

Desarticulado un grupo de hackers que habían obtenido datos bancarios de más de 20.000 personas a través de Internet

En la operación SILURO han sido detenidas 6 personas que disponían en sus sistemas informáticos de más de 200.000 direcciones de correo electrónico para ser utilizadas en sus campañas de phishing.

Se han intervenido más de 500 tarjetas de crédito falsificadas y abundante documentación también falsificada de diversos países de la Unión Europea.

El grupo disponía de diversas páginas web para la recarga de tarjetas prepago de telefonía, a mitad de precio, que utilizaban para capturar los datos bancarios de las personas que recargaban sus tarjetas.

La Guardia Civil, en la denominada operación SILURO, llevada a cabo en Navarra y Málaga, ha detenido a 6 personas de nacionalidad marroquí, integrantes de un grupo de hackers informáticos dedicados al fraude en la banca electrónica, que habían obtenido datos bancarios de más de 20.000 personas.

La operación se inició hace un año, cuando una persona denunció ante la Guardia Civil que le habían sustraído la totalidad del dinero existente en su cuenta bancaria mediante transferencias no autorizadas.

Tras las primeras investigaciones, la Guardia Civil detectó en Internet un gran número de campañas de phishing, consistentes en el envío masivo de correos electrónicos, suplantando la identidad de varias entidades bancarias nacionales.

Estas campañas se llevaban a cabo utilizando patrones comunes y presentaban una apariencia idéntica, por lo que se tuvo la sospecha de que podrían haber sido realizadas por una misma persona.

Posteriores investigaciones condujeron hasta el cerebro del grupo, que se encargaba de diseñar páginas web casi idénticas a las de determinadas entidades bancarias, con el fin de conseguir que los destinatarios de sus correos accedieran a estas páginas y de esta forma obtener sus datos personales y bancarios.

Una vez localizados todos los integrantes del grupo, fueron detenidos en Fuengirola (Málaga): M.E.A., de 19 años de edad y cerebro de la red; M.I., de 27; M.E.M., de 28; A.R., de 30; y A.N., de 30, todos ellos de nacionalidad marroquí; y C.N.M.R., de 21 años, natural de Ceuta y vecina de Fuengirola.

Modus Operandi

Para disponer de anonimato en sus acciones, establecían las conexiones desde ordenadores hackeados o a través de conexiones inalámbricas (wifi) abiertas, mediante la técnica conocida como wardriving, consistente en el acceso a las redes inalámbricas de su entorno, vulnerando su

seguridad y accediendo a su configuración para utilizarlos como puntos de envío del phishing.

De esta manera se conseguía desviar la investigación hacia conexiones de otros usuarios que desconocían el uso fraudulento que se estaba haciendo de sus conexiones a Internet.

Paralela a esta actividad delictiva, accedían ilegalmente a sistemas informáticos de empresas, vulnerando la seguridad y accediendo a sus bases de datos, para robar información personal y económica de los clientes de las mismas.

En los sistemas informáticos intervenidos ya se han localizado informaciones personales y bancarias de más de 20.000 personas y además disponían de más de 200.000 direcciones de correo electrónico de ciudadanos españoles que eran utilizados para realizar las distintas campañas de phishing.

En su poder también se han intervenido documentaciones falsificadas de diversos países de la Unión Europea y más de 500 tarjetas de crédito falsificadas, lectores de tarjeta, grabadores, varios sistemas informáticos un distorsionador de frecuencias para dificultar el seguimiento de sus comunicaciones y un vehículo sustraído.

Fraude en recargas de tarjetas telefónicas

Los detenidos disponían también de diversas páginas web para la recarga de tarjetas prepago de telefonía, a mitad de precio, que utilizaban igualmente para capturar los datos bancarios de las personas que recargaban sus tarjetas. Estos datos eran utilizados en ocasiones para realizar compras fraudulentas a través de la red.

Estas recargas eran válidas tanto en la zona de cobertura de telefonía española del norte de Marruecos, como en España y otros países de la Unión Europea.

Para blanquear el dinero sustraído a través del phishing y evitar la localización de los ordenadores desde los que operaban, empleaban el denominado sistema de utilización de mulas, consistente en la transferencia de las cantidades obtenidas a otra cuenta bancaria que era ofrecida por una tercera persona (mula), a cambio de un porcentaje de la cantidad transferida.

Hasta el momento no se han cuantificado las cantidades totales del fraude cometido, aunque se estima que es considerablemente elevado por la multitud de datos recabados referentes a clientes de entidades bancarias.

Las páginas web falsas de recargas telefónicas, que han sido inhabilitadas, son:

- www.recargas-express.com
- www.recargas-epagado.com
- www.tele2-mobile.net
- www.recargas-terra.com
- www.recarga-facil.net
- www.recargas-4b.com
- www.recargas-red.com

- www.recarga-web.com
- www.rrecarga-prepago.com
- www.recarga-facil.com

Las investigaciones han sido llevadas conjuntamente por efectivos del Equipo de Investigación Tecnológica (EDITE) de la Guardia Civil de Navarra y del Grupo de Delitos telemáticos (GDT) de la Unidad Central Operativa de la Guardia Civil, bajo la dirección del Juzgado de Instrucción núm. 1 de Pamplona.

Consejos de seguridad

La adopción de las medidas que a continuación se exponen no garantiza la seguridad de nuestros sistemas pero pueden reducir significativamente la proliferación de este tipo de estafas:

- No abra mensajes de correo electrónico no solicitados o de procedencia desconocida. Elimínelos directamente sin previsualizarlos.
- Cuando navegue por Internet, busque páginas de confianza, a ser posible, avalados por sellos o certificados de calidad, evitando contenidos dudosos. Su exigencia de calidad ayudará a hacer una Internet más segura.
- Utilice siempre software legal. Evite las descargas de programas de lugares no seguros de Internet.
- Si recibe mensajes que piden el reenvío a sus conocidos, informando de noticias llamativas o apelando a motivos filantrópicos, desconfíe por sistema. Muchos de ellos buscan captar direcciones de correo electrónico para prospectivas comerciales, y son un engaño (hoax).
- Desconfíe de los mensajes de correo procedentes de supuestas entidades bancarias. Confirme vía telefónica, en su sucursal bancaria, cualquier petición que reciba de datos de banca electrónica.

Fuente: Guardia Civil

Nota: La mayoría de estas web fraudulentas fueron denunciadas por la Comisión de Seguridad de Asociación de Internautas.

Ejemplos de webs de recargas descubierta y denunciada por la AI;

<http://www.autorecargas.com>
<http://www.tele2-mobile.net>
<http://www.recargas-terra.com>
<http://www.recargateloahora.com>
<http://www.recarga-facil.net>
<http://www.recargas-4b.com>
www.recargas-red.com
www.recarga-web.com
<http://www.hifiwebhosting.com/vodafone/>
www.recargas-express.com
www.recargatusaldo.com
www.recarga-prepago.com

Fecha artículo: 2006-12-21 15:21:12 - url artículo: <http://www.internautas.org/html/998.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org