



Dirty Money on the Wires: The Business Models of Cyber Criminals

-
Guillaume Lovet



Presentation Objectives

- Identify different **Cyber Criminals profiles**
- Understand their **business models**, based quantified **examples**
- Recognize **the channels** through which cyber crime money is flowing
- Raise public awareness and industry anticipation on **mobile threats** based criminal business models

Agenda

- Cybercrime zoology
- Cyber criminals profiles
- The Marketplace
- The Currency
- The Business Models: schemes and numbers

Introduction

- Reported offenses are the tip of the iceberg
- FBI reported **\$67 billion** in damages last year (US)
- NHTCU reported **£2.45 billion** (UK)
- Credit card fraud alone costs **\$400 million** per year

Introduction (II)

- Famous quote from Valerie McNiven, US Treasury advisor on cybercrime:

“Last year was the first year that proceeds from cybercrime were greater than proceeds from the sales of illegal drugs, and that was, I believe, over \$105 billion” [1]

[1] Reuters, 2005

Cybercrime Zoology

- Spamming
- Carding
- Phishing
- Herding
- Industrial Spying

Carding with your 6th Sense

```
XChat  View  Server  Settings  Window  Help
-----
* Now talking on #ccmastahs
M4sterMindz i have a secret...
  G-Dogg    what secret?
M4sterMindz i see cc numbers...
  overlord  lol
  G-Dogg    lol
```

Cybercrime Zoology

- Spamming
- Carding
- Phishing
- Herding
- Industrial Spying

Typical Phishing e-mail

From: Barclays Bank Security Department <online@barclays.co.uk>
To: [REDACTED]
Subject: Online Banking Safety Alert From Barclays Bank PLC
Date: Fri, 16 Jun 2006 20:05:07 +0200

BARCLAYS

Dear Customer,

Our comprehensive fraud-prevention program is one of the key reasons Barclays online services is a safe way to bank online. We believe that innovation and careful analysis is the way to beat fraud. That's why Barclays bank has developed industry-leading models to review every transaction—and help detect suspicious activity.

WHAT TO DO NOW

Follow the below reference to update your Barclays Online Banking details:-

<https://Update.barclays.co.uk/olb/q/LoginMember.do>

Cybercrime Zoology

- Spamming
- Carding
- Phishing
- Botnet Herding
- Industrial Spying

Cyber criminals profiles

- **Coders**
the skilled
- **Kids**
the workforce
- **Mob**
the puppet masters?
- **Drops**
the mules

Coders – *the skilled*

- Aged between 20 and 25 years old
- 5+ years of experience in the hacking community
- Young self-made programmers or pro coders
- **Sell** ready-to-use tools or services to the **Kids**
- Fees are in the hundreds of USD
- Limited risks (disclaimers, etc...)
- Scam artists fall in that category

Kids – *the workforce*

- Aged from 13 to 20
- Hang around IRC carding channels
- Buy and re-sell basic bricks needed for scams
- 2 digits monthly income
- Rip offs are very common
- A few percentage of actual “doers”

Mob – *the puppet masters?*

- Bringing in-depth inputs about the real mafia raises issues
- Staying in the strict boundaries of the law
- Bigger investigation means
- Years-long infiltration commitment, possibly on the field
- One of the undeniable cybercrime back-ends

Drops – *the mules*

- Older than **Kids**
- Turn **virtual** money into **real cash**
- Transfers are done to their **legal bank account**
- Keep **50%** and **wire back** the rest of the cash
- Importance of **Webs of Trust**
- Live in countries with “no digital laws”

The Marketplace: IRC

```
* raise I can cashout MANY small and independent US banks! PM ME with your bin to
check my list.
* DeathX I need valid visa cards with full info ///I have roots , shells , paypals
, master and amex cards , php mailers , ebay acc's and more msg me fast
* rrrlll need paypal accounts / i pay 10$ per via WU or egold.
JTOVI i have root's ... i need cc's fresh ... mes me
ser22 PASTE CCS
* TheOne` Cashout fresh CHEMICAL BANK AND TRUST COMPANY(all bins) ,FLAGSTAR , GE
CAPITAL FINANCIAL(all bins) , CU/FCU(all bins) , TRANSALLIANCE(all bins) ,
Southtrust(allbins) , ZIP NETWORK(some bins) , MID AMERICA(all bins) , FIRST
NATIONAL BANK(all ins) , NORTH FORK BANK(all bins) , MONEY ACCESS(all bins) , NC
NAMES(some bins) , and many others , four more bins prv me!50% cashout share !
* GOLDEN I CAN CASHOUT UK BANK ACCOUNTS( HALIFAX HSBC BARCLAYS ) MSG ME IF U HAVE
THNX
JTOVI i have root's ... i need cc's fresh ... mes me
* DeathX I need valid visa cards with full info ///I have roots , shells , paypals
, master and amex cards , php mailers , ebay acc's and more msg me fast
* woodrow ( [REDACTED] ) has joined #ccpower
JTOVI i have root's ... i need cc's fresh ... mes me
sil^^ I Need PHP SENDER I have mail lists validated with email validator , new
track2gen encoder , and many other things
* The^Judge I need urgently Capital One or any C.U F.C.U Logins are cashable 100%
also i can leave on Empty any Bank Login NOTE: I also make Cashout to ATM many
bins but only fresh Ones / I have Western Union Drop and also i can pick up MTCL
in USA and UK ! INFO: I have mail list and many scam pages and hack programs
/msg me but dont waste my time
```


The Currencies

- e-gold
 - Anonymity
 - Irreversibility
 - Independence
- Wired cash
 - Irreversible
 - Crosses borders instantly
 - Fairly anonymous

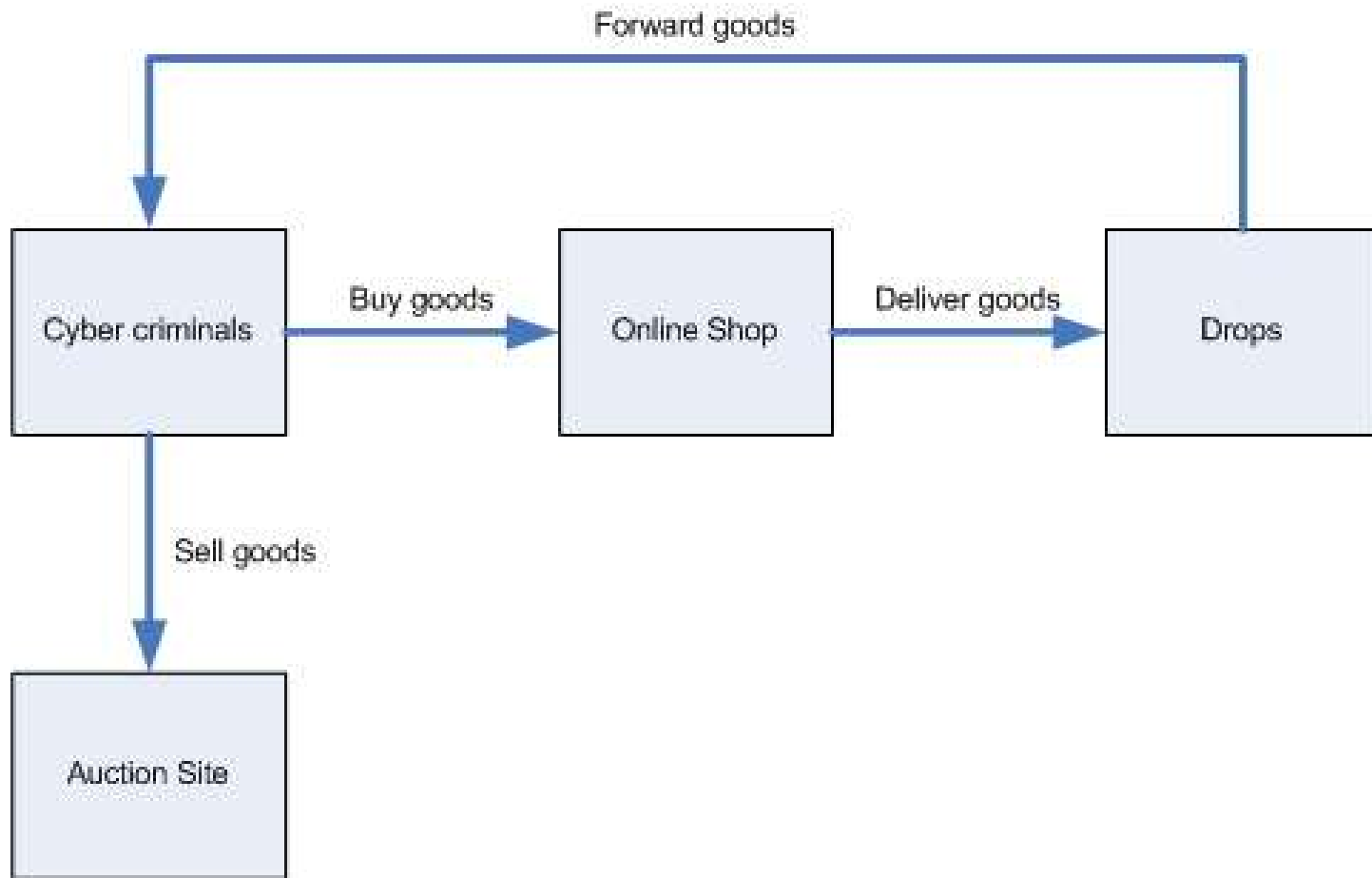
Carding Business Model

- A “CC Full” costs \$2 to \$5 (payable by e-gold)
- Around 80% of CCs traded on IRC are not valid
 - ⇒Importance of Webs of Trust
- CCs are bought by packs
 - ⇒Resembles a drug deal

Carding Business Model: The Hidden Truth

```
G-Dogg | That's a joke dude. What can u do anyways with stolen cc?  
sk4tan | buy stuff.
```

Carding Business Model: Scheme



Carding Business Model: By the Numbers

- Costs

 - Buying 40 valid CC info: **\$200**

 - Bribing 10 drops to forward one package per week: **\$800**

 - Drops to cyber criminal packages delivery costs: **\$800**

- Profits

 - Selling the goods on eBay: **\$16,000** (\$400 per package)

- Total Cost, monthly: **\$1,800**

- Total Profit, monthly: **\$16,000**

- Net Gains, monthly: **\$14,200**

- Productivity index (Profits/Costs): **8.9**

Adware Planting Business Model

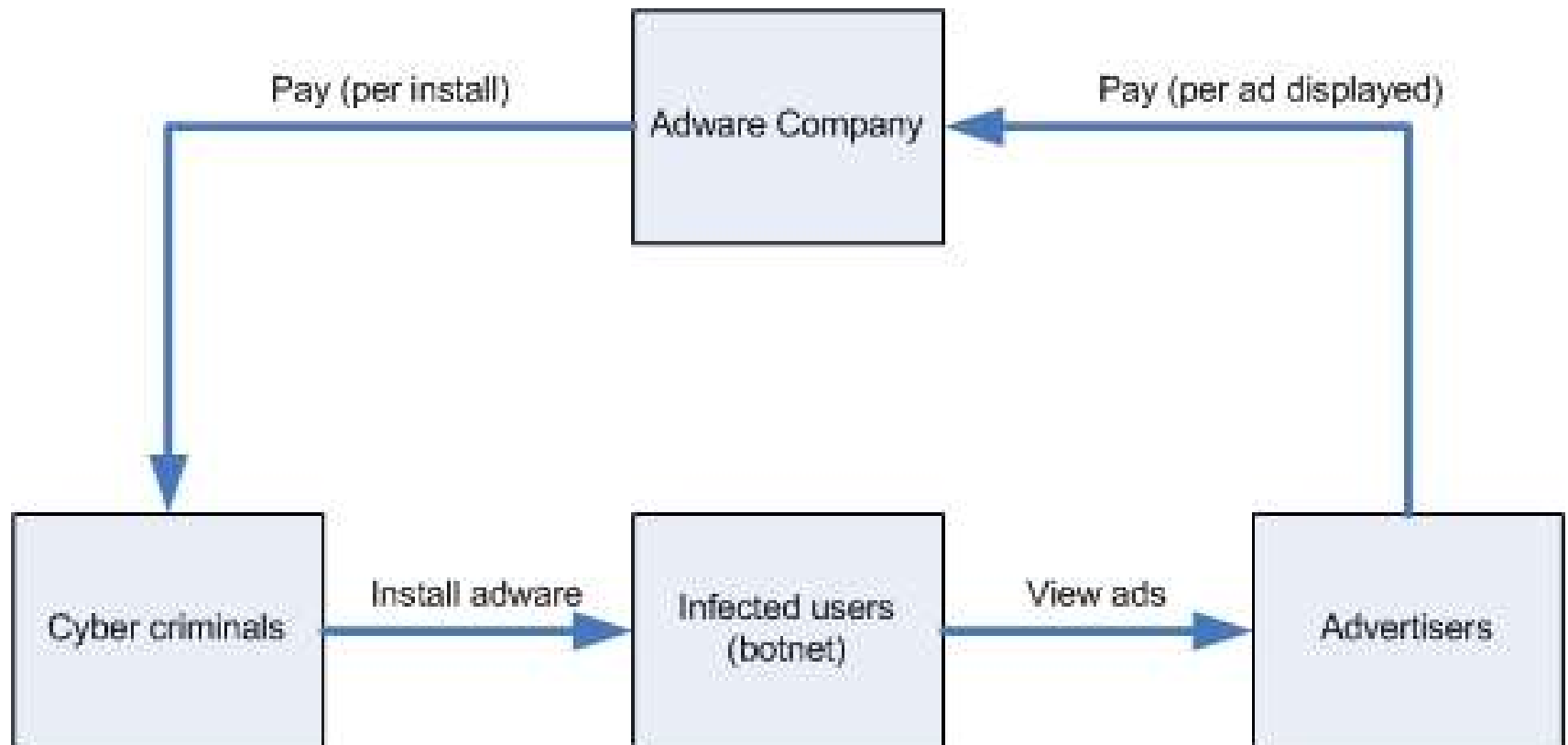
- Tightly linked to Spyware/Adware companies
BM:

Adware company 'A' edits a software that displays ads

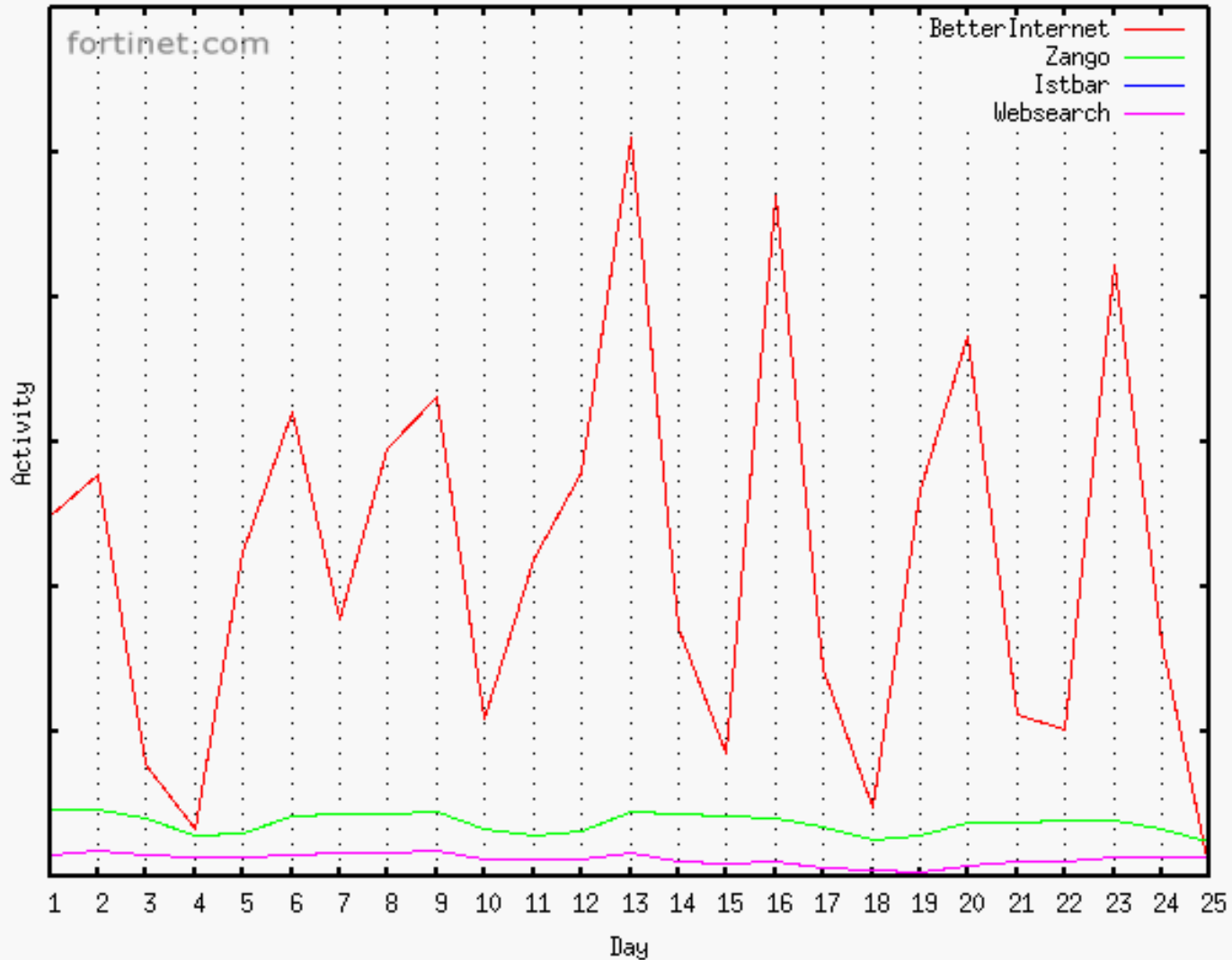
Advertisers pay company 'A' to get their ads displayed

Company 'A' pays its partners/affiliates for each install of the Spyware/Adware on end-users computers

Adware/Spyware planting Business Model: scheme



Adware/Spyware planting Business Model: Stats



Adware/Spyware planting Business Model: By the Numbers

- The costs involved mainly sum up to building a botnet:
 - “Root” to host the Command & Control channel: **\$15**
 - Stolen CC to register the domain name of the C&C: **\$2**
 - Bot source: **\$2**
 - Making it go through main AV for 1 or 2 days: **\$100**
 - Fresh spam list (i.e. list of active e-mail addresses): **\$8**
 - A fistful of mailers to spam out 100K mails for 6 hours: **\$30**
- *Total Cost: \$157 (once)*
- *Total Profit: $0.4 \times 5000 \times 8 = \$16,000$ (monthly)*
- *Gain: \$15,843 (first month)*
- *Productivity index (Profits/Costs): 100 (first month)*

Phishing Business Model: Phase 1, the Phishing Operation

- *Costs covering the actual Phishing operation:*
 - Phishing Kit: Scam letter + scam page: **\$5**
 - Fresh spam list: **\$8**
 - A fistful of php-mailers to spam out 100K emails for 6 hours: **\$30**
 - Hacked site for hosting scam page for a couple of days: **\$10**
 - Valid cc to register domain name: **\$10**
- *Total costs for the phishing operation: **\$63***

Phishing Business Model: php-mailer

The screenshot shows a web browser window with the address bar displaying 'http://.../mailer.php'. Below the address bar is a toolbar with various navigation and utility icons. The main content area contains a form titled 'eMailer' with the following fields and controls:

- Your Email:** A text input field.
- Your Name:** A text input field.
- Reply-To:** A text input field.
- Attach File:** A text input field with a 'Choose' button next to it.
- Subject:** A text input field.
- Body:** A large text area containing the placeholder text '<enter body>'. To its right is another text area containing the placeholder text '<enter spam list>'. Both text areas have vertical scrollbars.
- Format:** Radio buttons for 'Plain' (selected) and 'HTML'.
- Send eMails:** A button to submit the form.

Phishing Business Model: Direct 2 Inbox

```
virus_peete | is this phpmailer direct to inbox?  
G-Dogg     | whut u mean direct to inbox?  
virus_peete | i mean does it send emails direct to target inbox  
G-Dogg     | where else is it supposed to send emails to? Detroit?  
*          | virus_peete has quit (Quit: Leaving)
```

Phishing Business Model: Big Phish

[Sign Off](#) | [Home](#) | [Location](#)

 [Help](#)

Account Number	Available Balance
	\$171,431.47
	\$171,431.47

Phishing Business Model: Selling the Stolen Credentials

- *Total Cost: \$63*
- *Total Profit: \$200 - \$2,000*
- *Gain: \$137 - \$1,937*
- *Productivity index (Profits/Costs): 3.17 - 31.7*

Phishing Business Model: Cashing the money via drops

- Assuming:
 - typical drops charging 50%
 - a "rip-off rate" of 0.5
 - total stolen balance from \$10,000 to \$100,000
- *Total Cost: \$63*
- *Total Profit: \$2,500 - \$25,000*
- *Productivity index (Profits/Costs): 40 - 400*

Phishing Business Model: Cashing the money via offshore accounts

- Breaks down to 3 steps involving 2 layers of anonymity:
 - Buying e-gold with the stolen account
 - Loading debit cards issued by offshore companies
 - Withdrawing cash
- *Total Cost: \$9,863*
- *Total Profit: \$100,000*
- *Gain: \$90,137*
- *Productivity index (Profits/Costs): 10*

A word on the Mafia

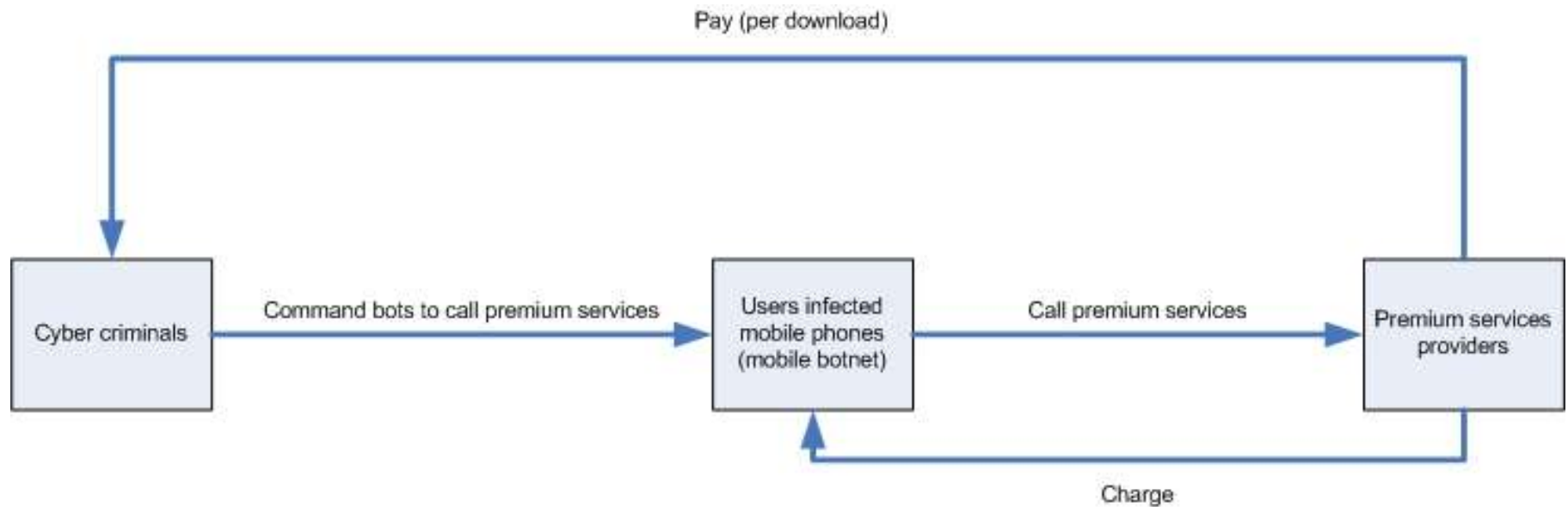
- Stolen credentials buyers?
- Have their own, safe, local drops
- Productivity becomes outstanding (**400+**)
- Comparison with heroin business:
 - 10 kg of opium costs **\$100 - \$1000**
 - Produces 850 gr of pure heroin
 - Each individual dose of 0.085 grams is sold **\$100**

= > Productivity Index: $\$1 \text{ M} / \$1000 = \mathbf{1000}$

Future Threats: Mobile Phones abuse or The Return of Dialers

- Dialers date back from old analogic modem days
- Back then, botnets were not popular, and above all, not meant to generate money
- Today, smartphones make the dangerous encounter Dialers / Botnets possible

Mobile Phones Dialers Business Model: Scheme



Mobile Phones Dialers Business Model: Possible Scenario by the Numbers

- A botnet herder controls a botnet featuring 5,000 zombies, all running on infected mobile phones
- Advertise his botnet on IRC
- The owner of an offshore ringtones company offers **\$500** e-gold to have each bot download 10 ringtones from his company
- Assuming each ringtone costs \$2, this almost instantly generates a raw income of $5,000 \times 2 \times 10 = \mathbf{\$100,000}$ (P.I. = 200)

Conclusion

- Profit and productivity yielded by cyber criminal activities sometimes surpass those of illegal drugs business
- Is combating this possible? (I.e. will “good prevail over evil”?)
- Main point of failure: The lack of congruency among laws relative to digital acts in the world, and questionable law enforcement cooperation
- One axis to combat phishing: user education

Add-on: what Fortinet does against Phishing?

- Fortinet Fortigates: 3 layers of protection

Antispam engine

Antivirus engine

Webfiltering service



Questions?

**(No, I do not drive a
Mercedes 600SL)**

