Los ámbitos tecnológico, de investigación y gubernamental en la región de Asia-Pacífico han sido objeto de atención por parte de un grupo de amenaza conocido como BlackTech en el marco de una reciente ola de ciberataques.

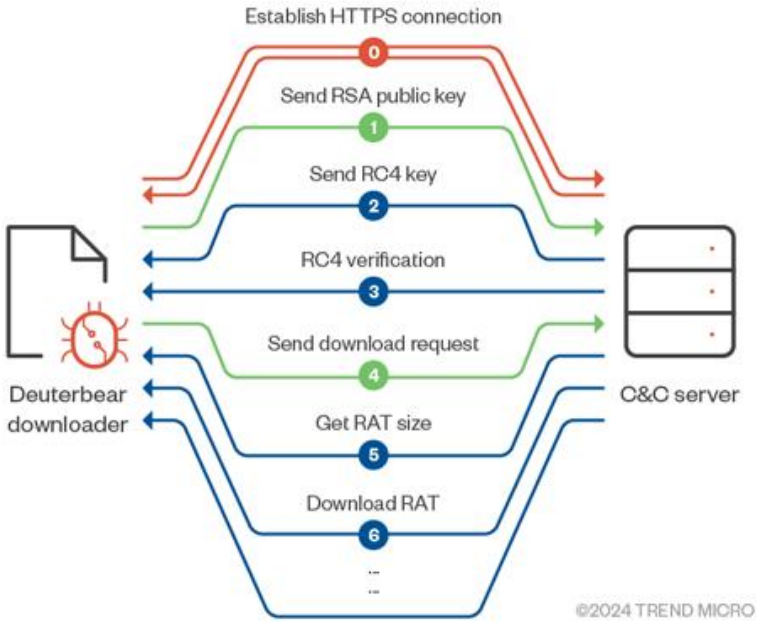
Estas intrusiones allanan el camino para una versión actualizada de una puerta trasera modular denominada Waterbear, así como para su sucesor mejorado conocido como Deuterbear.

> *«Waterbear se destaca por su complejidad, ya que emplea diversos mecanismos de evasión para reducir al mínimo las probabilidades de ser detectado y analizado»,* explicaron los investigadores de Trend Micro Cyris Tseng y Pierre Lee en un análisis la semana pasada.
>
> *«En 2022, Earth Hundun empezó a utilizar la última versión de Waterbear, también llamada Deuterbear, que presenta varios cambios, incluidas rutinas de escaneo y desencriptación anti-memoria, lo que nos lleva a considerarlo como una entidad de malware distinta al Waterbear original».*

La firma de ciberseguridad está siguiendo los pasos del grupo de amenazas bajo el nombre de Earth Hundun, que se sabe que está activo desde al menos 2007. También se le conoce con otros nombres como Circuit Panda, HUAPI, Manga Taurus, Palmerworm, Red Djinn y Temp.Overboard.

En un aviso conjunto publicado en septiembre pasado, agencias de ciberseguridad e inteligencia de Japón y Estados Unidos atribuyeron al adversario a China, describiendo su habilidad para modificar el firmware de los enrutadores y aprovechar las relaciones de confianza de dominio de los enrutadores para pivotar desde subsidiarias internacionales hasta las sedes corporativas basadas en los dos países.

> *«Los actores de BlackTech emplean software malicioso personalizado, herramientas con usos duales y tácticas de ocultamiento de operaciones, como la desactivación de registros en los enrutadores»,* afirmaron los gobiernos.



> *«Tras lograr un punto de apoyo inicial en una red objetivo y obtener acceso de administrador a los dispositivos de borde de la red, los actores cibernéticos de BlackTech a menudo modifican el firmware para ocultar su actividad en los dispositivos de borde y así mantener la persistencia en la red.»*

Una de las herramientas cruciales en su arsenal multifacético es Waterbear (también conocido como DBGPRINT), que ha estado en uso desde 2009 y ha sido consistentemente actualizado a lo largo de los años con características mejoradas de evasión de defensas.

El troyano de acceso remoto central es recuperado de un servidor de comando y control (C2) mediante un descargador, que es lanzado utilizando un cargador que, a su vez, es ejecutado

a través de una técnica conocida como carga lateral de DLL.

La versión más reciente del implante admite casi 50 comandos, lo que le permite realizar una amplia gama de actividades, incluyendo enumeración y terminación de procesos, operaciones de archivos, gestión de ventanas, inicio y cierre de consola remota, captura de pantalla y modificación del Registro de Windows, entre otros.

También entregado utilizando un flujo de infección similar desde 2022 está Deuterbear, cuyo descargador implementa una serie de métodos de ofuscación para resistir el análisis anti-malware y utiliza HTTPS para comunicaciones C2.

> *«Desde 2009, Earth Hundun ha evolucionado y refinado continuamente la puerta trasera Waterbear, así como sus muchas variantes y ramas»,* dijeron los investigadores.
>
> *«El descargador de Deuterbear emplea cifrado HTTPS para la protección del tráfico de red e implementa varias actualizaciones en la ejecución del malware, como modificar la función de desencriptación, verificar la presencia de depuradores o entornos de pruebas y modificar los protocolos de tráfico».*