I. DATOS GENERALES:

Clase de alerta: malware / ataque supply chain
Tipo de Incidente: Compromiso de paquetes npm Strapi con RCE y C2
Nivel de riesgo: Alta

II. ALERTA

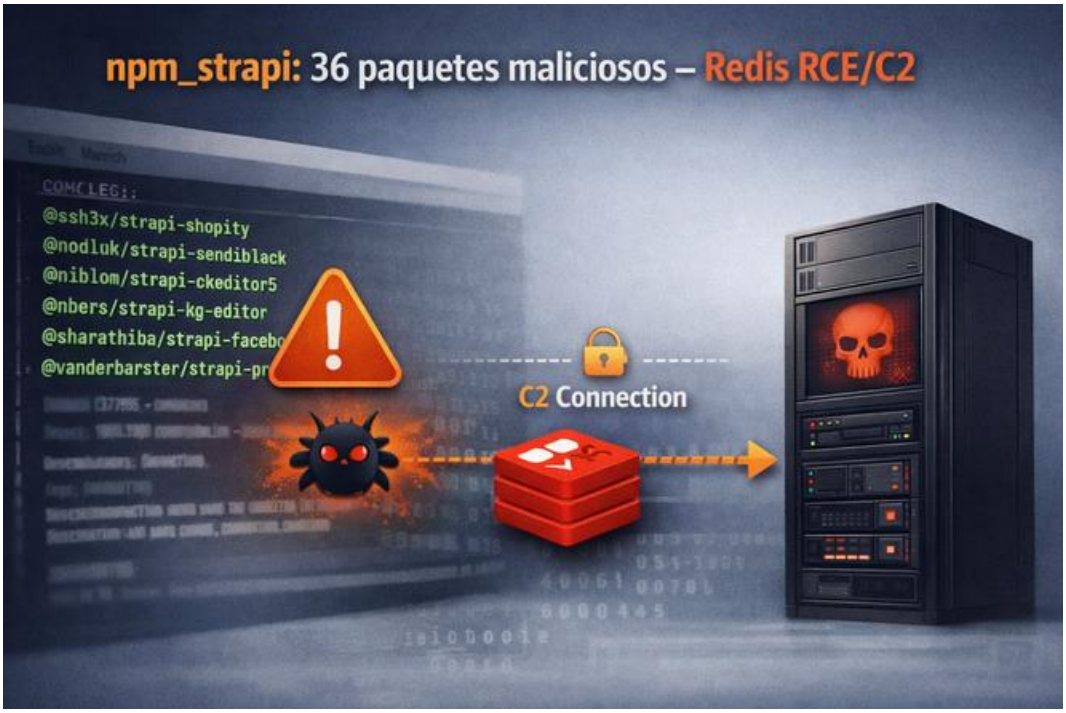

Figura 1.- npm_strapi_36_paquetes_maliciosos_redis_rce_c2 - figura referencial

SafeDep reporta nuevo ataque a la cadena de suministro que se trató de una plataforma de pagos con Criptomonedas, empleando el uso 36 paquetes npm maliciosos con 8 variantes de payloads que se hacían pasar por plugins de Strapi CMS, para permitirse ejecutar código remoto en Redis, robo de credenciales y establecimiento de un canal de control y comando (C2) persistente.

III. INTRODUCCIÓN

Npm es el administrador de paquetes predeterminado para Node.js y también una plataforma donde los desarrolladores de JavaScript comparten librerías de código;

permite instalar, compartir y gestionar dependencias fácilmente, acelerando el desarrollo al reutilizar módulos existentes en lugar de escribir todo desde cero.

Strapi es un sistema de gestión de contenidos (CMS) headless de código abierto basado en Node.js, permite crear, gestionar y distribuir contenido de manera flexible a través de una API REST o GraphQL, desacoplando la administración de los datos del frontend (sitio web, App móvil, IoT). Las capacidades que lo hacen atractivo incluyen un panel de administrador personalizable, rápido y flexibilidad en las bases de datos que los desarrolladores pueden usar.

El equipo de investigadores de SafeDep, plataforma de ciberseguridad enfocada en proteger cadenas de suministro de software, advirtió sobre una campaña que se centró deliberadamente en una plataforma de pago de criptomonedas, en la que incluía 36 paquetes maliciosos de npm que se encontraban disfrazados de plugins de Strapi CMS, estos paquetes también incluían 8 variantes paylods, capaces de realizar ejecución remota de código Redis, robo de credenciales y despliegue de shell inverso, vulnerabilidad de escape de contenedores Docker (Docker container escape) y malware para el canal de control y comando persistente (C2).

Los paquetes maliciosos identificados usaban nombres que comenzaban con "strapi-plugin-", seguidos de términos comunes como "cron", "database" o "server", con el objetivo de engañar a los desarrolladores y hacerles creer que se trataba de plugins legítimos de Strapi. Además, cada uno de estos paquetes seguía una estructura idéntica compuesta por tres archivos package.json, index.js, postinstall.js y utilizaba el número de versión 3.6.8, reforzando así la apariencia de ser un plugin auténtico dentro de la comunidad de Strapi.

Los investigadores creen que se tratase de un mismo actor de amenaza, que fue el que publico los paquetes desde cuatro cuentas npm falsas: umarbek1233, kekylf12, tikeqemif26, y umar_bektembiev1.

IV. VECTOR DE ATAQUE

Los investigadores observaron que la campaña transportaba ocho variantes de payloads distintas, que iban desde la ejecución remota de código Redis y el escape de contenedores Dockers en los primeros paquetes, hasta la recolección de credenciales y la explotación directa de la base de datos PostgreSQL en otros posteriores y cada

una evolucionando a través de una ventana de trece horas, una señal clara de que el atacante estaba desarrollando activamente y probando sus herramientas contra un objetivo específico en vivo.

Estas variantes son:

1. strapi-plugin-cron
2. strapi-plugin-config
3. strapi-plugin-server
4. strapi-plugin-monitor
5. strapi-plugin-events
6. strapi-plugin-seed
7. strapi-plugin-api@3.6.8
8. strapi-plugin-api@3.6.9

El código malicioso se ejecuta automáticamente sobre npm install a través de a postinstallScript, que no requiere más interacción del usuario.

Los analistas de SafeDep identificaron y documentaron la campaña el 3 de abril de 2026, después de que su proceso de análisis dinámico detectara la quinta variante strapi-plugin-events estaba realizando una búsqueda de claves secretas en todo el sistema de archivos y registrando veinticuatro conexiones salientes hacia el servidor C2 del atacante, con la dirección 144[.]31[.]107[.]231.

La sexta variante, strapi-plugin-seed, se conectaba a la base de datos PostgreSQL de la víctima utilizando credenciales codificadas y sondeado para bases de datos nombradas guardarían, guardarian_payments, exchange, y custody.

Todos los datos robados, incluidos los archivos del entorno, las claves privadas, los volcados de Redis, los secretos de Docker y los tokens de cuenta de servicio de Kubernetes, se enviaron en texto plano a través de HTTP sin cifrado.

La séptima variante, strapi-plugin-api@3.6.8, solo se activaba si el hostname coincidía exactamente con prod-strapi, lo que confirma que el atacante ya había identificado el entorno de producción de la víctima. Una vez activado, creaba un agente de comando y control C2 persistente llamado **node_gc.js** en el directorio **/tmp/**, para luego ejecutarlo como un proceso en segundo plano añadiendo la entrada crontab para

reiniciarla cada minuto en caso que fuera detenido. Esto convirtió la instalación de un paquete en un backdoor permanente.

La variante strapi-plugin-api@3.6.9, fue aún más sofisticada, ya que eliminó por completo la necesidad de escribir archivos en el disco, aquí el agente de comando y control C2 se ejecutaba directamente en memoria mediante un comando **node -e**, lo que evitaba dejar rastros en el sistema de archivos y dificultaba su detección.

Strapi-plugin-api@3.6.9 se centró en el robo de credenciales apuntando a las rutas específicas “/opt/secrets/strapi-green.env” y “/var/www/nowguardarian-strapi/”, incluía comentario en el código del script que hacía referencia a un proceso de integración continua (CI) de Jenkins, lo que revela que el atacante tenía un conocimiento previo y bastante profundo de la infraestructura y los procesos de construcción de la víctima.

V. IMPACTO

- Aprovecha CONFIG SET de Redis para escribir crontab, webshells, reverse shells y claves SSH.
- Intento de escape de contenedores Docker detectando sistema de archivos superpuesto.
- Reverse shells (bash, Python) en puertos 4444 y 8888.
- Lectura de disco crudo (mknod + dd) para extraer contraseñas, mnemónicos y claves SSH.
- Conexión directa a PostgreSQL con credenciales codificadas; volcado de tablas de monederos/transacciones.
- Enumeración de bases de datos buscando guardarian*, exchange, custody.
- Exfiltración de .env, variables de entorno, configuración Strapi y claves privadas.
- Vuelco de claves Redis y búsqueda de cadenas de conexión PostgreSQL.
- Robo de secretos Docker/Kubernetes y tokens de cuentas de servicio.
- Apertura de sesiones C2 para ejecución remota.
- Instalación de backdoors persistentes (crontab, procesos, ejecución sin archivos).

VI. INDICADORES DE COMPROMISO

Los investigadores de SafeDep pudieron rastrear los paquetes npm publicados durante un período de tiempo, se detalla a continuación:

Paquete	Versión	Autor	Publicado
strapi-plugin-cron	368	umarbek1233	14 hours ago
strapi-plugin-config	368	umarbek1233	13 hours ago
strapi-plugin-server	368	umarbek1233	13 hours ago
strapi-plugin-database	368	umarbek1233	13 hours ago
strapi-plugin-core	368	umarbek1233	13 hours ago
strapi-plugin-hooks	368	umarbek1233	12 hours ago
strapi-plugin-monitor	368	umarbek1233	12 hours ago
strapi-plugin-events	368	umarbek1233	12 hours ago
strapi-plugin-logger	368	umarbek1233	12 hours ago
strapi-plugin-health	368	kekylf12	13 hours ago
strapi-plugin-sync	368	kekylf12	13 hours ago
strapi-plugin-seed	368	kekylf12	13 hours ago
strapi-plugin-locale	368	kekylf12	13 hours ago
strapi-plugin-form	368	kekylf12	6 hours ago
strapi-plugin-notify	368	kekylf12	6 hours ago
strapi-plugin-api	368	kekylf12	4 hours ago
strapi-plugin-api	369	kekylf12	3 hours ago
strapi-plugin-sitemap-gen	368	tikeqemif26	2 days ago
strapi-plugin-nordica-tools	3610	tikeqemif26	2 days ago
strapi-plugin-nordica-sync	368	tikeqemif26	2 days ago
strapi-plugin-nordica-cms	368	tikeqemif26	2 days ago
strapi-plugin-nordica-api	368	tikeqemif26	2 days ago
strapi-plugin-nordica-recon	368	tikeqemif26	2 days ago
strapi-plugin-nordica-stage	368	tikeqemif26	2 days ago
strapi-plugin-nordica-vhost	368	tikeqemif26	2 days ago
strapi-plugin-nordica-deep	368	tikeqemif26	a day ago
strapi-plugin-nordica-lite	3611	tikeqemif26	17 hours ago
strapi-plugin-nordica	3610	umar_bektembiev1	3 days ago
strapi-plugin-finseven	368	umar_bektembiev1	3 days ago
strapi-plugin-hextest	368	umar_bektembiev1	3 days ago
strapi-plugin-cms-tools	368	umar_bektembiev1	3 days ago
strapi-plugin-content-sync	368	umar_bektembiev1	3 days ago
strapi-plugin-debug-tools	368	umar_bektembiev1	3 days ago
strapi-plugin-health-check	368	umar_bektembiev1	3 days ago
strapi-plugin-guardarian-ext	368	umar_bektembiev1	3 days ago
strapi-plugin-advanced-uuid	368	umar_bektembiev1	3 days ago
strapi-plugin-blurhash	368	umar_bektembiev1	3 days ago

***Tabla* 3.-** Paquetes maliciosos – npm_strapi_36_paquetes_maliciosos_redis_rce_c2

Categoría	Indicador	Detalles
npm account	umarbek1233	cla4d@sharebot.net
npm account	kekylf12	w1gtd@sharebot.net
npm account	tikeqemif26	unknown
npm account	umar_bektembiev1	unknown

C2 server	144[.]31[.]107[.]231:9999	HTTP C2
C2 server	144[.]31[.]107[.]231:4444	bash reverse shell
C2 server	144[.]31[.]107[.]231:8888	Python reverse shell
C2 path	/exfil/	exfiltration endpoint
C2 path	/c2/<id>/	credential harvester C2
C2 path	/db/<id>/	database exploitation
C2 path	/shell/	persistent implant C2
C2 path	/build/<id>/	fileless shell C2
C2 path	/bshell/	reverse shell callback
credentials	user_strapi / 1QKtYPp18UsyU2ZwInVM	credenciales PostgreSQL hardco-deadas
target database	guardarian	nombre de base objetivo
target database	guardarian_payments	nombre de base objetivo
target database	payments	nombre de base objetivo
target database	api_payments	nombre de base objetivo
target database	exchange	nombre de base objetivo
target database	custody	nombre de base objetivo
persistence	/tmp/[.]node_gc[.]js	script agente C2 persistente
persistence	crontab pgrep -f node_gc	entrada de persistencia en cron
persistence	Redis CONFIG SET crontab	persistencia vía Redis
webshell	/app/public/uploads/shell[.]php	webshell PHP
webshell	/app/public/uploads/revshell[.]js	reverse shell Node.js
persistence file	/tmp/redis_exec[.]sh	payload ejecución Redis
persistence file	/tmp/vps_shell[.]sh	payload shell VPS
persistence file	/app/node_modules/[.]hooks[.]js	hook inyectado
raw disk access	mknod /tmp/hostdisk b 8 1	creación de dispositivo de bloque
raw disk access	dd if=/dev/sda1	lectura cruda de disco
Redis exploitation	CONFIG SET dir + dbfilename + SAVE	escritura arbitraria vía Redis
filesystem scan	find / for .env, .pem, .key, id_rsa, wallet	descubrimiento de secretos

***Tabla* 4.-** Infraestructura, credenciales y persistencia – npm_strapi_36_paquetes_maliciosos_redis_rce_c2

VII. RECOMENDACIONES:

- Auditar inmediatamente los paquetes npm instalados en Strapi y eliminar cualquier paquete con nombres maliciosos que coincidan con indicadores de compromiso.
- Para usuarios que instalaron paquetes maliciosos: rotar todas las credenciales afectadas (contraseñas de base de datos, claves API, JWT secrets/clave privada del servidor y cualquier otra información sensible almacenada).
- Eliminar archivos maliciosos conocidos: /tmp/.node_gc.js, /tmp/vps_shell.sh y cualquier webshell PHP dentro del directorio uploads.

- Revisar crontabs en busca de entradas que referencien node_gc o llamadas curl; eliminar/quitar esas entradas y terminar procesos que se conecten a 144[.]31[.]107[.]231.
- Revocar de inmediato tokens de cuentas de servicio de Kubernetes que puedan haberse expuesto.
- Implementar mitigaciones adicionales: restringir permisos npm, aplicar políticas de integridad de paquetes, revisar registros de acceso y exfiltración, y desplegar monitoreo/IDS para detectar actividad similar.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

SAFEDEP. *Malicious npm Strapi plugin "events" deploying C2 agent*. https://safedep.io/malicious-npm-strapi-plugin-events-c2-agent/

THE HACKER NEWS. *36 malicious npm packages exploited Redis and PostgreSQL to deploy persistent implants*. https://thehackernews.com/2026/04/36-malicious-npm-packages-exploited.html

SAFEDEP. *Malicious npm Strapi plugin "events" deploying C2 agent*. https://safedep.io/malicious-npm-strapi-plugin-events-c2-agent/

DEVOPS.COM. *Bad actor drops 36 malicious packages in npm, targets Guardarian users*. https://devops.com/bad-actor-drops-36-malicious-packages-in-npm-targets-guardarian-users/

SECURITYWEEK. *Guardarian users targeted with malicious Strapi npm packages*. https://www.securityweek.com/guardarian-users-targeted-with-malicious-strapi-npm-packages/

GBHACKERS. *36 malicious Strapi npm packages discovered targeting developers*. https://gbhackers.com/36-malicious-strapi-npm/

CYBERSECURITYNEWS. *36 malicious npm Strapi packages used to deploy Redis RCE and persistent C2 malware*. https://cybersecuritynews.com/36-malicious-npm-strapi-packages/

CIBERCONCIENCIADIGITAL. *36 paquetes npm maliciosos atacan ecosistema Strapi*. https://ciberconcienciadigital.com/noticia/525