Boletín de alerta

Boletín Nro.:
Fecha de publicación: 25/05/2026
Tema: Alerta 2026-55 Ataque a la cadena de suministro afecta paquetes Composer de Laravel Lang
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

Paquetes comprometidos de Laravel Lang publicados en Composer/Packagist:

- laravel-lang/lang
- laravel-lang/http-statuses
- laravel-lang/attributes

Versiones afectadas:

- Múltiples versiones históricas fueron modificadas maliciosamente.

https://socket.dev/supply-chain-attacks/laravel-lang-compromise

Descripción

Se identificó una campaña de ataque a la cadena de suministro dirigida al ecosistema PHP/Laravel mediante el compromiso de paquetes de localización de Laravel Lang, una popular colección de paquetes de código abierto que proporciona traducciones preconfiguradas para funcionalidades nativas de Laravel, como validación, paginación, autenticación y recuperación de contraseñas, permitiendo adaptar aplicaciones a múltiples idiomas distintos del inglés, incluyendo español.

Debido a que Laravel utiliza el idioma inglés de forma predeterminada, estos paquetes son ampliamente utilizados por desarrolladores y organizaciones para localizar aplicaciones en distintos entornos y regiones. Como consecuencia, el compromiso de estos componentes representa un riesgo significativo dentro de proyectos empresariales y entornos de desarrollo basados en PHP.

El ataque no modificó directamente el código principal de los repositorios oficiales; en su lugar, los atacantes abusaron del sistema de etiquetas (tags) de GitHub, redirigiendo versiones legítimas hacia commits maliciosos controlados externamente. Esta técnica permitió que versiones aparentemente válidas y confiables descargaran código malicioso sin generar alertas inmediatas.

El ataque se basa en una técnica avanzada de compromiso de la cadena de suministro (“Supply Chain Attack”), en la que los atacantes manipularon paquetes legítimos utilizados por miles de desarrolladores dentro del ecosistema Laravel y Composer. A diferencia de ataques tradicionales, los actores maliciosos no publicaron nuevas versiones sospechosas, sino que reutilizaron versiones históricas aparentemente legítimas mediante la modificación de etiquetas (tags) en GitHub, apuntándolas hacia commits maliciosos alojados en bifurcaciones controladas por el atacante.

Cuando los desarrolladores o pipelines automatizados ejecutaban comandos como composer install o composer update, Composer descargaba automáticamente estas versiones comprometidas creyendo que eran oficiales y confiables. Esto permitió que el código malicioso ingresara silenciosamente en servidores de desarrollo, entornos productivos, runners CI/CD y estaciones de trabajo de desarrolladores.

El principal componente malicioso agregado fue el archivo src/helpers.php, el cual fue registrado dentro de la sección autoload.files del archivo composer.json. Esta técnica es especialmente peligrosa porque los archivos definidos en autoload.files son ejecutados automáticamente cada vez que una aplicación PHP carga vendor/autoload.php, algo común en prácticamente todas las aplicaciones Laravel y Symfony.

Una vez ejecutado, el malware construía dinámicamente la dirección del servidor de comando y control (C2) flipboxstudio[.]info utilizando técnicas de ofuscación para evitar ser detectado por herramientas de seguridad o análisis estático. Posteriormente, descargaba una segunda carga útil desde internet y la almacenaba temporalmente en directorios ocultos del sistema, como /tmp/.laravel_locale/ en Linux/macOS o carpetas temporales en Windows.

El malware también implementaba mecanismos de persistencia y evasión. Por ejemplo, creaba identificadores únicos por sistema infectado para evitar ejecuciones repetidas, ejecutaba procesos en segundo plano desvinculados del proceso principal y eliminaba automáticamente archivos temporales utilizados durante la infección para dificultar el análisis forense posterior.

En sistemas Windows, además del payload PHP, se desplegaba un ejecutable adicional denominado “DebugElevator”, diseñado específicamente para descifrar credenciales protegidas mediante DPAPI en navegadores basados en Chromium como Chrome, Edge y Brave.

Indicadores de Compromiso (IoC)

Indicadores de red

- flipboxstudio.info
- https://flipboxstudio.info/payload
- https://flipboxstudio.info/exfil

Indicadores de archivos

Linux/macOS:

- /tmp/.laravel_locale/<12_hex>.php
- /tmp/.<8_hex>

Windows:

- %TEMP%*.exe
- %TEMP%*.vbs

Indicadores de procesos

- Procesos php huérfanos con ppid=1
- Procesos ELF ejecutándose desde rutas eliminadas en /tmp

Indicadores Git

Autor malicioso:

- Your Name
- you@example.com

Archivos modificados:

- composer.json
- src/helpers.php

Solución:

Se recomiendan la siguientes acciones de forma inmediata:

- Identificar y eliminar versiones comprometidas de los paquetes Laravel Lang
- Rotación de credenciales
- Revisión de infraestructura

Información adicional:

- https://www.stepsecurity.io/blog/laravel-lang-supply-chain-attack
- https://socket.dev/blog/laravel-lang-compromise
- https://socket.dev/supply-chain-attacks/laravel-lang-compromise
- https://www.aikido.dev/blog/supply-chain-attack-targets-laravel-lang-packages-with-credential-stealer
- https://www.bleepingcomputer.com/news/security/laravel-lang-packages-hijacked-to-deploy-credential-stealing-malware/