인터넷침해사고대응지원센터 분석대응팀

악성코드와 씨름하는 사람들

기자의 학창시절 중 가장 큰 고통(?)을 안겨 준 수업 시간은 화학시간이었다. 눈에는 보이지 않는, 하지만 여러 개의 분자와 원자로 구성된 성분을 어떻게 구분해야 할지, 또 눈에 보이지 않는 성분이 도무지 이해되지 않았던 탓이었다. 악성코드나 웜·바이러스를 대하는 일반인들의 심정도 그러하지 않을까. 같아 보이지만 서로 다른 악성코드와 웜·바이러스. 분석대응팀은 그 미세한 차이를 구별하고 분석하는 일을 한다.

글 · 사진 정보보호뉴스 취재팀

인터넷침해사고대응지원센터의 각 팀들은 서로 유기적으로 얽혀있다. 침해사고에 대응하기 위해 365일 24시간 국내 네트워크와 시스템의 이상징후를 모니터링하는 팀이 있는가 하면, 사고발생 시 현장으로 급파돼 문제를 해결하는 팀도 있고, 또 어떤 팀은 침해사고가 확산되지 않도록 여러 기관 및 기업들과 공조를 유지하는 팀도 있다. 분석대응팀은 주로 해킹대응팀이나, 상황관제팀을 통해 접수된 악성코드나 웜·바이러스 등의 코드를 수집하고 분석하는 것이 첫 번째 임무다.

"악성코드 분석이요? 노동집약적인 업무죠"

"일반인들은 웜·바이러스나 최근 등장하는 악성코드의 종류가 그리 많지 않을 것이라고 생각하실 거예요. 하지만 질병 중에서도 변종이라는 것이 있듯, 악성코드와 웜·바이러스 역시 다양한 변종이 있고, 형태도 모두 조금씩 다르죠." 인터넷침해사고대응지원센터 분석대응팀 류찬호 팀장은 분석대응팀을 악성코드와 씨름하는 사람들이라고 소개한다.

일반적으로 악성코드 분석은 초동분석과 상세분석으로 구분된다. 악성코드의 유무를 판단하고 긴급조치가 필요한 지 여부만을 간단하게 조사해 관련 팀에서 알려주는 것이 초동분석이라면, 악성코드가 컴퓨터에서 어떤 나쁜 행위를 하는지 또 어떻게 삽입됐지 등을 구체적으로 파악하는 것은 상세분석 과정에서 이뤄지게 된다. 그럼 악성코드를 분석하는데 걸리는 시간은 과연 얼마나 될까. "평균을 내는 것은 정말 어려워요. 간단하게 분석되는 경우 4~5시간이 지나면 그 결과가 나오기도 하지만, 어떤 것은 일주일씩 소요되기도 해요" 라는 류 팀장은 심지어는 하나의 악성코드를 분석하는데 한 달 이상이 필요할 때도 있다고 한다. 특히, 악성코드 20~30개가 특정기간동안 집중되면 10명의 분석대응팀 원들은 그

야말로 숨 쉴 틈 없이 바빠진다고 한다.

"일반인들이 생각하는 것처럼 몇 가지 분석 툴을 이용해 간단하게 분석되는 것은 거의 없어요. 특히, 최근의 봇은 전파방법이나, 악성행위 기법이 교묘하고 치밀해져 분석과정이 쉽지 않죠." 그러면서 류 팀장은 악성코드나 웜·바이러스 분석업무가 노동집약적인 업무라고 덧붙인다.

진화하고 있는 악성코드

그렇다면 교묘해지고 또 치밀해지는 악성코드에는 어떤 것들이 있을까. "정말 다양하죠. 해커가 특정 서버에서 악성코드에 감염된 PC에게 악성행위를 지시하는 사례는 들어보셨을 거예요. 최근에는 여기에서 한발 더 나아가 특정 서버를 두지 않고 악성코드에 감염된 PC가 서버가 되기도 하고, 감염 PC가 되기도 하는 P2P 봇이라는 녀석이 등장하고 있어요" 라는 류 팀장은 컴퓨터 바이러스 백신 프로그램에는 잡히지 않는 은닉형 악성코드가 '득세'를 하는가 하면, 미디어플레이어와 휴대전화 기기에 삽입되는 악성코드들이 등장하는 등 IT 기술의 진화 속도만큼 악성코드의 기법도 발전하고 있다고 한다. 물론 그로 인해 요구되어지는 보다 효과적이고 또 효율적인 분석방법의 모색도 이들 분석대응팀의 몫이 된다.

이런 분석대응팀이 최근 관심을 갖는 악성코드 분석기술은 행위 기반으로 악성코드를 자동 필터링하는 기술이다. "대부분의 바이러스 백신은 악성행위의 패턴을 분석해 업데이트를 하는 방식을 취하지만, 최근의 악성코드는 너무나 많은 변종이 등장함에 따라, 패턴 기반 이외에도 악성 행위를 자동화된 분석 툴을 통해 탐지하는 기술을 연구하고 있어요" 라고 류 팀장은 설명한다.

분석대응팀의 악성코드에 대한 효과적인 대응 노력은 이 뿐만이 아니다. "웜·바이러스나 악성코드가 삽입되는 것은 소프트웨어가 가진 취약점에서 출발해요. 특히, 우리가 정상적인 프로그램으로 간주하는 소프트웨어들에서도 얼마든지 발생할 수 있습니다. 악성코드에 대한 예방적 차원에서 그리고 정보보호 측면에서 소프트웨어들의 완성도를 살펴보려고 해요" 라는 류 팀장의 말 속에서 악성코드 대응활동을 위한 이들의 진정성이 느껴진다. S

◀ 인터넷침해사고대응지원센터 분석대응팀 류찬호 팀장은 "갈수록 치밀해지고 교묘해지는 악성코드를 분석하기 위해서는 대응기술도 예방차원에서 점차 고도화되어야 해요. 행위 기반의 탐지기술을 접목하거나, 이미 잘 알려져 있는 소프트웨어의 취약점을 다시 한번 점검해 보는 노력이 그 예들이죠"라며 악성코드에 대한 발전된 대응기술을 선보일 것이라고 강조한다.