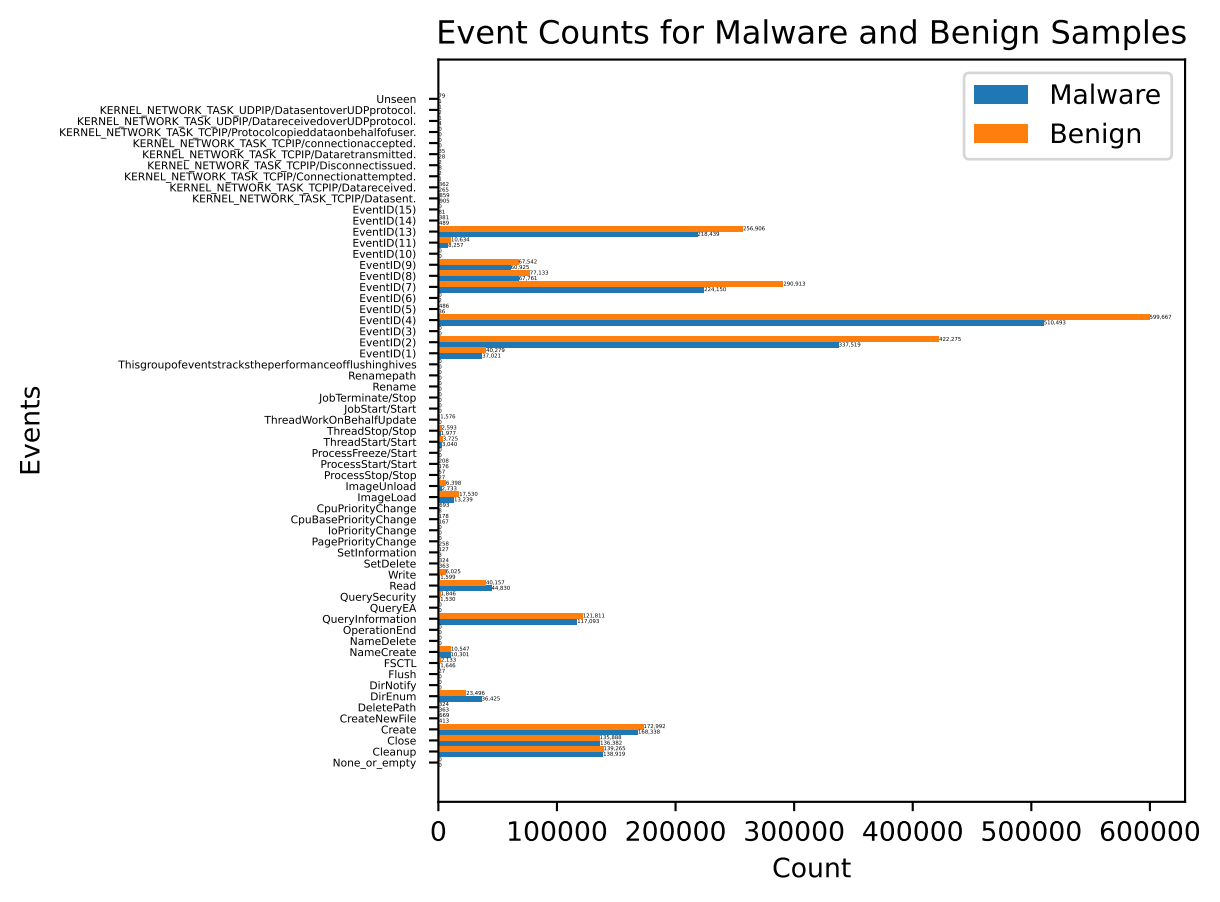
Event Counts for Malware and Benign Samples
Malware
Benign
Events
Count
Unseen
KERNEL_NETWORK_TASK_UDPIP/DatasentoverUDPprotocol.
KERNEL_NETWORK_TASK_UDPIP/DatareceivedoverUDPprotocol.
KERNEL_NETWORK_TASK_TCPIP/Protocolcopieddataonbehalfofuser.
KERNEL_NETWORK_TASK_TCPIP/connectionaccepted.
KERNEL_NETWORK_TASK_TCPIP/Dataretransmitted.
KERNEL_NETWORK_TASK_TCPIP/Disconnectissued.
KERNEL_NETWORK_TASK_TCPIP/Connectionattempted.
KERNEL_NETWORK_TASK_TCPIP/Datareceived.
KERNEL_NETWORK_TASK_TCPIP/Datasent.
EventID(15)
EventID(14)
EventID(13)
EventID(11)
EventID(10)
EventID(9)
EventID(8)
EventID(7)
EventID(6)
EventID(5)
EventID(4)
EventID(3)
EventID(2)
EventID(1)
Thisgroupofeventstracktheperformanceofflushinghives
Renamepath
Rename
JobTerminate/Stop
JobStart/Start
ThreadWorkOnBehalfUpdate
ThreadStop/Stop
ThreadStart/Start
ProcessFreeze/Start
ProcessStart/Start
ProcessStop/Stop
ImageUnload
ImageLoad
CpuPriorityChange
CpuBasePriorityChange
IoPriorityChange
PagePriorityChange
SetInformation
SetDelete
Write
Read
QuerySecurity
QueryEA
QueryInformation
OperationEnd
NameDelete
NameCreate
FSCTL
Flush
DirNotify
DirEnum
DeletePath
CreateNewFile
Create
Close
Cleanup
None_or_empty
0
100000
200000
300000
400000
500000
600000