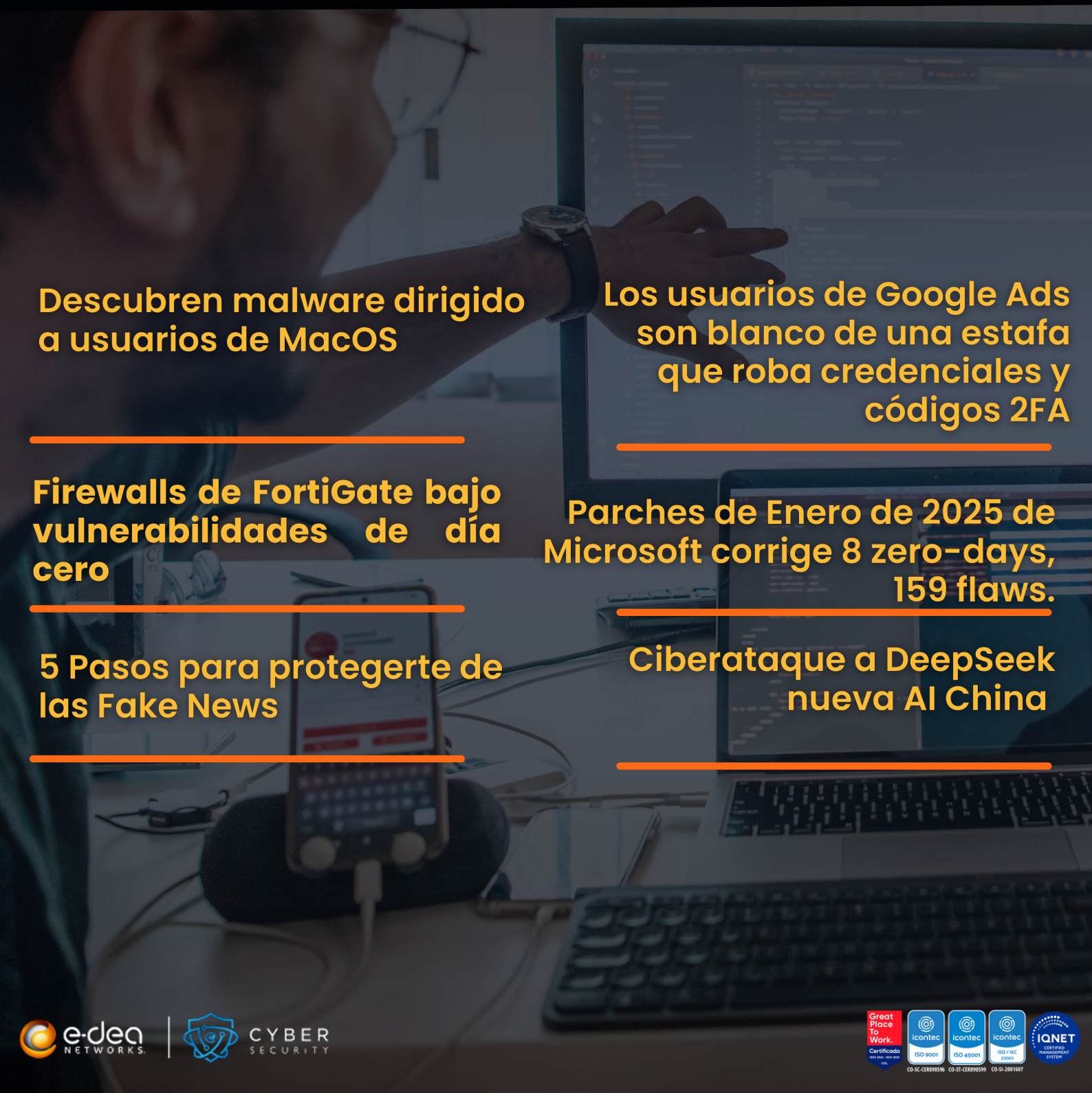
CIBER E-DEA

Boletín de Seguridad



Descubren malware dirigido a usuarios de MacOS

Los usuarios de Google Ads son blanco de una estafa que roba credenciales y códigos 2FA

Firewalls de FortiGate bajo vulnerabilidades de día cero

Parches de Enero de 2025 de Microsoft corrige 8 zero-days, 159 flaws.

5 Pasos para protegerte de las Fake News

Ciberataque a DeepSeek nueva AI China

Descubren malware dirigido a usuarios de MacOS

Investigadores de ciberseguridad descubrieron un malware que roba información de usuarios macOS. El nombre como es conocido este malware es Banshee Stealer. Esta versión actualizada fue descubierta en septiembre de 2024, donde este malware se distribuye por medio de sitios web de phishing y repositorios falsos de GitHub.

Condiciones Relevantes de Banshee Stealer

- Destaca el creciente número de muestras de malware de macOS
- Tiene un precio mensual de $3,000.
- Apunta a una amplia gama de navegadores, lo que lo convierte en una amenaza muy versátil y peligrosa.

Análisis de Banshee Stealer

Según los investigadores manifiestan que durante la valoración del Malware contenía todos los símbolos de C++ esto permitió identificar el código del proyecto. Donde pudieron conocer el nombre de los archivos de código fuente. En la siguiente imagen muestra un resumen de los .cpp nombre de los archivos filtrados a través de los símbolos en el binarios.

Nombre del archivo	Descripción
Controller.cpp	Gestiona tareas de ejecución básicas, incluidas medidas antidepuración, comprobaciones de idioma, recopilación de datos y exfiltración.
Browsers.cpp	Maneja la recopilación de datos de varios navegadores web.
System.cpp	Ejecuta AppleScripts para recopilar información del sistema y realizar phishing de contraseñas.
Tools.cpp	Proporciona funciones de utilidad para cifrado, creación de directorios y compresión, etc.
Wallets.cpp	Responsable de recopilar datos de las billeteras de criptomonedas.

Ejecución

Contraseña de Usuario

En la ejecución del malware, este crea una solicitud de contraseña por medio de Osascript, arrojando un cuadro de diálogo que dice “para iniciar la aplicación, debe actualizar la configuración del sistema. Ingrese su contraseña.

Recopilación de Información

La forma en que el malware recopila la información de archivos, Software y Hardware está compuesta de varios procedimientos, ejecutado el comando **system_profiler SPSoftware DataType SPHardwareDataType**, proporciona detalles sobre el software y el hardware del sistema.

Volcar contraseñas de llavero

Copia el llavero del sistema Library/Keychains/login.keychain-dba<temporary_path>/Passwords

Navegadores Capturados

El BANSHEE captura datos de 9 navegadores diferentes, junto con el historial del navegador, las cookies, los inicios de sesión, etc.

Exfiltración

Al momento que Banshee Stealer termina de recopilar datos, lo primero que realiza es comprimir. Posterior, cifra con XOR y se codifica y se transfiere a una solicitud de publicación a la URL http://45.142.122[.]92/send/ con el comando integrado cURL.

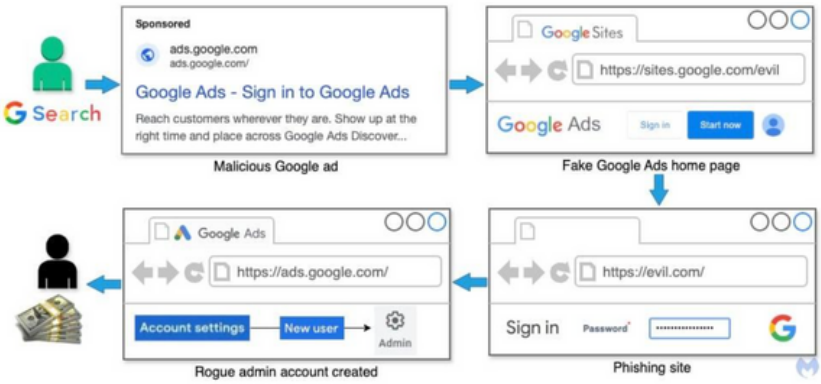
Más información

Los usuarios de Google Ads son blanco de una estafa de publicidad maliciosa que roba credenciales y códigos 2FA

Investigadores de ciberseguridad han alertado sobre una nueva campaña maliciosa que se dirige a usuarios y empresas que utilizan Google Ads. Los atacantes publican anuncios fraudulentos que redirigen a páginas de inicio de sesión falsas para robar credenciales de las cuentas de Google Ads. El objetivo es secuestrar las cuentas y utilizarlas para difundir más anuncios maliciosos, además de vender las credenciales robadas en foros clandestinos.

La campaña aprovecha una vulnerabilidad en Google Ads, permitiendo que los atacantes usen URLs fraudulentas que parecen legítimas.

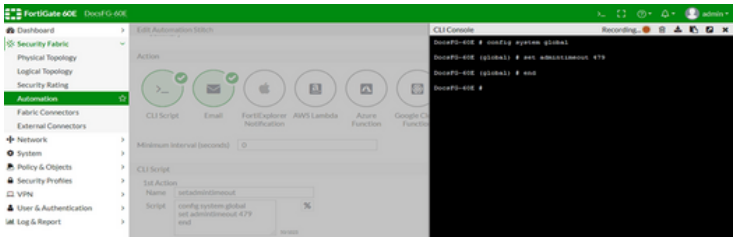
Las víctimas son llevadas a sitios de phishing alojados en Google Sites, donde sus datos de inicio de sesión y códigos 2FA son exfiltrados. Los atacantes luego toman control de las cuentas de Google Ads para crear nuevos anuncios falsos y seguir propagando la estafa.Se ha identificado que el grupo de atacantes probablemente opera desde Brasil y utiliza dominios portugueses para esconder la infraestructura de phishing. Aunque estas prácticas no violan directamente las políticas de Google Ads, la empresa aún no ha tomado medidas para detener las cuentas comprometidas.



1. La víctima ingresa la información de su cuenta de Google en la página de phishing.
2. El kit de phishing recopila identificadores únicos, cookies y credenciales.
3. La víctima puede recibir un correo electrónico indicando un inicio de sesión desde una ubicación inusual.
4. Si la víctima no logra detener este intento, se agrega un nuevo administrador a la cuenta de Google Ads a través de una dirección de Gmail diferente.
5. El actor de amenazas se lanza a una ola de gastos y excluye a las víctimas si pueden

Mas información

Firewalls de FortiGate bajo vulnerabilidades de día cero



Los dispositivos de firewall FortiGate de Fortinet están siendo atacados debido a vulnerabilidades de día cero.

Los ciberdelincuentes están explotando las interfaces de administración expuestas en redes públicas, obteniendo acceso no autorizado, comprometiendo las configuraciones del firewall mediante FortiOSy y violar las redes empresariales con FortiProxy.

Dispositivos afectados: Los dispositivos que ejecutan las versiones de firmware 7.0.14 a 7.0.16 (lanzadas entre febrero y octubre de 2024).

FortiOS 7.0.0 a 7.0.16, FortiProxy 7.0.0 a 7.0.19 y FortiProxy 7.2.0 a 7.2.12.

Fases de Ataque: El ataque implica un enfoque de múltiples fases observado entre noviembre y diciembre de 2024, que incluye:

- Escaneo de dispositivos vulnerables.
- Modificación de configuraciones para probar privilegios de administrador.
- Creación o secuestro de cuentas de administrador para configurar el acceso VPN SSL.
- Extracción de información confidencial de cuentas mediante la replicación de dominio.
- Los atacantes utilizaron direcciones IP falsificadas, como 127.0.0.1 y 8.8.8.8, para ocultar actividades

Respuesta de Fortinet: Fortinet está investigando el problema tras ser informado por Arctic Wolf.

Es crucial tomar medidas inmediatas para desactivar el acceso público, actualizar el firmware y monitorear las anomalías para evitar una mayor explotación. Mantenerse alerta y ser proactivo es esencial para contrarrestar estas amenazas en constante evolución.

Recomendaciones:

Deshabilitar inmediatamente el acceso a la interfaz de administración pública.

- Actualizar periódicamente el firmware a la última versión estable.
- Monitorear comportamientos inusuales como inicios de sesión de administrador de corta duración o uso de IP sospechoso.
- Habilitar la autenticación multifactor (MFA) para el acceso de administrador.
- Realizar una búsqueda exhaustiva de amenazas para detectar actividades sospechosas.

Más información

Parches de Enero de 2025 de Microsoft corrige 8 zero-days, 159 flaws

Microsoft lanzó actualizaciones de seguridad para 159 fallos, incluyendo ocho vulnerabilidades de día cero.

Vulnerabilidades Críticas: Se corrigieron doce vulnerabilidades críticas que incluyen divulgación de información, elevación de privilegios y ejecución remota de código.

CVE-2025-21380 - Azure Marketplace SaaS Resources Information Disclosure Vulnerability

CVE-2025-21296 - BranchCache Remote Code Execution Vulnerability

Vulnerabilidades Públicas: Cinco vulnerabilidades de día cero fueron divulgadas públicamente, incluyendo problemas en Windows App Package Installer y Windows Themes.

CVE-2025-21275 - Vulnerabilidad de elevación de privilegios del instalador de paquetes de aplicaciones de Windows

CVE-2025-21308 - Vulnerabilidad de suplantación de temas de Windows

CVE-2025-21186, CVE-2025-21366, CVE-2025-21395 - Vulnerabilidad de ejecución

Día Cero Activo: Tres vulnerabilidades de día cero fueron explotadas activamente en ataques, todas relacionadas con Windows Hyper-V.

CVE-2025-21333
CVE-2025-21334,
CVE-2025-21335

Vulnerabilidad de elevación de privilegios de VSP de integración de kernel de Windows Hyper-V NT

Más Información

5 Pasos para protegerte de las Fake News

1. **Se cauteloso:** Las redes sociales permiten que los usuarios publiquen información. Esta información puede ser falsa con el objetivo de maximizar las visualizaciones y tiempos de permanencia.

2. **Sé consciente de tus propios sesgos:** Reconoce tus propias creencias y prejuicios que pueden influir en cómo interpretas la información.

3. **Cuestiona los titulares:** Los titulares pueden ser engañosos o sensacionalistas. Lee más allá del titular y evalúa el contenido completo para obtener un contexto adecuado.

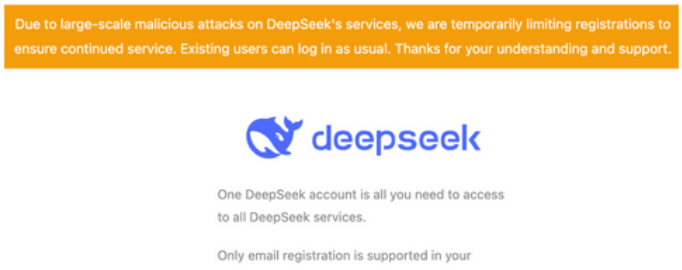
4. **Identifica el sesgo:** Aprende a reconocer el sesgo en los medios. Algunos medios pueden tener inclinaciones políticas o comerciales .

5. **Verifica las fuentes:** Asegúrate de que la información provenga de fuentes confiables y reconocidas. fijate en la fecha, Investiga sobre el autor, y la organización detrás del contenido

Ciberataque a Deepseek nueva AI China

DeepSeek dijo que su nueva aplicación popular fue víctima de un ciberataque el lunes 27 de enero, lo que obligó a la compañía china a limitar temporalmente los registros. El ataque se produjo después de que la aplicación de asistente de inteligencia artificial DeepSeek se disparara a la cima de la App Store de Apple, convirtiéndose en la aplicación gratuita mejor calificada en los EE. UU., y escalara posiciones en la Play Store de Google.

En su página de estado , DeepSeek dijo que comenzó a investigar el problema el lunes por la noche, hora de Beijing. Después de aproximadamente dos horas de monitoreo, la compañía dijo que fue víctima de un "ataque malicioso a gran escala". Si bien DeepSeek limitó los registros, los usuarios existentes aún pudieron iniciar sesión como de costumbre. La aplicación ahora permite registros nuevamente



La aplicación de DeepSeek es un asistente de inteligencia artificial similar al chatbot ChatGPT de OpenAI. La noticia del ascenso de la aplicación en Estados Unidos (y su capacidad para superar a los rivales estadounidenses por una fracción del costo) hizo que las acciones de tecnología cayeran el lunes. Nvidia, el fabricante de chips de inteligencia artificial y la empresa más valiosa de Estados Unidos, vio sus acciones desplomarse un 13,6% en las primeras operaciones, eliminando unos 500.000 millones de dólares en capitalización de mercado.

Más información

CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

www.e-dea.co