El sello ya no garantiza seguridad.

Análisis técnico del ataque TanStack / Mini Shai-Hulud: cuando la cadena de suministro de software fue envenenada por dentro — con sello criptográfico válido.

01 · QUÉ PASÓ

El 11 de mayo de 2026, entre las **19:20 y 19:26 UTC**, atacantes publicaron **84 versiones maliciosas** de 42 paquetes oficiales de **@tanstack** en el registro npm. La campaña, atribuida al grupo **TeamPCP** y bautizada **Mini Shai-Hulud**, se extendió el mismo día a más de **170 paquetes** en npm y PyPI, afectando también a **Mistral AI, UiPath, OpenSearch, Guardrails AI y Squawk**.

Lo histórico: es el primer caso documentado de paquetes maliciosos publicados con **atestación SLSA válida**. El sello criptográfico de origen estaba correcto. Los paquetes envenenados eran indistinguibles de los legítimos para cualquier herramienta de verificación.

19:20 UTC
Primera publicación maliciosa @tanstack

19:26 UTC
84 versiones maliciosas publicadas

19:40 UTC
Detección externa (StepSecurity)

+24 H
Extensión a 170+ paquetes (npm + PyPI)

02 · LA ANALOGÍA PEDAGÓGICA

Imagine una **fábrica de medicamentos** con cajas fuertes (2FA), sello holográfico oficial (SLSA) y auditorías rigurosas. El atacante no robó ninguna llave ni falsificó el sello. **Se coló por la línea de producción, envenenó los frascos, y dejó que la propia fábrica los empacara, sellara con el holograma oficial y los enviara a las farmacias.**

Para cualquier verificador, los frascos son auténticos. Porque sí son auténticos. Solo que el contenido está envenenado.

03 · QUÉ HACE EL VENENO

01 · ROBO

Credenciales masivas

Exfiltra claves AWS, GCP, Azure, Kubernetes, Vault, GitHub y npm vía **Session Messenger** encriptada. Imposible de bloquear por IP o dominio tradicional.

02 · PROPAGACIÓN

Tipo gusano

Republica **todos los paquetes** que mantiene el desarrollador comprometido con la misma carga. Tu equipo se convierte en el siguiente vehículo de infección.

03 · TRAMPA

Dead-man's switch

Detecta cuando revocas el token cada 60 seg y ejecuta `rm -rf` sobre el directorio del usuario. **Responder al ataque dispara la bomba.**

6 min

La ventana de publicación de las **84 versiones maliciosas**. La quinta ola del grupo TeamPCP en 8 meses. **El patrón apunta a una sexta ola en las próximas semanas.**

LA DEFENSA

Dos pilares. Una arquitectura.

Una sola plataforma no resuelve este ataque. **Globaltek integra prevención y detección en una arquitectura defensiva coordinada** para proteger su cadena de suministro de software end-to-end.

PILAR 01 · PREVENCIÓN — aikido

Bloquea la entrada del veneno.

Aikido Intel detectó y catalogó esta campaña Mini Shai-Hulud específicamente. **Aikido Safe Chain** intercepta cada `npm install` y `pip install`, bloquea paquetes maliciosos antes de que entren a la máquina o al pipeline, y aplica **cuarentena de 24–48 horas** a paquetes recién publicados — la ventana donde estos ataques son más peligrosos.

PILAR 02 · DETECCIÓN — SOPHOS

Detecta si el veneno entra.

Sophos Intercept X + ITDR + MDR detecta el comportamiento post-explotación: persistencia (LaunchAgent / systemd), intentos de robo de credenciales, conexiones a infraestructura sospechosa. **ITDR** específicamente cubre el escenario donde un token robado se usa más tarde desde una ubicación anómala. Es la red de seguridad cuando la prevención falla.

SOPORTE COMPLEMENTARIO · SEGÚN CONTEXTO DEL CLIENTE

SOLUCIÓN	FUNCIÓN EN ESTE ESCENARIO
Forcepoint DLP / SWG / CASB	Detección de exfiltración de credenciales hacia dominios externos.
Fidelis NDR	Análisis de tráfico anómalo desde estaciones de desarrollador.
Rapid7 InsightIDR	Correlación y hunting retrospectivo de indicadores de compromiso.
Vicarius vRx	Higiene general de la workstation del desarrollador.

El patrón apunta a una sexta ola en las próximas semanas.

Si su organización desarrolla software internamente o contrata consultoras de desarrollo, hable con Globaltek antes del próximo ataque. **Su cadena de suministro merece una defensa coordinada, no una colección de herramientas.**

www.globaltek.co
comercial@globalteksecurity.com