

# From Russia with love.exe

Underground Hacking Forums from Former East Bloc

# Outline

- Digging in a pile of trash
- Lingo
- Monetization
- Surprises
- Conclusions

# 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

# Intelligence Gathering



- Automated and manual analysis of publically available data

Digging in a pile of trash

# Forums


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

Брут для Вконтакте py, bruteforce вконтакте

 [Sloyka](#)  [Vk Bruter, bruteforce vkontakte.ru , Брут Вконтакте.py , 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><u>FTP, Трафф, Загрузки</u></b> В разделе покупается/продается/меняется все что связано с FTP, траффом, загрузками.	<b><u>Продаю полностью...</u></b> от <a href="#">hulern</a> Сегодня 05:30 >>	424	1,169
 <b><u>DDoS, Spam, Flood</u></b> (просматривают: 1) В разделе предлагается/ищется все что связано с DDOS'ом, Спамом, Флудом (спам базы, софт и т.д.)	<b><u>База емэйлов.100\$ за одну базу</u></b> от <a href="#">Jaroslav</a> Сегодня 02:58 >>	221	623
 <b><u>ICQ - купля/продажа/услуги</u></b> Купля, продажа, обмен номеров ICQ. А так же софта (бруты, спамеры, флудеры и т.д.)	<b><u>Огромный выбор ICQ номеров!</u></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



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

---

**Интересует адалт/биз траф.**

**ПМ 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 не надо 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 the money?

- Extortion
- Partnerka
- Services
- Goods



# Extortion

- Malware that demands payment
- Fake windows “warning”

# Extortion

## ОС Windows заблокирована!

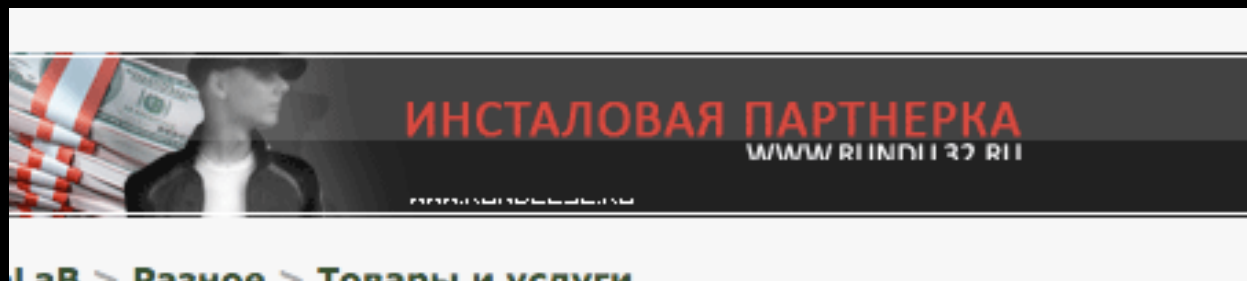
Вы используете нелегальное программное обеспечение!

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



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.

Сабакжаунты подробно:

Получить

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



# 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	8517f97998c888e9ad08af4437a1e8c2
4748	newforis	93260.64	0a6b521c6fc01eb7c98b29dee9c98efd
2	rstwm	95021.16	698d51a19d8a121ce581499d7b701668
56	krab	105955.76	1c34c2260ef82bbbe4e64d97f1087f59
4928	nenastniy	158568.86	286ec30a4ef7ec649ecddd04bfcc5c7a

# Virtual Currencies

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

# Conversion Gateway

**ОБМЕН ЭЛЕКТРОННЫХ ВАЛЮТ**

**EX**change **W**ebmoney and **P**aypal

**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

[websites go here]

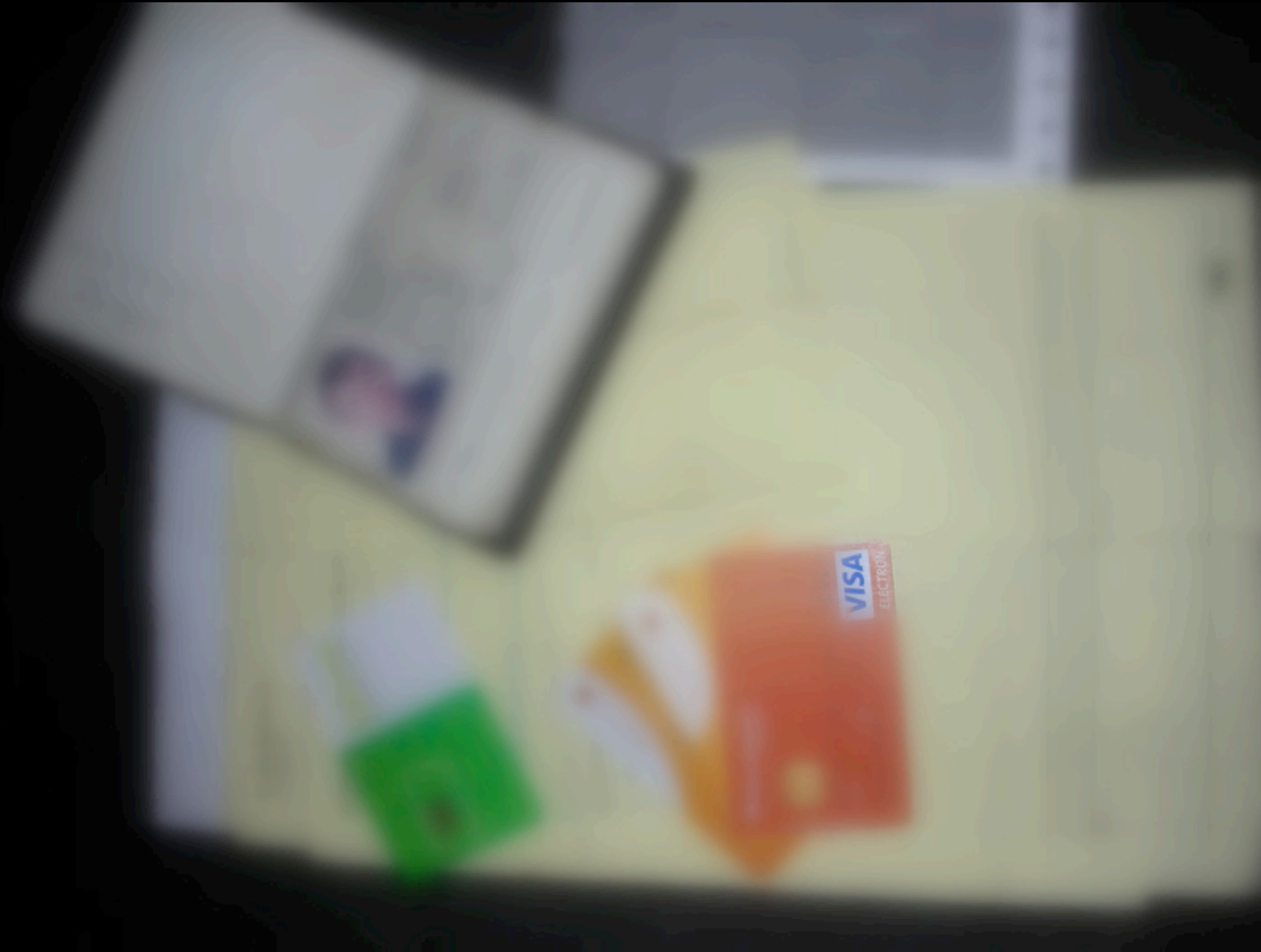
# Identity Services

# 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 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:44821501416190  
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](#)

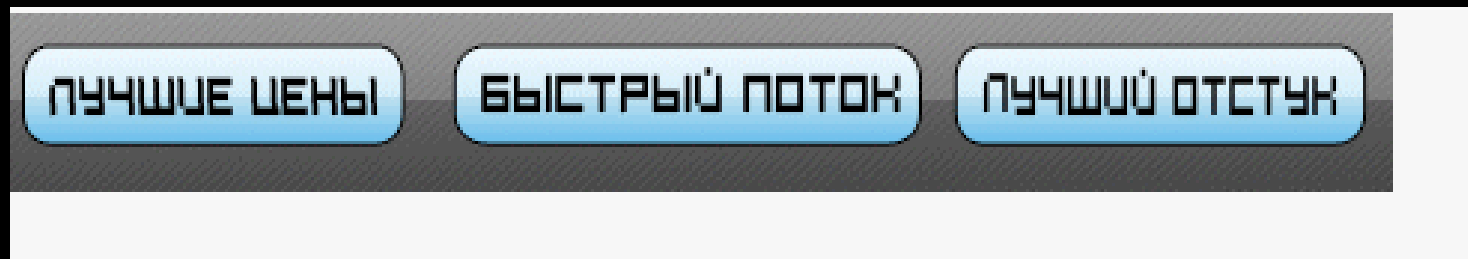
Автор: *Hunter410*

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 Infection Ratio

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

Surprises



why was twitter down?

cuxumu



# Conclusions

# Conclusion

- Geeks not Gangsters
- Hacker culture is youth culture
- Profit driven