Эволюция мошенничества в системах интернет-банкинга

Способы мошенничества

Статистика хищений

Большинство хищений — это результат сетевых атак на клиентов банков

Принцип хищений

Способы совершения хищений

1. Копирование ключей электронной подписи на компьютер злоумышленника.

Способы совершения хищений

1. Копирование ключей электронной подписи на компьютер злоумышленника.

2. Скрытное формирование платежного поручения на компьютере бухгалтера (при подключенном носителе ключей).

Способы совершения хищений

1. Копирование ключей электронной подписи на компьютер злоумышленника.

2. Скрытное формирование платежного поручения на компьютере бухгалтера (при подключенном носителе ключей).

3. Подмена реквизитов легитимного платежного поручения перед подписанием.

Инструменты злоумышленника

1. Вредоносные программы:

   ZeuS, SpyEye, Carberp, RDPdoor, Shiz и др.

Инструменты злоумышленника

1. Вредоносные программы:

   ZeuS, SpyEye, Carberp, RDPdoor, Shiz и др.

2. Программы для удаленного управления компьютером:

   Radmin, TeamViewer, RDP-сервер Windows и др.

Инструменты злоумышленника

1. Вредоносные программы:

   ZeuS, SpyEye, Carberp, RDPdoor, Shiz и др.

2. Программы для удаленного управления компьютером:

   Radmin, TeamViewer, RDP-сервер Windows и др.

3. Связки эксплоитов:

   Blackhole, Nuclear Pack и др.

Инструменты злоумышленника

Carberp
Vendor of:
bot

Carberp is offline

Join Date: Dec 2010

Posts: 9

Deposit: $0 ?

Carberp bot + Bootkit

Банкбот Carberp

Мы решили возобновить продажи после долгого перерыва в связи с выходом новой версии бота с буткитом.
По сравнению с предыдущей версией улучшились стабильность, живучесть и функциональность.
Так же хочу отметить появление возможности аренды софта.

Все наши текущие клиенты, по каким-либо причинам потерявшие с нами связь, могут получить обновление своей сборки.
В качестве обновления будет предоставлена одна из вариций минимальной сборки, в зависимости от ранее приобретенной комплектации.
Новым клиентам такие вариации предоставляться не будут, для них существует только одна минимальная сборка.

Мы открыты для разного рода предложений, в т.ч. по написанию А3 и работе под %.
Предложения с условиями, при которых вы получаете текущий софт бесплатно, рассматриваться не будут.

Все вопросы и предложения просьба отправлять в jabber.
Все что оставляете в текущей теме, отправляете в PM или куда-то еще может остаться без внимания.
При накоплении достаточного количества вопросов я организую FAQ.

Краткое описание:

Каждая последующая сборка включает в себя предыдущие

Минимальная:
- Лоадер
- ФТП граббер (31 клиент)
- Пассворд граббер
- Форм граббер (IE, FF, Opera)
- ФТП сниффер
- Граббер basic-авторизации в IE
- Удаление cookie и sol в IE и FF
- DDOS
- Socks5 прокси
- Поддержка инжектов в IE и FF
- Программа для написания и отладки инжектов с удобным GUI
- Шифрование траффика
- Билдер
- Многофункциональная админка бота

Цена: от 5.000 до 40.000 USD

Инструменты злоумышленника

21.09.2012, 23:28 #1

nuc_support

Nuclear Pack
Вне форума
Регистрация: 17.09.2012
Сообщений: 3
Фонд: 0$?
Доверие: 0 ?
[TopicStarter]

Связка эксплойтов Nuclear Pack 2.0

Связка эксплойтов Nuclear Pack 2.0

Данный продукт предназначен для сетевого тестирования на наличие уязвимостей операционных систем, браузеров и их плагинов.
Запрещается использование связки и\или элементов связки в целях, нарущающих законы УК РФ, а так же в неправомерных действиях.
За использование данного продукта автор не несет ответственности, вы используете его на свой собственный страх и риск.
На данный момент присутствуют актуальные уязвимости Java.
Детальная статистика, поддержка нескольких потоков.
Постоянно чистые ip адреса и своевременные чистки.
Аренда на наших сервера с полной поддержкой.
На рынке с 2008 года.

Прайс цен:
price :
month:
50k / day limit / 1 month - 500 wmz
100k / day limit / 1 month - 800 wmz
200k / day limit / 1 month - 1200 wmz
300k / day limit / 1 month - 1600 wmz

2 week:
50k / day limit / 2 week - 300 wmz
100k / day limit / 2 week - 500 wmz

Инструменты злоумышленника

Логин/Email: Регистрация

Пароль: Войти Забыл пароль!

Вход с использованием SSL-сертификата

Войти через

ГЛАВНАЯ	РЕГИСТРАЦИЯ	FAQ	КОНТАКТЫ	ФОРУМ

Свободные потоки (детализированные выборки):

Страницы: 1 | 2

Россия (RU), Москва, Разное:	от **212** руб. за 1000 (~$7.07/K)	Свободно:	вчера - **20,118**	сегодня - **26,040**	Заказ
Россия (RU), Москва, Развлечения:	от **240** руб. за 1000 (~$8/K)	Свободно:	вчера - **33,222**	сегодня - **18,886**	Заказ
Россия (RU), Москва, Эротика и секс:	от **175** руб. за 1000 (~$5.83/K)	Свободно:	вчера - **21,224**	сегодня - **15,106**	Заказ
Россия (RU), Москва, Игры:	от **220** руб. за 1000 (~$7.33/K)	Свободно:	вчера - **16,506**	сегодня - **11,501**	Заказ
Россия (RU), Москва, Кино, Видео:	от **138** руб. за 1000 (~$4.6/K)	Свободно:	вчера - **26,656**	сегодня - **11,207**	Заказ
Россия (RU), Москва, Порталы:	от **139** руб. за 1000 (~$4.63/K)	Свободно:	вчера - **8,050**	сегодня - **10,521**	Заказ
Россия (RU), Москва, Программы:	от **151** руб. за 1000 (~$5.03/K)	Свободно:	вчера - **12,642**	сегодня - **7,798**	Заказ
Россия (RU), Москва, Музыка:	от **131** руб. за 1000 (~$4.37/K)	Свободно:	вчера - **11,613**	сегодня - **7,175**	Заказ
Россия (RU), Москва, Форумы:	от **131** руб. за 1000 (~$4.37/K)	Свободно:	вчера - **8,820**	сегодня - **5,866**	Заказ
Россия (RU), Москва, Мода и красота:	от **231** руб. за 1000 (~$7.7/K)	Свободно:	вчера - **1,449**	сегодня - **5,558**	Заказ
Россия (RU), Москва, Юмор:	от **131** руб. за 1000 (~$4.37/K)	Свободно:	вчера - **8,099**	сегодня - **5,369**	Заказ
Россия (RU), Москва, Интернет:	от **169** руб. за 1000 (~$5.63/K)	Свободно:	вчера - **6,293**	сегодня - **4,431**	Заказ

Инструменты злоумышленника

Продаже шеллов Ру от MaKaKaZ

17.05.2011, 21:59

antichat

MaKaKaZ
Новичок
Регистрация: 30.10.2009
Сообщения: 1
Провел на форуме:
9 часов 58 минут 25 секунд

Репутация: 0

Продаже шеллов Ру от MaKaKaZ

Шелы появляются ежедневно.
Только Ру.

Цена от 2 вмз за 10 тиц в зависимости от кол-ва страниц в индексе.

Как првило - правка всего, заливка и анзип, консоль.

152585582

08.03.2013, 22:50

kol78
Новичок

kol78 вне форума

Регистрация: 08.03.2013

Сообщений: 1

Репутация: 0

Продаю Шеллы

Тиц 0, меньше 100 страниц в индексе -0.5-1$
Тиц 0, больше 100 страниц в индексе - 1.5$
Тиц 10 -- 2.5$
Тиц больше 10, - 2.5$ за каждые 10 ТиЦ
есть сервера (крупные и не очень)
бывает с трафом

При оптовых покупках, хорошие скидки

ICQ: 488078879

Обналичивание

1. Перевод на банковскую карту, снятие через банкомат.

Обналичивание

1. Перевод на банковскую карту, снятие через банкомат.

2. Пополнение счета у оператора сотовой связи, снятие при расторжении договора.

Обналичивание

1. Перевод на банковскую карту, снятие через банкомат.

2. Пополнение счета у оператора сотовой связи, снятие при расторжении договора.

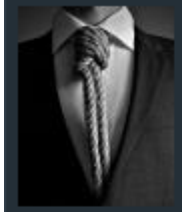
3. Перевод на счет ИП, снятие через кассу банка.

4. Перевод на счет юр. лица, снятие через кассу банка.

Обналичивание

05.09.2011, 01:54 #1

sanya



sanya is offline

Join Date: 20.04.2011

Posts: 49

Reputation: 16 +/-

Cashing in RU - [ru] Обналичка в РУ

Сервис по обналу в РУ.

Спектр услуг:

- Изготовление и продажа ATM карт Российских банков - от 250 lr*
- Обналичивание переводов WesternUnion, MoneyGram, Юнистрим, Контакт и других на территории России.
- **Предоставим свои счета под любые цели.** Трансфер, обнал, транзит. Физики и юрики в наличии.

Правила Сервиса:

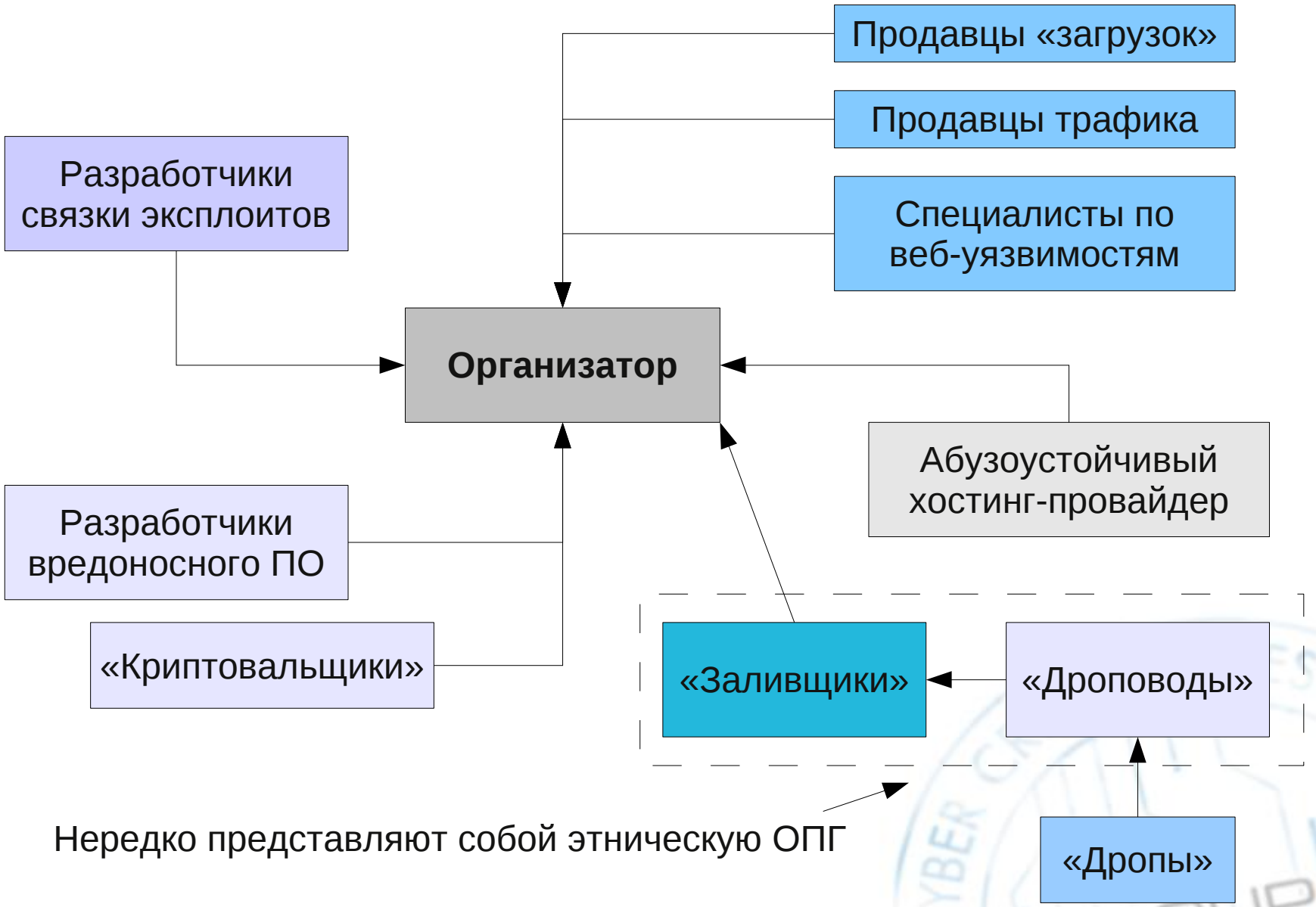
- **Сервис с удовольствием работает с грязными и серыми деньгами!**
- Сервис несёт ответственность только за своих дропов, работоспособность и комплектацию товара. Мы не несём ответственность за утерю Вами документов или информации, за действия ЭПС, СБ банков, Ваши действия и Ваших партнёров.
- Не рекомендуется хранить деньги на картах. Это инструмент для обнала, а не банковская ячейка.
- Гарантия работоспособности товара 6 месяцев, только в случае отсутствия манипуляций с Вашей стороны.
- Проверяйте товар после получения. Претензии принимаются в течении суток после получения товара.
- Обнал денежных переводов возможен только на наши имена (мужские и женские) и только при наличии полной информации к переводу.
- Сервис полностью анонимен. Все разговоры вне форума конфиденциальны и должны там и остаться.
- Сервис оставляет за собой право отказать любому в предоставлении услуг.
- **Сервис в праве отказать Вам в общении при отсутствии софта шифрующего переписку.**
- Оплата LibertyReserve. Гарант за Ваш счёт.
- Первый контакт ПМ.

*Цены на ATM карты варьируются в зависимости от банка, в котором нужна карта, уровня карты(моментум, классика, голд) и цели приобретения товара. Мы продаём ATM карты под любые цели, в том числе грязь. Пожалуйста максимально точно укажите цель приобретения инструмента. От этого зависит не только цена товара, но и наша с Вами безопасность. Дропы подбираются в зависимости от уровня желаемой анонимности. Само собой, что дроп под вывод чистых ВМ и дроп под грязь, будут отличаться. Не экономьте на безопасности!

Last edited by sanya : 08.02.2012 at 07:37. Reason: Новые услуги

QUOTE

Схема преступной группы



Эволюция мошенничества

Защитные меры и контрмеры

→ криптографическая подпись документов

← копирование ключей подписи злоумышленником

Защитные меры и контрмеры

→ криптографическая подпись документов

← копирование ключей подписи злоумышленником

→ применение неизвлекаемых ключей подписи

← подпись документа при установленном носителе ключей

Защитные меры и контрмеры

→ подтверждение переводов по телефону

← мошенники инициируют подтверждающий звонок в банк

Защитные меры и контрмеры

→ подтверждение переводов по телефону

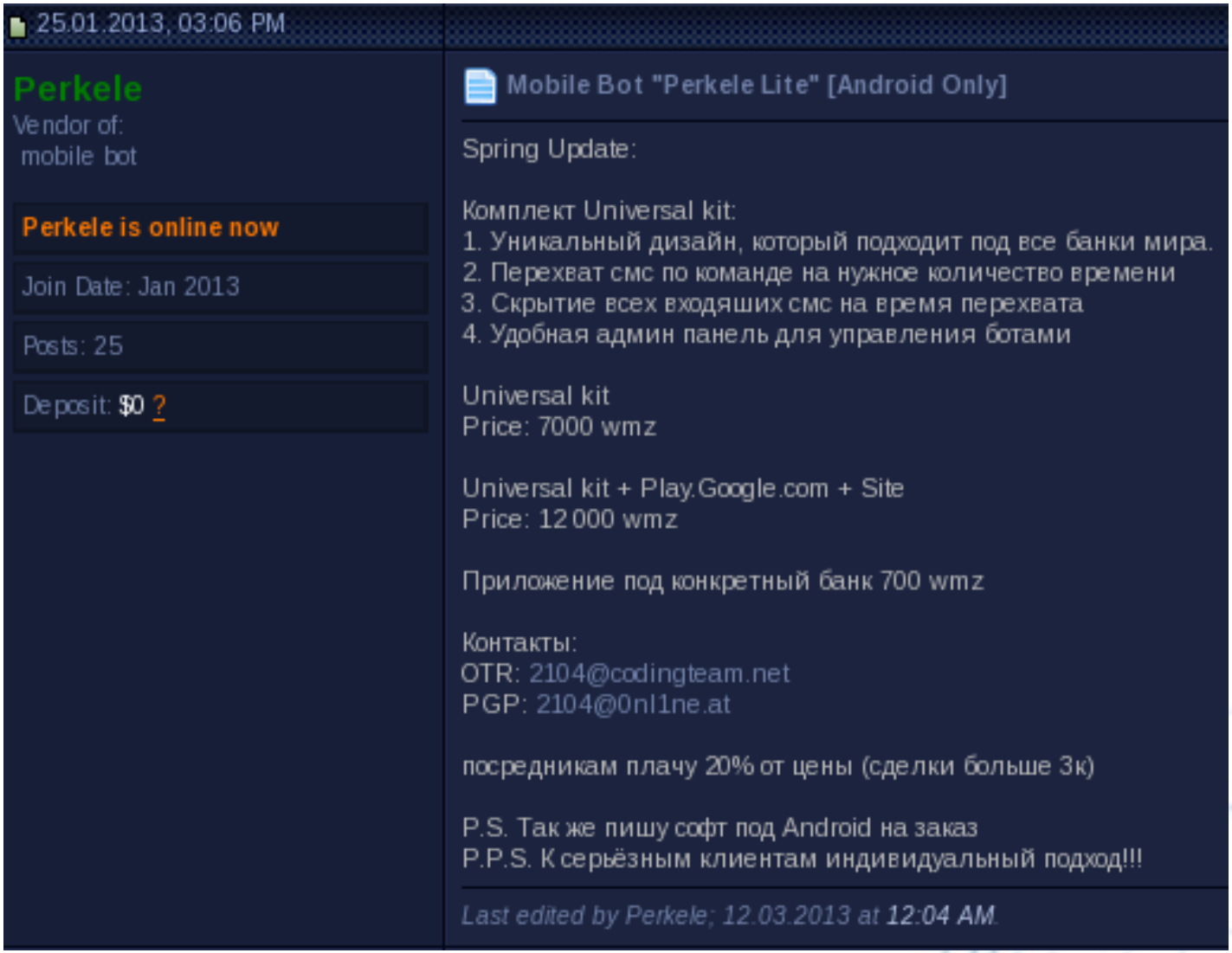
← мошенники инициируют подтверждающий звонок в банк

→ внедрение СМС-подтверждений

← восстановление SIM-карт по поддельным доверенностям

← применение вредоносных программ для моб. телефонов

Защитные меры и контрмеры



25.01.2013, 03:06 PM

Perkele
Vendor of:
mobile bot

Perkele is online now

Join Date: Jan 2013

Posts: 25

Deposit: $0 ?

Mobile Bot "Perkele Lite" [Android Only]

Spring Update:

Комплект Universal kit:
1. Уникальный дизайн, который подходит под все банки мира.
2. Перехват смс по команде на нужное количество времени
3. Скрытие всех входяших смс на время перехвата
4. Удобная админ панель для управления ботами

Universal kit
Price: 7000 wmz

Universal kit + Play.Google.com + Site
Price: 12 000 wmz

Приложение под конкретный банк 700 wmz

Контакты:
OTR: 2104@codingteam.net
PGP: 2104@0nl1ne.at

посредникам плачу 20% от цены (сделки больше 3к)

P.S. Так же пишу софт под Android на заказ
P.P.S. К серьёзным клиентам индивидуальный подход!!!

Last edited by Perkele; 12.03.2013 at 12:04 AM.

Защитные меры и контрмеры

→ внедрение «антифрод»-систем

← появление различных методов противодействия:

1. назначение платежа соответствует деятельности организации;
2. отправка платежного поручения с компьютера потерпевшего;
3. учет ограничения по сумме платежа и т. п.

Защитные меры и контрмеры

→ увеличение скорости реакции на мошенничество

← сокрытие факта мошенничества:

1. удаление файлов операционной системы;
2. перезапись первых секторов накопителя;
3. перезапись всего содержимого накопителя.

Защитные меры и контрмеры

→ увеличение скорости реакции на мошенничество

← сокрытие факта мошенничества:

1. удаление файлов операционной системы;
2. перезапись первых секторов накопителя;
3. перезапись всего содержимого накопителя;

4. подмена отображаемого остатка на счете;
5. сокрытие мошеннических платежных поручений.

Какие следы искать при расследовании?

В банках

✔ IP-адреса, с которых входили в систему ДБО потерпевшего

✔ MAC-адреса компьютеров, с которых входили в систему ДБО потерпевшего

✔ То же самое и для систем ДБО «дропов» и их юр. лиц

✔ Сообщения эл. почты, полученные банками от «дропов» (перевыпуск ключей, технические проблемы)

У пострадавшего клиента

✔ Машинные носители информации из бухгалтерского компьютера (НЖМД, SSD), копия его оперативной памяти

✔ Носители ключевой информации (дискеты, USB Flash, Token)

✔ Лог-файлы сетевых устройств (прокси-серверы, NAPT)

✔ Копия (дамп) сетевого трафика

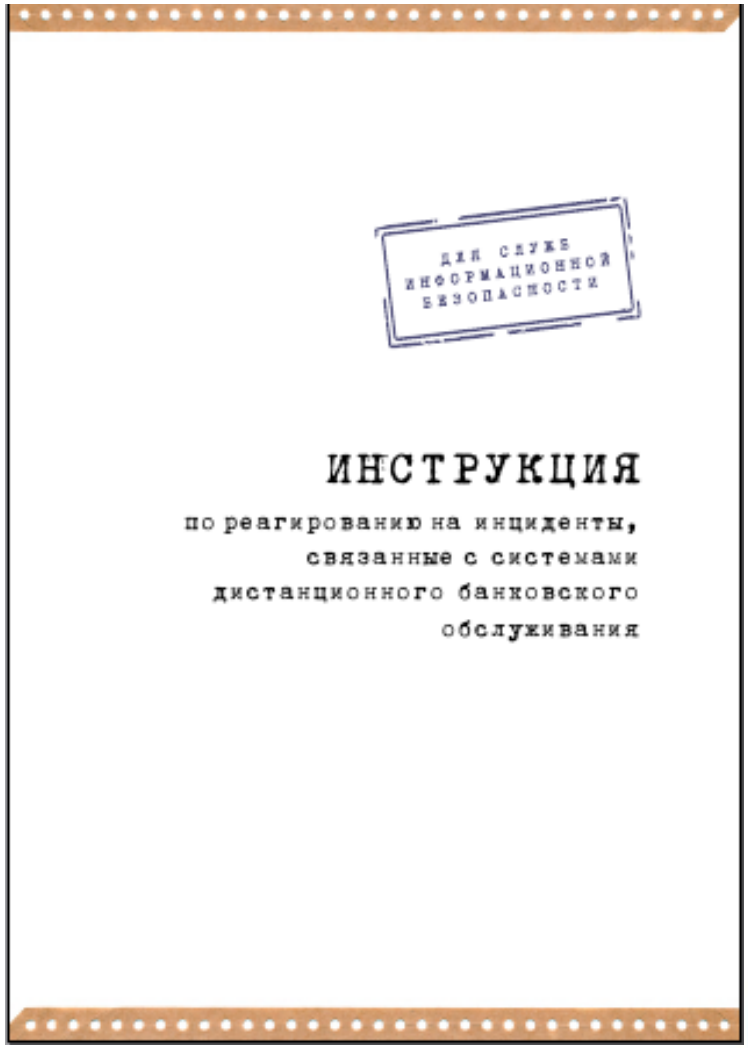
✔ Описание инцидента со слов работников

У интернет-провайдера клиента

- ✔ Любые журналы сетевых подключений потерпевшего

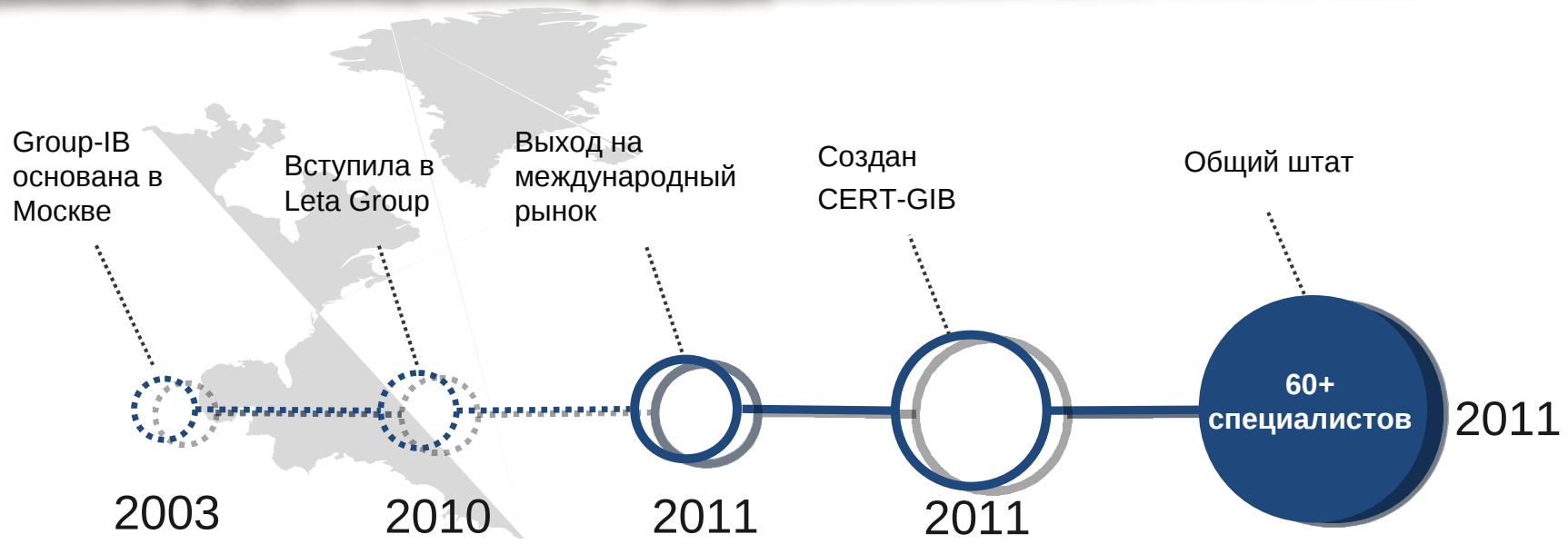
Инструкция по реагированию

http://www.group-ib.ru/images/files/Group-IB_dbo_instruction.pdf



Group-IB

Group-IB



Этапы развития

Российский лидер в сфере РКП
Первая и единственная компания в СНГ, предоставляющая весь спектр услуг в области расследования инцидентов ИБ.

Комплекс услуг
Прединцидентный консалтинг.
Реагирование.
Криминалистическое исследование.
Расследование.
Юридическое сопровождение.
Постинцидентный консалтинг.

Резидент Сколково
Проект — комплексная система противодействия киберпреступности CyberCop.

Первый 24/7 CERT в Восточной Европе
CERT-GIB — первый частный круглосуточный центр реагирования на инциденты ИБ в России.

Наши партнеры

- ✓ Группы по реагированию на инциденты (CERT) в 56 странах мира
- ✓ Антивирусные компании
- ✓ Производители решений по компьютерной криминалистике и информационной безопасности
- ✓ Университеты США и Европы
- ✓ Международные организации по компьютерной криминалистике
- ✓ Ассоциация сертифицированных специалистов по борьбе с мошенничествами (ACFE)
- ✓ Центры изучения угроз информационной безопасности

Наши награды

Благодарственные письма

Swedbank

Генерал
ООО «Г
безопаси
САЧКО

Уважаемый Илья Константинович!

От лица ОАО «Сведбанк» и от себя лично благодарю Вас
активное содействие в борьбе с киберпреступностью. Наш банк и
процветания, успеха в делах и финансового благополучия, и надее
плодотворное сотрудничество.

Начальник Управления
риск-менеджмента,
член Правления

QIWI

ЗАО «Объединенная система моментальных платежей»

Генеральному директору компании
ООО «Группа Информационной безопасности»
Сачкову И.К.

Уважаемый Илья Константинович!

От лица ЗАО «Объединенная система моментальных платежей», благодарим Вас и специалистов компании ООО «Группа Информационной безопасности», за активное содействие в борьбе с киберпреступностью.

Благодаря тесному сотрудничеству компаний, нам удалось предотвратить ряд инцидентов, связанных с информационной безопасностью. Департамент безопасности, в лице Вице-президента Загибелина В.Л., надеется на дальнейшее эффективное сотрудничество.

ecco

Генеральному директ
ООО «Группа инфор
безопасности»
Сачкову И.К.

Уважаемый Илья Константинович!

«ЭККО-РОС» выражает Вам и сотрудникам
ионных технологий» свою признательность за проделан
сайта http://ecco-russia.ru, незаконно использовавшего т
для совершения мошеннических действий.
емся на дальнейшее плодотворное сотрудничество.

ый директор

ZURICH

Общество с ограниченной ответственностью
Страховая компания «Цюрих»

г. Москва
30 декабря 2010 г.

Уважаемые господа,

Страховая компания "Цюрих" выражает свою благодарность специалистам Group-IB за помощь в расследовании инцидента информационной безопасности.

В ходе проведения криминалистических исследований эксперты Group-IB показали высокий уровень профессионализма, скорость реакции и готовность к решению самого широкого спектра задач в области реагирования на инциденты.

Мы оцениваем компанию Group-IB как надежного поставщика услуг в области расследования инцидентов и обеспечения информационной безопасности и будем рекомендовать ее нашим партнерам.

С уважением,
Усов А.В.

Открытое акционерное общество "Российский Сельскохозяйственный банк"
(ОАО "РОССЕЛЬХОЗБАНК")

Генеральному директору компании
"Группа информационной
безопасности – Group-IB
И.К.Сачкову

Уважаемый Илья Константинович!

А. М. Сычев

ООО «Майкрософт Рус»
Россия
121614, г.Москва
Ул. Крылатская, 17, стр. 1

Тел.: +7 (495) 967 8585
Факс: +7 (495) 967 8500

Microsoft Rus LLC
17 Krylatskaya st., bld. 1
121614, Moscow
Russia

Microsoft

Генеральному директору
Компании Group-IB
Сачкову Илье Константиновичу

Уважаемый Илья Константинович!

ООО «Майкрософт Рус» выражает Вам и вашим сотрудникам глубокую признательность за работу в области предупреждения и пресечения нарушений прав на интеллектуальную собственность.

Особенно хочется отметить вашу активную и последовательную работу в области предупреждения нарушений интеллектуальных прав в сети Интернет, а также в банковской сфере.

В течение последних лет мы наблюдаем значительное снижение уровня компьютерного пиратства в России, со своей стороны мы готовы оказать всестороннюю поддержку и оперативно предоставлять всю необходимую информацию, позволяющую максимально точно выявлять признаки незаконного использования программных продуктов.

Защита интеллектуальной собственности является важнейшим фактором развития экономики России, укрепления позиций нашей страны в мире, развития ее интеллектуального потенциала, мы рассчитываем, что Вы продолжите свою эффективную и значимую работу на этом направлении.

С уважением,

Евгений Шагалов

Руководитель Службы расследований
Департамента по правовым и корпоративным вопросам ООО «Майкрософт Рус»

Альфа-Банк

Генеральному директору Group-IB
Сачкову И. К.

Уважаемый Илья Константинович!

ОАО «Альфа-Банк» благодарит экспертов Group-IB за тесное сотрудничество в сфере противодействия киберпреступности. В рамках мониторинга существующих бот-сетей специалистами Вашей компании удается регулярно собирать данные, от которых зависит безопасность наших клиентов и репутация Банка. Благодаря высокому уровню профессионализма и качественному выполнению взятых на себя обязательств сотрудники Group-IB предоставляют Банку достоверные данные о скомпрометированных реквизитах наших клиентов, что позволяет успешно избегать возможных мошенничеств.

Надеемся на дальнейшее плодотворное сотрудничество с Вашей компанией в интересах обеспечения информационной безопасности клиентов нашего Банка.

С уважением,
Заместитель Руководителя Блока «Безопасность»
Директор Департамента информационно-технологической безопасности

Бутенко В. В.

СБЕРБАНК РОССИИ

ДЕПАРТАМЕНТ БЕЗОПАСНОСТИ

Генеральному директору
ООО «Группа информационной
безопасности»
И.К. Сачкову

Уважаемый Илья Константинович!

И.о. Директора
Департамента безопасности

В.В. Крайнов

Антифишинг.Ру

antiphishing.ru

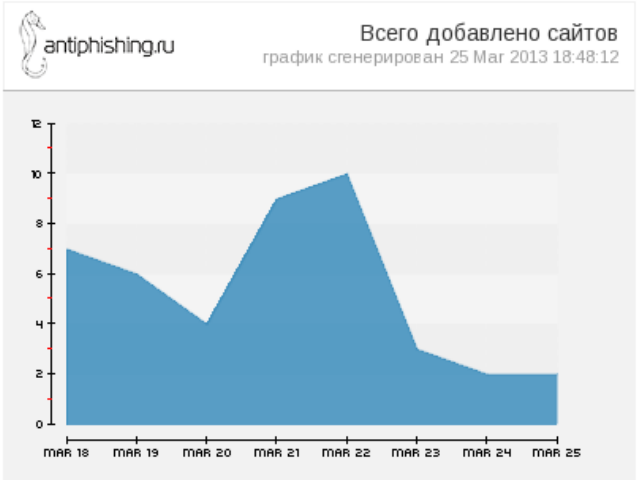
Статистика

Всего сайтов добавлено
14886

Всего сайтов подтверждено как фишинговые
607

Лучшие 10 анти-фишеров

№	Репортер	Количество фишинговых сайтов
1	tomb-raider	19
2	germanov	2
3	egermanov	1
4	Northore	1



Вопросы?

Максим Суханов

suhanov@group-ib.ru

+7 495 66I 55 38 www.group-ib.ru www.letagroup.ru