Se está observando a un atacante centrado en el espionaje utilizando un truco esteganográfico para ocultar una puerta trasera previamente no documentada en un logotipo de Windows en sus ataques contra los gobiernos de Medio Oriente.

Symantec Threat Hunter Team de Broadcom atribuyó las herramientas actualizadas a un grupo de hacking que se rastrea bajo el nombre de Witchetty, también conocido como LookingFrog, un subgrupo que opera bajo el alias TA410.

Las intrusiones que involucran a TA410, que se cree que comparten conexiones con un grupo de amenazas chino conocido como APT10 (también conocido como Cicada, Stone Panda o TA429), presentan principalmente un implante modular llamado LookBack.

El último análisis de Symantec de los ataques entre febrero y septiembre de 2022, durante los cuales el grupo apuntó a los gobiernos de dos países del Medio Oriente y la bolsa de valores de una nación africada, destaca el uso de otra puerta trasera denominada Stegmap.

El nuevo malware aprovecha la esteganografía, una técnica usada para incrustar un mensaje (en este caso, malware) en un documento no secreto, con el fin de extraer código malicioso de una imagen de mapa de bits de un antiguo logotipo de Microsoft Windows alojado en un repositorio de GitHub.

> *«Ocultar la carga útil de esta forma permitió a los atacantes alojarla en un servicio gratuito y confiable. Es mucho menos probable que las descargas desde hosts confiables como GitHub generen señales de alerta que las descargas desde un servidor de comando y control (C&C) controlado por un atacante»*, dijeron los investigadores.

Stegmap, como cualquier otra backdoor, tiene una amplia gama de funciones que le permiten realizar operaciones de manipulación de archivos, descargar y ejecutar ejecutables, finalizar procesos y realizar modificaciones en el Registro de Windows.

Los ataques que conducen al despliegue de Stegmap utilizan las vulnerabilidades ProxyLogon y ProxyShell en Exchange Server para eliminar el shell web de China Chopper, que después de usa para llevar a cabo actividades de robo de credenciales y movimiento lateral, antes de lanzar el malware LookBack.

Una línea de tiempo de una intrusión en una agencia gubernamental en el Medio Oriente revela que witchetty mantuvo el acceso remoto por seis meses y montó una amplia gama de esfuerzos posteriores a la explotación, incluyendo la enumeración de la red y la instalación de malware personalizado, hasta el 1 de septiembre de 2022.

> *«Witchtery ha demostrado la capacidad de refinar y actualizar continuamente su conjunto de herramientas para comprometer objetivos de interés»,* dijeron los investigadores.

> *«La explotación de las vulnerabilidades en los servidores públicos le proporciona una ruta hacia las organizaciones, mientras que las herramientas personalizadas combinadas con el uso excepto de tácticas de vivir de la tierra permiten mantener una presencia persistente a largo plazo en las organizaciones objetivo».*