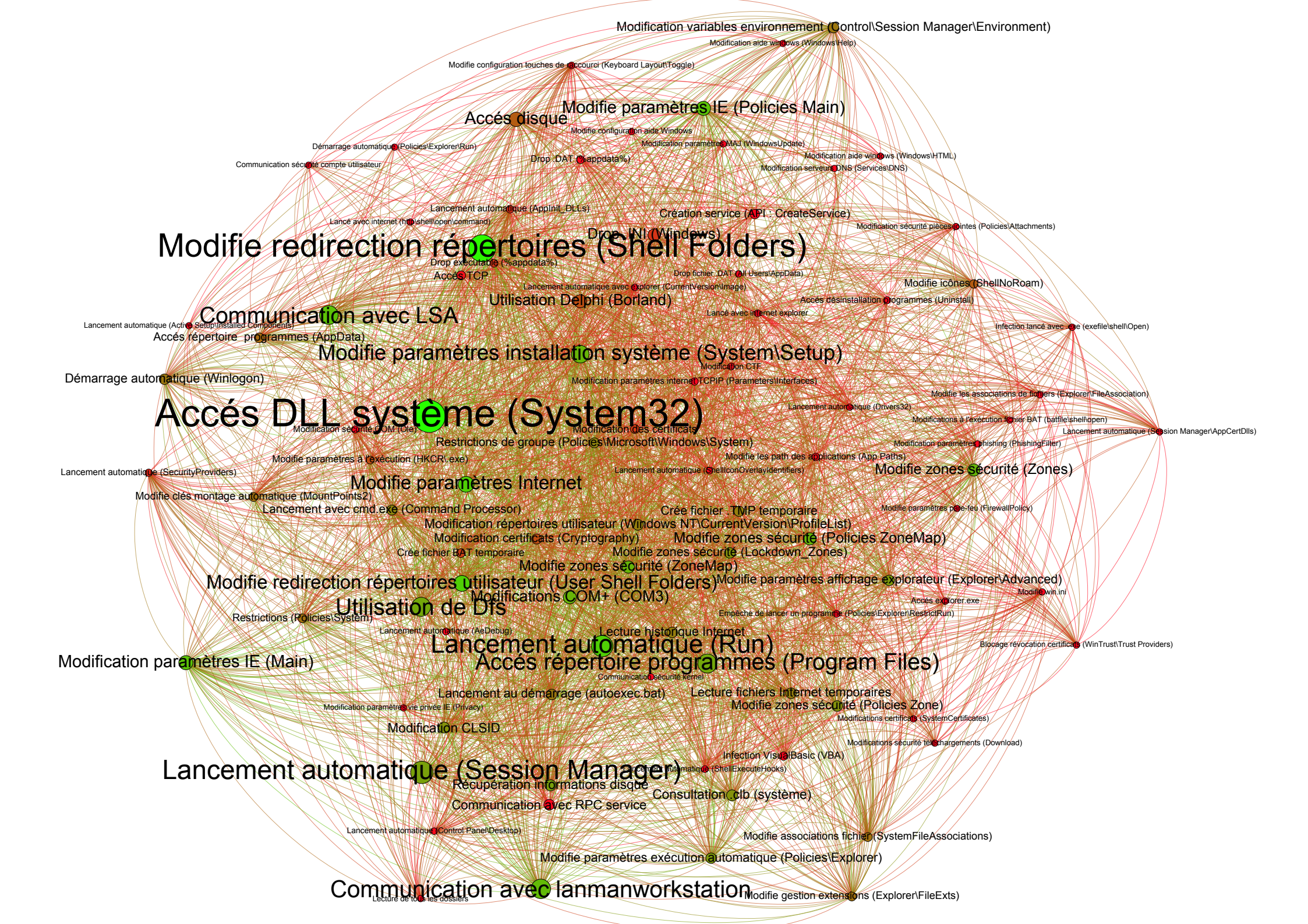
Modification variables environnement (Control\Session Manager\Environment)
Modification aide windows (Windows\Help)
Modifie configuration touches de raccourci (Keyboard Layout\Toggle)
Modifie paramètres IE (Policies Main)
Accès disque
Modifie configuration aide Windows
Démarrage automatique (Policies\Explorer\Run)
Modification paramètres MAJ (WindowsUpdate)
Drop .DAT (%appdata%)
Modification aide windows (Windows\HTML)
Communication sécurité compte utilisateur
Modification serveurs DNS (Services\DNS)
Lancement automatique (AppInit_DLLs)
Création service (API : CreateService)
Lancé avec internet (http\shell\open\command)
Modification sécurité pièces jointes (Policies\Attachments)
Drop .INI (Windows)
Modifie redirection répertoires (Shell Folders)
Drop exécutable (%appdata%)
Accès TCP
Drop fichier .DAT (All Users\AppData)
Lancement automatique avec explorer (CurrentVersion\Image)
Modifie icônes (ShellNoRoam)
Utilisation Delphi (Borland)
Accès désinstallation programmes (Uninstall)
Communication avec LSA
Lancé avec internet explorer
Lancement automatique (ActiveSetup\Installed Components)
Infection lancé avec exe (exefile\shell\Open)
Accès répertoire programmes (AppData)
Modifie paramètres installation système (System\Setup)
Modification CTF
Démarrage automatique (Winlogon)
Modification paramètres internet TCPIP (Parameters\Interfaces)
Modifie les associations de fichiers (Explorer\FileAssociation)
Accès DLL système (System32)
Lancement automatique (Drivers32)
Modifications à l'exécution fichier BAT (batfile\shell\open)
Modification sécurité (COM TOle)
Modification des certificats
Lancement automatique (Session Manager\AppCertDlls)
Restrictions de groupe (Policies\Microsoft\Windows\System)
Modification paramètres phishing (PhishingFilter)
Modifie paramètres à l'exécution (HKCR\.exe)
Modifie les path des applications (App Paths)
Lancement automatique (SecurityProviders)
Lancement automatique (ShellIconOverlayIdentifiers)
Modifie zones sécurité (Zones)
Modifie paramètres Internet
Modifie clés montage automatique (MountPoints2)
Lancement avec cmd.exe (Command Processor)
Crée fichier .TMP temporaire
Modifie paramètres pare-feu (FirewallPolicy)
Modification répertoires utilisateur (Windows NT\CurrentVersion\ProfileList)
Modification certificats (Cryptography)
Modifie zones sécurité (Policies ZoneMap)
Crée fichier BAT temporaire
Modifie zones sécurité (Lockdown_Zones)
Modifie zones sécurité (ZoneMap)
Modifie redirection répertoires utilisateur (User Shell Folders)
Modifie paramètres affichage explorateur (Explorer\Advanced)
Modifications COM+ (COM3)
Modifie win.ini
Utilisation de Dfs
Accès explorer.exe
Restrictions (Policies\System)
Empêche de lancer un programme (Policies\Explorer\RestrictRun)
Lancement automatique (AeDebug)
Lecture historique Internet
Lancement automatique (Run)
Blocage révocation certificats (WinTrust\Trust Providers)
Modification paramètres IE (Main)
Accès répertoire programmes (Program Files)
Communication sécurité kernel
Lancement au démarrage (autoexec.bat)
Lecture fichiers Internet temporaires
Modification paramètres vie privée IE (Privacy)
Modifie zones sécurité (Policies Zone)
Modifications certificats (SystemCertificates)
Modification CLSID
Modifications sécurité téléchargements (Download)
Infection VisualBasic (VBA)
Lancement automatique (Session Manager)
Lancement automatique (ShellExecuteHooks)
Récupération informations disque
Consultation .clb (système)
Communication avec RPC service
Lancement automatique (Control Panel\Desktop)
Modifie associations fichier (SystemFileAssociations)
Modifie paramètres exécution automatique (Policies\Explorer)
Communication avec lanmanworkstation
Lecture de tous les dossiers
Modifie gestion extensions (Explorer\FileExts)