Edición 1

Septiembre 2024

CIBER E-DEA

Boletín de Seguridad

Malware “Voldermort”

Usa google Sheets para almacenar datos robados.

“Blind Eagle”

La amenaza que acecha al sector financiero en Colombia.

KIA

Vulnerabilidad en el portal web de KIA que afecta a millones de vehículos

TIPS

Consejos para la seguridad de tus dispositivos móviles

Ciber Incidentes

Incidentes en septiembre en Colombia y en el mundo

e-dea NETWORKS | CYBER SECURITY

Malware “Voldermort”

Más de 70 organizaciones a nivel global, abarcando sectores como la educación, el transporte, los seguros y la industria aeroespacial, han sido blanco de la nueva puerta trasera 'Voldermort', en lo que parece ser una campaña de ciberespionaje iniciada a principios del mes pasado.

El modus operandi de 'Voldermort' combina técnicas tanto avanzadas como convencionales, lo que ha llevado a los expertos a describirla como una 'mezcla frankensteiniana'.

Los atacantes inician la campaña enviando correos de phishing que aparentan ser comunicaciones legítimas de autoridades fiscales, como las agencias tributarias de Estados Unidos, Europa y Asia.

Estos correos están adaptados a la ubicación geográfica de las víctimas y contienen enlaces que supuestamente proporcionan información fiscal actualizada.

Al hacer clic en el enlace, los usuarios son redirigidos a una página falsa que parece auténtica. Si están en Windows y hacen clic en el botón “Haz clic para ver el documento”, se descarga un archivo malicioso que parece un PDF legítimo.

Noticia completa:
https://blackswan-cybersecurity.com/wp-content/uploads/2024/09/Threat-Advisory_090324.pdf

Multa a Meta por contraseñas almacenadas en texto plano.

Noticia completa:
https://www.securityweek.com/meta-hit-with-102-million-privacy-fine-from-european-union-over-2019-password-security-apse/

La Comisión de Protección de Datos de Irlanda impuso a Meta una sanción de 91 millones de euros tras confirmarse que, en 2019, se violó el Reglamento General de Protección de Datos (RGPD) de Europa. La infracción se debió a que ciertas contraseñas fueron almacenadas en texto plano, es decir, sin cifrar.

El RGPD establece que los responsables del tratamiento de datos deben aplicar medidas de seguridad adecuadas al procesar información personal, teniendo en cuenta factores como los riesgos asociados para los usuarios del servicio y la naturaleza del procesamiento de datos. En su comunicado, el organismo afirma: "Para garantizar la seguridad, los responsables del tratamiento de datos deben evaluar los riesgos inherentes al procesamiento e implementar medidas para mitigarlos.

Ataques dirigidos a controladores de Windows

Los controladores vulnerables pueden ser explotados para llevar a cabo una amplia gama de ataques, incluidos ataques de ransomware y Amenazas Persistentes Avanzadas (APT).
Los ciberatacantes aprovechan las vulnerabilidades en estos controladores para intentar desactivar las soluciones de seguridad en un sistema y escalar privilegios, lo que les permite realizar diversas actividades maliciosas, como la instalación de ransomware o el establecimiento de persistencia para fines de espionaje o sabotaje, especialmente cuando un grupo de APT está detrás del ataque.

Noticia completa:
https://cybersecuritynews.es/aumentan-un-23-los-ataques-dirigidos-a-controladores-vulnerables-de-windows/

“Blind Eagle” la amenaza que acecha al sector financiero en Colombia.

Blind Eagle, un grupo de hackers reconocido por su habilidad para ejecutar ciberataques selectivos, ha enfocado sus acciones en el sector financiero de Colombia.

Estos ataques iniciaron con campañas de phishing que simulaban ser comunicaciones oficiales de la DIAN, engañando a las víctimas para que instalaran malware a través de cuentas comprometidas de Google Drive.

Este grupo de cibercriminales, conocido como Águila Ciega, APT-C-36 o APT-Q-98, tiene un historial de ataques en América del Sur, dirigido principalmente a organizaciones y personas de los sectores gubernamental y financiero en Colombia y Ecuador

Estos enlaces, ya sea dentro de un archivo PDF adjunto o directamente en el cuerpo del correo, llevan a archivos ZIP alojados en una carpeta de Google Drive vinculada a una cuenta comprometida de una organización gubernamental regional en Colombia.

Este malware tiene funciones avanzadas como registrar las pulsaciones de teclado, ejecutar comandos de shell, robar información de navegadores web y clientes FTP, además de monitorear las interacciones de la víctima con servicios bancarios y de pago específicos en Colombia y Ecuador.

Noticia completa: https://thehackernews.com/2024/09/blind-eagle-targets-colombian-insurance.html

SIM Swap, robo de tu identidad y SIM Card

El SIM Swapping es un tipo de estafa en la que se duplica el número de teléfono móvil de la víctima, lo que permite a los delincuentes obtener los códigos de seguridad necesarios para acceder fácilmente a las cuentas bancarias del titular. Una vez que la tarjeta SIM duplicada se activa, la tarjeta original pierde automáticamente su cobertura, quedando el número en manos de un tercero.

Se recomienda no compartir información personal, limitar la exposición en redes sociales, evitar introducir datos sensibles en redes WiFi públicas y descargar aplicaciones únicamente de tiendas oficiales, como Google Play.

Vulnerabilidad en el portal web de KIA que afecta a millones de vehículos

Un grupo de investigadores de seguridad ha descubierto una vulnerabilidad en un portal web de Kia que permite a los atacantes tomar el control de las funciones conectadas a internet de los vehículos modernos de la marca. Mediante el uso de esta falla y una aplicación personalizada, los hackers pudieron rastrear la ubicación, desbloquear, hacer sonar el claxon e incluso encender los vehículos en cuestión de segundos.

El año pasado se descubrió una técnica similar para hackear los sistemas digitales de los vehículos Kia, siendo esta una de varias vulnerabilidades web encontradas en los últimos dos años que también han afectado a marcas como Acura, Genesis, Honda, Hyundai, Infiniti y Toyota.

Noticia completa:
https://www.techradar.com/pro/security/millions-of-kia-cars-could-have-been-hacked-due-to-dealer-software-portal-flaw

Consejos para la seguridad de tus dispositivos móviles

Los dispositivos móviles se han convertido en un accesorio indispensable, casi de igual importancia que una cartera o nuestro documento de identidad.

Con la gran variedad de aplicaciones de streaming, redes sociales, bancos y etc.
Tienden a ser blanco de ataques cibernéticos
Lo que significa que incluso si tu teléfono o tableta siempre está en tu poder, es posible que tus datos no estén seguros.

Algunas de las principales amenazas a la seguridad del teléfono son las siguientes:

- Aplicaciones y sitios web maliciosos
- Ataques Man-in-the-middle (MiTM)
- Jailbreaking y rooting
- Phishing

Aquí tienes algunos consejos y recomendaciones para mantener seguros tus dispositivos móviles:

- Usa contraseñas fuertes y autenticación biométrica.
- Mantén el sistema operativo y las aplicaciones actualizadas.
- Descarga aplicaciones solo de fuentes oficiales.
- Instala aplicaciones de seguridad como antivirus y antimalware.
- Activa el cifrado de datos.
- Evita redes Wi-Fi públicas o usa una VPN.
- Desactiva Bluetooth y ubicación cuando no los uses.
- Realiza copias de seguridad regularmente.
- Revisa los permisos de las aplicaciones.

Vulnerabilidades destacadas

CVE-2024-20439 Y CVE-2024-20440

Cisco ha revelado recientemente múltiples vulnerabilidades críticas en su Smart Licensing Utility (CSLU), que podrían permitir a atacantes remotos no autenticados obtener acceso administrativo o recopilar información confidencial de los sistemas afectados.

Cisco

Versiones afectadas

Cisco Smart Licensing Utility

Noticia completa: https://www.cve.org/CVERecord?id=CVE-2024-20439

CVE-2024-38063

Microsoft - Windows

Versiones afectadas:

- Windows 10, Windows 11
- Windows Server 2008 a 2022

Noticia completa: https://nvd.nist.gov/vuln/detail/CVE-2024-38063

La vulnerabilidad afecta al sistema operativo Windows. Este problema permite a un atacante ejecutar código malicioso en el sistema afectado enviando paquetes IPv6 especialmente diseñados.

Ciber incidentes en Colombia y en el mundo

Colombia

1
Ciber incidentes

Sector: Energia

Fecha: 2024-09-02

Afectación: Infraestructura crítica

Atribución: Desconocida

El 2 de septiembre de 2024, la empresa colombiana de energía **Air-e** fue objeto de un ataque dirigido con ransomware, lo que comprometió la integridad de su sistema de seguridad.

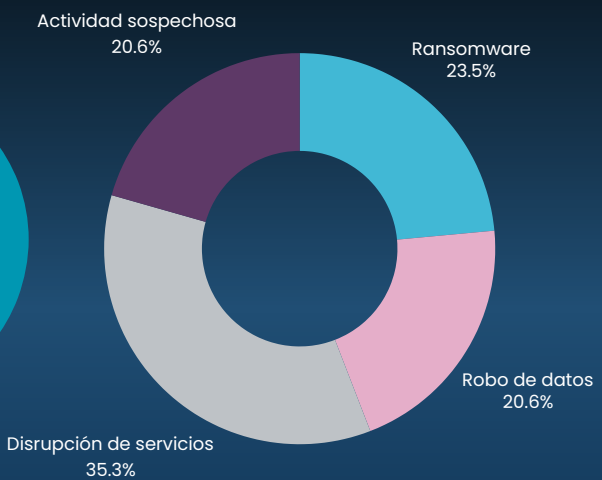
El incidente tuvo un impacto significativo, afectando tanto su sistema de facturación en línea como su servicio de atención al cliente, generando interrupciones en el servicio.

Fuente: https://eurepoc.eu/dashboard/

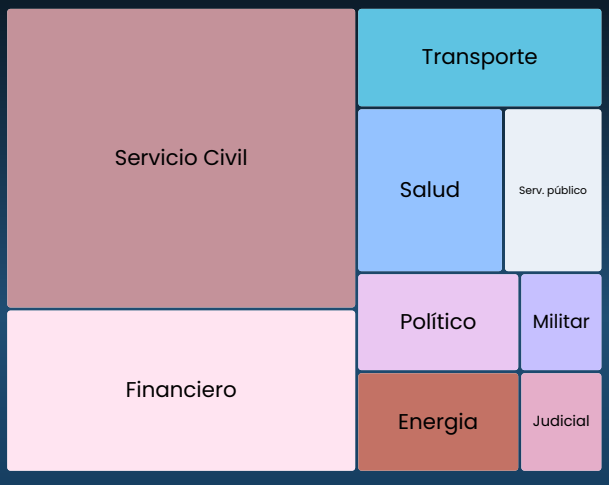
El mundo

34
Ciber incidentes

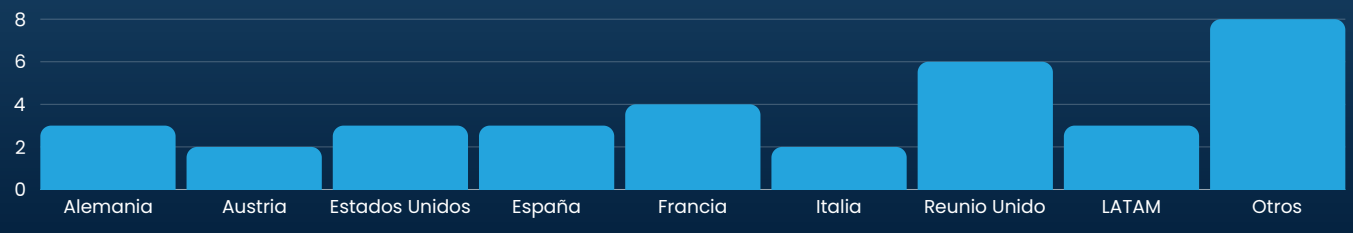
TIPO DE INCIDENTE



SECTORES AFECTADOS



PAISES ATACADOS



CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

www.e-dea.co