Una campaña de amenazas en curso llamada VEILDrive ha estado utilizando servicios legítimos de Microsoft, como Teams, SharePoint, Quick Assist y OneDrive, como parte de sus tácticas.

> *«Aprovechando los servicios de Microsoft SaaS, que incluyen Teams, SharePoint, Quick Assist y OneDrive, el atacante empleó infraestructuras confiables de organizaciones ya comprometidas para distribuir ataques de spear-phishing y almacenar malware,»* explicó la empresa israelí de ciberseguridad Hunters en un informe reciente.
>
> *«Esta estrategia centrada en la nube permitió al actor malicioso evadir la detección por los sistemas de monitoreo tradicionales.»*

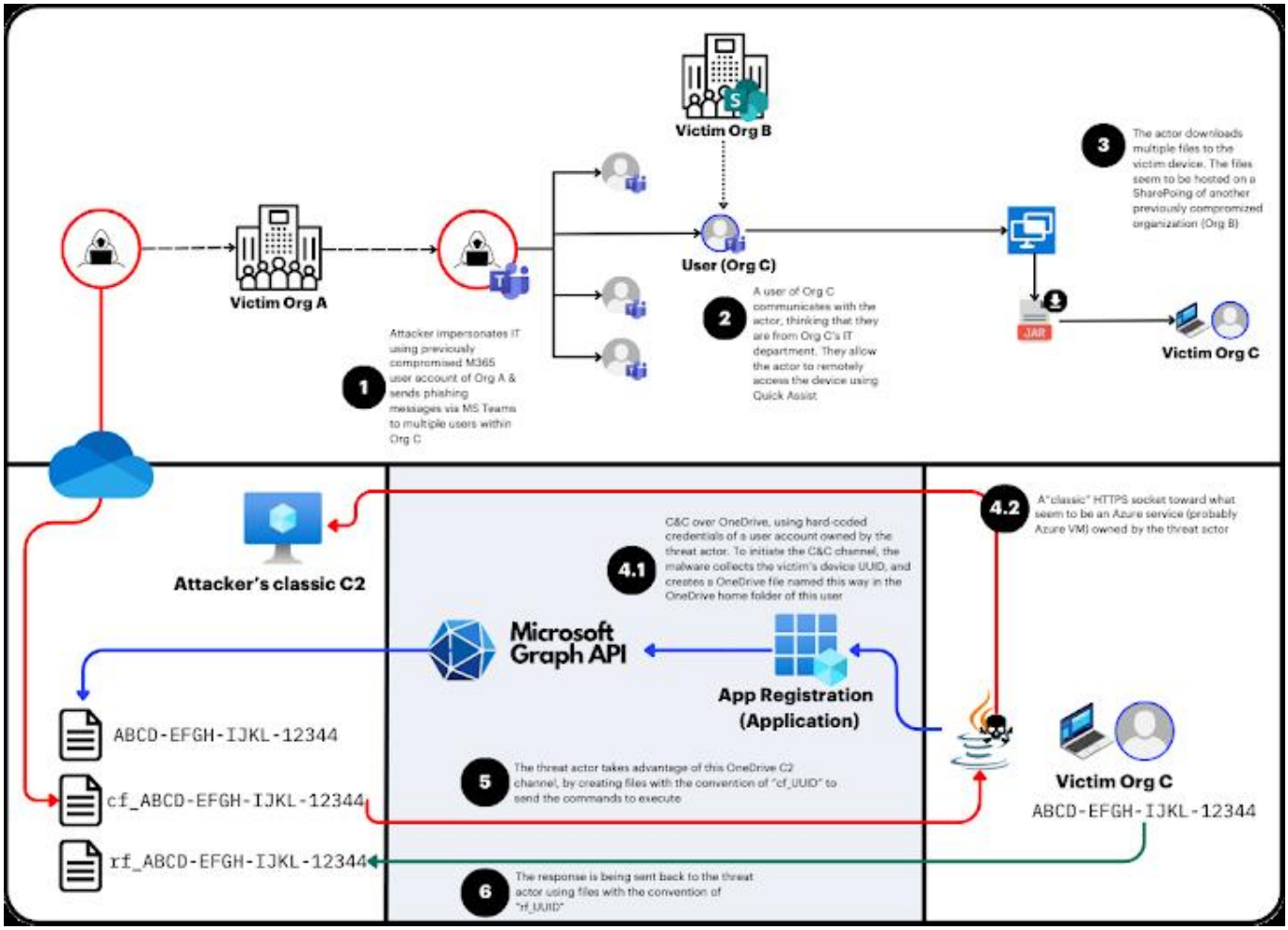
Hunters informó que detectó la campaña en septiembre de 204, tras intervenir en un incidente de ciberseguridad dirigido contra una organización de infraestructura crítica en los Estados Unidos. La empresa prefirió no revelar el nombre de la organización afectada, a la cual denominó «Org C.»

Se sospecha que esta actividad comenzó un mes antes y culminó en la implementación de un malware basado en Java que utiliza OneDrive como mecanismo de comando y control (C2).

El grupo de amenazas detrás de esta operación habría enviado mensajes en Teams a cuatro empleados de Org C, haciéndose pasar por un miembro del equipo de TI y solicitando acceso remoto a sus sistemas mediante la herramienta Quick Assist.

Lo que hizo notable este método de compromiso inicial es que el atacante utilizó una cuenta de usuario que pertenecía a una posible víctima anterior (Org A), en lugar de crear una cuenta nueva para este fin.

> *«Los mensajes de Microsoft Teams que recibieron los usuarios objetivo de Org C fueron posibles gracias a la funcionalidad de 'Acceso Externo' de Teams, que permite la comunicación directa con cualquier organización externa de forma predeterminada,»* señaló Hunters.



En el siguiente paso, el actor de amenazas compartió un enlace de descarga a través del chat, a un archivo ZIP de SharePoint («Client_v8.16L.zip») alojado en otro inquilino (Org B). El archivo ZIP incluía, entre otros archivos, otra herramienta de acceso remoto llamada LiteManager.

El acceso remoto conseguido a través de Quick Assist fue utilizado para crear tareas programadas en el sistema y ejecutar periódicamente el software de administración remota (RMM) LiteManager.

También se descargó un segundo archivo ZIP («Cliento.zip») de forma similar, el cual contenía el malware basado en Java como un archivo JAR junto con el Java Development Kit (JDK) necesario para ejecutarlo.

El malware fue diseñado para conectarse a una cuenta de OneDrive controlada por el atacante usando credenciales de Entra ID (anteriormente Azure Active Directory) incluidas en el código, usándola como un C2 para recuperar y ejecutar comandos de PowerShell en el sistema infectado a través de la API de Microsoft Graph.

Incluye además un mecanismo de respaldo que establece un socket HTTPS hacia una máquina virtual de Azure, utilizada para recibir y ejecutar comandos en el contexto de PowerShell.

No es la primera vez que el programa Quick Assist se ha usado de esta forma. En mayo, Microsoft advirtió que un grupo de ciberdelincuentes motivado por ganancias financieras, conocido como Storm-1811, había abusado de las funciones de Quick Assist, haciéndose pasar por profesionales de TI o personal de soporte técnico para acceder y desplegar el ransomware Black Basta.

Este desarrollo llega semanas después de que Microsoft alertara sobre campañas que explotan servicios legítimos de alojamiento de archivos, como SharePoint, OneDrive y Dropbox, para evitar la detección.

> *«Esta estrategia basada en SaaS dificulta la detección en tiempo real y supera las defensas convencionales. Sin ningún tipo de ofuscación y con un código bien estructurado, este malware desafía el diseño típico orientado a la evasión, resultando inusualmente claro y directo»,* declaró Hunters.