Voilà comment faire quelques vérifications sur la provenance de mails, surtout quand il y a une grosse somme en jeu.

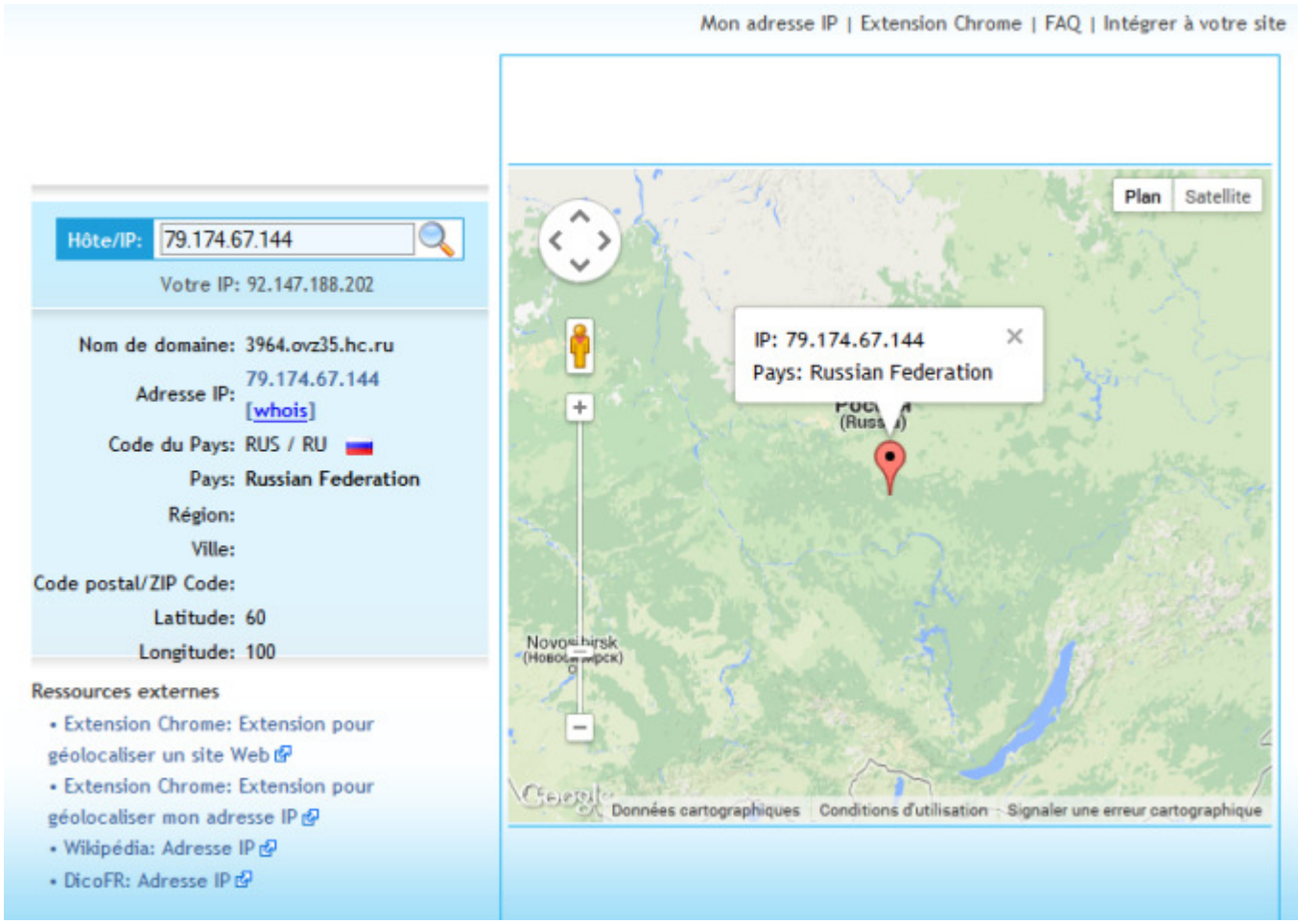
Outils :
- Whois, pour trouver qui est le propriétaire d'une plage d'adresses.
http://www.frameip.com/whois/
- Localiser sur une carte, l'adresse de l'expéditeur. http://fr.geoipview.com/

Dernière attaque en date : un faux mail i Tunes. Rien qu'à le voir on sait que c'est un faux, mais le principe reste le même.
- Dans la messagerie, il y a moyen de voir l'ip de l'expéditeur, tout du moins de son serveur de messagerie, ce qui donne normalement sa position géographique. Il est clair, que quelqu'un qui ouvre une B.a.l sur laposte.net, aura une adresse en France.
Donc, il y a par exemple "voir l'entête complet", "détails"...et quand on clique, on voit ceci :

Après avoir mis l'adresse dans Frameip, on a ceci:
inetnum: 79.174.64.0 - 79.174.95.255
netname: HOSTING-COMPANY-NET
descr: Hosting center Ltd.
country: RU
org: ORG-HCO1-RIPE
admin-c: GPT-RIPE
tech-c: GPT-RIPE
status: ASSIGNED PI
mnt-by: RIPE-NCC-END-MNT
mnt-lower: RIPE-NCC-END-MNT
mnt-by: AS5537-MNT
mnt-routes: AS5537-MNT
mnt-domains: AS5537-MNT
source: RIPE # Filtered

organisation: ORG-HCO1-RIPE
org-name: Hosting center Ltd.
org-type: OTHER
descr: OOO Hosting Company, data center
address: 5th Donskoy str., build 15-4
address: RUSSIAN FEDERATION, Moscow
phone: +7 495 5445566
fax-no: +7 495 5140957
admin-c: IA327-RIPE
tech-c: IA327-RIPE
mnt-ref: AS5537-MNT
mnt-by: AS5537-MNT
source: RIPE # Filtered

C'est clair, ça ne vient pas des US. Sur la carte ...



Une autre attaque de soit disant ma banque...

Un vrai mail de Paypal envoyé par une société spécialisée...

NetRange: 96.47.16.0 - 96.47.31.255
CIDR: 96.47.16.0/20
OriginAS: AS46263
NetName: E-DIALOG
NetHandle: NET-96-47-16-0-1
Parent: NET-96-0-0-0-0
NetType: Direct Allocation
RegDate: 2009-11-05
Updated: 2012-03-02
Ref: http://whois.arin.net/rest/net/NET-96-47-16-0-1

OrgName: e-Dialog, Inc
OrgId: EDIAL-2
Address: 65 Network Drive
City: Burlington
StateProv: MA
PostalCode: 01803
Country: US
RegDate: 2008-04-08
Updated: 2013-06-06
Ref: http://whois.arin.net/rest/org/EDIAL-2

La plage d'adresse de paypal.com est enregistrée par E-Bay

NetRange: 66.211.160.0 - 66.211.191.255
CIDR: 66.211.160.0/19
OriginAS:
NetName: EBAY-2
NetHandle: NET-66-211-160-0-1
Parent: NET-66-0-0-0-0
NetType: Direct Assignment
RegDate: 2006-01-25
Updated: 2012-03-02
Ref: http://whois.arin.net/rest/net/NET-66-211-160-0-1

OrgName: eBay, Inc
OrgId: EBAY
Address: 2145 Hamilton Ave
City: San Jose
StateProv: CA
PostalCode: 95008
Country: US
RegDate: 1998-11-02
Updated: 2011-09-24
Ref: http://whois.arin.net/rest/org/EBAY