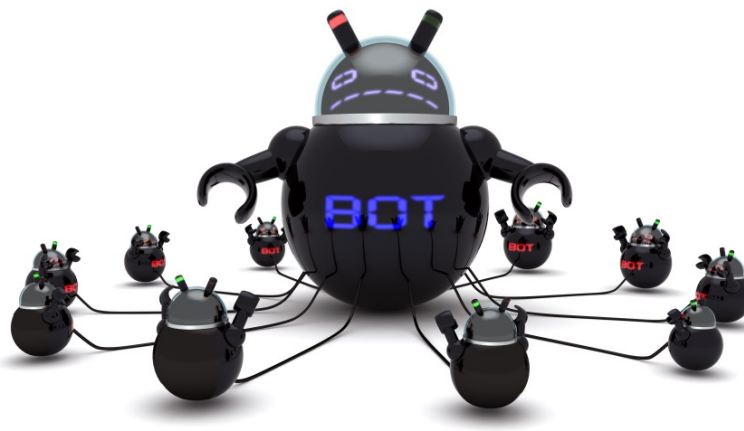


# Botnets – Organiseret kriminalitet på nettet

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...

ERSITAS



# 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://64.171.100.200/?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<sup>®</sup> 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It has come to our attention that your **Amazon** order Information records are out of date.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://www.amazon.com/exec/obidos/account-access-login/ref=/index>

Best Regards,  
**Amazon Security Department**

[Conditions of Use](#) | [Privacy Notice](#)  
c 1995-2007, Amazon.com, Inc. or its affiliates.

<http://165.236.100.100/gsinternal/ama.html>  
Click to follow link

## Cyberkriminalitet har mange ansigter



## Cyberkriminalitet har mange ansigter



## Cyberkriminalitet har mange ansigter



## Cyberkriminalitet har mange ansigter...



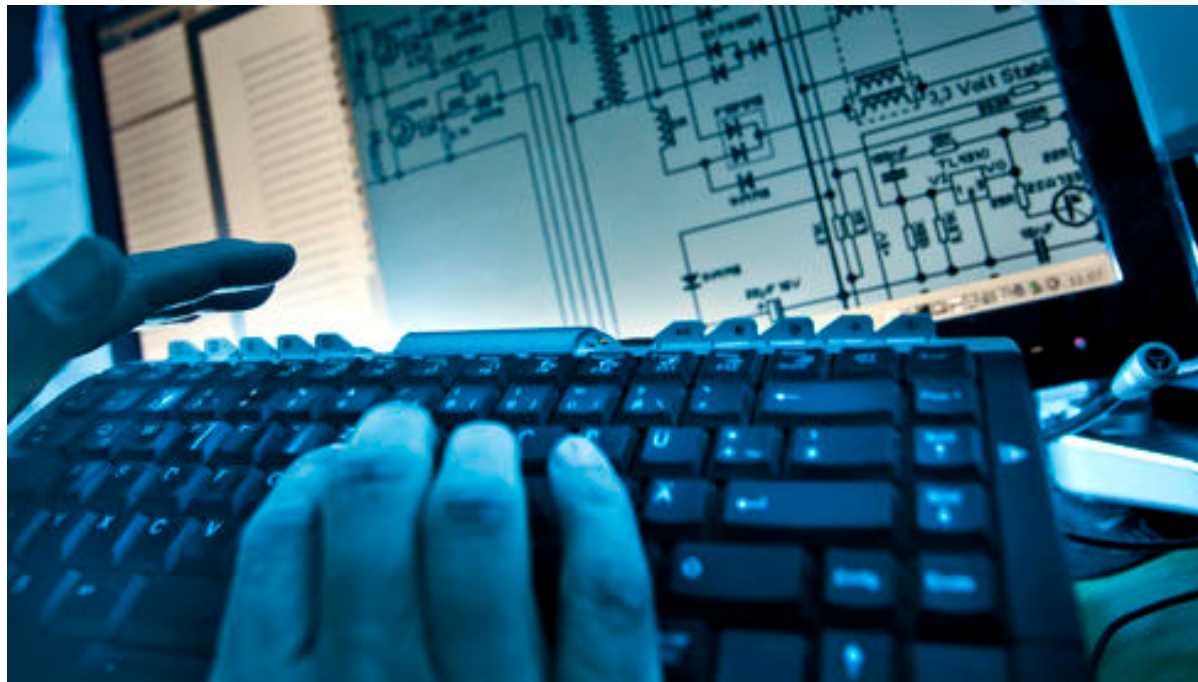
## Botnets – Organiseret kriminalitet på nettet

- 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



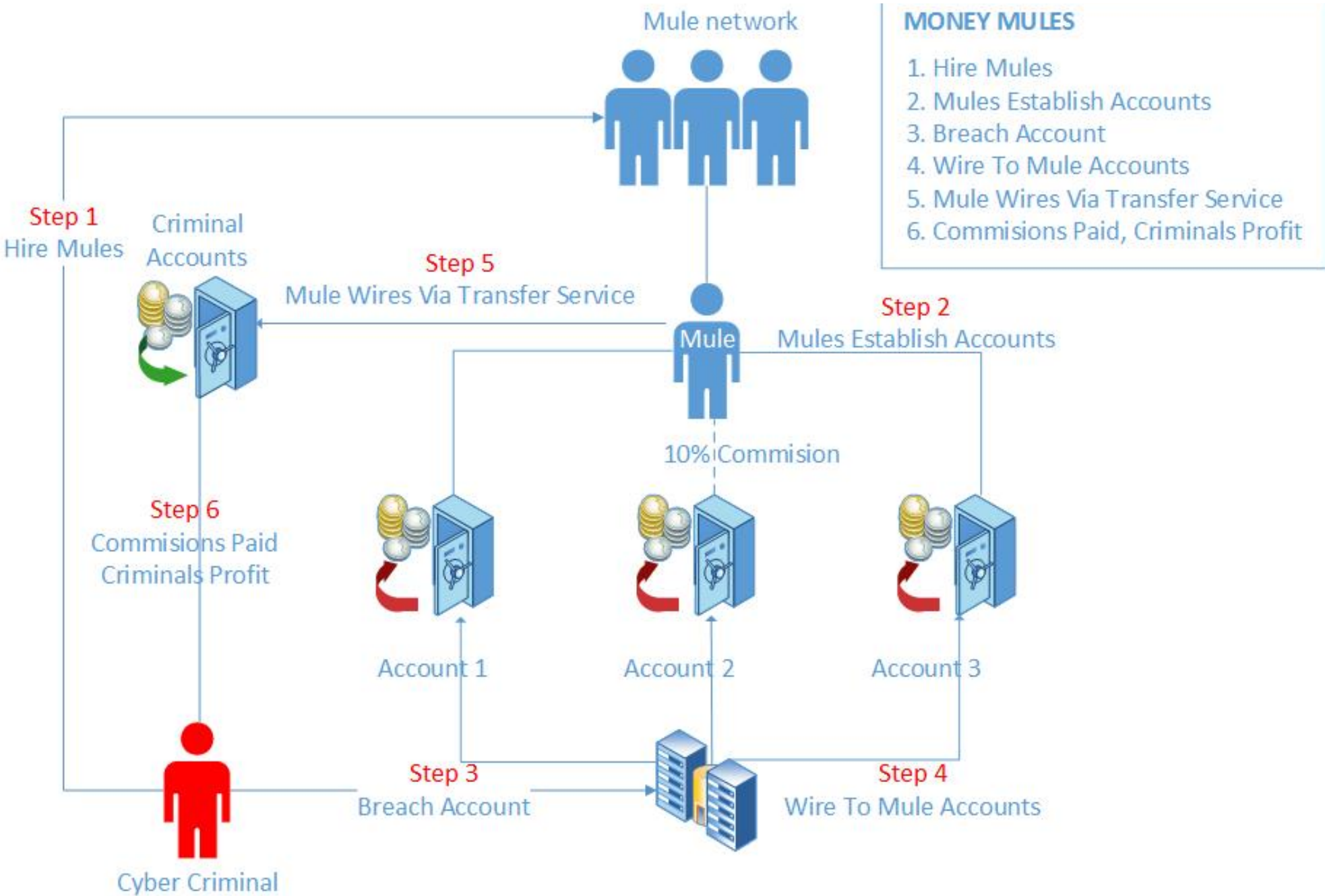
## Eks. I: Stjålne forretningshemmeligheder

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



## Eks. 2: Steffen fra Thyborøn





## Eks. 3: DDoS angreb på ...

The screenshot shows a Mozilla Firefox browser window displaying a news article from dr.dk. The article is titled "Elever hakede skolers computere" and is dated 23. apr. 2014 12.22 Indland. The main text describes a DDoS attack on school computers, where students from a primary school in Hedensted used their computers to flood the school's network, preventing access to the internet for 27 schools and 7000 computers. The article mentions that the students were unaware of the attack and that the school is considering reporting the incident to the police.

**Elever hakede skolers computere**  
23. apr. 2014 12.22 Indland

**Elever fra en folkeskole ville ikke tage en test. De lavede et hacker-angreb, som ramte cirka 7000 computere på 27 forskellige skoler.**

Hvert år skal eleverne i folkeskolen til prøve for at vise, hvor dygtige de er.

Prøven foregår blandt andet via internettet, men for en måneds tid siden måtte en skole i Hedensted udsætte dette års tests.

Skolens computere kunne ikke komme på internettet på grund af et hacker-angreb.

Bag angrebet stod nogle af skolens ældste elever, der ikke ville til prøve.

**Eleverne kan blive meldt til politiet**

Eleverne forstyrrede internetforbindelsen til 27 skoler, og cirka 7000 computere blev ramt af hacker-angrebet, fortæller P4 Trekanten.

Hedensted Kommune har fundet eleverne bag angrebet. De risikerer at blive meldt til politiet.

Kommunen siger, at eleverne nok ikke ville have lavet hacker-angrebet, hvis de havde vidst, at det ville

**Læs op**

**Læs også**

- » Politiet sætter hårdere ind mod it-kriminelle
- » Hackere har fået adgang til cpr-numre
- » Hackere har angrebet politiets registre
- » Hackere elsker Facebook
- » Hackere stjal fra EU og NATO i fem år
- » Hacker-angreb er den største trussel mod Danmark
- » Stort angreb mod svenske hjemmesider

**Del artiklen:**

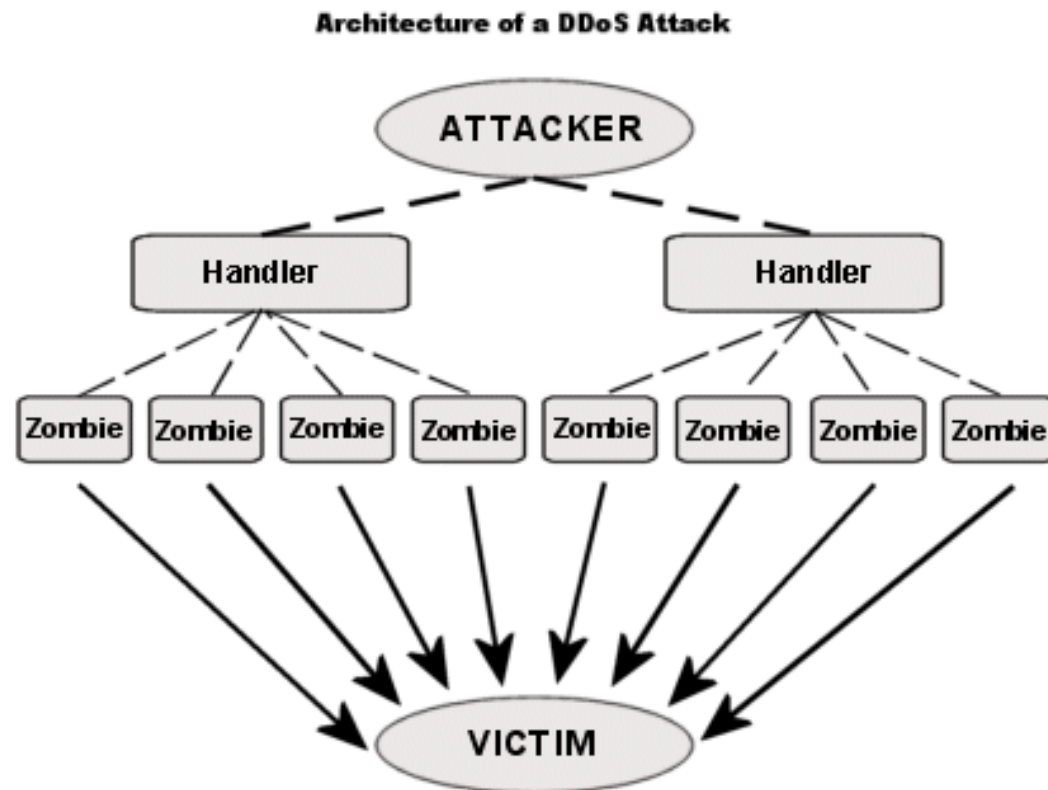
- » Mail

**Ogens vigtigste historier**  
[Læs mere](#)

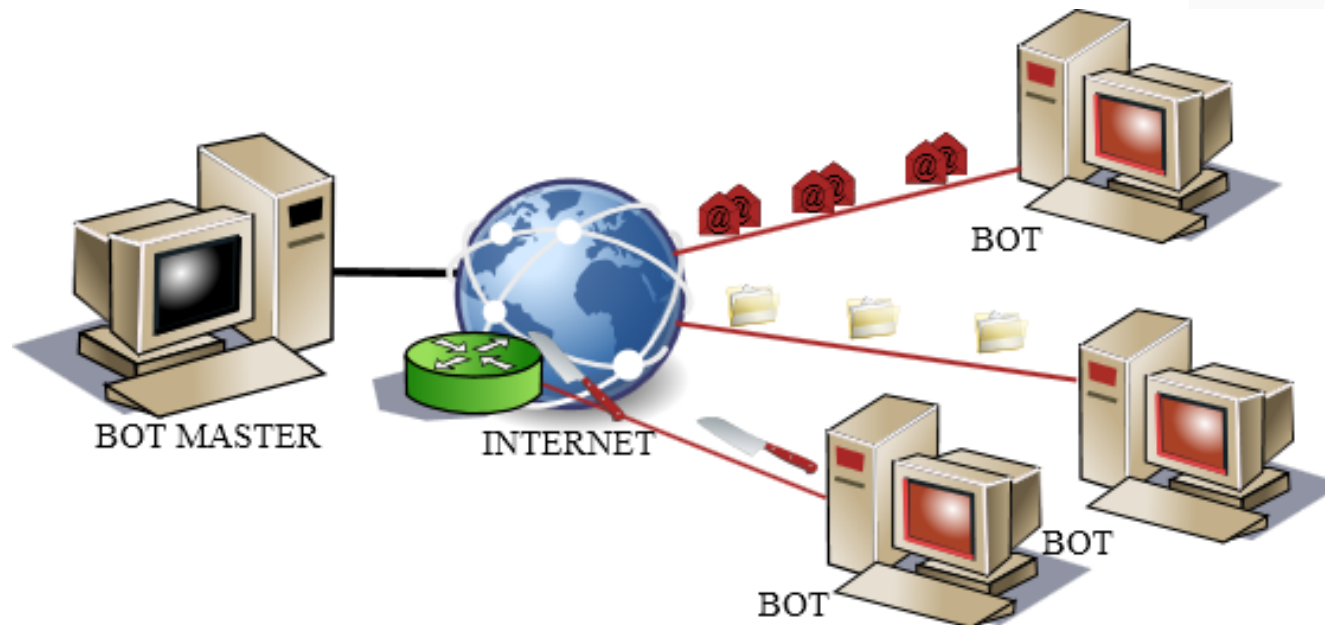
**Billedserie: Vandfestival i Myanmar**  
[Læs mere](#)

**RSS-feed med Ligetils nyheder**

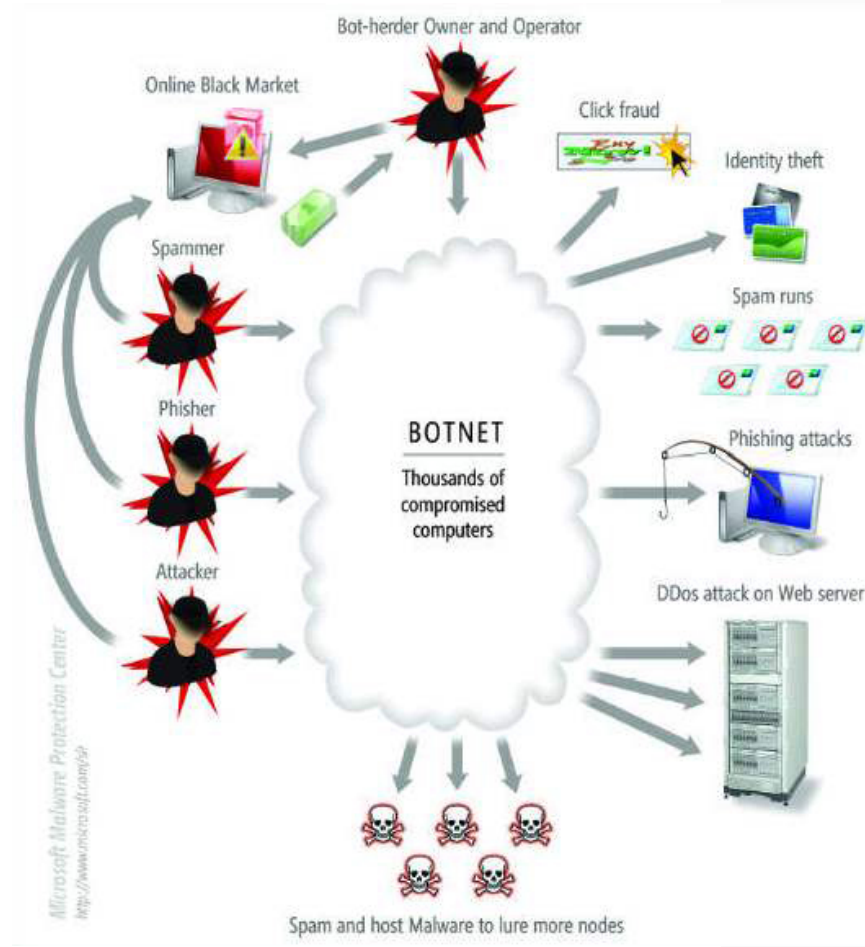
## Eks. 3: DDoS angreb på Nem ID



## Hvad er så et Botnet for noget?

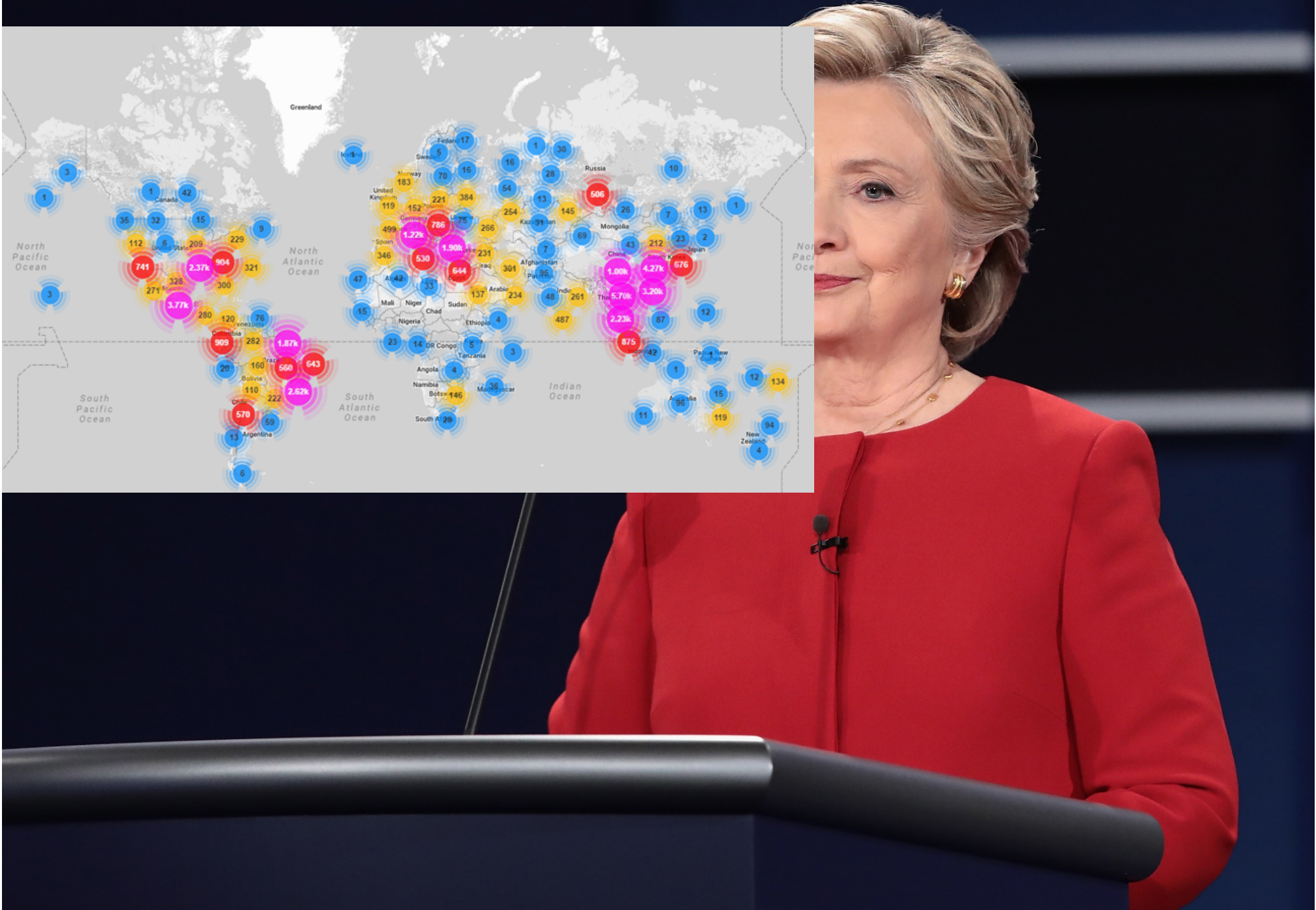
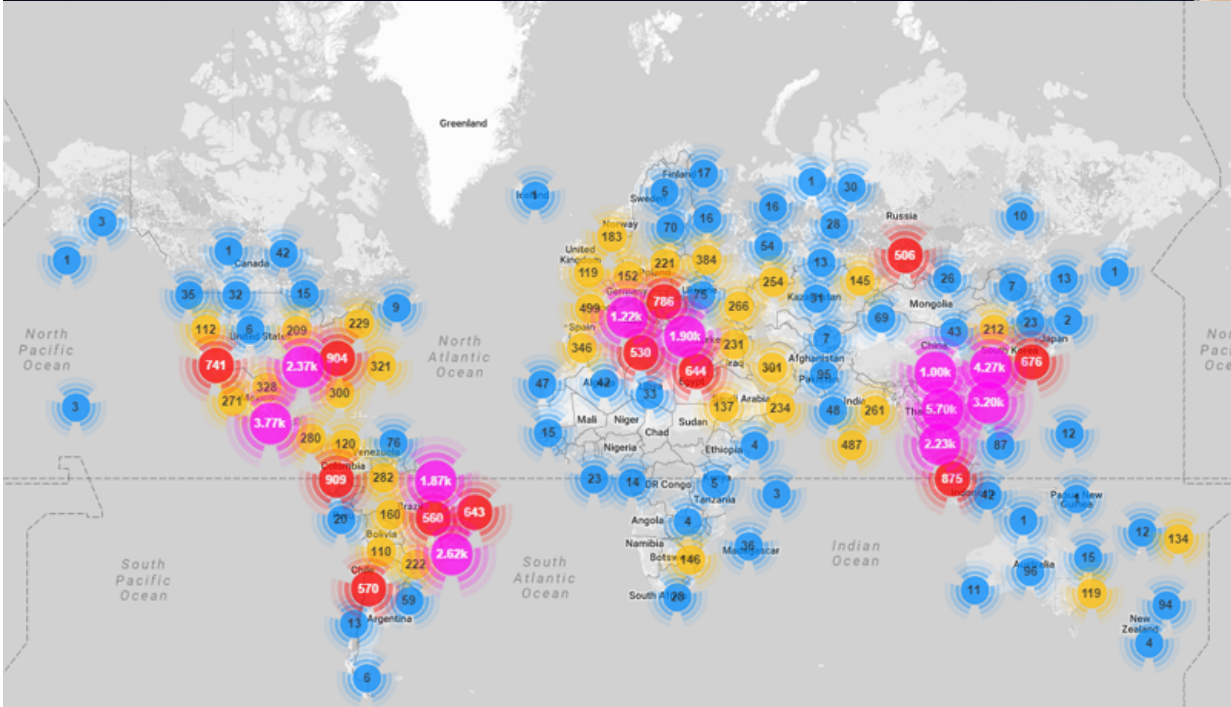


# Hvad er et Botnet?









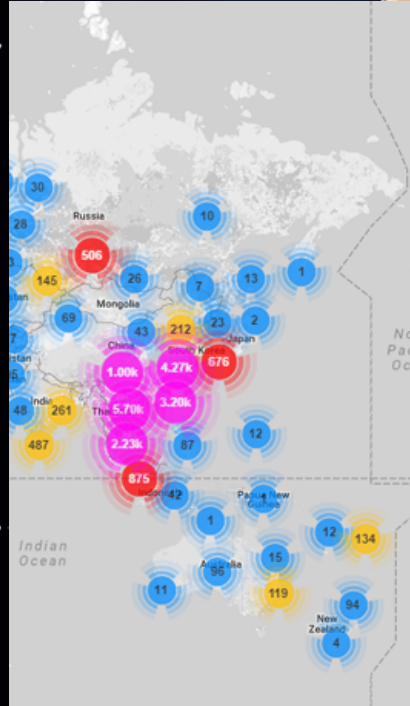
# 2 KINDS OF CLICK FRAUD

## 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.

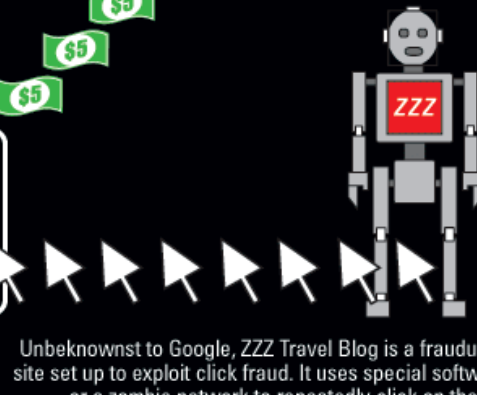


## AFFILIATE CLICK FRAUD

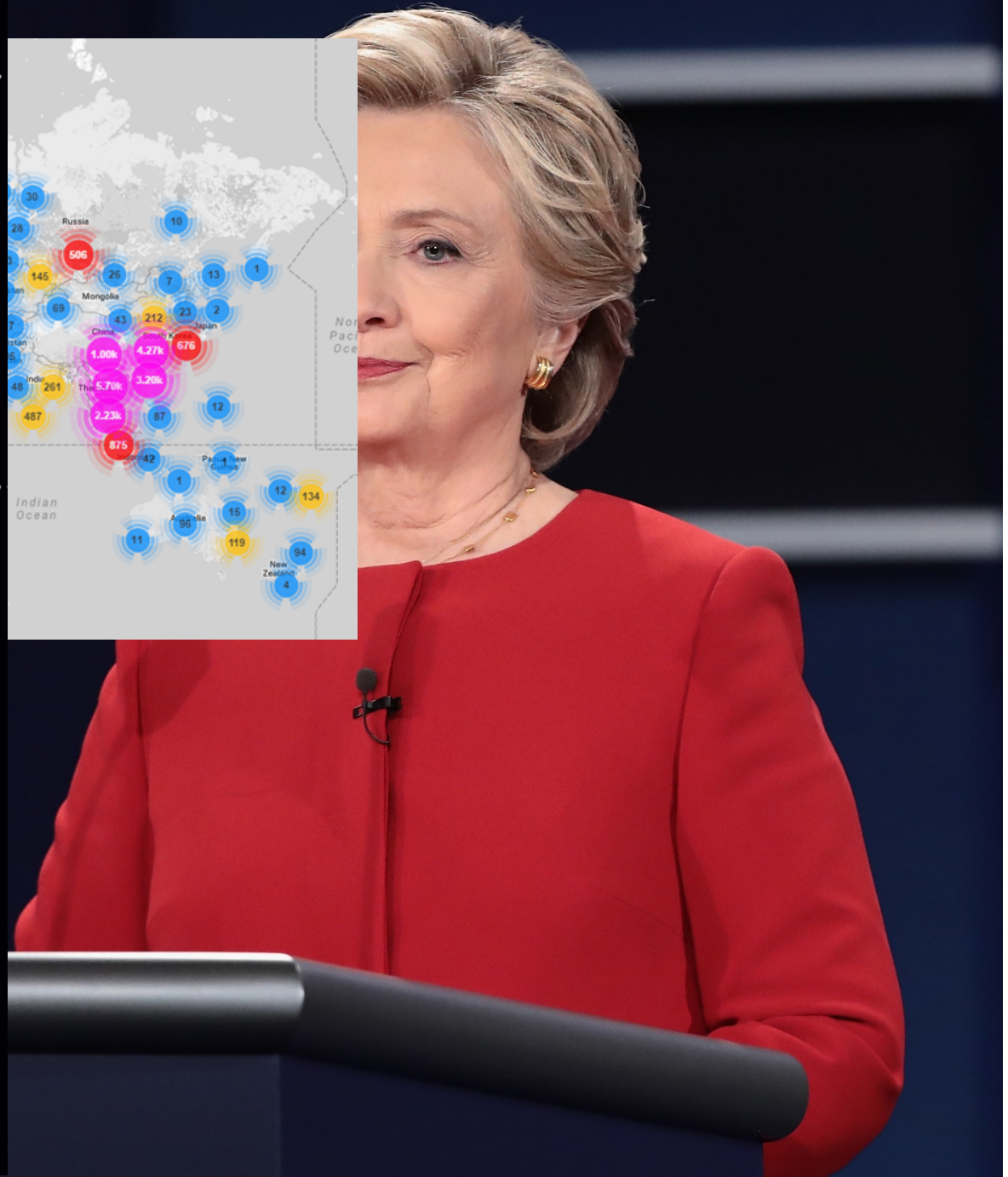


Acme Charters hires Google to place its ad on relevant sites using keywords. Acme agrees to pay Google \$10 per click.

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



\*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**

Sources  
<http://www.eta.gov/tools/faqs/faq.cfm?id=97&t=3>  
[http://www.eta.gov/electricity/monthly/epm\\_table\\_grapher.cfm?reprint\\_5\\_6\\_a](http://www.eta.gov/electricity/monthly/epm_table_grapher.cfm?reprint_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 11,280 KWh.

# 2 KINDS OF CLICK FRAUD

## IMPACT OF ZEROACCESS BOTNET

COMPETIT

ACME CHART

Acme Charts pay Google \$... Web surfer on a Google

AFFILIATE

ACME CHART

Acme Charts place its ad using keywords to pay Google

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 =>

the largest P2P ever known

million

is out two on activities

CLICK FRAUD

rates...

click fraud generates 488 TB network traffic/day per annum earnings: tens 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.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 11,280 KWh.

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.

Symantec.

@threatintel | www.symantec.com

# 2 KINDS OF CLICK FRAUD

## IMPACT OF ZEROACCESS BOTNET

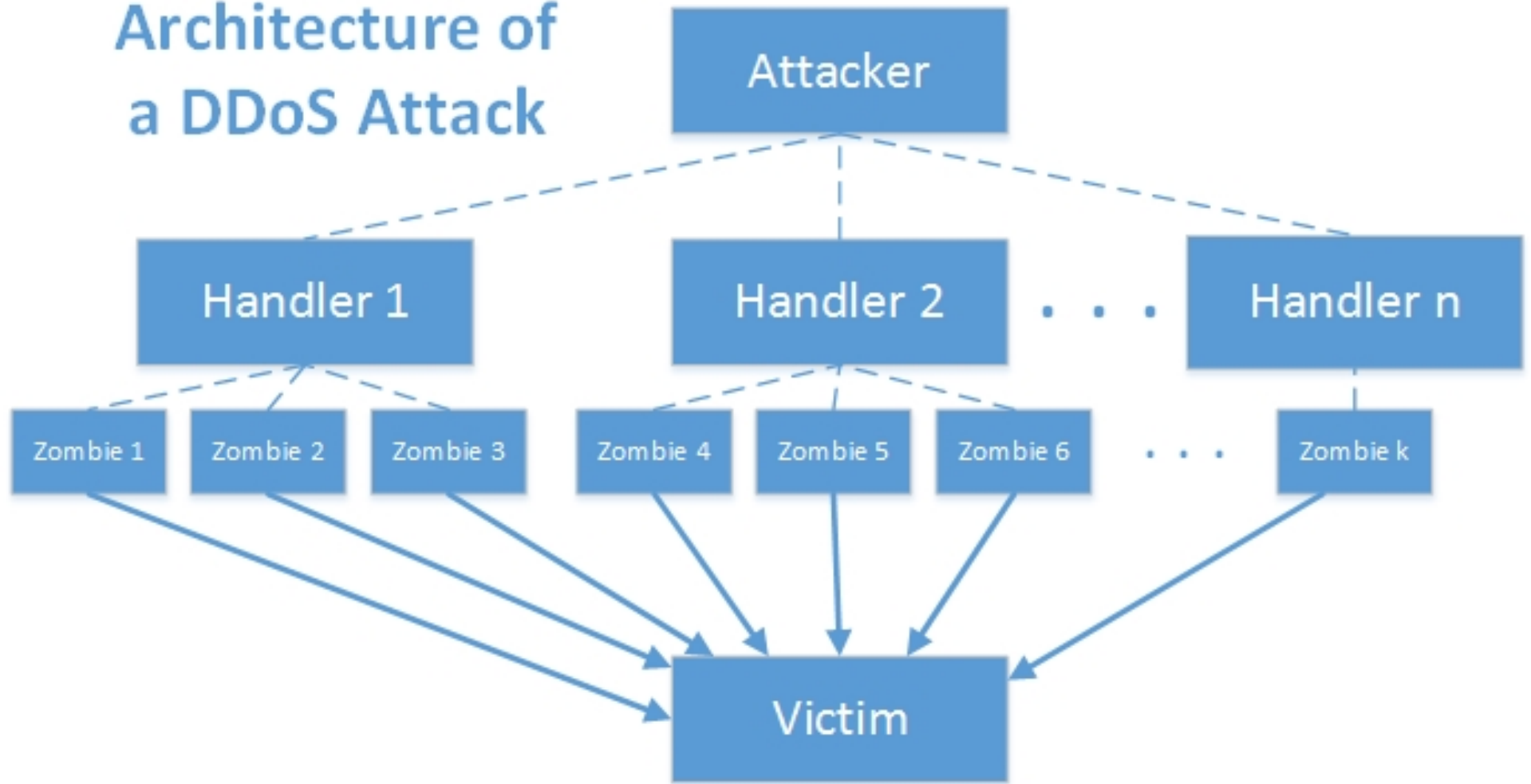
CryptoLocker

COMPETI

Your personal files are encrypted!

e largest P2P  
ever known

### Architecture of a DDoS Attack



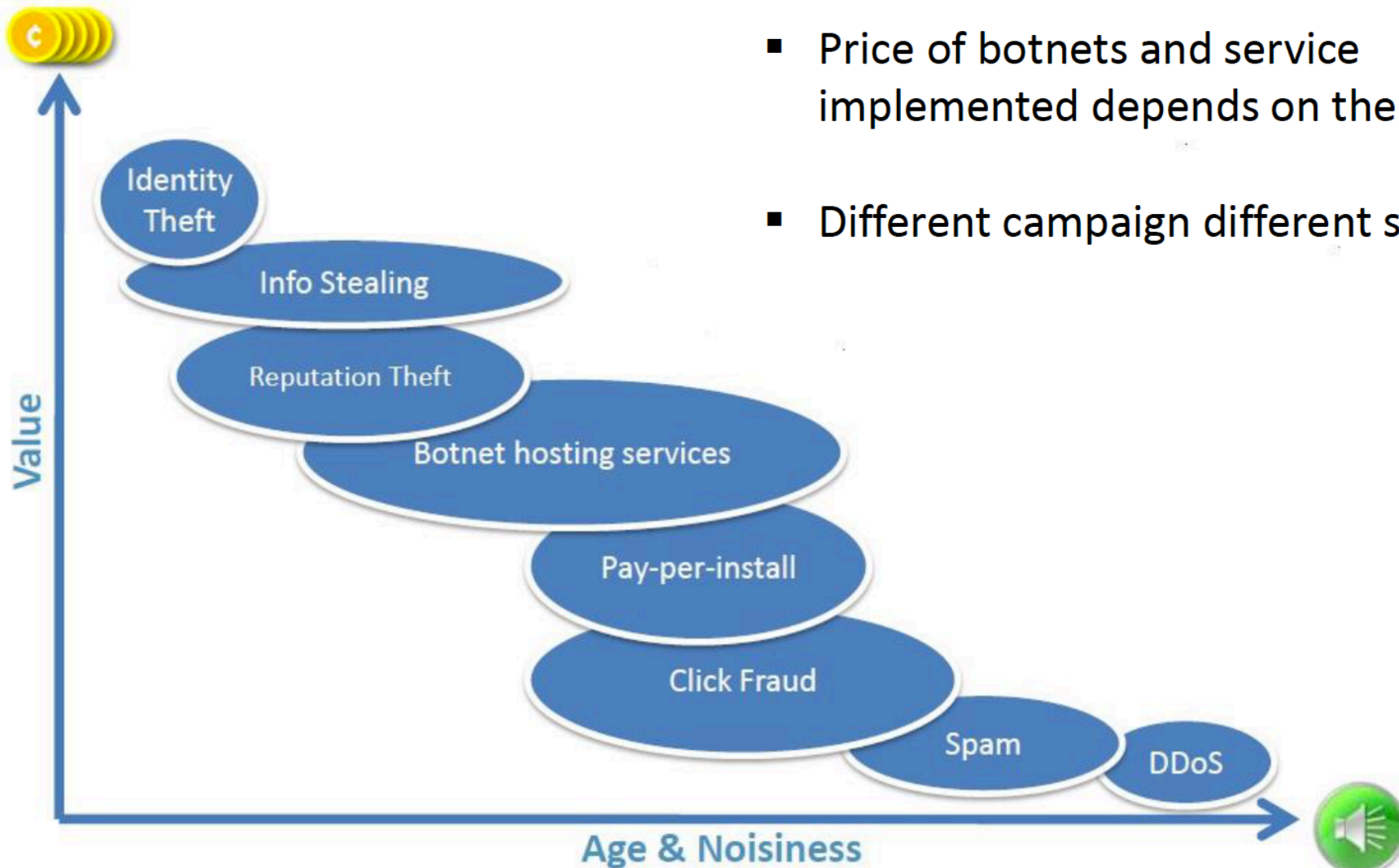
Unbeknownst to Google, ZZZ Travel Blog is a fraudulent site set up to exploit click fraud. It uses special software or a zombie network to repeatedly click on the ad. ZZZ Travel Blog gets rich; Acme Charters goes broke.

#### Sources

<http://www.eta.gov/tools/faq/faq.cfm?id=97&t=3>  
[http://www.eta.gov/electricity/monthly/egm\\_table\\_grapher.cfm?reprint\\_5\\_6\\_a](http://www.eta.gov/electricity/monthly/egm_table_grapher.cfm?reprint_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 11,280 KWh.



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

## 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!!

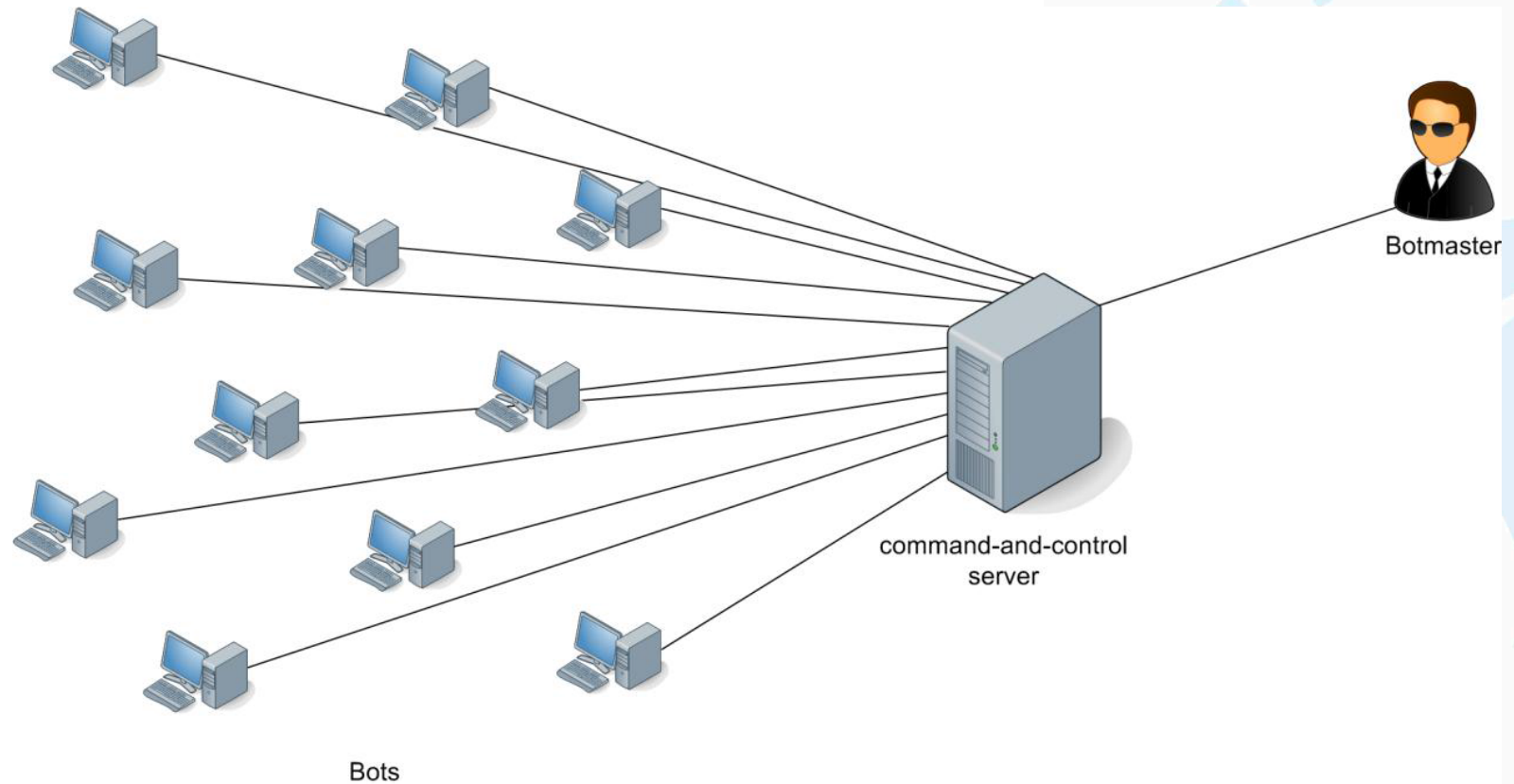
## Pay per install

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

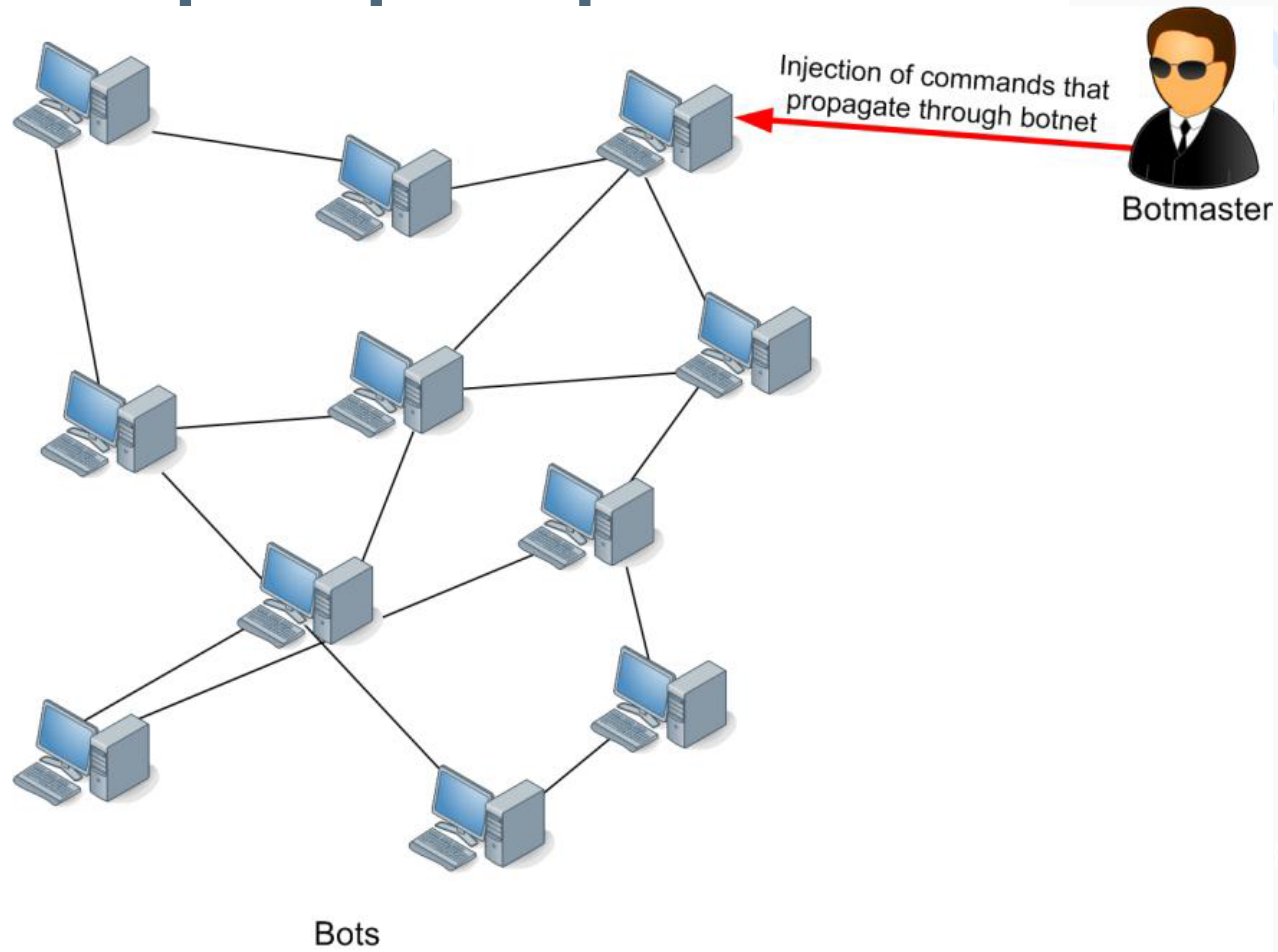
Tier	Countries
1	United States, United Kingdom
2	Canada, France, Germany, Netherlands
3	Australia, Austria, Belgium, Denmark, Finland, Ireland, Italy, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland



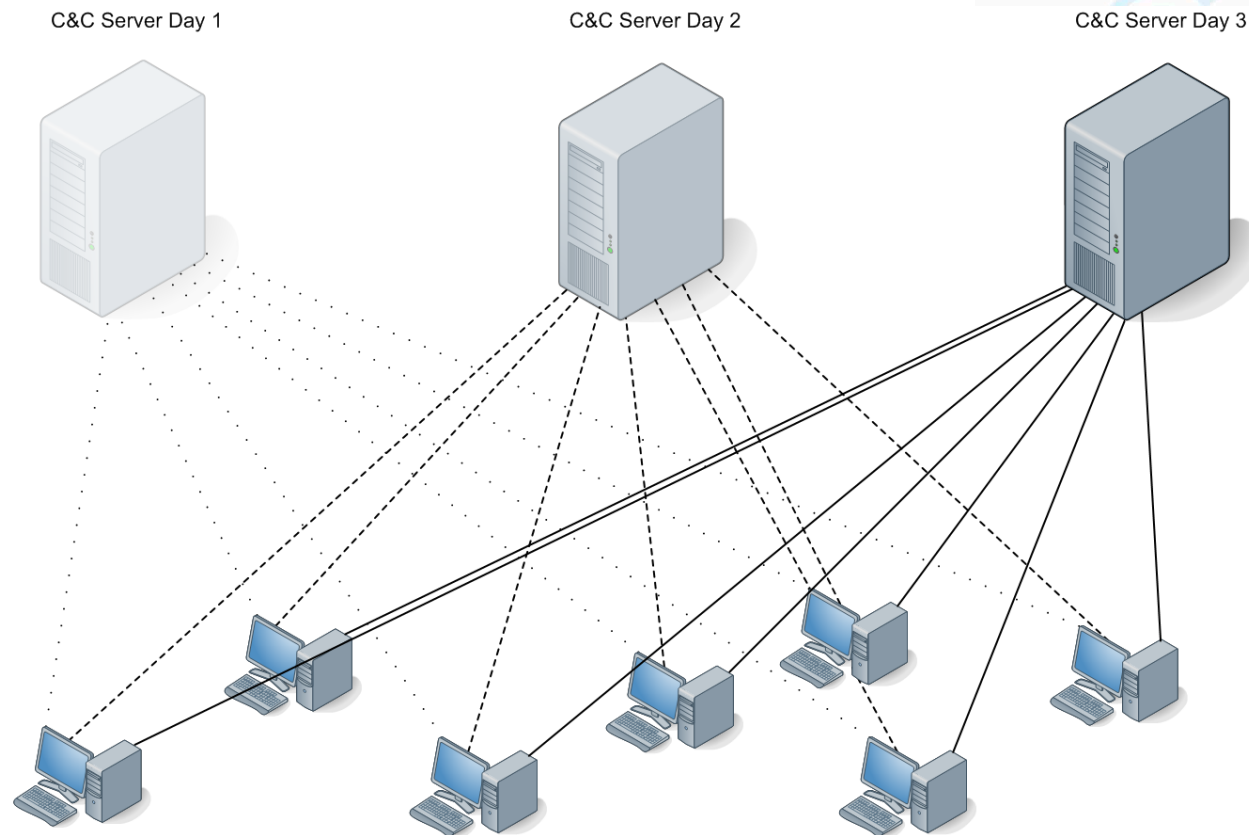
## Eksempel - centraliseret



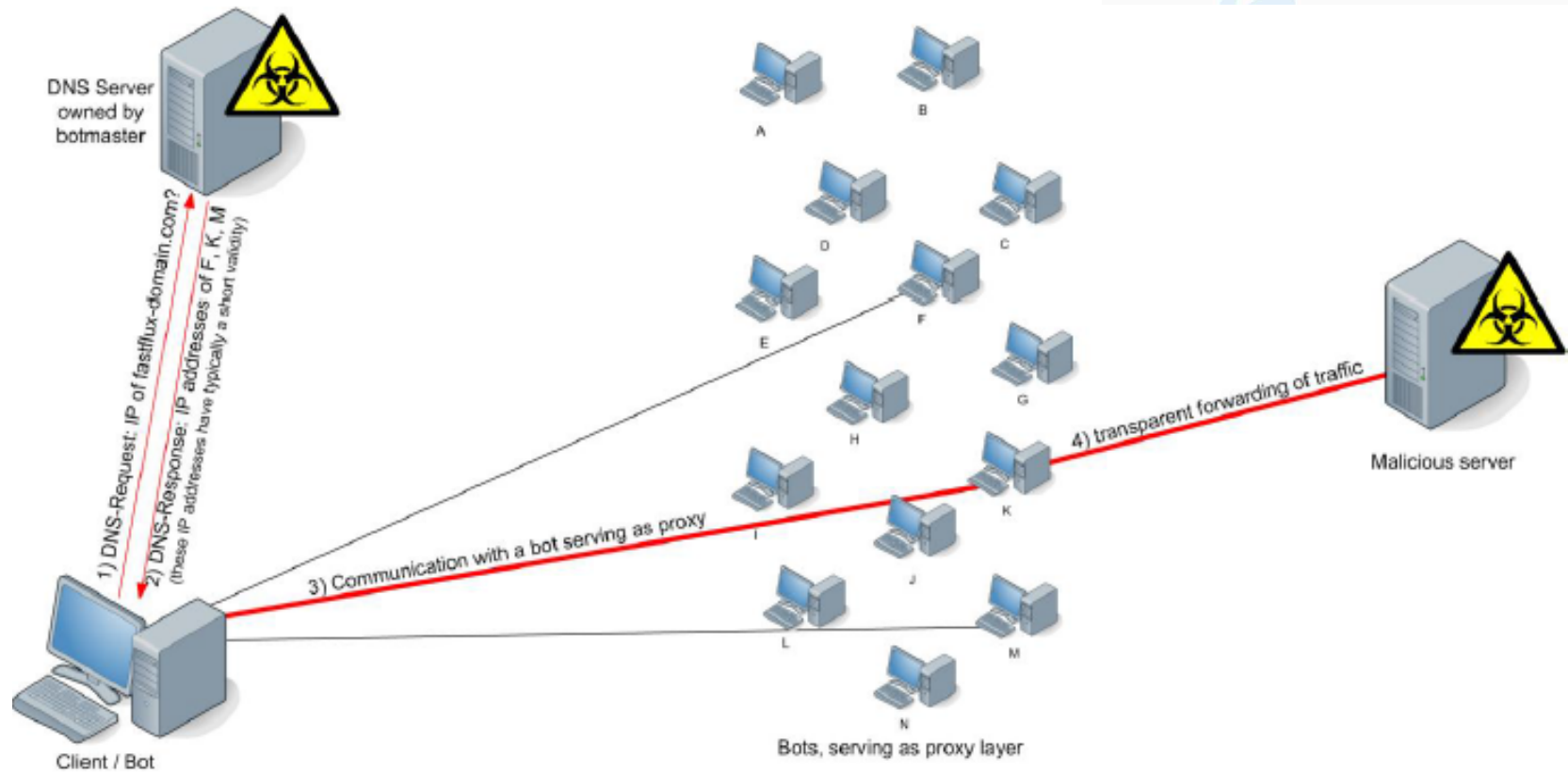
## Eksempel – peer2peer



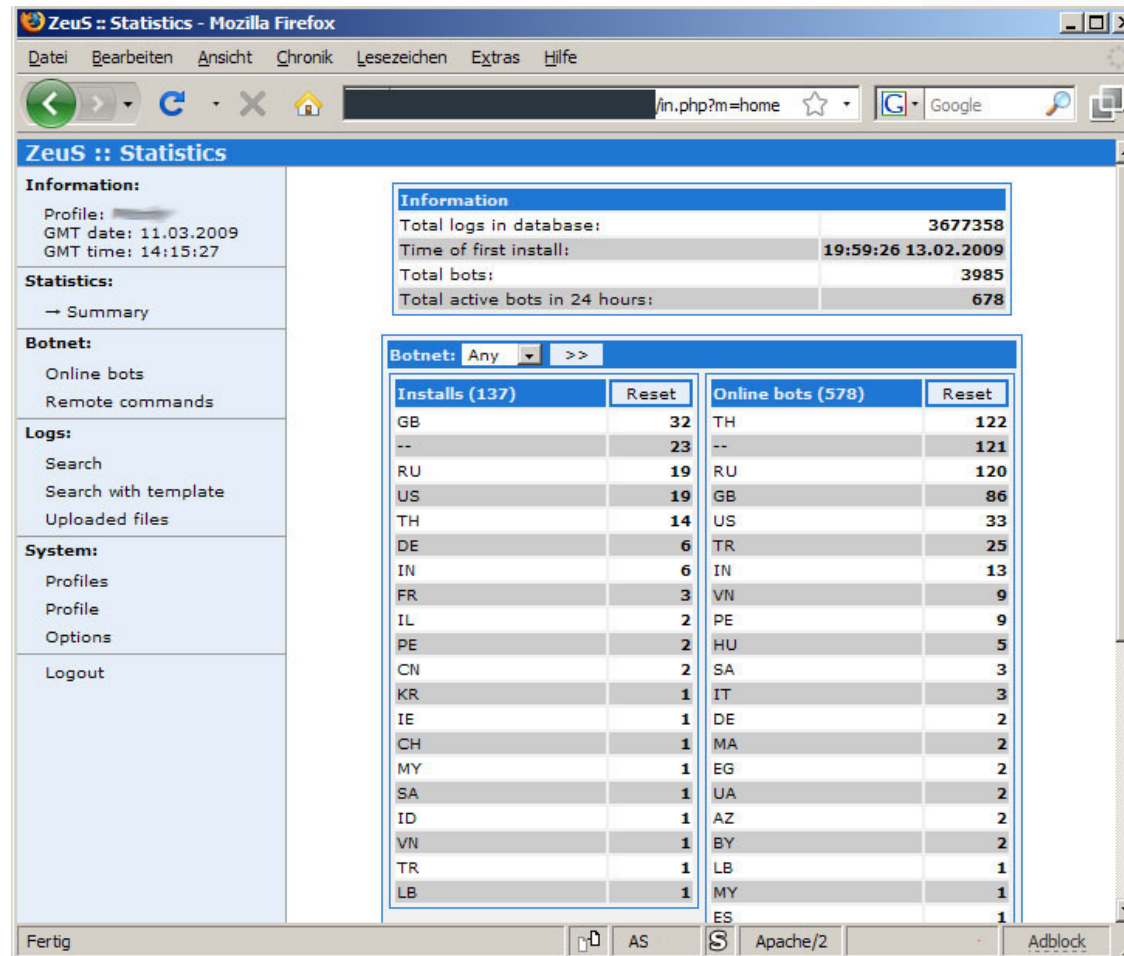
## Eksempel – Servere kan skifte ofte



# DNS kan også bruges til at gemme sig



# Example of Zeus User Interface (abuse.ch)



**Zeus :: Statistics**

**Information:**  
 Profile: ██████████  
 GMT date: 11.03.2009  
 GMT time: 14:15:27

**Statistics:**  
 → Summary

**Botnet:**  
 Online bots  
 Remote commands

**Logs:**  
 Search  
 Search with template  
 Uploaded files

**System:**  
 Profiles  
 Profile  
 Options  
 Logout

**Information**

Total logs in database:	3677358
Time of first install:	19:59:26 13.02.2009
Total bots:	3985
Total active bots in 24 hours:	678

Botnet: Any >>

Installs (137)		Online bots (578)	
	Reset		Reset
GB	32	TH	122
--	23	--	121
RU	19	RU	120
US	19	GB	86
TH	14	US	33
DE	6	TR	25
IN	6	IN	13
FR	3	VN	9
IL	2	PE	9
PE	2	HU	5
CN	2	SA	3
KR	1	IT	3
IE	1	DE	2
CH	1	MA	2
MY	1	EG	2
SA	1	UA	2
ID	1	AZ	2
VN	1	BY	2
TR	1	LB	1
LB	1	MY	1
		ES	1

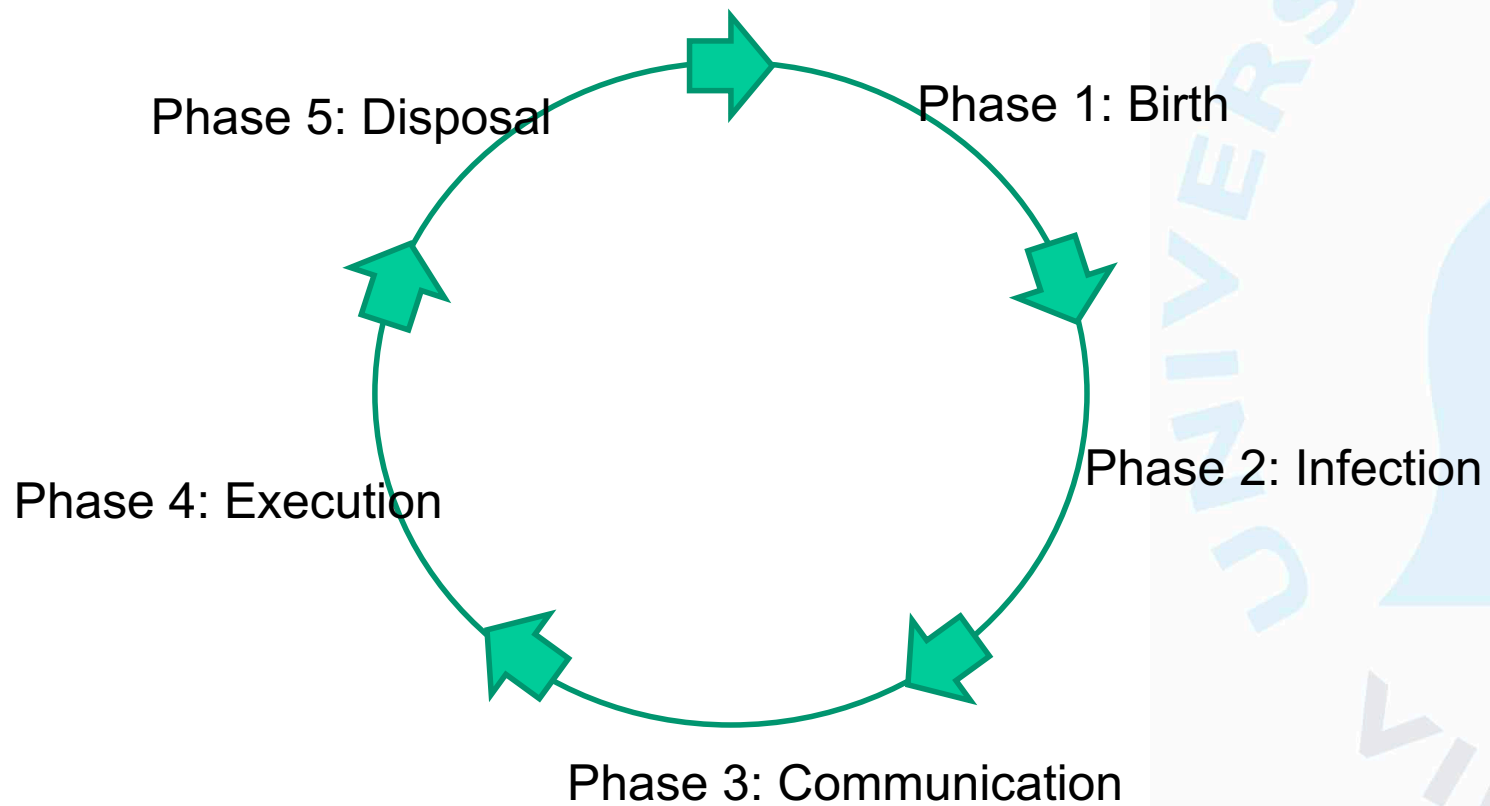
Fertig AS Apache/2 Adblock

# Example of Zeus User Interface (abuse.ch)

The screenshot shows the Zeus Bots user interface in a Mozilla Firefox browser window. The interface includes a navigation menu on the left, a filter box at the top right, and a main table displaying a list of bots. The table columns are: #, CompID, Ver/Botnet, IP, Country, Socks, Proxy, Screenshot, Kill OS, Online time, and Lag. The table contains 30 rows of bot information.

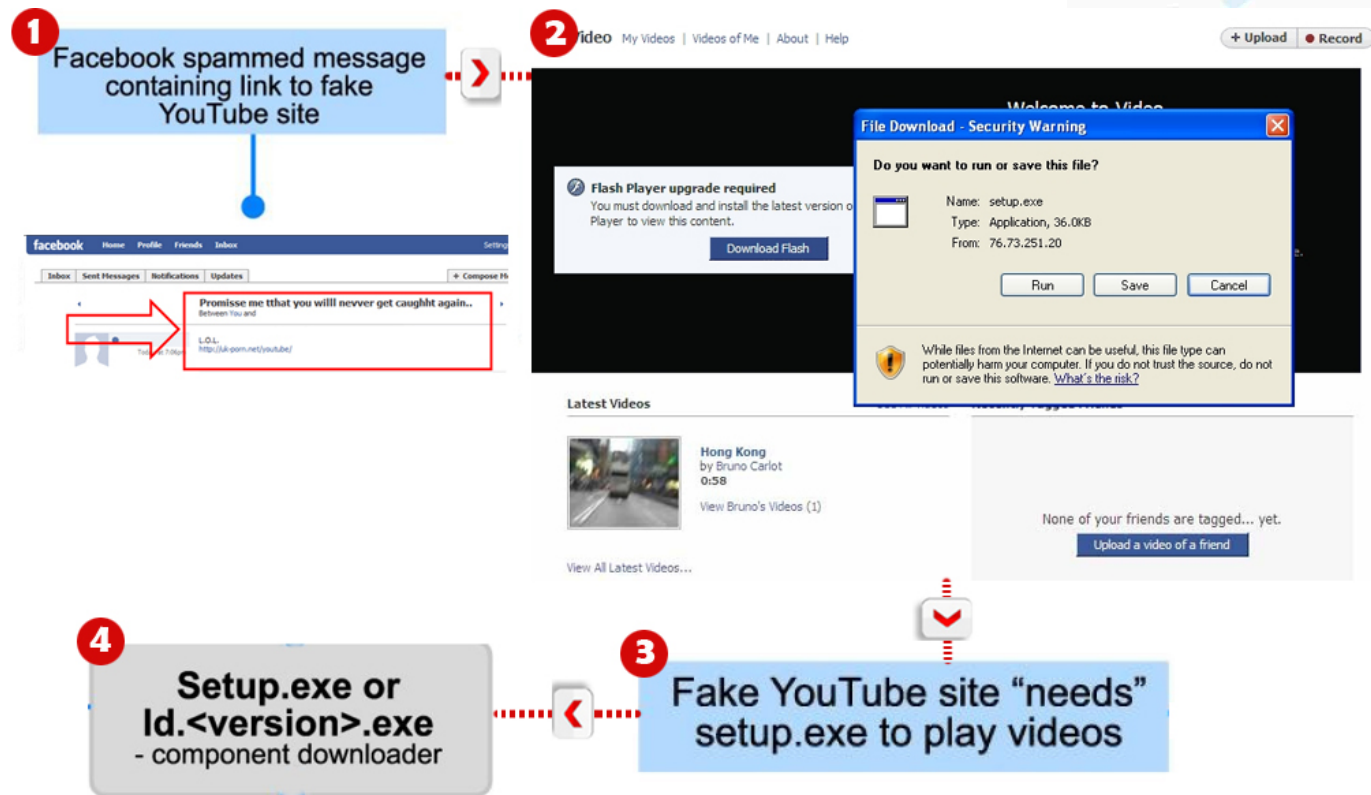
#	CompID	Ver/Botnet	IP	Country	Socks	Proxy	Screenshot	Kill OS	Online time	Lag
1	user_1d9ce10c45_01d6e996	1.1.1.0/main	213.139.225.55	RU	213.139.225.38345	213.139.225.10051	View	Kill	96:13:39	0.968
2	fic_000ebb9b	1.1.2.2/main	94.130.139.1025	--	94.130.139.1025	94.130.139.34451	View	Kill	96:32:47	0.765
3	family_01207eeb	1.1.2.2/main	86.130.139.1027	GB	86.130.139.1027	86.130.139.22093	View	Kill	98:58:44	0.328
4	d719sf2j_0019064f	1.1.2.2/main	87.130.139.1025	GB	87.130.139.1025	-	View	Kill	96:49:07	0.235
5	218_u_1_00ac3738	1.1.2.2/main	195.130.139.1025	RU	195.130.139.1025	195.130.139.10359	View	Kill	96:27:06	0.141
6	illusion_f2243e_00576c9d	1.1.2.2/main	124.130.139.1025	TH	124.130.139.1025	-	View	Kill	104:12:36	0.844
7	brian_ally_0228d16c	1.1.2.2/main	82.130.139.1027	GB	82.130.139.1027	-	View	Kill	97:49:55	0.313
8	telekit_7482b02_00b07900	1.1.2.2/main	94.130.139.1025	--	94.130.139.1025	94.130.139.33846	View	Kill	98:00:42	0.157
9	your_jaxvxzedk_00a364bc	1.1.2.2/main	82.130.139.1025	GB	82.130.139.1025	-	View	Kill	96:10:44	26.75
10	home_881b31b48d_00170f87	1.1.2.2/main	58.130.139.1048	TH	58.130.139.1048	58.130.139.32353	View	Kill	103:14:13	1.042
11	your_	1.1.2.2/main	68.130.139.1025	--	68.130.139.1025	68.130.139.17992	View	Kill	104:12:03	0.578
12	blackxp_000325d8	1.1.2.2/main	124.130.139.1025	TH	-	124.130.139.47:37760	-	-	98:38:15	0.187
13	b154bc1afca840e_00397f1d	1.1.2.2/main	77.130.139.1027	RU	77.130.139.1027	77.130.139.14804	View	Kill	104:11:25	0.078
14	xp_0051dba0	1.1.2.2/main	58.130.139.1025	TH	58.130.139.1025	58.130.139.37112	View	Kill	97:37:17	3.938
15	desktop_02659af2	1.1.2.2/main	190.130.139.1025	AR	190.130.139.1025	190.130.139.32639	View	Kill	107:20:49	0.657
16	davie_0085eb43	1.1.2.2/main	62.130.139.1036	GB	62.130.139.1036	62.130.139.37719	View	Kill	96:34:49	0.188
17	i_d07192a7a4944_0025f597	1.1.2.2/main	95.130.139.1026	--	95.130.139.1026	95.130.139.10385	View	Kill	100:53:01	3.25
18	microsof_886bea_01bd77ea	1.1.2.2/main	92.130.139.1025	--	92.130.139.1025	92.130.139.10278	View	Kill	96:36:01	3.266
19	mircik_00069abc	1.1.2.2/main	193.80.139.1025	SK	193.80.139.1025	193.80.139.2664	View	Kill	96:41:51	0.187
20	ammo_00135651	1.1.2.2/main	82.130.139.1025	GB	82.130.139.1025	82.130.139.15589	View	Kill	96:31:56	0.156
21	freedom_867dc59_000050cf	1.1.2.2/main	82.130.139.1027	RU	82.130.139.1027	-	View	Kill	98:18:30	0.078
22	pc_fec662b1943d_00153eae	1.1.2.2/main	86.130.139.1027	GB	86.130.139.1027	-	View	Kill	104:11:26	0.15
23	pen_003f0760	1.1.2.2/main	95.130.139.1025	--	95.130.139.1025	95.130.139.31003	View	Kill	96:39:22	0.312
24	home_	1.1.2.2/main	24.130.139.54537	--	24.130.139.54537	24.130.139.27755	View	Kill	104:12:37	0.624
25	bsaftpz_7e2bb74_017743b0	1.1.2.2/main	89.130.139.1025	HU	89.130.139.1025	89.130.139.18514	View	Kill	97:55:18	0.266
26	client_df77fa69_0d6210d8	1.1.2.2/main	89.130.139.1025	RO	89.130.139.1025	89.130.139.38462	View	Kill	96:14:16	0.701
27	acer_4d30879900_004dca2	1.1.2.2/main	202.130.139.1027	TH	-	202.130.139.25983	-	-	97:16:11	0
28	abc_67365a4e5b6_00204191	1.1.2.2/main	115.130.139.1027	--	115.130.139.1027	115.130.139.34129	View	Kill	98:45:29	8.437
29	skz_fd19c55e0a2_003d5664	1.1.2.2/main	61.130.139.1025	TH	61.130.139.1025	61.130.139.35502	View	Kill	96:32:12	10.016
30	compas2510b_2_00010c5d	1.1.2.2/main	67.214.139.205	DE	67.214.139.205	67.214.139.49883	View	Kill	06:25:17	6.234

# BotNet Lifecycle



# Noget om infektioner

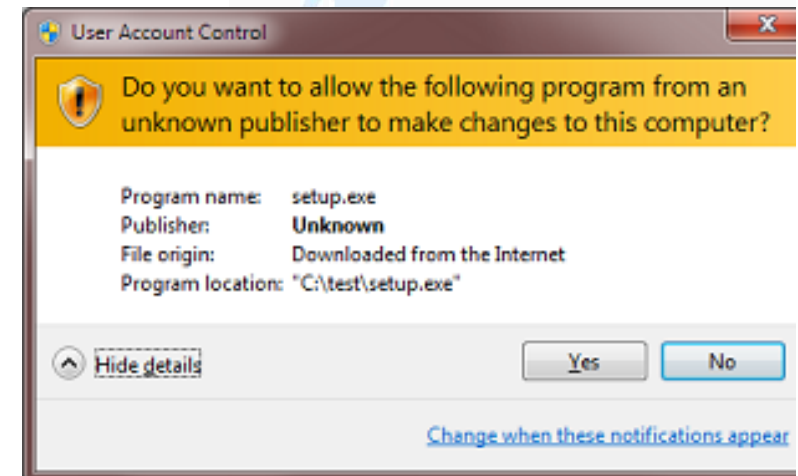
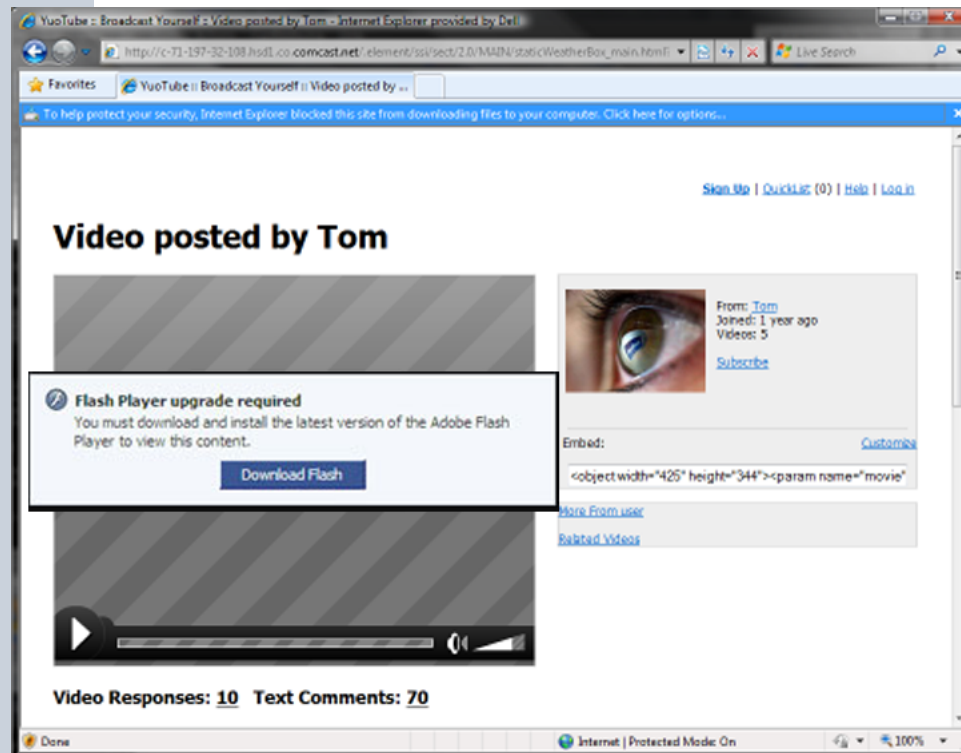
- Users – Social Engineering





# Noget om infektioner

- Users – Social Engineering



## According to Norton...

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

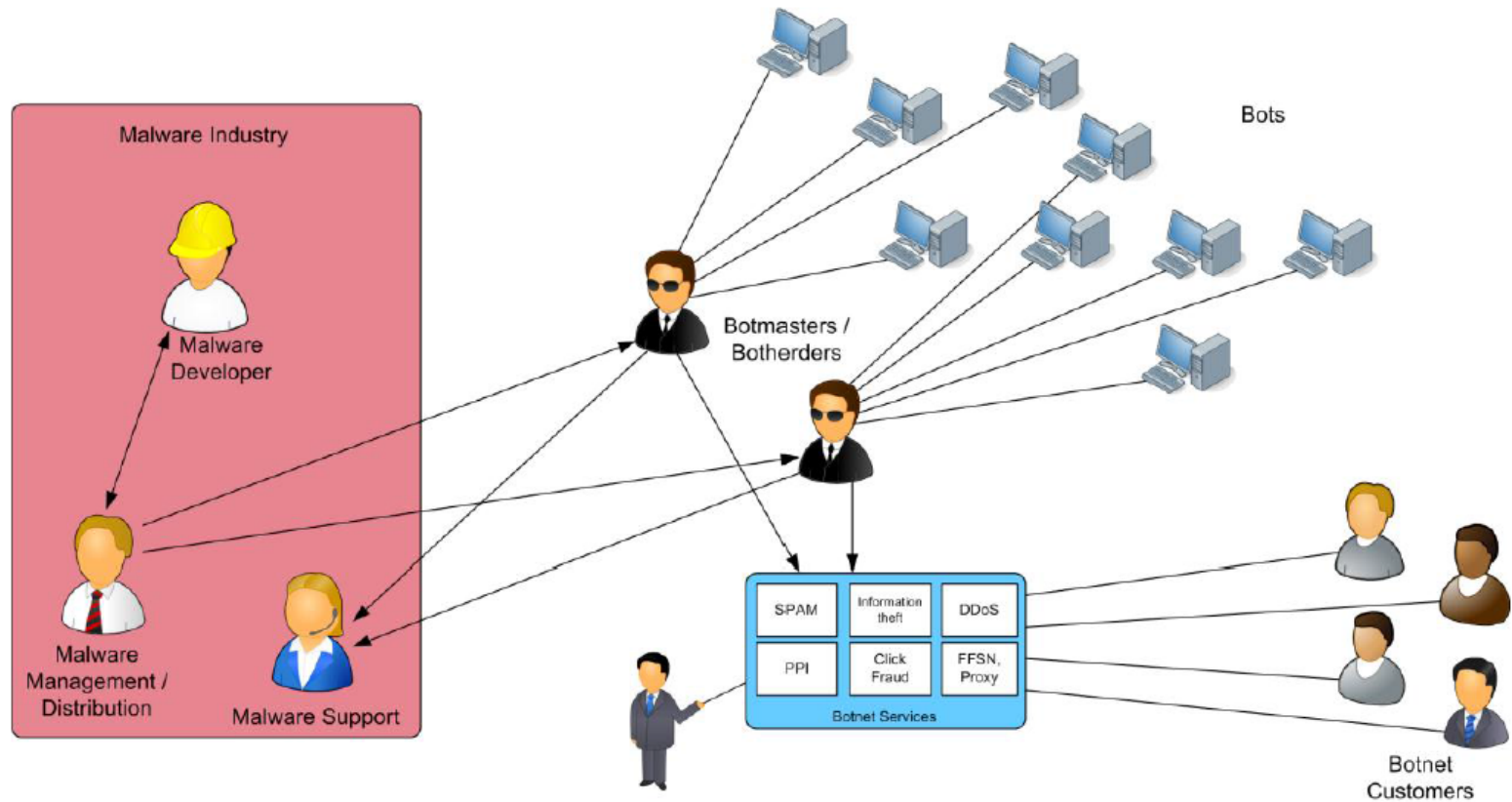


**One in three** do not have a password on their smartphone or desktop computer at all!

## 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

The screenshot shows a browser window with the URL `onion/p/cjAt3Vj0dt`. The page is from 'Agora Beta' and displays a listing for 'Botnet Setup' for 0.16089108 BTC. The listing includes a list of services such as a .ru domain, offshore hosting, and FUD Crypt. A 'BUY...' button is visible at the bottom right of the listing. The left sidebar contains a search bar and a list of service categories like Hacking, Money, and Counterfeits.

Botnet Setup

0.16089108 BTC  
Can setup your own botnet

- 1 year .ru domain
- 1 year offshore hosting
- 1 FUD Crypt
- Some free bots to get you started
- LTC (GPU+CPU) miner if you want to start mining

Brought to you by:  
Dipsy 4.8/5, 10-15 deals

From: Torland

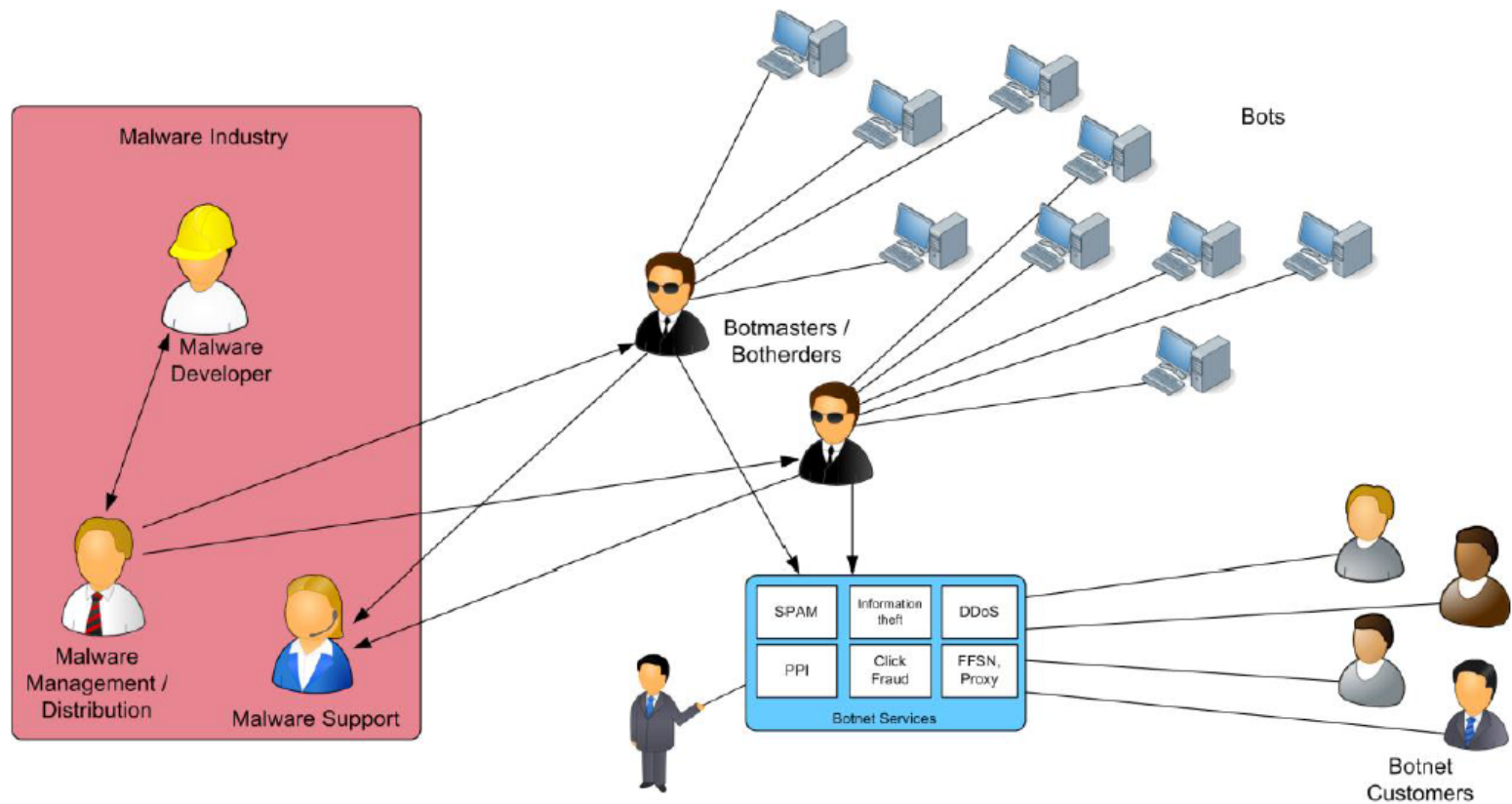
0.16089108 BTC

**Feedbacks:**  
No feedbacks found.

[BUY...](#)

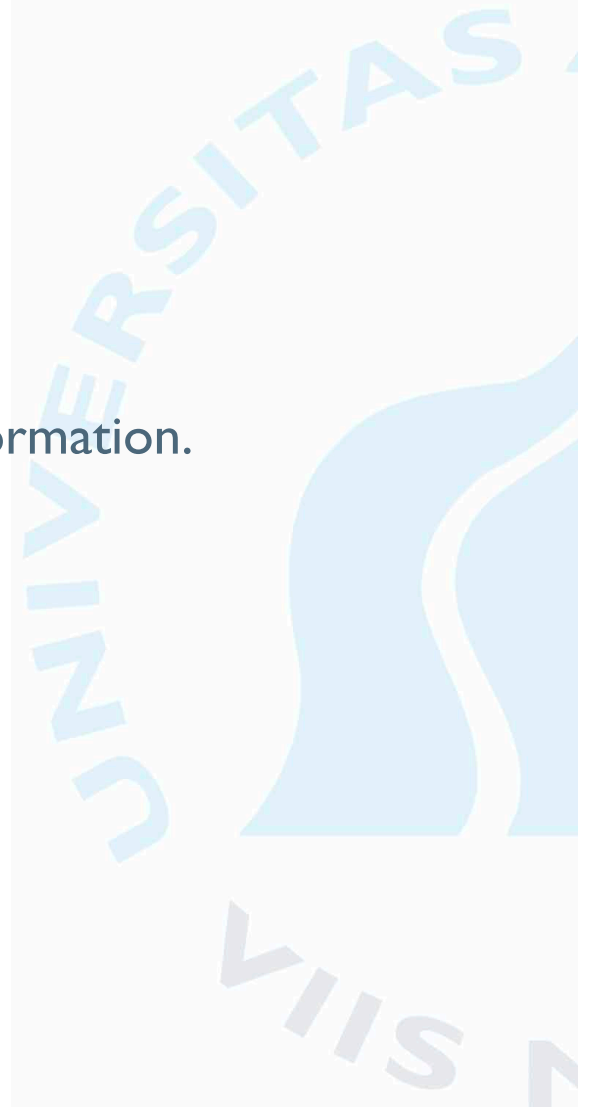
# Botnets – ren business

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



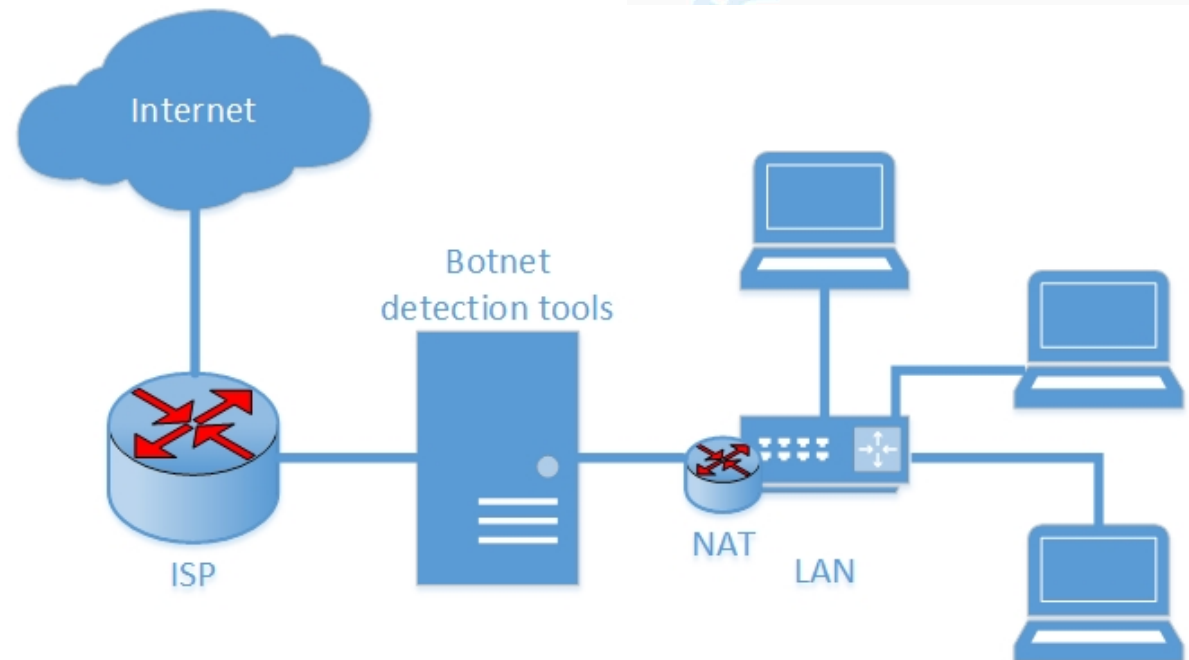
## Zeus – King of Bots

- 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...

No.	Time	Source	Destination	Protocol	Length	Info
717	31.546926	10.1.1.37	192.168.236.12	DNS	76	Standard query 0x8834 A www.msftncsi.com
718	31.590503	192.168.236.12	10.1.1.37	DNS	181	Standard query response 0x8834 A www.msftncsi.com CNAME www.msftnc...
719	31.593970	10.1.1.37	93.158.110.210	TCP	66	49188 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
720	31.644018	93.158.110.210	10.1.1.37	TCP	66	80 → 49188 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PE...
721	31.644287	10.1.1.37	93.158.110.210	TCP	60	49188 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
722	31.644515	10.1.1.37	93.158.110.210	HTTP	151	GET /ncsi.txt HTTP/1.1
723	31.653959	10.1.1.37	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
724	31.669446	10.1.1.37	157.56.77.156	TCP	178	[TCP Retransmission] 49187 → 443 [PSH, ACK] Seq=1 Ack=1 Win=65392 ...
725	31.693979	93.158.110.210	10.1.1.37	TCP	54	80 → 49188 [ACK] Seq=1 Ack=98 Win=14600 Len=0
726	31.694154	93.158.110.210	10.1.1.37	HTTP	233	HTTP/1.1 200 OK (text/plain)
727	31.694174	93.158.110.210	10.1.1.37	TCP	54	80 → 49188 [FIN, ACK] Seq=180 Ack=98 Win=14600 Len=0
728	31.694295	10.1.1.37	93.158.110.210	TCP	60	49188 → 80 [ACK] Seq=98 Ack=181 Win=65280 Len=0
729	31.694403	10.1.1.37	93.158.110.210	TCP	60	49188 → 80 [FIN, ACK] Seq=98 Ack=181 Win=65280 Len=0
730	31.696849	10.1.1.37	192.168.236.12	DNS	77	Standard query 0x275c A ipv6.msftncsi.com
731	31.729422	192.168.236.12	10.1.1.37	DNS	214	Standard query response 0x275c A ipv6.msftncsi.com CNAME ipv6.msft...
732	31.743541	93.158.110.210	10.1.1.37	TCP	54	80 → 49188 [ACK] Seq=181 Ack=99 Win=14600 Len=0
733	31.945994	10.1.1.37	173.194.65.156	TCP	60	49183 → 80 [RST, ACK] Seq=282 Ack=1 Win=0 Len=0
734	31.947916	10.1.1.37	192.168.236.12	DNS	72	Standard query 0xd551 A stanford.edu
735	31.986911	192.168.236.12	10.1.1.37	DNS	325	Standard query response 0xd551 A stanford.edu A 171.67.215.200 NS ...
736	31.988193	10.1.1.37	171.67.215.200	TCP	66	49190 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
737	31.988218	10.1.1.37	171.67.215.200	TCP	66	49189 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
738	32.192819	171.67.215.200	10.1.1.37	TCP	66	80 → 49190 [SYN, ACK] Seq=0 Ack=1 Win=4080 Len=0 MSS=1460 WS=1 SAC...
739	32.193118	10.1.1.37	171.67.215.200	TCP	60	49190 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
740	32.193380	10.1.1.37	171.67.215.200	HTTP	294	GET / HTTP/1.1
741	32.193647	171.67.215.200	10.1.1.37	TCP	66	80 → 49189 [SYN, ACK] Seq=0 Ack=1 Win=4080 Len=0 MSS=1460 WS=1 SAC...
742	32.193863	10.1.1.37	171.67.215.200	TCP	60	49189 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
743	32.410324	171.67.215.200	10.1.1.37	HTTP	1414	HTTP/1.1 200 OK [Malformed Packet]
0000	68 05 ca 0f 74 1b 00 30 05 97 57 16 08 00 45 00					h...t..0 ..W...E.
0010	00 42 02 05 00 00 80 11 80 cb 0a 01 01 25 c0 a8					.B..... ..%..
0020	ec 0c f6 3c 00 35 00 2e 62 cd bb f4 01 00 00 01					...<.5.. b.....
0030	00 00 00 00 00 00 06 75 70 64 61 74 65 09 6d 69					.....u pdate.mi
0040	63 72 6f 73 6f 66 74 03 63 6f 6d 00 00 01 00 01					crosoft. com.....

# Eksempler på hvad vi ser...

No.	Time	Source	Destination	Protocol	Length	Info
3852	73.715382	fe80::6d84:d710:c6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
3853	73.950742	10.1.1.37	192.168.236.12	DNS	76	Standard query 0xa729 A dns.msftncsi.com
3854	73.983286	192.168.236.12	10.1.1.37	DNS	92	Standard query response 0xa729 A dns.msftncsi.com A 131.107.255.255
3855	76.715308	fe80::6d84:d710:c6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
3856	78.600818	10.1.1.37	204.79.197.200	TCP	60	49223 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3857	78.600846	10.1.1.37	204.79.197.200	TCP	60	49224 → 80 [RST, ACK] Seq=202 Ack=1 Win=0 Len=0
3858	80.715451	fe80::6d84:d710:c6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
3859	83.715317	fe80::6d84:d710:c6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
3860	86.208567	10.1.1.37	192.168.236.12	DNS	80	Standard query 0xf124 A killa.darkforces.biz
3861	86.209211	10.1.1.37	192.168.236.12	DNS	75	Standard query 0xddcd A www.schlund.net
3862	86.331092	192.168.236.12	10.1.1.37	DNS	142	Standard query response 0xf124 No such name A killa.darkforces.biz...
3863	86.422414	192.168.236.12	10.1.1.37	DNS	139	Standard query response 0xddcd No such name A www.schlund.net SOA ...
3864	86.423435	10.1.1.37	10.1.1.255	NBNS	92	Name query NB WWW.SCHLUND.NET<00>
3865	86.715309	fe80::6d84:d710:c6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
3866	87.168222	10.1.1.37	10.1.1.255	NBNS	92	Name query NB WWW.SCHLUND.NET<00>
3867	87.918226	10.1.1.37	10.1.1.255	NBNS	92	Name query NB WWW.SCHLUND.NET<00>
3868	88.669443	10.1.1.37	192.168.236.12	DNS	74	Standard query 0x8b01 A www.utwente.nl
3869	88.757958	192.168.236.12	10.1.1.37	DNS	240	Standard query response 0x8b01 A www.utwente.nl CNAME webhare.civ...
3870	88.758892	10.1.1.37	130.89.3.249	TCP	66	49227 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3871	88.811582	130.89.3.249	10.1.1.37	TCP	66	80 → 49227 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PE...
3872	88.811887	10.1.1.37	130.89.3.249	TCP	60	49227 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
3873	88.813056	10.1.1.37	130.89.3.249	TCP	1078	[TCP segment of a reassembled PDU]
3874	88.813170	10.1.1.37	130.89.3.249	TCP	1514	[TCP segment of a reassembled PDU]
3875	88.867085	130.89.3.249	10.1.1.37	TCP	54	80 → 49227 [ACK] Seq=1 Ack=1025 Win=16768 Len=0
3876	88.867365	10.1.1.37	130.89.3.249	TCP	1514	[TCP segment of a reassembled PDU]
3877	88.867379	10.1.1.37	130.89.3.249	TCP	1078	[TCP segment of a reassembled PDU]
3878	88.914030	130.89.3.249	10.1.1.37	TCP	66	[TCP Dup ACK 3875#1] 80 → 49227 [ACK] Seq=1 Ack=1025 Win=16768 Len...
0000	68 05 ca 0f 74 1b 00 30 05 97 57 16 08 00 45 00					h...t..0 ..W...E.
0010	00 42 02 05 00 00 80 11 80 cb 0a 01 01 25 c0 a8					.B..... ..%..
0020	ec 0c f6 3c 00 35 00 2e 62 cd bb f4 01 00 00 01					...<.5. b.....
0030	00 00 00 00 00 00 06 75 70 64 61 74 65 09 6d 69					.....u pdate.mi
0040	63 72 6f 73 6f 66 74 03 63 6f 6d 00 00 01 00 01					crosoft. com.....

# Eksempler på hvad vi ser...

No.	Time	Source	Destination	Protocol	Length	Info
4861	119.441008	fe80::6d84:d710:c6...	ff02::1:3	LLMNR	84	Standard query 0xd9b2 A wpad
4862	119.441461	10.1.1.37	224.0.0.252	LLMNR	64	Standard query 0xd9b2 A wpad
4863	119.542362	fe80::6d84:d710:c6...	ff02::1:3	LLMNR	84	Standard query 0xd9b2 A wpad
4864	119.542493	10.1.1.37	224.0.0.252	LLMNR	64	Standard query 0xd9b2 A wpad
4865	119.746080	10.1.1.37	10.1.1.255	NBNS	92	Name query NB WPAD<00>
4866	120.042230	10.1.1.37	207.155.248.73	TCP	60	49230 → 80 [RST, ACK] Seq=537 Ack=1 Win=0 Len=0
4867	120.043027	10.1.1.37	192.168.236.12	DNS	76	Standard query 0xea75 A www.stanford.edu
4868	120.363575	192.168.236.12	10.1.1.37	DNS	329	Standard query response 0xea75 A www.stanford.edu A 171.67.215.200...
4869	120.364584	10.1.1.37	171.67.215.200	TCP	62	49233 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
4870	120.495415	10.1.1.37	10.1.1.255	NBNS	92	Name query NB WPAD<00>
4871	120.568628	171.67.215.200	10.1.1.37	TCP	62	80 → 49233 [SYN, ACK] Seq=0 Ack=1 Win=4080 Len=0 MSS=1460 SACK_PER...
4872	120.568876	10.1.1.37	171.67.215.200	TCP	60	49233 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4873	120.569801	10.1.1.37	171.67.215.200	TCP	1078	[TCP segment of a reassembled PDU]
4874	120.569914	10.1.1.37	171.67.215.200	TCP	1514	[TCP segment of a reassembled PDU]
4875	120.714547	fe80::6d84:d710:c6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
4876	120.876241	171.67.215.200	10.1.1.37	TCP	54	80 → 49233 [ACK] Seq=1 Ack=1025 Win=5104 Len=0
4877	120.876535	10.1.1.37	171.67.215.200	TCP	1514	[TCP segment of a reassembled PDU]
4878	120.876563	10.1.1.37	171.67.215.200	TCP	1078	[TCP segment of a reassembled PDU]
4879	121.087019	171.67.215.200	10.1.1.37	TCP	66	[TCP Dup ACK 4876#1] 80 → 49233 [ACK] Seq=1 Ack=1025 Win=5104 Len=...
4880	121.245445	10.1.1.37	10.1.1.255	NBNS	92	Name query NB WPAD<00>
4881	121.495331	10.1.1.37	171.67.215.200	TCP	1514	[TCP Retransmission] 49233 → 80 [PSH, ACK] Seq=1025 Ack=1 Win=6424...
4882	122.745333	10.1.1.37	171.67.215.200	TCP	1514	[TCP Retransmission] 49233 → 80 [PSH, ACK] Seq=1025 Ack=1 Win=6424...
4883	123.714209	fe80::6d84:d710:c6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
4884	125.245256	10.1.1.37	171.67.215.200	TCP	590	[TCP Retransmission] 49233 → 80 [ACK] Seq=1025 Ack=1 Win=64240 Len=...
4885	125.453547	171.67.215.200	10.1.1.37	TCP	66	80 → 49233 [ACK] Seq=1 Ack=1561 Win=5640 Len=0 SLE=3945 SRE=4969
4886	125.453816	10.1.1.37	171.67.215.200	TCP	590	[TCP Retransmission] 49233 → 80 [PSH, ACK] Seq=1561 Ack=1 Win=6424...
4887	125.453841	10.1.1.37	171.67.215.200	TCP	590	[TCP Retransmission] 49233 → 80 [ACK] Seq=2097 Ack=1 Win=64240 Len=...
4888	125.665477	171.67.215.200	10.1.1.37	TCP	66	80 → 49233 [ACK] Seq=1 Ack=2097 Win=5136 Len=0 SLE=3945 SRE=4969
0000	68 05 ca 0f 74 1b 00 30 05 97 57 16 08 00 45 00			h...t..0 ..W...E.		
0010	00 42 02 05 00 00 80 11 80 cb 0a 01 01 25 c0 a8			.B.....%..		
0020	ec 0c f6 3c 00 35 00 2e 62 cd bb f4 01 00 00 01			...<.5.. b.....		
0030	00 00 00 00 00 00 06 75 70 64 61 74 65 09 6d 69			.....u pdate.mi		
0040	63 72 6f 73 6f 66 74 03 63 6f 6d 00 00 01 00 01			crosoft. com.....		

agobot-ee-test2

Packets: 8016 · Displayed: 8016 (100.0%) · Load time: 0:0.108 Profile: Default

## 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 business.
- 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 præcist 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](mailto:jens@es.aau.dk)

