Se ha observado que Lazarus Group, respaldado por Corea del Norte, implementa un rootkit de Windows aprovechando un exploit en un controlador de firmware de Dell, destacando las nuevas tácticas adoptadas por el adversario patrocinado por el estado.

El ataque Bring Your Own Vulnerable Driver (BYOVD), que tuvo lugar en otoño de 2021, es otra variante de la actividad orientada al espionaje del atacante, llamada Operation In(ter)ception, que está dirigida contra las industrias aeroespacial y de defensa.

> *«La campaña comenzó con correos electrónicos de phishing selectivo que contenían documentos maliciosos con el tema de Amazon y se dirigió a un empleado de una empresa aeroespacial en los Países Bajos y a un periodista político en Bélgica»,* dijo Peter Kálnai, investigador de ESET.

Las cadenas de ataque se desarrollan tras la apertura de los documentos señuelo, lo que condujo a la distribución de droppers maliciosos que eran versiones troyanizadas de proyectos de código abierto, lo que corrobora informes recientes de Mandiant de Google y Microsoft.

ESET dijo que descubrió evidencia de que Lazarus lanzó versiones armadas de FingerText y sslSniffer, un componente de la biblioteca wolfSSL, además de descargadores y cargadores basados en HTTPS.

Las intrusiones también allanaron el camino para la backdoor elegida por el grupo, denominada BLINDINGCAN, también conocida como AIRDRY y ZetaNile, que un operador puede usar para controlar y explorar sistemas comprometidos.

Pero lo notable de los ataques de 2021 fue un módulo de rootkit que aprovechó una falla del controlador de Dell para obtener la capacidad de leer y escribir en la memoria del kernel. El problema, rastreado como CVE-2021-21551, se relaciona con un conjunto de vulnerabilidades críticas de escalada de privilegios en dbutil_2_3.sys.

> *«Esto representa el primero abuso registrado de la vulnerabilidad CVE-2021-21551. Esta herramienta, en combinación con la vulnerabilidad, deshabilita el monitoreo de todas las soluciones de seguridad en las máquinas comprometidas»*, dijo Kálnai.

Denominado FudModule, el malware previamente indocumentado logra sus objetivos por medio de múltiples métodos *«no conocidos antes o familiares solo para investigadores de seguridad especializados y desarrolladores (anti-)trampas»,* dijo ESET.

> *«Luego, los atacantes usaron su acceso de escritura a la memoria del kernel para deshabilitar siete mecanismos que ofrece el sistema operativo Windows para monitorear sus acciones, como registro, sistemas de archivos, creación de procesos, seguimiento de eventos, etc., básicamente cegando las soluciones de seguridad de una forma muy genérica y robusta. Sin duda, esto requirió habilidades profundas de investigación, desarrollo y prueba»,* dijo Kálnai.

Esta no es la primera vez que el atacante recurre al uso de un controlador vulnerable para montar sus ataques de rootkit. El mes pasado, ASEC de AhnLab detalló la explotación de un controlador legítimo conocido como «ene.sys» para desarmar el software de seguridad instalado en las máquinas.

Los hallazgos son una demostración de la tenacidad y la capacidad de Lazarus Group para innovar y cambiar sus tácticas según sea necesario a lo largo de los años a pesar del intenso escrutinio de las actividades del colectivo tanto por parte de las fuerzas del orden público como de la comunidad investigadora en general.

> *«La diversidad, el número y la excentricidad en la implementación de las campañas de Lazarus definen a este grupo, así como también que realiza los tres pilares de las actividades ciberciminales: espionaje cibernético, sabotaje cibernético y búsqueda de ganancias financieras»,* dijo la compañía.