redir.ballysbs.com malvertising (fake 888poker.fr)

Une autre malvertising via une applet SWF sur redir.ballysbs.com

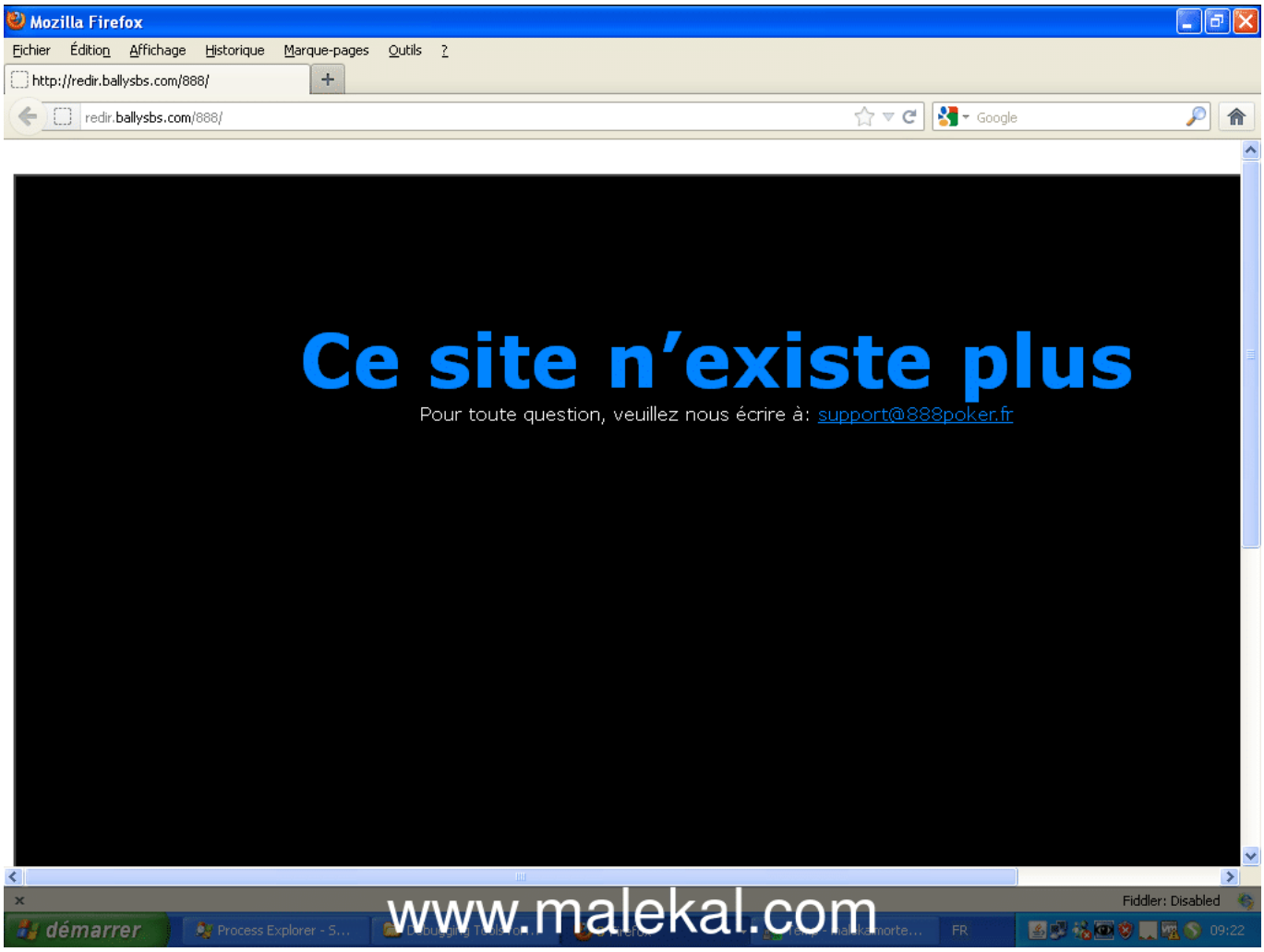
Domain Name: BALLYSBS.COM
Registrar: ENOM, INC.
Whois Server: whois.enom.com
Referral URL: http://www.enom.com
Name Server: NS1.AFRAID.ORG
Name Server: NS1.FREEDNS.WS
Name Server: NS2.AFRAID.ORG
Name Server: NS2.FREEDNS.WS
Status: clientTransferProhibited
Updated Date: 11-dec-2012
Creation Date: 08-dec-2012
Expiration Date: 08-dec-2013

Registrant Contact:
Private
John Young ()

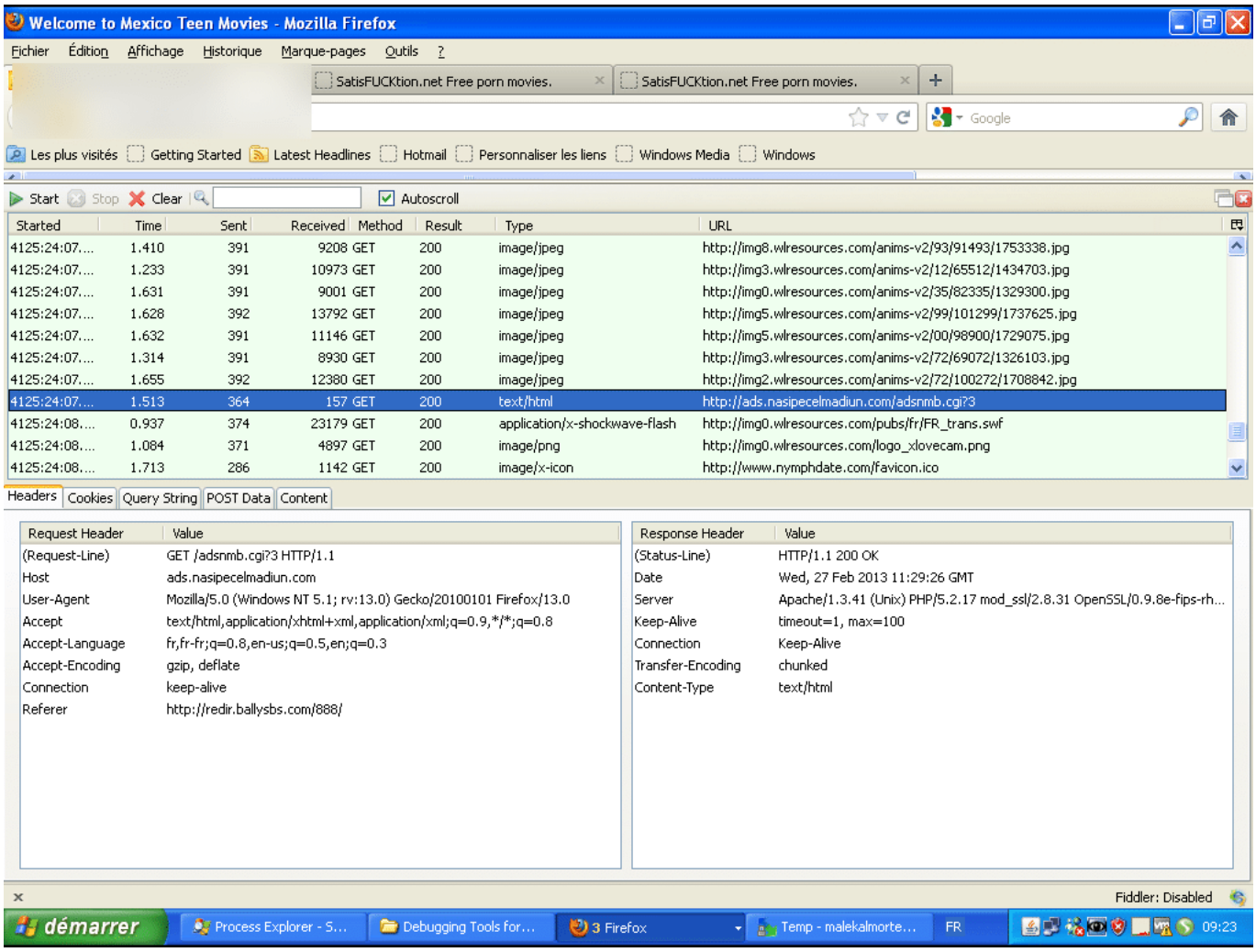
Fax:
jl.kuningan no 33
JakSel, Jakarta 12785
ID

Administrative Contact:
Private
John Young (swtoto888@gmail.com)
+62.085319062831
Fax:
jl.kuningan no 33
JakSel, Jakarta 12785

ID



L'infection utilise un TDS http://ads.nasipecelmadiun.com/adsnmb.cgi?3 (188.72.202.169 NETDIRECT-NET).
Ce dernier redirige vers l'exploit kit : http://tj5jjk.northernpalmbeachcounty.com/lis8DpSfoiE5ITNYeL8xDlcofgK8



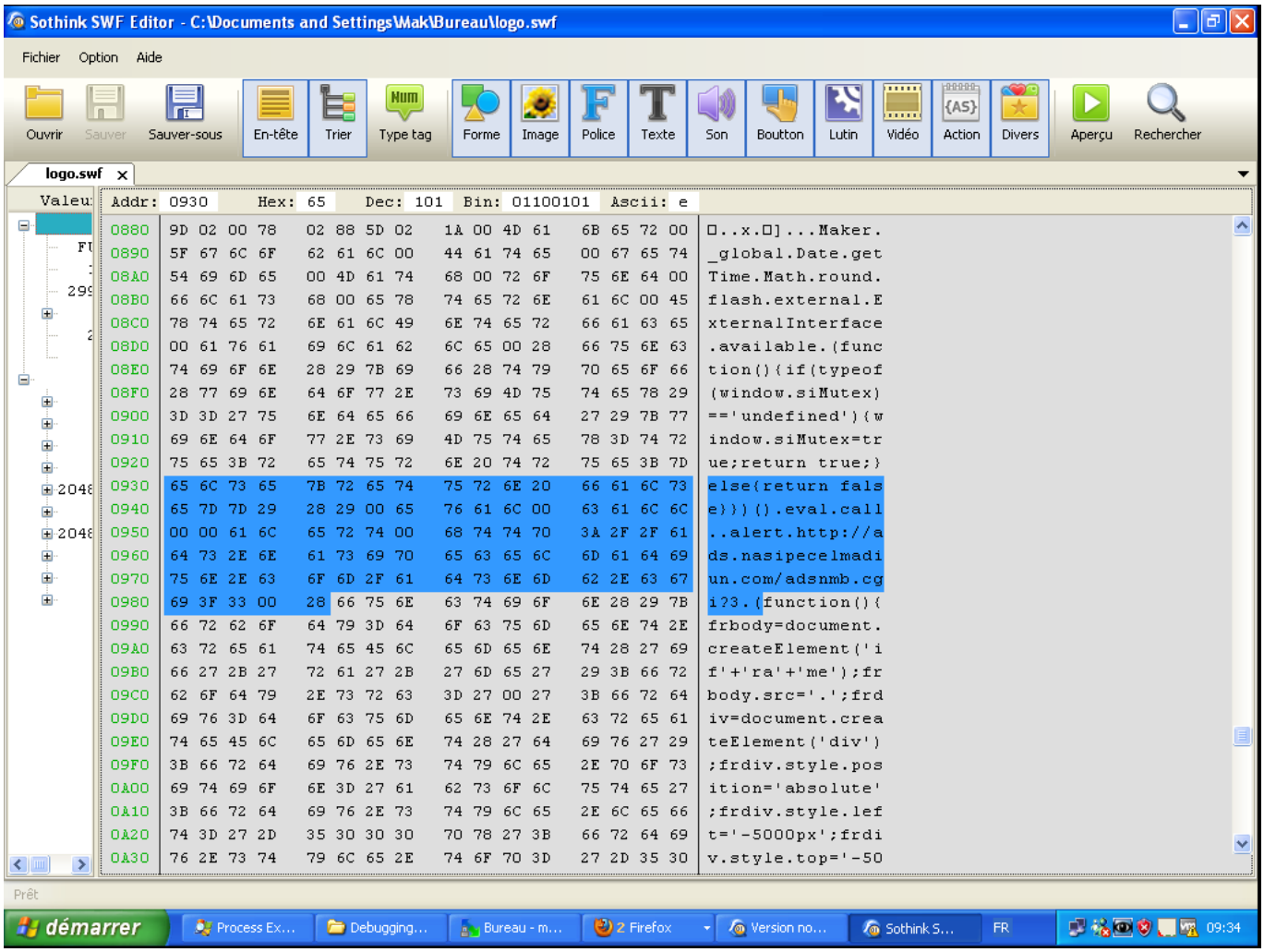
Dans le code source de la page, on voit qu'une page du site de Casino 888.com est référencée (elle n'existe plus) et que la page charge aussi une applet SWF :

Source de : http://redir.ballysbs.com/888/ - Mozilla Firefox

Fichier Édition Affichage ?

```
1  <html>
2  <body>
3  <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" codebase="http://fpdownload.macromedia.com/pub/shockwave/cabs
4  <param name="allowScriptAccess" value="always" />
5  <param name="movie" value="logo.swf" />
6  <param name="quality" value="high" />
7  <param name="bgcolor" value="#ffffff" />
8  <embed src="logo.swf" id="124" quality="high" bgcolor="#ffffff" width="1" height="1" name="Casino" align="middle" allowScr
9  </object>
10 <iframe src="http://www.888.com/casino-hp/?utm_medium=mb&utm_source=3725" width="1158" height="962"></iframe>
11 </body>
12 </html>
```

C’est cette applet qui provoque la redirection en créant une iframe :



La SWF n'est pas détectée : http://malwaredb.malekal.com/index.php?hash=0aeeb8d8d9457e3dd7662f3b308c9bcb

https://www.virustotal.com/fr/file/76e06abca3f8b1ea33e60e4082cb47a31e2a8a5b00e25d593ddbcb94af0ca61f/analysis/1361954392/

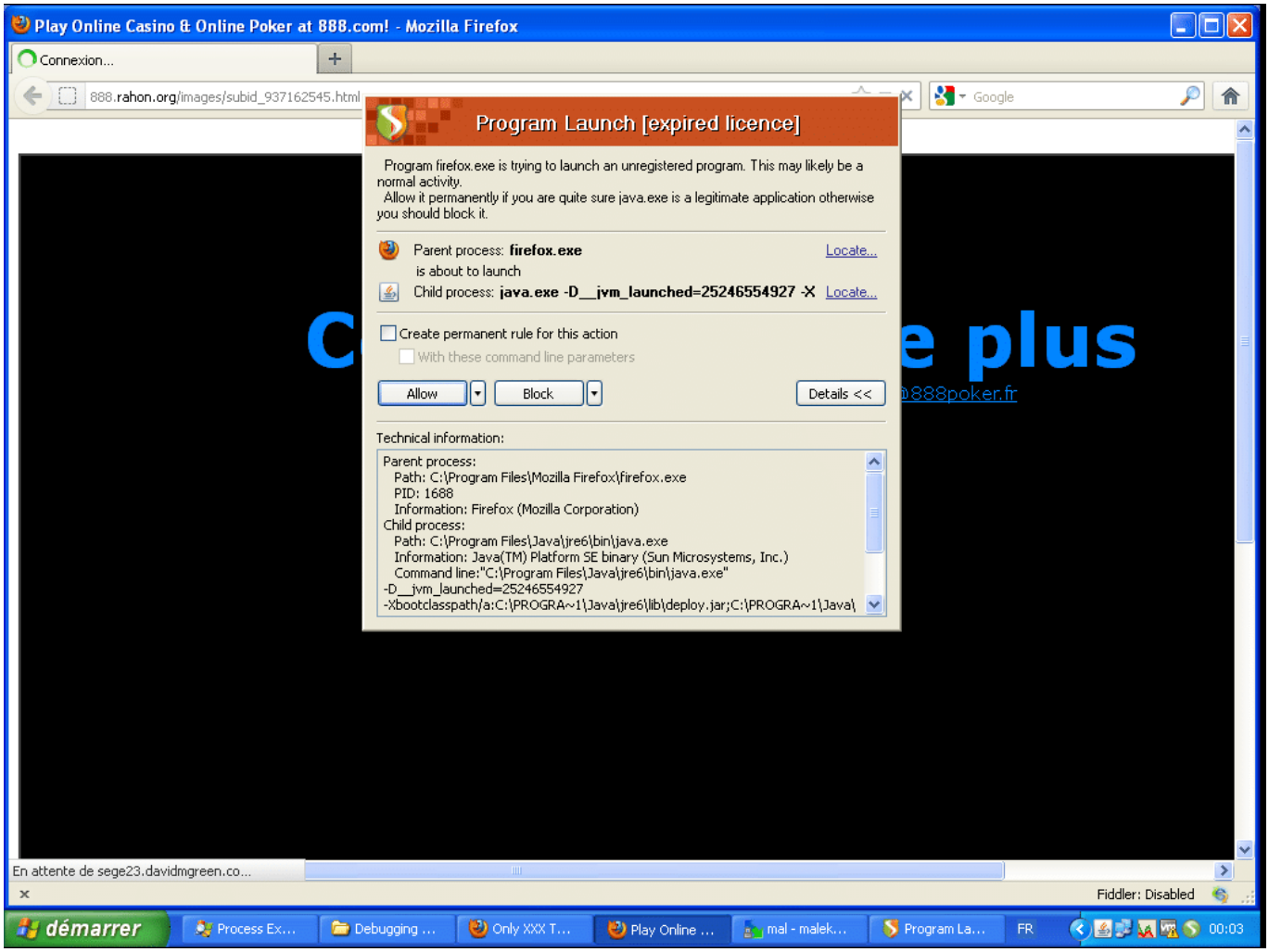
SHA256: 76e06abca3f8b1ea33e60e4082cb47a31e2a8a5b00e25d593ddbcb94af0ca61f
Nom du fichier : logo.swf
Ratio de détection : 0 / 46
Date d'analyse : 2013-02-27 08:39:52 UTC (il y a 0 minute)

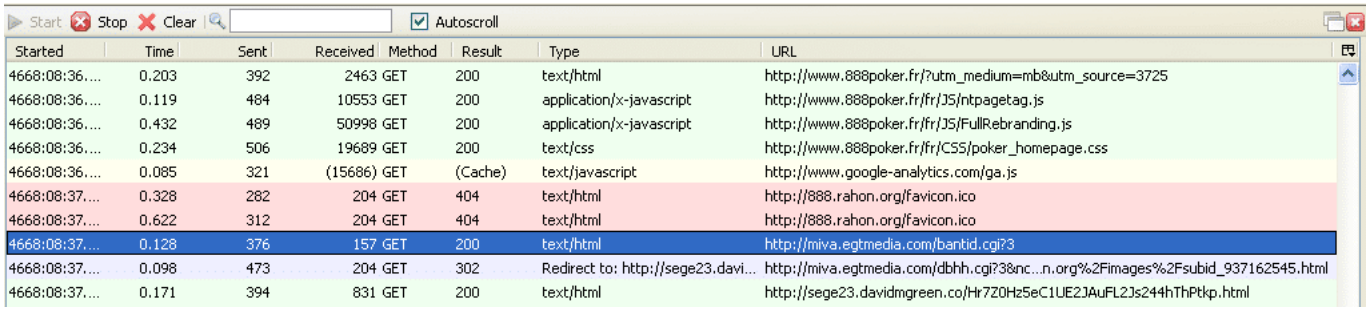
Le dropper : http://malwaredb.malekal.com/index.php?hash=4432cd9516926d344223afcfae795f59

EDIT 22 Mars

De nouveau tombé dessus :

http://miva.egtmedia.com/bantid.cgi?3 (188.72.202.169)
http://888.rahon.org/images/subid_937162545.html (8.29.154.138)





Started	Time	Sent	Received	Method	Result	Type	URL
4668:08:36....	0.203	392	2463	GET	200	text/html	http://www.888poker.fr/?utm_medium=mb&utm_source=3725
4668:08:36....	0.119	484	10553	GET	200	application/x-javascript	http://www.888poker.fr/fr/JS/ntpagetag.js
4668:08:36....	0.432	489	50998	GET	200	application/x-javascript	http://www.888poker.fr/fr/JS/FullRebranding.js
4668:08:36....	0.234	506	19689	GET	200	text/css	http://www.888poker.fr/fr/CSS/poker_homepage.css
4668:08:36....	0.085	321	(15686)	GET	(Cache)	text/javascript	http://www.google-analytics.com/ga.js
4668:08:37....	0.328	282	204	GET	404	text/html	http://888.rahon.org/favicon.ico
4668:08:37....	0.622	312	204	GET	404	text/html	http://888.rahon.org/favicon.ico
4668:08:37....	0.128	376	157	GET	200	text/html	http://miva.egtmedia.com/bantid.cgi?3
4668:08:37....	0.098	473	204	GET	302	Redirect to: http://sege23.davi...	http://miva.egtmedia.com/dbhh.cgi?3&nc...n.org%2Fimages%2Fsubid_937162545.html
4668:08:37....	0.171	394	831	GET	200	text/html	http://sege23.davidmgreen.co/Hr7Z0Hz5eC1UE2JAuFL2Js244hThPtkp.html

La détection est plutôt bonne pour un Urausy en liberté : http://malwaredb.malekal.com/index.php?hash=cf23bfe0730ae2312a

5911186d665535

https://www.virustotal.com/fr/file/ae8a272df98b02d31965131250ef2778ead4228e2b31423b2723eff7345c1673/analysis/1363907608/

SHA256:
ae8a272df98b02d31965131250ef2778ead4228e2b31423b2723eff7345c1673
Nom du fichier : Software.exe.__ProductName
Ratio de détection : 8 / 41
Date d’analyse : 2013-03-21 23:13:28 UTC (il y a 0 minute)
AhnLab-V3 Trojan/Win32.Foreign 20130321
CAT-QuickHeal (Suspicious) – DNAScan 20130321
ESET-NOD32 a variant of Win32/Kryptik.AXDB 20130321
Kaspersky UDS:DangerousObject.Multi.Generic 20130321
Malwarebytes Trojan.Winlock 20130321
McAfee-GW-Edition Heuristic.LooksLike.Win32.SuspiciousPE.J!80 20130321
Norman Hlux.VQ 20130321
Panda Suspicious file 20130321