Los investigadores de ciberseguridad están alertando sobre una nueva campaña de phishing que tiene como objetivo a los usuarios de Microsoft OneDrive con el propósito de ejecutar un script malicioso de PowerShell.

> *«Esta campaña depende en gran medida de tácticas de ingeniería social para engañar a los usuarios y hacer que ejecuten un script de PowerShell, comprometiendo así sus sistemas»*, dijo el investigador de seguridad de Trellix, Rafael Pena, en un análisis publicado el lunes.

La empresa de ciberseguridad está rastreando esta «*astuta*» campaña de phishing y descarga bajo el nombre de OneDrive Pastejacking.

El ataque se desarrolla a través de un correo electrónico que contiene un archivo HTML que, al abrirse, muestra una imagen que simula una página de OneDrive e incluye un mensaje de error que dice: *«No se pudo conectar al servicio en la nube 'OneDrive'. Para solucionar el error, necesita actualizar manualmente la caché de DNS».*

El mensaje también ofrece dos opciones, «*Cómo solucionar*» y «*Detalles*«, siendo esta última la que dirige al destinatario del correo electrónico a una página legítima de Microsoft Learn sobre solución de problemas de DNS.

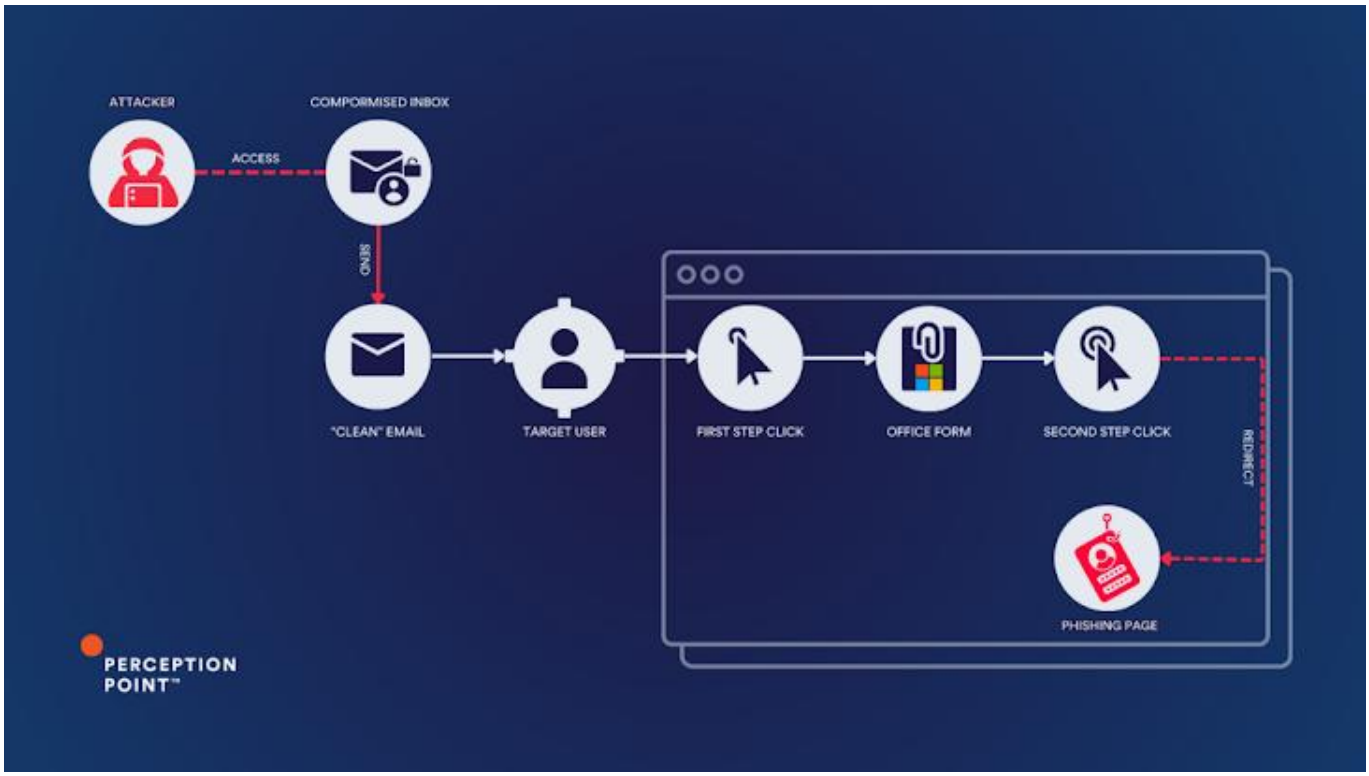
Sin embargo, al hacer clic en «Cómo solucionar», se solicita al usuario que siga una serie de pasos, que incluyen presionar «Tecla de Windows + X» para abrir el menú de Enlace rápido, iniciar el terminal de PowerShell y pegar un comando codificado en Base64 para supuestamente solucionar el problema.

> *«El comando [...] primero ejecuta ipconfig /flushdns, luego crea una carpeta en la unidad C: llamada 'downloads'. Posteriormente, descarga un archivo comprimido en esta ubicación, lo renombra, extrae su contenido ('script.a3x' y 'AutoIt3.exe') y ejecuta script.a3x usando AutoIt3.exe»,* explicó Pena

Se ha observado que la campaña tiene como objetivo a usuarios en EE.UU., Corea del Sur, Alemania, India, Irlanda, Italia, Noruega y el Reino Unido.

La divulgación se basa en hallazgos similares de ReliaQuest, Proofpoint y McAfee Labs, indicando que los ataques de phishing que emplean esta técnica, también conocidos como ClickFix, se están volviendo cada vez más comunes.

El desarrollo se produce en medio del descubrimiento de una nueva campaña de ingeniería social basada en correos electrónicos que distribuye archivos de acceso directo de Windows falsos que conducen a la ejecución de cargas maliciosas alojadas en la infraestructura de la Red de Entrega de Contenido (CDN) de Discord.



Las campañas de phishing también se han observado cada vez más enviando correos electrónicos que contienen enlaces a Microsoft Office Forms desde cuentas de correo

electrónico legítimas previamente comprometidas para atraer a las víctimas a divulgar sus credenciales de inicio de sesión de Microsoft 365 bajo el pretexto de restaurar sus mensajes de Outlook.

> *«Los atacantes crean formularios que parecen legítimos en Microsoft Office Forms, incrustando enlaces maliciosos dentro de los formularios. Estos formularios luego se envían a las víctimas en masa por correo electrónico bajo la apariencia de solicitudes legítimas, como cambiar contraseñas o acceder a documentos importantes, imitando plataformas y marcas confiables como Adobe o el visor de documentos de Microsoft SharePoint»*, dijo Perception Point.

Además, otras oleadas de ataques han utilizado señuelos temáticos de facturas para engañar a las víctimas a compartir sus credenciales en páginas de phishing alojadas en Cloudflare R2, que luego son exfiltradas al actor de la amenaza a través de un bot de Telegram.

No es sorprendente que los adversarios estén constantemente buscando diferentes formas de contrabandear malware sigilosamente a través de las Pasarelas de Correo Electrónico Seguro (SEG) para aumentar la probabilidad de éxito de sus ataques.

Según un informe reciente de Cofense, los actores maliciosos están abusando de la forma en que las SEG escanean los archivos adjuntos en formato ZIP para entregar el ladrón de información Formbook mediante DBatLoader (también conocido como ModiLoader y NatsoLoader).

Específicamente, esto implica hacer pasar la carga útil HTML como un archivo MPEG para evadir la detección aprovechando el hecho de que muchos extractores de archivos comunes y las SEG analizan la información del encabezado del archivo, pero ignoran el pie de página que puede contener información más precisa sobre el formato del archivo.

> *«Los actores de la amenaza utilizaron un archivo adjunto en formato ZIP y cuando*

> *la SEG escaneó el contenido del archivo, el archivo comprimido fue detectado como un archivo de video MPEG y no fue bloqueado ni filtrado»,* señaló la compañía.
>
> *«Cuando este archivo adjunto se abrió con herramientas comunes/populares de extracción de archivos como 7-Zip o Power ISO, también parecía contener un archivo de video MPEG, pero no se reproducía. Sin embargo, cuando el archivo comprimido se abrió en un cliente de Outlook o a través del administrador de archivos comprimidos de Windows Explorer, el archivo MPEG se detecta (correctamente) como un archivo HTML».*