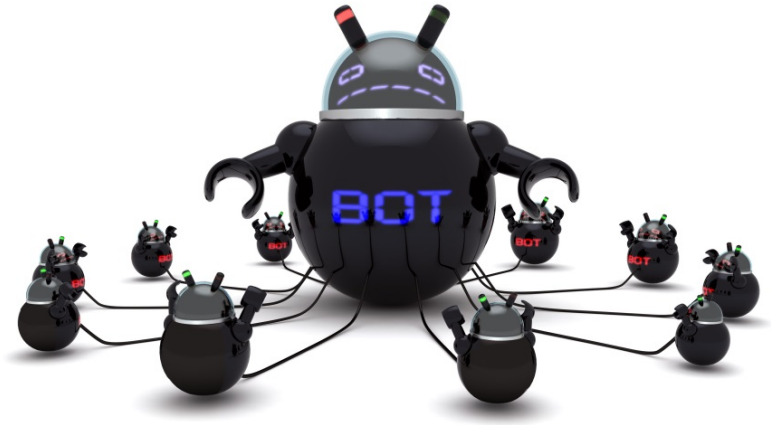
AALBORG UNIVERSITY

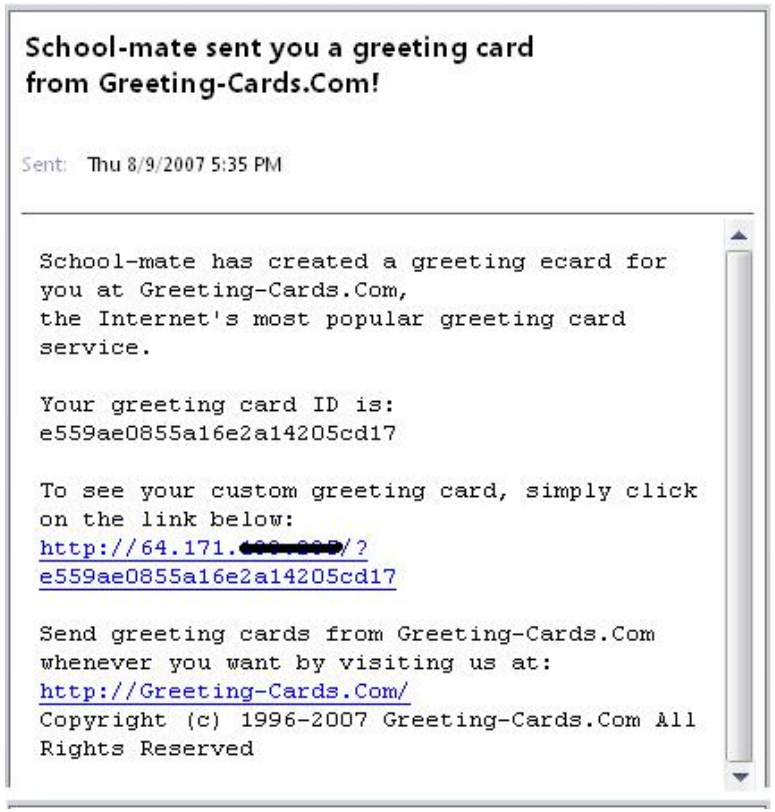
Botnets – Organiseret kriminalitet på nettet

Jens Myrup Pedersen
Lektor, Institut for Elektroniske Systemer
Aalborg Universitet (Aalborg)
jens@es.aau.dk



- Sikkerhed er mange ting – nogle eksempler
- Forskellige motivationer og grupperinger
- Botnets/Trojans: Forskellige typer af angreb
- Forretningsmodeller som drivere
- Et kig ind i fremtiden…

Cyberkriminalitet har mange ansigter



School-mate sent you a greeting card from Greeting-Cards.Com!

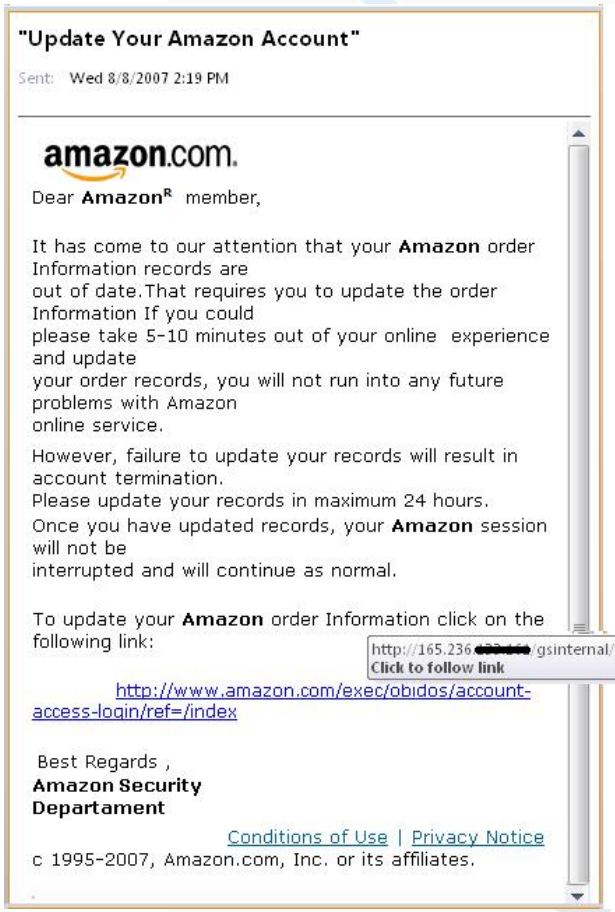
Sent: Thu 8/9/2007 5:35 PM

School-mate has created a greeting ecard for you at Greeting-Cards.Com, the Internet's most popular greeting card service.

Your greeting card ID is: e559ae0855a16e2a14205cd17

To see your custom greeting card, simply click on the link below:
http://64.171.[redacted]/?e559ae0855a16e2a14205cd17

Send greeting cards from Greeting-Cards.Com whenever you want by visiting us at:
http://Greeting-Cards.Com/
Copyright (c) 1996-2007 Greeting-Cards.Com All Rights Reserved



"Update Your Amazon Account"

Sent: Wed 8/8/2007 2:19 PM

amazon.com.

Dear **Amazon**[R] member,

It has come to our attention that your **Amazon** order Information records are out of date.That requires you to update the order Information If you could please take 5-10 minutes out of your online experience and update your order records, you will not run into any future problems with Amazon online service.

However, failure to update your records will result in account termination.
Please update your records in maximum 24 hours.
Once you have updated records, your **Amazon** session will not be interrupted and will continue as normal.

To update your **Amazon** order Information click on the following link:

http://165.236.[redacted]/gsinternal/ama.htm
Click to follow link

http://www.amazon.com/exec/obidos/account-access-login/ref=/index

Best Regards ,
Amazon Security Departament

Conditions of Use | Privacy Notice
c 1995-2007, Amazon.com, Inc. or its affiliates.

Cyberkriminalitet har mange ansigter

Cyberkriminalitet har mange ansigter

Cyberkriminalitet har mange ansigter

Cyberkriminalitet har mange ansigter...

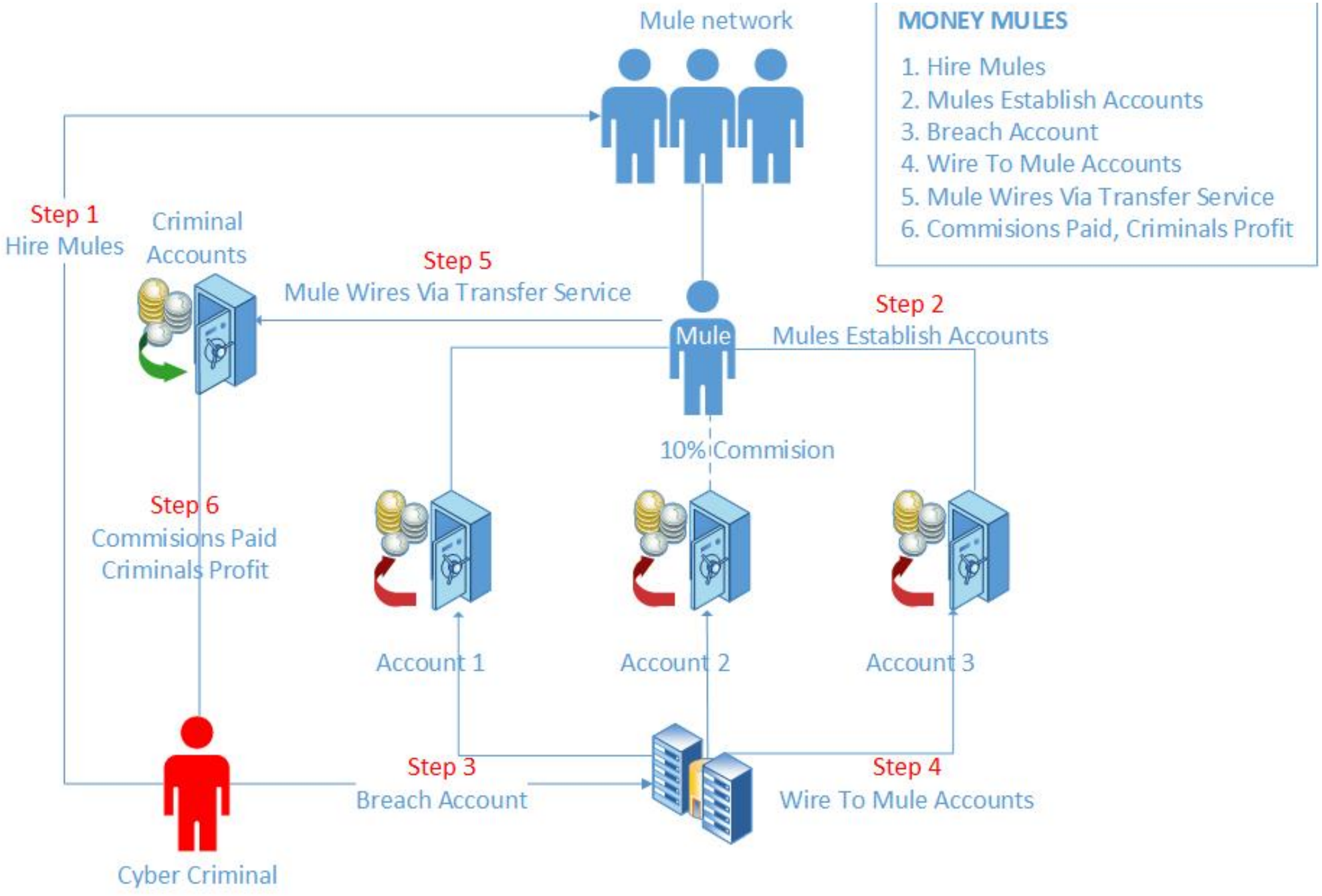
Botnets – Organiseret kriminalitet på nettet

- 3 Eksempler på typiske angreb på Internettet
- Botnets – hvad er de, og hvordan er de opbygget?
- Hvad er forretningen bag?
- Hvordan kan botnets bekæmpes
- Vores forskning – hvad arbejder vi med
- Spørgsmål og (måske) svar

Eks. 1: Stjålne forretningshemmeligheder

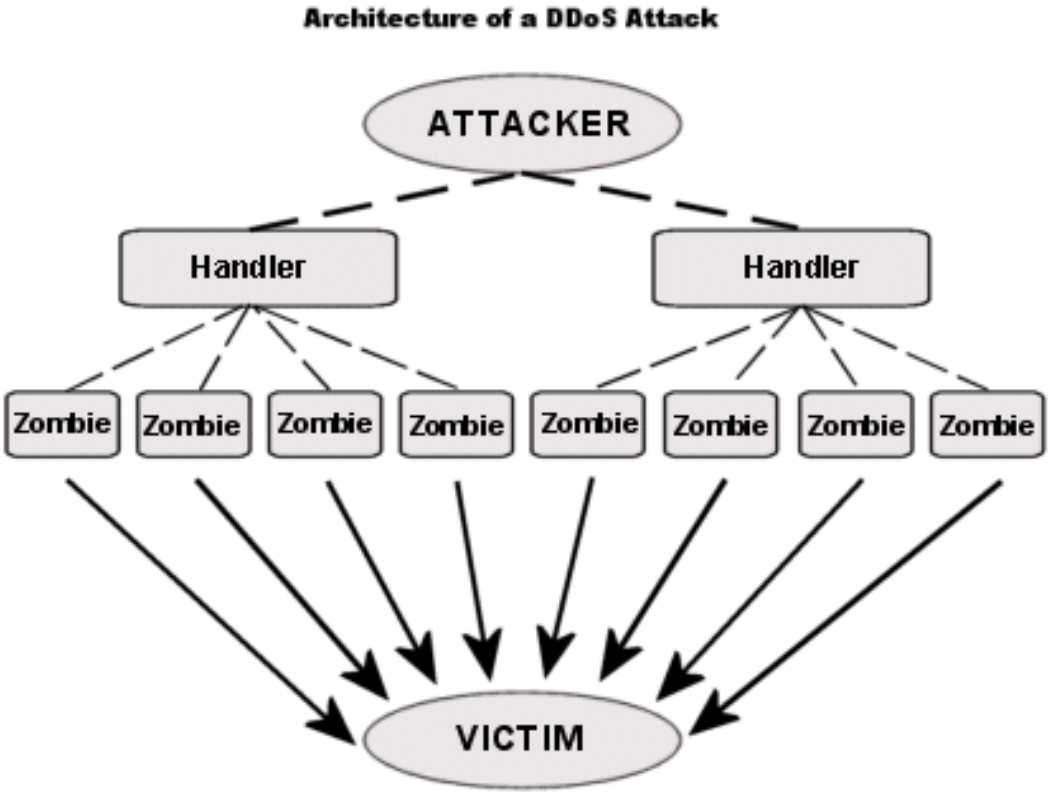
- De gode eksempler er der, men de kommer sjældent frem i offentligheden.

Eks. 2: Steffen fra Thyborøn

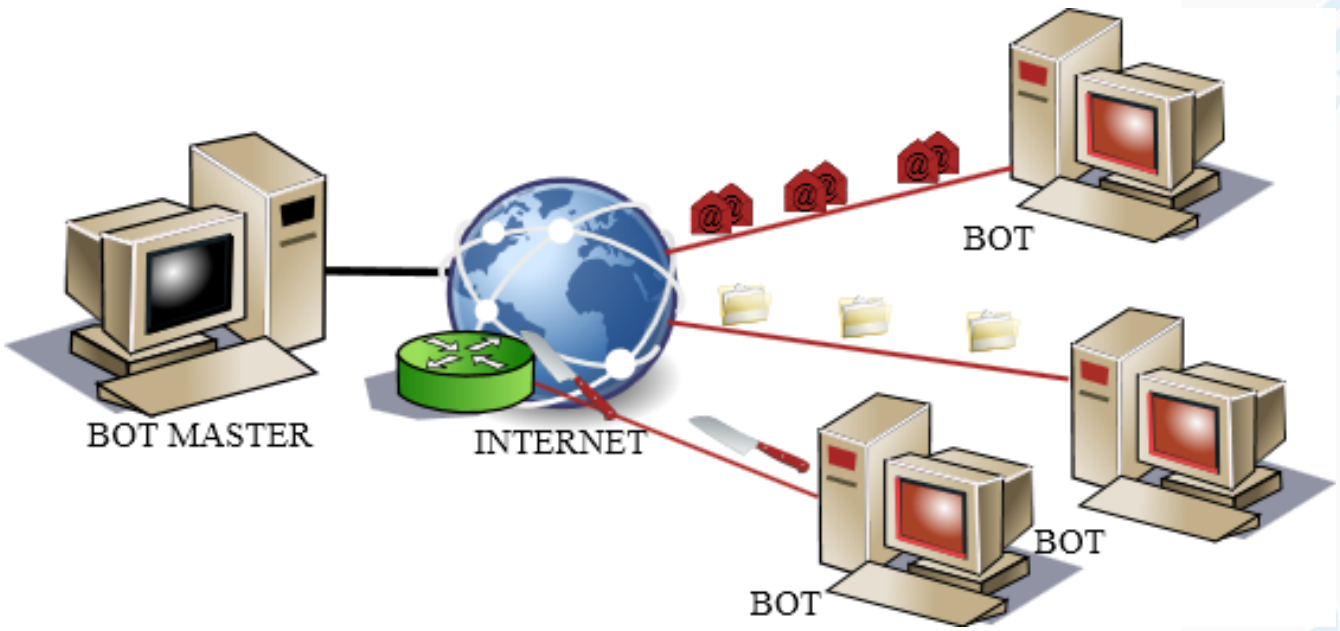

Mule network
MONEY MULES
1. Hire Mules
2. Mules Establish Accounts
3. Breach Account
4. Wire To Mule Accounts
5. Mule Wires Via Transfer Service
6. Commisions Paid, Criminals Profit
Step 1
Hire Mules
Criminal
Accounts
Step 5
Mule Wires Via Transfer Service
Mule
Step 2
Mules Establish Accounts
10% Commision
Step 6
Commisions Paid
Criminals Profit
Account 1
Account 2
Account 3
Step 3
Breach Account
Step 4
Wire To Mule Accounts
Cyber Criminal

Eks. 3: DDoS angreb på ...

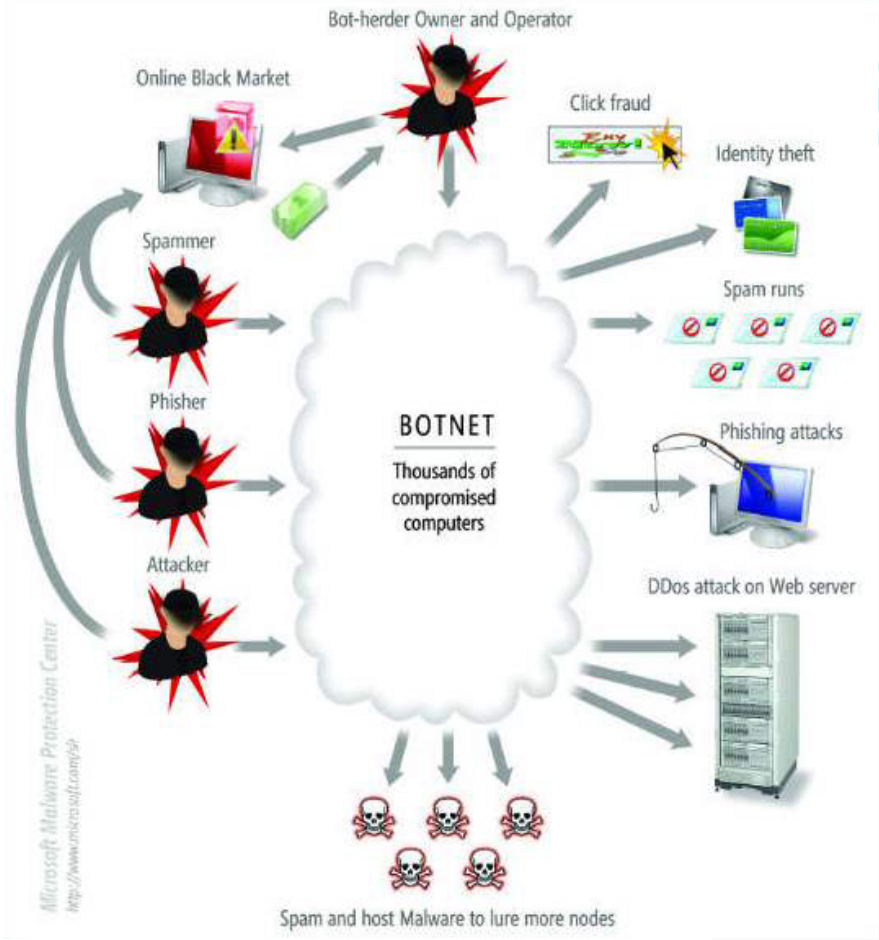
Eks. 3: DDoS angreb på Nem ID

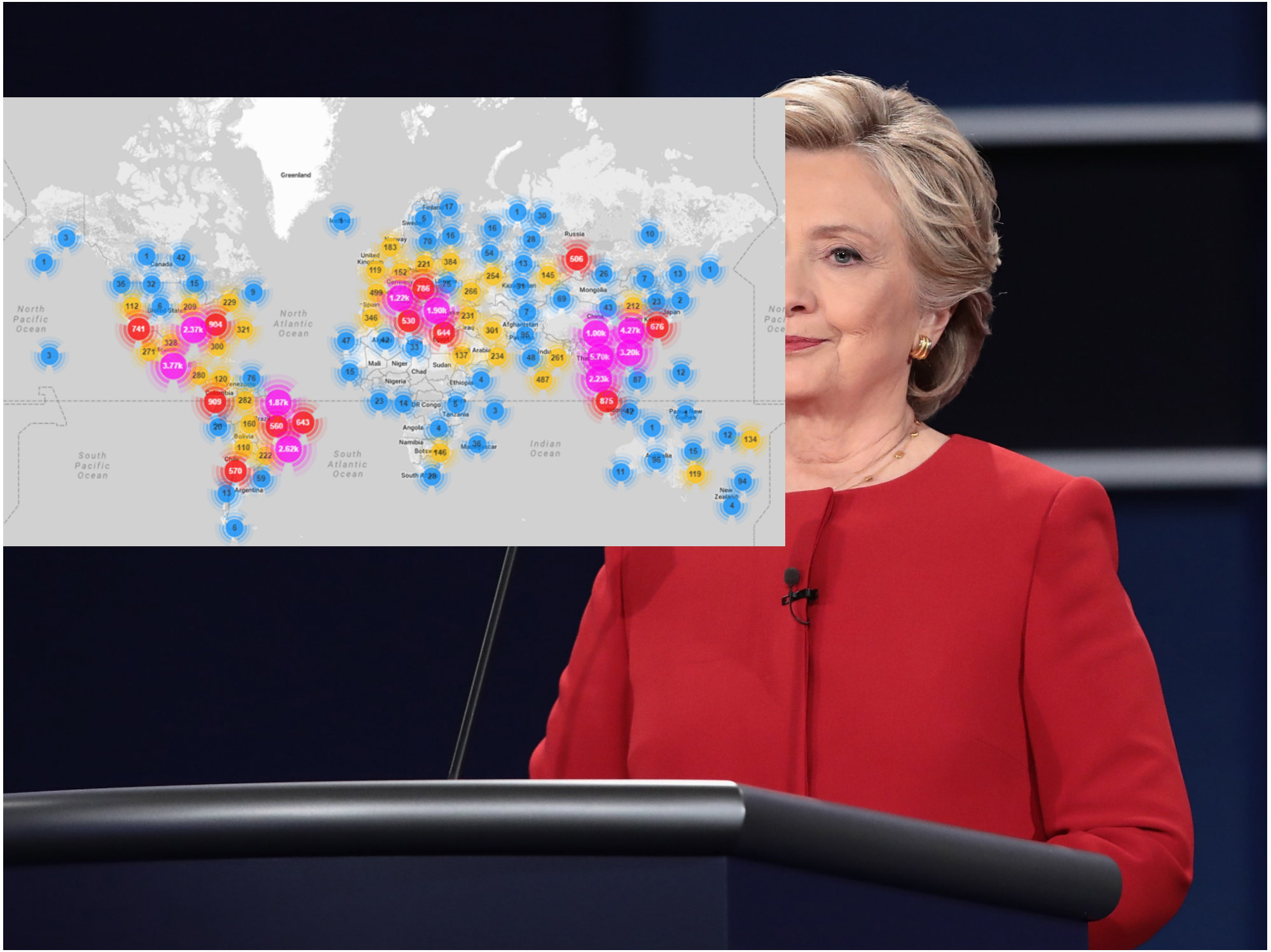


Hvad er så et Botnet for noget?



Hvad er et Botnet?




Greenland
North Pacific Ocean
North Atlantic Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Russia
Mongolia
Canada
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Angola
Namibia
Tanzania
Argentina
Bolivia
Venezuela
Colombia
Afghanistan
Japan
New Zealand

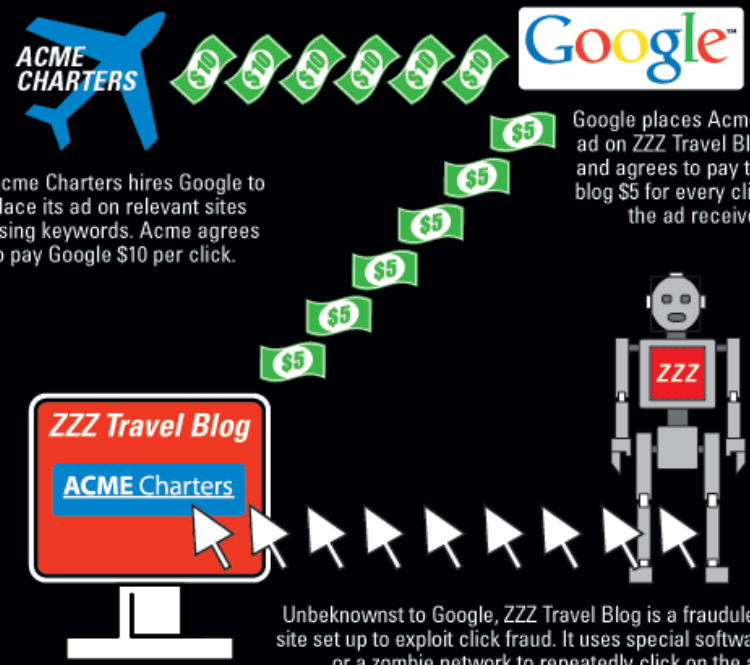
2 KINDS OF CLICK FRAUD

COMPETITIVE CLICK FRAUD

Acme Charters agrees to pay Google $10 each time a Web surfer clicks on its ad on a Google search page.

XYZ Charters, a rival, clicks repeatedly on Acme's ad, costing Acme $10 per click.

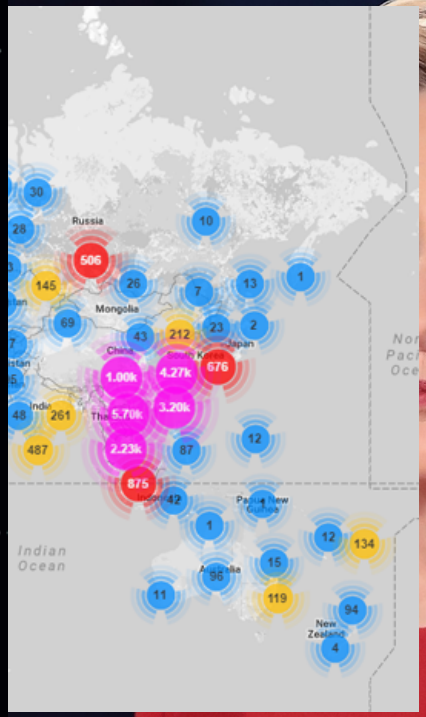
AFFILIATE CLICK FRAUD



Acme Charters hires Google to place its ad on relevant sites using keywords. Acme agrees to pay Google $10 per click.

Google places Acme's ad on ZZZ Travel Blog and agrees to pay the blog $5 for every click the ad receives.

Unbeknownst to Google, ZZZ Travel Blog is a fraudulent site set up to exploit click fraud. It uses special software or a zombie network to repeatedly click on the ad. ZZZ Travel Blog gets rich; Acme Charters goes broke.



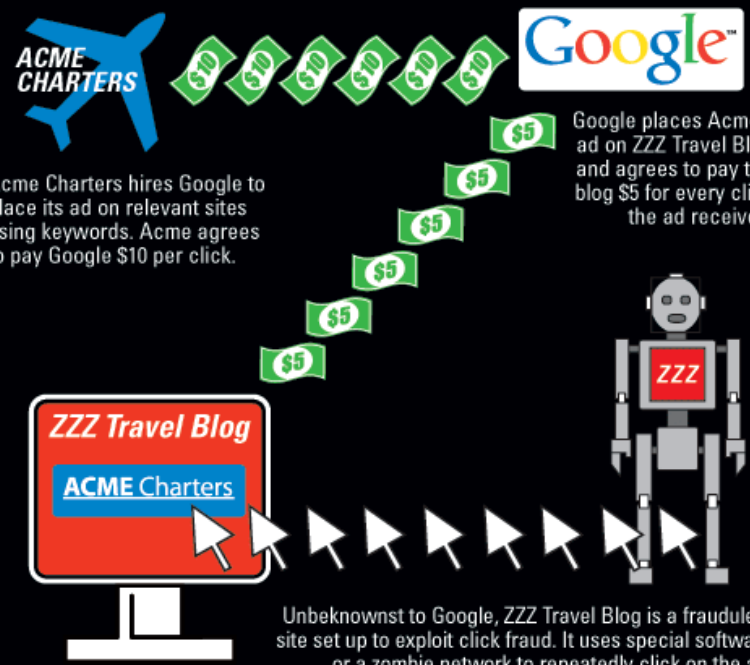
2 KINDS OF CLICK FRAUD

COMPETITIVE CLICK FRAUD

Acme Charters agrees to pay Google $10 each time a Web surfer clicks on its ad on a Google search page.

XYZ Charters, a rival, clicks repeatedly on Acme's ad, costing Acme $10 per click.

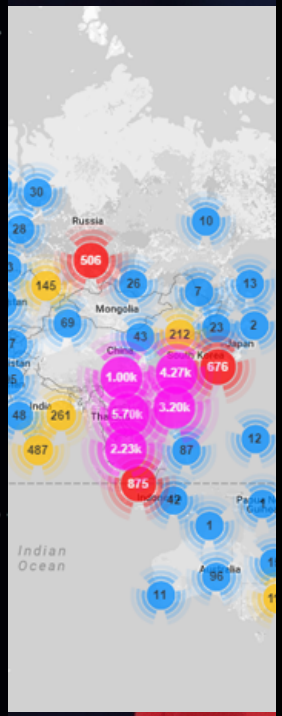
AFFILIATE CLICK FRAUD



Acme Charters hires Google to place its ad on relevant sites using keywords. Acme agrees to pay Google $10 per click.

Google places Acme's ad on ZZZ Travel Blog and agrees to pay the blog $5 for every click the ad receives.

Unbeknownst to Google, ZZZ Travel Blog is a fraudulent site set up to exploit click fraud. It uses special software or a zombie network to repeatedly click on the ad. ZZZ Travel Blog gets rich; Acme Charters goes broke.



IMPACT OF ZEROACCESS BOTNET

One of the largest P2P botnets ever known

X 1.9 million

ZeroAccess carries out two revenue generation activities

BITCOIN MINING

CLICK FRAUD

*Botnet generates...

1.9M x

Earns US$ 2,165/day

Click fraud generates 488 TB network traffic/day

Per annum earnings: Tens of millions US$!!!

Uses

3,458 MWh/day

=

Power for > 111,000 homes/day

Cost of electricity > US$ 560,887/day

SEP2013

Sources

http://www.eia.gov/tools/faqs/faq.cfm?id=97&t=3
http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_6_a
http://www.symantec.com/connect/symantec-blogs/sr

* Based on a test PC with Pentium D 945 3.4 GHz CPU running 24 hours a day.
Unit price of electricity of $0.1622 KWh.
Annual US average home electricity usage of 11280 KWh.

Symantec.

@threatintel | www.symantec.com


2 KINDS OF CLICK FRAUD
COMPETI
ACME CHART
Acme Charte
pay Google
Web surfer
on a Google
AFFILIATE
ACME CHART
Acme Charte
place its ad
using keywo
to pay Googl
CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a performance list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; After the time specified in this window, the cost of data recovery will be increased 2 times.
In a month, the private key will be automatically deleted from the secret server. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 600 USD / 600 EUR / similar amount in another currency.
Click "Next" to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Price will be increased by 2 times
06 / 03 / 2014
3:43:04
Time left
86:54:22
Next =>
ZZZ
Unbeknownst to Google, ZZZ Travel Blog is a fraudulent site set up to exploit click fraud. It uses special software or a zombie network to repeatedly click on the ad. ZZZ Travel Blog gets rich; Acme Charters goes broke.
IMPACT OF ZEROACCESS BOTNET
e largest P2P
ever known
million
s out two
n activities
CLICK FRAUD
rates...
ick fraud generates
488 TB network
traffic/day
er annum earnings:
ns of millions US$!!!
Power for > 111,000
homes/day
Cost of electricity > US$ 560,887/day
Sources
http://www.eia.gov/tools/faqs/faq.cfm?id=97&t=3
http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_6_a
http://www.symantec.com/connect/symantec-blogs/sr
SEP2013
* Based on a test PC with Pentium D 945 3.4 GHz CPU running 24 hours a day.
Unit price of electricity of $0.1622 KWh.
Annual US average home electricity usage of 11280 KWh.
Symantec.
@threatintel | www.symantec.com

2 KINDS OF CLICK FRAUD

COMPETI

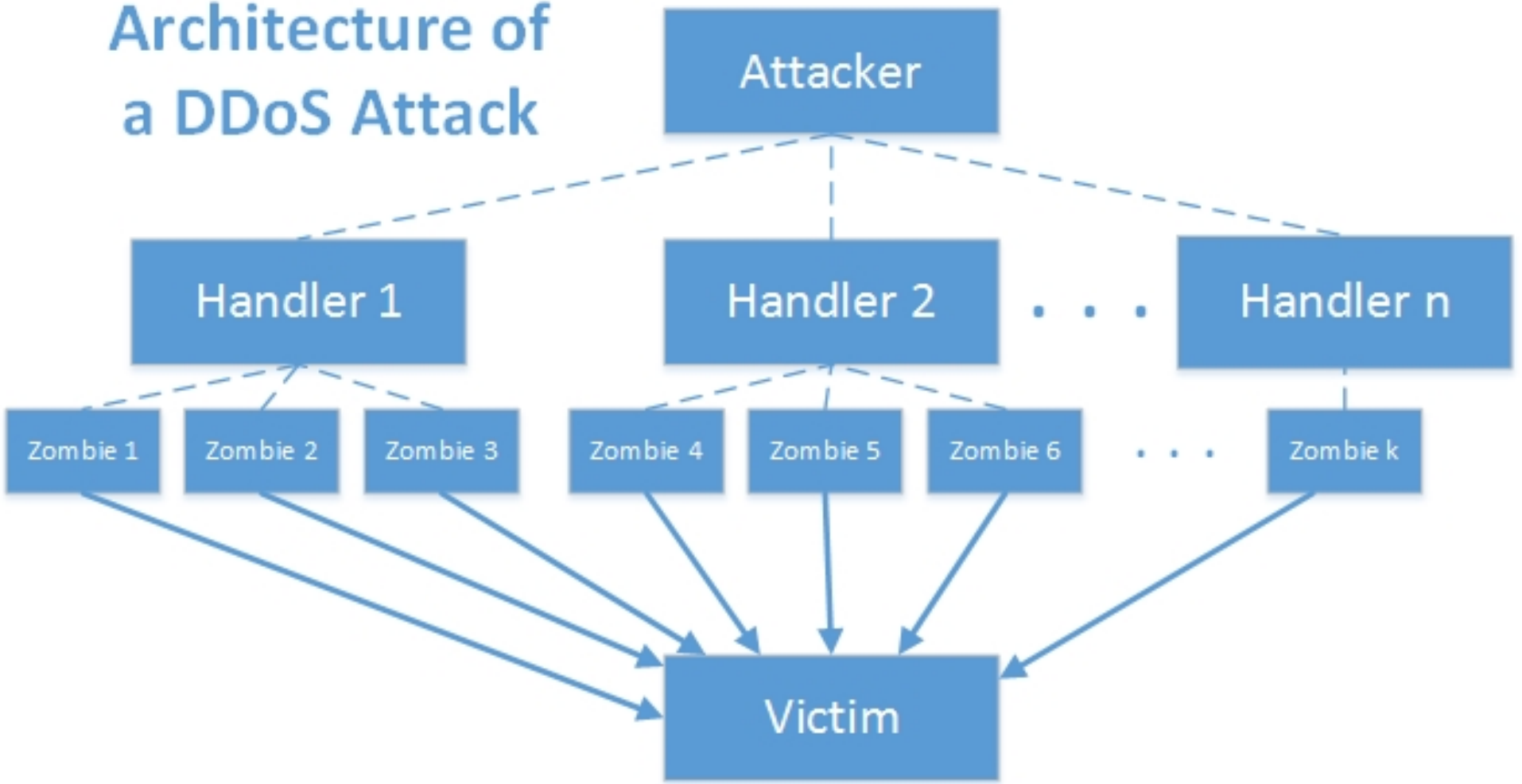
CryptoLocker

Your personal files are encrypted!

IMPACT OF ZEROACCESS BOTNET

e largest P2P

Architecture of a DDoS Attack



Unbeknownst to Google, ZZZ Travel Blog is a fraudulent site set up to exploit click fraud. It uses special software or a zombie network to repeatedly click on the ad. ZZZ Travel Blog gets rich; Acme Charters goes broke.

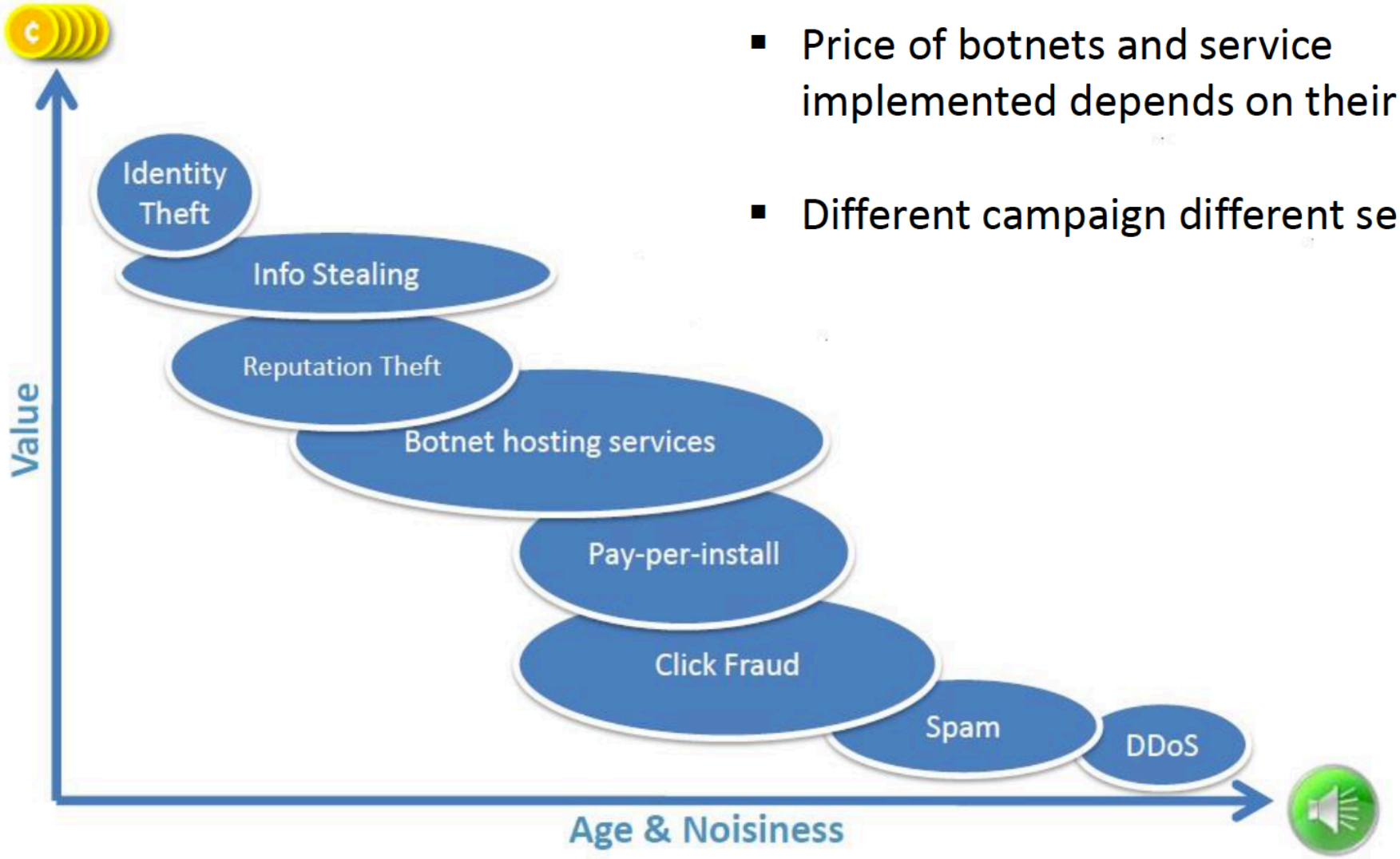
SEP2013

Sources
http://www.eia.gov/tools/faqs/faq.cfm?id=97&t=3
http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_6_a
http://www.symantec.com/connect/symantec-blogs/sr

* Based on a test PC with Pentium D 945 3.4 GHz CPU running 24 hours a day.
Unit price of electricity of $0.1622 KWh.
Annual US average home electricity usage of 11280 KWh.

Symantec.

@threatintel | www.symantec.com



- Price of botnets and service implemented depends on their age.
- Different campaign different service

http://www.damballa.com/downloads/r_pubs/DoD-Cyber-crime_Gunter-Ollmann_How-Criminals-Profit.pdf

Eksempler på brug af botnet

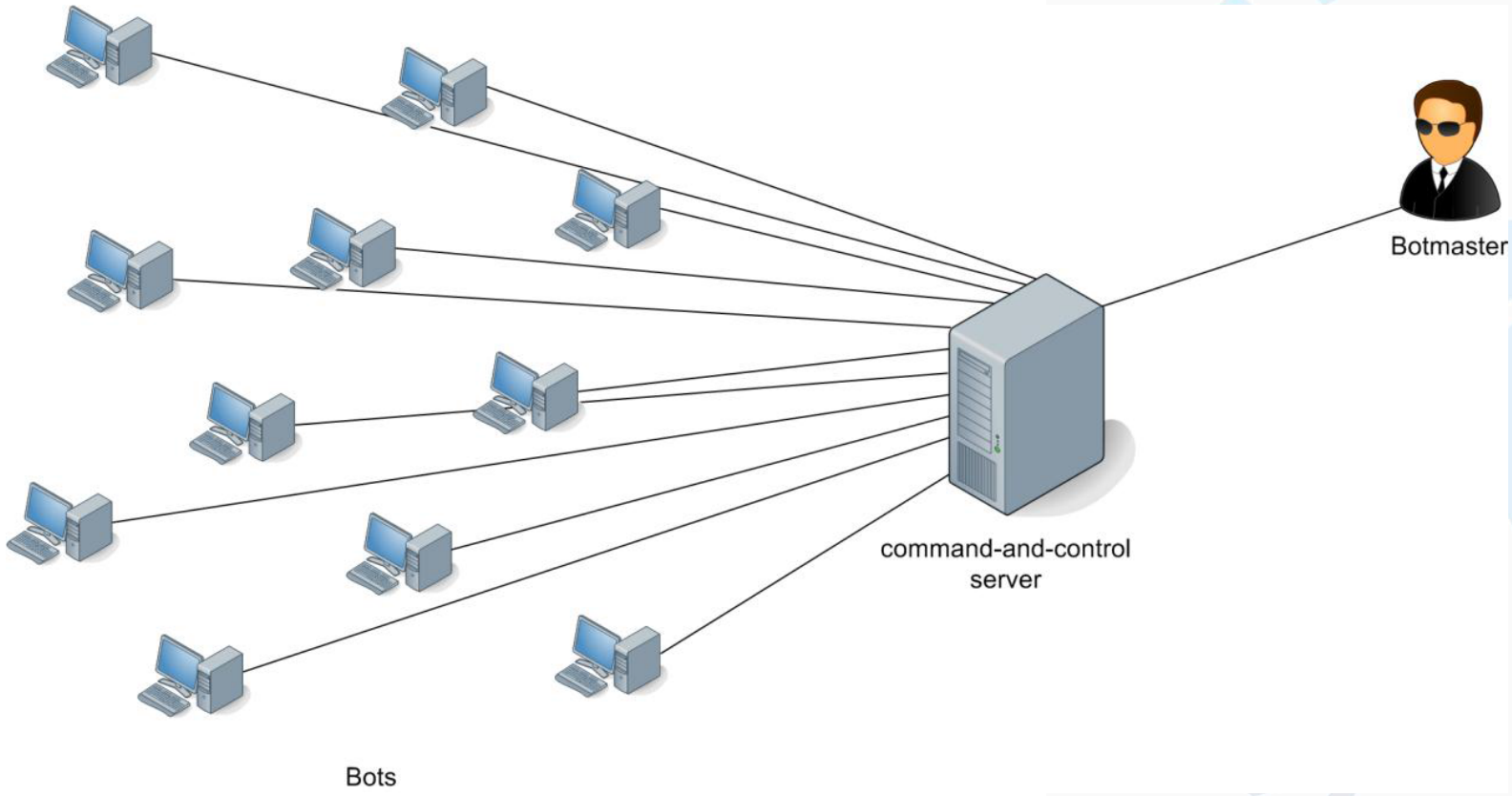
- Botnet Ad Fraud generer en indtjening på $7.2 milliarder i 2016 (ANA and White Ops).
- Grum blev primært brugt til SPAM. Da det peakede I 2010 kunne det sende 39,6 milliarder beskeder om dagen.
- Lizardstresser er et IoT botnet, det bl.a. deltog I et 400GBPS angreb (Juni 2016). Det bestod især af webcams og blev brugt til angreb på Brasilianske banker og regeringskontorer.
- ZeroAccess kontrollerede op til 1,9 mio. Computere. Det blev især brugt til click fraud og til at generere bitcoins, og havde et energiforbrug svarende til 111.000 husholdninger.
- Zeus er kendt for at være ekstremt svært at detektere og blev brugt til at kontrollere 3-4 mio. Computere i USA. Især brugt til at stjæle bankinformationer, men GameOver Zeus havde også cryptolocker funktionalitet. Meget levedygtigt!!

Pay per install

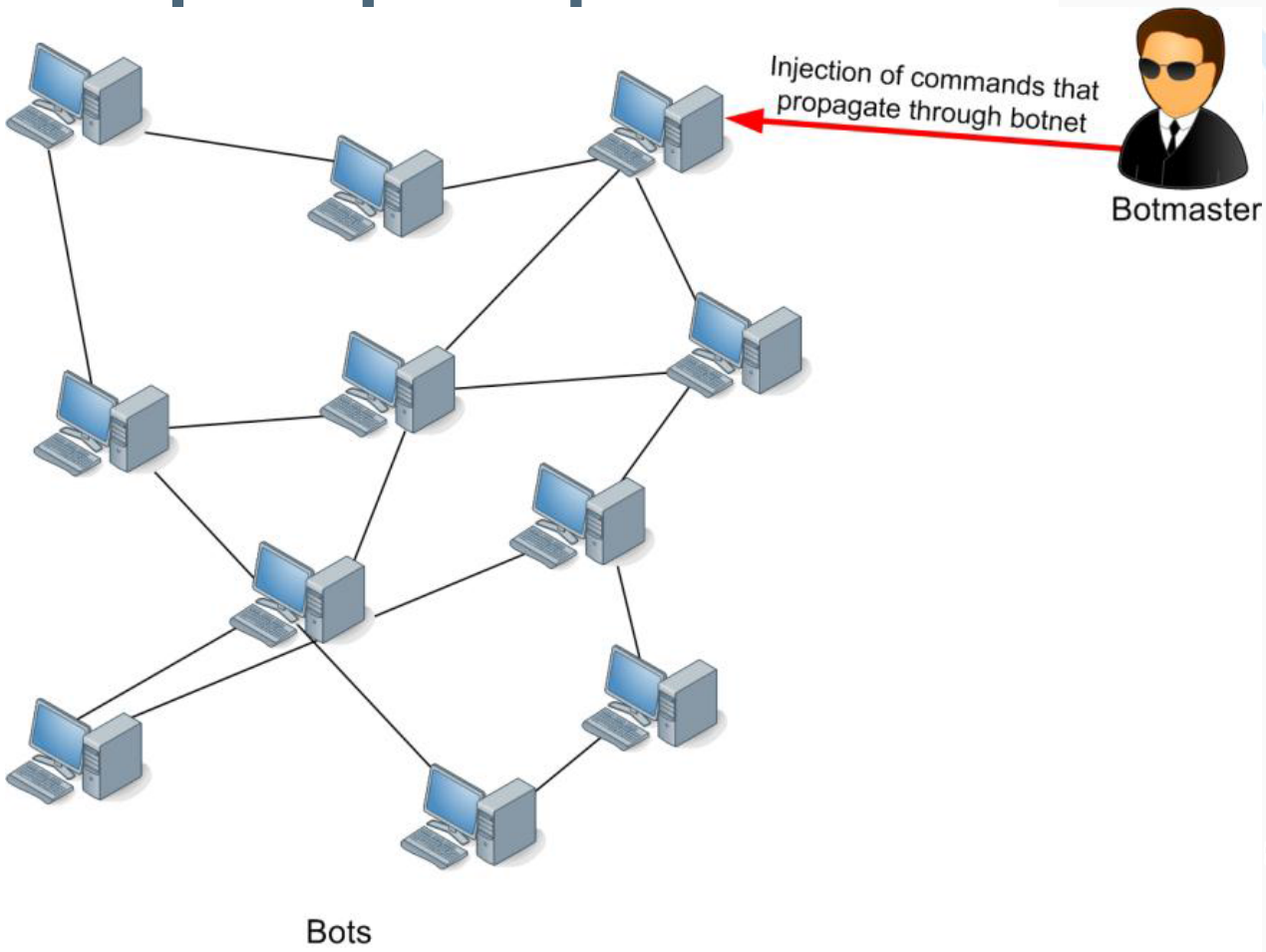
INSTALL RATES			
Monthly Installs	**Tier 1**	**Tier 2**	**Tier 3**
1 to 3,000	$0.75	$0.40	$0.10
3,001 to 10,000	$1.00	$0.53	$0.15
10,001 to 20,000	$1.13	$0.59	$0.18
20,001 to 40,000	$1.21	$0.63	$0.19
40,001 to 80,000	$1.29	$0.67	$0.21
80,001 to 160,000	$1.37	$0.71	$0.22
over 160,000	$1.45	$0.75	$0.24

Tier	Countries
1	United States, United Kingdom
2	Canada, France, Germany, Netherlands
3	Australia, Austria, Belgium, Denmark, Finland, Ireland, Italy, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland

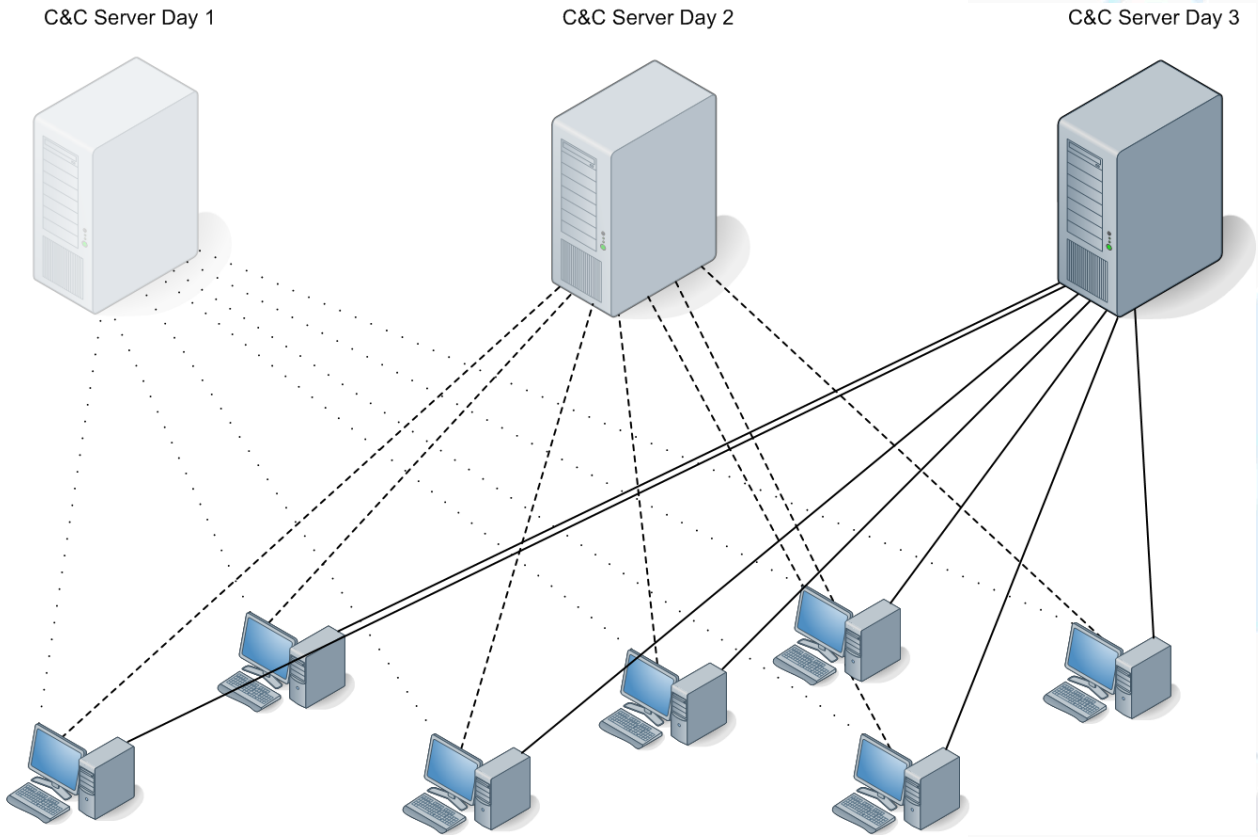
Eksempel - centraliseret



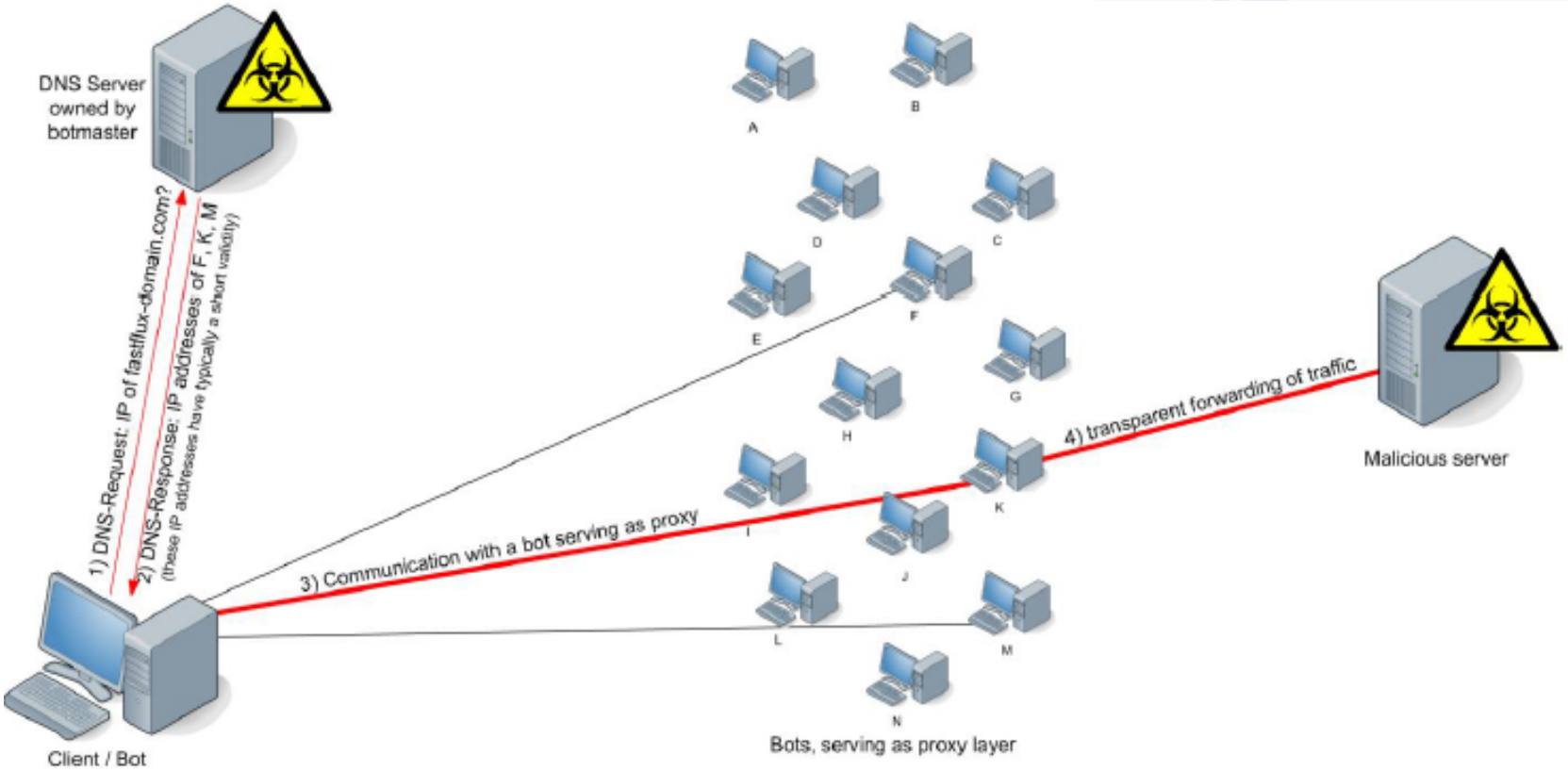
Eksempel – peer2peer



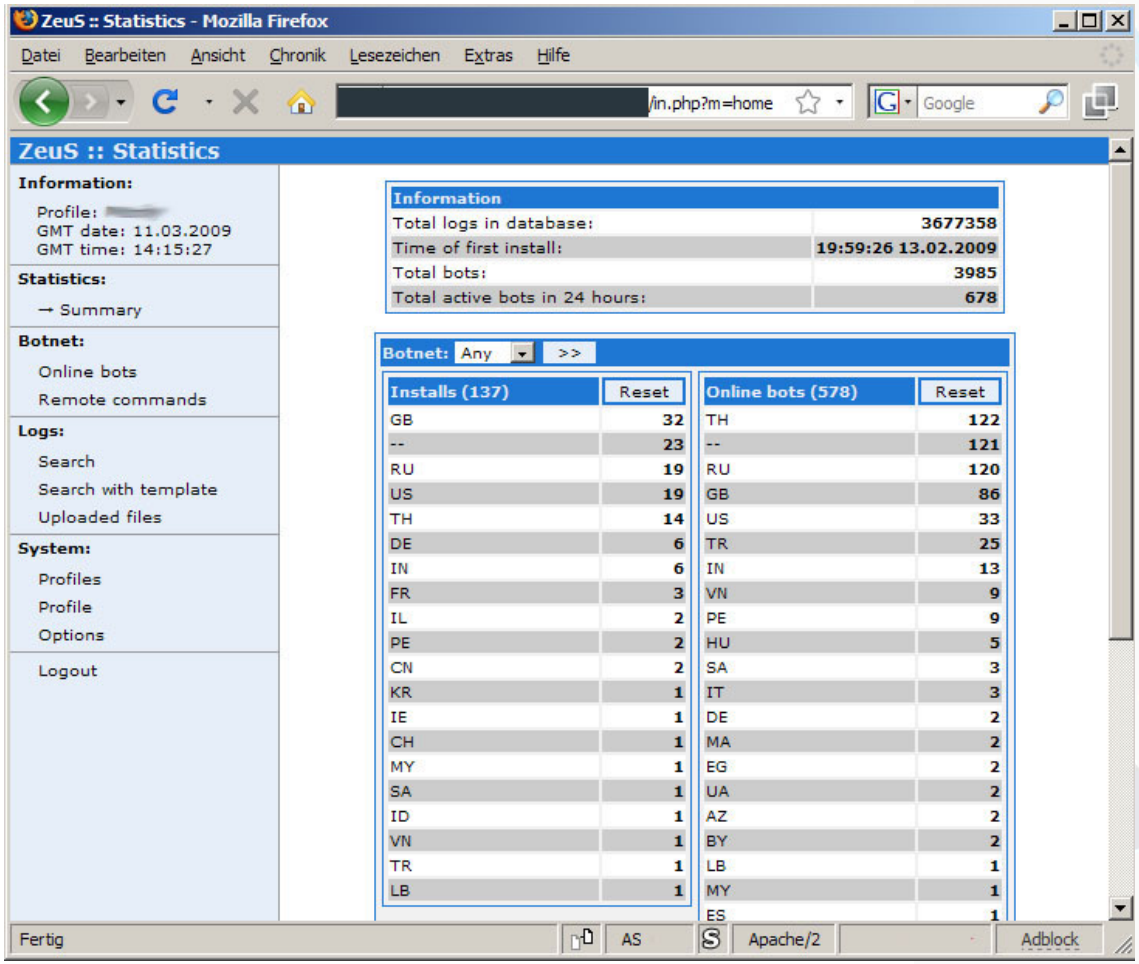
Eksempel – Servere kan skifte ofte



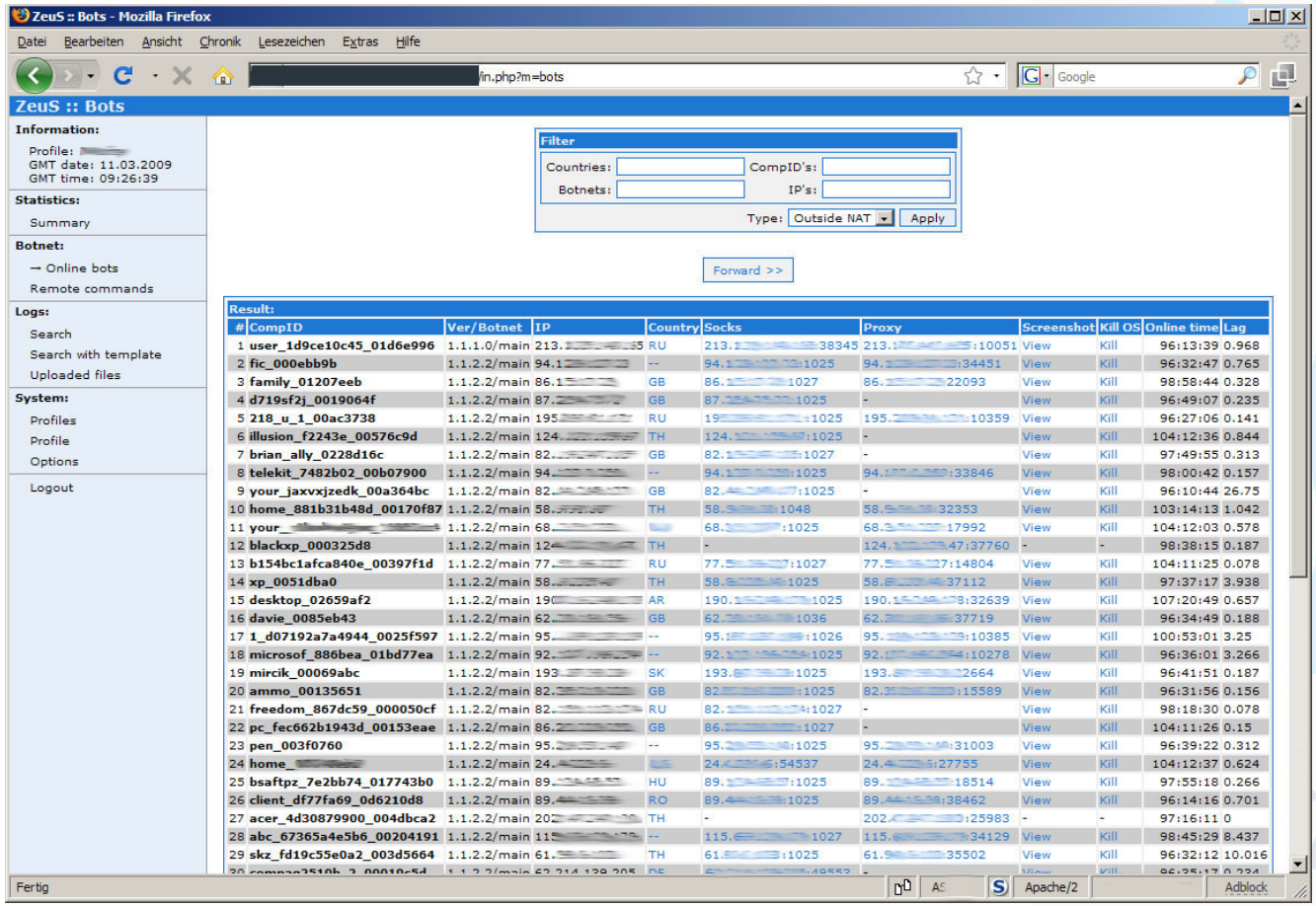
DNS kan også bruges til at gemme sig



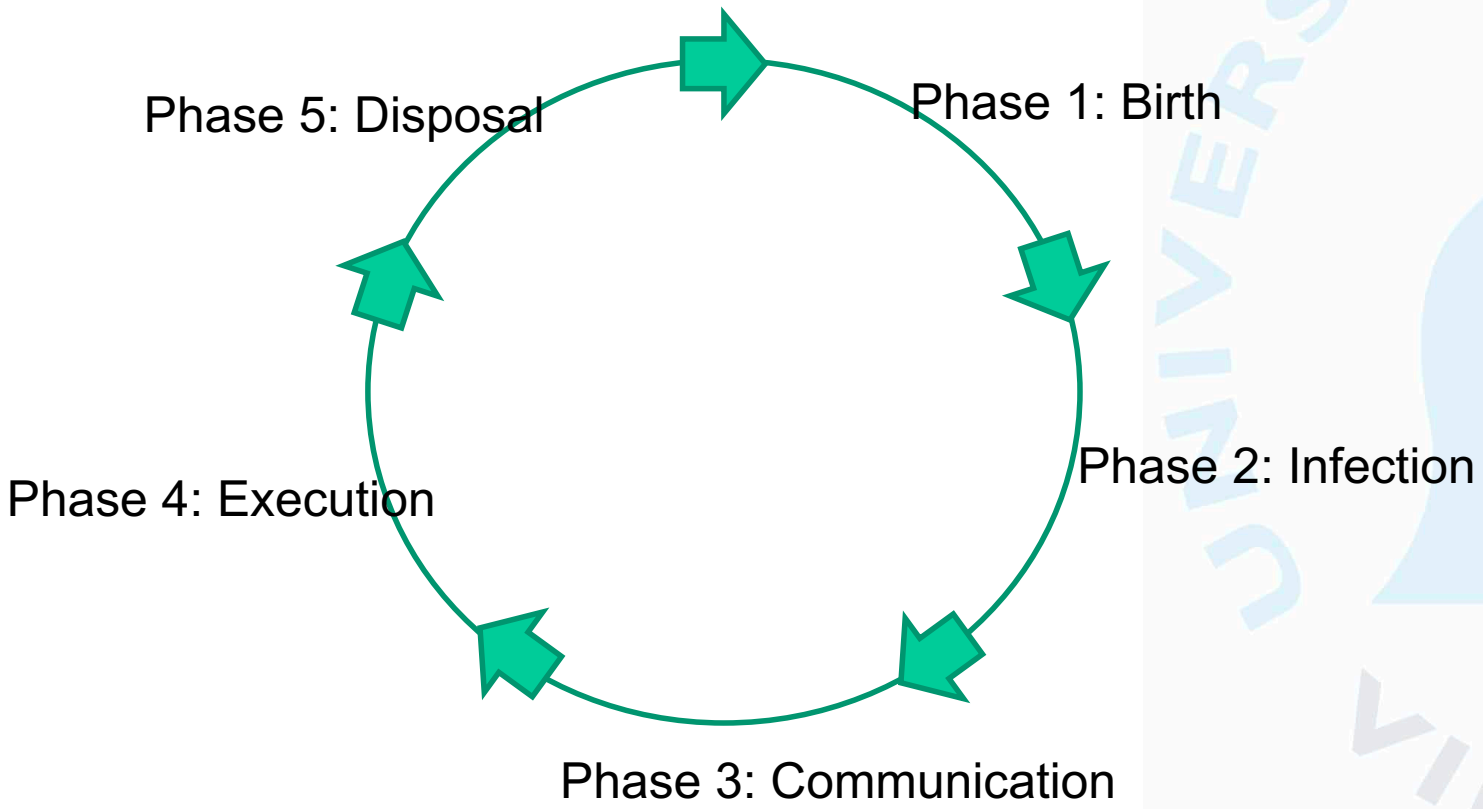
Example of Zeus User Interface (abuse.ch)



Example of Zeus User Interface (abuse.ch)

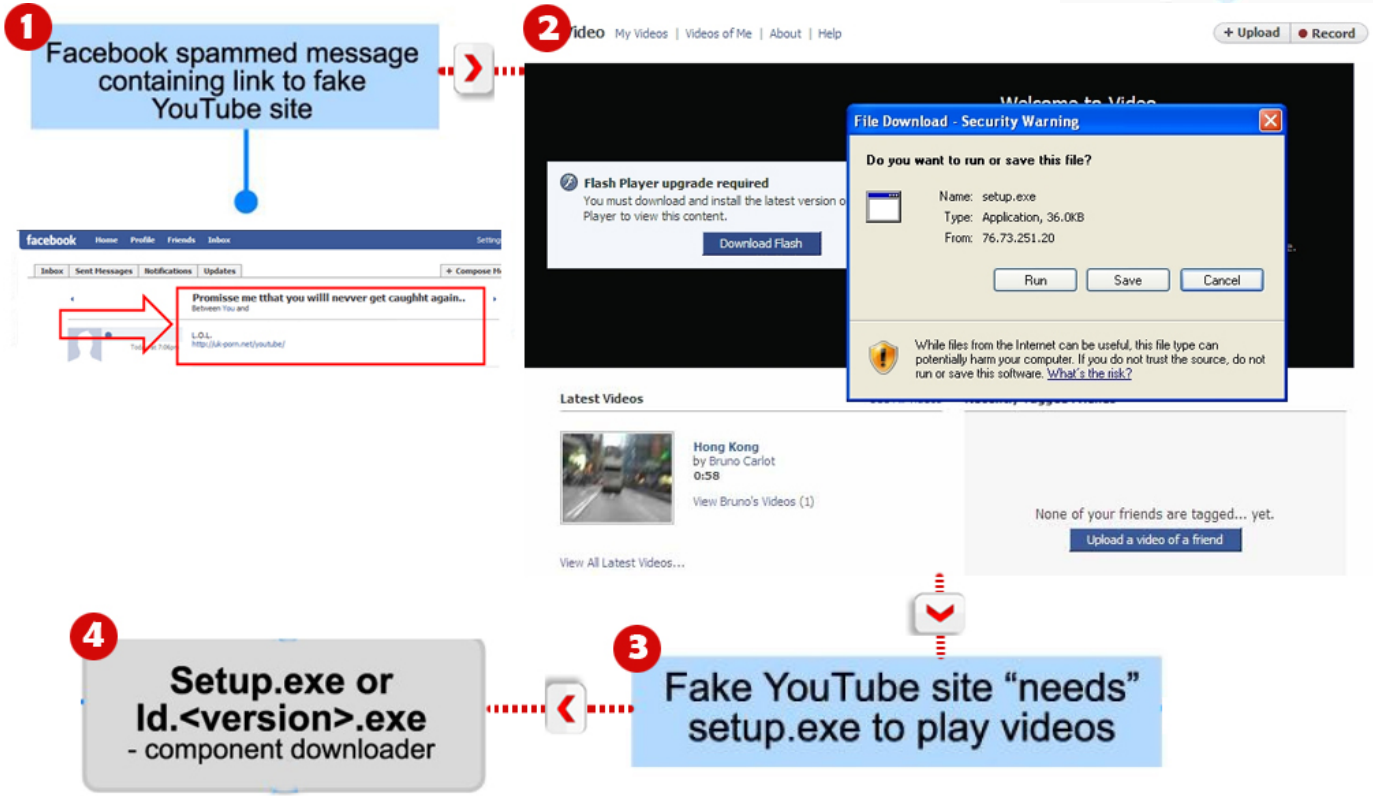


BotNet Lifecycle



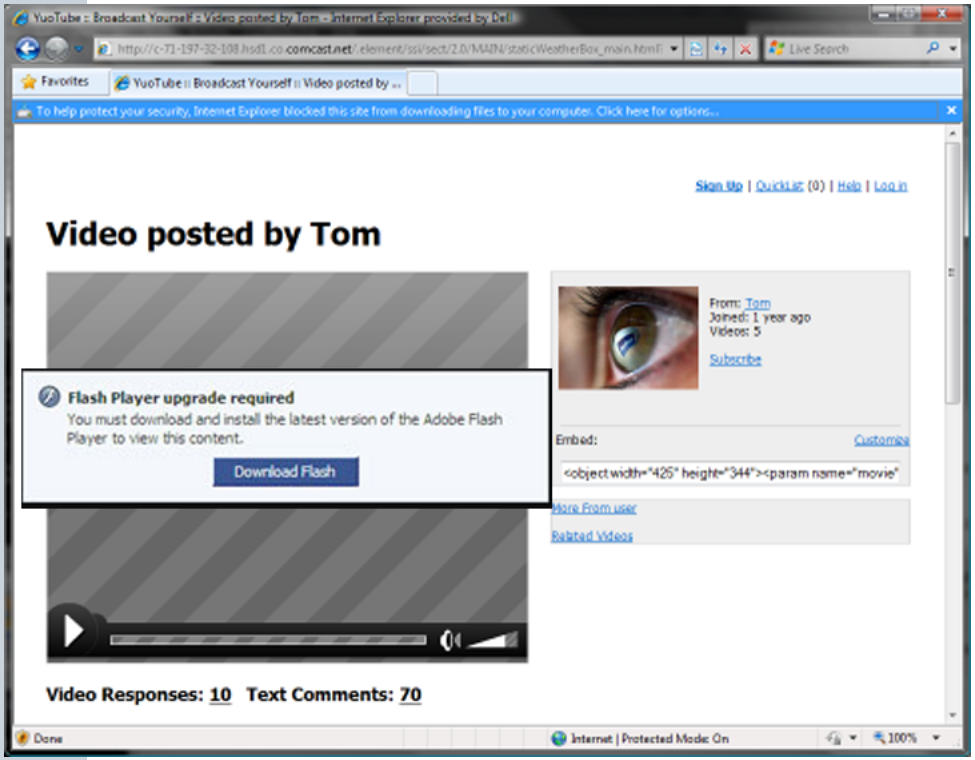
Noget om infektioner

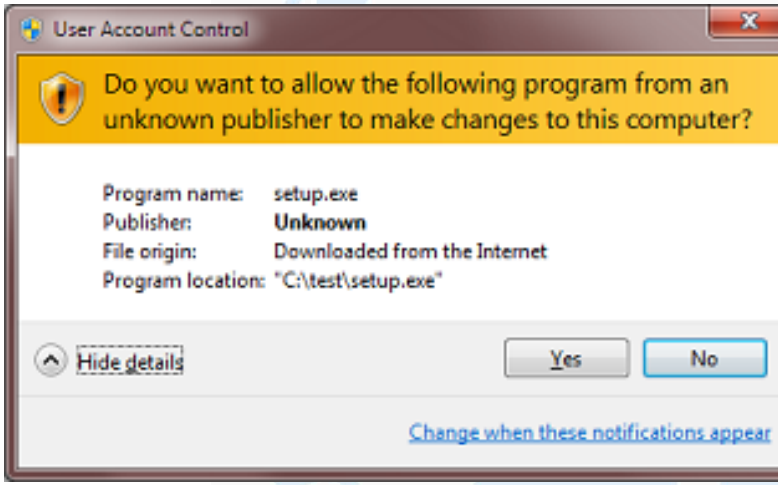
- Users – Social Engineering



Noget om infektioner

- Users – Social Engineering





According to Norton…

Of those using passwords, less than half of consumers "always" use a secure password.

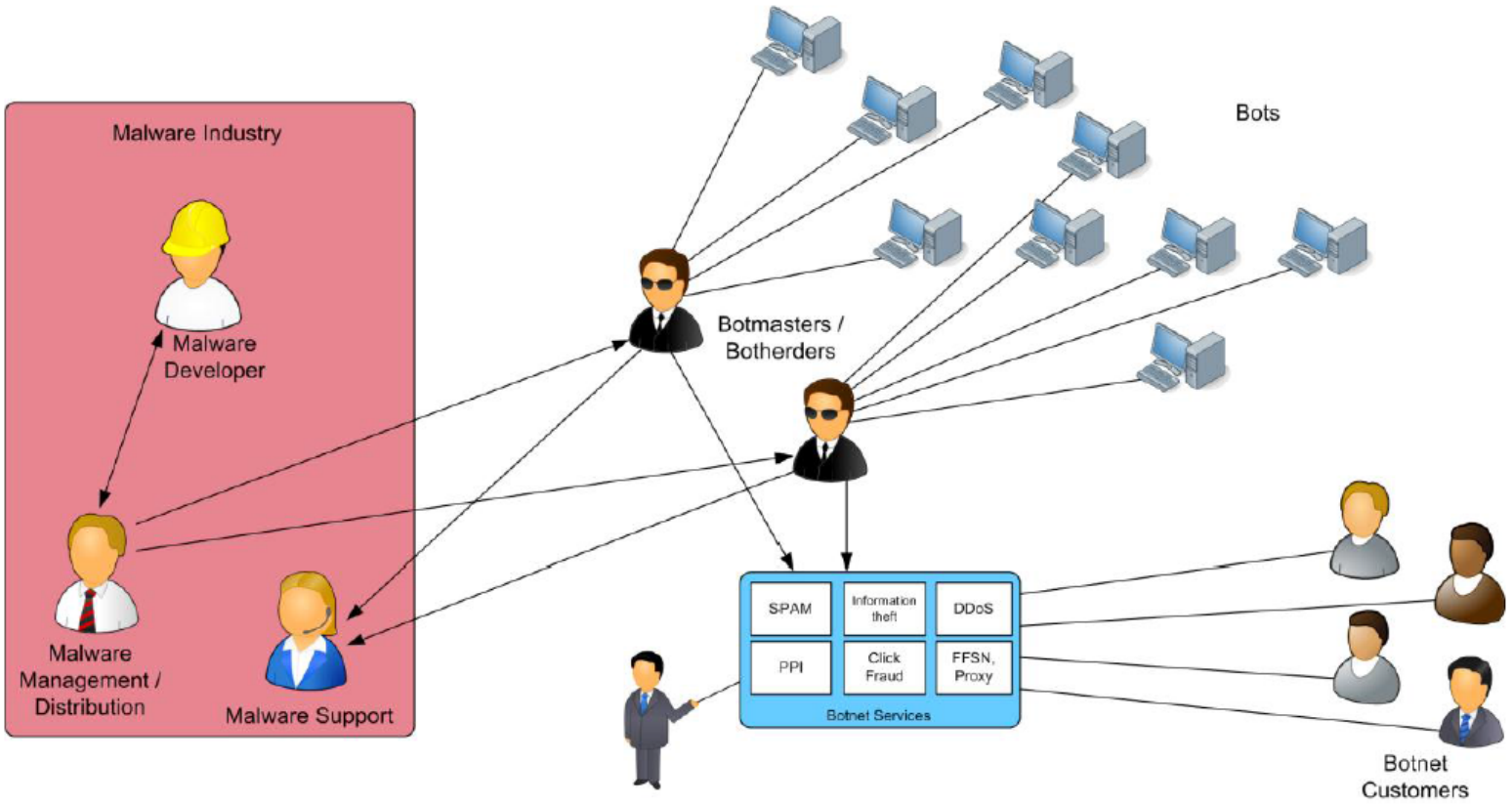
One in three do not have a password on their smartphone or desktop computer at all!

Dong Energy: Five forces against hacking

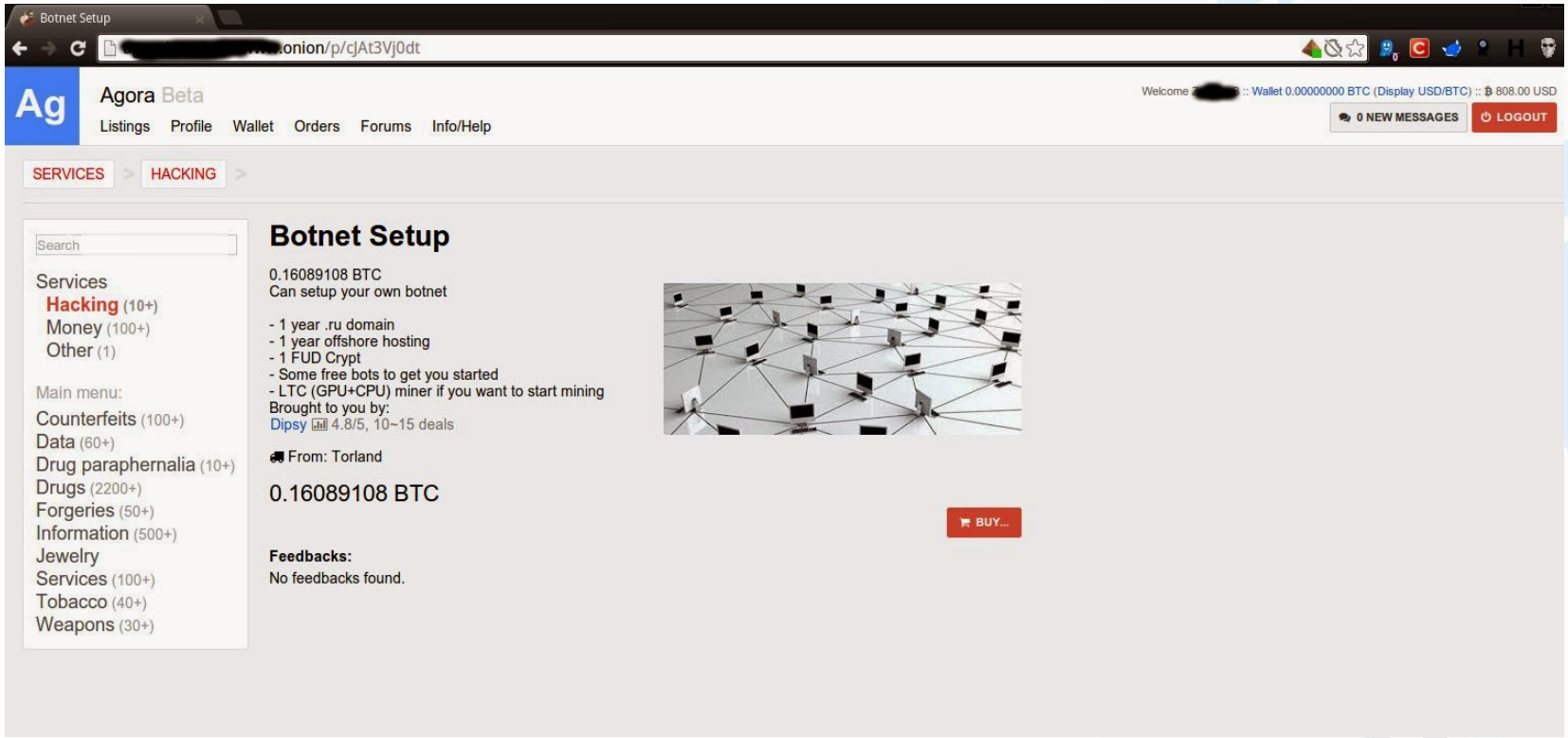
- Education, Gamification, Five recommendations:
  - Lock your computer when you leave it
  - Delete emails from unknown senders
  - Don't share passwords with colleagues
  - Be careful in using USB sticks with unknown origins
  - Avoid letting strangers into the building

- 6.000 (test) phishing emails sent:
  - 3.000 users clicked on the links
  - 1.000 users started filling out information on false websites
  - 500 users filled in passwords on false websites
  - (note that the attack was very well done)

Botnets – ren business

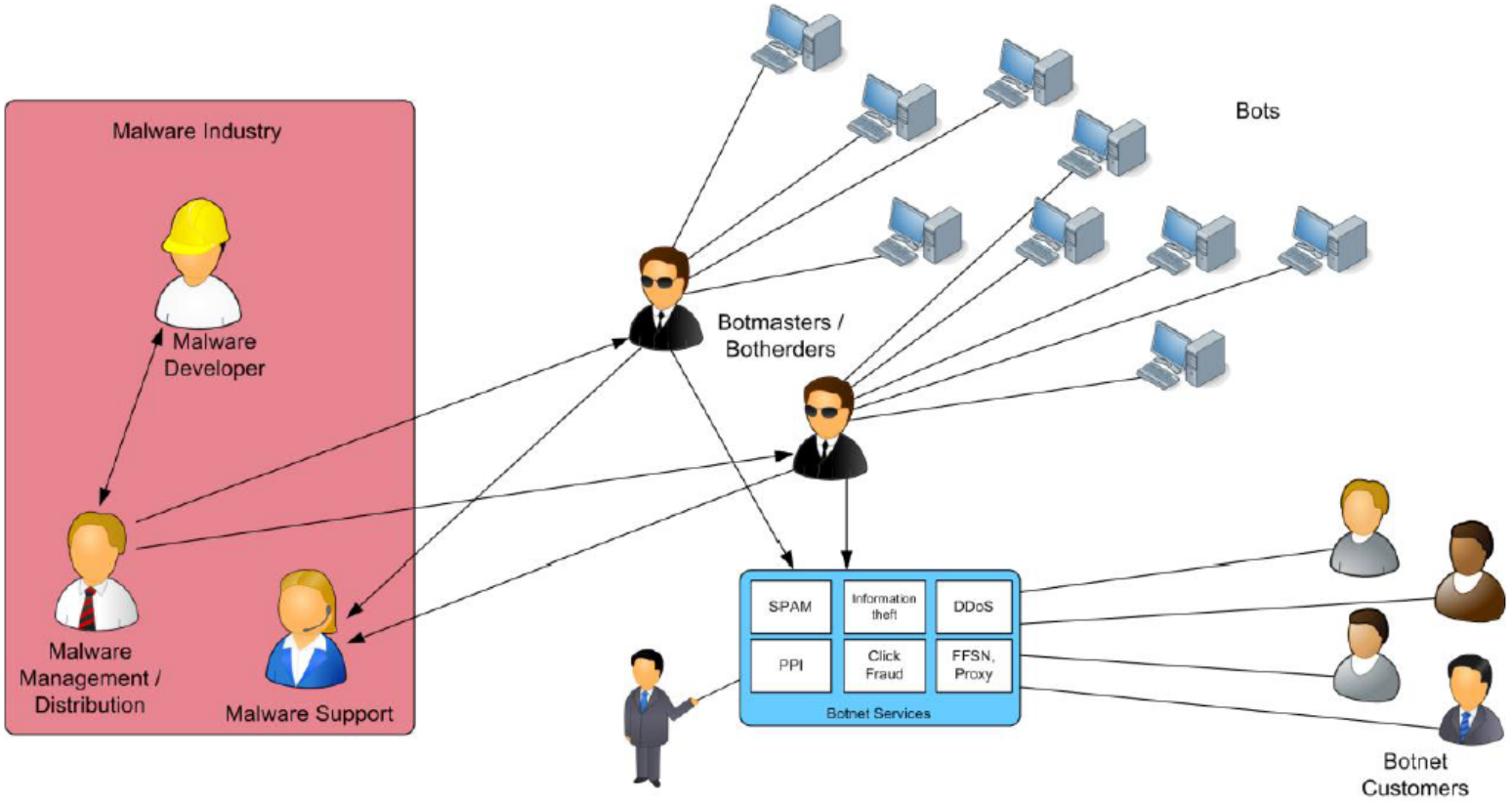


The roles when operating a botnet



Botnets – ren business

Det er overraskende let at købe f.eks. et DDoS-angreb.

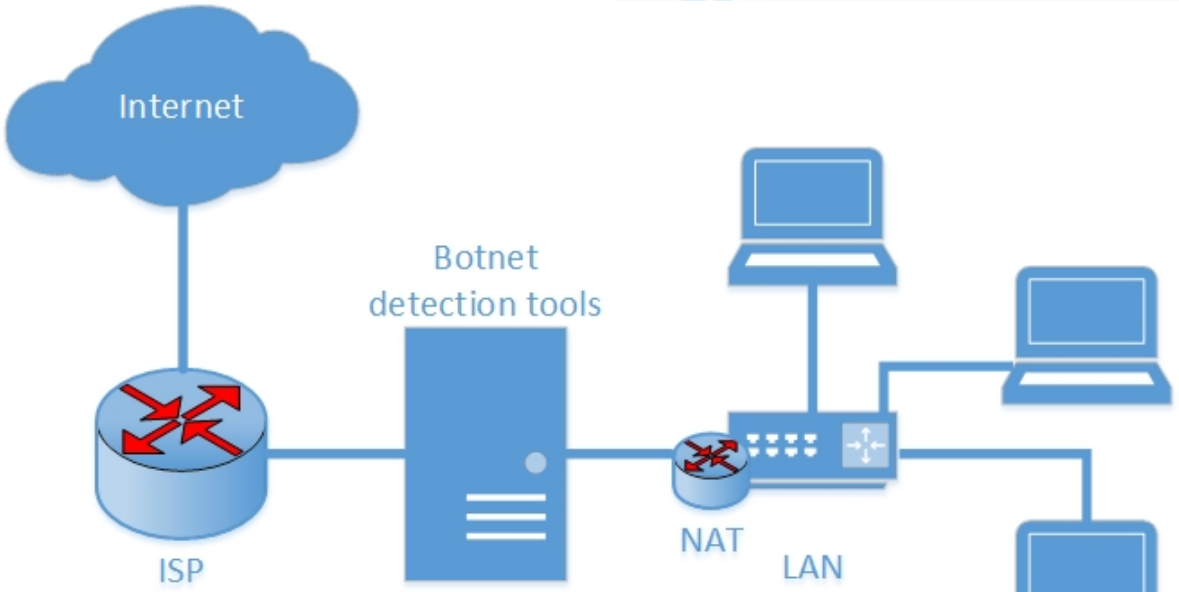


Zeus – King of Bots

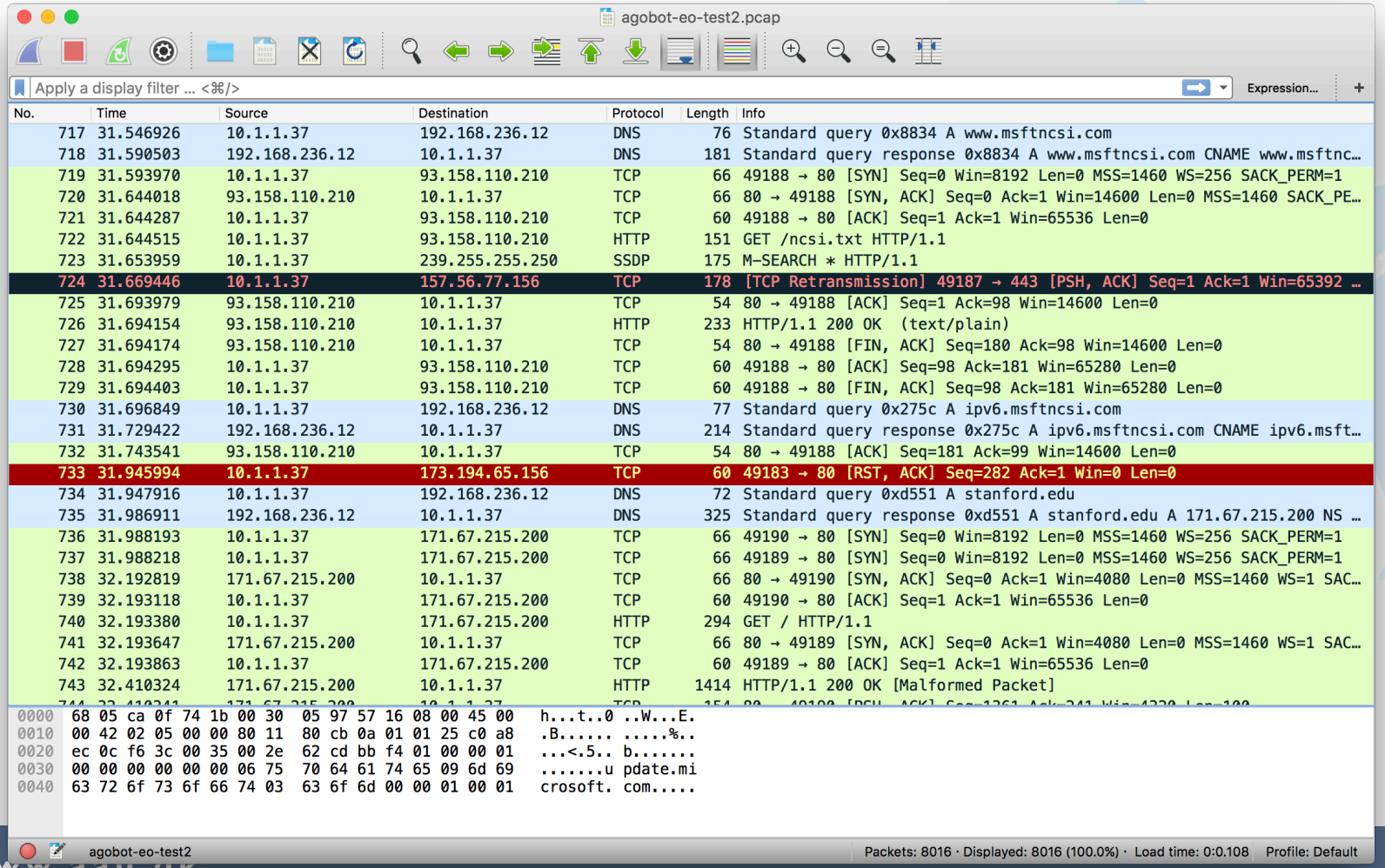
- Køb et "kit" på nettet, og du er kørende….
- Let og intuitivt bruger interface for Botmaster
- Især populært til at stjæle f.eks. Kreditkort-information.
- Estimat: 3.600.000 inficerede maskiner i USA.

Hvordan kan Botnet bekæmpes?

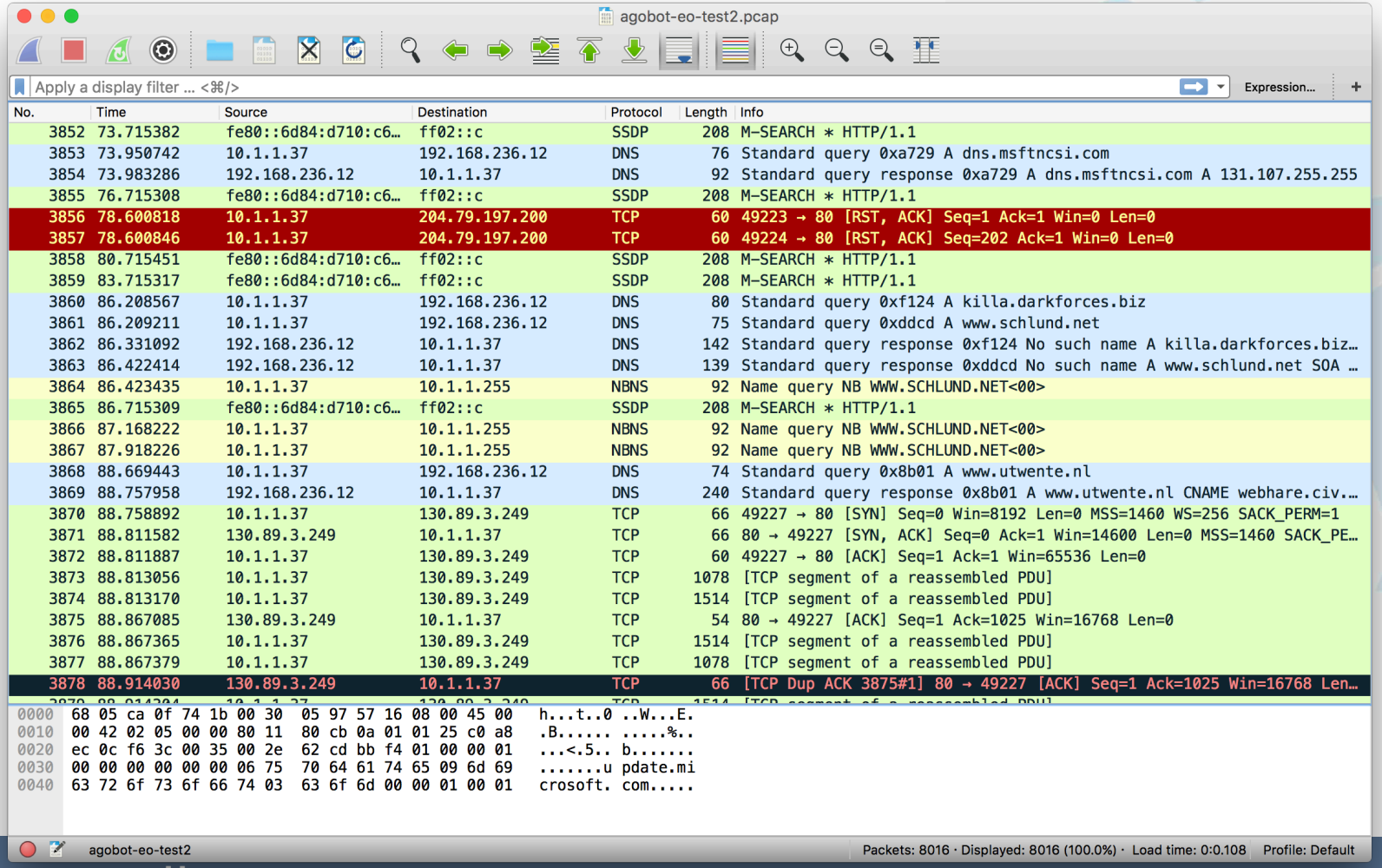
- Hvem skal gøre det?
- Host-baseret
- Netværks-baseret



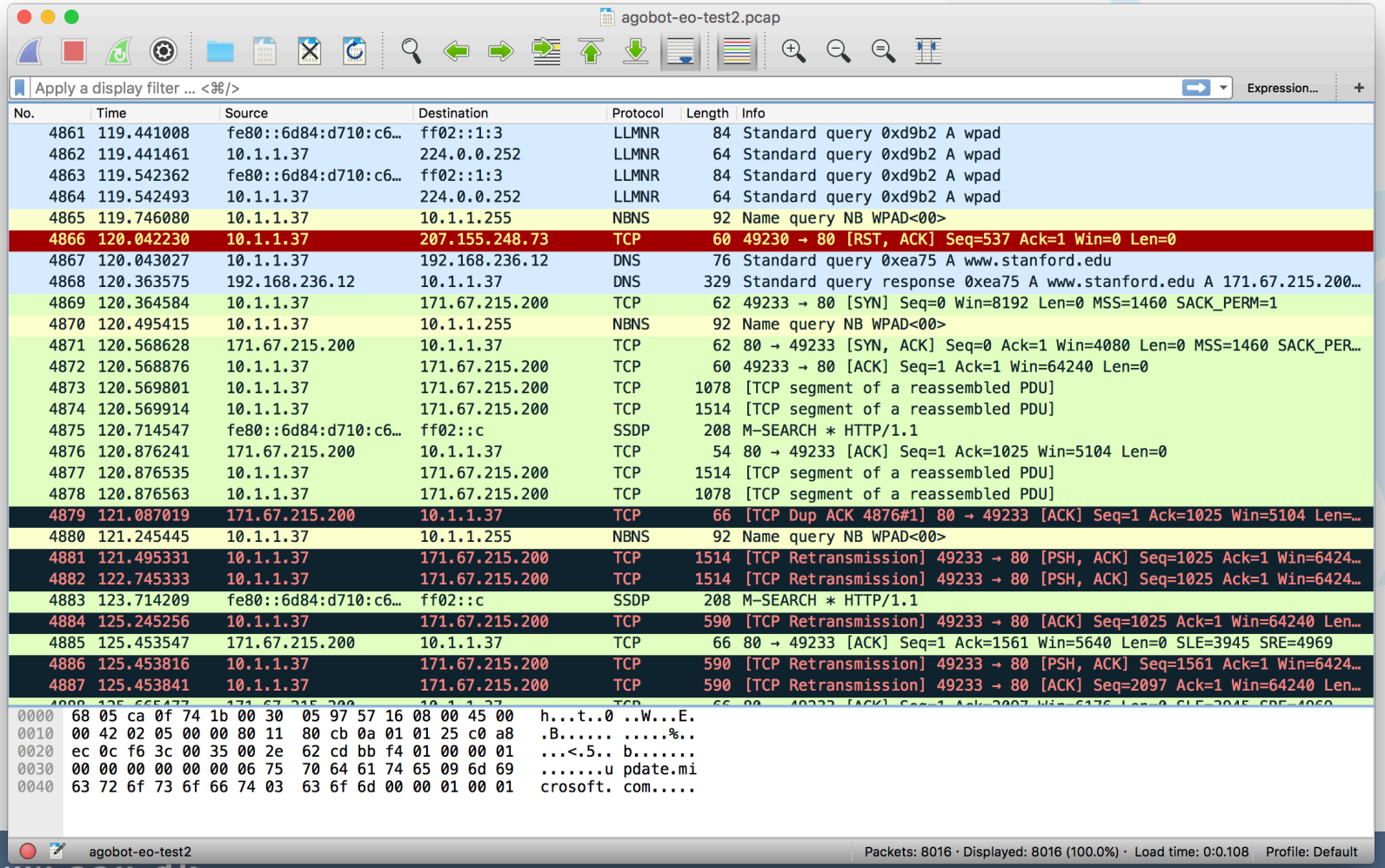
Eksempler på hvad vi ser…



Eksempler på hvad vi ser…



Eksempler på hvad vi ser…



Opsummering

- Botnets er en trussel mod IT-sikkerheden på flere måder. Det giver kriminelle adgang til at kontrollere computere med henblik på f.eks. DDoS-angreb og informationstyveri.
- Vi har allerede set eksempler på hvad angreb kan medføre – f.eks. nedlæggelse af offentlige systemer som NEM-ID.
- Botnets skal ses I sammenhæng med et veletableret netværk af IT-kriminelle, og en del af en større undergrundsøkonomi med egne forretningsmodeller – det er big busines.
- Vi arbejder med at detektere inficerede maskiner allerede i kontrolfasen, så man kan forebygge kriminelle handlinger.
- Det gør vi ved at udvikle systemer der hurtigt men præist kan se forskel på "god" og "dårlig" trafik. Det er udfordrende og spændende – både at udvikle metoder og teste/udvikle dem!

Tak for opmærksomheden

Spørgsmål

jens@es.aau.dk