IBM X-Force 2012년 동향 및 위험 보고서

2013년 3월

도움주신 분들

X-Force 동향 및 위험 보고서는 많은 IBM 직원들의 도움으로 얻은 결실입니다.
이 보고서의 발간을 위해 깊은 관심과 헌신을 보여 주신 다음 분들께 심심한 감사를 표합니다.

도움주신 분	직책
Andrew Franklin	사고 대응 분석 선임 연구원, IBM 프로페셔널 서비스
Brad Sherrill	IBM X-Force 데이터베이스팀 관리자
Bryan Ivey	MSS 사이버 위협 및 정보 분석가, 팀장
Carsten Hagemann	IBM X-Force 소프트웨어 엔지니어, 컨텐츠 보안
Cynthia Schneider	IBM 보안 시스템, 기술 편집자
David McMillen	IBM 보안 서비스, 보안 정보 분석가
David Merrill	STSM, IBM 보안 솔루션, CISA
Jens Thamm 박사	데이터베이스 관리 컨텐츠 보안
Gina Stefanelli	IBM X-Force 마케팅 관리자
Jason Kravitz	IBM 보안 시스템 Techline 전문가
Jay Bretzmann	WW 시장 세그먼트 관리자
John Kuhn	IBM 보안 서비스 위협 분석 선임 연구원
Larry Oliver	선임 사이버 위협/보안 정보 분석가
Leslie Horacek	IBM X-Force 위협 대응 관리자
Marc Noske	데이터베이스 관리, 컨텐츠 보안
Mark E. Wallis	IBM 보안 시스템, 선임 정보 개발자
Mark Yason	IBM X-Force 선임 연구원
Michael Montecillo	MSS(Managed Security Services) 위협 연구 및 정보 분석 팀장
Ralf Iffert	IBM X-Force 컨텐츠 보안 관리자
Randy Stone	계약 리드, IBM 비상 대응 서비스(ERS)
Robert Freeman	IBM X-Force 선임 연구 관리자
Robert Lelewski	계약 리드, IBM 비상 대응 서비스(ERS)
Scott Craig	IBM 보안 서비스, 데이터 정보 팀장
Scott Moore	IBM X-Force 소프트웨어 개발자 겸 IBM X-Force 데이터베이스 팀장
Veronica Shelley	신원 및 액세스 관리 세그먼트 마케팅 관리자

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 보안 협업

IBM 보안에는 광범위한 보안 역량을 제공하는 다양한 브랜드가 포함되어 있습니다.

- IBM X-Force 연구개발팀은 광범위한 컴퓨터 보안 위협, 취약점, 최근 동향과 공격자의 수법을 조사, 분석, 모니터링하고 기록하며, 그 외의 IBM 팀은 여기서 얻어진 풍부한 데이터를 이용하여 고객을 위한 보호 기술을 개발하는 데 주력하고 있습니다.
- IBM X-Force 컨텐츠 보안 팀은 크롤링(crawling) 및 자체 조사, IBM MSS(Managed Security Service)가 제공하는 정보를 활용하여 인터넷을 독자적으로 조사하고 안전 수준을 분류합니다.
- IBM MSS는 고객의 엔드포인트, 서버(웹 서버 포함), 일반 네트워크 인프라와 관련된 공격 행위를 감시하는 업무를 담당하고 있습니다. MSS는 웹, 이메일 및 인스턴트 메시지 등의 다양한 경로를 통해 이뤄지는 공격 사례를 추적합니다.
- IBM PSS(Professional Security Service)는 효과적인 정보 보안 솔루션을 구축할 수 있도록 전사적인 보안 평가, 설계 및 설치 컨설팅 서비스를 제공합니다.

목차

목차

개요

지난 한 해 동안 IT 보안 분야에는 여러 가지 주요 사건이 있었습니다. Flame과 같이 위협적인 이름의 정교한 툴킷의 발견에서부터 여러 플랫폼에 걸친 제로 데이(zero-day) 취약점에 이르기까지, 소비자와 기업은 새로운 위협에 대한 수없이 많은 경고와 경보를 접했습니다. 이미 2011년에 사상 최고치를 기록한 데이터 유출 및 사고의 빈도는 지속적으로 증가했습니다.

2012년 상반기 보고서에서는 상반기에 나타난 공격자 및 보안 침해 사고의 폭발적인 증가 추세가 지속될 것으로 예측한 바 있습니다. 그리고 실제로 예측한 상황이 발생했습니다.

정교한 공격 및 광범위한 분산 서비스 거부 공격(DDoS) 시도에 관한 기사는 2012년의 헤드라인을 장식했으며, 상당수의 침해 사고는 SQL 인젝션과 같이 이미 검증된 기법을 통해 이루어졌습니다. 여전히 명확한 점은, 운영의 정교함에 상관없이 공격자들은 목적을 달성하기 위해 계속해서 가장 쉬운 방법으로 접근할 것이라는 점입니다.

모바일 디바이스를 기업에 통합하는 작업은 여전히 어려운 과제입니다. 이전 보고서에서는 모바일 디바이스의 사용을 지원하기 위해 엄격한 정책 및 거버넌스가 구성되지 않은 상태에서 BYOD 프로그램을 구현할 경우의 위험성과 유해성을 살펴보았습니다. 또한, 최근의 개발을 통해 이러한 위험이 여전히 존재하고 있으며, 2014년까지는 모바일 디바이스의 보안을 기존 사용자 컴퓨팅 디바이스의 보안보다 강화해야 한다는 것이 밝혀졌습니다.

이러한 예측은 표면적으로는 설득력이 없는 것처럼 보일 수 있지만, 보안 통제 동향 및 식견을 갖춘 보안 관리자가 관련 시장에 주장하고 있는 요구사항을 근거로 하고 있습니다. 이번 보고서에서는 보안 관리자가 주장하고 있는 직원 소유의 디바이스에서의 개인 환경 또는 역할 분리에 대해 살펴봅니다. 또한, 현재 진행 중인 안전한 소프트웨어 모바일 애플리케이션 개발 이니셔티브에 대해 논의합니다.

일반 사용자 시스템에 대한 악성코드의 배포 및 설치는 악성코드 배포 및 설치를 목적으로 개발된 웹 브라우저 공격 키트를 이용하면서 크게 증가했습니다. 공격 키트는 2006년에 처음으로 등장하기 시작했으며, 공격 키트 개발자는 다수의 시스템에 악성코드를 설치하려는 공격자에게 공격 키트를 제공하거나 판매했습니다. 공격 키트는 일반 사용자 시스템에 악성코드를 설치하는 데 즉시 이용할 수 있는 턴키 솔루션을 공격자에게 제공하므로, 꾸준히 널리 이용되고 있습니다.

Java 취약점은 공격 키트의 주요 목표가 되었으며 공격자는 신뢰할 수 있는 공격, 샌드박스를 이용하지 않은 코드 실행 및 다양한 운영 체제를 이용한 여러 플랫폼에서의 이용가능성이라는 Java와 관련된 세 가지 주요 요소를 이용했습니다. Java 공격은 2012년에 주요 공격 대상이 되었으며, IBM X-Force는 이러한 공격 활동이 2013년까지 지속될 것으로 예상하고 있습니다.

2012년 상반기 보고서 내용에 따르면, 2012년에도 스팸의 양은 거의 일정하게 유지되었으며, 스팸 발송 국가 1위는 인도인 것으로 나타났지만, 스팸의 특성은 변화하고 있습니다. 광범위한 대상의 피싱 사기(phishing scam) 및 더욱 개인화된 스피어 피싱(spear phishing)은 합법적인 비즈니스로 위장한 간교한 소셜 엔지니어링 이메일 메시지를 이용해 끊임없이 일반 사용자를 속이고 있습니다. 또한, 고객이 일반적으로 수신하는 정식 메시지인 것처럼 보이도록 공격자들이 메시지를 정교하게 꾸미기 때문에 은행 업무 관련 거짓 경보 및 거짓 패키지 제공 서비스 이메일에 속는 경우가 자주 발생하고 있습니다. 공격 대상이 개인인지 기업인지의 여부에 상관없이, 많은 수의 침해 사고는 보안 기본사항 및 정책이 제대로 적용되지 않아 발생했으며 약간의 기본적인 보안 예방책을 실시함으로써 이러한 사고를 예방할 수 있다는 것을 다시 한 번 명심하시기 바랍니다.

가장 많이 노출된 취약점들 중에서 웹 애플리케이션은 여전히 1위를 기록하고 있으며, 2012년에는 2011년 말 수치에 비해 14% 증가했습니다. 2012년 상반기 보고서에 따르면, XSS(cross-site scripting)는 대중에 공개된 모든 취약점 중 53%를 차지했습니다. SQL 인젝션 공격 방식이 1위의 공격 기법으로 기록되었지만, 실질적으로 새롭게 공개된 SQL 인젝션 취약점은 2010년의 절정기에 비하면 그 수가 줄었습니다.

소셜 미디어는 의사소통에 대한 새로운 방법을 통해 개인적인 생활 방식 또는 업무 방식을 변화시키고 있습니다. 이와 같이 개인에 대한 정보를 지속적으로 이용 가능함에 따라서, 공격자는 공격 활동에 이용하기 위한 데이터에 쉽게 접근할 수 있게 되었습니다. 현재, 소셜 프로필에 개인 신상 정보를 공개하는 직원은 그 어느 때보다 공격의 대상이 될 가능성이 큽니다.

2012년 상반기 이후부터 2012년 말까지 상황이 어떻게 변했는지 자세히 살펴보겠습니다.

2012년 하이라이트

위협

악성코드 및 악성 웹사이트

- 2012년에는 거의 매일 개인정보 유출 피해자에 대한 소식이 트위터 및 다른 소셜 미디어를 통해 보도되었습니다. 공개된 사이트에서 이메일 주소, 비밀번호(암호화된 비밀번호 및 일반 텍스트 비밀번호), 심지어는 주민등록번호와 같은 개인 신상 정보를 확인할 수 있었습니다. (10 페이지)
- 2012년 데이터를 기준으로, 상용규격 도구 및 기법을 통해 광범위한 대상을 공격하는 방식으로 대부분의 보안 사고가 발생했다는 점은 놀라운 사실이 아닙니다. 이러한 공격의 원인은 공격 툴킷이 공개적으로 광범위하게 보급된 점과 인터넷에 존재하는 수많은 웹 애플리케이션의 취약점 때문인 것으로 판단됩니다. (12 페이지)
- 2012년 한 해 동안, 은행 업계를 대상으로 정치적인 동기를 지닌 이슈가 될만한 DDoS 공격이 끊임없이 발생했습니다. 은행 업계를 대상으로 한 DDoS 공격과 관련하여 흥미로운 사실은, 이러한 공격이 높은 대역폭을 갖는 데이터 센터에 존재하는 손상된 웹 서버에 봇넷을 구현함으로써 이루어졌다는 점입니다.[1] 이러한 수법을 통해 일반 가정의 PC보다 훨씬 높은 연결 시간 및 대역폭을 이용해 공격을 실행할 수 있었습니다. (14 페이지)
- 2012년에 발생한 보안 사고 사례 중 미국에서 가장 많은 사고가 발생했으며, 이는 46%를 차지했습니다. 영국에서는 전체 사고 중 8%가 발생하여 2위를 기록했으며, 호주와 인도는 3%로 공동 3위를 기록했습니다. (16 페이지)
- IBM MSS(Managed Security Services) 보안 사고 동향은 전 세계의 보안 현황을 나타내는 지표입니다. 다양한 경보의 상대적인 양을 확인하여 공격이 어떻게 이루어지고 실행되는지 설명할 수 있습니다. IBM MSS 보안 사고 동향은 공격 방식이 어떻게 전개되어 왔는지에 대한 정보를 제공하기도 합니다. IBM MSS 보안 사고 동향을 기준으로, 2012년의 주안점은 매우 광범위한 인터넷 경로를 통해 실행된 대규모의 조직적인 공격을 이용한 시스템 공격이었다고 할 수 있습니다. (20 페이지)

1 http://threatpost.com/en_us/blogs/bank-ddos-attacks-using-compromised-web-servers-bots-011113

- IBM MSS는 SQL 인젝션 기반의 트래픽이 지속적으로 급격하게 증가한 사실을 확인했으며, 이는 대부분 아시아 태평양 지역에서의 꾸준한 영향 때문입니다. 이러한 경보는 모든 산업 분야에서 발생했으며, 은행 및 금융 분야는 그 빈도가 더 높았습니다. (23 페이지)
- 공격 팩(exploit pack)으로도 알려져 있는 웹 브라우저 공격 키트는 일반 사용자 시스템에 악성코드를 설치한다는 한 가지 특정한 목적을 가지고 개발된 것입니다. 2012년에는 웹 브라우저 공격 키트 개발 및 활동이 급증했으며, 이러한 활동의 1차적인 대상은 Java 취약점이었습니다. 본 보고서에서는 향후의 공격에 대비하기 위한 전략 및 정보를 제공합니다. (31 페이지)
- Java는 지속적으로 공격의 주요 대상이 되고 있습니다. Java는 여러 브라우저 및 플랫폼에서 이용할 수 있다는 장점을 가지고 있지만, 동시에 공격자에게 비용 대비 큰 효과를 제공하기도 합니다. (35 페이지)

웹 컨텐츠 동향, 스팸 및 피싱

웹 컨텐츠 동향

- 가장 많이 이용되는 웹사이트는 IPv6 지원 가능 상태로 배치되지만, 공격자들은 아직까지는 IPv6를 대규모 공격의 대상으로 삼지 않고 있습니다. (38 페이지)
- 전체 웹 액세스 중 3분의 1은 사용자가 웹 애플리케이션 및 소셜 미디어 등의 컨텐츠를 제출할 수 있도록 허용하는 웹사이트를 통해 이루어집니다. (40 페이지)
- 관련 웹사이트의 거의 50%는 현재 소셜 네트워크 플랫폼과 연계되어 있으며, 소셜 네트워크의 급속한 확산은 기밀 정보의 공유를 통제해야 하는 기업에 새로운 과제로 대두되고 있습니다. (42 페이지)

스팸 및 피싱

- 2012년에 스팸의 양은 거의 일정하게 유지되었습니다. (43 페이지)
- 인도는 2012년 가을에 전체 스팸의 20% 이상을 발송하여, 여전히 스팸 발송 국가 1위를 차지했습니다. 인도에 이어, 미국이 2012년 하반기에 발송된 전체 스팸의 8% 이상을 발송하여 2위를 기록했습니다. 상위 5개 스팸 발송 국가에는 인도와 미국에 이어 베트남, 페루, 스페인이 포함되었습니다. (47 페이지)
- 2012년 말, IBM은 기존의 스팸은 후퇴하고 있으며 악성 첨부 파일이 포함된 사기 메일 및 스팸 메일이 증가하고 있다고 보고했습니다. 또한, 공격자들은 봇넷 근절에도 불구하고 복원 능력을 보이고 있으며, 이로 인해 스팸은 중단되지 않고 계속 발송되고 있습니다. (49 페이지)

운영 보안 현황

취약점 및 공격

- 2012년에는 8,168개의 취약점이 대중에 공개되었습니다. 2012년 상반기 데이터를 검토한 후 예상했던 수준의 기록은 아니지만, 이는 2011년 대비 14% 증가한 수치입니다. (50 페이지)
- 2011년에 2,921건이 공개되었던 웹 애플리케이션 취약점은 2012년에 3,511건으로 14% 증가했습니다. XSS(Cross-site scripting) 취약점은 2012년에 공개된 모든 웹 애플리케이션 취약점 중 절반 이상을 차지했습니다. (51 페이지)
- XSS는 공개된 웹 취약점 중 대부분을 차지했습니다. 대중에 공개된 모든 웹 애플리케이션 취약점 중 53%가 XSS와 관련된 취약점이었습니다. 이러한 높은 비율은 전례가 없는 높은 수치입니다. XSS 발생이 극적으로 증가하는 한편, SQL 인젝션 취약점은 2011년보다 증가했지만 2010년에 비하면 크게 약화되었습니다. (52 페이지)
- 2012년에는 3,436건의 공개적인 공격이 있었습니다. 이는 전체 취약점 수의 42%를 차지하며, 2011년에 비해 4% 증가한 수치입니다. (54 페이지)

- 웹 브라우저 취약점의 수는 2012년에 약간 감소했지만 문서 포맷 문제만큼 높은 수준은 아니었습니다. 웹 브라우저 취약점의 전반적인 수는 2011년에 비해 6% 밖에 감소하지 않았지만, 심각도가 "심각" 또는 "높음"인 웹 브라우저 취약점은 한 해 동안 59% 증가했습니다. (59 페이지)
- 소셜 미디어만큼 의사소통 방식에 영향을 미친 혁신적인 사건은 거의 없었습니다. 그러나 각 개인 간에 대규모 상호연결과 지속적인 연락이 가능해짐에 따라 정보 수집 기능의 새로운 취약점 및 근본적인 전환이 결과적으로, 공격자 및 보안 전문가 모두에게 더 많은 활동을 할 수 있도록 유용한 정보를 제공했습니다. (74 페이지)
- 공격자는 특정한 기업을 개별적인 개체로 보는 대신 기업을 개인들의 집합으로서 볼 수 있게 되었습니다. 이러한 시각은 공격자에게 기업 인프라 또는 애플리케이션이 아닌 특정한 사람들을 공격 대상으로 삼을 수 있는 기회를 제공합니다. 또한, 공격 대상이 된 사람들은 단순한 직원이 아닌 개인으로서 표적이 될 수도 있습니다. 즉, 직원들의 개인적인 활동 및 일상을 이용해 기업을 공격의 대상으로 삼을 수 있게 되었습니다. (77 페이지)

새로운 보안 추세

모바일

- **전망:** 2014년까지 모바일 컴퓨팅 디바이스의 보안을 기존의 사용자 컴퓨팅 디바이스 보안보다 강화해야 합니다. 이러한 예측은 IBM의 기술 동향 전망의 일환으로, 확실한 예측입니다. 또한 표면적으로는 설득력이 없는 것처럼 보일 수 있지만, 보안 통제 동향 및 식견을 갖춘 보안 관리자가 관련 시장에 주장하고 있는 요구사항을 근거로 하고 있습니다. (85 페이지)
- 개인 환경 또는 역할의 분리: 소수의 기업만이 가상화된 데스크톱 솔루션을 이용하여 기업용 애플리케이션과 데이터를 개인 소유 디바이스에서 분리시켜 BYOD를 해결해 왔지만, 더 많은 수의 기업은 모바일 디바이스에서 개인 환경(persona)을 분리하거나 이중으로 개인 환경을 구성하기 위한 방법을 필요로 하거나 요구해 왔습니다. 사용 방식이나 도입에 있어서의 이러한 차이점은 개인 소유 모바일 디바이스의 수가 훨씬 많아 위험이 발생할 확률이 BYOD 프로그램으로 관리되는 개인 소유 PC에 비해 더 높기 때문일 수 있습니다. (88 페이지)
- 많은 기업은 SSDLC(Secure Software Development Life Cycle) 프로세스 구현을 위해 상당한 투자를 해왔습니다. 오늘날의 모바일 애플리케이션 개발은 SSDLC 프로세스를 도입하여 많은 이점을 얻을 수 있습니다. 자격 취득 또는 프로덕션 단계에서 개발이 이루어지는 대신, SSDLC 프로세스의 일부로 안전한 개발을 지원하기 위한 도구가 이용됩니다. 결과적으로, 더 많은 기업은 기존의 레거시 애플리케이션에 비해 더욱 안전하게 애플리케이션을 개발하게 될 것입니다. 취약점이 공개되지 않은 기존의 일부 컴퓨팅 애플리케이션은 더 이상 사용되지 않을 수도 있고, 기존의 버전은 도태되고, 새롭고 더욱 안전하게 개발된 대체 애플리케이션으로 교체될 것입니다. (90 페이지)
- 2012년 동안 이전에 비해 더 많은 기업이 BYOD 또는 개인 소유 디바이스의 사용을 지지했다고 결론을 내려도 무방할 것입니다. 지난 2년 동안, IBM Security는 전 세계적인 고객사 2,000곳 중 수백 곳의 고객사와 논의했으며, 이들 중 오직 세 곳만이 어떠한 종류의 BYOD 프로그램도 실행할 계획이 없다고 답했습니다. (91 페이지)

단원 I 위협

이 단원에서는 위협과 관련한 주제를 살펴보고 기업 보안 전문가들이 경험하게 되는 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 대한 새로운 정보를 제공합니다.

보안 사고의 거센 물결

보안 침해 사고는 지난 몇 년간 IBM X-Force 팀의 가장 중점적인 논의 주제 중 하나였습니다. 전자상거래와 소셜 네트워크 관련 거대 기업에서부터 의료 업체, 대학, 은행, 정부 및 게이머에 이르기까지, 2012년에 발생한 보안 침해 대상의 범위는 매우 광범위했습니다. IBM은 2011년을 "보안 침해의 해"로 선언했으며, 그 이유는 기록된 데이터 손실 사고의 발생 수가 그 당시 최고 수준에 이르렀기 때문이었습니다. Open Security Foundation은 2011년에 개인식별정보의 손실, 도난 및 노출 사고가 1,088건[2] 발생했다고 보고했습니다. 2012년에는 1,502건의 사고가 기록되었으며 이는 거의 40% 정도 증가한 수치입니다.

2012년에는 거의 매일 개인정보 유출 피해자에 대한 소식이 트위터 및 다른 소셜 미디어를 통해 보도되었습니다. 공개된 사이트에서 이메일 주소, 비밀번호(암호화된 비밀번호 및 일반 텍스트 비밀번호), 심지어는 주민등록번호와 같은 개인 신상 정보를 확인할 수 있었습니다. 어떻게 하여 이러한 상황이 발생했는지 자세히 살펴보겠습니다.

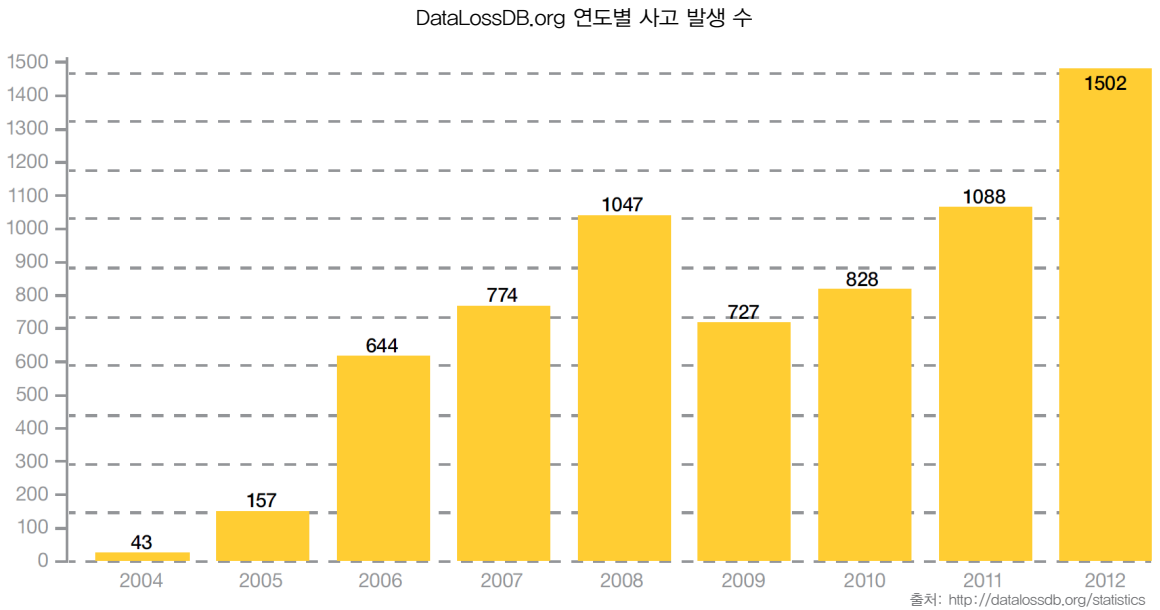


그림 1: DataLossDB.org 연도별 사고 발생 수 – 출처: Open Security Foundation/DataLossDB.org http://datalossdb.org/statistics

2010년 초, Google은 몇 개월 동안 지속되어 온 자사 기업 네트워크에 대한 공격을 공개했습니다. "오퍼레이션 오로라(Operation Aurora)"로 명명된 이러한 공격은 과학적인 증거를 통해 정교한 수준이라는 것이 밝혀졌으며 이는 특정 국가에서 지원하는 공격이었을 가능성을 나타냈습니다. 곧, 다른 기업들도 자사 네트워크에서 이와 유사한 공격 패턴이 감지되었다고 주장하기 시작했습니다. APT(Advanced Persistent Threat)라는 용어는 이전부터 제한적으로 이용되어 왔지만, 이제는 흔히 사용되고 있으며 때로는 지나치게 자주 사용되고 있습니다. APT라는 용어는 일반적으로 개인, 조직, 정부 기관 또는 기업에 대한 민감한 정보를 획득하기 위한 일련의 복잡한 공격을 의미하며 오랫동안 이 공격이 지속되는 경우가 많습니다. 예전에는 이러한 공격을 기술적인 면에서 매우 진보된 공격으로 간주했지만 시간이 지나면서 이러한 관점이 발전하여 현재, APT는 운영적인 정교함을 이용한 공격이며 필요한 경우에는 제로 데이(zero-day) 공격 및 신종 맞춤식 악성코드를 이용하는 것으로 파악되고 있습니다.

이렇게 지능적인 유형의 공격은 지속적으로 발생하고 있습니다. 2013년 초, 뉴욕 타임즈 및 월 스트리트 저널과 같은 몇몇 주요 미디어는 연속된 복잡한 공격으로 인해 보안 침해가 발생했다고 보고했습니다. 이 경우에도, 특정 국가가 이 공격 활동을 지원했다는 의견이 있었습니다. 그러나 이러한 사이버 스파이 시나리오가 큰 화제가 될 수는 있지만, 전체적인 보안 침해 사고의 양으로 볼 때는 전체 사고에서 적은 비중을 차지하고 있습니다.

정교함의 다양화

IBM의 2011년 상반기 보고서에서 IBM X-Force는 공격 목표 및 정교함의 수준에 따라 공격자를 분류했습니다. 어떤 공격자는 가능한 한 가장 광범위한 범위의 대상을 선택할 수도 있습니다. APT와 관련해 언급되는 공격자와 같은 다른 공격자들은 특정한 대상 네트워크 및 대상 기관 또는 인물을 신중하게 선택할 수도 있습니다.

2012년의 공격자 유형 및 기법

그림 2: 2012년의 공격자 유형 및 기법

이용된 취약점 및 공격 유형과 같은 공개된 사고 정보를 살펴보면, 2012년에 공개된 대부분의 보안 사고는 그림 2에서 좌측 상단의 사분면에 속한다는 것을 알 수 있으며, 이러한 공격자는 상용규격의 도구 및 기법을 이용하여 광범위한 대상에 공격을 실행합니다. 이는 공격 툴킷의 공개적인 광범위한 보급 및 인터넷에 존재하는 웹 애플리케이션의 수많은 취약점 때문인 것으로 판단됩니다.

그림 3에 나타난 것과 같이, SQL 인젝션(SQLi)은 웹사이트에서 데이터를 추출하기 위해 지속적으로 가장 많이 이용되는 진입점으로 기록되고 있습니다. 개방형 워크프레임, CMS 시스템 및 부속 플러그인에 SQLi 취약점의 수가 많으면 공격자는 자동화된 스크립트를 효과적으로 이용해 대상 웹사이트를 검색할 수 있습니다.

또한, 공격자는 웹 애플리케이션 취약점을 악용해 합법적인 웹사이트에 악성 스크립트 및 실행 파일을 주입할 수 있으며, 이는 Internet Explorer 및 Java와 같은 클라이언트 측의 브라우저 코어 및 플러그인 취약점을 대상으로 합니다.

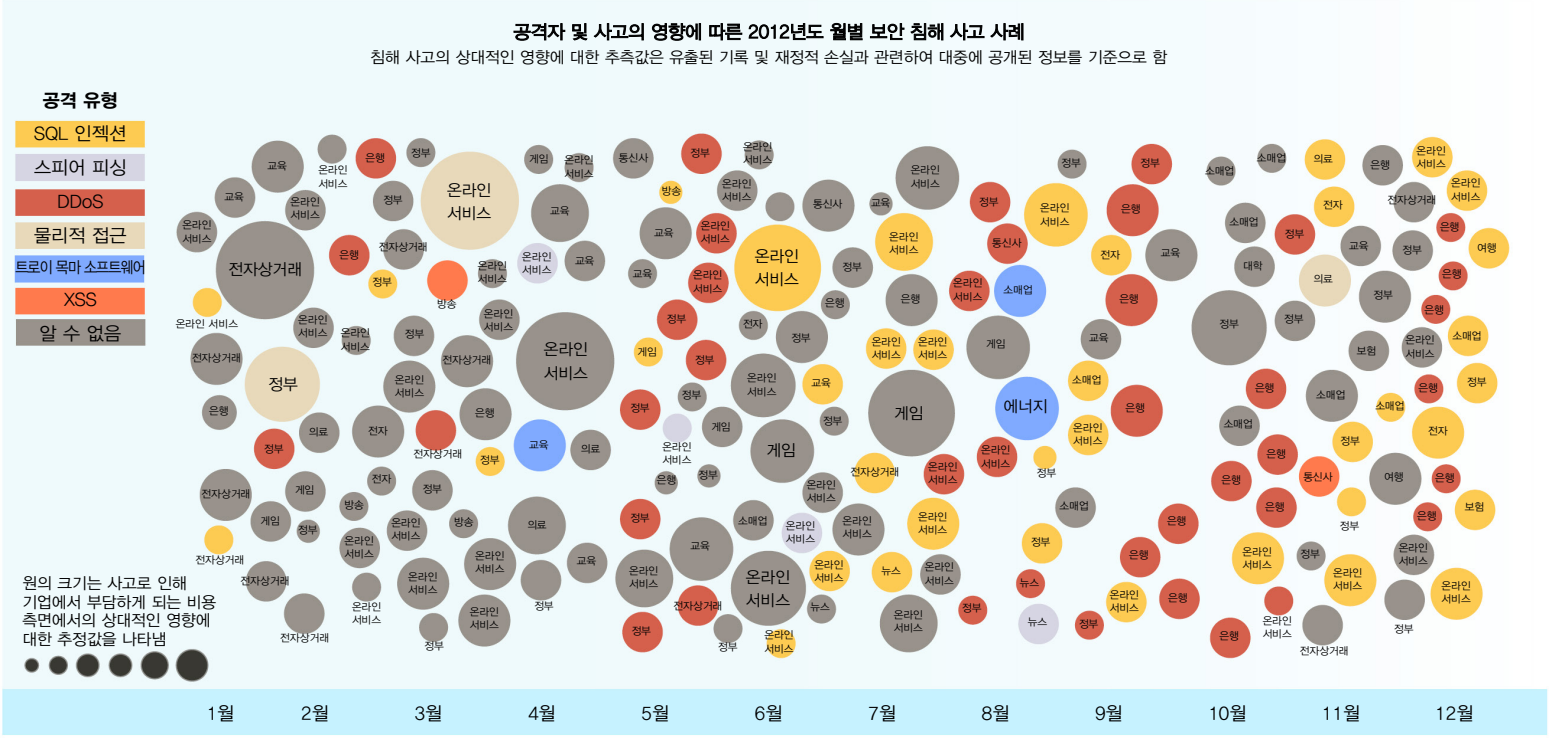


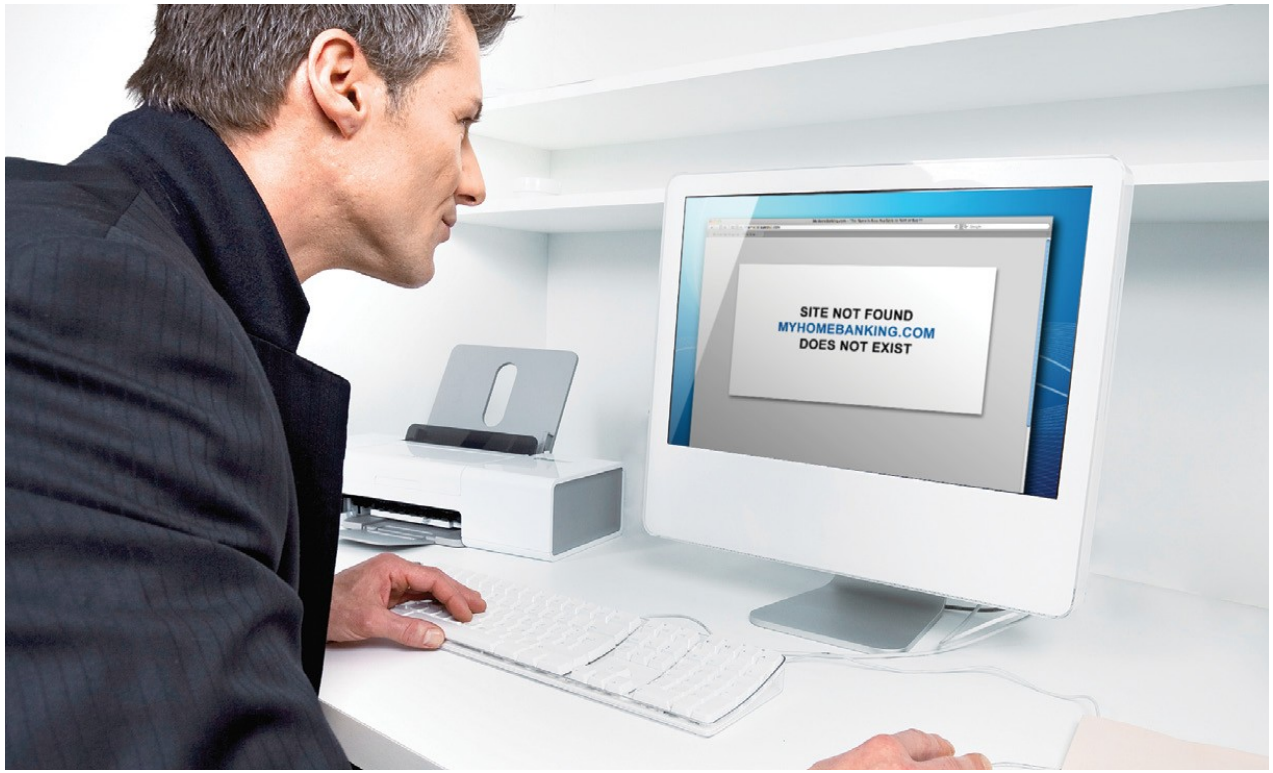
그림 3: 공격자 및 사고의 영향에 따른 2012년도 월별 보안 침해 사고 사례

보안 기본사항 및 DDoS

공개된 침해 사고 사례를 심도 있게 살펴보면, 몇 가지 높은 수준의 동향을 관측할 수 있습니다.

2012년 한 해 동안, 은행 업계를 대상으로 정치적인 동기를 지닌 이슈가 될만한 분산 서비스 거부(DDoS) 공격이 끊임없이 발생했습니다. 2012년 초, 브라질[3]의 여러 은행에 평소와 달리 높은 수준의 트래픽을 겪는 사고가 발생했습니다. 이러한 공격은 브라질에 널리 퍼져있는 불평등 문제를 구실로 이루어졌습니다.

9월에는 미국의 은행을 대상으로 한 새로운 DDoS 공격이 시작되었습니다.[4] 이러한 공격은 YouTube에 게시된 반이슬람적인 동영상의 공개에 대한 보복이라는 공개적인 성명이 있었으나, 많은 수의 연구자 및 언론 매체는 이러한 공격이 더욱 은밀한 다른 활동을 은폐하기 위한 것은 아닌지 의심했습니다. 2012년 말까지 지속된 미국의 은행에 대한 DDoS 공격은 과도한 양의 트래픽을 통해 해당 기업의 네트워크에 큰 부담을 주기 위한 것이었다는 점이 중요합니다. 이전까지의 DDoS 공격은 10GB~15GB 정도의 데이터를 이용했습니다. 하지만 이번 공격의 경우에는 60GB~70GB의 데이터에 해당하는 트래픽이 여러 곳에서 보고되었습니다.



3 http://www.techweekeurope.co.uk/news/anonymous-targets-brazilian-banks-in-fight-against-inequality-58800
4 http://threatpost.com/en_us/blogs/ddos-attacks-major-us-banks-resurface-121412

이러한 공격자는 특정 유형의 공격 및 특정 유형의 서버를 이용해 공격함으로써 유례 없는 수준의 트래픽을 발생시킬 수 있었던 것으로 파악되고 있습니다. IBM X-Force가 과거에 보고한 바와 같이, 많은 수의 DDoS 운영은 공격 대상을 공격하도록 구성된 원격으로 제어되는 악성코드를 실행하는 훼손된 PC를 이용해 이루어집니다. 이러한 봇(bot)은 블랙 마켓에서 몇천 개씩 구매할 수 있으며, 매우 효과적으로 이용될 수 있습니다. 그러나 PC는 항상 인터넷에 연결되어 있는 것은 아니므로 성능이 제한되며, ISP의 대역폭은 예측 불가능할 수 있습니다.

2012년의 은행 DDoS 공격에는 감염된 PC가 이용된 것이 아니라 높은 대역폭의 데이터 센터에 설치된 훼손된 웹 서버[5]가 이용된 것으로 보입니다. 공격자는 CMS 시스템 및 다른 널리 이용되는 웹 프레임워크의 보안 취약점을 이용하여 웹 서버 봇넷을 구축할 수 있으며, 이러한 봇넷은 일반적으로 PC보다 가동 시간이 훨씬 길고 더욱 큰 대역폭을 갖습니다. 이로 인해, 공격자는 더 적은 수의 봇을 이용하여 더 효과적으로 더 많은 트래픽을 발생시킬 수 있습니다.

지난해에는 공격자가 "Itsoknoproblembro"와 같이 취약한 웹 서버를 대상으로 하는 여러 가지 툴킷을 이용할 수 있었습니다. Prolexic은 Itsoknoproblembro 소프트웨어가 "고유한 2티어 방식의 명령 모드를 이용해 다수의 고대역폭 공격 유형을 동시에 실행하는 치명적인 DDoS 위협"이라고 말했습니다. 또한 "일반적으로 대부분의 네트워크 인프라를 압도하는 수준의 트래픽인 최대 70Gbps의 트래픽, 즉 3천만pps(packets per second)의 트래픽"을 이용한 공격을 관측했다고 밝혔습니다.[6]

새로운 툴킷 및 감염된 웹 서버의 봇넷뿐만 아니라, 증폭 공격(amplification attacks)과 같은 기존의 신뢰할 수 있는 방법도 높은 수준의 트래픽을 유발하는 데 효과적으로 이용되고 있습니다. ICMP(Internet Control Message Protocol) 기반의 "스머프 공격(Smurf Attack)"과 같은 증폭 공격은 10년 이상 이용되어 왔으며, 현재 공격자는 동일한 기본 원리를 이용해 더 많은 트래픽을 발생시키고 있습니다. 특히 DNS Amplification 공격[7]은 인터넷상의 공개된 또는 잘못 구성된 DNS 분석 서버로 인해 그동안 성공적으로 공격에 이용되어 왔습니다. 이 공격의 전제 조건은 공격자가 위장 IP를 이용해 작은 크기의 UDP(User Datagram Protocol) 요청, 예를 들면 64바이트의 DNS dig 명령을 공개된 제3자 DNS 서버에 전송할 수 있어야 한다는 것입니다. 이러한 명령은 64바이트 요청의 50배가 넘는 3Kb~4Kb의 데이터를 반환합니다. 이러한 수준으로 트래픽이 크게 증가하므로, 공격자가 더 많은 트래픽을 전송할 수 있으면 공격 대상은 더 쉽게 손상될 수 있습니다.

2012년에는 주목할 만한 다른 보안 침해 사고도 많이 발생했으며, 여기에는 뉴스의 헤드라인을 장식한 유명 온라인 서비스 회사 사례도 포함됩니다. 2012년 초, 한 전자상거래 거대 기업[8]에는 보안 침해 사고가 발생했으며, 이를 대중에 공개하고 고객에게 비밀번호를 쉽게 변경할 수 있는 방법을 제공하여 상황을 해결하기 위한 적극적인 조치를 취했다고 발표했습니다. 2012년 6월에는 3대 보안

5 http://threatpost.com/en_us/blogs/bank-ddos-attacks-using-compromised-web-servers-bots-011113
6 http://www.prolexic.com/knowledge-center-ddos-threat-advisory-itsok.html
7 http://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack
8 http://usatoday30.usatoday.com/tech/news/story/2012-01-16/mark-smith-zappos-breach-tips/52593484/1

침해 사고가 보고되었으며, 음악 소셜 사이트[9], 온라인 데이트 커뮤니티[10] 및 최대 규모의 전문 소셜 네트워크[11] 중 한 곳에서 발생한 사고가 있습니다. 이러한 각 보안 침해 사고로 인해 이메일 주소 및 취약하게 암호화된 비밀번호를 포함한 막대한 양의 사용자 데이터가 대중에 유출되었습니다. 그리고 몇 주 후, 한 주요 웹 포털[12]에 위치한 오래된 사이트에서 450,000개의 이메일 주소와 암호화되지 않은 비밀번호가 포함된 파일을 입수할 수 있었습니다.

공격자는 동일한 비밀번호를 소셜 네트워크 로그인 정보 및 웹메일 계정에 재사용하는 실수를 한 많은 고객들의 이메일을 훼손하고 다른 개인 데이터에 접근할 수 있었으며, 고객들은 비밀번호 재사용으로 인한 위험을 직접 경험했습니다. 이러한 보안 침해 사고의 한 가지 긍정적인 결과는 웹 개발자 및 각 개인에게 비밀번호 보안에 대한 새로운 관심을 불러일으켰다는 것입니다.

이전과 마찬가지로, 보안이 열악한 대학 및 정부 조직들은 2012년 동안 보안 침해를 겪었습니다. 이러한 조직들이 여전히 비밀번호 및 기타 데이터 암호화와 같은 보안 기본사항을 적용하지 않고 있다는 것은 놀라운 일입니다.

미국의 의료 업계에도 동일한 수준의 데이터 유출 사고가 발생했으나, 이러한 사고는 SQL 인젝션이나 웹 기반 공격에 의한 사고가 아닌 직원 랩톱 및 백업 테이프의 열악한 관리로 인해 발생한 사고였습니다. 미국 의료 업계는 지난 3년 동안 데이터 유출 사고로 인해 미국 내 2,100만 명의 환자에 대한 의료 기록이 유출되었다고 보고했습니다.[13] 이러한 유형의 데이터 유출 사고는 의료 업계에 더욱 엄격한 보안 통제 및 보안 정책이 필요하다는 것을 잘 보여주고 있습니다.

2012년에 발생한 또 다른 흥미로운 공격 대상은 미국을 기반으로 한 프렌차이즈 기업의 전 세계 지점의 공식 웹사이트였습니다. 예를 들면, 유명 패스트 푸드 음식점의 호주[14], 헝가리[15], 인도[16] 및 태국[17] 지점이 모두 공격 대상이 되었으며 고객 데이터가 유출되었습니다. 각 지점의 웹사이트가 모기업의 브랜드 정체성을 가지고 있기는 하지만, 각 지점이 항상 모기업과 동일한 IT 인프라를 통해 조직 또는 운영되거나, 항상 모기업과 동일한 정책을 이용해 규정을 준수하는 것은 아닙니다. 이러한 유출 사고가 대중에게 알려지면 해당 브랜드의 평판은 타격을 받거나 손상될 수 있습니다.

대부분의 유출 사고는 해시 태그를 갖는 코드 이름으로 식별되는 더 큰 "작전(operation)"의 일부였습니다. 이러한 작전은 일 년 내내 추적되었으며, 그 결과 공통점이 별로 없는 다양한 공격 대상으로부터 수십만 건의 기록이 유출되었습니다. 예를 들면, #opleak[18]은 처음에는 더욱 강력한 웹사이트 보안에 대한 필요성을 드러내기 위한 작전으로 발표되었습니다. 200곳이 넘는 서로 다른 웹사이트로부터 총 45,000건 이상의 이메일, 비밀번호 및 다른 민감한 데이터가 유출되었습니다. 이러한 유출 사고의 대부분은 SQLi 취약점으로 인해 발생했습니다.

9 http://www.last.fm/passwordsecurity
10 http://www.cbsnews.com/8301-501465_162-57448965-501465/eharmony-suffers-password-breach-on-heels-of-linkedin/
11 Ibid
12 http://www.pcworld.com/article/259136/450_000_yahoo_voice_passwords_breached_hacking_group_claims.html
13 http://www.computerworld.com/s/article/9230028/_Wall_of_Shame_exposes_21M_medical_record_breaches
14 http://arstechnica.com/security/2012/11/australian-pizza-hut-customers-served-a-deep-dish-of-info-leaks/
15 http://www.cyberwarnews.info/2012/10/12/pepsi-hungary-hacked-50000-user-credentials-leaked/
16 http://www.computerworld.com/s/article/9231198/Domino_s_Pizza_says_website_hacked
17 http://www.hotforsecurity.com/blog/mcdonalds-thailand-serves-2000-customers-with-a-side-of-data-leak-4040.html
18 http://www.cyberwarnews.info/tag/opleak/

일부 작전은 특정 사건에 대해 항의하는 형태로 실행되었으며, #opleak과 같은 다른 작전은 더 나은 보안 환경에 대한 필요성을 보이기 위한 의도로 실행되었습니다.

그림 4에 표시된 보안 사고 사례에서, 가장 많은 유출 사고가 발생한 국가는 46%의 비중을 차지한 미국입니다. 영국에서는 전체 사고 중 8%가 발생하여 2위를 기록했으며, 호주와 인도는 3%로 공동 3위를 기록했습니다.

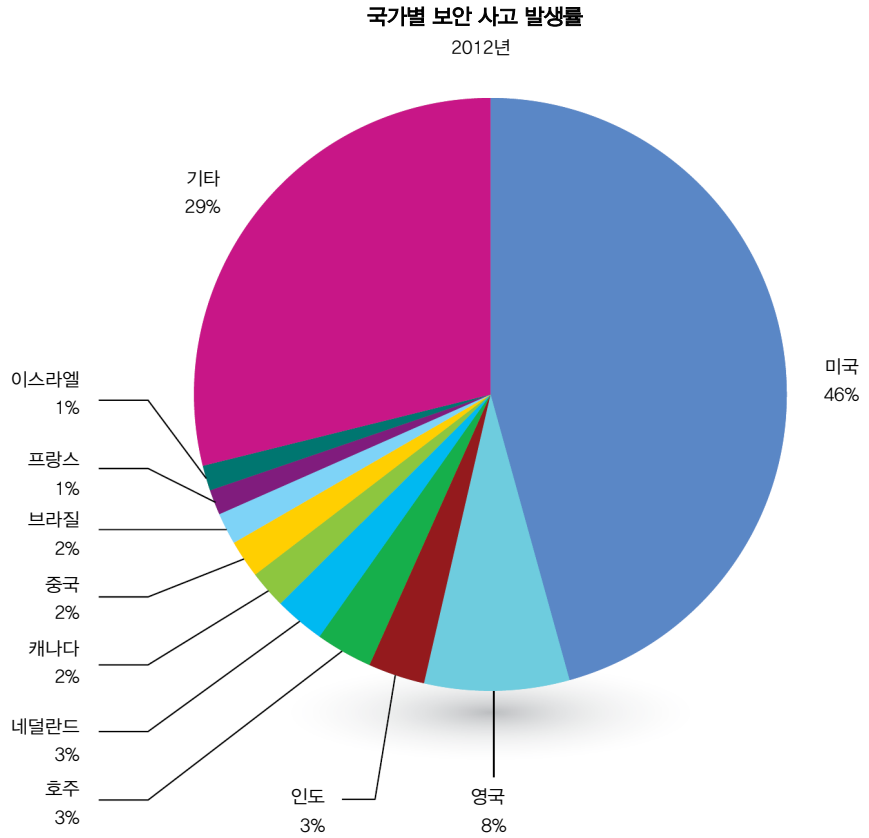


그림 4: 2012년 국가별 보안 사고 발생률

무엇을 배웠는가?

2011년에 발생한 수많은 유출 사고에 이어서 2012년에는 사고 발생 횟수가 늘어나 최대치에 이르렀으며, 그 결과 개인식별정보 및 기업 데이터에 대해 보다 견고한 보안이 필요함을 인식하게 되었습니다.

IBM은 2012년 상반기 동향 보고서에서 더욱 계산이 복잡한 해싱 알고리즘을 이용해 각 웹사이트가 저장하고 있는 비밀번호를 더욱 안전하게 암호화하는 방법에 대해 보고했습니다. 또한, 웹 사용자용 비밀번호 기초사항을 중심적으로 살펴보았습니다. 이를 통해 비밀번호 재사용이 개인의 정보와 기업의 네트워크에 얼마나 해로운지 명확해졌습니다.

과거와 마찬가지로, 많은 수의 유출 사고는 보안 기본사항 및 정책을 열악하게 적용함으로써 발생한 사고였으며, 이러한 사고는 약간의 기본적인 보안 예방책을 실시함으로써 예방할 수 있었습니다. IBM은 보안 분야 관련 베스트 프랙티스 중 일부를 다음과 같이 요약했습니다.

"만일 IBM X-Force가 IT 부서를 운영한다면"

1. 제3자에 의한 외부 및 내부 보안 감사를 정기적으로 실시합니다.
2. 엔드포인트를 관리합니다.
3. 민감한 시스템 및 정보를 분할하여 관리합니다.
4. 기초사항(방화벽, 안티바이러스, 침입 방지 디바이스 등)을 통해 네트워크를 보호합니다.
5. 웹 애플리케이션에 대한 감사를 실시합니다.
6. 일반 사용자에게 피싱 및 스피어 피싱에 대한 교육을 실시합니다.
7. 부적절한 비밀번호를 사용 중인지 검사합니다.
8. 모든 프로젝트 계획에 보안을 포함시킵니다.
9. 비즈니스파트너의 정책을 검사합니다.
10. 견고한 사고 대응 계획을 수립합니다.

보안 사고의 세부사항을 보고하는 기업의 수는 크게 증가하지 않았지만, 공격자는 대중에게 자신들이 사용한 취약점이나 기법을 기꺼이 알리고자 하는 것 같습니다. Pastebin 등과 같은 공공 사이트에 개인 데이터를 덤프하는 것뿐만 아니라, 공격자는 공격의 동기 및 진입을 위해 사용한 방법 등과 같은 추가적인 정보를 문서화합니다.

기업들은 당연히 보안 사고를 보고하는 것을 꺼리지만, 사고를 보고함으로써 고객에게 개인 데이터가 위험할 가능성을 알릴 수 있으며, 다른 기업이 과거의 실수를 통해 교훈을 얻고 향후에 동일한 사고가 발생하는 것을 방지할 수도 있습니다. 공개된 정교한 수법의 공격 중 일부를 파악하여, 한 기업이 보안 사고를 공개하면 다른 여러 기업도 이와 유사한 보안 사고를 경험하고 있다는 것을 알 수 있습니다.

보안 침해 사고의 빈도, 동기 및 사용 기법에 대한 더욱 개방된 논의를 통해 이러한 핵심적인 문제가 주목을 받게 되었습니다. 현재의 문제는 "이러한 인식을 어떻게 적용하면 사고 발생의 증가 추세를 역전시킬 수 있을 것인가?"입니다.

보안 기본사항에 다시 주안점을 두는 것이 매우 훌륭한 출발점이라는 것을 논의한 적이 있습니다. 기업들이 모든 영역에서의 위험을 평가함에 따라, 여러 부분에서 기업이 조직적인 노력을 해야 한다는 것이 명확해졌습니다.

SQL 인젝션을 방지하기 위해 웹 애플리케이션에 대한 감사를 실시하고 보안을 확실히 하는 것과 같은 기술적인 과제가 존재합니다. 또한 접근 통제 및 데이터 무결성과 같은 정책 관련 과제를 비롯하여 안전한 컴퓨팅 작업에 대한 지속적인 직원 교육 등의 인적 과제도 존재합니다. 이러한 과제 중 어느 하나라도 적절히 처리하지 못하는 경우에는 한 걸음 후퇴하게 될 것입니다.

이러한 중요 분야 각각에 시간과 자원을 투자하는 것은 어려운 일이지만, 이 과정에서 이사회 수준에서의 논의 필요성에 대한 인식이 증가하게 되었습니다. 그리고 점차적으로 지속해서 조금씩 개선해 나가는 것은 문제 해결을 위한 긍정적인 밑바탕이 될 수 있습니다.

핵티비즘(Hacktivism)의 역사

"핵티비즘(Hacktivism)"이라는 용어는 언론에서 자주 이용하는 유행어가 되었습니다. 그 기원을 찾아보면, 이 용어는 1996년에 해킹 집단인 Cult of Dead Cow(cDc)의 한 멤버가 처음으로 사용한 것으로 추정됩니다. 이후 2004년, cDc는 "기술을 이용해 전자 매체 전반에서 인권을 향상시키는 행위"라는 보다 공식적인 정의를 내렸습니다.[19] 이러한 선언은 서비스 거부 공격(정보에 접근할 수 있는 권한을 빼앗는 행위) 금지 또는 웹사이트 파손(자유롭게 발언할 수 있는 권한을 빼앗는 행위) 금지와 같은 몇 가지 기본적인 규칙을 제시합니다. 그러나 아이러니하게도, 현재 핵티비즘을 구실 삼아 발생한 대부분의 보안 사고는 서비스 거부 공격 및 웹사이트 파손을 기본적인 방법론으로 이용하고 있습니다.

많은 경우, 핵티비즘이라는 용어는 공격자의 불법적인 활동에 대해 충분한 정당성을 부여하지 못하고 있습니다. 이 용어는 일반적으로 인지도를 높이고, 잘못된 행위에 대한 보복 또는 변화를 강요할 목적을 지닌 모든 종류의 사이버 공격을 포함하는 용어로 발전되었습니다.

어나니머스(Anonymous)와 같이 잘 알려진 해킹 그룹은 다양한 종류의 공격을 이용하며, 때로는 분산 서비스 거부(DDoS) 공격을 이용하기도 합니다. 어나니머스는 DDoS 공격을 이용해 자신들의 의견을 홍보할 수 있으므로, 이는 옳은 행위라고 주장합니다. 어나니머스는 미국 정부에 DDoS 공격을 합법적인 형태의 저항으로 인정해 줄 것을 청원하기에 이르렀습니다. 본 글을 작성하고 있는 현재, 이러한 청원을 위해 6,000명 이상이 서명했으며, 미국 정부의 공식적인 답변을 받기 위해서는 25,000명의 서명이 필요합니다.[20]

19 http://www.cultdeadcow.com/cDc_files/cDc-0384.php
20 http://www.huffingtonpost.com/2013/01/12/anonymous-ddos-petition-white-house_n_2463009.html

IBM MSS(Managed Security Services)—전세계 위협 현황

IBM MSS(Managed Security Service)는 1년 365일 하루 24시간, 130여 국가에서 수백억 건의 이벤트를 모니터링하고 있습니다. IBM MSS는 이러한 국제적인 입지를 바탕으로 IBM 분석가에게 현재의 위협 및 사이버 위협 현황을 전체적으로 이해할 수 있도록 풍부한 데이터를 제공합니다. 이 단원에서는 전 세계에 위치한 IBM의 보안 운영 센터(Security Operations Centers)에서 확인한 보안 사고 및 위협의 유형에 대한 개요를 제공합니다. 위협 동향 정보는 보안 전략을 수립하고 개인에 대한 위협의 중요성을 이해하는 데 필수적인 요소입니다.

MSS 위협 동향 보고는 이번 호부터 새로운 보고 양식을 도입하기 시작했습니다. 매일 MSS 엔드포인트에 노출되는 수억 개의 잠재적인 위협에 대해 이야기하는 대신, 휴리스틱(heuristic) 프로세스 및 MSS 담당 직원을 통해 확인된 보안 사고에 대해 보고하도록 하겠습니다.

MSS 모니터링 팀이 수행하는 작업의 규모를 설명하기 위해, 먼저 몇 가지 시스템 통계를 확인하겠습니다.

MSS 모니터링 서비스는 1년에 2,500억(250,000,000,000) 건이 넘는 보안 이벤트에 노출됩니다. 침투 탐지 및 방지 기술에 초점을 두는 경우 이러한 양은 거의 40% 가까이 감소하여 대략적으로 1,400억(140,000,000,000) 건의 이벤트가 남습니다. 휴리스틱 시스템은 이러한 수십억 건의 이벤트를 철저히 검사하여 다양한 공격 정보를 번들로 결합한 일련의 경보를 생성하며, 이러한 경우 추가적으로 감소하는 이벤트의 수는 약 99.999%이며, 이는 2백만 건이 넘는 경보에 해당합니다. 이 수치는 추가적인 정보 및 자동화된 시스템을 경보에 결합하여 더욱 감소시킬 수 있으며, 최종적으로 10만 건의 이벤트가 사람이 수행하는 작업과 휴리스틱 작업을 통한 반복적인 방식으로 검토됩니다. 이러한 작업을 통해 고객에게는 경고 정보를 제공하고 일반 대중에게는 조언을 제공하게 됩니다.

따라서, 이 보고서는 2,500억 건의 이벤트로부터 IBM의 다양한 고객에게 제공하는 수십만 건의 경보를 추출하는 기술을 기반으로 작성된 것입니다.

MSS—2012년 보안 사고 동향

보안 사고 동향은 전 세계의 보안 현황을 나타내는 지표입니다. 다양한 경보의 상대적인 양을 통해 공격의 성립 및 실행 방법을 설명하고, 대개 공격 방법이 최근에 발전하게 된 방식에 대한 정보를 제공할 수 있습니다. 각 경보 유형별 양은 공격자가 이용하는 프로세스에 대한 정보를 제공합니다.

용어	설명
보안 사고	의도된 결과를 기반으로 분류된 유사한 경보의 범주 또는 그룹. "문제(Issues)"라고도 함
경보	일정한 패턴의 이벤트가 탐지되었으며 조치를 취할 필요가 있다는 것을 모니터링 담당 직원에게 알리기 위한 통지사항
이벤트	모니터링되고 있는 보안 엔드포인트 중 한 곳에서 전송하는 활동 보고서

Alan Boulanger는 1998년에 발표한 *Catapults and grappling hooks: The tools and techniques of information warfare*라는 논문에서 오늘날까지 대부분의 침입 작업에 이용되고 있는 방법을 수량화하는 데 큰 기여를 했습니다.[21] 그는 중세의 공성전 이미지와 시스템 및 네트워크에 대한 공격을 연관시켜 크래킹 프로세스를 명확하게 설명했습니다. 전쟁의 원리와 마찬가지로, 그의 견해는 대부분 아직도 유효하게 적용되고 있습니다.

각 시나리오에서, 침입자는 순서대로 각각의 단계를 실행합니다. 이러한 단계들은 하나의 *"시스템 침투 프로토콜"*을 구성합니다. 시스템 침투의 7가지 단계는 다음과 같습니다.

1. **정찰:** 대상 시스템 또는 네트워크에 대한 정보를 수집
2. **정밀 검사 및 공격:** 시스템의 약점을 정밀 검사한 후 도구를 배치
3. **발판 마련:** 보안 약점을 공격하여 시스템에 진입
4. **등급 향상:** 권한이 없는 계정에서 권한을 갖는 계정으로 등급 향상
5. **숨김:** 흔적을 감춤, 백도어를 설치
6. **정보 수집 거점:** 정보 수집을 위한 거점을 설치
7. **장악:** 네트워크의 한 호스트로부터 다른 호스트로 제어권을 확장

이러한 프로토콜의 첫 번째 두 단계, 즉 **1. 정찰**과 **2. 정밀 검사 및 공격**은 보안 사고 범주인 "정밀 검사 및 스캔"에 해당합니다. MSS 휴리스틱은 대량의 개별적인 행동을 하나의 이벤트로 축소시키며, 따라서 "정밀 검사 및 스캔" 범주에 표시되는 각각의 경보는 모니터링 소프트웨어로 그룹화된 수십만 개의 개별적인 시그니처를 의미하는 경우도 있습니다.

취약점이 발견되면, 다음 단계는 **3. 발판을 마련**하는 것입니다. 정찰의 결과 및 공격자의 의도에 따라서 다양한 기법이 이용됩니다. 이 단계는 "정밀 검사 및 스캔"에 "비인가 접근" 시도와 "악성코드" 공격을 결합한 것과 유사합니다. 공격의 목적이 확산 또는 소규모 시스템의 하이재킹이 아닌 경우, 더욱 직접적인 접근법을 이용하여 보다 중요한 대상의 보안 통제권에 침해 시도를 합니다.

21 http://www.lieb.com/Readings/IBMInfoWar.pdf

4. 등급 향상 단계가 필요한 경우, 이전에 언급했던 거의 모든 보안 사고 범주에 해당하는 공격이 실행되며, "정밀 검사 및 스캔"을 집중적으로 실행하여 다음 공격 대상을 찾게 됩니다. 공격 대상을 확인하면, "비인가 접근", "악성코드" 및 "부적절한 사용" 범주에 해당하는 도구를 사용합니다. "부적절한 사용" 범주에 포함되는 시스템 자원의 악용은 보안 침해 사고로 이어질 수 있습니다. P2P(peer to peer) 파일 공유와 관련된 정책 위반을 탐지함으로써 관리자가 향후 더 큰 문제를 초래할 수 있는 소규모의 침해를 검색하는 작업을 도울 수 있습니다.

마지막 세 가지 단계인 **5. 숨김, 6. 정보 수집 거점 및 7. 장악**에서는 네 가지 이전 단계의 도구를 이용하여 목적을 달성합니다. 따라서, "정밀 검사 및 스캔" 범주에 해당하는 대규모의 활동이 진행된 후 "악성코드" 범주에 해당하는 활동이 실행되며, 이후에는 "정밀 검사 및 스캔" 범주에 해당하는 활동이 다소 소강 상태를 보일 것이라는 것을 예상할 수 있습니다. 예를 들면, 2012년의 3월과 4월, 또는 9월과 10월 자료에서 이러한 추세를 대략적으로 확인할 수 있습니다.

마지막으로, 사이트의 평판을 깎아내리거나 사이트를 파괴하기 위한 전면적인 시도가 진행됩니다. 공격의 출처가 확인되는 경우에는 곧바로 공격을 막을 수 있기 때문에(서비스 거부 공격) 이러한 작업은 매우 드물게 실행되며, 보통 일시적으로 발생합니다.

다양한 보안 사고 범주의 상대적인 양에 기초한 정보에 따르면, 2012년의 주안점은 매우 광범위한 인터넷 경로를 통해 실행된 대규모의 조직적인 공격을 이용한 시스템 공격이었다고 할 수 있습니다. 공격 도구를 사용한 침투의 일반적인 개요를 따르는 활동 조직은 증가하고 있습니다. 잠재적인 공격 대상을 식별하고, 다양한 공격을 실행하며, 취약점을 악용하기 위한 시도가 점점 조직화되고 있습니다. 향후에 분석을 통해 이러한 동향에 대한 더욱 확실한 정보를 밝힐 수 있을 것입니다.

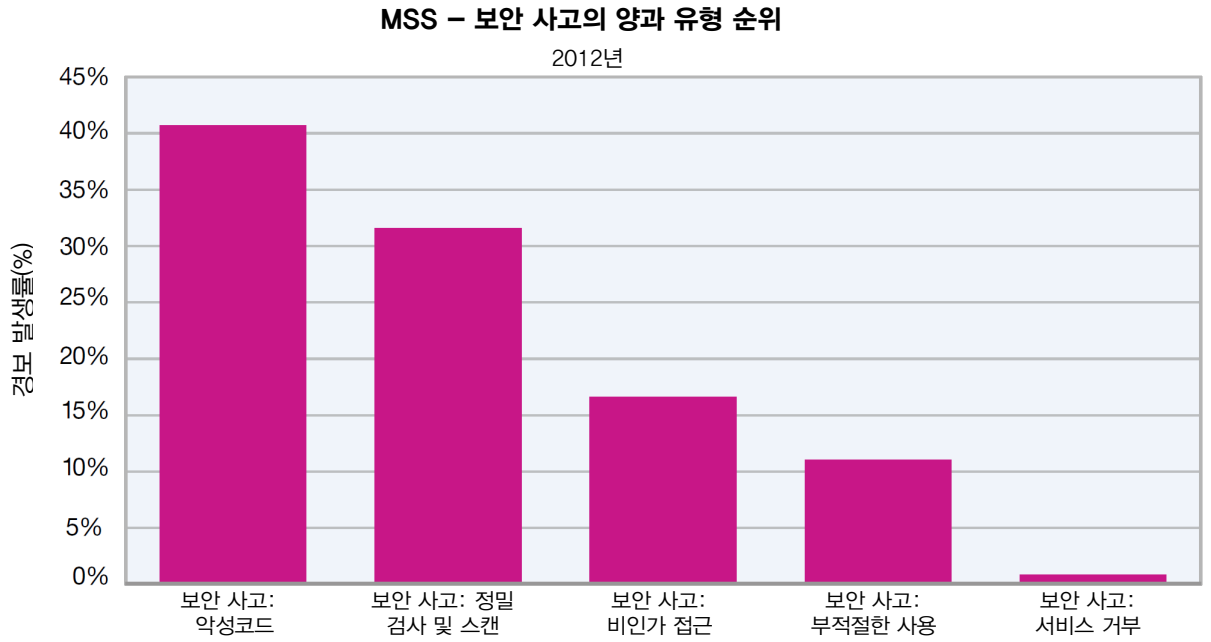


그림 5: MSS – 2012년에 발생한 보안 사고의 양과 유형 순위

보안 사고(SI) 경보 발생 동향은 2012년 동안 일정하게 유지되었으며, 수학적으로만 "가시적인" 동향이 증가했습니다. SI 경보의 전체 양은 트래픽 양의 변화 또는 출처의 수에 상관없이 지속적으로 증가하고 있습니다.

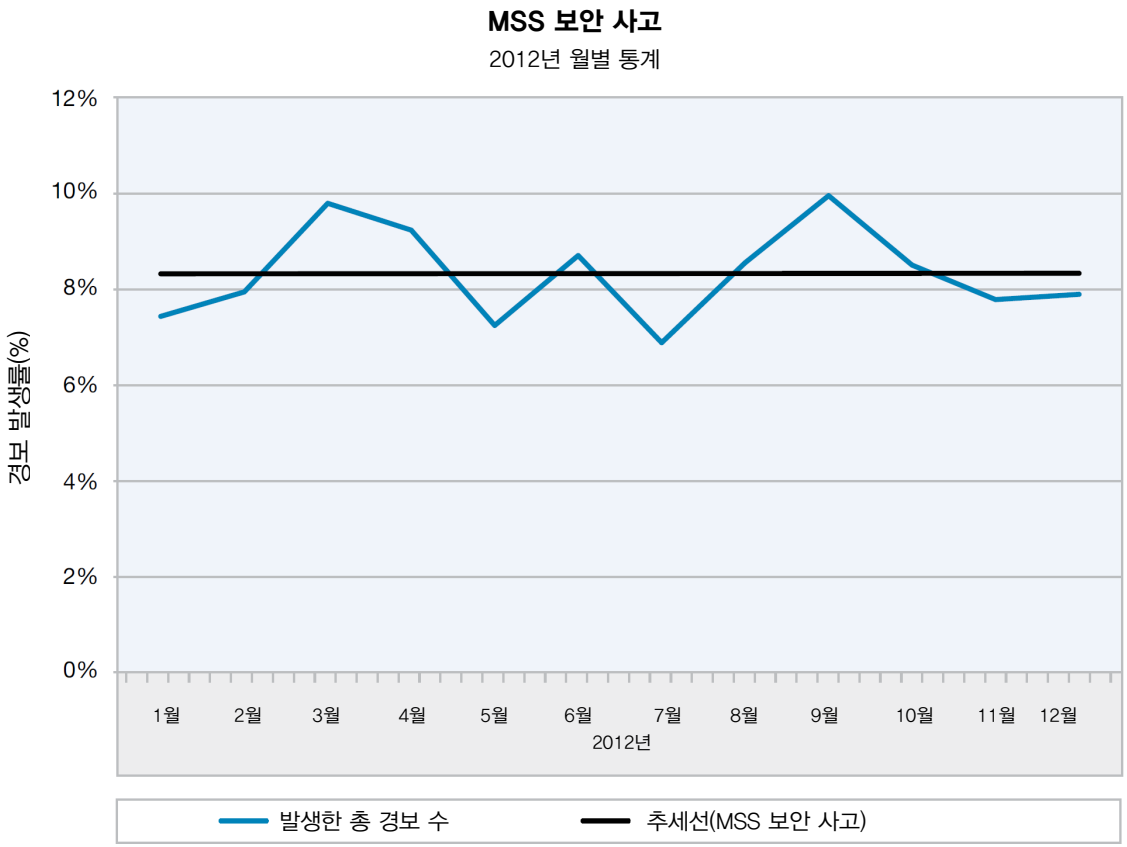


그림 6: 2012년 MSS 보안 사고 월별 통계

악성코드

보안 모니터링 관점에서 악성코드라는 공격 범주를 정의할 경우, 공격 및 악성코드 활동 모두와 관련된 복합적인 공격 벡터를 고려합니다. 발생 횟수가 증가한 보안 사고의 대부분은 SQL 인젝션에 의해 발생했습니다. IBM MSS는 SQL 인젝션 기반의 트래픽에서 지속적이고 엄청난 증가를 확인했으며, 이는 대부분 아시아 태평양 지역에서의 꾸준한 활동으로 인한 것이었습니다. 이러한 경보는 모든 산업 분야에서 발생했으며, 은행 및 금융 분야는 그 빈도가 더 높았습니다. IBM은 악성코드의 증가에 대한 최근의 언론 보도와 일치하는, 주로 매우 빠른 속도로 진행되는 다수의 인젝션 기법을 확인했습니다.[22, 23, 24] 특히 IBM은 의심스러운 호스트에 대해 정리된 목록을 이용해 봇넷 트래픽을 식별하고 지속적으로 CnC(Command and Control) 연결을 탐지했습니다.

악성 코드 활동은 가벼운 공격자, 내부자 위협, 사이버 범죄 및 APT(Advanced Persistent Threats) 등이 결합함에 따라 전체적으로 증가하고 있습니다. 그림 7은 오늘날의 컴퓨터 보안 분야에서 이루어지고 있는 "군비 확장 경쟁"을 나타내고 있습니다. 시스템을 손상시키기 위한 기법의 수는 지속적으로 증가하다가, 감소한 후, 다시 증가하고 있습니다.

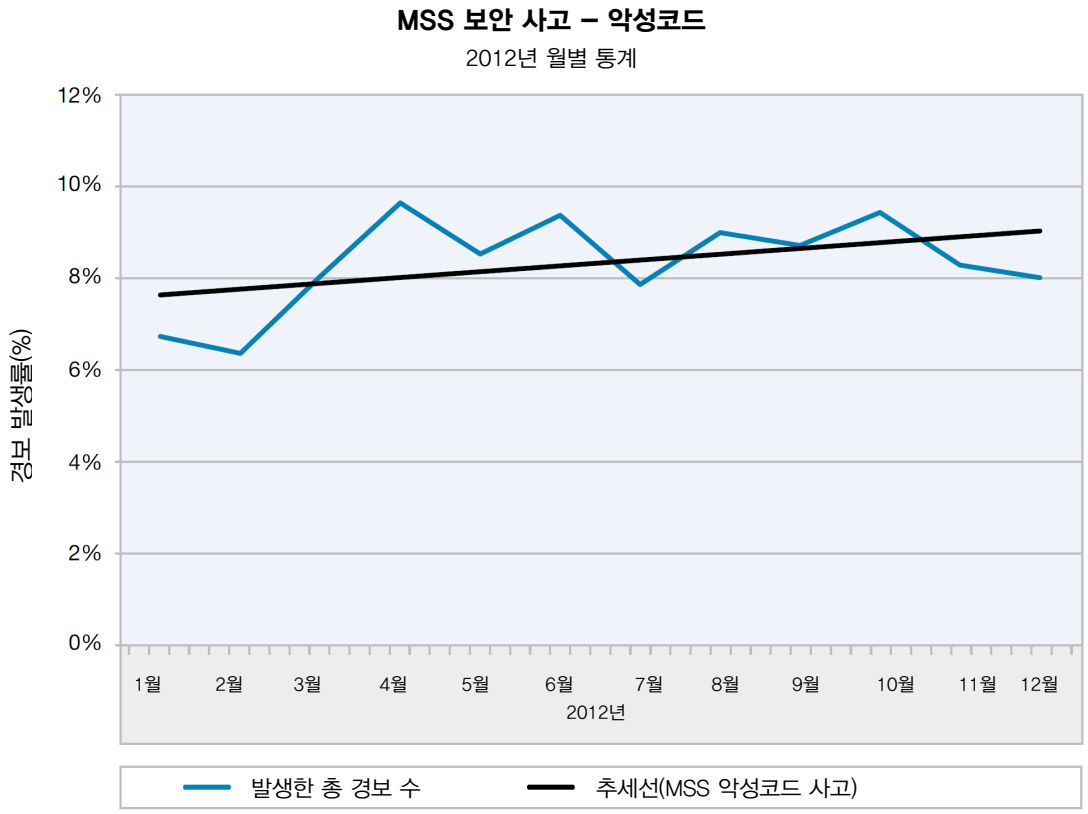


그림 7: MSS 보안 사고 – 2012년 악성코드 경보 월별 통계

22 http://www.computerweekly.com/news/2240160266/SQL-injection-attacks-rise-sharply-in-second-quarter-of-2012
23 https://www.informationweek.com/security/attacks/hackers-trade-tips-on-ddos-sql-injection/240012531
24 http://www.zdnet.com/sql-injection-attacks-up-69-7000001742/

정밀 검사 및 스캔

취약점 스캐닝은 시스템의 보안 태세를 시험하는 기본적인 방법 중 하나입니다. 정밀 검사 및 스캔에 이용되는 도구 및 기법은 시스템 운영에 매우 필수적인 요소이며, 공격자 및 방어자 모두는 동일한 도구를 이용해 시스템이 크래킹 작업의 대상이 될 수 있는지를 결정합니다. 이러한 기술은 매우 수준 높은 단계의 효과적인 기술이며, 일부 공격 툴킷 및 웜에 포함되어 잠재적인 공격 대상을 식별하는 데 이용됩니다.

정밀 검사 및 스캔 경보는 스캔 명령의 출처를 추적하고 알려진 스캐닝 도구 및 서비스와 비교 검사하는 작업 등 취약점 스캐너가 이용하는 것과 동일한 기술을 분석합니다. 모니터링 시스템은 허가된 출처로부터 스캔 명령이 실행되는지의 여부를 결정하기 위해 시스템 사용자 및 책임자로부터 수집한 데이터를 이용합니다. 허가된 것으로 시스템에서 식별한 스캔 또는 스윕(sweep)은 통보만 되며 경보를 생성하지는 않습니다. 비인가 활동은 작업자가 검토하는 대상이 되며, 모니터링 시스템에서 추가적인 경보가 필요한지 결정하기 위한 다른 유형의 분석에 이용될 수 있도록 경보가 추가됩니다.

그림 8에는 현재의 일반적인 상승 추세가 나타나 있으며, 이는 공격을 위한 정찰의 증가 수치와 일치합니다.

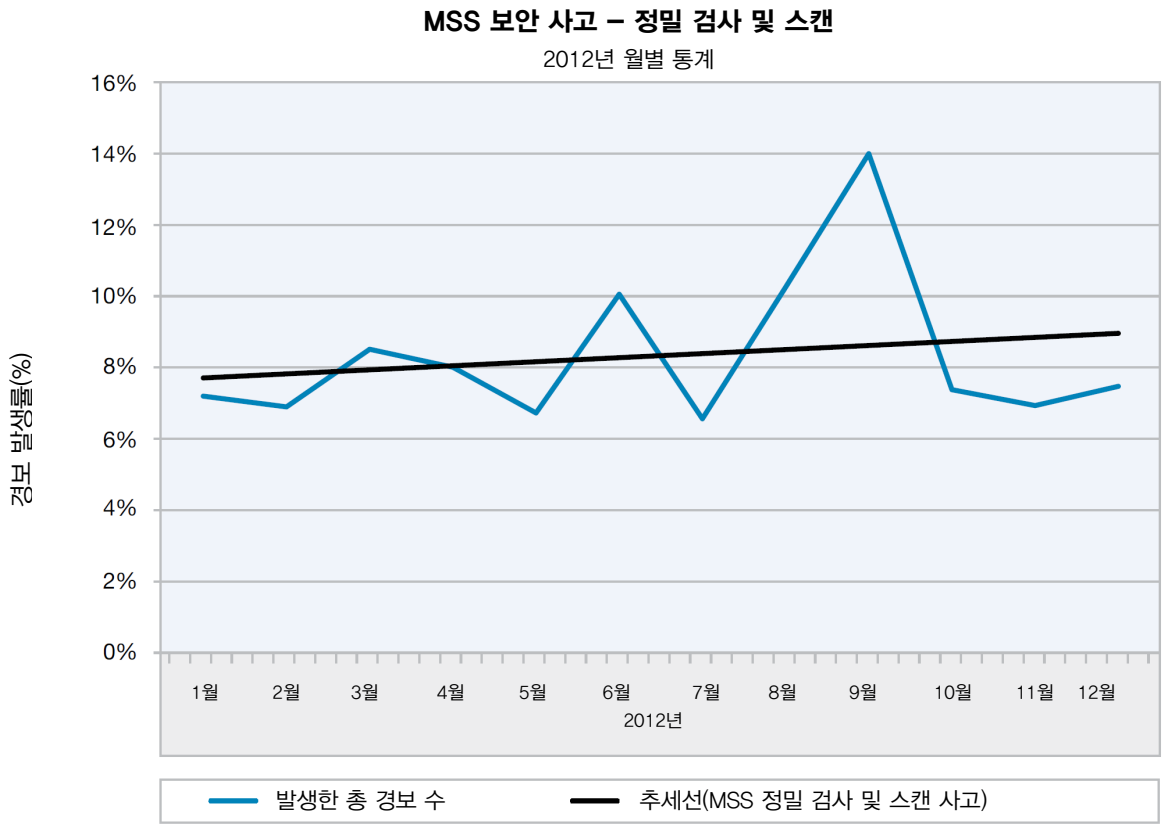


그림 8: MSS 보안 사고 – 2012년 정밀 검사 및 스캔 경보 월별 통계

비인가 접근 시도

2012년은 비인가 접근 시도가 성공적이었던 한 해인 것으로 증명되었습니다. 이러한 공격 벡터는 항상 활발했지만 2012년에는 특히 더욱 활발했습니다. 비인가 접근 시도로 분류되는 공격 중 가장 많이 이용되는 개별적인 공격은 FTP 무차별 공격, HTTP Cisco IOS 관리자에 대한 접근, Unix 비밀번호 파일에 대한 접근 시도 및 PSExec 서비스에 대한 접근이었습니다. HTTP 기반의 비밀번호 파일에 대한 접근 시도가 3월을 전후로 한 연초에 눈에 띄게 증가했으며, 9월에도 3월보다는 덜하지만 이러한 시도가 급증했다는 점도 흥미로운 사실이었습니다. 이러한 접근 시도는 특정한 공격 그룹이나 동기에 국한되지 않습니다. 이 공격 유형은 널리 이용되고 있으며, 어느 특정한 지역에서만 주로 발생하는 공격은 아닙니다.

비인가 접근 시도에는 백도어 공격, 무차별 공격, 특수한 1회성 공격 및 고객의 시스템에 침입하기 위한 시도에 이용되는 기타 수단이 포함됩니다. MSS 모니터링 시스템은 일상적으로 항상 수백 개의 비인가 접근 공격을 추적하고 있으며, 200개 미만의 공격만이 고객에게 실질적인 위협이 되는 수준으로 발전했습니다.

그림 9는 일반적인 하향 추세를 나타냅니다. 그러나 과거 추세의 주기적인 특성을 고려하면 이러한 하향 추세는 일시적인 상태일 가능성이 높습니다.

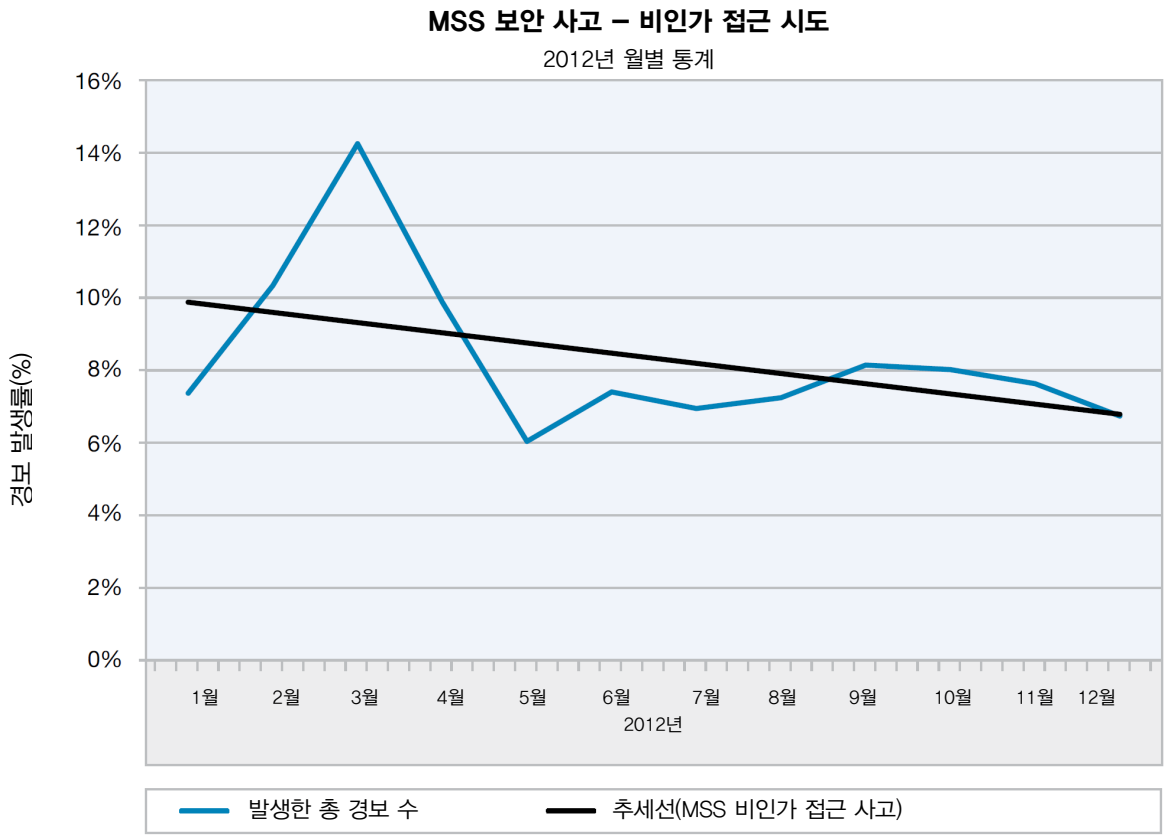


그림 9: MSS 보안 사고 – 2012년 비인가 접근 시도 월별 통계

부적절한 사용

부적절한 사용 이벤트는 일반적으로 파일 공유 P2P(peer to peer) 서버 및 인가되지 않은 클라이언트의 운영 등과 같은 자원의 오남용에 대한 경고입니다. 이러한 경보 그룹은 시스템에 대한 사용자 ID 접근 권한을 얻기 위한 무차별 공격과 같이 공격 초기 징후를 나타낼 수도 있습니다.

2012년 한 해 동안 SSH 무차별 공격은 이러한 공격 범주의 주요 원인이었습니다. 주로 아시아 태평양 지역을 기반으로 발생하는 이러한 유형의 공격은 다수의 외부 출처에서 실행되는 분산된 시도의 형태로 나타나는 경우가 많았으며, 현재 증가하는 추세를 보이고 있습니다. P2P (peer to peer) 트래픽 또한 부적절한 사용으로 인해 트래픽이 증가하는 원인 중 하나였습니다. P2P 트래픽은 민감한 정보 및 개인정보를 포함할 수도 있는 개별적인 호스트 시스템을 외부에 노출시킬 수 있으므로, 모든 비즈니스 네트워크에 위험한 요소입니다. P2P 기반의 탐지는 엄격한 정책을 기반으로 하며 디폴트 값은 비활성화로 지정되어 있습니다. IBM은 가능한 경우 모든 P2P 기반의 시그니처를 블로킹 모드로 활성화할 것을 권장합니다.

부적절한 사용에 해당하는 공격은 다양하므로, 정책 위반을 해결하고 인증 시스템이 강화되면 급격한 변화가 발생합니다. 이러한 프로세스로 인해 그림 10에서처럼 짧은 시간 동안 활동이 "소강 상태(lull)"를 보일 수도 있습니다.

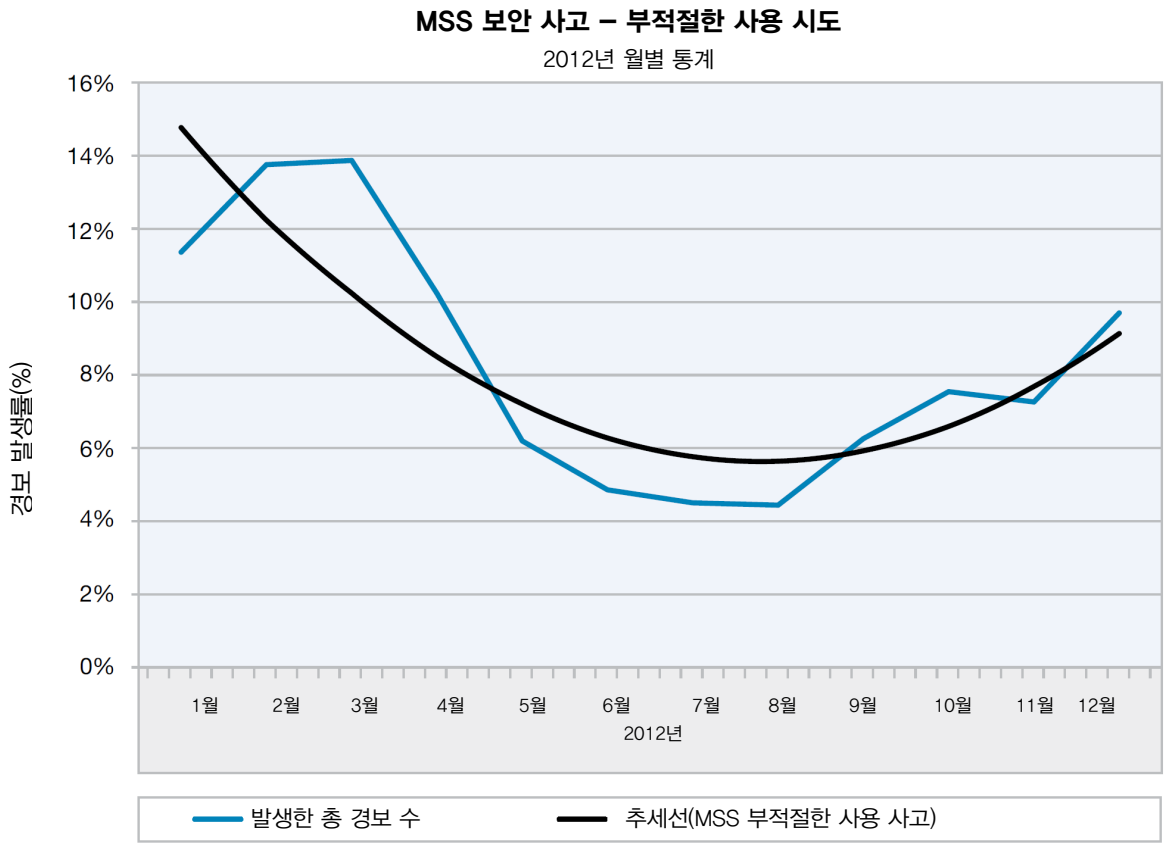


그림 10: MSS 보안 사고 – 2012년 부적절한 사용 시도 월별 통계

서비스 거부(DoS)

DoS 공격은 주로 목표로 삼은 사용자가 시스템의 일부를 사용하지 못하도록 만들기 위한 시도이며, 중요한 의사소통 수단을 사용하지 못하게 하거나 이러한 수단을 파괴하는 작업과 연관된 경우가 많습니다. DoS 공격에 대한 대책은 주로 아키텍처의 네트워크 계층에서 연결 유형 및 속도를 조정하는 것입니다. 그러면 공격자는 SlowLoris와 같은 솔루션을 배치하여 최소한의 네트워크 대역폭을 이용해 웹 서비스를 중단시킵니다. 이러한 "군비 확장 경쟁"은 전 세계의 컴퓨팅 인프라에 지속적으로 발생하고 있습니다.

2012년에 언론 매체는 다양한 그룹에서 실행한 서비스 거부(DoS) 공격에 대해 폭넓게 보도했습니다.[25,26,27] 위험도 측면에서 보면, DoS로 인해 1년에 약 12시간 동안 가용성이 저하되거나 아예 서비스를 제공하지 못할 수 있습니다. DoS로 인해 24시간 동안 시스템이 중단될 수도 있지만, 이러한 경우는 극히 드뭅니다. DoS 공격은 연간 60만 달러에서 백만 달러의 비용을 초래할 수 있으며, 대부분의 경우 시스템 가동 중단으로 인해 발생하는 데이터 센터 비용입니다.[28] DoS 공격은 단기적으로 재정에

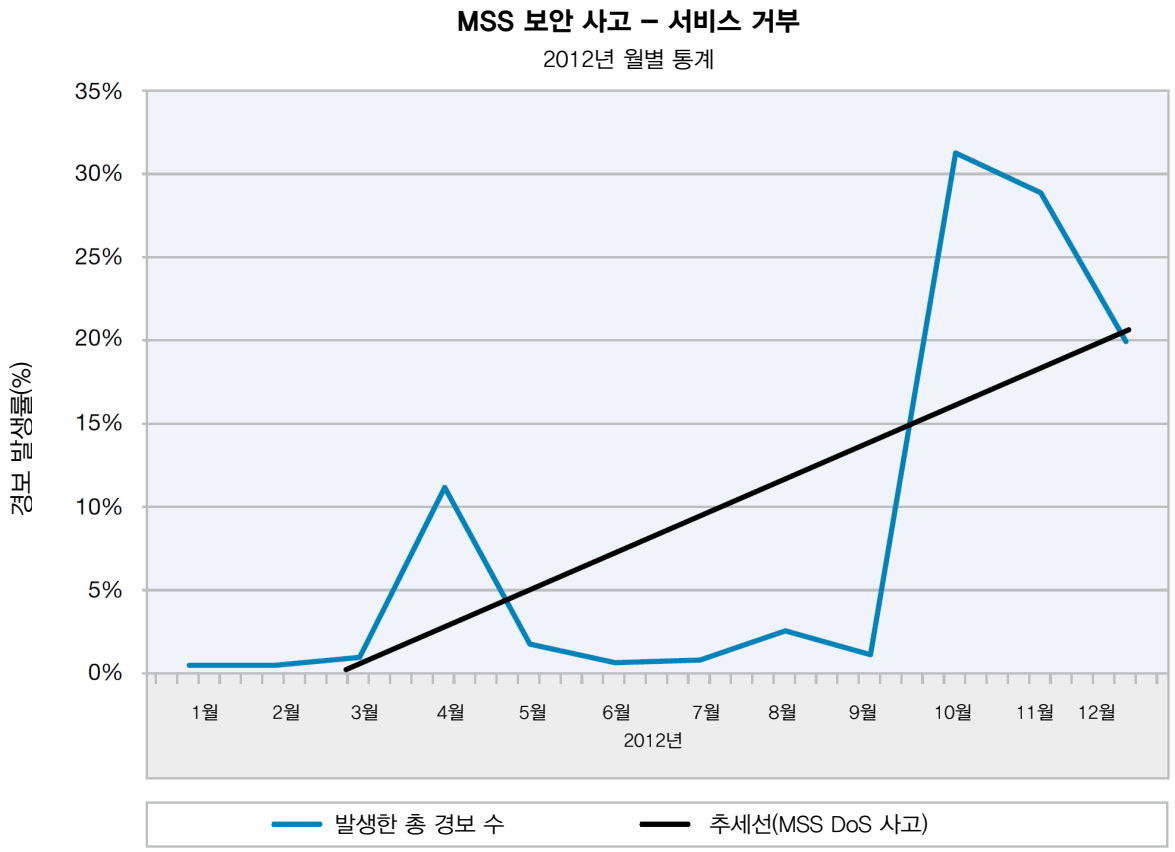


그림 11: MSS 보안 사고 – 2012년 월별 서비스 거부 경보

25 http://itcblogs.currentanalysis.com/2012/08/31/hacktivists-have-the-upper-hand-in-an-environment-where-most-attacks-go-unreported/
26 https://cyber.law.harvard.edu/events/luncheon/2013/01/sauter
27 http://blog.q1labs.com/2012/05/16/back-to-the-future-in-the-uk/

영향을 미칠 수 있지만, 비즈니스 또는 브랜드에 오랫동안 지속적인 피해를 입히지는 않는 것으로 판단됩니다. 특징상, 널리 알려진 DoS 공격은 시스템 가동 중단으로 인해 관련 비용을 발생시켜 특정 대상의 자산[29,30]에 심각한 수준의 피해를 입히기 위한 공격이라기보다는 홍보성 성격의 공격인 경우가 더 많다는 점입니다. 대부분의 피해자는 DoS 공격을 대중에게 공개하는 데 따른 잠재적인 비용이 발생하여 기업의 평판에 피해를 입었고 그 결과 복합적인 손실이 발생한다고 판단했습니다. [31] 평판 및 브랜드 관리에 대한 최근의 조사에 따르면 실제로는 이와 반대인 것으로 나타났지만[32,33], 이 차이점에 대한 인식은 아직 널리 확산되지 않았습니다.

다른 유형의 공격에 비하면 심각한 수준의 DoS 공격은 드물지만[34], 이러한 공격은 갑작스럽게 발생하고, 효과적이며, 대중 매체에 보도되지 않은 경우가 많습니다.[35,36]

그림 11은 갑작스럽게 단기간 내에 이루어지는 DoS 공격의 특성을 나타내며, DoS 공격은 발생한 후 곧 사라집니다. 앞서 언급한 Slowloris 공격처럼 낮은 수준의 다양한 이벤트가 인터넷 전반에서 지속적으로 발생하고 있으며, 때로는 급증하기도 합니다. 또 다른 공격은 불연속적이고 발생한 후 곧 사라지며, 동일한 출처에서는 거의 발생하지 않습니다.

29 http://www.bankinfosecurity.com/bank-attacks-what-have-we-learned-a-5197
30 Ibid.
31 http://www.dw.de/cyber-attack-victims-fear-exposure/a-16245535
32 https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=gts-LITS-bus-conn-NA&S_PKG=2012RepRisk&S_TACT=601B666W
33 http://www.bankinfosecurity.com/interviews/luba-i-1696
34 http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf
35 http://www.businessinsurance.com/article/20120411/NEWS07/120419975#sthash.caTs1Po7.dpuf
36 http://www.forbes.com/sites/ciocentral/2012/05/08/figuring-ddos-attack-risks-into-it-security-budgets/

인젝션 공격

인젝션 공격은 임베드된 명령어가 포함된 데이터 항목이 공격 대상 시스템에서 허가된 애플리케이션에 제공될 때 감지되며, 대상 시스템은 공격에 속아 임베드된 명령어를 실행하게 됩니다. 이러한 시도는 보안 환경에서 꾸준하게 두드러진 현상입니다. 보안 경보 추세를 참조하면 인젝션 공격이 매우 빠르게 증가하고 있음을 확인할 수 있습니다. 인젝션 공격은 공격자가 서버 내에 발판을 마련하는 데 쉽게 이용할 수 있는 방법입니다. 공격의 발판을 마련하면, 공격자는 더 많은 대상 시스템에 대한 공격을 실행할 수 있는 거점을 확보하고 경계 방어 체계 내에서 다른 시스템에 접근할 수 있는 도약대를 확보할 수 있는 전략적 이점을 얻습니다.

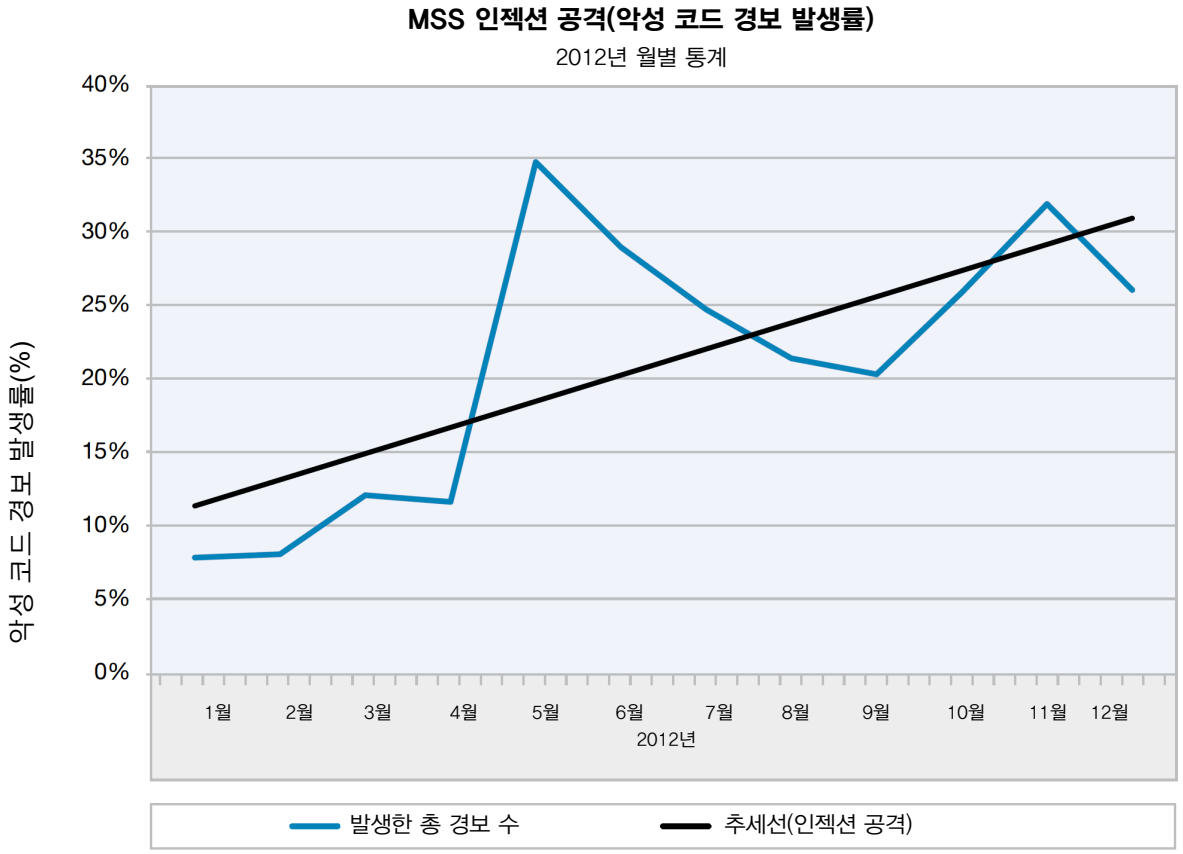


그림 12: MSS – 인젝션 공격(악성코드 경보 발생률) – 2012년 월별 통계

가장 일반적인 유형의 인젝션 공격 두 가지는 SQL 인젝션과 쉘 명령어 인젝션입니다. 인터프리터 및 LDAP 인젝션은 이와 유사한 전략을 이용하지만 더욱 제한된 결과를 얻습니다. 이전 보고서에 따르면, SQL_Injection 시그니처는 2010년에 2위를 기록했으며 2011년에는 1위로 상승했습니다. 2011년은 SQL 약점을 악용한 공격이 성공적이었던 한 해가 되었습니다. SQL 인젝션은 2012년 상반기에 1위 자리를 고수했으며, 연말까지 이러한 추세는 지속되었습니다.

쉘 명령어 인젝션은, 발견된 이후 지속적으로 공격 키트에 포함되어 온 RCE(Remote Command Execution)의 한 형태라고 할 수 있습니다.[37] 쉘 명령어는 운영 체제별로 다르므로, 쉘 명령어 인젝션은 SQL 인젝션만큼 널리 이용되지는 않습니다. SQL은 모든 유형의 데이터베이스에 접속 가능하므로 널리 이용되고 있으며, 이를 이용해 로그인 신임 정보에서부터 기업의 기밀 데이터에 이르는 다양한 대상에 대한 공격을 유도합니다.

인젝션 공격은 전체적으로 눈에 띄는 상승세를 보이고 있으며, 실제로 2012년에는 두 배 이상 증가했습니다. 데이터 채널을 통해 시스템을 공격하는 전략은 2년 전에 논의했던 "쉬운 공격 대상"을 목표로 하는 공격의 연장선에 있는 것이 분명합니다.

눈여겨볼 만한 다른 추세는 악성코드 공격에 포함되거나 결합된 인젝션 공격의 꾸준한 증가입니다. 그림 12에서 논의한 악성코드 부분에서 확인할 수 있듯이, 악성 코드 공격은 지속적으로 증가하고 있지만, 악성코드와 결합된 인젝션 공격은 더욱 빠른 속도로 증가하고 있습니다. 악성코드의 증가 추세는 2012년에 2%를 나타냈지만, 결합된 형태의 인젝션 공격은 거의 세 배 정도 증가했습니다.

IBM은 이러한 새로운 모델을 자세히 관찰하여 전략의 성공률 변화를 확인할 계획입니다.

37 http://xforce.iss.net/xforce/xfdb/6944

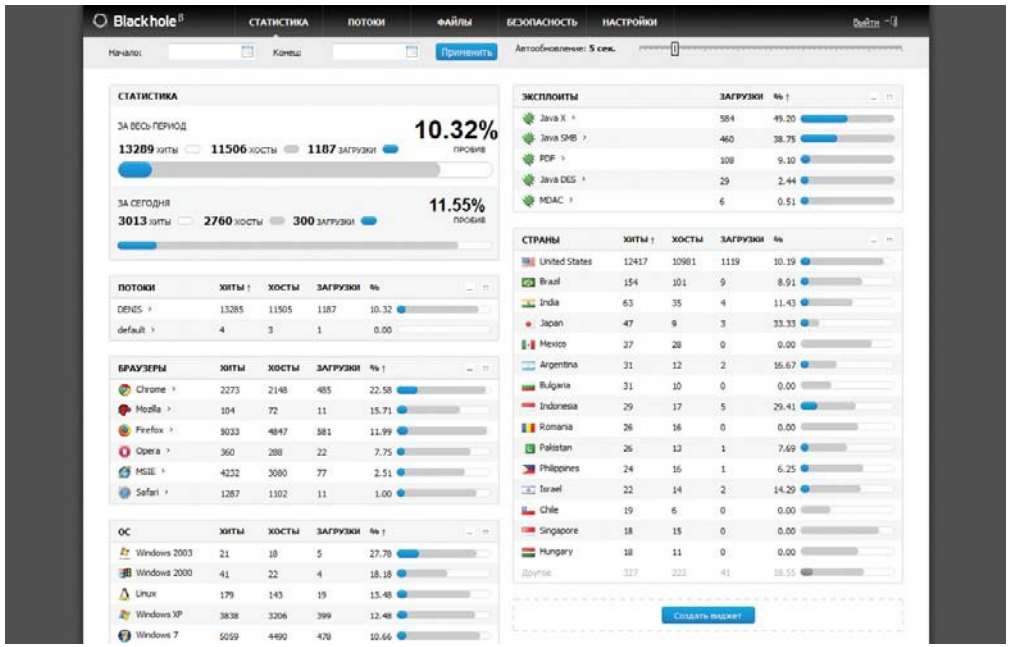
공격 키트: Java 관련 공격

2012년에는 웹 브라우저 공격 키트의 개발 및 활동이 급증했습니다. 주요 원인은 새로운 Java 취약점이었습니다.

Crimepack 공격 키트의 로그인 페이지

웹 브라우저 공격 키트(공격 팩으로도 알려져 있음)는 한 가지 특정한 목적을 위해 개발되며, 그 목적은 일반 사용자 시스템에 악성코드를 설치하는 것입니다. 공격 키트는 2006년에 처음 등장했으며, 공격 키트 개발자는 대규모의 시스템에 악성코드를 설치하려는 공격자에게 공격 키트를 제공했습니다. 공격 키트는 일반 사용자 시스템에 악성코드를 설치하는 데 즉시 이용 가능한 턴키 솔루션을 공격자에게 제공하므로, 꾸준히 널리 이용되었습니다. 공격 키트는 주로 해커 포럼을 통해 광고를 게재하며 현재 렌탈 비용은 한 달에 미화 500달러부터 미화 1,000달러까지 다양하며, 구매 비용은 미화 500달러에서 미화 3,000달러 사이입니다.

사용자는 주로 손상된 웹사이트를 방문하거나 공격 키트를 호스팅하는 덫이 설치된 웹사이트로 연결되는 링크를 클릭하여 감염됩니다. 감염 성공률을 높이기 위해, 공격 키트는 주로 다수의 브라우저 또는 브라우저 플러그인 취약점을 이용해 시스템을 훼손하여 악성코드를 설치합니다(아래의 스크린샷 참조). 2012년에 공격 키트 개발자는 새롭게 발견된 Java 취약점을 대상으로 하는 공격을 이용했다는 것이 분명합니다. 그렇다면 왜 Java를 대상으로 했을까요? 다른 제로 데이 (zero-day) 취약점(패치되지 않은 취약점을 통해 공격 코드를 유포)이 작년에 발견되었지만, 공격 키트 개발자가 가장 관심을 많이 가진 것은 Java 취약점인 것 같습니다.



Blackhole 공격 키트의 대시보드

(스크린샷은 공격 키트 개발자가 해커 포럼에 게재한 광고의 일부입니다.)

먼저, Java 취약점에 대한 공격이 어떻게 점차 공격 키트에 통합되었는지 살펴보겠습니다. 이를 통해 공격 키트 개발자가 Java 공격을 공격 키트에 포함시키는 데 얼마나 큰 관심이 있는지 확인할 수 있습니다.

CVE-2012-0507 타임라인

이 취약점은 Oracle에서 발표되었으며, 자세한 정보는 이후에 취약점 발견자가 2012년 2월 말에 공개했습니다.[38] 한 달 후, 취약점에 관한 자세한 정보가 공개된 후, 효과가 있는 공격이 Blackhole[39] 공격 키트에 통합되었고, 이틀도 지나지 않아 Phoenix[40] 공격 키트에 통합되었습니다.

그 후, 5월 초에 동일한 취약점에 대한 공격이 RedKit[41] 공격 키트에서 발견되었습니다. 2월 14일에 Oracle에서 패치를 발표했다는 것을 고려하면, 공격자들은 각 조직과 개인의 패치 적용률이 충분히 높지 않으며, 그 결과 최근에 패치가 적용된 취약점에 대한 공격이 성공할 것으로 예측했다는 것을 알 수 있습니다.

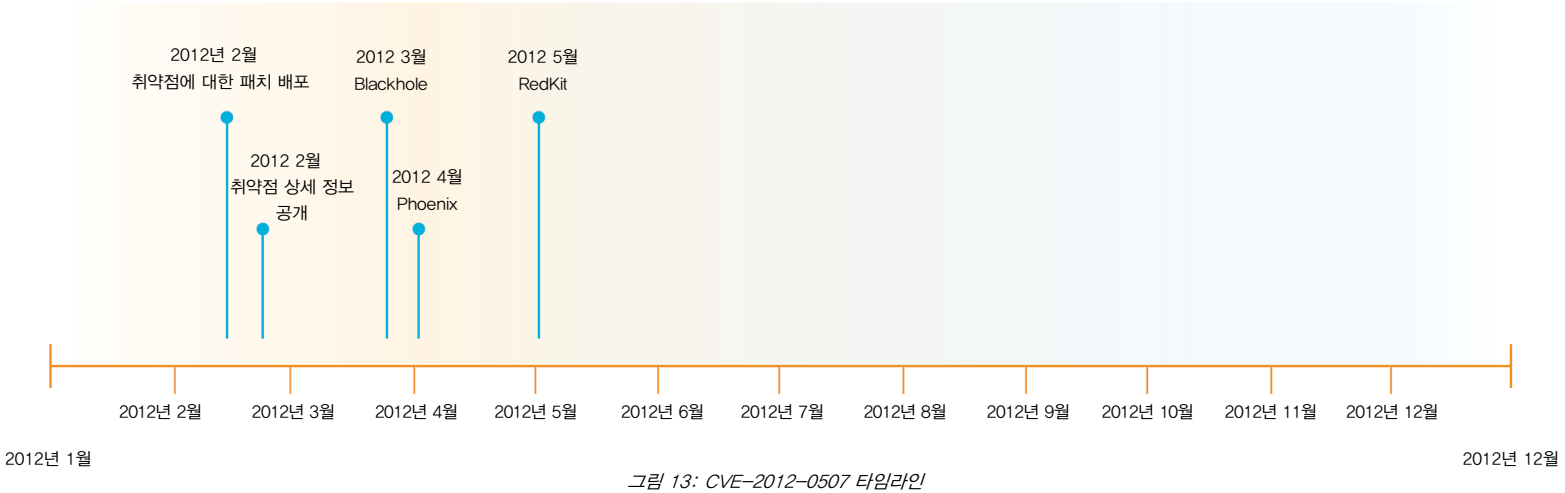


그림 13: CVE-2012-0507 타임라인

38 http://weblog.ikvm.net/PermaLink.aspx?guid=cd48169a-9405-4f63-9087-798c4a1866d3
39 http://malware.dontneedcoffee.com/2012/04/cve-2012-0507-on-windows-xp.html
40 http://malware.dontneedcoffee.com/2012/04/phoenix-exploit-kit-v31.html
41 http://blog.spiderlabs.com/2012/05/a-wild-exploit-kit-appears.html

CVE-2012-1723 타임라인

이 취약점에 대한 자세한 정보는 한 연구원이 2012년 6월에 공개했으며[42], 바로 며칠 후에 Oracle에서 패치를 발표했습니다. 약 3주 후, 이 취약점에 효과가 있는 공격이 Blackhole[43] 공격 키트에 통합되었습니다. 그리고 한 달 후, Kein[44] 공격 키트에서도 공격이 발견되었으며 Nuclear[45], Neosploit[46] 및 Cool[47] 공격 키트도 마찬가지였습니다.

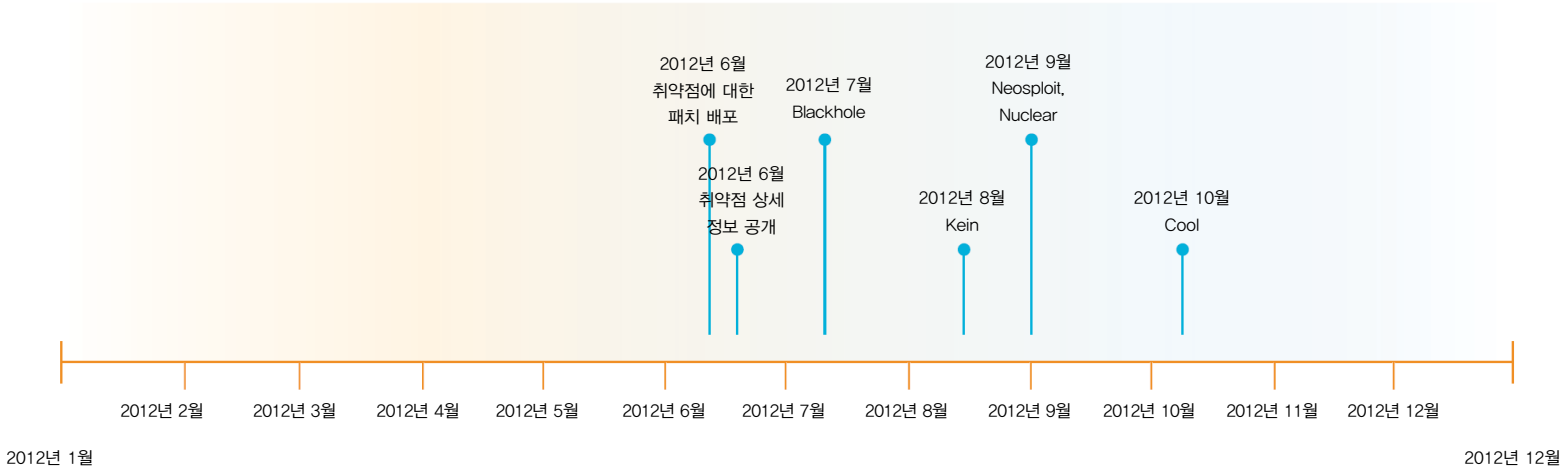


그림 14: CVE-2012-1723 타임라인

42 http://schierlm.users.sourceforge.net/CVE-2012-1723.html
43 http://malware.dontneedcoffee.com/2012/07/inside-blackhole-exploits-kit-v124.html
44 http://www.kahusecurity.com/2012/analyzing-a-new-exploit-pack/
45 https://blog.avast.com/2012/08/30/blackhats-adopt-latest-java0day
46 http://www.kahusecurity.com/2012/neosploit-gets-java-0-day/
47 http://malware.dontneedcoffee.com/2012/10/newcoolek.html

CVE-2012-4681 타임라인

앞서 언급된 두 취약점과는 달리 이 취약점은 제로 데이 취약점이며, 2012년 8월 말에 이 취약점을 이용한 공격이 발견되었습니다.[48] 그리고 바로 며칠 후, Oracle이 패치를 배포하기도 전에 Blackhole[49] 개발자는 제로 데이 공격이 해당 공격 키트에 통합되었다고 발표했습니다. 며칠 후, 패치되지 않은 취약점에 대한 공격 코드가 Sakura[50], RedKit[51], Sweet Orange[52] 및 Neosploit 공격 키트에 통합된 것이 발견되었습니다. CrimeBoss[53] 및 Cool 공격 키트도 마찬가지였습니다.

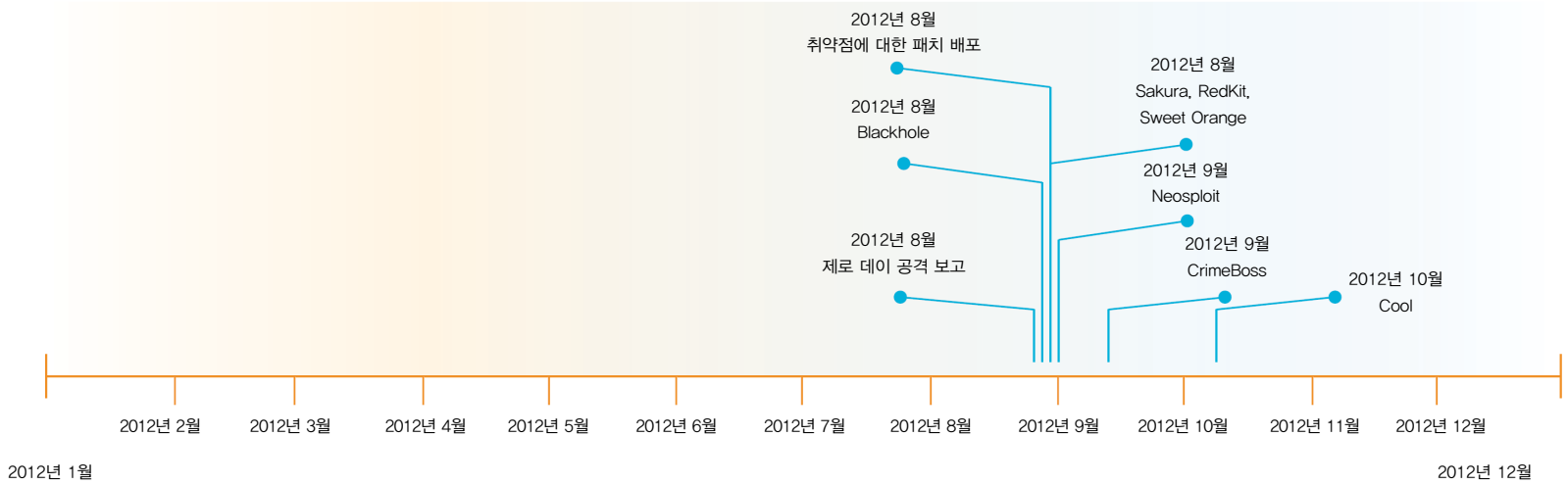


그림 15: CVE-2012-4681 타임라인

48 http://blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html
49 http://malware.dontneedcoffee.com/2012/08/java-0day-cve-2012-4681-update.html
50 http://malware.dontneedcoffee.com/2012/08/cve-2012-4681-on-its-way-to-sakura.html
51 http://malware.dontneedcoffee.com/2012/08/cve-2012-4681-redkit-exploit-kit-i-want.html
52 http://malware.dontneedcoffee.com/2012/08/cve-2012-4681-sweet-orange.html
53 http://www.kahusecurity.com/2012/crimeboss-exploit-pack/

Java 공격에 대한 관심의 증가

앞서 언급한 타임라인을 살펴보면 Java 공격이 공격 키트에 도입되는 정도를 확실히 파악할 수 있습니다. 공격 코드를 이용할 수 있거나 취약점의 상세 정보가 공개된 후 2~3개월 이내에 3개에서 4개의 공격 키트에 해당 Java 공격이 통합되며, 이러한 취약점이 제로 데이 공격일 경우 그 수는 더 증가합니다.

2012년에는 CVE-2012-1875, CVE-2012-4969와 같은 다른 제로 데이 취약점이 발견되었으며, 이 두 가지 취약점은 모두 Internet Explorer의 취약점이고 공격 코드가 공개되었습니다. 그러나 공격 키트 개발자로부터 Java 취약점과 같은 수준의 관심을 받지는 못했습니다.

왜 Java인가?

공격 키트 개발자가 공격 키트에 Java 공격을 우선적으로 포함시키는 이유는 가능한 한 가장 많은 수의 시스템을 감염시킨다는 대규모 공격 키트의 목적을 살펴보면 설명이 가능합니다. Java는 다음과 같은 중요한 특성을 지니고 있어 Java 공격은 확실히 공격 키트의 목적에 부합합니다.

1. **신뢰할 수 있는 공격**. Java의 취약점, 특히 논리적 취약점을 대상으로 개발된 공격을 실행하면 Java 가상 머신(JVM) 샌드박스 우회가 가능하며, 매우 신뢰성이 높고, ASLR(Address Space Layout Randomization), DEP(Data Execution Prevention) 및 다양한 메모리 보호 메커니즘과 같은 최신 운영 체제에 포함된 공격 완화 장치를 피하기 위한 작업이 필요없습니다. 따라서, JVM 샌드박스 우회를 통해 대규모의 시스템 공격을 할 때 높은 성공률을 보장할 수 있습니다.

2. **샌드박스를 이용하지 않은 플러그인**. Java 플러그인은 선호도가 높은 공격 대상이며, 그 이유는 프로세스 샌드박스를 이용하지 않고 실행되기 때문입니다. 즉, 공격을 통해 Java 플러그인이 훼손되면 공격자는 별도의 권한 상승 취약점을 이용하지 않고도 시스템에 계속해서 악성코드를 설치할 수 있습니다. 이는 현재 샌드박스에서 실행되는 Adobe Reader 및 Adobe Flash Player와 같은 다른 유명 플러그인과는 대조되는 점입니다. 공격 키트 개발자의 입장에서, 이러한 특징은 공격을 받은 시스템에 지속적으로 쉽게 악성코드를 설치할 수 있는 경로를 제공합니다.

3. **다양한 브라우저 및 여러 플랫폼**. 취약점이 있는 Java 플러그인이 설치된 모든 브라우저는 잠재적인 공격 대상이 될 수 있습니다. 이는 매우 많은 수의 시스템이 공격받을 수 있다는 것을 의미합니다. 또한, Java는 다양한 운영 체제에서 이용 가능하므로, 여러 플랫폼에 대한 공격의 기회를 제공하기도 합니다. 바로 이 점이 관심을 가질 만한 요소이며, 그 이유는 이 방법이 자동 다운로드(drive-by download)를 통해 Mac OS X 플랫폼을 공격할 수 있는 주요 방법 중 한 가지이기 때문입니다. 이러한 공격의 한 가지 예는 **IBM X-Force 2012년 상반기 동향 및 위험 보고서**에서 다루었던 Flashback 악성코드의 출현입니다.

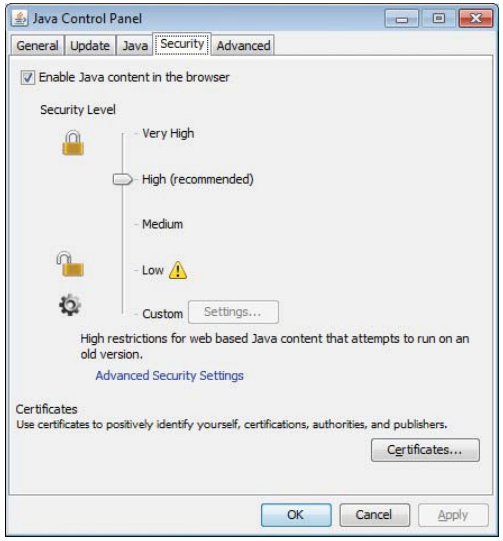
브라우저에 설치된 서명되지 않은 Java 애플리케이션을 실행하기 전에 기본적으로 사용자에게 경고하도록 수정된 최근의 Java 업데이트는 공격자가 Java 공격에 관심을 덜 가지도록 하는 바람직한 조치입니다. 또한, 오래된 플러그인의 로딩을 비활성화하거나 방지하기 위해 Mozilla(Firefox 브라우저), Google(Chrome 브라우저) 및 Apple(OS X 운영 체제) 같은 브라우저 및 운영 체제 벤더가 실행한 조치는 이미 패치된 취약점에 대한 공격을 예방하기 위한 또 다른 훌륭한 접근법입니다.

결론 및 조치사항

Java 샌드박스 우회 사례가 급증함에 따라 보안 연구가 및 악성코드 공격자 모두는 Java 샌드박스 구현을 자세히 관찰하여 유사한 결함을 찾아내야 할 것입니다. 반면, Java 취약점은 현재 공격 키트의 성공에 영향을 미치는 핵심 구성요소 중 하나이므로 공격 키트 개발자는 아마도 지속적으로 이러한 Java 취약점을 주시할 가능성이 높습니다.

공격을 받는 입장에서는, 대규모 공격 키트 개발자의 다음 행보가 무엇인지에 상관없이 공격에 대한 준비를 해야 합니다. 따라서, 최신 버전의 브라우저 및 브라우저 플러그인을 이용할 뿐만 아니라, 공격 키트를 이용한 공격을 방해할 수 있는 다음과 같은 추가적인 조치를 취해야 합니다.

- **공격 가능성을 줄이십시오.** 브라우저 플러그인이 꼭 필요한지 평가하십시오. 꼭 필요하지 않은 경우에는 플러그인을 삭제하여 공격 가능성을 줄이십시오.



Java 제어판의 보안 탭

특히 Java의 경우, 데스크톱의 독립형 애플리케이션을 실행하는 데 Java가 필요하지만 브라우저에서 Java 애플리케이션을 실행할 필요가 없을 때에는 Java 7u10을 이용하면 Java 제어판(스크린샷 참조) 보안 탭의 "브라우저의 Java 콘텐츠 사용" 옵션의 체크를 해제하여 Java 애플리케이션(서명된 애플리케이션 및 서명되지 않은 애플리케이션)이 브라우저에서 실행되는 것을 방지할 수 있습니다. 오래된 버전의 Java를 이용하는 경우, US-CERT에서 공개한 다양한 브라우저에서 Java를 비활성화하는 방법의 목록[54]을 참조하시기 바랍니다.

- **클릭 투 플레이(Click-to-Play) 활성화.** 이용 중인 브라우저가 클릭 투 플레이를 지원하는 경우, 이를 활성화하십시오. 클릭 투 플레이를 이용하면 플러그인을 활성화하기 전에 사용자가 추가적인 동작을 수행해야 하므로, 자동으로 또는 "조용히" 실행되는 브라우저 플러그인 공격을 방지할 수 있습니다.
- **서명되지 않은 애플리케이션의 보안 수준을 설정하십시오.** 특히 Java의 경우, 브라우저에서 꼭 Java 애플리케이션을 실행해야 할 때에는 Java 7u10을 이용하면 Java 제어판(스크린샷 참조)에 포함된 보안 수준 슬라이더를 이용해 서명되지 않은 Java 애플리케이션을 브라우저에서 실행하는 방법을 설정할 수 있습니다. 상황에 따라 보안 수준을 "높음" 또는 "매우 높음"으로 설정하시기 바랍니다. Java 7u11의 기본값인 "높음"으로 설정된 경우, 서명되지 않은 Java 애플리케이션을 실행할 때는 사용자의 확인이 필요합니다. "매우 높음"으로 설정하면 서명되지 않은 Java 애플리케이션이 브라우저에서 실행되는 것을 자동으로 방지합니다. 새로운 보안 수준에 대한 자세한 내용은 Orace 웹사이트의 "Java 클라이언트의 보안 수준 설정"[55] 페이지에서 확인할 수 있습니다.

54 http://www.kb.cert.org/vuls/id/636312#solution
55 http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/client-security.html

일반적으로 Java 및 브라우저 플러그인 악용에 대한 방어 장치를 추가하기 위한 소프트웨어 벤더들의 여러 가지 노력에 공격 방법 개발자 및 공격 키트 개발자가 어떻게 대응하는지 확인하는 것은 흥미로울 것입니다. 공격 가능성을 줄이고, 소프트웨어를 최신 버전으로 유지하고, 브라우저 및 브라우저 플러그인이 제공하는 보안 기능을 이용하면 앞으로의 공격에 더욱 확실히 대비할 수 있을 것입니다.

웹 컨텐츠 동향

IBM Content 데이터 센터는 새로운 웹 컨텐츠를 지속적으로 검토하여 분석하고 있으며 매달 1억 5000만 건의 신규 웹 페이지 및 이미지를 분석하고 있습니다. 데이터 센터는 1999년 이후 190억 건의 웹 페이지 및 이미지를 분석하였습니다.

IBM 웹 필터 데이터베이스는 69가지의 필터 범주와 7,500만 건의 항목을 갖추고 있으며, 매일 150,000건의 신규 또는 업데이트 항목이 추가되고 있습니다.

이 단원에서는 다음 주제에 대하여 검토해 봅니다.

- 분석 방법론
- 웹사이트에 IPv6 도입
- 컨텐츠 범주별 인터넷 사용 현황
- 소셜 네트워크의 인터넷 침투

분석 방법론

IBM X-Force는 IBM 보안 시스템 웹 필터 데이터베이스의 분류 기준에 따라 호스트 수를 산정하여 인터넷 상의 컨텐츠 배포에 관한 정보를 수집합니다. 호스트 수 산정은 컨텐츠 배포를 확인하는 적절한 방법이며 실질적인 평가를 제공합니다. 웹 페이지 및 하위 페이지 수 산정 등의 방법을 사용할 경우에는 결과가 달라질 수 있습니다.

웹사이트에 IPv6 도입

웹사이트의 IPv6 도입률을 측정하기 위해, X-Force는 매주 수백 만 개의 호스트에 대한 DNS 요청(DNS의 AAAA 레코드 대조용)을 실시했습니다. 할당할 수 있는 IPv4 주소가 거의 없는 상태이기 때문에, IPv6 주소로 전환하는 사이트의 수가 갈수록 늘어날 전망입니다. 가장 유명하고 많이 이용되는 웹사이트[56] 분석에 중점을 두어 이들 중 몇 개의 웹사이트가 이미 IPv6를 도입했는지 확인했습니다.

- 가장 많이 이용되는 상위 100개 웹사이트 중 22%가 IPv6 도입 준비를 마쳤습니다.
- 가장 많이 이용되는 상위 1,000개 웹사이트 중 거의 10%가 IPv6 도입 준비를 마쳤습니다.
- 가장 많이 이용되는 상위 10,000개 웹사이트 중 4.5% 이상이 IPv6를 제공합니다.

따라서, 가장 많이 이용되는 웹사이트에서의 IPv6 도입률이 더 높을 것으로 예상할 수 있습니다.

가장 많이 이용되는 사이트 중 IPv6가 준비된 사이트의 비율

2012년 12월

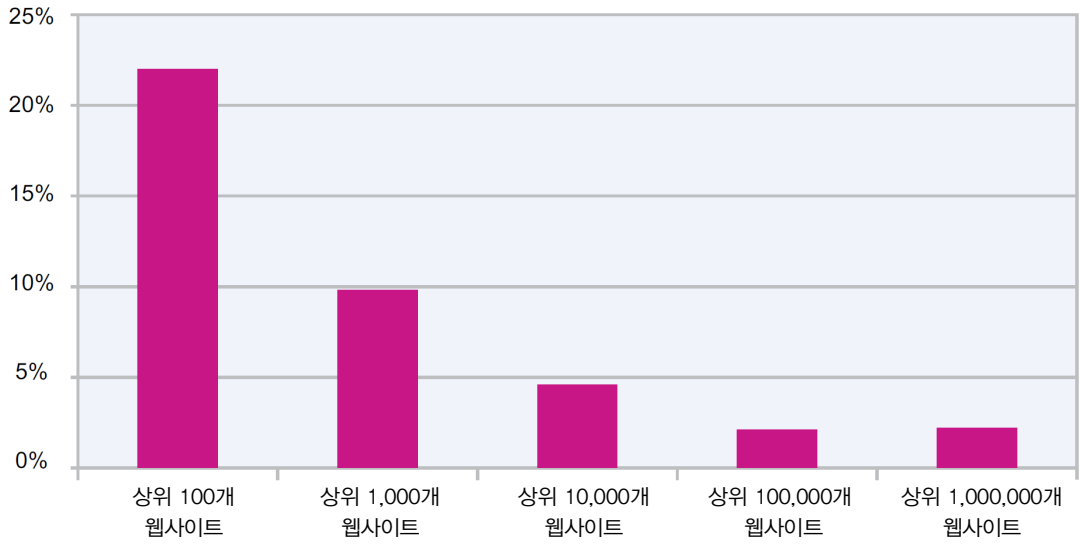


그림 16: 가장 많이 이용되는 사이트 중 IPv6가 준비된 사이트의 비율 – 2012년 12월 기준

56 Alexa가 제공한 사이트 순위: http://www.alexa.com/

또 다른 흥미로운 관점은, 최상위 도메인별 IPv6 통계치입니다. 다음 도표는 최상위 도메인별로 가장 많이 이용되는 사이트 중 IPv6가 준비된 도메인의 비율을 나타냅니다.

- 4개의 최상위 일반 도메인인 .gov(정부 조직), .edu(교육), .org(단체) 및 .com(상업)은 각각 22.2%, 12.4%, 8.6% 및 6.8%를 나타냈습니다.
- 국가 코드 최상위 도메인 중 1위인 .cz(체코 공화국)는 해당 도메인 내의 가장 많이 이용되는 .cz 사이트 중 13.4%가 IPv6 준비를 마친 도메인이었으며, .sg(싱가포르), .de(독일), .tw(타이완), .pt(포르투갈) 및 .se(스웨덴)가 그 뒤를 따랐습니다.

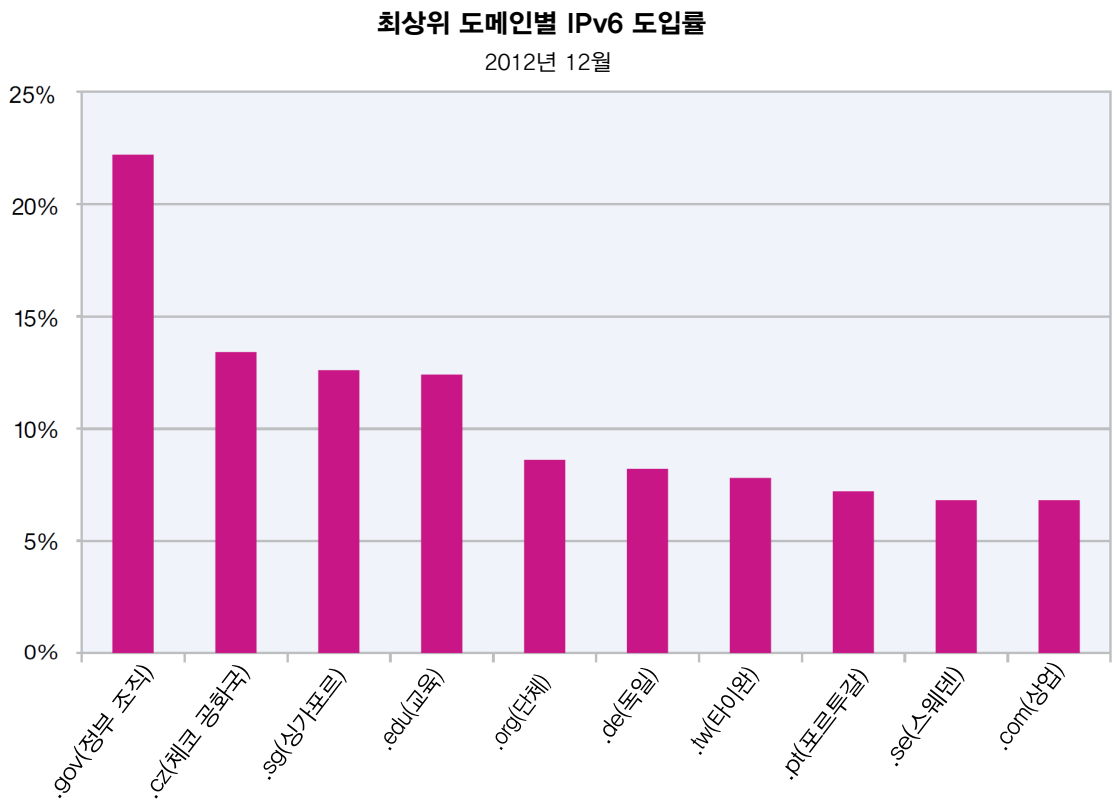


그림 17: 최상위 도메인별 IPv6 도입률 – 2012년 12월 기준

컨텐츠 범주별 인터넷 사용 현황

지난 2년 동안 개인 환경뿐만 아니라 비즈니스 환경에서도 쌍방향 웹사이트 및 웹 애플리케이션[57]의 사용이 더욱 증가했습니다. 이로 인해 직원은 소셜 네트워크 또는 웹 메일 프로그램 등의 웹 애플리케이션을 통해 모든 종류의 문서를 쉽게 공유할 수 있게 되어 새로운 보안 과제가 대두되었습니다. 예를 들면, 기밀 문서가 의도치 않게 웹 애플리케이션에 업로드될 수도 있습니다. 이 단원에서는 웹 애플리케이션 액세스의 확산성에 대해 살펴봅니다. 다른 흥미로운 관점은 악성코드가 포함된 사이트와 같은 부정한 웹사이트의 이용 비율입니다.

다음의 수치는 IBM의 필터 데이터베이스 서버로부터 수집된 수치입니다. 필터 서버는 IBM의 웹 필터 데이터베이스를 호스팅하며, IBM의 컨텐츠 필터 제품은 대부분 이 데이터베이스를 이용합니다. 이 서버는 매일 수억 건의 URL 요청을 처리합니다. 다음은 이러한 URL 요청을 기반으로 한 수치입니다.

- 전체 웹 액세스의 3분의 1 이상은 웹 애플리케이션 사이트를 통해 이루어집니다.
- 전체 웹 트래픽의 약 11%는 배너 광고로 분류됩니다.
- 쇼핑 사이트는 웹 액세스의 10%를 차지하지만, 크리스마스 직전에는 11.3%로 증가합니다.

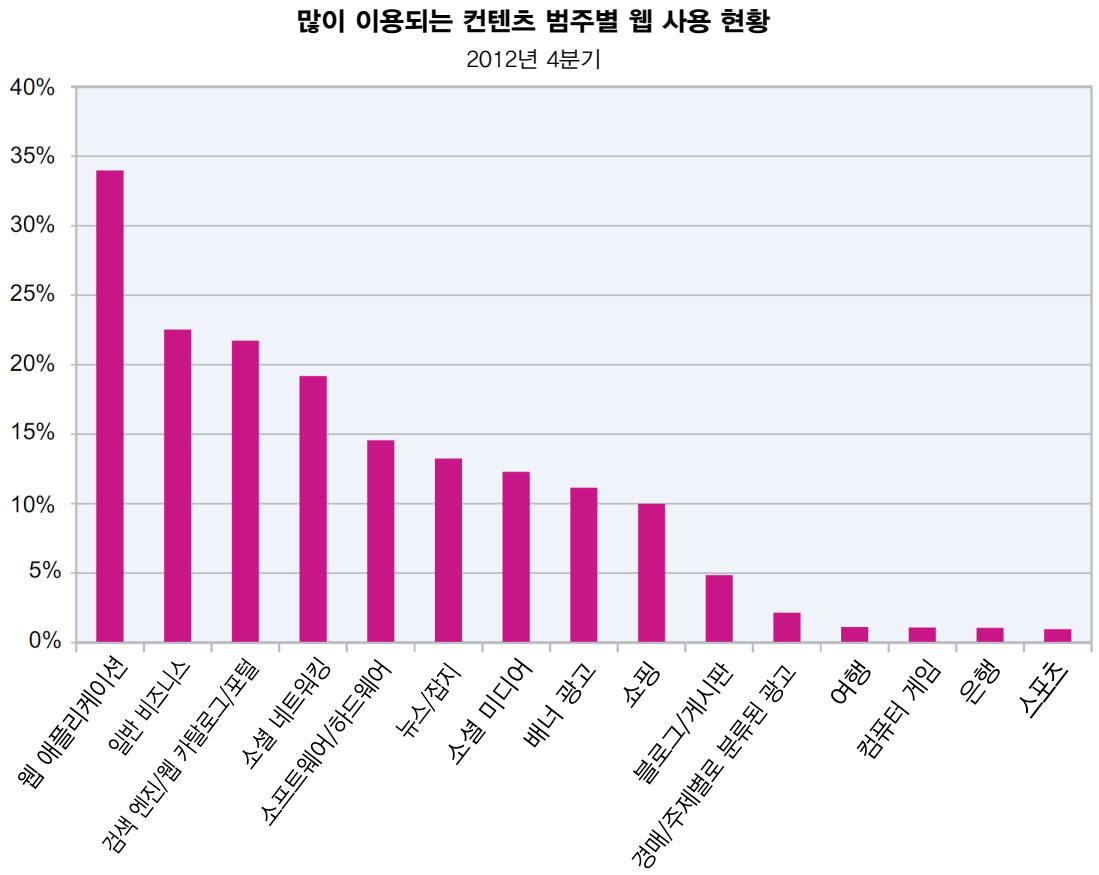


그림 18: 많이 이용되는 컨텐츠 범주별 웹 사용 현황 – 2012년 4분기

57 웹 애플리케이션은 사용자가 인터넷 또는 인트라넷과 같은 네트워크상에서 이용하는 애플리케이션을 말합니다. 일반적으로 웹 애플리케이션은 인터넷 브라우저를 통해 이용하며 파일 업로드 또는 글 게시와 같은 쌍방향 기능을 제공합니다. 대표적인 웹 애플리케이션은 소셜 네트워크, 웹 메일 프로그램 및 소셜 미디어 사이트입니다. 웹사이트는 둘 이상의 컨텐츠 범주(대부분의 소셜 네트워크는 웹 애플리케이션으로도 분류됨)에 속할 수 있으므로 전체 비율의 합은 100%보다 큽니다. 자세한 정보는 http://en.wikipedia.org/wiki/Web_application을 참조하십시오.

이전 IBM X-Force 동향 및 위험 보고서에서 유명 악성코드가 포함된 사이트는 대부분 포르노 및 도박/복권 사이트라는 사실을 확인했습니다. 이러한 범주에 속하는 사이트의 상대적인 웹 액세스 비율을 전체 웹 액세스와 비교해 보겠습니다.

- 포르노 사이트는 전체 웹 액세스 중 0.79%의 비중을 차지합니다.
- 도박 사이트에 대한 요청은 0.22%를 차지합니다.
- 악성코드가 포함된 사이트는 전체 웹 액세스 중 0.17%를 차지합니다.
- 익명 프록시는 여전히 0.07%를 차지합니다.

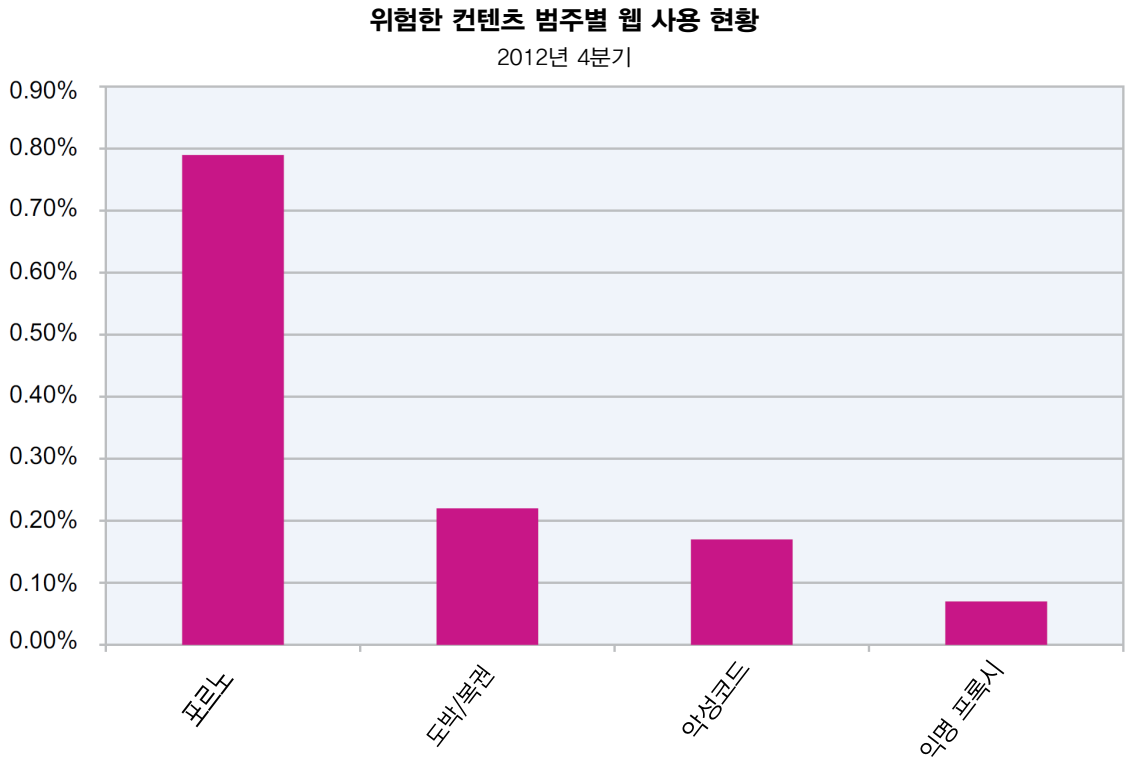


그림 19: 위험한 컨텐츠 범주별 웹 사용 현황 – 2012년 4분기

소셜 네트워크의 인터넷 침투

가정, 직장 및 학교 생활에서 소셜 네트워크가 점차 중요한 비중을 차지하고 있는 상황에서 인터넷상에서의 소셜 네트워크의 침투에 대해 살펴보겠습니다. 현재 인터넷 사이트에 포함된 소셜 네트워크에 대한 링크 수를 확인하면 인터넷 침투 활동을 측정할 수 있습니다. 소셜 네트워크에 연결된 링크 수를 측정하기 위해, 모든 웹 도메인을 살펴본 후 소셜 네트워크에 연결된 링크를 하나 이상 포함한 사이트의 수를 산정했습니다.

- 모두가 예상하는 바와 같이, 가장 많이 이용되는 상위 10개의 웹사이트[58]는 모두 소셜 네트워크에 대한 링크를 포함하고 있습니다.
- 상위 100만 개의 가장 많이 이용되는 웹사이트 중 48%는 소셜 네트워크로 연결됩니다.
- 알려진 모든 웹사이트 중 13%는 하나 이상의 소셜 네트워크로 연결됩니다.

인터넷 전반에서 소셜 네트워크의 급속한 확산은 기밀 정보의 공유를 통제해야 하는 기업에 새로운 과제로 대두되고 있습니다. 인터넷을 이용할 수 있는 모든 직원은 소셜 네트워크 사이트에 노출될 것이며, 소셜 네트워크는 이용 빈도가 매우 높으므로 이미 사기 및 피싱의 주요 대상이 되었습니다(다음 단원 참조).

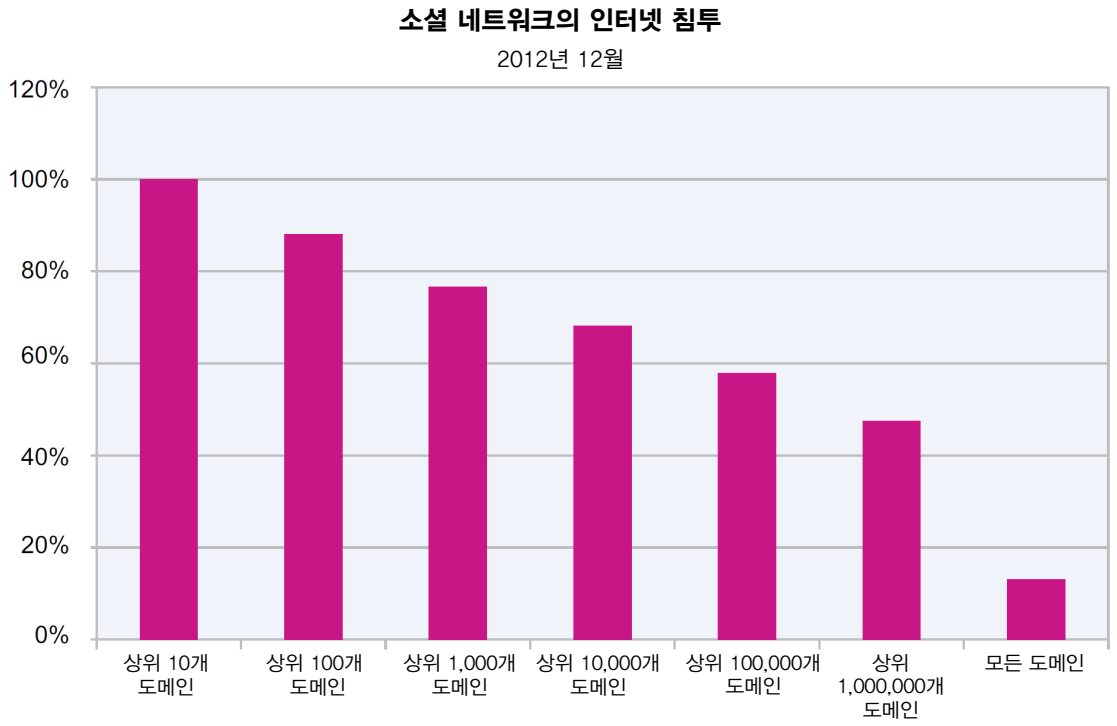


그림 20: 소셜 네트워크의 인터넷 침투 – 2012년 12월 기준

58 Alexa가 제공한 사이트 순위: http://www.alexa.com/

스팸과 피싱

IBM 스팸 및 URL 필터 데이터베이스는 스팸과 피싱 공격에 대한 폭넓은 시야를 제공합니다. 수백만 개의 이메일 주소가 감시되는 동안에도 공격자가 사용하는 스팸 및 피싱 기술은 다양하게 발전해 왔습니다.

현재, 스팸 필터 데이터베이스에는 4천만 개 이상의 관련 스팸 시그니처가 저장되어 있습니다. 각각의 스팸은 몇 가지 논리적 부분(문장, 단락 등)으로 나뉘어집니다. 128비트의 고유 시그니처는 각 부분 및 수백만 개의 스팸 URL을 대상으로 산출됩니다. 현재 매일 백만 개 정도의 시그니처가 스팸 필터 데이터베이스에 신규 등록되거나 업데이트 또는 삭제되고 있으며, 업데이트는 5분 단위로 제공됩니다.

이 단원에서는 다음 주제에 대해 살펴봅니다.

- 2012년 하반기, 스팸의 양 소폭 증가
- 주요 스팸 동향
- 이메일 사기 및 피싱
- 스팸—발송 국가[59] 추세
- 봇넷 근절에 대한 공격자의 대응

2012년 하반기, 스팸의 양 소폭 증가

2012년 초여름에는 3년 이상의 기간 중 가장 낮은 수준의 스팸이 발송되었습니다. 그 후 2012년 9월까지 스패머는 스팸 발송량을 3분의 1이상 증가시켰습니다. 2012년 10월에는 스팸 양이 다시 하락했지만 하락 폭은 크지 않았으며, 스팸 양은 여전히 2012년 상반기에 비해 20% 이상 많았습니다.

이러한 수치를 통해 스팸 관련 활동은 많지 않다는 것을 확인할 수 있습니다. 다음 단원에서는 이와 반대의 상황이 나타납니다.

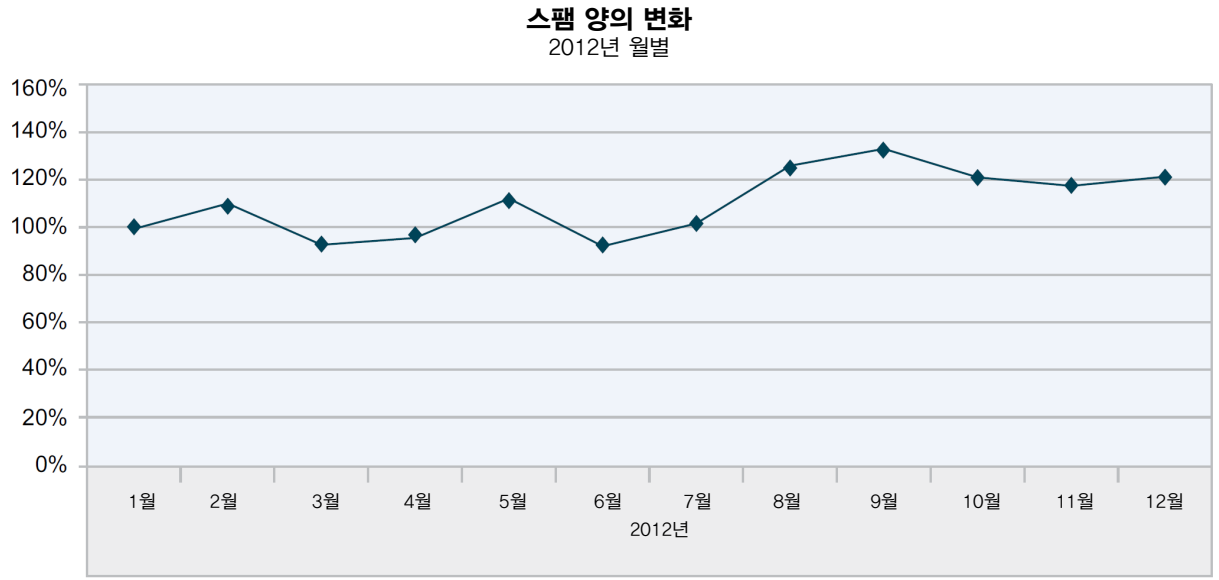


그림 21: 2012년 월별 스팸 양의 변화

59 이 보고서에 포함된 스팸, 피싱 및 URL에 관한 통계 자료는 5곳의 인터넷주소자원 관리기관(ARIN, AfriNIC, APNIC, RipeNCC, LacNIC)으로부터 직접 전달된 IP-to-County 정보를 이용합니다. 지리적 분포는 해당 IP-to-County 정보와 관련된 호스트(컨텐츠 분포의 경우) 또는 메일 발송 서버(스팸 및 피싱의 경우)의 IP 주소를 요청하여 결정했습니다.

주요 스팸 동향

그림 22에는 2011년부터 X-Force가 관측한 스팸과 관련된 주요 동향이 네 가지 매개변수를 기준으로 요약되어 있습니다.

- **이미지 스팸**: 2010년 말, X-Force는 이미지 기반 스팸의 양이 일시적으로 회복된 것을 발견했습니다. 이후에 이미지 기반 스팸의 양은 다시 감소했습니다.
- **ZIP/RAR 스팸**: 스패머는 확실히 지난 2년 동안 ZIP/RAR 스팸 접근법을 반복적으로 이용했습니다. 그렇다면 "ZIP/RAR 스팸의 양이 감소했을 경우에는 스패머가 어떤 방법을 이용하는가?"라는 의문이 생깁니다. 이 질문에 대한 대답은 악성코드를 첨부 파일의 형태로 제공하는 대신 간단하게 링크의 형태로 제공한다는 것입니다. 링크를 클릭하면 첨부 파일을 클릭할 때와 유사한 결과가 발생합니다. 스팸의 양이 증가함에 따라 스패머는 이러한 유형의 스팸을 이용했으며 특히, 2012년 11월에 급격한 증가가 나타났습니다.
- **스팸의 평균 바이트 크기:** 지난 2년 동안 스팸의 용량은 지속적으로 증가했습니다. 그러나, 특히 ZIP/RAR 스팸의 발송량이 많았을 때는, 스팸의 바이트 크기 또한 컸습니다. 결과적으로 스팸의 용량을 확인하여 스패머가 악성 코드가 첨부된 스팸 발송 작업을 확대하고 있다는 것을 다시 한 번 확인할 수 있습니다.
- **발신자와 수신자가 동일한 스팸**: 수신자와 동일한 도메인의 가짜 발신자 이메일 주소를 갖는 스팸을 발송하는 것은 스패머가 간헐적으로 이용하는 방식입니다. 이러한 스팸의 비율은 지난 2년 동안 0%부터 거의 50%까지 다양하게 변화했습니다. 스패머는 동일한 기업에서 발송한 것으로 착각되는 이메일을 누군가가 읽거나 신뢰하기를 아직도 기대하고 있을지도 모릅니다.

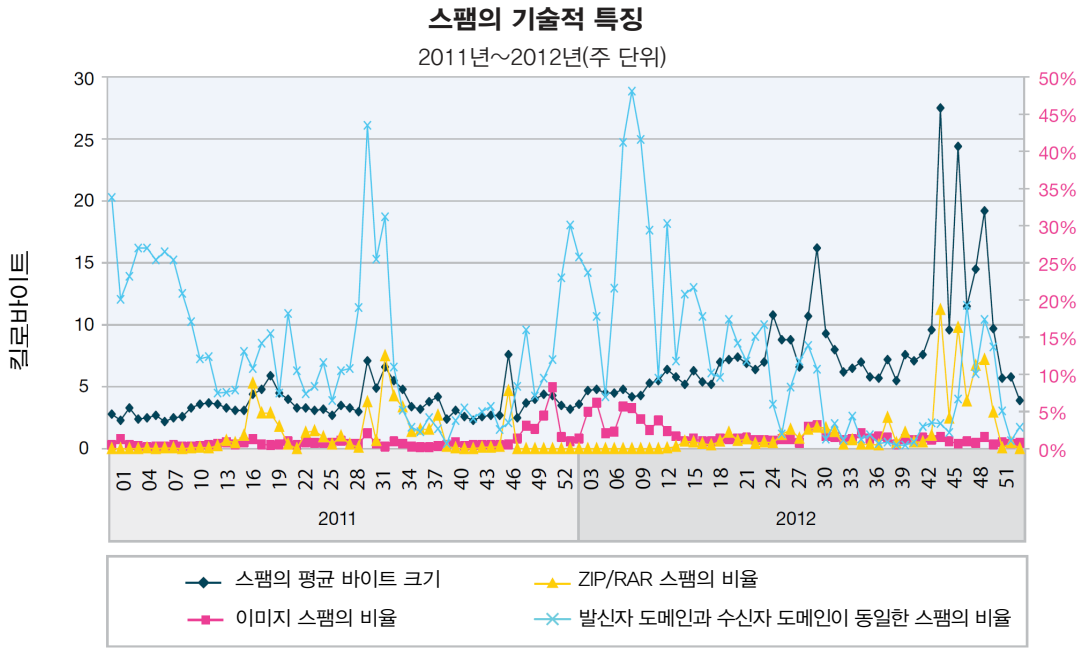


그림 22: 스팸의 기술적 특징 – 2011년~2012년(주 단위)

이메일 사기 및 피싱

방법론

이메일 사기 및 피싱의 최신 동향을 파악하기 위해 다음과 같은 방법을 이용했습니다.

- 통계치는 이메일을 통해 발송된 사기 및 피싱만을 기준으로 합니다.
- 통계치에는 신뢰할 수 있는 잘 알려진 브랜드 이름을 이용해 사용자가 첨부 파일 또는 링크를 클릭하도록 유도하는 모든 이메일이 포함되며, 이러한 첨부 파일 또는 링크가 피싱과 관련이 없는 경우도 포함됩니다. 따라서, 여기에 포함되는 이메일 중 일부는 피싱은 아니지만 "피싱과 유사한" 이메일일 수도 있습니다.
- 통계치는 자동 다운로드를 통해 설치된 피싱 악성코드를 기록하는 키스트로크 등 이메일과 관련이 없는 피싱 시도를 포함하지 않습니다.

사기 및 피싱의 통계치를 제공하기 위한 방법론에 대한 자세한 정보는 IBM X-Force 2011년 동향 및 위험 보고서의 관련 단원에서 확인할 수 있습니다.

이메일 사기 및 피싱의 최근 동향

앞서 언급한 방법론을 고려하면, 2008년과 2012년 사이의 (스팸 및 사기/피싱 모두에 대해 2008년은 100%의 양을 기준으로 함) 스팸의 양과 이메일 사기 및 피싱의 양에 큰 차이가 있다는 것을 확인할 수 있습니다.

- 2008년부터 2010년까지 스팸의 양은 거의 2배로 증가했습니다.
- 2008년부터 2010년까지 이메일 사기/피싱의 양은 크게 감소하여 2008년의 약 4분의 1 수준으로 감소했습니다.
- 2010년부터 2011년까지 스팸의 양은 거의 절반으로 감소했으며, 2011년부터 2012년까지 더 감소했지만 감소폭은 크지 않았습니다.
- 2010년부터 2012년까지 이메일 사기/스팸의 양은 그 직전의 수준에 비해 8배 이상 증가했습니다.

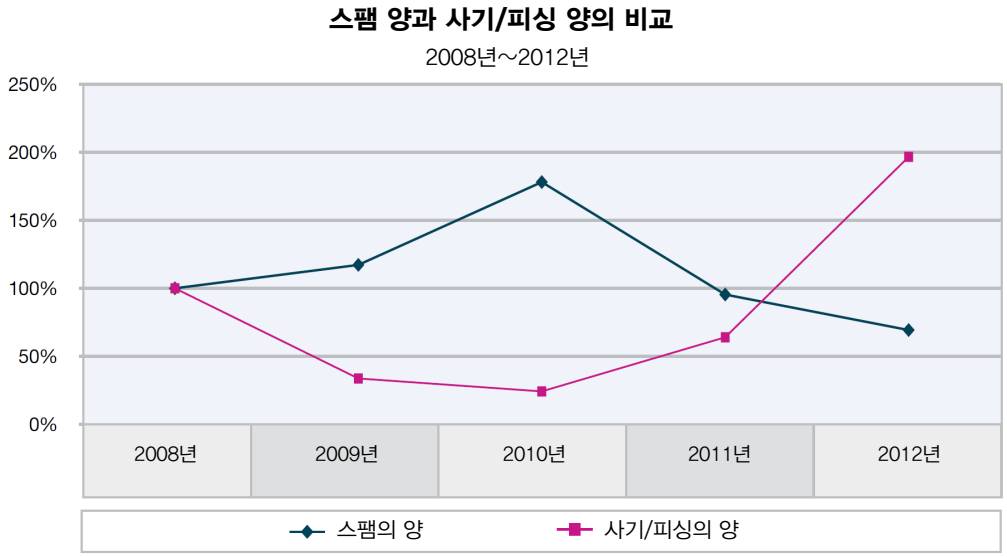


그림 23: 스팸의 양과 사기/피싱의 양의 비교 – 2008년~2012년

결론적으로 말해, 스팸의 양과 사기 및 피싱의 양은 서로 반대되는 움직임을 나타냈습니다. 스팸 양의 변동은 크지 않았지만, 기존의 스팸으로부터 이메일 사기로 전환하는 추세는 두드러졌습니다.

이메일 사기 및 피싱의 유형을 살펴보면 좀 더 흥미로운 추세를 확실히 파악할 수 있습니다.

이메일 사기 발생 횟수가 수차례 상승 및 하락한 것을 통해, 사기 이메일 발송자가 공격 대상을 "순환"시키고 있다는 것을 유추할 수 있습니다. 또한 2012년에는 비영리 기관, 소셜 네트워크, 운송 서비스 업체, 온라인 상점의 모조된 확정서 및 송장, 스캐너 및 팩스 사기(예: "기업의 eFax 메시지")에 중점을 두어 사기 이메일을 발송했습니다. 대부분의 경우 이러한 사기 이메일에는 위에서 언급한 ZIP 첨부 파일이 포함되어 있습니다.

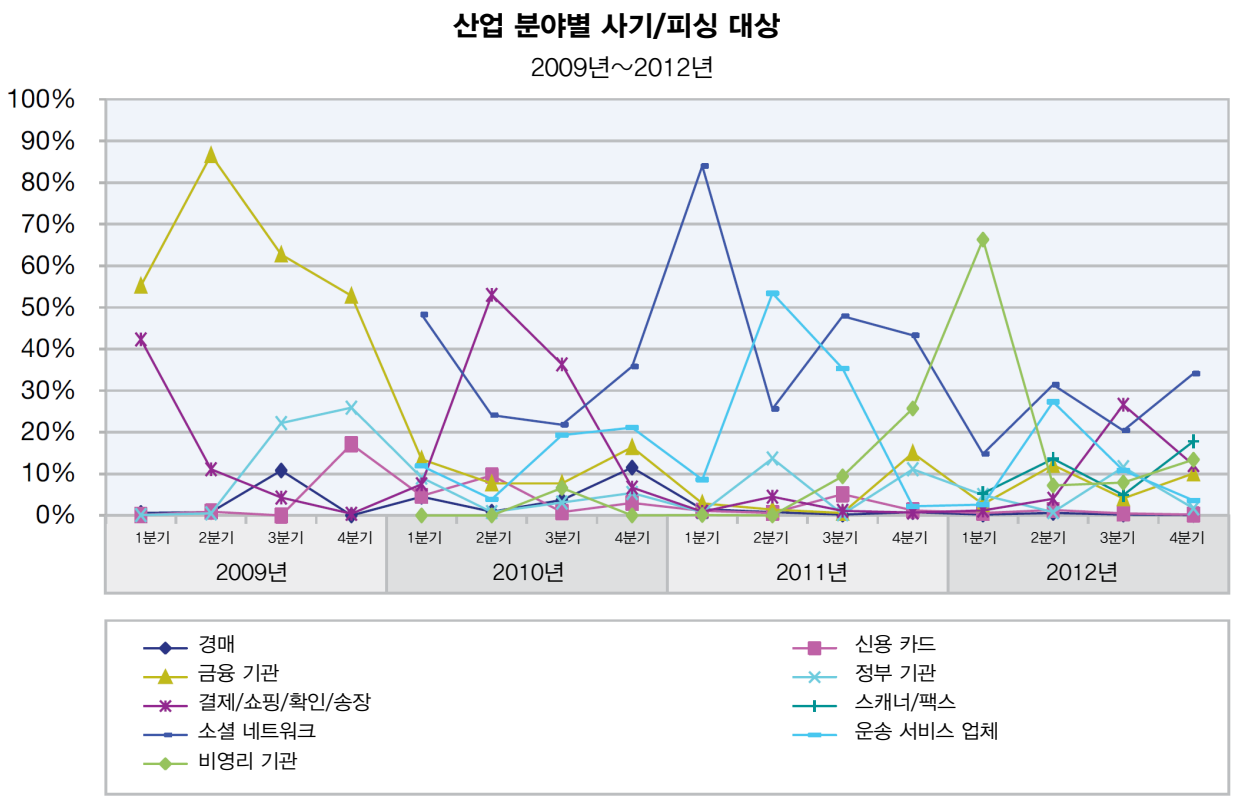


그림 24: 산업 분야별 사기/피싱 대상 – 2009년~2012년[60]

60 소셜 네트워크, 운송 서비스 업체 및 비영리 기관 관련 수치는 2010년부터 기록된 것이며, 스캐너/팩스 관련 수치는 2012년부터 기록되었습니다.

스팸—발송 국가 추세

지난 2년간 가장 많은 스팸을 발송한 국가를 살펴보면, 다음과 같이 흥미로운 장기적인 추세를 확인할 수 있습니다.

- 인도는 2012년 가을에 전체 스팸의 20% 이상을 발송하여 큰 차이로 1위를 기록했습니다. 이는 인도의 인터넷 사용자 수가 지난 12개월 동안 24% 증가했기 때문일 수도 있습니다.[61] 한 국가에서 전체 스팸의 20% 이상을 발송한 것은 이번이 처음입니다. 2012년 말에는 11% 미만으로 감소했지만, 여전히 1위의 스팸 발송 국가로 남았습니다.
- 미국은 마지막 9달 동안 전체 스팸의 8% 이상을 발송했습니다.
- 베트남은 2011년 하반기에는 2위를 기록했지만 2012년 하반기에는 전체 스팸의 6% 미만을 발송했습니다.
- 페루와 스페인은 각각 2012년 말에 전체 스팸의 5%를 발송하여 처음으로 5위 이내에 진입했습니다.
- 사우디 아라비아는 2012년 3분기에 전체 스팸 중 거의 13%를 발송하여 2위를 기록했습니다.
- 2012년 3분기의 1위와 2위인 인도와 사우디아라비아는 각각 4분기에 10% 정도의 큰 감소를 보였습니다. 감소된 부분은 4분기에 페루와 스페인(앞에서 언급)뿐만 아니라 콜럼비아(3.4% 발송), 중국(3.3% 발송), 영국(2.7% 발송) 및 터키(2.5% 발송)가 대체했습니다.

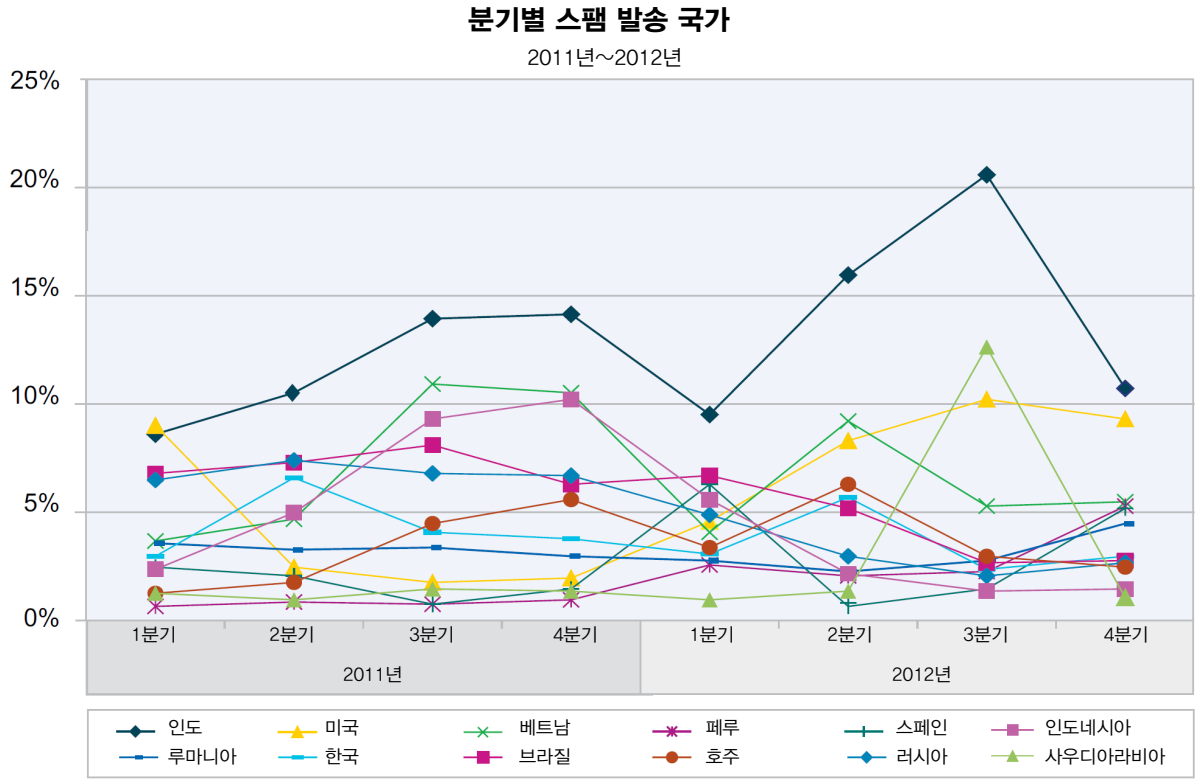


그림 25: 분기별 스팸 발송 국가 – 2011년~2012년

61 http://www.bbc.co.uk/news/business-16354076

2012년 가을에 사우디아라비아에서 사상 최대의 스팸을 발송했다는 것을 흥미로운 사실입니다. 자세한 내용을 살펴보겠습니다.

보다 짧은 기간을 기준으로 살펴보면, 사우디아라비아는 7월 중순(28주)과 9월 초(36주) 사이에 가장 많은 양의 스팸을 발송했다는 것을 확인할 수 있습니다. 8월 초(32주)에는 다른 모든 국가보다 더 많은 스팸을 발송하여 인도까지 제쳤습니다. 하지만 이후에는 어떻게 되었을까요? 사우디아라비아에서 발송한 스팸의 양은 9월 중순에 급감했습니다. 동시에, 페루와 스페인에서 발송한 스팸의 양은 2% 미만에서 3%~10%로 크게 증가했습니다. 이러한 수준은 2012년 말까지 유지되었습니다.

전체 스팸 양과 사우디아라비아, 인도, 페루 및 스페인에서 발송한 스팸 양 비교

2012년 6월~12월(주 단위)

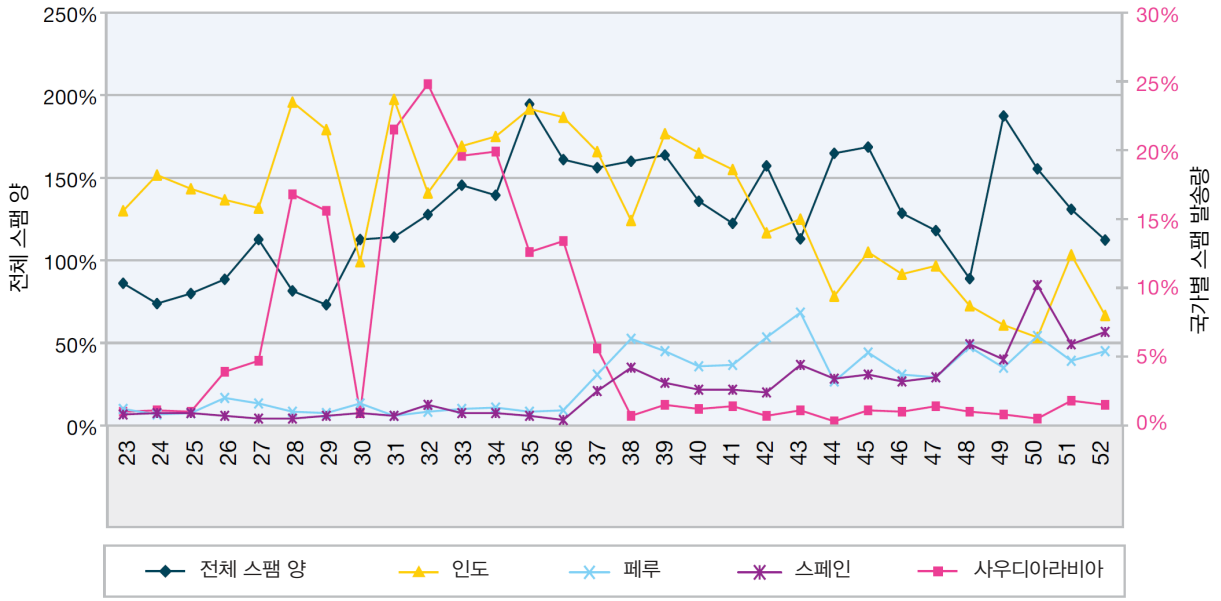


그림 26: 전체 스팸 양과 사우디아라비아, 인도, 페루 및 스페인에서 발송한 스팸 양의 비교 – 2012년 6월~12월(주 단위)

봇넷 근절에 대한 공격자의 대응

사우디아라비아에서 발송한 스팸 양의 감소와 함께, 전체적인 스팸의 양 또한 감소했다는 것을 확인했습니다. 2012년 10월의 스팸 양은 2012년 9월에 비해 12% 낮았습니다. 일부에서는 Festi 봇넷의 활동이 2012년 9월[62]에 크게 감소했다고 보고했으며, 이로 인해 사우디아라비아의 스팸 양이 감소한 것일 수도 있습니다. 만일 이것이 사실이라면, 스패머는 봇넷 근절에 대응하기 위한 방법을 찾았을 수도 있습니다. 이러한 사실은 지난 몇 년간 진행된 봇넷 근절을 살펴보면 명확해집니다.

2008년 11월에 있었던 McColo의 근절[63] 이후 스팸 양은 급격하게 75%나 감소했으며, 2년 반 후인 2011년 3월에 있었던 Rustock의 근절[64] 이후에는 스팸 양이 35% 감소했습니다. 아래 그림 27에 나타난 것과 같이, 2012년에 있었던 Grum[65] 및 Festi의 근절 이후에는 각각 27%와 12%의 스팸 양 감소만이 나타났습니다.

2012년 9월에 있었던 Festi 근절의 맥락에서 살펴보면, 스패머는 이러한 감소량을 보상하기 위해 간단하게 사우디아라비아의 봇넷 드론에서 페루와 스페인의 봇넷 드론으로 이동한 것으로 보입니다.

봇넷 근절 이후의 스팸 양 감소

2008년~2012년

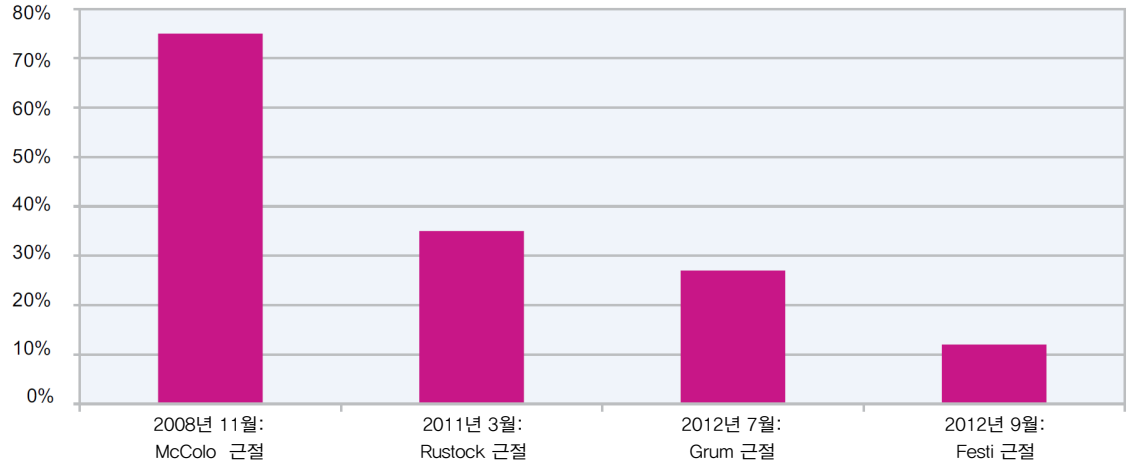


그림 27: 봇넷 근절 이후의 스팸 양 감소 – 2008년~2012년

봇넷 근절은 무엇이며 공격자는 어떻게 대응하는가?

더 자세히 설명하면, 봇넷은 공격자가 원격으로 악성 작업을 실행하는 데 이용하는 통제된 컴퓨터의 집단입니다. 봇넷은 주로 웹사이트에 대한 서비스 거부 공격, 클릭 사기, 새로운 형태의 악성 소프트웨어 배포 및 스팸 관련 활동 등의 작전을 수행하는 데 이용됩니다.

봇넷은 지금까지 중앙 집중식 C&C(command and control) 서버를 통해 운영되어 왔습니다. 과거에는, 측정 가능한 스팸 양의 감소로 나타나는 효과적인 봇넷 방지 방법은 봇넷 C&C 서버를 "근절(take down)"하는 것이었습니다.

그러나 최근의 데이터는 공격자가 이러한 전략에 대한 더욱 뛰어난 복원성을 갖게 되었다는 것을 의미할 수도 있으며, 이는 더욱 분산된 C&C 네트워크, 심지어는 다수의 봇넷 그룹을 운영할 가능성을 나타내고 있습니다. 이와 같이, 하나의 C&C 서버 또는 봇넷 그룹이 근절되면 공격자는 이미 이용되고 있는 다른 봇넷을 이용해 이에 대한 트래픽 손실을 보상하고 있습니다.

62 http://www.eleven.de/eleven-security-reports-reader.612/items/eleven-e-mail-security-report-october-2012.html
63 http://blogs.iss.net/archive/mccolo.html
64 http://blogs.iss.net/archive/RustockSpam.html
65 http://www-03.ibm.com/security/xforce/downloads.html

단원 II
운영 보안 현황

이 단원에서는 오늘날 공격자들이 노리는 프로세스, 소프트웨어, 인프라의 약점에 대해 살펴봅니다. 구체적으로 말해서, 이 단원에서는 보안 컴플라이언스의 베스트 프랙티스, 운영비 절감 아이디어, 자동화, 소유 비용 절감, 그리고 업무, 제품 및 역할 통합에 대해 논의합니다. 또한, 이러한 문제를 관리하거나 완화하는 과정에서 IBM이 얻은 정보도 소개합니다.

2012에 공개된 취약점

1997년 이후, IBM X-Force는 공개된 보안 취약점을 문서화해 왔습니다. 그 당시에는 일주일에 문서화해야 할 취약점의 수가 많지 않았습니다. 15년이 넘게 지난 지금은 일주일에 평균 150개가 넘는 취약점을 문서화하고 있습니다. 월드 와이드 웹을 조사하고, 메시지 보드와 RSS 피드를 읽고, IBM XFDB(X-Force Vulnerability Database)에 대한 데이터를 조사하는 데 수많은 인력과 시간이 투입되었습니다. IBM X-Force의 데이터베이스는 현재 70,000개의 취약점에 대한 정보를 포함하고 있으며, 지난 5년간 지속적으로 꾸준히 연간 평균 7,700개의 취약점을 문서화했습니다. 웹 애플리케이션 취약점은 아직 조사할 부분이 많습니다. XFDB의 데이터를 통해 알 수 있는 더욱 놀라운 사실 중 하나는 지난해에 보고된 XSS(cross-site scripting)의 두드러진 증가 추세입니다. 웹 애플리케이션 취약점 중 절반 이상이 XSS와 관련이 있었습니다.

2012년에는 8,168개의 취약점이 대중에 공개되었습니다. 2012년 상반기 데이터를 검토한 후 예상했던 수준의 기록은 아니지만, 이는 여전히 2011년 대비 14%의 증가를 나타냅니다. 2006년 이후에는 상승과 하락이 교차했으며, 2010년에는 총 8,730개의 취약점이 공개되어 가장 높은 수치를 기록했습니다. 그림 29는 지난 6년간 발견된 상승과 하락이 교차하는 추세를 나타내고 있습니다.

누적 취약점의 합계
1996년~2012년

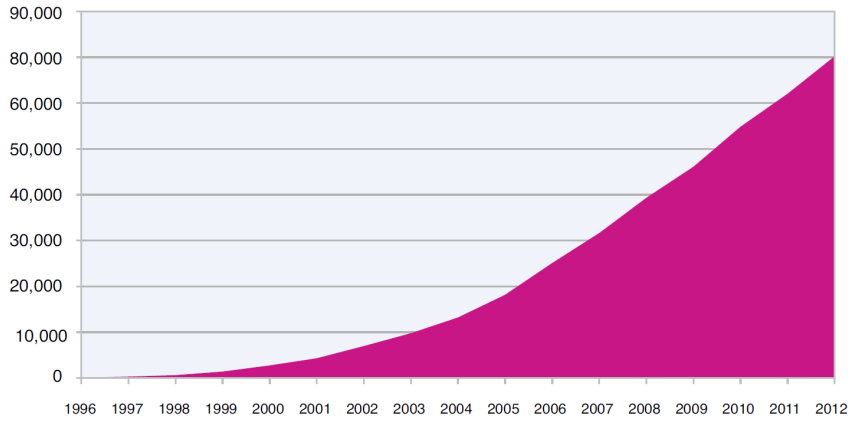


그림 28: 누적 취약점의 합계 – 1996년~2012년

연도별 취약점 공개의 증가
1996년~2012년

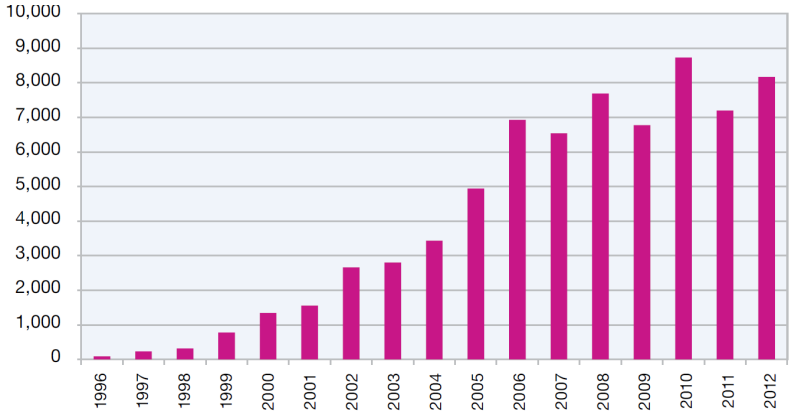


그림 29: 연도별 취약점 공개의 증가 – 1996년~2012년

웹 애플리케이션

2011년에 2,921건이 공개되었던 웹 애플리케이션 취약점은 2012년에 3,511건으로 14% 증가했습니다. XSS(Cross-site scripting) 취약점은 2012년에 공개된 모든 웹 애플리케이션 취약점 중 절반 이상을 차지했습니다. 그림 30에 나타난 것과 같이, 매년 번갈아 가며 상승과 하락이 반복되었던 전체 취약점의 수가 웹 애플리케이션 취약점의 수와 일치하는 것은 놀라운 일이 아닙니다.

IBM X-Force가 2012년에 문서화한 전체 취약점의 43%는 웹 애플리케이션 취약점인 것으로 판단되며, 다음과 같은 방법으로 분류됩니다.

XSS(Cross-site scripting): XSS 취약점은 웹 애플리케이션이 폼 필드, URL 구문 등의 사용자의 입력에 대한 유효성을 올바르게 검증하지 않을 때 발생합니다. 이러한 취약점을 이용하면 공격자는 자신의 스크립트를 사용자가 방문하는 페이지에 임베드하여 해당 페이지의 동작이나 외관을 조작할 수 있습니다. 악성 페이지 변경은 민감한 정보를 도용하거나, 웹 애플리케이션을 의도하지 않은 방식으로 조작하거나, 다른 취약점을 악용하는 페이지에 컨텐츠를 임베드하는 데 이용될 수 있습니다. 공격자는 먼저 특수하게 제작한 웹 링크를 생성해야 하며, 이후 공격 대상이 스팸, 사용자 포럼 또는 다른 방법을 통해 이 링크를 클릭하도록 유도해야 합니다. URL의 도메인 이름이 신뢰할 수 있는 또는 친숙한 기업인 경우에는 사용자가 쉽게 속아서 이 링크를 클릭할 가능성이 더 높습니다. 사용자에게는 해당 조직의 취약점을 이용한 공격이 아닌, 신뢰할 수 있는 조직 자체에서 공격 시도가 발생하는 것처럼 보일 수도 있습니다.

SQL 인젝션: SQL 인젝션 취약점 또한 사용자의 입력에 대한 유효성을 올바르게 검증하지 않는 것과 관련이 있으며, SQL 인젝션 공격은 이러한 입력(예: 폼 필드)에 SQL 명령문을 동적으로 포함시킨 후 데이터베이스에서 실행할 수 있는 경우에 발생합니다. 백엔드 데이터베이스에 대한 접근을 통해 공격자는 민감한 정보를 읽고, 삭제하고, 수정할 수도 있으며, 임의적인 코드를 실행할 수도 있습니다.

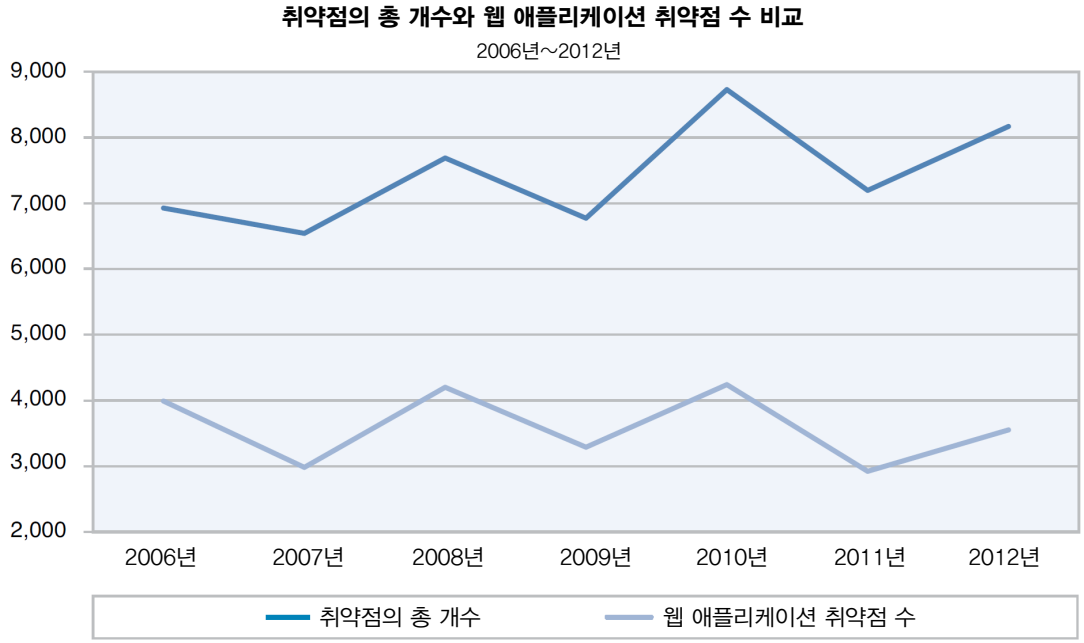


그림 30: 취약점의 총 개수와 웹 애플리케이션 취약점 수의 비교 – 2006년~2012년

공격자는 SQL 인젝션 취약점을 이용해 고객의 기밀 정보(예: 신용 카드 데이터)를 노출시킬 뿐만 아니라 데이터베이스 내에 다른 공격을 임베드할 수도 있으며, 이후 웹사이트 방문자는 이러한 데이터베이스를 이용할 수도 있습니다. 이 보고서에서 앞서 논의한 것과 같이, IBM MSS 그룹은 SQL 인젝션 공격을 고객 네트워크에 지속적으로 가장 많이 발생하는 공격 중 하나로 분류합니다.

파일 첨부: 일반적으로 PHP 애플리케이션에서 발견되는 파일 첨부 취약점은 애플리케이션이 로컬 애플리케이션에서 실행할 코드를 원격 소스로부터 검색할 때 발생합니다. 이 경우 원격 소스는 인증에 대한 유효성 검증을 받지 않으며, 그 결과 공격자는 웹 애플리케이션을 이용해 원격으로 악성코드를 실행할 수 있게 됩니다.

기타: 이 범주에는 일부 서비스 거부 공격 및 공격자가 비인가 정보를 확인하거나 획득하고, 파일, 디렉토리, 사용자 정보 또는 웹 애플리케이션의 다른 구성요소를 변경하도록 허용하는 여러 가지 기술이 포함됩니다.

XSS는 공개된 웹 취약점의 상당수를 차지합니다. 대중에 공개된 웹 애플리케이션 취약점의 53%가 XSS와 관련이 있었습니다. 이러한 수치는 그 어느 때보다 높은 수치입니다.

이러한 극적인 증가는 SQL 인젝션 취약점이 2011년보다는 증가했지만 2010년에 비해서는 크게 감소한 가운데 발생한 것입니다.

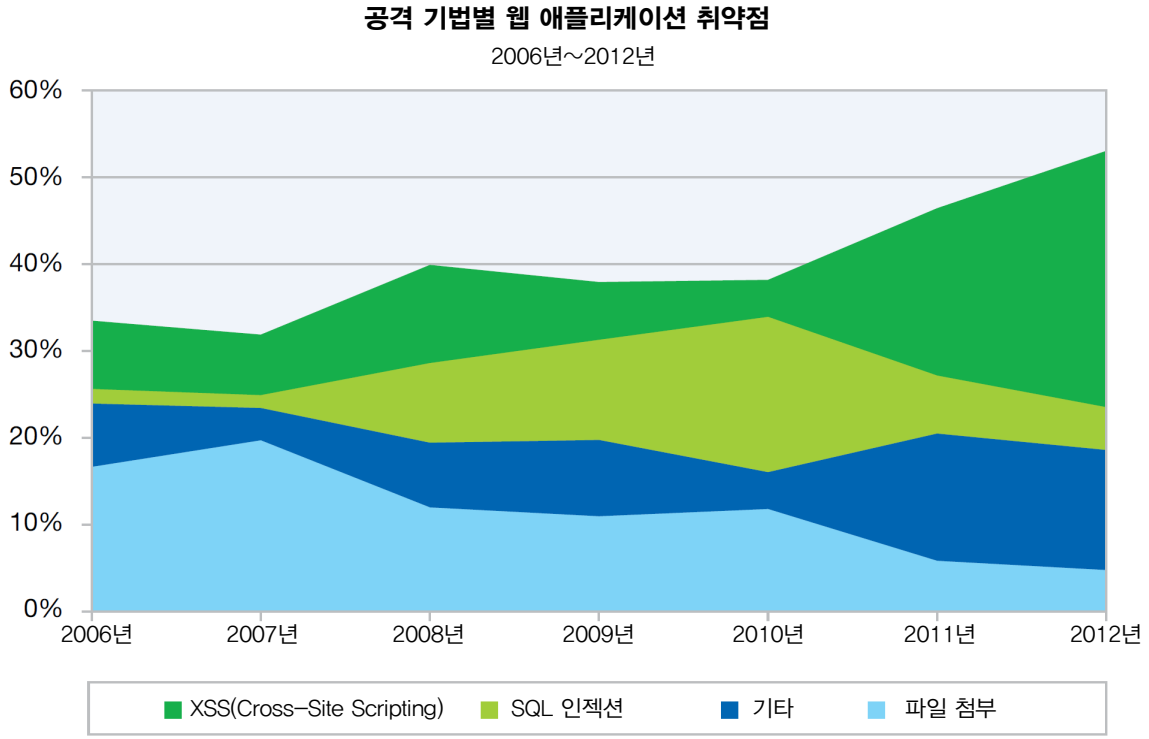


그림 31: 공격 기법별 웹 애플리케이션 취약점 – 2006년~2012년

웹 애플리케이션과 관련된 것으로 간주되는 대부분의 취약점은 공격 데이터베이스 웹사이트에 공개되어 있습니다. 이러한 취약점의 대부분은 CMS(Content Management Systems)용 제3자 추가 기능 또는 플러그인에 속합니다. CMS 프로그램은 사용의 편리성, 다목적성 및 유지보수와 관리의 간편함 덕분에 월드 와이드 웹에 가장 많이 배치된 소프트웨어 중 하나입니다. 공격자는 이러한 시스템을 공격 대상으로 삼아 악용 가능한 취약점 및 결함 찾기를 선호합니다. CMS 애플리케이션 및 플러그인은 웹에서 이용 가능하므로, 웹 애플리케이션 취약점을 식별하기 위한 자동화된 스캐닝 도구의 공격 대상이 되기 쉽습니다. 공격자는 자동화를 이용할 뿐만 아니라 직접 CMS 애플리케이션 및 플러그인을 검토하기도 합니다.

CMS 프로그램에 대한 핵심적인 취약점은 일반적으로 공격을 받은 벤더가 공개하고 수정합니다. 그러나 대부분의 추가 기능 및 플러그인은 개인 또는 제3자 기업에서 개발 및 유지보수하고 있습니다. 대규모의 CMS 벤더는 새로운 취약점이 공개되면 자사 제품에 대한 패치를 지속적으로 배포하고 유지보수하여 취약점에 잘 대처하고 있습니다. 대중에 공개된 핵심 CMS 프로그램에 대한 취약점은 공개 후 71%가 패치되었으나, 플러그인의 경우에는 51%에 그치고 있습니다.

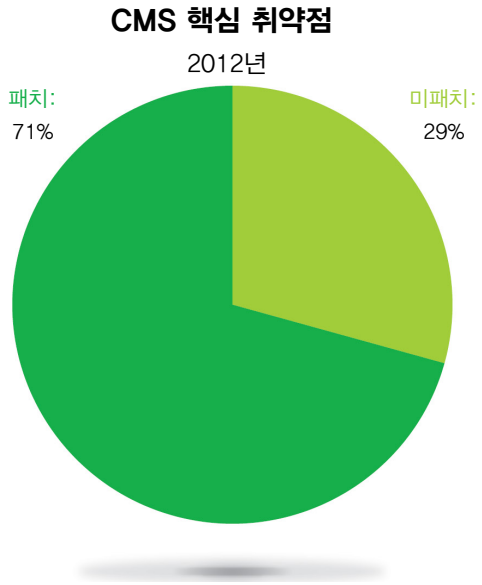


그림 32: 핵심 CMS 시스템의 공개된 취약점 – 2012년의 패치율 및 미패치율

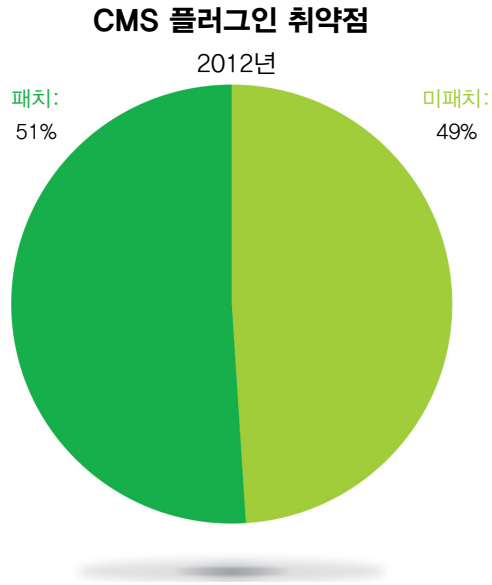


그림 33: 플러그인 CMS 시스템의 공개된 취약점 – 2012년의 패치율 및 미패치율

공격

2012년에는 공개적인 공격의 가능성이 있는 취약점이 3,436개 발견되었으며, 이러한 수치는 2012년에 발생한 공개적인 공격의 총 개수에 포함됩니다. 이러한 취약점은 전체 취약점의 42%를 차지하며, 2011년에 비해 4% 상승했습니다. IBM X-Force는 공격의 총 개수("실질적인 공격이 아닌 경우"로 분류된 공격 포함)가 취약점의 총 개수 도표에 나타난 연간 상승 및 하락 수준과 일치하는 것을 발견했습니다. 실제로, 이 두 수치는 확실히 웹 애플리케이션 취약점의 총 개수를 반영하고 있었습니다.

공격이 공개되면 일반적으로 공격에 이용되는 취약점이 노출됩니다. 웹 애플리케이션의 경우에는 특히 그러하며, 공격이 공개될 때 실질적으로 취약점이 공개됩니다.

공격에 이용된 모든 취약점 중 77%는 해당 취약점이 공개된 날에 공격이 공개되었으며, 15%의 공격은 취약점이 공개된 후 30일 이내에 공개되었습니다. 나머지 8%의 공격은 해당 취약점이 공개된 후 30일이 지나서 공개되었습니다.

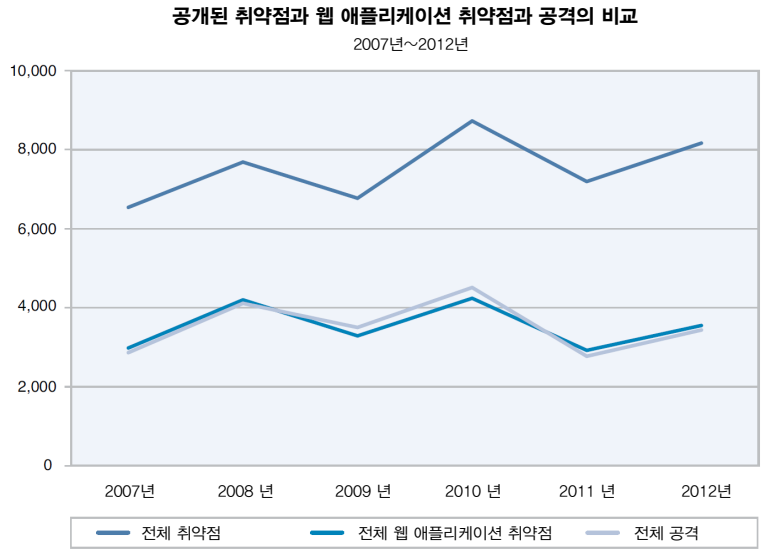


그림 34: 2007년과 2012년 사이에 공개된 취약점과 웹 애플리케이션 취약점과 공격의 비교

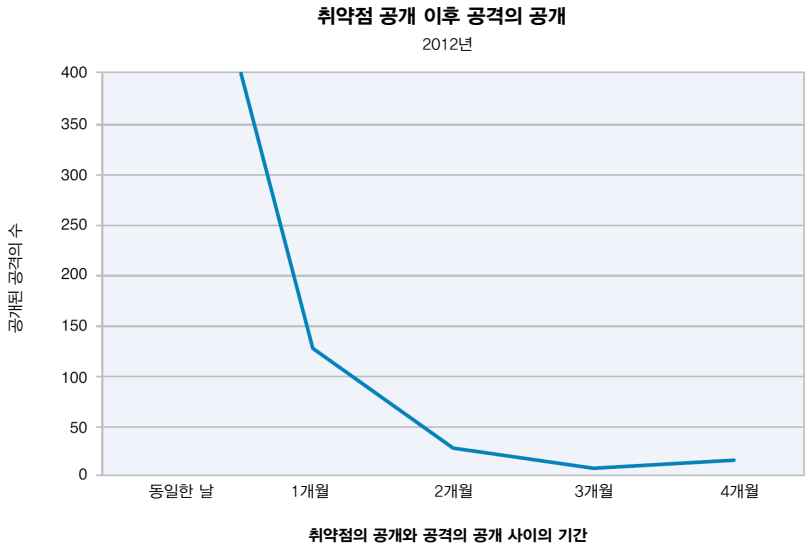


그림 35: 취약점 공개 이후 공격의 공개 – 2012년

IBM X-Force는 공격을 두 가지 범주로 분류하고 있습니다. 개념 증명 코드를 이용하는 간단한 스니펫은 공격으로 간주되지만, 컴퓨터를 공격할 수 있는 완전한 기능의 프로그램은 "실제 공격"으로 분류됩니다.

2012년 상반기 보고서에서, IBM X-Force는 연말에 전체 공격은 858건이 될 것으로 추정했습니다. 총 864건의 실제 공격이 공개되었으며, 이는 예상치를 크게 벗어나지 않은 것입니다. IBM X-Force는 이러한 공격을 표준 웹 브라우저의 주소창을 통해 악용할 수 있는 많은 수의 웹 애플리케이션 취약점을 포함하지 않는 기능적인 공격으로 정의합니다. IBM X-Force는 대중에게 공개되는 공격의 수가 지속적으로 감소할 것으로 예측했으나, 2012년의 수치는 2011년의 수치에 비해 약간 상승했지만 여전히 전체적으로 낮은 수치이며, 이는 대중에게 공개된 모든 취약점의 10.6%에 해당합니다.

	2006년	2007년	2008년	2009년	2010년	2011년	2012년
실제 공격	498	1067	1033	1061	1297	826	864
대비 비율	7.2%	16.3%	13.4%	15.7%	14.9%	10.5%	10.6%

표 1: 공개된 실제 공격 – 2006년~2012년

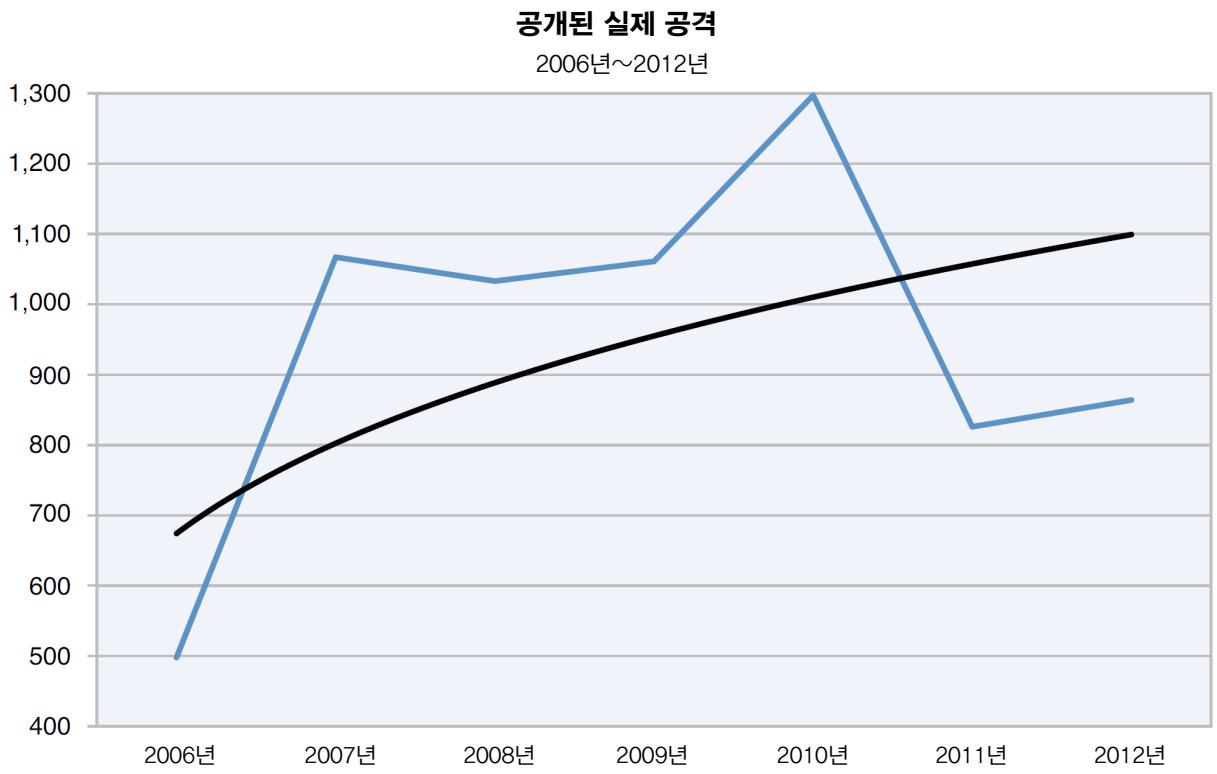


그림 36: 공개된 실제 공격 – 2006년~2012년

CVSS 스코어링

IBM X-Force는 CVSS(Common Vulnerability Scoring System)를 이용해 조사하는 모든 취약점에 심각도를 부여합니다. X-Force는 '제3자 취약점 노출을 추적하는 취약점 데이터베이스', '새로운 취약점을 찾아내는 보안 연구 조직', '고객이 제품에 내재된 취약점의 심각도를 정확히 평가하기 위한 대형 소프트웨어 공급업체의 지원'이라는 세 가지 관점에서 점수를 부여하고 있습니다.

IBM X-Force는 현재 다른 업체와의 협력 하에 새로운 CVSS 버전 3 표준을 개발하고 있습니다. 2012년의 취약점에 점수를 부여해본 결과, 2년 연속으로 대다수 취약점(65%)이 중간 범위에 속했다는 것을 확인했습니다. 심각한 수준의 취약점의 총 개수는 2011년에 비해 약간 감소했지만 심각도가 높은 취약점의 전체적인 비율은 지난해와 동일하게 29%를 기록했습니다.

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

표 2: CVSS 점수와 심각도

전체적인 심각도 분류는 지난 몇 년간 상대적으로 변화폭이 적었지만, 데이터를 자세히 확인해 보면 기업 소프트웨어 취약점에 대한 흥미로운 추세를 확인할 수 있습니다.

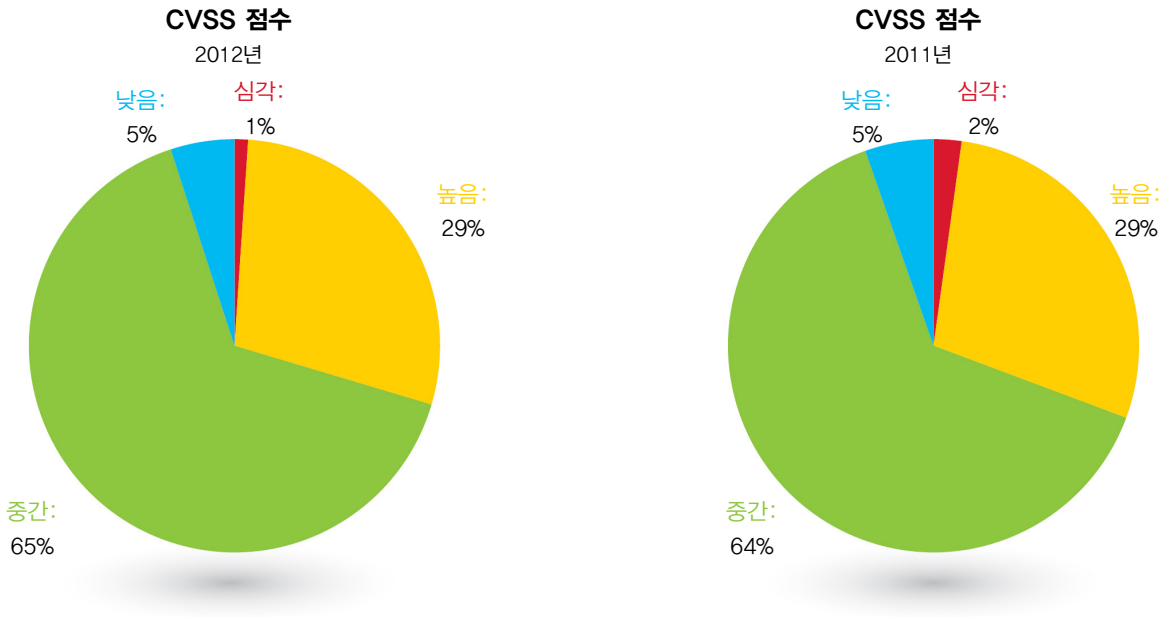


그림 37: CVSS 점수의 백분율 비교 – 2011년과 2012년의 비교

기업용 소프트웨어의 취약점

기업용 소프트웨어의 추세를 조사할 때, IBM X-Force는 가장 다양한 기업용 소프트웨어를 개발하는 대형 소프트웨어 벤더를 조사합니다. 수 천에 달하는 소프트웨어 벤더를 조사해본 결과, 이 업체들은 상당 수에 달하는 보안 취약점을 꾸준히 노출하고 있었습니다. 이러한 벤더들은 상위 10대 그룹으로 분류되며, CMS(Content Management System) 취약점은 대다수가 타사 플러그인 및 추가 기능에서 발생하며 엔터프라이즈급 소프트웨어와 같이 널리 쓰이지는 않기 때문에 CMS 취약점은 제외하였습니다.

2008년 이후 상위 10대 벤더의 전체적인 취약점 노출 비율이 증가하여, 2011년에는 대규모 기업용 소프트웨어 벤더가 노출하는 취약점은 33%를 기록했습니다. 그러나 2012년에는 이러한 업체에서 노출하는 취약점의 전체적인 비율이 26%로 감소했습니다. 이러한 감소는 이 범주에서 지난 5년간 처음으로 발생한 것이었으며, 2013년에는 면밀히 관찰하여 이러한 감소 추세가 1회성으로 발생한 것인지 또는 기업용 소프트웨어 벤더가 소프트웨어 개발 수명주기 내에 지속적으로 안전한 소프트웨어 개발 환경을 조성하여 나타난 것인지 확인함으로써 벤더들이 새로운 소프트웨어를 개발하기 전에 취약점을 파악하고 해결하게 할 것입니다.

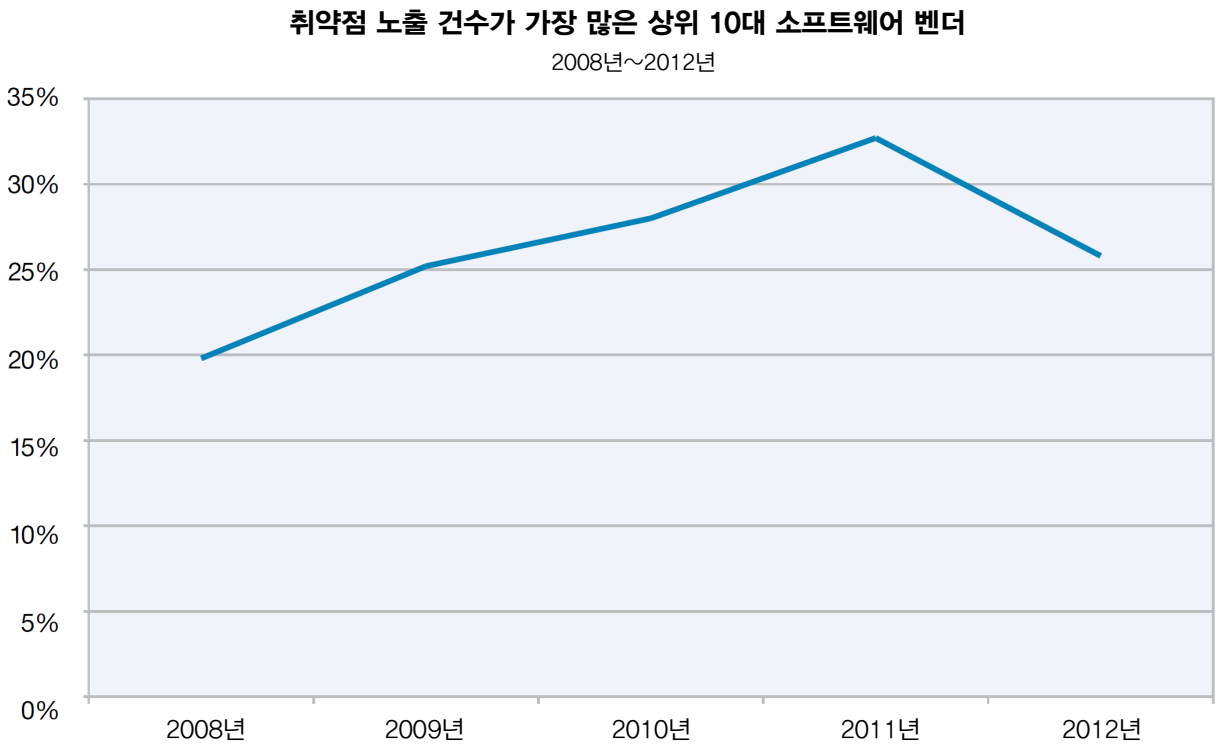


그림 38: 취약점 노출 건수가 가장 많은 상위 10대 소프트웨어 벤더 – 2008년~2012년

2012년에는 상위 10대 벤더가 대중에 노출한 취약점의 전체 비율은 감소했지만, 취약점 심각도와 관련된 새로운 추세가 확인되었습니다. 지난 5년간 CVSS 점수로 측정한 상위 10대 기업용 소프트웨어 벤더의 취약점의 평균 심각도는 2008년의 5.8에서 2012년에는 6.7로 거의 1점 가까이 증가했습니다. 이러한 점수는 2012년에 보고된 전체 취약점의 평균 CVSS 점수보다 1점 가까이 높은 점수입니다. 실제로, 2012년에 보고된 모든 심각한 취약점의 67% 및 심각도가 높은 모든 취약점의 33%는 상위 10대 벤더에서 발생한 것입니다. 공격자는 널리 이용 가능한 공격 및 잠재적으로 더 큰 보상을 위해 취약점을 찾을 것이므로 이러한 추세는 2013년에도 지속될 것으로 전망되며, 이러한 상황은 IBM X-Force의 분석에서 더 높은 CVSS 점수로 나타납니다.

보고된 Java 취약점의 수는 2011년과 2012년 사이에 변동이 없었지만, 평균 CVSS 심각도는 증가했으며, 이는 상위 10대 벤더의 평균 심각도보다 높습니다. 이 보고서의 이전 단원에서는 공격 키트에 포함된 Java 취약점의 이용에 대해 논의한 바가 있습니다.

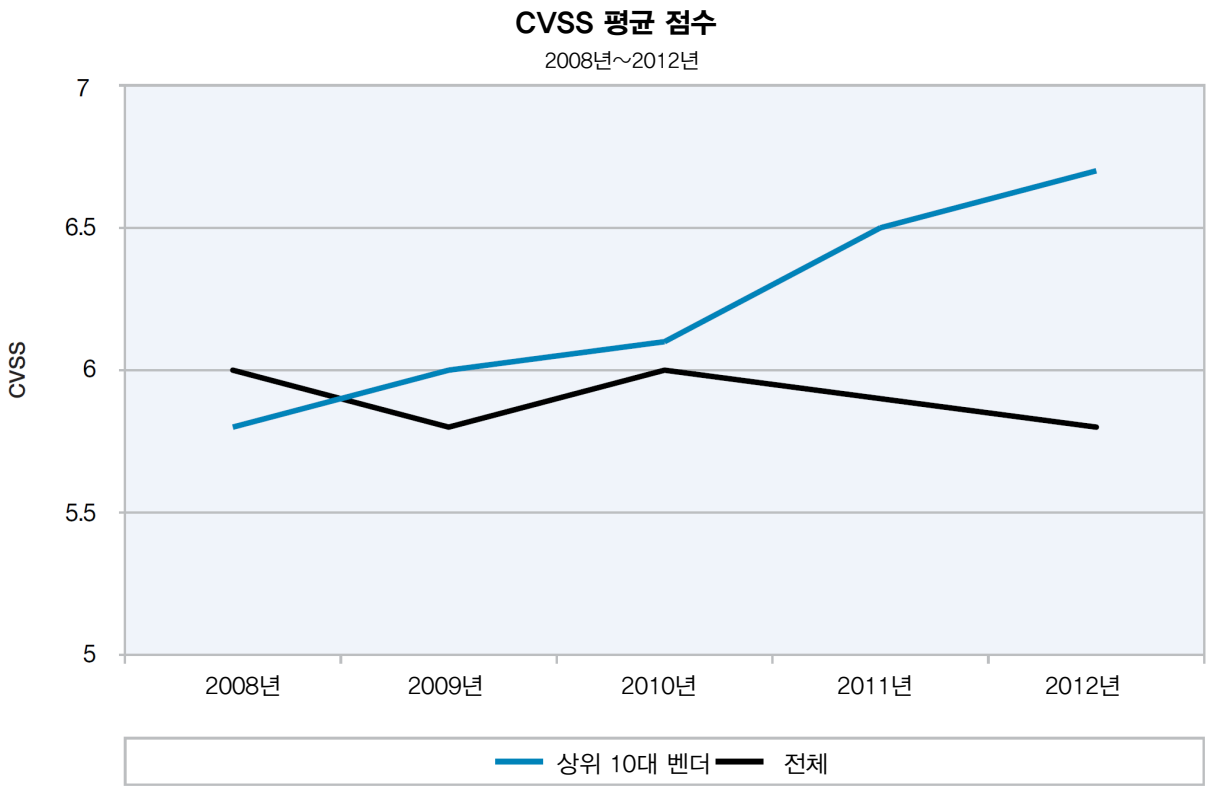


그림 39: CVSS 평균 점수 – 2008년~2012년

2012년 상반기 동향 및 위험 보고서에서 언급한 바와 같이, IBM X-Force는 2012년 동안 오피스 소프트웨어 및 PDF (Portable Document Format)에 대한 취약점이 크게 감소한 것을 발견했으며, 이러한 PDF 취약점 노출의 감소는 Adobe Acrobat Reader X 샌드박스와 직접적인 상관관계가 있다고 확신했습니다. 이러한 감소 추세는 예상했던 만큼 크지 않았지만, 오피스 소프트웨어 및 PDF 취약점의 기록을 세웠던 2010년에 비하면 여전히 큰 의미가 있었습니다. 최신 버전의 Acrobat Reader에 적용된 샌드박스 기술은 확실한 공격에 대한 기대치를 높였습니다. 그 이유는 이러한 공격을 위해서는 샌드박스 우회와 원격 코드 실행 취약점을 모두 이용해야 하기 때문입니다. 이러한 변화로 인해 공격자는 새로운 PDF 취약점을 찾기 위해 시간을 할애하는 데 흥미를 잃게 되었습니다.

샌드박스는 공격받은 시스템에서 공격자와 연구자가 얻을 수 있는 권한을 줄이도록 설계되었기 때문에, 이와 같은 이점을 보안 환경에 제공할 수 있습니다.

웹 브라우저 취약점의 수는 2012년에 약간 감소했지만 문서 포맷 문제만큼 높은 수준은 아니었습니다. 웹 브라우저 취약점의 전체적인 수는 2011년에 비해 6%밖에 감소하지 않았지만, 심각도가 "심각" 또는 "높음"인 웹 브라우저 취약점은 한 해 동안 59% 증가했습니다.

"최신 버전의 Acrobat Reader에 적용된 샌드박스 기술은 확실한 공격에 대한 기대치를 높였습니다. 그 이유는 이러한 공격을 위해서는 샌드박스 우회와 원격 코드 실행 취약점을 모두 이용해야 하기 때문입니다. 이러한 변화로 인해 공격자는 새로운 PDF 취약점을 찾기 위해 시간을 할애하는 데 흥미를 잃게 되었습니다."

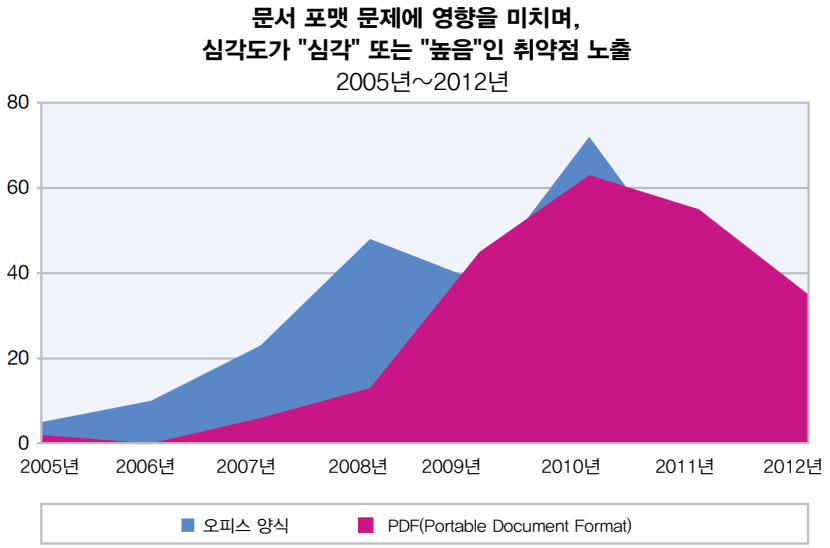


그림 40: 문서 포맷 문제에 영향을 미치며, 심각도가 "심각" 또는 "높음"인 취약점 노출 – 2005년~2012년

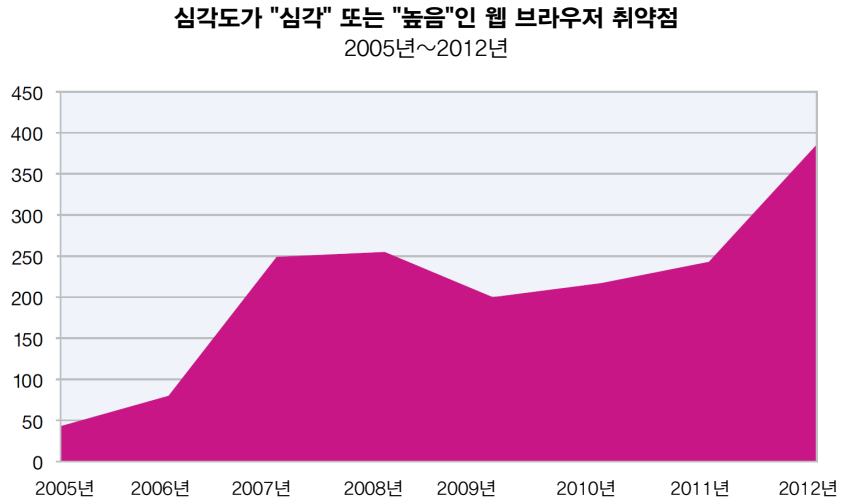


그림 41: 심각도가 "심각" 또는 "높음"인 웹 브라우저 취약점 – 2005년~2012년

상위 10대 벤더의 취약점 패치율에 엄청난 발전이 있었는데, 이는 안전한 개발 환경과 PSIRT(Product Security Incident Response Team) 프로그램의 지속적인 구현과 개선이 있었기 때문입니다. 상위 10대 엔터프라이즈급 벤더의 패치 수정률은 94%를 약간 넘는 정도입니다. 실제로, 상위 10대 벤더 중 세 곳은 2012년에 100%의 패치 수정률을 기록했습니다.

이러한 소식은 상위 10대 기업용 소프트웨어 벤더에게는 희소식이지만, 나머지 취약점 부문에서는 그렇지 않습니다. 2012년에 패치가 적용되지 않은 취약점의 비율은 2008년 이후 처음으로 증가했습니다. 2012년에 노출된 전체 취약점 중 42%에 대한 패치 수정이 아직 이루어지지 않았습니다.

증가가 반드시 나쁜 징조라고 볼 수는 없습니다. 대형 소프트웨어 벤더들은 5년 전에 비해 취약점 해소에 더욱 많은 노력을 기울이고 있습니다. 소규모 웹 애플리케이션과 개인 또는 소규모 기업이 개발한 유명하지 않은 소프트웨어의 취약점 증가가 2012년도 증가 추세의 주된 원인으로 보입니다. 이러한 취약점의 다수는 심각도가 낮으며, 제품 수명이 다할 때까지 패치나 지원이 제공되지 않을 가능성이 높습니다.

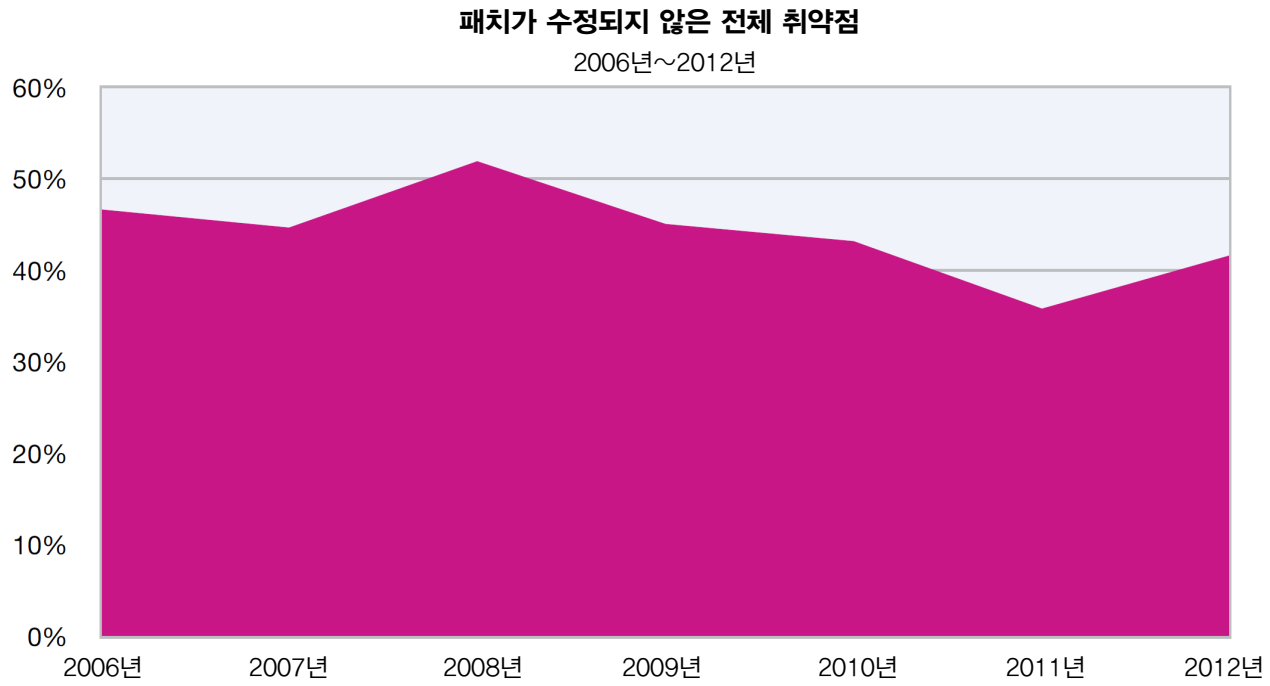


그림 42: 패치가 수정되지 않은 전체 취약점 – 2006년~2012년

혼란을 피하고 협력하기 위한 사고 대응팀 활용 방법

지난해, IBM의 ERS(Emergency Response Service)는 CSIRP (Computer Security Incident Response Plan)를 수립 및 구현할 때 많은 조직에서 범하기 쉬운 실수를 선별했습니다. 이번 보고서에서는 적절한 SCIRP를 실행하고 있지만 제3자 사고 대응 팀으로부터 지원을 요청하기 위한 만반의 준비를 갖추지 못한 조직에게 영향을 미칠 수 있는 일반적인 시나리오를 살펴봅니다. 이와 같은 시나리오는 주로 다음과 같이 전개됩니다.

오전 2시가 조금 넘은 시간에 전화벨이 울리고, 당신은 잠을 방해하는 사람이 누구인지 생각해보려 합니다. 전화기에서는 네트워크 관리자가 평소보다 매우 피곤한 기색이 느껴지는 목소리로 늦은 밤에 연락하게 된 것을 사과합니다. 네트워크 관리자가 네트워크 로그에 당신의 리서치 네트워크에서 대량의 데이터를 아시아 지역의 IP 주소로 발송한 기록이 있다고 말하자 당신의 심장은 빠르게 뛰기 시작합니다. 네트워크 관리자가 확인한 사실을 상세하게 듣고 나서, 당신은 리서치 네트워크에 회사의 가장 귀중한 지적 재산 중 일부가 저장되어 있다는 것을 깨닫게 됩니다. 대응 조치에 대한 대화가 진행되자 당신은 몇몇 직원에게

실시하려 했으나 예산 삭감으로 인해 실시하지 못한 네트워크 침입 교육을 떠올립니다. 당신은 우수한 네트워크 팀을 보유하고 있지만 지금의 사고 대응을 위해 필요한 기술은 개발하지 못했습니다. 마지막 순간에 YouTube에서 "사고 대응" 전략을 검색하려는 판단을 포기한 후, 당신은 이러한 과제에 정기적으로 대처하고 있는 외부 리소스를 신속히 불러와야 한다는 것을 깨닫게 됩니다.

안타깝지만, 이러한 가상 시나리오는 IBM의 ERS 팀이 경험하는 일반적인 현실 상황인 경우가 많습니다. 가장 세심하게 수립된 CSRIP로도 이러한 시나리오의 모든 문제를 제거할 수는 없지만, IBM은 각 조직이 10가지 사항을 이해하고 구현한다면 추가적인 사고 대응(IR) 지원을 효과적으로 실행하기 위한 적절한 준비 절차 마련할 수 있다고 생각합니다. 몇 가지 간단한 준비를 통해 사고 대응을 위한 시간과 노력을 아낄 수 있을 뿐만 아니라 비용을 크게 절감하고 새로운 해답을 신속하게 찾을 수 있는 가능성을 높일 수 있습니다.

1 자격을 갖춘 IR(Incidence Response) 팀과 사전에 관계를 형성하십시오.

사고가 발생하면 최후에 하게 되는 것은 해당 시설에 찾아와 줄 수 있는, 자격을 갖춘 IR 팀을 찾는 것입니다. 언제든지 준비를 갖추고 있으며, 사고가 발생한 장소로 곧바로 출동할 수 있는 자격을 갖춘 IR 팀에 지금 바로 연락하여 관계를 형성하십시오. 이러한 IR 팀은 디지털 포렌식 및 사고 대응(Digital Forensics and Incident Response) 자격증을 소유한 전문가를 보유하고 있어야 하며 사고 대응 작업 및 분석을 지원하기 위한 적절한 장비를 갖추고 있어야 합니다.

2 만일의 경우를 대비해 계약을 조정할 수 있는 사람을 지정하십시오.

IR 팀을 확보하기 위한 첫 번째 핵심 단계를 이미 실행했다면, 사고가 발생하기 전에 첫 번째 계약이 체결되어 있을 것입니다. 불행히도, 계약 문제는 사고 발생 후 중대한 지연을 발생시키는 원인 중 하나입니다. 이러한 지연이 발생하는 상황은 내부의 고문 변호사가 컴퓨터 앞에 앉아서 계약서의 도착을 기다리고 있거나, 회계부서 직원에게 구매 발주서를 작성하게 해야 하는 상황 등이 있으며, 계약 프로세스는 간소화되고 신속하게 진행할 수 있어야 합니다. 사고가 발생하기 전에, 조직에서 몇 명의 인력을 지정하여 외부 업체와 계약을 체결할 수 있는 권한을 부여하십시오. 사고 발생 시에 계약을 체결해야 하는 경우, 대기 중인 지정된 사람에게 새로운 계약을 체결하거나 요청을 변경할 수 있는 권한을 부여해야 합니다.

3 현재의 네트워크 및 환경에 대한 문서를 관리하십시오.

외부의 IR 팀은 사고가 발생한 환경에 대해 거의 모르고 있으며, 최초의 통화에서 몇 가지 기본적인 사항만을 파악하고 있는 경우가 많다는 사실을 명심해야 합니다. 따라서, IR 팀이 제기할 수 있는 질문에 답하기 위해서는 현재의 네트워크 토폴로지에 관한 상세한 내용이 담긴 문서가 필수적입니다. 이러한 문서를 몇 부 인쇄해 두어야 하며, IR 팀은 도착한 후 곧바로 관련 지식을 갖춘 관리자와 대화할 수 있어야 합니다.

4 IR팀에게 적합한 작업 환경을 준비하십시오.

IR 팀이 사고 장소를 향해 출발하면, 적어도 일주일간 이들이 이용할 수 있는 전용 공간을 마련해야 합니다. 대부분의 IR 분석가는 적응 능력이 매우 뛰어나지만, 작업을 쉽게 진행할 수 있으면 사고 대응 목표를 더욱 훌륭하게 달성할 수 있습니다.

중앙 부근에 위치한, 문을 잠글 수 있는 회의실은 IR 팀과 조직 내 직원 모두에게 매우 중요한 요소입니다. 이러한 회의실은 핵심 인력과 인접한 곳에 배치해야 하고, 분석가가 편안하게 이용할 수 있어야 하며, 정상적으로 작동하는 스피커폰이 설치되어 있어야 하고, 충분한 조명을 갖추고 있어야 합니다. 또한 여러 개의 전원 콘센트, 네트워크 콘센트 및 테이블 공간이 있어야 합니다. 문을 잠글 수 있는 회의실은, 특히 민감한 데이터를 처리하는 경우, 밤새 장비를 안전하게 보관하는 데 도움이 됩니다.

5 관련 네트워크 로그를 사전에 수집하십시오.

네트워크 로그를 찾아서 확보하는 데에는 반드시 시간이 걸릴 것입니다. 사고 확인 후 최초의 몇 시간이 가장 중요한 경우가 많으며, 일반적으로 네트워크 로그에는 이러한 가장 중요한 정보가 일부 포함되어 있습니다. 로그를 사전에 수집한 경우, 일반적으로 이러한 로그는 안전한 파일 전송 서버로 쉽게 업로드할 수 있으며, 사고 현장에 출동하지 않는 IR 팀원이 원격으로 로그를 검토할 수 있습니다. 동시에 진행되는 분석을 통해 핵심적이고 생생한 정보를 현장에 도착한 IR 팀원에게 제공할 수 있어 시간과 노력을 아낄 수 있습니다.

6 사고 조정 담당자를 지정하십시오.

IR 팀의 도착을 돕는 가장 핵심적인 작업 중 몇 가지는 인사 관리와 관련되어 있습니다. IR 팀은 사고 지점을 방문한 경험이 전혀 없을 수도 있으며, 해당 조직의 환경과 문화에 익숙하지 않을 가능성이 높습니다. IR 팀에게 전담 조정 담당자를 지정하여 요구사항을 확인하고 도움을 주도록 하면 의사소통을 원활하게 진행하고 효율적으로 업무를 처리할 수 있는 경우가 많습니다. 사고 조정 담당자는 입구에서 IR 팀의 도착을 기다리고, 보안 절차에 동행할 준비를 마치고, 지정된 작업 영역으로 안내해야 합니다. 또한, 조정 담당자는 연락, 시설 이용 및 핵심 담당자와의 의사소통에 대한 1차 담당자여야 합니다. 그리고 현지 식당, 커피숍 및 정수기를 찾을 수 있도록 지원하는 것은 크게 도움이 됩니다.

7 야간 및 주말에도 최소한의 인원은 배치하십시오.

일반적으로 IR 팀은 장시간 근무하거나 중요한 사고인 경우에는 주말에도 근무하는 경우가 많습니다. 적어도 소규모의 핵심 인원으로 구성된 대표단을 파견하여 IR팀의 주말 작업을 돕는 것은 매우 중요합니다. 매우 중요한 손상 지표가 있는 시스템에 접근하려면 관리자가 월요일 아침에 출근할 때까지 기다려야 한다는 사실처럼 IR 팀의 기분을 상하게 하는 일은 없습니다. 일정은 사전에 조정해야 하며, 때에 따라서는 지원이 필요한 상황에 연락할 수 있는 핵심 인원의 전화번호를 IR 팀에게 제공해야 합니다.

8 IR 팀이 참석해야 하는 장시간의 회의는 피하십시오.

IR 팀이 도착하면 장시간이 걸리는 회의는 열지 않도록 해야 합니다. 정당한 사유가 있는 경우에도, 모든 회의는 짧은 상황 보고로 제한되어야 합니다. CEO 및 여러 명의 관리자가 참석하는 장시간이 걸리는 회의는 시간 낭비일 뿐입니다. 분석가에게는 밝은 조명이 갖추어진 방과 현지 피자 가게의 전화번호, 그리고 일할 시간이 필요할 뿐입니다. 하루에 세 시간씩 회의를 한다면, 원하는 성과를 얻기가 더 어려워집니다.

9 최초 대응자 작업 절차를 개발한 후 실습하십시오.

소멸성 데이터 수집에 주의를 기울여 사고 대응자가 훼손된 시스템의 악성 코드 및 의심스러운 활동을 식별할 수 있도록 하십시오. IR 팀과 협력하여 소멸성 데이터 수집에 대한 확실한 최초 대응자 작업 절차를 문서화하고 이를 실습한 후 실습 결과에 대한 IR 팀의 피드백을 확인하십시오. 사고가 발생하여 분주할 때 소멸성 데이터를 즉시 수집할 수 있는 인력을 구축하기 위해 최초 대응자 작업 절차를 시스템 관리자 교육에 포함시키십시오. 이를 통해 IR 팀은 분석 작업에 집중할 수 있게 됩니다.

10 CSIRP(Computer Security Incident Response Plan)를 업데이트하십시오.

앞서 언급한 9가지 항목의 대부분이 조직의 CSIRP에 포함되어 있어야 합니다. 조직 내에서 이러한 항목에 대한 작업을 진행하는 중에 CSIRP의 핵심적인 측면을 문서화한 후 자주 검토하여 계획에 포함된 구성요소가 여전히 적용 가능하며 통용 가능한지 확인하십시오. IR 팀에 연락하여 CSIRP에 대한 피드백을 얻는 것은 CSIRP를 통해 사고 대응 수명주기의 중요한 측면을 올바르게 처리하는 데 도움이 됩니다. 신뢰할 수 있는 외부의 피드백을 통해 이전에 간과했던 사실을 파악하게 될 수도 있습니다.

전문적인 사고 대응 팀의 지원이 필요한 보안 사고에 더욱 철저히 대비하기 위한 방법을 찾을 때에는, 최대한 신속하게 데이터 유출을 방지하고 상황 파악을 목표로 삼아야 한다는 것을 기억하십시오. 누군가의 생사가 걸린 상황을 돕기 위해 응급 의료 서비스 팀이 서두르는 경우와 같이, 시간은 가장 중요한 요소입니다.

이번 보고서에서 다룬 각각의 항목을 개별적으로 생각할 경우 시간과 자원의 낭비를 막을 수 없습니다. 그러나 이 모든 사항을 함께 실행하는 경우에는 오랜 시간 동안 계속되는 불안한 싸움을 피하고, 빠른 시간 내에 성공적으로 복원을 완료할 수 있을 것입니다. 더욱 조직화된 사고 대응 프레임워크를 위해 노력해야 하는 중요한 이유 중 한 가지는 재정적 지출의 큰 절감이라고 할 수 있습니다. 오전 2시에 연락을 받게 되는 일이 다시 생기면, 그때는 효율적이고 효과적으로 작업을 진행할 준비가 되어 있을 것입니다.

알파벳 "T"를 이용한 위험 모델링, 평가 및 관리

네트워크 보안 업계는 위협을 예측하고 사전에 조치를 취하기 위해 주기적으로 위험 모델링, 평가 및 위험 관리를 실시할 것을 권장합니다. 이러한 작업은 위대한 모험과도 같지만, "위험 평가"에 대한 최근의 인터넷 검색 결과는 3천 8백만 개의 결과물을 보이고 있으며, 이들 중 많은 수의 위험 모델링 프로세스는 위험이 발생했을 때 위험 평가 및 관리 프로세스 내에서 투자수익률(ROI)을 결정하는 다양한 방법이 존재할 때의 복구 비용과 비교한 위험 관리 비용의 계산 방법을 포함하고 있습니다. 이러한 해결책 중 일부는 너무 난해하고 추상적이어서 거의 실행이 불가능합니다. 지금 필요한 것은 실행이 간편한 위험 모델링 및 평가 프로세스입니다.

위협을 처리하라(Treat the Threat)

식별된 보안 위협을 해결하는 기본적인 방법은 위협을 *처리(Treat)*하기 위한 계획을 수립하여 허용 가능한 수준까지 위협을 감소시키는 것입니다. 이를 달성하기 위한 한 가지 프로세스는 다음과 같습니다.

1 위협을 식별하십시오. 이러한 작업에는 공격자의 전략, 기법 및 공격 절차(TTP)에 대한 높은 수준의 상황 인식이 필요하며, 이러한 위협을 이용한 공격이 성공할 수 있을지 판단하기 위해서는 조직의 네트워크에 대한 지식도 필요합니다. 위협은 네트워크의 내부와 외부 모두에서 공격자의 관점으로 평가해야 하며, 여기에는 물리적 보안에서부터 네트워크 및 개인 디지털 보안에 이르는 여러 가지 주제가 포함될 수 있습니다. 이러한 위협의 예는 다음과 같습니다.

- 건물의 물리적 보안: 절도, 화재, 홍수, 항의성 시위
- 루트 계정 또는 관리자 계정의 신임 정보의 훼손
- 분산 서비스 거부(DDoS) 공격
- 보호 중인 데이터의 손실: 랩톱의 분실/도난, 민감한 시스템에 대한 침입, 직원의 데이터 절도 등
- 직원이 소셜 네트워크에 남긴 정보를 이용한 데이터 마이닝

2 위협을 식별하고, 위협을 관리하기 위한 절차를 개발 및 실행하십시오. 이러한 절차는 각각의 위협을 구체적으로 처리할 수 있는 구성을 갖추어야 하며, 그 결과를 측정할 수 있어야 합니다. 보안에 대한 피로도 상승과 보안 예산의 삭감으로 인해 조직은, 위협이 구체화되지 않은 경우에도, 점차 더 적은 자원을 투입하여 위협을 처리하려는 경향을 보이는 경우가 많습니다.

3 위험 관리 프로세스를 모니터링하고 감독하십시오. 특히, 위협의 존재를 감시하기 위한 모니터링 메커니즘을 확인하고, 경보를 모니터링하여 대응할 수 있는 담당자를 지정하십시오. 모니터링 메커니즘의 예에는 네트워크 취약점 스캐닝, 네트워크 안티바이러스 콘솔, SIEM(Security Information and Event Management) 시스템 및 침입 탐지/방지 시스템이 포함될 수 있습니다.

4 나머지 위협을 평가하여 해당 위협이 조직에서 정한 허용 가능한 수준까지 감소했는지 확인하십시오.

평가된 위협 및 나머지 위협의 가치는 위협의 발생 가능성 또는 발생 빈도(높음, 중간, 낮음)를 해당 위협이 발생했을 때 받을 수 있는 피해(치명적, 높음, 중간, 낮음)와 비교하여 결정할 수 있습니다. 이러한 작업의 목표는 위협 발생의 빈도를 낮추거나 실제로 위협이 발생했을 때의 영향을 낮추는 위험 관리 프로세스를 구현하는 것입니다. 피해 평가에 영향을 미칠 수 있는 한 가지 요소에는 네트워크의 다양한 영역에 저장된 데이터의 특성이 포함될 수 있으며, 이로 인해 네트워크의 다양한 영역에 대해 서로 다른 수준의 위협 평가를 얻을 수도 있습니다. 서버의 루트 계정 신임 정보의 훼손은 워크스테이션의 경우에 비해 더 높은 영향을 미치는 것으로 평가할 수도 있으며, 이를 위해서는 서로 다른 위험 관리 프로세스가 필요합니다. PCI(payment card industry) 또는 다른 민감한 데이터 환경에서 발견되는 악성코드는 나머지 다른 네트워크의 경우에 비해 위험성이 더 높은 것으로 평가할 수 있으며, 그 이유는 이러한 데이터가 노출되었을 때 발생하는 영향력의 차이가 크기 때문입니다.

이러한 작업을 성공적으로 완료하려면 특별히 지정된 모니터링 메커니즘을 통해 위협 처리 프로세스의 구현을 모니터링하고 위협의 존재를 모니터링해야 합니다. 모니터링 메커니즘을 모니터링하여 경보에 대응해야 합니다. 네트워크 전체의 바이러스 경보에 대한 정보를 수집하는 네트워크 기반의 안티바이러스 콘솔을 보유하고 있는 경우에도, 안티바이러스 콘솔을 모니터링하고 경보에 대응할 담당자가 지정되어있지 않으면 아무 소용이 없습니다. 모니터링 및 대응은 위험 관리 프로세스에 포함됩니다. (위협 평가 및 위험 관리 프로세스 표가 아래에 예시로 표시되어 있습니다. 그러나 IR 팀에서는 더 많은 내용이 담긴 목록을 이용할 수도 있습니다.)

위협의 식별	위협 수준의 평가	위험 관리 프로세스	위험 관리 프로세스 구현 및 모니터링 담당자	나머지 위협 수준	허용 가능한 위험인가?
루트 계정 신임 정보의 훼손	높음(낮은 빈도, 치명적인 영향력)	이중 요소 인증, 네트워크 분할, 역할 기반 액세스 제어 *계정 훼손의 빈도 및 영향력을 낮춤*	ID 관리 팀, 시스템 관리자, 네트워크 팀	낮음(낮은 빈도, 중간 수준의 영향력)	예
랩톱, USB 디바이스 또는 스마트폰의 분실	높음(중간 수준의 빈도, 높은 영향력)	디스크 전체의 암호화, 견고한 비밀번호 정책, 원격 삭제 기능, 랩톱 추적 기능 *데이터 유출의 빈도를 낮춤*	랩톱 및 휴대 전화 관리 팀, 직원	낮음(높은 빈도, 낮은 영향력)	예
악성코드의 네트워크 유입	높음(중간 수준의 빈도, 높은 영향력)	보안 인식 교육, USB 자동 실행 기능을 끄도록 그룹 정책 개체(GPO)를 설정, 안티바이러스 소프트웨어, 견고한 비밀번호, 이메일과 인터넷 및 네트워크의 필터링, 네트워크 분할 *악성코드 이벤트의 빈도를 낮춤, 데이터 유출을 줄이기 위한 대응 역량 강화*	교육 팀, 시스템 관리자, 안티바이러스 관리자, 네트워크 팀	낮음(낮은 빈도, 낮은 영향력)	예

표 3: 위협 평가 및 위험 관리 프로세스 예시

위협을 이전하라(Transfer the Threat)

기업들은 다른 개체로 위협을 *이전(Transfer)*하여 해당 개체가 위협의 관리를 담당하도록 하는 경우가 많습니다. 이러한 프로세스는 주로 방화벽 관리 및 모니터링, 침입 탐지/방지 시스템 및 안티바이러스 소프트웨어와 같은 관리되는 보안 서비스 프로세스를 위한 아웃소싱을 이용합니다. 올바른 위협 평가 후, 해당 기업에서는 자체적으로 적절히 관리할 수 없는 프로세스를 통해 발견된 위협을 한 벤더에게 이전하도록 결정할 수도 있습니다. 예를 들면, 조직들은 안티바이러스 소프트웨어 벤더를 통해 일종의 위협 이전을 이미 실행하고 있습니다. 자체적으로 기업 내부의 안티바이러스 솔루션을 개발 및 구현하는 대신 악성코드 탐지 및 위험 관리 작업을 벤더에게 이전함으로써, 악성코드에 의해 발생하는 위협의 상당수를 이전할 수 있습니다. 그러나 재원 확보 및 프로세스를 이전한 개체가 위협 관리 작업을 잘 수행하는지 여부의 모니터링을 포함해 위협 관리 작업의 이전을 위한 올바른 자원 할당의 부담이 여전히 남게 됩니다.

위협을 제거하라(Terminate the Threat)

위협 처리 프로세스 중, 남아 있는 위협이 조직에서 정한 허용 수준보다 너무 높다는 최종 결론을 내릴 수도 있습니다. 이렇게 위험 요소를 이전할 수 없는 경우, 위협에 대한 노출을 *제거(Terminate)*하기로 결정할 수도 있습니다. 예를 들어, 직원의 "BYOD(Bring Your Own Device)"를 허용하기 위해 모든 위험 관리 프로세스를 적용한 후에도 남아 있는 위협이 너무 높다고 판단되는 경우에 BYOD로 인해 발생하는 위협을 제거하려면, 회사가 적절하게 통제할 수 없거나, 보안 소프트웨어를 구현 및 모니터링하기가 어렵거나, 직원이 퇴사한 후에도 회사의 데이터가 남아 있을 수 있는 직원 소유의 디바이스를 이용하지 못하도록 할 수 있습니다.

위협을 허용하라(Tolerate the Threat)

위협 모델링 및 위험 완화 절차의 모든 단계를 완료하는 경우, 비즈니스 의사결정을 통해 남아 있는 위협을 *허용(Tolerate)*할 것인지 *제거(Terminate)*할 것인지 결정해야 합니다. 이 프로세스 전체의 목표는 식별된 위협을 기업이 남아 있는 위협을 허용할 수 있는 수준으로 줄이는 것입니다. 대부분의 위협은 완전히 제거할 수 없으며 각 위협의 발생 가능성은 위협 벡터에 의해 달라집니다. 예를 들어, 정당한 루트 수준 또는 관리자 수준의 접근 권한을 갖는 내부자가 뜻하지 않게 또는 고의적으로 위해를 가하게 되는 빈도는 외부자가 루트 계정 또는 관리자 계정의 신임 정보를 획득하는 것보다 더 높거나 더 낮을 수 있습니다.

서버의 루트 접근 위협 관리 예시

이전 페이지에서 설명한 위험 평가 모델을 기반으로, 서버 루트 계정(또는 동등한 수준의 계정)의 훼손으로 인한 잠재적인 피해량을 제한하기 위한 위험 관리 전략은 다음의 두 가지 목표를 달성하는 데 초점을 두게 됩니다.

- 루트 계정 훼손의 발생 빈도 또는 가능성을 줄임
- 루트 계정 훼손으로 발생할 수 있는 잠재적인 피해를 줄임

배스천 호스트(bastion host)는 공격을 견디기 위해 특별히 설계 및 구성된 네트워크에 설치되는 특수한 목적의 컴퓨터입니다. 이러한 컴퓨터는 일반적으로 프록시 서버와 같은 하나의 애플리케이션을 호스트하며, 해당 컴퓨터에 대한 위협을 줄이기 위해 다른 모든 서비스는 제거되거나 제한됩니다. 설치 위치 및 목적 때문에 배스천 호스트는 이와 같은 방법으로 강화되고, 방화벽의 외부 또는 DMZ 내에 존재하게 되며, 일반적으로 신뢰할 수 없는 네트워크 또는 컴퓨터로부터의 액세스를 담당하게 됩니다.

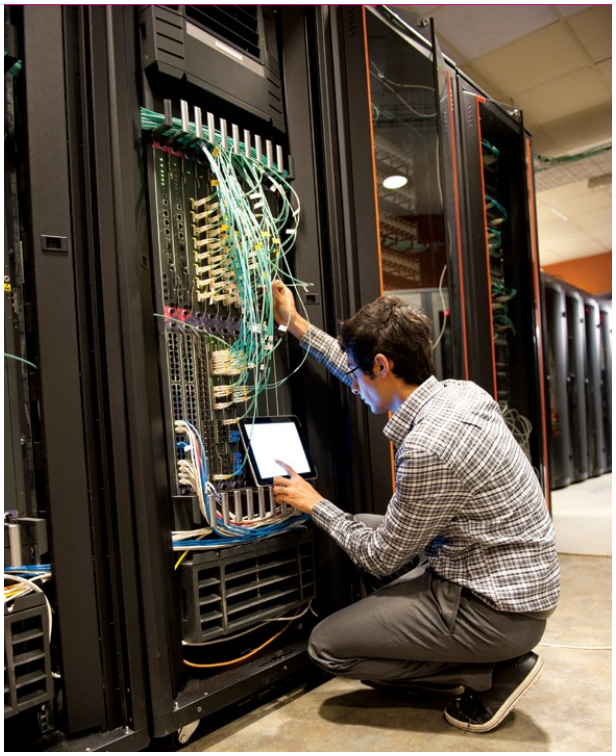
http://en.wikipedia.org/wiki/Bastion_host

다음 두 가지 목표를 달성하는 데 도움이 되는 몇 가지 옵션이 있습니다.

루트 계정 신임 정보 훼손 및 이용의 발생 빈도 또는 가능성을 줄임

여러 개의 정책 및 기술 프로세스를 구현하면 루트 계정 신임 정보의 훼손 및 훼손된 루트 계정 신임 정보의 이용 가능성을 줄이는 데 도움이 됩니다. 이 프로세스에는 다음이 포함됩니다.

- 루트 계정 신임 정보의 훼손을 통해 접근 권한을 획득할 수 있는 가능성을 줄이기 위해 루트 계정 로그인에 대한 이중 요소 인증을 구현.
- 서버에 대한 모든 사용자의 접근을 인증 및 로깅하기 위한 배스천 호스트로 작동시키기 위해 "점프 박스(jump box)"를 구현.
- 방화벽을 통해 허가된 접근 권한을 가진 시스템만이 네트워크상에서 서버에 연결할 수 있도록 방화벽을 구현.



루트 계정 훼손으로 발생할 수 있는 잠재적인 피해를 줄임

루트 계정은 완전한 명령 권한과 액세스 권한을 가지고 있으므로 시스템상에서 모든 작업을 수행할 수 있습니다. 일부 운영 체제는 역할 기반 액세스 제어(RBAC)를 이용해 루트 사용자의 일부 역할을 다른 사용자에게 이전합니다. 예를 들어, 루트 계정은 사용자 계정을 추가, 삭제 및 수정할 수 있는 권한을 가지고 있습니다. 그러나, 조직들은 역할을 기반으로 루트 계정의 권한을 다른 계정으로 옮기는 경우가 많으며 IMT(Identity Management Team)를 구성하여 사용자 계정을 관리합니다. IMT 그룹 계정에는 이러한 기능을 실행하기 위한 충분한 권한이 주어지며, 루트 사용자는 사용자 계정의 관리를 담당하지 않을 수도 있습니다. 공격자가 루트 계정에 대한 액세스 권한을 획득하는 경우, 이러한 계정 생성 권한을 통해 이점을 얻을 수 있습니다. 이 시나리오를 활용하여, RBAC 메커니즘을 구현해 루트 계정의 사용자 계정 생성 권한을 축소 또는 제거할 수 있습니다.

모니터링 메커니즘은 루트 계정에서 사용자 계정의 비인가 생성 또는 생성 시도했으나 이러한 작업은 루트 계정의 역할을 벗어난 행동인 경우를 나타내는 로깅 이벤트가 발생하면 일종의 덫으로 작동하도록 구현할 수 있습니다.

루트 계정 훼손의 가능성 및 발생 가능한 데이터 유출의 양을 줄이기 위한 대응책을 구현하면, 최종적으로 전체적인 위험이 조직에서 허용 가능한 수준으로 감소할 것입니다. IBM ERS(Emergency Response Service)는 위험 관리 절차를 실행 중인 고객과 협력하고 있으며, ERS 팀은 위협이 적절하게 모델링되어 있고 위험 관리 프로세스가 구현되어 있는 경우를 자주 접합니다. 그러나, 위험 관리 프로세스의 적절한 감독 및 모니터링은 이루어지지 않았으며, 이로 인해 결국 위험 관리 절차를 성공적으로 실행하지 못했습니다.

식별 및 구현된 모든 위험 완화 프로세스에는 위험 완화가 성공적으로 이루어지고 있고, 적절한 위협 감소가 달성되었으며, 안전장치를 구현하고 초기의 일정 기간이 지난 후에도 올바르게 구현 및 유지되고 있다는 것을 확인하기 위해 활발한 감독 및 모니터링 프로세스가 구현되어야 합니다.

소셜 미디어 및 인텔리전스 수집 개요

글로벌 커뮤니티는 상대적으로 새롭고 개방된 연결 방법에 열광하고 있으며, 이를 통해 전 세계의 사람들과 연락을 주고받고 있습니다. 실제로, 소셜 미디어만큼 의사소통 방식에 영향을 미친 혁신적인 사건은 거의 없었습니다. 그러나 각 개인 간에 대규모 상호연결과 지속적인 연락이 가능해짐에 따라 인텔리전스 수집 기능의 새로운 취약점 및 근본적인 전환이 발생했습니다. 그 결과 공격자 및 보안 전문가 모두에게 더 많은 활동을 할 수 있또록 유용한 정보를 제공하게 되었습니다.

즉, 공격자는 소셜 네트워크에 호스트되는 자유롭게 이용 가능한 데이터에 액세스하고 이러한 정보를 수집하기 위한 특별한 방법들을 개발하고, 여러 방법 중 어떤 방법이 공격 대상을 선정하는 데 가장 좋은 방법인지 결정하는 작업을 수행하게 되었습니다.

그 대신, 소셜 미디어의 폭발적인 성장 덕분에 기업 보안 전문가는 공격자가 기업을 공격하는 데 이용하는 것과 동일한 데이터에 자유롭게 액세스할 수 있게 되었으며, 공격자에 대한 잠재적인 정보를 얻을 수 있게 되었습니다.

이러한 상황은 보안 전문가에게 매우 도움이 되지만, 정보를 보호하기 위한 작업을 진행하면서 소셜 미디어 및 기술에 적응할 수 있는 환경을 조성해야 하는 경우에는 통제하기 어려운 환경에 처하게 됩니다. 정보 보호를 위한 이러한 노력이 실패하자 기업 및 정부가 공격받는 방식은 이미 눈에 띄게 달라졌습니다.

어떠한 관점에서건, 소셜 미디어는 인텔리전스 수집의 핵심적인 영역이라는 것이 분명합니다. 이 단원에서는 소셜 미디어로 인한 인텔리전스의 근본적인 전환, 인텔리전스 수집에 있어 취약점의 원인이 되는 소셜 미디어의 측면, 그리고 조직이 스스로를 보호하기 위해 이용할 수 있는 방법을 논의합니다.

인텔리전스 수집 관련 배경 지식

그러나 인텔리전스 수집의 전환이 어떻게 이루어졌는지 살펴보기 전에 "*인텔리전스(intelligence)*"라는 용어가 무엇을 의미하는지 이해하는 것이 중요합니다. 인텔리전스는 학습 또는 이해하는 능력이라고 정의할 수 있습니다. 여기서, 학습 및 이해의 맥락은 개인 사용자 또는 기업 내의 사용자 집단과 같은 특정한 개체에 대한 정보의 발견과 직접적으로 연관됩니다.

정보의 발견은 다수의 데이터 아티팩트를 수집하고 이를 분석하는 작업을 통해 이루어지며, 분석 작업은 주로 "인텔리전스 수집"으로 불립니다. 인텔리전스 수집은 현존하는 여러 가지 다양한 수집 기법을 기반으로 정의됩니다. 수집 기법은 인텔리전스를 수집하기 위해 이용되는 다양한 프로세스 및 인텔리전스 정보 자체를 설명하는 데 이용될 수 있습니다. 이러한 설명은 "인텔리전스 유형"으로 축약될 수 있습니다. 여러 가지 인텔리전스 유형은 다음과 같습니다.

1. **HUMINT(Human intelligence)**: 개인 간의 접촉을 통한 또는 사람으로부터 직접 얻은 인텔리전스의 수집
2. **SIGINT(Signal intelligence)**: 의사소통 인텔리전스 및 전자 인텔리전스를 설명하는 데 이용되는 용어
3. **OSINT(Open-source intelligence)**: 공개적으로 이용 가능한 정보 및 공개적인 배포 또는 액세스가 제한된 기타 미분류 정보를 이용한 인텔리전스의 수집
4. **MASINT(Measurement and signature intelligence)**: 감지 장치[66]를 통해 획득한 데이터의 분석을 통해 유추된 과학적이고 기술적인 인텔리전스

기업 보안 조직은 이러한 인텔리전스 유형을 모두 이용하지만 공격자는 주로 HUMINT 및 OSINT에 중점을 둡니다. 소셜 미디어는 다수의 공격자 활동이 HUMINT에서 OSINT로 전환되는 데 핵심적인 역할을 해왔습니다. 이러한 변화는 이전에는 HUMINT였던 대부분의 데이터가 공개적으로 게시되고 있으며, OSINT 활동을 통해 이러한 데이터를 복원할 수 있다는 사실 때문입니다. 이전에는 다양한 데이터 아티팩트에 대한 수집 및 분석이 필요했던 인텔리전스, 특히 HUMINT는 이제 단 한 가지 유형의 인텔리전스 수집(OSINT)을 이용해 소셜 미디어 사이트에서 수집할 수 있게 되었습니다. 즉, 과거와 같이 공격 대상의 정보를 얻기 위해 쓰레기통을 뒤지는 것과 같은 작업이나 소셜 엔지니어링 작업을 할 필요가 거의 없습니다.

66 NATO 용어집 및 Definitions AAP-6(2008년)의 정의를 따름

데이터 가용성/취약점

이러한 속성을 갖는 정보의 저장소가 존재하는 경우, 저장소가 단일 시스템인지 또는 여러 개별 플랫폼의 집합인지의 여부에 상관없이, 이 저장소는 공격의 대상이 될 수 있습니다. 불행히도, 대부분의 보안 책임은 보안 또는 개인정보에 신경을 쓰지 않거나 이러한 인식이 부족한 사용자 커뮤니티에 바로 전가됩니다. 끊임없이 변화하고 있으며 난해한 경우가 많은 개인정보 관리로 인해 이러한 상황은 더욱 복잡해졌으나, 개인정보 관리는 사용자가 자유롭게 정보를 공개하면서도 소셜 미디어를 완전하게 이용하도록 하기 위한 가장 좋은 방어 수단입니다.

광범위한 소셜 미디어 사이트에서 인텔리전스 수집에 유용한 대량의 데이터를 생산하고 있습니다. 여기에는 Facebook의 개인 데이터에서부터 Linkedin의 고용 정보에 이르는 다양한 정보가 포함되며, 한 개인이 Spotify에서 어떤 음악을 듣고 있는지에 대한 정보도 포함될 수 있습니다. 이러한 네트워크의 상당수가 단일 로그인 방식의 인증을 통해 통합됨으로써 데이터의 악용 문제는 더욱 심각해졌습니다. Facebook 및 Twitter 등의 사이트는 정보 공급자에게 잠재적으로 중요한 데이터를 제공하고 있으며, 중요한 데이터를 포함하고 있는 다른 별도의 사이트를 사용자가 인증하는 것을 허용하고 있습니다.

결국 공격자는 특정한 공격 대상이 될 수 있는 개인에 대한 정보를 검색할 수 있습니다.

기업은 개인의 집합

개인에 집중한 결과, 공격자가 기업을 보는 방식에도 엄청난 변화가 생겼습니다. 공격자는 특정한 기업을 개별적인 개체로 보는 대신 기업을 개인들의 집합으로서 볼 수 있게 되었습니다. 이러한 시각은 공격자에게 기업 인프라 또는 애플리케이션이 아닌 특정한 사람들을 공격 대상으로 삼을 수 있는 기회를 제공합니다. 또한, 공격 대상이 된 사람들은 단순한 직원이 아닌 개인으로서 표적이 될 수도 있습니다. 즉, 직원들의 개인적인 활동 및 생활을 이용해 기업을 공격의 대상으로 삼을 수 있게 되었습니다.

조직 내에서 외부와 접촉하는 직원에게 위험은 항상 존재해 왔습니다. 그러나, 이러한 위험은 대부분 계산 가능하고 쉽게 방지할 수 있었습니다. 소셜 미디어의 등장으로 인해 이제, 위험은 소셜 미디어 사이트를 이용하는 모든 개인으로 확대되었습니다.

소셜 미디어는 사용자와 접촉할 수 있는 방법을 제공하므로, 소셜 네트워크를 통해 사용자와 직접적으로 접촉할 수 있어 공격 작업은 간편해졌습니다. 이 방법은 사용자를 악성 웹사이트로 이동시키거나 사용자에게 악성코드를 직접 전송하는 등의 모든 부정한 목적에 이용될 수 있습니다. 그 결과 공격자는 기업 이메일 보안 대책을 우회할 수 있게 됩니다. 사용자가 집에서 사내 이메일을 확인하는 경우에도 공격자는 기업의 외부 침입 감지를 완벽하게 우회할 수 있습니다.

쉽게 말해서, 기업에 대한 액세스 권한을 획득하기 위한 수단으로서 개인을 공격하는 쪽으로 전환함으로써 각 개인은 가장 취약한 공격 대상이 되었습니다. 개인의 사적인 계정을 공격하는 것이 해당 계정이 이용되는 기업 환경에 대한 실제적인 침입으로 이어지는지의 여부에 상관없이, 이러한 사실은 명백합니다.

개인정보 보호

공격 대상 기업을 찾는 방법은 사용자가 소셜 미디어 사이트에 공개하는 정보에 의해 결정된다는 사실을 염두에 두면, 각 개인의 개인정보는 더욱 더 중요해집니다. 불행히도, 각 개인의 개인정보는 사용자의 개인정보 설정에 영향을 받을 뿐만 아니라, 사용자가 관계를 유지하고 있는 다른 사람의 개인정보 및 조심성에도 영향을 받게 됩니다.

예를 들어, "Jessie Smith"라는 이름의 사용자가 본인의 직장 정보를 볼 수 있는 사람을 제한한다고 해도 어떤 친구가 "제 친구 Jessie Smith가 IBM의 이사가 된 것을 축하합니다."라는 메시지를 게시하면 Jessie라는 사용자가 설정한 제한은 별로 효과가 없게 됩니다. 공격자는 개인 사용자의 계정을 인텔리전스 수집의 대상으로 삼는 대신 해당 사용자와 관련된 모든 계정을 대상으로 삼을 수 있습니다.

이러한 유형의 공격에는 훨씬 더 많은 시간이 소요되며 쓸모 없는 정보를 더욱 많이 입수하게 되지만, 결과는 매우 효과적일 수 있습니다.

또한, 이러한 정보 수집 방법은 소셜 미디어 플랫폼 자체의 논리적 문제를 이용해 실행될 수도 있습니다. 다른 사람과의 연결을 권장하는 방법은 다른 사용자에 대한 정보 입수를 시도하는 공격자에게 특히 취약할 수 있습니다. 이러한 취약점의 대부분은 어떤 면에서는 악성 행위의 여부를 파악하기 어렵게 만드는 핵심 기능을 이용합니다. 결과적으로, 이러한 취약점의 대부분은 빠른 시일 내에 해결될 가능성이 낮습니다.

보조 도구

물론, 공격자는 수집 작업을 직접 실행하지 않습니다. 사용자가 특정 대상에 대한 인텔리전스를 입수하는 것을 돕는 많은 도구가 존재합니다. 이러한 도구에는 인텔리전스 검색 서비스를 제공하는 서브스크립션 사이트에서부터 단순한 Google 검색, 또는 자동화된 방식으로 이용 가능한 특정한 검색, 소셜 미디어 사이트에서 정보를 입수할 목적으로 특별히 개발된 더욱 정교한 도구에 이르는 다양한 도구가 포함됩니다. 이 도구들은 데이터의 수집 및 정리 작업을 보조합니다. 일반적으로 처리해야 할 데이터의 양은 매우 많으므로, 시각화를 이용한 작업은 매우 중요합니다. 결과적으로, 이러한 사이트 및 도구의 대부분은 더 나은 데이터 정리를 위해 특수하게 제작된 시각화 기법을 포함하고 있습니다.

요약하면, 수많은 데이터가 존재하고 이 데이터는 쉽게 수집 가능하며, 데이터의 수집을 지원하는 특정한 목적을 갖는 다수의 유틸리티 및 서비스가 존재합니다.

기업의 보호

불행히도, 다른 많은 보안 문제와 마찬가지로, 소셜 미디어로 인해 발생하는 문제를 해결하기 위한 간단한 해결책은 없습니다. 소셜 미디어 정보를 이용하는 공격에 맞서기 위한 총체적인 기술적 해결책은 없습니다. 또한, 소셜 네트워크상에 민감한 정보가 전파되는 것을 방지하기 위해 따라야 할 특정한 프레임워크도 존재하지 않습니다. 그러나 기본적인 인식, 평가 및 대상 보안 기술을 이용하면 조직은 소셜 미디어를 통해 인텔리전스 수집을 이용하는 공격의 영향을 최소화할 수 있습니다.

직원의 인식

직원들 사이에 소셜 미디어가 조직의 보안에 어떠한 영향을 미치는지에 대한 인식을 형성하는 것은 문제를 해결하기 위한 첫 번째 단계입니다. 직원들은 본인이 공개하는 정보의 양과 모든 특정한 조직 내에서의 지위로 인해 공격의 대상이 될 수 있다는 것을 인식해야 합니다. 또한, 다른 직원 및 기업의 행사에 대해 게시된 정보는 공격에 이용될 수 있습니다.

각각의 개인 사용자가 무엇이 허용 가능한 소셜 미디어 행위인지를 이해하여 직접적인 모니터링 없이도 훌륭한 판단을 내릴 수 있게 되는 것은 매우 중요합니다. 물론, "허용 가능한 행위"에 어떠한 행위가 포함되는지에 대한 정의를 내리는 것은 각 조직의 책임이며, 이러한 행위는 각 기업마다 서로 다를 수 있습니다. IBM은 소셜 미디어 사이트에서의 올바른 행위가 무엇인지에 대한 기준을 세운 기업의 훌륭한 본보기입니다.

IBM 내에서 이 기준은 "IBM 소셜 컴퓨팅 가이드라인"으로 불리며, 모든 IBM 직원이 필수적으로 충실히 이행해야 하는 더 넓은 범위의 비즈니스 행동 가이드라인(BCG)에 포함됩니다. 이러한 가이드라인은 IBM이 소셜 미디어 사이트에서의 "올바른 행위"로 인정하는 행위에 대한 기준을 정합니다. 더욱 중요한 점은, 올바른 행위가 무엇인지 정의함으로써, IBM이 어느 정도 재제를 가할 수 있는 올바르지 않은 행위 수준이 결정된다는 것입니다.

평가

사용자의 인식 및 기업의 기준도 중요하지만, 이것만으로는 기업을 공격으로부터 충분히 보호할 수 없는 경우가 많습니다. 또한, OSINT 평가 절차를 구현 및 실행하는 것이 중요합니다. 침투 테스트와 마찬가지로, OSINT 수집은 보안 전문가가 공격자가 해당 기업을 바라보는 시각을 이해하고, 나아가 특정한 취약점이 어디에 있는지 파악하는 것을 돕습니다. 그리고 기업은 이 지식을 통해 소셜 미디어 사이트로부터 수집 가능한 인텔리전스를 이용한 2차 또는 3차 공격을 해결하기 위한 보안 작업의 우선순위를 결정할 수 있습니다.

대부분의 OSINT 수집 프로세스는 높은 품질의 침투 테스트 프로세스에 통합되어 있습니다. 실제로, PTES(Penetration Testing Execution Standard), 특히 OISINT를 포함하고 있는 PTES는 OSINT 관련 활동을 실행하기 위한 가이드라인의 본보기가 됩니다. 가이드라인은 일회성 활동에 주로 중점을 두고 있지만, 기업은 이러한 프로세스를 지속적으로 이용하기를 원합니다. 따라서, OSINT 데이터 및 이용되는 프로세스에 대한 보고를 표준화하는 것이 중요합니다.

프로세스가 실행되어 데이터가 생성되면, 잠재적인 공격 지점을 확인하기 위해 이후에 OSINT 데이터를 이용하는 침투 테스트와 마찬가지로, 동일한 데이터를 이용해 잠재적인 대상을 확인할 수 있습니다. 대상을 확인한 후에는, 보안 모니터링 및 보호를 통해 위험 및 이러한 공격 대상에 대한 영향을 줄일 수 있습니다.

결론

소셜 미디어는 보안 환경 및 인텔리전스 수집 방법을 바꾸어 놓았으며 이전에 일반적이라고 생각했던 상태로 되돌아갈 가능성은 낮습니다. 그 결과, 공격자가 최적의 공격 대상 및 공격 방법을 결정하는 데 이용할 수 있는 데이터가 풍부한 환경이 조성되었습니다. 반대로, 이러한 환경에서 기업의 보안 팀은 동일한 정보를 이용하여 조직 내의 "어떠한 대상"이 공격을 받을 가능성이 높은지 더 확실히 예측할 수 있게 되었습니다.

공격자가 이 프로세스를 도입하여 공격 방법론을 발전시키고 있다는 것은 분명합니다. 기업의 보안 팀도 반드시 해당하는 기능을 확보해야 합니다. 이러한 작업은 소셜 미디어가 어떻게 공격에 이용될 수 있는지를 이해하는 것에서부터 시작하며, 공격자가 데이터를 수집하는 데 이용하는 방법론을 이해할 수 있게 됩니다. 수집된 데이터는 기업의 보안 팀이 유용하게 이용할 수 있도록 정리하고 저장해야 합니다. 마지막으로, 보안 작업이 완료되면, 관련 데이터를 이용하여 패턴을 확인할 수 있으며, 분석을 통한 더욱 직관적인 보안 프로세스를 위한 위험 관리 등식에 통합될 수 있습니다.

기업의 신원 및 액세스 인텔리전스

사용자에게 온라인 자원에 대한 안전하고 통제 가능한 액세스 권한을 제공하는 동시에 이 자원을 비인가 사용자로부터 보호해야 할 필요성은 과거 그 어느 때보다 커지고 복잡해졌습니다. 이러한 결과의 원인으로는 여러 가지 요인이 있으며, 예를 들어 내부 및 외부 사용자의 기하급수적인 증가 및 변화, 데이터 및 애플리케이션에 액세스하기 위해 이용하는 디바이스 수와 유형, 그리고 자원에 액세스하는 장소 및 방법이 포함됩니다.

비즈니스파트너와의 웹 기반 협업, 제3자 공급업체 및 온라인 소비자에게 액세스 권한을 개방해야 할 필요성, 그리고 클라우드 기반 서비스 이용의 증가로 인해 지속적으로 조직의 경계선이 불분명해 졌으며 조직이 외부 위협, 부주의한 직원과 부정한 내부자 때문에 발생하는 위협에 노출되어 있습니다.

동시에, 사이버 범죄, 스피어 피싱 공격 및 산업 스파이도 모두 증가하고 있습니다. 이러한 위험은 지속적으로 증가하고 있는 복잡한 규정 요구사항 및 개인정보 관련 문제의 증가와 복합적으로 발생하여 액세스 및 인증 수준의 관리가 비즈니스 및 IT 과제로 대두되었습니다. 최근에는 뉴욕 타임즈, 월 스트리트 저널, 미국 연방 준비은행 등과 같은 일류 조직에서 발생한 유명 보안 침해 사고가 언론을 통해 보도되었으며, 이러한 사실은 기업 전체에서 사용자 액세스 권한 및 활동을 통제하고 모니터링하는 작업이 매우 중요하다는 것을 일깨워 주고 있습니다.

데이터 및 평판 보호의 중요성

보안 위험 관리 및 보안 정책의 지원은 대부분의 CIO와 보안 및 위험 전문가의 주요 과제가 되었습니다. 그 이유는 무엇일까요? 기업들은 시스템의 보안이 침해되거나 기밀 데이터가 유출되는 경우 해당 기업의 평판 및 기업의 경쟁력에 악영향을 미칠 수 있다는 것을 이해하고 있으며, 컴플라이언스 미이행에 대한 벌금이나 제재가 가해질 수도 있기 때문입니다. 실제로, 2012년 IBM 글로벌 평판 위험 및 IT 연구[67]에서 이사진들은 데이터 도난/사이버 범죄가 기업의 평판 및 경쟁력에 대한 가장 심각한 위협이라고 진술했으며, 이는 시스템 고장 또는 다른 문제보다 훨씬 중요한 것으로 나타났습니다.

오늘날의 신원 및 액세스 관리 솔루션은 "이로운 사람은 허용하고 해로운 사람은 허용하지 않는" 수준 이상의 해결책을 포함해야 합니다. 직원들이 비밀번호를 공유하거나 기업의 데이터를 분실하고, 불만을 가진 내부자가 정보를 도용하는 경우에는 "이로운 사람"도 보안 위험을 발생시킬

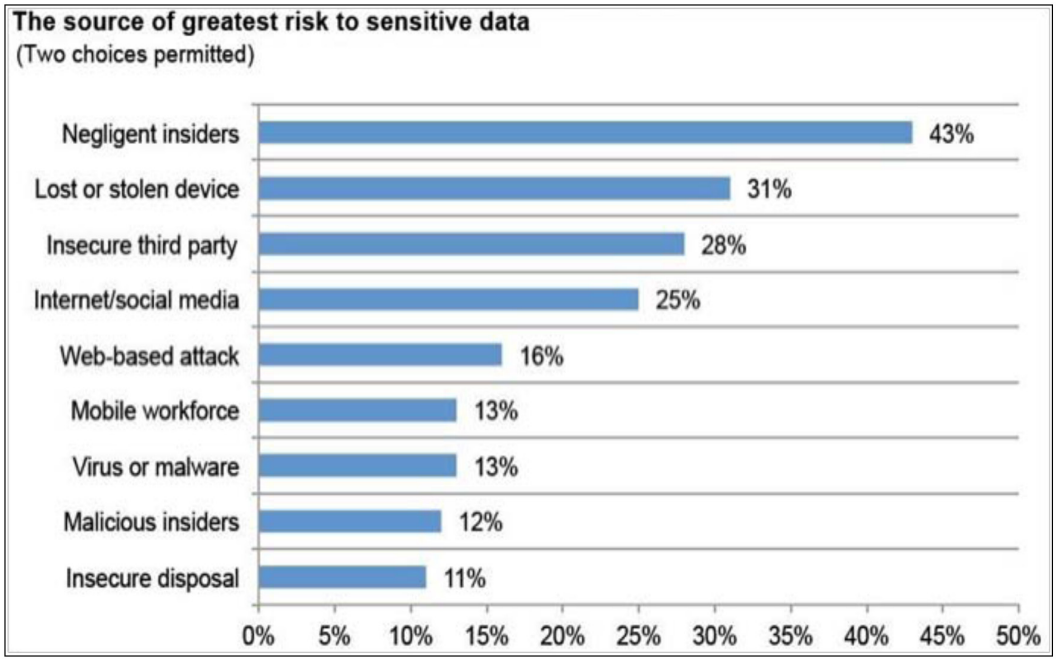
67 2012년 9월에 IBM Global Technology Services에서 발행한 2012년 IBM 평판 위험 및 IT 연구

수 있습니다. 2012년에 IBM/Ponemon이 실시한 C-레벨 이사진에 대한 연구에서 민감한 데이터에 대한 가장 큰 위험은 불만을 가진 내부자인 것으로 나타났습니다.[68] 직원, 계약업체, 공급업체, 클라우드와 SaaS 공급업체 및 소비자를 포함한 다양한 사용자 층을 고려하면, 사용자 액세스 관리 및 모니터링이 전체적인 보안에 매우 중요한 이유를 쉽게 알 수 있습니다.

실제로, 내부자의 위협 문제는 널리 퍼져 있으며, 미국의 백악관에서도 이와 관련하여 반응이 있었습니다. 2012년 11월, 미국의 버락 오바마 대통령은 내부자 위협 프로그램 시행을 위한 최소한의 요소에 대한 개요를 설명한 대통령 지침[69]을 발표했습니다. 이러한 권고사항 중 일부는 핵심 위협과 관련된 정보를 수집 및 통합하고 중앙 집중식으로 분석 및 대응하기 위한 역량을 개발할 것과 직원이 보호된 네트워크를 이용하는 것을 모니터링하도록 지시하고 있습니다. 이러한 권고사항은 보안 이벤트의 보고와 분석 및 직원의 사용 패턴 감시가 조직의 내부 위협 식별 및 방지에 얼마나 도움이 되는지를 잘 나타내고 있습니다. 많은 조직의 경우, 이러한 권고사항은 향후 미국 정부 기관과 비즈니스를 하기 위해 필요한 요구사항이 될 수도 있습니다.

2012년 IBM/Ponemon Institute의 조사 결과

2012년 2월 27일: IBM과 Ponemon Institute는 최근 민감한 데이터 및 엄격한 보안 규정의 준수를 고려했을 때 각 조직에서 가장 중요하다고 생각하는 요인을 확인하기 위해 265명의 C-레벨 이사진을 대상으로 조사를 실시했습니다.



68 2012년 2월에 IBM과 Ponemon이 265명의 C-Level 이사진을 대상으로 실시한 조사, "민감한 데이터에 대한 가장 큰 위험의 근원(The Source of Greatest Risk to Sensitive Data)"

69 http://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand

신원 및 액세스 거버넌스 관련 위험을 감소시키는 방법

사용자가 기한이 지난 또는 부적절한 수준의 액세스 권한을 갖게 되는 경우 보안 침해 사고 및 컴플라이언스 관련 문제가 발생할 수 있습니다. 액세스 권한에 현재의 요구사항 및 실제 사용 패턴이 반영되어 있지 않은 경우 내부자 위협 활동의 가능성은 상당히 높아집니다. 또한, 공격자는 열악하게 통제되는 관리자 권한을 이용해 공격을 발생시키거나 시스템을 변경하여 사용자 액세스 신임 정보 등의 민감한 정보를 포착하기 위한 도청을 실행할 수도 있습니다. 열악하게 통제 및 모니터링되는 사용자 액세스 권한 문제가 권한의 오남용에 대한 가시성의 부족과 복합적으로 발생하는 경우에는, 1차적인 보안 절차에 대해 그 누구도 진지하게 생각하고 있지 않다는 것을 나타낼 수 있으며, 이는 부정한 활동이 발생할 가능성을 높일 수도 있습니다.

신원 및 액세스 거버넌스는 사용자 역할을 정의하고 사용자의 수명주기 전체에서 액세스를 준비, 관리 및 실시하는 방법에 대한 가이드라인을 제공합니다. 조직은 더 큰 책임감과 투명성을 통해 사용자의 액세스 요구사항을 관리하기 위한 자원을 확보하려고 할 수도 있으며, 이러한 해결책을 이용하면 거버넌스를 견고히 하고 사용자의 액세스를 더욱 효과적으로 실행할 수 있습니다. 관리자는 이러한 도구를 이용해 사용자의 계정 및 권한이 해당 사용자의 역할에 알맞게 업데이트되도록 할 수 있습니다. 또한, 신원 및 액세스 거버넌스는 조직이 특정 사용자가 어떠한 자원을 이용해 어떠한 작업을 할 수 있는지에 대해 더욱 철저하고 지속적으로 실행되는 세밀한 통제를 구현할 수 있도록 도울 수 있습니다. B2B(business to business) 및 B2C(business to consumer) 환경에서는 사용자의 역할 및 실제적인 필요에 따라 사용자의 액세스 권한이 부여되었는지 여부를 확인하는 것이 특히, 중요합니다. 액세스 권한은 이미 수립되어 있는 보안 정책을 따라야 하며 사용자의 행위를 모니터링하기 위한 감사 및 보고 도구를 통해 뒷받침 되어야 합니다.

내부자 위협을 관리하기 위한 보안 인텔리전스

SIEM(Security Information and Event Manager)과 로그 관리 도구는 이상 징후를 식별하고, 위험하거나 부적절한 행위를 강조하고, 컴플라이언스 보고를 지원하는 데 유용한 로그 파일 및 측정 기준을 제공할 수 있습니다. IAM(Identity and Access Management)와 관련된 로그 및 정보를 수집하고 이를 다른 중요 보안 이벤트 및 정보와 연관시키는 작업은 부적절한 또는 의심스러운 사용자 행위 또는 내부자 위협을 신속히 발견하는 데 도움이 됩니다.

신원 거버넌스 프로세스를 구축하고 기업이 클라우드 및 모바일 환경을 더욱 안전한 방법으로 관리하기 위해서 이러한 수준의 신원 및 액세스 인텔리전스가 점점 더 많이 요구되고 있습니다.

신원 및 액세스 인텔리전스는 다음과 같은 역할을 수행할 수 있습니다.

- 모바일 및 기존 엔드포인트로부터의 액세스 상황에 대한 더욱 심도 있고 풍부한 이해를 제공
- 일반 사용자 및 권한을 갖는 사용자의 신원 역할을 더욱 정확하게 정의하기 위한 활동에 대한 정보를 제공
- 위협을 발생시키는 이상 징후 행위를 인지
- 고객이 빠르고 정확하게 위협에 대응하여 보안 침해가 발생하기 전에 기업을 보호

보안 인텔리전스를 이용하면, 관리자는 어떤 사용자가 드러내고 있는 액세스 패턴이 해당 사용자의 조직 내 역할 및 권한과 일치하는지 신속하게 확인할 수 있습니다. 예를 들어, 정당한 사용자이지만 활동은 의심스러울 수도 있습니다(비인가된 기록에 액세스). IBM Security 포트폴리오에서 제공하는 것과 같은 보안 인텔리전스 도구는 다양한 로그 데이터 및 네트워크 흐름을 실행 가능한 IT 포렌식으로 통합하고 상호 연관시켜 공격의 패턴, 이상 징후, 액세스, 기밀 데이터 사용 현황 및 내부자 위협을 식별할 수 있습니다. 데이터 정규화, 사전에 정의된 사용자 정의 가능한 상관관계 규칙 및 정책과 컴플라이언스 중심 검색을 이용하면, 보안 데이터 및 네트워크 원격 측정 정보의 다양한 집합을 쉽게 분석하고, 보안 위협을 빠르게 조사 및 해결하여 위험을 낮출 수 있습니다. 완벽한 SIEM(Security Information and Event Management) 솔루션을 이용하면 위와 같은 기능에 고급 위협 보호 및 정책 인지 컴플라이언스 관리 기능을 추가하여 전체 IT 인프라에 대해 상황별로 실행 가능한 감시 기능을 제공할 수도 있습니다. 이를 통해, 오랜 시간 동안 발생하는 애플리케이션의 부적절한 사용, 악성 활동 및 내부자 부정행위 등의 발전된 위협을 탐지 및 해결할 수 있습니다.

요약

사용자 관리 및 액세스 통제는 비즈니스의 가장 중요한 요소가 되었으며, 이로 인해 기업의 경계선 내의 모든 영역을 포괄하는 광범위한 IAM 인텔리전스 솔루션에 대한 수요가 증가하고 있습니다. 클라우드 및 모바일 자원에 대한 사용자 액세스를 확대하려는 경우에는, 사용자 액세스 활동을 모니터링하고, 이상 징후 및 자산의 오남용을 식별하고, 컴플라이언스를 외부에 검증할 수 있는 신원 및 액세스 인텔리전스 솔루션의 사용을 고려해야 합니다. 클라우드 및 모바일 보안에는 많은 구성요소가 포함되며, 사용자 액세스에 대한 모니터링 및 보고는 경계가 없는 새로운 형태의 근무 공간에서 이용되는 기업의 자산을 보호하는 데 매우 중요한 요소입니다.

신원 및 액세스 인텔리전스가 IT 자산을 사전에 보호하고 클라우드/모바일 사용자의 액세스를 강화하는 데 어떠한 도움을 제공할 수 있는지에 대한 자세한 정보를 확인하려면, EMA Associates의 백서 **신원 및 액세스 인텔리전스: 기업 보안의 혁신(Identity and Access Intelligence: Transforming Enterprise Security)**을 다운로드하십시오. .

단원 III
새로운 보안 추세

이 단원에서는 지금이 투자해야 할 시기가 아닌가 기업들이 고민할 정도로 급속도로 발전하고 있는 기술 분야를 살펴보겠습니다. 또한, 빠른 기술 채택을 통해 위협 및 악용이 이용되고 있는 분야 및 기업이 보안에 집중력을 유지할 수 있는 방법을 설명하겠습니다.

2014년까지 기존의 사용자 컴퓨팅 디바이스 보안보다 모바일 컴퓨팅 디바이스 보안 강화

이러한 예측은 IBM의 기술 동향 전망의 일환으로, 확실한 예측입니다. 또한 표면적으로는 설득력이 없는 것처럼 보일 수 있지만, 기존의 보안 통제 동향 및 식견을 갖춘 보안 관리자가 관련 시장에 요구하고 있는 필수조건을 근거로 하고 있습니다. 이러한 통제 동향의 일부 및 관련 기술을 살펴보기 전에, 원인부터 살펴보겠습니다.

대부분의 기업에게 모바일 사용의 정착은 BYOD(bring your own device)를 지원하는데 있어 가장 중요하고 광범위한 과제입니다. 모바일 계획을 실행하기 전에 몇몇 기업은 BYOD 프로그램을 실행해 왔으며, 이러한 프로그램의 대부분은 단순히 기업의 데스크톱에 대한 관점을 제공했던 VDI(Virtual Desktop Infrastructure)의 사용에 의존하여 존재했습니다. 그리고 모든 보안 통제를 처리하지 않음으로 인해 신뢰할 수 없는 하드웨어에서의 Type 2 하이퍼바이저 사용을 초래했던 경우도 있었습니다.

그러나 몇몇 기업은 이러한 VDI 접근법을 통한 데이터 및 인프라에 대한 액세스의 분리 및 통제에 만족했지만, 이는 모바일 디바이스 사용을 방해하는 요소였습니다.

모바일 BYOD 시나리오에서 VDI 접근법을 사용함에 따라 몇 가지 과제가 발생했으며, 대부분은 사용성 및 이용 사례 영역과 순수한 보안 통제 관련 사항의 충돌이었습니다. VDI는 일반적으로 중단되지 않는 고속 연결성에 의존하며, 이 연결성은 일반적인 모바일 디바이스 이용 사례에서는 존재하지 않습니다. 4G 네트워크의 보급으로 인해 모바일 네트워크의 속도가 상승함에 따라서 지속적인 연결성의 비용(화폐 가치적 비용 및 디바이스 배터리 수명의 비용)은 계속해서 하락했으며, 이로 인해 VDI를 모바일 디바이스 환경에서 사용하는 것과 관련하여 해결해야 할 과제가 생겼습니다. 대부분의 모바일 디바이스의 폼팩터는 데스크톱에서 일반적으로 이용되는 많은 수의 VDI 호스트 솔루션과 충돌합니다. 이전에는 이러한 VDI 환경을 사용하려면 마우스와 키보드에 의존했지만, 대부분의 애플리케이션은 순수한 터치 인터페이스의 이용을 위해 개발되지 않았으므로, 일반적인 스마트폰의 작은 화면을 방치해 왔습니다. 결과적으로, VDI의 장기적인 이용이 모바일 디바이스에 널리 수용되는 경우에는 애플리케이션 재설계 및 스트리밍 접근법이 필요할 수도 있습니다.

순수한 모바일 환경에서의 VDI를 사용할 때 발생하는 이러한 과제로 인해 많은 수의 보안 관리자로부터 개인 모바일 디바이스를 민감한 기업에서의 이용을 위한 시나리오에서 사용할 수 있도록 하기 위한 새로운 요구사항이 발생했습니다. 개인 소유 디바이스 환경에서 기업의 보안 관련 사항을 처리하고자 하는 요구사항은 보안 기술 업계가 이러한 필요사항을 처리하기 위한 혁신을 시도하는 데 큰 동기부여로 작용했습니다. 이러한 상황은 IBM이 모바일 컴퓨팅 디바이스에는 기존의 엔드포인드 디바이스에 존재하지 않았던 향상된 보안 통제 및 기술이 필요할 것이라고 예측하는 근거가 되었습니다. 또한, 모바일 통제 및 기술의 동향이 기존 디바이스의 사용에도 점차적으로 영향을 미치는 뚜렷한 추세가 확인되었습니다.

이와 관련하여 이미 발생했거나 곧 발생할 것으로 예상하는 몇 가지 구체적인 예시를 살펴보겠습니다.

애플리케이션 샌드박싱

대부분의 모바일 운영 체제는 처음부터 자체적으로 애플리케이션 샌드박싱을 지원해 왔습니다. 실제로, 애플리케이션 샌드박싱은 운영 체제의 동작 방식에 있어서 매우 기본적인 부분이며, 단순한 보안 관련 이유 이상의 다른 이유(디바이스를 통해 이용할 수 있는 애플리케이션 환경 또는 "스토어(store)"의 제한)로 인해 포함된 것입니다. 널리 이용되고 있는 다양한 모바일 운영 체제 전반에서의 애플리케이션 샌드박싱 구현에서 확인한 유일한 차이점은 "개방성"의 정도였으며, 이는 애플리케이션 개발자용 프로그래밍 인터페이스를 통해 노출되는 시스템 서비스와 관련이 있습니다. 이러한 시스템 수준 서비스의 제한 및 다른 애플리케이션과 관련된 정보에 대한 액세스의 제한은 이전에 기존의 컴퓨터 운영 체제에서는 볼 수 없었던 근본적인 차이점입니다. 그리고 샌드박스를 이용한 브라우저 등이 기존의 컴퓨터 운영 체제에서 이용되는 것은 이미 확인했습니다. 지난해에는 기존의 일부 운영 체제에서도 이러한 기능을 이용할 수 있게 되었습니다. 데스크톱 운영 체제 벤더들은 이러한 접근법의 위험 감소에 대한 이점을 이해하고 있으며 새로운 버전에서 이 접근법을 구현하기 시작했지만, 기존 레거시 애플리케이션에 대한 지속적인 의존성으로 인해 접근법이 표준화되기 까지는 시간이 걸릴 것입니다.

서명된 코드 제어

애플리케이션 샌드박싱과 마찬가지로, 디지털 방식으로 서명된 애플리케이션의 설치 및/또는 실행만을 허용하는 방식을 이용 또는 시행하는 것은 현재 널리 이용되고 있는 모바일 운영 체제가 처음부터 제공했던 또 다른 일반적인 모바일 운영 체제의 특징입니다. 많은 사람들은 이러한 방식이 모바일 운영 체제 벤더가 금전적인 이익을 위해 요구하는 필수적인 통제 사항이라고 말합니다. 모바일 OS마다 그 복원성이나 실행 사항은 차이가 있지만, 승인된 애플리케이션만을 설치할 수 있다는 것은 일반적인 사용자에게 기존의 운영 체제는 널리 제공하지 않았던 근본적인 보안 향상을 제공합니다. 이것은 기존의 데스크톱 시스템에서 도입할 것으로 예상되는 또 다른 분야입니다.

원격 디바이스 또는 데이터 삭제

모바일 디바이스에 발생하는 분실 및 도난의 위험이 증가함으로 인해, 모바일 운영 체제 벤더들은 개발 초기부터 원격으로 디바이스의 모든 내용 또는 선택된 애플리케이션 및 관련 데이터를 삭제하는 기능을 포함시켜 왔습니다. 이는 이러한 삭제 기능을 지원하지 않았던 기존의 데스크톱 운영 체제에서 사용되었던 통제 방식과는 큰 차이를 보입니다. 이와 관련된 일화로서, 1% 미만의 기업만이 제3자 기술을 통해 원격 삭제 기능을 포함 또는 요구해 왔다고 합니다. 확실히, 기존 데스크톱 컴퓨팅에 대해 이러한 요구사항이 없었다는 것은 모바일 디바이스의 분실 및 도난의 위험이 증가했기 때문일 가능성이 높습니다. 일부에서는 원격으로 데이터, 애플리케이션 및 디바이스를 삭제해야 할 필요성은 직원들이 랩톱을 기업 외부로 반출하기 시작했을 때부터 존재해 왔다고 말합니다. 많은 기업에서는 대부분의 기존 컴퓨팅 디바이스에 저장된 정보의 노출을 방지하기 위해 디스크 전체의 암호화를 요구합니다. 어떠한 경우에서도, 원격 삭제 기능이 기존의 운영 체제에 곧 포함될 것 같은 조짐은 없었습니다.

생체 및 상황 인식 인증

확실히, 기존의 컴퓨팅 디바이스는 얼마 전부터 생체 인식 기능을 포함해 왔지만, 생체 및 상황 인식 인증 (biocontextual authentication) 기능은 포함하지 않았습니다. 먼저 모바일 컴퓨팅에서 이용되는 이러한 새로운 용어를 살펴보겠습니다. 지난해쯤, 인증에 대한 위험 기반 접근법을 제공하기 위한 연구가 시작되고 관련 기술이 발표되기 시작되었습니다. 이 접근법은 인증 관련 결정을 평가하기 위해 더 많은 양의 정보를 이용합니다. 일반적으로 모바일 디바이스는 위험 기반 인증 결정에 이용될 수 있는 추가적인 정보 요소를 제공할 수 있습니다. 이러한 요소로 물리적인 위치, 네트워크 ID, 음성 인식, 눈 또는 얼굴 인식 등을 생각해 볼 수 있습니다. 이러한 요소는 모두 결합되어 엔트로피를 증가시킬 수 있으며, 이는 기존의 데스크톱 컴퓨팅 시나리오에서 일반적으로 이용되는 비밀번호에 대한 잠재적인 강화 또는 대체로 작용할 수 있습니다.

이러한 연구 및 혁신의 대부분은 모바일 디바이스에서 인증 보안성을 낮추지 않으면서도 사용성을 향상시키는 데 이용되고 있습니다. 대부분의 모바일 디바이스에서 제한된 화면 공간을 이용하는 소프트웨어 기반 키보드로는 복잡한 비밀번호를 입력하기가 어렵습니다.

이 접근법이 발전되고 기존의 사용자ID/비밀번호 조합에 대한 개선사항으로 받아들여짐에 따라, 이러한 기능은 기존의 컴퓨팅 디바이스에서 복잡한 비밀번호 사용에 대한 보안성 향상이라는 점차적인 효과로 작용할 것으로 예상됩니다.

개인 환경 또는 역할의 분리

소수의 기업만이 가상화된 데스크톱 솔루션을 이용해 BYOD를 처리하여 기업의 애플리케이션과 데이터를 나머지 개인 소유 디바이스로부터 분리해 왔지만, 더 많은 수의 기업은 모바일 디바이스에서 개인 환경(persona)을 분리하거나 두 개의 개인 환경을 구성하기 위한 방법을 원하거나 요구해 왔습니다. 사용 또는 도입에 대한 이러한 차이는 더 많은 수의 디바이스로 인해 개인 소유 모바일 디바이스에서 위험이 발생할 확률이 BYOD 프로그램으로 관리되는 개인 소유 PC에 비해 더 높기 때문일 수 있습니다.

일부 기업은 개인 소유 디바이스에 저장된 데이터에 대한 컨테이너 또는 통제된 별도의 환경을 제공하기 위한 솔루션을 도입했습니다. 이러한 접근법은 위험을 낮출 수 있지만, 또한 기반 디바이스 및 운영 체제의 무결성과 관련된 일부 위험을 방치하고, 제한된 기능을 제공(기업용 애플리케이션을 컨테이너로 이식해야 하는 경우가 많으며 컨테이너로 이식된 애플리케이션의 수가

많지 않음)한다는 것이 밝혀졌으며, 사용성에 대한 절충 사항이 존재한다는 것이 확인되었습니다. 이는 모바일 디바이스의 특성상 많은 사람들이 기존에 사용하던 원래 OS 애플리케이션을 컨테이너 내에 존재하는 자신만의 유사 애플리케이션으로 교체하기 때문입니다. 이러한 많은 이유로 인해, 기업들은 해당 기능을 기본적으로 제공하는 솔루션이 등장할 때까지 이 기술을 주로 임시적인 대응책으로 이용해 왔습니다.

이 솔루션은 RIM의 기존 Blackberry 제품인 Balance의 형태로 구현된 모바일 운영 체제의 기본적인 기능이라는 것을 이미 확인했습니다. 기존의 데스크톱 컴퓨팅 환경에는 이와 유사한 접근법이 존재하지 않으며, 이 접근법이 MEAP(이후에 논의)의 사용과 결합되는 경우에는 기업에게 기존의 컴퓨팅 운영 체제를 뛰어 넘는 일련의 보안 통제 기능을 제공하게 될 수도 있습니다.

Type 2 하이퍼바이저 기술은 기존 컴퓨팅 디바이스에서 이용되어 왔으며, 역할을 분리하기 위한 방법으로서 이용된 적도 있지만, Type 1 하이퍼바이저가 사용자의 컴퓨팅 디바이스에서 사용되는 것은 본 적이 없습니다. (Type 2 접근법에 비해) 위험 표면의 면적을 감소시키는 Type 1 하이퍼바이저의 장점을 설명하려는 것은 아니지만, Type 1 하이퍼바이저의 기능을 일부 모바일 디바이스에 포함시키기 위한 작업이 이미 진행 중이라는 것을 언급할 필요가 있습니다. 예상할 수 있는 바와 같이, 이러한 작업의 목적은 최소한의 자원 오버헤드 및 사용자 복잡성을 유입시키는 방법으로 하나의 디바이스 내에서 실제로 한정적인 역할 분리 기능을 제공하는 것입니다. 이를 통해 기업에는 사용의 개인 애플리케이션, 데이터 및 컴퓨팅 환경에 대한 높은 수준의 분리 기능을 제공하면서도 모바일 사용자에게는 하나의 물리적 디바이스 내에 두 개의 디바이스를 제공할 수 있게 됩니다.

Type 1과 Type 2 하이퍼바이저 기술의 차이점은?
차이점을 좀 더 자세히 설명하면, Type 1 하이퍼바이저는 하나의 "주(host)" 운영 체제가 필요하지 않으며, 따라서 다수의 게스트 운영 체제를 디바이스의 하드웨어에 직접 설치할 수 있습니다. Type 2 하이퍼바이저에서는 디바이스 하드웨어와 게스트 운영 체제 사이에 디바이스 운영체제가 필요합니다. 예상할 수 있는 바와 같이, Type 2 하이퍼바이저 시나리오에 존재하는 이러한 주 운영 체제에 대한 필요성으로 인해 추가적인 공격 가능성이 발생하며, 주 운영 체제는 보안 통제를 강화하여 위험을 통제해야 합니다.

안전한 모바일 애플리케이션 개발

지난 몇 년간 애플리케이션 취약점은 기업에 대한 주요 공격 벡터가 되었습니다. 많은 경우, 원인은 웹 애플리케이션이나 미들웨어였지만 기본 클라이언트 애플리케이션 또한 공격이 증가하는 데 기여했습니다. 기존의 컴퓨팅 디바이스를 위해 개발된 대부분의 레거시 애플리케이션과는 달리, 오늘날의 하이브리드 및 기본 모바일 애플리케이션은 개발 프로세스의 중요한 부분인 보안성을 유지한 상태로 개발되었을 가능성이 더 높습니다. 많은 기업은 SSDLC(Secure Software Development Life Cycle) 이니셔티브에 대한 큰 발전을 이루었으며 오늘날의 모바일 애플리케이션 개발은 SSDLC 프로세스로 인해 많은 이점을 얻을 수 있습니다. 또한, 현재는 자격 취득 또는 프로덕션 환경에서 개발이 이루어지는 대신, SSDLC 프로세스에 포함되는 안전한 개발을 지원하기 위한 도구가 이용됩니다. 결과적으로, 더 많은 기업은 기존의 레거시 애플리케이션에 비해 더욱 안전하게 애플리케이션을 개발하게 될 것입니다. 기존의 일부 컴퓨팅 애플리케이션은 취약점의 미공개로 인해 그 수명을 마치게 될 수도 있으며, 기존의 버전은 도태되고, 새롭고 더욱 안전하게 개발된 대체 애플리케이션으로 교체될 것입니다.

MEAP(Mobile Enterprise Application Platform)

기업 내 모바일 사용의 정착으로 인해 기존에는 없었던 완전히 새로운 기술이 등장하게 되었습니다. MEAP는 다수의 모바일 운영 체제에서 애플리케이션 개발의 다양성과 복잡성으로 인해 개발되었습니다. MEAP의 목적은 이러한 다양성 속에서도 개발자가 지속적으로 개발 및 배치 작업을 진행할 수 있도록 여러 모바일 운영 체제에서 다수의 디바이스 폼팩터를 처리하는 것을 돕는 것입니다. 모바일 애플리케이션의 개발 및 서비스에 이용되는 특정한 도구를 제공하는 데는 큰 부가적인 이점이 있습니다. 그것은 바로 애플리케이션 수준에서 보안 통제를 실행할 수 있는 가능성입니다. 이를 이용해 다수의 이용 사례를 통해 알 수 있듯이 여러 가지 방법 및 이점을 제공할 수 있다는 점이 중요합니다.

많은 기업은 고객에게 모바일 애플리케이션을 제공하기를 원합니다. 이러한 상황은 디바이스 자체의 신뢰성이나 통제 기능이 전무한 일반적인 시나리오에 해당합니다. MEAP를 이용하여 애플리케이션 수준에서 보안의 일부 측면을 통제함으로써, 데이터를 디바이스에 남길 데이터, 암호화의 여부, 통제되는 시간의 길이, 주어진 데이터 세트 또는 기능을 이용하기 위해 필요한 인증 수준, 그리고 애플리케이션 수준의 통제를 이용하지 않으면 처리하기 어려운 다른 많은 시나리오를 통제할 수 있습니다.

직원용 애플리케이션을 개발하는 기업의 경우, 이와 유사한 접근법을 어느 정도의 디바이스 수준의 통제 기능과 함께 이용하거나 또는 단독으로 이용하여 모바일 디바이스에 저장된 기업의 데이터에 대한 액세스 및 사용을 통제할 수 있습니다. 이러한 접근법은 일반적으로 기존의 컴퓨팅 시나리오에는 존재하지 않았던 애플리케이션 수준의 데이터 통제를 제공하므로, 이러한 접근법이 기존의 접근법에 비해 더욱 한정적인 통제 기능을 제공하는

이유를 쉽게 파악할 수 있습니다. 이 보고서에서 다룬 생체 및 상황 인식 인증과 같은 다른 개념과 결합되면 MEAP가 확장되어 위험 기반 접근법을 기반으로 애플리케이션 기능 및 데이터에 대한 액세스를 제공할 수 있습니다. 대부분의 기업의 경우 MEAP의 도입은 아직 초기 단계이지만, 기업들이 디바이스 수준 및 애플리케이션 수준의 보안 통제의 균형에 더욱 익숙해지면 MEAP는 앞으로 기본적인 접근법이 될 수도 있습니다. 또한, 이러한 접근법을 이용하면 기존에는 신뢰도가 낮으며 분실 및 도난에 취약한 것으로 여겨졌던 디바이스에서의 모바일 금융 거래와 같은 더욱 위험한 컴퓨팅 작업을 실행할 수 있습니다.

MEM(Mobile Enterprise Management)

기업용 디바이스 관리와 기업용 애플리케이션 관리가 결합되면 일부에서 MEM(Mobile Enterprise Management)이라고 일컫는 상태를 초래할 것입니다. 이러한 접근법은 여러 디바이스 플랫폼 및 애플리케이션에서 풍부하게 결합된 통제 기능을 제공하면서 동시에 위험 기반 컴퓨팅 접근법을 이용할 수 있도록 해주는 생체 및 상황 인식 인증을 이용할 수 있습니다. 또한, MEM을 위한 기술 솔루션을 지속적으로 추진하면 관리 복잡성이 감소되고 보안 책임자는 현재 이용 가능한 것보다 더욱 세밀한 통제 기능을 이용할 수 있을 것입니다. 이상적으로는, 기존의 디바이스에 대한 낙수 효과로서 기업이 광범위한 단일 플랫폼을 이용해 인프라 위험 및 애플리케이션 위험을 관리할 수 있게 되는 것을 기대할 수 있습니다. 이러한 MEM 추세는 실제로 일어나고 있는 일이라기 보다는 예측에 가깝지만, 모든 컴퓨팅 디바이스의 관리를 단일 플랫폼으로 통합하는 것은 이치에 맞으므로, 이와 밀접하게 관련된 애플리케이션 수준의 통제를 동일한 플랫폼에 통합하여 위험 관련 의사 결정 작업을 향상시키고 사용성을 최대화하는 것은 적절한 판단이라고 할 수 있겠습니다.

예측 결론

이러한 항목들은 모바일 컴퓨팅으로 인해 기업 보안 업계에 도입된 새로운 보안 통제 접근법의 일부만을 보여주고 있지만, 이 중 많은 수는 기존 디바이스의 운영 체제에 유입되어 전체적인 보안성을 높이고 위험을 낮출 수도 있습니다.

모바일 보안 통제—현재 상황은?

이 보고서의 앞 부분에서는 기업에서 모바일 디바이스 분야에 도입하고 있는 또는 요구하고 있는 통제 기능과 관련하여 산업 전반에 걸쳐 관측된 베스트 프랙티스 및 추세의 진행 상황을 확인했습니다. 2012년 동안 이전에 비해 더 많은 기업이 BYOD 또는 개인 소유 디바이스를 지원했으며 이는 계속 진행되는 추세인 것으로 결론을 내려도 무방할 것입니다. 지난 2년 동안, IBM Security는 전 세계적인 고객사 2,000곳 중 수백 곳의 고객사와 대화했으며, 이들 중 단 세 곳만이 어떠한 종류의 BYOD

프로그램도 실행할 계획이 없다고 답했습니다. 대부분의 BYOD 프로그램은 제한된 기능을 가지고 있으며, 일정한 수준의 기본적인 연결성, 그리고 이메일 및 달력과 같은 기업 정보 관련 기능을 제공합니다. 훨씬 더 적은 수의 기업은 협업 및 메시지 전송과 같은 더욱 광범위한 비즈니스 기능을 포함하도록 BYOD 프로그램을 발전시켰습니다. 그리고 더 적은 수의 기업은 비즈니스 애플리케이션에 포함된 매우 민감한 데이터를 지원하는 수준까지 발전했으며, 이 중 일부는 이전에 논의한 MEAP 등을 통해 이러한 발전을 이루었습니다. BYOD로 인해 발생할 수 있는 추가적인 비용 및 복잡성을 고려하면, 빠르게 이루어진 발전은 놀라운 일이 아닙니다.

또한, 개인 소유 디바이스에서 기업의 데이터를 완벽히 분리하고자 하는 업계의 명확한 추세를 지속적으로 확인하고 있습니다. 특히, 금융과 의료 분야의 기업 및 정부 부문은 이러한 분리 기술을 선호하는 것으로 나타났으며, 이들은 모바일 기능을 제한하고, 모바일 기능의 확장에 대한 MEAP의 역할을 평가하고 있습니다.

또한, 전 세계의 정부 중 다수로부터 입수한 모바일 보안 베스트 프랙티스 문서의 초기에 작성된 초안을 살펴봤습니다. 이 문서는 대부분은 적절한 보안 통제의 관점에서 기대할 수 있는 것에 대한 지시 사항을 정부 기관 내에 전달하는 데 초점을 두고 있지만, 포함된 내용은 산업 전반에 걸쳐 광범위하게 이용될 수 있는 모바일 관련 베스트 프랙티스에 영향을 미칠 것입니다. 문서는 주로 모바일 보안 분야에서 규정한 상식적인 접근법을 이용해 다른 플랫폼에 저장된 유사한 데이터의 보호를 위한 기존의 요구사항을 다루고 있습니다. 모바일 운영 체제가 다른 컴퓨터 운영 체제와 같이 사용되고, 제어되고, 지원되는 수준까지 계속해서 발전하기를 기대합니다.

메모

메모

메모

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

Produced in the United States of America
March 2013


Please Recycle

WGL03027-USEN-00