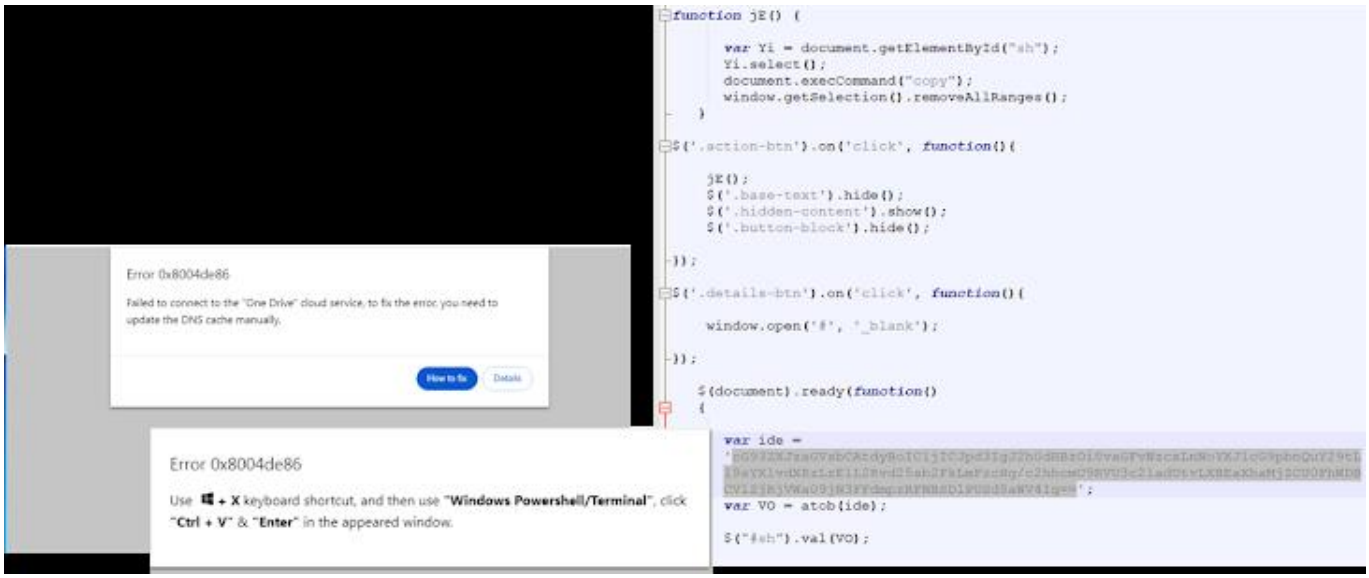
Investigadores en ciberseguridad han alertado sobre una nueva campaña de phishing que utiliza la técnica ClickFix para distribuir Havoc, un marco de comando y control (C2) de código abierto.

«El actor de amenaza oculta cada etapa del malware detrás de un sitio de SharePoint y emplea una versión modificada de Havoc Demon junto con la API de Microsoft Graph para disfrazar las comunicaciones C2 dentro de servicios confiables y ampliamente conocidos», señaló Fortinet ForEGuard Labs en un informe técnico.

El ataque comienza con un correo electrónico de phishing que contiene un archivo HTML adjunto («Documents.html»). Al abrirlo, se muestra un mensaje de error diseñado para engañar a los usuarios mediante la técnica ClickFix, incitándolos a copiar y ejecutar un comando malicioso de PowerShell en su terminal. Este paso desencadena la siguiente fase del ataque.

El comando ejecutado descarga y ejecuta un script de PowerShell alojado en un servidor SharePoint controlado por los atacantes. Antes de continuar, el script verifica si se está ejecutando en un entorno de análisis (sandbox). Si no lo está, descarga el intérprete de Python («pythonw.exe») en caso de que aún no esté presente en el sistema.



Posteriormente, se obtiene y ejecuta un script de Python desde el mismo servidor de SharePoint, el cual actúa como cargador de shellcode para KaynLdr, un cargador reflectivo escrito en C y ensamblador (ASM) que permite lanzar una DLL incrustada. En este caso, dicha DLL corresponde al agente Havoc Demon en el equipo infectado.

> *«El actor de amenaza utiliza Havoc junto con la API de Microsoft Graph para ocultar la comunicación C2 dentro de servicios ampliamente conocidos»,* explicó Fortinet, agregando que el marco permite recopilar información, gestionar archivos, ejecutar comandos y cargas útiles, manipular tokens e incluso llevar a cabo ataques de Kerberos.

Este hallazgo se produce en un contexto donde Malwarebytes ha revelado que los ciberdelincuentes siguen explotando una vulnerabilidad en las políticas de anuncios de Google para atacar a usuarios de PayPal mediante anuncios fraudulentos en cuentas de anunciantes comprometidas.

Los anuncios buscan engañar a víctimas que buscan ayuda con problemas de cuenta o pagos, dirigiéndolos a llamar a un número fraudulento donde, probablemente, terminan proporcionando su información personal y financiera.

> «Una debilidad en las políticas de Google sobre páginas de destino (también conocidas como URLs finales) permite a cualquier persona suplantar sitios web populares, siempre que la página de destino y la URL visible en el anuncio compartan el mismo dominio», explicó Jérôme Segura, director sénior de investigación en Malwarebytes.
>
> *«Los estafadores de soporte técnico actúan como buitres sobrevolando los términos de búsqueda más populares en Google, especialmente aquellos relacionados con asistencia en línea o atención al cliente.»*