ARBOR®
NETWORKS

Adventures In Open Directories

```
env x='() { :;}; echo "#vb2014"' bash -c true
```

Matt Bing

mbing@arbor.net

@mattbing

About Me

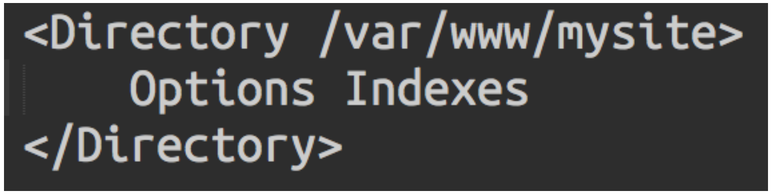
- *2012-Present* - security research analyst

ARBOR SERT

- *2004-2012* – incident response coordinator

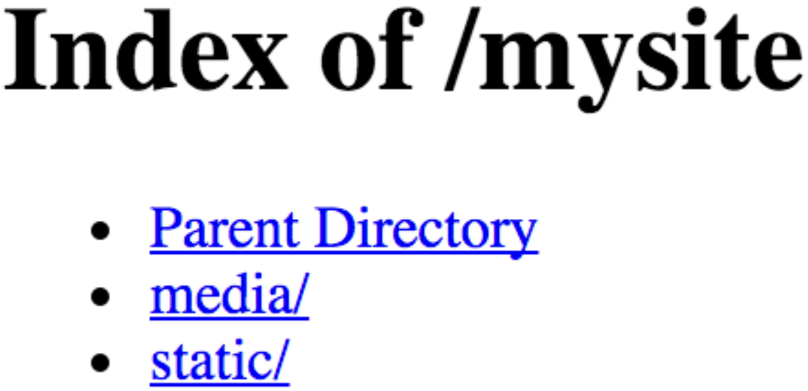
UNIVERSITY OF
MICHIGAN

mod_autoindex



```
<Directory /var/www/mysite>
    Options Indexes
</Directory>
```

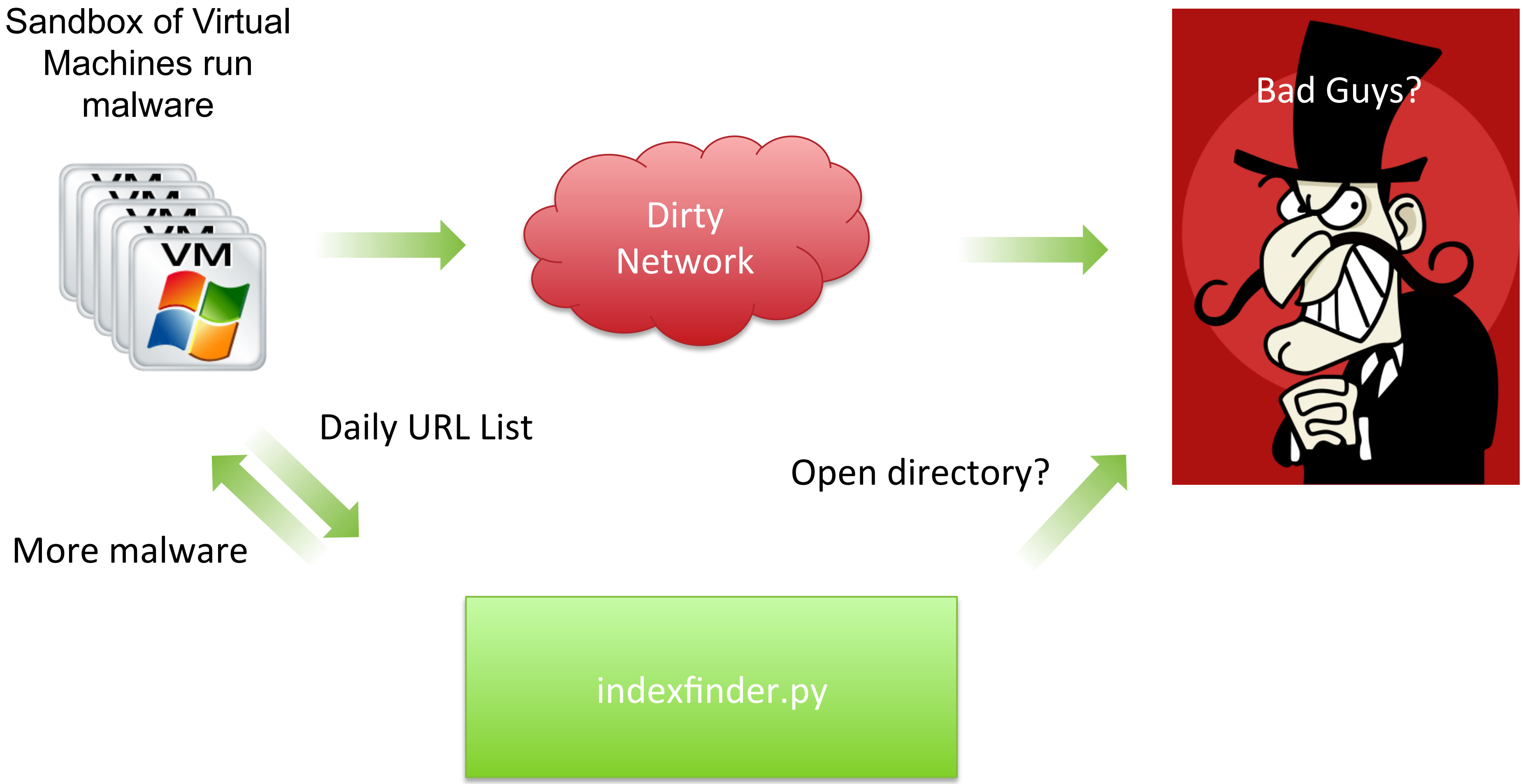
On by default! (mostly)



Index of /mysite

- Parent Directory
- media/
- static/

Architecture Overview



Sandbox of Virtual Machines run malware

Dirty Network

Bad Guys?

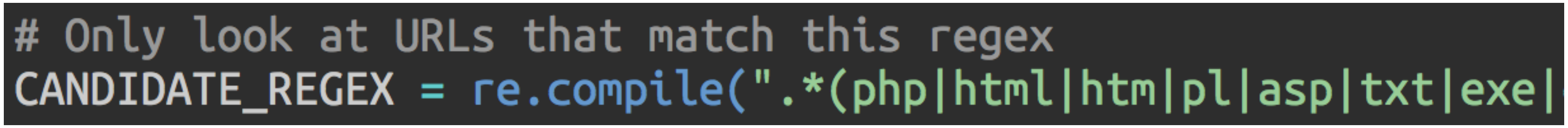
Daily URL List

Open directory?

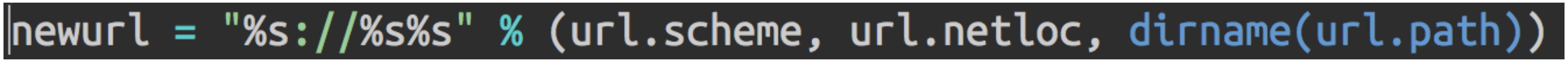
More malware

indexfinder.py

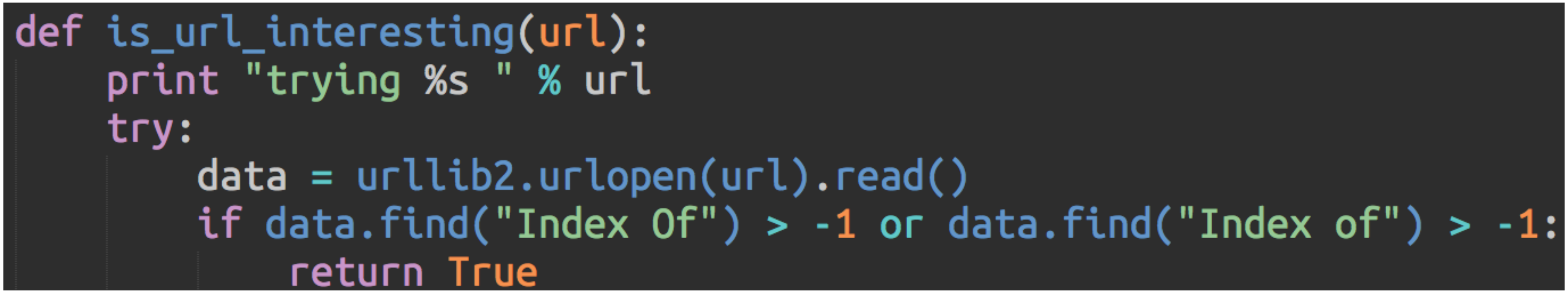
indexfinder.py



```
# Only look at URLs that match this regex
CANDIDATE_REGEX = re.compile(".*(php|html|htm|pl|asp|txt|exe|
```



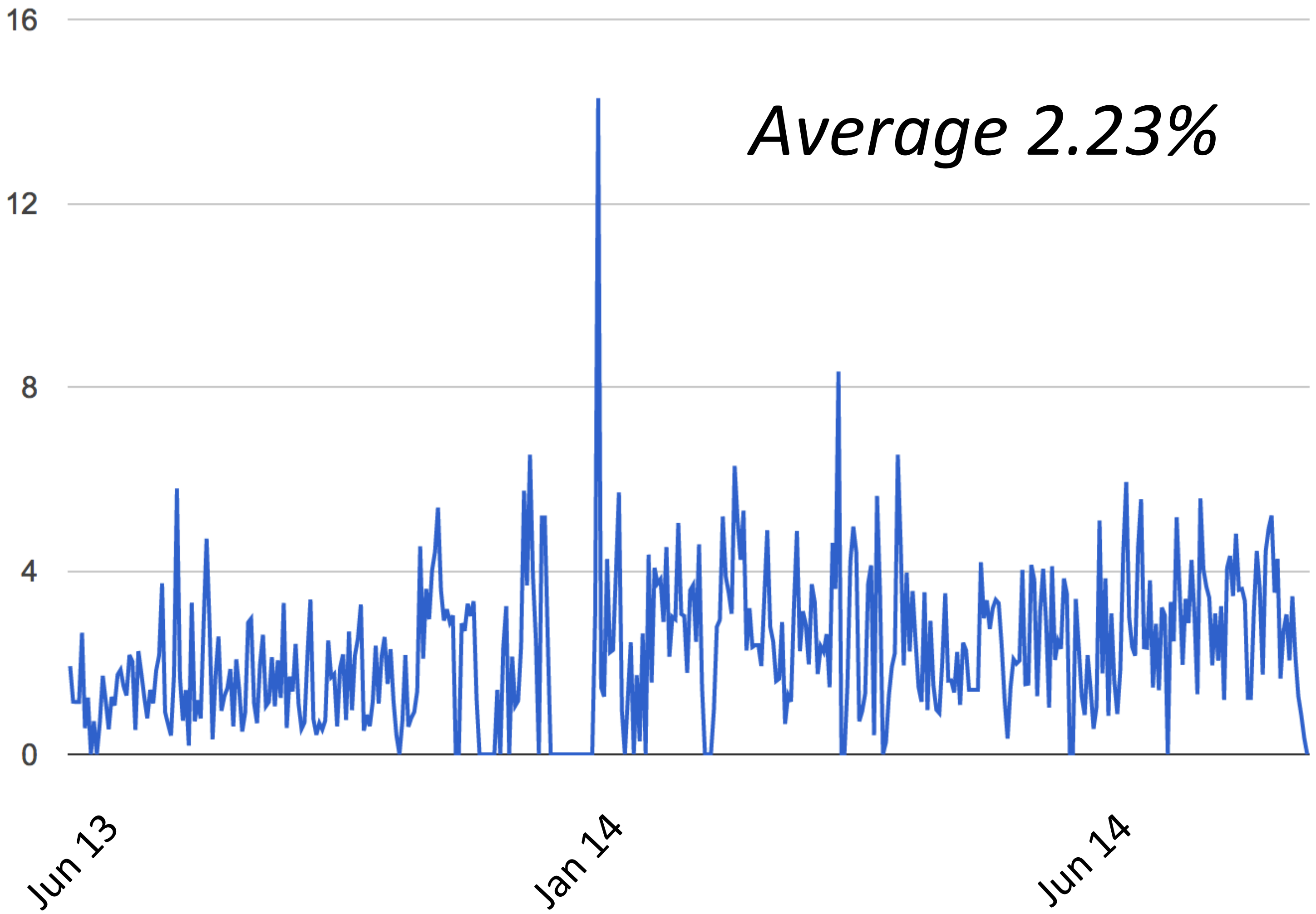
```
newurl = "%s://%s%s" % (url.scheme, url.netloc, dirname(url.path))
```



```
def is_url_interesting(url):
    print "trying %s " % url
    try:
        data = urllib2.urlopen(url).read()
        if data.find("Index Of") > -1 or data.find("Index of") > -1:
            return True
```

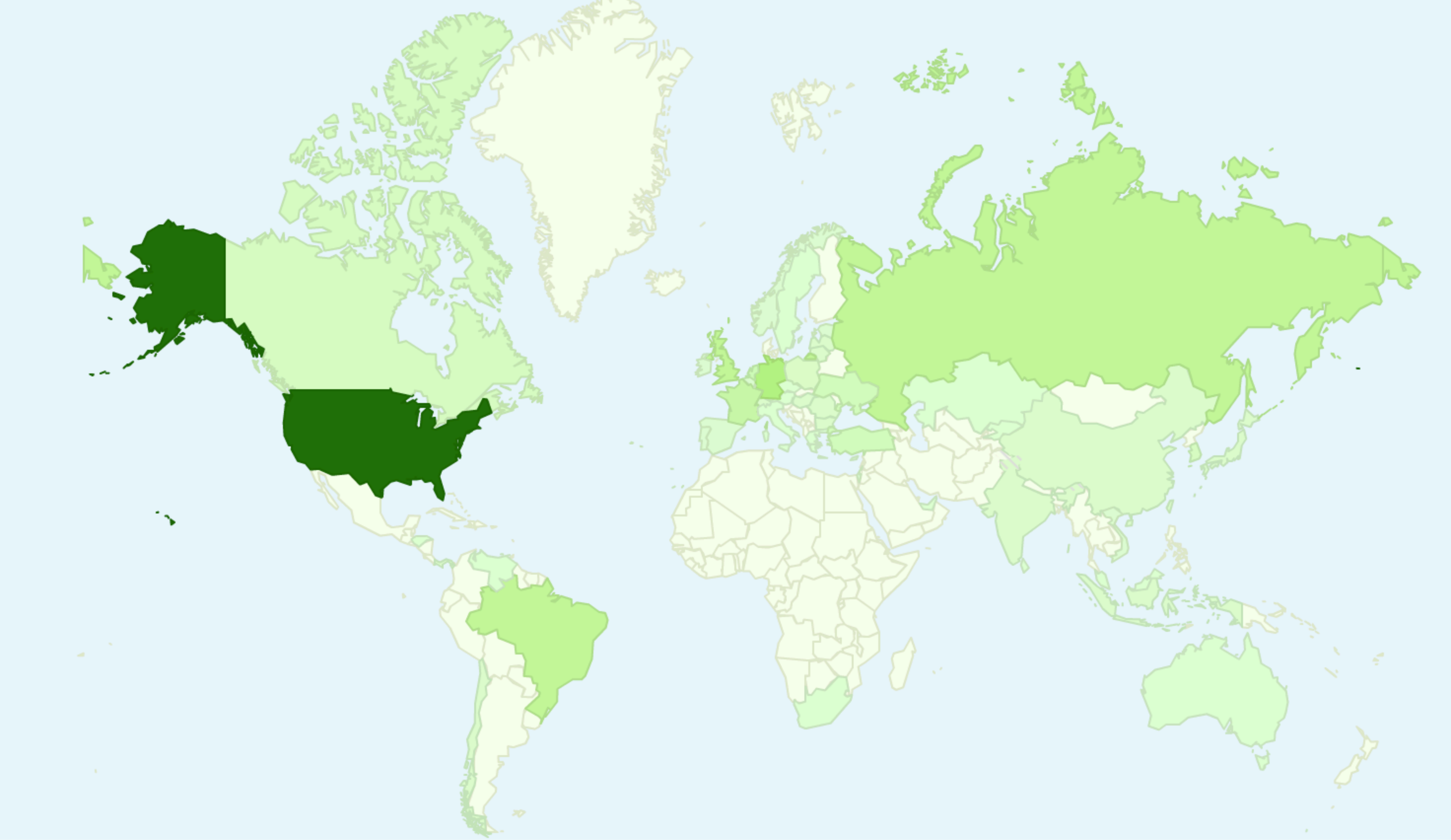
ARBOR®
NETWORKS

Percentage Of Open Directories

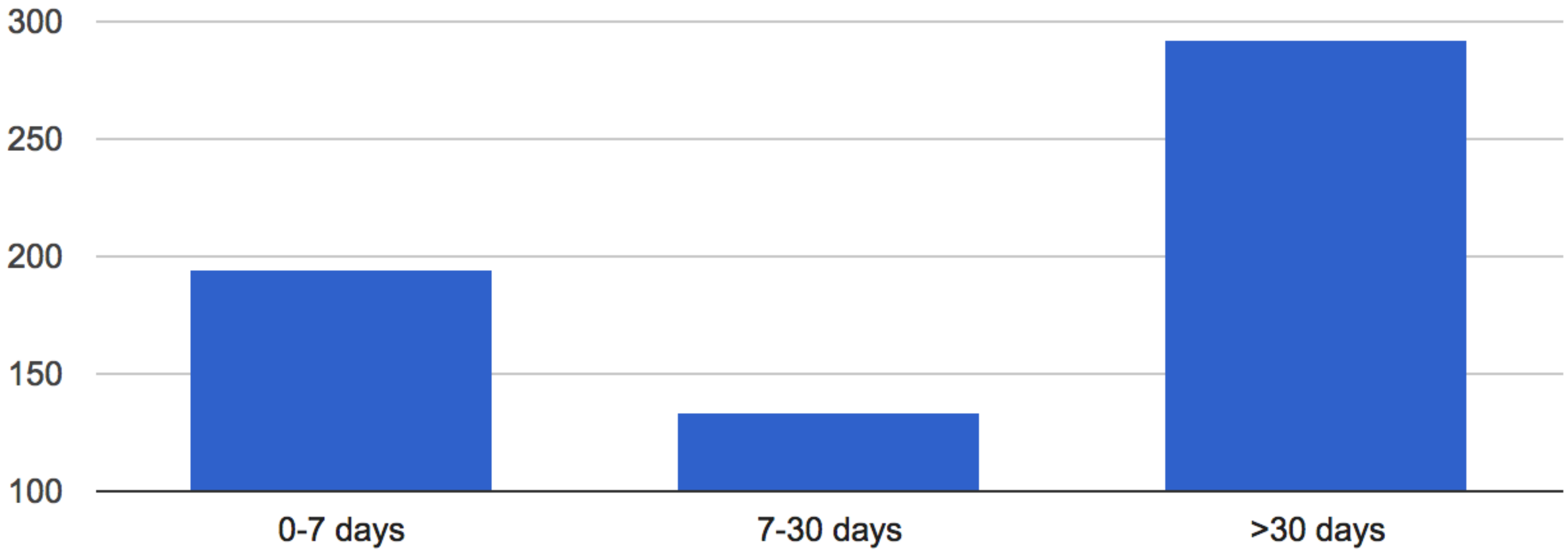


Average 2.23%

Open Directory Heatmap



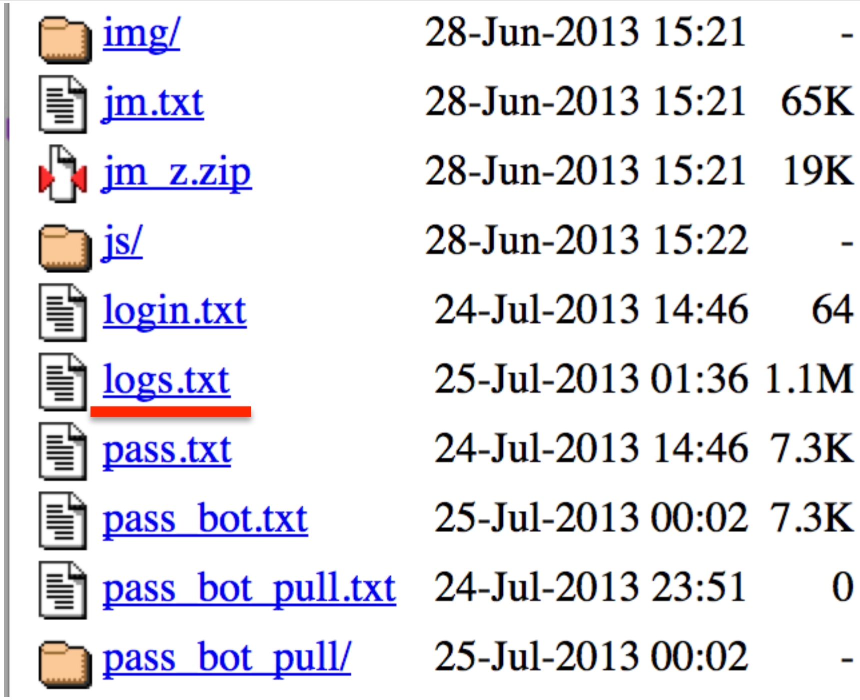
Hot New Malware



Discovery Time - Compile Time*

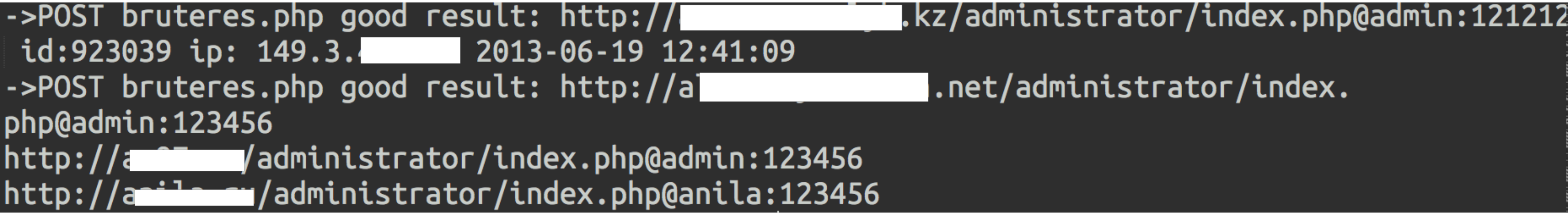
** Yes, compile time can be faked*

Fort Disco



img/	28-Jun-2013 15:21	-
jm.txt	28-Jun-2013 15:21	65K
jm_z.zip	28-Jun-2013 15:21	19K
js/	28-Jun-2013 15:22	-
login.txt	24-Jul-2013 14:46	64
logs.txt	25-Jul-2013 01:36	1.1M
pass.txt	24-Jul-2013 14:46	7.3K
pass_bot.txt	25-Jul-2013 00:02	7.3K
pass_bot_pull.txt	24-Jul-2013 23:51	0
pass_bot_pull/	25-Jul-2013 00:02	-

What 'Fort Disco' Might Look Like



```
->POST bruteres.php good result: http://[redacted].kz/administrator/index.php@admin:121212
 id:923039 ip: 149.3.[redacted] 2013-06-19 12:41:09
->POST bruteres.php good result: http://a[redacted].net/administrator/index.
php@admin:123456
http://a[redacted]/administrator/index.php@admin:123456
http://a[redacted]/administrator/index.php@anila:123456
```

Description Fort Disco Mild Fore Mend Beeps

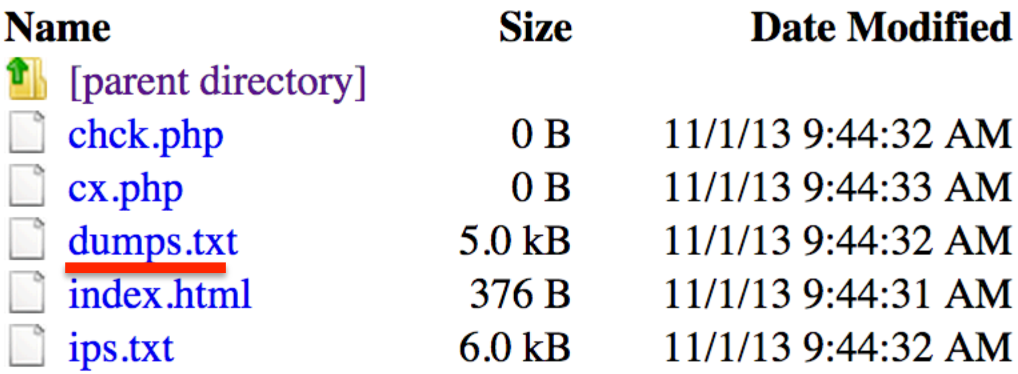
6,000+ Compromised sites

25,000+ Infected hosts

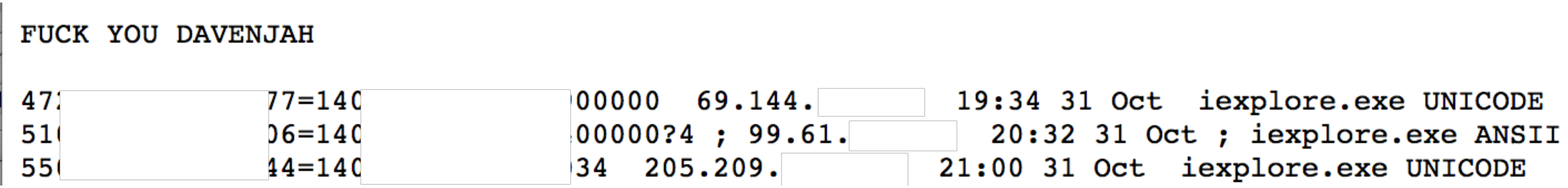
ARBOR NETWORKS

Source: https://community.webroot.com/t5/Security-Industry-News/quot-Fort-Disco-quot-Botnet-Hustles-onto-the-Stage/td-p/53080

Carders



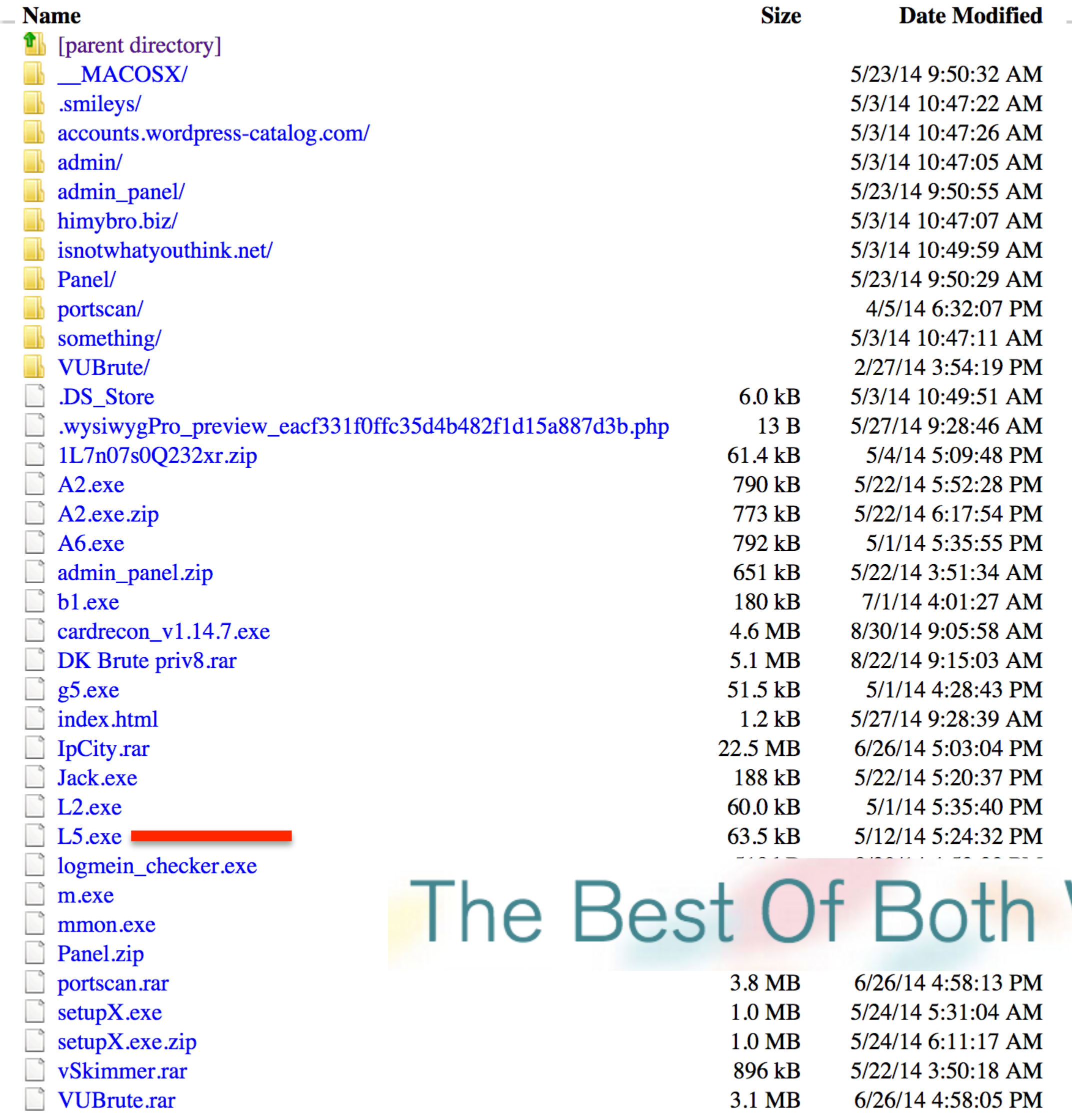
Name	Size	Date Modified
[parent directory]		
chck.php	0 B	11/1/13 9:44:32 AM
cx.php	0 B	11/1/13 9:44:33 AM
dumps.txt	5.0 kB	11/1/13 9:44:32 AM
index.html	376 B	11/1/13 9:44:31 AM
ips.txt	6.0 kB	11/1/13 9:44:32 AM



```
FUCK YOU DAVENJAH

47[redacted]77=140[redacted]00000  69.144.[redacted]  19:34 31 Oct  iexplore.exe UNICODE
51[redacted]06=140[redacted]00000?4 ; 99.61.[redacted]  20:32 31 Oct ; iexplore.exe ANSII
55[redacted]44=140[redacted]34  205.209.[redacted]  21:00 31 Oct  iexplore.exe UNICODE
```

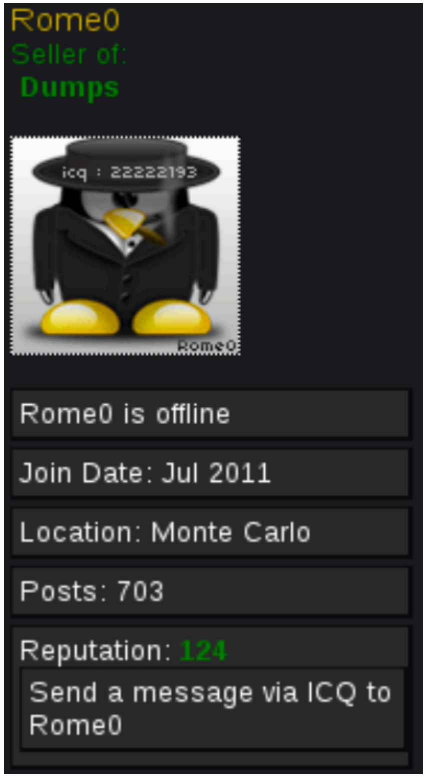
- Project Hook log file
- 200+ track1/track2 card data

Wherefore Art Thou Rome0?



Name	Size	Date Modified
[parent directory]		
__MACOSX/		5/23/14 9:50:32 AM
.smileys/		5/3/14 10:47:22 AM
accounts.wordpress-catalog.com/		5/3/14 10:47:26 AM
admin/		5/3/14 10:47:05 AM
admin_panel/		5/23/14 9:50:55 AM
himybro.biz/		5/3/14 10:47:07 AM
isnotwhatyouthink.net/		5/3/14 10:49:59 AM
Panel/		5/23/14 9:50:29 AM
portscan/		4/5/14 6:32:07 PM
something/		5/3/14 10:47:11 AM
VUBrute/		2/27/14 3:54:19 PM
.DS_Store	6.0 kB	5/3/14 10:49:51 AM
.wysiwygPro_preview_eacf331f0ffc35d4b482f1d15a887d3b.php	13 B	5/27/14 9:28:46 AM
1L7n07s0Q232xr.zip	61.4 kB	5/4/14 5:09:48 PM
A2.exe	790 kB	5/22/14 5:52:28 PM
A2.exe.zip	773 kB	5/22/14 6:17:54 PM
A6.exe	792 kB	5/1/14 5:35:55 PM
admin_panel.zip	651 kB	5/22/14 3:51:34 AM
b1.exe	180 kB	7/1/14 4:01:27 AM
cardrecon_v1.14.7.exe	4.6 MB	8/30/14 9:05:58 AM
DK Brute priv8.rar	5.1 MB	8/22/14 9:15:03 AM
g5.exe	51.5 kB	5/1/14 4:28:43 PM
index.html	1.2 kB	5/27/14 9:28:39 AM
IpCity.rar	22.5 MB	6/26/14 5:03:04 PM
Jack.exe	188 kB	5/22/14 5:20:37 PM
L2.exe	60.0 kB	5/1/14 5:35:40 PM
L5.exe	63.5 kB	5/12/14 5:24:32 PM
logmein_checker.exe		
m.exe		
mmon.exe		
Panel.zip		
portscan.rar	3.8 MB	6/26/14 4:58:13 PM
setupX.exe	1.0 MB	5/24/14 5:31:04 AM
setupX.exe.zip	1.0 MB	5/24/14 6:11:17 AM
vSkimmer.rar	896 kB	5/22/14 3:50:18 AM
VUBrute.rar	3.1 MB	6/26/14 4:58:05 PM

The Best Of Both Worlds – Soraya



Rome0
Seller of:
Dumps

Rome0 is offline

Join Date: Jul 2011

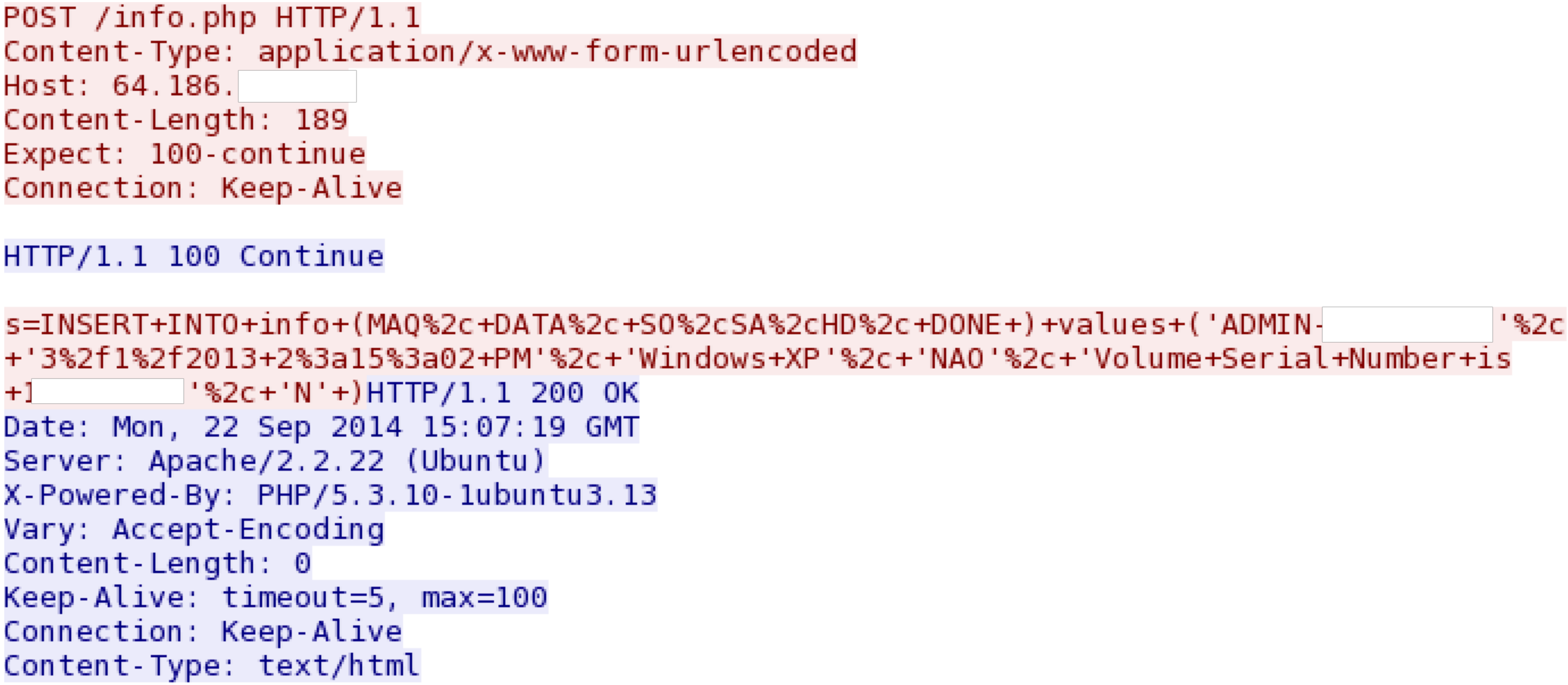
Location: Monte Carlo

Posts: 703

Reputation: 124

Send a message via ICQ to Rome0

What Could Go Wrong?



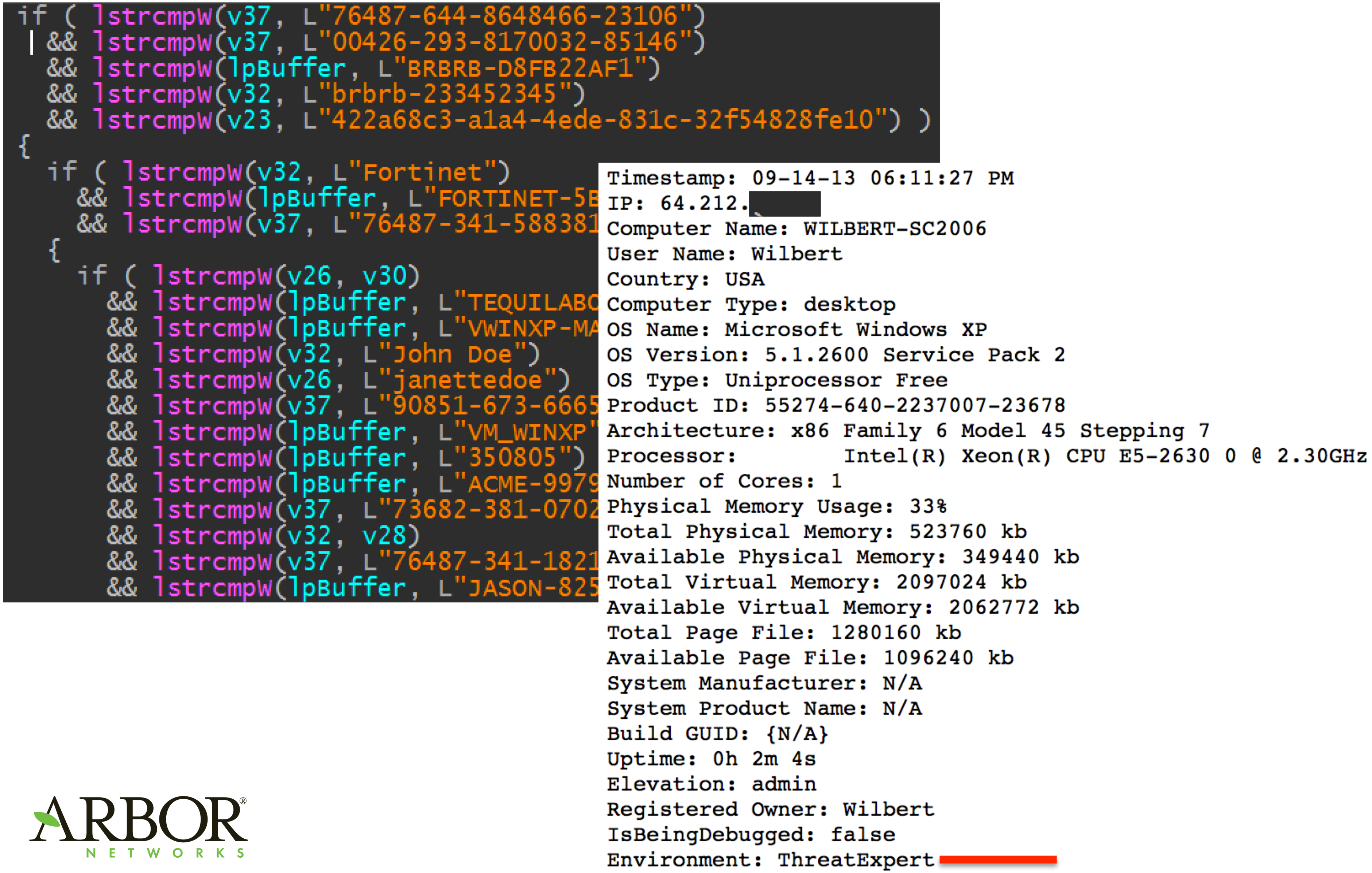
```
POST /info.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: 64.186.[redacted]
Content-Length: 189
Expect: 100-continue
Connection: Keep-Alive

HTTP/1.1 100 Continue

s=INSERT+INTO+info+(MAQ%2c+DATA%2c+SO%2cSA%2cHD%2c+DONE+)+values+('ADMIN-[redacted]'%2c
+'3%2f1%2f2013+2%3a15%3a02+PM'%2c+'Windows+XP'%2c+'NAO'%2c+'Volume+Serial+Number+is
+[redacted]'%2c+'N'+)HTTP/1.1 200 OK
Date: Mon, 22 Sep 2014 15:07:19 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.13
Vary: Accept-Encoding
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Advanced Persistent Directory

- Not just dumb cyber criminals
- Attack against XXXXXXX gov’t agency
- Custom C2 with an open directory

```
0000000:                                              GOV-PC
0000010:
0000020:
0000030:
0000040:
```

Researcher Profiling

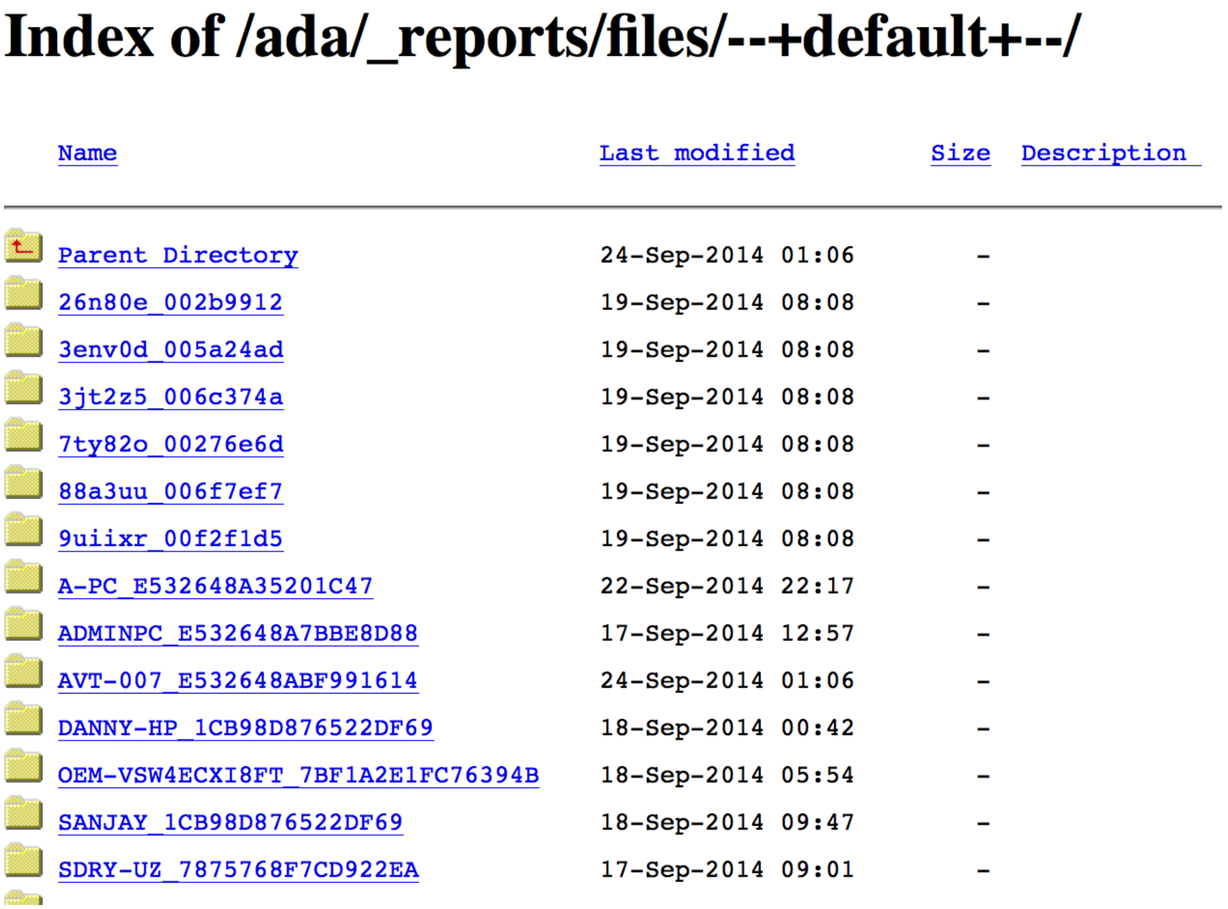


```
if ( lstrcmpW(v37, L"76487-644-8648466-23106")
  && lstrcmpW(v37, L"00426-293-8170032-85146")
  && lstrcmpW(lpBuffer, L"BRBRB-D8FB22AF1")
  && lstrcmpW(v32, L"brbrb-233452345")
  && lstrcmpW(v23, L"422a68c3-a1a4-4ede-831c-32f54828fe10") )
{
  if ( lstrcmpW(v32, L"Fortinet")
    && lstrcmpW(lpBuffer, L"FORTINET-5B
    && lstrcmpW(v37, L"76487-341-588381
  {
    if ( lstrcmpW(v26, v30)
      && lstrcmpW(lpBuffer, L"TEQUILABC
      && lstrcmpW(lpBuffer, L"VWINXP-MA
      && lstrcmpW(v32, L"John Doe")
      && lstrcmpW(v26, L"janettedoe")
      && lstrcmpW(v37, L"90851-673-6665
      && lstrcmpW(lpBuffer, L"VM_WINXP"
      && lstrcmpW(lpBuffer, L"350805")
      && lstrcmpW(lpBuffer, L"ACME-9979
      && lstrcmpW(v37, L"73682-381-0702
      && lstrcmpW(v32, v28)
      && lstrcmpW(v37, L"76487-341-1821
      && lstrcmpW(lpBuffer, L"JASON-825
```

```
Timestamp: 09-14-13 06:11:27 PM
IP: 64.212.[redacted]
Computer Name: WILBERT-SC2006
User Name: Wilbert
Country: USA
Computer Type: desktop
OS Name: Microsoft Windows XP
OS Version: 5.1.2600 Service Pack 2
OS Type: Uniprocessor Free
Product ID: 55274-640-2237007-23678
Architecture: x86 Family 6 Model 45 Stepping 7
Processor:          Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz
Number of Cores: 1
Physical Memory Usage: 33%
Total Physical Memory: 523760 kb
Available Physical Memory: 349440 kb
Total Virtual Memory: 2097024 kb
Available Virtual Memory: 2062772 kb
Total Page File: 1280160 kb
Available Page File: 1096240 kb
System Manufacturer: N/A
System Product Name: N/A
Build GUID: {N/A}
Uptime: 0h 2m 4s
Elevation: admin
Registered Owner: Wilbert
IsBeingDebugged: false
Environment: ThreatExpert
```

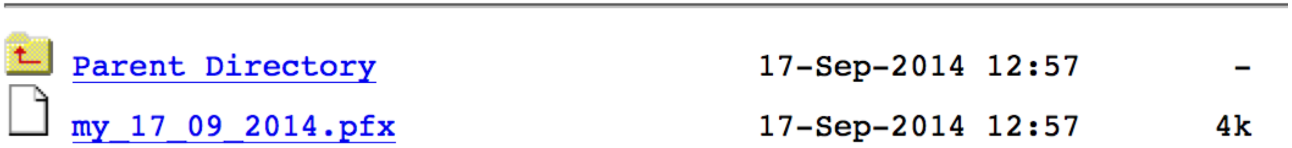
ARBOR® NETWORKS

Zeus Variant



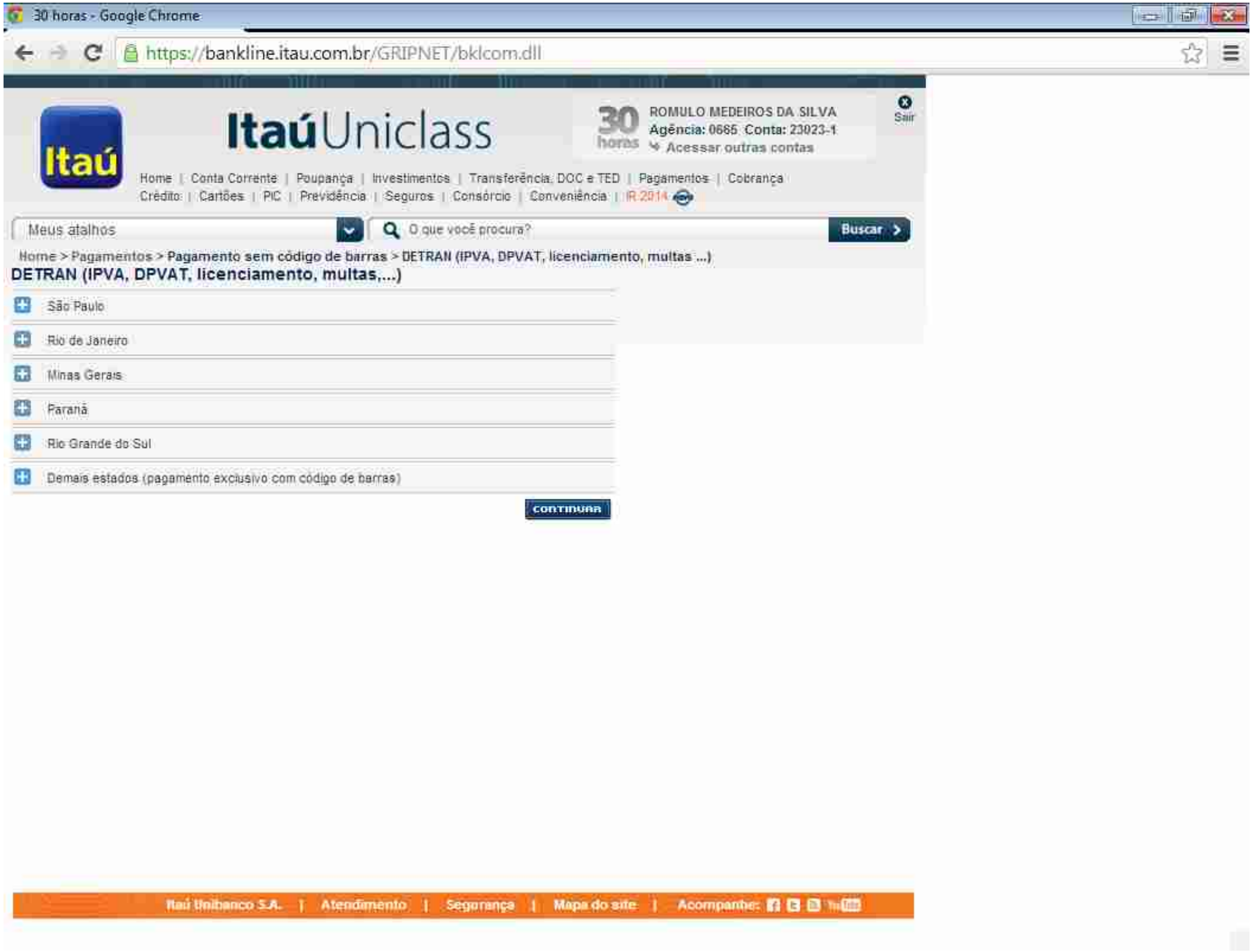
Index of /ada/_reports/files/--+default+--/

Name	Last modified	Size	Description
Parent Directory	24-Sep-2014 01:06	-	
26n80e_002b9912	19-Sep-2014 08:08	-	
3env0d_005a24ad	19-Sep-2014 08:08	-	
3jt2z5_006c374a	19-Sep-2014 08:08	-	
7ty82o_00276e6d	19-Sep-2014 08:08	-	
88a3uu_006f7ef7	19-Sep-2014 08:08	-	
9uiixr_00f2f1d5	19-Sep-2014 08:08	-	
A-PC_E532648A35201C47	22-Sep-2014 22:17	-	
ADMINPC_E532648A7BBE8D88	17-Sep-2014 12:57	-	
AVT-007_E532648ABF991614	24-Sep-2014 01:06	-	
DANNY-HP_1CB98D876522DF69	18-Sep-2014 00:42	-	
OEM-VSW4ECXI8FT_7BF1A2E1FC76394B	18-Sep-2014 05:54	-	
SANJAY_1CB98D876522DF69	18-Sep-2014 09:47	-	
SDRY-UZ_7875768F7CD922EA	17-Sep-2014 09:01	-	



Parent Directory	17-Sep-2014 12:57	-
my_17_09_2014.pfx	17-Sep-2014 12:57	4k

?????



30 horas - Google Chrome
https://bankline.itau.com.br/GRIPNET/bklcom.dll
Itaú
ItaúUniclass
30 horas
Sair
Home | Conta Corrente | Poupança | Investimentos | Transferência, DOC e TED | Pagamentos | Cobrança
Crédito | Cartões | PIC | Previdência | Seguros | Consórcio | Conveniência | IR 2014
Meus atalhos
O que você procura?
Buscar
CONTINUAR
Itaú Unibanco S.A. | Atendimento | Segurança | Mapa do site | Acompanhe:

ROMULO MEDEIROS DA SILVA
Agência: 0665 Conta: 23023-1
Acessar outras contas

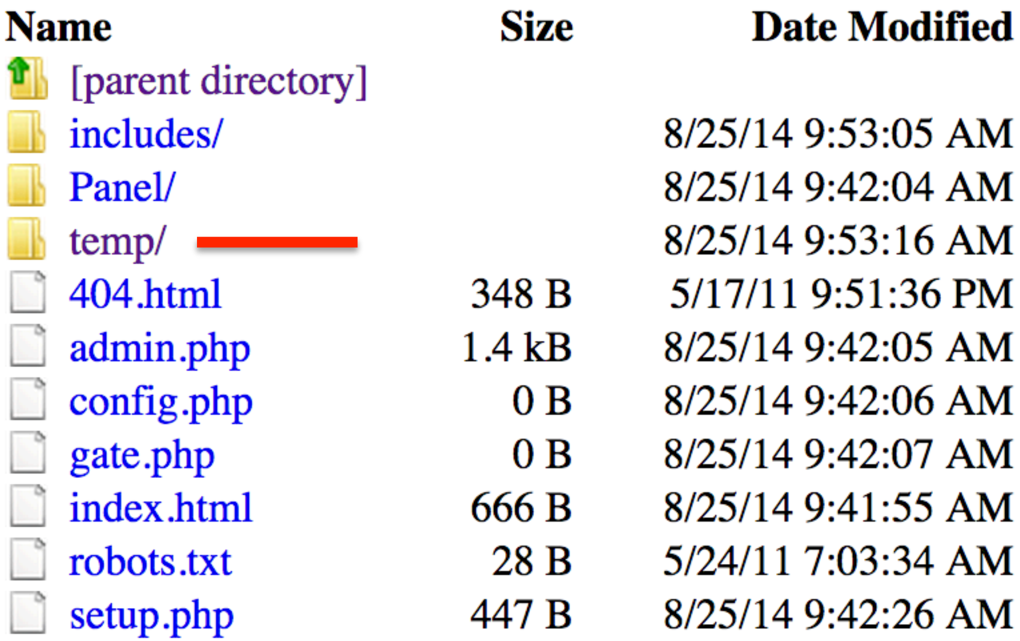
Home > Pagamentos > Pagamento sem código de barras > DETRAN (IPVA, DPVAT, licenciamento, multas ...)

DETRAN (IPVA, DPVAT, licenciamento, multas,...)

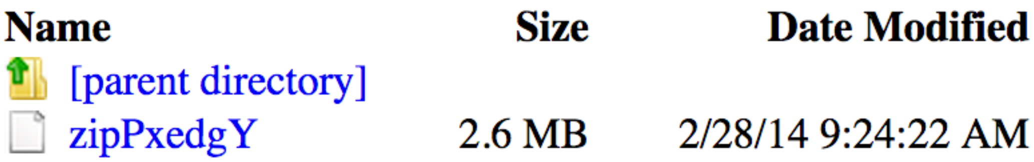
- ⊞ São Paulo
- ⊞ Rio de Janeiro
- ⊞ Minas Gerais
- ⊞ Paraná
- ⊞ Rio Grande do Sul
- ⊞ Demais estados (pagamento exclusivo com código de barras)

Pony Panel After Pony Panel After Pony Panel After Pony Panel After Pony Panel

- I can spot a Pony panel from two towns over
- Not interesting, until it is

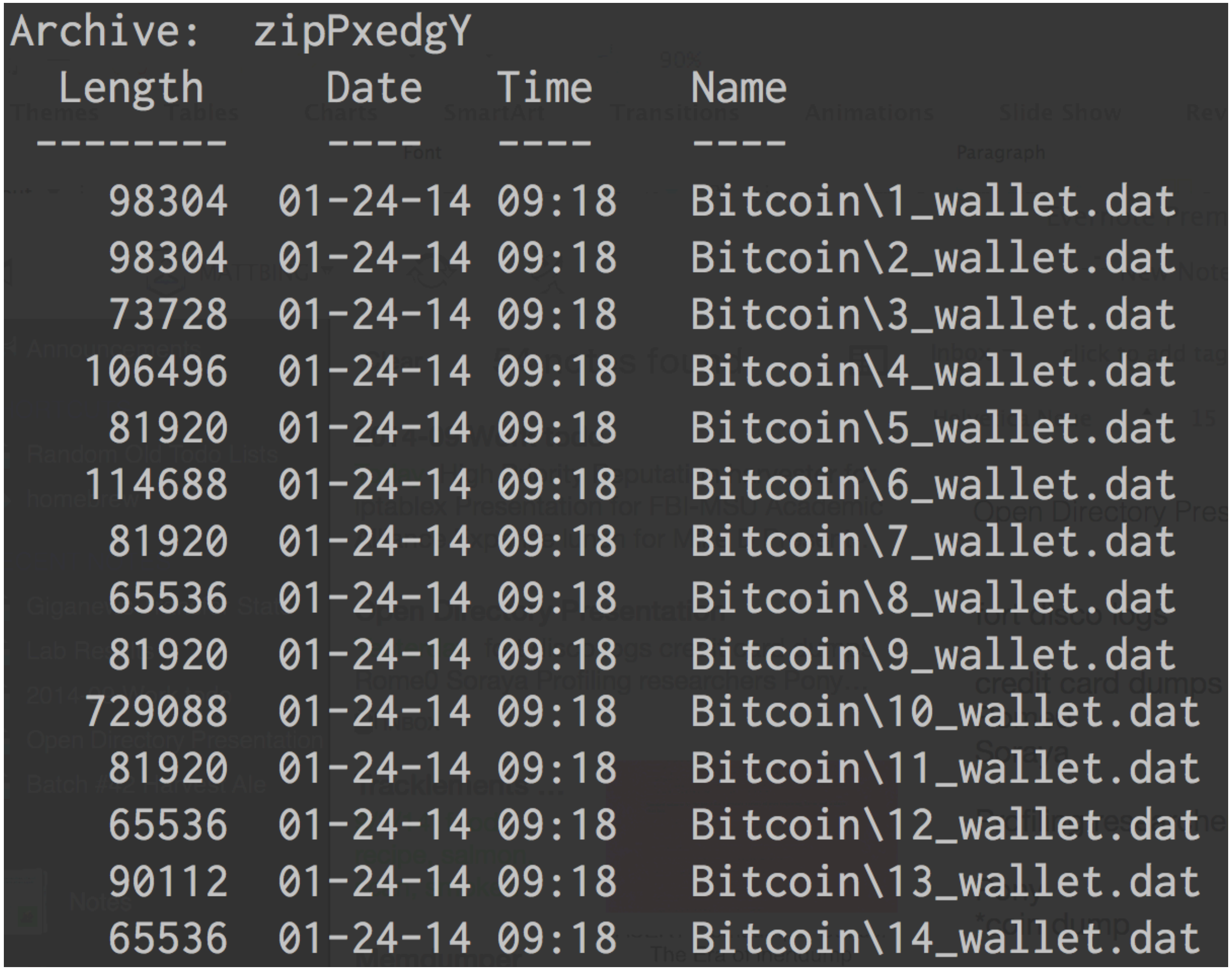


Name	Size	Date Modified
[parent directory]		
includes/		8/25/14 9:53:05 AM
Panel/		8/25/14 9:42:04 AM
temp/		8/25/14 9:53:16 AM
404.html	348 B	5/17/11 9:51:36 PM
admin.php	1.4 kB	8/25/14 9:42:05 AM
config.php	0 B	8/25/14 9:42:06 AM
gate.php	0 B	8/25/14 9:42:07 AM
index.html	666 B	8/25/14 9:41:55 AM
robots.txt	28 B	5/24/11 7:03:34 AM
setup.php	447 B	8/25/14 9:42:26 AM



Name	Size	Date Modified
[parent directory]		
zipPxedgY	2.6 MB	2/28/14 9:24:22 AM

WALLET.DAT

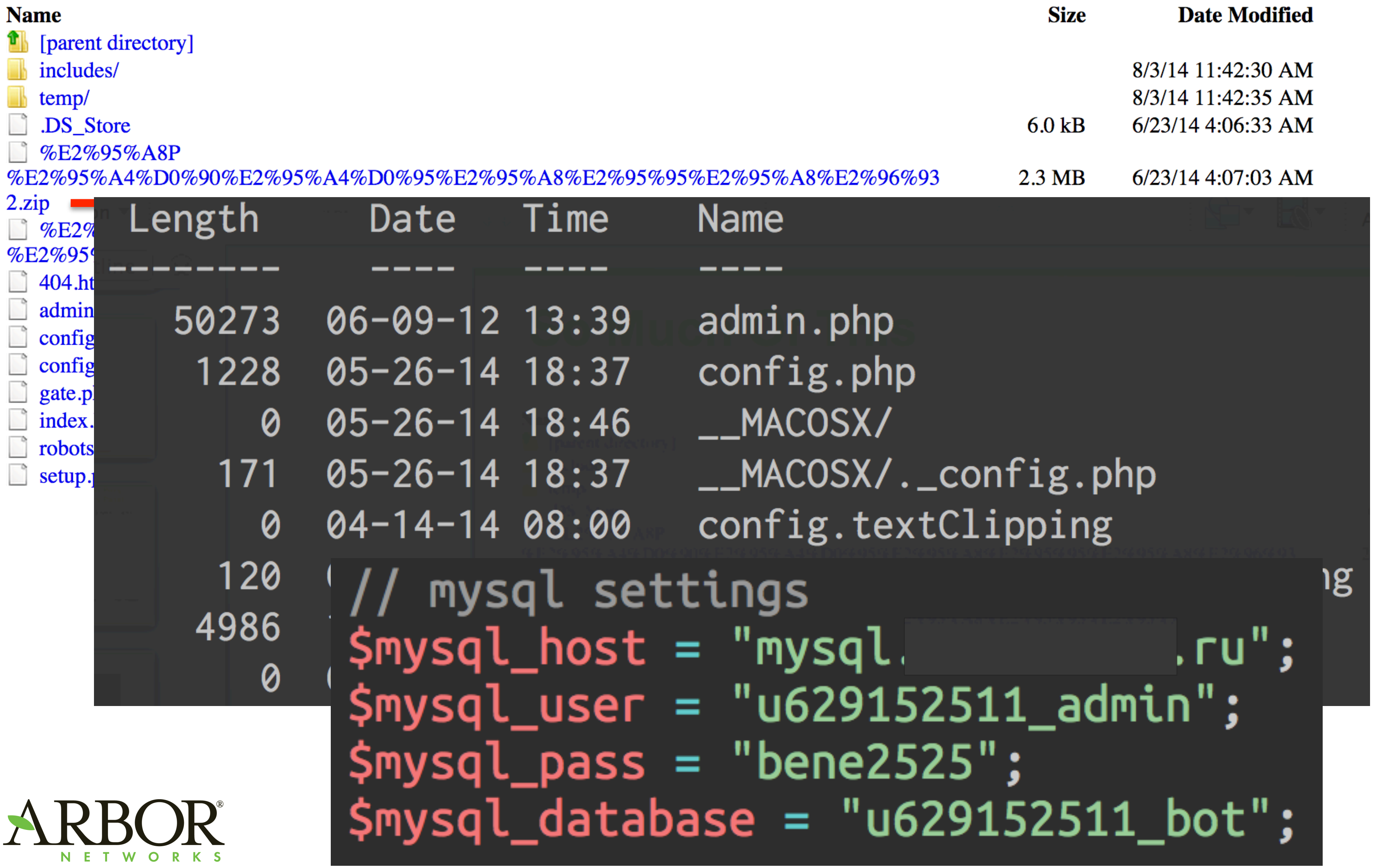


```
Archive:  zipPxedgY
  Length      Date    Time     Name
 ---------   ----    ----     ----
     98304  01-24-14 09:18   Bitcoin\1_wallet.dat
     98304  01-24-14 09:18   Bitcoin\2_wallet.dat
     73728  01-24-14 09:18   Bitcoin\3_wallet.dat
    106496  01-24-14 09:18   Bitcoin\4_wallet.dat
     81920  01-24-14 09:18   Bitcoin\5_wallet.dat
    114688  01-24-14 09:18   Bitcoin\6_wallet.dat
     81920  01-24-14 09:18   Bitcoin\7_wallet.dat
     65536  01-24-14 09:18   Bitcoin\8_wallet.dat
     81920  01-24-14 09:18   Bitcoin\9_wallet.dat
    729088  01-24-14 09:18   Bitcoin\10_wallet.dat
     81920  01-24-14 09:18   Bitcoin\11_wallet.dat
     65536  01-24-14 09:18   Bitcoin\12_wallet.dat
     90112  01-24-14 09:18   Bitcoin\13_wallet.dat
     65536  01-24-14 09:18   Bitcoin\14_wallet.dat
```

Passwords And Source Code

- Password goes into source code
- Source code goes into open directory
- Passwords in the source code
- Our source code

So Much Of This

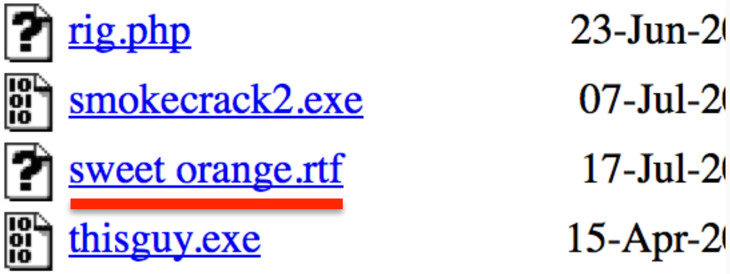


Name	Size	Date Modified
[parent directory]		
includes/		8/3/14 11:42:30 AM
temp/		8/3/14 11:42:35 AM
.DS_Store	6.0 kB	6/23/14 4:06:33 AM
%E2%95%A8P %E2%95%A4%D0%90%E2%95%A4%D0%95%E2%95%A8%E2%95%95%E2%95%A8%E2%96%93 2.zip	2.3 MB	6/23/14 4:07:03 AM
%E2% %E2%95		
404.ht		
admin		
config		
config		
gate.p		
index.		
robots		
setup.		

```
   Length     Date    Time     Name
 ---------    ----    ----     ----
     50273  06-09-12 13:39    admin.php
      1228  05-26-14 18:37    config.php
         0  05-26-14 18:46    __MACOSX/
       171  05-26-14 18:37    __MACOSX/._config.php
         0  04-14-14 08:00    config.textClipping
       120                                         ng
      4986
         0
```

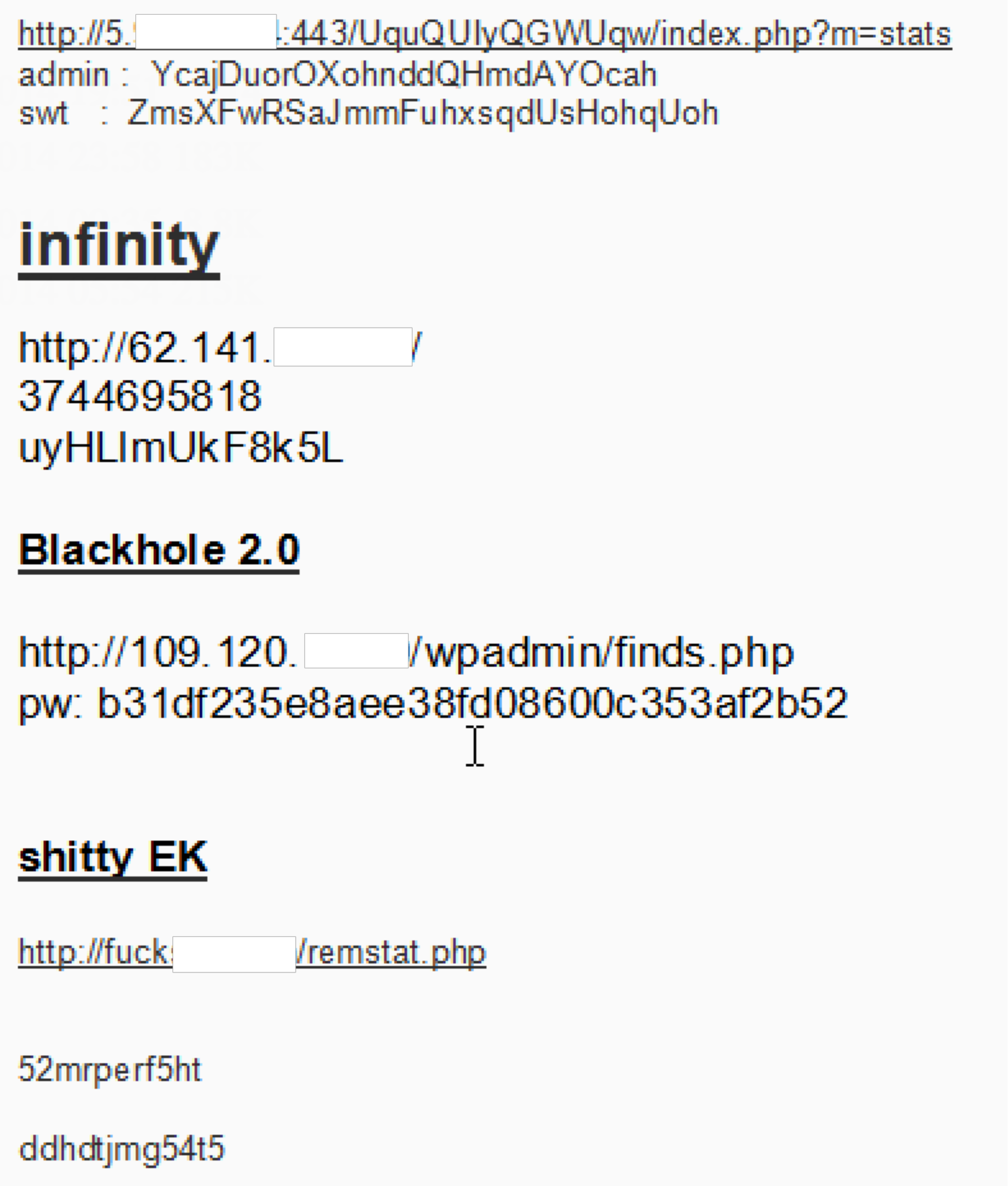
```
// mysql settings
$mysql_host = "mysql.[redacted].ru";
$mysql_user = "u629152511_admin";
$mysql_pass = "bene2525";
$mysql_database = "u629152511_bot";
```

So It Goes



rig.php 23-Jun-2
smokecrack2.exe 07-Jul-2
sweet orange.rtf 17-Jul-2
thisguy.exe 15-Apr-2

This is *four pages* long



http://5.[redacted]:443/UquQUlyQGWUqw/index.php?m=stats
admin : YcajDuorOXohnddQHmdAYOcah
swt : ZmsXFwRSaJmmFuhxsqdUsHohqUoh

infinity

http://62.141.[redacted]/
3744695818
uyHLImUkF8k5L

Blackhole 2.0

http://109.120.[redacted]/wpadmin/finds.php
pw: b31df235e8aee38fd08600c353af2b52

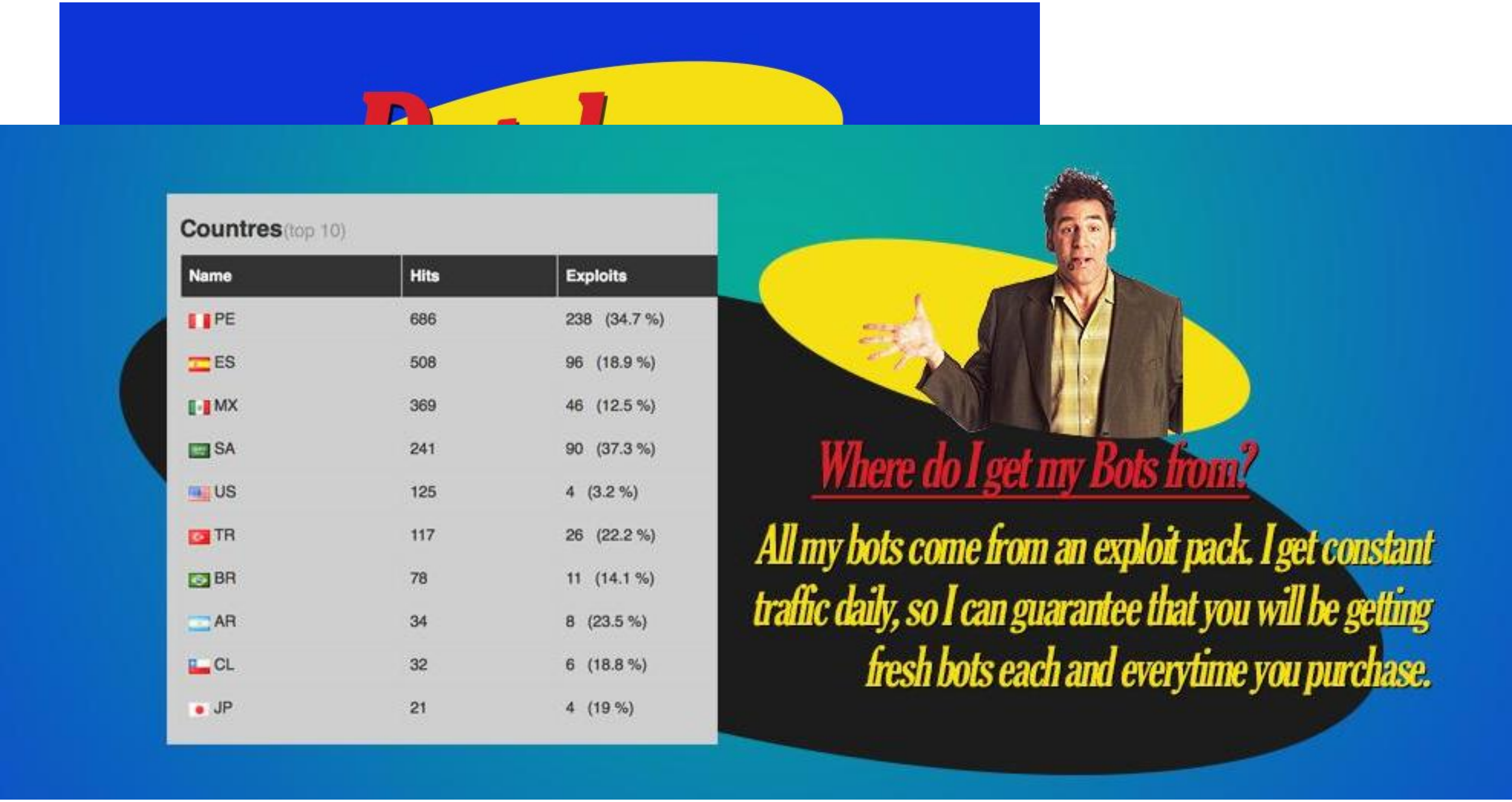
shitty EK

http://fuck[redacted]/remstat.php

52mrperf5ht

ddhdtjmg54t5

Malware About Nothing



Countres(top 10)

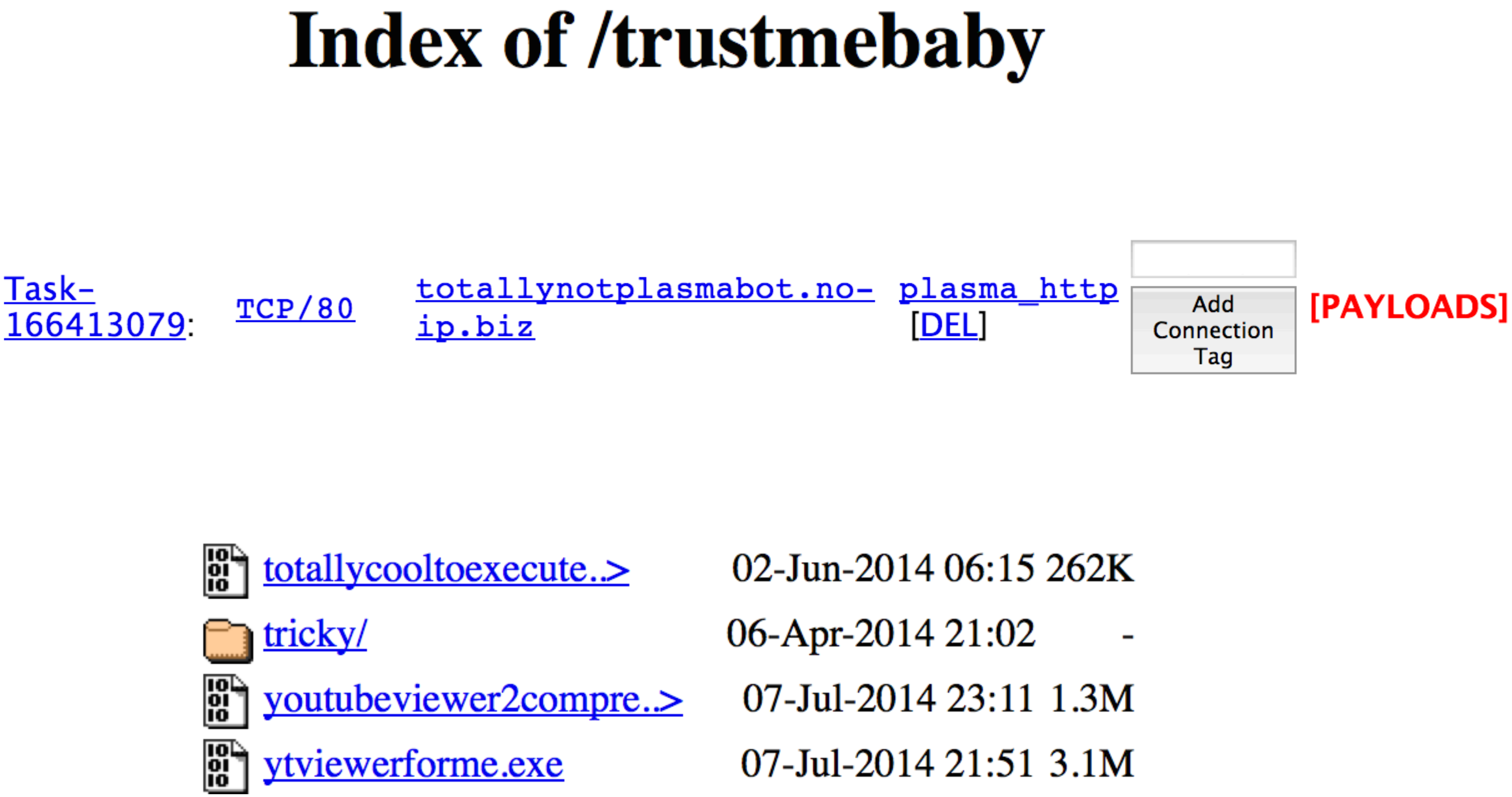
Name	Hits	Exploits
PE	686	238 (34.7 %)
ES	508	96 (18.9 %)
MX	369	46 (12.5 %)
SA	241	90 (37.3 %)
US	125	4 (3.2 %)
TR	117	26 (22.2 %)
BR	78	11 (14.1 %)
AR	34	8 (23.5 %)
CL	32	6 (18.8 %)
JP	21	4 (19 %)

Where do I get my Bots from?

All my bots come from an exploit pack. I get constant traffic daily, so I can guarantee that you will be getting fresh bots each and everytime you purchase.

ARBOR® NETWORKS

They Haven’t Forgotten OPSEC



Index of /trustmebaby

Task-166413079: TCP/80 totallynotplasmabot.no-ip.biz plasma_http [DEL] [PAYLOADS]

```
totallycooltoexecute..>    02-Jun-2014 06:15 262K
tricky/                    06-Apr-2014 21:02    -
youtubeviewer2compre..>    07-Jul-2014 23:11 1.3M
ytviewerforme.exe          07-Jul-2014 21:51 3.1M
```

Themes

- Any malicious URL list can be mined
  - 2% of a lot is still a lot
- The best data comes from manual review
  - Much can be automated, think ‘wget –r’
- Infection logs take the sinkholing out of sinkholing
- There is always something interesting
- If not, there’s something entertaining

ARBOR®
NETWORKS

Questions?