19/09/24

Desarticulada una red criminal internacional dedicada a desbloquear teléfonos móviles sustraídos y a robar la vida digital de las víctimas

Resumen

En el desarrollo de la operación se ha detenido a un total de 17 personas en seis países –España, Argentina, Colombia, Chile, Ecuador y Perú- y se han llevado a cabo 28 registros domiciliarios en los que se han intervenido un total de 921 dispositivos electrónicos –teléfonos móviles, tablets y portátiles

En España han sido arrestadas tres personas vinculadas con la organización criminal -en Móstoles, Leganés y Manresa-, se han llevado tres registros domiciliarios en los que se han intervenido 47 teléfonos móviles, seis tablets y tres ordenadores portátiles y se ha bloqueado el acceso a las páginas web fraudulentas asociadas a la red criminal

La actividad ilícita de la estructura criminal dedicada al Crime as Service, se iniciaba con el robo de terminales telefónicos que desbloqueaban mediante técnicas combinadas y simultáneas de phising, smishing y vishing con las que obtenían de sus víctimas las credenciales de acceso al dispositivo para apoderarse de su vida digital. La plataforma informática que utilizaban se estima que habría desbloqueado 1.300.000 dispositivos telefónicos de alta gama sustraídos

Operación coordinada entre seis países por EUROPOL y AMERIPOL a través del programa EL PACCTO 2.0

Contenido

Agentes de la Guardia Civil y de la Policía Nacional, han participado en una operación internacional coordinada por EUROPOL y AMERIPOL a través del programa EL PACCTO 2.0, en la que se ha desarticulado una estructura criminal internacional dedicada a desbloquear teléfonos móviles de alta gama sustraídos y a robar la vida digital de las víctimas. En el desarrollo de la operación, denominada “KAERB”, se ha detenido a un total de 17 personas en seis países –España, Argentina, Colombia, Chile, Ecuador y Perú- y se han llevado a cabo 28 registros en los que se ha podido intervenir un total de 921 dispositivos electrónicos. En España han sido arrestadas tres personas vinculadas con la organización criminal, se han llevado a cabo tres registros en los que se han intervenido 47 teléfonos móviles, seis tablets, tres ordenadores portátiles y se ha bloqueado el acceso a las páginas web fraudulentas asociadas a la red criminal.

La investigación se inició en España en España en julio de 2022 ante las informaciones recibidas por EUROPOL en las que se indicaba la existencia de una plataforma informática dedicada al desbloqueo ilegal de dispositivos electrónicos de alta gama, principalmente teléfonos móviles y que actuaba principalmente en países de habla hispana.

Un SMS simulando ser del fabricante del teléfono para iniciar el engaño

Las investigaciones de los agentes permitieron detectar la existencia de una organización criminal cuyos líderes, habían creado y comercializado a través de la web, un servicio online que permitía obtener las credenciales de acceso a este tipo de teléfonos. El servicio permitía automatizar la creación de páginas web que simulaban a las de la página web de la empresa comercializadora de teléfonos y enviar un mensaje SMS a los titulares legítimos a los que les habían sustraído el terminal. Para ello habrían utilizado un total de 5.300 páginas web falsas habiendo desbloqueado ilegalmente alrededor de 1.300.000 dispositivos de alta gama, unos 30.000 en España.

Previamente al desbloqueo la organización realizaba un perfilado social de las víctimas, ya que, en muchas ocasiones, además del terminal sustraído, también disponían de los efectos personales de la víctima como la documentación personal y, con esa información y técnicas OSINT obtenían los números de teléfono de las víctimas para enviarles el SMS malicioso (smishing). Además, también se ha detectado que llegaron a realizar llamadas a las víctimas (vishing) a algunas de las víctimas para obtener más información y poder personalizar los mensajes fraudulentos y las páginas web falsas (phising).

Los mensajes automatizados incitaban a acceder a las supuestas páginas del fabricante para obtener información sobre la ubicación del dispositivo sustraído y de esta manera poder recuperarlo. Con la falsa esperanza de recuperar los teléfonos, las víctimas accedían a estas páginas creadas por la red criminal e introducían las claves de desbloqueo, que eran recopiladas por el servidor ilícito y eran proporcionadas a los usuarios que habían adquirido los teléfonos robados.

Agentes españoles desplazados a Argentina

Una vez detectada toda la estructura criminal y su forma de actuar, se estableció un operativo de actuación simultánea en todos los países implicados, estableciendo un Centro de Coordinación en la ciudad argentina de Buenos Aires donde se desplazaron agentes de la Policía Nacional y de la Guardia Civil.

Durante el operativo se ha detenido a un total de 17 personas (tres en España), entre los que se encuentra el líder de la organización criminal arrestado en Argentina. En las 28 entradas y registros se han intervenido 921 (630 de ellos robados) dispositivos electrónicos, 56 de ellos en los tres registros llevados a cabo en España. Además de los dispositivos electrónicos, durante los registros se han intervenido tres vehículos, dos armas de fuego, 6.500 euros en efectivo, numeroso material informático relacionado con la actividad criminal, dos armas de fuego, un dron, criptoactivos y pastillas de MDMA.

La operación ha permitido desactivar el servicio que proporcionaba la plataforma a nivel internacional y ha sido desmantelada mediante el apagado de los servidores digitales, redireccionando el tráfico online que recibía a un dominio controlado por la Policía Nacional.

La investigación ha permitido desentraña esta estructura criminal que combinaba hechos delictivos cometidos en el mundo material y en el mundo del ciberespacio, configurando un complejo entramado criminal. En la cúspide se encontraba un ciudadano argentino, el administrador de la plataforma iServer, residente en la Provincia de Santa Fe, Argentina. Proveía la venta y el soporte de la plataforma a otros cibercriminales, conocidos como desbloqueadores, estos se encargaban de ofrecer servicios fraudulentos a través de la plataforma, facilitando el desbloqueo de dispositivos móviles robados o perdidos a terceros.

Casi medio millón de víctimas

La plataforma iServer fue identificada como un punto central en esta red criminal, operando bajo diferentes dominios y utilizando métodos de pago anónimos. La red criminal opera desde hace al menos 5 años, tiene más de 2.000 usuarios registrados y se estima que las víctimas alcanzan la cifra de 483.000 usuarios (Chile 77.000, Colombia 70.000, Ecuador 42.000, Perú 41.500, España 30.000, Argentina 29.000, otros 193.500).

La operación ha sido posible gracias a la cooperación policial y judicial internacional, llevada a cabo durante dos años, siendo la primera investigación donde han intervenido EUROPOL, AMERIPOL, y EL PACCTO 2.0 junto los cuerpos policiales, fiscales y judiciales de España, Argentina, Ecuador, Perú, y Colombia. De igual forma han participado la Fiscalía Española de Coordinación de la Ciberdelincuencia y la Consejería de Interior en Argentina.

Las autoridades continúan trabajando para rastrear y recuperar los dispositivos móviles robados y adquiridos ilegalmente, y no se descartan nuevas detenciones de los implicados en la red criminal internacional.

Imágenes


POLICIA NACIONAL
GUARDIA CIVIL
Mº INTERIOR


POLICIA NACIONAL
GUARDIA CIVIL
Mº INTERIOR
GUARDIA CIVIL
UCO
POLICIA NACIONAL


POLICIA NACIONAL
GUARDIA CIVIL
Mº INTERIOR
GUARDIA CIVIL
UCO