Lazarus, un grupo avanzado de amenazas persistentes (APT), amplió su alcance con el desarrollo y uso de un troyano diseñado para atacar sistemas Linux.

APT, que se sospecha que proviene de Corea del Norte, se conectó previamente a ataques cibernéticos mundiales y brotes de malware, incluido el ataque WannaCry, el robo a un banco de Banhladesh de 80 millones de dólares y una nueva campaña que afecta a las instituciones financieras de todo el mundo.

Informes recientes sugieren que Lazarus se ha convertido en cliente de Trickbot, una compañía criminal que ofrece a los actores de amenazas patrocinados por el estado, acceso a sistemas infectados junto con una colección de herramientas de piratería.

Lazarus puedes estar dispuesto a comprar herramientas de otros pero también puede ser capaz de crear las suyas propias, como en el caso de un nuevo troyano de acceso remoto (RAT) detectado por investigadores de Netlab 360.

El martes, la compañía de seguridad cibernética dijo que el troyano, llamado Dacls, pudo haber aparecido en la escena tan pronto como en mayo de este año, y aunque fue identificado por más de 20 proveedores de antivirus, según VirusTotal, todavía se considera como *«desconocido».*

Luego de investigar una muestra de malware cargada en el sitio web, el equipo determinó que era un *«programa completamente funcional, encubierto y RAT para plataformas Windows y Linux»* probablemente conectado con Lazarus.

Finalmente, los investigadores obtuvieron cinco muestras. Una de las muestras de Windows se citó en el informe, CES Themed Targeting de Lazarus, mientras que otra muestra fue etiquetada como el trabajo de Lazarus por CyberWar.

Un dominio vinculado al malware, thevagabondsatchel.com, es una indicación más de la participación de Lazarus, ya que el sitio web fue utilizado previamente por la APT para almacenar malware.

Aunque el módulo de Windows se carga dinámicamente por medio de una URL remota, la variedad de Linux se compila directamente e incluye seis módulos generales para la ejecución de comandos, gestión de archivos y procesos, pruebas de acceso a la red, escaneo de red y conexiones C2.

Los investigadores creen que CVE-2019-3396, un error de ejecución remota de código que afecta la macro Widget Connector en el servidor Atlassian Confluence versión 6.6.12 y posteriores, se usa para infectar sistemas e implementar Dacls.

El RAT, que viene en diferentes versiones según el sistema operativo al que se dirige, comparte su protocolo de comando y control (C2). Dacls es el malware modular y utiliza el cifrado TLS y RC4 cuando se comunica con su C2, así como el cifrado AES para proteger los archivos de configuración.

Una vez que la versión de Linux aterriza en una máquina vulnerable, el malware se ejecutará en segundo plano y buscará actualizaciones. Dacls luego descomprimirá y descifrará su archivo de configuración y se conecta a su C2.

El troyano puede realizar funciones que incluyen robar, eliminar y ejecutar archivos, escanear estructuras de directorios, descargar cargas útiles adicionales, eliminar procesos, crear procesos de daemon y cargar datos, incluidos resultados de escaneo y salida de ejecución de comandos.

Como el malware se propaga por medio de una vulnerabilidad conocida con un parche fácilmente disponible, se recomienda que los administradores de TI se aseguren de que sus configuraciones de Confluence estén siempre actualizadas.

Trend Micro descubrió otra forma interesante de malware de Linux, denominada Skidmap, en septiembre de este año. El código malicioso usa rootkits en un intento de enterrarse en el núcleo y permanecer discreto mientras despliega mineros de criptomonedas ilícitos.