SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Quincenal de Ciberinteligencia Securesoft

Fecha:

9 agosto de 2021

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia

CIB-FOR-2021-015

Índice

1. Objetivo 4

2. Alcance 4

3. Resumen 5

Amenazas analizadas por tipología 5

Indicadores de Compromiso (IoC) 5

Tendencias en nuevas vulnerabilidades 6

Tendencias en actividades maliciosas 6

4. Detalles 7

Vulnerabilidades 7

NUEVA CAMPAÑA DEL ATAQUE DE FUERZA BRUTA DIICOT BRUTE 7

ACTUALIZACIÓN DE SEGURIDAD DE VMWARE 8

NUEVA VULNERABILIDAD EN WINDOWS PRINT SPOOLER 9

ACTUALIZACIÓN DE SEGURIDAD DE DÍA CERO GOOGLE CHROME 10

ACTUALIZACIÓN DE SEGURIDAD D-LINK DIR-3040 11

NUEVA TÉCNICA PARA EXTRAER DATOS 12

NUEVA VULNERABILIDAD EN IMPRESORAS HP, XEROX Y SAMSUNG 13

NUEVAS VULNERABILIDADES 0-DAY EN INTERNET EXPLORER, SAFARI Y CHROME 14

NUEVA ACTUALIZACIÓN DE SEGURIDAD EN CISCO ASA Y FTD 15

NUEVA VULNERABILIDAD EN WINDOWS 16

NUEVAS VULNERABILIDADES EN JUNIPER 17

ACTUALIZACIÓN DE SEGURIDAD FORTINET 18

ACTUALIZACIÓN DE SEGURIDAD DE ORACLE 19

NUEVAS VULNERABILIDADES ENCONTRADAS EN PULSE CONNECT SECURE 20

ACTUALIZACIÓN DE SEGURIDAD DE DELL 21

MITIGACIÓN DE LA VULNERABILIDAD SERIOUSSAM EN WINDOWS 22

ACTUALIZACIONES DE SEGURIDAD DE ESPOCRM, PIMCORE Y AKAUNTING 23

MITIGACIÓN DE MICROSOFT PARA EL ATAQUE PETITPOTAM NTLM 24

ACTUALIZACIÓN DE SEGURIDAD DE ORACLE 25

Amenazas 26

NUEVA ACTIVIDAD DEL MALWARE MATRYOSHKA 26

NUEVA ACTIVIDAD DEL MALWARE HANCITOR 27

HELLOKITTY RANSOMWARE APUNTA A SERVIDORES VMWARE ESXI 28

NUEVA TÉCNICA DE OFUSCACIÓN POR GRUPO MAGECART CODIFICA DATOS ROBADOS DE TARJETA DE CRÉDITO EN MALWARE 29

NUEVA ACTIVIDAD DEL TROYANO TRICKBOT 30
NUEVAS HERRAMIENTAS DE ATAQUE DEL RANSOMWARE MESPINOZA 31
NUEVA ACTIVIDAD DEL GRUPO ZEROX 32
NUEVA ACTIVIDAD DEL RANSOMWARE RANSOMEXX 33
NUEVA CAMPAÑA DE PHISHING POR EL GRUPO DE CIBERDELINCUENTES LUMINOUSMOTH 34
NUEVA MALWARE MOSAICLOADER 35
NUEVA VARIANTE DEL MALWARE FORMBOOK 36
NUEVA MALWARE NPM ROBA CREDENCIALES DE GOOGLE CHROME 37
NUEVA CAMPAÑA DE PHISHING ENVÍA MALWARE MEDIANTE DOCUMENTOS WORD POR CORREO 38
NUEVA ACTIVIDAD DEL MALWARE TAURUS 39
NUEVA CAMPAÑA DEL CRYPTOJACKING LEMONDUCK 40
NUEVA CAMPAÑA DEL GRUPO DE CIBERDELINCUENTES APT31 41
NUEVO RANSOMWARE AVOSLOCKER 42
NUEVA ACTIVIDAD DEL RANSOMWARE LOCKBIT 43
5. Recomendaciones 44

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

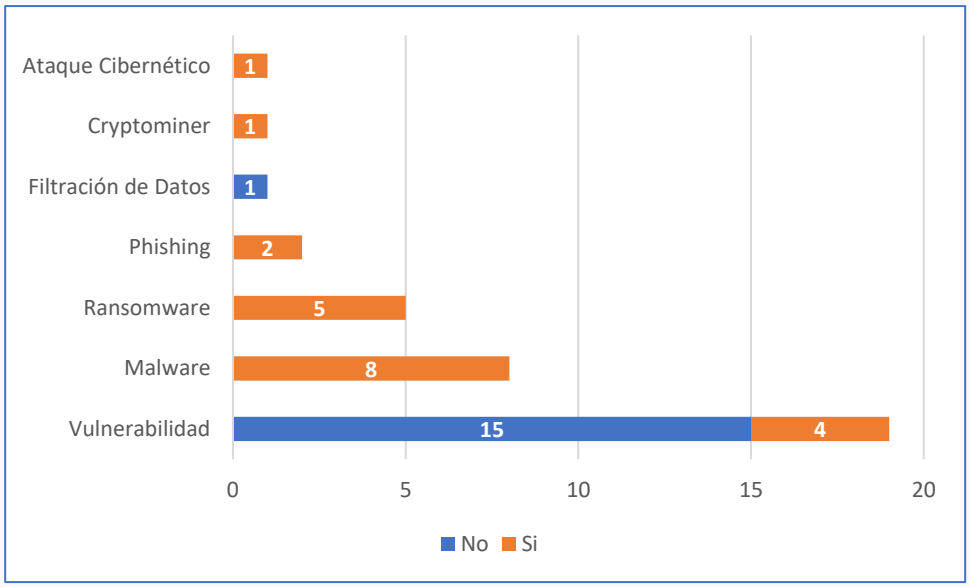
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 16 de julio hasta el 31 de julio del 2021.

3. Resumen

En el presente informe se exponen 37 análisis de vulnerabilidad y amenazas, de las cuales 36 tienen severidad alta y 1 severidad crítica.

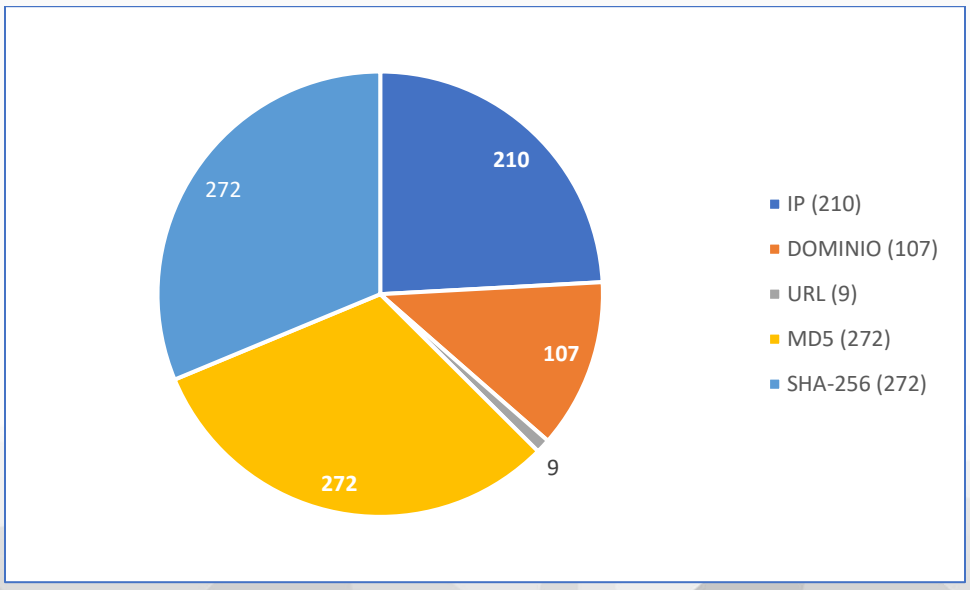
Amenazas analizadas por tipología

En las investigaciones elaboradas para el presente informe se trataron malware, vulnerabilidad, ransomware y phishing. Los que se detallan a continuación, separándolas de acuerdo con si contaban con indicadores de compromiso (IoC) o no.



Indicadores de Compromiso (IoC)

En las investigaciones elaboradas para el presente informe, se han distribuido 870 IoCs entre direcciones IP, Dominios, URL, MD5 y SHA256.



Tendencias en nuevas vulnerabilidades

- Recientemente, se han descubierto cuatro vulnerabilidades de día cero que tienen como objetivo a los navegadores Chrome, Internet Explorer 11 y Safari. Para más información leer el Boletín 2021-335.

- Recientemente se ha observado una vulnerabilidad en el software Cisco Adaptive Security Appliance (ASA) y en el software Cisco Firepower Threat Defense (FTD), el cual podría permitir que un atacante realice un ataque de denegación de servicio (DoS). Para más información leer el Boletín 2021-337.

- Fortinet ha publicado actualizaciones de seguridad para sus soluciones de administración de red FortiManager y FortiAnalyzer, las cuales corrige una vulnerabilidad grave que podría explotarse para ejecutar código arbitrario con los privilegios más altos. Para más información leer el Boletín 2021-342.

- Recientemente la Agencia de Seguridad de Infraestructura y Ciberseguridad de los EE.UU(CISA), hizo una publicación en el cual describía que la herramienta Pulse Connect Secure se encuentran expuestos a archivos malicioso que no son detectados por los productos de antivirus. Para más información leer el Boletín 2021-344.

Tendencias en actividades maliciosas

- Ciberdelincuentes de ransomware HelloKitty están utilizando una variante de Linux de su malware para apuntar a la plataforma de máquina virtual VMware ESXi, para más información leer Boletín 2021-323.

- Recientemente se observó un ataque hacia los sistemas de una empresa en América Latina aparentemente afectada por el ransomware RansomEXX, el cual le obligó a interrumpir con sus operaciones comerciales, portal de pagos y la atención al cliente, para más información leer Boletín 2021-331.

- Recientemente se ha observado una campaña de phishing dirigida por un grupo de ciberdelincuentes conocida como LuminousMoth, el cual tiene el propósito de exfiltrar datos confidenciales mediante archivos maliciosos los cuales son enviados en un formato RAR que se encuentra en correos propagados por LuminousMoth, para más información leer Boletín 2021-333.

- Recientemente se observó que el malware LemonDuck ha venido desarrollándose y mejorando sus técnicas los cuales permitió a los ciberdelincuentes utilizar el malware como herramienta para recaudar información confidencial, eliminar controles de seguridad y propagarse a través de correos electrónicos, para más información leer Boletín 2021-349.

4. Detalles

Vulnerabilidades

Boletín	2021-321
Asunto	NUEVA CAMPAÑA DEL ATAQUE DE FUERZA BRUTA DIICOT BRUTE
Emisión	16/07/2021
CVE	No
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Linux

Descripción

El objetivo de la campaña es principalmente implementar un malware de minería de Monero. Las direcciones IP de las que se originan estos ataques de fuerza bruta pertenecen a un grupo pequeño de atacantes. Esto indica que el malware aún no está utilizando a los sistemas comprometidos para propagarse.

La técnica usada incluye ofuscación con scripts de Bash que se compilan con un compilador de scripts de shell (shc). Además, se ha observado que el ataque utiliza un servidor API centralizado para distribuirse.

Los atacantes proporcionan su clave API en los scripts de esta herramienta que tiene una interfaz que combina el idioma rumano e inglés. Utilizan el escaneo para encontrar credenciales débiles y alojan varios archivos en su servidor incluidos jack[.]tar[.]gz, juanito[.]tar[.]gz, scn[.]tar[.]gz y skamelot[.]tar[.]gz. Estos archivos contienen cadenas de herramientas para descifrar servidores con credenciales SSH débiles, un proceso que incluye estas tres etapas:

- Reconocimiento: identificación de servidores SSH mediante escaneo de puertos y banner grabbing.
- Credenciales de acceso: identificación de credenciales válidas mediante fuerza bruta.
- Acceso inicial: conectarse a través de SSH y ejecutar el payload.

Los ciberdelincuentes utilizaron las herramientas "ps" y "masscan" para el reconocimiento, mientras que "99x / haiduc" y "brute" se usaron para las credenciales de acceso y el acceso inicial. Además, el conjunto de herramientas incluía Diicot Brute, escrita en Go.

Actualización o Mitigación

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

Boletín	2021-322
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE VMWARE
Emisión	16/07/2021
CVE	CVE-2021-21994, CVE-2021-21995 y CVE-2021-22000
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- Sistemas Operativos Windows
- VMware ESXi
- VMware Cloud Foundation
- VMware Thinapp versión 5.x anterior a 5.2.10

Descripción

El más grave de estos problemas es CVE-2021-21994, una falla de autenticación incorrecta en SFCB (Small Footprint CIM Broker) como se usa en ESXi. Con una puntuación CVSS de 7.0, el error se considera importante. Un atacante que tiene acceso de red al puerto 5989 en ESXi puede enviar una solicitud especialmente diseñada para omitir la autenticación SFCB. La vulnerabilidad solo se puede aprovechar si el servicio SFCB está en ejecución. Sin embargo, de forma predeterminada, el servicio no está habilitado.

La vulnerabilidad rastreada como CVE-2021-21995 es un problema de lectura fuera de límites en ESXi OpenSLP que podría conducir a la denegación de servicio (DoS). Con una puntuación CVSS de 5,3, la vulnerabilidad se considera de gravedad moderada. El error podría ser aprovechado por un actor malintencionado que tiene acceso de red al puerto 427 en ESXi para causar una condición DoS.

Registrado como CVE-2021-22000 y con una puntuación CVSS de 6,8, el agujero de seguridad en VMware ThinApp se debe a la carga insegura de archivos DLL. El error de secuestro de DLL podría ser aprovechado por un actor malintencionado con privilegios no administrativos para elevar los privilegios al nivel de administrador en el sistema operativo Windows en el que está instalado ThinApp. VMware ThinApp versión 5.2.10 corrige el error.

Actualización o Mitigación

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

Boletín	2021-325
Asunto	NUEVA VULNERABILIDAD EN WINDOWS PRINT SPOOLER
Emisión	16/07/2021
CVE	CVE-2021-34481
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Servicio de Windows Print Spooler

Descripción

Microsoft advirtió sobre una vulnerabilidad que se ha descubierto en su Windows Print Spooler que puede permitir a los ciberdelincuentes escalar privilegios para obtener credenciales de “admin” en un sistema. El aviso viene inmediatamente después de parchear otros dos errores de ejecución remota de código (RCE) encontrados en el servicio de impresión que se conocieron colectivamente como PrintNightmare.
Esta vulnerabilidad de escalamiento de privilegios de Windows Print Spooler está siendo rastreada como CVE-2021-34481. Los atacantes que explotan con éxito la vulnerabilidad pueden ejecutar código arbitrario con privilegios del sistema, lo que les permite instalar programas, cambiar o eliminar datos o crear nuevas cuentas con privilegios de usuario.

Actualización o Mitigación

• Implementar las soluciones recomendadas por Microsoft en la sección de avisos de seguridad.

Boletín	2021-328
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE DÍA CERO GOOGLE CHROME
Emisión	17/07/2021
CVE	CVE-2021-30559, CVE-2021-30541, CVE-2021-30560, CVE-2021-30561, CVE-2021-30562, CVE-2021-30563 y CVE-2021-30564
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Google Chrome anteriores a la versión 91.0.4472.114

Descripción

Google ha lanzado Chrome 91.0.4472.164 para Windows, Mac y Linux donde corrige siete vulnerabilidades, incluida una vulnerabilidad de día cero de alta gravedad, rastreada como CVE-2021-30563, es un problema de "confusión de tipos" que afecta al motor V8 JavaScript y WebAssembly. Los problemas de confusión de tipos son errores lógicos que resultan de la confusión entre los tipos de objetos, su explotación conduciría a fallas del navegador debido al desbordamiento de búfer, también pueden conducir potencialmente a la ejecución de código arbitrario. Google declaró que existe un exploit para CVE-2021-30563.

No se ha mencionado información sobre los ataques aprovechando la falla ni la naturaleza de los actores de la amenaza. Ninguno de los problemas que solucionó Google con la nueva versión ha sido calificado como crítico.

Actualización o Mitigación

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

Boletín	2021-329
Asunto	ACTUALIZACIÓN DE SEGURIDAD D-LINK DIR-3040
Emisión	17/07/2021
CVE	CVE-2021-21816, CVE-2021-21817, CVE-2021-21818, CVE-2021-21819 y CVE-2021-21820
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Zebra IP Routing Manager D-LINK DIR-3040 versiones anteriores a 1.13B03
• Libcli Test Environment functionality of D-LINK DIR-3040 versiones anteriores 1.13B03

Descripción

Después de una explotación exitosa, los ciberdelincuentes pueden ejecutar código arbitrario en routers sin parches, obtener acceso a información confidencial o bloquearlos después de activar un estado de denegación de servicio. Las fallas de seguridad del DIR-3040 descubiertas e informadas incluyen contraseñas codificadas, inyección de comandos y errores de divulgación de información.

Las vulnerabilidades de contraseñas y credenciales codificadas de forma rígida existen en la funcionalidad Zebra IP Routing Manager y Libcli Test Environment del router los cuales se encuentran rastreados como CVE-2021-21818 y CVE-2021-21820. Ambos permiten a los atacantes eludir el proceso de autenticación configurado por el administrador del software.

El CVE-2021-21819, es una vulnerabilidad crítica de inyección de comandos del sistema operativo que se encuentra en la funcionalidad del entorno de prueba Libcli del router, también puede ser abusada por los adversarios para la ejecución de código.

Se resolvieron los errores encontrados en la versión de firmware 1.13B03. La lista completa de vulnerabilidades abordadas por D-Link son:

• CVE-2021-21816: vulnerabilidad de divulgación de información de Syslog.

• CVE-2021-21817: vulnerabilidad de divulgación de información de Zebra IP Routing Manager.

• CVE-2021-21818: vulnerabilidad de contraseña codificada de Zebra IP Routing Manager.

• CVE-2021-21819: vulnerabilidad de inyección de comando Libcli.

• CVE-2021-21820: vulnerabilidad de contraseña codificada en el entorno de prueba Libcli.

Actualización o Mitigación

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

Boletín	2021-332
Asunto	NUEVA TÉCNICA PARA EXTRAER DATOS
Emisión	19/07/2021
CVE	No
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Los atacantes están usando un tipo específico de malware, agregado a sus herramientas de intrusión, para realizar extracciones de información. Suben un conjunto de archivos desde la computadora de la víctima a los servidores de comando y control que son propiedad de OVH SAS. El malware sigue la extracción de la información con un comando de PowerShell de una sola línea que detiene el proceso de ejecución del malware y luego elimina el archivo que se ejecutó. Además, tiene un tipo de comportamiento anti-análisis llamado "Reubicar código API". También, lee una copia de las DLL del sistema en la memoria y resuelve las importaciones desde allí. Esto causa un problema para los depuradores como x64dbg.

El proceso de extracción de datos comienza enumerando las unidades lógicas que están disponibles en la computadora de la víctima. Para cada una de estas unidades lógicas, se llama a una función que recorre el sistema buscando archivos específicos y extrayéndolos.

A continuación, el tamaño del archivo se determina mediante una llamada a “GetFileSize”. Esta información se incluye en los datos extraídos. A medida que avanza el recorrido del sistema de archivos, las cadenas de ruta se emiten como cadenas de depuración mediante una llamada a “OutputDebugString”. Este malware puede extraer archivos grandes. Para ello, divide el archivo en trozos de acuerdo con un tamaño de trama codificado de forma rígida.

Una vez que se ha completado todo el recorrido del sistema de archivos, la siguiente función llamada envía un archivo ficticio de fin de transmisión al servidor de comando y control. El nombre del archivo es [.]lock y el contenido está bloqueado.

Finalmente, la última acción realizada es ejecutar un comando de PowerShell desde una cadena. Este comando obtiene el ID del proceso padre del propio comando. Utiliza ese ID para eliminar el proceso del malware y luego elimina el archivo de malware del sistema de archivos.

Actualización o Mitigación

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

Boletín	2021-334
Asunto	NUEVA VULNERABILIDAD EN IMPRESORAS HP, XEROX Y SAMSUNG
Emisión	20/07/2021
CVE	CVE-2021-3438
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

La falla de seguridad, rastreada como CVE-2021-3438, es un desbordamiento de búfer en el controlador SSPORT[.]SYS para modelos de impresora específicos que podría conducir a un escalamiento local de privilegios de usuario.

El controlador con errores se instala automáticamente con el software de la impresora y Windows lo cargará después de cada reinicio del sistema. Esto lo convierte en el objetivo perfecto para los atacantes que necesitan una forma fácil de escalar privilegios, ya que se puede usar la vulnerabilidad incluso cuando la impresora no está conectada al dispositivo de la víctima.

Para que la explotación sea exitosa, se requiere el acceso de los usuarios locales. Una vez logrado esto, los atacantes pueden usar esta vulnerabilidad para escalar privilegios en ataques de baja complejidad sin requerir la interacción del usuario.

El resultado es que los ciberdelincuentes con privilegios de usuario básicos pueden elevar sus privilegios a SYSTEM y ejecutar código en modo kernel. De esta manera, podrían instalar programas, ver, cambiar, cifrar o eliminar datos y crear nuevas cuentas con derechos completos de usuario.

Actualización o Mitigación

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

Boletín	2021-335
Asunto	NUEVAS VULNERABILIDADES 0-DAY EN INTERNET EXPLORER, SAFARI Y CHROME
Emisión	20/07/2021
CVE	CVE-2021-1879, CVE-2021-21166, CVE-2021-30551 y CVE-2021-33742
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- Sistemas Operativos Windows
- Sistema Operativo iOS 12.4-13.7
- Google Chrome
- Internet Explorer 11
- Safari

Descripción

Las vulnerabilidades CVE-2021-21166 y CVE-2021-30551, utilizadas en Google Chrome, son usadas para ejecutar código arbitrario de forma remota. Los atacantes envían un enlace especialmente diseñado a la víctima objetivo. El enlace lleva a un dominio bajo el control del atacante que imita a un sitio legítimo. Cuando la víctima visita el enlace, es redirigida a otra página que recolecta la información necesaria sobre el dispositivo y ejecuta el exploit.

La vulnerabilidad CVE-2021-33742 apunta a usuarios de Internet Explorer 11. El proceso es similar al de los exploits para Chrome. Tras una fase de reconocimiento, se carga el exploit que, en caso de ser fructífero, permitiría al atacante ejecutar código arbitrario en el dispositivo de la víctima.

Finalmente, los atacantes utilizan la vulnerabilidad CVE-2021-1879 con mensajes de LinkedIn a través de los cuales envían los enlaces maliciosos a objetivos concretos. Cuando la víctima visita el enlace desde un dispositivo iOS 12.4-13.7, el exploit intentará extraer información sobre cookies de sesión y páginas web abiertas en el navegador Safari del dispositivo.

Actualización o Mitigación

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

Boletín	2021-337
Asunto	NUEVA ACTUALIZACIÓN DE SEGURIDAD EN CISCO ASA Y FTD
Emisión	21/07/2021
CVE	CVE-2021-1422
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- Cisco Adaptive Security Appliance 9.16.1.
- Cisco Firepower Threat Defense 7.0.0.
- Cisco Firepower 2100 Series.
- Cisco Firepower NGFW Virtual.
- Cisco Adaptive Security Virtual Appliance

Descripción

Recientemente se ha observado una vulnerabilidad en el software Cisco Adaptive Security Appliance (ASA) y en el software Cisco Firepower Threat Defense (FTD), el cual podría permitir que un atacante realice un ataque de denegación de servicio (DoS).

La vulnerabilidad CVE-2021-1422 se debe a un "logic error" encontrada en productos de Cisco en el software cryptography module de Cisco ASA que maneja errores de descifrado. Un atacante podría aprovechar esta vulnerabilidad enviando paquetes maliciosos a través de una conexión IPsec establecida.

Un exploit exitoso podría hacer que el dispositivo se bloquee y obligarlo a fallar con el objetivo de provocar un ataque de denegación de servicios (DoS). Sin embargo, en la publicación realizada por Cisco indican que la explotación exitosa de esta vulnerabilidad no comprometerá ningún dato confidencial. Adicionalmente Cisco ha publicado nuevas actualizaciones en sus productos con sus respectivos parches de seguridad para cubrir esta vulnerabilidad.

Actualización o Mitigación

- Implementar la actualización recomendadas por Cisco en la sección de avisos de seguridad.

Boletín	2021-338
Asunto	NUEVA VULNERABILIDAD EN WINDOWS
Emisión	21/07/2021
CVE	CVE-2021-36934
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Sistema Operativo Windows 10

• Sistema Operativo Windows 11

Descripción

Esta vulnerabilidad de elevación local de privilegios permite que los usuarios con privilegios limitados puedan acceder a archivos confidenciales de la base de datos del registro.
El registro de Windows actúa como un repositorio de configuración para el sistema operativo y contiene contraseñas cifradas, personalizaciones de usuario, opciones de configuración para aplicaciones, claves de descifrado del sistema y más.
Los archivos de la base de datos asociados con el registro de Windows se almacenan en la carpeta "C:\Windows\system32\config" y se dividen en diferentes archivos: SYSTEM, SECURITY, SAM, DEFAULT y SOFTWARE.
Dado que estos archivos contienen información confidencial sobre todas las cuentas de usuario en un dispositivo y los tokens de seguridad utilizados por las funciones de Windows, deben estar restringidos para que los usuarios normales sin privilegios elevados no los vean.
Un ciberdelincuente con privilegios limitados en un dispositivo puede extraer los hashes de las contraseñas NTLM de todas las cuentas y usarlos en ataques pass-the-hash para obtener privilegios elevados.
Como los archivos del registro, como SAM, están siempre en uso por el sistema operativo, cuando intente acceder recibirá una advertencia de acceso ya que los archivos están abiertos y bloqueados por otro programa. Sin embargo, como los archivos de registro, incluido el SAM, suelen estar respaldados por snapshots, se puede acceder sin recibir una advertencia de acceso.

Actualización o Mitigación

• Restringir el acceso al contenido de "%windir%\system32\config". Para lograrlo, abra el símbolo del sistema o Windows PowerShell como administrador y ejecute el comando "icacls %windir%\system32\config*.* /inheritance:e".

Boletín	2021-339
Asunto	NUEVAS VULNERABILIDADES EN JUNIPER
Emisión	22/07/2021
CVE	CVE-2021-0276 y CVE-2021-0277
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Juniper Networks SBR Carrier 8.4.1

• Juniper Networks SBR Carrier 8.5.0

• Juniper Networks SBR Carrier 8.6.0

• Sistemas Operativos Junos

• Sistema Operativo Junos Evolved

Descripción

Los operadores de telecomunicaciones utilizan el servidor SBR Carrier para administrar las políticas sobre cómo los suscriptores acceden a sus redes, centralizando la autenticación del usuario, brindando el nivel adecuado de acceso y asegurando el cumplimiento de las políticas de seguridad.

La vulnerabilidad, registrada como CVE-2021-0276, afecta a las versiones 8.4.1, 8.5.0 y 8.6.0 de SBR Carrier que utilizan el protocolo de autenticación extensible. Además, se ha observado que es una vulnerabilidad de desbordamiento de búfer que un atacante puede explotar enviando paquetes especialmente diseñados a la plataforma, lo que hace que RADIUS se bloquee. Con esto, los ciberdelincuentes pueden ejecutar código de manera remota o usar ataques de denegación de servicio (DoS) que evitaría que los suscriptores tengan una conexión de red.

También se ha descubierto una vulnerabilidad (CVE-2021-0277) de lectura fuera de los límites que afecta al sistema operativo Junos y Junos OS Evolved. El problema existe en el procesamiento de tramas LLDP especialmente diseñadas por protocolo de control de capa 2 (l2cpd). La recepción y el procesamiento continuos de estas tramas, enviadas desde el dominio de transmisión local, bloqueará repetidamente el proceso l2cpd y mantendrá la condición DoS.

Actualización o Mitigación

• Considerar la configuración del dispositivo para que no permita el protocolo l2cpd.

Boletín	2021-342
Asunto	ACTUALIZACIÓN DE SEGURIDAD FORTINET
Emisión	24/07/2021
CVE	CVE-2021-32589
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• FortiManager y FortiAnalyzer

Descripción

La vulnerabilidad CVE-2021-32589, es de uso después de la liberación (UAF) en FortiManager y FortiAnalyzer fgfmsd daemon. Este tipo de error ocurre cuando una sección de la memoria se marca erróneamente como libre y luego un programa intenta usarla, lo que resulta en un bloqueo.

Además, Fortinet incida que enviar una solicitud especialmente diseñada al puerto "FGFM" de un dispositivo de destino puede permitir que un atacante remoto no autenticado ejecute código no autorizado como root.

Por lo cual, Fortinet está deshabilitado FGFM de forma predeterminada en FortiAnalyzer y solo se puede activar en algunos modelos de hardware: 1000D, 1000E, 2000E, 3000D, 3000E, 3000F, 3500E, 3500F, 3700F, 3900E.

Los productos afectados por CVE-2021-32589 son los siguientes:

FortiManager	FortiAnalyzer
versiones 5.6.10 y anteriores	versiones 5.6.10 y anteriores
versiones 6.0.10 y anteriores	versiones 6.0.10 y anteriores
versiones 6.2.7 y anteriores	versiones 6.2.7 y anteriores
versiones 6.4.5 y anteriores	versiones 6.4.5 y anteriores
versión 7.0.0	versión 7.0.0
versiones 5.4.x	

Tabla 1: Versiones afectadas por la vulnerabilidad

Actualización o Mitigación

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

Boletín	2021-343
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE ORACLE
Emisión	24/07/2021
CVE	CVE-2019-2729, CVE-2021-2376, CVE-2021-2378, CVE-2021-2382, CVE-2021-2394, CVE-2021-2397 y CVE-2021-2403
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Oracle WebLogic Server versión 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 y 14.1.1.0.0

Descripción

Recientemente, Oracle ha publicado actualizaciones de seguridad para corregir varias vulnerabilidades que podrían ser explotadas por un atacante para tomar el control del sistema afectado.

La principal vulnerabilidad corregida es CVE-2019-2729, una vulnerabilidad de deserialización crítica a través de XMLDecoder en los servicios web de Oracle WebLogic Server que se puede explotar de forma remota sin autenticación.

La falla afecta a las versiones 11.1.2.4 y 11.2.5.0 de WebLogic Server y existe dentro de la tecnología de infraestructura Oracle Hyperion.

Otras vulnerabilidades corregidas en esta actualización fueron registradas como CVE-2021-2376, CVE-2021-2378, CVE-2021-2382, CVE-2021-2394, CVE-2021-2397 y CVE-2021-2403. Permiten que un atacante no autenticado con acceso a la red a través de T3 o IIOP vulnere el servidor Oracle WebLogic.

Si los ataques son exitosos, los ciberdelincuentes podrían tener el control total o provocar un bloqueo del servidor Oracle WebLogic.

Actualización o Mitigación

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

Boletín	2021-344
Asunto	NUEVAS VULNERABILIDADES ENCONTRADAS EN PULSE CONNECT SECURE
Emisión	26/07/2021
CVE	CVE-2019-11510, CVE-2020-8260, CVE-2020-8243 y CVE-2021-2289
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Pulse Connect Secure.

Descripción

Recientemente la Agencia de Seguridad de Infraestructura y Ciberseguridad de los EE.UU(CISA), hizo una publicación en el cual describía que la herramienta Pulse Connect Secure se encuentran expuestos a archivos malicioso que no son detectados por los productos de antivirus.

Recientemente CISA publicó informes con análisis de diferentes archivos que involucran la herramienta PulseConnect Secure, algunas de ellas compuestas por varios archivos.

Algunos de los archivos anteriores se han modificado con fines maliciosos en incidentes a principios de este año investigados por el equipo de seguridad Mandiant. En abril se señaló que el presunto ciberdelincuente había aprovechado la vulnerabilidad rastreada como CVE-2021-22893 para la entrada inicial con el propósito de comprometer la herramienta Pulse Secure, para mayor información revisar el Boletín 2021-231.

Todos los archivos que analizó CISA se encontraron en la herramienta Pulse Connect Secure y algunos de ellos eran versiones modificadas de scripts en el software legítimo Pulse Secure. En la mayoría de los casos, los archivos maliciosos eran webshells para activar y ejecutar comandos remotos para lograr una persistencia y lograr accesos remotos.

Así mismo indicar que la mayoría de los archivos que CISA encontró en Pulse Secure no son detectados por las soluciones antivirus; y solo uno de ellos estaba presente en la plataforma de escaneo de archivos VirusTotal.

Actualización o Mitigación

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

Boletín	2021-346
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE DELL
Emisión	26/07/2021
CVE	CVE-2021-21564, CVE-2021-21585 y CVE-2021-21596
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Dell OpenManage Enterprise

Descripción

Recientemente, DELL ha publicado actualizaciones de seguridad para corregir múltiples vulnerabilidades en su producto OpenManage Enterprise.

Dell OpenManage Enterprise es una aplicación de supervisión y administración de sistemas. Proporciona a los administradores una vista completa de los servidores, conmutadores de red y almacenamiento de Dell EMC en su entorno.

La vulnerabilidad más grave fue registrada como CVE-2021-21564, un error de autenticación incorrecta que podría permitir a un atacante secuestrar una sesión o realizar acciones no autorizadas enviando datos con formato incorrecto. La explotación de la vulnerabilidad no requiere autenticación.

Otra vulnerabilidad que Dell corrigió en OpenManage Enterprise es CVE-2021-21585, un error de inyección de comandos del sistema operativo en las herramientas RACADM e IPMI que podrían permitir que un ciberdelincuente que ya tiene altos privilegios ejecute comandos arbitrarios del sistema operativo.

Un tercer defecto parcheado en Dell OpenManage Enterprise es CVE-2021-21596, un problema de ejecución remota de código que podría permitir que un atacante que tiene acceso a la subred inmediata acceda a información confidencial y potencialmente eleve privilegios.

Actualización o Mitigación

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

Boletín	2021-348
Asunto	MITIGACIÓN DE LA VULNERABILIDAD SERIOUSSAM EN WINDOWS
Emisión	26/07/2021
CVE	CVE-2021-36934
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows 10
- Sistema Operativo Windows 11

Descripción

Recientemente, se han publicado algunas recomendaciones para mitigar la vulnerabilidad SeriousSAM en Windows 10 y 11.

La vulnerabilidad SeriousSAM permite a los atacantes con permisos de bajo nivel, acceder a los archivos del sistema de Windows para realizar ataques Pass-the-Hash y, potencialmente, ataques Silver Ticket.

Los ciberdelincuentes pueden aprovechar esta vulnerabilidad para obtener hashes de contraseñas almacenadas en el Administrador de Cuentas de Seguridad (SAM) y en el Registro y, en última instancia, ejecutar código arbitrario con privilegios de sistema.

Esta vulnerabilidad fue registrada como CVE-2021-36934 y existe en la configuración predeterminada de Windows 10 y Windows 11, específicamente debido a una configuración que otorga permisos de lectura para el grupo de usuarios que contiene a todos los usuarios locales.

Como resultado, los usuarios locales integrados tienen acceso para leer los archivos SAM y el Registro, donde también pueden ver los hashes. Una vez que el atacante tiene acceso de “Usuario”, puede usar una herramienta como Mimikatz para obtener acceso al Registro o SAM, robar los hashes y convertirlos en contraseñas. Invadir a los usuarios del dominio de esa manera les dará a los ciberdelincuentes privilegios elevados en la red.

Debido a que todavía no hay un parche oficial disponible de Microsoft, la mejor manera de proteger su entorno de la vulnerabilidad SeriousSAM es implementar medidas de refuerzo que se detallan en las recomendaciones.

Actualización o Mitigación

- No permitir el almacenamiento de contraseñas y credenciales para la autenticación de red. Al implementar esta regla, no habrá hash almacenado en el SAM o el Registro, mitigando así esta vulnerabilidad por completo.

Boletín	2021-352
Asunto	ACTUALIZACIONES DE SEGURIDAD DE ESPOCRM, PIMCORE Y AKAUNTING
Emisión	30/07/2021
CVE	CVE-2021-3539, CVE-2021-31867, CVE-2021-31869, CVE-2021-36800, CVE-2021-36801, CVE-2021-36802, CVE-2021-36803, CVE-2021-36804 y CVE-2021-36805
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- EspoCRM v6.1.6
- Pimcore Customer Data Framework v3.0.0
- Pimcore AdminBundle v6.8.0
- Akaunting v2.1.12

Descripción

Recientemente, se han publicado actualizaciones de seguridad para corregir varias vulnerabilidades en EspoCRM, Pimcore y Akauting.
EspoCRM es una aplicación de gestión de relaciones con el cliente (CRM) de código abierto, mientras que Pimcore es una plataforma de software empresarial de código abierto para la gestión de datos de clientes, gestión de activos digitales, gestión de contenido y comercio digital. Akaunting, por otro lado, es un software de contabilidad en línea y de código abierto diseñado para el seguimiento de facturas y gastos.
La vulnerabilidad registrada como CVE-2021-3539 permite que cualquier usuario con privilegios predeterminados que cargue su propio avatar, pueda abusar de la API proporcionando un código Javascript ejecutable en lugar de una imagen. Debido a que EspoCRM permite a los administradores instalar extensiones arbitrarias personalizadas, un atacante puede aprovechar este XSS para obligar silenciosamente a un administrador (que ve el avatar del atacante) a instalar una extensión maliciosa, manteniendo así el control permanente de la aplicación web.
Otras vulnerabilidades corregidas fueron registradas como CVE-2021-31867 y CVE-2021-31869. Se tratan de vulnerabilidades de inyección de código SQL en el paquete de marco de gestión de clientes de Pimcore Customer Data Framework, específicamente en el componente SegmentAssignmentController[.]php. El campo “$id” se recupera de los parámetros de solicitud, luego se coloca directamente en la consulta SQL mediante el uso de “sprintf” y después se ejecuta. Esto permite que un ciberdelincuente inyecte la consulta SQL mediante el uso de una comilla simple.

Actualización o Mitigación

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

Boletín	2021-353
Asunto	MITIGACIÓN DE MICROSOFT PARA EL ATAQUE PETITPOTAM NTLM
Emisión	30/07/2021
CVE	No
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows Server

Descripción

Recientemente, Microsoft ha publicado algunas recomendaciones para mitigar el ataque PetitPotam NTLM.

PetitPotam es un nuevo método que se puede utilizar para realizar un ataque de retransmisión NTLM. Este método se dio a conocer recientemente junto con un script de prueba de concepto (PoC).

El nuevo ataque utiliza el protocolo remoto del sistema de cifrado de archivos de Microsoft (EFSRPC) para obligar a un dispositivo, incluidos los controladores de dominio, a autenticarse en una retransmisión NTLM remota controlada por un atacante.

Una vez que un dispositivo se autentica en un servidor NTLM malintencionado, un ciberdelincuente puede robar hashes y certificados que pueden usarse para asumir la identidad del dispositivo y sus privilegios.

Actualización o Mitigación

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

Boletín	2021-354
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE ORACLE
Emisión	31/07/2021
CVE	Según Tabla Boletín
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Según Lista Boletín

Descripción

Oracle anunció la disponibilidad de un total de 342 nuevos parches de seguridad como parte de su Actualización de parches críticos (CPU) de julio de 2021. Más de la mitad de las vulnerabilidades abordadas podrían explotarse de forma remota sin autenticación.

Aproximadamente 50 se consideran de gravedad crítica, y una de ellas presenta una puntuación CVSS de 10. El más grave de estos problemas es CVE-2021-2244, un error de seguridad en el producto Essbase Analytic Provider Services de Oracle Essbase (JAPI) que podría explotarse de forma remota sin autenticación y que podría conducir a la adquisición completa del producto afectado.

La vulnerabilidad fácilmente explotable permite que un atacante no autenticado con acceso a la red a través de HTTP comprometa los servicios de proveedores analíticos de Essbase. Si bien la vulnerabilidad se encuentra en Essbase Analytic Provider Services, los ataques pueden afectar significativamente a productos adicionales.

Otras aplicaciones de Oracle que han recibido parches este mes incluyen PeopleSoft, Systems Risk, Commerce, Construction and Engineering, Essbase, JD Edwards, Enterprise Manager, Java SE, Hyperion y Virtualization, entre otras.

Oracle insta a los clientes a que apliquen los parches disponibles lo antes posible, ya que esto reduciría significativamente la amenaza que representan los ataques exitosos. El gigante tecnológico también señala que recibe periódicamente informes de ataques maliciosos a vulnerabilidades para las que se lanzaron parches de seguridad en el pasado.

Actualización o Mitigación

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

Amenazas

Boletín	2021-319
Asunto	NUEVA ACTIVIDAD DEL MALWARE MATRYOSHKA
Emisión	16/07/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

Matryoshka es una variante del malware ROKRAT que permite a los atacantes robar información de las víctimas y enviarla a un servicio en la nube. Este ataque está relacionado al grupo de ciberdelincuentes norcoreanos Scarcruft (también conocido como APT37).
El nombre del directorio y el nombre de los archivos maliciosos descargados se disfrazan con nombres de controladores aparentemente legítimos como ReadyBoost Driver, Microsoft Filesystem Filter Manager, Link-Layer Topology Responder Driver para NDIS 6, etc. Además, se asigna la ruta de descarga por defecto "%PROGRAMDATA%". Luego, se ejecuta el script de Ruby a través del archivo Link-Layer Topology Responder Driver for NDIS 6[.]ini en la ruta "%APPDATA%\Local\Microsoft\Ruby27-x64".
Posteriormente, se decodifica el archivo PE mediante la rutina de decodificación XOR y se ejecuta en la memoria.
Después de decodificar, se hace un llamado a las librerías y se verifica el antivirus registrado en el Centro de Seguridad de Windows a través de la consulta WMI.
Los ciberdelincuentes han utilizado pCloud, Yandex, Dropbox y Backblaze como servicios en la nube.

Actualización o Mitigación

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

Boletín	2021-320
Asunto	NUEVA ACTIVIDAD DEL MALWARE HANCITOR
Emisión	16/07/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Una nueva técnica de los actores detrás de Hancitor evita que los rastreadores accedan a los documentos maliciosos utilizados para descargar el payload de Hancitor.

El ataque comienza cuando el objetivo recibe un correo electrónico con una plantilla de DocuSign falsa que parece tener un enlace o feedproxy[.]Google[.]Com, un servicio que permite a los usuarios publicar actualizaciones de sitios web.

Sin embargo, el enlace en realidad dirige a un sitio malicioso, que verifica el User-Agent del navegador. Si no es Windows, la víctima es redirigida a google[.]Com.

Sin embargo, si la víctima está usando una máquina con Windows, el sitio malicioso crea una cookie usando JavaScript y vuelve a cargar el sitio. Se utiliza un código para crear la cookie.

El código escribe la zona horaria en el valor 'n' y el desplazamiento de tiempo en UTC en el valor 'd'. El encabezado de la cookie está configurado para HTTP a GET Request. Los valores de 'n' y 'd' cambian según la zona horaria .

Actualización o Mitigación

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

Boletín	2021-323
Asunto	HELLOKITTY RANSOMWARE APUNTA A SERVIDORES VMWARE ESXI
Emisión	16/07/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• VMware ESXi
• Linux ELF64

Descripción

La banda de ransomware tiene como objetivo expandir las operaciones dirigidas a empresas que están adoptando en gran medida plataformas de virtualización. Dirigiéndose a los sistemas VMware ESXi, los ciberdelincuentes podrían cifrar tantas máquinas virtuales como fuera posible con un impacto significativo en las víctimas.

Recientemente se detectaron múltiples versiones ELF64 de Linux del ransomware HelloKitty diseñadas para apuntar a servidores VMware ESXi y cifrar las máquinas virtuales alojadas en ellos. Se analizó muestras de la nueva variante y confirmó que el malware intenta apagar las máquinas virtuales que se ejecutan en los servidores de destino para cifrar los archivos, evitando que los archivos se bloqueen.

Una vez que se apagan las máquinas virtuales, el ransomware cifrará los archivos .vmdk (disco duro virtual), .vmsd (metadatos e información de instantáneas) y .vmsn (contiene el estado activo de la máquina virtual). El ransomware HelloKitty no es la única amenaza que se dirige a los servidores ESXi, Babuk, RansomExx, Mespinoza y DarkSide ransomware también implementan esta capacidad.

Actualización o Mitigación

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

Boletín	2021-324
Asunto	NUEVA TÉCNICA DE OFUSCACIÓN POR GRUPO MAGECART CODIFICA DATOS ROBADOS DE TARJETA DE CRÉDITO EN MALWARE
Emisión	16/07/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Magecart está dirigido a sitios web de comercio electrónico con el objetivo de extraer los números de tarjetas de crédito mediante la inyección de skimmers javascript maliciosos y venderlos en el mercado negro.

El ataque al Grupo Magecart basándose en superposiciones en las tácticas, técnicas y procedimientos (TTP) adoptados por el ciberdelincuente. Donde, la táctica que emplean algunos ciberdelincuentes de Magecart es el volcado de los detalles de la tarjeta de crédito en archivos de imagen en el servidor para evitar levantar sospechas. Estos se pueden descargar más adelante utilizando una simple solicitud GET en una fecha posterior.

En un caso de una infección de sitio web de comercio electrónico, se encontró que el skimmer se insertó en uno de los archivos PHP involucrados en el proceso de pago en forma de una cadena comprimida codificada en Base64.

Para enmascarar aún más la presencia de código malicioso en el archivo PHP, los ciberdelincuentes han utilizado una técnica llamada concatenación en la que el código se combinó con fragmentos de comentario adicionales que no hacen nada funcionalmente, pero agrega una capa de ofuscación que lo hace algo más difícil de detectar.

En última instancia, el objetivo de los ciberdelincuentes es capturar los detalles de la tarjeta de pago de los clientes en tiempo real en el sitio web comprometido, que luego se guardan en un archivo de hoja de estilo falso (.CSS) en el servidor y descargado posteriormente en el extremo del actor de amenaza mediante la realización de una solicitud GET.

Actualización o Mitigación

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

Boletín	2021-326
Asunto	NUEVA ACTIVIDAD DEL TROYANO TRICKBOT
Emisión	17/07/2021
CVE	CVE-2017-0199
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Esta campaña distribuye archivos DOCX que aprovechan la vulnerabilidad registrada como CVE-2017-0199 que aprovecha un enlace integrado que ejecuta inmediatamente un payload, sin pasar por los controles de seguridad normales. Este nuevo archivo incluye un script VBS que descargará el ejecutable final.

Principalmente, fueron afectados por esta campaña los clientes que utilizan Microsoft Office 365. Ambas URL de infección hacen referencia a Microsoft 365: “micrsoft365[.]live” y “mcsoft365[.]club”.

La plantilla del correo electrónico utilizada en esta campaña hace referencia a un formulario W9 en el asunto, pero el documento de Word se llama "factura". También da un número aleatorio en el asunto como un número de cotización y concluye con una firma relacionada con el propietario del correo electrónico comprometido.

Como Microsoft ha exigido que los usuarios de macros de Office habiliten la edición, este documento malicioso va a engañar e intentar guiar al usuario victima paso a paso para deshabilitar la protección de macros. Durante la vista previa, el usuario verá un acuerdo financiero de apariencia legítima y no las plantillas habituales que generan señales de alerta.

La macro de Office creará la carpeta "\Documents\Adobe Help Center" y copiará un script de VBS en ella. La secuencia de comandos VBS se iniciará utilizando Wscript[.]exe. La mayoría de las infecciones de macro de Office comienzan con la función Auto_Open (), pero en este ataque se utiliza una función que se ejecuta cuando se cierra el documento. Cuando eso ocurre, lanza una shell de WScript con código VBS.

La macro también empieza a copiar el código VBS a un nuevo archivo de texto. Dentro de este archivo, hay una función y filas de valores codificados que luego son decodificados por WScript mientras se ejecuta. Al analizar el código en la memoria, se observa el payload utilizado para obtener el ejecutable final. A continuación, se ejecutan varias comprobaciones para herramientas de análisis como Wireshark, Process Explorer y TCPdump. Finalmente, WScript lanzará el ejecutable.

Actualización o Mitigación

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

Boletín	2021-327
Asunto	NUEVAS HERRAMIENTAS DE ATAQUE DEL RANSOMWARE MESPINOZA
Emisión	17/07/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Mespinoza ha robado con éxito datos importantes como pasaportes, facturas de alquiler, datos de tripulación e información de inteligencia sobre la comunidad de seguridad. Además, los datos robados en los ataques exitosos se han filtrado en los sitios web públicos.

Las herramientas Gasket y MagicSocks, así como los datos extraídos en el sitio filtrado, se remontan a abril de 2020, lo que sugiere que la banda de ransomware Mespinoza ha estado activa durante más de un año. Si bien hay informes que sugieren que la banda de ransomware de Mespinoza ha adoptado un modelo de ransomware como servicio (RaaS), no se ha observado este comportamiento del grupo basado en los casos detectados del ransomware.

A diferencia de otros ransomware, Mespinoza no elimina las instantáneas antes del cifrado, lo que significa que las copias de seguridad proporcionarán una contramedida viable para remediar el ataque.

Los desarrolladores de Gasket escribieron esta puerta trasera en Golang y usaron la herramienta Gobfuscate de código abierto para ofuscar el payload. Los actores utilizan esta puerta trasera como respaldo de RDP para mantener el acceso a la red. Gasket analiza los argumentos de la línea de comando que se le pasan para determinar si debe ejecutarse como un proceso independiente, instalarse como un servicio o para controlar un servicio Gasket instalado previamente.

La herramienta Gasket hacía referencia a una capacidad de creación de túneles y proxy conocida como MagicSocks, que se basa en el proyecto Chisel de código abierto. Los actores también crearon una versión independiente de MagicSocks que usarían además de Gasket. La herramienta independiente MagicSocks viene como una biblioteca de enlaces dinámicos (DLL), que el actor también escribió en Golang.

Actualización o Mitigación

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

Boletín	2021-330
Asunto	NUEVA ACTIVIDAD DEL GRUPO ZEROX
Emisión	19/07/2021
CVE	No
Categoría	Filtración de Datos
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

Recientemente, se ha descubierto los ciberdelincuentes del grupo ZeroX han robado 1 TB de datos patentados que pertenecen a Saudi Aramco y lo están ofreciendo a la venta en la Dark Web.

Los atacantes han utilizado un exploit de día cero para vulnerar la red y servidores de Saudi Aramco. De esta manera, lograron robar 1 TB de información de la empresa que datan del año 1993 hasta la actualidad. Además, ZeroX publicó una pequeña muestra de planos y documentos patentados de Aramco en la Dark Web con la finalidad de generar interés en sus compradores.

La información robada incluye documentos pertenecientes a las refinerías de Saudi Aramco ubicadas en varias ciudades de Arabia Saudita incluidas Yanbu, Jazan, Jeddah, Ras Tanura, Riyadh y Dhahran. Los datos incluyen información personal de más de diez mil empleados, especificaciones de proyectos y topología de red que contiene direcciones IP, puntos Scada, puntos de acceso Wi-Fi, cámaras IP y dispositivos IoT.

Se ha verificado que no se trata de un ataque de ransomware, sino que la filtración de información ocurrió porque los datos de la empresa estaban en manos de terceros contratistas.

Hasta el momento no hay más detalles técnicos sobre el exploit usado.

Actualización o Mitigación

• Monitorear, identificar y prevenir fugas de información con sistemas como DLP.

Boletín	2021-331
Asunto	NUEVA ACTIVIDAD DEL RANSOMWARE RANSOMEXX
Emisión	19/07/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Recientemente la empresa afectada presentó una denuncia mediante una publicación oficial por el delito de atentado a sistemas informáticos para que se lleve a cabo la investigación e identificación de los responsables del ataque.

Si bien, la empresa no ha declarado oficialmente que sufrieron un ataque de ransomware, BleepingComputer indica que el ataque fue realizado por una operación de ransomware conocida como RansomEXX y un investigador de seguridad compartió un enlace de la nota de rescate de la DarkWeb.

Actualmente, esta página está oculta al público y solo se puede acceder a ella a través del enlace directo. Estas páginas ocultas se incluyen comúnmente en notas de rescate para demostrar que una operación de ransomware robó datos durante un ataque e indicar los pasos para que se pague el rescate solicitado por los cibercriminales.

Según en BleepingComputer la banda RansomEXX afirma haber robado 190 GB de datos y haber compartido screenshot de algunos de los documentos en la página de filtración de datos. Donde se observan listas de contactos, contratos y registros de soporte.

La operación de ransomware se lanzó originalmente con el nombre de Defray en 2018, pero se volvió más activa en junio de 2020 cuando cambió su nombre a RansomEXX y comenzó a apuntar a grandes entidades corporativas. Al igual que otras bandas de ransomware, RansomEXX comprometerá una red a través de credenciales compradas, servidores RDP, servidores ESXI o mediante la utilización de exploits. Una vez que obtienen acceso a una red, se propagarán silenciosamente por toda la red mientras roban archivos no cifrados para usarlos en intentos de extorsión, para mayor información revisar el Boletin 2021-052.

Como se está volviendo común entre las operaciones de ransomware, RansomEXX creó una versión de Linux para garantizar que puedan apuntar a todos los servidores y máquinas virtuales críticos. Actualmente este ransomware ha estado siendo seguido por la mayoría de empresas de Antivirus los cuales están bloqueando de manera proactiva los IOC relacionados a RansomEXX, para mayor información revisar el Boletín 2020-351.

Actualización o Mitigación

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

Boletín	2021-333
Asunto	NUEVA CAMPAÑA DE PHISHING POR EL GRUPO DE CIBERDELINCUENTES LUMINOUSMOTH
Emisión	19/07/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Recientemente se identificaron dos vectores iniciales de infección utilizados por el grupo de ciberdelincuentes LuminousMoth, el primer vector inicial proporciona a los atacantes acceso inicial a un sistema mediante un spear-phishing a la víctima que contiene un enlace de descarga de Dropbox. El enlace conduce a un archivo RAR que se hace pasar por un documento de Word estableciendo el parámetro "file_subpath" para que apunte a un nombre de archivo con una extensión .DOCX.

El archivo contiene dos archivos ejecutables que descargan archivos DLL maliciosos. En estos correos de phishing pretenden hacerse pasar como documentos con información de proyectos legítimos, como por ejemplo "COVID-19 Case 12-11-2020 (MOTC) .rar" o "DACU Projects.r01".

El segundo vector de infección entra en juego después de que el primero haya finalizado con éxito, mediante el cual el malware intenta propagarse infectando unidades USB extraíbles. Esto es posible mediante el uso de dos componentes el primero es un archivo malicioso "version.dll", el segundo es "wwlib.dll", otro archivo malicioso descargado por el archivo binario legítimo de "winword.exe". El propósito del archivo "version.dll" es propagarse a dispositivos extraíbles, mientras que el propósito de "wwlib.dll" es descargar Cobalt Strike beacon. Luego los cibercriminales instalan una herramienta maliciosa adicional en algunos de los dispositivos infectados, que aparenta ser el software popular Zoom, con el propósito de exfiltrar archivos y datos confidenciales mediante la comunicación de un servidor C2.

Actualización o Mitigación

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

Boletín	2021-336
Asunto	NUEVA MALWARE MOSAICLOADER
Emisión	20/07/2021
CVE	No
Categoría	Malware
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	2021-340
Asunto	NUEVA VARIANTE DEL MALWARE FORMBOOK
Emisión	22/07/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Sistemas Operativos Windows.
- Sistemas Operativos MacOS

Descripción

El equipo de Check Point informó en diciembre de 2020 que Formbook afectó al 4% de las organizaciones en todo el mundo, ha estado activo durante más de 5 años, actualmente es considerado uno de los programas maliciosos más frecuentes en campañas de phishing.

Formbook se ejecuta como un backdoor que recopila credenciales de varios navegadores web, recopila capturas de pantalla, monitorea y registra las pulsaciones de teclas como un Keylogger, y puede descargar y ejecutar archivos de acuerdo con las órdenes recibidas mediante los servidores Command-and-Control (C&C), perteneciente a los cibercriminales. Este malware está escrito en un lenguaje de programación tipo C y con herramientas capaces de dificultar el análisis de los investigadores.

Formbook estaba destinado a ser "un simple Keylogger". Sin embargo, los clientes que compraron el malware en la darkweb lo observaron como una herramienta para utilizarlo en campañas de phishing dirigidas a grandes empresas.

Recientemente Formbook se está vendiendo como un malware con el nombre XLoader, el malware se encuentra disponible en un foro de ventas ubicado en la Darkweb. Actualmente XLoader ha adquirido nuevas capacidades que lo ayudan a operar en sistemas macOS.

Actualización o Mitigación

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

Boletín	2021-341
Asunto	NUEVA MALWARE NPM ROBA CREDENCIALES DE GOOGLE CHROME
Emisión	23/07/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Sistemas Operativos Windows
- Google Chrome

Descripción

Este malware escucha las conexiones entrantes del servidor comando y control del atacante y proporciona capacidades avanzadas como acceso a la pantalla y la cámara, lista de directorios, búsqueda de archivos, carga de archivos y ejecución de comandos de shell.

Se ha descubierto dos paquetes NPM maliciosos que roban secretamente contraseñas del navegador web Google Chrome. Estos paquetes se llaman “nodejs_net_server” y “temptesttempfile”. El enfoque principal está en “nodejs_net_server” que contiene la funcionalidad principal del malware.

El malware se dirige a las máquinas con Windows para robar las credenciales de los usuarios y también configura backdoors para que el atacante realice actividades de vigilancia. Para facilitar sus actividades, el malware, específicamente "nodejs_net_server", usa la utilidad legítima de software gratuito ChromePass para Windows. Esta utilidad está empaquetada dentro del paquete NPM con nombres engañosos como a[.]exe.

Al instalar el paquete, este intenta ganar persistencia en la máquina Windows abusando de la conocida opción de configuración npm, "bin". La opción "bin" en el archivo del paquete, package.json, tiene como objetivo secuestrar el paquete "jstest", en caso de que esté preinstalado en la máquina de la víctima.

El archivo "jstest" cargado por el malware intenta sobrescribir el contenido del enlace simbólico "jstest" existente y agrega otro archivo JS (test[.]js) como un servicio de Windows que ahora se ejecutará de manera persistente.

Este servicio de Windows recién agregado, abre el puerto 7353 al que el atacante debe conectarse y realizar diversas actividades de vigilancia.

Actualización o Mitigación

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

Boletín	2021-345
Asunto	NUEVA CAMPAÑA DE PHISHING ENVÍA MALWARE MEDIANTE DOCUMENTOS WORD POR CORREO
Emisión	26/07/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Recientemente una nueva campaña de phishing utiliza la estrategia de adjuntar un documento malicioso de Microsoft Word a un correo electrónico no solicitado. Este documento de Word entrega un nuevo malware diseñado para robar información y credenciales de la billetera criptográfica de los dispositivos infectados de las víctimas. Este malware no parece pertenecer a ninguna familia de malware conocida, por lo cual será denominado como "dmechant".

En esta campaña el correo electrónico no deseado parece un recordatorio de pedido urgente de un administrador de compras. Al igual que con los documentos de Word utilizados en otras campañas de phishing, este incluye una macro maliciosa. Muestra una barra de advertencia de seguridad para informar al usuario del riesgo de abrirlo. El contenido de este documento está escrito en español. Esta campaña está dirigida a múltiples regiones y se adjuntó el documento incorrecto, o esto se hizo deliberadamente para disfrazar la advertencia.

La macro maliciosa se ejecuta una vez que se hace clic en el botón Habilitar contenido. Tiene una función de VBA llamada Document_Open(). Esta es una función incorporada de la macro y se llama automáticamente cuando se abre el documento. Luego llama a otras funciones para extraer un código JS (JavaScript) en un archivo (rtbdxsdcb[.]js) en la carpeta% temp%. Después de eso, ejecuta este archivo "JS" para terminar el trabajo de la Macro. Esto descarga un archivo ejecutable en% Temp% y lo guarda como erbxcb[.]exe, que es el archivo de payload del malware. Más tarde, crea un objeto WScript[.]Shell para iniciar el archivo ejecutable de payload en el dispositivo infectado.

Cuando se inicia, primero recopila información básica sobre el dispositivo de la víctima, como la hora actual del sistema, la versión de Windows, el nombre de usuario, el nombre de la computadora, etc. Esta información se enviará al atacante junto con otros datos robados.

Actualización o Mitigación

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

Boletín	2021-347
Asunto	NUEVA ACTIVIDAD DEL MALWARE TAURUS
Emisión	26/07/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

El malware Taurus se descarga mediante supuestos sitios de software craqueados los cuales se muestran en el motor de búsqueda de Google como programas promocionados legítimos, al ingresar a esta página y se descargue el archivo se instruirá al usuario durante un proceso de instalación del software que aparenta ser legítimo. Recientemente se ha observado un gran aumento en su actividad lo que ocasionaría un riesgo de infección hacia dispositivos pertenecientes a grandes empresas.

Al seguir con la instalación del supuesto software legítimo, se instalarán payloads pertenecientes al malware Taurus. Adicionalmente se observó que la página de descarga está protegida contra bots mediante captcha, lo que evitaría que se extraigan los payloads del malware Taurus.

Finalmente, en su ciclo de infección, al ejecutarse con éxito Taurus usará AutoIt para realizar varias técnicas de evasión con el fin de ejecutar un payload que se descifrará en la memoria y se ejecutará. En lugar de implementar su algoritmo de descifrado en AutoIt, los desarrolladores de malware han optado por diseñar un sistema de cifrado de flujo RC4.

Actualización o Mitigación

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

Boletín	2021-349
Asunto	NUEVA CAMPAÑA DEL CRYPTOJACKING LEMONDUCK
Emisión	26/07/2021
CVE	No
Categoría	Cryptominer
Severidad	Alta

Servicios Afectados

- Sistemas Operativos Windows.
- Sistemas Operativos Linux.

Descripción

Un malware de minería criptográfica ha seguido perfeccionando y mejorando sus técnicas para atacar tanto a los sistemas operativos Windows como Linux al dirigirse a vulnerabilidades antiguas, mientras que simultáneamente mejora su método de propagación para tener una mayor efectividad en sus campañas.

Las actividades de LemonDuck se detectaron por primera vez en China en el 2019, antes de que comenzara a adoptar señuelos con temática de COVID-19 en ataques por correo electrónico en 2020, recientemente se observó que pretende obtener acceso a sistemas sin parches. El malware LemonDuck es conocido por su capacidad de propagarse rápidamente a través de una red infectada para facilitar el robo de información y convertir las máquinas en bots mineros de criptomonedas.

LemonDuck es un malware activamente actualizado, conocido por sus objetivos en las criptomonedas, actualmente los cibercriminales de LemonDuck también pretende robar credenciales, eliminar controles de seguridad, propagarse a través de correos electrónicos, moverse lateralmente y utilizar una infraestructura de comando y control (C2) lo que permitirá que pueda recaudar toda la información obtenida por el malware.

Actualización o Mitigación

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

Boletín	2021-350
Asunto	NUEVA CAMPAÑA DEL GRUPO DE CIBERDELINCUENTES APT31
Emisión	27/07/2021
CVE	No
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

• Dispositivos de enrutamiento.

• Sistemas Operativos Windows.

Descripción

Recientemente se ha observado que el grupo APT31 ha observado una campaña en Francia el cual se mantiene activa, el propósito de esta campaña es comprometer enrutadores para usarlos para llevar a cabo un ciclo de infección.

Recientemente se observó nuevas actividades del grupo de cibercriminales “APT31”, en el cual actualmente está ejecutando una campaña que compromete enrutadores para utilizarlos como vector inicial de ataque.

LA Agencia Nacional Francesa de Ciberseguridad también advirtió sobre una serie de ataques en curso contra una gran cantidad de organizaciones francesas coordinadas por el grupo de ciberdelincuentes APT31. APT31 (también conocido como Zirconium y Judgement Panda) es un grupo de ciberdelincuentes que trabaja a instancias del gobierno chino conocido por sus numerosas operaciones de espionaje y robo de información.

El año pasado, Microsoft observó ataques APT31 dirigidos a personas de alto cargo asociadas con la campaña presidencial de Joe Biden. APT31 también fue detectado por Google mientras apuntaba a robar credenciales de correos electrónicos personales mediante una campaña de phishing.

Actualización o Mitigación

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

Boletín	2021-351
Asunto	NUEVO RANSOMWARE AVOSLOCKER
Emisión	28/07/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

Se descubrió un ransomware relativamente nuevo, que se observó su actividad a finales de junio y principios de julio. Sus autores comenzaron a buscar socios a través de foros clandestinos.

El nuevo ransomware detectado se le asigno el nombre de AvosLocker y recientemente han anunciado un reclutamiento de "pentesters con experiencia en la red de Active Directory" y "corredores de acceso", lo que sugiere que quieren cooperar con personas que tienen acceso remoto a la infraestructura vulnerada.

AvosLocker es ejecutado manualmente por un atacante que accedió de forma remota al equipo. Por esta razón, no intenta ser sigiloso durante su ejecución. En el modo predeterminado, funciona como una aplicación de consola que informa detalles sobre su progreso en la pantalla. Al observar el registro, se observa que el ransomware primero "mapea" las unidades accesibles enumerando todos sus archivos. Después de eso, pasa al cifrado. Los archivos se seleccionan para el cifrado en función de sus extensiones.

Los archivos que han sido cifrados por AvosLocker se pueden identificar con la extensión .avos donde también adjunta al nombre del archivo original. Si bien el contenido es ilegible, al final encontramos un bloque codificado en Base64.

Los datos codificados en Base64 contienen una clave AES protegida por RSA que se utilizó para cifrar este archivo. Cada directorio atacado tiene una nota de rescate, llamada GET_YOUR_FILES_BACK[.]txt.

Actualización o Mitigación

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

Boletín	2021-355
Asunto	NUEVA ACTIVIDAD DEL RANSOMWARE LOCKBIT
Emisión	31/07/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

Una nueva versión del ransomware LockBit 2.0 automatiza el cifrado de un dominio de Windows mediante políticas de grupo de Active Directory.

La operación de ransomware LockBit se lanzó en septiembre de 2019 como un ransomware-as-a-service, donde los actores de amenazas son reclutados para comprometer redes y utilizar software de terceros para implementar scripts que deshabilitan el antivirus y luego ejecutan el ransomware en las computadoras de la red.

Se descubrió que los ciberdelincuentes han automatizado este proceso para que el ransomware se distribuya a través de un dominio cuando se ejecuta en un controlador de dominio.

El ransomware creará nuevas políticas de grupo en el controlador de dominio que luego se envían a todos los dispositivos de la red. Estas políticas deshabilitan la protección en tiempo real de Microsoft Defender, las alertas, el envío de muestras a Microsoft y las acciones predeterminadas al detectar archivos maliciosos. Durante este proceso, el ransomware también usará las API de Windows Active Directory para realizar consultas LDAP contra el ADS del controlador de dominio para obtener una lista de computadoras.

Al obtener la lista, el ejecutable del ransomware se copiará en el escritorio de cada dispositivo y la tarea programada configurada por las políticas de grupo iniciará el ransomware utilizando la omisión de UAC, lo cual le permite ejecutarse silenciosamente en segundo plano sin ninguna alerta externa sobre el dispositivo que se está cifrando.

Actualización o Mitigación

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

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.