El grupo de hackers patrocinado por el estado ruso, conocido como APT29, se ha atribuido una nueva campaña de phishing que aprovecha los servicios en la nube legítimos como Google Drive y Dropbox para entregar cargas útiles maliciosas en sistemas comprometidos.

> *«Se cree que estas campañas se dirigieron a varias misiones diplomáticas occidentales entre mayo y junio de 2022. Los señuelos incluidos en estas campañas sugieren apuntar a una embajada extranjera en Portugal, así como a una embajada extranjera en Brasil»,* dijo Unit42 de Palo Alto Networks.

APT29, también conocido como Cozy Bear, Cloaked Ursa o The Dukes, se caracteriza como un grupo de ciberespionaje organizado que trabaja para recopilar inteligencia que se alinea con los objetivos estratégicos de Rusia.

Microsoft rastrea por separado algunos aspectos de las actividades de la amenaza persistente avanzada, incluido el ataque a la cadena de suministro de SolarWinds de 2020, con el nombre de Nobelium, y Mandiant lo llama un actor de amenazas en evolución, disciplinado y altamente calificado que opera con un mayor nivel de seguridad operativa.

Las intrusiones más recientes son una continuación de la misma operación encubierta previamente detallada por Mandiant y Cluster25 en mayo de 2022, en la que los correos electrónicos de phishing dirigido condujeron al despliegue de Cobalt Strike Beacons por medio de un archivo adjunto HTML denominado EnvyScout (también conocido como ROOTSAW) adjunto directamente en las misivas.

Lo que cambió en las iteraciones más recientes es el uso de servicios en la nube como Dropbox y Google Drive para ocultar sus acciones y recuperar malware adicional en los entornos de destino. Se dice que una segunda versión del ataque observado a fines de mayo de 2022 se adaptó aún más para alojar el cuentagotas HTML en Dropbox.

> *«Las campañas y las cargas útiles analizadas a lo largo del tiempo muestran un fuerte enfoque en operar bajo el radar y reducir las tasas de detección. En este sentido, incluso el uso de servicios legítimos como Trello y Dropbox sugiere que la voluntad del adversario de operar durante mucho tiempo dentro de los entornos de las víctimas permanece sin ser detectada»,* dijo Cluster25.

EnvyScout, por otro lado, sirve como una herramienta auxiliar para infectar aún más al objetivo con el implante elegido por el atacante, en este caso, un ejecutable basado en .NET que está oculto en múltiples capas de ofuscación y se utiliza para extraer información del sistema y ejecutar binarios de próxima etapa como Cobalt Strike obtenidos de Google Drive.

> *«El uso de los servicios de Dropbox y Google Drive es una nueva técnica para este actor y resulta difícil de detectar debido a la naturaleza omnipresente de estos servicios y al hecho de que millones de clientes en todo el mundo confían en ellos»,* dijeron los investigadores.

Estos hallazgos también coinciden con una nueva declaración del Consejo de la Unión Europea, que denuncia el aumento de las actividades cibernéticas maliciosas perpetradas por los atacantes rusos y *«condena este comportamiento inaceptable en el ciberespacio».*

> *«Este aumento de actividades cibernéticas maliciosas, en el contexto de la guerra contra Ucrania, crea riesgos inaceptables de efectos indirectos, malas interpretaciones y una posible escalada»,* dijo el Consejo en un comunicado.