Investigadores en ciberseguridad han revelado detalles sobre una campaña persistente, activa durante nueve meses, que ha tenido como objetivo dispositivos del Internet de las Cosas (IoT) y aplicaciones web para integrarlos en una botnet conocida como RondoDox.

Hasta diciembre de 2025, la actividad ha sido observada explotando la vulnerabilidad recientemente divulgada React2Shell (CVE-2025-55182, puntuación CVSS: 10.0) como vector de acceso inicial, señaló CloudSEK en un análisis.

React2Shell es el nombre asignado a una falla de seguridad crítica en React Server Components (RSC) y Next.js, que podría permitir a atacantes no autenticados lograr ejecución remota de código en sistemas vulnerables.

De acuerdo con estadísticas de la Shadowserver Foundation, al 31 de diciembre de 2025 existen alrededor de 90,300 instancias que continúan siendo vulnerables a esta falla, de las cuales 68,400 se encuentran en Estados Unidos, seguidas por Alemania (4,300), Francia (2,800) e India (1,500).

RondoDox, que apareció a inicios de 2025, ha ampliado su alcance incorporando nuevas vulnerabilidades de seguridad tipo N-day a su repertorio, entre ellas CVE-2023-1389 y CVE-2025-24893. Cabe destacar que el uso indebido de React2Shell para propagar la botnet ya había sido señalado previamente por Darktrace, Kaspersky y VulnCheck.

Se considera que la campaña de la botnet RondoDox atravesó tres fases bien definidas antes de la explotación de CVE-2025-55182:

Marzo – abril de 2025: reconocimiento inicial y escaneo manual de vulnerabilidades
Abril – junio de 2025: sondeo masivo diario de vulnerabilidades en aplicaciones web como WordPress, Drupal y Struts2, así como en dispositivos IoT como routers Wavlink
Julio – principios de diciembre de 2025: despliegue automatizado a gran escala de forma horaria

En los ataques detectados durante diciembre de 2025, se afirma que los actores maliciosos

iniciaron escaneos para identificar servidores Next.js vulnerables, seguidos de intentos por instalar mineros de criptomonedas (*«/nuts/poop»*), un cargador de botnet y verificador de estado (*«/nuts/bolts»*), así como una variante de la botnet Mirai (*«/nuts/x86»*) en los dispositivos comprometidos.

El componente *«/nuts/bolts»* está diseñado para finalizar malware y mineros de criptomonedas competidores antes de descargar el binario principal de la botnet desde su servidor de comando y control (C2). Se ha identificado una variante de esta herramienta capaz de eliminar botnets conocidas, cargas útiles basadas en Docker, rastros dejados por campañas anteriores y sus tareas programadas, además de establecer persistencia mediante *«/etc/crontab»*.

«Escanea de forma continua /proc para enumerar los ejecutables en ejecución y elimina procesos que no estén en la lista blanca cada ~45 segundos, evitando de manera efectiva la reinfección por actores rivales», indicó CloudSEK.

Para reducir el riesgo asociado a esta amenaza, se recomienda a las organizaciones actualizar Next.js a una versión corregida lo antes posible, segmentar todos los dispositivos IoT en VLAN dedicadas, implementar firewalls de aplicaciones web (WAF), monitorear ejecuciones de procesos sospechosos y bloquear la infraestructura C2 conocida.