Una grave vulnerabilidad de seguridad recientemente revelada en SAP NetWeaver está siendo aprovechada por varios actores estatales vinculados a China para atacar infraestructuras críticas.

"Los actores explotaron la CVE-2025-31324, una vulnerabilidad de carga de archivos sin autenticación que permite la ejecución remota de código (RCE)", explicó el investigador de EclecticIQ, Arda Büyükkaya, en un informe publicado hoy.

Entre los objetivos de esta campaña se encuentran redes de distribución de gas natural, servicios de agua y gestión integral de residuos en el Reino Unido, fábricas de dispositivos médicos, empresas de exploración y producción de petróleo y gas en Estados Unidos, así como ministerios gubernamentales en Arabia Saudita encargados de estrategias de inversión y regulación financiera.

Las conclusiones se basan en un directorio expuesto públicamente hallado en infraestructura controlada por los atacantes («15.204.56[.]106»), el cual contenía registros de eventos que documentan actividades en múltiples sistemas comprometidos.

La empresa de ciberseguridad con sede en los Países Bajos ha atribuido los accesos no autorizados a agrupaciones de amenazas chinas identificadas como UNC5221, UNC5174 y CL-STA-0048. Este último grupo fue vinculado a ataques contra objetivos estratégicos en el sur de Asia, utilizando vulnerabilidades conocidas en servidores públicos IIS, Apache Tomcat y MS-SQL para instalar web shells, reverse shells y el backdoor PlugX.

También se detectó que otro actor de amenazas vinculado a China, aún no clasificado, está llevando a cabo una campaña masiva de escaneo y explotación contra sistemas SAP NetWeaver. El servidor alojado en la dirección IP «15.204.56[.]106» contiene diversos archivos, entre ellos:

- «CVE-2025-31324-results.txt», que registra 581 instancias de SAP NetWeaver comprometidas e infectadas con un web shell.
- «□□□□_20250427_212229.txt», que enumera 800 dominios que ejecutan SAP

NetWeaver y que podrían ser blancos en el futuro.

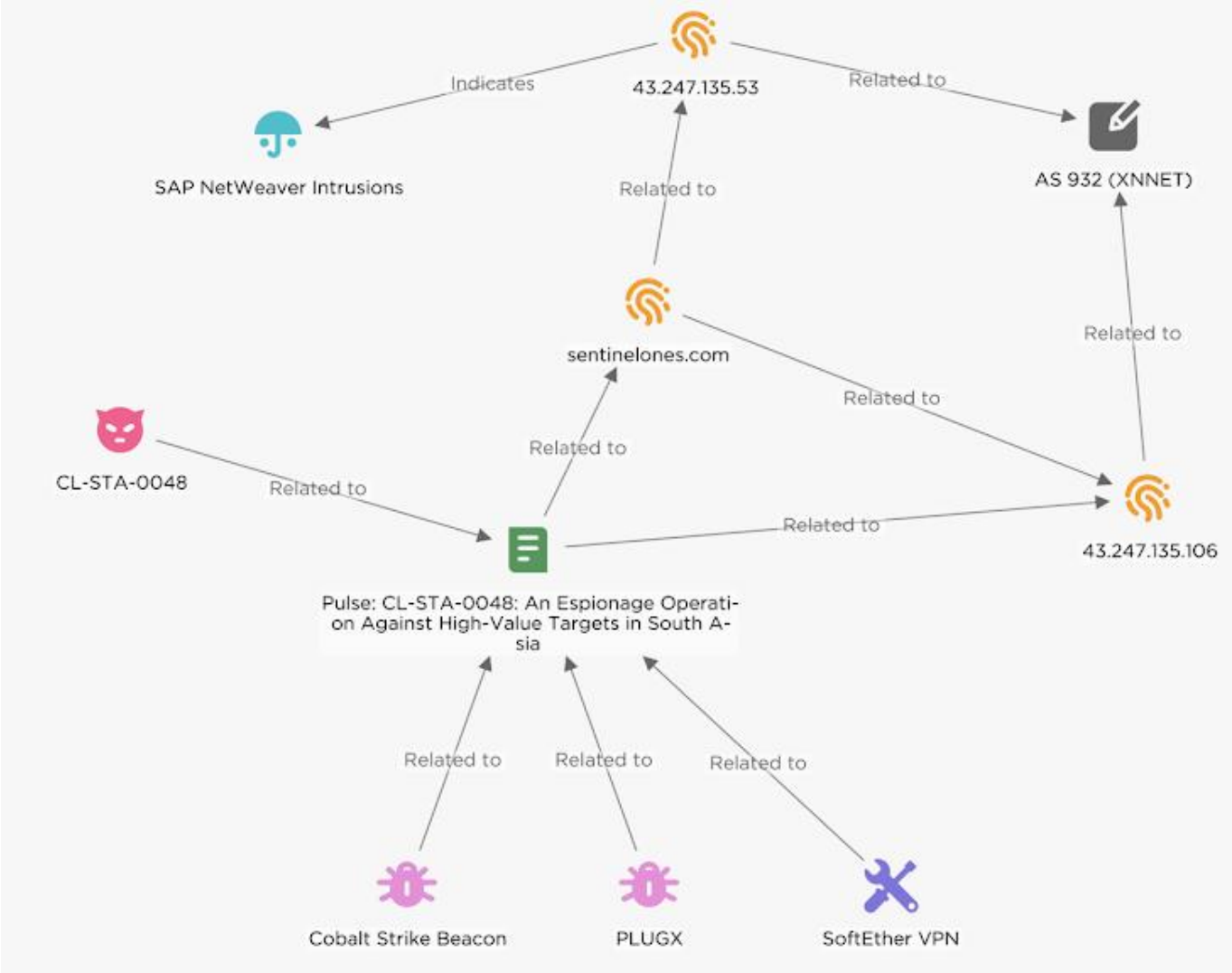
> *"La infraestructura de directorios abiertos revela intrusiones confirmadas y expone los objetivos planeados del grupo, proporcionando una visión clara tanto de operaciones pasadas como futuras"*, comentó Büyükkaya.

Una vez explotada la CVE-2025-31324, los atacantes instalan dos web shells que les permiten mantener acceso persistente a los sistemas comprometidos y ejecutar comandos arbitrarios.

Asimismo, se ha observado a tres grupos de hackers chinos utilizando esta vulnerabilidad como parte de operaciones más amplias de acceso remoto, reconocimiento y distribución de malware:

- CL-STA-0048, que intentó establecer una conexión tipo reverse shell con «43.247.135[.]53», una dirección IP previamente vinculada al grupo.
- UNC5221, que desplegó un web shell para instalar *KrustyLoader*, un malware desarrollado en Rust capaz de ejecutar cargas adicionales como *Sliver*, mantener persistencia y ejecutar comandos.
- UNC5174, que utilizó un web shell para descargar *SNOWLIGHT*, un cargador que se comunica con un servidor codificado para obtener *VShell*, un troyano de acceso remoto escrito en Go, y un backdoor denominado *GOREVERSE*.

> *"Es muy probable que los APT vinculados a China continúen atacando aplicaciones empresariales expuestas a internet y dispositivos de borde para lograr acceso persistente y estratégico a redes de infraestructura crítica a nivel mundial",* añadió Büyükkaya.



> *"El enfoque en plataformas ampliamente utilizadas como SAP NetWeaver es una estrategia deliberada, ya que estos sistemas están profundamente integrados en entornos empresariales y, con frecuencia, presentan vulnerabilidades sin parchear".*

SAP corrige nueva vulnerabilidad activamente explotada en

NetWeaver

La divulgación se produce poco después de que otro actor de amenazas chino, no identificado y denominado Chaya_004, fuera vinculado a la explotación de la CVE-2025-31324 con el fin de desplegar una reverse shell en Go llamada *SuperShell*.

La firma de seguridad SAP Onapsis afirmó que está *"observando una actividad significativa por parte de atacantes que utilizan información pública para activar la explotación y reutilizar web shells instalados por los atacantes originales, quienes actualmente han cesado sus actividades".*

El análisis más reciente ha permitido identificar otra falla crítica en el componente Visual Composer Metadata Uploader de NetWeaver. Esta nueva vulnerabilidad, catalogada como CVE-2025-42999 (con una puntuación CVSS de 9.1), consiste en una deserialización insegura que podría ser explotada por un usuario con privilegios para cargar contenido malicioso.

> *"Los ataques observados durante marzo de 2025 (que comenzaron con pruebas simples en enero) están explotando tanto la falta de autenticación (CVE-2025-31324) como la deserialización insegura (CVE-2025-42999)",* explicó el CTO de Onapsis, Juan Pablo (JP) Perez-Etchegoyen.
>
> *"Esta combinación permitió a los atacantes ejecutar comandos arbitrarios de manera remota y sin privilegios en el sistema. Las organizaciones que aplicaron oportunamente la Nota de Seguridad de SAP 3594142 (parche para la CVE-2025-31324) redujeron significativamente el riesgo de explotación".*
>
> *"Ahora, las organizaciones deben aplicar la Nota de Seguridad de SAP 3604119 para eliminar cualquier riesgo residual en las aplicaciones SAP. Este riesgo residual es una vulnerabilidad de deserialización que solo puede ser explotada por usuarios con el rol VisualComposerUser en el sistema SAP objetivo".*

Dado que la explotación sigue activa, se recomienda a los usuarios de SAP NetWeaver actualizar sus instancias a la versión más reciente lo antes posible.

> *(La noticia fue actualizada tras su publicación el 14 de mayo de 2025 para confirmar la explotación activa de CVE-2025-42999.)*