo que significa que, si eres uno de los 1.500.000.000 usuarios de WhatsApp, debe actualizar a la última versión.

Es muy probable que su aplicación ya se haya actualizado, pero esta es una vulnerabilidad grave, por lo que le recomendamos que lo compruebe de todos modos.

WhatsApp no está haciendo mucho ruido sobre esto. La página de Seguridad de Facebook, la web y el Twitter de WhatsApp no ofrecen ninguna información.

En el apartado de Novedades de la aplicación Google Play y del Apple App Store dicen que, con la última versión de la aplicación, ahora puede ver los stickers a tamaño completo cuando se presiona en la notificación, pero no informa nada sobre el hecho de que es la única versión que no permite el espionaje remoto.

En su lugar, Facebook ha hecho el equivalente digital de colocar un aviso de seguridad para CVE-2019-3568 en la parte posterior de la puerta del inodoro en un sótano sin luz mientras nadie estaba mirando. Lee como sigue:

Descripción: una vulnerabilidad de desbordamiento de búfer en la pila de VOIP de WhatsApp permitía la ejecución de código remoto a través de una serie de paquetes SRTCP especialmente diseñados y enviados a un número de teléfono.

Versiones afectadas: El problema afecta a WhatsApp para Android anterior a v2.19.134, WhatsApp Business para Android anterior a v2.19.44, WhatsApp para iOS anterior a v2.19.51, WhatsApp Business para iOS anterior a v2.19.51, WhatsApp para Windows Phone antes de v2.18.348 y WhatsApp para Tizen antes de v2.18.15.

Lo que la descripción está tratando de decir, es que algunas personas que conocían esta vulnerabilidad utilizaron llamadas telefónicas a dispositivos vulnerables para instalar programas espía que podían activar el micrófono, leer mensajes y encender la cámara.

El Telegraph informa que un "número selecto" de usuarios se vio afectado y ha vinculado el software espía instalado por WhatsApp al Grupo NSO, la compañía detrás del famoso software espía vendido a gobiernos conocida como Pegasus.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Esa descripción hace que el incidente suene como un ataque contra individuos específicos, en lugar de un intento indiscriminado de espiar a tantos usuarios de WhatsApp como fuera posible.

Pero eso no impide que otros abusen de la vulnerabilidad de otras maneras, por lo que se debe actualizar, incluso si crees que es poco probable que se te afecte este ataque.

Cómo actualizar WhatsApp
iOS

Visitar la App Store> Actualizaciones. Si WhatsApp se ha actualizado automáticamente, aparecerá Abrir junto a él, por lo que no necesita actualizarlo. Si dice Actualizar, seguir adelante para instalar la última versión (2.19.51). Si desea verificar el número de la versión actual, vaya a Configuración> Ayuda dentro de la aplicación.

Android

Visitar Google Play> Mis aplicaciones y juegos. Si WhatsApp se ha actualizado automáticamente, aparecerá Abrir junto a él, por lo que no necesita actualizarlo. Si dice Actualizar, sigue adelante e instala la última versión (2.19.134). Si desea verificar el número de la versión actual, vaya a Configuración> Ayuda> Información de la aplicación en la propia aplicación.

FUENTES:

Naked Security. (2019, 15 mayo). ¡Actualiza WhatsApp ya! Con una llamada pueden acceder a tu teléfono. Recuperado 20 mayo, 2019, de https://news.sophos.com/es-es/2019/05/15/actualiza-whatsapp-ya-con-una-llamada-pueden-acceder-a-tu-telefono/