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

Nouvelle version possible du botnet Storm/Waldeac

Actuellement seul Microsoft a créé une nouvella 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 expoits 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

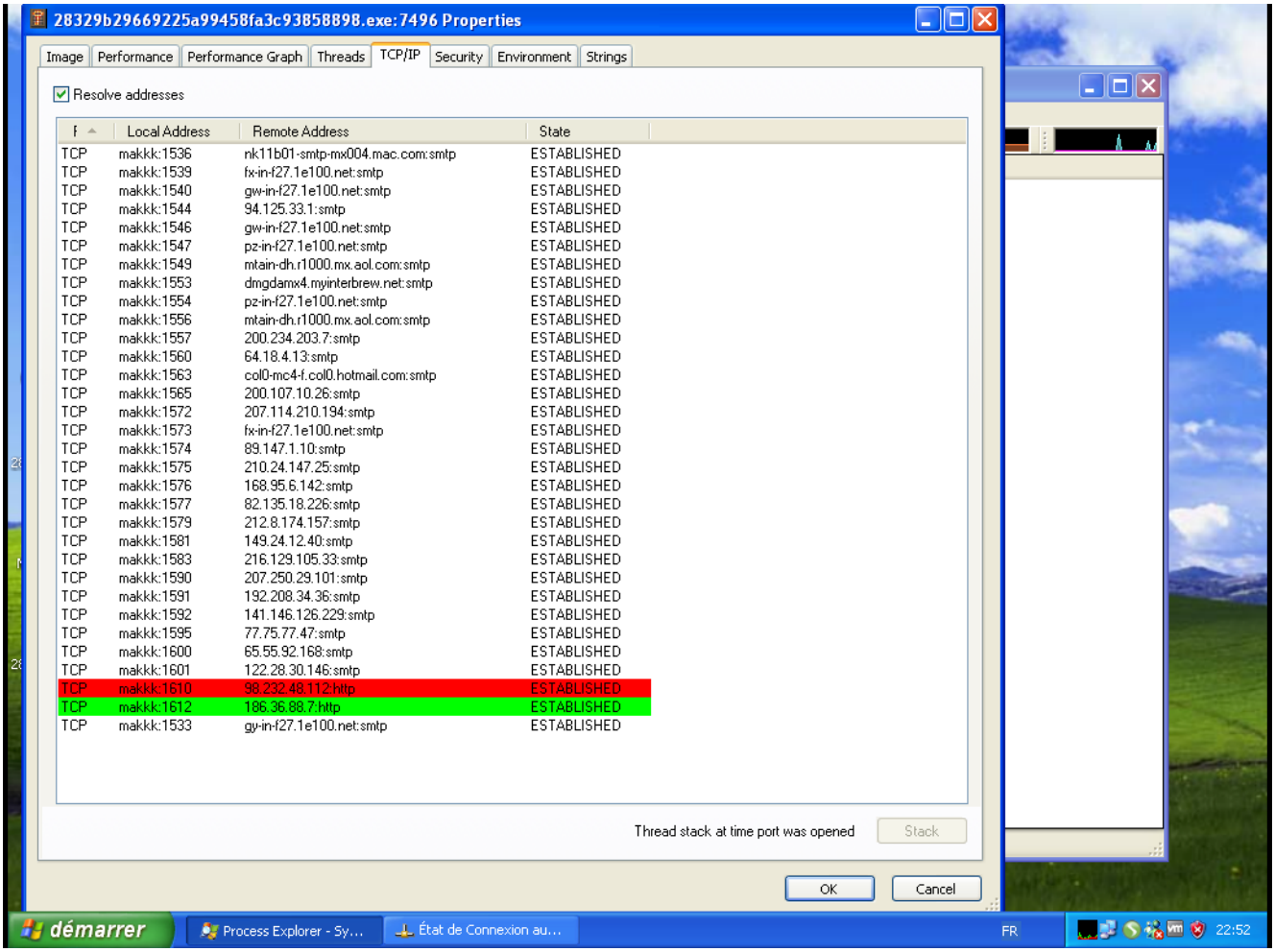
Backdoor:Win32/Kelihos.A

Le malware ajoute une clef Run *SmartIndex* pour se charger – exemple :
[quote]*
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
o SmartIndex = « %System%\cu5wcgc5e.exe »[/quote]

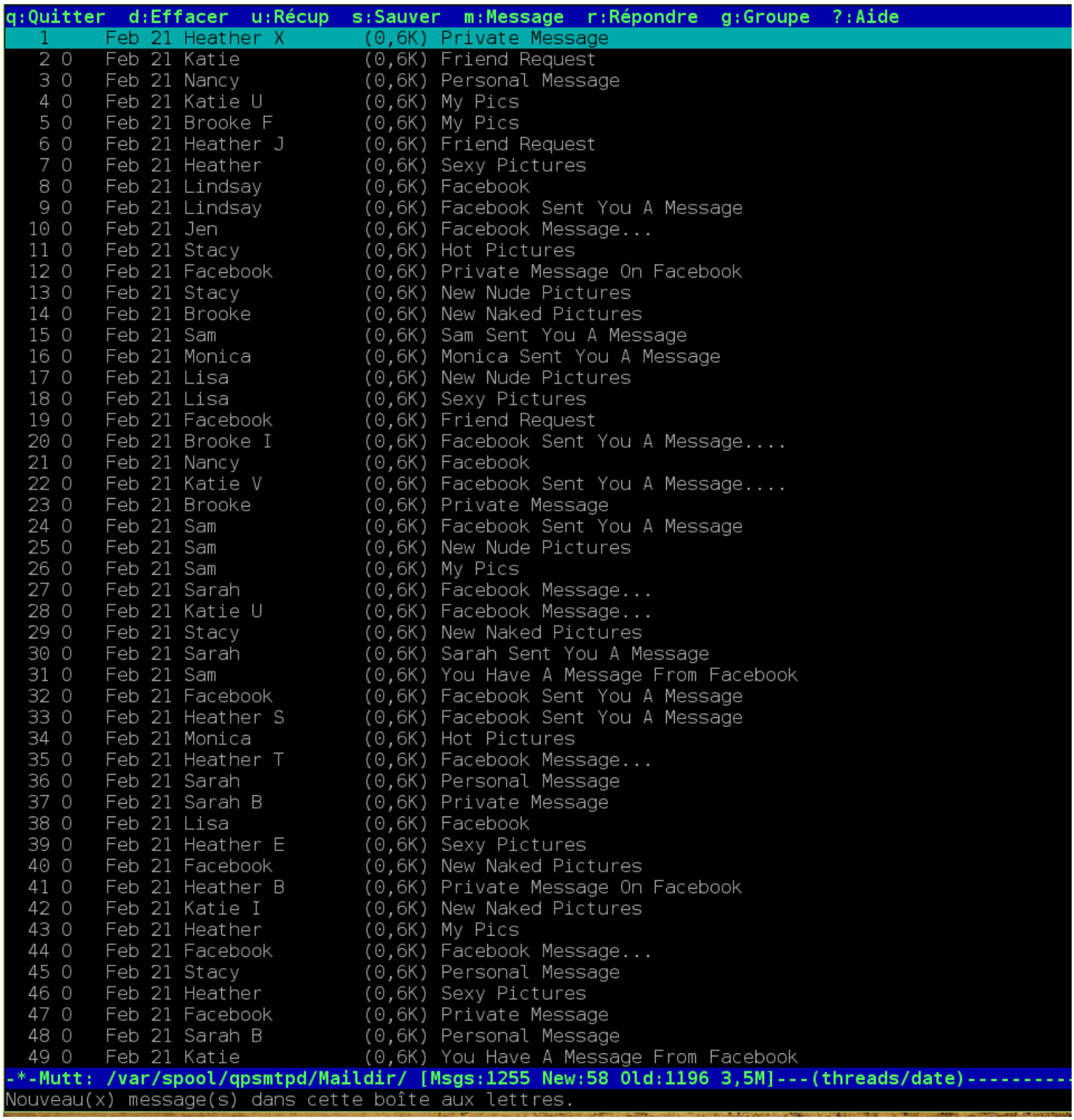
Se connecte aux URLS suivantes :

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 /fOnoxXpVU2wPFUMq.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 /KbGO.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 :



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