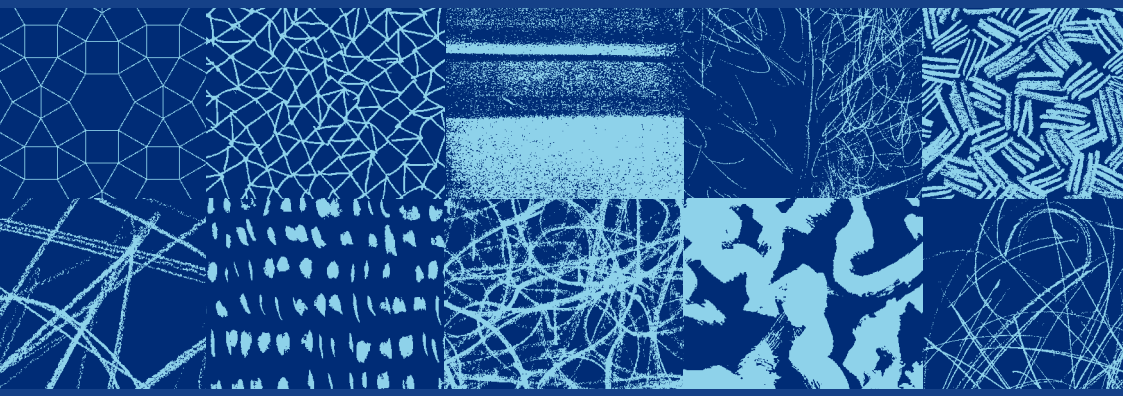
AhnLab



2015 연간 보고서

2015 ANNUAL REPORT

01
2015년 보안 위협 결산

2015년을 뒤흔든 보안 위협 Top 5

1. 깨어난 랜섬웨어의 광풍

랜섬웨어는 국내뿐만 아니라 전 세계적으로 보안 분야의 가장 큰 이슈였다. 북미 지역 및 유럽 등을 중심으로 폭발적인 증가 추세를 보인 가운데, 국내에서는 지난 2015년 4월 국내 유명 커뮤니티 사이트를 통해 한글화된 크립토락커가 대량 유포된 때를 기점으로 랜섬웨어가 급격하게 증가하고 있다.

기존에는 주로 문서 파일(doc, ppt 등)과 이미지 파일(jpeg 등)을 암호화했으나 최근에는 실행 파일(exe)을 포함한 140여 개의 확장자가 암호화 대상이 되었다. 또한, 데이터를 암호화하는 방식에서 더 나아가 화면 잠금을 통해 PC 구동 자체를 불가능하게 하는 랜섬웨어도 등장했다.

랜섬웨어의 '지역화' 양상도 나타났다. 북미와 유럽 지역에서는 비트크립트(BitCrypt)와 코인볼트(CoinValut)가, 러시아 및 터키 등 동유럽 지역에서는 트롤데시(TrolDesh) 등의 랜섬웨어가 큰 피해를 입혔다. 반면 국내에서는 크립토락커, 크립토월(CryptoWall), 테슬라크립트(TaslaCrypt), 나부커(Nabucur) 등의 랜섬웨어 감염 빈도가 높았다.

2. 결국은 '돈', 계속되는 금융 정보 위협

2015년에도 금융 정보를 노린 악성코드가 기승을 부렸다. 전 세계 1,000여 개 은행과 기업을 노리며 악명을 떨쳤던 다이어(Dyre) 악성코드가 올해 초 국내 은행을 공격 대상에 포함해 국내 금융 업계를 긴장시켰다. 최근에는 Windows 10과 엣지 브라우저(Edge Browser) 등 최신 운영체제와 브라우저에서도 정보를 탈취하는 등 더욱 진화하는 양상을 보인다. 파밍(Pharming) 사이트로 사용자를 유도해 금융 정보를 탈취하는 뱅키(Banki)류의 악성코드도 2015년 하반기에는 유포 방식을 바꾸는 등 여전히 기승을 부리고 있다.

금융 정보를 탈취하는 악성코드의 공격 대상은 은행만이 아니다. POS(Point of Sale) 시스템을 통해 카드 정보를 유출하는 POS 악성코드가 2015년 들어 다시 증가하기 시작한 것이다. 체리피커(Cherry Picker), 모드포스(ModPOS) 등이 2015년 등장한 대표적인 POS 악성코드다. POS 악성코드의 위험성은 지난 2013년 말 해외 대형 마트에서 대규모 카드 정보 유출 사건이 발생하면서 수면 위로 떠올랐다. 국내에서도 POS 단말기를 통한 카드 정보 유출 및 이에 따른 금전적 피해가 발생하며 POS 위협이 나날이 심화되고 있다.

3. 웹 익스플로잇 툴킷의 역습

랜섬웨어를 비롯해 2015년을 뒤흔든 수많은 보안 위협의 뒤에는 웹 익스플로잇 툴킷(Web Exploit ToolKit)이 있었다. 게다가 이전보다 훨씬 정교한 방식으로 존재감을 드러내고 있다.

'웹 익스플로잇 툴킷'은 다수의 취약점을 악용해 사용자 PC에 악성코드를 감염시키기 위한 공격 도구로, 공격자들은 이를 이용해 악성코드를 손쉽게 제작하고 유포한다. 2015년에 맹위를 떨친 대표적인 웹 익스플로잇 툴킷은 '앵글러(Angler) 툴킷'이다. 지난 4월 국내 유명 커뮤니티에서 유포된 랜섬웨어 공격의 배후에도 바로 이 앵글러 툴킷이 있었다.

공격자들은 웹 익스플로잇 툴킷을 이용한 악성코드의 유포 경로 추적을 더욱 어렵게 만들기 위해 다양한 블로그 제작툴이나 콘텐츠 관리 시스템 등을 이용하거나 동적 콘텐츠를 생성하는 광고 사이트를 악성코드 배포에 이용하는 방식인 '멀버타이징(Malvertising)' 기법을 이용하기도 했다. 또한 백신의 탐지를 우회하려는 시도도 더욱 정교화되어 웹 익스플로잇 툴킷은 더욱 심각한 위협으로 자리잡았다.

4. 애드웨어, 모바일 환경으로 영역 확장

과다한 광고 노출 등으로 사용자 불편을 야기하는 '애드웨어(adware)'가 모바일 환경으로 영역을 확장했다.

2015년 발견된 모바일 애드웨어 수가 전년 대비 약 2.5배가량 증가했다. 모바일 애드웨어는 개인 정보 수집, 과도한 광고 노출, 앱 바꿔치기 등 스마트폰 이용의 불편함을 넘어 악의적인 행위로 피해를 야기하고 있다. 특히 최신 모바일 애드웨어는 다른 앱을 사칭하거나 루트 권한을 획득해 삭제를 방해하는 등 한층 교묘해진 수법으로 스마트폰 사용자를 노리고 있다.

그 밖에 2015년 모바일 위협은 전년과 비슷하거나 다소 감소하는 추세를 보였다. 2012년 이후 매년 2배 이상 급증세를 보이던 모바일 뱅킹 악성코드는 전년도와 비슷한 수를 유지했고, 모바일 악성코드의 유포 방법으로 이용되던 스미싱은 2015년 하반기 들어 감소 추세를 보였다. 이는 미래부, KISA(Korea Internet & Security Agency, 한국인터넷진흥원), 경찰청 등 관련 기관의 적극적인 스미싱 메시지 및 네트워크 차단 노력, 보안 업체 및 이동통신사 등 민간업체들의 이용자 보호 조치, 언론 보도 및 캠페인을 통한 국민 보안 의식 증진 등에 의한 결과로 풀이된다.

5. 공유기, IoT 등 '연결'을 노리는 위협의 대두

2014년에 이어 2015년 초부터 국내 유명 제작사의 유 • 무선 공유기의 취약점을 노린 해킹 시도가 지속적으로 발견됐다. 공유기의 취약점을 이용해 관리 권한을 획득하면 공유기와 연결된 모바일 기기나 PC를 동시에 공격할 수 있어 위험도가 높다.

네트워크에 연결된 기기에 대한 보안 위협은 공유기뿐 아니라 사물 인터넷까지 공격 범위를 확장하고 있다. 최근 각종 웨어러블 기기(Wearable device) 등 개인용 사물 인터넷 기기(Internet of Things)가 증가함에 따라 이들 기기의 보안에 대한 우려도 커지고 있다. 대표적인 사물 인터넷 기기인 IP 카메라, NAS(Network Attached Storage), CCTV 등

은 일반 컴퓨터와 유사한 운영체제를 가지고 있어 공격자들이 쉽게 접근할 수 있다. 특히 이러한 기기들은 네트워크에 항상 연결되어 있는 반면 아직 마땅한 보안 대책은 없는 형편이다. 인터넷 공유기나 사물 인터넷 관련 기기 등 항상 '연결'된 상태의 기기를 안전하게 이용하려면 각 제조사에서 제공하는 펌웨어 업데이트나 관리 비밀번호 수시 변경 등의 사용자 노력이 중요하다.

02
2016년 보안 위협 전망

2016년을 장악할 보안 위협 Top 5

1. 랜섬웨어의 지속적인 고도화

랜섬웨어 위협은 2016년에 더욱 거세질 전망이다. 랜섬웨어의 암호화 대상 확대, 화면 잠금 등 사용자의 조치를 방해하는 기능 추가 등 지속적인 진화가 예상된다. 특히 안랩을 비롯한 보안 업체들이 랜섬웨어 진단 및 차단 기능을 강화함에 따라 보안 제품의 탐지를 우회하거나 방해하는 등의 고도화된 랜섬웨어가 등장할 것으로 예측된다.

모바일 랜섬웨어가 국내에 상륙할 가능성도 점쳐진

다. 아직 국내에서는 모바일 랜섬웨어 감염이 확인된 바 없으며, 대부분의 모바일 랜섬웨어는 영어로 제작되어 있다. 그러나 PC 랜섬웨어가 그랬듯, 향후 한글화된 모바일 랜섬웨어가 등장해 국내 스마트폰 사용자들에게 막대한 피해를 준다 해도 전혀 이상할 것이 없다. 모바일 랜섬웨어가 국내 스마트폰 사용자를 노리기 시작하면 지난 2014년 사회적 화두가 됐던 스미싱 악성코드와는 비교할 수 없을 정도의 피해를 야기할 수도 있다.

한편 안드로이드를 대상으로 하는 랜섬웨어 수는 2014년 2,220건에서 2015년 27,845건으로, 1년새 12배가 넘게 증가했다. 2016년에도 모바일 랜섬웨어 변형은 계속해서 증가할 것으로 보인다.

2. 사라지지 않는 사이버 테러 및 국가 기반 시설 위협

지난 2015년 연말 발생한 '파리 테러' 사건은 전 세계를 충격으로 몰아넣었다. 종교적 • 이념적 갈등에 따른 국가 간의 대립은 사이버 세계에서도 별반 다르지 않다. 과거에는 테러가 물리적인 파괴에 국한됐던 것에 반해 최근 인터넷을 통한 테러리스트들의 이념 선전 및 정보 수집, 적대국 도 • 감청과 정보 유출 등의 테러는 이미 사이버 환경에 깊숙이 침투해 있다.

일반 대중에게 공포감을 조성하는 것이 테러의 목적이라는 점에서 국가 기반 시설을 노린 고도화된 지능형 위협인 APT(Advanced Persistent Threat)의 가능성도 배제할 수 없다. 물론 국가 기반 시설은 다수의 보안 시스템으로 겹겹이 보호되고 있을 뿐만 아니라 대부분 직접 인터넷에 연결하지 않는 것을 원칙으로 폐쇄망 환경에서 운영되고 있어 비교적 위협에 노출될 가능성이 작다. 그러나 이란 부셰르 핵발전소의 스턱스넷(Stuxnet) 감염, 일본 핵 발전소 정보 유출 사건, 그리고 최근의 미국 뉴욕 댐 통제 시스템 보안 침해 등 국가기반 시설을 노린 사이버 공격 사례가 국내 • 외에 지속적으로 발생하고 있다. 정치적 갈등과 장기적인 세계 경기 침체의 영향으로 국제 정세가 급변함에 따라 국가 기반 시설 보안의 중요성도 더욱 강조된다.

3. 웹 브라우저부터 클라우드와 가상 환경까지 노리는 취약점 공격

2016년에는 인기 있는 소프트웨어의 취약점을 활용한 공격이 더욱 기승을 부릴 것으로 보인다.

마이크로소프트(Microsoft)는 2016년 1월 12일을 기점으로 자사 웹 브라우저인 인터넷 익스플로러(Internet Explorer, 이하 IE)의 최신 버전을 제외한 이전 버전에 대한 지원을 종료하겠다고 밝혔다. 즉, 최신 버전이 아닌 구 버전의 IE에서 새로운 취약점이 발견되더라도 2016년 1월 12일 이후에는 해당 취약점에 대한 패치가 제공되지 않기 때문에, 이를 노린 공격이 증가할 것으로 예상된다.

지난해에는 국내에서 많이 사용 중인 문서 편집 프로그램이나 기타 프로그램의 취약점도 다수 발견됐다. 대중적인 소프트웨어의 신규 취약점을 이용한 공격은 비교적 사용자의 의심을 쉽게 피할 수 있어 앞으로도 주요 공격 방식으로 사용될 것이 분명하다. 2016년에는 단순 취약점 보고를 넘어 취약점 이용 공격으로

인한 구체적인 피해 사례가 발생할 것으로 예상된다.

또한 2015년에는 가상 환경 시스템에서 발생 가능한 '베놈(VENOM, Virtualized Environment Neglected Operations Manipulation)' 취약점을 비롯해 특정 가상화 솔루션의 임의 코드 실행 취약점 등이 발견됐다. 최근 다수의 국내 기업에서 클라우드 또는 가상화 인프라 도입을 검토함에 따라 이들 환경에 대한 보안 위협도 구체화될 것으로 보인다.

4. 사물인터넷(IoT), 스마트홈을 둘러싼 위협의 현실화

IT 기술과 기기가 빠른 속도로 발전함에 따라 이제 사이버 위협의 범위는 PC를 벗어나 광범위하게 확대되고 있다. 사실상 컴퓨터와 성능과 기능 면에서 큰 차이가 없는 사물인터넷 기기가 속속 등장하는 등 인터넷에 연결되는 기기가 늘어날수록 새로운 사이버 위협 또한 계속해서 증가할 전망이다.

일반 가정에서도 흔히 볼 수 있는 무선공유기를 비롯해 가정용 전원 컨트롤, 난방 제품 제어시스템 등 스마트홈 기술이 발전하면서 이에 대한 보안 위협의 고려가 시급하다. 이 밖에도 현재 각국에서 유효성 검증과 관련 법제 마련이 한창인 드론(Drone)이나 인터넷에 연결되어 구동되는 자동차(Connected Car), 이른바 스마트카에 대한 위협 또한 머지않아 현실화될 전망이다.

5. 새로운 금융 환경을 노리는 위협의 등장

금융 정보, 금융 시스템은 언제나 사이버 위협의 핵심 타깃이었으며, 금융 환경이 온라인화될수록 위협의 정도 또한 심화되었다. 2016년에는 인터넷 전문 은행이 출범함에 따라 이를 둘러싼 보안 위협이 증가할 전망이다.

인터넷 전문 은행은 오프라인 영업점이 존재하지 않기 때문에 본인 확인 시 비대면 실명 확인이 필수불가결하다. 이에 실명 확인 절차부터 중요한 보안 이슈로 떠오르고 있다. 또한, 스마트폰을 이용한 모바일 거래 위협에 대한 우려도 크다. 인터넷 전문 은행이 출범하면 스마트폰을 이용한 모바일 거래가 많아질 수밖에 없다. 지난 몇 년간 소액 결제나 뱅쿤 등 모바일 악성코드를 통한 금융 정보 탈취 피해가 빈번하게 발생하고 있으며 스마트폰 사용자를 노린 파밍 공격 등도 증가하고 있는 만큼, 인터넷 전문 은행 도입과 관련해 모바일 금융 거래의 보안 강화가 시급한 시점이다.