보안 관련 기사

㈜IT 미디어 그룹 ▌김 용 석
yskim@com-world.co.kr
출처 : 컴퓨터월드와 IT DAILY

더존비즈온, 포렌식 기반 DLP 솔루션 공급 잇따라

정보 유출 사전 차단 목적으로 신기인터모빌, 트러스, 대우공업 등이 도입

국내 소프트웨어 전문기업인 더존비즈온(대표이사 김용우, www.duzon.co.kr)은 자사의 정보유출방지(Data Loss Prevention: DLP) 솔루션인 '아르고스 이아이엠(Argos EIM)'을 최근 현대기아차그룹 1차 협력사인 신기인터모빌과 한국쓰리엠의 1차 협력사인 트러스 등에 잇달아 공급했다고 2일 밝혔다.

더존IT그룹의 계열사인 IT보안 전문기업 ㈜더존정보보호서비스(대표이사 이찬우)가 개발한 '아르고스 이아이엠(Argos EIM)'은 디지털 포렌식 기반 DLP 솔루션으로, 작년 10월에 기업에서 업무 수행 중에 작성되는 각종 문서들 가운데 중요 정보가 포함된 문서의 효율적인 관리 및 기밀의 외부 유출을 방지하기 위해 설계되었다.

특히, 이 제품은 중요한 기업 정보에 대한 조사, 관리 및 파일 생성과 저장 현황 등을 관리자가 직접 감시할 수 있을 뿐만 아니라, 유출시점의 화면 캡처와 녹화, 기업/개인 정보가 포함된 파일의 실시간 감시 및 차단, 사내 메일과 웹 메일, 메신저, FTP, P2P를 통한 첨부파일 유출 차단, 이동저장장치 및 출력물의 통제가 가능하며, 공유폴더 해제, 네트워크 드라이브 연결 통제와 같은 네트워크 취약성을 보완할 수 있고 S/W의 라이선스 정보 및 IP변경 이력 등의 기능을 제공한다.

이 밖에도 문서의 생성, 복사, 수정, 삭제 이동 등 모든 문서 관련 히스토리를 추적하며, 주요 정보문서 보유 여부에 따라 통제정책을 다르게 적용할 수 있도록 유연하게 지원하는 등 개별 기업의 요구에 따라 맞춤형으로 구축이 가능하다.

경찰청 위장한 악성코드 이메일 확산

업데이트 기능 가진 악성코드 통해 좀비 PC 양산 가능성 커

지방경찰청 사이버범죄수사대의 명의를 위장한 악성코드 이메일이 11월 3일부터 유포되고 있어 PC 사용자들의 주의가 요구된다. 이스트소프트(대표 김장중 www.estsoft.co.kr)는 지방경찰청 사이버범죄수사대의 명의를 위장하여 가짜 참고인 출석 요구서 내용과 악성코드가 담긴 이메일을 유포하고 있다고 3일 밝혔다.

악성코드는 사설 스포츠 도박 광고를 보여주도록 개발되어 있으며, 윈도우 부팅마다 악성코드가 같이 실행되도록 시스템 레지스트리를 변조한다. 또한, 자기 자신을 업데이트할 수 있는 기능을 가지고 있어 악성코드 제작자의 의도에 따라 추후 새로운 악성코드를 다운로드 받을 수 있다.

이스트소프트에서는 현재 이들 악성코드에 대한 진단 및 삭제(진단명: V.TRJ.Agent.Win018.A, V.DRP.Agent.593498) 기능을 알약을 통해 제공하고 있으며, 경찰청에서는 정상적인 참고인의 출석 요구에 대해 등기우편과 이메일, 문자로 당사자에게 통보하고 있으므로 피싱(Phishing)으로 의심될 경우 지체 없이 경찰청에 전화로 직접 확인해 달라고 당부했다.

이스트소프트 알약 분석팀 이상희 팀장은 "전화를 통한 피싱은 최근 범죄 수법이 잘 알려져 경찰청 같은 신뢰도 높은 기관을 가장한 사회공학 기법의 피싱 및 악성코드 이메일 유포로 새롭게 진화하고 있다"며, "최근 G-20을 앞두고 업데이트 기능을 가진 악성코드를 통해 좀비 PC를 양산 시킬 가능성이 있으므로 출처가 불분명한 이메일에서 첨부파일은 절대로 실행하지 말고 알약 같은 최신 백신을 사용해 이를 예방해야 한다"고 강조했다.

'구버전 IE 제로데이 취약점' 악용한 표적 공격 경고

기업 특정인 대상 악성코드 심어진 웹페이지로 접속 유도

시만텍 보안 연구소가 마이크로소프트 윈도우 익스플로러 6 및 7에서 표적 공격(Targeted attack)에 사용되는

새로운 제로데이 취약점이 발견돼 사용자들의 주의가 요구된다고 밝혔다. 이번 취약점은 공격자들이 공격할 기업의 특정인들에게 이메일을 발송, 악의적인 웹사이트로의 접속을 유도해 악성코드를 설치하도록 만든다. 공격자들은 합법적인 웹사이트의 접근 권한을 획득한 후 소유자 몰래 악성코드가 포함된 특정 웹페이지를 심어둔 후 이메일에 해당 웹페이지로의 링크를 삽입해 접속을 유도한다. 이 링크에는 사용자의 웹브라우저와 운영체제 버전을 확인할 수 있는 스크립트가 포함되어 있기 때문에 해당 인터넷 익스플로러 6 및 7 사용자만을 골라 악성코드가 심어진 웹페이지로의 방문을 허용한다.

일단 해당 웹페이지에 접속하게 되면 부지불식간에 사용자의 컴퓨터로 악성코드가 다운로드되며, 이후 사용자 몰래 원격으로 실행시킬 수 있는 프로그램을 설치한다. 감염된 후 악성코드는 컴퓨터를 재구동 시킨 후 '넷웨어 워크스테이션(NetWare Workstation)'이란 서비스 명으로 구동된다. 또한 악성코드의 일부는 컴퓨터에 백도어를 설치한 후 폴란드에 있는 특정 원격 서버와의 연결을 시도해 .gif 확장자를 가진 소용량 파일들을 내려받는다. 이 암호화된 파일들은 트로이 목마가 이후 어떤 공격을 할 지 알려주는 명령어들을 포함한다. 시만텍은 처음 이 인터넷 익스플로러의 취약점을 발견했을 당시 '다운로더(Downloader)'로 분류했다가 이후 '다운로더 및 트로이 목마(Downloader and Trojan Horse)'로 명명했으며, 현재는 해당 취약점을 Backdoor.Pirpi로 명명하고 있다.

시만텍은 악성코드가 심어진 웹페이지를 호스팅하던 두 개의 웹사이트를 발견해 해당 소유자들에게 통보한 상태다. 하지만 아직까지 마이크로소프트에서 해당 문제점에 대한 패치를 발표하지 않은 상황인 만큼 시만텍은 해당 제로데이 취약점을 악용한 공격 시도를 주의 깊게 모니터링하면서 추가 정보가 확인되는 즉시 관련 내용을 공지할 예정이다. 시만텍은 마이크로소프트가 보안 패치를 배포하기 전까지 제로데이 공격에 대한 응급조치로 데이터실행방지(DEP) 기능을 활성화시키고, 인터넷 익스플로러 옵션창에서 인터넷 보안수준을 높게 설정하거나 액티브 스크립트의 사용을 제한해야 하며, 안티바이러스 프로그램을 최신버전으로 유지하고, 신뢰할 수 있는 웹사이트만 방문할 것을 권장하고 있다.

건강보험공단, 스마트폰 서비스에 공인인증 기술 적용

안전한 스마트 서비스 위해 '소프트포럼 제큐어스마트' 도입

국민건강보험공단(www.nhic.or.kr)이 공공기관 최초로 공인인증 기술을 적용함에 따라, 앞으로 국민들은 민원서비스, 건강정보, 병원·약국 찾기 등의 다양한 서비스를 스마트폰에서 보다 안전하게 이용할 수 있게 된다. 유비쿼터스 보안 전문기업인 소프트포럼(대표 김상철, www.softforum.com)은 국민건강보험공단 스마트폰 서비스에 스마트폰 통합보안 솔루션인 XecureSmart(이하 제큐어스마트)를 공급했다고 4일 밝혔다. 제큐어스마트는 본인 인증을 위한 스마트폰 보안 인증 모듈, 전자서명, 공인인증서 이동(중계), 본인인증을 무선 통신 구간 암호화를 함께 제공하는 스마트폰용 통합보안 솔루션이다. 특히 공인인증서 이동(중계) 기능 제공으로 제3의 공간에 머무르지 않고, 스마트폰으로 바로 이동될 수 있도록 하여 안전한 서비스를 이용하게 한다. 국민건강보험공단은 공공기관 최초로 공인인증 기술을 적용하여 개인 정보를 다루는 주요한 메뉴에는 공인인증서를 통해 본인 인증을 거쳐야만 사용이 가능하도록 보안 수준을 높였다. 또한 아이폰, 안드로이드폰, 윈도우모바일폰 등을 모두 지원하고 있다.

LG U+, DDoS 백본 차단 서비스 출시

인터넷 회선 고객인 전국 대학 및 시도교육청 대상 무상 제공

LG U+(부회장 이상철 / www.lguplus.com)는 인터넷 백본(Back-Bone)망에서 분산서비스거부공격(DDoS)을 사전에 탐지하고 차단할 수 있는 'DDoS 백본 차단 서비스'를 출시하고 고객망 보호를 위해 전국의 대학 및 시도 교육청 등에 무상으로 제공한다고 14일 밝혔다.

DDoS 백본 차단서비스는 LG U+의 인터넷 백본에 DDoS 탐지 및 차단장비를 설치하고 탐지된 DDoS 트래픽을 차단하여 고객망으로 정상적인 트래픽만을 전달하는 서비스이다.

LG U+는 전국의 대학 및 시도 교육청과 주요 기업 고객을 대상으로 DDoS 차단 장비를 구축하고 비상관제센터를 24시간 운영해 DDoS 발생을 실시간으로 감시한다. 또 고객의 인터넷 트래픽을 분석, 탐지하는 트래픽 분석 서비스와 고객의 NW 및 서버 장비의 보안 취약점을 진단하고 대응책을 리포트로 제공하는 취약점 점검서비스도 함께 제공할 계획이다. 현재 시범 서비스를 이용중인 광운대 관계자는 "DDoS 백본차단 서비스는 DDoS로부터 대학망을 보호하여 보안 및 인터넷의 품질 향상에 도움이 되고 있다"고 말했다.

LG U+는 현재 서울시내의 6개 대학을 포함, 수도권의 20여개 대학 및 기업에 서비스를 우선 적용하고 연말까지 전국의 대학 및 시도 교육청과 주요 기업 고객으로 서비스 범위를 확대할 계획이다.

개인정보보호 관리체계(PIMS) 인증제 도입

본격적인 인증 신청 및 심사는 2011년부터 수행 예정

방송통신위원회(이하 방통위)는 계속되는 개인정보 대량 유출 사고를 방지하고 기업의 사회적 책임을 강화하기 위한 일환으로 기업 스스로 고객의 개인정보를 보호할 수 있는 관리체계를 수립하여 지속적인 보호활동을 수행할 수 있도록 "개인정보보호 관리체계(PIMS: Personal Information Management System) 인증제" 도입을 의결하였다.

"개인정보보호 관리체계 인증제"란 개인정보를 취급하는 기업이 전사차원에서 개인정보 보호 활동을 체계적·지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 것으로, 고객의 개인정보 보호를 위해 필요한 법적인(정보통신망법 등) 요구사항을 포함한 총 3개 분야 119개 통제항목에 대한 점검 과정을 거치게 된다. 특히 인증제도의 신뢰성과 공정성 확보를 위하여 방송통신위원회가 인증제를 직접 관리·감독하고, 한국인터넷진흥원이 인증 신청 기업의 심사를 수행할 예정이다.

방통위 관계자는 "인증제도 도입으로 법률에 명시된 최소한의 보호대책만으로 개인정보 침해사고 방지에 어려움을 겪었던 기업들에게 체계적 개인정보 보호활동을 위한 세부 기준과 방법이 제시되었으며, 국민들에게는 개인정보를 안전하게 관리하는 기업을 객관적으로 식별할 수 있는 기준이 마련되었다는 점에서 의미가 크다"고 밝혔다. 또한 방통위는 12월 중에 사업자를 대상으로 인증제 설명회를 개최할 계획이며, 인증 신청 및 심사는 2011년부터 수행할 예정이다.

이글루시큐리티, 3D화면 이용한 보안관리기술 특허

신속하고 직관적인 보안관제 화면 구현, 즉각 대처 가능

융복합보안관리전문기업인 이글루시큐리티(대표 이득춘, www.igloosec.co.kr)는 '3차원 화면을 이용한 통합보안관리시스템' 기술에 대한 특허를 획득했다고 15일 밝혔다. 이글루시큐리티의 통합보안관리(ESM) 제품인 'SPiDER TM'과 융복합보안관제솔루션인 '라이거(LIGER)-1'에 적용된 이 기술은 3차원 화면을 이용해 언제, 어디서, 어떤 유형의 보안 이벤트가 얼마만큼의 빈도 수로 발생하는지 일목요연하게 표시하여 사용자가 직관적으로 인지하고 신속하게 대처할 수 있도록 한다. 기존의 보안 관제 화면의 경우 발생하는 보안이벤트 현황을 표나 그래프를 이용하여 표시하는 형태에 그쳐 수많은 보안이벤트가 발생하는 경우 보안담당자가 그 현황을 한번에 인지하기란 매우 어려웠으며 언제 어떤 유형으로 이벤트가 변화되는지 신속하고 직관적으로 인지하는데 한계를 갖고 있었다.

하지만 3차원 화면을 이용한 통합보안관리시스템은 신속한 대응을 할 수 있을 뿐 아니라 각 사이트의 보안장비에서 전송, 수집되는 보안 이벤트 데이터를 수집하여 저장하는 정보수집부, 저장된 데이터를 분류하고 처리하는 정보처리부, 정보처리부에서 분류된 데이터들을 3차원 화면으로 표시하는 정보표시부를 포함하고 있어 이용자가 보안침해상황에 즉각적이고 효율적으로 대처하는 것이 가능하다.

이글루시큐리티 R&D 부문장 이용균 전무는 "이미 국내 최초로 상용화 시킨 '3차원 화면을 이용한 통합보안관리시스템'은 보안이벤트가 발생한 국가, 발생시각, 유형 및 발생빈도, 보안 위험 알람 발생 상황을 표시하는 영역 등 발생하는 보안이벤트 통계정보가 영역화 되어 있다"며 "따라서 각 영역의 보안이벤트 정보들이 3D화면에 일목요연하게 표시되어 신속한 대응 처리는 물론 시스템 관리 및 유지비용 절감에도 효과가 있다"고 밝혔다.

KISA, 글로벌 모바일 스팸 방지 프로젝트 참여

세계 이동통신사업자협회와 협력, 모바일 스팸 문제 대응 위해

한국인터넷진흥원(KISA, 원장 서종렬)은 스팸 대응 국제 공조를 위해 '글로벌 모바일 스팸방지 프로젝트'에 참여한다고 18일 밝혔다. 세계 최대의 이동통신사업자협회인 'GSMA'가 주축이 되어 추진하고 있는 '글로벌 모바일 스팸방지 프로젝트'는 전 세계 주요 이통사가 자사의 가입자로부터 접수한 모바일 스팸정보를 취합하고, 이를 토대로 네트워크상에서 스팸의 유통량, 유형, 전송경로 등을 분석하여 결과를 다시 국가 간 공유하는 것이다. 프로젝트에 참여하는 기관·사업자는 전 세계 여러 나라들의 모바일 스팸에 관한 주요 현황과 최신 동향을 파악하여 스팸예방 및 대응에 활용할 수 있다.

동 프로젝트는 올해 3월부터 시범사업의 형태로 추진되어 왔으며, 그 동안 한국의 KT, 미국 AT&T, 캐나다 Bell Mobility, 프랑스 SFR이 참여해왔다. 이번에 KISA와 해외 타 이통사들의 신규 참여에 따라 참여기관의 수가 총 7개로 확대되었으며, GSMA는 내년 중 프로젝트를 정식 사업화하여 더 많은 이통사 등에게 확대 서비스할 계획이다. 또한, 이용자가 수신한 스팸을 휴대전화 상에서 간단한 메뉴버튼 조작만으로 신고할 수 있는 KISA의 '간편신고 서비스'가 향후 GSMA의 '스팸신고 가이드라인'에 신고방식의 하나

로 반영되어 국제공조를 위한 논의에서 주도권을 확보할 수 있는 기회가 될 것으로 전망되고 있다.

GSMA의 정보보호 책임자 제임스 모런(James Moran)은 "GSMA의 프로젝트가 전 세계적으로 점차 심화되고 있는 모바일 스팸 문제의 해결을 위한 중요한 요소가 될 것"이라며, "KISA가 정부기관으로서는 처음으로 프로젝트에 참여하게 된 것을 무척 기쁘게 생각하며 좋은 선례가 되기를 바란다"고 밝혔다.

* GSMA(세계이동통신사업자협회) : 이동통신 분야에서 규모와 영향력이 가장 큰 사업자 단체로, 219개국의 800여개 이통사 및 200여개 단말기 제조사가 참여하고 있으며, 이동통신 산업의 트렌드 및 방향 결정 등 다양한 분야에서 상호협력을 도모함.

방통위, 개인정보보호 포털 사이트 운영

개인정보 정책, 법제도, 교육 등 개인정보보호 관련 정보 제공

방송통신위원회(이하 방통위)와 한국인터넷진흥원은 개인정보 정책, 법제도, 교육 등 개인정보보호 관련 모든 정보를 쉽게 하나의 사이트에서 얻을 수 있는 '개인정보보호 포털 사이트(www.i-privacy.kr)'를 구축·운영한다고 밝혔다. 개인정보보호 포털 사이트는 이용자와 사업자에게 개인정보보호를 위한 정부 정책, 동향 등 각종 정보를 제공하며 여태까지 여러 사이트에서 분산 제공 되었던 개인정보에 관한 다양한 정보들을 하나의 사이트에서 이용할 수 있도록 한 것이 장점이다. 또한 이용자와 사업자의 커뮤니티를 운영할 수 있도록 하여 개인정보에 대한 양방향적 의사소통을 가능하게 하였으며, 개인정보취급자 대상의 온라인 교육을 제공하여 수료증을 발급받을 수 있는 시스템을 구축하였다. 개인정보보호 포털사이트는 크게 '알리미'(개인정보보호 동향, 법령 등 소개), '지키미'(개인정보보호 정책 및 방법 소개), '배우미'(온라인교육), '나누미'(개인정보보호 커뮤니티), '자료실' 메뉴로 구성되어 개인정보에 관한 종합적인 정보를 제공한다.

방통위는 "개인정보보호 포털 중 특히 온라인 교육은 개인정보 분야의 여러 전문가가 강의하는 형태로 플래시 동영상과 접목시켜 실질적인 교육의 효과를 높였으며 개인정보보호에 대해 쉽게 이해할 수 있도록 실제적인 사례 등을 위주로 구성하였다"고 밝히고 "앞으로도 일반 이용자 및 중·소규모 사업자에게 도움이 되도록 온라인 교육을 계속적으로 확대하고 포털 사이트를 이용한 지속적인 교육과 홍보를 통해 국민들의 개인정보가 더욱더 안전하게 보호될 수 있는 기반을 다져나가겠다"고 말했다.

소셜 미디어 겨냥한 피싱 사이트 급증

전월 대비 80% 증가, 개인정보 입력 시 각별한 주의 요구

시만텍(www.symantec.co.kr)이 전세계 스팸 및 피싱 동향을 조사 분석한 '시만텍 월간 스팸 및 피싱 현황 보고서' 11월호에 따르면, 10월 한 달 간 전체 메일 중 스팸이 차지하는 비중은 86.61%로 지속적인 감소세를 보였으며, 전세계 스팸 양도 전월 대비 22.5%, 지난 8월과 비교하면 무려 47%나 감소한 것으로 나타났다. 이는 지난 2009년 9월 이래 가장 낮은 수치이다.

시만텍은 이처럼 전세계 스팸 물량이 감소한 원인으로 지난 9월 러시아의 '스팸잇닷컴(SpamIt.com)' 사이트 폐쇄와 최악의 사이버 범죄로 불리는 '제우스(Zeus)' 관련 범죄조직의 검거를 꼽았다.

전세계 스팸 양이 줄어들고 있는 가운데 주목할 점은 소셜 미디어를 겨냥한 피싱이 증가하고 있다는 점이다. 소셜 미디어의 인기가 높아지면서 지난 10월 소셜 미디어를 겨냥한 피싱 사이트 숫자는 전월 대비 무려 80%나 증가했으며, 피싱 공격용 자동화 툴킷으로 생성된 피싱 웹사이트도 41%나 증가한 것으로 나타났다.

소셜 미디어 피싱 웹사이트의 대부분은 전세계적으로 큰 인기를 얻고 있는 2개의 소셜 네트워킹 서비스(SNS) 브랜드를 사칭하고 있었다. 이처럼 SNS가 사이버 범죄자들에게 강력한 공격 매개체로 인기를 끌고 있는 이유는 SNS가 온라인 범죄활동에 가장 좋은 표적이 되는 사용자 수와 사용자 간의 높은 신뢰도 등 두 가지 요건을 모두 충족해 SNS를 통해 악성 코드나 악성 링크를 손쉽게 퍼뜨릴 수 있기 때문이다. 또한 친구, 지인 간의 친밀한 인간관계로 이어지는 SNS의 특성상 사용자들이 피싱 메시지에 대한 의심이 다소 느슨하다는 점 역시 공격 증가의 주요 원인으로 분석된다.

시만텍은 SNS에 대한 공격 유형으로 ▲가짜 초대: SNS의 인지도를 이용, 가짜 초청장을 개발해 사용자들에게 메시지를 발송, 악의적인 스팸 웹사이트로 유도 ▲계정 통합: 알림 메시지를 사칭해 사용자에게 계정 통합을 내세워 개인 정보 탈취 ▲사진 관련 댓글: 합법적인 SNS 웹사이트의 사진 관련 댓글 알림창을 만들어 사용자에게 전송하고 메시지 상의 URL 링크를 클릭해 스팸 웹사이트로 이동하도록 유도 ▲애플리케이션 정보: SNS 웹사이트에서 제공되는 인기 게임 등의 정보를 알려준다고 위장 ▲악성코드 유포: 악성코드를 퍼뜨리기 위한 다양한 스팸 메시지 등장. 일례로 SNS 툴바 다운로드 안내 메시지로 가장한 트

로이목마 바이러스가 탐지되기도 함 ▲개인 사생활보호 및 보안 업데이트: 개인 사생활보호를 위해 개인정보 관리 실태에 대한 조사가 필요하다고 속이며 개인정보 요구 ▲가짜 설문조사: SNS 사용자 대상 설문조사로 위장한 메시지를 통해 사용자들에게 개인 정보 공유를 요청하거나 스팸 웹사이트로의 방문 유도 등을 들었다.

시만텍코리아의 윤광택 이사는 "소셜 미디어가 생활의 일부로 자리잡으면서 소셜 미디어 및 그 이용자들이 새로운 피싱 공격 대상으로 떠오르고 있다"며, "소셜 미디어를 겨냥한 대부분의 피싱 웹사이트들은 합법적인 사이트처럼 감쪽같이 위장해 한눈에 식별하기 어려운 만큼 소셜 미디어 관련 개인 정보 입력시 이용자들의 각별한 주의가 요구된다"고 당부했다.

2011년 주목해야 할 보안 트렌드

주요 인프라 겨냥한 사이버 공격 증가

스턱스넷은 의도적으로 하드웨어 시스템이 오작동을 일으키도록 설계된 가장 대표적인 컴퓨터 바이러스다. 스턱스넷의 등장으로 주요 인프라를 겨냥한 공격이 얼마나 큰 충격과 피해를 야기할 수 있는지 깨닫게 된 사이버 테러리스트들은 2011년에 주요 인프라를 대상으로 유사한 추가공격을 감행할 것으로 전망된다. 공격의 시작은 더디겠으나, 빈도는 계속해서 증가할 것으로 보인다.

최근 시만텍이 한국을 포함한 전세계 15개국에서 핵심 기간 인프라를 공급하는 1,580개 기업을 대상으로 조사한 '핵심 기간 인프라 보호 현황(Critical Infrastructure Protection Survey)' 보고서도 이 같은 전망을 뒷받침한다. 설문 응답자의 48%가 내년에도 사이버 공격을 받을 것으로 예상했으며, 80%는 공격 빈도가 증가할 것이라고 답했다. 주요 인프라 제공업체들은 이러한 공격 위험을 잘 인지하고 있으며, 주요 인프라 보안을 최우선 과제로 삼고 있는 것으로 나타났다.

1. 표적 공격과 제로데이 취약점 이용 공격 증가

올해 초 특정 조직 또는 특정 컴퓨터 시스템을 겨냥했던, 이른바 오로라(Aurora)로 알려진 하이드락(Hydraq) 공격은 소프트웨어의 잘 알려지지 않은 제로데이 취약점을 악용한 표적 공격의 한 예로, 그 위험 수위가 지속적으로 높아지는 상황이다. 사이버 공격자들은 수년간 다양한 보안 취약점을 악용해 왔으나 2011년에는 이러한 경향이 더욱 가속화되면서 제로데이 취약점을 악용한 표적 공격이 이전보다 훨씬 더 많이, 자주 등장할 것으로 예상된다.

2009년 시만텍은 총 12건의 제로데이 취약점 공격을 탐지했지만 2010년에는 11월 기준으로 사이버 공격에 이미 사용되었거나 활발히 사용되고 있는 18건의 제로데이 취약점을 발견했다. 이 중 이번 달에 확인된 하이드락, Sykipot, Pirpi 등을 포함해 절반 이상은 표적 공격에 사용된 것으로 나타났고, 특히 스턱스넷은 동시에 4개의 제로데이 취약점을 이용한 것으로 확인됐다. 이처럼 특정 표적 공격시 제로데이 취약점을 악용하는 가장 큰 이유는 표적 공격용 악성코드가 소수의 공격 대상만을 노리기 때문이다.

은밀히 소수의 대상만을 노리는 표적 공격이 증가함에 따라 기존 시그니처 기반의 탐지 방식으로는 이 같은 보안 위협에 대응하기가 사실상 불가능해졌다. 따라서 향후에는 보안위협의 행위(Behavior)에 기반한 탐지 기술인 시만텍의 SONAR 및 평판기반의 보안(Reputation-Based Security)과 같은 신기술을 통해 표적 공격을 포함한 새로운 보안 위협에 적극 대응할 필요가 있다.

2. 스마트 기기의 증가로 새로운 IT 보안 모델 등장

모바일 기기의 활용도가 증가하면서 2011년에는 모바일 기기와 그 이용자들을 겨냥한 사이버 공격이 본격화 될 전망이다. 특히 오늘날의 모바일 기기는 공격의 타깃일 뿐만 아니라 악성 코드의 배포 매개체로 활용될 수 있어 각별한 주의가 요구된다. 모바일 기기의 활용도가 급증함에 따라 기업들은 모바일 기기를 안전하게 사용하고, 기기에 담긴 민감한 정보를 효과적으로 보호하기 위한 새로운 보안 모델을 필요로 하고 있다. 특히 모바일 기기를 통해 점점 더 많은 개인 및 기업 업무를 수행함에 따라 IT 조직, 소비자 및 통신사업자 모두 복잡한 정보 보안 및 관리과제에 직면하고 있다. 다수의 이용자를 확보한 모바일 플랫폼이 시장을 주도하게 되면 2011년에는 특정 OS를 탑재한 모바일 기기를 겨냥한 공격이 증가할 것으로 예상된다. 시만텍을 비롯한 보안 솔루션 업계는 이미 모바일 보안 위협의 증가세를 인지하고 있으며, 모바일 분야 전문업체인 '모카나(Mocana)'의 설문조사 결과 응답 기업의 65%가 모바일 기기를 겨냥한 보안 공격이 IT 담당자의 지속적인 관심을 끌 것으로 내다봤다.

3. 컴플라이언스 준수 위한 암호화 기술 도입 증가

기업의 모바일 기기 사용 급증으로 인해 기기를 안전하게 사용하고, 기기에 저장된 데이터의 안전한 사용과 보안을 위해 기업들은 다양한 데이터 보호 및 프라이버시 법규를 준수해야 한다. 실제 기업이 준수해야 하는 규제가 다양해지면서 기업은 많은 압력을

받고 있다. 지난해 미국은 정보보호를 위한 의료법 'HITECH(개인의료정보보호 관련 법안)'를 제정하였고, 몇몇 주에서도 정보보호를 위한 법률을 제정했다. 또한 전 세계적으로 PCI DSS(지불카드용 데이터 보안 표준)가 2.0 버전으로 업데이트되었다. 많은 법적 규제에도 불구하고 대다수 조직들은 노트북 분실은 보고하면서도 중요한 데이터가 들어 있는 모바일 기기 분실은 공개하지 않는 경우가 많다. 2011년에는 이러한 이슈에 대해 조치가 취해질 것으로 예상되며, 이에 따라 기업들은 모바일 기기를 중심으로 암호화 기술 도입을 크게 늘릴 것으로 보인다. 2011년 기업들은 암호화 기술을 통해 데이터 보호를 위한 더욱 선제적인 조치를 취할 것으로 예상되며, 이를 통해 컴플라이언스 요건을 충족하고, 데이터 유실에 따른 브랜드 피해를 최소화할 것이다.

4. 정치적 의도를 지닌 새로운 보안 위협의 대두

시만텍의 '핵심 기간 인프라 보호 현황' 보고서에 따르면 조사대상 기업의 절반 이상이 자신들이 경험한 사이버 공격에 특정 정치적 의도가 있었다고 답했다. 과거 이러한 정치적 의도를 지닌 공격은 대부분 사이버 스파이 활동이나 웹 서비스 대상의 서비스 거부 공격이 주를 이뤘다. 그러나 이제 사이버 공격은 단순 스파이 게임이나 교란 성격을 넘어 실제적인 물리적 타격을 입히는 공격으로 발전할 전망이다. 특정 산업제어시스템으로 관리되는 시설을 조작함으로써 실제적인 물리적 타격을 입히는 스턱스넷이 대표적인 예다. 스턱스넷은 매우 복잡한 위협으로 산업제어시스템을 재프로그램하는 것이 목적이다. 즉, 발전소, 정유사 및 가스 파이프라인 등 기간산업을 관리하는 프로그램을 표적으로 삼는다. 아직까지 스턱스넷의 실제 표적은 알려지지 않았으나, 정황상 충분한 자금을 받은 그룹 또는 국가가 정치적인 의도로 악성 코드를 생성하여 이란 또는 이란 내 특정 조직이나 시설을 공격한 것으로 추정된다. 시만텍은 스턱스넷이 사이버 전쟁을 촉발하기 위한 그간의 여러 시도 중 단지 처음으로 포착된 징후이며, 2011년에는 사이버 전쟁을 염두에 둔 더 많은 징후가 포착될 것으로 전망하고 있다.

내년 4월 공인인증서 암호체계 고도화 추진

은행 · 정부 등 전자거래사이트, 공인인증서 SW 업그레이드 필요

한국인터넷진흥원(KISA, 원장 서종렬)은 행정안전부의 공인인증서비스 안전성 강화 조치에 따라 2011년 4월 1일부터 보안 기술이 강화된 새로운 공인인증서를 발급하는 공인인증서 암호체계 고도화를 추진한다고 밝혔다. 이번 조치로 인해 새로 발급되는 공인인증서는 2,048비트의 전자서명키(현행 1,024비트)가 사용되고 전자문서 축약에도 256비트(현행 160비트) 출력값을 가지는 새로운 해쉬(hash) 함수가 사용된다. 이는 실생활에서 인감도장의 직인 모양을 보다 정교하게 만들어 인감도장의 복제를 원천적으로 불가능하게 만드는 것과 유사한 원리이다. 신규 공인인증서가 발급되더라도, 일반 국민들은 별다른 불편없이 기존 공인인증서를 유효기간 만료일까지 그대로 사용할 수 있으며, 공인인증서의 유효기간이 만료되어 갱신 또는 재발급 받는 시점에 새로운 공인인증서로 교체되어 발급된다. 다만, 공인인증서를 이용하는 금융회사(은행, 증권, 보험 등), 전자정부, 공공기관, 기업 등의 웹 사이트에서는 고도화된 신규 공인인증서를 처리할 수 있도록 사전에 기존 공인인증서 SW를 업그레이드 하여야 한다. 국인터넷진흥원 서종렬 원장은 "암호체계 고도화는 우리나라 뿐만 아니라 미국 등 전 세계적으로 진행되는 사안으로, 금번 고도화 조치를 통해 공인인증서는 2030년까지 세계 최고 수준의 안전성을 담보할 수 있다"며, "현재, 5개 공인인증기관, 전문보안업체에서 공인인증서 SW 업그레이드를 위한 기술지원을 진행 중이기 때문에, 전자거래업체(기관)에서는 일정 내에 공인인증기관이나 전문보안업체와 협의하여 기술지원을 받을 것"을 당부했다.

기업 모바일 보안 및 관리를 위한 7계명

시만텍, 기업 네트워크에 모바일 기기 도입 시 보안 수칙 제시

시만텍(www.symantec.co.kr)이 엔터프라이즈 환경에서 과도한 비용이나 위험 부담 없이 효과적으로 모바일 기기를 도입하고, 모바일 상의 정보를 보호 및 관리하기 위한 '7가지 모바일 보안 및 관리 수칙'을 발표했다. 모바일 기기는 휴대성이 뛰어나고 대용량 데이터를 저장할 수 있으며, Wi-Fi, 블루투스, 적외선 및 다양한 모바일 통신 표준을 통해 단말기 및 네트워크에 연결된다. 모바일 기기의 활용이 기업의 업무환경 및 생산성 향상에 기여하는 바가 크지만 그로 인한 분실 및 도난의 위험이 높아졌고, 고기능의 대용량 스토리지를 탑재하고 있기 때문에 기업 정보의 유출 위험 또한 증가하고 있는 상황이다.

시만텍은 기업들이 모바일 기기를 '기업 네트워크 상의 개인소비자 디바이스'에서 '기업 네트워크에 연결된 또 하나의 엔드포인트'로 전환할 수 있도록 돕기 위한 '7가지 모바일 보안 및 관리 수칙'을 제시했다.

1. 모바일 기기의 가시성 확보

모바일 기기 재고 조사를 필두로 한 자산 관리는 모바일 인프라 정의, 보호 및 관리를 위한 중요한 첫 단계이다. 가시성을 확보하기 위해서는 다양한 네트워크 상에서 모바일 기기를 보호할 필요가 있다. 또한 모델, 시리얼 번호 및 기타 모바일 기기에 관한 정보뿐만 아니라 현재 보안 소프트웨어 및 OS 패치 버전에 대한 검사를 실행해야 한다.

2. 다계층 보안 기능 적용

모바일 기기는 기본적으로 휴대형 컴퓨터이기 때문에 기업 엔드포인트에 적용하고 있는 것과 동일한 다계층 보안 기능을 필요로 한다. ▲모바일 기기가 연결된 네트워크 종류에 상관없이 포트와 프로토콜 별로 기기 및 콘텐츠를 보호하기 위한 방화벽 ▲MMS, 적외선, 블루투스, 이메일 등 다양한 공격 루트를 포함한 안티바이러스 ▲시그니처가 아직 배포되지 않은 제로데이 공격을 차단하기 위한 휴리스틱 및 침입방지, 보안 공격의 진행상황을 알려주는 사용자 및 관리자 경고 등 실시간 보호기능 ▲증가하고 있는 SMS 스팸 문제 해결을 위한 안티스팸 등의 기능이 적용되어야 한다.

3. 하드웨어 플랫폼 및 운영체제와 동일한 관리

모바일 기기 역시 엔드포인트이다. 따라서 모바일 기기의 보안 및 관리 기능은 기업의 보안 및 관리 시스템 내에 통합되어 동일하게 관리해야 한다. 이때 운영 효율성을 높이고 기업 인프라상에서 일관된 보안 정책을 적용하기 위해서는 호환되는 솔루션을 사용해야 하는 것이 이상적이다. 심비안, 윈도우 모바일, 블랙베리, 안드로이드, 아이패드, 아이폰 OS나 향후 출시될 OS에 상관없이 동일한 보안정책을 적용해야 한다. 노트북에 최신 엔드포인트 소프트웨어가 필요한 것처럼 보안정책을 따르지 않은 휴대전화는 검사가 끝날 때까지 또는, 필요시 패치, 업그레이드 혹은 복구작업이 완료될 때까지 네트워크 접근을 거부해야 한다.

4. 분실 및 도난에 대비한 암호화 필수

모바일 기기에서 분실 및 도난은 큰 위험에 속한다. 비즈니스위크에 따르면 미국에서만 2억8,500만대의 휴대폰이 사용되고 있는데 이 중 3,000만대가 매년 '사라진다'고 한다. 도둑이나 해커가 장기간 휴대폰을 물리적으로 소유하고 있을 때 비밀번호는 안전한 보호장치가 되지 못한다. 따라서 연락처뿐만 아니라 이메일 및 이메일 첨부파일 등 휴대폰 데이터에 관한 보호장치가 마련되어야 한다.

5. 모바일 기기 상의 기밀 정보 보호

모바일 기기에 저장되어 있거나 모바일 기기를 통해 접근 가능한 기밀 데이터가 유출되면 직접적인 매출 하락과 복구비용은 물론 장기적인 고객 및 브랜드 충성도 감소 등의 결과를 초래할 수 있다. 데이터 유출 및 사이버공격은 네트워크의 가장 취약한 지점에서 발생하는 만큼 기업 네트워크 환경에서 데이터손실방지(DLP) 기술을 채택하는 경우 반드시 그 대상을 모바일 기기까지 확대할 필요가 있다.

6. 보안 및 관리 통합

네트워크에 연결된 모바일 기기 검색, 패치상태 확인, 취약성 검사 외에도 보안 수준을 향상시키기 위해서는 엄격한 관리가 요구된다. 이를 위해서는 ▲운영체제, 보안 애플리케이션 안티바이러스 시그니쳐 및 안티스팸 데이터에 대한 자동 업데이트 기능 ▲네트워크 종류에 상관없는 원격 설정 및 정책 이행· 향후 데이터손실방지로 범위 확대 ▲도난 시 디바이스 사용을 정지시키고 기밀 정보가 노출되기 전에 데이터를 제거하는 원격 잠금 및 삭제기능 ▲확장된 기업 네트워크 상에서 폐쇄형 보안을 제공하고 모바일 기기 위협을 감시하는 이벤트 로깅 기능 등이 필요하다.

7. 기업규모에 맞춰 확장 가능한 관리 능력

모바일 기기를 겨냥하거나 모바일 기기를 통해 발생하는 보안 위협은 개인 소비자, 중소기업 및 대기업 모두에 동일하다. 기기별 보안 관리는 개인 소비자에 적절한 방법이지만, 기업규모가 커질수록 자동화된 정책기반의 보안 및 관리가 필요하다. 따라서 모바일 보안 및 관리 솔루션 제공업체는 소기업에서 대규모 통신사업자에 이르기까지 기업고객의 비즈니스 성장에 발맞춰 규모를 확대할 수 있는 능력을 갖춰야 한다.

시만텍코리아의 정경원 사장은 "기업의 업무 환경에서 모바일 기기 활용이 갈수록 증가하고 있는 만큼 모바일 기기의 효율적인 도입과 이에 대한 보호 및 관리 전략은 기업의 최우선 과제가 된 상황"이라며, "시만텍의 폭넓은 모바일 보안 및 관리 솔루션을 통해 고객들은 개인 및 기업 정보를 안전하게 유지하면서 모바일 기기를 효율적으로 보호 및 관리할 수 있을 것"이라고 강조했다.

트위터 가짜 단축 URL 조심하세요!

URL 클릭 시 악성코드 삽입된 웹사이트로 사용자 유도

시만텍 보안 연구소는 인기 소셜네트워킹서비스(SNS)인 트위터(Twitter)에서 단축 URL을 악용한 보안 위협이 늘고 있어 트위터 사용자들의 주의가 요구된다고 밝혔다. 140자로 글자 수가 제한되어 있는 트위터의 경우, 긴 URL을 짧게 줄여서 올리는 단축 URL이 널리 사용되고 있다. 트위터 메시지에서 자주 접하게

되는 'http:// bit.ly/****' 등의 URL이 바로 단축 URL의 예. 최근 트위터 상의 단축 URL을 가짜 단축 URL로 바꿔서 사용자들을 악성코드가 삽입된 웹사이트로 유도하는 사례가 빈번히 발생해 사용자들의 피해가 늘고 있다. 특히, 트위터에 리트윗(RT) 등을 통해 올라오는 메시지들의 경우 동일 텍스트가 반복되기 때문에 메시지에 삽입된 URL이 바뀌어도 사용자는 큰 의심없이 가짜 단축 URL을 클릭하게 된다. 이렇게 연결되는 가짜 웹사이트는 외관상 합법적인 웹사이트의 형태를 띄고 있지만 드라이브바이다운로드(drive-by download) 방식으로 사용자 모르게 악성코드를 PC에 설치하기 때문에 더욱 위험하다.

시만텍은 트위터 가짜 단축 URL로 인한 피해를 최소화하기 위해 사용자들이 보안 소프트웨어를 설치하고 브라우저를 포함해 컴퓨터와 소프트웨어를 최신 상태로 업데이트하는 한편, 트위터의 단축 URL을 섣불리 클릭하지 않는 등 인터넷 사용시 일반적인 보안 수칙을 준수할 것을 권고하고 있다.

기타 트위터 가짜 단축 URL 보안 위협에 대한 보다 자세한 정보는 시만텍 보안 블로그 포스팅(http://www.symantec.com/connect/blogs/turning-good-news-bad-news)을 통해 확인 할 수 있다. 한편, 트위터는 단축 URL을 펼쳐서 보여주는 '확장(Expand)' 기능을 도입해 실제로 링크를 클릭하기 전에 연결되는 페이지를 확인할 수 있도록 지원하는 작업을 진행하고 있다.

신종 랜섬웨어 바이러스 확산 경보

감염된 컴퓨터의 데이터 손상 또는 결제 요구

콘텐츠 보안 업체인 카스퍼스키 랩은 악성 프로그램에 감염된 컴퓨터의 데이터를 손상시키는 매우 위험한 신종 랜섬웨어(Ransomware) 바이러스 두 가지에 대한 긴급경보를 발령했다. 첫 번째 악성 프로그램은 악명 높은 GpCode 트로이 목마의 새로운 변종으로 Trojan-Ransom.Win32.GpCode. ax로 명명됐다. 이 악성 프로그램은 Adobe Reader, Java, Quicktime Player, Adobe Flash의 취약점을 이용하여 감염된 웹사이트를 통해 확산되고 있다. 일단 감염이 되면 doc, docx, txt, pdf, xls, jpg, mp3, zip, avi, mdb, rar, psd 등의 다양한 확장자를 가진 파일들을 사용자의 동의 없이 암호화(RSA-1024와 AES-256 알고리즘 사용) 한 후 데이터 복구 소프트웨어로 복구하지 못하도록 원본 데이터를 덮어쓰기하는 게 특징이다.

두 번째 신종 랜덤웨어 바이러스는 컴퓨터의 MBR을 감염시키는 트로이목마다. 드로퍼 역할을 하는 Trojan- Ransom.Win32.Seftad.a와 MBR을 감염시키는 Trojan- Ransom.Boot.Seftad에 감염이 되면, 컴퓨터의 부트 영역을 덮어쓰기 하며, 컴퓨터 사용자에게 MBR 복구를 위한 암호를 얻기 위해 결제하도록 요구한다. 만일 사용자가 잘못된 암호를 세 번 입력되면 감염 컴퓨터를 강제로 재부팅하고 결제를 계속 요구하는 게 특징이다.

카스퍼스키 랩은 "신종 랜섬웨어 바이러스 모두를 자사의 안티 바이러스 데이터베이스에 추가했다. 따라서 최신 업데이트를 적용한 카스퍼스키 랩 제품 사용자들은 이 신종 랜섬웨어 바이러스로부터 안전하다"며 "카스퍼스키 랩은 관련 취약점을 해결하기 위해 컴퓨터에 설치된 타사 프로그램들도 정기적인 업데이트할 것을 권장한다"고 강조했다.