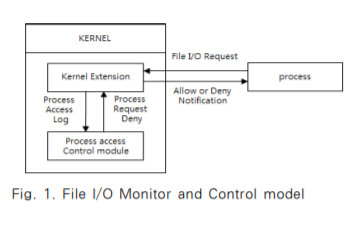
1.커널을 이용한 파일 I/O 모니터링 및 제어 모델

파일 처리를 요청한 프로세스가 파일내용을 변경하기 위해서는 반드시 파일을 열어야 하며, 커널은 파일을 열었을 때 발생하는 신호를 커널 모듈에 전달함으로써 해당 프로세스가 파일에 접근한 시간 및 파일경로를 커널 모듈에서 확인할 수 있다.

pid값을 통하여 각각의 프로세스를 식별 가능하며, 이를 이용하여 특정 프로세스의 파일접근을 제어할 수 있다

파일 I/O 모니터링 모델은 정보 송수신 모델로부터 받은 정보를 이용해 랜섬웨어의 프로세스로 인지하고 해당 프로세스의 파일접근권한을 차단한다.



2.파일 접근정보 송수신 모델

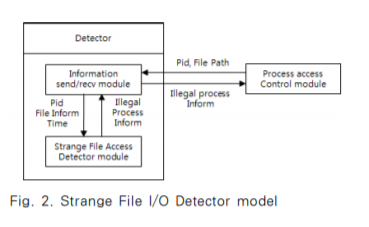
차단해야 할 프로세스에 대한 정보와 파일 처리 요청에 대한 정보를 파일 I/O 모니터링 및 제어모델과 공유한다

이 정보는 소켓을 이용해 유저영역에서 동작하는 Detector와 주고받는다.

소켓으로 송수신하는 메세지의 내용은 파일 I/O 모니터링 및 제어모델이 특정한 프로세스가 파일에 접근할 경우 탐지했던 pid와 시간, 파일경로가 있다. 소켓은 해당 정보를 보관하고 있다가 Detector와의 연결이 확인되면 Detector에게 메세지를 송신한다.

Detector는 수신한 메세지를 열어서 특정 파일에 접근하려는 프로세스를 확인하고 접근이 정상적인지 비정상적인지를 판단한다.

3.비정상적 파일접근 탐지 모델(Detector)



3.2.1 파일 접근 정보 수신 및 파일 접근 명령 송신 모델

특정 프로세스가 커널에게 파일 접근을 요청할 경우 파일 I/O 모니터링 및 제어모델은 관련 정보를 담은 메세지를 Detector에게 송신한다

커널에서 작동하는 파일정보 송수신 모델은 소켓을 가지고 있다.

이 소켓을 이용하여 사용자 레벨에서 작동하는 Detector의 파일정보 송수신 모델이 가지고 있는 소켓에게 정보 메세지를 송신한다.

이 모델은 지속적으로 파일 접근정보 메세지를 수신하고 메세지 내용을 이상징후 탐지모델과 공유한다. 리시브(recv)함수를 통해 수신한 이 정보 메세지는 정보를 문자열타입의 변수를 이용하여 보관한다. 메세지에 담을 정보의 최대 길이는 1024바이트로 설정했다.

정보 메세지는 pid, 파일접근시간, 파일경로가 들어있다.

윈도우 운영체제 같은 경우에는 폴더 및 파일의 전체 경로길이를 담는 변수의 최대 길이는 260바이트이다

Detector의 정보 송수신 모듈이 수신한 메세지는 텍스트파일에 수신한 내용을 저장한다. 텍스트파일에 저장하지 않고 실시간으로 메세지를 확인해서 비정상적인 파일접근을 판단할 수도 있지만 로그를 남겨서 파일 접근판단에 대한 근거자료를 가지고 있는 것이 추후 에러가 발생한 경우에 더 능동적으로 대처할 수 있다.

커널의 정보 송수신 모델이 메세지를 송신하는 시점을 모르기 때문에 Detector의 정보 송수신 모델은 계속 대기하면서 메세지를 수신할 때마다 텍스트파일에 메세지를 추가한다.

3.2.2 이상징후 탐지 모델

PID, 파일 접근 시간, 파일의 전체 경로에 대한 정보를 구조체 형태로 저장하고 있으며, 이를 이용할 경우 빠른 검색 및 비교가 가능하다.

탐지 조건

일반적인 프로세스에서도 요청하기 때문에 단순히 한 번의 파일 I/O 요청만으로는 비정상적인 접근을 판단할 수 없다. 이상징후 탐지 모델은 가장 최근에 저장된 10개의 메세지를 확인한다.

10개의 메시지 중에서 동일한 프로세스가 5개 이상이면 동일한 프로세스의 메세지들을 가져온다. 가져온 메시지 중에서 가장 최근의 메세지와 가장 오래된 메세지의 시간차이가 0.01초 이하일 경우에 비정상적인 접근으로 판단한다.

비정상적인 파일접근으로 판단할 경우, 정보 송수신 모델과 정보를 공유하고, 이 정보를 담은 메세지를 커널의 정보 송수신 모델에 전송한다. 메세지를 수신하면 해당 정보를 파일 I/O 모니터링 및 제어 모델이 확인하고 해당 프로세스의 파일 접근권한을 차단한다.

이상징후 탐지 모델은 pid를 기준으로 비정상적으로 파일을 접근한 프로세스의 명령어 또는 경로를 확인하고 pid와 관련 정보를 사용자에게 알려준다.

이상징후 모델은 비정상적으로 파일에 접근하는 프로세스를 사용자에게 알리고 차단여부를 묻는 역할을 한다. 사용자가 차단을 원하지 않은 경우 이상징후 탐지모델은 정보 송수신 모델에게 차단초기화 메시지 송신을 요청한다. 이 메세지를 커널 영역의 정보 송수신 모델이 수신하면 파일 I/O 모니터링 탐지 및 제어 모델과 메시지 내용을 공유하며, 파일 I/O 모니터링 탐지 및 제어 모델은 차단하고 있던 프로세스의 파일접근 권한을 원래 상태로 되돌려 놓는다.