



Это перевод является черновым

III ВСЕМИРНЫЙ КОНГРЕСС ПРОТИВ СЕКСУАЛЬНОЙ ЭКСПЛУАТАЦИИ ДЕТЕЙ И ПОДРОСТКОВ

**Финансовая Коалиция Против Детской Порнографии:
Пример того, как частный сектор, правоохранительные органы и неправительственные организации объединяются для борьбы с коммерческой сексуальной эксплуатацией**

Цели

Этот документ представляет участникам III Всемирного конгресса механизмы, пользу и вызовы Финансовой Коалиции Против Детской Порнографии (ФКПДП)/ Financial Coalition against Child Pornography (FCACP). ФКПДП - это пример уникального сотрудничества частного сектора, правоохранительных органов и неправительственных организации (НПО). Мы надеемся, что участники III Всемирного конгресса смогут использовать эту информацию для построения подобного сотрудничества в других странах мира.

Данный документ содержит:

- информацию о ФКПДП и поддерживающих его организаций, Международном центре для пропавших и пострадавших от эксплуатации детей/International Centre for Missing & Exploited Children (ICMEC) и его сестринской организации Национальном центре для пропавших и пострадавших от эксплуатации детей, США/ National Centre for Missing & Exploited Children (NCMEC);
- статистические данные и описание проблемы эксплуатации детей и коммерческой детской порнографии в частности;
- примеры того, как работают механизмы ФКПДП, информацию о том, что уже достигнуто и с какими сложностями еще предстоит столкнуться.

История

Финансовая Коалиция Против Детской Порнографии (ФКПДП/ FCACP), сформировавшаяся в 2006, является союзом частного и общественного сектора в борьбе с детской коммерческой порнографией. Она состоит из крупнейших банков, кредитных союзов, других коммерческих структур, кампаний, предоставляющих Интернет услуги. ФКПДП делает большой шаг вперед к своей цели по искоренению коммерческой детской порнографии путем отслеживания денежных потоков и закрытия тех, которые используются противозаконными структурами.

То, что делает ФКПДП уникальной структурой – отказ от следования традиционной модели социальной ответственности в виде грантов и пожертвований. Она имеет операционный фокус и в то время, как некоторые компании делают пожертвования, это не является условием для участия.

ФКПДП финансируется и управляется Международным центром для пропавших и пострадавших от эксплуатации детей и Национальным центром для пропавших и пострадавших от эксплуатации детей, США.

ИСМЕС осуществляет идентификацию и координацию глобальной сети организаций, борющихся с детской сексуальной эксплуатацией и похищениями. Деятельность ИСМЕС дает надежду детям и семьям путем создания глобальных возможностей для поиска пропавших детей и предотвращения сексуальной эксплуатации детей; создания национальных центров и отделений по всему миру; построения международной сети для распространения фотографий и информации о детях, которые исчезли и подверглись эксплуатации; проведения тренингов для представителей правоохранительных органов, прокуроров, судей, юристов, представителей неправительственных организаций и государственных структур; лоббирования изменений в законодательстве, соглашениях и систем по защите детей во всех странах мира.

НСМЕС это неприбыльная организация подмандатная Конгрессу США и работающая в партнерстве с Департаментом юстиции США. В течении 24 лет НСМЕС работала под мандатом Конгресса и служила национальным ресурсным центром по пропавшим и подвергнувшимся эксплуатации детям. Мандат включает специфические операционные функции, предписанные Конгрессом США, включая круглосуточную работу «горячей линии» - CyberTipline для сообщения информации о пропавших и подвергшихся эксплуатации детей; систему кейс менеджмента для правоохранительных органов и семей; техническую помощь правоохранительным органам в идентификации и определении сексуальных насильников; и реализации программ по противодействию сексуальной эксплуатации детей.

Проблема

Понимание тревожного увеличения сексуальной эксплуатации детей и подростков является приоритетным заданием участников III Всемирного конгресса. Определение масштабов проблемы является вызовом для структур и обществ, работающих в сфере защиты прав детей. Данные ИСМЕС и НСМЕС:

- За время 10 лет работы «горячей линии» CyberTipline, НСМЕС получил и обработал более 600,000 обращений. Подавляющее большинство этих обращений касалось детской порнографии. На данный момент Интернет провайдеры сообщили на CyberTipline о более чем 5 миллионах изображений детей, подвергшихся сексуальной эксплуатации. В 2007, НСМЕС отметили увеличение количества обращений практически по всем категориям: на 23% - обращений о детской порнографии, на 66% - обращений по развратным действиям он-лайн; на 58% - обращений по детской проституции; на 10% - по детскому сексуальному туризму и на 9% - обращений о домогательстве по отношению к детям.
- Все более и более маленькие дети становятся жертвами, изображения становятся все более графическими и жестокими. Среди преступников, идентифицированных в результате последнего исследования в США, 39% имели изображения детей младше 6 лет, 19% - изображения детей младше 3 лет.
- На CyberTipline также поступают обращения от членов Международной Ассоциации «Горячих Линий» Интернет Провайдеров (INHOPE). На сегодняшний день, члены подали на CyberTipline около 50 000 сообщений о детской порнографии. В Ассоциацию (INHOPE)

входят 33 «горячие линии» из 29 стран, борющиеся за изъятие незаконного контента из Интернета.

В рамках этого широкого контекста отмечается рост коммерческой детской порнографии, а именно, деятельность организованной преступности и других структур для получения прибыли от изображений детей и подростков, над которыми совершается сексуальное насилие. Коммерческая детская проституция стала многомиллионной индустрией, и дети во всем мире используются как предмет для продажи или торговли.

Чтобы управлять этим бизнесом, криминальные организации должны иметь доступ к инфраструктуре, для того чтобы начать производство. Как результат, финансовые структуры и Интернет компании намеренно или ненамеренно вовлекаются в бесчестный бизнес. Таким образом, необходимо, чтобы частный сектор присоединился к усилиям правоохранительных органов и НПО в борьбе с коммерческой детской порнографией.

Финансовая Коалиция Против Детской Порнографии

ФКПДП – это уникальная инициатива, которая объединяет ресурсы общественного и частного секторов для искоренения бизнеса коммерческой порнографии.

ФКПДП состоит из крупнейших банков, кредитных союзов, других коммерческих структур, кампаний, предоставляющих Интернет услуги, и представляет 95% платежной индустрии США. Ее цель – искоренить прибыльность коммерческой детской порнографии путем отслеживания денежных потоков и закрытия тех, которые используются такими противозаконными структурами.

До того как в 2006 году была основана ФКПДП, многие компании, в том числе компании, предоставляющие Интернет услуги, самостоятельно боролись с веб сайтами с детской порнографией. Но учитывая масштабы проблемы, их разрозненные усилия не были достаточно эффективными. ФКПДП предоставляет возможность объединить ресурсы, опыт и кадры для того, чтобы сделать шаг вперед в борьбе с этой проблемой.

Члены ФКПДП:

America Online	Global Payments Inc.
American Express Company	Google
Authorize.Net	HSBC – North America
Bank of America	JP Morgan Chase
The Bank of New York Mellon	MasterCard
Capital One	Microsoft
Chase Paymentech Solutions	North American Bancard
CheckFree	PayPal
Citigroup	ProPay Inc.
Deutsche Bank Americas	Premier Bankcard, LLC
Discover Financial Services	Standard Chartered Bank
Elavon	Visa
First Data Corporation	Washington Mutual
First National Bank of Omaha	Wells Fargo

Юридические фирмы, финансовые ассоциации, эксперты по кибер безопасности, инспекторы США также оказывают содействие ФКПДП.

Эта инициатива признает, что число лиц, вовлеченных в эту всемирную коммерческую индустрию, препятствует ведению судебного преследования, не смотря на то, насколько жестко действуют правоохранительные органы. ФКПДП, которая в основном является гражданской инициативой, предлагает различные подходы: основываясь на рекомендациях CyberTipline, NCMEC идентифицирует веб сайты, содержащие противозаконные изображения, а также способы платежей. Эта информация передается агентам из федеральных правоохранительных органов США, которые продолжают изучение конкретных сайтов с целью сбора доказательств и определения противозаконного контента и действий. Если правоохранительные органы не продолжают расследование, финансовая компания будет уведомлена и предпримет соответствующие действия.

Достижения

Некоторые позитивные тенденции свидетельствуют о том, что усилия ФКПДП и правоохранительных органов оказывают влияние на бизнес, связанный с коммерческой детской порнографией.

Например, стало труднее использовать кредитные карты для теневых транзакций. Если правоохранительные органы сталкиваются с трудностями, в процессе установления этих транзакции, то и потребители тоже. Стоимость изображений сексуальной эксплуатации детей значительно выросла, что может является индикатором влияния деятельности ФКПДП.

ФКПДП нацелена на то, чтобы лучше понять, как торговцы детской порнографией использовали систему оплаты в прошлом, для того, чтобы избежать подобных ситуаций в будущем. Результатом такой работы стала публикация «Коммерческие приобретения через Интернет и мониторинг лучших практик по предотвращению и выявлению коммерческой детской порнографии» (“Internet Merchant Acquisition and Monitoring Best Practices for Prevention and Detection of Commercial Child Pornography”). Орган США, контролирующий денежный оборот (U.S. Comptroller of the Currency (ОСС), распространил этот документ среди руководителей банков по всей стране и других заинтересованных групп, таких как NCMEC и FCACP. Кроме этого, ОСС анонсировал эту инициативу.

ФКПДП опубликовал свой второй выпуск лучших практик в 2008, на который ссылается далее.

Предстоящие трудности

ФКПДП делает значительный прогресс в США. Следующим шагом должно стать распространение данной модели и в других странах, для борьбы с глобальной проблемой. Цель ФКПДП – разрушить экономику структур, занимающихся детской порнографией, путем построения альянса финансовых и Интернет компаний, НПО, юристов и правоохранительных органов и выработки

решений, гармонизированных с местным законодательством и традициями. К целевым регионам относятся Европа и Юго-Восточная Азия.

Компании регулярно обращаются в NCMES и ISMES с просьбой вступить в ФКПДП. Некоторые из этих институций являются хорошо известными брендами, работающими под всесторонним наблюдением. Другие менее известны, но являются потенциально важными участниками новых платежных методов. Необходимо тщательно отбирать новых аппликантов, чтобы быть уверенными, что их бизнес модель, корпоративная этика и репутация соответствует целям ФКПДП. В настоящее время идет апробация недавно разработанного Процесса Отбора.

Пристальное внимание уделяется сайтам, содержащим детскую порнографию, выявляются структуры, которые ими управляют. Это особенно актуально в сферах веб хостинга и альтернативных способов оплаты. Рабочая Группа ФКПДП по Технологическим Проблемам (Technology Challenges Working Group of FCACP) недавно опубликовала тематический выпуск по соответствующим проблемам. Этот документ подается в качестве приложения к данному материалу, и является примером преимущества сотрудничества, которое является частью ФКПДП.

Дополнение: Отчет Рабочей Группы ФКПДП по Технологическим Проблемам 2008 г. (Technology Challenges Working Group Report 2008). «Тенденции в миграции, хостинга и платежей по веб сайтам, содержащим коммерческую детскую порнографию» (Trends in Migration, Hosting and Payment for Commercial Child Pornography Websites).

-

**ОТЧЕТ РАБОЧЕЙ ГРУППЫ ФКПДП ПО ТЕХНОЛОГИЧЕСКИМ ПРОБЛЕМАМ 2008:
«ТЕНДЕНЦИИ В МИГРАЦИИ, ХОСТИНГА И ПЛАТЕЖЕЙ ПО ВЕБ САЙТАМ, СОДЕРЖАЩИМ
КОММЕРЧЕСКУЮ ДЕТСКУЮ ПОРНОГРАФИЮ»**

История

Финансовая Коалиция Против Детской Порнографии сформировалась в 2006 году в ответ на угрожающий рост масштабов распространения коммерческой детской порнографии через Интернет. ФКПДП состоит из крупнейших банков, кредитных союзов, других коммерческих структур, кампаний, предоставляющих Интернет услуги. Одна из задач Коалиции – отслеживать и предвидеть, как развивается механизм коммерческой детской порнографии. С этой целью, Рабочая Группа предлагает следующие наблюдения.

Предупреждение

Этот отчет был подготовлен волонтерами от имени Рабочей Группы и представляет точку зрения Рабочей Группы на вопросы, рассмотренные в публикации. Содержание базируется на индивидуальном вкладе участников и не обязательно отражает мнение или политику компаний, в которых работают участники. Допускается наличие неточностей и неактуальной информации с момента, когда данный отчет готовился.

Данный отчет может быть использован в качестве источника информации и не предназначен для предоставления специфических юридических, финансовых или бизнес рекомендаций. Если вам необходимы специфические рекомендации или консультации, необходимо обратиться к соответствующим специалистам. Рабочая Группа не дает никаких гарантий, высказанных, подразумеваемых или установленных в отношении информации, изложенной в данном отчете. Список организаций или лиц, приведенных в отчете, не подразумевает одобрение таких организаций или лиц.

Вы несете ответственность за соблюдение всех авторских прав. Разрешается бесплатное распространение этого отчета при сохранении его целостности, и условии, что все официальные данные, включая авторские права, указаны. Запрещается продажа с целью получения прибыли или использование в коммерческих документах без письменного разрешения Рабочей Группы, выдача которого является исключительно правом Рабочей Группы.

Тенденции в миграции

Одной из центральных проблем правительств и правоохранительных органов, которые занимаются борьбой с он-лайн коммерческой детской порнографии, является анонимность,

-6-

свойственная Интернету. Преступники изобретательно защищают свои он-лайн операции, имея возможность скрывать часть своих транзакций и контент.

Для информации:

- ❖ Коммерческая детская порнография может размещаться в странах, которые уделяют недостаточно внимания этому вопросу, или удаленных от прямого влияния юридически инструментов, или она может непреднамеренно размещаться на различных компьютерных системах, которые сами могут кооптированы технически опытными поставщиками детской порнографии.
- ❖ Он-лайн оплата за просмотр детской порнографии анонимна. Хотя традиционно платежные операции осуществляются через банк или подобные структуры в соответствии с национальными банковскими правилами, Рабочая Группа обнаружила тенденцию возникновения («альтернативных») услуг по оплате и финансовых организаций, чей статус позволяет им обходить существующие правила, которые требуют идентификации плательщика и получателя.

Основной проблемой в выявлении и предотвращении он-лайн детской порнографии является то, что Интернет предоставляет анонимный хостинг, что позволяет кибер преступникам, действовать с относительной безнаказанностью и совершать множество других преступлений, помимо продажи детской порнографии. Анонимность способствует проведению он-лайн операций с коммерческой детской порнографией тремя путями: легко укрывать контент; возможность быстро создавать платежные сайты («на высоте сегодня, внизу завтра, на высоте послезавтра») для того, чтобы избежать обнаружения; и недостаток инструментов, которые регулировали бы появляющиеся способы платежей.

Обычно Интернет пестрит ссылками на источники с детской порнографией. Некоторые ссылки имеют несколько переадресаций, приводя потенциального покупателя на несвязанный домен. Когда потенциальный покупатель попадает на сайт, который предлагает платное членство, возможны следующие действия. Хост сайт может предложить использовать кредитную карту, чтобы заплатить за сайт. На этом этапе незакодированная веб страница может быть использована для подтверждения имени, адреса, номера телефона и данных кредитной карты. Большинство ссылок на сайты с детской порнографией, которые предлагают членство, проводят платежи по кредитным картам без использования https технологии, подвергая таким образом покупателя высокой степени риску. Информация незащищена от вторжения и использования кибер преступниками. Рабочая Группа может только предполагать, что ссылки на сайты с детской порнографией не получают SSL сертификат, так как они должны были бы отказаться от своей анонимности.

Некоторые сайты предлагают материалы, содержащие детскую коммерческую порнографию на продажу через подтверждение по электронной почте. Покупатель отправляет электронное сообщение неизвестному лицу для завершения транзакции, иногда используя платежную систему webmoney, или просто использует почту США для отправки наличности. Другие сайты содержащие детскую порнографию, предлагают членство, но переадресовывают покупателя на специальный сайт для проведения оплаты посредством кредитных карт. Некоторые из таких

сайтов предлагают как надежные так и ненадежные транзакции. Такие сайты обычно: не шифруют переводы с использованием кредитных карт; фальсифицируют или «обманывают» страницы с транзакциями по кредитным картам, чтобы они выглядели как законные или частично законные. Рабочая Группа не обнаружила значительной части платежей на сайты с детской порнографией, но обнаружила снижение успешной идентификации сайтов с детской порнографией. Причиной этого, может быть применение более строгих мер по отношению к тем, кто получает прибыль от детской порнографии, что заставляет их уходить в большую тень и затрудняет процесс последующей идентификации.

Хостинг¹

Хостинговые компании

Многие хостинговые компании стали каналом для накопления коммерческой детской порнографии. Поэтому, в большинстве случаев фирменные URL или контент сайты меняют друг друга среди потенциальных торговцев и способов оплаты, до тех пор, пока не будут закрыты. В таком случае фирменные сайты создают новые счета и способы оплаты. Таким образом, отдельный сайт, имеющий контент возможность проведения платежей, может вновь появиться с новыми хостами и торговцами, в случае его внезапного удаления. Обычному наблюдателю кажется, что эти сайты продолжают работать без перерыва. Для тренированного и информированного наблюдателя понятно, что на самом деле, эти сайты фактически были заблокированы для того, чтобы возникнуть вновь. Тщетность такого процесса можно сравнить с аркадной игрой «Ударь крота» (“Whack-A-Mole”), в которую играют дети.

Интересно, что «белый знак» (“white label”) (предполагающий безопасность) контент сайтов и URL имеет абсолютно другой жизненный цикл. Обычно эти URL используются для того, чтобы привести покупателей к временному контенту с белым знаком или к временному расположению фирменного контента. Таким образом, эти URL являются «пушечным мясом» в борьбе за коммерческую жизнеспособность. Действительно, можно видеть 10-20 различных URL, появляющихся в массовых спам кампаниях, где в итоге все URL содержат соответствующий контент.

В настоящее время многие хостинговые компании фокусируются на надежности и оценке и зачастую не имеют прописанной политики по отношению к нелегальному контенту. В некоторых случаях их правила соглашения содержат позиции, которые говорят о том, что размещение нелегального контента их покупателями могут привести к прекращению предоставления услуги. Однако остается вопросом, насколько они придерживаются таких превентивных мер. На практике, хосты не проверяют контент, и зависят от сообщений о том, что они размещают коммерческую детскую порнографию, до того как смогут предпринять определенные меры. Рабочая Группа получила информацию от одного из экспертов, о том, что хосты, которые обычно не консультируются с юристом или другим экспертом, владеющим информацией по данному вопросу, часто в ответ на поступление жалоб, предпринимая внутреннее расследование. Тот же эксперт заявил, что это рискованная и опрометчивая практика по следующим причинам: а)

¹ Веб хостинг сервис – вид услуги Интернет хостинга, которая позволяет отдельным лицам и организациям создавать свои собственные веб сайты, доступные через Всемирную Паутину. Веб хосты это компании, которые предоставляют клиентам место на своих серверах для использования, а также Интернет соединения, обычно в центре данных. См http://en.wikipedia.org/wiki/Web_hosting.

«патрулирование» контента не относится к функциям хоста; б) веб хосты не имеют достаточной квалификации для определения того, что относится к коммерческой детской порнографии; в) хосты могут нарушать законы владения относительно коммерческой детской порнографии. Те, которые следуют юридическим советам, имеют специальную действующую процедуру для изоляции материала и сообщения в Национальный центр для пропавших и пострадавших от эксплуатации детей (NCMEC);

Первым шагом должно стать использование и внедрение лучших практик хостинговыми компаниями. Исследование Рабочей Группы показало, что на данный момент отсутствуют торговые организации для веб хостингов подобные Ассоциации Провайдеров Интернет Услуг в США (U.S. Internet Service Providers Association). Такие организации были бы полезны для установления стандартов и могли бы служить механизмом, отвечающим вопросам, затронутым Рабочей Группой.

Представленный ниже список служит рекомендацией и определяет минимальный уровень ответственности хостинговых компаний для предотвращения размещения коммерческой детской порнографии.

- Политика в отношении детской порнографии: Проводить политику в отношении выявления и реагирования на хостинг и хранение детской порнографии. Следующий веб сайт был приведен экспертом в качестве примера реагирования на проблему коммерческой детской порнографии: <http://www.peakinternet.com/legal/aup/>. Хотя Рабочая Группа не подтверждает этот язык как модель, по крайней мере он делает попытку реагировать на проблему.
- Мониторинг: Частые изменения в способах, технологии, URL и т.д. являются явными преднамеренными попытками преступников избежать обнаружения. Они также предпринимают различные меры для сохранения своей анонимности. В связи с этим, Рабочая Группа рекомендует хостам ежеквартально идентифицировать сайты, содержащие детскую порнографию с целью еженедельного обзора всех известных активных сайтов. Робот поисковой системы (Spider and bot technology) легко позволяют определять лексику и изображения, имеющие отношение с коммерческой детской порнографией. Как только оно будет найдено, эти сайты должны быть удалены хостами.
- WRT Фильтр: Во многом похож на действия Провайдеров Интернет Услуг, когда используются технологии для удаления из их систем противозаконных материалов, хосты должны удалять все незаконные материалы со своих серверов.
- Обмен информацией с NCMEC о противозаконных хостах (хосты, на которых размещен нелегальный контент): В соответствии со своей политикой, хостам рекомендуется передавать информацию, о лицах или компаниях, которые подозреваются в распространении детской порнографии в NCMEC.
- Руководство поведения в отношении покупателей: Так же как и банки обязаны следовать правилу «знай своих клиентов», для избегания быть использованными с целью отмывания денег торговцами наркотиками и террористами, веб хостам следует проводить соответствующую политику в отношении покупателей и их контента.

И наконец, Коалиции следует рассмотреть возможность создания «черного списка» хостинговых компаний, которые известны тем, что сознательно размещают детскую порнографию или практикуют сознательное отстранение от препятствования этому, а также тех, которые не желают следовать 5 пунктам руководства к действию, указанным выше.

Корпоративные серверы как hosts коммерческой детской порнографии

Пробелы в безопасности корпоративной сети открытые преступниками с помощью вредоносных программ, которые контролируют любого удаленного пользователя, прикрепленного к сети, и в свою очередь, подвергают опасности всю сеть, делают интеллектуальную собственность и финансовые данные уязвимыми для использования организованной преступности, или, в случае с детской порнографией, позволяют размещать на ней или распространять через нее подобную информацию.²

Представьте сервер большой корпорации, университета или финансового учреждения, используемый для продажи детской порнографии. Существующие примеры нарушения безопасности делают такое предположение не только возможным, а вполне допустимым. Лучшие практики проверок в Приложении могут быть использованы для обмена опытом между членами Коалиции.

Платежные системы он лайн

Во введении «Национальной оценке угрозы отмывания денег»³ (“U.S. National Money Laundering Threat Assessment,” (“NMLTA”) (США, декабрь 2005), правительство США отмечает, что «преступники используют новые преимущества глобализации и появление новых финансовых услуг, таких как смарт карты, в которых хранится цифровая наличность и платежные системы он лайн». NMLTA выявила и оценила тринадцать систематических финансовых угроз для США и 2 из этих 13 - платежные системы он лайн и смарт карты, в которых хранится цифровая наличность – представляют новый этап, который не мог бы появиться несколько лет назад. Эти новые угрозы финансовой системе, появляющиеся частично в результате необходимости избегать использования банковских услуг, и частично в результате глобализации финансовых систем и их реакций на реальность Интернета, создают потенциальные угрозы со стороны преступности и иного противозаконного использования не только для экономики США, но и для глобальной экономики в целом.

В заявлении NMLTA говорится о том, что “новые и инновационные платежные системы он лайн появляются во всем мире в ответ на рыночный спрос со стороны отдельных лиц и он лайн коммерсантов... Он лайн коммерсанты, особенно действующие в секторе с высоким уровнем «отказа от платежей», аккумулируют спрос на новые способы оплаты. Эти рынки охватывают платежные системы он лайн, которые устанавливают свои собственные клиринговые и установочные правила, включая отсутствие процедуры защиты потребителей. Обычно, транзакции через таких провайдеров, являются окончательными без обращения к конкретным лицам, которых обманули.

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

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

В соответствии с федеральными правоохранительными органами, эти системы становятся предпочтительными механизмами оплаты для он лайн преступников в сфере обманных инвестиционных схем и другой незаконной деятельности.⁴

NMLTA предоставила обзор «электронных платежных систем», таких как недавно появившиеся системы электронных платежей - e-gold, Ltd. и другие. NMLTA оценила уязвимость этих технологий, отметив, что от отправителей денег требуется регистрация в FinCEN,⁵ они подчиняются требованиям по фиксированию и сообщению об отмывании денег (“AML”), также как общим лицензионным требованиям. Требования АМЛ к платежным системам он лайн или электронным платежным систем «зависит от расположения и способов проведения транзакций».⁶

Эти новые и появляющиеся механизмы оплаты, включая два, которые не рассматривались NMLTA – он лайн игры, такие как Entropia Universe, которые имеют свою собственную конвертируемую денежную единицу и связь с возможностями снятия в реальном мире, а так же появившиеся возможности мобильного банкинга через мобильные телефон – указывают на кардинально отличающиеся от таких традиционных способов как наличные, чеки и кредитные карты. Эти новые механизмы платежей, особенно те, которые осуществляются через Интернет, могут способствовать развитию новых способов совершения преступлений или объединять новые виды криминальной деятельности, которые совершаются по отношению к самим технологиям. Финансовый поток может иметь криминальное происхождение или быть механизмом отмывания денег.

На международном уровне, Международная организация по борьбе с отмывание денег) (FATF)⁷ включающая 34 государства, в октябре 2006 года подготовила отчет⁸, в котором рассматривается способ, в результате которого могут отмываться деньги через использование новых технологий платежей (карты предоплаты, платежные системы Интернет, мобильные платежи, цифровая платежная система «digital precious metals»). В отчете отмечается, что в то время как легальный рынок нуждается в таких способах платежей, они являются чрезвычайно уязвимыми для отмывания денег и схем финансирования терроризма. Международные провайдеры новых платежных методов могут подвергать большему риску, чем провайдеры, действующие исключительно в пределах отдельной страны. В своем отчете FATF рекомендует всем странам усилить бдительность по отношению к дальнейшей оценке влияния появляющихся технологий в рамках международных и национальных регулятивных инструментов. Однако, признавая уровень коррупции или сговора со стороны некоторых иностранных правительств в различных видах криминальной активности, жесткий мониторинг и регулирование финансовых транзакций может быть проблематичным.

Система электронных платежей (PayPal) представляет значительный уровень проверки платежной системы он лайн и может служить моделью для других. Благодаря эффективной политике, частным моделям, способам аудита и расследования, и общественного/частного партнерство,

⁴ NMLTA на 25.

⁵ U.S. Treasury Financial Center.

⁶ NMLTA at 27.

⁷ С момента создания, FATF стимулирует международные усилия принять и внедрить меры по противодействию использованию глобальных финансовых систем преступниками. Она издала серию из 40 Рекомендаций в 1990, пересмотренных в 1996 2003, для обеспечения их актуальности и развивающийся угрозе отмывания денег.

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

PayPal демонстрирует твердость, которой должны подражать другие платежные системы он-лайн для противодействия платежам за детскую порнографию. Политика и процедуры PayPal для проведения соответствующей оценки:

Политика

- PayPal не приемлет толерантной политике по отношению к использованию своей системы для любых противозаконных материалов и услуг.
- Соглашения пользователя PayPal четко гласят, что любые **экзаунты**, предлагающие противозаконные материалы и/или услуги, нарушают существующую политику пользования и будут немедленно закрыты.

Модели и другие инструменты выявления

- Соответствующие модели PayPal, разработанные специально для противодействия эксплуатации детей.
- PayPal насчитывает более 1700 ключевых слов на различных языках, входящих в моделирующие методы.
- PayPal делает значительные инвестиции в инструменты мониторинга и выявления детской эксплуатации.
- PayPal использует методы, которые контролируют систему изнутри и снаружи на предмет нарушений.
- Ключевые слова и моделирующие техники обновляются еженедельно.
- PayPal призывает лиц, имеющих информацию о потенциальном противозаконном использовании PayPal, обращаться в компанию.

Аудит

PayPal привлекает продавцов, которые проверяют Интернет на предмет потенциальных нарушений в отношении своего бренда.

Агенты, занимающиеся расследованиями, аналитики, Группа глобальных операций правоохранительных органов

- PayPal имеет команду, состоящую приблизительно из 100 агентов (в Омахе, Дублине и Шанхае), которые осуществляют поиск, делают обзор и расследуют риски нарушений, включая те, которые относятся к эксплуатации детской.
- Кроме того, PayPal имеет специализированную команду агентов, которые работают исключительно в сфере противодействия эксплуатации детей – в течении нескольких лет они проходили специальные тренинги, проводимые NCMEC и регулярно проходят тематические тестирования.

- PayPal делает значительные инвестиции в тренинговые программы для команд по расследованию и аналитиков, включая внутренние и внешние тренинги, он-лайн библиотеки, и другие источники, для обеспечения PayPal наиболее современными материалами.
- PayPal имеет исследовательскую программу, в которой агенты исследуют тенденции, новости, события и следующее поколение технологий.

Общественное и частное партнерство

- PayPal тесно сотрудничает с Иммиграционной и таможенной полицией США, ФБР и другими структурами для того, чтобы иметь информацию о противозаконном контенте.
- PayPal привлекают различных представителей правоохранительных органов в работе своего Всемирного операционного центра в Омахе, как часть тренинговой программы.
- В Группу глобальных операций правоохранительных органов входят бывшие сотрудники правоохранительных органов, адвокаты, профессионалы в сфере производства, которые тесно сотрудничают со своими коллегами в правоохранительных органах, различных агентствах и НПО для установления коммуникации и сотрудничества в процессе расследований.

Заключение

Отход платежей за детскую порнографию и веб-хостинга от традиционных финансовых способов и хостинговых моделей является серьезной тенденцией, которая не просто требует к себе внимания, но также значительного понимания, и также как и в других аспектах Интернет-коммерции, возможно даже большего регулирования. Теневая экономика и распространение детской порнографии имеет динамичный характер перед лицом усилий Коалиции по борьбе с ними. Как и многие другие, имеющие отношение к Интернет-индустрии, создаются и входят в сообщество добросовестных граждан, для Коалиции является важным донести до них и стимулировать их использовать лучшие практики, такие как соответствующая проверка, фильтрация и мониторинг сайтов.

ПРИЛОЖЕНИЕ: ПРАКТИКА БЕЗОПАСНОСТИ ВЕБ СЕРВЕРА⁹

Безопасность Веб Сервера
1. Помните, что неправильная инсталляция HTTP может привести к атакам DDoS и злоупотребление конфиденциальной информацией, что делает сервер уязвимым для проникновения.
2. Используйте SSL или SSH.
3. Не запускайте другие приложения в системе. Ограничьтесь HTTP и другими необходимыми услугами.
4. Используйте последние сервисные пакеты, обновления и патчи.
5. Ограниченный доступ пользователя: ограничьте список пользователей, которые имеют доступ к веб серверу путем использования двухступенчатой аутентификацией.
6. Проводите тестовое проникновение для проверки уязвимости веб сервера.
7. Уменьшит ли риски внедрение сменного контроля? Производится ли отслеживание и мониторинг изменений системы?
8. Удалите любые образцы CGI программы с сервера
9. Используйте сканнер для симуляции проникновения на веб сайт и определения его безопасности. Используйте его во время фазы разработки и еженедельно сканируйте на предмет появления новых элементов уязвимости.
10. Регулярно делайте обзор всех журналов посещения сайтов. Все журналы должны быть включены. Если это возможно, проверяйте все журналы для выявления тенденций или сходства с другими серверами.
11. Внимательно планируйте и принимайте во внимание вопросы безопасности при открытии любого публичного веб сервера ¹⁰
12. Внедрите соответствующую практику безопасности и контроля в процессе поддержки и осуществления безопасного веб присутствия ¹¹
13. Для обеспечения безопасности веб сервера и поддерживающей инфраструктуры сети, рекомендуется использовать следующие практики: <ul style="list-style-type: none">▪ Всеобщая организационная политика безопасности информационной системы.▪ Контроль и менеджмент конфигурации/смена контроля

⁹ World Bank Treasury Technology Risk Checklist 7.3.

¹⁰ Поскольку сложнее обращать внимание на вопросы безопасности, когда система уже создана и действует, необходимо принимать во внимание вопросы безопасности на этапе планирования. Организации чаще принимают решения относительно соответствующей конфигурации и защиты компьютеров, когда разрабатывают детальный план запуска. Разработка такого плана приводит организации к принятию сбалансированного решения между доступностью использования, представительством и риском. Организации часто не принимают во внимание человеческий ресурс в требованиях, как к запуску так и к операционным фазам веб сервера и поддерживающей инфраструктуры. Организации должны учитывать следующие моменты в разработке плана:

- Категории специалистов, которые требуются (например, системные и веб администраторы, веб мастера, сетевые администраторы, офицеры безопасности информационных систем [ISSO]);
- Требования по навыкам и тренингам к персоналу;
- Индивидуальные (уровень требуемый для определенной категории специалистов) и коллективные человеческие ресурсы (общий уровень) требований.

¹¹ Соответствующий менеджмент очень важен для организации работы безопасного веб сервера. Практика безопасности влечет за собой идентификацию активов информационной систем, развитие, документирование и внедрение политик, стандартов, процедур и руководств, которые обеспечат конфиденциальность, целостность и доступность ресурсов информационной системы.

- Оценка риска и менеджмент
- Стандартизированное обеспечение конфигураций, соответствующая политика безопасности информационной системы.
- Информирование и тренинги по безопасности.
- Планирование резервов, продолжение деятельности и восстановление после разрушения.