ZDNet Korea news print

프린트 닫기

인터넷

보안업체 코드서명 정보 유출, 파장은?

손경호 기자 입력 : 2016.02.22.16:42 수정 : 2016.02.22.18:27

모 보안업체가 인터넷에서 자사 프로그램(보안 모듈)을 배포하는데 쓰는 일종의 인감 도장과 같은 성격의 코드 서명 정보가 유출돼 악성 프로그램 유포에 악용되는 사건이 벌어졌다.

일각에서는 이 사건이 보안회사를 통해 공격을 시도했다는 점에서 3.20 사이버테러 때와 유사하다는 분석이 나오고 있지만 현재로서는 공격자가 어떤 의도를 갖고 있는지 확신할 수 있는 단계는 아니란게 전문가들 설명이다.

공격자가 사이버테러 수준의 공격을 계획했는지, 특정 타깃을 노려 정보유출을 시도했는지, 금융정보를 빼내 돈을 벌려고 했는지 등에 대한 모든 가능성이 열려있는 상황이다. 현재 검찰에서 이 사건을 조사 중이다.

코드서명은 인터넷에 프로그램을 유포하기 위해 자사가 만든 것이 맞다는 것을 증명하기 위해 일종의 인감도장을 찍는 것과 같다. 이 과정에서 사용되는 것이 인증서와 개인키다. 이 사건의 경우 금융권 등 고객사에 제공하는 일부 보안모듈을 우리가 개발한 것이 맞다고 증명하는데 필요한 인감도장 정보(개인키)가 유출됐다.

코드서명 정보를 유출 당한 보안회사는 코드서명에 사용되는 개인키(온라인 상 인감도장 역할을 하는 정보)를 개발자들 PC에 저장해 사용해 왔다. 일부 개발자들 PC가 외부 공격자로 인해 악성코드에 감염되면서 이러한 개인키가 유출된 것이다.

공격자는 이 정보로 코드서명을 거쳐 악성 프로그램을 배포했다. 마치 실제 보안회사가 배포하는 것처럼 위장했다.

해당 사실을 확인했던 보안업계 관계자는 "(코드서명을 악용한) 악성코드가 배포됐으면 광범위하게 모니터링 됐을 것인데 아직까지 그런 정황은 확인되지 않고 있다"며 " 현재까지 파악하기로는 공격자가 코드서명을 악용해 악성코드를 배포할 수 있는지 테스트 작업까지만 진행한 것으로 판단된다"고 말했다. 이 관계자는 또 "소수 타겟을 노려 배포 됐을 가능성도 배제할 수 없다"고 덧붙였다.

그러나 3.20 사이버테러에서처럼 보안회사가 관리하는 업데이트 서버를 통해 대량으로 코드서명된 악성코드가 유포될 가능성은 아직까지 확인되지 않았다. 이렇게 하려면 피해를 입은 보안회사가 관리하는 업데이트 서버에까지 공격자가 악성코드를 심어놨어야 한다. 하지만 현재 사건에서는 업데이트 서버까지 해킹됐는지에 대한 정황은 파악되지 않고 있다.

한국인터넷진흥원(KISA) 인터넷침해대응본부 침해사고분석단 신대규 단장은 "아직 악성코드에 감염된 개발자 PC가 해당 회사에서 관리하는 업데이트 서버에 접속했는지 여부는 확인되지 않았다"며 "초동수사를 마치고 검찰에 관련 자료를 넘긴 상황"이라고 설명했다.

신 단장은 "일반적으로 공격자들이 대상 PC들을 악성코드에 감염시키는 것 자체가 목적인 경우가 많다"며 "이를 통해 해당 PC 사용자를 모니터링하고, 정보를 탈취하는 등 작업은 나중에 일어나게 된다"고 밝혔다.

코드서명 정보를 유출당한 보안회사는 이달 초부터 중순까지 자사 이름으로 코드서명이 끝난 악성 프로그램이 유포되고 있다는 사실을 확인해 문제가 된 인증서와 개인키를 폐기하고 다시 발급했다. 해당 보안모듈을 사용했던 고객사에서는 새로운 인감도장을 찍은 보안모듈을 쓸 수 있게 교체하는 작업을 진행 중이다.

현재까지 정확한 피해규모를 확인하기는 어렵지만 일반적인 개발자들 사이에서도 공공연하게 문제가 됐던 코드서명(코드사이닝, code signing)용 키 관리 문제가 보안회사로까지 번졌다는

점에서 보다 철저한 대응이 필요하다는 지적이다.

sontech@zdnet.co.kr 손경호 기자

프린트 닫기