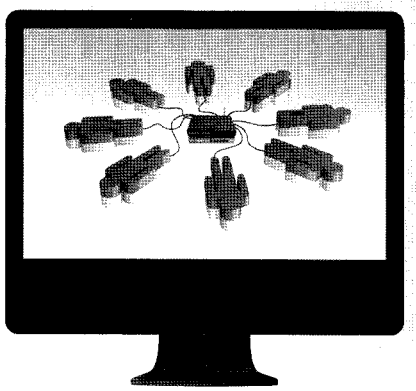
클라우드 기술도입을 통한 보안 서비스의 새로운 패러다임



권진욱 | 안철수연구소 제품기획팀 차장

1. 머리말

악성코드가 금전적인 이득을 목적으로 변화됨에 따라 특정 대상을 목표로 하는 전문화, 조직화, 국지화 경향을 띠고 있다. 이러한 패러다임의 변화 속에 악성코드에 대응하는 보안 기술도 빠르게 변화하고 있다. 특히 지난 20년간 블랙리스트(Blacklist) 기반의 안티바이러스 솔루션을 제공하던 보안 업체들로서는 기존의 테크놀로지만으로는 현재와 같이 폭발적인 증가세를 보이고 있는 악성코드 이슈를 모두 해결할 수 없다. 따라서 보안 기술에 있어서 새로운 변화를 수용해야 할 시점이 되었다.

본 고에서는 최근 악성코드의 동향을 살펴보고, 기존 대응 방법의 문제점 그리고 이를 보완할 수 있는 클라우드 컴퓨팅 기술도입을 통한 보안 서비스의 새로운 패러다임에 대해 기술하고자 한다.

2. 최근 악성코드 동향

2003년 이후 악성코드의 제작 동기가 호기심 또는 자기과시에서 금전적인 목적으로 변하면서 새로운 전환점을 맞이하게 되었다. 기존에 불특정 다수에게 배포하던 악성코드가 점차 특정 대상을 노리는 타깃 공격으로 변화하고 있다. 또한 제작 동기가 협박이나 인터넷 뱅킹처럼 직접적으로 돈과 연결되거나, 내부 정보를 유출하여 2차적인 위협을 하기 위한 도구로 변형되었다.

· 사이버 블랙마켓의 활성화

개인정보를 사고 파는 지하경제 시장의 활성화에 따라, 금전적 이익을 목적으로 한 악성코드 배포 및 해킹 범죄가 증가하고 있다. 특히 이러한 악성코드 배포 방법은 범죄조직의 입장에서는 비용이 적게 드는 반면에, 즉각적인 효과를 볼 수 있다는 점에서 비용 대비 효과가 큰 방법으로 인식되고 있다.

예를 들어, 주민등록번호, 은행계좌 번호, 신용카드 정보 등 개인정보는 사이버 블랙마켓에서 팔면 바로 돈이 되기 때문에 개인정보를 빼내가기 위한 악성코드의 배포가 급증하고 있는 것이다. 실제로 지난해 미국 경찰은 40만 대의 컴퓨터를 감염시킨 소베라는 별명을 사용하는 청년을 검거했다. 그는 감염된 컴퓨터를 조종하는 봇넷(BotNet)이라는 기술을 이용해 연 5만 8천 달

러를 벌어들인 것으로 알려졌다.

또 하나 주목해야 할 것은 컴퓨터 전문가가 아니더라도 사이버 블랙마켓을 통해 쉽게 해킹 툴이나 악성코드 제작 툴 등을 저렴한 가격에 구매하여 개인정보를 탈취하기 위한 해킹을 할 수 있게 되었다는 것이다. 이에 따라 신종 악성코드 갯수 및 해킹 시도가 폭발적으로 증가하고 있다.

이러한 사이버 블랙마켓 활성화는 세계적인 경기 불황 및 인터넷 보급률 증가와 맞물려 앞으로도 심각한 위협으로 작용할 것으로 보인다.

· 악성코드의 폭증

이와 같이 특정 타깃을 대상으로 공격을 하다 보니 계속 같은 악성코드로 공격하면 안티바이러스 솔루션에서 차단될 확률이 높기 때문에 변종을 만들어 공격할 필요성이 생겨났다. 악성코드를 대량생산하고 자동적으로 변종을 만들 수 있는 툴들이 악성코드 제작자들 사이에 만들어지고, 또한 거래되고 있다. 이로 인해 악성코드의 숫자가 이전에는 상상할 수 없었을 정도로 폭발적으로 증가하게 되었다.

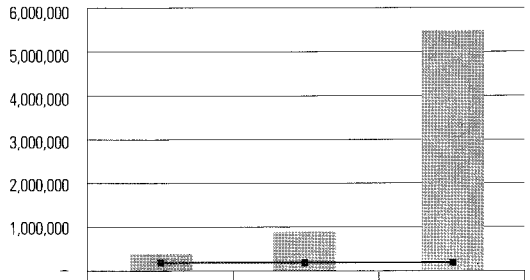
안티바이러스 제품을 테스트하고 있는 Av-test.org에 따르면 신종 악성코드의 수는 2005년 333,000개, 2006년 972,000개, 2007년 5,490,000개로 증가하고 있다. 또한 안철수연구소의 ASEC 2008 Annual Report에 의하면 2008년 한 해 동안에만 전 세계적으로 800만 개 이상의 악성코드가 만들어졌다고 한다. 이러한 전문기관의 분석 자료를 통해 알 수 있듯이 악성코드의 숫자는 이전에는 상상할 수 없는 수준으로 매년 기하급수적으로 증가하고 있다.

3. 현재 안티바이러스 업체의 대응 방법 및 한계점

악성코드의 폭발적 증가는 모든 안티바이러스 솔루션 개발 업체에 기존에 경험해 보지 못한 새로운 이슈로 다가왔다. 악성코드의 숫자가 이전에는 상상할 수 없이 많아짐에 따라 결과적으로 기존에 크게 이슈가 되지 않았던 안티바이러스 소프트웨어의 두 가지 문제점이 부각되고 있다.

· 진단율 이슈

매시간 수백~수천 개의 신종 악성코드를 처리함에도



	2005년	2006년	2007년
신종 악성코드 수	333,000	972,000	5,490,000
안티바이러스 제품의 시그니처 수	111,566	134,484	148,869

※출처: AV-test.org

[그림 1] 연도별 신종 악성코드 수

불구하고, 점점 더 많은 변종 악성코드가 만들어짐에 따라 기존에 악성코드를 수집하고, 분석하고, 엔진에 포함시키는 일련의 작업들 만으로는 모든 악성코드를 처리할 수 없게 되었다.

[그림 1]에서 보듯이 매해 새로 만들어지는 신종 악성코드 수 대비 안티바이러스 제품이 처리하는 악성코드 수는 점점 격차가 벌어지고 있다.

많은 안티바이러스 솔루션 개발사들이 이러한 악성코드에 대항하여 진단율을 높이기 위해 시그니처 기반의 블랙리스트 방식 이외에도 휴리스틱 검사(Heuristic Detection), 프로액티브 프리벤션(Proactive Prevention), 샌드박스(Sandbox) 등의 다양한 기법을 사용하고 있다. 그러나 이러한 방식은 안티바이러스 솔루션이 설치되는 PC 환경의 다양성, PC 사양의 제한, 업데이트 관리, 그리고 오진 등의 이슈로 인해 범용적으로 사용하기에는 한계가 있는 게 사실이다.

또한 진단 개수가 증가하면 엔진 사이즈가 커지고 메모리 점유율이 증가하며 검사 속도가 느려지는 등의 부작용이 발생한다. 아울러 오진의 가능성도 높아진다.

· 업데이트 속도 이슈

또한 악성코드의 숫자가 많아질수록 빠른 업데이트가 상당히 중요해진다. 과거와 달리 이제는 단 한 시간 업데이트가 지연되어도 수천 개 이상의 신종 악성코드에 감염될 위험에 노출된다. 이에 따라 안티바이러스 솔루션 개발 업체의 경우 업데이트 주기를 단축하는 방법을 우선적으로 사용하고 있다. 현재 대부분의 업체에서 이전에 일주일에 한 번 업데이트를 제공하던 방식에서 하루에 한 번 이상의 시그니처 업데이트를 제공하고 있는 중이다. 그러나 하루에 수만 개 이상의 신종 악성코드가 제작되는 현 시점에서 이러한 업데이트 주기 변경만으로 신종 악성코드에 완벽히 대응하는 것은 불가능하다.

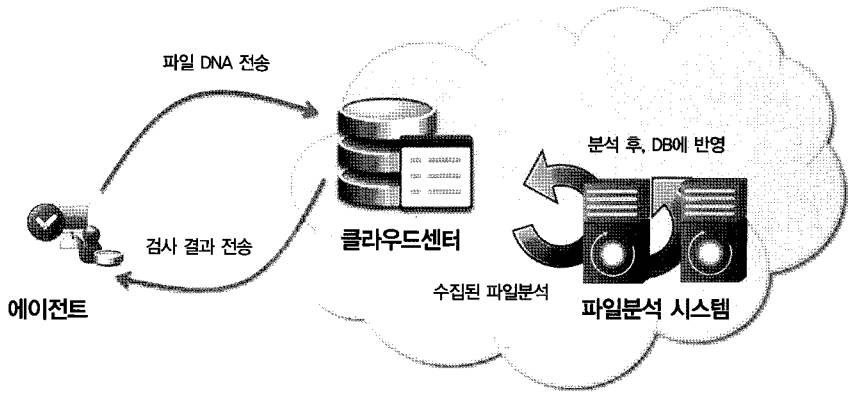
4. 클라우드 기술도입을 통한 보안 서비스의 새로운 패러다임

상기에 언급한 바와 같이 이제는 기존의 방식만으로는 악성코드의 위협으로부터 100% 안심할 수 있다고 이야기하기가 힘든 상황이 도래했다. 이에 대응하고자 안티바이러스 솔루션 개발업체에서는 클라우드 컴퓨팅 기술을 도입하여 새로운 개념의 악성코드 대응 기술을 만들게 되었다. 클라우드 컴퓨팅 기술을 도입한 악성코드 대응 기술은 기존에 악성코드에 대한 모든 데이터를 PC로 다운로드한 후 PC에서 처리하던 방식과 달리 클라우드 컴퓨팅 개념을 이용한 새로운 기술이다. 즉, 대규모 파일 데이터베이스를 중앙서버에서 관리하며, PC에 설치되어 있는 에이전트에서 파일의 악성 여부에 대해 문의하면 이에 대해 응답을 해주는 방식이다. 클라우드 컴퓨팅 기술을 도입한 악성코드 대응 기술의 작동 방법은 [그림 2]와 같다.

① 클라우드 센터에서는 파일의 기본 정보, 프로그램 디지털 서명 정보 분석, 평판 시스템을 통한 분석, 파일에 대한 활동 동향 분석, 행위 기반 활동 분석, 파일 간 관계 분석 등 다양한 기술을 이용해 파일의 정상 또는 악성 여부를 판단하고, 이를 파일 DNA 데이터베이스로 관리한다.

② PC에 설치된 에이전트를 통해 파일의 엑세스가 있으면 클라우드 센터로 파일 DNA를 전송한다.

③ 클라우드 센터에서는 대용량 DNA 데이터베이스에서 해당 DNA의 유형이 있는 지 확인하고, 같은 유형의 DNA가 존재하면 기 분석된 DNA정보, 즉 악성코드인지 정상 파일인지 확인해 알려준다.



[그림 2] 클라우드 컴퓨팅 기술을 도입한 악성코드 대응 기술 구성도

5. 클라우드 컴퓨팅 기술을 도입한 악성코드 대응 기술의 효과

앞서 현재 안티바이러스 개발업체의 대응 방법 및 한계점에 대해 언급한 바 있다. 클라우드 컴퓨팅 기술을 도입한 악성코드 대응 기술을 사용할 경우 이러한 문제들에 대한 해결이 가능하다.

· 진단율 이슈 해결

이제는 단순히 블랙리스트의 시그니처 방식만으로는 쏟아져 나오는 악성코드에 모두 대응이 불가능하다. 따라서 시그니처 방식을 보완하는 다양한 방법을 사용해야 하나, 기존의 PC에 모든 엔진과 기능을 내리고 실행하는 것은 PC 환경의 다양성, PC의 사양, 오진 등 또 다른 문제를 야기시킨다. 따라서 안티바이러스 개발업체에서 모든 보유 기술을 적용하기에는 제약이 있었던 것이 사실이다. 예전의 악성코드 대응 프로그램은 악성코드에 대한 모든 데이터를 PC로 다운로드 해 감염 여부를 확인한다. 반면, 클라우드 컴퓨팅 기술을 도입한 악성코드 대응 기술은 수천만 건 이상의 유형별 파일 DNA 데이터베이스를 중앙 서버에서 관리하며, 사용자가 파일의 악성 여부를 문의하면 클라우드에서 실시간으로 확인할 수 있다. 특히 많은 컴퓨팅 리소스를 필요로 하는 분석 작업을 클라우드에 있는 서버에서 수행함으로써 기존에 제품에 적용하지 못했던 수많은 기술을 적용하여 파일의 정상 또는 악성 여부를 실시간으로 판단해 줄 수 있으며, 이에 따라 기존 방식 대비 월등히 향상된 진단율을 제공할 수 있다.

· PC 리소스 점유율 감소 및 검사 속도 향상

지금까지의 안티바이러스 제품은 엔진을 PC에 다운로드 시키고 검사하는 방식을 취하고 있다. 따라서 수백만 개 이상의 악성코드 정보를 엔진에 포함해야 하므로 진단율이 높아질수록 엔진 사이즈가 커질 수 밖에 없다. 엔진 사이즈가 커지게 되면 메모리 등 리소스 점유율, 업데이트 사이즈 증가로 인해 PC가 느려지는 사용상의 불편을 겪게 된다. 또한 파일 하나하나마다 매번 수백만 개의 정보를 비교해봐야 하므로 진단율이 높아질수록 악성코드 검사속도가 느려질 수 밖에 없다.

반면, 클라우드 컴퓨팅 기술을 도입한 악성코드 대응 기술은 모든 정보를 클라우드에서 관리하고, PC에는 실제 설치되어 있는 파일에 대한 정보만 관리하면

된다. 즉, PC는 저용량의 데이터만으로도 악성코드에 대응 할 수 있게 되는 것이다. 클라우드 컴퓨팅 기술을 도입한 악성코드 대응 기술은 이러한 기술 구현을 통해 좀더 높은 진단율을 제공하면서도 메모리나 CPU 사용량을 극적으로 향상시킬 수 있다.

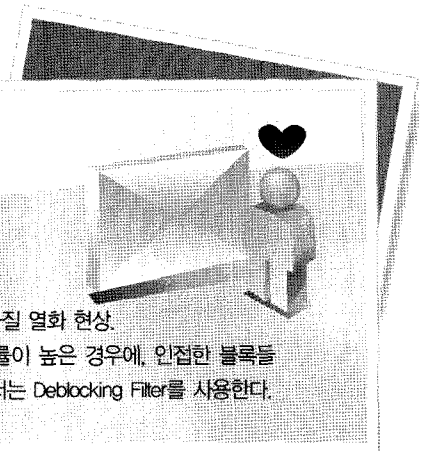
· 업데이트 관리 이슈 해결

기존의 안티바이러스 솔루션은 구조적으로 신종 파일 수집에서 배포까지 어느 정도의 시간이 소요될 수 밖에 없다. 클라우드 컴퓨팅 기술을 도입한 악성코드 대응 기술의 경우 PC에서 파일의 생성 또는 액세스가 있을 경우 서버에 악성코드 여부를 문의하는 시스템으로 서버에 새로운 정보가 업데이트되면 실시간으로 PC에 그 정보를 전달할 수가 있다. 따라서 신종 악성코드 분석 후 수분 이내에 분석 결과를 모든 PC가 활용할 수 있게 됨으로써 기존 업데이트 주기에 의한 위험을 효과적으로 감소시킬 수 있다.

6. 맺음말

악성코드 제작이 리스크가 적은 쉬운 돈벌이 수단이 되면서 많은 범죄조직이 악성코드 제작에 달려들어 점점 고도화되고 수많은 변종을 양산하고 있다. 특히 수적으로 이전에는 상상도 못할 정도의 엄청난 양의 악성코드가 생성되고 있다. 이에 대응하기 위한 안티바이러스 업체의 대응 방법도 치열해지고 있다. 그러나 기존의 시그니처 방식만으로는 현재 발생하고 있는 진단율 이슈와 업데이트 관리 이슈를 벗어나기에는 힘겨운 것이 사실이다.

따라서 이제는 더 이상 기존의 개념에서 벗어나 새로운 접근 방법이 필요한 시점이다. 새로운 개념인 클라우드 컴퓨팅 기술을 도입한 악성코드 대응 기술이 기존 시그니처 방식과 시너지 효과를 가져다 주면서 사용자들에게 좀더 안전한 컴퓨팅 환경을 조성해 줄 것으로 기대한다. TTA



정보통신용어해설

블록킹 현상

Blocking Effect, -現狀 [방송]

디지털 영상부호화를 위한 블록 단위의 양자화 과정에서 오차로 인하여 발생되는 화질 열화 현상.
블록 단위의 양자화 과정에서 각각의 블록들이 각기 독립적으로 처리되는 중 압축률이 높은 경우에, 인접한 블록들의 경계에서 불연속성이 나타나 화질의 열화를 일으킨다. 대처방안으로 H.264 등에서는 Deblocking Filter를 사용한다.