SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]

AÑO 02 EDICIÓN 3.0

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"

UN NUEVO MALWARE APUNTA HACIA LOS SERVIDORES DE MICROSOFT EXCHANGE

ESET, la compañía de seguridad informática, ha anunciado el descubrimiento de un nuevo tipo de malware dirigido específicamente a los servidores de Microsoft Exchange y que se lleva usando desde hace 5 años para ofrecer un control casi total del correo de las compañías afectadas.

IÚltimamente se han descubierto un par más de amenazas de seguridad para Microsoft como la de hace un par de semanas referente a los hackers que obtuvieron durante 3 o 6 meses un control total de las cuentas de Outlook al hacerse con la herramienta de la que el SAT dispone para solucionar los problemas de los usuarios y que incluso han llegado a hacerse con 1 Bitcoin.

Lightneuron es una de las backdoors más complejas que se hayan visto en un servidor de correo electrónico y los hackers (cómo no) rusos lo están usando como un MTA (Agente de Transferencia de Mensajes) para los servidores de correo de Exchange.

Los hackers tendrían control total sobre todo lo que pasa a través de un servidor de correo electrónico infectado, pudiendo interceptar y editar el contenido del mensaje tanto de los correos entrantes como de los salientes.
Lo que hace único a este malware es su mecanismo de control y el uso de la esteganografía, la práctica de ocultar un archivo, mensaje o imagen dentro de otro archivo, mensaje o imagen.
Los piratas ocultan los comandos dentro de imágenes PDF y JPEG enviadas por correo que la puerta trasera lee y ejecuta.
ESET ha publicado un documento con instrucciones para su control y eliminación, sin embargo, al utilizar LightNeuron a los niveles más bajos posibles, se antoja un poco complicado.

FUENTES:

Fuente: Rodríguez Martín (8 de Mayo 2019). Microsoft Insider. Un nuevo malware apunta hacia los servidores de Microsoft Exchange. Recuperado de: https://www.microsoftinsider.es/137063/un-nuevo-malware-apunta-hacia-los-servidores-de-microsoft-exchange/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

UN HACKER ESTÁ EXIGIENDO EL RESCATE DE CIENTOS DE REPOSITORIOS DE CÓDIGO GIT ROBADOS

A fines de la semana pasada, un pirata informático robó datos de cientos de repositorios de código Git y los retiene en sus servidores, amenazando con liberar el código al público si los propietarios afectados no pagan. Los usuarios de GitHub, Bitbucket y GitLab que informaron que su código había desaparecido encontraron la siguiente nota de rescate en su lugar:

"Para recuperar su código perdido y evitar perderlo: envíenos 0.1 Bitcoin (BTC) a nuestra dirección de Bitcoin ES14c7qLb5CYhLMUekctxLgc1FV2Ti9DA y contáctenos por correo electrónico a admin@gitsbackup.com con su nombre de usuario Git y una Prueba de pago. Si no está seguro si tenemos sus datos, contáctenos y le enviaremos un comprobante. Su código es descargado y respaldado en nuestros servidores. Si no recibimos su pago en los próximos 10 días, publicaremos su código o lo utilizaremos de otra manera ".

Cuando la nota de rescate apareció por primera vez el viernes, declaró que los propietarios tienen 10 días para pagar 0.1 bitcoin, que actualmente es de alrededor de $ 565. Aunque el tiempo se está reduciendo hasta el 13 de mayo, puede haber un recurso para recuperar sus datos sin pagar. Ponerse en contacto con la línea de soporte para su servicio puede ser útil a corto y largo plazo, ya que estas compañías siempre están trabajando para solucionar las vulnerabilidades a través de las cuales el hacker encontró la forma de ingresar.

Si todavía no se ha contactado con el soporte, ZDNet también señala que un usuario de StackExchange tiene algunos consejos para recuperar datos robados, aunque puede recuperarse en un estado de mutilación.

El hacker supuestamente hurgó en Internet los archivos de configuración de Git y luego extrajo las credenciales enumeradas en texto sin formato para obtener acceso. ¿La leccion? No almacene sus contraseñas en texto plano. Incluso las cuentas con contraseñas aparentemente a prueba de hackers estaban en riesgo. Kathy Wang, directora de seguridad de GitLab, insistió en una declaración a ZDNet de que los usuarios pueden protegerse contra ataques futuros como éste mediante el uso de herramientas de administración de contraseñas bloqueadas con autenticación de dos factores.

FUENTES:

Fuente: Cameron Faulkner (06 de Mayo de 2019). The Verge. A hacker is demanding ransom for hundreds of stolen Git code repositories. Recuperado de: https://www.theverge.com/2019/5/6/18531222/hacker-data-theft-ransom-stolen-git-code-bitcoin

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

AMAZON, OBJETIVO DE UN IMPORTANTE ATAQUE DE PHISHING

Amazon ha revelado que fue el objetivo de un ataque de phishing que afectó a las cuentas de los vendedores con los que trabaja. Los cibercriminales podrían haberse hecho con miles de dólares suplantando la identidad de la compañía.

Según ha desvelado Bloomberg, que ha tenido acceso a la presentación ante el consejo regulador de Reino Unido en la que Amazon reconoció haber sido objetivo de este fraude, los hackers accedieron a las cuenta de los vendedores con los que trabaja y sustrajeron importantes cantidades de dinero.

Este fraude se produjo durante un período de seis meses, empezando en mayo de 2018 y aprovechando la práctica de Amazon de otorgar préstamos a sus vendedores externos en los mercados en los que opera.

Los hackers accedieron a estas cuentas y cambiaron los detalles de pago mediante correos en los que suplantaban la identidad de Amazon para cambiar detalles de los pagos y desviarlos a sus propias cuentas bancarias. Un dinero que estaba destinado para utilizarse para cubrir costes de inicio y negocios pero que se desvió y que podría sumar cientos de miles de dólares.

EL PASADO AÑO, AMAZON PRESTÓ 1.000 MILLONES DE DÓLARES A SUS VENDEDORES Y SOCIOS EXTERNOS.

Se trata de una práctica muy común en Amazon en los mercados en los que opera, prestando a sus vendedores externos. De hecho, hace unos días desvelaba en su informe anual de pymes que el pasado 2018 otorgó más de 1.000 millones de dólares en préstamos a sus vendedores y socios externos.

Por el momento, Amazon se ha negado a hacer declaraciones relacionadas con este tema. No obstante, un portavoz de la compañía sí ha manifestado que cualquier vendedor que considere que puede haber recibido un correo electrónico malicioso suplantando la identidad de Amazon debe enviar debe enviar un mensaje a stop-spoofing@amazon.com para poner en conocimiento de la firma esta problemática y solventarla.

FUENTES:

Enrique Gomez. (2019). Amazon fue objetivo de un ciberataque de phishing. 12/Mayo/2019, de Muy Seguridad Sitio web: https://www.muyseguridad.net/2019/05/12/amazon-objetivo-de-un-importante-ataque-de-phishing/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

EL RANSOMWARE «ROBBINHOOD» TUMBA LAS REDES GUBERNAMENTALES DE BALTIMORE

Un ataque de ransomware mediante el conocido «RobbinHood» ha tumbado las redes gubernamentales de la ciudad de Baltimore. Es un nuevo recordatorio de la peligrosidad de este tipo de malware, especialmente en redes empresariales.

El Ransomware mantiene la supremacía como la principal ciberamenaza de malware en la mayoría de los estados miembros de la Unión Europea, según el informe de Europol, Internet Organised Crime Threat Assessment(IOCTA) correspondiente a 2018. Ya en 2019, la detección de ataques por ransomware en empresas aumentaron un 200%, según el último informe trimestral de amenazas de Malwarebytes.

El Director de Información de Baltimore, Frank Johnson, confirmó en una conferencia de prensa que el malware era RobbinHood, un Ransomware muy agresivo que el FBI ha identificado como una «variante bastante nueva» del malware y similar a una de las múltiples versiones detectadas como la que afectó al municipio de Greenville, Carolina del Norte, en abril.

En este caso, RobbinHood ha logrado bloquear las redes gubernamentales de Baltimore, una ciudad con un área metropolitana con cerca de 3 millones de habitantes que tiene fuera de línea casi todos sus servicios, exceptuando los de emergencias, policías y bomberos.

El investigador de seguridad Vitali Kremez, quien recientemente diseñó una muestra de RobbinHood por ingeniería inversa, explica que el malware parece apuntar solo a archivos en un solo sistema y no se propaga a través de redes compartidas. «Se cree que se propaga directamente a las máquinas individuales. Ello significaría que el atacante debería haber obtenido acceso de nivel administrativo a un sistema dentro de la red debido a la forma en que el ransomware interactúa con el directorio C: \ Windows \ Temp».

Cómo prevenir el Ransomware
Al igual que con otros tipos de malware, los ciberataques por Ransomware son cada vez más numerosos, sofisticados, peligrosos y masivos, como mostró WanaCryptor, un ataque bien planificado y estructurado cuyo objetivo fue lograr una infección masiva a nivel mundial, poniendo contra las cuerdas a un buen número de grandes empresas de decenas de países.

FUENTES:

Juan Ranchal. (2019). NOTICIASEl ransomware «RobbinHood» tumba las redes gubernamentales de Baltimore. 09/Mayo/2019, de Muy Seguridad Sitio web: https://www.muyseguridad.net/2019/05/09/ransomware-robbinhood-baltimore/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD DE AMPLIACIÓN DE PRIVILEGIOS DEL CONTROLADOR DE INFRAESTRUCTURA DE POLÍTICAS DE APLICACIONES DE CISCO

Criticidad: *Alta*
Impacto: *Escalación de privilegios*
Vulnerabilidad:
Ejecución: *Local*
Plataforma(s)
Afectada(s):
Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión del Software del Controlador de Infraestructura de la Política de Aplicación (APIC) de Cisco antes de la versión 3.2 (6i) o 4.1 (1i).
Referencia: *CVE-2019-1682*

Descripción:
Una vulnerabilidad en la funcionalidad del sistema de archivos FUSE para el software del Controlador de infraestructura de políticas de aplicación (APIC) de Cisco podría permitir a un atacante local autenticado escalar privilegios a la raíz en un dispositivo afectado.

La vulnerabilidad se debe a una validación de entrada insuficiente para ciertas cadenas de comando emitidas en la CLI del dispositivo afectado. Un atacante con permisos de escritura para archivos dentro de una carpeta legible en el dispositivo podría alterar ciertas definiciones en el archivo afectado. Una explotación exitosa podría permitir a un atacante hacer que el controlador FUSE subyacente ejecute dichos comandos diseñados, elevando los privilegios del atacante a la raíz en un dispositivo afectado.

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

FUENTES:

Vulnerabilidad de ampliación de privilegios del Controlador de infraestructura de políticas de aplicaciones de Cisco
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-apic-priv-escalation

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD DE LA ESCALADA DE PRIVILEGIOS DE RAÍZ EN EL MODO DE INFRAESTRUCTURA CENTRADA EN LA APLICACIÓN CISCO NEXUS 9000 SERIES FABRIC SWITCHS

Criticidad: *Alta*
Impacto: *Escalación de privilegios*
Vulnerabilidad:
Ejecución: *Local*
Plataforma(s) Afectada(s):
Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión de software del interruptor de modo ACI de la serie 9000 de Cisco Nexus antes de 13.2 (6i), 14.1 (1i) y versiones posteriores:

Nexus 9000 Series Fabric Switches en modo de Infraestructura centrada en la aplicación (ACI)
Referencia: *CVE-2019-1803*

Descripción:
Una vulnerabilidad en la administración del sistema de archivos para el software del conmutador de modo de infraestructura centrada en la aplicación (ACI) de la serie Cisco Nexus 9000 podría permitir a un atacante local autenticado con derechos de administrador obtener privilegios elevados como usuario root en un dispositivo afectado.

La vulnerabilidad se debe a los permisos de archivos excesivamente permisivos de archivos específicos del sistema. Un atacante podría explotar esta vulnerabilidad al autenticarse en un dispositivo afectado, crear una cadena de comandos diseñada y escribir esta cadena en una ubicación específica del archivo. Una explotación exitosa podría permitir al atacante ejecutar comandos de sistema operativo arbitrarios como root en un dispositivo afectado. El atacante necesitaría tener credenciales de administrador válidas para el dispositivo.

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

FUENTES:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-nexus9k-rpe

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD DE LA CLAVE SSH PREDETERMINADA EN EL MODO DE INFRAESTRUCTURA CÉNTRICA DE LA APLICACIÓN CISCO NEXUS 9000 SERIES FABRICS

Criticidad: Crítica
Impacto: Acceso no autorizado
Vulnerabilidad:
Ejecución: Remota
Plataforma(s) Afectada(s):
Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión de software del interruptor de modo ACI de la serie Nexus 9000 de Cisco antes de 13.2 (6i) o 14.1 (1i):

Nexus 9000 Series Fabric Switches en modo de Infraestructura centrada en la aplicación (ACI)
Referencia: CVE-2019-1804

Descripción:
Una vulnerabilidad en la administración de claves SSH para el software del conmutador de modo de infraestructura centrada en la aplicación (ACI) de Cisco Nexus 9000 Series podría permitir a un atacante remoto no autenticado conectarse al sistema afectado con los privilegios del usuario raíz.

La vulnerabilidad se debe a la presencia de un par de claves SSH predeterminado que está presente en todos los dispositivos. Un atacante podría aprovechar esta vulnerabilidad abriendo una conexión SSH a través de IPv6 a un dispositivo específico utilizando los materiales clave extraídos. Un exploit podría permitir al atacante acceder al sistema con los privilegios del usuario root . Esta vulnerabilidad solo es explotable sobre IPv6; IPv4 no es vulnerable.

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

FUENTES:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-nexus9k-sshkey