



PERÚ

Presidencia
del Consejo de Ministros

Secretaría de Gobierno
y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL



 Asociación de
Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

335-2026-CNSD

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

Repositorios Hugging Face secuestrados para entrega RAT de Android, evitando las defensas tradicionales 4

Vulnerabilidad de ejecución de código arbitrario en Symfony en Windows..... 6

Índice alfabético 7

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 335		Fecha: 28-01-2026
			Página: 4 de 7
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Repositorios Hugging Face secuestrados para entrega RAT de Android, evitando las defensas tradicionales		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Disponibilidad del Servicio		

Descripción

1. ANTECEDENTES:

Los atacantes están aprovechando plataformas legítimas de alojamiento para “camuflar” la descarga de payloads maliciosos y reducir alertas por reputación de dominio, desplazando parte del riesgo desde sitios evidentemente sospechosos hacia servicios ampliamente usados por desarrolladores. En esta campaña, la puerta de entrada es una app falsa de “seguridad” que se presenta como útil/gratuita, y luego conduce al usuario a instalar componentes adicionales que realmente son el RAT



Ilustración 1: Hugging Face secuestrado para RAT de Android (Fuente: Bitdefender).

2. DETALLES:


Bitdefender identificó una cadena de infección que inicia cuando el usuario instala manualmente una app Android maliciosa llamada TrustBastion, generalmente tras ver anuncios/alertas falsas que indican que el teléfono está infectado. La app funciona como “dropper” (al inicio no parece peligrosa) y rápidamente fuerza un supuesto “update” con pantallas que imitan diálogos de Google Play/actualización del sistema. En lugar de descargar el APK final desde un dominio claramente malicioso, el dropper consulta un endpoint cifrado (trustbastion[.]com) que responde con un enlace/redirección hacia un repositorio público en Hugging Face (datasets) desde donde se descarga el payload. Los investigadores observaron alta rotación/polimorfismo: nuevos APKs generados aproximadamente cada 15 minutos y más de 6,000 commits en ~29 días, buscando evadir detección basada en hash. Una vez instalado, el payload solicita permisos altamente invasivos (Accesibilidad, superposición/overlay, grabación/casting de pantalla), permitiendo monitoreo de actividad, captura de pantalla y robo de credenciales mediante interfaces falsas, además de comunicación persistente con su C2. Hugging Face retiró los datasets maliciosos tras ser notificado, pero la operación migró/reapareció con cambios cosméticos y código similar.

3. RECOMENDACIONES:

- Restringir la instalación de APKs fuera de Google Play (bloquear “Unknown sources” vía MDM/UEM) y aplicar allowlist de aplicaciones en móviles corporativos.
- Capacitar a usuarios frente a “scareware”: desconfiar de anuncios/ventanas que indiquen infección y pidan instalar “antivirus” o “actualizaciones” fuera de canales oficiales.
- Endurecer permisos: bloquear o controlar el uso de Accesibilidad, overlay y capacidades de captura de pantalla para apps no autorizadas (políticas MDM, revisiones de permisos y detección de abuso).
- Implementar defensa móvil: MTD/EDR para Android con detección por comportamiento (más efectiva que hashes ante polimorfismo) y telemetría centralizada hacia el SOC.
- Controles de red: inspección/filtrado de DNS/HTTP(S) en dispositivos gestionados y alertas por descargas de APK desde repositorios públicos no aprobados (incluyendo CDNs/hosting legítimo cuando no sea necesario para negocio).
- Respuesta ante sospecha: aislar el dispositivo, revocar sesiones/tokens, rotar credenciales y revisar actividad en apps financieras/corporativas, ya que el RAT puede capturar pantallas e inputs de autenticación.

Fuente de Información:

- <https://gbhackers.com/hugging-face-hijacked-for-android-rats/>

	ALERTA DE SEGURIDAD DIGITAL N°051		Fecha: 28-01-2026
			Página: 6 de 7
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución de código arbitrario en Symfony en Windows.		
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			
<p>1. ANTECEDENTES:</p> <p>SensioLabs ha publicado una vulnerabilidad de severidad MEDIA clasificada como CWE-88: Inyección o modificación de argumentos que afecta al framework PHP para aplicaciones web y de consola Symfony para Windows. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución de código arbitrario y comprometer el sistema. La vulnerabilidad afecta únicamente a las instalaciones de Windows.</p> <p>2. DETALLES:</p> <p>Symfony en Windows es el uso del framework PHP Symfony para desarrollar aplicaciones web y APIs dentro de un sistema operativo Windows, ya sea mediante una instalación nativa con PHP y un servidor web local, o utilizando tecnologías como WSL2 o Docker que permiten ejecutar Symfony en un entorno Linux integrado, manteniendo todas sus capacidades de seguridad, escalabilidad y arquitectura profesional.</p> <p>La vulnerabilidad de severidad media identificada por MITRE como CVE-2026-24739 de tipo inyección o modificación de argumentos que afecta al software Symfony en Windows, podría permitir a un atacante remoto comprometer el sistema afectado.</p> <p>La vulnerabilidad existe debido a una validación de entrada incorrecta al ejecutar PHP desde un entorno basado en MSYS2 (p. ej., Git Bash). Si una aplicación (o herramientas como scripts de Composer) utiliza el proceso Symfony para invocar comandos de gestión de archivos (p. ej., rmdir, del, etc.) con un argumento de ruta que contiene =, la capa de conversión de MSYS2 puede alterar el argumento en tiempo de ejecución. Un atacante remoto puede engañar a la víctima para que pase una entrada especialmente diseñada a la aplicación y ejecutar comandos peligrosos en el sistema.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – Symfony para Windows: 5.4.0 - 8.0.4. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Actualizar el producto afectado a la última versión de software que aborda esta vulnerabilidad. 			
Fuente de Información:		<ul style="list-style-type: none"> • hxxps://github.com/symfony/symfony/security/advisories/GHSA-r39x-jcww-82v6 • hxxps://github.com/symfony/symfony/issues/62921 • hxxps://github.com/symfony/symfony/pull/63164 	

Índice alfabético

Malware	4
Explotación de vulnerabilidades conocidas	6