Monetizing Attacks / The Underground Economy

original slides by

Prof. Vern Paxson

University of California, Berkeley
Today

• A look at profit-driven cybercrime …
  – Monetization of malware
  – Monetization of spam

• … including the *Underground Economy*
  – Elements
  – Significance
  – Infiltration/disruption
Cybercrime
Monetizing Malware Locally

- General malware monetization approaches:
  - Keylogging: steal financial/email/social network accounts
  - Ransomware
  - Scareware ("fake AV")
Your Computer is Infected!

Threats and actions:

<table>
<thead>
<tr>
<th>Name</th>
<th>Risk level</th>
<th>Date</th>
<th>Files infected</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email-Worm.Win32.Myd</td>
<td>Critical</td>
<td>11.18.2008</td>
<td>65</td>
<td>Waiting removal</td>
</tr>
<tr>
<td>Win 32:Delf-XQ</td>
<td>Critical</td>
<td>11.18.2008</td>
<td>44</td>
<td>Waiting removal</td>
</tr>
</tbody>
</table>

Description:
This program is potentially dangerous for your system. Trojan-Downloader stealing passwords, credit cards and other personal information from your computer.

Advice:
You need to remove this threat as soon as possible!
Monetizing Malware Locally

• General malware monetization approaches:
  – Keylogging: steal financial/email/social network accounts
  – Ransomware
  – Scareware (“fake AV”)
  – *Transaction generators* (“man-in-the-browser”)
    • Malware watches user’s surfing …
    • … waits for them to log into banking site (say) …
    • … and then injects *additional* banking transactions like “send $50,000 to Nigeria” …
    • … and *alters* web server replies to mask the change in the user’s balance
Monetizing Large-Scale Malware

- Monetization that leverages *botnet scale*
  - DDoS (extortion)
  - Spam
  - *Click fraud*
  - Scam infrastructure
    - Hosting web pages (e.g., phishing)
    - Redirection to evade blacklisting/takedown (DNS)
    - Proxying traffic to thwart tracing / provide *IP diversity*

- Which of these cause serious pain for infected user?
  - *None*. Users have *little incentive* to prevent

  ⇒ *Externality* (cost one party’s actions impose on another)
Spam & Spam Profit
Monetizing Spam

• In what different ways can spammers make money off of sending spam?
  – And who has incentives to thwart these schemes?
    • (Other than law enforcement)

• Scheme #1: advertise goods or services
  – Examples: fake Rolexes, Viagra, university degrees
  – Profit angle: increased sales
  – Who’ll try to stop: brand holders
Anatomy of a modern Pharma spam campaign

Spammer
- Bulk email sender
- Open proxies/botnet

Spam emails
- Email with link
- Redirects

Email recipient
- Curious?
- Clicks on link

Affiliate program
- Commission (up to 40%)

Generic pills
- Sildenafil citrate
- Non-US supply (India, Mexico etc.)
- Patent expired
- Mere cents per pill = massive markup

Viagra/pharmacy site
- VGR100
- Sale made
- Typical value $50-100

Shipped to customer

Diagram by Stuart Brown
modernlifeisrubbish.co.uk
Monetizing Spam

• In what different ways can spammers make money off of sending spam?
  – And who has incentives to thwart these schemes?
    • (Other than law enforcement)

• Scheme #1: advertise goods or services
  – Examples: fake Rolexes, Viagra, university degrees
  – Profit angle: increased sales
  – Who’ll try to stop: brand holders

• Scheme #2: phishing
  – Profit angle: transfer $$$ out of accounts; sell accounts to others; use accounts for better spamming (e.g. Facebook)
  – Opponents: issuers of accounts
  – Note: targeted phishing (“spear-phishing”) doesn’t actually need much in the way of spam due to low volume
Monetizing Spam, con’t

• Scheme #3: scams
  – Examples: pen pal relationships, 419 (”Nigerian”)
  – Profit angle: con victim into sending money
  – Opponents: scambaiters (e.g., www.419eater.com)

• Scheme #4: recruiting crooks/underlings
  – Examples: money mules, reshippers
  – Profit angle: enables profiting from cybercrime
  – Opponents: ?
Monetizing Spam, con’t

- **Scheme #3: scams**
  - Examples: pen pal relationships, 419 (“Nigerian”)
  - Profit angle: con victim into sending money
  - Opponents: scambaiters (e.g., www.419eater.com)

- **Scheme #4: recruiting crooks/underlings**
  - Examples: money mules, reshippers
  - Profit angle: enables profiting from cybercrime
  - Opponents: ?

Money mules take incoming (fraudulent) financial transfers to their bank accounts, wire-transfer 90% out of country, keep 10%
Monetizing Spam, con’t

• Scheme #3: scams
  – Examples: pen pal relationships, 419 ("Nigerian")
  – Profit angle: con victim into sending money
  – Opponents: scambaiters

• Scheme #4: recruiting
  – Examples: money mules, reshippers
  – Profit angle: enables profiting from cybercrime
  – Opponents: ?
Monetizing Spam, con’t

• Scheme #5: pump-and-dump
  – Example: “Falcon Energy (FPK) is about to go through the roof! Don’t miss out on $eriou$ Profit$!$”
  – Profit angle: penny-stock momentarily goes up, dump pre-bought shares when it does
  – Opponents: Securities and Exchange Commission
  – Note: unlike other monetization techniques, the “back channel” is out-of-band
    • No link in messages back to the scammer

• Scheme #6: recruiting bots
  – Examples: “important security patch!”,”someone sent you a greeting card!”
  – Profit angle: get malware installed on new machines
  – Opponents: ?
Welcome to Storm!
"230 dead as storm batters Europe“
(Windows virus spread by spam)

Would you like to be one of our newest bots?
Just read your postcard!
(Or even easier: just wait 5 seconds!)
The *Storm* Spambot

- Infected systems
- Overnet P2P protocol (UDP)
- Reachability check

Diagram showing a network of infected systems connected to a central Overnet P2P protocol (UDP) node through reachability checks.
The **Storm** Botnet

- **Botmaster**
- **Hosted infrastructure**
  - HTTP proxies
  - HTTP
- **Infected machines**
  - Proxy bots
  - TCP
- **Workers**

Operated using "bulletproof hosting"
Spam “Campaign” Mechanics

Botmaster

HTTP proxies

HTTP

Proxy bots

TCP

Workers
Campaign Mechanics: Harvest

give me a task!
Campaign Mechanics: Spamming

- Botmaster
- HTTP proxies
- HTTP
- Proxy bots
- TCP
- Workers
- templates
dictionaries
addresses
Synthetic diversity aims to thwart content-based anti-spam filtering.

Figure 2: Snippet of a spam template, showing the transformation of an email header from template (top) to resulting content (bottom). The \texttt{\textbackslash b} symbol indicates line continuations. Bold text corresponds to the formatting macros and their evaluation.
<table>
<thead>
<tr>
<th>Macro</th>
<th>Seen Live</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0)</td>
<td>✓</td>
<td>Spam target email address.</td>
</tr>
<tr>
<td>(A)</td>
<td>✓</td>
<td>FQDN of sending bot, as reported to the bot as part of the preceding C&amp;C exchange.</td>
</tr>
<tr>
<td>(B)</td>
<td>✓</td>
<td>Creates content-boundary strings for multi-part messages.</td>
</tr>
<tr>
<td>(Cnum)</td>
<td>✓</td>
<td>Labels a field’s resulting content, so it can be used elsewhere through (V); see below.</td>
</tr>
<tr>
<td>(D)</td>
<td>✓</td>
<td>Date and time, formatted per RFC 2822.</td>
</tr>
<tr>
<td>(E)</td>
<td>✓</td>
<td>ROT-3–encodes the target email address.</td>
</tr>
<tr>
<td>(Fstring)</td>
<td>✓</td>
<td>Random value from the dictionary named string.</td>
</tr>
<tr>
<td>(Gstring)</td>
<td>✓</td>
<td>Line-wrap string into 72 characters per line.</td>
</tr>
<tr>
<td>(Hstring)</td>
<td>✓</td>
<td>Defines hidden text snippets with substitutions, for use in HTML- and plain-text parts.</td>
</tr>
<tr>
<td>(I)</td>
<td>✓</td>
<td>Random number between 1 and 255, used to generate fake IP addresses.</td>
</tr>
<tr>
<td>(Jstring)</td>
<td>✓</td>
<td>Produces quoted-printable ‘=” linewrapping.</td>
</tr>
<tr>
<td>(K)</td>
<td></td>
<td>IP address of SMTP client.</td>
</tr>
<tr>
<td>(M)</td>
<td>✓</td>
<td>6-character string compatible with Exim’s message identifiers (keyed on time).</td>
</tr>
<tr>
<td>(N)</td>
<td>✓</td>
<td>16-bit prefix of SMTP client’s IP address.</td>
</tr>
<tr>
<td>(Ostring:num)</td>
<td>✓</td>
<td>Randomized message identifier element compatible with Microsoft SMTPSVC.</td>
</tr>
<tr>
<td>(Pnum1[-num2]:string)</td>
<td>✓</td>
<td>Random string of num1 (up to num2, if provided) characters taken from string.</td>
</tr>
<tr>
<td>(Qstring)</td>
<td>✓</td>
<td>Quoted-printable ‘=” linewrapping.</td>
</tr>
<tr>
<td>(Rnum1-num2)</td>
<td>✓</td>
<td>Random number between num1 and num2. Note, special-cased when used with (D).</td>
</tr>
<tr>
<td>(Ustring)</td>
<td></td>
<td>Randomized percent-encoding of string.</td>
</tr>
<tr>
<td>(Vnum)</td>
<td>✓</td>
<td>Inserts the value of the field identified by (Cnum).</td>
</tr>
<tr>
<td>(W)</td>
<td></td>
<td>Time and date as plain numbers, e.g. “20080225190434”.</td>
</tr>
<tr>
<td>(X)</td>
<td></td>
<td>Previously selected member of the “names” dictionary.</td>
</tr>
<tr>
<td>(Ynum)</td>
<td>✓</td>
<td>8-character alphanumeric string, compatible with Sendmail message identifiers.</td>
</tr>
<tr>
<td>(Z)</td>
<td>✓</td>
<td>Another Sendmail-compatible generator for message identifiers.</td>
</tr>
</tbody>
</table>

Table 2: Storm’s spam-generation templating language.
Campaign Mechanics: Spamming

- Botmaster
- HTTP proxies
- HTTP
- Proxy bots
- TCP

templates
dictionaries
addresses
Campaign Mechanics: Reporting
The Rise of the *Underground Economy*
**ProAgent v2.1**

- 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 Bypass in all of our bots.

Winsock (Multi-threaded) Bots

Click here for 30+ MySpace Bots

Become an Affiliate and Start Earning Now

<table>
<thead>
<tr>
<th>Accounts Creator</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(You Just Need To Type In The CAPTCHAs To Create Accounts)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Social Networks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MySpace Accounts Creator with Picture Uploader, Profile &amp; Layout Manager</td>
<td>$180.95 - $140.00</td>
</tr>
<tr>
<td>MySpace Accounts Creator with Picture Uploader, Profile &amp; Layout Manager (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></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
Одобрятор 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

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
BuyAcchs.com: Bulk Accounts with Instant Delivery After Payment. We Accept Paypal

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.

Buy Yahoo Accounts
Buy Twitter Accounts
Buy Livejournal Accounts
Buy Hotmail Accounts

---

### For sale

<table>
<thead>
<tr>
<th>Provider</th>
<th>Quantity</th>
<th>Rate for 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotmail.com</td>
<td>449292</td>
<td>1K-10K: $5</td>
</tr>
<tr>
<td>Hotmail.com Verified</td>
<td>423418</td>
<td>1K-10K: $6</td>
</tr>
<tr>
<td>Outlook.com Plus</td>
<td>9661</td>
<td>1K-10K: $4</td>
</tr>
<tr>
<td>Gmail.com USA PVA</td>
<td>4340</td>
<td>1K-10K: $100</td>
</tr>
<tr>
<td>Yahoo.com</td>
<td>14058</td>
<td>1K-10K: $8</td>
</tr>
<tr>
<td>Yahoo.com USA</td>
<td>8688</td>
<td>1K-10K: $15</td>
</tr>
<tr>
<td>Nokiamail.com</td>
<td>0</td>
<td>1K-10K: $10</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!
List of available accounts
Service for the sale of eBay auction accounts.
Dear users of eBay accounts, we are offering our accounts for your attention.
Regular clients and those that buy more than 5 accounts will get various bonuses and discounts.
All accounts come with access to the holder's email.
You can select an account (or accounts) from a list. Just tell me. Pay and receive. All accounts are verified before sale; if something doesn't work – 100% replacement.
Active or inactive – see for yourself for each user ID. I don't sort by activeness, since this is a subjective factor for each person.
Also for sale are PayPal accounts. Market prices. Not always available.
Payment with Webmoney.
Before buying be sure to read the FAQ.
I don't offer advice on use of my products.
I welcome work through Garant Service
Seller/buyer accounts up to 10 feeds -- $5
Etc.
Advertisement

i have boa wells and barclays bank logins....
have hacked hosts, mail lists, php mailer send to all inbox
i need 1 mastercard i give 1 linux hacked root
i have verified paypal accounts with good balance...and i can cashout paypals
Marketplace Ads for Services

Percentage of Labeled Data

Ad Type (Services)
Marketplace Ads for Goods

![Bar Chart]

- Bank Login Sale
- Credit Card Want
- PayPal Account Sale
- Mailer Sale
- Hacked Host Sale
- Root Sale
- Emailist Sale
- Bank Login Want
- Credit Card Sale
cv2 Sale
- Mailer Want
- Scam Page Sale
- Drop Sale
- Full Info Sale
- Bank Account Sale
- Other Acct. Sale
- Fresh CC Sale
- Hacked Host Want
- E-gold Acct. Sale
- Shop Admin Sale
- Shop Want
- PayPal Want
cv2 Want
- Fresh CC Want
- Exploit Want
- Root Want
- Full Info Want
- Other Acct. Want
- Emailist Want
- Dump Want
- E-gold Want

Percentage of Labeled Data

Ad Type (Goods)
Pay-Per-Install (PPI)
Installs4Sale.net - надежный сервис по загрузкам, достойный доверия

Контакты:
- 560869831
- 550525933
- info[at]installs4sale.net

Приемущества:
- Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на миассы стран по вашему выбору.
- Для постоянных клиентов действуют скидки и бонусы в виде дополнительного объема загрузок.
- Договоримся по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!
Installs4Sale.net - надежный сервис по загрузкам, достойный доверия

Contacts
Контакты
- 560869831
- 550525933
- info[at]installs4sale.net

ADVANTAGES
We deliver fast for allmost anywhere. We take orders for a mix of countries of your choice. For regular clients there are discounts and bonuses in the form of extra installs. You can agree on prices and get personal terms in our service of support. Just write!

ПРИЕМУЩЕСТВА
- Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на ми克斯 стран по вашему выбору.
- Для постоянных клиентов действуют скидки и бонусы в виде дополнительного объема загрузок.
- Договориться по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!
GangstaBucks.com - it pays on time! We pay for all installs!

Join our ranks and by tomorrow you could get your first payout!
Goldinstall Rates for 1K Installs for each Country.

<table>
<thead>
<tr>
<th>Country</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTH</td>
<td>13$</td>
</tr>
<tr>
<td>US</td>
<td>150$</td>
</tr>
<tr>
<td>GB</td>
<td>110$</td>
</tr>
<tr>
<td>CA</td>
<td>110$</td>
</tr>
<tr>
<td>DE</td>
<td>30$</td>
</tr>
<tr>
<td>BE</td>
<td>20$</td>
</tr>
<tr>
<td>IT</td>
<td>65$</td>
</tr>
<tr>
<td>CH</td>
<td>20$</td>
</tr>
<tr>
<td>CZ</td>
<td>20$</td>
</tr>
<tr>
<td>DK</td>
<td>20$</td>
</tr>
<tr>
<td>ES</td>
<td>30$</td>
</tr>
<tr>
<td>AU</td>
<td>55$</td>
</tr>
<tr>
<td>FR</td>
<td>30$</td>
</tr>
<tr>
<td>NL</td>
<td>20$</td>
</tr>
<tr>
<td>NO</td>
<td>20$</td>
</tr>
<tr>
<td>PT</td>
<td>30$</td>
</tr>
<tr>
<td>LB</td>
<td>6$</td>
</tr>
</tbody>
</table>
60-70% of revenue
3-5% with referrals

Our advantages:
- Best exhaust of similar solutions
- Stable payments
- Reliability cooperation
- Individual approach
- Friendly support service
- Advert impression conversion

Additional information:
Successfully convert the following countries: US, CA, AU, GB, DE, FR. Increased long-term performance and exhaust from each instance. We offer individual and payment rates for constant partners. You can use your own landing to drive traffic.

Standard conditions:
You get 65% of total revenue with install.
You get 3% of the income for associated artists.
Stable paid 2 times a month, the 1st and the 5th.
Wide range of payment methods: Wire transfer, EPS, Bank transfer, Credit card, PayPal and others.
you get a stable, efficient and, most importantly, a reliable means of converting your traffic into good money.

News
06.05.2010
Happy Holidays!
Dear webmaster! We congratulate you on the Day of Victory! Today, xenonics.com German website is now.

09.05.2010
Access to auto-update
Dear webmaster! In order to improve the stability of the affiliate program and prevent discharges of our mobile users, Autopilot temporarily closed until 15:00.
To select a phone: 455-057-795. No access will be in a separate order.

14.04.2010
XML Stats
Dear admin! To get statistics, log in to your account, then select the summary statistic:
XML Stats. 111 stats N.1. Now! 1 user is the main account and only information on it is the same with respect to the sub-accounts.

Copyright © 2009, Dogma Millions
The Underground Economy

• Why is its emergence significant?

• Markets enable efficiencies
  – Specialization: individuals rewarded for doing a single thing particularly well

• Lowers barrier-to-entry
  – Only need a single skill
  – Some underground market activities are legal

• Competition spurs innovation
  – Accelerates arms race
  – Defenders must assume a more pessimistic threat model

• Facilitates non-$ Internet attacks (political, nation-state)
  – Provides actors with cheap attack components
  – Provides stealthy actors with plausible cover
26K Twitter accounts tweet 440K junk messages to drown out discourse / coordination.
Geolocation of Logins

Nonspam Logins

56%
Geolocation of Logins

56% Nonspam Logins
1% Spam Logins

26K accounts purchased from *spam-as-a-service* program. Part of a “lot” of 975K. Used ~20K distinct IP addresses.
The Underground Economy, con’t

• What problems do underground markets face?

• Depending on marketplace architecture, can present a target / single point of failure

• By definition, deals are between crooks
  – Major issue of betrayal by “rippers”

• Markets only provide major efficiencies if they facilitate deals between strangers
  – Susceptible to infiltration
Welcome to **Storm**! What can we sell you?
Kirill Levchenko
klevchen@cs.ucsd.edu

I am a project scientist with the Systems and Networking group in the Computer Science department at the University of California, San Diego. My current research
Template points to spammer’s server

Modified template points to our server

Under our control

Bot Controller

Proxying Bot

Re-writing Proxy

WWW server

real email accounts

our webmail accounts

our domain

n00b
Life As A Spammer …

• Storm infiltration study found:
  – Modern spam campaigns can send 10s of billions of spams using mailing lists of 100s of millions of addresses
  – 3/4 to 5/6 of all spam delivery attempts fail before the message is even sent to the receiver’s server …
    • … due to heavy & effective use of black-listing
  – It takes around 20,000 “postcard” spams to get one person to visit the postcard site
    • 1 in 10 of the visitors will click to download the postcard
  – It takes around 12,000,000 Viagra spams to get one person to visit the site and make a purchase (~$100)
  – Even given those low rates, huge volume ⇒ profitable

~ $1.5-2M/year revenue
Life As A Spammer …

- Storm infiltration study found:
  - Modern spam campaigns can send 10s of billions of messages
    - 3/4 to 5/6 of all spam delivery attempts fail before the message is even sent to the receiver's server …
      - due to heavy & effective use of black-listing
    - It takes around 20,000 “postcard” spams to get one person to visit the postcard site
    - 1 in 10 of the visitors will click to download the postcard
    - It takes around 12,000,000 Viagra spams to get one person to visit the site and make a purchase (~$100)
    - Even given those low rates, huge volume ⇒ profitable
      - ~ $1.5-2M/year revenue

Another study based on making purchases of spam-advertised pharmaceuticals found that 3 merchant banks hosted 95+% of all sales …

… suggesting a novel way to suppress spam is to undermine the credit-card processing
If we were to “snip” a link in this chain, which one would be the most disruptive for our least expenditure?

Measuring URLs, DNS servers, HTTP redirection, etc. all a matter of energetic crawling & recording.

But merchant banks / Visa / “fulfillment”?
Merchant Bank bottlenecks

3 banks host 95+% of all sales
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.
6/29/2012

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.
Measuring Pay-per-Install: The Commoditization of Malware Distribution

Juan Caballero, Chris Grier, Christian Kreibich, Vern Paxson

USENIX Security Symposium, August 2011
Infiltration opportunity
Via protocol emulation, extracted ("milked")
> 1M malicious binaries over 6 months
The majority of the world’s top malware appeared in PPI downloads.

<table>
<thead>
<tr>
<th>Name</th>
<th>%</th>
<th>Monetization</th>
<th>Kit Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Palevo</td>
<td>7.50</td>
<td>DoS, Info stealer</td>
<td>✓</td>
</tr>
<tr>
<td>Hiloti</td>
<td>4.69</td>
<td>Downloader/PPI</td>
<td>✓</td>
</tr>
<tr>
<td>Zbot</td>
<td>3.62</td>
<td>Info stealer</td>
<td>✓</td>
</tr>
<tr>
<td>FakeRean</td>
<td>3.47</td>
<td>Rogue AV(s)</td>
<td>✓</td>
</tr>
<tr>
<td>Onlinegames</td>
<td>2.94</td>
<td>Info stealer</td>
<td>?</td>
</tr>
<tr>
<td>Rustock</td>
<td>2.66</td>
<td>Spam</td>
<td>✓</td>
</tr>
<tr>
<td>Ldpinch</td>
<td>2.64</td>
<td>Info stealer</td>
<td>✓</td>
</tr>
<tr>
<td>Renos</td>
<td>2.58</td>
<td>Rogue AV(s)</td>
<td>?</td>
</tr>
<tr>
<td>Zlob</td>
<td>2.54</td>
<td>Rogue software</td>
<td>✓</td>
</tr>
<tr>
<td>Autoit</td>
<td>2.53</td>
<td>Downloader/PPI</td>
<td>✓</td>
</tr>
<tr>
<td>Conficker</td>
<td>2.48</td>
<td>Worm</td>
<td></td>
</tr>
<tr>
<td>Opachki</td>
<td>1.95</td>
<td>Click Fraud</td>
<td>✓</td>
</tr>
<tr>
<td>Buzus</td>
<td>1.91</td>
<td>Info stealer</td>
<td></td>
</tr>
<tr>
<td>Koobface</td>
<td>1.17</td>
<td>Downloader</td>
<td></td>
</tr>
<tr>
<td>Alureon</td>
<td>1.16</td>
<td>Downloader</td>
<td>✓</td>
</tr>
<tr>
<td>Bredolab</td>
<td>1.15</td>
<td>Downloader/PPI</td>
<td>✓</td>
</tr>
<tr>
<td>Piptea</td>
<td>1.13</td>
<td>Downloader/PPI</td>
<td>✓</td>
</tr>
<tr>
<td>Erfor</td>
<td>0.91</td>
<td>Rogue AV(s)</td>
<td></td>
</tr>
<tr>
<td>Virut</td>
<td>0.91</td>
<td>Downloader/PPI</td>
<td>✓</td>
</tr>
<tr>
<td>Storm 2.0</td>
<td>0.80</td>
<td>Spam</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 2: FireEye’s top 20 malware families observed in their MAX Cloud network on the April–June 2010 time.
Axiom of Criminal Laziness
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

(* Vern: This is my own working hypothesis to explain the observed pace of attacker innovation - not something concretely established)