BackdoorDiplomacy

A través de aplicaciones vulnerables expuestas a Internet en servidores web
ataca principalmente a Ministerios de Relaciones Exteriores y empresas de telecomunicaciones de África y Oriente Medio

Instala un backdoor es decir una puerta trasera para entrar siempre al SO y obtiene acceso remoto de código abierto.

BackdoorDiplomacy apuntó a servidores con puertos expuestos a Internet, probablemente explotando vulnerabilidades sin parchear o la pobre implementación de la seguridad de carga de archivos. En un caso específico, observamos a los operadores explotar una vulnerabilidad en F5 BIG-IP (CVE-2020-5902) para droppear un backdoor para Linux. Windows y Linux fueron blancos de ataque

A menudo el usuario debe limpiar y reinstalar el sistema operativo de una computadora infectada por un rootkit

El rootkit modifica el SO para crear una puerta trasera

¿Que tipo de amenaza es?
Backdoor una puerta trasera que permite ingresar al SO y manejarlo de manera remota, permiten al usuario malicioso controla el equipo infectado, pudiendo enviar y recibir archivos, ejecutarlos o eliminarlos, mostrar mensajes, borrar o robar datos, reiniciar el equipo, etc. Es decir, puede controlar el equipo como si estuviese sentado delante de él y a los mandos.

¿Cómo comienza y se propaga?
Aplicaciones vulnerables expuestas a internet

Método de Propagación Backdoor llega a los ordenadores a través de distintas vías: mensajes de correo electrónico que contengan ficheros infectados, redes de ordenadores, CD-ROMs, descargas desde Internet, FTP, disquetes, etc.

¿Más de una amenaza aplicada?

Acceso a usuarios maliciosos al control de un equipo infectado de manera remota.

¿Qué solución o medida se recomienda?
limpiar y reinstalar el sistema operativo