적은 IT 자산으로, 최대의 악성코드 샘플을

KISA, 악성코드 수집 시스템 및 방법 특허등록 완료

웜·바이러스, 애드웨어, 스파이웨어 등은 시도 때도 없이 등장한다. 이들 악성코드는 매번 고유한 소스코드를 통해 시스템의 취약점을 노린다. 또 악성코드는 시간과 장소를 가리지 않는다. 반면, 국내 유관기관과 보안 업체들이 가진 한정된 인력과 분석 툴만으로는 신속하고 다양해지는 웜·바이러스에 대응하기 어렵다. 왜냐하면 이들 악성코드에 대응하기 위해서는 새롭게 등장한 악성코드를 신속하게 찾아내 분석해야 하기 때문이다. 문제는 시간과 수집능력의 싸움이다. 상황이 이런 가운데 KISA가 지난 2005년 특허출원을 신청한 악성코드 수집 시스템 및 방법이 지난 5월말 특허 출원을 마쳤다고 한다. 적은 IT 자산을 통해 최대한 많은 악성코드 정보를 자동수집할 수 있는 이 특허 기술을 살펴보자.

| 편집자 주 |

실시간 악성코드 샘플수집에서 위협분석까지

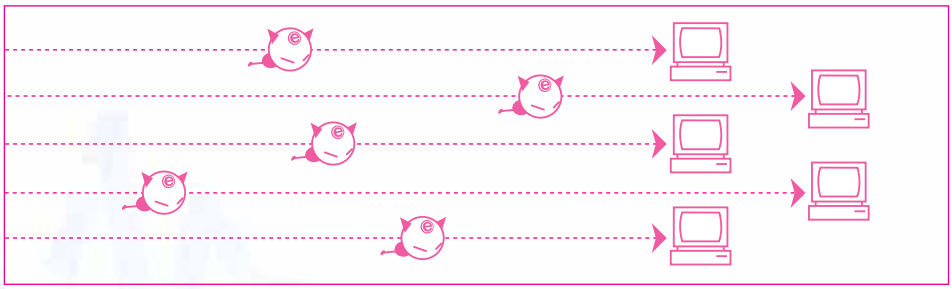
김지상 | 분석대응팀 선임연구원 jisang@kisa.or.kr

대개 악성코드는 인터넷 사용 중 사용자가 인지하지 못하는 사이에 컴퓨터에 설치된다. 현재의 악성코드 확산추세를 감안해 보면, 컴퓨터 3대당 한 대 꼴로 감염이 돼 있는 것으로 파악되고 있다. 이런 상황에서 과거에는 악성코드에 감염된 사용자 즉, 바이러스나 웜에 컴퓨터가 감염된 사용자가 KISA와 같은 대응기관이나 일반 백신업체에 신고함으로써 악성코드 샘플을 채취할 수 있었지만, 이런 방법은 악성코드의 수가 감당할 수 없을 정도로 크게 증가함에 따라 효과적인 대응책으로서의 기능을 상실했다. 특히 각종 침해사고에서 볼 수 있듯, 악성코드가 등장해서 확산되는 시점까지 걸리는 시간이 점점 짧아지고 있다는 점에서 기존의 수동적인 방법으로는 더더욱 한계가 느껴지는 상황이다.

KISA가 지난 5월 특허등록을 완료한 '악성코드 수집 시스템 및 방법'은 단시간 내에 대량의 악성코드 수집을 위한 다중 IP 환경과 감염된 PC에서 악성코드 샘플을 자동으로 추출하는 방법을 주요내용으로 한다. 특허기술의 가장 큰 특징은 취약한 상태의 PC를 인터넷에 고의로 노출시킴으로써 악성코드에 감염되게 한 후 샘플을 자동 채취하는 방법이며, '다중 IP' 환경을 이용해 적은 수의 시스템으로도 대량의 악성코드 수집하는 방법이다.

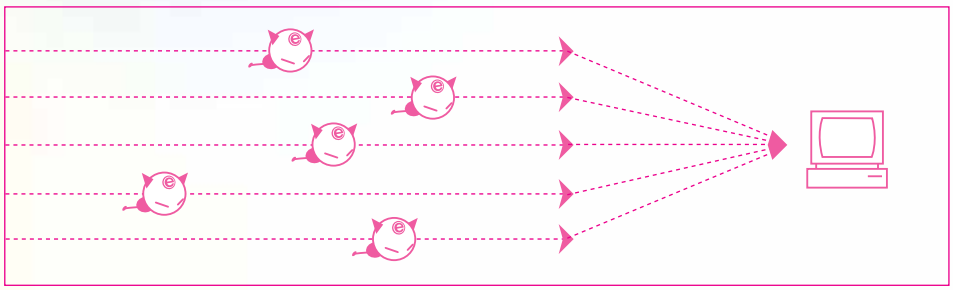
짧은 시간으로 최다 악성코드를 수집하라

우선, 단시간에 악성코드를 대량으로 수집하기 위한 '다중 IP 환경'에 대한 설명이 필요할 것이다. 기존의 악성코드 수집 단계에서 호스트에는 단일 IP가 설정되며, 악성코드는 셋팅된 호스트의 IP를 통해 취약 PC에 침투하는 과정을 거치게 된다. 때문에 악성코드 감염비율을 N배로 효율을 높이기 위해서는 그에 상응하는 N개의 추가 호스트가 필요하게 된다.



▲ 그림 1 수집효율을 N배 개선시키기 위해 N개의 수집 호스트 추가 필요

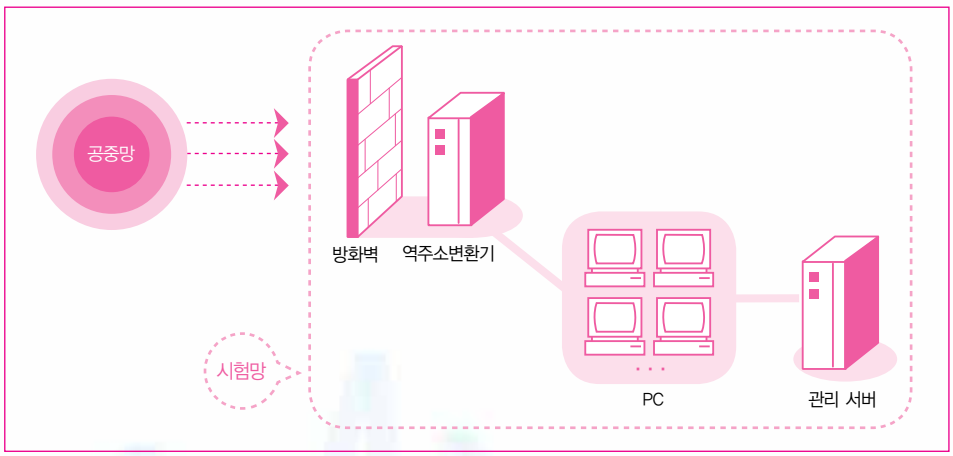
반면, 단시간 내에 대량의 악성코드 수집을 위한 다중 IP 환경은 네트워크 트래픽의 IP 치환 기술을 이용한 것으로, 아래와 같이 네트워크 단에서 IP 주소를 치환하시켜 줌으로써, 단일 호스트가 마치 N개의 호스트인 것과 같은 효과를 얻을 수 있게 하는 것이다. 여러 목적지를 가지는 유해 트래픽을 하나의 샘플 수집용 호스트에 전송되도록 함으로써, 샘플 수집을 극대화할 수 있다.



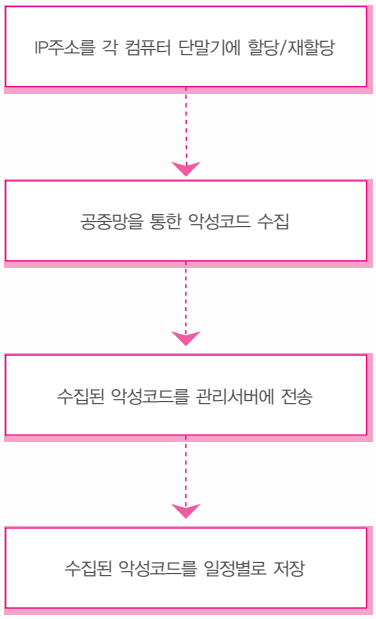
▲ 그림 2 목적지 IP치환을 통해 다중 IP사용 환경을 구현할 경우, 하나의 수집 시스템이 N개의 수집 시스템 역할 가능

RNAT를 이용한 역주소변환 기술 핵심

이번 기술을 구현하기 위해서는 그림 3에서 볼 수 있는 것처럼 흔히 인터넷망이라고 불리는 공중망에 접속된 별도의 시험망을 구성하게 된다. 시험망의 구성은 취약점을 가진 시스템을 공중망에 노출시키게 되며, 서버로부터 정보를 수집하기 위해 PC가 추가로 배치된다. 이때 PC는 IP 주소를 확보하게 되며, 공중망을 통해 유입되는 악성코드나 해커에 의한 침입 및 공격 등에 따른 공격기법을 수집하는 시험망에 설치된다.



▲ 그림 3 악성코드 수집 시스템 개요



▲ 그림 4 악성코드 수집 4단계

시험망은 공중망에 접속할 수 있는 다수의 IP 주소를 그룹단위로 내부 PC에 매핑시키는 역할을 하는 역주소변환기(이하 RNAT : Reverse Network Address Translator)와 역주소변환기에 의해 변화된 그룹 단위의 내부주소에 매핑돼 실질적으로 다수의 IP 주소를 공중망에 노출시킬 수 있는 설치 가능한 수의 PC와 방화벽을 설치하게 된다.

기존의 NAT(Network Address Translator)를 이용해 IP 주소를 그룹으로 매핑시키는 RNAT 기술은 추가 장비설치 없이도 기존 장비를 재조정해 구성할 수 있어, 추가재원이 소요되지 않는다는 장점이 있다. 여기에서는 5대의 PC에 600개의 IP 주소를 할당하는 것을 가정했으며, 일정시간이 지난 후에는 다시 IP 주소를 새롭게 설정함으로써, 적은 수의 PC로도 많은 수의 IP를 확보해 악성코드를 수집할 수 있게 했다.

이와 같은 기술은 PC가 허용할 수 있는 IP 주소의 매핑 크기에 따라 더 많은 IP 주소가 매핑될 수 있고, 또 RNAT를 통해 주기적인 IP 주소 전환이 가능하다는 점에서 다량의 IP 주소 확보를 가능하게 만든다. RNAT 기술은 취약점을 가진 서버 앞단에 방화벽을 설치함으로써 가능해지는데, 방화벽이 가진 NAT 기능을 응용해 역주소변환 기능을 구현하게 되며, 필요 시 PC의 성능 및 단말기 각각에 형성된 트래픽을 고려해 불균등할당도 이뤄질 수 있다.

이렇게 설정된 시스템은 공중망에 확산된 악성코드를 600개의 IP 주소 일부 또는 전체를 통해 수집하게 된다. 물론 수집 호스트가 악성코드에 감염되게 되면, 악성파일은 자동으로 채취된다.

한편, 악성파일의 자동채취는 파일 생성 이벤트 모니터링을 통해 이루어진다. 즉, 파일생성 이벤트 발생을 실시간으로 모니터링하고, 이유 없이 생성되는 파일을 추적해 채취하도록 함으로써 관리자 개입 없

▲ 그림 5 수집 샘플 저장 예시

이도 악성코드가 자동으로 수집되도록 한다. 또한, 유입주기를 확인해 위험도를 측정할 수 있으며, 수집된 웜·바이러스는 관리 서버를 이용해 일자별로 저장 관리함으로써 악성코드의 유포시기 등을 파악할 수 있게 된다.

▲ 그림 6 수집된 샘플 예

▲ 그림 7 악성코드 모니터링 화면

악성코드 수집 시스템, 2008년 지금도 유효한 기술

최근 등장하는 각종 침해사고에서 볼 수 있듯, 악성코드가 등장한 시점에서 확산되는 시점까지 걸리는 시간이 매우 짧아지고 있다는 점에서 기존의 수동적인 방법으로는 분명 한계가 있다. KISA는 갈수록 지능화 고도화되고 있는 악성코드에 대한 효과적인 대응을 위해 이번에 소개한 악성코드 수집 시스템을 활용해 예방활동은 물론, 활용범위를 확대하고 있는 실정이다.

이번 특허출원을 하게 된 기술은 지난 2005년 개발돼 현재 KISA 내부에서 악성코드 대응을 위한 귀중한 도구로 자리잡고 있으며, 2008년 지금 이 순간에도 백신업체의 패턴 업데이트를 위한 샘플지원 등 악성코드 확산 방지의 중요한 수단으로 활용되고 있다.

또 단순한 악성코드를 수집하는 데 그치는 것이 아니라, 이번 특허기술을 악성코드에 대한 종합적인 대응이 가능하도록 개선해 나갈 예정이다. 특히, 진화하는 악성코드에 효과적으로 대응하기 위해 수집샘플의 관리를 체계화하고 분석대응 업무처리를 자동화해, 기존보다 정확하고 신속하게 악성코드 위협에 대응할 수 있도록 할 예정이다. 악성코드는 해킹공격 시 대부분 중요역할을 하는 불법 도구로 악용되게 되므로, 사용자 감염피해 최소화를 위한 보안업체 및 유관기관의 지속적인 노력과 관심이 필요하다. S