Los individuos que representan una amenaza han estado cada vez más utilizando la API de Microsoft Graph con propósitos maliciosos con el fin de evitar ser detectados.

Este uso tiene como objetivo *«facilitar las comunicaciones con la infraestructura de comando y control (C&C) alojada en los servicios en la nube de Microsoft»,* según un informe compartido por el Equipo de Cazadores de Amenazas de Symantec, una división de Broadcom.

Desde enero de 2022, se ha observado que varios grupos de piratas informáticos alineados con estados nación han estado empleando la API de Microsoft Graph para llevar a cabo operaciones de comando y control. Esto incluye a actores de amenazas identificados como APT28, REF2924, Red Stinger, Flea, APT29 y OilRig.

La primera vez que se tiene conocimiento del uso de la API de Microsoft Graph antes de su adopción más generalizada se remonta a junio de 2021, en relación con un conjunto de actividades denominado Harvester, que se descubrió utilizando un implante personalizado conocido como Graphon, que se valía de la API para comunicarse con la infraestructura de Microsoft.

Symantec ha informado de que recientemente detectó el empleo de la misma táctica contra una organización no especificada en Ucrania, que implicaba el despliegue de un malware previamente desconocido llamado BirdyClient (también conocido como OneDriveBirdyClient).

Un archivo DLL denominado «vxdiff.dll», idéntico a un DLL legítimo asociado con una aplicación llamada Apoint («apoint.exe»), está diseñado para conectarse a la API de Microsoft Graph y utilizar OneDrive como servidor C&C para cargar y descargar archivos.

Se desconoce el método exacto de distribución del archivo DLL, y si implica la carga lateral de DLL. Además, no está claro quiénes son los actores de amenazas ni cuáles son sus objetivos finales.

> *«Las comunicaciones del atacante con los servidores C&C a menudo pueden levantar alertas en las organizaciones objetivo. La popularidad de la API de Graph entre los atacantes puede deberse a la creencia de que el tráfico hacia entidades conocidas, como los servicios en la nube ampliamente utilizados, es menos probable que despierte sospechas»*, señaló Symantec.
>
> *«Además de parecer inocuas, estas acciones representan una fuente económica y segura de infraestructura para los atacantes, ya que las cuentas básicas para servicios como OneDrive son gratuitas.»*

Este desarrollo se produce en un momento en que Permiso reveló cómo los comandos de administración en la nube podrían ser explotados por adversarios con acceso privilegiado para ejecutar comandos en máquinas virtuales.

> *«En la mayoría de los casos, los atacantes aprovechan las relaciones de confianza para ejecutar comandos en instancias de cómputo conectadas (VM) o entornos híbridos al comprometer terceros proveedores externos o contratistas que tienen acceso privilegiado para administrar entornos basados en la nube internos»*, explicó la empresa de seguridad en la nube.
>
> *«Al comprometer estas entidades externas, los atacantes pueden obtener acceso elevado que les permite ejecutar comandos dentro de instancias de cómputo (VM) o entornos híbridos.»*