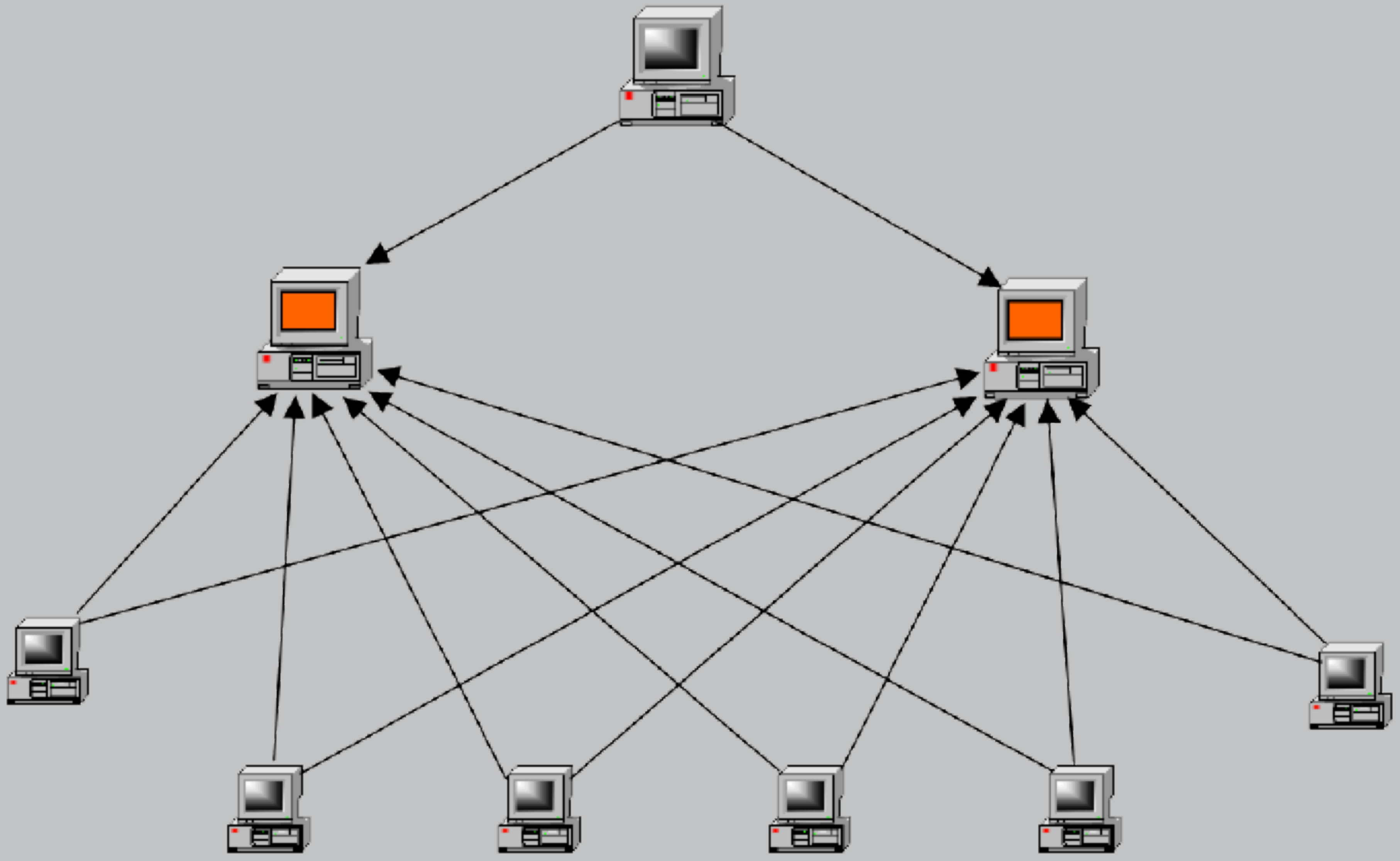
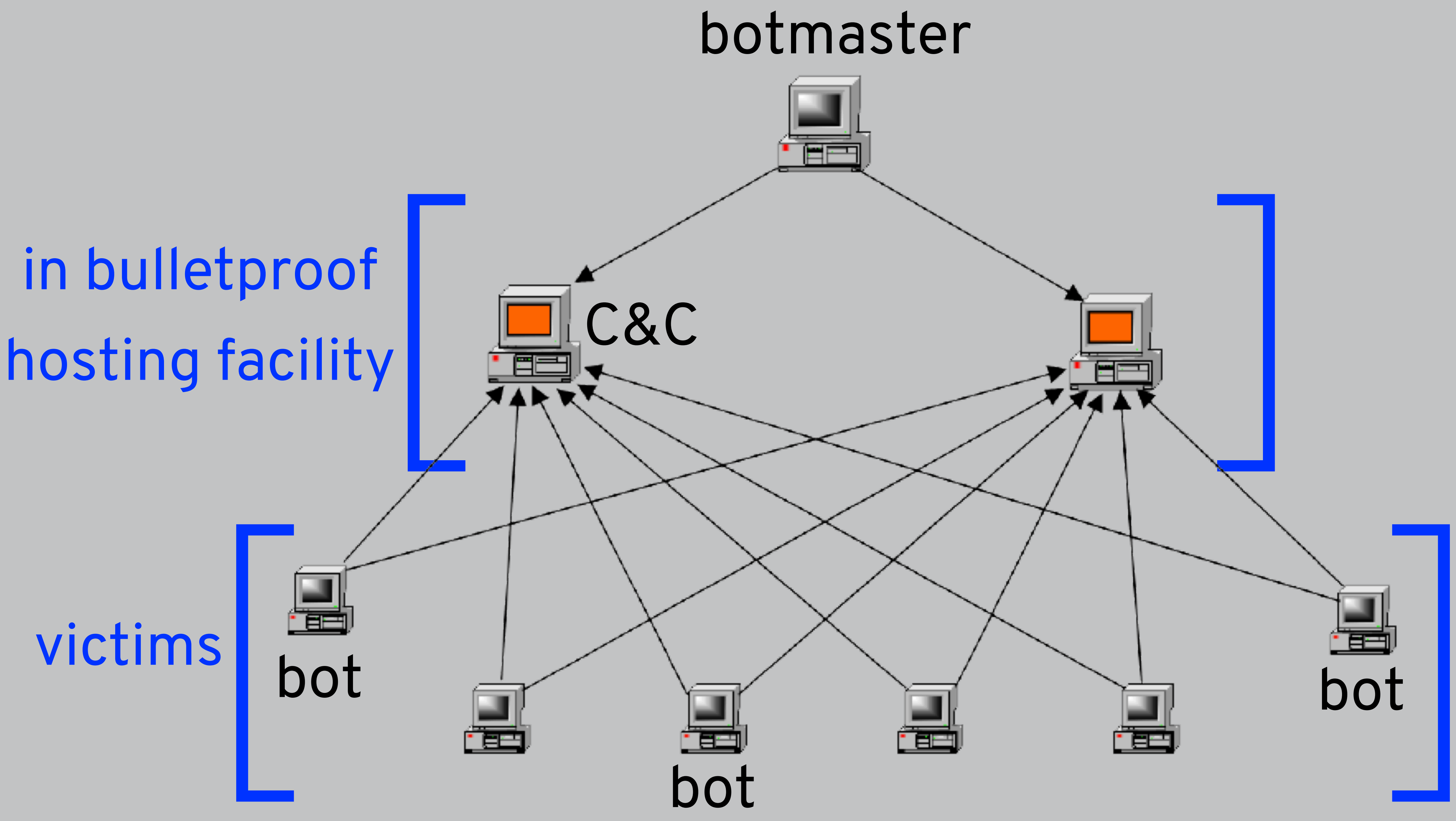
SECURITY (COMP0141): BOTNETS

BOTNETS



BOTNET TOPOLOGY

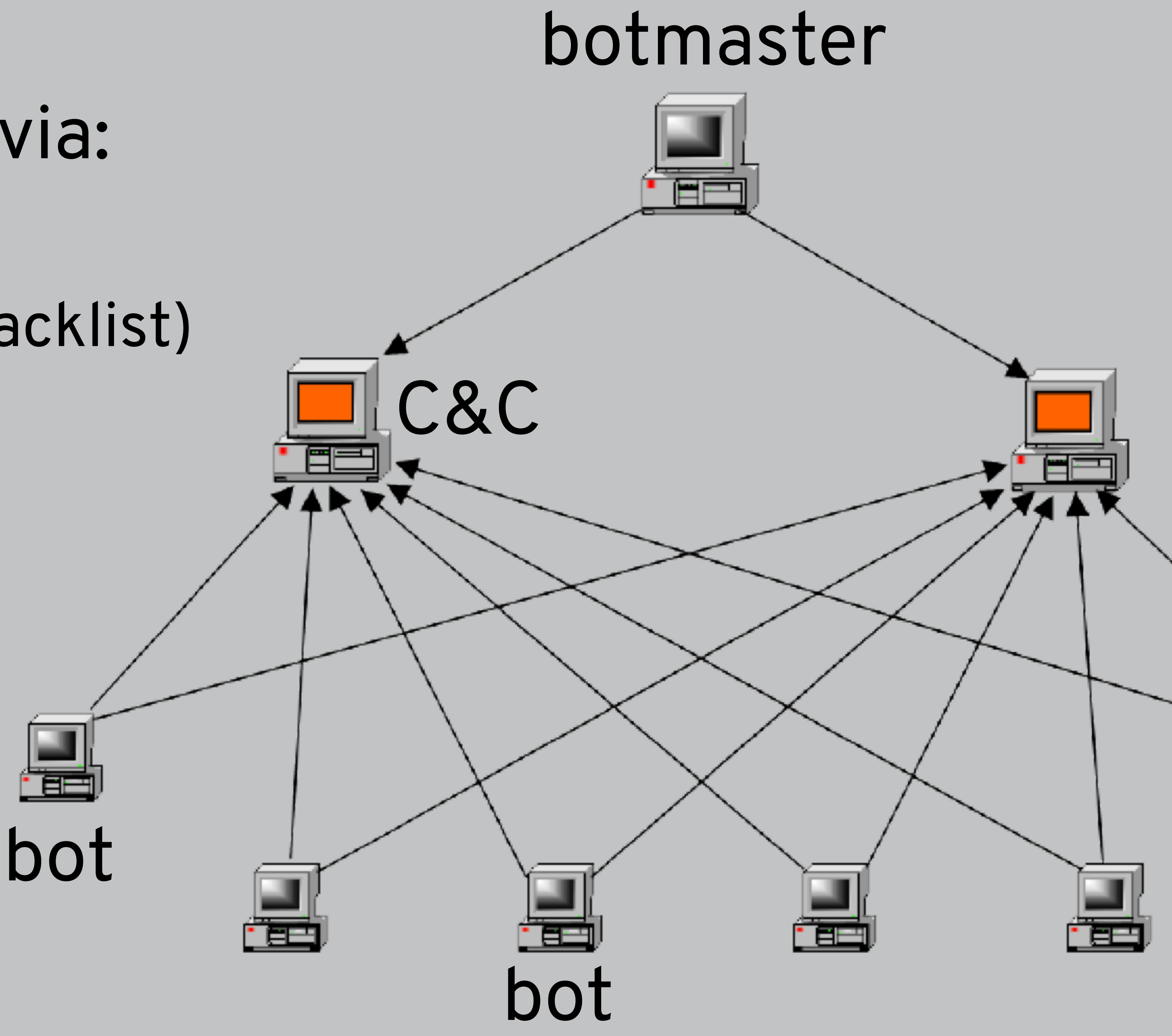


BOTNET ORGANISATION

communication takes place via:

-IRC (easy to infiltrate)

-proprietary channels (easy to blacklist)



HONEYPOTS

A **honeypot** is designed to be highly attractive to an attacker

- unlocked car with keys in the ignition
- computer with unpatched OS, old browser version, etc.

Operated to find out more information about them (IP address, location, etc.) or provide enough evidence to report

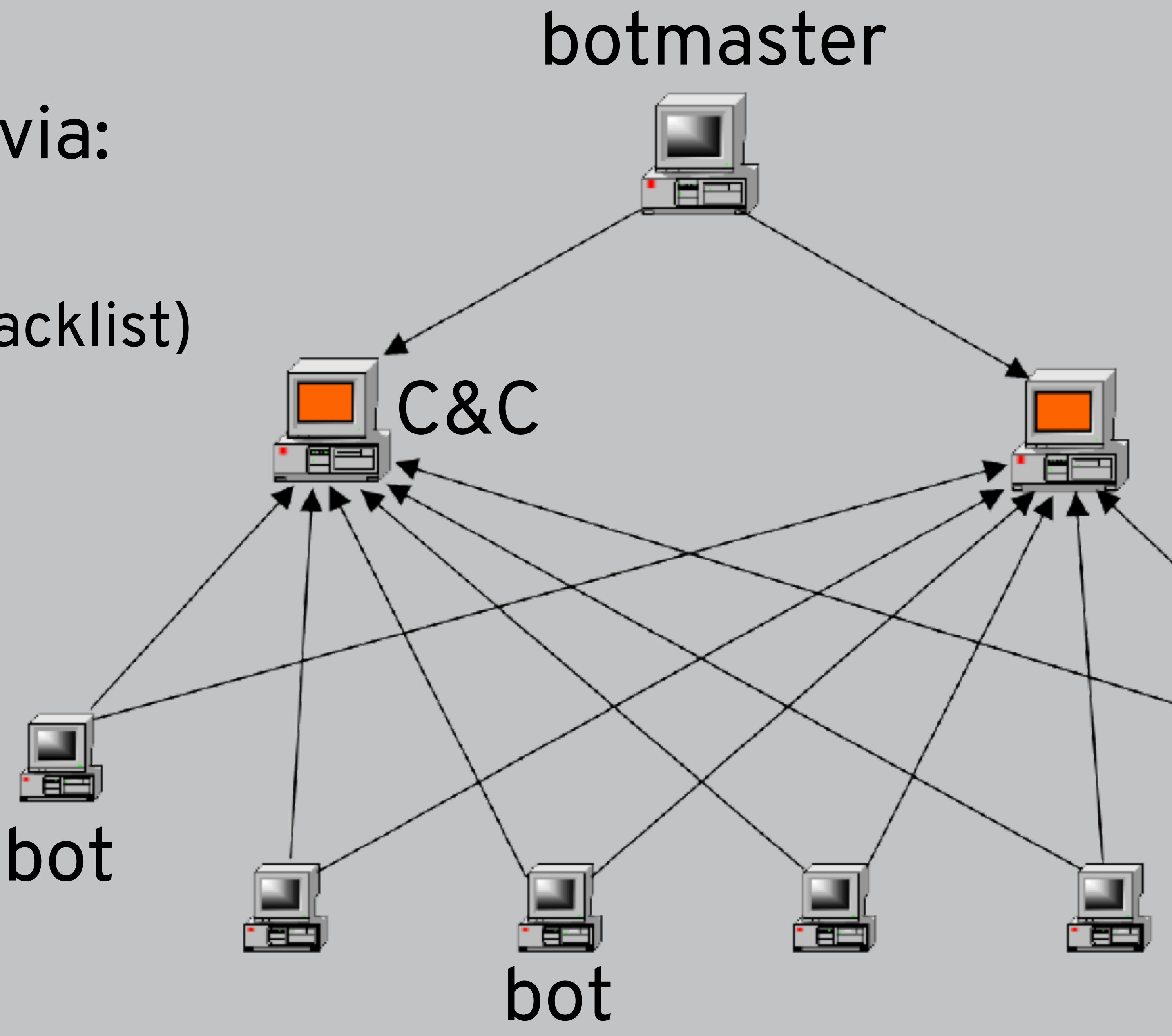
BOTNET ORGANISATION

communication takes place via:

- IRC (easy to infiltrate)
- proprietary channels (easy to blacklist)

structure uses:

- multiple tiers (expensive)
- p2p (easy to infiltrate)
- fast flux/domain flux (hard!)



EXAMPLES

Grum

-shut down in 2012

-500-900K infected

ZeroAccess

-shut down in 2013

-2M infected

Cutwail

-shut down in 2010

-1.5-2M infected

Storm

-peak in 2007

-1-50M infected

BUSINESS MODEL

q: but how do booter services work? how to do it myself?

a: use a **botnet.**

q: what is the monetary point of creating a botnet?

a: DDoS as a service, **click fraud, spam.**

PAY PER CLICK

Pay-per-click (PPC) advertising means advertiser (Alice) pays publisher every time the ad is clicked

Coming this fall...

Worth its wait in wonders!

Walt Disney's Alice in Wonderland will be your happiest experience in years!

To bring happiness is the greatest of all arts.

And in this, Walt Disney is the master—the painter of laughter on the lips of mankind.

Now he has lavished his talents on a masterpiece, selecting for it an immortal from among the world's most treasured favorites—Lewis Carroll's beloved Alice in Wonderland.

Walt Disney has created a new world of wonderment. So brilliant is its enchantment, so beguiling are its people, so fascinating is its beauty that it will take you beyond known horizons of entertainment.

Here are the Mad Hatter, the March Hare, the Cheshire Cat, the White Rabbit, the Walrus and the Carpenter—all the fantastic funny-folk who make Wonderland an unforgettably joyous experience for everyone.

Bewitched by it all, as is Alice herself, you'll enter a realm of colorful radiance, where hearts are filled with laughter and the air filled with music.

Even before you see Alice in Wonderland you'll be hearing—and humming "All in a Golden Afternoon," "Very Good Advice," "The Unbirthday Song," "I'm Late," and many other captivating melodies.

Alice in Wonderland is nearing completion, and you'll see it this Fall.

This is Walt Disney's triumph!

Walt Disney's

ALICE in WONDERLAND

The All-Cartoon Musical Wonder-Film

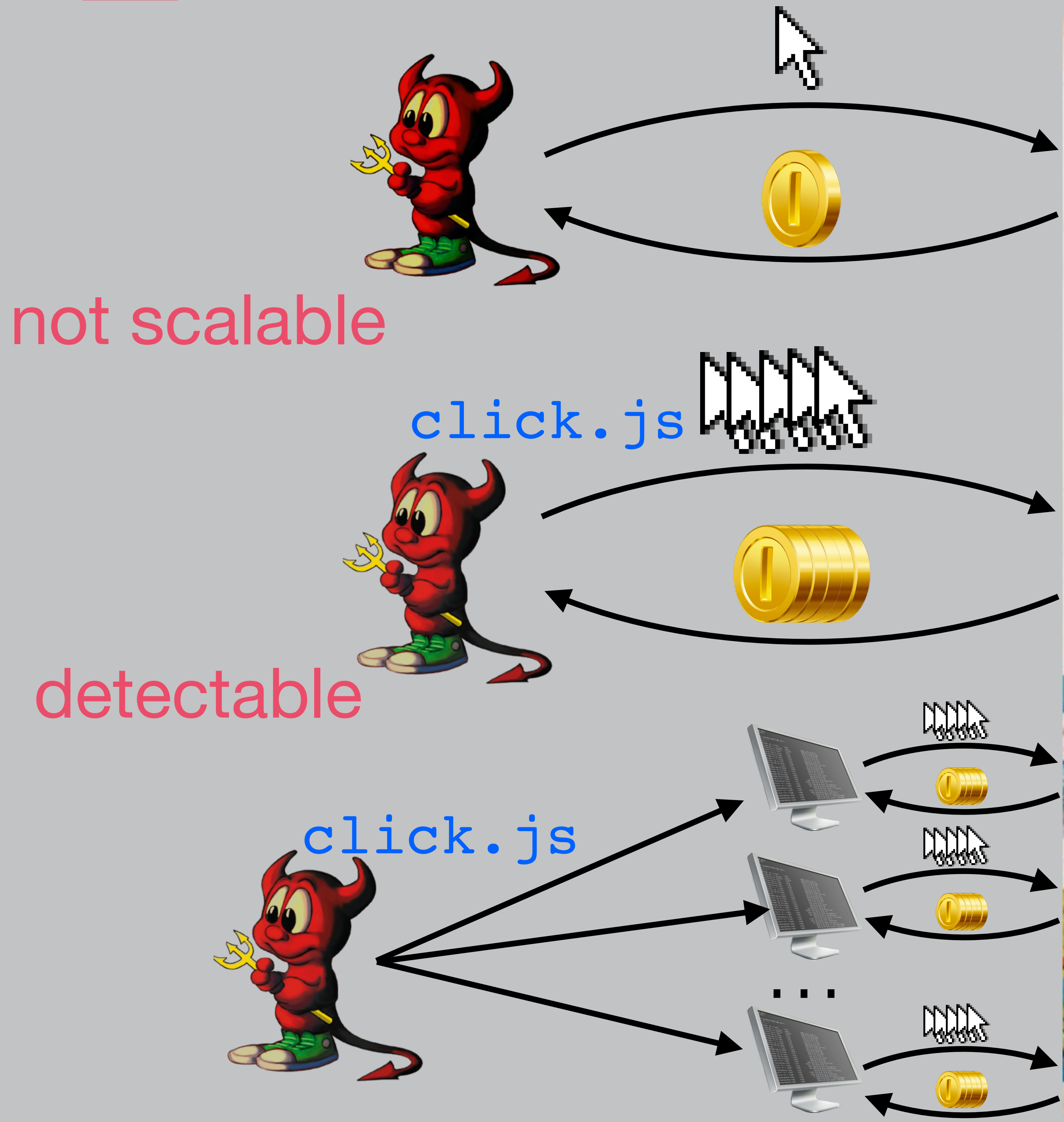
Color by TECHNICOLOR

STARRING THE VOICES OF

ED WYNN	*The Mad Hatter*
RICHARD HAYDN	*The Caterpillar*
STERLING HOLLOWAY .	*The Cheshire Cat*
JERRY COLONNA . . .	*The March Hare*
KATHRYN BEAUMONT	*ALICE*

Distributed by RKO Radio Pictures

CLICK FRAUD



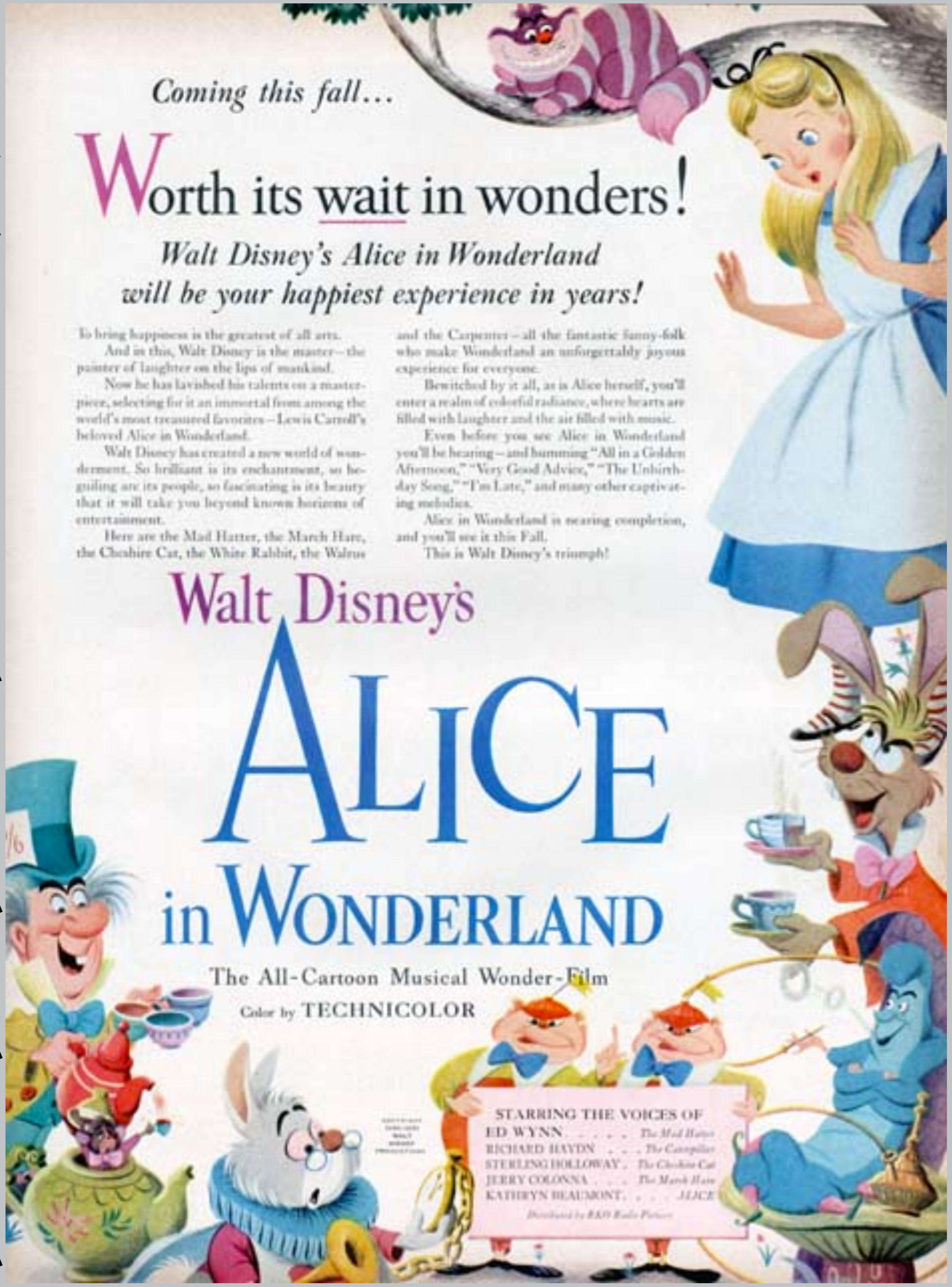
not scalable

click.js

detectable

click.js

...



Coming this fall...

Worth its wait in wonders!

Walt Disney's Alice in Wonderland will be your happiest experience in years!

To bring happiness is the greatest of all arts.

And in this, Walt Disney is the master—the painter of laughter on the lips of mankind.

Now he has lavished his talents on a masterpiece, selecting for it an immortal from among the world's most treasured favorites—Lewis Carroll's beloved *Alice in Wonderland.*

Walt Disney has created a new world of wonderment. So brilliant is its enchantment, so beguiling are its people, so fascinating is its beauty that it will take you beyond known horizons of entertainment.

Here are the Mad Hatter, the March Hare, the Cheshire Cat, the White Rabbit, the Walrus and the Carpenter—all the fantastic funny-folk who make Wonderland an unforgettably joyous experience for everyone.

Bewitched by it all, as is Alice herself, you'll enter a realm of colorful radiance, where hearts are filled with laughter and the air filled with music.

Even before you see *Alice in Wonderland* you'll be hearing—and humming "All in a Golden Afternoon," "Very Good Advice," "The Unbirthday Song," "I'm Late," and many other captivating melodies.

Alice in Wonderland is nearing completion, and you'll see it this Fall.

This is Walt Disney's triumph!

Walt Disney's

ALICE in WONDERLAND

The All-Cartoon Musical Wonder-Film

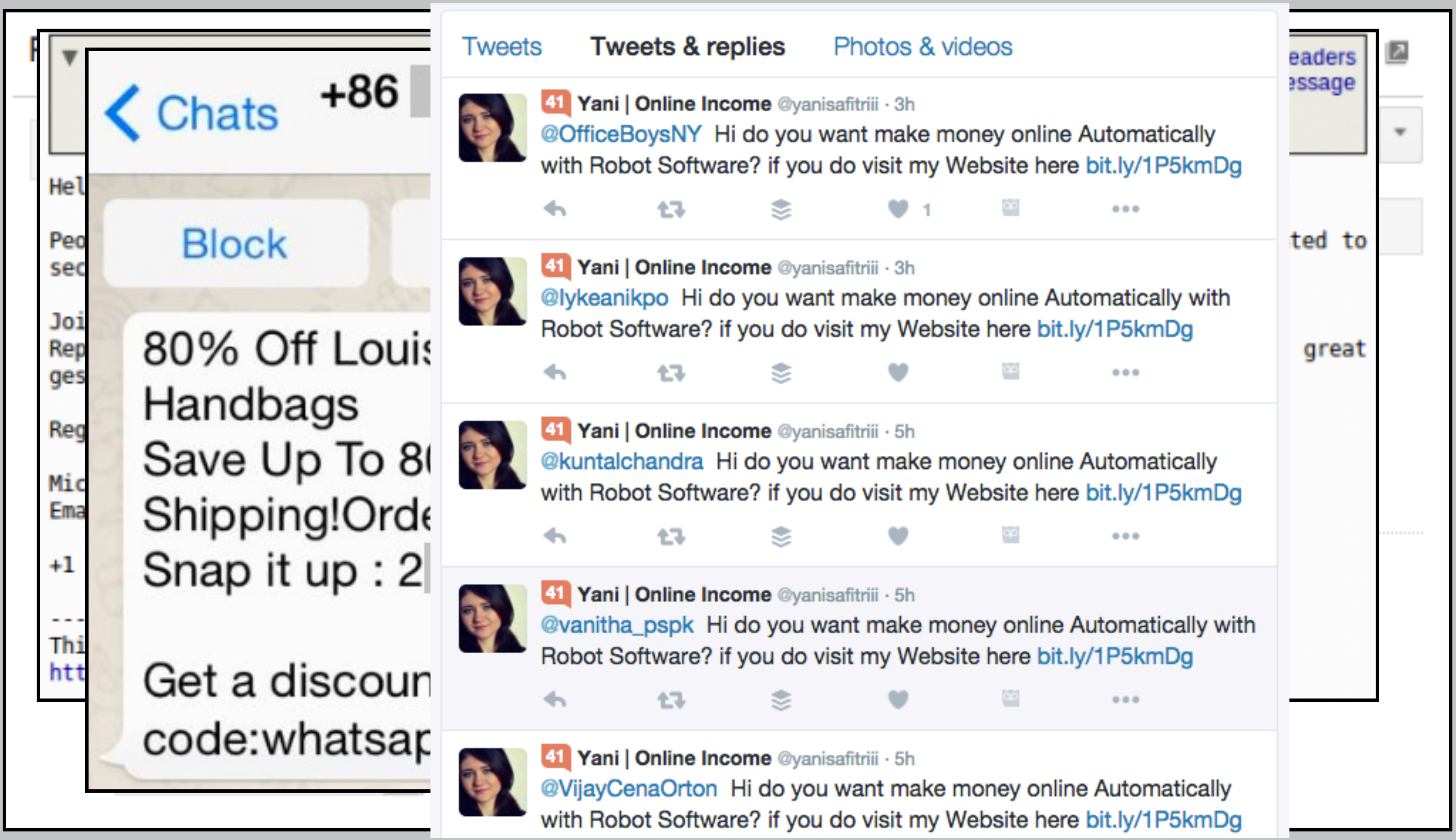
Color by TECHNICOLOR

STARRING THE VOICES OF

ED WYNN . . . . . *The Mad Hatter*
RICHARD HAYDN . . . . *The Caterpillar*
STERLING HOLLOWAY . *The Cheshire Cat*
JERRY COLONNA . . . *The March Hare*
KATHRYN BEAUMONT . . . . *ALICE*

Distributed by RKO Radio Pictures

SPAM



< Chats +86

Block

80% Off Louis
Handbags
Save Up To 8
Shipping!Orde
Snap it up : 2

Get a discoun
code:whatsap

Tweets | **Tweets & replies** | Photos & videos

Yani | Online Income @yanisafitriii · 3h
@OfficeBoysNY Hi do you want make money online Automatically with Robot Software? if you do visit my Website here bit.ly/1P5kmDg

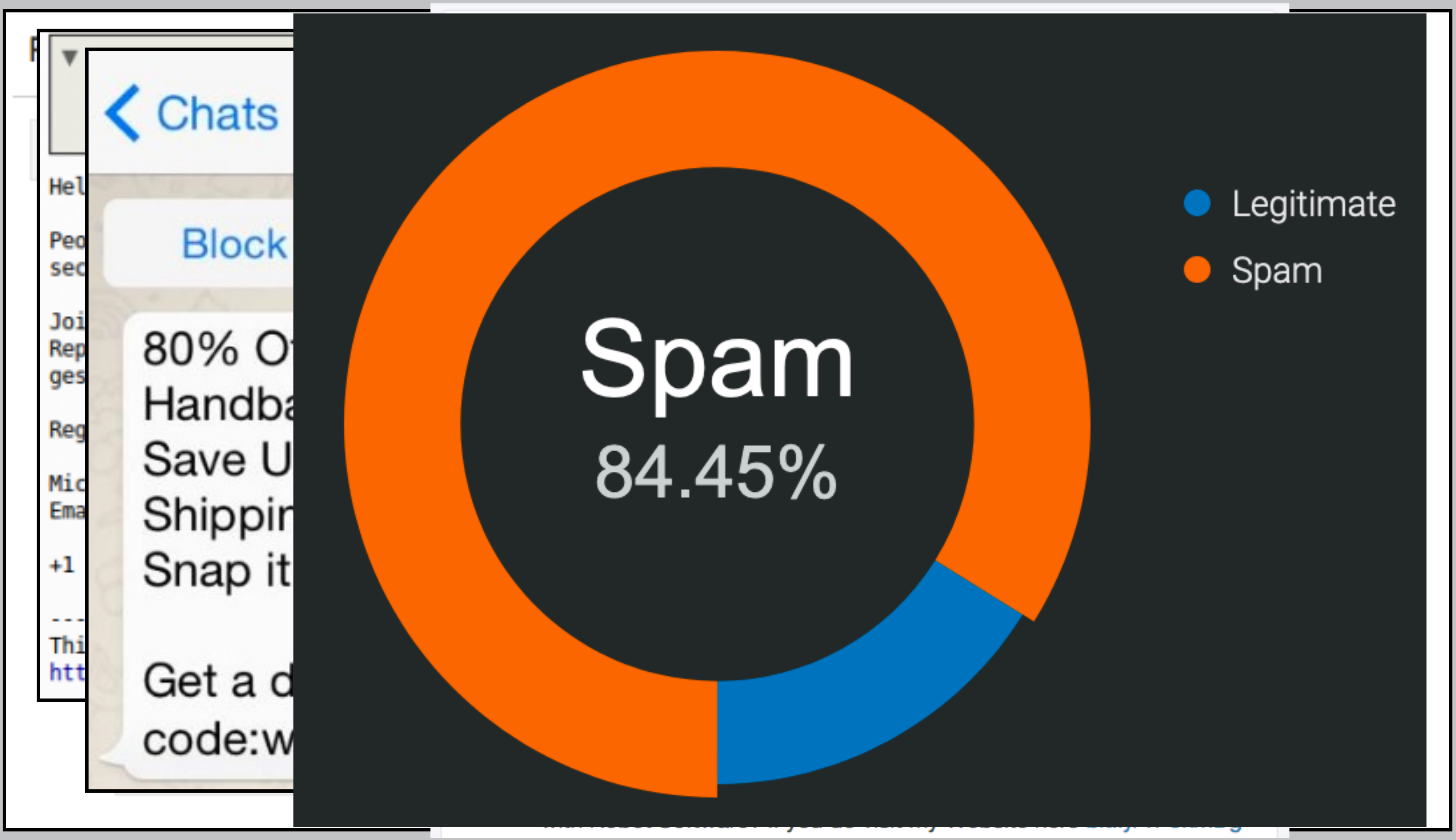
Yani | Online Income @yanisafitriii · 3h
@lykeanikpo Hi do you want make money online Automatically with Robot Software? if you do visit my Website here bit.ly/1P5kmDg

Yani | Online Income @yanisafitriii · 5h
@kuntalchandra Hi do you want make money online Automatically with Robot Software? if you do visit my Website here bit.ly/1P5kmDg

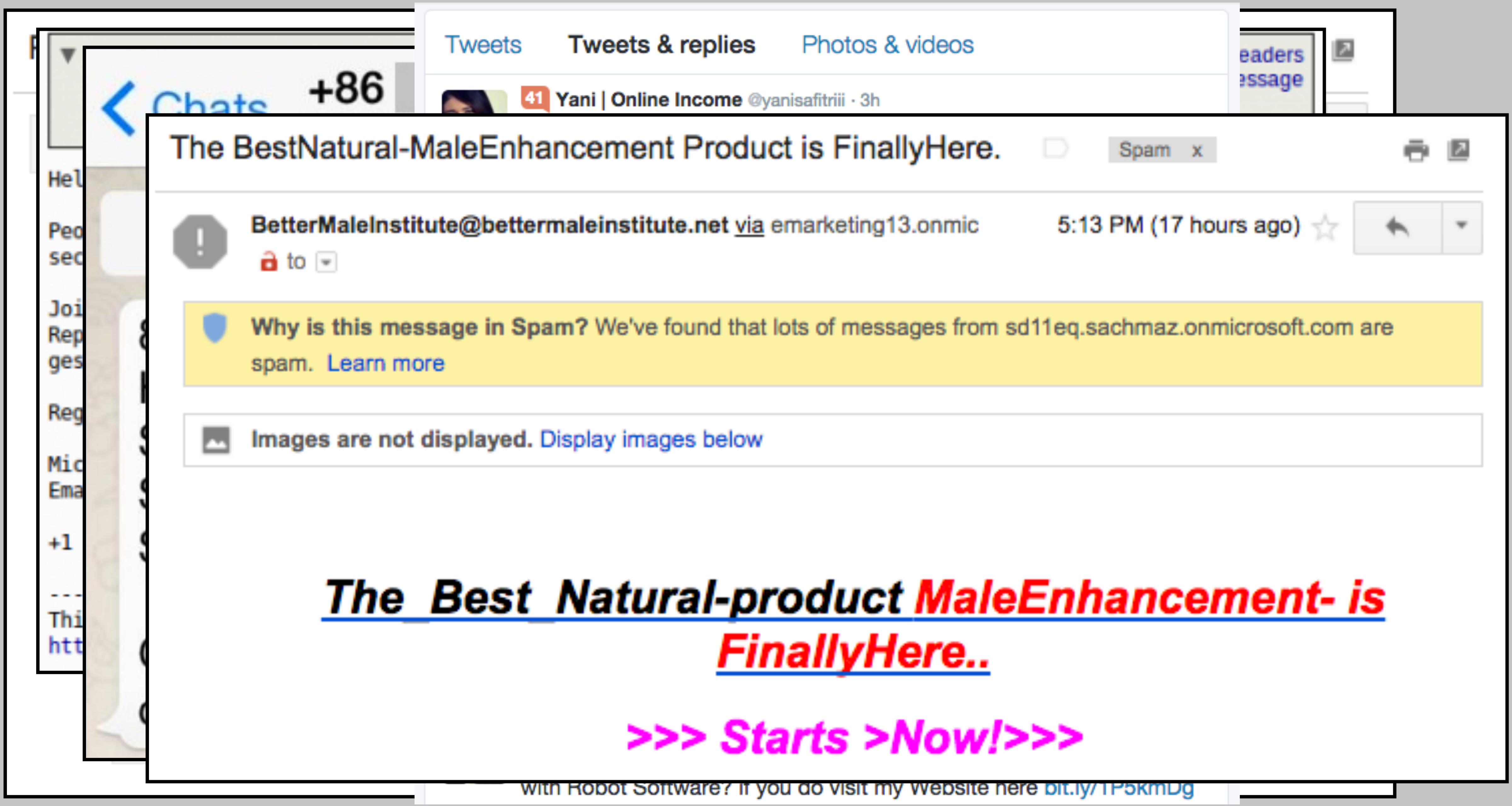
Yani | Online Income @yanisafitriii · 5h
@vanitha_pspk Hi do you want make money online Automatically with Robot Software? if you do visit my Website here bit.ly/1P5kmDg

Yani | Online Income @yanisafitriii · 5h
@VijayCenaOrton Hi do you want make money online Automatically with Robot Software? if you do visit my Website here bit.ly/1P5kmDg

SPAM


Chats
Block
80% O
Handba
Save U
Shippin
Snap it
Get a d
code:w
Hel
Peo
sec
Joi
Rep
ges
Reg
Mic
Ema
+1
Thi
htt
Spam
84.45%
● Legitimate
● Spam

SPAM



The BestNatural-MaleEnhancement Product is FinallyHere.

Spam x

BetterMaleInstitute@bettermaleinstitute.net via emarketing13.onmic

to

5:13 PM (17 hours ago)

Why is this message in Spam? We've found that lots of messages from sd11eq.sachmaz.onmicrosoft.com are spam. Learn more

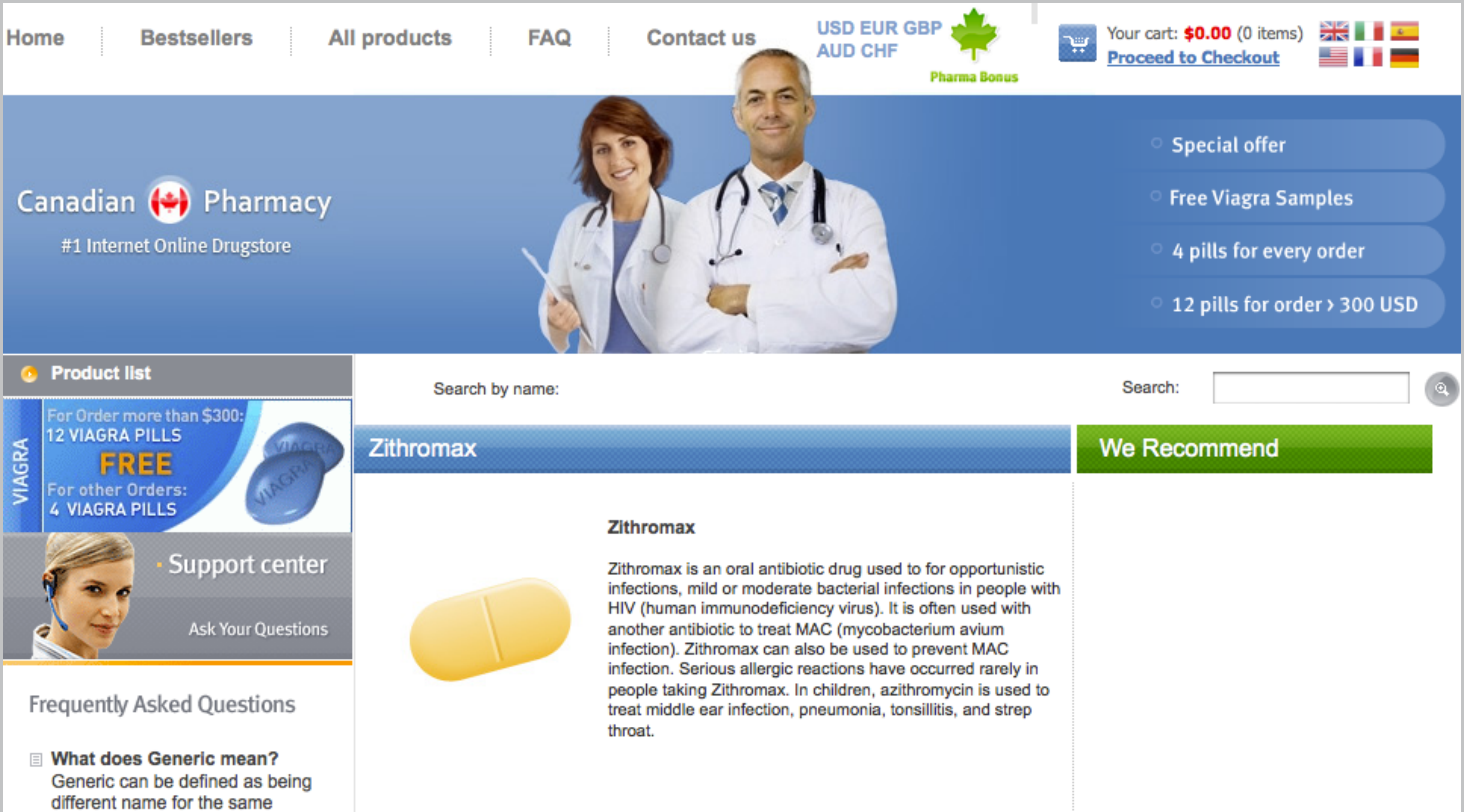
Images are not displayed. Display images below

The Best Natural-product MaleEnhancement- is FinallyHere..

>>> Starts >Now!>>>

Tweets
Tweets & replies
Photos & videos
41 Yani | Online Income @yanisafitriii · 3h
with Robot Software? If you do visit my Website here bit.ly/1P5kmDg
Chats
+86
Hel
Peo
sec
Joi
Rep
ges
Reg
Mic
Ema
+1
Thi
htt
eaders
essage

AFFILIATE PROGRAMS



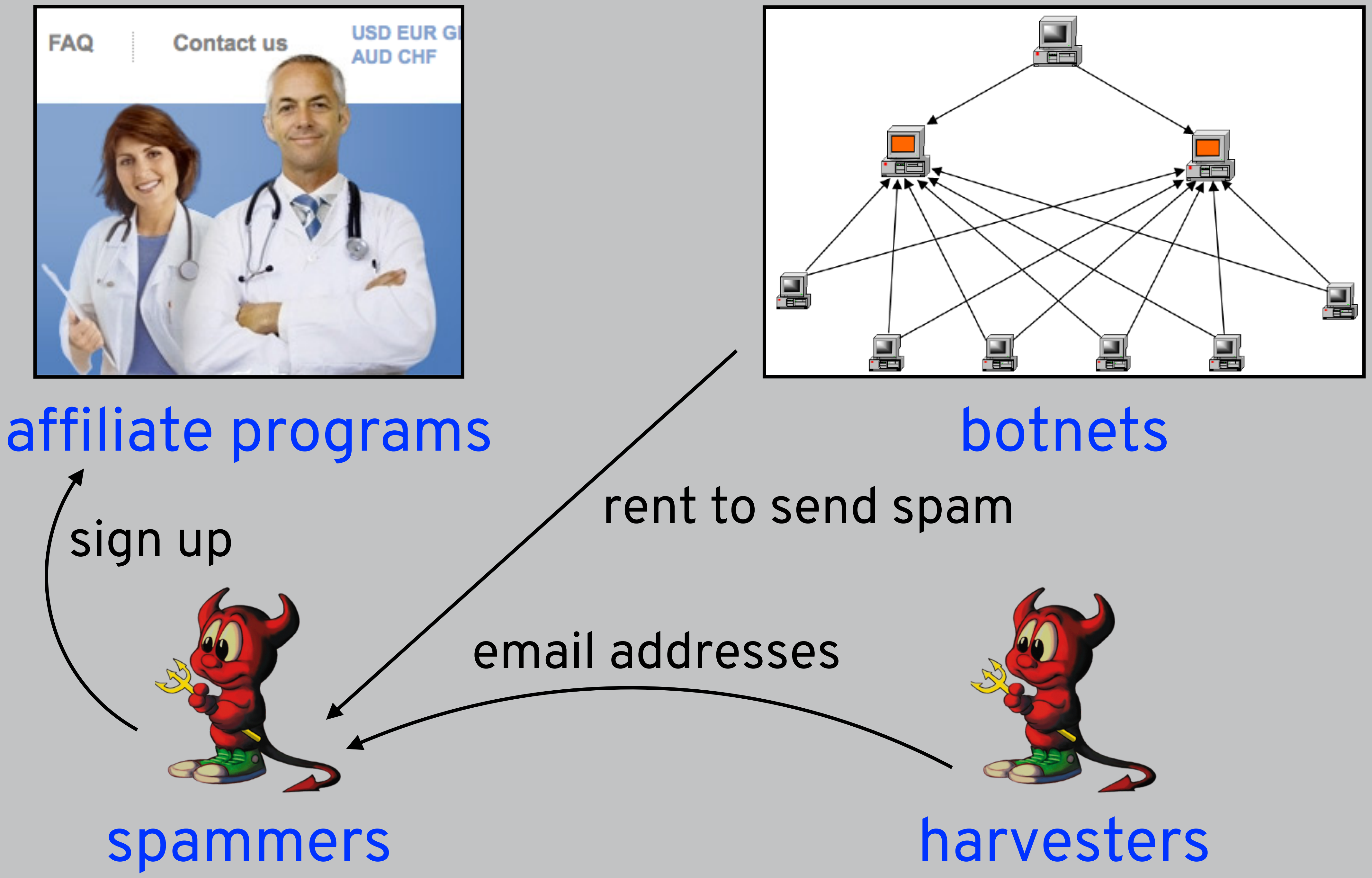
Zithromax

Zithromax is an oral antibiotic drug used to for opportunistic infections, mild or moderate bacterial infections in people with HIV (human immunodeficiency virus). It is often used with another antibiotic to treat MAC (mycobacterium avium infection). Zithromax can also be used to prevent MAC infection. Serious allergic reactions have occurred rarely in people taking Zithromax. In children, azithromycin is used to treat middle ear infection, pneumonia, tonsillitis, and strep throat.

Frequently Asked Questions

What does Generic mean?
Generic can be defined as being different name for the same

SPAM ECOSYSTEM



affiliate programs

botnets

sign up

rent to send spam

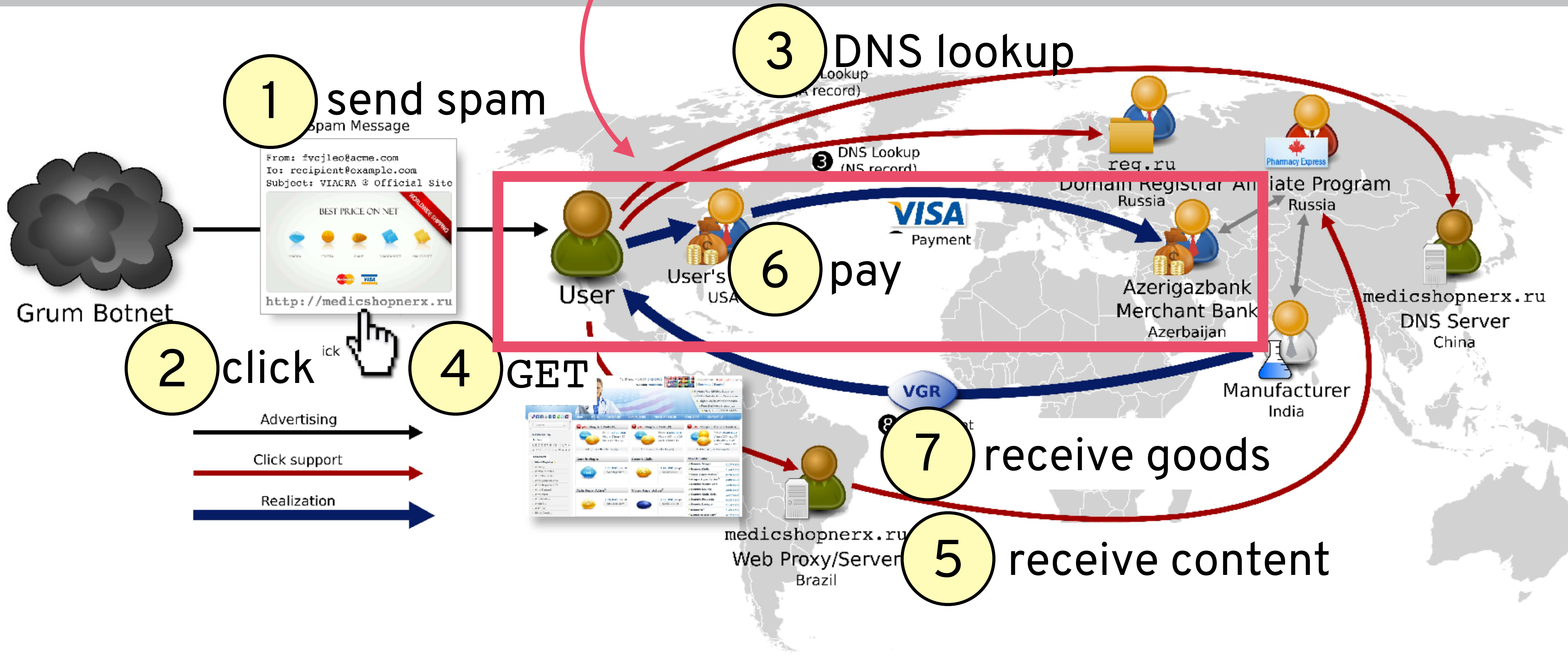
email addresses

spammers

harvesters

SPAM ECOSYSTEM

payment was weak link



1 send spam

2 click

3 DNS lookup

4 GET

5 receive content

6 pay

7 receive goods

(from “Click Trajectories” by Levchenko et al.)

EXAMPLES

Grum

-shut down in 2012

-500-900K infected

-26% of spam in 2010 (40B/day)

ZeroAccess

-shut down in 2013

-2M infected

-click fraud/Bitcoin mining

Cutwail

-shut down in 2010

-1.5-2M infected

-46% of spam in 2009 (74B/day)

Storm

-peak in 2007

-1-50M infected

-20% of spam in 2008

WHERE DO BOTNETS COME FROM?

q: but how do booter services work? how to do it myself?

a: use a **botnet**.

q: what is the monetary point of creating a botnet?

a: DDoS as a service, **click fraud**, **spam**.

q: but how do I create a botnet in the first place?

a: infect computers with **malware**.