DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 01

29 • 01 • 25

Tipo de Amenaza:

Vulnerabilidad

Plataforma

Dispositivos iPhone, iPad y Mac

MUY ALTO

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre una vulnerabilidad crítica en el componente Core Media del Sistema Operativo de los dispositivos de la empresa Apple, identificada como CVE-2025-24085, CVE-2025-24160, CVE-2025-24161 y CVE-2025-24163. Si un ciberdelincuente llegase a explotar la vulnerabilidad, podría obtener permisos de administrador en los dispositivos, lo que le permitiría obtener el control total del mismo y poner en riesgo su integridad.

Para mitigar este riesgo, se han lanzado actualizaciones de seguridad en las siguientes versiones y dispositivos:

•IOS 18.3 y iPadOS 18.3: iPhone XS y modelos posteriores, iPad Pro de 13 pulgadas, iPad Pro de 12,9 pulgadas de 3ª generación , iPad Pro de 11 pulgadas de 1ª generación, iPad Air de 3ª generación, iPad de 7ª generación y iPad mini de 5ª generación y modelos posteriores.

•tvOS 18.3: Apple TV HD y Apple TV 4K (todos los modelos).

•visionOS 2.3: Apple Vision Pro.

•watchOS 11.3: Apple Watch Series 6 y modelos

RECOMENDACIONES:

Apple ha lanzado una actualización de seguridad crítica en sus Sistemas Operativos. Se recomienda a todos los usuarios actualizar sus dispositivos a la versión más reciente para protegerse de posibles ataques.

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 02

10 • 02 • 25

MUY ALTO

Tipo de Amenaza:

Phishing

Plataforma

Correo Electrónico / Mercado Libre

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre una modalidad de engaño del tipo phishing, con la finalidad de infectar los dispositivos con un malware. El mismo consiste en un aparente correo electrónico de Mercado Libre, mediante el cual informan sobre una alerta de seguridad relacionada con la cuenta del usuario, receptor del e-mail. En este caso invitan hacer clic en el enlace **"NO FUI YO"**, redirigiendo a la persona a una página falsa, diseñada visualmente similar a la de Mercado Libre, con el propósito de robar información personal y financiera.

RECOMENDACIONES:

- En caso de recibir correos de dudosa procedencia, no ingrese a enlaces o archivos adjuntos.
- Verifica la URL: Revisa cuidadosamente la dirección del navegador antes de ingresar cualquier dato. Si tenés dudas, accedé directamente a la página desde el navegador escribiendo la URL, en lugar de hacer clic en el enlace del correo.
- Revisá la autenticidad del correo: Corrobora que provenga de una dirección oficial.
- Nunca compartas tus datos personales: Ninguna empresa te solicitará contraseñas, tarjetas de crédito o información personal a través de un correo electrónico o mensaje.
- Actualiza siempre el software de seguridad, aplicaciones y sistema operativo, en todos tus dispositivos.
- Infórmate sobre las nuevas amenazas cibernéticas.

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 03

12 • 02 • 25

Tipo de Amenaza:

Vulnerabilidad

Plataforma

Dispositivos iPhone, iPad y Mac

MUY ALTO

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre una vulnerabilidad crítica de tipo zero-day en iOS y iPadOS de los dispositivos de la empresa Apple, identificada como CVE-2025-24200. Este fallo, que afecta el modo de restricción USB, permite a los atacantes desactivar esta protección sin necesidad de un código de desbloqueo, facilitando el acceso físico no autorizado a dispositivos bloqueados. Para mitigar este riesgo, se han lanzado actualizaciones de seguridad en las siguientes versiones y dispositivos:

- iOS 18.3.1 y iPadOS 18.3.1: iPhone XS y modelos posteriores, iPad Pro de 13 pulgadas, iPad Air de tercera generación y modelos más recientes.

- PadOS 17.7.5: iPad Pro de 12.9 pulgadas (segunda generación) y modelos más antiguos.

RECOMENDACIONES:

Para actualizar su dispositivo móvil y activar las actualizaciones automáticas, vaya a Ajustes > General > Actualización de software > Personalizar actualizaciones automáticas y, a continuación, active 'Instalar actualizaciones de iOS'. Para actualizar su computadora, diríjase a "Preferencias del Sistema" en el menú Apple y, después haga clic en 'Actualización de software' para comprobar si hay actualizaciones disponibles. Si las hay, haga clic en el botón 'Actualizar ahora' para instalarlas o en 'Más información' para ver detalles sobre cada actualización.

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 04

14 • 02 • 25

Tipo de Amenaza:

Vulnerabilidad

Plataforma

Sistema Operativo Windows

MUY ALTO

DESCRIPCIÓN:

Se informa que el Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre varias vulnerabilidades en el Sistema Operativo Microsoft Windows.

Estas vulnerabilidades, explotadas activamente, permiten la elevación de privilegios y comprometen la seguridad de dicho Sistema Operativo, facilitando el acceso no autorizado y el control total de los dispositivos. Dichas fallas estan identificadas con el código CVE-2025-21391 y CVE-2025-21418.

Si un ciberdelincuente llegase a explotar estas vulnerabilidades, podría:

- Elevar privilegios en el subsistema de almacenamiento y en el núcleo del sistema.
- Comprometer de manera total el sistema, permitiendo la ejecución de código malicioso.
- Obtener acceso no autorizado a datos sensibles y recursos críticos.

RECOMENDACIONES:

- Aplicar las actualizaciones de seguridad proporcionadas por Microsoft a través de Windows Update.
- Revisar y reforzar las configuraciones de seguridad en los sistemas afectados.
- Monitorizar los dispositivos en busca de actividades sospechosas que puedan indicar intentos de explotación.
- Implementar controles de acceso y segmentación de red para limitar el alcance de un posible compromiso.

Windows

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 05

25 • 03 • 25

Tipo de Amenaza:

Vulnerabilidad

Plataforma

Navegador Google Chrome

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento, sobre una vulnerabilidad crítica en el navegador Google Chrome identificada como StilachiRAT.

Se trata de un troyano de acceso remoto que actúa desde el navegador de Chrome en Windows con el objetivo de recopilar información sobre el equipo infectado (sistema operativo, sesiones activas de escritorio remoto, aplicaciones en ejecución), de la billetera digital, de las credenciales almacenadas en el navegador de Google y la información sobre el portapapeles.

El desarrollador advierte que StilachiRAT puede instalarse en el equipo mediante diversos vectores, como lo son herramientas de software y actualizaciones que simulan ser legítimas o proceden de fuentes no oficiales ni fiables.

RECOMENDACIONES:

- Mantener actualizados los navegadores web en su última version.
- Emplear soluciones de seguridad antivirus preferentemente licenciadas.
- Examinar las extensiones instaladas en el navegador y eliminar las que no sean esenciales o que provengan de fuentes poco confiables.
- Evitar acceder a sitios web dudosos o hacer clic en enlaces desconocidos.
- Evitar el guardado de credenciales de acceso al navegador y borrar el historial periódicamente.

Google Chrome

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 06

25.03.25

Tipo de Amenaza:

Phishing

Plataforma

Correo electrónico

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre una nueva modalidad de engaño, a través de un correo electrónico de dudosa procedencia, que fue recibido en varias cuentas del correo Institucional.

Del análisis preliminar surge que el mismo corresponde a un correo del tipo phishing, proveniente de la cuenta salud.bienestar@santafe.gob.ar con el asunto "Policiafederal.gov.ar Portal de resolución |Case No. #729261", simulando ser el administrador de las cuentas oficiales del correo electrónico Institucional, donde sugieren hacer clic en un enlace **"Validar ahora"** para actualizar la cuenta.

Una vez que se ingresa al link, redirige a un sitio determinado, el cual intenta suplantar la identidad de un portal similar al correo institucional de esta Policía Federal Argentina, cuyo fin es el robo de las credenciales.

RECOMENDACIONES:

- En caso de recibir un mensaje con las características descriptas, no respondas ni hagas clic en el enlace proporcionado. Es recomendable eliminarlo y poner en conocimiento a su entorno sobre este intento de fraude y así poder evitar otras posibles víctimas.
- Verificar siempre la URL en la cual se van a ingresar las credenciales de acceso.

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 07

14 • 04 • 25

Tipo de Amenaza:

Vulnerabilidad

Plataforma

WinRAR

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento, sobre una nueva vulnerabilidad en el software de compresión de datos WinRAR identificada como CVE-2025-31334.

Todas las versiones de WinRAR a excepción de la más reciente (7.11) se vieron afectadas por esta vulnerabilidad.

Los ciberdelincuentes pueden crear archivos .RAR con enlaces simbólicos maliciosos que apuntan a archivos ejecutables, engañando así a los usuarios para que ejecuten código no confiable sin el aviso habitual de MotW (Marca de la Web) de Windows, el cual advierte a los usuarios antes de abrir contenido potencialmente peligroso. Esta vulnerabilidad permite a los atacantes eludir esta protección, pudiendo así obtener acceso remoto a nuestro equipo, instalar malware de forma oculta, robar nuestros datos personales o afectar nuestro sistema operativo.

RECOMENDACIONES:

- Actualizar el programa a la última versión 7.11.
- Utilizar soluciones antivirus preferentemente licenciadas.
- No hacer clic en enlaces de dudosa procedencia.
- Actualizar el sistema operativo a la última versión disponible que incluya los parches de seguridad correspondientes.

RARLAB®

WinRAR®

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 08

12 • 05 • 25

ALTO

Tipo de Amenaza:

Phishing

Plataforma

Correo Electronico

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre una nueva modalidad de engaño, a través de un correo electrónico de dudosa procedencia, que fue recibido en varias cuentas del correo Institucional.

Del análisis preliminar surge que el mismo corresponde a un correo del tipo phishing, donde sugieren hacer clic en un enlace " **haga clic aqui"** para actualizar la cuenta.

Una vez que se ingresa al link, se redirige a un sitio malicioso, el cual intenta suplantar la identidad de un portal cuyo fin es el robo de las credenciales.

LINK MALICIOSO

RECOMENDACIONES:

¿Qué hacer si recibís un correo similar?

- No hagas clic en ningún enlace ni descargues archivos adjuntos.
- No ingreses tus credenciales (usuario y contraseña) en sitios web de dudosa reputación.
- Reportalo inmediatamente al Centro de Operaciones de Seguridad (SOC) de esta Unidad.
- En caso de recibir un mensaje con las características descriptas, es recomendable eliminarlo y poner en conocimiento a su entorno sobre este intento de fraude y así poder evitar otras posibles victimas.
- Verificar siempre la URL en la cual se van a ingresar las credenciales de acceso. Al pasar el cursor sobre "haga clic aquí" se observa un dominio ajeno a nuestra Institución.

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 09

27 05 25

Tipo de Amenaza:

Vulnerabilidad Navegador Web

Plataforma

Mozilla Firefox

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre dos vulnerabilidades críticas de tipo zero-day en el navegador Mozilla Firefox identificadas como CVE-2025-4918 y CVE-2025-4919.

La primera vulnerabilidad permite a un atacante ejecutar código malicioso de manera remota, lo que puede comprometer el sistema afectado, facilitando la instalación de software dañino o permitiendo que el atacante tome el control del dispositivo a distancia.

La segunda vulnerabilidad está vinculada al manejo de ciertos componentes de la memoria por parte del navegador web; si un atacante logra aprovechar esta falla, podría provocar una alteración en dicha memoria que le permitiría ejecutar un código de forma remota, comprometiendo así la seguridad e integridad del sistema.

RECOMENDACIONES:

- Actualizá Mozilla Firefox a la ultima versión para mitigar las vulnerabilidades.
- Configurá políticas de navegación segura y evitá el acceso a sitios web no confiables.
- Mantené el software antivirus actualizado para detectar y eliminar diversas amenazas.
- Revisá las extensiones instaladas en el navegador y eliminá las que no sean esenciales o provengan de fuentes poco confiables.
- Asegurá que todos los sistemas afectados tengan habilitadas las últimas actualizaciones.
- No utilices la extensión de doble autenticación en el navegador web, limitando esta función exclusivamente a tu teléfono celular.

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 10

03
06
25

ALTO

Tipo de Amenaza:

Estafa de Acceso Remoto

Plataforma

Billeteras virtuales

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre un tipo de estafa virtual en la que utilizan aplicaciones de acceso remoto para vaciar cuentas bancarias.

La estafa comienza con una llamada telefónica, un mensaje en redes sociales o un correo electrónico donde el ciberdelincuente refiere ser representante del Banco de la Nación Argentina y solicita al usuario que descargue una app como "TeamViewer" o "AnyDesk" con la excusa de ayudar a solucionar un inconveniente en la cuenta o activar una promoción exclusiva. Una vez instalada, esa aplicación de acceso remoto, habilita a los delincuentes a controlar el celular o la computadora de la víctima, a distancia.

Además, los estafadores instan al usuario a que les envíen un código que "verifica" la operación. En realidad, se trata de un código de autenticación que les da acceso directo al home banking o a billeteras virtuales como BNA+, Mercado Pago o Ualá.

RECOMENDACIONES:

Qué hacer si instalaste una app de acceso remoto sin querer:

1. Apagá el dispositivo de inmediato para cortar la conexión.
2. Sin volver a conectarte a internet, desinstalá la app.
3. Cambiá todas tus contraseñas desde un equipo seguro.
4. Llamá a tu banco para notificar lo sucedido.

TeamViewer

AnyDesk

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 11

10
06
25

Tipo de Amenaza:

Phishing

Plataforma

Correo electrónico

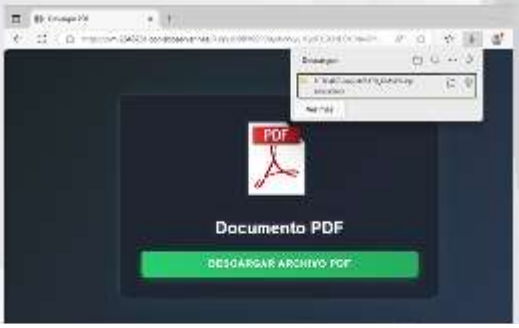
DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre una nueva modalidad de engaño, a través de un correo electrónico de dudosa procedencia, simulando ser la Agencia de Recaudación y Control Aduanero (ARCA).

Del análisis preliminar surge que el mismo corresponde a un correo del tipo phishing, proveniente de la cuenta serviciosarca@afip.com con el asunto "Multa Registrada en su Documento 900061", el cuerpo del menaje proporciona un link adjunto para visualizar el "documento fiscal", el cual al hacer clic sobre el mismo, redirige a la descarga de un archivo comprimido .ZIP. Este contiene un programa malicioso, que si se ejecuta podría comprometer la seguridad del equipo.

RECOMENDACIONES:

- En caso de recibir un mensaje con las características descriptas, no responda ni haga clic en el enlace proporcionado.
- En caso de haber descargado el archivo pero no haberlo ejecutado asegúrese de eliminarlo de la carpeta de descargas como de la papelera de reciclaje. Si el mismo fue ejecutado, desconectar el equipo de la red y contactarse con esta Dependencia.
- Contar con una solución antivirus actualizada, para evitar infecciones y bloquear posibles comunicaciones de spam.



DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 12

10
07
25

Tipo de Amenaza:

Phishing

Plataforma

Correo electrónico

MEDIO

DESCRIPCIÓN:

El Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre una nueva modalidad de engaño, a través de un correo electrónico de dudosa procedencia.

Del análisis preliminar surge que el mismo corresponde a un correo del tipo phishing, proveniente de la cuenta nghiand4@msb.com.vn con el asunto "Aviso de encuesta sobre servicios TI" donde sugieren hacer clic en un enlace "**Hace clic acá para comenzar la Encuesta de Servicios TI**" para realizar una encuesta de satisfacción, con la excusa de migrar a un servidor Webmail, debido a un aumento de amenzas como el spam y el phishing.

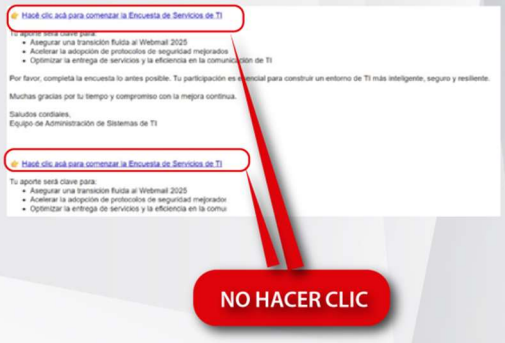
Una vez que se ingresa al link descripto, redirige a una URL maliciosa: **https://dancing-naiad5cfd65.netlify.app/** cuyo fin es el robo de credenciales o infección por malware.

RECOMENDACIONES:

• En caso de recibir un mensaje con las características mencionadas, no respondas ni hagas clic en el enlace proporcionado. Es recomendable eliminarlo y poner en conocimiento a su entorno sobre este intento de fraude y así poder evitar otras posibles víctimas.

• Cambiar contraseñas si se sospecha de compromiso de credenciales.

• Verificar siempre la URL en la cual se van a ingresar las credenciales de acceso.



DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 13

24
07
25

Tipo de Amenaza:

Smishing

Plataforma

Mensaje de Texto (SMS)

DESCRIPCIÓN:

El Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre una nueva modalidad de engaño, que circula a través de un mensaje de texto (SMS), suplantando la identidad del Correo Argentino, intentando convencer a la víctima de actualizar la dirección de destino para recibir un supuesto paquete, acompañado del siguiente enlace:
"https://shorturl.at/21cpx"
El mismo redirecciona al estado de entrega de su paquete, y al hacer clic en "Continuar", ingresa a un formulario similar al que se utiliza para el seguimiento de envíos, donde el usuario tiene que acceder con sus datos personales.
Después de completar el formulario, es redirigido a la página de "Pago en Línea", donde se le solicitan los datos de una tarjeta de crédito y/o débito como método de pago.

Recordatorio de Correos de Argentina:
Debido a un problema con su dirección, su paquete ha sido almacenado temporalmente en el almacén. Aunque intentamos entregarlo dos veces, no fue posible. Para evitar una devolución, actualice su dirección

Tras la actualización, intentaremos entregarlo nuevamente en un plazo de 8 horas.
¡Buen día y buen trabajo! Correos de Argentina.
(responder Y volver a abrir este

RECOMENDACIONES:

- En caso de recibir un mensaje con las características descriptas, no responda ni haga clic en el enlace proporcionado.
- Nunca compartas tus datos personales: ninguna empresa te solicitará contraseñas, tarjetas de crédito o información personal a través de un mensaje.
- Contar con una solución antivirus actualizada, para evitar infecciones y bloquear posibles comunicaciones de spam.
- Infórmate sobre las nuevas amenazas cibernéticas.

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 14

07
08
25

Tipo de Amenaza:

Phishing

Plataforma

Correo Electronico

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre una nueva modalidad de engaño, a través de un correo electrónico de dudosa procedencia, con asunto **"Confirmación de Documento Laboral - Expediente 7831560"**.

Del análisis preliminar surge que el mismo corresponde a un correo del tipo phishing, en el coxtexto de una relación laboral previamente registrada, donde sugieren que accedas al archivo PDF adjunto con contraseña (aparentemente inofensivo). Una vez descargado el PDF te incita a hacer clic en **Certificado,** infectando tu computadora con malware.

RECOMENDACIONES:

- En caso de recibir un mensaje con las características descriptas, no responda ni haga clic en el enlace proporcionado.
- En caso de haber descargado el archivo pero no haberlo ejecutado asegúrese de eliminarlo de la carpeta de descargas como de la papelera de reciclaje. Si el mismo fue ejecutado, desconectar el equipo de la red y contactarse con esta Dependencia.
- Contar con una solución antivirus actualizada, para evitar infecciones y bloquear posibles comunicaciones de spam.
- Cambiar contraseñas si se sospecha de compromiso de credenciales.

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 16

14 08 25

Tipo de Amenaza:

Vulnerabilidad

Plataforma

Zoom

DESCRIPCIÓN:

El Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento, sobre nuevas vulnerabilidades en la plataforma Zoom, estas vulnerabilidades críticas detectadas en la aplicación podrían permitir a un ciberatacante realizar una escalada de privilegios a través del acceso a la red y la ejecución remota de código. En el caso de que las mismas fueran explotadas, el atacante podría hacerse con el acceso no autorizado de una cuenta, divulgar o capturar información sensible de forma local o realizar acciones que impidan el desarrollo de una reunión o llamada.

El problema reportado afecta a los siguientes productos:

- Zoom Workplace (versión anterior a la 6.3.10).
- Zoom Workplace VDI (excepto 6.1.16 y 6.2.12).
- Zoom Rooms y Zoom Rooms Controller (versión anterior a la 6.3.10).
- Zoom Meeting SDK (versión anterior a la 6.3.10).

RECOMENDACIONES:

- Desde la página oficial actualizar el programa a la última versión 6.3.10 y, en entornos VDI, aplicar las versiones corregidas 6.1.16 o 6.2.12, o superiores.
- Utilizar soluciones antivirus preferentemente licenciadas.
- No hacer clic en enlaces de dudosa procedencia.
- Actualizar el sistema operativo a la última versión disponible que incluya los parches de seguridad correspondientes.

zoom

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 17

20
08
25

Tipo de Amenaza:

Phishing

Plataforma

Correo electrónico

ALTO

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre una nueva modalidad de engaño, a través de diferentes correos electrónicos: contabilidadintegral@mpba.gov.ar,estudiodecontadores@colon.gov.ar, planificacioncontable@iosper.gov.ar, los cuales son de dudosa procedencia.

Del análisis preliminar surge que corresponden a un correo del tipo phishing, con el asunto "Tu recibo esta disponible para bajar" o "Ya podes descargar tu factura", donde en el cuerpo del menaje se proporciona un link adjunto para visualizar la factura. Al hacer clic sobre el mismo, redirige a un sitio malicioso, conteniendo una URL que simula ser un acceso a correo real, y que puede llevar al robo de credenciales.

RECOMENDACIONES:

- En caso de recibir un mensaje con las características descriptas, no responda ni haga clic en el enlace proporcionado.
- En caso de haber descargado el archivo pero no haberlo ejecutado asegúrese de eliminarlo de la carpeta de descargas como de la papelera de reciclaje. Si el mismo fue ejecutado, desconectar el equipo de la red y contactarse con esta Dependencia.
- Contar con una solución antivirus actualizada, para evitar infecciones y bloquear posibles comunicaciones de spam.

DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 18

21.08.25

Tipo de Amenaza:

Ingeniería Social

Plataforma

Navegadores Web

MEDIO

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento, sobre una nueva modalidad de engaño que involucra el uso de CAPTCHAs falsos.

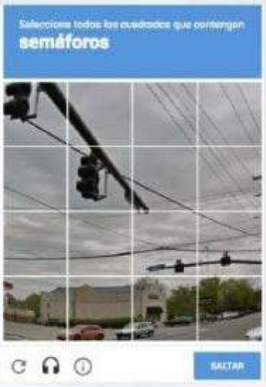
Los ciberdelincuentes utilizan anuncios web engañosos que redirigen al usuario a páginas que imitan CAPTCHAs legítimos.

Una vez que el usuario ingresa a este sitio web es persuadido de ingresar comandos o combinaciones de teclas, lo cual permitirá la instalación de un software malicioso, sin que la víctima se percate de esta acción.

La finalidad del mismo es el robo de contraseñas, información financiera y personal.

RECOMENDACIONES:

- No ingreses a sitios web de dudosa procedencia, verifica siempre la URL y asegurate de que sea legítima y segura.
- Mantenete atento a comportamientos inusuales, como la solicitud de ejecución de comandos o combinaciones de teclas.
- Si sos redirigido a una página web desconocida cerrala de inmediato.
- Evita realizar clics compulsivos, dedica unos segundos extras para verificar la legitimidad del desafio.



DIVISION SEGURIDAD INFORMATICA

BOLETIN INFORMATIVO 19

22.08.25

Tipo de Amenaza:

Vulnerabilidad

Plataforma

Sistemas operativos iOS, iPadOS y macOS

DESCRIPCIÓN:

Este Centro de Operaciones de Seguridad (SOC), ha tomado conocimiento sobre una vulnerabilidad crítica de tipo zero-day en iOS, macOS y iPadOS de los dispositivos de la empresa Apple, identificada como CVE-2025-43300. La vulnerabilidad, permite a un atacante no autenticado ejecutar código malicioso de forma remota simplemente enviando una imagen manipulada al dispositivo de la víctima. Para mitigar este riesgo, se han lanzado actualizaciones de seguridad en los siguientes productos afectados:

- iPhone XS , iPad Pro de 13 pulgadas, iPad mini, iPad Air de tercera generación y modelos más recientes.
- Macs con el sistema macOS Ventura, macOS Sonoma, macOS Sequoia

RECOMENDACIONES:

Para actualizar su dispositivo móvil y activar las actualizaciones automáticas, vaya a Ajustes > General > Actualización de software > Personalizar actualizaciones automáticas y, a continuación, active 'Instalar actualizaciones de iOS'. Para actualizar su computadora, diríjase a "Preferencias del Sistema" en el menú Apple y, después haga clic en 'Actualización de software' para comprobar si hay actualizaciones disponibles. Si las hay, haga clic en el botón 'Actualizar ahora' para instalarlas o en 'Más información' para ver detalles sobre cada actualización.