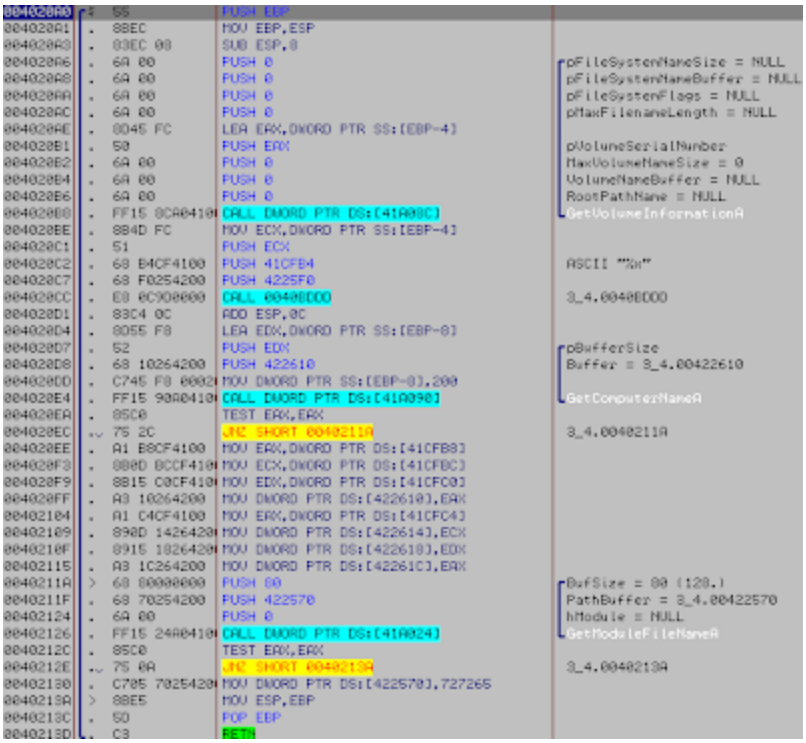
Alina 3.4 (POS Malware)

xylibox.com/2013/02/alina-34-pos-malware.html

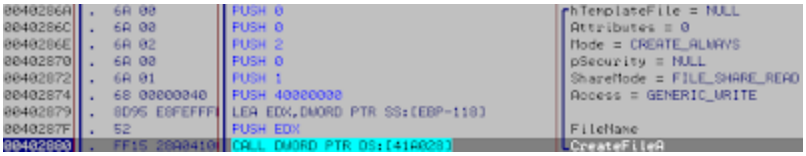
The malware come from: http://vxvault.siri-urz.net/ViriFiche.php?ID=23179
Hosted on the site of a deputy.

GetPCname:



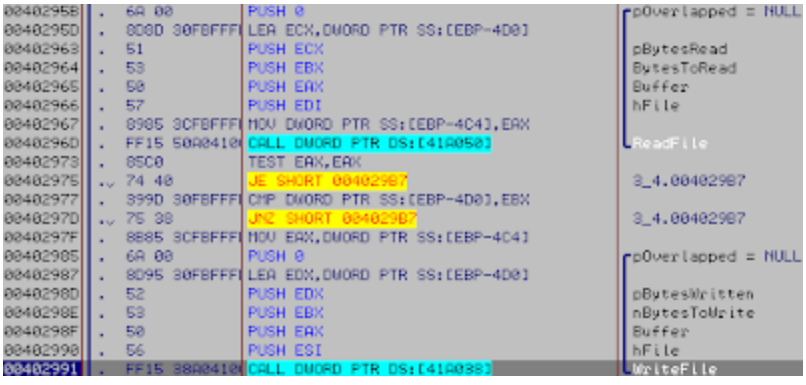
Create a mutex:

Create /%appdata%/java.exe

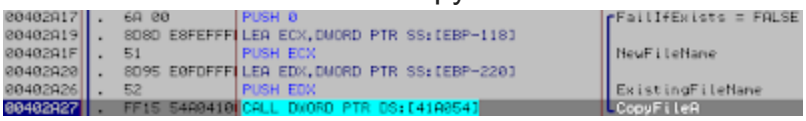


If the malware can't he will try with different name (jusched.exe, jucheck.exe, desktop.exe, dwm.exe, win-firewall.exe, adobeflash.exe)

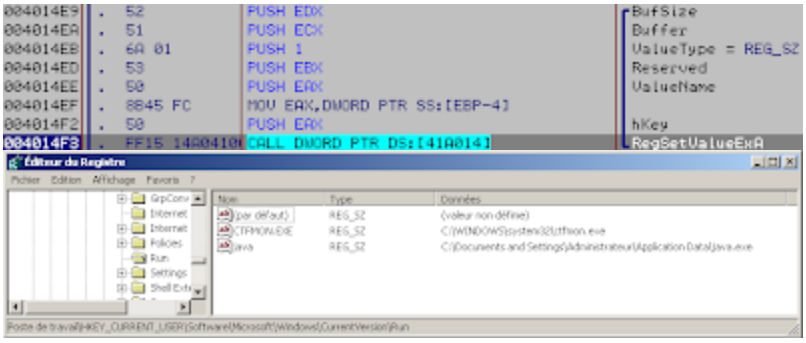
If all names are take and in read only mode the malware is trapped on infinit loop :))) Write the file:



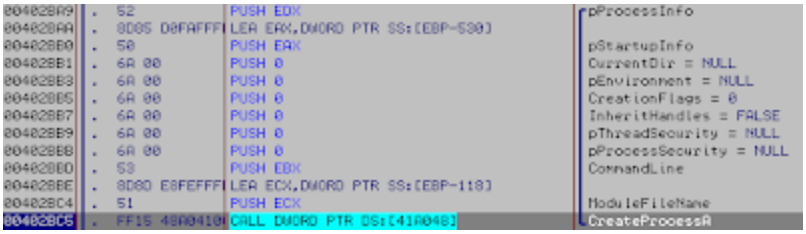
and if he fail to write he will Copy it:



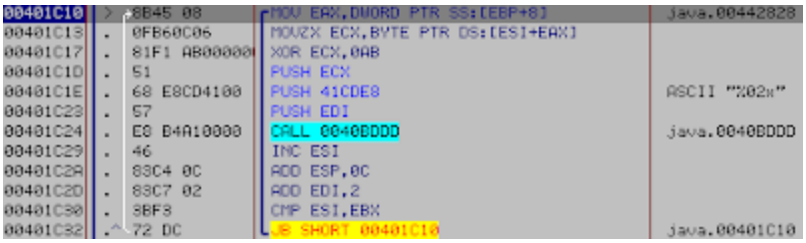
Add a registry persistence:



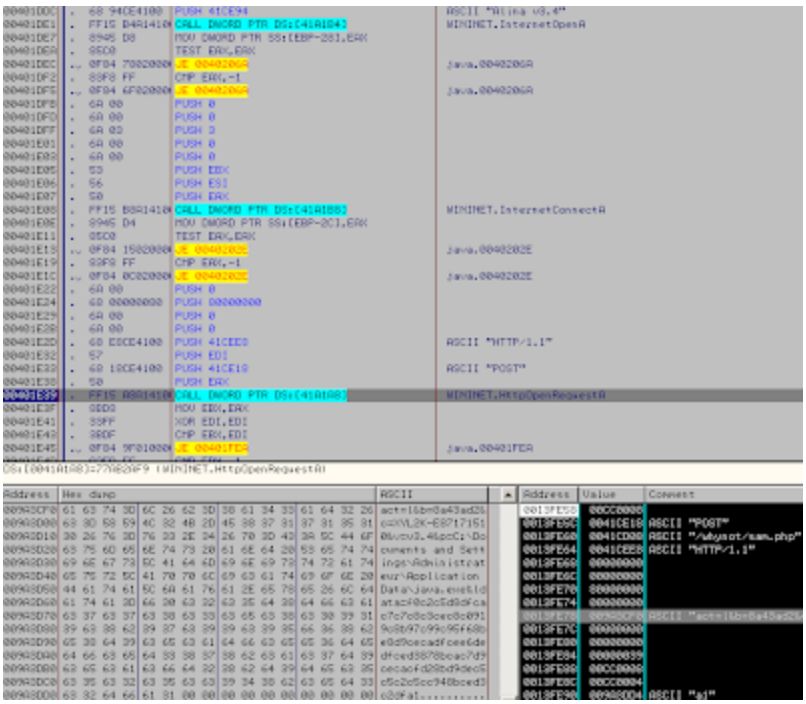
Launch the process:



Encode something (i've not checked what)

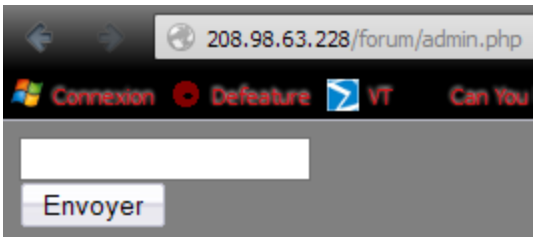


Call the C&C

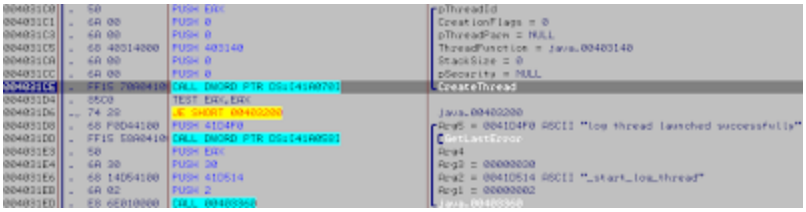


And fail because the first is dead, so retry with 208.98.63.228
Backend info:
208.98.63.228:
OrgName: Sharktech
OrgId: SHARK-7
Address: 100 Pinehurst Ct.
City: Missoula
StateProv: MT
PostalCode: 59803
Country: US

http://xxx.98.63.228/main.php
http://xxx.98.63.228/info.php
http://xxx.98.63.228/test.php
http://xxx.98.63.228/test2.php
http://xxx.98.63.228/api.php
http://xxx.98.63.228/config.php
http://xxx.98.63.228/autoupdate.php
http://xxx.98.63.228/404.html
http://xxx.98.63.228/wordpress/admin.php
http://xxx.98.63.228/forum/admin.php
http://xxx.98.63.228/blog/admin.php
http://xxx.98.63.228/blog/export.php
http://xxx.98.63.228/blog/config.php
http://xxx.98.63.228/blog/front/stats.php
http://xxx.98.63.228/blog/front/cards.php
http://xxx.98.63.228/blog/front/settings.php
http://xxx.98.63.228/blog/front/logs.php



This one is cool because coder leaved comments for each action...



I tried to trigger it to send data but i've not succeeded yet.
I will see the rest later.
Alina is interesting i've found many version: http://www.kernelmode.info/forum/viewtopic.php?f=16&t=1756&start=40#p18008
Still i've not checked these files for the moment, i don't know differences.