SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]

AÑO 01 EDICIÓN 3.06

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"

SYSTEMBC: CUIDADO CON ESTE MALWARE QUE UTILIZA TU ORDENADOR PARA OCULTAR TRÁFICO MALICIOSO

Siempre que navegamos por la red nos podemos topar con múltiples tipos de malware que comprometan nuestra seguridad y privacidad. Los piratas informáticos buscan constantemente la manera de perfeccionar sus técnicas y tener un mayor éxito. Hoy nos hacemos eco de SystemBC. Se trata de un nuevo malware que es capaz de ocultar el tráfico malicioso de la comunicación del servidor de control en el propio equipo de la víctima. Esto lo consigue al configurar una conexión proxy SOCKS5.

SystemBC, el malware que se oculta en el equipo de la víctima
Este malware denominado SystemBC está diseñado para llevar a cabo diferentes campañas de explotación de troyanos bancarios o envío de ransomware. Como sabemos, son dos de los tipos de amenazas más presentes hoy en día.

Según informan investigadores de seguridad de Proofpoint, este malware está presente desde al menos abril de 2019. Esto es así ya que el día 2 del mismo mes se toparon con un anuncio en la Deep Web donde promocionaban una amenaza que coincide con su descripción.

Este malware SystemBC, como ha sido denominado por Proofpoint, usa conexiones HTTP seguras para lograr cifrar la información que envía a los servidores de control desde el propio equipo de la víctima que ha sido infectado.

Como hemos mencionado, esta amenaza es capaz de configurar servidores proxy SOCKS5 en el dispositivo de la víctima. Posteriormente pueden ser utilizados por los ciberdelincuentes para ocultar el tráfico malicioso de otro tipo de malware. Así pueden obtener una vía libre de entrada al equipo.

Campaña dirigida a Windows
Hay que mencionar que este nuevo malware capaz de instalar un proxy en el equipo infectado está dirigido a sistemas operativos Windows. Como sabemos, los sistemas de Microsoft son hoy en día los más utilizados en equipos de escritorio. Por ello pueden ser muchos los usuarios que pueden verse infectados por esta amenaza.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Lo más preocupante es que esta amenaza lo normal es que no venga sola. Hemos visto que los piratas informáticos pueden utilizarlo para desplegar otro tipo de malware. Por tanto, si un usuario es víctima de SystemBC lo normal es que tenga también en su sistema un troyano bancario, ransomware o cualquier otra amenaza que comprometa su seguridad y privacidad.

También hay que destacar la dificultad para ser detectado. Esto sin duda abre la puerta a nuevas posibles amenazas que se basen en este malware que utiliza proxys para ocultar el tráfico.

Cómo evitar ser víctima de estas amenazas
Los usuarios podemos tener en cuenta una serie de consejos importantes para evitar la entrada de malware en nuestro sistema. Lo primero y más importante es contar siempre con aplicaciones de seguridad. Esto nos permite detectar la entrada de malware y poder frenar posibles ataques.

También es vital tener los sistemas actualizados a la última versión. A veces surgen vulnerabilidades que son aprovechadas por los ciberdelincuentes para llevar a cabo sus ataques. Es importante tener los últimos parches y actualizaciones para corregir esos fallos.

Pero sin duda el sentido común tiene que estar presente. Muchas de estas amenazas requieren de la interacción del usuario. Hablamos por ejemplo de descargar software fraudulento desde sitios de terceros o hacer clic en un enlace falso. Hay que estar siempre alerta.

FUENTE:

Javier Jiménez. (2019, 2 agosto). SystemBC: cuidado con este malware que utiliza tu ordenador para ocultar tráfico malicioso.02 agosto, 2019, de Redes Zone sitio Web: https://www.redeszone.net/2019/08/02/systembc-malware-utiliza-equipo-victima/

TROYANOS BANCARIOS DE AMÉRICA LATINA: ANÁLISIS DE NUEVAS FAMILIAS DE MALWARE

Serie bimensual en la que iremos publicando los resultados de una investigación realizada por ESET sobre nuevas familias de troyanos bancarios dirigidos a América Latina

A fines de 2017, un grupo de investigadores del laboratorio de malware ESET Praga decidieron analizar en profundidad los infames troyanos bancarios escritos en Delphi que son conocidos por afectar a Brasil. Extendimos nuestro foco hacia otras partes de América Latina (México y Chile) poco después de notar que muchos de estos troyanos bancarios apuntaban a estos países también. Nuestro objetivo principal era descubrir si existe una forma de clasificar estos troyanos bancarios y aprender más sobre su comportamiento en general.

Hemos aprendido mucho –hemos identificado más de 10 nuevas familias de malware, estudiado las cadenas de distribución y las hemos asociado a las nuevas familias de manera acorde, además de haber analizado su comportamiento interno.
Así fue que decidimos trabajar en una serie de artículos (que publicaremos con una frecuencia bimensual) en los que compartiremos los resultados de nuestra investigación y el análisis de cada una de las familias que se identificaron. Al final de este artículo iremos colocando el enlace a cada uno de los artículos correspondiente al análisis de cada una de las familias de troyanos bancarios, en la medida en que vayan siendo publicados
¿Cuáles son las particularidades de los troyanos bancarios de América Latina?
Hemos encontrado otras características comunes durante nuestra investigación. En este sentido, la mayoría de los troyanos bancarios de América Latina que hemos analizado se conectan al servidor de C&C y se mantienen conectados a la espera de recibir cualquier comando que envíe el servidor. Una vez que reciben un comando, lo ejecutan y esperan a recibir uno nuevo. Los comandos probablemente sean enviados de forma manual por los atacantes. Puede pensarse en esta forma de operar como si

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

si fuese una sala de chat en la que todos los miembros reaccionan a lo que el administrador escribe.

La dirección del servidor C&C parece ser la información que los autores de estos malware protegen más. Hemos encontrado muchas formas diferentes de esconder la actual dirección; algo que discutiremos en esta serie de artículos. Además del servidor de C&C, una URL diferente es utilizada por el malware para enviar información sobre la identificación de la víctima. Esto ayuda al atacante a mantener un registro de las infecciones exitosas.

Los troyanos bancarios de América Latina suelen utilizar algoritmos criptográficos generalmente desconocidos y es común que diferentes familias utilicen los mismos. Hemos identificado un libro y una librería gratuita en Delphi en la que aparentemente los autores se inspiraron.

El hecho de que este malware esté escrito en Delphi indica que los archivos ejecutables son de al menos unos pocos megabytes de tamaño porque el núcleo de Delphi está presente en cada binario. Adicionalmente, la mayoría de los troyanos bancarios en América Latina contienen un gran número de recursos, lo que provoca un gran incremento en el tamaño de los archivos. En este sentido, hemos incluso descubierto muestras con tamaños de archivos que alcanzan varios cientos de megabytes. En esos casos, el tamaño del archivo se incrementó de manera deliberada con el objetivo de evitar la detección.

Descubriendo familias de malware
Cuando analizamos tales ejecutables, no resulta difícil determinar rápidamente que se trata de un troyano bancario malicioso. Junto a las características anteriormente mencionadas, los autores tienden a copiar el trabajo realizado por otros o elaborar su malware a partir de una fuente común. Como consecuencia de ello, la mayoría de los troyanos bancarios terminan siendo similares entre sí. Esta es la razón principal por la que generalmente solo vemos detecciones genéricas.

Nuestra investigación comenzó con la identificación de fuertes características que nos permitiesen establecer familias de malware. Con el tiempo, fuimos capaces de hacer esto y de identificar más de 10 nuevas familias diferentes. Las características que hemos utilizado fueron principalmente cómo están almacenados los strings, cómo se obtiene la dirección del servidor C&C y otras similitudes de código.

Siguiendo la cadena de distribución
La manera más sencilla en la que estos troyanos bancarios son distribuidos es mediante la utilización de un único downloader (un archivo ejecutable de Windows) específico para esa familia. Este downloader algunas veces se hace pasar por el instalador de un software legítimo. Este método es simple, pero también el menos común.

Mucho más común es utilizar una cadena de distribución de múltiples etapas que típicamente emplea varias capas de downloaders escritos en lenguajes de scripting, tales como JavaScript, PowerShell o Visual Basic Script (VBS). Este tipo de cadena típicamente consiste de al menos tres etapas. El payload final es comúnmente entregado a través de un archivo zip que contiene, ya sea el troyano bancario solamente o componentes adicionales junto a él. La principal ventaja que los autores del malware obtienen a partir de este método es que resulta muy complicado para investigadores de malware llegar al final de la cadena y por lo tanto analizar el payload final. Sin embargo, también es más sencillo para una solución antivirus detener la amenaza porque solo necesita romper un eslabón de la cadena.

FUENTE:

Naked Security. (2019, 01 agosto). Troyanos bancarios de América Latina: análisis de nuevas familias de malware Recuperado 01 agosto, 2019, de We live security https://www.welivesecurity.com/la-es/2019/08/01/troyanos-bancarios-america-latina-analisis-nuevas-familias-malware/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDADES CRÍTICAS DE SEGURIDAD PARA TOMAR LAS MEDIDAS PREVENTIVAS Y CORRECTIVAS FRENTE A LAS AMENAZAS TECNOLÓGICAS

SISTEMA OPERATIVO JUNOS: SERIE EX4300: DENEGACIÓN DE SERVICIO AL RECIBIR UNA GRAN CANTIDAD DE PAQUETES VÁLIDOS ESPECÍFICOS EN LA INTERFAZ DE ADMINISTRACIÓN. (CVE-2019-0046)

Criticidad: Medio
Vulnerabilidad: -
Ejecución: Remota
Plataforma(s) afectada(s): Junos OS 16.1, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2 en la serie EX4300.
Referencia: (CVE-2019-0046)
Descripción:
Una vulnerabilidad en el demonio pfe-chassisd Chassis Manager (CMLC) de Juniper Networks Junos OS permite que un atacante provoque una Denegación de servicio (DoS) al EX4300 cuando paquetes de transmisión válidos específicos crean una condición de tormenta de transmisión cuando se recibe en la interfaz me0 de El dispositivo de la serie EX4300. Es necesario reiniciar el dispositivo para restaurar el servicio. La recepción continua de estos paquetes de transmisión válidos creará una Denegación de servicio (DoS) sostenida contra el dispositivo.

Las versiones afectadas son Juniper Networks Junos OS:

16.1 versiones anteriores e incluidas 16.1R1 anteriores a 16.1R7-S5;
17.1 versiones anteriores a 17.1R3;
17.2 versiones anteriores a 17.2R3;
17.3 versiones anteriores a 17.3R3-S2;
17.4 versiones anteriores a 17.4R2;
18.1 versiones anteriores a 18.1R3;
18.2 versiones anteriores a 18.2R2.

Se requiere la siguiente configuración mínima:
set interfaces me0
Juniper SIRT no tiene conocimiento de ninguna explotación maliciosa de esta vulnerabilidad.
Este problema se observó durante el uso de producción.

Solución:
Las siguientes versiones de software se han actualizado para resolver este problema específico: 16.1R7-S5, 17.1R3, 17.2R3, 17.3R3-S2, 17.4R2, 18.1R3, 18.2R2, 18.3R1 y todas las versiones posteriores.

Este problema se está rastreando como PR 1329430, que está visible en el sitio web de Atención al cliente.

Nota: La política de Juniper SIRT no es evaluar las versiones que están más allá del final de la ingeniería (EOE) o el final de la vida útil (EOL).

FUENTES:

Junos OS: Sistema operativo Junos: Serie EX4300: Denegación de servicio al recibir una gran cantidad de paquetes válidos específicos en la interfaz de administración. (CVE-2019-0046) , Julio 2019 de Juniper Networks, Sitio Web:
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10938&cat=SIRT_1&actp=LIST

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

SERIE EX4300: CUANDO SE APLICA UN FILTRO DE FIREWALL A UNA INTERFAZ DE BUCLE INVERTIDO, PUEDEN FALLAR OTROS FILTROS DE FIREWALL PARA TRÁFICO DE MULTIDIFUSIÓN (CVE-2019-0048)

Criticidad: Medio
Impacto: Inyección de comandos
Vulnerabilidad:
Ejecución: Remota
Plataforma(s) Afectada(s):
EX4300 que ejecuta el sistema operativo Junos.
Referencia: (CVE-2019-0048)

Descripción:

En los conmutadores de la serie EX4300 con la optimización TCAM habilitada, el tráfico de multidifusión entrante coincide primero con una regla de filtro de bucle invertido implícito, ya que tiene alta prioridad. Esta regla está destinada a las direcciones de multidifusión reservadas 224.0.0.x, pero coincide incorrectamente en 224.xxx Debido a este error, cuando se aplica un filtro de firewall en la interfaz de bucle invertido, otros filtros de firewall pueden dejar de funcionar para el tráfico de multidifusión.

El comando ‘ show firewall filter’ se puede usar para confirmar si el filtro está funcionando.

Este problema solo afecta al conmutador EX4300. Ningún otro producto o plataforma se ve afectado por esta vulnerabilidad.

Este problema afecta a Juniper Networks Junos OS:

Versiones 14.1X53 anteriores a 14.1X53-D51, 14.1X53-D115 en la serie EX4300;
17.1 versiones anteriores a 17.1R3 en la serie EX4300;
17.2 versiones anteriores a 17.2R3-S2 en la serie EX4300;
17.3 versiones anteriores a 17.3R3-S3 en la serie EX4300;
17.4 versiones anteriores a 17.4R2-S5, 17.4R3 en la serie EX4300;
Versiones 18.1 anteriores a 18.1R3-S1 en la serie EX4300;
Versiones 18.2 anteriores a 18.2R2 en la serie EX4300;
Versiones 18.3 anteriores a 18.3R2 en la serie EX4300.

Este problema solo afecta a los conmutadores de la serie EX con la optimización TCAM habilitada:

set system packet-forwarding-options tcam-group-optimization

Juniper SIRT no tiene conocimiento de ninguna explotación maliciosa de esta vulnerabilidad.

Este problema se observó durante el uso de producción.

FUENTES:

Junos OS: Serie EX4300: cuando se aplica un filtro de firewall a una interfaz de bucle invertido, pueden fallar otros filtros de firewall para tráfico de multidifusión (CVE-2019-0048), Julio 2019 de Juniper Networks, Sitio Web:
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10942&cat=SIRT_1&actp=LIST