SECURESOFT CORPORATION

e-Secure Consulting Group

REPORTE SEMANAL DE CIBERINTELIGENCIA

SECURESOFT

Fecha:

13 abril de 2020

Equipo de Ciber inteligencia
CIB-FOR-2020-002

El presente documento contiene información para la comunidad de ciberseguridad.

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 a cada vulnerabilidad y amenaza que se ha hecho pública en el transcurso del 06 hasta el 14 de abril del 2020.

3. Amenazas

Boletín	Boletín 2020-135
Asunto	Malware Anarchygrabber Discord
Emisión	06/04/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows.

Descripción

AnarchyGrabber es un malware popular distribuido en foros de hacking y en videos de YouTube, el cual puede robar tokens de usuarios de Discord conectado cuando se ejecuta.

Estos tokens de usuario se vuelven a cargar en un canal de Discord bajo el control del atacante, donde el actor de la amenaza puede recolectarlos y usarlos para iniciar sesión como sus víctimas.

La versión original del malware es detectada fácilmente por los softwares de seguridad y solo roba tokens mientras se está ejecutando. Para que sea más difícil de detectar mediante antivirus y ofrecer persistencia, los cibercriminales han actualizado el malware AnarchyGrabber para que modifique los archivos JavaScript utilizados por el cliente Discord e inyecte su código cada vez que se ejecuta.

La nueva versión denominada AnarchyGrabber2, cuando se ejecuta, modifica el archivo % AppData% \ Discord \ [versión] \ modules \ discord_desktop_core \ index.js para inyectar JavaScript. Cuando se ejecuta AnarchyGrabber2, el archivo index.js se modifica para inyectar archivos JavaScript adicionales desde una subcarpeta 4n4rchy.

Imagen 1. Logo del producto afectado

Boletín	Boletín 2020-136
Asunto	Interpol advierte de incremento de ataques de ransomware a hospitales
Emisión	07/04/2020
CVE	CVE-2019-11510 y CVE-2019-19781
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows, Pulse Secure VPN, Citrix ADC, entre otros.

Descripción

Los atacantes detrás de Maze publicaron datos robados de una compañía de análisis de medicinas; por otro lado, Ryuk continúa atacando hospitales a pesar de que la mayoría de ellos están que atienden los nuevos casos de covid-19. Microsoft advirtió a varios hospitales sobre vulnerabilidades en dispositivos VPN, esto con el fin de ayudarlos ante los ataques de REvil ransomware, entre las vulnerabilidades que notificó se encuentra la CVE-2019-19781. La Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA, por sus siglas en inglés) notificó una vulnerabilidad rastreada con el CVE-2019-11510, esta afecta a servidores VPN de Pulse Secure.

Los ciberdelincuentes utilizan correos de malspam para atacar estas organizaciones, estos por lo general vienen con un archivo malicioso adjunto, el cual contienen algún malware.

Ante esto el equipo de Respuesta ante amenazas cibernéticas (CTR, por sus siglas en inglés) de la INTERPOL, comunicó que ha detectado un incremento significativo de ataques de ransomware contra organizaciones e infraestructura dedicada a combatir el Covid-19. Por lo que el CTR de INTERPOL se encuentra recopilando información sobre las amenazas relacionadas con la pandemia del Covid-19.

Imagen 2. Publicación en twitter de la Interpol.

Boletín	Boletín 2020-137
Asunto	Botnet Dark_nexus es usada para realizar DDoS
Emisión	08/04/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Routers, grabadoras de video y cámaras térmicas.

Descripción

La Botnet Dark_nexus, comparte características similares con otras. Sin embargo, debido a la forma en la que ha sido desarrollado, posee módulos especiales que lo hace más potente y robusto que otros.

Esta botnet tiene características similares con el malware bancario Qbot y Mirai. Cuando la botnet se empieza a ejecutar en la computadora de la víctima se bifurca varias veces, bloquea señales, y se separa de la terminal; comportamiento similar al de Qbot. Luego, al igual que Mirai, se une a un puerto fijo, asegurándose de que sólo haya una instancia de este bot ejecutándose.

Cuenta con un Servidor de Comando y Control (C2, abreviado en inglés), desde el cual se emite comandos a los bots infectados y se registra la arquitectura de CPU de la víctima para posteriormente enviar el payload a través de Telnet.

Dark_nexus también puede evitar que el dispositivo se reinicie, eliminando servicios que podrían usarse para lograr ello.

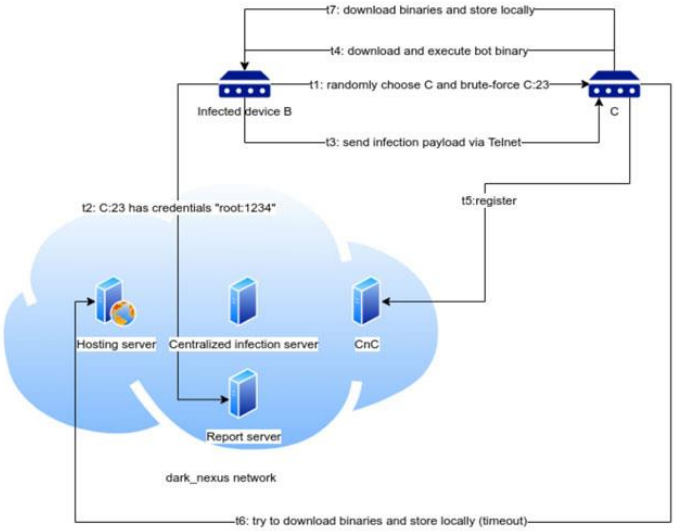

Imagen 3. Descripción de la red y proceso de infección de Dark_nexus

Boletín	Boletín 2020-138
Asunto	Vulnerabilidades críticas de Grandstream y Draytek son explotadas
Emisión	08/04/2020
CVE	CVE-2020-5722 y CVE-2020-8515
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

Grandstream UCM6200 y Draytek Vigor 2960, 3900 y 300B.

Descripción

Las vulnerabilidades asignadas a los CVE-2020-5722 y CVE-2020-8515 son consideradas críticas debido a que son fácilmente explotables. Si un atacante tiene éxito al momento de explotar estas vulnerabilidades puede ejecutar comandos de manera arbitraria en el dispositivo.

• La vulnerabilidad asignada al CVE-2020-8515 se debe a que el ejecutable /www/cgi-bin/mainfunction.cgi no filtra correctamente el parámetro keyPath durante la autenticación, lo que permite inyectar comandos.

• La vulnerabilidad asignada al CVE-2020-5722, se debe a que no se valida correctamente el parámetro user_name, lo que genera una inyección de SQL.

A raíz de estas vulnerabilidades, los atacantes han creado un malware denominado "Hoaxcalls", el cual es capaz de realizar una variedad de ataques de DDoS, comunicandose con un Servidor de Comando y Control (C2, abreviado en inglés) para recibir comandos y explotar las vulnerabilidades anteriormente mencionadas.

Hoaxcalls es un bot DDoS que se comunica con su servidor C2 a través del protocolo Internet Relay Chat (IRC). Al recibir un comando C2, se propaga escaneando e infectando dispositivos vulnerables utilizando exploits de CVE-2020-8515 y CVE-2020-5722.

El malware cifra sus comunicaciones utilizando el esquema de cifrado XOR estándar, este tipo de cifrado es usado por las variantes del malware Mirai. Luego de que la computadora infectada establece contacto con su servidor C2 utilizando el puerto TCP 1337 a través de IRC. El nick, ident y user enviados al servidor son cadenas con longitud de 13 caracteres, estos comienzan con XTC, seguidas de 9 caracteres aleatorios. Basado en los comandos que recibe la computadora infectada desde el C2, hoaxcalls realiza diferentes tipos de operaciones.

Boletín	Boletín 2020-139
Asunto	VMware corrige vulnerabilidad crítica de vCenter Server
Emisión	13/04/2020
CVE	CVE-2020-3952
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

vCenter Server desde 6.7 hasta versiones anteriores 6.7u3f

Descripción

vCenter Server es una utilidad de VMware que proporciona a los administradores de TI una administración centralizada de hosts virtualizados, y máquinas virtuales dentro de entornos empresariales desde una sola consola.

La vulnerabilidad asignada al CVE-2020-3952, tiene una severidad crítica. Esta sólo afecta al servicio de directorio VMware (vmdir, abreviado en inglés) en instalaciones actualizadas, y se debe a controles de acceso implementados incorrectamente, si es que se actualizó desde una línea de lanzamiento anterior como 6.0 o 6.5. Las instalaciones limpias de vCenter Server 6.7 no se ven afectadas.

Esta vulnerabilidad puede ser aprovechado por un atacante para obtener información confidencial que puede usarse para comprometer vCenter Server u otros servicios que dependen de vmdir para autenticarse.

Actualización o mitigación

Aplicar las actualizaciones ubicadas en el punto “4.References” en el siguiente enlace, VMware Security Advisories

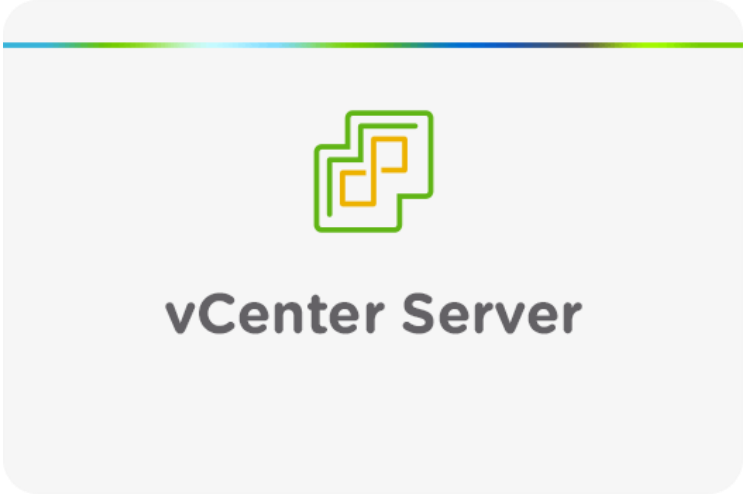

Imagen 4. Logo del producto afectado.

Boletín	Boletín 2020-140
Asunto	Actualizaciones en productos de Palo Alto Networks
Emisión	13/04/2020
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Secdo para Windows, todas las versiones

• GlobalProtect Agent para Linux ARM, versiones anteriores a la 5.0.8 y la 5.1.1

• PAN-OS, versiones anteriores a la 8.1.13 y 9.0.7, y anteriores a la 9.0.7 en las series PA-7000 con LFC

• Traps para Windows, versiones anteriores a la 5.0.8 y la 6.1.4

Descripción

- **CVE-2020-1984**

  Secdo intenta ejecutar un script en una ruta de código, esto podría permitir a un usuario local, autentificado, acceder a la raíz del disco del sistema operativo (C:\), mediante 'crear carpetas o añadir datos', para obtener privilegios del sistema si la ruta no existe, o si se permite la escritura en ella.

- **CVE-2020-1985**

  En Secdo, los permisos por defecto incorrectos en la carpeta C:\Programdata\Secdo\N-Logs, podría permitir a los usuarios locales, autentificados, sobrescribir los archivos de sistema y obtener la escalada de privilegios.

- **CVE-2020-1989**

  La asignación inadecuada de privilegios cuando se escriben archivos específicos de la aplicación en el Agente GlobalProtect, podría permitir a un usuario local, autentificado, obtener privilegios de root en el sistema.

- **CVE-2020-1990**

  Vulnerabilidad de desbordamiento de búfer “basado en pila” en el componente del servidor de gestión de PAN-OS, podría permitir a un usuario autentificado subir una configuración de PAN-OS corrupta y ejecutar código con privilegios de root.

- **CVE-2020-1991**

  Vulnerabilidad de archivo temporal inseguro en Traps, podría permitir a un usuario local, autentificado, escalar privilegios o sobrescribir archivos de sistema.

- **CVE-2020-1992**

  Vulnerabilidad de cadena de formato en el demonio Varrcvr de PAN-OS, en dispositivos de la serie PA-7000 con una tarjeta de reenvío de registros (LFC, Log Forwarding Card), podría permitir a los atacantes remotos bloquear el demonio creando una condición de negación de servicio, o ejecutar potencialmente códigos con privilegios de root.

Actualización o mitigación

Para ver las actualizaciones o mitigaciones de cada vulnerabilidad consultar el enlace del Boletín 2020-140, ubicado en la tabla de la página anterior.

Boletín	Boletín 2020-141
Asunto	Explotación de vulnerabilidades de día cero cada vez es más común
Emisión	13/04/2020
CVE	CVE-2018-0802, CVE-2018-4878, CVE-2018-15982, CVE-2019-0703, CVE-2019-0859, CVE-2019-2215 y CVE-2019-3568
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Sistema operativo iOS

• Sistema operativo Android

• Sistema operativo Windows

Descripción

Desde fines del 2017, se observó cómo se incrementó significativamente el número de ataques de este tipo realizados por grupos de ciberdelincuentes. Estos ataques fueron contra objetivos ubicados en Medio Oriente.

Asimismo, se notó la explotación de estas vulnerabilidades por parte de grupos que no se han conseguido identificar. Ejemplo de esto fue en el 2019, cuando se informó de un exploit de día cero de WhatsApp, la vulnerabilidad que se explotó fue asignada al CVE-2019-3568, se aprovecha esta vulnerabilidad para distribuir spyware, malware de espionaje.

Finalmente se detectó que algunos grupos de espionaje de países también se han aprovechado de estas vulnerabilidades:

• En el 2016 se detectó que un grupo de espionaje chino, APT33, explotó la vulnerabilidad CVE-2019-0703.

• En el 2017 el grupo norcoreano APT37 explotó una vulnerabilidad de Adobe Flash, la cual fue asignada al CVE-2018-4878.

• A fines del 2017 y 2018, grupos chinos se aprovecharon de la vulnerabilidad CVE-2018-0802.

Boletín	Boletín 2020-142
Asunto	Aumento del número de estafas relacionados al Coronavirus
Emisión	14/04/2020
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Páginas web de comercio electrónico y Servicios de VoIP

Descripción

Según la Comisión Federal de Comercio (FTC, por sus siglas en inglés), los consumidores informaron más de 16 mil fraudes relacionados con el coronavirus. La mayoría de estos vienen de California con 2010 víctimas, seguido de Florida, Nueva York y Texas con más de 1000 víctimas cada uno.

Por otro lado, también se registraron más de 2800 intentos de estafa relacionados a viajes y vacaciones, mientras que las relacionadas a las compras en línea y basadas en mensajes de texto registraron 1741 y 1017 informes.

Ante esto la FTC notificó a los consumidores que los atacantes se están aprovechando del actual contexto mundial creando sitios web para vender productos falsos, para ello utilizan mensajes de texto, correos electrónicos y publicaciones en redes sociales para atraer a sus víctimas.

En el mes de marzo se advirtió que los atacantes usaron los servicios de VoIP para realizar estafas, esto fue notificado por la FTC. En abril, el Servicio de Impuestos Internos (IRS, por sus siglas en inglés) publicó que los atacantes estaban usando correos electrónicos, redes sociales y llamadas telefónicas, solicitando información personal de la víctima, para lograr ello le hacen creer que obtendrá algún tipo de beneficio económico.

Imagen 5. Escudo de la Comisión Federal de Comercio, FTC.

Asunto	Actualización de amenazas identificadas durante el periodo del Coronavirus
Emisión	14/04/2020
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Navegador web y VPN

Descripción

- Se sospecha que el grupo DarkHotel, es el responsable detrás de los ataques realizados al gobierno chino. En este ataque se distribuían archivos maliciosos los cuales afectaron a más de 200 servidores VPN, en estos servidores se instalaron backdoors. A este mismo grupo se le atribuye un intento de ataque contra la Organización Mundial de la Salud (OMS) registrado en marzo del 2020.

- Se detectó que el navegador Safari presenta varias vulnerabilidades las cuales pueden ser aprovechadas por los atacantes para tener acceso a la cámara web de la víctima. Las vulnerabilidades son las siguientes: CVE2020-3852, CVE-2020-3864, CVE-2020-3865, CVE-2020-3885, CVE-2020-3887, CVE-2020-9784, y CVE-2020-9787.

- El FBI detectó una campaña en la cual un atacante pretende estafar a sus víctimas haciéndoles creer que vende equipo de protección y suministros para combatir el Coronavirus. Este es un ataque de ingeniería social, según un reporte del FBI este tipo de ataques a generado pérdidas por 1,7 mil millones de dólares americanos en el 2019.

Imagen 6. Escudo del FBI, una de las fuentes citadas.

Asunto	Campañas de phishing detectadas
Emisión	14/04/2020
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Cisco Webex y WhatsApp

Descripción

- Los ciberdelincuentes se están aprovechando del actual contexto mundial para atacar plataformas de trabajo remoto como Cisco Webex. Para ello utilizan correos maliciosos con los cuales pretenden engañar a las víctimas haciéndoles creer que necesitan actualizar su aplicación, el correo enviado tiene como asunto "¡Actualización crítica" o "¡Alerta!", en este mismo correo se le solicita a la víctima que ingrese al siguiente enlace hxxps://globalpagee-prod-webex[.]com/signin, el correo es enviado desde Meetings[@]webex[.]com.

- Se detectó una campaña de phishing que estaba siendo distribuida a través de WhatsApp. Esta pretende obtener información de la víctima haciéndole creer que si llena un formulario obtendrá gigabytes adicionales para navegar por internet. Cuando la víctima llena el formulario, le aparece un mensaje en el cual se le felicita por haber ganado 500 GB por 90 días y se le sugiere compartir el link de la página vía WhatsApp, comprometiendo a los dispositivos que reciban y lo abran.

Indicadores de Compromiso (IoC's)

Correo

Meetings[@]webex[.]com

Dominio

cdn[.]foxpush[.]net

URL

hXXps://xmasth[.]me/Activar-4G/
hxxps://globalpagee-prod-webex[.]com/signin

4. Recomendaciones

- Leer los boletines citados en las amenazas que tengan uno asociado, 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, para evitar 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.
- 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.
- Si detectan un correo spam, phishing o cualquier actividad anómala, repórtalo inmediatamente a los encargados de seguridad de la información de su institución.

* Antes de realizar el bloqueo de IOCs es importante que previamente en el 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.