Source:
Tomado de sitio web Segurmática.

Windows es el sistema operativo más utilizado en equipos de escritorio. Esto hace que los ciberdelincuentes pongan aquí sus miras para crear software malicioso capaz de infectar este tipo de dispositivos. En ocasiones incluso pueden saltarse las barreras de seguridad, que cada vez son más las que tenemos a nuestra disposición.

Esto es lo que ocurre con PowerPepper, un nuevo malware creado por el grupo DeathStalker y que es capaz de saltarse el antivirus de Windows para poder atacar el sistema. Según el grupo de investigadores de seguridad del que nos hacemos eco, los atacantes han creado una nueva campaña de publicidad maliciosa para enviar este malware.

Lo que hacen es alojar su contenido de manera oculta en servicios tan populares como YouTube o Twitter con el objetivo de llegar a las víctimas. Sin embargo lo más peculiar de este asunto es que logra evadir las medidas de seguridad. Esto les permite pasar sin ser detectados como amenaza.

Los investigadores de seguridad indican que PowerPepper aprovechó DNS sobre HTTPS como un canal C2. Ha utilizado ataques de Spear Phishing. De esta forma logran llegar a la víctima y usar un documento Word que contiene la carga útil.

Este malware es una puerta trasera PowerShell en la memoria de Windows y se puede ejecutar de forma remota. Utiliza diferentes técnicas, entre las que podemos nombrar detectar el movimiento del ratón, filtrar las direcciones MAC y evadir los antivirus.

El servidor de comando y control que se utiliza para esta campaña se basa en las comunicaciones a través de DNS sobre HTTPS. Para establecer una solicitud de DoH a un servidor C2, PowerPepper inicialmente intenta aprovechar el programa de Microsoft Excel como cliente web y luego regresa al cliente web estándar de PowerShell.

Para protegernos de este problema es muy importante mantener los sistemas y dispositivos actualizados correctamente. Los investigadores de seguridad recomiendan que para evitar PowerShell los propietarios de sitios web actualicen con frecuencia su CMS y todos los complementos que tengan instalados.

Además es esencial el sentido común. Es muy importante que no cometamos errores que puedan provocar la entrada de este tipo de software malicioso. Hemos visto que utilizan archivos de Microsoft Word para colar la carga útil y llegar a infectar los equipos. Este tipo de amenazas puede llegar a través de correos electrónicos maliciosos, con archivos adjuntos que descargamos inconscientemente y que pueden ser un problema importante. Por ello debemos evitar siempre este tipo de errores.