Affiliate Web-based Malware

Paul O Baccas (paul.baccas@sophos.com)

1st October, 2008

This talk will cover

- A definition of the title
- A look at examples
- A look at defences
- A look at tricks

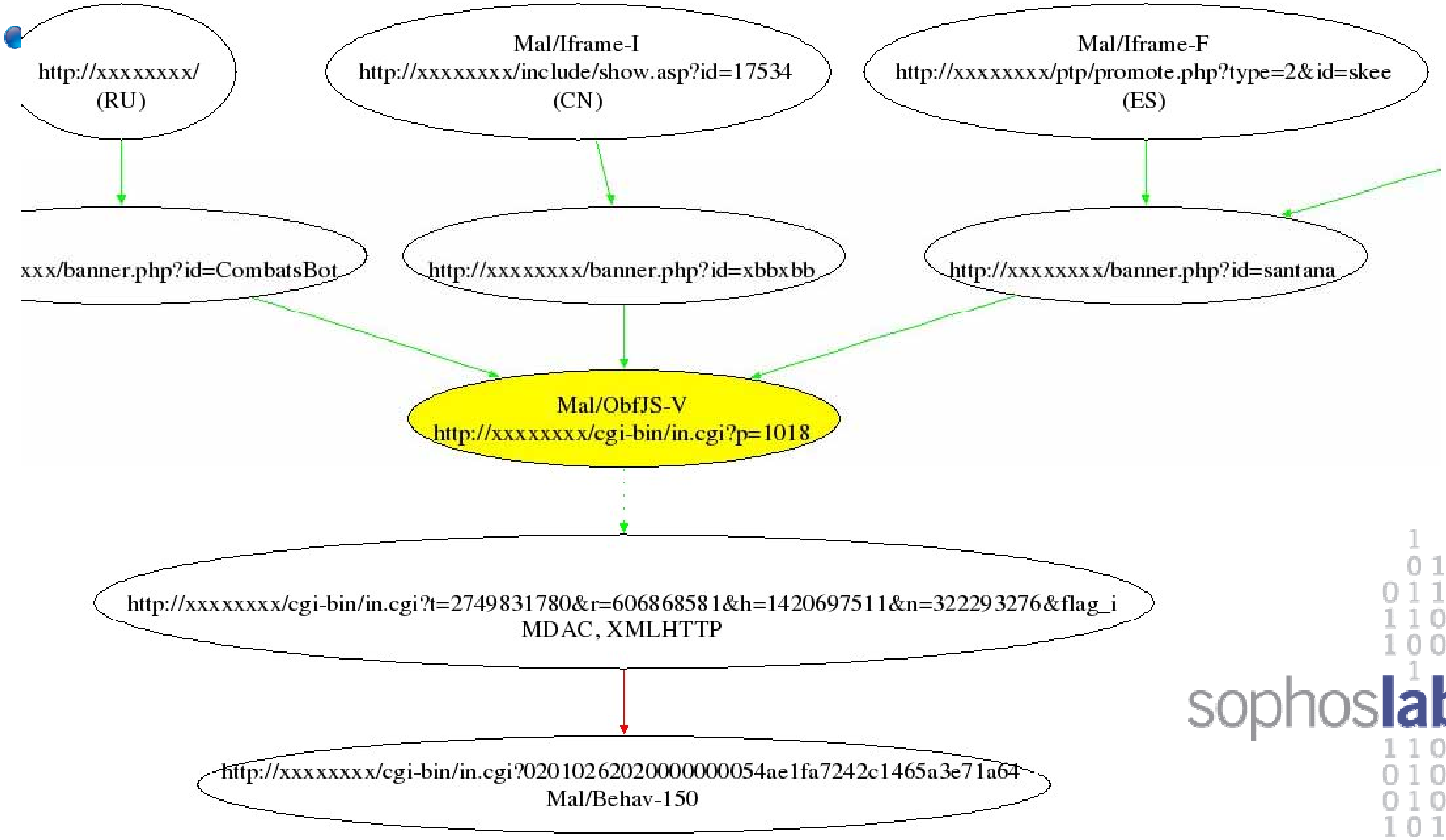
What do we mean by ‘Affiliate Web-based Malware’?

- Affiliate websites
  - Those connected via links for purpose of generating revenue
- Web-based Malware
  - Malware that by design or exploit redirects users to sites that
    - Install malware on the local machine
    - Or generate fictitious clicks on ad-sites

Installing malware on local systems

- By making use of drive-by technology
  - Browser exploits
  - Social engineering

Examples – santana



Mal/Iframe-I
http://xxxxxxxx/include/show.asp?id=17534
(CN)

Mal/Iframe-F
http://xxxxxxxx/ptp/promote.php?type=2&id=skee
(ES)

http://xxxxxxxx/
(RU)

xxx/banner.php?id=CombatsBot

http://xxxxxxxx/banner.php?id=xbbxbb

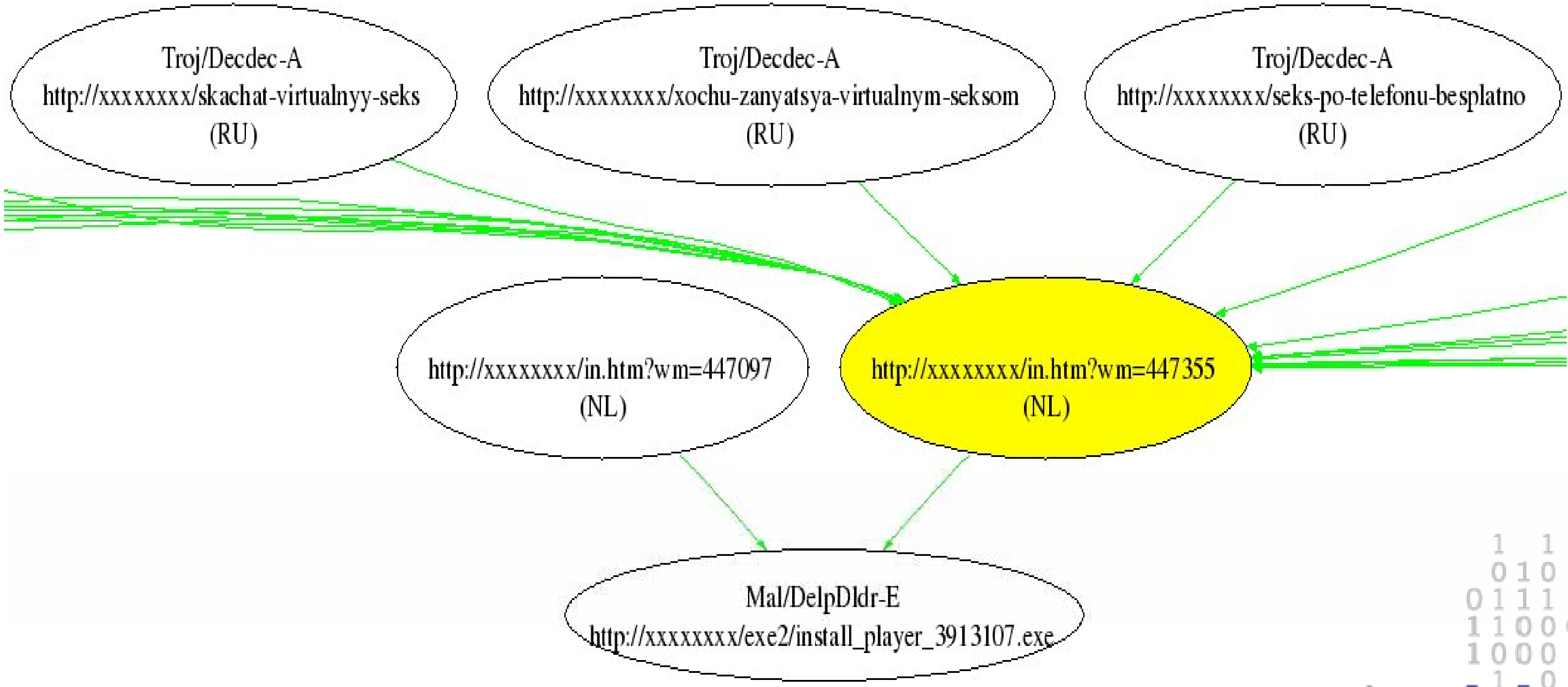
http://xxxxxxxx/banner.php?id=santana

Mal/ObfJS-V
http://xxxxxxxx/cgi-bin/in.cgi?p=1018

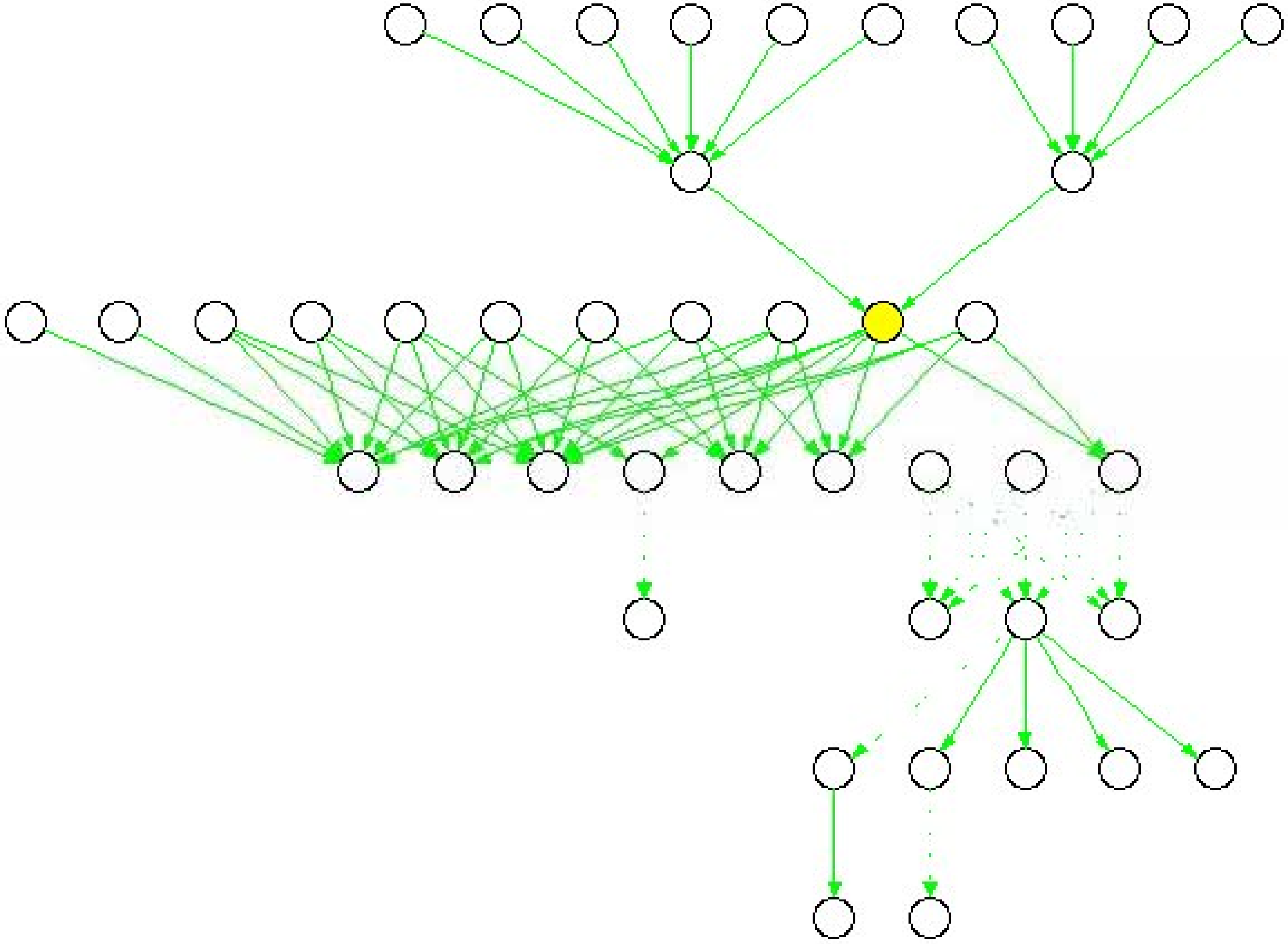
http://xxxxxxxx/cgi-bin/in.cgi?t=2749831780&r=606868581&h=1420697511&n=322293276&flag_i
MDAC, XMLHTTP

http://xxxxxxxx/cgi-bin/in.cgi?020102620200000000054ae1fa7242c1465a3e71a64
Mal/Behav-150

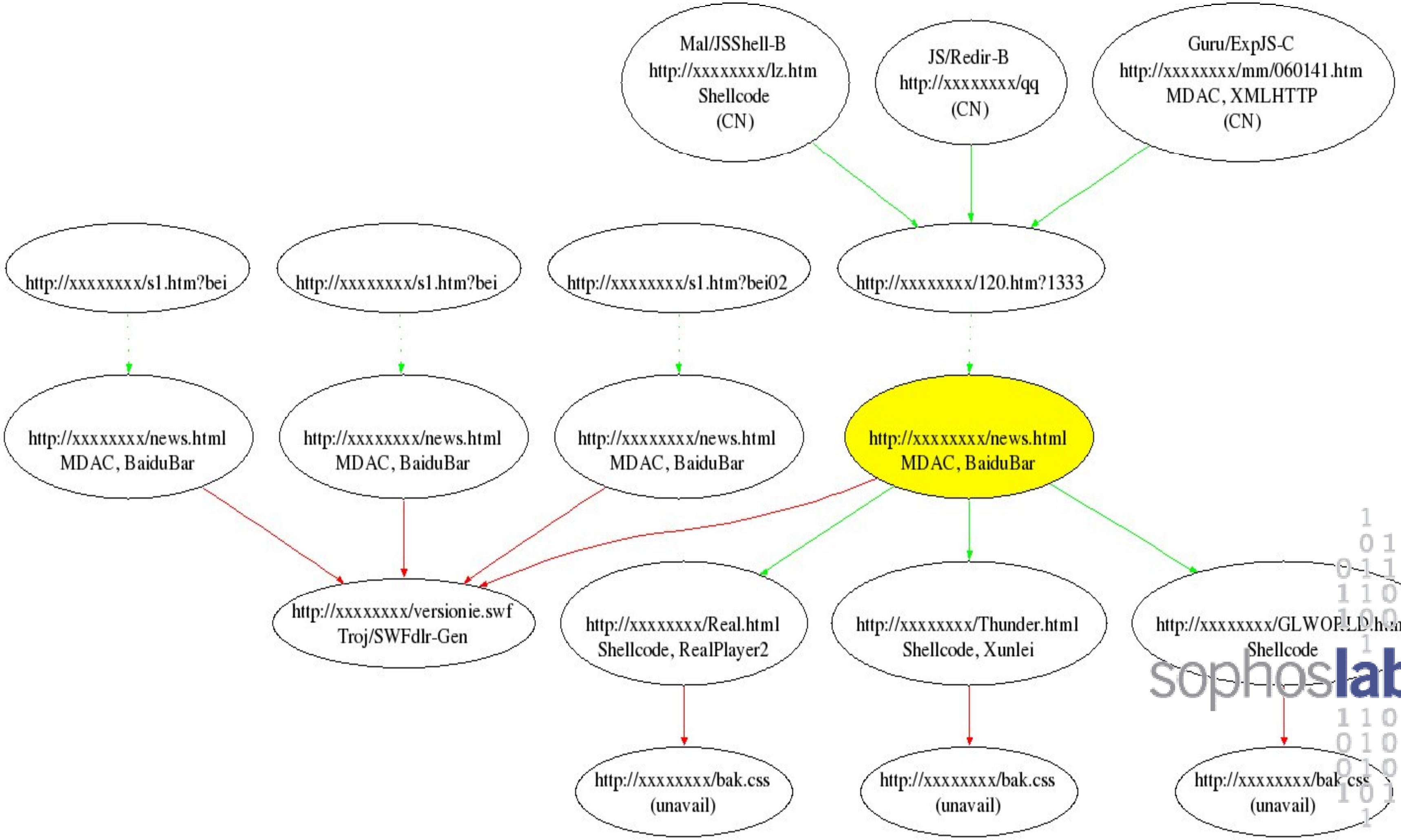
Example -- clickcash


Troj/Decdec-A
http://xxxxxxxx/skachat-virtualnyy-seks
(RU)
Troj/Decdec-A
http://xxxxxxxx/xochu-zanyatsya-virtualnym-seksom
(RU)
Troj/Decdec-A
http://xxxxxxxx/seks-po-telefonu-besplatno
(RU)
http://xxxxxxxx/in.htm?wm=447097
(NL)
http://xxxxxxxx/in.htm?wm=447355
(NL)
Mal/DelpDldr-E
http://xxxxxxxx/exe2/install_player_3913107.exe

Example -- meteorx



Example -- ActionScript



Mal/JSShell-B
http://xxxxxxxx/lz.htm
Shellcode
(CN)

JS/Redir-B
http://xxxxxxxx/qq
(CN)

Guru/ExpJS-C
http://xxxxxxxx/mm/060141.htm
MDAC, XMLHTTP
(CN)

http://xxxxxxxx/s1.htm?bei

http://xxxxxxxx/s1.htm?bei

http://xxxxxxxx/s1.htm?bei02

http://xxxxxxxx/120.htm?1333

http://xxxxxxxx/news.html
MDAC, BaiduBar

http://xxxxxxxx/news.html
MDAC, BaiduBar

http://xxxxxxxx/news.html
MDAC, BaiduBar

http://xxxxxxxx/news.html
MDAC, BaiduBar

http://xxxxxxxx/versionie.swf
Troj/SWFdlr-Gen

http://xxxxxxxx/Real.html
Shellcode, RealPlayer2

http://xxxxxxxx/Thunder.html
Shellcode, Xunlei

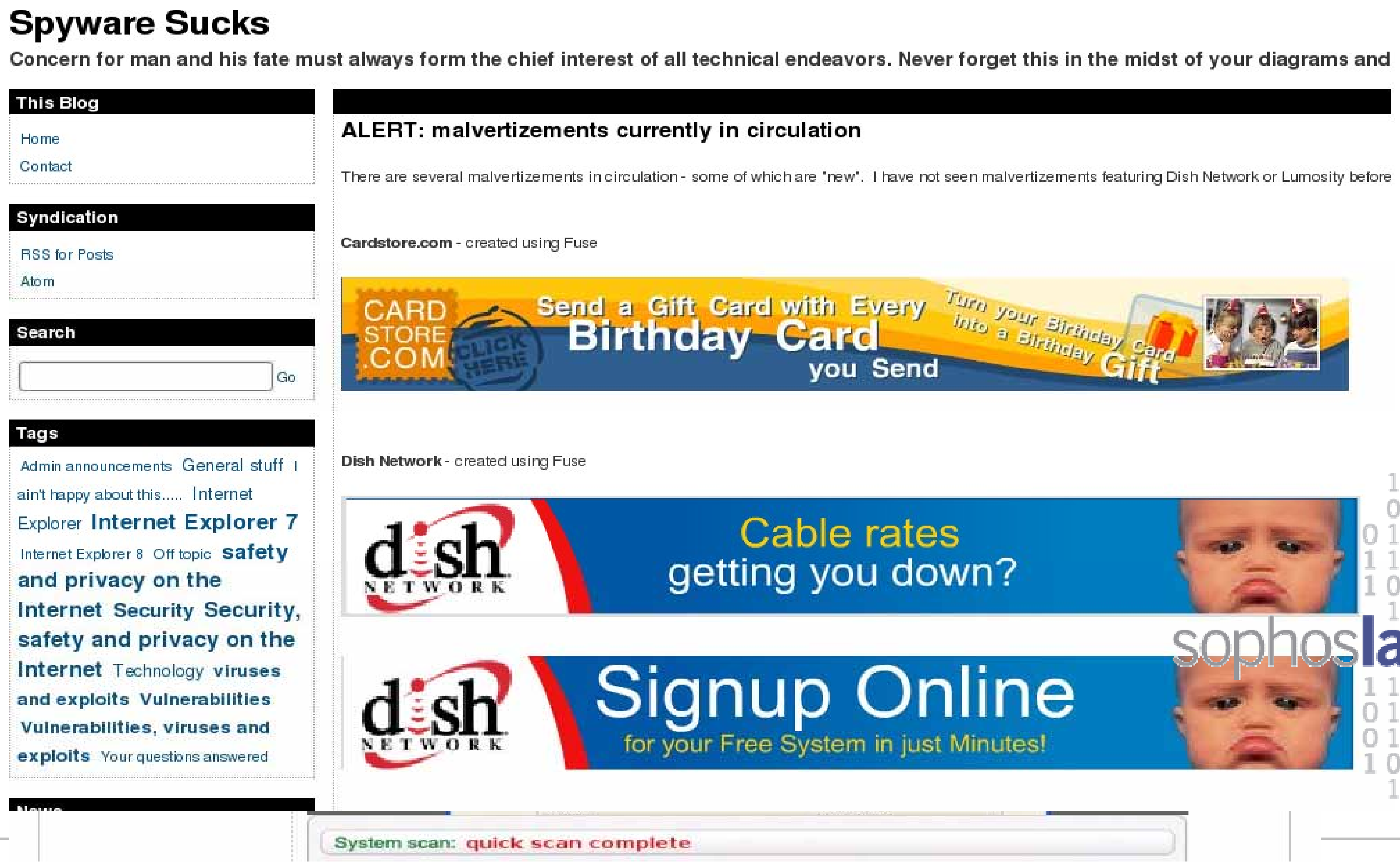
http://xxxxxxxx/GLWORLD.html
Shellcode

http://xxxxxxxx/bak.css
(unavail)

http://xxxxxxxx/bak.css
(unavail)

http://xxxxxxxx/bak.css
(unavail)

Example -- Poisoning



Spyware Sucks

Concern for man and his fate must always form the chief interest of all technical endeavors. Never forget this in the midst of your diagrams and

This Blog

Home

Contact

Syndication

RSS for Posts

Atom

Search

Go

Tags

Admin announcements General stuff I ain't happy about this..... Internet Explorer Internet Explorer 7 Internet Explorer 8 Off topic safety and privacy on the Internet Security Security, safety and privacy on the Internet Technology viruses and exploits Vulnerabilities Vulnerabilities, viruses and exploits Your questions answered

News

ALERT: malvertizements currently in circulation

There are several malvertizements in circulation - some of which are "new". I have not seen malvertizements featuring Dish Network or Lumosity before

Cardstore.com - created using Fuse

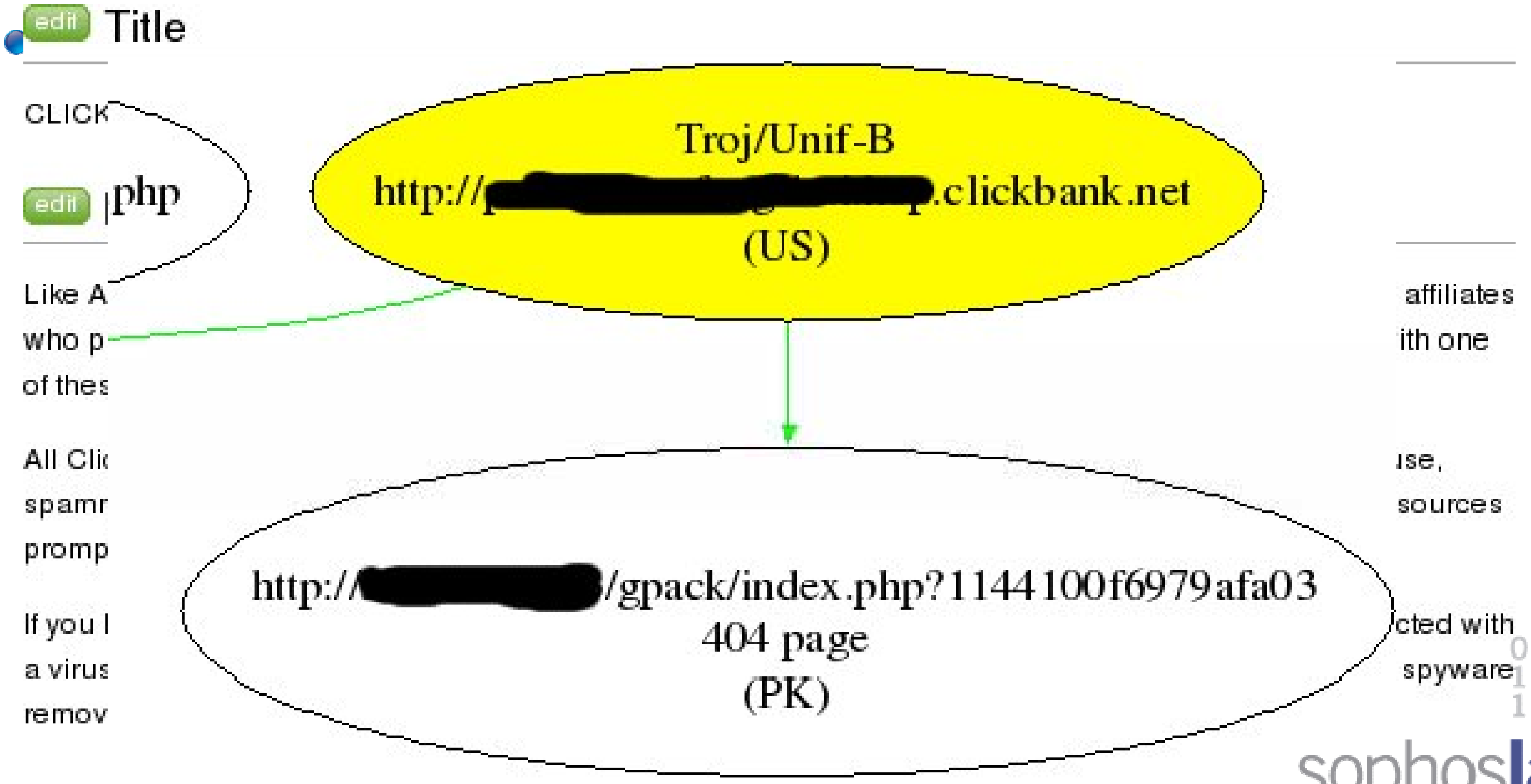
CARD STORE .COM
CLICK HERE
Send a Gift Card with Every
Birthday Card
you Send
Turn your Birthday Card into a Birthday Gift

Dish Network - created using Fuse

dish NETWORK
Cable rates getting you down?
dish NETWORK
Signup Online
for your Free System in just Minutes!

System scan: quick scan complete

Example -- Clickbank



edit Title

CLICK

edit |php

Like A
who p
of thes

affiliates
ith one

All Cli
spamr
promp

ıse,
sources

If you l
a virus
remov

cted with
spyware

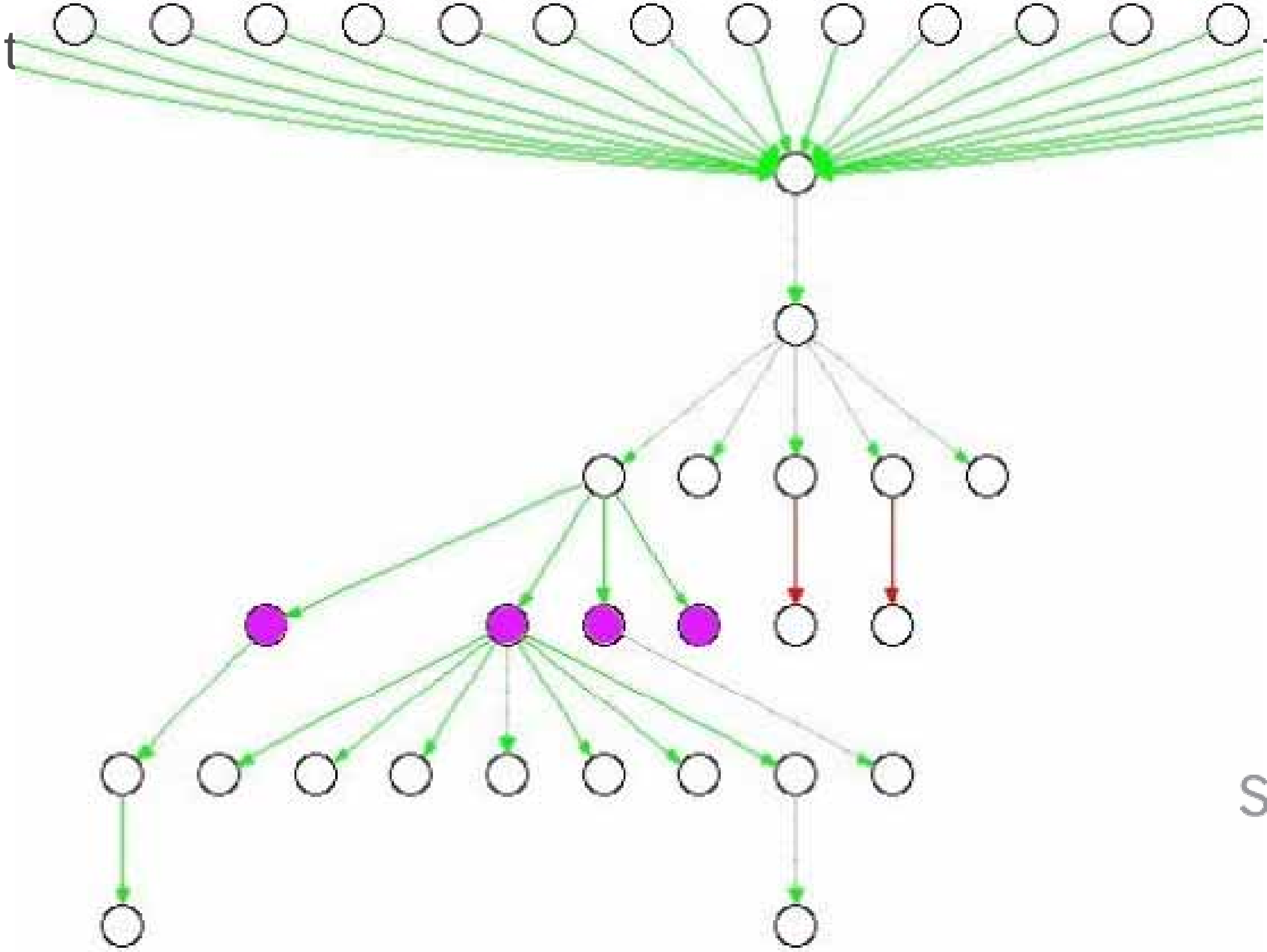
Troj/Unif-B
http://[redacted].clickbank.net
(US)

http://[redacted]/gpack/index.php?1144100f6979afa03
404 page
(PK)

sophoslabs

Example -- blog

- ht html



Summary

- Malware author are using these techniques
  - To increase coverage
  - To make it harder to track
  - And to generate revenue
- Anti-malware vendors are providing solutions

Questions

- Thank you