White Paper

악성코드 대응 기술의 새로운 패러다임

AhnLab Smart Defense

Revision Version: AhnLab Smart Defense White Paper ver. 1.0

Release Date: May 26, 2009

AhnLab, Inc.
6th Fl., CCMM Bldg.
12 Yeouido-dong,
Yeongdeungpo-gu, Seoul 150-869,
Korea
82-2-2186-6000
www.ahnlab.com

Contents

1. 개요(INTRODUCTION)

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 테크놀로지 만으로는 현재와 같이 폭발적인 증가세를 보이고 있는 악성코드 이슈를 모두 해결할 수 없다. 따라서 보안 기술에 있어서 새로운 변화를 수용해야 할 시점이 되었다.

본 문서에서는 최근 악성코드의 동향을 살펴보고, 기존 대응 방법의 문제점 그리고 이를 보완할 수 있는 클라우드 컴퓨팅 개념의 악성코드 대응 기술인 AhnLab Smart Defense에 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 변형이 되었다.

- **사이버 블랙 마켓의 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 블랙 마켓에서 팔면 바로 돈이 되기 때문에 개인정보를 빼내가기 위한 악성코드의 배포가 급증하고 있는 것이다. 실제로 지난해 미국 경찰은 40만대의 컴퓨터를 감염시킨 소베라는 별명을 사용하는 청년을 검거했다. 그는 감염된 컴퓨터를 조종하는 봇넷(BotNet)*이라는 기술을 이용해 연 58만 달러를 벌어들인 것으로 알려졌다.

*** 봇넷(BotNet)**
봇넷이란 컴퓨터를 좀비처럼 만들어 사용자도 모르는 사이에 스팸이나 바이러스 등을 전파하도록 하는 악성코드를 봇(Bot)이라고 하고, 봇에 감염된 컴퓨터가 네트워크를 형성한 것을 봇넷(BotNet)이라고 한다.

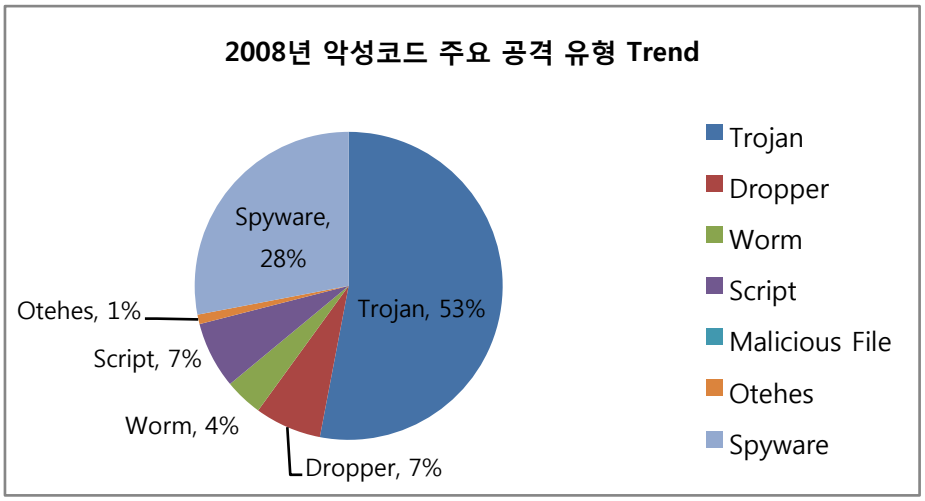
또 하나 주목해야 할 것은 컴퓨터 전문가가 아니더라도 사이버 블랙마켓을 통해 쉽게 해킹 툴이나 악성코드 제작 툴 등을 저렴한 가격에 구매하여 개인정보를 탈취해가기 위한 해킹을 할 수 있게 되었다는 것이다. 이에 따라 신종 악성코드 개수 및 해킹 시도가 폭발적으로 증가하고 있다.

한 예로 최근 중국의 해킹 사이트에서는 단 돈 $10에 피싱 사이트를 구축할 수 있고, 해킹 툴도 5만4천원에서 25만2천원 사이에 쉽게 구매할 수 있다고 광고하고 있다. 이러한 사이트는 일반인들도 손쉽게 접근할 수 있으며, 해킹 툴을 판매하는 사이버 블랙마

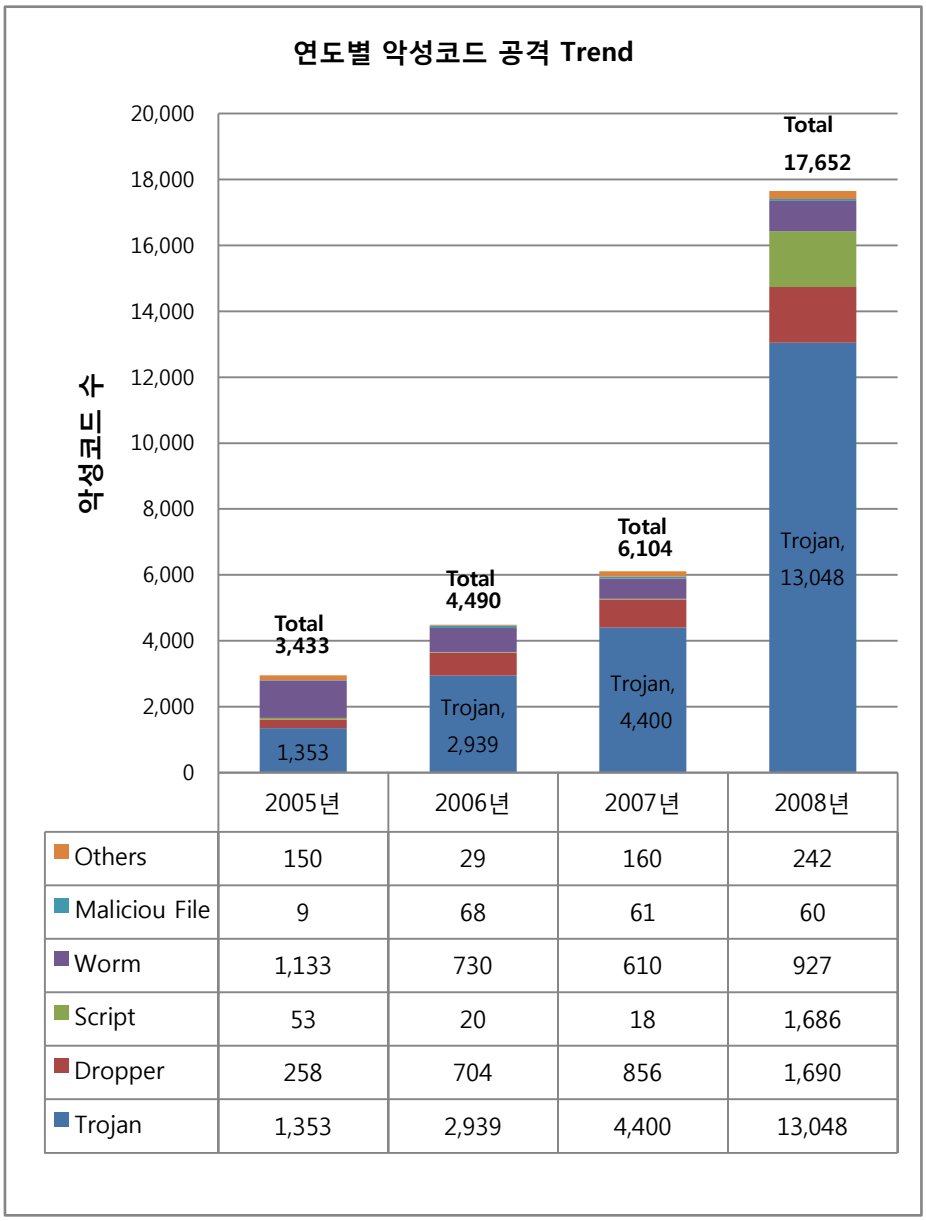
켓이 광범위하게 활성화 되고 있다.
이러한 사이버블랙마켓 활성화는 세계적인 경기 불황 및 인터넷의 보급률 증가와 맞물려 앞으로도 심각한 위협으로 작용할 것으로 보인다.

- **Trojan, Spyware, Dropper의 증가**

이러한 경향에 따라 기존에 악성코드의 대부분을 차지하던 바이러스의 비율이 줄어들고, 내부정보 유출에 악용되는 트로이목마, 스파이웨어, 드롭퍼 등의 악성코드가 급증하고 있다.



[그림 1] 2008 년 악성코드 주요 공격 유형 Trend
출처: 안철수연구소 ASEC Report (2008 년 12 월)



	2005년	2006년	2007년	2008년
Others	150	29	160	242
Maliciou File	9	68	61	60
Worm	1,133	730	610	927
Script	53	20	18	1,686
Dropper	258	704	856	1,690
Trojan	1,353	2,939	4,400	13,048

[그림 2] 2005 년 ~ 2008 년 악성코드 공격 Trend

출처: 안철수연구소 ASEC Report

특히 과거에는 악성코드 제작 목적이 자기 과시형이라 악성코드에 감염되면 바로 확인할 수 있었다. 하지만 최근의 악성코드 제작은 돈이 목적이기 때문에 악성코드도 복잡해지고 은폐기능이 고도화되어 전문가들조차도 시스템의 감염상태를 파악하기 어렵다. 그 배포방법 또한 메일, 인터넷, 취약점 공격, USB 등으로 다양해 어떻게 시스템에 감염되었는지 조차 확인할 수 없을 정도로 고도화되고 있다.

- **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 대량 생산하고 자동적으로 변종을 만들 수 있는 툴들이 악성코드 제작자들 사이에 만들어지고, 또한 거래되고 있다. 이로 인해 악성코드의 숫자가 이전에는 상상할 수 없었을 정도로 폭발적으로 증가하게 된다.

*** AV-Test.Org (www.av-test.org)**
독일의 독립 안티바이러스 연구소로 4대 국제 안티바이러스 인증 기관 중 하나로 인정받고 있다.

*** ASEC (AhnLab Security Emergency response Center)**
최고의 악성코드 분석가 및 보안전문가로 구성된 안철수연구소의 글로벌 대응조직. 매월 국내 및 전세계 보안 위협과 이에 대응하는 보안 기술의 최신 동향 보고서를 발행하고 있다.

안티바이러스 제품을 테스트 하고 있는 Av-test.org*에 따르면 신종 악성코드의 수는 2005년 333,000개, 2006년 972,000개, 2007년 5,490,000개로 증가하고 있다. 또한 ASEC* 2008 Annual Report에 의하면 2008년에도 한해 동안에만도 전세계적으로 800만개 이상의 악성코드가 만들어졌다고 한다.
이러한 전문기관의 분석 자료를 통해 알 수 있듯이 악성코드의 숫자는 이전에는 상상할 수 없는 수준으로 매년 기하급수적으로 증가하고 있다.

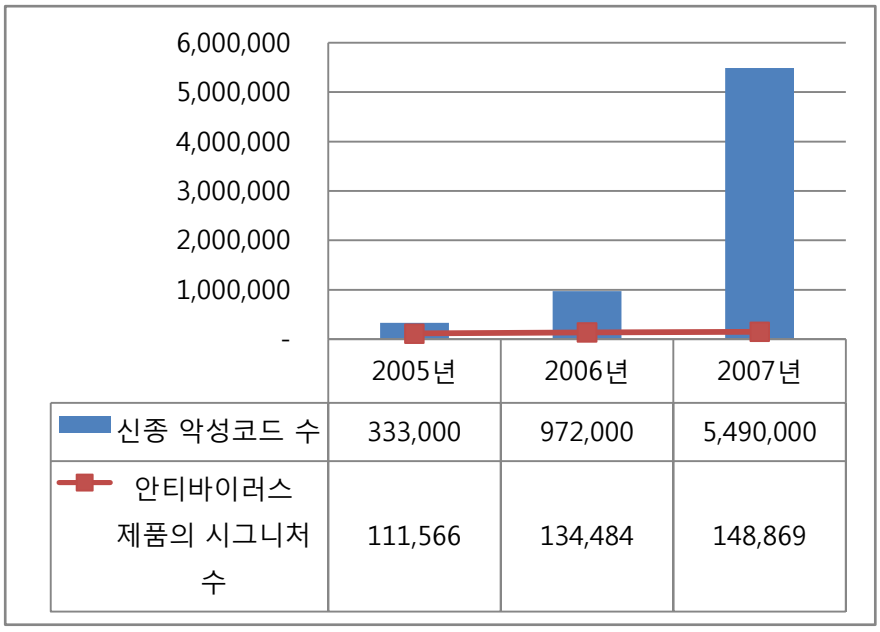
3. 현재 안티바이러스 업체의 대응 방법 및 한계점

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

Av-test.org에 따르면 45개의 안티바이러스 제품을 분석해본 결과 신종 악성코드의 수는 2005년 333,000개, 2006년 972,000개, 2007년 5,490,000개로 기하급수적으로 증가하였다. 이에 비해 안티바이러스 제품의 시그니처 수 증가는 2005년 111,566개, 2006년 134,484개, 2007년 148,869개로 신종 악성코드 수에 턱없이 못 미치고 있다.



[그림 3] 연도별 신종 악성코드 수 출처: AV-test.org

*** 블랙리스트 (Blacklist) 방식**
악성코드의 시그니처를 추출하여 이를 데이터베이스 DB 로 만드는 방식

*** Heuristic Detection**
인공지능 분야 용어로 주어진 문제의 해결을 결정적인 연산 방식에 의하지 않고 시행착오를 통해 축적된 경험적인 지식을 동원하여 구하는 것, 또는 그 경험적인 지식.

*** Proactive prevention**
과거의 학습 내용을 바탕으로 동일한 증상을 보이는 패턴이 발견되면 실행되지 않도록 사전에 예방하는 방법

*** Sandbox**
외부로부터 들어온 프로그램이 보호된 영역에서 동작해 시스템이 부정하게 조작되는 것을 막는 보안 형태

많은 안티바이러스 솔루션 개발사들이 이러한 악성코드에 대항하여 진단율을 높이기 위해 시그니처 기반의 블랙리스트(Blacklist)* 방식 이외에도 Heuristic Detection*, Proactive Prevention*, Sandbox* 등의 다양한 기법을 사용하고 있다. 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 개수 증가는 엔진 사이즈 증가와 더불어 검사 속도 증가 및 더 많은 메모리 사용을 필요로 하며, 그만큼 오진의 가능성을 높이고 있다.

- **업데이트 속도 이슈**

이렇게 악성코드의 숫자가 많아질수록 빠른 업데이트가 상당히 중요해진다. 과거와 달리 이제는 단 한 시간 업데이트가 지연되어도 수 천 개 이상의 신종 악성코드에 감염될 위험에 노출된다.

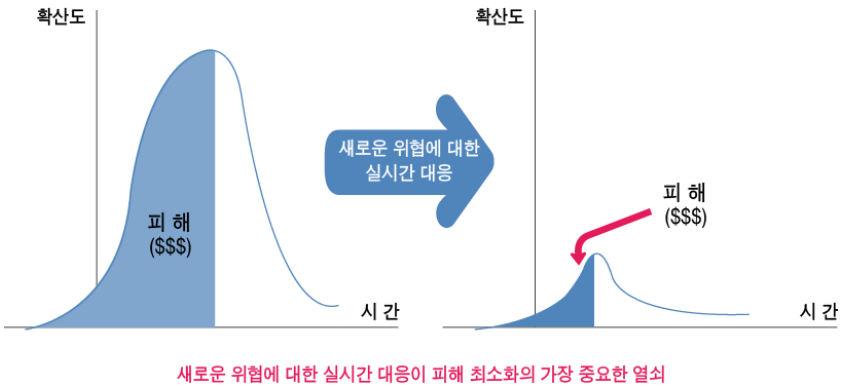
이에 따라 악성코드의 숫자의 폭발적 증가에 대응하기 위해 안티바이러스 솔루션 개발 업체의 경우 업데이트 주기를 단축하는 방법을 우선적으로 사용하고 있다. 현재 대부분의 업체에서 이전에 일주엔 한번 업데이트를 제공하던 방식에서 하루에 한번 이상의 시그니처 업데이트를 제공하고 있는 중이다. 그러나 이러한 업데이트 주기 변경 만으로는 현재의 이슈를 해결하는 것은 불가능하다.

현재 악성코드 대응 방식은 다음과 같은 문제점을 안고 있다.

- 최신 업데이트 미 적용: 사용자가 PC에 자동업데이트 설정해 놓지 않아 최신 업데이트를 적용하지 않았다면 위험에 그대로 노출
- 엔진 대응: 악성코드 출현 시 샘플 수집에서 엔진 제작까지 여러 단계를 거쳐야 하므로 이 시간 동안 위협에 무방비 노출
- 엔진 배포: 업데이트 주기를 단축하는 방법을 사용하고 있으나 업데이트 시간차에 따른 위험 여전히 존재

[그림 4]와 같이 새로운 위협에 대한 실시간 대응이 피해 최소화에

가장 중요한 역할을 하게 되는 현시점에서 기존의 안티바이러스 엔진 업데이트 방식은 개선되어야 할 당면 과제이다.



[그림 4] 실시간 대응과 피해 규모의 상관 관계

이 밖에도 대응 시그니처 수의 증가는 엔진 사이즈의 증가를 동반하고 있다. 과거 18개월간 대부분의 안티바이러스 솔루션들의 엔진 사이즈가 두 배로 증가되었으며, 심한 경우 3배까지도 증가했다고 한다. 또한 엔진 사이즈가 커지고, 업데이트 빈도가 늘어남에 따라 업데이트 사이즈도 기하급수적으로 증가하고 있다.

	2005년	2006년	2007년
45개 백신업체 업데이트 사이즈	520GB	1.0TB	1.6TB

[표] 백신업체 누적 시그니처 업데이트 사이즈 출처: AV-test.org

4. Cloud Computing 개념의 새로운 접근 방법: AhnLab Smart Defense

상기에 언급한 바와 같이 이제는 기존의 방식만으로는 악성코드의 위협으로부터 100% 안심할 수 있다고 이야기하기가 힘든 상황이 도래했다.

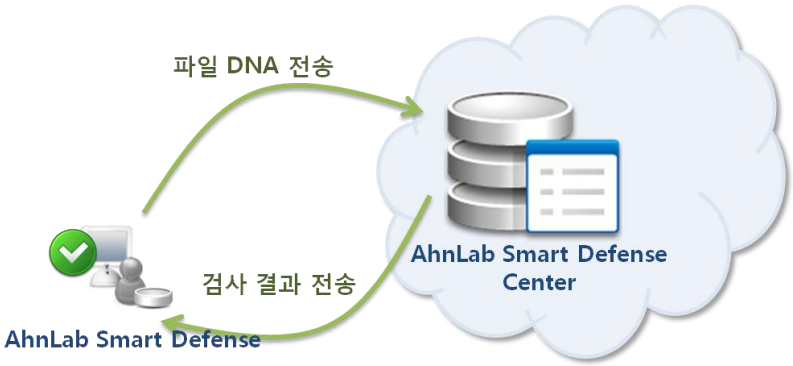
이에 대응하고자 안철수연구소에서는 AhnLab Smart Defense 라는 새로운 개념의 악성코드 대응 기술을 만들게 되었다.

AhnLab Smart Defense 는 기존에 악성코드에 대한 모든 데이터를 PC로 다운로드한 후 PC에서 처리하던 방식과 달리 Cloud Computing* 개념을 이용한 새로운 기술이다. 즉, 대규모 파일 DB를 중앙서버에서 관리하며, PC에 설치되어 있는 AhnLab Smart Defense 엔진에서 파일의 악성여부에 대해 문의하면 이에 대해 응답을 해주는 방식이다.

*** 클라우드 컴퓨팅 (Cloud Computing)**
대용량 데이터베이스를 인터넷 가상 공간에서 분산처리하고, 이 데이터를 데스크톱 PC 등 다양한 단말기에서 불러오거나 가공할 수 있게 하는 환경을 말한다.

AhnLab Smart Defense 의 작동 방법은 아래와 같다.

*** 파일 DNA**
파일 고유의 특징을 추출한 데이터.

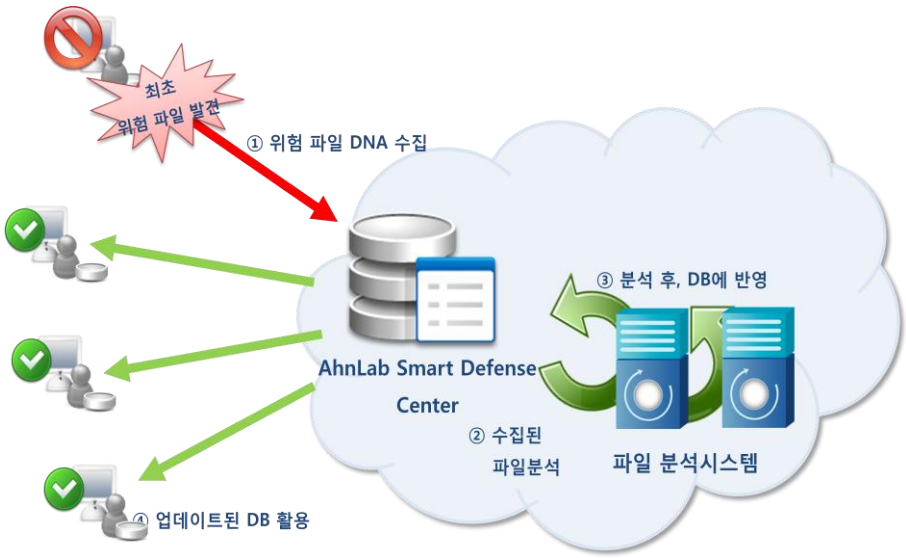


[그림 5] AhnLab Smart Defense 구성도

1. PC에 설치된 AhnLab Smart Defense 엔진을 통해 생성된 DB에서 기존에 검사한 파일인지 확인한다.

2. 새로운 파일로 확인되면, AhnLab Smart Defense Center로 파일 DNA*를 전송한다.

3. AhnLab Smart Defense Center는 전송된 파일 DNA 정보를 대용량 DNA DB에서 해당 DNA의 유형이 있는지 확인하고, 같은 유형의 DNA가 존재하면 기 분석된 DNA정보, 즉 악성코드인지 정상 파일인지 확인하여 알려준다. 만약 전송 받은 파일 DNA가 DB에서 확인이 되지 않으면, 새로운 유형으로 간주하여 분석에 필요한 파일의 특정 부분을 전송받는다. 전송받은 파일은 즉시 자동 분석 시스템으로 보내져 새로운 DNA의 악성 여부를 분석하게 된다.



[그림 6] AhnLab Smart Defense Center

4. AhnLab Smart Defense Center에서는 파일의 기본 정보, 프로그램 디지털 서명 정보 분석, 평판 시스템을 통한 분석, 파일에 대한 Activity 동향 분석, 행위 기반 Activity 분석, 파일간 Relation 분석 등 다양한 기술을 이용하여 파일의 정상 또는 악성 여부를 판단하고, 이를 AhnLab Smart Defense 엔진에 알려준다. 이와 동시에 파일 DNA DB를 업데이트하여 다른 AhnLab Smart Defense 엔진에서 활용할 수 있도록 한다.

4. AhnLab Smart Defense의 효과

앞서 현재 안티바이러스 개발업체의 대응 방법 및 한계점에 대해 언급한 바 있다. AhnLab Smart Defense 를 사용할 경우 이러한 문제들에 대한 해결이 가능하다.

- **진단율 이슈 해결**

이제는 단순히 Blacklist의 시그니처 방식만으로는 쏟아져 나오는 악성코드에 모두 대응이 불가능하다. 따라서 시그니처 방식을 보완하는 다양한 방법을 사용해야 하나, 기존의 PC에 모든 엔진과 기능을 내리고 실행하는 것은 PC환경의 다양성, PC의 사양, 오진 등 또 다른 문제를 야기시킨다. 따라서 안티바이러스 개발 업체에서 모든 보유 기술을 적용하기에는 제약이 있었던 것이 사실이다.

예전의 악성코드 대응 프로그램은 악성코드에 대한 모든 데이터를 PC로 다운로드하여 감염 여부를 확인한다. 반면, AhnLab Smart Defense는 수천만 건 이상의 유형별 파일 DNA 데이터베이스를 중앙 서버에서 관리하며, 사용자가 파일의 악성여부에 대해 문의하면 AhnLab Smart Defense Center에서 실시간으로 확인할 수 있다.
더불어 해당 데이터베이스에 없던 파일이라도 파일의 DNA를 실시간으로 수집하고, 많은 리소스를 필요로 하는 분석 작업을 서버에서 수행함으로써 기존에 제품에 적용하지 못했던 수많은 Technology를 적용하여 파일의 정상 또는 악성 여부를 실시간으로 판단해 줄 수 있으며, 이에 따라 월등히 향상된 진단율을 제공할 수 있다.
실제로 안철수연구소의 테스트 결과 단순히 Blacklist 기반의 제품만 사용했을 때 보다 AhnLab Smart Defense를 같이 사용했을 경우 20% 정도의 진단율 향상 효과를 볼 수 있었다.

- **PC 리소스 점유율 감소 및 검사속도 향상**

지금까지의 안티바이러스 제품은 엔진을 PC 에 다운로드 시키고 검사하는 방식을 취하고 있다. 따라서 수백만 개 이상의 악성코드 정보를 엔진에 포함해야 하므로 진단율이 높아질수록 엔진 사이

즈가 커질 수 밖에 없다. 엔진 사이즈가 커지게 되면 메모리 등 리소스 점유율, 업데이트 사이즈 증가로 인해 PC 가 느려지는 사용상의 불편을 겪게 된다. 또한 파일 하나하나마다 매번 수 백만 개의 정보를 비교해봐야 하므로 진단율이 높아질수록 악성코드 검사속도가 느려질 수 밖에 없다.
반면, AhnLab Smart Defense 는 모든 정보를 AhnLab Smart Defense Center 에서 관리하고, PC 에는 실제 설치되어 있는 파일에 대한 정보만 관리하면 된다. 즉, PC 는 저 용량의 데이터만으로도 악성코드에 대응 할 수 있게 되는 것이다. 또한 새로운 파일이 생성되어도 AhnLab Smart Defense Center 에 실시간으로 확인 후 해당 파일에 대한 파일 DNA 만 관리하면 되므로 새로이 유입될 가능성이 있는 악성코드 대응을 위한 별도의 데이터 관리가 필요 없게 된다.
AhnLab Smart Defense 는 이러한 기술 구현을 통해 좀더 높은 진단율을 제공하면서도 메모리나 CPU 사용량을 극적으로 향상시킬 수 있다.

- **업데이트 관리 이슈 해결**

기존 안티바이러스 솔루션이 악성코드의 발견에서 처리까지는 다음과 같은 복잡한 단계를 거쳐야 한다.

악성코드 발견에서 엔진 배포까지의 과정: 신종 파일 수집 → 파일 분석 → 증상 분석 → 정보 분석→ 코드 분석 → 엔진 제작 → 배포

이처럼 기존의 안티바이러스 솔루션은 구조적으로 신종 파일 수집에서 배포까지 어느 정도의 시간이 소요될 수 밖에 없다.
즉, 일반적으로 아무리 신속히 처리하더라도 신종 파일 수집 후 사용자 PC에 실제 업데이트 되기까지는 약 4~5시간 소요되고 있다. 그러나 과거와 달리 4~5시간은 수백 ~ 수 천 개 이상의 신종 악성코드에 감염될 위험에 노출될 가능성이 있다. 따라서 좀더 신속한 업데이트의 필요성이 강조되고 있다.
또한 관리 툴 등을 사용하여 모든 PC의 엔진을 최신 엔진으로 관리한다고 하더라도 구 버전의 엔진을 사용하는 PC는 존재하고 있기 때문에 안티바이러스 솔루션을 사용하더라도 구 버전의 엔진

에서 처리하지 못하는 수천, 수만 개의 신종 악성코드에는 무방비 상태로 노출되게 된다.
AhnLab Smart Defense 의 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. 결론

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 치열해 지고 있다. 그러나 기존의 시그니처 방식 만으로는 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 AhnLab Smart Defense 가 기존 시그니처 방식과 시너지 효과를 가져다 주면서 사용자들에게 좀더 안전한 컴퓨팅 환경을 조성해줄 것으로 기대한다.