Investigadores de seguridad cibernética detallaron un mecanismo de persistencia *«simple pero eficiente»* adoptado por un cargador de malware relativamente incipiente llamado Colibri, que se ha observado implementando un ladrón de información de Windows conocido como Vidar como parte de una nueva campaña.

> *«El ataque comienza con un documento de Word malicioso que despliega un bot Colibri que luego entrega el Vidar Stealer. El documento contacta con un servidor remoto en (securetunnel[.]co) para cargar una plantilla remota llamada 'trkal0.dot' que contacta con una macro maliciosa»,* dijeron los investigadores.

Colibri, documentado por primera vez por FR3D.HK y la compañía india de seguridad cibernética CloudSEK a inicios de 2022, es una plataforma de malware como servicio (MaaS) que está diseñada para colocar cargas útiles adicionales en sistemas comprometidos. Los primeros signos del cargador aparecieron en los foros clandestinos rusos en agosto de 2021.

> *«Este cargador tiene múltiples técnicas que ayudan a evitar la detección. Esto incluye omitir la IAT (Tabla de direcciones de importación) junto con las cadenas cifradas para dificultar el análisis»,* dijo Marah Aboud, investigadora de CloudSEK.

La cadena de ataques de la campaña observada por Malwarebytes aprovecha una técnica llamada inyección remota de plantillas para descargar el cargador Colibri («setup.exe») por medio de un documento de Microsoft Word armado.

Después, el cargador utiliza un método de persistencia no documentado anteriormente para sobrevivir a los reinicios de la máquina, primero, se coloca su propia copia en la ubicación «%APPDATA%\Local\Microsoft\WindowsApps» y la nombra como «Get-Variable.exe«.

> *«Sucede que Get-Variable es un cmdlet de PowerShell válido (un cmdlet es un*

> *comando liviano que se utiliza en el entorno de Windows PowerShell) que se usa para recuperar el valor de una variable en la consola actual»,* explicaron los administradores.

Pero debido a que PowerShell se ejecuta de forma predeterminada en la ruta de WindowsApps, el comando emitido durante la creación de la tarea programada da como resultado la ejecución del binario malicioso en lugar de su contraparte legítima.

Esto significa efectivamente que *«un adversario puede lograr fácilmente la persistencia al combinar una tarea programada y cualquier carga útil (siempre que se llame Get-Variable.exe y se coloque en la ubicación adecuada)»,* dijeron los investigadores.

Estos hallazgos se producen cuando la empresa de seguridad cibernética Trustwave detalló el mes pasado una campaña de phishing basada en correo electrónico que aprovecha os archivos de ayuda HTML compilada (CHM) de Microsoft para distribuir el malware Vidar en un esfuerzo por pasar desapercibido.