

Backdoor:Win32/Kelihos.A : Possible nouveau Storm/Waledac

Nouvelle version possible du [botnet Storm/Waldeac](#)

Actuellement seul Microsoft a créé une nouvelle famille, les détections peuvent donner ceci :

- *Trojan.ADH [PCTools]*
- *Trojan.ADH.2 [Symantec]*
- *Trojan-Downloader.Win32.FraudLoad.ybnn [Kaspersky Lab]*
- *Backdoor:Win32/Kelihos.A [Microsoft]*

Le malware peut se propager par des emails en proposant par exemple de fausses cartes de voeux, ce qui fut le cas en Janvier 2011, soit donc les mêmes procédés qu'utilisait Storm. Le malware est aussi installé par les infections Trojan.Karagany/Trojan.Oficla qui se propage via [des exploits sur site WEB](#), se reporter à la page : [Trojan.Karagany et Trojan.Oficla: Les malwares en .co.cc sont de retour !](#)

Les URL sont actuellement via des fichiers flash2.exe :

- <http://darlev.com/flash2.exe>
- <http://91.200.240.36/flash2.exe>

Deux liens sur le malware :

<http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20101230>

<http://community.websense.com/blogs/securitylabs/archive/2010/12/31/yesterday-s-new-year-email-theme-post-is-storm-waledac.aspx>

Détection

de

Backdoor:Win32/Kelihos.A

Le malware ajoute une clef Run *SmartIndex* pour se charger – exemple :

[quote]*

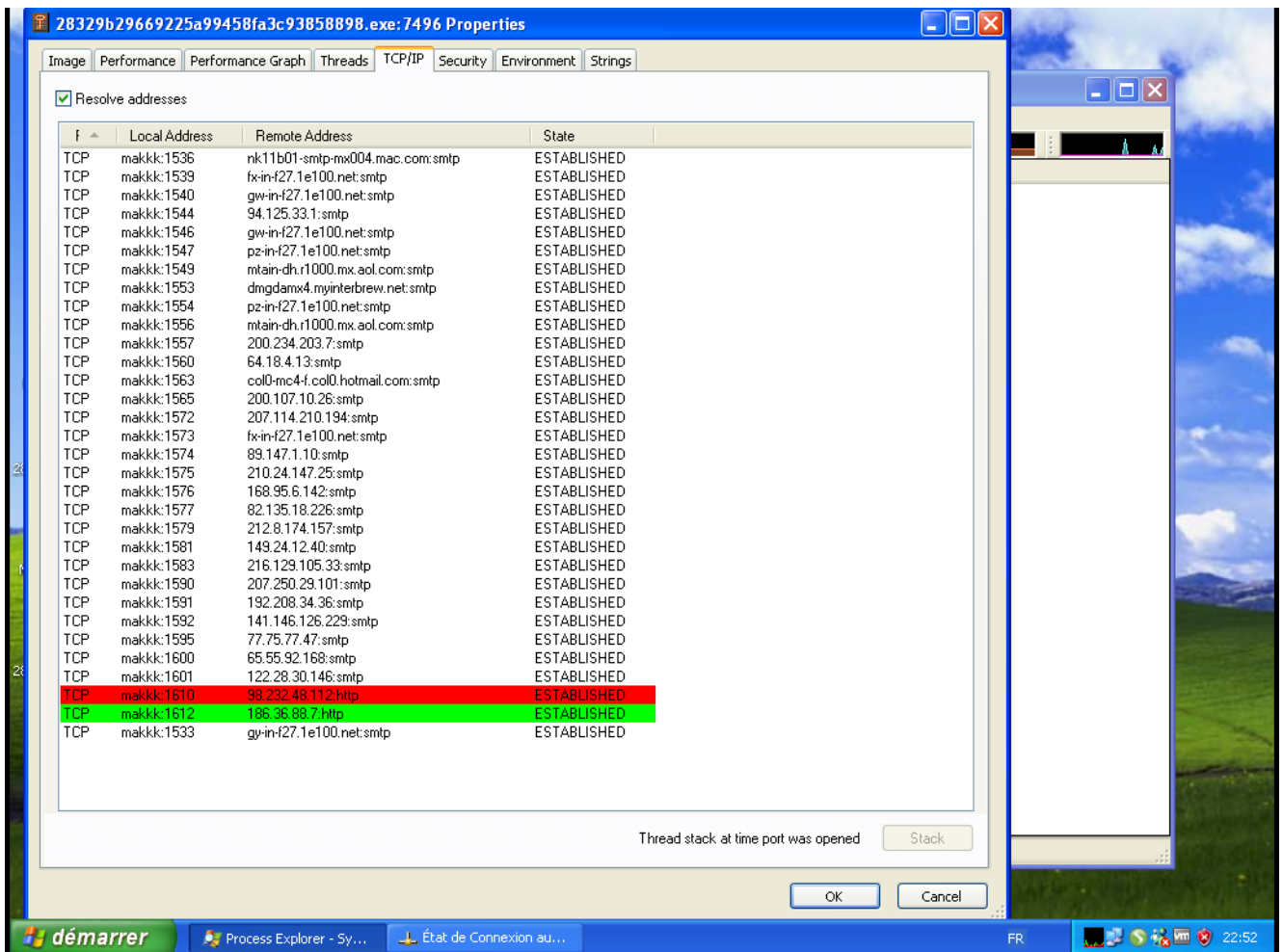
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

o SmartIndex = « %System%\cu5wgc5e.exe »[/quote]

Se connecte aux URLS suivantes :

```
4046 14.723831000 192.168.1.27
124.125.65.28 HTTP GET /vYho/w5/pMSeoeJQF.htm
HTTP/1.1
4073 14.755151000 192.168.1.27
95.168.185.46 HTTP GET /ughB3/T2YqxM.htm HTTP/1.1
4095 14.771043000 192.168.1.27
96.10.183.50 HTTP GET /SWPGbUA.htm HTTP/1.1
20598 74.778758000 192.168.1.27
86.5.55.51 HTTP GET /f0noxXpVU2wPFUMq.htm
HTTP/1.1
45091 134.800070000 192.168.1.27
85.204.200.123 HTTP GET /kZoF.htm HTTP/1.1
60697 194.821729000 192.168.1.27
75.82.161.198 HTTP GET /KbG0.htm HTTP/1.1
76864 254.828514000 192.168.1.27
202.144.33.227 HTTP GET /kpTghns.htm HTTP/1.1
93848 314.844942000 192.168.1.27
77.41.10.228 HTTP GET /QXwYISJF9AuF1r.htm
HTTP/1.1
```

Comme précédemment, le malware est un Spambot :



Dans cette exemple, la campagne est pour un site de rencontre :

```
q:Quitter d:Effacer u:Récup s:Sauver m:Message r:Répondre g:Groupe ?:Aide
 1 Feb 21 Heather X (0,6K) Private Message
 2 0 Feb 21 Katie (0,6K) Friend Request
 3 0 Feb 21 Nancy (0,6K) Personal Message
 4 0 Feb 21 Katie U (0,6K) My Pics
 5 0 Feb 21 Brooke F (0,6K) My Pics
 6 0 Feb 21 Heather J (0,6K) Friend Request
 7 0 Feb 21 Heather (0,6K) Sexy Pictures
 8 0 Feb 21 Lindsay (0,6K) Facebook
 9 0 Feb 21 Lindsay (0,6K) Facebook Sent You A Message
10 0 Feb 21 Jen (0,6K) Facebook Message...
11 0 Feb 21 Stacy (0,6K) Hot Pictures
12 0 Feb 21 Facebook (0,6K) Private Message On Facebook
13 0 Feb 21 Stacy (0,6K) New Nude Pictures
14 0 Feb 21 Brooke (0,6K) New Naked Pictures
15 0 Feb 21 Sam (0,6K) Sam Sent You A Message
16 0 Feb 21 Monica (0,6K) Monica Sent You A Message
17 0 Feb 21 Lisa (0,6K) New Nude Pictures
18 0 Feb 21 Lisa (0,6K) Sexy Pictures
19 0 Feb 21 Facebook (0,6K) Friend Request
20 0 Feb 21 Brooke I (0,6K) Facebook Sent You A Message....
21 0 Feb 21 Nancy (0,6K) Facebook
22 0 Feb 21 Katie V (0,6K) Facebook Sent You A Message....
23 0 Feb 21 Brooke (0,6K) Private Message
24 0 Feb 21 Sam (0,6K) Facebook Sent You A Message
25 0 Feb 21 Sam (0,6K) New Nude Pictures
26 0 Feb 21 Sam (0,6K) My Pics
27 0 Feb 21 Sarah (0,6K) Facebook Message...
28 0 Feb 21 Katie U (0,6K) Facebook Message...
29 0 Feb 21 Stacy (0,6K) New Naked Pictures
30 0 Feb 21 Sarah (0,6K) Sarah Sent You A Message
31 0 Feb 21 Sam (0,6K) You Have A Message From Facebook
32 0 Feb 21 Facebook (0,6K) Facebook Sent You A Message
33 0 Feb 21 Heather S (0,6K) Facebook Sent You A Message
34 0 Feb 21 Monica (0,6K) Hot Pictures
35 0 Feb 21 Heather T (0,6K) Facebook Message...
36 0 Feb 21 Sarah (0,6K) Personal Message
37 0 Feb 21 Sarah B (0,6K) Private Message
38 0 Feb 21 Lisa (0,6K) Facebook
39 0 Feb 21 Heather E (0,6K) Sexy Pictures
40 0 Feb 21 Facebook (0,6K) New Naked Pictures
41 0 Feb 21 Heather B (0,6K) Private Message On Facebook
42 0 Feb 21 Katie I (0,6K) New Naked Pictures
43 0 Feb 21 Heather (0,6K) My Pics
44 0 Feb 21 Facebook (0,6K) Facebook Message...
45 0 Feb 21 Stacy (0,6K) Personal Message
46 0 Feb 21 Heather (0,6K) Sexy Pictures
47 0 Feb 21 Facebook (0,6K) Private Message
48 0 Feb 21 Sarah B (0,6K) Personal Message
49 0 Feb 21 Katie (0,6K) You Have A Message From Facebook
.*-Mutt: /var/spool/qpsmtpd/Maildir/ [Msgs:1255 New:58 Old:1196 3,5M]---(threads/date)-----
Nouveau(x) message(s) dans cette boîte aux lettres.
```

Exemple de mail :

Date: Wed, 21 Feb 2001 06:11:56 -0500
From: Katie U <notification+akfjmruo@93BiwvN0.com>
To: hidiat <hidiat@hotmail.com>
Subject: My Pics
X-Mailer: ZuckMail [version 1.00]

Katie U sent you a message...

Hey,

How are you doing today? It was nice chatting with you the other day. We should talk more, it was fun.

You can find me on this new site <http://www.localgirlhookups.net> come check it out and see my new pics i just posted for you.

Katie U

Supression de Backdoor:Win32/Kelihos.A

Il est donc conseillé de suivre le [Tutorial et Guide Procédure standard de désinfection de virus](#)