SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Quincenal de Ciberinteligencia Securesoft

Fecha:

8 julio de 2021

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia

CIB-FOR-2021-013

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

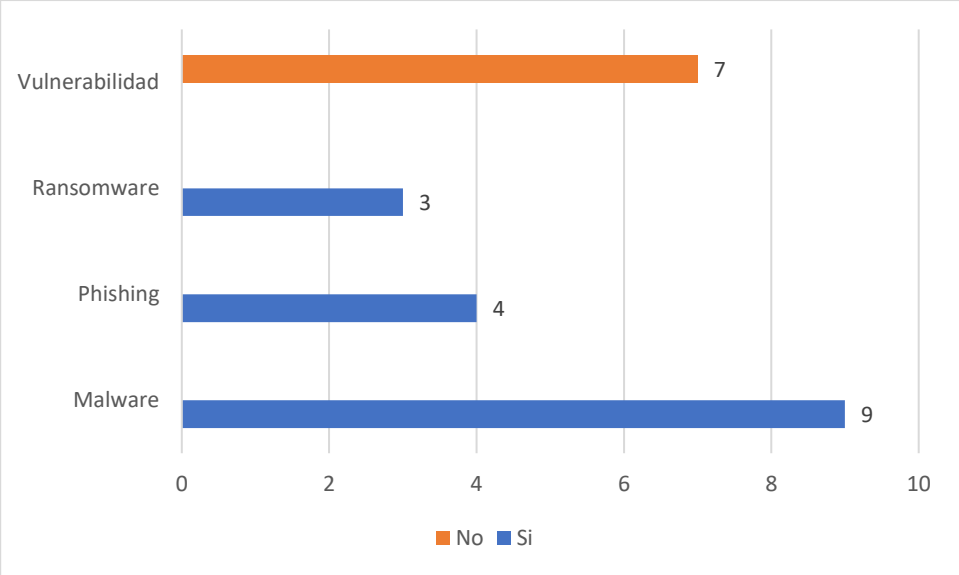
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 16 de junio hasta el 30 de junio del 2021.

3. Resumen

En el presente informe se exponen 23 análisis de vulnerabilidad y amenazas, de las cuales 20 tienen severidad alta y 3 severidad crítica.

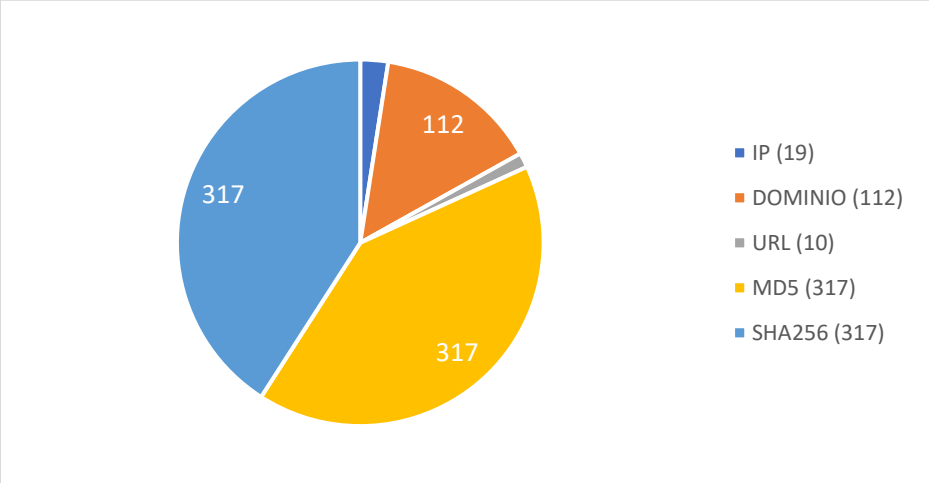
Amenazas analizadas por tipología

En las investigaciones elaboradas para el presente informe se trataron malware, vulnerabilidad, ransomware y phishing. 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 775 IoCs entre direcciones IP, Dominios, URL, MD5 y SHA256.



Tendencias en nuevas vulnerabilidades

- Cisco ha publicado actualizaciones de software que abordan vulnerabilidades en la interfaz de administración basada en web de los Cisco Small Business 220 Series Smart Switches. Para más información leer el Boletín 2021-266.

- Google ha emitido una actualización del navegador Chrome para Windows, Mac y Linux donde soluciona cuatro vulnerabilidades de seguridad, incluida una falla de día cero que está siendo explotada. Para más información leer el Boletín 2021-267.

- Se ha descubierto que una vulnerabilidad crítica en los dispositivos VPN de SonicWall que se creía que había sido parcheada el año pasado estaba "estropeada", y la empresa dejó sin resolver una falla de fuga de memoria, hasta ahora, que podría permitir que un atacante remoto obtenga acceso a información sensible. Para más información leer el Boletín 2021-278.

- Una vulnerabilidad de alta gravedad parcheada recientemente por Fortinet en su firewall de aplicaciones web (WAF) FortiWeb puede explotarse para ejecutar comandos arbitrarios. La falla puede representar un riesgo aún más serio si está encadenada con una configuración incorrecta y otro agujero de seguridad descubierto recientemente. Para más información leer el Boletín 2021-282.

Tendencias en actividades maliciosas

- Recientemente se ha observado un ciberataque hacia una empresa televisiva, esta empresa compartió IOC´s, los cuales al ser analizados se observó que están asociados al Ransomware Sodinokibi el cual ha experimentado una gran evolución desde sus inicios, pudiendo identificar una gran cantidad de familias diferentes en la actualidad, dirigidas a entidades públicas y privadas, para más información leer Boletín 2021-264.

- Recientemente se ha detectado una serie de sitios web WordPress comprometidos con atacantes que abusan de la funcionalidad de carga de complementos en el panel de wp-admin para redirigir a los visitantes y propietarios de sitios web a sitios web maliciosos, para más información leer Boletín 2021-273.

- Recientemente se ha observado que el malware Agent Tesla está activo en Internet a través de una campaña de phishing que utiliza correos electrónicos con el propósito de solicitar a los destinatarios que revisen un "problema" con el registro de vacunación mediante un Calendario de vacunación COVID-19 como señuelo, para más información leer Boletín 2021-276.

- Recientemente se observaron dos nuevas campañas activas que contenían archivos adjuntos en formato ZIP o enlaces hacia archivos ZIP, con el objetivo de distribuir backdoors bancarios para pretender conseguir datos confidenciales de la víctima, para más información leer Boletín 2021-280.

Equipo de Ciberinteligencia
CIB-FOR-2021-013

4. Detalles

Vulnerabilidades

Boletín	2021-262
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE INTEL
Emisión	17/06/2021
CVE	Según Tabla Boletín
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- 2nd, 3rd Generation Intel® Xeon® Scalable Processor
- 6th, 7th, 8th, 10th, 11th Generation Intel® Core™ processors
- All Linux kernel versions prior to 5.13 that support BlueZ
- Intel Atom® Processor P5000 Series

Descripción

Intel ha abordado múltiples vulnerabilidades de seguridad como parte de parches de junio de 2021, incluidas las de alta gravedad que afectan algunas versiones de la biblioteca de seguridad de Intel y el firmware de BIOS para procesadores Intel.

Se ha emitido 29 avisos de seguridad publicados por Intel, donde proporciona una lista de productos afectados y recomendaciones para productos vulnerables al final de cada aviso, junto con los datos de contacto de los investigadores de seguridad que desean informar sobre problemas de seguridad o vulnerabilidades que se encuentran en la tecnología de la marca Intel. El primero de ellos (registrado como CVE-2021-24489) es causado por una limpieza incompleta en algunos productos Intel VT-d que podría permitir a los atacantes autenticados escalar privilegios a través del acceso local.

Intel corrigió cuatro errores más (rastreados como CVE-2020-12357, CVE-2020-8670, CVE-2020-8700 y CVE-2020-12359) causados por una inicialización incorrecta, condición de carrera, validación de entrada incorrecta y administración de flujo de control insuficiente en el firmware del BIOS de la CPU que permite la escalada de privilegios a través del acceso local o físico. Se parcheó otras 11 vulnerabilidades de seguridad de alta gravedad que afectan a los NUC de Intel, el controlador Intel y el asistente de soporte (DSA), Intel RealSense ID, el controlador del motor de aceleración programable abierto (OPAE) de la matriz de puerta programable de campo Intel (FPGA) para Linux y los controladores Intel Thunderbolt.

Actualización o Mitigación

- Implementar la actualización que corresponda a cada producto según la información proporcionada por Intel en la sección de "Security Center Home" accediendo por medio del hipervínculo de la columna de "Actualización" de la "Tabla 1" del presente boletín de acuerdo a cada vulnerabilidad mencionada.

Boletín	2021-263
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE POLKIT
Emisión	17/06/2021
CVE	CVE-2021-3560
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• RHEL 8

• Fedora 21

• Sistemas Operativos Debian "Bullsey".

• Ubuntu 20.04

Descripción

Se descubrió un error crítico de escalada de privilegios de Linux de siete años en el servicio del sistema Polkit, que anteriormente se llamaba PoilcyKit, que podría permitir a un ciberdelincuente eludir la autorización para obtener acceso de root en el sistema afectado.

El error descubierto recientemente se ha rastreado como CVE-2021-3560 y se encuentra principalmente en el servicio Polkit que en realidad está asociado con un sistema Linux y un componente de administrador de servicios, "systemd".

Desafortunadamente, ya que systemd utiliza Polkit en lugar de sudo, la vulnerabilidad podría haber otorgado a usuarios no autorizados la capacidad de ejecutar procesos con privilegios. Estos procesos privilegiados no se pueden ejecutar de ninguna otra manera. En otras palabras, Polkit podría haber sido utilizado para obtener acceso de root al sistema Linux vulnerable.

La vulnerabilidad Polkit ocurre cuando un proceso de solicitud se desconecta de dbus-daemon justo antes de que comience la llamada a polkit_system_bus_name_get_creds_sync, el proceso no puede obtener un uid y pid únicos del proceso y no puede verificar los privilegios del proceso solicitante. La mayor amenaza de esta vulnerabilidad es la confidencialidad e integridad de los datos, así como la disponibilidad del sistema.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-266
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE CISCO
Emisión	21/06/2021
CVE	CVE-2021-24370
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Cisco Small Business 220 Series Smart Switches con firmware anterior a la versión 1.2.0.6

Descripción

La primera vulnerabilidad rastreada como CVE-2021-1541, se debe a la falta de validación de parámetros para la configuración TFTP. Un exploit exitoso podría permitir al ciberdelincuente ejecutar comandos arbitrarios como usuario root en el sistema operativo.

El fallo registrado como CVE-2021-1542, se debe al uso de una gestión de sesión débil para los valores del identificador de sesión. Un atacante podría aprovechar esta vulnerabilidad mediante el uso de métodos de reconocimiento para determinar cómo crear un identificador de sesión válido. Un exploit exitoso podría permitir al atacante tomar acciones dentro de la interfaz de administración con privilegios hasta el nivel del usuario root.

Un ciberdelincuente podría aprovechar el CVE-2021-1543 persuadiendo a un usuario para que haga clic en un enlace malicioso y acceda a una página específica. Un exploit exitoso podría permitir al atacante ejecutar código de secuencia de comandos arbitrario en el contexto de la interfaz afectada o acceder a información confidencial basada en el navegador y redirigir al usuario a una página arbitraria.

Por último, el CVE-2021-1571 se debe a una función desconocida del componente Web-based Management Interface. Un ciberdelincuente podría aprovechar esta vulnerabilidad persuadiendo a un usuario para que siga un vínculo creado que está diseñado para pasar código HTML a un parámetro afectado. Un exploit exitoso podría permitir al atacante alterar el contenido de una página web para redirigir al usuario a sitios web potencialmente maliciosos.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-267
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE DÍA CERO GOOGLE CHROME
Emisión	21/06/2021
CVE	CVE-2021-30554, CVE-2021-30555, CVE-2021-30556 y CVE-2021-30557
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Google Chrome anteriores a la versión 91.0.4472.114

Descripción

Google ha emitido una actualización del navegador Chrome para Windows, Mac y Linux donde soluciona cuatro vulnerabilidades de seguridad, incluida una falla de día cero que está siendo explotada.

Rastreado como CVE-2021-30554, el defecto de alta gravedad se refiere a una vulnerabilidad de uso posterior libre en WebGL (también conocida como Biblioteca de gráficos web), una API de JavaScript para renderizar gráficos interactivos 2D y 3D dentro del navegador. La explotación exitosa de la falla podría significar la corrupción de datos válidos, lo que provocaría un bloqueo e incluso la ejecución de códigos o comandos no autorizados.

El problema se informó a Google de forma anónima el 15 de junio, señaló el gerente del programa técnico de Chrome, Srinivas Sista , y agregó que la compañía es "consciente de que existe un exploit para CVE-2021-30554".

CVE-2021-30554 es también el octavo defecto de día cero parcheado por Google desde principios de año. Los usuarios de Chrome pueden actualizar la plataforma a la última versión (91.0.4472.114) dirigiéndose a Configuración> Ayuda> 'Acerca de Google Chrome' para mitigar el riesgo asociado con la falla. Esta actualización incluye 4 correcciones de seguridad.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-278
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE DÍA CERO SONICWALL
Emisión	25/06/2021
CVE	CVE-2021-20019 y CVE-2020-5135
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

- SonicOS 6.0.5.3-94o y versiones anteriores
- SonicOS 6.5.1.12-3n y versiones anteriores
- SonicOSv 6.5.4.4-44v-21-955 y versiones inferiores
- SonicOS 6.5.4.7-83n y versiones anteriores
- SonicOS 7.0.0-R713 y versiones anteriores
- SonicOS 7.0.1-R1036 y versiones anteriores
- SonicOS 7.0.0.376 y versiones anteriores

Descripción

Se ha descubierto que una vulnerabilidad crítica en los dispositivos VPN de SonicWall que se creía que había sido parcheada el año pasado estaba "estropeada", y la empresa dejó sin resolver una falla de fuga de memoria, hasta ahora, que podría permitir que un atacante remoto obtenga acceso a información sensible.

La deficiencia se corrigió en una actualización emitida a SonicOS el 22 de junio. Registrada como CVE-2021-20019 (puntuación CVSS: 5.3), la vulnerabilidad es la consecuencia de una pérdida de memoria al enviar una solicitud HTTP no autenticada especialmente diseñada, que culmina en la divulgación de información.

Cabe resaltar que la decisión de SonicWall de retener el parche se produce en medio de múltiples revelaciones de día cero, que afectan su VPN de acceso remoto y productos de seguridad de correo electrónico que han sido explotados en una serie de ataques para implementar puertas traseras y una nueva cepa de ransomware llamado FIVEHANDS. Para mayor detalle del ransomware puede ingresar al siguiente Boletín 2021-182 NUEVO RANSOMWARE FIVEHANDS SE ENFOCA EN EL SECTOR FINANCIERO. La falla original, identificada como CVE-2020-5135 (puntaje CVSS: 9.4), se refería a una vulnerabilidad de desbordamiento de búfer en SonicOS que podría permitir que un atacante remoto causara denegación de servicio (DoS) y potencialmente ejecutara código arbitrario enviando un código malicioso. solicitud al cortafuegos.

Si bien SonicWall emitió un parche en octubre de 2020, las pruebas adicionales realizadas por la empresa de ciberseguridad Tripwire revelaron una pérdida de memoria como resultado de una solución incorrecta para CVE-2020-5135 problema que se informó a SonicWall el 6 de octubre de 2020.

Actualización o Mitigación

- Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-281
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE DOVECOT
Emisión	30/06/2021
CVE	CVE-2021-33515
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Dovecot antes de la versión 2.3.15

Descripción

Dovecot ha parcheado un ataque de prueba de concepto de hace un año que permite a un atacante eludir las protecciones de correo electrónico TLS para espiar los mensajes.

Ciberdelincuentes pueden espiar los mensajes de correo electrónico, aprovechando un error en la tecnología subyacente utilizada por la mayoría de los servidores de correo electrónico que ejecutan el Protocolo de acceso a mensajes de Internet, comúnmente conocido como IMAP. El error, informado por primera vez en agosto de 2020 y recientemente parcheado, está vinculado al software del servidor de correo electrónico Dovecot, utilizado por más de las tres cuartas partes de los servidores IMAP.

La vulnerabilidad permite que un atacante MITM entre un cliente de correo y Dovecot inyecte comandos no cifrados en el contexto TLS cifrado, omitiendo las funciones de seguridad de SMTP como el bloqueo de inicio de sesión de texto sin formato permitiendo montar un ataque de fijación de sesión el cual redirige las credenciales de usuario y los correos electrónicos al atacante.

Para llevar a cabo el ataque, un atacante primero crea una cuenta legítima en un servidor Dovecot. Después espera e intercepta una conexión cifrada en el puerto 465 del cliente de correo electrónico de la víctima. Tan pronto como el cliente se conecta, el atacante inicia una conexión START-TLS separada a Dovecot e inyecta su propio prefijo malicioso.

Actualización o Mitigación

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

Boletín	2021-282
Asunto	ACTUALIZACIÓN DE SEGURIDAD FORTINET
Emisión	30/06/2021
CVE	CVE-2021-22123 y CVE-2020-29015
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- FortiWeb versiones 6.1.x, 6.0.x, 5.9.x
- FortiWeb versiones anteriores a 6.2.4 y 6.3.8.

Descripción

Una vulnerabilidad de alta gravedad parcheada recientemente por Fortinetx, en su firewall de aplicaciones web (WAF) FortiWeb, puede explotarse para ejecutar comandos arbitrarios. La falla puede representar un riesgo aún más serio si está encadenada con una configuración incorrecta y otro agujero de seguridad descubierto recientemente.

Se descubrió que el firewall FortiWeb, específicamente su interfaz de administración, se ve afectado por una vulnerabilidad que puede permitir que un atacante remoto y autenticado ejecute comandos en el sistema a través de la página de configuración del servidor SAML.

La falla, rastreada como CVE-2021-22123, se corrigió con el lanzamiento de las versiones 6.3.8 y 6.2.4 de FortiWeb.

La vulnerabilidad rastreada como CVE-2020-29015 y revelada por Fortinet en enero, es un problema de inyección de SQL de gravedad media que puede permitir que un atacante remoto no autenticado ejecute comandos o consultas de SQL enviando una solicitud especialmente diseñada. Con el resultado de una configuración incorrecta, la interfaz de administración del firewall está disponible en Internet y el producto en sí no está actualizado a las últimas versiones, entonces la combinación de CVE-2021-22123 y CVE-2020-29015 pueden permitir que un atacante penetre en la red interna.

Actualización o Mitigación

- Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Amenazas

Boletín	2021-261
Asunto	EL GRUPO BELIALDEMON DISTRIBUYE NUEVO MALWARE MATANBUCHUS
Emisión	16/06/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

Recientemente se ha observado que el grupo de ciberdelincuentes BelialDemon anunciaba en su foro un nuevo MaaS (Malware_as_a_Service), el cual se distribuye con la principal función de recolectar información confidencial y mantener una conexión remota con los dispositivos infectados con un C2.

Recientemente se observó que el malware Matanbuchus, tiene las capacidades de ejecutar un archivo .exe o .dll en la memoria, aprovechar schtasks.exe para agregar o modificar programas de tareas, lanzar comandos personalizados de PowerShell y aprovechar un ejecutable independiente para cargar la DLL si el atacante no tiene forma de hacerlo.

En general, Matanbuchus usa dos DLL durante el ciclo de ejecución. Pero debe tenerse en cuenta que la primera DLL tiene un nombre interno de MatanbuchusDroper.dll mientras que la segunda DLL se llama “Matanbuchus.dll”. Una vez que el Excel descarga la DLL inicial, MatanbuchusDroper.dll, desde el sitio idea-secure-login[.]com , la macro de Excel se iniciará y llamará a la exportación dentro de la DLL con el nombre RunDtaLL32COM .

La función principal de esta primera DLL es eliminar la DLL principal de Matanbuchus. Sin embargo, antes de eso, realizará una serie de llamadas a la API que normalmente se observan en las comprobaciones anti-virtualización y anti-depuración. Estos pueden perfilar un sistema para proporcionar indicadores al malware que le permitan determinar si se está ejecutando en un entorno controlado (es decir, un sandbox). La DLL pasará a la siguiente fase y descomprimirá la URL para descargar la DLL principal de Matanbuchus, disfrazada como un archivo XML llamado AveBelial.xml . Este archivo descargado se guarda en "Users \ ADMINI ~ 1 \ AppData \ Local \ Temp \ Run_32DLL_COM32 \ shell96.dll ". La persistencia se establece mediante la creación de una tarea programada para ejecutar la nueva DLL.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-264
Asunto	NUEVAS ACTIVIDADES DEL RANSOMWARE SODINOKIBI
Emisión	17/06/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Recientemente se ha observado un ciberataque hacia una empresa televisiva, esta empresa compartió IOC´s, los cuales al ser analizados se observó que están asociados al Ransomware Sodinokibi el cual ha experimentado una gran evolución desde sus inicios, pudiendo identificar una gran cantidad de familias diferentes en la actualidad, dirigidas a entidades públicas y privadas.

Recientemente se observó que una empresa televisiva informó que sufrió un incidente de ciberseguridad provocado por una campaña de ransomware el cual está relacionado a Sodinokibi. Este ransomware es utilizado para infectar sistemas Windows cuya propagación sigue el modelo RaaS (Ramsonware as a Service), es decir, es un código malicioso que se comercializa de forma personalizada, ajustándose a las necesidades de cada uno de los suscriptores.

El ransomware Sodinokibi podría explotar vulnerabilidades como vector inicial con el propósito de obtener acceso a la máquina del objetivo. Una vez que está dentro, el malware intenta acoplarse escalando privilegios para acceder a todos los archivos, así como a los recursos del sistema sin restricciones.

Este ransomware utiliza AES y también el algoritmo Salsa20 para encriptar los datos individuales, AES que es utilizado para encriptar las sesiones y también los datos que se envían al servidor de control, los datos individuales se encriptan utilizando la seguridad Salsa20.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-265
Asunto	NUEVA CAMPAÑA DE PHISHING PRETENDE INFILTRARSE COMO ARCHIVOS EN WETRANSFER
Emisión	18/06/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Recientemente se ha observado una campaña de phishing que imita las aplicaciones legítimas de WeTransfer, mediante la creación de sitios web falsos que parecen oficiales con el propósito de obtener archivos y credenciales.

Los ciberdelincuentes han realizado una campaña de phishing con el método de enviar correos electrónicos con importancia alta, en conjunto dentro del cuerpo de correo contiene el siguiente texto "Los archivos pendientes se eliminarán en breve", esto con el fin de agregar urgencia a través de las marcas de tiempo.

Dentro del correo también se observa una imagen con el texto “Get your files”, en el cual al darle click te redirige hacia una URL maliciosa que aparenta ser una página oficial de WeTransfer. En conjunto, se observó que este correo tiene una cuenta de origen clonado utilizando el dominio wetransfer[.]com.

Como etapa final del ataque, se le solicita al usuario que ingrese sus credenciales para descargar el archivo compartido. La página de inicio de phishing se rellena previamente con la dirección de correo electrónico del usuario en el campo de inicio de sesión. Después de ingresar la contraseña, se muestra al usuario un intento fallido de inicio de sesión.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) mostrados en el Boletín, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-268
Asunto	NUEVA ACTIVIDAD DEL MALWARE STARSLORD
Emisión	21/06/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Recientemente, se ha observado una nueva actividad del malware Starslord con una nueva etapa en el inicio su ciclo con el propósito de pretender recopilar y extraer información de los dispositivos infectados, evaluando al objetico para insertar un payload más sofisticado.

Recientemente se observó que los ciberdelincuentes de Starslord han hecho cambios en la primera etapa del ciclo que presentaba este malware; sin embargo, las etapas continuas permanecen sin cambios. El malware Starslord inicialmente utilizaba un archivo LNK falso para descargar un script de PowerShell, que eventualmente descargará y ejecutará Sload. Posteriormente en su nueva actividad comenzará con scripts WSF / VBS, que con frecuencia se modifican para evitar la detección de AV.

La secuencia de comandos que se observó sobre Starslord es una secuencia de comandos WSF que decodifica un conjunto de comandos maliciosos, una vez ejecutados, descargará y ejecutará un payload remoto en la memoria.

Esto finalmente se logrará mediante una técnica de evasión, donde el script cambia el nombre de los archivos binarios legítimos de Windows. Tanto “bitsadmin.exe” como “Powershell.exe” se copian y renombran, el primero se usa para descargar un script de PowerShell malicioso y el segundo lo carga en la memoria y comienza su ejecución.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-269
Asunto	NUEVO RANSOMWARE DARKRADIATION
Emisión	22/06/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Linux

Descripción

DarkRadiation es un nuevo ransomware que se dirige a los contenedores en la nube de Linux y Docker. Codificado en Bash, el ransomware se dirige específicamente a distribuciones de Red Hat / CentOS y Debian Linux.

En términos de infección, el ransomware está programado para llevar a cabo un ataque en varias etapas, mientras se basa en múltiples scripts Bash para recuperar el payload y cifrar los datos en un sistema infectado. También utiliza la API de Telegram para comunicarse con el servidor de comando y control mediante claves API codificadas.

Antes del proceso de cifrado, el ransomware recupera una lista de todos los usuarios disponibles en un sistema infectado consultando el archivo "/ etc / shadow". Sobrescribe todas las contraseñas de usuario existentes con "megapassword" y elimina todos los usuarios existentes excepto "ferrum". Después de eso, el malware crea un nuevo usuario desde su sección de configuración con el nombre de usuario "ferrum" y la contraseña "MegPw0rD3". Ejecuta el comando "usermod –shell / bin / nologin" para deshabilitar a todos los usuarios de shell existentes en un sistema infectado.

Cabe destacar que algunas de las variantes de ransomware que encontró Trend Micro, intentan eliminar todos los usuarios existentes, excepto el nombre de usuario "ferrum" y "root". El malware también comprueba si existe 0.txt en el servidor de comando y control. En caso de que no exista, no ejecutará el proceso de encriptación y dormirá durante 60 segundos; luego vuelve a intentar el proceso.

DarkRadiation utiliza el algoritmo AES de OpenSSL en modo CBC para su cifrado, y recibe su contraseña de cifrado a través de un argumento de línea de comandos pasado por un script de gusano. El ransomware también detiene y deshabilita todos los contenedores Docker en ejecución en el host infectado y crea una nota de rescate.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-270
Asunto	CIBERDELINCUENTES REALIZAN NUEVA CAMPAÑA FALSA DE DARKSIDE
Emisión	22/06/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Recientemente empresas de la industria energética y alimentaria han recibido recientemente correos electrónicos amenazadores supuestamente de DarkSide. En este correo electrónico, el ciberdelincuente afirma que ha vulnerado con éxito la red del objetivo y obtenido acceso a información confidencial, que se divulgará públicamente si no se paga un rescate.

Al revisar el contenido utilizado en los correos electrónicos se ha detectado que no provienen de dicho grupo de amenazas, sino de otro ciberdelincuente de bajo nivel que intenta sacar provecho de la situación actual en torno a las actividades del ransomware DarkSide.

La campaña de correo electrónico comenzó en junio mediante correos electrónicos con contenido amenazante, los cuales se enviaron a las direcciones de correo electrónico genéricas de empresas seleccionadas.

El comportamiento detrás de esta campaña de fraude es muy diferente al que DarkSide utilizó en sus campañas anteriores. DarkSide siempre ha podido demostrar que obtuvieron datos confidenciales robados. También llevan a sus objetivos a un sitio web alojado en la red Tor. Sin embargo, en esta campaña, el correo electrónico no menciona nada que demuestre que efectivamente han obtenido información confidencial o sensible.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín asociado, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-271
Asunto	NUEVA VARIANTE DEL MALWARE DJVU
Emisión	22/06/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

Recientemente se ha observado una nueva variante del malware DJVU el cual pertenece a la familia del ransomware STOP. Esta nueva variante utiliza algoritmos de cifrado avanzado estándar o RSA para cifrar archivos en los dispositivos de las víctimas.

La nueva variante del malware DJVU inicia su ciclo de ataque a los sistemas de los usuarios mediante descargas de archivos maliciosos que luego son ejecutados. Estos archivos maliciosos se hacen pasar por cracks de software o generadores de claves que permiten a los usuarios utilizar software de pago de forma gratuita, mediante la descarga desde torrent. La técnica de evasión que utilizan los archivos maliciosos es deshabilitando las funcionalidades del antivirus de Windows Defender mediante un script de Powershell.

El malware se ha desarrollado utilizando el lenguaje C / C ++, en el cual se observa un payload que utiliza algoritmos de cifrado AES o RSA personalizados para cifrar archivos y agregar varias extensiones.

Una vez que el malware ingresa a la máquina víctima, realiza una secuencia de infección en varios pasos. Estos implican modificar los archivos del sistema, cambiar las entradas del registro de Windows y eliminar los snapshot para evitar la recuperación de archivos.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín asociado, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-272
Asunto	NUEVA CAMPAÑA DEL GRUPO APT TA402
Emisión	23/06/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

• Dropbox API

Descripción

Un grupo de amenaza persistente avanzada (APT) de Oriente Medio ha resurgido después de una pausa de dos meses, para apuntar a instituciones gubernamentales en Oriente Medio y entidades gubernamentales globales, en una serie de nuevas campañas observadas a principios del mes de junio.

Se atribuye la actividad a un grupo de ciberdelincuentes con motivaciones políticas que se encuentra rastreado como TA402, y conocido por otros apodos como Molerats y GazaHackerTeam. El grupo APT abarca múltiples rubros como tecnología, telecomunicaciones, finanzas, academia, militares, medios de comunicación y gobiernos.

La última ola de ataques comenzó con correos electrónicos de spear-phishing escritos en árabe y que contienen archivos adjuntos PDF que vienen incrustados con una URL maliciosa para dirigir selectivamente a las víctimas a un archivo protegido con contraseña. El método mencionado busca propagar el malware LastConn distribuido por TA402. La motivación principal de este grupo es recopilar información y documentos sensibles de objetivos de alto valor para recopilar inteligencia.

La primera vez que se ejecuta LastConn, se ejecuta una función "RunFileOnes". Esta función utiliza la API legítima de Dropbox y el token de autenticación "txt_TokenRunOne" para descargar el archivo "txt_FileOpen" en "txt_PathDir". A continuación, se abre este archivo el cual se utiliza para mostrar un documento señuelo. El documento de señuelo de febrero se llamaba "hamas.docx".

Después de la funcionalidad de documento señuelo, se ejecuta una función "StartFolder". Con la API de Dropbox y el token de autenticación "txt_MyToken", se crea un directorio de trabajo en el Dropbox del malware llamado "<nombre_computadora> <nombredeusuario>". A continuación, se carga un archivo "txt_FileToDown" vacío en el directorio de trabajo. Se cree que este archivo vacío se utiliza para indicar que el malware se ha inicializado y está listo para ejecutar comandos.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín asociado, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-273
Asunto	CAMPAÑA DE MALWARE DIRIGIDA A SITIOS CONECTADOS A WORDPRESS
Emisión	23/06/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Complemento Jetpack de WordPress

Descripción

Recientemente se ha detectado una serie de sitios web WordPress comprometidos con atacantes que abusan de la funcionalidad de carga de complementos en el panel de wp-admin para redirigir a los visitantes y propietarios de sitios web a sitios web maliciosos.

Jetpack es uno de los complementos más populares en el repositorio de WordPress y tiene una increíble variedad de características que requieren que los usuarios conecten sus sitios a una cuenta de WordPress[.]com. Una de estas características permite a los usuarios que han iniciado sesión en WordPress[.]com realizar tareas administrativas, incluida la instalación de complementos, en sitios que están conectados a WordPress[.]com a través de Jetpack.

Desafortunadamente, esto significa que si las credenciales de una cuenta de WordPress[.]com están comprometidas, un atacante puede iniciar sesión en esa cuenta de WordPress[.]com e instalar complementos arbitrarios en el sitio de WordPress conectado sin importar dónde esté alojado. Esto incluye el complemento malicioso utilizado en esta campaña. Una vez que los atacantes establecen su punto de apoyo en el área de wp-admin, instalan una versión con puerta trasera del complemento log-http-orders a través de la función "upload plugin" del panel de control de wp-admin. También instalan su falso complemento de payload “plugs.php” que ocultan con el nombre de “PHP Everywhere”. Una vez que se instala ese complemento, el propietario del sitio web y los visitantes del sitio son redirigidos a esos dominios de spam.

Estos complementos maliciosos verifican si el visitante del sitio está en la página de inicio de sesión o si inició sesión como administrador. Cualquier visitante que no cumpla con estos criterios será redirigido a una de las varias docenas de dominios punycode maliciosos.

Otro Webshell “FilesMan” proporciona a los atacantes un control total del sistema de archivos. Esto les permite reinfectar el sitio web si se cambian las contraseñas de administrador.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín asociado, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-274
Asunto	NUEVO BACKDOOR REVERSERAT
Emisión	23/06/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

Recientemente se ha observado actividad de un grupo de ciberdelincuentes vinculados a Pakistán en el cual se ha visto involucrado una empresa eléctrica, en este ataque se observó un nuevo backdoor conocido como ReverseRat e en conjunto con un RAT de código abierto llamado Allakoe con el propósito de infectar máquinas y lograr persistencia.

El malware ReverseRat utiliza dominios maliciosos como fase inicial para alojar sus archivos maliciosos con la intención de evadir la detección y mezclarse con la actividad de navegación web estándar en la red. Cuando se hace clic en estos enlaces se descarga un archivo .zip que contiene un archivo de acceso directo de Microsoft (.lnk) y un archivo PDF benigno. El archivo PDF actuaba como un señuelo para distraer al usuario, mientras que el archivo de acceso directo ejecutaba un archivo HTA (aplicación HTML) del mismo sitio web comprometido. En las campañas observadas, los archivos HTA creados por el ciberdelincuente se alojaron en el mismo sitio que el archivo .zip, pero en diferentes rutas de URL.

En la siguiente fase de la infección, el primer archivo HTA recuperado contenía código JavaScript basado en un proyecto de GitHub llamado CactusTorch con el propósito de inyectar un shellcode de 32 bits en un proceso de ejecución para ejecutar un programa .NET llamado preBotHta.pdb, esta variante se ejecuta en la memoria y contiene una lógica para alterar la ubicación de ReverseRat. Si el archivo preBotHta detectaba un determinado producto AV, como Kaspersky, colocaba ReverseRat en la ruta MyMusic; de lo contrario, coloca el archivo en la carpeta Inicio.

La última acción que toma preBotHta es iniciar la ejecución de ReverseRat para obtener información de componentes (dirección MAC, información sobre el procesor, sistema operativo, dirección IP entre otros) a través de Windows Management Instrumentation (WMI).

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-275
Asunto	NUEVO BACKDOOR CHACHI ES UTILIZADO EN CAMPAÑAS DE PYSA
Emisión	24/06/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Recientemente se ha observado un nuevo backdoor ChaChi que está escrito en un lenguaje de programación GO, el cual ha sido utilizado por los ciberdelincuentes del ransomware PYSA como parte de su conjunto de herramientas con el fin de obtener información confidencial.

El malware ChaChi se llama así debido a Cha shell y Chi sel, dos herramientas listas para ser utilizadas por el malware durante los ataques. ChaChi es utilizado como vector inicial en correos electrónicos con contenido malicioso para poder utilizarse como un backdoor en el cual permitirá que los ciberdelincuentes recolecten credenciales. ChaChi está escrito en programación GO, un lenguaje de programación que ahora está siendo ampliamente adoptado por ciberdelincuentes en un cambio de C y C ++ debido a su versatilidad y la facilidad de compilación de código.

Esta herramienta utiliza la herramienta gobfuscated Golang con fines de ofuscación, gobfuscated ofusca la tabla de símbolos en tiempo de ejecución reemplazándolos con nombres generados aleatoriamente reemplazándolas con funciones. Esta ofuscación se diseñó con el propósito de evitar la filtración de información relacionada con el código fuente de Go, como cadenas, rutas de paquetes y nombres de campo. Desde entonces, ha sido adoptado por los ciberdelincuentes del malware como un medio para obstaculizar el análisis y los esfuerzos de ingeniería inversa.

ChaChi pretende ejecutarse con privilegios administrativos, si no se llega a ejecutar de esta forma, omite su código de persistencia y comienza a inicializar las comunicaciones de comando y control (C2). Si el backdoor se ejecuta con privilegios, se instalará como un nuevo servicio que está configurado para iniciarse automáticamente.

ChaChi utiliza dos protocolos para las comunicaciones C2 entre ellas se encuentran DNS y HTTP. El método principal y preferido de comunicación C2 es el túnel de DNS mediante consultas TXT. Si las comunicaciones de DNS fallan, ChaChi usa un mecanismo de conmutación por error en el que utiliza HTTP en forma de solicitudes POST codificadas para comunicarse con sus servidores C2. Las solicitudes HTTP POST se utilizan generalmente para enviar datos a un servidor para crear o actualizar un recurso en ese servidor.

Actualización o Mitigación

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

Boletín	2021-276
Asunto	CAMPAÑA DEL AGENT TESLA MEDIANTE SOLICITUD DE REGISTRO DE VACUNACIÓN DEL COVID-19
Emisión	25/06/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Recientemente se ha observado que el malware Agent Tesla está activo en Internet a través de una campaña de phishing que utiliza correos electrónicos con el propósito de solicitar a los destinatarios que revisen un "problema" con el registro de vacunación mediante un Calendario de vacunación COVID-19 como señuelo.

El Agente Tesla se ha implementado en varias iteraciones desde que apareció por primera vez alrededor de 2014. Luego, se observó una primera campaña que fue analizada bajo indicadores publicados en el blog Morphisec, desde noviembre de 2020 donde se detectó cada servicio (HTTP, FTP y SMTP) que usa el agente Tesla para la exfiltración de datos en la IP explorada anteriormente. Donde las IP asociadas con subdominios que muestran el comportamiento del Agente Tesla también usan la misma pila de servicios web (MariaDB, Apache, PHP) con SMB abierto, para más información ver el Boletín 2021-128.

En la actual campaña de phishing, el archivo malicioso que se encuentra en el cuerpo del correo resulta ser un documento .RTF que explota la conocida vulnerabilidad de Microsoft Office rastreada como CVE-2017-11882, un error de ejecución remota de código (RCE) derivado de un manejo inadecuado de la memoria. Una vez abierto, el documento descarga y ejecuta el malware Agent Tesla.

Una vez ejecutado, el agente Tesla se pone a recopilar información del sistema de la víctima y a recoger las credenciales y otros datos confidenciales. Luego envía la información a los ciberdelincuentes a través del protocolo SMTP, a una cuenta de correo electrónico registrada por los atacantes.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-277
Asunto	NUEVA ACTIVIDAD DEL RANSOMWARE BLACK KINGDOM
Emisión	25/06/2021
CVE	CVE-2019-11510, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 y CVE-2021-27065
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Pulse Secure (PCS) antes de 8.2R12.1, 8.3R7.1 y 9.0R3.4
• Servidores Microsoft Exchange

Descripción

El ransomware Black Kingdom apareció en escena en 2019, pero observamos nueva actividad en 2021. Un ciberdelincuente desconocido utilizó el ransomware para explotar una vulnerabilidad de Microsoft Exchange (CVE-2021-27065).

La actividad pasada de Black Kingdom indica que el ransomware se utilizó en campañas de explotación de vulnerabilidades más importantes relacionadas con Pulse Secure o Microsoft Exchange. Los informes públicos indicaron que el adversario detrás de la campaña, después de explotar con éxito la vulnerabilidad, instaló un webshell en el sistema comprometido. El webshell permitió al atacante ejecutar comandos arbitrarios, como un script de PowerShell para descargar y ejecutar el ejecutable de Black Kingdom.

Black Kingdom está codificado en Python y compilado en un ejecutable usando PyInstaller. Al analizar el código de forma estática, se descubrió que la mayor parte de la lógica del ransomware estaba codificada en un archivo llamado 0xfff.py. El ransomware está escrito en Python 3.7. Antes del cifrado de archivos, Black Kingdom usa PowerShell para intentar detener todos los procesos en el sistema que contienen "sql". Una vez hecho esto, Black Kingdom eliminará el historial de PowerShell en el sistema. Combinado con una limpieza de los registros del sistema, esto respalda la teoría de que los atacantes intentan permanecer ocultos en el sistema eliminando todos los rastros de su actividad.

Se examino la implementación del cifrado de archivos por parte del autor y se encontró varios errores que podrían afectar a las víctimas directamente. Durante el proceso de cifrado, Black Kingdom no comprueba si el archivo ya está cifrado o no. Otras familias de ransomware normalmente agregan una extensión específica o un marcador a todos los archivos cifrados. Sin embargo, si el sistema ha sido infectado por Black Kingdom dos veces, los archivos del sistema también se cifrarán dos veces, lo que puede impedir la recuperación con una clave de cifrado válida.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) mostrados en el boletín, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-279
Asunto	CAMPAÑA DE PHISHING UTILIZA NUEVO FORMATO DE ARCHIVOS PARA DISTRIBUIR MALWARE
Emisión	25/06/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

Recientemente se ha observado que las campañas de phishing utilizan el formato WIM (Windows Imaging Format), el cual contiene archivos ejecutables, para distribuir el malware Agent Tesla, con el propósito de robar credenciales y datos confidenciales.

Recientemente se observó que se está utilizando un nuevo formato de archivos malicioso conocido como WIM (Windows Imaging Format) que pretende presentarse como facturas. WIM es un formato de imagen de disco basado en archivos desarrollado por Microsoft. El formato de archivo se utiliza para implementar componentes de software de Windows y actualizaciones de Windows. Este formato utiliza una extensión ".wim" y su contenido se puede extraer mediante herramientas de archivo como 7Zip, PowerISO y PeaZip.

En esta campaña de phishing se utiliza una extensión de archivo '.wim.001' el cual denota que son la primera parte de un archivo WIM más grande. Al analizar los archivos se observó que contienen un solo archivo adjunto WIM que no está comprimido, también contiene un archivo oculto que se observó mediante un editor hexadecimal.

El propósito de estos archivos es ejecutar el backdoor Agent Tesla, el cual está siendo utilizado en múltiples campañas de phishing durante el año 2021, una vez ejecutado el agente Tesla, se pone a recopilar información del sistema de la víctima y a recoger las credenciales y otros datos confidenciales, para más información ver el Boletín 2021-276.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-280
Asunto	NUEVAS CAMPAÑAS DE PHISHING DISTRIBUYEN BACKDOORS BANCARIOS
Emisión	30/06/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Recientemente se observaron dos nuevas campañas activas que contenían archivos adjuntos en formato ZIP o enlaces hacia archivos ZIP, con el objetivo de distribuir backdoors bancarios para pretender conseguir datos confidenciales de la víctima.

La campaña recientemente observada conocida como DotDat distribuyó archivos adjuntos ZIP, el cual contenía un archivo Excel malicioso. El propósito del Excel es descargar un payload malicioso a través de una macro que genera una URL con el fin de ejecutar backdoors entre estos se encuentra ICEID y QBOT.

IcedID: Este malware tiene un payload que envía cierta confidencial del usuario (nombre de usuario, dirección MAC, versión de Windows, etc.) a un servidor C&C. Si bien todavía se distribuye como una imagen PNG, los métodos de ejecutar su payload y comunicación C&C siguen siendo los mismos, los ciberdelincuentes dejaron de utilizar un shellcode. En cambio, IcedID se distribuye como un archivo PE estándar con algunos datos relacionados con el payload usado al inicio del ataque, para mayor información revisar el Boletín NRO 2021-225.

Qbot: A diferencia de IcedID, QBot contiene un único archivo ejecutable DLL para realizar el robo de contraseñas, realizar inyecciones web y tomar el control remoto del sistema infectado, descarga módulos adicionales, hVNC (módulo de control remoto), recolección de correos electrónicos y otros, para mayor información revisar el Boletín NRO 2020-307.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-283
Asunto	NUEVA CAMPAÑA DEL MALWARE HANCITOR
Emisión	30/06/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Recientemente se observó nueva campaña que distribuye el backdoor Hancitor que es utilizado para insertar malware, mediante documentos Word el cual tiene como principal objetivo obtener información confidencial.

El malware Hancitor se encontraba dentro de un documento Word basado en macros. Este documento de una sola página contenía una imagen con instrucciones, intentando engañar a la víctima para que pueda habilitar macros maliciosas.

Cuando se habilita la macro, se inicia un ciclo de infección en el cual el archivo DLL de Hancitor es utilizada como vector inicial. El archivo DLL de Hancitor es utilizada como objeto de incrustación y enlazado de objetos, llamado "rem.r", el cual se ejecutará a través de rundll32.exe. En conjunto, pretende inyectar malware Cobalt Strike mediante rundll32.exe.

Finalmente, el malware de Hancitor realizará búsquedas de la dirección IP externa del sistema infectado. Luego se conecta mediante un servidor C2, a través de solicitudes HTTP POST, para compartir información del sistema, nombres de usuario, nombre de host, entre otros.

Actualización o Mitigación

• Considerar deshabilitar macros en archivos de Office, evitando que pueda ser aprovechado por softwares maliciosos.

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.
- 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 el boletín asociado, 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.