Security Trend

ASEC REPORT

2014 Annual Report

AhnLab

ASEC REPORT

2014 ANNUAL REPORT

ASEC(AhnLab Security Emergency response Center)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 안랩의 ASEC에서 작성하며, 매월 발생한 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 자세한 내용은 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

2014년 연간 보고서

Table of Contents

연간 위협 동향

2014년 보안 위협 동향

2014 보안 위협, 영역과 경계를 파괴하다

연초 대규모 개인정보 유출부터 연말 공공기관 해킹까지 2014년은 사회 전반에 걸쳐 '정보 보안(보호)'이 핫이슈가 된 해였다. 특히 개인정보 유출 사건 • 사고는 거의 매달 발생했다고 해도 과언이 아닐 정도로, 안전행정부 발표 자료에 따르면 2014년 상반기에만 5,300만 명의 개인정보 8,600만 여건이 유출된 것으로 추정된다. 그야말로 '보안 위협'이 개인과 기업을 넘나들며 사회적 • 국가적 피해를 야기하고 있다.

2014년의 주요 보안 이슈는 ▲스마트폰 보안 위협 ▲인터넷 뱅킹을 노린 파밍 악성코드 ▲공격 경로의 다양화 ▲POS(Point-of-Sales) 시스템 해킹 ▲ 다수의 오픈소스 취약점 등장 등으로 요약할 수 있다. 스마트폰, POS 시스템, 오픈소스 등의 키워드에서 볼 수 있는 것처럼 지난 한해 보안 위협은 다양한 플랫폼(platform)으로 확대되었다.

1. 스마트폰으로 확대되는 보안 위협

지금까지 주로 PC 환경에서 자주 등장했던 보안 위협이 2014년에는 스마트폰 환경으로 옮겨가는 한편 본격적으로 모바일 환경에 특화된 보안 위협이 대거 등장했다.

우선 '랜섬웨어(Ransomeware)'가 PC에 이어 스마트폰으로 확산됐다. 사용자의 데이터를 볼모로 금전을 요구하는 랜섬웨어는 지난 한해 동안 PC와 스마트폰 등 플랫폼을 가리지 않고 꾸준히 발견됐다. 해외에서는 FBI를 사칭한 조직이 스마트폰 사용자들을 노리고 유포한 랜섬웨어인 '심플로커(SimpleLocker)'로 실질적인 피해가 발생하기도 했다.

PC를 노리던 이른바 '몸캠피싱'도 스마트폰으로 확대되기도 했다. 몸캠피싱이란 화상채팅 등을 통해 음란 행위를 하는 것을 뜻하는 '몸캠'과 사용자를 허위 사이트 또는 프로그램으로 유도하는, 즉 낚는 것을 뜻하는 '피싱'의 합성어다. 스마트폰 상에서의 몸캠피싱 기법은, 공격자가 스마트폰 채팅 애플리케이션을 이용해 음란 화상 채팅을 유도하여 사용자의 얼굴과 알몸 등을 동영상으로 녹화하는 한편 악성 앱 설치를 유도해 스마트폰 내 주소록을 탈취하는 방식이다. 이후 공격자는 수집한 주소록에 있는 사용자의 지인에게 몸캠 동영상을 전송한다고 협박하며 금전을 요구한다.

'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. 사용자를 현혹하는 스미싱 문구 또한 '택배', '청첩장/돌잔치/생일 초대장', '예비군/민방위' 등을 사칭하는 사례가 지속적으로 발견되는 가운데 층간 소음, 분리수거 위반, 쓰레기 무단투기 등 실생활에서 쉽게 경험할 수 있는 민원을 사칭한 이른바 '생활 밀착형' 스미싱이 등장했다.

이처럼 스마트폰을 노리는 보안 위협이 심화되는 가운데 주요 정보를 스마트폰에 저장하는 빈도가 높아지는 만큼 각별한 주의가 필요하며, 특히 출처가 불분명한 스마트폰 앱을 다운로드할 시에는 더욱 유의해야 한다.

2. 인터넷 뱅킹을 노린 파밍 악성코드, '메모리 해킹'까지

2013년 이후 인터넷 뱅킹 정보를 노리는 '파밍(Pharming)' 악성코드의 피해가 이어졌고 2014년에는 더욱 심화되는 양상을 보였다.

기존 파밍 악성코드는 PC의 호스트 파일을 변조해 가짜 인터넷 뱅킹 사이트로 유도하는 방식이었다. 2014년에는 인터넷 도메인네임시스템(DNS) 정보를 담고 있는 메모리를 변조해 사용자가 가짜 사이트로 이동하는 것을 더욱 인지하기 어렵게 하는 방식이 등장했다. 또한 정상 사이트에 방문했어도 이체거래 과정에서 금융거래정보 등을 실시간 변조하기 위해 인터넷 뱅킹 모듈의 메모리 영역을 해킹하는 형태까지 진화했다. 인터넷 뱅킹의 메모리 해킹이란 컴퓨터의 메모리에 있는 수취인의 계좌번호, 송금액을 변조하거나 보안카드 비밀번호를 탈취한 후 돈을 빼돌리는 새로운 해킹 방식이다. 정상적인 인터넷 뱅킹 사이트에 접속하더라도 이체거래 과정에서 금융거래 정보 등을 실시간 위 • 변조하는 것이 특징이다.

이처럼 인터넷 뱅킹을 노리는 공격 기법이 갈수록 사용자가 인지하기 어렵게 진화하고 있어 사용자 및 기관의 주의가 요구된다.

3. 공격 경로의 다양화

기존의 취약점 공격은 악용하는 프로그램이 한정적이었다. 그러나 공격 대상이 확대됨에 따라, 특히 특정 타깃을 노리는 맞춤형 공격이 자행되면서 공격에 사용되는 프로그램, 즉 공격 경로도 다양화되고 있다.

2014년은 이메일, 전자결재, DRM(Digital Rights Management, 디지털콘텐츠 저작권 보호 기술), 그룹웨어, 암호화 솔루션 등 다양한 프로그램의 취약점을 이용해 악성코드 제작이 증가함과 동시에 이들 프로그램을 공격 경로로 이용하는 복합적인 형태의 공격이 빈번하게 포착됐다. 대표적으로 문서 프로그램의 취약점을 이용한 MBR 파괴 악성코드를 이메일의 첨부 파일 형태로 전송한 사례가 있었다. 또는 특정 프로그램의 구동과 관련된 정상 파일을 악성 파일로 교체해 악성코드를 배포하는 사례도 발견됐다.

많은 기업들이 보안에 노력을 기울이고 있음에도 불

구하고 이러한 고도화된 형태의 공격으로 악성코드에 감염된 프로그램이 고객에게 피해를 줄 수 있어 더욱 주의가 필요하다.

4. POS(Point-of-Sales) 시스템 해킹

국내외를 막론하고 지난 2014년에는 POS 단말기를 해킹해 중요 거래정보를 빼내고, 이 정보로 부당거래를 일으킨 피해가 빈번히 발생했다.

해외의 경우, 2013년 말 미국 내 대형 유통사의 POS 시스템이 해킹 당해 7천만 명 이상의 개인정보가 유출된 사건을 시작으로 2014년에는 세계 곳곳에서 백화점 • 식당 등의 POS 시스템이 해킹 당해 신용카드 정보가 유출된 사례가 지속적으로 보고됐다. 국내에서도 POS 시스템 공급 업체의 서버를 해킹해 정상 파일을 악성 파일로 교체하는 방식을 이용한 공격 사례가 발견되기도 했다.

사실 보안 전문가들은 수년 전부터 POS 시스템 보안에 대한 우려를 제기해왔다. 최근 가시적인 피해가 발생함에 따라 관련 업계 및 기업들의 POS 시스템 보안 방안 마련이 시급해지고 있다.

5. 다수의 오픈소스 취약점 등장

지금까지는 MS 오피스, 어도비, 오라클 등 다수의 개인과 기관이 사용하고 있는 프로그램들에서 취약점이 발견되는 경우가 대부분이었다. 그러나 2014년에는 특정 조직이나 시스템에서 사용하는 오픈소스 프로그램과 관련된 심각한 취약점이 발견돼 전 세계적으로 큰 충격을 주었다. '하트블리드(Heartbleed)'와 '쉘쇼크(ShellShock)' 등이 그것이다. '하트블리드'는 전 세계 웹사이트에서 대다수가 사용하는 오픈SSL(Open Secure Socket Layer)에서 발견된 취약점으로, 웹 서비스 및 모바일 비즈니스에 잠재적인 위협이 되고 있다.

이른바 '쉘쇼크'로 불리는 배쉬(Bash) 취약점은 대부분의 서버 OS로 사용되는 유닉스 및 리눅스와 관련된 취약점으로, 이를 통해 공격자가 원하는 코드를 손쉽게 실행할 수 있어 심각한 위협으로 대두되었다. 프로그램 자체의 취약점뿐만 아니라 리눅스 계열 시스템에서 동작하는 웜까지 등장하면서 보안 위협의 범위가 오픈소스 프로그램까지 크게 확장되었다.

2015년 보안 위협 전망

2015년 보안 위협 키워드, '다변화·고도화·타깃화'

최근 영역과 경계를 허물기 시작한 보안 위협은 2015년에 더욱 다변화되고 고도화될 것으로 보인다. 또한 2014년 연말의 국내외 주요 해킹 사례와 같은 타깃 공격이 더욱 거세질 것으로 전망된다. 다변화 • 고도화 • 타깃화의 키워드를 중심으로 예측 가능한 2015년 보안 위협은 ▲모바일 결제 및 인터넷 뱅킹 공격 심화 ▲공격 대상별 맞춤형 악성코드 유포와 동작 방식의 진화 ▲POS 시스템 보안 위협 본격화 ▲오픈소스 취약점 공격 및 타깃 공격을 통한 정보 유출 가속화 ▲IoT 보안 위협 등이다.

1. 모바일 결제 및 인터넷 뱅킹 공격 심화

모바일 금융 서비스가 단순 '모바일 뱅킹'에서 '모바일 결제시장'으로 그 영역과 규모가 크게 확장되고 있다. LG경제연구원에 따르면 매년 30~40%씩 성장해 2017년 800조 원에 가까운 금액이 모바일 기기를 통해 결제될 것으로 전망된다. 또한 글로벌 시장조사기관 가트너는 2016년 모바일 거래액이 6,169억 달러, 이용자 수는 4억 4,793만 명, 거래 건수로는 209억 건에 달할 것으로 추정했다.

모바일 결제가 확대됨에 따라 이를 노리는 보안 위협 또한 증가하리라는 것은 명약관화다. 2012년 소액 결제 서비스 관련 모바일 악성코드가 발견된 이후 모바일 뱅킹을 노리는 악성코드는 지속적으로 발견되고 있다. 향후 모바일 결제와 관련해 각종 피해를 유발하는 알려지지 않은 악성코드가 대량 등장할 것으로 예상되는 만큼 관련 서비스 제공 업체와 사용자의 각별한 주의가 요구된다.

한편 2015년에도 다양한 웹 익스플로잇 툴킷(Web Exploit Toolkit)을 이용한 '뱅킹 악성코드' 유포가 급증할 것으로 보인다. 웹 익스플로잇 툴킷은 다수의 취약점을 악용해 사용자 PC에 악성코드를 감염시키는 공격 코드를 만드는데 쓰인다. 메모리해킹 및 파밍뿐만 아니라 각 은행의 거래 시스템에 최적화된 악성코드가 등장할 가능성이 있으며 은행권 이외에도 카드사, 증권사 등 금융권 전반에 걸쳐 유사한 피해 사례가 등장할 것으로 예상된다.

2. 공격 대상별 맞춤형 악성코드 유포와 동작 방식의 진화

올해는 타깃형 악성코드의 증가와 함께 악성코드의 유포 및 동작 방식 또한 더욱 진화할 것으로 예측된다. 예를 들어 연말이나 연초 등 특정한 시기에 이메일 제목뿐만 아니라 첨부 문서 자체의 내용 또한 송년회 초대 또는 새해 인사 등의 내용으로 보이도록 교묘

하게 제작하여 사용자의 의심을 따돌리는 것 등이다. 또한 최근에는 시스템에서 오랫동안 은닉하는 악성코드가 주로 등장했다면 앞으로는 은닉한 상태에서 머무는 것이 아니라 수시로 은밀히 변형을 업데이트하여 보안 제품의 탐지를 효과적으로 피하는 등 동작 방식 또한 점차 진화하는 양상을 보일 전망이다.

이 밖에도 불특정 다수를 대상으로 유포되는 악성코드들이 양적으로도 뚜렷하게 증가하는 추세를 보이고 있다. 블랙마켓에서 판매되는 악성코드 자동 생성기나 익스플로잇 킷 등이 이러한 추세를 더욱 가속화할 것으로 보인다.

3. POS 시스템 보안 위협 본격화

최근 POS 시스템(Point Of Sales System) 해킹이 지속적으로 발생하면서 업체들이 보안을 강화하고 있지만 이를 뛰어넘는 다양한 방식의 공격이 등장할 것으로 예상된다. POS 시스템 제작 업체를 노리는 해킹 시도 또한 증가할 것으로 보인다.

국내외에서 POS 시스템 해킹이 증가함에 따라 보안 기능이 강화된 신용카드 결제 방식으로 전환을 서두르고 있다. 그러나 시스템과 신용카드를 모두 교체하기까지는 수년의 시간과 막대한 비용이 소요될 것으로 예상돼 당분간 POS 시스템에 대한 보안 위협은 지속될 것으로 보인다.

4. 오픈소스 취약점 공격 및 타깃 공격을 통한 정보 유출 가속화

오픈소스 프로그램들의 새로운 취약점이 등장할 것으로 예상된다. 2014년에 연이어 확인된 주요 오픈소스 프로그램의 취약점들은 예상되는 피해 범위가 심각해 하트블리드(Heartbleed), 쉘쇼크(ShellShock)로 표현되기도 했다. 오픈소스의 특성상 지속적인 개선이 가능해 상대적으로 안전한 것으로 알려졌던 프로그램에서 새로운 취약점이 잇따라 발생함에 따라 기업과 관련 업계의 대응 방안이 요구된다.

한편 지능형 지속 위협 APT(Advanced Persistent Threat)와 같은 타깃 공격이 꾸준히 증가할 것으로 보인다. 공격 대상 또한 다양한 산업군 및 국가기관으로 확대되고 기업기밀, 금융정보, 군사안보 정보 등을 목표로 하는 타깃 공격이 심화될 전망이다. 유출된 정보를 범죄에 악용하는 사례 또한 더욱 증가할 것으로 예측된다. 아울러 최근 정치, 사회적으로 국가 간 이해관계가 첨예하게 대립됨에 따라 사이버 전을 통한 정보 유출 시도는 더욱 격화될 전망이다.

5. IoT 보안 위협의 증가

사물인터넷 IoT(Internet of Things) 기술의 개발 및 발전으로 IoT 시장이 지속적으로 성장하면서 이와 관련된 보안 위협이 등장할 것으로 예상된다.

지금까지 사물인터넷에 대한 주요 이슈는 관련 기술 개발과 IoT 플랫폼 표준화 작업이었으나 향후 사물인터넷 기술의 표준화와 함께 관련 시장이 급격히 확대될 것으로 보인다. 우리 주변의 모든 사물이 인터넷을 통해 정보를 주고받고 연결되어 있다는 것은 이 모든 사물이 사이버 범죄자들의 공격 대상이 될 수 있다는 것을 의미한다. IoT 기기는 종류와 성능 또한 다양해 기존의 보안 기능을 적용하기 어렵다. 또한 대부분 무선 네트워크를 통한 통신이 이루어지기 때문에 무선 공유기 등 무선 네트워크 보안 위협이 증가할 것으로 보인다.

AhnLab

ASEC REPORT 2014 Annual Report

집필	안랩 시큐리티대응센터 (ASEC)	발행처	주식회사 안랩
편집	안랩 콘텐츠기획팀		경기도 성남시 분당구 판교역로 220
디자인	안랩 UX디자인팀		T. 031-722-8000
			F. 031-722-8901