Appendix 4 – Activity Designations in the Event Chain

- New Process
- Autostart
- New Service
- Code Injection
- Keyboard Access
- Code Injection Access
- Access to Autostart Registry
- Extraction of Executable File
- Internet Connection Established
- Waiting for Incoming Connection
- Local Network Connection
- Internet Connection Attempt (Failed)
- Moving an Important File
- Opening Another Executable File
- Writing to Another Executable File (Modification)
- Infecting Another Executable File (Code Injection into File)
- Opening Multiple Executable Files

- Writing to Multiple Executable Files (Mass Modification)
- Infecting Multiple Executable Files (Mass Code Injection into Files)
- Creating a New System Task for Task Scheduler
- Setting an Executable File for Autostart (via Task Scheduler)
- Suspicious Process Invaded a LEGITIMATE Process (DLL Injection)
- Untrusted Process Delays Execution (Possibly to Evade Detection)
- Low-Level Disk Access
- Low-Level Access to Multiple Disks
- Low-Level Disk Management
- Registry Key Monitoring
- Windows Installation Identification
- Unique Computer Identification
- Reads Internet Settings
- Attempting Multiple Internet Connections
- Low-Level Disk Write
- Deleting Another Executable File
- Deleting Multiple Executable Files (Mass Deletion)
- Opening an Important File
- Opening Multiple Important Files
- Modifying an Important File
- Modifying Multiple Important Files

- Deleting an Important File

- Deleting Multiple Important Files

Edit this page