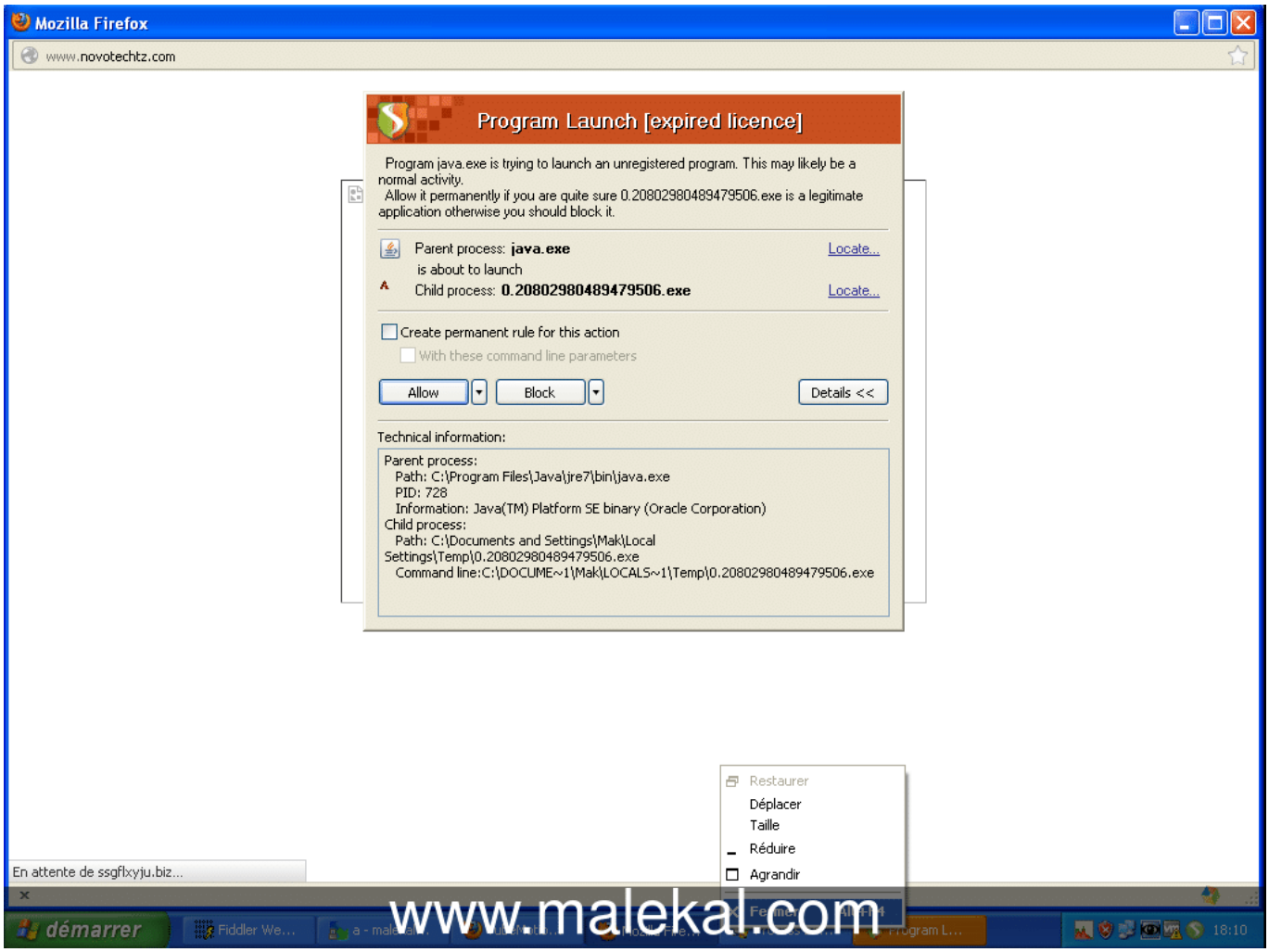
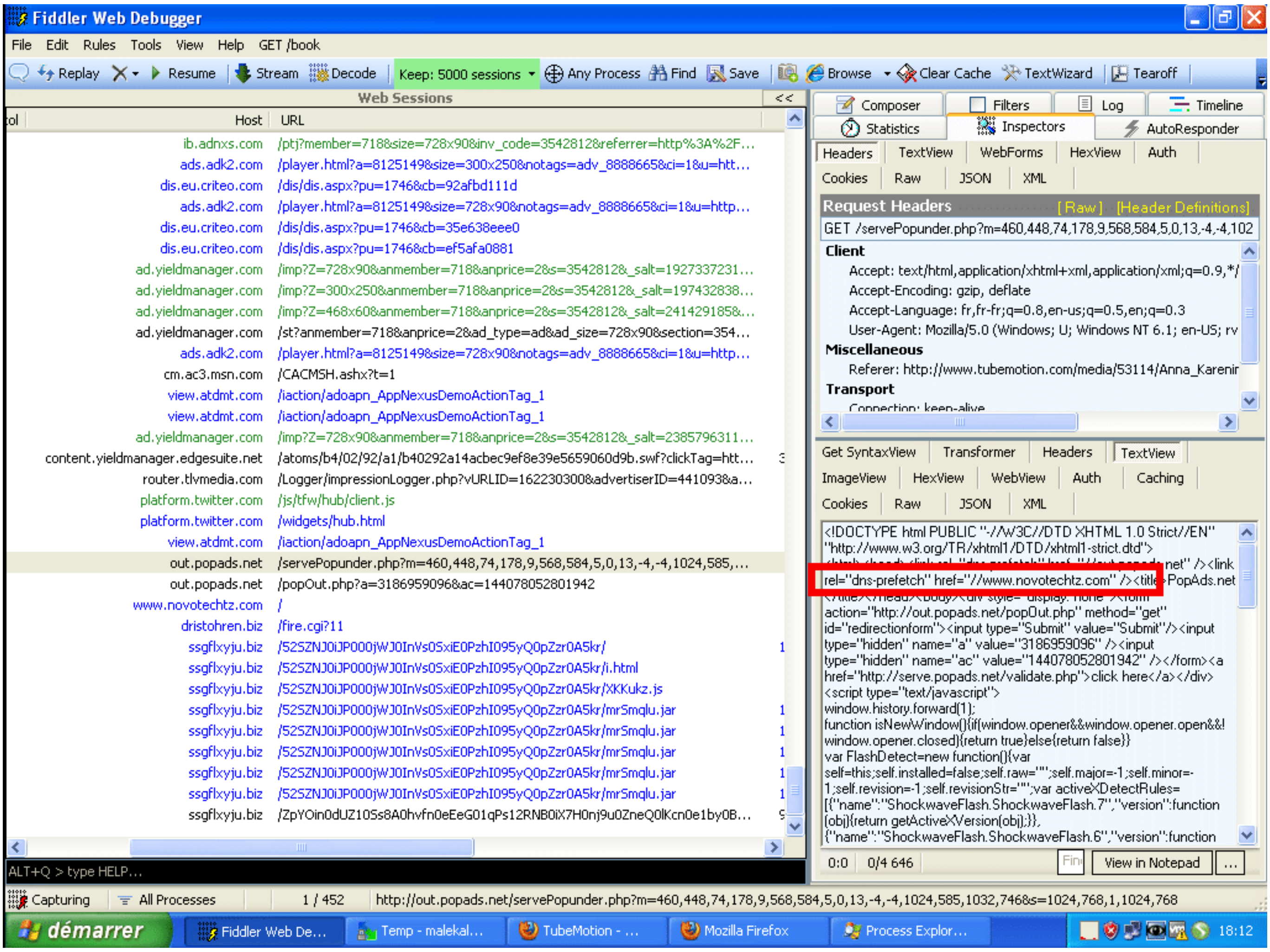
[en] Ramnit via Malvertising

Got a Malvertising from a Warez Website that leads to [Ramnit virus] :

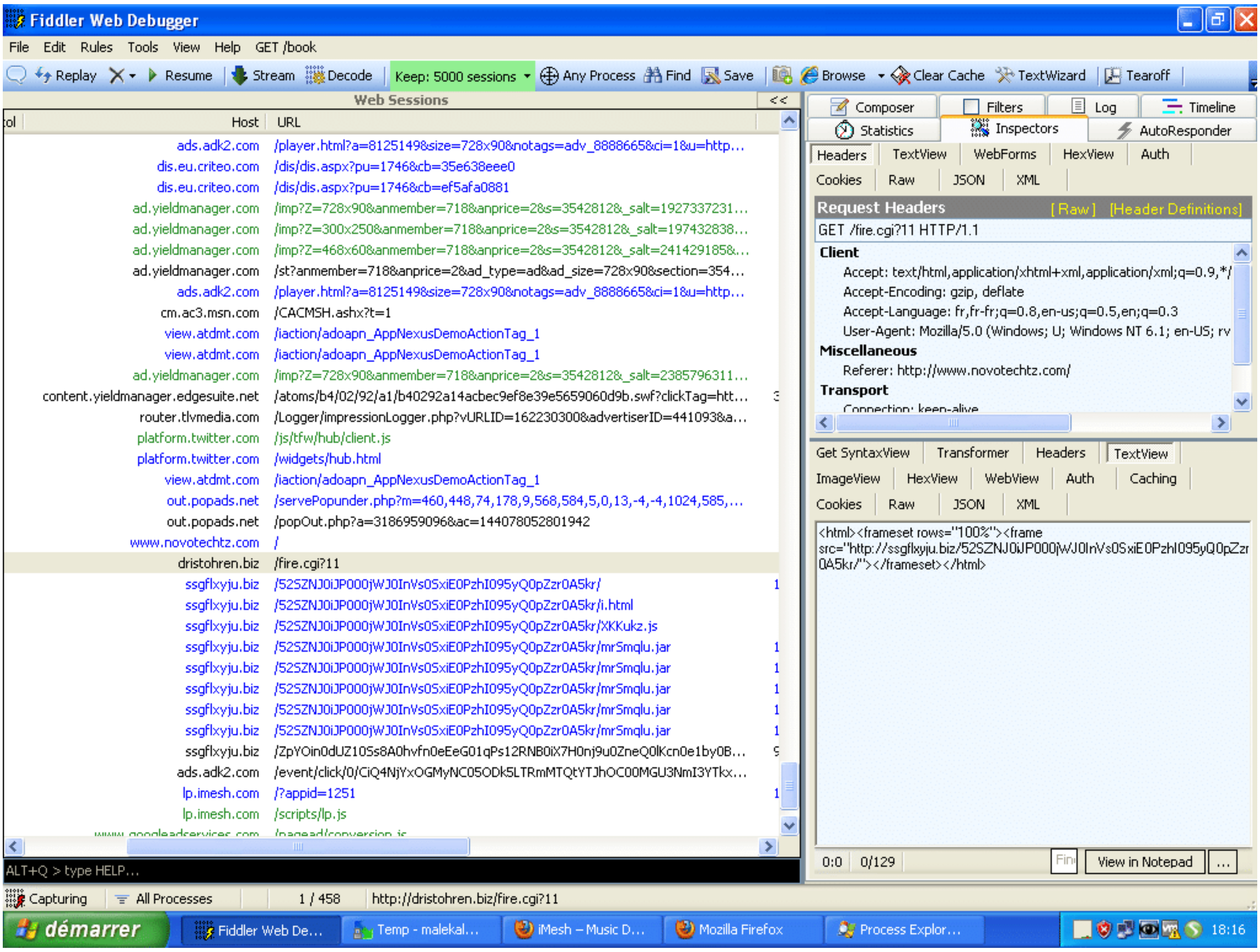


from popads.net



the TDS : http://dristohren.biz (64.120.137.35)

NetRange: 64.120.128.0 – 64.120.255.255
CIDR: 64.120.128.0/17
OriginAS: AS21788
NetName: HOSTNOC-5BLK
NetHandle: NET-64-120-128-0-1
Parent: NET-64-0-0-0-0
NetType: Direct Allocation
RegDate: 2009-04-27
Updated: 2012-03-02
Ref: http://whois.arin.net/rest/net/NET-64-120-128-0-1



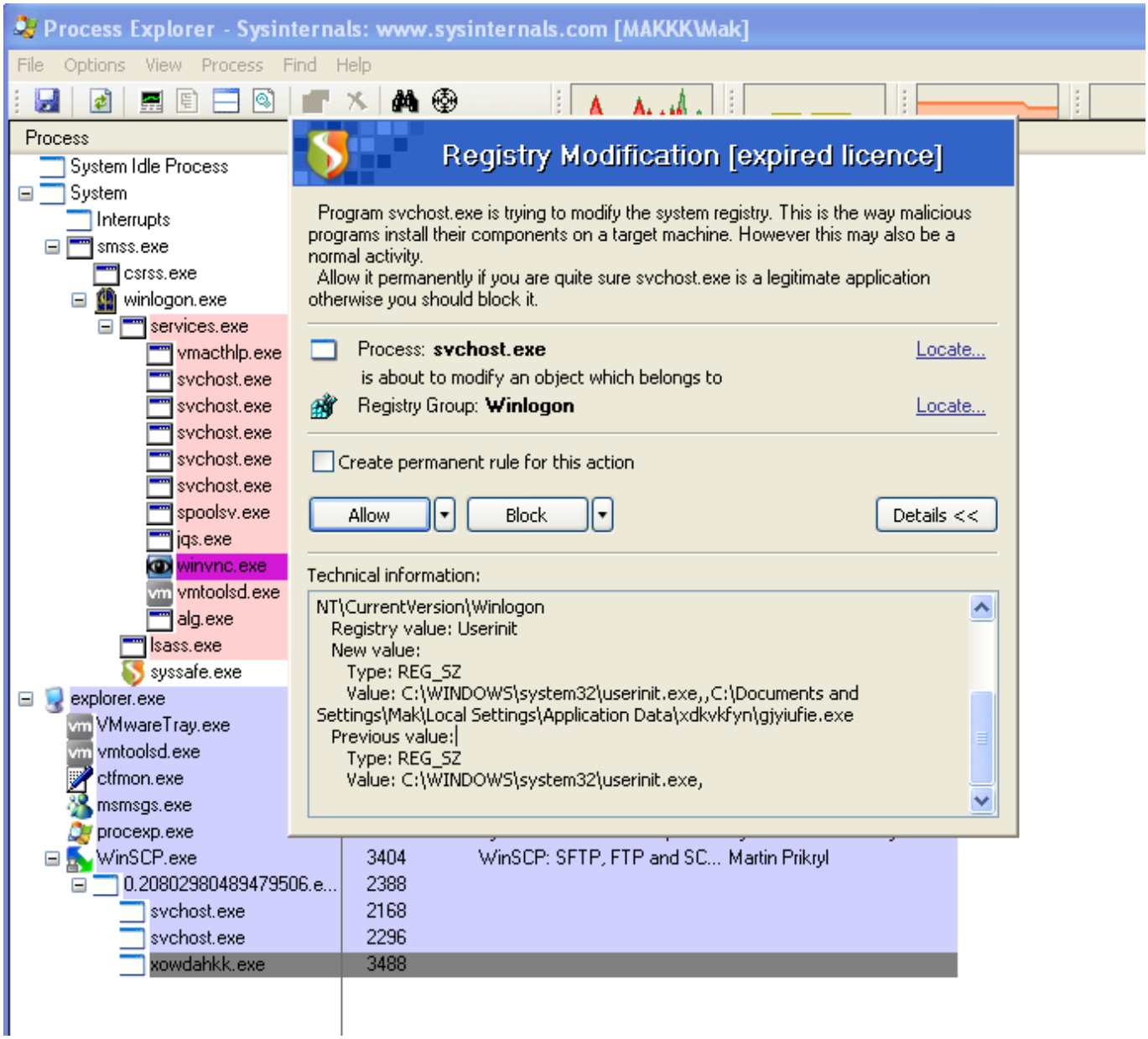
The dropper : http://malwaredb.malekal.com/index.php?hash=8388ea91a2d7fd290a6b0c32f3dd5f7c

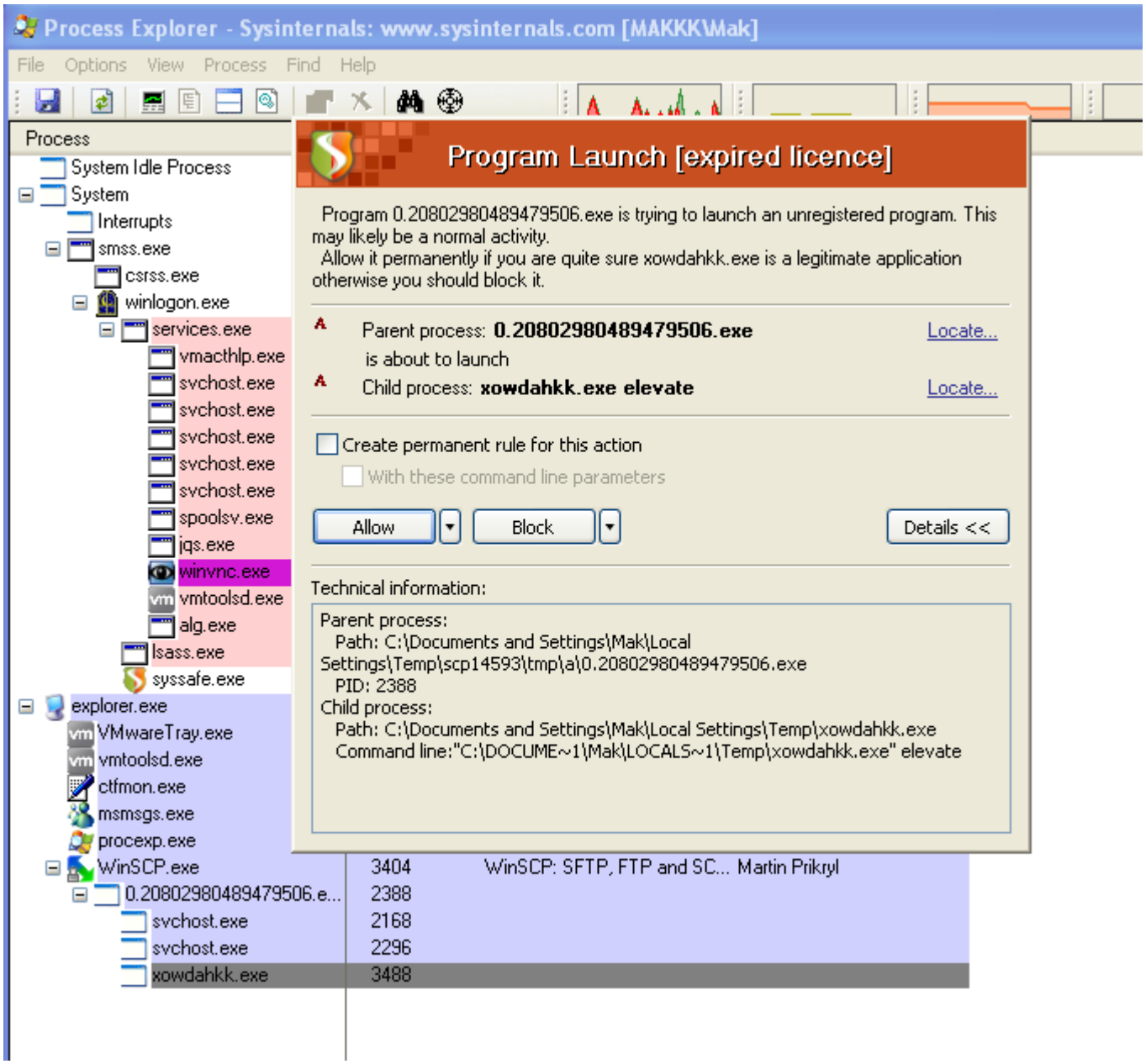
Detections are good : https://www.virustotal.com/fr/file/d64b3eff3613e301acb95dc057d604526aeb396854a73b1eca327262da5d85fb/analysis/1362590163/

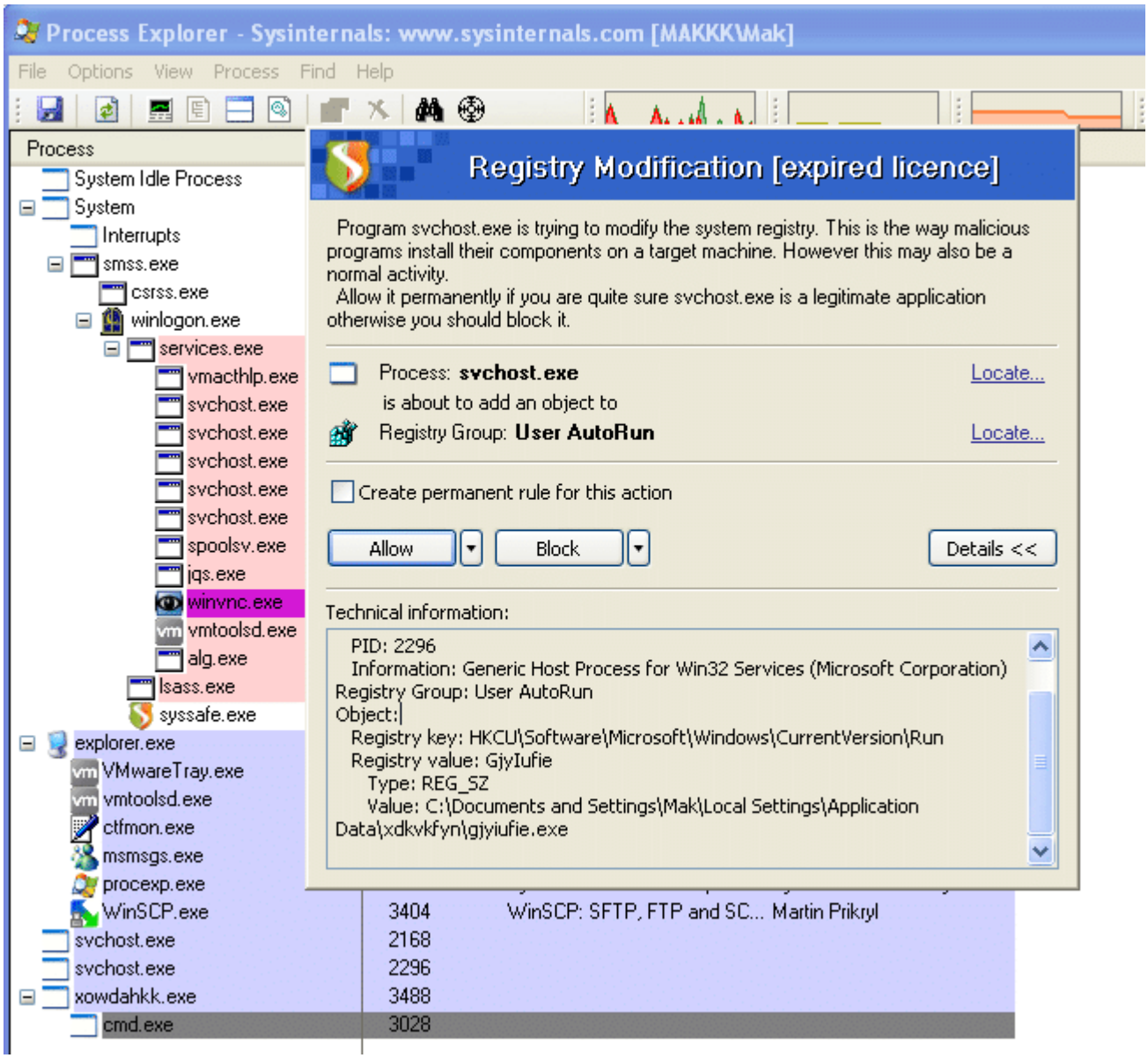
SHA256: d64b3eff3613e301acb95dc057d604526aeb396854a73b1eca327262da5d85fb
Nom du fichier : 0.20802980489479506.exe
Ratio de détection : 11 / 46
Date d'analyse : 2013-03-06 17:16:03 UTC (il y a 10 minutes)

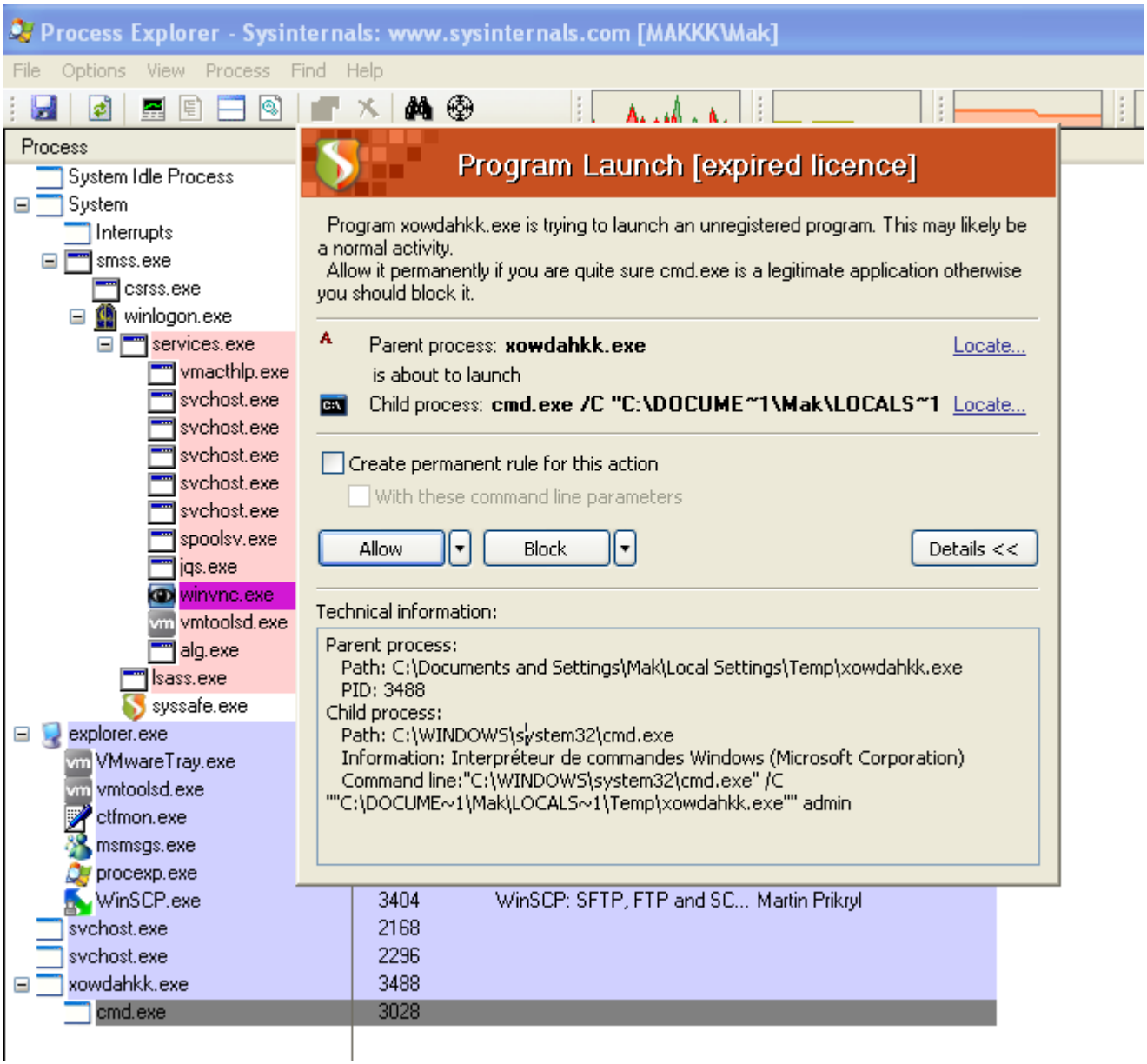
AhnLab-V3 Trojan/Win32.Lebag 20130306
CAT-QuickHeal (Suspicious) – DNAScan 20130306
DrWeb Trojan.Inject1.15519 20130306

Jiangmin Trojan/Lebag.bee 20130304
Kaspersky HEUR:Trojan.Win32.Generic 20130306
Malwarebytes Trojan.Lebag 20130306
McAfee-GW-Edition Heuristic.BehavesLike.Win32.Obfuscated.D 20130306
Panda Trj/Genetic.gen 20130306
TrendMicro PAK_Generic.005 20130306
TrendMicro-HouseCall PAK_Generic.005 20130306



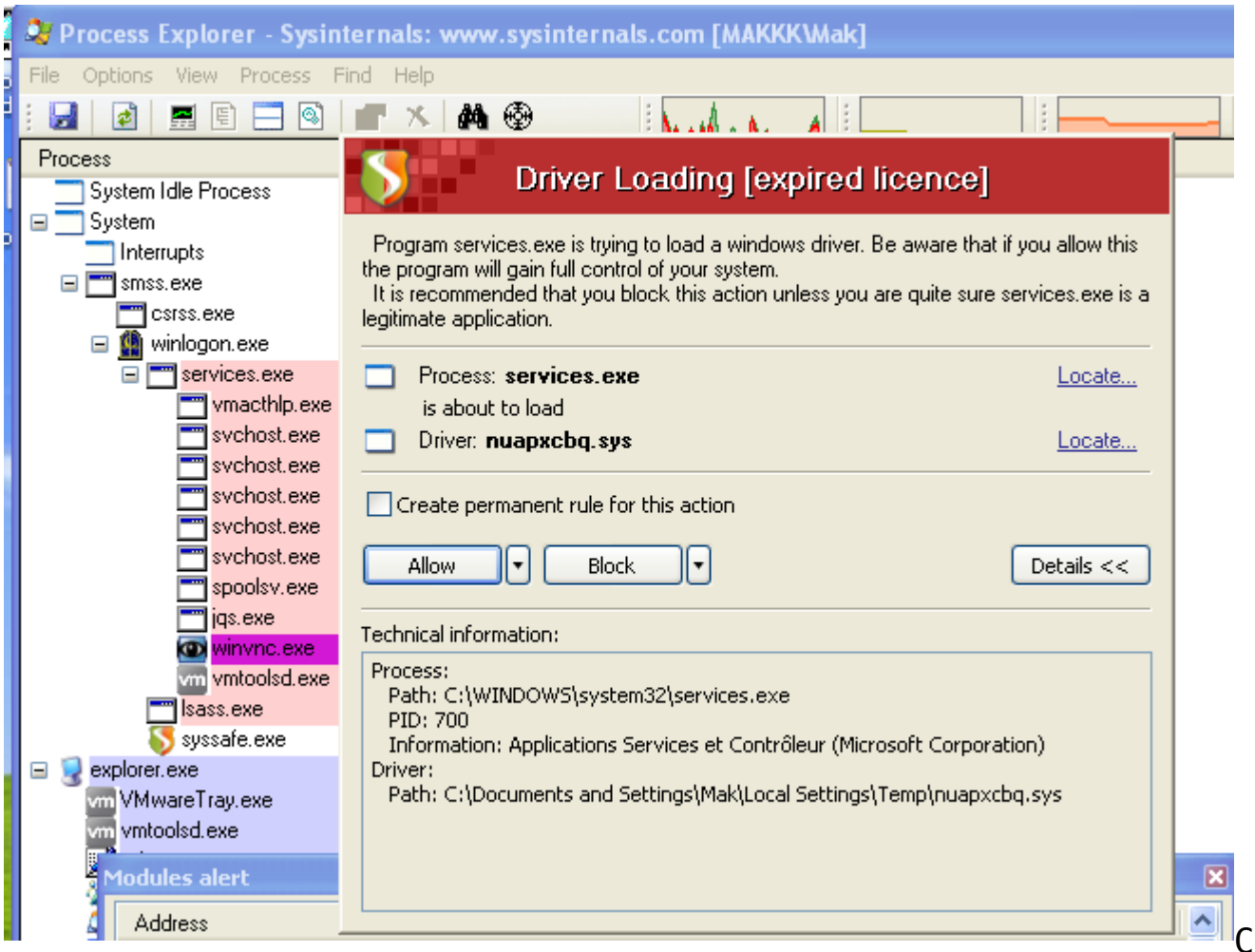

Process Explorer - Sysinternals: www.sysinternals.com [MAKKK\Mak]
File Options View Process Find Help
Process
System Idle Process
System
Interrupts
smss.exe
csrss.exe
winlogon.exe
services.exe
vmacthlp.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
spoolsv.exe
jqs.exe
winvnc.exe
vmtoolsd.exe
alg.exe
lsass.exe
syssafe.exe
explorer.exe
VMwareTray.exe
vmtoolsd.exe
ctfmon.exe
msmsgs.exe
procexp.exe
WinSCP.exe 3404 WinSCP: SFTP, FTP and SC... Martin Prikryl
0.20802980489479506.e... 2388
svchost.exe 2168
svchost.exe 2296
xowdahkk.exe 3488
Program Launch [expired licence]
Program 0.20802980489479506.exe is trying to launch an unregistered program. This may likely be a normal activity.
Allow it permanently if you are quite sure xowdahkk.exe is a legitimate application otherwise you should block it.
Parent process: 0.20802980489479506.exe
Locate...
is about to launch
Child process: xowdahkk.exe elevate
Locate...
Create permanent rule for this action
With these command line parameters
Allow
Block
Details <<
Technical information:
Parent process:
Path: C:\Documents and Settings\Mak\Local Settings\Temp\scp14593\tmp\a\0.20802980489479506.exe
PID: 2388
Child process:
Path: C:\Documents and Settings\Mak\Local Settings\Temp\xowdahkk.exe
Command line:"C:\DOCUME~1\Mak\LOCALS~1\Temp\xowdahkk.exe" elevate


Process Explorer - Sysinternals: www.sysinternals.com [MAKKK\Mak]
File Options View Process Find Help
Process
System Idle Process
System
Interrupts
smss.exe
csrss.exe
winlogon.exe
services.exe
vmacthlp.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
spoolsv.exe
jqs.exe
winvnc.exe
vmtoolsd.exe
alg.exe
lsass.exe
syssafe.exe
explorer.exe
VMwareTray.exe
vmtoolsd.exe
ctfmon.exe
msmsgs.exe
procexp.exe
WinSCP.exe
svchost.exe
svchost.exe
xowdahkk.exe
cmd.exe
3404 WinSCP: SFTP, FTP and SC... Martin Prikryl
2168
2296
3488
3028
Registry Modification [expired licence]
Program svchost.exe is trying to modify the system registry. This is the way malicious programs install their components on a target machine. However this may also be a normal activity.
Allow it permanently if you are quite sure svchost.exe is a legitimate application otherwise you should block it.
Process: svchost.exe
Locate...
is about to add an object to
Registry Group: User AutoRun
Locate...
Create permanent rule for this action
Allow
Block
Details <<
Technical information:
PID: 2296
Information: Generic Host Process for Win32 Services (Microsoft Corporation)
Registry Group: User AutoRun
Object:
Registry key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Registry value: GjyIufie
Type: REG_SZ
Value: C:\Documents and Settings\Mak\Local Settings\Application Data\xdkvkfyn\gjyiufie.exe



The driver : https://www.virustotal.com/fr/file/c1293f8dd8a243391d087742fc22c99b8263f70c6937f784c15e9e20252b38ae/analysis/

SHA256:	c1293f8dd8a243391d087742fc22c99b8263f70c6937f784c15e9e20252b38ae
Nom du fichier :	dnsgvbny.sys
Ratio de détection :	43 / 46
Date d'analyse :	2013-02-22 15:35:49 UTC (il y a 1 semaine, 5 jours)



Con

```
nect to : 188.40.45.67:443

inetnum: 188.40.45.64 – 188.40.45.127
netname: HETZNER-RZ10
descr: Hetzner Online AG
descr: Datacenter 10
country: DE
admin-c: HOAC1-RIPE
tech-c: HOAC1-RIPE
status: ASSIGNED PA
mnt-by: HOS-GUN
mnt-lower: HOS-GUN
mnt-routes: HOS-GUN
source: RIPE # Filtered
```

EDIT April 18 2013

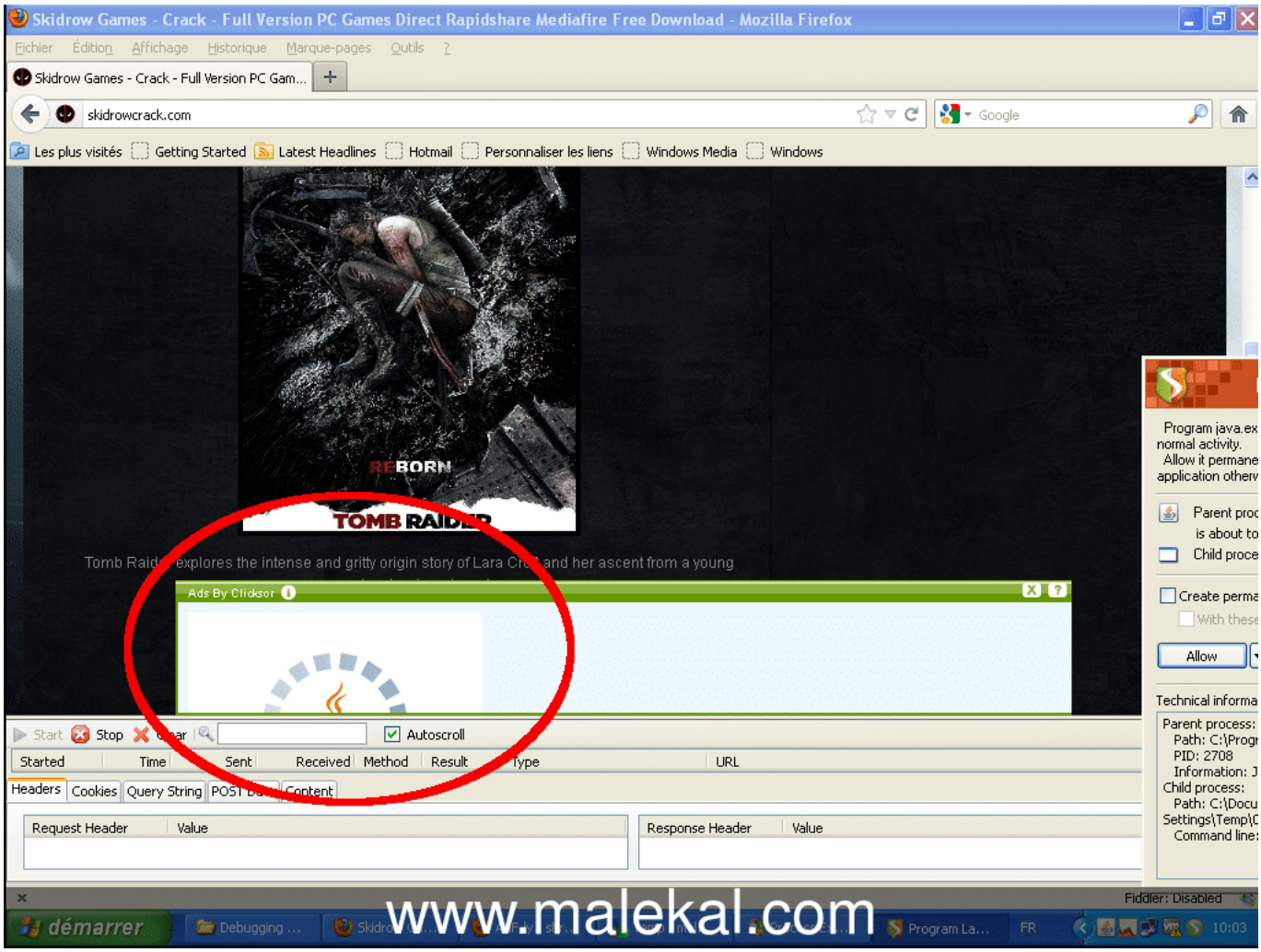
An other one : http://malwaredb.malekal.com/index.php?hash=3324d8f9d58a37d92b0c44a021e2a1f9

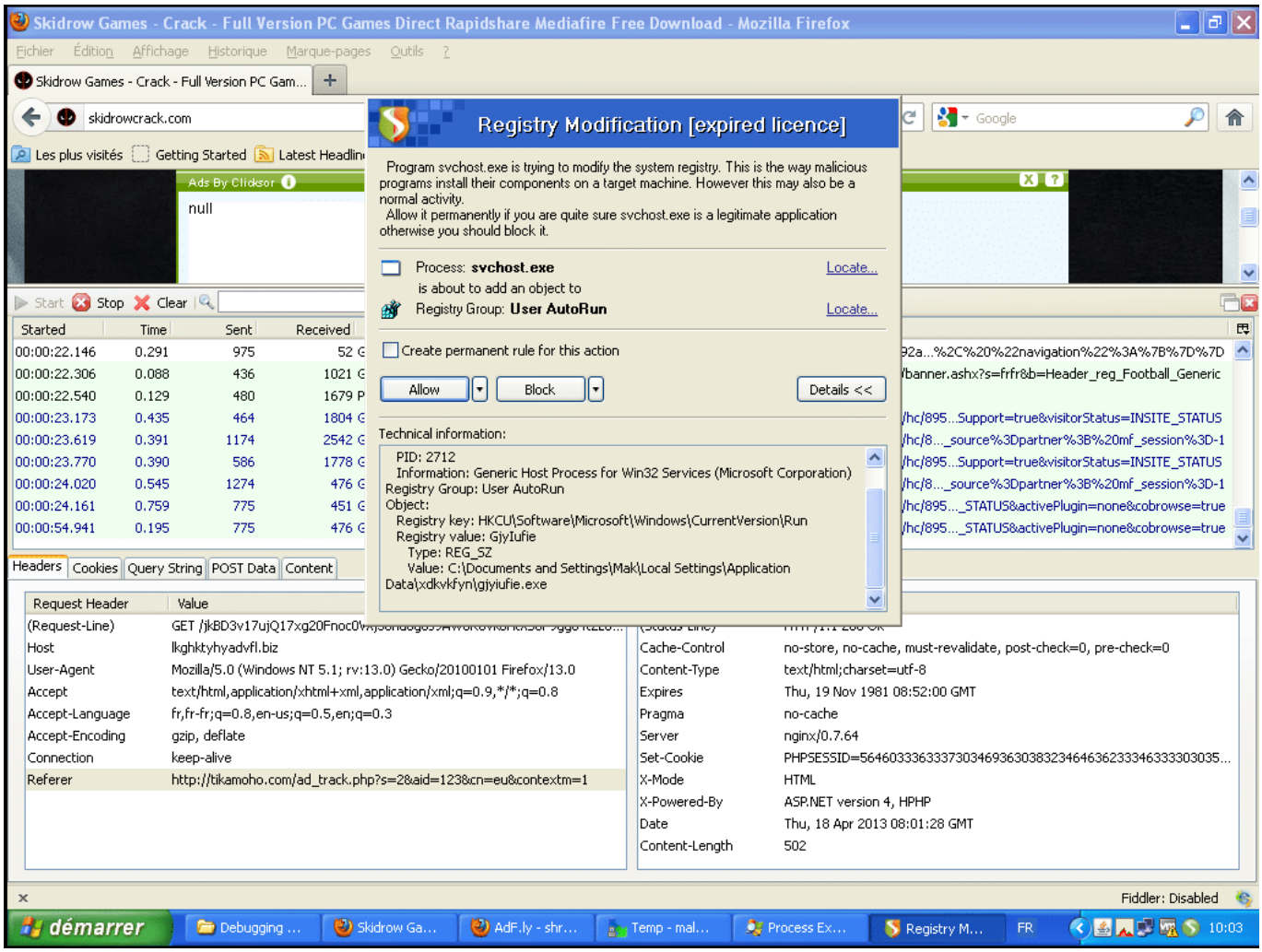
https://www.virustotal.com/fr/file/634ec041368d4e8a10cb1c7cf1e99b4a758bc5a3449635bc07354fb58f2ff20c/analysis/1366272286/

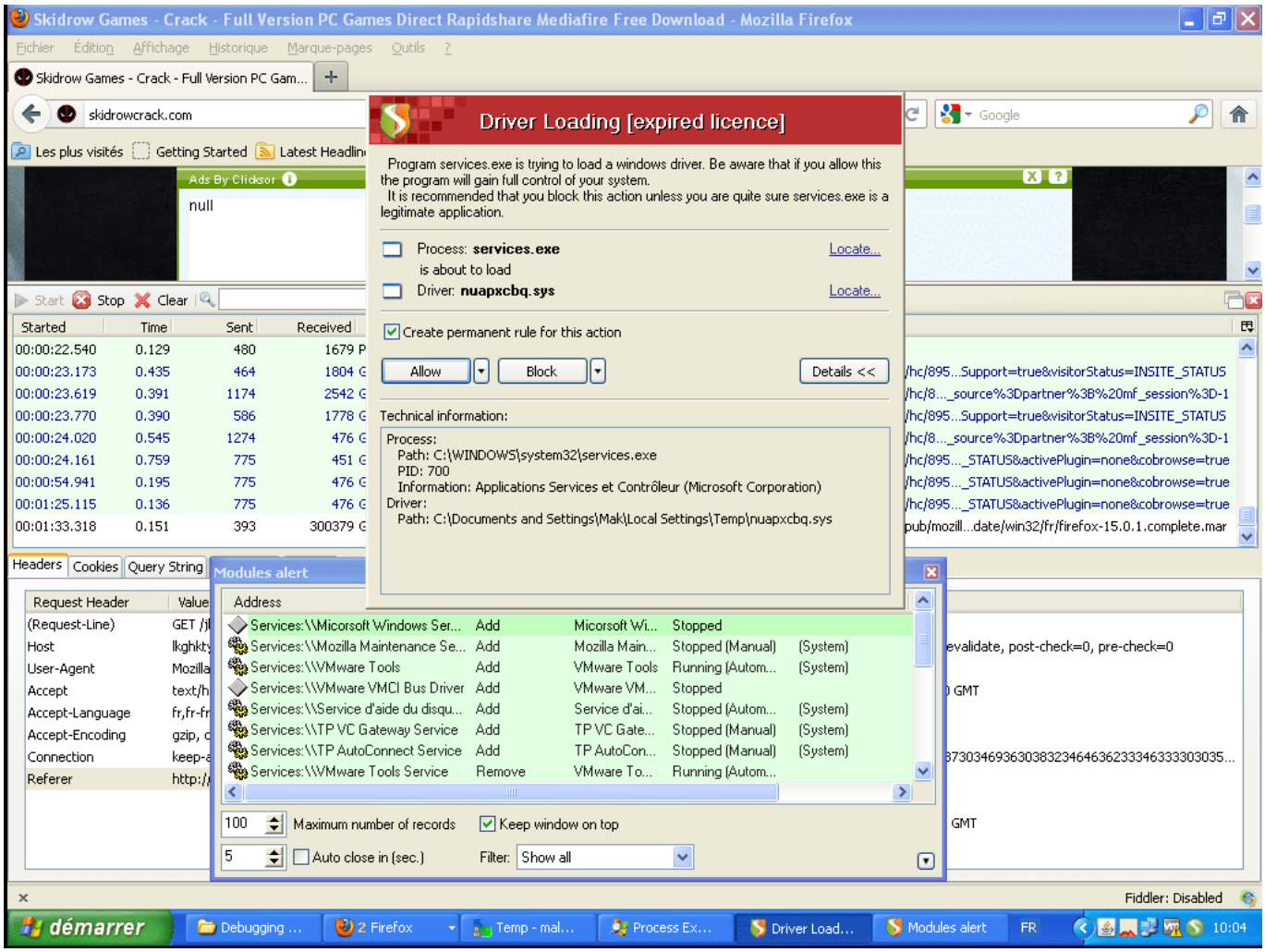
SHA256:
634ec041368d4e8a10cb1c7cf1e99b4a758bc5a3449635bc07354fb58f2ff20c
Nom du fichier : 0.5107251914043918.bfg
Ratio de détection : 12 / 46
Date d'analyse : 2013-04-18 08:04:46 UTC (il y a 0 minute)

BitDefender Gen:Variant.Kazy.165322 20130418
Comodo Heur.Suspicious 20130418
Emsisoft Gen:Variant.Kazy.165322 (B) 20130418
F-Secure Gen:Variant.Kazy.165322 20130418
Fortinet W32/Kryptik.AYLT!tr 20130418
GData Gen:Variant.Kazy.165322 20130418
Kaspersky Trojan.Win32.Lebag.uet 20130418
McAfee-GW-Edition Heuristic.LooksLike.Win32.SuspiciousPE.F 20130418
Microsoft Trojan:Win32/Ramnit.A 20130418
MicroWorld-eScan Gen:Variant.Kazy.165322 20130418
Symantec WS.Reputation.1 20130418

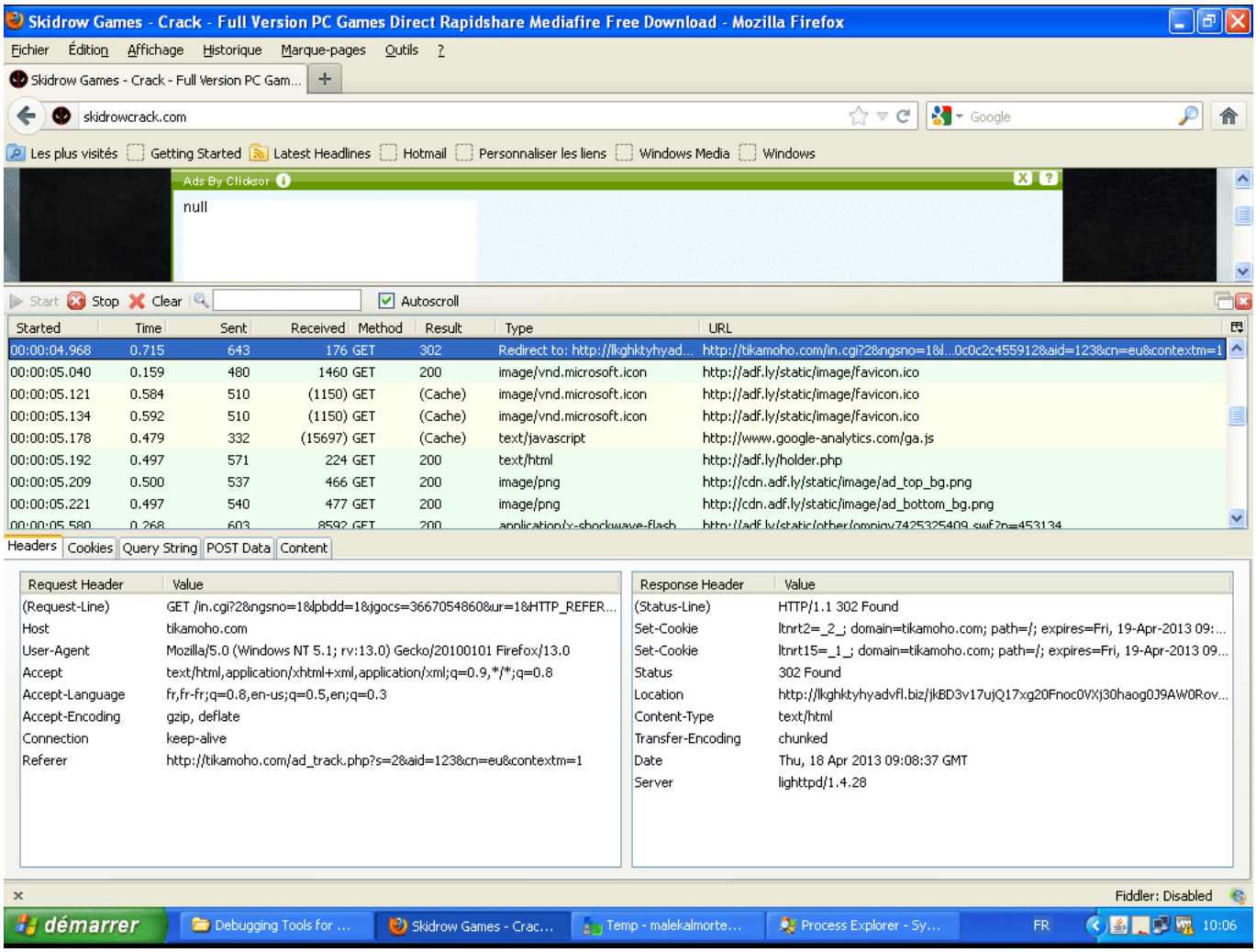
Malvertising from Clicksor :


Skidrow Games - Crack - Full Version PC Games Direct Rapidshare Mediafire Free Download - Mozilla Firefox
skidrowcrack.com
Les plus visités
Getting Started
Latest Headlines
Hotmail
Personnaliser les liens
Windows Media
Windows
REBORN
TOMB RAIDER
Ads By Clicksor
Allow
Start
Stop
Autoscroll
Started
Time
Sent
Received
Method
Result
Type
URL
Headers
Cookies
Query String
Content
Request Header
Value
Response Header
Value
Fiddler: Disabled
démarrer
www.malekal.com


Skidrow Games - Crack - Full Version PC Games Direct Rapidshare Mediafire Free Download - Mozilla Firefox
Registry Modification [expired licence]
Program svchost.exe is trying to modify the system registry. This is the way malicious programs install their components on a target machine. However this may also be a normal activity.
Allow it permanently if you are quite sure svchost.exe is a legitimate application otherwise you should block it.
Process: svchost.exe
is about to add an object to
Registry Group: User AutoRun
Locate...
Locate...
Create permanent rule for this action
Allow
Block
Details <<
Technical information:
PID: 2712
Information: Generic Host Process for Win32 Services (Microsoft Corporation)
Registry Group: User AutoRun
Object:
Registry key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Registry value: GjyIufie
Type: REG_SZ
Value: C:\Documents and Settings\Mak\Local Settings\Application Data\xdkvkfyn\gjyiufie.exe
Request Header
Value
(Request-Line)
GET /jkBD3v17ujQ17xg20Fnoc0
Host
lkghktyhyadvfl.biz
User-Agent
Mozilla/5.0 (Windows NT 5.1; rv:13.0) Gecko/20100101 Firefox/13.0
Accept
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language
fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding
gzip, deflate
Connection
keep-alive
Referer
http://tikamoho.com/ad_track.php?s=2&aid=123&cn=eu&contextm=1
Cache-Control
no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Type
text/html;charset=utf-8
Expires
Thu, 19 Nov 1981 08:52:00 GMT
Pragma
no-cache
Server
nginx/0.7.64
Set-Cookie
PHPSESSID=5646033363337303469363038323464636233346333303035...
X-Mode
HTML
X-Powered-By
ASP.NET version 4, HPHP
Date
Thu, 18 Apr 2013 08:01:28 GMT
Content-Length
502
Fiddler: Disabled
démarrer
Debugging ...
Skidrow Ga...
AdF.ly - shr...
Temp - mal...
Process Ex...
Registry M...
FR
10:03



http://tikamoho.com/ad_track.php?s=2&aid=123&cn=eu&contextm=1 (31.207.2.154 – CEUSERVERS – CZ)
http://tikamoho.com/in.cgi?2&ngsno=1&lpbdd=1&jgocs=3667054860&ur=1&HTTP_REFERER=http%3A%2F%2Fads%2Ehooqy%2Ecom%2FnewServing%2Fbanner%5Fframe%2Ephp%3Fnid%3D1%26pid%3D102042%26sid%3D301172%26zone%3D%2D1%26image%3D3%26adtype%3D1%26key%3De9ecd422a05a733728190c0c2c455912&aid=123&cn=eu&contextm=1
http://lkghktyhyadvfl.biz/jkBD3v17ujQ17xg20Fnoc0VXj30haog0J9AW0Rovk0HtXS0F9gg04t2L0Gjch/ (94.198.96.9 – SEFLOW-DEDICATED-NET – IT)


Skidrow Games - Crack - Full Version PC Games Direct Rapidshare Mediafire Free Download - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
Skidrow Games - Crack - Full Version PC Gam...
skidrowcrack.com
Google
Les plus visités Getting Started Latest Headlines Hotmail Personnaliser les liens Windows Media Windows
Ads By Clicksor
null
Start Stop Clear Autoscroll
Started Time Sent Received Method Result Type URL
00:00:04.968 0.715 643 176 GET 302 Redirect to: http://lkghktyhyad... http://tikamoho.com/in.cgi?2&ngsno=1&l...0c0c2c455912&aid=123&cn=eu&contextm=1
00:00:05.040 0.159 480 1460 GET 200 image/vnd.microsoft.icon http://adf.ly/static/image/favicon.ico
00:00:05.121 0.584 510 (1150) GET (Cache) image/vnd.microsoft.icon http://adf.ly/static/image/favicon.ico
00:00:05.134 0.592 510 (1150) GET (Cache) image/vnd.microsoft.icon http://adf.ly/static/image/favicon.ico
00:00:05.178 0.479 332 (15697) GET (Cache) text/javascript http://www.google-analytics.com/ga.js
00:00:05.192 0.497 571 224 GET 200 text/html http://adf.ly/holder.php
00:00:05.209 0.500 537 466 GET 200 image/png http://cdn.adf.ly/static/image/ad_top_bg.png
00:00:05.221 0.497 540 477 GET 200 image/png http://cdn.adf.ly/static/image/ad_bottom_bg.png
Headers Cookies Query String POST Data Content
Request Header Value
(Request-Line) GET /in.cgi?2&ngsno=1&lpbdd=1&jgocs=3667054860&ur=1&HTTP_REFER...
Host tikamoho.com
User-Agent Mozilla/5.0 (Windows NT 5.1; rv:13.0) Gecko/20100101 Firefox/13.0
Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding gzip, deflate
Connection keep-alive
Referer http://tikamoho.com/ad_track.php?s=2&aid=123&cn=eu&contextm=1
Response Header Value
(Status-Line) HTTP/1.1 302 Found
Set-Cookie ltnrt2=_2_; domain=tikamoho.com; path=/; expires=Fri, 19-Apr-2013 09:...
Set-Cookie ltnrt15=_1_; domain=tikamoho.com; path=/; expires=Fri, 19-Apr-2013 09...
Status 302 Found
Location http://lkghktyhyadvfl.biz/jkBD3v17ujQ17xg20Fnoc0WXj30haog0J9AW0Rov...
Content-Type text/html
Transfer-Encoding chunked
Date Thu, 18 Apr 2013 09:08:37 GMT
Server lighttpd/1.4.28
Fiddler: Disabled
démarrer
Debugging Tools for ...
Skidrow Games - Crac...
Temp - malekalmorte...
Process Explorer - Sy...
FR
10:06