SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Quincenal de Ciberinteligencia Securesoft

Fecha:

08 Septiembre de 2020

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia

CIB-FOR-2020-011

Índice

1. Objetivo

El presente documento de inteligencia tiene como objetivo informar sobre las principales vulnerabilidades y amenazas que se han detectado en el ciberespacio.

2. Alcance

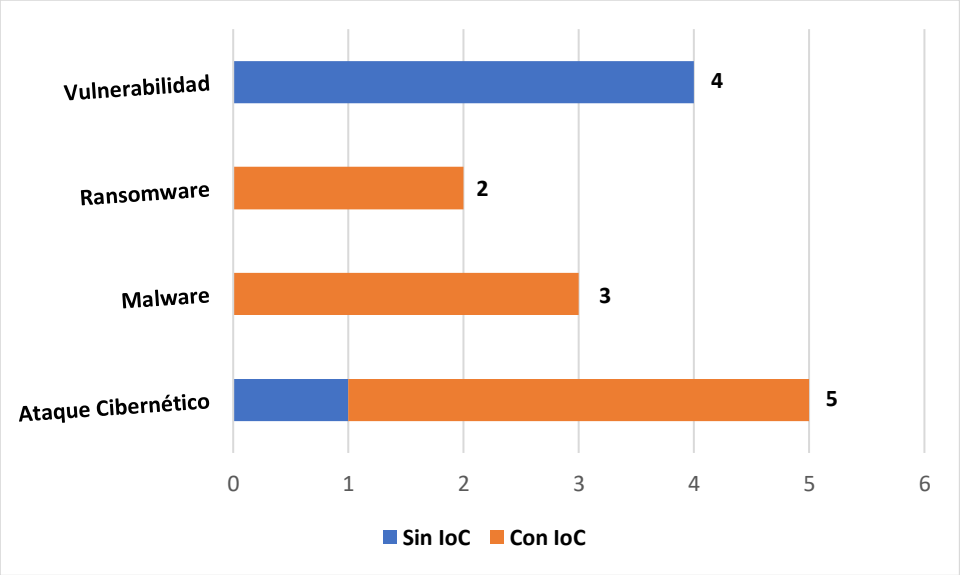
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 20 de agosto hasta el 07 de septiembre del 2020.

3. Resumen

En el presente informe se exponen 14 análisis de vulnerabilidad y amenazas, de las cuales todas tienen una severidad Alta.

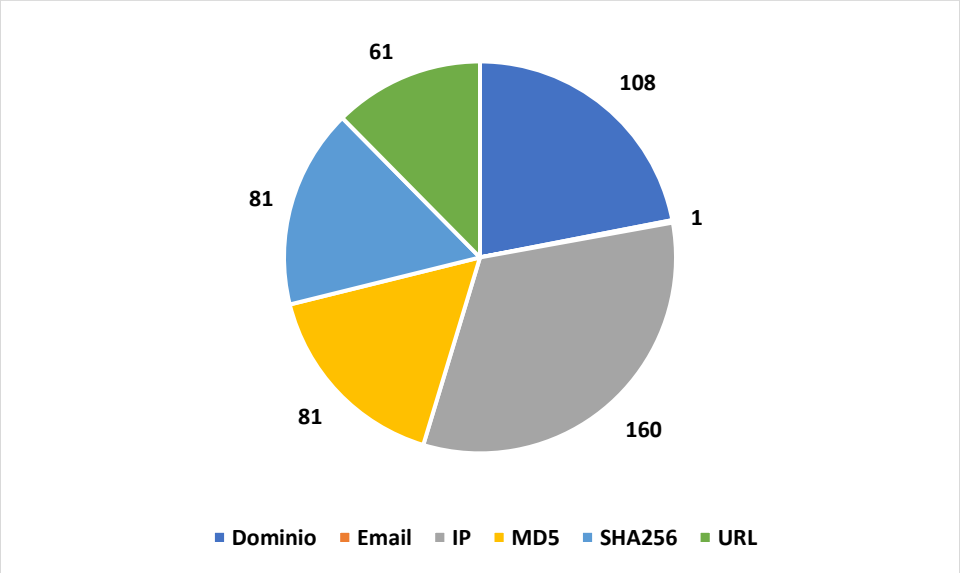
Amenazas analizadas por tipología

En las investigaciones elaboradas para el presente informe se trataron vulnerabilidades, malware, ataques cibernéticos y ransomware. Los que se detallan a continuación, separándolas de acuerdo con si contaban con indicadores de compromiso (IoC) o no.



Indicadores de Compromiso (IoC)

En las investigaciones elaboradas para el presente informe, se han distribuido 492 IoC entre Dominios, Email, IP, MD5 y SHA256.



Tendencias en nuevas vulnerabilidades

- De acuerdo con nuestras fuentes de inteligencia la nueva vulnerabilidad asignada al CVE-2020-3566 está siendo tratada de ser explotada por los cibercriminales. Esta vulnerabilidad afecta al software Cisco IOS XR. Para más información leer el Boletín 2020-263, en la cual podrá encontrar la actualización para esta vulnerabilidad.

Actividades maliciosas asociadas a grupo de cibercriminales

- Durante las últimas semanas se ha detectado que grupos de origen norcoreano e iraní han estado atacando a diversas organizaciones haciendo uso de distintos tipos de malwares y vectores de distribución, para más información leer Boletín 2020-255, Boletín 2020-257 y Boletín 2020-262.

4. Detalles

Vulnerabilidades

Boletín	2020-256
Asunto	ACTUALIZACIONES DE SEGURIDAD EN PRODUCTOS F5
Emisión	26/08/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Varios productos F5

Descripción

Se publicó una alerta de seguridad relacionado a los productos de la compañía F5. En total son 17 vulnerabilidad y 3 notificaciones de seguridad. Estas vulnerabilidades pueden ser utilizadas para sobrescribir archivos de manera arbitraria, ataques de man-in-the-middle, ataque de denegación de servicio (DoS, por sus siglas en inglés), ejecutar de manera remota código, entre otras.

La mayoría de las vulnerabilidades tienen una severidad alta.

Actualización o Mitigación

Aplicar las actualizaciones para estas vulnerabilidades proporcionadas por F5. Para ello haga clic aquí.

Imagen 1. Imagen de referencia de la marca de los productos afectados

Boletín	2020-258
Asunto	CISCO PUBLICA ACTUALIZACIONES DE SEGURIDAD
Emisión	28/08/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Varios productos que hacen uso del software Cisco NX-OS

• Software Cisco UCS Manager en el producto Cisco UCS 6400 Series Fabric Interconnects

Descripción

Cisco publicó actualizaciones de seguridad para corregir siete vulnerabilidades, las cuales en su mayoría tienen una severidad alta. Estas vulnerabilidades afectan a switches y soluciones de almacenamiento de fibra.

El producto más afectado fue el NX-OS, con seis alertas de seguridad vinculados al sistema operativo de red que usan los switches Ethernet de la serie Nexus, y los switches de red de área de almacenamiento Fibre Channel de la serie MDS. La vulnerabilidad asignada al CVE-2020-3504 es la única considerada de severidad media.

Actualización o Mitigación

Aplicar las actualizaciones para estas vulnerabilidades proporcionadas por Cisco. Para ello haga clic aquí.

Imagen 2. Imagen de referencia de la marca de los productos afectados

Boletín	2020-263
Asunto	VULNERABILIDADES EN SOFTWARE DE CISCO
Emisión	03/09/2020
CVE	CVE-2020-3566 y CVE-2020-3569
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Cualquier versión del software Cisco IOS XR si una interfaz activa está configurada en enrutamiento de multidifusión

Descripción

El sistema operativo de red IOS XR de Cisco se encuentra implementado en múltiples routers de la serie NCS 540 y 560, NCS 5500, 8000 y ASR 9000.

Hasta el momento Cisco no ha publicado una actualización de software para corregir las vulnerabilidades CVE-2020-3566 y CVE-2020-3569. Sin embargo, la compañía ha proporcionado una mitigación.

Las vulnerabilidades se deben a que el protocolo de enrutamiento de multidifusión por vector de distancia (DVMRP, por sus siglas en inglés) del software IOS XR permite que atacantes remotos no autenticados agoten la memoria del dispositivo afectado. Para lograrlo, un atacante tiene que enviar paquetes del Protocolo de administración de grupos de Internet (IGMP, por sus siglas en inglés), esto ocasiona que haya inestabilidad en los procesos del dispositivo.

Actualización o Mitigación

Cisco comunicó que los administradores pueden tomar medidas para eliminar parcial o totalmente las amenazas de exploits, que los atacantes podrían usar en ataques dirigidos a dispositivos afectados.

Para lograrlo se puede limitar la velocidad para reducir las tasas de tráfico IGMP, y aumentar el tiempo necesario para explotar con éxito las dos vulnerabilidades. También se puede implementar una entrada de control de acceso (ACE, por sus siglas en inglés) a una lista de control de acceso (ACL, por sus siglas en inglés), o una nueva ACL para denegar el tráfico DVRMP entrante a interfaces con enrutamiento de multidifusión habilitado.

Cisco recomienda deshabilitar el enrutamiento IGMP en interfaces donde no es necesario procesar el tráfico IGMP ingresando al modo de configuración del router IGMP. Esto se puede hacer emitiendo el comando router IGMP.

Aplicar las actualizaciones para estas vulnerabilidades proporcionadas por Cisco. Para ello haga clic aquí.

Boletín	2020-265
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE FILE MANAGER
Emisión	07/09/2020
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Versiones del complemento File Manager anteriores a la 6.9

Descripción

El complemento de File Manager, proporciona a los administradores de sitios de WordPress funciones de copiar, pegar, editar, eliminar, descargar y cargar carpetas y archivos. Este complemento tiene más de 700,000 instalaciones activas.

La vulnerabilidad posee una puntuación de 10 en la escala de CVSS, por lo que es considerada una vulnerabilidad con una severidad crítica. Un atacante puede aprovecharse de esto para subir archivos y ejecutar código de forma remota en un sitio afectado.

Se detectó que la vulnerabilidad está siendo explotada por botnets. La vulnerabilidad radica en el código que se tomó del proyecto elFinder, un framework que provee una GUI de exploración de archivos para aplicaciones web. El código se publicó como ejemplo, pero se agregó al complemento de WordPress, lo que brinda a los atacantes acceso no autorizado para cargar archivos.

Los atacantes pueden aprovecharse de este tipo de vulnerabilidades para obtener acceso privilegiado a un sitio web y plantar código JavaScript malicioso, el cual les permite obtener los datos del usuario o propagar malware.

Actualización o Mitigación

Aplicar las actualizaciones para estas vulnerabilidades proporcionadas por WordPress. Para ello haga clic aquí.

Imagen 3. Imagen de referencia del producto afectado

Amenazas

Boletín	2020-253
Asunto	BOTNET FRITZFROG
Emisión	21/08/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Linux

Descripción

El malware ensambla y ejecuta un payload malicioso en la memoria, haciendo que esta sea volátil. Además, debido a su implementación personalizada de P2P, no se tiene un único servidor de comando y control (C2, abreviado en inglés) que envía instrucciones al malware.

Para comprometer servidores SSH FritzFrog hace uso de tácticas de fuerza bruta, obteniendo gran éxito. Desde que se detectó esta amenaza se identificó 20 versiones diferentes del binario de Fritzfrog.

El malware primero intenta conectarse a un servidor de destino a través de los puertos SSH 22 o 2222. Después de esto, FritzFrog ejecuta un cliente netcat en el puerto 1234 del servidor comprometido, este último se conecta con el servidor de la amenaza. Gracias a esto el malware puede recibir comandos.

FritzFrog también se comunica a través de un canal cifrado con más de 30 comandos. El malware utiliza el algoritmo Diffie-Hellman para su funcionalidad de intercambio de claves secretas, los comandos y las respuestas son enviados como objetos JSON. Los datos se cifran simétricamente mediante AES y se codifican con base64.

Se observó que todos los nodos de la botnet utilizan la misma clave SSH. Cuando surge la necesidad de compartir archivos entre los nodos de la botnet, Fritzfrog divide en los archivos en blobs, binarios con sumas de verificación, que se guardan en la memoria, esto garantiza la integridad de los archivos.

Cada nodo puede revisar a otro para obtener una lista de blobs que contiene, mediante el comando getblobstats. Uno por uno, todos los blobs son recibidos de esta manera por el nodo solicitante y se unen para producir un archivo.

Este en un malware particular, debido a la manera en la que se distribuye, tiene cierto aparecido a la amenaza Rakos, debido a que ambas son una botnet P2P y están escritas en Golang.

Boletín	2020-254
Asunto	NUEVO RANSOMWARE SMAUG
Emisión	25/08/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows, Linux y MacOS X

Descripción

Actualmente existen delincuentes que ponen ransomware que han desarrollado como servicio, a esto se le denominada RaaS, gracias a esto los ciberdelincuentes obtienen todo lo que necesitan para atacar a su víctima pese a que algunos no tienen el conocimiento o tiempo necesario para desarrollar esta herramienta maliciosa. Entre las características de este RaaS se tiene:

• Afecta a cualquier sistema operativo de 64 bits, de acuerdo con los creadores afecta tanto a Windows, Linux y MacOS X.

• La gestión del ataque, campaña, se hace a través de interfaz gráfica, debido a esto no es necesario tener muchos conocimientos técnicos.

• Los procesos relacionados con Smaug como la generación de claves, interacción con las víctimas, entre otros; se realizan de manera autónoma.

• El sistema de gestión Smaug permite gestionar distintos aspectos de la campaña como: La nota de rescate y el plazo máximo de pago.

• Smaug permite crear campañas masivas, en las que cada payload generará una clave única, así como específicas para empresas, en las que todas las amenazas emplearán la misma clave, esto se hace con el fin de facilitar el descifrado de todos los activos, si finalmente optan por pagar.

Smaug cuenta con un servicio de atención a la víctima para facilitar el proceso de recuperación de los archivos una vez se haya pagado el rescate.

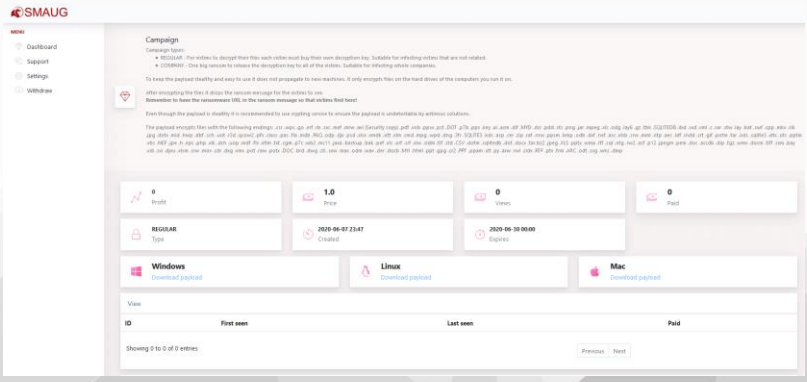


Imagen 4. Imagen de referencia de la interfaz del software malicioso

Boletín	2020-255
Asunto	CIBERCRIMINALES DE ORIGEN IRANÍ USAN DHARMA
Emisión	26/08/2020
CVE	CVE-2017-0213
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

• RDP

Descripción

Los atacantes detrás de esta campaña encuentran a sus víctimas escaneando direcciones IP de Internet en busca de conexiones de escritorio remoto (RDP, por sus siglas en inglés) expuestas, la herramienta que utilizan es Masscan, el cual es un scanner de puertos de código abierto.

Luego de esto utilizan NLBrute, la cual prueba una lista de contraseñas RDP con la intención de encontrar una que funcione. Una vez obtenido el acceso, intentan escalar en privilegios mediante la explotación de la vulnerabilidad CVE-2017-0213.

Se identificó que utilizan Dharma ransomware, este al ser un ransomware como servicio (RaaS, por sus siglas en inglés), hace posible que personas sin conocimientos técnicos puedan hacer ataques cibernéticos. Debido a que este proporciona un conjunto de herramientas que facilitan realizar esto.

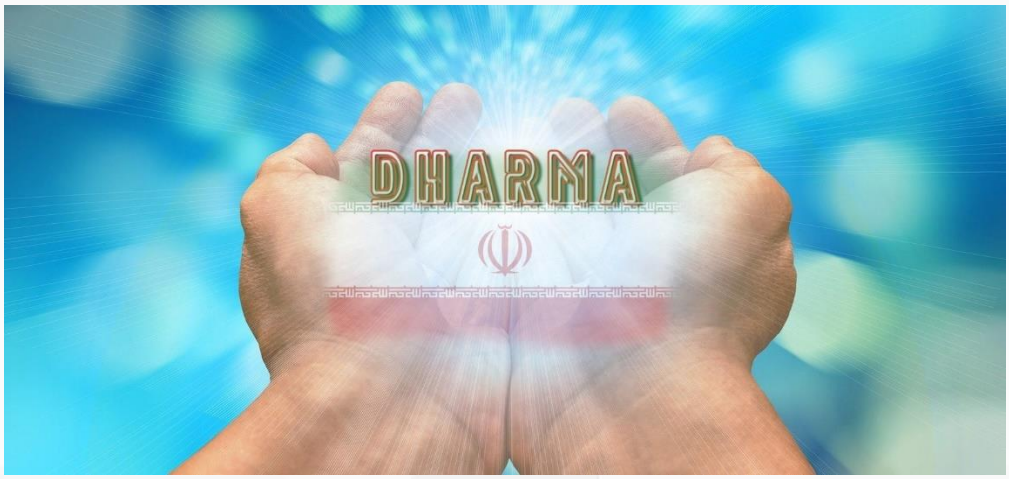


Imagen 5. Imagen de referencia de la amenaza

Boletín	2020-257
Asunto	LAZARUS ATACA A ORGANIZACIONES DE CRIPTOMONEDAS
Emisión	28/08/2020
CVE	No tiene
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

El Consejo de Seguridad de las Naciones Unidas publicó que los ciberdelincuentes de origen norcoreano estuvieron detrás de ataques de criptomonedas lo cual provocó una pérdida de 571 millones de dólares entre el 2017 y 2018. Se estima que actualmente hay más de seis mil atacantes de origen norcoreano.

Se detectó que recientemente Lazarus está detrás de un ataque de phishing dirigido a organizaciones del sector de las criptomonedas. Esta identificación fue posible debido a unos rasgos que se encontraron, los cuales son propios de este grupo como: La desactivación de las soluciones anti-malware y la eliminación de sus programas maliciosos en los dispositivos afectados.

Gracias al análisis de uno de los programas maliciosos, que se obtuvo a partir de un sistema infectado, gracias a esto se identificó las herramientas y las tácticas, técnicas y procedimientos (TPP, por sus siglas en inglés) usados los cuales se relacionan con Lazarus.

Para esta campaña los ciberdelincuentes están usando un documento word, el cual tiene una macro maliciosa incrustada, este se conecta a un enlace bit.ly, desde este se despliega los payloads finales del malware después de recopilar y filtrar la información del sistema afectado a los atacantes. Se ha observado que Lazarus también usa la herramienta de post-explotación Mimikatz de código abierto para obtener credenciales. Este grupo se encuentra continuamente en actividad.

Imagen 6. País de origen de los atacantes

Boletín	2020-259
Asunto	QBOT ROBA HILOS DE CORREO ELECTRÓNICO PARA DISTRIBUIRSE
Emisión	31/08/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operative Windows

Descripción

Qbot es un malware bancario y de robo de información, el cual tiene actividad registrada desde hace más de diez años. Una vez que la amenaza se instala en la computadora de la víctima, este intentará obtener la contraseña, cookies, tarjetas de crédito, correos electrónicos y credenciales bancarias de este.

En el 2019, Qbot comenzó a robar hilos de correo electrónico de sus víctimas, los cuales fueron usados en una campaña de phishing la cual fue detectada a fines de marzo de 2019. Esta táctica ha sido utilizada por los troyanos Gozi ISFB, URSNIF y Emotet.

Un ataque de phishing en cadena de respuesta se da cuando los atacantes de una amenaza usan un hilo de correo electrónico robado y luego responden ese correo con un mensaje el cual contiene un documento adjunto malicioso.

Después de infectar a la víctima, una de las primeras actividades maliciosas realizadas por Qbot es obtener correos electrónicos del cliente Outlook. Estos correos son enviados a los servidores que se encuentran bajo el control de las atacantes, la finalidad detrás de esto es usarlos en futuras campañas.

El archivo adjunto enviado contiene un ZIP con un script VBS malicioso. Cuando este se ejecuta se descarga el malware Qbot en el sistema e infectará al usuario. Los correos en los que es enviado esta amenaza tienen como temáticas pago de impuestos, la pandemia de Covid-19 y ofertas de trabajo.

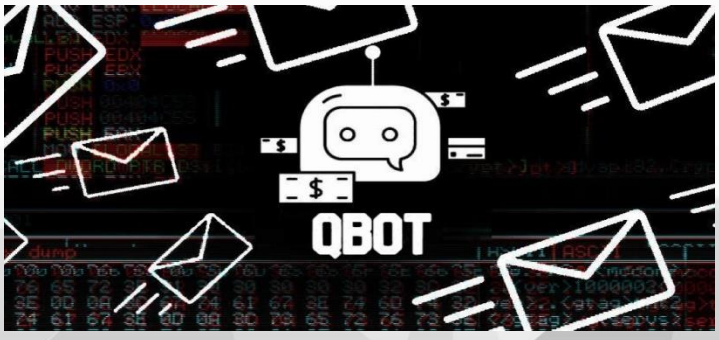


Imagen 7. Imagen de referencia de la amenaza

Boletín	2020-260
Asunto	NUEVA CAMPAÑA DE EMOTET
Emisión	31/08/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema Operativo Windows

Descripción

Esta campaña de spam pretende hacerse pasar por facturas, información de envío, información del covid-19, currículums, documentos financieros o documentos escaneados. En estos correos se adjuntan archivos maliciosos de Word o un enlace para descargar uno.

Cuando se abren los archivos, estos piden que se "habilite el contenido" para ejecutar macros. La nueva plantilla usada por esta amenaza fue detectada el 25 de agosto de 2020 y fue denominada "Red Dawn". En esta al igual que las anteriores se pide que se "habilite el contenido", lo cual conduce a que se ejecuten macros maliciosas que descargan e instalan el malware Emotet en la computadora de la víctima.

Emotet es actualmente el malware más extendido dirigido a los usuarios en la actualidad. Este puede instalar otros malwares como Trickbot y QBot en la computadora de la víctima.

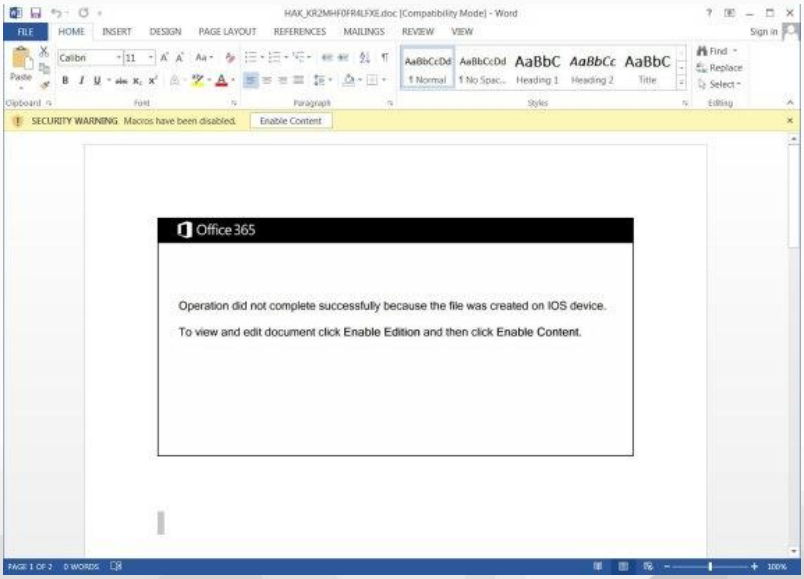


Imagen 8. Imagen de referencia del archivo usado por la amenaza

Boletín	2020-261
Asunto	ATAQUES DEL GRUPO ULTRARANK
Emisión	01/09/2020
CVE	No tiene
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

Sistema Operativo Windows

Descripción

UltraRank a través de tiempo ha cambiado sus tácticas e infraestructura varias veces. Lo cual dificulta asociar una campaña o ataque a este grupo. Sin embargo, se ha conseguido asociar este grupo a los incidentes del grupo 2, 5 y 12 de Magecart.

Entre estas tres campañas ejecutadas en 2015, 2016 y 2018; los ciberdelincuentes consiguieron instalar JS-sniffers en 691 sitios web con una gran cantidad de tráfico. Sin embargo, esta cifra podría variar, debido a que los ciberdelincuentes han afectado a 13 proveedores de servicios web de diseño, marketing, desarrollo, publicidad y notificaciones del navegador; los cuales probablemente son usados en todo el mundo.

Las tres campañas se basaron JS-sniffers denominadas FakeLogistics, WebRank y SnifLite. Estas comparten algunas características e infraestructura como:

Métodos similares para ocultar la ubicación del servidor y los patrones para el registro de dominio. Almacenar el código malicioso en varias ubicaciones con diferentes nombres de dominio. Ataques a la cadena de suministro y a un solo objetivo.

A fines del 2019 UltraRank ganó hasta 50,000 dólares americanos. La monetización fue posible gracias a ValidCC, una tienda que vende datos a cambio de un pago. Se pudo observar que la relación entre UltraRank y ValidCC va más allá de la venta, debido a que UltraRank ha utilizado su infraestructura para atacar sitios web de phishing que se hacen pasar por ValidCC.

Imagen 9. Imagen de referencia de la amenaza

Boletín	2020-262
Asunto	ACTIVIDAD DEL GRUPO BEAGLEBOYZ
Emisión	01/09/2020
CVE	No tiene
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

Infraestructura de sistemas financieros

Descripción

BeagleBoyz tiene como objetivo a bancos en más de 30 países, esto tiene como intención obtener 2 millones de dólares en ganancias. Esta información ha sido confirmada por el Comando Cibernético de Estados Unidos (USA, por sus siglas en inglés).

Desde febrero de 2020, Corea del Norte ha vuelto a apuntar a bancos en varios países para iniciar transferencias de dinero internacionales fraudulentas y retiros de efectivo en cajeros automáticos. El reciente resurgimiento sigue a una pausa desde finales de 2019.

De acuerdo con lo observado, en un solo ataque, se detectó que los atacantes pudieron retirar efectivo de los automáticos de decenas de distintos bancos de distintas partes del mundo, incluido USA.

BeagleBoyz también hace uso del esquema de fraude SWIFT, lo cual le permitió obtener ganancias ilícitas por 81 millones de dólares americanos del Banco Bangladesh en el año 2016.

BeagleBoyz forma parte de la Oficina General de Reconocimiento del gobierno de Corea del Norte y ha estado activo desde el año 2014, afectando a distintos bancos en todo el mundo. Para sus ataques BeagleBoyz utiliza distintas herramientas y técnicas para obtener acceso a la red de una institución financiera, aprender la topología, descubrir sistemas clave y monetizar su acceso.

Imagen 10. Imagen de referencia de los países que han sido víctimas de BeagleBoyz

Boletín	2020-264
Asunto	TELEGRAM ES APROVECHADO POR LOS ATACANTES
Emisión	03/09/2020
CVE	No tiene
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

Páginas de e-commerce

Descripción

El servicio de mensajería encriptado está siendo utilizado por los grupos de Magecart para enviar detalles de pagos obtenidos de sitios web comprometidos por los ciberdelincuentes. Para estos, este mecanismo es eficiente y no requiere que se mantenga una infraestructura que se podría bloquear o inhabilitar.

Inyectar e-skimmers en sitios web de compras mediante la explotación de una vulnerabilidad conocida o credenciales obtenidas ilícitamente para conseguir detalles de tarjetas de crédito es un modus operandi propio de Magecart, un consorcio de diferentes grupos de cibercriminales.

Durante los últimos meses han estado intentando ocultar el código malicioso del skimer dentro de los metadatos de las imágenes, e incluso llevar a cabo ataques homógrafos. Lo novedoso es que ahora los atacantes envían los datos como el nombre, la dirección, el número de la tarjeta de crédito, la fecha de vencimiento y el CVV a través de un canal privado de Telegram usando un ID de bot codificado en el código del skimmer.

La ventaja de usar Telegram es que los atacantes ya no tienen que configurar una infraestructura de comando y control (C2, abreviado en inglés) separado para transmitir la información recopilada ni arriesgarse a enfrentar la posibilidad de que esos dominios sean eliminados o bloqueados por servicios anti-malware.

Imagen 11. Imagen del servicio que se encuentra siendo aprovechado

Boletín	2020-266
Asunto	ACTIVIDAD DEL RANSOMWARE SODINOKIBI
Emisión	07/09/2020
CVE	CVE-2018-8453 y CVE-2019-2725
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

Páginas de e-commerce

Descripción

Sodinokibi es un ransomware para sistemas Windows cuya propagación sigue el modelo de ransomware como servicio (RaaS, por sus siglas en inglés). Para infectar a sus víctimas, recurre a diferentes técnicas de ofuscación, principalmente basada en criptografía, para dificultar su análisis e identificación de sus firmas por parte de otros programas de seguridad, como antivirus o sistemas de detección de intrusión (IDS, por sus siglas en inglés).

Este ransomware se ha distribuido a nivel mundial, siendo Asia la región más afectada. Sus principales vectores de propagación son:

• Envío de correos maliciosos, mediante campañas de spam.

• Publicidad maliciosa o malvertising, es decir código malicioso presente en los anuncios que aparecen durante la navegación web, tanto para ser ejecutado directamente en el equipo, como para redirigir a servidores donde se descargan otros ejecutables.

• Ataques de fuerza bruta sobre el protocolo Remote Desktop Protocol (RDP, por sus siglas en inglés).

• Explotación de vulnerabilidad CVE-2019-2725 que afecta a sistemas Oracle (actualización disponible desde el 26 de abril de 2019).

Para ejecutarse la amenaza se empaqueta de forma personalizada, todas las cadenas de texto, nombres de librerías y archivos DLL se empaquetan mediante el algoritmo criptográfico RC4, empleando una clave aleatoria diferente y de longitud variable para cada uno de los elementos cifrados. De esta forma, las cadenas de texto, las tablas API y las referencias a librerías en las que se basa habitualmente el software antivirus para detectar código malicioso resultan ineficaces en su identificación.

Una vez que el código malicioso se ejecuta en el sistema de la víctima, su primera acción es generar un identificador o mutex, para evitar que entre más de un proceso a la vez en la sección crítica.

De esta forma, previene fallos de funcionamiento y dificulta su detección. El siguiente paso es descifrar la configuración incrustada en su código en formato JSON, que dará las operaciones que llevará a cabo en función de los parámetros que haya seleccionado el suscriptor del servicio malicioso, por lo que podrán variar de unos a otros.

Posteriormente intenta la escalada de privilegios en el sistema. Si no obtiene estos privilegios, el programa finaliza y el ataque fracasa, en caso contrario, el programa recopila datos de configuración del sistema y de sesión, también comprueba el idioma del interfaz o del teclado y si coincide con alguno de los excluidos en la configuración, el programa finaliza. En caso no se confirme la exclusión por el idioma, la amenaza continua su ejecución desactivando las opciones de restauración del sistema, el proceso vssadmin y utilizando bcdedit, para evitar las copias de seguridad y borrar todas las instantáneas.

Antes de proceder al cifrado de los archivos, Sodinokibi buscará el proceso "explorer.exe" para obtener el token de sesión del usuario que está utilizando el equipo, y, mediante la función ImpersonateLoggedOnUser, disminuir los privilegios del código malicioso, evitando de esta forma que el entorno de usuario de "SYSTEM" se vea afectado en la operación de cifrado de los archivos.

Una vez hecho esto, comienza el cifrado de los archivos, tanto de las unidades locales como de las unidades de red conectadas al mismo.

Sodinokibi se distribuye con dos claves públicas diferentes: una clave, como parte de la configuración JSON que corresponde con el parámetro pk, y otra clave que está integrada en el binario. Estas claves públicas son utilizadas para cifrar el par de claves pública-privada que se genera localmente.

De acuerdo con lo observado y a múltiples fuentes recientemente Telecom Argentina, Agrosuper y Banco Estado de Chile se vieron afectados por este ransomware. Telecom Argentina se vio afectado durante el mes de agosto de 2020, mientras que las últimas organizaciones durante el mes de septiembre de 2020. Para más información sobre esta amenaza ver Boletín 2020-136, Boletín 2020-180 y Boletín 2020-198.

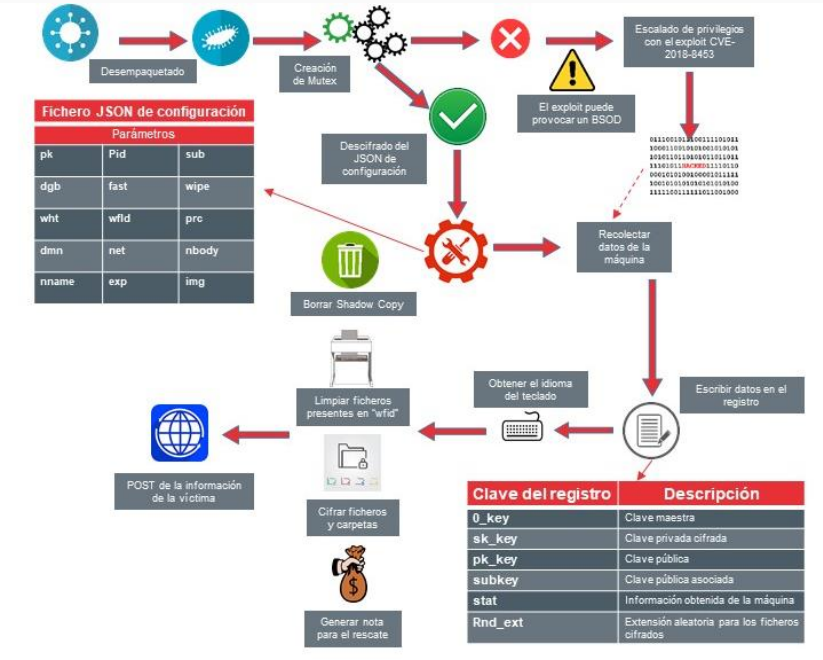


Imagen 12. Imagen de referencia del esquema de funcionamiento de Sodinokibi

5. Recomendaciones

- Leer los boletines citados en las amenazas que tengan uno asociado, esto con la finalidad de encontrar más información de la amenaza como: Una mayor descripción, Indicadores de compromiso, recomendaciones personalizada y fuentes por amenaza.
- Considerar deshabilitar PowerShell y Macros de Microsoft, evitando que pueda ser aprovechado por softwares maliciosos.
- Utilizar una política de uso de contraseñas seguras considerando la complejidad, el cambio de credenciales por defecto y la no reutilización de las mismas.
- Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad. (Conectados y desconectados)
- No exponer servicios RDP (Escritorio Remoto) a Internet, para acceso remoto utilizar sistemas VPN actualizados.
- Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.
- Bloquear los indicadores de compromisos (IOC) compartidos, en los dispositivos de seguridad de su infraestructura.
- Verificar la información de la cuenta que envía el correo, el nombre y la dirección del destinatario para identificar si son sospechosas.
- No abrir correos electrónicos de dudosa procedencia (remitente desconocido), ni dar clic en enlaces, ni descargar archivos adjuntos desconocidos.
- Escanear todo el software descargado de Internet antes de la ejecución.
- De detectar un correo spam, phishing o cualquier actividad anómala reportarlo. inmediatamente a los encargados de seguridad de la información de su institución.

* Antes de realizar el bloqueo de IoC’s es importante que previamente en ambiente de desarrollo se valide y confirme a nivel de sus servicios internos y externos, con el propósito de aplicar los cambios de manera controlada.

** Es importante que previamente en ambiente de desarrollo se valide y confirme a nivel de los servicios, con el propósito de aplicar los cambios de manera controlada.