¿Qué tipo de amenaza es?
BackdoorDiplomacy es también un grupo multiplataforma dirigido a sistemas Windows y Linux. El grupo apunta a servidores con puertos expuestos a Internet, probablemente explotando la seguridad de carga de archivos mal ejecutada o vulnerabilidades sin parchear.

Troyanos: no causan daños en sí mismos sino que están basados en el caballo de troya, una estructura utilizada para cargar cosas ocultas como virus, gusanos y demás. En general, son programas sin licencias y cracks que instalamos pensando que no harán ningún daño porque no somos conscientes de que pueden ser un troyano.
Pueden crear backdoors, que es una puerta trasera para que un dispositivo pueda ser controlado de forma remota por alguien más. Pueden usarlo como un servidor proxy para ocultar ataques o para introducir span.

¿Cómo comienza y cómo se propaga esta amenaza?

Un subconjunto de víctimas fue atacado con ejecutables de recopilación de datos que fueron diseñados para buscar medios extraíbles (probablemente unidades flash –USB). El implante busca de forma rutinaria dichas unidades y, al detectar la inserción de un medio extraíble, intenta copiar todos los archivos que contienen en un archivo protegido con contraseña. BackdoorDiplomacy es capaz de robar la información del sistema de la víctima, tomar capturas de pantalla y escribir, mover o eliminar archivos.

¿Hay más de una amenaza aplicada?

Su metodología de ataque inicial consiste en explotar aplicaciones vulnerables expuestas a Internet en servidores web, con el fin de droppear y ejecutar un webshell. Después del compromiso, a través del webshell, BackdoorDiplomacy utiliza software de código abierto para el reconocimiento y la recopilación de información, y hace uso de la técnica DLL search order hijacking para instalar su backdoor: Turian. Finalmente, BackdoorDiplomacy emplea de manera separada un ejecutable para detectar medios extraíbles, probablemente unidades flash USB, y copiar su contenido en la papelera de reciclaje de la unidad principal.

¿Qué solución o medida recomendarían?

La eliminación manual de un backdoor no es fácil y, de hecho, lo mejor es recurrir a una herramienta para su eliminación automática; los antivirus cuentan con esta opción, de manera que cuando encuentran un virus lo marcan para su posterior eliminación. Este proceso viene explicado paso a paso por el propio antivirus que estemos usando, por lo que generalmente es sencillo de hacer. También podemos recurrir a otros programas de limpieza, como CCleaner o Malwarebytes Anty-malware, para usarlos tras realizar el análisis con el antivirus.