# Boletín de Ciberseguridad N°72

Fecha de publicación: 11/12/2023

Mes de Diciembre

29/11/2023 – 11/12/2023

Datasec

BOLETÍN DE CIBERSEGURIDAD

# Indice


Introducción....3

Malware del agente Tesla que utiliza compresión ZPAQ....5

CISA agrega tres fallas de seguridad con explotación activa....6

Apple lanza parches para iOS, macOS y Safari para dos fallas explotadas activamente....7

Anuncios maliciosos de Google engañan a los usuarios de WinSCP....9

Evolución de las tácticas de evasión y robo de credenciales de COLDRIVER....10

APT28 explota una vulnerabilidad crítica de Outlook....11

LogoFAIL podría afectar a casi todos los dispositivos Windows y Linux....12

Conclusiones....14

# Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención. La publicación de dichas noticias dependerá de la importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta primera quincena del mes de diciembre se destacan 7 noticias de relevancia: 3 sobre vulnerabilidades tecnológicas, y 4 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

CISA agrega tres fallas de seguridad con explotación activa

CISA agregó el jueves tres fallas de seguridad a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV) basándose en evidencia de explotación activa en la naturaleza.

Anuncios maliciosos de Google engañan a los usuarios de WinSCP

Los actores de amenazas están aprovechando resultados de búsqueda manipulados y anuncios falsos de Google que engañan a los usuarios que buscan descargar software legítimo como WinSCP para que instalen malware.

Microsoft advierte sobre la evolución de las tácticas de evasión y robo de credenciales

El actor de amenazas conocido como COLDRIVER ha seguido participando en actividades de robo de credenciales contra entidades que son de interés estratégico para Rusia y, al mismo tiempo, ha mejorado sus capacidades de evasión de detección.


# Vulnerabilidad Crítica

## Malware del agente Tesla que utiliza compresión ZPAQ

CRÍTICO

Descripción

Se ha observado que una nueva variante del malware Agent Tesla se entrega a través de un archivo señuelo con el formato de compresión ZPAQ para recopilar datos de varios clientes de correo electrónico y casi 40 navegadores web.

Estado

Agent Tesla, que apareció por primera vez en 2014, es un registrador de teclas y un troyano de acceso remoto (RAT) escrito en .NET que se ofrece a otros actores de amenazas como parte de un modelo de malware como servicio (MaaS).

A menudo se utiliza como carga útil de primera etapa, brinda acceso remoto a un sistema comprometido y se utiliza para descargar herramientas de segunda etapa más sofisticadas, como ransomware.

El agente Tesla generalmente se entrega a través de correos electrónicos de phishing, y campañas recientes aprovechan una vulnerabilidad de corrupción de memoria de hace seis años en el Editor de ecuaciones de Microsoft Office (CVE-2017-11882).

La última cadena de ataques comienza con un correo electrónico que contiene un archivo adjunto ZPAQ que pretende ser un documento PDF, al abrirse se extrae un ejecutable .NET inflado que en su mayor parte está relleno con cero bytes para inflar artificialmente el tamaño de la muestra a 1 GB en un esfuerzo por evitar las medidas tradicionales de seguridad.

Remediación / Referencias

El desarrollo es una señal de que los actores de amenazas están experimentando con formatos de archivos poco comunes para la entrega de malware, lo que requiere que los usuarios estén atentos a los correos electrónicos sospechosos y mantengan sus sistemas actualizados.

Por mayor información acceder a:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-11882

| | | |
|---|---|---|
| | CISA agrega tres fallas de seguridad con explotación activa | CRÍTICO |

Descripción

CISA agregó el jueves tres fallas de seguridad a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV) basándose en evidencia de explotación activa en la naturaleza.

Estado

Las vulnerabilidades son las siguientes:

- CVE-2023-36584 (puntuación CVSS: 5,4): vulnerabilidad de omisión de característica de seguridad de marca de la web (MotW) de Microsoft Windows.
- CVE-2023-1671 (puntuación CVSS: 9,8): vulnerabilidad de inyección de comandos del dispositivo web de Sophos.
- CVE-2020-2551 (puntuación CVSS: 9,8): vulnerabilidad no especificada de Oracle Fusion Middleware.

CVE-2023-1671 se relaciona con una vulnerabilidad crítica de inyección de comando previo a la autenticación que permite la ejecución de código arbitrario.

CVE-2020-2551 es una falla en los componentes principales de WLS que permite que un atacante no autenticado con acceso a la red comprometa el servidor WebLogic.

Remediación / Referencias

Se recomienda tener en cuenta la nueva valorización de estas vulnerabilidades antes publicadas, y ajustar sus controles de seguridad para mitigar o remediar las mismas, según las recomendaciones de los propios fabricantes.

Toda la información aquí:

https://nvd.nist.gov/vuln/detail/CVE-2023-1671

## Apple lanza parches para iOS, macOS y Safari para dos fallas

CRÍTICO

Descripción

Apple ha lanzado actualizaciones de software para iOS, iPadOS, macOS y el navegador web Safari para abordar dos fallas de seguridad que, según dijo, han sido explotadas activamente en versiones anteriores de su software.

Estado

Las vulnerabilidades, las cuales residen en el motor del navegador web WebKit, se describen a continuación:

- CVE-2023-42916: un problema de lectura fuera de límites que podría aprovecharse para filtrar información confidencial al procesar contenido web.
- CVE-2023-42917: un error de corrupción de memoria que podría provocar la ejecución de código arbitrario al procesar contenido web.

El fabricante de iPhone no proporcionó información adicional sobre la explotación en curso, pero previamente se reveló que los días cero en iOS se han utilizado para entregar software espía mercenario dirigido a personas de alto riesgo, como activistas, disidentes, periodistas y políticos.

Vale la pena señalar aquí que todos los navegadores web de terceros disponibles para iOS y iPadOS, incluidos Google Chrome, Mozilla Firefox y Microsoft Edge, entre otros, funcionan con el motor de renderizado WebKit debido a las restricciones impuestas por Apple, lo que lo convierte en una superficie de ataque lucrativa y amplia.

Remediación / Referencias

Las actualizaciones están disponibles para los siguientes dispositivos y sistemas operativos:

- iOS 17.1.2 y iPadOS 17.1.2: iPhone XS y posteriores, iPad Pro de 12,9 pulgadas de segunda generación y posteriores, iPad Pro de 10,5 pulgadas, iPad Pro de 11 pulgadas de primera generación y posteriores, iPad Air de tercera generación y posteriores, iPad de sexta generación y posteriores, y iPad mini de 5.ª generación y posteriores.
- macOS Sonoma 14.1.2: Mac que ejecutan macOS Sonoma.
- Safari 17.1.2: Mac con macOS Monterey y macOS Ventura.

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-6345

# Prevención

| | | |
|---|---|---|
| Google | Anuncios maliciosos de Google engañan a los usuarios de WinSCP | PREVENCIÓN |

Descripción

Los actores de amenazas están aprovechando resultados de búsqueda manipulados y anuncios falsos de Google que engañan a los usuarios que buscan descargar software legítimo como WinSCP para que instalen malware.

Estado

Se cree que los actores de amenazas aprovechan los anuncios de búsqueda dinámica (DSA) de Google, que generan automáticamente anuncios basados en el contenido de un sitio para mostrar anuncios maliciosos que llevan a las víctimas al sitio infectado.

El objetivo final de la compleja cadena de ataque de varias etapas es atraer a los usuarios para que hagan clic en el sitio web falso WinSCP, winccp[.]net, y descarguen el malware.

La carga útil final toma la forma de un archivo ZIP ("WinSCP_v.6.1.zip") que viene con un ejecutable de configuración que, cuando se inicia, emplea carga lateral de DLL para cargar y ejecutar un archivo DLL llamado python311.dll que está presente en el archivo.

Esta no es la primera vez que se abusa de los anuncios dinámicos de búsqueda de Google para distribuir malware. A finales del mes pasado, Malwarebytes levantó la tapa de una campaña dirigida a los usuarios que buscan PyCharm con enlaces a un sitio web pirateado que alberga un instalador fraudulento que allana el camino para la implementación de malware que roba información.

La publicidad maliciosa ha ganado popularidad entre los ciberdelincuentes en los últimos años, y en los últimos meses numerosas campañas de malware han utilizado esta táctica para atacar.

Remediación / Referencias

La publicidad maliciosa ha ganado popularidad entre los ciberdelincuentes en los últimos años, y en los últimos meses numerosas campañas de malware han utilizado esta táctica para atacar.

Por mayor información acceder a:

https://cyware.com/news/malicious-google-ads-trick-winscp-users-into-installing-malware-6999fb3a

| Microsoft | Evolución de las tácticas de evasión y robo de credenciales de COLDRIVER | PREVENCIÓN |
|---|---|---|

Descripción

El actor de amenazas conocido como COLDRIVER ha seguido participando en actividades de robo de credenciales contra entidades que son de interés estratégico para Rusia y, al mismo tiempo, ha mejorado sus capacidades de evasión de detección.

Estado

El equipo de Microsoft Threat Intelligence está rastreando el clúster como Star Blizzard (anteriormente SEABORGIUM). También se llama Blue Callisto, BlueCharlie (o TAG-53), Calisto (alternativamente escrito Callisto) y TA446.

El adversario "continúa atacando prolíficamente a personas y organizaciones involucradas en asuntos internacionales, defensa y apoyo logístico a Ucrania, así como a la academia, empresas de seguridad de la información y otras entidades alineadas con los intereses estatales rusos", dijo Redmond.

Star Blizzard, vinculada al Servicio Federal de Seguridad (FSB) de Rusia, tiene un historial de creación de dominios similares que se hacen pasar por las páginas de inicio de sesión de empresas específicas. Se sabe que está activo desde al menos 2017.

Microsoft dijo que observó al adversario aprovechando scripts del lado del servidor para evitar el escaneo automatizado de la infraestructura controlada por el actor a partir de abril de 2023, alejándose de hCaptcha para determinar objetivos de interés y redirigiendo la sesión de navegación al servidor Evilginx.

El código JavaScript del lado del servidor está diseñado para verificar si el navegador tiene algún complemento instalado, si se accede a la página mediante una herramienta de automatización como Selenium o PhantomJS, y transmitir los resultados al servidor en forma de una solicitud HTTP POST.

Remediación / Referencias

A pesar de estos cambios, las actividades de Star Blizzard siguen centradas en el robo de credenciales de correo electrónico, principalmente dirigidas a proveedores de correo electrónico basados en la nube que alojan cuentas de correo electrónico organizacionales y/o personales.

Por mayor información acceder a:

https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/

| Microsoft | APT28 explota una vulnerabilidad crítica de Outlook | PREVENCIÓN |
|---|---|---|

Descripción

Microsoft dijo que detectó actividad de un estado-nación respaldado por el Kremlin que explotaba una falla de seguridad crítica ahora parcheada en su servicio de correo electrónico Outlook para obtener acceso no autorizado a las cuentas de las víctimas dentro de los servidores Exchange.

Estado

La vulnerabilidad de seguridad en cuestión es CVE-2023-23397 (puntuación CVSS: 9,8), un error crítico de escalada de privilegios que podría permitir a un adversario acceder al hash Net-NTLMv2 de un usuario que luego podría usarse para realizar un ataque de retransmisión contra otro servicio para autenticarse como usuario. Microsoft lo parchó en marzo de 2023.

El objetivo, según el Comando Cibernético Polaco (DKWOC), es obtener acceso no autorizado a buzones de correo de entidades públicas y privadas del país.

Microsoft reveló anteriormente que la deficiencia de seguridad había sido utilizada como arma por actores de amenazas con sede en Rusia como un día cero en ataques dirigidos a los sectores gubernamental, de transporte, energético y militar en Europa desde abril de 2022.

Posteriormente, en junio de 2023, la empresa de ciberseguridad Recorded Future reveló detalles de una campaña de phishing orquestada por APT28 que explota múltiples vulnerabilidades en el software de correo web de código abierto Roundcube, al tiempo que señaló que la campaña se superpone con la actividad que emplea la vulnerabilidad de Microsoft Outlook.

La Agencia Nacional de Ciberseguridad de Francia (ANSSI), a finales de octubre, también culpó al equipo de piratería de atacar a entidades gubernamentales, empresas, universidades, institutos de investigación y grupos de expertos desde la segunda mitad de 2021 aprovechando varias fallas, contando CVE- 2023-23397, para implementar implantes como CredoMap.

Remediación / Referencias

La empresa de ciberseguridad Proofpoint, en un análisis independiente, dijo que observó campañas de phishing de gran volumen a finales de marzo y septiembre de 2023 que aprovecharon CVE-2023-23397 y CVE-2023-38831, respectivamente, para objetivos en Europa y América del Norte.

Por mayor información acceder a:

https://www.oodaloop.com/cyber/2023/12/05/microsoft-warns-of-kremlin-backed-apt-28-exploiting-critical-outlook-vulnerability/

## LogoFAIL podría afectar a casi todos los dispositivos Windows y Linux

PREVENCIÓN

Descripción

Han creado un ataque de firmware que puede afectar a casi todos los dispositivos Windows o Linux. El ataque se conoce como LogoFAIL y es excepcionalmente fácil de llevar a cabo y podría dejar tanto los dispositivos empresariales como los de los consumidores susceptibles a los malos actores.

Estado

El ataque es especialmente tortuoso porque, en muchos casos, puede ejecutarse de forma remota en situaciones posteriores a la explotación utilizando técnicas que son casi imposibles de detectar para los productos tradicionales de seguridad de terminales. El exploit también se ejecuta durante las primeras etapas del proceso de arranque, lo que permite a los delincuentes eludir varias de las defensas integradas del sistema operativo.

Llamar al ataque al firmware LogoFAIL un ataque sin precedentes a la seguridad de consumidores y empresas, es quedarse corto. Además, los investigadores que idearon el ataque dicen que las casi dos docenas de vulnerabilidades en las que se basa han acechado durante años, si no décadas, dentro de las Interfaces de firmware extensibles unificadas (UEFI), que son responsables de arrancar dispositivos Linux y Windows modernos.

Se titula LogoFAIL porque ataca durante el logotipo de inicio del dispositivo, utilizando aproximadamente una docena de vulnerabilidades críticas que, según los investigadores, han permanecido desapercibidas y no descubiertas hasta ahora. La buena noticia es que los malos probablemente no conocían estas vulnerabilidades, lo que significa que aún no han sido explotadas.

Remediación / Referencias

No está claro qué tan rápido se solucionarán los exploits que hacen posible el ataque al firmware LogoFAIL. Debido a que LogoFAIL no requiere acceso físico al dispositivo, es excepcionalmente poderoso y peligroso.

Los investigadores también dicen que es probable que estos exploits hayan permanecido sin descubrir durante tanto tiempo porque las empresas no probaron los analizadores de imágenes que muestran el logotipo de la empresa durante el arranque.

Por mayor información acceder a:

https://it.slashdot.org/story/23/12/06/223245/nearly-every-windows-and-linux-device-vulnerable-to-new-logofail-firmware-attack

# Conclusiones

En un escenario laboral remoto en constante evolución, la seguridad de las conexiones sigue siendo una prioridad fundamental.

Preservarnos contra posibles amenazas es esencial, y para ello, la actualización constante y la configuración segura de los componentes son elementos clave. Resulta imperativo evaluar la seguridad de los dispositivos remotos mediante herramientas especializadas, asegurando que los sistemas operativos estén al día y que los controles de seguridad estén plenamente activos.

Estas medidas no solo actúan como barrera ante posibles abusos o compromisos, sino que también refuerzan globalmente la ciberseguridad. La adopción de soluciones como el FortiClient Health Check de Fortinet o el Device Health de Duo Security, entre otras opciones, puede marcar la diferencia en la postura de seguridad de cualquier organización. La autenticación de doble factor desempeña un papel crucial en la protección de los accesos remotos, reduciendo significativamente la probabilidad de incidentes de seguridad.

En Datasec, mantenemos nuestro firme compromiso de salvaguardar la seguridad de nuestros clientes, socios y colaboradores, instando a todos a mantener una atención constante en materia de seguridad cibernética.

En resumen, la seguridad en las conexiones remotas implica un compromiso continuo.

Al mantenerse actualizados y aplicar configuraciones seguras, las organizaciones pueden blindarse contra amenazas y garantizar un entorno de trabajo remoto seguro y confiable.

¡Sigamos colaborando para asegurarnos de mantenernos protegidos!