Lecture Outline

• Announcements:
  – Exit survey
  – Exemplars

• Cybercrime
  – Spammer $$
  – The *Underground Economy*
  – The power of *infiltration*
  – *Beyond Technical Security*
How Much $$ Do Spammers Make?
Spam conversion experiment

Instrumented ~1.5% of Storm’s total output (2008)

<table>
<thead>
<tr>
<th></th>
<th>Pharmacy Campaign</th>
<th>E-card Campaigns</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Postcard</td>
</tr>
<tr>
<td>Worker bots</td>
<td>31,348</td>
<td>17,639</td>
</tr>
<tr>
<td>Emails</td>
<td>347,590,389</td>
<td>83,665,479</td>
</tr>
<tr>
<td>Duration</td>
<td>19 days</td>
<td>7 days</td>
</tr>
</tbody>
</table>
Site needs to be up hours to days to reap real users rather than just crawlers.
The Spammer’s Bottom Line

- 28 purchases in 26 days, avg. “sale” ~$100
  - Total: $2,731.88, $140/day
- **But**: interposed on only ~1.5% of workers:
  - $9,500/day (**OR**: 8,500 new bots per day)
  - $3.5M/year (back of envelope - be very careful!)
    - Though if selling Viagra via *Glavmed affiliation*, cut is **40%**
- **Storm**: service provider or integrated operation?
  - Retail price of spam ~$80 per million
    - Pharmacy spam would have cost 10x the profit!
  - Strongly suggests Storm operates as an integrated operation rather than a reseller
The Underground Economy
ProAgent V2.0 Public Edition

Send Menu
- Send Passwords
- Send CD-Keys
- Send KeyLog
- Send System Information
- Send Address Book
- Send URL History
- Send Processes Log

Options
- Give a fake error message
- Melt server on install
- Disable AntiVirus Programs
- Clear Windows XP Restore Points
- Protection for removing Local Server

Server Icon
You can choose any icon for server
Choose Icon

Bind with File
- Bind with File
Select File To Bind

Notification
Your e-mail address which you will to receive information from ProAgent.
E-Mail: bomberman@yahoo.com
Test

Decryptor
Remove Server
About
Buy Undetectable
Help
Create Server

ProAgent - Professional Agent Copyright © 2005 SIS-Team

Recycle Bin
ProAgent Spy Software is one of the most powerful monitoring and surveillance applications available today.

It is an ultimate solution for monitoring spouses, children, employees, or anyone else!

ProAgent records all typed keystrokes, all active window texts, all visited web sites, usernames, passwords and more and sends e-mail reports to your e-mail address that you specified when creating the server, completely hidden!

ProAgent can work in all kind of networks, it doesn’t matter if the PC is behind a firewall or behind a router or in a LAN, ProAgent works in all of these conditions without any problems.

Click here to purchase ProAgent v2.1 Special Edition...

Click here to download ProAgent v2.1 Public Edition...
allBots Inc.

Social Networking Bots

GOOD News!!! We have something more for you! Yes, we have just integrated CAPTCHA Bypassers in all of our bots.

Winsock (Multi-threaded) Bots
Click here for 30+ MySpace Bots

Become an Affiliate and Start Earning Now

---

**Accounts Creator**
(You Just Need To Type In The CAPTCHA As To Create Accounts)

<table>
<thead>
<tr>
<th>Social Networks</th>
<th>Price Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySpace Accounts Creator</td>
<td>$180.95 - $140.00</td>
</tr>
<tr>
<td>MySpace Accounts Creator (Winsock)</td>
<td>$360.95 - $320.00</td>
</tr>
<tr>
<td>YouTube Accounts Creator</td>
<td>$120.95 - $95.00</td>
</tr>
<tr>
<td>Friendster Accounts Creator</td>
<td>$120.95 - $95.00</td>
</tr>
<tr>
<td>Hi5 Accounts Creator</td>
<td>$120.95 - $95.00</td>
</tr>
<tr>
<td>TagWorld Accounts Creator</td>
<td>$120.95 - $95.00</td>
</tr>
</tbody>
</table>

---

**Friend Adders, Message Senders, Comment Posters & Others**
(All Bots Work In A Conventional Manner, They Gather Friend IDs/Names And Send Friend Requests, Messages, Comments Automatically)

**Chaining Feature** Is Available On All Bots for All Networks Except Facebook
Наш магазин аккаунтов рад предложить аккаунты различных почтовых служб и бесплатных хостингов для любых задач. Вы получите аккаунты СРАЗУ после оплаты заказа через Webmoney.

Также доступна услуга залива редиректов на Pochta.ru, Cwahi.net и 0catch.com что является уникальной услугой - вы получаете готовые редиректы в течение часа после заказа.

При покупке аккаунтов менее 1000 штук действует специальный тариф.

**www.FreedomScripts.org** - разработка софта на заказ
**Mega Софт для дорвеев - Zerber**
**Одобритель друзей - Мой мир**

**Twidium** - безопасный и профессиональный инструмент для раскрутки твиттера
накрутить фолловеров в Твиттер

Заработай на продаже аккаунтов

Купить аккаунты Одноклассников

Сейчас в продаже

<table>
<thead>
<tr>
<th>Служба</th>
<th>Кол-во акков</th>
<th>Цена за 1K аккаунтов</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail.ru</td>
<td>117025</td>
<td>до 10К: $5</td>
</tr>
<tr>
<td>Mail.ru Mix</td>
<td>327199</td>
<td>до 10К: $5</td>
</tr>
<tr>
<td>Mail.ru Second Hand</td>
<td>0</td>
<td>до 10К: $4</td>
</tr>
<tr>
<td>Mail.ru Mix S/H</td>
<td>15811</td>
<td>до 10К: $4</td>
</tr>
<tr>
<td>Yandex.ru</td>
<td>4758</td>
<td>до 10К: $20</td>
</tr>
<tr>
<td>Narod.ru</td>
<td>5315</td>
<td>до 10К: $50</td>
</tr>
</tbody>
</table>

Новости

**06 Апр 2013**
Временно не продаем аккаунты
Twitter.com

**15 Мар 2013**
Отличная цена на аккаунты
Facebook.com! Всего $80 за 1000 шт.
Дешевле не бывает!

**07 Фев 2013**
Сенсационная цена на аккаунты
Yahoo.com. Теперь отличные аккаунты со всеми регистрационными данными по цене от $7 за 1000 шт!

**06 Фев 2013**
Список доступных акков

Сервис по продаже аккаунтов аукциона eBay.

Добрые юзеры аукциона eBay предлагают вашему вниманию свои аккаунты.
Постоянным клиентам и тем, кто берет более 5 акков, различные бонусы и скидки.
Все аккаунты с доступом к мылу холдера.

Вы сами выбираете акк (несколько акков) из списка. Говорите мне. Оплачиваете и получаете.
Все акки предварительно проверяются перед продажей, в случае, если что-то не работает - 100% замена.

Актив/не актив смотрите сами по юзер ид. По активности не сортирую, так как это для каждого субъективно.

Также в продаже бывают акки PayPal. Цены рыночные. Постоянно не продаю.

Оплата по WM.
Перед покупкой следует обязательно ознакомиться с FAQ.
По работе с товаром не консультирую.
Работа через гарант сервис приветствуется.

Мои цены:
seller/баер акк до 10 фидов = 5$
seller/баер акк 10-25 фидов = 10$
seller/баер акк 25-50 фидов = 15$
seller/баер акк более 50 фидов = 25$
Welcome to PP24! Please use Width Fluid to view full details

You balance is empty, please deposit money to buy paypals

### SEARCH PAYPALS

<table>
<thead>
<tr>
<th>VERIFY (+$0.10)</th>
<th>TYPE (+$0.15)</th>
<th>COUNTRY (+$0.20)</th>
<th>MAIL (+$0.20)</th>
<th>BALANCE (+$0.20)</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Verify</td>
<td>All Type</td>
<td>All Country</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### AVAILABLE PAYPALS

<table>
<thead>
<tr>
<th>PAYPAL EMAIL</th>
<th>VERIFY</th>
<th>TYPE</th>
<th>CARD</th>
<th>BANK</th>
<th>MAIL</th>
<th>BALANCE</th>
<th>FIRST NAME</th>
<th>ADDRESS</th>
<th>COUNTRY</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>****<a href="mailto:alksmommy@yahoo.com">alksmommy@yahoo.com</a></td>
<td>Yes</td>
<td>Premier</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>$6.42</td>
<td>Joanna</td>
<td>Panama City</td>
<td>USA</td>
<td>$2.50</td>
</tr>
<tr>
<td>****<a href="mailto:eans123@yahoo.com">eans123@yahoo.com</a></td>
<td>Yes</td>
<td>Premier</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>$1.00</td>
<td>Regina</td>
<td>Clifton Park</td>
<td>USA</td>
<td>$2.50</td>
</tr>
<tr>
<td>****<a href="mailto:ibsack@gmail.com">ibsack@gmail.com</a></td>
<td>Yes</td>
<td>Premier</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>$121.07</td>
<td>Abigail</td>
<td>Jefferson</td>
<td>USA</td>
<td>$15.00</td>
</tr>
<tr>
<td>****<a href="mailto:ie@gambit.net">ie@gambit.net</a></td>
<td>Yes</td>
<td>Premier</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>$1,102.37</td>
<td>Gwynn</td>
<td>Tallmadge</td>
<td>USA</td>
<td>$45.00</td>
</tr>
<tr>
<td>****<a href="mailto:l.stevenson@gmail.com">l.stevenson@gmail.com</a></td>
<td>Yes</td>
<td>Premier</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>$209.03</td>
<td>Michal</td>
<td>Galloway</td>
<td>USA</td>
<td>$20.00</td>
</tr>
<tr>
<td>****<a href="mailto:ney_bruesch@yahoo.com">ney_bruesch@yahoo.com</a></td>
<td>Yes</td>
<td>Premier</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>$18.41</td>
<td>Courtney</td>
<td>Gurnee</td>
<td>USA</td>
<td>$4.00</td>
</tr>
</tbody>
</table>
Study programs:
“Axiom of Criminal Laziness”

Cybercrooks will work energetically to sustain their current cash flow ...

... but will not look out strategically beyond it to serve their long-term interests
Web Gang Operating in the Open

By RIVA RICHMOND
Published: January 16, 2012

Five men believed to be responsible for spreading a notorious computer worm on Facebook and other social networks — and pocketing several million dollars from online schemes — are hiding in plain sight in St. Petersburg, Russia, according to investigators at Facebook and several independent computer security researchers.

The men live comfortable lives in St. Petersburg — and have frolicked on luxury vacations in places like Monte Carlo, Bali and, earlier this month, Turkey, according to photographs posted on social network sites — even

Mr. Droemer said the gang’s success was more attributable to workaday persistence and willingness to adapt than technical sophistication. They could have spread Koobface to many more PCs, he said. “They could have done a lot more technical things to make it more perfect, more marvelous. But there was just no need to do it. They were just investing as much to get the revenue they wanted to get.”
Від 29 вересня до 2 жовтня ц.р. Служба безпеки України завершила свій етап міжнародної спецоперації з протидії кіберзлочинності.

Злочинна схема виглядала таким чином: злочинці здійснювали ураження шкідливим програмним забезпеченням комп’ютерів жертв, з якими здійснювалося управління розрахунковими рахунками, і викралили персональні коди доступу. Використовуючи отриману інформацію, злочинці незаконно перераховували викрадені гроші на рахунки українських банківських установ або переводили у готівку на території України з використанням міжнародних електронних платіжних систем.

За попередніми оцінками, завдані європейські збитки сягають понад 40 млн. доларів США.

Отримані кошти спрямовувались на розвиток протиправної діяльності ОЗГ, а також на придбання рухомого та нерухомого майна, автотранспорту, коштовних товарів і повсякденного попиту тощо.

Під час проведення спецоперації у фігурантів вилучено потужне комп’ютерне обладнання, яке служило знайомим злочинці, загальною вартістю близько 100 тис. доларів США, грошові кошти, коштовні речі та дороговість.

Вилучене обладнання скеровано на експертизу, після завершення якої буде порушено кримінальну справу.

Прес-центр СБ України
Security Service of Ukraine completed the next stage of international special operations to combat cybercrime

From September 29 to October 2, Security Service of Ukraine completed its phase of international sting operation that was carried out in cooperation with law enforcement agencies in the U.S., the UK and the Netherlands. As a result of coordinated interaction stopped the illegal activities of the Ukrainian branch of the international criminal gang that carried out the large-scale computer crime aimed at kidnapping of foreign banks funds on a large scale with subsequent legalization.

The activities of this group are involved about 20 people - inhabitants of different regions of Ukraine, five of whom were detained employees of Security Service of Ukraine.

Criminal scheme looked like this: criminals committed defeat malware victim's computer, of which manages a checking account and steal personal access codes. Using this information, the criminals kidnapped illegally transferred money to accounts of Ukrainian banks in cash or transferred in Ukraine using international payment systems.

It is estimated that caused damage thus reaching more than 40 million.

The funds were directed to the development of illegal activities OCG, as well as the acquisition of movable and immovable property, vehicles, valuable consumer goods and more.

During the special operation in the defendants removed the powerful hardware, which served as an instrument of crime, worth about 100 thousand dollars, cash, valuables and jewelry.

Remote equipment taken to the examination, after which will be prosecuted.

Press SAT Ukraine

2010: Ukrainian Secret Service documents a “bust”
Службою безпеки України у координації з правоохоронними органами США, Великої Британії, Нідерландів, Франції, Німеччини, Кіпру та Латвії (усього – 10 країн) припинено протиправну діяльність міжнародного злочинного угруповання хакерів, організованого та координованого громадянами України під прикриттям легально діючої комерційної структури, які шляхом використання спеціалізованого комп’ютерного віруса “Confiscer” отримували доступ до рахунків в іноземних банківських установах різних країн світу, незаконно знижуючи з них кошти та переводили їх у готівку з використанням банківських рахунків та міжнародних платіжних систем.

Отримані у такий спосіб кошти легалізувалися шляхом придбання рухомого та нерухомого майна. За попередніми оцінками, внаслідок протиправної діяльності клієнтів банківських установ завдано шкоди на суму понад 72 мільйони доларів США.

"Зловмисники запускали вірус, що вражає комп’ютерну техніку, і пропонували антивірусну програму, в якій містився як один вірус, який, у свою чергу, дозволяв отримувати дані про платіжні банківські карти люди. Це перша такої масштабної операції у сфері боротьби з кіберзлочинністю", – наголосив начальник Управління контровіддіального забезпечення інформаційної безпеки держави СБ України Віталій Хлевицький.

21 червня ц. р. однаково у кількох країнах світу було проведено понад 30 обшуків (в Україні – 19). Іноземними партнерськими службами вилучено близько 30 серверів, правоохоронними органами Латвії затримано 2 особи. Накладені арешти на понад 40 рахунків у банківських установах Латвії та Кіпру.

Під час обшуків, проведених співробітниками СБ України в житлових приміщеннях, що належать встановленим членам злочинного угруповання та в орендованих ними офісах, вилучено понад 74 одиниці комп’ютерної техніки, близько 300 одиниць електронних носіїв інформації, документальні матеріали та грошові кошти.

Слідами СБ України у Києві, Харкові та Луганську допитано 16 встановлених учасників міжнародного злочинного угрупования, у т.ч. його організаторів та координаторів.

За попередньою оцінкою використовуваної комп’ютерної техніки на предмет зберігання в ній інформації, що підтверджує протиправну діяльність встановлених осіб, встановлено, що програмне забезпечення, яке створено (або модифіковано) та використане окремими членами злочинного угруповання, відноситься до шкідливого програмного забезпечення.

У слідчих діях, що проводились на території України, взяли участь спеціалісти ФБР США. За інформацією офіційних представників ФБР, організація та результати спільної операції отримали високу оцінку Уряду США.

Старший спеціальний агент ФБР США Норм Олдверхов розповів, що ФБР розслідувалою це справу протягом трьох років. Обмінюючи інформацією з СБУ, стало зрозуміло, що служби в обох країнах здійснюють злочинні дії тих самих осіб.

"Без підтімки СБУ не вдалося б здійснити цю спецоперацію", - сказав він.

З словами в. о. керівника представництва ФБР США в Україні Бренда Сміта, кіберзлочинність може бути охопленою усе світ, і не можна говорити, що Україна є однією з країн, в якій хакерство найбільш поширене.
Security Service in cooperation with foreign intelligence services by partner international criminal group exposed by hackers

23 June 2011

Службою безпеки України у координації з правоохоронними органами США, Великої Британії, Нідерландів, Франції, Німеччини, Кіпру та Латвії (усього – 10 країн) припинено протидіянчу діяльність міжнародного злочинного угрупування хакерів, організованого та координованого громадянами України під прикриттям легально діючої комерційної структури, які шляхом використання спеціалізованого комп’ютерного вірусу «Confiscator» отримували доступ до рахунків в іноземних банківських установах різних країн світу, незаконно переводили отримані кошти і перекидно в інших банках. Накопичені кошти виділено в обігу на суму іще більше 72 млн доларів.

"The attackers ran a virus that attacks computers, and offered an anti-virus program, which contained another virus which, in turn, allowed to obtain data on bank card payment people. This is the first of this scale operation in combating cybercrime," - said Head of counterintelligence information security State Security Service of Ukraine Vitaliy Klyuytsky.

June 21 this year simultaneously in several countries conducted more than 30 searches (in Ukraine - 19). Foreign partner services seized about 30 servers Latvian law enforcement agencies arrested two persons. Seized more than 40 accounts in banks in Latvia and Cyprus.

During the searches conducted by the Security Service of Ukraine in premises belonging to the established members of the criminal group and rented offices, seized more than 74 units of computer equipment, 300 pieces of electronic media, documentary materials and cash.

Investigators Security Service of Ukraine in Kyiv, Kharkiv and Luhansk interviewed 16 participants established an international criminal group, including the organizers and coordinators.

According to preliminary estimates seized computer equipment for the purpose of storage of information in it that proves unlawful activities established by individuals, found that the software that created (or modified) and used by individual members of the criminal group refers to malicious software.

In the investigation, carried out on the territory of Ukraine, attended by experts of the FBI. According to FBI officials, organization and results Joint operations were commenced the U.S. Government.

Senior FBI Special Agent Norman Sanders told the U.S. that the FBI investigated the case for three years. Exchanging information with the Security Service, it became clear that the security services of both countries to investigate the criminal acts of the same person.

"Without the support of the Security Service failed to make this special operation," - he said.

According to. about. head of the FBI offices in Ukraine Brenda Smith, cybercrime can be covered by the whole world, and we can not say that Ukraine is a country in which the most common hacking.

He noted that similar offenses committed around the world.

Main Investigation Department of Security Service of Ukraine addressed the issue of criminal hacking.
Equipment confiscated in 2011 bust
Equipment confiscated in 2010 bust
Equipment confiscated in 2010 bust
The Power of Infiltration
The PPI Eco-system

Infiltration opportunity

Clients

Fake AV
Spambot
Keylogger

PPI Service

PPI Affiliate

Target Host

Downloader
Install
Payment

4

1

2

3

Infiltration opportunity
Advanced malware intelligence via PPI infiltration

Milking = mimic downloader, repeatedly ask PPI service for next program to install

Reverse engineering the downloader protocol allows shamelessly aggressive downloading of PPI Badness
Advanced malware intelligence via PPI infiltration

Milking = mimic downloader, repeatedly ask PPI service for next program to install

Run binaries in controlled environment to characterize activity
Advanced malware intelligence via PPI infiltration

Milking = mimic downloader, repeatedly ask PPI service for next program to install

Associate activity with different malware families
Running for five months, downloaded ("milked") > 1M binaries (9K distinct) from 4 different affiliate programs
The majority of the world’s top malware appeared in the “milk”
A handful of specimens were “old news”.

20%+ had yet to be seen.

Most specimens took days to have broad anti-virus recognition.

Malware that targets Europe.

Exclusive to USA.

Omnivore.

Avg. PPI specimen “lifetime”: 11 days.
Cybercrime Meets Political Manipulation
Russian election protests – Saturday 10 December 2011

- Largest political event of its kind since the fall of the USSR
- An estimated 50,000 people gathered in Moscow and 10,000 in St Petersburg
- They allege widespread fraud in Sunday’s polls
- More than 1,000 arrests
- Protestors pledge to take to the streets again on December 24
- They want Sunday’s election results annulled

26K Twitter accounts tweet 440K junk messages to drown out discourse / coordination.
Geolocation of Logins

26K accounts purchased from *spam-as-a-service* program. Part of a lot of 975K.
Наш магазин аккаунтов рад предложить аккаунты различных почтовых служб и бесплатных хостингов для любых задач. Вы получите аккаунты СРАЗУ после оплаты заказа через Webmoney.

Также доступна услуга залива редиректов на Pochta.ru, Cwahi.net и 0catch.com что является уникальной услугой - вы получаете готовые редиректы в течение часа после заказа. При покупке аккаунтов менее 1000 штук действует специальный тариф.

www.FreedomScripts.org - разработка софта на заказ
Mega Софт для дорасев - Zerber
Одобратор друзей - Мой мир

Twidium - безопасный и профессиональный инструмент для раскрутки твиттера
накрутить фолловеров в Твиттер

Заработай на продаже аккаунтов

Купить аккаунты Одноклассников
Купить аккаунты Вконтакте

<table>
<thead>
<tr>
<th>Служба</th>
<th>Кол-во акков</th>
<th>Цена за 1K аккаунтов</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail.ru</td>
<td>117025</td>
<td>до 10К: $5</td>
</tr>
<tr>
<td>Mail.ru Mix</td>
<td>327199</td>
<td>до 10К: $5</td>
</tr>
<tr>
<td>Mail.ru Second Hand</td>
<td>0</td>
<td>до 10К: $4</td>
</tr>
<tr>
<td>Mail.ru Mix S/H</td>
<td>15811</td>
<td>до 10К: $4</td>
</tr>
<tr>
<td>Yandex.ru</td>
<td>4758</td>
<td>до 10К: $20</td>
</tr>
<tr>
<td>Narod.ru</td>
<td>5315</td>
<td>до 10К: $50</td>
</tr>
</tbody>
</table>

**Новости**

*06 Апр 2013*  
Временно не продаем аккаунты Twitter.com

*15 Мар 2013*  
Отличная цена на аккаунты Facebook.com! Всего $80 за 1000 шт.  
Дешевле не бывает!

*07 Фев 2013*  
Сенсационная цена на аккаунты Yahoo.com. Теперь отличные аккаунты со всеми регистрационными данными по цене от $7 за 1000 шт!

*06 Фев 2013*
Beyond Technical Security
Motivation
The “Failure” of Technical Security

• Decades of work on security principles, mechanisms & detection have **not led to a secure Internet**

• We defenders face **structural disadvantages**:
  – Defenses public, attacker develops/tests in private
    • Arms race where best case for defender is to “catch up”
  – Attacker not tied to any particular technology; cheaper for them to change than us
  – Minimal deterrence

• *Is there a different way to fight the war?*
Наш магазин аккаунтов рад предложить аккаунты различных почтовых служб и бесплатных хостингов для любых задач. Вы получите аккаунты СРАЗУ после оплаты заказа через Webmoney.

Также доступна услуга залива редиректов на Pochta.ru, Cwahi.net и 0catch.com что является уникальной услугой - вы получаете готовые редиректы в течение часа после заказа. При покупке аккаунтов менее 1000 штук действует специальный тариф.

www.FreedomScripts.org - разработка софта на заказ
Mega Софт для дорогов - Zerber
Одобряет друзей - Мой мир

Twidiium - безопасный и профессиональный инструмент для раскрутки твиттера накрутить фолловеров в Твиттер

Заработай от продажи аккаунтов

Купить аккаунты Одноклассников
Купить аккаунты Вконтакте

### Сейчас в продаже

<table>
<thead>
<tr>
<th>Служба</th>
<th>Кол-во акков</th>
<th>Цена за 1К аккаунтов</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail.ru</td>
<td>117025</td>
<td>до 10K: $5</td>
</tr>
<tr>
<td>Mail.ru Mix</td>
<td>327199</td>
<td>до 10K: $5</td>
</tr>
<tr>
<td>Mail.ru Second Hand</td>
<td>0</td>
<td>до 10K: $4</td>
</tr>
<tr>
<td>Mail.ru Mix S/H</td>
<td>15811</td>
<td>до 10K: $4</td>
</tr>
<tr>
<td>Yandex.ru</td>
<td>4758</td>
<td>до 10K: $20</td>
</tr>
<tr>
<td>Narod.ru</td>
<td>5315</td>
<td>до 10K: $50</td>
</tr>
</tbody>
</table>

### Новости

#### 06 Апр 2013
Временно не продаём аккаунты Twitter.com

#### 15 Мар 2013
О отличная цена на аккаунты Facebook.com! Всего $80 за 1000 шт. Дешевле не бывает!

#### 07 Фев 2013
Сенсационная цена на аккаунты Yahoo.com. Теперь отличные аккаунты со всеми регистрационными данными по цене от $7 за 1000 шт!

#### 06 Фев 2013
Spent ~$5K to purchase 120K fake Twitter accounts from 27 merchants

<table>
<thead>
<tr>
<th>Merchant</th>
<th>Period</th>
<th>#</th>
<th>Accts</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>alexissmalley</td>
<td>06/12–03/13</td>
<td>14</td>
<td>13,000</td>
<td>$4</td>
</tr>
<tr>
<td>naveedakhtar</td>
<td>01/13–03/13</td>
<td>4</td>
<td>2,044</td>
<td>$5</td>
</tr>
<tr>
<td>truepals</td>
<td>02/13–03/13</td>
<td>3</td>
<td>820</td>
<td>$8</td>
</tr>
<tr>
<td>victoryservices</td>
<td>06/12–03/13</td>
<td>15</td>
<td>15,819</td>
<td>$6</td>
</tr>
<tr>
<td>webmentors2009</td>
<td>10/12–03/13</td>
<td>9</td>
<td>9,006</td>
<td>$3–4</td>
</tr>
<tr>
<td>buuman</td>
<td>10/12–10/12</td>
<td>1</td>
<td>75</td>
<td>$7</td>
</tr>
<tr>
<td>danyelgallu</td>
<td>10/12–10/12</td>
<td>1</td>
<td>74</td>
<td>$7</td>
</tr>
<tr>
<td>denial93</td>
<td>10/12–10/12</td>
<td>1</td>
<td>255</td>
<td>$20</td>
</tr>
<tr>
<td>formefor</td>
<td>09/12–11/12</td>
<td>3</td>
<td>408</td>
<td>$2–10</td>
</tr>
<tr>
<td>gethumarian</td>
<td>09/12–10/12</td>
<td>3</td>
<td>320</td>
<td>$4–5</td>
</tr>
<tr>
<td>jackhack08</td>
<td>09/12–09/12</td>
<td>2</td>
<td>755</td>
<td>$1</td>
</tr>
<tr>
<td>kathlyn</td>
<td>10/12–10/12</td>
<td>1</td>
<td>74</td>
<td>$7</td>
</tr>
<tr>
<td>smokinbluelady</td>
<td>08/12–08/12</td>
<td>1</td>
<td>275</td>
<td>$2</td>
</tr>
<tr>
<td>twitfollowers</td>
<td>10/12–10/12</td>
<td>1</td>
<td>80</td>
<td>$6</td>
</tr>
<tr>
<td>twitter007</td>
<td>10/12–10/12</td>
<td>1</td>
<td>75</td>
<td>$7</td>
</tr>
<tr>
<td>kamalkishover</td>
<td>06/12–03/13</td>
<td>14</td>
<td>12,094</td>
<td>$4–7</td>
</tr>
<tr>
<td>shivnagshudhakar</td>
<td>06/12–06/12</td>
<td>1</td>
<td>1,002</td>
<td>$4</td>
</tr>
<tr>
<td>accts.biz</td>
<td>05/12–03/13</td>
<td>15</td>
<td>17,984</td>
<td>$2–3</td>
</tr>
<tr>
<td>buyaccountsnow.com</td>
<td>06/12–11/12</td>
<td>8</td>
<td>7,999</td>
<td>$5–8</td>
</tr>
<tr>
<td>buyaccs.com</td>
<td>06/12–03/13</td>
<td>14</td>
<td>13,794</td>
<td>$1–3</td>
</tr>
<tr>
<td>buytwitteraccounts.biz</td>
<td>09/12–10/12</td>
<td>3</td>
<td>2,875</td>
<td>$5</td>
</tr>
<tr>
<td>buytwitteraccounts.info</td>
<td>10/12–03/13</td>
<td>9</td>
<td>9,200</td>
<td>$3–4</td>
</tr>
<tr>
<td>dataentryassistant.com</td>
<td>10/12–03/13</td>
<td>9</td>
<td>5,498</td>
<td>$10</td>
</tr>
<tr>
<td>getbulkaccounts.com</td>
<td>09/12–09/12</td>
<td>1</td>
<td>1,000</td>
<td>$2</td>
</tr>
<tr>
<td>quickaccounts.bigcartel</td>
<td>11/12–11/12</td>
<td>2</td>
<td>1,501</td>
<td>$3</td>
</tr>
<tr>
<td>spamvilla.com</td>
<td>06/12–10/12</td>
<td>3</td>
<td>2,992</td>
<td>$4</td>
</tr>
<tr>
<td>xlinternetmarketing.com</td>
<td>10/12–10/12</td>
<td>1</td>
<td>1,000</td>
<td>$7</td>
</tr>
</tbody>
</table>

Total  05/12–03/13  140  120,019  $1–20
Developed classifiers to match **all** accounts registered from the same template.
Worked with Twitter to assess classifier:
- Precision: 99.9942%
- Recall: 95%

Detected “millions” of accounts …
If you need quality **bulk accounts**, you've come to the right place. You can get your accounts **immediately** after your payment - there is no need to wait.

All the accounts are provided in **any format** you like. Just use our **free account converter** to get them in the way you need.

Special rates are applied if you purchase less than 1000 accounts.

We accept Liberty Reserve and Paypal.

Please, review our **terms and conditions** before purchasing any accounts.

---

<table>
<thead>
<tr>
<th>For sale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provider</strong></td>
</tr>
<tr>
<td>Hotmail.com</td>
</tr>
<tr>
<td>Hotmail.com Verified</td>
</tr>
<tr>
<td>Outlook.com Plus</td>
</tr>
<tr>
<td>Gmail.com USA PVA</td>
</tr>
<tr>
<td>Yahoo.com</td>
</tr>
<tr>
<td>Yahoo.com USA</td>
</tr>
<tr>
<td>Nokiamail.com</td>
</tr>
</tbody>
</table>

---

**06 Apr 2013**

Twitter accounts are not available. We will start selling them shortly.

---

**07 Feb 2013**

Added Instagram accounts at a great rate: $50 per 1000.

**04 Dec 2012**

Just added Fully Profiled Twitter Accounts at a great rate - $30 per 1000. Accounts come with avatar, bio and random background.

**19 Nov 2012**

Great prices for wholesale Twitter.com and Hotmail.com orders!
Merchant Reactions

“... All of the stock got suspended ... Not just mine .. It happened with all of the sellers .. Don't know what twitter has done ...”

- Immediately after:
  - 90% of purchased accounts suspended on arrival
- 2 weeks after:
  - 50% of purchased accounts suspended on arrival
- Strangely, no price changes!
“Click Trajectories”
Phases of the Spam Value Chain

If we were to “snip” a link in this chain, which one would be the most disruptive for our least expenditure?
<table>
<thead>
<tr>
<th>Feed Name</th>
<th>Feed Description</th>
<th>Received URLs</th>
<th>Distinct Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feed A</td>
<td>MX honeypot</td>
<td>32,548,304</td>
<td>100,631</td>
</tr>
<tr>
<td>Feed B</td>
<td>Seeded honey accounts</td>
<td>73,614,895</td>
<td>35,506</td>
</tr>
<tr>
<td>Feed C</td>
<td>MX honeypot</td>
<td>451,603,575</td>
<td>1,315,292</td>
</tr>
<tr>
<td>Feed D</td>
<td>Seeded honey accounts</td>
<td>30,991,248</td>
<td>79,040</td>
</tr>
<tr>
<td>Feed X</td>
<td>MX honeypot</td>
<td>198,871,030</td>
<td>2,127,164</td>
</tr>
<tr>
<td>Feed Y</td>
<td>Human identified</td>
<td>10,733,231</td>
<td>1,051,211</td>
</tr>
<tr>
<td>Feed Z</td>
<td>MX honeypot</td>
<td>12,517,244</td>
<td>67,856</td>
</tr>
<tr>
<td>Cutwail</td>
<td>Bot</td>
<td>3,267,575</td>
<td>65</td>
</tr>
<tr>
<td>Grum</td>
<td></td>
<td>11,920,449</td>
<td>348</td>
</tr>
<tr>
<td>MegaD</td>
<td></td>
<td>1,221,253</td>
<td>4</td>
</tr>
<tr>
<td>Rustock</td>
<td>Bot</td>
<td>141,621,731</td>
<td>13,612,815</td>
</tr>
<tr>
<td>Other bots</td>
<td>Bot</td>
<td>7,768</td>
<td>4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>968,918,303</strong></td>
<td><strong>17,813,952</strong></td>
</tr>
</tbody>
</table>

Table I: Feeds of spam-advertised URLs used in this study. We collected feed data from August 1, 2010 through October 31, 2010.
Looked at three categories: *Pharma, Replica, Software*

Covered all the major affiliate programs

<table>
<thead>
<tr>
<th>Affiliate Program</th>
<th>URLs</th>
<th>Volume</th>
<th>Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pharma Total</strong></td>
<td>347,053,630</td>
<td>93.74%</td>
<td>54,142</td>
</tr>
<tr>
<td>RX-Promotion</td>
<td>160,522,026</td>
<td>21.7%</td>
<td>10,586</td>
</tr>
<tr>
<td>Mailien</td>
<td>69,961,211</td>
<td>23.57%</td>
<td>14,444</td>
</tr>
<tr>
<td>Pharmacy Express</td>
<td>69,959,633</td>
<td>23.57%</td>
<td>14,381</td>
</tr>
<tr>
<td>ED Express</td>
<td>1,578</td>
<td>&lt;0.01%</td>
<td>63</td>
</tr>
<tr>
<td>ZedCash (Pharma)</td>
<td>42,297,130</td>
<td>18.93%</td>
<td>6,981</td>
</tr>
<tr>
<td>Dr. Maxman</td>
<td>32,184,860</td>
<td>13.19%</td>
<td>5,641</td>
</tr>
<tr>
<td>Viagrow</td>
<td>5,222,658</td>
<td>3.57%</td>
<td>386</td>
</tr>
<tr>
<td>US HealthCare Inc.</td>
<td>3,196,538</td>
<td>1.42%</td>
<td>167</td>
</tr>
<tr>
<td>MaxGentleman</td>
<td>1,144,703</td>
<td>0.39%</td>
<td>672</td>
</tr>
<tr>
<td>VigREX</td>
<td>426,873</td>
<td>0.31%</td>
<td>39</td>
</tr>
<tr>
<td>Stud Extreme</td>
<td>71,104</td>
<td>0.05%</td>
<td>43</td>
</tr>
<tr>
<td>ManXtenz</td>
<td>50,394</td>
<td>&lt;0.01%</td>
<td>33</td>
</tr>
<tr>
<td>GlavMed</td>
<td>28,313,136</td>
<td>7.84%</td>
<td>2,933</td>
</tr>
<tr>
<td>Online Pharmacy</td>
<td>17,266,034</td>
<td>5.07%</td>
<td>2,922</td>
</tr>
<tr>
<td>EvaPharmacy</td>
<td>12,798,999</td>
<td>5.79%</td>
<td>11,285</td>
</tr>
<tr>
<td>World Pharmacy</td>
<td>10,412,850</td>
<td>5.88%</td>
<td>691</td>
</tr>
<tr>
<td>PH Online</td>
<td>2,971,368</td>
<td>2.14%</td>
<td>101</td>
</tr>
<tr>
<td>Swiss Apotheke</td>
<td>1,593,532</td>
<td>0.21%</td>
<td>118</td>
</tr>
<tr>
<td>HerbalGrowth</td>
<td>265,131</td>
<td>0.19%</td>
<td>17</td>
</tr>
<tr>
<td>RX Partners</td>
<td>229,248</td>
<td>0.15%</td>
<td>448</td>
</tr>
<tr>
<td>Stimul-cash</td>
<td>157,537</td>
<td>0.07%</td>
<td>50</td>
</tr>
<tr>
<td>MAXX Extend</td>
<td>104,201</td>
<td>&lt;0.01%</td>
<td>23</td>
</tr>
<tr>
<td>DrugRevenue</td>
<td>56,167</td>
<td>0.05%</td>
<td>122</td>
</tr>
<tr>
<td>Ultimate Pharmacy</td>
<td>44,126</td>
<td>0.02%</td>
<td>12</td>
</tr>
<tr>
<td>Greenline</td>
<td>25,021</td>
<td>&lt;0.01%</td>
<td>1,766</td>
</tr>
<tr>
<td>Virility</td>
<td>23,528</td>
<td>0.01%</td>
<td>9</td>
</tr>
<tr>
<td>MediTrust</td>
<td>6,156</td>
<td>&lt;0.01%</td>
<td>24</td>
</tr>
<tr>
<td>RX Rev Share</td>
<td>5,690</td>
<td>&lt;0.01%</td>
<td>183</td>
</tr>
<tr>
<td>Unknown Program</td>
<td>3,310</td>
<td>&lt;0.01%</td>
<td>1,270</td>
</tr>
<tr>
<td>Canadian Pharmacy</td>
<td>1,392</td>
<td>&lt;0.01%</td>
<td>133</td>
</tr>
<tr>
<td>RXCash</td>
<td>287</td>
<td>&lt;0.01%</td>
<td>22</td>
</tr>
<tr>
<td>Stallion</td>
<td>80</td>
<td>&lt;0.01%</td>
<td>2</td>
</tr>
</tbody>
</table>

| **Software Total**     | 3,071,828 | 1.79% | 7,252 |
| Royal Software         | 2,291,571 | 1.48% | 572    |
| EuroSoft               | 694,810   | 0.31% | 1,161  |
| Auth. Soft. Resellers  | 65,918    | <0.01% | 4,117 |
| OEM Soft Store         | 19,436    | <0.01% | 1,367 |
| Soft Sales             | 93        | <0.01% | 35     |

| **Replica Total**      | 15,351,038 | 4.46% | 7,558 |
| ZedCash (Replica)      | 13,264,108 | 4.29% | 7,011 |
| Ultimate Replica       | 10,464,930 | 3.35% | 5,032 |
| Distinction Replica    | 1,252,816  | 0.3%  | 130    |
| Diamond Replicas       | 506,486    | 0.14% | 1,307  |
| Prestige Replicas      | 382,964    | 0.16% | 101    |
| Exquisite Replicas     | 620,642    | 0.32% | 128    |
| One Replica            | 21,318     | 0.02% | 83     |
| Luxury Replica         | 11,207     | <0.01% | 28    |
| Aff. Accessories       | 3,669      | <0.01% | 187   |
| Swiss Rep. & Co.       | 76         | <0.01% | 15     |
| WatchShop              | 2,086,930  | 0.17% | 547    |
Order approved

Your transaction has been approved.

Your order ID: 138731
First name: Kirill
Last name: Levchenko
Card used with this order: 46****2288
Total amount charged: $52.95

The following billing descriptor appear on your credit card statement:

medissue.com +12175686119

Tracking number will be sent on your email once medications will be shipped.

NOTE: Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

Dear Kirill Levchenko, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: www.rxsup24.com
If we were to “snip” a link in this chain, which one would be the most disruptive for our least expenditure?
Hosting bottlenecks

- No hosting bottleneck -- long tail
Small number of registrars over-represented in spam

But ... many alternatives, low switching cost, slow intervention, and long tail
Merchant Bank bottlenecks

% Spam

0 10 20 30 40 50 60 70 80 90 100

AZ1  KN1  LV2  LV1  GR1  IS1  IS2  GE  MR  RU  US  GR2

Bank

Azerigazbank
Saint Kitts
DnB Nord
Bingo


Merchant Bank bottlenecks

3 banks hosted 95+% of all sales
In early 2004 Bill Gates claimed that “two years from now, spam will be solved.” Today it amounts to 70 percent of all e-mail. Yet there may be a chance to cut it back.

In March, spam volumes tumbled as United States marshals seized computers at Internet hosting facilities that controlled Rustock, a

The good news is there may be other ways to disrupt spammers. The Times’s John Markoff reported that computer scientists at two University of California campuses have found another vulnerability: spammers’ banks.

To track the flow of information, the researchers made hundreds of purchases. Buying Viagra from the Pharmacy Express group in Russia involved computers in Brazil, China and Turkey. The Viagra came from India. But 95 percent of the purchases were handled by three banks — in Azerbaijan, Latvia and St. Kitts and Nevis. This suggests that if banks
Dear webmasters,

Due to the recent developments which led to all our bank and processing accounts being jeopardized, we have to inform you, that functioning of the Medinc partnership program will be discontinued, as no reliable solution has been found to keep it working, and the debts to suppliers and partners keep increasing.

We were happy to work with all of you, and we are very sorry that we can’t cooperate with you anymore within this project.

If we manage to find a reliable processing solution to resume working, all webmasters will receive an email notification sent to the address submitted during registration.
Dear Partners,

As you may have noticed, in the last couple of days we've had problems with processing. We don't have a solution yet, and there is no concrete time when it will be resolved.

From this point forward, GlavMed is switching to a "PAUSED" mode. No new orders will be processed until the processing issue is resolved.

We urge you to temporarily switch your traffic to other shops/projects.
“Right now most affiliate programs have a mass of declines, cancels and pendings, and it doesn't depend much on the program imho, there is a general sad picture, fucking Visa is burning us with napalm (for problematic countries, it's totally fucked, on a couple of programs you're lucky if you get 50% through).”