Se ha observado una nueva ola de campañas de phishing que propaga un malware previamente documentado llamado SVCReady.

> *«El malware se destaca por la forma inusual en que se entrega a las PC de destino, utilizando un código de shell oculto en las propiedades de los documentos de Microsoft Office»,* dijo Patrick Schläpfer, analista de amenazas de HP.

Se cree que SVCReady se encuentra en su etapa inicial de desarrollo, y los autores actualizaron iterativamente el malware varias veces el mes pasado. Los primeros signos de actividad datan del 22 de abril de 2022.

Las cadenas de infección implican el envío de archivos adjuntos de documentos de Microsoft Word a los objetivos por correo electrónico, que contienen macros de VBA para activar la implementación de cargas útiles maliciosas.

Pero esta campaña se destaca porque en primer lugar emplea PowerShell o MSHTA para recuperar los ejecutables de la siguiente etapa desde un servidor remoto, la macro ejecuta el código de shell almacenado en las propiedades del documento, que posteriormente elimina el malware SVCReady.

Además de lograr la persistencia en el host infectado por medio de una tarea programada, el malware tiene la capacidad de recopilar información del sistema, capturar pantalla, ejecutar comandos de shell, así como descargar y ejecutar archivos arbitrarios.

Esto también incluye la entrega de RedLine Stealer como carga útil de seguimiento en una instancia el 26 de abril, luego de que las máquinas se vieran comprometidas inicialmente con SVCReady.

HP dijo que identificó superposiciones entre los nombres de archivo de los documentos de señuelo y las imágenes contenidas en los archivos utilizados para distribuir SVCReady y los empleados por otro grupo llamado TA551 (también conocido como Hive0106 o Shathak),

pero no está claro hasta ahora si es el mismo actor de amenazas detrás de la última campaña.

> *«Es posible que estemos viendo los artefactos dejados por dos atacantes diferentes que utilizan las mismas herramientas. Sin embargo, nuestros hallazgos muestran que los actores detrás de las campañas TA551 y SVCReady están utilizando plantillas similares y potencialmente creadores de documentos»,* dijo Schläpfer.