Publicado en el 30/12/2013

# Cae la rama española de una red de hackers responsable de extraer más de 60 millones de dólares en cajeros de todo el mundo

**Una operación conjunta de la Policía Nacional española y una agencia de seguridad estadounidense ha permitido desmantelar la rama española de una red de hackers responsable de extraer más de 60 millones de dólares en cajeros de todo el mundo.**

Esta red actuó el pasado febrero de forma simultánea en 23 países y en pocas horas se hicieron con 40 millones de dólares en 34.000 retiradas de efectivo. 446 de esas disposiciones de efectivo se realizaron en una sola noche en cajeros de Madrid, donde la rama española de la organización obtuvo cerca de 400.000 dólares. Los ocho detenidos en Madrid seguían precisas instrucciones del líder de la red, un experto informático arrestado en Alemania capaz de vulnerar las bases de datos de entidades bancarias para inhabilitar todas las medidas de seguridad y restricciones sobre el uso de tarjetas.

La estructura de esta red mundial nacía de una sola persona, quien definía las relaciones a mantener por el resto de miembros y el momento concreto en el que activarlos para obtener la mayor cantidad de efectivo en el menor tiempo posible. Este líder era capaz de atacar las bases de datos de compañías procesadoras de los datos de tarjetas de crédito de las entidades bancarias para robar información altamente sensible. Cuando lograba comprometer el sistema, tenía acceso a inhabilitar todas las medidas de seguridad, incluyendo restricciones de velocidad, restricciones geográficas, restricciones de balance (permitiendo realizar transacciones con balances negativos) y hasta restricciones del PIN (permitiendo a los autores incorporar cualquier PIN).

Para llevar a la práctica la estafa, el cerebro de la red comunicaba determinadas numeraciones de tarjetas bancarias a personas de su confianza repartidas por todo el mundo. Los líderes de cada célula copiaban estas numeraciones en tarjetas blancas dotadas de bandas magnéticas y las distribuían entre su red de colaboradores. En el momento exacto en el que el líder eliminaba los límites de retirada y restricciones geográficas de estas tarjetas comenzaba una operación coordinada a escala mundial para extraer en cajeros automáticos y de forma simultánea la mayor cantidad de efectivo disponible. El citado líder controlaba toda la operación y monitorizaba la cantidad exacta que había sacado cada célula, de forma que en caso de intentar engañarle, éste podía precisar la hora, fecha, lugar y cantidad que habían extraído.

60 millones de euros

Estados Unidos investigaba desde el año 2007 las actividades ilícitas de una compleja organización involucrada de forma regular en actividades de extracción de efectivo en cajeros automáticos. Entre las transacciones se incluían operaciones ilimitadas en las cuales los investigados pudieron manipular los balances, límites de retirada y controles de las bases de datos de varias tarjetas de débito de prepago asociadas a diversas entidades bancarias.

La información que obtuvieron señalaba las fechas en las que componentes de la organización investigada habían actuado en España. Para ello utilizaron en diversos cajeros automáticos de varias entidades bancarias localizadas en Madrid numeraciones de tarjetas procedentes en su mayoría de Estados Unidos.

A finales de 2012 los investigadores identificaron el ataque coordinado a las bases de datos de una compañía de procesamiento de pagos ubicadas en India. Esta intrusión permitió a los miembros de este entramado realizar los días 22 y 24 de diciembre extracciones que superaron los 7.000.000 de dólares USA, en cuentas de dos entidades financieras. Pocos días más tarde, en un nuevo ataque a otra compañía procesadora de tarjetas de crédito situada en Florida, inhabilitaron todas las medidas de seguridad de la base de datos de tarjetas prepago, incluyendo restricciones geográficas o de PIN.

Con estos cambios, los cerebros de la organización distribuyeron aproximadamente 20 cuentas a las distintas a células de la organización ubicadas en aproximadamente 16 países. Los miembros de las células grabaron esta información en tarjetas con banda magnética y comenzaron a realizar las extracciones de forma masiva y simultánea cuando les fue dada la orden. En total realizaron 9.300 transacciones fraudulentas en algo más de 15 horas con las que obtuvieron unos beneficios ilícitos de más de 9.000.000 de dólares USA.

Del total de operaciones realizadas en estos tres días por la trama investigada, se identificaron en España 200 extracciones fraudulentas en cajeros automáticos de las provincias de Madrid, Málaga y Barcelona con las que obtuvieron cerca de 68.000 euros.

En febrero de 2013, ejecutaron un nuevo ataque masivo y coordinado en cajeros automáticos de 23 países, entre los que se encontraba España. Durante aproximadamente 13 horas retiraron más de 39 millones de dólares americanos en más de 34.000 operaciones ilícitas. Solo en nuestro país se realizaron 446 disposiciones en cerca de siete horas, siempre de madrugada, por un importe total que superaba los 390.000 dólares –alrededor de 285.000 euros-. Algunos de los cajeros utilizados ahora coinciden con los empleados en el ataque de finales de 2012, lo que apuntaba a que los autores podrían ser los mismos, y que permitió además ser identificados por la Policía Nacional.

Ocho detenidos en España

Las investigaciones desarrolladas en EEUU permitieron la identificación y posterior desarticulación a primeros de mayo de la célula encargada de realizar las operaciones en la ciudad de Nueva York, compuesta por ocho individuos. Siete de ellos fueron detenidos y el octavo, supuesto líder de la célula, habría sido asesinado en República Dominicana el pasado 27 de abril.

Por su parte, los investigadores españoles lograron identificar a las personas que formarían la célula de la organización asentada en España. Una de las personas identificadas, que contaba con antecedentes por el uso fraudulento de tarjetas desde que era menor, se había convertido una vez alcanzada la mayoría de edad en el cerebro del grupo de la organización residente en España. Ocho personas fueron finalmente detenidas, seis de nacionalidad rumana y dos naturales de Marruecos, en

las localidades madrileñas de Mejorada del Campo y Fuenlabrada. Además se practicaron tres registros domiciliarios en los que se han intervenido 25.000 euros en efectivo, dos lectores grabadores de tarjetas de crédito, alrededor de 1.000 tarjetas vírgenes con banda magnética, material informático, y gran cantidad de joyas y documentación pendiente de análisis. Igualmente se han bloqueado dos inmuebles valorados en más de 500.000 euros.

La operación policial se precipitó a raíz de la detención en Alemania del hacker, donde había viajado desde su lugar de residencia habitual, en compañía de otro ciudadano rumano con antecedentes en España e identificado como el principal responsable de un ataque realizado en Rumanía en noviembre con el que consiguieron más de 3,5 millones de dólares. Con esta operación se ha conseguido desarticular la mayor parte de la organización asentada en España cuando estaba empezando a reorganizarse para realizar un ataque similar a los anteriores por diversos países de la Unión Europea e, incluso, en Japón.

En la operación han participado agentes de la Sección de Medios de Pago de la UDEF Central de la Comisaría General de Policía Judicial y del Grupo XX de la Brigada Provincial de Policía Judicial de Madrid, con el apoyo de la Unidad de Investigación Tecnológica de la Policía Nacional, con la colaboración de una agencia de seguridad americana.

NOTA: Los medios de comunicación que lo deseen podrán obtener imágenes en el siguiente enlace: http://prensa.policia.es/carpatos.rar

**Datos de contacto:**
Ministerio del Interior

Nota de prensa publicada en:

Categorías: Nacional Ciberseguridad