

MARC BLANCHARD VIRUS DOCTEUR

Poison.63 ..un code sur mesure qui vous espionne via webcam et micro...

Ce code sous forme de fichier exécutable, permet à un pirate d'ouvrir des connexions à distance sur un ordinateur, victime d'avoir exécuter ce code.

Il fait partie de la famille de codes malicieux nommée BackDoor.Poison.63.

L'exécutable étudié n'est qu'en fait une partie du code malicieux, car pour permettre la prise de main à distance, il est nécessaire d'avoir un programme client et un programme serveur.

Le serveur est celui qui s'installe sur l'ordinateur de la victime

Le client est celui qui est installé sur l'ordinateur du pirate

Il contourne les parefeux des postes victimes.

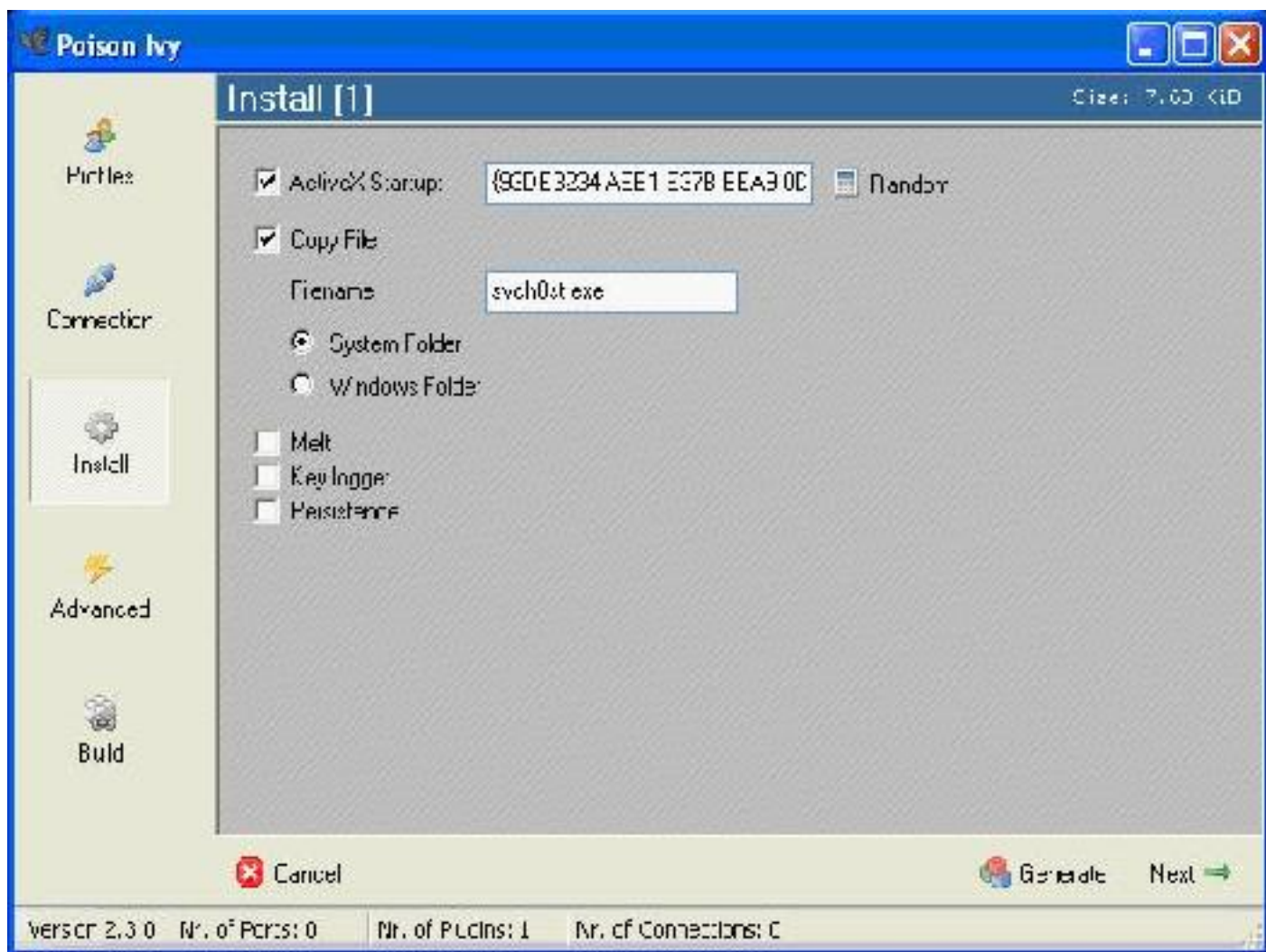
Toutes les connexions, lors des prises de mains a distances sont encryptées avec une technique appelée CAMELLIA en 256 bits.

Le code serveur est développé en langage assembleur (donc très petit environ 5Ko), tandis que le code client est développé en Delphi (langage évolué). Le code serveur s'installe sur les operating systems Windows y compris XP, Vista en 32bits ou 64 bits.

Une technologie de keylogger (écouteur de clavier) a été intégré au code serveur, permettant une écoute quasi-permanente de ce que tape au clavier la victime. Cette technologie permet ainsi de récupérer tous les mots de passes de internet explorer, firefox, msn, etc.

Cette technique a été également ajoutée une possibilité de lancer la **webcam** de la victime de façon invisible et d'enclencher le **microphone** de l'ordinateur, permettant ainsi un espionnage complet.

Il ne faut pas se fier au nom, car le pirate peut générer le nom du programme comme il le souhaite, comme nous le montre la copie écran ci-dessous :



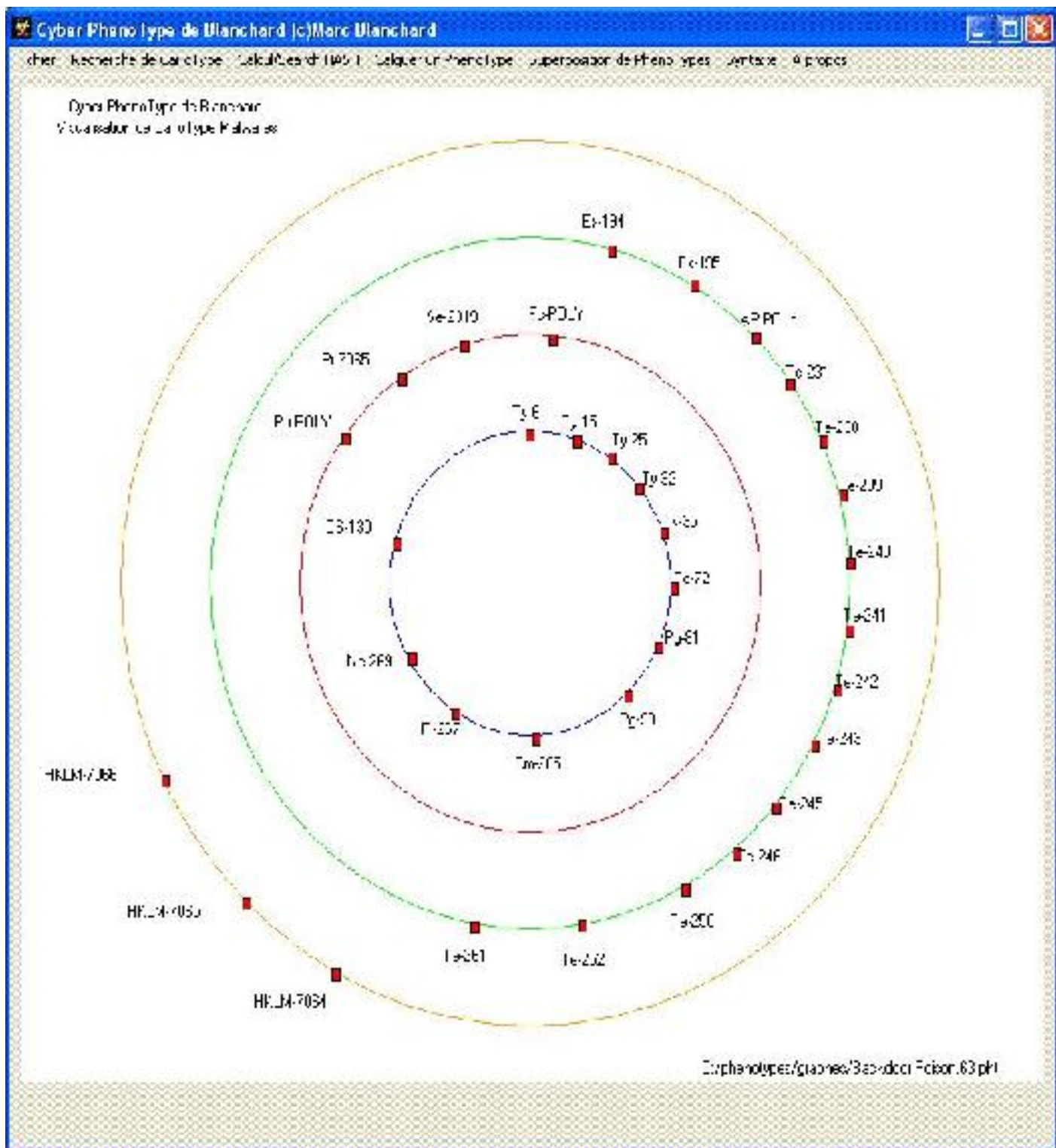
Comme on peut le constater, ce code possède également des actions de polymorphismes (changement d'actions, de code, de méthodes d'implémentation dans le système aléatoire, etc).

Le pirate peut également demander à son code d'utiliser des serveurs proxys y compris les proxys génériques Socks 4 et Socks5 extérieurs ou DNS afin d'être certains de pouvoir accéder au poste de sa victime.

La victime n'a pas besoin d'être administrateur de son poste, simple utilisateur suffit car les implémentations de ce code sont possible dans la registre de l'utilisateur

Ce code est capable d'établir des connexions en tant que redirection de port et d'écouter le trafic sur le réseau local la victime est connecté pour espionnage l'ensemble du parc informatique.

Voici le phénotype de ce code :



Comme on peut le constater, de nombreuses technologies de polymorphies sont utilisées ainsi qu'une multiplication des technologies ont été insérées dans ce code qui se veut très intrusif.

Voici la description du Phénotype :

Ty-6;Backdoor

Ty-15;Keylogger

Ty-25;ACTIVEX

Ty-32;SPYWARE

Ty-35;Drop de fichiers sains par sous appel (ex:svchost.exe virus.exe)

Pg-72;Open Door

Pg-81;Rebond TCPIP LSASS/RPC

Pg-90;Download via other malware

Cm-265;Complexite Niveau 3 (Difficile)

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

Ne-269;Niveau d'Emergence Niveau 1 (Faible)

OS-130;Windows ALL

%SYS%\svchost.exe

Ex-194;Exploit OS

Ex-195;Exploit Application

Te-231;Scan Reseau

Te-238;Autre Server charge sur la victime

Te-239;BOT

Te-240;Modular

Te-241;Stealth

Te-242;Polymorphique

Te-243;Encryptage de donnees

Te-245;MUTEX

Te-246;File creation

Te-250;CPU Analysis

Te-252;PE

Te-261;Residant en memoire

HKLM\SOFTWARE\Microsoft\Active Setup\Installed
Components\{2B81DA45-7941-1AAB-0607-050404050708} "StubPath"

HKLM\SOFTWARE\Microsoft\Active Setup\Installed
Components\{255959D1-EAA2-3478-0804-030805050803} "StubPath" data:
C:\WINDOWS\System32\svchost.exe

Nota: svchost.exe dans cette clef peut changer en fonction de la volonté du pirate.

HKLM\SOFTWARE\Microsoft\Active Setup\Installed
Components\{112B7F82-1892-E4D0-0602-070704020806} "StubPath"

Copyright : Blanchard [Virus Docteur] Marc - 2009-05-27 17:41:53
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/>