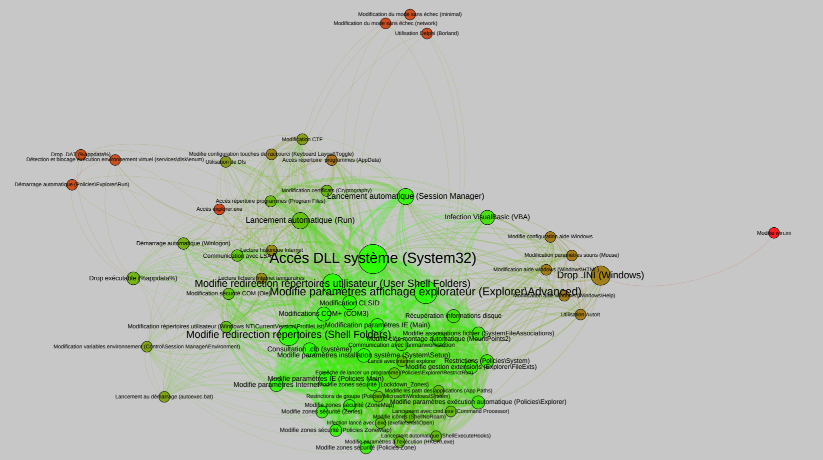

Modification du mode sans échec (minimal)
Modification du mode sans échec (network)
Utilisation Delphi (Borland)
Modification CTF
Drop .DAT (%appdata%)
Détection et blocage exécution environnement virtuel (services\disk\enum)
Modifie configuration touches de raccourci (Keyboard Layout\Toggle)
Utilisation de Dfs
Accés répertoire programmes (AppData)
Démarrage automatique (Policies\Explorer\Run)
Modification certificats (Cryptography)
Lancement automatique (Session Manager)
Accés répertoire programmes (Program Files)
Accés explorer.exe
Lancement automatique (Run)
Infection VisualBasic (VBA)
Modifie configuration aide Windows
Modification paramètres souris (Mouse)
Modifie win.ini
Démarrage automatique (Winlogon)
Lecture historique Internet
Communication avec LSA
Accés DLL système (System32)
Modification aide windows (Windows\HTML)
Drop .INI (Windows)
Drop exécutable (%appdata%)
Lecture fichiers Internet temporaires
Modifie redirection répertoires utilisateur (User Shell Folders)
Modifie paramètres affichage explorateur (Explorer\Advanced)
Modification sécurité COM (Ole)
Modification aide windows (Windows\Help)
Modification CLSID
Modifications COM+ (COM3)
Récupération informations disque
Utilisation AutoIt
Modification répertoires utilisateur (Windows NT\CurrentVersion\ProfileList)
Modification paramètres IE (Main)
Modifie redirection répertoires (Shell Folders)
Modifie associations fichier (SystemFileAssociations)
Modifie clés montage automatique (MountPoints2)
Modification variables environnement (Control\Session Manager\Environment)
Communication avec lanmanworkstation
Consultation .clb (système)
Modifie paramètres installation système (System\Setup)
Lancé avec internet explorer
Restrictions (Policies\System)
Modifie gestion extensions (Explorer\FileExts)
Empêche de lancer un programme (Policies\Explorer\RestrictRun)
Modifie paramètres IE (Policies Main)
Modifie paramètres Internet
Modifie zones sécurité (Lockdown_Zones)
Lancement au démarrage (autoexec.bat)
Modifie les path des applications (App Paths)
Restrictions de groupe (Policies\Microsoft\Windows\System)
Modifie paramètres exécution automatique (Policies\Explorer)
Modifie zones sécurité (ZoneMap)
Lancement avec cmd.exe (Command Processor)
Modifie zones sécurité (Zones)
Modifie icônes (ShellNoRoam)
Infection lancé avec .exe (exefile\shell\Open)
Modifie zones sécurité (Policies ZoneMap)
Lancement automatique (ShellExecuteHooks)
Modifie paramètres à l'exécution (HKCR\.exe)
Modifie zones sécurité (Policies Zone)