

ALERTA INTEGRADA DE SEGURIDAD DIGITAL



La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.


Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Un sitio web falso que ofrece "Notepad++ para Mac" podría representar un riesgo de malware para los usuarios de Mac. 4

Índice alfabético 6

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 065			Fecha: 05-05-2026
				Página: 4 de 6
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL			
Nombre de la alerta	Un sitio web falso que ofrece "Notepad++ para Mac" podría representar un riesgo de malware para los usuarios de Mac.			
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC	
Medios de propagación	Red, Internet			
Código de familia	H	Código de Sub familia	H01	
Clasificación temática familia	Intento de intrusión			

Descripción

1. ANTECEDENTES:

En mayo de 2026 se detectó la circulación de un sitio web fraudulento que afirma ofrecer una versión oficial de "Notepad++ para macOS", aprovechándose de la popularidad y reputación de este editor de texto. La alerta fue difundida tras confirmarse que el proyecto legítimo Notepad++ nunca ha publicado una versión nativa para Mac, y que el dominio fraudulento fue diseñado para parecer una extensión oficial del proyecto original, incluso llegando a confundir a usuarios y a algunos medios tecnológicos. Este caso evidencia cómo las técnicas de suplantación de marca siguen siendo un vector efectivo para comprometer la seguridad de los usuarios finales.



Ilustración 1 Un sitio web falso que ofrece "Notepad++ para Mac" podría representar un riesgo de malware para los usuarios de Mac.

2. DETALLES:

El sitio identificado, notepad-plus-plus-mac[.]org, replica el nombre, logotipo, colores y lenguaje visual de Notepad++ para generar confianza. Incluso incluye una sección de "autores" donde aparece el fundador real del proyecto, Don Ho, sin su consentimiento, dando la falsa impresión de legitimidad. Aunque el software descargable podría basarse en código abierto, el riesgo principal radica en la forma engañosa de distribución, que induce a los usuarios a instalar una aplicación creyendo que es oficial. Este tipo de portales falsos se asocia frecuentemente con campañas de malware, ya sea a través de instaladores alterados, publicidad maliciosa o futuras actualizaciones comprometidas. El propio fundador de Notepad++ confirmó que el sitio no está autorizado ni afiliado al proyecto y constituye una violación de marca que pone en riesgo a los usuarios.

3. RECOMENDACIONES:

- Descargar software únicamente desde los sitios oficiales de los desarrolladores o repositorios reconocidos.
- Verificar si una aplicación realmente existe para el sistema operativo antes de instalarla.
- Desconfiar de dominios “no oficiales” que imitan nombres populares añadiendo palabras como mac, download o official.
- Mantener activo y actualizado un antimalware compatible con macOS.
- Evitar instalar aplicaciones que soliciten permisos innecesarios o que no estén firmadas digitalmente.
- Implementar políticas de control de aplicaciones permitidas en entornos corporativos (allow-listing).
- Capacitar a usuarios en identificación de software falso y suplantación de marca, especialmente en descargas desde buscadores.

Fuente de Información:

- <https://gbhackers.com/fake-notepad-for-mac-site/>

Índice alfabético

Explotación de vulnerabilidades conocidas 4