컴퓨터 포렌식 도구를 이용해 가치있는 증거를 수집하자

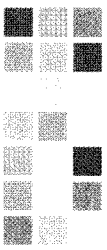
컴퓨터 포렌식은 사고와 관련된 시스템을 조사해 범죄에 이용된 증거를 수집해 입증하는 분야이다. 국내에서는 아직 증거수집에 대한 프로세스가 공개되지 않고 있는데, 그 이유는 일반기업에서 해당 업무를 수행할 권한이 없기 때문이다. 이에 반해 해외의 경우, 해당 프로세스에 대한 'Rfc3227(http://www.ietf.org/rfc/rfc3227.txt)' 지침이 마련돼 있으며, 이것은 IETF(The Internet Engineering Task Force)의 BCP(Best Current Practice)로 등록돼 있는 표준화 절차다. 이는 증거수집 및 보관이라는 업무가 반드시 사법적인 권한을 가지고 수행해야 하는 업무가 아니라, 사고가 발생한 시스템에 대한 원인을 파악하고 재발 방지를 위한 목적을 가지고 있기 때문이다. 위와 같은 목적으로 국내에서도 딱딱한 컴퓨터 포렌식이 아닌 현업에게 활용 가능한 컴퓨터 포렌식에 대해 정리해 보고자 한다.

글 **최재규** | 한국통신인터넷기술 부장

일반 기업의 경우, 보안 사고에 대한 증거물 수집과 증거보관 프로세스는 공개되어있지 않다. 그러나 그 필요성 및 중요성에 대해서 충분히 인지하고 있으며, 실제 일부 IDC에서는 포렌식 서비스를 상품으로 만들어 판매하고 있다. 포렌식에 대한 관심 정도는 시장규모로도 파악이 가능한데, Socha Consulting에 따르면 미국의 포렌식 시장은 2006년 19억 달러 규모로 파악됐으며 오는 2010년까지 약 41억달러 규모로 확대될 것으로 예상된다.

포렌식 증거의 가치는 수집한 증거가 실제 보안사고를 유발시킨 정황을 증명할 수 있느냐와 증거의 무결성이 훼손되어있지 않았음이 입증되어야 증거로서 가치를 지니게 된다. 이와 같은 기준을 만족시키기 위해서는 어떻게 해야 할까.

IETF(The Internet Engineering Task Force)가 발표한 증거 수집 절차인 Rfc(Reguest for comment)3227은 시스템 관리자에게 시스템 보안사고에 관한 증거물 수집과 파일보관에 관한 지침을 제공하기 위한 것으로, 이를 통해 정확한 절차에 의해 수집된 증거가 공격자를 체포하는데 도움을 제공할 뿐만 아니라, 법정 증거로 인정받게 하는데 그 목적이 있다. Rfc3227이 의미하는 증거수집 과정과 운영지침을 살펴보면 다음과 같다.



▶ 기업/기관의 보안 정책에 기반하고, 사고처리나 법집행을 하한 인원을 고용하라.

▶ 가능한 모든 자료(Picture)를 수집하라.

▶ 날짜와 시간을 포함해 자세히 기록하라. 이때 가능하다면 자동으로 기록할 수 있는 장치를 사용해야 한다(예를 들어, 유닉스에서 스크립트(script) 프로그램의 사용. 이 프로그램의 출력이 동일한 디스크(증거물 디스크)에 생기지 않도록 조심해야 한다).

▷ 시스템 시간과 UTC(Universal Time Coordinated)와의 차이를 기록한다. 타임스탬프(Timestamp)를 남길 때마다 UTC를 사용했는지 로컬타임을 사용했는지 표시한다.

▶ 관리자가 언제 어떤 행동을 취했는지 증명(증명하는 시기는 몇 년 후가 될 수 있다)할 수 있도록 준비해라.

▷ 수집과정에서 데이터의 변형을 최소화 하라. 이것은 파일의 내용뿐 아니라 파일이나 디렉토리의 접속시간(Access Time)도 포함한다.

▶ 변경에 대한 외부 수단을 제거하라.

▷ 수집을 할 것인가 분석을 할 것인가 선택해야 한다면 먼저 수집을 하라.

▶ 절차를 계획할 때는 실행 가능한 것이어야 한다. 사고대응 정책이나 절차는 특히 결정적인 순간에 실행 가능한지 사전에 테스트되어야 한다. 가능하다면 절차들은 정확성과 속도문제를 고려한다면 자동화하는 것이 좋다. 조직적으로 질서있게 움직여라.

▷ 각각의 장치에 대해 수집절차 지침서에 입각한 조직적인 접근이 필요하다. 속도가 중요하기 때문에 많은 수의 장치에 대한 수집이 필요할 경우, 팀에게 분배해 병렬로 증거수집을 하는 것이 좋다. 단, 하나의 시스템에 대해서는 한단계씩 차례로 절차를 수행해야 한다.

▶ 휘발성이 있는 것을 먼저 진행하고 그렇지 않은 것을 나중에 진행한다.

▷ 시스템 저장장치에 대해 비트(bit) 레벨의 복사를 수행해야 한다. 포렌식 분석을 할 때 파일의 접속시간 정보가 변경되기 쉽기 때문에 분석을 하기 위해서는 증거복사물에 대한 비트 레벨 복사를 해야 한다. 증거복사물을 가지고 분석을 하는 일이 없도록 한다.

Rfc3227 구성에 있어 가장 중요한 원칙은 각각을 이루고 있는 지침과 절차 수행 시 신뢰할 수 있는 조사자나 연구자에 의해 시행됐다는 것이 확인되어야 한다는 점이다. 때문에 일반적으로 법적 권한을 가지고 있는 조사자와 수집가로 2인 1조를 구성하게 된다.

현업에 사용 가능한 포렌식 절차

조금 번거로운 작업일 수도 있지만 사고발생 시 소요되는 시간과 노력을 생각한다면 일상적인 작업 프로세스에 포렌식에 필요한 절차를 접목시켜 놓는다면 보안사고 발생 시 매우 유용하게 활용할 수 있다. 그에 따른 기준을 제시하면 다음과 같다.

▶ 정상적인 상태의 시스템 구성 보관

사내 시스템 하드웨어를 처음 설치하고 필요한 서비스 및 어플리케이션을 설치하고 운영을 시작한다. 운영 시작 후 시스템 운영이 가장 한가한 시간에 시스템 구성을 백업하여 저장한다. 시스템이 정상적으로 문제없이 운영되었을 때 상황을 정기적으로 조사하고 구성을 파일로 저장한다.
이를 통해 해당 프로세스를 정기적으로 수행할 경우, 보안사고 발생 시 단시간 내 원인분석 및 복구가 가능할 것이다.

▶ 사용 가능한 분석 도구를 제작하라

- 필요정보

▷ 레지스트리 정보, 캐쉬 정보
▷ 라우팅 테이블, arp 캐쉬, 프로세스 테이블, 커널 통계, 메모리
▷ 임시 파일 시스템들
▷ 디스크 정보
▷ 시스템에서 확인할 수 있는 원격 로깅과 모니터링 정보
▷ 물리적인 구성 및 네트워크 토폴로지
▷ 귀중한 미디어

- 필요 프로그램

▷ 프로세스 검사하기 위한 프로그램
▷ 시스템 상태를 검사하기 위한 프로그램
▷ Bit-to-bit 복사를 할 수 있는 프로그램
▷ 체크섬이나 서명을 할 수 있는 프로그램
▷ Core image를 생성할 수 있는 프로그램
▷ 증거 수집을 할 수 있는 스크립트

Rfc3227에서 보여주는 프로그램 및 정보는 포렌식 과정에서 원칙으로 삼기에 유용한 정보다. 하지만 아무리 좋은 원칙과 프로그램이라도 사용하기 어려우면 별 의미가 없다. 이런 문제를 해결하려면 사고 분석을 하는 실무자가 쉽게 사용할 수 있는 도구를 모아 자신만의 프로그램 도구를 만드는 것이다. 이런 프로그램들을 만들기 위해선 무상으로 제공되는 포렌식 분석 도구를 살펴보면 충분히 활용이 가능하다. 예를 들어 F.I.R.E, Helix, IRCR 등의 포렌식 프로그램을 인터넷을 통해 얻은 후 익숙하게 사용할 수 있을 때까지 실습하는 것이 필요하다. 이런 과정을 거친 후 가장 많이 사용할 수 있는 프로그램을 추출해 자신만이 사용할 수 있는 도구를 만드는 것이다.

한편, 필요한 도구 역시 프로그램 개발언어 펄(perl)을 사용하면 쉽게 제작이 가능하다. 공개용 포렌식 도구는 대부분 시스템 보안사고 분석에 필요한 모든 정보를 수집할 수 있는 프로그램이 제공되며, 수집한 증거를 파일로 보관할 수 있는 기능을 제공한다. 또한 파일로 증거를 저장함과 동시에 해쉬함수를 이용한 무결성 값 부여 기능이 필수기능으로 포함되어 있다. 이를 통해 증거에 대한 재현과 무결성 입증이 가능해 포렌식 증거를 통해 수집된 증거는 증거로서의 가치를 지니게 된다.

실용적인 컴퓨터 포렌식을 위해

보안사고가 발생한 시스템에서 수집한 증거의 양은 너무 방대하기 때문에 실제 수동으로 증거를 수집할 경우 오류가 발생하고 필요한 증거가 누락될 가능성이 있다. 사람이 하는 일에는 실수가 따르기 마련이다. 그렇지만 컴퓨터 포렌식 도구를 이용할 경우, 이런 문제를 해결할 수 있고 이런 이유로 도구를 통해 수집한 증거는 가치가 있는 것이다.

컴퓨터 포렌식은 어렵다. 보안사고 발생 시스템에서 증거를 수집하는 것은 복잡하고, 시간이 많이 소요되는 일이다. 그러나 시스템이 정상적으로 운영될 때의 정보를 정확히 알고 있다면 보안사고가 발생했을 때 문제점을 신속하고 명확하게 밝혀낼 수 있다. 이것이 실용적인 컴퓨터 포렌식인 것이다.

적어도 자신이 운영하고 있는 시스템의 정상적인 상태를 명확히 알고 있고, 해당 상태에 대한 변화를 쉽게 인지하고 정보를 수집할 수 있는 자신만의 프로그램이 있다면 보안 정책을 위반하고 문제를 발생시킨 원인을 쉽게 해결할 수 있다. 컴퓨터 포렌식이 정보보호 분야 뿐만 아니라 IT 전체에 필수적인 분야로 자리잡을 날을 기대해 본다. **S**