情 報 保 護 學 會 誌
第23卷 第1號, 2013. 2

APT공격에 대한 금융권에서의 대응방안

한 성 백*, 홍 성 권**

요 약

APT 공격은 특정 기업 또는 기관의 핵심 정보통신 설비에 대한 중단 또는 핵심정보의 획득을 목적으로 공격자는 장기간 동안 공격대상에 대해 IT인프라, 업무환경, 임직원 정보 등 다양한 정보를 수집하고, 이를 바탕으로 제로데이공격·사회공학적 기법 등을 이용하여 공격대상이 보유한 취약점을 수집·악용해 공격을 실행하는 것을 말한다. APT 공격의 특징은 명확한 공격대상을 정하고 장기간 동안 다양한 정보를 수집하여 취약점을 악용할 수 있는 정교한 프로그램을 사용하여 매우 치밀하게 공격을 수행하는 것으로 현존하고 있는 보안솔루션이나 기술로는 탐지와 대응이 어려운 측면이 있다. 본 논문에서는 APT 공격의 정의와 국내외 사고사례에 대한 분석, 금융권에서의 APT 공격에 대응하기 위한 관리적 방안과 기술적 방안 그리고 이에 대한 보안솔루션에 대해 검토하여 금융권에 적절한 대응방안을 제시하고자 한다.

Ⅰ. 서 론

금융기관은 현재 다양한 보안위협에 직면하고 있다. 특히 IT기술을 활용한 온라인 거래 및 스마트 금융거래가 활성화되면서 악성코드 감염에 의한 가용성 저하 및 내부정보 유출 가능성, 내부직원에 의한 의도적인 정보유출, 정보시스템 등의 서비스 중단을 노린 DDoS 공격, 웹 애플리케이션의 취약점을 이용한 홈페이지 변조 및 정보유출 시도 등 다양한 공격들이 늘어나고 있다. 이러한 보안 위협을 고려하여 금융기관은 심층 방어를 위해 네트워크 보안 측면에서 방화벽, IPS, DDoS 대응장비 등을 구축하고 있고, 단말 보안측면에서 백신, PC 보안, DRM, DLP 등 다양한 보안솔루션을 구축 및 운영하고 있다. 보안사고에 대한 신속한 식별과 공격 시도 모니터링, 즉각 대응을 위해 보안시스템에 대한 통합 보안관제를 실시하고 있다. 또한, 금융기관은 보안통제 목표를 효율적으로 달성하기 위해 정보보호 관리체계를 수립하여 이행하고 있으며 이를 통해 임직원의 보안의식 제고와 보안사고를 예방하기 위한 체계적인 활동을 수행하고 있다. 금융기관의 다양한 심층방어를 우회하기 위해 공격자들도 정교한 프로그램을 개발하고 공격대상에 대해 전방위적으로 정보를 수집하여 취약한 연결고리를 찾아 다양한 공격기법을 적용하여 장기적으로 공격을 실시하고 있다. 금융기관의 보안담당자는 해당 조직이 보유하고 있는 정보 및 정보자산에 대해 모두 식별을 하고 발생 가능한 취약점과 위험에 대해 평가를 하여 보안대책을 수립하여야 한다. 취약점과 위험은 신규 정보자산의 추가, 응용시스템의 신규 개발 및 변경 등으로 인해 제거된 취약점이 다시 발생할 수 있으므로 지속적으로 취약점을 분석 평가하고 이에 대한 이력 관리를 실시하여야 한다. APT공격은 새로운 기법이 아닌 기존의 알려진 공격기법을 특정 공격 대상에 대해 복합적으로 적용하여 지속적으로 정보를 수집하고 목표로 한 타켓에 대해 정보유출 또는 시스템 중단 등을 시키는 것으로 이에 대한 대응방안을 명확하게 수립하기 어려운 부분이 있다. 본 논문에서는 금융권에서 APT 공격에 대해 대응하고자 할 때 업무 및 정보시스템의 특성에 맞게 대응할 수 있도록 관리적 측면, 기술적 측면, 솔루션 측면 등에 대해 대응방안을 정리해보고자 한다. 제 2장에서는 APT의 개념 및 공격방법과 이를 활용한 국내외 공격사례에 대해 분석을 하고 제 3장에서는 APT 공격에 대해 효율적으로 대응하기 위한 관리적,

* 신한데이타시스템 인프라사업본부 정보보안센터 (han@shinhan.com)
** 신한데이타시스템 인프라사업본부 정보보안센터 (sungkwoon.hong@shinhan.com)

기술적 측면과 대응솔루션에 대해 분석을 실시하여 적절한 대응방안을 제시하고자 한다.

Ⅱ. APT 개념

2.1. APT 공격의 목적 및 정의

홈페이지 변조, 시스템 침투 등 단순히 해커의 기술 수준을 과시하거나 단순 지적 호기심을 충족시키기 위해 해킹 공격이 발생하는 것과는 달리 특정 조직이 공격 대상에 대한 경제적, 정치적 이득을 확보할 수 있는 핵심 정보를 가져오기 위한 것이다. 이를 위해서 공격 대상의 IT인프라를 장악하여 지속적으로 유지하고 필요 시 재방문이 용이하도록 악성코드 등을 설치하며, 특히 장기간 동안 특정 목적을 위해 공격이 진행되었음에도 공격대상이 이를 인지하지 못하고 지나치는 경우가 많은 것이 특징이다. APT의 'Advanced'는 공격자가 단일 기술이 아닌 해당 공격목표에 맞는 제로데이 취약점, 기존 보안제품을 우회하는 특수 목적의 악성코드, 사회공학 기법 등 다양한 기술을 조합하여 공격을 수행한다는 의미를 포함하고 있다. 'Persistent'는 공격 목적을 달성하기까지 지속적으로 새로운 기술과 방식이 적용된 공격을 지속적으로 하는 것으로 탐지 및 대응을 회피하기 위해 탐지방해, 대응방안 조치 회피 시도 등을 포함하고 있어 피해 범위 및 규모가 상당할 것이다. 'Threat'은 정보보호 분야의 위협 자체를 말하는 것이며, 여기에는 악성코드, 취약점, 해킹 등의 IT 기술에 의해 발생하는 위협으로 자동화된 툴이나 단순 스캐닝 기술에만 의존하지 않고 사람이 직접 표적을 분석하고 이를 바탕으로 다양한 공격을 시도하는 사회공학적 기법을 모두 포함한다.

2.2. APT 공격기법

APT 공격자는 사전조사, 제로데이 취약점 공격, 사회공학 기법 적용, 은닉, 적응, 지속 등의 공격기법을 조합하여 사용하는 것으로 알려져 있다. ①사전조사(Reconnaissance): 공격자는 공격 목표에 대한 Kill Chain을 구성하기 위해 공격 목표의 홈페이지, 외부 공개자료, 조직도, 주요 임직원 정보, 협력업체, 정보시스템 유형 및 버전, 애플리케이션의 종류 및 버전 등 공격목표에 대해 전방위적으로 정보를 수집하고 공격에 활용할 수 있는 취약점을 식별한다. ②Zero-Day 공격: 사전 조사된 정보를 바탕으로 정보시스템, 웹 어플리케이션 등의 알려지지 않은 취약점 및 보안시스템에서 탐지되지 않는 악성코드 등을 감염시키는 것이다. 제로데이 취약점은 백신 또는 IPS 등에서 탐지되지 않으므로 해당 취약점에 의해 악성코드에 감염된 PC는 동일한 취약점을 보유하고 있는 PC를 스캔하여 감염시킨다. ③사회공학 (Social Engineering): 공격목표의 중요 임직원 및 외부 유명인사 등을 가장하여 제로데이 취약점을 악용한 악성코드, 프로그램 등을 이메일, SNS, App 등을 통해 전송한다. ④은닉(Convert): 트로이목마 등 악성 프로그램을 설치하고 정상적인 이용자로 가장하여 시스템 접속정보 등에 대한 정보수집과 서비스 이용패턴, 방법 등에 대한 모니터링을 수행하는 것으로, 관리자 계정의 확보를 시도하여 관리자 권한으로 상승 후 수집 가능한 모든 정보를 수집한다. ⑤적응(Adaption): 권한상승을 통해 목표로 한 정보를 획득한 이후 공격대상의 내부 서버에 암호화하여 저장하거나 압축파일로 저장하여 비정기적으로 공격자의 단말기로 유출하는 등 공격이 탐지되지 않도록 하는 활동, 공격이 탐지 되었는지를 지속적으로 모니터링 하는 활동, 공격이 탐지된 경우 대응을 하는 활동 등을 포함한다. ⑥지속(Persistent): 공격자가 핵심정보를 지속적으로 유출시키기 위해 백도어 등의 프로그램을 설치하여 표적대상에 지속적으로 접근할 수 있도록 한다.

2.3. APT 공격기법이 적용된 사례

2.3.1 영국 RBS 월드페이 해킹

2008년 일명 '캐쉬어(Cashier)'로 알려진 러시아, 에스토니아, 몰도바 등 8명의 다국적자로 구성된 해킹그룹이 영국의 RBS은행의 월드페이 시스템에 침입하여 신용카드 정보를 훔쳐 복제카드를 만들고, 신용카드 한도를 올려서 12시간 동안 미국, 러시아, 우크라이나, 에스토니아, 이탈리아, 홍콩, 일본, 캐나다 등 전 세계에 있는 49개 도시의 2,100개 ATM 기기에서 약 950만 달러를 인출한 사건이 발생하였다. 해커들은 네트워크에 접속하여 암호화된 방화벽을 뚫고 카드번호와 패스워드를 알아내고, 이를 은폐하기 위해 시스템 데이터를 파괴

하였으며, 이 사건으로 월드페이 서버에서 150만 카드 이용자들의 개인정보와 금융정보, 100만 노동자들의 사회보장번호가 유출됨.

2.3.2 글로벌 에너지 기업 해킹 (나이트 드래곤 사건)

2011년 엑슨모빌, 마라톤오일, 코노코필립스, BP, 베이커휴즈 등 미국의 글로벌 에너지 기업 5곳이 해킹을 당하는 일명 '나이트 드래곤' 사건이 발생하였다. 이 해킹은 2009년부터 2년 동안 중국의 서버에서 이루어졌으며, 미국과 네덜란드에 구축한 통제 서버를 이용하여 카자흐스탄, 대만, 그리스, 미국의 컴퓨터 시스템에 접근하여 가스와 석유분야의 생산시스템, 석유 탐사와 관련된 재정 문서, 석유 및 가스의 임대 계약 및 산업 통제 시스템에 대한 정보가 유출됨.

2.3.3 이란 원자력 발전 시설 해킹 (스턱스넷)

일명 'Stuxnet'이라 불리는 악성코드에 의해 2010년 7월 이란 원자력 발전 시설을 마비시킨 공격이 발생하였다. 이 공격으로 이란 원자력 발전 시설의 원심분리기 중 20%가 가동이 중단되었다. 스턱스넷에 의한 공격은 독일 지멘스사의 산업자동화 제어 시스템인 SCADA (Supervisory Control And Data Acquisition)의 소프트웨어를 그 공격대상으로 하였고, 내부망인 SCADA를 공격하기 위해 USB를 통해 감염되도록 하였으며, 원자력 발전소 내부에서 다른 시스템으로 유포시키기 위해 기존에 알려진 MS08-067 취약점과 함께 패치가 없는 Microsoft사의 4개의 제로데이 취약점을 사용하였다. 또한 훔친 디지털 전자인증서로 서명된 컴포넌트를 사용하는 등 상당히 고도화된 공격기술로 APT 공격의 대표적인 사례라고 할 수 있음.

2.3.4 미국 국립 오크리지 연구소 해킹

2011년 4월 미국 에너지부(DOE) 산하의 국립 오크리지 연구소(ORNL)가 사이버 공격을 당한 것이 발견되었다. 이 공격은 ORNL에서 가지고 있는 기술 데이터를 훔치기 위한 것으로 분석되었으며, 약 1GB 정도의 기술 데이터가 유출된 것으로 파악되었다. 이 공격은 회사 복지와 관련된 이메일을 연구소 인사부에서 발송하는 것처럼 만든 스피어 피싱 메시지를 통해 연구소 시스템에 접근하였으며, 이메일 메시지 수신자들이 링크를 클릭하는 순간 악성코드가 시스템에 다운로드 되고, 그 중 단지 2대의 컴퓨터가 감염되었음에도 약 1주일 간 잠복하여 있다가 원격 서버에 데이터를 수집하여 전송한 것으로 파악됨.

2.3.5 모건 스탠리 해킹 (오로라 사건)

2010년 1월 구글과 모건 스탠리 등에서 해킹을 통해 중요 정보를 훔쳐가는 일명 '오로라' 사건이 발견되었다. 이 공격은 2009년 6월에 시작하여 6개월 여 기간 동안 200여 개 이상의 회사를 대상으로 지속되었으며, 중국의 서버를 이용해서 공격이 이루어졌음이 확인되었다. 규모가 큰 첨단 정보통신 사업체들인 구글 등을 대상으로 기업들이 가지고 있는 SW 소스코드와 같은 중요 데이터를 탈취할 목적으로 이루어졌다. 이 과정에서 Microsoft사의 인터넷 익스플로러 제로데이 취약점이었던 MS10-002가 사회공학적으로 악용되었으며, 안티바이러스에서도 탐지되지 않도록 특별히 제작된 원격제어 형태의 악성코드도 공격에 이용되었음.

2.3.6 RSA 해킹

2011년 3월 암호 전문 보안기업인 미국 RSA의 정보보안사업부가 해킹 당하는 사건이 발생하여, 이 사건으로 RSA의 OTP 제품인 시큐어 ID (접속할 때마다 다른 비밀번호를 써야 하는 토큰 등 이중 인증요소에 기반해 기업데이터와 네트워크를 보호하는 기술)의 기밀 정보가 유출되었으며, 현재까지 훔친 정보를 이용한 피해 사례는 보고되지 않고 있으나, 온라인 IT 미디어 미국 씨넷에서 보도한 바에 따르면 RSA OTP솔루션을 사용하는 기업들에게는 이를 대체할 만한 인증수단이 필요하며 의외로 해킹사건의 여파가 심각할 수 있다고 한다. RSA의 기술을 이용하는 기업이나 기관의 보안 위험이 높아지게 됨.

2.3.7 농협 해킹

2011년 4월 농협 전산망에 있는 자료가 대규모로 손상되어 수일에 걸쳐 서비스가 마비되는 사건이 발생하

였다. 이 사건은 외주업체 직원이 2010년 9월에 커피숍에서 받은 웹하드 무료 다운로드 쿠폰으로 업무 노트북에 영화를 다운로드 받다가 악성코드에 감염됨으로써 발생하였다. 해커들은 이 악성코드를 통해 노트북을 점령하여 7개월 동안 각종 악성코드를 심고, 최고위관리자의 비밀번호 등 전산망 관리를 위한 각종 정보들을 탈취하고, 도청 프로그램까지 설치하였으며, 사건이 발생한 2011년 4월 12일에 공격 명령 파일을 설치한 후, 원격으로 공격 명령을 실행하였다. 이때부터 1차 공격을 받은 서버들이 좀비 컴퓨터로 변해 다른 서버들을 공격하였으며, 공격 개시 30분 만에 운영 시스템의 절반이 파괴됨.

2.3.8 네이트, 싸이월드 개인 정보 유출

2011년 7월 네이트의 데이터베이스에 가입자 3,500만 명의 아이디, 비밀번호, 이름, 주민등록번호, 연락처 등 개인정보가 유출된 사고가 발생하였다. 이 사건은 IP주소로 볼 때, 중국의 해킹그룹에서 수행한 것으로 추정되며, 해킹그룹은 내부 개발자의 PC를 장기간 집중 공격하여 이를 통해 해킹에 성공한 대표적인 APT 공격 사례라고 추정됨.

2.3.9 현대캐피탈 해킹

2011년 4월 현대캐피탈의 고객정보가 유출되는 사고가 발생하였다. 이 사건은 해커 그룹이 업무관리자의 아이디와 비밀번호를 습득한 후, 광고메일 발송 서버와 정비내역 조회 서버에 침입해 화면을 복사하거나 해킹 프로그램을 통해 다운로드하는 방법으로 175만 명의 고객정보를 해킹한 사건이다. 특히 이슈 사항으로는 현대캐피탈은 퇴사자의 아이디와 비밀번호를 삭제하지 않았으며, 퇴사자가 사용했던 아이디와 비밀번호를 통해 총 7회에 걸쳐 무단 접속이 발생함.

Ⅲ. 금융권에서의 APT대응방안

금융권은 이메일 또는 문자메시지 등을 통해 해당 금융기관의 위장사이트로 유인하여 금융정보를 노리는 피싱, 금융서비스의 중단 또는 지연 등을 노리는 DDoS 공격 등이 사회적 이슈가 되고 있다. 최근에는 APT 공격 등 전자금융 사고가 점차 복잡·지능화 되고 있는 추세이다. APT 공격은 다양한 공격기법을 복합적으로 적용하여 즉각적인 대응기술의 확보가 곤란하고, 보안패치가 적용되지 않은 제로데이 공격일 경우 바이러스 백신에 의해 탐지 및 치료가 되지 않아 정보유출 등이 지속적으로 발생될 것이다. APT공격의 효과적인 대응을 위해서는 조직 내부의 보안정책 및 체계를 분석하여 관리적, 기술적 대책을 수립하고 보안관리 체계를 정비하여야 한다. 또한 제로데이 취약점을 악용한 공격과 보안시스템에 탐지/차단되지 않는 악성코드 등에 대응하기 위한 APT 대응 솔루션을 구축하고 분석을 통해 보안사고를 예방하여야 한다.

3.1 관리적 보안대책

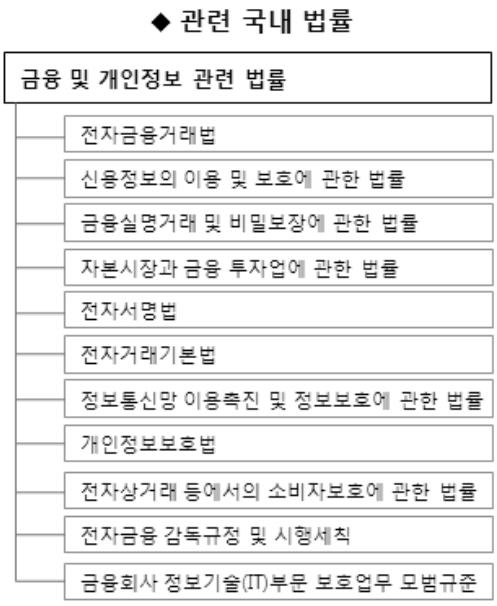
3.1.1 정보보호관리체계 강화

대부분의 금융권에서는 ISO27001 등의 표준을 고려하여 수립된 정보보호관리체계를 유지하고 있으며 이를 지속적으로 유지 및 효과적인 체계 수립을 위해 노력하고 있다. 하지만 기 수립된 정보보호관리체계는 대부분 정보보안 조직을 중심으로 한 IT부서에 적용이 되고 있으며 전사적으로 이에 대한 이해와 준수 여부에 대해서는 인식이 부족하다. 정보보호관리체계가 정보보안조직 위주의 활동이 아닌 전사 차원에서 수행될 수 있도록 경영진의 지속적인 관심과, 후원뿐만 아니라 정보보안 조직에서의 지속적인 인식제고 및 홍보활동 등도 매우 중요하다. 또한 상시 보안관제와 정기적인 취약점 진단 및 대책적용, 정보보안 컨설팅, 보안감사 등을 수행할 필요가 있으며, 세부적인 강화 방안은 다음과 같다.

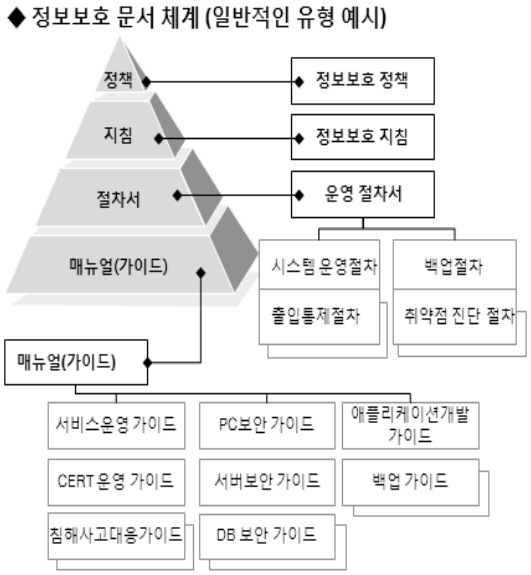
3.1.2 정보보호 규정 및 지침 강화

최근 개인정보, 금융정보와 주요 정보통신 기반시설에 대한 정보보호의 중요성이 날로 증대하여 감독기관에서는 이와 관련된 법률 및 지침, 가이드 등을 제정하여 시행하고 있으며 이에 대한 요건이 지속적으로 강화되고 있다. 이와 관련하여 정보보호위원회나 최고의사결정기구에서는 제/개정되는 정보보호 관련 법규 및 감독기관의 기준, 가이드, 전자금융거래법, 전자금융감독규정, 정보통신망 이용촉진 및 정보보호에 관한 법률..

등 [그림 1]참조 이에 따라 금융기관에서는 법률 및 제도의 시행에 따른 적용 대상 여부 및 파급 효과에 대해 종합적으로 검토하여 내부 규정 및 지침 제/개정을 실시하고 있다. [그림 2] 정보보안정책 문서 체계 참조



〔그림 1〕 현재 금융회사들이 준수하고 있는 국내 법률



〔그림 2〕 정보보안 정책 문서체계

3.1.3 임직원 인식제고 강화

최근 내부 임직원의 정보보안 사고와 관련하여 다음과 같은 조사 결과가 보고되었다. 정보보안 사고의70%가 근무중인 임직원 등 내부자 소행(Garthner research), 산업기술정보 유출자의 90% 이상이 현직/퇴직 사원(한국산업기술진흥원), 내부의 중요기밀 보유자가 기밀유출을 시도할 경우 성공가능성에 대해 전체기업의 59.7%가 기밀유출이 가능하다고 응답하였으며 중소기업의 경우 67.6%가 성공가능성이 높음(대한상공회의소). 외부 해커에 비해 내부 임직원의 핵심정보에 접근하기 용이할 뿐만 아니라 국내 여건상 특정 인력에게 과도한 권한이 부여되거나 보안정책의 예외적인 적용이 많이 발생하고 있다. 임직원의 보안사고에 의한 비용손실이 해커에 의한 손실의 2배(Information Week) 정도로 알려져 있으며, 임직원의 보안의식 결여와 임금, 처우, 근무환경에 대한 불만으로 외부세력의 금전적 유혹에 의해 핵심 정보의 유출 등이 발생할 수 있는 가능성이 있으며, 특히 금융권은 금전과 직접적인 영향 및 피해가 있으므로 지속적인 보안교육에 힘써야 한다.

정보보안 교육 대상을 고려하여 일반 과정, 책임자 과정, 실무자 과정으로 구별하여 정보보호 교육 및 훈련 계획을 수립하여야 하고, 각 부문별 직위 및 담당 업무, 입사 시점 (신입사원, 기구성원)을 고려하여 교육계획을 세우고 교육을 실시하여야 한다.

〔표 1〕 대상자별 교육과정

일반 과정	전 직원 및 아웃소싱 직원	정보보안의 개념과 필요성 등 기본소양 교육, 내부 보안규정 등의 전반적인 내용 및 최신 정보 동향, 보안사고 사례
책임자 과정	팀장급 이상 실무 책임자	정보보안 규정에서 명시된 책임 및 권한 등의 내용 및 IT 컴플라이언스
실무자 과정	보안관리자 중요 정보시스템 담당자	담당업무와 관련하여 요구되는 보안 교육 및 신규기술교육

APT 공격에 대해 효과적인 대응을 위해서 사회공학적 공격을 대비한 대응방안, 악성코드 등을 포함한 이메일 등의 대응방안, 정보유출 등 보안사고 신고 및 대응방안 등에 대해서도 추가적인 교육이 필요하다.

3.1.4 정보보호 전담 조직의 강화

대부분의 기업 정보보안 조직은 IT개발 및 운영을 담당하는 부서 또는 경영지원부서 등에서 겸직 형태로 수행하고 있으며 정보보호 업무에 대한 체계적인 계획 수립 및 이행이 어려운 실정이다.

금융권의 경우 타 산업분야에 비해 전담조직의 구성 및 보안인력의 비율이 높은 편이나 제1금융권을 제외한 나머지 금융권에서는 전담조직 운영비율이나 전문인력이 부족한 현실이다. 금융권에서는 금융회사 정보기술(IT)부문보호업무 모범규준에 따라 총 임직원수의 5/100이상을 정보기술부문 인력으로, 정보기술부문 인력의 5/100이상을 정보보호인력으로 각각 확보하도록 규정되어 있어 법적 요건의 만족을 위해서라도 보안인력의 추가 확충은 필수적인 사항이 되고 있다.

다만, 보안 전문인력의 확충에 따라 보안인력의 책임과 역할 등에 대해 충분한 고려를 하여 인력 운영방안을 수립하여야 하며 그렇지 않을 경우 장기적으로 인력간의 업무중복이 발생하거나 업무누락, 보안업무 활동의 책임소재 불분명 등으로 인해 보안조직의 정보보안 활동에 부정적인 영향을 줄 수 있다.

3.1.5 정보자산 분류 활동 강화

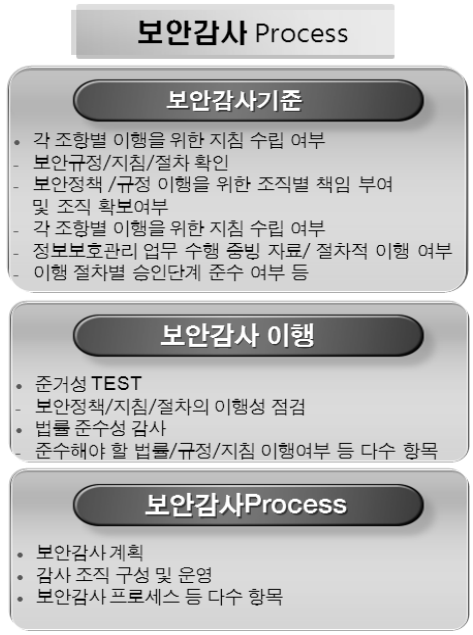
금융권에서 보유하고 운영중인 정보 및 정보시스템 등의 보유자산에 대한 분류 기준과 자산의 취급 절차에 의거하여 자산관리 담당자는 정보 자산을 분류하고 주기적인 개선 활동을 실시하여야 한다.

①정보자산 조사: 기밀성, 무결성, 가용성 기준에 따라 연 1회 주기적인 정보자산 보유현황 파악 및 중요도 평가가 실시하여야 한다. ②정보자산 지속적 관리: 정보자산의 사용용도 변화, 추가 도입장비 등 변경 발생 시 해당자산에 대한 정보자산 중요도 평가를 실시하며 정보자산 보유현황을 갱신하여 관리하여야 한다.

③보안등급 표시 및 취급 절차: 서버, 네트워크, 보안장비 별 정보자산의 보안등급을 표시하며 주기적으로 등급 표시 상태를 점검 및 관리하여, 표시상태가 적정수준을 유지토록 하여야 하며 정보자산의 보안 등급에 따른 보안대책과 취급절차를 수립하여야 한다.

3.1.6 정보보안감사 체계화

감사의 범위는 일반적으로 수립된 정책, 지침 및 절차의 이행여부, 통제의 적절성, 부당행위 발견, 프로그램 완전성, 시스템 설계 및 이행, IT자원 접근권한 등이며 처벌과 적발이 목적이 아닌 조직의 보안능력 향상과 사고예방의 방향으로 지속적이고 주기적인 감사를 계획하고 수행하여야 한다. 특히, 정보시스템의 계정 및 접근권한, 비정상 행위의 수행여부, 비인가 프로그램의 설치 여부 등 악의적인 행위가 없는지 이에 대한 집중적인 감사가 필요하다. IT부문의 보안감사를 성공적으로 수행하기 위해서, 해당 금융기관의 IT환경에 대한 전문지식을 보유한 내부 전문인력을 활용하거나, 정보보호 컨설팅 전문업체나 회계법인 등에 소속된 정보보안전문가 등의 외부인력을 이용하여 감사를 수행하도록 한다.



〔그림 3〕 보안감사 프로세스

3.1.7 정보보안 활동 실시

금융권에서 주기적으로 임직원의 보안의식 제고 및 보안사고의 사전 예방을 위해 정보보안의 날 등을 지정하여 운영하고 있다. 각 금융사의 정보보안 규정을 고려하여 주기적인 기본보안점검 및 보안의식을 고취할 수

있는 다음과 같은 활동을 실시하여야 한다.

① 안티바이러스 백신의 주기적 실행
② 불법소프트웨어 및 비인가 프로그램의 지속적 관리
③ 운영체제의 주기적 보안패치
④ Clean Desk 및 Clean Office 활동

3.1.8 정기적인 대응훈련

발생할 수 있는 각종 보안사고 및 사이버테러에 관한 대응훈련을 정기적으로 실시하여야 하며, 이를 통해 보안위기 상황을 가정한 조직 내 각 부문 및 담당자의 역할 및 책임, 행동요령 등을 숙지시킴으로써, 능동적인 대응 실습을 통한 역량강화를 기대할 수 있다.

정기적인 대응 훈련 시 형식적인 내용에 따른 보여주기식 대응훈련이 아닌 조직의 실제 대응 능력이 내재화될 수 있도록 정교한 시나리오를 바탕으로 각 담당자들의 적극적인 훈련 참여가 필요하다.

3.2 기술적 보안대책

3.2.1 단말보안

APT공격은 서버, DB 뿐만 아니라 임직원의 개인단말에 대한 공격도 고려할 수 있으며 이는 단말에 설치된 프로그램의 신규 취약성을 이용한 제로데이 공격이다. APT 공격은 목표의 취약성을 파고드는 지능적인 공격이므로, 최신 보안 패치에 대한 실시간 업데이트 기능이 강화된 PMS, 백신 등을 통해 보호하며 내부 보안정책을 따르지 않으면 업무망/내부망 접속을 차단하는 NAC(Network Access Control), 내부정보가 외부로 유출되는 것을 차단하는 PC보안솔루션, 내부 업무망과 인터넷망의 분리 등을 고려할 수 있다.

3.2.2 인증요소추가

APT는 공격자가 내부에 침투한 이후 중요 시스템을 공격하는 특성이 있으므로 중요 시스템의 로그인시, OTP와 같은 two-factor 인증 요소를 추가하여 내부 접근통제 기능을 강화하면, 정상적인 사용자를 도용하거나 가장하여 내부시스템에서 정보를 탈취하려는 내부 공격을 지연시키거나 더욱 어렵게 할 수 있다.

3.2.3 무선망 통제

내부 업무망과 인터넷망의 분리 등 인터넷 사용을 통제 하면 이에 따라 무분별한 Wi-Fi, Wibro, 비인가 AP를 통한 테더링 사용 등이 나타날 수 있다. 이는 위험에 직접 노출되는 격이므로 위험이 크게 증가 하게 된다. 이에 무선침입방지시스템(WIPS)을 통한 비인가 AP 무선기기 사용을 적극적으로 차단하여야 한다.

3.2.4 인간 및 정보중심 보안정책

기존의 보안정책은 통신, 시스템 등 정보시스템 위주였으나, 인간 및 정보중심의 보안정책으로 접근이 필요하다. 보안사슬의 가장 약한 부분인 인적보안을 강화하고 접근제어 강화와 암호화 등의 정보중심의 대응방안을 강화하면 정보 유출시에도 공격자는 정보를 악용할 수 없을 것이다. DRM (Digital Rights Management), DB암호화, DLP(내부정보유출방지)의 도입 검토와 주기적인 인식제고 교육이 필요하다.

3.3 APT 솔루션

3.3.1 APT 솔루션 개요

기존 보안 시스템은 APT 공격에 대해 직접적인 방어 기능은 없으며 [표 2]와 같은 문제점을 가지고 있다.

기존 보안솔루션으로 대응이 어려운 악성코드로 인한 고객정보 유출, 전산망 마비 등 보안사고의 발생 위협이 증가하고 있기 때문에 최신 신종 보안위협에 대한 선제적 대응 필요성이 증가하게 된다. 단말장비에 가장 많이 설치되어 있는 보안솔루션인 안티바이러스 백신은 알려진 시그니처에 기반해 바이너리 패턴을 매치시키는 방식을 사용한다. 바이러스가 발견되면 매번 일대일로 적용되는 업데이트가 필수적으로 동반되지만 이는 APT와 같이 알려지지 않은 공격 패턴에 대해서는 효과적인 대응책이 되지 못하는 것이 사실이다. 이러한 문제점을 고려하여 행동기반 탐지 솔루션이나 평판 기반 기술, 지능형 동적 콘텐츠 분석 기술 등을 융합하여 정보중심적인 접근법과 인공지능 기술을 접목해 알려지지 않은 보안 위협에 대응하고자 보안솔루션 업체들은 앞다투어 APT 솔루션을 제시하고 있다. APT솔루션은 실

〔표 2〕 기존 보안장비가 가진 APT대응 문제점

보안장비	문제점
DDX	Victim PC, C&C 서버 등 DDoS 공격 IP에 대한 차단 정책 적용 악성코드 유포 사이트에 대해 IP 차단 정책 적용
방화벽	외부 -> 내부로의 접근은 통제, 내부 -> 외부는 허용하는 정책 적용 최근 악성코드는 Back-connection을 이용하여 내부에서 외부에 있는 Command and Control 서버로 연결 웹사이트 접속을 위한 80번 포트는 기본적으로 Open되어 있으며 이를 통해 악성코드 등 감염 또는 유포 가능
NAC	필수 보안프로그램 미설치 시 네트워크 사용을 통제하나 악성코드의 탐지 및 차단과는 무관
IPS/백신	Signature 기반의 탐지 및 차단 해커는 Signature가 알려지지 않은 신종/변종 악성코드 사용
PC보안	PC의 이동저장매체 및 CD/DVD 등 저장매체 사용 통제 악성코드의 탐지 및 차단과는 무관
보안관제	원하는 정보를 확보할 때까지 장기간에 걸쳐 은밀히 활동 Worm 및 공격 탐지 패턴에 발각되지 않음 비정형적인 통신을 이용한 정보유출은 탐지하지 못함

행 파일의 특성, 유입 경로, 행위를 기반으로 알려지지 않은 신규/변종 악성 코드 탐지에 특화된 차세대 보안 위협 대응 솔루션이다.

APT솔루션은 네트워크 트래픽 분석을 통해 악성코드에 감염된 좀비PC가 외부의 해커에게 접속하는 행위를 탐지하는 등 모든 네트워크 트래픽을 저장하고 분석할 수 있는 기능을 제공 한다.

3.3.2 APT 솔루션

기존의 좀비 PC 대응 솔루션은 '악성 판정'에만 중점을 두기 때문에 가장 중요한 오진 최소화에 맹점이 있으며, 분석 기술에 이용되는 정책 또한 악성코드 전문기업 보다 기술력이 낮다는 악성코드 분석의 한계가 존재한다. APT대응 솔루션의 경우 모든 트래픽을 수집하고, 트래픽의 관계 분석 또는 행동기반의 파일 분석이 특징이며, 악성코드 분석 시스템의 어플라이언스화를 통해 정확도 및 오진율을 극대화 하고, 1차 진단에서 알려지지 않은 신종 악성코드일 경우 탑재된 가상분석 OS에 실행하여 악성여부를 2차로 판별한다. 금융권의 경우 단말장비에 다양한 Agent가 설치되어 있어 임직원이 단말 이용 시 속도저하, 보안Agent간의 충돌 등이 발생할 수 있으므로 Agentless 방식을 고려하여야 하며 향

분류	A사	B사	C사	D사
주요 기술	-모든 트래픽 저장 및 조회 -Content 기반 이상 트래픽 판별 -L7단위 트래픽 조합 및 가시화 -실행 파일 추출 및 위험도 분석	-Behavior 기반 파일 분석 -동적 컨텐츠 기반 파일 분석	-Behavior 기반 파일 분석	-Av엔진 기반 파일 분석
구성 및 성능	-Agent 없음 -Out-of-band 방식 -무제한 / 복수장비 분산 처리 -10G fiber 옵션 제공	-Agent 를 통한 치료 가능 -Out-of-band 방식 -Max: 4.0 Gbps -10G fiber 옵션 제공	-Agent 없음 -In-line/Out-of-band 방식 -Max 1.2 Gbps -10G fiber 미지원: 별도 Smart TAP 구매 필요	-Agent 를 통한 치료 가능 -Out-of-band 방식 -Max 1.0 Gbps -10G fiber 미지원: 별도 Smart TAP 구매 필요
악성코드 분석 체계	-파일 속성/유입 경로 기반 분석 -평판/Signature 기반 분석 -Behavior 기반 분석(가상시스템)	-Signature 기반 분석 -Behavior/Content 기반 분석 (가상시스템)	-Signature 기반 분석 -Behavior 기반 분석 (가상시스템)	-Signature 기반 분석 -Sandbox simulation
알려진 정상/악성 파일 판정 기능	-VirusTotal 백신 엔진 -악성 파일 및 정상 파일 동시 판정	-내장 및 클라우드 기반 DB 이용, 악성 파일 및 정상 파일 동시 판정	-내장 및 클라우드 기반 DB 이용, Behavior 기반 분석 결과로 악성/정상 판정 모호	-AV엔진을 이용 악성 파일에 대해서만 판정
알려지지 않은 악성 파일 판정 기술	-Behavior/Content 기반 분석 (악성/정상 판정)	-Behavior/Content 기반 분석 (악성/정상 판정)	-Behavior 기반 분석 결과로악성/정상 판정 모호	-Sandbox simulation -해외 분석 센터로 의뢰 판정
오진 대응력	-정상 파일 오탐지 가능성존재	-국내 대부분 정상 상태 파일 정보 보유로 정상 파일에 대한 오탐지 매우 낮음	-정상 파일 정보 없음 -정상 파일에 대한 오탐지 가능성 존재	-정상 파일 정보 없음 -정상 파일에 대한 오탐지 가능성 존재
폐쇄망 고객	-사용 가능	-사용 가능	-사용 가능	-불가

〔그림 4〕 APT솔루션 비교

후 네트워크 확장성을 고려하여 10Gbps의 대역폭 지원 여부를 고려하여야 한다. 또한 국내외에서 발생하는 알려지지 않은 악성코드 및 제로데이 취약점에 대한 기술 지원 능력 등에 대해서도 종합적인 고려가 필요하다. 어떠한 보안시스템도 100% 완벽한 보안을 보장할 수 없다. 금융권에서 APT의 위협은 해당 금융사와 대고객, 나아가 국가경제에 파급력을 미치기 때문에 조직과 업무 구성원에 맞게 선택하고 잘 운영하여 그 피해를 최소화 한다는 개념으로 검토를 하여야 할 것이다.

3.3.3 APT 운영 및 고려 사항

APT 운영의 중점사항으로는 크게 3가지로 구분할 수 있다.

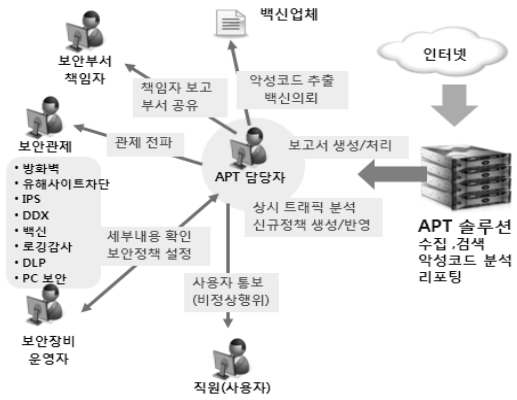
① 내부직원의 비인가 행위탐지/분석 (Proxy 프로그램 등 보안장비 우회 프로그램, 메신저, 비인가 클라우드 서비스 접속)

② 이상 트래픽 탐지 및 분석 (RDP(Remote Desktop Protocol) 등의 비정형 트래픽, 대량 트래픽, Packing 트래픽 등의 검출)

③ 의심되는 악성코드 분석 및 유해 트래픽 탐지 (악성코드, Trojan, BOTNet 및 사회공학을 고려한 악성코드를 포함한 메일 전송 검출). 1번의 경우는 내부 보안정책에 위반되는 행위를 막는 것이 주목적이고, 2 - 3번 의 경우가 중점 운영하여야 할 부분이다, 최근 많이 검출 되고 있는 패턴은 직원들의 클라우드 서비스 접속, Proxy tool을 이용한 유해사이트 우회접속, 80번 포트를 사용한 지속적인 데이터 업로드/다운로드를 하는 이상 트래픽 위협(내부정보 유출위협)과 알려지지 않은 지능형 악성코드 위협이다. APT 담당자는 상시트래픽 분석을 통해 이상징후 및 비정상 행위 탐지와 악성코드 의심파일을 추출하여 백신업체 분석의뢰를 하며, 이에 모니터링을 위한 Alert 설정을 한다. 보안장비 운영자는 APT담당자가 요청한 보안정책을 담당하는 보안장비에 적용하고, 보안정책 적용에 따른 탐지 및 차단 여부 모니터링을 실시한다. 백신업체는 APT 담당자가 요청한 악성코드 분석 및 백신 엔진 업데이트, 실시간 해외 동향 파악 등의 업무를 하게 되며, APT 운영에 있어서 APT담당자와 기존 보안솔루션 운영자, 백신 업체와는 긴밀한 공조가 필요하다.

〔표 3〕 APT관련 담당자별 역할

구분	역할
APT 담당자	악성코드 의심파일 추출 및 백신업체 분석의뢰 상시트래픽 분석을 통해 이상징후 및 비정상 행위 탐지 위 2가지 항목의 모니터링을 위한 Alert 설정 최적화
보안 장비 운영자	APT담당자가 요청한 보안정책을 담당하는 보안장비에 적용 보안정책 적용에 따른 탐지 및 차단 여부 모니터링 실시
백신 업체	APT담당자가 요청한 악성코드 분석 및 백신 엔진 업데이트



〔그림 5〕 APT 대응장비 관련 R & R

또한 운영 시 고려하여 할 사항은 다음과 같다.

1. 기존 보안장비 운영(정책 적용 등)과 달리 비인가 행위, 이상 트래픽 탐지, 악성코드 등에 대한 분석 업무 위주로 실시됨
2. 장비 담당자는 트래픽 분석, 악성코드 분석 및 분석 Tool의 활용 능력과 보안장비의 운영 경험이 필요
3. 대용량 트래픽을 효과적으로 분석하기 위해서는 분석능력을 갖춘 최소 2인 이상의 전문 인력이 필요함
4. 기존 보안장비의 운영과 달리 운영담당자의 비인가 행위, 이상 트래픽 탐지, 악성코드 등의 분석 역량에 따라 대응 수준이 달라짐

어떤 목표를 가지고, 어떤 것을 사례를 중점으로 운영 할 것인지, 기타 문제점들은 없는지 충분한 시범 운

영을 통해 운영지표를 확립한 후 운영해야 한다.

Ⅳ. 결론

APT 공격은 다양한 보안장비와 정보보호관리체계를 구축·운영하고 있더라도 조기 식별 및 대응이 어려운 측면이 있다. 금융권에서는 중요정보를 보유하고 있는 시스템에 대한 주기적 감사와 내부시스템 접근통제 강화 등의 대응 방안을 수립하고 적극적으로 이행한다면, 금융회사는 공격자가 침투에 성공하더라도 중요한 정보의 유출을 방지할 뿐만 아니라 이상 징후를 조기에 발견하여 신속히 대응하는 효과를 기대할 수 있을 것이다.

금융회사의 정보보안 업무도 일반 기업과 크게 다른 점은 없으나, 내부 정보가 외부에 유출되거나, 업무가 중지되었을 때 발생하는 피해는 해당 금융회사뿐만 아니라 동종업계와 국가 경제 전체에 심각한 영향을 미칠 수 있으므로 무엇보다도 사전예방과 투자, 교육 등에 꾸준한 관심과 지원이 필요할 것이다.

참고문헌

[1] RSA, "Mobilizing Intelligent Security Operations for Advanced Persistent Threats", *RSA Security Brief*, Feb 2011

[2] McAfee, "Global Energy Cyberattacks: Night Dragon", *McAfee white paper*, Feb 2011

[3] Ahnlab, "최신 해킹 유형과 하반기 위협 예측", *안철수 연구소 보안매거진 월간 安*, Jul 2011

[4] Frankie Li, ran2, "A Detailed Analysis of an Advanced Persistent Threat Malware", *SANS Institute Infosec Reading Room*, Oct 2011

[5] 주윤경, 서현범, "2012년 IT 트렌드 전망 및 정책 방향", *한국정보화진흥원 IT정책연구시리즈 23호*, Dec 2011

[6] Cisco, "2011년 2분기 글로벌 위협보고서", 2011

[7] 남기효, 김윤홍, 권한우, "최신 정보보호기술 동향: APT 공격 및 대응", *정보통신산업진흥원 주간기술동향 1513호*, Sep 2011

[8] Ahnlab, "보안위협, 점차 교활하고 정교해진다", *Ahnlab [Special Report]2부*, Jan 2012

[9] 구헌, "APT공격의 위험성과 전자금융의 대응과제", *금융보안연구원 이슈리포트 Vol.2012-004*, Feb 2012

[10] Trend Micro, "IXESHE An APT Campaign", *Trend Micro Incorporated Research Paper*, May 2012

[11] 박종훈, "1분기 보안 보고서 키워드:APT, SNS, 애플", *정보통신산업진흥원 주간기술동향 1544호*, May 2012

[12] Ahnlab, "이메일로 시도되는 APT 공격 주의", *ASEC 보안 위협 동향 리포트 2012 Vol.31*, Jul 2012

[13] Trend Micro, "The HeartBeat APT Campaign", *Trend Micro Incorporated Research Paper*, Dec 2012

〈著者紹介〉

한 성 백 (Sung-Baek HAN)
2005년 2월 : 인제대학교 환경공학과 학사 졸업
2007년 2월 : 인제대학교 환경학과 석사 졸업
2010-2012.3월 STG 시큐리티 선임(과장) 컨설턴트
2012년 4월~현재 신한데이타시스템 정보보안센터 과장
<관심분야> IT Compliance, 디지털포렌식, 모바일보안, 보안관리체계, 스마트그리드보안, 스마트워크보안, 보안성 평가

홍 성 권 (Sung-Kwon Hong)
1996년 2월 : 강원대학교 전자공학과 졸업
2006년 10월-2012년 4월 에이쓰리 시큐리티 수석(부장) 컨설턴트
2012년 4월~현재 신한데이터시스템 정보보안센터 차장
<관심분야> :BIMS, ROSI, ISMS/PIMS, PCI DSS, Risk Management