안랩 온라인 보안 매거진

월간 安

2015. 09

Mobile Threat & Response

CONTENTS

사물인터넷 시대와 보안, 상상 속 우려가 현실되나

많은 사람들이 사물인터넷 시대가 본격적으로 도래하면 보안 문제도 증가할 것이라고 예상했다. 사물인터넷 시대가 언제쯤 열릴 것인가에 대해 얼마 전까지만 해도 아직 시간적 여유가 있다고 생각했다. 하지만 2015년 상반기에 발생한 여러 징조를 보면서 어쩌면 예상보다 문제가 빨리 일어날 수 있다는 생각도 든다.

공격자들은 이미 컴퓨터와 스마트폰뿐 아니라 다른 분야로 공격 영역을 확장하고 있다.

2014년 말 소니와 마이크로소프트의 게임 관련 사이트는 리자드 스쿼드(Lizard Squard)의 디도스 공격을 받는다. 이 공격에는 인터넷 공유기가 이용된 것으로 알려졌다. 국내에서도 인터넷 공유기의 취약점을 이용한 공격이 2014년 말부터 계속 발견되고 있다.

지난 5월에는 영화 속 이야기 같은 사건이 발생해 화제가 되었다. 워싱턴 포스트에 따르면 5월 15일 미 연방 수사국(FBI)은 크리스 로버츠(Chris Roberts)에게 비행기 해킹 혐의가 있다고 밝혔다. 크리스 로버츠는 비행기 해킹은 사실이 아니라면서 혐의를 부인하고 있다고 한다. 사실 관계 확인이 좀 더 필요하겠지만 비행기 해킹 가능성도 열렸다.

단순 해킹 시도 외 실제 장애도 발생했다. 지난 6월 21일 폴란드 바르샤바의 프레데릭 쇼팽 공항에서 비행기 이착륙이 장시간 지연되는 사건이 발생했다. 이 사건에 대해 시스템 장애, 악성코드 감염 등의 추정이 나왔지만 디도스 공격으로 인한 시스템 장애가 발생한 것으로 알려졌다. 디도스 공격이 맞다면 관련 시스템이 인터넷에 직접 연결되어 있었거나 연결된 다른 시스템에 과부하가 걸려 전체 시스템에 문제가 발생했을 수 있다. 생각보다 공항의 시스템 관리가 허술할 수 있다는 점에서 놀라운 사건이었다.

또, 7월 8일 미국에서는 유나이티드 항공 자동화 시스템에 이상이 발견돼 곧바로 이 항공사 여객기 및 연결 항공편의 이륙을 금지했다. 같은 날 뉴욕증권거래소(NYSE) 거래도 중단되고 월스트리트 저널 웹 사이트도 장애가 있었다. 연쇄 공격이 아니냐는 관측도 있었지만 원인은 단순한 시스템 장애로 밝혀졌다.

하늘뿐 아니라 땅 위의 자동차도 커넥티드 카(connected car)로 발전하면서 점차 움직이는 컴퓨터가 되고 있다. 자동차 해킹은 오래 전부터 예견되었고 이제 현실화되기 시작했다. 7월 13일 소프트웨어 버그로 65,000대의 레인지 로버(Range Rover) 차량이 리콜 되었다. 또, 피아트 크라이슬러(Fiat Chrysler)는 지프 체로키(Jeep Cherokee)의 취약점으로 140만대의 리콜을 결정했다.

이처럼 많은 전자기기가 컴퓨터화되고 프로그램으로 운영되고 있다. 불행히도 모든 소프트웨어는 잠재적으로 버그를 포함할 수 있고 설계 단계부터 보안을 고려하지 않으면 공격자들에게 더 쉽게 취약점이 노출될 수 있다. 특히 테러리스트들이 자동차, 비행기, 기차 등의 교통 시설을 해킹해 테러를 일으킬 수도 있다.

국가적으로도 사회 기반을 이루는 소프트웨어의 문제점을 진단하고 예방하기 위한 노력을 해야겠지만 기업 입장에서도 잠재적으로 발생할 수 있는 소프트웨어 문제를 해결해야 할 필요가 있다. 만약 자동차나 비행기가 소프트웨어 문제로 사고가 발생해 인명 피해가 발생한다면 해당 업체의 신뢰는 추락할 것이다. 그래도 다행인 것은 세계 완성 차 업계가 정보공유분석센터를 설립해 차량 해킹 방지를 위해 협력하기로 했다는 점이다. 하지만 규모가 큰 업체들의 이런 행보 속에 앞으로 다가올 사물인터넷 시대에 다른 제조 업체들은 어떤 준비가 되어 있을까? 전통적 제조 업체의 시각으로만 접근할 경우 변화하는 시대를 따라가지 못해 장기적으로 회사의 존망까지 위협받지 않을까 싶다.

어쩌면 소비자들도 제품을 사용할 때마다 안전에 대해 가슴을 졸이며 써야 할 시대가, 그리고 보안성이 강력하다고 알려진 제품이나 장애 또는 보안 문제가 발생했을 때 빨리 대처할 수 있는 업체의 제품을 선택하는 시대가 올 지도 모르겠다.

AhnLab ISF SQUARE 2015 for Banking

안랩, 금융 지성들과 보안 대책을 논하다

안랩은 '고객 주도형 보안(Customer driven Security)' 전략의 일환으로 고객을 찾아가 특성과 요구를 듣고 이에 최적화된 해결책(Resolution)을 고객과 함께 마련하는 AhnLab ISF(Integration Security Fair) SQUARE 2015를 진행하고 있다. 지난 6월 증권업계에 이어 8월에는 은행업계 CISO를 초청해 은행업계가 당면한 보안 이슈와 해결책을 함께 논의하는 자리를 가졌다.
은행업계 CISO와 함께 한 'AhnLab ISF SQUARE 2015' 그 두 번째 이야기를 전한다.

안랩은 8월 25일 소공동 롯데 호텔에서 은행권 정보보호최고책임자(Chief Information Security Officer, CISO)를 초청해 '자율 금융 시대의 보안 트렌드와 안랩의 대응 방안'을 소개하는 '안랩 ISF 스퀘어 2015'를 개최했다.

이 행사에는 은행업계 CISO가 참석해 자율 금융 시대의 IT 환경 변화에 따른 보안 위협과 대책은 무엇인지에 대해 의견을 나누는 자리를 가졌다.

▲ 안랩ISF SQUARE 2015 현장 모습(좌) & 행사의 취지를 설명 중인 안랩 강석균 전무(우)

안랩 강석균 전무는 "은행은 IT와 보안 인프라 측면에서 가장 앞서있는 산업이라고 해도 지나치지 않다. 은행에서는 기간계 시스템부터 고객의 PC 환경까지 고려한 IT 인프라를 갖추고 있다. 그 모든 것이 고객에게 더 나은 금융 서비스를 제공하기 위한 목적일 것이다. 오늘 이 행사가 이러한 금융 서비스를 좀 더 안전하게 구현할 수 있는 방안을 안랩과 함께 고민할 수 있는 자리가 되기를 바란다"고 말했다.

첫 번째 세션에서는 안랩 전상수 기술기획실 부장이 'PC에서 사물인터넷까지 – 자율 금융 시대의 보안을 다시 생각하며'라는 주제로 IT 흐름에 따라 보안의 관점이 어떻게 변화하고 있는지에 대해 소개했다.

전상수 부장은 "지금 우리가 살고 있는 시대는 PC와 프로그램에서 모바일과 애플리케이션으로 중심 축이 이동했다. 최근 트렌드를 살펴보면 메시징 앱이 지불(Payment) 시스템을 껴안는 시대가 되었다"며 "이제 금융 회사가 ICT(Information and Communication Technology) 기업과

경쟁할 수 밖에 없는 구도가 되었다"고 설명했다.

실제로 모바일에서도 금융 거래를 위한 앱을 별도로 설치하는 시대를 지나 카카오톡, 라인, 페이스북 등과 같은 각종 SNS 서비스에서 결제를 할 수 있는 환경으로 급속하게 변화하고 있다. 또한 IT 기술과 금융이 접목된 핀테크가 확대되면서 ICT 기업들은 기존 금융기관이 충족시키지 못한 고객을 타깃으로 신규 금융 시장 진출을 가속화하고 있다. 이들은 금융 비용 절감, 편의성과 신속성, 차별화된 서비스를 내세워 기존 금융기관의 영역을 거세게 두드리고 있다.

이러한 새로운 환경과 더불어 금융 거버넌스는 자율 금융을 확대하되 보안 사고 시 금융 회사가 책임을 져야 하는 방향으로 강화되었다.

전상수 부장은 "자율 금융 시대에서는 리스크 매니지먼트 관점에서 자산을 재평가하고, 내 • 외부 위협에 대한 공유와 협력 체계를 수립하여 고객에게 안전성과 편의성을 갖춘 서비스를 제공하는 것이 핵심"이라며 "결국 보안에 대한 철학과 수준을 갖춘 기업이 디지털 시대의 승자가 될 것이다"라고 강조했다.

▲ 안랩 전상수 기술기획실 부장(좌)과 백민경 제품기획팀 차장(우) 강연 모습

두 번째 세션으로 안랩 백민경 제품기획팀 차장의 '핀테크 시대의 보안 트렌드 변화와 안랩의 대응 방안' 강연이 이어졌다. 기업과 일반 사용자가 이미 핀테크 시대를 경험하고 있는 현 시점에서의 보안 트렌트를 살펴보고, 최근 이슈가 되는 있는 Non-Active X 그리고 2차 인증 관련 보안 위협에 대응하기 위한 방안들을 상세하게 소개했다.

백민경 차장은 "급격한 기술 발전과 더불어 새로운 패러다임의 서비스들이 등장하고 있다. 그런데 실제로 사용자들에게 피해를 입히는 건 여전히 웜, 악성코드다. 그리고 공격자의 목적 또한 사용자의 '돈'을 노리는 것이 대부분이다"라며 "이러한 측면에서 금융기관은 공격자에게 여전히 매력적인 타깃"이라고 금융 보안의 중요성을 설명했다.

이어 백민경 차장은 기존 공격은 인터넷 익스플로러와 윈도의 취약점을 노린 반면, 최근에는 다양한 애플리케이션의 취약점이 공격에 이용되고 있음을 소개했다. 특히, 전세계적으로 이슈가 되고 있는 다이어 악성코드를 비롯해 국내에서 문제가 되고 있는 파밍 악성코드, 메모리 해킹을 통한 실제 금융 사기 사례를 설명해 CISO들의 이해를 도왔다.

안랩은 이러한 금융 서비스를 위협하는 악의적인 공격으로부터 고객을 보호할 수 있는 다양한 보안 솔루션을 제공하고 있다. 가장 대표적인 솔루션은 Non-Active X 기반의 온라인 통합 보안 제품인 '안랩 세이프 트랜잭션'이다. 이 제품은 키보드 보안을 통해 사용자의 거래 정보, 개인 정보 등의 주요 콘텐츠의 유출과 변조를 방지할 뿐 아니라, 동시에 악성코드 감지, 네트워크 차단, 취약점 차단, 피싱/파밍 차단, 최신 메모리 해킹 방어 등의 종합적인 보안 기능을 제공함으로써 금융 서비스 이용 시 발생할 수 있는 사용자의 피해를 줄일 수 있는 솔루션이다.

또한 9월 출시 예정인 '안랩 간편인증'도 금융 고객을 위한 최적의 보안 솔루션이다. 안랩 간편인증은 안랩의 강력한 보안 모듈과 USIM, 그리고 통신사의 단말 정보를 활용한 새로운 인증 서비스로 ARS(자동응답전화)나 SMS(문자 메시지) 등의 기존 방식보다 인증단계를 줄여 고객이 한층 더 편리하게 사용할 수 있다.

백민경 차장은 "안랩 간편인증은 많은 은행 고객들이 이미 사용하고 있는 안랩 V3 모바일 플러스를 통해 구동되므로 고객 입장에서는 본인인증을 위해 추가로 애플리케이션을 설치하는 부담이 줄어든다. 또한 은행 입장에서는 기존 ARS 방식보다 저렴해 비용 절감 효과를 가져올 수 있다"고 강조했다.

세션이 끝난 후 은행 CISO들은 핀테크, 옴니 채널, 오픈 플랫폼 등 은행업계에서 화두가 되고 있는 이슈에 대해 안랩의 보안 전문가들과 함께 논의하고, 각자의 경험과 노하우를 공유하는 시간을 가졌다.

안랩은 지난 6월 증권업계, 8월 은행업계 CISO를 대상으로 '안랩 ISF 스퀘어 2015' 진행했으며, 이후 건설, 유통 업계 등 산업별 고객을 찾아갈 계획이다. 또한 8월 27일 전주를 시작으로 9월 부산 등 지역별 고객을 위한 AhnLab ISF SQUARE 2015도 준비 중이다.

'새로운' 2채널 인증 방법을 찾아라!

인터넷망과 통신망 등 2개의 인증 채널을 함께 이용해 사용자 인증 절차를 밟는 것을 '2채널(또는 2팩터) 인증'이라고 한다. 인터넷 뱅킹 시 공인인증서로 본인 확인을 하고 SMS나 ARS 등 통신망을 이용해 추가로 본인 인증을 하는 방식이 대표적인 2채널 인증이다. 그러나 최근 SMS나 ARS를 이용한 2채널 인증 방식의 허점이 드러나면서 새로운 2채널 인증 방법에 대한 관심이 높아지고 있다. 특히 '핀테크(FinTech)'와 관련해 본인 인증 방식의 보안성과 함께 편의성이 중요한 요소로 부각되고 있다.

금융위원회와 금융감독원이 '전자금융사기 예방서비스' 제도를 도입한 2013년 이후 현재 인터넷 뱅킹 뿐만 아니라 온라인 쇼핑 결제 시에도 SMS나 ARS를 이용한 2채널 인증 방식이 이용되고 있다. 그러나 최근 '스미싱(Smishing)' 및 스마트폰의 금융 정보를 탈취하는 모바일 악성코드 유포가 증가함에 따라 SMS 등의 본인 인증 정보가 탈취될 가능성이 높아지고 있다.

또한 ARS 인증 방식의 경우 '착신 전환'을 이용해 사용자 모르게 금융 이체나 결제가 이루어질 수도 있다. 착신 전환이란 유선 또는 무선 전화로 수신되는 전화를 다른 전화기로 받을 수 있게 해주는 통신사의 서비스이다. 예를 들어 사무실 전화를 휴대전화나 집 전화로 받을 수 있게 설정하는 것이다. 이러한 착신 전화 서비스의 허점과 대포폰을 이용해 사용자 몰래 인증 정보를 가로채거나 금융 이체 또는 결제한 사건이 종종 발생하고 있다.

이처럼 SMS나 ARS를 통한 2채널 인증 방식의 보안 허점이 드러나면서 보다 안전한 2채널 인증 기술에 대한 요구가 늘고 있다. 이와 관련해 최근에는 USIM을 기반으로 한 인증 방식이 활발하게 등장하고 있다.

[그림 1] 인터넷 뱅킹 이용 시 추가인증수단으로 제공되는 2채널 인증

다양한 'USIM' 기반 인증 방식, 차이는?

USIM(Universal Subscriber Identity Module)은 '범용가입자 식별체계'를 뜻하는 용어로, 사용자 인증과 로밍, 전자상거래 등 다양한 서비스와 관련된 사용자의 개인 정보를 1장의 칩 또는 카드에 담는 기술이다. USIM 카드 또는 USIM 칩은 암•복호화 기능으로 사용자를 식별하는 초소형 CPU와 스마트폰의 부가서비스에 이용하는 저장공간인 메모리로 구성된다. 한국인터넷진흥원(이하 KISA)이 USIM 카드를 '보안 1등급 매체'로 지정한 점도 USIM 기반의 인증 기술 또는 서비스가 출시되고 있는 이유다.

USIM을 이용한 대표적인 인증 방식으로는 ▲USIM 스마트 인증 ▲USIM 기반 일회용비밀번호(OTP) 등이 있다. 'USIM 스마트 인증'은 스마트폰에 장착된 USIM 칩에 공인인증서를 저장하여 금융 거래 시 전자서명과 함께 본인 인증에 이용하는 공인인증서비스이다. 안드로이드 스마트폰 사용자들은 일정 금액의 월 서비스 이용료만 지불하면 현재 이용 중인 통신사의 'USIM 스마트 인증' 애플리케이션을 설치하여 이용할 수 있다.

이른바 '스마트 OTP'로 불리는 USIM 기반 일회용비밀번호(OTP)는 스마트폰에 앱을 설치하여 금융 거래 시 일회용 비밀번호를 스마트폰 화면에 나타나게 하는 방식이다. 기존 OTP 방식이나 인증 방식에 비해 불편함이 많이 해소되었다는 것이 장점이지만 일각에서는 스마트 OTP 기술의 '시간 동기화' 방식으로 인한 구조적 결함 등을 이유로 보안에 대한 우려를 제기하고 있다. 스마트폰의 시간을 앞선 시간, 즉 미래로 설정해 놓으면 해당 시간에 발생할 OTP 번호를 미리 받을 수 있다는 것이다. 또한 스마트폰 단말기에 악성코드가 설치되어 있을 경우 일회용 비밀번호가 전달되는 과정에서 유출될 수 있으며 앱

변조에 의한 보안 위협도 간과하기 어렵다.

핀테크 시대, 'AhnLab 간편인증'에 시선 집중

USIM 기반의 새로운 인증 방식이 등장했음에도 불구하고 사용자 편의성이나 보안이 여전히 발목을 잡고 있다. 특히 핀테크 시대로 접어들면서 사용자들이 얼마나 쉽고 안전하게 본인 인증을 할 수 있느냐가 핀테크 서비스의 성패를 좌우할 것으로 보인다.

이와 관련해 안랩은 지난 2월 SK텔레콤, KT, LG유플러스 등 이동통신 3사와 '스마트폰 간편인증' 방식의 새로운 인증서비스 추진을 위한 양해각서를 체결하고, 9월 중 'AhnLab 간편인증' 서비스를 출시할 예정이다.

AhnLab 간편인증 서비스는 안랩의 강력한 보안 모듈과 USIM, 그리고 통신사의 단말 정보를 활용한 새로운 인증 서비스이다. 간편결제 서비스 회사가 사용자 인증을 요청하면 안랩이 구축한 간편인증 서버를 통해 국내 이동통신사의 USIM 명의인증시스템에 접속한다. 이와 동시에 V3 Mobile Plus가 설치된 스마트폰에 인증 진행 여부를 확인하는 알림 메시지가 나타나며, 인증을 요청한 사용자의 USIM 칩 내에 저장된 정보와 단말기 정보가 해당 통신사에 정상적으로 등록된 명의와 기기 정보에 일치하는지 등으로 본인 여부를 확인한 뒤 인증 요청을 완료하게 된다.

V3 Mobile Plus는 국내 주요 금융사에서 사용하고 있는 모바일 금융거래 보안 솔루션으로, 현재 약 2,900 만 명의 스마트폰 금융거래 사용자들이 이용하고 있어 신속한 서비스 적용이 가능하다는 것이 장점이다. 아이폰 사용자는 앱 스토어를 통해 제공되는 별도의 "AhnLab 간편인증" 앱을 이용 할 수 있다.

[그림 2] AhnLab 간편인증 서비스 (안드로이드용 및 아이폰용)

무엇보다 길고 복잡한 개인정보를 입력하고 인증코드를 확인하여 직접 입력하던 기존 방식과 달리 AhnLab 간편인증 서비스는 한 번의 클릭만으로 사용자의 본인 인증이 가능하다. 즉, 계좌이체나 결제 시 인증번호를 입력하는 기존 인증 방식의 단계를 줄이고, 본인식별 정보 가로채기 등을 방지할 수 있어 강력한 보안과 더불어 사용자 편의성도 높일 수 있을 것으로 기대된다. 또한 금융거래 서비스 외에도 고객 정보가 불필요한 서비스의 로그인 시, 또는 주요 정보 변경 과정에서 필요한 본인 인증 시에도 적용할 수 있어 다양한 분야에서 활용이 가능하다.

모바일 악성코드 증가와 V3 모바일

안랩 V3 모바일, 왜 강력한가?

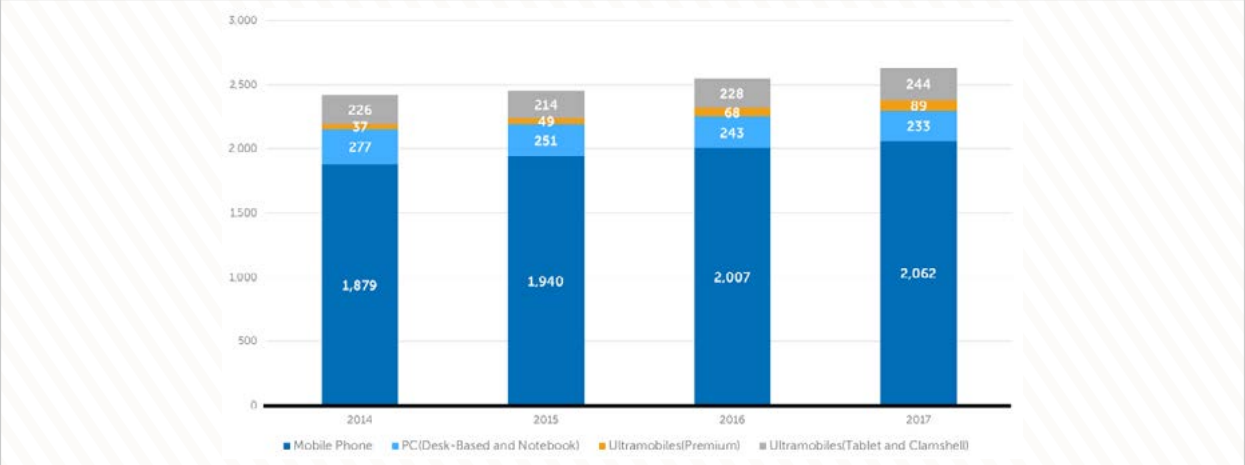
2015년 모바일 디바이스(Mobile Device)가 전세계 디바이스 출하량의 78.4%를 차지할 것으로 예상된다. 이처럼 모바일 기기 이용자가 늘어나고, 많은 개인정보와 데이터가 저장되는 만큼 악성코드 공격자에게 더 없이 매력적인 먹잇감이 되고 있다. 실제로 2013년 이후 모바일 악성코드도 급격히 증가하고 있으며, 유포 방식 또한 교묘해지고 있다. 이에 따라 모바일 악성코드의 탐지 및 차단에 대한 중요성이 더욱 부각되고 있는 시점이다.

이 글에서는 모바일 악성코드의 위협과 글로벌 독립 평가 기관에서 최상위권 성적을 기록하며 기술력을 검증 받은 '안랩 V3 모바일'의 경쟁력을 소개하고자 한다.

모바일 시장 변화와 모바일 악성코드의 증가

모바일 온리(mobile only). 바야흐로 모바일 온리 시대가 도래했다. 모바일 온리는 PC에서 모바일로 옮겨가는 모바일 퍼스트(mobile first) 시대를 넘어 모바일에서만 전자상거래, 은행 거래, 음악 • 영화 소비 등 일상 생활을 하고 비즈니스를 처리하는 시대를 말한다.

세계적인 리서치 기관인 가트너에 따르면 모바일 기기가 2014년 전세계 디바이스 출하량의 77.4% 를 차지하고 있다([그림 1] 참조). 국내의 경우 지난 2014년 9월 국내 스마트폰 가입자수가 4천만 명을 돌파했으며, 2015년 5월 기준 전체 인구 대비 스마트폰 가입자 비율은 약 81.0%이다. 즉, 2015년 5월 기준 대한민국 인구 수는 51,413,925명(행정자치부 자료)이고, 스마트폰 가입자 수는 41,669,694명(미래창조과학부 자료).



[그림 1] 전세계 기기 종류별 출하량 (*출처: Gartner,July 2015)

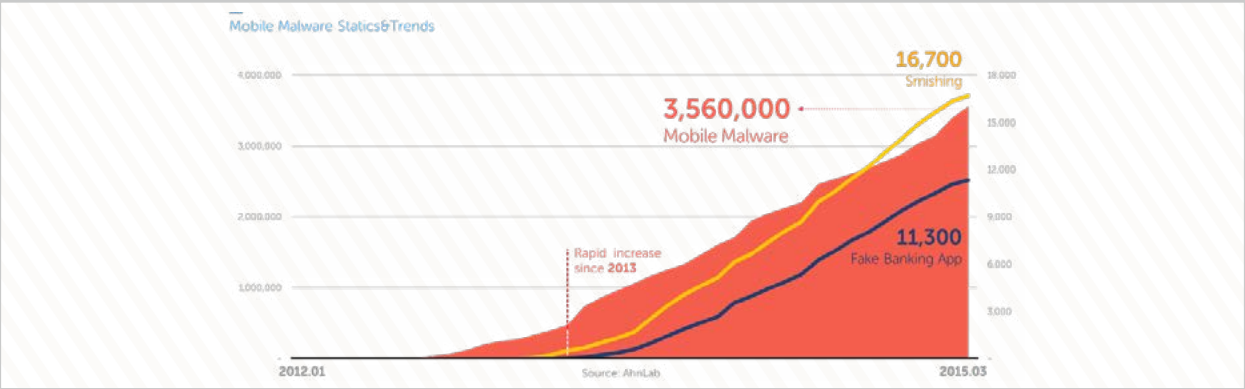
Manufacturers	Operation System	Market Share		
		2012	2013	2014
Samsung	Android	30.30%	31.00%	24.70%
Apple	iOS	19.10%	15.60%	15.40%
Huawei	Android	4.00%	4.80%	5.50%
LG Electronics	Android	3.80%	4.80%	4.60%
Lenovo	Android	3.20%	4.50%	4.50%
Others		39.60%	39.30%	45.30%
Total		**100.00%**	**100.00%**	**100.00%**

[표 1] Top 5 스마트폰 제조사 전세계 시장 점유율 (*출처: Gartner, March 2015)

이러한 환경 변화에 따라 지금까지 주로 PC 환경에서 자주 등장했던 보안 위협이 2014년부터는 본격적으로 스마트폰 환경으로 옮겨갔다. 특히 모바일 환경에 특화된 보안 위협이 대거 등장했다. 해외에서는 FBI를 사칭한 조직이 스마트폰 사용자들을 노리고 유포한 랜섬웨어인 '심플락커(SimpleLocker)'로 실질적인 피해가 발생하기도 했다.

국내에서는 '스미싱(Smishing)'이라는 스마트폰에 특화된 보안 위협이 사회 전반의 화두로 떠올랐다. 문자메시지(SMS)와 피싱(Phishing)의 합성어인 스미싱은 악성코드의 유형과 문구 측면에서 더욱 진화했다. 기존에는 소액결제를 노렸으나 최근에는 인터넷 뱅킹에 필요한 금융 정보를 노리는 악성코드를 사용하는 등 더 큰 금전적 피해를 야기하고 있다.

실제로 모바일 악성코드가 과거와 비교할 수 없을 만큼 급격히 증가하고 있다. 안랩 시큐리티대응센터에 따르면 지금까지 발견된 모바일 악성코드는 2015년 3월 기준 3,560,000여 개이며, 2012년 하반기부터 나타나기 시작한 스미싱 악성코드가 16,700여 개로 집계되었다. 특히, 국내의 경우 모바일 뱅킹 인구가 급증하면서 뱅킹 사칭 앱의 급증한 한 것으로 나타났다([그림 2] 참조).



[그림 2] 모바일 악성코드 현황 및 트렌드

또한 루팅(Rooting) 및 탈옥(Jail-Breaking)에 의한 메모리 조작, 모바일 해킹 등의 위협 요소뿐만 아니라 최근에는 스미싱, 리패키징, 앱 위•변조 등 모바일 앱을 노리는 위협이 증가하고 있다.

주요 모바일 위협	공격 기법
Rooting(Android)	안드로이드 모바일 플랫폼에서 최상위 권한(root)을 획득한 상태 모바일 기기를 원하는 형태로 변경하여 사용 가능
Jail-Breaking(iOS)	'탈옥'이라고 불리기도 하며 안드로이드의 루팅(Rooting)과 동일한 개념 모바일 기기를 원하는 상태로 변경하고 공식 앱 스토어 외에 외부 앱 설치 가능
Memory Searching	외부 프로세스(모바일 뱅킹 등)의 메모리에 접근 아이템 및 주요 데이터를 찾아 위•변조 (예: 금융 관련 데이터 조작, 타임 조작
Repacking	정상적인 앱을 조작하여 원하는 형태로 앱 조작 (예: 은행 사칭 앱) 루팅(Rooting) 작업 필요하지 않음.
File Manipulation	모바일 기기의 스토리지에 저장된 데이터(저장 파일)를 조작
Pixel Sampling	화면에서 특정한 픽셀의 RGB 값을 확보 및 분석하여 콘트롤 조작
Malware	악성코드를 이용한 모바일 해킹 모바일 DDoS (Distributed Denial of Service) 공격에 이용
Packet Manipulation	앱에서 통신 시 전송되는 패킷을 조작하는 형태

[표 2] 주요 모바일 위협 및 공격 기법

안랩의 V3 모바일과 강력한 엔진

안랩은 이러한 모바일 환경을 보호하기 위해 ▲안랩 V3 모바일(AhnLab V3 Mobile) 2.0 ▲안랩 V3 모바일 플러스(AhnLab V3 Mobile Plus) ▲안랩 안전한 문자(AhnLab SafeMessage) ▲안랩 V3 모바일 시큐리티(AhnLab V3 Mobile Security) 등 다양한 모바일 보안 제품을 제공하고 있다. 안랩 V3 모바일 2.0은 모바일 전용 백신(Anti-Virus)으로 삼성, LG 등 국내 주요 스마트폰에 기본 탑재되어 있다. 또한 안랩 V3 모바일 플러스는 은행, 증권 등 금융 애플리케이션 사용 시 연동되는 모바일 트랜잭션 보안 솔루션으로, 90여 개 국내 금융 기관을 고객사로 확보하고 있다. 안전한 문자는 스마트폰 사용자의 스미싱 피해를 예방하기 위해 제공되는 스미싱 차단 전용 애플리케이션이다.

지난 4월 출시된 안랩 V3 모바일 시큐리티는 악성코드 검사에서부터 사생활 보호 기능까지 지원하는 안드로이드 기반 스마트폰 전용 보안 솔루션으로, 글로벌 구글 플레이에서 판매되고 있다.

이들 안랩 모바일 제품의 가장 큰 경쟁력은 글로벌 독립 평가 기관 AV-Comparatives 및 AV-TEST에서 세계 최상위권 성적을 기록하며 기술력을 검증 받은 '안랩 V3 모바일 엔진'을 기반으로 강력한 안드로이드 악성코드 탐지 성능을 제공한다는 것이다.

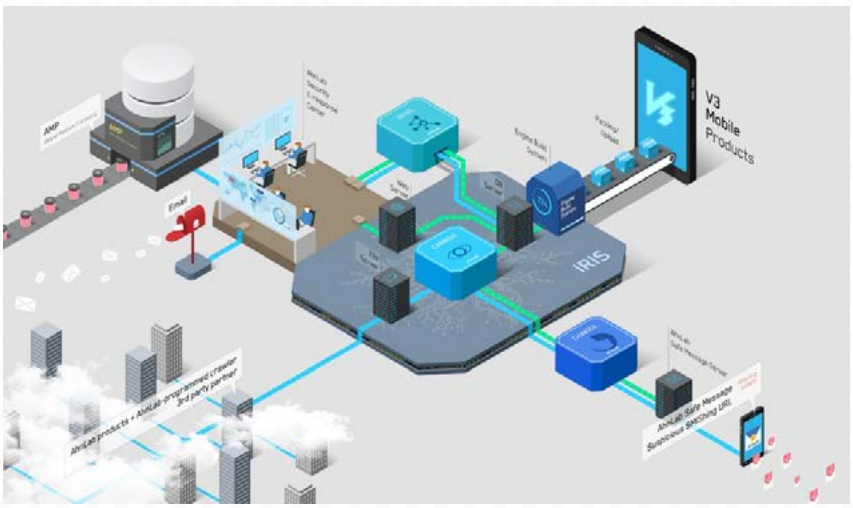
안랩 V3 모바일 엔진은 국내에서 유일하게 AV-TEST가 모바일 분야 테스트를 시작한 2013년부터 매회 빠짐없이 참가해 16회 연속 인증을 획득(2015년 7월 기준)했을 뿐만 아니라, 2014년부터 올해 7월까지 열린 총 10회의 테스트 중 8회에 걸쳐 100%의 악성코드 진단율을 기록했다. 특히, AV-TEST가 2015년 7월에 진행한 모바일 보안 테스트에서 안랩의 모바일 제품은 진단율(protection) 테스트와 새롭게 추가된 '리얼타임(real-time)' 테스트에서 각각 100%의 진단율을 기록해 해당 부문에서 만점을 받았다. 실행 시 배터리 소모, 단말기 속도에 미치는 영향 등을 평가하는 사용성(Usability)에서도 만점을 기록하고, 추가 기능(Features)에서도 점수를 받아 종합점수 13점 만점에 13점을 기록해 인증을 획득했다.

[그림 3] 안랩 V3 모바일 글로벌 평가기관 테스트 결과

안랩 V3 모바일 엔진의 저력

안랩 V3 모바일 제품이 글로벌 평가기관으로부터 기술력으로 인정받고 최상위권의 기록을 유지할 수 있는 비결은 무엇일까.

안랩은 20여 년의 노하우를 지닌 국내 최대 보안업체로서 '악성코드 수집–분석–분류–대응' 측면에서 최고의 기술력을 보유하고 있다. 안랩 V3 모바일에는 이러한 악성코드 관련 기술력과 자체 개발된 자동화 프로그램을 기반으로 한 모바일 대응 프로세스 체계가 갖추어져 있기 때문이다.



[그림 4] 안랩 모바일 악성코드 대응 프로세스

안랩 모바일 악성코드 대응 프로세스는 안랩 시큐리티대응센터의 분석가와 분석가들의 노하우가 적용된 자동화 프로그램이 유기적으로 작동하여 샘플 수집에서 엔진의 룰(rule) 반영까지 20분 이내에 대응이 가능하다([그림 4] 참조).

우선 각종 악성코드 샘플은 고객 문의/신고, 자사 제품군과 자체 제작한 크롤러, 써드파티 파트너사, 그리고 스미싱 샘플은 안랩의 안티스미싱 애플리케이션인 '안전한 문자'를 통해 수집된다. 특히, 안랩은 웹 기반의 악성코드 처리 시스템인 AMP(AhnLab Malicious code Processing system)를 자체 개발해 고객사에서 접수한 샘플 수집, 문의, 업무 요청 등을 자동화했다.

이렇게 수집된 샘플은 안랩의 시큐리티대응센터에서 자체 개발한 모바일 휴리스틱 자동 분석 시스템인 아이리스(IRIS)로 보내진다. 아이리스는 대량의 안드로이드 앱 수집 → 자동 분석 → 악성 특징 추출 → 유사 그룹 분류 → 최종 진단할 수 있도록 일련의 과정을 처리한다. 즉, 진단 값과 샘플 정보를 우선 순위에 따라 보여줌으로써 공격적인 진단이 가능하다.

특히, 이 과정 속에 안랩 분석가들의 노하우가 반영한 특별한 인프라가 다수 존재한다. 캐논(CANNON)은 악성/정상 진단을 위한 값과 샘플 정보를 추출하는 실시간 대용량 샘플 처리 인프라(Real-Time Sample Processor)이다. 분석가는 캐논에서 추출한 안드로이드 파일에 관련된 정보들을 바탕으로 룰(Rule)을 만들어 데이터베이스(DB)에 저장한다. 최근 증가하는 스미싱을 통해 유포되는 악성코드를 진단하는 것은 샤크라(CHARKA)로, 스미싱 위협에 대한 대응 인프라로 실시간 대용량 네트워크 진단 엔진이다. 안랩의 안전한 문자를 통해 스미싱 의심 샘플이 접수되면 안전한 문자 서버에서 샘플을 다운로드하고, 이를 샤크라를 통해 처리한다.

[그림 5] 모바일 앱의 라이프 사이클을 그래프로 제공하는 안랩 DEVIL

최근 개발된 프로그램인 DEVIL(DEx VIsualLizer)은 모바일 앱의 라이프사이클(Life Cycle)을 그래프 형태로 보여주는 애널라이저(Analyzer)이다. 이 프로그램은 악성 앱의 컴포넌트들의 연관 관계가 그래프에 표시되며, 그 컴포넌트들이 엮여 있는 클래스를 보면서 악성 행위를 진단할 수 있는 것이다.

안랩은 2014년부터 이러한 '안랩만의 독자적인 모바일 악성코드 대응 프로세스'를 구축하여 수집–분류–분석–대응 시스템을 자동화하였다. 이를 통해 1일 10만 개의 악성코드 샘플을 처리함으로써 빠른 대응이 가능해졌다. 또한 실제 스마트폰에서 기본 앱과 안드로이드 마켓에서 정상 앱을 수집하여 이를 화이트리스트 룰(Whitelist Rule)로 처리함으로써 오진률을 최소화했다. 특히 '안드로이드 파일에 특화된 캐쉬&핑거프린트 기법'을 이용해 진단 속도 향상을 이뤄냈다.

안랩은 이러한 노력을 통해 글로벌 평가기관인 AV-TEST의 테스트에서 16회 연속 인증 획득, 7회의 테스트에서 진단율 100%이라는 놀라운 성과를 거뒀다. 또한 앞으로도 끊임없는 진단법 연구, 자동 분류에 대한 프로젝트를 지속하여 글로벌 진단율 1위를 유지할 계획이다.

POS 위협과 AhnLab EPS

한동안 뜸했던 POS 위협, '빈틈'을 파고들다

가본 적도 없는 곳에서 신용카드로 200만원이나 결제되었다?!
신용카드를 빌려준 적도, 카드를 분실한 적도 없다. 도대체 이게 어떻게 된 일인가?
카드사와 경찰에 신고했더니 평소 자주 가던 회사 근처 음식점의 신용카드 결제 단말기(POS)가 해킹되어 카드가 복제되었다는 것이다. 게다가 같은 음식점을 이용하던 몇몇 사람들도 똑같은 피해를 입었다고 한다. 말로만 듣던 불법복제카드와 POS 해킹의 피해자가 바로 내가 될 줄이야.

지난 2013년 말, POS 시스템 해킹으로 인한 대규모 신용카드 정보 유출 사건이 발생한 이후 잠잠해진 것 같던 POS 해킹 사건이 또 다시 발생했다. 지난 7월 초, 인천 지역에서 실제 사용자가 알지 못하는 사이에 신용카드로 거액이 결제되는 피해가 잇따라 발생한 것이다. 피해자들은 모두 신용카드를 분실한 적이 없었다. 카드사와 경찰은 일부 피해자가 특정 음식점에서 신용카드를 사용했다는 점으로 미루어 해당 음식점의 신용카드 결제용 POS(Point-of-Sales) 단말기가 해킹된 것으로 판단하고 있다. 한편 해외에서도 최근 POS 시스템을 노리는 신종 악성코드가 잇따라 발견되는 등 POS 해킹이 다시 거세질 조짐을 보이고 있다.

[그림 1] POS 단말기 해킹 언론 보도 (*출처: KBS 뉴스광장, 2015년 7월)

POS 보안 대응책 마련 '잰 걸음', 실효성은 '글쎄…'

금융감독원(이하금감원)과 '신용카드 결제 단말기 IC전환 태스크포스(TF)'가 지난 7월 1일 'POS단말기 보안표준 규격안'을 발표했다. 2015년 3월부터 약 4개월에 걸쳐 논의된 POS단말기 보안표준은 ▲물리적 해킹 시도 시 POS 단말기 메모리 자동 파괴 ▲정보 유출 차단을 위한 엔드투엔드(End-to-End) 방식의 '전체 암호화' 등을 골자로 하고 있다.

금감원은 또한 여신금융협회와 함께 '여신전문금융업법(이하 여전법)'을 개정해 신용카드 결제대행업체(Value Added Network, 이하 VAN) 등록제도 병행하고 있다. 이에 따라 지난 7월 21일부터 신규 가맹점 및 신규 POS 단말기 설치 시 보안표준에 따라 제작되어 인증에 통과한 단말기만 설치 및 사용해야 하며, 이를 어길 시 VAN사와 가맹점에 5천만 원 이하의 과징금이 부과된다. 단, 기존 가맹점들의 POS 단말기에 대해서는 3년의 유예기간을 두고 신규 단말기로 교체할 것을 유도하고 있다. 그러나 기존 가맹점에서도 POS 단말기 고장 등이 발생했을 경우에는 무조건 신규 단말기로 교체해야 한다. 문제는 비용 부담이 만만치 않아 영세한 가맹점의 경우 신규 POS 단말기 도입 또는 교체가 쉽지 않다는 점이다. 또한 이른바 전자칩(IC) 단말기 전환 사업자로 선정된 VAN사 세 곳 중 두 곳은 아직 단말기 인증을 받지 못한 상황이라 신규 단말기 공급 물량이 부족하다는 지적도 있다. 앞서 언급한 POS 단말기를 이용한 카드 불법복제 사건도 공

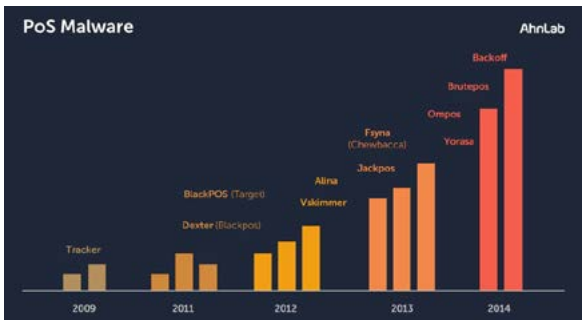
교롭게도 금감원이 POS 단말기 보안표준을 발표한 이후 발생했다. 금융 당국이 마련한 신용카드 및 POS 해킹 사고 방지 대응책에 대해 실효성 측면에서 의구심을 떨치기 어려운 이유다. 게다가 국내외에서 진화된 형태의 POS 악성코드가 계속 발견되고 있어 POS 보안 위협은 쉽게 해결되지 않을 것으로 보인다.

POS 위협, 악성코드의 진화 vs 태생적 위협

POS 악성코드가 전세계적으로 주목을 끌게 된 계기는 지난 2013년 12월 발생한 미국 대형 유통업체 타겟(Target)사 해킹 사건이다. 약 4천만 건의 신용카드 정보를 탈취하고 7천만 명에 달하는 피해자를 기록한 타겟사의 POS 시스템 해킹에 사용된 악성코드는 '블랙POS(BlackPOS)'로 알려졌다.

2014년 7월에는 POS 시스템을 감염시켜 고객의 이름, 주소, 신용카드 번호 등의 정보를 유출하는 '백오프(Backoff)' 악성코드가 발견되기도 했다. 북미 지역에 폭넓게 유포된 것으로 알려진 백오프 악성코드는 메모리 내에서의 트랙 데이터 수집 및 키로깅 기능을 갖고 있으며, 다양한 변종이 존재하는 것으로 확인되었다.

올해 발견된 POS 악성코드로는 '포세이돈(PoSeidon)', '말럼POS(MalumPOS)' 등이 있다. 지난 3월 발견된 포세이돈 악성코드는 앞서 타겟사 POS 해킹에 이용된 블랙POS와 대표적인 인터넷 뱅킹 악성코드인 '제우스(Zeus)'의 기능이 합쳐진 형태로 알려져 있다. 포세이돈은 POS 시스템의 메모리 영역에 저장된 신용카드 정보를 찾아낼 뿐만 아니라 카드 번호의 유효성까지 검사하는 기능이 있으며, 시스템을 재부팅하더도 시스템에 그대로 존재한다.



[그림 2] 주요 POS 악성코드 추이 (2009~2014)

지난 6월에 발견된 말럼POS 악성코드는 오라클의 POS 시스템 운영 플랫폼인 '마이크로스(MICROS)'에서 카드 소유자의 이름과 카드 번호를 탈취하는 것으로 알려져있다. 마이크로스는 전세계 33만여 고객사의 POS 플랫폼으로 제공되어 있어 잠재적인 피해가 우려되고 있다.

POS 악성코드는 국내에서도 심심치 않게 발견되고 있다. 대표적으로 지난 2014년 초 'Ompos'라는 악성코드를 이용해 POS 시스템 관리 업체의 서버를 해킹한 후 POS 시스템을 감염시켜 신용카드 정보를 노린 사례가 있다.

악성코드뿐만 아니라 POS 시스템의 특수성도 핵심적인 위협 요인이라 할 수 있다. POS 시스템의 태생적 위협 요인으로는 ▲다양한 네트워크 연결 ▲부적절한 POS 단말기 이용 행태 ▲애플리케이션 취약점 등을 들 수 있다.

대부분의 POS 시스템은 폐쇄망이 아닌 일반적인 상용 인터넷망을 사용하고 있다. 일부 대형 유통업체는 POS 시스템과 지불 승인 네트워크를 별도의 전용선으로 운용하지만 수많은 중소 규모의 업체나 영세 가맹점의 경우에는 상용 인터넷을 통해 POS 시스템을 연결하여 지불 승인을 하고 있다. 게다가 최근 POS 시스템은 고객 정보, 포인트 정보 등 다양한 고객 관리 정보와의 연계 등을 위해 다른 네트워크와 연결하는 경우도 많다. 이러한 네트워크 연결 환경에서는 보안에 취약한 지점이 존재할 수 밖에 없으며, 만일 무선인터넷을 이용하는 경우라면 네트워크를 통한 공격의 가능성이 더욱 높아진다.

가맹점 주인 또는 직원들이 POS 단말기를 이용해 개인 PC를 사용하듯 온라인 쇼핑이나 SNS 등 인터넷 이용을 하는 경우가 많다는 점도 문제다. 이처럼 부적절한 POS 시스템 사용으로 인해 악성코드 감염에 노출되기 쉽다.

또한 필요에 따라 원격 제어 프로그램, 인터넷 익스플로러, 어도비 리더, 마이크로소프트 오피스 등 다양한 애플리케이션을 POS 시스템에 설치하기도 한다. 이 경우 웹 브라우저, PDF/DOC 등 문서 프로그램, 자바(JAVA) 등의 취약점을 이용한 악성코드 유입과 같은 일반적인 PC 환경에서의 보안 위협이 고스란히 존재한다. 이 밖에도 비용 부담 등으로 인해 POS 시스템을 저사양 PC나 오래된 운영체제에 POS 프로그램을 설치·운용하는 경우가 많다는 점도 문제다. 특히 일부 가맹점의 POS 단말기는 서비스가 종료된 윈도 XP(Windows XP) 및 윈도 XP를 기반으로 한 WEPOS(Windows Embedded for Point of Service), 윈도 임베디드 POSReady 2009(Windows Embedded POSReady 2009)를 운영체제로 사용하고 있어 보안에 매우 취약하다.

이처럼 대부분의 POS 시스템은 악성코드를 비롯해 환경적 특수성에 의해 다양한 위협에 노출되어 있다. 금융 당국의 주도로 '전체 암호화' 등 보안 기술이 적용된 IC 단말기로의 교체가 진행되고는 있지만 모든 POS 단말기를 신규 단말기로 교체 완료하기까지는 상당 시일이 걸릴 것으로 예상돼 POS 시스템은 여전히 보안에 취약한 상태다.

그렇다고 손 놓고 있을 수도 없는 일. 현재 가능한 방법으로는 백신(Anti-virus)을 사용하거나 데이터 암호화 및 암호 통신을 적용하는 것인데, 이미 악성코드에 감염된 POS 시스템일 경우 데이터 암호화나 암호 통신은 무의미하다. 또한 백신은 신종 악성코드 대응에는 적합하지 않으며, 저사양 시스템이나 네트워크 속도가 제한적인 환경에서 운용되는 POS 시스템의 경우 시그니처 업데이트가 필요한 백신 프로그램으로 리소스 문제가 발생할 수 있다. 상황이 이렇다 보니 POS 시스템의 특수한 환경적 요인과 최신 POS 위협을 다각도로 고려한 보안 솔루션에 대한 요구가 늘고 있다.

AhnLab EPS, POS 위협에 답하다

안랩은 POS 단말기와 같은 특수 목적 시스템을 위한 전용 보안 솔루션인 AhnLab EPS(Endpoint Protection System)를 제공하고 있다. AhnLab EPS는 안정적 운용에 대한 민감도가 높고 정해진 프로그램만 사용하는 특수 목적 시스템에 최적화된 보안 솔루션으로, 강력한 악성코드 억제 및 보안 성능을 제공한다.

AhnLab EPS는 화이트리스트(Whitelist) 기반으로 불필요한 프로그램의 실행을 차단하고 악성코드의 유입 및 활동을 억제한다. 특히 전문적인 보안 지식 없이도 운용이 가능하며, 중앙 관리를 통해 매장에서의 보안 솔루션 운용에 대한 부담이 적다. 또한 강력한 락다운

(Lockdown) 기능으로 POS 시스템 운용에 필요 없는 애플리케이션 및 시스템 기능과 매체 • 네트워크 연결 통제 기술을 통해 모든 POS 시스템이 외부의 공격과 알려지지 않은 위협으로부터 항상 안전하게 유지할 수 있게 해준다.

[그림 3] 특수 목적 시스템 전용 보안 솔루션 AhnLab EPS

AhnLab EPS는 서버에 탑재되는 악성코드 분석 엔진을 통해 단말 시스템의 자원을 거의 사용하지 않고도 시스템에 생성되는 모든 실행 파일에 대한 실시간 검사와 분석을 수행할 수 있다. 이로써 단말 시스템에서는 주기적인 백신 업데이트나 이로 인한 네트워크 및 시스템 자원 점유 부담에서 자유롭다. 특히 POS 시스템 단말의 악성코드 대응과 알려지지 않은(Unknown) 위협 분석까지 수행이 가능하다. 즉, POS 시스템의 안정적인 운용에 중점을 두고, 뒷단에서의 악성코드 탐지 및 대응을 통해 추가적인 보안 정책을 강화할 수 있다는 것이 장점이다.

이처럼 AhnLab EPS는 비즈니스 운용에 영향 없이 사전적인 악성코드 차단과 통제가 가능해 생산성 향상 및 운용 비용 절감에 기여한다. 이에 AhnLab EPS는 현재 다이소, 신세계 등 대형 유통 업체의 POS 시스템에 적용되어 있으며, 반도체 및 가전 생산 라인, 산업 설비 제어, 키오스크(KIOSK), ATM 등 다양한 분야의 특수 목적 시스템에 도입돼 그 성능과 효과를 인정받고 있다.

모바일 랜섬웨어 상세 분석

스마트폰마저 점령한 '크립토락커'

2015년 상반기를 강타한 보안 위협 중에서 눈에 띄는 것은 단연 '랜섬웨어(Ransomware)'이다. 불과 몇 년 전까지만 해도 랜섬웨어는 해외에서만 언급되던 '남의 일'이었지만 올해는 국내에서도 랜섬웨어가 지속적으로 나타나고 있다. 특히 지난 4월에는 국내 유명 커뮤니티 사이트의 배너 링크를 통해 '크립토락커(Cryptolocker)' 랜섬웨어가 유포되면서 큰 이슈가 됐다. 해당 랜섬웨어는 '한국어'를 지원해 국내 사용자를 겨냥한 랜섬웨어라는 점에서 더욱 주목을 받았다. 최근에는 PC뿐만 아니라 안드로이드 기반의 스마트폰을 노린 랜섬웨어까지 등장해 더욱 심각한 위협이 되고 있다. 이 글에서는 최근 발견된 모바일 랜섬웨어의 구조와 동작 방식에 대해 상세히 살펴본다.

안랩은 지난 7월 안드로이드 스마트폰 사용자의 데이터를 인질로 삼아 금전을 요구하는 '스마트폰 랜섬웨어'를 발견, 관련 정보를 관계 당국과 공유하는 한편 사용자의 주의를 당부한 바 있다. 공격자는 '어도비 플래시 플레이어(Adobe Flash Player)'를 사칭해 '어도비 플래시(Adobe Flash)'라는 이름의 악성 앱을 제작•유포했다. 해당 악성 앱은 설치 과정에서 사용자에게 과도한 권한 및 관리자 활성화를 추가로 요구하는데, 사용자가 앱 이름을 눈여겨 보지 않거나 과도한 권한 요구에도 별 다른 의심없이 해당 앱을 설치하면 랜섬웨어에 감염된다.

[그림 1] 악성 앱(왼쪽) 및 앱 설치 목록(오른쪽)의 악성 앱

안드로이드 매니페스트(Manifest) 정보를 통해 앱 설치와 관련된 권한 정보를 알 수 있는데, 해당 악성 앱의 매니페스트 정보는 [그림 2]와 같다.

[그림 2] 악성 앱의 Android Manifest.xml 정보

해당 앱의 설치 과정과 함께 이 앱이 요구하는 권한을 좀 더 자세히 살펴보자. 우선, 해당 앱은 [그림 3]과 같이 네트워크 통신, 전화 통화, 시스템 도구 등의 권한과 함께 휴대폰 관리자(기기 관리자) 권한을 요구한다.

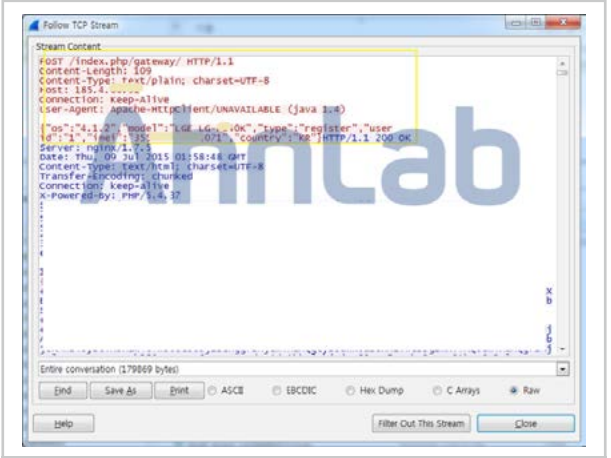
[그림 3] 악성 앱의 권한 요구 내용

이 악성 앱은 리소스 영역에 존재하는 서버 주소와 com.lock.a.f class에 존재하는 코드를 조합하여 다음과 같은 단말기 정보를 수집하여 [그림 4]와 같이 공격자에게 전송한다.

- 운영체제 버전
- 스마트폰 모델명
- IMEI(국제 이동 단말기 식별 번호)
- 국가 정보

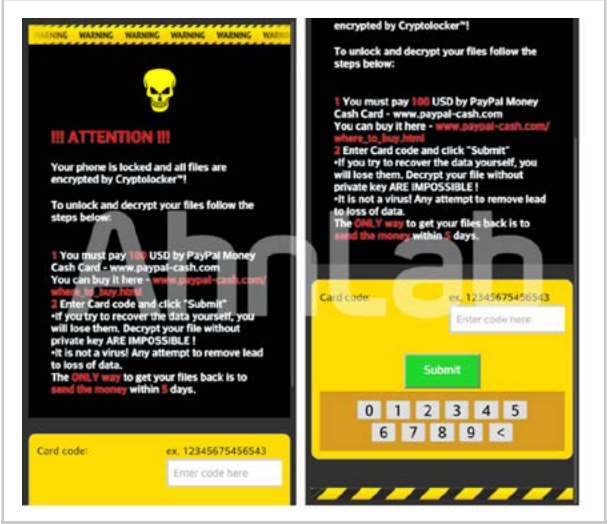
[그림 4] 악성 앱이 수집한 단말기 정보 및 외부 전송(서버 주소)

[그림 5]는 악성 앱이 수집한 정보를 전송하는 네트워크 패킷이다.



[그림 5] 수집한 스마트폰 정보 전송 패킷 분석

이와 함께 스마트폰에는 [그림 6]과 같이 '스마트폰의 파일들이 암호화되었고 스마트폰이 잠겼으니 정상적으로 이용하고 싶다면 일정 기간 내에 100달러를 지불하라'는 내용의 화면이 나타난다. 실제로 이 악성 앱에 의해 랜섬웨어에 감염되면 스마트폰이 잠기고 다른 화면으로 전환하는 등의 스마트폰 조작이 불가능해진다.



[그림 6] 악성 앱 감염 시 나타나는 랜섬웨어 화면

한편 이 악성 앱에서 또 다른 흥미로운 점이 발견되었다. 바로 스마트폰의 국가 정보가 러시아인 경우에는 랜섬웨어가 동작하지 않도록 설계되었다는 점이다. [그림 7]은 악성 앱이 국가 정보를 확인하는 코드이다.

[그림 7] 악성 앱의 국가 정보 확인 코드

랜섬웨어 악성 앱, 제거하기 까다로워

스마트폰이 랜섬웨어에 감염되면 사용자는 스마트폰을 조작할 수 없게 된다. 따라서 악성 앱을 삭제하는 것은 물론 평소 이용하던 앱도 실행할 수 없는 경우가 대부분이다.

이번에 발견된 '어도비 플래시 플레이어' 악성 앱에 의해 감염되었을 경우, 스마트폰을 '안전 모드'로 부팅한 다음 [그림 8]과 같이 [설정] – [기기 관리자(휴대폰 관리자)] 메뉴에서 랜섬웨어를 포함하고 있는 악성 앱의 비활성화에 체크한다. 이후 애플리케이션 목록에서 해당 앱을 제거하면 된다. 단, 스마트폰 제조사별로 안전모드로 부팅하는 방법이 각기 다르기 때문에 제조사가 제공하는 설명서 등을 참고해야 한다.

[그림 8] 안전모드 부팅 후 기기 관리자에서 악성 앱 권한 해제 및 제거

이와 같은 스마트폰 보안 위협의 피해를 최소화하려면 앱 다운로드 시 평판 정보를 확인하고 설치하는 습관을 갖는 것이 필요하다. 공식 마켓을 통한 앱 다운로드 시에도 마찬가지다. 또한 문자메시지(SMS) 등에 포함된 URL을 무심코 클릭하지 않도록 주의해야 한다. 평소 V3 Mobile 등 모바일 전용 백신이나 '안랩 안전한 문자' 등 스미싱 탐지 앱을 이용하는 것이 바람직하다.

한편 V3 Mobile 제품은 해당 악성 앱을 아래와 같은 진단명으로 탐지하고 있다.

〈V3 Mobile 제품 진단명〉

Android-Trojan/Slocker

Windows 10 업데이트로 위장한 랜섬웨어

‘Windows 10 · 랜섬웨어’ 악성코드가 주목하는 트렌드?

하루가 멀다 하고 진보하는 IT 기술 덕분에 사용자들은 어제보다 더 스마트한 오늘을 살고 있다. 하지만 과연 보안 의식 또한 스마트해지고 있는 것일까? 이 질문에 대해 답하긴 쉽지 않지만 악성코드 제작자는 IT 기술의 트렌드를 스마트하게 악용하고 있는 건 분명한 사실인 듯하다.

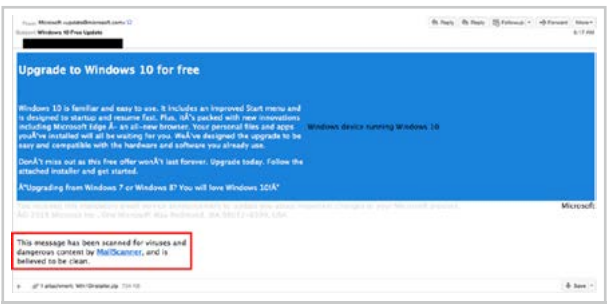
Windows 10이 출시된지 얼마 되지 않아 Windows 10 업그레이드를 사칭한 랜섬웨어가 등장했다.

이번에 발견된 랜섬웨어도 그 동안 안랩에서 소개했던 여러 랜섬웨어들과 크게 다르진 않다. 하지만 이번 사례에서 이용된 사회공학 기법은 악성코드 유포 방법이 점차 지능화되고 있으며, 결국 사람이 가장 큰 취약점이란 것을 다시 한 번 일깨워준다.

이 글에서 Windows 10 업데이트 파일로 위장한 랜섬웨어에 대한 상세 분석 정보를 소개한다.

마이크로소프트사(이하 MS)의 마지막 Windows OS가 될 Windows 10이 7월 29일 출시됐다. 출시 후 며칠이 지나지 않아 Windows 10 업데이트 파일로 위장한 랜섬웨어가 메일로 유포된 것을 볼 때, Windows 10의 출시는 일반 사용자뿐만 아니라 악성코드 제작자들의 흥미 또한 유발한 것으로 보인다. 특히, 해당 악성코드를 첨부한 메일 본문에서 공격자의 치밀함이 여실히 드러난다.

공격자는 발신인, 본문 내용과 더불어 ‘악성코드 스캔 후 이상 없다’는 마지막 문장([그림 1] 참조)을 첨부하여, 수신자가 해당 메일을 읽은 뒤에 의심 없이 첨부파일을 다운로드 및 실행하도록 유도했다. 심지어 메일 내 첨부된 악성파일의 아이콘이 아래 [그림 2]와 같이 Windows 로고를 표시하므로, 평소 보안 의식이 강한 사용자가 아니라면 거부감 없이 해당 파일로 마우스 포인터를 옮길 것이다.



[그림 1] 악성코드가 첨부 된 메일 본문 (*출처: Cisco Blogs)

[그림 2] Windows 10 파일로 위장한 악성코드

이 파일을 실행하면 Windows 10 업데이트가 아닌 랜섬웨어가 실행돼 사용자 시스템 내 파일이 암호화되어 버린다. 실행된 랜섬웨어 악성코드는 C:₩DOCUME~1₩[사용자 계정]₩LOCALS~1₩Temp₩ 경로에 파일명 "lrxjxii.exe"로 자가 복제하고, 레지스트리를 통해 서비스에 등록되어 시스템 시작 시마다 실행된다.

[그림 3] 랜섬웨어 감염 시 바탕화면

랜섬웨어 악성코드는 시스템 내 파일을 암호화한 뒤 파일 복호화 안내를 상단의 [그림 3]과 같이 바탕화면에 표시한다.

이번에 발견된 랜섬웨어도 그 동안 안랩에서 소개했던 여러 랜섬웨어들과 크게 다르진 않다. 하지만 이번 사례에서 이용된 사회공학 기법은 악성코드 유포 방법이 점차 지능화되고 있으며, 결국 사람이 가장 큰 취약점이란 것을 새삼 느끼게 해준다.

올해 4월 국내 특정 대형커뮤니티에서 드라이브 바이 다운로드(Drive-by Download)를 통해 유포되었던 랜섬웨어의 경우, 사용자의 취약한 시스템을 노린 공격이었으므로, 평소 Windows 보안 패치 및 응용프로그램(Adobe, java 등)의 업데이트를 성실히 수행해 온 사용자라면 악성코드 감염을 피할 수 있었을 것이다. 하지만 이번 사례와 같이 메일을 통해 유포되는 악성코드를 친절하게 다운로드 및 실행하는 건 사용자의 판단에 기반한 행동이다. 보안 패치로 굳게 닫혀 있는 시스템을, 악성코드의 노크에 직접 문을 열어주는 것은 사용자의 판단 부재에 따른 것이다. "절대로 메일 내 첨부파일을 함부로 다운로드 및 실행해선 안 된다"는 시스템의 안전을 위한 가장 기초적이고 중요한 사항을 수없이 강조하게 되는 이유는 바로 이 때문이기도 하다.

현재 MS는 Windows 10을 '더욱 익숙하고 친숙한 OS'라 칭하며, '예상하지 못했던 작업을 하세요'라는 슬로건을 내세우고 있다. 하지만 이 말은 즉, '예상하지 못했던 보안 위협'을 뜻하기도 한다. 새로운 기능은 새로운 위험 요소를 내재할 수 있으며, 새로운 위험 요소는 또 다른 공격의 통로가 될 수 있다.

하루가 멀다 하고 진보하는 IT 기술 덕분에 사용자들은 어제보다 더 스마트한 오늘을 살고 있다. 하지만 과연 보안 의식도 스마트해지고 있는 것일까? 백신만으로 모든 공격을 막을 수 없는 현실 속에서 최소한의 보안에 대한 이해와 생활화된 보안 의식이 동반된다면, 그것이 바로 사용자를 끊임없는 악성코드 공격으로부터 보호할 수 있는 최선의, 또한 최고의 방어라고 생각한다.

지금 바로 내 곁의 '스마트홈', 남은 숙제는?

아침 7시, 안방의 인기척에 집안 조명이 은은하게 켜지고 커피머신은 알아서 커피를 내리기 시작한다. 미리 설정해 둔 뉴스를 들으며 서둘러 출근 준비를 마친다. 집을 나서자 집안 조명이 꺼지고 방범 기능이 설정된다. 로봇 청소기는 그제야 집안을 돌며 청소를 한다. 아! 아침을 하고 나서 가스 밸브를 잠갔던가? '이 놈의 건망증!' 스마트폰을 꺼내 가스 밸브의 상태를 확인한다. 오전 근무를 마친 시간, 집에 홀로 남겨진 반려견의 안부가 궁금해 스마트 카메라 앱을 실행한다. 하루 일과를 마치고 돌아오는 길, 집에 도착하기 20분 전 미리 에어컨을 켜둔다. 현관 도어락에 스마트폰을 가까이 대자 잠금이 해제되고 문이 열린다. 일단 소파에 몸을 기댄다. "알렉사(음성인식 비서인 아마존 에코를 부르는 이름), 음악을 켜 줘." 잔잔한 음악이 흘러나온다. 밤 11시, 침대에 눕자 침대에 내장된 센서가 알아서 심장박동과 호흡 등을 파악해 깊은 잠을 잘 수 있도록 해준다.

미래소설에 나올 법한 이 이야기는 과연 얼마나 실현 가능할까? 결론부터 답하자면 지금, 당장, 100% 가능하다.

먼 일 같이 느껴지던 스마트홈이 착착 우리 곁을 파고 들고 있다. 모든 사물이 인터넷으로 연결되어 서로 데이터를 주고 받으며 유기적으로 반응하는 사물인터넷(Internet of Things, IoT)이 집에 주목하면서 스마트홈의 대중화가 속력을 내고 있다. 조명, 에너지 관리, 보안, 홈 엔터테인먼트, 네트워크 등 가정 내 기기를 네트워크화하여 제어할 수 있는 스마트홈은 지금 우리 곁에 얼마나 가까이 다가와 있을까? 현재 상용화된 디바이스를 통해 스마트홈의 오늘을 만나보자.

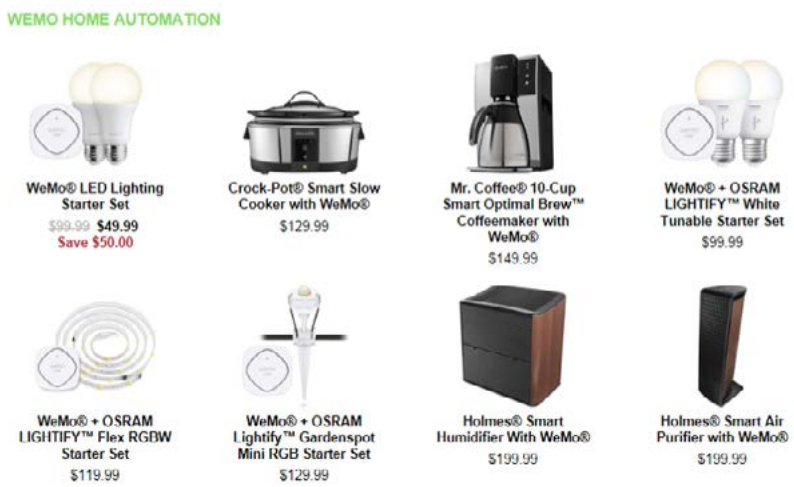
스마트홈 '플랫폼' 경쟁 시작!

스마트폰에서 그랬듯 스마트홈 시장에서도 플랫폼을 누가 지배하느냐가 앞으로 스마트홈 시장의 꽤나 중요한 부분을 차지할 것으로 보인다. 현재는 벨킨(Belkin)의 '위모(WeMo)'와 퀄키(Quirky)의 '윙크(Wink)', 그리고 지난해 8월 삼성이 인수한 '스마트싱스(SmartThings)' 정도가 대표적인 스마트홈(또는 사물인터넷) 플랫폼이다.

스마트홈 컨트롤러인 '윙크 허브(Wink Hub)'는 GE, 필립스, 네스트 등 다양한 브랜드의 스마트홈 제품과 연동해 사용할 수 있으며 조명, 전원 관리, 에너지 관리 등이 가능하다. 터치스크린 스위치인 '윙크 릴레이(Wink Relay)'도 집안의 모든 전자제품과 연결해 사용할 수 있다.

[그림 1] 스마트홈 플랫폼 '윙크 허브'와 '윙크 릴레이' (왼쪽부터, *출처 : wink.com)

벨킨의 위모(WeMo)는 콘센트에 위모 스위치를 꽂고 그 위에 가전제품을 꽂으면 언제 어디서든 스마트폰 전용 앱으로 가전제품을 제어할 수 있는 구조다. 현재 위모는 스위치뿐 아니라 조명, 전원 관리 등의 일반적인 스마트홈 제품과 함께 위모 기반의 커피메이커, 가습기, 조리기구, 네트워크 카메라, 공기 정화기 등을 출시했다.



[그림 2] 위모의 홈 오토메이션 기기 (*출처 : belkin.com)

'스마트싱스' 역시 사물인터넷 플랫폼의 하나다. 스마트싱스는 허브와 앱을 활용해 서로 다른 기업의 150여 개 스마트 기기를 네트워크화할 수 있다. 앱과 허브, 스마트 기기만 있으면 전 세계 어디서든 집안의 스마트 기기를 제어할 수 있는 것이다.

[그림 3] 스마트싱스 허브 (*출처 : smartthings.com)

스마트홈 관련 기기도 다양해

스마트홈의 본격화를 앞두고 다양한 스마트홈 관련 기기도 주목을 받고 있다. 집안의 분위기까지 밝혀줄 듯한 스마트 조명, 똑똑한 음성 인식 비서 기기 등이 그것이다.

대표적인 스마트 조명기기에는 필립스(Philips)의 휴(Hue)가 있다. 휴는 무선 네트워크 기능이 있는 전구를 소켓에 꽂아 간편하게 사용할 수 있다. 스마트 폰 앱을 이용해 색과 밝기를 조절할 수 있는데 출시된 지 꽤 된 만큼 국내에서도 사용자가 많다. 샤오미(Xiaomi)가 지난 6월 발표한 스마트 램프 이라이트(Yeelight)는 휴와 비교했을 때 일단 가격 경쟁력면에서 우수하다. 휴의 5분의 1도 안 되는 가격으로 출시됐기 때문이다. 터치슬라이드로 컬러와 밝기를 조절할 수 있고 블루투스 원격조정이 가능하다. 스택(Stack)의 알바(AIba)는 좀 더 진화한 형태의 스마트 전구로, 사용자의 제어 없이도 사람의 움직임이나 실내 밝기 등을 감지해 자동으로 상황에 맞는 빛의 강도 및 색상을 조절한다.

음성인식 비서 아마존(Amazon) 에코(Echo)는 엄밀히 따지면 인터넷과 블루투스가 가능한 스피커다. 하지만 실제 하는 일은 정말 비서라 부를 만하다. 마이크와 스피커를 갖고 있어 사용자가 '알렉사(Alexa)'라고 부른 뒤 음성 명령을 내리면 적절한 결과를 음성으로 알려준다. 알렉사는 아마존이 개발해 온 클라우드 기반의 음성 인식기술인데, 에코는 알렉사와 연결해 음성을 인식하는 것이다. 온라인 쇼핑뿐 아니라 검색, 음악 재생, 일정 관리, 날씨, 알람, 타이머 등 컴퓨터와 스마트폰의 역할을 일정부분 대체할 수 있다는 점에서 유용하다. 에코는 벨킨의 위모, 필립스 휴 등 과도 연동된다. 앞으로 많은 기기와의 호환성 확장 여부에 따라 스마트홈 플랫폼 역할을 대체할 수 있을 지 기대된다.

[그림 4] 음성 인식 기술이 적용된 아마존 에코 (*출처 : Amazon.com)

국내도 스마트홈 시장 선점 경쟁 치열

국내에서도 이동통신 3사와 가전업체 등에서 사물인터넷 시장선점을 위한 분주한 움직임을 볼 수 있다. SK텔레콤은 '모비우스(Mobius)', KT는 '올레 기가 IoT 플랫폼', LG유플러스는 '홈챗(HomeChat)'이라는 이름의 사물인터넷 플랫폼을 각각 출시 및 계획하고 있다. SK텔레콤은 모비우스를 바탕으로 도어락(아이레보), 제습기(위닉스), 보일러(경동 나비엔) 가스밸브차단(타임밸브) 등의 제품을 내놓았다. LG 유플러스는 가스밸브 차단, 홈CCTV 이외에도 스위치, 플러그, 에너지 관리 제품을 계획하고 있다. KT 역시 홈피트니스와 보안카메라를 출시했다. 삼성과 LG는 이미 스마트 TV, 스마트 오븐, 스마트 에어컨, 스마트 세탁기, 스마트 냉장고, 로봇 청소기 등을 내놓으며 스마트홈 구축에 열을 올리고 있다. 이들 제품 중 하나를 쓰고 있다면 이미 스마트홈 세계에 발을 들여놓은 것이라고 봐도 좋다.

편리하고 똑똑한 스마트홈, 과제는?

하지만 스마트홈 구축에 앞서 생각해야 하는 것이 보안이다. 가정의 사물인터넷 기기는 개인과 아주 밀접한 많은 양의 정보를 처리하고 있는 만큼 해킹을 당할 경우 개인정보 유출의 문제는 현재의 심각성을 훨씬 뛰어넘을 것으로 보이기 때문이다. 보안의 뒷받침 없이는 사물인터넷의 발전을 논하는 것이 무의미한 이유가 바로 여기에 있다. 네트워크에 연결된 기기의 수가 증가하고 이들간의 상호작용이 더 늘어날수록 보안이 더 강화돼야 하지만 현재의 스마트홈 기기는 비밀번호 정도의 낮은 보안이 적용돼 있는 실정이다.

스마트홈은 조만간 우리 생활 곳곳에 깊숙이 자리잡아 더 이상 없어서는 안 될 존재가 될 것이다. 지금은 편리하고 익숙한 스마트홈 전성기를 향해 달려가는 과도기 정도로 보는 게 좋겠다. 머지 않아 많은 사람들은 스마트홈의 편리함에 익숙해질 것이다. 스마트폰에 그랬던 것처럼.

안랩, 여성 일자리 창출을 위한 무료 SW 교육 제공

안랩은 최근 여성의 일자리 창출을 돕는 '안랩 샘(AhnLab SEM(Software Education Manager)'을 안랩의 주요 사회공헌 프로그램으로 채택하고, 올해 하반기 수강생을 모집한다고 밝혔다.

'안랩 샘'은 출산/육아 등으로 수년간 직장을 떠나 있었던 이른바 경력단절여성이나 여성 구직자를 소프트웨어 교사 및 강사로 만드는 체계적인 소프트웨어 코딩 교육강사 양성과정이다. 안랩은 지난해(2014년) 소셜벤처 (주)맘이랜서와 함께 해당 프로그램의 공동 시범운영을 진행한 바 있으며, 올해 하반기 1회 교육 진행 후 추후 매년 3회씩 교육프로그램을 확대 진행해 다수의 코딩교사를 양성할 계획이다.

특히 '안랩 샘'은 안랩의 사회공헌 강화 차원의 무료교육 과정으로 안랩이 교육비 전액과 교육시설을 무료로 제공하고, (주)맘이랜서는 교육 프로그램의 구성 및 실행을 담당한다. 교육용 테크키트 개발 기업 헬로긱스와 한빛미디어 출판사는 교육과정 콘텐츠 개발 및 교육, 교재 출판을 지원한다.

'안랩 샘'은 PC, 인터넷, SNS 등 기본적인 IT 활용능력을 갖춘 20세 이상의 여성이라면 누구나 신청할 수 있다. 또한 경력단절여성 및 교육 분야 구직 활동 중인 여성을 우대하며, 남성 지원자의 경우 전체 모집정원 15% 이내에서 구직자 우선으로 선발한다.

'안랩 샘' 수료자들은 코딩교육 서비스 전문가로서 기업/교육기관 등에서 진행하는 코딩교육 강사 취업이나 개인 창업, 안랩 샘 교육과정의 강사 및 안랩 샘 파트너 주관의 각종 코딩 교육 프로그램의 강사 등으로 활동할 수 있다.

한편 안랩은 '안랩 샘'을 우선 사회공헌(CSR, Corporate Social Responsibility) 프로그램으로 진행하고 추후 사회와 기업의 공유가치를 만들어 내는 '공유가치창출(CSV, Creating Shared Value)' 사업으로 점진적으로 발전시킬 계획이다. 이와 관련해 안랩 김기인 전무는 "SW가 생활 속에 존재하는 환경에서 코딩 교육은 점차 중요해질 수밖에 없다"라며, "안랩은 안랩이 가장 잘 할 수 있는 방법으로 사회공헌활동을 지속할 것이다"고 말했다.

안랩, 모바일 최적화 웹사이트로 새단장

안랩이 지난달 스마트폰, 태블릿 등 모바일 환경에서 안랩의 보안 콘텐츠와 언어권별 일관된 웹서비스를 효과적으로 제공하기 위해 국내 및 글로벌 모바일 전용 웹사이트를 새롭게 오픈했다.

이번에 선보인 안랩의 모바일 웹사이트는 ▲모바일 환경에 최적화된 보안정보, 동영상 등 콘텐츠 제공 ▲1:1 상담, 교육신청 등 모바일 고객지원 서비스 업그레이드 ▲국내 및 해외 모바일 사용자에게 일관성 있는 사용자 경험(UX) 제공 ▲안랩의 보안 동영상 콘텐츠 플랫폼 '안랩TV'를 반응형 웹으로 개편한 것이 특징이다. '반응형 웹(Responsive Web)'이란 사용자의 스마트폰, 태블릿 등의 사용환경에 따라 유연하고 적절하게 반응하는 웹 디자인 구조를 의미한다.

안랩은 기존 국내 모바일 웹사이트 개편과 글로벌 모바일 웹사이트 신규 구축을 동시에 진행했다. 이로써 국내 사용자뿐만 아니라 영어권/중국어권/일본어권 등의 사용자도 모바일 환경에서 일관성 있는 사용자 인터페이스(UI)로 안랩의 보안정보와 제품 소개자료, 고객지원 서비스 등을 사용할 수 있다.

특히 보안과 관련된 다양한 동영상 콘텐츠 플랫폼인 '안랩TV'를 '반응형 웹'으로 설계해 사용자의 다양한 기기 디스플레이 환경에 따라 자동으로 사용자의 디바이스 해상도에 따른 최적의 레이아웃과 사용성을 제공한다. 모바일 '안랩 TV'의 콘텐츠는 국내 모바일 웹사이트에서만 제공된다.

안랩 EP 사업기획실 이상국 실장은 "안랩은 모바일 환경이 점차 확산됨에 따라 고객의 정보 접근성 향상을 위해 모바일 웹에 대한 개편 및 신규 오픈을 진행했다"며 "향후에도 모바일 웹 플랫폼을 발전시켜 모바일을 활용한 마케팅과 다양한 프로모션을 펼쳐 나갈 것"이라고 말했다.

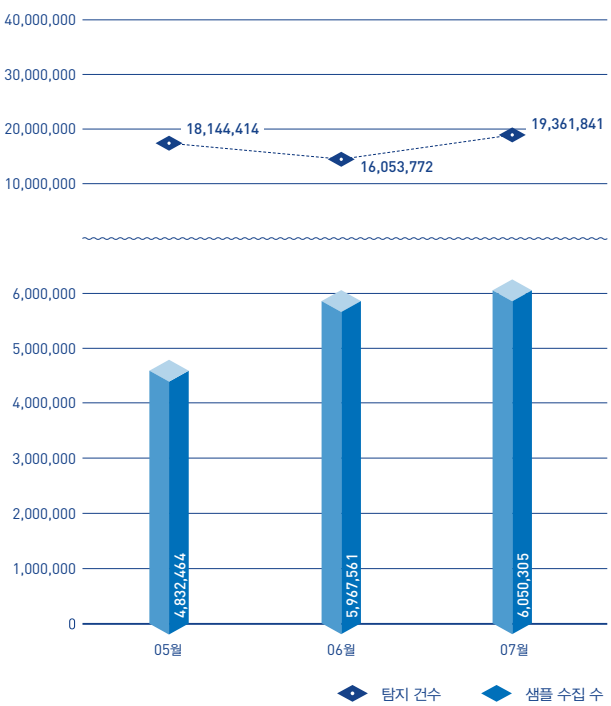
ASEC, 7월 악성코드 통계 및 보안 이슈 발표

'즐겨찾기' 노리는 파밍 악성코드 등장

안랩 시큐리티대응센터(ASEC)는 ASEC Report Vol.67을 통해 지난 2015년 7월의 보안 통계 및 이슈를 전했다. 7월의 주요 보안 이슈를 살펴본다.

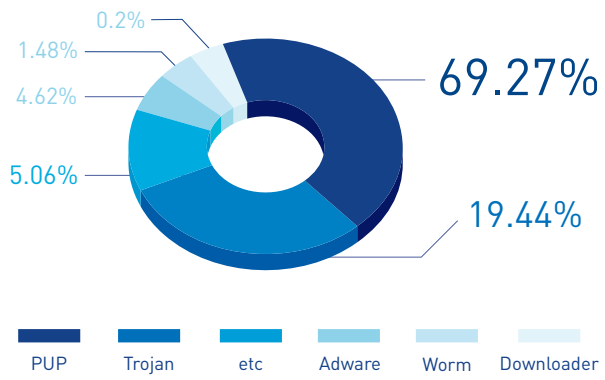
ASEC이 집계한 바에 따르면 2015년 7월 한 달간 탐지된 악성코드 수는 1,936만 1,841건이다. 이는 전월 1,605만 3,772건에 비해 330만 8,069건 증가한 수치다. 한편 7월에 수집된 악성코드 샘플 수는 605만 305건이다.

[그림 1]의 '탐지 건수'란 고객이 사용 중인 V3 등 안랩의 제품이 탐지한 악성코드의 수를 의미하며, '샘플 수집 수'는 안랩이 자체적으로 수집한 전체 악성코드 샘플 수를 의미한다.



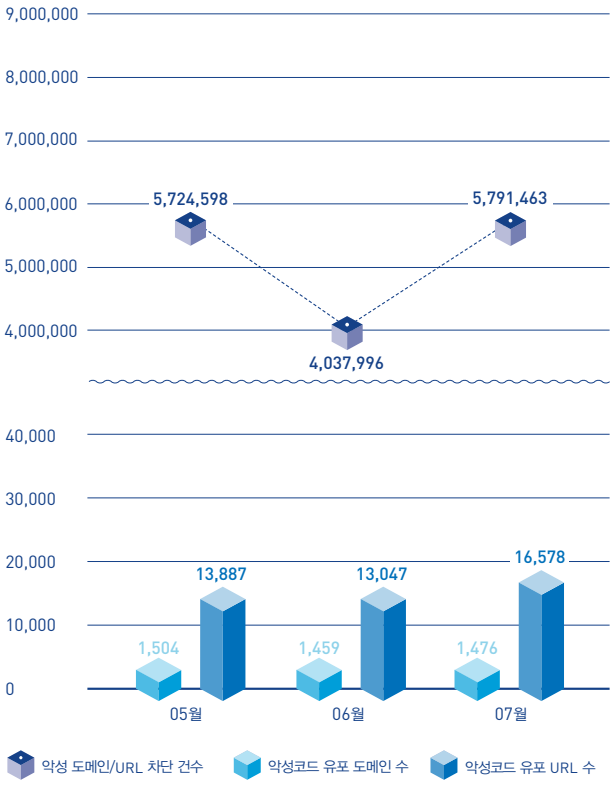
[그림 1] 악성코드 추이(2015년 5월 ~ 2015년 7월)

[그림 2]는 2015년 7월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 69.27%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 19.44%, 애드웨어(Adware)가 4.62%로 그 뒤를 이었다.



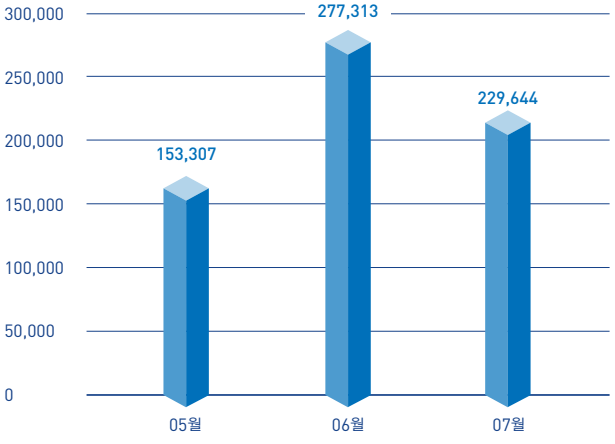
[그림 2] 2015년 7월 주요 악성코드 유형

지난 7월 악성코드 유포지로 악용된 도메인은 1,476개, URL은 1만 6,578개로 집계됐다. 또한 7월의 악성 도메인 및 URL 차단 건수는 총 579만 1,463건이다. 악성 도메인 및 URL 차단 건수는 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트의 접속을 차단한 수이다.



[그림 3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 5월 ~ 2015년 7월)

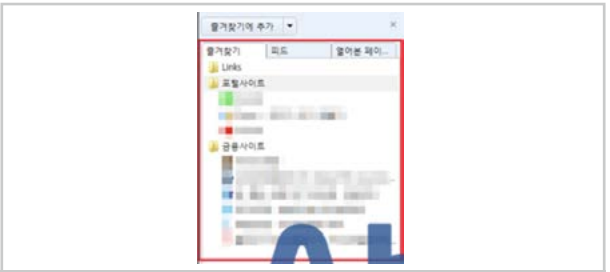
또한 지난 7월 한 달간 탐지된 모바일 악성코드는 22만 9,644건으로 집계됐다.



[그림 4] 모바일 악성코드 추이(2015년 5월 ~ 2015년 7월)

사용자의 '즐겨찾기'를 조작하는 파밍 악성코드

최근 사용자의 즐겨찾기 주소를 변경해 사용자를 가짜 웹 페이지로 유도하는 '파밍(Pharming)' 악성코드가 확인돼 사용자들의 주의가 필요하다. 이번에 발견된 파밍 악성코드는 많은 사용자들이 금융 사이트를 즐겨찾기에 등록해두고 사용한다는 점을 노렸다.



[그림 5] 인터넷 익스플로러(IE)의 '즐겨찾기' 기능

'파밍(Pharming)'이란 사용자의 컴퓨터에 악성코드를 감염시켜 사용자가 은행 사이트에 접속할 때 가짜 사이트로 연결되도록 조작하여 금융정보를 탈취하는 공격 방법이다. 이번에 발견된 '즐겨찾기'에 등록해둔 금융 사이트를 변조하는 파밍 악성코드는 [그림 6]과 같이 실행 파일(.exe) 형식을 하고 있다.

[그림 6] '즐겨찾기' 변조 파밍 악성코드

[그림 6]의 'exp.exe' 파일을 실행하면 [그림 7]과 같이 '4.exe', '5.exe'라는 파일이 같은 경로에 생성 및 실행된다.

[그림 7] 4.exe, 5.exe

'4.exe' 파일이 실행되면 'user.qzone.qq.com'라는 사이트에 접속하여 아래와 같은 가짜 웹 페이지 주소 및 카운터 페이지 주소를 가져온다. 또한 사용자의 IP주소를 수집하기 위해 'www.get-ip.me'에 접속하고 감염 시스템의 운영체제 정보를 수집한다.

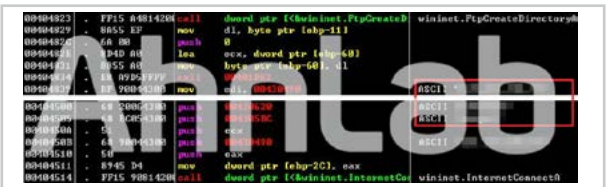
[가짜 웹 페이지 주소 정보]

... 생략
<title>my********.com [http://3********4.qzone.qq.com]</title>
... 이하 생략

[카운터 페이지 주소 정보]

... 생략
<title>s********1.com [http://5******2.qzone.qq.com]</title>
... 이하 생략

또한 '5.exe' 파일은 사용자 PC 내의 공인인증서 경로를 탐색한다. 공인인증서 폴더가 존재하면 이를 압축하여 FTP를 통해 외부로 전송한다.



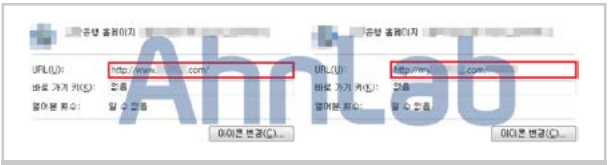
[그림 8] 외부 서버 FTP 정보

해당 악성코드는 사용자가 저장해둔 즐겨찾기 주소를 변조하기 위해 인터넷익스플로러(IE), 크롬 등의 웹 브라우저의 즐겨찾기 파일이 저장된 경로를 확인한다. 이렇게 확인 및 수집한 즐겨찾기의 URL주소 중에 [표 1]의 금융 기관 리스트에 포함되는 은행 및 이와 관련된 특정 단어가 포함되어 있을 경우, 해당 URL을 가짜 웹 페이지의 주소로 변경한다.

금융 사이트	단어(Keyword)
A 은행	*****r
B 은행	*****bank
C 은행	******n
D 은행	**k
E 은행	******p
F 은행	*****bank
G 은행	****bank
H 은행	**bank
I 은행	**b
J 은행	***c
K 은행	***************d

[표 1] 변조 대상인 금융 사이트 및 관련 단어

이러한 사실을 알리 없는 사용자가 평소와 같이 즐겨찾기를 통해 해당 금융 사이트에 접속하면, 변조된 URL의 가짜 금융 사이트([그림 9]의 오른쪽)로 연결된다. 물론 이 가짜 금융 사이트는 실제 금융 사이트를 교묘하게 모방해 사용자들의 의심을 피한다.



[그림 9] 정상 URL주소 (왼쪽) / 변조된 URL 주소(오른쪽)

가짜 웹 페이지 내부에는 특정한 코드가 삽입되어 있으며, 사용자가 해당 페이지에서 어떤 버튼이라도 클릭하면 [그림 10]과 같은 경고창이 나타난다.

[그림 10] 경고 메시지

이 경고창의 확인 버튼을 클릭하면 [그림 11]과 같이 사용자의 개인정보 및 금융정보 입력을 유도하는 페이지가 나타난다.

[그림 11] 개인정보 및 금융정보 탈취 페이지

'금융사기 주의 안내'라는 내용으로 위장한 해당 페이지는 오히려 사용자의 이름, 주민등록번호, 핸드폰 번호를 요구하고 있을 뿐만 아니라 [그림 12]와 같이 계좌번호와 비밀번호, 사용자 아이디 및 비밀번호, 인증서 비밀번호, 보안카드 일렬번호, 보안카드 번호까지 요구하고 있다. 만일 사용자가 해당 페이지에서 요구하는 정보들을 입력하면 해당 정보는 고스란히 악성코드 제작자에게 전송된다.

[그림 12] 개인정보 및 금융정보 탈취페이지

파밍 악성코드가 등장한 것은 꽤 오래 전으로, 지난 2011년 이후 본격적인 피해가 발생한 지속적으로 증가하고 있다. 특히 최근에는 백신(Anti-Virus) 등 보안 솔루션의 탐지를 피하고 사용자들을 속이기 위해 점점 더 교묘하게 진화하고 있다. 특히 이번에 발견된 '즐겨찾기'를 변조하는 파밍 악성코드는 기존의 악성코드와 달리 시작프로그램이나 서비스 영역에 악성 파일을 등록하지 않는다. 따라서 악성 파일이 처음 실행된 이후 다시 실행되지 않기 때문에 해당 악성코드에 의한 감염 여부를 확인하기가 쉽지 않다.

한편 V3 제품은 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

〈V3 제품군의 진단명〉

Trojan/Win32.Banki (2015.07.04.01)

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

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