情 報 保 護 學 會 誌
第20卷 第2號, 2010. 4

클라우드 컴퓨팅 기반의 악성코드 대응 방법 및 사례

김 정 훈*, 황 용 석**, 김 성 현***, 조 시 행****

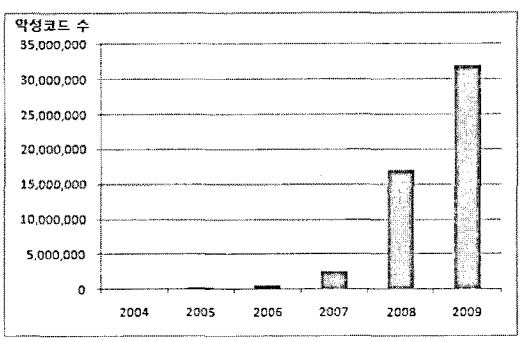
요 약

오늘날 안티바이러스 분야는 다양한 도전에 직면해 있다. 악성코드의 수 자체가 급격히 증가하고 있고, 첨단 기술로 무장하여 루트킷 등으로 자신을 은폐하기도 하며, 널리 사용되는 애플리케이션의 취약점을 이용하여 침입하고, 보안 프로그램의 동작을 방해하기 까지 한다. 이런 상황에서 클라우드 컴퓨팅은 악성코드에 대응함에 있어 새로운 패러다임을 가져왔다. 그 결과 폭발적으로 증가하는 악성코드의 수에 효과적으로 대응할 수 있게 되었다. 뿐만 아니라 샘플과 위협 정보 수집 방식의 변화와 악성코드 분석 방식의 변혁이 이루어졌다. 이를 기반으로 의심 파일의 신고와 수집을 자동화하고 다각도로 분석하여 위협에 대응하는 것이 실시간으로 이루어 질 수 있게 되었다. 본 논문에서는 안철수연구소의 클라우드 기반 보안 서비스인 AhnLab Smart Defense(이하 ASD)의 사례를 통하여 클라우드 컴퓨팅 기반의 악성코드 대응 방법을 살펴본다.

Ⅰ. 서 론

2008년부터 악성코드의 수가 급격히 증가하기 시작하였다. 인터넷 상에서 어렵지 않게 구할 수 있는 악성코드 자동 제작 툴로 쉽게 제작하고 배포할 수 있기 때문인 것으로 분석된다[1][2]. 악성코드 수의 증가는 배포되는 시그니처 엔진 크기의 증가로 직결된다. 이는 네트워크에 부하를 주고 메모리와 같은 단말의 자원을 과하게 점유하는 결과로 이어진다. Generic Detection과 같이 하나의 룰로 다수의 악성코드를 탐지하려는 노력이 계속되고 있지만, 폭발적으로 증가하는 악성코드의 수에 대한 근본적인 해결책은 되지 못하고 있다.

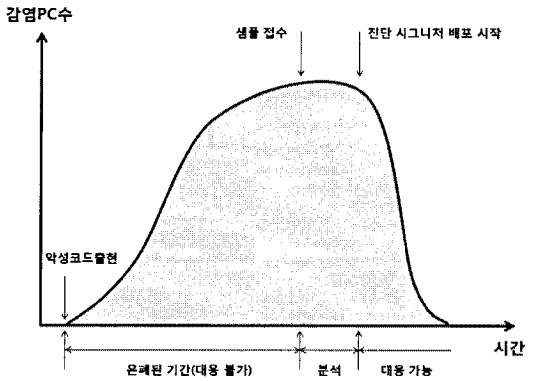
2005년부터 악성코드 제작 목적이 금전적 이득을 취하기 위한 것으로 본격적으로 바뀌기 시작하였다[3]. 금전적 이득이 목표가 되면서부터 시스템을 손상시키거나 느려지게 만드는 등의 악성행위가 줄어들고, 탐지되지 않기 위하여 루트킷 기술을 사용하여 은폐되는 경우가 늘어나기 시작했다[4]. 악성코드가 은폐되거나 은밀히 활동하여 발견이 어려워지면 악성코드의 샘플 수집에 오랜 시간이 걸리게 되고 결과적으로 대응이 늦어진다. 폭증한 악성코드의 수와 은폐되거나 분석을 방해하는 등 고도화된 악성코드 제작 기법, 불완전하고 늦게 수집되는 샘플은 악성코드의 분석과 대응을 한층 어렵게 한다.



〔그림 1〕 급격히 증가하는 악성코드 수[2]

클라우드 컴퓨팅은 로컬 PC나 스마트폰과 같은 단말의 소프트웨어나 자원을 사용하는 대신 인터넷을 통하여 광범위하게 공유된 자원을 활용하는 컴퓨팅 방법이다[5]. 안티바이러스 분야에서는 단방향으로 배포되는 시그니처 엔진을 사용하는 대신 실시간으로 인터넷을

* 안철수연구소 기반기술팀 수석연구원 (kimjh@ahnlab.com)
** 안철수연구소 기반기술팀 선임연구원 (hwang@ahnlab.com)
*** 안철수연구소 기반기술팀장 (shkim@ahnlab.com)
**** 안철수연구소 연구소장 (shcho@ahnlab.com)



〔그림 2〕 악성코드가 은폐된 경우 대응까지 소요되는 시간과 피해정도

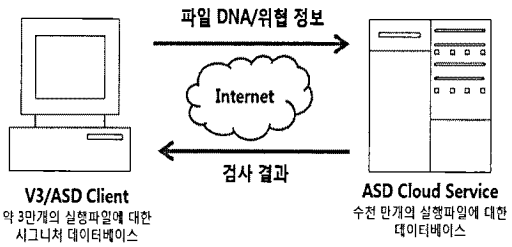
통하여 서버에 악성여부를 질의하는 방식으로 클라우드 컴퓨팅을 적용하고 있다. 2008년 맥아피의 아르테미스 기술[6]을 필두로 여러 회사에서 클라우드 기반의 안티바이러스 기술을 발표하고 있으며 안철수연구소에서는 2009년 상반기 AhnLab Smart Defense란 이름으로 기술을 발표하고 V3 제품군에 탑재하기 시작하였다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 클라우드 컴퓨팅 기반의 악성코드 방법에 대해서 설명하고, 3장에서는 악성코드 대응을 위한 클라우드 시스템의 설계와 구현에 대해서 설명하다. 마지막 4장에서는 결론 및 향후 발전 방향에 대해서 논의한다.

Ⅱ. 클라우드 컴퓨팅 기반 악성코드 대응 방법

클라우드 기반의 악성코드 대응 방법은 악성코드에 대한 시그니처 데이터베이스를 모두 PC에 다운로드한 후 처리하던 방식과 달리 필요할 때 마다 서버에 질의를 통해서 대응하는 방식이다. 악성코드의 수는 수천만 개에 달하는 반면 일반 PC나 서버와 같은 단말에 존재하는 검사 대상 파일 수는 2~3만개 정도 밖에 되지 않기 때문에 네트워크 트래픽이 적고 단말에서 차지하는 자원의 양도 상대적으로 매우 적다. 또, 악성코드의 수는 폭증하고 있지만, 실제 개별 단말에서 검사해야 하는 파일의 수는 보통 일정하게 유지되기 때문에 악성코드가 빠르게 증가하는 문제에 대해 근본적인 해결이 가능하다.

과거와 달리 지금은 서버뿐만 아니라 PC와 노트북 심지어 스마트폰까지 대다수의 단말이 동작하는 동안 상시적으로 유/무선으로 인터넷에 연결되어 클라우드

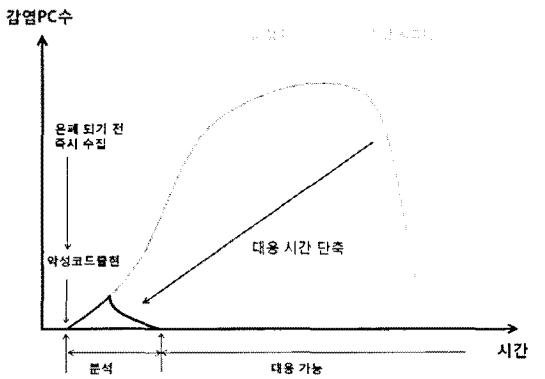


〔그림 3〕 인터넷을 통한 악성코드 검사

기반으로 악성코드에 대응할 태세가 되어있다. 또, USB메모리와 같은 이동식 저장장치를 통해 전파되는 일부 AUTORUN 타입의 악성코드를 제외한 상당수의 악성코드는 네트워크를 통해서 시스템에 유입되기 때문에 인터넷이 가능한 경우에만 동작할 수 있다는 클라우드의 제약사항은 극복가능 하다. 더욱이 이 제약은 유행하는 악성코드에 대해서 별도의 전통적인 방식의 시그니처 엔진을 배포하거나 사전방어기술을 사용하여 적절히 대처가 가능하다.

클라우드 기반이 도입되면서 단말과 서버 간에 상시적인 커뮤니케이션 채널이 생겼다. 이것은 악성코드 시그니처 엔진의 배포에 의한 위협 대응이라는 단방향 커뮤니케이션에서 개별 단말이 단말에서 발생한 의심 사항을 서버에 질의하고 서버는 질의된 사항을 분석하고 실시간으로 응답하는 양방향 커뮤니케이션으로의 변화를 의미한다. 사용자에 의하여 위협이 발견되었을 때 대응을 시작하는 것이 아니라 위협이 발생한 즉시 탐지하고 대응을 시작할 수 있게 된 것이다. 이런 특성은 은폐되거나 악성코드를 생성하는 본체를 삭제하는 등의 행위로 분석과 탐지를 회피하는 악성코드의 대응에 효과적으로 적용될 수 있다. 예를 들면 시스템에 분석되지 않거나 의심스런 경로로 생성 된 실행파일에 대해서 즉시 클라우드 서버로 분석을 요청하는 것이다. 의심스런 부분(예를 들면 .jpg 확장자를 가지는 실행파일)을 발견하는 즉시 분석 요청이 이루어지기 때문에 과거에는 불가능 했던 악성코드가 자신을 은폐하거나 삭제하기 전에 해당 악성코드를 분석하고 대응할 수 있는 기회를 가질 수 있게 되었다.

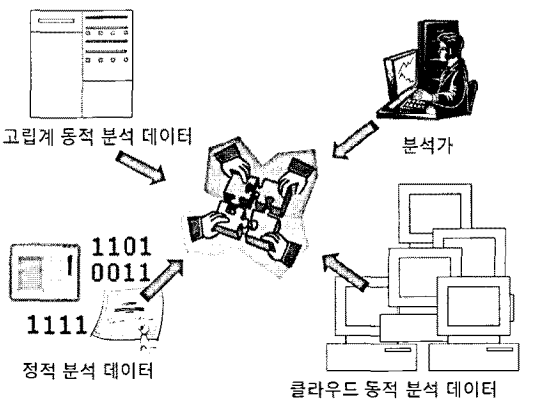
양방향 커뮤니케이션이 가능해 짐에 따라 단말에서 발생하는 의심행위를 클라우드를 통하여 실시간으로 분석할 수 있게 되었다. 분석을 요청하는 의심행위로는 부팅 시 또는 특정 시점에 자동으로 실행되도록 하는 레



〔그림 4〕 은폐된 악성코드를 포함한 위협 정보의 실시간 수집으로 단축된 대응 시간과 피해

지스트리 설정 여부와 AUTORUN과 같은 각종 설정 값, 시스템의 보안 수준을 낮추는 행위, 자신을 은폐하는 행위, 타 프로세스에 코드나 모듈을 인젝션 하는 행위, 코드 영역이 아닌 스택이나 힙 영역에서의 코드 실행 등과 같이 악성코드가 수행하는 특이 행위를 전송한다. 샘플과 위협 정보가 실시간으로 서버에 집중되면서 악성코드에 대한 다각적인 분석이 가능해졌고, 분석 품질 향상과 대응시간의 단축이 가능해졌다.

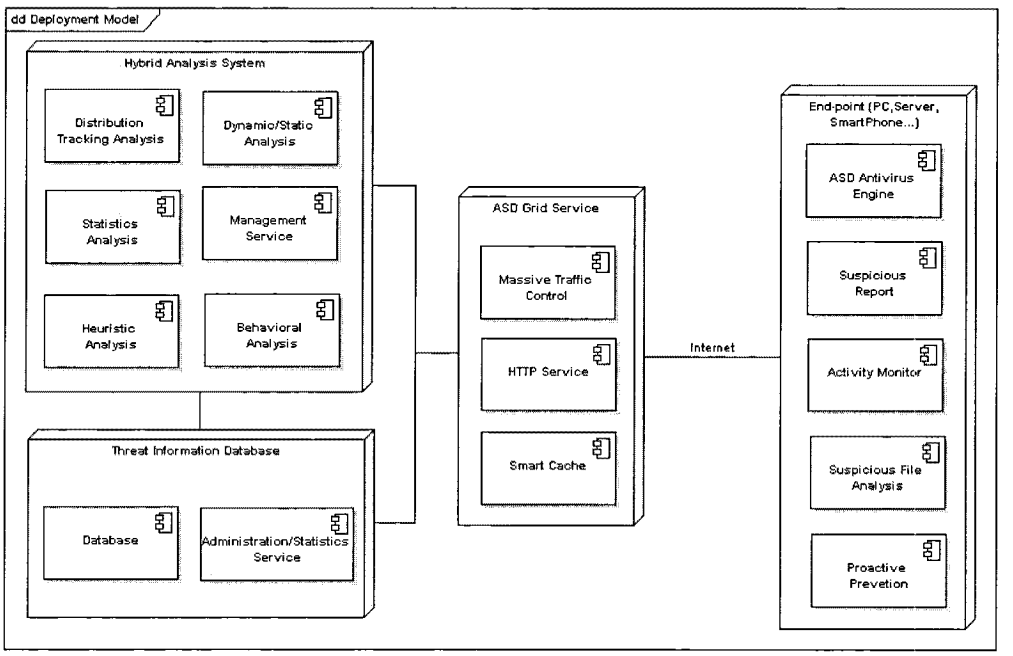
악성코드가 폭증하면서부터 악성코드 분석방법이 분석가에 의한 직접적 분석에서 시스템에 의한 자동분석으로 전환되고 있다. 기존의 자동분석시스템은 주로 수집된 샘플을 동적 행위 요소를 분석하는 시스템에서 실행을 통하여 분석을 수행하였다. 이 시스템은 완전히 고립된 환경을 제공하기 때문에 이 시스템에서 분석된 정보는 완전히 신뢰가능 하다. 반면, 시스템이 사용자 환경과 다른 가상환경과 같은 어떤 제한된 플랫폼이기 때문에 상당수의 샘플은 동작하지 않는 제약이 있다. 또한, 복수의 샘플로 구성된 악성코드 같은 경우에도 실행이 되지 않아 분석이 되지 않기도 하였다. 클라우드 기반에서는 양방향 실시간 통신이 가능하기 때문에 단말에서 발생한 의심행위를 서버에 즉시 질의해 볼 수 있다. 예를 들어 A라는 프로세스가 B라는 실행 파일을 자동 실행되도록 레지스트리 정보에 등록한다고 가정해 보자. 단말에서는 자동 실행 가능한 레지스트리에 등록하는 행위를 탐지하고 서버에 질의를 한다. 서버는 레지스트리에 등록되려는 실행 파일 B에 대한 정보와 해당 행위를 요청하는 단말의 수에 대한 통계정보, 그리고 프로세스 A에 대한 정보를 사용하여 해당 행위에 대한 악성여부를 판단할 수 있게 된다. 최근 서로 다른 악성코드를 조합한 공격이 늘어나면서 이와 같은 접근 방법은 효과적인 탐지 방법이 된다. 서로 다른 단말에서 발생한 서로 다른 행위 정보를 통합하여 분석함으로써 과거와는 다른 시각에서 분석이 가능하다. 퍼즐의 한 조각만을 보고 전체 퍼즐 그림을 추정하는 것이 과거의 방식이었다면, 클라우드 기반의 방식에서는 퍼즐의 조각을 가능한 많이 모아서 한 번에 전체를 추정하는 방식이라고 할 수 있다.



〔그림 5〕 다양한 소스로부터 얻어진 분석 데이터를 실시간으로 통합하여 악성여부를 판단할 수 있다.

Ⅲ. 악성코드 대응을 위한 클라우드 시스템의 구현 사례

안철수연구소에서 구현한 악성코드 대응을 위한 클라우드 시스템은 크게 단말 쪽 컴포넌트와 서버 시스템으로 나눌 수 있다. 단말 쪽에는 검사 대상 파일 탐지와 의심 행위 탐지, 파일 DNA 추출, 네트워크 질의 등 위협이 될 수 있는 것을 탐지하고 서버에 질의하는 기능이 들어간다. 이 때 고려되어야 하는 사항은 다음과 같다. 수천만 명이 사용될 시스템이므로 서버 쪽이 뛰어난 성능을 발휘 할 수 있도록 클라이언트가 설계되어야 한다. 불필요한 질의를 없애고 반복적인 질의가 발생할 때 빠른 응답을 얻기 위해 로컬 캐시를 두고 바이너리기반으로 프로토콜을 설계하는 등의 고려가 필요하다. 두 번째는 성능을 해치지 않으면서도 확실한 보안이다. 컴포넌트가 서버와 단말에 나뉘어있고 단말과 네트워크 구간을 신뢰하지 못하는 상황이기 때문에 보안에 대한 고



〔그림 6〕 AhnLab Smart Defense Technology Architecture

려는 매우 중요하다. 충분히 고려되지 않는 경우 ARP 스푸핑 등의 공격에 의해 쉽게 무력화될 수 있다. ASD에서는 SSL과 유사한 개념의 공개키 기반의 암호화를 통하여 이를 해결하고 있다. 세 번째 고려사항은 개인정보의 유출에 대한 것이다. 단말에서 발생한 행위나 단말에 존재하는 의심스러운 실행 파일과 같은 것을 서버에 보내서 분석하기 때문에 개인정보가 원천적으로 유출되지 않도록 데이터를 가공할 필요가 있다.

서버 쪽 시스템은 서비스 Gateway로써 단말의 엔진과 통신을 담당하는 ASD Grid Service와 위협에 대한 다각도 분석을 수행하는 Hybrid Analysis System(이하 HAS), 위협 정보 데이터베이스 등으로 구성된다. ASD Grid Server는 대규모의 사용자가 요청하는 트래픽을 고속으로 처리하기 위하여 최적화된 전용커널과 캐시 시스템 등으로 구성되어 있다. 또한 DDoS 공격 등에 대응하기 위하여 패킷 통제와 QoS 관리뿐만 아니라, 충분한 대역폭 또한 확보되어야 한다. HAS는 단말의 엔진으로부터 수집된 위협 정보와 전자서명 검증, 제작자 추적, 타 샘플과의 유사성 분석과 같은 정적 분석 결과, 고립된 환경에서의 실행을 통한 동적 분석 결과, 필요한 경우 분석가에 의한 세부적인 분석 결과를 모두 통합하여 자동으로 악성여부를 판단한다. 이들 서버들은 fail-over를 위한 이중화되어 있으며, 오류의 전파를 막고 사용자 수의 증가에 장비 대수만 늘리는 것으로 유연히 대처할 수 있도록 하기 위하여 Global Task Queue에서 작업을 꺼내서 개별적으로 처리하는 방식으로 설계되어 있다.

구현된 설계된 시스템은 단일 파일을 검사함에 있어 약 230 바이트를 사용하며, 의심 행위를 질의할 때는 약 50~500 바이트를 사용한다. 일반적인 사용 환경에서 PC의 경우 검사대상 실행파일이 2~3만개 정도 존재하므로 시스템 전체를 처음 검사하게 되는 경우에라도 5~6 메가바이트 정도의 트래픽만을 유발한다(두 번째 검사부터는 로컬 캐시의 정보를 사용하기 때문에 사용하는 트래픽이 현저히 줄어든다). 검색 포털의 첫 페이지에서 발생하는 트래픽이 500 킬로바이트에서 1 메가바이트 까지 발생하는 것을 비춰볼 때 적절한 수준으로 초고속망으로 연결되지 않은 경우에도 충분히 사용할 수 있다. 또한 스마트폰의 경우 PC와 비교해서 검사 대상 파일의 수가 현저히 적기 때문에 사용요금이 부담될 수 있는 3G망에서도 부담 없이 사용할 수 있을 것이다. 특히 스마트폰은 PC와 달리 로컬 자원이 넉넉하지 않기 때문에 그 효과는 더욱 클 것으로 예상된다.

Ⅳ. 결론 및 향후 발전 방향

지금까지 클라우드 컴퓨팅을 악성코드 대응 분야에 적용하는 방법과 사례를 살펴보았다. 클라우드 컴퓨팅 개념의 도입으로 급증하는 악성코드에 대하여 근본적인 대처가 가능하게 되었다. 그리고, 구현된 양방향 커뮤니케이션 채널을 통하여 실시간으로 위협정보를 교환 할 수 있게 됨에 따라 루트킷을 비롯한 최근의 고도화된 악성코드에도 신속히 대응할 수 있는 기반을 마련하였다. 또한 다양한 경로로 수집되는 위협 정보를 실시간으로 통합 분석할 수 있게 되어 분석 가능한 악성코드의 수가 늘었고 정확도가 향상시킬 수 있게 되었다.

클라우드 컴퓨팅은 공격이 발생한 후 처리를 시작하여 피해의 확산을 막는 것이 주목적인 안티바이러스의 개념을 거의 실시간에 준하여 대응할 수 있도록 하는 발판을 마련해 주었다. 의심 행위 탐지 기능과 행동 기반의 사전 방어 기능, Generic Detection 등이 더욱 고도화되면 신종 악성코드에도 피해가 발생하기 전에 신속하고 유연하게 대처할 수 있는 안티바이러스 시스템이 될 것이다.

참고문헌

[1] 안철수연구소, 2008년 10대 보안 위협 트렌드 발표, 2008 http://kr.ahnlab.com/company/pr/comIntroKoNDView.ahn?B_SEQ=143220.

[2] Eugene Aseev, Alexander Gostev, Denis Maslennikov, Kaspersky Security Bulletin 2009. Malware Evolution 2009, 2010 http://www.viruslist.com/en/analysis?pubid=204792101.

[3] 차민석, 악성코드의 역사 - 2005년 - 금전적 이득을 위한 제작 동기의 변화, 2008 http://kr.ahnlab.com/info/securityinfo/secuinfo/newSecuNewsView.ahn?category=001&mid_cate=001&cPage=1&seq=12681.

[4] 악성코드, 이렇게 움직인다#1 - 날 찾지마! 탐지/진단을 피하기 위한 악성코드의 발전, 2010 http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=2&menu_dist=3&seq=15722&columnist=0&dir_group_dist=0&dir_code=.

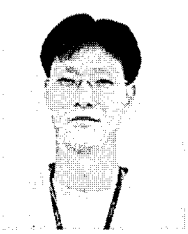
[5] wikipedia, Cloud Computing http://en.wikipedia.org/wiki/Cloud_computing.

[6] McAfee Artemis Technology http://www.mcafee.com/us/enterprise/products/artemis_technology/index.html.

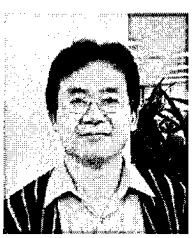
〈著者紹介〉

김 정 훈 (Jeong Kim)
2003년~현재: 안철수연구소 기반기술팀 수석연구원
<관심분야> 클라우드 컴퓨팅, 네트워크 보안, 정보보호

황 용 석 (YongSeok Hwang)
1998년 2월: 건국대학교 항공우주공학과 학사
2002년 2월: 건국대학교 항공우주공학과 석사
2004년~현재: 안철수연구소 기반기술팀 선임연구원
<관심분야> 정보보호, 단말보안, 클라우드 컴퓨팅



김 성 현 (SungHyun Kim)
1996년 2월: 국민대학교 전자공학과 학사
1998년 2월: 국민대학교 전자공학과 석사
1999년~현재: 안철수연구소 기반기술팀 팀장
<관심분야> 클라우드 컴퓨팅, 루트킷, 정보보안



조 시 행 (SiHaeng Cho)
1984년 2월: 한양대학교 건축공학과 학사
1986년~1991년: (주)쌍용컴퓨터시스템연구소
1992년~1995년: 한컴퓨터주식회사
1996년~현재: 안철수연구소 연구소장
<관심분야> 정보보호, 보안