

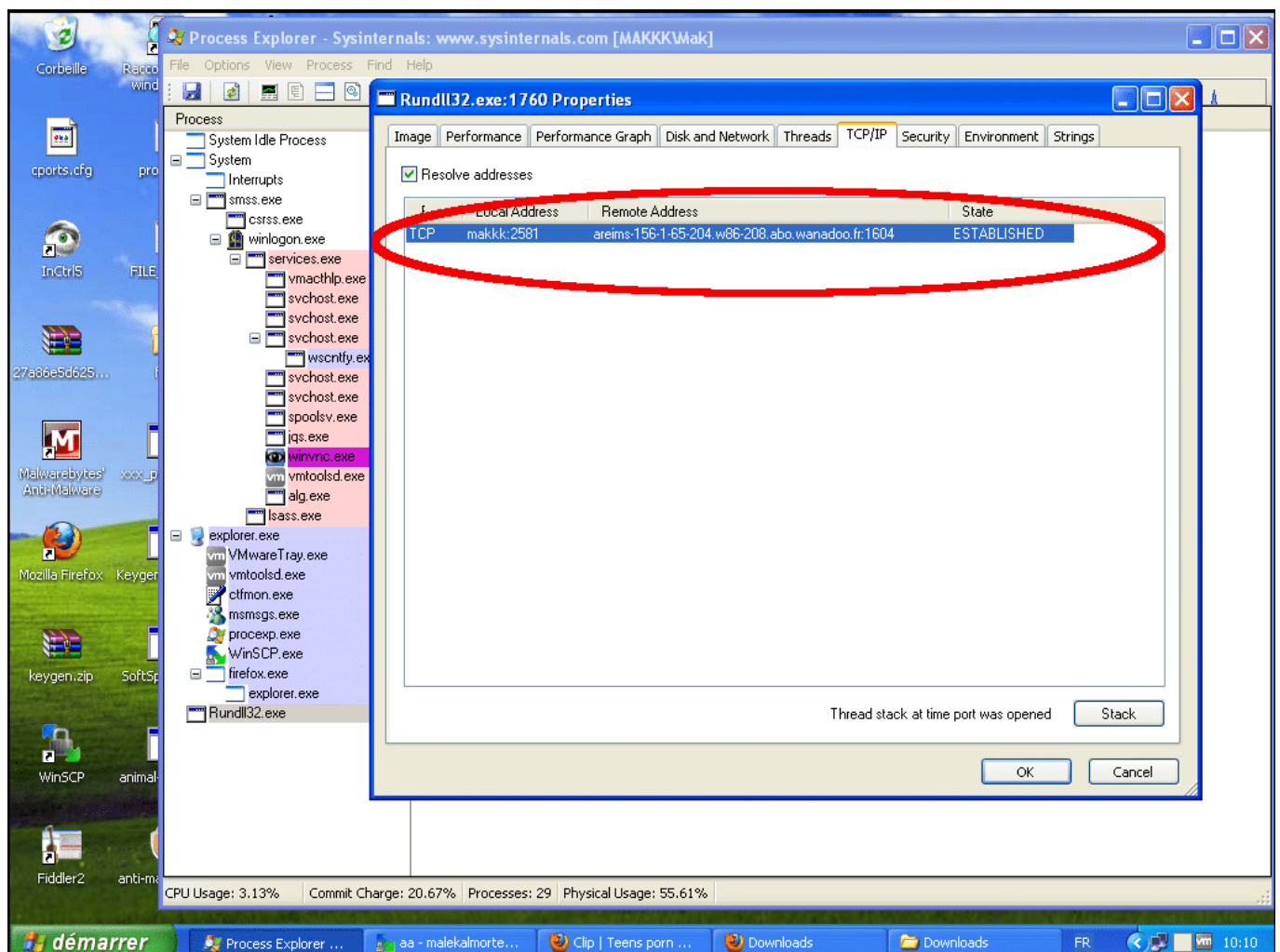
Backdoor:Win32/Fynloski.A sur Orange via no-ip.org

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.)



No.	Time	Source	Destination	Protocol	Info
5929	22.679064000	192.168.1.27	80.10.246.2	DNS	Standard query A wiked.no-ip.org
5930	22.679072000	192.168.1.27	80.10.246.2	DNS	Standard query A wiked.no-ip.org
6114	23.679187000	192.168.1.27	80.10.246.2	DNS	Standard query A wiked.no-ip.org
6415	23.679192000	192.168.1.27	80.10.246.2	DNS	Standard query A wiked.no-ip.org
6417	23.722260000	80.10.246.2	192.168.1.27	DNS	Standard query response A 86.208.8.204
6418	23.722290000	192.168.1.27	86.208.8.204	TCP	delibo > icabrowser [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6523	24.483785000	86.208.8.204	192.168.1.27	TCP	86.208.8.204 > 192.168.1.27:80 [RST] Win=0 Len=0
7772	26.757025000	192.168.1.27	86.208.8.204	TCP	delibo > icabrowser [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
7773	26.757034000	192.168.1.27	86.208.8.204	TCP	delibo > icabrowser [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8226	27.873887000	212.30.5.35	192.168.1.27	TCP	http > udrawgraph [FIN, ACK] Seq=1 Ack=1 Win=6432 Len=0
8227	27.874018000	192.168.1.27	212.30.5.35	TCP	udrawgraph > http [ACK] Seq=1 Ack=2 Win=64240 Len=0
8228	27.874023000	192.168.1.27	212.30.5.35	TCP	[TCP Dup ACK 8227#1] udrawgraph > http [ACK] Seq=1 Ack=2 Win=64240 Len=0
8568	28.873613000	195.81.248.139	192.168.1.27	TCP	http > upgrade [FIN, ACK] Seq=1 Ack=1 Win=11248 Len=0
8569	28.873644000	195.81.248.139	192.168.1.27	TCP	http > vnk-prapi [FIN, ACK] Seq=1 Ack=1 Win=10242 Len=0
8570	28.873673000	195.81.248.139	192.168.1.27	TCP	http > vsiadmin [FIN, ACK] Seq=1 Ack=1 Win=8595 Len=0
8571	28.873706000	195.81.248.139	192.168.1.27	TCP	http > http2audctrl [FIN, ACK] Seq=1 Ack=1 Win=11016 Len=0
8572	28.873748000	195.81.248.139	192.168.1.27	TCP	http > lonworks [FIN, ACK] Seq=1 Ack=1 Win=10132 Len=0
8573	28.873781000	87.248.221.253	192.168.1.27	TCP	http > lonworks2 [FIN, ACK] Seq=1 Ack=1 Win=8008 Len=0
8574	28.873801000	192.168.1.27	195.81.248.139	TCP	upgrade > http [ACK] Seq=1 Ack=2 Win=64240 Len=0
8575	28.873807000	192.168.1.27	195.81.248.139	TCP	[TCP Dup ACK 8574#1] upgrade > http [ACK] Seq=1 Ack=2 Win=64240 Len=0
8576	28.873815000	77.67.20.188	192.168.1.27	TCP	http > reftak [FIN, ACK] Seq=1 Ack=1 Win=6596 Len=0
8577	28.873820000	192.168.1.27	195.81.248.139	TCP	vnk-prapi > http [ACK] Seq=1 Ack=2 Win=63206 Len=0
8578	28.873825000	192.168.1.27	195.81.248.139	TCP	[TCP Dup ACK 8577#1] vnk-prapi > http [ACK] Seq=1 Ack=2 Win=63206 Len=0
8579	28.873887000	192.168.1.27	195.81.248.139	TCP	vsadmin > http [ACK] Seq=1 Ack=2 Win=64240 Len=0
8580	28.873890000	192.168.1.27	195.81.248.139	TCP	[TCP Dup ACK 8579#1] vsadmin > http [ACK] Seq=1 Ack=2 Win=64240 Len=0
8581	28.873898000	192.168.1.27	195.81.248.139	TCP	http > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
8582	28.873900000	192.168.1.27	195.81.248.139	TCP	http > http [ACK] Seq=1 Ack=1 Win=64240 Len=0

www.malekal.com

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.