

# From Russia with love.exe Pt. 2

Underground Hacking Forums from Former East Bloc

# Shhpeakers.. :)



# FY & grugq

Two lingual experts well known for their skillful tongues, the grugq and fyodor have spent 6 months actively monitoring dozens of russian web forums to uncover the secrets of the russian hacker culture. This talk focuses on new threats and trends which are discussed in the open on these sites, but are generally inaccessible to the larger security community due to the language barrier. Ladies! Ask about our private demonstrations! :D

# Outline

- Hax0r Revolution Intro
- Intelligence: Digging in a pile of trash
- Personalities, Lingo, Monetization
- Technology behind: Tools of trade
- Future Plans

# Hax0r Revolution

# Hax0r Revolution

- 100% money-driven
- Prerequisites:
  - Imbalance of Economic system
  - Globalization of payment systems
  - Accessibility
  - Laws, Languages, Cold War, ...

# Revolutionist targets

- Average PC users (your mom and dad)
- Rarely - corporations

# You being Own3d

- Exploiting vulnerabilities in Client software (mostly browsers, browser's add-ons, browser's plugins, ..)
- Social engineering (computer users are dumb) -> “fake av software”, .pdf.exe things and other old tricks



# Peeking behind the scene

- Looking at the market
- Items and patterns of trade
- Personalities
- Quantified analysis

# Digging in a pile of trash

# Forums

## [Брут Вконтакте ru Vkontakte.ru brute](#)

Брут для Вконтакте ru, bruteforce вконтакте

 [Sloyka](#)  [Vk Bruter, bruteforce vkontakte.ru, Брут Вконтакте.ru, Взлом анк](#)  
[Брутом, Вконтакте Брут 2009, Новый Брут Вконтакте, Рабочий Брут Вконтакте](#)




## [причины и решения маленькой скорости брута](#)

причины и решения маленькой скорости брута

 [erta](#)  [причины и решения маленькой скорости брута](#) [4 сохр.](#) 

## [Словари для Брута Вконтакте](#)

Словари для Брута Вконтакте

 [Sloyka](#)  [bruteforce vkontakte, password list for brute vkontakte.ru, Брут Вк](#)  
[Вконтакте, Вконтакте, Словари для Брута Вконтакте, взлом vkontakte.ru](#) 




## [Брут дедиков](#)

Инструкция о том, как без проблем сбрутить дедик для себя

 [Heromant2008](#)  [брут дедиков, брут дедов, дедики](#) 

# Need for Automation

- Massive amounts of content
  - Over 10 top level domains

Раздел	Последнее сообщение	Темы	Сообщения
 <b><a href="#">FTP, Трафф, Загрузки</a></b> В разделе покупается/продается/меняется все что связано с FTP, траффом, загрузками.	<b><a href="#">Продаю полностью...</a></b> от <a href="#">hulern</a> Сегодня 05:30 >>	424	1,169
 <b><a href="#">DDoS, Spam, Flood</a></b> (просматривают: 1) В разделе предлагается/ищется все что связано с DDOS'ом, Спамом, Флудом (спам базы, софт и т.д.)	<b><a href="#">База емэйлов.100\$ за одну базу</a></b> от <a href="#">Jaroslav</a> Сегодня 02:58 >>	221	623
 <b><a href="#">ICQ - купля/продажа/услуги</a></b> Купля, продажа, обмен номеров ICQ. А так же софта (бруты, спамеры, флудеры и т.д.)	<b><a href="#">Огромный выбор ICQ номеров!</a></b> от <a href="#">GiZZZ</a> 05.10.2009 19:31 >>	424	1,217

Multiple sub forums

# Manually

- Natural language
  - Too complicated for automated processing
  - Misspellings, multiple spellings
- Unformatted postings

# Amusing Discoveries

# Personalities



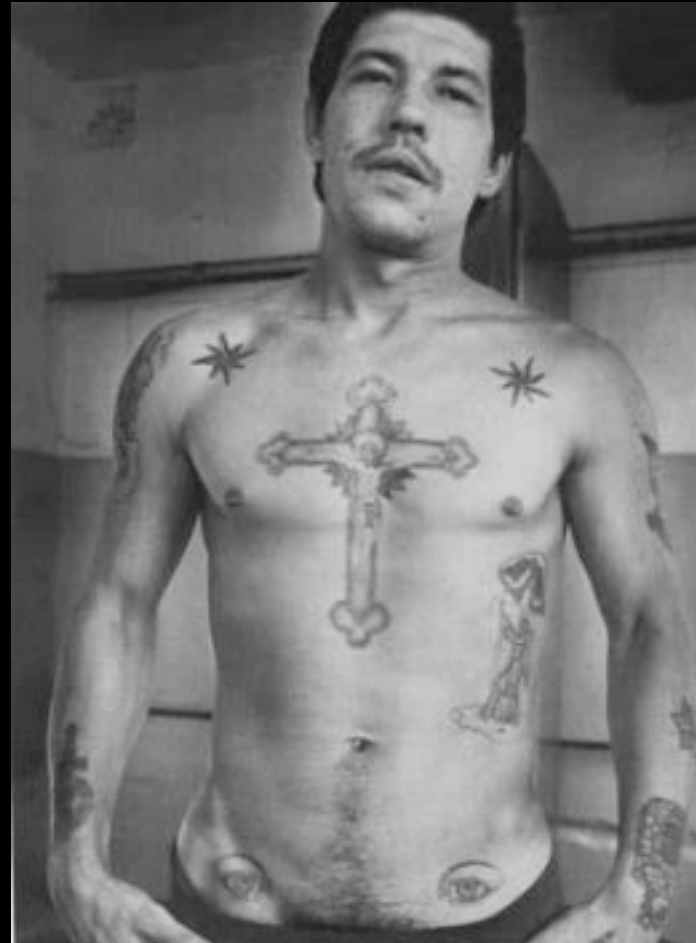
Thursday, July 1, 2010



# Geeks, not Gangsters

# Gangsters







Thursday, July 1, 2010

# Extremely Nonprofessional Criminals

# Geeks



Lingo

# What does this say?

**Re: Racing Money СОФТ 32\$ с продажи**

---

Работаем давно, знаем рынок и все потребности ;)

адекватные трафогоны и люди с лоадами - всегда велком.

Кстати минималок не надо набирать для пэймента, даже с 1 продой всё домой приедет по запросу ;)

---

**Интересует адалт/биз траф.**

**PM ONLY!!!**



# Can Google help?

**Sanche-ZZ**

Users



Registration: 03.06.2007

Address: Siberia

Posts: 179

Thanks: 18

Thanked 23 Times in 19 Posts

**Re: Racing Money SOFT 32 \$ from the sale**

We work long, know the market and the needs of all;)

adequate trafogony and people with loadami - always Wellcome.

Way minimalok inappropriately recruit for peymenta, even with 1 Sell all come home on request;)

---

**Interested in adult / biz cores.**

**PM ONLY!!!**

Good luck with that.

# Just FYI

**Re: Racing Money СОФТ 32\$ с продажи**

---

Работаем давно, знаем рынок и все потребности ;)

адекватные трафогоны и люди с лоадами - всегда велком.

Кстати минималок ненадо набирать для пэймента, даже с 1 продай всё домой приедет по запросу ;)

---

**Интересует адалт/биз траф.  
ПМ ONLY!!!**

# Hacker Slang

- Fenya - Russian prison slang
- Anglonims - English loan words
- Rhyming slang - Sounds like the English word
- Direct translation

# Scams & Schemes

# Wheres money?

- Extortion
- Job recruitment (Partnerkas, Drops, SMS regs, ..)
- Services
- Goods

# Extortion

- Malware that demands payment
- Fake windows “warning”

# Extortion

## ОС Windows заблокирована!

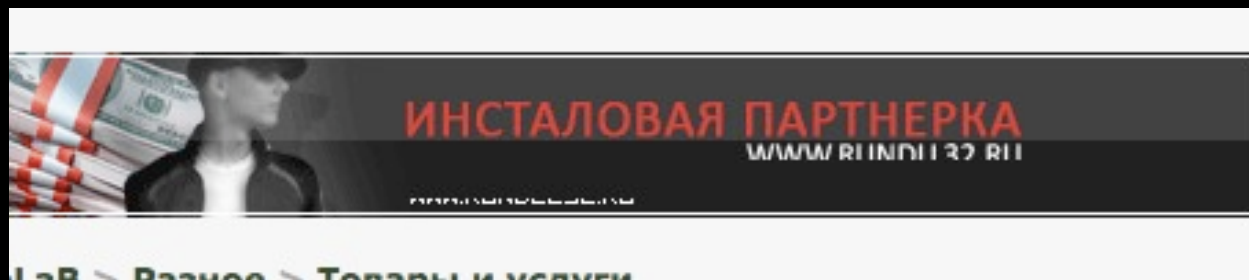
Вы используете нелицензионное программное обеспечение!

Для того, чтобы продолжить использование ОС Windows, Вам необходимо получить лицензию.  
Теперь это сделать очень просто, достаточно следовать следующим инструкциям:

1. Вам необходимо отправить SMS-сообщение
2. В ответ Вы получите сообщение с кодом активации
3. Введите полученный код, для активации ОС Windows



# Partnerka



# Partnerka

- Credit card payment gateways
  - Visa / Mastercard regulation compliant
  - PCI compliant
- Partnerships with webmasters and other scum
  - Percentage payouts for purchases



Вы вошли как rstwm | Выход  
Время на сервере: 09/06/08 09:25:49 Обновлено: 09/06/08

## СТАТИСТИКА

Пользовательская статистика обновляется в режиме реального времени, что позволит Вам постоянно отслеживать уровень продаж и контролировать Вашу финансовую жизнь в Bakas.  
Периодичность обновления - 10 минут.

### Ежедневная статистика:

August 23 2008 - August 28 2008  
 Продукт: Все продукты  
 Детальный вид: Нет  
 Сабаккаунты подробно: Нет

Получить

### Показана сводная статистика:

С 2008-08-23 по 2008-08-28, Продукт: Все продукты

Страна	Сабаккаунт	Дата	Продукт	Unq	Raw	Loader	Сетапы	Покупки	Сумма, USD		
									Покупки	Возвраты	Рефералы
Все	Все	2008-08-28	Все продукты	508	508	7	8	198	6909.13	-886.34	0.00
Все	Все	2008-08-27	Все продукты	1023	1023	8	6	848	31686.52	-4068.87	0.00
Все	Все	2008-08-26	Все продукты	1019	1020	8	8	795	28659.07	-2970.27	0.00
Все	Все	2008-08-25	Все продукты	1061	1061	10	7	243	8640.59	-105.13	0.00
Все	Все	2008-08-24	Все продукты	1072	1073	6	5	82	2898.02	-373.11	0.00
Все	Все	2008-08-23	Все продукты	772	775	9	7	71	2515.28	-511.60	0.00
Итого				5455	5460	48	41	2237	81388.61	-8915.32	0.00

# Partnerka Payouts

Ид	Логин	Баланс	Хеш пароля
4048	dp32	58160.20	417f5a94d12926ccb633bcd11c688f58
3886	iamthevip	61552.63	fe38da46c717da5e5b9d4f60d48cd914
5050	dp322	75631.26	417f5a94d12926ccb633bcd11c688f58
3750	cosma2k	78824.88	c60617b3bc972fc0f99ba895079b90ea
3684	ultra	82174.54	3fc0a7acf087f549ac2b266baf94b8b1
5016	slyers	85220.22	8517f97998c888e9ad08af4437ale8c2
4748	newforis	93260.64	0a6b521c6fc01eb7c98b29dee9c98efd
2	rstwm	95021.16	698d51a19d8a121ce581499d7b701668
56	krab	105955.76	1c34c2260ef82bbbe4e64d97f1087f59
4928	nenastniy	158568.86	286ec30a4ef7ec649ecddd04bfcc5c7a

# SMS scams :)

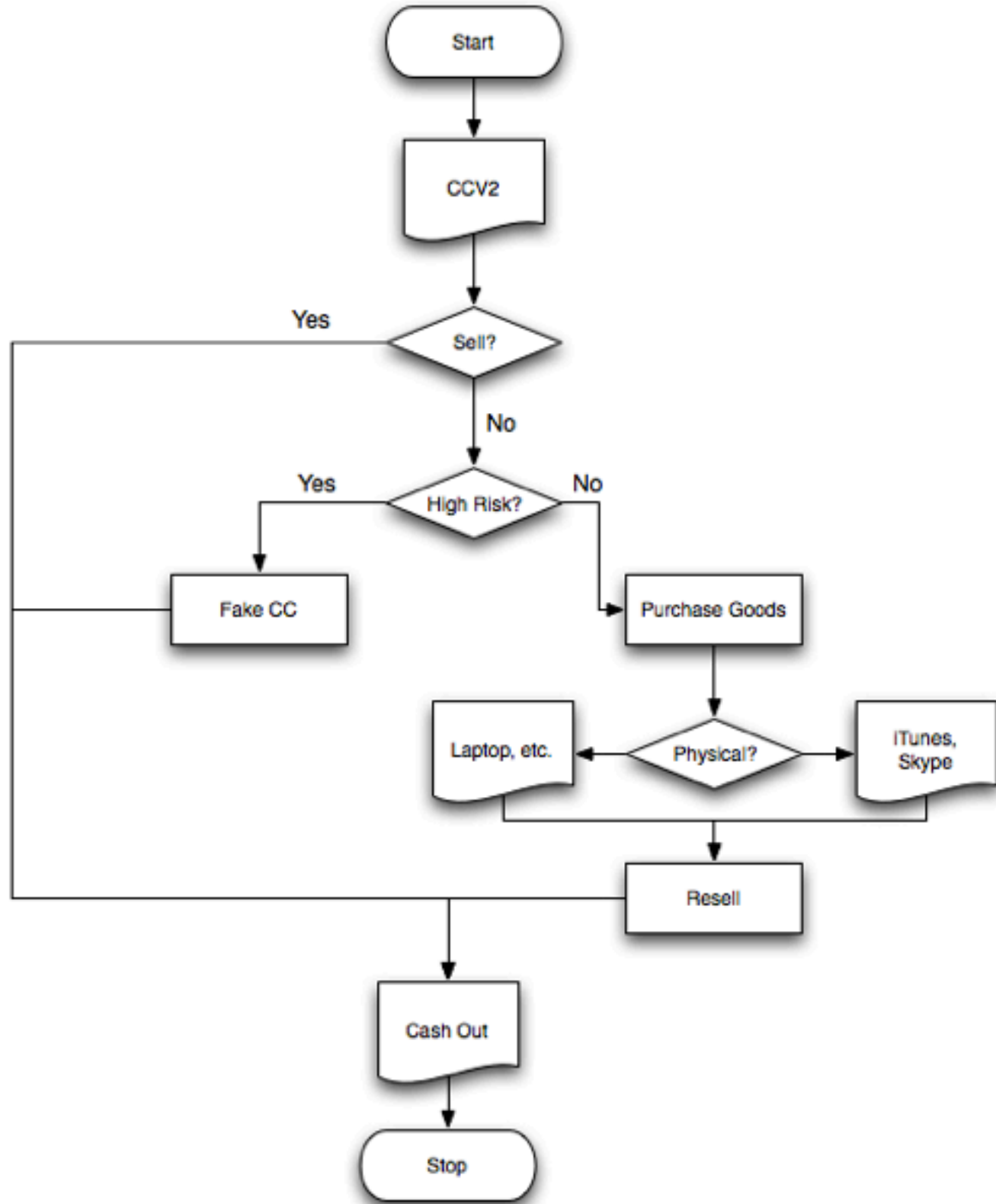
## Код

```
program SMS_Trojan;  
begin  
drawText('Hello world!', 0, 0);  
repaint;  
delay(2000);
```


## Код

```
begin  
if not SmsStartSend('sms://+5550000', 'Hello!') then Halt;  
while SmsIsSending do // wait for the message to be sent  
Delay(100);  
if not SmsWasSuccessfull then Halt;
```

# Cash Out



# “Дроп”

**Вouba** 

12.02.2010, 20:03



Ньюбби



Jest nerazvodnije dropi pocti pod liuboj staff v LT,NL,IRL.  
Rabotajem 50/50

S predlozen



moderator



группа: Пользователь  
сообщений: 1 080  
регистрация: 04.03.2009  
пользователь №: 18 746  
деятельность: [seo](#)

USA NY Brooklyn 11235 Dmitry Pechenskiy  
USA NY Ozone Park 11417 Alli Allen  
USA CA La Mesa 91942 Andrey Melnikov  
USA AZ Phoenix 85016 Anthony Zajicek  
USA NY Brooklyn 11235 Dmitry Pechenskiy  
USA AZ Youngtown 85363 IVIS O. DUARTE  
USA NY Longislandsity 11106 Johanna Gorlov  
USA CA West Hills 91304 Emilia Flore  
USA CA San Diego 92122 Megan Simmons  
USA NY Bronx 10460 Thierno Habib



-> STORE -> DROP (share) ->





# Virtual Currencies

- Online payment systems for service transactions
- Web Money
- Yandex Money
- eGold [dead]

# Conversion Gateway

**ОБМЕН ЭЛЕКТРОННЫХ ВАЛЮТ**

**EXchange Webmoney and Paypal**

**EXWP.COM**

# Web Money offices

<a href="#">Webmoney Gate Czech</a>	Прага	Чехия
<a href="#">Webmoney в Брянске</a>	Брянск	Россия
<a href="#">WebMoney Club</a>	Орел	Россия
<a href="#">WmPerm.RU</a>	Пермь	Россия
<a href="#">wmTrader.BIZ</a>	ОМСК	Россия
<a href="#">WMCashing</a>	Санкт-Петербург	Россия
<a href="#">WebMoney центр в Великобритании</a>	Нортхэмптон	Великобритания
<a href="#">oWMT.ru - Генеральный дилер Webmoney Transfer</a>	ОМСК	Россия
<a href="#">Webmoney.kg</a>	Бишкек	Кыргызстан
<a href="#">WMT-Tula, сервис WebMoney в г. Тула</a>	Тула	Россия
<a href="#">Moscow Transfer</a>	Москва	Россия
<a href="#">WMZ.lv</a>	Рига	Латвия
<a href="#">Webmoney Israel</a>	Хадера	Израиль
<a href="#">WebMoney Exchange Point, Pattaya, Thailand</a>	Патайя	Тайланд
<a href="#">Финансовый центр erMoney.com</a>	Берлин	Германия
<a href="#">Ростовский обменный пункт Webmoney</a>	Ростов-на-Дону	Россия
<a href="#">Webmoney24</a>	Санкт-Петербург	Россия
<a href="#">Обменный пункт Webmoney в Екатеринбурге</a>	Екатеринбург	Россия
<a href="#">E-money - электронные деньги в Кыргызстане</a>	Бишкек	Кыргызстан

# Goods

# Skype

Продам:

- аккаунты телефонии Skype с 10\$ на счету. 5\$
- номер(почти в любой стране), для принятия в

сделаю на заказ ◀ SKYPE ▶ аккаунты  
10 баксов --- 4 вМЗ  
стучите 265876 возможен и другой лимит

С акков можно звонить на любой телефон мира, как на сотовый, так и домашний.

Могу предоставить отзывы о моем сервисе.

**Продам готовые Skype аккаунты. В наличии и под заказ.**

lсq: :

## **Skype OUT:**

Коэффициент 1 к 2.5 (За Ваш Один доллар, на счёте Два с Половиной)

## **Skype IN**

Любые ареа коды. 9\$ за год.

## **Звонки без ограничений(Включая Всю Россию)\* - 25\$**

Подробности в lсq

Регистрирую для Вас лично, никто этими акками раньше не пользовался.

Для себя занимаюсь этим не один год, лок встречается крайне редко.

Консультирую бесплатно.

Оплата:

Для людей с хорошей репой на крупных хак форумах(нужно подтверждение), передаю имя\пароль первым.

Остальные, либо гарант, либо предоплата.

# iTunes cards



一手**itunes code us 100美金=12元** 详情咨询店掌柜

一口价  
**12.00**

卖家: dahaidada1  和我联系



**itunes account 50 100 200 500 1000美金**(详情请咨询)

一口价  
**1.00**

卖家: wzz60257  和我联系



三钻老店 **APPLE ID iTunes Store** 【美国】账号  
保证最低**\$150**消费

一口价  
**15.00**

 卖家: liuyi\_1985  和我联系

# Loaders, ExploitKits, ...

## Характеристики:

Пробив на iframe-mix трафике: 15-20%

Пробив на обычном US трафике: 10-20%

Пробив на хорошем US трафике: от 15%

Пробив на среднем ES: от 8%

Пробив на биржевом трафике(gudclicks.com:весь трафик): 11-12%

Пробив на микс-трафике(преимущественный US), шедшем в несколько рук: 9-10%

Пробив на хреновом трафике с worldtraff(Full mix): 3-6%

Отстук на лодере 2k8 Loader: 80%. На вашем софте отстук может быть как больше, так и меньше.

На борту более 15 эксплоитов:

Util.printf, Collab.collectEmailInfo, Collab.getIcon, MS09-002, DirectShow(MPEG2), MDAC, Adodb, XML Parsing, Sp  
TN3270, compareTo, JNObject

+Other: включает в себя несколько эксплоитов.

И в ближайшее время кол-во будет увеличено.

Связка поддерживает модули и плагины.

Изначально для вас доступно несколько интегрированных модулей и плагинов, в будущем будут писаться отдельные  
пользователи смогут устанавливать себе по желанию.

Есть возможность банить: IP зашедшего; Зашедшего по Cookies; IP пробитого; Пробитого по Cookies;

Связка пробивает как XP, так и Vista, ну и естественно пробивает другие Win-системы.

Эксплоиты работают достаточно тихо, браузеры не "лопаются".





Все эксплоиты генерируются и криптируются "на лету" в вашем распоряжении 3 алгоритма шифрования основной в  
использовать.

Если один спалился, вы переключаетесь на другой, таким образом связка всегда остается чистой и вы не теряете

Отдельное шифрование PDF-выдачи.

Отдельное шифрование подгрузки PDF-файла.

# Passports

Испания		Дополнительно с паспортом можно заказать испанские права – 700\$	13300 евро
Италия		Дополнительно с паспортом можно заказать итальянские права – 700\$	14470 евро
Китай		Оформление паспортов и гражданства, права не делаем.	7650 евро
Латвия		Оформление паспортов и гражданства, права не делаем.	11700 евро



# CCs

	AmEx Corporate	Канада
	AmEx	Канада
	Visa, exp. date текущего месяца	Все страны
	MasterCard, exp. date текущего месяца	Все страны
	Visa Classic	Латинская Америка
	MasterCard	Латинская Америка
	Visa Classic	Океания

# Equipment

**Модель MSR206-3HL для считывания и записи карт с магнитной полосой**



Модель MSR206-3HL была специально разработана для  
low-

[websites go here]

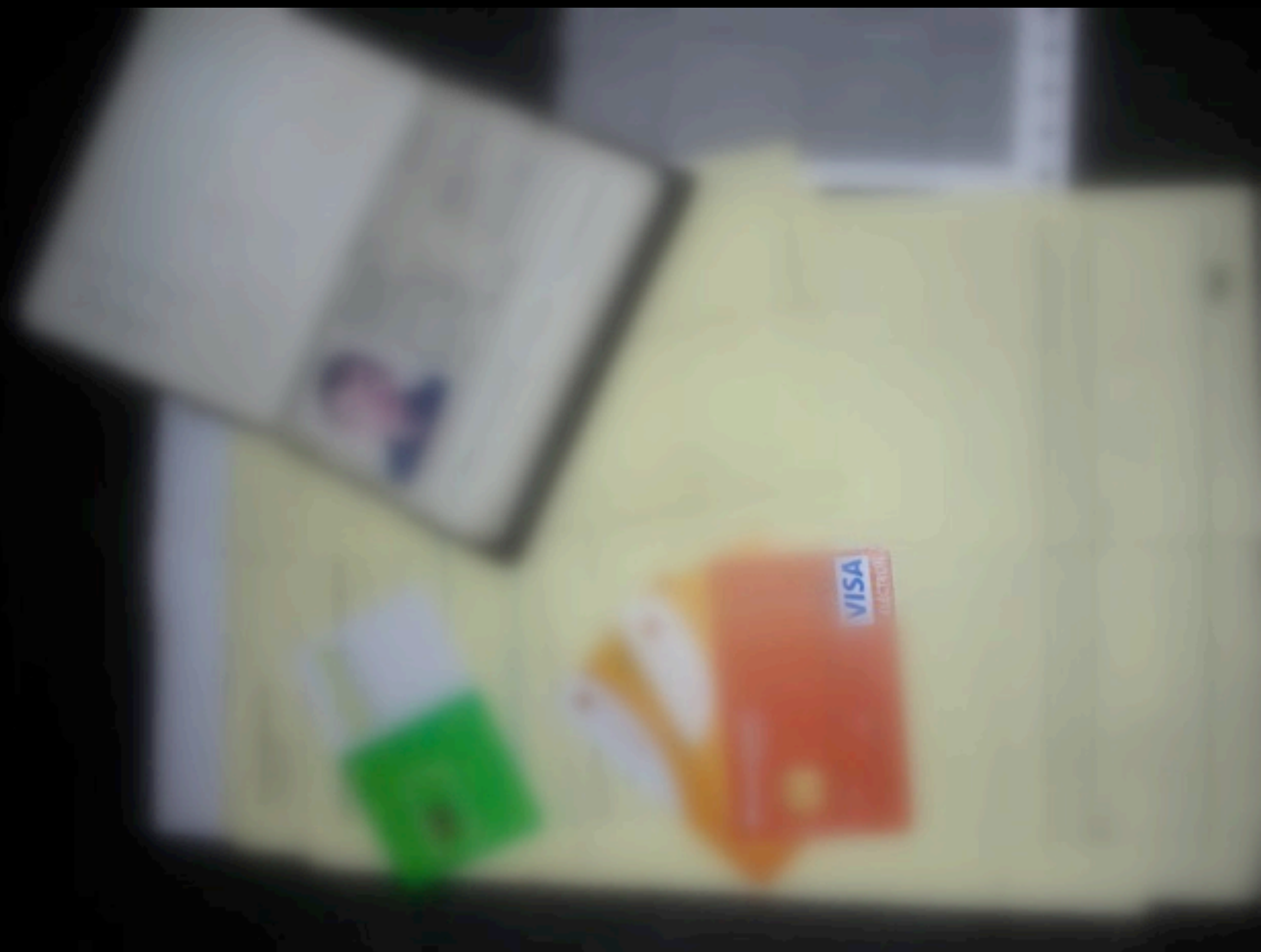
# Identity Services

# Complete Package

Под средства любой загрязненности!

В комплект входит:

- 1.Банковский акк(online доступ)
- 2.АТМ карта(Дневной лимит на снятие средств 1000\$/6000\$ В МЕСЯЦ-Возможно увеличение лимита +30\$-)
- 3.Карта кодов (для online доступа)
- 4.Копия паспорта дропа
- 5.Sim-ka



How long does it take  
to find a usable CC?

# 5 seconds

Яндекс

Найти



# first link...

1:50:Wesley Maxwell::756 Post Drive::Whiteman AFB:Missouri:65305:United States:Wesley Maxwell:5471691100  
2:34:Andrew Martin::840 21st Ave North::south saint paul:Minnesota:55075-1314:United States:Andrew Martin:40  
0:56:Eric Wentorf::3510 Haven Ave::Racine:Wisconsin:53405:United States:Eric Wentorf:4356874055603252:030  
8:19:Luz Owens::521 Southbridge Creek Drive::Jacksonville:Florida:32259:United States:Luz Owens:5490993293  
6:59:Luz Owens::521 Southbridge Creek Drive::Jacksonville:Florida:32259:United States:Luz Owens:5490993293  
0:31:Allan Gonzalez Muniz::420 Declaration Ave::Billings:Montana:59105:United States:Allan Gonzalez Muniz:44  
3:46:Jamie Kozak::w3804 Hemlock Drive:54555:Phillips:Wisconsin:54555:United States:Jamie Kozak:601100611  
2:55:Leslie Oster , III::2604 N. E. 1st Ave.::Ocala:Florida:34470:United States:Leslie Oster , III:511122000201678  
2:34:Ronald Gieseke:Arachnid, Inc.:6212 Material Ave.::Love's Park:Illinois:61132:United States:Ronald Gieseke:  
0:57:Travis Jones::250 Meadow Lane::Secaucus:New Jersey:07094:United States:Travis Jones:4482150141619  
5:50:Allan Papworth::3570 Corey Rd::Malabar:Florida:32950:United States:Allan Papworth:5466160047269145:0  
2:48:Grigoriy Ter-Oganov:E.T.G.:100 Morain st. #302::Kennewick:Washington:99336:United States:Grigoriy

# and washing service..

## Помойка для грязи

[Оригинальный топик на форуме](#)

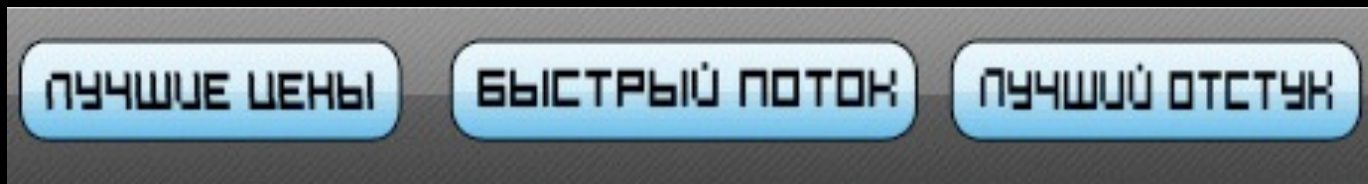
Автор: *Hunter410*

Приму корп грязь ..... условия, цены, и доп инфо в - 576ноль ноль7403

Куплю грязый, серый ЯД. Пока до 120 т.р... беру 40%. т.е. за 100 грязи, получите 60 чистыми.

Оплата: Альфой, Телебанком, либо чистым ЯД-ом

# Traffic Generation




- Best Prices
- Fast Stream
- Best “Conversion”/Infection Ratio

# Infection: rates and nums

Всего трафика: 1762  
Всего загрузок: 333  
Процент пробива: 18.9%  
# Микс айфрейм, преобладающие TR и US, качество и происхождение трафа мне не в  
Всего трафика: 9408  
Всего загрузок: 1688  
Процент пробива: 17.94%  
# Микс айфрейм, преобладающие TR, BR, DE, RU, трафик среднего качества + очень  
Всего трафика: 871  
Всего загрузок: 135  
Процент пробива: 15.5%  
# Микс айфрейм, страны СНГ, сам по себе трафик среднего качества, на сколько свя  
Всего трафика: 2588  
Всего загрузок: 484  
Процент пробива: 18.7%  
# Микс айфрейм, преобладающие US, RU, качество трафа норм ... #  
Всего трафика: 2087  
Всего загрузок: 441  
Процент пробива: 21.13%  
# Микс айфрейм, практически весь трафик US и TR, качество трафика норм ... #  
Всего трафика: 2341  
Всего загрузок: 758  
Процент пробива: 32.37%  
# United States, чистый, сео. #  
Всего трафика: 4352  
Всего загрузок: 615  
Процент пробива: 14.13%  
# айфрейм трафик с 95% BR. #  
Всего трафика: 3350  
Всего загрузок: 654  
Процент пробива: 19.52%

how much to take down  
twitter?

 **DDoS Service 911**

**DDoS Service 911**

Наш DDoS сервис - лучшее средство от надоедливых конкурентов, которые мешают Вам работать. Главное отличие нашего сервиса - мы **работаем независимо от тематики атакуемого сайта!**

Срочная помощь в решении Ваших проблем - **в сети практически круглосуточно!**

Наши цены самые доступные на рынке ддоса. Средняя цена составляет 80\$ в сутки. Конечная цена может колебаться как в большую, так и в меньшую сторону. Оптовым заказчикам индивидуальные условия!

Способы оплаты:

**Avg. US\$80 per diem**

# Question

why was twitter down?



cuxumu

# Technology: Tools of Trade

Overview & demos

# Intelligence Gathering

- Automated and manual analysis of publicly available data

# Tools of trade

- Mostly open-source. With custom extensions

# Tools: Nutch

- Content Fetcher; extended with custom Indexers
- Changes to Spider behavior (“proper” robots.txt handling etc)
- Custom “Seeders”
- Distributed Indexing (w/ hadoop)

# Tools: RSS feeds “eater”

- A bunch of python scripts thrown together to fetch rss feeds

# Google App Engine

- Public Interface with transforms, dictionaries and other misc. Stuff.

# Tools: SOLR

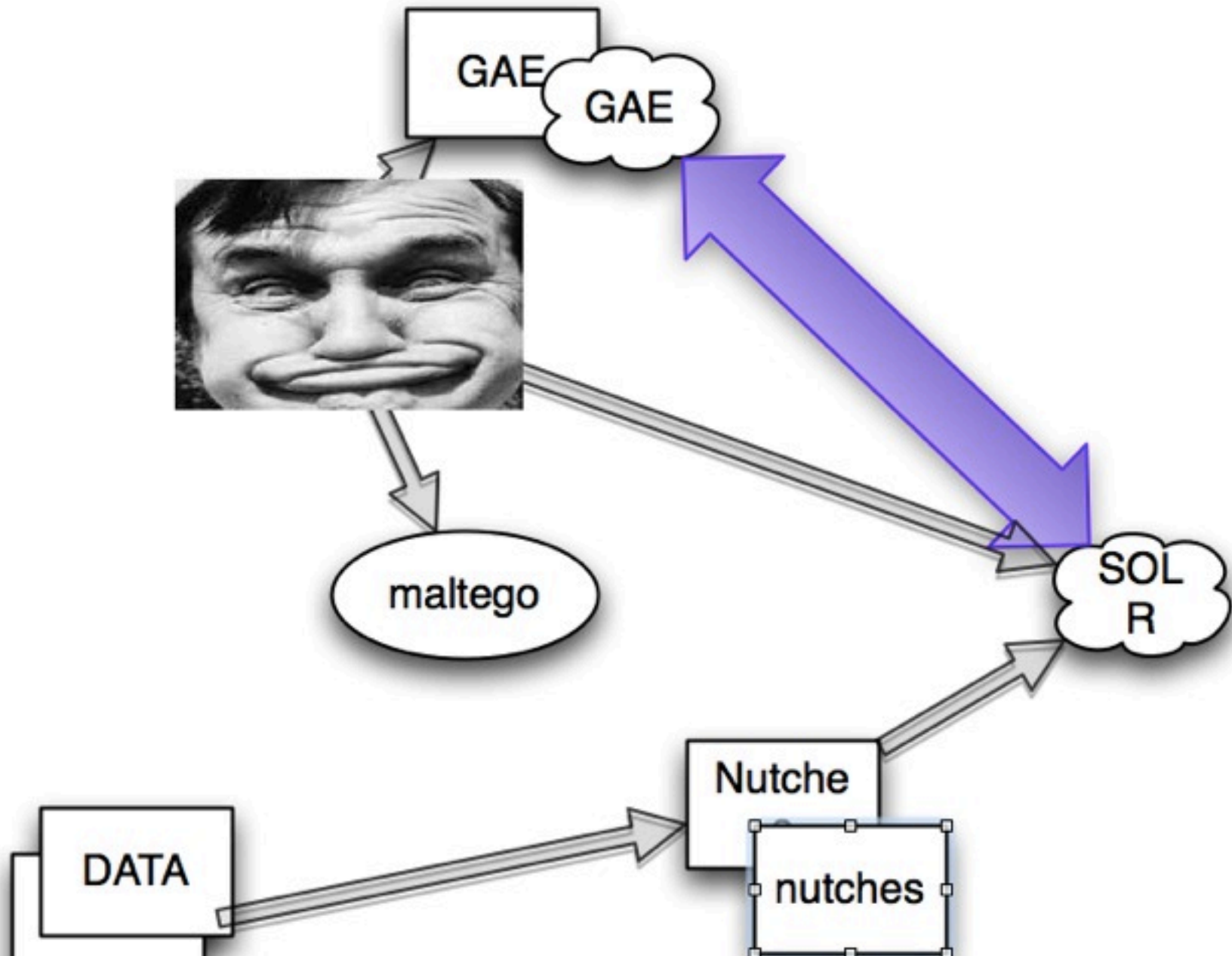
- Customized Data indexing and search
- Custom schema and search fields
- JSON output used
- Language “projection” (lingo/slang support)



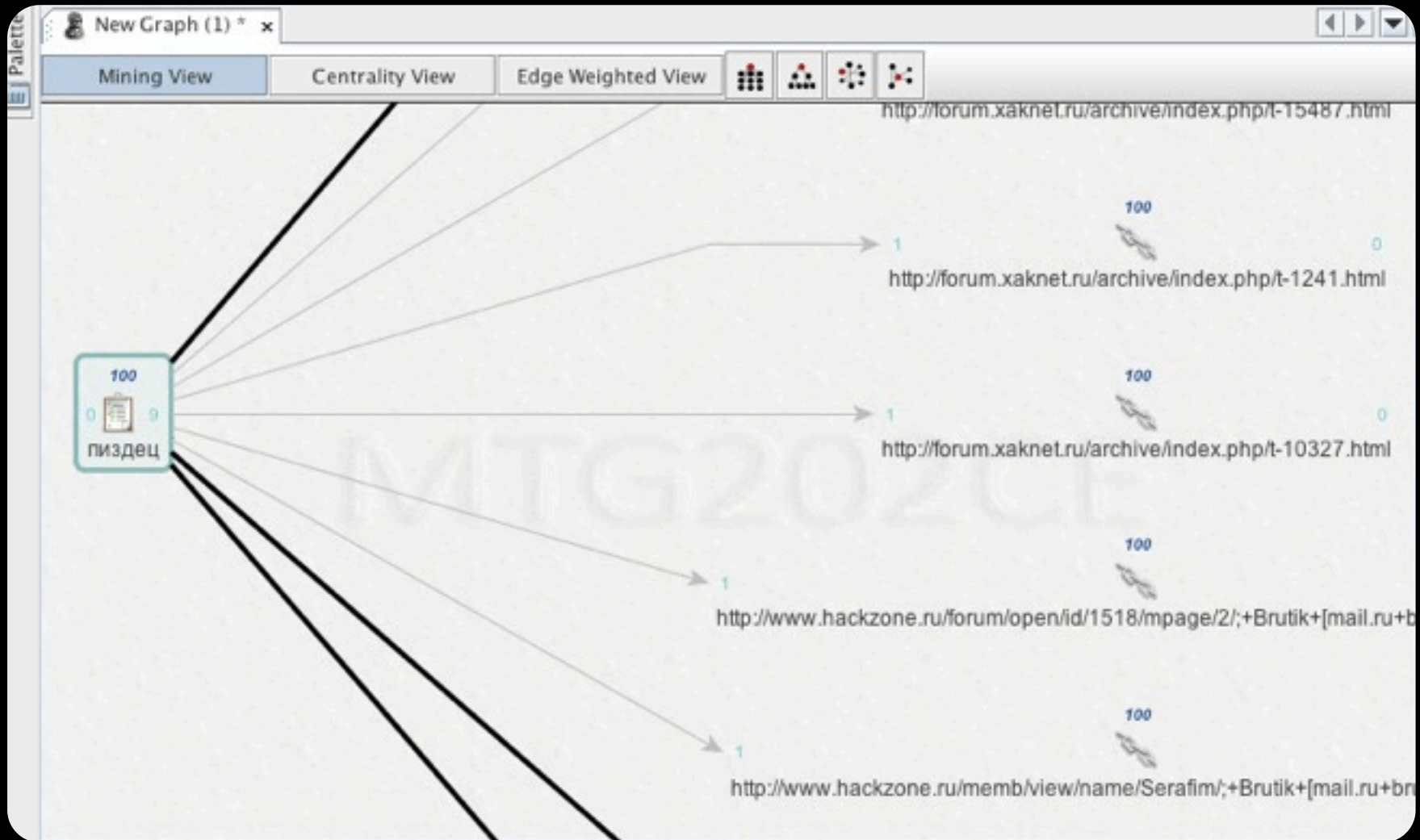
# Tools: Web UI/Maltego

- Web UI: easier
- Visualization: Maltego Custom Transforms

# Overall picturesque



# Maltego



Lets look at some

%^@%#

# Future Plans

# Future Integration

- Maltego and other viz. tools
- Online Engine Availability
- Scale more, dig more ;-)
- Feed “eaters” (BBSes hear me?;))
- MultiLang: Spanish/Italian/Portuguese

# Availability

- <http://www.o0o.nu/projects/intelligence-collection> - tools, slides, howto's etc
- <http://383rat.appspot.com> - transforms on GAE, indexes, dictionaries etc

# Feedback And Questions

(fygrave@o0o.nu

or

grugq@research.coseinc.com)