



Está traducción es preliminar y no representa la versión final.

III CONGRESO MUNDIAL CONTRA LA EXPLOTACIÓN SEXUAL DE NIÑOS, NIÑAS Y ADOLESCENTES

**La Coalición Financiera contra la Pornografía Infantil:
Un caso de estudio sobre cómo el sector privado, la aplicación de la ley y las organizaciones no gubernamentales convergen para luchar contra la pornografía infantil comercial**

Objetivos

Este Libro Blanco trata de describir la mecánica, los beneficios y los retos de la Coalición Financiera contra la Pornografía Infantil (FCACP) para los participantes del Tercer Congreso Mundial. FCACP representa una colaboración única entre el sector privado, los órganos encargados de aplicar la ley y las organizaciones no gubernamentales (ONG). Es nuestra esperanza que los participantes del Tercer Congreso Mundial sean capaces de utilizar esta información para construir similares asociaciones público-privadas en todo el mundo.

Este documento:

- proporciona antecedentes sobre FCACP y sus organizaciones patrocinadoras, el Centro Internacional para Menores Desaparecidos y Explotados (ICMEC) y su agencia hermana, el Centro Nacional para Menores Desaparecidos y Explotados, con base en Estados Unidos (NCMEC);
- ofrece estadísticas y antecedentes sobre el problema de la explotación de los niños, y más específicamente, sobre la pornografía infantil comercial, y
- da ejemplos de cómo funcionan los mecanismos de trabajo de FCACP, sus logros y sus retos futuros.

Antecedentes

La Coalición Financiera contra la Pornografía Infantil, formada en 2006, es una organización pionera que aúna los esfuerzos de la industria privada y el sector público en la lucha contra la pornografía infantil. Se compone de los principales bancos, compañías de tarjetas de crédito y empresas procesadoras, empresas de pagos a terceros y empresas de servicios de Internet. FCACP está haciendo grandes avances en su objetivo de poner trabas a las economías basadas en la pornografía infantil, mediante el seguimiento de sus flujo de fondos y la cancelación de las cuentas de pagos que sean utilizadas por estas empresas ilegales.

Lo que hace única a la Coalición FCACP es el hecho de que no siga el modelo tradicional de responsabilidad social corporativa en cuanto a subsidios y contribuciones. Su enfoque es

fundamentalmente operativo y si bien algunas de las empresas han hecho contribuciones, esto no es un requisito para la participación.

FCACP está patrocinada y administrada por el Centro Internacional para Menores Desaparecidos y Explotados (ICMEC) y su Centro Nacional ubicado en Estados Unidos (NCMEC).

ICMEC trabaja identificando y coordinando una red mundial de organizaciones que luchan contra la explotación sexual infantil y el secuestro. La labor de ICMEC ofrece promesas a niños y familias mediante: el establecimiento de recursos globales para encontrar a los niños desaparecidos y prevenir la explotación sexual infantil; la creación de centros nacionales y filiales en todo el mundo; la construcción de una red internacional para difundir imágenes e información sobre los niños desaparecidos y explotados; proporcionar cursos de capacitación a los encargados de aplicar la ley, fiscales, jueces, profesionales del derecho, organizaciones no gubernamentales y funcionarios de gobierno; la promoción de cambios en las leyes, los tratados y los sistemas para proteger a los niños en todo el mundo.

Por su parte NCMEC es una organización sin ánimo de lucro, encomendada por el Congreso de los Estados Unidos y trabajando en asociación con el Departamento de Justicia de los Estados Unidos. Durante 24 años NCMEC ha operado bajo mandato del Congreso para actuar como el centro nacional de recursos y de información sobre los niños desaparecidos y explotados. Este mandato estatutario incluye funciones operativas específicas encomendadas por el Congreso de los Estados Unidos, tales como una línea telefónica 24 horas gratuita de información sobre niños desaparecidos y explotados llamada CyberTipline; un sistema de gestión de casos para los organismos encargados de aplicar la ley y las familias; asistencia técnica a las agencias encargadas de hacer cumplir la ley para identificar y localizar a delincuentes sexuales; una serie de programas para poner fin a la explotación sexual de los niños.

El Problema

Hacer frente al alarmante crecimiento de casos de explotación sexual de niños y adolescentes es una prioridad para los participantes del Tercer Congreso Mundial Definir el alcance del problema es un reto para la comunidad de defensa del menor. ICMEC y NCMEC ofrecen las siguientes estadísticas:

- En los 10 años que lleva funcionando CyberTipline, NCMEC ha recibido y procesado más de 600.000 informes. La inmensa mayoría de estos informes se refieren a la pornografía infantil. Hasta la fecha, los proveedores de servicios electrónicos han informado de más de 5 millones de imágenes de niños explotados sexualmente a CyberTipline. En 2007, NCMEC registró un aumento en los informes para casi todas las categorías: 23% de aumento en informes sobre pornografía infantil, 66% de aumento en informes sobre la incitación online; 58% de aumento en informes sobre prostitución infantil, 10% de aumento en los casos de turismo sexual con menores y un 9 % de aumento en informes sobre casos de abuso sexual infantil.
- Los jóvenes y los niños más pequeños están siendo víctimas, las imágenes son cada vez más gráficas y más violentas. De todos los delincuentes identificados en un estudio reciente realizado en los Estados Unidos, el 39% de éstos han estado en posesión de las imágenes de los niños menores de seis años, y el 19% imágenes de menores de 3.
- CyberTipline también recibe informes de los miembros de la Asociación Internacional de Proveedores de Líneas de Internet (INHOPE). Hasta la fecha, los miembros han enviado casi

50.000 informes manifestando casos de pornografía infantil a CyberTipline. Hay un total de 33 miembros de líneas directas de INHOPE ubicados en 29 países trabajando para eliminar los contenidos ilícitos de Internet.

En este contexto más amplio se ubica el crecimiento comercial de la pornografía infantil, es decir, los esfuerzos realizados por la delincuencia organizada y otros para obtener beneficio a partir de las imágenes de los niños, niñas y adolescentes que son víctimas de abusos sexuales. La pornografía sexual comercial se ha convertido en una industria multimillonaria y niños de todo el mundo están siendo utilizados como mercancías para su venta o comercio.

Con el fin de gestionar estos negocios las organizaciones delictivas debe acceder a la infraestructura de industrias ya establecidas. Como resultado, existen empresas de servicios financieros y empresas de servicios de Internet que a sabiendas o involuntariamente participan en este nefasto negocio. En consecuencia, es imperativo que el sector privado aúne esfuerzos en torno a los organismos encargados de la aplicación de la ley y las organizaciones no gubernamentales dedicadas a luchar contra la pornografía infantil comercial.

La Coalición Financiera contra la Pornografía Infantil

FCACP es una iniciativa única que combina los recursos de los sectores público y privado a fin de desarticular y desmantelar seriamente el negocio de la pornografía infantil comercial.

FCACP está compuesta por los principales bancos, compañías de tarjetas de crédito, compañías de pagos a terceros y empresas de servicios de Internet, y representa el 95% de la industria de pagos de los Estados Unidos. Su objetivo es erradicar la rentabilidad comercial que procede del negocio de la pornografía infantil, siguiendo el flujo de fondos y ordenando el cierre de las cuentas de los pagos que sean utilizados por estas empresas ilegales.

Antes de que FCACP empezara a operar en 2006, muchos de las empresas de pagos y empresas de servicios de Internet han estado combatiendo la pornografía infantil en los sitios web por sí mismos. Sin embargo, sus esfuerzos han sido insuficientes dada la magnitud del problema. Por su parte, FCACP permite un foro donde se pueden combinar recursos, experiencia y capital intelectual con el fin de hacer serios esfuerzos en esta lucha.

Los miembros de la FCACP son los siguientes:

America Online	Elavon
American Express Company	First Data Corporation
Authorize.Net	First National Bank of Omaha
Bank of America	Global Payments Inc.
The Bank of New York Mellon	Google
Capital One	HSBC – Norte América
Chase Paymentech Solutions	JP Morgan Chase
CheckFree	MasterCard
Citigroup	Microsoft
Deutsche Bank Americas	North American Bancard
Discover Financial Services	PayPal

ProPay Inc.
Premier Bankcard, LLC
Standard Chartered Bank
Visa

Washington Mutual
Wells Fargo
Western Union
Yahoo! Inc.

FCACP también se beneficia de los consejos proporcionados por bufetes de abogados, asociaciones financieras, expertos en seguridad cibernética y los reguladores estadounidenses.

Esta iniciativa reconoce que el gran número de personas que participan en esta industria en todo el mundo hace imposible el enjuiciamiento de todos ellos, sin importar lo agresivo del cumplimiento de la ley. FCACP, que es básicamente una iniciativa civil, surgió con un enfoque diferente: sobre la base de consejos de la línea CyberTipline, NCMEC identifica los sitios web que contienen imágenes ilegales, junto con el método de pago de dicha información. Esta información se transmite a los agentes federales de los EE.UU. encargados de hacer cumplir la ley, quienes hacen un seguimiento de las investigaciones de determinados sitios web, en un esfuerzo por reunir pruebas y determinar los contenidos ilícitos y la acción. Si la aplicación de la ley no deriva en un proceso judicial, la empresa es notificada y habrá de adoptar las medidas oportunas a cuenta de sus términos de servicio.

Logros

Hay una serie de tendencias positivas que sugieren que los esfuerzos de la FCACP y los organismos encargados de la aplicación de la ley están teniendo un impacto en el negocio de pornografía infantil comercial.

Por ejemplo, se ha hecho más difícil el uso de la tarjeta de crédito en las operaciones encubiertas. Si la aplicación de la ley tiene problemas para hacer estas operaciones, es lógico que el consumidor también los tenga. Y el precio de compra de estas imágenes de niños explotados sexualmente ha aumentado dramáticamente - indicación de que los esfuerzos de FCACP pueden estar afectando la rentabilidad de estos sitios.

FCACP se ha centrado en lograr una mejor comprensión de cómo las compras de pornografía infantil comercial se ha incluido en el sistema de pagos en el pasado, como medida para evitar situaciones similares en el futuro. El resultado de esa labor fue la publicación de la "Adquisición de Comercio en Internet y Seguimiento de Mejores Prácticas para la Prevención y Detección de la Pornografía Infantil Comercial". El Organismo controlador de la Moneda de EE.UU. (OCC) y la Corporación federal de Depósitos de Seguros de EE.UU. distribuyeron dicho documento a los ejecutivos de los bancos en todo el país y a otros grupos interesados como un servicio a NCMEC y FCACP. Adicionalmente, la OCC emitió un comunicado de prensa anunciando esta iniciativa.

FCACP publicó su segundo Libro Blanco de mejores prácticas en 2008, publicación a la que se hace referencia a continuación.

Retos por cumplir

FCACP está haciendo progresos significativos en los Estados Unidos. Como siguiente paso, es fundamental que el modelo se expanda a otros países para hacer frente a este problema mundial. El

objetivo de FCACP es perturbar la economía de los negocios de pornografía infantil mediante la creación de alianzas con empresas financieras y compañías de Internet, organizaciones no gubernamentales, expertos jurídicos y organismos encargados de hacer cumplir la ley, así como la elaboración de soluciones que sean armoniosas con las leyes locales y costumbres. Las regiones objetivo incluyen Europa y Asia Pacífico.

En términos generales, las empresas se acercan a NCMEC y ICMEC y piden unirse a FCACP. Algunas de estas instituciones son marcas bien conocidas que operan bajo sistemas de control regulatorio amplio. Otras son menos conocidas, pero son potencialmente importantes en los nuevos métodos de pago que están surgiendo. Es importante supervisar a los nuevos solicitantes de pantalla a fin de asegurarse de que su modelo de negocio, su ética corporativa y su reputación son coherentes con los objetivos de FCACP. Un recientemente desarrollado Proceso de Selección está siendo actualmente objeto de prueba.

Dado que se presiona a los sitios web de pornografía infantil comercial, las empresas que los ejecutan están evolucionando. Esto es especialmente cierto en las áreas de hosting de espacios web y de instrumentos alternativos de pago. El Grupo de Trabajo Desafíos de la Tecnología, de FCACP, publicó recientemente un libro blanco sobre esos temas. Ese documento se presenta como una adición a este resumen debido al valor de su contenido, y porque es una sólida demostración de los beneficios de la colaboración de la que FCACP es parte integrante.

Adición: Informe de 2008 del Grupo de Trabajo Desafíos de la Tecnología. "Tendencias en la Migración, Acogida y el Pago de los sitios web de pornografía infantil comercial".

- FIN -

**INFORME 2008 DEL GRUPO DE TRABAJO DESAFÍOS DE LA TECNOLOGÍA:
"TENDENCIAS DE LA MIGRACIÓN, LA ACOGIDA Y EL PAGO DE
LOS SITIOS WEB DE PORNOGRAFÍA INFANTIL COMERCIAL"**

Antecedentes

La Coalición Financiera contra la Pornografía Infantil (la Coalición) se formó en 2006 para hacer frente al alarmante crecimiento en el comercio de pornografía infantil a través de Internet. Sus miembros incluyen líderes en la banca y las industrias de pagos, así como empresas de servicios de Internet. Una de los cometidos de la Coalición es seguir y anticipar la forma en que la mecánica comercial de la pornografía infantil está evolucionando. Con ese fin, el Grupo de Trabajo de Desafíos de la Tecnología de la Coalición (TCWG) ofrece las siguientes observaciones.

Cláusula de exención de responsabilidad

Este Informe (el Informe) fue creado y escrito por voluntarios, en nombre de TCWG y representa el punto de vista actual de TCWG sobre las cuestiones abordadas a partir de la fecha de publicación. El contenido se basa en la aportación individual de los contribuyentes, y no necesariamente reflejan las opiniones o políticas de las empresas en las que las personas trabajan. Puede haber inexactitudes e información que ha quedado obsoleta desde que el presente Informe fuera originalmente escrito.

Este Informe es sólo de referencia y no pretende proporcionar un asesoramiento jurídico específico, financiero o empresarial. En el caso de que necesite asesoramiento específico o un abogado, se recomienda consultar con un profesional adecuado. TCWG NO OTORGA NINGUNA GARANTÍA, EXPRESA, IMPLÍCITA O LEGAL, EN CUANTO A LA INFORMACIÓN CONTENIDA EN ESTE INFORME. La citación o listado de una organización o entidad en este documento no implica ningún tipo de respaldo por parte de tal organización o entidad.

Es de su responsabilidad el cumplir con todas las leyes sobre los derechos de autor. Este informe puede ser redistribuido libremente en su totalidad y de forma gratuita a condición de que cualquiera de sus avisos legales, incluidos todos los avisos de copyright, no se quiten. No podrá ser vendido con fines de lucro o utilizado en documentos comerciales sin el permiso escrito de TCWG, pudiendo ser retenidos a discreción de TCWG.

Tendencias en Migración

El problema central para los gobiernos y encargados de aplicar la ley que tratan de hacer frente al comercio online de pornografía infantil (CCP) es el anonimato inherente que proporciona Internet. Los delincuentes cuentan con múltiples modos para defender sus operaciones online, en última instancia gracias al anonimato de sus transacciones seleccionadas y el contenido medio.

A saber:

- ❖ El contenido de material comercial pornográfico (CCP) puede ser acogido en países que no lo persiguen, alejados de recurso legal directo, o puede ser involuntariamente alojado en un sistema de plataformas de ordenador que a su vez han sido captadas por proveedores de CCP técnicamente cualificados.
- ❖ El pago online para ver material comercial pornográfico es, en efecto, anónimo. Aunque los proveedores tradicionales de pago son los bancos o instituciones semi-bancarias que siguen la normativa bancaria nacional, TCWG observa una tendencia hacia nuevos ("alternativas") servicios de pago y entidades financieras, cuya condición de no-banco les da derecho a eludir el cumplimiento de las normas que les exige conocer las identidades del ordenante y del beneficiario.

El problema central a la hora de detectar y prever los contenidos online de pornografía infantil es que Internet provee un espacio anónimo en el que los delincuentes cibernéticos pueden operar con relativa impunidad y llevar a cabo una multitud de delitos, además de la venta de tales contenidos. El anonimato facilita las operaciones de intercambio online de material pornográfico de tres maneras: la facilidad de ocultación del contenido almacenado, la capacidad de los criminales de operar rápidamente en los sitios dinámicos de pago ("hasta el día de hoy, por mañana, hasta el día siguiente") para evitar la detección, y la falta de regulación de los nuevos métodos alternativos de pago.

En general Internet está salpicado de vínculos de pornografía infantil (child pornography links, CPL). Algunos de estos sitios tienen un número de redirecciones, eventualmente, moviendo al cliente potencial hacia un dominio no relacionado. Cuando un consumidor potencial llega a un sitio que ofrece hacerse miembro del sitio a cambio de una tarifa, varias cosas pueden ocurrir. El sitio de acogida puede ofrecer la opción de hacer el pago mediante tarjeta de crédito. En ese momento una página web no cifrada puede ser usada para documentar el nombre, dirección, teléfono y tarjeta de crédito. La mayoría de los CPL ofrecen pagar el ingreso como miembro de estos sitios mediante tarjeta de crédito sin el uso de la tecnología de la página https, lo que expone al consumidor a un alto grado de riesgo. La información es vulnerable a ser explotada por los delincuentes cibernéticos. TCWG sólo puede explicar que los CPL elijan no obtener un certificado SSL debido a que eso les haría sacrificar parte de su anonimato.

Algunos sitios ofrecen material de pornografía infantil para la venta a través de confirmación vía correo electrónico. El cliente envía un mensaje de correo electrónico a una persona desconocida para completar la transacción, utilizando a veces las transferencias de dinero en la web (webmoney) o simplemente utilizando el servicio de correos de EE.UU. para enviar dinero en efectivo. Sin embargo, otros sitios ofrecen la opción de ser miembro de contenidos CCP, pero redirigiendo al cliente a un sitio agregador de pago con tarjeta de crédito. Algunos de estos agregadores ofrecen transacciones seguras y no seguras. Estos agregador de sitios en general: no cifran las transacciones con tarjeta de crédito, y falsifican paginas para hacer que los espacio para transacciones con tarjeta de crédito parezcan páginas legítimas y semi-legítimas con terceros procesadores. Aunque TCWG no ha visto un descenso significativo en el número de sitios de pago por contenidos de CPP, sí ha visto una disminución en el éxito de la identificación de los sitios de CCP probablemente gracias a una aplicación más estricta de aquéllos que se benefician de los CCP, debiendo hacer más esfuerzos por identificar estos espacios.

Empresas de Hosting

Muchas empresas de acogida de Internet se han convertido en conductos para el almacenamiento de los contenidos de pornografía infantil comercial (CCP). Con ese fin, en la mayoría de los casos, sitios URL o de marca deben rotar a través de decenas de comerciantes y posibles métodos de pago hasta que cada uno está apagado. La marca de los sitios a continuación, deberá establecer nuevas cuentas y métodos de pago. De esta manera, es posible que un sitio individual haya tenido tanto su contenido como sus capacidades de pago eliminadas en varias ocasiones sólo para copia de seguridad de los nuevos hosts y comerciantes. Para el observador casual, sin embargo, parece que estos sitios han seguido funcionando sin intervención. Pero para los ojos experimentados y educados, está claro que estos sitios han sido repetidamente deshabilitados sólo para poder reaparecer. La inutilidad de este proceso puede compararse con el "Whack-A-Mole" juego que los niños disfrutaban.

Curiosamente, los contenidos "white label" (aparentemente inofensivos) y los URL tienen un ciclo de vida completamente diferente. Normalmente, estas URL se utilizan simplemente para redireccionar a los consumidores temporalmente hacia contenidos de etiqueta blanca o inofensiva, o hacia la ubicación temporal de contenidos de marca. En este sentido, estas URL son los "carne de cañón" en la actual batalla por la viabilidad comercial. De hecho, es posible ver 10-20 diferentes URL aparecer en días en campañas de spam en masa, donde todas las URL acaban por alojar el mismo contenido de marca.

Actualmente muchas compañías de hosting simplemente se centran en la fiabilidad y la fijación de precios y la mayoría no tienen políticas escritas con respecto a posibles contenidos ilícitos. En algunos casos sus términos de uso contienen acuerdos que establecen que la recepción de cualquier contenido ilegal por parte de sus clientes podría dar lugar a la rescisión del servicio. Sin embargo hacer cumplir de manera proactiva estos acuerdos es la cuestión clave. En términos generales, los hosts no revisan los contenidos de la pantalla, y dependen de los informes que digan que son espacio de alojamiento de material CCP antes de estar dispuestos a tomar medidas. TCWG ha sido asesorado por un experto jurídico a cerca de que los espacios de almacenamiento no han consultado a un abogado o alguien con conocimientos sobre el tema para dar respuesta a las denuncias acerca de este material sino que hacen su propia investigación interna; el mismo experto afirma que se trata de una práctica arriesgada y mal aconsejada por las siguientes razones: a) el papel del espacio de almacenaje o host no debe ser el de fiscalizador de contenidos, b) los espacios de almacenamiento de información no están calificados para determinar lo que constituye material CCP; y c) los espacios hosts podrían estar violando las leyes relativas a la posesión de material de contenido pornográfico comercial. Aquellos que han buscado asesoramiento jurídico tienen los procedimientos institucionales pertinentes para aislar el material e informar de éste al Centro Nacional para Menores Desaparecidos y Explotados (NCMEC).

El primer paso sería lograr que las empresas de hosting adoptaran mejores prácticas. Investigaciones hechas por TCWG han demostrado que actualmente no existe una organización de comercio de espacios de almacenamiento de sitios de Internet similar a la Asociación de Proveedores de Servicios de Internet

¹ **Un servicio de alojamiento web** es un tipo de servicio de alojamiento de Internet que permite a individuos y organizaciones proporcionar sus propios sitios web accesibles a través de la World Wide Web. Las web hosts son compañías que proporcionan espacio en un servidor propio para su uso por parte de sus clientes, así como proporcionan la conectividad a Internet, típicamente en un centro de datos. Véase http://en.wikipedia.org/wiki/Web_hosting.

de Estados Unidos. Tal organización sería útil en el establecimiento de estándares de la industria y podría servir como un mecanismo para responder a las preocupaciones de TCWG.

La siguiente lista sirve para destacar y recomendar un nivel mínimo de diligencia debida por parte de las empresas de hosting, con el propósito de erradicar el almacenamiento de material CCP.

- Política de Pornografía Infantil: Mantener una política sobre cómo detectar y reaccionar a la acogida y el almacenamiento de material CCP. La siguiente web del sitio de acogida ha sido sugerida por un experto jurídico como una que trata la cuestión del contenido CCP: <http://www.peakinternet.com/legal/aup/>. Si bien TCWG no apoyar este ejemplo como un modelo, sí al menos lo presenta como uno que intenta abordar la cuestión.
- Seguimiento: Los frecuentes cambios en los métodos, la tecnología, la URL, etc. son claramente esfuerzos deliberados utilizados por los delincuentes para evitar la detección. También acuden a otras medidas con objeto de mantener su anonimato. TCWG, por lo tanto, recomienda que los espacios de almacenamiento establezcan la búsqueda de sitios conocidos por contener material CCP sobre una base trimestral y con el objetivo de la revisión semanal de todos los sitios activos. Spider y la tecnología bot existen para ayudar a localizar a todo aquello asociado al léxico de CCP y a imágenes con facilidad. Una vez encontrados, estos sitios deberían ser destituidos por el host.
- Filtrado WRT: Muy parecido a lo que hacen los Proveedores de Servicios de Internet actualmente, cuando utilizan la tecnología para librarse de sus sistemas de aquel material que resulte ilegal, deberían hacer los hosts, y así eliminar todos los contenidos ilícitos de sus servidores.
- Intercambio de información con NCMEC por medio de Nefarious Hosts (por ejemplo, los hosts que almacenan contenidos ilícitos): De conformidad con sus políticas, a los hosts se les anima a compartir la información que poseen con el NCMEC, en relación con las personas o empresas que se cree que participan en la distribución de material CCP.
- Conducta de debida diligencia sobre los clientes: Al igual que los bancos se han visto obligados a adoptar políticas de "conozca a su cliente" para evitar ser utilizados por los narcotraficantes y terroristas para operaciones de lavado de dinero, los alojadores de sitios de Internet deberían ser alentados, si no requerido como necesario, a cabo la debida diligencia sobre los clientes y sobre sus contenidos.

Por último, se prevé que la Coalición pueda considerar la posibilidad de crear una "lista negra" de empresas que son conocidas, ya sea a sabiendas por contener material CCP o en la práctica voluntaria de omisión, y otros que no están dispuestos a seguir los cinco pasos de la debida diligencia citados anteriormente.

Servidores Corporativos comprometidos como anfitriones de material CCP

Constantemente ocurre que los espacios en una red corporativa de seguridad son abiertos por los criminales con malas intenciones, tomando el control de un usuario remoto conectado a una red y, a su vez, comprometiendo a toda la red, al dejar tanto la propiedad intelectual como los datos financieros

vulnerables a la explotación delictiva, o en el caso de material CCP, a distribuir desde estas redes comprometidas.²

Imagine que el servidor de una importante corporación, universidad, o institución financiera fuera interceptado y se alojaran una serie de contenidos de CCP para su venta. La evidencia de posibles brechas en la seguridad hace que este pensamiento no sólo sea posible sino probable. La lista de las mejores prácticas en el apéndice debería ser compartida con CTOS y CIOs de instituciones miembros de la Coalición.

Sistemas de Pago Telemáticos

En la Introducción al Informe de diciembre de 2005 "EE.UU., Evaluación de la Amenaza del Blanqueo de Dinero Nacional" (NMLTA)³ el Gobierno de los EE.UU. declaró que "los criminales disfrutaban de nuevas ventajas con la globalización y el advenimiento de nuevos servicios financieros tales como tarjetas de valor almacenado y servicios de pago en línea". La NMLTA identificó y evaluó trece amenazas financieras sistémicas contra los Estados Unidos y, de las trece, dos -los sistemas de pago en línea y las tarjetas de valor almacenado- representan nuevos capítulos que no han aparecido en este tipo de informes de NMLTA hasta hace unos pocos años. Estas nuevas y cambiantes amenazas en el sistema financiero, basado en parte como una respuesta a las demandas de carecen de él, y, en parte, en respuesta a la globalización de los sistemas financieros y sus reacciones a la realidad de Internet, plantean amenazas potenciales a partir de usos criminales e ilícitos no sólo a la economía de los EE.UU., sino también a la economía mundial.

Como el NMLTA afirmó, "[n]uevos e innovadores servicios de pago telemáticos a nivel mundial están surgiendo en respuesta a la demanda del mercado de particulares y comerciantes online... comerciantes [O]nline, en particular de aquellos sectores con altas tasas de 'carga', están generando demanda de nuevos métodos de pago. Hay cientos de estos sistemas de pago online. Estos mercados generan una serie de sistemas de pago online que establecen sus propios mecanismos de compensación y liquidación al margen de cualquier normativa de protección de los consumidores. Normalmente las transacciones a través de los proveedores de estos servicios se considerarán definitivas sin recurso para las personas que creen haber sido defraudadas. La consecuencia, de acuerdo con los organismos encargados de hacer cumplir la ley federal, es que estos sistemas se han convertido en los mecanismos favoritos de pago online para los autores de fraudulentos planes de inversión y otras actividades ilegales".⁴

NMLTA presentó un panorama general sobre "los servicios de la moneda digital" tales como el recientemente acusado de e-gold, Ltd, así como otros sistemas de pago online. NMLTA evaluó la vulnerabilidad de estas nuevas tecnologías señalando que los transmisores de dinero están obligados a inscribirse con FinCEN,⁵ y están sujetos a tomar medidas contra el blanqueo de dinero, a obligaciones de registros y requisitos de presentación de informes, así como, en general, los requisitos de concesión de licencias estatales. Los requisitos contra el blanqueo de dinero (AML) de un sistema de pago online o una moneda digital "depende de su ubicación y la forma en la que participa en las operaciones o conductas"⁶.

² Consulte <http://www.securityfocus.com/brief/691>.

³ Consulte <http://www.treas.gov/press/releases/docs/nmls.pdf>.

⁴ NMLTA en 25.

⁵ Centro Financiero del Tesoro de los Estados Unidos.

⁶ NMLTA en 27.

Estos nuevos y cambiantes mecanismos de pago, incluidos los dos que no se abordan en la NMLTA - juegos en línea, tales como Entropia Universe, que tienen sus propias monedas convertibles con vínculos con la capacidad del mundo real de sacar dinero, así como la llegada de la banca móvil a través de teléfono móvil – apuntan al cambio radical del paisaje de los métodos tradicionales de dinero en efectivo, cheque y tarjeta de crédito. Estos nuevos mecanismos de pago, especialmente cuando actúan en conjunto con Internet, puede facilitar nuevas formas de delincuencia o generar nuevas actividades delictivas que no podría haber ocurrido sin el uso de las tecnologías mismas. El flujo financiero puede ser el origen del delito, o el mecanismo de blanqueo para mover el producto, una vez generado.

El Grupo de Acción Financiera Internacional de las 34 naciones ("GAFI"),⁷ en octubre de 2006, publicó un informe ⁸ que examinaba la forma en que el dinero puede ser blanqueado a través de la explotación de las nuevas tecnologías de pago (tarjetas de pago, Internet de los sistemas de pago, los pagos por teléfono móvil y metales preciosos digitales). El informe mostró que, si bien existe una legítima demanda del mercado de estos métodos de pago, éstos resultan altamente vulnerables al blanqueo de capitales y la financiación del terrorismo. En concreto, los proveedores transfronterizos de nuevos métodos de pago pueden representar más riesgo que los proveedores que operen exclusivamente dentro de un determinado país. El informe del GAFI recomienda mantener la vigilancia por parte de todos los países y evaluar el impacto de la evolución de las tecnologías en las transacciones y los marcos normativos nacionales. Sin embargo, dado el nivel de corrupción o de colusión por parte de algunos gobiernos extranjeros en diversos tipos de actividades delictivas, una estricta supervisión y la ejecución de las transacciones financieras es poco probable.

PayPal ha mostrado un extraordinario nivel de diligencia debida como ejemplo de sistema de pago online y puede ser un modelo para otros en la industria. A través de políticas racionales, modelos de propiedad, de auditoría y medios de investigación, y las asociaciones públicas / privadas, PayPal demuestra un rigor que otros sistemas de pago telemáticos deberían emular, a fin de frustrar el pago de la pornografía infantil. PayPal, sus políticas y procedimientos de diligencia debida se detallan a continuación:

Política

- PayPal tiene política de tolerancia cero a la hora de usar su sistema para cualquier material y servicios ilegales.
- El Acuerdo de Usuario de PayPal establece claramente que cualquier cuenta que ofrezca materiales y/ o servicios ilegales viola la política de uso y será por tanto objeto de cierre inmediato.

Modelos y Otras Herramientas de Detección

- PayPal tiene modelos de propiedad que están diseñados específicamente para la explotación de niños.
- PayPal tiene más de 1700 palabras clave en varios idiomas construido en herramientas de modelaje.
- PayPal invierte fuertemente en la supervisión y herramientas de detección en el ámbito de la explotación infantil.

⁷ Desde su creación, el GAFI ha encabezado los esfuerzos internacionales para adoptar y aplicar medidas destinadas a contrarrestar la utilización del sistema financiero mundial por los delincuentes. Se estableció una serie de 40 recomendaciones en 1990, revisadas en 1996 y en 2003, para asegurarse de que sean actualizados y pertinentes a la evolución de la amenaza del blanqueo de capitales.

⁸ http://www.fatfgafi.org/document/17/0,3343,en_32250379_32237217_37627409_1_1_1_1,00.html.

- PayPal, utiliza herramientas de rastreo y analiza su sistema interno y externo en la web en busca de violaciones.
- Tanto las palabras clave como las técnicas de modelado se actualizan semanalmente.
- PayPal alienta a cualquier persona que tenga información sobre el potencial uso ilegal de PayPal, a ponerse en contacto con la empresa

Auditoría

PayPal involucra a varios agentes a la hora de "rastrear" las web en busca de posibles violaciones asociadas con su marca.

Agentes de investigación, analista, y Equipo Mundial de Aplicación de la Ley de Operaciones

- PayPal cuenta con un equipo de cerca de 100 agentes a nivel mundial (en Omaha, Dublín, y Shangai) que buscan, examinan e investigan violaciones de alto riesgo, incluidos los relacionados con la explotación infantil.
- Además, PayPal cuenta con un equipo de agentes especializados que trabajan exclusivamente en el ámbito de la lucha contra la explotación de los niños - formados durante varios años por el NCMEC y que son examinados regularmente para comprobar los conocimientos sobre el tema.
- PayPal invierte fuertemente en la capacitación y programas de mentores para su equipo de investigadores y analistas, incluidos los de capacitación interna y externa, bibliotecas online, y otros recursos que garanticen que PayPal tiene los más actualizados materiales de referencia.
- PayPal tiene un programa de investigación donde los agentes investigan las tendencias de la industria, noticias y eventos, y exploran la tecnología de próxima generación.

Asociaciones públicas y privadas

- PayPal trabaja en estrecha colaboración con el Departamento de Inmigración y Aduanas estadounidense, el FBI y otros organismos reguladores para garantizar que está bien informado en los problemas con contenidos ilegales.
- PayPal ha tenido varios representantes de la aplicación de la ley como invitados a su Centro Global de Operaciones en Omaha, como parte de su Programa de distinguidos oradores para la formación.
- Como parte de su Equipo de Cumplimiento de la Ley Global de Operaciones, PayPal cuenta con abogados de EE.UU. y profesionales de la industria que trabajan en estrecha colaboración con sus homólogos en la aplicación de la ley, los organismos reguladores, y las organizaciones no gubernamentales para fomentar la comunicación y para colaborar en las investigaciones.

Conclusión

La migración de los medios de pagos de materiales de contenido pornográfico y empresas de web hosting fuera de los vehículos financieros y modelos conocidos, es una tendencia muy difícil que requiere no sólo

la atención sino también una mayor comprensión y, como en otros aspectos de comercio por Internet, tal vez una mayor regulación. La economía subterránea y la distribución de CCP son dinámicas y flexibles ante los mejores esfuerzos de la Coalición por combatirlo. Al tiempo que las diversas industrias relacionadas con Internet maduran y entran en la comunidad de buenos ciudadanos corporativos, es decisivo para la Coalición el alentarlos a adoptar buenas políticas, como las de diligencia debida y un cierto grado de filtrado y seguimiento de sus sitios alojados.

APÉNDICE: GUÍA PRÁCTICA DE SEGURIDAD DEL SERVIDOR WEB⁹

Servidor Web de Seguridad
1. Recuerde que la instalación por defecto de HTTP puede dar lugar a ataques DDoS y a la exposición de información confidencial haciendo al servidor vulnerable a un ataque.
2. Use SSL o SSH.
3. No ejecute otras aplicaciones en el sistema. Límitese a HTTP y otros servicios necesarios.
4. Aplique la versión más reciente del Service Pack, actualizaciones y parches.
5. Cuestiones de control de acceso: restrinja la lista de usuarios con acceso de servidor Web mediante la utilización de la autenticación de factor dos.
6. Lleve a cabo una prueba de permeabilidad con comprobaciones de los niveles de vulnerabilidad asociados analizando los servidores web ante posibles vulnerabilidades críticas.
7. ¿Se aplica el cambio de control para reducir el riesgo global? ¿Se siguen y controlan los cambios en el sistema?
8. Elimine cualquier muestra de programas CGI del servidor.
9. Ejecute la aplicación web escáner para simular un ataque de la página web y determinar su seguridad. Ejecútela con frecuencia durante la fase de diseño y ponga en práctica semanal exploraciones para comprobar si hay nuevas vulnerabilidades.
10. Revise todos los registros con frecuencia. Todos deben estar encendido. Si es posible uno debe empujar a todos los registros de ubicación central para comprobar si las tendencias o similitudes entre otros servidores web.
11. Planee cuidadosamente y ocúpese de la seguridad los aspectos del despliegue de cualquier servidor web público. ¹⁰
12. Aplique prácticas de gestión de la seguridad y los controles cuando haga el mantenimiento y la explotación de una presencia segura en la Web. ¹¹
13. Con el fin de garantizar la seguridad del servidor web y el apoyo a la infraestructura de la red, las siguientes prácticas deberían aplicarse: <ul style="list-style-type: none">▪ Organización en todo el sistema de información de la política de seguridad.▪ Configuración / control de cambios y la gestión.

⁹ World Bank Treasury Technology Risk Checklist 7.3.

¹⁰ Dado que es mucho más difícil determinar las cuestiones de seguridad una vez que el despliegue y la aplicación se han producido, la seguridad debe considerarse desde la etapa de planificación inicial. Las Organizaciones tienen más probabilidades de tomar decisiones acerca de cómo configurar adecuada y coherentemente los ordenadores cuando se desarrolla y utiliza un detallado y bien diseñado plan de despliegue que también considere la seguridad. El establecimiento de este tipo de planes guía a las Organizaciones en la toma de las decisiones a la hora de elegir entre utilidad, rendimiento y riesgo. Las organizaciones a menudo no toman en consideración las necesidades de recursos humanos tanto para el despliegue y las fases operacionales de la web del servidor e infraestructura de apoyo. Las organizaciones deberán abordar los siguientes elementos en un plan de despliegue:

- Tipos de personal necesario (por ejemplo, el sistema y los administradores de web, web master, los administradores de red, sistemas de información oficiales de seguridad [ISSO]);
- Habilidades y formación requeridas por el personal asignado;
- Requisitos de mano de obra individual (nivel de esfuerzo exigido a los tipos específicos de personal) y colectiva (nivel general de esfuerzo).

¹¹ Las prácticas de gestión adecuadas son esenciales para el funcionamiento y el mantenimiento de un servidor web seguro. Las prácticas de seguridad supondrá la identificación por parte de una organización del sistema de información de activos y el desarrollo, documentación, y la aplicación de políticas, normas, procedimientos y directrices que garanticen la confidencialidad, integridad y disponibilidad de los recursos del sistema de información.

- Evaluación y gestión de riesgos.
- Normalización de configuraciones de software que satisfagan la política de seguridad del sistema de información.
- Seguridad de sensibilización y formación.
- Planificación, continuidad de las operaciones y recuperación de desastres.