Boletín de Ciberseguridad N°62

Fecha de publicación: 10/07/2023

Mes de julio

26/06/2023 – 10/07/2023

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 julio se destacan 6 noticias de relevancia: 4 sobre vulnerabilidades tecnológicas, y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Nueva función de Mozilla bloquea complementos riesgosos

Mozilla ha anunciado que se puede bloquear la ejecución de algunos complementos en ciertos sitios como parte de una nueva función llamada Dominios en cuarentena.

Nickelodeon sufre una fuga de datos de 500GB

La compañía de televisión estadounidense Nickelodeon ha sufrido una supuesta fuga de datos de 500GB de información propietaria, incluidos detalles de programas inéditos.

Juego de Super Mario utilizado para propagar malware

Un instalador troyanizado para el juego de Nintendo está propagando malware de criptominería.

Vulnerabilidad Crítica

	Juego de Super Mario utilizado para propagar malware	CRÍTICO

Descripción

Un instalador troyanizado para el juego de Nintendo está propagando malware de criptominería.

Estado

Se está utilizando un instalador troyanizado para el popular juego de Nintendo Super Mario Forever para propagar malware.

Los investigadores descubrieron que los actores maliciosos estaban propagando un minero Monero (XMR), un cliente de minería SupremeBot y un ladrón Umbral de código abierto, todo incluido con un instalador legítimo para Super Mario Forever.

Una vez que se ha instalado correctamente en un dispositivo y se inicia el juego, el malware ejecuta en secreto archivos de malware en el dispositivo infectado. El minero XMR usa el dispositivo infectado para extraer la criptomoneda Monero. El minero opera discretamente en los procesos de fondo del dispositivo, lo que significa que la minería no autorizada está oculta para la víctima.

El minero XMR también recolecta datos de la computadora de la víctima, incluido el nombre de la computadora, el nombre de usuario, la unidad de procesamiento de gráficos y la unidad central de procesamiento, y los transfiere a un centro de comando y control.

El cliente de minería SupremeBot ejecuta procesos en el dispositivo infectado para recuperar y ejecutar software malicioso de robo de datos desde un centro de comando y control hasta el dispositivo. Esto luego descarga el ladrón de Umbral en la memoria de proceso del dispositivo. Luego, el ladrón de Umbral recopila rápidamente datos del dispositivo y los envía al actor malintencionado que cargó el software troyanizado a través de la plataforma de mensajería instantánea Discord utilizando webhooks.

Investigadores señalaron que el ladrón de Umbral puede ejecutar los siguientes procesos:

- Capturas de pantalla.
- Recuperación de contraseñas y cookies del navegador.
- Captura de imágenes de la cámara web.
- Obtención de archivos de sesión de Telegram y tokens de Discord.
- Adquirir cookies de Roblox y archivos de sesión de Minecraft.
- Recopilación de archivos asociados con billeteras de criptomonedas.

Juntos, este paquete de carga maliciosa puede afectar significativamente a las víctimas, tanto monetariamente a través de criptomonedas robadas o transferencias bancarias fraudulentas como materialmente, a través del impacto que tendrá la criptominería en su

dispositivo. Esto se debe a que la criptominería interrumpe masivamente los procesos de un sistema y agota sus recursos.

Remediación / Referencias

Por mayor información acceder a:

https://www.cshub.com/malware/news/super-mario-game-used-to-spread-malware

	Proveedor de Apple sufre ataque de ransomware de 70 millones de dólares	CRÍTICO

Descripción

El fabricante y proveedor de semiconductores de la empresa de tecnología Apple, Taiwan Semiconductor Manufacturing Company (TSMC), ha sufrido una filtración de datos relacionada con un ataque de ransomware de terceros.

Estado

El ataque fué lanzado por la pandilla rusa de ransomware, LockBit, contra uno de los proveedores de TSMC, Kinmax Technology. La pandilla confirmó el ataque cibernético a través de una publicación en su sitio de fugas en la dark web donde nombró a TSMC como víctima. LockBit exigió que la empresa les pagara 70 millones de dólares o la pandilla publicaría en línea los datos robados durante el ataque.

La pandilla también informó que “en caso de rechazo de pago”, también publicará puntos de entrada a la red y contraseñas e información de inicio de sesión, así como los datos robados. LockBit, sin embargo, aún no ha publicado pruebas firmes de los datos que afirma haber robado.

La demanda de rescate es una de las mayores demandas de ransomware jamás realizadas, según investigadores del área.

Un portavoz anónimo de TSMC confirmó el ataque a través de un correo electrónico, en su declaración, el portavoz dijo que un "incidente de seguridad cibernética" en Kinmax Technology había provocado la filtración de "información pertinente a la configuración y configuración inicial del servidor".

Según el portavoz, el incidente no afectó las operaciones comerciales de TSMC ni provocó que la información de los clientes de TSMC se viera comprometida.

Después del incidente, TSMC finalizó de inmediato su intercambio de datos con este proveedor en cuestión de acuerdo con los protocolos de seguridad y los procedimientos operativos estándar de la Compañía.

En un aviso sobre la infracción, Kinmax Technology dijo que el ataque cibernético se lanzó contra su entorno de prueba interno, lo que provocó una fuga de datos. La empresa dijo que la información filtrada "consistía principalmente en la preparación de la instalación del sistema que la empresa proporcionaba a nuestros clientes como configuraciones predeterminadas".

Kinmax Technology expresó su disculpa a los clientes afectados, pero no dio ninguna información sobre cuántos de sus clientes se vieron afectados por este ataque.

Remediación / Referencias

Por mayor información acceder a:

https://www.cshub.com/attacks/news/apple-supplier-faces-70-million-ransomware-attack

nickelodeon	**Nickelodeon sufre una fuga de datos de 500GB**	CRÍTICO

Descripción

La compañía de televisión estadounidense Nickelodeon ha sufrido una supuesta fuga de datos de 500GB de información propietaria, incluidos detalles de programas inéditos.

Estado

La noticia de la filtración fué compartida por un usuario de Twitter que usa el nombre de pantalla GhostyTongue. El usuario de Twitter compartió un video que mostraba varios archivos supuestamente pertenecientes a Nickelodeon que habían sido robados y distribuidos, incluidos detalles de programas y guiones inéditos.

Aparentemente, la fuga de datos fue causada por una vulnerabilidad de autenticación dentro del portal de experiencia y productos de consumo de Nickelodeon, que permitió el acceso no autorizado a contenido confidencial dentro del departamento de animación de Nickelodeon. La vulnerabilidad del software que condujo al ataque cibernético supuestamente fue reparada dos meses después.

El robo de datos supuestamente tuvo lugar en enero de 2023, y la información se compartió inicialmente en Discord. Dos usuarios de Discord, que usan los nombres de pantalla BowDown e IncidentalSeventy, fueron vinculados al ataque cibernético de GhostyTongue, quien afirmó que "los federales los han derribado" y que "van a ir a los tribunales pronto".

Según los informes, Nickelodeon ha tomado medidas contra la fuga de datos, presentando eliminaciones de la Ley de derechos de autor del milenio digital (DMCA) para que los datos se desconecten.

Ghosty Tongue luego se sumó a los reclamos el 2 de julio, agregando que un servidor de discordia privado había compartido una URL de descarga a un nuevo conjunto de información robada de Nickelodeon, posiblemente durante el primer ataque cibernético. Los datos robados supuestamente incluyen el código fuente de todos los juegos flash de Nickelodeon.

La gente recurrió a otros sitios de redes sociales para discutir la filtración, y un usuario del sitio de redes sociales 4chan afirmó que los sistemas internos de Nickelodeon habían estado comprometidos durante más de un año. El usuario alegó que las comunidades privadas en línea han estado compartiendo datos por valor de 500 GB, incluidos archivos de animación, documentos de Photoshop y guiones.

Estas afirmaciones coinciden con las acusaciones y el clip compartido por GhostyTongue en Twitter, sin embargo, Nickelodeon aún no ha confirmado el ataque cibernético y la posterior filtración de datos.

Las compañías de televisión pueden ser un objetivo atractivo para los piratas informáticos, ya que la información que transmiten es valiosa para varias personas, no solo para los actores malintencionados.

Remediación / Referencias

Por mayor información acceder a:

https://www.cshub.com/attacks/news/iotw-nickelodeon-allegedly-suffers-500gb-data-leak

Troyano bancario TOITOIN dirigido a empresas latinoamericanas

CRÍTICO

Descripción

Las empresas que operan en la región de América Latina (LATAM) son el objetivo de un nuevo troyano bancario basado en Windows llamado TOITOIN desde mayo de 2023.

Estado

Investigadores informan que esta campaña sofisticada emplea un troyano que sigue una cadena de infección de múltiples etapas, utilizando módulos especialmente diseñados en cada etapa.

Estos módulos están diseñados a medida para llevar a cabo actividades maliciosas, como inyectar código dañino en procesos remotos, eludir el Control de cuentas de usuario a través de COM Elevation Moniker y evadir la detección de Sandboxes a través de técnicas inteligentes como reinicios del sistema y verificaciones de procesos principales.

El esfuerzo de seis etapas tiene todas las características de una secuencia de ataque bien diseñada, comenzando con un correo electrónico de phishing que contiene un enlace incrustado que apunta a un archivo ZIP alojado en una instancia de Amazon EC2 para evadir las detecciones basadas en el dominio.

Los mensajes de correo electrónico aprovechan un señuelo con el tema de la factura para engañar a los destinatarios involuntarios para que los abran, activando así la infección. Dentro del archivo ZIP hay un ejecutable de descarga que está diseñado para configurar la persistencia por medio de un archivo LNK en la carpeta de inicio de Windows y comunicarse con un servidor remoto para recuperar seis cargas útiles de la próxima etapa en forma de archivos MP3.

El descargador también es responsable de generar un script por lotes que reinicia el sistema después de un tiempo de espera de 10 segundos. Esto se hace para evadir la detección de sandbox, ya que las acciones maliciosas ocurren sólo después del reinicio.

Entre las cargas útiles obtenidas se incluye "icepdfeditor.exe", un binario válido firmado por ZOHO Corporation Private Limited, que, cuando se ejecuta, descarga una DLL no autorizada ("ffmpeg.dll") con el nombre en código Krita Loader.

El cargador, por su parte, está diseñado para decodificar un archivo JPG descargado junto con las otras cargas útiles y lanzar otro ejecutable conocido como el módulo InjectorDLL que invierte un segundo archivo JPG para formar lo que se llama el módulo ElevateInjectorDLL.

Posteriormente, el componente InjectorDLL pasa a inyectar ElevateInjectorDLL en el proceso "explorer.exe", luego de lo cual se realiza una omisión del Control de cuentas de usuario (UAC), si es necesario, para elevar los privilegios del proceso y el troyano TOITOIN se descifra e inyecta en el " proceso svchost.exe".

Esta técnica permite que el malware manipule los archivos del sistema y ejecute comandos con privilegios elevados, lo que facilita más actividades maliciosas.

TOITOIN viene con capacidades para recopilar información del sistema, así como datos de recolección de navegadores web instalados como Google Chrome, Microsoft Edge e Internet Explorer, Mozilla Firefox y Opera. Además, verifica la presencia de Topaz Online Fraud Detection (OFD), un módulo antifraude integrado en las plataformas bancarias en la región LATAM.

Actualmente se desconoce la naturaleza de las respuestas del servidor de comando y control (C2) debido a que el servidor ya no está disponible.

A través de correos electrónicos de phishing engañosos, mecanismos de redireccionamiento intrincados y diversificación de dominios, los actores de amenazas entregan con éxito su carga maliciosa. La cadena de infección de múltiples etapas observada en esta campaña implica el uso de módulos desarrollados a medida que emplean varias técnicas de evasión y métodos de encriptación.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/07/new-toitoin-banking-trojan-targeting.html

Prevención

Google parchea 3 vulnerabilidades explotadas activamente en Android

PREVENCIÓN

Descripción

Google ha lanzado sus actualizaciones de seguridad mensuales para el sistema operativo Android, abordando 46 nuevas vulnerabilidades de software. Entre estas, se han identificado tres vulnerabilidades que se explotan activamente en ataques dirigidos.

Estado

Una de las vulnerabilidades rastreadas, se trata de una falla de fuga de memoria que afecta al controlador de GPU Arm Mali para chips Bifrost, Avalon y Valhall. Esta vulnerabilidad en particular se aprovechó en un ataque anterior que permitió la infiltración de spyware en dispositivos Samsung en diciembre de 2022.

Esta vulnerabilidad se consideró lo suficientemente grave como para que la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) emitiera una orden de parcheo para las agencias federales en abril de 2023.

Otra vulnerabilidad importante, es un problema de alta gravedad que afecta a versiones específicas de los controladores de núcleo de GPU Bifrost y Midgard Arm Mali. Esta falla permite que un usuario sin privilegios obtenga acceso no autorizado a datos confidenciales y aumente los privilegios al nivel raíz.

La tercera vulnerabilidad explotada, se trata de un error de gravedad crítica descubierto en Skia, la biblioteca de gráficos 2D multiplataforma de código abierto de Google. Inicialmente se reveló como una vulnerabilidad de día cero en el navegador Chrome y permite que un atacante remoto que se ha hecho cargo del proceso de representación realice un escape de sandbox e implemente código remoto en dispositivos Android.

Además de estos, el boletín de seguridad de Android de julio de Google destaca otra vulnerabilidad crítica, que afecta al componente del sistema Android. Este problema puede causar la ejecución remota de código sin interacción del usuario o privilegios de ejecución adicionales, lo que lo hace particularmente precario.

Estas actualizaciones de seguridad se implementan en dos niveles de parches. El nivel de parche inicial, disponible el 1 de julio, se centra en los componentes principales de Android y aborda 22 defectos de seguridad en los componentes Framework y System.

El segundo nivel de parche, lanzado el 5 de julio, tiene como objetivo los componentes de código cerrado y kernel, y aborda 20 vulnerabilidades en los componentes Kernel, Arm, Imagination Technologies, MediaTek y Qualcomm.

Es importante tener en cuenta que el impacto de las vulnerabilidades abordadas puede extenderse más allá de las versiones compatibles de Android (11, 12 y 13), lo que podría afectar a las versiones anteriores del sistema operativo que ya no reciben soporte oficial.

Google ha lanzado además parches de seguridad específicos para sus dispositivos Pixel, que se ocupan de 14 vulnerabilidades en los componentes Kernel, Pixel y Qualcomm. Dos de estas debilidades críticas podrían resultar en ataques de denegación de servicio y elevación de privilegios.

Remediación / Referencias

Por mayor información acceder a:

https://source.android.com/docs/security/bulletin/2023-07-01?hl=es-419

https://thehackernews.com/2023/07/google-releases-android-patch-update.html

Descripción

Mozilla ha anunciado que se puede bloquear la ejecución de algunos complementos en ciertos sitios como parte de una nueva función llamada Dominios en cuarentena.

Estado

Se ha introducido una nueva función de back-end para permitir que solo algunas extensiones monitoreadas por Mozilla se ejecuten en sitios web específicos por varias razones, incluidas las preocupaciones de seguridad.

La compañía dijo que la apertura que ofrece el ecosistema de complementos podría ser explotada por actores malintencionados en su beneficio.

"Esta característica nos permite prevenir ataques de actores maliciosos que se dirigen a dominios específicos cuando tenemos razones para creer que puede haber complementos maliciosos que aún no hemos descubierto", dijo Mozilla en un documento de soporte.

Se espera que los usuarios tengan más control sobre la configuración de cada complemento, comenzando con la versión 116 de Firefox. Dicho esto, se puede desactivar cargando "about:config" en la barra de direcciones y configurando "extensions.quarantinedDomains.enabled" en FALSO.

El desarrollo se suma a la capacidad existente de Mozilla para deshabilitar de forma remota extensiones individuales que representan un riesgo para la privacidad y seguridad del usuario.

Vale la pena señalar que la advertencia aparece en la ventana emergente de Extensiones en lugar del icono de Extensiones en la implementación actual, por lo que las alertas no se muestran si se fija un complemento a la barra de herramientas.

Resulta que cuando anclas una extensión a la barra de herramientas, ya no aparece en la ventana emergente Extensiones", señalaron investigadores de seguridad.

En consecuencia, la advertencia de dominios en cuarentena ya no aparece en la ventana emergente de Extensiones. De hecho, ya no hay una ventana emergente de Extensiones: al hacer clic en el ícono de la barra de herramientas de Extensiones, simplemente se abre la página about:addons, que no muestra la advertencia de dominios en cuarentena en ninguna parte.

Este es un diseño de interfaz de usuario terrible para la nueva función llamada 'seguridad', que deshabilita silenciosamente las extensiones mientras oculta la advertencia al usuario.

Mozilla ha dicho que tiene la intención de mejorar la experiencia del usuario en futuras versiones, aunque no dio una línea de tiempo definitiva.

El cambio también se produce cuando Mozilla denunció una propuesta de bloqueo de sitios web basada en navegador presentada por Francia que requeriría que los proveedores de navegadores establezcan mecanismos para bloquear obligatoriamente los sitios web presentes en una lista proporcionada por el gobierno para abordar el fraude en línea.

“Tal movimiento anulará décadas de normas de moderación de contenido establecidas y proporcionará un libro de jugadas para gobiernos autoritarios que negará fácilmente la existencia de herramientas para eludir la censura”, dijo la compañía.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/07/new-mozilla-feature-blocks-risky-add.htm

Conclusiones

La seguridad de la información se ha convertido en un tema de vital importancia en el mundo digital actual. El uso cada vez más frecuente de malware sofisticado ha demostrado la necesidad urgente de implementar medidas de prevención y protección adecuadas.

La evolución constante de las tecnologías ha permitido el desarrollo de malware altamente avanzado, capaz de infiltrarse en sistemas y redes con el propósito de acceder, robar o corromper información sensible. Estos ataques representan una amenaza significativa tanto para individuos como para organizaciones, ya que pueden causar daños financieros, pérdida de reputación y violaciones a la privacidad.

Es fundamental que los usuarios de la tecnología estén conscientes de los riesgos asociados con la seguridad de la información y adopten medidas proactivas para protegerse. Esto implica implementar prácticas sólidas de higiene digital, como mantener el software actualizado, utilizar contraseñas seguras y evitar hacer clic en enlaces o descargar archivos sospechosos.

La seguridad de la información es un desafío constante en un mundo digital en constante evolución. Al adoptar prácticas seguras y utilizar soluciones de seguridad adecuadas, tanto a nivel individual como organizacional, podemos mitigar los riesgos y salvaguardar nuestra información valiosa en el entorno digital actual.

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

¡Hasta la próxima!