은닉 데이터베이스 시스템 탐지 방안†

이근기 **이석희 ***이상진

*고려대학교 정보경영공학전문대학원

*lifetop@korea.ac.kr, **gosky7@korea.ac.kr, ***sangjin@korea.ac.kr

A Study on Detection of Covert Database System.

*Keungi Lee **Seokhee Lee ***Sangjin Lee

Graduate School of Information Management and Security, Korea University

요 약

수사관이 사건 관련 조직의 데이터베이스 시스템을 조사할 때, 조직 내부의 많은 시스템을 수작업으로 조사하여 데이터베이스 시스템을 찾는 것은 비효율적이다. 게다가 용의자가 사건 은폐나 알리바이 조작을 목적으로 데이터베이스 시스템을 은닉하는 경우, 수사관이 시스템을 찾기 위해 더욱 많은 인력과 시간을 소비한다. 따라서 간단한 조사로부터 얻은 정보를 통해 어떤 시스템부터 조사해야 할지 결정해야 한다. 데이터베이스 시스템이 네트워크에 연결되어 있는 경우는 접속 오류 정보를 분석하여 데이터베이스 시스템 사용 유무 정보를 수집할 수 있고, 네트워크에 연결되어 있지 않은 경우는 데이터베이스 시스템 흔적 정보 분석을 통하여 데이터베이스로 예상되는 시스템을 찾아 낼 수 있다. 본 논문에서는 데이터베이스 시스템을 은닉하는 사례에 대해 논하고 네트워크상의 은닉된 데이터베이스 시스템을 탐지하는 기법에 대해 살펴보기로 한다.

1. 서론

기존의 아날로그 정보가 디지털 정보로 대체되고 이러한 정보를 기업들이 저장하고 관리하는데 데이터베이스 관리 시스템을 사용한다. 현재의 데이터베이스 기술은 데이터베이스 관리 자동화 기술에 네트워크 기술이 응용되어 분산 환경에서 정보서비스가 이루어지는 새로운 개념의 정보처리환경으로 발전하고 있다.

하지만 이러한 기술동향으로 인하여 디지털 수사 현장에서 많은 시스템 중 특정한 목적으로 사용되는 데이터베이스 시스템을 찾아 전산자료를 획득하는 것은 어려운 점이 많다. 게다가 사건 관련 조직은 종종 수사에 비협조적이고, 심지어는 데이터베이스 서버를 은닉하거나 데이터베이스 관리자가 자리를 비우는 것과 같이 고의적으로 수사에 혼선을 빚게 하기 때문에 더욱 많은 수사 인력 낭비를 초래한다. 용의자가 고의적으로 데이터베이스 서버를 은닉하더라도 조사를 신속하게 진행할 수 있도록 사건 관련 조직 내부의 일반 컴퓨터에서 조직 내의 데이터베이스 시스템 설치 흔적과 사용 정보를 조사한 후, 수집한 객관적인 증거를 통해 전산 자료 제출을 요구해야 한다.

따라서 본 논문에서는 데이터베이스 시스템을 은닉하는 사례에 대해 설명하고 데이터베이스 시스템의 종류에 무관한 시스템 탐지의 일반적인 디지털 포렌식 기법에 대하여 연구해보고자 한다.

2. 은닉 데이터베이스

가. 은닉 데이터베이스 시나리오

수사관이 디지털 수사 현장에서 조사할 때, 조직의 대응 상황을 살펴서 해당 상황에 맞게 조사를 진행하여야 한다. 대응 상황은 상황에 따라 많은 변수가 있지만, 크게 4가지로 나눌 수 있다.[1)]

첫 번째 대응 상황의 경우는 양호한 협조 상황이다. 이 경우는 관리자 또는 책임자가 수사에 적극적으로 협조하는 경우이다. 하지만 이 상황에서 주의해야 할 점은 그 데이터가 사전에 준비한 데이터가 아닌지 정확한 검증이 필요하다는 것이다.

두 번째 대응 상황은 형식적인 협조 상황이다. 이 경우는 전산관리자 또는 책임자가 수사관의 질문과 요구에 대해 형식적으로만 대응하고 정확히 알려주지 않는 경우이다. 수사관은 준비한 디지털 포렌식 툴과 탐지 기법을 사용해서 객관적인 데이터를 수집하여 자료가 법적 효력을 가질 수 있도록 한다.

세 번째 대응 상황은 즉흥적인 비협조 상황이다. 예고치 않은 수사를 실시하여 미처 숨기지 못한 데이터를 감추기 위해 데이터베이스 관리자가 자리를 비우거나 시스템의 전원을 급히 끄거나 시스템을 잠근다. 이 경우는 급하게 정보를 은닉하려 시도했기 때문에 꼼꼼히 정보를 숨기지 못했을 가능성이 높다. 클라이언트에서 데이터베이스 시스템 흔적 정보를 위주로 조사를 하여 객관적인 증거를 확보할 수 있다.

네 번째 대응 상황은 고의적 비협조 상황이다. 수사가 예고되거나 수사관의 조사가 시행되기 전 충분한 시간 간격이 있을 경우, 조직은

† 본 연구는 과학재단 디지털 정보 획득 기반기술 연구(M10740030004-07N4003-00410)의 지원으로 수행되었습니다.

시스템의 연결을 단절하고 흔적을 제거함으로써 수사관의 조사를 방해한다.

나. 데이터베이스 은닉 사례

이러한 두 가지 비협조 대응 상황인 경우는 [그림 1]과 같이 데이터베이스 시스템을 은닉할 수 있는데 특정 클라이언트 시스템에서 데이터베이스 시스템에는 접근할 수 없지만 웹 서버나 메일 서버 시스템과 같은 기타 서버 시스템에는 문제없이 접근할 수 있다. 이러한 경우에는 고의적으로 데이터베이스 서버를 은닉했다고 판단할 수 있다.

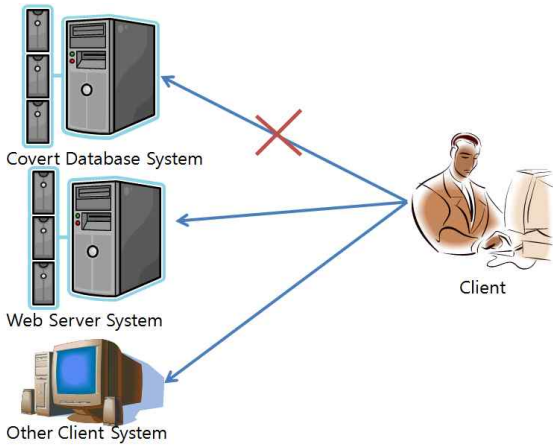

그림 1 은닉 데이터베이스 시스템 구성 예

또 다른 은닉 사례는 특정 클라이언트만 접근을 허용하는 데이터베이스 시스템이 존재하는 것이다. 대기업 등의 데이터베이스는 다수의 서버들이 서로 연계되어 있으므로 중간에 데이터를 위·변조하는 경우 데이터가 파괴되어 모든 데이터를 유실할 가능성이 있으므로 백업 중간에 데이터를 위·변조하는 일은 드물다.[2] 이와 같이 대기업 등의 데이터베이스의 경우에는 접근 자체를 막는 것은 전체 네트워크 서비스의 대한 가용성에 큰 영향을 미친다. 따라서 접근 자체를 막는 은닉을 시도하기는 어렵기 때문에 관리자를 비롯한 소수의 클라이언트에서만 접근이 가능하게 권한을 설정한다. 이러한 방법으로 비밀 자료를 관리할 경우 수사관은 이러한 데이터베이스 시스템이 존재하는지 파악하기가 힘들다.

수사관이 디지털 수사 현장에서 데이터베이스 시스템으로 추정되는 시스템이 없거나 은닉했다고 판단할 경우 조사 대상 조직 내부의 다른 컴퓨터를 조사하여 획득한 인접 네트워크 정보를 통해 데이터베이스의 사용 흔적을 찾아야 한다. 이러한 방식으로 데이터베이스 시스템을 은닉하는 경우는 비록 접속하여 실제 전산 자료를 얻을 수는 없지만 사용 흔적 정보를 통해 객관적인 자료를 획득할 수 있다. 획득한 자료를 토대로 조사 대상 조직에게 증거 제출을 요구할 수 있다.

3. 데이터베이스 시스템 탐지 방안

가. 데이터베이스 탐지 개요

데이터베이스 시스템을 탐지할 때 해당 시스템이 온라인 상황인지 오프라인 상황인가에 따라 다른 기법을 적용할 수 있다.

데이터베이스 시스템이 온라인일 경우에는 Microsoft ActiveX Data Object 기술을 사용하여 데이터베이스 시스템으로 사용하고 있을 가능성이 있는 IP로 접근을 시도해 볼 수 있다. 통상 데이터베이스에 접근하기 위해서는 ID, 비밀 번호, IP, Port 번호, 그리고 데이터베이스 서비스 이름과 같은 정보가 필요하다. 하지만 비협조 대응 상황에서는 IP, Port 번호, 그리고 데이터베이스 서비스 이름과 같은 정보는 사용 흔적 정보를 통해 쉽게 수집할 수 있지만 ID, 비밀번호와 같은 정보는 수집하기가 쉽지 않다. 수사 비협조 상황에서 데이터베이스 시스템에 접근할 때 중요한 것은 실제 전산 자료를 획득하는 것이 아니라 의심 가는 IP를 가진 시스템이 데이터베이스 서버로 사용되고 있는가 하는 점이다. 이 사실은 ADO 기술을 사용해서 접속하는 과정에서 반환하는 오류 정보로 판단할 수 있기 때문에 해당 서버의 IP와 비밀번호를 알 수 없어도 데이터베이스 시스템을 탐지할 수 있다.

데이터베이스 시스템이 오프라인일 경우에는 조사 대상 조직 내부의 다른 클라이언트 시스템을 조사하여 사용흔적 정보를 분석한다.

나. 데이터베이스 사용 흔적 수집 기법

먼저 수사 대상 기업에 데이터베이스가 설치되어 있는지 확인하기 위해 설치 및 사용 흔적을 조사하고, 획득한 흔적 정보를 바탕으로 디지털 포렌식 분석을 위한 실제 데이터베이스 파일을 획득할 수 있다. 데이터베이스 흔적 정보를 수집하기 위한 방안으로는 디지털 포렌식 관점에서 특정 응용프로그램을 분석할 때 이용하는 접근법이 있다.

먼저 파일 모니터링 분석은 실시간으로 파일시스템의 활동을 모니터링 하는 툴인 FileMon[3][그림 1] 프로그램을 이용한다. 데이터베이스 시스템이 실행 중에 참조하는 파일 정보를 수집해서 분석한다. 분석 대상이 되는 파일에는 로그 파일, 설정 파일, 데이터베이스 파일 등이 있다. 일단 수집된 파일 정보를 기반으로 파일 내부를 분석해서 데이터베이스 설정 정보에 관한 내용을 획득할 수 있다.

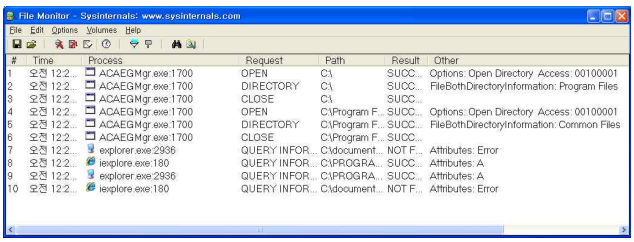

그림 2 Sysinternal 의 File Monitoring 도구

레지스트리 모니터링 분석은 RegMon[4][그림 2] 프로그램을 이용하여 실시간으로 데이터베이스 시스템이 접근하는 레지스트리 정보를 모니터링하고 이를 통해 참조하는 데이터를 수집할 수 있다. 분석 대상이 되는 레지스트리에는 IP와 포트번호, IP, 서비스 이름 등의 데이터를 포함한다.

로그 파일 분석은 파일 모니터링 분석 방법으로 수집한 로그 파일에 대한 정보를 바탕으로 실제 파일 내부 정보를 분석하여 의미 있는

정보를 추출한다.

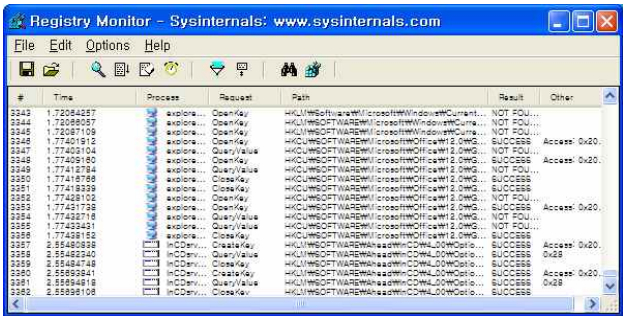

그림 3 Sysinternal 의 Registry Monitoring 도구

조사해야할 사용 흔적 정보는 데이터베이스 관리 시스템 소프트웨어에 따라 조금씩 다르다. 이 흔적 정보를 기반으로 조직 내의 많은 시스템 중 데이터베이스 시스템을 찾기 위해 조사해야할 항목 리스트를 만들 수 있다. 이 항목 리스트를 바탕으로 데이터베이스 서버의 IP 주소와 포트번호, 데이터베이스 서비스 이름, IP와 비밀번호를 수집할 수 있기 때문에 클라이언트에서 신속하게 흔적 정보를 수집한 후 데이터베이스의 사용 유무를 판단할 수 있다.

다. ADO를 이용한 데이터베이스 서버 탐지 기법

ADO(ActiveX Data Object)는 Microsoft 사에서 개발하고 배포 중인 객체 지향형 인터페이스이다. Microsoft 사는 다양한 종류의 데이터베이스에 대해 공통적으로 적용할 수 있는 접근 기술의 필요성을 느끼고 이러한 작업을 위해 다른 주요 데이터베이스 회사들과 함께 데이터베이스와 Microsoft의 데이터베이스 인터페이스인 OLE DB 사이를 연결할 수 있는 계층을 정의하였다. OLE DB는 ADO를 사용하는 프로그래머가 실제로 사용하는 기본적인 시스템 서비스이다. ADO는 ActiveX의 하위 기술이며 Microsoft의 컴포넌트지향 기반구조인 COM(Component Object Model)의 일부이기도하다.

통상 데이터에 접근하기 위해서는 SQL(Structure Query Language)를 사용하는데 모든 데이터베이스 업체가 표준을 따르지는 않는다. 보통 업체는 속도 향상, 저장 공간 최적화나 저장 프로시저와 같은 SQL에서 부족한 기능을 지원하기 위해서 업체만의 고유한 언어를 사용하기도 한다. 하지만 ADO는 프로그래머가 실제 데이터베이스 시스템이 어떻게 구현되어 있는지 알 필요 없이 데이터에 접근하는 프로그램을 구현할 수 있도록 프로그래밍 언어와 OLE DB 사이의 계층을 제공한다.[5] 따라서 ADO 기술을 응용하면 조사 대상의 데이터베이스 종류에 관계없이 조사를 진행할 수 있다.

ADO는 [그림 4]와 같은 여러 객체들로 구성되어 있다.

- Connection Object - 응용 프로그램과 데이터베이스 사이의 의사소통을 관리함.
- Recordset Object - 데이터베이스의 레코드 정보를 가지고 있음
- Command Object - SQL 명령을 실행하거나 저장 프로시저 관련 정보를 기술함.
- Record Object - 다른 데이터 구조들과의 호환성을 위해 사용됨
- Stream Object - 텍스트 파일이나 웹 페이지 정보를 저장함
- Error Object - 오류 정보를 저장함
- Field Object - 데이터베이스의 열 정보를 저장함
- Parameter Object - SQL 명령의 인자값을 저장함
- Property Object - 객체들의 정보를 저장함

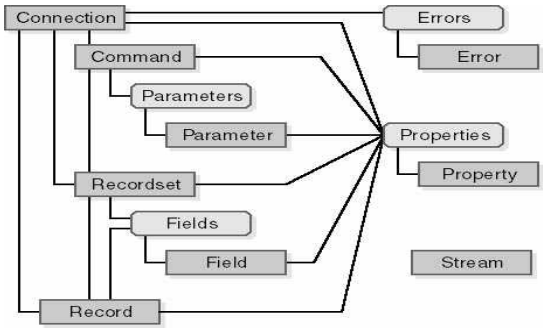

그림 4 ADO 객체 모델

네트워크 침입 탐지할 때 가장 흔한 2가지 방법으로 특정 컴퓨터에서 열린 포트를 알아내기 위한 Port Scan과 특정 네트워크에 있는 클라이언트를 대상으로 동작 여부를 알아내기 위한 Ping Sweep이 있다.

이렇게 IP 정보를 얻고 나면 해당 시스템에 접근을 시도해볼 수 있다. 미처 수집하지 못한 ID, 비밀번호, 데이터베이스 서비스 이름은 임의로 설정하거나 생략한다.

그림 5 올바르지 않는 데이터베이스에 접근

만약 해당 IP를 사용하는 시스템이 데이터베이스 시스템으로 사용하고 있지 않거나 네트워크에 접속하지 않은 경우에는 [그림 5]와 같은 오류 정보를 반환한다.

그림 6 올바른 데이터베이스에 접근

[그림 6]은 데이터베이스 서버로 사용하는 시스템에 접근했을 경우 반환받는 오류 정보이다. 이와 같은 경우 지정한 IP는 데이터베이스 시스템으로 사용하고 있으며 정상적으로 운영되고 있다는 사실을 알 수 있다. 다만 포트 정보와 ID, 비밀번호 정보를 알 수 없기 때문에 정상

적인 접근을 할 수 없는 상태이다. 이 경우에는 서버 관리자나 데이터베이스 관리자에게 위와 같은 증거를 제시하고 정상적인 접근을 위한 계정 정보를 요구할 수 있다.

4. 결론

데이터베이스 포렌식 수사 현장에서 중요한 것은 데이터베이스 시스템 사용 여부와 실제 전산 증거의 신속한 확보이다. 전산 관리자나 데이터베이스 관리자가 비협조적으로 수사를 받을 때 디지털 증거에 대한 법적효력을 갖기 위해 원본 데이터베이스에 대한 정보를 파악해야 한다.

본 논문에서는 데이터베이스 시스템을 탐지하기 위한 방안에 대해 살펴보았다. 파일 모니터링 분석, 레지스트리 분석, 로그 분석와 같은 데이터베이스 흔적 정보 분석을 통해 데이터베이스 서버를 사용했던 흔적과 IP주소, 포트에 대한 정보를 수집하고 이를 기반으로 실제 데이터베이스 파일을 획득할 수 있다. 또한 네트워크상의 데이터베이스 서버 시스템을 찾기 위해서 ADO 기술을 응용, 연결 오류 정보를 분석하여 서버가 데이터베이스 서버로 사용하고 있는지에 관한 정보를 확인할 수 있다. 수사 환경을 고려하여 신속하게 데이터베이스 포렌식 수사를 진행할 수 있는 방안을 확인하였다.

참 고 문 헌

1) 이구택, “은닉 자원탐지의 관한 연구”, 고려대학교, 2007

2) 이규안, 박대우, 신용태, “포렌식 자료의 무결성 확보를 위한 수사현장의 연계관리 방법 연구”, 한국 컴퓨터정보학회 학회지 제 11권 제 6호 175-184, 2006. 12

3) FileMon for Windows v7.04 By Mark Russinovich and Bryce Cogswell
Available at :
http://technet.microsoft.com/ko-kr/sysinternals/bb896642(en-us).aspx

4) RegMon for Windows v7.04 By Mark Russinovich and Bryce Cogswell
Available at :
http://technet.microsoft.com/ko-kr/sysinternals/bb896652(en-us).aspx

5) David Sceppa, "Programming ADO", Microsoft, 2001