

Entity

Process

Dll

Registry Key

File

IP:Port

Relation

- ✓ Read
- ✓ Write
- ✓ Delete
- ✓ Access
- ✓ Create
- ✓ RegOpenKey
- ✓ RegQueryKey
- ✓ RegSetValue
- ✓ RegDelValue
- ✓ RegAddValue
- ✓ Connect
- ✓ load

Basic Event

Create, write, read, delete

Create, Access

Process

load

connect

File

Dll

IP:Port

Registry
Key

RegOpenKey
RegQueryKey
RegSetValue
RegDelValue
RegAddValue

Temporal Event

e1: <Src, Rel, Dst, time1>

e2:<Src, Rel, Dst, time2>

e3:<Src, Rel, Dst, time3>