Una vulnerabilidad de ejecución remota de código en Langflow permitió desplegar un minero de Monero en puntos finales de aplicaciones de IA expuestas

Los actores de amenazas continúan aprovechando una vulnerabilidad crítica en Langflow como parte de una nueva campaña de ataques destinada a desplegar un minero de criptomonedas Monero.

La actividad maliciosa explota la vulnerabilidad CVE-2026-33017 (puntuación CVSS: 9.3), una falla de ejecución remota de código (RCE) sin autenticación presente en Langflow. Esto indica que los atacantes están escaneando y atacando puntos finales expuestos de aplicaciones de inteligencia artificial (IA) con el objetivo de obtener acceso inicial a redes empresariales. La campaña fue observada durante un período de 19 días, comprendido entre el 27 de marzo y el 15 de abril de 2026.

«En esta campaña, una única línea de código Python, evaluada dentro de un punto final de la API de Langflow sin autenticación, descarga un script de shell, obtiene un binario de minería y lo ejecuta como un proceso independiente», señalaron los investigadores de Trend Micro, Simon Dulude y John Zhang, en un informe técnico publicado la semana pasada.

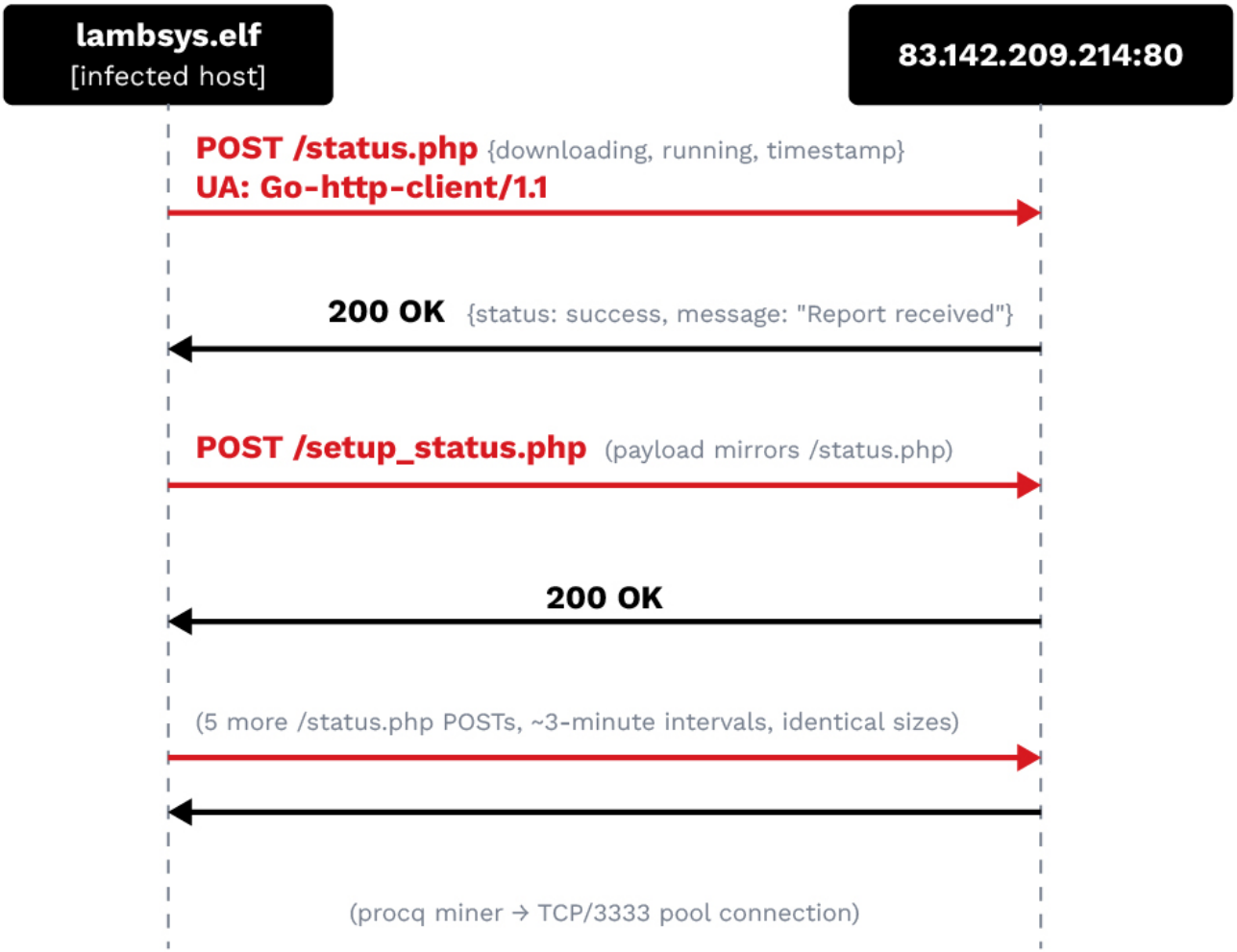
En términos generales, el malware está diseñado para finalizar procesos de minería de criptomonedas pertenecientes a campañas rivales como Kinsing, WatchDog, Rocke y Outlaw; eliminar billeteras y materiales criptográficos de otros operadores; desactivar mecanismos de seguridad del sistema anfitrión; establecer persistencia mediante tareas cron; comunicarse con un servidor externo («83.142.209[.]214:80»); e instalar un minero personalizado. Asimismo, puede propagarse hacia otros sistemas utilizando claves SSH reutilizadas, convirtiendo una instancia expuesta de Langflow en un punto de acceso para comprometer una infraestructura más amplia.

El ataque comienza explotando la vulnerabilidad de Langflow para ejecutar un script de Python proporcionado por el atacante. Dicho script inicia posteriormente un script de shell alojado de forma remota que actúa como dropper, cuya función principal consiste en comprobar si un binario denominado «lambsys» ya se encuentra en ejecución en el sistema comprometido.

Posteriormente, el malware descarga ese binario mediante curl o wget, lo ejecuta como un

proceso independiente y se propaga hacia todos los equipos accesibles mediante SSH a los que la víctima tenga capacidad de autenticación. El binario, un ejecutable ELF desarrollado en Go, también ha sido diseñado para deshabilitar AppArmor, Ubuntu Uncomplicated Firewall (UFW), iptables, SELinux, el kernel NMI watchdog y el agente Aliyun de Alibaba Cloud.

Además, el malware elimina registros del sistema con el fin de ocultar su actividad. También retira el atributo de inmutabilidad de archivos y directorios como «~/.ssh/», «~/.ssh/authorized_keys», «/etc/crontab», «/etc/ld.so.preload», «/tmp/», «/var/tmp/» y «/var/spool/cron», lo que le permite modificar su contenido. Una vez realizados los cambios, vuelve a aplicar dicho atributo de inmutabilidad a «/tmp/» y «/var/tmp/».



Las operaciones ilícitas de minería de criptomonedas suelen establecer el atributo «chattr +i» sobre estos archivos para impedir que cualquier usuario, incluso el superusuario, pueda modificarlos, renombrarlos o eliminarlos. El comportamiento observado en el binario demuestra que el actor de amenazas conoce las técnicas de persistencia utilizadas por otros grupos dedicados al cryptojacking.

En la fase final de la infección, el binario establece comunicación con el mismo servidor para descargar un archivo TAR, desde el cual extrae una versión personalizada del minero XMRig. Una vez que el minero entra en funcionamiento, el archivo comprimido es eliminado del sistema de archivos. Además, realiza una solicitud al servicio ipinfo[.]io para obtener la dirección IP pública y la ubicación geográfica del equipo comprometido, información que permite a los atacantes adaptar sus decisiones operativas en tiempo real.

El primer propósito de esta información es seleccionar el pool de minería más adecuado. Dado que estos servidores suelen distribuirse geográficamente, conectarse a uno cercano a la víctima reduce la latencia y mejora el rendimiento del proceso de minería. El segundo objetivo es implementar mecanismos de geovallado (geo-fencing), permitiendo excluir deliberadamente a víctimas ubicadas en determinadas regiones.

«Lambsys no ejecuta su lógica de ataque mediante funciones propias de Go. En su lugar, crea una cascada de procesos temporales mediante `sh -c`*, donde cada uno ejecuta un único comando de shell (por ejemplo, un* `pkill`*, un* `chattr` *o un* `sysctl`*). Este diseño prioriza la confiabilidad sobre el sigilo. Si uno de los 51 comandos* `pkill` *falla, el error queda limitado a ese proceso, mientras que los otros 50 continúan ejecutándose normalmente»*, explicaron los investigadores.

Trend Micro indicó que un artefacto perteneciente a una versión anterior del mismo binario fue compilado en mayo de 2024, lo que sugiere que los responsables de esta campaña han estado evolucionando esta familia de malware durante más de dos años, incorporando además técnicas destinadas a evadir la detección por parte de soluciones antivirus.

Durante el último año, diversas vulnerabilidades de seguridad en Langflow han sido explotadas activamente. En junio de 2025, otra falla crítica (CVE-2025-3248, con una puntuación CVSS de 9.8) fue utilizada para distribuir el malware de botnet Flodrix.

«Esta campaña de minería ilícita de criptomonedas demuestra que los puntos finales expuestos de aplicaciones de inteligencia artificial se están convirtiendo en una nueva vía de acceso a los entornos empresariales. Aunque la carga útil resulte conocida, el mecanismo de

entrega representa una novedad. Una vulnerabilidad en Langflow proporciona a los operadores de criptominería una nueva puerta de entrada hacia los sistemas que ejecutan infraestructura de aplicaciones de IA», concluyó Trend Micro.