

ТЕХНИЧЕСКОЕ ЗАКЛЮЧЕНИЕ

По фактам несанкционированного доступа к ящику электронной почты gousseau@mail.ru.

Введение

24 января 2009 г. автором данного документа был получен запрос от владельца ящика электронной почты gousseau@mail.ru с просьбой провести анализ и сделать заключение по фактам предположительного несанкционированного доступа к указанному ящику электронной почты. Предоставленная для анализа информация перечислена в разделе "Исходные факты" и приведена в приложениях к настоящему документу.

Об авторе

Амиран Алавидзе является обладателем степеней CISA (Certified Information Systems Auditor) и CISSP (Certified Information Systems Security Professional) и имеет более чем семилетний опыт в области информационной безопасности, в том числе расследования компьютерных инцидентов. С автором можно связаться по электронной почте amiran@alavidze.org. Данный документ отражает личную точку зрения автора и не может быть связан с его работодателем.

Исходные факты

1. Электронные письма, содержащие уникальные ссылки, отправленные на адрес gousseau@mail.ru. (Приложение 1)
2. Выдержки из журналов доступа к серверам kknop.com и quest2009.mhost.ru. (Приложение 2).
3. Снимок экрана с комментарием, оставленным пользователем [anatbel](http://livejournal.com) ("Анатолий Белкин") на сайте livejournal.com. (Приложение 3)

Заключение

При анализе исходных фактов было выяснено следующее:

- IP адрес **85.93.137.235**, фигурирующий в исходных фактах, принадлежит к динамическому пулу адресов Московского провайдера Интернет–Космос (www.spacenet.ru) – см. Приложение 4.
- Поиск по сайту livejournal.com с использованием сервиса <http://deep-water.ru/luser/> дает однозначное соответствие IP адреса 85.93.137.235 пользователю **anatbel** (см. Приложение 5).
- Поиск истории редактирования по сайту ru.wikipedia.org с IP адреса 85.93.137.235 содержит большое количество страниц со ссылками на Анатолия Белкина (см. Приложение 6, доступно по ссылке <http://ru.wikipedia.org/wiki/Служебная:Contributions/85.93.137.235>).

По проведенному анализу основной версией необходимо считать, что несанкционированный доступ к ящику электронной почты gousseau@mail.ru и комментарии на сайте livejournal.com под именем [anatbel](http://livejournal.com) ("Анатолий Белкин") сделаны с одного и того же компьютера. Данная версия предполагает, что уникальные ссылки (пункт 1 исходных фактов) были посланы только на адрес

электронной почты rousseau@mail.ru (что подтверждается отправителю указанных писем), и что IP адрес 85.93.137.235 не является адресом коллективного пользования (т.е., например, не выделен какой-нибудь организации), что частично подтверждается имеющейся информацией (диапазон адресов, к которому он принадлежит, помечен провайдером как "VPN-Block-3"). Окончательные выводы можно сделать при наличии информации от провайдера о принадлежности адреса.

Комментарии

Данный анализ основывается исключительно на предоставленных фактах, а также на оценке вероятности событий в различных схемах, которые могли привести к таким же фактам. В случае поступления дополнительной информации или признании некоторых базовых фактов (1-3) неверными, вывод либо вероятности описанных вариантов могут измениться. Однако необходимо заметить, что одно только появление дополнительных фактов (не опровергающих факты 1-3) не может изменить сути данного заключения, которые согласуются также с косвенными факторами в исходной информации.

03 февраля 2009 года
Амиран Алавидзе

Приложение 1

E-mail сообщения, отправленные на адрес rousseau@mail.ru

Первое сообщение (текст сообщения: "Макс, распечатай, плз, в цвете до следующей субботы.")

Date: Thu, 22 Jan 2009 21:07:34 +0300
From: Maxim Potashev <max_po@rambler.ru>
Reply-To: Maxim Potashev <max_po@rambler.ru>
X-Priority: 3 (Normal)
Message-ID: <633711632.20090122210734@rambler.ru>
To: rousseau@mail.ru
Subject: =?windows-1251?B?8ODn5ODy6ugg6iDi7u/w7vHg7A==?=
In-Reply-To: <618baad40901220911n7e77dc7cye05d25004604afe6@mail.gmail.com>
References: <618baad40901220911n7e77dc7cye05d25004604afe6@mail.gmail.com>
MIME-Version: 1.0
Content-Type: text/plain; charset=windows-1251
Content-Transfer-Encoding: quoted-printable

=CC=E0=EA=F1, =F0=E0=F1=EF=E5=F7=E0=F2=E0=E9, =EF=EB=E7, =E2 =F6=E2=E5=F2=
=E5 =E4=EE =F1=EB=E5=E4=F3=FE=F9=E5=E9 =F1=F3=E1=E1=EE=F2=FB.

<http://quest2009.mhost.ru/0026d398.jpg>
http://quest2009.mhost.ru/caricature_charles_philipon.jpg
http://quest2009.mhost.ru/caricature_charles_philipon_pear.jpg
<http://quest2009.mhost.ru/perun.jpg>

Второе сообщение

Date: Sat, 24 Jan 2009 01:23:02 +0300
From: Konstantin Knop <kostyaknop@gmail.com>
X-Mailer: The Bat! (v4.1.9) Home
X-Priority: 3 (Normal)
Message-ID: <85780526.20090124012302@gmail.com>
To: rousseau@mail.ru
Subject: IP-adresa, o kotoryx ty sprashival
MIME-Version: 1.0
Content-Type: text/plain; charset=koi8-r
Content-Transfer-Encoding: 8bit

Здравствуйте, Rousseau.

Я сделал скриншотики и положил к себе на временное хранение

<http://www.kknop.com/temp/iptemp/200812250810ip.jpg>

<http://www.kknop.com/temp/iptemp/200812290844ip.jpg>

Свистни, когда выкачаешь, - я уберу их оттуда.

--

С уважением,

Konstantin

<mailto:kostyaknop@gmail.com>

=====

Приложение 2

Выдержка из журналов доступа к сайту quest2009.mhost.ru

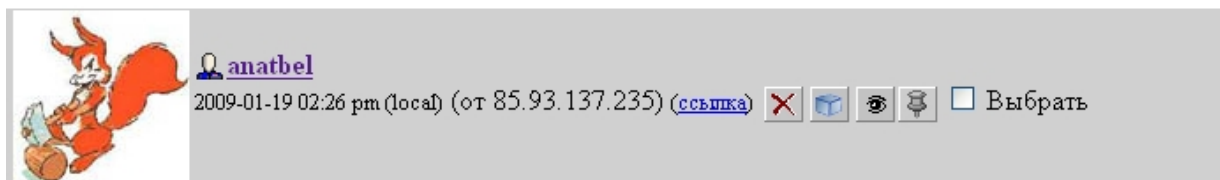
```
85.93.137.235 - - [22/Jan/2009:22:46:21 +0300] "GET /
caricature_charles_philipon.jpg HTTP/1.0" 200 164714 "-" "Mozilla/
5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.0.5) Gecko/2008120122 Firefox/
3.0.5;MEGAUPLOAD 1.0"
85.93.137.235 - - [22/Jan/2009:22:46:28 +0300] "GET /
caricature_charles_philipon_pear.jpg HTTP/1.0" 200 120055 "-" "Mozilla/5.0
(Windows; U; Windows NT 5.1; ru; rv:1.9.0.5) Gecko/2008120122 Firefox/
3.0.5;MEGAUPLOAD 1.0"
85.93.137.235 - - [22/Jan/2009:22:46:35 +0300] "GET /0026d398.jpg HTTP/1.0"
200 389214 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.0.5)
Gecko/2008120122 Firefox/3.0.5;MEGAUPLOAD 1.0"
85.93.137.235 - - [22/Jan/2009:22:46:42 +0300] "GET /perun.jpg HTTP/1.0" 200
267289 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.0.5) Gecko/
2008120122 Firefox/3.0.5;MEGAUPLOAD 1.0"
```

Выдержка из журналов доступа к сайту kknop.com

```
85.93.137.235 - - [24/Jan/2009:00:18:32 -0500] "GET /temp/iptemp/
200812250810ip.jpg HTTP/1.1" 200 16511 "-" "Mozilla/5.0 (Windows; U; Windows
NT 5.1; ru; rv:1.9.0.5) Gecko/2008120122 Firefox/3.0.5;MEGAUPLOAD 1.0"
kknop.com
85.93.137.235 - - [24/Jan/2009:00:18:39 -0500] "GET /temp/iptemp/
200812290844ip.jpg HTTP/1.1" 200 17090 "-" "Mozilla/5.0 (Windows; U; Windows
NT 5.1; ru; rv:1.9.0.5) Gecko/2008120122 Firefox/3.0.5;MEGAUPLOAD 1.0"
kknop.com
```

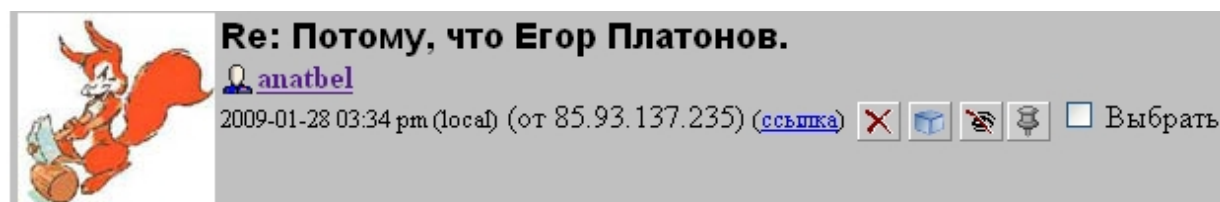
Приложение 3

Снимки экрана с комментариями, оставленным пользователем **anatbel** ("Анатолий Белкин") на сайте **livejournal.com**



The screenshot shows a comment header for user **anatbel**. On the left is a profile picture of a red cartoon rabbit. To the right of the picture is the user's name **anatbel** with a small profile icon. Below the name is the timestamp "2009-01-19 02:26 pm (local) (от 85.93.137.235)" and a blue link labeled "(ссылка)". To the right of the link are four small icons: a red 'X', a blue cube, an eye, and a speech bubble. Further right is a checkbox labeled "Выбрать".

Работу? Это тьяканье называется работой? :))



The screenshot shows a comment header for user **anatbel**. On the left is a profile picture of a red cartoon rabbit. To the right of the picture is the user's name **anatbel** with a small profile icon. Below the name is the timestamp "2009-01-28 03:34 pm (local) (от 85.93.137.235)" and a blue link labeled "(ссылка)". To the right of the link are four small icons: a red 'X', a blue cube, a hand with a slash, and a speech bubble. Further right is a checkbox labeled "Выбрать".

Смотри-ка!

Приложение 4

Информация об IP адресе 85.93.137.235

235.137.93.85.IN-ADDR.ARPA.icosmos.ru (85.93.137.235)



85.93.137.0 - 85.93.137.255

Internet-Cosmos, VPN Block-3



Internet-Cosmos contacts

Internet-Cosmos Ltd.
Nijnyaya Krasnoselskaya str.,39
105066, Moscow
Russia
phone: +7 095 7421026
+7 495 7421026
fax-no: +7 095 2612655
+7 495 2612655



Oleg A Lukashin

Internet-Cosmos Ltd.
Nijnyaya Krasnoselskaya str.,39
105066, Moscow
Russia
phone: +7 095 7421026
+7 495 7421026
phone: +7 095 7421027
+7 495 7421027
fax-no: +7 095 7421028
+7 495 7421028







Приложение 5

Результаты поиска по сайту livejournal.com через сервис <http://deerp-water.ru/ljuser/>

Поиск по IP адресу:

Страницы: **1** Введите точное имя пользователя LiveJournal: Или укажите IP для поиска:

2 элементов < предыдущая следующая >











№	ИнтернетАдрес	Имя пользователя(ссылка на список его адрессов) ↓	Версия его браузера	Когда смотрел?(MSK)
1	 85.93.137.235 RUSSIAN FEDERATION 	http://anatbel.livejournal.com/friends/ -  anatbel	Mozilla/5.0 (Windows; U; Windows	08-08-2008 9:35
2	 85.93.137.235 RUSSIAN FEDERATION 	http://anatbel.livejournal.com/friends/ -  anatbel	Mozilla/5.0 (Windows; U; Windows	19-01-2009 18:43

Страницы: **1** < предыдущая следующая >

Поиск по имени пользователя:

Страницы: **1** Введите точное имя пользователя LiveJournal: Или укажите IP для поиска:


4 элементов < предыдущая следующая >

№	ИнтернетАдрес	Имя пользователя(ссылка на список его адрессов) ↓	Версия его браузера	Когда смотрел?(MSK)
1	 85.93.137.235 RUSSIAN FEDERATION 	http://anatbel.livejournal.com/friends/ -  anatbel	Mozilla/5.0 (Windows; U; Windows	08-08-2008 9:35
2	 62.105.143.90 RUSSIAN FEDERATION 	http://anatbel.livejournal.com/friends/ -  anatbel	Mozilla/4.0 (compatible; MSIE 6.0	08-08-2008 11:06
3	79.111.134.77	http://anatbel.livejournal.com/friends/ -  anatbel	Mozilla/5.0 (Windows; U; Windows	19-01-2009 19:06
4	 85.93.137.235 RUSSIAN FEDERATION 	http://anatbel.livejournal.com/friends/ -  anatbel	Mozilla/5.0 (Windows; U; Windows	19-01-2009 18:43

Страницы: **1** < предыдущая следующая >

Приложение 6

Результат поиска истории редактирования с IP адреса 85.93.137.235 по сайту ru.wikipedia.org



Википедия
Свободная энциклопедия

навигация

- Заглавная страница
- Рубрикация
- Индекс А — Я
- Избранные статьи
- Случайная статья
- Текущие события

поиск

Перейти Найти

участие

- Сообщить об ошибке
- Портал сообщества
- Форум
- Свежие правки
- Новые страницы
- Справка
- Пожертвования

инструменты

- RSS Atom
- Спецстраницы

[Представиться / зарегистрироваться](#)

[служебная страница](#)

Вклад участника

Материал из Википедии — свободной энциклопедии
Вклад 85.93.137.235 ([обсуждение](#) | [Журнал блокировок](#) | [Журналы](#))

Поиск вклада

Показать только вклад, сделанный с новых учётных записей

IP-адрес или имя участника: Пространство имён:

С года (и ранее): С месяца (и ранее):

(недавние | [старейшие](#)) [Просмотреть](#) ([более новые 50](#)) ([более старые 50](#)) ([20](#) | [50](#) | [100](#) | [250](#) | [500](#))

- 13:38, 28 декабря 2008 (история) (разн.) Неспроста (команда ЧГК)
- 18:34, 27 сентября 2008 (история) (разн.) Чемпионат мира по «Что? Где? Когда?» (*→2008*)
- 20:48, 13 июля 2008 (история) (разн.) Список пользователей «Живого журнала» (*→Список*)
- 20:10, 25 октября 2007 (история) (разн.) Белкин, Анатолий Рафаилович
- 20:09, 25 октября 2007 (история) (разн.) Белкин, Анатолий Рафаилович
- 20:08, 25 октября 2007 (история) (разн.) Белкин, Анатолий Рафаилович
- 07:16, 19 октября 2007 (история) (разн.) Белкин, Анатолий Рафаилович
- 09:04, 7 августа 2007 (история) (разн.) Неспроста (команда ЧГК)
- 09:01, 7 августа 2007 (история) (разн.) Неспроста (команда ЧГК)
- 09:00, 7 августа 2007 (история) (разн.) Неспроста (команда ЧГК)
- 19:30, 30 июля 2007 (история) (разн.) Факультет управления и прикладной математики МФТИ (*→Известные выпускники*)
- 19:29, 30 июля 2007 (история) (разн.) Факультет управления и прикладной математики МФТИ (*→Известные выпускники*)
- 19:27, 30 июля 2007 (история) (разн.) Факультет управления и прикладной математики МФТИ (*→Известные выпускники*)
- 19:21, 30 июля 2007 (история) (разн.) Белкин, Анатолий Рафаилович
- 18:46, 16 июля 2007 (история) (разн.) Белкин, Рафаил Самуилович (*→Биография*)
- 18:39, 16 июля 2007 (история) (разн.) Белкин, Анатолий Рафаилович
- 20:53, 10 января 2007 (история) (разн.) Белкин, Анатолий Рафаилович
- 20:52, 10 января 2007 (история) (разн.) Белкин, Анатолий Рафаилович
- 20:43, 27 сентября 2006 (история) (разн.) Белкин, Анатолий Рафаилович

