2013년 금융IT 정보보호동향 예측 분석

신휴근*

* 금융결제원 금융정보보호부 과장(E-mail: hkshin@kftc.or.kr)

〈요 약〉

금융결제원은 한 해를 정리하고 다음 해를 준비하는 차원에서 발표되는 정보보호업계의 동향 예측 보고서를 수집 · 분석하여 TOP 10 이슈를 도출하고 금융IT 분야의 이슈를 예측해왔다. 2012년 정보보호 이슈를 보면 2011년에 비해 표면으로 드러난 대형 침해사고 건수는 줄었지만 지적재산 등 특정 내부 정보 유출을 목표로 하는 표적 공격 과정은 보다 치밀하고 정교해졌다. 또한 스마트폰의 이용 확대에 따라 스마트폰 악성 프로그램이 폭발적으로 늘어나는 등 모바일 전자금융서비스에 대한 보안 위협이 증가하고 있다. 아울러 고도화된 보안 위협을 효과적으로 탐지하고 대응하기 위한 보안 관제 변화 움직임이 포착된 한해였다.

본 보고서에서는 국내 · 외 정보보호 업체, 언론 및 관련 기관에서 발표한 총 29개의 '2013년 정보보호동향 예측 자료'에 포함된 190건의 이슈를 분석하여 '스마트폰 등 모바일 관련 위협', '목표 대상이 명확한 조직적 공격', '악성 프로그램 위협', '보안 관제의 변화', '클라우드 컴퓨팅 보안'을 포함한 TOP 10 이슈를 선정하였다. 그 중에서도 특히 안드로이드OS 악성 프로그램의 급증, 드라이브 바이 다운로드 및 SMS를 이용한 악성 프로그램 유포, 고도화된 스마트폰 봇넷의 증가, 개인기기에 대한 보안 위협 증가와 관련된 '스마트폰 등 모바일 관련 위협' 항목, 국가 주도의 사이버 공격과 관련된 '목표 대상이 명확한 조직적 공격' 항목, 가상화 기술 탐지, 디지털저작권 관리기술 적용, 도메인 생성 알고리즘 이용, 정보를 인질로 삼는 랜섬웨어와 관련된 '악성 프로그램 위협' 항목이 2013년에 주를 이룰 것으로 예상된다. 또한 각 기관은 현실화 · 고도화되어가고 있는 보안 위협과 최신IT 트렌드를 이용한 서비스 활성화로 인해 파생되는 보안 위협을 완화하기 위하여 보안 관제 서비스가 변화할 것으로 예상하고 있다.

금융IT 관련 주요 이슈로서 금융IT 정책 방향은 금융IT 인력 · 예산 확보, 취약점 분석 및 평가 내실화, 정보기술 부문 내부통제강화, 정보기술 부문 실태 평가, 전자금융거래 인증체계 개선 등을 중점 이슈로 다루고 있다. 또한 금융IT 감독 방향은 IT보안강화 종합대책 지속 추진, 스마트 금융 감독강화, 공인인증서 발급 및 사용절차 강화, IT보안시스템 등 고객정보보호관리 체계 테마검사 실시, 인증방법의 다양화 추진 등을 지향한다. 이와 더불어 모바일 전자금융서비스 관련 보안 위협이 증가하고 있는 가운데, 특히 모바일 전자지갑에 대한 보안 위협에 대응할 필요가 있다.

본 보고서를 통해 발생 가능한 위협들의 보안 리스크를 분석하여 선제적인 대응방안을 마련함으로써, 금융회사의 보안성과 안전성 향상에 기여할 수 있을 것으로 기대한다.

Ⅰ. 개 요

정보보호업계에서는 한 해를 정리하고 다음 해를 준비하는 차원에서 매년 동향 예측 보고서를 발표한다. 이와 관련하여 금융결제원은 정보보호업계의 동향 예측자료들을 수집 · 분석하여 TOP 10 이슈를 도출하고 금융IT 분야의 이슈를 예측하여 왔다.

2012년은 2011년에 비해 표면으로 드러난 대형 침해사고 건수는 줄었지만 고객 정보뿐만 아니라 기관이 보유하고 있는 지적재산 등 내부 정보 유출을 목표로 하는 표적 공격 과정은 보다 치밀하고 정교해졌다. 또한 스마트폰의 보급과 이용이 늘어나면서 스마트폰 악성 프로그램이 폭발적으로 증가하는 등 공격자들이 PC에서 모바일 기기로 공격 대상을 확대하기 시작했으며, 금전적 이득을 취하기 위해 모바일 전자금융서비스 등에 관심을 갖기 시작했다. 아울러 기존의 퍼리미터(perimeter) 보안 관제 체계로는 고도화된 공격 기법에 대응하는데 한계가 있어 보안 관제 체계의 개선 필요성이 제기된 한해였다.

본 보고서의 구성은 다음과 같다. 우선 제 II장에서는 '2012년 금융IT 정보보호동향 예측 분석'에서 선정한 '2012 정보보호동향 TOP 10'과 실제 현실화된 대표사례를 비교 · 분석하여 지난 2012년의 주요 이슈들을 정리하였다. 제 III장에서는 국내외 정보보호업체, 관련 기관 및 언론 등 총 29개 기관에서 발표한 '2013 정보보호동향 예측 자료'를 분석하고, 2013년의 주요 쟁점이 될 것으로 예상되는 '2013 정보보호동향 예측 TOP 10' 및 '금융IT 관련 주요 이슈'를 선정하였다. 마지막으로 제 IV장에서는 3년간의 '정보보호동향 예측 TOP 10'을 비교 · 분석하고 결론을 맺었다.

본 보고서를 통해 발생 가능한 위협들의 보안 리스크를 분석하여 선제적인 대응방안을 마련함으로써, 금융회사의 보안성과 안전성 향상에 기여할 수 있을 것으로 기대한다.

Ⅱ. 2012년 주요 이슈

1. 이슈 분석 개요

2012년은 악의적인 목적 달성을 위한 악성 프로그램 공격이 주를 이루었던 한 해였다. 특히, 금융권에서는 피싱 · 파밍을 비롯한 전자금융사기가 급격히 증가하였으며, 스마트폰 보급이 크게 증가하는 추세와 더불어 스마트폰을 대상으로한 악성 프로그램도 급증하였다. 심지어 최근에는 직접적으로 금전적인 이득을 취하기 위해 승인문자를 갈취하여 소액결제 사기범죄에 이용하는 악성 파일도 발견되는 등 스마트폰을 이용한 보안 위협이 크

게 증가할 것으로 예상된다.

이에 '2012년 금융IT 정보보호동향 예측 분석' 보고서에서 선정한 '2012 정보보호동향 TOP 10'을 기준으로 올해 발생한 침해사고 및 보안이슈를 정리하였다.

〈표1〉 2012 정보보호동향 TOP 10 및 대표 사례

순위	2012 정보보호동향 TOP 10	대표 사례
1	목표대상이 명확한 조직적 공격	– 일본 재무성 등에 대한 악성 프로그램 공격 – 국내 특정 기업 및 기관에 대한 표적 공격
2	스마트폰 등 모바일 관련 위협	– 안드로이드 기반 악성 프로그램 급증 – 톨프로드(Toll Fraud) 성격의 금전적 이득을 취하기 위한 악성 프로그램 증가
3	악성 프로그램 위협	– 응용 프로그램의 제로데이 취약점 악용 – 맥OS용 악성 프로그램(Flashback, Sabpab 등) 등장 – 지능형지속위협 공격에 활용되는 플레이머(Flamer) 악성 프로그램
4	데이터 유출	– 산업비밀, 금융, 개인정보 유출 – 특정 데이터 유출을 노리는 표적 공격
5	소셜 네트워크 서비스 위협	– SNS를 이용한 악성 프로그램 유포 – SNS의 기능을 활용한 조직적인 유포
6	소셜 엔지니어링 위협	– 피싱 · 파밍 공격의 급증
7	클라우드 컴퓨팅 보안	– 클라우드 서비스를 이용한 해킹 – 클라우드 서비스 해킹에 의한 개인정보 유출 및 삭제
8	사이버범죄 조직화	– 사이버범죄 시장의 거래 금액 증가
9	보안 관제의 변화	– 지능형 상황관제 체계 구축 필요
10	HTML5 보안	– HTML5 적용 서비스 증가에 따른 HTML 보안 위협 증가 예상

2. 이슈 분석 결과

가. 목표대상이 명확한 조직적 공격

2012년 한 해 동안 Advanced Persistent Threat(APT)라고 일컬어지는 '목표대상이 명확한 조직적 공격' 사례는 일본 재무성 APT 공격, 국내 특정 기업 및 기관에 대한 표적 공격, 미국 록히드마틴社 대상 사이버 공격 등을 꼽을 수 있다.

2012년 7월 21일 일본 언론을 통해 일본 재무성에 있는 2,000여대의 PC 중 123대가 정보 탈취 목적의 트로이목마에 감염되었고 약 2년간(2010년~2011년) 기밀 정보가 유출

되었을 것으로 추정된다는 기사가 발표되었다. 악성 프로그램 감염 경로의 불명확성, 안티바이러스 미탐지, 오랜 기간동안 발견되지 않은 점으로 미루어보아 표적 공격으로 추정하고 있다. 이 표적 공격에 사용된 악성 프로그램은 키로깅, 파일 생성 · 삭제, 운영체제 정보 전송 등의 기능을 통해 감염된 시스템을 거점으로 내부 네트워크의 다양한 정보들을 수집하기 위해 제작된 것으로 추정되고 있다.

이런 유형의 공격은 해외만의 이야기는 아니다. 국내의 특정 기업 및 기관에 대한 다양하고 국지적인 공격 시도 정황이 수차례 포착되었고, 보안취약점이 제거되지 않은 제로데이 공격도 꾸준히 발견되고 있다.[1)]

〈그림1〉 국내 대기업 대상 악성 메일

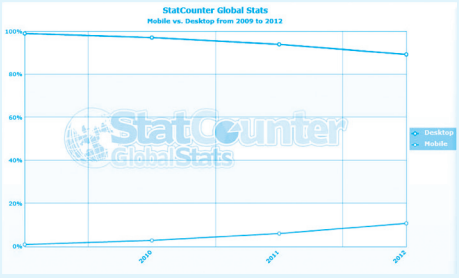
이와 같은 표적 공격을 통해 기업에서 관리하는 고객 정보를 빼내거나 시스템을 파괴하려는 목적의 공격이 많았던 2011년의 동향과는 달리, 2012년에는 고객 정보 뿐만 아니라 지적재산 등 공격자가 원하는 특정 내부 정보로 공격 목표를 한정한 사례도 많았다. 특히 시스템 관리자보다는 주요 내부 정보를 관리하는 직원을 표적으로 한 공격이 많았고, 악성 프로그램 유포 방법은 취약한 문서 파일을 첨부한 이메일, 정상 프로그램의 업데이트 취약점을 악용한 경우가 많았다. APT 공격이 공격 대상 기관의 주요 지적재산 등 내부 정보를 겨냥한다는 사실은 산업스파이 활동에서 사이버 범죄자들이 정보 중개인으로 활동할 수 있다는 점을 시사하고 있다.[2)]

1) 키워드로 돌아보는 2012년 10대 보안위협 선정, 잉카인터넷, 2012.12. 3.(http://erteam.nprotect.com/364).
2) 2012년 상반기 5대 보안 위협 트렌드, AhnLab 뉴스, 안철수연구소, 2012. 7.20, (http://blog.ahnlab.com/ahnlab/1554)

나. 스마트폰 등 모바일 관련 위협

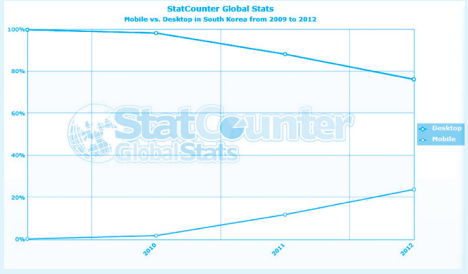
2012년은 스마트폰의 보급이 전 세계적으로 크게 증가하면서 '스마트폰 등 모바일 관련 위협'이 주목받았다. 특히 2012년 인터넷 이용 관련 모바일 기기 국내 점유율은 23.84%로, 전세계의 증가 추이보다 빠르게 상승하고 있다.

〈그림2〉 데스크톱 vs 모바일(전세계)



자료: StatCounter (http://gs.statcounter.com/)

〈그림3〉 데스크톱 vs 모바일(국내)



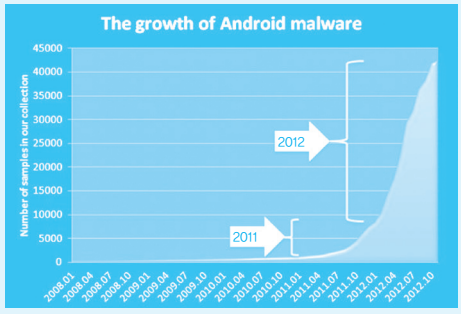
그 중에서도 특히 앱의 설치와 배포가 용이한 안드로이드 기반의 스마트폰 이용자가 기하급수적으로 증가함에 따라 안드로이드 이용자를 겨냥한 보안위협도 비례적으로 증가 추이를 보이고 있다.

〈그림4〉 스마트폰 OS별 점유율

Operating System	3Q12 Units	3Q12 Market Share (%)	3Q11 Units	3Q11 Market Share (%)
Android	122,480.0	72.4	60,490.4	52.5
iOS	23,550.3	13.9	17,295.3	15.0
Research In Motion	8,946.8	5.3	12,701.1	11.0
Bada	5,054.7	3.0	2,478.5	2.2
Symbian	4,404.9	2.6	19,500.1	16.9
Microsoft	4,058.2	2.4	1,701.9	1.5
Others	683.7	0.4	1,018.1	0.9
Total	169,178.6	100.0	115,185.4	100.0

자료: Smartphone market share 2012, Gartner.

〈그림5〉 안드로이드 악성 프로그램 증가 추이

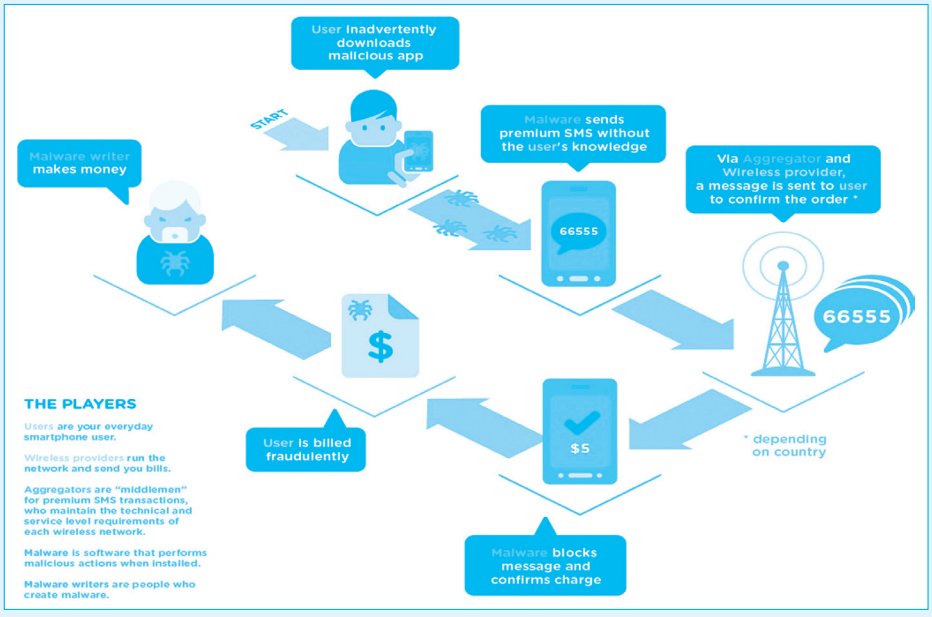


자료: Kaspersky Security Bulletin 2012 Malware Evolution.

2012년은 안드로이드 외산 악성 프로그램이 폭발적으로 증가한 해이며, 카스퍼스키(Kaspersky) 발표에 따르면 전체 모바일 악성 코드 중 99%는 안드로이드용으로 2011년보다 약 6배 증가한 것이다. 또한 2012년에 발견된 안드로이드 악성 프로그램의 72%는

금전적 이득을 취하기 위해 제작된 톨프로드 성격의 악성 프로그램이었다. 톨프로드 악성 프로그램은 PC 기반 악성 프로그램이 스팸메일 발송, 디도스 공격 등에 악용되었던 것과는 달리 모바일 기기에 특화된 결제시스템(프리미엄 SMS 등)을 이용하여 금전적 이득을 취하고 있다. 다만 안드로이드 기반 외산 악성 프로그램이 악용하는 프리미엄 SMS 기능은 국내 환경과 차이가 있기 때문에 국내에서 직접적인 피해가 발생할 가능성은 낮은 편이다.

〈그림6〉 톨프로드 악성 프로그램 동작 방식



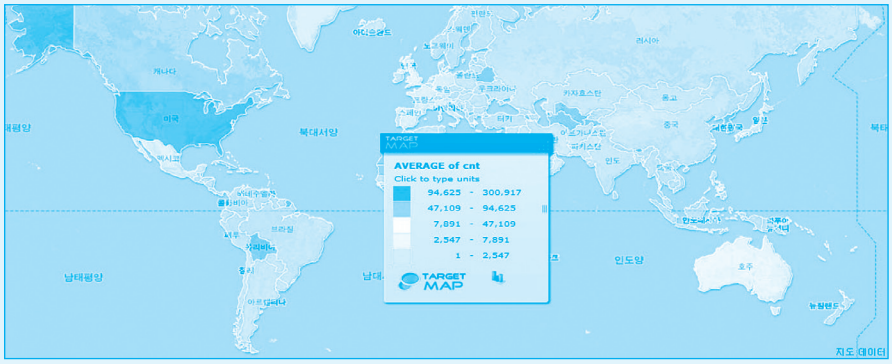
자료 : State of Mobile Security 2012, Lookout, 2012.

다. 악성 프로그램 위협

'악성 프로그램 위협' 측면에서는 2011년과 유사하게 금전적 이득을 취하거나 정보를 수집 · 유출하는 목적을 가진 악성 프로그램과 일반적으로 널리 사용되고 있는 응용 프로그램의 취약점을 이용하는 악성 프로그램이 주를 이루었다. 또한 운영체제 측면에서는 2012년 4월 맥OS용 Flashback 악성 프로그램이 등장하여 JAVA 보안 취약점을 통해 전 세계 70만대 이상의 컴퓨터를 감염시켰으며 이후 Sabpab 트로이목마가 맥OS용 MS워드를 통해 전파되었다. 이 사건으로 인해 맥OS도 이제는 더 이상 안전지대가 아니라는 인

식이 확산되기 시작했다.

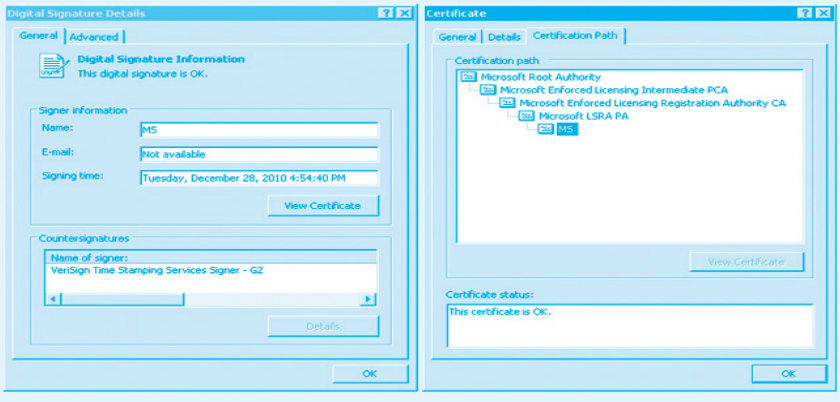
〈그림7〉 Flashback 악성 프로그램 감염 통계



자료: Mac OS X Flashback Malware, Target Map (http://http://www.targetmap.com)

6월경, 이란과 중동지역에서 APT 공격에 활용되는 플레이머 악성 프로그램이 확산되어 주의가 요구되었다. 플레이머는 국가 기간시설에 침투해 중요 정보를 빼돌리는 매우 정교한 표적공격용 악성 프로그램으로 2010년 '스턱스넷(Stuxnet)', 2011년 이와 유사한 '듀큐(Duqu)', 전세계 화학 · 방산업체를 공격한 '니트로(Nitro)' 등에 이어 전세계를 긴장케 했다. 플레이머는 감염PC를 윈도우즈 업데이트 서버로 만든 후 감염되지 않은 주변 PC에 대한 중간자 공격(Man-in-the-middle)을 통해 플레이머 악성 프로그램을 전파하였다.

〈그림8〉 플레이머 악성 모듈(WUSETUPV.EXE)을 서명하는데 사용된 인증서 경로



자료: Microsoft Update and The Nightmare Scenario, F-Secure

국내에서는 정치적 이슈 등을 통해 사용자의 호기심을 유발하는 악성 프로그램 유포가 여전히 빈번히 발견되고 있다.

〈표2〉 유포 악성 프로그램 주요 내역

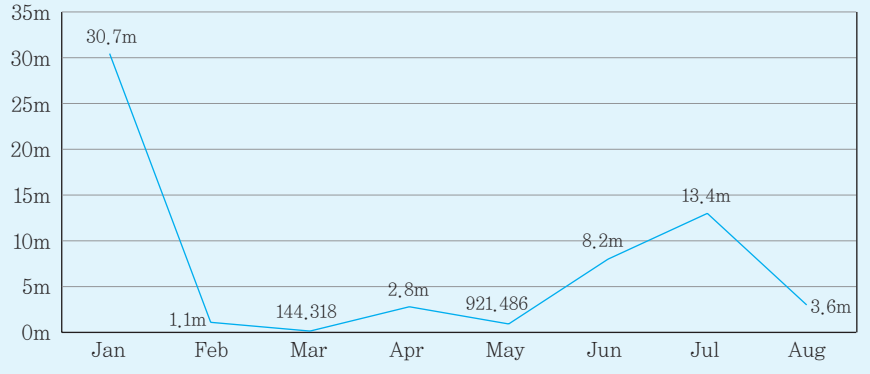
시기	악성 프로그램 파일명	비고
2012.04	Sorean intelligence officials say North Korea may be preparing for nuclear test.doc	북한 핵실험
	Early Check-In 2012 London Olympics.doc	런던올림픽
	Seoul_Communique.pdf	핵안보정상회의
2012.05	국가안보전략 개요.hlp	국가안보전략
2012.06	삼위일체의 북핵전략.hwp, 북핵해결 3대 전략.hwp	북한 핵 관련 전략
2012.11	국방융합기술.hwp	국방 관련 문서파일

자료: 잉카인터넷 대응팀 블로그(http://erteam.nprotect.com/)

라. 데이터 유출

2012년 역시 2011년과 마찬가지로 '데이터 유출' 사고가 자주 발생했던 해이다. 다만, 2011년에 비해 데이터 유출 건수는 감소했지만 특정 데이터를 노리는 표적 공격은 증가했다. 1월부터 8월까지 전세계에서 발생한 데이터 침해사고는 월 평균 14건으로 2011년 5월부터 12월까지의 월 평균 16.5건보다 감소했고 지난해 조사 기간 평균 1,311,629건에 달했던 데이터 침해사고당 개인정보 유출 건수도 2012년 640,169건으로 절반 이상 감소한 것으로 집계됐다. 하지만 유출된 개인정보의 중앙값은 사고당 6,800건으로 지난해 4,000건보다 41%나 늘었다.[3)]

〈그림9〉 2012년 월별 개인정보 유출 건수

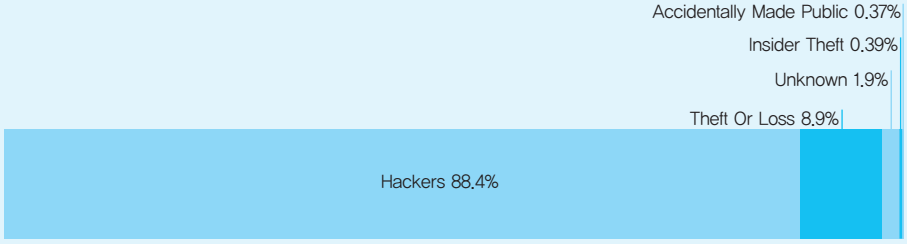


자료: Symantec(2012. 8.).

3) Symantec Intelligence Report, Symantec, 2012. 8.

또한 데이터 유출 사고의 원인은 88.4%가 해킹인데, 이는 2011년 5월부터 12월까지보다 14% 증가한 수치이다.

〈그림10〉 데이터 유출 사고 원인



자료: Symantec(2012. 8.).

〈표3〉 2012년에 발생한 대규모 데이터 유출 사고

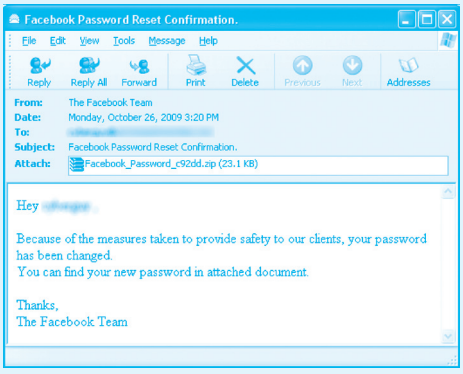
피해기업	시기	유출내용
뉴욕주 전력공사 (New York State Electric & Gas Co.)	2012.01	– 특정 도급업체의 인가되지 않은 접근 – 고객의 사회보장번호, 생일, 은행 계좌번호가 담긴 180만개의 파일
잡포스 (Zappos)	2012.01	– 해킹에 의해 암호화된 신용카드 및 지불관련 정보 유출 – 고객의 이름, 이메일, 주소, 휴대폰 번호, 신용카드번호 등 고객정보(2,400만건) 유출
캘리포니아주 아동복지국 (California Dept. of Child Support Services)	2012.03	– 저장 장치 이송 중 분실 – 80만개의 성인 및 어린이 정보가 담긴 4개의 컴퓨터 저장 장치 분실
글로벌 페이먼트 (Global Payments, Inc.)	2012.04	– 취약한 인증 메커니즘을 악용한 시스템 관리자 계정의 확보 – 150만개의 신용카드 번호, 가맹점에서 수집한 개인정보를 보관하고 있는 서버에 무단 접근
유타주 기술서비스국 (Utah Dept. of Technology Services)	2012.04	– 유타주 기술서비스국 서비스 서버의 취약한 패스워드 – 국민의료보조 청구를 한 환자들의 파일 78만개 유출
이란은행	2012.04	– 정치적 핵티비즘 성격의 해킹 – 은행 계좌번호, PIN 번호 등 고객정보(300만건) 유출
한국교육방송공사 (EBS)	2012.05	– 중국發 웹쉘 업로드 공격 – 이름, 아이디, 전화번호, 이메일, 주소, 비밀번호 등 고객정보(400만건) 유출
링크드인 (LinkedIn)	2012.06	– 러시아 해커들에 의해 해킹당한 후 러시아 온라인 포럼에 게시되어 알려짐 – 솔트를 적용하지 않은 SHA-1 해시 패스워드(650만건) 유출
야후 보이스 (Yahoo! Voice)	2012.07	– D33DS 해커그룹에 의한 SQL Injection 공격 – 암호화되지 않은 텍스트로 저장된 고객 계정정보(40만건) 유출

케이티 (KT)	2012.07	– 텔레마케팅 사업에 이용할 목적으로 해킹 프로그램을 제작하여 KT 휴대전화 고객정보를 유출 · 판매 – 이름, 주소, 휴대전화번호, 휴대폰모델명, 기기변경일 등 고객정보(800만건) 유출
국제전자전기공학회 (IEEE)	2012.09	– 일반 사용자들이 접근 가능한 IEEE FTP 서버에서 회원 정보를 관리하는 허술함을 악용 – IEEE 회원 정보(10만건) 유출
Vmware	2012.11	– 어나니머스 해커그룹에서 소스코드 획득 후 토렌트를 통해 공유 – Vmware ESX 소스코드 유출

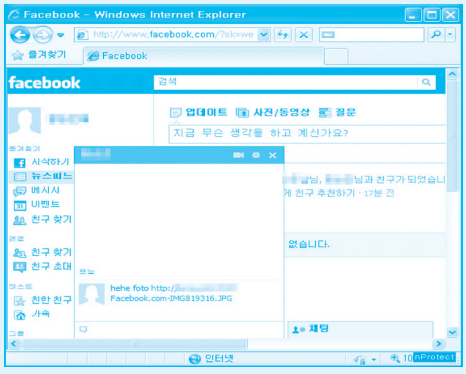
마. 소셜 네트워크 서비스 위협

'소셜 네트워크 서비스 위협' 측면에서는 페이스북, 트위터, 링크드인과 같은 소셜 네트워크 서비스(Social Network Service, SNS)를 이용해 악성 프로그램을 유포하고 스팸메일을 발송하는 등 다양한 보안 위협이 발견되었던 한 해이다. 기존에는 페이스북 측에서 보낸 메일로 위장해 비밀번호 변경 등의 이유로 첨부파일을 클릭하도록 유도하는 방식이었던 반면 지금은 SNS의 사진파일, 공지사항, 친구신청 등을 위장하는 등 사회공학적인 기법이 등장하고, 조직적으로 악성 프로그램이 유포되는 사례가 늘고 있다. 더불어 단축 URL 주소 서비스를 이용해서 악의적인 웹 사이트로 연결을 유도하거나 페이스북 채팅창을 통해서 친구 계정으로 전송된 메시지에 포함되어 있는 악의적 URL 주소를 클릭하게 만드는 방법을 이용하고 있다.

〈그림11〉 페이스북 위장 이메일



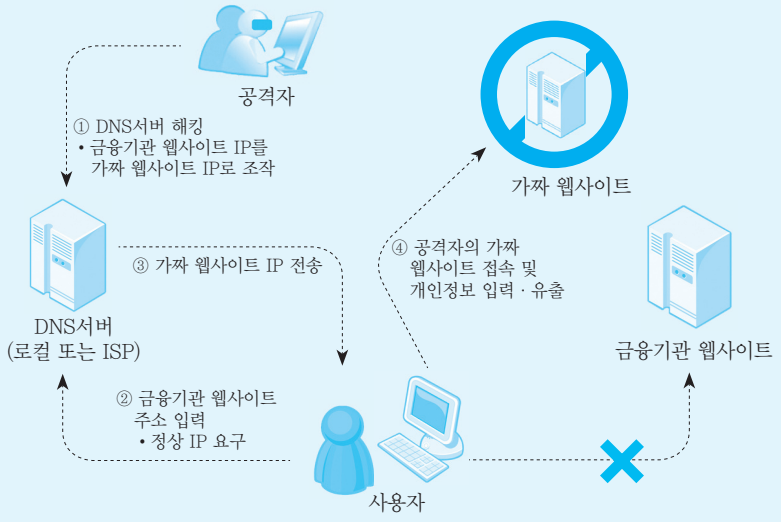
〈그림12〉 페이스북 채팅창 이용 웜 전파



바. 소셜 엔지니어링 위협

'소셜 엔지니어링 위협' 측면에서는 금융당국, 대검찰청, 경찰청, 금융회사 등의 홈페이지를 사칭해 사용자 개인정보, 금융정보, 비밀번호 등의 입력을 유도하는 피싱 공격이 있다. 이전부터 기승을 부리고 있는 보이스피싱에서 더 나아가 SMS 문자와 피싱사이트를 결합하여 피싱 공격이 이루어졌으며, 이후 인터넷 뱅킹 이용자들의 예금탈취를 직접적으로 노린 악성 프로그램(KRBanker)과 결합되는 파밍 공격으로 진화하였다. 파밍 공격은 브라우저 주소창에 정상 홈페이지 주소를 입력하더라도 피싱사이트로 접속이 유도되기 때문에 사용자의 각별한 주의가 필요하다.

〈그림13〉 파밍 공격 흐름도



자료 : 김소이, 전자금융사고 발생유형 및 대응현황, 지급결제와 정보기술 제38호, 금융결제원, 2009.10, 42쪽.

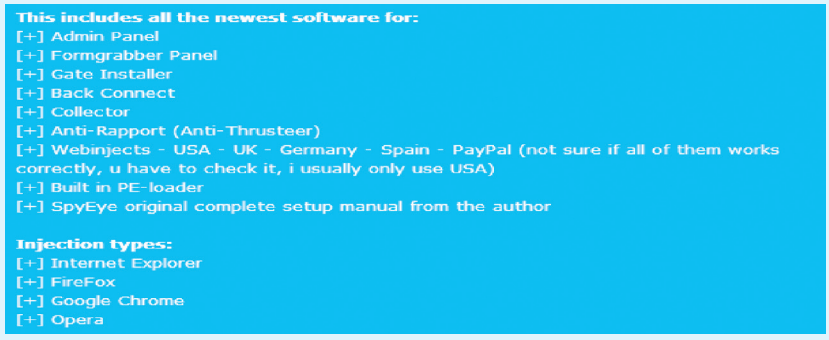
사. 클라우드 컴퓨팅 보안

2011년 룰즈섹(Lulzsec) 해커 그룹은 아마존 클라우드 서비스인 Elastic Compute Cloud(EC2)의 클라우드 컴퓨팅 파워를 이용해 소니픽쳐스 및 소니컴퓨터엔터테인먼트 등을 공격해 약 1억 명의 사용자 정보를 탈취했다.[4] 이와 같이 클라우드 서비스는 고객들

4) Joseph Galante, Olga Kharif & Pavel Alpeyev, Sony Network Breach Shows Amazon Cloud's Appeal for Hackers, Bloomberg, 2011. 5.17. (http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html)

의 정보를 안전하게 보관해주기도 하지만, 해커들이 공격할 수 있는 도구로 변질될 수 있다. 2012년, '클라우드 컴퓨팅 보안' 측면에서는 어떤 사건이 있었을까? 지난 5월에 스파이아이(SpyEye)와 제우스(Zeus)는 유럽, 미국, 콜롬비아 등의 금융회사를 대상으로 일회용 토큰 등 투팩터(two factor) 보안인증을 우회하는데 클라우드 컴퓨팅을 활용했다. 공격자는 사용자의 온라인 뱅킹 세션을 이용하여 실시간으로 불법 이체를 수행하기 위해 서버 사이트 스크립트와 결합된 Man-in-the-browser(MITB) 기법을 사용했다.[5)]

〈그림14〉 스파이아이 악성 프로그램 기능



또한 지난 8월 개인 클라우드 서비스인 애플의 아이클라우드와 드롭박스가 해킹당해 일부 이용자의 정보가 삭제되는 사건이 발생했다. 이 과정에서 해커는 iOS 기기에 보관중인 자료와 여기에 연동된 이메일 및 트위터 내용까지 삭제했다. 클라우드 서비스 보안 사고에 따른 이런 우려 때문에 우리나라 정부와 공공기관에서는 클라우드 서비스 이용을 제한하고 있는 실정이다.

아. 사이버범죄 조직화

사이버범죄 조직은 리더에서 자금운반책에 이르기까지 조직 구성원들 각각의 역할과 책임이 명확히 구분되어 있을 정도로 탄탄한 조직력을 갖춘 전형적인 계층 구조로 구성되어 있다. 사이버범죄의 핵심은 고도화된 악성 프로그램을 배포하여 봇넷을 구성하고 허위 백신 소프트웨어와 효율적인 익스플로잇 툴킷을 개발하는 등의 기술력 보유에 있다. 합법적인 조직처럼 개발된 코드는 엄격한 검증 프로세스를 거쳐 배포되며 대규모 공격,

5) Dave Marcus, Ryan Sherstobitoff, Dissecting Operation High Roller, McAfee and Guardian Analytics, 2012.

CAPTCHA 크랙킹 등 보다 고도화된 작업의 경우에는 해킹 그룹 등 다른 조직에 개발 연구를 의뢰하거나 기술을 보유한 외부 인력을 채용하여 범죄 조직의 기술력을 향상시키고 있다.

사이버범죄 조직은 인터넷 구인 게시판, 해킹 포럼, 언더그라운드 IRC 채널을 통해 해킹 서비스에서부터 클라이언트의 요구에 맞춘 악성 프로그램 제작에 이르기까지 다양한 서비스를 홍보하고 있다.[6)]

〈그림15〉 봇넷 렌탈 가격 정책

자료: Fortinet(2012.12).

자. 보안 관제의 변화

'보안 관제의 변화' 관련해서는 현재의 보안 관제 체계에서는 정밀하게 진행되는 APT 공격이나 사회공학적 공격을 완벽하게 탐지할 수 없으므로 대용량 데이터에 대한 실시간 분석, 취약점 분석 결과 연동, 위험관리 프로세스 도입, 프로파일링 기술 등 지능형 상황 관제 체계 구축의 필요성이 언급되었다.

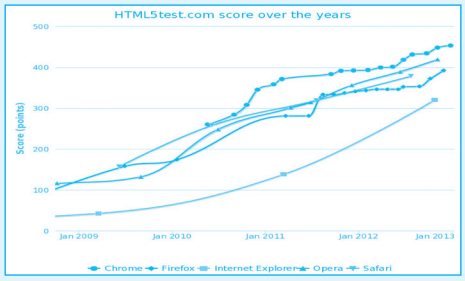
차. HTML5 보안

'HTML5 보안' 관련한 동향으로는 아직까지 보고된 해킹 사례는 없다. 다만 2012년

6) Cybercriminals Today Mirror Legitimate Business Processes, Fortinet 2013 Cybercrime Report, Fortinet, 2012.12.

12월 현재 HTML5을 완벽하게 지원하는 브라우저는 없으나 점차 HTML5를 지원하는 범위가 확대되는 상황이고 구글이 자사의 주요 서비스 중 하나인 유투브(Youtube)에서 HTML5 기반의 서비스를 시작하는 등 HTML5 기반 서비스의 증가가 예상됨에 따라 HTML5에 대한 보안 위협도 비례하여 증가할 것으로 예상된다.

〈그림16〉 HTML5 호환성 점수 추이



자료: HTML5TEST(http://html5test.com)

〈그림17〉 HTML5 호환성 점수(475점 만점)

	Score	Bonus
Maxthon 3.4.5 »	457	15
Chrome 23 »	448	13
Opera 12.10 »	419	9
Firefox 17 »	392	10
Safari 6.0 »	378	8
Internet Explorer 10 »	320	6

Ⅲ. 2013년 동향 예측

1. 예측 분석 개요

본고에서는 웹센스(WebSense), 카스퍼스키, 잉카인터넷 등 국내 · 외 정보보호 업체, 언론 및 관련 기관에서 발표한 총 29개의 '2013년 정보보호동향 예측 자료'를 토대로 전반적인 보안업계의 예측을 분석하였다. 각 기관에서 예측한 총 190건의 이슈에 대해 공통점을 찾아 분류하고, 2013년의 주요 쟁점이 될 것으로 예상되는 '2013 정보보호동향 예측 분석 TOP 10'을 선정하였다.

외부 기관의 2013년 정보보호동향 예측은 크게 플랫폼 보안, 공격 트렌드, 악성 프로그램, 대응 트렌드, 서비스 보안, 정책 이슈의 6가지 부문으로 분류하였다. 이 중 '플랫폼 보안'에 대한 예측이 31%로 가장 많았고, '공격 트렌드' 28%, '악성 프로그램' 16%, '대응 트렌드' 14%로 그 뒤를 이었다.

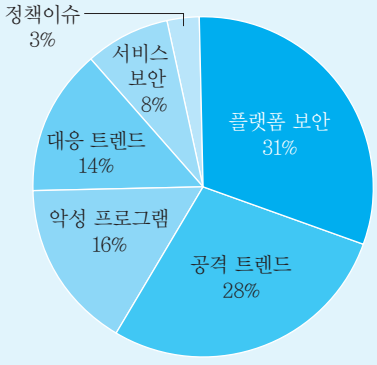
'플랫폼 보안' 부문에서는 모바일 관련 위협, 클라우드 컴퓨팅 보안, 개인기기(Bring Your Own Device, BYOD) 및 빅데이터 보안 위협, 윈도우 및 맥OS 관련 보안 이슈 등의 주제들이 선정되었다. '공격 트렌드' 부문에서는 APT와 같은 목표대상이 명확한 조직

적 공격, 국가(정부)차원의 사이버 활동 강화, 사회 전반으로의 공격 확대, 핵티비즘 등의 공격행위, 클라우드 서비스를 통한 데이터 유출 등에 대한 전망이 있었다. 또한 '악성 프로그램' 부문에서는 악성 프로그램의 고도화, 응용 프로그램 취약점 공격 지속, 랜섬웨어(Ransomware) 증가 등이 예측되었다. '대응 트렌드' 부문에서는 보안 관제의 변화에 관한 언급이 가장 많았으며, 보안 관제 대상의 확대, 정보보호 체계 개선을 다루었다. '서비스 보안' 부문에서는 소셜 네트워크 서비스 위협과 전자금융보안을 다루었고, '정책 이슈' 부문에서는 국제 공조 체계의 강화, 인터넷 실명제를 비롯한 인터넷 통제 움직임 등이 주로 언급되었다.

〈표4〉 2013 정보보호동향 예측 분류

예측 분류	세부 내용	건수
플랫폼 보안	모바일 관련 위협, 클라우드 컴퓨팅, BYOD 및 빅데이터, 윈도우, 맥OS 등	58
공격 트렌드	조직적 사이버 범죄, 국가 차원의 사이버 활동, 사회 전반에 대한 공격, 핵티비즘, 데이터 유출 등	53
악성 프로그램	고도화된 악성 프로그램 위협 증가, 응용 프로그램 취약점 이용 지속, 랜섬웨어 등	31
대응 트렌드	보안 관제의 변화, 보안 관제 대상의 확대 등	26
서비스 보안	소셜 네트워크 서비스 위협, 전자금융보안 등	16
정책 이슈	국제 공조 체계, 인터넷 통제 움직임 등	6
합 계		190

〈그림18〉 정보보호동향 예측 분류 비율



2013년 정보보호동향 예측자료 분석결과를 토대로 선정된 '2013 정보보호동향 예측 TOP 10'은 다음과 같다.

1위는 모바일 시장의 확대에 따른 '스마트폰 등 모바일 관련 위협'에 대한 예측이고, 2위는 91%의 기업들이 우려하고 있는 APT와 관련된 '목표 대상이 명확한 조직적 공격'이다. 3위는 현재의 탐지 · 대응 체계를 우회하는 등 갈수록 고도화되어가고 있는 '악성 프로그램 위협'이고, 4위는 점차 고도화 · 다양화되고 있는 보안 위협에 효과적으로 대응하기 위한 '보안 관제의 변화'이다. 5위는 '클라우드 컴퓨팅 보안'이다. 클라우드 컴퓨팅은 가상화 기술을 기반으로 컴퓨팅 자원을 효율적으로 분배 · 통합할 수 있기 때문에 기업뿐만 아니라 개인 컴퓨팅에도 빠르게 확산되고 있다.

6위는 국가기반시설, 공급망 등 사회의 토대가 되고 있는 서비스에 대한 공격 가능성이 높아질 것이라는 예측이고, 7위는 트위터나 페이스북과 같은 SNS의 서비스 영역 확대에 따른 위협의 증가이다. 8위는 BYOD 등 새로운 업무 및 서비스의 증가에 따른 보안 관제 대상의 확대이고 9위와 10위는 각각 빅데이터에 대한 보안 위협과 데이터 유출이다.

〈표5〉 2013 정보보호동향 예측 TOP 10

순위	세부 내용	건수
1	스마트폰 등 모바일 관련 위협	27
2	목표 대상이 명확한 조직적 공격	26
3	악성 프로그램 위협	18
4	보안 관제의 변화	13
5	클라우드 컴퓨팅 보안	12
6	사회 전반에 대한 공격 대상의 확대	8
7	소셜 네트워크 서비스 위협	6
8	보안 관제 대상의 확대	5
9	빅데이터 보안 위협	4
10	데이터 유출	4

2. 예측 분석 주요 결과

가. 스마트폰 등 모바일 관련 위협

스마트폰, 태블릿PC 등 모바일 기기의 기하급수적인 보급 증가가 설명해주고 있듯이 점점 모바일 시대가 다가오고 있다. 2013년에는 더 많은 사람들이 사생활 및 회사 업무의 목적으로 모바일 기기를 활용할 것이고, 이를 통한 생활의 편리함도 증대할 것으로 예상된다. 하지만 사람들의 생활 패턴에서 모바일 기기에 대한 의존성이 높아지고 모바일 기

기로 중요 정보를 많이 다룰수록 보안 위협도 커져, 2013년에는 다양한 모바일 관련 보안 위협이 증가할 것으로 예상된다.

그 중에서도 특히 높은 시장 점유율, 앱 개발의 편리성, 앱의 설치와 배포 용이성 등의 이유로 안드로이드 OS에 대한 악성 프로그램이 급증할 것으로 예상된다. 모바일 운영체제의 취약점을 이용하여 드라이브 바이 다운로드(Drive-By Download) 공격을 통해 악성 프로그램을 설치하거나 SMS를 통해 웜바이러스 성격의 악성 프로그램을 전파할 수 있다. 또한 2012년 1/4분기에 3만여대의 안드로이드 기기를 감염시킨 루트스마트(RootSmart) 봇넷과 같은 높은 수준의 봇넷이 보다 많이 발견될 것으로 예상된다. 공격자는 이런 고도화된 악성 프로그램을 이용해 모바일 기기 내에 있는 중요 정보 및 모바일 거래 인증 번호(mobile Transaction Authentication Numbers, mTANs) 등을 탈취하여 금전적 이득을 얻고 있는데, 2013년엔 더 나아가 직접적으로 모바일 뱅킹을 공격할 가능성도 제기되고 있다.

또한 2012년도와 마찬가지로 BYOD에 대한 보안 위협이 제기되고 있다. 기업의 IT통제권 상실, 악성 프로그램에 감염된 기기를 이용한 기업 IT자산에의 접근, 분실로 인한 데이터 유출 등 BYOD로 인한 다양한 보안 위협이 존재한다. 이와 관련하여 기업 차원에서는 모바일단말관리솔루션(Mobile Device Management, MDM) 등을 활용한 단말기 관리, 직원의 인식제고를 위한 교육 등 모바일 기기에 대한 추가적인 보안 대책 마련과 적극적인 실천이 필요한 시점이다.

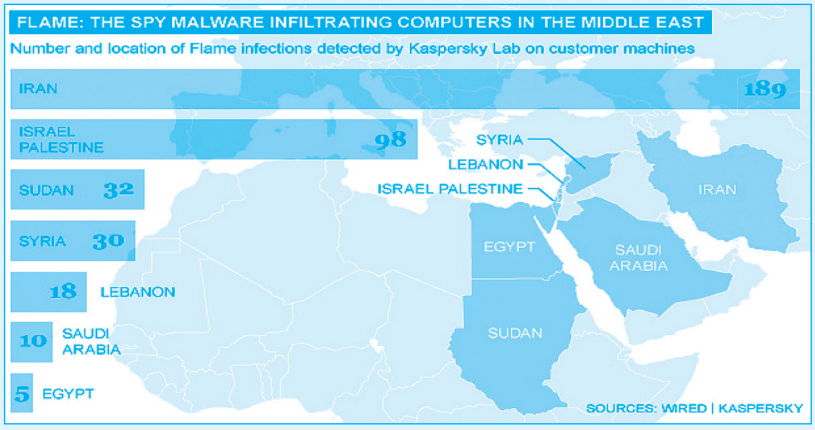
나. 목표 대상이 명확한 조직적 공격

2013년 역시 APT 등 목표 대상이 명확한 조직적 공격이 TOP 10으로 선정되었다. 2012년은 기업과 공공 부문을 표적으로 하는 공격(Gauss, Flamer 등)이 많았다. APT 공격으로 알려진 이런 악성 프로그램은 매우 정교하고 치밀하게 설계되었으며, 네트워크에 침투하여 조용하게 정보를 수집한 후 수집된 정보를 유출시켰다. 또한 플레이머는 스턱스넷(2010년), 듀큐(2011년)와 유사하지만 특정 지역을 대상으로한 공격이라는 점에서 차이점을 보이고 있다. 특정 지역을 대상으로 한다는 점을 볼 때 국가 주도로 이루어지는 '목표 대상이 명확한 조직적 공격'이 발생하고 있음을 알 수 있다.

기존 사이버 공격은 해커와 범죄 조직 혹은 특정한 반정부 세력들의 금전적 목적이나 자기 과시적인 이유 그리고 정보를 수집하려는 목적으로 행해졌으나, 2010년 스턱스넷 이후 국가가 주도하거나 제3의 세력을 지원하여 상대 국가의 정보통신시스템을 공격하여 무력화하거나 파괴하려는 시도가 빈번히 발생하고 있다. 상대 국가의 주요 시설에 대한

폭격이나 미사일 공격 등의 물리적 대응이 가져올 수 있는 위험과 문제점을 일소하고, 공격 주체가 명확히 드러나지 않는 사이버 공격의 특징을 이용하여 향후 국가 주도의 혹은 지원의 조직적 공격이 더욱 빈번히 발생할 것으로 예상된다.

〈그림19〉 플레이머 공격 대상 지역



자료: Flame virus 'has infected 189 systems in Iran', Kaspersky, 2012. 5.

다. 악성 프로그램 위협

2012년의 악성 프로그램 위협은 현 악성 프로그램 탐지 체계에 대한 우회 기술의 발전, 제우스 · 스파이아이와 같은 금융사기 악성 프로그램의 등장으로 요약할 수 있다.

악성 프로그램 탐지는 크게 패턴 방식과 가상화 기술을 이용한 탐지 방식으로 나눌 수 있는데, 최근 많은 기업들이 가상화 기술을 이용한 탐지 방식을 적용하여 운영 중에 있으며 일정 부분 효과를 보고 있다. 공격자는 악성 프로그램 탐지 체계를 우회하기 위해 가상화 기술 환경을 인식하는 기법을 사용하기 시작했다. 예를 들면, 가상화 기술을 이용하여 악성 프로그램이 실행된 경우 악성 프로그램 본연의 기능이 작동되지 않도록 하면서 악성 프로그램 탐지를 우회할 수 있다. 또한 디지털 저작권 관리(Digital Rights Management, DRM) 기술을 사용하거나 도메인 생성 알고리즘(Domain Generation Algorithm)을 통해 Command & Control(C&C) 리스트를 생성하고, 일정 시간 간격으로 접속도메인을 변경함으로써 악성 프로그램 탐지 · 분석을 방해할 수 있다.

또한 러시아에서 처음 발견되어 동유럽, 미국, 캐나다 등으로 확산되기 시작한 랜섬웨어가 기승을 부리고 있다. 랜섬웨어는 악성 프로그램을 PC에 감염시킨 다음 문서 파일

에 암호를 걸어놓고 암호를 풀어주는 조건으로 금품을 요구하는 목적의 악성 프로그램을 의미한다. 랜섬웨어는 구현 난이도가 높지 않고 잠재적인 공격 대상이 풍부하기 때문에 2013년에 보다 증가할 것으로 예상된다.

〈그림20〉 랜섬웨어 동작 화면

마지막으로 지난 한 해 동안 멀티 플랫폼에서 이용 가능한 익스플로잇 툴킷 및 자바 기반 악성 프로그램의 등장, HTML5를 표적으로 하는 많은 개념증명코드(Proof-of-Concept, POC) 공개, 다양한 플랫폼에 대한 편리한 개발 환경 지원 등의 사례들이 발견되었다. 이런 징후들을 통해 2013년에는 보다 많은 크로스 플랫폼을 지원하는 악성 프로그램이 등장할 것으로 예상된다. 또한 PC 악성 프로그램의 난독화 기법, 프래그먼트 공격 등을 지원하는 수많은 라이브러리가 모바일 악성 프로그램의 고도화를 촉진할 것으로 예상된다.

라. 보안 관제의 변화

기업 자산을 침해하기 위한 보안 위협이 고도화·정교화되고 있는 가운데 기존의 퍼리미터 보안 관제 체계로는 이를 신속하고 효과적으로 탐지하는데 한계가 있다. 이에 대한 해법으로 위험 지향(risk-oriented), 상황 인식 지향(situationally-oriented)의 지식 기반 보안 관제 모델이 해법으로 제시되고 있다. 또한 기업 내부 보안 인력의 보안 기술 숙련도가 높지 않은 경우에는 클라우드 지향 보안 서비스(cloud-oriented security service)에 대한 수요가 증가할 것으로 예상된다. 이를 통해 보안 제품 운용에 따른 부하를 경감하거나 보안 전문가의 분석 노하우를 이용할 수 있다.

또한 많은 기업들이 편리성 · 효율성 · 생산성 증대 목적으로 개인기기(BYOD)와 업무

를 접목하고 있지만 기기의 통제가 용이하지 않아 보안 관제를 소홀하고 있다. 하지만 2013년 동안 BYOD로 인한 보안 위협의 증가가 예상되어 BYOD 영역이 기존의 보안 관제 영역에 추가될 것으로 예상된다.

마. 기타

1) 클라우드 컴퓨팅 보안

많은 기업과 개인은 클라우드 컴퓨팅을 통해 비용을 절감하고 사용의 편리성을 향상시킬 수 있다. 그러나 클라우드 컴퓨팅의 활용이 증가하면 증가할수록 사이버 공격자들에게도 매력적인 공격 대상으로 부각될 수 있다. 공격자는 클라우드 서비스를 봇넷 제어, 유출데이터 공개, 해킹도구 등의 악의적인 목적으로 이용할 수 있다. 또한 클라우드 스토리지에 저장되어 있는 기업의 중요한 정보가 외부로 유출되는 사고가 발생할 수 있다.

2) 소셜 네트워크 서비스의 보안 위협

개인 정보 공유, 아이템 선물 등 소셜 네트워크 서비스에 대한 사용자들의 신뢰는 높은 편이며 회원 간에 실제 선물을 구매하고 보내는 등 소셜 네트워크 서비스를 이용한 구매 트렌드가 확대되면 될수록 사이버 공격자들은 소셜 네트워크 서비스를 통해 새로운 기회를 찾을 수 있다. 소셜 네트워크 서비스에서 결제 정보를 빼내거나 가짜 선물 통보, 집주소와 기타 개인 정보를 요구하는 이메일 악성 프로그램 등을 통해 사용자의 중요 정보를 외부로 유출시킬 수도 있다.

3. 금융IT 관련 주요 이슈

가. 금융IT 정책 및 감독 방향

신속하고 편리한 전자금융서비스에 대한 금융고객의 니즈에 맞추어 금융회사들은 다양한 전자금융서비스를 창출하고 있다. 그러나 그 과정에서 개인정보 유출 등 다양한 정보보호 위협들이 출현하여 전자금융서비스의 안전성을 저해할 수 있다. 또한 '전자금융거래 기본약관' 등 표준약관의 개정에 따라 전자금융거래법상 접근매체의 위 · 변조 사고로 인하여 손해가 발생하는 경우에는 원칙적으로 금융회사 또는 전자금융업자가 책임을 부담

하되, 예외적으로 은행이 면책사유를 입증하는 경우에 한하여 그 책임을 경감할 수 있도록 하였다.

상기와 같은 금융 환경의 변화에 맞추어 금융이 갖고 있는 '신뢰'라는 본질을 강화하고, 안전한 전자금융서비스를 위한 보안 대책을 철저히 강구하여 실천할 필요가 있다. 이에 금융위원회와 금융감독원은 금융IT 정책 및 감독 방향을 다음과 같이 발표하였다.[7)]

〈표6〉 **금융IT 중점 정책 방향**

정책 분류	정책 내용
금융 IT인력/예산 확보	– 금융 회사는 IT인력(5%), IT보안인력(5%) 및 IT보안예산(7%) 확보 – 이의 준수 여부를 경영 실태에 평가 – 권고 수준 미충족 시 홈페이지를 통해 사업연도 종료 후 1개월 이내 공시
취약점 분석, 평가 내실화	– 자체 운영반 운영 : 정보 보호 최고 책임자(CISO) 총괄 – 평가 전문기관 의뢰 (정보 공유 분석 센터, 지식 정보 보안 컨설팅) – 취약점 점검 강화 및 불시 점검을 실시하여 금융 회사 이행실태 점검 및 부실한 금융회사에 대한 시정 조치
정보기술 부문 내부 통제 강화	– 정보기술 부문 계획을 수립하고 이행 실적을 관련 임원의 성과 평가에 반영 – 정보기술 부문과 관련된 외부 주문 등의 감리 기준을 포함한 정보 처리 시스템 감리 지침을 작성 · 운영
정보기술 부문 실태 평가	– 금융 기관의 정보기술 부문 운영 실태 평가 – IT경영관리가 양호한 금융기관은 IT평가 결과에 가점 부여
전자 금융 거래 인증체계 개선	– 공인인증서 (재)발급 및 사용 절차 강화를 규정한 전자 금융사기 예방 서비스 전면 시행 – 공인인증서 외의 추가적 인증 방법의 다양화 · 자율화

7) 금융위원회는 디지털타임스가 주최한 2012 U뱅킹 콘퍼런스(2012.11.28)에서(http://blog.naver.com/blogfsc?Redirect=Log&logNo=50157234404 참조)에서, 금융감독원은 디지털데일리가 주최한 금융IT 혁신 컨퍼런스(2012.12.4)에서(http://www.ddaily.co.kr/news/news_view.php?uid=98310 참조) 각각 발표하였다.

〈표7〉 금융IT 감독 방향

감독 방향	주요 내용
IT보안 강화 종합대책 지속 추진	– 정보보호최고책임자(CISO) 임명, 정보보호 예산 및 인력의 적정 수준 유지 유도 – IT보안 인프라 및 내부통제 감독강화 – 금융회사 IT보안사고에 대한 검사 및 제재수준 강화
스마트 금융 감독강화	– 스마트폰 전자금융서비스 안전대책(2010.1월) – 스마트폰 이용자에 대해 금융거래 10계명을 홍보(2011.2월) – 스마트폰 앱 위·변조 보안대책(2012.6월) – 스마트폰 금융 이용 실태 점검
공인인증서 발급 및 사용절차 강화	– '공인인증서 재발급' 또는 '300만원 이상 자금이체용' 단말기 지정 – (은행권) 국내은행은 2012.9.25일부터 시범 시행, (비은행권) 증권, 저축은행 등은 2013년 1/4분기 중 시범 시행 예정
IT보안시스템 등 고객정보보호 관리 체계 테마검사 실시	– 고객정보보호 및 해킹 예방을 위해 IT보안 내부통제 체계, IT보안 시스템 취약점 및 개인정보보호법 준수여부 등을 중점 검사 – 고객동의 없이 정보를 조회하여 영업 등에 사용여부 – 향후 금융회사 제도개선 등에 반영하고, 중대한 위법·부당 행위에 대해서는 엄정 제재
인증방법의 다양화 추진	– 공인인증서 이외에 다양한 인증방법 도입을 위한 평가위원회 활동을 강화
사이버테러에 대한 대응역량 강화	– 사이버테러 공격 탐지·차단시스템 기능 강화 및 정보보호관리체계(ISMS) 인증 취득 유도 – 정보시스템 및 정보통신망에 대해 연 1회 취약점을 분석·평가하고 CEO 보고 의무화 및 CISO의 역할 강화 유도 – 업무지속성 확보대책(BCP)을 수시점검 개선하고 연 1회 비상대응훈련 실시 – 금융ISAC 가입 확대 등을 통해 위험탐지/정보분석 → 사고 대응 → 정보공유 체계 강화
금융회사 IT부문 보호업무 모범규준 보완 시행	– 모범규준상 인정되는 재하청 인력의 범위를 명확히 규정 – 홈페이지가 없는 외국계 국내지점 등과 같은 금융회사는 IT인력 및 예산 권고수준 미충족 시 협회를 통한 공시 요청 – 금융회사의 금융ISAC 연계시기 조정 및 금융ISAC 참여유도
장애인 차별금지 등 대비	– 금융회사에 대해서 장차법 시행에 대비하도록 지도하고 이행 상황을 지속적으로 모니터링

나. 모바일 전자금융서비스 관련 보안 위협

방송통신위원회와 한국인터넷진흥원이 수행한 제5차 스마트폰 이용 실태조사(2012년 상반기) 결과에 따르면, 스마트폰을 통한 모바일쇼핑 경험자는 4차 조사 대비(47.0%) 12.9%p 증가한 59.9%이며, 스마트폰뱅킹 경험자도 10.7%p 증가한 58.6%로 스마트폰을 이용한 경제활동이 더욱 활발해진 것으로 조사되었다. 하지만 스마트폰을 이용한 경제활

동과 비례하여 스마트폰에 대한 보안 위협도 증가하고 있다.

스마트폰에 대한 금전적인 보안 위협 사례는 러시아에서 성행하고 있는 프리미엄 소액결제서비스 악성 프로그램과 이를 응용하여 2012년 12월에 국내에서 발생한 체스트 악성 프로그램이 있다. 국내 사례의 경우 정상 앱(스팸 블록커, 스팸가드 등)으로 위장한 악성 앱을 설치하게 되면 전화번호, 통신사정보, 특정사이트(인터넷 쇼핑몰, 소액결제 전문업체 등)에서 수신된 메시지가 특정 서버로 전송되고 공격자는 이 정보를 이용하여 소액결제를 수행함으로써 금전적 이득을 취했다. 두 사례 모두 단문문자메시지(SMS)를 가로채는 비교적 단순한 방법으로 이루어졌지만 위변조된 앱을 이용하여 모바일 뱅킹 서비스를 악용하는 방법으로 발전할 수 있기 때문에 주의가 요구된다.

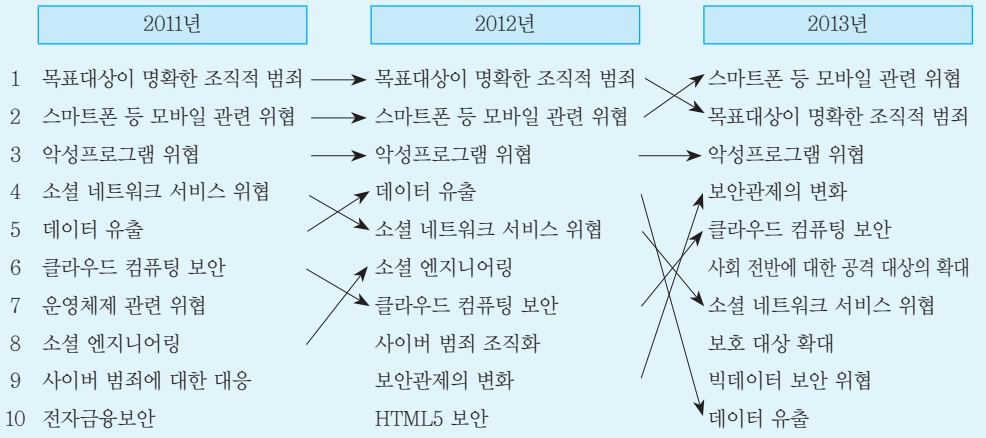
또한 모바일 뱅킹에 대한 위협뿐만 아니라 모바일 전자지갑에 대한 보안 위협도 예측되고 있다. 국내 전자지갑 시장의 경우 은행과 금융결제원 공동으로 전자지갑서비스를 제공하고 있고, 다수의 이동통신사가 카드사와 제휴하여 사업을 추진하고 있다. 또한 구글 등 일부 기업의 경우 결제에 필요한 모든 정보를 서버에 저장하는 등 클라우드 서비스 기반으로 전환할 예정이다. 편리성, 이동성의 강점으로 일반 PC보다 지급결제 비중이 높아 모바일 기기를 겨냥한 공격의 가치가 갈수록 높아지고 있기 때문에 충분한 보안 대책을 마련하여 추진할 필요가 있다. 아울러 향후 모바일 기기 기반의 금융 서비스를 기획할 때에도 보안 대책에 대한 충분한 고민이 필요하다.

Ⅳ. 결론

본 보고서에서는 지난해 선정된 '2012 정보보호동향 TOP 10'을 기준으로 한 해 동안 발생한 주요 이슈들을 비교 · 정리하고, 국내 · 외 정보보호 업체, 관련기관 및 언론 등에서 발표한 총 190건의 이슈를 분석하여 '2013 정보보호동향 예측 TOP 10'을 선정하였다.

최근 3년 동안 선정한 정보보호동향 예측 TOP 10의 추이를 살펴보면 모바일 관련 위협이 본격화되기 시작한 2012년의 동향을 반영하여 2013년에는 '스마트폰 등 모바일 관련 위협'이 1위로 선정되었다. '목표대상이 명확한 조직적 범죄', '악성 프로그램 위협'은 최근 3년 동안 여전히 높은 순위를 유지하고 있다. 또한 기존 보안 관제 체계를 이용한 대응의 한계, 클라우드 서비스 활성화 예상 등의 요인으로 '보안 관제의 변화', '클라우드 컴퓨팅 보안'이 급상승하였다.

〈그림21〉 정보보호동향 예측 TOP 10 추이



정보보호업계에서 예측하는 2013년은 현실화 · 고도화되어가고 있는 위협(모바일, APT, 악성 프로그램 등)과 최신IT 트렌드(클라우드, 소셜 네트워크, 빅데이터 등)를 이용한 서비스의 활성화로 인해 파생되는 보안 위협에 대한 위험을 완화하기 위하여 보안 관제 서비스의 변화가 이루어질 것으로 예상하고 있다.

최근 확산되고 있는 스마트폰, 태블릿PC, 인터넷TV(IPTV) 등을 통한 금융서비스에는 보안 위협도 같이 따라오고 있고, 앞서 언급한 보안 위협으로 인한 금융사고 발생시 금융회사의 책임을 강화하는 방향으로 관련 제도가 변화하고 있으므로 금융회사 경영진은 수반되는 IT리스크 관리를 위해 지속적으로 노력해야 할 것이다.

〈참 고 문 헌〉

1. 2012년 주요 이슈 관련

- 잉카인터넷, 키워드로 돌아보는 2012년 10대 보안위협 선정, http://erteam.nprotect.com/364
- 안철수연구소, 2012년 상반기 5대 보안 위협 트렌드, http://blog.ahnlab.com/ahnlab/1554
- LookOut, State of Mobile Security 2012, https://www.lookout.com/resources/reports/state-of-mobile-security-2012
- 잉카인터넷 대응팀 블로그, http://erteam.nprotect.com/
- Symantec, Symantec Intelligence Report: August 2012
- Bloomberg, Sony Network Breach Shows Amazon Cloud's Appeal for Hackers http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html
- Mcafee, Dissecting Operation High Roller, http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf
- Fortinet, Cybercriminals Today Mirror Legitimate Business Processes http://www.fortinet.com/sites/default/files/whitepapers/Cybercrime_Report.pdf

2. 2013년 동향 예측 관련

- Websense, 2013 Security Predictions, 2012.11, http://community.websense.com/blogs/websense-news-releases/archive/2012/11/13/seven-2013-cybersecurity-predictions-from-websense-security-labs.aspx
- Booz Allen, Top 10 Financial Services Cyber Risk Trends for 2013, 2012.11, http://www.boozallen.com/media-center/press-releases/48399320/cyber-top-ten-2013-press-release

- Imperva, Top Security Trends for 2013, 2012.12, http://blog.imperva.com/2012/12/security-trends-2013-trend-1.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Imperviews+%28ImperViews%29
- TrendMicro, Trend Micro Predictions for 2013 and Beyond: Threats to Business, the Digital Lifestyle, and the Cloud, 2012.12, http://blog.trendmicro.com/trendlabs-security-intelligence/predictions-for-2013/
- Fortinet, Fortinet's FortiGuard Labs Reveals 2013 Threat Predictions, 2012.12, http://blog.fortinet.com/fortinets-fortiguard-labs-reveals-2013-threat-predictions/
- PandaLabs, Security Trends in 2013, 2012.12, http://pandalabs.pandasecurity.com/security-trends-in-2013/
- Kaspersky, Kaspersky Security Bulletin 2012. Malware Evolution, 2012.12, http://www.securelist.com/en/analysis/204792254/Kaspersky_Security_Bulletin_2012_Malware_Evolution
- Zscaler, 2013 Security Predictions, 2012.12, http://research.zscaler.com/2012/12/2013-security-predictions.html
- Mcafee, McAfee's Top 10 Threat Predictions For 2013, 2012.12, http://biztech2.in.com/news/security/mcafees-top-10-threat-predictions-for-2013/150612/0
- WatchGuard, WatchGuard Predicts the Future of Network Security, 2012.12, http://www.watchguard.com/docs/brochure/wg_2013_security_predictions.pdf
- Lancope, 5 Key Computer Network Security Challenges For 2013, 2012.12, http://www.forbes.com/sites/ciocentral/2012/12/11/5-key-computer-network-security-challenges-for-2013/
- Trusteer, Five Most Dangerous Malware Trends of 2013, 2012.12, http://www.trusteer.com/blog/five-most-dangerous-malware-trends-of-2013

- AppRiver, 2013 IT Security Predictions from AppRiver, 2012.12, http://www.schwartzmsl.com/tangledweb/2012/12/mobile-mobile-mobile-it.php
- CNET, Four security trends defined 2012, will impact 2013, 2012.12, http://news.cnet.com/8301-1009_3-57560373-83/four-security-trends-defined-2012-will-impact-2013/
- Lookout, 2013 Mobile Threat Predictions, 2012.12, https://blog.lookout.com/blog/2012/12/13/2013-mobile-threat-predictions/
- E-Com Technology & Accounting Solutions, Security Lab Predictions for 2013, 2012.10, http://www.e-easi.com/index.php/2012/10/security-lab-predictions-for-2013/
- Symantec, Top 5 Security Predictions for 2013 from Symantec, 2012.11, http://www.symantec.com/connect/blogs/top-5-security-predictions-2013-symantec-0
- Microsoft, Using the Past to Predict the Future: Top 5 Threat Predictions for 2013, 2012.12, http://blogs.technet.com/b/security/archive/2012/12/13/using-the-past-to-predict-the-future-top-5-threat-predictions-for-2013.aspx
- Gartner, Gartner Cloud Security Predictions for 2013, 2012.12, http://cloudtimes.org/2012/12/14/gartner-cloud-security-predictions-for-2013/
- Lumension, 2013 Prediction Series Starts with Malware, 2012.12, http://blog.lumension.com/6175/2013-prediction-series-starts-with-malware/
- F-Secure, Top 7 Predictions for 2013, 2012.12, http://www.f-secure.com/weblog/archives/00002472.html
- RSA, 8 Computer Security Predictions For 2013, 2012.12, http://www.forbes.com/sites/ericsavitz/2012/12/07/rsas-art-coviello-8-computer-security-predictions-for-2013/
- Georgia Institute of Technology, Emerging Cyber Threats Report 2013,

2012.11,
http://www.gtsecuritysummit.com/pdf/2013ThreatsReport.pdf
- Sophos, Security Threat Report 2013, 2012.12,
http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx
- Checkpoint, Check Point 2013 Security Predictions, 2012.12,
http://www.cio-asia.com/resource/guest-blogs/blog-check-point-2013-security-predictions/
- 이니텍, 2013년 보안위협, 2012.12,
http://www.ddaily.co.kr/news/news_view.php?uid=98309
- ISF(Information Security Forum), Top 5 Security Predictions for 2013, 2012.11,
http://www.net-security.org/secworld.php?id=14033
- CIO, The Only 2013 Cybersecurity Predictions List You Need to Read, 2012.12,
http://blogs.cio.com/security/17647/only-2013-cybersecurity-predictions-list-you-need-read
- Bluecoat, 2013 IT Security Predictions from BlueCoat, 2012.12,
http://www.schwartzmsl.com/tangledweb/2012/12/2013-it-security-predictions-f-3.php