El grupo de hackers Lazarus está explotando una vulnerabilidad Zero Day de Windows para obtener acceso al sistema e implementar una backdoor

El actor de amenazas norcoreano conocido como Lazarus Group ha sido vinculado con la explotación de una vulnerabilidad de día cero recientemente corregida en Microsoft Windows, utilizada para desplegar una puerta trasera inédita dirigida contra organizaciones de los sectores de defensa y aeroespacial en Francia, Alemania, Brasil e India.

Según Check Point Research, esta actividad forma parte de la operación Dream Job, una campaña de ciberespionaje e ingeniería social mantenida durante años por actores respaldados por Corea del Norte. El objetivo consiste en atraer a profesionales de distintas partes del mundo mediante ofertas laborales falsas, pero creíbles, supuestamente provenientes de empresas como Lockheed Martin y Enveil. Los atacantes establecen contacto a través de plataformas como LinkedIn, haciéndose pasar por reclutadores para generar confianza, robar información sensible e instalar malware.

Los ataques aprovechan la vulnerabilidad CVE-2026-68820 (CVSS: 7.0), una falla de escalamiento de privilegios presente en el controlador Windows Ancillary Function Driver para WinSock (AFD.sys), la cual fue corregida por Microsoft en la actualización Patch Tuesday de agosto de 2026.

Tal como se ha observado en campañas anteriores, las víctimas son contactadas mediante mensajes fraudulentos de reclutamiento y convencidas de abrir un PDF malicioso o instalar un visor PDF troyanizado. Posteriormente, este componente sirve para desplegar una nueva puerta trasera denominada Troy, que concede acceso remoto al sistema comprometido. El propósito final de la operación es obtener control total del equipo infectado y evadir los mecanismos de seguridad.

El uso de visores PDF manipulados es una táctica ampliamente probada por el Grupo Lazarus dentro de la campaña Dream Job. De hecho, los atacantes vienen aprovechando este método al menos desde 2022.

Se identificaron dos cadenas de infección paralelas durante esta campaña:

- Carga lateral de DLL (DLL Side-Loading): las víctimas reciben instrucciones para

descargar un archivo cifrado que inicia una cadena de carga lateral de DLL. La biblioteca maliciosa («libmupdf.dll») muestra una supuesta descripción de empleo para distraer al usuario, mientras descarga y ejecuta en memoria un descargador ligero llamado MISTPEN. Este malware se comunica con infraestructura controlada por los atacantes utilizando Microsoft Graph API y OneDrive para obtener y ejecutar módulos de reconocimiento y persistencia, activar el exploit contra AFD.sys y finalmente desplegar ForestTiger (también conocido como ScoringMathTea), una herramienta que proporciona acceso remoto al sistema.

- Visor PDF troyanizado «SecurityPDF»: en este escenario, la víctima descarga SecurityPDF desde un sitio web que suplanta a la empresa Enveil. Una vez instalado, el programa supervisa los documentos PDF abiertos y busca una marca específica: («This document is encrypted with sumatrapdf reader!!!!!!!!!!!»). Cuando detecta dicha cadena, descifra y ejecuta una carga útil oculta encargada de cargar en memoria la puerta trasera Troy. Este implante DLL admite 17 comandos distintos que permiten enumerar archivos, cargar y descargar información, comprimir y exfiltrar datos, acceder a una consola interactiva, terminar procesos, realizar inyecciones DLL en memoria y actualizar configuraciones.

Por su parte, MISTPEN carga al menos cuatro módulos diferentes:

- GetInfoPlugin («Release_GetInfoPlugin_x64.dll»): recopila información detallada del sistema comprometido y la exfiltra como una única cadena de caracteres extendidos.
- PvPlugin («Release_PvPlugin_x64.dll»): obtiene datos de reconocimiento del equipo y detalles de los procesos en ejecución.
- OneScreenCapture («OneScreenCapture64.dll»): realiza capturas de pantalla del escritorio completo, incluidos todos los monitores conectados, y las transmite en formato JPEG.
- Cargador LPE (escalamiento local de privilegios): recopila datos del sistema, genera nuevo material criptográfico mediante el algoritmo post-cuántico ML-KEM y utiliza la clave negociada durante el proceso de autenticación para descifrar y ejecutar FudModule.

La cadena de ataque incorpora una versión actualizada del rootkit en modo kernel que el Grupo Lazarus ha utilizado de forma reiterada desde al menos 2022 para ocultar herramientas maliciosas de las soluciones de seguridad instaladas en los sistemas afectados.

En concreto, el malware explota la vulnerabilidad de escalamiento local de privilegios en AFD.sys, obtiene permisos de nivel SYSTEM e inyecta una nueva instancia de MISTPEN dentro de un proceso SYSTEM. Esto le permite operar con privilegios elevados mientras permanece fuera del alcance de muchos mecanismos de detección.

La nueva variante, denominada FudModule 3.1, amplía las capacidades de versiones anteriores al manipular una característica de Windows conocida como Smart App Control, diseñada para verificar la confiabilidad de las aplicaciones antes de su ejecución.

"Dentro del proceso hijo msiexec.exe ejecutado con privilegios SYSTEM, el stub remoto establece VerifiedAndReputablePolicyState en cero e invoca la clase NtSetSystemInformation 0xA4 con la opción 0x10000000, provocando una recarga inmediata de la política de integridad de código", señaló Check Point.

Además, los investigadores indicaron que los atacantes crearon al menos tres sitios web falsos que suplantan a Enveil para distribuir SecurityPDF. No obstante, aún no está completamente claro cómo estos portales fueron integrados en la campaña de ingeniería social. La hipótesis más probable es que primero se envía el documento PDF mediante phishing y luego se solicita a la víctima descargar el visor desde el sitio fraudulento para poder abrirlo.

Los dominios identificados son los siguientes:

- envell[.]xyz
- enveil[.]online
- uxtramine[.]org

Un aspecto particularmente relevante es que la campaña no depende de una infraestructura

propia dedicada. En cambio, aprovecha sitios legítimos comprometidos basados en WordPress y SharePoint, así como servidores vulnerables de correo web Roundcube, para utilizarlos como servidores de comando y control (C2) de ForestTiger. Esta estrategia dificulta significativamente distinguir el tráfico malicioso del tráfico web legítimo.

Numerosos servidores Roundcube afectados resultaron vulnerables a CVE-2025-49113. Los atacantes aprovecharon esta falla para instalar una web shell PHP previamente desconocida, denominada RelayShell, utilizada para intercambiar comandos y respuestas mediante archivos de texto. En al menos un incidente, una organización francesa que ya había sido comprometida fue empleada para enviar nuevos correos de phishing, permitiendo eludir filtros basados en reputación.

Los hallazgos más recientes evidencian que el Grupo Lazarus continúa perfeccionando tanto sus capacidades de malware como sus técnicas operativas, manteniendo intactos los fundamentos de la campaña Dream Job mientras dirige sus operaciones contra sectores estratégicos alrededor del mundo.

"Lo que vuelve especialmente peligrosa a esta campaña no es únicamente la vulnerabilidad de día cero, sino la forma en que Lazarus integró infraestructura legítima y confiable en cada etapa del ataque", afirmó Sergey Shykevich, director de inteligencia de amenazas de Check Point Software. *"Los atacantes se ocultaron a plena vista, aprovechando resultados destacados en motores de búsqueda, marcas legítimas de proveedores y la reputación de organizaciones que ya habían comprometido previamente."*

"Cuando el sitio web, la descarga y el reclutador parecen completamente auténticos, el consejo tradicional de identificar enlaces de phishing deja de ser suficiente. Mantenerse protegido implica asumir que incluso la confianza puede ser falsificada: aplicar actualizaciones tan pronto como estén disponibles, verificar el software a través de canales oficiales en lugar de confiar en resultados de búsqueda y extender los principios de confianza cero también a los sitios y socios aparentemente legítimos con los que interactuamos diariamente."