Denaro sporco in rete

Stefano Chiccarelli – Consultant Engineer
schiccarelli@fortinet.com

FORTINET

Agenda

- Zoologia del Cybercrime
- I profili
- Il Mercato
- La Moneta
- I modelli di business: schemi e numeri

Introduzione

- Le frodi denunciate sono solo la punta di un iceberg
- L'FBI ha denunciato **$67 miliardi di dollari di danni** provenienti da questa attività lo scorso anno. (US)
- NHTCU ha denunciato **£2.45 miliardi di sterline** (UK)
- Le sole frodi legate alle carte di credito fruttano **$400 milioni di dollari** all'anno

FORTINET

Introduzione (II)

- Famosa citazione di Valerie McNiven, US Treasury advisor per il cybercrime:

  “L’anno scorso per la prima volta I proventi dal cybercrime sono stati più elevati dei proventi legati al traffico di droga e si può stimare un cifra attorno ai $105 miliardi di dollari” [1]

[1] Reuters, 2005

C’erano una volta … gli hackers

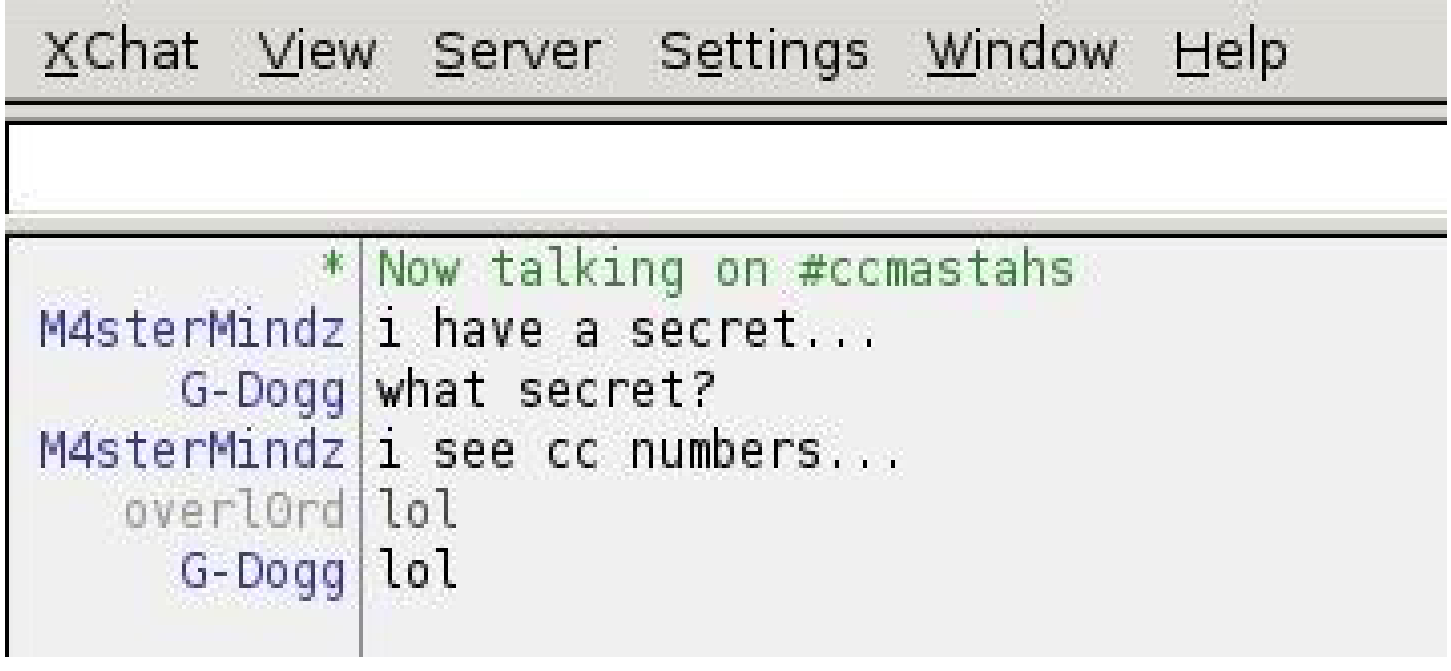
“la parola hacker è diventata una sorta di palla da biliardo, sottoposta a differenti sfumature etiche e interpretazioni politiche. Forse perché molti giornalisti e molti tra gli stessi hacker si divertono a usarla. Ma dove questa palla rimbalzerà la prossima volta, non è dato sapere.” Richard Stallman GNU Project.

- HACKER
- CRACKER
- PHREAKER
- SCRIPT KID
- DEFACER
- BLACK HAT – WHITE HAT
- WAREZ: CRACKER, COURIER, SUPPLIER.
- **CYBER CRIMINAL**

Zoologia del Cybercrime

- Spamming
- Carding
- Phishing
- Spionaggio Industriale

Le carte di credito con il sesto senso



Tipica e-mail di Phishing

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 refrence to update your Barclays Online Banking

details:-

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

Profili dei criminali informatici

- **Coders**
  Gli skillati
- **Kids**
  La forza lavoro
- **Drops**
  I "Muli"
- **Mob**
  I burattinai?

Coders – *Gli Skillati*

- Tra I 20 e 25 anni
- 5+ anni di esperienza nella comunità hackers
- Programmatori professionali o coders auto didatti
- Realizzano Tool o servizi pronti per essere utilizzati dai kid
- I guadagni sono nell'ordine di centinaia di dollari
- Rischi limitati (disclaimers, etc…)
- In questa categoria rientrano gli artisti dello scam.

Kids – *la forza lavoro*

- Tra i 13 e i 20 anni
- Gravitano attorno ai canali IRC per attività di carding
- Comprano e rivendono i mattoni di base per lo scam
- Introiti mensili a due cifre
- Le “fregature” sono molto comuni
- Bassa percentuale di questi “fanno veramente”

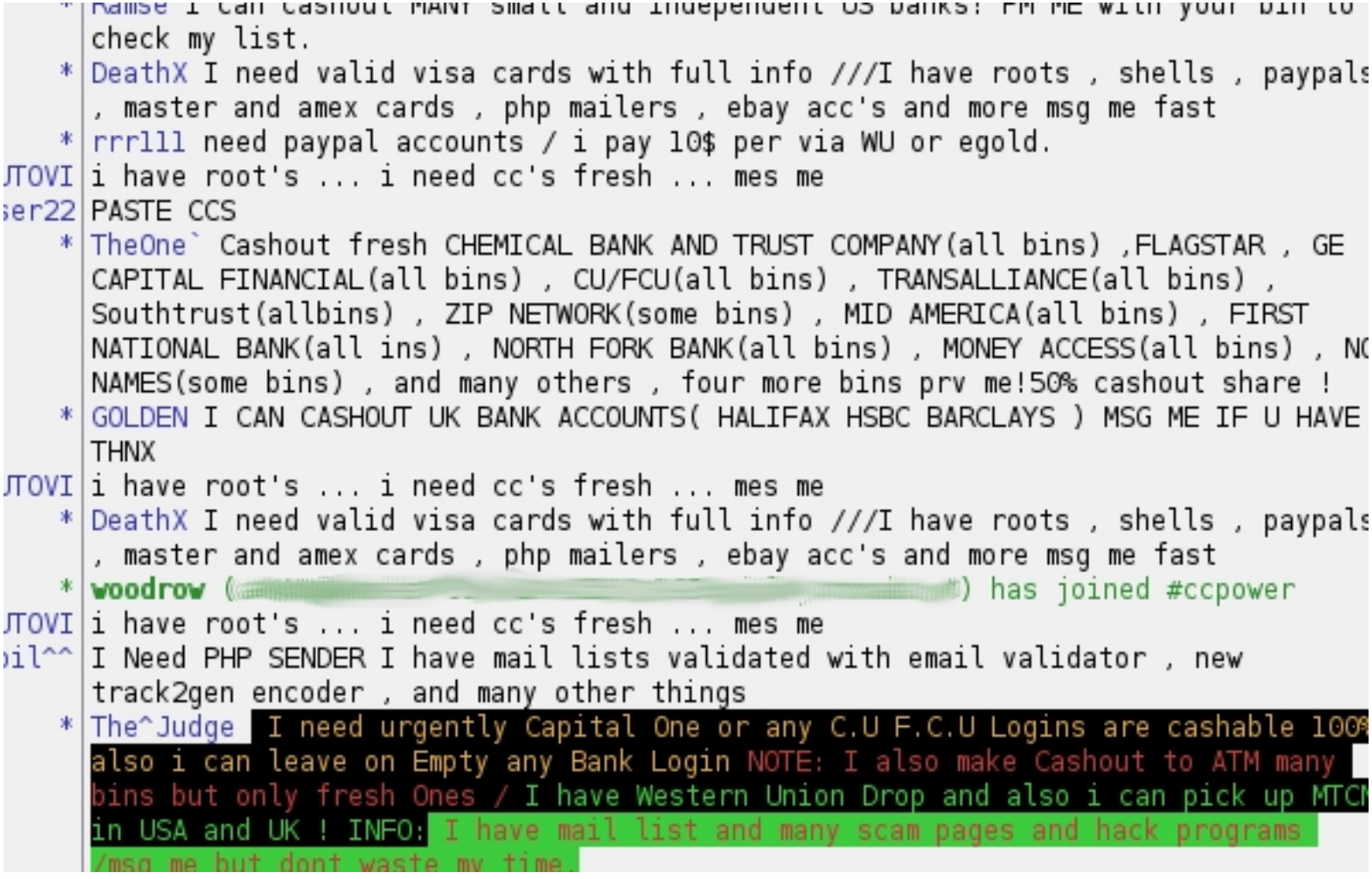
Drops – *the mules*

- Più vecchi dei **Kids**
- Convertono **denaro virtuale** in vero **cash**
- Trasferimenti di denaro presso **il loro conto in banca legale**
- Trattengono il **50%** e rimettono in circolo il resto del denaro
- Importanza di **Reti di fiducia**
- Vivono in paesi con **leggi digitali per nulla rigide**

Mob – *I burattinai?*

- Portano in/out dettagliati sulle reali problematiche sollevate dall'organizzazione criminale
- Si mantengono negli stretti confini della legge.
- Grandi mezzi di investigazione
- Impegno ad agire da infiltrati a lungo termine, possibilmente sul campo
- Uno degli innegabili back end del crimine informatico

Il luogo di scambio: IRC



Le monete

- e-gold
  - Anonimato
  - Irreversibilità
  - Indipendenza
- Denaro cash wired
  - Irreversibile
  - Attraversa I confini istantaneamente
  - Mantiene l'anonimato

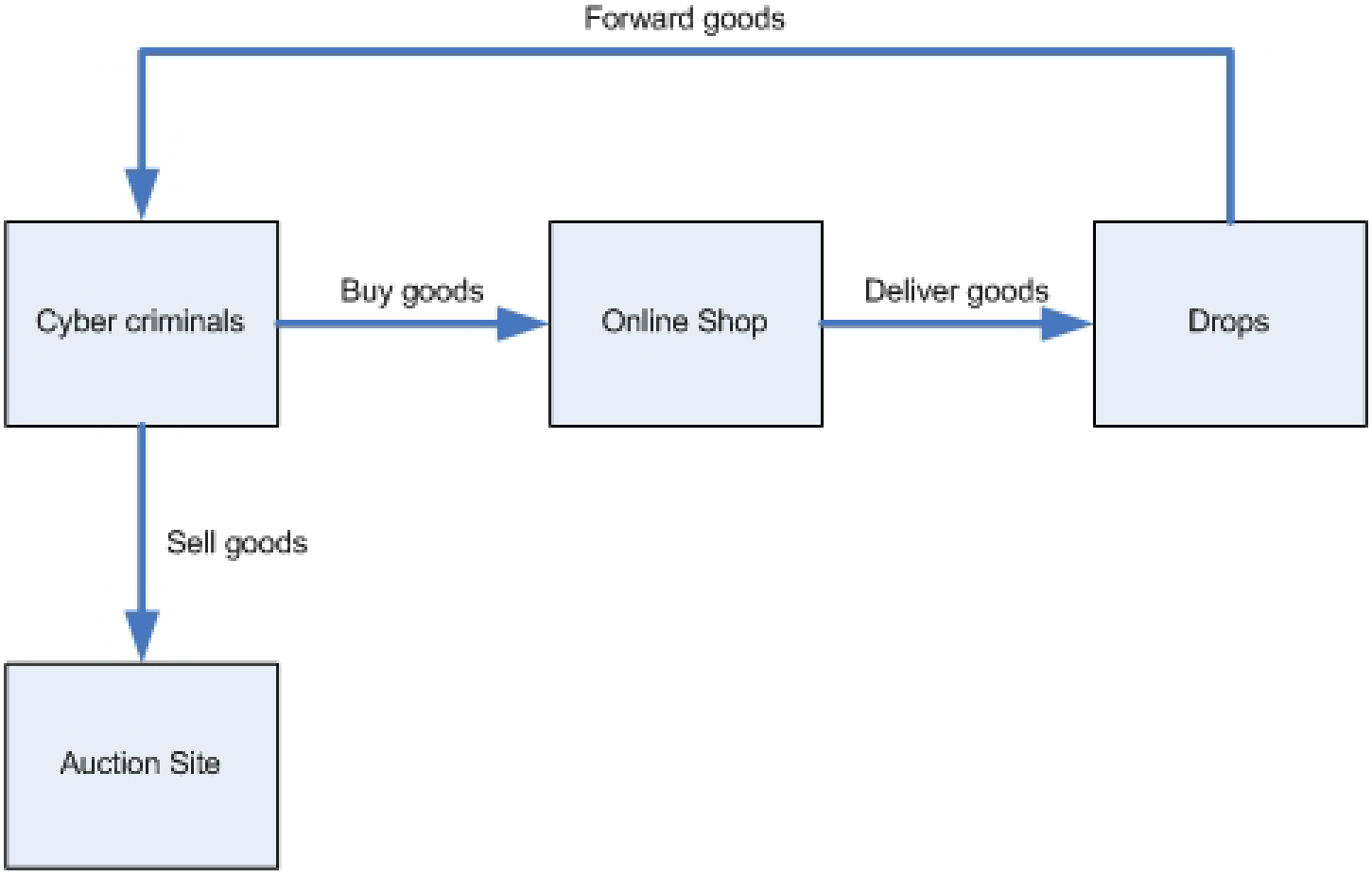
Modello di business del Carding

- Un set “CC Full” costa da $2 a $5 dollari (pagabili con e-gold)
- Circa l’80% delle CCs commercializzate su IRC non sono valide
  $\Rightarrow$ Importanza di reti di Fiducia
- CCs vengono comprate in pacchetti
  $\Rightarrow$ Molto simile a un traffico di droga.

Modello di business del carding : La verità nascosta

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

Schema del modello di business del Carding



Modello di business del carding: i numeri

- Costi
  - ✓ Comprare informazioni relative a 40 CC valide: **$200 dollari**
  - ✓ Pagare 10 drop per inoltrare un pacchetto alla settimana: **$800 dollari**
  - ✓ Drops to cyber criminal packages delivery costs: **$800**
- Profitti
  - ✓ Vendere le merci su eBay: **$16,000 (**$400 per pacchetto)

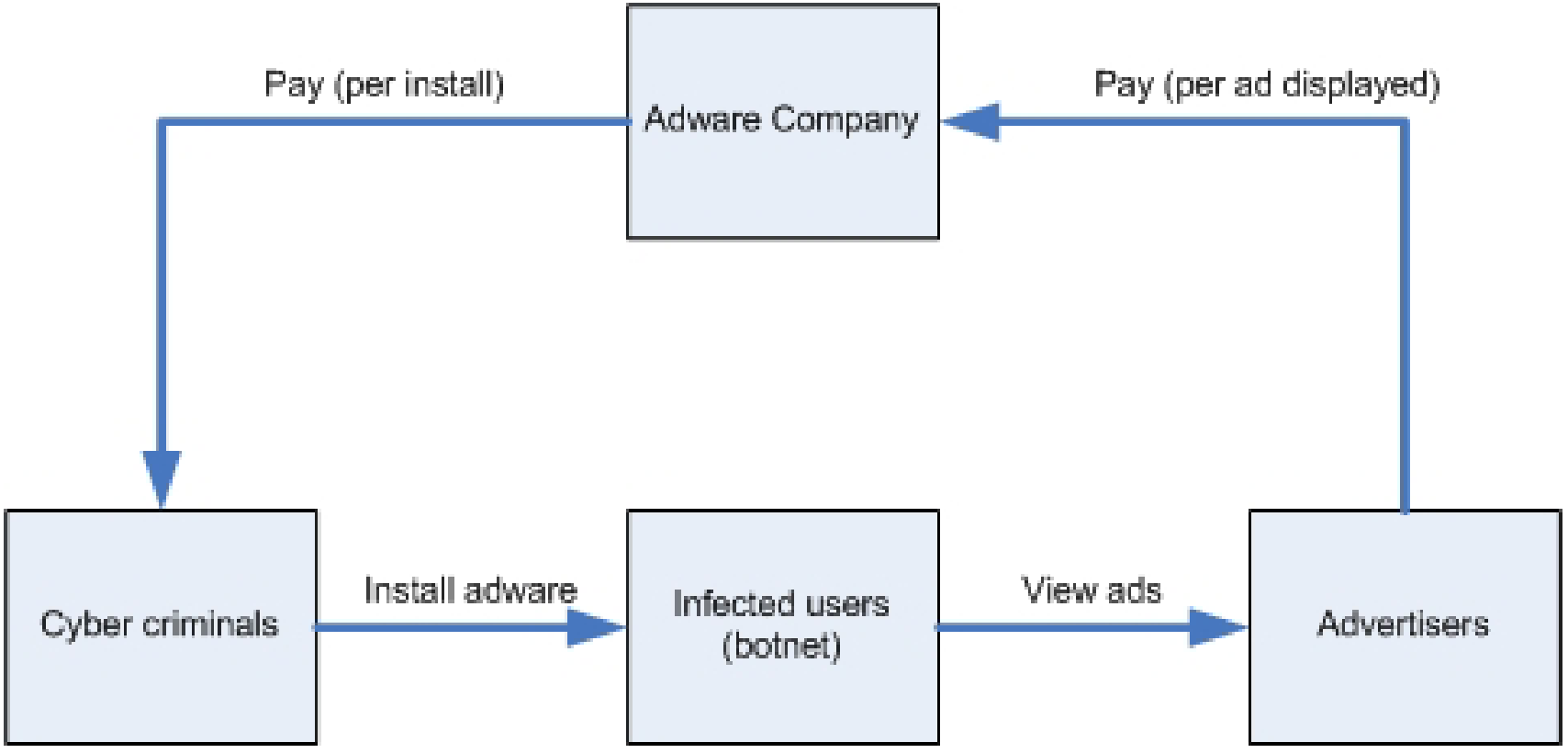
- Costo totale, mensile: **$1,800**
- Profitto totale, mensile: **$16,000**
- Guadagno netto al mese **$14,200**
- Indice di produttività (Profitti/Costi): **8.9**

Modello di business degli installatori di Adware/Spyware

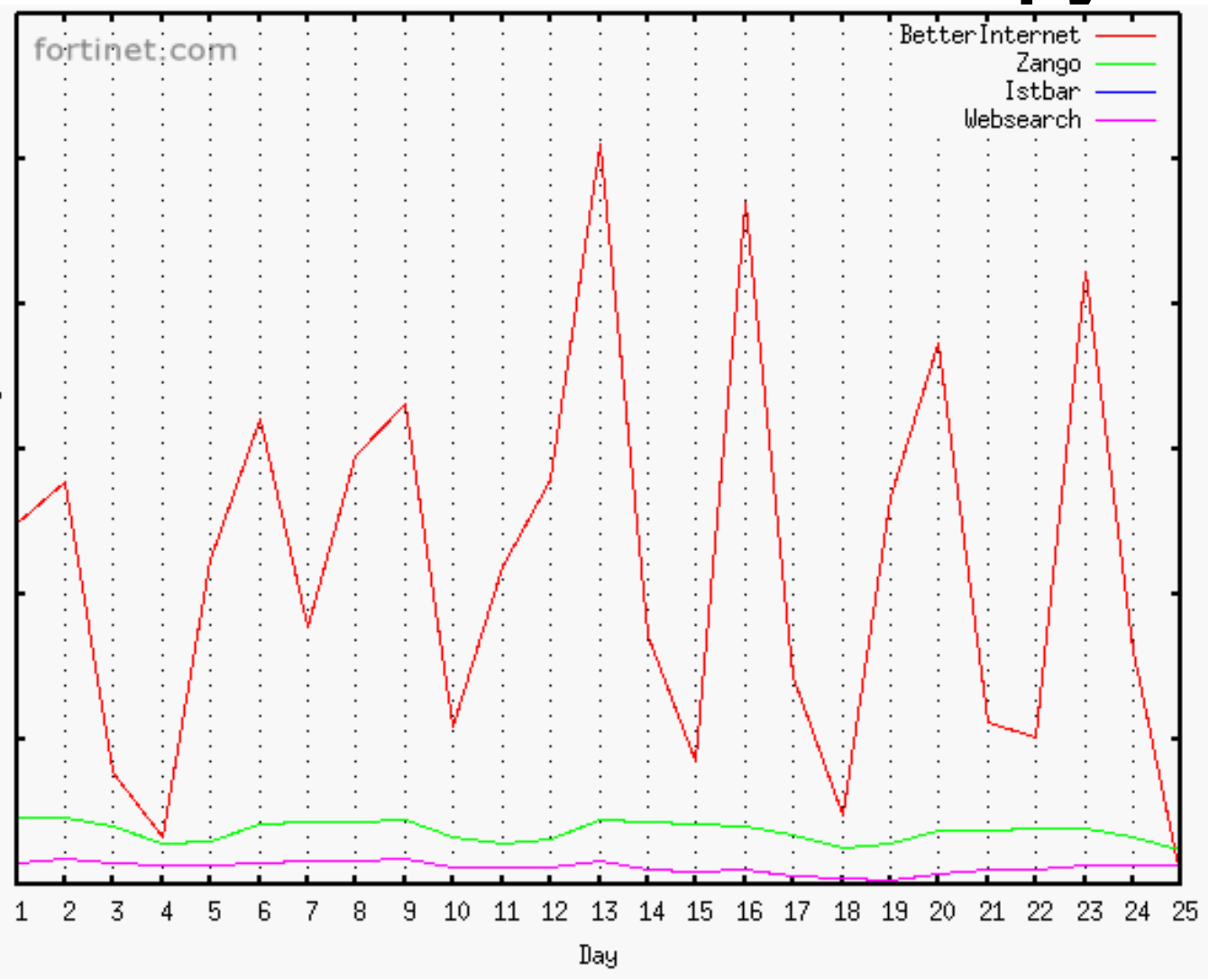
- Modello di business strettamente legato alle aziende di Spyware/Adware:
  - L'azienda di Adware 'A' produce un software che mostra messaggi pubblicitari
  - I pubblicitari pagano l'azienda 'A' per avere visualizzati I loro annunci.
  - L'azienda 'A' paga I suoi partner o affiliati per ogni installazione dello Spyware/Adware sui computer degli utenti finali

FORTINET

Modello di business degli installatori di Adware/Spyware



Modello di business degli installatori di Adware/Spyware



Modello di business degli installatori di Adware/Spyware

- I costi sono simili a quelli necessari per costruire una rete di bot.

  - ✓ “Shell “root” per ospitare il canale di Comando & Controllo: **$15**
  - ✓ CC rubate per registrare il nome del dominio della C&C: **$2**
  - ✓ Codici sorgenti di un Bot : **$2**
  - ✓ Farlo passando attraverso un AV per uno o due giorni : **$100**
  - ✓ Lista nuova per lo spam (i.e. lista di indirizzi mail attivi): **$8**
  - ✓ Un tot di mailer per spammare 100K mails in 6 ore: **$30**

- *Costo totale*: **$157** (una volta)
- *Profitto Totale*: 0.4 x 5000 x 8 = **$16,000** (mensili)
- *Guadagno*: **$15,843** (first month)
- *Indice di produttività (Profitti/Costi)*: **102** (primo mese)

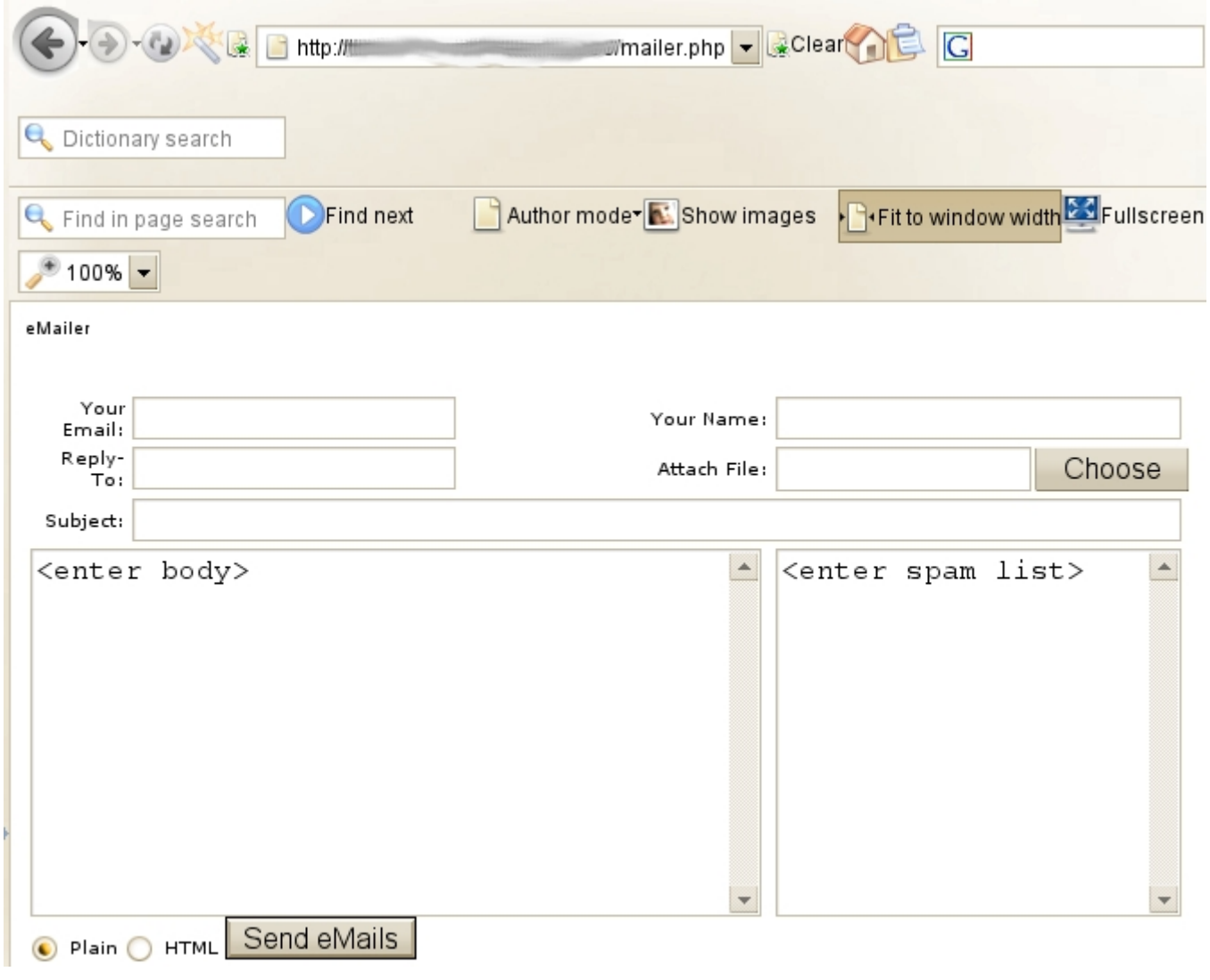
Modello di Business delle operazioni di Phishing

- *Costi per coprire un'operazione di Phishing :*

  - ✓ Kit per il Phishing: lettera di Scam + pagina di scam: **$5**
  - ✓ Lista nuova di spam: **$8**
  - ✓ Un tot di mailers-php per spammare 100K emails in 6 ore: **$30**
  - ✓ Sito "hackerato" per ospitare una pagina di scam per un paio di giorni: **$10**
  - ✓ Cc valide per registrare il nome del dominio: **$10**

- *Costo totale per l'operazione di phishing* : **$63**

Modello di business di Phishing: mailer-php



Modello di business di phishing: Diretamente nell' 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)

FORTINET

Modello di business del Phishing: Un pesce grosso

Modello di Business del Phishing: Vendere le credenziali rubate

- *Costo totale*: **$63**
- *Profitto totale*: **$200 - $2,000**
- *Guadagno*: **$137 - $1,937**
- *Indice di produttività (Costi/profitti)*: **3.17 - 31.7**

Modello di Business del Phishing: Trasformare il denaro in cash tramite i drops

- Assumendo che :
  - ✓ I drops richiedono una commissione che tipicamente si aggira sul 50%
  - ✓ Una possibilità di furto dello 0.5
  - ✓ Quantità totale di soldi rubata da $10,000 a $100,000

- *Costo totale*: **$63**
- *Profitto totale*: **$2,500 - $25,000**
- *Indice di produttività (Profitti/Costi):* **40 - 400**

Modello di Business del Phishing: Trasformare il denaro in cash via conti offshore

- Processo in 3 step che comprende 2 livelli di anonimato:
  - Comprare e-gold con il conto rubato
  - Caricare le debit cards emesse da conti offshore
  - Ritirare il cash
- *Costo totale*: **$9,863**
- *Profitto totale:* **$100,000**
- *Guadagno*: **$90,137**
- *Indice di produttività (Profitti/Costi):* **10**

L’organizzazione criminale

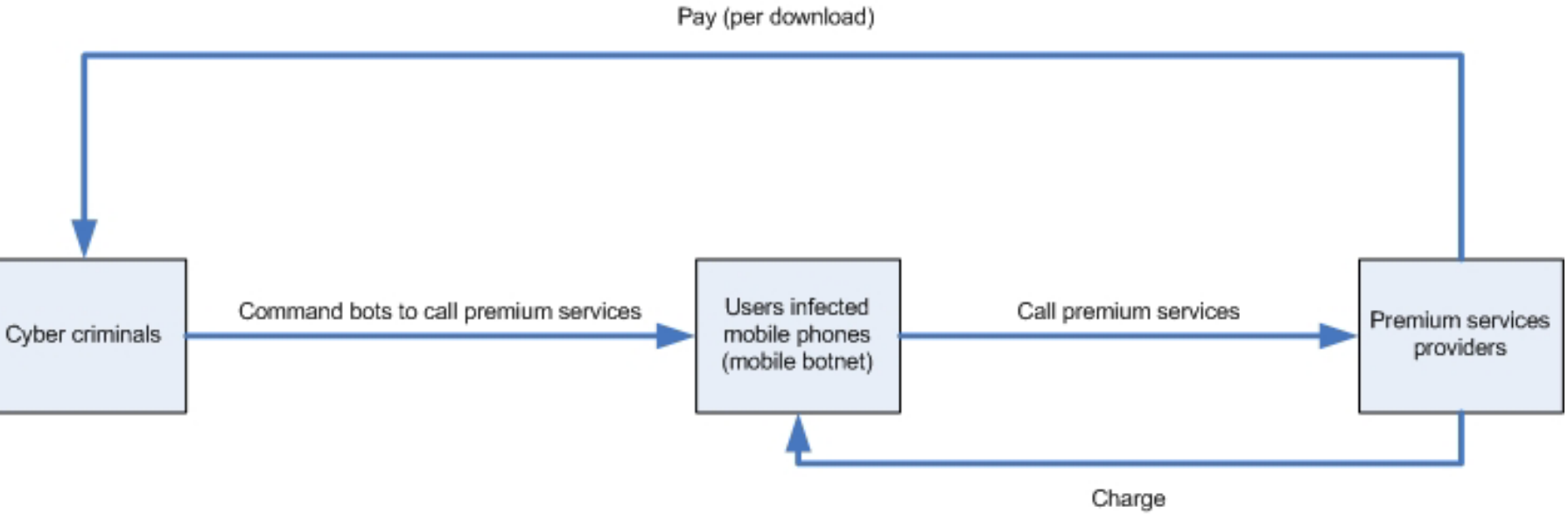
- Compratori di credenziali rubate?
- Hanno I loro drop locali e sicuri
- Indice di produttività fuori dal comune (**400**+)
- Paragone con il business dell’eroina:
  - 10 kg di oppio costano **$100 - $1000**
  - producono 850 gr di eroina pura
  - Ogni dose individuale di 0.085 grammi è venduta a **$100**

  => Indice di produttività: $1 M / $1000 = **1000**

Future minacce: abuso di telefoni cellulari o ritorno dei Dialers

- I Dialers risalgono ai giorni dei vecchi modem analogici
- Allora, le reti bot non erano popolari e soprattutto non si pensava potessero generare guadagno.
- Oggi, gli smartphones rendono possibile il pericoloso incontro Dialers / Botnets

Modello di Business dei Dialers



Modello di business dei dialers su telefoni cellulari: un possibile scenario per numeri

- Una persona che controlla I botnet dispone di una rete di 5,000 zombies, che girano tutti su telefoni portatili infetti.
- Pubblica la sua rete di bot su IRC
- Il proprietario di un'azienda offshore di suonerie telefoniche offre **$500 dollari** e-gold per effettuare il download di 10 suonerie su ogni bot
- Assumendo che ogni suoneria costi $2 questo genera quasi istantaneamente un guadagno netto di 5,000 x 2 x 10 = **$100,000** (P.I. = 200)

Conclusioni

- I Profitti e la produttività che provengono dalle attività dei cyber criminali a volte sorpassano quelli del traffico illegale di droga.
- E' possibile combatterlo?? (Sarà il bene o il male a prevalere?)
- Debolezza principale: la mancanza di coerenza tra le leggi internazionali relative ai crimini informatici e una discutibile collaborazione nel rafforzare queste leggi
- Un modo per combattere il phishing: l'educazione dell'utente.

Inoltre:
Che cosa fa Fortinet contro il Phishing?

- Fortinet Fortigates: 3 livelli di protezione:
  - Motore Antispam
  - Motore Antivirus
  - Servizio Webfiltering

- Fortinet FortiClient :
  - Antivirus Mobile
  - Firewall Mobile
  - Protezione della rubrica telefonica

FORTINET

Grazie!

For more information please visit
http://www.fortinet.com