Boletín de Ciberseguridad N°59

Fecha de publicación: 23/05/2023

Mes de mayo

09/05/2023 – 23/05/2023

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 segunda quincena del mes de mayo se destacan 7 noticias de relevancia: 4 sobre vulnerabilidades tecnológicas, y 3 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Google eliminará gradualmente las cookies de terceros a partir de 2024

Google ha anunciado planes para cambiar oficialmente el interruptor de sus iniciativas de Privacy Sandbox, lentamente eliminará el soporte para cookies de terceros en el navegador Chrome.

AWS: utilizado en operaciones de criptominería

Se ha observado a un actor de amenazas con motivación financiera de origen indonesio que aprovecha las instancias de Amazon Web Services (AWS) Elastic Compute Cloud (EC2) para llevar a cabo operaciones ilícitas de criptominería.

Samsung bajo ataque: nueva falla de seguridad expuesta

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) advirtió sobre la explotación activa de una falla de gravedad media que afecta a los dispositivos Samsung.

Vulnerabilidad Crítica

SAMSUNG	**Samsung bajo ataque: nueva falla de seguridad expuesta**	CRÍTICO

Descripción

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) advirtió sobre la explotación activa de una falla de gravedad media que afecta a los dispositivos Samsung.

Estado

El ataque cuenta con un puntaje CVSS de 4.4, afecta a dispositivos Samsung seleccionados que ejecutan las versiones 11, 12 y 13 de Android.

El gigante de la electrónica de Corea del Sur describió el problema como una falla de divulgación de información que podría ser aprovechada por un atacante privilegiado para eludir las protecciones de aleatorización del diseño del espacio de direcciones (ASLR).

ASLR es una técnica de seguridad diseñada para evitar la corrupción de la memoria y las fallas en la ejecución del código ocultando la ubicación de un ejecutable en la memoria de un dispositivo.

Samsung, en un aviso publicado este mes, dijo que fue "notificado de que había existido un exploit para este problema", y agregó que se reveló de forma privada a la compañía el 17 de enero de 2023.

Actualmente no se conocen otros detalles sobre cómo se explota la falla, pero en el pasado los vendedores comerciales de spyware han utilizado las vulnerabilidades en los teléfonos Samsung para implementar software malicioso.

A la luz del abuso activo, CISA agregó la deficiencia a su catálogo de vulnerabilidades conocidas explotadas (KEV).

Una hoja de cálculo de seguimiento mantenida por Google Project Zero que documenta casos conocidos de exploits de día cero detectados muestra que la vulnerabilidad de seguridad de Samsung fue descubierta por el Google Threat Analysis Group (TAG), lo que indica un posible abuso en relación con una campaña de spyware.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/05/samsung-devices-under-active.html

	KeePass: exploit permite recuperar contraseñas maestras de la memoria	CRÍTICO

Descripción

Se puso a disposición una prueba de concepto (PoC) para una falla de seguridad que afecta al administrador de contraseñas KeePass que podría explotarse para recuperar la contraseña maestra de una víctima en texto sin cifrar en circunstancias específicas.

Estado

Afecta las versiones 2.x de KeePass para Windows, Linux y macOS, y se espera que se corrija en la versión 2.54, que probablemente se lanzará a principios del próximo mes.

Además del primer carácter de la contraseña, en su mayoría es capaz de recuperar la contraseña en texto sin formato. No se requiere la ejecución de código en el sistema de destino, solo un volcado de memoria.

No importa de dónde provenga la memoria, no importa si el espacio de trabajo está bloqueado o no. También es posible volcar la contraseña de la RAM después de que KeePass ya no se esté ejecutando, aunque la posibilidad de que eso funcione disminuye con el tiempo que ha pasado desde entonces.

Vale la pena señalar que la explotación exitosa de los bancos de fallas con la condición de que un atacante ya haya comprometido la computadora de un objetivo potencial. También requiere que la contraseña se escriba en un teclado y no se copie del portapapeles del dispositivo.

La vulnerabilidad tiene que ver con la forma en que un campo de cuadro de texto personalizado utilizado para ingresar la contraseña maestra maneja la entrada del usuario. Específicamente, se ha descubierto que deja rastros de cada carácter que el usuario escribe en la memoria del programa.

Esto conduce a un escenario en el que un atacante podría volcar la memoria del programa y volver a ensamblar la contraseña en texto sin formato con la excepción del primer carácter.

Remediación / Referencias

Se recomienda a los usuarios que actualicen a KeePass 2.54 una vez que esté disponible.

Por mayor información acceder a:

https://thehackernews.com/2023/05/keepass-exploit-allows-attackers-to.html

python Package Index	**Repositorio de PyPI bajo ataque**	CRÍTICO

Descripción

Python Package Index (PyPI), el repositorio oficial de software de terceros para el lenguaje de programación Python, ha deshabilitado temporalmente la capacidad de los usuarios para registrarse y cargar nuevos paquetes hasta nuevo aviso.

Estado

El volumen de usuarios maliciosos y proyectos maliciosos que se crearon en el índice durante la última semana ha superado la capacidad para responder de manera oportuna, especialmente con varios administradores de PyPI en licencia, según informaron administradores.

No se revelaron detalles adicionales sobre la naturaleza del malware y los actores de amenazas involucrados en la publicación de esos paquetes maliciosos en PyPI.

La decisión de congelar los registros de nuevos usuarios y proyectos se produce cuando los registros de software como PyPI han demostrado una y otra vez que son un objetivo popular para los atacantes que buscan envenenar la cadena de suministro de software y comprometer los entornos de desarrollo.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/05/pypi-repository-under-attack-user-sign.html

AWS: utilizado en operaciones de criptominería

CRÍTICO

Descripción

Se ha observado a un actor de amenazas con motivación financiera de origen indonesio que aprovecha las instancias de Amazon Web Services (AWS) Elastic Compute Cloud (EC2) para llevar a cabo operaciones ilícitas de criptominería.

Estado

Permiso P0 Labs, de la compañía de seguridad en la nube, que detectó por primera vez al grupo en noviembre de 2021, le asignó el apodo GUI-vil.

El grupo muestra una preferencia por las herramientas de interfaz gráfica de usuario (GUI), específicamente el navegador S3 (versión 9.5.5) para sus operaciones iniciales. Al obtener acceso a la consola de AWS, realizan sus operaciones directamente a través del navegador web.

Las cadenas de ataque montadas por GUI-vil implican obtener acceso inicial mediante el armamento de claves de AWS en repositorios de código fuente expuestos públicamente en GitHub o escaneando instancias de GitLab que son vulnerables a fallas de ejecución remota de código.

A un ingreso exitoso le sigue una escalada de privilegios y un reconocimiento interno para revisar todos los depósitos S3 disponibles y determinar los servicios a los que se puede acceder a través de la consola web de AWS.

Un aspecto notable del modus operandi del actor de amenazas es su intento de mezclarse y persistir dentro del entorno de la víctima mediante la creación de nuevos usuarios que se ajustan a la misma convención de nomenclatura y, en última instancia, cumplen sus objetivos.

“GUI-vil también creará claves de acceso para las nuevas identidades que están creando para que puedan continuar usando el navegador S3 con estos nuevos usuarios", informó la compañía.

Alternativamente, también se ha visto al grupo creando perfiles de inicio de sesión para usuarios existentes que no los tienen para permitir el acceso a la consola de AWS sin generar señales de alerta.

Los vínculos de GUI-vil con Indonesia se derivan del hecho de que las direcciones IP de origen asociadas con las actividades están vinculadas a dos Números de Sistema Autónomo (ASN) ubicados en el país del sudeste asiático.

La misión principal del grupo, impulsada financieramente, es crear instancias EC2 para facilitar sus actividades de criptominería. En muchos casos, las ganancias que obtienen de la criptominería son solo una pequeña parte del gasto que las organizaciones víctimas tienen que pagar por ejecutar las instancias EC2.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/05/indonesian-cybercriminals-exploit-aws.html

Prevención

Apple emite parches de emergencia para 3 nuevas vulnerabilidades de día cero

PREVENCIÓN

Descripción

Apple lanzó el jueves actualizaciones de seguridad para iOS, iPadOS, macOS, tvOS, watchOS y el navegador web Safari para abordar docenas de fallas, incluidos tres nuevos días cero que, según informó, se están explotando activamente en la naturaleza.

Estado

Las tres deficiencias de seguridad se enumeran a continuación:

- Una falla de WebKit que podría ser aprovechada por un actor malicioso para salir del entorno limitado de contenido web. Se solucionó con controles de límites mejorados.
- Un problema de lectura fuera de los límites en WebKit que podría abusarse para revelar información confidencial al procesar contenido web. Se solucionó mejorando la validación de entrada.
- Un error gratuito de uso posterior en WebKit que podría conducir a la ejecución de código arbitrario al procesar contenido web creado con fines malintencionados. Se solucionó mejorando la gestión de la memoria.

Vale la pena señalar que las dos primeras deficiencias se parchearon como parte de las actualizaciones de Rapid Security Response: iOS 16.4.1 (a) y iPadOS 16.4.1 (a), que la compañía lanzó al comienzo del mes.

Actualmente no hay detalles técnicos adicionales sobre las fallas, la naturaleza de los ataques o la identidad de los actores de amenazas que pueden estar explotándolos.

Dicho esto, tales debilidades se han aprovechado históricamente como parte de intrusiones altamente dirigidas para desplegar spyware mercenario en los dispositivos de disidentes, periodistas y activistas de derechos humanos, entre otros.

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

- iOS 16.5 y iPadOS 16.5: iPhone 8 y posteriores, iPad Pro (todos los modelos), iPad Air de 3.ª generación y posteriores, iPad de 5.ª generación y posteriores y iPad mini de 5.ª generación y posteriores
- iOS 15.7.6 y iPadOS 15.7.6: iPhone 6s (todos los modelos), iPhone 7 (todos los modelos), iPhone SE (1.ª generación), iPad Air 2, iPad mini (4.ª generación) y iPod touch (7.ª generación)
- macOS Ventura 13.4 - macOS Ventura
- tvOS 16.5 - Apple TV 4K (todos los modelos) y Apple TV HD
- watchOS 9.5 - Apple Watch Serie 4 y posterior

- Safari 16.5: macOS Big Sur y macOS Monterey

Hasta ahora, Apple ha reparado un total de seis días cero explotados activamente desde el comienzo de 2023.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/05/webkit-under-attack-apple-issues.html

Descripción

Google ha anunciado planes para cambiar oficialmente el interruptor de sus iniciativas de Privacy Sandbox, lentamente eliminará el soporte para cookies de terceros en el navegador Chrome.

Estado

El gigante informó que tiene la intención de eliminar gradualmente las cookies de terceros para el 1% de los usuarios de Chrome en todo el mundo en el primer trimestre de 2024.

Esto ayudará a los desarrolladores a realizar experimentos en el mundo real que evalúen la preparación y la eficacia de sus productos sin cookies de terceros.

Antes de la implementación, Google informó que introduciría la capacidad para que los desarrolladores externos simulen el proceso para un subconjunto configurable de sus usuarios (hasta el 10 %) en el cuarto trimestre de 2023.

Google enfatizó además que los planes se diseñaron y desarrollaron con supervisión regulatoria y aportes de la Autoridad de Mercados y Competencia (CMA) del Reino Unido, que supervisa la implementación para garantizar que las propuestas no inclinen la igualdad de condiciones en el negocio de la empresa.

Privacy Sandbox es un proyecto doble para la web y Android que tiene como objetivo limitar el seguimiento encubierto eliminando la necesidad de cookies de terceros e identificadores de aplicaciones cruzadas y aún ofreciendo contenido y anuncios relevantes de una manera que preserva la privacidad.

Google, a principios de febrero, comenzó a probar Privacy Sandbox en Android en versión beta para dispositivos móviles elegibles con Android 13.

Se espera que las API de Privacy Sandbox, incluidos los temas, estén disponibles en general para todos los usuarios sin la necesidad de participar en una prueba de origen en Chrome 115, que se lanzará a finales de julio de 2023.

La idea, en pocas palabras, es inferir señales de interés de grano grueso (llamados temas) en el dispositivo en función de la actividad de navegación de los usuarios durante un período de una semana (llamado epoch) y compartir esa información con los proveedores de tecnología publicitaria para publicar anuncios dirigidos.

También tiene como objetivo dar a los usuarios el control sobre sus intereses en evolución, con las categorías seleccionadas para cada época seleccionadas al azar de los temas vistos con más frecuencia para ese período de tiempo.

El objetivo de Google es desactivar por completo las cookies de terceros en Chrome en la segunda mitad de 2024, aunque la compañía señaló que la línea de tiempo podría cambiar según las discusiones, los comentarios y las pruebas de las partes interesadas.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/05/privacy-sandbox-initiative-google-to.html

¿Buscando herramientas de IA? Cuidado con los sitios no autorizados

PREVENCIÓN

Descripción

Los anuncios maliciosos de búsqueda de Google para servicios de IA generativa como OpenAI ChatGPT y Midjourney se utilizan para dirigir a los usuarios a sitios web incompletos como parte de una campaña BATLOADER diseñada para entregar el malware RedLine Stealer.

Estado

Ambos servicios de IA son extremadamente populares, pero carecen de aplicaciones independientes propias, es decir, los usuarios interactúan con ChatGPT a través de su interfaz web, mientras que Midjourney usa Discord.

Este vacío ha sido explotado por actores de amenazas que buscan llevar a los buscadores de aplicaciones de IA a páginas web impostoras que promocionan aplicaciones falsas".

BATLOADER es un malware de carga que se propaga a través de descargas ocultas en las que los usuarios que buscan ciertas palabras clave en los motores de búsqueda ven anuncios falsos que, cuando se hace clic, los redireccionan a páginas de destino falsas que alojan malware.

El archivo de instalación está equipado con un archivo ejecutable (ChatGPT.exe o midjourney.exe) y un script de PowerShell (Chat.ps1 o Chat-Ready.ps1) que descarga y carga RedLine Stealer desde un servidor remoto.

Una vez que se completa la instalación, el binario utiliza Microsoft Edge WebView2 para cargar chat.openai[.]com o www.midjourney[.]com, las URL legítimas de ChatGPT y Midjourney, en una ventana emergente para no mostrar cualquier bandera roja.

El uso del adversario de ChatGPT y señuelos temáticos de Midjourney para publicar anuncios maliciosos y, en última instancia, eliminar el malware RedLine Stealer también fue destacado la semana pasada por investigadores.

Esta no es la primera vez que los operadores detrás de BATLOADER capitalizan la moda de la IA para distribuir malware. Investigadores de ciberseguridad señalaron además que el abuso de los anuncios de búsqueda de Google ha disminuido desde su pico de principios de 2023, lo que sugiere que el gigante tecnológico está tomando medidas activas para reducir su explotación.

El desarrollo se alinea con una ola más amplia de campañas de phishing y estafa, en las que los actores de amenazas intentan sacar provecho del uso creciente de estas herramientas de inteligencia artificial para distribuir malware y otras aplicaciones falsas.

El proveedor de seguridad Sophos, en una investigación relacionada, describió un conjunto de aplicaciones de fleeceware relacionadas con ChatGPT en Google Play y Apple App Store, denominadas colectivamente FleeceGPT, que obligan a los usuarios a suscribirse a suscripciones no deseadas.

"Debido a que las aplicaciones de fleeceware están diseñadas para mantenerse al margen de los términos de servicio de Apple y Google y no acceden a información privada ni intentan eludir la seguridad de la plataforma, rara vez se rechazan durante la revisión y se permiten en las tiendas de aplicaciones", informaron investigadores de Sophos.

En las últimas semanas, Check Point, Meta han advertido sobre el aumento de la actividad fraudulenta que imita el servicio ChatGPT para recopilar los datos de las tarjetas de crédito de los usuarios, perpetrar fraudes con tarjetas de crédito y robar los datos de las cuentas de Facebook de las víctimas a través del navegador web imitador de chatbot. extensiones

Entre noviembre de 2022 y principios de abril de 2023, se ha detectado un aumento del 910 % en los registros mensuales de dominios relacionados con ChatGPT.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/05/searching-for-ai-tools-watch-out-for.html

Conclusiones

La utilización de la inteligencia artificial con fines fraudulentos es un triste ejemplo de cómo una herramienta innovadora puede ser mal utilizada para dañar a los demás. En un mundo cada vez más digitalizado, donde confiamos en la tecnología para realizar nuestras transacciones y compartir información personal, es crucial estar conscientes de los peligros que acechan en línea y cómo protegernos.

La proliferación de estafas y engaños impulsados por la inteligencia artificial ha alcanzado proporciones alarmantes. Los delincuentes han encontrado formas ingeniosas de aprovecharse de la confianza y la vulnerabilidad de las personas, utilizando sofisticados algoritmos y técnicas de manipulación para engañar a las víctimas y obtener acceso a sus datos confidenciales. Desde correos electrónicos de phishing hasta llamadas telefónicas falsas, estas tácticas se han vuelto cada vez más sofisticadas y difíciles de detectar.

Ante esta realidad, es fundamental que todos nos eduquemos y tomemos medidas proactivas para salvaguardar nuestra privacidad y seguridad.

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

¡Hasta la próxima!