Se ha identificado una campaña maliciosa que distribuye el malware XLoader empleando la técnica de carga lateral de DLL (*DLL side-loading*), aprovechando una aplicación legítima vinculada a la Fundación Eclipse.

> *«La aplicación utilizada en el ataque, jarsigner, es un archivo generado durante la instalación del paquete IDE proporcionado por la Fundación Eclipse. Se trata de una herramienta utilizada para firmar archivos JAR (Java Archive)»*, explicó el Centro de Inteligencia de Seguridad de AhnLab (ASEC).

Según la empresa surcoreana de ciberseguridad, el malware se difunde a través de un archivo comprimido en formato ZIP que contiene tanto el ejecutable legítimo como las bibliotecas DLL que se cargan lateralmente para ejecutar el código malicioso:

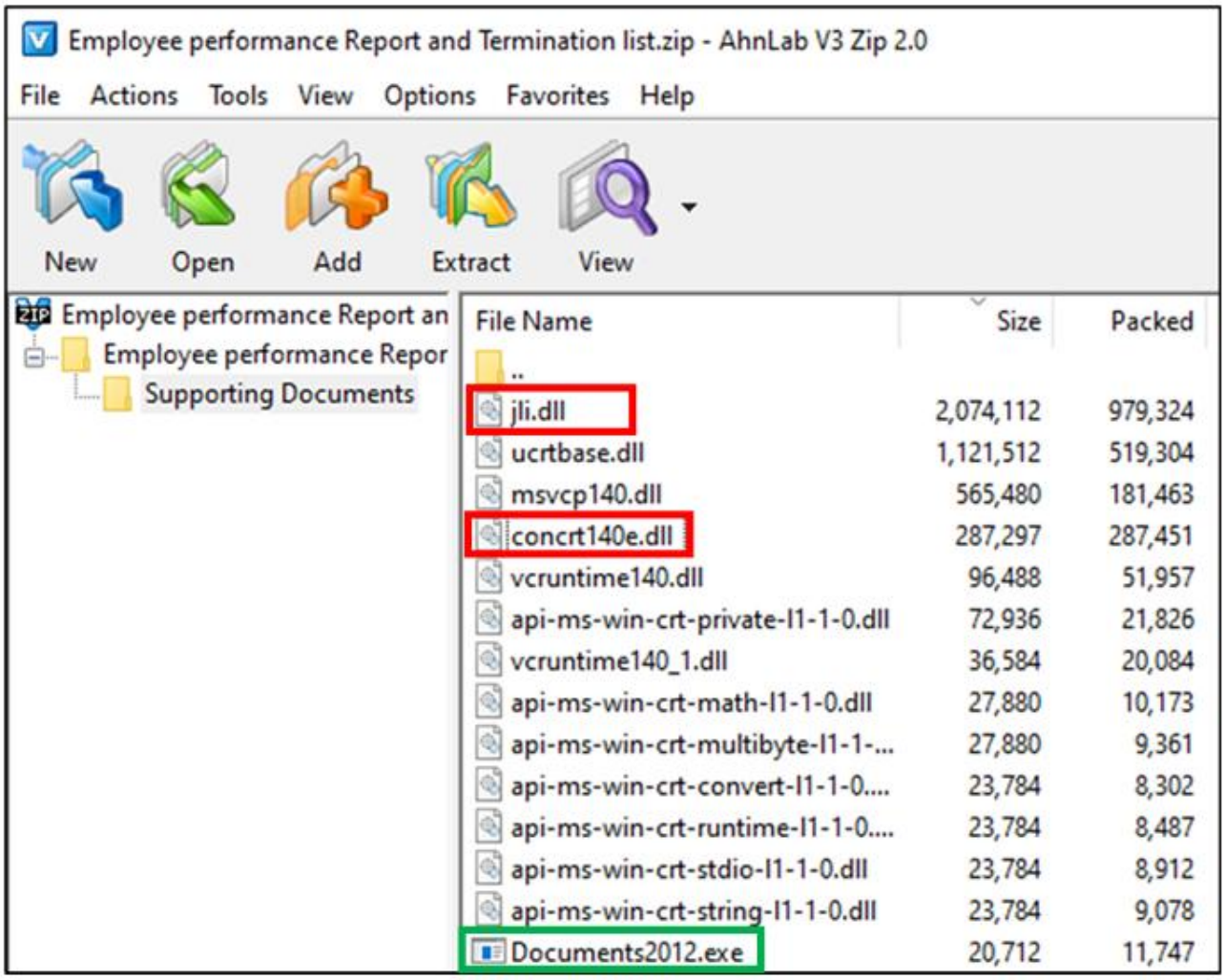
- Documents2012.exe: una copia renombrada del ejecutable original *jarsigner.exe*.
- jli.dll: una DLL alterada por los atacantes para descifrar e inyectar *concrt140e.dll*.
- concrt140e.dll: el código malicioso de XLoader.

El ataque se activa cuando *Documents2012.exe* se ejecuta, lo que provoca la carga de la biblioteca modificada *jli.dll*, permitiendo así la ejecución del malware XLoader.

> *«El archivo concrt140e.dll distribuido es una carga maliciosa cifrada que, durante la ejecución del ataque, se descifra y se introduce en el proceso legítimo aspnet_wp.exe»*, detalló ASEC.
>
> *«Una vez dentro del sistema, XLoader recopila información sensible, como datos del equipo y del navegador del usuario, además de realizar otras acciones como la descarga de software malicioso adicional».*

XLoader, sucesor del malware Formbook, fue detectado por primera vez en 2020 y se comercializa bajo el modelo *Malware-as-a-Service* (MaaS), permitiendo su uso por otros ciberdelincuentes. En agosto de 2023, se identificó una variante para macOS que se hacía pasar por Microsoft Office.

> *«Las versiones 6 y 7 de XLoader incorporan técnicas avanzadas de ofuscación y cifrado diseñadas para ocultar secciones críticas del código y dificultar tanto la detección basada en firmas como los intentos de ingeniería inversa»,* reveló *Zscaler ThreatLabz* en un informe reciente.



> *«XLoader ha adoptado estrategias previamente vistas en SmokeLoader, incluyendo el cifrado dinámico de fragmentos de código y la evasión de NTDLL hook».*

Un examen más detallado del malware reveló que emplea listas de direcciones señuelo predefinidas para disfrazar las comunicaciones reales de comando y control (*C2*), combinándolas con tráfico legítimo. Tanto las conexiones a servidores C2 auténticos como las simuladas están protegidas mediante cifrados distintos.

Como ocurre con otras familias de malware como Pushdo, el uso de señuelos busca generar tráfico de red hacia sitios legítimos para encubrir las comunicaciones reales con los servidores de control.

La técnica de carga lateral de DLL también ha sido aprovechada por el grupo de amenazas SmartApeSG (también conocido como *ZPHP* o *HANEYMANEY*) para distribuir *NetSupport RAT* a través de sitios web legítimos comprometidos con inyecciones de código JavaScript. Este troyano de acceso remoto facilita la instalación de StealC, un *stealer* de información.

Este descubrimiento coincide con un análisis de Zscaler sobre dos nuevos *loaders* de malware, *NodeLoader* y *RiseLoader*, empleados en la distribución de diversos tipos de software malicioso, como *stealers* de datos, *cryptominers* y *botnets*, incluyendo Vidar, Lumma, Phemedrone, XMRig y Socks5Systemz.

«RiseLoader y RisePro presentan múltiples coincidencias en sus mecanismos de comunicación en red, como la estructura de los mensajes, el proceso de inicialización y el formato de la carga útil. Estas similitudes sugieren que ambas familias de malware podrían haber sido desarrolladas por el mismo grupo de atacantes», señala el informe.