BOLETÍN
CYBEROMAX

CONTENIDO

INCIDENTES FEB 24

ESTADÍSTICAS

TENDENCIAS

FEBRERO 2024

VERSIÓN NO 2

INCIDENTES FEBRERO 2024

Ransomware a Southern Water

23-01-24 – 01-02-24

Ataque de Ransomware a la empresa de agua con sede en Reino unido, perpetrado por la pandilla Black Basta, deja 750GB de datos confidenciales robados de clientes.

Ingeniería social a diplomáticos UE

30-01-24

Malware difundido a través de una campaña de ingeniería social a funcionarios europeos. La campaña fue apodada vino con púas", y su estrategia fue enviar por correo electrónico una invitación a una supuesta cata de vino a través de un archivo PDF.

Ciberataque AnyDesk

03-02-24

Proveedor líder de soluciones de acceso remoto, confirmó haber sido víctima de un ciberataque que permitió a los actores obtener código fuente y acceso a los sistemas de producción de la compañía.

Ciberataque a Onclusive

06-02-24

Una de las principales compañías en análisis de medios ha sufrido un ciberataque que deja a sus clientes sin la información sobre apariciones en prensa. Los atacantes dejaron servidores inoperativos.

INCIDENTES FEBRERO 2024

Robo de USD 300 Millones a PlayDapp

09-02-24

Incidente afecta a la plataforma basada en blockchain que usa e intercambia tokens no fungibles (NFT) dentro de los juegos, ciberdelincuentes habrían usado clave privada para realizar el robo.

Ransomware afecta 100 hospitales

11 y 12-02-24

Ataque de ransomware derribara sistema de gestión de atención médica en 100 hospitales de Rumanía, dejando como consecuencia paralización del funcionamiento médico y bases de datos encriptadas. El Incidente aún está siendo investigado.

Ciberataque a Varta

12-02-24

Empresa de baterías de origen alemán paralizó su operación a causa de un ataque informático, ocasionando interrupción en la producción de baterías y sus procesos administrativos, empresa se encuentra investigando.

Ciberataque a transporte público Madrid

14-02-24

Incidente de seguridad realizado en nov-23, pero informado en febrero, el cual consistió en la sustracción de datos personales de los titulares de las tarjetas de la red de transporte, no se tiene prueba de alguna filtración a sitios oscuros, sin embargo, los funcionarios invitan a los ciudadanos a no caer en campañas de phishing.

INCIDENTES FEBRERO 2024

Ciberataque a policías de Cataluña

15-02-24

Filtración de datos a través de Telegram de 70 agentes policiales, organización ha admitido el incidente e informan que se encuentran en investigación del ataque.

Ciberataque a Cencora

21-02-24

Empresa farmacéutica confirma incidente de robo de datos en sus sistemas TI. Se encuentran trabajando en investigar el caso, aún se desconoce responsables del incidente y cantidad de datos comprometidos.

Ataque de Ransomware Optum

28-02-24

Ataque de ransomware de grupo BlackCat a empresa filial de UnitedHealth, provocó un robo de 6TB de datos médicos, información de pago y datos personales de clientes. Se rumora un pago de USD 22 Millones.

Filtración de datos a cadena de restaurantes

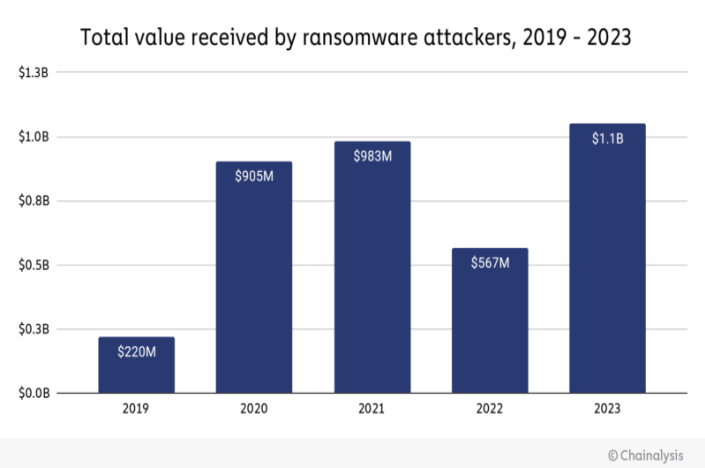
29-02-24

Famosa cadena de restaurantes en EEUU y Puerto Rico confirma filtración de datos confidenciales de 183 personas entre empleados, socios y clientes tras incidente suscitado en agosto del 2023, pero comunicado en el mes de Febrero.

ESTADÍSTICAS

90%

Es el incremento de las víctimas extorsionadas por ransomware públicamente. *Informe Security Report 2024 Check Point*

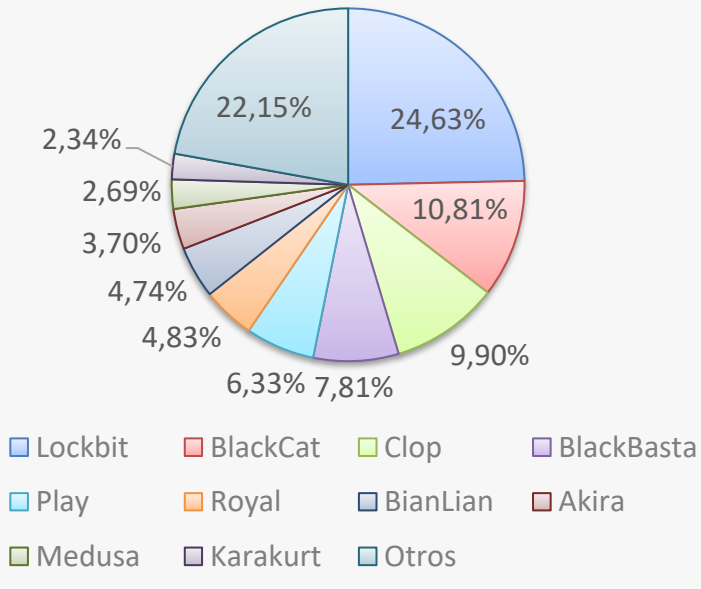


$1.1 B

Los pagos de ransomware alcanzaron un récord de USD 1.100 millones en 2023.*Chainalysis*

GRUPOS DE EXTORSIÓN MÁS ACTIVOS

noviembre 2022 - octubre 2023



Fuente: Kaspersky

RECOMENDACIONES DE CIBERSEGURIDAD

AVANCE DE LOS CIBERATAQUES CON IA

En la era digital actual, los avances en inteligencia artificial (IA) han revolucionado la forma en que interactuamos con la tecnología. Proporcionando automatización en los procesos de las empresas, Sin embargo, junto con los beneficios vienen nuevos desafíos, y uno de los más preocupantes es el aumento de los ciberataques impulsados por la IA. En esta oportunidad, exploraremos cómo los ciberdelincuentes están utilizando la IA para perpetrar ataques sofisticados y cómo podemos defendernos contra esta creciente amenaza.

Los atacantes aprovechan la capacidad de la IA para analizar grandes cantidades de datos, aprender patrones y adaptarse rápidamente. Estudio de SlashNext reveló que **los ataques de vishing, smishing y phishing se disparan un 1265% después de ChatGPT**.

En una encuesta realizada en junio de 2023 a 650 expertos en ciberseguridad realizada por la empresa cibernética de Nueva York Deep Instinct, 3 de cada 4 de los expertos encuestados observaron un aumento en los ataques cibernéticos y el 85% atribuyó este aumento a los malos actores que utilizan IA generativa.

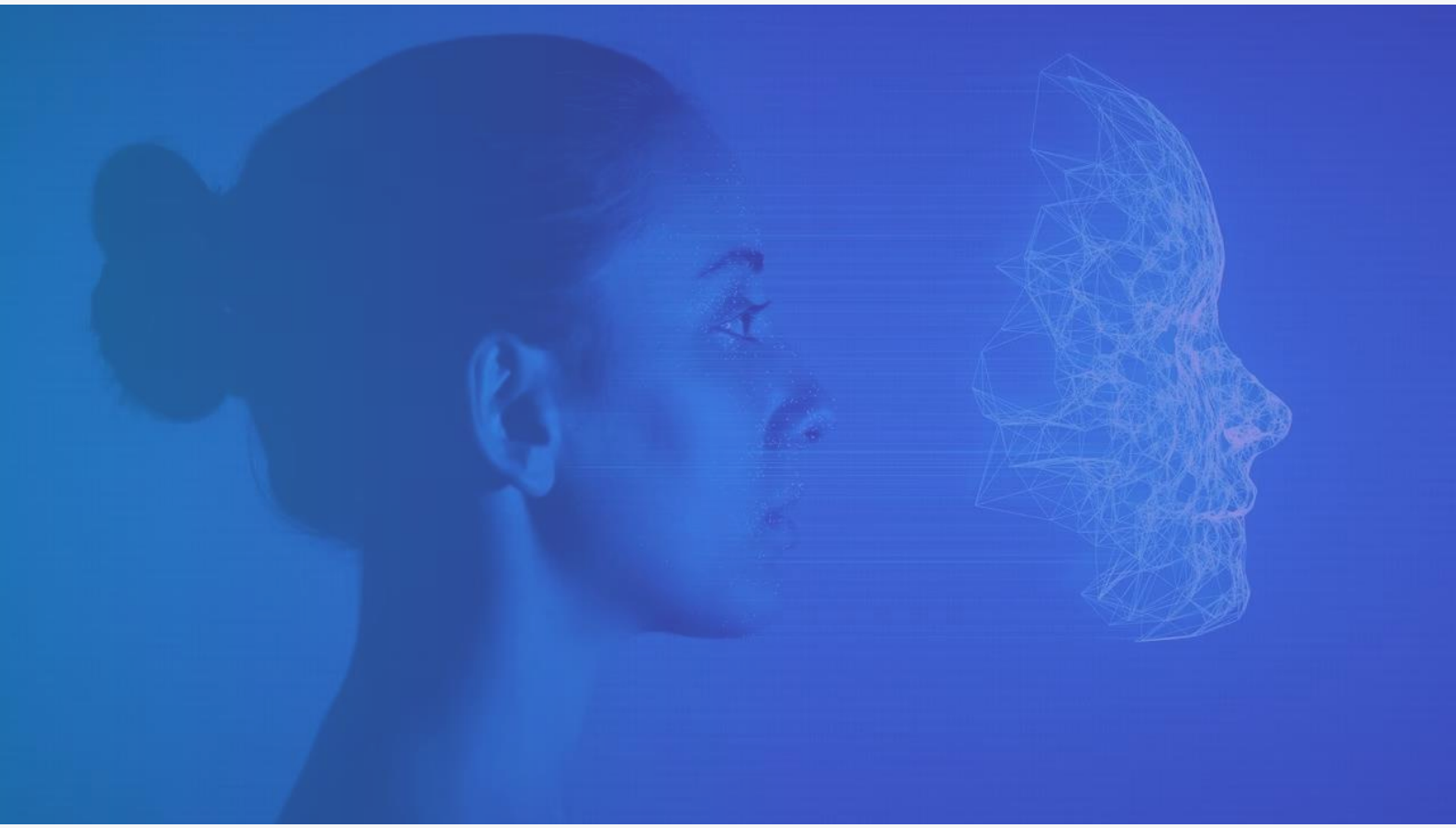
Los deepfakes son cada vez más cotidianos con la clonación de voz, ya se puede suplantar a cualquier persona, en internet y redes sociales constantemente se promocionan nuevas aplicaciones con estas funciones y muchas de ellas más que ser usadas para entretenimiento o para transmitir mensajes positivos, está siendo usada por ciberdelincuentes, quienes utilizan la IA generativa de diversas formas, pueden analizar diferentes publicaciones, campañas y la regularidad de difusión. Luego pueden enviar

RECOMENDACIONES DE CIBERSEGURIDAD

mensajes de texto con tu estilo a tus familiares, implorándoles que te envíen dinero para ayudarte a salir de un apuro. Aún más aterrador es que si tienen una breve muestra de audio de la voz de un niño, pueden llamar a los padres y hacerse pasar por el niño, fingir que ha sido secuestrado y exigir el pago de un rescate.

Del mismo modo delincuentes más sofisticados con financiamiento aplican estas herramientas para engañar a los colaboradores de una empresa a través de ingeniería social potenciada con IA, pudiendo apropiarse incluso a la red interna de la compañía y llegar a paralizar la operación.

Parece ser que los ciberdelincuentes siempre van un pie adelante con la tecnología, mientras los entes policiales y de gobierno les cuesta ponerse al día, un ejemplo de ello son los casos que expuso Forbes de cómo los ladrones en 1989 utilizaban computadoras comunes e impresoras láser para falsificar cheques lo suficientemente buenos como para engañar a los bancos.



RECOMENDACIONES DE CIBERSEGURIDAD

Conociendo el contexto de cómo está operando los ciberdelincuentes con herramientas potenciadas por IA, les compartimos cómo podemos proteger a nuestras empresas.

1. **Reforzar los controles de identidad, accesos y autenticación:** La gestión de la identidad y acceso es fundamental para garantizar la seguridad dentro de las empresas, la mayor cantidad de campañas están dirigidas a los usuarios, quienes son la puerta de entrada a los ciberdelincuentes, por lo que implementar controles, protocolos de autenticación fuerte y definir políticas de acceso adecuadas, estas medidas acompañadas de tecnología y gestión nos ayudará a minimizar el impacto.

2. **Formación a todos los colaboradores:** Esta medida en conjunto de la anterior son los pilares principales de la batalla ante los ciberataques. Educar a nuestros colaboradores va más allá de compartir un reportaje, un video o imagen vía correo. Debe existir una estrategia, una metodología, cuando vamos a la universidad o hacemos algún curso para formarnos, nuestros coach no nos pasan simplemente una información, ellos implementan distintas formas de difusión de los conocimientos, prácticas y conversaciones bidireccionales. Apoyémonos en las áreas de comunicaciones, trabajemos de la mano con las distintas áreas de la empresa.

3. **Realizar pruebas técnicas:** A través de Test de penetración, scan de vulnerabilidades y ethical Hacking podemos determinar el alcance de los fallos de nuestros sistemas, así tener mayor información de las brechas de seguridad para tomar medidas antes de que se produjese un incidente.

RECOMENDACIONES DE CIBERSEGURIDAD

4 **Gestión de proveedores y bakups:** La entrada a cibercriminales puede ser también por nuestras terceras partes, debemos hacernos preguntas relacionadas al vínculo de ellos en nuestros procesos como: ¿Cuáles son los activos críticos de información a los cuales tienen acceso?, ¿Me ofrece garantías de confidencialidad y protección de mis datos?, ¿implementa mi proveedor en su empresa buenas prácticas de seguridad de la información? ¿me ofrece garantía de disponibilidad? Estas son alguna de las preguntas que podemos realizarnos, acompañado de gestionar los hallazgos que puedan surgir. Otro punto relevante en proteger nuestros activos de información es disponer de un backup automático y fiable que posibilité la recuperación rápida en caso de algún fallo.

5 **Actualización de software y conocimientos:** Así como los ciberdelincuentes se actualizan constantemente en las formas de atacar, así debemos mantener a los equipos de TI, S.I y Ciberseguridad. Es recomendable hacer actualización de nuestros sistemas, software, aplicativos y su debido seguimiento, así como también estar en la vanguardia de las soluciones innovadoras que podemos implementar, siempre y cuando podamos dimensionar la necesidad de la compañía.

Sí necesitas asesoría en tu organización, no sabes cómo iniciar o ayuda en alguna de tus iniciativas de ciberseguridad.

¡Contáctanos hoy mismo y juntos transformemos la ciberseguridad!

RoMaX Technologies

Empresa consultora de Seguridad de la Información y Ciberseguridad especializada en abordar sus servicios, asesorías y soluciones desde una mirada estratégica formada por expertos en ciberseguridad con +27 años de experiencia, calidad y excelencia comprobada.

#JuntosTransformamosLaCiberseguridad

Contacto@romaxtechs.com