

Capital Collect – преступная халатность или неумение работать ?

Capital Collect – новости плохие и очень плохие

Сначала коротко о главном: платежный сервер [Capital Collect Services](#) был вероятно взломан **17 ноября 2006** года (а возможно и ранее) и **полный** доступ к нему оставался у злоумышленников вплоть до **24 апреля 2007** года.

Замечу, найдена или нет в итоге уязвимость – я до сих пор так и не знаю, так как «находили» все новые и новые дыры за эти почти **6 месяцев НЕОДНОКРАТНО**.

Что я рекомендую сделать **НЕЗАМЕДЛИТЕЛЬНО** – если вы пользуетесь их картами (Chexcard EBSG ATM Card) поменяйте пин-код. Вся личная информация, которая хранилась на сервере и пины к картам, давно имеются в распоряжении у злоумышленников.

Сделать это можно либо с сайта <http://www.chexcard.com/> (эта ссылка есть на бумажках с пин-кодом, которые вы получили вместе с картой) или на сайте эмитента этих карт <http://www.ebsg.net/>

В данный момент имеется неурегулированная задолженность, по сделкам проведенным около месяца назад, которую владелец компании отказывается погашать. Мотивируется это тем, что я сам во всем виноват, а то, что я получил в явном виде от него лично и от его сотрудника подтверждение легальности происхождения денег на счетах этих клиентов ничего не значит.

Краткая предистория

В конце 2006 года шло разбирательство с тремя обменными пунктами (см. [CapitalCollect - очередное кидалово](#) или [CapitalCollect - очередное кидалово](#)), через которые вывели пропущенные в систему деньги по сделке на Ebay. Ко мне стукнулся Главный Начальник CCS (*Mitch*), что бы проконсультироваться:

Mitch, 17.11.2006 18:28 :

summa - 12K.

Mitch, 17.11.2006 18:28 :

arbitrazh WM - otvetil chto na obmennik

Momentalno.org, 17.11.2006 18:28 :

Ё

Mitch, 17.11.2006 18:28 :

aga

Momentalno.org, 17.11.2006 18:28 :

а откуда у вас столько ВМ то было

Mitch, 17.11.2006 18:29 :

da bilo, bilo... prichem sdelano ne cherez sistemu. voobsche - neponyatno kak.

Mitch, 17.11.2006 18:29 :

dengi perevedeni 2-mya summami - po 6500 i 4800 s pometkoi "platezh viconu". tak to....

Почему я отношу взлом к этому времени? Ключевые слова «*voobsche - neponyatno kak*» - т.е. деньги выведены из служебного кошелька и каким образом это произошло **НИКТО так и не выяснил**.

В пылу разборок на этот инцидент не обратили должного внимания, деньги были «повешены» на один из обменных пунктов, который отказался «договариваться» по хорошему. И судя по всему, выяснять каким же образом деньги были украдены, никто разбираться не стал.

Mitch, 17.11.2006 18:36 :

>> Средства были выведены через обменный пункт.
>> Информация (ФИО и паспортные данные получателя, данные и ip-адрес владельца кошелька) может быть передана в правоохранительные органы по официальному запросу.
>>
>>
>> >Z667896747759 12.11.2006 19:41 6510.00 50,00 5,17 Z123070177542 payment for vicon
>> >Z667896747759 16.11.2006 14:05 4835.00 38,68 1,44 Z123070177542 payment for vicon
>> >Z667896747759 13.11.2006 4:14 5.00 0,04 0,13 Z123070177542 моральная компенсация
>> >
>> >Эти переводы наша компания не делала
>> >сообщите пожалуйста с какого IP адреса это было сделано и куда ушли деньги. ВЕРНИТЕ ИХ ПОЖАЛУЙСТА!
>> >

Последовали ужесточения в плане внутренних переводов, у всех были очень сильно уменьшены лимиты на р2р платежи внутри системы, более внимательно стали смотреть на зачисления от физических лиц, в общем, весь комплекс организационных мер (но не технических!) был проведен.

А вот продолжение этой истории

Mitch, 29.01.2007 23:41 :

dlya etih akkov - 7559083, 7559085, 7559087, 7559144 - s kotorih ti poluchal vnutrennie perevodi - voobsche NIKOGDA realnih deneg NE postupalo.

Mitch, 29.01.2007 23:42 :

seichas tehniki sidyat i viyasnayut - kak voobsche eto moglo poluchitsya.

Mitch, 29.01.2007 23:48 :

skoree - dira .. no ya poka NE znayu.... chto dumat...

Mitch, 29.01.2007 23:48 :

WMZ - bolshe ne voruyut - vrode vse zakrili.... a tut...

Mitch, 29.01.2007 23:48 :

vot i dumayu, chto delat dalshe...

Momentalno.org, 29.01.2007 23:50 :

я вообще не понимаю как с этим бороться...если люди имеют такой вход...да они будут кидать на другие акки тогда , и почуть чуть переводить с них на обменники.

Momentalno.org, 29.01.2007 23:53 :

слушай , не начинай

мы с тобой вчера еще говорили. про это не было ни слова сказано

проблему как то надо решать...что это 100% ваша дыра и тут я ничего не мог сделать ты согласен ?

лимиты у людей были большие и поскольку лимиты поднимаете вы у меня не было

особых причин сомневаться, что там все ок.

крысу ты ПОЛНОСТЬЮ исключаешь ?

Mitch, 29.01.2007 23:54 :

seichas uzhe ne znayu.... etim akkam NE podnimali llimiti...

Momentarno.org, 29.01.2007 23:54 :

Эти же деньги, точнее их приход должен же, как-то отмечаться, и проводится ...даже у меня это делается

Mitch, 29.01.2007 23:55 :

verno - dolzhen... no po history - nichego net. nichego.

Momentarno.org, 29.01.2007 23:55 :

ну фиг с ними , с лимитами... деньги то туда КАК ТО попадали ?

Mitch, 29.01.2007 23:55 :

nikakih deneg voobsche ne bilo . ZERO. tolko v baze dannih.

Momentarno.org, 29.01.2007 23:56 :

а в базе там что у вас plain text ?

ничего не подписывается и ничего не шифруется ?

Mitch, 29.01.2007 23:56 :

shfruetsya.. i baza - na OTDELNOM server...

Momentarno.org, 29.01.2007 23:56 :

т.е. просто может доступ к базе кто то получил...сделал акки

снял лимиты, добавил деньги ...доки на эти аккаунты есть ?

Momentarno.org, 29.01.2007 23:57 :

или аккаунты тоже пустые, без данных ?

Mitch, 29.01.2007 23:57 :

net - tam vse pusto...

Momentarno.org, 29.01.2007 23:59 :

ну сам понимаешь , варианта 2 либо взлом...причем вы его не нашли как я понимаю

пока...либо крыса...но если там нет данных, то ничего вы тут и не найдете..деньги то никто не заводил и акки эти никто не регистрировал.

И вот фраза на которую стоит обратить внимание, точнее на саму фразу и дату когда это было сказано. Важность ее [будет понятна позже](#)

Mitch, 30.01.2007 0:09 :

oni ne vse mogut.. oni - ne smogli pomenyat balansi.. i esche кое-что.... ladno... siechas nado dumat chto delat s tvoimi dengami

Momentarno.org, 30.01.2007 0:11 :

а балансы никто менять не будет

будет честный перевод из ниоткуда на проверенного клиента, а потом с него в

обменник...если у них есть доступ к базе то и и переводы от имени клиентов они думаю тоже смогут делать...хоть и мелкие

А вот что касается «найденной» спустя 2 месяца дыры.

Почему пишу найденной в кавычках – то что нашли была явно не дыра , а ее последствия. Саму дыры возможно не нашли до сих пор.

Mitch, 30.01.2007 1:00 :

viyasnili.. PHP

Momentalno.org, 30.01.2007 1:00 :

т.е. скрипты ломанули ?

Mitch, 30.01.2007 1:01 :

net. u nas - vse na C++ stoyal PHP esche na server....

Momentalno.org, 30.01.2007 1:01 :

мммм...не понял... написали работу с базой на нем ?

Momentalno.org, 30.01.2007 1:02 :

но там же шифрование какое никакое должно быть

Mitch, 30.01.2007 1:02 :

net

Mitch, 30.01.2007 1:02 :

prosto - stoyal PHP. oni - cherez neg. php - chasikami upravlyal

Momentalno.org, 30.01.2007 1:03 :

chasikami upravlyal - что за часики ?

Mitch, 30.01.2007 1:03 :

kotorie vremya pokazivayut - nashe i klienta.

Momentalno.org, 30.01.2007 1:03 :

и ?

Mitch, 30.01.2007 1:03 :

i cherez etot PHP - sozdali svoi Shell

Momentalno.org, 30.01.2007 1:04 :

ну это я понял

Momentalno.org, 30.01.2007 1:04 :

но база то должна быть зашифрованная...как они с ней работали ? как минимум откуда пароль к базе у них взялся...не могли же они без авторизации работать ?

Mitch, 30.01.2007 1:08 :

ne mogli .. пока - ne znayu...

Momentalno.org, 30.01.2007 1:09 :

php как я понимаю оказался дырявый... ну и фиг бы с ним... навесить свой шелл то недостаточно... нужно все равно как то до базы добраться, иметь минимальное представление о структуре.

Mitch, 30.01.2007 1:10 :

konechno.. no пока ya tebe na eti voprosi - otvetit ne mogu - ne znayu

Momentalno.org, 30.01.2007 1:11 :

мне и не обязательно...но не факт что такой шелл не навесят снова, надо найти КАК его навесили

Mitch, 30.01.2007 1:14 :

ne fakt... пока razbiraemsa...

Momentalno.org, 30.01.2007 1:16 :

WMZ все выводились на акки созданные в прошлом году...причем не с нулевым BL, маленьким, но не нулевым

явно все готовили заранее....т.е. дыра была видать еще в прошлом году...просто они возможно со счетами работать не могли , а перевод с вашего кошелька сделали и затаились

потом накопили как делать и пополнять счета

Mitch, 30.01.2007 1:16 :

uzhe ne popolnyat...

По выведенным суммам была достигнута договоренность – 50% уходит на HOLD на 2 месяца, проверяется происхождение денег на ВСЕХ счетах, с которых кто то и что то хочет менять.

В итоге деньги по этой «договоренности» с hold'a были выданы с задержкой в 3 недели, после долгой ругани, да и толку от этого было не очень много – заявки на вывод этих средств все равно в итоге выполнены не были.

Новая дыра (19/03/2007)

TechDept, 19.03.2007 18:17 :

da nichego ne budet
v novi account zalezet...hm

Momentalno.org, 19.03.2007 18:17 :

даже так ?

Momentalno.org, 19.03.2007 18:17 :

там именно взлом старых акков ?

TechDept, 19.03.2007 18:18 :

ochevidno

Momentalno.org, 19.03.2007 18:18 :

а пополняются они как ?

TechDept, 19.03.2007 18:19 :

stranni vopros
skazal zhe - webmoney hack
nasha sistema думаet chto nam pereveli WMZ

Momentalno.org, 19.03.2007 18:19 :

а...ну понял...берется старый акк , и якобы приходит ВМ

Momentalno.org, 19.03.2007 18:19 :

а кодовые таблицы ?

TechDept, 19.03.2007 18:19 :

пока ne znayu

24.04.2007 - А вот то о чем я говорил еще 3 месяца назад

И на что, судя по всему никто, просто не обращал внимание

Mitch, 24.04.2007 23:39 :

eto OCHEN horoshi i STARI klient.

Mitch, 24.04.2007 23:39 :

u nego - BOLSHIE limiti

Momentalno.org, 24.04.2007 23:41 :

и приходы внутренним переводом больших сумм для него нормальны ?

Mitch, 24.04.2007 23:42 :

tam ochen neplohie prihodi. imenno takogo poryadka

Momentalno.org, 24.04.2007 23:44 :

в общем я пока при своем мнении , более того ты подтверждаешь сам что я тебя предупреждал о такой возможности воровства денег...как я понимаю вся база клиентов в паролями и кодовыми картами была слита...либо написан генератор карт...и они пошли раскидывать деньги на крупных клиентов у которых большие обороты...

Momentalno.org, 24.04.2007 23:44 :

и эта дыра была до вчерашнего дня...просто охренеть

Mitch, 24.04.2007 23:45 :

OVMENNIKI - VOT SAMAYA BOLSHAYA DIRA !

Случилось именно , то что случилось – все дыры были на своем месте , никакие уязвимости системы ликвидированы не были. А по счетам этих клиентов, мною было получено одобрение на обмен – потому как это старые и проверенные клиенты. Откуда к ним пришли деньги никто проверять не стал.

Mitch, 28.04.2007 21:23 :

ti SAM - rasskazal mne istoriyu - o tom - chto hakeri - budut ispolzovat scheta normalnih klientov dlya progona deneg (est v HISTORY). ti sam podtverdil - chto obmeni - bili podozritelnie.

Momentalno.org, 28.04.2007 21:24 :

ну и ? сказал ...и вы НИЧЕГО не делали

Mitch, 28.04.2007 21:25 :

dalee. ti ZNAL - chto TechDept mozhet osibatsya (kak i bilo v sluchae s Viconom). MI - DELALI VSE CHTO MOGLI. mi - ne Angeli Gospodni - i VSEGO znat ne mozhem.

Mitch, 28.04.2007 21:25 :

eto ochevidno.

Случилось именно то про что я говорил еще в январе. Вот запросы на счет происхождения денег на счетах клиентов:

Momentalno.org, 29.03.2007 16:21 :

Добрый день.

Не посмотрите 75XXX62

хочет менять порядка 10k на webmoney

TechDept, 29.03.2007 17:18 :

Zdraste

posmotrel. vse ok s nim

Momentalno.org, 29.03.2007 17:35 :

отлично, спасибо

Momentalno.org, 27.03.2007 0:17 :

глянь плз 75XXX56

2к хочет менять на ВМ

Mitch, 27.03.2007 0:40 :

obichni klient.. пока ya ne vizhu nichego podozritelnogo..

Momentalno.org, 27.03.2007 0:40 :

ок... понял

И спустя **месяц (!)** выясняется что деньги взялись на счетах этих клиентов неизвестно откуда – по крайней мере так мне было заявлено.

Решение проблемы

В общем то неожиданностью это предложение для меня не стало . После моих ссылок на договор (CCS AgencyAgreement) я был послан именно туда , куда вы и подумали

Mitch, 28.04.2007 21:28 :

ya tebe uzhe skazal - 100% zamorozka.

Momentalno.org, 28.04.2007 21:28 :

нет

Mitch, 28.04.2007 21:28 :

ok. mozhesh podavat v sud.

Отношение к безопасности

Что касается отношения к безопасности транзакции и личных данных клиентов, приведу без комментариев наш разговор на эту тему:

Речь шла о том что никто и никогда не слышал про взлом webmoney и fethard и о пострадавших от таких взломов (как клиентов, так и обменных пунктов).

Momentalno.org, 25.04.2007 1:30 :

я работаю с фетом дольше, чем с вами - ну вот не страдают там обменники ...и в вебмани не страдают

Mitch, 25.04.2007 1:31 :

verno. WM i Fet - oni russkie. mi - ne russkie. **i u nas - net lishnih deneg**, Andrew

Сроки вывода денег

Все конечно заметили, что за последний месяц сроки увеличились с 2 недель до 4-6 недель. Причем даже если вам обещают 4 недели , то это совсем ничего не значит. Рискну предположить о какой сумме денег клиентов , находящейся ГДЕ ТО идет речь.

Mitch, 30.01.2007 1:21 :

tolko vot cheki - ludi stali k nam perevodit.. segodnya chekov na 240K prishlo...

Даже если не учитывать другие приходы на счета компании (wire transfer, АСН) и оценить ежедневную сумму приходов в 250 К\$ то получится сумма задержанных платежей это как минимум **2-2,5 млн.** долларов

Дальнейшая работа с русским рынком

Mitch, 30.01.2007 1:57 :

blyat... russkie - ZAEBALI.. rabotaem s mexikoi (eto osnovnoe dlya EBSG), rabotaem s Afrikoi (shikarni rinok), думаем про nekotorie arabskie strani.. nikakogo gemmora...

Momentalno.org, 30.01.2007 1:58 :

потому что тут жизнь такая

Mitch, 30.01.2007 1:58 :

v Afrike - esche HUZHE

Momentalno.org, 30.01.2007 1:58 :

неее...там проще...хотя может и хуже

Mitch, 30.01.2007 1:59 :

mozhet bit.. tolko menya ozhe ochen zaebalo nahoditsya mezhdru klientami i ihnimi zakonami....

Mitch, 30.01.2007 2:00 :

davno uzhe ne reklamiruemsya.. a oni lezut i lezut...

Mitch, 30.01.2007 2:00 :

kak tarakani...

Я думаю, что у клиентов не из бывшего СССР возможно и нет никаких проблем и месячных задержек с выводом - по крайней мере, никакой информации на западных форумах о таких сложностях найти не удалось. Хотя и не исключаю, что «множество клиентов» из стран Африки и Латинской Америки, с которым нет проблем, это просто фикция.