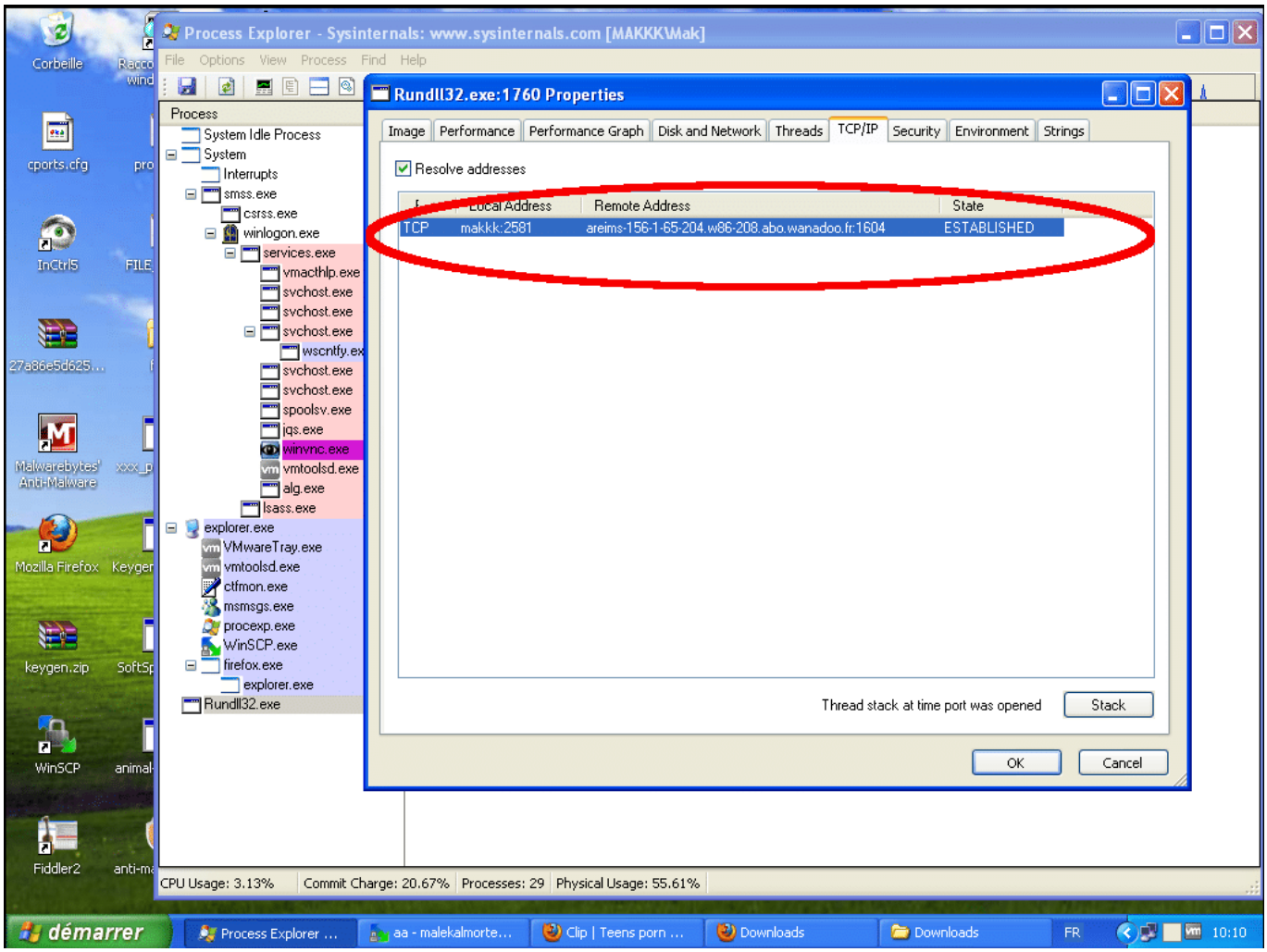
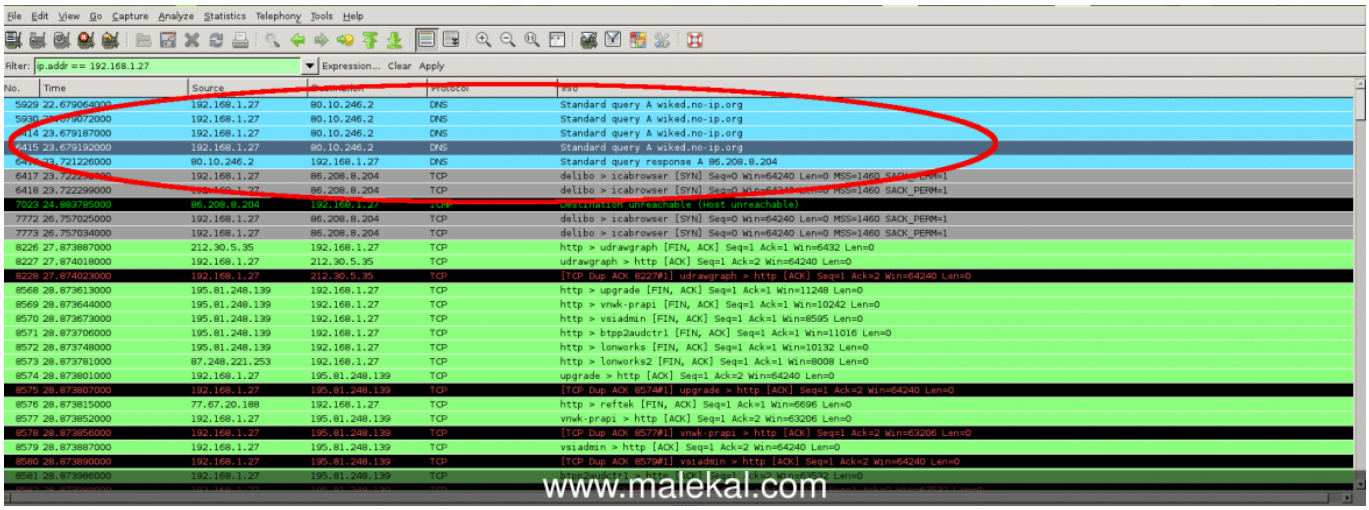
Backdoor:Win32/Fynloski.A sur Orange via no-ip.org

Suite en quelque sorte du billet planete-lolo : cracks et….. RATs – où je suis depuis quelques jours les cracks qui y sont postés sur ce boad Warez.
La majorité sont des malwares et notamment, il y a une campagne de malware détecté en Backdoor:Win32/Fynloski.A par Microsoft qui sont postés par le même auteur.
Les détections sont relativement mauvaises, le pirate utilisant des stubs pour bypasser les détections.

Ces derniers conduisent via des adresses no-ip.org à une IP Orange sur le BAS de Reims-156 (IP en 86.208.)





Le premier thesheitan.no-ip.org a été fermé par l'abuse de no-ip, il y a quelques jours :

thesheitan.no-ip.org :
http://www3.malekal.com/malwares/index.php?&hash=bd1829843641d264c9ef57ee175a68ae
http://www3.malekal.com/malwares/index.php?&hash=23164d9a65009224da40f273e742e268
http://www3.malekal.com/malwares/index.php?&hash=f629ee640abd8be3ede2f57f4fe66057
http://www3.malekal.com/malwares/index.php?&hash=e0fa1ac1c9b50c988b970408fede0585

Du coup, le pirate est passé sur un autre no-ip.org **wiked.no-ip.org** qui vient d'être fermé à l'instant :
http://www3.malekal.com/malwares/index.php?&hash=98ec68e0b73728b2bfc0fb2cbca31227
http://www3.malekal.com/malwares/index.php?&hash=5d0a0678b0c710afaf9e0a0a8bc3dae8

```
malekalmorte@MaK-tux:/tmp$ host wiked.no-ip.org ; host thesheitan.no-ip.org
wiked.no-ip.org has address 0.0.0.0
thesheitan.no-ip.org has address 86.208.78.41
```

Très certainement donc le pirate a perdu des machines infectées suite à ces coupures, ce dernier ne semble pas vouloir d'ailleurs maintenant ses machines infectées car il ne

semble pas faire télécharger des mises à jour non détectées.

Je profite de ce billet pour saluer l'abuse de no-ip qui est super réactif, ça fait plaisir (d'ailleurs ils m'ont parlé d'un troisième compte inti-fada.no-ip.org).
J'ai aussi maillé l'Abuse d'Orange, mais pas certains qu'il y aura des suites.

On verra si de nouveaux malwares avec de nouveaux no-ip.org vont être mis en ligne.
Le traditionnel jeu du chat et de la souris.