El gobierno federal de Estados Unidos acusó a un ciudadano paquistaní por sobornar a los empleados de la compañía de telecomunicaciones AT&T durante un período de cinco años para ayudar a desbloquear más de 2 millones de teléfonos y plantar malware en la red de la compañía.

Según una acusación revelada el lunes, Fahd reclutó y pagó a personas de AT&T que trabajaban en un centro de llamadas en Bothell, Washington, más de 1 millón de dólares en sobornos entre 2012 y 2017 para ayudarlos a desbloquear teléfonos celulares asociados con números IMEI específicos que de otra forma no serían elegibles para ser eliminados de la red AT&T.

Muhammad Fahd, un sujeto de 34 años de edad de Pakistán, fue arrestado en Hong Kong el año pasado en febrero, como pedido del gobierno de Estados Unidos y fue extraditado a este último país el viernes 2 de agosto de 2019.

Algunas compañía de telecomunicaciones como AT&T, Verizon, T-Mobile y Sprint, venden teléfonos inteligentes a precios reducidos, pero con SIM bloqueadas que evitan que los usuarios cambien su servicio de red por cualquier otro servicio de telecomunicaciones.

Con sus socios delictivos en AT&T, Fahd y su co conspirador, Ghulam Jiwani, quien ya falleció, administraron un negocio exitoso donde cobraba millones de dólares a usuarios por desbloquear sus dispositivos, permitiéndoles utilizar una tarjeta SIM de cualquier otro operador, a nivel nacional o internacional.

Fahd también pagó sobornos a los empleados de AT&T por instalar malware en las computadoras internas de la compañía en el centro de llamadas de Bothell, lo que permitió a Fahd recopilar información confidencial y patentada sobre cómo funcionan la red de computadoras y las aplicaciones de software de AT&T.

Aparentemente, utilizando el malware y las credenciales de su conspirador en AT&T, Fahd puso procesar de forma automática las solicitudes de desbloqueo no autorizadas para cualquier teléfono celular desde una ubicación remota.

> *«Después de que AT&T despidió a algunos de los conspiradores, los empleados restantes de los conspiradores ayudaron a Fahd a desarrollar e instalar herramientas adicionales que permitirían a Fahd utilizar las computadoras de AT&T para desbloquear teléfonos celulares desde una ubicación remota. Hasta ahora, tres de esos conspiradores se han declarado culpables al admitir que les pagaron miles de dólares por facilitar el esquema fraudulento de Fahd»,* dijo el Departamento de Justicia.

Después, cuando Fahd no pudo controlar de forma remota su malware, nuevamente sobornó a los empleados de AT&T para que instalen dispositivos de hardware, incluidos puntos de acceso inalámbrico, que lo ayudaron a obtener acceso a la red interna de AT&T y seguir desbloqueando teléfonos remotamente.

En total, Fahd pagó más de 1 millón de dólares en sobornos a los empleados de AT&T, y un empleado recibió 428,500 dólares durante el esquema de cinco años, que reciben en sus cuentas bancarias o cuentas comerciales a nombre de empresas fantasmas creadas para recibir pagos.

El sospechoso contactó a los empleados de AT&T por teléfono, Facebook y otros canales de comunicación e indicó que obtuvieran teléfonos celulares prepagos y cuentas de correo electrónico anónimas para comunicarse con él.

Fahd está acusado por un total de 14 cargos, que incluyen un cargo por cometer fraude electrónico, uno por violar la Ley de Viajes y la Ley de Abuso y Fraude Informático, cuatro cargos de fraude electrónico, dos cargos de acceso a una computadora protegida para fomentar el fraude, dos cargos de daño intencional a una computadora protegida y cuatro cargos de violar la Ley de Viajes.

> *«Este acusado pensó que podría ejecutar su esquema de soborno y piratería de forma segura desde el extranjero, ganando millones de dólares mientras inducía a los jóvenes trabajadores a elegir la avaricia sobre la conducta ética. Ahora será*

> *responsable por el fraude y las vidas que ha descarrilado»*, dijo el abogado Brian T. Moran.