FASCÍCULO DOCTRINAL No. 13

Intercambio de experiencias y conocimiento de los delitos transnacionales

CIBERCRIMEN

FASCÍCULO DOCTRINAL No. 13

Intercambio de experiencias y conocimientos de los delitos transnacionales

C I B E R C R I M E N

"INTEGRACIÓN PARA LA PROTECCIÓN Y SEGURIDAD CIUDADANA"

Fascículos Doctrinales

Intercambio de experiencias y conocimientos de los delitos transnacionales

Maestro
Enrique Francisco Galindo Ceballos
Comisionado General de la Policía Federal de México
Presidente de AMERIPOL

General Superior de Policía
Diego Alejandro Mejía Valencia
Comandante General de la Policía Nacional del Ecuador
Secretaria Ejecutiva de AMERIPOL

Agradecimientos:

Policía Federal de Brasil
Policía Nacional de Colombia
Policía Nacional de Ecuador
Cuerpo Nacional de Policía de España
Guardia Civil de España
Policía Nacional Civil de Guatemala
Policía Nacional de Honduras
Policía Nacional de la República Dominicana

Secretaría Ejecutiva de AMERIPOL
Avenida 39 No. 8-60 Bogotá – Colombia
Tel. (57) (1) 3159230
Correo electrónico: secretaria-privada@comunidad-ameripol.org

Contenido


AMERIPO
COMU DAD DE


POLICIAS E AMERICA

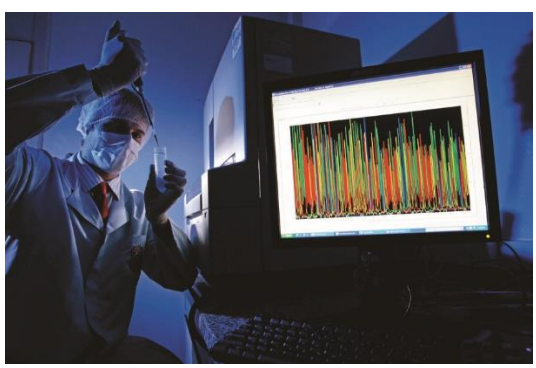
ALESSANDRO GONÇALVES DIAS
Sector de Tecnología de la Información (STI)
alessandro.agd@dpf.gov.br
Policía Federal de Brasil

SISTEMA NACIONAL DE GESTIÓN DE ACTIVIDAD CRIMINAL (SISCRIM)

El Sistema Nacional de Gestión de Actividad Criminal (SISCRIM) es un sistema informático que permite la integración de la información de toda la experiencia de las unidades, y el control efectivo de documentos y materiales enviados para ser periciados. Es una característica ampliamente utilizado y mejorado continuamente. Facilita la supervisión y realización de trabajos de expertos.

Cual finalidad de las tareas poniendo en práctica esta experiencia

El SISCRIM es un sistema computarizado para fines de controlar a nivel nacional, la tramitación de expedientes y materiales de examen, así como otras actividades afines a la Criminalística.



Contexto de la Experiencia

Los factores determinantes para el éxito del proyecto fue el apoyo del Director Técnico - Científico y la dedicación de los expertos, que desarrollarán y mantiene el sistema.

Medios Utilizados

Los recursos humanos, físicos y financieros son de la propia institución.

Resultados Obtenidos

La implementación del SISCRIM mejoró el control y la ejecución de los trabajos de expertos en las áreas de gestión, administrativas y técnicas, en las unidades centrales y descentralizadas. El SICRIM facilitó el control de la cadena de custodia de documentos y materiales en la experiencia, así como para mejorar la gestión de las personas y la información.

ÉLVIO DIAS BOTELHO
Servicio de Pericias de Laboratorio (SEPLAB)
elvio.edb@dpf.gov.br

KÁTIA MICHELIN
Área de Pericias en Genética Forense (APGEF)
katia.km@dpf.gov.br
Policía Federal de Brasil

ACREDITACIÓN DE LABORATORIOS

Los laboratorios químicos y de ADN del Instituto Nacional de Criminología (INC), con sede en Brasilia, participaron en un proceso de acreditación internacional. El certificado de acreditación prevé el reconocimiento mutuo de los exámenes entre los laboratorios nacionales e internacionales acreditados.

Cual la finalidad de las tareas Poniendo en práctica esta experiencia

El objetivo de la acreditación de laboratorios de ciencias forenses y ADN es garantizar la excelencia de los resultados técnicos y el desarrollo científico del Instituto Nacional de Criminología, que busca satisfacer las nuevas demandas, debido a los crecientes niveles de conocimiento y experiencia requeridos en la evaluación de los rastros de procedimientos pre - procesales y judiciales del ámbito penal. Otro objetivo es satisfacer las necesidades de las partes implicadas, como resultado de la modernización de las garantías en las etapas de investigación y de procedimiento.

Contexto de la Experiencia

El certificado fue entregado por el ANSI - ASQ (National Accreditation Board / FQS Forensic Accreditation), un organismo internacional que certifica la calidad de los análisis realizados en los laboratorios forenses. Los Laboratorios de Genética Forense y Química INC son los primeros laboratorios forenses en el país acreditado según la norma ISO / IEC 17025:2005, y fueron los primeros laboratorios forenses en América Latina acreditados por organismos de acreditación internacional.

Medios Utilizados

Los recursos humanos, físicos y financieros son de la propia institución.

Resultados Obtenidos

La obtención del certificado de acreditación del cumplimiento de la norma ISO / IEC 17025:2005 define los requisitos para la gestión de calidad en los laboratorios analíticos.

Agente de Polícia Federal **ERIK PEREIRA DE SIQUEIRA**
Jefe del Servicio de Represion al Crimen Cibernetico
Especialista en Gestión de Seguridad de la Información
Policía Federal de Brasil

ESTRATEGIAS POLICÍAL PARA LA OBTENCIÓN DE PRUEBAS EN EL DELITO CIBERNÉTICO UN CASO REAL DESARROLLADO EN LA OPERACIÓN DARKODE [1] - POLICÍA FEDERAL DE BRASIL Y EL FBI

Una de las acciones más comunes de los Ciberdelincuentes en fraude bancario por Internet es la transferencia de los valores para las cuentas de receptores, es decir, el estafador obtiene mediante diversas técnicas de suplantación de identidad (phishing, Rat´s[2], etc) las credenciales de acceso de cliente víctima y realiza transferencias a cuentas de terceros (naranjas[3]), participantes en el esquema criminal que realizan el saque en cajeros automáticos.

A partir de la experiencia de investigación obtenida en diversas operaciones policiales, se observó que en muchos casos los responsables de las transferencias fraudulentas con el fin de comprobar si ocurrió la retirada por parte del receptor (naranja), acceda a la cuenta de destino en Internet para comprobar el saldo, se trata de una medida adoptada por uno de los miembros del grupo criminal para asegúrese de que el "naranja" hizo el saque para después hacer la solicitud el importe de la prestación económica previamente acordado entre ellos. De este modo, el operador de transporte fraudulento quiere evitar que el "naranja" lo engañe, diciendo que no pudo lograr la retirada fraudulenta.

En la parte represiva, tradicionalmente, la policía centró medidas de investigación en los registros de transacciones fraudulentas registradas en la cuenta de la víctima y en el rastreo del dinero transferido, el conocido “follow the Money”. Esta estrategia generalmente no obtener llegar a los niveles jerárquicamente superiores de los defraudadores, sólo en los beneficiarios de las transacciones fraudulentas.

En este sentido, con el fin de mejorar el trabajo realizado, la Policía Federal buscó estrategias para avanzar en las actividades de investigación, tales como la creación del proyecto “Tentáculos4”, base nacional de fraude de banca electrónica modelado para correlacionar eventos criminales tratando de identificar los principales grupos criminales. Así, la presente investigación no sólo se basa en el objetivo de identificar los destinos de las transacciones financieras fraudulentas y en los logs IP de cuentas de las víctimas de fraude, sino también en otros datos obtenidos de las instituciones bancarias, proveedores de acceso y otras instituciones privadas.

Los bancos brasileños utilizan como medio de prevención la identificación de dispositivos de clientes de computación en el acceso a la banca por Internet. Este mecanismo es una aplicación de software instalado en el equipo del cliente del banco y se utiliza para identificar de forma única las computadoras, teléfonos móviles, etc., utilizados en el canal internet banking, es decir, se trata de una medida preventiva tomada por los bancos para evitar transacciones bancarias a través de Internet por computadoras no registradas por sus clientes.

Así que cuando un cliente desea utilizar el servicio de banca por Internet, es necesario el registro y la identificación del equipo autorizado para acceder a lo que se

requiere. En esta identificación, el software genera un identificador único (ID) al dispositivo del cliente que se verifica por los sistemas de prevención de banco en el momento de acceso a la cuenta. Todo este proceso es transparente para el titular de la cuenta, es decir, se realiza automáticamente por el banco a través de la instalación de software en el lado del cliente.

Con el uso de dicha identificación los bancos brasileños alcanzaron reducir en gran medida la cantidad de víctimas de fraude por el canal de banca por Internet. Los defraudadores entonces comenzaron a adoptar otros métodos para llevar a cabo el fraude a través de Internet, sea mediante la clonación del identificador de dispositivo de computación y / o el uso de técnicas de acceso remoto a través de Ratps (Remote Access Trojan) para eludir la prevención de los bancos, es decir, con el uso de estas técnicas en los registros de los servidores web de los bancos, que siempre se registran las direcciones IP y el identificador de dispositivo (ID) de las víctimas de fraude, lo cual evita este mecanismo para prevenir y obstaculizar la acción de investigación realizado por las fuerzas de la ley como evidencia encontrados, registros de IP criminales y los ID de dispositivo son de las propias víctimas, dejando sólo rastrear el destino de las transferencias fraudulentas.

OPERACIÓN DARKODE

A principios de 2015, el FBI envió a la Policía Federal de Brasil, los informes sobre agentes usuarios brasileños de foro Hacking International Darkode. A través de los registros de Internet enviados por el FBI, la Policía Federal llegó al abonado de la conexión.

Después de comprobar la conexión del abonado, la Policía Federal no tenía todavía evidencia en contra de la investigación, pero sabía el mismo, estaba operando fraude bancario en Internet basada en informaciones obtenidas en otros procedimientos.

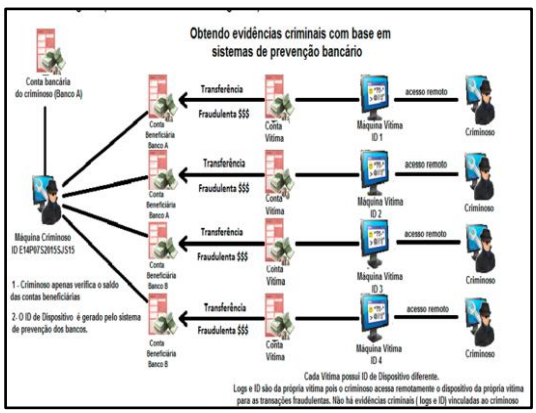
A través de investigaciones de campo, el equipo de la Policía Federal identificó que el sospechoso tenía cuenta en el Banco A. Se adoptó, a continuación, una estrategia de investigación basada en la percepción de que el criminal podría utilizar el mismo equipo que se utiliza para acceder a su cuenta bancaria personal para acceder a otras cuentas sin la preocupación y el cuidado que utiliza al hacer transferencias fraudulentas, ya que su objetivo es sólo para comprobar saldos de las cuentas de beneficiarios (naranjas) para asegurarse de que el otro miembro de la banda hizo la transferencia del valor.

En este sentido, la Policía Federal solicitó al Banco A, posibles evidencias de fraude o transacciones fraudulentas relacionadas a la cuenta personal del investigado. El Banco “A”, dijo que el identificador de dispositivo E14P07S2015SJS15 generado por el software de seguridad del banco, relacionado con la cuenta del investigado, también se ha utilizado en otras 02 cuentas bancarias que recibieron transferencias fraudulentas a través de Internet, lo que confirma la percepción obtenida por el equipo investigación.

Sobre la base de esta información, la Policía Federal, pidió a los otros bancos brasileños, que utilizan el mismo sistema de dispositivos de identificación, para indicar si el ID de dispositivo E14P07S2015SJS15 5 estaba relacionado con otros tipos de fraude bancario en Internet.

Por lo tanto, la Policía Federal, obtuvo con el Banco “B”, que el dispositivo de identificación E14P07S2015SJS15 utilizado para acceder a cuenta personal del

investigado 6, también había sido utilizado para acceder a las otras dos cuentas bancarias, 02 también beneficiarias de las transferencias fraudulentas a través de Internet. Así evidencia criminal se recogió en 04 cuentas de beneficiarios, ahora con materialidad necesaria para el enjuiciamiento del sospechoso (como se muestra en la Figura 1).



Enfoque tradicional de investigación, en fraude de Internet, se basa en la información proporcionada por los bancos relacionados con las víctimas de fraude (registros de acceso, etc.) y el camino del efectivo transferido, pero a menudo limita la persecución a uno solo de los miembros del esquema criminal, es decir, el propio beneficiario que presta su cuenta para recibir a la ventaja financiera indebida. Sin embargo, con el avance de las técnicas utilizadas por los estafadores (acceso remoto a las cuentas de las víctimas de fraude), datos sobre el uso de las cuentas de los beneficiarios (naranjas) transacciones fraudulentas vuelven fundamentales para la obtención de evidencia criminal contra otros miembros de la organización criminal.

Desde la operación Darkode, en conjunto con el FBI, la Policía Federal ha trabajado no sólo en la obtención de datos relativos a las cuentas de las víctimas, sino también las cuentas del beneficiario como un elemento clave en la obtención de pruebas en materia penal. Así que esta información ya está incluido en la base de datos del Proyecto Tentáculos que ya tiene información de cientos de miles de fraude bancario en Internet.

Como se muestra, los mecanismos de prevención bancarias, específicamente utilizado por los bancos brasileños, que identifican el dispositivo de usuario para tener acceso a las cuentas bancarias a través de Internet, también pueden ser utilizados en actividades represivas por parte del organismo de aplicación de la ley, ya menudo el único elemento de materialidad utilizado por la acusación.

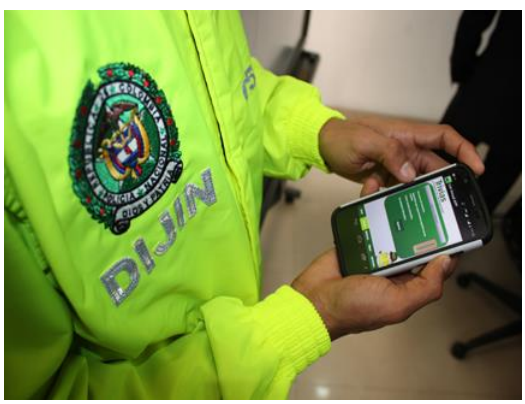
1. A operação Darkode, nome utilizado pela Policía Federal, foi uma ação em cooperação internacional com o FBI e EUROPOL deflagrada em 14/07/2015 simultâneamente em mais de 20 países, para combater os usuários do fórum criminoso darkode.com < http://noticias.terra.com.br/brasil/policia/pf-deflagra-operacao-com- o-fbi- contra-crimes-ciberneticos, bbc4678c8db59cae8aaa3b5d570e153forslRCRD.html> - acesso em 28/04/2016.
2. Os (RATs) são programas maliciosos que são executados de forma invisível em PCs e permite ao invasor acesso e controle remoto. Em um nível básico, muitos RATs imitam a funcionalidade de programas de controle remoto legítimos (Definição em https://technet.microsoft.com/en-us/library/dd632947.aspx - tradução livre).
3. Os beneficiários de transações fraudulentas são conhecidos como "laranjas" no jargão policial brasileiro.
4. SIQUEIRA, Erik Pereira de. O projeto Tentáculos da Polícia Federal: Da concepção à proposta de modelo aplicável na Segurança Pública Brasileira. UnB 2014.
5. Identificação única gerada por software instalado no computador do cliente bancário (número fictício alterado para manter o sigilo dos dados reais da operação).
6. Esta evidência criminal foi a utilizada na acusação inicial do criminoso que foi sentenciado em 20/04/2016 à 07 anos e meio de prisão.

Teniente Coronel **FREDY BAUTISTA GARCÍA**
Jefe del Centro Cibernetico Policial
Direccion de Investigacion Criminal e INTERPOL
Policía Nacional de Colombia

ESFUERZOS EN CIBERSEGURIDAD CONTRA EL CIBERCRIMEN: POLICIA NACIONAL DE COLOMBIA CENTRO CIBERNÉTICO POLICIAL

El Centro Cibernético Policial, es la dependencia de la Dirección de Investigación Criminal e INTERPOL, responsable de liderar los esfuerzos institucionales para enfrentar la amenaza del Cibercrimen y Ciberterrorismo en Colombia.

A partir de la publicación del CONPES 3701 de 2011, la Policía Nacional ha consolidado su rol misional en el marco de la construcción de una estrategia nacional de Ciberseguridad y Ciberdefensa, mediante el desarrollo de las capacidades para prevenir, atender, judicializar y perseguir los incidentes que afectan la Ciberseguridad nacional.



La Ciberseguridad: Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas, directrices, métodos de gestión del riesgo, acciones de prevención, investigación y atención del delito, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos informáticos y los usuarios en el ciberespacio.

Laboratorio de Análisis contra el Malware

Integración de fuentes: El modelo de investigación forense en malware tiene como fuente de información de diferentes orígenes: Caí Virtual, Asobancaria, entidades financieras, empresas, Pymes, entidades privadas y públicas.

Análisis y reporte de amenazas: Se cuenta actualmente con análisis de comportamiento de malware por medio de sandboxing (entornos virtuales controlados), Europol Malware Analysis Solution donde existen usuarios concurrentes de acceso a nivel de las regiones de policía para la carga de archivos (muestras de código malicioso) y posterior reporte de la amenaza encontrada.

Diagnóstico predictivo: El Centro Cibernético Policial cuenta con la capacidad de realizar consultas a otros validadores de información del cual tiene actualmente punto de enlace en la Oficina de Europol en Holanda, donde se pueden remitir las muestras y documentos SIENA para la consulta a lo homólogos en esa tarea investigativa.

Implementación y despliegue de hallazgo de APT (Amenazas Avanzadas Persistentes), se fortaleció en el CCP la actividad de respuesta a incidentes informáticos en caso de un ataque

informático en las infraestructuras críticas del país.

Base de datos y correlación de eventos: Se posee base de datos de consulta para relacionar información de código malicioso e identificar posibles amenazas y construcción de boletines de Ciberseguridad.

Resultados tangibles: Colaboración oportuna y mancomunada en operaciones, como Darkcode en colaboración con Ec3, (EUROPOL CYBER CRIME CENTRE) ATM Diebold y NCR para cajeros automáticos, Malware avanzado y polimófico en ataques a la banca y sus componentes tecnológicos.

Chat de la Ciberseguridad: WWW.CCP.GOV.CO

Este espacio fue concebido para garantizar la interacción de forma ininterrumpida, entre los cibernautas y policías expertos en la atención de incidentes cibernéticos.

Siempre a la vanguardia tecnológica, el C.C.P. dispone de herramientas desarrolladas para la atención en línea de múltiples usuarios, lo que permitió que en 2014 fueran atendidos un total de 172.576 ciudadanos.

Durante el 2015 la cifra ha venido en aumento y 55.286 ciudadanos han utilizado este medio de atención policial como alternativa para la denuncia y reporte de delitos o amenazas cibernéticas con atención personalizada desde un computador, un teléfono inteligente o una tableta.

Las consultas más frecuentes están orientadas a denunciar nuevas amenazas cibernéticas, correos fraudulentos, estafas en internet y mensajes con contenido difamatorio o amenazante a través de redes sociales. No obstante una franja importante de usuarios utiliza este servicio para consultar otros temas institucionales como la ubicación de sedes policiales, los procesos de incorporación, casos de convivencia ciudadana y otros.

Difusión de alertas en las redes sociales

El Centro Cibernético Policial viene fortaleciendo su presencia en redes sociales, las cuales permiten replicar masivamente las alertas generadas a partir de los avisos que los usuarios envían informando nuevas modalidades o amenazas cibernéticas en Colombia. Twitter y Facebook siguen siendo las redes sociales más populares en el país, millones de perfiles interactúan en el ciberespacio, por ello el CCP ha generado en el último año 7.684 alertas de amenazas a la Ciberseguridad o recomendaciones para enfrentar o mitigar los riesgos del Cibercrimen.

Casos como el llamado VIRUS de la DIAN, fue alertado por primera vez por el CAI VIRTUAL, como lo consignaron medios de comunicación nacionales y sitios Web especializados, donde la institución policial es referente de consulta por parte de expertos y Ciberusuarios.

Para garantizar el acceso e interacción entre los diferentes sectores involucrados en la Estrategia Nacional de Ciberseguridad, el CCP dispuso de un micro sitio en el cual pueden acceder distintos interlocutores del sector privado para generar discusión, adoptar y proponer buenas prácticas, conocer de nuevas amenazas y tendencias del Cibercrimen, o solicitar una atención más especializada a los problemas que en materia cibernética les afectan.

Actualmente el espacio denominado Café de Expertos cuenta con participación de distintos sectores, entre ellos el financiero y bancario, educativo, gobierno, servicios públicos, telecomunicaciones, energético e hidrocarburos, entre otros. Además de facilitar la comunicación con los homólogos de las Seccionales de Investigación Criminal responsables de la Estrategia Integral Contra los Delitos Informáticos a quienes se les asignó usuario y contraseña de acceso a la plataforma CAFÉ DE EXPERTOS.

CENTRO CIBERNÉTICO POLICIAL

Teniente Coronel **CARLOS ALFREDO CURREA BARRERA**
Jefe Unidad AMERIPOL - Colombia
Policía Nacional de Colombia

CUARTA CONFERENCIA GLOBAL SOBRE CIBERESPACIO EN HOLANDA

El 16 y 17 de abril de 2015 se llevó a cabo en La Haya (Holanda), la Cuarta Conferencia Global sobre Ciberespacio, donde participó el señor Teniente Coronel Carlos Alfredo Currea Barrera, jefe de la Unidad Nacional de AMERIPOL-Colombia en representación de la Comunidad de Policías de América; en este escenario hizo parte del panel de expertos mundiales frente a la Ciberseguridad, cuyo objetivo principal fue establecer los mecanismos de cooperación internacional entre entidades gubernamentales, sector privado y los diferentes organismos de seguridad internacional.

Aspectos de interés:

Es de resaltar que este evento es el principal foro mundial sobre asuntos de ciberespacio y seguridad, al cual asisten importantes personalidades y organizaciones de seguridad; las tres conferencias anteriores se realizaron en Londres (Inglaterra), Budapest (Hungría) y Seúl (Corea del Sur) y la V conferencia se realizará en México en el año 2017.

Es la primera participación de la Comunidad de Policías de América – AMERIPOL en este escenario, lo cual representa la credibilidad que ha ido adquiriendo la organización en el escenario internacional y la confianza de los organismos internacionales hacia AMERIPOL para enfrentar las nuevas amenazas que se ciernen sobre los hemisferios.

El evento contó con más de 1.800 especialistas en el tema, como el primer ministro Holandés, Mark Rutte, la alta representante de la Unión Europea para asuntos exteriores y para la política de seguridad, Federica Mogherini, la viceministra de tecnologías y sistemas de la información de Colombia, María Isabel Mejía Jaramillo, el director de EUROPOL, Rob Wainwright y la presidente de INTERPOL, Mireille Ballestrazzi, entre otros.

Entre los temas que el Oficial de la Policía Nacional de Colombia planteó en el marco del evento, se encuentran los siguientes:

Sofisticación criminal: se resaltó la importancia de las Tecnologías de la información y la comunicación (TIC) para la sociedad, especialmente para las organizaciones policiales, sin embargo los delincuentes han tomado provecho de estas herramientas para cometer diversos delitos entre los que se encuentran el fraude informático, Ciberacoso, terrorismo virtual, y delitos tradicionales como la trata de personas, narcotráfico entre otros delitos que a menudo tiene un impacto transnacional, generando limitaciones (legales) a los diferentes organismos de judiciales para la aplicación de la ley.

Se resaltó que existen procedimientos de asistencia judicial recíproca que a menudo requieren mucho tiempo para su utilización, lo que favorece a los criminales cibernéticos para que sus acciones queden en la impunidad.

Avances de AMERIPOL de cara a la Cibercriminalidad

En pro de la cooperación internacional para combatir la delincuencia organizada transnacional, AMERIPOL ha establecido en su agenda la Cibercriminalidad como la prioridad para abordar en la cooperación operacional entre las fuerzas del orden en las Américas.

Se resaltó el convenio existente entre la Policía Nacional de España y AMERIPOL, donde se estableció la implementación de un centro de Cibercriminalidad en la sede permanente de la Secretaría Ejecutiva de AMERIPOL, ubicada en la Ciudad de Bogotá (Colombia); para la adecuación de la infraestructura se contará con el respaldo de la Policía Nacional de Colombia a través de la DIJIN, frente a la estructuración de un Staff en esta materia.

AMERIPOL está avanzando en relaciones de cooperación estratégica con entidades como la Organización de los Estados Americanos - OEA y EUROPOL, para contribuir al compromiso de hacer frente a los delitos cibernéticos.

Así mismo, la comunidad de policías participó activamente en la publicación del libro sobre tendencias de la seguridad cibernética en América Latina y el Caribe con OEA y Symantec.

Conclusiones de la Cuarta Conferencia Global sobre el Ciberespacio

- En el desarrollo de la agenda programada en la conferencia, los diferentes organismos gubernamentales y privados dedujeron que para combatir la Cibercriminalidad, se tenían que trazar tareas en común, coordinación y cooperación hemisférica basada en el compromiso y responsabilidad de cada uno de los estados.

- Señalaron que no era necesario realizar un tratado internacional en la lucha contra los delitos informáticos a nivel de la Organización de las Naciones Unidas (ONU), teniendo en cuenta que ya existe la convención de Budapest, la cual busca atender los delitos por internet a través de la armonización de las leyes nacionales, mejorar las técnicas de investigación y aumentar la cooperación entre las naciones.

- De igual forma, se planteó la necesidad de diseñar estrategias para aplicar el derecho internacional con el objetivo de evitar conflictos y mantener un Ciberdominio estable.

- Por otra parte el señor Chen Xu, embajador de China en Holanda, resaltó que China, Rusia y otros países, presentaron una iniciativa en 2011, sobre un Código Internacional de Conducta para la Seguridad que había sido expuesto ante la Asamblea General de la ONU y fue actualizado en enero de 2015. El proyecto expone una serie de propuestas de normas internacionales sobre conducta responsable en materia de ciberespacio.

Inquietudes que podrían surgir en la próxima GCCS2017:

¿Cómo podemos mejorar la cooperación internacional para la adquisición de la prueba electrónica, en ambos casos de delitos informáticos y los casos más tradicionales?

¿Existen mejores prácticas de cooperación internacional?

¿Cuál podría ser el papel de las organizaciones regionales de Policía y la INTERPOL?

¿Cómo pueden las organizaciones gubernamentales y privadas trabajar juntos?

¿Cómo se puede mejorar la cooperación y cuáles son los límites de la cooperación?

Consideraciones

Este y otros eventos donde AMERIPOL ha sido invitado, ha venido impulsando la consolidación de esta Institución como un organismo más ante el mundo; dando a conocer la importancia de la institucionalidad de la misma para que así se logre el desarrollo total de los grandes y significativos proyectos que se vienen adelantando en esta Comunidad de Policías de América.

Es de resaltar la valiosa participación de la Policía Nacional de Colombia, la cual a través de estos espacios ha representado de manera significativa la Institución y ha demostrado el alto compromiso que tiene con AMERIPOL en busca de avance hacia la consolidación de la misma como organismo de cooperación, en la trascendente lucha de combatir crímenes trasnacionales.

Así mismo, utiliza estos espacios otorgados para afianzar la cooperación entre las diferentes Instituciones que hacen parte de AMERIPOL; incentivándolas a participar en eventos de talla mundial, donde con cada paso reconozcan la importancia y capacidades de esta comunidad.

Teniente Coronel **CARLOS ALFREDO CURREA BARRERA**
Jefe Unidad AMERIPOL - Colombia
Policía Nacional de Colombia

TRÁFICO DE CELULARES EN EL HEMISFERIO

En la actualidad los Equipos Terminales Móviles (E.T.M), permiten accesibilidad e interacción en tiempo real en escenarios laborales, educativos y sociales. En 2015 se registraron 7.630 millones de conexiones móviles en el planeta, mientras que el censo de población mundial es de 7.293 millones.[1]

El valor en promedio de un Smartphone en américa no supera los 500 dólares a excepción de Argentina donde es de US$ 568 un 17,6 % más alto en comparación con México, con US$ 483; mientras que en Ecuador es de US$ 450; en Brasil es de US$ 445; Chile US$ 358; Perú US$344 y Colombia US$ 223.[2]

Teniendo en cuenta las cifras anteriormente mencionadas, las estructuras delincuenciales han incursionado en una nueva modalidad de captación ilegal de dinero, desplegando su accionar criminal, hacia el hurto o robo de celulares, y de esta manera abriendo un mercado negro con tentáculos transnacionales que mueven cerca 830 mil millones de pesos colombianos al año.[3]

Por esta razón el hurto[4] o robo de celulares es el principal foco de percepción de inseguridad de los ciudadanos en países de la región como Colombia, Ecuador, Perú, Brasil, Argentina, México y Estados Unidos ya que generalmente está acompañado de delitos conexos como lesiones personales e incluso homicidio.

Durante diciembre del 2015, en Bogotá (Colombia) se realizó la encuesta de percepción y victimización de Cámara de Comercio a 9.867 personas, los entrevistados manifestaron que aumentó la inseguridad y que el hurto es el delito que más les preocupa al 49% de los ciudadanos y el objeto más robado es el celular con un 35%.

1. Cifras tomadas de la Global System for Mobile Association GSMA.
2. www.infobae.com consultora que comparó el precio de 705 Smartphone en la región.
3. http://www.elheraldo.co/nacional/acusaran-de-concierto-para-delinquir-quien-robe-celulares-212771
4. En países de la región se entiende por hurto cuando se da sin violencia y robo con violencia o intimidación.

Delincuencia Común: son personas, motivadas por ánimo de lucro, casi nunca tienen conexión con las organizaciones criminales transnacionales pero de manera indirecta es su brazo operativo ya que son quienes ejecutan el hurto o robo.

Receptador: Su rol es determinante pues es aquí, donde inician las estructuras criminales de carácter nacional con conexión al mercado negro internacional. Su función es comprar los celulares robados hasta por un 90% menos de su valor real. Es aquí donde los equipos son manipulados para modificar su código IMEI (International Mobile Station Equipment Identity) y reactivarlos de manera fraudulenta ante las compañías telefónicas.

Comercialización: Una vez realizado el procedimiento anterior hay dos opciones, la primera de ellas es comercializar al interior del país los equipos que se les modificó su código IMEI. La segunda opción, generalmente se da cuando no pueden ser modificados, dando lugar al tráfico ilícito de tarjetas madre entre los países de la región.

Tráfico en el hemisferio: las redes ilegales, coordinan el flujo de tarjetas madre, ya sea aéreo, fluvial o terrestre mediante empresas de logística o correos humanos, entre países como Argentina, Brasil, Chile, Colombia, Ecuador, Estados Unidos, Perú y México.

Organización criminal transnacional: aunque es el último eslabón; esta es la cabeza del tráfico ilegal de celulares, y si bien parece aislada del fenómeno local entendido en el hemisferio como hurto (sin violencia) o robo (con violencia) de celulares en territorio nacional, realmente es un factor importante ya que genera demanda en el mercado negro de Equipos de comunicación.

Con información aportada por la Unidad Nacional de AMERIPOL - Ecuador y la Dirección de Investigación Criminal de la Policía Nacional de Colombia DIJIN se pudo establecer que la demanda en el mercado negro de Equipos Terminales Móviles coinciden con los países donde el valor promedio es más alto (Argentina, México, Ecuador y Venezuela) y la oferta se da donde los teléfonos son más económicos (Colombia, Perú y Chile).

Estrategia adoptadas por Colombia para combatir el hurto de E.T.M

La principal estrategia liderada por la Policía Nacional de Colombia se enfoca al análisis del fenómeno y el comportamiento criminal a partir del reporte de la ciudadanía ante los operadores telefónicos para de esta manera estructurar investigaciones contra organizaciones criminales.

En la actualidad hay 23 millones de celulares que no han sido reportados y aparecen como activos. En los próximos meses los operadores contactaran directamente a los usuarios cuyo teléfono no ha sido registrado o posiblemente ha sido clonado. Si el usuario no aclara la situación, los operadores deben bloquear el aparato.

El Estado catalogó el hurto de a celulares como una cadena de crimen organizado. “Por lo tanto, es tratado como el delito de concierto para delinquir y lavado de activos”. Por lo que la Policía Nacional creó la estrategia integral contra el hurto de celulares a cargo un Grupo Élite para combatir el fenómeno.

Además, se están simplificando los procesos para allanar los sitios donde se comercializan los celulares robados, para que se puedan sellar e incluso aplicar la extinción de dominio.

Y para controlar las exportaciones e importaciones de celulares en el país, la DIAN y el Ministerio de Comercio reforzaron los controles en las fronteras para la importación de celulares y restricciones para la salida del país.

Consideraciones

Para desestimular el hurto y tráfico de celulares se debe articular esfuerzos entre las instituciones policiales homologas a fin de intercambiar experiencias que permitan detectar modalidades, estructuras y rutas de tráfico para hacer frente al delito que aunque parece interno tiene alcance transnacional.

Desde el 2012 La Policía Nacional de Colombia en el marco de la estrategia integral contra el hurto de celulares, ha atacado frontalmente las estructuras dedicadas a la receptación y manipulación de celulares robados. Dejando como resultado en el 2015 comparado con el año anterior una reducción del 9%[5] en el reporte de celulares hurtados, evidenciando que se desestimula la demanda de equipos hurtados cuando la estructura locales (dedicadas al hurto) carecen compradores y manipuladores.

Finalmente un aspecto que merece ser analizado, es el de desarrollar e incluir en los equipos móviles de comunicación un software que permita dar muerte tecnológica al aparato hurtado, tomando como referencia experiencias exitosas de otros países.

5. Cifra tomadas del balance 2015 de la estrategia ESHUC del Centro Cibernético Policial DIJIN.

CASO TUTELA

Después del respectivo sorteo en la Fiscalía, la denuncia recayó en la Fiscalía Especializada en Delincuencia Organizada, Transnacional e Internacional No. 5 de Pichincha a cargo del Dr. Fernando Guerrero, quien a su vez remitió la respectiva delegación fiscal a esta Unidad Especializada para que se realicen las investigaciones correspondientes, en sentido se realizó las siguientes diligencias:

- Se realizó el análisis de técnico digital de todas las direcciones IP por las cuales se conectaban las cuentas de la red social Facebook, determinando que pertenecen a varias ISP (Proveedora de Servicio de Internet) del Ecuador como son CNT, NETLIFE, ECUADOR TELECOM, entre otras, en este sentido a través de Fiscalía se solicitó a cada una de estas Proveedoras información acerca de los abonados e instalación física del servicio de internet, para dar con ubicación.

- Con información obtenida a esta ese momento y contando con la respectiva autorización para realizar vigilancias y seguimientos, con colaboración del personal de la UNASE pedido por el señor Fiscal, mediante la utilización de Operaciones Policiales de Recolección de Información (OPRI), se logró la ubicación e individualización del ciudadano VICTOR ELÍAS GUAMÁN REMACHE, conociéndose que el ciudadano se dedica a la actividad de albañilería y frecuenta un inmueble ubicado en el sector de San Rafael; barrio Huertos Familiares.

- Además se realizó el análisis de las fotografías y videos que reposan en el expediente fiscal mediante la utilización de Operaciones Policiales de Recolección de Información (OPRI) se logró la ubicación e individualización de la menor de edad (7 años) que responde a los nombres de LISBETH ESTEFANIA TROYA TROYA, con características fisiológicas similares a la de la menor que se observa en las fotografías que son materia de investigación y cuya madre responde a los nombres de María Rebeca Troya Troya, madre e hija frecuentan un inmueble ubicado en el mismo sector de San Rafael, Huertos Familiares, en lo que se conoció que el padrastro de la menor Lisbeth Estefanía Troya Troya responde a los nombres de Segundo Gustavo Guaman Remache quien sería hermano del ciudadano VICTOR ELÍAS GUAMÁN REMACHE.

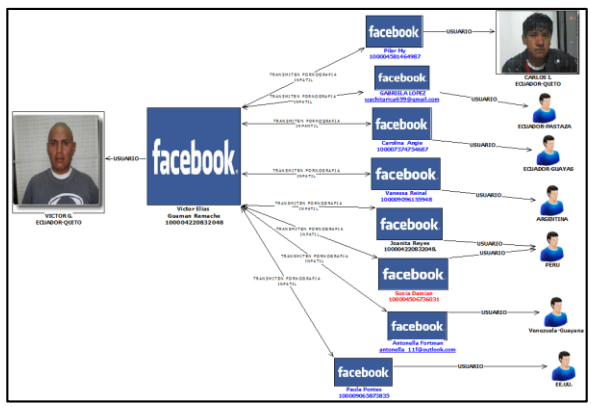
- Con todos los indicios recabados se solicitó a la Autoridad Competente la boleta de detención del ciudadano VICTOR ELÍAS GUAMÁN REMACHE y las respectivas órdenes de allanamiento de los inmuebles ubicados en el sector de San Rafael, Huertos Familiares.

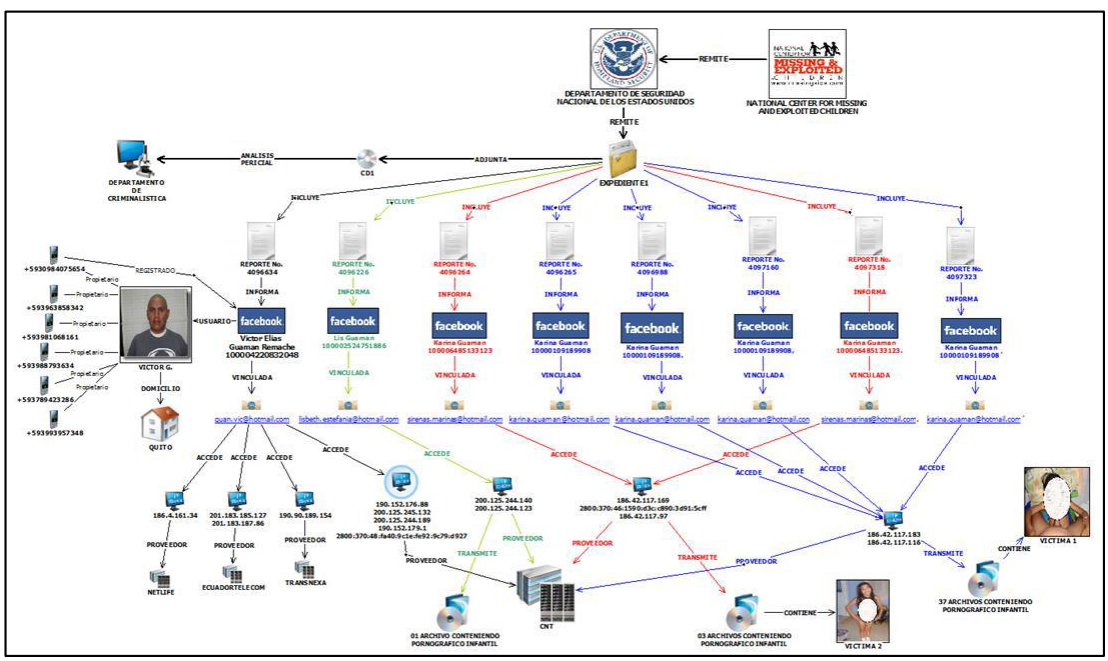
- El día jueves 02 de abril de 2015 a las 02:00 en compañía del señor Fiscal que conoce la causa personal de más unidades especiales de la Policía Nacional se procedió a la detención del ciudadano VICTOR ELÍAS GUAMÁN REMACHE, y el allanamiento de su domicilio en donde se incautó varios son equipos informáticos, vestimenta que utilizaba las víctimas y más indicios que tiene relación con el presente caso; así mismo en el segundo inmueble allanado

se pudo rescatar a dos menores de edad víctimas de este delito las mismas que responden a los nombres de LISBETH ESTEFANIA TROYA TROYA (7 años) y JESSICA JAZMIN GUAMAN TROYA (2 años), así mismo se incautó equipos informáticos .

VICTOR ELIAS GUAMAN REMACHE
CC 171197444-2

INDICIOS INCAUTADOS EN LOS INMUEBLES ALLANADOS





Inspector Jefe **PEDRO CRUZ GALLEGO**
Oficial Enlace del Cuerpo Nacional de Policia de España Ante AMERIPOL
Cuerpo Nacional de Policia de España

ENTREVISTA AL SEÑOR COMISARIO PRINCIPAL EUGENIO PEREIRO JEFE DE LA UNIDAD DE INVESTIGACIÓN TECNOLÓGICA DEL CUERPO NACIONAL DE POLICIA DE ESPAÑA

Confiesa que no es un experto en el aspecto técnico, pero el comisario principal Eugenio Pereiro cuenta con una extensa hoja de servicios que le ha llevado a liderar una de las áreas con más proyección de la Policía Nacional, la Unidad de Investigación Tecnológica. Gracias a su labor y a la de los 85 miembros de esta Unidad, el año pasado se detuvieron a más de 750 personas por delitos tan graves como la explotación sexual infantil online o el fraude. En esta entrevista desgrana algunas de las claves y dificultades de la investigación policial en la Red.

La Ciberseguridad es actualmente una de las principales preocupaciones para el Ministerio del Interior. ¿Qué acciones lleva a cabo el Cuerpo Nacional de Policía (CNP) frente a este reto?

El Plan Estratégico del Cuerpo Nacional de Policía 2013 - 2016 reconoce la Ciberseguridad como una de las prioridades de la institución. El Plan establece como objetivos generales la lucha especializada contra el Cibercrimen; la colaboración con los sectores público, privado y académico; la formación específica en el ámbito de la Ciberseguridad; la contribución al establecimiento de una cultura de la Ciberseguridad en la sociedad, las instituciones y el sector privado; y la participación en las principales estructuras policiales internacionales de carácter multilateral (Europol, Interpol y Ameripol).

¿A qué amenazas se enfrenta la sociedad española cuando hablamos de la Red?

Las amenazas son reales, graves y crecientes. En general se caracterizan por su globalidad, transnacionalidad, sofisticación y constante evolución. El espectro en el que operan es muy variado, pero destaca la explotación sexual infantil online, los fraudes digitales, los ciberataques y la comisión de variadas actividades delictivas a través de las redes sociales, especialmente las que adoptan formas de acoso.

¿Qué tipo de técnicas y herramientas utilizan más los Ciberdelincuentes?

La ingeniería social constituye una técnica recurrente para los Ciberdelincuentes. Combinan actividades de los mundos offline y online para engañar a las potenciales víctimas obteniendo información muy relevante para la posterior comisión de Ciberdelitos.

También las técnicas basadas en el anonimato y la encriptación están de plena actualidad. Igualmente la Ciberextorsión a ciudadanos, instituciones y empresas ha experimentado un notable incremento. En estos casos, los pagos económicos se exigen, de forma prioritaria, a través de criptomonedas, lo que supone un añadido a la complejidad investigativa dada su difícil trazabilidad y la ausencia de un organismo centralizado y regulador.

Las principales herramientas utilizadas por los cibercriminales son las redes anónimas, como TOR, la Deep Web, las VPN, foros cerrados, datos de registro falsos, conexiones ajenas, bullet proof hostings o servidores anónimos, sistemas de pago anónimo y el uso de servicios de comunicación cifrados.

Cuando hablamos de Internet, el concepto de territorio es algo difuso porque lo que se provoca en un país se manifiesta en otro u otros; es decir, no hay fronteras. Desde esta perspectiva, ¿cómo se pueden perseguir los delitos eficazmente cuanto hay tal indefinición de la normativa internacional para el entorno online?

Desde un punto de vista técnico - jurídico, la eficacia en la lucha contra una amenaza eminentemente transnacional como el Cibercrimen pasa por tres exigencias. La primera es la adopción de legislaciones nacionales adecuadas, que contemplen la tipificación, la persecución, los procedimientos, la jurisdicción y la responsabilidad de los proveedores de servicios de Internet. La segunda es la armonización de las legislaciones nacionales en el plano internacional. Y la tercera es la cooperación internacional, cimentada a través de la extradición, la asistencia legal mutua, el reconocimiento de las sentencias judiciales de otros países y, debido a la naturaleza volátil de las evidencias digitales, la preservación de los datos informáticos. Y todo ello bajo parámetros de dinamismo y rapidez.

> “Necesitamos procedimientos más ágiles y eficaces para afrontar los desafíos tecnológicos”

Además, es preciso avanzar en algunos aspectos que no gozan de un consenso generalizado. La tipificación de los actos cibercriminales no es uniforme a nivel global. Sirvan como ejemplo las actividades relativas al spam y, en menor medida, al racismo y la xenofobia online, así como el fenómeno del Grooming. Incluso la libertad de expresión constituye un elemento de desencuentro en el plano global. Mientras que la mayoría de los países persiguen formas de expresión extremas, como la incitación al genocidio, odio, discriminación, violencia, terrorismo o propaganda para la guerra, otros países mantienen un cierto margen de apreciación por razones culturales o tradiciones legales.

¿Qué mecanismos ha articulado el CNP en los últimos años para potenciar la colaboración en Ciberseguridad con los actores públicos y los privados?

En el CNP se ha instalado la necesaria concienciación en materia de Ciberseguridad. A este respecto, hay diferentes unidades policiales que operan en varios ámbitos: prevención, protección, investigación.

En el plano investigativo, a la concienciación se suma una inequívoca mentalidad abierta, flexible y colaboradora con los principales agentes críticos que operan en el ámbito de la Ciberseguridad, como pueden ser jueces, fiscales, instituciones, empresas, universidades.

La UIT está representada en la Fiscalía de Criminalidad Informática de la Fiscalía General del Estado. Además, mantiene canales de comunicación permanentes con los departamentos de seguridad de las principales empresas y corporaciones de nuestro país.

Miembros de esta Unidad participan de forma continua y activa en la mayoría de foros de Ciberseguridad, ya sean públicos, privados o académicos.

En el escenario internacional, ¿qué iniciativas en las que participa el CNP están dando fruto en ese sentido?

Estamos representados y participamos muy activamente en los principales foros de carácter multilateral, como son el Interpol Global Complex for Innovation, con sede en Singapur, y el Centro de Lucha contra el Cibercrimen (EC3) de Europol, con sede en La Haya (Holanda). Además, el Cuerpo Nacional de Policía ha protagonizado en la última cumbre de directores de policía de Ameripol, celebrada en México DF, la presentación de un proyecto de creación de un centro de lucha contra el Cibercrimen en el seno de dicho organismo.

Así mismo, varios especialistas investigadores de la UIT participan (y en varios casos lideran) en grupos de trabajo específicos del ámbito internacional competentes en las principales actividades de las tres grandes áreas del Cibercrimen: la explotación sexual infantil online, los fraudes digitales y los ciberataques.

En ocasiones, las compañías que quieren denunciar un caso tienen dudas en torno a qué institución deben dirigirse para abordar su problema. ¿En qué casos deben acudir a la UIT?

En materia de lucha contra el Cibercrimen, el CNP dispone de una estructura integrada por miembros de la Policía Judicial coordinada en los ámbitos central y territorial. En cada comisaría provincial y en las principales comisarías locales disponemos de grupos específicos dedicados a la investigación de los Ciberdelitos.

A nivel central se encuentra la UIT. En cualquier comisaría de Policía se pueden presentar denuncias por la comisión de Ciberdelitos. Dependiendo de las circunstancias, la investigación se desarrollará por los ámbitos local, provincial, regional o central. En todo caso, las denuncias serán investigadas. Además, a nivel central, el CNP dispone de canales de notificación de cualquier sospecha o consulta en este ámbito: vía web, redes sociales y correos electrónicos gestionados por especialistas de la UIT.

En el ámbito empresarial, estamos a disposición de los usuarios de la Red Azul.

En España, la seguridad en Internet ha calado en normativas como la nueva Ley de Seguridad Privada. ¿Cuál es su valoración sobre esta norma?

La referencia en este asunto es el artículo 6 de la Ley 5/2014 de Seguridad Privada. Ese apartado establece que a las empresas, sean o no de seguridad privada, que se dediquen a las actividades de seguridad informática se les podrán imponer reglamentariamente requisitos específicos para garantizar la calidad de los servicios que presten.

Obviamente, esta incorporación es necesaria. En este momento se sigue trabajando sobre el borrador de Reglamento de desarrollo de la citada ley en tres aspectos concretos: la anotación en el Registro Nacional de Seguridad Privada de las empresas dedicadas a la seguridad informática; la posibilidad de establecer requisitos a dichas empresas, en función de los servicios que prestan, para asegurar su calidad; y definir una serie de medidas exigibles en materia de seguridad informática, así como un catálogo de sujetos obligados a su cumplimiento.

¿En qué aspectos ha de avanzar la legislación española para facilitar y hacer más eficaz la persecución de los delitos en la Red?

En el plano técnico-jurídico, el año pasado se caracterizó por las relevantes reformas que hubo en materia de Derecho Penal sustantivo y Procesal Penal, introduciendo y actualizando nuevas figuras delictivas y mejores instrumentos para la lucha contra el Cibercrimen. En este momento, demandamos medios y procedimientos que aseguren más agilidad, rapidez y eficacia para afrontar los continuos desafíos que plantean los avances tecnológicos.

La concienciación y la formación son la base de muchas acciones dirigidas a la sociedad para hacer un uso seguro de Internet. ¿Cuáles ha emprendido en ese sentido la UIT con las empresas?

La primera concienciación es la de los profesionales del CNP que luchan contra el Cibercrimen. A continuación contribuimos a la necesaria concienciación de los sectores afectados y potenciales víctimas a través de diferentes iniciativas. Las más visibles son nuestras aportaciones y participaciones en las redes sociales oficiales (como Twitter y Facebook), la página web de la Policía, correos electrónicos específicos, etcétera.

Además, participamos en reuniones, eventos, foros, grupos de trabajo organizados por los sectores empresarial y académico.

De igual modo, esa participación y colaboración se traduce en la promoción de actividades formativas para nuestros investigadores, que necesitan no sólo una formación y especialización policial, sino también la actualización que nos proporcionan las instituciones, empresas y corporaciones que sufren la actividad cibercriminal.

Inspector Jefe **PEDRO CRUZ GALLEGO**
Oficial Enlace del Cuerpo Nacional de Policia de España Ante AMERIPOL
Cuerpo Nacional de Policia de España

A continuación se reproduce el reportaje integro sobre la Unidad de Investigación Tecnológica (UIT) del Cuerpo Nacional de Policía de España, así como la entrevista a su responsable, que la Revista ***RED SEGURIDAD*** *publicó recientemente.*

La revista ***RED SEGURIDAD*** *se ha conformado en referente indiscutible en la industria de la Seguridad de la Información en España y en publicación de consulta tecnológica en el sector de la Seguridad en general. Su primer número salió de la imprenta en noviembre 2002 y poco a poco, se ha erigido en un espacio común y abierto en el que todos los agentes implicados en el sector de la Seguridad de la Información pueden exponer sus productos, ideas, contrariedades e inquietudes, incluyendo informaciones especiales y artículos técnicos elaborados por expertos y especialistas. http://www.redseguridad.com.*

REPORTAJE TRAS LOS DELITOS EN LA RED, VISITA A LA UNIDAD DE INVESTIGACIÓN TECNOLÓGICA DEL CUERPO NACIONAL DE POLICÍA DE ESPAÑA

Bucean diariamente en las profundidades de la Red para pescar a los malos. Desde organizaciones criminales hasta empleados desleales, pasado por explotadores sexuales infantiles, estafadores o piratas informáticos caen cada año en manos de la Justicia gracias a la labor que desempeñan los agentes de la Unidad de Investigación Tecnológica de la Policía Nacional. El año pasado fueron capaces de detener en el complejo entramado de Internet a más de 750 presuntos delincuentes, entre los que predominaron los pedófilos que se sirven de las nuevas tecnologías para intercambiar sus deleznables imágenes. Sin ir más lejos, el pasado octubre fueron arrestadas 81 personas en una de las últimas macro operaciones contra la explotación sexual infantil online, cuya investigación partió de un “Ciberpatrullaje” de los agentes de esta Unidad.

Red Seguridad ha accedido al centro de operaciones de estos 'guardianes de la red', que desde 2013 forman la Unidad de Investigación Tecnológica (UIT). Antes de ese año, la Policía Nacional perseguía los Ciberdelitos a través de la Brigada de Investigación Tecnológica (conocida como la BIT) que ha conseguido muchos éxitos policiales pero que necesitaba crecer ante el aumento de las prácticas ilícitas a través de Internet. Hoy, la estructura de la UIT está dividida en dos brigadas, la de Seguridad Informática y la de Investigación Tecnológica, y una Sección Técnica.

Nos recibe en su despacho el comisario principal Eugenio Pereiro, un profesional con un amplio bagaje policial que ahora dirige a un equipo de 85 funcionarios de diferentes escalas y perfiles. “Aquí combinamos la capacitación técnica con la experiencia policial”, explica este firme defensor del trabajo en equipo como elemento imprescindible en una labor tan compleja como perseguir los delitos en la Red. La UIT cuenta con ingenieros, peritos y técnicos informáticos que, además de reunir las capacidades tecnológicas que

requiere su trabajo, participan en todo tipo de foros nacionales e internacionales donde “cada día es más necesario estar”. No en vano, según indica el comisario principal Pereiro, una gran parte de las operaciones que llevan a cabo tienen conexiones internacionales.

El año pasado, la UIT realizó 516 investigaciones entre las que destacan 188 relacionadas con la explotación sexual infantil online, 76 fraudes digitales (sobre todo en las telecomunicaciones), 67 de seguridad lógica (antipiratería, ciberataques o hacktivismo) y 66 en redes sociales. Además, la Sección Técnica participó en 119 operaciones para realizar volcados en caliente o gestionar evidencias digitales procedentes de ordenadores y otros dispositivos.

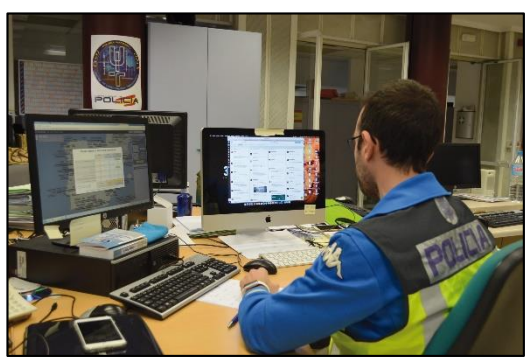
Seguridad Informática

El comienzo de nuestra visita nos lleva a conocer la Brigada de Seguridad Informática, que está dividida en dos secciones: Seguridad Lógica y Fraudes Digitales. “Las investigaciones que practicamos aquí son muy diferentes unas de otras, pero el grupo dedicado a los ciberataques es el que quizás más complejidad tiene”, explica el comisario Tomás Vicente, jefe de esta brigada.

La Sección de Seguridad Lógica está especializada en perseguir la piratería online, los ciberataques y el hacktivismo. Cuenta para ello con dos grupos: el de antipiratería y el de ciberataques. El primero de ellos se encarga de averiguar los delitos contra la propiedad intelectual, como pueden ser la descarga de películas, series, videojuegos o música. Un problema que ha aumentado tanto que hoy “el 95 por ciento de la piratería se produce a través de Internet”, apunta el inspector jefe de la Sección Lógica.

Los miembros del grupo antipiratería sacan pecho por haber llevado a cabo con éxito operaciones que han dado como resultado el cierre de varias páginas web de descargas. Como fue el caso de la Operación Youkioske (una plataforma de descargas gratuitas de libros y revistas), en el año 2012, “que fue paradigmática porque por fin se condenaba a los autores como grupo criminal”. Otros ejemplos son la clausura de Series Pepito o Series Ly.

Pero si la piratería en Internet es un delito al alza, también lo son los ciberataques. Con el añadido de que el grupo dedicado a este asunto se encuentra “todas las complejidades que puedan imaginarse” a la hora de investigar. La anonimización, las redes Peer to Peer, el crime as a service, los black markets, el cifrado de las comunicaciones y los equipos… son muchos los obstáculos tras los que se esconden los malos para evitar que les descubran. Aún con eso, son también numerosos los logros en este campo, entre los que destaca el desmantelamiento de la organización criminal que estaba detrás del llamado "virus de la policía”, un Ransomware predecesor de Criptolocker, uno de los ciberataques más dañinos para las empresas el año pasado.



Continuamos la visita a la Brigada de Seguridad Informática a través de la Sección de Fraudes Digitales, que está compuesta por tres grupos: fraude bancario, fraude en Internet y fraude en el

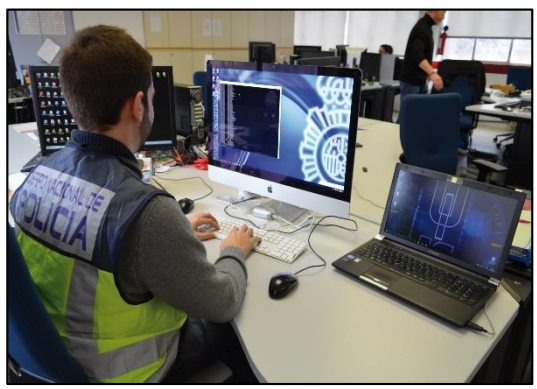
uso de las telecomunicaciones. Entre las paredes de esta sección se ha conseguido desmantelar organizaciones criminales como la de la Operación Triangle, que utilizaba técnicas de ingeniería social y aplicaciones malware para obtener las credenciales de correos electrónicos de empresas. De esta manera terminaban accediendo a las claves que les permitían solicitar a las entidades bancarias transferencias en nombre de sus víctimas.

La Operación Overyn fue otra de las llevadas a cabo por la Sección de Fraudes Digitales, concretamente desde el grupo de fraude en el uso de las telecomunicaciones. Según relata Enrique, uno de los miembros de este grupo, los delincuentes utilizaron como gancho el casting celebrado el año pasado en España para aparecer como extra en la popular serie de televisión Juego de Tronos. “Se hacían pasar por la productora encargada del casting a través de una página web con la misma apariencia que la real. En ella publicitaban un número de abonado de tarificación superior a una llamada normal, pero hacían creer a los candidatos que era el teléfono con el que acceder a la prueba. De ese modo obtuvieron por las llamadas una elevada cantidad de dinero".

Cuando preguntamos a los miembros de la Brigada de Seguridad Informática sobre las dificultades a la hora de investigar los Ciberdelitos, a técnicas como el cifrado o la anonimización que utilizan los malos para esconderse, se suma la complejidad judicial internacional. “Para acceder a un servidor de otro país hay que solicitar un comisión rogatoria. Los pitaras saben que esto tarda en aprobarse el tiempo suficiente como para cambiar sus parámetros, o directamente se sitúan en países no colaborativos”, lamenta el comisario Vicente.

Colaboración

Aunque la Brigada de Seguridad Informática es proactiva a la hora emprender investigaciones, por lo general todo comienza tras una denuncia. En el caso de la Operación Storm, realizada el año pasado, un insider que trabajaba para una empresa española extraía información para después venderla en black markets mediante transferencias en Bitcoins (moneda virtual). La compañía lo denunció y, gracias a la colaboración con la UIT, los agentes dieron con él. En total, con su actividad causó un perjuicio de al menos tres millones de euros para la compañía.



Otro ejemplo de colaboración fue la Operación Walker: “desde hace un par de años detectamos que se robaban muchos teléfonos móviles de turistas extranjeros que visitaban Barcelona. Días después de la sustracción, recibían llamadas de sus operadoras que les informaban de que sus tarjetas telefónicas habían sido utilizadas para realizar llamadas por grandes sumas de dinero. Trabajamos junto con varios operadores internacionales para conseguir desmantelar la organización. Una sola de estas operadoras estimó pérdidas de 53 millones en sólo tres años”, nos cuenta uno de los agentes que participó en el caso.

La colaboración con las empresas es, pues, una práctica habitual y necesaria para perseguir los delitos informáticos. “Las denuncias se ponen directamente aquí o a través de canales como la Red Azul de la Policía Nacional. Lo normal es que si una empresa tiene un incidente nos informe y le orientemos sobre cómo enfocar la denuncia”, explica el comisario Tomás Vicente. En cualquier caso, “la colaboración con las empresas es imprescindible; por eso una de nuestras funciones consiste en mantener abiertas las vías de comunicación con los CISO y otros profesionales de la seguridad. Fomentamos las relaciones bilaterales”, añade.

La BIT

Nuestra visita avanza hacia las dependencias de la Brigada de Investigación Tecnológica, conocida como la BIT. Hasta 2013, esta brigada asumía dentro de la Policía Nacional los delitos en la Red. Hoy forma parte de la UIT para hacerse cargo especialmente de los relacionados con el abuso infantil online y en las redes sociales. Como explica el comisario Miguel Manzanas, jefe de la BIT, estamos ante un área que “se centra más en las personas que en el patrimonio”.

La creación de la UIT potenció actividades que entonces la BIT realizaba de manera menos estructurada que en la actualidad, como la investigación de delitos en las redes sociales y redes abiertas. Ahora cuenta con más recursos, agentes especializados en estos entornos y herramientas específicas. “Es una brigada proactiva, porque en Internet no tenemos que ir sólo a demanda”, asegura el comisario Manzanas.

La BIT Consta actualmente de dos grandes bloques: la Sección de Protección al Menor y la Sección de Redes. Operaciones como Nanisex supusieron en su momento un gran golpe contra la explotación sexual infantil online, pero se trata de una lacra que no sólo permanece sino que ha ido en aumento en los últimos años. Este tipo de delitos se persiguen desde la Sección Operativa de Protección al Menor. Según nos explica su responsable, el inspector jefe Luis García, está dividida en tres grupos: el de Colaboración con el FBI, mediante el cual se organizan y coordinan operaciones de colaboración con la institución policial estadounidense; el de Investigación de Redes P2P, donde se investiga el intercambio de archivos y la ‘red oculta’; y el Grupo primero de Protección al Menor, que se dedica al acoso sexual a menores y a la coordinación de la oficina virtual con la Interpol para la identificación de víctimas.

La principal dificultad del trabajo de esta sección está en el anonimato en la Red de los pedófilos, tal y como afirman los componentes de la sección. “Los delincuentes utilizan herramientas opacas para ocultarse, pero la Policía cuenta con la colaboración de todas las instituciones y las universidades. Normalmente llegamos hasta ellos, si bien cuando tenemos controlada una aplicación se van a otra para que no les detectemos”, explica el inspector jefe García.

Según el responsable de la Sección de Protección al Menor, en los últimos años se han producido avances judiciales para la persecución de los delitos sexuales online relacionados con menores. Pero también, subraya, es fundamental la colaboración que existe con los proveedores de Internet y redes sociales. “La sensibilidad de los operadores en materia de protección sexual infantil online es muy grande y, por ello, nos facilitan mucho la labor de investigación”, añade el comisario Manzanas.

La BIT también cuenta en su estructura actual con la Sección de Redes, “la más

joven de la Unidad" puesto que se creó a principios de 2014 "con el boom de las redes sociales", explica el inspector jefe de esta área, Roberto Fernández. "La actividad de las sección se divide, por un lado, en la monitorización para ver qué está pasando en Internet, en general y, por otro lado, en las redes sociales, especialmente con temas que son trending topic", explica el policía.

No obstante, en esta sección también se lleva a cabo la investigación de otros delitos. Existen ejemplos de operaciones relacionadas con el juego online, la extorsión, injurias, calumnias… En torno a estos últimos, el inspector jefe de la Sección de Redes indica que "en Internet se dan muchas acciones que están entre la libertad de expresión y el delito".

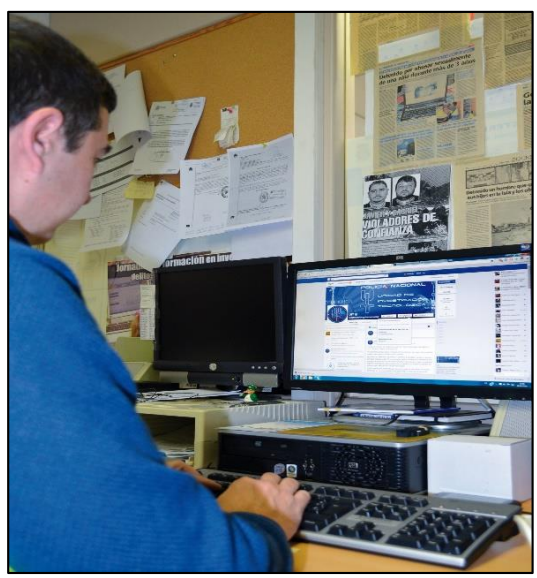
Sección Técnica

Dejamos atrás a los miembros de la Brigada de Investigación Tecnológica para conocer el área donde se concentra el mayor conocimiento técnico de toda la UIT, es decir, la Sección Técnica, que depende directamente del comisario principal Pereiro. La inspectora Silvia Barrera es la responsable de esta sección, que no sólo da soporte a las brigadas de la UIT sino a todas las unidades de la Policía. "Analizamos equipos en los registros durante las operaciones, realizamos análisis forenses de los equipos, hacemos I+D de algunas herramientas", enumera la inspectora Barrera.

La Sección Técnica cuenta con un laboratorio equipado con tecnología para extraer información en diferentes soportes. En él trabajan agentes como David, que recurre a potentes ordenadores forenses para analizar copias de los discos duros de los equipos de los presuntos delincuentes o herramientas para obtener evidencias digitales de dispositivos móviles. Aunque, como explica, "hay ocasiones en las que se sacan las pruebas en el propio juzgado porque alguna de las partes quiere ver cómo se extraen".

Hoy en día, gran parte de las operaciones policiales acaban de una manera u otra con un soporte electrónico en esta sección. Y es que, como señala la inspectora Barrera, "en el 95 por ciento de los casos la prueba está en algún ordenador o dispositivo móvil". De ahí la cada vez mayor cantidad de material con datos que llegan hasta esta área de la UIT. Una tendencia que va en aumento. Más si se repiten casos como la Operación Emperador (organización de blanqueo de capitales y fraude fiscal), que dejó tantos ordenadores para analizar y extraer datos que podría "ponerse una tienda", afirma con ironía la jefa de la Sección Técnica.

Ella y el resto de miembros de la UIT saben que el volumen de su trabajo irá a más cada día que pase. El uso de las tecnologías es hoy la principal vía para llevar a cabo delitos de todo tipo y los malos están cada vez mejor preparados para ocultarse en la Red. La UIT estará detrás para tratar de evitarlo.



30 AÑOS DE HISTORIA

Para encontrar el origen de la investigación de delitos informáticos por parte de la Policía Nacional hay que remontarse a 1986, en el ámbito de la Unidad de Delincuencia Económica y Financiera (UDEF). Pero hubo que esperar hasta nueva años después para que se creara en esta unidad el Grupo de Delitos Informáticos, "del que formaban parte sólo dos compañeros que investigaban fraudes, la venta de ordenadores sin factura, programas informáticos pirata...", recuerda el inspector Enrique, uno de los veteranos de la UIT.

Entre 1995 y 1999 se crearon nuevos grupos especializados y comenzó a definirse una estructura contra los delitos informáticos.

En 2002 se creó la Brigada de Investigación Tecnológica, que seguiría enmarcada en la UDEF hasta 2006, cuando paso a formar parte de la Unidad de Delincuencia Especializada y Violenta.

Así llegó al año 2013, en el que fue constituida la actual Unidad de Investigación Tecnológica.

Capitán **ALBERTO REDONDO SÁNCHEZ**
Jefe de Grupo de Delitos Tecnológicos
Unidad Técnica de Policía Judicial
dg-utecnicapj-4ctecnologico@guardiacivil.org
Guardia Civil de España

"OPERACIÓN ONYMUS" COMO EJEMPLO DE BUENAS PRÁCTICAS EN MATERIA DE INVESTIGACIÓN TECNOLÓGICA

Antecedentes

La Operación ONYMOUS se planeó como una acción internacional operativa dirigida a desmantelar los market de productos ilegales a los que se accedía desde The Onion Route (TOR) impulsada por el FBI, EC3-EUROPOL y EUROJUST. La idea era hacer partícipes a las unidades de ciberdelincuencia de las principales fuerzas policiales de los países implicados en una actividad conjunta.

Con esta actuación se pretendió, en primer lugar, desmantelar los principales sitios web con acceso desde TOR donde se mercadeaba con productos ilícitos. El segundo gran objetivo, lanzar el mensaje que TOR no es tan anónimo y seguro para las organizaciones criminales como se cree. Por último recabar información, para elaborar inteligencia en aras de identificar tendencias y nuevos patrones de distribución.

Desarrollo de la Investigación

La investigación se inició fruto de la colaboración que mantiene la Guardia Civil con cuerpos y agencias policiales de otros países, dentro de los distintos foros internacionales a los que se asiste para la prevención del delito a través de Internet. En este marco de trabajo se comunicó una iniciativa, liderada por el FBI y coordinada por EUROPOL y EUROJUST, dirigida a cerrar los principales sitios web que surgieron a raíz del cierre de SILK ROAD, proponiendo a la Guardia Civil participar en la misma.

Imagen 1.- Banner del dominio intervenido

Como consecuencia de las labores de investigación y análisis de la información proporcionada por las autoridades estadounidenses, se descubrió la existencia de una página web, muy probablemente administrada desde una IP española, desde donde se ofertaban productos aparentemente ilícitos. Por todo ello, a través de EUROPOL, se pidió a la Guardia Civil que iniciara gestiones para poder identificar a la persona que se escondía detrás de ella.

La actividad comenzó con el estudio de esa IP concreta, concluyendo que a través de la misma existían conexiones al panel de control desde donde se administraba una URL de un sitio web al que se accedía por TOR. La principal actividad de esta página, denominada ""Fast Cash!" -

http://5oulvdsnka55buw6.onion/ era a facilitar dinero falsificado previo pago de Bitcoins.

Identificadas las necesidades para el desarrollo de la operación, se mantuvo contacto con la Fiscalía de Criminalidad Informática para impulsar las actuaciones a nivel nacional, e identificar así al titular de la línea habitual desde la que se realizaban las acciones presumiblemente ilícitas. El primer contratiempo que surgió es que el perfil de este titular no coincidía con el patrón de un "Ciberdelincuente" (edad avanzada, trabajo alejado a las nuevas tecnologías y sin apenas conocimientos técnicos), por lo que se comenzaron a realizar las labores operativas sobre el terreno. La primera teoría que se barajó, fue la intrusión ilícita a la red inalámbrica por terceras personas, pero una vez en lugar no se observó ningún indicio que confirmara esta idea.

Descartada esta hipótesis, se realizó un análisis en fuentes abiertas y redes sociales vinculadas al titular de la línea con la intención de identificar cuáles eran sus contactos y amistades, para así de esta forma identificar a un tercero que encajara con el perfil requerido. Así se pudo localizar a una persona bastante activa en internet, y una vez analizada su actividad, se concluyó que su perfil cuadraba con alguien que tuviera profundos conocimientos en informática y, principalmente, asiduo al empleo de TOR y Bitcoin. Una vez identificado, se corroboró que tenía relación familiar con el propietario de la red Wifi.

Una vez situada la zona aproximada por la geolocalización de la IP, se localizó el domicilio exacto en la localidad de Arenys de Mar (Barcelona), dando cuenta de estos hechos en los Juzgados de esa localidad. Se solicitaron los correspondientes mandamientos judiciales para lograr identificar fehacientemente al titular de la IP, así como la pertinente orden de entrada y registro con la intención de localizar nuevos indicios que complementaran la imputación de la actividad criminal.

Dentro del domicilio del principal sospechoso se identificaron elementos que apoyaban la teoría de los investigadores, tales como la existencia de papel moneda falsificada, soportes para clonar tarjetas de pago o documentos con claves de acceso a Wifi de redes vecinas, aunque el verdadero objetivo se orientó desde el primer momento al análisis de los equipos informáticos. Para ello se programaron unos script que pudieran localizar cualquier tipo de monedero electrónico en sus dispositivos para así lograr identificar la recepción de pagos mediante criptomoneda. Una vez fijado esto, se procedió a corroborar que desde sus equipos se accedía a la web que administraba en TOR (localizándose la clave privada de acceso), dándose por concluida la actividad operativa en el domicilio.

Paralelamente a este registro, se accedió al domicilio desde donde se detectó inicialmente la IP de acceso, localizando la instalación de un equipo que ejercía de servidor desde donde el implicado se conectaba en remoto para administrar la web objeto de la investigación. Se procedió a imputar al titular.

Concluida esta fase, se presentó al detenido a la autoridad judicial competente y se realizaron los pertinentes informes técnico-policiales que plasmaron la actividad operativa.

Imagen 2.- Parte de los objetos intervenidos

Imagen 3.- Servidor de la página web en TOR montado en el domicilio

Impacto y Trascendencia

En la Operación ONYMOUS, una de las mayores desde el punto de vista estratégico para la seguridad en internet, se desmantelaron 410 servicios alojados en TOR de dominio ".oinion", interviniendo más de un millón de dólares en criptomonedas (principalmente Bitcoin) y cerca de 180.000 euros en metálico. Se culminó con la detención de 17 personas vinculadas a sitios web dedicados al tráfico de drogas, armas, falsificaciones de moneda y distribución de pornografía infantil. Alguno de ellos, como SILK ROAD 2.0, tenían cerca de 150.000 usuarios repartidos por todo el mundo. En el operativo han participado las unidades de Ciberdelincuencia de las principales policías de 18 países, coordinadas por EUROPOL, EUROJUST y el Departamento de Justica de los EEUU.

El principal mensaje que se quiso trasmitir con la actuación fue desmitificar la idea de impunidad que parece rodear a este tipo de markets, dejando claro que empleando las herramientas existentes en materia de cooperación judicial y policial internacional se puede investigar positivamente.

A raíz de la caída de estos mercados se ha detectado el aumento del uso de otros sistemas descentralizados de navegación por la Deep Web, como en el caso de las redes I2P, lo que se considera ya una de las alternativas cada vez más consolidadas. En la misma línea y consecuente a esta presión policial a nivel internacional, se ha propiciado la implementación de medidas de seguridad en los markets, como es la doble autentificación, la encriptación de las comunicaciones end-to-end y los sistemas de garantía tipo escrow.

1. A través del *Joint Cybercrime Action Taskforce* (J-CAT)
2. Octubre de 2013

FUNDAMENTO LEGAL DE LA SECCION CONTRA DELITOS INFORMATICOS ORDEN GENERAL 67-2014

Artículo 1. De la Organización y Designación de Funciones de la División Especializada en Investigación Criminal. Se organiza y designa funciones a la División Especializada en Investigación Criminal de la Policía Nacional Civil, con el propósito de brindar un servicio eficaz y coordinado en la investigación criminal.

Artículo 6. Estructura Organizativa. La División Especializada en Investigación Criminal, tiene la siguiente estructura:

3.5. Departamento de Investigación de Delitos contra la Delincuencia Organizada

3.5.6. Sección contra Delitos Informáticos.

Artículo 53. Sección Contra Delitos Informáticos: La Sección Contra Delitos Informáticos, depende de la Jefatura del Departamento Contra la Delincuencia Organizada; está a cargo de un Oficial Primero de Policía en servicio activo, con Especialidad en Investigación Criminal; es nombrado por el Jefe de la División a propuesta del Jefe del Departamento.

Funciones:

a. Investigar los Delitos Informáticos contemplados en el Código Penal y otras leyes conexas;

b. Auxiliar al Ministerio Público en el Proceso de Investigación;

c. Coordinar ante el Órgano Jurisdiccional competente las medidas de coerción;

d. Documentar las Diligencias de Investigación Criminal desarrolladas dentro del Proceso de Investigación; y,

e. Otras que se le sean asignadas por el Jefe del Departamento de conformidad con la ley.

Estrategias Utilizadas para la Resolución de Casos Contra Cibercrimen

Una de las principales estrategias a utilizar para el desempeño de nuestro trabajo ha sido establecer contactos nacionales e internacionales de los cuales se ha recibido apoyo para el desarrollo y la resolución de hechos ilícitos cometidos a través de la red de redes (INTERNET), entre los contactos nacionales podemos mencionar a los Proveedores de Servicio de Internet (ISP) también hacemos mención, que es indispensable tener una buena coordinación de trabajo con el Ministerio Publico, ya que es el ente encargado de la persecución penal en nuestro país. En los contactos internacionales, podemos hacer mención de unidades contra el Cibercrimen del resto de países latinoamericanos, con las cuales se ha coordinado y colaborado en materia de investigación.

Experiencia Exitosa en Materia de Cibercrimen

Con fecha 01 de marzo del año 2016, a esta Sección Contra Delitos Informáticos se avocó personal de la sección del

Comando Antisecuestros de la División Especializada en Investigación Criminal, de la Policía Nacional Civil, con la finalidad de solicitar apoyo en la investigación de un caso, debido a que a esa sección presentaron una denuncia del secuestro de una menor de edad, en donde los victimarios solicitaban a los familiares de la víctima el rescate por medio de mensajes de la red social de Facebook, utilizando el perfil de la menor de edad secuestrada, con el objeto de evadir cualquier investigación y de esta manera no ser identificados.

Evidenciando la urgencia del caso por parte de esta sección se realizaron las diligencias correspondientes al caso procediendo a contactar a los administradores de la red social de Facebook realizando una solicitud formal de información sobre las conexiones realizadas por el perfil desde donde los victimarios se contactaban con los familiares de la víctima solicitando el rescate, a lo cual el personal de Facebook respondió positivamente, enviando una serie de direcciones IP sobre las conexiones que el perfil había tenido. Utilizando la información proporcionada por Facebook y el trabajo conjunto con el Ministerio Publico se logró ubicar la dirección desde donde se originaban las conexiones del perfil de Facebook utilizado por las personas responsables del secuestro de la menor.

Realizando vigilancias estáticas en la dirección obtenida y mediante el análisis de videos e imágenes que los victimarios enviaban a los familiares de la menor secuestrada se logró establecer que la residencia en donde tenían en cautiverio a la menor no era la residencia a la cual pertenecía el servicio de internet, se estableció que los victimarios robaban señal a los propietarios del servicio de internet. Al momento de establecer el inmueble donde se encontraba la menor secuestrada se procedió a solicitar orden de allanamiento en el inmueble en el cual se tenía la certeza que se encontraba la menor víctima de secuestro, logrando con esto el rescate de la menor y posterior la captura del responsable, Ver:

http://www.soy502.com/articulo/hijo-pastor-administrador-colegio-secuestrador

EXPERIENCIA EXITOSA POLICIA NACIONAL DE HONDURAS

El día 29 de enero de 2014, el (CENCOSS) Centro Nacional de Control y Seguimiento de Seguridad recibió un mensaje por medio de comunicación electrónica de la compañía celular TIGO, que provee servicios de GPS para la Secretaria de Seguridad, en el cual se reporta que una persona (Anónima), utilizando Facebook consulto a la compañía sobre que numero de línea corresponde al número de tarjeta SIM 5555###, por lo que la compañía procede a verificar los datos proporcionados y encuentra que corresponde a un dispositivo GPS asignado a la Red Oficial de la Policía Nacional, ante este hecho la compañía pregunto a esta persona si él es el propietario de dicha línea, a lo que responde "el numero pertenece a un GPS que estoy reparando por el cual necesito esa información" finalizando la conversación.

ANEXO "F" Captura de pantalla del chat de Facebook realizada por Luis Reinaldo Rodríguez Elvir

Fotografías relacionadas a la cuenta de Facebook de Luis Reinaldo Rodríguez Elvir.

En vista de lo anterior, este Centro dio ejecución al procedimiento de verificación de dispositivos móviles (GPS vehicular y otros) en la plataforma de virtual de Control Monitoreo y Seguimiento encontrando la siguiente información:

1. El número de tarjeta SIM 5555### proporcionado, según la base de datos de la compañía proveedora del servicio está asociado a otro número, que según la base de datos de control de instalación de GPS a vehículos de la Policía Nacional corresponde a un vehículo marca Nissan, con serie de GPS, instalado en Tegucigalpa.

2. Posteriormente el día 30 de enero del 2014, aproximadamente a las 14:30 horas este centro procedió a localizar el vehículo involucrado que según la plataforma de control monitoreo y seguimiento, el cual estuvo estacionado en las instalaciones de la Dirección Nacional de Tránsito.

   Así mismo se envió un equipo conformado por funcionarios policiales y los técnicos representantes de la compañía proveedora del Servicio GPS, con la finalidad de localizar el vehículo descrito anteriormente y verificar si el dispositivo GPS había sido manipulado por personal ajeno a la compañía proveedora del servicio.

   En dicha inspección se constató que el vehículo marca Nissan Frontier, doble cabina, color verde, año 2013, tipo pick up se encuentra en los inventarios de la Dirección Nacional de Transito, Según personal de transito dicho vehículo es normalmente utilizado por el funcionario policial.

Así mismo, el personal técnico confirmo que el sello de garantía del dispositivo GPS había sido removido y vuelto a pegar con súper pegamento.

Ver Anexo “A” Fotografías tomadas en el momento de la inspección.

ANEXO “A-1” Fotografías tomadas al momento de la Inspección

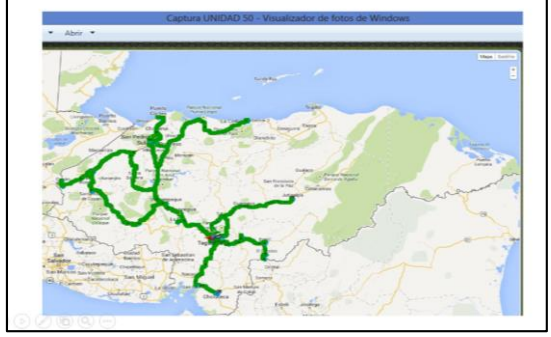
3. Se establecieron dos comunicaciones vía celular con el funcionario policial, quien nos consultó sobre lo que sucedía con el vehículo, se le informo que había un reporte sobre la posible violación al dispositivo GPS de un vehículo asignado a la Dirección Nacional de Tránsito, por lo que se requería el vehículo para que los técnicos lo inspeccionaran, minutos más tarde el vehículo fue puesto a nuestra disposición ya que se encontraba realizando diligencias, así mismo el señor funcionario policial manifestó que el vehículo pasaba mayormente estacionado en las instalaciones de la Dirección Nacional de Tránsito, que había sido utilizado para hacer auditorías a nivel nacional, y que días atrás había sido participante en una colisión junto con una motocicleta y que debido a los seguros se envió a reparar a un taller en la colonia San Miguel, que de ser necesario proporcionaría la información del mismo.

4. Se constató que el dispositivo había estado funcionando y que había hecho recorridos por los siguientes ejes carreteros:

   a. Tegucigalpa – Danli, frontera de las manos.
   b. Tegucigalpa – Choluteca.
   c. Tegucigalpa – Juticalpa.
   d. Tegucigalpa – Comayagua – Siguatepeque – San Pedro Sula – El Progreso – Choloma – La Lima – Puerto Cortes.
   e. San Pedro Sula – Santa Bárbara – Santa Rosa de Copan – Copan Ruinas – Gracias Lempira – La Esperanza.

Ver Anexo “C” captura de pantalla de ejes carreteros recorridos

ANEXO “C” Captura de pantalla de ejes carreteros recorridos por la unidad 50



5. Por otra parte, se llevó a cabo una investigación preliminar del nombre, según la base de datos de Investigación criminal, la información obtenida se cotejo con la Red Social de Facebook y se encontró lo siguiente:

   I. Que en dicha Red Social se encontró una cuenta con el Nombre: xxxxxxxx.

   II. Junto a este nombre y entre paréntesis se encuentra lo que parece ser un Alias, que se presenta como “Posho”.

III. También muestra una imagen con la inscripción en llamas CIBER YANROX, y como foto de perfil muestra a dos menores de edad del sexo femenino, se hace notar que dicha fotografía es la misma que se muestra junto al nombre que hizo la consulta a la compañía TIGO.

Ver Anexo “E” Captura de pantalla de la cuenta de Facebook con el hipervínculo respectivo, Anexo “F” Captura de la Pantalla del Chat de Facebook, en el cual se muestra la foto de las dos menores de Edad.

CONCLUSIÓN

Según las investigaciones preliminares realizadas podemos inferir que el dispositivo GPS había sido manipulado sin previa autorización con fines desconocidos, esto como resultado de la inspección llevada a cabo por personal técnico certificado de la compañía que hace las instalaciones del dispositivo GPS, por lo que se remite dicho informe a inspectoría General de la Secretaria de Seguridad para gestionar el procedimiento correspondiente.

ANEXO “E” Captura de pantalla de la cuenta de Facebook con el hipervínculo respectivo

https://www.facebook.com/luis.elvir.50/info?collection_token=100001632963943%3A2327158227%3A8

Primer Teniente **ALEXANDER FELIZ**
Encargado de la Sección de Inteligencia
Departamento de Investigaciones de Crímenes y Delitos de Alta Tecnología – DICAT
Policia Nacional de la Republica Dominicana

CASO DE ÉXITO CONTRA LA CIBERDELICUENCIA

En el año 2012, se llevamos a cabo una operación internacional simultánea denominada "UnMask", donde fueron realizados arrestos y allanamiento contra miembro de la organización Ciberterrorista denominada Anonymous, la misma fue ejecutada en España, Chile, Argentina, Colombia y República Dominicana. Dichas operaciones fueron realizadas en razón a que el grupo denominado "Anonymous Dominicano", habían realizados varios ataques informáticos a la infraestructura critica Nacional y a empresas privadas, mediante la metodología de ataques de denegación de servicios e inyección de SQL, para obtener credenciales de los servidores y bases de datos.

En el caso nuestro la metodología que utilizamos fue las siguientes:

1. Infiltración en la comunidad Anonymous, con el objetivo de identificar a sus líderes y miembros más activos, se identificó su ideología y que perseguían.

   La célula de Anonymous Dominicana no está totalmente organizada, está liderada por un individuo que se hace llamar Nmap en los canales de chat IRC, el cual es el fundador del canal de IRC #Anonymousdominicana

   Los Ciberterroristas de Anonymous gestionan todo lo que hacen mediante operaciones creadas por sus propios usuarios. Las operaciones son propuestas, modificadas y aprobadas por el colectivo, nadie crea una operación por libremente y sin consultar. Cuando las operaciones son aprobadas por una de la célula de anonymous, estas operaciones son distribuidas a través de diferentes servicios público de la Internet como YouTube, Twitter, Facebook, los Blogs, canales de chat IRC y Foro, en donde exponen el motivo del ataque y la fecha en la que se realizara el ataque. Ejemplo:

RESUMEN DE LOGS CON PARTE DE LAS CONVERSACIONES GRABADAS NMAP
Aug 16 20:14:14 * Nmap escuchen
Aug 16 20:14:47 * Nmap el pad ya está casi completado, me comunican de la cúpula que solo debemos pasar los targets ya cuando completemos el pad
Aug 16 20:15:19 * Nmap por favor vamos todos en este momento a discutir cuales serán los targets para la opmaleducados dominicana
Aug 16 20:16:11 * Nmap maleyco por favor
Aug 16 20:16:33 * Nmap dejen esos ayuntamientos tranquilos
Aug 16 20:16:46 * Nmap nos estamos centrando en una operación sobre la educación
Aug 16 20:17:13 * Nmap cuál sería el primer target???
Aug 16 20:17:46 <Nmap> secretaria de educación?
Aug 16 20:18:44 <Nmap> todavía no han publicado xtreme?
Aug 16 20:19:30 <Nmap> sería un gran llamado
Aug 16 20:19:33 <Nmap> nos haríamos sentir
Aug 16 20:19:35 <Nmap> es lo que buscamos
Aug 16 20:19:40 <Nmap> para que el estado se enderece
Aug 16 20:20:38 <Nmap> Opmaleducados en apoyo total a la mejoría de la educación
Aug 16 20:20:41 <Nmap> del 4%
Aug 16 20:41:01 <Nmap> * targets 1: www.seescyt.gov.do 2:http://www.see.gob.do 3:dgii.gov.do
Aug 17 23:08:48 * Nmap vamos todos a atacar

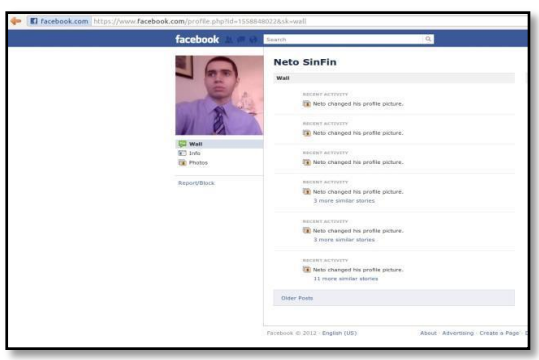
2. Levantamientos de logs en los servidores atacados, con la finalidad de obtener direcciones ips de los atacantes, ya que estos habían realizado un ataque de denegación de servicios (DDOS) a la página de la Dirección General de Impuesto Interno, en fecha 22 de agosto de 2011. Algunas de las direcciones IPs levantadas.

C-IP	DATE	TIME	TIME ZONE
64.32.97.7	22/08/2011	17:31:08	GMT/UCT 0:00
64.32.105.134	22/08/2011	15:22:55	GMT/UCT 0:00
64.32.107.14	22/08/2011	17:34:58	GMT/UCT 0:00
64.32.117.91	22/08/2011	16:53:55	GMT/UCT 0:00
64.32.126.144	22/08/2011	17:13:28	GMT/UCT 0:00
66.98.38.162	22/08/2011	16:51:51	GMT/UCT 0:00
66.98.71.70	22/08/2011	16:59:18	GMT/UCT 0:00
66.98.72.234	22/08/2011	16:55:47	GMT/UCT 0:00
66.98.89.94	22/08/2011	17:03:54	GMT/UCT 0:00
186.6.6.66	22/08/2011	17:13:15	GMT/UCT 0:00
186.6.14.63	22/08/2011	16:37:09	GMT/UCT 0:00
186.6.17.202	22/08/2011	16:58:58	GMT/UCT 0:00

3. Ingeniería social para obtener información sobre los próximos ataques a realizar.

4. Búsqueda de perfiles en las redes sociales, una vez identificados los miembros de esta célula, se procedió a solicitar las órdenes judiciales de arrestos y allanamientos. Ejemplo:

Perfil de Facebook de (xtreme):



5. Se incautaron los equipos utilizados por los arrestados y fueron enviados a los laboratorios forenses para realizarles las experticias correspondientes, ejemplo del análisis forense a unos de los equipos incautados:

Usuarios que contiene la instalación de Windows XP del disco duro WESTERN DIGITAL serial: WXE905391350 en el cual está el nombre de usuario MoT en la red de anonymous para realizar ataques en diferentes web del país.

Realizamos una búsqueda en la carpeta H:\Documents and Settings\MoT\Escritorio, en la cual se encuentran las siguientes carpetas en la ruta H:\Documents and Settings\MoT\Escritorio\Datos, donde hay se encuentra la aplicación llamada loic movile la cual se utiliza para realizar denegación de servicios de páginas web.

6. Luego se procedió a enviar a los arrestados y las evidencias encontradas ante el Ministerio Publico para su sometimiento.

Set fotográfico de personas sometidas a la acción de la justicia, como resultado de la operación.	Parte de las Evidencias Encontradas.
	

AMERIPOL

Modelo de Cooperación Policial para las Américas