컴퓨터 방열 팬 회전 소리도 해킹 대상이다

김형자 과학칼럼니스트

"만약 누군가 지금 나의 컴퓨터를 지켜보고 있지는 않을까?"
최근 디지털 정보화 사회가 되면서 항상 신경 쓰이는 문제, 보안이다. 컴퓨터가 발전하면 할수록 악성코드와 바이러스가 더욱 진화하기 때문이다. 인터넷이 대중화되기 이전에는 해킹 방식의 바이러스보다는 컴퓨터를 다운시키거나 하드디스크를 날리는 악성코드가 유행했지만, 요즘은 사용자의 개인정보에서 공인인증서까지 빼내는 해킹 수법이 다양해지고 있다.
아무리 백신 프로그램을 사용하고, 기술적으로 고도화된 암호를 만들어 첨단 방화벽을 사용한다 한들, 작정하고 취약점을 찾는 해커의 공격을 완전히 피하기는 어렵다. 해킹을 통해 철통 같은 보안 능력을 갖춘 대기업의 기밀문서를 빼내는 건 종종 있는 일이고, 포털 사이트의 회원 정보를 통째로 훔쳐가는 일도 간혹 벌어진다. 하물며 민간인이 사용하는 개인 컴퓨터의 보안쯤이야 전문 해커들에게는 종잇장 같은 수준이 아닐까.

네트워크 분리된 컴퓨터도 뚫릴 수 있다

컴퓨터가 인터넷에 연결되어 있는 이상 해킹을 100% 완벽하게 차단할 수는 없다. 암호화된 디지털 정보를 빼내기 위해 해커들이 사용하는 해킹 기술도 각양각색. 그럼 컴퓨터를 아예 분리시켜 인터넷에 연결하지 않는다면 해킹으로부터 안전할까?

컴퓨터를 인터넷에 연결시키지 않고 물리적으로 해킹을 원천 차단하는 보안법을 에어 갭(Air Gap)이라고 한다. 에어 갭은 '온라인 컴퓨터'와 '오프라인 컴퓨터' 2대를 사용하는 방식으로 이뤄진다. 온라인 컴퓨터는 인터넷 접속이나 네트워크 통신 용도로만 사용하고, 데이터 보관이나 프로그램 작업 등은 오프라인 컴퓨터만을 사용하는 것. 온라인 컴퓨터의 자료를 오프라인 컴퓨터로 옮길 때는 네트워크 통신이 아닌 전송수단(USB 등)을 사용한다. 이럴 경우 정보를 빼가기 어렵고, 온라인 컴퓨터가 해킹당하더라도 중요 데이터는 오프라인 컴퓨터에만 있으니 해킹 피해를 최소화할 수 있다.

그러나 네트워크가 분리된 컴퓨터도 완벽한 건 아니다. 그런 환경에서도 해커들은 정보를 빼내기 위해 온갖 방법을 동원하고 있기 때문이다. 컴퓨터에 연결된 스피커에서 사람 귀에 들리지 않는 고주파 신호를 발생시켜 정보를 유출하는 방법이나 컴퓨터 내부에서 발생하는 주파수를 이용하여 정보를 빼내는 방법을 찾아낸 것도 그들이다. 이 때문에 아주 민감한 시설에서는 아예 스피커 없는 컴퓨터를 사용하기도 한다.

또 우리가 상상도 못할, 아주 독특한 해킹 방법도

찾아냈다. 컴퓨터의 방열 팬을 이용하는 기술이 그것. 모든 컴퓨터에는 열 센서가 구축되어 있다. 열 센서를 통해 컴퓨터는 내부의 열을 측정하고, 열이 감지되면 방열 팬을 돌려 방출시킴으로써 컴퓨터가 손상되는 것을 막는다. 열 센서가 없다면 컴퓨터의 회선이 전부 타버려 컴퓨터가 오래가지 못할 것이다. 그런데 열 센서 시스템이 생각지도 못한 해킹의 대상이 되고 있는 것이다.

최근 이스라엘 벤구리온대학 사이버 보안 연구센터의 연구진들은 스피커도 없고 네트워크 연결이 차단된 상황에서도 실현 가능한, 컴퓨터 방열 팬으로부터의 정보 빼가기 방법을 제시했다. 컴퓨터의 열을 식히는 방열 팬이 회전할 때 발생하는 소음을 이용해, 침투한 컴퓨터 내부의 데이터를 빼낸다는 것이다. 컴퓨터는 팬이 윙윙 돌면서 소음을 만들어 낸다. 예를 들어 CPU는 동작하면서 매우 높은 소음을 방출하고, 다른 부품들이 실행되는 것에 따라 소음이 변동된다. 소음은 팬의 회전 속도에 따라 달라지는데, 속도가 빨라질수록 더 크게 발생한다. 이런 소음의 차이를 녹음 장비로 저장한 후 데이터를 빼낸다.

이스라엘 연구팀은 방열 팬의 이런 특징을 이용할 목적으로 악의적인 소프트웨어를 개발했다. 모든 데이터가 1과 0으로 조합된 원리를 바탕으로 만든 '팬스미터(Fansmitter)'가 그것. 컴퓨터의 뽑아낼 데이터를 1=1000RPM, 0=1600RPM이라는 팬 속도로 환원해 아날로그 사운드로 변환시키는 원리다. 이 프로그램이 컴퓨터에 설치될 경우 팬의 회전 속도를 제어하게 되는데, 팬이 서로 다른 속도로 회전하면 각각 1과 0에 대응한다.

이런 식으로 컴퓨터에 저장된 암호화 키나 패스워드 등의 데이터를 분당 15~20비트의 속도로 전송한다. 데이터가 반경 8m 안에 있는 스마트폰에 문자나 와이파이 등의 방법으로 전송되면, 스마트폰은 다시 이를 공격자에게 전달해 주는 방식이다.

네트워크 분리된 컴퓨터와 해커 스마트폰에 멀웨어 심어야 가능

물론 이것은 실험실 환경에서의 가상적 공격이다. 실질적으로 이 공격을 실행하려면 먼저 네트워크와 분리된 데이터가 든 컴퓨터와 해커가 그 컴퓨터 주변 인근에 있어야 한다는 전제하에서만 가능하다. 즉, 해커의 컴퓨터(스파트폰)가 공격 대상 컴퓨터와 가까이 위치해 있어서 분리된 컴퓨터와 해커의 스마트폰에 동시에 멀웨어(malware, 컴퓨터에 감염되는 모든 악성코드)를 심어 감염시켜야 한다.

또 공격 속도가 빨라야 안전하다. '팬스미터'의 공격 속도는 너무 느리다. 팬 회전 속도 1=1000RPM, 0=1600RPM의 방법으로 테스트한 결과, 분 단위로 빼낼 수 있는 데이터는 3비트. 같은 방법으로 각각 4,000/4,250RPM로 업그레이드한 결과는 15비트에 불과했다. 데이터 전송 속도가 낮으면 오염될 소지가 있다. 이런 면에서 방열 팬을 이용한 해킹은 실용성이 떨어진다고 볼 수 있다.

그렇다고 네트워크에서 분리된 컴퓨터에 멀웨어를 감염시키는 일이 불가능하기만 할까. 아니다. 미국 정보 당국이 만든 스틱스넷(Stuxnet)은 외부 네트워크와 분리돼 철저한 보안을 유지하던 이란의 핵 시설을 감염시켜 프로그램을 연기하게 한 적이 있다. 이란 핵 시설 관련 업무를 하는 외부 사람의 USB 드라이브를 감염시켜 핵 시설 내의 컴퓨터까지 감염시킨 것이다.

이처럼 오프라인 컴퓨터도 언제든 악성코드 감염의 대상이 될 수 있다. 더구나 어떤 컴퓨터든 방열 팬은 적어도 몇 개씩 달려 있지 않은가. 오늘도 누군가가 회전하는 당신의 방열 팬을 훔쳐보고 있을지 모를 일이다. TTA