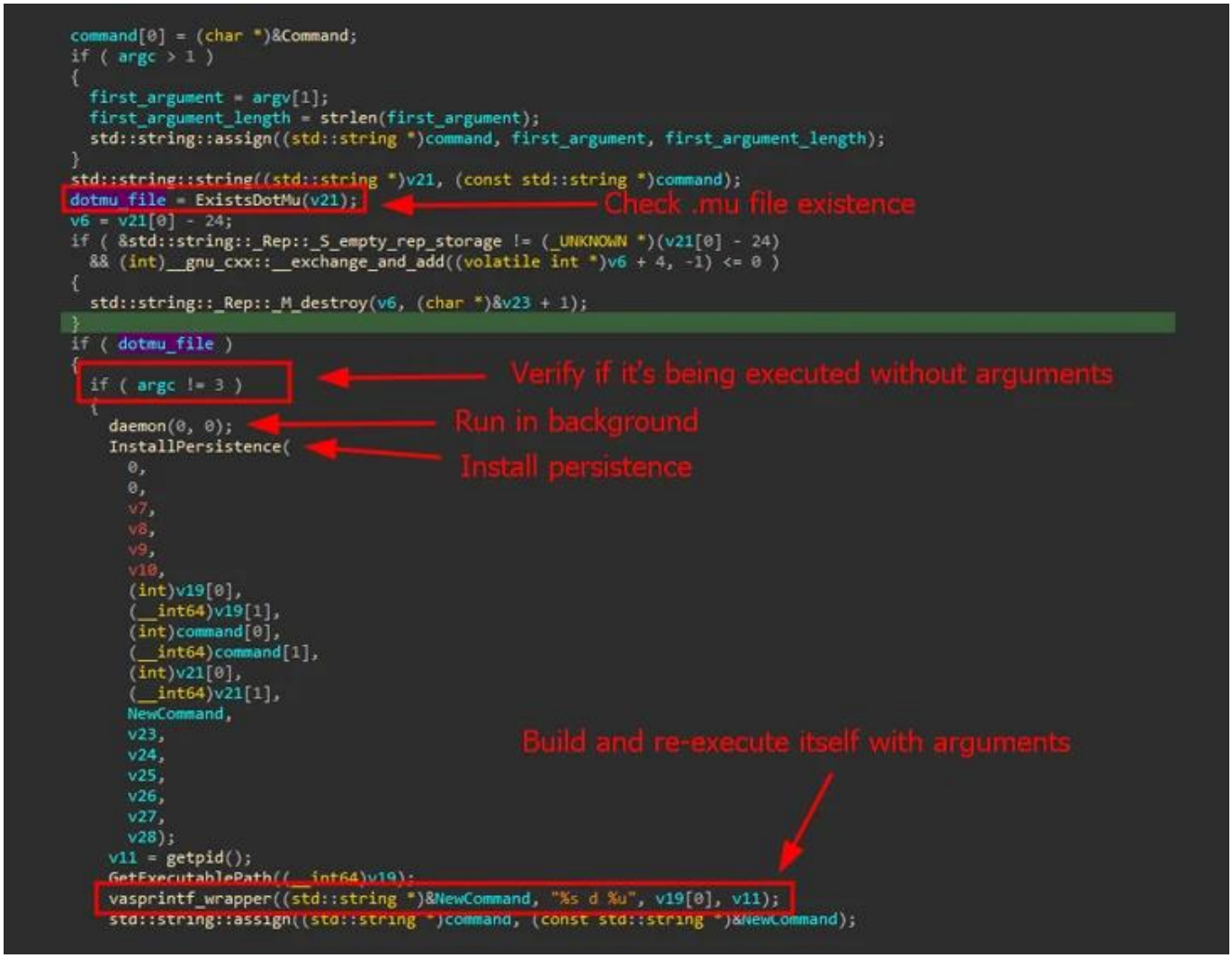
Se ha identificado en el mundo salvaje una variante de Linux de un backdoor multiplataforma llamado DinodasRAT, dirigido a China, Taiwán, Turquía y Uzbekistán, según nuevos descubrimientos de Kaspersky.

DinodasRAT, también conocido como XDealer, es un malware desarrollado en C++ que ofrece la capacidad de extraer una amplia variedad de datos sensibles de dispositivos comprometidos.

En octubre de 2023, la firma de ciberseguridad eslovaca ESET informó que una entidad gubernamental en Guyana había sido blanco de una campaña de espionaje cibernético llamada Operación Jacana, que utilizaba la versión de Windows del implante.

Posteriormente, la semana pasada, Trend Micro describió un conjunto de actividades de amenazas identificadas como Earth Krahang, que había cambiado a DinodasRAT desde 2023 en sus ataques dirigidos a varias entidades gubernamentales en todo el mundo.

El uso de DinodasRAT se ha asociado con varios actores de amenazas vinculados a China, como LuoYu, lo que demuestra nuevamente el intercambio de herramientas común entre grupos de piratas informáticos que actúan en nombre del país.




Kaspersky reveló que descubrió una versión de Linux del malware (V10) a principios de octubre de 2023. Las pruebas recopiladas hasta ahora indican que la primera variante conocida (V7) se remonta a 2021.

Está diseñado principalmente para atacar distribuciones basadas en Red Hat y Ubuntu Linux. Al ejecutarse, establece la persistencia en el host mediante scripts de inicio de SystemV o SystemD y se comunica periódicamente con un servidor remoto a través de TCP o UDP para obtener los comandos que debe ejecutar.

DinodasRAT está fully equipped para llevar a cabo operaciones de archivos, cambiar las direcciones de comando y control (C2), enumerar y finalizar procesos en ejecución, ejecutar comandos de shell, descargar una nueva versión del backdoor e incluso desinstalarse.

Además, toma medidas para evitar la detección por parte de herramientas de depuración y monitoreo, y, al igual que su contraparte de Windows, emplea el Tiny Encryption Algorithm (TEA) para cifrar las comunicaciones de C2.

> *«El uso principal de DinodasRAT es obtener y mantener acceso a través de servidores Linux en lugar de realizar tareas de reconocimiento. El backdoor es completamente funcional, proporcionando al operador control total sobre la máquina infectada, lo que permite la exfiltración de datos y actividades de espionaje»*, explicó Kaspersky.