Tracking the “Who” and “Why” behind targeted, semi-targeted and widespread attacks

Michael La Pilla
VeriSign iDefense Malicious Code Operations Team

21st Annual FIRST Conference Kyoto, Japan
29 June 2009

Topics For Today

- Misinformation vs Disinformation vs Truth
- Large Scale Incident Attribution Methods
- Spotting Other Researchers
- Scope Determination Techniques
- Aggressive Counter-attack Methods

Information

- information (n) - the communication or reception of knowledge or intelligence

Source: Merriam-Webster

Misnformation

- misinformation (n) - the *unintentional* communication or reception of false knowledge or intelligence

Source: Merriam-Webster

Disnformation

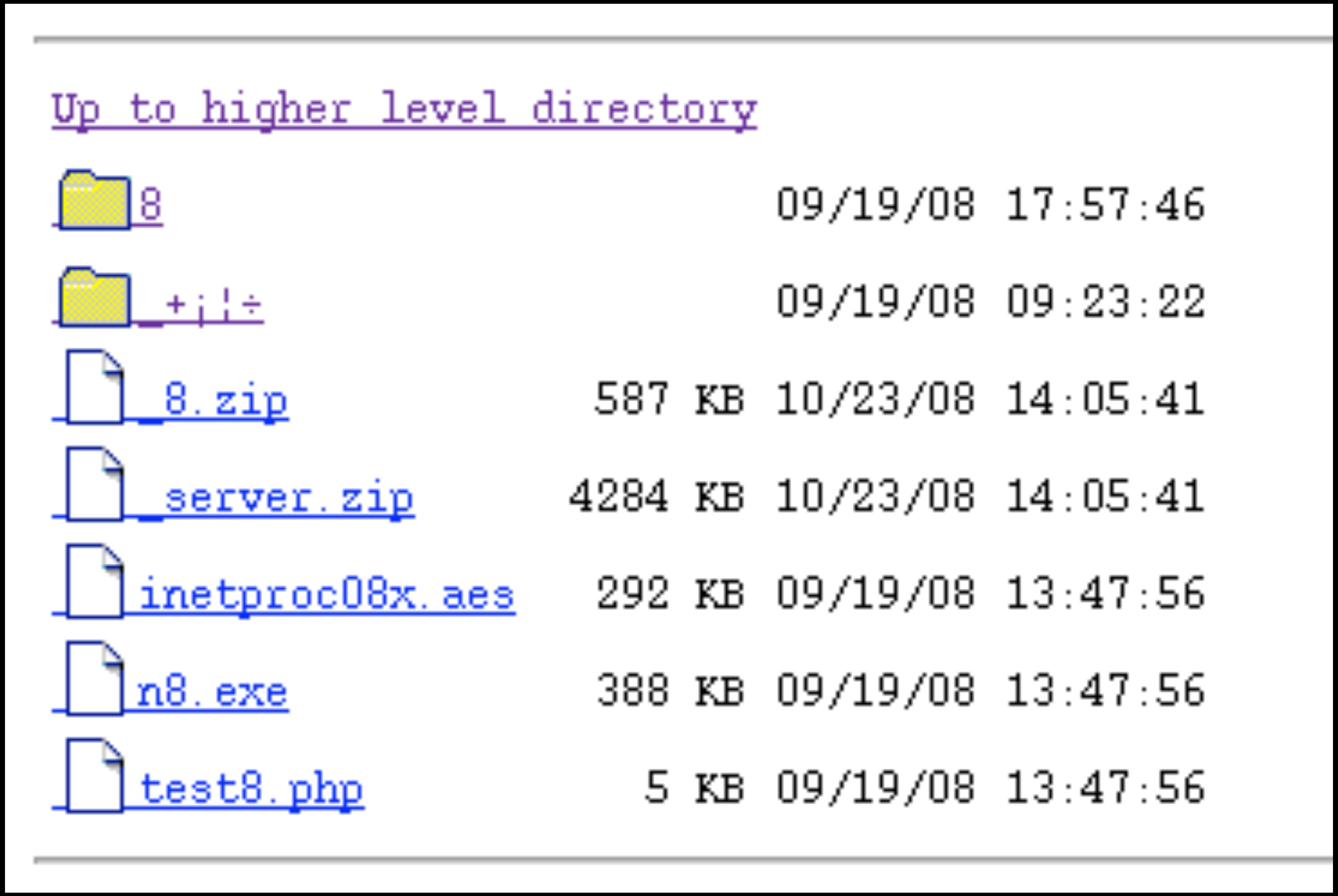
- disinformation (n) - false information *deliberately* and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth

Source: Merriam-Webster

Gimmiv

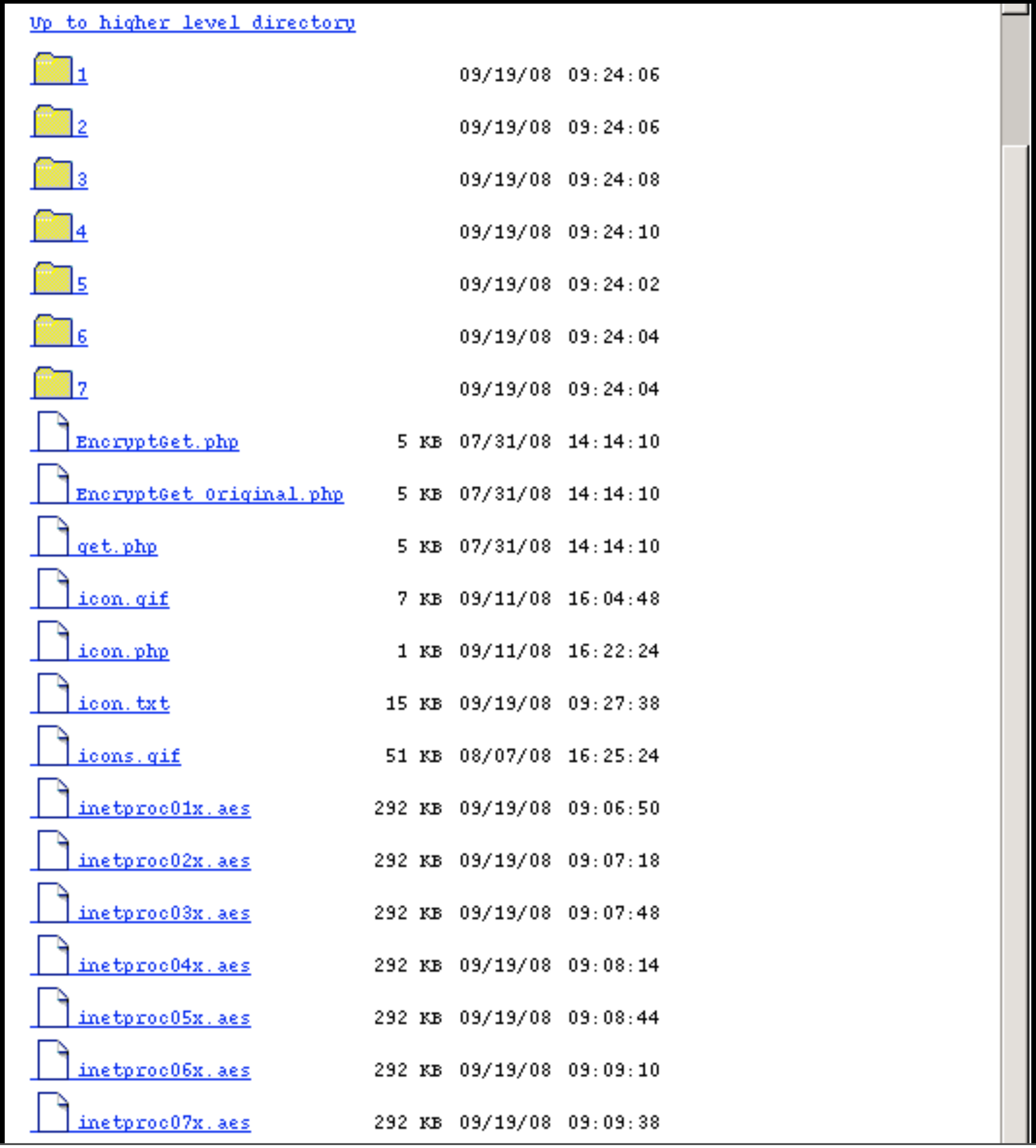
- See where stolen data gets posted
- Anyone can retrieve data files if they know the file name
- Uses combinations of encryption and encoding so people can’t decrypt data
- See if they did anything stupid...

Gimmiv (con’t)



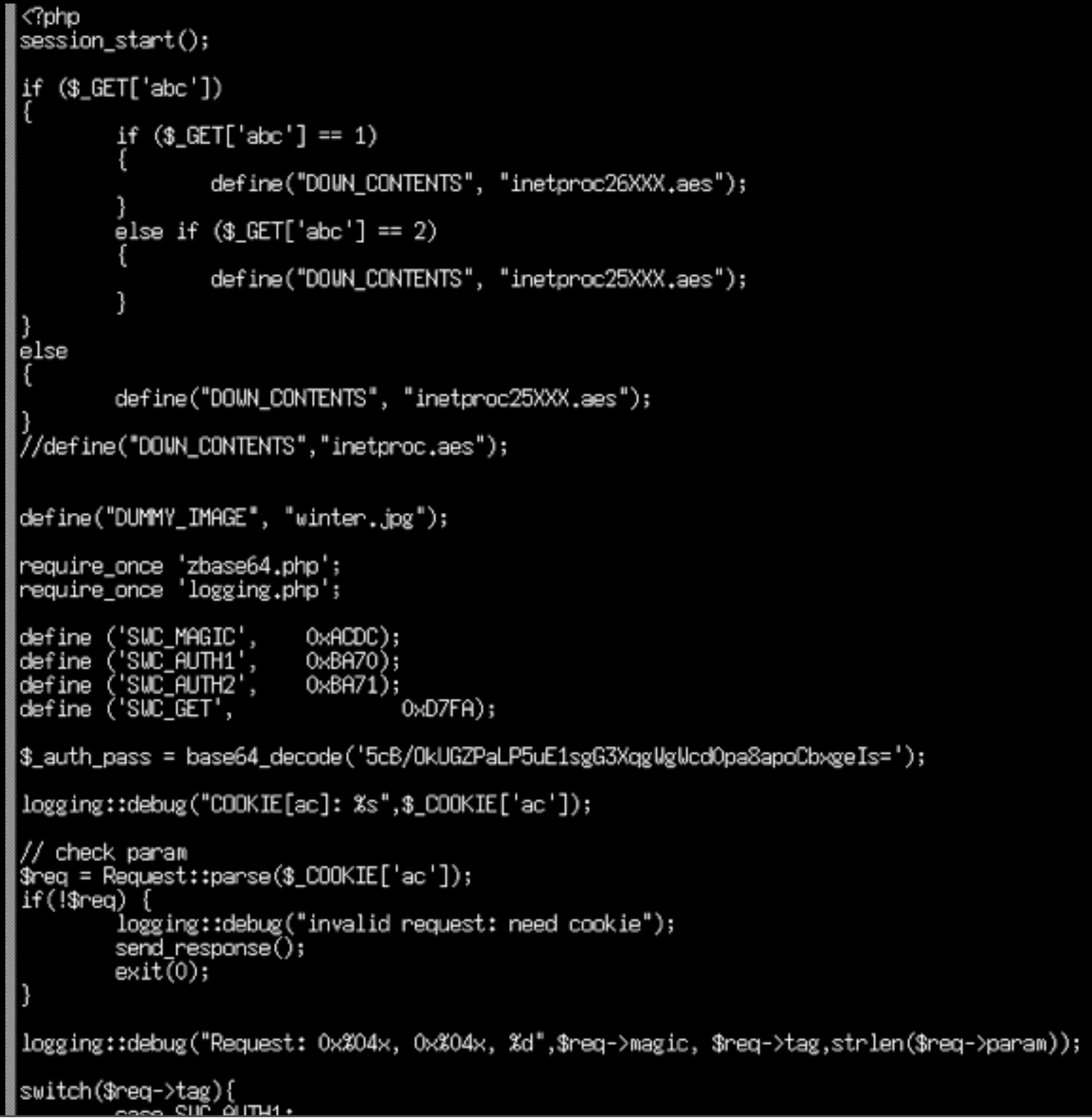
```
Up to higher level directory
 8                                   09/19/08 17:57:46
 _+¡¦÷                               09/19/08 09:23:22
 _8.zip                     587 KB  10/23/08 14:05:41
 _server.zip               4284 KB  10/23/08 14:05:41
 inetproc08x.aes            292 KB  09/19/08 13:47:56
 n8.exe                     388 KB  09/19/08 13:47:56
 test8.php                    5 KB  09/19/08 13:47:56
```

Gimmiv (con't)



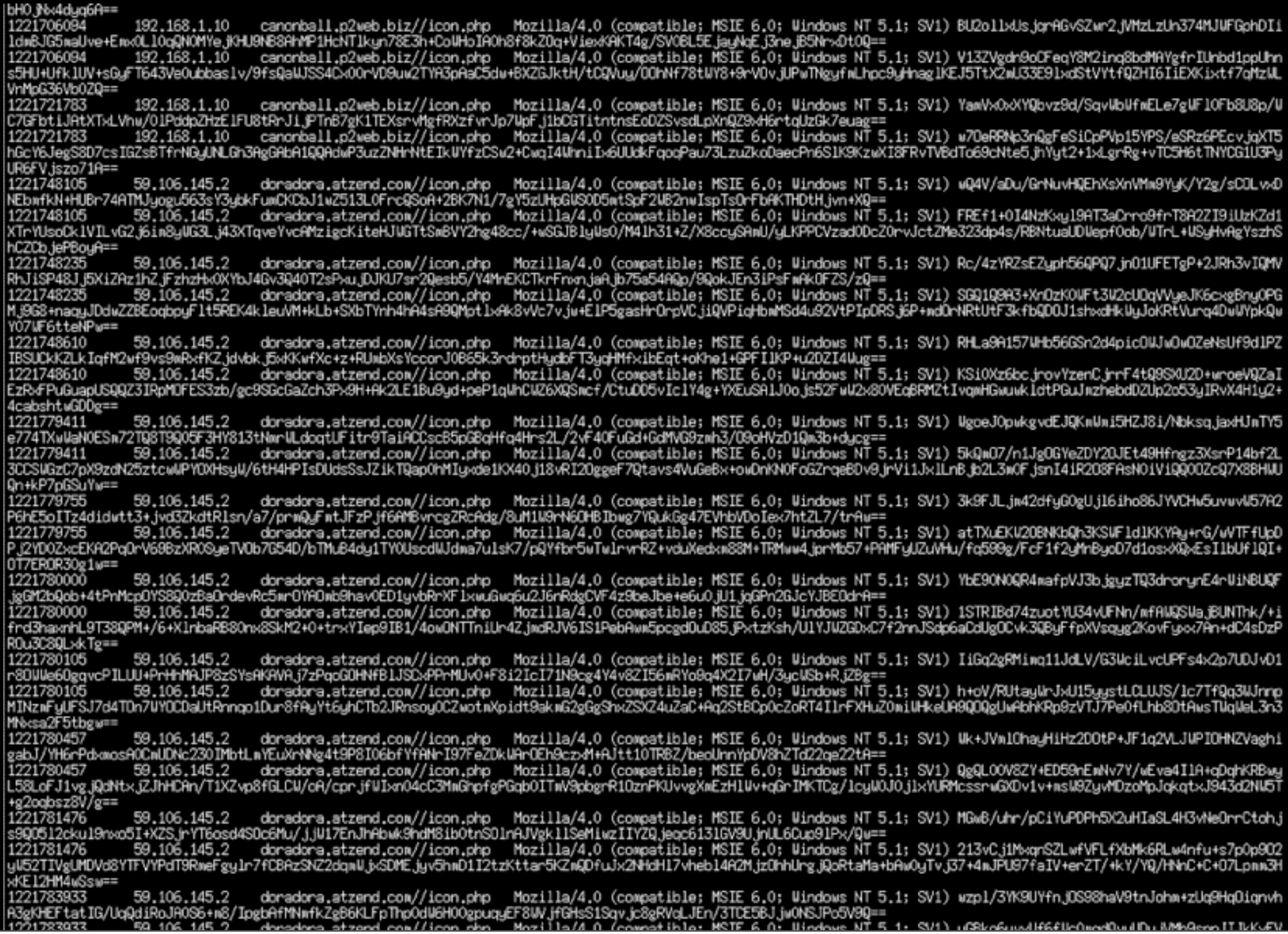
```
Up to higher level directory

1                                    09/19/08  09:24:06
2                                    09/19/08  09:24:06
3                                    09/19/08  09:24:08
4                                    09/19/08  09:24:10
5                                    09/19/08  09:24:02
6                                    09/19/08  09:24:04
7                                    09/19/08  09:24:04
EncryptGet.php                 5 KB  07/31/08  14:14:10
EncryptGet Original.php        5 KB  07/31/08  14:14:10
get.php                        5 KB  07/31/08  14:14:10
icon.gif                       7 KB  09/11/08  16:04:48
icon.php                       1 KB  09/11/08  16:22:24
icon.txt                      15 KB  09/19/08  09:27:38
icons.gif                     51 KB  08/07/08  16:25:24
inetproc01x.aes              292 KB  09/19/08  09:06:50
inetproc02x.aes              292 KB  09/19/08  09:07:18
inetproc03x.aes              292 KB  09/19/08  09:07:48
inetproc04x.aes              292 KB  09/19/08  09:08:14
inetproc05x.aes              292 KB  09/19/08  09:08:44
inetproc06x.aes              292 KB  09/19/08  09:09:10
inetproc07x.aes              292 KB  09/19/08  09:09:38
```

Gimmiv (con’t)



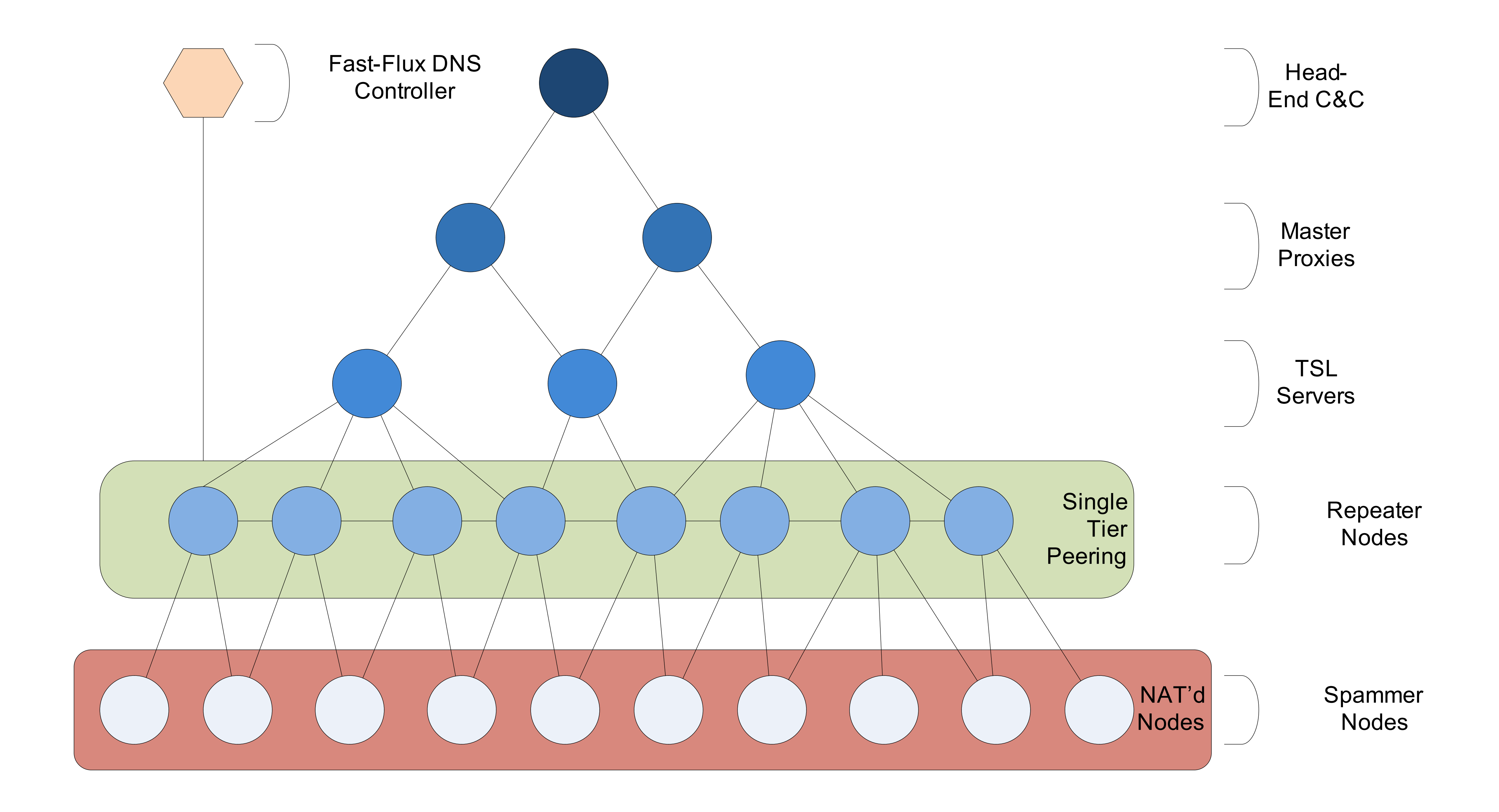
```
<?php
session_start();

if ($_GET['abc'])
{
        if ($_GET['abc'] == 1)
        {
                define("DOWN_CONTENTS", "inetproc26XXX.aes");
        }
        else if ($_GET['abc'] == 2)
        {
                define("DOWN_CONTENTS", "inetproc25XXX.aes");
        }
}
else
{
        define("DOWN_CONTENTS", "inetproc25XXX.aes");
}
//define("DOWN_CONTENTS","inetproc.aes");


define("DUMMY_IMAGE", "winter.jpg");

require_once 'zbase64.php';
require_once 'logging.php';

define ('SWC_MAGIC',    0xACDC);
define ('SWC_AUTH1',    0xBA70);
define ('SWC_AUTH2',    0xBA71);
define ('SWC_GET',              0xD7FA);

$_auth_pass = base64_decode('5cB/OkUGZPaLP5uE1sgG3XqgWgWcdOpa8apoCbxgeIs=');

logging::debug("COOKIE[ac]: %s",$_COOKIE['ac']);

// check param
$req = Request::parse($_COOKIE['ac']);
if(!$req) {
        logging::debug("invalid request: need cookie");
        send_response();
        exit(0);
}

logging::debug("Request: 0x%04x, 0x%04x, %d",$req->magic, $req->tag,strlen($req->param));

switch($req->tag){
        case SWC_AUTH1:
```

Gimmiv (con't)



```
bH0jNx4dyq6A==
1221706094      192.168.1.10    canonball.p2web.biz//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) BU2ollxUsjgrAGvSZwr2jVMzLzUn374MJWFGphDIi
ldmBJG5maUve+EmxOLl0qQNOMYejKHU9NB8AhMP1HcNTlkyn78E3h+CoWHoIAOh8f8kZ0q+ViexKAKT4g/SVOBL5EjayNqEj3nejB5NrxDt0Q==
1221706094      192.168.1.10    canonball.p2web.biz//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) V13ZVgdn9oCFeqY8M2inq8bdMAYgfrIUnbd1ppUhn
s5HU+UfklUV+sGyFT643Ve0ubbaslv/9fsQaWJSS4Cx00rVD9uw2TYA3pAaC5dw+8XZGJktH/tCQVuy/OOhNf78tWY8+9rV0vjUPwTNgyfmLhpc9yHnaglKEJ5TtX2mU33E91xdStVYtfQZHI6IiEXKixtf7qMzWL
VnMpG36Vb0ZQ==
1221721783      192.168.1.10    canonball.p2web.biz//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) YamVx0xXYQbvz9d/SqvWbWfmELe7gWFl0Fb8U8p/W
C7GFbtiJAtXTxLVhw/0lPddpZHzElFU8tRrJijPTnB7gK1TEXsrvMgfRXzfvrJp7WpFj1bCGTitntnsEoDZSvsdLpXnQZ9xH6rtqUzGk7euag==
1221721783      192.168.1.10    canonball.p2web.biz//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) w70eRRNp3nQgFeSiCpPVp15YPS/eSRz6PEcvjqXT5
hGcY6JegS8D7csIGZsBTfrNGyUNLGh3AgGAbA1QQAdwP3uzZNHrNtEIkWYfzCSw2+CwqI4WhniIx6UUdkFqoqPau73LzuZkoDaecPn6SlK9KzwXI8FRvTVBdTo69cNte5jhYyt2+1xLgrRg+vTC5H6tTNYCG1U3Py
UR6FVjszo71A==
1221748105      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) wQ4V/aDu/GrNuvHQEhXsXnVMm9YyK/Y2g/sCOLvxD
NEbwfkN+HUBr74ATMJyogu563sY3ybkFumCKCbJ1wZ513L0FrcQSoA+2BK7N1/7gY5zUHpGWSOD5wtSpF2W82nwIspTsOrFbAKTHDtHjvn+XQ==
1221748105      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) FREf1+0I4NzKxyl9AT3aCrro9frT8A2ZI9iUzKZd1
XTrYUsoCklVILvG2j6im8yWG3Lj43XTqveYvcAMzigcKiteHJWGTtSmBVY2hg48cc/+wSGJBlyWs0/M41h31+Z/X8ccySAmU/yLKPPCVzad0DcZ0rvJctZMe323dp4s/RBNtuaUDWepf0ob/WTrL+WSyHvAgYszhS
hCZCbjePBoyA==
1221748235      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Rc/4zYRZsEZyph56QPQ7jn01UFETgP+2JRh3vIQMV
RhJiSP48JjJ5XiZAz1hZjFzhzHxOXYbJ4Gv3Q40T2sPxujDJKU7sr2Qesb5/Y4MnEKCTkrFrxnjaAjb75a54AQp/9QokJEn3iPsFmAkOFZS/zQ==
1221748235      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) SGQ1Q9A3+XnOzKOWFt3W2cUDqVVyeJK6cxgBnyOPG
Mj9G8+naqyJDdwZZBEoqbpyFlt5REK4kleuVM+kLb+SXbTYnh4hA4sA9QMptlxAk8vVc7vjw+ElP5gasHrOrpVCjiQVPiqHbmMSd4u92VtPIpDRSj6P+mdOrNRtUtF3kfbQD0J1shxdHkWyJoKRtVurq4DwWYpkQw
YO7WF6tteNPw==
1221748610      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) RHLa9A157WHb56GSn2d4picOWJwOwOZeNsUf9dlPZ
IBSUCkKZLkIqfM2wf9vs9mRxfKZjdvbkj5xKKwfXc+z+RUmbXsYccorJ0B65k3rdrptHydbFT3yqHMfxibEqt+oKhe1+GPFIlKP+u2DZI4Wug==
1221748610      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) KSi0Xz6bcjrovYzenCjrrF4tQ9SXU2D+wroeVQZaI
EzRxFPuGuapUSQQZ3IRpMOFES3zb/gc9SGcGaZch3Px9H+Ak2LE1Bu9yd+peP1qWhCWZ6XQSmcf/CtuDO5vIclY4g+YXEuSAlJ0ojs52FwW2x80VEqBRMZtIvqmHGwuwkldtPGuJmzhebdDZUp2o53yIRvX4H1y2+
4cabshtwGDDg==
1221779411      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) WgoeJOpwkgvdEJQKmWmi5HZJ8i/NbksqjaxHJmTY5
e774TXwWaN0ESm72TQ8T9Q05F3HY813tNmrWLdoqtUFitr9TaiACCsc85pG8qHfq4Hrs2L/2vF40FuGd+GdMVG9zmh3/O9oHVzD1Qm3b+dycg==
1221779411      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 5kQm07/n1JgOGYeZDY20JEt49Hfngz3XsrP14bf2L
3CCSWGzC7pX9zdN25ztcwWPYOXHsyW/6tH4HPIsDUdsSsJZikTQap0hMIyxde1KX40j18vRI20ggeF7Qtavs4VuGeBx+owDnKN0FoGZrqeBDv9jrVi1JxlLnBjb2L3wOFjsnI4iR208FAsN0iViQQ00ZcQ7X8BHWU
Qn+kP7pGSuYw==
1221779755      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 3k9FJLjm42dfyG0gUjl6iho86JYVCHw5uvwvW57A2
P6hE5oITz4didwtt3+jvd3ZkdtRlsn/a7/prmQyFmtJFzPjf6AMBvrcgZRcAdg/8uM1W9rN6OHBIbwg7YQukGg47EVhbVDoIex7htZL7/trAw==
1221779755      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) atTXuEKU20BNKbQh3KSWFldlKKYAy+rG/wVTFfUpD
Pj2YDOZxcEKA2PqOrV69BzXR0SyeTVOb7G54D/bTMuB4dy1TYOUscdWJdma7ulsK7/pQYfbr5wTwlrvrRZ+vduXedxm88M+TRMww4jprMb57+PAMFyUZuVHu/fq599g/FcF1f2yMnByoD7d1osxXQxEsIlbUflQI+
OT7EROR30g1w==
1221780000      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) YbE90N0QR4mafpVJ3bjgyzTQ3droryrE4rWiNBUQF
jgGM2bQob+4tPnMcpOYS8Q0zBaOrdevRc5mrOYAOmb9havOED1yvbRrXFlxwuGwq6u2J6nRdgCVF4z9beJbe+e6u0jU1jqGPn2GJcYJBEOdrA==
1221780000      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 1STRIBd74zuotYU34vUFNn/mfAWQSWajBUNThk/+i
frd3haxnhL9T38QPM+/6+XlnbaRB80nx8SkM2+0+trxYIep9IB1/4owONTTniUr4ZjmdRJV6IS1PebAwm5pcgdOuD85jPxtzKsh/UlYJWZGDxC7f2nnJSdp6aCdUgOCvk3QByFfpXVsqyg2KovFyxx7An+dC4sDzP
ROu3C8QLxkTg==
1221780105      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) IiGq2gRMimq11JdLV/G3WciLvcUPFs4x2p7UDJvO1
r8DWWe60gqvcPILUU+PrHhMAJP8zSYsAKAVAj7zPqoGOHNfBlJSCxPPrMUv0+F8i2IcI71N9cg4Y4v8ZI56mRYo9q4X2I7wH/3ycWSb+RjZBg==
1221780105      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) h+oV/RUtayWrJxU15yystLCLUJS/lc7TfQq3WJnmp
MINzmFyUFSJ7d4TOn7WYOCDaUtRnnqo1Dur8fAyYt6yhCTb2JRnsoyOCZwotmXpidt9akmG2gGgShxZSXZ4uZaC+Aq2StBCp0cZoRT4IlrFXHuZ0miWHkeUA9QOQgUwAbhKRp9zVTJ7Pe0fLhb8DtAwsTWqWeL3n3
MNxsa2F5tbgw==
1221780457      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Wk+JVmlOhayHiHz2DOtP+JF1q2VLJWPIOHNZVaghi
gabJ/YH6rPdxmosA0CmUDNc230IMbtLmYEuXrNNg4t9P8I06bfYfANrI97FeZDkWArOEh9czxM+AJtt10TRBZ/beoUnnYpDV8hZTd22qe22tA==
1221780457      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) QgQLOOV8ZY+ED59nEmNv7Y/wEva4IlA+qDqhKRBwy
L58LoFJ1vgjQdNtxjZJhHCAn/T1XZvp8fGLCW/cA/cprjfWIxn04cC3MmGhpfgPGqb0ITmV9pbgrR10znPKUvvgXmEzHlWv+qGrIMKTCg/lcyWOJ0jlxYURMcssrwGXDv1v+msW9ZyvMDzoMpJqkqtxJ943d2NW5T
+g2oqbsz8V/g==
1221781476      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) MGwB/uhr/pCiYuPDPh5X2uHIaSL4H3vNeOrrCtohj
s9Q05l2ckul9nxo5I+XZSjrYT6osd4SOc6Mu/jjW17EnJhAbwk9hdM8ib0tnSOlnAJVgkllSeMiwzIIYZQjeqc6131GV9UjnUL6Cup91Px/Qw==
1221781476      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) 213vCj1MxqnSZLwfVFLfXbMk6RLw4nfu+s7p0p902
yW52TIVgUMDVd8YTFVYPdT9RmeFgylr7fCBAzSNZ2dqmWjxSDMEjyv5hmD1I2tzKttar5KZmQDfuJx2NHdH17vheb14A2MjzOhhUrgjQoRtaMa+bAw0yTvj37+4mJPU97faIV+erZT/+kY/YQ/HNnC+C+O7Lpmm3H
xKEl2HM4wSsw==
1221783933      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) wzpl/3YK9UYfnjOS98haV9tnJohm+zUq9HqOiqnvh
A3gKHEFtatIG/UqQdiRoJA0S6+m8/IpgbAfMNmfkZgB6KLFpThp0dW6H00gpuqyEF8WVjfGHsS1SqvJc8gRVqLJEn/3TCE5BJjw0NSJPo5V8Q==
1221783933      59.106.145.2    doradora.atzend.com//icon.php   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
```

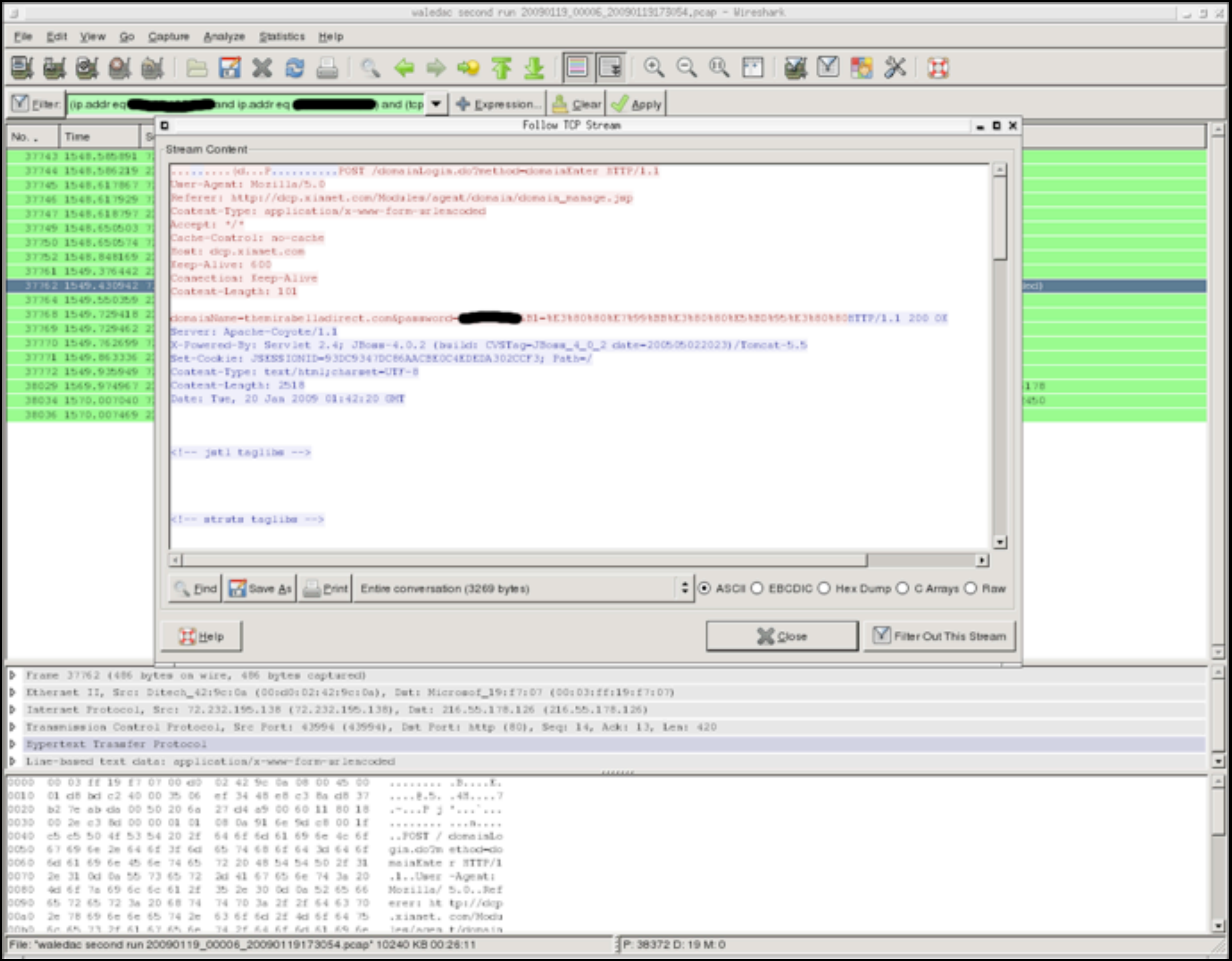
Waledac


Fast-Flux DNS Controller
Head-End C&C
Master Proxies
TSL Servers
Single Tier Peering
Repeater Nodes
NAT'd Nodes
Spammer Nodes

Waledac

- Uses Nodes From Repeater (or Higher) as Proxies
- Manage DNS For Waledac Through These Proxies

Waledac



waledac second run 20090119_00006_20090119173054.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: (ip.addr eq [redacted] and ip.addr eq [redacted] and (tcp

Expression... Clear Apply

```
No. .   Time
37743 1548.585891
37744 1548.586219
37745 1548.617867
37746 1548.617929
37747 1548.618797
37749 1548.650503
37750 1548.650574
37752 1548.848169
37761 1549.376442
37762 1549.430942
37764 1549.550359
37768 1549.729418
37769 1549.729462
37770 1549.762699
37771 1549.863336
37772 1549.935949
38029 1569.974967
38034 1570.007040
38036 1570.007469
```

Follow TCP Stream

Stream Content

```
.........(d...P...........POST /domainLogin.do?method=domainEnter HTTP/1.1
User-Agent: Mozilla/5.0
Referer: http://dcp.xinnet.com/Modules/agent/domain/domain_manage.jsp
Content-Type: application/x-www-form-urlencoded
Accept: */*
Cache-Control: no-cache
Host: dcp.xinnet.com
Keep-Alive: 600
Connection: Keep-Alive
Content-Length: 101

domainName=themirabelladirect.com&password=[redacted]&B1=%E3%80%80%E7%99%BB%E3%80%80%E5%BD%95%E3%80%80HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.4; JBoss-4.0.2 (build: CVSTag=JBoss_4_0_2 date=200505022023)/Tomcat-5.5
Set-Cookie: JSESSIONID=93DC9347DC86AACBE0C4EDEDA302CCF3; Path=/
Content-Type: text/html;charset=UTF-8
Content-Length: 2518
Date: Tue, 20 Jan 2009 01:42:20 GMT



<!-- jstl taglibs -->



<!-- struts taglibs -->
```

Entire conversation (3269 bytes)

● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw

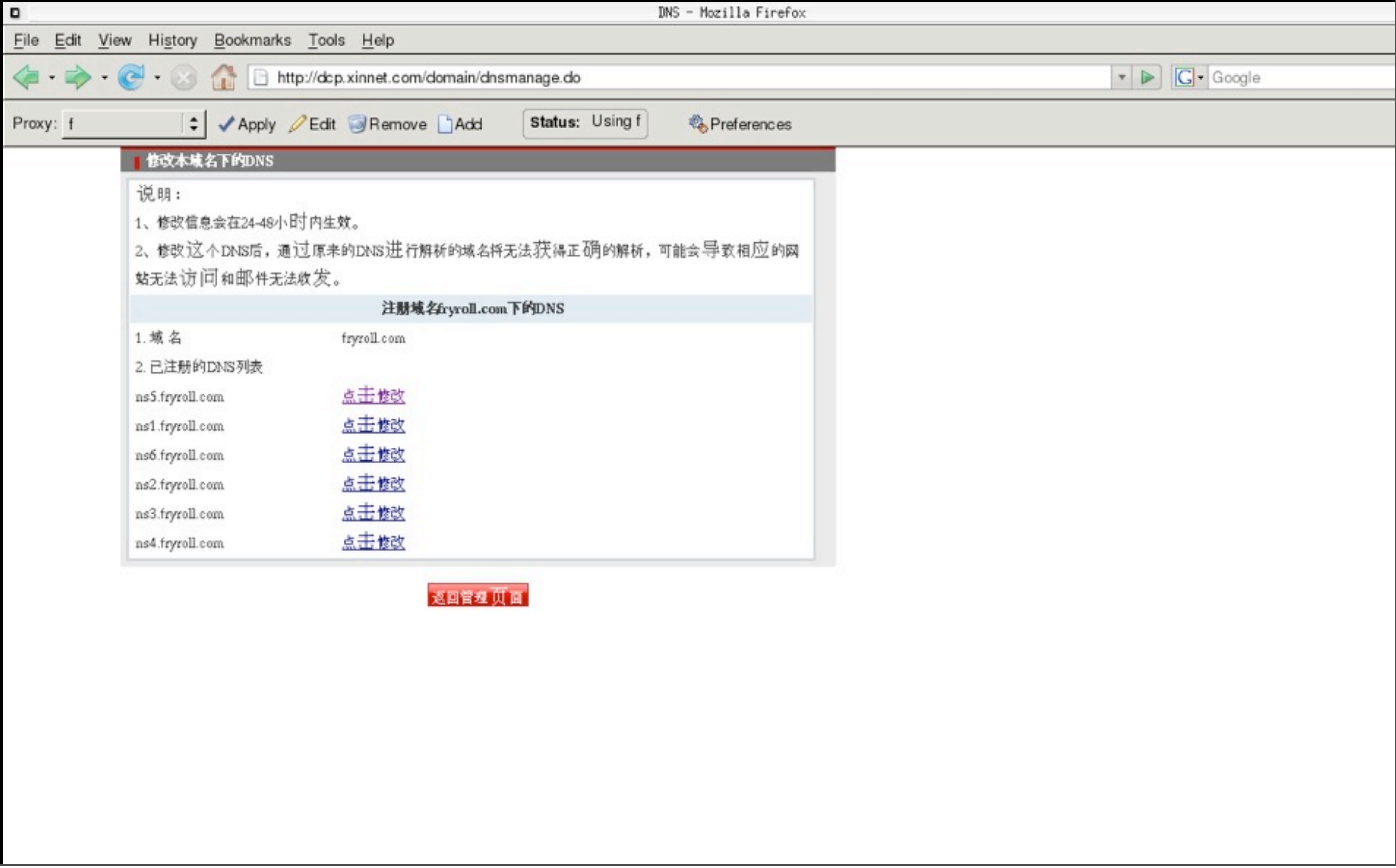
```
▷ Frame 37762 (486 bytes on wire, 486 bytes captured)
▷ Ethernet II, Src: Ditech_42:9c:0a (00:d0:02:42:9c:0a), Dst: Microsof_19:f7:07 (00:03:ff:19:f7:07)
▷ Internet Protocol, Src: 72.232.195.138 (72.232.195.138), Dst: 216.55.178.126 (216.55.178.126)
▷ Transmission Control Protocol, Src Port: 43994 (43994), Dst Port: http (80), Seq: 14, Ack: 13, Len: 420
▷ Hypertext Transfer Protocol
▷ Line-based text data: application/x-www-form-urlencoded
```

```
0000  00 03 ff 19 f7 07 00 d0  02 42 9c 0a 08 00 45 00   ........ .B....E.
0010  01 d8 bd c2 40 00 35 06  ef 34 48 e8 c3 8a d8 37   ....@.5. .4H....7
0020  b2 7e ab da 00 50 20 6a  27 d4 a9 00 60 11 80 18   .~...P j '...`...
0030  00 2e c3 8d 00 00 01 01  08 0a 91 6e 9d c8 00 1f   ........ ...n....
0040  c5 c5 50 4f 53 54 20 2f  64 6f 6d 61 69 6e 4c 6f   ..POST / domainLo
0050  67 69 6e 2e 64 6f 3f 6d  65 74 68 6f 64 3d 64 6f   gin.do?m ethod=do
0060  6d 61 69 6e 45 6e 74 65  72 20 48 54 54 50 2f 31   mainEnte r HTTP/1
0070  2e 31 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   .1..User -Agent: 
0080  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 0d 0a 52 65 66   Mozilla/ 5.0..Ref
0090  65 72 65 72 3a 20 68 74  74 70 3a 2f 2f 64 63 70   erer: ht tp://dcp
00a0  2e 78 69 6e 6e 65 74 2e  63 6f 6d 2f 4d 6f 64 75   .xinnet. com/Modu
00b0  6c 65 73 2f 61 67 65 6e  74 2f 64 6f 6d 61 69 6e   les/agen t/domain
```

File: "waledac second run 20090119_00006_20090119173054.pcap" 10240 KB 00:26:11

P: 38372 D: 19 M: 0

Waledac


DNS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://dcp.xinnet.com/domain/dnsmanage.do
Google
Proxy: f
Apply
Edit
Remove
Add
Status: Using f
Preferences

修改本域名下的DNS

说明：

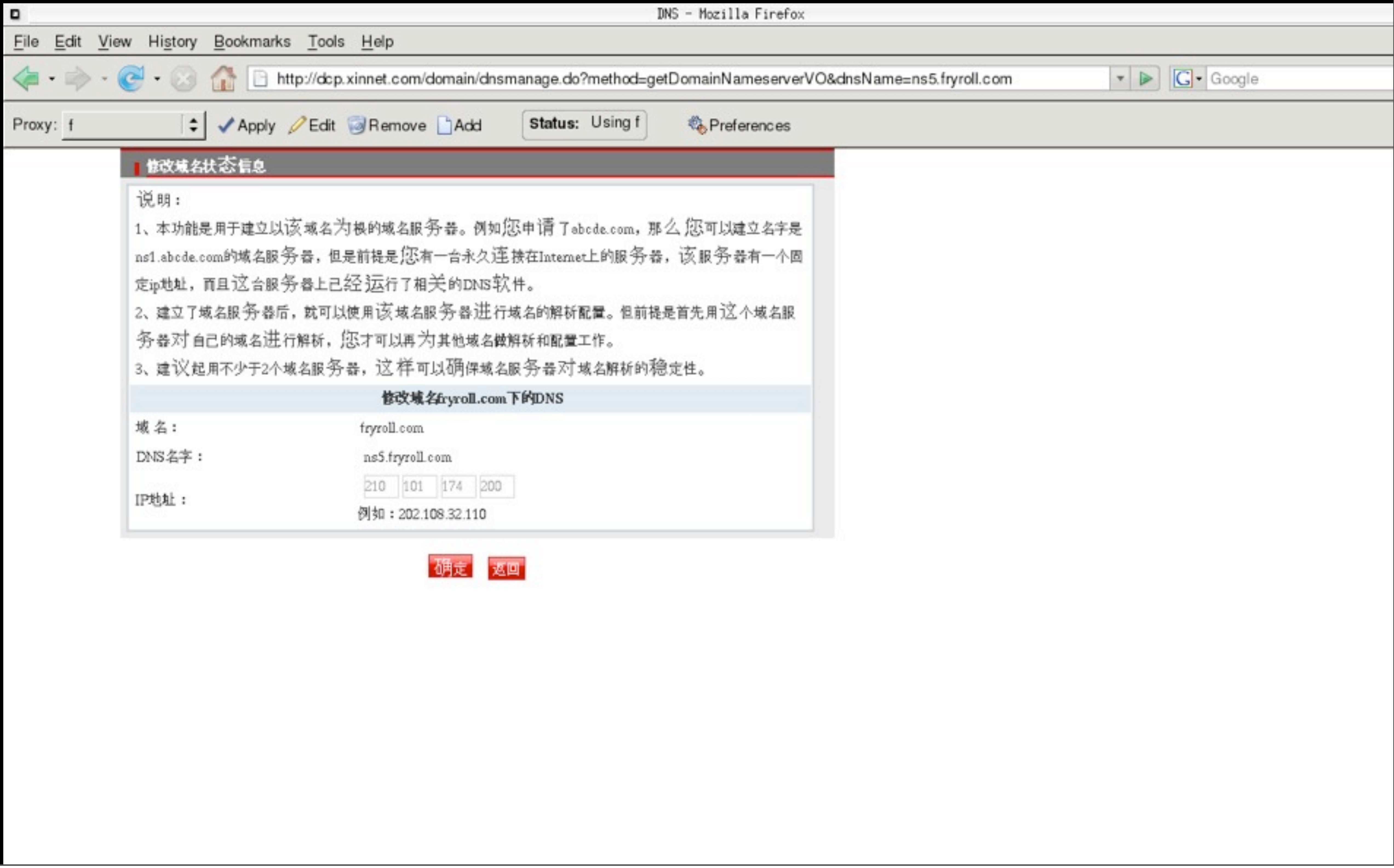
1、修改信息会在24-48小时内生效。

2、修改这个DNS后，通过原来的DNS进行解析的域名将无法获得正确的解析，可能会导致相应的网站无法访问和邮件无法收发。

注册域名fryroll.com下的DNS

1. 域 名	fryroll.com
2. 已注册的DNS列表	
ns5.fryroll.com	点击修改
ns1.fryroll.com	点击修改
ns6.fryroll.com	点击修改
ns2.fryroll.com	点击修改
ns3.fryroll.com	点击修改
ns4.fryroll.com	点击修改

Waledac



http://dcp.xinnet.com/domain/dnsmanage.do?method=getDomainNameserverVO&dnsName=ns5.fryroll.com

修改域名状态信息

说明：

1、本功能是用于建立以该域名为根的域名服务器。例如您申请了abcde.com，那么您可以建立名字是ns1.abcde.com的域名服务器，但是前提是您有一台永久连接在Internet上的服务器，该服务器有一个固定ip地址，而且这台服务器上已经运行了相关的DNS软件。

2、建立了域名服务器后，就可以使用该域名服务器进行域名的解析配置。但前提是首先用这个域名服务器对自己的域名进行解析，您才可以再为其他域名做解析和配置工作。

3、建议起用不少于2个域名服务器，这样可以确保域名服务器对域名解析的稳定性。

修改域名fryroll.com下的DNS

域 名：	fryroll.com
DNS名字：	ns5.fryroll.com
IP地址：	210 101 174 200 例如：202.108.32.110

Waledac

- Have Control
- Legal Issues
- Originating IP Not Waledac-based
- Original IP Tunneling Through LayeredTech
  - Seize Machine
  - Trace Next Hop Backward

Attackers vs Researchers

- Researcher Footprints
  - IPs
  - UAs
  - OSs
  - Files on the system (more on this later)
- Unavoidable

Attackers vs Researchers

- bad guys finding researchers (BBB)

Attackers vs Researchers

- researchers trying to hide (tigger)

Researcher vs Researcher

- researchers deceiving other researchers (TE)

Mike's Top 5 Worst Researcher Actions of 2009

5. Blogging someone else's exploit to get into an attacker's control panel
4. Using an attacker's shell shared on a mailing list to rm -rf stolen data and insert profanities to attacker
3. Helping an attacker firewall researchers
2. Destroying two years worth of access for press
1. Manually killing researchers connections that try to recover data

Small Scale Attacks

- [CONTENT REMOVED FROM PUBLICLY PUBLISHED SLIDES]

How Targeted Is It?

- [CONTENT REMOVED FROM PUBLICLY PUBLISHED SLIDES]

Dangers of Previous Slide

- [CONTENT REMOVED FROM PUBLICLY PUBLISHED SLIDES]

Or You Can Do This...

- [SS of Fake Return Address e-mail]

Counter-Attack Methods

- Counter-Attack Disinformation Campaigns
- Tracking
- Hack-Back Attacks

Disinformation Diagramming

- [CONTENT REMOVED FROM PUBLICLY PUBLISHED SLIDES]

Pre-Attack Tracking

- Search Web Site Logs
- Analyze and Correlate Visitors
  - Focus on Pages with Contacts
  - Pay Attention to Referrer

Post-Attack Tracking

- Save All E-mail Header Information
- Entice Attacker to Click URL
    - E-mail back if address real
    - Visit special URLs that will be keylogged

“Special” URLs

- Use scripts to capture IP and attempt to determine whether a proxy is used
  - Javascript
  - Java
  - Flash
  - Silverlight
  - DNS Resolution

“Special” URL Demo

- [CONTENT REMOVED FROM PUBLICLY PUBLISHED SLIDES]

Hacking Back

- Direct Connection Backdoors Often Relayed Through Proxy
- Most Backdoors We Care About Written in C/C++
- Web-based Connect Back Usually ASP/PHP

Hacking Back Example

- [CONTENT REMOVED FROM PUBLICLY PUBLISHED SLIDES]

Conclusions

Learn the Law

Conclusions

You Can’t Fight If You Don’t Know Who Your Enemy Is

Conclusions

- Fingerprint
- Look for footprints
- Use disinformation
- Beware of misinformation and disinformation
- Be careful what you say and do publicly

Q & A

Michael La Pilla
VeriSign iDefense Malicious Code Operations Team
mlapilla@idefense.com