Boletín de Ciberseguridad N°73

Fecha de publicación: 08/01/2024

Mes de enero

26/12/2023 – 08/01/2023

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

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 enero se destacan 6 noticias de relevancia, siendo estas sobre vulnerabilidades tecnológicas.

Aquellas noticias a tener especial recaudo son las siguientes:

NIST: advierte sobre riesgos de seguridad y privacidad

NIST advierte sobre riesgos de seguridad y privacidad derivados del rápido despliegue de sistemas de IA.

Nueva variante de DLL evita protecciones de Windows 10 y 11

Investigadores descubren una nueva variante de una técnica de secuestro de órdenes de búsqueda de biblioteca de enlaces dinámicos (DLL) que los actores de amenazas podrían utilizar para eludir los mecanismos de seguridad y lograr la ejecución de código malicioso en sistemas que ejecutan Microsoft Windows 10 y Windows 11.

Malware utiliza exploit de Google MultiLogin

Malware que utiliza el exploit Google MultiLogin para mantener el acceso a pesar del restablecimiento de la contraseña.

Vulnerabilidad Crítica

Resurge Troyano Bandook RAT dirigido a Windows

CRÍTICO

Descripción

Investigadores informan de nueva variante de Bandook RAT, el troyano de acceso remoto se propaga mediante ataques de phishing con el objetivo de infiltrarse en máquinas con Windows

Estado

Bandook, detectado por primera vez en 2007, es un malware disponible en el mercado que viene con una amplia gama de funciones para obtener control remoto de los sistemas infectados.

Fortinet FortiGuard Labs, identificó la actividad informando que el malware se distribuye a través de un archivo PDF que incorpora un enlace a un archivo .7z protegido con contraseña.

Luego de que la víctima extrae el malware con la contraseña del archivo PDF, el malware inyecta su carga útil en "msinfo32.exe".

A su vez la empresa eslovaca de ciberseguridad ESET detalló una campaña de ciberespionaje que aprovechó una variante mejorada de Bandook para violar redes corporativas en países de habla hispana como Venezuela.

El punto de partida de la última secuencia de ataque es un componente inyector diseñado para descifrar y cargar la carga útil en msinfo32.exe, un binario legítimo de Windows que recopila información del sistema para diagnosticar problemas informáticos.

El malware, además de realizar cambios en el Registro de Windows para establecer persistencia en el host comprometido, establece contacto con un servidor de comando y control (C2) para recuperar cargas útiles e instrucciones adicionales.

Estas acciones se pueden clasificar a grandes rasgos como manipulación de archivos, manipulación de registros, descargas, robo de información, ejecución de archivos, invocación de funciones en archivos DLL desde el C2, control de la computadora de la víctima, eliminación de procesos y desinstalación de malware.

Remediación / Referencias

Por mayor información acceder a:

https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf
https://malpedia.caad.fkie.fraunhofer.de/details/win.bandook
https://thehackernews.com/2024/01/new-bandook-rat-variant-resurfaces.html

	Nueva variante de DLL evita protecciones de Windows 10 y 11	CRÍTICO

Descripción

Investigadores descubren una nueva variante de una técnica de secuestro de órdenes de búsqueda de biblioteca de enlaces dinámicos (DLL) que los actores de amenazas podrían utilizar para eludir los mecanismos de seguridad y lograr la ejecución de código malicioso en sistemas que ejecutan Microsoft Windows 10 y Windows 11.

Estado

El enfoque aprovecha los ejecutables que se encuentran comúnmente en la carpeta confiable WinSxS y los explota a través de la técnica clásica de secuestro de orden de búsqueda de DLL.

Al hacerlo, permite a los adversarios eliminar la necesidad de privilegios elevados cuando intentan ejecutar código nefasto en una máquina comprometida, así como introducir archivos binarios potencialmente vulnerables en la cadena de ataque, como se observó en el pasado.

El secuestro del orden de búsqueda de DLL, como su nombre lo indica, implica jugar con el orden de búsqueda utilizado para cargar archivos DLL con el fin de ejecutar cargas útiles maliciosas con fines de evasión de defensa, persistencia y escalada de privilegios.

Específicamente, los ataques que explotan la técnica señalan aplicaciones que no especifican la ruta completa a las bibliotecas que necesitan y, en cambio, se basan en un orden de búsqueda predefinido para localizar las DLL necesarias en el disco.

Los actores de amenazas aprovechan este comportamiento moviendo archivos binarios legítimos del sistema a directorios no estándar que incluyen archivos DLL maliciosos que llevan el nombre de archivos legítimos, de modo que la biblioteca que contiene el código de ataque se selecciona en lugar de este último.

Esto, a su vez, funciona porque el proceso que llama a la DLL buscará primero en el directorio desde el que se está ejecutando antes de iterar recursivamente a través de otras ubicaciones en un orden particular para localizar y cargar el recurso en cuestión.

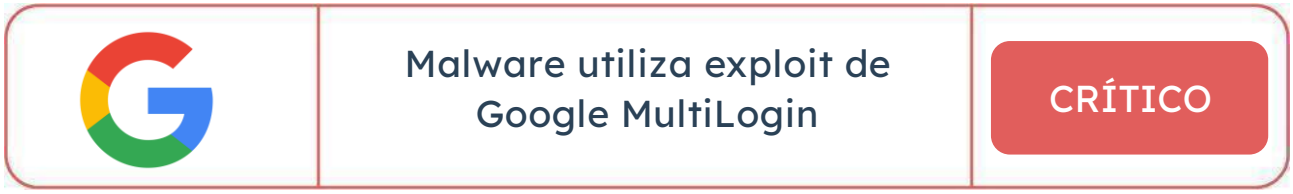
Expertos advirtieron que podría haber archivos binarios adicionales en la carpeta WinSxS que son susceptibles a este tipo de secuestro de orden de búsqueda de DLL, lo que requiere que las organizaciones tomen las precauciones adecuadas para mitigar el método de explotación dentro de sus entornos.

Es necesario examinar las relaciones padre-hijo entre procesos, con un enfoque específico en binarios confiables, asimismo, supervise de cerca todas las actividades realizadas por los archivos binarios que residen en la carpeta WinSxS, centrándose tanto en las comunicaciones de red como en las operaciones de archivos.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2024/01/new-variant-of-dll-search-order.html



Descripción

Malware que utiliza el exploit Google MultiLogin para mantener el acceso a pesar del restablecimiento de la contraseña.

Estado

El malware que roba información está aprovechando activamente un punto final indocumentado de Google OAuth llamado MultiLogin para secuestrar las sesiones de los usuarios y permitir el acceso continuo a los servicios de Google incluso después de restablecer la contraseña.

El exploit crítico facilita la persistencia de la sesión y la generación de cookies, lo que permite a los actores de amenazas mantener el acceso a una sesión válida de forma no autorizada.

La técnica fue revelada por primera vez por un actor de amenazas llamado PRISMA el 20 de octubre de 2023 en su canal de Telegram. Desde entonces, se ha incorporado a varias familias de ladrones de malware como servicio (MaaS), como Lumma, Rhadamanthys, Stealc, Meduza, RisePro y WhiteSnake.

El punto final de autenticación MultiLogin está diseñado principalmente para sincronizar cuentas de Google entre servicios cuando los usuarios inician sesión en sus cuentas en el navegador web Chrome (es decir, perfiles).

Una ingeniería inversa del código de Lumma Stealer ha revelado que la técnica apunta a la "tabla token_service de Chrome de WebData para extraer tokens e ID de cuenta de los perfiles de Chrome conectados. Esta tabla contiene dos columnas cruciales: servicio (ID de GAIA) y token_encriptado.

Este token: par de ID de GAIA se combina con el punto final MultiLogin para regenerar las cookies de autenticación de Google.

Los investigadores probaron tres escenarios diferentes de generación de cookies simbólicas:

- Cuando el usuario inicia sesión con el navegador, en cuyo caso el token se puede utilizar cualquier cantidad de veces.
- Cuando el usuario cambia la contraseña, pero permite que Google permanezca conectado, en cuyo caso el token sólo se puede usar una vez, ya que ya se usó una vez para permitir que el usuario permanezca conectado.
- Si el usuario cierra sesión en el navegador, el token será revocado y eliminado del almacenamiento local del navegador, que se regenerará al iniciar sesión nuevamente.

Cuando se le contactó para hacer comentarios, Google reconoció la existencia del método de ataque, pero señaló que los usuarios pueden revocar las sesiones robadas cerrando sesión en el navegador afectado.

"Google está al tanto de informes recientes sobre una familia de malware que roba tokens de sesión", informó la compañía. "Los ataques que involucran malware que roba cookies y tokens no son nuevos; actualizamos rutinariamente nuestras defensas contra tales técnicas y para proteger a los usuarios que son víctimas del malware. En este caso, Google ha tomado medidas para proteger cualquier cuenta comprometida detectada".

"Sin embargo, es importante tener en cuenta una idea errónea en los informes que sugieren que el usuario no puede revocar los tokens y las cookies robadas", añadió. "Esto es incorrecto, ya que las sesiones robadas pueden invalidarse simplemente cerrando sesión en el navegador afectado o revocarse de forma remota a través de la página de dispositivos del usuario. Continuaremos monitoreando la situación y brindando actualizaciones según sea necesario".

La compañía recomendó además a los usuarios activar la navegación segura mejorada en Chrome para protegerse contra el phishing y las descargas de malware.

"Se recomienda cambiar las contraseñas para que los actores de amenazas no utilicen flujos de autenticación de restablecimiento de contraseñas para restaurarlas". "Además, se debe recomendar a los usuarios que controlen la actividad de su cuenta en busca de sesiones sospechosas que provengan de direcciones IP y ubicaciones que no reconocen".

La aclaración de Google es un aspecto importante de la seguridad del usuario, sin embargo, el incidente arroja luz sobre un exploit sofisticado que puede desafiar los métodos tradicionales de seguridad de cuentas. Si bien las medidas de Google son valiosas, esta situación resalta la necesidad de soluciones de seguridad más avanzadas para contrarrestar las amenazas cibernéticas en evolución, como en el caso de los ladrones de información, que son tremendamente populares entre los cibercriminales hoy en día.

Remediación / Referencias

Por mayor información acceder a: https://thehackernews.com/2024/01/malware-using-google-multilogin-exploit.html

orange™	Orange España atacado mediante malware	CRÍTICO

Descripción

Orange España se enfrenta a un secuestro de tráfico BGP después de que un malware pirateara su cuenta RIPE.

Estado

El operador de red móvil Orange España sufrió una interrupción de Internet durante varias horas después de que un actor de amenazas utilizara credenciales de administrador capturadas mediante un malware para secuestrar el tráfico del protocolo de puerta de enlace fronterizo (BGP).

"La cuenta de Orange en el centro de coordinación de redes IP (RIPE) ha sufrido un acceso indebido que ha afectado a la navegación de algunos de nuestros clientes", publicó la firma a través de X (antes Twitter).

Sin embargo, la empresa enfatizó que no se comprometió ningún dato personal y que el incidente sólo afectó a algunos servicios de navegación.

El actor de amenazas, que se conoce con el nombre de Ms_Snow_OwO en X, afirmó haber obtenido acceso a la cuenta RIPE de Orange España. RIPE es un registro regional de Internet (RIR) que supervisa la asignación y el registro de direcciones IP y números de sistemas autónomos (AS) en Europa, Asia central, Rusia y Asia occidental.

Utilizando la cuenta robada, el actor de amenazas modificó el número AS perteneciente a la dirección IP de Orange, lo que provocó importantes interrupciones en Orange y una pérdida de tráfico del 50%.

Un análisis más detallado ha revelado que la dirección de correo electrónico de la cuenta de administrador está asociada con la computadora de un empleado de Orange España que fue infiltrado por el malware Raccoon Stealer el 4 de septiembre de 2023.

Actualmente no se sabe cómo el ladrón llegó al sistema del empleado, pero estas familias de malware generalmente se propagan a través de publicidad maliciosa o estafas de phishing.

Entre las credenciales corporativas identificadas en la máquina, el empleado tenía credenciales específicas para 'https://access.ripe.net' utilizando la dirección de correo electrónico revelada por el actor de la amenaza (adminripe-ipnt@orange.es).

Peor aún, la contraseña utilizada para proteger la cuenta de administrador RIPE de Orange era "ripadmin", que es débil y fácilmente predecible.

Investigadores de seguridad informaron además que RIPE no exige autenticación de dos factores (2FA) ni aplica una política de contraseñas segura para sus cuentas, lo que la hace propicia para el abuso.

Actualmente, los mercados de robo de información están vendiendo miles de credenciales para access.ripe.net, lo que permite efectivamente repetir esto en organizaciones e ISP de toda Europa.

RIPE, que actualmente está investigando para ver si otras cuentas se han visto afectadas de manera similar, dijo que se comunicará directamente con los titulares de cuentas afectadas. También instó a los usuarios de cuentas de RIPE NCC Access a actualizar sus contraseñas y habilitar la autenticación multifactor para sus cuentas.

"A largo plazo, estamos acelerando la implementación de 2FA para que sea obligatoria para todas las cuentas de RIPE NCC Access lo antes posible e introducir una variedad de mecanismos de verificación", añadió la compañía.

El incidente sirve para resaltar las consecuencias de las infecciones por robo de información, lo que requiere que las organizaciones tomen medidas para proteger sus redes de vectores de ataque iniciales conocidos.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/11/warning-3-critical-vulnerabilities.html

NIST	NIST: advierte sobre riesgos de seguridad y privacidad	CRÍTICO

Descripción

NIST advierte sobre riesgos de seguridad y privacidad derivados del rápido despliegue de sistemas de IA.

Estado

El Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. llama la atención sobre los desafíos de privacidad y seguridad que surgen como resultado del mayor despliegue de sistemas de inteligencia artificial (IA) en los últimos años.

"Estos desafíos de seguridad y privacidad incluyen el potencial de manipulación adversa de los datos de entrenamiento, explotación adversaria de las vulnerabilidades del modelo para afectar negativamente el rendimiento del sistema de IA, e incluso manipulaciones maliciosas, modificaciones o mera interacción con modelos para filtrar información sensible sobre las personas representadas en los datos, sobre el modelo en sí o datos empresariales patentados", informó el NIST.

A medida que los sistemas de IA se integran rápidamente en los servicios en línea, en parte impulsado por la aparición de sistemas de IA generativos como OpenAI ChatGPT y Google Bard, los modelos que impulsan estas tecnologías enfrentan una serie de amenazas en diversas etapas de las operaciones de aprendizaje automático.

Estos incluyen datos de capacitación corruptos, fallas de seguridad en los componentes del software, envenenamiento del modelo de datos, debilidades de la cadena de suministro y violaciones de la privacidad que surgen como resultado de ataques de inyección rápida.

"En su mayor parte, los desarrolladores de software necesitan que más personas utilicen su producto para que pueda mejorar con la exposición", detallaron científicos del NIST. "Pero no hay garantía de que la exposición sea buena. Un chatbot puede arrojar información mala o tóxica cuando se le solicita con un lenguaje cuidadosamente diseñado".

Los ataques, que pueden tener impactos significativos en la disponibilidad, la integridad y la privacidad, se clasifican en términos generales de la siguiente manera:

- Ataques de evasión, que tienen como objetivo generar resultados adversarios después de implementar un modelo.
- Ataques de envenenamiento, que apuntan a la fase de entrenamiento del algoritmo mediante la introducción de datos corruptos.
- Ataques a la privacidad, que tienen como objetivo obtener información confidencial sobre el sistema o los datos con los que fue entrenado planteando preguntas que eluden las barreras de seguridad existentes.
- Ataques de abuso, cuyo objetivo es comprometer fuentes legítimas de información, como una página web con información incorrecta, para reutilizar el uso previsto del sistema.

Dichos ataques, dijo el NIST, pueden ser llevados a cabo por actores de amenazas con pleno conocimiento (caja blanca), conocimiento mínimo (caja negra) o con una comprensión parcial de algunos de los aspectos del sistema de IA (caja gris).

La agencia señaló además la falta de medidas de mitigación sólidas para contrarrestar estos riesgos, e instó a la comunidad tecnológica en general a "idear mejores defensas".

El desarrollo llega más de un mes después de que el Reino Unido, los EE. UU. y socios internacionales de otros 16 países publicaran directrices para el desarrollo de sistemas seguros de inteligencia artificial (IA).

"A pesar de los importantes avances que han logrado la IA y el aprendizaje automático, estas tecnologías son vulnerables a ataques que pueden provocar fallos espectaculares con consecuencias nefastas", afirmó la organización "Hay problemas teóricos con la seguridad de los algoritmos de IA que simplemente no se han resuelto todavía".

Remediación / Referencias

Por mayor información acceder a:

https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems

THE APACHE SOFTWARE FOUNDATION	Vulnerabilidad dia cero en sistema ERP Apache OfBiz	CRÍTICO

Descripción

El día cero crítico en el sistema ERP Apache OfBiz expone a las empresas a ataques.

Estado

Se ha descubierto una nueva falla de seguridad de día cero en Apache OfBiz, un sistema de planificación de recursos empresariales (ERP) de código abierto que podría explotarse para eludir las protecciones de autenticación.

La vulnerabilidad identificada reside en la funcionalidad de inicio de sesión y es el resultado de un parche incompleto para otra vulnerabilidad crítica la cual cuenta con una puntuación CVSS de 9.8 que se lanzó a principios de este mes.

Las medidas de seguridad tomadas para parchearla dejaron intacta la raíz del problema y, por lo tanto, la omisión de autenticación aún estaba presente.

Ahora nos encontramos frente a una falla de ejecución remota de código previamente autenticada que afecta a las versiones anteriores a la 18.12.10 y que, cuando se explota con éxito, podría permitir a los actores de amenazas obtener control total sobre el servidor y desviar datos confidenciales. Se debe a un componente XML-RPC obsoleto dentro de Apache OFBiz.

Esta vulnerabilidad podría activarse utilizando parámetros NOMBRE DE USUARIO y CONTRASEÑA vacíos e inválidos en una solicitud HTTP para devolver un mensaje de autenticación exitosa, eludiendo efectivamente la protección y permitiendo que un actor de amenazas acceda a recursos internos que de otro modo no estarían autorizados.

El ataque depende del hecho de que el parámetro "requirePasswordChange" está establecido en "Y" (es decir, sí) en la URL, lo que provoca que la autenticación se omita trivialmente independientemente de los valores pasados en los campos de nombre de usuario y contraseña.

"La vulnerabilidad permite a los atacantes eludir la autenticación para lograr una falsificación de solicitud del lado del servidor (SSRF) simple", según una descripción de la falla en la Base de datos nacional de vulnerabilidades (NVD) del NIST.

Se han observado "varios" intentos de explotación de esta vulnerabilidad, por lo que es imperativo que los usuarios actúen rápidamente para proteger sus instancias de Apache OFbiz, actualizando a la versión 18.12.11 o posterior lo antes posible para mitigar cualquier amenaza potencial.

Remediación / Referencias

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-51467

https://issues.apache.org/jira/browse/OFBIZ-12873

Conclusiones

La ciberseguridad se ha convertido en una prioridad ineludible. Las amenazas evolucionan a un ritmo alarmante, destacando la necesidad imperante de un monitoreo constante para salvaguardar la integridad de nuestros sistemas y datos. La proliferación de campañas de phishing y la constante divulgación de malware exigen una atención inquebrantable a la seguridad cibernética.

El phishing, en particular, ha alcanzado cotas alarmantes, siendo un anzuelo sofisticado para engañar incluso a los usuarios más precavidos. La clave para enfrentar este desafío radica en el monitoreo constante de las actividades en línea, identificando patrones sospechosos y anticipando posibles amenazas. La ciberseguridad ya no puede ser reactiva; debe ser un proceso dinámico y en tiempo real.

Además, al adentrarnos en la era de la inteligencia artificial, las facilidades que esta tecnología ofrece se entrelazan estrechamente con los riesgos potenciales. La implementación de sistemas de inteligencia artificial sin salvaguardas robustas puede abrir brechas significativas en la seguridad, exponiendo a las organizaciones a vulnerabilidades graves. La combinación de una vigilancia constante y la adopción de sistemas de seguridad sólidos se torna esencial para mitigar los riesgos inherentes al uso de la inteligencia artificial.

En resumen, la ciberseguridad se ha vuelto más vital que nunca. La caza constante de amenazas, en particular, el phishing y la lucha contra el malware, exige una dedicación continua. Mantener sistemas de seguridad robustos, especialmente al implementar la inteligencia artificial, no solo es una medida preventiva, sino un requisito en la preservación de la integridad digital.

En este paradigma de amenazas en constante evolución, la vigilancia y la preparación constante son nuestras mejores defensas.

Desde el equipo de Datasec seguimos protegiendo la seguridad de nuestros clientes, socios y colaboradores.

¡Hasta la próxima!