Edición 23 - Junio 2026

Ciber E-dea

Revista de Ciberseguridad

e-dea NETWORKS. CYBER SECURITY

FIRST MEMBER

Great Place To Work. Certificada

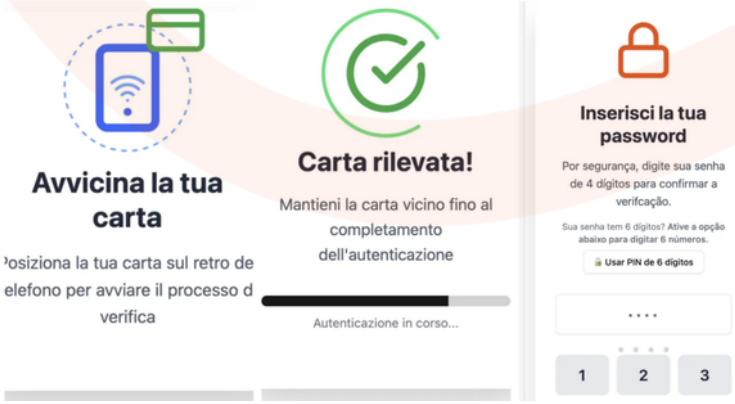
icontec ISO 9001 CO-SC-CER899598

icontec ISO 45001 CO-ST-CER896599

icontec ISO / IEC 27001 CO-SI-2001007

IQNET

01 NFCShare: El Malware de Android que usa el Lector NFC.



Fuente:D3lab

Una nueva y evolucionada cepa de malware para Android, conocida como NFCShare, está poniendo en grave riesgo a usuarios de teléfonos móviles en toda Europa. Este sofisticado troyano bancario se distribuye a través de versiones falsificadas de aplicaciones bancarias legítimas y está diseñado para robar silenciosamente los datos de las tarjetas de pago y el PIN utilizando el chip NFC del teléfono de la víctima

¿Cómo funciona?

1. Combina ingeniería social avanzada con capacidades técnicas de suplantación.

2.Las víctimas son atraídas a portales web fraudulentos que imitan a la perfección la interfaz de su banco.

3.Una vez que el usuario ingresa sus credenciales bancarias en la página falsa, aparece un mensaje indicando que su aplicación bancaria necesita ser actualizada de manera urgente.

4.La página redirige a la víctima mediante una URL acortada (como TinyURL) para descargar un archivo APK malicioso con nombres que imitan a los reales.

5.Una vez que la víctima instala y abre la aplicación falsa, se encuentra con una pantalla que simula ser un proceso de verificación de tarjeta de seguridad estándar.

6.La aplicación pide al usuario que acerque su tarjeta de crédito o débito física a la parte posterior del teléfono. Utilizando el lector NFC nativo de Android y el protocolo EMV estándar, el malware extrae silenciosamente la información de la tarjeta: número, fecha de caducidad y el tipo de tarjeta. Posteriormente, la interfaz solicita que el usuario introduzca su PIN de 4 dígitos "por seguridad".

7.Todos estos datos son empaquetados y enviados en tiempo real a un servidor de comando y control (C2) controlado por los delincuentes a través de una conexión WebSocket, dejando la cuenta bancaria de la víctima completamente expuesta.

¡Conoce más aquí!

02 Amenazas de Ciberseguridad – Mundial de la FIFA 2026

La Copa Mundial de la FIFA 2026 presenta un riesgo cibernético debido a su enorme evento, la dispersión geográfica en tres países y el uso de Inteligencia Artificial (IA) por parte de los ciberdelincuentes para generar sus ataques.

1. Principales Vectores de Ataque

- Combina Fraude con entradas: Se han detectado más de 4,300 dominios falsos que clonan la web oficial de la FIFA, generando pérdidas millonarias.
- Redes sociales y Apps falsas: Más de 1,700 cuentas falsas (90% en Facebook e Instagram) y distribución de malware camuflado en apps de apuestas, transporte o transmisión de partidos.
- Robo de credenciales: Ofertas de empleo falsas para trabajadores temporales y la filtración de miles de credenciales de empleados y usuarios de la FIFA, facilitando futuros ataques.

2. El Factor de la IA y la Ingeniería Social

- Ataques perfectos: La IA permite crear correos de phishing sin errores ortográficos y generar deepfakes de audio y video altamente realistas.
- Phishing temporal: Los ataques basados en la urgencia y la emoción del torneo cuadruplican su tasa de éxito.
- Riesgo corporativo a largo plazo: Las contraseñas robadas a los aficionados suelen reutilizarse en cuentas corporativas, facilitando ataques a empresas meses después.

3. Vulnerabilidades de Infraestructura y Dispositivos Móviles

- Cadena de suministro débil: Más del 33% de los patrocinadores y proveedores carecen de protección DMARC, permitiendo la suplantación de sus correos oficiales.
- Dispositivos móviles en la mira: El tráfico masivo de 6.5 millones de viajeros camufla ataques basados en códigos QR falsos y secuestro de sesiones en redes de roaming.

4. Recomendaciones Clave

Para Aficionados y Viajeros	Para Organizaciones y Proveedores
• Comprar y operar solo en canales oficiales.	• Implementar MFA resistente al phishing para personal y voluntarios.
• Usar contraseñas fuertes y no reutilizarlas.	• Configurar la protección DMARC en todos los dominios de correo.
• Activar la autenticación multifactor (MFA).	• Monitorear en tiempo real la actividad en dispositivos móviles, no solo en la red tradicional.

¡Conoce más aquí!

03 Un ataque **de secuestro de agentes engaña** a los agentes de codificación de IA para que ejecuten código malicioso.

Investigadores de ciberseguridad han identificado una nueva técnica de ataque denominada Agentjacking, la cual permite a atacantes engañar a agentes de IA utilizados en desarrollo de software para que ejecuten código malicioso directamente en las máquinas de los desarrolladores.

¿En qué consiste el ataque?

El ataque aprovecha una debilidad en la integración entre herramientas de monitoreo de errores como Sentry y asistentes de IA conectados mediante el Model Context Protocol (MCP).

El vector de ataque funciona de la siguiente forma:

- El atacante obtiene un Sentry DSN (Data Source Name) expuesto públicamente.
- Envía eventos de error falsos con contenido manipulado (Markdown malicioso).
- Estos eventos son interpretados por la IA como información legítima de depuración.
- Cuando el desarrollador solicita a la IA resolver errores, el agente recupera esos eventos.
- El asistente ejecuta comandos maliciosos creyendo que son instrucciones válidas.

Impacto del ataque

Si el agente de IA ejecuta el contenido malicioso, el atacante puede:
Ejecutar comandos en la máquina del desarrollador
Robar credenciales (Git, variables de entorno, tokens)
Acceder a repositorios privados
Exfiltrar información sensible del entorno de desarrollo

Este tipo de ataque es especialmente crítico porque no requiere vulnerar directamente la infraestructura, sino que abusa de la confianza entre herramientas.

Alcance y relevancia

- Se han identificado más de 2.300 organizaciones potencialmente expuestas mediante DSN accesibles.
- Pruebas controladas mostraron tasas de éxito de explotación superiores al 80% en asistentes como Cursor y Claude Code.
- El ataque se basa en técnicas de prompt injection indirecta, donde la IA no distingue entre datos legítimos y contenido malicioso.

Recomendaciones

- Evitar exponer públicamente credenciales DSN o restringir su uso.
- Validar y sanitizar entradas provenientes de sistemas externos.
- Ejecutar asistentes de IA en entornos aislados o sandbox.
- Implementar controles de “allowlist” para comandos ejecutados por agentes.
- Limitar privilegios de herramientas conectadas al agente de IA.
- Monitorear interacciones MCP y logs de acciones ejecutadas por la IA.

¡Conoce más aquí!

Vulnerabilidades **destacadas**

Microsoft Windows DHCP Client Remote Code Execution

CVE-2026-44815

Un atacante puede ejecutar código de forma remota enviando respuestas DHCP especialmente diseñadas desde un servidor DHCP malicioso. No requiere interacción del usuario y puede comprometer equipos que obtienen su configuración de red automáticamente.

Microsoft HTTP.sys Remote Code Execution

CVE-2026-47291

Afecta al controlador del kernel que procesa solicitudes HTTP. Un atacante puede enviar paquetes HTTP especialmente manipulados a un servidor vulnerable para ejecutar código con privilegios elevados. Es especialmente relevante para servidores con servicios web habilitados.

Microsoft Exchange Server Spoofing

CVE-2026-42897

Microsoft informó que esta vulnerabilidad había sido explotada y que permitía realizar ataques de suplantación a través de OWA, lo que incrementó su prioridad de remediación.

¡Conoce más aquí!

06 Ciberincidentes en Colombia y en el mundo

Ciberataque a revista SEMANA

El 19 de junio de 2026, Publicaciones SEMANA informó que sufrió un incidente informático que afectó parte de su infraestructura tecnológica. La organización comunicó que activó sus protocolos de respuesta, inició una investigación y trabajó para restablecer sus servicios. En ese momento no se confirmó públicamente el tipo de ataque (por ejemplo, ransomware o intrusión) ni el alcance definitivo sobre los datos comprometidos.

El medio dio a conocer la situación por medio de un comunicado en el que aseguró que ya activó sus protocolos de respuesta y notificó a las autoridades competentes.

Ataque contra cuatro bancos de Irán

El 14 de junio de 2026, un ciberataque afectó la infraestructura de comunicaciones compartida por cuatro de los principales bancos iraníes:

- Bank Melli
- Bank Tejarat
- Bank Saderat
- Export Development Bank of Iran

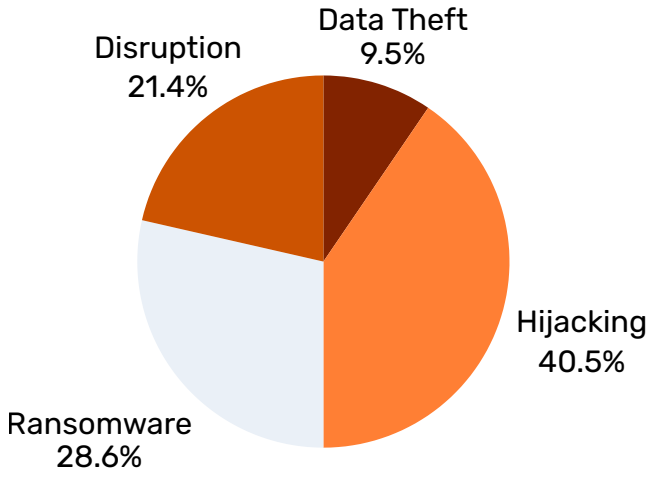
El ataque provocó interrupciones en los servicios bancarios durante un periodo de tiempo. Las autoridades iraníes indicaron que no existían evidencias de robo o eliminación de datos de clientes, aunque el incidente afectó una infraestructura crítica del sistema financiero. Ocurrió en un contexto de elevada tensión geopolítica, lo que incrementó su relevancia internacional.

El mundo

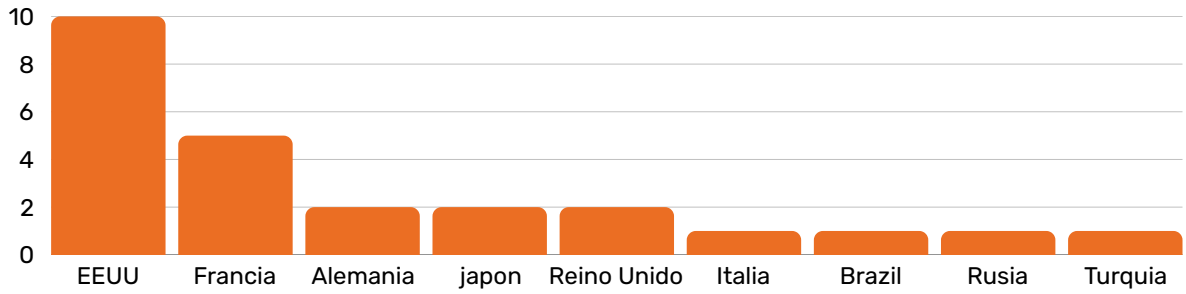
42
Ciber incidentes

Sectores afectados

Tipo de incidente



Países destacados



¡Conoce más aquí!

E-dea Networks

Para información adicional sobre cualquiera de nuestros productos o servicios, por favor contáctanos:

Email: contacto@e-dea.co
Teléfono: (601) 57 1 5188433 opción 2
Celular: (601) 57 3152231023

Visita nuestro sitio para más información: www.e-dea.co
Encuéntranos en: Carrera 7 # 156-10 Of. 1906-1801.
Torre Krystal - Centro Empresarial North Point