En otro caso de ataque a la cadena de suministro de software, hackers no identificados violaron el sitio web de MonPass, una de las principales autoridades de certificación de Mongolia, para crear una puerta trasera en su software de instalación con los binarios de Cobalt Strike.

El cliente troyano estuvo disponible para su descarga entre el 8 de febrero de 2021 y el 3 de marzo de 2021, dijo la compañía checa de software de seguridad cibernética Avast en un informe publicado el jueves.

Además, un servidor web público alojado por MonPass se infiltró potencialmente hasta ocho veces por separado, y los investigadores descubrieron ocho shells web diferentes y puertas traseras en el servidor comprometido.

La investigación de Avast acerca del incidente comenzó luego de que se descubrió el instalador con puerta trasera y el implante en uno de los sistemas de sus clientes.

> *«El instalador malicioso es un archivo sin firmar. Comienza descargando la versión legítima del instalador del sitio web oficial de MonPass. Esta versión legítima se coloca en la carpeta 'C:\Users\Public\' y se ejecuta bajo un nuevo proceso. Esto garantiza que el instalador se comporta como se esperaba, lo que significa que es poco probable que un usuario habitual note algo sospechoso»*, dijeron los investigadores.

El modus operandi también es notable por el uso de esteganografía para transferir el código shell a la máquina víctima, con el instalador descargando un archivo de imagen de mapa de bits (.BMP) desde un servidor remoto para extraer e implementar una carga útil de baliza Cobalt Strike cifrada.

MonPass fue notificado del incidente el 22 de abril, luego de lo cual, la autoridad de certificación tomó medidas para abordar su servidor comprometido y notificar a quienes descargaron el cliente con puerta trasera.

El incidente marca la segunda vez que el software proporcionado por una autoridad de certificación se ve comprometido para infectar objetivos con puertas traseras maliciosas. En diciembre de 2020, ESET reveló una campaña llamada «*Operation SignSight*», en la que se manipuló un conjunto de herramientas de firma digital de la Autoridad de Certificación del Gobierno de Vietnam (VGCA) para incluir software espía capaz de acumular información del sistema e instalar malware adicional.