SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Semanal de Ciberinteligencia Securesoft

Fecha:

22 mayo de 2020

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia
CIB-FOR-2020-002

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 29 de abril hasta el 22 de mayo del 2020.

3. Amenazas

Boletín	2020-155
Asunto	ASNARÖK MALWARE EXPLOTA LA VULNERABILIDAD EN LOS FIREWALLS SOPHOS XG
Emisión	29/04/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Todas las versiones del firmware de Sophos XG Firewall físicos y virtuales, sin el hotfix aplicado

Descripción

La vulnerabilidad radica en un error SQL de pre-autorización, el ataque permite a los cibercriminales realizar la ejecución remota de código. Desde entonces, Sophos ha publicado una actualización para mitigar el riesgo de ataques de Asnarök.

Los atacantes detrás de la campaña utilizan nombres de dominio que parezcan legítimos con las palabras "Actualización del firewall de Sophos" para alojar los scripts de shell de Linux.

Al insertar un comando de una línea en una tabla de base de datos en dispositivos específicos, los atacantes pueden usar un servidor remoto para descargar Install.sh. Luego, la cadena de interrupción continúa con una serie de tareas que se ejecutan cada tres a seis horas, intentando descargar otros scripts hasta que el troyano se guarda en el sistema de archivos como el payload final.

El malware funciona buscando información en el firewall, como la licencia y el número de serie, la cuenta de correo electrónico del administrador y cualquier otra cuenta de correo electrónico de usuarios que pueda estar almacenada en el dispositivo. Asnarök también tiene el potencial de robar el hash del administrador, las contraseñas cifradas, las ID de usuario, y los detalles del sistema operativo.

Los actores de amenazas pueden cubrir sus huellas haciendo que el troyano elimine todos los archivos temporales creados. Esto generalmente ocurre solo una vez que ha recopilado los datos, los ha cifrado con OpenSSL y los ha enviado a una dirección IP de terceros.

Boletín	2020-156
Asunto	VULNERABILIDADES CRÍTICAS DE PLUGINS DE ELEARNING PARA WORDPRESS
Emisión	30/04/2020
CVE	CVE-2020-6008 y CVE-2020-6009, CVE-2020-6010 y CVE-2020-11511
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

Plugins LMS para WordPress (LearnPress, LearnDash y LifterLMS)

Descripción

Las vulnerabilidades presentes en las plataformas de LMS son:

LearnPress: De inyección SQL Blind (CVE-2020-6010) hasta el escalamiento de privilegios (CVE-2020-11511), que puede autorizar a un usuario existente a obtener el rol de maestro.

LearnDash: De inyección SQL (CVE-2020-6009) que permite a un adversario a través del simulador de servicio de mensajes de Notificación de Pago Instantáneo (IPN, por sus siglas en inglés) de PayPal activar transacciones de inscripción en cursos.

LifterLMS: De escritura arbitraria de archivos (CVE-2020-6008) explota la naturaleza dinámica de las aplicaciones PHP para permitir que un atacante, por ejemplo, un estudiante registrado en un curso específico cambie su nombre de perfil en el código PHP.

Imagen 1. Logo del producto afectado

Boletín	2020-157
Asunto	NUEVO RANSOMWARE VCRYPT
Emisión	04/05/2020
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

Plugins LMS para WordPress (LearnPress, LearnDash y LifterLMS)

Descripción

Cuando se ejecuta el ransomware en la computadora de la víctima, primero inicia Internet Explorer, en esta aplicación se muestra una nota de rescate llamada help.html, la cual se encuentra escrita en francés. En ella, se le sugiere a la víctima acceder al enlace de la nota para poder recuperar sus archivos. En paralelo se elimina los archivos de las carpetas, luego crea una carpeta la cual posee la extensión vcrypt.

Después de analizar una muestra del ransomware se determinó que este no encripta ningún archivo. Lo que hace es configurarse para ejecutarse automáticamente y extraer el programa 7za.exe en la carpeta %Temp%, el cual permite al atacante ejecutar comandos de 7zip.

Luego el ransomware ejecuta comandos que le permiten crear carpetas de Windows protegidas con contraseña. Todos los archivos creados poseen la misma contraseña. De momento no se ha identificado cual es el vector de infección de este ransomware.

Imagen 2. Logo de uno de los productos afectados

Boletín	2020-158
Asunto	VULNERABILIDADES EN EL SOFTWARE SALTSTACK
Emisión	05/05/2020
CVE	CVE-2020-11651 y CVE-2020-11652
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

SaltStack Salt versiones anteriores a la 3000.2

Descripción

Las vulnerabilidades fueron asignadas al CVE-2020-11651 y CVE-2020-11652, a continuación, la descripción de ambas vulnerabilidades:

• El CVE-2020-11651, es una vulnerabilidad de omisión de autenticación. Esta se debe a que la clase ClearFuncs procesa solicitudes no auténticas, exponiendo el método _send_pub(). Este último es usado para poner en cola mensajes al servidor, estos pueden ser usados para ejecutar comandos arbitrarios como root.

• El CVE-2020-11652, es una vulnerabilidad de directorio transversal. Esta se debe a que el método get_token(), se encuentra dentro de una clase que permite solicitudes sin autenticación. Esto permite la inserción de elementos y lectura de archivos fuera del directorio previsto.

Ambas vulnerabilidades se encuentran en ZeroMQ, protocolo de comunicaciones de alto rendimiento orientado a mensajes, y destinada a la construcción de aplicaciones distribuidas. Hasta el momento se ha detectado 6,000 instancias vulnerables de Salt expuesta en internet. No se han encontrado exploits que permitan aprovechar estas vulnerabilidades.

Actualización o Mitigación

Aplicar las actualizaciones proporcionada por SaltStack para corregir las vulnerabilidades. Haga clic en el siguiente link https://docs.saltstack.com/en/latest/topics/releases/3000.2.html

Imagen 3. Logo del producto afectado

Boletín	2020-159
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE CITRIX SHAREFILE
Emisión	06/05/2020
CVE	CVE-2020-7473, CVE-2020-8982 y CVE-2020-8983
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

ShareFile locales versiones 5.9.0 / 5.8.0 /5.7.0/ 5.6.0 / 5.5.0 y anteriores

Descripción

Los problemas de seguridad identificados afectan específicamente a los controladores de la zona de almacenamiento de Citrix ShareFile, componente encargado de almacenar los datos corporativos.

Las vulnerabilidades han sido asignados al CVE-2020-7473, CVE-2020-8982 y CVE-2020-8983. Según Citrix, sí un atacante no autenticado explota de manera exitosa estas vulnerabilidades puede comprometer el controlador de zonas de almacenamiento, permitiéndole acceder a los documentos y carpetas de los usuarios de ShareFile.

Se sospecha que estas vulnerabilidades se deben al uso de un antiguo kit de herramientas de ASP.net que Citrix Sharefile utilizaba. Ese kit es AjaxControlToolkit, este posee una vulnerabilidad de ejecución remota de código y recorrido de directorio, las cuales fueron asignadas al CVE-2015-4670 en el año 2015. Se publicó que este kit fue utilizado en las versiones vulnerables de Sharefile.

Actualización o Mitigación

Aplicar las actualizaciones y recomendaciones de Citrix. Haga clic en el siguiente link: https://support.citrix.com/article/CTX269106

Imagen 4. Logo del producto afectado

Boletín	2020-160
Asunto	TRICKBOT APROVECHA TEMÁTICA DE CORONAVIRUS PARA DISTRIBUIRSE
Emisión	07/05/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Trickbot es un troyano bancario, que al infectar la computadora de una víctima la agrega a una red de bots que permite a los atacantes tener control sobre ella. Esto también trae como consecuencia la filtración de cuentas bancarias, fraude electrónico, y el posible uso de la computadora comprometida en futuros ataques.

El correo electrónico usado en esta campaña contiene tres archivos, dos son imágenes y un documento. El documento pide al usuario que habilite las macros, para otorgarle autenticidad a este archivo ponen por nombre "Licencia familiar y médica de la Ley 22.04.doc" dando la apariencia de que es un archivo del gobierno de Estados Unidos. Pero lo que en verdad hace el archivo es descargar un archivo bat denominado terop.bat.

El archivo terop.bat al ejecutarse intenta descargar un ejecutable de la siguiente url sospechosa: hxxps://www[.]omegasystemsuae[.]com/9hfudnsfl[.]exe.

Este archivo está configurado para guardase en %APPDATA%\Bio_Tecs.exe. Adicionalmente, se ha identificado que terop.bat contiene los comandos TIMEOUT/T 30 y ping 8.8.8.8, los cuales utiliza para evadir la detección y retrasar la ejecución.

Actualización o Mitigación

Bloquear a nivel de antispam los correos con extensiones de adjuntos sospechosos o no confiables como .exe, .ps, .bat, .vbs, .scr, .vbe, .js, .jse, .cmd, .dll, .iqy, .oqy, .dqy y .rqy.

Imagen 5. Logo del producto afectado

Boletín	2020-161
Asunto	INSTALADORES DE ZOOM SON USADOS PARA DISTRIBUIR RAT
Emisión	07/05/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

El confinamiento provocado por la pandemia del Coronavirus ha incrementado el uso de aplicaciones de videoconferencia como Zoom. Esto está siendo aprovechado por los ciberdelincuentes, los cuales están que atacan a distintos perfiles de usuario en busca de obtener beneficios.

Desde inicios del año 2020, Zoom ha sido víctima de ataques en las cuales se han explotado múltiples vulnerabilidades, que han ido corrigiendo a lo largo de estos meses. Sin embargo, en la actual campaña los atacantes no explotan una vulnerabilidad, si no que distribuyen instaladores legítimos en los que está incrustado un backdoor que permite controlar de manera remota la computadora de la víctima.

Este troyano ha sido denominado RevCode WebMonitor RAT y permite realizar las siguientes acciones en la computadora infectada:

- Añadir, borrar o modificar ficheros e información del registro.
- Cerrar conexiones.
- Filtrar información sobre el software o el hardware.
- Tomar capturas de la webcam.
- Grabar audio y pulsaciones de teclado.
- Iniciar, suspender o terminar procesos o servicios.
- Retransmitir en directo la pantalla de la víctima.
- Conectar o desconectar el WiFi.

El troyano para asegurar su persistencia instala el archivo Zoom.vbs en la carpeta de inicio de usuario, lo que permite que se ejecute cuando se inicia el sistema. Adicionalmente, comprueba la existencia de software que pueda revelar su actividad o si se está ejecutando en una máquina virtual. Todo esto dificulta el análisis del malware. Se detectó que el troyano posee un servidor de Comando y Control (C2, abreviado en inglés).

Boletín	2020-162
Asunto	NUEVA CAMPAÑA DE SNAKE RANSOMWARE
Emisión	08/05/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

En enero del 2020 se detectó por primera vez este ransomware, ver Boletín 2020-024. Sin embargo, este se ha mantenido inactivo hasta inicios de mayo del 2020. Es así como durante los primeros días del mes se ha detectado un incremento en la actividad de Snake.

Se sospecha que una de las organizaciones afectadas por la actual campaña es Fresenius Group, el proveedor de hospitales más grande Europa. También se informó que una firma de arquitectos en Francia y una compañía de tarjetas de débito prepagadas se vieron afectadas por Snake.

Se publicó que ahora Snake antes de cifrar los archivos de sus víctimas, los roba para luego recién cifrarlos dándole a las víctimas 48 horas para pagar el rescate antes de empezar a publicar la información obtenida, está se ha vuelto una práctica común entre los atacantes de ransomware. Hasta el momento no se ha confirmado si esta información es cierta o si es que los operadores tienen algún sitio en la que publiquen los datos de su víctima.

Imagen 6. Logo del producto afectado

Boletín	2020-163
Asunto	CISCO PUBLICA ACTUALIZACIONES DE SEGURIDAD
Emisión	11/05/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Adaptive Security Appliance (ASA, por sus siglas en inglés) versiones 9.6.4.40, 9.8.4.15, 9.9.2.66, 9.10.1.37, 9.12.3.2 y 9.13.1.7

• Firepower Threat Defense (FTD, por sus siglas en inglés) versiones 6.4.0.8 y 6.5.0.4

Descripción

• La vulnerabilidad más grave fue asignada al CVE-2020-3187 y afecta a las interfaces de servicio web de ASA y FTD. Esta permite a un atacante remoto no autenticado realizar ataques transversales de directorio.

• La vulnerabilidad asignada al CVE-2020-3125 permite a un atacante remoto no autenticado hacerse pasar por el Centro de Distribución de Claves de Kerberos (KDC, por sus siglas en inglés), lo que le abre la posibilidad de evitar la autenticación al momento de conectar a dispositivos locales o VPN.

• Las vulnerabilidades asignadas a los CVE-2020-3298, CVE-2020-3191, CVE-2020-3254 y CVE-2020-3196 permiten a un atacante realizar un DoS.

• La vulnerabilidad asignada al CVE-2020-3195 permiten a un atacante remoto causar pérdida de memoria en el producto afectado, esta se debe al procesamiento incorrecto de ciertos paquetes OSPF.

• La vulnerabilidad asignada al CVE-2020-3259 permite la divulgación de información confidencial, esta se debe a un problema de seguimiento de búfer.

Se publicó que existen 4 vulnerabilidades que afectan sólo al software FTD:

• La vulnerabilidad asignada al CVE-2020-3189 se debe a que la memoria del sistema no se libera correctamente para un evento de registro del sistema VPN generado cuando se crea o elimina una sesión VPN, la correcta explotación de esta vulnerabilidad puede ocasionar un estado de DoS.

• La vulnerabilidad asignada al CVE-2020-3255 permite ocasionar un estado de DoS, esto se debe a una gestión de memoria ineficiente.

• La vulnerabilidad asignada al CVE-2020-3179 permite a un atacante remoto no autenticado ocasionar una condición de DoS, esto se debe a un mal manejo de memoria cuando se procesa el tráfico GRE sobre IPv6.

• La vulnerabilidad asignada al CVE-2020-3283 permite a un atacante remoto no autenticado ocasionar una condición de DoS, esto se debe a un mal manejo de comunicación entre funciones internas. Para explotar esta vulnerabilidad se puede enviar un mensaje SSL/TLS malicioso.

Imagen 7. Logo del producto afectado

Boletín	2020-164
Asunto	VULNERABILIDADES EN COMPLEMENTO PAGE BUILDER DE WORDPRESS
Emisión	12/05/2020
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Complemento Page Builder versiones anteriores a la 2.10.16

Descripción

Page Builder es un complemento que ayuda a los usuarios a crear contenido para páginas webs, utilizando un editor basado en widgets.

Las vulnerabilidades fueron detectadas el 4 de mayo del 2020, un día después los desarrolladores del complemento publicaron una actualización que corregía las vulnerabilidades. Esta consistió en agregar controles a la función Live Editor y a builder_content donde se encontraron los dos errores. La correcta explotación de estas permite a los atacantes crear nuevas cuentas de administrador, instalar backdoors y posiblemente tomar el control del sitio web.

Hasta el momento se ha detectado que solo un poco más de doscientos veinte mil de los más de un millón de sitios afectados han aplicado la actualización publicada por el equipo de desarrollo de Page Builder.

Actualización o mitigación

Instalar la última versión de Page Builder. Haga clic en el siguiente link: https://wordpress.org/plugins/siteorigin-panels/

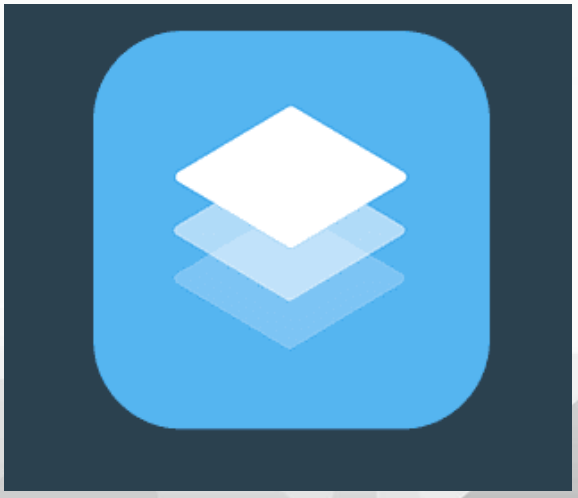

Imagen 8. Logo del producto afectado

Boletín	2020-165
Asunto	NUEVOS MALWARES UTILIZADOS POR ATACANTES NORCOREANOS
Emisión	12/05/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

• COPPERHEDGE: Es una Herramienta de Acceso Remoto (RAT, por sus siglas en inglés), permite a los atacantes obtener información del sistema, ejecutar comandos de forma arbitraria en sistemas comprometidos y extraer datos.

• TAINTEDSCRIBE: Es un troyano que descarga su módulo de ejecución de comandos desde un servidor de comando y control (C2, abreviado en inglés), para luego tener las funcionalidades de descargar, cargar, eliminar y ejecutar archivos; habilitar el acceso a la Interfaz de Línea de Comandos (CLI, por sus siglas en inglés) de Windows; crear y terminar procesos.

• PEBBLEDASH: Es un troyano que tiene las mismas funcionalidades de TAINTEDSCRIBE, no se ha determinado si se conecta a un servidor C2, como es el caso del anterior troyano.

Imagen 9. Bandera del país de origen de los atacantes

Boletín	2020-166
Asunto	DOMINIOS INFECTADOS CON MAGECART
Emisión	13/05/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Utilizando distintas herramientas, se pudo identificar una lista de 1,236 dominios que fueron afectados por un skimmer web alojado en un dominio externo.

Lo primero que se hizo fue escanear un dominio que contenía un skimmer, para lograr ello se utilizó el sitio web "Urlscan.io". Este proceso se repitió varias veces con distintos dominios sospechosos. Estos dominios contienen código JavaScript malicioso que permite al atacante robar información de tarjetas de crédito o débito.

Para mejorar la identificación de estos dominios se utilizaron reglas que permiten detectar código JavaScript malicioso. Luego se eliminaron los subdominios incorrectos o duplicados. Al analizar los resultados se pudo rastrear la actividad del Grupo12 de MageCart, el cual es considerado un actor de amenazas avanzado

Se publicó que las tiendas más afectadas se encuentran en los Estados Unidos (EE.UU. por sus siglas en inglés), seguido por el Reino Unido, el cual tiene 68 tiendas afectadas. Las tiendas de servicios y de productos alimentarios han sido los más afectados.

Boletín	2020-167
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE MICROSOFT - MAYO 2020
Emisión	13/05/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

Sistema operativo Windows

Descripción

En el mes de mayo del 2020, Microsoft ha publicado actualizaciones para 111 vulnerabilidades. De las cuales 16 son consideradas como críticas y 95 como importantes.

En este paquete de actualizaciones Microsoft, entre las 16 vulnerabilidades críticas corregidas 3 son de Microsoft Edge, las cuales fueron: CVE-2020-1056, CVE-2020-1059 y CVE-2020-1096. La primera de estas permite el escalamiento de privilegios, la segunda es de suplantación de identidad y la tercera es de ejecución de código remoto. Estas son algunas de las vulnerabilidades críticas que Microsoft ha corregido este mes.

Actualización o Mitigación

Se recomienda ver el contenido completo de esta noticia, para ello haga clic en el boletín que está en la tabla superior de esta página. En ese enlace encontrará mayor detalle de todas las vulnerabilidades junto con la actualización de cada vulnerabilidad.

Microsoft

Imagen 10. Logo de la marca del producto afectado

Boletín	2020-168
Asunto	LAS VULNERABILIDADES MÁS EXPLOTADAS EN LOS ÚLTIMOS AÑOS
Emisión	15/05/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Sistema operativo Windows, Citrix VPN y Pulse Secure VPN

Descripción

• CVE-2012-0158: Permite a los atacantes la ejecución de código remoto a través de un sitio web, archivo .rtf o documento de Office. Esta ha sido asociada al malware Dridex.

• CVE-2015-1641: Permite a los atacantes remotos la ejecución de código arbitrario a través de un documento RTF diseñado. Esta ha sido asociada a los malwares Toshliph y Uwarrior.

• CVE-2017-0143: Permite a los atacantes remotos la ejecución de código arbitrario a través de paquetes diseñados, también es conocido como "Vulnerabilidad de ejecución remota de código SMB de Windows". Esta ha sido asociada a EternalSynergy y EternalBlue Exploit Kit.

• CVE-2017-0199: Permite a los atacantes remotos la ejecución de código arbitrario a través de un documento elaborado, también es conocido como "Microsoft Vulnerabilidad de ejecución remota de código de Office / WordPad con API de Windows ". Esta ha sido asociada a los malwares FINSPY, LATENTBOT y Dridex.

• CVE-2017-5638: Permite a los atacantes remotos la ejecución de código arbitrario, esta se debe a que el analizador multiparte de Yakarta en Apache Struts maneja las excepciones de manera incorrecta. Esta ha sido asociada al malware JexBoss.

• CVE-2017-8759: Permite a los atacantes remotos la ejecución de código arbitrario, también es conocido como "Vulnerabilidad de ejecución remota de código de .NET Framework". Esta ha sido asociada a los malwares FINSPY, FinFisher y WingBird.

• CVE-2017-11882: Permite a los atacantes remotos la ejecución de código arbitrario en el entorno del usuario actual, esta se debe a un mal manejo de los objetos en la memoria y ha sido asociada a los malwares Loki, FormBook y Pony.

• CVE-2018-4878: Permite a los atacantes remotos la ejecución de código arbitrario. Esta ha sido asociada al malware DOGCALL.

• CVE-2018-7600: Permite a los atacantes remotos la ejecución de código arbitrario debido a un problema que afecta a múltiples subsistemas con configuraciones de módulos comunes o predeterminadas. Esta ha sido asociada al malware Kitty.

• CVE-2019-0604: Permite a los atacantes remotos la ejecución de código arbitrario en Microsoft SharePoint, esto se debe a que este software no puede verificar el marcador de origen. Está a sido asociada al malware China Chopper.

Actualización o Mitigación

Se recomienda ver el contenido completo de esta noticia, para ello haga clic en el boletín que está en la tabla superior de esta página.

Imagen 10. Logo de una de las marcas afectadas

Boletín	2020-169
Asunto	NUEVA VERSIÓN DEL RAT COMPFUN
Emisión	15/05/2020
CVE	Varios
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Se sospecha que los operadores detrás de COMpfun es el grupo Turla, de origen ruso. Este grupo ha realizado ataques de espionaje en contra de gobiernos, embajadas, militares, entre otros.

En el año 2019 COMpfun, recibió una actualización que le permitía espiar la actividad del navegador de una víctima, esto lo lograba realizando ataques de hombre en el medio (MitM, por sus siglas en inglés). Este RAT también posee las siguientes funciones: Captura de pulsaciones de teclado, captura de pantalla y filtración de datos. Este recibe sus instrucciones desde un Servidor de Comando y Control (C2, abreviado en inglés).

El C2 es el encargado de enviarle códigos de estado HTTP, a través de estos los atacantes envían instrucciones hacia el RAT. Los atacantes utilizan estos códigos para evadir la detección de actividad maliciosa, ya que estos son normalmente utilizados para saber el estado de un servidor. Por ejemplo, el código 200 es usado para enviar un mensaje de "Ok" por parte del servidor, sin embargo, en este caso es aprovechado para indicarle al RAT que tiene que enviar los datos recopilados al C2. Otros códigos que han sido aprovechados por los atacantes:

• 422: Desinstalar Eliminar la persistencia y los archivos en el disco.

• 423: Instalar persistencia en la computadora de la víctima.

• 424: Enviar datos de host, red y geolocalización.

• 428: Propagarse a dispositivo USB conectado a la computadora infectada.

• 429: Enumerar los recursos de red de la víctima.

Se ha identificado que en esta versión los atacantes han mantenido la clave pública RSA y la HTTP ETag. También se identificó que el troyano usa la comprensión LZNT1 y el cifrado XOR de un byte.

Boletín	2020-170
Asunto	CAMPAÑAS DISTRIBUYEN RAT Y MALWARES
Emisión	18/05/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Estas campañas fueron dirigidas a varias entidades del sector industrial, desde compañías de manufactura hasta empresas de inversión y de internet.

Para infectar sus objetivos, los atacantes usaron dos cadenas de infección, ambas a través de correos electrónicos de phishing, pero con algunas diferencias en su implementación. La primera usa unos archivos adjuntos maliciosos ZIP, UDP e IMG que contienen los instaladores NSIS maliciosos, mientras que la segunda usa documentos XLS y RTF para descargar los instaladores desde un servidor remoto a la computadora de la víctima.

Los instaladores NSIS distribuidos en esta campaña pueden eliminar imágenes y archivos de código fuente como scripts de shell y binarios de python, lo cual ayuda a ocultar el malware que distribuye.

En total se detectaron 5 campañas que distribuían un payload similar y compartían la misma infraestructura para su Servidor de Comando y Control (C2, abreviado en inglés). Los payloads eran de las siguientes amenazas: Betabot, Lokibot, Formbook, AgentTesla, entre otros.

También se identificó que, durante el mes de marzo de 2020, los atacantes detrás de RATicate se aprovecharon de la temática del Coronavirus para distribuirse.

Boletín	2020-171
Asunto	QNODESERVICE RAT BASADO EN NODE.JS
Emisión	19/05/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

El correo malicioso que se está distribuyendo contiene un archivo adjunto malicioso llamado CONTRACT PAYMENT.zip, el cual contiene otro archivo llamado CONTRACT PAYMENT.jar.

Cuando se ejecuta el archivo .jar descarga Node.js, el script wizard.js y almacena los paquetes descargados en la carpeta %UserProfile\qnodejs-node-v13.13.0-win-x64. Para que el malware se ejecute cada vez que la víctima inicie sesión en Windows, crea un valor de ejecución de registro. Este tiene por nombre qnodejs-2826976c.

Una vez que se instala QNodeService, tomará control total sobre la computadora afectada. Permitiéndole lo siguiente:

• Actualizarse.

• Obtener información de la máquina como: Dirección IP, nombre de la computadora, nombre de usuario y versión del sistema operativo.

• Ejecutar comandos.

• Eliminar y escribir archivos.

• Robar contraseñas de aplicaciones como Chrome y Firefox.

Se sospecha que este RAT también puede obtener acceso a otros dispositivos de la red e infectarlos.

Imagen 11. Logo de la tecnología en la que se basa QNodeService

Boletín	2020-172
Asunto	MICROSOFT PUBLICA MITIGACIÓN PARA EL ATAQUE NXNSATTACK
Emisión	20/05/2020
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Según lo publicado por microsoft un atacante que tiene éxito al momento de explotar esta vulnerabilidad puede ocasionar que el servidor DNS deje de responder.

Para lograr lo anterior un atacante necesita una máquina cliente y un dominio que pueda responder una gran cantidad de registros de referencia y que apunte a los subdominios externos de la víctima. Usando esto los atacantes pueden ocasionar una gran cantidad de intercambio de información entre el solucionador recursivo y el servidor DNS de la víctima, lo cual puede causar un DDoS.

Mitigación proporcionada por Microsoft

Los administradores pueden utilizar Set-DnsServerResponseRateLimiting, para habilitar la limitación de la tasa de respuesta. La limitación de la tasa de respuesta es una opción de configuración utilizada por los servidores DNS para evitar que se usen en ataques DDoS que utilizan amplificación DNS. Para verificar que está habilitado se puede ejecutar el comando Get-DnsServerResponseRateLimiting en PowerShell.

Cabe señalar que la utilización de la limitación de la tasa de respuesta evita que un servidor DNS de Windows sea aprovechado para realizar un ataque de amplificación de DNS contra otro, este no protege en si al mismo servidor de ser afectado por este tipo de ataque.

La vulnerabilidad NXNSAttack tambien ha afectado a empresas como Google, Amazon, Cloudflare, entre otras.

Para más información, haga clic en el siguiente link: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV200009

Imagen 12. Logo de la marca del producto afectado

Boletín	2020-173
Asunto	NUEVO MALWARE LLAMADO PIPEMON
Emisión	22/05/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

En febrero de 2020 se identificó un backdoor relacionado con Winnti. Se encontraron variantes del malware en servidores de múltiples desarrolladores de Juego Multijugador Masivo en línea (MMO, por sus siglas en inglés) de Corea del Sur y Taiwan. Se sospecha que los atacantes reutilizaron algunos dominios de Comando y Control (C2, por sus siglas en inglés) y un stealer de inicio de sesión personalizado que se vio anteriormente en otras víctimas de Winnti.

De las variantes de PipeMon descubiertas, se consiguió establecer cómo se instala y logra la persistencia.

Los atacantes para asegurarse que el malware permanezca activo, se aprovechan de los procesadores de impresión de Windows, para ello cargan un DLL malicioso, el cual se registra como un procesador de impresión alternativo. Después el malware reinicia el servicio de cola de impresión, para que de esta manera cargar el proceso malicioso. Como el servicio se ejecuta cada vez que se inicia la computadora, se logra la persistencia.

Hasta el momento se sabe que PipeMon es una puerta trasera modular, cada componente DLL que posee tiene una funcionalidad diferente. Estos se encuentran encriptados en la computadora de la víctima.

4. 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.
- 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, y reportarlo inmediatamente a los encargados de seguridad de la información de su institución.

* Antes de realizar el bloqueo de IOCs 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.