

# MARC BLANCHARD VIRUS DOCTEUR

## Phenotype de Blanchard du malware Renos.aco

Voici ci-dessous le phénotype du malware Renos.aco qui est un storm worm utilisant plusieurs techniques.

Il se telecharge automatiquement via des sites webs publiques contamines par des ajouts de IFRAME, pour enfin pointer sur des serveurs hebergeurs du code malicieux Renos.



Ty-36;Disable System Restore

Ty-3;Worm

Commande Non Documentee dans Base de connaissances Cariotypes de Blanchard  
(marc.blanchard@viruslab.ath.cx)

Ty-4;Virus

OS-130;Windows ALL

Pg-61;HTTP

Pg-78;Automatic download

Pg-84;AUTORUN

Pg-90;Download via other malware

%System%\lphc3pgj0e3ct.exe

%System%\blphc3pgj0e3ct.scr

%System%\lphc3pgj0e3ct.exe

%System%\blphc3pgj0e3ct.scr

%System%\lphc3pgj0e3ct.exe

%System%\blphc3pgj0e3ct.scr

%System%\lphc3pgj0e3ct.bmp

Ex-182;HTTP

Ex-199;Automatic download

Ex-205;AUTORUN

Rm-216;Requette HTTP normalisee

%System%\lphc3pgj0e3ct.exe

%System%\blphc3pgj0e3ct.scr

%System%\lphc3pgj0e3ct.bmp

Te-246;File creation

Te-249;Autorun

Te-251;desktop wallpaper change

Te-252;PE

Te-258;scr

Te-261;Residant en memoire

Te-262;Residant en memoire en mode sans echec

HKLM\SYSTEM\CurrentControlSet\Services\sr\Parameters\FirstRun =  
"0" HKLM\SYSTEM\CurrentControlSet\Services\sr\Start = "0"

HKLM\SYSTEM\CurrentControlSet\Services\sr\ImagePath = "\System32\DRIVERS\sr.sys"

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\DisableSR = "0"

HKLM\SOFTWARE\Microsoft\Software Notifier

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\lphc3pgj0e3ct

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoDispBackgroundPage =  
"1"

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoDispScrSavPage = "1"

HKCU\Software\Sysinternals\Bluescreen Screen Saver

HKCU\Control Panel\Colors\Background = "0 0 255"

HKCU\Control Panel\Desktop\ConvertedWallpaper = "%System%\phc3pgj0e3ct.bmp"

HKCU\Control Panel\Desktop\ScreenSaveActive = "1"

HKCU\Control Panel\Desktop\SCRNSAVE.EXE = "%System%\blphc3pgj0e3ct.scr"

HKCU\Control Panel\Desktop\TileWallpaper = "0"

HKCU\Control Panel\Desktop\Wallpaper = "%System%\phc3pgj0e3ct.bmp"

HKCU\Software\Microsoft\Internet Explorer\Desktop\Components\GeneralFlags = "0"

Copyright : Blanchard [Virus Docteur] Marc - 2008-07-30 20:05:10  
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/>