IBM X-Force 2011년
동향 및 위험 보고서

2012년 3월

도움 주신 분들

X-Force 동향 및 위험 보고서는 IBM에서 일하는 모든 직원들의 공조를 통해 얻은 결실입니다.
이 보고서 발간을 위해 깊은 관심과 헌신을 마다 않은 다음 분들께 심심한 감사를 드립니다.

도움 주신 분	직함
Bryan Casey	IBM 보안 시스템, 마케팅 책임자
Carsten Hagemann	컨텐츠 보안 담당, X-Force 소프트웨어 엔지니어
Colin Bell	IBM 보안 시스템, 서비스 및 지원 담당, 보안 솔루션 설계자
Clay Blankenship	사고 대응 분석 선임 연구원
Cynthia Schneider	정보 개발자
David McMillen	IBM 보안 서비스, 보안 정보 분석가
David Merrill	CISA, IBM 최고 정보 보안 책임자, STSM
Dr. Jens Thamm	컨텐츠 보안, 데이터베이스 관리자
Dr. Ashok Kallarakkal	제품 관리 및 베타 테스트 사업, 선임 부장
Gina Stefanelli	X-Force 마케팅 책임자
Jason Kravitz	IBM 보안 시스템 및 온라인 구성 도구 기술 전문가
John C. Pierce	MSS 수석 위험 분석가
John Kuhn	IBM 보안 서비스, 보안 정보 분석가
Kimberly Madia	InfoSphere Guardium & Optim, 데이터 보안 전략가
Leslie Horacek	X-Force 위협 대응 관리자
Marc Noske	컨텐츠 보안, 데이터베이스 관리자

도움 주신 분	직함
Mark E. Wallis	IBM 보안 시스템, 정보 개발 수석
Marne Gordan	IBM 보안 시스템, 규제 분석가
Michael Applebaum	Q1 Labs 제품 마케팅 책임자
Michael Montecillo	MSS 위협 연구 및 정보 총책
Michelle Alvarez	MSS 국제 사업부장
Paul Sabanal	X-Force 고등 연구원
Phil Neray	IBM 보안 시스템, Q1 Labs 마케팅 책임자
Ralf Iffert	X-Force 컨텐츠 보안 관리자
Randy Burton	사고 대응 분석 선임 연구원
Robert Lelewski	사고 대응 분석 선임 연구원
Ron Black	사고 대응 분석 선임 연구원
Ryan Berg	클라우드 보안 전략 수석
Scott Moore	X-Force 소프트웨어 개발자 겸 X-Force 데이터베이스 팀장
Shane Garrett	X-Force 고등 연구 팀장
Tom Cross	X-Force 전략 및 위협 정보 관리자
Veronica Shelley	IBM 보안 시스템, 세그먼트 마케팅 책임자

X-Force란?

IBM X-Force® 연구개발팀은 취약점, 악용 및 적극적 공격, 바이러스 및 기타 악성코드, 스팸, 피싱, 악성 웹 컨텐츠 등의 최근 위협 동향을 연구 및 모니터링합니다. X-Force는 고객과 일반 대중에게 새로운 주요 위협에 대해 경고하고 IBM 고객을 이러한 위협으로부터 보호하기 위해 보안 컨텐츠를 제공합니다.

IBM 보안 협업

IBM 보안은 광범위한 보안 역량을 제공하는 여러 브랜드를 나타냅니다.

- X-Force® 연구개발팀은 최근 동향과 공격자의 수법을 분석하느라 여념이 없으며, IBM의 다른 조직은 X-Force® 연구개발팀의 분석 데이터를 이용하여 고객을 위한 보호 기술을 개발하는 데 주력합니다.
- X-Force® 연구개발팀은 다양한 컴퓨터 보안 위협 및 취약점을 발견하고 분석하며 감시하고 기록합니다.
- IBM MSS(Managed Security Service) 는 엔드포인트, 서버(웹 서버 포함) 및 일반 네트워크 인프라와 관련한 악용 행위 감시 업무를 담당하고 있습니다. MSS는 인터넷뿐 아니라 이메일 및 인스턴트 메시지와 같은 다른 분야에서 이뤄지는 악용 사례를 추적합니다.
- IBM PSS(Professional Security Service) 는 효과적인 정보 보안 솔루션을 구축할 수 있도록 전사적 보안 평가, 설계 및 설치 서비스를 제공합니다.
- IBM X-Force® 컨텐츠 보안 팀은 크롤링(crawling) 및 자체 조사를 통해, 혹은 MSS가 제공하는 정보를 활용하여 인터넷을 독자적으로 조사하고 안전 수준을 분류합니다.
- IBM은 지난 수년 간 실시한 IBM AppScan® OnDemand Premium Service의 보안 테스트에서 얻은 실세계의 취약점 데이터를 분석해왔습니다. 이 서비스는 IBM AppScan에서 수동 보안 테스트 및 검사를 통해 얻은 애플리케이션 보안 평가 결과를 취합한 것입니다.
- IBM 보안 서비스는 두 가지 방법, 즉 보안 전문 지식을 제공함으로써 클라우드를 도입하려는 고객을 돕는 클라우드 보안 서비스, 그리고 비용과 복잡성을 최소화하고 보안 능력을 개선하여 규제 요건을 충족하는 데 효과적인 클라우드 기반 모델의 보안을 통해 클라우드를 지원합니다.
- IBM ID 및 액세스 관리 솔루션은 승인 받은 사용자의 ID 프로파일 및 액세스 권한 관리를 효율적으로 중앙 집중화 및 자동화하는 데 효과적입니다. 이 솔루션은 사용자 액세스 현황을 모니터링할 수 있는 강력한 인증, SSO 및 감사/보고 도구로 보안을 강화합니다.
- IBM 데이터 및 정보 보안 솔루션은 데이터를 보호하고 액세스를 관리하는 기능을 제공하므로 기업 전체의 정보 수명 주기 보안 문제를 해결하는 데 유용합니다.
- IBM InfoSphere® Guardium® 은 최소 자원으로 데이터베이스 보안 및 규정을 신속하게 배치 및 관리할 수 있고 확장이 용이한 기업용 솔루션입니다.
- IBM 계열사인 Q1 Labs가 개발한 QRadar Security Intelligence Platform은 SIEM, 로그 관리, 구성 관리 및 이상 징후 감지용 통합 솔루션입니다. 이 솔루션은 사람, 데이터, 애플리케이션 및 인프라와 관련된 보안 및 규정 위반 위험을 실시간으로 확인할 수 있는 통합 대시보드를 제공합니다.

목차
단원 1

목차
단원 2, 3, 4

단원 1
위협

이 단원에서는 위협과 관련된 주제를 살펴보고 기업 보안 전문가들이 접하는 공격에 대해 알아봅니다. 또한 IBM이 관리하는 범위 내에서 관측된 악성 활동을 설명하고 이러한 위협으로부터 네트워크를 보호하기 위해 IBM이 어떻게 대응하고 있는지 소개합니다. 또한 IBM이 파악한 최근 공격 동향에 대해 새로운 정보를 제공합니다.

개요

IT 보안 측면에서 2011년은 특별한 한 해였습니다. 데이터 유출 사고, DoS 공격 및 사회적 핵티비즘(hacktivism)이 빈번히 보고됐던 2011년 중반 무렵 IBM은 2011년을 '보안 침해의 해'로 선언한 바 있습니다. 2011년 말까지도 이런 사고의 빈도와 범위가 좀처럼 줄어들 기미를 보이지 않자 갈수록 긴밀하게 연결되는 세상에서 기업을 운영하면서 자산을 보호할 기본적인 자구책이 필요하다는 의식이 꾸준히 확대됐습니다. 2011년 동안 세간의 이목을 집중시킨 다수의 대규모 사고는 경영진과 기업 지도자들이 기업의 기존 구조, 정책 및 기술의 효과를 재평가하도록 하는 촉매제가 됐습니다.

아무리 큰 난제가 도사리고 있더라도 교훈을 얻어 상황을 개선할 기회가 찾아오기 마련입니다. 침해 사고가 발생했을 때 기업은 사고 발생 사실과 고객에게 미칠 수 있는 영향은 공개하지만 사고가 발생한 경위와 어떻게 이를 막을 수 있었는지에 대해서는 거의 언급하지 않습니다. 보안 산업에서 우리가 직면하는 한 가지 어려움은 침해 사실을 책임감 있게 공개함으로써 다른 기업이 세부적 기술 정보를 얻어 유사한 피해를 막을 수 있도록 하는 것입니다. 이 보고서에서는 불운한 사고에서 얻은 교훈을 되짚어보고, 침해 사고 정보를 알려 미래를 위해 유용한 정보를 서로 공유하는 문화를 형성하기 위한 방안을 고찰합니다.

보고된 데이터 침해 사고를 종합해본 결과, SQL 인젝션 공격은 여전히 공격자들이 선호하는 진입점인 것으로 확인되었습니다. LizaMoon과 같이 자동화된 SQL 인젝션 공격은 인터넷을 검사해서 취약한 호스트를 악용합니다. 이런 SQL 인젝션 공격 수법은 오래 전부터 보편적으로 사용되어 왔습니다. 최근에는 쉘 명령어 인젝션 취약점을 노리는 공격도 증가하는 추세입니다. X-Force가 조사한 바에 의하면 연초에 비해 2011년 말에 쉘 명령어 인젝션 공격 빈도가 두세 배 더 많아진 것으로 확인됐습니다. 또한 2011년 종반에 SSH 패스워드 크래킹(password cracking) 공격도 급증했습니다.

2011년에는 완전히 새로운 공격 수법도 등장했는데 여러 인증기관의 취약점을 노린 공격이 대표적입니다. 이런 유형의 공격은 방문하는 SSL 페이지가 암호화되어 있으면 안전할 것이라는 사용자의 기본적인 믿음을 무너뜨립니다. 전통적인 피싱 및 스팸과 같은 오래된 공격 수법 대신, 이제는 악성 코드를 심는 수법이 흔히 사용되고 있습니다. 소셜 미디어 공격이 증가하고 있으며 공격자들은 친구나 팔로워에게 침투함으로써 공격 대상의 '신뢰 영역'에 침입하는 데 성공하고 있습니다.

이런 어려움이 있었지만, 자료를 통해 몇 가지 긍정적인 동향과 개선된 부분이 확인되었습니다. X-Force가 집계, 보고한 웹 애플리케이션 취약점 공격 건수가 2005년 이후 감소했으며 악성 코드가 대중에게 유포된 건수도 눈에 띄게 줄고 있습니다. 악성 코드가 인터넷에 유포된 경우 공격자가 취약점을 손쉽게 공략할 수 있습니다. 지난 몇 년간 대중에게 공개된 취약점 공격에서 악성 코드가 차지하는 비율은 15% 정도였습니다. 2011년에는 그 비율이 11%로 하락했습니다. 웹 브라우저뿐 아니라 문서 판독 애플리케이션과 편집 도구를 노린 악성 코드 유포 빈도는 지난 4년간 최저치로 감소했습니다. 대중에게 유포되는 취약점 공격도 이전에 비해 패치를 통해 차단되는 경우가 많아졌습니다. 패치를 통해 차단되지 않은 취약점 공격 비율은 2010년 43%에서 36%로 감소했습니다.

IBM AppScan 팀이 웹 애플리케이션 취약점 테스트를 실시한 결과, CSRF(Cross-Site Request Forgery)와 XSS(Cross-Site Scripting)의 취약점이 눈에 띄게 개선된 것으로 확인됐습니다.

연결성, 개방성, 이동성 및 사회성이 갈수록 향상되는 온라인 세상에 대한 개인과 기업의 참여도가 높아짐에 따라, 공격자도 호시탐탐 기회를 노리며 다각적이고 손쉬운 시스템 공격 수법을 새로 개발하고 있습니다. 공격자들은 인간의 본성을 악용하고 신뢰를 먹잇감으로 삼는 최소공분모(lowest common denominator) 수법을 이용해서 기술뿐 아니라 개인을 직접 공격하고 있습니다. 소셜 미디어 및 모바일 디바이스가 보편화되자 기업과 외부 세계의 경계선이 모호해지고 있습니다.

X-Force는 이런 맥락에서 이 보고서를 통해 기업이 모바일 디바이스와 클라우드의 복잡성에 대응하는 방법을 살펴볼 것입니다. 모바일 디바이스가 대대적으로 보급되면서 IBM의 'BYOD(bring your own device)' 프로그램에 대한 논의와 함께 이 프로그램에 영향을 미치는 가장 큰 위협과 BYOD 정책에 수반되는 위험을 최소화하는 방안이 세상의 주목을 받고 있습니다.

클라우드 보급도 그와 유사한 양상을 보이고 있습니다. 문제는 클라우드가 얼마만큼 안전한가가 아니라 클라우드 환경에서 위험을 해소하고 보안을 확보하기 위해 구체적으로 어떤 통제와 비즈니스 프로세스가 필요한가에 있습니다. 널리 보급된 클라우드 기반의 인프라를 도입하려는 조직이라면 보안 및 위험 최소화를 위해 맡아야 할 조직의 역할과 클라우드 서비스 제공업체의 역할을 이해하는 것이 중요합니다.

2011년 내내 각 기업의 보안 팀은 더 좋은 성과를 거두는 데 빈번히 어려움을 겪었습니다. 많은 보안 팀이 프로세스 및 기술 개선하거나, 직원과 고객을 대상으로 보안 교육을 실시하거나, 혹은 기업의 보안 상황에 대한 가시성을 개선함으로써 보안 정보 경보 체계를 강화하느라 진통을 겪었습니다. 보다 나은 예측과 감지를 위해 조직 전체에 IBM의 분석 및 정보 수집 능력을 활용하는 것이야말로 고객이 보안 위협을 효과적으로 극복하는 방법이라고 IBM은 믿습니다. IBM은 2011년 10월에 Q1 Labs를 인수 합병하고 보안 시스템 사업부를 발족하는 커다란 변화를 단행했습니다. 꾸준히 들려오는 IBM의 보안 정보 플랫폼 개선 소식은 IBM이 시장의 고민을 해결하는 데 얼마나 많은 노력을 기울이고 있는지 보여주는 방증입니다. 행동과 변화를 위해서는 상황 인식이 선행되어야 합니다. 그리고 변화는 곧 IBM의 바람입니다.

2011년 하이라이트

위협:

악성 코드 및 악성 웹사이트

- 2011년 초부터 데이터 침해 사고가 폭발적으로 증가하고 그런 추세가 한 해 동안 지속되자 IBM X-Force는 2011년을 "보안 침해의 해"로 선포했습니다(12 페이지).
- 2011년에도 SQL 인젝션은 기업을 공략하는 데 가장 흔히 사용된 취약점이었습니다. SQL 인젝션 수법은 등장한 지 상당히 오래됐지만 여전히 효과적인 공격 수단으로 사용되고 있습니다(17 페이지).
- 공격자들이 다수의 인증기관을 유린하는 또 한 차례의 초유의 사태가 2011년에 발생했습니다. 그 중에서도 네덜란드의 인증기관인 DigiNotar가 특히 큰 피해를 입었습니다. 공격자들은 승인되지 않은 인증서를 생성한 후 암호화된 통신을 '도청'하는 수단으로 메시지 가로채기(man-in-the-middle) 공격 수법을 이용하여 인증서를 가로챌 수 있었습니다. 이런 유형의 공격은 방문하는 SSL 페이지가 암호화되어 있으면 안전할 것이라는 사용자의 기본적인 믿음을 무너뜨립니다(33 페이지).
- SSL/TLS를 통해 통신하는 서버를 대상으로 서비스 거부(DoS) 공격을 할 수 있는 개념 증명 도구가 2011년에 등장했습니다. 이 도구는 일반적인 방식으로 연결된 랩탑 컴퓨터를 악용해서 기업의 웹 서버를 마비시킬 수 있다는 것을 보여주었습니다(33 페이지).
- IBM MSS(Managed Security Service)가 확보한 다량의 데이터를 분석한 결과, 공격자들이 선호하는 방법은 SQL 인젝션 공격이고, SSH 무차별 인젝션 공격과 쉘 명령어 인젝션 공격이 증가했으며, 프록시 바운스 공격이 MSS 센서 트래픽 상위에 오른 것으로 확인됐습니다 (16 페이지).
- 2011년에는 Mac용 악성 코드가 그 어느 해보다 심하게 활개를 친 것으로 조사됐습니다. Mac용 악성 코드의 빈도가 이전에 비해 늘었을 뿐 아니라 그 기능 역시 다양해졌습니다. 이전에는 Windows® 용 악성 코드에서만 볼 수 있었던 기능들이 Mac용 악성 코드에도 추가되기 시작한 것으로 조사됐습니다(39 페이지).

웹 컨텐츠 동향, 스팸 및 피싱

- 2011년 상반기에 익명 프록시가 꾸준히 늘어 3년 전에 비해 4배 이상 증가했습니다. 그러나 2011년 하반기에는 2009년 이후 처음으로 익명 프록시 증가세에 제동이 걸렸습니다. 익명 프록시는 사람들이 악의적 의도를 감출 수 있기 때문에 대단히 위험한 유형의 웹사이트입니다(44 페이지).
- 공격자들이 ZIP 첨부파일로 악성코드를 전달하는 방식을 선택하기 시작하면서 2011년 초반의 스팸 감소 추세가 연말까지 이어졌습니다(49 페이지).
- 2011년에는 현재까지 발송된 것으로 보고된 스팸 중 인도가 약 14%를 차지하면서 스팸 발신 국가 명단 1위에 이름을 올렸습니다. 미국은 2010년에 불명예스러운 1위를 차지했지만 2011년에는 미국에서 발송된 스팸이 전체 스팸의 2% 미만에 그쳤습니다. 인도에 이어 베트남, 인도네시아, 러시아, 브라질이 뒤를 이었고 호주가 2011년 말까지 유포된 스팸의 5.6%를 차지하면서 처음으로 6위를 기록했습니다(55 페이지).
- 2011년 막바지에 피싱 이메일과 유사하게 웹사이트 링크가 추가된 이메일이 등장하기 시작했습니다. 이 이메일의 특징은 피싱 공격을 반드시 행하는 건 아니라는 것입니다. 이 메일은 널리 알려진 브랜드의 명성을 이용해서 사용자가 악성 링크나 경우에 따라 온라인 쇼핑 센터와 같은 무해한 사이트로 이동하는 링크를 클릭하도록 유도합니다. 무해한 사이트로 이동하는 링크를 클릭하도록 유도하는 방식의 이메일에 대한 한 가지 가능한 설명은 광고료를 받는 대가로 사이트의 트래픽을 유도하는 일종의 클릭 사기 수법이라는 것입니다. 이러한 설명과는 관계 없이, 이 수법으로 2011년 후반에 피싱 방식의 이메일이 급증한 것으로 확인됐습니다(56 페이지).

보안 인프라 운영:

취약점 및 악용

- 2011년에는 새로 보고된 보안 취약점은 7,000건을 약간 상회합니다. 역대로 가장 많은 취약점이 보고된 해였던 2010년에 비하면 크게 감소한 수치지만 2006년 이후 취약점 발견 건수가 2년을 주기로 등락을 반복하고 있습니다. 다만, 상승한 해와 하락한 해 모두 그 수치가 꾸준히 높아지고 있습니다(74 페이지).
- 지난 몇 년간 발생한 보안 취약점 발견 건수 중 절반 정도가 웹 애플리케이션 취약점이었습니다. 그러나 2011년에는 그 수치가 2005년 이후 가장 낮은 41%로 하락했습니다(75 페이지).
- 공개적으로 노출된 취약점이면서 다수의 공격 빈도를 기록한 웹 애플리케이션 중 하나는 애플리케이션 웹 기반 컨텐츠 관리 시스템(CMS)입니다. 널리 사용되는 네 가지 웹 기반 컨텐트 관리 시스템을 IBM X-Force가 분석해본 결과, 이런 시스템의 가장 중대한 취약점은 해당 시스템이 지원하는 타사의 플러그인 환경에 기인한 것으로 확인됐습니다(77 페이지).
- 2011년에는 실제로 대중에게 악성 코드를 유포한 공격 건수가 크게 감소했습니다. 이는 2006년 이후 가장 낮은 수치이며 실제 건수뿐 아니라 비율 역시 이전에 비해 감소했습니다. 지난 몇 년간 취약점의 공개적 악용 비율은 15% 내외였지만 2011년에는 11%에 그쳤습니다(78 페이지).
- 중대하거나 심각한 브라우저 취약점이 해를 거듭할수록 늘고 있으며, 브라우저 자체가 아니라 타사 브라우저 플러그인을 그 대상으로 하여 악성 코드를 자동으로 다운로드하는 공격 수법(drive-by-download)이 증가한 것으로 확인됐습니다. 이런 유형의 공격에서 공격자들이 선호하는 수단은 문서 뷰어 도구입니다. 왜냐하면 악성 문서 파일을 이메일에 첨부하거나 악성 코드를 자동으로 다운로드하는 수법에 사용할 수 있기 때문입니다(78 페이지).
- 멀티미디어 플레이어를 노린 취약점 공격 건수도 꾸준히 증가하고 있는데 2011년에도 2010년 못지않게 멀티미디어 취약점을 노린 대규모 공격이 빈번히 발생했습니다(81 페이지).
- 세계에서 손꼽히는 기업용 소프트웨어 제공업체들의 취약점 발견 건수가 전체 건수에서 차지하는 비율이 2008년 19%에서 2011년 31%로 상승한 데서 짐작할 수 있듯이 지속적으로 증가하고 있습니다. 그렇다고 소프트웨어 산업 통합만이 능사는 아니라는 게 X-Force의 판단입니다. 안전한 개발 환경이 소프트웨어 개발 수명주기에서 차지하는 비중이 갈수록 커지고 있으며, 지난 몇 년간 책임감 있는 소프트웨어 개발업체는 자사의 코드에 내재된 취약점을 찾아서 제거하는 능력을 개선하는 데 전력을 기울여 왔습니다(84 페이지).
- 비주류의 취미에 불가했던 소셜 네트워크가 지난 몇 년 새에 검색 엔진의 이용률마저 추월해서 세계 최대 규모의 온라인 활동 공간으로 성장했습니다. 온라인 이용자의 활동이 집중되다 보니 당연히 범죄의 온상으로 떠올랐습니다. 몇 년 전 이메일을 통한 사기로 톡톡히 재미를 봤던 범죄자들이 소셜 미디어 포럼을 새로운 잠재적 공격 목표이자 새로운 삶의 터전으로 삼게 된 것입니다(89 페이지).

소프트웨어 개발 환경 보안 현황

웹 애플리케이션 취약점

- OWASP(Open Web Application Security Project)가 발표한 상위 10가지 취약점 명단에 오른 여러 가지 문제가 IBM AppScan의 On-demand 애플리케이션 취약점 테스트 서비스에 테스트를 의뢰한 소프트웨어에서도 빈번히 나타났습니다. 특히, 취약한 인증 및 세션 관리 문제는 10번의 테스트에서 거의 8번이나 발견됐습니다. 테스트 대상이 된 애플리케이션 중 다수는 세션 조작을 막을 능력이 미흡해서 세션 무단 변경 방식의 공격에 취약했습니다. 또한 세션 종료 및 세션 재사용과 관련된 문제 역시 애플리케이션 테스트에서 취약한 인증 및 세션 관리 문제가 빈번히 발견된 주요 요인이었습니다(113 페이지).
- 2011년에 실시한 애플리케이션 취약점 테스트에서 CSRF(Cross-Site Request Forgery) 취약점이 발견된 비율은 59%였던 2010년에 비해 크게 줄어든 28%였습니다. 이런 감소세를 보인 주된 이유는 이런 유형의 취약점에 대한 인지도가 높아졌고 CRSF 토큰 사용 방법이 개선됐기 때문인 것으로 판단됩니다(116 페이지).
- XSS(Cross-Site Scripting) 취약점이 애플리케이션 취약점 테스트에서 40% 이상 발견된 점으로 미루어보아 보안 코딩 규칙을 제대로 따르지 않은 애플리케이션이 여전히 많은 것으로 추정됩니다. 여러 가지로 개선되고 있는 건 분명하지만 아직 만족하기엔 턱없이 부족합니다. 아주 쉽게 이해할 수 있고, 아주 쉽게 시험해볼 수 있으며, 아주 쉽게 수정할 수 있는 애플리케이션에서 XSS 취약점이 40% 이상 발견됐다는 사실은 특히 우려할만합니다. 웹 애플리케이션의 취약점은 여전히 많은 데이터 침해 사고의 원인으로 작용하고 있습니다. 데이터 침해 사고는 2011년 상반기에도 증가했습니다. IBM X-Force가 2011년을 '보안 침해의 해'로 선언할 정도로 데이터 침해 사고는 폭발적인 증가세를 기록했습니다(114 페이지).
- IBM X-Force가 주목한 또 다른 중요한 측정점(data point)은 '보안 테스트에서 해당 인스턴스가 발견되는 평균 건수'입니다. XSS 취약점이 발견된 경우 XSS의 인스턴스는 감소하는 것으로 분석됐습니다. 실제로 2009년에 평균 건수가 40건 이상이었던 반면 2011년의 평균 건수는 3건을 약간 상회하는 수준에 불과했습니다. 따라서 이제 애플리케이션에서 입력 제어가 완전히 배제될 가능성이 훨씬 낮아진 셈입니다(114 페이지).
- 2011년에 금융 서비스용 애플리케이션은 다시 가장 보안성이 우수한 부문으로 복귀했습니다. 정부용 애플리케이션은 세 가지 취약점 모두에서 가장 미흡한 것으로 조사됐습니다. 이런 변화의 원인이 확실하지는 않으나, 이미지 훼손이 한 가지 요인으로 작용한 것으로 판단됩니다. 정부용 애플리케이션에서 데이터 침해 사고가 발생한 경우 보안 강화에 대한 투자를 늘릴 가능성은 금융 서비스용 애플리케이션에 비해 낮습니다(116 페이지).

새로운 보안 추세:

모바일

- 모바일 디바이스 역시 중요도가 급증하고 있는 또 다른 분야입니다. 현재까지 다양한 모바일 운영체제에서 취약점이 발견되었으며 이런 취약점을 노린 악성 코드가 대중에게 배포된 사례가 많습니다. 모바일 디바이스의 '탈옥(Jail break)'이나 최상위 관리자 권한 획득(루팅 – Rooting)은 사용자들이 모바일 악성 코드를 온라인에 게시하도록 유도하는 주요 동기로 손꼽힙니다. 물론, 일단 활성화된 코드는 탈옥 상태가 아닌 모바일 디바이스에 악의적 용도로 사용될 수 있습니다(82 페이지).
- 감염된 모바일 디바이스를 이용한 대규모 봇넷 공격이 본격적으로 등장하고 있는데, 이는 시작에 불과합니다(83 페이지).
- 모바일 디바이스는 일반적으로 음성, 메시지 전송 및 데이터 서비스와 함께 GPS 하드웨어가 탑재되어 있어 위치 정보 저장, 메시지, 이메일, 음성 통화를 비롯한 사용자의 다양한 행동 패턴을 모니터링해서 공격자에게 전송하는 스파이 애플리케이션의 존재가 감지됩니다. 이런 방식의 공격은 개인용 컴퓨터에서 나타나는 현상과 비교해 보면 특히 우려할만합니다. 더군다나 모바일 디바이스가 실제로 '손 안에 있는 사무실'이 됐기 때문에 스파이 애플리케이션의 공격 수법은 날로 진화할 것으로 예상됩니다(122 페이지).

- 2011년에 눈에 띄었던 전개 양상 중 하나는 기업용 애플리케이션 및 데이터를 직원의 개인 애플리케이션 및 데이터와 분리하는 방안에 대한 관심이 고조됐다는 점입니다. 이런 양상이 전개되는 데는 많은 관심과 공감대가 형성된 BYOD(bring your own device) 프로그램도 크게 작용했습니다(125 페이지).

클라우드 보안

- 문제는 클라우드가 얼마나 안전한가가 아니라, 클라우드 환경에서 위험을 해소하고 보안을 확보하기 위해 구체적으로 어떤 통제 환경과 비즈니스 프로세스에 관심을 기울여야 하는가에 있습니다. 널리 보급된 클라우드 기반의 인프라 도입을 고려 중인 조직이라면 보안 및 위험 최소화와 관련된 조직의 역할과 클라우드 서비스 제공업체의 역할을 이해하는 것이 중요합니다(126 페이지).
- 클라우드 컴퓨팅의 보안은 단순히 계약 관리 문제를 떠나서 클라우드 도입의 성공 여부를 판가름하는 중요한 변수가 될 수 있습니다. 수명 주기 관리 및 철수 전략을 고려한 유연한 SLA(Service Level Agreement)를 마련한다면 도움이 될 수 있습니다(128 페이지).
- SLA는 계약 기간과 범위가 구체적으로 명시되고 적절한 통지를 통해서만 수정이 가능하며 조직의 구체적인 비즈니스 및 정보 보안 요건을 인식한다는 점에서 진짜 계약서나 다름없습니다(131페이지).

2011년 — 보안 침해의 해

2011년 중반부터 새해까지 보안 침해 사고는 여전히 진행형

2011년 중반에 IBM X-Force는 세간의 화제를 모은 다양한 외부 네트워크 보안 침해 사고로 얼룩진데다 발생 빈도뿐 아니라 피해자 중 다수가 우수한 보안 능력을 믿어 의심치 않았던 기업이기에 충격이 더 컸던 2011년을 '보안 침해의 해'로 선언했습니다.

2011년 하반기에는 누출된 고객 정보, 마비된 웹 서비스, 수십억 달러의 금전적 피해라는 파장을 일으킨 대대적인 주간 네트워크 보안 침해 사고에 대한 보고가 끊이지 않았습니다. IT 보안은 비즈니스 결과, 브랜드 이미지, 공급망, 법적 공개 및 감사 위험에 영향을 미치기 때문에 이제 중역 회의실의 흔한 논의 주제가 되고 있습니다. IBM X-Force 2011년 상반기 동향 및 위험 보고서에서 IBM X-Force는 2011년을 불가피하게 보안 침해의 해로 선언하게 된 근원적인 동기와 공격 방식, 기본적인 보안 현황을 살펴본 바 있습니다.

보안 사고는 산업과 부문을 가리지 않고 발생했습니다. 법 집행기관, 정부, 소셜 네트워크 커뮤니티, 소매, 엔터테인먼트, 은행, 비영리 기관, Fortune 500대 기업, 그리고 심지어 보안 회사마저도 공격 대상이 됐습니다. 공격은 특정 지역으로 집중된 것이 아니라 전 세계에서 무차별적으로 행해졌습니다.

2011년 한 해가 저물어갈 무렵에도 그런 추세는 좀처럼 둔화될 기미를 보이지 않았습니다. 12월에는 중국의 여러 대형 소셜 네트워크 및 엔터테인먼트 사이트에 대규모의 피해를 입힌 공격이 있었습니다. 이로 인한 잠정 피해액만 수십억 달러에 이르기도 했습니다.

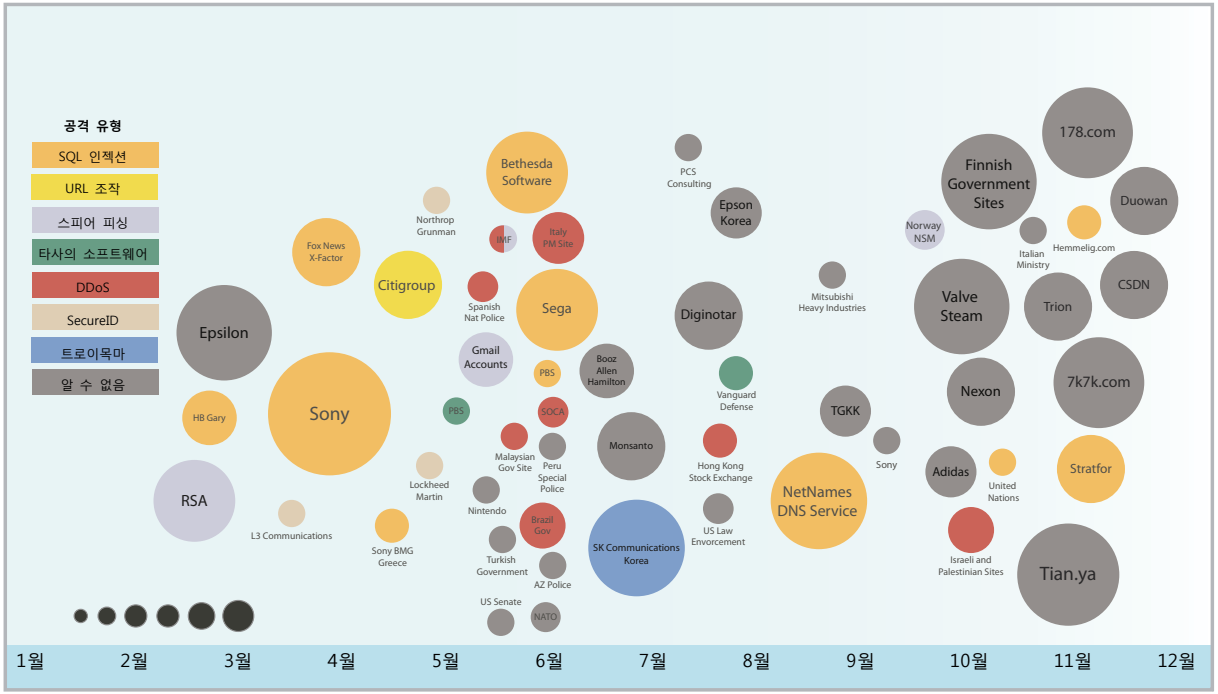


그림 1: 공격 유형, 시간 및 영향을 기준으로 2011년 보안 사고 분류

2011년 하반기의 판도 변화

그림 1에서 볼 수 있듯이 SQL 인젝션 공격은 기업을 공략하는 데 가장 흔히 사용된 취약점이었습니다. SQL 인젝션 수법은 등장한 지 상당히 오래됐지만 여전히 효과적인 공격 수단입니다. 이 글의 후반에서는 SQL 인젝션 공격의 복잡성과 이런 공격 수법을 감지하고 네트워크를 보호하기가 왜 어려운지 설명하겠습니다.

2011년에는 공격 수법이 더욱 정교해지면서 일단 핵심 기술을 공략한 후 다른 목표를 노려 대대적인 공격으로 확대한 사례가 여러 차례 보고되었습니다. 2011년 초에 RSA를 대상으로 한 공격으로 RSA의 SecureID 인증 제품과 관련된 민감한 코드와 데이터가 누출되었습니다. 그리고 나중에 최소한 세 개의 다른 기업에 침투하는 데도 이 때 사용됐던 기술이 쓰인 것으로 밝혀졌습니다.[1] 이는 공격자가 최종 공격 목표를 공략하는 건 물론이고 더욱 폭넓은 잠재적 피해자가 사용하는 근본적인 기술에 침투할 수 있는 복합적 관계가 늘어남을 시사합니다.

2012년까지 이어지고 있는 또 다른 새로운 추세는 공격자가 잘 알려진 사이트로 가장한 악성 사이트로 사용자를 리디렉션(redirection)하는 수단으로 DNS 서버를 이용한다는 것입니다. 사용자가 http://www.somecompany.com과 같은 웹 도메인을 브라우저에 입력할 때마다 해당 이름은 사이트를 호스팅하는 서버의 IP 주소로 바뀌어야 합니다.

NetNames의 DNS 이름 서버에 SQL를 주입함으로써 공격자는 The Register, The Daily Telegraph, UPS와 같은 여러 유명 사이트의 DNS 레코드를 갱신할 수 있었습니다.[2]

흔히, DNS 이름 서버 자체를 공격하는 데 성공한 공격자는 유명 웹사이트와 유사해 보이지만 사실 다운로드 가능한 악성 코드가 포함되어 있거나 민감한 정보를 빼내도록 설정되어 있는 사이트를 만든 후 요청 경로를 해당 서버로 변경합니다. 이런 방식의 공격은 웹사이트 이름을 직접 입력할 경우 다른 서버로 이동하지 않을 것이란 기본적인 믿음을 무너뜨립니다.

공격자들이 다수의 인증기관을 유린하는 또 한 차례의 사태가 2011년에 발생했습니다.[3] 그 중에서도 네덜란드의 인증기관인 DigiNotar는 특히 큰 피해를 입었습니다. 이 인증기관은 사용자부터 온라인 서비스까지 트래픽을 암호화하는 데 사용되는 안전한 기능의 HTTPS 프로토콜을 지원하는 보안 인증서를 배포합니다. 공격자들은 승인되지 않은 인증서를 생성한 후 암호화된 통신을 메시지 가로채기(man-in-the-middle) 공격 수법으로 '도청'하여 인증서를 가로챌 수 있었습니다. 이런 유형의 공격 역시 암호화된 SSL 페이지를 방문하는 경우 안전하다는 사용자의 기본적인 믿음을 무너뜨립니다. 현재의 SSL 신뢰 모델에 수반된 위험에 대해서는 뒤에서 더 자세히 다루겠습니다. 이 두 경우에서 공격자는 다단계 전략을 사용하여 핵심 기술을 공략한 후 공략에 성공한 수법을 이용해서 넓은 그물을 쳐 두고 잠재적 피해자가 걸리기를 기다립니다.

1. http://www.nytimes.com/2011년/06/04/technology/04security.html
   http://www.infosecisland.com/blogview/14142-RSA-SecurID-Breach-Spreads-to-L3-and-Northrop.html
2. http://www.theregister.co.uk/2011년/09/05/dns_hijack_service_updated/
3. http://www.theregister.co.uk/2011년/10/27/ssl_certificate_authorities_hacked/

우리가 얻는 교훈

2011년 보안 사고 도표에서 볼 수 있듯이 2011년 하반기에는 많은 사고가 발생해서 대중에 공개됐지만 사고가 발생한 배경에 대한 정보는 아직 확보하지 못한 상태입니다. 보안 침해 사고를 대중에 공개하는 이유는 여러 가지 다른 동기가 있지만 공격자에 의해 악용된 기술적 취약점을 대중에게 알리려는 목적인 경우는 그리 흔치 않습니다. 개인정보나 기업의 데이터가 노출됐을 가능성이 있다거나 해당 기업이 개발한 기술이 취약하다는 사실을 고객에게 알리려는 의도로 대중에 공개하는 경우는 이따금 있습니다. 최근 들어 금융 전문가들이 컴퓨터 보안 위험에 대한 정보를 투자 결정 평가에 반영하는 경우가 늘고 있습니다. 그러나 기업들은 보통 컴퓨터 보안 문제가 발생한 다른 회사에 세간의 관심이 쏠리길 원하며, 솔선수범하여 자사의 보안 침해 사실을 공개하는 경우는 비교적 드뭅니다. 다른 기업이 겪은 사고를 통해 어렵게 얻은 교훈에서 보안 전문가가 해법을 찾을 가능성이 많기 때문에 이런 태도는 바람직하지 않다는 게 IBM X-Force의 입장입니다.

다수의 항해 및 비행 전문 잡지들은 매달 대단히 위험하거나 사고로 이어졌던 실제 상황을 설명한 칼럼을 게재합니다. 조종사와 선장들은 이런 기사를 매달 읽고 과거에 취했던 서로의 행동을 정기적으로 검토할 수 있습니다. 이런 과정을 통해 난관을 극복하는 방법을 배우고 위험이 닥쳤을 때 큰 도움이 되는 자신감을 배양할 수 있습니다. 이와 유사하게 컴퓨터 네트워크를 공격으로부터 보호할 책임이 있는 사람들은 함정을 피할 수 있는 직관력을 계발할 수 있도록 보안 유지 실패 사례를 정기적으로 공유해야 합니다. 보안 침해의 원인이 된 정확한 기술적 결함과 절차상의 오류를 파악하면 자사에 내재된 문제를 해소할 실마리를 찾을 수 있습니다.

기업은 컴퓨터 보안 비용 역시 사업상의 경비로 간주하고, 다시 재발할지도 확신할 수 없는 보안 결함의 해결에는 투자를 꺼리기 일쑤입니다. 회사를 보호하기 적당한 정도로 보안에 비용을 투자하고 있으니 이 정도면 '안정권'일 것이라는 기대 속에 단 1달러도 더 투자하려 들지 않습니다. 따라서 단순히 기술적 혹은 절차상 결함을 찾는 것만으로는 기업이 문제를 해결하는 데 투자하도록 설득하기 어렵습니다. 이런 문제를 수정하지 않을 경우 사고가 발생했을 때 실제로 어떤 위험이 따르는지 증명해야만 합니다. 보안 침입의 피해를 입은 기업이 사고의 원인이 된 기술적 결함과 절차상 오류를 자세하게 공개하면 이 정보는 다른 기업이 유사한 문제를 해소하는 데 필요한 투자의 정당성을 입증하는 데 도움이 됩니다. 기술적으로 유사한 침해 사고가 여러 기업에서 발생한 경우 그와 관련된 구체적인 기술적 취약점을 공개하면 '동업자 정신'으로 이런 종류의 취약점을 해결하는 공조 분위기를 조성할 수 있습니다.

컴퓨터 범죄의 피해자는 '무엇이 잘못됐는가?'에 대한 기술적 세부 정보를 대중과 논의하는 것이 얼마나 유익한지 인식해야 합니다. 그렇지 않을 경우 대중이 보안 침해에 무방비로 노출될 수 있기 때문입니다. 이런 종류의 정보를 공개하는 데 따르는 위험이 그 이득보다 큰 경우도 있을 것입니다. 너무 많은 기술적 세부 정보를 공개할 경우에는 향후 공격의 지침이 될 수도 있습니다. 그러나 공개할 경우 어떤 이득이 있는지 알아야 합니다. 다른 기업이 자사의 불행으로부터 교훈을 얻도록 돕는 일이야말로 자사의 네트워크를 공격했던 부류의 범죄자들이 향후 공격에 성공하는 것을 억제하는 보호기제가 될 수 있기 때문입니다.

나아가야 할 길

X-Force 2011년 상반기 동향 및 위험 보고서에서 X-Force는 2011년에 발생했던 공격을 근절하기 위해 취할 수 있는 10가지 조치를 제안한 바 있습니다. 물론, X-Force가 추천한 조치 중 IT 보안 전문가다운 획기적인 아이디어라 자랑할만한 것은 없습니다. 관건은, 어떻게 해야 하는지를 아는 것이 아니라 복잡하게 분산된 조직 환경에서 꾸준히 이를 실천에 옮기는 것입니다. 보안 프로그램이 성공을 거두려면 전사적 차원에서 모범 사례를 준수하는 데 필요한 자원, 정치적 지원, 그리고 기관의 존중이 반드시 수반되어야 합니다. 이런 수준의 효율성을 확보하는 것이 IT 보안 관리 부서가 반드시 해결해야 할 과제입니다.

만약 IBM X-FORCE®가 IT 부서를 운영한다면...

1. 정기적으로 타사의 외부 및 내부 보안 솔루션 감리 실시
2. 엔드포인트 통제
3. 민감한 시스템 및 정보 세분화
4. 네트워크 보호
5. 웹 애플리케이션 감리
6. 최종 사용자에게 피싱 및 스피어 피싱 교육 실시
7. 불량 비밀번호 조사
8. 보안을 모든 프로젝트 계획에 반영
9. 협력업체의 보안 정책 검토
10. 확실한 사고 대응 계획 마련

위의 권장안에 대한 자세한 정보를 원하는 경우 IBM X-Force 2011년 상반기 동향 및 위험 보고서를 다운로드해서 읽으십시오.

IBM MSS(Managed Security Service) — 세계 위협 현황

IBM MSS는 1년 365일 24시간 내내 130여 개국에서 발생하는 하루 평균 수백억 건의 이벤트를 감시합니다. IBM MSS는 국제적 입지를 바탕으로 현재의 위협에 대한 직접적인 견해를 제시합니다. IBM 분석가는 풍부한 데이터를 사용하여 사이버 위협 현황에 대한 참신한 분석 결과를 제공합니다. 위협 동향 파악은 미래를 염두해 둔 보안 전략을 수립하고 위협의 중대성을 이해하는 데 대단히 유용합니다.

MSS - 2011년에 대량 발생한 상위 시그니처

대량 발행한 상위 시그니처

도표 1은 2010년 말과 비교한 2011년의 하향/상향 곡선과 대량으로 발생한 상위 시그니처의 순위를 보여주고 있습니다. 2010년 상위 10개의 시그니처 중 4개가 2010년 순위 명단에도 자리를 차지하고 있습니다. SQL_Injection 및 SQL_SSRP_Slammer_Worm은 2년간 계속 상위권을 유지하고 있는 반면, 슬래머 활동은 소폭 하향세를 보였습니다. 하향세를 그리던 SQL_Injection이 2011년에 다시 1위에 올랐고 SSH_Brute_Force는 이번에도 순위 목록에 이름을 올렸지만 9위로 하락했습니다. HTTP_Unix_Passwords는 2011년에 처음으로 순위에 올랐지만 상반기에 비해 하반기에는 기세가 한풀 꺾이면서 6위에서 10위로 떨어졌습니다.

이벤트 명칭	2011년 순위	추세	2010년 순위	추세
SQL_Injection	1	상승	2	하락
HTTP_Suspicious_Unknown_Content	2	하락		
SQL_SSRP_Slammer_Worm	3	소폭 하락	1	하락
SNMP_Crack	4	하락		
HTTP_GET_DotDot_Data	5	상승		
Cross_Site_Scripting	6	소폭 상승		
SSH_Brute_Force	7	소폭 상승	4	소폭 하락
HTTP_Unix_Passwords	8	상승	6	소폭 상승
Shell_Command_Injection	9	상승		
Proxy_Bounce_Deep	10	상승		

도표 1: 대량 발생한 상위 시그니처와 2010년 말과 2011년 말을 비교한 하향/상향 곡선(IBM MSS 통계)

SQL 인젝션 공격

IBM X-Force의 조사에서 2010년에 2위를 기록했던 SQL 시그니처가 1위에 올랐으며 계속 상승세를 보이고 있습니다. 2011년은 SQL 취약점 공격이 큰 성공을 거둔 한 해로 여러 건의 SQL 인젝션 공격 사례가 언론과 대중의 엄청난 관심을 모았습니다. Anonymous 및 Lulzsec과 같은 핵티비스트 단체가 대다수 SQL 인젝션 공격을 주동했으며 새로운 인젝션 공격 수법으로 공격 기술을 꾸준히 갈고 닦았습니다. 또한 인터넷을 조사해서 취약한 호스트를 찾아내는 수법이자 현재 활성화된 공격 수법의 기원이기도 한 LizaMoon과 같은 자동화된 SQL 인젝션 공격도 등장했습니다. IBM MSS는 보안 정보 및 이벤트 관리(SIEM) 규칙 세트에 여러 가지 새로운 공격 수법을 추가했으며, 꾸준한 모니터링과 분석을 통해 새로운 공격 수법이 나타나는지 주시하고 있습니다. '여전히 활개를 치고 있는 SQL 인젝션 공격'라는 제목의 다음 단원에서는 이런 위협의 성격을 심층적으로 논의하고 기업이 자사의 웹 애플리케이션 코드, 서버 및 네트워크를 SQL 인젝션 공격으로부터 보호하기 위해 취할 수 있는 조치를 설명합니다.

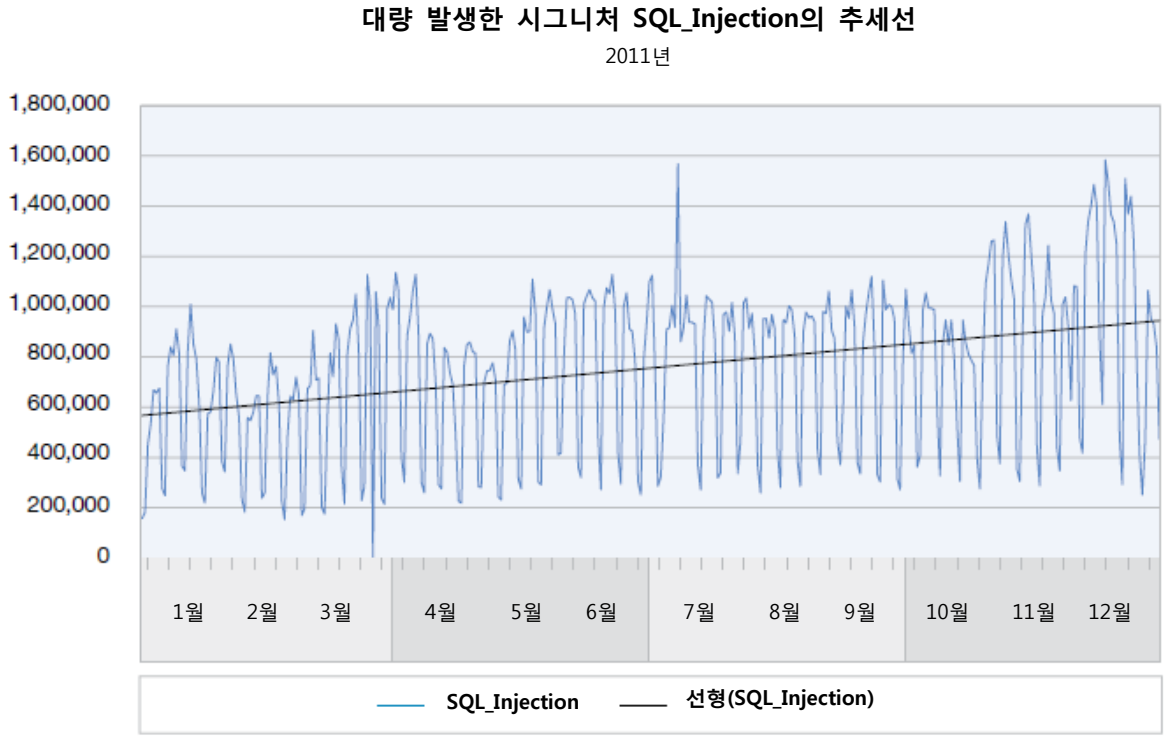


그림 2: 2011년에 대량 발생한 시그니처 SQL_Injection의 추세선(IBM MSS 통계)

우리 안에 Zeus가 있다?

HTTP_Suspicious_Unknown_Content가 대량 발생한 상위 시그니처 목록 2위에 오르는 데 HTTP 활동이 결정적인 영향을 미친 사실은 당연한 것일 수도 있습니다. 그러나 이는 Zeus와 같은 봇넷이 우리의 네트워크에서 활동하고 있는 가능성이 있다는 뜻이기도 합니다. Zeus는 2007년 7월에 처음 발견되어 널리 알려진 온라인 뱅킹 트로이목마로서 2009년 중반에 널리 확산되었습니다. 주요 감염 수법은 자동 다운로드(drive-by-download)와 피싱입니다. 여러 개인과 단체가 Zeus 봇넷을 설치하는데, 그 목적은 일반적으로 개인정보를 훔치는 것입니다. 공격자가 원하는 개인정보는 일반적으로 은행 계좌에 접속해서 송금하는 데 사용할 수 있는 온라인 뱅킹 데이터입니다.

FBI는 Zeus를 이용해서 봇넷을 만드는 단체들을 적극적으로 추적해 왔습니다. 그러나 MSS가 추적한 바에 따르면 2010년에 기존의 Zeus 명령 및 제어 서버 중 다수를 '박멸'하는 데 성공했음에도 불구하고, 엄청나게 많은 수의 컴퓨터가 Zeus에 감염된 상태입니다. Zeus는 막기가 매우 어려우며 바이러스 예방 프로그램도 기껏해야 일시적으로 Zeus의 확산을 늦출 수 있을 뿐이므로 Zeus를 막는 효과적인 방법은 사용자 교육 밖에 없습니다. 이메일 혹은 웹에 추가된 악성 링크나 미심쩍은 링크를 클릭하지 않도록 직원을 교육하는 한편, 바이러스 예방 프로그램을 지속적으로 업데이트하는 것이 바람직합니다.

SQL 슬래머의 꾸준한 하향세

2003년 1월 25일 Microsoft Resolution Service의 버퍼 오버플로우를 악용하는 공격적인 웜이 인터넷에 연결된 서버를 대규모로 감염시키기 시작했습니다. 이 웜은 감염 확산에 SQL 취약점을 악용하지 않고도 Microsoft SQL Server Desktop Engine (MSDE)을 실행하는 서버에 대규모 감염을 유발했습니다. 슬래머 감염 패킷이 인터넷의 UDP 트래픽 중 상당 부분을 차지하는 가운데, 슬래머가 지난 몇 년간 꾸준히 확산되었습니다. 실제로 SQL_SSRP_Slammer_Worm은 2010년 대량 발생 시그니처 1위였습니다. 그러나 이 시그니처는 IBM X-Force의 2011년 상반기 조사에서 2위로 내려앉은 데 이어 하반기 조사에서 3위로 떨어졌습니다. X-Force 2011년 상반기 동향 및 위험 보고서의 'SQL 슬래머가 자취를 감춘 날' 절에는 2011년 3월 SQL 슬래머 활동이 급격하게 감소하면서 목록에서 하위권으로 떨어진 설명이 나와 있습니다.

그림 3에 보이는 것처럼 2011년에 SQL 슬래머 활동은 상당한 회복세를 보이다가 다시 급격히 하락하는 양상을 몇 차례 반복했습니다.

12월에 SQL 슬래머 활동이 평소에 비해 큰 폭으로 증가한 것으로 조사되었지만 3월 이전의 양상으로 회복할 가능성은 별로 없어 보입니다. IBM X-Force는 상황을 계속 모니터링하면서 새로운 동향이 나타나는지 주시할 계획입니다.

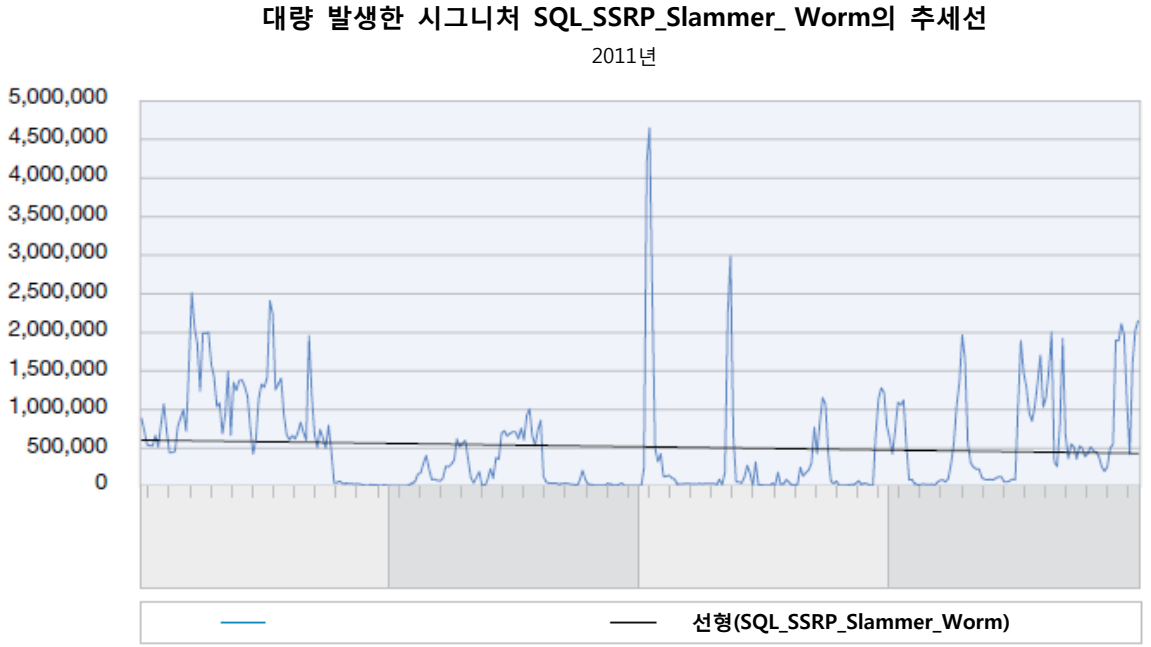


그림 3: 2011년에 대량 발생한 시그니처 SQL_SSRP_Slammer_ Worm의 추세선(IBM MSS 통계)

SNMP 취약점

SNMP_Crack 시그니처는 SNMP 커뮤니티 문자열을 무차별로 주입하는 공격 수법입니다. SNMP는 네트워크 관리자가 손쉽게 네트워크 디바이스 상태를 모니터링하고 디바이스 구성을 관리할 수도 있는 서비스입니다. 운영체제, 허브, 스위치, 그리고 라우터도 SNMP를 이용합니다. SNMP는 비밀번호와 같은 커뮤니티 문자열을 이용해서 민감한 정보 및 관리 권한을 보호합니다. SNMP 서비스가 기본 커뮤니티 스트링으로 설정되어 있는 경우가 빈번한데 공격자들은 일단 이런 커뮤니티 스트링을 찾는 데 주력합니다. SNMP 서비스가 기본 커뮤니티 스트링으로 설정되어 있지 않은 경우, 공격자는 무차별 주입 공격을 통해 커뮤니티 스트링을 유추하려고 시도할 수 있습니다. IBM X-Force는 기업이 자사의 디바이스에 SNMP를 활성화할 필요가 있는지 검토해보고 필요 없는 경우 비활성화할 것을 권장합니다.

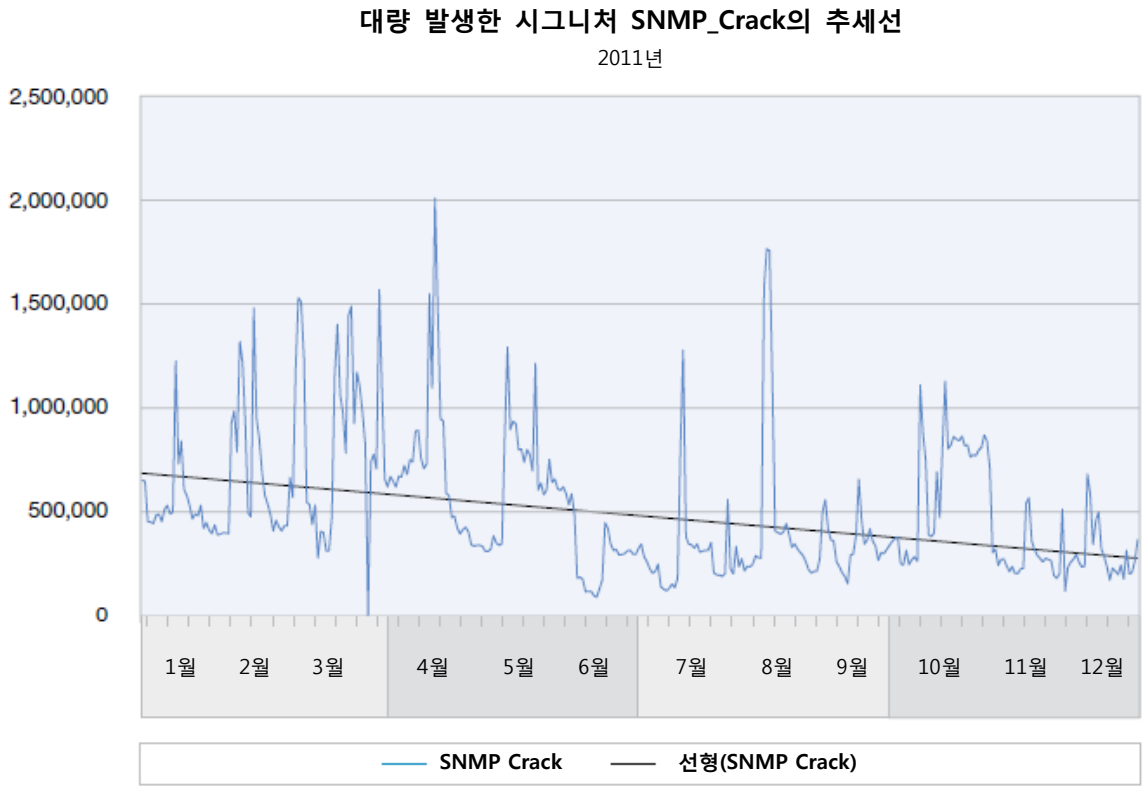


그림 4: 2011년에 대량 발생한 시그니처 SNMP_Crack의 추세선(IBM MSS 통계)

디렉토리 통과

HTTP_GET_DotDot_Data 시그니처는 웹 서버가 적용한 정상적인 보안 절차를 우회하여 정상적으로 접근 제한된 파일에 접근하려는 공격자의 시도를 감지합니다. 공격자는 URL의 '/../' 시퀀스를 사용하여 취약한 웹 서버의 디렉토리를 통과할 수 있습니다. 이로써 공격자는 누구든지 읽을 수 있거나 HTTP 프로세스 ID로 읽을 수 있는 대상 HTTP 서버의 모든 파일을 읽을 수 있습니다. 예를 들어 URL을 http://www.domain.com/..₩.. 형식으로 사용하면 누구나 웹 서버 컨텐츠 루트 디렉토리 밖의 파일을 검색하고 다운로드할 수 있습니다. http://www.domain.com/ scripts..₩..₩와 같은 URL 스크립트 이름을 통해 공격자는 대상 스크립트를 실행할 수 있습니다. 공격자는 이 디렉토리의 목록을 체계적인 공격 계획을 위한 추가 정보로 사용할 수 있으며, 파일 시스템 어디서든 파일을 다운로드할 수 있습니다.

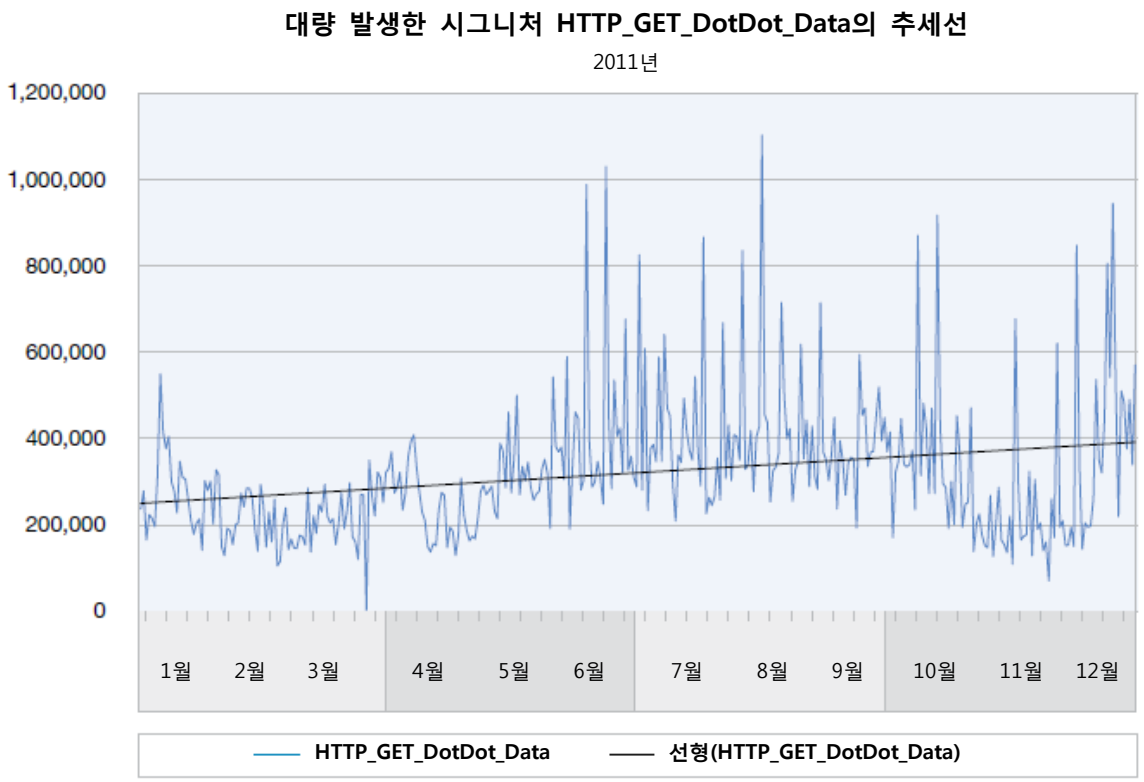


그림 5: 2011년에 대량 발생한 시그니처 HTTP_GET_DotDot_Data의 추세선(IBM MSS 통계)

XSS(Cross-Site Scripting) 공격

일반적으로 웹 애플리케이션을 공략하는 XSS 공격은 공격자가 클라이언트 측의 스크립트를 다른 사용자가 열람한 웹 페이지에 주입하는 공격 수법입니다. 이 공격 수법은 공격자가 접근 통제 수단을 우회하는 데 사용되기도 합니다. 이 공격 수법은 엄청나게 인기가 많으며 보안 위험 역시 상당히 높습니다. XSS 공격은 1990년대부터 인기를 끌어왔으며 가장 일반적인 유형의 웹 애플리케이션 취약점입니다. Cross_Site_Scripting 시그니처는 IBM X-Force의 2011년 대량 발생 시그니처 상위 10개 목록에서 8위에 올랐습니다. 이 시그니처의 위협이 줄어든 것은 HTML 입력 검사, 쿠키 보안, 클라이언트 측의 스크립트 비활성화와 같은 여러 가지 대책이 마련된 덕분입니다. 최근에는 위협을 줄이는 데 도움이 되는 새로운 기술(예: Mozilla의 컨텐츠 보안 정책(Content Security Policy), Javascript Sandbox 도구, 자동 종료 템플릿)이 개발되어 꾸준히 개선되고 있습니다.

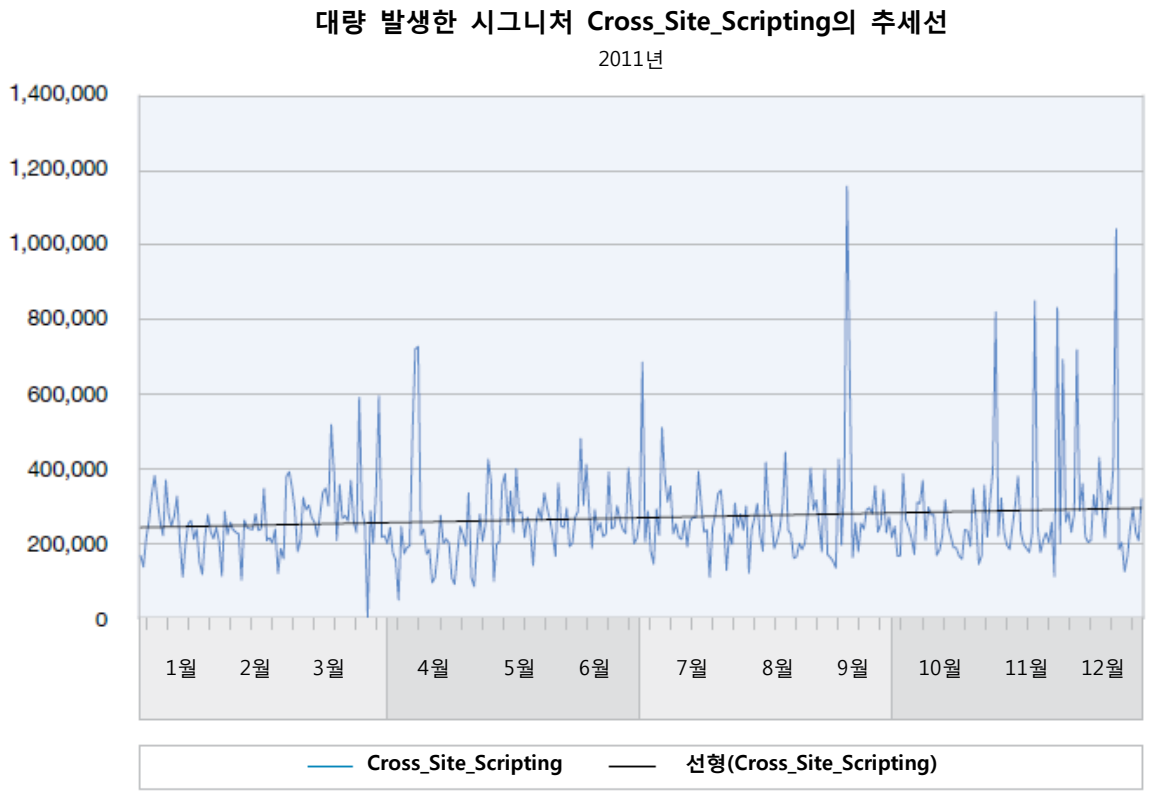


그림 6: 2011년에 대량 발생한 시그니처 Cross_Site_Scripting의 추세선(IBM MSS 통계)

무차별 인젝션 공격

SSH_Brute_Force 시그니처는 2010년 4위에서 7위로 세 단계 내려앉았습니다. 무차별 주입 공격은 공격자가 무수한 비밀번호 조합을 무작위로 입력해서 시스템에 무단 접속하는 공격 수법입니다. 이 시그니처는 정해진 시간 동안 SSH 서버에 입력되는 SSH 서버 ID가 과도하게 많은 경우 이를 감지합니다. 이 유형의 공격을 통해 악의적 공격자는 접속한 서버에서 중요 파일을 조회, 복사 또는 삭제하거나 악성 코드를 실행할 수 있습니다. 2011년에 IBM X-Force는 비밀번호가 취약한 SSH 서버를 찾기 위해 인터넷을 검사하는 활동을 꾸준히 관찰했습니다. 기업은 루트 계정에 대한 직접 접속을 차단하고, 추정하기 어려운 사용자 이름과 비밀번호를 사용하여 무차별 인젝션 공격을 방지해야 합니다.

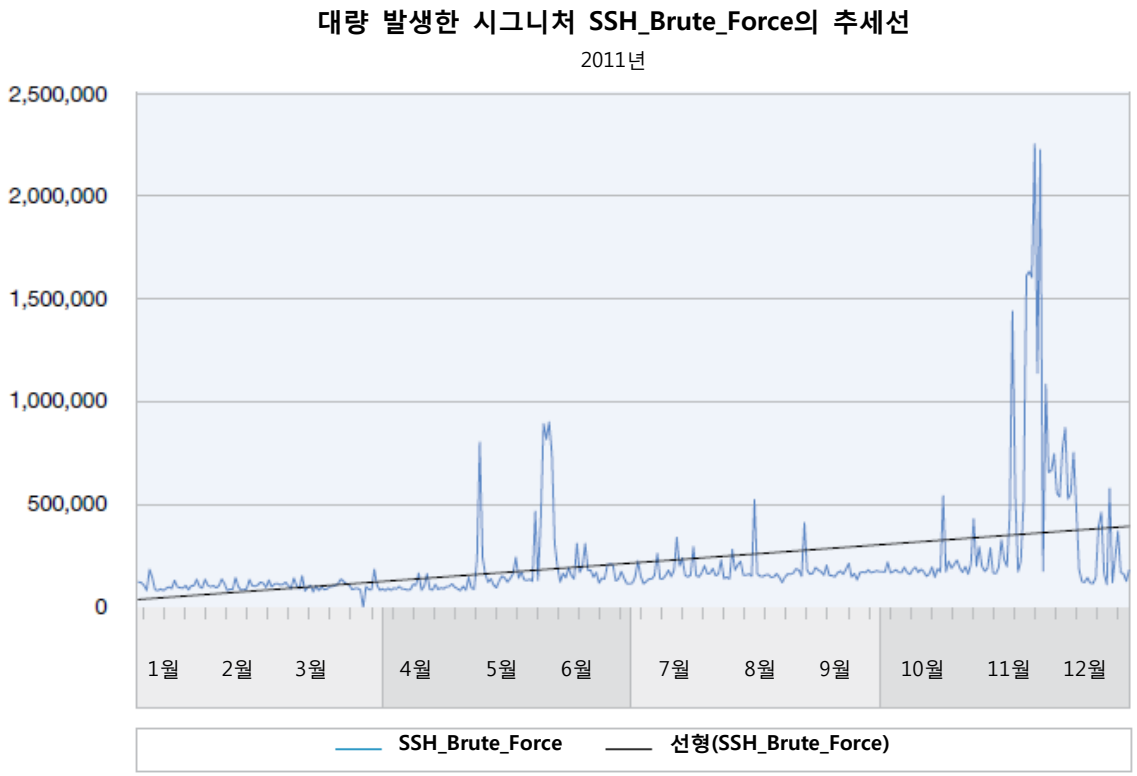


그림 7: 2011년에 대량 발생한 시그니처 SSH_Brute_Force의 추세선(IBM MSS 통계)

UNIX를 대상으로 한 공격

HTTP_Unix_Passwords 시그니처는 IBM X-Force의 2011년 대량 발생 시그니처 상위 10개 목록에서 여전히 건재하고 있고 꾸준히 증가세를 보이고 있지만 2010년에 6위였던 순위는 2011년에는 10위로 하락했습니다. 이 시그니처는 웹(HTTP) 서버를 통해 UNIX 시스템의 /etc/passwd 파일에 접근하려는 시도를 감지합니다. 인증을 받아서 파일에 접근하는 경우라도 상황에 따라 의심해 볼 필요가 있습니다. 이 수법은 대단히 고전적인 공격 수법이지만 오늘날에도 여전히 효과가 있습니다.

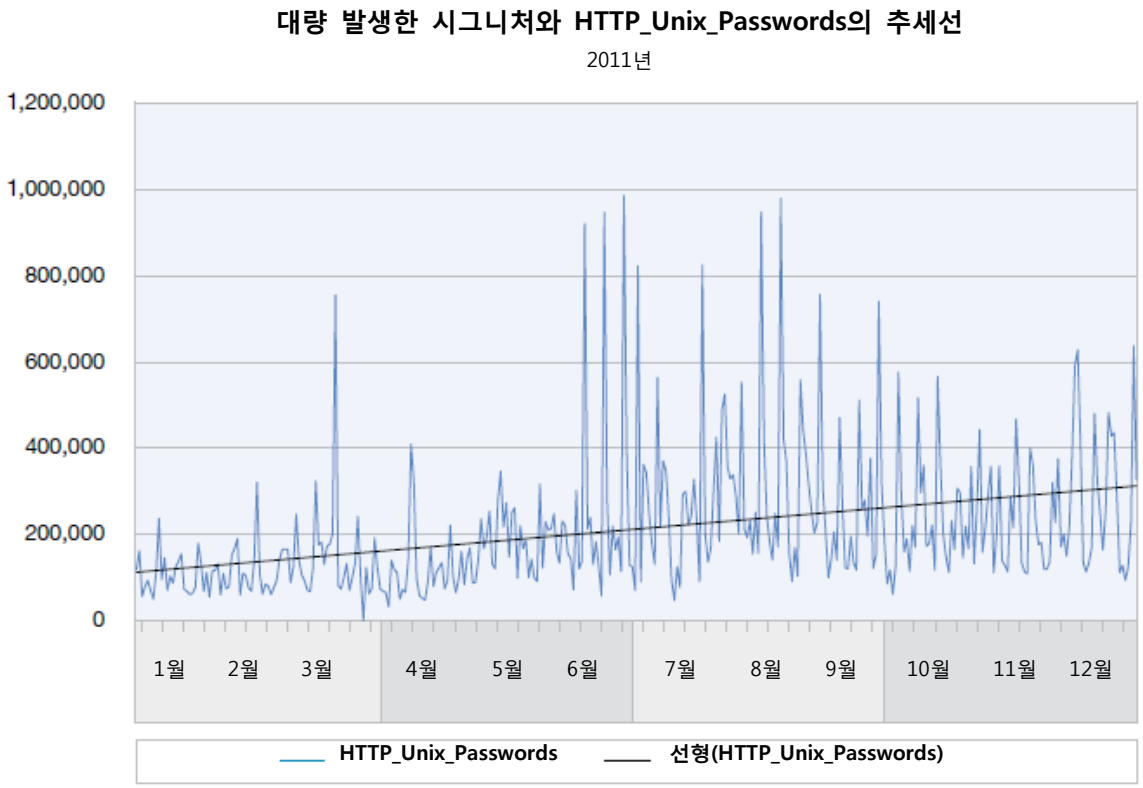


그림 8: 2011년에 대량 발생한 시그니처와 HTTP_Unix_Passwords의 추세선(IBM MSS 통계)

원격 명령어 인젝션 공격

IBM MSS는 전 세계의 원격 명령어 인젝션 공격 현황을 추적해 왔습니다. 이 취약점은 사용자 입력 정보가 적절히 삭제되지 않은 경우 시스템 쉘 명령어를 실행하는 함수(예: exec() 및 system()과 같은 PHP 함수)와 함께 악용됩니다. 공격자는 이 수법으로 웹 서버에서 명령어를 실행할 수 있습니다. 이 공격 수법은 아주 기초적이지만 SQL 인젝션 공격과 마찬가지로 애플리케이션 수준에서 적절한 보안이 마련되지 않은 경우 성공 확률이 높습니다.

IBM X-Force가 조사한 페이로드 중 다수는 웹 서버가 wget이란 명령어를 통해 원격 스크립트를 다운로드해서 임시(tmp) 디렉토리에 저장한 후 실행하는 방식으로 이뤄져 있습니다. 스크립트는 시스템에 원격 접속을 유지하면서 정보를 수집하고 지휘 통제 기능을 하다가 공격자의 서버로 다시 복귀하도록 설계됩니다. 그리고 나서 로컬 혹은 원격으로 Google을 통해 찾은 다른 서버를 검사해서 공격하는 데 이 서버가 사용됩니다. 이 공격 수법을 이용하면 매우 빠르고 효과적으로 수백 개의 취약한 웹사이트를 장악할 수 있습니다. 2012년에는 일부 봇넷이 진화하고 다른 공격자들도 저마다의 목적으로 이 취약점을 악용하기 시작하면서 원격 명령어 인젝션 공격이 꾸준히 증가할 것으로 예상됩니다.

passwd, wget, dir 등과 같은 자주 사용되는 다수의 쉘 명령어를 제거하도록 웹사이트에서 사용자 입력 정보를 삭제하는 것만으로도 효과적인 보호 조치가 될 수 있습니다.

또한 wget 명령어를 서버에서 삭제하면 최소한 공격자의 파상적인 공격을 확실히 막을 수 있습니다.

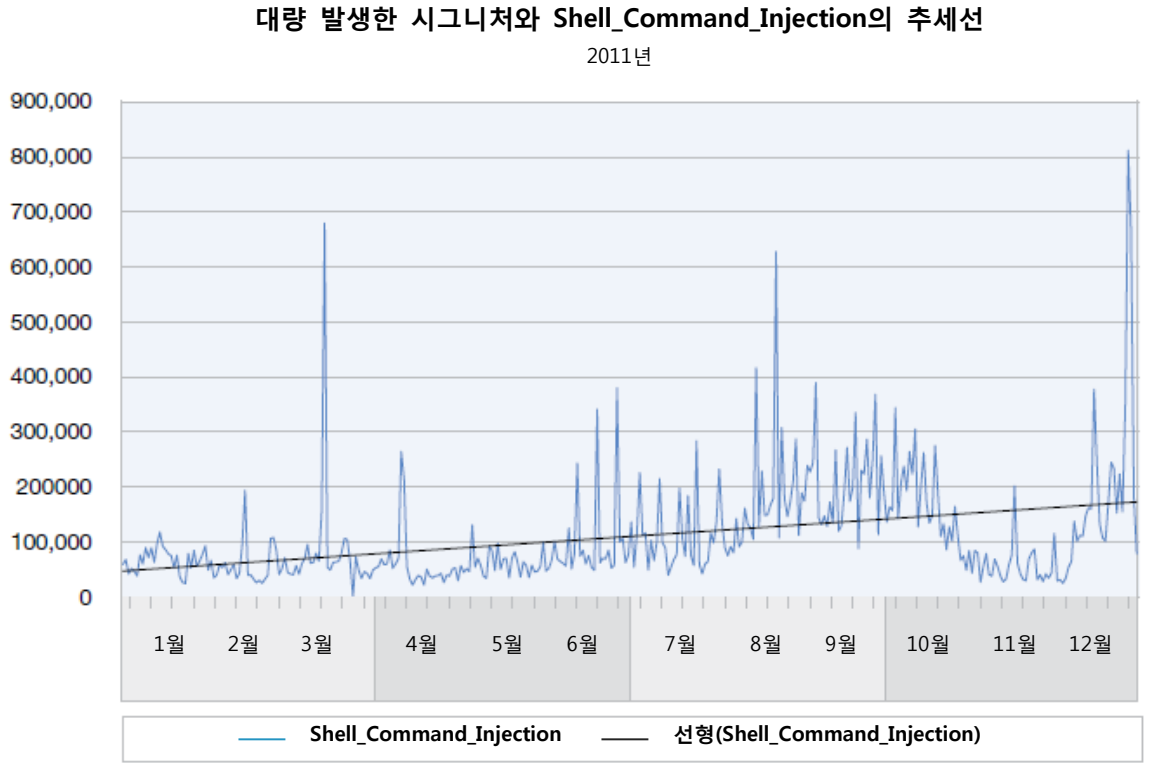


그림 9: 2011년에 대량 발생한 시그니처와 Shell_Command_Injection의 추세선(IBM MSS 통계)

내부 익명 프록시

X-Force Proxy_Bounce_Deep 시그니처는 클라이언트가 일련의 HTTP 프록시를 통해 웹사이트에 접속하려고 시도하는 상황을 감지합니다. 다른 여러 클라이언트로 연결된 네트워크에서 갑자기 일괄 처리 방식을 통해 이런 활동이 대대적으로 나타나는 경우가 있습니다. 다분히 편집증적으로 보일 수도 있는 이런 행위는 엄연히 합법적인 웹 서핑입니다. 때때로 공격자는 웹 서버를 대상으로 공격을 개시할 때 근거지 주소를 알기 어렵게 하기 위해 이 수법을 이용합니다. 지난 몇 년간 이런 용도로 사용될 수 있는 익명 프록시 개수가 인터넷에 급증했습니다. 이에 대한 자세한 내용은 이 보고서의 웹 컨텐츠 동향 > 익명 프록시 급증 항목을 참조하십시오.

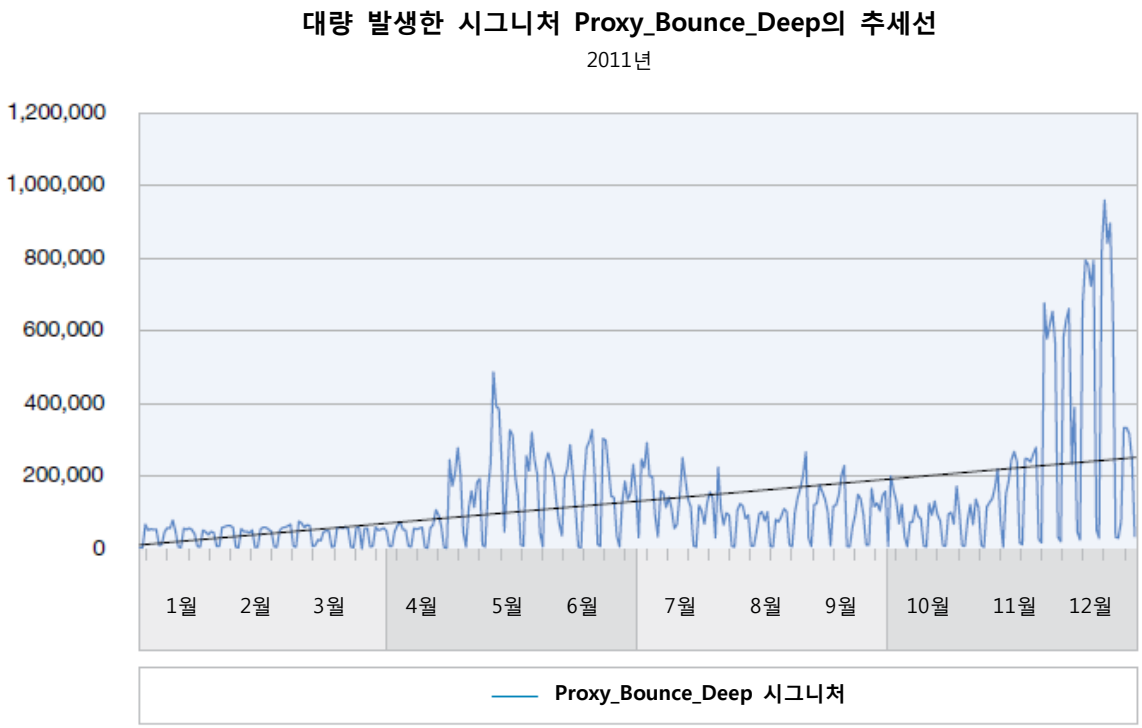


그림 10: 2011년에 대량 발생한 시그니처 Proxy_Bounce_Deep의 추세선(IBM MSS 통계)

여전히 활개를 치고 있는 SQL 인젝션 공격

SQL 인젝션 공격

1970년대에 처음 구상된 SQL(Structured Query Language)은 관계형 데이터베이스의 데이터를 관리하는 데 효과적인 언어입니다. 관계형 데이터베이스는 대규모 데이터 팜(data farm)에 사용할 목적으로 개발되었지만 인터넷의 양방향성과 짝을 이루면서 새로운 역할을 맡게 되었습니다. 검색 창, 계정 관리, 주문 추적 및 협업 도구는 이 두 가지 기술의 결합이 있기에 사용할 수 있는 기능입니다. 두 가지 기술 조합은 혁신을 창출했지만 효과적인 공격 수단이 되면서 데이터 유출 위험도 함께 나타나게 되었습니다.

지난 몇 년간 공격자들은 인터넷 검색 창과 웹 애플리케이션 프로그래밍 인터페이스에 특별한 포맷의 스트링을 사용해 왔습니다. 이 스트링은 SQL 선언문을 웹 애플리케이션 코드에 주입하는 방법으로 기본 데이터베이스를 조종하도록 설계되어 있습니다. SQL 인젝션으로 알려진 이 과정은 인증을 우회하여 데이터베이스의 비공개 컨텐츠에 접근하거나 데이터베이스를 관장하는 운영체제를 공략하는 데 사용될 수 있습니다.

데이터베이스 스키마와 웹 애플리케이션 코드가 사이트마다 다르기 때문에 SQL 인젝션 공격은 일단 특정 대상을 목표로 사용되었습니다. 그러다가 공격자가 취약한 웹 애플리케이션을 찾아낸 이후부터 공을 들여 제작한 쿼리를 이용해서 데이터베이스를 장악했습니다. 테이블 및 필드 이름을 확보한 공격자는 정보에 접근하고 권한 허용 문제를 조사할 수 있었던 것입니다. 이 공격은 느리고 특정 대상을 목표로 하며 그 과정은 비교적 수동으로 이뤄졌습니다. 특정 대상을 노린 이런 유형의 공격은 여전히 존재합니다. HBGary Federal CEO Aaron Barr는 자사의 웹사이트에 SQL 인젝션 공격을 감행한 해커 단체인 Anonymous의 고위 간부의 신원을 파악했다고 발표했습니다. Anonymous는 이에 대한 보복으로 HBGary Federal 네트워크를 송두리째 유린하면서 민감한 데이터가 노출되고 Aaron Barr가 사임하는 파국으로 치달았습니다. Sony가 사상 최대 규모의 고객정보 유출 사고가 발생한 이후에서 자사의 네트워크에 문제가 없었다고 발표했을 때 또 다른 해커 단체인 LulzSec은 맞불작전으로 SQL 인젝션 공격을 이용해서 빼낸 15,000명의 고객정보를 인터넷에 게시했습니다.

2008년 초에 기본 데이터베이스 구조나 웹 애플리케이션 코드를 몰라도 되는 새로운 SQL 인젝션 공격 수법이 등장했습니다. 공격자는 데이터베이스에 저장된 데이터에 접근할 필요 없이 스크립트를 주입해서 데이터베이스가 스크립트를 실행하도록 조작할 수 있었습니다. 이런 유형의 공격은 취약한 서버를 찾기만 하면 공격 준비가 끝난 셈이었기 때문에 자동화가 대단히 쉬웠습니다. 그리하여 최초의 대규모 SQL 인젝션 공격 수법이 등장한 것입니다. 이런 유형의 공격은 일반적으로 데이터베이스의 컨텐츠를 노리기 보다는 루트 접속 권한을 획득하거나 웹 서버를 이용해서 사이트에 접속하는 사용자를 공격하는 데 그 목적이 있습니다. 이런 목적은 XSS 취약점 혹은 다른 악성 컨텐츠를 웹 애플리케이션이나 웹 애플리케이션의 캐시에 주입하는 방법으로 달성할 수 있습니다.

이 공격의 특징은 스크립트와 함께 스크립트를 실행할 EXEC 선언문을 삽입할 목적으로 DECLARE 선언문이 포함된 SQL 인젝션 공격을 시도한다는 점입니다. IBM MSS의 조사에 따르면 그림 11에 보이는 것처럼 2011년에 이런 유형의 공격 빈도가 크게 늘었는데, 악성 코드가 설치된 jjghui와 다른 변종 사이트가 ASP.NET 사이트들을 무차별적으로 공격했던 하반기에 특히 증가세가 두드러졌습니다. Jjghui는 특정 웹사이트로 트래픽을 리디렉션한 후 그 사이트를 참조하는 SQL 대량 인젝션 공격 사이트입니다.

스크립트를 실행하는 페이로드에 기본 데이터베이스 구조에 대한 몇 가지 정보를 조합한 새로운 대량 인젝션 수법이 2011년에 등장했습니다. 이 공격 수법은 그 해 3월에 LizaMoon 공격으로 처음 알려졌습니다. 이 공격 수법은 모호한 DECLARE 및 EXEC 명령어 대신 UPDATE 및 REPLACE 명령어를 유효 테이블에 사용합니다. 이 공격은 준비하는 데 더 많은 공을 들여야 하지만 (URL을 위장한 경우 특히) 단순한 패턴 매칭 기술(pattern matching)로 감지하기가 상대적으로 더 어렵습니다.

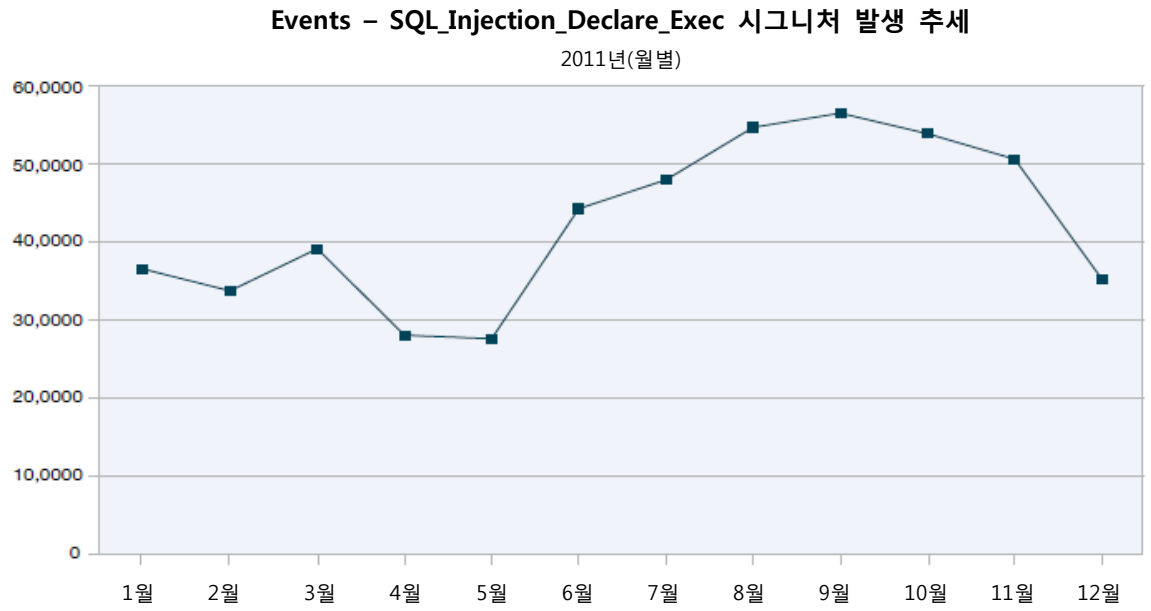


그림 11: 2011년 Events – SQL_Injection_Declare_Exec 시그니처 발생 추세(월별)

위협 유형

SQL 인젝션 공격은 오래 전부터 사용되어 왔지만 여전히 인터넷에서 가장 보편적으로 사용되는 공격 수법입니다 SQL 인젝션 공격은 성공을 거두는 경우가 빈번하나 일반적으로 모든 사용자 입력 정보를 삭제하고 데이터베이스에 보안 체제를 구축하면 막을 수 있습니다. 보안 측면에서 이런 유형의 공격에 취약한 시스템은 두 가지 종류가 있습니다. 기업이 알고 있는 웹 연결 방식의 데이터베이스, 그리고 기업이 모르고 있는 웹 연결 방식의 데이터베이스입니다. 네트워크에는 로그인 계정, 직원 서비스, 온라인 상점, 혹은 대중에게 공개된 사이트가 제공되는 웹 페이지가 있습니다. 이런 웹 페이지가 바로 기업이 알고 있는 사이트에 해당됩니다. 이 사이트에는 사용자 계정, 신용카드 번호 혹은 고객 연락처 정보와 같은 민감한 정보가 포함되어 있는 경우가 많습니다. 이런 종류의 정보가 저장된 데이터베이스가 사용자 웹 서버와 소통하는 경우 기업은 데이터의 보안을 확보하는 데 필요한 조치를 취하기 마련입니다. 하지만 그것으로 충분할까요?

일반적으로 기업은 웹사이트를 처음 제작해서 배치할 때 안전한 코딩 정책을 시행하고 철저한 보안 검토를 거치게 됩니다. 그러나 시간이 지나면서 여러 가지 취약점이 생겨날 수 있습니다. 가령, 새 기능을 배치할 때 코드에 대한 검토가 제대로 이뤄지지 않을 수 있습니다.

혹은 스크립트나 소프트웨어 애플리케이션을 새로 추가할 때 취약점에 대한 조사와 테스트가 미흡한 경우도 있습니다. 그리고 새 테이블과 필드를 데이터베이스에 추가할 때 적절하지 않은 접근 권한이 설정될 가능성도 배제할 수 없습니다. 개발자를 새로 채용할 때 웹 프로그래밍 보안에 대한 교육을 실시하고 있습니까? 기밀 정보가 유출될 경우 심각한 파장이 일 수 있습니다. 비단 직접적인 금전적 손해 말고도 고객과의 신뢰 문제가 발생할 수도 있습니다.

기업이 알고 있는 서버 외에도 기업이 모르고 있는 서버가 자사의 네트워크에 존재할 수도 있습니다. 오픈 소스 데이터베이스와 웹 도구가 등장하면서 데이터베이스 및 웹 서버의 통합이 상당히 간편해졌습니다. 웹 애플리케이션에 대한 새로운 아이디어가 있고 조사에 충분한 시간을 할애할 의향이 있는 사람이라면 누구나 Apache 웹 서버, MySQL 또는 Postgres 데이터베이스, 그리고 커뮤니티 지원 방식의 웹 코드를 이용해서 웹 애플리케이션을 구축할 수 있게 되었습니다. 이런 일반적인 사내 애플리케이션으로는 지식 기반, 협업 도구, 티켓 추적 및 테스트 도구를 예로 들 수 있습니다. 이런 애플리케이션을 이용하면 혁신을 이룰 수 있을 것입니다. 하지만 애플리케이션 개발자들은 웹 개발 환경의 보안에 대한 교육을 제대로 받지 못하는 경우가 종종 있습니다.

모범 사례를 익힐 수 있는 자원은 많지만 단기 근무제로 일하는 웹 개발자는 보안보다 기능에 더 관심을 기울이는 게 일반적입니다. 웹 개발자에게 적절한 교육이 실시하지 않는다면 SQL 인젝션 공격의 가능성을 인지하지 못할 수 있습니다. 또한 경험이 미숙한 개발자일수록 미리 제작된 모듈을 다운로드하거나 샘플 코드를 복사할 가능성이 높아지는데 그로 인해 대량 인젝션 공격의 피해를 입을 가능성 역시 크게 높아질 수 있습니다.

이런 유형의 시스템에는 신용카드 번호와 같은 정보가 보관되어 있을 가능성이 상대적으로 적지만 그렇다고 민감한 데이터가 아예 존재하지 않는 건 아닙니다. 데이터베이스에 민감한 정보가 저장되어 있지 않더라도 데이터베이스 사용자 이름과 비밀번호는 저장되어 있을 수 있습니다. 데이터베이스 접근 권한을 지나치게 관대하게 설정해둔 경우 공격자가 데이터베이스를 운용하는 시스템에 대한 루트 접속 권한을 확보할 수도 있습니다. 네트워크에서 교두보를 마련한 공격자는 한발 더 나아가 더욱 큰 목표를 공격할 수 있습니다. 또한 공격자가 봇넷을 설치하거나 이미 장악한 네트워크를 이용해서 다른 네트워크를 공격할 가능성도 있습니다.

코드 보호 방안

다른 취약점과 마찬가지로 SQL 인젝션 공격을 막는 가장 효과적인 방법은 계층적 방어입니다. 웹 애플리케이션 코드는 SQL 인젝션 공격의 진입점으로 악용될 수 있기 때문에 1차 방어선이라 할 수 있습니다. 웹 애플리케이션 코드로부터 데이터베이스를 보호하려면 다음과 같은 조치가 필요합니다.

- 사용자 입력 정보에서 SQL 이스케이프 문자(escape character)와 불필요하게 보존된 문자를 모두 삭제하십시오. 본인이 직접 삭제하려고 시도하지 말고 선호하는 프로그래밍 언어가 제공하는 검증된 라이브러리를 이용할 것을 권장합니다. 위험한 문자를 인코딩하는 방법이 아주 다양하기 때문에 그것들을 모두 아는 사용자는 많지 않을 것입니다.
- 사용자가 반환한 인코딩 및 데이터 유형을 검사하십시오. 가령, 정수가 예상될 경우 검사했을 때 정수 결과가 나와야 정상입니다.
- 사용자 입력 정보가 직접 데이터베이스와 교류하지 못하게 하십시오. 사용자 입력 정보를 삭제한 경우라도 SQL 선언문에 그 데이터가 포함되지 않아야 합니다. 그 대신, 사전 정의된 선언문, 매개변수화 된 선언문 혹은 저장된 프로시저를 이용해서 SQL 코드를 사용자가 입력하는 데이터와 격리하십시오.
- 절대로 사용자에게 디버그 정보를 반환하지 말고, 로컬로 저장하십시오.

- 현재 사용 중인 프로그래밍 언어, 서버 프레임워크 또는 상용 소프트웨어에 알려진 취약점이 존재하지 않는지 정기적으로 검사하십시오.

모든 사용자 입력 정보를 삭제하고 나면 공격자가 데이터베이스에 침투할 수 있는 길을 차단해야 합니다. 하지만 검사하지 않은 필드가 하나만 존재해도 공격자에게 침입할 수 있는 여지를 주는 셈이라서 이 방법만으로 무조건 안전해진다는 보장은 없습니다. 따라서 웹 애플리케이션의 코드를 수정하는 모든 사람에게 안전하게 프로그래밍하는 방법에 대한 교육을 실시해야 합니다. 코드에 접근할 수 있는 조건을 정하거나 정기적으로 코드 보안의 중요성에 대한 의식 강화 교육을 실시하는 것도 좋은 방법입니다.

최고의 개발자조차 서두르다가 실수를 범하거나, 사소한 수정 작업을 대수롭지 않게 여길 수 있습니다. 이런 실수를 막는 최상의 방법은 동료 간의 코드 교차 검토입니다. 또 다른 두 개의 눈이 더해진다면 간단한 실수를 줄이는 데 큰 도움이 될 것입니다. 신기술 배치, 대대적인 기능 추가 혹은 민감한 데이터가 저장된 시스템에 대한 상당한 수준의 수정 작업을 실시할 때는 애플리케이션을 일반에게 선보이기에 앞서 외부에 코드 검토를 의뢰하거나 침입 테스트를 수행하는 방안을 고려할 필요가 있습니다.

서버 보호 방안

2차 방어선은 데이터베이스와의 연결 방법입니다. 다음과 같은 조치를 취할 것을 권장합니다.

- 웹 애플리케이션이 루트 계정이나 슈퍼유저 계정을 사용하지 못하도록 설정하십시오.
- 데이터베이스 서버에 접속하는 데 사용하는 계정의 접근 권한을 가장 엄격한 수준으로 제한하십시오. 데이터베이스가 반드시 접근해야 하는 필드에 대해서만 접근을 허용하고 쓰기 허용 역시 필요한 필드로 제한하십시오.
- 기본 계정, 샘플 코드, 테스트 애플리케이션이 데이터베이스 서버에 설치되어 있는 경우 모두 삭제하십시오. 사용하지 않는다면 굳이 남겨둘 이유가 전혀 없습니다.
- 강력한 비밀번호 조합을 사용하고 절대로 비밀번호를 평문으로 저장하지 마십시오.
- 데이터베이스 및 웹 애플리케이션 로드를 정기적으로 검사해서 미심쩍거나 반복적인 오류가 발생하고 있는 건 아닌지 확인하십시오.
- 침입을 막거나 침입 사실을 통지 받을 수 있도록 데이터베이스 또는 로그 모니터링 소프트웨어를 사용하는 방안을 고려하십시오.

데이터베이스 서버를 적절히 구성하면 데이터 및 루트 시스템 공격을 막는 데 큰 도움이 됩니다. 데이터가 비교적 민감하지 않은 경우라도 웹 서버와 소통할 때는 데이터베이스의 보안을 가장 중시해야 합니다. 따라서 정기적으로 데이터베이스의 접근 권한을 검토하고 불필요한 계정이 있는지 확인해서 삭제해야 합니다. 이렇게 하지 않으면 필드와 테이블을 새로 추가할 때 보안에 구멍이 생기기 쉽습니다.

공격자가 SQL 인젝션 공격을 감행해서 충분한 접근 권한을 획득한 경우 운영체제의 보안이 최종 방어선 역할을 하게 됩니다. 시스템 보안을 위해 취할 수 있는 조치는 다음과 같습니다.

- 데이터베이스와 웹 서버의 계정 및 파일 시스템에 대한 접근 권한을 철저히 통제하십시오.
- 침입 시도를 감시하는 호스트 기반의 침입 탐지 및 방어 시스템를 구축하십시오.
- 바이러스 예방 및 악성 코드 감지 소프트웨어를 이용해서 봇넷 감염을 감시하십시오.
- 미심쩍은 징후가 보이는지 알 수 있도록 웹 애플리케이션, 웹 서버 및 데이터베이스 로그를 모니터링하십시오.

네트워크 보호 방안

이전 단원에서 권장한 조치를 취하면 SQL 침입으로부터 서버를 지속적으로 보호하는 데 도움이 될 것입니다. 하지만 서버에 대한 접근을 통제하는 것만으로는 SQL 침입으로부터 네트워크를 보호하기에 충분하지 않을 수도 있습니다. 네트워크에 보호 받지 않거나 알 수 없는 서버가 존재할 경우 공격의 온상이 될 수 있습니다. 방화벽과 네트워크 기반의 침입 방지 또는 탐지 기능을 적절히 사용하면 이런 허점을 메우는 데 도움이 될 수 있습니다. 또한 인증 받은 서버를 제외한 다른 서버로부터 인바운드 웹 요청을 차단하면 사내 애플리케이션을 외부 공격으로부터 보호하는 데 도움이 될 수 있습니다. 웹 애플리케이션 방화벽이나 프록시 기반의 방어망을 이용해서 네트워크에 유입되는 웹 트래픽을 통제하는 방법도 고려해 볼만합니다. 또한 대표적인 네트워크 기반의 침입 방지 솔루션 제공업체들은 모두 일정 수준의 SQL 침입 탐지 기능을 제공하고 있습니다. 탐지 방법은 침입 방지 솔루션 제공업체마다 다르며 지원 범위도 알려진 공격 스트링에 대한 간단한 정규식 대조부터 복잡한 스코어링 알고리즘(scoring algorithm)에 이르기까지 다양합니다. 다음과 같은 조치를 통해 SQL 침입으로부터 네트워크를 보호할 것을 권장합니다.

- 이용 중인 솔루션 제공업체가 제공하는 SQL 인젝션 시그니처에 대한 설명을 꼼꼼히 읽으십시오. 일부 시그니처는 대단히 한정적이라서 정해진 환경에서만 가동되는 반면, 일부 시그니처는 훨씬 광범위해서 잘못된 오탐(false positive) 반응을 유발하기 쉽습니다. 따라서 각 경보에 어떤 기준이 적용되는지 알 필요가 있습니다.
- 침입 방지 시스템은 여러 가지 현상을 SQL 침입으로 오인하는 경우가 있습니다. 예를 들어, 검색 결과, YQL(Yahoo Query Language), FQL(Facebook Query Language), Twitter 피드를 이따금 SQL 침입으로 오인해서 잘못된 오탐 반응이 발생할 수 있습니다. 동일한 주소에서 많은 이벤트가 유입될 경우 아웃바운드 SQL 인젝션 이벤트가 우려될 수 있으나, 사용자가 실행한 이벤트 때문에 여러 SQL 침입 시그니처에서 잘못된 오탐 반응이 발생하는 경우도 흔합니다. 인바운드 SQL 인젝션 공격이 네트워크를 노릴 수 있기 때문에 이런 시도에 더 관심을 기울여야 합니다.
- 주기적으로 네트워크를 검사해서 알 수 없는 웹 서버가 존재하는지 확인해야 합니다. 알 수 없는 웹 서버가 존재할 경우 소유자를 추적해서 SQL 인젝션 공격을 막을 조치가 취해진 상태인지 확인하십시오. 또한 침입 테스트를 외부에 의뢰하거나 SQL 인젝션 공격에 취약한 사이트를 찾아내도록 특별히 설계된 소프트웨어를 구매하는 방안도 고려해보십시오.
- 잠재적 보안 문제를 파악할 보안 정책 지침을 마련하고 솔루션을 확보하십시오.

네트워크 보호만으로는 충분하지 않지만 보안 침입을 조기에 인지해서 해결한다면 공격자가 입힐 수 있는 피해를 최소화할 수 있습니다. 민감한 데이터가 저장되지 않은 시스템에는 이런 대비책이 특히 중요합니다. 왜냐하면 민감한 데이터가 포함되지 않은 시스템은 비교적 보안이 취약하기 마련이기 때문입니다. 시스템 자체가 중요하지 않더라도 네트워크 루트 수준의 침입은 큰 위험 부담이 따릅니다.

결론

적절한 예방책이 마련된 경우 SQL 인젝션 공격의 성공 확률이 낮아집니다. 그러나 새로운 비즈니스에서는 새로운 기능과 기술을 필요로 하는 경향이 있기 때문에 항상 경계를 늦추지 말아야 합니다. 웹 애플리케이션에 연결된 데이터베이스를 설치하거나 코드 개편 작업을 진행할 때마다 위험이 수반된다는 점을 염두에 둬야 합니다. 수정된 모든 코드는 철저히 검사하고, 웹 개발자를 대상으로 꾸준히 교육을 실시해야 합니다. 공격자가 삭제되지 않은 사용자 입력 정보를 입수하는 데 성공할 경우 지속적으로 SQL 인젝션 공격을 시도할 가능성이 높습니다. 따라서 봇넷 주입 방식의 대량 인젝션 공격을 통해 누군가가 자사의 사이트를 노릴 확률이 거의 100%라고 해도 과언이 아니므로 철저히 대비해야 합니다.

SQL 인젝션 공격으로부터 서버를 보호하는 방법에 대한 자세한 내용을 보려면 아래 홈페이지를 방문하십시오.

Java 보안:
http://today.java.net/pub/a/today/2005년/09/08/handling-java-web-app-input.html

ASP.NET 보안:
http://msdn.microsoft.com/en-us/library/ff648339.aspx

PHP 보안:
http://php.net/manual/en/security.database.sql-injection.php

데이터베이스 보안 팁:
http://en.wikipedia.org/wiki/Database_security

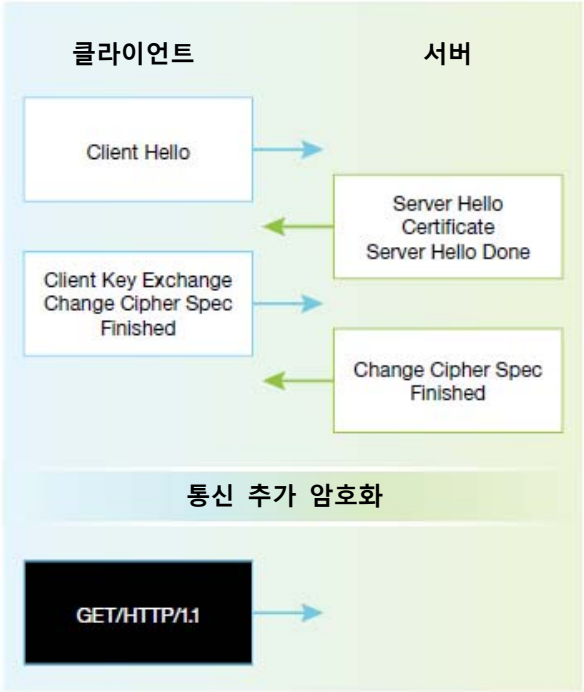
SSL 보안의 당면 과제

2010년에 Firesheep 플러그인이 등장하면서 HTTP가 본질적으로 보안에 취약하다는 사실과 민감한 개인정보를 다루는 유명 웹사이트에 얼마나 만연되어 있는지 입증되었습니다. 이에 대한 대응책으로 Facebook 및 Twitter와 같은 웹사이트는 HTTPS를 도입하여 사용자의 보안과 프라이버시를 강화했습니다. 그 과정을 비추어 보면 2011년에 HTTPS를 지원하는 SSL 및 TLS 프로토콜과 관련된 다수의 심각한 문제가 해소될 것이란 기대와 달리 결과는 다소 실망스러웠습니다. 이번 절에서는 2011년에 SSL 및 TLS 프로토콜에 영향을 미친 주요 사건 세 가지와 두 프로토콜이 위협 상황에 미친 영향을 면밀히 살펴보겠습니다.

THC-SSL-DOS

2011년 2월(이후 10월 말에도 다시 한 번 세간의 화제가 되었습니다)에 보안 단체인 The Hacker's Choice는 SSL/TLS를 통해 통신하는 서버에 DoS(denial of service) 공격을 감행할 수 있는 개념 증명 도구를 공개했습니다. 이 도구는 일반적인 방식으로 연결된 랩탑 컴퓨터를 악용해서 기업의 웹 서버를 마비시킬 수 있다는 것을 입증했습니다. 공격 원리는 TLS 핸드쉐이크(handshake)가 진행되는 동안 암호화를 실시하는 데 필요한 컴퓨팅 자원의 암묵적 비대칭성을 악용하는 것입니다.

TLS 핸드쉐이크



보편적인 TLS 핸드쉐이크가 진행되는 동안에는 여러 가지 일이 발생합니다. 먼저, 지원되는 일련의 암호 세트(cipher suite)를 나열하는 'Client Hello' 메시지를 클라이언트가 서버에 전송하여 핸드쉐이크를 시작합니다. 그러면 서버가 'Server Hello' 메시지로 응답하여 통신 암호화 목적으로 선택한 암호 세트를 알려줍니다. 또한 서버는 동일한 패킷에 신원을 증명하고 암호화용 공개 키를 제공하는 사이트의 인증서가 포함된 'Certificate' 메시지를 추가합니다.

제공된 정보가 클라이언트에 부합한 경우 클라이언트는 'Client Key Exchange' 메시지로 응답합니다(그 뒤에 'Change Cipher Spec' 메시지와 'Finished' 메시지를 전송합니다). 'Client Key Exchange' 메시지에는 서버 인증서의 공개 키로 암호화된 PMS(pre-master secret)가 포함되어 있습니다. 서버가 'Client Key Exchange' 메시지를 수신한 즉시 개인 키로 PMS를 해독합니다(그리고 나서 'Change Cipher Spec' 메시지와 'Finished' 메시지를 전송합니다). 이 시점에서 클라이언트와 서버는 마스터 키를 생성하고 암호화를 시작하여 나머지 세션에 사용합니다.

핸드쉐이크와 그 이후의 트래픽 대칭 암호화에서 'Client Key Exchange' 메시지에 포함된 PMS를 암호화 및 해독하는 데 '계산 비용(computational cost)'이 가장 많이 증가합니다. 클라이언트와 서버 모두 RSA 알고리즘을 사용하지만 서버의 계산 비용이 더 많아서 작업에 따라 훨씬 더 많은 계산 비용을 사용하기도 합니다(예: RSA 키 길이). 이런 원리를 좀 더 자세히 다루는 것도 흥미로울 테지만 주제를 벗어나므로 이만 생략하겠습니다.

이 도구는 클라이언트의 암호 세트 재교섭 시작 속성을 악용하여 서버를 마비시키는 데 특히 효과적입니다. TLS 프로토콜에는 사용되는 암호 세트를 암호화된 채널의 한쪽 끝에서 재교섭할 수 있는 기능이 포함되어 있습니다. 재교섭은 본질적으로 또 한 차례의 핸드쉐이크를 유발하는데 이 때에도 동일한 계산 비용이 사용됩니다. 클라이언트의 암호 세트 재교섭 시작 속성을 이용할 경우 한 대의 서버로 요청 가능한 최대 속도로 클라이언트가 TLS 핸드쉐이크를 실시하도록 유도할 수 있습니다. 게다가 재교섭을 이용하면 적은 수의 시스템으로도 공격이 가능하기 때문에 일반적인 DDoS(Distributed Denial of Service) 연결 임계값의 '레이더망'을 피할 수 있습니다.

완화

이런 악용의 영향을 줄일 수 있는 방법은 다양하지만 완벽하게 막을 수 있는 '특효약'은 존재하지 않습니다. 가장 간단한 방법은 클라이언트의 재교섭 시작을 비활성화하는 것입니다. 웹사이트 중 99%는 이 기능을 지원할 필요가 없습니다. 따라서 굳이 필요하지 않다면 비활성화해야 합니다. 기존의 TLS 메시지 가로채기(man-in-the-middle) 취약점(CVE-2009-3555) 때문에 다수의 웹 서버가 이 기능을 비활성화하도록 기본 설정된 상태입니다.

모든 암호 세트가 RSA 알고리즘처럼 서버 측의 계산 비용을 유발하는 건 아닙니다. 유감스럽게도 모든 브라우저가 이 암호 세트를 지원하는 건 아니며 모바일 디바이스처럼 비교적 성능이 미흡한 클라이언트에서는 브라우저를 사용하기 부적합할 수도 있습니다. 특히 TLS 1.1 및 1.2에는 RSA가 의무적으로 지원돼야 한다는 점을 고려하면 RSA 알고리즘 지원 여부는 임의대로 결정할 수 있는 사안이 아닙니다.

클라이언트 재교섭 시작 설정이 비활성화된 경우 클라이언트 10,000대로 한 번의 핸드쉐이크를 수행하여 클라이언트 한 대로 수행한 10,000번의 핸드쉐이크와 동일한 계산 비용 효과를 달성할 수 있습니다. 이런 수법이 바로 전통적인 DDoS 공격입니다. DDoS 공격의 피해는 기존의 예비용 침입 탐지 시스템(IDS)을 사용하거나 하드웨어를 추가로 투입해서 줄일 수 있습니다.

TLS/SSL 프로토콜에 특정 암호 세트를 사용할 경우 계산의 비대칭도가 수정되지 않는다는 점에 주목할 필요가 있습니다. 클라이언트가 더 많은 작업을 수행하도록 요구하는 '클라이언트 퍼즐(client puzzle)' 프로토콜을 통해 클라이언트 측에 계산의 비대칭도를 강제 적용할 수 있습니다. Eric Rescorla가 한 블로그 게시판에서 이 문제를 지적했듯이 "DoS 공격자는 일반적으로 봇넷(즉, 다른 사람들의 취약한 컴퓨터)를 이용해서 공격을 시작하므로 대단히 많은 수의 CPU를 이용할 수 있습니다. 그런 점 때문에 공격자가 도저히 풀 수 없는 퍼즐을 만들어서 모바일 디바이스처럼 계산 자원이 적은 디바이스 사용자에게 심각한 영향을 주지 않은 채 공격 위험을 줄이기가 대단히 어렵습니다."[4]

BEAST

9월 23일에 보안 연구원 Juliano Rizzo와 Thai Duong은 Ekoparty 보안 컨퍼런스 참석자들 앞에서 클라이언트 HTTPS를 통해 paypal.com에 연결된 클라이언트의 세션 쿠키 암호를 해독하는 공격을 시연했습니다. 시연에는 BEAST(Browser Exploit Against SSL/TLS)라는 도구가 사용되었습니다. 공격 수법은 CBC(Cipher Block Chaining) 모드를 사용할 때 암시적 IV(Initialization Vector)를 이용하는 SSL 3.0과 TLS 1.0의 오래 전부터 알려진 취약점을 악용하는 것입니다. 이 취약점은 이미 오래 전부터 알려졌지만 두 연구원이 현실적으로 공격이 가능하다는 사실을 입증하기 전까지만 해도 가설에 불과하다는 게 지배적인 시각이었습니다.

앞에서는 키 교환 알고리즘을 중심으로 TLS 핸드쉐이크의 암호 세트를 설명했지만, 암호 세트는 TLS 고정 연결 상태에서 데이터를 암호화하는 데 사용되는 대량 암호화 알고리즘을 정의하는 역할도 합니다. TLS는 두 부류의 대량 암호화 알고리즘(스트림 암호(stream cipher), 블록 암호(block cipher))를 지원합니다. 그리고 CBC 모드에서 실행되는 건 블록 암호입니다.

블록 암호의 암호화 원리는 평문(plain text)을 고정 크기의 개별 블록들로 나눈 다음 블록을 암호화하는 것입니다. CBC 모드에서는 한 블록의 평문이 이전 블록의 암호문과 배타적 논리합(XOR)을 이룬 다음 암호화됩니다. 그러나 암호화될 첫 번째 블록에 선행하는 암호문이 없기 때문에 IV를 대체해야 합니다. 취약점은 새 레코드를 암호화할 때 SSL/TLS 버전이 마지막 블록에 존재하는 암호문의 암시적 IV를 이용하는 방법에 있습니다.

공격자가 공격에 성공하려면 몇 가지 요건을 충족해야 합니다. 첫째, 공격자가 클라이언트의 암호화된 HTTPS 데이터를 모니터링할 수 있어야 합니다. 둘째, 공격자가 여러 개로 나뉜 채 URL 경로와 같은 HTTPS 채널을 통해 클라이언트로부터 전송된 평문과 마지막으로 암호화된 블록의 평문을 제어할 수 있어야 합니다. 첫 번째 요건은 자동 다운로드 수법보다 더 어렵기 때문에 충족하기가 거의 불가능합니다. 인터넷 사용자들이 중계소를 신뢰하지 않지만 그렇다고 해서 무방비 상태의 무선 네트워크를 무턱대고 이용할 수는 없는 노릇이기 때문에 TLS/SSL 프로토콜이 존재합니다.

4 http://www.educatedguesswork.org/2011년/10/ssltls_and_computational_dos.html

보안 연구원들은 두 번째 요건을 충족하여 트래픽을 조작하고 쿠키를 추가할 수 있는 Java 및 Silverlight와 같은 다수의 보편적 기술을 문제로 삼았습니다. 한 출처(예: http://www.attacker.com)의 애플릿(applet)이 다른 출처(예: https://www.paypal.com)로 요청을 전송할 수 있는 Java 플러그인의 동일 출처 정책(SOP) 검사의 취약점을 활용하는 방법으로 두 번째 요건을 손쉽게 충족한다는 사실이 시연을 통해 입증되었습니다.

이 수법을 이용해서 공격자는 평문의 알 수 없는 부분들을 한 번에 1바이트씩 손쉽게 해독할 수 있습니다. 가령, 공격자가 평문의 1바이트를 제외한 전부를 이미 알고 있는 경우 필요한 블록을 전송하라고 클라이언트가 요청하도록 조작할 수 있습니다. 그리고 나서 전송 중인 암호화된 블록을 가로채서 기억해두고 알 수 없는 바이트가 무엇일지 추측한 후, 다음 레코드에 IV(Initialization Vector)로 사용되도록 레코드 끝에 배치합니다. 평균적으로 이런 시행착오를 126번 반복하면 공격자가 원하는 것과 일치하는 암호화된 블록을 확보할 수 있습니다. 이제 공격자는 그 바이트가 무엇인지 알고 있으며 다음 바이트를 해독하기 위해 또 한 차례 요청을 조작합니다. 공격자는 세션 쿠키(혹은 자신이 원하는 것)를 해독할 때까지 이 과정을 반복합니다.

완화

암시적 IV를 이용하는 데 따르는 문제는 오래 전부터 알려져서 TLS 1.1에서 수정되었습니다. 그러나 거의 대부분의 브라우저는 TLS 1.1을 지원하지 않습니다. 따라서 TLS 1.1만 사용하도록 서버를 설정하는 건 현실적으로 불가능할 수 있습니다. RC4과 같은 스트림 암호는 이런 문제가 없습니다. 따라서 서버가 통신에 스트림 암호를 우선적으로 사용하도록 설정하는 것이 서버 측에서 이런 문제를 막을 수 있는 유일한 방법이었습니다. 이 문제의 해결책은 클라이언트 측에서 찾아야 합니다. 유감스럽게도 일부 SSL/TLS 구현 버전은 백포트 방식의 TLS 1.1 픽스와 호환되지 않습니다. 솔루션 제공업체가 이 문제를 해결하는 데 주력해 왔지만 호환성 문제 때문에 해결하기 쉽지 않습니다. 가령, Microsoft는 2012년 1월 월간 업데이트에서 이런 취약점을 해결한 패치를 배포했습니다.

DigiNotar와 Comodo 보안 사고

3월에 Comodo 인증기관과 관련된 한 등록 기관이 해킹 피해를 입어서 신뢰할 수 있는 UTN-USERFirst-Hardware용 루트 인증서로부터 "*.google.com" 및 "*.yahoo.com"과 같은 일반 도메인용 가짜 인증서 9개가 발급되었습니다. 이는 명백히 참사라 할 수 있는 보안 사고였습니다. 앞서 언급한 일반 도메인과의 안전한 통신을 유지하기 위해 Microsoft, Google, Mozilla 및 Apple 브라우저 제공업체들은 인증서 효력을 취소하기 위해 즉시 업데이트를 배포해야만 했습니다. Comodo의 보고서에 따르면 다행히도 가짜 인증서 중 인터넷에서 실제로 사용된 건 한 개(Yahoo용)뿐이었습니다.

6월 중순에 또 다른 보안 사고가 발생했는데 이번은 DigiNotar 인증기관이었습니다. Comodo의 보안 사고가 참사였다면 이번은 대참사였습니다. "*.google. com"뿐 아니라 훨씬 더 광범위한 "*.*.com"과 같은 도메인에 사용할 수 있는 가짜 인증서 500개 이상 발급된 것입니다. Fox-IT 공식 보고서에서는 이 보안 사고에 대해 30만 개 이상의 고유 IP가 Google용 가짜 인증서에 접속했다고 밝힌 바 있습니다. 이전의 보안 사고와 유사하게 이에 대한 대책으로 브라우저 제공업체들은 가급적 빨리 인증서 효력을 취소하기 위해 허겁지겁 자사 제품용 업데이트를 배포했습니다.

제품 업데이트는 인증서를 취소하는 극적인 조치로 보일 수 있지만 오늘날의 메커니즘 때문에 자주 배포되다 보니 당연하게 여겨지고 있습니다.

인증서 폐기

사기나 정보 업데이트 때문에 인증서 폐기가 불가피하다는 사실이 널리 공감대를 형성한 덕분에 그에 대한 해결책이 마련되었습니다. 인증서 폐기 상태를 검사하는 데 보편적으로 사용되는 두 가지 방법은 인증서 해지 목록(CRL)과 온라인 인증서 상태 프로토콜(OCSP)입니다. 유감스럽게도 이 두 가지 솔루션이 결정적인 효과가 있는 건 아닙니다.

첫 번째 방법을 이용하면 인증서에 CRL 정보가 추가됩니다. 클라이언트가 인증서를 인증할 때 지정된 CRL을 다운로드한 후 폐기된 인증서 일련번호 목록을 다운로드해서 해당 인증서가 유효한지 검사할 수 있습니다. 전체 목록을 다운로드해서 폐기 상태를 검사하는 첫 번째 방법과 대조적으로, OCSP는 클라이언트가 개별 인증서를 요청할 수 있도록 개발된 프로토콜입니다.

그러나 이 두 접근법은 구현 절차에 본질적으로 문제가 있어서 효과적이지 못합니다. 클라이언트가 폐기 통보를 받지 못한 경우 서버가 다운돼서 인증서가 유효하다고 잠정 결론을 내립니다. 명백한 문제는 공격자가 메시지 가로채기(man-in-the-middle: MITM) 수법으로 트래픽을 가로채서 유효하지 않은 인증서를 클라이언트에 전송하고 폐기 응답도 함께 차단할 수 있다는 것입니다.

가짜 인증서의 효력을 취소할 더 좋은 방법이 없다는 것보다 더 심각한 사실은 이런 취약점이 해결되지 않는다는 건 SSL 신뢰 모델 그 자체에 훨씬 더 큰 문제가 있음을 의미한다는 사실입니다.

SSL 신뢰 모델

SSL과 TLS의 두 가지 핵심 목표는 인증서의 진위를 판별하고 통신의 기밀성을 유지하는 것입니다. 인증서의 진위를 판별하고 서버를 가장하는 메시지 가로채기 수법을 막기 위해 SSL은 인증서와 인증기관의 관점에서 설계되었습니다. 어떤 웹사이트가 HTTPS를 지원하려는 경우 인증서가 필요하므로 인증기관에 요청해야 합니다. 인증기관은 Verisign, Thawte, Comodo 혹은 DIgiNotar와 같은 기업으로 대표되는 신뢰할 수 있는 기관이며 인증기관의 업무는 해당 사이트의 '신원'이 맞는지 검사한 후 이 사실을 증명할 인증서를 발급하는 것입니다.

그리고 나면 웹 브라우저가 이런 신뢰할 수 있는 기관이 발급한 인증서를 미리 설치해뒀다가 어떤 이유로 임의의 인증서가 제시됐을 때 설치된 인증서와 비교하여 임의의 인증서가 유효한지 검사할 수 있습니다. 그러나 메시지 가로채기 공격 사례를 다시 언급하자면, 공격자는 특정 웹사이트용 위조 인증서를 제작해서 합법적인 웹사이트에 연결하려는 클라이언트에 제시할 수 있습니다. 그런데 공격자의 인증서는 신뢰할 수 있는 인증기관의 서명을 받지 않았기 때문에 클라이언트의 웹 브라우저가 경고를 보내고 합법적인 웹사이트에 연결되지 않았다는 것을 인지하게 됩니다.

SSL 신뢰 모델이 안고 있는 문제

이 모델에는 몇 가지 문제가 있습니다. 시스템에서 모든 인증기관은 동일하게 취급됩니다. 한 인증기관이 발급한 인증서는 다른 인증기관이 발급한 인증서와 정확히 동일하게 유효합니다. 예를 들어, 웹 브라우저는 임의의 인증기관에서 "*.google.com"용으로 발급한 인증서를 Google의 실제 도메인 등록 기관에서 발급한 인증서와 동일하게 유효한 것으로 인식합니다.

EFF(Electronic Frontier Foundation)의 SSL 관측 프로젝트에 따르면 인증서를 발급할 수 있는 기업은 600개가 넘습니다. 기업의 수가 이렇게 많은 것을 감안하면 요청 받은 인증서에 대한 검사 수준뿐 아니라 웹사이트 보안의 품질 수준도 큰 차이를 보이는 것도 놀라운 일은 아닙니다. 굳이 해킹을 당하지 않더라도 인증기관이 잘못된 대상에게 인증서를 발급할 수 있는 것입니다. 실제로 과거에 이런 일이 일어났었고 앞으로 같은 일이 벌어지지 않는다는 보장도 없습니다.

또 다른 문제는 인증기관이 한 번 신뢰하면 신뢰 상태가 계속 유지된다는 점입니다. 인증기관은 수백만 개의 웹사이트에 인증서를 발급할 수 있습니다. 웹사이트가 인증기관을 더 이상 신뢰하지 못하겠다고 판단하고 저장된 인증서를 삭제한 경우 그 인증기관이 서명한 웹사이트의 모든 인증서는 HTTPS에서 더 이상 유효하지 않은 것으로 간주됩니다.

SSL 신뢰 모델 개정

이런 문제를 해결하기 위해 다양한 해결책이 제시되었습니다. 그 중에는 DANE(DNS-based Authentication of Named Entities) 및 CAA(Certificate Authority Authorization)와 같은 DNS를 이용하여 신뢰 문제를 해결하자는 제안도 있습니다. 이 두 제안의 핵심은 공인된 인증기관에 대한 정보를 도메인의 DNS 레코드에 삽입할 수 있다는 점입니다. 인증기관은 이 정보를 이용해서 해당 도메인에 인증서를 발급하려는 기관의 적법성을 검사하여 잘못된 대상에게 무분별하게 발급되는 것을 막을 수 있습니다. 그리고 클라이언트는 이 정보를 이용해서 인증서가 적절한 인증기관에서 발급됐는지 검사할 수 있습니다.

또한 DANE은 인증기관의 신탁 메커니즘에 대한 대안이 될 수 있습니다. 웹사이트는 인증서 정보를 도메인의 레코드에 추가할 수 있습니다. 그리고 클라이언트가 웹사이트에 연결될 때 도메인 인증서를 이전에 제공 받은 인증서와 비교할 수 있습니다. 두 인증서가 일치하는 경우 해당 웹사이트가 적법한 인증을 받은 것으로 간주됩니다. 이 두 가지 접근법의 단점은 보안을 유지하려면 DNSSEC(Domain Name System Security Extensions)이 있어야 하는데 DNSSEC가 아직 보편적으로 사용되지 않고 있다는 점입니다.

현재 신탁 메커니즘의 대체 방안 및 DNS 이용 사례는 한 블로그 기사에서 Moxie Marlinspike5에 의해 처음 소개됐으며, 그 뒤에 BlackHat USA에서 정식 발표되었습니다. Marlinspike는 DNS를 이용한다고 해서 인증서의 신뢰도가 더 높아지는 건 아니라고 지적했습니다. 클라이언트 정부가 운영하는 인증기관에 의해 발행된 인증서가 트래픽을 '도청'하는 데 악용되고 있다고 인식하더라도 동일 국가의 DNS 서버로부터 받은 인증 데이터에 의존하는 상황을 개선해야 하는 과제가 여전히 남습니다.

Marlinspike는 SSL에 '민첩한 신탁(trust agility)'이 필요하다고 강조했습니다. 두 가지 핵심 원칙은 클라이언트가 언제든지 인증기관 신탁을 철회할 수 있고, 신탁할 인증기관을 선택할 수 있다는 것입니다. 그에 대한 일환으로 Marlinspike는 사용자가 웹사이트의 인증서를 인증하는 다수의 '공증기관'을 선택할 수 있게 함으로써 이런 요건들을 충족하는 'Convergence'란 Firefox용 플러그인을 개발했습니다. 이렇게 해서 공증기관이 자체적으로 인증 보안 요건을 적용할 수 있고 사용자는 신탁하려는 공증기관을 선택할 수 있는 유연한 제도가 탄생하는 것입니다.

5 http://blog.thoughtcrime.org/ssl-and-the-future-of-authenticity
http://www.youtube.com/watch?v=Z7Wl2FW2TcA

오늘날의 인증기관 모델은 한번 신뢰한 인증기관을 영원히 신뢰할 수밖에 없는 구조입니다. 인증기관은 인터넷의 웹사이트에 사용되는 수백만 개의 인증서를 발급할 수 있습니다. 가령, 어떤 시점에 이르러 사용자가 Verisign을 더 이상 신뢰하지 못하겠다고 판단하고 저장된 인증서를 삭제한 경우 그 인증기관을 신뢰했을 때 발급 받았던 인증서가 단 한 개라도 존재하는 웹사이트는 HTTPS를 통해 접속할 수 없습니다. 이런 구조는 여러 공증기관 중 특정 공증기관만 더 이상 신뢰하지 않기로 결정한 경우 나머지 공증기관은 여전히 그 웹사이트에게 발급된 인증서의 보안을 인증할 수 있는 Convergence의 '민첩한 신탁'과 대조를 이룹니다. 공증 제도는 특히 사용자에게 더없이 좋은 아이디어처럼 보이지만 명확한 금전적 이득이 없다면 기업이 이 제도를 도입하고 유지하게 만들 동기 부여가 불확실합니다.

민첩한 신탁을 보장하는 또 다른 해결책은 다수의 인증서를 지원하도록 TLS/SSL을 확대하는 것입니다. 만일 웹사이트가 각기 다른 인증기관(예: DigiNotar, Verisign)으로부터 서명 받은 다수의 인증서를 제공할 수 있는 경우 사용자가 DigiNotar에게 신탁하지 않겠다고 결정하더라도 여전히 Verisign에 신탁할 수 있으므로 안전한 연결을 보장 받을 수 있습니다.

이런 해결책의 큰 걸림돌은 TLS 프로토콜을 그에 맞게 수정해야 하는데 새 프로토콜 버전의 보편화가 더디게 이뤄진다는 점입니다.

향후 전망

SSL는 소수 웹사이트의 통신 보안을 위해 1990년대 초반에 처음 개발되었습니다. SSL은 TLS 1.2 버전까지 업그레이드됐으며 2백만 개 이상의 웹사이트에서 사용되고 있습니다. TLS 1.1이 여전히 널리 사용되고 있지만 이론상으로나 가능하다고 여겨졌던 문제들이 실제로 나타나고 있기 때문에 새 버전이 더욱 빠른 속도로 보편화될 가능성이 높습니다. 그리고 유출된 인증서 개인 키가 이전에 레코드에 저장된 트래픽을 해독하는 데 악용되지 못하도록 통신의 기밀성을 유지할 수 있는 ECDHE_RSA와 같은 최신 암호 세트가 클라이언트와 서버에 더욱 보편적으로 설치될 것이란 긍정적인 전망도 있습니다. 현재의 SSL 신뢰 모델은 변화가 불가피하지만 프로토콜의 고치기 힘든 결함이 완벽하게 해소되기까지는 앞으로도 오랜 시간이 걸릴 것으로 보입니다.

Mac용 악성 코드 등장

개요

2011년에는 Mac용 악성 코드가 전례 없이 왕성하게 활개를 친 한 해였습니다.[6] 이전에 비해 빈도가 늘었을 뿐 아니라 그 기능 역시 다양했습니다. 이전에는 Windows® 용 악성 코드에서만 볼 수 있었던 기능들이 2011년부터 Mac용 악성 코드에도 추가되기 시작한 것으로 조사되었습니다. 이런 현상은 사이버 범죄자들이 이제 OS X를 공격 대상으로 삼는 것이 얼마나 수익성이 있는지 깨닫기 시작한 데 따른 것으로 보입니다.

그럼 2011년에 발견된 몇 가지 주목할만한 Mac용 악성 코드를 살펴보겠습니다.

MacDefender

MacDefender는 2011년 5월에 처음 발견됐으며 이후 몇 달간 MacSecurity, MacProtector, MacGuard, MacShield 같은 여러 가지 변종이 속속 등장했습니다. MacDefender가 흥미로운 점은 과거 몇 년 동안 Windows 세계에서 만연했던 증식 메커니즘이 적용된 악성 코드라는 것입니다.

MacDefender는 스스로를 합법적인 바이러스 예방 프로그램으로 위장하는 '로그 안티바이러스(Rogue Antivirus)'란 악성 코드 범주에 속합니다. MacDefender가 설치되면 시스템을 검사하는 척하면서 임의의 파일들을 악성 파일로 표시하여 사용자의 시스템이 심하게 감염된 것처럼 보이게 만듭니다.

사용자 인터페이스 역시 전문적이고 워낙 정교하게 만들어서 사용자가 합법적인 애플리케이션으로 속아 넘어가기 쉽습니다. 사용자 인터페이스에는 등록(Register) 버튼이 있는데 이 버튼을 누르면 신용카드를 이용해서 MacDefender 라이선스를 구매할 수 있는 웹사이트로 이동하게 됩니다.

그림 12: 악성 코드 MacDefender 2011년 버전 스크린샷

MacDefender는 불안감을 조성해서 라이선스를 구매하도록 유도하기 위해, 감지된 악성 코드를 제거하라는 메시지를 표시하고 위기감을 느낀 사용자는 어쩔 수 없이 등록 버튼을 누르게 됩니다. 그러면 사용자의 신용카드에 라이선스 요금이 부과되며, 그 보다 더 심각한 문제는 피해자의 신용카드 번호가 다른 목적으로도 악용될 수 있다는 점입니다.

MacDefender와 변종 코드는 SEO 감염 공격 수법을 통해 사용자를 공략함으로써 전파되며, 악성 코드 제작자는 악성 코드가 포함된 자신의 링크가 검색엔진 결과 상위에 오른 것처럼 보이도록 검색 엔진 결과를 조작합니다. 사용자가 이 링크 중 하나를 클릭하면 Javascript가 MacDefender 설치 프로그램을 시스템에 다운로드합니다. 다운로드가 완료되면 안전한 파일을 자동으로 열도록 브라우저가 설정된 경우 설치 프로그램이 자동으로 열립니다.

로그 안티바이러스는 아주 수익성 높은 범죄에 해당됩니다. 따라서 이런 유형의 악성 코드가 앞으로 더 기승을 부릴 것으로 전망됩니다. 사용자는 검색 결과에 있는 링크를 클릭할 때 항상 조심해야 합니다. 링크를 클릭하기에 앞서 그 링크의 도메인 이름이 본인이 찾고자 하는 것과 관련이 있는 링크인지 확인할 필요가 있습니다. 또한 믿을 수 있는 곳에서 개발한 것으로 확인되지 전에는 절대 소프트웨어를 설치하지 말아야 합니다.

Flashback

Flashback은 2011년 9월에 처음 발견된 트로이목마입니다. 그리고 이 악성 코드의 변종들이 최초 버전보다 여러 가지 측면에서 개선된 상태로 몇 달 만에 등장했습니다. Flashback은 Flash Player 설치 프로그램으로 위장하여 악성 웹사이트를 방문한 사용자가 그곳에 표시된 Flash Player 다운로드 혹은 설치 아이콘을 클릭해서 다운로드하도록 유도합니다.

그림 13: Flashback 트라이목마 2011년 버전 스크린샷

Flashback이 설치되면 공유형 동적 라이브러리 파일을 다운로드하고 DYLD_INSERT_LIBRARIES 환경 변수를 이용해서 사용자가 실행한 애플리케이션에 코드를 삽입합니다. 뒤에 등장한 변종 코드들은 Safari 및 Firefox와 같은 특정 애플리케이션에 코드를 삽입하도록 특화되었습니다. 삽입된 코드는 원격 서버에 접속하여 감염된 시스템에서 데이터를 전송하거나 업데이트 파일을 다운로드하도록 유도합니다. 이 코드 삽입 수법은 Zeus와 같은 일부 악명 높은 Windows용 악성 코드가 웹 브라우저에 코드를 삽입하는 방식과 유사합니다. Zeus는 서버에서 웹 브라우저로 전송되는 웹 페이지를 가로챈 후 즉석에서 웹 페이지를 수정하여 사용자 화면에 표시합니다. 수정된 웹 페이지에는 일반적으로 악성 코드가 민감한 정보를 훔칠 수 있는 가짜 로그인 페이지가 표시됩니다. 다행히 웹 브라우저 삽입 기능을 갖춘 Flashback의 변종 코드는 아직까지 발견되지 않았습니다.

한편 Flashback은 일부 관련 파일을 덮어쓰는 방법으로 XProtect 업데이트를 막으려고 시도합니다. XProtect란 스트링 대조 기술을 이용해서 악성 코드를 감지하는 Apple의 기본 설치형 악성 코드 보호 시스템입니다. Apple은 Mac용 악성 코드가 광범위하게 발견될 때마다 XProtect를 업데이트하고 있습니다.

또한 Flashback은 VMWare 가상 머신에서 실행될 경우 이를 감지하여 보안 전문가들의 분석을 방해하려고 시도합니다. 이 감지 회피 메커니즘은 Windows용 악성 코드에서 흔히 사용되고 있지만 Mac용 악성 코드에서 이런 수법이 발견된 건 Flashback이 처음입니다. 이는 Mac용 악성 코드의 기술 수준이 Windows용 악성 코드와 유사해지고 있음을 시사합니다.

DevilRobber

DevilRobber는 2011년에 세간의 관심을 모은 최신 OS X 악성 코드로서 2011년 10월에 처음 발견됐으며 11월과 12월에 변종 코드도 등장했습니다. DevilRobber는 GraphicConverter, Flux, CorelPainter, Pixelmator와 같은 BitTorrent에서 불법으로 다운로드할 수 있는 Mac 애플리케이션 내부에서 발견되었습니다.

DevilRobber는 IBM X-Force가 지금까지 발견한 악성 코드 중 가장 정교하며 여러 가지 구성 요소가 포함되어 있습니다. DevilRobber의 특징은 감염된 시스템의 포트를 개방하여 원격 공격자로부터 명령을 받는 백도어 악성 코드라는 점이지만 DevilRobber의 한 가지 흥미로운 기능은 BitCoin 마이닝입니다. DevilRobber는 BitCoin 마이닝 애플리케이션인 DiabloMiner를 설치한 후 (고성능 그래픽카드가 탑재된) 감염 시스템의 CPU 및 GPU의 컴퓨팅 자원을 사용하여 Bitcoin을 발굴합니다.

DevilRobber는 Bitcoin 전자지갑을 발견한 경우 훔치려고 시도하기도 합니다. 또한 DevilRobber는 감염된 시스템으로부터 다른 정보와 함께 사용자의 키체인(Keychain)을 훔쳐서 원격 FTP 서버에 업로드합니다.

그 밖에도 DevilRobber는 감염된 시스템이 게이트웨이 디바이스 뒤에 있는 경우 이를 감지하여 UPnP를 통해 포트를 개방(port-forwarding)할 수 있습니다. 감염된 시스템이 게이트웨이 디바이스 뒤에 있는 경우 공격자는 DevilRobber가 개방한 포트를 통해 원격으로 감염된 시스템에 접속할 수 있습니다.

결론

일부 독자는 이미 눈치 챘겠지만 지금까지 소개한 악성 코드 중 소프트웨어의 취약점을 악용해서 전파되는 것은 하나도 없습니다. 이 이유는 OS X에 공공연하게 알려져 있고 악용하기 적합한 취약점이 그리 많지 않기 때문으로 풀이됩니다. 취약점을 악용하는 대다수 Windows용 악성 코드는 이따금 Metasploit와 같은 취약점 테스트용 프레임워크에서 발견되어 공공연하게 알려진 취약점을 사소한 수정만으로 악용하기도 합니다. 그러나 OS X는 공공연하게 알려진 취약점이 비교적 적습니다. 그 이유는 플랫폼의 시장점유율이 비교적 낮아서 취약점을 찾아내려는 관심이 부족하거나 악용하는 데 필요한 기술 정보가 많지 않기 때문입니다.

최신 OS X 버전에서 보안 문제가 다각적으로 개선된 덕분에 공격자의 진입 장벽이 더욱 높아졌습니다. OS X Lion은 완벽한 ASLR과 샌드박싱 프레임워크(sandboxing framework)를 구현하고 64비트 프로세스를 기본적으로 지원합니다. 또한 Apple은 2012년 6월부터 Mac App Store에 전송되는 모든 애플리케이션이 샌드박스 환경을 구현하는 것을 의무화하여 제 3의 애플리케이션을 통한 취약점 악용 시도를 차단할 계획입니다.

당연히 Mac 사용자에게는 반가운 소식입니다. 그러나 앞서 설명한 예에서 짐작할 수 있듯이 공격자들은 악성 코드를 유포할 또 다른 대안을 찾아낼 것입니다. 또한 Apple의 보안 개선은 악용 방지 및 최소화에 중점을 두고 있을 뿐 앞서 언급한 유형의 악성 코드 문제가 근본적으로 해결된 건 아닙니다. 따라서 Mac용 악성 코드는 2012년에 더욱 활개를 칠 것으로 예상됩니다.

반면에 Apple은 OS X용 악성 코드 개발 예산을 추가로 편성하는 단호한 조치를 취하고 있습니다. Apple은 최근 발표한 다음 OS X 버전인 Mountain Lion에 Gatekeeper라는 기능이 새로 추가했습니다. 사용자는 Gatekeeper 기능을 이용하여 애플리케이션의 출처를 기준으로 본인의 시스템에 설치 및 실행되는 것을 허용할 애플리케이션을 직접 선택할 수 있습니다. 가령, 사용자는 출처가 Apple App Store인 애플리케이션만 설치 및 실행을 허용하거나 출처가 Apple App Store이거나 검증된 개발업체(관련 Apple Developer ID가 있는 애플리케이션)인 애플리케이션의 설치 및 실행을 허용할 수 있습니다. 또한 사용자가 원하는 경우 이 기능을 비활성화할 수도 있습니다. 참고로, 기본 설정 상태에서는 출처가 Apple App Store이거나 검증된 개발업체인 애플리케이션만 설치 또는 실행됩니다. 이 기능은 대대적이고 장기적인 악성 코드 출현을 막는 데 큰 도움이 될 것으로 예상됩니다.

공격자들과 마찬가지로 보안 솔루션 제공업체들 역시 OS X에 주목하고 있습니다. 따라서 새로 등장하는 Mac용 악성 코드에는 감지 및 분석을 피할 수 있는 방법이 채용될 것으로 IBM X-Force는 전망합니다. 놀랍게도 지금까지 IBM X-Force가 발견한 Mac용 악성 코드 중 대부분에는 회피 메커니즘이 사용되지 않았습니다. 하지만 Mac용 악성 코드에도 Windows 환경에서 흔히 볼 수 있는 압축(packing), 안티디버깅(anti-debugging), VM(virtual machine) 감지와 같은 회피 수법이 앞으로 더 많이 사용될 것으로 전망됩니다. 또한 Windows용 악성 코드로 톡톡한 재미를 봤던 고급 수법(예: Rootkit과 같은 잠입 기술이나 Zeus 방식의 웹 브라우저 인젝션 수법)들이 Mac용 악성 코드에도 사용될 것으로 보입니다. 새로운 악성 코드는 결국 앞서 소개한 Gatekeeper 기능을 극복해야 합니다. 따라서 악성 코드가 어떻게든 Gatekeeper를 회피하려고 안간힘 쓸 것으로 예상됩니다.

Windows용 악성 코드에 비해 그 수치는 여전히 미미하지만 Mac 컴퓨터가 수지맞는 공격 목표로 성장하고 있다고 공격자들이 느끼기 시작한 건 분명합니다. Mac 사용자는 이제까지 Windows에서만 볼 수 있었던 악성 코드가 OS X에서도 나타날 수 있다는 사실을 명심해야 합니다.

웹 컨텐츠 동향

IBM X-Force® 컨텐츠 보안 팀은 매달 새로운 웹 컨텐츠 데이터와 1억 5천만 개의 새로운 웹 페이지 및 이미지를 지속적으로 검토 및 분석합니다. IBM X-Force® 컨텐츠 보안 팀이 1999년부터 지금까지 분석한 웹 페이지와 이미지는 160억 개에 달합니다.

IBM 웹 필터 데이터베이스에는 68개의 필터 범주와 7천만 개의 항목이 존재하며 있으며 하루에 15만 개의 새 항목이나 업데이트된 항목이 추가됩니다.

이번 단원에서는 다음 사항을 살펴보겠습니다.

- 분석 방법론
- 웹사이트에 IPv6 도입
- 익명 프록시 증가
- 악성 웹사이트

분석 방법론

X-Force는 IBM 보안 시스템의 웹 필터 데이터베이스에 범주화된 기준에 따라 호스트를 산정하여 인터넷의 컨텐츠 배포 정보를 수집합니다. 호스트 산정은 컨텐츠 배포를 확인하는 방법으로 현실적 평가에 적절합니다. 그리고 웹 페이지 및 하위 페이지 산정과 같은 다른 방법을 사용할 경우 결과가 달라질 수 있습니다.

웹사이트에 IPv6 도입

배분할 수 있는 IPv4가 거의 바닥난 상태이기 때문에 IPv6로 전환하는 인터넷 사이트가 갈수록 늘어날 전망입니다. 그러나 최근 5개월간의 추이를 살펴보면 IPv6 전환 속도는 예상보다 더딥니다. X-Force는 웹사이트의 IPv6 도입률을 파악하기 위해 매달 수백만 개의 호스트에 DNS를 요청했습니다(DNS의 AAAA 레코드 검사).

최소 하나의 호스트가 IPv6을 지원하는 도메인의 비율은 2.2~2.6% 정도로 비교적 저조했습니다.

많은 기업과 조직이 영구적인 IPv6 배치 환경을 구현할 계획이기 때문에 2012년 6월 6일에 열릴 World IPv6 Day[7] 를 계기로 IPv6 지원이 크게 증가할 것인지 지켜볼 만합니다.

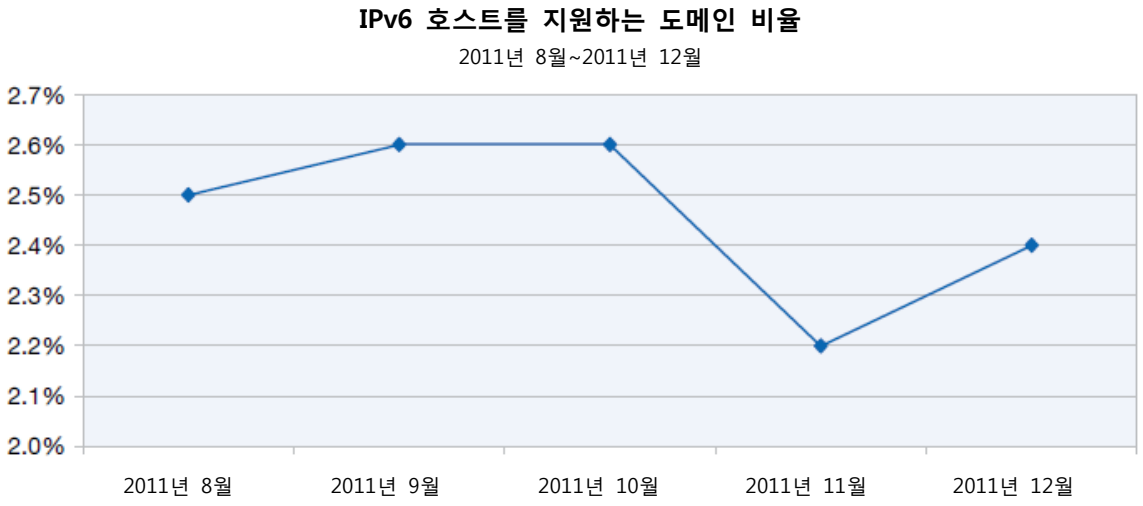


그림 14: IPv6 호스트를 지원하는 도메인 비율(2011년 8월~12월)

7 http://en.wikipedia.org/wiki/World_ipv6_day

익명 프록시 증가

인터넷이 가정, 직장, 학교 등에서 우리 생활에 필수불가결한 부분이 되자 적절한 환경을 유지 관리해야 할 책임이 있는 조직은 공공장소에서 인터넷을 이용하는 사람들을 통제할 필요성을 더욱 절감하고 있습니다.

이러한 통제 방법 중 하나는 부적절한 웹사이트에 대한 접근을 막는 컨텐츠 필터링 시스템입니다. 어떤 사람들은 웹 필터링 기술을 우회하기 위해 (웹 프록시라고도 불리는) 익명 프록시를 사용하기도 합니다.

웹 프록시를 이용하면 대상 웹사이트를 직접 방문하는 대신 웹 양식에 URL을 입력할 수 있습니다. 프록시를 사용하면 대상 URL이 웹 필터를 우회하게 됩니다. 웹 필터가 익명 프록시를 감시 또는 차단하도록 설정되지 않은 경우, 일반적으로 차단되었을 이 활동이 필터를 우회하여 공격자가 무단으로 웹사이트에 접속할 수 있게 됩니다.

새로 등록된 익명 프록시 웹사이트의 증가는 이런 추세를 반영합니다.

2011년 상반기에 등록된 익명 프록시는 3년 전에 비해 4배 정도 많습니다. 그리고 2011년 하반기에 등록된 익명 프록시는 3년 전에 비해 3배 이상 많습니다. 그러나 익명 프록시 증가율이 하락세를 보인 건 2009년 초 이후 이번이 처음입니다.

아마도 이는 인터넷 활동이 소셜 네트워크에 더 집중된 데 따른 것으로 해석됩니다. 직장이나 학교에서는 이런 웹사이트를 차단하지 않은 상태인 경우가 많아서 더 이상 컨텐츠 필터링 시스템을 우회할 필요가 없습니다.

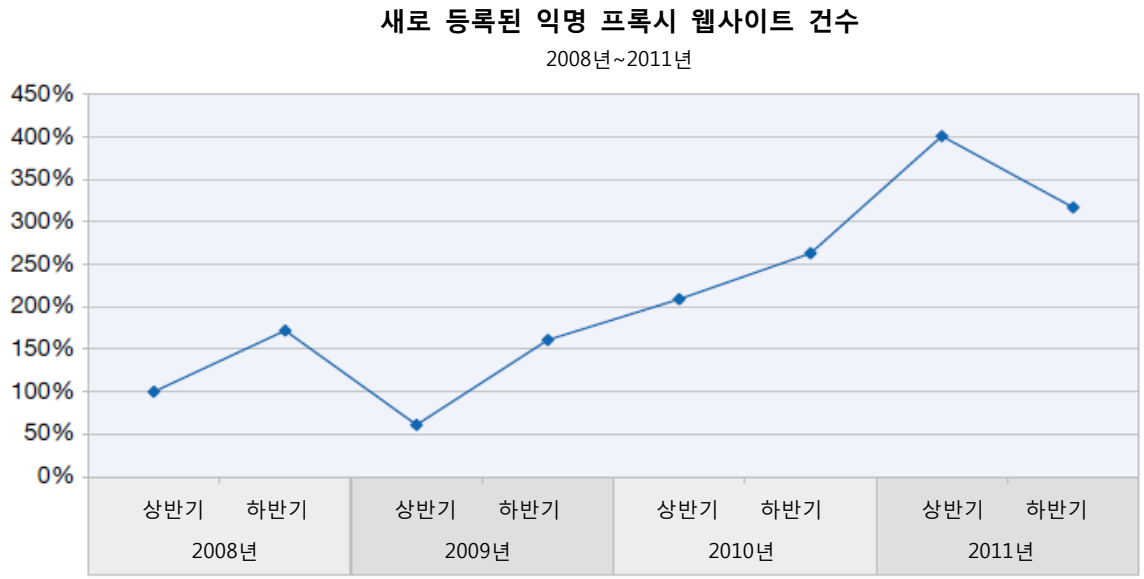


그림 15: 새로 등록된 익명 프록시 웹사이트 건수(2008년~2011년)

그러나 소셜 네트워킹 플랫폼을 사용하게 되면서 특히, 다른 사용자들과 공유하는 정보를 통제하고 기밀 정보 공유를 방지해야 하는 기업에는 새로운 과제가 대두되었습니다. 그래서 웹 애플리케이션 제어 시스템을 차세대 방화벽의 일환으로 사용하는 기업이 늘고 있습니다.

익명 프록시는 공격자가 악의적 의도를 감출 수 있기 때문에 대단히 위험한 유형의 웹사이트입니다.

새로 등록된 익명 프록시의 최상위 도메인을 살펴보면 IBM X-Force 2011년 상반기 동향 및 위험 보고서에 자세히 설명된 것처럼 2011년 상반기의 추세가 계속 이어지고 있습니다. .tk 및 .com 도메인이 새로 등록된 익명 프록시의 70% 이상을 차지할 정도로 여전히 강세를 보이고 있습니다.

악성 웹사이트

이 단원에서는 악성 링크가 운영되는 국가와 이러한 악성 웹사이트에 가장 자주 링크되는 웹사이트 유형을 논의합니다. 2011년의 취약점 발견 현황 단원에는 취약점 악용 의도를 지닌 악성 웹사이트에 대한 자세한 정보가 소개되어 있습니다.

악성 웹사이트 링크의 지리적 위치

미국이 계속 악성 링크 운영 국가로 1위를 달리고 있습니다. 악성 코드 링크의 1/3 이상이 미국에서 운영되고 있으며 2위는 루마니아로 8.5%가 운영되고 있습니다. 지난 3년간 계속 2위를 유지했던 중국은 그림 16에 보이는 것처럼 5.7%를 점유하면서 프랑스와 함께 공동 3위를 기록했습니다.

중위권 국가 역시 순위 변동이 있었지만 2010년 수치를 2011년이 비교했을 때 변동 비율은 1% 미만이었습니다.

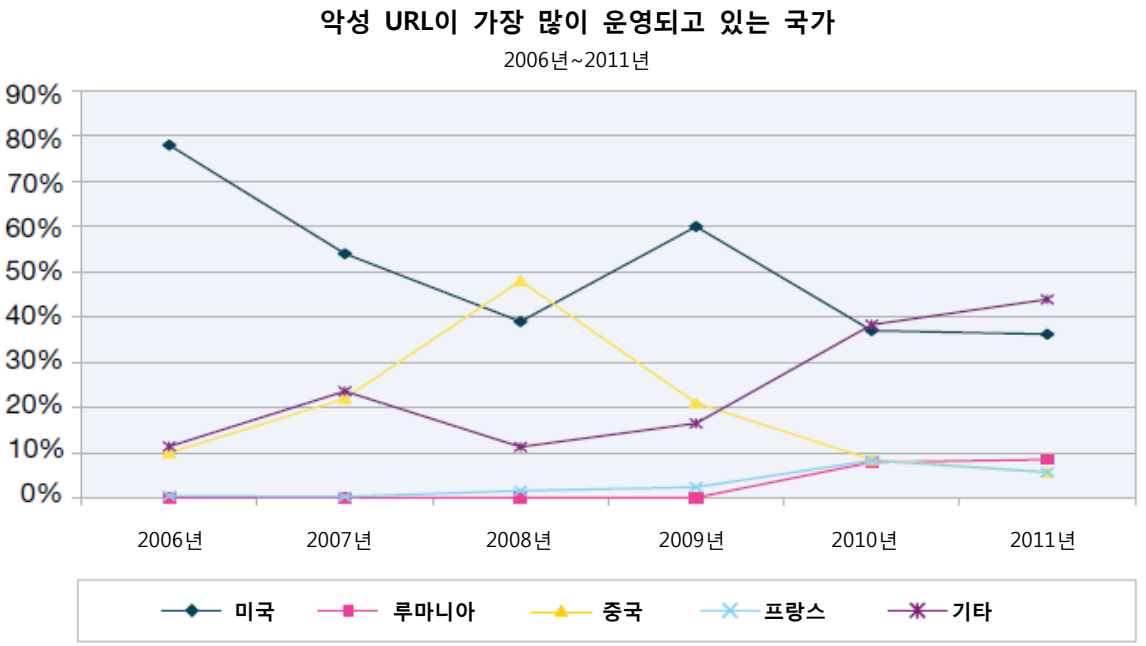


그림 16: 악성 URL이 가장 많이 운영되고 있는 국가(2006년~2011년)

불량 링크가 있는 우량 웹사이트

2011년 상반기의 IBM X-Force 동향 및 위험 보고서에 언급된 것처럼 공격자는 여전히 신뢰성 있는 웹사이트의 인지도 있는 이름을 사용하여 일반 사용자의 경계를 늦추고 보호 기술을 통해 공격을 위장하는 데 더더욱 주력하고 있습니다. 악성 웹 컨텐츠가 사용된다는 점은 변하지 않았습니다. 이번에는 가장 빈번하게 알려진 악성 링크가 포함된 웹사이트의 유형을 개괄적으로 분석하겠습니다.

상위 범주 몇 개는 예상에서 크게 벗어나지 않았습니다. 예를 들어, 포르노 및 도박을 목록 상위로 예상할 수 있습니다. 사실 이 두 개가 모든 악성 링크의 거의 40%를 차지합니다. 하지만 '2군 후보들'은 더 신뢰성 있는 범주에 속해 있습니다.

검색 엔진, 블로그, 게시판, 개인 웹사이트가 이 두 번째 계층의 '신뢰성 있는' 범주에 속합니다. 이런 웹사이트 중 대다수는 사용자가 컨텐츠를 업로드하거나 자신의 웹사이트를 설계할 수 있는 서비스를 제공합니다. 다시 말해서, 이런 유형의 웹사이트가 의도적으로 악성 링크를 게시한다고는 생각되지 않습니다.

다음 도표는 악성 코드 링크 유포 이력을 보여주고 있습니다.

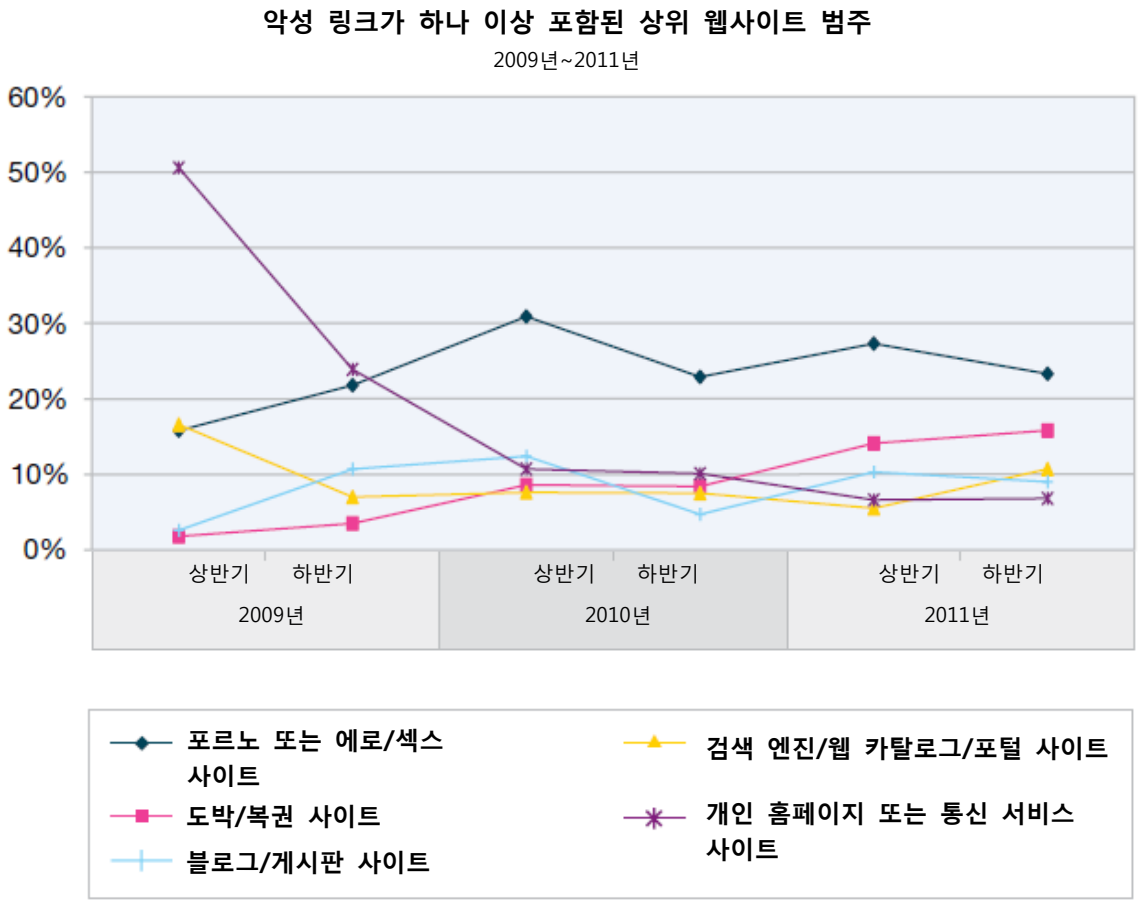


그림 17: 악성 링크가 하나 이상 포함된 상위 웹사이트 범주(2009년~2011년)

지난 3년을 되짚어보면 흥미로운 추세가 나타납니다.

- 포르노 및 도박과 같은 전문 '불량' 웹사이트가 악성 코드를 체계적으로 유포하면서 점유율 1, 2위를 다투고 있습니다.
- 포르노가 25% 내외의 점유율을 꾸준히 유지하면서 1위에 올랐습니다.
- 도박의 점유율이 유일하게 매 분기마다 큰 폭으로 상승하고 있습니다. 도박 중독에 걸린 성인 인구는 0.6%에 불과한데도 도박 사이트는 악성 코드 유포자들이 선호하는 표적이 되고 있습니다.
- 블로그/게시판이 지난 6개월간 9%로 감소했습니다.
- 개인 홈페이지(전통적인 1.0 웹사이트)의 점유율이 크게 줄었습니다. 주된 원인으로 개인 홈페이지가 소셜 네트워크나 비즈니스 네트워크의 프로필과 같은 웹 2.0 애플리케이션에 비해 유행에 뒤떨어진다는 점을 꼽을 수 있습니다.
- 검색 엔진, 웹 카탈로그 및 포털 사이트가 회복세를 보이면서 2년 6개월 만에 처음으로 10%를 넘어섰습니다.

8 http://en.wikipedia.org/wiki/Gambling_addiction#Prevalence

스팸과 피싱

IBM 스팸 및 URL 필터 데이터베이스는 전 세계 스팸 및 피싱 공격 상황 정보를 제공합니다. 수백만 개의 이메일 주소가 감시되는 와중에도 공격자가 사용하는 스팸 및 피싱 기술에 다양한 발전이 있는 것으로 확인되었습니다.

현재 스팸 필터 데이터베이스에는 4천만 개 이상의 관련 스팸 시그니처가 저장되어 있습니다. 각 스팸은 몇 가지 논리적 부분(문장, 단락 등)으로 나누어집니다. 128비트의 고유 시그니처는 각 부분 및 수백만 개의 스팸 URL을 대상으로 산출됩니다 현재 하루 평균 백만 개 정도의 신규, 갱신 또는 삭제된 시그니처가 매일 스팸 필터 데이터베이스에 저장됩니다.

이번 절에서는 다음과 같은 사항을 설명합니다.

- 지속적 감소세인 스팸양
- 2011년의 주요 스팸 동향
- URL 스팸의 보편적 최상위 도메인
- 스팸 — 발신 국가[9]의 동향
- 이메일 사기 및 피싱
- 스팸의 과거와 미래 전망

지속적 감소세인 스팸양

IBM X-Force는 2011년 상반기 동향 및 위험 보고서에서 지난 몇 년간 스팸이 꾸준히 감소하고 있는 배경에 대해 심층적으로 분석한 바 있습니다.

이전 보고서에서 이미 설명했듯이 여러 차례의 대대적인 봇넷 근절 활동이 스팸 감소의 원인으로 추정됩니다. 다음 도표에서는 전반적인 수치가 어떻게 감소하고 있는지 확인할 수 있습니다.

스팸 수량 변화

4월 2008년~12월 2011년

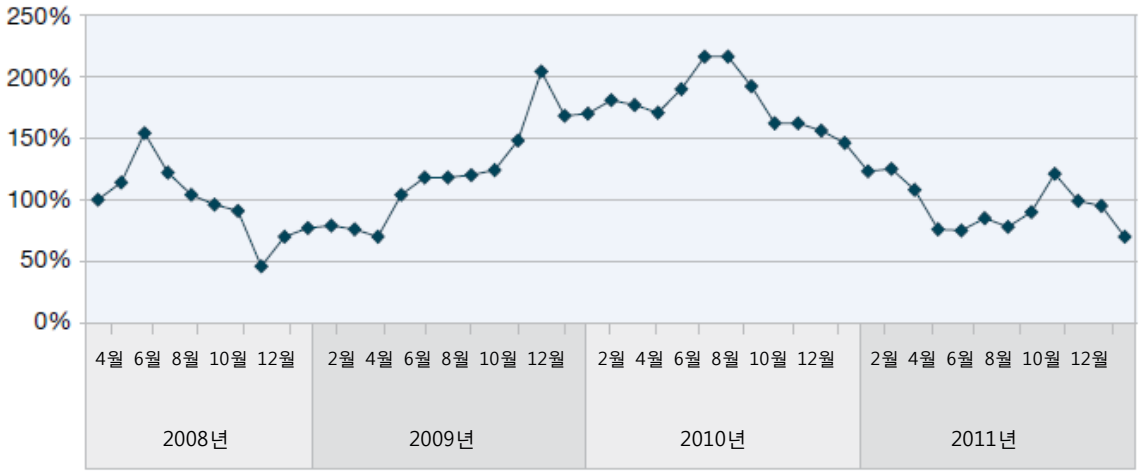


그림 18: 스팸 수량 변화(2008년 4월~2011년 12월)

9 스팸, 피싱, URL에 대한 이 보고서의 통계에는 WebHosting.Info(http://www.webhosting.info)의 http://ip-to-country.webhosting.info에서 제공하는 IP-to-Country Database가 사용되었습니다. 지리적 위치 분포는 컨텐츠 분포도의 경우 IP-to-Country Database에 호스트의 IP 주소를 요청하여 파악했으며 스팸 및 피싱의 경우 전송 메일 서버를 요청하여 파악했습니다.

2011년의 주요 스팸 동향

다음 도표는 2011년에 관측된 스팸의 주요 동향을 요약해서 보여주고 있습니다.

2011년에 발송된 스팸 동향에 여러 가지 변화가 있었는데 이런 변화 양상을 좀 더 알기 쉽게 다음과 같은 여러 단계로 나눌 수 있습니다.

- 0 단계 — 초기 상황:
  2010년 12월 초
- 1 단계 — Rustock 1차 박멸:
  2010년 12월 25일~2011년 1월 9일
- 2 단계 — Rustock 박멸 과도기:
  2011년 1월 10일~2011년 3월 15일
- 3 단계 — Rustock 2차 박멸 이후:
  2011년 3월 16일~2011년 5월 18일
- 4 단계 — 스팸 수량 1차 회복:
  2011년 5월 19일~2011년 8월 22일
- 5 단계 — 스팸 수량 2차 회복:
  2011년 8월 23일~2011년 11월 29일
- 6 단계 — 연말 스팸 수량 감소:
  2011년 11월 30일 이후

0 단계부터 4 단계까지는 이미 IBM X-Force 2011년 상반기 동향 및 분석 보고서에서 자세히 다룬 바 있습니다. 새로 추가된 5 단계와 6 단계에서는 이미지 기반의 스팸과 (다시) ZIP 또는 RAR 악성 코드 스팸이 강세를 보였는데 다음 두 개의 단원에서는 이에 대해 살펴보겠습니다.

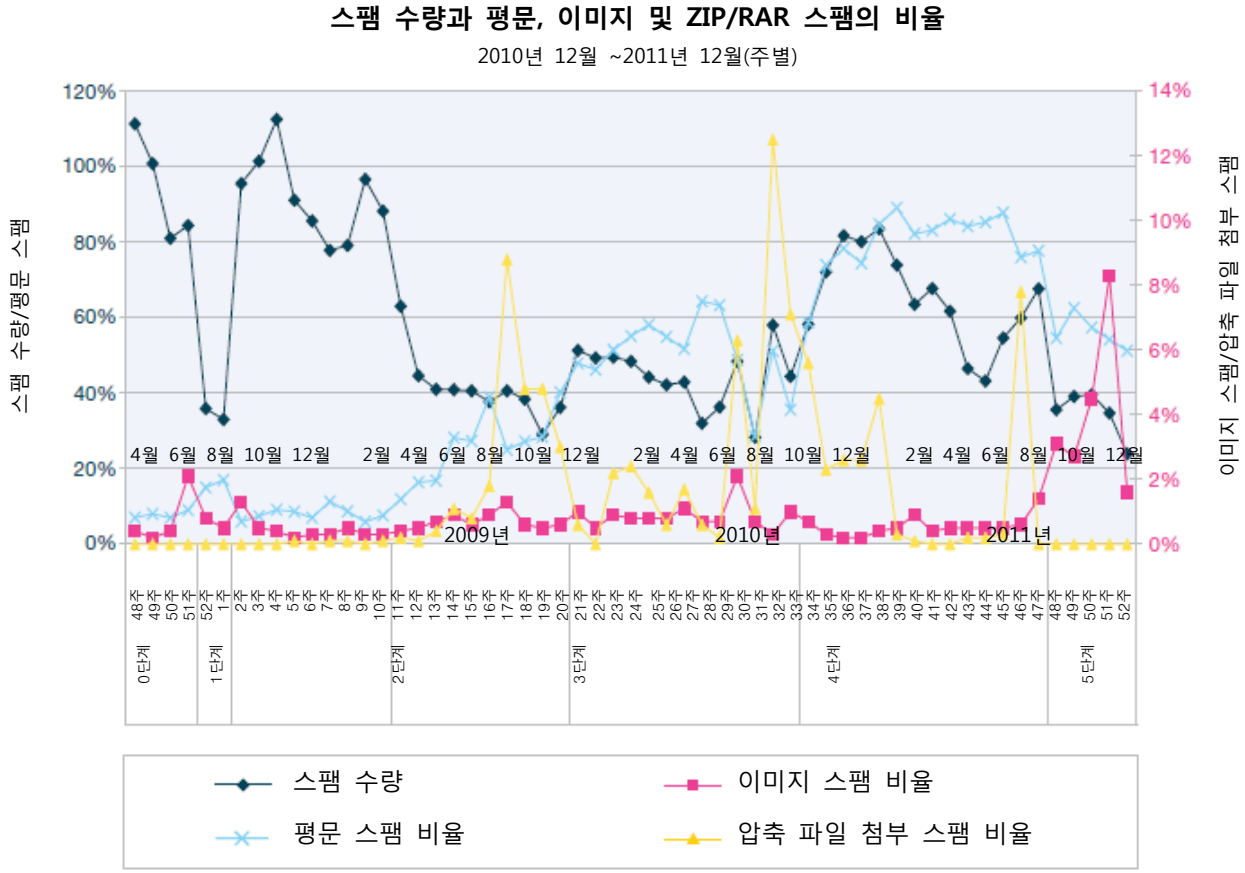


그림 19: 스팸 수량과 평문, 이미지 및 ZIP/RAR 스팸의 비율(2010

전체 기간을 보면 평문 스팸의 꾸준한 증가가 특히 두드러집니다. 그 이전에는 평문으로 작성된 스팸이 5~30%를 차지했는데 5 단계에 80%를 오르내리고 더 장기적으로 봤을 때도 이렇게 높은 수치를 기록한 건 처음입니다. 6단계에서는 55% 정도로 감소했습니다.

평문으로 된 스팸은 정해진 특징(예: 일정한 패턴을 형성하는 특별한 종류의 첨부파일이나 비정상적으로 분할된 html 코드)이 전혀 없기 때문에 컨텐츠 기반의 스팸 탐지가 훨씬 더 어렵습니다.

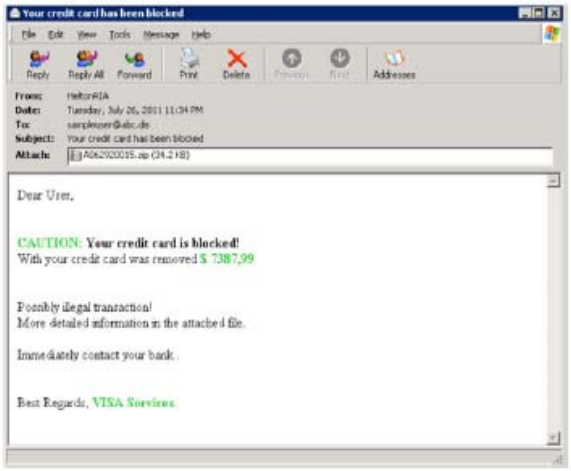


그림 20: 가짜 신용카드 결제 대금 메시지(2011년 7월)

그러나 합법적 이메일의 추세는 오히려 거꾸로 되었습니다. html을 사용하지 않는 상태 메시지나 뉴스레터 형식의 이메일은 소수만 남아 있습니다. 이런 이메일의 특징 때문에 조만간 단순한 평문 스팸이 의심을 살 확률이 갈수록 높아지고 있습니다. 심지어 이것이 차단 기준으로 사용될 날도 멀지 않은 듯합니다.

2011년의 악성 코드 ZIP 스팸

3단계의 ZIP 파일이 첨부된 스팸은 IBM 2011년 상반기 동향 및 위험 보고서에서 자세히 소개되어 있습니다.

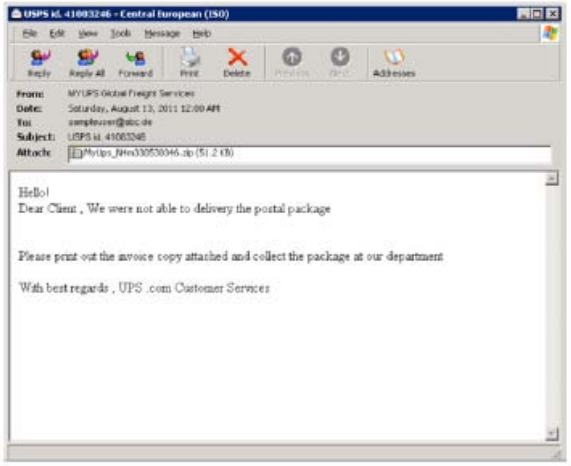


그림 21: 가짜 배송 통지 메시지(2011년 8월)

2011년 하반기에 ZIP 파일이 첨부된 스팸은 매일 측정한 결과를 기준으로 했을 때 세 차례에 거쳐 급증(18%~43%)했습니다. 트로이 목마는 공격자들이 가장 선호하는 악성 코드 첨부 형식입니다. 절정을 이룬 6월 말에 ZIP 파일이 첨부된 스팸 중 50% 이상의 스팸에 Trojan:Win32/Fivfrom.gen!B가 존재했습니다. 이런 첨부파일을 열고 이진 형식의 악성 코드를 클릭하도록 유도하기 위해 스팸 발송자들은 3 단계에 사용됐던 것과 유사한 여러가지 변칙적인 수법을 사용했습니다. 그 중 가장 대표적인 수법은 사용자가 신용카드로 100달러 이상의 금액을 결제했으며 세부 정보는 첨부파일을 참조하라는 메시지였습니다.

스팸이 급증했던 나머지 두 번의 시점에서도 그와 유사한 현상이 나타났습니다. 8월 중순에 가장 흔히 사용된 악성 코드 종류는 TrojanDownloader:Win32/Cbeplay.M이었습니다. 절정기가 지나고 2주 뒤 ZIP 파일이 첨부된 스팸의 비율은 하루 평균 약 10%였습니다. 대표적인 형식으로는 사용자가 첨부파일을 열고 이진 형식의 악성 코드를 클릭하도록 유도하기 위해 유명 택배 서비스가 보낸 것으로 위장한 가짜 배송 메시지가 손꼽힙니다.

세 번째 절정기는 9월 20일경이었습니다. 가장 보편적인 형식의 악성 코드는 TrojanDownloader:Win32/Chepvil.N이었습니다.

2011년의 이미지 스팸

이미지 스팸이 다시 고개를 든 건 약간 의외였습니다. 지난 2년간 이런 유형의 스팸은 그리 많지 않았습니다. 매일 측정한 결과를 기준으로 했을 때 이런 유형의 스팸은 대부분 1%를 밑돌았습니다. 그러나 11월 말부터 이미지 스팸이 급증했습니다.

과거의 이미지 스팸은 실제 스팸 메시지를 전송할 목적으로 이미지를 사용했습니다(예: URL을 표시하고 사용자에게 그 URL을 브라우저에 입력하라고 요구) 이런 고전적인 방식의 이미지 스팸이 여전히 일부 존재하지만 최신 이미지 스팸 대다수는 합법적인 조직이나 기업의 로고입니다. 그리고 이메일은 다음과 유사한 내용이 기재됩니다.

- 거래 과정에 오류가 발생했습니다. 자세한 내용을 보려면 링크를 클릭하십시오.
- 귀하의 업무에 대한 불만사항이 접수되었습니다. 여기를 클릭하십시오.

이런 로고를 사용하는 실제 목적은 사용자가 이메일에 있는 링크, 즉 사용자의 시스템을 감염시킬 악성 코드 링크를 클릭하게 만드는 것입니다. 이런 유형의 이메일은 피싱과 유사합니다. 이런 유형의 스팸에 대한 자세한 내용은 '이메일 사기 및 피싱' 단원을 참조하십시오.

악성 링크를 클릭하도록 유도하기 위해 스팸 발송자가 2012년에 사용할만한 다른 접근법을 살펴보는 것도 흥미로울 듯싶습니다.

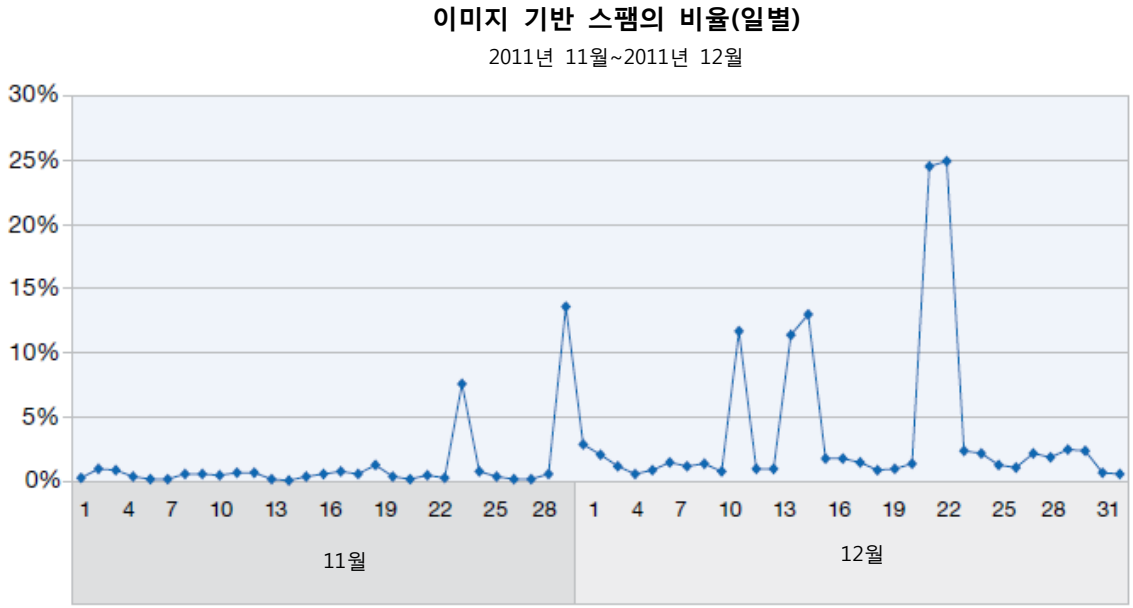


그림 22: 이미지 기반 스팸의 비율(2011년 11월~2011년 12월(매일 측정한 통계 기준))

지난 몇 년간 URL 스팸의 보편적 최상위 도메인 통계

2011년 스팸 발송자의 최상위 도메인 사용률은 2010년과 비슷한 수준이었습니다. 다만, 우크라이나 최상위 도메인인 .ua는 예외였습니다. 이 도메인은 인터넷에 새 컨텐츠를 배치하는 데 사용되었습니다. 스팸과 피싱은 항상 사용자가 링크를 클릭하도록 유도합니다. 그러면 악의적 의도를 지닌 사람들이 이용한 최상위 도메인 동향을 장기적인 관점에서 살펴보겠습니다. 지난 4년간 큰 변화가 있었습니다.

- 2008년부터 2011년까지 가장 많이 사용된 최상위 도메인은 .com으로, 항상 1위나 2위를 고수했습니다.
- 지난 몇 년간 스팸 발송자들이 애용한 다른 보편적 최상위 도메인으로는 .net, .info, .org가 있습니다. 그러나 이 도메인들의 사용량은 2011년 들어 크게 감소했습니다.
- 2010년 초부터 .cn(중국)이 눈에 띄게 감소해서 상위 15위 이내에 단 한 번도 들지 못했습니다.
- .cn을 대신해서 .ru(러시아)가 2008년에 15위에 진입하더니 2010년부터 .com과 번갈아 가며 수위를 차지했습니다.
- 2011년에는 .ua(우크라이나)가 급부상하여 2011년 봄 이후 3위를 유지했습니다.

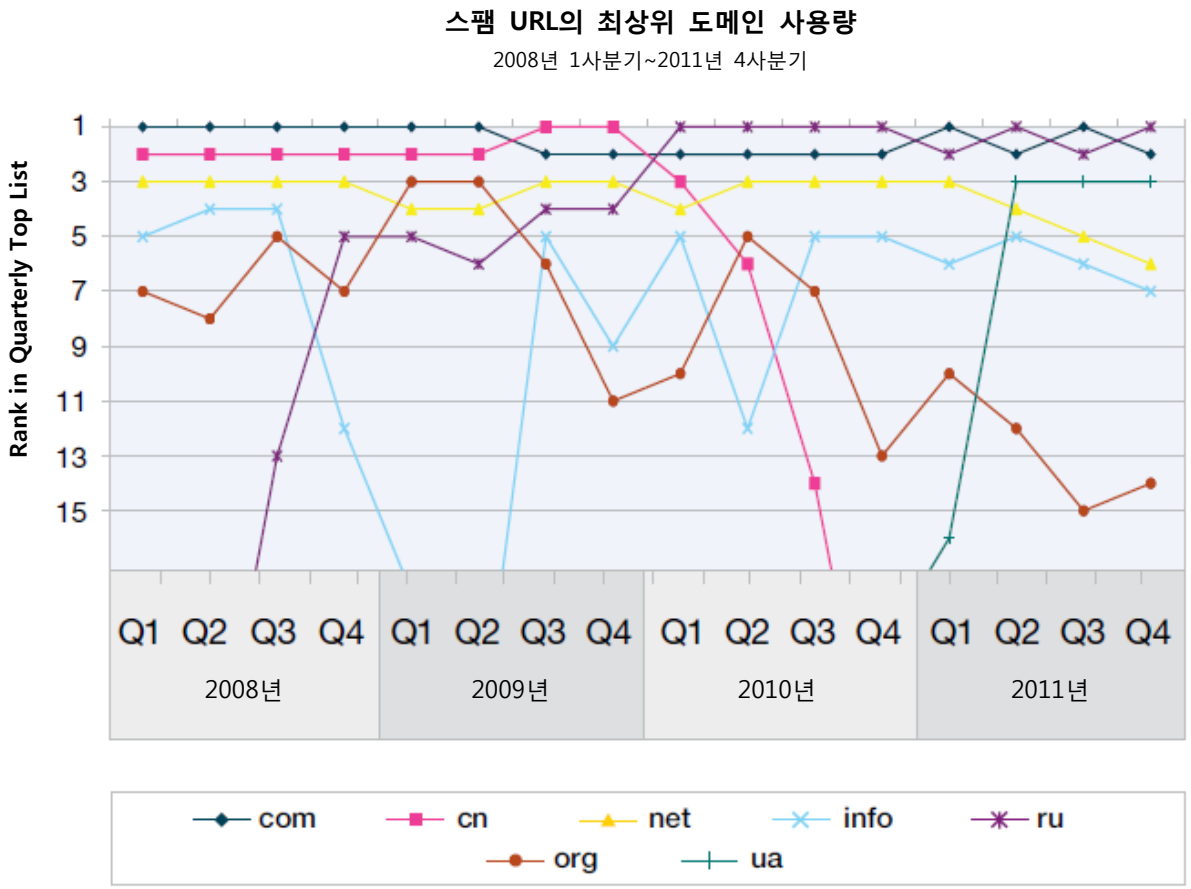


그림 23: 스팸 URL의 최상위 도메인 사용량(2008년 1사분기~2011년 4사분기)

이와 같은 장기적인 통계를 보면 다음과 같은 몇 가지 흥미로운 의구심이 생깁니다.

- **.com이 스팸 발송자에게 인기가 많은 이유는 무엇인가?** .com 도메인은 지금까지 인터넷에서 가장 많이 사용된 최상위 도메인입니다. .com 도메인은 등록비가 저렴하고 등록하기도 쉽습니다. 게다가 .com URL로 된 이메일은 전혀 의심을 사지 않습니다.
- **.cn(중국) 최상위 도메인 사용량이 크게 감소한 배경은 무엇인가?** 2008년과 2009년에 중국 도메인은 스팸 발송자들이 선호하는 도메인이었습니다. 그러나 중국이 2009년 11월 중순부터 .cn 도메인 등록 규정을 강화[10]했기 때문에 스팸 발송자들이 흥미를 잃게 된 것입니다.
- **러시아(.ru) 도메인이 중국 도메인과 같은 현상을 보이지 않은 이유는 무엇인가?** 러시아 역시 강화 정책을 시행했습니다. 2010년 4월 1일에 러시아 NIC는 새 도메인 등록 규정을 강화했습니다.[11] 그리고 18개월 뒤에도 러시아는 또 한 차례 규정을 강화했습니다.[12] 그러나 스팸 발송자들은 여전히 스팸 발송에 .ru 도메인을 애용하고 있습니다. 현재 .ru는 스팸 발송에 가장 많이 사용되는 국가 코드 최상위 도메인입니다.
- **소수 국가의 최상위 도메인만 스팸 발송에 널리 사용되고 있는데 이런 양상이면 스팸을 근절하기가 쉽지 않은가?** 답은 그럴 수도 있고 아닐 수도 있습니다. 여러 도메인 등록기관들이 중국과 동일한 규정을 적용하는 조치를 단행하기로 합의한다면 스팸을 줄이는 데 도움이 될 수 있습니다. 그러나 이는 현실적으로 기대하기 힘든 일입니다. 도메인 등록은 국가마다 다르게 다루는 법적 문제입니다. 그리고 느슨한 규정으로 스팸 발송자에게 문호를 개방하는 등록 기관은 항상 존재할 가능성이 높습니다. 또한 도메인 등록은 스팸 컨텐츠의 호스트로 이용하는 한 가지 방법일 뿐입니다. 나머지 방법은 도메인을 등록할 필요 없이 다른 컨텐츠 호스트를 이용하는 것입니다.

10 http://www.cnnic.net.cn/html/Dir/2009년/12/12/5750.htm
11 http://news.softpedia.com/news/Enhanced-Security-Measures-for-RU-Domain-Registrations-138234.shtml
12 http://www.abuse.ch/?p=3581

스팸 — 발송 국가 추세

지난 3년간 가장 많은 스팸이 발송된 장기적으로 국가를 살펴보면 다음과 같은 흥미로운 추세가 드러납니다.

- 3년 전에는 브라질과 미국이 1위를 다퉜습니다.
- 인도의 스팸 발송률이 꾸준히 증가해서 현재 14%가 넘는 점유율로 2위와 큰 격차를 벌이며 1위에 올랐습니다.
- 미국은 2010년에 불명예스러운 1위를 차지했지만 2011년에 미국에서 발송된 스팸은 전체 스팸의 2%에 불과합니다.
- 2009년에 주요 스팸 발원지였던 베트남은 2011년 1사분기에 점유율이 크게 감소했지만 2사분기에 소폭 회복해서 전체 스팸의 10% 이상을 차지했습니다.
- 브라질은 최근 18개월 동안 점유율이 절반으로 떨어졌습니다.
- 인도네시아가 급부상하고 있습니다. 인도네시아는 3년간 꾸준히 증가세를 보이면서 현재 전체 스팸의 10%를 차지하고 있습니다
- 호주도 급부상하고 있습니다. 2011년 말까지 호주에서 발송된 스팸 비율은 전체 스팸의 5.6%입니다.

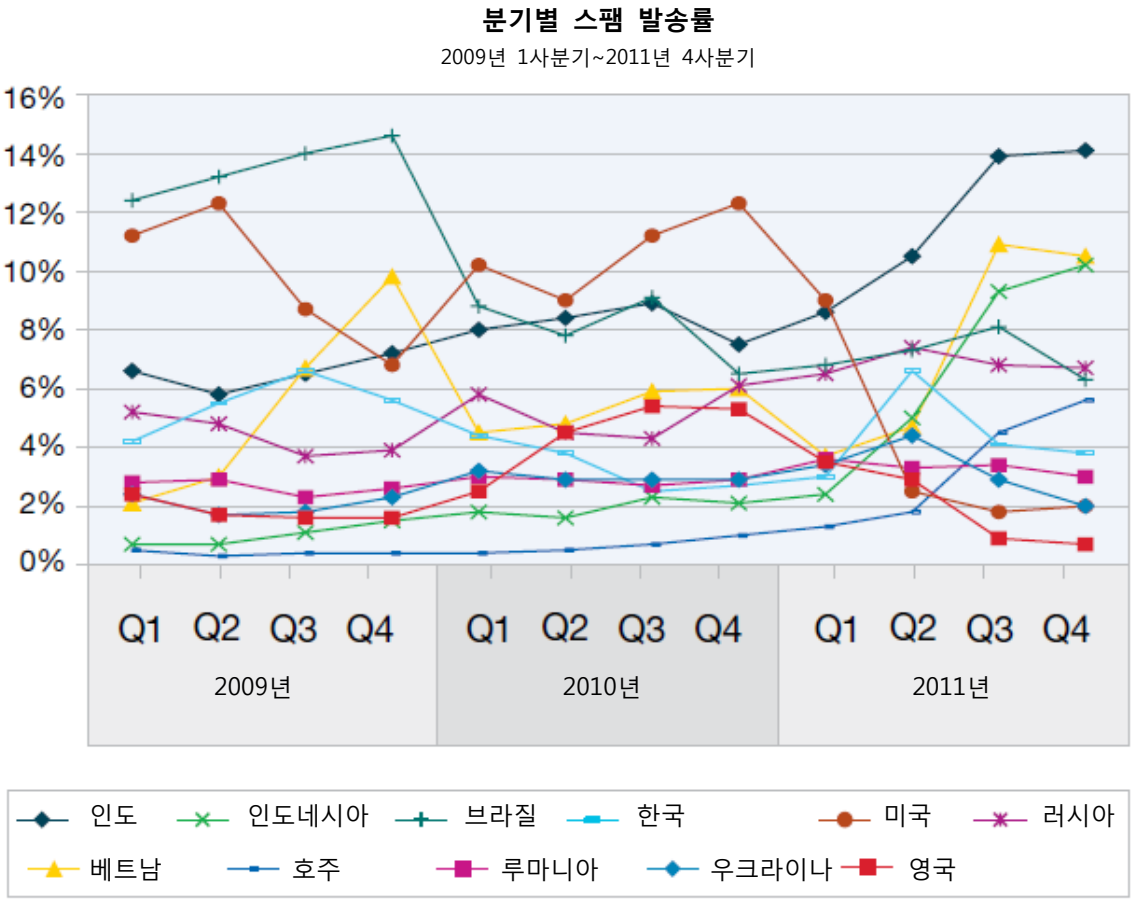


그림 24: 분기별 스팸 발송률(2009년 1사분기~2011년 4사분기)

이메일 사기 및 피싱

사기 수법과 피싱 통계

2011년 상반기 동향 및 분석 보고서에서 언급되어 있듯이 2010년과 2011년 상반기에 전통적인 이메일 피싱이 감소했습니다.
그러나 이메일 피싱이 사라질 운명에 처한 건 아닙니다. 온라인 범죄자들은 전통적인 이메일 피싱을 대신할 몇 가지 새로운 수법을 개발했지만 차이점이 뚜렷하지 않습니다. 다음과 같은 일반적인 피싱 이메일 형식의 스팸이 여전히 만연해 있습니다.

- 은행에서 보낸 것처럼 위장하여 계정 업데이트나 데이터 확인 등을 위해 사용자에게 제공되는 링크를 클릭하라는 이메일
- 소셜 네트워크에서 보낸 것처럼 위장하여 새 친구 신청을 확인하려면 제공되는 링크를 클릭하라는 이메일

얼마 전부터 전통적인 이메일 피싱에 큰 변화가 나타났습니다. 새로 등록된 도메인에서는 전통적인 피싱 이메일에 포함됐던 피싱 페이지 중 다수가 사라졌습니다. 새로 등록된 도메인의 장점은 피싱 공격자가 피싱 피해자에게 익숙한 도메인 이름(예: hxxp://www.<철자가 살짝 다른 은행 이름>)을 선택할 수 있다는 것입니다.

피싱 공격자는 (때때로 새로운 다국어 도메인 이름과 조합하여) 이를 악용합니다.[13] 한 가지 대책은 신속하게 그런 도메인을 강제로 폐쇄하는 것이었습니다. 그래서 이런 피싱 사이트를 중점 관리하는 새 도메인 폐쇄 서비스가 등장했습니다.

하지만 똑똑하고 끈질긴 피싱 공격자들은 이와 같은 강제 폐쇄 조치를 피할 수 있는 방법을 찾아냈습니다. 오늘날의 피싱 페이지 중 다수는 합법적인 웹사이트의 하위 페이지(예: hxxp://www.<합법적인 사이트>.com/<불특정한 단어>.html)로 배치됩니다. 피싱 공격자에게 유리한 점은 이런 하위 페이지의 도메인은 합법적인 웹사이트나 경우에 따라 합법적인 비즈니스 관련 웹사이트에 속하기 때문에 강제로 폐쇄할 수 없다는 것입니다. 피싱 공격자들은 이런 하위 페이지를 배치하기 위해 합법적인 웹사이트를 공격합니다. 피싱 공격자는 일단 침투에 성공하면 아주 간단하게 웹 서버에 수 킬로바이트에 불과한 페이지를 추가할 수 있습니다. 그런 다음 새 하위 페이지로 이동하는 링크가 포함된 피싱 이메일을 발송합니다. 피싱 공격자는 일반적으로 은행 로그인 페이지로 위장한 이 하위 페이지에 사용자가 입력한 기밀 정보를 수집합니다.

심지어 피싱 공격자는 이 링크를 클릭한 특정 비율의 사용자에게만 페이지를 표시하는 수법을 이용해서 보안 전문가들이 이런 페이지를 감지하기 더욱 어렵게 만들 수도 있습니다.

그러나 한 가지 의외인 점은 이런 피싱 이메일에 포함된 링크가 항상 피싱 웹사이트로 이동하는 링크는 아니라는 사실입니다. 대신, 링크를 클릭했을 때 다음과 같은 결과가 발생합니다.

a) 일반 스팸이 제공하는 링크와 동일하게 의약품, 패션 액세서리 또는 소프트웨어를 판매하는 온라인 쇼핑 사이트로 이동
b) 링크를 클릭했을 때 컴퓨터를 감염시킬 수 있는 악성 코드

그렇다면 피싱 공격자가 기존의 수법을 (특히 (a)의 경우처럼) 납득하기 힘든 수법으로 바꾸는 이유는 도대체 무엇일까요? 그 이유는 다음과 같습니다.

- 이메일이 은행이나 소셜 네트워크와 같은 합법적인 조직이 보낸 것처럼 보일 경우 사용자가 링크를 클릭하기 쉽다는 건 이미 입증되었습니다. 따라서 이것은 단순한 클릭 사기일 가능성이 농후합니다.[14] 이런 웹사이트가 홍보를 위해 피싱 공격자에게 대가를 지불하고 있을 가능성이 높지만 홍보 효과는 미지수입니다.

13 http://en.wikipedia.org/wiki/IDN_homograph_attack

14 클릭 사기는 클릭 횟수당 비용을 지불한다는 점에서 일종의 인터넷 범죄에 해당됩니다(http://en.wikipedia.org/wiki/Pay_per_click 온라인 광고를 참조하십시오). 사기는 광고를 실제 사용자들이 클릭한 것처럼 위장하거나 실제 사용자들의 클릭을 유도하는 방식으로 이뤄집니다. 그리고 클릭할 때마다 요금이 발생합니다. 광고 링크의 내용에 정말 관심이 있는 사용자와 달리, 이런 클릭은 전혀 관심이 없는 상태로 이뤄지기 때문에 아무런 이득 없이 요금만 부과되는 셈입니다. 자세한 사항은 http://en.wikipedia.org/wiki/Click_fraud를 참조하십시오.

- 단 몇 분 만에 보안 솔루션에 의해 차단될지도 모르는 가짜 은행 사이트를 개설하는 데는 지나치게 많은 공을 들어야 합니다. 오히려 사용자의 컴퓨터에 트로이목마를 설치하는 방법이 훨씬 더 저렴하고 편리합니다. 왜냐하면 트로이목마가 사용자의 주거래 은행과 무관하게 개인의 금융 거래용 기밀 정보를 수집할 수 있기 때문입니다.
- 모조 의약품, 소프트웨어 및 패션 액세서리 판매는 여전히 수익성 높은 사업인데 일부 사용자는 은행이나 소셜 네트워크에서 발송한 이메일에 있는 링크를 클릭할 때 온라인 쇼핑 사이트가 나타나는 이유를 대수롭지 않게 여길 수도 있습니다. 이것은 사용자를 온라인 쇼핑 사이트로 유인하는 여러 가지 방법 중 하나일 뿐입니다.

IBM X-Force가 조사한 (특히 2011년에 두드러진) 최근 피싱 동향에서 나타난 또 다른 수리학적, 통계적 결과가 있습니다. 피싱 이메일처럼 보이는 스팸 중 다수가 일반적인 의약품 판매 스팸이나 악성 코드 스팸이라는 것입니다. 그러나 많은 통계에서는 이런 스팸도 피싱 이메일로 간주해서 집계합니다. 그렇다고 이런 집계가 반드시 잘못됐다고 보기는 어렵습니다. 왜냐하면 악성 코드 링크의 경우 데이터 절도용 악성 코드가 기밀 정보를 수집할 가능성이 있어서 이런 스팸을 피싱 이메일로 분류하는 게 옳을 수도 있기 때문입니다.

일반적인 스팸, 피싱, 그리고 악성 코드 스팸 간의 차이점이 갈수록 모호해지고 있습니다. 피싱 통계에 큰 영향을 미칠 수 있는 기타 양상으로는 다음과 같은 것들이 있습니다.

- 이번 단원에서는 일반적인 이메일 형식으로 발송되는 피싱 이메일만 거론합니다. 따라서 소셜 네트워크에서 발송한 것처럼 위장한 피싱 메시지는 제외됩니다.
- 여기서 언급하는 통계는 수신한 피싱 이메일의 무명수(absolute number)를 집계한 것입니다. 2008년에 비해 공격 빈도가 2011년 중반까지 감소했습니다. 반면에 여러 보고서에는 피싱 이메일이 증가한 것으로 조사되어 있습니다. 이는 공격 횟수만 집계한 것이므로 이 두 통계가 상충하는 건 아닙니다. 즉, 공격 횟수는 늘었지만 이메일이 동원된 공격은 오히려 줄었을 수 있습니다. 스피어 피싱(오른쪽 참조)은 이메일 종류 중 하나일 뿐입니다.
- 악성 코드가 사용자의 금융 거래용 기밀 정보를 노리는 경우라도 이메일의 내용이 표적이 된 브랜드와 무관한 악성 코드 첨부 파일이나 악성 코드 링크가 있는 스팸은 지금부터 제공되는 통계에 포함되지 않았습니다.

따라서 여러 가지 조건에 따라 피싱 이메일 통계가 달리질 수 있습니다. 다음 페이지부터 소개되는 통계는 앞서 언급한 양상 때문에 '피싱 이메일처럼 보이는" 스팸을 포함해서 산정한 결과입니다. 온라인 범죄자들이 사용자가 악성 링크를 클릭하도록 유도하는 데 어떤 종류의 브랜드가 악용되는지 조사해서 분석하는 것도 흥미로울 듯합니다. 이런 사기 이메일을 일반 용어로 '스캠(scam)'이라고 합니다.

스피어 피싱
스피어 피싱은 일종의 맞춤형 피싱입니다. 피싱 공격자는 사회공학 기법을 활용하여 일단 각종 개인정보를 수집합니다. 그런 다음 수집한 데이터를 이용해서 피해자에게 맞는 메시지를 작성합니다. 메시지가 개인적인 내용이라 피해자는 메시지를 합법적으로 여기고 곧장 함정에 빠지게 됩니다. 자세한 내용은 http://en.wikipedia.org/wiki/Spear_phishing#phishing_techniques를 참조하십시오.

이메일 사기와 스팸의 최근 동향

앞서 언급한 수법을 조사해본 결과, 전통적인 피싱 이메일이 (특히 2010년에) 눈에 띄게 감소한 것으로 나타났습니다. 그러나 2011년 하반기에는 신뢰할 수 있는 기업이나 조직의 이름을 도용하여 사용자가 링크를 클릭하도록 유도하는 수법이 유행하면서 이런 피싱 이메일 형식의 스팸과 사기 이메일이 각각 크게 증가했습니다.

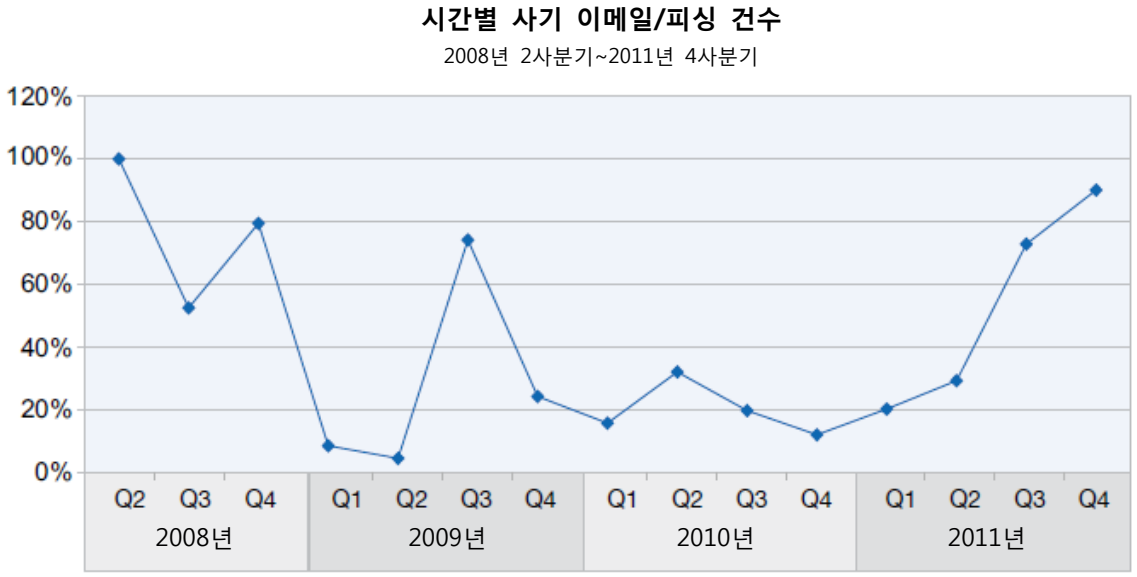


그림 25: 시간별 사기 이메일/피싱 건수(2008년 2사분기~2011년 4사분기)

다음 지도는 국가별 피싱 이메일 형식의 스팸 발송 비율을 보여주고 있습니다.[15]

그림 26: 피싱 이메일 발송 국가 지리적 분포

국가	피싱 이메일 비율	국가	피싱 이메일 비율
인도네시아	15.1%	호주	5.0%
인도	10.7%	한국	4.5%
중국	6.9%	미국	4.4%
브라질	5.9%	페루	3.8%
베트남	5.8%	파키스탄	2.6%

도표 2: 사기 이메일/피싱 이메일 발송 국가 상위 10개국(2011년)

15 사기 이메일/피싱 이메일 발송 국가란 이런 종류의 이메일을 발송한 서버가 위치한 국가를 의미합니다. 대다수 사기 이메일/피싱 이메일은 봇 네트워크에 의해 발송되는 것으로 IBM X-Force는 추정하고 있습니다. 봇은 어디에서든 제어가 가능하므로 사기 이메일/피싱 이메일을 보내는 실제 배후의 국적은 피싱 이메일 발송 국가와 다를 수 있습니다.

이 단원 초반에 설명한 사기 이메일/피싱 이메일의 변화로 인해 공격 목표로 삼는 산업도 바뀌었습니다. [16]

- 2009년까지 금융기관을 가장한 전통적인 피싱 이메일이 전체 피싱 이메일의 50%의 이상을 차지할 정도로 압도적으로 많았습니다. 금융 기관을 가장한 피싱 이메일이 2010년부터 2011년 가을까지 급감하더니 2011년 말경에 15% 내외로 회복되었습니다.
- 온라인 쇼핑 사이트는 2010년 중반에 온라인 범죄자들이 가장 선호하는 공격 수법이었지만 2011년에는 비중이 크게 줄었습니다.
- 택배 서비스가 2010년 하반기에 널리 악용되어 전체 사기 이메일/피싱 이메일의 20% 정도를 차지했습니다. 그리고 2011년 2사분기에는 평판이 좋은 택배 서비스 회사를 가장한 스팸이 50% 이상이었지만 2011년 종반에 이런 유형의 스팸은 거의 자취를 감췄습니다.
- IBM X-Force가 이런 유형의 이메일을 모니터링하기 시작한 2010년 초 이후 소셜 네트워크가 항상 1, 2위를 유지할 정도를 강세를 보이고 있습니다. 2011년 초에 평판 좋은 합법적인 브랜드를 이용하여 소셜 네트워크에서 보낸 것처럼 위장한 이메일이 80% 이상을 차지하다가 2011년 하반기에 43%로 안정세를 찾았습니다.

사기 이메일/피싱 이메일의 각 산업 위장 비율

2009년~2011년

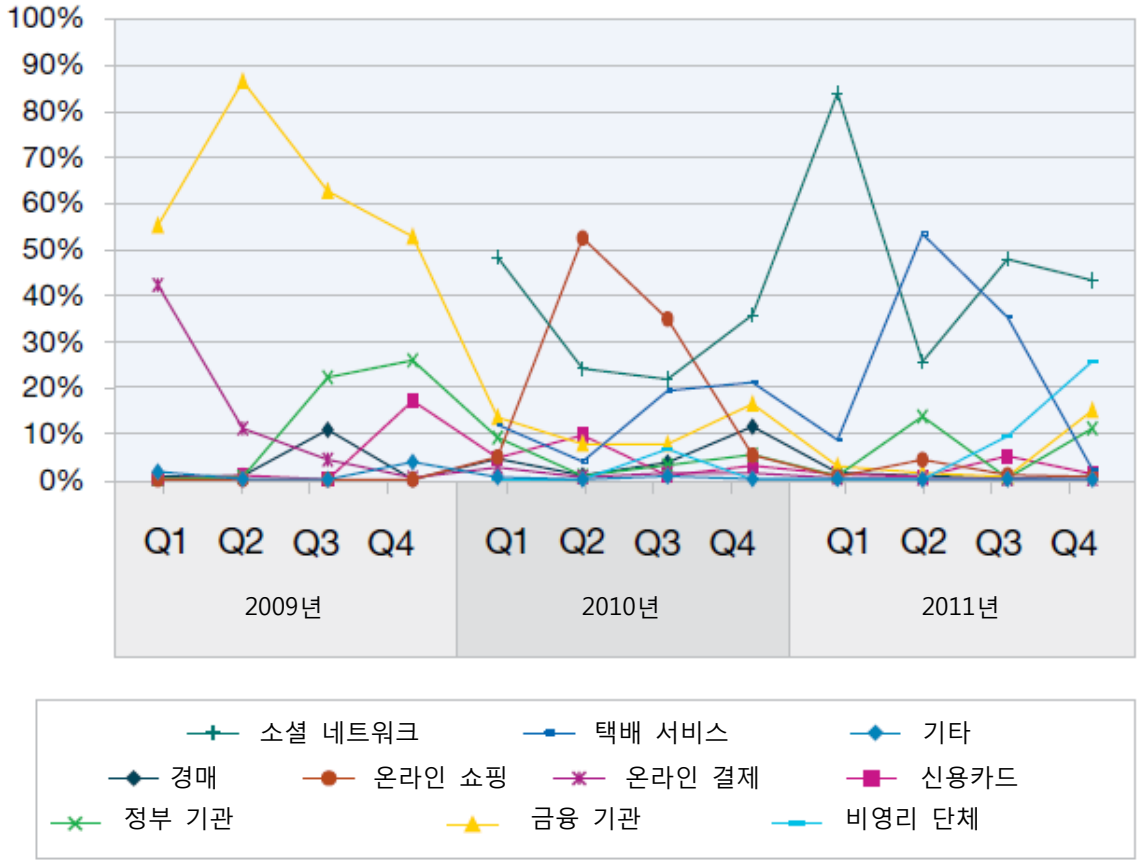


그림 27: 사기 이메일/피싱 이메일의 각 산업 위장 비율(2009년~2011년)[17]

16 2011년 상반기 동향 및 위험 보고서에서는 소셜 네트워크, 택배 서비스 및 비영리 단체를 취합하지 않은 데다 실제로 전통적인 피싱 수법은 사용하지 않고 브랜드의 이름만 악용한 이메일은 통계에서 제외했기 때문에 이번의 통계 수치와 크게 다릅니다.

17 소셜 네트워크, 택배 서비스 및 비영리 단체에 관한 2010년 이전 통계는 존재하지 않습니다.

스팸의 진화

IBM X-Force는 지난 몇 년간 스팸의 여러 동향과 유형을 조사하여 2011년 상반기 동향 및 위험 보고서에 소개했는데, 세월이 흐르면서 스팸이 어떻게 변해왔는지 되짚어보는 것도 흥미로울 듯합니다.

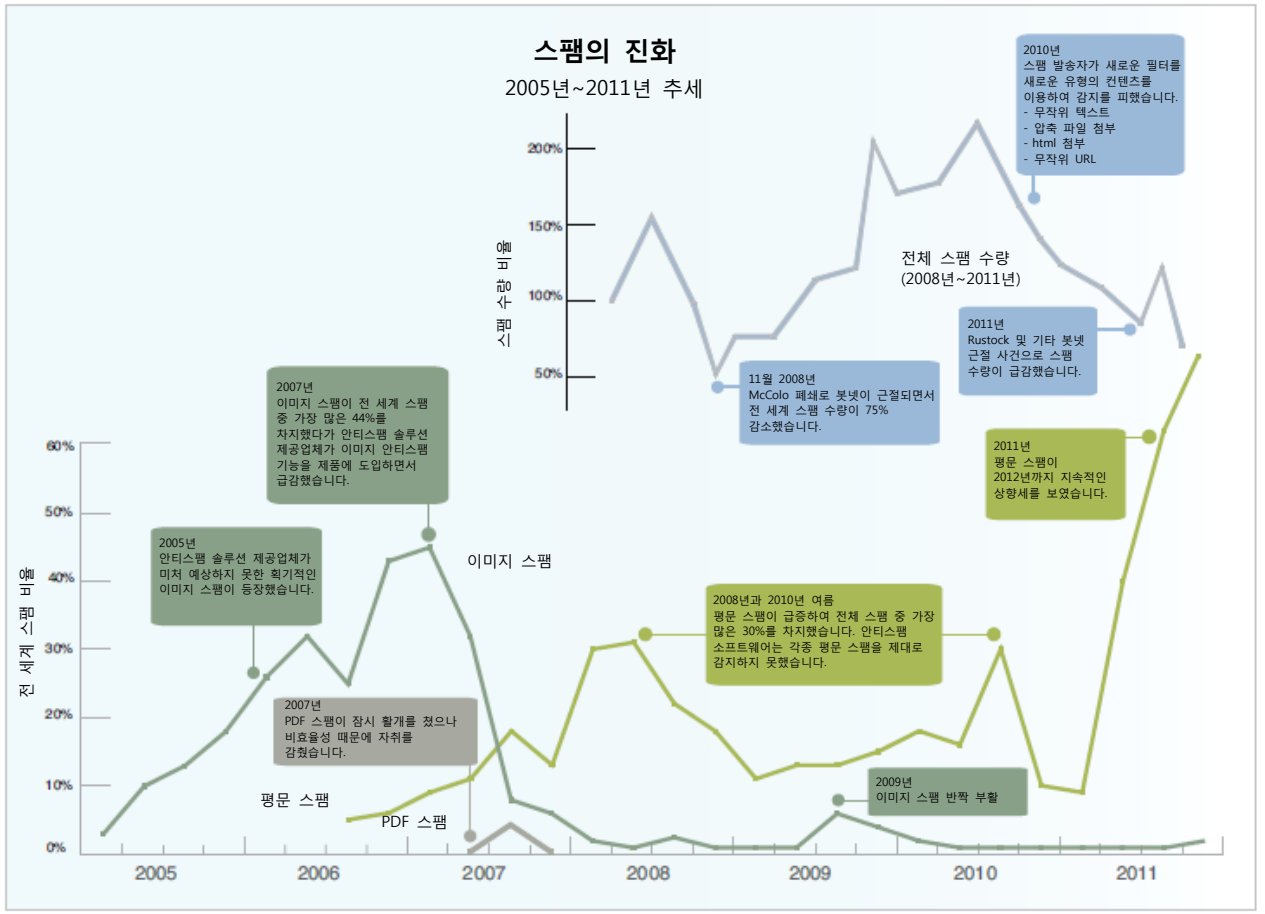


그림 28: 스팸의 진화 - 2005년부터 2011년까지의 추세 변화

2005년~2006년 – 이미지 스팸

2005년에 스팸 발송자들은 대대적으로 이미지 중심의 스팸을 사용하기 시작했습니다. 2005년 말경에 이미지 중심의 스팸은 전체 스팸의 20%를 육박하더니 2007년 초에 44% 이상으로 급증했습니다. 하지만 그 뒤로 급격히 감소했는데 그 이유는 무엇일까요?

처음에는 대다수 안티스팸 솔루션 제공업체가 이런 유형의 스팸을 예상하지 못한 것은 물론이고 심지어 일부 안티스팸 솔루션 제공업체는 이미지가 첨부된 이메일을 합법적인 이메일의 기준으로 삼았기 때문에 스팸 발송자들이 효과를 톡톡히 보았습니다. 그러나 이미지 중심의 스팸이 기승을 부린지 2년 뒤 모든 안티스팸 솔루션 제공업체가 이런 유형의 스팸을 불법 이메일로 분류하도록 감지 방식을 수정했습니다. 이런 유형의 스팸은 여러 가지 특징이 명확히 나타나기 때문에 미심쩍은 패턴을 검사하기가 오히려 쉬워서 2007년에 이르자 거의 완벽하게 차단되었습니다.

2007년 PDF 스팸

2007년 봄과 초여름에 이미지 중심의 스팸이 급감하더니 PDF 첨부 파일을 사용한 스팸이 고개를 들기 시작했습니다. 2007년 8월에 전체 스팸의 거의 20%를 차지할 정도로 많은 양의 PDF 스팸이 사용되었습니다. PDF 스팸 추세에 대한 자세한 사항은 Frequency-X 블로그를 참조하십시오.

PDF 스팸은 수명이 짧았습니다. 스팸 발송자들은 안티스팸 솔루션 제공업체가 이런 종류의 첨부 파일에 미처 대비하지 않았기를 기대하고 이미지 중심의 스팸으로 초반에 거뒀던 '성공'을 한 번 더 누리고자 애썼겠지만 그들의 희망이 물거품이 되자 스팸 발송자들은 재빨리 이 수법을 포기했습니다.

MP3 스팸은 PDF 스팸보다 훨씬 더 생명이 짧았습니다. 이 수법은 10월에 등장했다가 단 며칠 만에 자취를 감췄습니다. 여름 동안 유포된 MP3 스팸 분량은 PDF 스팸보다 훨씬 적었습니다. 흥미롭게도 MP3 스팸의 소스 코드는 PDF 스팸과 대단히 유사했습니다. MP3 스팸에 대한 자세한 내용은 Frequency-X 블로그를 참조하십시오.

2008년 McColo 폐쇄로 인한 1차 스팸 급감

2008년 상반기에 (HTML 코드가 없는) 평문 스팸의 비율이 큰 폭으로 증가했습니다. 평문으로 작성된 스팸이 처음으로 30%를 넘어섰습니다. 2010년 여름에도 이와 유사하게 평문 스팸이 급증하더니 2011년 말에 전체 스팸의 70%를 상회하는 역대 최고치를 기록했습니다. 평문으로 된 스팸은 정해진 특징(예: 일정한 패턴을 형성하는 특별한 종류의 첨부파일이나 비정상적으로 분할된 html 코드)이 전혀 없기 때문에 컨텐츠 기반의 스팸 감지가 훨씬 더 어렵습니다. 그러나 합법적 이메일의 추세는 오히려 거꾸로 되었습니다. 현재 HTML를 사용하지 않는 메시지나 뉴스레터는 예전에 비해 줄었습니다. 이런 이메일의 특징 때문에 단순한 평문 스팸이 의심을 살 확률이 높아졌는데 이것이 차단 기준으로 사용될 날도 멀지 않은 듯합니다.

2008년 11월 11일에 스팸양 증가에 가장 큰 타격을 입힌 사건이 발생했는데 다름 아닌 McColo 폐쇄 사건입니다. 그날 하루에 전 세계 스팸양이 75%나 감소했습니다!

더 흥미로운 점은 스팸 발원지(일반적으로 스팸 봇이 위치한 국가)의 뚜렷한 변화입니다. 전 세계의 스팸 봇 운영 본부나 다름없던 McColo가 미국에서 퇴출되자 McColo 폐쇄 시점을 직후로 갑자기 스팸 유포 국가 및 유포량에 엄청난 변화가 나타났습니다. 미국은 수년간 스팸 발원지 목록 최상단에 이름을 올리고 있었고 McColo 폐쇄 사건 6일 전만 해도 1위를 지키고 있었습니다.

그런데 McColo 폐쇄 사건 6일 후 미국의 스팸 산출량은 이전 분량의 14%로 급감했습니다. 그러니 미국이 마침내 1위 자리를 내준 건 그리 놀라운 결과도 아닙니다.

2009년 – 1차 스팸양 절정기

3월에 스팸 발송자들은 또 다시 이미지 중심의 스팸을 이용해서 여러 차례 공격을 감행했습니다. 기술적 측면에서 새로운 수법이 개발된 건 전혀 아니었기 때문에 대다수 안티스팸 필터가 이미지 스팸을 인식해서 차단하는 데 별 어려움이 없었습니다. 그러나 이 시기의 스팸에 첨부된 이미지 내용은 차이가 있었습니다. 2007년에 발송된 대다수 이미지 스팸의 주제는 주식 거래였습니다. 그런데 이번에는 금융 위기가 닥치자 마약의 유혹에 대한 관심이 높아졌던 것입니다. 부활한 이미지 스팸에 대한 자세한 내용은 Frequency-X 블로그를 참조하십시오.

그렇다면 스팸 발송자들이 (이미지만 보여지고 클릭은 불가능하기 때문에) 사용자가 실제로 URL을 브라우저에 직접 입력해야만 성공할 수 있는데도 고전적인 수법으로 회귀한 이유는 대체 무엇일까요?
한 가지 이유는 2009년에 스팸 발송자들이 전체 스팸양을 크게 늘린 데서 찾을 수 있습니다. 그런 맥락에서 이미지 스팸은 동시다발적 공격이 가능하다는 장점이 있습니다.

McColo가 폐쇄된 지 1년 뒤인 2009년 11월에 전 세계 스팸 발송량은 1차 절정기를 맞았습니다.

McColo 폐쇄 이전의 상위 스팸 발송 국가 5개	
미국	14.2%
러시아	11.0%
터키	7.4%
스페인	5.9%
브라질	4.8%

McColo 폐쇄 이후의 상위 스팸 발송 국가 5개	
중국	12.7%
러시아	11.4%
미국	8.0%
한국	6.2%
브라질	5.8%

2008년 말의 상위 스팸 발송 국가 5개	
브라질	11.7%
미국	8.1%
중국	6.6%
터키	5.7%
러시아	5.7%

도표 3: McColo 폐쇄 이전과 이후의 상위 스팸 발송 국가 변화

2010년 – 1차 장기적 스팸 감소 및 HTML 첨부 파일과 같은 스팸 내용의 대대적인 급변
과거와 대조적으로 2010년에는 사상 처음으로 스팸양이 별다른 증가세를 보이지 않았습니다. 대신, 스팸 내용에 과거에 볼 수 없었던 다양한 변화가 나타났습니다. 2010년에 나타난 변화를 예로 들자면 다음과 같습니다.

- 무작위 텍스트와 무작위 URL이 조합된 스팸이 등장하면서 스팸의 평균 용량이 크게 증가했습니다.
- 2010년 8월 초에 스팸 발송자들은 ZIP 파일이 첨부된 스팸을 발송하기 시작했습니다. IBM X-Force가 이 메시지를 조사해보니 ZIP 파일에는 각기 하나의 악성 EXE 파일이 포함되어 있었습니다. ZIP 파일이 첨부된 스팸에 대한 자세한 사항은 Frequency-X 블로그에서 확인하실 수 있습니다.
- 1년간 나타난 스팸 내용의 다양성에 미루어 봤을 때 스팸 발송자들이 양보다 '질'을 중시하게 됐음을 알 수 있습니다. 대량 발송은 더 이상 스팸 필터를 통과할 수 있는 해결책이 되지 못했습니다.

2011년 – Rustock 봇넷 박멸의 영향에 힘입은 2차 스팸 감소세
3월 16일에 Rustock 봇넷 박멸에 힘입어 스팸 발송량이 절반으로 감소하는 흥미로운 현상이 발생했습니다. Rustock 봇넷 박멸에 대한 자세한 내용은 IBM X-Force 2011년 상반기 동향 및 위험 보고서에 소개되어 있습니다. 2008년 11월의 McColo 폐쇄 사건과 달리 이 때는 스팸 발송량이 빠른 회복세를 보이지 않았습니다. 그러나 스팸 발송자들은 이에 굴하지 않고 필터에 감지되지 않는 방법을 찾기 위해 다음과 같은 새로운 수법을 동원했습니다.

- 악성 코드 ZIP 스팸(여름과 가을)
- 이미지 스팸(11월)

이에 대한 자세한 내용은 이미 이전 단원에서 소개했습니다.

장기적 스팸 동향 – 발송 국가
- 인도는 전 세계에서 유일하게 꾸준히 스팸 발송량이 증가했습니다.
- 브라질은 2009년의 McColo 폐쇄로 가장 큰 폭으로 스팸양이 증가했지만 이후 꾸준한 감소세입니다.
- McColo 폐쇄로 인해 스팸양이 대폭 감소했지만 2009년부터 증가세로 돌아섰습니다.
- 인도네시아는 2011년 3월 Rustock 박멸의 영향을 받아 가장 큰 폭으로 스팸양이 증가하여 처음으로 스팸 발송 국가 상위권 명단에 올랐습니다.
- 주로 Rustock 봇넷 박멸에 힘입어 미국의 스팸 발송량이 사상 처음으로 총 스팸의 4% 미만으로 떨어졌습니다.
- 대한민국은 4% 수준을 꾸준히 유지하고 있습니다.
- 프랑스, 스페인, 터키는 전년도에 비해 스팸 발송량이 크게 감소했습니다.

장기적 스팸 동향 – 불변의 원칙
앞서 언급한 모든 변화와 별도로 다음과 같은 몇 가지 기본 원칙은 변하지 않았습니다.

- 모조 명품 시계, 의약품 및 소프트웨어와 같은 고전적인 주제를 활용한 스팸이 여전히 기승을 부리고 있습니다. 그 이유는 이런 수법이 불법적으로 돈을 버는 데 효과적인 것으로 이미 검증되었기 때문으로 분석됩니다.
- 스팸과 특히 피싱에는 여전히 사용자가 링크를 클릭하도록 유도하는 수법이 사용되고 있습니다. 그러나 스팸 발송자들은 사용자가 링크를 클릭했을 때 발생하는 결과와 무관한 내용을 스팸의 메시지에 기재했는데, 그로 인해 스팸은 다음과 같은 특징을 보이고 있습니다.
  - 모조 명품 시계, 의약품 및 소프트웨어와 같은 제품 판매에 목적을 둔 완벽한 피싱 이메일 형식의 스팸

  - 화제가 되는 뉴스나 기타 관심을 끌만한 주제를 소개한 후 그에 대한 자세한 내용을 보려면 링크를 클릭하라고 유도하고 링크를 클릭하면 사용자의 시스템을 감염시키는 스팸
  - 다른 내용은 전혀 없이 링크만 있는 스팸

- 적응 속도가 빨라졌습니다. 스팸 발송자들은 스팸을 차단하려는 온갖 노력을 무용지물로 만들기 위해 신속하게 수법을 보완했습니다. 이미지 스팸이 2년(2005년~2007년) 넘게 널리 사용된 반면, 2011년에 등장한 다른 스팸 발송 수법의 수명은 고작 10~14주입니다. 그러나 스팸 발송 국가는 훨씬 느린 속도로 바뀌고 있습니다. 봇넷 역시 보급 속도가 비교적 더딥니다. 스팸 발송자들이 향후 봇넷 확보 속도를 개선할 수 있을지 지켜볼 만합니다.
- 스팸의 평균 용량이 2008년 이후 다시 꾸준히 증가해서 3킬로바이트에 이르게 되었습니다. 이 크기를 스팸의 표준 용량으로 봐도 무방할 것 같습니다.
- 스팸 발송자들이 항상 새로운 수법을 시도하고 있습니다. 다음 단원에서는 어떤 일이 벌어질 수 있는지 예측해보겠습니다.

스팸의 미래 전망

2011년 상반기에는 과거의 추세와 달리 회복세 없이 스팸 수량이 상당히 큰 폭으로 하락했습니다. 전통적인 이메일 스팸의 '사업 여건'이 변한 것입니다.

- McColo 또는 Rustock 스팸 근절 사건에서 알 수 있듯이 조직이나 기업들이 스팸 유포 용도로 사용되는 봇넷이나 인프라를 근절하는 데 성공했습니다. (그에 대한 자세한 내용은 2011년 상반기 동향 및 분석 보고서를 참조하십시오.)
- 스팸 필터가 지속적으로 개선되고 있습니다.
- "Click Trajectories: End-to-End Analysis of the Spam Value Chain(궤도 추적: 스팸의 가치사슬 종합 분석)[18]에서 언급했듯이 스팸 발송자의 활동을 무력화 할만한 다른 접근법들이 등장하고 있습니다. 이 연구 자료에 따르면 스팸 광고 상품의 결제 금액 중 95%가 세 은행에서 집중 처리되고 있습니다. 스팸 피해자의 은행들은 이 세 은행에 지급되는 결제를 차단할 수 있습니다.

이런 조치가 취해질 경우 스팸 발송자들은 소셜 네트워크에서 스팸을 유포하거나 분산 서비스 거부(DDoS) 공격을 감행하는 등 다른 방법에 관심을 돌리게 될 것입니다. 일부 노련한 스팸 발송자는 스팸 사업이 더 이상 매력적이지 않다고 판단하고 있습니다.[19] 그와 대조적으로 기존의 공격자나 새로운 공격자가 더 많은 스팸을 전송하게 될 요인도 존재합니다.

- 인터넷 사용자 수가 여전히 늘고 있습니다. 따라서 수신자가 실제로 읽게 되는 스팸 이메일이 만 개 중 단 하나에 불과하더라도, 스팸 및 피싱 공격의 새로운 피해자는 얼마든지 있습니다.
- 공격자가 노릴 수 있는 시스템 대수 역시 꾸준히 증가하고 있습니다. 게다가 새로운 유형의 기기까지 등장했습니다. 대표적인 기기가 바로 스마트폰입니다. 스팸 발송자의 관점에서 보자면 이 휴대형 컴퓨터는 또 다른 매력이 있습니다. 사용하지 않을 때는 전원을 끄는 데스크탑 PC와 달리, 스마트폰은 항상 온라인 상태입니다. 현재 대다수 사용자가 모바일 인터넷 사용료를 정액제로 부담하지 않기 때문에 여전히 스마트폰의 대역폭이 제한되어 있습니다. 하지만 앞으로는 이런 양상이 바뀔 가능성이 높습니다. 자세한 사항은 '모바일 악성 코드 전망' 절을 참조하십시오.
- 스팸 컨텐츠의 유형 측면에서 스팸 발송자가 아직 사용하지 않는 수법이 몇 가지 있습니다(예: Open Office 문서를 스팸에 첨부하는 수법).
- 사용자가 스팸의 링크를 클릭할 가능성을 높이기 위해 스팸 발송자가 가짜 발신자로 이용할만한 유명 브랜드 이름이 많습니다.
- IPv6 덕분에, 특히 IP 차단 기능에만 의존할 경우 스팸 발송자가 사용자를 귀찮게 하고 안티스팸 솔루션 제공업체를 괴롭힐만한 여러 가지 새로운 수법이 등장할 수 있습니다.

18 http://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf
19 http://www.itworld.com/security/178991/internet-evolves-there-place-spam

단원 2
운영 보안 현황

이 단원에서는 오늘날의 공격자들이 노리는 프로세스, 소프트웨어 및 인프라의 약점과 관련한 주제를 탐구합니다. 구체적으로 말해서, 이 단원에서는 보안 규정 준수 모범 사례, 운영비 절감 아이디어, 자동화, 소유 비용 절감, 그리고 업무, 제품 및 역할 통합에 대해 논의합니다. 또한 이런 문제를 관리하거나 최소화하는 과정에서 IBM이 얻은 정보도 소개합니다.

SI(Security Intelligence) 도입: 실시간 보안에 관한 통합 접근법

지난 몇 년간의 보안 공격 증가, 컴퓨팅 모델 확대(그에 따른 공격 범위 확대), 그리고 폭발적인 데이터 증가로 인해 보안 전문가들은 중대한 과제에 직면했습니다. 그리고 기업은 전례 없이 다양해지는 위협을 막는 데 주력하고 있습니다.

보안 침입 사고가 발생했는지 파악하는 일조차 여의치 않아서 심각한 침해 사실을 모른 채 몇 달간 방치하는 기업도 있습니다. 일부 기업은 원시 데이터를 보유하고 있지만 보안 침해를 감지할 가시성과 분석 능력이 부족합니다. Verizon의 2011년 데이터 침해 조사 보고서는 69%의 보안 침입 사건에서 기업의 로그 파일에 명확한 침입 증거가 있었는데도 데이터 과부하 때문에 그런 증거를 거의 발견하지 못했다고 결론 짓고 있습니다.

따라서 오늘날의 침해 감지 여부는 두 가지 요소에 달려 있습니다. 두 가지 요소란 수백만 개에 달하는 데이터 요소의 미심쩍은 활동을 포착하는 것과 다수의 미심쩍은 사고에서 중요한 사고를 추려내는 것입니다. 이 두 가지 작업을 위해 기업은 1) 모든 관련 데이터를 분석하고, 2) 문제의 징후를 지능적으로 포착하며, 3) 그 정보를 사전 예방에 활용할 수 있는 접근법을 갖춰야 합니다.

이를 충족하기 위해 보안 현황 전체를 중앙 집중식으로 모니터링하고 실시간으로 분석할 수 있는 SI(Security Intelligence)라는 새로운 계열의 솔루션이 개발되었습니다.

새로운 현실을 인식한 IBM은 보안 정보 수집 및 분석의 미래를 지원하기 위해 과감한 조치를 단행했습니다. IBM은 단일한 IBM Security Systems 사업부를 통해 다양한 정보 보안 원칙을 통합하는 한편, 보안 정보 및 이벤트 관리(SIEM)와 보안 정보 수집 분야의 선두업체인 Q1 Labs를 인수함으로써 이 문제를 정면 돌파하고 있습니다.

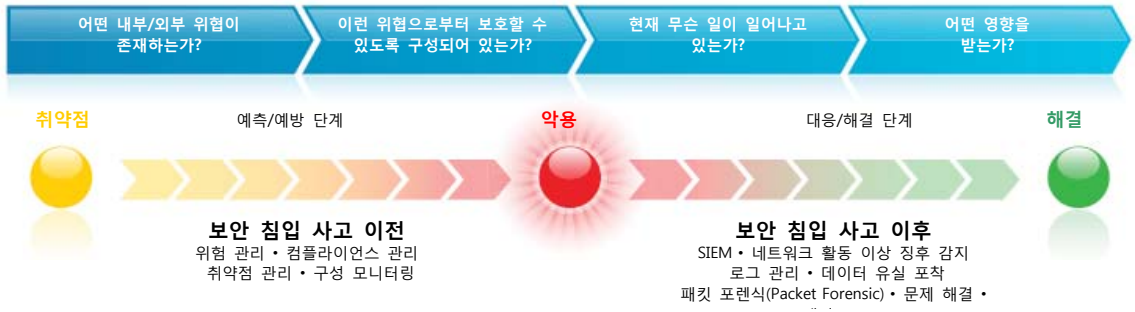
SI(Security Intelligence) 정의

SI(Security Intelligence)는 다음과 같이 정의할 수 있습니다.

SI(Security Intelligence)는 사용자, 애플리케이션 및 인프라에 의해 생성되며 기업의 IT 보안 및 위험 상황에 영향을 미치는 데이터를 실시간으로 수집, 정규화 및 분석하는 솔루션입니다. SI의 목표는 모든 규모의 조직이 위험 부담을 줄이고 운영 효율성을 개선할 수 있도록 유용하고 폭넓은 통찰력을 제공하는 것입니다.

SI 솔루션은 로그, 이벤트, 네트워크 흐름, 사용자 ID 및 활동, 자원 프로파일 및 위치, 취약점, 자원 구성, 그리고 외부 위협 데이터를 수집해서 보관합니다. SI 솔루션은 모든 시간대의 위험 및 위협 관리를 포괄하는 기본적인 문제에 대한 해답을 얻을 수 있는 분석 기술을 지원합니다.

각 시점에서 SI(Security Intelligence)의 역할



SI(Security Intelligence) 솔루션은 네 가지 핵심 위험 영역인 사람, 데이터, 애플리케이션, 그리고 인프라를 포괄하여 기업의 보안 및 위험 상황을 종합적으로 관리하는 데 효과적입니다.

SIEM 및 로그 관리 제품에 익숙한 사람들은 SI 솔루션을 차세대 기술로 인정할 지도 모르겠습니다. SI 솔루션은 악용 방지 기능, 더욱 폭넓어진 데이터 수집 능력, 그리고 더욱 심층적인 정보 제공 능력이 더해져서 SIEM와 로그 관리 제품을 능가합니다.

SI 솔루션은 보다 우수한 내외부의 위협 방지, 감지 및 우선순위 지정 기능을 지원하며 컴플라이언스 문제를 자동으로 모니터링 및 보고합니다.

또한 SI 솔루션은 보안 사고에 대해 폭넓은 가시성을 제공합니다. 예를 들어, SI 솔루션은 심층적인 패킷 검사를 통해 네트워크 흐름을 분석하고 사용자 활동을 모니터링하여 이상 징후를 감지하므로 직원의 행동이 미심쩍어서 내부자의 데이터 절취나 외부인의 계정 도용 가능성이 엿보일 경우 이를 포착하는 데 유용합니다.

뿐만 아니라 SI 솔루션은 IPS 경보에 네트워크 토폴로지의 취약점 검사 결과 및 정보를 반영하므로 취약한 자산을 노리고 있는 침입 시도와 무시해도 좋을 침입 시도를 구분하기가 수월합니다.

BI(Business Intelligence)와의 유사점

BI(Business Intelligence)와 SI(Security Intelligence)의 유사점을 살펴보는 것도 유익할 듯 싶습니다. BI는 대량의 비즈니스 정보를 취합해서 다음과 같이 유용한 고급 비즈니스 정보를 추출합니다.

어떤 제품이 어떤 고객 부분에서 잘 팔리는가?

최근 판촉 활동에 대해 어떤 지리적 장소의 반응이 가장 좋은가?

한 제품 라인은 수익성이 향상되고 있는 반면 다른 제품 라인의 수익성이 떨어지고 있는 이유는 무엇인가?

이와 유사하게 SI(Security Intelligence)는 대량의 보안 정보를 취합해서 다음과 같이 IT 부서 및 LOB(Line Of Business)와 관련된 유용한 고급 보안 정보를 추출합니다.

자사가 어떤 유형의 공격에 가장 취약한가? (보안 방침 및 관리 방식을 어떻게 수정해야 하는가?)

자사에 가장 심각한 보안 위협을 초래할 가능성이 있는 비즈니스 파트너와 협력업체는 어디인가? (자사의 접근 통제 수준을 높이거나 해당 업체에 더 엄격한 통제를 요구해야 하는가?)

모바일 컴퓨팅 환경으로 인해 새로운 보안 문제나 컴플라이언스 문제가 발생할 우려가 있는가? (만일 그렇다면 어떤 문제에 관심을 기울여야 하는가?)

SI와 BI의 한 가지 차이점은 SI는 실시간 정보 수집 및 모니터링 기능을 제공하는 반면, 일반적으로 BI는 특정 시점의 정보를 반영한다는 점입니다. 두 솔루션 모두 대단히 유용한 관리 도구이지만 보안 및 컴플라이언스 문제에서는 실시간 정보가 무엇보다 중요합니다.

BI는 비즈니스 계획 수립 및 비즈니스 운영 환경의 가시성 확보에 이상적인 표준 도구로 자리잡았습니다. 마찬가지로 SI는 보안 계획 수립 및 보안 운영 환경의 가시성 확보에 이상적인 표준 도구로 자리잡고 있습니다. 게다가 SI는 IT 부서와 LOB(Line Of Business)가 보안 협의를 통해 사업 방식 및 제안에 수반되는 위험이나 대가를 평가할 수 있는 실질적인 기반으로 활용하기 적합합니다.

SI(Security Intelligence)의 핵심 개념

SI(security Intelligence)의 세 가지 핵심 개념인 지능, 통합 및 자동화는 사용자가 신속하게 생산성을 확보하는 데 도움이 됩니다.

몇 가지 예를 들어서 세 가지 원칙의 특징을 설명하겠습니다.

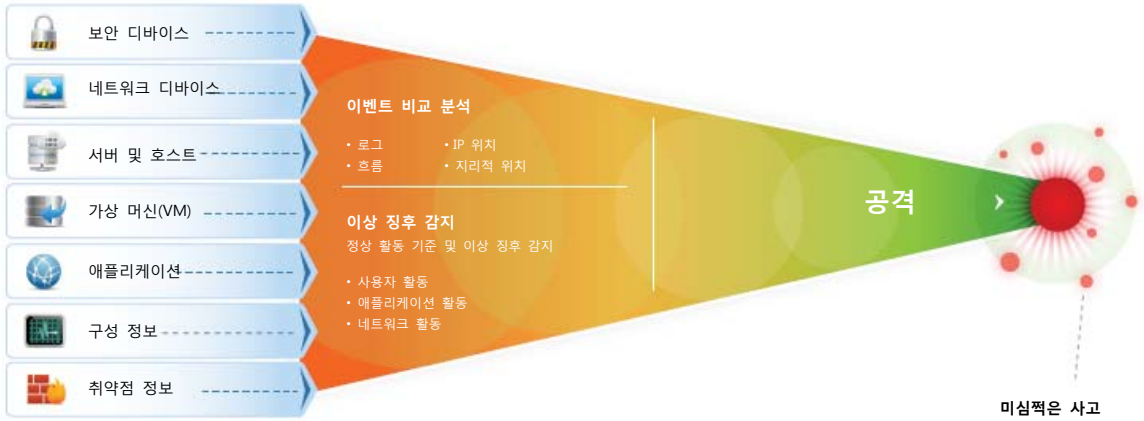
1. **지능**: SI는 대량의 보안 및 컴플라이언스 관련 데이터를 인식할 수 있습니다. 따라서 빅 데이터(Big Data)(보안 정보 자체가 빅 데이터입니다) 규모의 다양한 정보를 저장, 비교 분석, 보고 및 조사하여 유용한 고급 정보를 제공합니다.

2. **통합**: 지능의 토대 역할을 하며 이질적인 데이터에 대한 일관적이고 표준화된 분석을 실현합니다. 유형과 용량이 각기 다른 보안 관련 데이터를 수집 및 취합하므로 보안 이벤트에 대한 제한적이고 2차원적인 시야를 다각적으로 폭넓게 상황을 인식하는 시야로 확대할 수 있습니다.

– **예:** SI(Security Intelligence) 솔루션이 기본적으로 지원하는 통합 능력은 보안 분석가의 생산성에 막대한 영향을 미칩니다. 수백 가지 출처에서 확보한 데이터를 표준화하므로 고객(및 컨설턴트)가 각 솔루션 제공업체의 데이터 구조에 대해 전문적인 지식이 없어도 무방합니다. 가령, 컴플라이언스 의무 때문에 인증 이벤트(로그인 실패, 로그인 성공, 접근 권한 상승 이후의 로그인 성공 등)를 문서화할 필요가 없습니다. SI를 이용하면 더 이상 데이터 구조가 각기 다른 수십 가지 자원을 수동으로 추적할 필요가 없습니다.

3. **자동화:** 자동화는 불필요한 복잡성 해소 및 총소유비용(TCO) 절감을 통해 SI가 신개념의 기술로 각광 받게 된 데 일조하고 있습니다. 보다 폭넓은 데이터 사용(예: 네트워크 흐름)과 손쉽게 활용할 수 있도록 제품화된 지적 자산에 의해 업무 자동화가 실현됩니다.

가장 다양한 종류의 데이터에 고급 분석 기술 응용



SI(Security Intelligence)는 SIEM과 어떻게 다른가?

SI(Security Intelligence)는 다음과 같은 중요한 측면에서 1세대 SIEM(Security Information and Event Management) 기술보다 우수합니다.

네트워크 활동 모니터링 및 네트워크 흐름 분석: 과거에는 디바이스, 애플리케이션, 서버 및 인프라 서비스의 로그를 통해 상황을 추론했습니다. 그러나 이제 로그는 실마리일 뿐입니다. 3차원적 상황 이해 및 가시성을 확보하려면 네트워크 흐름 수집, 패킷 심층 조사 및 패킷(컨텐츠) 포착이 필요합니다. SI는 다음과 같은 흐름 분석을 통해 사용자의 습성, 소셜 미디어 이용 상황, 모바일 현황, 클라우드 현황 등을 실시간으로 파악합니다.

해당 통신에 포트 80 웹 트래픽이나 은닉한 봇넷 IRC 통신이 사용되고 있는가?

침입자가 취약한 직원 계정을 도용하여 민감한 데이터를 절취하고 있는가?

직원이 부적절한 방법으로 민감한 지적 자산에 접근하고 있는가?

SI(Security Intelligence)는 SIEM(Security Information and Event Management) 및 네트워크 활동 모니터링(컨텐츠 포착) 기능 통합으로 패킷 수준의 가시성을 확보했기 때문에 그와 같은 고급 정보를 제공할 수 있습니다.

예측 분석 및 악용 사전 인식: SI에는 악용 방지 옵션과 취약점 관리 기능이 통합되어 있습니다. 따라서 SI를 이용하면 잘못 구성된 디바이스(예: 방화벽)이나 해결되지 않은 취약점으로 인해 수반되는 위험을 파악하고 우선순위를 정하여 체계적으로 해소할 수 있습니다.

이상 징후 감지: 다수의 전통적인 보안 솔루션은 대중에게 공개된 취약점 및 일반적인 악성 코드와 같은 알려진 위협으로부터 기업을 보호하는 데 초점이 맞춰져 있습니다. 그러나 오늘날의 보안 환경에서는 완전히 새로운 공격 수법이 사용되는 정교한 집중 공격을 감지해야 할 필요성이 갈수록 커지고 있습니다. 또한 내부자의 위협은 승인 받은 활동에 대한 분석을 통해서만 감지할 수 있는 경우가 빈번합니다. 이상 징후 중심의 분석 방식은 이런 유형의 활동을 파악하는 데 효과적입니다.

더욱 손쉬운 배치 및 필요 인력 감소: SIEM 제품이 처음 출시됐을 때 얼리 어댑터(early adopter)는 이 제품을 실용화하는 데 상당한 시간과 비용을 주저 없이 투자했습니다. 가령, 커넥터와 규칙을 새로 구축해야 했고 사용자는 사용법에 관한 교육을 받아야 했습니다. 하지만 실용화가 끝난 이후에도 조사를 요하는 '거짓 양성' 경보가 발령되는 비율이 높았기 때문에 상당히 많은 인력이 필요했습니다. SI 솔루션은 더욱 폭넓은 종류의 정보(이벤트, 흐름, 자산 프로파일, 네트워크 토폴로지, 취약점 등)를 활용하고 더욱 우수한 자동화를 지원하므로 데이터와 필요한 인력을 크게 줄일 수 있습니다.

주요 이점은 무엇인가?

SI 솔루션을 도입한 기업이 누릴 수 있는 이점을 살펴보겠습니다.

컴플라이언스 향상

SI는 기업 전반의 다양한 정보를 기록하고 사전 예방적으로 모니터링하는 방법으로 컴플라이언스 활동을 지원합니다. 가령, SI는 개방된 네트워크를 통해 민감한 데이터가 암호화되지 않은 채 전송되는지 모니터링하거나 방화벽이 적절히 구성되어 있는지 검사하거나 사용자가 중요한 시스템에 적절한 방법으로 접속하고 있는지 모니터링합니다. 또한 SI는 운영 효율성을 개선할 수 있습니다. 경우에 따라 보고 자동화 및 손쉬운 로그 및 흐름 검색을 통해 수천 시간의 수작업을 덜 수도 있습니다.

더욱 신속한 위협 감지 및 해소

경계가 사라진 오늘날의 세상에서 방지나 감지/치료 중 한 가지에만 주력하는 일은 질 게 뻔한 게임을 하는 것이나 다름없습니다. 두 가지 능력을 모두 갖춰야 합니다. 모바일 컴퓨팅, 소셜 미디어 혹은 클라우드 컴퓨팅 때문에 경계에 언제든 구멍이 생기기 쉽습니다. Forrester Research는 이를 '신뢰성 0(zero-trust)'의 환경으로 칭합니다. SI(Security Intelligence)는 기업이 침입을 방지함과 동시에 더욱 신속하게 침입을 감지해서 차단하므로 이런 문제를 해결하는 데 효과적입니다(아래의 '악용 방지로 위험 최소화' 참조). SI는 대량의 데이터를 실시간으로 비교 분석합니다. 다시 말해서, 네트워크 및 보안 디바이스, 서버, 애플리케이션, 디렉토리 서버에서 발생한 이벤트, 네트워크 활동 흐름(및 패킷 포착), 자산 정보, 구성 데이터, 그리고 취약점 정보를 분석하여 말 그대로 '건초더미에서 바늘을 찾아냅니다'. 또한 SI는 자산과 사용자가 공격을 당할 우려가 있는지 파악하고 포렌식(forensic) 조사 기법에 컨텐츠 포착 기능을 활용함으로써 더욱 신속하게 문제를 해결할 수 있습니다.

이를테면, Conficker이란 악성 코드가 2008년 말에 유포되기 시작한 시점에 인터넷의 TCP 포트 445 트래픽이 급증했습니다. SI 시스템은 보안 전문가들이 이 악성 코드를 Conficker라고 칭하기 훨씬 전에 이 트래픽 급증 현상을 감지해서 경고했습니다. 이런 방식의 예측 감지는 시그니처나 패치가 아직 개발되지 않은 상황에서 정교한 제로데이(zero day) 위협으로부터 컴퓨터 네트워크를 보호하는 데 도움이 됩니다.

내부자의 사기, 절취 및 데이터 누출 감소

세간의 이목을 끄는 공격은 대부분 외부 공격이지만 소중한 지적 자산이 누출되거나 심지어 국가 안보가 위험에 처할 수 있다는 점에서 내부자의 위협이 오히려 훨씬 더 치명적일 수 있습니다. SI는 다음과 같은 상황을 감지함으로써 이런 유형의 위협을 파악하고 최소화하는 데 유용합니다.

- 애플리케이션 무단 접근 또는 사용
- 데이터 유실(예: 인증 받지 않거나 생소한 목적지로 데이터 전송)
- 사용자 접속 문제(예: 권한 있는 사용자의 예외적인 접속)
- 애플리케이션 성능 문제(예: 서비스 장애 또는 과다 이용)

악용 방지로 위험 최소화

SI는 방화벽 및 IPS 디바이스와 같은 기본적인 침입 방지 도구를 기반으로 구축되며 기업이 공격을 차단하는 데 도움이 되는 새로운 비교 분석 기능과 함께 다음과 같은 기능을 지원합니다.

- (방화벽과 같은) 디바이스 구성 자동 모니터링 및 보안 취약점 및 정책 위반에 대한 자동 경보
- 네트워크 토폴로지 및 자산 가치를 토대로 취약점 조사 도구가 감지한 취약점의 해결 우선순위 지정
- 예측적 위협 모델링 및 네트워크 변화 시뮬레이션

SI 솔루션은 이전보다 훨씬 더 다양한 침입 방지 시나리오에 더욱 정밀한 정보를 제공할 수 있습니다. 가령, 컨텐츠 포착을 기반으로 네트워크 활동 흐름을 분석하여 보안 디바이스 규칙의 효과를 평가할 수 있는데, 그렇게 얻은 평가 결과는 구성 데이터 그 차체보다 훨씬 더 신뢰할 만합니다.

최근 어느 블로그 게시판에 게시된 내용을 인용하자면 "(구성 데이터만으로는) 구성이 적절하다고 생각했는데 어떤 이유로든 잠재적으로 위험한 네트워크 트래픽 때문에 문제가 확산될 소지가 여전히 존재하는 상황을 간파하지 못할 수 있습니다." 마찬가지로, 네트워크 토폴로지에 대한 정보를 확보하면 "취약점 검사 도구에서 흔히 발생하는 거짓 양성 반응을 최소화하고 네트워크 구성 방식 때문에 손쉽게 노출될 수 있는 취약점의 해결 우선순위를 정할 수 있습니다."

간편한 운영 및 필요 자원 최소화

SI(Security Intelligence) 솔루션은 지능적인 자동화를 활용하여 보안 운영을 능률화하고 보안 및 네트워크 전문가의 부담을 최소화합니다. 따라서 상당한 비용 절감 효과를 기대할 수 있습니다. 이런 이점은 지루하기 짝이 없는 수작업을 없애고 효율성을 개선한 데 기인합니다.

SI(Security Intelligence) 모범 사례

SI 솔루션을 배치할 때는 조직의 접근 방식과 기술적 능력에 따라 성공 가능성이 크게 달라지며, 다음과 같은 몇 가지 사항을 우선적으로 고려해야 합니다.

사고 보고 체계 정의: SI 솔루션은 방화벽 관리, 시스템 관리, 네트워크 관리를 비롯한 관리 그룹에 서비스를 제공한다는 점에서 사내 클라우드 서비스와 일맥상통합니다. 공공 클라우드 서비스와 마찬가지로 SI 솔루션 제공업체(일반적으로 보안 또는 위험 관리 그룹)은 솔루션 소비자와 협의하여 보안 사고 처리 및 보고 체계를 계약서에 명시해야 합니다. 경영진에게 직접 문제를 보고하는 체계는 적절하지 않을 수 있으며 소비자와의 관계가 훼손되어 소비자가 향후에 데이터를 제공하기 꺼릴 수 있습니다.

초기 배치 단계에 주요 용도 및 보고 사안 결정: 기업은 배치 초기에 모니터링 및 보고를 어떤 사안에 집중할 것인지 결정해야 합니다. 참고로, (봇넷 및 다크넷의 트래픽 같은) 보편적 외부 위협, 특정 산업의 위험, 내부자 위협, 정책 위반 및 접속 권한이 있는 사용자의 활동 등에 모니터링 및 보고를 집중하는 것이 일반적입니다.

지능적으로 이상 징후 감지: 특이한 징후를 감지하려면 SI 솔루션이 관측된 활동을 토대로 관심 영역(사용자, 애플리케이션, 네트워크) 전체의 정상 상태에 대한 기준을 정해서 그 기준을 벗어난 이례적 활동을 포착해야 합니다. 상황에 맞게 탄력적으로 기준을 적용하는 환경을 자동화하면 기준 수정에 수반되는 수작업을 줄일 수 있습니다.

심층적 패킷 검사를 토대로 한 흐름 분석: 앞서 설명했듯이 패킷 포착을 활용한 흐름 분석은 보안 및 컴플라이언스 문제를 파악하는 데 효과적입니다. 패킷 검사를 토대로 한 흐름 분석은 잘못된 네트워크 구성을 파악함으로써 침입 방지 능력을 개선하고, 패킷 수준의 가시성을 제공함으로써 보안 문제 감지 능력을 강화하며, 다양한 이용 상황에서 누가 어떤 데이터에 접근하는지 알려줌으로써 포렌식(forensic) 조사 능력을 극대화할 수 있습니다.

예측 분석: 예방 능력이 강화된 보안 체제를 원하는 기업은 디바이스 구성 모니터링, 컴플라이언스 정책 모니터링, 그리고 취약점 해결 우선순위와 같은 작업의 우선순위를 정해야 합니다.

결론

요약하자면, SI(Security Intelligence) 솔루션은 강력한 기업 보안 지원 도구이며 실시간 정보와 심층적 분석을 통해 유용한 정보를 제공할 수 있습니다. SI 솔루션은 보안 솔루션의 고질적인 아킬레스건이었던 지능, 통합, 그리고 자동화를 개선함으로써 IT 부서와 LOB(Line Of Business) 모두에게 상당한 이득을 선사합니다. SI 솔루션은 대기업 뿐 아니라 중소기업도 구현 및 관리하기 적합하며 실제 문제의 합리적인 해결책이 될 수 있습니다.

참조:

1. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations- report-2011년_en_xg.pdf
2. http://blog.q1labs.com/2011년/07/28/defining-security-intelligence/
3. http://blog.q1labs.com/2010년/08/26/do-we-need-a-security-analog-for-business-intelligence- absolutely-we-do/
4. http://q1labs.com/resource-center/white-papers/details.aspx?id=113
5. http://blog.q1labs.com/2011년/10/20/three-ways-to-embrace-the-zero-trust-environment/
6. http://q1labs.com/resource-center/case-studies/details.aspx?id=114
7. http://blog.q1labs.com/2011년/06/16/latest-gartner-report-shines-bright-light-on-qradar-risk- manager/
8. http://q1labs.com/resource-center/white-papers/details.aspx?id=113
9. http://blog.q1labs.com/2010년/09/17/siem-is-a-security-intelligence-cloud/
10. http://q1labs.com/resource-center/brochures/details.aspx?id=129

2011년의 취약점 발견

1997년 이후 X-Force는 공개적으로 노출된 소프트웨어 제품의 보안 취약점을 추적해 왔습니다. X-Force 분석가들은 취약점, 패치 정보 및 악용 사례가 노출된 일반 이메일 주소 목록과 웹사이트를 분석하고 대중에게 공개된 사항을 기록하고 있습니다.

2011년에는 새로 보고된 보안 취약점은 7,000건을 약간 상회했습니다. 역대로 가장 많은 취약점이 보고된 해였던 2010년에 비하면 크게 감소한 수치지만 2006년 이후 취약점 발견 건수는 2년을 주기로 등락을 반복하고 있습니다. 다만, 상승한 해와 하락한 해 모두 그 비율은 꾸준히 높아지고 있습니다.

2007년에 처음으로 전체 취약점 건수가 감소했는데 가장 큰 이유는 취약점 발생 여건이 변하고 있기 때문으로 추정됩니다. 그러나 돌이켜 보면 이는 일시적인 이상 현상이었을 뿐, 그 이후로 전체 취약점 건수는 다시 오름세로 돌아섰습니다. 과거 6년간 나타났던 주기가 올해에도 반복된다면 2012년은 취약점 발견 건수가 또 한 번 갱신될 가능성이 높습니다.

웹 애플리케이션

2011년에 가장 큰 감소세를 보인 보안 취약점의 범주는 웹 애플리케이션 취약점입니다. 지난 몇 년간 발생한 보안 취약점 발견 건수 중 절반 정도가 웹 애플리케이션 취약점이었습니다.

그러나 2011년에는 그 수치가 2005년 이후 가장 낮은 41%로 하락했습니다. 2010년 이후의 웹 애플리케이션 취약점을 보여주고 있는 그림 30을 참조하십시오. 웹 애플리케이션 취약점의 유형을 살펴보자면, 크게 감소한 범주로는 SQL 인젝션 취약점이 두드러집니다.

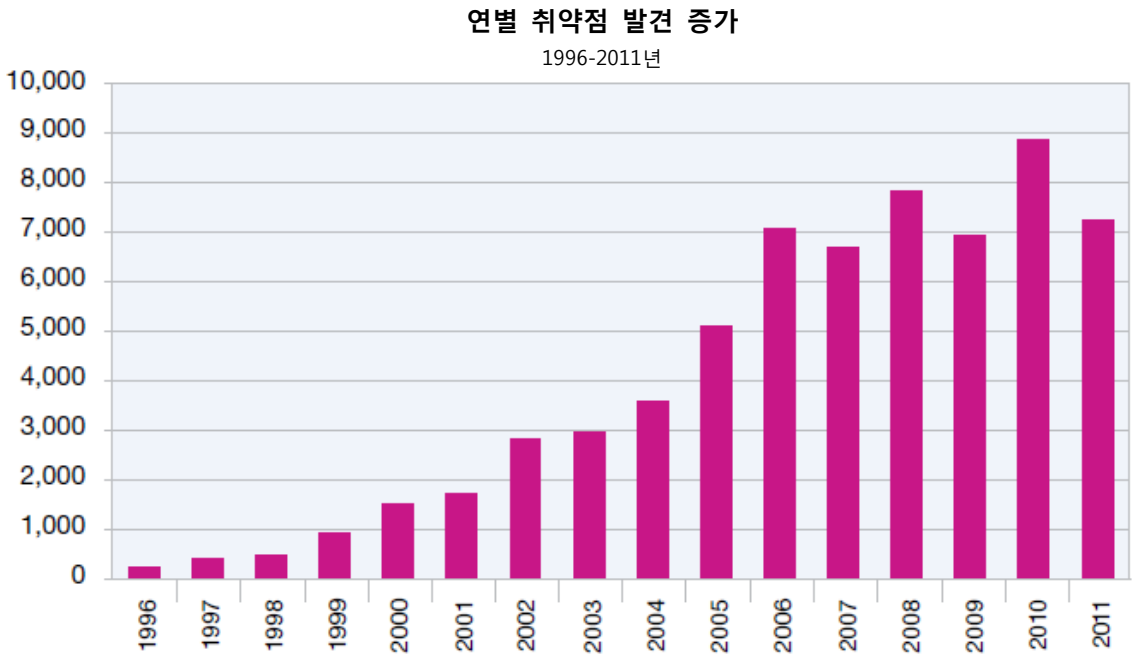


그림 29: 연별 취약점 발견 증가(1996년~2011년)

SQL 인젝션 취약점은 IBM이 전 세계 수천 개의 네트워크를 모니터링 및 보호하면서 가장 흔히 볼 수 있었던 공격 수법이기 때문에 특히 중요합니다. 봇넷 개발자가 금전을 노리고 감행한 SQL 인젝션 공격은 취약한 웹사이트를 자동으로 찾습니다. 이런 사이트는 자바스크립트 리디렉터(redirctor)에 감염되어 방문자를 위험에 빠뜨릴 수 있습니다.

SQL 인젝션 공격은 손쉬운 상대를 공략하기 위해 웹을 뒤지는 세련되지 못한 공격자가 선호하는 수법입니다. 특이하게도 2011년에는 비교적 정교한 공격자들이 몇 차례 대규모 침입 공격에 SQL 인젝션 공격 수법을 사용했습니다.

SQL 인젝션 취약점이 있는 인터넷 기반의 웹 애플리케이션을 사용하는 경우 머지않아 공격 목표가 될 가능성이 높습니다. 따라서 이런 취약점을 해소할 필요가 있습니다. SQL 인젝션 공격 빈도가 감소한 것은 웹 애플리케이션 개발자가 더욱 현명해져서 애플리케이션의 취약점이 줄었기 때문으로 해석할 수도 있습니다. 만일 그렇다면 긍정적인 소식이지만 아직도 풀어야 할 숙제가 많습니다.

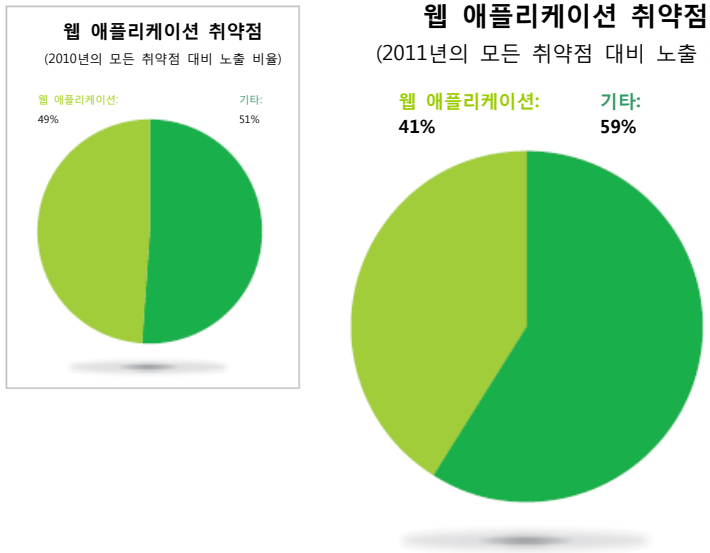


그림 30: 웹 애플리케이션 취약점(2011년의 모든 취약점 대비 노출 비율)

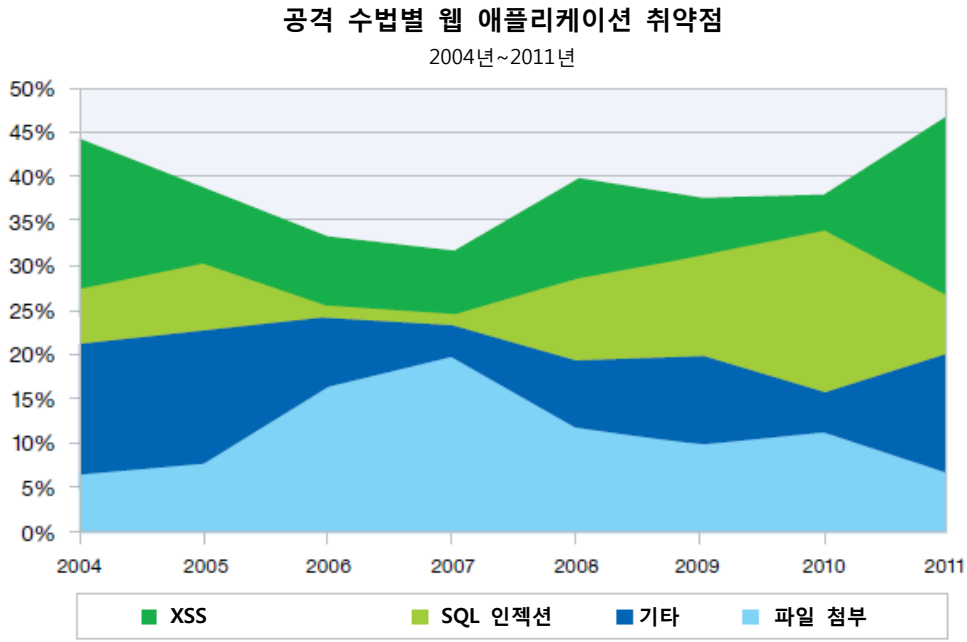


그림 31: 공격 수법별 웹 애플리케이션 취약점(2004년~2011년)

2011년에는 거의 3천 건의 웹 애플리케이션 취약점이 노출됐는데, X-Force가 파악한 웹 애플리케이션 취약점 총 건수는 개방적인 인터넷에 존재하는 것 중 빙산의 일각에 불과할지도 모릅니다. 그 이유는 X-Force가 오직 공개적으로 노출된 취약점만 추적하고 있기 때문입니다. 기업이 관리하는 웹 애플리케이션이나 제 3자에게 배포할 목적으로 추진하는 오픈 소스 프로젝트는 취약점을 공개할 의무가 있습니다.

그러나 웹 애플리케이션의 대부분은 조직 내부나 사기업에 의해 특정 웹사이트에 독점 사용할 목적으로 개발되는 맞춤형 소프트웨어가 차지합니다. 이런 맞춤형 웹 애플리케이션은 취약점이 공개되는 경우가 많지 않습니다. 맞춤형 웹 애플리케이션은 사용자가 한정되어 있기 때문에 취약점을 대중에게 알릴 필요가 전혀 없습니다.

IBM AppScan OnDemand 사용자를 대상으로 한 설문조사를 통해 맞춤형 웹 애플리케이션의 상태를 분석한 결과, 맞춤형 웹 애플리케이션의 취약점이 상당 수준 개선된 것으로 확인되었습니다. 그러나 이 조사 표본은 한정적일 가능성도 없지 않습니다. 사실, 코드의 보안성을 개선하기 위해 IBM을 선택할 만큼 현명한 개발자라면 일단 보안 문제를 피하는 데 급급한 일반 개발자들보다 개선 수준이 더 높을 것으로 미루어 짐작할 수 있습니다. 그러므로 인터넷에서 사용되고 있는 웹 애플리케이션의 실제 보안 상태는 X-Force가 조사한 것보다 더 나쁠 가능성이 있습니다. X-Force가 파악한 공격 활동 횟수 역시 이런 결론을 확실히 뒷받침합니다.

대중에게 노출된 취약점이면서 다수의 공격 빈도를 기록한 웹 애플리케이션 중 하나는 웹 기반 컨텐츠 관리 시스템(CMS)입니다. IBM X-Force가 네 가지 웹 기반 컨텐츠 관리 시스템을 분석해 본 결과, 이런 시스템의 가장 심각한 약점은 그 시스템이 지원하는 타사의 플러그인 환경에 기인한 것으로 확인되었습니다.

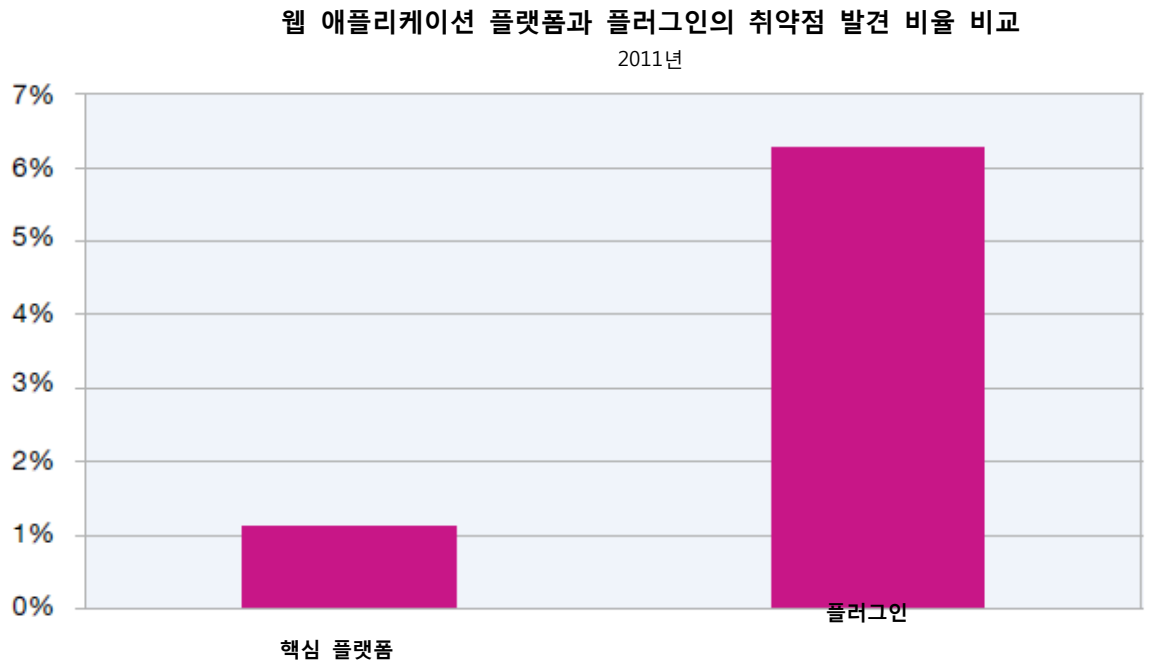


그림 32: 웹 애플리케이션 플랫폼과 플러그인의 취약점 발견 비율 비교(2011년)

CMS 플러그인보다 핵심 CMS 플랫폼에서 노출된 취약점이 훨씬 더 적으며 핵심 CMS 플랫폼의 취약점은 패치가 배포되는 비율도 훨씬 더 높습니다. 이런 이유 중 하나는 많은 플러그인 개발자들의 보안 문제에 대한 지원과 관심 수준이 제각기 큰 차이가 있기 때문입니다.

웹 기반 CMS의 취약점은 공개적으로 노출되는 데다 인터넷의 수많은 웹사이트에 영향을 미치고 있기 때문에 공격자들이 선호하는 공격 목표입니다. 2011년에 CMS의 제로데이 취약점은 수많은 보안 침입 사고에 악용되었습니다. 웹 기반 CMS 소프트웨어 사용자는 본인이 이용하는 플러그인 제공업체의 보안 정책에 관심을 기울일 필요가 있습니다.

그리고 핵심 소프트웨어와 플러그인의 보안 취약점 발견을 면밀히 모니터링하고 꾸준한 패치를 무엇보다 중시해야 합니다. 또한 애플리케이션 계층의 방화벽 배치나 침입 방지를 통해 웹사이트 보호 대책을 강화하는 것도 고려해 볼 만합니다.

CMS 플랫폼 취약점(2011년)

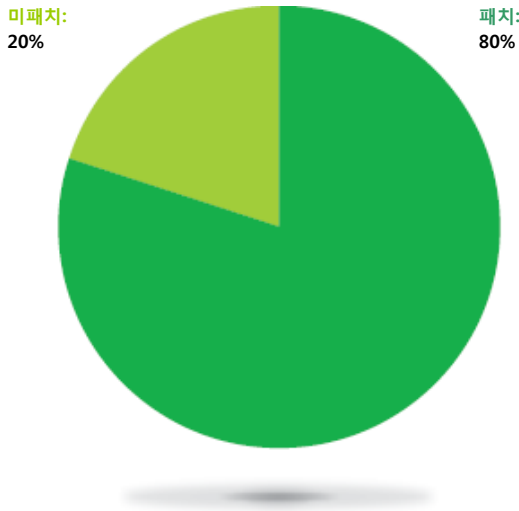


그림 33: 패치를 실시한 상태와 실시하지 않은 상태의 핵심 컨텐츠 관리 시스템의 취약점 발견 비율 비교(2011년)

CMS 플러그인 취약점(2011년)

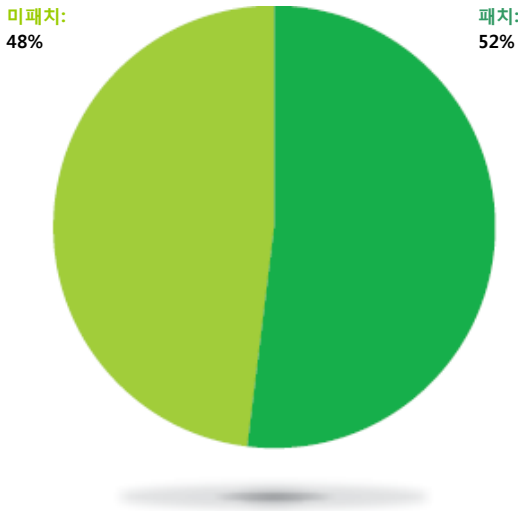


그림 34: 패치를 실시한 상태와 실시하지 않은 상태의 플러그인 컨텐츠 관리 시스템의 취약점 발견 비율 비교(2011년)

악용 건수 감소

웹 애플리케이션의 보안 향상 외에도 낙관론을 가질만한 또 다른 이유가 있습니다. 2011년에 공개적으로 노출된 악용 건수는 크게 감소하여 2006년 이후 가장 적은 건수를 기록했습니다. 실제 건수뿐 아니라 비율 역시 줄었습니다. 지난 몇 년간 공개적 취약점 악용 비율은 15% 내외였지만 2011년에는 11%에 그쳤습니다.

이런 감소세는 지난 몇 년간 대규모 공격의 표적이 됐던 특정 분야에도 나타났습니다. 웹 브라우저는 수년간 자동 다운로드(drive-by-download) 공격 수법의 주요 표적이었습니다. 중대하거나 심각한 브라우저 취약점의 건수는 해마다 늘었지만 브라우저 취약점을 노리고 유포된 악성 코드 건수는 2006년 이후 가장 적었습니다. 브라우저 대신, 제 3의 브라우저 플러그인을 노린 자동 다운로드 공격은 증가했습니다.

이런 유형의 공격에 공격자들이 선호하는 수단은 문서 판독 도구입니다. 왜냐하면 악성 문서 파일을 이메일에 첨부하거나 악성 코드를 자동으로 다운로드하는 데 사용할 수 있기 때문입니다. 2010년에 문서 형식 취약점과 그와 관련한 악성 코드 유포 건수는 역대 최고치를 기록했지만, 2011년에는 취약점 발견 건수가 소폭 감소했으며 악성 코드 유포 건수 또한 2007년 이후 가장 적은 수준으로 급감했습니다. 이는 상당한 진전이라 할 수 있습니다.

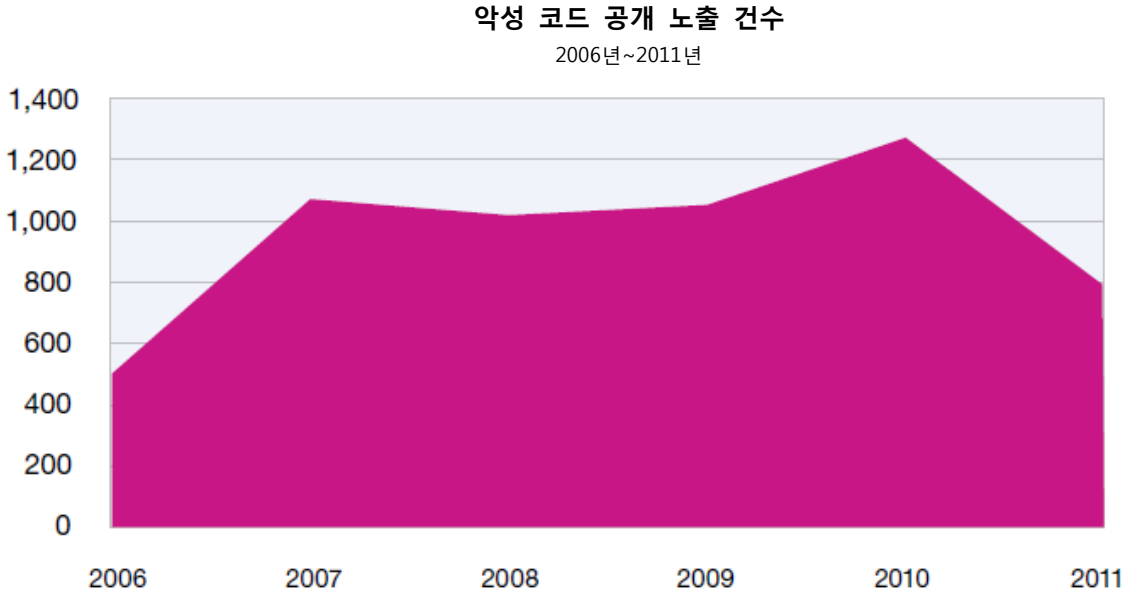


그림 35: 악성 코드 공개 노출 건수(2006년~2011년)

	2006년	2007년	2008년	2009년	2010년	2011년
공개 노출 건수	504	1078	1025	1059	1280	778
비율	7.3%	16.5%	13.3%	15.6%	14.7%	11.0%

도표 4: 악성 코드 공개 노출 건수 및 비율(2006년~2011년)

이런 진전은 지난 수년간 소프트웨어에 나타난 구조적 변화로 인해 악용하기가 더 까다로워진 데서 비롯된 것으로 보입니다. 이제 운영체제의 메모리 관리 도구에는 메모리 오류를 감지해서 안전하게 실행을 중단하는 다양한 기능을 지원하고 있습니다. 또한 많은 브라우저와 문서 판독기에 악성 코드가 침투에 성공하더라도 그 활동 범위를 제한하는 샌드박스(sandbox)가 구축되어 있습니다. 그로 인해 과거에는 단시간 내에 광범위하게 악용될 수 있었던 취약점이 이제 그 상태로도 수개월 동안 악용되지 않은 채 버틸 수 있게 되었습니다.

물론, 이와 같은 다양한 보안 대책이 마련됐다 해서 취약점을 악용하기가 불가능해진 건 아닙니다. X-Force 연구개발팀은 어려운 여건 속에서 코드가 실행되는 과정을 설명한 여러 가지 자료를 간행했습니다. 2012년에 X-Force 연구원 Mark Yason과 Paul Sabanal은 Blackhat USA에서 샌드박스가 구현된 애플리케이션 환경에서 악성 코드가 실행되는 방법을 논의한 Playing in the Reader X Sandbox를 발표한 바 있습니다. Chris Valasek 역시 같은 행사에서 방어가 철저한 Windows Heap에서도 코드가 실행되는 방법을 설명한 Understanding the Low Fragmentation Heap을 발표했습니다.

그러나 이 두 자료에 소개된 수법을 제대로 사용하려면 많은 시간과 노력, 기술이 필요합니다. 테스트 환경에서 악용할 수 있었던 심각한 취약점이 2011년에 실제로 표적이 된 횟수는 줄었습니다. 예전이라면 이렇게 얘기하는 게 섣부른 감이 있었지만, 이제는 컴퓨터 보안에 새로운 시대가 열리고 있다는 신호로 보아도 되지 않을까 싶습니다.

브라우저용 악성 코드 공개 노출 건수

2005년~2011년

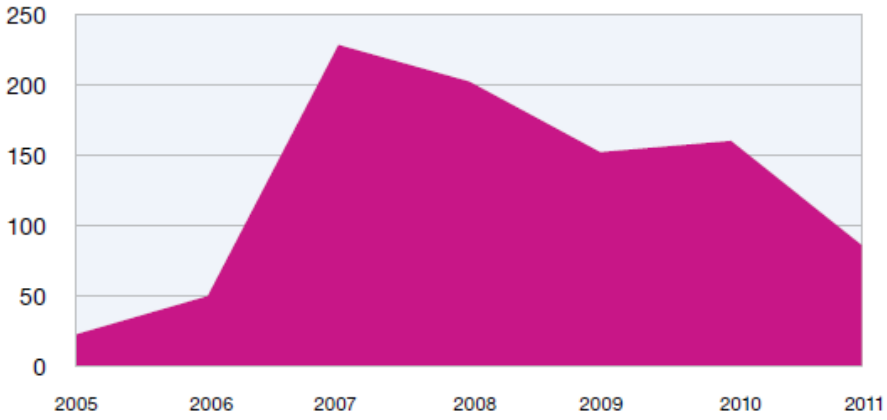


그림 36: 브라우저용 악성 코드 공개 노출 건수(2005년~2011년)

심각하거나 중대한 웹 브라우저 취약점 건수

2005년~2011년

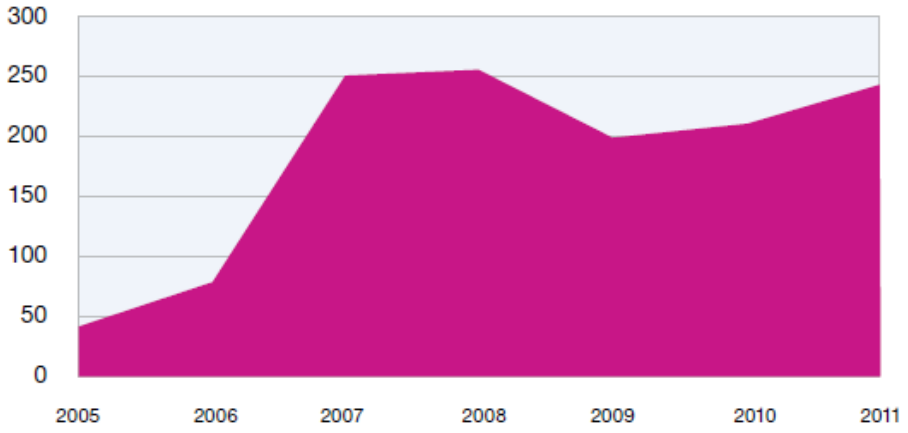


그림 37: 심각한 혹은 중대한 웹 브라우저 취약점 건수(2005년~-2011년)

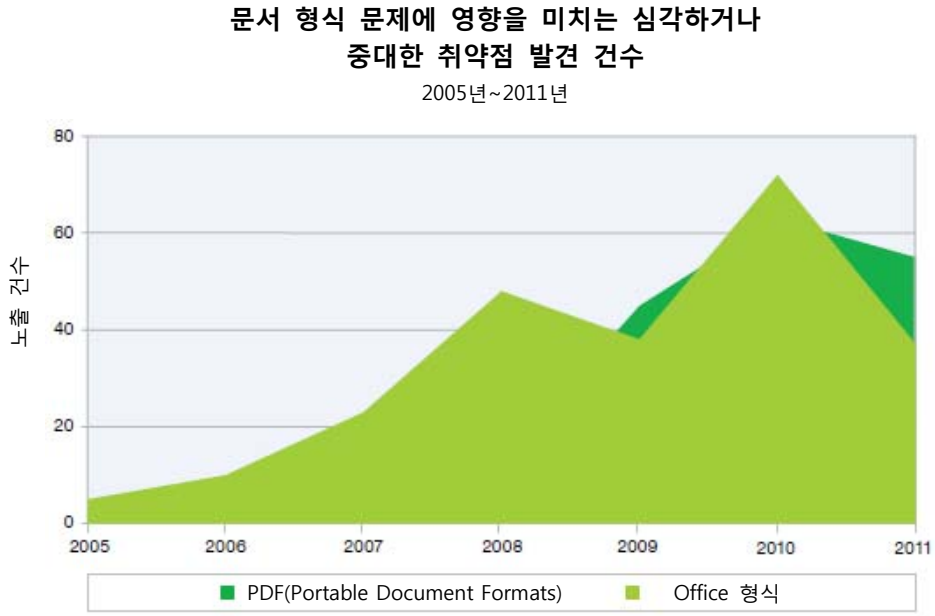


그림 38: 문서 형식 문제에 영향을 미치는 심각한 혹은 중대한 취약점 발견 건수(2005년~2011년)

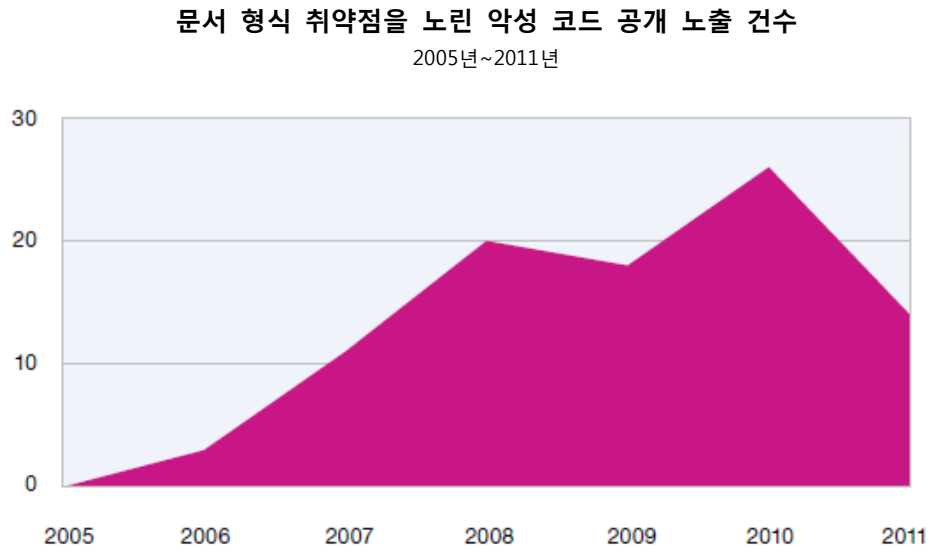


그림 39: 문서 형식 취약점을 노린 악성 코드 공개 노출 건수(2005년~2011년)

멀티미디어 소프트웨어에 영향을 미치는 심각하거나 중대한 취약점 발견
2005년~2011년

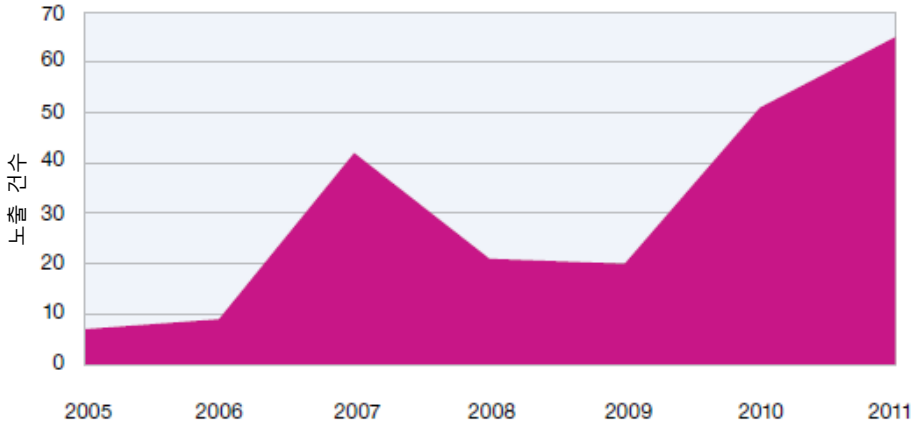


그림 40: 멀티미디어 소프트웨어에 영향을 미치는 심각한 혹은 중대한 취약점 발견(2005년~2011년)

멀티미디어 취약점을 노린 악성 코드 공개 노출 건수
2005년~2011년

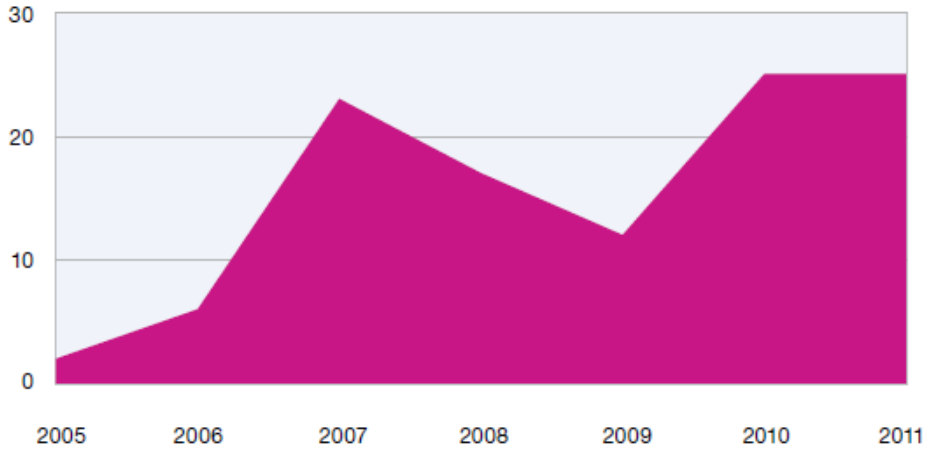


그림 41: 멀티미디어 취약점을 노린 악성 코드 공개 노출 건수(2005년~2011년)

공격자의 관심 분야 변화

물론, 해소해야 할 중요한 허점들이 여전히 있습니다. 멀티미디어 플레이어를 노린 취약점 공격 건수도 꾸준히 증가하고 있는데 2011년에도 2010년 못지않게 멀티미디어 취약점을 노린 대규모 공격이 빈번히 발생했습니다.

이 자료를 작성하는 시점을 기준으로 올해 초에 공개적으로 노출된 다수의 심각한 멀티미디어 취약점은 APT(Advanced Persistent Threat)가 수반된 정교한 표적형 공격에 계속 악용되고 있습니다. 이 악성 파일들은 이메일에 첨부해서 특정 피해자에 맞춰서 주의 깊게 작성한 이메일 문구와 함께 공격 대상에게 발송됩니다. 고도의 보안이 요구되는 환경에서는 멀티미디어 플레이어에 철저한 패치를 실시하거나 아예 사용하지 말아야 합니다.

모바일 디바이스 분야 역시 중요성이 부각되고 있는 분야입니다. 현재까지 다양한 모바일 운영체제의 취약점이 발견됐으며 이런 취약점을 노린 악성 코드가 대중에게 유포된 사례가 많습니다. 모바일 디바이스의 '탈옥'이나 최상위 관리자 권한 획득은 사용자들이 모바일 악성 코드를 온라인에 게시하도록 유도하는 주요 동기로 손꼽힙니다. 물론, 일단 활성화된 코드는 탈옥 상태가 아닌 모바일 디바이스에 악의적 용도로 사용될 수 있습니다.

모바일 운영체제 취약점 통계

2006년~2011년

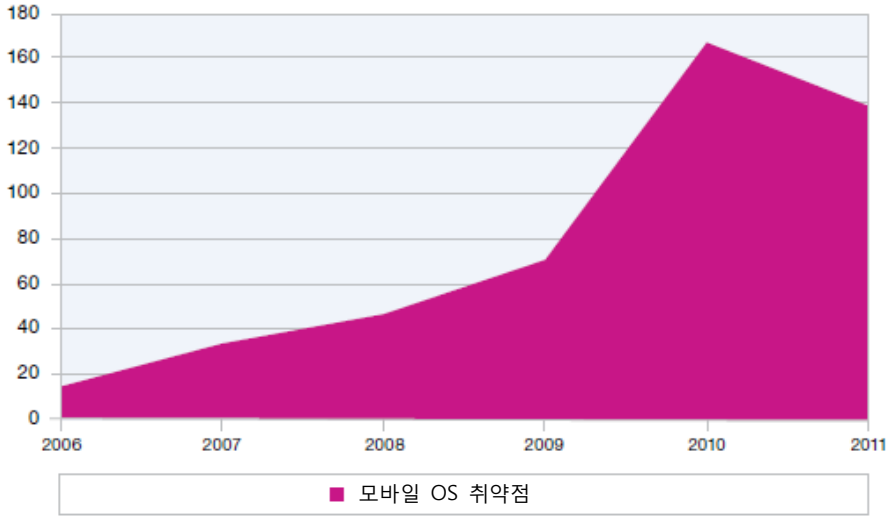


그림 42: 모바일 운영체제 취약점 통계(2006년~2011년)

모바일 운영체제를 노린 악성 코드 건수

2006년~2011년

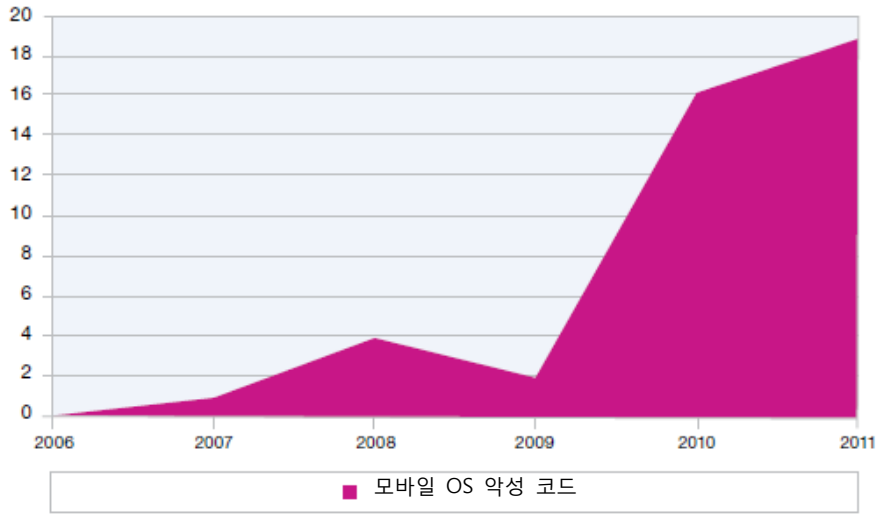


그림 43: 모바일 운영체제를 노린 악성 코드 건수(2006년~2011년)

2011년에 모바일 디바이스를 노리는 악성 코드 유포 건수가 증가했습니다. 일부 악성 애플리케이션은 흔히 사용되는 '탈옥'이란 수법을 악용하여 스마트폰에서 최고의 권한을 획득합니다. 스마트폰 최종 사용자, 통신사, 그리고 모바일 운영체제 제공업체 간의 이중 관계 때문에 이미 노출된 모바일 취약점이 경우에 따라 장기간 동안 패치가 이뤄지지 않아서 공격자에게 오랫동안 무방비 상태로 표적이 되기 쉽습니다.

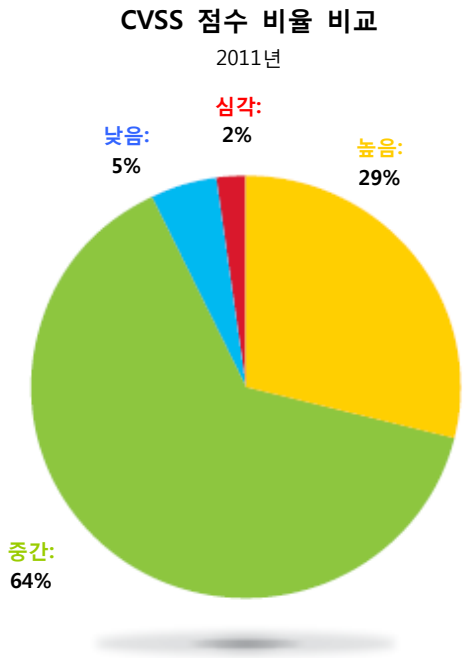


그림 44: CVSS 점수 비율 비교(2011년)

이런 상황은 법적 규정과 다양한 하드웨어 플랫폼이 보급되면서 더욱 심화되고 있습니다. 현재 모바일 디바이스를 노린 실제 공격 횟수는 전통적인 워크스테이션을 대상으로 한 공격 횟수에 비하면 극히 적은 수준이지만 모바일 디바이스에 관심을 갖는 공격자가 향후 꾸준히 늘어날 것으로 예상됩니다. 감염된 모바일 디바이스를 이용한 대규모 봇넷 공격이 본격적으로 등장하고 있는데 이는 시작에 불과합니다.

CVSS 점수	심각도
10	심각
7.0 - 9.9	높음
4.0 - 6.9	중간
0.0 - 3.9	낮음

도표 5: CVSS 점수와 상응하는 심각도 수준

2010년에 노출된 심각한 취약점 건수는 2011년에 비해 70% 증가했습니다. 심각한 취약점이란 CVSS(Common Vulnerability Scoring System)를 기준으로 10점 만점에서 10점을 기록한 보안 취약점을 말합니다. 증가세가 우려할만한 수준이지만 이런 증가세는 일시적인 이상 현상일 뿐, 2012년에 이런 유형의 취약점 건수가 다시 예전 수준으로 떨어질 것으로 X-Force는 예상합니다.

'탈옥'이란 승인되지 않은 제 3의 애플리케이션을 모바일 디바이스에 설치하는 과정을 말합니다. 탈옥에는 흔히 권한 상승 취약점을 악용하여 Unix 방식의 운영체제를 기반으로 하는 스마트폰에 대한 루트 접속 권한을 획득하는 과정이 수반되는데, 그로 인해 간혹 디바이스 '루팅'으로 일컬어지기도 합니다. 루트 접속 권한을 획득하면 승인되지 않은 소프트웨어가 설치되는 것을 막는 보안 기능을 마비시킬 수 있습니다.

기업용 소프트웨어의 취약점

장기적 측면에서 눈에 띄는 추세는 굴지의 소프트웨어 제공업체에 의해 공개된 취약점 비율이 증가했다는 점입니다. 가장 많은 보안 취약점을 공개한 상위 10개의 소프트웨어 제공업체가 곧 가장 다양한 기업용 소프트웨어를 개발한 굴지의 소프트웨어 제공업체이기도 합니다. 실제 상위 10개 목록에는 웹 기반 컨텐츠 관리 시스템 제공업체도 포함되어 있지만 인기 있는 기업용 소프트웨어 제품의 취약점에 대한 영향에 초점을 맞추고자 그런 제품들은 X-Force의 이번 분석에서 제외했습니다.

상위 10개의 기업용 소프트웨어 제공업체들의 취약점 발견 건수가 전체 건수에서 차지하는 비율은 2008년 19%에서 2011년 31%로 상승한 데서 짐작할 수 있듯이 지속적으로 증가하고 있습니다. 그렇다고 소프트웨어 산업 통합만이 능사는 아니라는 게 X-Force의 판단입니다. 안전한 개발 환경이 소프트웨어 개발 수명주기에서 차지하는 비중이 갈수록 커지고 있으며, 지난 몇 년간 책임감 있는 소프트웨어 개발업체는 자사의 코드에 내재된 취약점을 찾아서 해소하는 기술을 개선하는 데 전력을 기울여 왔습니다. 이런 노력의 일환으로 상위 10개의 기업용 소프트웨어 제공업체는 상용화했던 코드를 수정하고 패치를 배포했으며 그로 말미암아 취약점 발견 건수가 급증한 것입니다.

취약점 발견 건수가 가장 많은 상위 10개 소프트웨어 제공업체

2008년–2011년

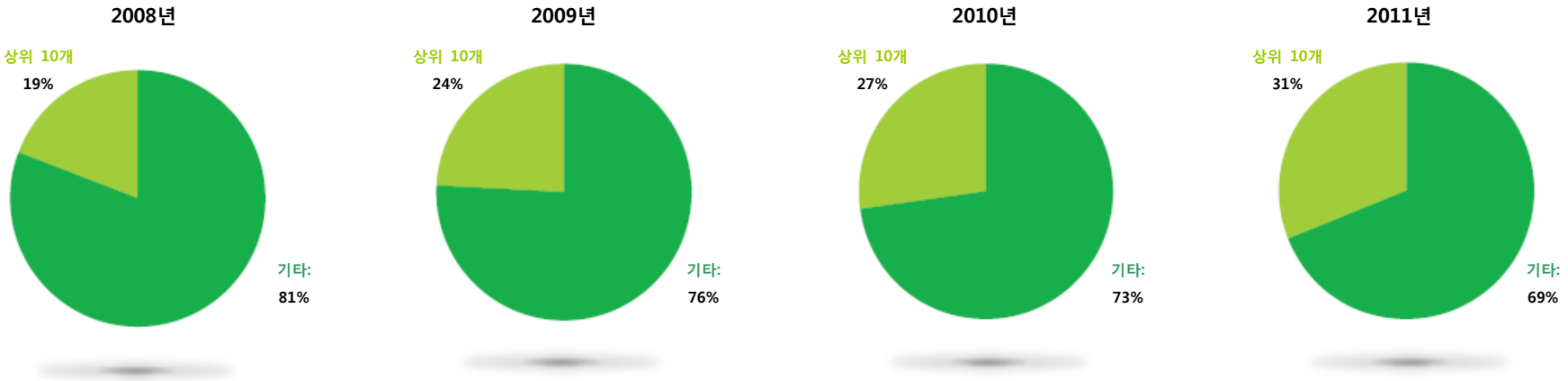


그림 45: 취약점 발견 건수가 가장 많은 상위 10개 소프트웨어 제공업체(2008년~2011년)

기업용 소프트웨어 제공업체의 이와 같은 적극적 대책 마련 덕분에 궁극적으로 2011년의 악성 코드 유포 건수는 감소했습니다. 그러나 단기적으로 인기 있는 기업용 소프트웨어에 영향을 미치는 취약점 건수 증가뿐 아니라 심각한 취약점 건수 증가로 인해 운영 환경의 컴퓨터 네트워크를 패치 및 보호해야 하는 IT 인력이 이런 취약점을 해소하기 위해 처리해야 할 업무량은 지난 몇 년간보다 크게 늘어난 셈입니다. 상위 10개 소프트웨어 제공업체의 실제 취약점 건수는 2008년 이후로 50% 가량 증가했습니다. 취약점을 해소할 인력을 배치할 때 이 통계를 염두에 둘 필요가 있습니다.

IT 인력이 대중에게 공개된 취약점으로부터 네트워크를 보호하기 위해 취할 조치는 패치 배포 여부와 패치가 배포되기까지 걸리는 기간에 따라 달라져야 합니다. 다행히 패치 배포 비율이 늘고 있는 것으로 조사되었습니다. 2011년에 노출된 취약점 중 해결책이나 패치가 배포되지 않은 비율은 36%에 불과했습니다. 이 수치는 45% 내외였던 전년도에 비해 크게 개선된 것입니다.

취약점이 공개된 당일에 패치가 배포되는 게 가장 바람직한데, 패치가 배포된 취약점 중 약 91%가 그런 경우에 해당되었습니다. 나머지 9%는 대부분 몇 주 이내에 패치가 배포됐지만 최악의 경우에는 아주 오랫동안 방치됐는데 심지어 취약점이 공개적으로 노출된 날로부터 수백 일이 지나서야 패치가 배포되기도 했습니다.

인기 있는 기업용 소프트웨어 제공업체나 악성 코드가 유포된 취약점으로 통계를 국한해도 상황은 별반 다르지 않습니다. X-Force가 조사한 바에 따르면 2011년에 굴지의 기업용 소프트웨어 제공업체가 공개적으로 노출되어 악성 코드가 유포된 취약점을 수정하는 데 일주일 이상 걸린 사례는 29건이었지만 다행히 공격자가 그런 취약점을 악용해서 컴퓨터 네트워크에 대대적인 피해를 입힌 경우는 한 건에 그쳤습니다.

	2006년	2007년	2008년	2009년	2010년	2011년
미패치 비율	46.6%	44.6%	51.9%	45.1%	43.3%	36.0%

도표 6: 공개적으로 패치가 배포된 비율(2006년~2011년)

패치 시간	전체	굴지의 제공업체	굴지의 제공업체 + 악성 코드 유포
당일	4054	2263	138
1주(1~7일)	132	19	4
2주(8~14일)	55	15	5
3주(15~21일)	26	3	2
4주(22~28일)	27	10	2
5주(29~35일)	27	8	2
6주(36~42일)	33	7	1
7주(43~49일)	14	6	2
8주(50~56일)	9	2	1

도표 7: 모든 소프트웨어 제공업체와 주요 소프트웨어 제공업체의 패치 배포 시점 비교(2011년 상반기)

이런 공백을 소프트웨어 제공업체의 태만 탓으로 돌리기에는 다소 무리가 있습니다. 시판 중인 소프트웨어 애플리케이션용 업데이트를 적절히 수정해서 일괄 프로그램으로 만든 후 테스트를 하려면 시간이 꽤 걸립니다. 경우에 따라 복잡한 호환성 문제가 이질적인 소프트웨어 구성 요소에 도미노 현상을 유발하기 때문에 한 가지 보안 문제를 해결하는 데 대대적인 수정이 필요하기도 합니다. 그러므로 소프트웨어 제공업체에게 비난의 화살을 돌리는 건 이런 문제를 해결하는 데 그리 큰 도움이 되지 않습니다. 취약점이 노출된 시점과 패치가 배포된 시기 사이에 공백이 존재할 수밖에 없는 불가피한 상황이 있기 마련이므로 네트워크 관리자는 이런 공백기 동안 네트워크를 보호할 전략을 수립할 필요가 있습니다.

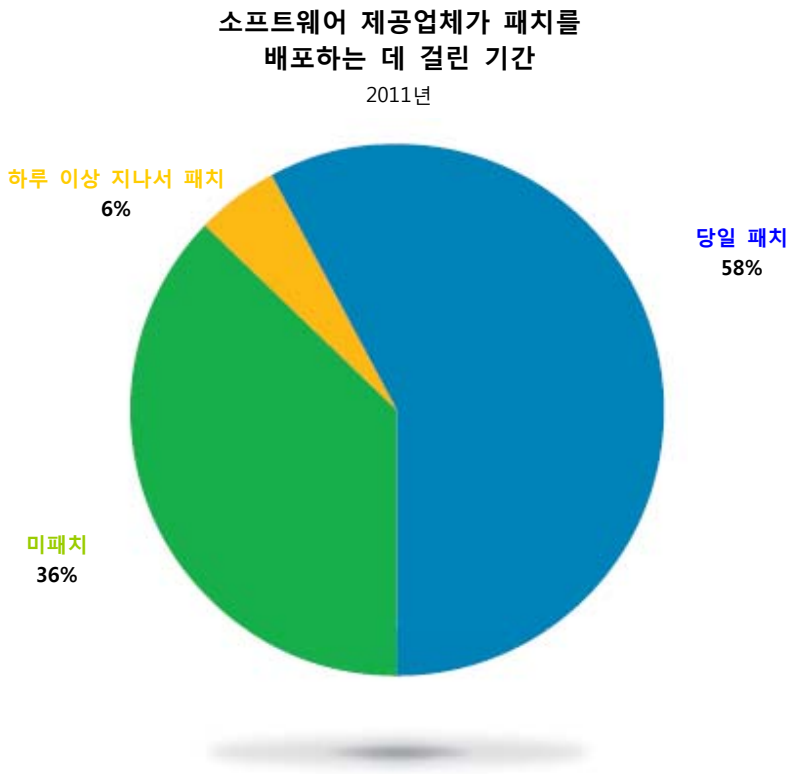


그림 46: 소프트웨어 제공업체가 패치를 배포하는 데 걸린 기간(2011년)

가장 심각한 보안 취약점이 대중에게 공개된 경우 X-Force는 경보 및 주의보를 발령합니다. 기본적으로 X-Force의 동향 및 위험 보고서에는 악용하기 얼마나 어려운가와 해당 취약점이 공격자에게 얼마나 유용한가를 토대로 한 경보 및 주의보가 2차원 그래프에 표시됩니다. 이런 지수는 어떤 취약점이 인터넷에서 널리 악용될 가능성이 높은지 예측하는 데 도움이 됩니다.

X-Force는 2011년에 도합 34회의 경보 및 주의보를 발령했습니다. 이 취약점 중 16건은 악용하기 쉽고 공격자에게 대단히 유용해서 악성 코드의 온상이 되기 더 없이 좋은 심각한 취약점에 해당됩니다. 자동 다운로드(drive-by- download)나 이메일 첨부 파일을 통해 악용할 수 있는 클라이언트 소프트웨어 원격 코드 실행 문제가 이런 취약점 중 거의 전부를 차지하고 있습니다. 이런 취약점 중 대부분이 지금도 널리 악용되고 있는 실정입니다.

이런 취약점 중 12건은 공격자에게 유용하지만 악용하기 어려운 취약점으로 분류됩니다. 악용하기 어려운 이유는 운영체제에 새로운 기능이 도입되어 원격 코드 실행 권한을 획득하기 어려워졌기 때문인데, 덕분에 이런 범주에 속하는 심각한 취약점이 갈수록 늘고 있는 것으로 확인되었습니다.

정교한 공격자가 이런 취약점 중 일부를 악용할 수 있는 여지는 여전히 있지만 인터넷에서 널리 악용될 우려는 없을 것으로 X-Force는 예상합니다. 심각한 취약점 범주와 대조적으로, 이런 범주에 속하는 취약점이 늘고 있는 것은 컴퓨터 범죄와의 전쟁에서 상당한 성과를 거두고 있음을 시사합니다.

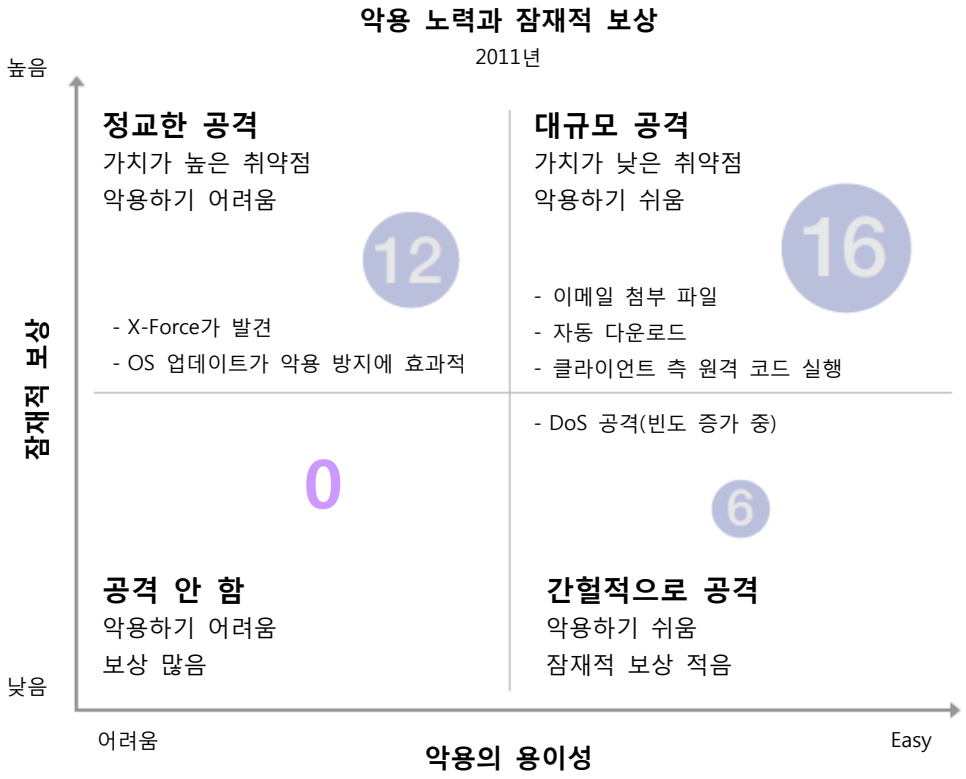


그림 47: 악용 노력과 잠재적 보상(2011년)

X-Force가 2011년에 경보를 발령한 취약점 중 6건은 서비스 거부(DoS - Denial of Service) 문제였습니다. 서비스 거부 취약점은 원격 코드 실행 취약점보다 공격자에게 덜 유용하지만 지난 6개월간 서비스 거부 취약점에 대한 공격자의 관심은 높아진 것으로 확인되었습니다. Anonymous와 같은 정치적 동기를 지닌 핵티비스트 단체는 다양한 정치적 성명을 발표할 목적으로 전 세계 기업과 정부 기관을 상대로 서비스 거부 공격을 감행해 왔습니다. 구체적인 취약점을 유발하는 공격 수법과 대조적으로, 이런 공격에는 대부분 합법을 가장하여 단속하기가 대단히 어려운 대규모 분산 트래픽이 동원됩니다. 그러나 최근 들어 공격자들은 공격 효과를 높일 수 있는 취약점을 유발하는 데 관심을 기울이기 시작했습니다.

또한 핵티비스트들이 개발해 온 도구와 기술이 금전을 노리는 공격자의 수중에 들어가면서 경쟁이 치열한 사업 영역에 서비스 거부 공격이 사용되는 빈도가 꾸준히 늘고 있습니다. 지적재산권법과 관련한 국제적 논란과 더불어 미국 선거가 있기 때문에 2012년에는 분산 서비스 거부(DDoS - Distributed Denial of Service) 공격이 더욱 두드러질 전망입니다.

사회공학적 소셜 미디어: 공격 수법

개요

인터넷이 널리 보급되면서 거의 모든 기술 혁신이 소셜 미디어의 영향을 받게 되었습니다. 소셜 미디어는 사회가 연결되고 소통하며 정보를 공유하는 방식을 변화시키고 있습니다. 이런 변화는 과거에 수집하기 어려웠던 개인정보가 인터넷이라는 중앙 저장고에 모이는 부수적 결과를 초래했습니다. 이 정보의 보고는 악의적 의도로 타인의 컴퓨터에 침입하는 데 특히 유용합니다.

비주류의 취미에 불과했던 소셜 네트워크가 지난 몇 년 새에 검색 엔진의 이용률마저 추월해서 세계 최대 규모의 온라인 활동 공간으로 성장했습니다. 2011년 말을 기준으로 세계 온라인 사용자 인구의 약 80%(10억 명 이상)가 소셜 미디어를 사용하고 있습니다.[20] 온라인 이용자의 활동이 집중되다 보니 당연히 범죄의 온상으로 떠올랐습니다. 몇 년 전 이메일을 통한 사기로 톡톡히 재미를 봤던 범죄자들이 새로운 잠재적 공격 목표와 더불어 소셜 미디어 포럼을 새로운 '삶의 터전'으로 삼게 된 것입니다.

사용자들이 소셜 네트워크에 쏟아내고 있는 엄청난 양의 개인정보가 정보 수집의 패러다임마저 바꿔 놓았습니다. 소셜 네트워크에서 수집한 정보는 이미 공공 부문 및 민간 부문의 컴퓨팅 네트워크에 침투하기 이전에 벌어지는 탐색전에서 상당한 역할을 하고 있습니다.

그로 인한 직접적인 결과로 2011년에 발생했던 가장 대대적인 해킹 공격 중 일부는 단순한 오픈 소스 정보(OSINT) 수집 및/또는 소셜 미디어를 통한 사회공학적 악성 코드 실행으로 시작되었습니다.

20 출처: comscore, It's a Social World Report, 2011년 12월

이런 공격은 조직의 영역에서 애매한 상황을 악용하여 개인 정보와 그 개인이 흔히 개인적인 용도로 제공하는 정보를 노립니다. 표적이 된 조직에 몸담고 있는 개인은 실수로 (또는 의도적으로) 중요한 정보를 제공하거나 자사의 데이터 자산을 절취하거나 파괴하는 악성 코드를 기업 시스템에 심게 됩니다.

소셜 미디어를 활용하여 성공한 악성 코드 공격을 체계적으로 정리하기는 쉽지 않은 일이지만, 공격 성공률과 그에 따른 대가는 공을 들일만한 가치가 있는 것으로 입증되었습니다. 이 단원에서는 소셜 미디어 플랫폼을 활용한 사회공학적 공격의 구조와 정보 수집의 변화에 특히 중점을 두고 소셜 미디어가 보안에 미치는 영향을 살펴보겠습니다. 이번 단원의 목적은 독자들에게 신종 공격 수법과 신종 수법이 공공 부문 및 민간 부문 조직에 미칠 수 있는 영향을 계도하는 것입니다.

정보 수집

정보 수집은 필요사항 파악, 계획 수립 및 지휘, 실제 수집, 처리, 분석, 그리고 배포로 구성된 비교적 간단한 구조에 따라 이뤄진다는 게 보편적인 시각입니다(구조에 존재하는 단계의 실제 개수는 달라질 수 있습니다). 이런 과정 속에서 수집되는 몇 가지 일반적 유형의 정보로는 인간정보(HUMINT), 오픈 소스 정보(OSINT), 신호정보(SIGINT), 측정 및 서명 정보(MASINT), 그리고 영상정보(IMINT)가 있습니다.

소셜 미디어가 등장하기 전에는 이런 유형의 정보를 수집하는 방법이 비교적 간단했으며 이따금 이런 유형의 정보 중 한 가지에 각별한 집중을 요하기도 했습니다. 소셜 미디어의 등장으로 원시 코드 수집 출처가 개별 영역에서 오픈 소스 정보(OSINT) 영역으로 바뀌었습니다.

인간정보(HUMINT)는 더 이상 대인 관계를 위해 물리적 접촉을 하지 않고서도 얻을 수 있게 됐으며 이전에 비해 훨씬 더 개방적으로 바뀌었습니다. 미디어가 공개적으로 널리 공유되고 있기 때문에 신호정보(SIGINT)를 수집하기 위해 신호를 도청할 필요 역시 없어졌으며 영상정보(IMINT)는 세계 최대의 영상 저장소(Fotki, Webshots, Facebook 등) 덕분에 수집하기가 수월해졌습니다.

소셜 미디어는 정보 수집가에게 인간의 역사에서 유례를 찾아볼 수 없을 정도로 많은 정보가 보관된 창고 역할을 하고 있습니다. 그러나 소셜 미디어를 사용하는 사람이 정보의 인위적 구조뿐 아니라 그 구조의 구체적 배경까지 공개한다는 점은 우려할만합니다. 소셜 미디어는 본질적으로 대중에게 목소리를 선사한 대신, 실수로 혹은 고의로 기밀 정보를 발설할 여지를 조성합니다. 미국 고위 공직자들이 기밀로 분류되는 정보를 실수로 게시했다거나 한 국회의원이 언젠가 "백악관의 지시로 이란에 대한 1급 기밀정보 확보"라고 게시했던 실제 사례가 있듯이 그런 증거는 쉽게 찾아볼 수 있습니다. 그러나 노골적인 기밀 누설은 둘째치고, 일반 사용자들 역시 개인 이메일 주소, 현재 거주 도시, 교육 배경과 같은 그다지 중요해 보이지 않은 정보를 소셜 미디어에 공개하기 일쑤입니다.

오픈 소스 정보 수집

막대한 양의 공개 정보나 오픈 소스 정보(OSINT)를 쉽게 수집할 수 있게 되면서 정보 보안과 공격이 새로운 국면을 맞고 있습니다. 2011년에 오픈 소스 정보(OSINT) 검색 빈도가 급증했으며 증가 추세는 2012년에도 계속될 전망입니다.

이와 같은 정보 급증으로 인해 검색 도구와 기술이 완전히 새로운 국면에 접어들었습니다. 오늘날의 검색 도구는 단순히 검색 기능만 갖춘 게 아니라, 가령 찾아낸 데이터를 매핑할 수 있는 기능을 지원하기도 합니다. Maltego처럼 흔히 사용되는 도구는 정보를 찾아서 손쉽게 소비할 수 있는 형식으로 변환하는 기능을 지원합니다. 반면에 Foca와 같은 도구는 정보를 찾은 다음, 그 정보를 활용하여 더 많은 고급 정보를 수집하는 데 사용됩니다.

법 집행기관이 소셜 미디어에 공개된 데이터를 분석할 수 있는 기존의 도구를 활용하는 건 물론이고, 더욱 강력하고 섬세한 최신 도구를 찾고 있다는 사실이 이미 언론을 통해 널리 알려진 바 있습니다. 공격자뿐 아니라 보안 전문가 역시 오픈 소스 정보(OSINT) 수집에 갈수록 많은 관심을 기울이고 있음을 미루어 짐작할 수 있다는 점에서 이런 현상은 흥미롭습니다. 실제로 누가 공격을 감행할지 예측하는 데 많은 정보가 유용하게 사용되고 있습니다.

컴퓨터 침입 측면에서 이와 같은 정보는 개인정보를 요청하는 암호 초기화 같은 인증 로직(authentication logic) 공격과 사회공학적 공격에 활용하기 적합한 '노다지'나 다름없습니다. 공격자들은 소셜 미디어에 존재하는 이런 약점을 가장 적극적으로 악용하여 표적으로 삼은 조직에 침투할 교두보를 마련하고 있습니다.

2011년에 감행된 여러 차례의 대규모 공격이 성공을 거둔 점을 고려하면 소셜 미디어를 통한 사회공학적 공격이 주시해야 할 APT(Advanced Persistent Threat)로 급부상하고 있음을 알 수 있습니다.

지극히 쉬운 공격 수법

예를 들어, 이 특이한 공격 수법은 사회공학적 수법, 스피어 피싱(spear-phishing), 그리고 제로데이 악성 코드로 구성되어 철저하게 준비된 3단계 공격입니다.

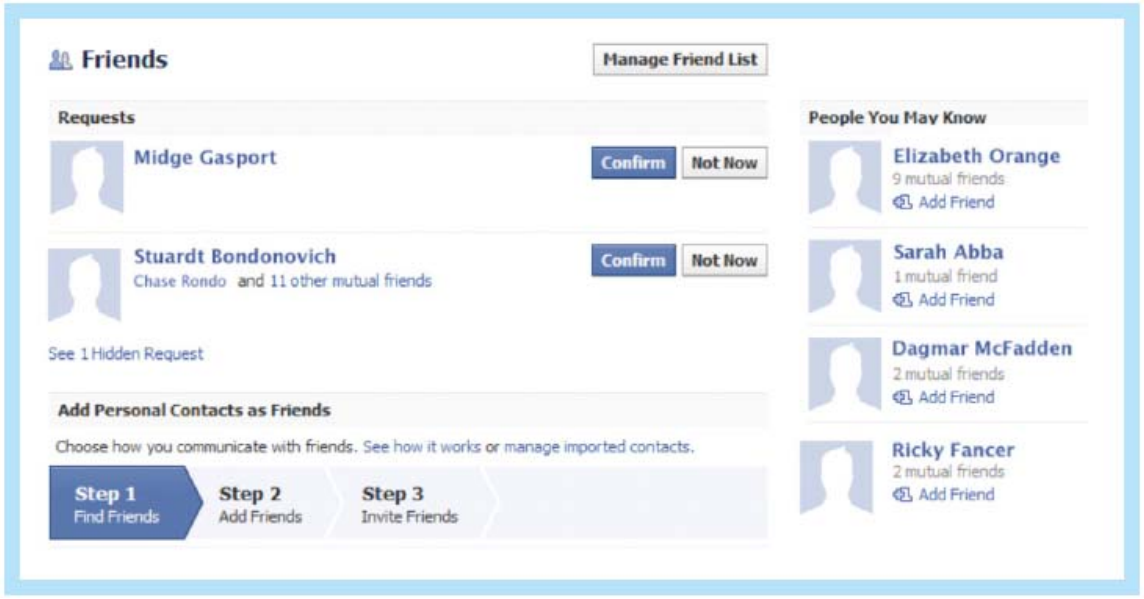


그림 48: 스피어 피싱에 악용할 수 있는 연락처 목록의 예(2011년)

사기 도박꾼이 라스베이거스 카지노를 돌아다니며 미숙한 딜러를 찾고 치타가 세렝게티를 배회하면서 다리 다친 얼룩말을 찾듯이, 공격자들은 소셜 네트워크에 덫을 쳐두고 유용하고 빼곡한 친구 목록을 가진 최종 사용자를 찾습니다.

먼저, 공격자는 공격할 기업을 선택합니다. 그런 다음 LinkedIn과 같은 소셜 미디어 포럼에 계정을 개설하고 그 기업과 직접적인 관계가 있음을 암시하는 별칭(예: former employee)과 프로필을 입력합니다. 경기 침체와 기업 인수 합병이 활발하게 이뤄지는 산업에서 공격 목표의 전 직원 행세를 하면 별칭이 그럴듯해 보이기 마련입니다. 계정을 개설했기 때문에 Facebook이나 LinkedIn과 같은 포럼은 공격자에게 공격할 기업의 직원과 연락이 닿을 수 있는 회원 명단을 제공합니다.

공격자가 접근해야 할 사람을 알아내고 나면 사회공학적 공격을 착수합니다. 공격자는 기업의 현 직원과 접촉하려고 시도합니다. 접근 수법은 간단하면서도 다양합니다. 가령, 몇 년 만에 다시 연락하고 싶은 사람을 찾는 중이라던가, 직장을 옮겼는데 인맥을 넓히고 싶다던가, 최근 실직했는데 다시 그 회사에 들어갈 생각이라던가, 혹은 업계 행사에서 만났는데 다시 연락하고 싶다는 수법을 예로 들 수 있습니다. 아주 정중한 어투를 구사하고 때때로 저자세로 나오는 수법은 여러 사람에게 접근하다 보면 성공하기 마련입니다. 처음 연락처를 얻기가 가장 어렵습니다. 때때로 공격자는 공격할 기업의 소속을 가장한 또 다른 가명 계정을 개설하고 두 계정을 연결해서 신뢰성을 높입니다. 소셜 미디어에서 이뤄지는 거짓 주장이나 허위 진술이 탄로날 제도적 장치는 전혀 마련되어 있지 않습니다. 그래서 포럼 대다수 사용자 계정은 액면 그대로 받아들여지고 합법적으로 취급됩니다.

일단 공격자가 공격할 기업에 소속된 직원의 연락처를 알아내면 다른 직원들의 연락처를 알아내기가 훨씬 쉬워집니다. 예를 들어, LinkedIn은 한 회원에 의해 제 2의 회원 혹은 제 3의 회원을 소개 받기 쉬운 여건이 마련되어 있으며 Facebook 역시 친구의 친구를 통해 친분을 쌓을 수 있습니다. 이외에도 주요 포럼의 계정들을 서로 연결한 덕분에 한두 명의 무고한 개인 접촉자와 맺은 친분을 이용하여 다양한 곳에서 연락처를 추가로 얻기가 더욱 수월합니다.

그리고 나서 공격자는 각 개인에게 접근하기 가장 효과적인 방법을 알아내기 위해 개인정보나 기업 관련 정보를 수집하거나 심지어 관심 분야를 파악하여 무고한 접촉자의 신상을 분석하기 시작합니다. 간단한 정보를 묻거나 관심을 가질만한 정보를 전송하는 방법으로 새로운 접촉자와 기초적인 수준의 신뢰를 쌓기란 그리 어렵지 않습니다.

이런 수법으로 공격자는 어떤 최종 사용자가 가장 적극적이고 목표로 삼은 기업에 침투하는 데 '협조'할 가능성이 가장 높은지 파악할 수 있습니다.

드디어 공격자는 만반의 준비를 마친 채 스피어 피싱 공격 단계에 돌입할 수 있습니다. 이 공격 수법은 공격자가 최종 사용자의 기업 이메일 계정에 대한 접속 권한을 확보했을 때 성공 확률이 가장 높습니다. 한두 개의 기업 이메일에 접속할 수만 있어도 명명 규칙(naming convention)을 파악하고 다른 이메일 계정을 짐작으로 알아낼 수 있습니다. 불만을 품은 직원을 대상으로 한 구인 정보, 구직자를 대상으로 한 전문직 선호도 조사, 이직을 고려 중인 직원을 대상으로 한 교육 동영상 링크 등 합법적으로 보이고 현재 업무와 어느 정도 연관이 있는 내용을 주제로 이메일을 공들여 작성할 경우 표적으로 삼은 기업의 컴퓨팅 환경과 연결된 최종 사용자의 관심을 끌고 수락 버튼을 누르도록 유도할 수 있습니다.

이런 이메일에는 일반적으로 악성 페이로드, 링크, 다운로드 혹은 실행 파일이 포함되어 있어서, 다름 아닌 최종 사용자가 최종 공격을 감행하는 셈입니다.

그림 49: 스피어 피싱 이메일의 예(2012년)[21]

그렇게 해서 공격자는 '내부'에 침투하여 제로데이 공격을 실행할 수 있습니다. 한 가지 편리한 점은 실패한 공격과 성공한 공격의 차이점이기도 한데, 그것은 바로 공격자가 직접 침투할 필요 없이 최종 사용자의 결정에 의해 악성 코드가 실행된다는 것입니다.

기업이 소셜 미디어의 보안 위협을 줄이기 위해 취할 수 있는 조치

2011년 9월에 Ponemon Institute가 실시한 설문조사[22]에서 소셜 미디어 정책이 명문화되어 있다고 답한 응답자는 35%에 불과했습니다. 게다가 그 중 35%만이 명문화된 소셜 미디어 정책을 적극적으로 시행하고 있는 것으로 조사되었습니다. 같은 설문조사에 따르면 직원들이 소셜 미디어를 이용하기 시작한 이후로 기업의 컴퓨팅 시스템을 노린 바이러스와 악성 코드 공격이 50% 이상 증가했습니다. 유감스럽게도, 손쉽게 배치할 수 있는 사회공학적 공격 방지용 소프트웨어나 완성형 제품 세트는 전무합니다. 대부분의 위협은 인간을 표적으로 삼기 때문에 그러한 위험을 완화하는 최선의 방법은 정책을 마련하고 교육을 실시하는 것입니다.

21 출처: http://contagiodump.blogspot.com/2011년/10/cve-2011년-0611-pdf-2011년-10-24-northkorea.html.

22 출처: http://www.ponemon.org/, 2011년 9월 전 세계 소셜 미디어 위험에 관한 설문조사(Global Survey on Social Media Risks September 2011) - 설문조사에는 미국, 캐나다, 영국, 프랑스, 독일, 이탈리아, 호주, 싱가포르, 홍콩, 인도, 브라질 및 멕시코의 IT 및 IT 보안 분야에 평균 10년의 경험을 지닌 전문가 4,640명이 참여했습니다.

위험 대응 방안을 마련해야 할 분야는 크게 두 가지(비즈니스 환경에 필요한 조치와 사용자에게 필요한 조치)로 나눌 수 있습니다. 소셜 미디어는 대부분 개인적인 용도로 직장 밖에서 주로 이용하므로 사용자는 본인의 프라이버시와 보안을 책임져야 합니다. 그와 별도로 기업은 직원들을 계도함과 동시에 자사의 브랜드와 자산을 보호하는 데 도움이 될만한 정책과 절차를 수립해야 합니다. 이런 자구책은 과거의 '보안 인식 강화' 프로그램과 일맥상통하지만 다음과 같은 최종 사용자의 책임에 대한 지침이 특별히 포함돼야 합니다.

보안 및 프라이버시 설정 지원: 주요 소셜 미디어 포럼은 사용자가 이용할 수 있는 기본적인 프라이버시 설정을 지원합니다. 최종 사용자는 적극적으로 활동할 계획이 없는 경우라도 본인이 정기적으로 이용하는 소셜 미디어 포럼에서 어떤 보안 및 프라이버시 통제 옵션을 설정할 수 있는지 확인해야 합니다. 스팸, 사기 이메일, 기회주의적인 공격자에 노출될 가능성을 줄일 수 있도록 보안 및 프라이버시 통제 옵션을 최고 수준으로 설정해야 합니다.

또한 최종 사용자는 본인이 적절한 보안 및 프라이버시 조치를 취하더라도 소셜 네트워크 내부에서는 그 조치가 가장 낮은 수준으로 작용할 수 있다는 사실을 반드시 명심해야 합니다. 가령, 한 친구가 최소 수준의 보안 및 프라이버시 통제 옵션을 설정한 경우 그 친구와 교류하는 사람들이 설령 더 높은 보안 통제 옵션을 설정했더라도 그들마저 노출될 우려가 커집니다. 다시 말해서, Facebook의 친구 1이 본인의 게시물과 연락처 공개를 본인의 친구들만으로 제한했지만 친구 2가 모두에게 게시물과 연락처를 공개한 경우, Facebook에 가입한 사람이라면 누구나 친구 2의 담벼락에 게시된 내용을 볼 수 있습니다. 심지어 친구 2의 프라이버시 설정에 따라 인터넷에서 게시물을 검색할 수도 있습니다.

최종 사용자에게 소셜 미디어의 접속 상태 표시 여부를 '거부'로 기본 설정하라고 권장하는 것이 소셜 미디어에 참여하는 본질적인 취지와 다소 모순되는 것처럼 보이지만 궁극적으로 사회공학적 공격으로부터 자신을 보호할 수 있는 것은 다름아닌 '보안 인식 수준'입니다.

본인의 친구만 진짜 친구: 사회공학적 공격 수법은 여러 가지 면에서 기발하지 않은 경우 성공 확률이 그다지 높지 않습니다. 실 세계의 사기꾼과 마찬가지로 소셜 미디어 공격자는 공격 목표로부터 특정 수준의 신뢰를 얻으려는 시도와 함께 공격을 착수합니다. 오래된 동창, 과거의 직장 동료 혹은 친구의 친구나 친척을 가장하는 수법은 전혀 새롭지 않습니다. 예를 들어, LinkedIn의 소셜 미디어 이미지가 비즈니스 지향적인 차분한 분위기의 포럼이라는 사실을 감안했을 때 LinkedIn을 통해 가벼운 업무 관계로 위장하면 공격자가 거의 즉각적으로 신뢰를 얻게 됩니다. 게다가 과거에 업무 관계로 아는 사람이라거나 비즈니스 컨퍼런스 혹은 행사에서 공격 대상을 만난 적이 있다는 거짓 주장을 하면서 LinkedIn을 통해 접근한 경우 공격 대상이 속아 넘어가서 친구 요청을 수락할 가능성이 충분합니다. 또한 온라인 입지나 영향력 범위를 넓히기를 원하는 최종 사용자는 단지 친구 숫자를 늘릴 욕심에 무작위 친구 요청을 습관적으로 수락하는 경향이 있습니다.

빼곡하고 다양한 팔로워 및 친구 목록을 갖추면 다양한 이득과 보상이 따르지만 그 점이 바로 공격자가 숨어들기 쉬운 맹점이라는 사실을 잊지 말아야 합니다. 최종 사용자는 친구 요청을 신중히 생각하고 실 세계에서 실제로 친분을 맺은 적이 있거나 소셜 미디어 포럼(예: 자선 모금 동호회나 공통 관심사 분야)에서 한동안 신뢰를 쌓은 사람에 한하여 수락해야 합니다. 제 2 혹은 제 3의 교감(mutual connection)을 근거로 한 무작위 친구 요청은 특히 신중을 기해서 확인해야 합니다. 소셜 미디어를 통해서 알게 된 새 친구가 개인적인 대화를 유도하거나 세부적인 개인정보를 묻는 경우, 특히 실 세계의 연락처 정보를 묻을 경우 경계를 늦추지 말아야 합니다.

신중을 기하여 링크 및 다운로드 클릭: 이메일이 보편화된 1990년대 말부터 링크와 다운로드는 공격자가 공격 대상에게 악성 코드를 심을 때 선호하는 매개체로 활용되어 왔습니다. 이러한 추세는 소셜 미디어 포럼까지 이어지고 있습니다. 최종 사용자는 알 수 없거나 신뢰할 수 없는 사람으로부터 이메일을 받은 경우 링크를 클릭하거나 무언가(특히 실행 파일)를 다운로드하기 전에 극도로 조심하고 그 출처를 주의 깊게 확인해야 합니다. '새 친구'가 재미있는 YouTube 동영상, 기발한 스크린세이버, 가짜 팬 포럼 혹은 멋진 무료 게임 프로그램을 소개한다는 개인적인 메시지를 통해 악성 페이로드를 전파하려고 시도할지도 모릅니다. 공격자는 스팸을 통해 무작위로 악성 페이로드를 전파하려고 시도하기도 합니다. Facebook과 기타 포럼은 대규모 공격을 인지했을 때 관례대로 경고문을 게시하는데, 최종 사용자는 해당 포럼이 제공하는 경보 서비스를 신청하는 것이 바람직합니다.

경품, 선물, 당첨, 특별 제안 주의보: "이미 당첨되신 거나 다름없습니다!" 경품이나 기타 특별 제안 사기 이메일은 이메일 초창기부터 흔히 쓰인 수법이지만 소셜 미디어 포럼에서 큰 효과를 거두고 있습니다. 사기 이메일 발송자는 일반적으로 "포럼 회원에게 고가의 기프트 카드를 무료로 드립니다"와 같은 구미 당기는 제안으로 최종 사용자를 쿠키나 심지어 스파이웨어를 유포하는 끔찍한 웹사이트, 합법적 기업 혹은 브랜드를 모방한 가짜 웹사이트로 유도한 후 가짜 경품에 응모하려면 복잡한 신청서나 설문조사 자료를 작성해야 한다고 유혹합니다. 둘 중 어떤 방법을 사용하든, 사기 이메일 발송자는 공격 목표로부터 개인정보를 수집할 수 있습니다. Facebook은 회원에게 사기 이메일을 경고하는 Facecrooks란 사용자 커뮤니티를 운영하면서 필요할 때 상세정보와 해결 대책을 제공하는데 해당 소셜 미디어 포럼이 제공하는 경보 서비스를 신청하는 것이 좋습니다.

업무 관련 정보 제한: 최종 사용자는 본인과 관련 있는 회사, 동료, 고객, 제품, 서비스 및 프로젝트에 대한 정보를 발설할 때 반드시 자사의 적절한 소셜 미디어 이용 정책을 숙지해서 준수해야 합니다. 구체적인 정보가 아니더라도, 최종 사용자는 무심코 중요한 정보를 노출하지 않도록 회사나 고용주를 언급할 때 일반적인 용어만 사용하는 것도 바람직합니다. 소셜 미디어를 통해 직장이나 인맥을 찾는 최종 사용자가 늘어나고 현직 직원이나 채용을 고려 중인 직원을 평가하기 위해 소셜 미디어를 검사하는 고용주가 늘어남에 따라 업무 관련 정보를 철저히 보호하는 일이 더더욱 중요해지고 있습니다.[23]

기업 정책이 명문화돼 있지 않은 경우 업무 관련 정보를 발설할 때 상식이 최선의 지침이 될 수 있습니다.

이따금 무심코 한 얘기가 원래 최종 사용자가 의도했던 것보다 많은 정보를 노출할 수 있습니다. 중요한 건 보안 및 프라이버시 설정이나 선의였는지 사고였는지가 아닙니다. 소셜 미디어 포럼에 정보를 게시할 때는 소셜 네트워크는 인터넷을 통해 전 세계가 정보를 공유하도록 설계됐다는 가장 상식적인 사실을 잊지 말아야 합니다. 어떤 정보를 게시하든 일단 공개하면 돌이킬 수 없으므로 먼저 신중하게 생각할 필요가 있습니다.

미래의 동향

소셜 미디어 공격의 영향과 범위는 계속 커질 전망입니다. 소셜 미디어 공격의 범위는 전혀 무관해 보이는 기술까지 확대될 것입니다. 예를 들어, 자동차에도 이미 인터넷이 활용되고 있을 뿐더러 자동차가 소셜 미디어를 통해 서로 연결되고 있습니다. 이런 확대 추세로 말미암아 소셜 미디어는 공격자가 손쉽게 악용할 수 있는 영역으로 자리잡게 될 것으로 예상됩니다.

기업은 정책을 개발 및 강화해야 하고 사용자는 스스로를 보호할 능력과 지식을 갖춰야 합니다.

23 이런 추세에 대한 2011년의 부정적인 반응에도 불구하고, 다수의 고용주는 배경 및 신용 확인 등의 채용 절차에 공개적으로 소셜 미디어를 활용하고 있습니다.

CSIRP에서 가장 보편적인 열 가지 실수

네트워크, 컴퓨터 또는 전자 데이터가 관련된 보안 사고에 대한 대응책을 수립할 때는 컴퓨터 보안 사고 대응 계획(Computer Security Incident Response Plan: CSIRP)이 절대적으로 중요합니다. CSIRP는 값비싼 계산기보다 더 발전된 무언가가 배치된 환경의 초석이 되기 때문입니다. 사고가 발생한 경우 CSIRP는 취해야 할 조치를 안내하는 지도 역할을 합니다.

여기서는 CSIRP에 가장 흔히 수반되는 여러 가지 실수를 소개합니다. IBM의 긴급 대응 서비스 (ERS - Emergency Response Service) 팀은 빈번히 고객의 긴급 상황에 대응하고 고객을 위해 맞춤형 CSIRP 계획을 개발하기 때문에 CSIRP 계획에 정통합니다. 공교롭게도, ERS 팀은 어떤 것이 효과적이고 어떤 것이 부적합한지 관찰을 해 왔습니다. 이번 절에서는 가장 흔히 관측되는 CSIRP 계획의 결점 10가지를 설명하겠습니다.

1. 너무 복잡하게 만든 CSIRP

자료 이용자가 문서를 읽는 건 위기가 닥쳤을 때라는 사실을 반드시 CSIRP를 구상할 때 염두에 둬야 합니다. 커피숍에서 커피에 곁들여 갓 구운 빵을 한 손에 든 채 편안히 클래식 음악을 들으면서 천천히 자료에 몰입할 상황이 아니라는 뜻입니다.

계획을 섭렵하고도 남을만한 넉넉한 시간과 뜨거운 빵이 곁들여진 사고는 꿈에서나 있을 법한 일일 뿐 실제로 일어날 리 없습니다. 중압감이 클지도 모릅니다. 일반 직원은 어떻게 해야 할지 모른 채 걱정만 하고 경영자는 (기술적 측면에서 어떤 일이 벌어지고 있는지 이해하든, 못하든) 지역 언론이 질문 세례를 퍼붓고 있기 때문에 잔뜩 흥분하게 될지도 모릅니다. 그러다간 얼마 못 가 양손으로 얼굴을 감싼 채 눈물을 흘릴지도 모르겠습니다. 나머지는 여러분도 짐작하리라 믿습니다.

여러분이 위에 묘사한 상황에 처한다면 세부적이고 광범위한 CSIRP 계획을 제대로 읽을 시간이 있을까요? 분명히 그렇지 못할 겁니다. CSIRP는 명쾌하고 명확하면서도 간결해야 합니다. 문서에 익숙하지 않은 직원이 CSIRP에 설명된 절차를 재빨리 살펴보지 못하거나, 복잡한 명령어를 이해하지 못하거나 혹은 필요한 조치를 취하지 못한다면 그 CSIRP가 너무 복잡하기 때문일지도 모릅니다. 물론, CSIRP를 너무 단순하게 만드는 것도 상황을 악화시킬 소지가 있습니다. 따라서 간결성과 유용한 지침 간의 적절한 균형을 맞추는 것이 성공적인 CSIRP의 핵심 과제입니다.

2. 핵심 인력의 과부하

모든 조직에는 '만물박사'로 통하는 걸출한 인재가 있기 마련입니다. 만물박사는 모든 사람과 모든 시스템, 라우터, 케이블, 그리고 심지어 회사에서 제일 좋은 커피 자판기도 알고 있습니다. 만물박사는 사고가 났을 때 사람들이 제일 먼저 찾는 사람입니다. 당연히 만물박사는 사소한 사고가 났을 때 최고의 실력을 발휘해서 처음부터 끝까지 혼자 해결할 수 있습니다. 고객을 위해 CSIRP를 개발하는 동안 다음과 같은 일반적인 질문을 하다 보면 어김없이 그 조직의 만물박사를 찾게 됩니다. '바이러스 예방은 누가 담당하지? 만물박사요. 경영진에게는 누가 보고하지? 만물박사요. 회사 단합 파티 일정은 누가 짜지? 만물박사요.'

만물박사는 근무 시간 내내 눈부신 활약을 펼칩니다. 하지만 사고가 며칠간 지속될 경우에도 만물박사가 72시간 내내 전담할 수는 없는 노릇입니다. 한여름에 잠을 쫓기 급급한 채 과중한 업무를 맡은 직원들이 대응 전략을 세우는 상황을 보고 싶지 않다면 사고가 발생했을 때 업무를 분담하고 미리 정해둔 지원 인력을 배치해야 합니다.

3. 순차적인 사고 처리 절차로 해결
대형 사고가 발생한 경우 동시 처리가 필수적입니다. 순차 처리 절차에만 의존하는 사고 관리자는 적시에 사고를 해결할 수 없습니다. 사고마다 각기 다른 특징을 보이지만 모든 사고는 다수의 단기적 목표로 구성됩니다. 새로운 안티바이러스 시그니처 개발, 시스템 패치, 조사 지휘, 직원과 고객에게 현재 상황 고지, 카페인이 함유된 음료수 보급, 그리고 기타 중요한 업무는 모두 고유한 절차이므로 그렇게 취급돼야 합니다. 흔히 저지르는 한 가지 실수는 기업이 한 번에 한 가지 업무에만 집중하고 동시에 진행해도 될 다른 중요한 업무를 소홀히 한다는 것입니다.

4. 적절한 연락망 구축 실패
사고에 대응할 때 여러 직원과 협력업체의 지원이 필요할 수 있습니다. 사고 관리자, 즉 '실전 병력' 지휘를 책임지는 사람은 최상위 소식통 역할을 해야 합니다. 연락은 질서 있고 효율적이어야 하며 적절한 채널을 따라야 합니다. 적절한 연락망은 아예 존재하지 않는데다 각각 15명의 다른 사람으로부터 명령을 받은 25명이 작전실에 함께 모여 있는 광경을 상상해보십시오. 진전은 더디기만 하고 24시간 전에 해결했어야 할 사고는 여전히 오리무중입니다. 사고가 닥쳤을 때는 의사소통 능력이 기술적 능력 못지않게 중요할 수 있습니다. 한 목소리, 하나의 비전, 그리고 한 명의 코치가 없다면 팀의 나머지 일원은 실패를 면하기 어렵습니다. CSIRP는 분산된 지휘 체계 때문에 난관에 봉착하지 않고 모든 정보가 필요로 하는 사람의 손에 들어갈 수 있도록 연락망을 수립하고 명문화해야 합니다.

5. 해야 할 일이 아니라 하기 쉬운 일에 집중
사고가 발생하면 해야 할 일이 아니라 쉬운 업무에 집중하고 싶은 충동이 듭니다. 하지만 이런 형국은 자동차 엔진이 고장 났는데 유리 세척용 비눗물을 채우는 것이나 진배없습니다. 물론 유리 세척용 비눗물도 언젠가는 채워야 하지만 엔진을 고치지 않는다면 그 차는 아무짝에도 쓸모 없습니다. 사고도 마찬가지입니다. 어려운 일도 있고 쉬운 일도 있지만 난이도에 관계없이 일부 업무는 시급하게 완료해야 합니다. 그 문제가 쉬운 일이든 혹은 어려운 일이든, 가장 중요한 문제에 힘을 쏟지 못하면 골칫거리는 사라지지 않고 사고는 장기화될 수 밖에 없습니다.

6. 해야 할 일이 아니라 호기심을 자극하는 일에 집중
사고가 발생했는데 대응 인력이 제법 흥미로운 정보를 발견하고 불필요하게 토끼굴을 쫓아 들어가느라 정신이 없는 경우가 있습니다. 새로 발견한 정보가 호기심을 크게 자극할 수 있지만 사고를 해결하는 데는 별 도움이 되지 않습니다. 토끼굴에서 원 없이 시간을 보낼 수도 있지만 토끼는 이미 다른 나라로 여행을 떠난 뒤입니다. 목적은 토끼굴이라는 신기한 구조물을 구경하는 게 아니라 토끼를 사냥하는 것이란 걸 명심하십시오.

7. CSIRP 무시
CSIRP가 당장 상황을 해결해 주지 못해서 CSIRP를 무시하고 싶은 충동이 생길 수 있습니다. CSIRP가 최신 이메일 바이러스를 해결하지 못하는 이유가 있습니다. CSIRP는 모든 상황에 대응하는 방법을 다룬 만능 지침서가 될 수 없기 때문입니다. CSIRP는 연락망, 역할, 필요한 통지, 사고에 대응하기 위해 취해야 할 조치에 대한 청사진입니다. 모든 사고는 각기 다른 특징이 있지만 배치해야 할 핵심 인력, 그들의 역할, 그리고 통신 프로토콜을 신속하게 파악함으로써 체계적인 대응 방안을 수립할 수 있게 하는 게 CSIRP 본연의 목표입니다. 이런 구조가 완성되면 필요한 조치를 취해서 가급적 빠른 시간 내에 사고를 해결할 수 있습니다.

8. 계획(Plan) 수립이 아닌, 방침(Policy) 수립
CSIRP에서 'P'는 'Plan'의 약어이지 'Policy'의 약어가 아니란 사실을 항상 기억하십시오. IBM ERS(Emergency Response Service) 팀은 이따금 CSIRP를 계획이 아니라 방침으로 받아들여지는 상황을 접하곤 합니다. 차이는 분명이 존재합니다. 계획에는 실행 가능한 조치와 역할이 포함되는 반면, 방침에는 조직 내부에 적용할 중대한 가이드라인이 명시됩니다. 사고가 발생한 경우 회사 방침을 읽고 계획을 수립하는 구조를 원하십니까? 물론 그렇지 않을 겁니다. 누구든 어떻게 대응해야 할지 알려주는 세심한 계획을 원할 것입니다.

9. 책임자 지정 소홀
CSIRP는 집에서 키우는 고양이와 많은 공통점을 갖고 있습니다. 둘 다 시간이 흐를수록 성장하고 관리와 관심을 필요로 하며 책임자가 미래를 책임져야 합니다. 사고가 발생했을 때 네트워크 어딘가에 깊숙이 처박혀 있던 CSIRP를 겨우 찾아냈지만 Windows Vista가 보편화되던 시기에 마지막으로 업데이트된 문서만 있다고 상상해 보십시오. 그곳에 적힌 핵심 인력의 전화번호로 차례차례 연락을 해보지만 허사입니다. 원래 작전실로 설계됐던 회의실은 사내 탁아소로 용도가 변경된 지 오래입니다. CSIRP 자료에 책임자가 아예 배정되어 있지 않았습니다. 관리하는 사람이 없다 보니 자료가 오래되어 무용지물이 된 것입니다.

CSIRP를 수립할 때는 이 자료의 책임자(관리자)를 배정해야 합니다. CSIRP 책임자는 자료를 업데이트하고, 그 자료에 명시된 절차가 여전히 적절한지 꾸준히 검토하며, 해마다 테스트 일정을 편성할 책임이 있습니다. 책임자가 정해지지 않으면 자료에 시대의 상황이 반영되지 못해 퇴보하고 사고 대응 시간이 길어지는 부작용을 초래할 수 있습니다.

10. 사후 검토 미흡
가장 소중한 교훈은 사고 수습이 끝나고 사후 검토를 통해 얻을 수 있습니다. 사고 수습 기간에 모든 것이 계획대로 진행된 것처럼 보였더라도 사후 검토를 실시하면 개선해야 할 부분을 찾아낼 수 있습니다. 개선돼야 할 실수나 문제를 지적하는 일을 부끄러워할 필요는 전혀 없습니다. 그런 과정을 거쳐야만 CSIRP의 효과와 효율성을 개선해서 미래의 사고에 대비하는 데 필요한 사항을 충족할 수 있습니다.

사고 마무리 단계에 핵심 인력들은 함께 모여 CSIRP가 얼마나 효과적이었는지 논의해야 합니다. 유감스럽게도 지난 몇 주간의 고생을 하루빨리 잊고 싶어서 CSIRP 절차에서 아주 중요한 과정인 사후 검토를 소홀히 하는 경우가 빈번합니다.

사고 대응 – 대규모 공격에 대비한 인프라 구축

대다수 보안 인력은 사고 대응을 일상 업무로 여기지 않습니다. 일반적으로 보안 인력은 방어적 자세와 공격적 자세, 신원 관리, 코드 검사, 그리고 기타 일상적인 업무에 치중합니다. 그러나 이런 메커니즘이 실제 사고가 닥쳤을 때 효과가 없다면 어떻게 될까요? 침입, 바이러스 감염 또는 민감한 데이터 유출 사고가 발생한다면 어떻게 수습해야 할까요? 치밀한 계획 속에 사고 대응 절차를 수립하고 필요한 사항을 미리 준비해둬야, 파장을 제대로 고려하지 않은 채 섣부른 결정을 내리는 상황을 피할 수 있습니다. 가장 단순히 말해서 사고 대응 계획에는 조직 내에서 심각한 보안 문제를 찾아내서 뿌리뽑는 데 가장 능한 문제 해결 전문가를 발굴하는 일이 흔히 수반됩니다. 이런 인재들은 굳이 사고 대응 전담 인력일 필요는 없지만 적어도 사고가 닥쳤을 때 즉시 투입할 수 있어야 합니다. 하지만 이와 유사한 상황에서는 사고 대응이 체계적이지 못한 게 보편적입니다.

보안 전문가들은 대대적인 모니터링과 대규모 정리 작업을 실시하기 보다는 임시방편에 의존해서 국부적 검사로 감염 파일을 개별적으로 치료하고 스니커넷(sneaker-net)과 부팅 CD로 문제를 해결하는 경향이 있습니다.

훌륭한 사고 대응에 정말 필요한 것은 모든 것을 보존하고 그것을 일관성 있고 철저하게 이해할 수 있는 능력입니다.

소기업이라면 이 정도만으로도 충분할 수 있습니다. 이런 접근방식이 그다지 잘못된 건 아니지만 얼마 못 가 소수의 시스템마저 감당하지 못하게 됩니다. 이 수준을 넘어서려면 일반적으로 인프라에 대한 실질적인 투자가 필요하고 전사적으로 데이터를 수집해서 분석할 수 있는 도구를 갖추고 사고 대응 팀을 구성해야 합니다. 현재 각종 로깅 및 분석 플랫폼과 장비가 시판 중인데도, 사고 대응은 단순히 장비를 갈아치우는 일과 다를 바 없을 거라고 생각하기 쉽습니다.

그러나 사고 대응은 그렇게 쉬운 일이 아니며 모든 것을 보존하고 그것을 일관성 있고 철저하게 이해할 수 있는 능력을 필요로 합니다. 유감스럽게도 피해를 입은 시스템이 소수가 아니라면 이런 접근방식으로도 감당할 수 없습니다. 사고에 연루된 시스템이 십여 대 이상인 경우 지나치게 단순화된 사고 대응 규범은 과도하게 많은 인력을 투입하도록 지시합니다. "완력이 먹히지 않은 건 아직도 힘이 부족하다는 증거"라는 뻔한 얘기를 적용하더라도 그에 따라 동원해야 할 대다수 프로세스에는 지나치게 많은 비용을 발생할 뿐더러 통제하기도 어렵습니다. 가령, 사고 대응 계획에 시스템 한 대가 정보 탈취 바이러스에 감염된 경우 그 시스템을 폐쇄하고 이미지 데이터를 생성해야 한다고 명시되어 있다고 예를 들어보겠습니다. 과연 50대의 시스템에도 그 방법이 얼마나 효과가 있을까요? 하물며 감염된 시스템이 1,500대라면 어떻게 될까요? 안티바이러스 솔루션이 바이러스를 감지한 지 수시간 혹은 수일이 지났다면 어떤 시스템이 감염됐는지 어떻게 파악할까요? 이번 단원에서는 재정적으로나 시간적으로 감당할 수 있는 방법으로 이와 유사한 상황에 대비하는 데 가장 도움이 될만한 몇 가지 기본적인 조치를 소개합니다.

준비: 모든 사고 대응의 탄탄한 기초

구체적인 약어는 사용하는 어휘에 따라 각기 달라지지만 전통적인 사고 대응 원칙의 개요는 'Preparation(준비)'의 약어인 'P'로 시작됩니다. 어느 정도 규모가 있는 사고 대응에는 소규모 환경보다 훨씬 더 많은 준비가 필요하지만 적절히 대비하면 차후에 들여야 할 노력을 크게 줄일 수 있습니다. 다행히, 적절한 사고 대응을 준비하는 데 수반되는 조치 중 (전부는 아니더라도) 다수는 우수한 인프라 구조를 필요로 하는데 IT 환경을 적절히 관리하고 있다면 이 문제는 이미 해결된 셈입니다. 실제로, 시스템 관리 자체를 '하위 등급' 사고 대응의 일환으로 볼 수 있습니다. 중앙 집중식 인증, 패치 관리, 자산 관리, 로깅, 접근 통제, 자동화는 컴퓨팅 인프라를 성공적으로 운영하는 데 필요한 기본적인 요소이며 이 각각의 요소들이 사고 대응의 일부로 봐도 무방합니다. 이 모든 요소를 다루는 건 이 자료의 범위를 벗어나지만 두 가지 요소인 로깅과 자동화는 어느 정도 규모가 있는 사고 대응에 무엇보다 중요합니다. 이 두 가지는 성패를 좌우하는 핵심 요소인데도 고객들은 이를 간과하기 일쑤입니다.

로그가 없을 경우 가장 큰 피해를 입는 건 다름아닌 고객

노련한 사고 대응 담당자가 가장 먼저 갖는 의문은 "로그가 어디 있지?"입니다. 사고 대응 담당자가 그에 대한 해답을 얻을 수 없는 경우 다른 방도를 찾겠지만 단시간 내에 문제를 찾아서 근본 원인을 뿌리뽑을 가능성은 급격히 낮아집니다. 사고 대응의 성공은 실현 불가능한 완벽한 마무리가 아니라 합리적인 마무리에 있다는 사실을 노련한 사고 대응 담당자는 경험을 통해 배웠습니다. 장시간 동안 시스템에 본인의 개인정보가 저장되어 있었고 노출된 기록이 수십 개에서 수백만 개로 늘어났다는 이유만으로 정보 유출 피해를 입은 사람들을 제대로 파악하지 못한다면 그 고객이 입는 상처는 더 커질 수밖에 없습니다.

로그는 사고 대응 담당자와 시스템 관리자에게 특정 시기(과거나 현재)에 인프라에 어떤 일이 일어났는지 파악하는 데 결정적인 단서를 제공합니다. 안타깝게도 적절히 운영되는 나머지 보안 환경과 아주 흡사하게 광범위한 로그는 간헐적으로만 필요한데도 소중한 시스템, 네트워크 및 재정적 자원을 소비하기 때문에 오늘날의 인프라에서 가장 먼저 삭제되는 경향이 있습니다.

로깅의 성패는 주로 여과와 중앙 집중화에 의해 좌우됩니다. 모든 작업에 대한 로그를 완벽하게 보관하려면 매우 치밀하게 계획된 환경이 필요합니다. 사고 대응 담당자는 빈번히 시스템 관리자와 공조해서 과도하게 자원을 소비하지 않으면서 합리적으로 대처하는 데 필요한 최소한의 로그 세트를 파악해야 합니다. 관건은 보존과 비용/성능 간의 균형을 맞추는 것입니다. Windows 시스템에서 모든 개체에 대한 접속 로그를 보관할 필요는 거의 없지만 권한 이용에 관한 로그를 보존하지 않을 경우 사고 대응과 관리에 심각한 타격을 입을 수 있습니다. 적절히 구성된 도메인에서 도메인 관리자가 (권한이 낮은 개인 인증서를 적절히 이용하여) DNS 설정을 바꾸려고 잠시 권한을 올렸다가 문제를 발견한 경우를 예로 들어보겠습니다. 이런 상황에서 관리자는 어떤 일이 벌어졌고 누가 그랬으며 어떻게 해결해야 하는지 신속하게 확인할 수 있습니다. 그런데 권한이 낮은 개인 인증서가 실은 그 사용자가 사용한 게 아니라 인증서를 도용한 공격자가 사용한 것으로 확인됐다고 가정해 보겠습니다.

일단 로그를 수집해서 저장해야 하는데 로그를 생성한 시스템에 로그를 저장하는 것은 절대적으로 바람직하지 않습니다. 로그는 소중한 디스크 공간을 소모하는데다가 시스템 오류가 발생할 경우 유실될 수 있으며 심지어 침투에 성공한 공격자가 조작할 수도 있습니다. 중앙 집중식 저장소는 이런 문제를 최소화하는 데 도움이 되며 최소한 별도의 시스템에 저장하므로 위험 부담을 분산할 수 있습니다. 로그를 중앙 시스템으로 전송하는 방식은 조직의 필요사항과 허용되는 데이터 유실 수준에 따르는 위험 정도 산정 결과에 따라 달라질 수 있습니다. 사고 대응 담당자의 관점에서 이상적인 구조는 RELP(Reliable Event Logging Protocol)와 같은 메커니즘을 통해 처음부터 끝까지 로그를 실시간으로 전송하여 침입자가 로그를 수정할 수 있는 여지를 효과적으로 없애는 것입니다. RELP는 네트워크에 대한 신뢰성 높은 이벤트 로그를 제공할 수 있습니다. 거듭 강조하지만 성패는 균형에 의해 좌우되며 너무 잘하려다 오히려 일을 그르칠 수 있습니다. 또한 시스템의 로그를 일괄적으로 조사하는 부분 최적화된 로그 수집 시스템을 갖추는 것이 아예 아무 것도 없는 것보다 낫습니다.

로그를 조사할 빈도를 어림짐작으로 결정할 때는 공백기가 얼마나 돼야 공격자가 로그를 수정할 여지가 생기는지 추산한 후 그 기간을 2로 나눠야 합니다. 일부 기업은 고속 SAN 디스크의 비용과 애플리케이션 서버 하드웨어의 가격에 대한 견적을 냈을 때 너무 비싸다고 생각하기 때문에 중앙 로그 저장소를 기피합니다.

그러나 중앙 로그 저장에 그리 많은 비용을 들일 필요는 없습니다. 나머지 환경과 별도로 관리(신탁 또는 공유형 인증서 전무)되고 독립적으로 가동되는 것이 이상적이며 로그 분석을 조직적으로 수행하려는 경우가 아니라면 하드웨어 및 가용성 요건이 일반적인 파일 서버보다 까다로울 필요가 없습니다.

자동화는 가장 든든한 지원군

시스템 관리와 사고 대응의 자동화 여부에 따라 메이저리그 야구와 동네 야구만큼 차이가 납니다. 자동화를 구현할 경우 기업은 경우에 따라 서버 대 관리자 비율을 1,000:1 이상으로 운영할 수 있으며 사고 대응 담당자는 수천 대의 감염된 시스템을 신속 정확하게 치료할 수 있습니다. 사고 대응 측면에서는 다행스럽게도 일반적으로 여러 대의 시스템으로 구성된 환경에는 최소한 부분적으로나마 자동화가 구현되어 있기 마련이며 시스템 관리자는 프로세스를 제어하는 일종의 패치 관리 도구를 이용하여 한꺼번에 두 대 이상의 시스템에 패치를 설치할 수 있습니다. 또한 많은 환경에는 엔드포인트 보안, 자산 관리, 안티바이러스 솔루션 관리, 그리고 일상적인 관리에 필요한 그 밖의 다양한 기능을 지원하는 '에이전트'가 설치되어 있습니다. 일부 사고 대응 담당자는 어떤 도구를 이용할 수 있고 어떻게 사용해야 하는지 아는 일이 이런 도구를 사용하면서 겪는 가장 큰 어려움이라고 토로합니다. 일부 자동화 도구에 의해 지원되는 다양한 시스템 상태에 대한 맞춤형 쿼리는 사고 대응 담당자가 대단히 유용하게 활용할 수 있지만 불응기(refractory period)와 시스템이 수정되는 정도를 고려하여 쿼리를 신중하게 선택해야 합니다.

가령, 안티바이러스 솔루션에 의해 아직 감지되지 않지만 특정 디렉토리 세트에 특정 정규식과 일치하는 파일을 생성하는 것으로 파악된 신종 바이러스를 사고 대응 팀이 발견했다고 가정해보겠습니다. 이런 상황에서 인프라 팀은 바이러스에 감염됐을 가능성이 있는 모든 시스템에 패치 관리 도구, 자산 관리 도구, 그리고 안티바이러스 도구를 실행하게 됩니다. 그리고 어떤 솔루션은 패치 관리 도구를 통해 시스템에서 지표 파일을 검색하여 결과 파일을 중앙 서버에 업로드하는 방식으로 결과를 보고하는 배치 파일(batch file)을 제공합니다.

선택의 여지 없이 이런 방법을 사용할 수 밖에 없는 경우가 있겠지만 그로 인해 바이러스에 감염됐을 가능성이 있는 시스템이 수정돼서 대응 절차에 공격자가 개입할 수 있는 여지가 더 많아지기도 합니다. 그러나 만약 특정 패턴에 부합하는 파일을 찾아주는 자산 관리 도구가 있다면 최종 시스템을 수정하지 않아서 공격자에게 평소와 다름없는 상태로 보이기 때문에 이 도구를 사용하는 편이 더 낫습니다. 바이러스 제거에는 패치 관리 도구나 안티바이러스 소프트웨어를 상황에 맞게 사용하면 됩니다. 먼저, 현재 환경에 어떤 도구와 기능을 사용할 수 있는지 파악한 후 그 작업에 가장 적합한 도구를 선택하거나 인프라 팀과 공조하여 각 팀이 사용하기 효과적인 도구를 구현하는 것이 바람직합니다.

자동화에서 또 한 가지 중요한 요소는 다름아닌 스크립트입니다. 자동화 도구는 유용하게 활용할 수 있는 스크립트 언어를 자체적으로 갖추고 있지만 사고 대응 담당자가 직접 Python이나 Perl 같은 포괄적 언어로 스크립트를 작성해서 자동화 도구를 제어하고 도구의 미흡한 부분을 보완하는 방법이 훨씬 더 효율적이고 효과적입니다. 또한 노련한 시스템 관리 프로그램 개발자를 사고 대응 팀에 배치하거나 필요할 때 즉시 사고 대응에 투입할 수 있는 경우, 사고 대응 속도와 능력을 크게 개선할 수 있습니다.

최우선 요소: 인증

사고 대응의 세 번째 핵심 요소이면서 흔히 간과되는 요소는 인증입니다. 일반적으로 앞서 언급한 환경에는 강력한 중앙 인증 방식이 구축되어 있습니다. 중앙 인증 방식이 구축되어 있지 않은 경우 시스템 관리자와 사고 대응 담당자가 효율적으로 시스템을 조사하거나, 패치를 적용하거나 혹은 각 시스템의 비밀번호 수집 및 보관과 같은 원시적인 방법을 동원하지 않고서 시스템을 관리할 수 있는 길이 전혀 없습니다. 일부 대규모 환경에서든 중앙 인증 방식 대신, 관리자 권한으로 주기적으로 스크립트를 실행하는 원격 에이전트가 사용되기도 하지만 이런 설정 방식은 미흡한 응답 시간 때문에 적절한 관리와 사고 대응을 기대하기 어려우므로 가급적 지양해야 합니다.

똑똑한 업무 환경과 지원군 확보

우수한 인프라 구조는 훌륭한 사고 대응과 직결됩니다. 장애 조치(fault-tolerant) 능력, 신뢰성 및 확장성이 더욱 우수한 컴퓨팅 인프라를 구축하는 데 효과적인 도구와 프로시저는 원활하고 신속하게 사고에 대응하는 데도 도움이 되기 마련입니다. 따라서 사고 대응 팀은 시스템 관리 팀과 꾸준히 소통하면서 어떤 도구가 배치되어 있는지 파악하여 도구 활용 방법을 미리 익히는 것이 좋습니다. 이런 관계가 유지되면 시스템 관리 팀 역시 필요할 때 사고 대응 팀의 지원을 받을 수 있습니다.

규정 준수를 위해 데이터 보안과 개인정보 보호의 차이 이해

기업은 데이터에 의존해서 일상적인 비즈니스 업무를 지원합니다. 따라서 보관된 위치에 관계없이 모든 데이터와 개인정보를 보호하는 일이 무엇보다 중시됩니다. Verizon의 개인정보 침해 조사 보고서(Verizon Data Breach Investigation Report)에 따르면 데이터베이스 서버에 저장된 데이터가 침해된 전체 데이터의 92%를 차지할 정도로 압도적으로 많습니다. 안타깝게도 공격자가 데이터베이스에 침투하는 데 걸리는 시간 대비 침입을 인지해서 문제를 해결하는 데 걸리는 시간은 큰 차이가 있습니다. 공격자는 수일 만에 방어벽을 뚫지만 기업이 언제, 어디서, 어떻게 침입이 이뤄졌는지 인지하는 데에만 수주나 수개월이 걸리는 데다 이후 문제를 해결하기까지 또 수주나 수개월이 소요되기도 합니다.

다양한 유형의 정보에 각기 다른 보호 및 개인정보 보호 요건이 적용되는 실정 때문에 데이터 보안 및 개인정보 보호가 훨씬 더 복잡해집니다. 따라서 기업은 다음과 같은 전체론적 접근법으로 정보를 보호해야 합니다.

- **데이터 분석 및 분류** — 기업은 데이터가 어디에 존재하고 어떻게 관련이 있는지 전사적으로 파악해야 합니다. 그렇게 해야 민감한 데이터를 적절히 분류해서 데이터 수명주기 내내 적절하게 관리할 수 있습니다.
- **데이터 삭제** — 민감한 데이터는 문서, 서식, 스캔 이미지 등으로 보존되기도 합니다. 이 비구조적 데이터를 보호하려면 필수 비즈니스 데이터의 공유를 허용하면서 개인정보 보호 정책에 따라 민감한 정보를 삭제하는 제도가 마련돼야 합니다. 이런 비구조적 문서는 데이터베이스에 보관할 수 있습니다.
- **데이터 암호화** — 많은 규정에는 데이터베이스 암호화가 의무화되어 있습니다. 기업은 다양한 데이터 유형을 보호하는 데 효과적인 일원화된 솔루션을 갖춰야 합니다. 솔루션을 갖추면 다중 보안 환경을 구현할 수 있기 때문에 데이터베이스 활동을 모니터링하는 데도 큰 도움이 됩니다.
- **정적 데이터 마스킹(Masking)** — 일반적으로 보안은 운영 환경에 큰 비중을 두지만 다른 환경의 보안 역시 소홀히 해서는 안 됩니다. 운영 환경 하의 데이터베이스 이외의 다른 데이터베이스에 저장된 민감한 데이터를 의미 없는 값으로 대체하되, 애플리케이션 개발, 테스트, 교육 프로세스 및 QA 작업에 필요한 데이터의 가용성을 유지하면, 비즈니스 프로세스를 능률화하는 데 도움이 될 뿐 아니라 최소 사용 권한 정책을 보장하는 데도 효과적입니다. 또한 업무적으로 알 필요가 없는 사람은 아예 민감한 데이터에 접근하지 못하게 해야 합니다.
- **모니터링** — 데이터베이스, 웨어하우스 및 파일 공유 시스템에 대한 접근을 통제하고 지속적으로 모니터링하면, 데이터 접근 대상, 시기, 방법 등을 완전히 파악하여 데이터 무결성을 유지할 수 있습니다.
- **취약점 평가** — 잘못된 구성이나 기본 설정 등의 위험을 최소화할 수 있도록 데이터베이스를 강화해야 합니다.

소문의 진상 파악: 데이터 보안에 대한 관심 상승 원인

Forrester Research가 독자적으로 발행한 2011년 2월 보고서 'Forrsights: 2010 ~2011년 IT 보안의 진화(Forrsights: The Evolution Of IT Security, 2010 To 2011)'에 따르면 IT 보안이 활기와 성장을 좌우하는 가운데, 기업들이 더욱 위협적이고 영리해지는 공격자와 싸우면서, 갈수록 까다로워지는 규제 기관과 외부의 요구를 충족하며, 유례없이 급변하는 IT 환경에 적응하느라 애를 먹고 있습니다. 기업이 처한 이와 같은 현실 중 대부분은 Stuxnet 및 Aurora 같은 새로운 사이버 보안 위협, 데이터센터 가상화와 같은 IT 아키텍처 변화, 그리고 외부의 요구로 인한 중압감 상승 등 몇 가지 핵심 주제와 맞물려 있습니다.

Forrester의 보고서에 따르면 지난 몇 년간 "보안에 대한 고위 경영진의 관심과 지원이 꾸준히 높아졌습니다." Forrester가 실시한 설문조사에서 기업의 최고 정보 보안 책임자(CISO) 중 54%는 최고 경영자에게 보안 상황을 보고하고 그 중 42%는 IT 부서 이외의 부서에 상황을 알리고 있는 것으로 확인되었습니다. 이 비율은 다양한 산업에 종사하는 모든 유형의 조직에서 업무에 미치는 보안의 영향이 증가하고 있음을 시사합니다. 보안을 중요한 혹은 가장 중요한 선결과제로 여기는 기업 역시 그 어느 때보다 많아졌습니다.

그러면 데이터 보안 및 개인정보 보호에 대한 관심도 증가의 원동력이 되는 여러 가지 요인을 자세히 파헤쳐보겠습니다.

IT 환경의 변화와 진화하는 비즈니스 프로젝트

기업들이 외주, 가상화, 클라우드, 모바일, 웹 2.0, 소셜 네트워크와 같은 진화하는 비즈니스 프로젝트를 수용함에 따라 보안 정책과 그에 상응하는 기술 역시 진화하고 있습니다. 따라서 기업은 민감한 데이터의 보관 장소와 접근 방법에 대해 보다 포괄적으로 생각해야 합니다. 또한 기업은 고객 정보, 영업 비밀, 개발 계획, 경쟁 차별화 동인과 같은 여러 가지 영역의 민감한 데이터를 고려해야 합니다.

더욱 지능적이고 치밀해지는 공격 수법

많은 기업들은 갈수록 벌어지는 공격자의 능력과 보안 능력의 격차 때문에 어려움을 겪고 있습니다. 기업은 끊임 없이 변하고 복잡하며 더욱 광범위해지는 외부 공격에 골머리를 앓고 있습니다. 앞서 언급한 Forrester의 보고서에 따르면 보안 공격이 10년 전에 비해 훨씬 더 심각한 피해를 기업에 입히고 있습니다. 과거에는 사업 운영에 일시적인 차질을 빚는 바이러스 감염이나 단기적인 서비스 거부(DoS) 공격이 가장 심각한 문제였습니다.

그러나 오늘날 고객 정보나 영업 기밀과 같은 기업 정보 절취는 수십억 달러의 영업 손실, 벌금 및 소송, 그리고 돌이킬 수 없는 기업 이미지 훼손을 초래할 수 있습니다.

규정 준수

준수해야 할 규정은 그 수와 종류가 많고 전 세계 기업에 영향을 미치고 있습니다.
준수해야 할 규정이 갈수록 늘고 있는데다 빠른 시간 내에 규정을 충족해야 하는 부담도 커지고 있습니다. 기업은 시간적 측면에서 엄청난 압박에 시달리며 규제 기관에 즉시 규정을 준수하고 있음을 입증해야 합니다. 그렇지 못할 경우 평판 훼손과 엄청난 벌금을 감수해야 합니다.

정보 급증

전자 정보가 믿기 어려울 정도로 급증하고 있습니다. IDC의 추산에 따르면 현재 세계 인구 한 명당 45기가바이트의 데이터, 즉 총 28,010억 기가바이트의 데이터가 존재하고 있습니다. 이 데이터 중 단 5%만 기업의 데이터 서버에 저장되었다가 사라지는데 기업 데이터는 1년에 무려 60%씩 증가하여 2011년을 기준으로 14엑사바이트에 이르는 것으로 추산됩니다. 정보가 급증하면서 공개 정보와 개인 정보를 일상 생활에서 손쉽게 접할 수 있게 되었습니다. 중요한 비즈니스 애플리케이션은 일반적으로 합법적 목적으로 이 정보를 수집합니다. 그러나 인터넷과 정보 시스템의 상호 연결성이란 특성뿐 아니라 기업용 ERP, CRM 및 맞춤형 비즈니스 애플리케이션 때문에 민감한 데이터가 도난 당하거나 오용될 소지가 있습니다.

내부 위협

데이터 침해 사고 중 상당 비율은 사실상 내부자의 실수나 악용 때문에 발생합니다. 결제 카드 번호나 기타 민감한 정보를 오용하는 직원부터 기밀정보를 랩탑에 저장했다가 도난 당하는 직원에 이르기까지 다양한 경우가 그런 사례에 해당됩니다. 비즈니스 파트너, 협력업체 혹은 다른 제 3자를 비롯해서 데이터가 어디에 존재하든 기업은 그 데이터를 보호할 책임이 있습니다.

따라서 기업은 데이터 보안 및 개인정보 보호 문제에 더욱 심혈을 기울여야 합니다. 최근 들어 기업은 특정 문제 해결용 맞춤형 솔루션을 개발하고 보안 정책, 개인정보 보호 정책 및 프로시저를 구축하는 데 관심을 돌리고 있습니다.

보안과 개인정보 보호의 차이 이해

보안과 개인정보 보호는 서로 관련이 있지만 서로 다른 개념입니다. 보안은 인증을 토대로 특정 영역이나 데이터에 대한 접근을 금지 또는 허용하는 인프라 수준의 제제입니다. 반면에 개인정보 보호는 특정 데이터 세트에 대한 접근 권한을 부여 받은 사용자를 위해 접근을 통제하는 것입니다. 개인정보 데이터 보호는 데이터에 접근할만한 합법적 업무 목적을 지닌 사람에 대한 제한 혹은 통제와 관련이 있습니다. 업무 목적은 일반적으로 직무를 기준으로 정해지며, 직무는 준수해야 할 규정에 의해 정의됩니다.

데이터 보안 솔루션의 용도로는 데이터베이스 활동 모니터링 및 데이터베이스 취약점 평가 등이 있습니다. 그리고 개인정보 데이터 보호 솔루션의 용도로는 민감한 데이터 삭제 또는 데이터 마스킹 등이 있습니다. 보안과 개인정보 보호의 차이점은 UCLA Medical Center의 의사들이 가수 브리트니 스피어스의 의료 기록을 조사하다 발각된 사례를 통해 쉽게 설명할 수 있습니다. 의사들이 의료 기록을 봐야 하기 때문에 이 병원의 보안 정책은 전혀 문제가 없었지만 의사들이 치료 목적이 아니라 단지 호기심 때문에 파일에 접근했기 때문에 개인정보 보호 논란이 일었던 것입니다.

손실액 증가: 미흡한 데이터 보안 및 개인정보 보호로 인해 초래되는 위험

Ponemon의 2010년 조사에 의하면 데이터 침해 사고 손실액이 5년 연속 증가했습니다. 기업의 2010년 데이터 침해 사고 평균 손실액은 2009년의 680만 달러보다 7% 증가한 720만 달러였습니다. 데이터 침해 사고 총 비용 역시 2006년 이후 매년 증가하고 있습니다. 그리고 데이터 침해 사고 피해를 입은 레코드당 기업의 2010년 평균 손실액은 2009년보다 10달러(5%) 증가한 214달러였습니다.

Ponemon의 조사에 따르면 2010년 최대 데이터 침해 사고 손실액은 2009년보다 480만 달러(15%) 더 많은 3,530억 달러였으며 최소 데이터 침해 사고 손실액은 2009년보다 3만 달러(4%) 증가한 78만 달러였습니다. 전년도와 마찬가지로 데이터 침해 사고 손실액은 피해를 입은 레코드의 수와 정비례했습니다.

그 밖에도 데이터 침해 사고를 당한 기업은 벌금이나 형사책임, 투자자의 우려로 인한 주가 하락, 부정적 여론 등의 잠재적 손해도 감수해야 합니다. 신뢰할 수 없는 기업으로 낙인 찍히면 돌이킬 수 없는 이미지 훼손을 입을 수밖에 없습니다.

일반적인 사고의 원인은 다음과 같습니다.

- **과도한 접근 권한과 접근 권한이 있는 사용자의 오용:** 직무에 필요한 수준 이상의 데이터베이스 접근 권한이 사용자(또는 애플리케이션)에게 부여되면 이 권한을 기밀 정보에 접근하는 데 악용할 소지가 있습니다.
- **접근 권한 무단 승격:** 공격자가 데이터베이스 관리 소프트웨어의 취약점을 악용해서 낮은 수준 접근 권한을 높은 수준 접근 권한으로 올릴 수 있습니다.
- **SQL 인젝션 공격:** SQL 인젝션 공격에는 공격자가 일반 사용자용 웹 애플리케이션과 저장된 프로시저의 취약점을 악용하여 (종종 무단으로 승격한 권한을 이용하여) 무단으로 데이터베이스 쿼리를 전송하는 과정이 수반됩니다. 심지어 공격자는 SQL 인젝션 공격 수법을 이용해서 전체 데이터베이스에 대한 무제한적인 접근 권한을 획득할 수도 있습니다.
- **서비스 거부(DoS - Denial Of Service):** DoS에는 다양한 수법이 사용될 수 있습니다. 일반적인 DoS 수법으로는 버퍼 오버플로우, 데이터 손상, 네트워크 트래픽 초과, 자원 소모 등이 있습니다. 자원 소모는 데이터베이스 환경에만 발생하는데 간과되기 일쑤입니다.
- **백업 데이터 노출:** 최근 발생한 일부 대규모 공격에는 암호화되지 않은 데이터베이스 백업 테이프와 하드 디스크 절취가 수반되었습니다.

거시적인 데이터 보안 및 개인정보 보호 접근법 활용

기업은 거시적인 관점에서 데이터를 보호해야 합니다. 거시적인 접근법은 운영 환경과 다른 환경(개발, 테스트 및 교육)의 구조적 데이터와 비구조적 데이터를 비롯해서 기업 전체의 여러 장소에 보관 중인 다양한 유형의 데이터를 보호하는 데 목적이 있습니다. 거시적인 접근법은 프로세스나 복잡성을 가중시키지 않으면서 한정된 자원을 최대한 활용하는 데 효과적입니다. 또한 거시적인 접근법은 중대한 비즈니스 프로세스나 일상적인 작업을 중단하지 않은 채 규정 준수 여부를 증명하는 데 도움이 됩니다.

거시적인 접근법을 도입하려는 기업은 아래 네 가지 질문을 고려해야 합니다. 이 질문들은 가장 심각한 데이터 취약점에 관심을 기울이는 데 유용합니다.

1. 민감한 데이터가 어디에 존재하는가?
2. 기업 데이터베이스에 대한 접근을 통제, 모니터링 및 조사하려면 어떻게 해야 하는가? 무단 접근뿐 아니라 허가 받은 접근으로부터 데이터를 보호하려면 어떻게 해야 하는가?
3. 필요에 맞게 문서 형식의 비즈니스용 기밀 정보의 공유를 허용함과 동시에 이를 보호하려면 어떻게 해야 하는가?
4. 애플리케이션 개발, 테스트, 교육 환경의 데이터에 대한 접근을 허용함과 동시에 이를 보호하려면 어떻게 해야 하는가?

이에 대한 답변은 거시적인 데이터 보호 접근법을 구축할 수 있는 초석이 되며 기존의 접근법에서 간과되기 쉬웠던 핵심 분야에 관심을 기울이는 데 도움이 됩니다.

1. 데이터가 어디에 존재하는지 알아야만 그 데이터를 보호할 수 있습니다. 민감한 데이터는 운영 환경과 기타 환경에 구조적 혹은 비구조적 형식으로 존재합니다. 기업은 그 출처가 어디든 모든 데이터 자산과 데이터 관계를 문서화하고 정의해야 합니다. 기업 데이터를 분류하고 데이터 관계를 이해하며 서비스 수준을 정의하는 일 역시 중요합니다. 데이터 분석 프로세스는 데이터의 가치와 데이터 패턴을 파악하여 개별 데이터 요소들을 논리적 정보 단위, 가령 고객, 환자 또는 청구서와 같은 '비즈니스 개체'로 분류할 수 있습니다.

2. 데이터베이스 활동 모니터링 솔루션은 데이터베이스 고유 로그 저장 및 감사 기능과 별도로, 권한 있는 혹은 권한 없는 사용자 및 애플리케이션의 접근 상황을 모니터링합니다. 이 솔루션은 관리자의 활동을 모니터링함으로써 권한 있는 사용자의 업무 분리 문제를 보완 통제하는 역할을 할 수 있습니다. 또한 데이터베이스 활동 모니터링 기술은 애플리케이션 계층에서 발생하는 특이한 데이터베이스 판독 및 업데이트 활동을 감지하여 데이터 보안을 개선할 수 있습니다. 데이터베이스 이벤트 취합, 관계 분석, 보고 기능은 데이터베이스 감사 작업을 지원하므로 데이터베이스 활동 모니터링의 또 다른 요소인 데이터베이스 고유 감사 기능을 별도로 사용할 필요가 없습니다. 데이터베이스 활동 모니터링 솔루션은 악의적 활동이나 부적절한 혹은 승인되지 않은 데이터베이스 관리자(DBA)의 접근을 감지할 수 있어야 합니다.

3. 데이터 삭제 솔루션은 업무 역할 또는 사업 용도를 토대로 양식과 문서에서 민감한 데이터를 삭제할 수 있습니다. 예를 들어, 의사는 증상 및 예후 데이터와 같은 민감한 정보를 열람해야 하지만, 진료비 청구 담당 직원은 환자의 의료보험 번호 및 진료비를 청구할 주소를 알아야 합니다. 데이터 삭제 솔루션의 목적은 데이터를 적절히 보호함과 동시에 비즈니스 필요사항을 충족하고 '알아야 할 필요성'을 기준으로 데이터를 관리하는 것입니다. 또한 데이터 삭제 솔루션은 비구조적 문서, 양식, 그리고 그래프 형식의 민감한 정보를 보호해야 합니다.

4. 일반 환경(개발, 테스트, 교육 환경)의 데이터에서 개인 식별 정보를 제거한다는 것은 개인을 식별하는 데 사용될 수 있는 데이터 구성 요소를 체계적으로 삭제, 마스킹 또는 변환하는 절차를 말합니다. 데이터에서 개인 식별 정보를 제거하면 개인정보 보호 규정을 준수하면서 개발자, 테스터 및 교육자가 실제 데이터를 이용하고 타당한 결과를 산출할 수 있습니다. 그런 방법으로 '정제'된 데이터는 사회통념상 개발, 테스트, 교육 환경에 사용해도 무방한 것으로 간주되며 데이터를 도난, 유출 또는 분실한 경우 누군가가 이를 사용하지 못하도록 막는 데 도움이 됩니다.

거시적인 데이터 보호를 위한 3단계 접근법

이해와 정의

기업은 민감한 데이터가 어디에 존재하는지 파악해서 데이터 유형을 분류 및 정의하고 데이터를 일관적으로 보호할 수 있는 체제와 정책을 마련해야 합니다. 데이터는 거의 문서화되지 않은 상태로 다수의 애플리케이션, 데이터베이스, 플랫폼에 분산되어 있는 경우가 많은데, 많은 기업들은 시스템 및 애플리케이션 전문가를 너무 지나치게 믿고 이런 정보를 맡깁니다. 그런데 때때로 이 정보가 애플리케이션 로직에 삽입되어 은연 중에 숨겨진 데이터 관계가 내재할 수 있습니다.

민감한 정보를 찾아서 데이터 관계를 파악하려면 면밀한 분석이 필요합니다. 그리고 데이터 출처와 관계를 확실히 이해하고 문서화해야만 민감한 데이터가 무방비 상태로 노출될 우려를 막을 수 있습니다. 또한 기업 데이터 보안 및 개인정보 보호 정책을 수립하려면 데이터 출처와 관계를 완벽하게 이해하는 일이 선행되어야 합니다.

보안과 보호

데이터 보안 및 개인정보 보호 솔루션은 이기종 환경을 아울러서 운영 환경과 기타 환경에 존재하는 구조적 데이터와 비구조적 데이터를 보호합니다. 데이터 보안 및 개인정보 보호 솔루션은 데이터베이스, ERP/CRM 애플리케이션, 그리고 양식 및 문서와 같은 비구조적 환경의 민감한 데이터를 보호하는 데 유용합니다. 이 솔루션의 핵심 기능으로는 데이터베이스 활동 모니터링, 데이터 마스킹, 데이터 삭제, 데이터 암호화 등이 있습니다. 거시적인 데이터 보호 접근법은 기업의 모든 데이터를 안전하게 지키는 데 효과적입니다.

구조적 데이터: 이 데이터는 데이터 모델을 기반으로 하며 데이터베이스나 XML 같은 구조적 형식으로 저장됩니다.

비구조적 데이터: 이 데이터는 자필 또는 워드 프로세싱 문서, 이메일 메시지, 디지털 오디오 및 비디오 같은 기계 입력 형식으로 존재합니다.

온라인 데이터: 이 데이터는 메타데이터, 구성 데이터 또는 로그 파일 등의 형식으로 일상적인 비즈니스를 지원하는 데 사용됩니다.

오프라인 데이터: 이 데이터는 백업 테이프나 스토리지 디바이스에 저장됩니다.

모니터링과 감사

데이터의 위치를 파악해서 접근을 통제할 준비가 완료된 기업은 규정 준수 사실을 입증하고 새로운 내외부의 위협에 대응할 수 있도록 준비하며 지속적으로 시스템을 모니터링해야 합니다. 사용자 활동, 개체 생성, 데이터베이스 구성, 사용자 접근 권한을 모니터링하면 IT 전문가와 감사 담당자가 애플리케이션 및 데이터베이스 사용자를 추적하기가 수월합니다. IT 전문가와 감사 담당자는 팀을 이뤄서 적절한 행동에 관한 정책을 세부적으로 지정하여 이 정책을 위반할 경우 경보를 수신할 수 있습니다. 기업은 규정 준수 사실을 신속하게 입증하고 감사 담당자에게 규정 준수 상황을 검사할 권한을 부여해야 합니다. 감사 보고 및 승인 기능은 비용을 억제하고 기술적, 업무적 차질을 최소화함과 동시에 규정 준수 프로세스를 능률화하는 데 유용합니다. 요약하자면, 이에 충실한 기업은 각 트랜잭션에 대한 '6하 원칙' 형식으로 모든 데이터베이스 상황을 지속적이고 세부적으로 추적한 기록을 확보할 수 있습니다.

결론

데이터 보안 및 개인정보 보호에 대한 지속적이고 철저한 보호는 모든 모범 사례에 반드시 수반돼야 할 요소입니다. 기업은 이해와 정의(Understand and Define), 보안과 보호(Secure and Protect), 모니터링과 감사(Monitor and Audit)로 이뤄진 3단계 전략으로 자사의 데이터 보안과 개인정보 보호하기 위한 거시적인 접근법을 지원하는 방안을 고려할 필요가 있습니다.

단원 3
소프트웨어 개발 환경 보안 현황

이 단원에서는 소프트웨어 개발 과정의 보안 문제를 해결하는 절차와 방법을 설명합니다. 또한 기업이 기존 취약점을 찾아내서 새로운 취약점이 추가로 발생하는 것을 막는 방법에 대해서도 논의합니다. 네트워크 또는 웹 애플리케이션을 이용하여 민감한 데이터를 수집하거나 교환하는 보안 전문가라면 특히 유용한 정보가 될 것입니다. 그 밖에도 IBM AppScan 그룹이 애플리케이션 개발 단계에서 실행한 정적 및 동적 보안 테스트와 그 결과를 소개하겠습니다.

웹 애플리케이션 실제 평가로 얻은 결론

방법론

IBM AppScan OnDemand Service는 소프트웨어를 구매해서 관리하거나 고도로 숙련된 전문 애플리케이션 보안 인력을 채용하지 않고서도 고객이 웹 애플리케이션 취약점을 파악해서 해소하는 데 유용한 클라우드 기반의 솔루션입니다. IBM 애플리케이션 보안 분석가들은 IBM AppScan Enterprise Edition 소프트웨어로 애플리케이션을 분석하여 고객 및 직원 기록 혹은 기업의 지적 자산과 같은 데이터의 침해 및 손실로 이어질 수 있는 보안 취약점을 찾아냅니다. IBM AppScan Enterprise Edition 소프트웨어는 크로스 사이트 스크립트(XSS), 버퍼 오버플로우, F/F(Flash/Flex) 애플리케이션 및 웹 2.0 노출 검사 등 일반적인 웹 애플리케이션 취약점을 테스트하는 데 사용됩니다. 그 밖에도 이 소프트웨어는 사이버 공격을 차단할 수 있도록 웹 속성에 내재된 악성 코드를 검사하여 감지하는 기능을 지원합니다.

IBM은 2011년에 IBM AppScan OnDemand Service을 이용하여 보안 평가를 실시하는 한편, 237차례의 보안 테스트를 실시하여 실 세계의 취약점에 대한 데이터를 수집했습니다. 이 평가 결과는 IBM AppScan OnDemand Service에서 수동 보안 테스트 및 검사를 통해 얻은 애플리케이션 보안 평가 결과를 종합한 것입니다. 모든 경우에 거짓 양성 반응은 평가 결과에서 제외됐으며 취약점은 OWASP(Open Web Application Security Project)이 발표한 다음과 같은 상위 10가지 취약점으로 나뉩니다.

1. 인젝션
2. XSS(Cross-Site Scripting)
3. 취약한 인증 및 세션 관리
4. 직접 개체 참조
5. CSRF(Cross Site Request Forgery)
6. 잘못된 보안 설정
7. 취약한 암호화 저장
8. URL 접근 통제 실패
9. 미흡한 전송 계층 보호
10. 무단 리디렉션 및 포워딩

각 범주를 대상으로 다음과 같은 두 가지 핵심적인 통계가 산정되었습니다.

1. 해당 범주에서 10대 취약점이 한 가지 이상 발견될 확률(%)
2. 해당 범주에서 발견되는 평균 취약점 개수

IBM은 2007년부터 유사 데이터를 수집하여 그 결과를 토대로 지난 5년간의 추세를 파악할 수 있었습니다. 또한 이 연도별 데이터는 2010년 OWASP 10대 취약점 명단으로 도식화되었습니다.

통계 요점

또한 IBM은 데이터를 더욱 심층적으로 분석하는 데 도움이 될만한 다음과 같은 통계를 추가적으로 분석했습니다.

테스트 데이터 분류 **기준이 된 사업 부문**:

- 금융
- 제조
- 정보 기술
- 물류
- 정부
- 기타

애플리케이션 보안 테스트 주기는 애플리케이션 테스트 유형에 따라 다음과 같은 분류되었습니다.

- **최초 테스트** — 처음 실시한 애플리케이션 테스트
- **분기별 평가** — 정기적으로 실시한 애플리케이션 테스트
- **재테스트** — 최초 테스트에서 얻은 결과를 확정하기 위해 실시한 후속 테스트

참고: 정보는 샘플 크기가 적절한 데이터를 지원하는 통계 그룹으로만 분류되었습니다. 샘플 크기가 너무 작은 경우 통계값은 무시되었습니다. 따라서 모든 사업 부문이나 기술을 대변하는 것은 아닙니다.

2011년 애플리케이션 취약점 동향

다음 도표에는 애플리케이션 보안 테스트에서 각각의 OWASP 10대 취약점이 발견된 비율이 제시되어 있습니다.

OWASP 10대 취약점 도표를 소개하는 이유는 더욱 심층적인 평가를 수행하고 업계 모범 사례와 비교하기 적합하다고 판단했기 때문입니다. 평가 결과가 OWASP 10대 취약점과 직결되지 않은 경우 그 결과는 '잘못된 보안 설정' 범주에 반영되었습니다. 따라서 당연히 이 잘못된 보안 설정의 수치가 원래보다 더 높습니다.

이 평가 결과에는 애플리케이션 문제를 최소화한 기업들이 포함되어 있다는 점에 주목할 필요가 있습니다. 그 기업들은 보안 프로그램을 이미 배치한 상태였거나 과거에 보안 침해 사고를 당한 적이 있을 가능성도 있습니다. 따라서 이 데이터는 보편적인 웹 애플리케이션이나 단 한 번도 평가를 받은 적이 없는 애플리케이션의 상태를 대변하지 않습니다. 일부 취약점의 비율은 눈에 띄는 감소세를 보이고 있으며 감소세는 투자 수익에 가장 큰 영향을 미칩니다.

취약한 인증 및 세션 관리 문제는 10회의 테스트에서 거의 8회나 발견되었습니다. 테스트 대상이 된 애플리케이션 중 다수는 세션 조작을 막을 능력이 미흡해서 세션 무단 변경 방식의 공격에 취약했습니다. 세션 종료 및 세션 재사용과 관련된 문제 역시 이렇게 높은 수치가 나오는 데 한몫 했습니다.

2011년에 실시한 애플리케이션 취약점 테스트에서 CSRF 취약점이 발견된 비율은 59%였던 2010년 비해 크게 줄어든 28%였습니다.

이런 감소세를 보인 주된 이유는 이런 유형의 취약점에 대한 인지도가 높아졌고 CRSF 토큰 사용 방법이 개선됐기 때문인 것으로 분석됩니다.

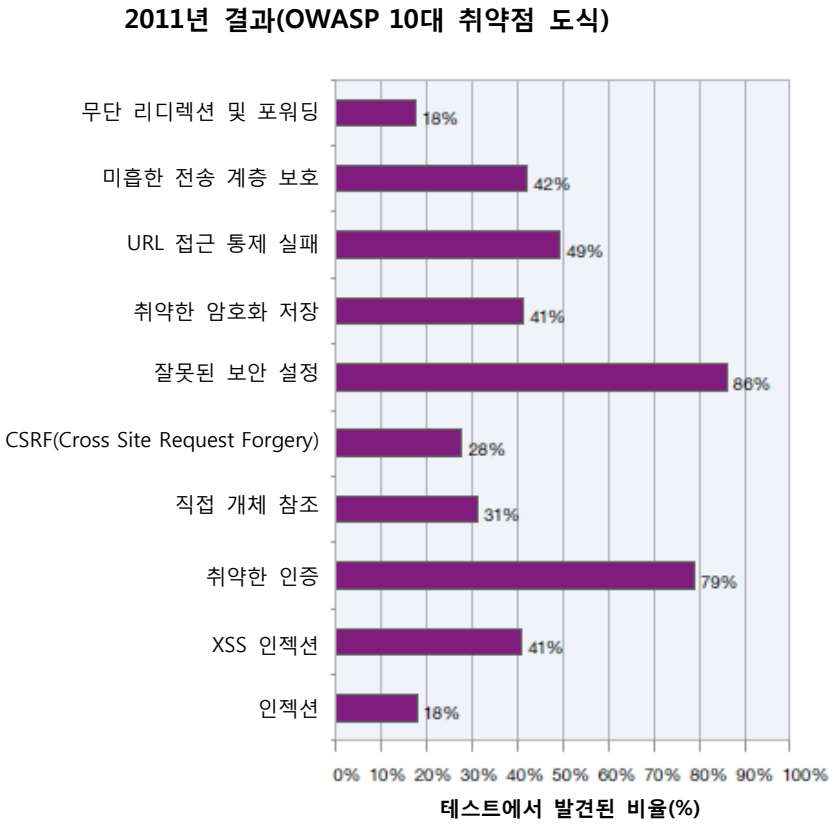


그림 50: 2011년 결과(OWASP 10대 취약점 도식)

연도별 동향(2007~2011년)

IBM이 2007년에 애플리케이션 보안 통계를 기록하기 시작한 이후로 XSS 및 SQL 인젝션과 같은 입력값 제어와 관련한 취약점 사례가 꾸준히 감소했습니다. 2011년에 실시한 테스트에서 XSS가 발견될 확률은 계속 감소했지만 발생 확률 40% 수준에서 정체될 기미를 보이고 있습니다. 인젝션 취약점, 그 중에서도 특히 SQL 인젝션 취약점은 테스트에서 20% 내외의 발생 확률을 꾸준히 유지할 것으로 보입니다.

통계만 보고 단정짓는 건 다소 무리가 있으나 IBM의 테스트에서 모범 사례와 안전한 코딩 규칙을 준수하여 유효하지 않은 입력값을 차단한 애플리케이션은 XSS과 같은 입력값 관련 문제가 거의 혹은 전혀 발생하지 않는 것으로 확인되었습니다. 그러나 XSS 취약점이 애플리케이션 취약점 테스트에서 40% 이상 발견된 점으로 미루어 보아 보안 코딩 규칙을 제대로 따르지 않은 애플리케이션이 여전히 많은 것으로 추정됩니다. 여러 가지로 개선되고 있는 건 분명하지만 아직 만족하기엔 턱없이 부족합니다. 아주 쉽게 이해할 수 있고 아주 쉽게 시험해 볼 수 있으며 아주 쉽게 수정할 수 있는 애플리케이션에서 XSS 취약점이 40% 이상 발견됐다는 사실은 특히 우려할만합니다. 웹 애플리케이션의 취약점이 여전히 많은 데이터 침해 사고의 원인으로 작용하고 있습니다. 데이터 침해 사고는 2011년 상반기에서도 증가했습니다. 더군다나 IBM X-Force가 2011년을 '보안 침해의 해'로 선언할 정도로 데이터 침해 사고는 폭발적인 증가세를 기록했습니다.

IBM X-Force가 주목한 또 다른 중요한 기준점은 '보안 테스트에서 해당 사례가 발견되는 평균 건수'입니다. XSS 취약점이 파악된 경우 XSS의 취약점 피해 사례는 감소하는 것으로 분석되었습니다. 실제로 2009년에 XSS 평균 건수는 40건 이상이었던 반면 2011년의 평균 건수는 3건을 약간 상회하는 수준에 불과했습니다.

입력값 제어 기능이 아예 존재하지 않는 애플리케이션은 찾아보기 훨씬 힘들어졌습니다. XSS 취약점이 발견된 애플리케이션 중 대다수는 일정 형식의 입력값 제어 기능을 갖추고 있지만 필터 및 제어 기술을 회피하도록 특화된 공격 수법에 대한 대응은 미흡했습니다.

두 가지 웹 애플리케이션 취약점의 연도별 추세
IBM AppScan OnDemand Premium Service

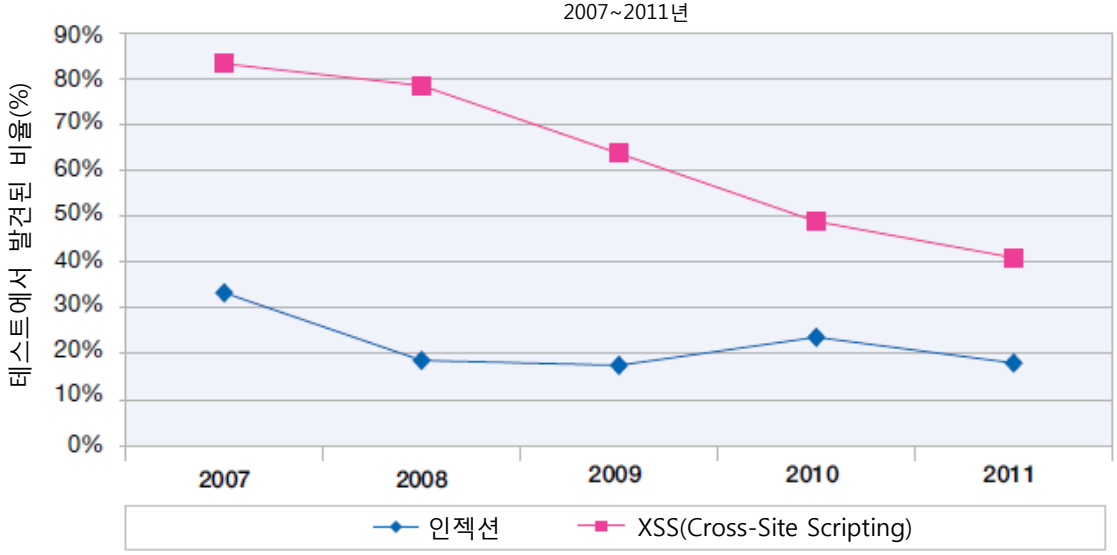


그림 51: 두 가지 웹 애플리케이션 취약점의 연도별 추세
IBM AppScan OnDemand Premium Service(2007~2011년)

연별 추세										
취약점 유형	2007년		2008년		2009년		2010년		2011년	
	테스트당 평균 취약점 건수	취약점이 발견될 가능성	테스트당 평균 취약점 건수	취약점이 발견될 가능성	테스트당 평균 취약점 건수	취약점이 발견될 가능성	테스트당 평균 취약점 건수	취약점이 발견될 가능성	테스트당 평균 취약점 건수	취약점이 발견될 가능성
인젝션	1.3	33%	5.3	19%	1.7	18%	2.3	24%	2.1	18%
XSS(Cross-Site Scripting)	12.7	83%	17.9	79%	40.8	64%	5.8	49%	3.3	41%
취약한 인증	11.2	83%	4.8	84%	3.2	65%	2.5	53%	9.7	79%
직접 개체 참조	2.6	50%	3.2	54%	3.0	51%	1.9	33%	1.6	31%
CSRF(Cross Site Request Forgery)	1.9	22%	1.8	20%	7.9	59%	3.8	53%	2.0	28%
잘못된 보안 설정	46.9	83%	22.6	74%	23.5	68%	15.3	56%	10.7	86%
취약한 암호화 저장	21.7	38%	17.9	56%	29.1	38%	19.8	45%	11.9	41%
URL 접근 통제 실패	7.2	13%	6.0	19%	9.7	13%	6.6	15%	5.0	49%
미흡한 전송 계층 보호	7.3	28%	2.4	17%	2.5	35%	1.6	22%	9.8	42%
무단 리디렉션 및 포워딩	1.7	7%	0.5	5%	0.1	3%	0.4	4%	0.3	18%

도표 8: 두 가지 웹 애플리케이션 취약점의 연도별 추세(2007~2011년), IBM Rational AppScan OnDemand Premium Service

산업 부문

2010년에 그랬던 것처럼 IBM은 2011년 통계를 데이터 기준에 부합하는 산업 부문별로 분류했습니다.

2011년에 금융 서비스용 애플리케이션이 다시 가장 보안 성능이 우수한 부문으로 복귀했습니다. 다음 도표는 각 사업 부문의 XSS, 인젝션 및 CSRF 취약점 발견 비율을 비교해서 보여주고 있습니다. 정부용 애플리케이션은 세 가지 취약점에서 모두 가장 성능이 미흡한 것으로 조사되었습니다. 이런 변화의 원인이 확실한 건 아니지만 이미지 훼손이 한 가지 요인으로 작용한 것으로 판단됩니다. 정부용 애플리케이션에서 데이터 침해 사고가 발생한 경우 보안 강화에 대한 투자를 늘릴 가능성이 금융 서비스용 애플리케이션에 비해 상대적으로 낮습니다.

CSRF 취약점은 다른 부문에 비해 금융 서비스용 애플리케이션에서 발견된 확률이 훨씬 낮습니다. 주요 원인은 CSRF 공격 방식이 미치게 될 파장으로 인해 금융 부문이 이 공격 방식을 훨씬 더 심각하게 받아들이고 있기 때문으로 추정됩니다. 이런 공격 방식의 주요 목적은 피해자를 사칭하는 것이며 금융 거래에 사용되는 애플리케이션이나 금융 서비스용 애플리케이션이 주요 공격 대상이 될 가능성이 높습니다.

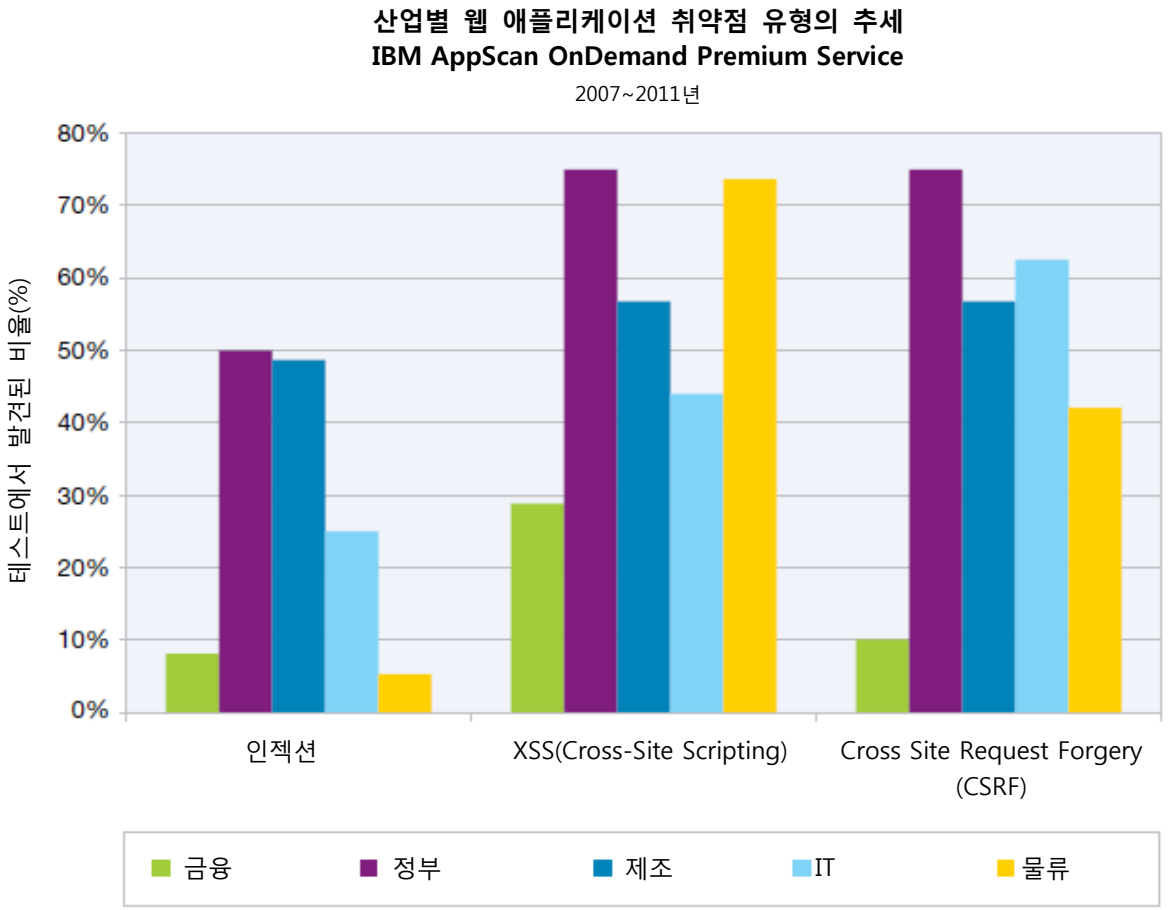


그림 52: 산업별 웹 애플리케이션 취약점 유형의 추세
IBM AppScan OnDemand Premium Service(2007~2011년)

산업 부문										
취약점 유형	금융 서비스		정부		제조		IT		물류	
	테스트당 평균 취약점 건수	취약점이 발견될 가능성	테스트당 평균 취약점 건수	취약점이 발견될 가능성	테스트당 평균 취약점 건수	취약점이 발견될 가능성	테스트당 평균 취약점 건수	취약점이 발견될 가능성	테스트당 평균 취약점 건수	취약점이 발견될 가능성
인젝션	0.1	8%	3.5	50%	10.9	49%	0.6	25%	0.3	5%
XSS(Cross-Site Scripting)	0.4	29%	5.8	75%	13.2	57%	6.1	44%	2.5	74%
취약한 인증	5.1	73%	12.7	94%	4.8	84%	26.5	100%	38.9	84%
직접 개체 참조	0.3	18%	5.6	94%	2.1	35%	4.8	63%	4.5	47%
CSRF(Cross Site Request Forgery)	1.1	10%	3.9	75%	3.0	57%	2.3	63%	5.7	42%
잘못된 보안 설정	2.9	82%	18.9	100%	25.9	97%	39.7	100%	10.5	74%
취약한 암호화 저장	4.8	22%	19.4	100%	12.3	51%	39.9	94%	37.1	79%
URL 접근 통제 실패	1.0	44%	14.9	100%	0.9	19%	29.4	81%	15.2	79%
미흡한 전송 계층 보호	3.8	25%	1.4	75%	13.6	59%	36.3	88%	34.3	79%
무단 리디렉션 및 포워딩	0.2	14%	0.2	19%	1.1	46%	0.1	6%	0.0	0%

도표 9: 각 산업에서 가장 흔히 발견되는 웹 애플리케이션 취약점, IBM AppScan OnDemand Premium Service

애플리케이션 보안 테스트 주기

IBM AppScan OnDemand Premium Service는 이 데이터가 수집된 경우 일반적으로 테스트 대상 애플리케이션에 대한 재테스트 옵션을 제공합니다. 일반적으로 재테스트는 최초 테스트를 실시한 지 60일 이내에 이뤄지며 항상 그 기간 내에 모든 문제를 기록하고 종결하는 건 아닙니다.

애플리케이션 재테스트에서 발견되는 취약점 건수는 최초 테스트에서 발견된 것보다 더 적기 마련입니다. 테스트에서 평균적으로 발견되는 취약점 건수를 살펴보면 그 차이가 상당히 큽니다. OWASP 10대 취약점 범주마다 최초 테스트와 재테스트에서 발견되는 건수 차이는 두 배 이상입니다.

아래 도표는 최초 테스트와 차후 실시한 재테스트에게 발견된 취약점 건수 차이를 보여주고 있습니다.

특별한 경우가 아닌 한 재테스트를 실시하여 문제가 해결됐는지 확인하는 것이 바람직합니다. 애플리케이션 최초 테스트 이후 충분한 조치를 취했다면 분기별 결과가 재테스트 결과와 비슷한 수준으로 나오는 게 정상이지만 그런 경우는 흔치 않습니다. 조만한 애플리케이션을 다시 테스트한다는 사실은 개발 팀에게 동기 요인으로 작용합니다. 그렇지 않을 경우 재테스트 결과는 분기별 결과와 별 차이가 없을 것입니다.

또 다른 동기 요인은 고객이 정기적으로 분기별 테스트를 실시하는 이유는 취약점을 줄여야 한다는 압박 때문이 아니라 규제 준수 때문이라는 점입니다. 결국, 항상 재테스트를 실시해서 문제가 해결됐는지 확인하는 것이 가장 이상적입니다. 재테스트를 비용 효율적으로 실시하려면 자사가 보유한 도구와 전문 지식을 활용하는 방안을 고려할 필요가 있습니다.

테스트 주기 사이의 개선 상태
IBM AppScan OnDemand Premium Service

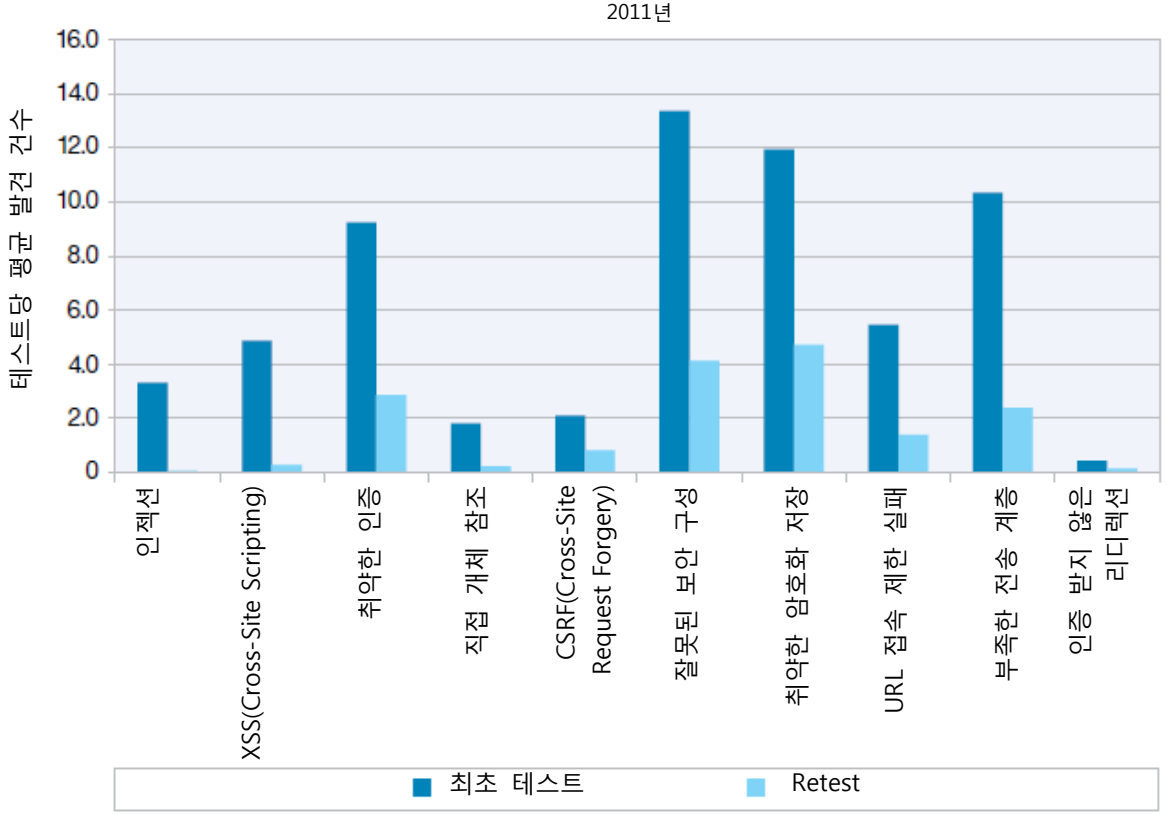


그림 52: 산업별 웹 애플리케이션 취약점 유형의 추세

IBM AppScan OnDemand Premium Service(2007~2011년)

보안 테스트 주기						
취약점 유형	최초 테스트		분기별 테스트		재테스트	
	테스트당 평균 취약점 건수	취약점이 발견될 가능성	테스트당 평균 취약점 건수	취약점이 발견될 가능성	테스트당 평균 취약점 건수	취약점이 발견될 가능성
인젝션	3.3	27%	0.2	5%	0.1	4%
XSS(Cross-Site Scripting)	4.9	46%	3.0	76%	0.3	21%
취약한 인증	9.2	82%	36.3	86%	2.9	70%
직접 개체 참조	1.8	37%	4.1	43%	0.2	15%
CSRF(Cross Site Request Forgery)	2.1	34%	5.5	43%	0.8	10%
잘못된 보안 설정	13.4	91%	14.1	76%	4.1	79%
취약한 암호화 저장	12.0	50%	35.7	76%	4.7	14%
URL 접근 통제 실패	5.5	51%	13.9	6%	1.4	38%
미흡한 전송 계층 보호	10.4	46%	31.0	71%	2.4	27%
무단 리디렉션 및 포워딩	0.4	23%	0.0	0%	0.2	13%

도표 10: 취약점 유형별 보안 테스트 주기, IBM AppScan OnDemand Premium Service(2011년)

단원 4
새로운 보안 추세

이 단원에서는 지금이 투자해야 할 시기가 아닌가 기업들이 고민할 정도로 급속도로 발전하고 있는 기술 분야를 살펴보겠습니다. 또한 신종 기술에서 악성 코드가 어떻게 악용되고 있으며 기업이 집중력을 유지할 수 있는 방법을 설명하겠습니다.

모바일 보안과 기업 – 되짚어 본 한해

모바일 구현 환경과 보안이 거의 모든 기업의 주요 관심사였습니다. 기술 혁신은 효율성의 증가와 거의 모든 비즈니스에 이동성을 이끄는 지속 연결된 업무 환경을 통해 업무 속도를 개선할 수 있게 되자 더 높은 수준의 모바일 환경 도입의 필요성을 절감하게 되었습니다. 한편 확실한 모바일 디바이스 보안 대책은 아직 미진한 실정이지만 꾸준히 개선되고 있습니다.

확실한 모바일 디바이스 보안 대책이 미흡한 실정 때문에 완전히 새로운 개념의 BYOD(Bring-Your-Own-Device) 프로그램을 수용하거나 최소한 지원해야 하는 기업의 고민이 더욱 깊어지고 있습니다. 모바일 디바이스를 개인적으로 구매한 직원들이 늘어나면서 최고 경영진뿐 아니라 직원들 역시 이 프로그램의 발전에 관심을 갖게 되었습니다. 그러나 보안을 우려하여 BYOD 프로그램 도입을 적극 반대하는 CISO가 적지 않습니다.

많은 CISO는 '어떻게'가 아니라 '무조건 안돼'라는 말만 고집하고 있지만 이런 자세는 결국 직원들이 개인적으로 구매한 모바일 디바이스를 사용하기 위해 기존의 인프라를 우회하는 것을 감지 및 차단해야 하는 복잡한 과제만 야기할 것입니다. 물론 이런 상황은 기업에 도움이 될 게 없습니다. 이런 상황에서 취할 수 있는 조치는 데이터 요소 분류에 중점을 두고 모바일 디바이스 사용을 제한적으로 허용하거나 통제하는 것밖에 없습니다.

어떻게 통제할 것인지 고심하는 기업은 데이터 요소와 관련된 기존의 보안 요건을 적절히 분석하여 지원 방안을 검토할 경우 그에 대한 실마리를 찾을 수 있을 것입니다. 이 데이터 중심의 접근법을 통해 기존의 보안 표준을 활용하면 머지않아 가장 이상적인 모바일 보안 대책을 마련할 수 있을 것입니다. 여러 가지 측면에서 봤을 때 이는 컴퓨팅 디바이스를 기반으로 데이터 보안을 확보하는 데 적합한 접근법입니다. 어차피 오늘날의 스마트폰과 태블릿도 컴퓨팅 디바이스입니다.

개인적으로 구매한 모바일 디바이스에 일부 데이터 요소가 저장된다는 점을 고려하면 일부 산업에서는 BYOD 접근법이 적절하지 않을 수도 있습니다. 중요한 것은 데이터에 초점을 맞춰서 지원 방안을 검토한 후 그에 관련하여 필요한 통제 방식을 적용해야 한다는 점입니다.

작년에 모바일 악성 코드에 대한 가시성이 눈에 띄게 개선되었습니다. 기업이 직면한 전반적인 위협 상황을 고려해서 이 모바일 악성 코드 문제를 검토할 필요가 있습니다. 주요 IT 언론 기사에서 빈번히 특정 모바일 디바이스용 악성 코드 공격을 다룬 탓인지 모바일 보안 공격 빈도가 전통적인 Windows XP 위협 상황을 넘어섰다는 믿음이 보편화되기에 이르렀습니다. 물론 이런 믿음은 사실과 전혀 다르지만, 작금의 현실을 비추어 봤을 때 모바일용 악성 코드가 증가하고 있으므로 이 문제를 해결할 견고한 보안 프로그램을 개발해야 한다는 의견이 설득력을 얻을 만합니다.

그렇다고 지난해에 모바일 디바이스용 악성 코드만 증가한 건 아닙니다. 새로운 모바일 관리 솔루션(일반적으로 모바일 디바이스 관리 - Mobile Device Management: MDM - 솔루션으로 통칭) 역시 일주일이 멀다 하고 등장했습니다. 많은 기술 혁신이 모바일 분야에 초점이 맞춰지다 보니 모바일 관리 솔루션의 필요성과 입지가 넓어진 것은 이미 예견된 일이기도 합니다. 선택과 경쟁은 소비자에게 항상 유익한 일이며, 덕분에 기업이 경쟁력 있는 가격에 가장 적합한 모바일 솔루션을 선택하여 필요한 모든 보안 통제 요건을 충족할 가능성도 높아졌습니다. 최근 들어 보안 분리 솔루션 역시 나날이 늘고 있습니다. 이 솔루션은 종종 데이터 유출 방지 솔루션으로 불리기도 하지만 모바일 환경 측면에서 기존의 워크스테이션용 DLP 솔루션과 판이합니다. 이런 솔루션들은 BYOD 프로그램의 일환으로 직원이 개인적으로 소유한 디바이스에 기업용 데이터 및 애플리케이션이 저장되는 문제를 더욱 효과적으로 해결할 수 있다고 장담하지만, 현존하는 대다수 보안 분리 솔루션은 비교적 제한적이고 완성도도 떨어집니다.

모바일 악성 코드 전망

지난해에 모바일용 악성 코드 위협 상황이 변하면서 모바일용 악성 코드가 관심사로 부각했습니다. 그러나 IT 최고 책임자가 실제 기대할 수 있는 적절한 통제 방안을 마련할 수 있음을 인지하게 됐다는 측면에서 이런 상황은 오히려 도움이 되었습니다. IBM은 이미 2011년 상반기 X-Force 동향 및 위험 보고서에서 모바일용 악성 코드 증가를 예측한 바 있습니다.

지난해에 모바일용 악성 코드 위협이 급증하게 된 배경을 언급하고 넘어가는 것도 좋을 듯합니다. 거의 모든 모바일용 악성 코드는 모바일 플랫폼을 다루는 합법적인 앱 스토어에 존재하다가 모바일 디바이스에 전파됩니다. 이는 특정 모바일 플랫폼과 모바일 스토어에 한정된 얘기가 아니라 모든 주요 모바일 플랫폼과 모바일 스토어에 공통적으로 나타난 현상이라는 점에 주목할 필요가 있습니다. 이런 상황은 여러 가지 이유로 중요한 의미가 있습니다. 거의 모든 앱 스토어에서 애플리케이션 다운로드가 증급했지만 고객 사용 소감을 검토해서 얻는 효과는 (아래 소개된 Google 앱 스토어를 제외하고) 예전과 별반 다를 게 없으며 IBM은 최근 들어 이런 상황을 주시하고 있습니다.

또 한 가지 우려되는 현상은 대다수 모바일 디바이스 소유자와 기업 직원들이 합법적인 앱 스토어에서만 애플리케이션을 다운로드하면 악성 애플리케이션의 피해를 입을 우려가 없다고 믿는다는 점입니다. 이는 사실이 아닙니다.

엄밀히 말해서, 인기 있는 앱 스토어 운영업체는 악성 애플리케이션을 적극적으로 찾아서 삭제하지만 이미 많은 사용자가 다운로드한 후라 사후 약방문인 경우가 빈번합니다. 또한 기존의 애플리케이션을 삭제할 수 없는 3자 연계 방식의 앱 스토어는 가급적 이용을 삼가는 것이 바람직합니다. 감시가 소홀할수록 악성 애플리케이션을 접할 가능성이 증가하는 건 당연하기 때문입니다. 수익성이 없다는 이유로 보안 연구소가 앱 스토어 운영업체에 보안 정보를 전달하는 체제는 아직 마련되지 않았습니다. 유감스럽게도 그로 인한 실질적인 피해자는 신뢰할 수 있다는 전제 하에 앱 스토어를 이용하는 일반 사용자와 기업입니다.

보안 솔루션 제공업체는 이런 문제로 고민하는 기업을 돕기 위해 다양한 악성 코드 방지 접근법을 선보이고 있습니다. 초기에만 해도 많은 기업들이 이에 대한 필요성을 간과했지만 모바일용 악성 코드가 꾸준히 늘고 있는데다 악성 코드를 은밀히 지원하는 불법 기업들의 기회는 늘어나는 데 반해, 일반 기업의 위험은 오히려 커지는 현실에 대해 경각심을 느끼는 기업이 늘고 있습니다. 악성 코드 방지 솔루션은 대다수 플랫폼을 지원하며, 경쟁에서 살아남을 플랫폼의 윤곽이 어느 정도 드러남에 따라 플랫폼 보급도 갈수록 쉬워지고 있습니다.

악성 코드 감지 솔루션이 설치되어 있지 않은 경우 디바이스 사용자가 일부 악성 애플리케이션을 알아채지 못할 수 있습니다. 일부 악성 애플리케이션은 사용자가 월별 대금 청구서를 받아본 후에야 깨닫게 되는 사기 거래를 실시할 용도로 유포되므로 절대 간과해서는 안 됩니다. PC용 악성 코드와 마찬가지로 공격자가 주로 노리는 것은 금전적 이득이므로 SMS를 지원하는 모바일 디바이스는 대단히 매력적인 표적이 될 수밖에 없습니다.

(일반적으로 음성, 메시지 전송 및 데이터 서비스와 함께 GPS 하드웨어가 탑재되기 때문에) 모바일 디바이스는 위치 저장, 메시지, 이메일, 음성 통화를 비롯한 사용자의 다양한 행동 패턴을 모니터링해서 공격자에게 전송하는 스파이 애플리케이션의 존재를 감지하고 있습니다. 이런 방식의 공격은 개인용 컴퓨터에서도 나타나고 있는 현상과 유사하기 때문에 특히 우려할만합니다. 더군다나 모바일 디바이스가 명실공히 '손안에 있는 사무실'로 자리잡았기 때문에 스파이 애플리케이션의 공격 수법이 날로 진화할 것으로 예상됩니다.

최근에 Google은 자사의 앱 스토어에 업로드 및 유지되는 애플리케이션에 대해 보안 감시 프로세스를 시작하는 애플리케이션 검사 기능을 구현했다고 발표한 바 있습니다. Google의 행보는 앱 스토어에 존재하는 애플리케이션에 대한 획기적인 보안 개선 조치이자 다른 앱 스토어 운영업체가 따를만한 선례가 된다는 점에서 특히 주목할 만합니다. Google이 새로 구현한 기능은 아직 개선해야 할 점이 많고 Google과 악성 애플리케이션을 유포하려는 사람들 간의 끝없는 암투가 계속될 것으로 예상되지만 사용자를 악성 애플리케이션으로부터 보호하겠다는 선전포고인 것만은 분명합니다. 다른 앱 스토어 소유업체/운영업체가 Google의 선례를 따를 것인지는 좀 더 지켜봐야 할 문제입니다.

모바일용 악성 코드와 관련하여 주시해야 할 위험 분야는 모바일 운영체제 버전입니다. 기본적인 플랫폼 취약점으로 말미암아 모바일 운영체제에서 자가 복제되는 대대적인 악성 코드 공격이 발생한 적은 아직 없으나 이런 우려가 현실이 되는 건 시간 문제일 뿐인데 일부 플랫폼은 다른 플랫폼에 비해 이런 문제를 해소하기 유리한 구조입니다. 순수하게 기업의 견지에서 현존하는 거의 모든 모바일 디바이스 관리(MDM) 솔루션은 운영체제 버전을 토대로 기업 정보 동기화를 제어할 수 있는 능력을 지원하므로 기업이 취약점이 패치되지 않은 운영체제 버전에 대한 지원을 중단할 수 있습니다. 그로 인해 (이 분야의 계약 구조에 따라 기업이 제공하는 프로그램처럼 디바이스 모델과 통신사가 제대로 관리되지 않는 탓에 BYOD 프로그램에 참여하는) 기업 직원들이 통신사와 이런 지원 문제로 생기는 갈등의 직접적인 피해를 입을 가능성이 높습니다. 머지않아 기업 내부에서 지원을 받지 못한 채 취약점이 방치되는 디바이스 때문에 직원과 모바일 디바이스 소유자가 난처한 입장에 처하게 될 것이며, 보조금을 지원 받는 현재 모델의 의무 사용 기간이 끝나기도 전에 새 디바이스로 업그레이드하는 것이 유일한 대안이 될 것입니다.

하드웨어 OEM이 디바이스 소유자가 가급적 자주 새 디바이스로 업그레이드하도록 유도하기 위해 디바이스의 취약점을 의도적으로 방치하고 있다고 의심하는 사람이 많습니다. 이런 특별한 문제는 랩탑과 같은 다른 보급형 소비자 컴퓨팅 디바이스 모델의 사정과 사뭇 다르기 때문에 이를 수용해야 하는 소비자의 불만이 폭발할 날이 올지도 모르겠습니다.

BYOD와 보안 분리 솔루션

앞서 언급했듯이 2011년에 눈에 띄었던 전개 양상 중 하나는 기업용 애플리케이션 및 데이터를 직원의 개인 애플리케이션 및 데이터와 분리하는 방안에 대한 관심이 고조됐다는 점입니다. 이런 양상이 전개되는 데는 많은 관심과 공감을 얻은 BYOD(Bring-Your-Own-Device) 프로그램도 크게 한몫 했습니다. 일부 솔루션은 전년도에도 존재했지만 기능과 유용성에 제약이 있어서 거의 관심을 끌지 못했습니다. 전년도에 비해 2011년에는 이 분야의 솔루션들이 우후죽순으로 늘었습니다. 대다수 솔루션은 아직 걸음마 수준이며 각기 다른 제약, 미흡한 유용성, 그리고 구현 문제를 안고 있지만 보안 분리 솔루션들이 속속 등장하고 있다는 것은 업계에서 전반적으로 이런 문제와 기업 고객이 필요로 하는 바를 인식하고 있다는 의미로 받아들여도 좋을 듯싶습니다. 관련 기업이 대단히 한정적이고 직원들의 모바일 디바이스를 파악할 수 있는 데이터 부재로 인해 보안 분리 솔루션이 특정 산업에서만 사용되는 틈새 시장으로 인식됐던 전년도에 비하면 이는 괄목할만한 진전입니다.

이 시장 부문이 성숙기로 접어들고 꾸준히 개선되고 있으므로 이제는 이 분야의 솔루션을 두 범주로 구분해야 할 시점이라고 여겨집니다. Android 분야에서는 하드웨어 기반의 가상화 기술을 이용하는 방식에 대한 활발한 활동과 공동 연구가 이뤄지고 있습니다. 가상화 기술은 칩 수준의 기능에 광범위하게 채택된 점 외에는 아직 이렇다 할 진전이 없는 실정인데, 굴지의 다국적 기업들이 사용하기 적합한 기술로 자리잡으려면 그에 상응하는 보급률과 더불어 다양한 통신사를 통해 전 세계에서 사용되고 있는 엄청나게 다양한 모바일 디바이스를 지원하는 일이 선행돼야 합니다. 이런 일이 실제로 각국에서 실현되려면 앞으로도 24개월~36개월은 지나야 할 것으로 전망되지만 칩 제조업체, 하드웨어 OEM, 그리고 통신사가 기업들의 요구사항과 그에 상응하는 시장 기회를 인식하면서 눈에 띄는 진전을 보이고 있는 것만은 분명합니다. 이 접근법이 대기업의 BYOD 프로그램에 이용하기 적합할 정도로 보편화될지는 좀 더 지켜볼 일입니다.

한편 컨테이너, 가상 컨테이너 혹은 자산 관리 기술을 통해 보안 분리를 구현하는 다양한 솔루션들이 얼리 어댑터를 위해 미흡한 부분을 채워주고 있습니다. 이런 기술들은 기업이 디바이스 전체를 지속적으로 통제하지 않고서도 직원들의 디바이스에 적용할 수 있는 일정 수준의 통제와 보안 분리 기능을 별도로 지원하지만 보안 분리 솔루션용 호스트로 믿고 사용하려면 디바이스 수준에서 어떤 통제가 필요한지 적극 파악해야 한다는 과제가 여전히 남아 있습니다. 앞서 언급한 가상화 기술에도 동일한 우려가 있지만 애플리케이션 컨테이너나 보안 분리 기술은 모바일 운영체제와 동일한 상황에서도 악성 코드나 악성 애플리케이션이 출현했을 때 위험 부담이 더 큽니다. 이 분야 역시 아직 표준이 정의되지 않았지만 기업이 보안 분리 솔루션을 도입하고 필요한 보안 기술 테스트를 수행하는 추세라 조만간 적절한 표준이 등장할 것으로 전망됩니다.

역할 중심의 업무 환경에서 디바이스 관리 통합의 중요성

기업 내부에서 기업 소유 혹은 직원 개인 소유의 모바일 디바이스나 이 두 가지를 모두 사용하는 사용자가 폭발적으로 증가함에 따라 기업의 위험 관리 차원에서 모바일 디바이스를 관리하는 일이 갈수록 중요해지고 있습니다. 모바일 디바이스 보급률이 랩탑과 같은 다른 컴퓨팅 디바이스에 필적한 수준에 올랐기 때문에 더 더욱 그렇습니다. 게다가 랩탑, 태블릿 및 스마트폰 사용자 대 디바이스 비율이 직원당 2~3대가 될 날도 머지않은 듯합니다. 결과적으로 기업 데이터의 분산이 더욱 심화되어 역할 중심의 보호 프로파일과 기업 위험 관리 체제를 활용하는 데 어려움이 가중될 것으로 전망됩니다.

기업들이 특정 사용자 역할과 관련된 데이터의 유형과 역할에 따라 맞춤화한 역할 중심의 사용자 보호 프로파일을 활용하는 방안을 강구하고 있지만 여러 가지 디바이스 관리 솔루션을 사용하면 디바이스 관리가 분산될 수밖에 없기 때문에 이런 접근법에는 갈수록 어려움이 따르게 될 것입니다.

실제로 기업들이 자체 개발한 컴퓨팅 프로그램에 의존하는 만능형(one-size-fits-all) 프로그램에서 탈피하여 BYOD 프로그램에 공통적으로 사용되는 보다 다양한 운영체제 플랫폼을 관리하는 방식에 관심을 돌리고 있습니다. 따라서 조만간 단일 플랫폼으로 디바이스 관리를 통합하여 합리적인 비용 범위 내에서 BYOD를 실현할 수 있을 것으로 전망됩니다. 그러나 비교적 규모가 작은 기업은 대다수 직원을 기준으로 동일한 범주 데이터의 역할과 용도로의 세분화가 미흡해서 이런 접근법을 기피할 지 모르겠습니다. 규모가 작은 기업은 두 가지 솔루션(아마도 표준 컴퓨팅 인프라용 솔루션과 스마트폰과 태블릿 같은 모바일 인프라용 솔루션)만으로도 그럭저럭 문제를 해결할 수 있지만 대기업은 두 가지 솔루션만으로는 극심한 제약이 따르기 때문에 만족할만할 성과를 얻기 어려울 것입니다.

예를 들어, 기업이 유독 민감한 계약, 고객 혹은 프로젝트가 요구하는 가장 높은 수준의 보안을 충족하려면 모바일 디바이스 및 표준 디바이스를 비롯한 모든 자산의 보안을 확보해야 하는데 직원들에 의해 사용되는 각기 다른 종류의 디바이스에 대해 다양한 역할 중심의 정책을 효과적으로 구현하지 못할 수 있습니다. 결국, 다양한 역할에 필요한 효율성과 고성능 최신 디바이스 지원 능력이 미흡한 경우, 모든 엔드포인트 디바이스를 관리할 수 있는 일원화된 플랫폼이 필요한 것입니다.

모든 엔드포인트 디바이스 관리를 일원화해야 하는 두 번째 이유는 포괄적 모니터링 능력과 기업 위험 관리의 필요성 때문입니다. 이기종 관리 시스템을 단일 위험 관리 콘솔에 통합하려고 시도해 보는 것도 불가능한 건 아니지만 단일 프레임워크 기술이 통합 모니터링과 기업 위험 관리를 지원한다면 성능 가능성은 훨씬 높아집니다. 게다가 이런 단일 플랫폼은 APT(Advanced Persistent Threat) 분석 및 대응 구조에 통합하기도 훨씬 더 쉽습니다.

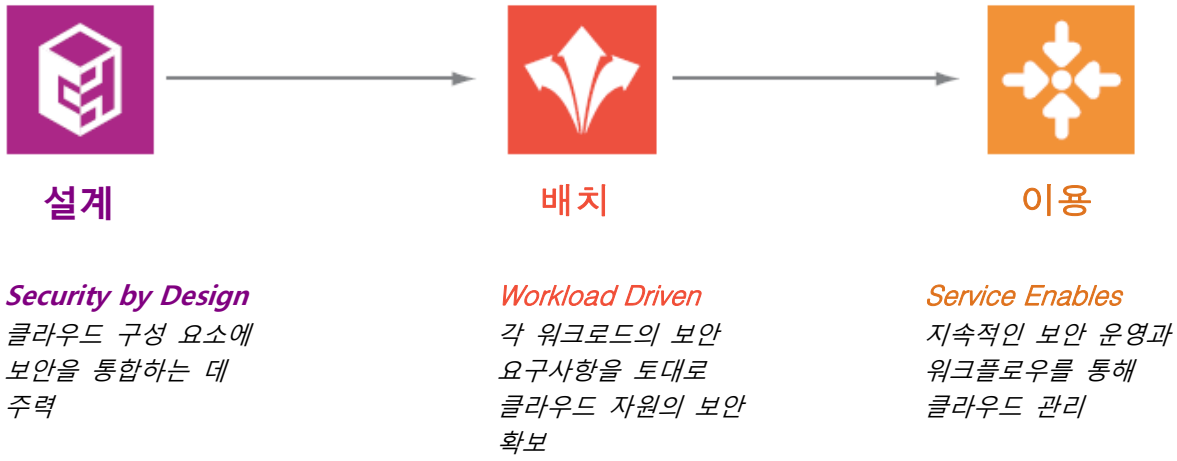
기본적으로, APT를 우려하여 폐쇄적 감지/ 대응 환경을 구현하려는 대다수 기업은 보안 운영 상황 분석 작업과 분석 기술에 엔드포인트 상태, 정보, 엔드포인트 시스템의 실시간 소통 능력을 통합해야 합니다. 엔드포인트 사용자를 고려하여 기업 전역의 보안 상황을 개선할 수 있는 효율성과 감시 체제를 구축함과 동시에 적절한 보안 관리 기술을 선택한다면, 효과적으로 규정 및 통제되는 보안 정책을 적용하여 계획에 따라 일관적으로 모든 엔드포인트를 관리하기가 수월해질 것입니다.

클라우드의 보안 상태 고찰

클라우드 환경의 보안 상태에 대해 많은 논란이 있는 가운데 기업들은 클라우드 솔루션을 도입하고 그에 대한 보안을 확보하는 방안에 대한 해답을 모색하고 있습니다. 점점 더 많은 기업들이 클라우드를 도입하는 데 관심을 기울이고 있기 때문에 보안은 가장 시급히 해결해야 할 사안입니다. 많은 기업들은 여전히 비즈니스-크리티컬 애플리케이션을 퍼블릭 클라우드로 이전하기를 주저해서 프라이빗 클라우드를 그 대안으로 선택하고 있습니다. 이런 현상은 비즈니스-크리티컬 애플리케이션을 인터넷이란 새로운 네트워크로 이전하기를 주저하고 그 대신 (흔히 전용선을 기반으로 하는) 사설 네트워크에 의존했던 인터넷 초창기와 유사합니다. 규모의 경제로 인해 결국 기업들이 어쩔 수 없이 대다수 비즈니스-크리티컬 애플리케이션이 인터넷으로 이전했던 것과 마찬가지로 클라우드 컴퓨팅에서 같은 현상이 나타나고 있습니다. 문제는 클라우드가 훨씬 더 안전한가가 아니라 클라우드 환경에서 위험을 해소하고 보안을 확보하려면 구체적으로 어떤 통제 환경과 비즈니스 프로세스에 관심을 기울여야 하는가에 있습니다. 널리 보급된 클라우드 기반의 인프라를 도입하는 방안을 고려 중인 조직이라면 보안 및 위험 최소화를 위해 맡아야 할 조직의 역할과 클라우드 서비스 제공업체의 역할을 이해하는 것이 중요합니다.

비즈니스-크리티컬 애플리케이션이나 서비스를 이용하는 기업은 자사의 위험 부담과 서비스 제공업체의 정책 및 절차를 적절히 조율해야 합니다. 새로운 인터넷 기술을 도입할 때는 모범적인 보안 지침을 따라야 하는데 클라우드 컴퓨팅 역시 전혀 다를 게 없습니다.

클라우드 환경 배치할 때는 모든 배치 단계에서 보안을 고려하는 것이 바람직합니다.



클라우드의 보안 선택

많은 기업들이 가질만한 한 가지 의문은 클라우드 기반의 애플리케이션 및 서비스가 전통적인 인터넷 및 인트라넷 애플리케이션보다 안전한가 하는 점입니다. 클라우드 기반의 배치 환경이 더 안전하다는 구체적인 자료는 없지만 클라우드 기반 환경을 배치할 때 보안에 더 많은 관심을 쏟게 된다는 것이 공통적인 견해입니다. 그리고 애플리케이션이나 서비스가 자사의 신뢰 영역(trust boundary) 내에 배치되기 때문에 기업이 더 안전하다고 느끼는 경우가 많습니다. 보안 애플리케이션 및 서비스 계약서에 보안에 관한 내용이 삽입되거나 설령 보안에 대해 논의를 한다고 해서 저절로 보안이 강화되는 건 당연히 아니지만, 클라우드 배치를 고려할 때 보안이 가장 중대한 사안이라 보안 애플리케이션 및 서비스 계약서에 보다 엄격한 보안 통제, 프로세스 및 프로시저에 대한 요구사항이 명시되는 건 흔히 볼 수 있습니다.

설계 단계의 고려사항

보안 개발 절차를 정해서 준수해야 합니다. 클라우드 애플리케이션 제공업체의 서비스를 이용하려는 경우 그 업체의 보안 개발 기준과 절차가 자사의 요구사항을 충족하는지 확인하는 것이 급선무입니다.

적절한 애플리케이션 및 엔드포인트 보안 대책이 마련돼야 합니다. 다시 말해서, 멀티 테넌트(multi-tenant) 클라우드 환경에서는 적절한 보안 환경과 데이터 분리 프로세스가 배치되지 않은 상태로 민감하고 중요한 애플리케이션이 동일한 하이퍼바이저를 공유하지 않도록 해야 합니다.

데이터 보안 요건을 파악하는 일 역시 중요합니다. 민감한 개인 정보를 이용하는 애플리케이션에는 일반적으로 기업, 정부, 그리고 적용 가능한 표준 및 규정이 요구하는 엄격한 보안 요건이 적용돼야 합니다. 따라서 클라우드 서비스 제공업체를 선정할 때 그 업체가 이런 사안을 충족하는지 확인해야 합니다.

배치 단계의 고려사항

물리적 엔드포인트를 관리하는 방식과 동일하게 가상 엔드포인트를 관리해야 합니다. 패치 및 설정 관리 측면에서 일관적이지 못한 보안 때문에 가상 라이브러리와 카탈로그에 문제가 발생하지 않도록 유의해야 합니다.

클라우드 환경과 물리적 환경에 일관적인 보안 통제 정책을 시행해야 합니다. 가상 환경, 그 중에서도 특히 기본적인 보안 통제가 미흡하기 쉬운 개발 및 테스트 환경에 배치된 애플리케이션에도 공공 인터넷 애플리케이션과 동일한 보안 조사를 실시해야 합니다.

모든 클라우드 애플리케이션을 정기적으로 검사해야 합니다. 그리고 소스 코드 분석과 동적 분석 서비스를 활용하여 클라우드에 배치된 모든 애플리케이션의 보안 노출을 최소화하는 것이 바람직합니다.

이용 단계의 고려사항

적절한 ID 및 접근: 클라우드 서비스 제공업체의 서비스형 소프트웨어(SaaS)를 도입한 경우 ID 및 접근 권한 지정 방식을 시행하고 ID를 통합하는 방안을 고려해야 합니다.

로그 및 보안 이벤트 관리: 가상 이벤트에 대한 로그 및 보안 이벤트를 효과적으로 관리해야 합니다.

데이터 포렌식(Forensic): 클라우드 서비스 제공업체를 선정할 때는 보안 사고 발생 시 그 업체가 어떻게 데이터 포렌식을 관리하는지 확인해야 합니다.

보다 우수한 보안을 확보하고 클라우드 기반의 인프라로 이전하는 데 수반되는 위험 부담을 최소화하는 데 가장 적합한 방법은 '설계 단계부터 보안을 고려하는 접근법(secure-by-design)'입니다. 클라우드로 이전하는 방안이 많은 IT 기업의 관심사로 떠올랐으며 통제력 미흡 때문에 보안에 대한 문제가 더욱 중시되고 있습니다. 또한 완벽하게 통제할 수 없는 환경의 보안을 확보하는 데 따르는 문제를 해소하려는 다각적인 노력이 고조되면서 보안이 향상되고 있습니다. 인프라에 대한 투명성이 미흡하다는 클라우드 환경의 단점이 오히려 보안 향상이라는 결실로 이어질 수 있습니다.

SLA를 통해 클라우드 보안 개선

개요

2011년은 클라우드 환경의 데이터 침해 사고로 얼룩진 한 해였습니다. 다수의 대기업들이 데이터 침해 사고를 당하면서 수백만 명의 고객 기록이 노출되는 피해를 입은 것입니다. 2011년 1사분기에는 한 굴지의 클라우드 서비스 제공업체에서 발생한 데이터 침해 사고가 소매업체와 금융기관의 고객 데이터베이스까지 연쇄 반응을 유발하면서 고객의 금융 거래 기록이 노출되는 불상사가 발생하기도 했습니다. 급기야 IBM X-Force는 2011년을 '보안 침해의 해'로 명명했으며 많은 기업들은 클라우드 컴퓨팅이 합리적인 수준의 보안을 보장할 수 있는가에 대해 의문을 갖기에 이르렀습니다.

클라우드 컴퓨팅의 보안은 단순히 계약 관리 문제를 떠나 클라우드 도입의 성공 여부를 판가름하는 중요한 변수가 될 수 있습니다. 표준 계약서와 서비스 약관은 일반적으로 클라우드 서비스 제공업체의 이익을 대변해서 기본 서비스를 정의하고 데이터 노출에 따른 법적 책임을 제한하는 데 목적을 두고 있습니다. 클라우드 서비스 제공업체가 기업 고객의 필요사항을 수행할 목적으로 표준 계약서를 수정하는 경우는 지극히 드뭅니다. 서비스 수준 합의서(SLA)는 그에 비해 좀 더 유연해서 기업 고객이 자사의 사업 방침, 법적 요건 및 규제 요건 혹은 기타 고려사항에 따라 요구사항을 정할 수 있습니다. 그러나 유감스럽게 클라우드 컴퓨팅의 본질인 유연성, 확장성, 그리고 신속한 배치 능력 때문에 중요한 SLA를 작성해서 유지하기가 대단히 어렵습니다.

고려해야 할 문제

기업이 현실적으로 클라우드 컴퓨팅 환경에 대해 행사할 수 있는 영향력이 한정되어 있기 때문에 가장 효과적인 정보 보안 관리 수단은 SLA를 활용하는 것입니다. 따라서 기업은 사전 대책을 강구하고 가급적 장기적인 관점에서 클라우드 컴퓨팅 프로젝트를 바라보는 자세를 취할 필요가 있습니다. 그런데도 단기적 관점을 고수하고 수명 주기 관리와 사업 철수 계획을 간과한 채 서비스 제공업체 선정과 서비스 착수에만 관심을 기울이는 얼리 어댑터가 너무나도 많습니다.

복구(Resiliency)는 대다수 클라우드 SLA의 핵심 사안이자 일부 클라우드 서비스 제공업체가 서비스 표준 약관의 중점 사안으로 다루는 항목입니다. 여기서 말하는 복구란 가동시간, 성능 및 응답 시간, 장애 조치 시간 등의 보증을 의미합니다. 일부 클라우드 서비스 제공업체는 멀티 테넌트 환경의 분할 및 격리와 같은 문제나 변경 관리 정책 및 프로시저를 복구 조항에 포함시키기도 합니다. 그러나 표준 SLA에는 정보 보안에 대해 일반적인 표현만 포함되어 있는 것이 일반적입니다. 그러므로 기업은 표준 서비스로 제공되는 정책, 프로시저 및 통제 수단을 꼼꼼히 살펴보고 처리, 전송 또는 저장될 데이터로 인해 생성되는 자사의 워크로드를 고려한 요구 조건을 클라우드 서비스 제공업체에 제시해야 합니다.

기업은 장기적으로 효과적인 정보 보안 관리를 위해 다음과 같은 사항을 고려해서 SLA를 작성해야 합니다.

- **소유권:** 기업은 민감하거나 중요한 데이터, 프로세스 혹은 지적 재산을 클라우드 서비스 제공업체에게 맡기기 전에 클라우드 서비스 제공업체의 표준 계약서, 서비스 약관, SLA 외에도, 애플리케이션, 기능성, 데이터 세트 혹은 클라우드 서비스 이용으로 파생되는 관련 작업 성과물에 대한 공동 소유권이나 완전한 소유권 규정이 명시된 기타 문서를 꼼꼼히 검토해야 합니다. 또한 클라우드 서비스 제공업체에게 자사가 노출하는 데이터나 자산에 대한 소유권이 유지된다는 내용을 서면으로 작성해야 합니다. 그래야만 필요한 경우 다른 클라우드 서비스 제공업체에게 그 자산을 이전하거나 자사로 회수할 수 있습니다. 이는 클라우드 기반의 XaaS(Anything-as-a-Service)을 이용하는 기업에게 특히 중요합니다. 기업이 프로젝트를 사내에 구현하거나 다른 클라우드 서비스 제공업체에게 이전하려는 경우 기존에 계약한 클라우드 서비스 제공업체의 독점 소프트웨어 및 프로세스는 이전하기 어려울 수 있습니다. 그런데 기업이 서비스 조건으로 그 자산에 대한 부분적 혹은 전체적 권리를 포기할 경우 어려운 상황이 더 복잡해질 수 있으므로 유의해야 합니다.
- **접근 관리:** 기업이 민감하거나 중대한 사내 데이터에 대한 사용자의 접근을 제한하듯이 클라우드 환경에 배치된 접근 관리 정책 및 메커니즘을 관리해야 합니다. 기업의 데이터에 대한 구체적인 접근 관리 요건은 클라우드 서비스 제공업체 직원이 각 워크로드의 특성에 맞게 정해야 합니다. 하지만 기업 역시 클라우드 서비스 제공업체의 실 운영 환경에 최소 권한 원칙이 어떻게 적용되고 있는지 대체로 알고 있어야 합니다. 퍼블릭 클라우드의 멀티 테넌트(multi-tenancy) 환경에서 이는 절대적으로 중요합니다. 공유형 호스팅 환경에 각 테넌트를 분리해서 배치하는 일 못지않게, 기업 고객에게 서비스를 제공하는 직무를 맡은 클라우드 서비스 제공업체의 기술 인력에 한하여 (타당한 정도 내에서) 접근을 허용하는 일도 중요합니다. 접근 허용 방식은 클라우드 서비스 제공업체의 사업 방침에 따라 다르겠지만 기업은 클라우드 서비스 제공업체가 테넌트 환경 및 데이터에 대한 물리적 접근, 논리적 접근, 원격 접근, 그리고 비상 접근 조건을 정확히 어떻게 관리하고 있는지 반드시 알아야 합니다. 또한 기업은 워크로드의 데이터에 대한 법적 요건 및 규제 사항을 심사하여 클라우드 서비스 제공업체가 이런 요건들을 충족할 수 있는지 확인하고 클라우드 서비스 제공업체가 이를 위해 최선을 다하고 있다는 믿을만한 증거를 확보해야 합니다. 클라우드 환경의 접근 관리에 대해서는 다음 절에서 좀 더 거론하겠습니다.
- 거버넌스: 정보 보안 체제 및 보안 능력에 대한 클라우드 서비스 제공업체의 설명은 기업이 워크로드에 적합한 클라우드 유형과 클라우드 서비스 제공업체를 선택할 때 고려하는 핵심 요인입니다. 기업은 클라우드 서비스 제공업체가 정보 보안 능력과 관련한 공개용 문서(공개용으로 편집한 감사 보고서나 요약 자료(예: SSAE 16 SOC 2 보고서 혹은 SOC 3 문서), 인증서(예: 운영 환경에 대한 ISO 27001 인증서) 또는 컴플라이언스 표준(예: BITS Shared Assessments AUP 또는 COBIT)에 준한 기타 문서를 검토해야 합니다. 그리고 기업은 법적 요건 및 규제 사항을 충족하는지 확인하는 데 필요한 그와 같은 문서를 클라우드 서비스 제공업체에 요청해야 합니다. 또한 기업은 SLA를 작성할 때 클라우드 서비스 제공업체와 다음과 같은 사항을 협상해야 합니다.
  - 기술 인력의 보안 교육 및 보안 의식 검증
  - 테넌트 환경과 직결되는 로깅 및 모니터링 정보에 대한 접근 권한
  - 데이터 침해 사고가 발생한 경우 보안 책임 및 법적 책임 명문화 - 작성하는 SLA가 복수인 경우 이 항목이 특히 중요합니다.

  - 법률 집행에 따른 소비자 통지 및 조사 목적으로 데이터 침해 사고와 관련된 포렌식 정보에 대한 접근
  - 정보, 조사, 소환 등에 대한 법 집행기관의 요구에 클라우드 서비스 제공업체가 어떻게 대응할 것인지 명시한 문서

- 계약 철회: 대다수 클라우드 서비스 제공업체의 표준 계약서와 서비스 약관에는 클라우드 서비스 제공업체 입장(예: 대금 미납)과 고객의 입장(가동시간 보증 위반)에서 합법적 이유로 계약을 철회할 수 있는 조항이 명시됩니다. 이외에도 기업은 기타 계약 위반 조건이 명시된 이와 같은 표준 문건을 면밀히 검토하고 클라우드 서비스 제공업체에 의해 제공되는 서비스의 내용 변화, 클라우드 서비스 제공업체의 능력 변화, 클라우드 서비스 제공업체의 사업 방침 변화 또는 단순한 클라우드 프로젝트 실패에 대비하여 확실한 계약 철회 계획을 세워둬야 합니다. 또한 기업은 다음과 같은 경우 부당하게 불이익을 당하지 않고 클라우드 서비스 제공업체와의 계약을 철회할 수 있는 합리적 권리를 가져야 합니다.
  - 클라우드 서비스 제공업체의 사업 방침 변화(예: 적법한 고지 절차를 거치지 않거나 실사 기회를 주지 않은 채 다른 SLA 추가)
  - 클라우드 서비스 제공업체의 소유권 변화(예: 인수 합병)
  - 적법한 고지 절차를 거치지 않은 채 상당한 이용료 변화
  - 적법한 고지 절차를 거치지 않은 채 서비스 철회 또는 상당한 서비스 변화

기업은 계약을 철회해야 할 경우 가상 인프라 이전 계획을 시행할 수 있도록 충분한 시간을 갖고 클라우드 서비스 계약 철회 대책을 세워둬야 합니다. 물론 이를 위해서는 기업의 이전 계획 명문화가 선행돼야 합니다. 인프라 이전 이유는 워크로드, 클라우드 유형, 그리고 서비스 품질에 따라 달라질 수 있지만 기대에 훨씬 못 미치는 비용 절감 효과, 외부 위탁 상황에서 관리하기 벅찬 프로젝트, 제품 또는 서비스의 자체적 문제 등 다양한 이유로 클라우드 배치 프로젝트가 실패로 돌아갈 수 있습니다. 그 이유야 무엇이든, 기업은 다른 서비스 제공업체로 프로젝트를 이전하거나 인프라를 사내로 다시 회수해야 할 경우에 대비한 계약 철회 계획을 세워야 합니다. 이전 계획서에는 다음과 같은 내용이 포함돼야 합니다.

- 클라우드 서비스 제공업체에게 제시할 목적으로 명문화한 계약 철회 이유
- 원래 기능 또는 서비스를 즉시 이용할 수 있도록 설계되지 않은 경우에 대비하여 인프라 이전에 걸리는 충분한 시간
- 클라우드 서비스 제공업체로부터 기업이 회수할 데이터의 형식과 이전 방법 등의 이전 지원 사항
- 백업 데이터를 비롯하여 기업 소유의 모든 데이터 및 자산 회수 방안
- 백업 데이터를 비롯하여 클라우드 환경에 잔존하는 데이터의 안전한 폐기 및/또는 처분
- 데이터 암호화로 말미암은 복잡성에 대한 대책

물론, 지금까지 언급한 내용은 기업이 고려해야 할 광범위한 문제의 일부에 지나지 않습니다. 워크로드에 대한 구체적인 필요사항을 파악하면 가장 적절한 유형의 클라우드(퍼블릭, 프라이빗, 하이브리드 또는 관리형)와 가장 적합한 클라우드 서비스 제공업체를 선택할 수 있습니다. 기업이 고려해야 할 사안은 배치하는 클라우드 모델의 종류에 따라 달라집니다. 예를 들어, 기업이 관리형 프라이빗 클라우드를 배치하려는 경우 멀티 테넌트 환경 분리는 고려해야 할 사안이 아닙니다. 그러나 일반적으로 일부 문제는 대단히 중요한데도 간과하기 일쑤인데, 클라우드 배치 환경을 효과적으로 관리하려면 이런 문제에 대비한 계획 및 명문화가 반드시 필요합니다.

결론

클라우드 컴퓨팅이 단순한 신종 기술에서 탈피하여 대세로 자리잡아 가면서 2013년 말까지 급성장이 예상됩니다. 클라우드 기술을 초기에 채용한 기업들로부터 소중한 교훈, 특히 정보 보안에 관한 교훈을 얻고 있습니다. 클라우드 컴퓨팅 프로젝트를 장기적 관점에서 계획하고 워크로드에 따라 서비스 및 보안 요건을 면밀히 검토하는 기업은 적절한 클라우드 모델과 클라우드 서비스 제공업체를 선택할 수 있습니다.

확실하고 적절하게 SLA를 협상하는 일은 클라우드 컴퓨팅 프로젝트 성공에 결정적인 역할을 할 뿐더러 계약하는 두 기업 모두에게 이롭습니다. 이를 위해서는 계획을 철저히 세우고 협상의 여지가 없는 '싫으면 말고 식'의 표준 계약서를 지양해야 합니다. 클라우드 서비스 제공업체가 SLA 협상에 소극적인 태도를 보일 경우 차라리 다른 업체를 찾는 것이 나을 수도 있습니다. SLA는 계약 기간과 범위가 구체적으로 명시되고 적절한 통지를 통해서만 수정이 가능하며 조직의 구체적인 비즈니스 및 정보 보안 요건을 이해할 수 있다는 점에서 진짜 계약서나 다름없습니다. SLA는 수동적 수단으로 여겨질 수 있지만 외부에 위탁한 클라우드 환경의 보안 상태를 관리 및 유지하는 데 가장 효과적인 방법이 될 수도 있습니다.

클라우드의 계정 및 접근 관리

클라우드 환경의 보안 과제

클라우드 컴퓨팅이 유연성, 비용 효율성, 그리고 확장이 용이한 '주문형' 모델 덕분에 갈수록 많은 인기를 모으고 있습니다. 여러 부서, 협력업체, 그리고 고객과 서비스 및 정보를 공유할 수 있다는 점이 클라우드 컴퓨팅의 주요 장점입니다. 게다가 클라우드 컴퓨팅은 사용자 경험을 개선하면서도 복잡성이 가중되지 않습니다. 따라서 사용자가 기본 기술이나 구현에 대해 아무것도 알아야 할 필요가 없습니다.

클라우드 컴퓨팅의 장점은 명확하지만 클라우드 구현을 위해 적절한 보안 환경을 구축할 필요가 있습니다. 클라우드 컴퓨팅을 도입하거나 도입을 고려 중인 기업이 갈수록 늘고 있지만 그에 수반되는 보안 위험에 대한 우려의 목소리도 만만치 않습니다. IBM의 기업가치연구소(Institute for Business Value)가 글로벌 위험 설문 조사(Global Risk Survey)를 실시한 결과, 고객들은 클라우드 컴퓨팅의 데이터 접근, 이용 및 통제 방식에 대해 심각하게 우려하고 있는 것으로 확인되었습니다. 실제로 77%의 응답자는 클라우드 컴퓨팅을 도입하면 개인정보를 보호하기가 더 어려워진다고 생각하고 50%의 응답자는 개인정보 침해나 유출에 대해 우려하고 있으며 23%의 응답자는 기업 네트워크 보안 약화가 염려된다고 답했습니다.

데이터와 애플리케이션이 공공 영역에서 운용되는 경우가 빈번해서 접근 관리가 우려를 낳고 있습니다. '클라우드 컴퓨팅이 데이터 센터만큼 안전할까? 데이터 센터나 프라이빗 클라우드와 연계해서 클라우드 서비스를 이용하며 어떨까? 민감한 데이터와 애플리케이션에 인증 받은 사람만 접근한다고 어떻게 장담하지? 클라우드 서비스 제공업체가 과연 산업 및 정부 규제 준수 사실을 증명할 감사 보고서를 제공할 수 있을까?' 이런 질문으로 생각해낼 수 있는 문제들을 해소하는 일이 성공적인 클라우드 보안의 열쇠입니다.

기업은 전통적인 데이터 센터, 프라이빗 클라우드 또는 퍼블릭 클라우드에 존재하는 주요 자원의 보호, 개인정보 보호, 거버넌스 및 접근 방법에 대한 균형을 유지해야 합니다. 클라우드 컴퓨팅은 무단 접근, 데이터 유출 및 기타 노출로부터 자원을 보호해야 할 필요성과 자원을 공유해야 할 필요성 간의 섬세한 균형을 필요로 합니다. 자사의 민감한 정보나 애플리케이션에 부적합한 사람이 접근하는 걸 용납할 기업은 없을 것입니다. 기업의 IT 자원이 어디에 존재하든 그 자원을 항상 보호하려면 반드시 계정 및 접근 관리 기술을 클라우드 아키텍처에 도입해야 합니다.

클라우드 보안에 필요한 사항을 간과해서는 안 되며, 이전을 시작한 이후에야 그 중요성을 강조하는 게 아니라 전반적인 클라우드 구현 계획에 미리 반영해야 합니다. 클라우드 보안은 단순히 기술만 필요로 하는 게 아니기 때문에, 필요한 경우 클라우드 구현 계획에 따라 비즈니스 프로세스 및 정책을 수정해야 합니다. 전통적인 보안 환경과 마찬가지로 기업은 비즈니스 목표와 규제 요건을 충족하도록 안전한 클라우드 환경의 보안 과제를 명문화하여 실천에 옮겨야 합니다. 보안 과제로는 클라우드 서비스 제공업체와 SLA 작성, 다양한 클라우드 사용자 그룹에 필요한 임무 분할, 그리고 동일한 물리적 하드웨어를 공유하는 다른 클라우드 고객으로부터 자사의 데이터를 격리하는 신뢰 영역(trust zone) 구현 등이 있습니다.

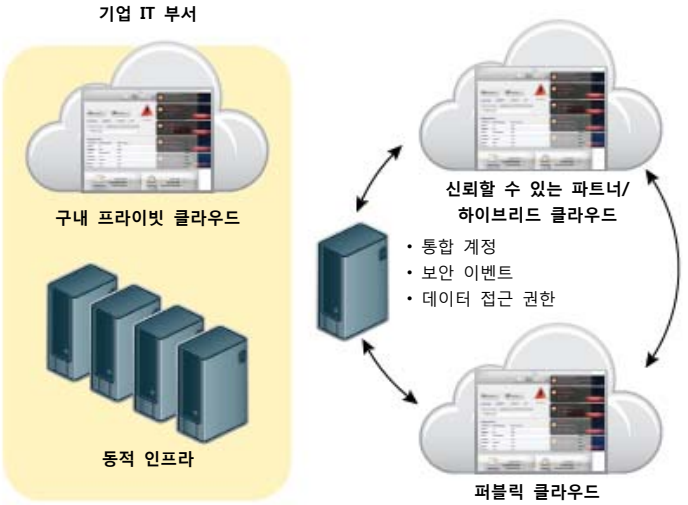
클라우드용 계정 및 접근 관리(IAM) 솔루션

클라우드로 이전하기로 결정한 애플리케이션이나 정보가 무엇이든, 우수한 계정 및 접근 관리(IAM) 솔루션은 나침반 역할을 할 수 있습니다. IAM 솔루션은 클라우드 컴퓨팅 환경과 전통적인 컴퓨팅 환경을 통합 관리하므로 두 가지 유형의 인증서를 각기 별도로 관리할 필요가 없습니다. IAM 솔루션의 주된 목적은 인증 받은 사용자가 필요할 때 언제든 애플리케이션, 데이터 및 도구를 이용할 수 있게 하면서 무단 접근을 차단하는 것입니다. IAM 솔루션은 인증 받은 적법한 사용자로 접근을 제한하기 때문에 클라우드 보안 계획에 반드시 포함되어야 할 요소입니다.

IAM 솔루션을 이용하면 누구에게, 어떤 정보를, 언제, 어느 곳에서, 그리고 정해진 시간 동안 얼마나 자주 접근을 허용할 것인지에 대한 정책을 설정해서 적용할 수 있습니다. 또한 IAM 솔루션을 이용하면 정해진 기간이 지나면 사업자 접근 권한을 재확인하여 필요한 경우 즉시 접근 권한을 취소할 수 있습니다. 그 밖에도 IAM 솔루션은 사전 예방 차원에서 정책 위반을 모니터링, 보고 및 방지하는 데도 효과적입니다.

전통적인 IT 환경과 마찬가지로 우수한 클라우드용 IAM 솔루션은 사용자 환경 구현(예: 업무 분할, 역할 기준의 접근 통제, 세부적 사용자 접근 권한 설정), 비밀번호 관리, 웹 및 통합 SSO(Single Sign-On), 로깅, 감사 보고서 작성 등의 기능을 겸비하고 있습니다. 뿐만 아니라 내부자가 고의나 부주의로 막대한 피해를 유발할 수 있기 때문에 계정 권한 관리는 특히 중요합니다.

클라우드 기반의 애플리케이션과 서비스의 접근 보안



계정 및 접근 관리(IAM) 솔루션을 이용하면 외부 업체가 운영하는 salesforce.com과 같은 클라우드 기반 서비스에 대한 수많은 사용자의 접근을 중앙 집중식으로 통제할 수 있습니다.

클라우드 환경에서는 직원, 고객 및 협력업체 등으로 구성된 대규모 사용자 커뮤니티가 각기 다른 보안 수준의 외부 장소에서 서비스, 애플리케이션, 그리고 자원을 공유할 수 있습니다. 기업이 클라우드 기반의 애플리케이션을 사내 애플리케이션과 통합하면 사용자가 SSO(Single Sign-On)를 이용하여 손쉽게 애플리케이션을 이용할 수 있습니다. 인증 방식을 기업의 백엔드 시스템 및 타사 시스템에 맞춰 조율하려면 계정 통합과 신속한 통합 기능이 필요합니다. 통합 계정 관리는 클라우드와 전통적인 컴퓨팅 인프라에서 계정과 접근을 관리하는 기술입니다. 또한 통합 계정 관리는 클라우드의 셀프 서비스 환경을 효율적으로 구축하는 데 유용합니다. 그 밖에도 사내에서 운용하는 애플리케이션 및 클라우드에 대한 최종 사용자의 로그온 과정을 효율화하여 최종 사용자가 손쉽고 빠르게 클라우드 서비스를 이용할 수 있도록 표준 기반의 SSO 기능을 갖춰야 합니다.

일반적으로 사용자 인증은 클라우드 외부에서 이뤄집니다. 그리고 인증이 완료되면 사용자 계정이 클라우드에 연결되는데 전체 프로세스는 사용자에게 나타납니다. SSO 기능을 이용하면 클라우드에서 계정을 따로 관리할 필요 없이 사용자가 직접 클라우드 기반의 애플리케이션과 정보로 이동할 수 있습니다.

기업이 컴플라이언스를 충족하려면 전사적 능력을 갖춰서 효과적인 인증 방식으로 내부 및 외부 접근을 통제하고, 인증 및 네트워크 트래픽을 모니터링하며, 다각적인 감사 및 보고 기능으로 시스템을 지원할 수 있어야 합니다. IAM 솔루션은 사용자가 누구든 보안 대책의 미흡한 부분을 보완함으로써 보안을 개선합니다. IAM 솔루션은 사기, 지적 자산 절도 또는 고객 정보 유출과 같은 위협을 최소화하고 사용자에게 자원 접근 권한을 부여하는 비즈니스 및 IT 프로세스를 능률화함으로써 비용을 절감하는 데 효과적입니다.

요약하자면, IAM 솔루션은 사용자 생산성 증대와 보안 침해 위험 최소화라는 유형의 운영 이득을 선사합니다. 자동화된 IAM 솔루션은 클라우드 보안 문제를 해결하고 클라우드 환경과 전통적인 컴퓨팅 환경을 통합할 수 있습니다. 끝.

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
March 2012

WGL03012-USEN-00