SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Quincenal de Ciberinteligencia Securesoft

Fecha:

16 agosto de 2021

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia

CIB-FOR-2021-016

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

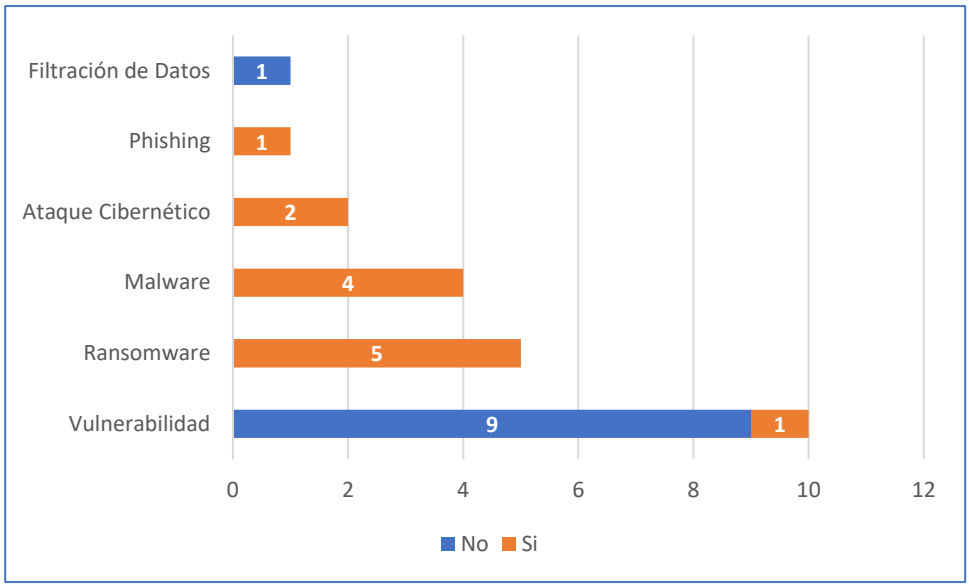
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 1 de agosto hasta el 15 de agosto del 2021.

3. Resumen

En el presente informe se exponen 23 análisis de vulnerabilidad y amenazas, de las cuales 16 tienen severidad alta, 5 severidad crítica y 2 severidad media.

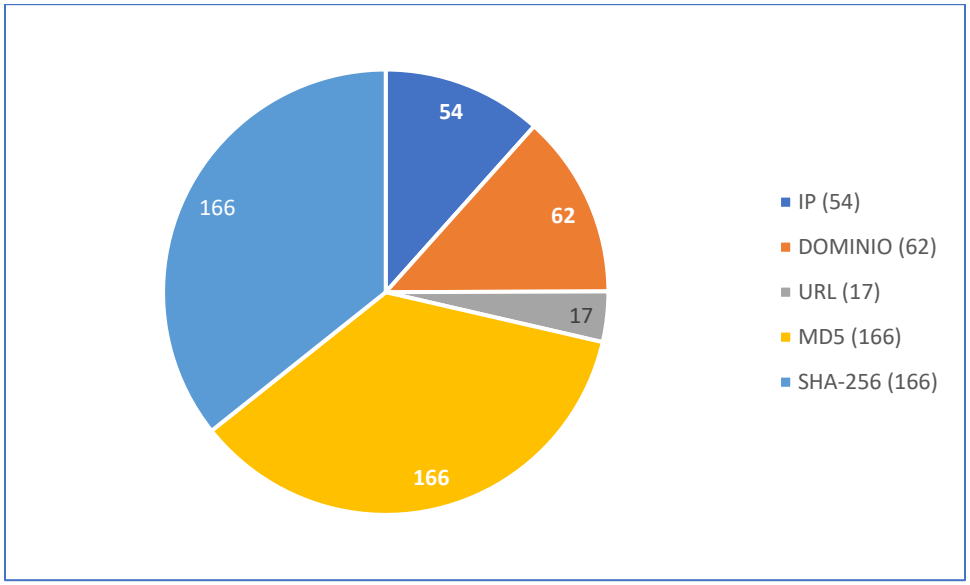
Amenazas analizadas por tipología

En las investigaciones elaboradas para el presente informe se trataron filtración de datos, phishing, ataque cibernético, malware, ransomware y vulnerabilidad. 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 465 IoCs entre direcciones IP, Dominios, URL, MD5 y SHA256.



Tendencias en nuevas vulnerabilidades

- Recientemente, se ha descubierto una nueva vulnerabilidad que podría permitir a un atacante ejecutar consultas SQL en la base de datos remota en IIS y SQL Server. Para más información leer el Boletín 2021-361.

- Recientemente se ha observado que Pulse Secure ha publicado nuevo parche de seguridad para vulnerabilidad crítica que podría explotarse para infiltrarse en una red interna comprometiendo a clientes VPN, y que está siendo explotada activamente por ciberdelincuentes. Para más información leer el Boletín 2021-367.

- Se ha implementado parches para abordar las vulnerabilidades críticas que afectan a los enrutadores VPN de Cisco para pequeñas empresas que podrían ser explotados por un atacante remoto para ejecutar código arbitrario. Para más información leer el Boletín 2021-373.

- Microsoft publicó el paquete de actualizaciones de seguridad correspondiente a agosto de 2021. En esta edición la compañía corrige un total de 44 vulnerabilidades, entre estas vulnerabilidades se encuentran 3 zero-days según Microsoft. Para más información leer el Boletín 2021-375.

Tendencias en actividades maliciosas

- BlackMatter es un nuevo grupo de ransomware que se ofrece como servicio (RaaS) que se fundó en julio de 2021. Según el foro de BlackMatter, los ciberdelincuentes han incorporado en su ransomware las mejores características de DarkSide, REvil y LockBit para recaudar afiliados que ayuden a infiltrarse en redes de grandes empresas, para más información leer Boletín 2021-357.

- Se ha descubierto que los atacantes utilizaron BazarCall, un malware que llega a los usuarios tras la recepción de un correo electrónico que pide llamar a un número de teléfono para cancelar una suscripción que se les va a cobrar en poco tiempo, para instalar Trickbot, para luego ejecutar el ransomware Conti en un dominio corporativo, para más información leer Boletín 2021-362.

- Recientemente se ha observado un nuevo backdoor que se distribuye a través de foros y canales de Telegram, el cual utiliza técnicas de ofuscación, evasión antisandbox y antivirus, ataque de fuerza bruta, el malware realiza todas estas acciones que toma el malware tiene el objetivo de recopilar información confidencial y luego enviarla a una máquina de comando y control C&C, para más información leer Boletín 2021-365.

- Synology, fabricante de NAS con sede en Taiwán, advirtió sobre la botnet StealthWorker está apuntando a sus dispositivos NAS de almacenamiento conectados a la red en ataques continuos de fuerza bruta que conducen a infecciones de ransomware, para más información leer Boletín 2021-370.

4. Detalles

Vulnerabilidades

Boletín	2021-358
Asunto	NUEVA INFORMACIÓN SOBRE ATAQUES HACIA SERVIDORES MICROSOFT EXCHANGE
Emisión	2/08/2021
CVE	CVE-2021-26855 y CVE-2021-27065
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Microsoft Exchange Server

Descripción

Recientemente el equipo de ciberseguridad UNIT42 publicó información relacionada al ataque que ocurrió en marzo del 2021, en el cual los ciberdelincuentes estuvieron explotando vulnerabilidades en servidores de Microsoft Exchange conocida como ProxyLogon.

Tras una explotación exitosa, se cargó un webshell ubicado en un directorio web de acceso público, luego los ciberdelincuentes utilizan una técnica conocida como "living off the land", que utiliza archivos binarios confiables para evitar la detección de antivirus. En este caso, se utilizó el binario bitsadmin.exe de Microsoft Windows para descargar un archivo llamado Aro.dat desde un repositorio de GitHub controlado por un ciberdelincuente.

Al igual que con las variantes anteriores de PlugX, la ejecución del código se logra mediante una técnica conocida como carga lateral de DLL. Una vez que es ejecutado el archivo en la memoria, Aro.dat comienza a descomprimirse e inicia la comunicación con un servidor comando y control.

Actualización o Mitigación

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

Boletín	2021-359
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE MICROSOFT HYPER-V
Emisión	3/08/2021
CVE	CVE-2021-28476
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows 10
- Sistema Operativo Windows Server 2012 y posteriores

Descripción

La falla reside en el controlador del conmutador de red de Microsoft Hyper-V (vmswitch[.]sys). Este problema permite que una máquina virtual fuerce al kernel del host de Hyper-V a leer desde una dirección arbitraria y potencialmente inválida. El contenido de la dirección leída no se devolvería a la máquina virtual. En la mayoría de las circunstancias, esto daría como resultado una denegación de servicio del host Hyper-V, debido a la lectura de una dirección no asignada. Es posible leer desde un registro de dispositivo mapeado en memoria correspondiente a un dispositivo de hardware conectado al host de Hyper-V que puede desencadenar efectos secundarios adicionales específicos del dispositivo de hardware que podrían comprometer la seguridad del host de Hyper-V.

Un atacante podría aprovechar esta vulnerabilidad enviando un paquete especialmente diseñado desde una máquina virtual al host de Hyper-V.

Algunas solicitudes de OID están destinadas al adaptador de red externo u otros adaptadores de red conectados a vmswitch. Mientras procesa las solicitudes de OID, vmswitch rastrea su contenido con fines de registro y depuración. Sin embargo, debido a su estructura encapsulada, vmswitch necesita tener un manejo especial de esta solicitud y eliminar la referencia a OidRequest para rastrear la solicitud interna también. El error es que vmswitch nunca valida el valor de OidRequest y, por lo tanto, puede eliminar la referencia a un puntero no válido.

Actualización o Mitigación

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

Boletín	2021-361
Asunto	NUEVA VULNERABILIDAD EN MICROSOFT IIS Y SQL SERVER
Emisión	3/08/2021
CVE	CVE-2021-28455
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

La nueva vulnerabilidad, registrada como CVE-2021-28455, permite a los ciberdelincuentes atacar de forma remota IIS y SQL Server para obtener privilegios de "SISTEMA" mediante el uso de las vulnerabilidades del motor de base de datos de Microsoft Jet.
La nueva superficie de ataque es causada por el acceso remoto a la base de datos compatible con Microsoft Jet Database Engine, incluido MS Jet Red (Jet Red Database Engine) y ACE (Access Connectivity Engine). Cuando se usa incorrectamente, la función permite a los atacantes ejecutar consultas SQL en el archivo de base de datos en el servidor controlado por el atacante de forma remota. Una vez que el archivo de base de datos legítimo se reemplaza con un archivo de base de datos con formato incorrecto, la ejecución de consultas SQL en él podría romper la condición previa del código y las suposiciones en Microsoft Jet/ACE, lo que generaría vulnerabilidades en muchos componentes de Jet.
El impacto general y la ruptura de los límites de seguridad de estas vulnerabilidades de Jet dependen de dónde se ejecute la consulta SQL. Los escenarios de ataque típicos son inyección SQL y ad hoc. En estos dos escenarios, los atacantes pueden ejecutar cualquier consulta SQL en las bases de datos con formato incorrecto en IIS y SQL Server.
El acceso remoto a la base de datos permite a los atacantes reemplazar una base de datos legítima con una base de datos mal formada.

Actualización o Mitigación

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

Boletín	2021-366
Asunto	NUEVAS VULNERABILIDADES EN VMWARE
Emisión	9/08/2021
CVE	CVE-2021-22002 y CVE-2021-22003
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• VMware Workspace ONE Access

•VMware Identity Manager (vIDM)

•VMware vRealize Automation (vRA)

•VMware Cloud Foundation

•vRealize Suite Lifecycle Manager

Descripción

La vulnerabilidad CVE-2021-22002 se refiere a un problema con la forma en que VMware Workspace One Access y Identity Manager, permiten acceder a la aplicación web "/cfg" y a los puntos finales de diagnóstico a través del puerto 443. Esto manipulando un encabezado de host personalizado, que da como resultado una solicitud del lado del servidor.

VMware también menciona una vulnerabilidad de divulgación de información que afecta a VMware Workspace One Access y Identity Manager, a través de una interfaz de inicio de sesión expuesta inadvertidamente en el puerto 7443. Un ciberdelincuente con acceso de red por el puerto 7443 podría ser utilizado para realizar un ataque de fuerza bruta.

Actualización o Mitigación

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

Boletín	2021-367
Asunto	NUEVA ACTUALIZACIÓN EN PULSE SECURE
Emisión	9/08/2021
CVE	CVE-2020-8260
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Pulse Connect Secure (PCS) 9.1Rx o versiones anteriores
•Pulse Policy Secure (PPS) 9.1Rx o versiones anteriores
•Pulse Secure Desktop Client (PDC) 9.1Rx o versiones anteriores

Descripción

El dispositivo Pulse Connect Secure sufre una vulnerabilidad de extracción de archivos no controlada que permite a un ciberdelincuente sobrescribir archivos maliciosos, lo que resulta en la ejecución remota de código como root. Un ciberdelincuente con tal acceso podrá eludir cualquier restricción impuesta a través de la aplicación web, así como volver a montar el sistema de archivos, lo que le permitirá crear una puerta trasera persistente, extraer y descifrar credenciales, comprometer clientes VPN o infiltrarse en la red interna.

La vulnerabilidad se debe a una falla en la forma en que los archivos de almacenamiento (.TAR), se extraen en la interfaz web del administrador. Si bien se agregaron más verificaciones para validar el archivo TAR para evitar la explotación de CVE-2020-8260, un análisis adicional de variantes y parches reveló que es posible explotar la misma vulnerabilidad de extracción en la parte del código fuente que maneja las bases de datos del dispositivo del generador de perfiles, obteniendo acceso a pesa de las mitigaciones pasadas implementadas.

La vulnerabilidad CVE-2020-8260 fue una de las cuatro fallas de Pulse Secure que los cibercriminales explotaron activamente a principios de abril, para organizar una serie de intrusiones dirigidas a entidades de defensa, gubernamentales y financieras en los EE. UU. Y más allá en un intento por eludir las protecciones de autenticación de múltiples factores y violar las redes empresariales. Dada la posibilidad de explotación en el mundo real, Pulse Secure recomienda actualizar su dispositivo a la versión Pulse Connect Secure (PCS) 9.1R12 o versiones posteriores.

Actualización o Mitigación

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

Boletín	2021-368
Asunto	SERVIDORES DE MICROSOFT EXCHANGE ANALIZADOS EN BUSCA DE VULNERABILIDAD PROXYSHELL
Emisión	9/08/2021
CVE	CVE-2021-34473, CVE-2021-34523 y CVE-2021-31207
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Servicio de acceso de cliente (CAS) de Microsoft Exchange

Descripción

ProxyShell es un conjunto de tres fallas de seguridad (CVE-2021-34473, CVE-2021-34523 y CVE-2021-31207) que, cuando se usan juntas, podrían permitir a un actor de amenazas realizar una ejecución remota de código (RCE) no autenticada en servidores de Microsoft Exchange sin parches. Estas vulnerabilidades encadenadas se explotan de forma remota a través del Servicio de acceso de cliente (CAS) de Microsoft Exchange que se ejecuta en el puerto 443 de IIS.

Las tres vulnerabilidades encadenadas que se utilizan en los ataques ProxyShell son:

• CVE-2021-34473: La confusión de ruta previa a la autenticación conduce a la derivación de ACL (parcheado en abril por KB5001779)

• CVE-2021-34523: Elevación de privilegios en el backend de Exchange PowerShell (parcheado en abril por KB5001779)

• CVE-2021-31207: Post-auth Arbitrary-File-Write conduce a RCE (parcheado en mayo por KB5003435)

Orange Tsai dio una charla de Black Hat sobre las vulnerabilidades recientes de Microsoft Exchange que descubrió al apuntar a la superficie de ataque del Servicio de acceso de cliente (CAS) de Microsoft Exchange. Como parte de la charla, Tsai explicó que uno de los componentes de la cadena de ataque ProxyShell apunta al servicio de detección automática de Microsoft Exchange.

Microsoft introdujo el servicio Detección automática para proporcionar una manera fácil de que el software de cliente de correo se autoconfigure con una entrada mínima del usuario.

Además, Kevin Beaumont (investigador) detectó que un ciberdeliente que intentaba apuntar a sus servidores de Microsoft Exchange, las cuales había configurado como un Honeypot (sistemas informáticos con vulnerabilidades de seguridad conocidas, que están expuestos en Internet para atraer ciberataques). Beaumont, indicó que, si bien los ataques iniciales no tuvieron éxito, luego observó entradas en el registro contra el servicio de detección automática del servidor, lo que sugiere que los atacantes habían logrado realizar ataques exitosos.

Actualización o Mitigación

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

Boletín	2021-373
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE CISCO
Emisión	11/08/2021
CVE	CVE-2021-1609, CVE-2021-1610 y CVE-2021-1602
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Cisco Small Business RV340, RV340W, RV345 y RV345P Dual WAN Gigabit VPN Routers con firmware anterior a la versión 1.0.03.22
• Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers con firmware anterior a la versión 1.0.01.04

Descripción

Los problemas, registrados como CVE-2021-1609 (puntuación CVSS: 9,8) y CVE-2021-1610 (puntuación CVSS: 7,2), residen en la interfaz de administración basada en web de Small Business RV340, RV340W, RV345 y RV345P Dual Enrutadores WAN Gigabit VPN. La explotación exitosa de CVE-2021-1609 podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el dispositivo o hacer que el dispositivo se recargue, lo que resultaría en una condición DoS. CVE-2021-1610, se refiere a una vulnerabilidad de inyección de comandos que, si se explota, podría permitir que un usuario autenticado ejecute de forma remota comandos arbitrarios con privilegios de root en un dispositivo afectado.

Cisco también aborda un error de ejecución remota de código de alta gravedad (CVE-2021-1602, puntuación CVSS: 8.2) que afecta a los enrutadores VPN RV160, RV160W, RV260, RV260P y RV260W de pequeñas empresas, que podrían ser aprovechados por un atacante remoto no autenticado, para ejecutar comandos arbitrarios en el sistema operativo subyacente de un dispositivo afectado. Esta vulnerabilidad, se debe a una validación insuficiente de la entrada del usuario. Un atacante podría aprovechar esta vulnerabilidad, enviando una solicitud diseñada a la interfaz de administración basada en web. Un exploit exitoso podría permitir al atacante ejecutar comandos arbitrarios en un dispositivo afectado usando privilegios de nivel de root. Debido a la naturaleza de la vulnerabilidad, solo se pueden ejecutar comandos sin parámetros. Hasta el momento no se ha evidenciado una explotación activa para las vulnerabilidades mencionadas.

Actualización o Mitigación

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

Boletín	2021-375
Asunto	MICROSOFT CORRIGE 44 VULNERABILIDADES EN EL PARCHE DE SEGURIDAD DE AGOSTO
Emisión	12/08/2021
CVE	Según Tabla Boletín
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Según Lista Boletín

Descripción

De las 44 vulnerabilidades publicadas por Microsoft, 13 son ejecución remota de código, ocho son divulgación de información, dos son denegación de servicio y cuatro son vulnerabilidades de suplantación.

Microsoft ha publicado actualizaciones de seguridad para dos vulnerabilidades de día cero que se anticiparon con impaciencia y que se descubrieron durante el mes pasado.

Una de las actualizaciones de seguridad corrige las vulnerabilidades de PrintNightmare que permiten a los ciberdelincuentes obtener privilegios conectándose a un servidor de impresión remoto bajo su control. Microsoft ha solucionado esta vulnerabilidad, al requerir que los usuarios tengan privilegios administrativos para instalar controladores de impresora utilizando la función de Windows Point and Print.

Microsoft también corrigió el vector de ataque de retransmisión PetitPotam NTLM, que usa la API MS-EFSRPC para forzar a un dispositivo a negociar con un servidor de retransmisión remoto bajo el control de un atacante. Un ciberdelincuente con pocos privilegios podría usar este ataque para hacerse cargo de un controlador de dominio y, por lo tanto, de todo el dominio de Windows.

El paquete de actualizaciones de agosto incluye tres vulnerabilidades de zero day, de las cuales se explotan activamente. Microsoft clasifica una vulnerabilidad como zero day si se divulga públicamente o se explota activamente sin actualizaciones de seguridad oficiales o se publica. Las dos vulnerabilidades zero day reveladas públicamente, pero no explotadas activamente, son:

- CVE-2021-36936: Verabilidad de suplantación de identidad de LSA de Windows.
- La vulnerabilidad CVE-2021-36942 está asociada con el vector de ataque de retransmisión PetitPotam NTLM que permite la toma de control de los controladores de dominio.

Finalmente, la tercera vulnerabilidad zero day mencionada es rastreada como el CVE-2021-36948.

- CVE-2021-36948: Vulnerabilidad de elevación de privilegios de Windows Update Medic.

Actualización o Mitigación

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

Boletín	2021-376
Asunto	ACTUALIZACIÓN DE SEGURIDAD ADOBE
Emisión	12/08/2021
CVE	Según Tabla Boletín 1 y 2
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Adobe Connect y Magento

Descripción

Adobe ha lanzado una gran actualización de seguridad donde solucionó 29 vulnerabilidades que corrige vulnerabilidades críticas en Magento y errores importantes en Adobe Connect.

Estas vulnerabilidades críticas podrían conducir a la ejecución de código arbitrario, lo que permitiría a los actores de amenazas ejecutar comandos en computadoras vulnerables. De las actualizaciones de seguridad de Adobe, Magento tiene la mayor cantidad de correcciones, con 26 vulnerabilidades, de las cuales, diez son vulnerabilidades de autenticación previa en Magento que pueden explotarse sin iniciar sesión en el sitio. Algunas de estas vulnerabilidades previas a la autenticación son la ejecución remota de código y omisiones de seguridad, lo que permite que un actor de amenazas controle un sitio y su servidor.

Además, Adobe también lanzó una actualización para Adobe Reader que corrige 26 fallas, la mayoría de ellas son Lecturas fuera de límites (OOB), pero también hay algunas Use-After-Free (UAF), OOB Write, agotamiento de pila y corrupción de memoria.

• APSB21-64: Actualizaciones de seguridad disponibles para Magento.

Actualización o Mitigación

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

Boletín	2021-377
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE SAP
Emisión	13/08/2021
CVE	CVE-2021-33690, CVE-2021-33701, CVE-2021-33702, CVE-2021-33703, CVE-2021-33705, CVE-2021-33707 y CVE-2021-33707
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• SAP Business One, SAP NetWeaver y SAP NetWeaver Enterprise Portal

Descripción

SAP ha publicado 19 parches de seguridad nuevos y actualizados, tres de ellos calificados como críticos "HotNews" y seis como de alta prioridad. Dos de los sizzlers de este mes, tienen una puntuación CVSS de 9,9 y afectan a SAP Business One y a la infraestructura de desarrollo de SAP NetWeaver.

El CVE-2021-33698 es un problema de carga de archivos sin restricciones que afecta a SAP Business One, que es el software de gestión empresarial de la compañía alemana para pequeñas y medianas empresas. La vulnerabilidad permite que un atacante cargue archivos, incluidos scripts maliciosos, en el servidor.

SAP describió el segundo error de seguridad crítico, CVE-2021-33690, como una falsificación de solicitud del lado del servidor (SSRF) que afecta a la Infraestructura de desarrollo de NetWeaver (SAP NWDI) en un servlet del Servicio de compilación de componentes. SAP advirtió que la gravedad de la falla depende de si los usuarios están ejecutando NWDI en la intranet o en Internet. Es una mala noticia para quienes lo ejecutan en Internet, enfatizó SAP, dado que podría comprometer por completo los datos confidenciales que residen en el servidor e impactar su disponibilidad.

En lo que respecta a la tercera vulnerabilidad de HotNews, CVE-2021-33701, la falla es una inyección SQL en el servicio SAP NZDT (Near Zero Downtime Technology) utilizado por S/4HANA y el complemento móvil DMIS. Su clasificación de gravedad CVSS es 9.1. La herramienta es utilizada por el servicio NZDT correspondiente de SAP para actualizaciones y conversiones del sistema optimizadas en el tiempo. Cuando se utiliza el servicio NZDT, el mantenimiento se realiza en un clon del sistema de producción. Todos los cambios se registran y se transfieren al clon después de que se completan las tareas de mantenimiento. Durante el tiempo de inactividad final, solo se ejecutan algunas actividades, incluido un cambio de producción al nuevo sistema (clon).

Actualización o Mitigación

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

Amenazas

Boletín	2021-356
Asunto	NUEVO WIPER ES ENCONTRADO EN ARCHIVOS PDF
Emisión	2/08/2021
CVE	No
Categoría	Malware
Severidad	Media

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

El malware esta incrustado en un archivo PDF con supuesto nombre perteneciente a los Juegos Olímpicos, el Wiper no solo elimina datos de un dispositivo infectado, sino que busca ciertos tipos de archivos ubicados en la carpeta personal de Windows del usuario, ubicada en la siguiente ruta "C:/Usuarios/<nombre de usuario>/".

Además, según el equipo de seguridad Mitsui Bussan Secure Directions (MBSD) el Wiper también apunta a archivos creados con el procesador de texto japonés conocido como Ichitaro, lo que aparententa dirigirse a los dispositivos en Japón, donde normalmente se instala la aplicación Ichitaro.

Otras características que se observaron en el malware también incluyen una serie de técnicas de detección de anti-análisis y anti-VM para evitar que el malware sea analizado y probado fácilmente y la capacidad de borrarse a sí mismo una vez que la operación de limpieza haya finalizado.

Actualización o Mitigación

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

Boletín	2021-357
Asunto	NUEVO RANSOMWARE BLACKMATTER
Emisión	2/08/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

- Sistemas Operativos Windows
- Sistemas Operativos Linux

Descripción

Recientemente se observó un nuevo grupo de Ransomware conocido como BlackMatter, el grupo actualmente está reclutando afiliados a través de anuncios publicados en dos foros de ciberdelincuencia llamados Exploit y XSS, con la intención de acceder a redes de empresas que tienen ingresos de $100 millones al año o más y que tienen entre 500 y 15,000 hosts ubicadas en los EE.UU, Reino Unido, Canadá o Australia.

Al igual que la mayoría de las bandas de ransomware, BlackMater también opera un sitio web ubicado en la darkweb, donde tiene la intención de publicar los datos que roban a sus víctimas si la empresa afectada no acepta pagar para descifrar sus archivos. Además, los ciberdelincuentes mencionan en su blog que están interesados en todas las industrias, excepto en el cuidado de la salud y los gobiernos.

El ransomware se proporciona para varias versiones y arquitecturas de sistemas operativos diferentes y se puede entregar en una variedad de formatos, incluida una variante de Windows con compatibilidad con SafeMode (EXE/Reflective DLL/PowerShell) y una variante de Linux con compatibilidad con NAS como Synology, OpenMediaVault, FreeNAS (TrueNAS). Según BlackMatter, la variante de ransomware de Windows se probó con éxito en Windows Server 2003 y Windows 7. La variante de ransomware de Linux se probó con éxito en ESXI, Ubuntu, Debian y CentOs.

Actualización o Mitigación

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

Boletín	2021-360
Asunto	NUEVO RANSOMWARE HARON
Emisión	3/08/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Recientemente se ha observado un nuevo ransomware el cual ha tomado características de los ransomware Avaddon y Thanos, con el objetivo de dirigirse a grandes empresas mediante un código de familias de ransomware más avanzados.

Al igual que la mayoría de ransomware en la actualidad, los ciberdelincuentes de Haron persiguen objetivos empresariales para maximizar sus ganancias y también administran un sitio de filtración donde amenaza con publicar datos robados a empresas que se niegan a pagar por descifrar sus archivos.

A pesar de las similitudes que comparte con otras familias de ransomware, no está claro si los cibercriminales de Haron compraron códigos de Avaddon o si contrataron a uno de sus exmiembros. Sin embargo, los investigadores de seguridad, mencionan que así la banda de Haron hubiera incorporado sistemas basados en la web de Avaddon en sus operaciones, no tenían acceso al código fuente del ransomware Avaddon.

Caracteristidcas del Ransomware Haron:

•Uso de un leaked builder del ransomware Thanos, el cual se encuentra publicado para ser utilizado de manera gratuita, para crear un archivo binario final del ransomware Haron.

•El sitio web o foro donde se les dice a las víctimas que vayan a negociar y paguen el rescate (el "payment site") es casi similar al que manejaba los ciberdelincuentes del ransomware Avaddon.

•La nota de rescate de la banda de Haron contiene grandes porciones de texto copiado y pegado de la nota de rescate que se observaba con el ransomware Avaddon.

•El servidor web de Haron también contenía iconos e imágenes que se encontraban anteriormente en el foro de Avaddon.

•Haron también utiliza una estrategia para inducir negociaciones dentro de ese período estableciendo el tiempo para la próxima actualización de datos, pero aún no hay ningún aviso de ataque DDoS. No se ha confirmado si llevarían a cabo un ataque DDoS como Avaddon.

Actualización o Mitigación

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

Boletín	2021-362
Asunto	NUEVA ACTIVIDAD DEL RANSOMWARE CONTI
Emisión	5/08/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

El payload de Trickbot provino de una campaña de phishing asociada con BazarCall, que distribuye archivos XLSB maliciosos. Tras la ejecución, certutil[.]exe se copia a %programdata% y se renombra con caracteres alfanuméricos aleatorios. Se utilizó Certutil para descargar y cargar la DLL de Trickbot en la memoria. A Trickbot se le asignó automáticamente la tarea de inyectar en el proceso wermgr[.]exe y usar su módulo "pwgrab" para robar las credenciales del navegador. Como parte de otras tareas automatizadas, Trickbot realiza un reconocimiento inicial del entorno utilizando herramientas nativas de Windows como nltest[.]exe y net[.]exe.

Para garantizar la ejecución de Cobalt Strike Beacon en el host, se utilizaron múltiples payloads. Uno de los Cobalt Strike Beacons tenía el mismo payload y la misma infraestructura de comando y control que se usó en un caso anterior. El método de acceso inicial para ese caso fue IcedID.

Una vez que se estableció el acceso a través de Cobalt Strike, los ciberdelincuentes procedieron inmediatamente con la enumeración de dominios a través de Nltest, AdFind, BloodHound y PowerSploit.

Después de la enumeración de dominios, los atacantes realizaron un movimiento lateral hacia dos endpoints en la red. Posteriormente, un cargador PowerShell Cobalt Strike se ejecutó como un servicio en un servidor. Luego, se deshabilitó la supervisión en tiempo real de Windows Defender, el proceso LSASS[.]exe se descargó mediante SysInternals ProcDump y el privilegio se escaló a "SISTEMA" mediante la suplantación de canalización con nombre.

Luego de la ejecución inicial, los ciberdelincuentes pasaron a un controlador de dominio utilizando credenciales de administrador de dominio y ejecutaron un Cobalt Strike Beacon. Una vez que tuvieron acceso al controlador de dominio, se utilizó ntdsutil para tomar un snapshot de "ntds[.]dit", guardado en "C:\Perflogs\1", para la extracción de hash de contraseña sin conexión.

Finalmente, se utilizó Psexec con dos archivos por lotes separados para ejecutar el ransomware Conti en todos los hosts de Windows unidos al dominio.

Actualización o Mitigación

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

Boletín	2021-363
Asunto	NUEVA CAMPAÑA DE PHISHING DIRIGIDA A USUARIOS DE OFFICE 365
Emisión	5/08/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Una campaña de phishing activa utiliza una combinación ingeniosa de direcciones de correo electrónico de remitentes originales de apariencia legítima, direcciones de remitentes de visualización falsificadas que contienen los nombres de usuario y dominios de destino, y nombres de visualización que imitan los servicios legítimos para intentar pasar por los filtros de correo electrónico.

Las direcciones de los remitentes originales contienen variaciones de la palabra" referencia "y utilizan varios dominios de nivel superior, incluido el dominio com[.]com, utilizado popularmente por las campañas de phishing para suplantar y erradicar errores tipográficos.

El grupo de phishing está utilizando Microsoft SharePoint en el nombre y contenido para atraer a las víctimas a hacer clic en el enlace. El correo electrónico se hace pasar por una solicitud de "archivo compartido" para acceder a "Informes del personal", "Bonificaciones", "Libros de precios" y otros contenidos falsos alojados en una supuesta hoja de cálculo de Excel.

Actualización o Mitigación

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

Boletín	2021-364
Asunto	NUEVA ACTIVIDAD DEL RANSOMWARE GRIEF
Emisión	6/08/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

A principios de mayo de 2021, la actividad del ransomware DoppelPaymer se redujo significativamente. Aunque el sitio de filtración de DoppelPaymer aún permanece en línea, no ha habido una nueva publicación de víctimas desde el 6 de mayo de 2021. Además, no se han actualizado publicaciones de víctimas desde finales de junio.

Recientemente se observó que un ransomware se encuentra ofreciéndose en el mercado de la DarkWeb conocido como Grief, al analizar este supuesto nuevo ransomware se observaron varias similutes con el ransomware DoppelPaymer.

Las diferencias de código de malware entre DoppelPaymer y Grief son relativamente mínimas, la nota de rescate que mostraba el ransomware Grief en los sistemas infectados apuntaba al portal DoppelPaymer, en conjunto también se observó que ambos ransomware compartía un código captcha en el sitio de filtración que impide el rastreo automático del sitio y un algoritmo de cifrado que es similar a DoppelPaymer, excepto que la clave RC4 que utiliza Grief aumentó de una longitud de 40 bytes a 48 bytes.

Actualmente, hay más de dos docenas de víctimas enumeradas en el sitio de filtración de Grief, lo que muestra que el grupo de ciberdelincuente se ha mantenido activa propagando su ransomware.

Actualización o Mitigación

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

Boletín	2021-365
Asunto	NUEVA BACKDOOR FATALRAT
Emisión	9/08/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

El malware FatalRAT es un backdoor con un amplio conjunto de capacidades que un ciberdelincuente puede ejecutar de forma remota. El malware ejecuta varias pruebas antes de infectar un dispositivo, verificando la existencia de múltiples productos de máquinas virtuales, espacio en disco y cantidad de procesadores físicos.

Si el dispositivo al cual se dirige FatalRat pasa las pruebas AntiVM, iniciará su ciclo de infección. Primero, descifra cada una de las cadenas de configuración por separado, estas cadenas de configuración incluyen la dirección de comando y control (C&C), el nombre del nuevo archivo de malware, el nombre del servicio y otras configuraciones. Luego FatalRat intentará lograr su persistencia modificando el registro, en donde se creará el registro "Software\ Microsoft\Windows\CurrentVersion\Run\SVP7" para que pueda ejecutarse en el momento del arranque del dispositivo.

Además, como técnica de evasión de defensa, FatalRAT identifica todos los productos de seguridad buscando la existencia de una lista predefinida de productos de seguridad. Luego, el malware espera los comandos remotos del ciberdelincuente, por ejemplo, tiene varias rutinas para manejar diferentes navegadores. Algunas de estas rutinas incluyen la eliminación de información de usuario para navegadores específicos (Edge, 360Secure Browser, QQBrowser, SogouBrowser y Firefox). Para el navegador Chrome, consultará la información del usuario y luego eliminará el contenido, eliminar la información guardada obligará al usuario a ingresar nuevamente el usuario y la contraseña el cual el malware puede capturar con su keylogger.

FatalRat también incluye comandos adicionales, para lo siguiente:

• Keylogger

• Desinstalar UltraViewer

• Descargue e instale AnyDesk

• Ejecutar comandos de shell

• Modificar claves de registro.

Actualización o Mitigación

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

Boletín	2021-369
Asunto	ATAQUE APT UTILIZA DOCUMENTOS PDF RELACIONADOS CON COREA DEL NORTE
Emisión	10/08/2021
CVE	CVE-2020-9715
Categoría	Ataque Cibernético
Severidad	Media

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Para este ataque se usó un archivo del documento PDF como carnada de ataque a través de la vulnerabilidad use-after-free CVE-2020-9715 del programa Adobe Acrobat, la cual ejecuta JavaScript malicioso contenido en documentos PDF y los archivos EXE maliciosos se ejecutan en la memoria del sistema. Esta vulnerabilidad está actualmente parcheada con actualizaciones de seguridad y aquellos que no se hayan actualizado pueden ser atacados.

Se identificaron un total de 7 archivos de documentos PDF maliciosos, de los cuales tres archivos se cree que son de prueba debido a que el JavaScript incluido en su interior y la función que finalmente se ejecuta son programas de calculadora.

El código JavaScript que causa la vulnerabilidad utilizó la API 'this.createDataObject'. Este código contenido en el archivo PDF es una secuencia de comandos ofuscada de manera similar de tamaño de archivo similar. Implementa la función de decodificar la cadena codificada, y la función final es ejecutar el archivo EXE malicioso en la memoria.

El archivo EXE que comienza a partir de un archivo de documento PDF y se ejecuta en la memoria es un archivo creado con Microsoft Visual C ++. Este tiene la función principal de acceder a la dirección C&C externa, descargar el archivo con un nombre de archivo específico y ejecutarlo. Es decir, el propósito es descargar archivos adicionales.

También se identificaron tres archivos DLL maliciosos, los cuales se distribuyeron a través de la ruta del archivo del documento PDF. La función principal del archivo DLL es acceder a la dirección C&C externa, descargar el archivo con un nombre de archivo específico y ejecutarlo.

Actualización o Mitigación

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

Boletín	2021-370
Asunto	SYNOLOGY ADVIERTE SOBRE MALWARE QUE INFECTA LOS DISPOSITIVOS NAS CON RANSOMWARE
Emisión	10/08/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows y Linux

Descripción

PSIRT (Equipo de respuesta a incidentes de seguridad de productos) de Synology, indica que los dispositivos Synology NAS comprometidos en estos ataques se están utilizando posteriormente en nuevos intentos de vulnerar más sistemas Linux y así estos aprovechan varios dispositivos ya infectados para intentar adivinar credenciales administrativas comunes y, si tienen éxito, accederán al sistema para instalar su payload maliciosa, que puede incluir ransomware.

Si bien Synology no compartió más información sobre el malware que se usa en esta campaña, los detalles compartidos se alinean con una fuerza bruta basada en Golang descubierto por Malwarebytes a fines de febrero de 2019 y apodado StealthWorker.

Hace dos años, StealthWorker se utilizó para comprometer sitios web de comercio electrónico al explotar las vulnerabilidades de Magento, phpMyAdmin y cPanel para implementar skimmers diseñados para exfiltrar información personal y de pago. Este malware también tiene capacidades de fuerza bruta que le permiten iniciar sesión en dispositivos expuestos a Internet utilizando contraseñas generadas en el lugar o de listas de credenciales previamente comprometidas.

A partir de marzo de 2019, StealthWorker cambió a un enfoque de solo fuerza bruta para escanear Internet en busca de hosts vulnerables con credenciales débiles o predeterminadas. Una vez implementado en una máquina comprometida, el malware crea tareas programadas tanto en Windows como en Linux para ganar persistencia y, como Synology advirtió, implementa un payload del malware de segunda etapa, incluido el ransomware.

Actualización o Mitigación

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

Boletín	2021-371
Asunto	NUEVOS ATAQUES POR APT DIRIGIDOS HACIA EMPRESAS DE TELECOMUNICACIONES
Emisión	11/08/2021
CVE	No
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

Recientemente se ha observado una nueva familia de malware conocido como MosaicLoader, el cual aparenta ser un software crackeado el cual se propaga a través de anuncios, estos anuncios se encuentran en los resultados de búsqueda con el objetivo de ser ejecutados para luego infectar dispositivos y robar información confidencial.

MosaicLoader es un downloader de malware diseñado por cibercriminales para implementar payloads en su segunda etapa en dispositivos infectados. Los atacantes están camuflando sus droppers como un software ejecutable que aparentan ser un software legítimo, usando íconos similares e incluyendo información como nombres de empresas y descripciones.

Después de ejecutarse en el dispositivo de una víctima, MosaicLoader podría descargar malware como mineros de criptomonedas hasta backdoors de acceso remoto (RAT) mediante una compleja cadena de procesos. El dropper de MosaicLoader descarga un archivo update-assets.zip, desde un servidor C2 que pertenece a los ciberdelincuentes, en la carpeta% TEMP%. El archivo .zip contiene los dos procesos necesarios para la segunda etapa, “appsetup.exe” y “prun.exe”, estos procesos son ubicados por el dropper en la ruta C:\Archivos de programa(x86)\PublicGaming\, para luego emitir en su segunda etapa comandos en Powershell para agregar exclusiones de los archivos maliciosos en Windows Defender. Estos procesos tendrán como objetivo lograr persistencia en el dispositivo infectado para descargar distintos malware con el fin de recopilar información confidencial.

Actualización o Mitigación

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

Boletín	2021-372
Asunto	NUEVA ACTIVIDAD DEL MALWARE RACCOON STEALER
Emisión	11/08/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Raccoon Stealer, cuya mayoría de clientes son novatos o aspirantes a ciberdelincuentes, ahora ofrece servicios listos para usar como robar contraseñas o cookies de autenticación almacenadas dentro de los navegadores web. Al deshacerse de las infecciones tradicionales basadas en el correo electrónico, ahora aprovecha las habilidades de SEO de Google para promover su sitio falso para software crackeado.

El método de infección normalmente comienza con la descarga de un archivo el cual contiene otro que está protegido por una contraseña y un documento de texto que guarda una contraseña que después será usada en la cadena de infección. Después de desempaquetar, el ejecutable de instalación puede omitir fácilmente el escaneo de malware porque está protegido con contraseña. Al abrir el archivo ejecutable, se activa el siguiente paso, recuperando más instaladores autoextraíbles. Después de la infección, el malware adicional entregado a las víctimas incluye cryptominers, clippers, extensiones de navegador maliciosas, bots de fraude de clic de YouTube y Djvu / Stop ransomware.

La reciente actualización de Raccoon Stealer muestra que el panorama de las amenazas cibernéticas ahora se está comercializando. La disponibilidad de herramientas y servicios maliciosos se ha vuelto más fácil que nunca, lo que ha resultado en un aumento drástico de los delitos cibernéticos en todo el mundo.

Actualización o Mitigación

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

Boletín	2021-374
Asunto	NUEVO MALWARE CHAOS
Emisión	11/08/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

El malware Chaos ha experimentado una rápida evolución desde su primera versión hasta su iteración actual, con la versión 1.0 lanzada el 9 de junio, la versión 2.0 el 17 de junio, la versión 3.0 el 5 de julio y la versión 4.0 el 5 de agosto.

Una de las funciones más interesantes de la versión 1.0 del malware de Chaos fue su función worming, que le permitió extenderse a todas las unidades que se encuentran en un sistema infectado. Esto podría permitir que el malware infecte unidades extraíbles y escape a otros sistemas fuera de la red interna. La segunda versión de Chaos agregó opciones avanzadas para realizar un escalamiento de privilegios, la capacidad de eliminar todas las instantáneas de volumen y la capacidad de deshabilitar el modo de recuperación de Windows. Con la versión 3.0, el ciberdelincuente del ransomware Chaos obtuvo la capacidad de cifrar archivos de menos de 1 MB mediante el cifrado AES / RSA, lo que lo hace parecerse con un ransomware. La cuarta versión de Chaos expande el cifrado AES / RSA al aumentar el límite superior de archivos que se pueden cifrar a 2 MB. Además, brinda a los usuarios del generador de ransomware la capacidad de agregar sus propias extensiones a los archivos afectados y la capacidad de cambiar el fondo de escritorio de sus víctimas. La característica más notable que se observó en la primera versión de Chaos es que tenía la marca Ryuk en su GUI, sin embargo, tenía poco en común con el ransomware. De hecho, ni siquiera tenía características de un ransomware, sino se observaron características de un wiper.

Actualmente el malware en lugar de cifrar archivos reemplazó el contenido de los archivos con bytes aleatorios, después de lo cual los archivos se codificaron en Base64. Esto significaba que los archivos afectados ya no podían restaurarse, lo que no ofrecía a las víctimas ningún incentivo para pagar el rescate.

Sin embargo, mostró ciertas características que se encuentran en otras familias de ransomware, infectando rutas conocidas como \\ Contactos, \\Escritorio, \\ Descargas, entre otros.

Luego mostrará una nota de ransomware llamada read_it.txt , con una demanda de un rescate considerable en bitcoin.

Actualización o Mitigación

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

Boletín	2021-378
Asunto	WINDOWS 365 EXPONE CREDENCIALES DE MICROSOFT AZURE
Emisión	13/08/2021
CVE	No
Categoría	Filtración de Datos
Severidad	Crítica

Servicios Afectados

- Microsoft Azure
- Microsoft Windows 365 Cloud PC

Descripción

Mimikatz es un proyecto de ciberseguridad de código abierto que permite probar varias vulnerabilidades de robo de credenciales y suplantación de identidad. Aunque está creado para investigadores, debido a la potencia de sus diversos módulos, los ciberdelincuentes lo utilizan comúnmente para extraer contraseñas en texto plano de la memoria del proceso LSASS o realizar ataques pass-the-hash utilizando hashes NTLM.

Recientemente, Microsoft lanzó su servicio de escritorio basado en la nube de Windows 365, que permite a los usuarios alquilar una PC en la nube y acceder a ellas a través de escritorio remoto o un navegador. Sin embargo, se ha descubierto que el nuevo servicio permite a un programa malicioso extraer la dirección de correo electrónico y las contraseñas en texto plano de Microsoft Azure para los usuarios que han iniciado sesión. Este robo de credenciales es posible debido a una vulnerabilidad que permite extraer las credenciales en texto plano para los usuarios conectados a un Terminal Server.

Si bien las credenciales de Terminal Server de un usuario se cifran cuando se almacenan en la memoria, un atacante podría engañar al proceso de Terminal Service para que las descifre.

Luego de que el ciberdelincuente ingresa a Microsoft Windows 365 Cloud PC y ejecuta Mimikatz con privilegios administrativos, usa el comando “ts::logonpasswords” para extraer las credenciales.

Con estas credenciales, el atacante puede realizar movimientos laterales a través de otros servicios de Microsoft y, potencialmente, de la red interna de una empresa.

Actualización o Mitigación

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

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.