Boletín de Ciberseguridad N°66

Fecha de publicación: 11/09/2023

Mes de setiembre

28/08/2023 – 11/09/2023

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 septiembre se destacan 6 noticias de relevancia, siendo estas 5 sobre vulnerabilidades tecnológicas y una de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Grupo de ciberdelincuentes Lockbit ataca empresas en todo el mundo

En los últimos meses, el grupo de ciberdelincuentes conocido como Lockbit ha estado haciendo titulares por sus ataques cibernéticos dirigidos a empresas en todo el mundo.

Discord.io expone datos de más de 760.000 usuarios

Un actor malintencionado puso a la venta la información en la dark web, correspondiente a datos personales de más de 760.000 usuarios.

Banda de ransomware roba 1.3 TB de datos de Sabre

La banda de ransomware Dunghill Leak publicó capturas de pantalla de los datos supuestamente robados en la dark web.

Vulnerabilidad Crítica

Sabre Travel Network	**Banda de ransomware roba 1.3 TB de datos de Sabre**	CRÍTICO

Descripción

La banda de ransomware Dunghill Leak publicó capturas de pantalla de los datos supuestamente robados en la dark web.

Estado

La banda de ransomware Dunghill Leak se ha atribuido la responsabilidad de un ciberataque contra la empresa de reservas de viajes Sabre.

Dunghill afirmó en una publicación en su sitio de filtración de datos en la dark web que había robado 1.3 terabytes de datos de Sabre, incluida información financiera corporativa, datos de rotación de pasajeros y venta de boletos e información personal de los empleados.

La banda de ransomware validó sus afirmaciones al compartir una parte de los datos robados, prometiendo que el resto de los datos estarán "disponibles pronto". A través de las capturas de pantalla de los datos proporcionados, se descubrió que la información de los empleados supuestamente robada incluye direcciones de correo electrónico de los empleados, lugares de trabajo, nombres, nacionalidades, números de pasaporte y visa e incluso los formularios I-9 de EE. UU. de ciertos empleados. De los pasaportes proporcionados, se confirmó que muchos de ellos eran de empleados actuales de Sabre, incluido un vicepresidente.

Sabre ha informado que se encuentra investigando las afirmaciones del grupo sobre un ciberataque. La portavoz de Sabre, informó que la empresa está al tanto de las afirmaciones de exfiltración de datos realizadas por el grupo de amenazas y actualmente se está investigando para determinar su validez.

Actualmente no se sabe cuándo ni cómo se produjo la filtración de datos, sin embargo, las capturas de pantalla proporcionadas por Dunghill implican que ocurrió alrededor de julio de 2022.

Remediación / Referencias

Por mayor información acceder a:

https://www.cshub.com/malware/news/iotw-ransomware-gang-steals-13tb-of-data-from-sabre

ROBLOX	**Desarrolladores de Roblox atacados con malware**	CRÍTICO

Descripción

Se han lanzado ataques de malware para robar información contra desarrolladores de Roblox.

Estado

Según informes, los desarrolladores del popular juego de plataformas en línea Roblox están siendo atacados con un malware que roba información.

Un actor malicioso desconocido ha estado sembrando docenas de paquetes de software de código abierto con malware denominado 'LunaGrabber', a partir del 1 de agosto de 2023. Se ha engañado a los desarrolladores para que hagan clic en los paquetes de software plagados de malware, ya que están disfrazados de uso común. Esto incluye el código legítimo que los desarrolladores buscaban y que también se incluye en el paquete, junto con el malware LunaGrabber.

Las acciones del actor malicioso fueron descubiertas por investigadores de seguridad informática, quienes publicaron sus hallazgos el 22 de agosto. Se descubrió que una vez descargado en un dispositivo, LunaGrabber se implementará en el navegador web de la víctima, en la aplicación Discord y en otras fuentes.

Los paquetes maliciosos imitaban el paquete legítimo noblox.js, un contenedor de interfaz de programación de aplicaciones (API) de Node.js Roblox utilizado para escribir scripts que interactúan con la plataforma de juegos Roblox.

Datos de desarrolladores de Roblox expuestos en violación de datos

Es posible que los asistentes a la Conferencia de desarrolladores de Roblox entre 2017 y 2021 hayan visto filtrados sus datos personales.

La noticia de la violación de datos fue dada a conocer el 18 de julio de 2023 en X (anteriormente conocido como Twitter) por el creador del sitio Have I Been Pwned.

Have I Been Pwned permite a los usuarios buscar su nombre y detalles para ver si se han filtrado en alguna violación de datos. En un mensaje anónimo enviado al creador, una fuente afirmó que a todos los que asistieron a la Conferencia de desarrolladores de Roblox se les filtraron sus datos. Según la fuente, los datos a los que se accedió durante el ciberataque incluían nombres completos, fechas de nacimiento, correo electrónico, direcciones IP y de casa y números de teléfono. La fuente también dijo que los datos habían sido publicados en línea.

La fuente informó que la filtración se volvió a publicar en línea recientemente, donde había atraído “atención significativa” tanto de partes maliciosas como de no maliciosas.

La fuente alegó que esta republicación de datos robados había provocado que "usuarios de alto perfil" recibieran "llamadas, mensajes de texto y correos electrónicos maliciosos".

El 20 de julio, Roblox abordó la filtración de datos y le dijo a Hunt que la compañía se había puesto en contacto con todos los afectados.

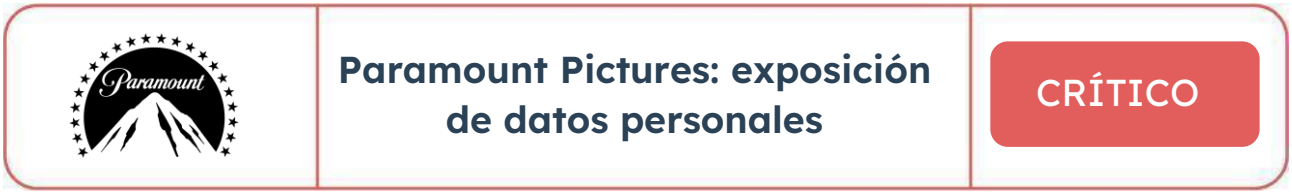
El portavoz de Roblox anunció que la compañía está al tanto de un problema de seguridad de terceros en el que había indicios de acceso no autorizado a información personal limitada de un subconjunto de la comunidad de creadores. Expertos independientes fueron contratados para apoyar la investigación dirigida por el equipo de seguridad de la información interna de la empresa.

Aquellos que se vieron afectados recibirán un correo electrónico informándoles los próximos pasos que se estarán tomando para ayudarlos.

Remediación / Referencias

Por mayor información acceder a:

https://www.cshub.com/malware/news/roblox-developers-targeted-with-malware-2



Descripción

Actores malintencionados obtuvieron acceso a la red de Paramount entre mayo y junio de 2023.

Estado

La productora Paramount Pictures ha revelado que recientemente sufrió una violación de datos que expuso información de identificación personal.

En una carta de notificación de violación de datos escrita a las partes afectadas, la productora explicó que una parte no autorizada había obtenido acceso a sus sistemas entre mayo y junio de este año, permitiéndoles acceder a la información personal de los clientes. La información a la que se accedió puede haber incluido: nombre, fecha de nacimiento, número de seguro social u otro número de identificación emitido por el gobierno (licencia de conducir o pasaporte), información sobre su relación con Paramount.

El portavoz de Paramount comunicó que "la parte no autorizada pudo haber accedido a la información personal de menos de 100 personas y esas personas y las autoridades pertinentes fueron notificadas". Aún no se ha revelado si los datos a los que se accedió estaban relacionados a clientes o empleados.

Paramount aseguró a los afectados por la violación que los sistemas afectados han sido protegidos y que se ha iniciado una investigación sobre la causa y el alcance de la violación de datos. La compañía señaló que “hasta la fecha no hay evidencia de que la información personal contenida en los archivos relevantes haya sido utilizada indebidamente” como resultado del incidente de seguridad cibernética. Asimismo, se están "implementando medidas mejoradas para ayudar a evitar que este tipo de problema vuelva a ocurrir", además de ofrecer servicios gratuitos de protección crediticia y monitoreo de robo de identidad a los afectados durante dos años.

Las empresas de producción de medios han sido blanco de ataques cibernéticos anteriormente, debido a la naturaleza de los datos que poseen.

Remediación / Referencias

Por mayor información acceder a:

https://www.cshub.com/attacks/news/paramount-pictures-data-breach-exposes-personal-data

	Brecha de datos en Tesla	CRÍTICO

Descripción

La brecha de datos provocó la filtración de datos confidenciales de más de 75.000 empleados de Tesla.

Estado

Se ha confirmado que una violación de datos que afectó al fabricante de automóviles Tesla en mayo de este año, según el aviso presentado ante el fiscal general de Maine el 18 de agosto, Tesla señaló que la violación de datos había afectado a 75.735 empleados y había sido causada por "actos ilícitos internos".

La brecha de datos se descubrió en mayo después de que el diario alemán Handelsplatt diera la noticia del incidente de seguridad cibernética, en el que se robaron y filtraron 100 GB de datos de Tesla. Handelsplatt informó en su cobertura de la infracción, que un

abogado de Tesla había difundido que la infracción había sido causada por un "ex empleado descontento". Al parecer, dicho empleado había abusado de su puesto como técnico de servicio para acceder a los datos.

Los datos, que estaban en más de 23.000 archivos, contenían datos confidenciales sobre empleados actuales y anteriores de Tesla. Esto incluía números de teléfono, direcciones de correo electrónico privadas y salarios de los empleados, datos bancarios de los clientes y datos confidenciales de la producción de Tesla. También incluía algunos números de seguridad social de los empleados, incluido el del director ejecutivo de Tesla, Elon Musk.

Otros datos filtrados incluyeron 2.400 quejas de clientes sobre sus vehículos Tesla.

El aviso presentado por Testa ante fiscalia, indica que lainvestigación sobre la violación de datos había "revelado que dos ex empleados de Tesla se apropiaron indebidamente de la información en violación de las políticas de seguridad de TI y protección de datos de Tesla" para obtener acceso a los datos. Posteriormente, los antiguos empleados comunicaron los datos a Handelsplatt. Asimismo, detalla que Handelsplatt "no tiene intención de publicar la información personal y, en cualquier caso, tiene legalmente prohibido utilizarla de forma inapropiada".

Tesla continuó explicando que, debido a una serie de demandas relacionadas con la violación de datos, se habían incautado los dispositivos que contenían los datos. El fabricante de automóviles también obtuvo órdenes judiciales que “prohíben a los ex empleados seguir utilizando, accediendo o difundiendo los datos”.

Remediación / Referencias

Por mayor información acceder a:

https://www.cshub.com/attacks/news/telsa-data-breach-caused-by-insider-wrongdoing

	**Discord.io expone datos de más de 760.000 usuarios**	CRÍTICO

Descripción

Un actor malintencionado puso a la venta la información en la dark web, correspondiente a datos personales de más de 760.000 usuarios.

Estado

Discord.io, un servicio de invitaciones personalizadas para el servicio de mensajería instantánea Discord, sufrió una violación de datos que expuso los datos personales de más de 760.000 usuarios.

Discord.io es un servicio de terceros que permite a los usuarios de Discord crear invitaciones personalizadas a sus canales en Discor. La infracción se descubrió el 14 de agosto, después de que se pusiera a la venta en la dark web una base de datos que contenía información personal de los usuarios de Discord.io.

El hacker, que utiliza el alias "Akhirah", compartió cuatro registros de usuarios de la base de datos como prueba de la autenticidad de los datos. Discord.io también confirmó que los datos eran legítimos.

En respuesta a la infracción, Discord.io cerró todas las operaciones y servicios e inició una investigación sobre la infracción. Hasta ahora, la investigación ha revelado que el hacker obtuvo acceso a la base de datos de Discord.io a través de una vulnerabilidad en el código del sitio web. Esto le permitió a Akhirah descargar toda la base de datos de Discord.io y ponerla a la venta en la nueva versión del infame sitio de piratería Breached Forums.

Los datos filtrados fueron extensos e incluyen información de cuenta confidencial y no confidencial.

Información de cuenta no confidencial:

- Identificación de usuario interno.
- Información sobre el avatar del usuario.
- Estado del usuario, p.e. moderador/admin/tiene anuncios/prohibidos/público/etc.
- Saldo de monedas del usuario y su racha actual en el minijuego gratuito de Discord.io.
- Clave API de usuario; sin embargo, esto no dará acceso a las cuentas de usuario y solo estaba disponible para menos de una docena de usuarios.
- Fecha de registro del usuario.
- La última fecha de pago y fecha de vencimiento de los usuarios con membresías premium.

Información de cuenta potencialmente confidencial:

- Nombre de usuario.
- ID de Discord, aunque esta información no es privada y puede ser obtenida por cualquier persona que comparta un servidor con dicho usuario. Sin embargo, podría significar que otras personas puedan vincular cuentas específicas de Discord con una dirección de correo electrónico determinada.
- Dirección de correo electrónico.
- La dirección de facturación de los usuarios que proporcionaron estos datos a Discord.io antes de que el sitio comenzara a utilizar el servicio de pago seguro Stripe.
- Las contraseñas y hash de las personas que se registraron en Discord.io antes de que ofreciera Discord exclusivamente como una opción de inicio de sesión, que comenzó en 2018.

Discord.io tomó la decisión de cerrar el sitio "hasta nuevo aviso" mientras continúa investigando las posibles causas de la infracción. El sitio dijo que "tomará medidas para garantizar que esto no vuelva a suceder", incluida una reescritura completa del código del sitio web y una revisión de sus prácticas de seguridad.

Remediación / Referencias

El sitio señaló que “no es necesario cambiar su contraseña ni realizar ninguna acción en Discord”, sin embargo, instó a los usuarios a cambiar sus contraseñas en cualquier sitio en el que hayan usado la misma contraseña que su Discord si se registraron en el sitio antes de 2018.

Un portavoz de Discord dijo sobre la infracción: “Discord no está afiliado a Discord.io. No compartimos ninguna información de usuario con Discord.io directamente y no tenemos acceso ni control de la información bajo la custodia de Discord.io.

"Hemos revocado los tokens de OAuth para cualquier usuario de Discord que haya usado Discord.io, por lo que la aplicación ya no puede realizar acciones en nombre de esos usuarios hasta que se vuelvan a autenticar".

Discord también recomendó que los usuarios habilitaran la autenticación de dos factores (2FA) para proteger sus cuentas y sugirió que consideran configurar la autenticación por SMS.

Por mayor información acceder a:

https://www.cshub.com/attacks/news/discordio-exposes-personal-data-of-more-than-760000-users

Prevención

LOCKBIT 3.0	**Grupo de ciberdelincuentes Lockbit ataca empresas en todo el mundo**	PREVENCIÓN

Descripción

En los últimos meses, el grupo de ciberdelincuentes conocido como Lockbit ha estado haciendo titulares por sus ataques cibernéticos dirigidos a empresas en todo el mundo.

Estado

Este grupo se especializa en ataques de ransomware, cifrando los sistemas de las víctimas y exigiendo un rescate a cambio de la clave de descifrado.Ataca empresas de todos los tamaños y sectores, lo que plantea una seria amenaza para la seguridad cibernética empresarial.

Métodos de ataque

Lockbit utiliza una variedad de métodos para infiltrarse en las redes empresariales. Principalmente, aprovechan vulnerabilidades en sistemas y software desactualizados, así como el descuido de la ciberseguridad por parte de los empleados.

Los ataques suelen comenzar con el envío de correos electrónicos de phishing, que pueden parecer legítimos, pero contienen archivos o enlaces maliciosos.

Una vez que se infiltran en la red de una empresa, Lockbit cifra los archivos y exige un rescate en criptomonedas para su liberación.

1. Phishing Sofisticado: Lockbit inicia sus ataques mediante el envío de correos electrónicos de phishing altamente sofisticados. Estos correos pueden parecer legítimos y a menudo están diseñados para engañar a los empleados y llevarlos a abrir archivos adjuntos o hacer clic en enlaces maliciosos. Una vez que un usuario interactúa con estos elementos, el malware de Lockbit se infiltra en la red de la empresa.

2. Explotación de Vulnerabilidades: Lockbit se aprovecha de las vulnerabilidades en sistemas y software desactualizados. Esta táctica incluye la explotación de brechas de seguridad conocidas que aún no han sido parcheadas.

3. Ataques de Fuerza Bruta: En algunos casos, utilizan ataques de fuerza bruta para descifrar contraseñas débiles o predecibles. Esto puede permitirles acceder a sistemas críticos o cuentas privilegiadas dentro de la red de la empresa.

4. Movimiento Lateral: Una vez que se ha ingresado a la red de una empresa, busca moverse lateralmente para obtener acceso a sistemas y datos más sensibles. Esto puede incluir la escalada de privilegios y la expansión de su presencia en la red, lo que aumenta el daño potencial.

5. Cifrado de Archivos y Demanda de Rescate: Una vez que Lockbit ha asegurado su posición en la red, procede a cifrar archivos críticos. Una vez que los archivos están bloqueados, los ciberdelincuentes exigen un rescate en criptomonedas a cambio de la clave de descifrado. Esta es la etapa final del ataque y puede ser devastadora para la operación normal de la empresa.

6. Uso de Doble Extorsión: Lockbit es conocido por su táctica de doble extorsión. No solo cifran los archivos, sino que también amenazan con filtrar datos confidenciales si la víctima no paga el rescate. Esta amenaza de divulgación pública agrega una capa adicional de presión a las organizaciones afectadas.

Recomendaciones de Prevención:

Recordemos que la ciberseguridad es una responsabilidad compartida y que la prevención es la mejor defensa contra los ciberdelincuentes como Lockbit.
La vigilancia constante y las prácticas sólidas de seguridad son esenciales para mantener a salvo sus datos y sistemas empresariales.

Es fundamental tomar medidas proactivas de seguridad cibernética:

- Educación y Concienciación: capacite a sus empleados para que reconozcan correos electrónicos de phishing y enseñe buenas prácticas de seguridad en línea.
- Actualizaciones y Parches: mantenga todo el software y sistemas actualizados con los últimos parches de seguridad para evitar vulnerabilidades explotables.
- Copias de Seguridad: realice copias de seguridad regulares de los datos críticos y almacénelas en un lugar seguro y desconectado de la red principal.
- Firewalls y Antivirus: implemente soluciones de seguridad como firewalls y programas antivirus de calidad para detectar y bloquear amenazas.
- Políticas de Acceso: establezca políticas de acceso estrictas y restrinja los privilegios de los empleados para minimizar el riesgo de movimientos laterales de los atacantes.
- Planes de Respuesta: elabore un plan de respuesta a incidentes que incluya procedimientos claros para manejar un ataque de ransomware, lo que ayudará a reducir el tiempo de inactividad y los daños.
- Seguridad de Correo Electrónico: implemente soluciones de seguridad de correo electrónico avanzadas que puedan detectar y bloquear correos electrónicos maliciosos.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/07/virustotal-data-leak-exposes-some.html

Conclusiones

En un mundo en constante evolución digital y con la creciente sofisticación de los grupos de ciberdelincuentes, la concienciación y la educación en ciberseguridad se han convertido en un escudo vital para proteger nuestros activos digitales y personales.
Los ataques cibernéticos avanzan a pasos agigantados, pero el conocimiento y la vigilancia son nuestras mejores defensas. Al aprender a identificar las señales de alerta, practicar la higiene cibernética y mantenerse actualizados sobre las amenazas emergentes, los usuarios pueden desempeñar un papel fundamental en la prevención de ataques cibernéticos.

Recordemos que, en última instancia, la ciberseguridad es un esfuerzo compartido que requiere la participación activa de todos nosotros. Mantengámonos informados y preparados, para construir un entorno digital más seguro y resistente ante las amenazas en constante evolución.

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

¡Hasta la próxima!