SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Quincenal de Ciberinteligencia Securesoft

Fecha:

07 junio de 2021

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia

CIB-FOR-2021-011

Índice

1. Objetivo

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

2. Alcance

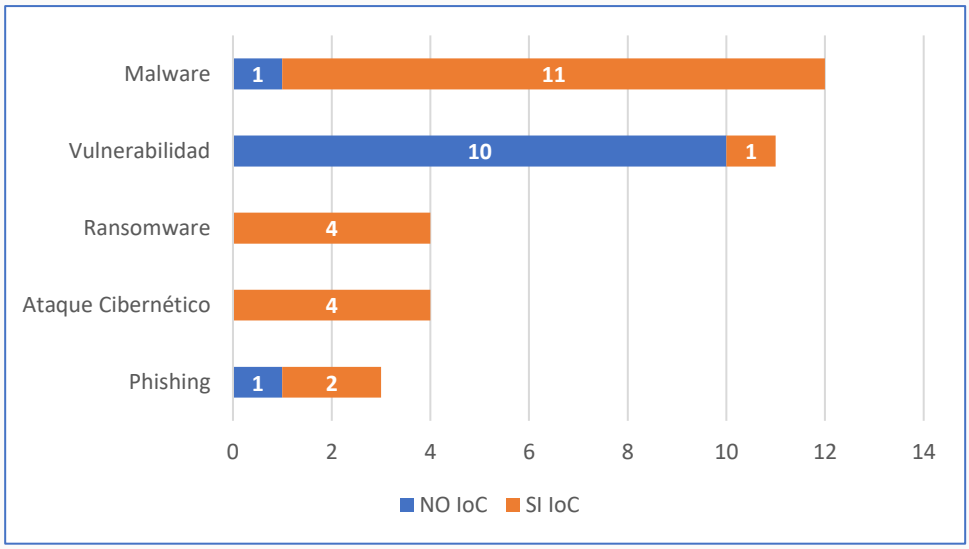
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 16 de mayo hasta el 31 de mayo del 2021.

3. Resumen

En el presente informe se exponen 34 análisis de vulnerabilidad y amenazas, de las cuales 2 tiene severidad media, 29 tienen severidad alta y 3 severidad crítica.

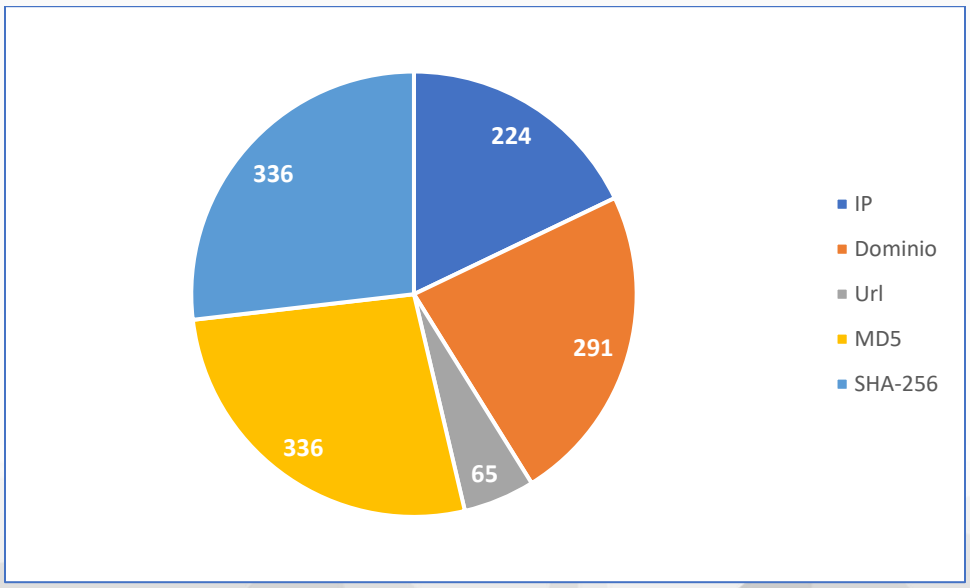
Amenazas analizadas por tipología

En las investigaciones elaboradas para el presente informe se trataron malware, vulnerabilidad, ransomware, ataque cibernético 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 1252 IoCs entre direcciones IP, Dominios, URL, MD5 y SHA256.



Tendencias en nuevas vulnerabilidades

- Recientemente se encontró una vulnerabilidad que puede ser explotada causando un ataque Zero-Day, con el fin de poder tomar capturas de pantallas sin autorización. Para más información leer el Boletín 2021-218.

- Recientemente VMware ha publicado parches de seguridad para vulnerabilidades que pueden ser explotadas mediante la ejecución remota de código en vCenter Server. Para más información leer el Boletín 2021-219.

- Se público un aviso de seguridad sobre una vulnerabilidad de alta gravedad que podría permitir que un atacante remoto autenticado ejecute código arbitrario con privilegios de root. Para más información leer el Boletín 2021-221.

- El equipo de Chrome publica una nueva actualización para sus servidores, el cual contiene parches para evitar la ejecución remota de códigos maliciosos como principal amenaza entre otras posibles afectaciones. Para más información leer el Boletín 2021-223.

- Recientemente SonicWall anunció la disponibilidad de parches para una vulnerabilidad grave en su producto Network Security Manager (NSM). Para más información leer el Boletín 2021-232.

Tendencias en actividades maliciosas

- Se descubrió una campaña de malware que está propagando un troyano de acceso remoto (RAT) registrado como STRRAT. El RAT fue diseñado para robar datos de las víctimas mientras se hace pasar por un ataque de ransomware, para más información leer Boletín 2021-216.

- Phorpiex, una botnet conocida por sus campañas de extorsión, ha comenzado a diversificar su infraestructura. La botnet ahora se ha vuelto más resistente y distribuye payloads más peligrosas. Según Microsoft, ahora mantiene una gran red de bots y realiza actividades maliciosas en nuevas geografías, para más información leer Boletín 2021-224.

- Se ha registrado campañas de spear-phishing distribuye mensajes que se hacen pasar por instituciones financieras para impulsar aplicaciones de Windows falsas que contenían troyanos de acceso remoto (RAT), para más información leer Boletín 2021-227.

- Este boletín es una actualización sobre el Boletin N° 2021-230 referente a una campaña de explotación hacia productos de Pulse Secure por APT´s, en esta campaña se observó el uso de la vulnerabilidad CVE-2021-22893 recientemente parcheada para comprometer los dispositivos Pulse Secure completamente parcheados, para más información leer Boletín 2021-231.

4. Detalles

Vulnerabilidades

Boletín	2021-202
Asunto	ACTUALIZACIÓN DE SEGURIDAD CISCO DÍA CERO ANYCONNECT VPN
Emisión	17/05/2021
CVE	CVE-2020-3556
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Cisco AnyConnect Secure Mobility Client anteriores a la versión 4.10.00093

Descripción

Esta vulnerabilidad de alta gravedad se encontró en el canal de comunicación entre procesos (IPC) del cliente de Cisco AnyConnect y puede permitir que atacantes locales y autenticados ejecuten scripts maliciosos a través de un usuario objetivo. El CVE-2020-3556 afecta a todas las versiones de cliente de Windows, Linux y macOS con configuraciones vulnerables; sin embargo, los clientes móviles iOS y Android no se ven afectados.

La empresa Cliente de movilidad segura AnyConnect le permite trabajar en dispositivos corporativos conectados a una red privada virtual segura (VPN) a través de Secure Sockets Layer (SSL) e IPsec IKEv2 utilizando clientes VPN disponibles para las principales plataformas móviles y de escritorio.

Cisco reveló el error de día cero monitoreado como CVE-2020-3556 en noviembre de 2020 sin publicar actualizaciones de seguridad, pero proporcionó medidas de mitigación para reducir la superficie de ataque.

Aunque el equipo de respuesta a incidentes de seguridad de productos de Cisco (PSIRT) dijo que el código de explotación de prueba de concepto CVE-2020-355 está disponible, también agregó que no hay evidencia de que los atacantes lo exploten en la naturaleza.

La vulnerabilidad ahora se soluciona con las versiones 4.10.00093 y posteriores del software de cliente Cisco AnyConnect Secure Mobility.

Estas nuevas versiones también introducen nuevas configuraciones para permitir / deshabilitar individualmente scripts, ayuda, recursos o actualizaciones de localización en la política local, configuraciones que se recomiendan encarecidamente para mayor seguridad.

Actualización o Mitigación

• Implementar la autenticación multifactor (MFA) para el acceso de los empleados.

Boletín	2021-207
Asunto	MICROSOFT PUBLICA NUEVA ACTUALIZACIÓN DE SEGURIDAD
Emisión	20/05/2021
CVE	CVE-2021-31166
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Microsoft descubrió una falla en sus productos, publicando un parche de seguridad el martes 11 de mayo. Este fue el error más grave en http.sys, un problema que no requiere ni la autenticación ni la interacción del usuario para explotarlo. La vulnerabilidad solo afecta a las últimas versiones de Windows 10 y Windows Server.

Esta vulnerabilidad podría ser explotada para provocar un ataque de denegación de servicio (DoS), en la mayoría de las situaciones, un atacante no autenticado podría enviar un paquete especialmente diseñado a un servidor de destino utilizando HTTP Protocol Stack (http.sys) para procesar paquetes de manera remota.

Recientemente se observó que el error ocurre en http!UlpParseContentCoding, donde la función tiene un local LIST_ENTRY. Un ciberdelincuente remoto no autenticado puede aprovechar esta vulnerabilidad enviando un encabezado HTTP Accept-Encoding diseñado en una solicitud web al sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en condiciones de denegación de servicio o ejecución de código con privilegios de kernel en el peor de los casos.

Actualización o Mitigación

• Realizar las actualizaciones recomendadas por Microsoft para descargar el parche de seguridad aquí.

Boletín	2021-210
Asunto	CISCO PUBLICA ACTUALIZACIONES DE SEGURIDAD
Emisión	21/05/2021
CVE	Según tabla boletín
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

- Versiones de Snort de código abierto anteriores a la versión 2.9.17.1
- Vulnerabilidad con TCP Fast Open (TFO) con el motor de detección Snort
- Versiones de Cisco Prime Infrastructure anteriores a la versión 3.9
- Versiones 2.0.0, 2.0.1, 2.1.0, 2.1.1, 2.1.2 y 2.1.3 del software Cisco Modeling Labs
- Versiones de Cisco Finesse anteriores a la versión 12.6
- Versiones de Cisco DNA Spaces Connector anteriores a la versión 2.3.1
- Versiones de software de Cisco DNA Spaces Connector anteriores a la versión 2.0.519
- Versiones anterior a la versión 5.0.1 EPN Manager
- Versiones de Cisco HCM-F anteriores a la versión 12.6
- Versiones de Cisco AnyConnect Secure Mobility Client anteriores a la versión 4.10.00093
- Software Cisco HyperFlex HX
- Cisco SD-WAN vManage
- Cisco SD-WAN vEdge

Descripción

Se ha analiza 12 vulnerabilidades en el estándar 802.11. Una vulnerabilidad está en la funcionalidad de agregación de marcos, dos vulnerabilidades están en la funcionalidad de fragmentación de marcos y las otras nueve son vulnerabilidades de implementación. Estas vulnerabilidades podrían permitir a un atacante falsificar marcos encriptados, lo que a su vez podría permitir la exfiltración de datos confidenciales de un dispositivo objetivo.
Además de varias vulnerabilidades en la interfaz de administración basada en web de Cisco HyperFlex HX podrían permitir a un atacante remoto no autenticado realizar ataques de inyección de comandos contra un dispositivo afectado.

Actualización o Mitigación

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

Boletín	2021-211
Asunto	ACTUALIZACIÓN DE SEGURIDAD WORDPRESS
Emisión	21/05/2021
CVE	CVE-2021-24340
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Versiones anteriores a 13.0.8 WP Statistics

Descripción

WP Statistics, es un complemento que ofrece análisis para los propietarios del sitio, incluida la cantidad de personas que visitan el sitio, de dónde provienen, qué navegadores y motores de búsqueda usan y qué páginas, categorías y etiquetas tienen la mayoría de las visitas.

Se encontró el error de alta gravedad registrado como CVE-2021-24340, en la función "Pages", que permite a los administradores ver qué páginas han recibido más tráfico. Luego, devuelve estos datos mediante consultas SQL a una base de datos de back-end, y los ciberdelincuentes no autenticados pueden secuestrar la función para realizar sus propias consultas, con el fin de robar información confidencial.

Si bien la página “Pages” estaba destinada solo a administradores y no mostraba información a usuarios que no fueran administradores, era posible comenzar a cargar el constructor de esta página enviando una solicitud a wp-admin/admin.php con el parámetro de página establecido en wps_pages_page. Dado que la consulta SQL se ejecutó en el constructor de la página “Pages”, esto significaba que cualquier visitante del sitio, incluso aquellos sin un inicio de sesión, podría hacer que se ejecute esta consulta SQL. Se podría proporcionar valores malintencionados para el ID o los parámetros de tipo.

En un ataque dirigido, esta vulnerabilidad podría usarse para extraer información de identificación personal de sitios comerciales que contienen información de clientes. Esto subraya la importancia de tener protecciones de seguridad con un firewall de punto final en el lugar donde se almacenan datos confidenciales.

Actualización o Mitigación

• Realizar actualización de seguridad a la versión 13.0.8.

Boletín	2021-212
Asunto	NUEVAS VULNERABILIDADES ENCONTRADAS POR FRAGATTACKS
Emisión	22/05/2021
CVE	Según tabla boletín
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- Sistemas operativos Windows
- Dispositivos WI-FI Cisco

Descripción

Se han publicado una serie de vulnerabilidades contra una gran cantidad de dispositivos WI-FI llamados Fragattacks. El problema radica en el diseño de los propios protocolos de WI-FI, cabe indicar que estas vulnerabilidades no son fáciles de aprovechar, sin embargo, hasta el momento aún no se han reportado ataques de esta vulnerabilidad. Si los atacantes están lo suficientemente cerca, podrían interceptar la información del propietario, activar código malicioso y / o apoderarse del dispositivo.

Sin embargo, eso no significa que se puedan ignorar. Si los atacantes están lo suficientemente cerca, podrían interceptar la información del propietario, activar código malicioso y / o apoderarse del dispositivo. Las vulnerabilidades descubiertas afectan a todos los protocolos de seguridad modernos de Wi-Fi, incluida la última especificación WPA3. Incluso el protocolo de seguridad original de Wi-Fi, llamado WEP, se ve afectado.

Mientras los proveedores trabajan para lanzar parches, es vital que los propietarios de dispositivos implementen las mejores prácticas de seguridad de Wi-Fi comprobadas. “Tanto los usuarios finales como los administradores deben coordinar sus esfuerzos para parchear regularmente los dispositivos conectados, que incluyen enrutadores, dispositivos IoT y teléfonos inteligentes

Ciertamente, debe considerar proteger sus datos mejorando la seguridad del sitio web para usar siempre HTTPS para cifrar todo el tráfico. Muchas aplicaciones web móviles ahora usan esto de forma predeterminada, lo que significa que los usuarios móviles no pueden verse comprometidos por FragAttacks. Debe prestar especial atención a los inicios de sesión en sitios web para asegurarse de que se realicen a través de conexiones cifradas. En segundo lugar, use esto como recordatorio de que necesita actualizar su firmware de banda ancha y Wi-Fi con regularidad.

Actualización o Mitigación

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

Boletín	2021-218
Asunto	NUEVA VULNERABILIDAD ENCONTRADA EN SISTEMA OPERATIVO MACOS
Emisión	25/05/2021
CVE	CVE-2021-30713
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Sistemas operativos MacOS

Descripción

En la última versión de macOS (11.4), Apple parcheó un exploit de día cero (CVE-2021-30713) que pasó por alto el marco de Control y Consentimiento de Transparencia (TCC), este es el sistema que controla a qué recursos tienen acceso las aplicaciones, como otorgar acceso al software de colaboración de video a la cámara web y al micrófono, para participar en reuniones virtuales. El exploit podría permitir que un atacante obtenga acceso completo al disco, grabación de pantalla u otros permisos sin requerir el consentimiento explícito del usuario.

El malware está escrito en AppleScript, un lenguaje de secuencias de comandos desarrollado por Apple, que facilita el control de las aplicaciones Mac habilitadas para secuencias de comandos.

El script ejecuta las siguientes acciones en esta secuencia:

1.El módulo de captura de pantalla XCSSET AppleScript se descarga desde el servidor de comando y control (C2) del autor del malware (en la carpeta ~ / Library / Caches / GameKit).

2.Con el comando osacompile, el módulo de captura de pantalla se convierte en una aplicación basada en AppleScript llamada avatarde.app. Cuando cualquier AppleScript se compila de esta manera, se coloca un ejecutable llamado “applet” en el directorio / Contenidos / MacOS / del paquete de aplicaciones recién creado y el script que ejecutará el applet se puede ubicar en / Contenidos / Recursos / Scripts / main. scpt.

3.Luego, el binario plutil modifica el Info.plist recién creado, cambiando la configuración de preferencia LSUIElement a true. Esto permite que la aplicación se ejecute como un proceso en segundo plano, ocultando su presencia al usuario.

4.A continuación, se descarga un icono en blanco y se aplica a la aplicación.

Actualización o Mitigación

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

Boletín	2021-219
Asunto	NUEVAS VULNERABILIDADES ENCONTRADAS EN SERVIDORES VCENTER
Emisión	25/05/2021
CVE	CVE-2021-21985 y CVE-2021-21986
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Vcente Server versión 6.5 3n, versión 6.7 3m y versión 7.0 2a

Descripción

Las vulnerabilidades que VMware ha publicado, reside en vCenter Server , una herramienta utilizada para administrar la virtualización en grandes centros de datos. vCenter Server se utiliza para administrar los productos de host vSphere y ESXi de VMware.

El CVE-2021-21985 es una vulnerabilidad de ejecución remota de código en vSphere Client a través del complemento de verificación de estado Virtual (vSAN), que está habilitado de forma predeterminada. El cliente vSphere (HTML5) contiene una vulnerabilidad de ejecución remota de código debido a la falta de validación de entrada en el complemento Virtual SAN Health Check, que está habilitado de forma predeterminada en vCenter Server.

Para aprovechar esta vulnerabilidad, un atacante debería poder acceder a vCenter Server a través del puerto 443. Incluso si una organización no ha expuesto vCenter Server externamente, los atacantes aún pueden aprovechar esta falla una vez dentro de una red. La explotación exitosa le daría a un atacante la capacidad de ejecutar comandos arbitrarios en el host vCenter subyacente.

CVE-2021-21986 es un problema del mecanismo de autenticación en varios complementos de vCenter Server, también se puede explotar a través del puerto 443 y permitir que un atacante realice funciones de complemento sin autenticación. Los complementos de vCenter Server afectados incluyen:

• Comprobación de estado de vSAN

• Recuperación del sitio

• Administrador del ciclo de vida de vSphere

• Disponibilidad de VMware Cloud director.

Actualización o Mitigación

• Actualizar a la versión reciente de VMware como vCenter Server 7.0 Update 2b, vCenter Server 6.7 Update 3n y vCenter Server 6.5 Update 3p.

Boletín	2021-220
Asunto	ERRORES EN BLUETOOTH PERMITEN SUPLANTAR DISPOSITIVO LEGÍTIMO Y LANZAR ATAQUES DDOS
Emisión	26/05/2021
CVE	CVE-2020-26559, CVE-2020-26556, CVE-2020-26557, CVE-2020-26560, CVE-2020-26555 y CVE-2020-26558
Categoría	Vulnerabilidad
Severidad	Media

Servicios Afectados

- Core Specification 5.2
- Mesh Profile 1.0.1

Descripción

Se identificaron siete vulnerabilidades, incluidas las vulnerabilidades afectadas durante el emparejamiento y el aprovisionamiento de dispositivos para unirse a una red de malla.

Los dispositivos que admiten la tecnología central de "Bluetooth" son vulnerables al protocolo de entrada de clave de acceso que se utiliza en Secure Simple Pairing (SSP), Secure Connections (SC) y LE Secure Connections (LESC). En estas circunstancias, si se recibe un ataque de intermediario, un atacante puede falsificar fácilmente el dispositivo.

Lista de vulnerabilidades:

- CVE-2020-26559: Bluetooth Mesh Profile AuthValue leak.

Especificaciones afectadas: Mesh Profile Spec, v1.0 to v1.0.1

- CVE-2020-26556: Malleable commitment in Bluetooth Mesh Profile provisioning

Especificaciones afectadas: Mesh Profile Spec, v1.0 to v1.0.1

- CVE-2020-26557: Predictable Authvalue in Bluetooth Mesh Profile

Especificaciones afectadas: Mesh Profile Spec, v1.0 to v1.0.1

- CVE-2020-26560: Impersonation attack in Bluetooth Mesh Profile provisioning

Especificaciones afectadas: Mesh Profile Spec, v1.0 to v1.0.1

- CVE-2020-26555: Impersonation in the BR/EDR pin-pairing protocol

Especificaciones afectadas: Core Spec, v1.0B to 5.2

- CVE-2020-26558: Impersonation in the Passkey entry protocol

Especificaciones afectadas: Core Spec, v2.1 to 5.2

Actualización o Mitigación

- Realizar las actualizaciones de seguridad y aplicar el modo de conexiones seguras.

Boletín	2021-221
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE VPN PULSE SECURE
Emisión	26/05/2021
CVE	CVE-2021-22908
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• VPN Pulse Connect Secure 9.0Rx y 9.1Rx.

Descripción

La vulnerabilidad, identificada como CVE-2021-22908, tiene una puntuación CVSS de 8.5 de un máximo de 10 e impacta en las versiones 9.0Rx y 9.1Rx de Pulse Connect Secure. En un informe que detalla la vulnerabilidad, el problema se deriva de la capacidad de la puerta de enlace para conectarse a los recursos compartidos de archivos de Windows a través de una serie de puntos finales CGI que podrían aprovecharse para llevar a cabo el ataque.

Al especificar un nombre de servidor largo para algunas operaciones pequeñas y medianas, la aplicación 'smbclt' puede bloquearse ya sea debido a un desbordamiento de pila o un desbordamiento de búfer de pila, dependiendo de la duración del nombre del servidor.

Se recomienda a los clientes de Pulse Secure que actualicen a PCS Server versión 9.1R.11.5 cuando esté disponible. Mientras tanto, Ivanti, la compañía detrás de los dispositivos Pulse Secure VPN, ha publicado un archivo de solución alternativa 'Workaround-2105.xml' que se puede importar para deshabilitar la función del navegador de archivos compartidos de Windows agregando los puntos finales de URL vulnerables a una lista de bloqueo y, por lo tanto, activar las mitigaciones necesarias para protegerse contra esta vulnerabilidad.

Cabe señalar que los usuarios que ejecutan PCS versiones 9.1R11.3 o inferiores necesitarían importar un archivo diferente llamado 'Solución alternativa-2104.xml', lo que requiere que el sistema PCS esté ejecutando 9.1R11.4 antes de aplicar las salvaguardas en 'Solución alternativa-2105.xml'.

Actualización o Mitigación

• Implementar la autenticación multifactor (MFA) para el acceso de los empleados.

Boletín	2021-223
Asunto	NUEVA ACTUALIZACIÓN DE SEGURIDAD DE GOOGLE CHROME
Emisión	27/05/2021
CVE	Según tabla boletín
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Google Chrome 90.0.4430.212.

Descripción

Google anunció recientemente el lanzamiento de Chrome 91 para los usuarios de Windows, Mac y Linux. La última actualización corrige un total de 32 vulnerabilidades.

De los problemas abordados, fuentes externas descubrieron 21 vulnerabilidades, incluidos 8 errores de gravedad alta, 8 defectos de gravedad media y 5 agujeros de seguridad de gravedad baja, el más importante de ellos es CVE-2021-30521.

La nueva versión del navegador también incluye parches para seis fallas de uso en WebAudio, WebRTC, TabStrip, TabGroups, WebUI y WebAuthentication. El octavo error de seguridad de alto riesgo es una escritura fuera de límites en TabStrip, Cuatro de los ocho problemas de gravedad media que se abordan con esta actualización de Chrome son un cumplimiento insuficiente de las políticas.

Google también parcheó la lectura fuera de límites de baja gravedad, el cumplimiento de políticas insuficientes y las vulnerabilidades de la interfaz de usuario de seguridad incorrectas.

Actualización o Mitigación

• Realizar la actualización del navegador web a Google Chrome 91.0.4472.77.

Boletín	2021-232
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE SONICWALL
Emisión	31/05/2021
CVE	CVE-2021-20026
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• NSM On-Prem 2.2.0-R10 y versiones anteriores.

Descripción

NSM es una aplicación de administración de firewall que brinda la capacidad de monitorear y administrar todos los servicios de seguridad de la red desde una única interfaz, así como de automatizar tareas para mejorar las operaciones de seguridad. La plataforma de SonicWall está disponible tanto para implementaciones locales como SaaS (Software-as-a-Service).

Registrada como CVE-2021-20026 y con una puntuación CVSS de 8.8, la vulnerabilidad recientemente parcheada afecta a las versiones locales de SonicWall NSM, pero no afecta a las versiones NSM SaaS.

El problema es una falla en la inyección de comandos del sistema operativo que podría ser aprovechada por un atacante que logro autenticarse en un sistema vulnerable. El hecho de que se requiera autenticación para la explotación reduce la gravedad de la falla. Una vez autenticado puede enviar solicitudes HTTP especialmente diseñadas para la aplicación vulnerable logrando ejecutar comandos con privilegios más altos(root).

La vulnerabilidad se solucionó con el lanzamiento de las versiones 2.2.1-R6 y 2.2.1-R6 de NSM.

Actualización o Mitigación

• Implementar la autenticación multifactor (MFA) para el acceso de los empleados.

Amenazas

Boletín	2021-199
Asunto	NUEVO RANSOMWARE LORENZ INTENTA REALIZAR ATAQUES PERSONALIZADOS
Emisión	17/05/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Un nuevo grupo de ransomware Lorenz se está haciendo conocido desde el mes pasado, desde entonces ha acumulado una lista cada vez mayor de víctimas cuyos datos robados se han publicado en un sitio web no seguro. Lorenz pretende abrirse paso mediante una red y extenderse lateralmente a otros dispositivos hasta que obtengan acceso a las credenciales de administrador de dominio en Windows.

Los ciberdelincuentes de Lorenz personalizan el ejecutable del malware diseñado para dirigir sus atacaques a empresas específicas, el ransomware pretende ejecutar un archivo llamado ScreenCon.exe que parece ser un controlador de dominio de la red local.

Al cifrar archivos, el ransomware utiliza cifrado AES y una clave RSA incorporada para cifrar la clave de cifrado. Para cada archivo cifrado, una de las acción del ransomware será la de renombrar el archivo agregando la extensión ".Lorenz.sz40".

Por ejemplo, un archivo llamado 1.doc se cifraría y se cambiaría el nombre a 1.doc.Lorenz.sz40.

A diferencia de otros ransomware dirigidos a empresas, Lorenz no eliminaría los procesos ni cerraría los servicios de Windows antes de la encriptación. Cada carpeta en la computadora será una nota de rescate llamada HELP_SECURITY_EVENT.html que contiene información sobre lo que sucedió con los archivos de la víctima. También incluirá un enlace al sitio de filtración de datos de Lorenz y un enlace a un sitio de pago único donde la víctima puede ver su demanda de rescate

Actualización o Mitigación

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

Boletín	2021-200
Asunto	CAMPAÑA DE PHISHING PROPAGA NUEVO CRYPTER SNIP3 RAT
Emisión	17/05/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

El Crypter se envía más comúnmente a través de correos electrónicos de phishing, que conducen a la descarga de un archivo visual básico. En algunos casos, sin embargo, la cadena de ataque comienza con un archivo de instalación grande, como un instalador de Adobe.

Crypter implementa varias técnicas avanzadas para evitar la detección, como:

• Ejecutar código de PowerShell con el parámetro 'remotesigned'.

• Validación de la existencia de virtualización de Windows Sandbox y VMWare usando Pastebin y top4top para la puesta en escena.

• Compilación de cargadores RunPE en el punto final en tiempo de ejecución.

Se ha nombrado al Crypter "Snip3" basado en el nombre de usuario del denominador común tomado del indicador PDB que se encontró en una variante anterior. La actividad de Crypter se observó por primera vez el 4 de febrero de 2021 y aún continúa. Los primeros envíos de la variante relacionada en VirusTotal demuestran su naturaleza evasiva, ya que pocas soluciones de seguridad pudieron detectarla.

La capacidad del Snip3 Crypter para identificar entornos virtuales y de espacio aislado lo hace especialmente capaz de eludir las soluciones centradas en la detección. Como resultado, las organizaciones centradas en la detección deben tener cuidado con los ataques como Snip3 y otros.

Actualización o Mitigación

• Considerar deshabilitar PowerShell, evitando que pueda ser aprovechado por softwares maliciosos.

Boletín	2021-201
Asunto	CAMPAÑA DE CIBERDELINCUENTES VULNERAN MICROSOFT BUILD ENGINES PARA PROPAGAR MALWARE
Emisión	17/05/2021
CVE	No
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

• Microsoft Build Engine (MSBuild)

Descripción

MSBuild es una plataforma de desarrollo de Microsoft legítima y de código abierto, similar a la utilidad make de Unix, para crear aplicaciones. Esta herramienta de desarrollo puede crear aplicaciones en cualquier sistema Windows si se le proporciona un archivo de proyecto de esquema XML que le indique cómo automatizar el proceso de creación (compilación, empaquetado, prueba e implementación).

Para esta campaña los ciberdelincuentes utilizan archivos de proyectos de MSBuild maliciosos que incluían ejecutables codificados y códigos de shell para inyectar payloads finales en la memoria de los procesos recién generados. Si bien no se puede determinar el método de distribución de los archivos [.]proj, el objetivo de estos archivos es ejecutar Remcos o RedLine Stealer.

Para lo cual, los ciberdelincuentes comenzaron a introducir payloads de Remcos RAT, Quasar RAT y RedLine Stealer en las computadoras de sus víctimas el mes pasado en ataques que aún estaban activos. Una vez que las RAT están instaladas en un sistema de destino, se pueden usar para recopilar pulsaciones de teclas, credenciales e instantáneas de pantalla, deshabilitar el software anti-malware, obtener persistencia y controlar completamente los dispositivos de forma remota.

En las computadoras donde los atacantes desplegaron el ladrón de información, el malware buscará navegadores web, aplicaciones de mensajería, VPN y software de criptomonedas para robar las credenciales de los usuarios.

Actualización o Mitigación

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

Boletín	2021-203
Asunto	NUEVO SKIMMER AFECTA A PLATAFORMAS DE MAGENTO
Emisión	18/05/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Plataforma ecommerce Magento

Descripción

La plataforma de comercio electrónico Magento se ha vuelto un blanco frecuente para los ciberdelincuentes de Magecart, que tienen una gran actividad para atacar plataformas de comercio electrónico vulnerables.

El grupo Magecart es bien conocido por distribuir continuamente nuevo malware para atacar sitios web de compras en línea al inyectar un skimmer en la página de pago para robar datos de tarjetas de crédito / débito.

Recientemente se ha descubierto que el grupo12 Magecart ha comenzado sus ataques con un nuevo skimmer basado en lenguaje PHP. Las campañas observadas actualmente por los Shells web conocida como Megalodon fueron desarrolladas por este grupo de Magecart para infectar tiendas en línea cargando código de skimming de JavaScript a través de solicitudes del lado del servidor de forma dinámica esto con el fin de robar detalles de tarjetas de los sitios web de Magento.

Actualización o Mitigación

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

Boletín	2021-204
Asunto	NUEVA CAMPAÑA DE PHISHING BAJO EL BACKDOOR QAKBOT
Emisión	18/05/2021
CVE	No
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

Recientemente se está observando una campaña de phishing que está dirigido a países de habla hispana, sus últimas campañas están dirigidas a Perú, esta campaña pretende inyectar un backdoor Qakbot. Las tácticas, técnicas y procedimientos del grupo son simples y efectivos, su asociación con el troyano bancario QakBot permite a los atacantes mapear la red, moverse lateralmente y finalmente implementar el ransomware.

EL ataque comienza con un correo electrónico de phishing que contiene un archivo ZIP adjunto o un enlace a un archivo ZIP que incluye un Visual Basic Script (VBS) malicioso, que luego procede a descargar payloads adicionales responsables de mantener un canal de comunicación adecuado con un atacante.

Una vez que QakBot se instala en la computadora, establece la persistencia y se asegura de que las defensas activas no lo detecten modificando el registro de Windows para agregar sus binarios en la lista de exclusiones de Windows Defender.

Además, Qakbot viene con un complemento hVNC que hace posible controlar el dispositivo infectado a través de una conexión VNC remota. Qakbot realiza esta operación con el fin de desviar grandes sumas de dinero.

Actualización o Mitigación

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

Boletín	2021-205
Asunto	NUEVA INFORMACIÓN DEL RANSOMWARE AVADDON
Emisión	19/05/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

El grupo de Ransomware Avaddon atacó a una empresa multinacional de seguros AXA deteniendo las operaciones de TI en sus oficinas ubicadas en Filipinas, Hong Kong, Malasia y Tailandia. Los ciberdelincuentes afirmaban en su sitio de filtración que tenía 3 TB de información confidencial entre reportes médicos,pago de clientes, entre otros.

Luego en conjunto los ciberdelincuentes provocaron un ataque DDoS en curso contra los sitios globales de AXA por el cual los hizo innaccesibles por un tiempo.

Los actores de amenazas combinan ransomware y ataques DDoS, ya que el ataque de DDoS les ayuda a convencer a algunas empresas a que realicen el pago rápido. Se puede revisar el siguiente boletín relacionado al caso anterior como en el Boletín 2020-184.

Actualización o Mitigación

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

Boletín	2021-206
Asunto	CIBERDELINCUENTES APT FIN7 USA UNA HERRAMIENTA DE PENTESTING PARA INFECTAR EQUIPOS
Emisión	20/05/2021
CVE	No
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Este grupo de ciberdelincuentes FIN7 ha estado atacando a diferentes organizaciones desde el 2015 y su método de ataque es principalmente usar diferentes ataques de phishing con malwares para robar datos clave como, por ejemplo, datos de tarjetas bancarias para luego venderlos.

Además, se conoce que FIN7 está usando un nuevo tipo de backdoor llamada “Lizar” que se está utilizando para controlar todos los equipos infectados con el malware, siendo la gran mayoría sistemas informáticos basados en Windows y pertenecientes a EEUU.

Lizar contiene varios tipos de plugins y un loader que sirven para realizar diferentes tipos de tareas. Es decir, los equipos infectados de Windows ejecutan el kit de herramientas, el cual, sirve para conectar al cliente con un servidor remoto. Este kit de herramientas tiene tres tipos de bots: DLLs, EXEs y PowerShell scripts.

Actualización o Mitigación

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

Boletín	2021-208
Asunto	ATAQUES CONTINUOS DE MALWARE BASADOS EN AUTOHOTKEY
Emisión	20/05/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Se ha descubierto una campaña de malware en curso que depende en gran medida del lenguaje de scripting AutoHotkey (AHK) para entregar múltiples troyanos de acceso remoto (RAT) como Revenge RAT, LimeRAT, AsyncRAT, Houdini y Vjw0rm en sistemas Windows.

Se han detectado al menos cuatro versiones diferentes de la campaña a partir de febrero de 2021. La campaña de entrega de RAT comienza con un script compilado de AutoHotKey (AHK), que es un lenguaje de secuencias de comandos personalizado de código abierto para Microsoft Windows que está destinado a proporcionar teclas de acceso rápido fáciles para la creación de macros y la automatización de software que permite a los usuarios automatizar tareas repetitivas en cualquier aplicación de Windows, y este es un ejecutable independiente que contiene lo siguiente: el intérprete AHK, el script AHK y cualquier archivo que haya incorporado mediante el comando FileInstall.

En esta campaña, los atacantes incorporan scripts/ejecutables maliciosos junto con una aplicación legítima para disfrazar sus intenciones. La infección comienza con un ejecutable AHK que procede a ejecutar diferentes VBScripts que eventualmente cargan el RAT en la máquina comprometida. En una variante del ataque detectado por primera vez el 31 de marzo, el adversario detrás de la campaña encapsuló la RAT eliminada con un ejecutable AHK, además de deshabilitar Microsoft Defender mediante la implementación de un script por lotes y un archivo de acceso directo (.LNK) que apunta a ese script.

Además, se descubrió que una segunda versión del malware bloquea las conexiones a soluciones antivirus populares al alterar el archivo de hosts de la víctima. Esta manipulación niega la resolución de DNS para esos dominios al resolver la dirección IP del host local en lugar de la real. En una línea similar, otra cadena de carga observada el 26 de abril implicó la entrega de LimeRAT a través de un VBScript ofuscado, que luego se decodifica en un comando de PowerShell que recupera una carga útil de C # que contiene el ejecutable de la etapa final de un servicio de plataforma de intercambio similar a Pastebin llamado " stikked.ch ".

Actualización o Mitigación

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

Boletín	2021-209
Asunto	TROYANO BANCARIO BIZARRO EXPANDE SUS ATAQUES
Emisión	20/05/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Bizarro tiene módulos x64 y puede engañar a los usuarios para que ingresen códigos de autenticación de dos factores en ventanas emergentes falsas. También puede utilizar la ingeniería social para convencer a las víctimas de que descarguen una aplicación para teléfonos inteligentes. El grupo detrás de Bizarro utiliza servidores alojados en Azure y Amazon (AWS) y servidores de WordPress comprometidos para almacenar el malware y recopilar la telemetría.

Se identifico esta campaña después de observar correos electrónicos de phishing incrustados con paquetes MSI que se utilizaron para entregar malware Bizarro. Basándose en la victimología, Bizarro se ha dirigido a usuarios de banca en línea en Brasil, Argentina, Chile, Alemania, España, Portugal, Francia e Italia. Los comandos que Bizarro recibe de su servidor de comando y control permite a los atacantes obtener datos sobre la víctima y administrar el estado de la conexión, controlar los archivos ubicados en el disco duro de la víctima, controlar el mouse y el teclado del usuario, controlar la puerta trasera, operar, apagar, reiniciar o borrar el sistema operativo, así como limitar la funcionalidad de Windows, registrar teclas y realizar ataques de ingeniería social que engañan a los usuarios para brindar a los atacantes acceso a las cuentas bancarias.

Una vez que la víctima descarga el instalador de MSI troyanizado, Bizarro descarga un archivo ZIP de un sitio web de WordPress comprometido. El instalador de MSI tiene dos enlaces integrados, el que se elija depende de la arquitectura del procesador de la víctima. El archivo zip contiene una DLL maliciosa escrita en Delphi, un ejecutable legítimo que es AutoHotkey y un pequeño script que llama a una función exportada desde la DLL maliciosa. Tras la ejecución, Bizarro mata todos los procesos del navegador para terminar las sesiones existentes con los sitios web de banca en línea. Una vez que el usuario reinicia el navegador, se verá obligado a volver a ingresar las credenciales de la cuenta bancaria, que luego serán comprometidas por Bizarro. Además de robar credenciales, Bizarro también recopila información del sistema, como el nombre de la computadora, el nombre predeterminado del navegador de la versión del sistema operativo y el nombre del software antivirus instalado.

Actualización o Mitigación

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

Boletín	2021-213
Asunto	NUEVA VARIANTE DEL MALWARE WASTEDLOCKER
Emisión	24/05/2021
CVE	CVE-2019-0752 y CVE-2018-8174
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows.
• Internet Explorer

Descripción

Recientemente se observó una nueva campaña RIG Exploit Kit que explota vulnerabilidades del motor de scripting en el navegador de Internet Explorer los cuales no cuentan con los parches (CVE-2019-0752 y CVE-2018-8174).

Recientemente se ha identificado una nueva variante del malware WastedLocker que explota dos vulnerabilidades del motor de secuencia de comandos en el navegador web de Internet Explorer.

Se ha detectado que WastedLocker usa el administrador de caché de Windows para evadir la detección. Esto se debe a que Windows mueve los archivos de uso común o archivos especificados por una aplicación que se leen o almacenan a la memoria cache que utiliza el sistema, para mas información ver Boletín 2020-240.

El nuevo malware se basa en la campaña RIG Exploit Kit descubierta en febrero del 2021. A diferencia de la campaña anterior, este nuevo malware no tiene el componente ransomware. Dado que simplemente actúa como un cargador, los investigadores lo llamaron WastedLoader.

Esta cadena de explotación de vulnerabilidades inicia con publicidad maliciosa colocada en sitios web legítimos, al hacer click anuncio malicioso te redirige a una pagina de destino RIG EK en el que tendrá incluidos dos exploits, ambos son capaces de descargar y ejecutar el malware de manera individual.

La campaña se basa en exploits de prueba de concepto para las dos vulnerabilidades de VBScript para descargar, descifrar y ejecutar malware malicioso para que intenten recopilar detalles sobre el sistema y enviarlos a un servidor de comando y control C2.

Actualización o Mitigación

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

Boletín	2021-214
Asunto	CAMPAÑA DE CORREO ELECTRÓNICO PROPAGA MALWARE STRRAT
Emisión	24/05/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

El equipo de Microsoft Security Intelligence (MSI) ha identificado una campaña masiva de correo electrónico que entrega el malware StrRAT con la versión 1.5 de la RAT, la cual, mantiene las mismas funciones de backdoor que las versiones anteriores de StrRAT.

StrRAT es una herramienta de acceso remoto basada en Java que roba las credenciales del navegador, registra las pulsaciones de teclas y toma el control remoto de los sistemas infectados, todos comportamientos típicos de las RAT. El RAT también tiene un módulo para descargar un payload adicional en la máquina infectada según el comando del servidor de comando y control (C2). StrRAT también tiene una característica única que no es común a este tipo de malware: un módulo de cifrado/descifrado de ransomware que cambia los nombres de los archivos de una manera que sugiere que el siguiente paso es el cifrado. Sin embargo, StrRAT no cumple con esta función, agregando la extensión de nombre de archivo [.]crimson a los archivos sin cifrarlos realmente.

Para lanzar la campaña, los ciberdelincuentes utilizaron cuentas de correo electrónico comprometidas para enviar varios correos electrónicos diferentes. Algunos de los mensajes utilizan la línea de asunto "Outgoing Payments". Otros se refieren a un pago específico supuestamente realizado por el "Accounts Payable Department", que es la forma en que se firman los correos electrónicos. La campaña incluye varios correos electrónicos diferentes que utilizan ingeniería social en torno a los recibos de pago para alentar a las personas a hacer clic en un archivo adjunto que parece ser un PDF pero que en realidad tiene intenciones maliciosas.

Un correo electrónico informa al destinatario que incluye un "Outgoing Payments" con un número específico, presumiblemente, el PDF adjunto. Otro dirige el mensaje a un "Proveedor" y parece informarle al destinatario que "your payment has been released as per attached payment advice", y le pide al destinatario que verifique los ajustes realizados en el PDF adjunto.

El archivo adjunto en todos estos casos, sin embargo, no es un PDF en absoluto, sino que conecta el sistema a un dominio malicioso para descargar el malware StrRAT, que luego se conecta a un servidor C2.

Actualización o Mitigación

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

Boletín	2021-215
Asunto	NUEVO BOTNET SIMPS UTILIZA MODULOS GAFGYT
Emisión	25/05/2021
CVE	CVE-2017-17215 y CVE-2018-10561
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Recientemente se ha descubierto un nuevo botnet que utiliza módulos GAFGYT el cual se basa en Linux con el fin de poder lanzar ataques DDOS a dispositivos infectados

Al ejecutar el binario de Simps, se conecta a C2 con dirección 23[.]95[.]80[.]200, el binario de Gafgyt (hash: e847dfbd831df6015519d03d42ada8241ce1174e9bd96f405452627617229c63) también estará descargando el binario de Simps desde la misma dirección del C2.

El payload de Simps se infiltra mediante la explotación de múltiples vulnerabilidades de ejecución remota de código en dispositivos IOT vulnerables para convertirlos en bots, para realizar ataques DDOS en direccionesIP específicas. Ambas vulnerabilidades pueden ser explotadas para descargar un binario empaquetado Simps MIPS UPX, para arquitecturas MIPS, con el fin de mostrar un mensaje en el cual dice que el dispositivo ha sido infectado por la botnet Simps.

También se observó que este malware podría dejar mostrar un archivo "keksec.infected.you.log" que contendrá un mensaje "usted ha sido infectado por urmommy, gracias por unirse a keksec".

Actualización o Mitigación

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

Boletín	2021-216
Asunto	NUEVA ACTUALIZACIÓN: CAMPAÑA DE MALWARE STRRAT RAT
Emisión	25/05/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Microsoft Internet Explorer
- Foxmail
- Mozilla Thunderbird
- Mozilla Firefox
- Google Chrome
- Outlook Web Access

Descripción

El STRRAT RAT basado en Java se distribuyó en una campaña masiva de spam, el malware muestra un comportamiento similar al ransomware al agregar la extensión de nombre de "archivo.crimson" a los archivos sin cifrarlos realmente.

Los ciberdelincuentes detrás de la campaña utilizaron cuentas de correo electrónico comprometidas para enviar mensajes de spam que contenían una imagen que se hacía pasar por un archivo PDF adjunto. Al abrir la imagen, el código malicioso se conecta a un dominio para descargar STRRAT RAT. Los investigadores notaron que la versión 1.5 de STRRAT es notablemente más confusa y modular que las versiones anteriores. El malware admite múltiples funciones, como recopilar contraseñas del navegador, ejecutar comandos remotos y PowerShell, y registrar pulsaciones de teclas.

La RAT se enfoca en robar credenciales de navegadores y clientes de correo electrónico, y contraseñas a través del registro de teclas. Es compatible con los siguientes navegadores y clientes de correo electrónico: Firefox, Internet Explorer, Chrome, Foxmail, Outlook y Thunderbird.

Actualización o Mitigación

- Considerar deshabilitar PowerShell, evitando que pueda ser aprovechado por softwares maliciosos.

Boletín	2021-217
Asunto	RANSOMWARE ZEPPELIN VUELVE CON VERSIONES ACTUALIZADAS
Emisión	25/05/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

Una variante reciente del malware estuvo disponible en un foro de ciberdelincuentes a fines del mes pasado. El ransomware Zeppelin también se conoce como Buran y tiene su origen en la familia Vega / VegaLocker, un ransomware-as-a-service (RaaS) basado en Delphi observado en foros de ciberdelincuentes de habla rusa en 2019.

Los desarrolladores suelen buscar socios para infiltrarse en una red comprometida, robar datos e implementar el malware de cifrado de archivos. Recientemente se descubrió que las actividades del malware se han reanudado en marzo. Además, se anunció en los foros de una actualización importante del software.

Tras la actualización principal, los desarrolladores de Zeppelin lanzaron una nueva variante del malware el 27 de abril que trajo pocos cambios en términos de características, pero aumentó la estabilidad del cifrado. Zeppelin se basa en vectores de ataque iniciales comunes, como RDP, vulnerabilidades de VPN y phishing. Sin embargo, como el ransomware no tiene un sitio de filtración, su objetivo principal es cifrar los datos de las víctimas.

Actualización o Mitigación

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

Boletín	2021-222
Asunto	NUEVA CAMPAÑA REALIZADA POR EL GRUPO AGRIUS
Emisión	27/05/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Inicialmente, el grupo Agrius distribuyó un wiper malware conocido como DEADWOOD (o Detbosit) diseñado para destruir datos en dispositivos infectados y previamente utilizado en ataques contra objetivos de Arabia Saudita en 2019, se cree que fue obra de APT33.

Agrius ha pasado lentamente al uso de un nuevo wiper malware utilizando una combinación de sus propios conjuntos de herramientas, el kit de herramientas de Agrius incluye una cepa de malware destructiva wiper, que se cree que fue obra de APT33.

Las herramientas personalizadas de Agrius tienen un software de seguridad ofensivo fácilmente disponible para implementar una variante personalizada convertido en ransomware y pretenderá retener datos para pedir un rescate como etapa final de los ataques.

Durante las primeras etapas del ataque, Agrius utilizará un software de red privada virtual (VPN) mientras accede a aplicaciones o servicios públicos que pertenecen a la víctima prevista antes de intentar un exploit, a menudo a través de cuentas comprometidas y vulnerabilidades de software.

Si tiene éxito, se implementan webshells, se utilizan herramientas públicas de ciberseguridad para la recolección de credenciales y el movimiento de la red, y luego se implementan los payloads de malware.

Actualización o Mitigación

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

Boletín	2021-224
Asunto	NUEVA ACTIVIDAD DE BOTNET PHORPIEX CENTRADA EN LA DISTRIBUCIÓN GLOBAL
Emisión	27/05/2021
CVE	No
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Desde 2018, se ha observado que la botnet realiza actividades de exfiltración de datos y entrega de ransomware. Tradicionalmente, realizaba actividades de extorsión y spam, sin embargo, ahora también se centra en la minería de criptomonedas.

Phorpiex puede propagarse a través de varios vectores de infección, como la carga de otro malware, programas no deseados, software gratuito o correos electrónicos de phishing de bots ya infectados. El bot puede deshabilitar el antivirus Microsoft Defender para establecer la persistencia en las máquinas de destino. Puede modificar las claves de registro para deshabilitar la funcionalidad de antivirus y firewall o ventanas emergentes. El malware también utiliza trucos de ingeniería social para atraer a sus víctimas, como enviar mensajes sobre errores de seguridad en Zoom.

Phorpiex está difundiendo varias familias de ransomware como Nemty, Knot, BitRansomware (DSoftCrypt / ReadMe), GandCrab, Avaddon y Pony. La orientación geográfica de la botnet también ha cambiado. Campañas anteriores estuvieron dirigidas a objetivos japoneses, mientras que las actividades recientes se centran en la distribución global. Sus tácticas, técnicas y procedimientos se mantuvieron prácticamente iguales, con nombres de archivo comunes, patrones de ejecución y comandos casi consistentes desde principios de 2020 hasta la fecha. Sin embargo, la botnet ha cambiado parte de su arquitectura de comando y control anterior de su alojamiento habitual. Ahora prefiere los dominios producto de algoritmo de generación de dominio sobre los dominios estáticos.

Actualización o Mitigación

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

Boletín	2021-225
Asunto	SERVIDORES DEL MALWARE BANCARIO ICEDID DETECTADOS
Emisión	27/05/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistema operativo Debian

Descripción

El malware bancario IcedID surgió por primera vez en septiembre de 2017 y ha logrado un progreso significativo desde entonces. Esta amenaza, también conocida como BokBot, ha crecido constantemente durante el último año y cuenta con una amplia gama de capacidades maliciosas como el enlace del navegador, el robo de credenciales, la configuración del proxy MiTM y un módulo VNC, entre otros.

Las versiones recientes de IcedID contienen tres componentes maliciosos: el DOC / XLS de punto de entrada que contiene macros maliciosas; un payload de primera etapa; y finalmente un payload de segunda etapa, que a su vez consta de dos subpartes: un cargador de DLL de 64 bits y el bot real cifrado disfrazado como un archivo ".dat".

Si se compara el certificado IcedID con un certificado autofirmado predeterminado, la diferencia más notable es el campo de nombre común. Los servidores públicos deben tener su FQDN en este campo y no localhost.

Se realizó una investigación donde se descubrió que la mayoría de los posibles resultados obtenidos estaban relacionados con IcedID, de lo cual, se obtuvo una lista de 52 servidores., donde se descubrió que estos servidores son componentes de la infraestructura IcedID C&C.

Análisis del servidor

Al analizar los banners orientados a Internet, se pudo encontrar varias propiedades similares para la mayoría de los servidores implementados. Las propiedades más comunes fueron puertos abiertos, sistema operativo y servidor web:

• Puertos abiertos: Servidores con los puertos 443, 80 y SSH (22) disponibles.

• Sistema operativo: Servidores ejecutan un sistema operativo Debian.

• Servidor web: Los servidores ejecutan el servidor web nginx

Actualización o Mitigación

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

Boletín	2021-226
Asunto	NUEVO ATAQUE BASADO EN CORREO ELECTRÓNICO DE NOBELIUM
Emisión	28/05/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

El Centro de Inteligencia de Amenazas de Microsoft (MSTIC) recientemente detectó que el grupo de ciberdelincuentes detrás del ataque SolarWinds vuelve a atacar con una sofisticada campaña de correo electrónico masivo destinada a entregar URL maliciosas con payloads que permitan la persistencia de la red para que los ciberdelincuentes puedan realizar más actividades maliciosas.

Los investigadores observaron que el grupo de ciberdelincuentes comenzó a hacerse pasar por una organización de desarrollo con sede en EE. UU., para distribuir correos electrónicos, incluidas las URL maliciosas, utilizando un servicio legítimo de correo electrónico masivo, Constant Contact. Los objetivos de este ataque en curso son 3.000 cuentas individuales en más de 150 organizaciones, empleando un patrón establecido de uso de infraestructura y herramientas únicas para cada objetivo. En esta campaña, después de que un usuario objetivo abre el archivo malicioso, un JavaScript dentro del HTML escribiría un archivo ISO en el disco e instaría al usuario objetivo a abrirlo. Esto daría como resultado que el archivo ISO se desplegara de manera muy similar a una unidad externa o de red, y un archivo de acceso directo (LNK) ejecutaría una DLL adjunto, lo que haría que Cobalt Strike Beacon se ejecutara en el sistema.

Nobelium comenzó a hacerse pasar por una organización llamada Agencia de los Estados Unidos para el Desarrollo Internacional, o USAID, y a utilizar una dirección de correo electrónico de remitente auténtica que coincide con el servicio estándar de Constant Contact. La dirección variaba para cada destinatario y terminaba en <@in[.]constantcontact[.]com> con una dirección de respuesta de < mhillary@usaid[.]gov>. Los correos electrónicos afirmaron ser una alerta de USAID sobre nuevos documentos publicados por el expresidente Donald Trump sobre el "fraude electoral", que Trump afirmó que ocurrió en las elecciones de 2020 que perdió ante el presidente Joe Biden.

Si un usuario hacía click en el enlace del correo electrónico, la URL lo dirigiría al servicio legítimo de Constant Contact y luego lo redirigiría a la infraestructura controlada por Nobelium a través de una URL que entrega un archivo ISO malicioso.

El despliegue exitoso de estos payloads permite a Nobelium lograr un acceso persistente a los sistemas comprometidos. Esta persistencia, a su vez, permite al grupo ejecutar otros objetivos maliciosos, como el movimiento lateral, la exfiltración de datos y la entrega de malware adicional.

Actualización o Mitigación

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

Boletín	2021-227
Asunto	CAMPAÑAS FINANCIERAS DE SPEAR-PHISHING DISTRIBUYEN RAT
Emisión	29/05/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Un ataque más reciente se hizo pasar por una institución financiera con sede en EE. UU. para apuntar a una empresa estadounidense de energía renovable. El correo electrónico de spear-phishing hacía referencia a un préstamo ficticio e indicaba a los empleados de la organización objetivo que descargaran una aplicación de Windows para completar el proceso de préstamo y recibir 62 millones de dólares.

El correo electrónico contenía dos archivos PDF, uno de los cuales usaba los nombres y la imagen de la Agencia Nacional del Crimen (NCA) del Reino Unido y la otra información SWIFT y tenía una URL desde la que descargar la aplicación. También contenía el nombre de usuario y la contraseña para acceder a él.

Los ciberdelincuentes han registrado un dominio a través del cual pueden compartir los enlaces a las aplicaciones falsas de Windows. Al menos cuatro firmas fueron suplantadas en este dominio: Cumberland Private UK, Truist, FNB America y MayBank.

Esta campaña en curso se ha estado ejecutando desde al menos 2017. Los ciberdelincuentes se han hecho pasar por varias instituciones financieras de todo el mundo, no solo de los EE. UU. y Reino Unido: esto incluye organizaciones de Panamá, África Occidental, Malasia y China. Además, se descubrió que varios sitios que utilizan los mismos servidores, creados en el mismo período de tiempo, disfrazados de bancos de inversión.

los atacantes envían un correo electrónico al objetivo que contiene una URL y credenciales de inicio de sesión para un sitio web falso. Cuando estas credenciales se utilizan para ingresar al sitio, se descarga un instalador que descomprime un archivo ZIP. Esto entrega la aplicación con backdoor que, si es ejecutada por el usuario, proporciona acceso remoto al dispositivo.

Actualización o Mitigación

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

Boletín	2021-228
Asunto	NUEVA ACTIVIDAD DEL RANSOMWARE RYUK
Emisión	28/05/2021
CVE	No
Categoría	Ransomware
Severidad	Media

Servicios Afectados

• Sistemas operativos Windows

Descripción

El ransomware Ryuk, que se detectó por primera vez en 2018, se derivó del código fuente utilizado por el ransomware Hermes. Los actores de amenazas lo implementan utilizando técnicas de fraude manual y herramientas de código abierto para moverse a través de las redes. Al hacer esto, aseguran el acceso administrativo a tantos sistemas como sea posible antes de encriptar archivos.

Habían estado usando Emotet y TrickBot como propagadores iniciales para el ransomware Ryuk y aprovechando los troyanos de productos básicos, pero recientemente cambiaron de táctica. Este cambio de estrategia está diseñado para evitar la detección y permitir que el ransomware Ryuk permanezca en las redes infectadas por más tiempo.

Los actores del ransomware Ryuk utilizaron recientemente estas nuevas herramientas para comprometer una organización gubernamental y cifrar cerca de 2000 sistemas y servicios críticos. Para hacerlo, los atacantes comprometieron una cuenta de administrador de dominio al acceder a las contraseñas almacenadas en una política de grupo. Luego, utilizaron PowerShell para deshabilitar la protección de monitoreo de malware y escanear la red. A continuación, utilizaron BitsAmin, WMIC y PowerShell con credenciales de cuenta privilegiada para copiar Ryuk en hosts adicionales.

Actualización o Mitigación

• Considerar deshabilitar PowerShell y WMIC, evitando que pueda ser aprovechado por softwares maliciosos.

Boletín	2021-229
Asunto	CAMPAÑA DE PUBLICIDAD DE INSTALADORES FALSOS DE ANYDESK
Emisión	29/05/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

La campaña de malvertising que se viene observando recientemente involucra un archivo malicioso que se hace pasar por un ejecutable de configuración para AnyDesk (AnyDeskSetup[.]exe), que al ejecutarse descarga un payload de PowerShell para acumular y exfiltrar información del sistema.

El script tenía algunas ofuscaciones y múltiples funciones que se asemejaban a un payload, así como un dominio codificado (zoomstatistic [.] Com) para el reconocimiento de información como el nombre de usuario, nombre de host, sistema operativo, dirección IP y el nombre del proceso actual.

La secuencia de comandos de PowerShell tiene todas las características de una puerta trasera típica, pero es la ruta de intrusión para un ciberdelincuente, lo que indica que está más allá de una operación de recopilación de datos típica.

El resultado del anuncio fraudulento, cuando se hace clic, redirige a los usuarios a una página de ingeniería social que es un clon del sitio web legítimo de AnyDesk, además de proporcionar al individuo un enlace al instalador troyano. Se estima que el 40% del contenido en el anuncio malicioso se convirtieron en instalaciones del binario de AnyDesk, y el 20% de esas instalaciones incluyeron actividad de seguimiento con el teclado.

Actualización o Mitigación

• Considerar deshabilitar PowerShell, evitando que pueda ser aprovechado por softwares maliciosos.

Boletín	2021-230
Asunto	CUATRO NUEVAS FAMILIAS DE MALWARE DISEÑADAS PARA EXPLOTAR LOS DISPOSITIVOS PULSE SECURE VPN
Emisión	29/05/2021
CVE	CVE-2021-22893, CVE-2019-11510, CVE-2020-8260 y CVE-2020-8243
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Pulse Secure VPN

Descripción

El 20 de abril, el equipo de FireEye, Mandiant, reveló ataques contra organizaciones de defensa, gubernamentales y financieras que utilizan vulnerabilidades en el software.

La vulnerabilidad CVE-2021-22893 descrita como una omisión de autenticación que afecta a Pulse Connect Secure permite a los atacantes no autenticados realizar la ejecución remota de código arbitrario (RCE). Para mayor información revisar el Boletín N° 2021-168. Otras fallas de seguridad relacionadas con los ataques son CVE-2019-11510, CVE-2020-8260 y CVE-2020-8243, que se pueden usar para establecer la persistencia en un dispositivo vulnerable y comprometer aún más los dispositivos. Para mayor información

Los investigadores por Mandiant indican que UNC2630 y UNC2717 son los principales grupos de amenazas persistentes avanzadas (APT) involucrados en estos ataques. Admás, ha encontrado 12 familias y herramientas de malware distintas, incluidas las webshells Atrium y Slightpulse, que afectan las vulnerabilidades de Pulse Secure.

Familias de malware vinculadas a UNC2630 son Bloodmine, Bloodbank, Cleanpulse y Rapidpulse.

Los objetivos de los ciberdelincuentes son robar credenciales, mantener el acceso persistente a largo plazo a las redes de las víctimas y acceder o filtrar datos confidenciales mediante:

• Nombrar archivos de exfiltración para que se parezcan a las actualizaciones de Windows (KB) o para que coincidan con el formato KB <dígitos>[.]zip

• Usar el formato de archivo JAR/ZIP para la exfiltración de datos.

• Eliminar archivos exfiltrados.

Actualización o Mitigación

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

Boletín	2021-231
Asunto	ACTUALIZACIÓN DEL MALWARE DISEÑADO PARA EXPLOTAR VULNERABILIDADES EN PULSE SECURE
Emisión	29/05/2021
CVE	CVE-2021-22893, CVE-2019-11510, CVE-2020-8260 y CVE-2020-8243
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Pulse Secure VPN

Descripción

Recientemente se ha observado la explotación de vulnerabilidades en los productos de Pulse Secure Connect por un ciberdelincuente. Estas entidades confirmaron la actividad maliciosa después de ejecutar la herramienta de integridad Pulse Secure Connect.

Un ciberdelincuente está utilizando este acceso para colocar webshells en el dispositivo Pulse Connect Secure para un mayor acceso y persistencia.

Los webshells permiten una variedad de funciones, incluida la omisión de autenticación, la omisión de autenticación multifactor, el registro de contraseñas y la persistencia a través de parches.

Para mayor información revisar el Boletín N° 2021-230.

Actualización o Mitigación

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

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.