Una operación de ciberespionaje alineada con Corea del Sur ha sido vinculada con la explotación de una vulnerabilidad crítica de ejecución remota de código, que ya ha sido corregida, en Kingsoft WPS Office para instalar una puerta trasera personalizada llamada SpyGlace.

Según las empresas de ciberseguridad ESET y DBAPPSecurity, esta actividad ha sido atribuida a un actor de amenazas conocido como APT-C-60. Los ataques han sido descubiertos infectando a usuarios en China y el Este de Asia con malware.

La vulnerabilidad en cuestión es CVE-2024-7262 (con una puntuación CVSS de 9.3), que se debe a la falta de validación adecuada de las rutas de archivos proporcionadas por los usuarios. Este fallo permite a un atacante cargar una biblioteca de Windows arbitraria y ejecutar código de manera remota.

El fallo *«permite la ejecución de código al secuestrar el flujo de control del componente del plugin de WPS Office promecefpluginhost.exe»,* explicó ESET, añadiendo que encontraron otra manera de lograr el mismo resultado. Esta segunda vulnerabilidad está catalogada como CVE-2024-7263 (con una puntuación CVSS de 9.3).

El ataque diseñado por APT-C-60 aprovecha la vulnerabilidad en un exploit de un solo clic que se presenta en forma de un documento de hoja de cálculo malicioso que fue subido a VirusTotal en febrero de 2024.

Específicamente, el archivo contiene un enlace malicioso que, al ser pulsado, activa una secuencia de infección en varias etapas para desplegar el troyano SpyGlace, un archivo DLL denominado TaskControler.dll con capacidades para robar archivos, cargar plugins y ejecutar comandos.

«Los desarrolladores del exploit incrustaron una imagen de las filas y columnas de la hoja de cálculo dentro del documento para engañar al usuario y hacerle creer que se trata de una hoja de cálculo normal», señaló el investigador de seguridad Romain Dumont. «El enlace malicioso estaba vinculado a la imagen para que al hacer clic en una celda de la imagen se

activara el exploit.»

Se cree que APT-C-60 ha estado activo desde 2021, con la detección de SpyGlace en estado salvaje desde junio de 2022, según la empresa de ciberseguridad con sede en Beijing ThreatBook.

> *«Ya sea que el grupo haya desarrollado o adquirido el exploit para CVE-2024-7262, ciertamente requirió una investigación detallada sobre los aspectos internos de la aplicación, así como conocimiento del comportamiento del proceso de carga en Windows»*, comentó Dumont.
>
> *«El exploit es astuto, ya que es lo suficientemente engañoso como para hacer que cualquier usuario haga clic en una hoja de cálculo que parece legítima, al mismo tiempo que es altamente efectivo y confiable. La elección del formato de archivo MHTML permitió a los atacantes transformar una vulnerabilidad de ejecución de código en una de ejecución remota.»*

La revelación se produce cuando la empresa eslovaca de ciberseguridad señaló que un plugin malicioso de terceros para la aplicación de mensajería Pidgin, llamado ScreenShareOTR (o ss-otr), contenía código diseñado para descargar binarios adicionales desde un servidor de comando y control (C&C), lo que finalmente condujo a la instalación del malware DarkGate.

> *«La funcionalidad anunciada del plugin incluye compartir pantalla utilizando el protocolo seguro de mensajería fuera de registro (OTR). Sin embargo, además de esto, el plugin contiene código malicioso. En particular, algunas versiones de pidgin-screenshare.dll pueden descargar y ejecutar un script de PowerShell desde el servidor C&C»*, indicó ESET.

El plugin, que también cuenta con funciones de keylogger y captura de pantalla, ha sido eliminado de la lista de plugins de terceros. Se recomienda a los usuarios que hayan instalado este plugin que lo eliminen de inmediato.

ESET también descubrió que el mismo código de puerta trasera maliciosa encontrado en ScreenShareOTR fue detectado en una aplicación llamada Cradle («cradle[.]im»), que afirma ser una bifurcación de código abierto de la aplicación de mensajería Signal. La aplicación estuvo disponible para su descarga durante casi un año desde septiembre de 2023.

El código malicioso se descarga ejecutando un script de PowerShell, que luego recupera y ejecuta un script AutoIt compilado que finalmente instala DarkGate. La versión de Cradle para Linux entrega un ejecutable ELF que descarga y ejecuta comandos de shell y envía los resultados a un servidor remoto.

Otro indicador común es que tanto el instalador del plugin como la aplicación Cradle están firmados con un certificado digital válido emitido a una empresa polaca llamada «INTERREX – SP. Z O.O.», lo que sugiere que los responsables están utilizando diferentes métodos para propagar malware.