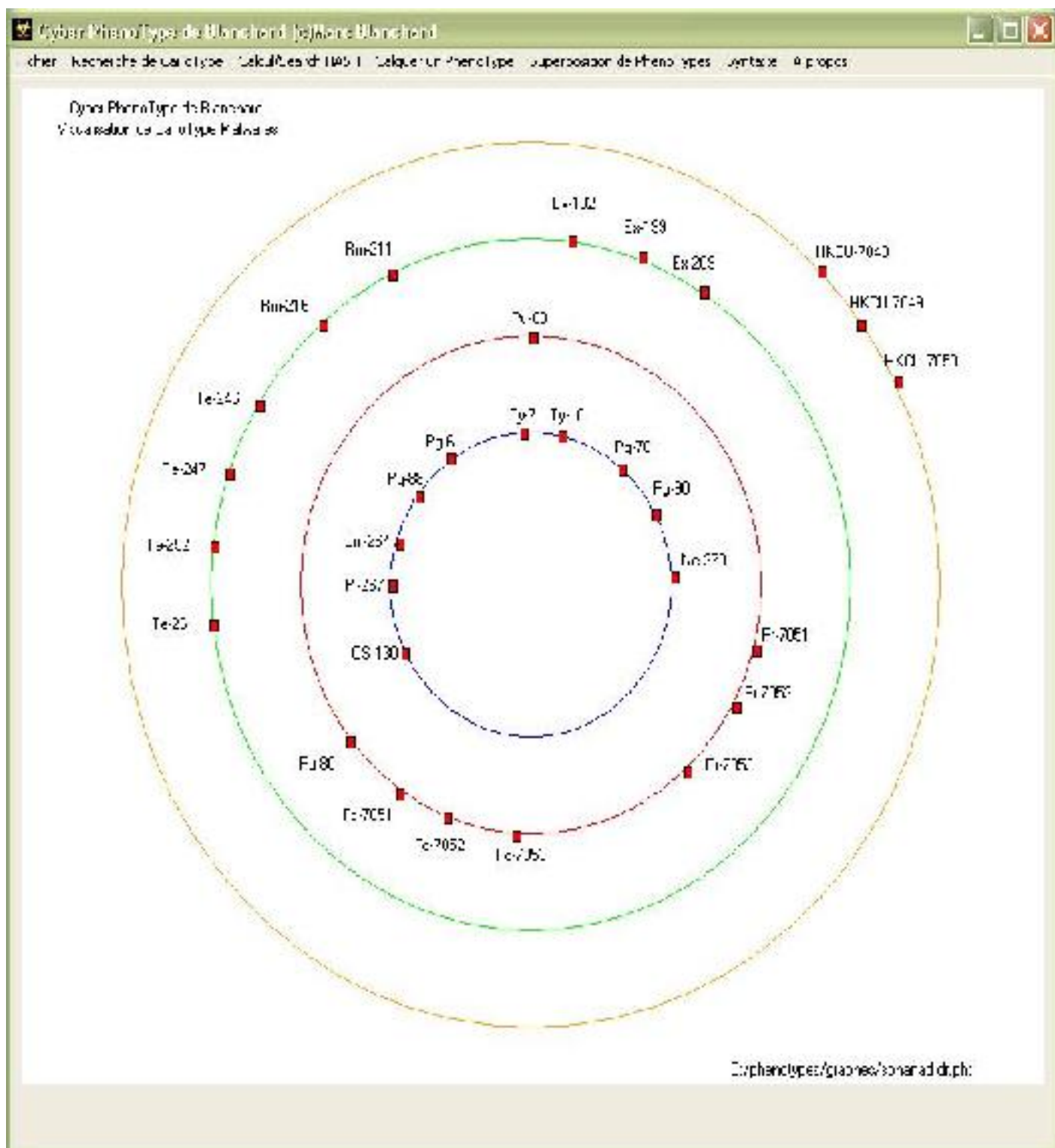


MARC BLANCHARD VIRUS DOCTEUR

PhenoType de Blanchard du malware Sohanad.dr

Ce PhenoType est interessant dans la mesure ou peu de technologies sont embarquees mais montrent bien que les perturbations du systeme...



Voici la description du phénotype Sohanad.dr :

Ty-7; Trojan Downloader

Ty-10; Storm Worm

Pg-61; HTTP

Pg-78;Automatic download

Pg-88;Injection HTTP

Pg-90;Download via other malware

Cm-264;Complexite Niveau 2 (Moyen)

Pi-267;Perception Infection Niveau 2 (Peu percevable pour l'utilisateur)

Ne-270;Niveau d'Emergence Niveau 2 (Moyen)

OS-130;Windows ALL

Pg-88;Injection HTTP

Pg-90;Download via autre Malware

C:\Windows\dc.exe

C:\Windows\SVIQ.EXE

C:\Windows\system\Fun.exe

Ex-182;HTTP

Ex-199;Automatic download

Ex-209;Injection HTTP

Rm-211;Requette malformee HTTP

Rm-216;Requette HTTP normalisee

Te-246;File creation

Te-247;BHO

Te-252;PE

Te-261;Residant en memoire

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\dc =
"C:\Windows\dc.exe"

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\dc2k5 =
"C:\Windows\SVIQ.EXE"

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Fun =
"C:\Windows\System\Fun.exe"

Copyright : Blanchard [Virus Docteur] Marc - 2008-08-17 19:31:22
Creative Commons Deed

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.5

Vous êtes libres :

- * de reproduire, distribuer et communiquer cette création au public

Selon les conditions suivantes :

Paternité. Vous devez citer le nom de l'auteur original.

Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.

Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

* A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

* Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Ceci est le Résumé Explicatif du Code Juridique (la version intégrale du contrat).

<http://creativecommons.org/licenses/by-nc-nd/2.5/>