Bonnes pratiques pour les Utilisateurs

CERT OSIRIS

UNIVERSITÉ DE STRASBOURG

Sensibilisation aux menaces Internet & Formation aux bonnes pratiques pour les utilisateurs (BPU) de systèmes informatiques

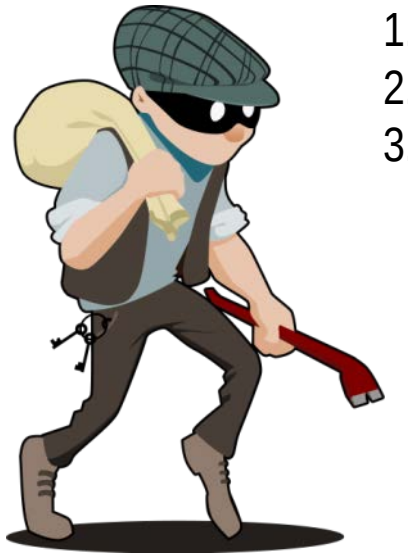
Goodies
Exemples d'incidents SSI

Septembre 2013

Vol d'informations sensibles
Perte de données scientifiques
Vol d'un ordinateur portable

Vulnérabilité exploitée :
naiveté/candeur de l'utilisateur

Gare de l'EST, Paris.
Un chercheur monte dans le train, place son ordinateur portable sur la tablette au dessus de son siège. Avant le départ du train, une dame échange discrètement sa sacoche avec une sacoche vide, il ne se rend compte de rien.



Incidences :

1. Perte financière
2. Le portable n'était pas chiffré : vol de données sensibles
3. La sauvegarde se trouvait … dans la sacoche : perte de 9 mois de données

Infection d'un ordinateur
(via lien piégé dans un mail)

Vulnérabilité exploitée : curiosité de l'utilisateur

De : Facebook [notification+zrdozoee1ohe@facebookmail.com] Date : ven. 26/11/2010 02:59
À : xxx yyy
Cc :
Objet : Amy Fibro commented on your photo.

Amy Fibro commented on your photo.

To see the comment thread, follow the link below:
http://www.facebook.com/n/?photo.php&fbid=155175754523620&set=a.145049682202894.23363.100000035890817&mid=33283faG5af34842cf81G...7f9cbG9
Thanks,
The Facebook Team

http://188.120.225.116/config/iqywjmypgzknisaugpkv.php
Cliquez pour suivre le lien

Journaux de gestion des clients - Journal de sécurité

Fichier Edition Afficher Filtrer Opération ?

Date et heure	Type d'événement	Gravité	Direction	Protocole	Hôte distant
26/11/2010 09:02:42	Réponse active	Majeure	Entrant	Aucun(e)	188.120.225.116
26/11/2010 09:02:42	Prévention d'intrusion	Critique	Entrant	TCP	188.120.225.116

[SID : 23528] Détection de HTTP Fragus Toolkit Download Activity.
Le trafic a été bloqué à partir de cette application : firefox.exe

adresse ip

188.120.225.116

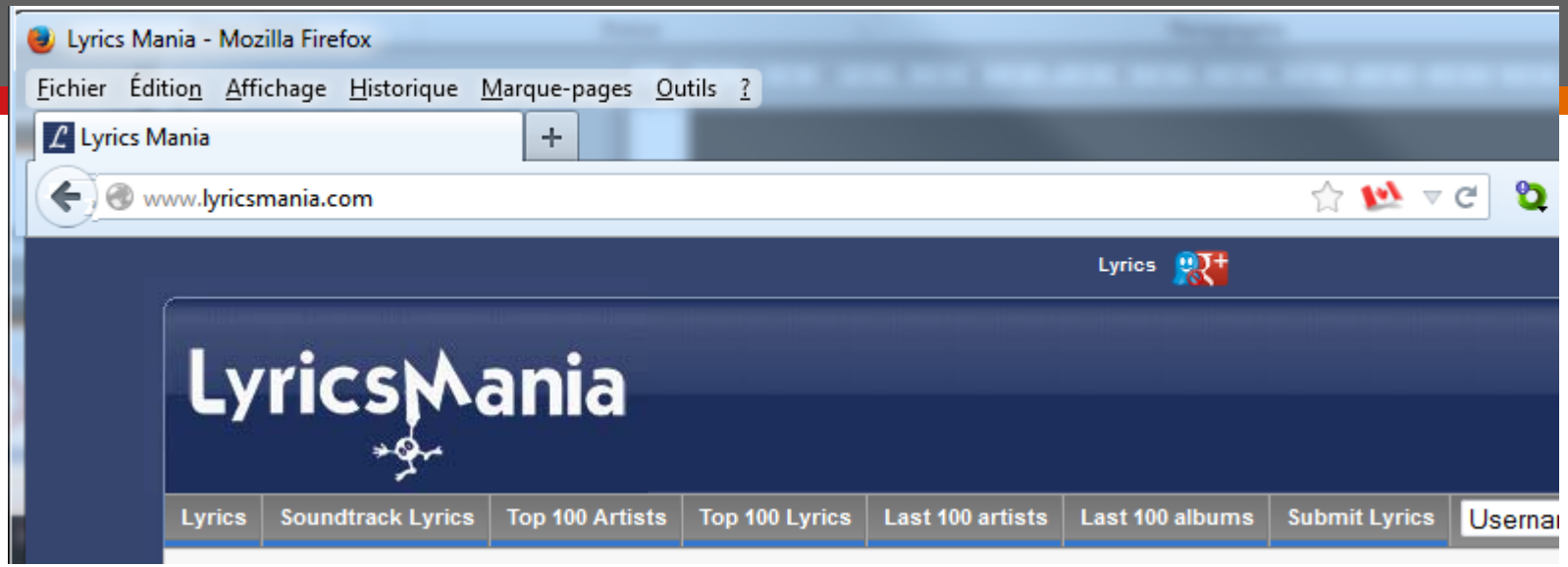
st35.ru

Moscow, RU
Latitude : 55.752201, Longitude : 37.615601
Fournisseur d'accès : ISPsystem, cjsc

Infection de poste par une simple connexion sur un site web

Vulnérabilité exploitée :

faille JAVA + logiciel non à jour



- La connexion sur la page d'accueil de *www.lyricsmania.com* a provoqué une rafale de 231 connexions sur 86 adresses différentes, durée : 20 secondes

  09:26:14 1ère connexion sur www.lyricsmania.com
  09:26:34 fin des connexions

Une charge virale a été transmise par le site *ndmuiyerxvcol.generation-string-vwa-gchk-lrn.org*

Adresse IP (91.237.153.23) localisée en Russie

Taille du fichier virus : 157184 octets

Et l'antivirus ?

Nous avons soumis la souche virale à l'analyse de 37 logiciels d'antivirus.

Seuls 3 ont découvert le malware …

VirSCAN.org
submit & scan your file

Suspicious file(s) to scan: [ ] Upload

1, You can UPLOAD any files, but there is 20Mb limit per file.
2, VirSCAN supports Rar/Zip decompression, but it must be less than 20 files.
3, VirSCAN can scan compressed files with password 'infected' or 'virus'.

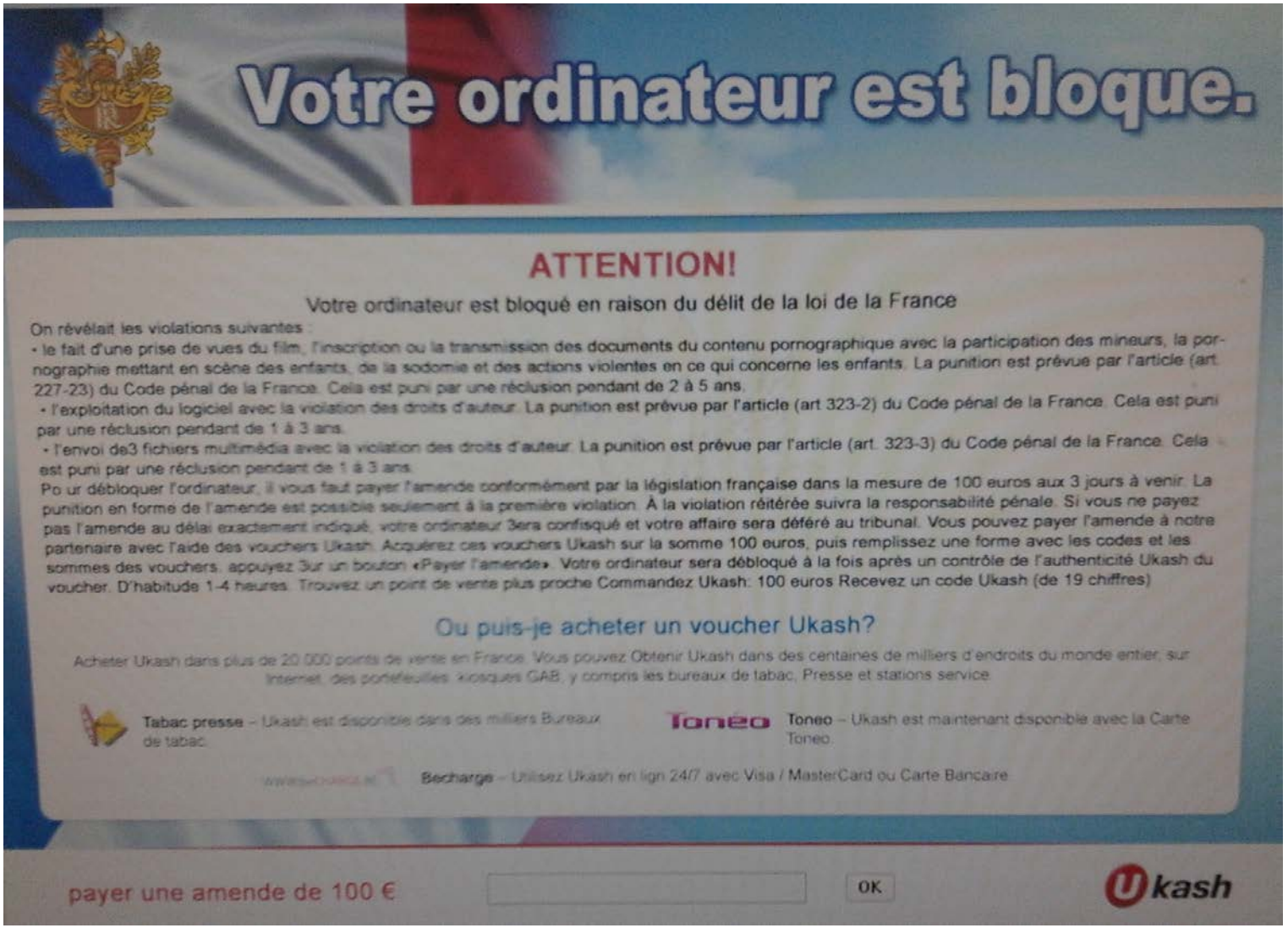
File information

File Name :	0.1927139202324737.ex1
File Size :	157184 byte
File Type :	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5 :	41ba3b2bfb7f4e5dc4c94dc29e2c4b92
SHA1 :	155d0544e4dd997ee5748defb542244b4b88e1a1

Scanner results

Scanner results : 8% Scanner(s) (3/37) found malware!
Time : 2012/09/10 15:47:40 (CEST)

Scanner	Engine Ver	Sig Ver	Sig Date	Scan result	Time
a-squared	5.1.0.4	20120910140339	2012-09-10	-	14.712
AhnLab V3	2012.09.10.00	2012.09.10	2012-09-10	-	2.724
AntiVir	8.2.10.150	7.11.41.132	2012-09-01	-	0.257
Antiy	2.0.18	2.0.18.	0002-18-00	-	0.412
Arcavir	2011	201206041805	2012-06-04	Heur.W32	7.376
Authentium	5.1.1	201209090949	2012-09-09	-	2.635
AVAST!	4.7.4	120910-0	2012-09-10	-	0.266
AVG	12.0.1787	2437/5259	2012-09-09	-	0.465
BitDefender	7.90123.7582943	7.43387	2012-09-10	-	4.715
ClamAV	0.97.5	15334	2012-09-10	-	0.357
Comodo	5.1	13487	2012-09-08	-	2.413
CP Secure	1.3.0.5	2012.09.10	2012-09-10	-	0.224

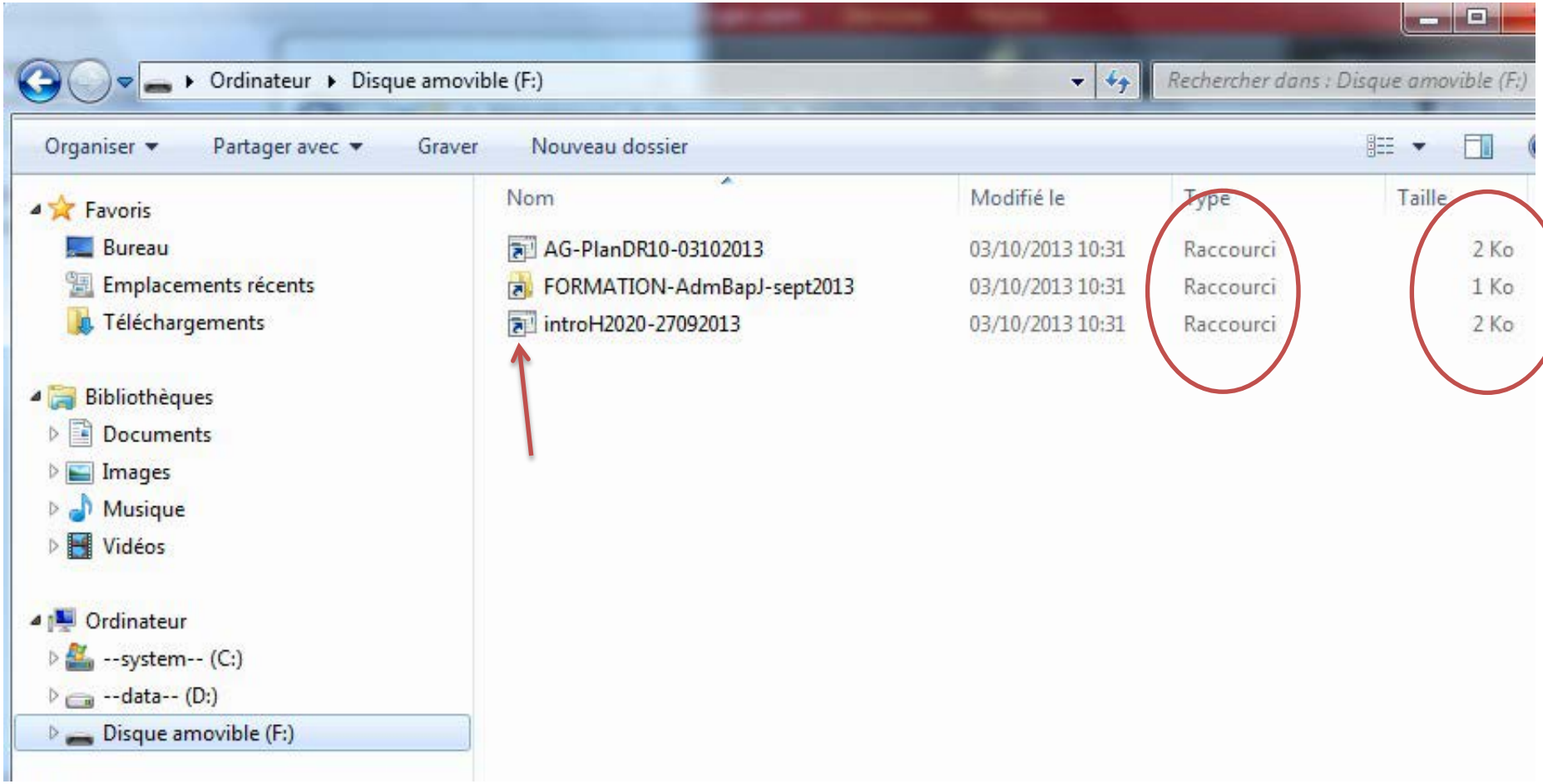

Votre ordinateur est bloque.
ATTENTION!
Votre ordinateur est bloqué en raison du délit de la loi de la France
On révélait les violations suivantes :
• le fait d'une prise de vues du film, l'inscription ou la transmission des documents du contenu pornographique avec la participation des mineurs, la pornographie mettant en scène des enfants, de la sodomie et des actions violentes en ce qui concerne les enfants. La punition est prévue par l'article (art. 227-23) du Code pénal de la France. Cela est puni par une réclusion pendant de 2 à 5 ans.
• l'exploitation du logiciel avec la violation des droits d'auteur. La punition est prévue par l'article (art 323-2) du Code pénal de la France. Cela est puni par une réclusion pendant de 1 à 3 ans.
• l'envoi de3 fichiers multimédia avec la violation des droits d'auteur. La punition est prévue par l'article (art. 323-3) du Code pénal de la France. Cela est puni par une réclusion pendant de 1 à 3 ans.
Po ur débloquer l'ordinateur, il vous faut payer l'amende conformément par la législation française dans la mesure de 100 euros aux 3 jours à venir. La punition en forme de l'amende est possible seulement à la première violation. À la violation réitérée suivra la responsabilité pénale. Si vous ne payez pas l'amende au délai exactement indiqué, votre ordinateur 3era confisqué et votre affaire sera déféré au tribunal. Vous pouvez payer l'amende à notre partenaire avec l'aide des vouchers Ukash. Acquérez ces vouchers Ukash sur la somme 100 euros, puis remplissez une forme avec les codes et les sommes des vouchers, appuyez 3ur un bouton «Payer l'amende». Votre ordinateur sera débloqué à la fois après un contrôle de l'authenticité Ukash du voucher. D'habitude 1-4 heures. Trouvez un point de vente plus proche Commandez Ukash: 100 euros Recevez un code Ukash (de 19 chiffres)
Ou puis-je acheter un voucher Ukash?
Acheter Ukash dans plus de 20 000 points de vente en France. Vous pouvez Obtenir Ukash dans des centaines de milliers d'endroits du monde entier, sur Internet, des portefeuilles, kiosques GAB, y compris les bureaux de tabac, Presse et stations service.
Tabac presse – Ukash est disponible dans des milliers Bureaux de tabac.
Toneo – Ukash est maintenant disponible avec la Carte Toneo.
Recharge – Utilisez Ukash en lign 24/7 avec Visa / MasterCard ou Carte Bancaire
payer une amende de 100 €
OK
Ukash

Infection du clé USB par un poste lui-même infecté

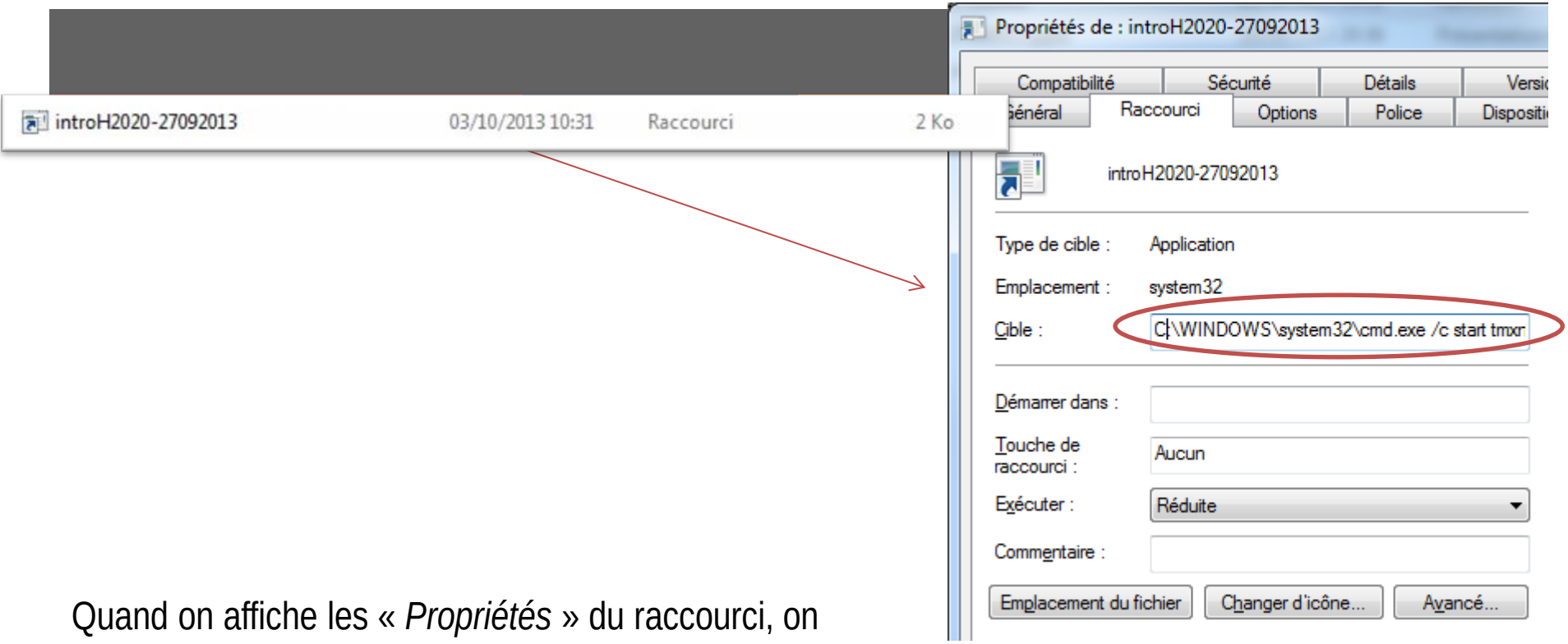
Vulnérabilités exploitées :

absence de protection des clés USB + manque de discernement de l'utilisateur

Les symptômes observés sur l'ordinateur :
Tous les fichiers sur la clé USB se présentent sous forme de raccourcis



INFO/RAPPEL : Les clés USB contiennent très rarement des raccourcis
(puisqu'un raccourci pointe par définition vers un autre emplacement, emplacement qui n'est plus disponible dès lors qu'on enlève la clé USB de l'ordinateur)



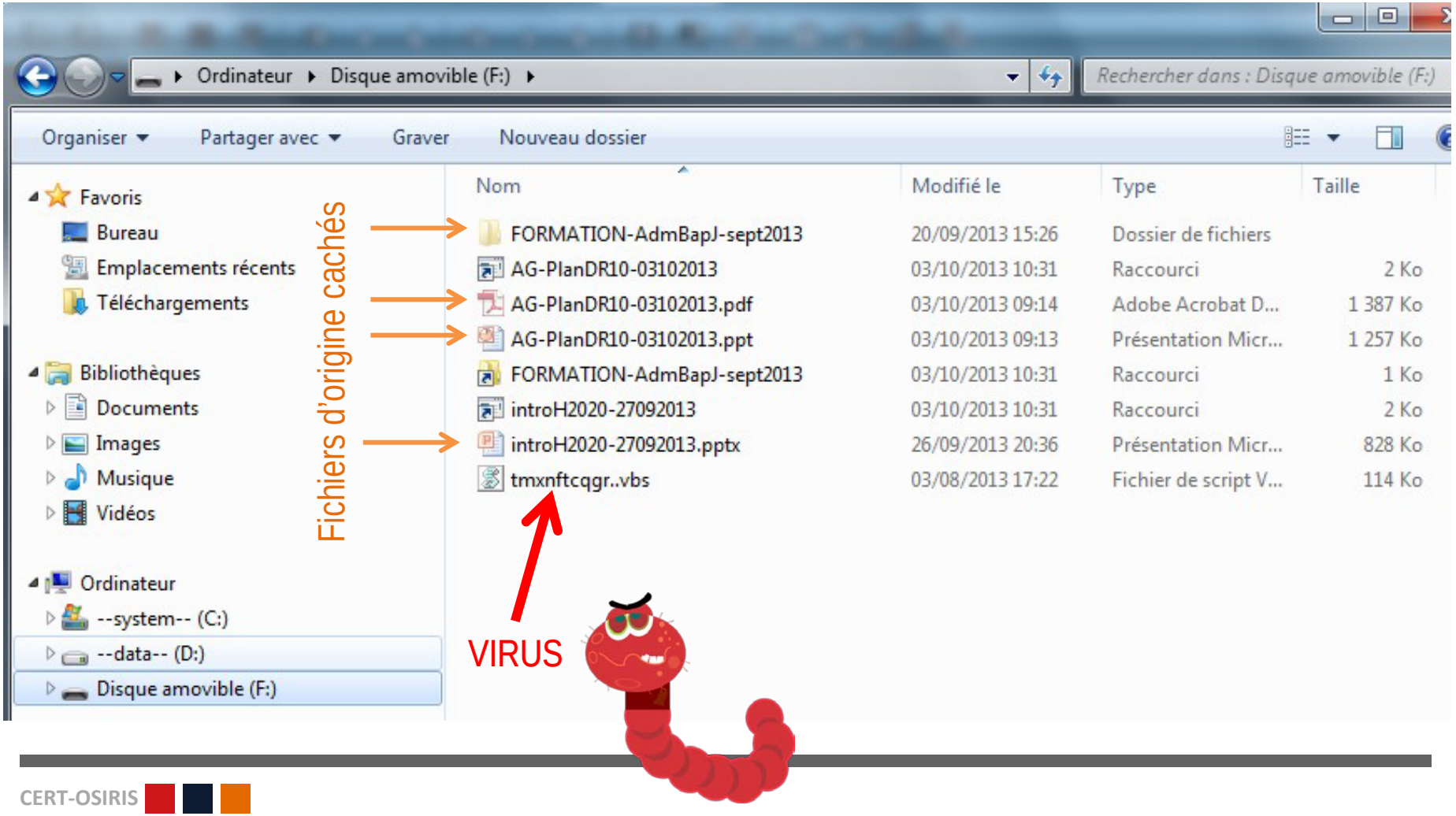
Quand on affiche les « *Propriétés* » du raccourci, on s'aperçoit qu'il lance la commande suivante :

C:\WINDOWS\system32\cmd.exe /c start **tmxnftcqgr..vbs** & start **introH2020-27092013.pptx**&exit

Exécution d'un programme inconnu nommé « *tmxnftcqgr..vbs* » …

… puis ouverture du fichier demandé
=> l'utilisateur ne se rend compte de rien, son fichier s'ouvre comme prévu…

Quand on visualise les fichiers « système » et les fichiers « caché » dans l'explorateur (voir diapo suivante), on découvre d'autre fichiers présents sur la clé USB :



Cible : serveur web (blog)

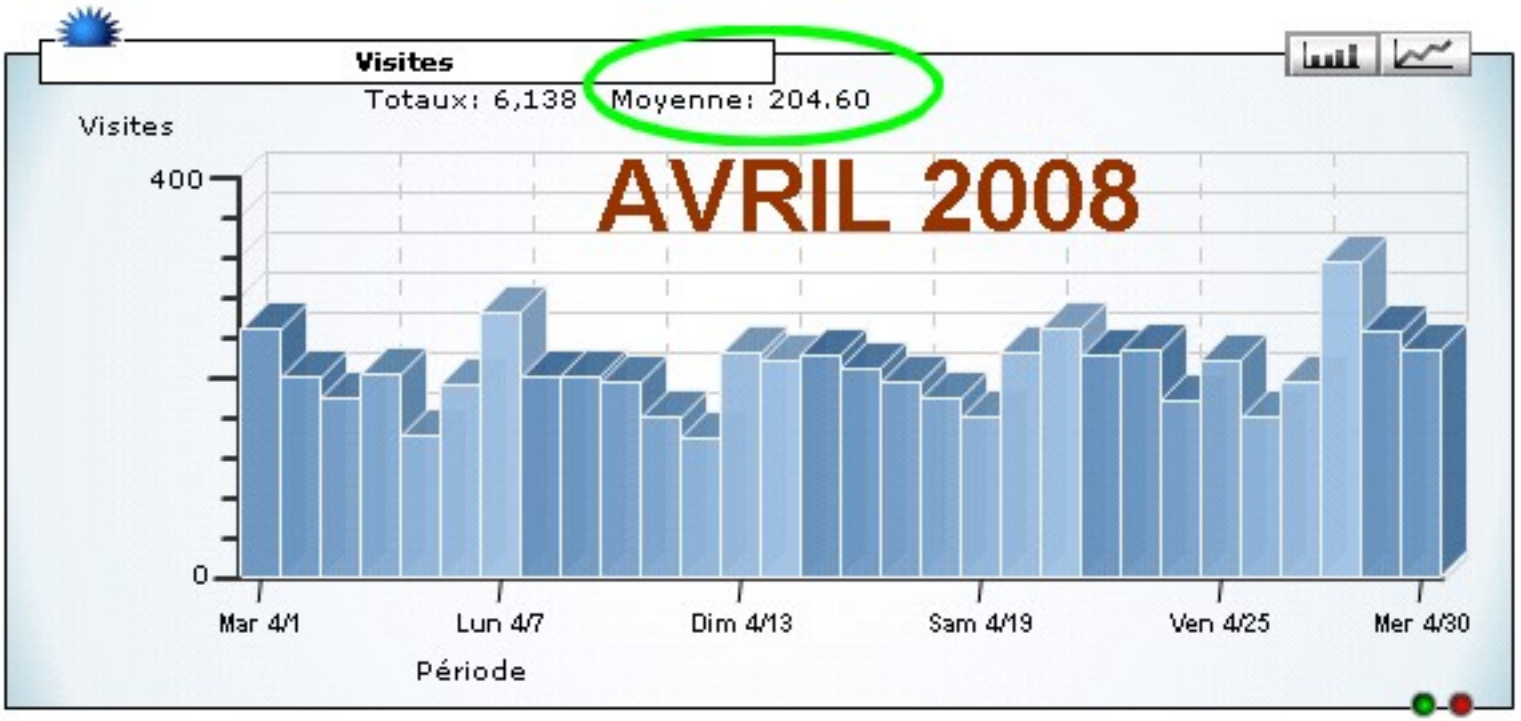
Méthode d'attaque : insertion de multiples commentaires sur le site attaqué contenant des liens vers un site frauduleux

Vulnérabilité exploitée :

Absence de modération sur le site + absence d'un module antispam

ATTAQUE D'UN SITE WEB PAR UN BOTNET

Moyenne de connexions / jour



ATTAQUE D'UN SITE WEB PAR UN BOTNET

Moyenne de connexions / jour

Origines géographiques des connexions

Période: 1/6/2008 - 30/6/2008 — Meilleurs pays

Précédent	Visiteurs	Précédent	Visiteurs	Précédent	Nbr. Affiché	Visiteurs
1. net (Network)	6 951	21. br (Brazil)	197	41. ve (Venezuela)		81
2. com (Commercial)	5 287	22. ru (Russian Federation)	188	42. il (Israel)		72
3. fr (France)	1 908	23. ar (Argentina)	187	43. id (Indonesia)		64
4. de (Germany)	1 627	24. lu (Luxembourg)	178	44. ni (Nicaragua)		63
5. jp (Japan)	1 362	25. tw (Taiwan)	162	45. si (Slovenia)		58
6. pl (Poland)	951	26. ae (United Arab Emirates)	151	46. mx (Mexico)		55
7. edu (Educational)	852	27. hu (Hungary)	145	47. kr (South Korea)		49
8. au (Australia)	753	28. gr (Greece)	145	48. ec (Ecuador)		47
9. org (Non-Profit Organizations)	694	29. no (Norway)	142	49. sk (Slovak Republic)		47
10. it (Italy)	576	30. th (Thailand)	139	50. hk (Hong Kong)		31
11. nl (Netherlands)	524	31. at (Austria)	128	51. be (Belgium)		28
12. ch (Switzerland)	448	32. ee (Estonia)	127	52. my (Malaysia)		26
13. es (Spain)	421	33. cz (Czech Republic)	123	53. tr (Turkey)		25
14. dk (Denmark)	391	34. jo (Jordan)	118	54. md (Moldavia)		5
15. ca (Canada)	369	35. za (South Africa)	112	55. ie (Ireland)		3
16. se (Sweden)	282	36. tv (Tuvalu)	107	56. ro (Romania)		3
17. us (United States)	274	37. nz (New Zealand)	104	57. lv (Latvia)		2
18. ua (Ukraine)	268	38. sa (Saudi Arabia)	97	58. bg (Bulgaria)		1
19. other	227	39. fi (Finland)	95	59. gov (USA Government)		1
20. uk (United Kingdom)	225	40. yu (Yugoslavia)	90			

Atteintes aux droits d'auteurs

TÉLÉCHARGEMENT ILLEGAL

Trafic Peer-to-Peer illégal depuis votre réseau

==========

Bonjour,

Nous avons été averti de la présence sur une machine de votre site d'un fichier sous copyright.

La machine concernée est le :
  130. [redacted] / 130. [redacted]

Vous trouverez, après la signature, une copie de la plainte que nous avons reçue et qui nous a permis de détecter la source.

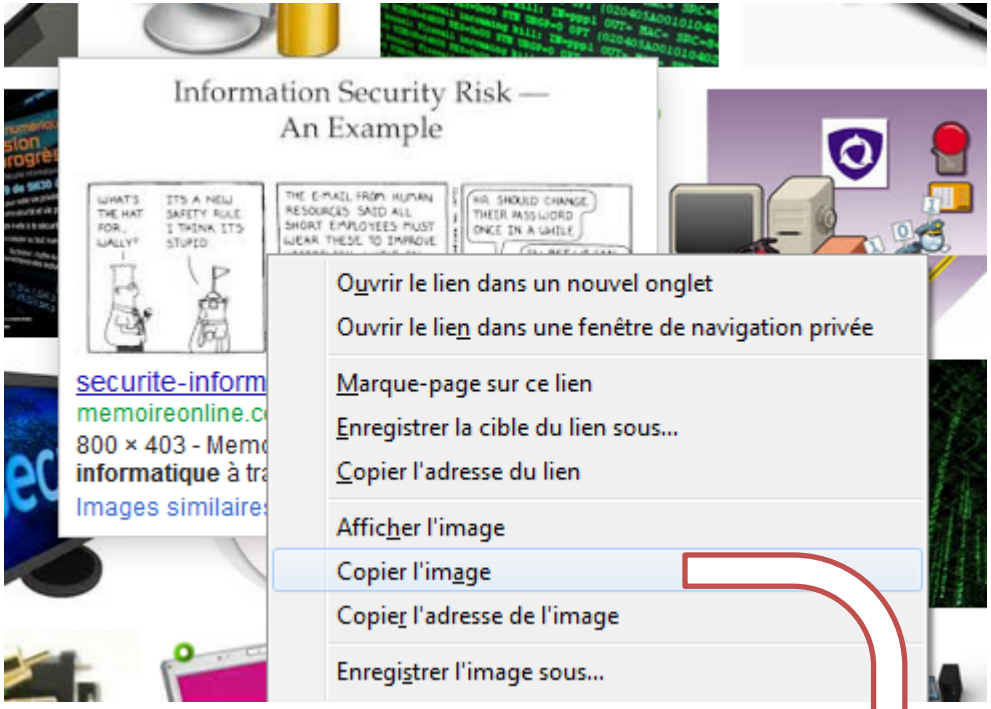
La mise à disposition de fichiers protégés par les droits d'auteurs est interdite par la loi et contraire à la charte RENATER. Nous vous saurions gré de bien vouloir faire fermer ce service. Si cette activité a lieu à l'insu de l'utilisateur, nous vous recommandons une analyse de la machine pour tenter de déterminer les modifications qui ont été apportées au système.

Nous vous serions reconnaissants de bien vouloir accuser réception de ce message et nous tenir informés de la suite donnée à cet incident et de vos découvertes s'il y a lieu.

==========
CERT-RENATER
tel : 01-53-94-20-44
fax : 01-53-94-20-41
23 - 25 Rue Daviel
75013 Paris
email: certsvp@renater.fr
==========

Evidentiary Information:
Notice ID: 22-61697909
Initial Infringement Timestamp: 15 Apr 2013 08:25:44 GMT
Recent Infringement Timestamp: 15 Apr 2013 08:25:44 GMT
Infringers IP Address: 130.[redacted]
Protocol: BitTorrent
Infringed Work: G.I. Joe

UTILISATION ILLEGALE D'UNE ŒUVRE PROTÉGÉE



Bonjour,

Je viens d'avoir connaissance du contenu de votre conférence Cyberespace, le "cyber Far-West" et j'ai eu l'occasion de remarquer que certaines présentations s'inspiraient très fortement du contenu de l'un de mes livres blancs "[redacted] cybercriminalité" et utilisaient les copies d'écrans de ce même ouvrage.

Je n'ai a aucun moment été consulté pour une quelconque utilisation et je ne crois pas également, sauf erreur de ma part, que le nom de ma société ait été cité.

Je vous prie de prendre les mesures nécessaires afin d'évoquer vos sources ou de retirer les contenus se référant à mon ouvrage que j'ai pu retrouver sur plusieurs sites.

[redacted]
Consultante Cybercriminalité