CIBER E-DEA

Boletín de Seguridad

Una línea de código que sacudió Internet: el fallo masivo de Google Cloud

La seguridad en la IA, sus preocupaciones y alternativas

Movistar bajo la mira: Posible brecha de seguridad que compromete datos de 21 millones de usuarios.

El malware Crocodilus se expandió a nivel mundial con nuevas funciones cripto y de robo bancario.

Ciber Incidentes en Colombia y en el Mundo

Vulnerabilidades más relevantes.

e-dea NETWORKS. | LevelBlue | ALIEN VAULT

| WEBINAR |

Panorama de Ciberseguridad:

Cómo adaptarse al nuevo entorno de amenazas

Jueves 17 de julio de 2025

10:00 a.m. CO | 9:00 a.m. MX

¡CONOCE MÁS AQUÍ!

Una línea de código que sacudió Internet: el fallo masivo de Google Cloud

El pasado 13 de junio, una interrupción en la infraestructura de Google Cloud dejó fuera de servicio durante horas a plataformas como Cloudflare, Spotify, Discord, Twitch, Gmail y muchas más. ¿La causa? Una simple línea de código con un error crítico que activó una cascada de fallos.

Todo comenzó semanas antes, con una actualización al componente Service Control, responsable de validar políticas de acceso y cuotas en la nube. El nuevo código tenía una condición que no se activó durante las pruebas. Pero el 12 de junio, una política con campos vacíos disparó esa condición oculta, causando un error de puntero nulo. El sistema entró en un bucle de reinicio global, afectando simultáneamente a todas las regiones.

Este componente no contaba con un feature flag que permitiera desactivarlo rápidamente, ni con manejo de errores adecuado. Aunque el equipo de Google reaccionó con rapidez, la sobrecarga de solicitudes en sus sistemas distribuidos prolongó la recuperación por casi tres horas en algunas zonas.

Este incidente nos recuerda que incluso en infraestructuras robustas, una sola línea de código mal gestionada puede afectar al mundo entero.

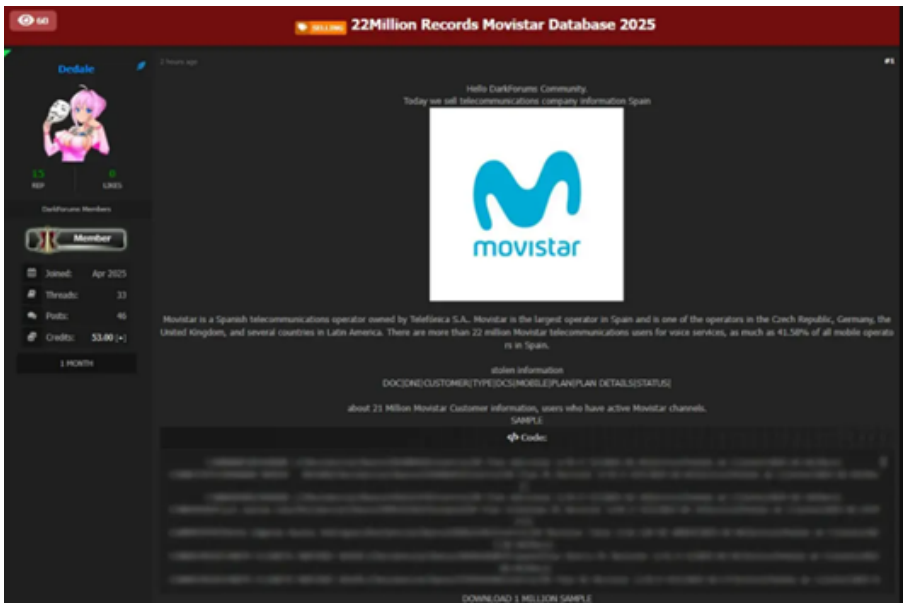
Reflexión para nuestro entorno

- **Exigir pruebas exhaustivas en actualizaciones de sistemas críticos.**
- **Evaluar la resiliencia y aislamiento de nuestros sistemas de monitoreo.**
- **Diseñar planes de contingencia ante interrupciones de proveedores externos.**

Google Cloud publicó en su cuenta de X que son conscientes del problema y que están trabajando para que podamos usar sus servicios "lo antes posible". También añadió un enlace para ver las actualizaciones de la falla.

Más información

Movistar bajo la mira: Posible brecha de seguridad que compromete datos de 21 millones de usuarios



Un hacker conocido como 'Dedale' ha puesto a la venta la base de datos en la dark web, ofreciendo una muestra de un millón de registros como prueba.

'Dedale' asegura poseer los datos de 21 millones de clientes, incluyendo nombres, documentos de identidad y datos sensibles que se encuentran comercializando mediante una base de datos por el valor de $1,500 USD y también donde proporciona como prueba la información de 1 millón de usuarios.

La filtración de datos de Movistar afecta principalmente a usuarios en España, pero también incluye información de usuarios de otros países donde opera la compañía.
Esto sugiere que el alcance del incidente podría ser global, afectando a múltiples regiones donde Movistar tiene presencia.

DECLARACIONES DE MOVISTAR:

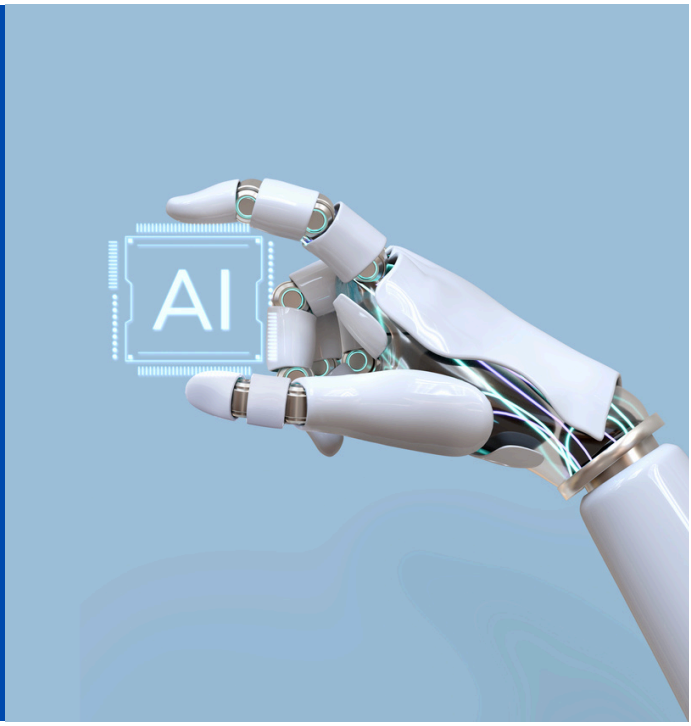
Por el momento, Movistar no ha confirmado o negado esta filtración de datos, ni ha detallado si ha identificado alguna violación a sus sistemas.
De confirmarse esta información, este sería el segundo incidente de seguridad que enfrentaría la empresa de telecomunicaciones en 2025 dado que en enero, Movistar reportó una intrusión en su sistema de gestión de tickets que expuso los datos de miles de empleados.

Más información

La seguridad en la IA, sus preocupaciones y alternativas

Un informe de Arctic Wolf revela que la inteligencia artificial (IA) y los modelos de lenguaje (LLM) son hoy la principal preocupación del 29 % de los líderes de seguridad, superando amenazas como el ransomware y el malware. A pesar de estos temores, el 99 % de las organizaciones ya ha implementado o está creando políticas de uso de IA generativa (GenAI).

Dan Schiappa, de Arctic Wolf, advierte que el entusiasmo por la IA no debe distraer de los principios esenciales de ciberseguridad, como la gestión de vulnerabilidades, detección y respuesta ante incidentes.



El informe también señala que el 70 % de las organizaciones sufrió al menos un ciberataque grave en el último año, siendo el malware y los ataques de compromiso de correo electrónico empresarial (BEC) los más comunes. Además, el 52 % reportó filtraciones de datos, reflejando una mejora en transparencia, ya que el 97 % de los incidentes fueron comunicados.

Respecto al uso de GenAI en ciberseguridad, se destacan lecciones clave: la IA debe aplicarse con enfoque técnico adecuado según cada caso, especialmente en entornos de datos complejos. No basta con contratar expertos en IA; es fundamental integrar conocimientos en ciberseguridad y comportamiento humano para desarrollar soluciones efectivas. Solo con este enfoque se pueden reducir falsos positivos y detectar amenazas reales.

Finalmente, se resalta que GenAI también representa una nueva superficie de ataque. Por ello, la IA debe emplearse en áreas críticas como la investigación, el análisis, la priorización y la respuesta ante incidentes. El futuro apunta hacia modelos híbridos, combinando GenAI y aprendizaje automático tradicional para hacer frente a ciberataques cada vez más avanzados.

Más información

El malware Crocodilus se expandió a nivel mundial con nuevas funciones cripto y de robo bancario

El troyano bancario Crocodilus se está expandiendo a nivel mundial con nuevas campañas dirigidas a billeteras cripto y aplicaciones bancarias, llegando ahora a Europa y Sudamérica.

Detectado por primera vez en marzo de 2025, las primeras muestras de Crocodilus se limitaron en gran medida a Turquía, donde el malware se hacía pasar por aplicaciones de casinos en línea o aplicaciones bancarias falsificadas para robar credenciales de inicio de sesión.

Crocodilus se centra en aplicaciones bancarias y de criptomonedas

Una vez instalado, Crocodilus superpone páginas de inicio de sesión falsas sobre aplicaciones bancarias y cripto legítimas. En España, se hizo pasar por una actualización del navegador y atacó a casi todos los principales bancos.

```
this.cryptoTarget1 = "[redacted]";
this.cryptoTarget2 = "[redacted]";
this.cryptoTarget3 = "[redacted]
this.regex1 = "[a-fA-F0-9]{64}";
this.regex2 = "^(\\d+)\\.?\\s*(\\w+)$";
this.regex3 = "\\d+";
this.regex4 = "\\w+";
this.regex5 = "^\\d+\\.?\\s*\\w+$";
```

¿Cómo actúa Crocodilus en los dispositivos móviles?

Crocodilus se instala a través de un dropper, un tipo de malware que contiene un archivo ejecutable oculto dentro de una app aparentemente legítima. Este dropper logra eludir las restricciones de seguridad de Android 13 y versiones superiores. Una vez ejecutado, solicita acceso al Servicio de Accesibilidad, un permiso que le da el control completo del dispositivo.

Recomendaciones para proteger tu Android del troyano Crocodilus

Descarga solo apps desde Google Play. Nunca instales APKs de fuentes desconocidas.

Verifica los permisos que otorgas. Si una app pide acceso a funciones innecesarias (como SMS o accesibilidad), es una señal de alerta.

Activa la verificación en dos pasos en todas tus aplicaciones bancarias o de criptomonedas.

Más información

Vulnerabilidades destacadas

CVE-2025-20282

Cisco

Versiones afectadas
ISE y PIC V.3.4.

Es una vulnerabilidad crítica de máxima gravedad en Cisco Identity Services Engine (ISE) y Passive Identity Connector (PIC) versión 3.4. Permite a atacantes no autenticados cargar archivos en directorios privilegiados y ejecutarlos con privilegios de root, lo que provoca el control total del sistema.

CVE-2025-47172

Microsoft

Versiones afectadas
Microsoft SharePoint Server 2016, 2019

Es una vulnerabilidad crítica en Microsoft SharePoint Server que permite la ejecución remota de código por parte de un atacante autenticado. Afecta a varias versiones de SharePoint y se debe a un manejo inadecuado de consultas SQL, lo que permite a un atacante inyectar comandos maliciosos y ejecutar código arbitrario en el servidor.

CVE-2025-32710

Microsoft

Versiones afectadas
Windows Server 2022, 2019, 2016

Es una vulnerabilidad crítica de uso posterior a la liberación (use after-free) en el componente Gateway de Servicios de Escritorio Remoto (RDS) de Microsoft. Esta falla permite a atacantes remotos no autenticados ejecutar código arbitrario en los sistemas objetivo aprovechando la gestión incorrecta de la memoria durante operaciones específicas del protocolo RDS.

Ciber incidentes en Colombia y en el mundo

Incidente cibernético en Justicia Penal Militar y Policial

El 15 de junio de 2025, el Departamento de Justicia Penal Militar y Policial de Colombia fue víctima de un ciberataque que comprometió su infraestructura tecnológica a nivel nacional. Durante el ataque, los perpetradores secuestraron información pública relacionada con servicios de red y comunicaciones, así como datos administrativos y jurisdiccionales. Los servicios digitales se suspendieron temporalmente y los plazos judiciales en los procedimientos bajo la Ley n.º 1407 de 2010 se suspendieron hasta nuevo aviso. La entidad se disculpó por los inconvenientes causados por el ataque y declaró que estaba enfocada en restablecer los servicios lo antes posible.

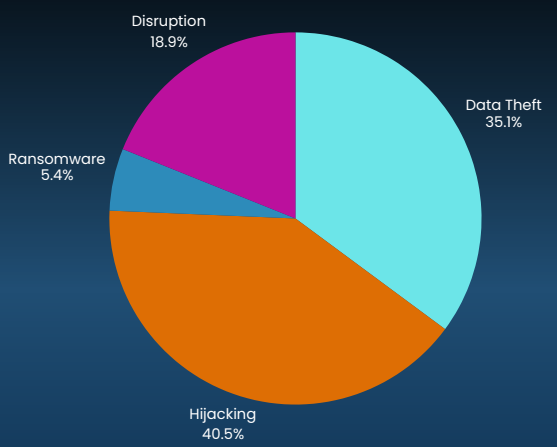
Tipo de incidente: Disrupción; secuestro con mal uso.

Más información

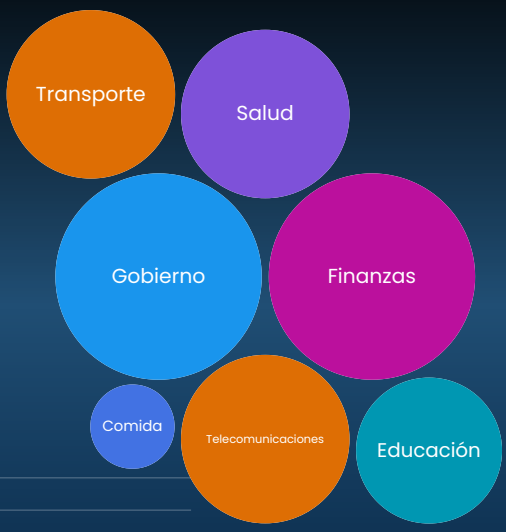
El mundo

37
Ciber incidentes

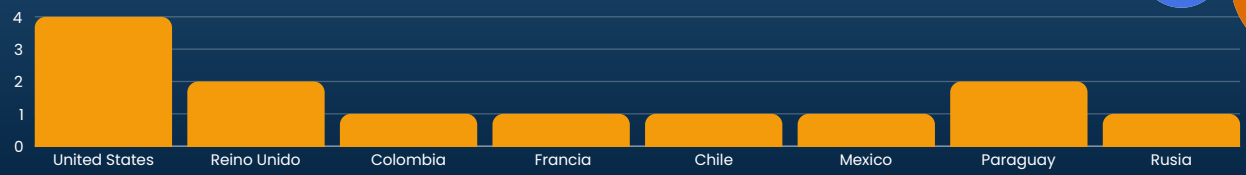
TIPO DE INCIDENTE



SECTORES AFECTADOS



PAISES ATACADOS



Más información

CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

Csirt E-dea

e-dea.co