La compañía china de seguridad cibernética, Qihoo 360 Netlab, dijo que se asoció con la compañía tecnológica Baidu para interrumpir una red de bots de malware que infecta a cientos de miles de sistemas.

La red de bots se atribuye a un grupo denominado ShuangQiang, también conocido como Double Gun, que ha estado detrás de distintos ataques desde 2017 destinados a comprometer computadoras con sistema operativos Windows con bootkits MBR y VBR, e instalar controladores maliciosos para obtener ganancias y secuestrar el tráfico web a sitios de comercio electrónico.

Además de utilizar imágenes cargadas en Baidu Tieba para distribuir archivos de configuración y malware, una técnica llamada esteganografía, el grupo comenzó a utilizar el almacenamiento de Alibaba Cloud para almacenar archivos de configuración y la plataforma de análisis de Baidu Tongji para administrar la actividad de sus hosts infectados, según los investigadores.

El compromiso inicial se basa en atraer a los usuarios desprevenidos para que instalen software de lanzamiento de juegos desde portales de juegos incompletos que tienen código malicioso bajo la apariencia de un parche.

Una vez que el usuario descarga e instala el parche, accede a la información de configuración para descargar un programa separado llamado *«cs.dll»* de Baidu Tieba que se almacena como un archivo de imagen.

En la siguientes etapas, cs.dll no dolo crea un ID de bot y lo informa al servidor controlado por el atacante, sino que también inyecta un segundo controlador que secuestra los procesos del sistema (por ejemplo, lassas.exe y svchost.exe) para descargar las cargas útiles de la siguiente etapa para avanzar.

Los investigadores de Qihoo también detallaron una segunda cadena de infección en la que el software del cliente del juego se altera con bibliotecas maliciosas (una versión modificada de photobase.dll), utilizando un método llamado secuestro de DLL para liberar y cargar el

controlador malicioso antes de cargar el módulo legítimo.

La compañía dijo que contactó al equipo de seguridad de Baidu el 14 de mayo y que tomaron medidas conjuntas para evitar una mayor propagación de la botnet al bloquear todas las descargas de las URL involucradas.

> *«Durante esta operación conjunta, a través del análisis, el intercambio y la respuesta de la información sobre amenazas, hemos logrado comprender mejor los medios técnicos, la lógica y las reglas de la pandilla Double Gun»*, dijo Baidu.