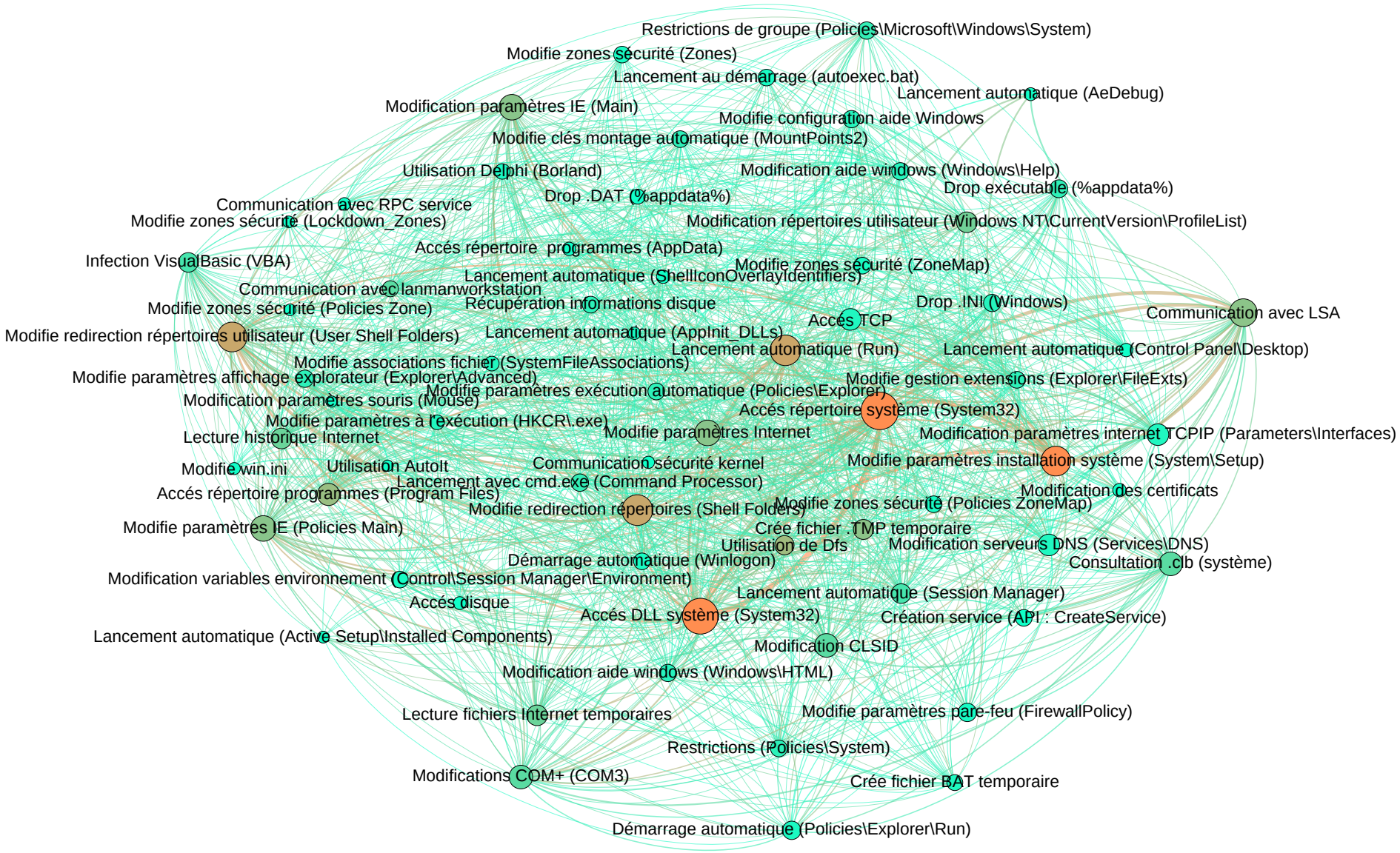
Restrictions de groupe (Policies\Microsoft\Windows\System)
Modifie zones sécurité (Zones)
Lancement au démarrage (autoexec.bat)
Lancement automatique (AeDebug)
Modification paramètres IE (Main)
Modifie configuration aide Windows
Modifie clés montage automatique (MountPoints2)
Utilisation Delphi (Borland)
Modification aide windows (Windows\Help)
Drop exécutable (%appdata%)
Drop .DAT (%appdata%)
Communication avec RPC service
Modifie zones sécurité (Lockdown_Zones)
Modification répertoires utilisateur (Windows NT\CurrentVersion\ProfileList)
Accés répertoire programmes (AppData)
Infection VisualBasic (VBA)
Modifie zones sécurité (ZoneMap)
Lancement automatique (ShellIconOverlayIdentifiers)
Communication avec lanmanworkstation
Modifie zones sécurité (Policies Zone)
Récupération informations disque
Drop .INI (Windows)
Communication avec LSA
Accés TCP
Modifie redirection répertoires utilisateur (User Shell Folders)
Lancement automatique (AppInit_DLLs)
Lancement automatique (Run)
Lancement automatique (Control Panel\Desktop)
Modifie associations fichier (SystemFileAssociations)
Modifie paramètres affichage explorateur (Explorer\Advanced)
Modifie gestion extensions (Explorer\FileExts)
Modifie paramètres exécution automatique (Policies\Explorer)
Modification paramètres souris (Mouse)
Accés répertoire système (System32)
Modifie paramètres à l'exécution (HKCR\.exe)
Modifie paramètres Internet
Modification paramètres internet TCPIP (Parameters\Interfaces)
Lecture historique Internet
Modifie win.ini
Utilisation AutoIt
Communication sécurité kernel
Modifie paramètres installation système (System\Setup)
Lancement avec cmd.exe (Command Processor)
Modification des certificats
Accés répertoire programmes (Program Files)
Modifie zones sécurité (Policies ZoneMap)
Modifie redirection répertoires (Shell Folders)
Modifie paramètres IE (Policies Main)
Crée fichier .TMP temporaire
Utilisation de Dfs
Modification serveurs DNS (Services\DNS)
Démarrage automatique (Winlogon)
Consultation .clb (système)
Modification variables environnement (Control\Session Manager\Environment)
Lancement automatique (Session Manager)
Accés disque
Accés DLL système (System32)
Création service (API : CreateService)
Lancement automatique (Active Setup\Installed Components)
Modification CLSID
Modification aide windows (Windows\HTML)
Lecture fichiers Internet temporaires
Modifie paramètres pare-feu (FirewallPolicy)
Restrictions (Policies\System)
Modifications COM+ (COM3)
Crée fichier BAT temporaire
Démarrage automatique (Policies\Explorer\Run)