

SOCIEDAD

Una estafa a números de móvil afectó a un millón de usuarios

La red desarticulada recaudó 30 millones de euros con llamadas automáticas y mensajes premium

AGENCIAS
MADRID

■ ■ ■ Más de tres años de investigación han permitido a la Guardia Civil destapar una estafa de al menos 30 millones de euros a un millón de usuarios de telefonía móvil a través de aplicaciones que realizaban llamadas automáticas a números de tarificación adicional o enviaban mensajes premium.

Siete detenidos y once registros ha sido el resultado de la Operación Rikati, que ayer explicaba en rueda de prensa el teniente coronel Juan Sotomayor, jefe del departamento de Delitos Telemáticos de la Unidad Central Operativa (UCO) de la Guardia Civil.

Una investigación que comenzó cuando las operadoras de telefonía en España se percataron de la existencia de un tráfico de llamadas a números de tarificación adicional poco habitual en un tramo horario concreto. Se trataba de llamadas automáticas que los teléfonos realizaban por la noche sin que el usuario se percatara y que se hacían a través de una aplicación aparentemente normal que lograba apagar el teléfono y quitarle el sonido mientras efectuaba la llamada, con un máximo de tiempo de media hora.

El teniente coronel resaltó el alto volumen de los mensajes y dijo que con solo 20 números de suscripción, generaron más de 21 millones de SMS Premium. Recordó que al usuario que recibía uno de estos mensajes se le cobraba un importe cercano a los 1,5 euros por cada uno, y como la media recibida era de entre 20 y 25, el fraude o la estafa al usuario era de unos 30 euros al mes. Como esa cifra no era muy elevada, los perjudicados no solían denunciar.

EMPRESAS PANTALLA

Al parecer, la organización, que llevaba operando desde 2013 y generó un perjuicio cercano a los 30 millones de euros, se encontraba ubicada en Cataluña y utilizaba a su vez un entramado societario de empresas pantalla para cometer el fraude, cuyas sedes se situaban en varias, Andorra, Luxemburgo y Hong Kong.

En el transcurso de la operación practicaron once registros, donde la Guardia Civil intervino cerca de 1.000 aplicaciones en distintas



Imagen de los miembros de la UCO de la Guardia Civil durante la operación.

ENGANCHABAN A LOS USUARIOS CON PÁGINAS DE NOMBRES ATRACTIVOS

Para que los usuarios se descargaran las aplicaciones maliciosas, la trama descubierta, que operaba a través de empresas legales y otras pantalla, utilizaban el nombre y los logos de otras muy conocidas o engancharon al usuario con nombres como "la linterna molona", los "mejores trucos para evitar la calvicie" o los mejores vídeos pornos. Y no solo eso, sino que, además, las anunciaban como gratuitas en redes sociales y páginas web y si en alguna ocasión informaban del coste, era muy complicado

para el usuario verlo, según los responsables de la investigación. El teniente coronel de la Guardia Civil Juan Sotomayor reiteró que, sobre todo, había dos tipos de aplicaciones fraudulentas: las que llamaban en modo silencioso número de líneas 803X y las que enviaban SMS a líneas de mensajería Premium. Ante cualquier queja o sospecha, la organización, liderada desde Barcelona, desactivaba esas aplicaciones o las eliminaba. Los detenidos tenían la capacidad de variar los contenidos que mostraban las aplicaciones de forma remota, lo que permitía, entre otras funcionalidades,

engañar a las operadoras y reguladores del sector, haciéndoles creer que se trataba de aplicaciones diferentes. Para asegurarse la continuidad delictiva explotaban gran cantidad de números cortos de SMS "Premium" y números de tarificación adicional, cedidos por un operador de telecomunicaciones establecido en Barcelona que resultó ser uno de los máximos responsables de los hechos investigados, facilitando, consintiendo e incluso ocultando su uso real a los organismos que controlan estos servicios, asegura el instituto armado.

fases de desarrollo, ya que los autores iban introduciendo modificaciones para perfeccionar más las técnicas de engaño.

Igualmente, los investigadores se incautaron en los centros de operaciones ubicados en Sant Cugat y Mollet del Vallés, ambas localidades de Barcelona, y en Santa Cruz de Tenerife datos de usuarios

estafados, aplicaciones móviles y vehículos de alta gama, en tanto que a la red les fue inmovilizado un patrimonio por valor de varios millones de euros.

La UCO estima que un millón de usuarios habían podido ser estafados durante este tiempo y creó una web donde se podrá comprobar, introduciendo el número de

teléfono, si se ha sido víctima del fraude. Puede hacerlo en la página <http://www.gdt.guardiacivil.es/webgdt/inforikati.php>

La operación continúa abierta y no descartan nuevas detenciones en una investigación, considerada como una de las más importantes en España contra el fraude masivo en el uso de la telefonía móvil. ■

Barcelona estrena el tercer computador más grande de Europa

AGENCIAS
BARCELONA

■ ■ ■ El Barcelona Supercomputing Center-Centro Nacional de Supercomputación (BSC-CNS) estrenó ayer el "MareNostrum 4", el tercer supercomputador más rápido de Europa y el decimotercero del mundo, multiplicando su potencia por diez en relación al "MareNostrum 3".

Según el director del BSC, Mateo Valero, el "MareNostrum 4" tiene una capacidad de 11,1 pentafllops, es decir, puede realizar 11.100 billones de operaciones por segundo, "esto significa que el MareNostrum 4 hará en un día, lo que el primer MareNostrum, de 2004, hacía en un año", ha ejemplificado el director.

Los superordenadores sirven a los científicos e ingenieros para la investigación básica y aplicada por su capacidad de realizar grandes cálculos, ejecutar grandes simulaciones complejas y analizar un gran

EL "MARENOSTRUM 4" TIENE UNA CAPACIDAD DE 11,1 PENTAFLOPS, PUEDE REALIZAR 11.100 BILLONES DE OPERACIONES POR SEGUNDO

volumen de datos, por lo que se utilizan en prácticamente todas las disciplinas, desde la astrofísica, pasando por la biomedicina hasta la industria.

La secretaria de Estado de Investigación, Desarrollo e Innovación, Carmen Vela, detalló que esta renovación del supercomputador supone una inversión estatal de 34 millones de euros, y aseguró que es "un dinero bien invertido" ya que genera "rendimiento y crea relaciones internacionales".

Este nuevo equipamiento estará formado por cuatro máquinas, aunque actualmente solo hay una en funcionamiento, la fabricada por Lenovo, pero las otras tres empresas adjudicatarias del supercomputador, IBM, Intel y Fujitsu, ya están terminando de construir el resto. "Un comité externo evalúa los proyectos de los investigadores cada cuatro meses, y si resultan seleccionados, pueden utilizar las instalaciones sin ningún coste", ha explicado Mateo Valero. ■