Una entidad gubernamental sin identificar en Afganistán fue objeto de un ataque utilizando una herramienta de acceso remoto previamente desconocida llamada HrServ, en lo que se sospecha que es un ataque de amenaza persistente avanzada (APT).

> *«El web shell en cuestión, una biblioteca de vínculos dinámicos (DLL) denominada «hrserv.dll», muestra características sofisticadas, como métodos de codificación personalizados para la comunicación con el cliente y ejecución en la memoria»,* según la análisis publicado esta semana por el investigador de seguridad de Kaspersky, Mert Degirmenci.

La empresa de ciberseguridad rusa afirma haber identificado variantes del malware que se remontan a principios de 2021, basándose en las marcas de tiempo de compilación de estos artefactos.

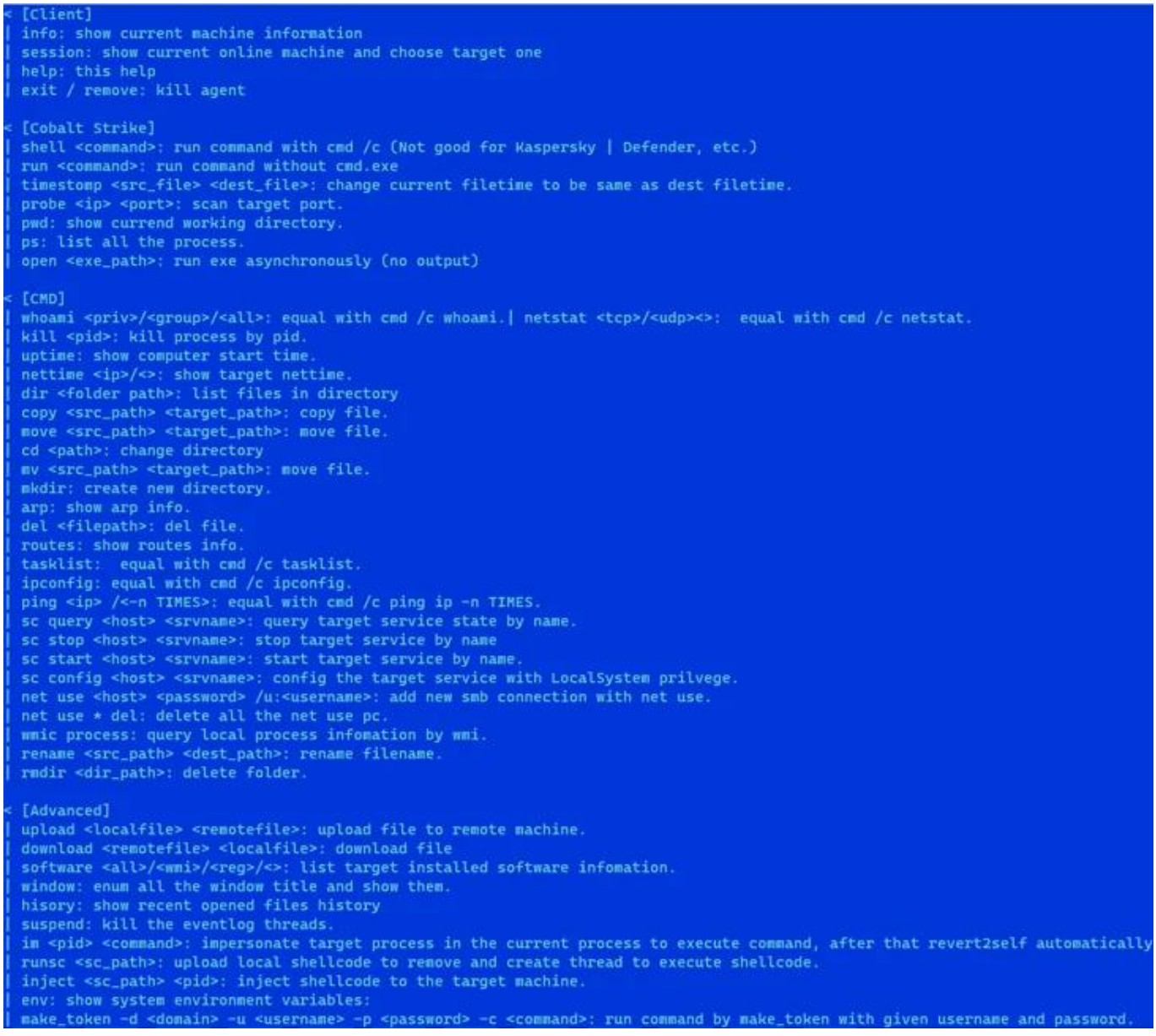
Por lo general, los web shells son herramientas maliciosas que proporcionan control remoto sobre un servidor comprometido. Una vez cargado, permite a los actores de amenazas llevar a cabo diversas actividades de post-explotación, como el robo de datos, el monitoreo del servidor y la expansión lateral dentro de la red.

El proceso del ataque implica el uso de la herramienta de administración remota PAExec, una alternativa a PsExec que sirve como punto de inicio para crear una tarea programada que se camufla como una actualización de Microsoft («MicrosoftsUpdate»), la cual se configura posteriormente para ejecutar un script por lotes de Windows («JKNLA.bat»).

Este script por lotes acepta la ruta absoluta de un archivo DLL («hrserv.dll») como argumento, el cual luego se ejecuta como un servicio para iniciar un servidor HTTP capaz de analizar las solicitudes HTTP entrantes para llevar a cabo acciones adicionales.

> Según Degirmenci, *«basándose en el tipo de información dentro de una solicitud HTTP, se activan funciones específicas». Además, señala que «los parámetros GET*

> *utilizados en el archivo hrserv.dll, que simula servicios de Google, incluyen 'hl'».*



Este parece ser un intento por parte del actor de amenazas de mezclar estas solicitudes fraudulentas en el tráfico de la red y dificultar la distinción entre actividades maliciosas y

eventos benignos.

Dentro de estas solicitudes HTTP GET y POST se encuentra un parámetro llamado «cp», cuyo valor, que varía de 0 a 7, determina la siguiente acción a realizar. Esto puede incluir la creación de nuevos hilos, la generación de archivos con datos arbitrarios, la lectura de archivos y el acceso a datos HTML de Outlook Web App.

Si el valor de «cp» en la solicitud POST es «6», se desencadena la ejecución de código al analizar los datos codificados y copiarlos en la memoria. Posteriormente, se crea un nuevo hilo y el proceso entra en un estado de reposo.

El web shell también tiene la capacidad de activar la ejecución de un *«implante multifuncional»* sigiloso en memoria, encargado de borrar las huellas forenses al eliminar la tarea «MicrosoftsUpdate», así como los archivos DLL y por lotes iniciales.

Aunque actualmente no se conoce al actor de amenazas detrás del web shell, la presencia de varios errores tipográficos en el código fuente sugiere que el autor del malware no es un hablante nativo de inglés.

> *«Es notable que el web shell y el implante de memoria utilicen cadenas diferentes para condiciones específicas. Además, el implante de memoria presenta un mensaje de ayuda meticulosamente elaborado»*, concluyó Degirmenci.

> *«Dados estos factores, las características del malware son más consistentes con actividades maliciosas motivadas financieramente. Sin embargo, su metodología operativa exhibe similitudes con el comportamiento de las APT».*