Organismos gubernamentales en la región de Asia-Pacífico (APAC) están siendo objeto de una prolongada campaña de ciberespionaje conocida como TetrisPhantom.

> *«El atacante llevó a cabo una vigilancia encubierta y recolectó información sensible de entidades gubernamentales en APAC al explotar un tipo específico de unidad USB segura, protegida mediante cifrado de hardware para garantizar el almacenamiento y transferencia segura de datos entre sistemas informáticos»,* informó Kaspersky en su informe sobre tendencias de APT para el tercer trimestre de 2023.

La empresa de ciberseguridad rusa, que detectó esta actividad continua a principios de 2023, destacó que las unidades USB ofrecen cifrado de hardware y son utilizadas por organizaciones gubernamentales de todo el mundo para almacenar y transferir datos de manera segura, lo que plantea la posibilidad de que los ataques puedan extenderse en el futuro para tener un alcance global.

Aunque no se ha relacionado este grupo de intrusión clandestina con ningún actor o grupo de amenazas conocidos, la alta sofisticación de la campaña sugiere la participación de un equipo respaldado por un estado-nación.

> *«Estas operaciones fueron llevadas a cabo por un actor de amenazas altamente capacitado y astuto, con un gran interés en actividades de espionaje dentro de redes gubernamentales sensibles y protegidas. Los ataques fueron altamente focalizados y afectaron a un número bastante limitado de víctimas»,* señaló Noushin Shabab, investigadora de seguridad sénior de Kaspersky.

Un rasgo distintivo de esta campaña es el uso de varios módulos maliciosos para ejecutar comandos, recopilar archivos e información de máquinas comprometidas y propagar la infección a otras máquinas utilizando las mismas unidades USB seguras o distintas como

vector.

Estos componentes de malware, además de autorreplicarse a través de unidades USB seguras conectadas para infiltrarse en redes aisladas, también tienen la capacidad de ejecutar otros archivos maliciosos en los sistemas infectados.

«El ataque involucra herramientas y técnicas de gran complejidad», señaló Kaspersky, y añadió que las secuencias de ataque también incluyeron la *«inyección de código en un programa legítimo de gestión de acceso en la unidad USB, el cual actúa como cargador para el malware en una nueva máquina».*

Esta revelación coincide con la identificación de un nuevo y desconocido actor de amenazas persistentes avanzadas (APT) vinculado a una serie de ataques dirigidos a organismos gubernamentales, contratistas militares, universidades y hospitales en Rusia a través de correos electrónicos de spear-phishing que contenían documentos de Microsoft Office preparados con trampas.

> *«Esto inicia un esquema de infección multinivel que lleva a la instalación de un nuevo troyano, diseñado principalmente para exfiltrar archivos de la máquina de la víctima y tomar el control mediante la ejecución de comandos arbitrarios»,* informó Kaspersky.

Los ataques, denominados BadRory por la empresa, se llevaron a cabo en forma de dos oleadas: una en octubre de 2022, seguida de una segunda en abril de 2023.