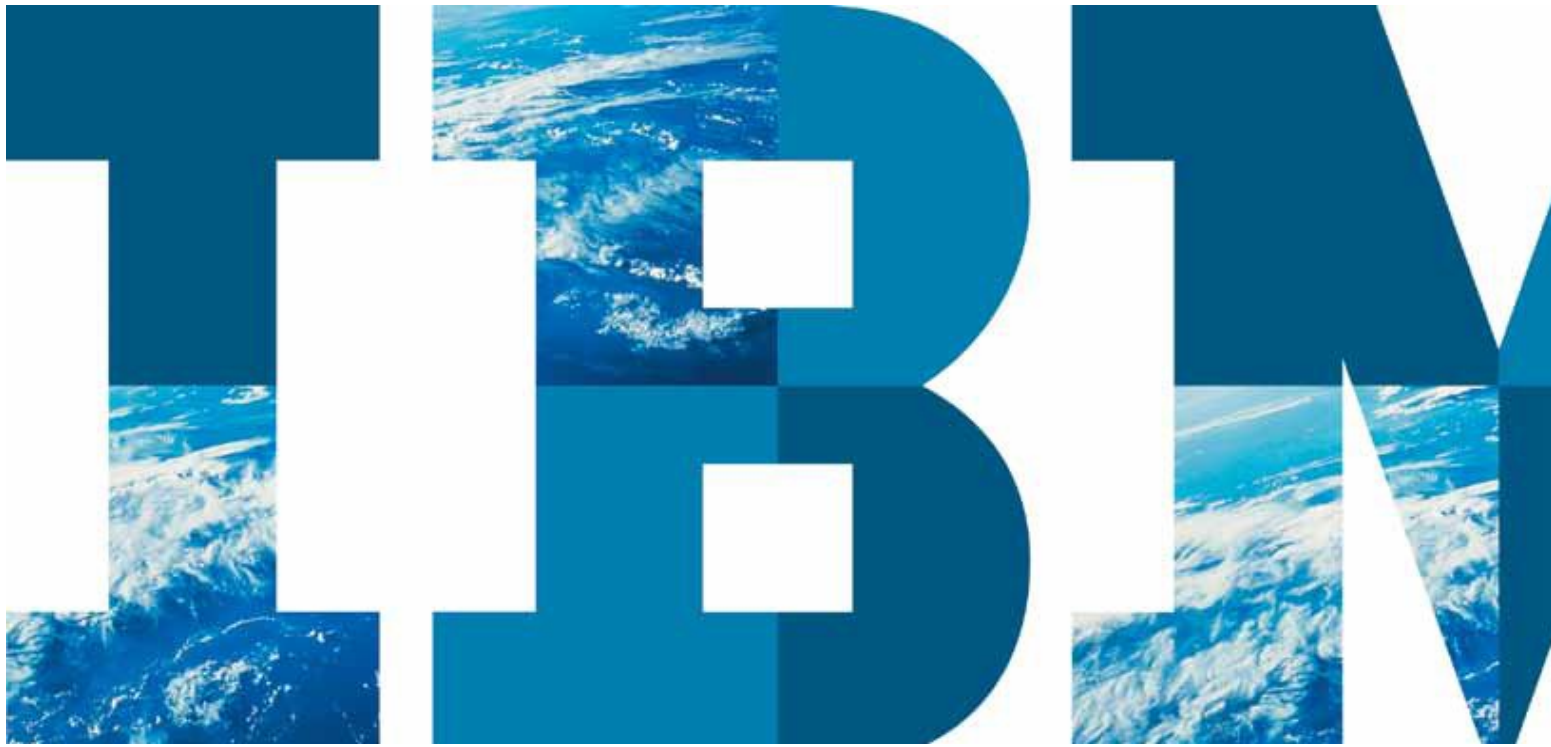
IBM X-Force 2012년
상반기 동향 및 위험 보고서

2012년 9월



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
Brian McGee	사용자 경험 그룹/사용성 – 시각 디자이너
Bryan Ivey	팀장, MSS 사이버 위협 및 정보 분석가
Carsten Hagemann	X-Force 소프트웨어 엔지니어, 컨텐츠 보안
Chadd Horanburg	사이버 위협 및 정보 분석가
Cynthia Schneider	IBM 보안 시스템, 기술 편집자
David Merrill	STSM, IBM 최고정보책임자, CISA
Jens Thamm 박사	데이터베이스 관리 컨텐츠 보안
Gina Stefanelli	X-Force 마케팅 관리자
Jason Kravitz	IBM 보안 시스템 Techline 전문가
Larry Oliver	선임 사이버 위협/보안 정보 분석가
Leslie Horacek	X-Force 위협 대응 관리자
Marc Noske	데이터베이스 관리, 컨텐츠 보안
Mark E. Wallis	IBM 보안 시스템, 선임 정보 개발자
Mark Yason	X-Force 선임 연구원
Michael Applebaum	Q1 Labs 제품 마케팅 책임자
Mike Warfield	X-Force 선임 명인
Nishad Herath	X-Force 선임 연구원
Paul M. Sabanal	X-Force 선임 연구원
Ralf Iffert	X-Force 컨텐츠 보안 관리자
Randy Stone	계약 리드, 비상 대응 서비스
Rob Hall	Sterling Connect:Enterprise, Sterling Secure Proxy 제품 관리자
Robert Freeman	X-Force 선임 연구 관리자
Rod Gifford	Sterling Connect:Enterprise, Sterling Secure Proxy 제품 마케팅 관리자
Scott Moore	X-Force 소프트웨어 개발자 겸 X-Force 데이터베이스 팀장
Thomas Millar	사고 대응 분석 선임 연구원

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 모니터링 합니다. X-Force는 고객과 일반 대중에게 새로운 주요 위협에 대해 경고하고 IBM 고객을 이러한 위협으로부터 보호하기 위해 보안 컨텐츠를 제공합니다.

헌정사

*IBM X-Force 2012년 상반기 동향 및 위험 보고서를 우리들의 벗이자 동료인 **Don Hall**을 애도하며 그에게 바칩니다. IBM 보안 시스템의 위협 플랫폼(Advanced Threat Platform) 담당 제품 개발 이사였던 Don은 이 보고서의 작성에 도움을 준 X-Force 보안 연구개발 팀을 포함한 전세계의 엔지니어 팀을 이끌었습니다.*
열정적인 팀의 챔피언이자 헌신적인 기술 리더였던 Don이 보안과 IBM에 기여한 공로는 영원히 기억될 것입니다.

IBM 보안 협업

IBM 보안은 광범위한 보안 역량을 제공하고 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 및 자체 조사, IBM MSS(Managed Security Service)가 제공하는 정보를 활용하여 인터넷을 독자적으로 조사하고 안전 수준을 분류합니다.
- IBM MSS(Managed Security Service)는 엔드포인트, 서버(웹 서버 포함), 일반 네트워크 인프라와 관련된 공격 행위를 감시하는 업무를 담당하고 있습니다. MSS는 웹뿐만 아니라 이메일 및 인스턴트 메시지 등의 분야에서 이뤄지는 공격 사례도 추적합니다.
- IBM PSS(Professional Security Service)는 효과적인 정보 보안 솔루션을 구축할 수 있도록 전사적인 보안 평가, 설계 및 설치 서비스를 제공합니다.
- IBM 계열사인 Q1 Labs가 개발한 QRadar Security Intelligence Platform은 SIEM, 로그 관리, 구성 관리, 이상 징후를 감지하는 통합 솔루션입니다. 이 솔루션은 사람, 데이터, 애플리케이션, 인프라와 관련된 보안 및 컴플라이언스 위험을 실시간으로 확인할 수 있는 통합 대시보드를 제공합니다.

- IBM Sterling **Secure** Proxy는 공공 인터넷에서의 파일 전송을 보호하는 DMZ(demilitarized zone) 기반 애플리케이션 프록시입니다.

IBM Sterling Connect:Direct®는 안전한 지점 간의 파일 전송을 위한 최고의 솔루션입니다. 이 솔루션은 기업 내부와 기업 간의 안전한 대용량 데이터 전송에 최적화되어 있으며, 연중 상시 무인 운영을 위한 스크립트 기반 자동화, 스케줄링, 경보 통지를 제공합니다.

목차

목차

단원 I—위협

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

개요

2011년 초, IBM X-Force는 2011년을 보안 침입의 해로 선언하였습니다. 대기업 및 중소기업이 모두 대상이었습니다. 2012년에 이러한 추세는 계속되었고 보안 침입에 관한 주제는 회사의 이사회에서 블로그 및 주요 언론 매체에 이르기까지 토론 목록의 최상위 항목으로 급부상하였습니다. 중요한 기업, 고객, 직원, 투자자/파트너의 데이터를 책임지는 임원들은 공격 활동이 발발하기 쉬운 환경에서 제대로 대처하는 방법을 파악하고자 했으며, 클라우드, 모바일, 아웃소싱 기술로 연결되어 있는 기업의 보안을 확보하는 방법을 끊임없이 연구하였습니다. 또한 조치 계획을 추진하는 단계를 논의하기 위해 기업 내의 보안 관리 담당자를 파악하였습니다.

보안 연구 조직인 IBM X-Force는 오래 전부터 기술에 초점을 두고 보안 침입을 검토해 왔습니다. 하지만, 시간이 지나면서 보다 광범위한 비즈니스 맥락을 수용하기 위해 공격과 침입의 관점을 달리해야 했습니다. 몇몇 유명 기업들이 비밀번호 및 기타 개인정보를 유출하면서 이에 따른 뒷수습을 해야 했으며, 이러한 침입 추세는 2012년에도 계속되고 있습니다. 특히 의료 산업은 상당한 타격을 입은 것으로 알려졌습니다.

보안 제품 및 기술이 이러한 침입 사건을 어느 정도 완화시킬 수 있었지만, 시스템 상호연결성, 부적절한 정책 시행, 인적 오류는 여전히 여느 단일 보안 취약점보다 심각한 영향을 미치고 있습니다.

악성코드, 키로거, 비밀번호 크래킹 또는 피해자의 컴퓨터나 디바이스의 액세스를 통하지 않고 디지털 신원이 심각하게 훼손된 사례가 몇 차례 대대적으로 보도되었습니다. 악의적 의도를 지닌 사람들은 개인정보를 위탁하는 기업 중 느슨한 정책을 찾아 교묘한 사회공학적 수법을 이용하여 개인정보를 수집합니다. 지금은 그 어느 때보다도 보안, 편의성과 개인정보 보호 간의 미묘한 균형이 관심의 대상이 되고 있습니다.

일례로, 공격자들은 모바일 전화 사업자들에게 사용자의 음성 메일을 이전하고 비밀번호를 재설정하는 데 필요한 데이터를 제공하여, 절대적으로 안전하다고 여겨지는 이중 요소(Two factor) 인증을 피하였습니다. 또 다른 예로는, 쉽게 볼 수 있는 신용카드 번호의 마지막 네 자리 숫자를 다른 서비스에서 계정의 재설정을 위한 주요 식별 데이터로 사용한 경우가 있습니다. 이러한 각 유형의 대규모 인시던트는 모두 레이더 망을 피해가는 유사한 모습을 보였습니다.

2012년의 침입 사례 공개에서 보듯이, SQL 인젝션 공격은 최상위 공격 수법의 자리를 계속 지킬 것으로 보입니다. 공격자들은 웹 애플리케이션의 XSS(cross-site scripting) 취약점을 노릴 것입니다. 2012년에 지금까지 보고된 전체 웹 애플리케이션 취약점의 51% 이상은 XSS로 분류됩니다.

이러한 끊임 없는 공격 속에서 긍정적인 면도 찾아볼 수 있었습니다. 2011년의 봇넷 근절 덕분에 스팸 및 피싱 수준이 낮은 수준을 유지하고 있으며, 가장 최근인 2012년 7월에는 Grum의 제거로 또 다른 봇넷이 근절되었습니다. 이러한 공격 활동의 감소 추세는 데이터에서 분명히 확인할 수 있습니다. IPv6 기술의 채택으로 긍정적인 웹 추세가 지속되고 있습니다. 공격자들이 언제 IPv6 기술을 채택할지는 알 수 없지만, 현재 IPv6를 활용하고 있는 기업과 정부에서는 악성 활동의 발생 빈도가 줄고 있습니다.

2012년의 중반 시점에서 볼 때, 전반적인 취약점이 증가 추세에 있으며 연말까지 사상 최고치를 기록할 가능성이 있습니다. 그렇다 할지라도, IBM X-Force 데이터는 일반에 공개된 전체 취약점 중에서 공격 대상이 된 경우는 단 9.7%에 머물렀으며, 실제 공격이 감소세임을 지속적으로 보여주고 있습니다. 특정 분야에 눈을 돌려보면, 지금이 변화의 교차로임을 알 수 있습니다. 소프트웨어 설계 및 기술의 향상이 개인용 모바일 디바이스 및 태블릿과 같은 신기술과 결합되어 기업에 융합되고 있습니다.

전체 IT 생태계에 대한 보다 전체론적인 접근방식이 필요한 때입니다. 사용자들은 자신의 개인정보가 온라인 상에서 쉽게 노출될 수 있다는 점을 인식해야 하며, 그 정보에 대한 액세스 권한을 누가 가지고 있는지 알아야 합니다. 또한, 이것이 자신에게 불리하게 사용될 수 있다는 점을 더욱 인식해야 합니다. 이는 자신의 소셜 네트워킹에 영향을 미칠 뿐만 아니라, 모바일 애플리케이션의 선택과 사용에도 영향을 미칩니다. 날로 증가 추세에 있는 모바일 애플리케이션은 상당한 권한을 요구하며, 사용자가 잠재적으로 악의적인 의도를 분간하기 어렵게 만듭니다. 더욱이 소비자와 기업들이 중요한 데이터를 클라우드로 이전하면서, 이 데이터의 액세스 방식에 대한 감사와 이해가 더욱 더 중요해지고 있습니다.

비즈니스는 이제 사무실을 벗어나 기업 네트워크로, 그리고 연결된 비즈니스로 확장되었으며, 디바이스와 서비스가 상호 연결된 세상이 도래했습니다. 시스템의 한 지점에서 발생한 정책이나 기술의 오류는 전반적인 시스템 기반을 뒤흔들 수 있습니다. IBM X-Force 동향 및 위험 보고서는 고객이 비즈니스에 올바른 의사결정을 내리는 데 필요한 인식을 제고할 것입니다.

이제, 2012년 상반기에 일어났던 몇 가지 주요 상황을 살펴보기로 하겠습니다.

2012년 하이라이트

위협

악성코드 및 악성 웹사이트

- 선거나 재해와 같은 큰 사건이 있을 때, 다수의 사람들로 인해 검색 엔진 최적화(SEO)가 이뤄집니다. 이러한 검색은 순수한 목적일수도, 악의적인 목적일 수도 있습니다. 최근의 뉴스 헤드라인은 스팸, SEO 공격 및 피싱, 또는 스피어 피싱 캠페인의 미끼를 제공하고 있습니다. Blackhole 등의 웹 브라우저 공격 키트를 가진 공격자들에게 이는 절호의 기회입니다. (11 페이지)
- 피해자의 컴퓨터를 완전히 무력화시키는 한 가지 방법은 신뢰할 수 있는 URL 또는 사이트에 XSS(cross-site scripting) 취약점을 이용하여 악성 페이로드를 탑재하는 것입니다. 견실하고 신뢰할 수 있는 기업이라 해도 웹사이트가 반영구적 XSS(cross-site scripting)에 취약한 경우가 허다합니다. (11 페이지)
- 이전에 IBM이 보고서를 발표한 이래, SQL 인젝션 공격이 꾸준히 증가하고 있습니다. 이와 함께, XSS와 HTTP "DotDot" 명령어와 같은 디렉토리 조회 명령어의 사용도 늘어나고 있습니다. 이 세 가지 공격 유형은 함께 사용할 경우 매우 강력해집니다. (11 페이지)
- 2011년 말에 IBM은 새로운 Mac용 악성코드 변종이 Windows 악성코드와 매우 유사해질 것이라고 예상한 바 있습니다. 2012년 상반기를 되돌아보면, 이 예상이 정확했던 것으로 보입니다. 지난 수 개월 동안 Flashback 출현과 APT(advanced persistent threat) Mac 악성코드의 발견을 포함한 Mac용 악성코드는 상당한 진전을 보였습니다. (29 페이지)
- 지난 IBM X-Force 동향 및 위험 보고서에서 IBM은 OS X 소프트웨어 공격의 기술적인 어려움이 대대적인 공격을 방지하는 주된 요인이라고 언급하였습니다. Flashback 감염은 Java 취약점을 이용한 다중 플랫폼 공격을 이용하여 OS 보안을 우회합니다. 즉, 공격 기술과 대부분의 관련 코드가 Windows나 Mac 모두에 대해 동일합니다. 일부 보안 솔루션 공급업체들은 싱크홀(sinkhole)을 구축하여 Flashback 감염 대수를 산정했으며, 600,000 대에 달하는 시스템이 감염된 것으로 추정되고 있습니다. (30 페이지)
- 올해 상반기 Mac용 악성코드의 또 다른 주요 양상은 특정 대상 악성코드(Mac APT)의 발견입니다. 일부 초기 변종은 Java 공격 CVE-2011-3544를 통해 확산되었습니다. 이는 Flashback이 사용하는 것과 동일한 Java Applet Rhino 스크립트 엔진 취약점을 공격합니다. 특정 대상을 목표로 하는 이 악성코드의 목적은 사용자의 데이터를 훔치는 것입니다. (30 페이지)

웹 컨텐츠 동향, 스팸 및 피싱

- IPv6 Day는 2012년 6월 6일로, 이 날 다수의 기업이 영구적인 IPv6 도입에 착수하였습니다. 완전히 채택된 경우는 많지 않으나, IBM X-Force 데이터는 웹 2.0 및 적법 사이트들이 현재 최신 IPv6에 대한 준비가 되어 있음을 보여주고 있습니다. 해킹 사이트, 불법 약물 거래 사이트, 익명 프록시, 음란물 및 도박 사이트와 같은 컨텐츠를 갖춘 웹사이트에서는 IPv6의 채택이 저조했습니다. 이는 IPv6에 대비하거나 최대한 많은 사용자들이 지속적으로 접속하게 하려면 별도의 기술적인 노력이 필요하기 때문입니다. (31-33 페이지)
- 전년에 비해 신규 등록된 익명 프록시 사이트의 수가 3배에 달하는 등, 익명 프록시의 등록은 2012년 상반기에 꾸준히 증가했습니다. 전체 익명 프록시의 2/3 이상이 .tk 도메인(뉴질랜드령인 토켈라우(Tokelau)의 최상위 도메인) 상에서 운영되었습니다. (35 페이지)
- 미국은 전체 악성 링크의 43% 이상을 호스팅하면서 악성 링크 최상위 호스트 국가의 자리를 계속 차지하고 있습니다. 독일이 9.2%를 호스팅하면서 2위를 차지하고 있습니다. 러시아는 처음으로 3위에 올랐으며, 중국은 최상위에서 4위로 하락하였습니다. 전체 악성 링크의 약 50%는 음란물 또는 도박 사이트가 차지하고 있습니다. (36 페이지)

- 2011년 말, 이미지 기반 스팸이 다시 등장하였습니다. 스패머들은 2012년 3월 말까지 이 유형의 스팸을 사용하였습니다. 한 때, 전체 스팸의 8% 이상에 이미지 첨부 파일이 들어 있었습니다. (39 페이지)
- 스팸의 크기에도 또 다른 추세가 나타났습니다. 전통적으로 스팸 메시지는 주어진 대역폭에서 최대한 많이 발송할 수 있도록 의도적으로 작은 크기를 유지해 왔습니다. 지금은 적절하지 않은 캐스캐이딩 스타일 시트(CSS)에서 비롯된 대용량의 메시지를 볼 수 있습니다. 최근의 이론에 따르면, 메시지 데이터나 포맷팅에 영향을 미치지 않는 것처럼 속여 탐지를 피하는 수단으로 데이터가 추가로 사용하고 있습니다. (41 페이지)
- 인도는 현재까지 보고된 전체 스팸의 약 16%라는 사상 최고 수치를 기록하면서 여전히 스팸 발송 국가 중에서 1위를 차지하고 있습니다. 2011년 봄 3% 미만으로 하락했던 미국은 2012년 봄에 증가하면서, 현재 8% 이상으로 베트남에 이어 3위를 차지하고 있습니다. 호주와 한국이 5위 내에 있으며, 브라질이 2012년 상반기에 발송된 전체 스팸의 6%를 차지하면서 6위에 올랐습니다. (44 페이지)
- 2012년 7월 18일, Grum 봇넷이 상당히 줄었습니다. Grum은 미국, 베트남, 호주, 독일, 브라질의 고객들을 주 대상으로 삼았으며, 근절 전에는 전세계 스팸의 29.9%가 이들 국가에서 발송되었지만 그 후에는 22.5%에 머물렀습니다. (47 페이지)
- 2011년 말, 피싱과 유사한 이메일이 등장하기 시작했습니다. 여기서 연결되는 웹사이트는 피싱 공격을 수행하지 않는 경우도 있었습니다. 2012년에도 이 활동은 지속되어, 사용자를 속이기 위해 이러한 택배 서비스를 사용하는 경우가 전체 사기 및 피싱의 27% 이상에 도달하였습니다. 피싱 공격자들은 비영리 기관에도 눈을 돌렸으며, 한 때 66%를 차지하기도 했던 이 유형의 공격은 2012년 상반기에는 7%로 하락하였습니다. (49 페이지)

보안 인프라 운영

취약점 및 공격

- 2012년 상반기에 새로 보고된 보안 취약점은 4,400 건을 약간 상회합니다. 이 추세가 올해 그대로 지속된다면, 전체 예상 취약점은 2010년도 기록을 다소 상회하는 9,000 건에 달할 것으로 보입니다. (58 페이지)
- 보고된 SQL 인젝션 취약점의 감소 추세는 2012년에도 이어졌지만 XSS(cross-site scripting) 취약점은 사상 최고 수준까지 다시 증가하였습니다. XSS는 공격자가 클라이언트 측의 스크립트를 다른 사용자가 열람한 웹 페이지에 주입할 수 있는 웹 애플리케이션 취약점을 설명할 때 쓰이는 용어입니다. 2012년에 지금까지 보고된 전체 웹 애플리케이션 취약점의 51% 이상이 현재 XSS로 분류되어 있습니다. (59 페이지)
- 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. 실제 공격의 감소 추세는 2012년에도 지속되고 있으며, 최초 6개월간의 데이터에 의거해볼 때, 대중에 공개된 전체 취약점의 9.7%만이 공격에 포함될 것으로 예상됩니다. (62 페이지)
- Office 및 PDF(Portable Document Format)의 취약점은 급격히 감소된 것으로 나타났습니다. PDF 취약점 노출의 감소와 Adobe Acrobat Reader X 샌드박스 간에는 상당한 연관성이 확인되었습니다. (67 페이지)

- 상위 10대 솔루션 공급업체의 패치를 통한 취약점 보완은 지속적으로 발전해 왔으며, 이는 안전한 개발 관행 및 PSIRT(Product Security Incident Response Team) 프로그램의 지속적인 시행과 개선 덕택이라고 볼 수 있습니다. 상위 10대 솔루션 공급업체들은 공개된 전체 취약점의 94%를 약간 상회하는 인상적인 패치 치료율을 보이고 있습니다. (67 페이지)
- 2012년 상반기의 패치를 통해 차단되지 않은 취약점(상위 10대 솔루션 공급업체 제외)의 비율은 2008년 이래 최고치를 기록했습니다. 올해 공개된 전체 취약점의 47%가 치료되지 않은 상태이지만, 이는 주로 비기업용 소프트웨어 때문입니다. (68 페이지)

소프트웨어 개발 환경 보안 환경 현황

이메일 비밀번호 보안

- 웹사이트, 클라우드 기반 서비스, 웹메일 간의 연결은 디바이스에서 디바이스로 진정한 사용자 경험(seamless experience)을 제공하지만, 사용자들은 이 계정들이 연결되어 있는 방식, 비밀번호의 보안과 비밀번호 복구 및 계정 재설정에 어떤 개인정보를 제공했는지에 유의해야 합니다. (87 페이지)
- 비밀번호 복구 도구의 신속성을 감안할 때, 취약한 비밀번호는 유출된 데이터베이스 해쉬에서 수 초 안에 드러날 수 있습니다. 웹 개발자에게 최상의 솔루션은 안전한 비밀번호 보관을 위해 설계된 해싱 기능을 사용하는 것입니다. 즉, 솔팅(Salting)을 사용해야 하며 해쉬 변환 자체에 긴 시간이 소요되게 하여 평문 비밀번호 복구를 훨씬 더 어렵게 만들어야 합니다. 솔팅은 해싱 기능으로 전송되기 전에 비밀번호와 결합되는 임의 문자열과 같은 일종의 추가 요소입니다. (91 페이지)

새로운 보안 추세

모바일 악성코드

- 2012년 상반기에 보고된 모바일 취약점 및 공격은 2008년 이래 최저 수준으로 하락하였습니다. IBM X-Force는 그 이유를 여러 가지로 보고 있습니다. 첫째, 모바일 운영 체제 개발자들이 사내 취약점 발견과 공격으로부터 취약점을 보호하기 위한 보안 모델을 개선하기 위해 지속적으로 투자하고 있습니다. 모바일과 같이 비교적 새로운 분야에는 일종의 패턴이 있습니다. 간단한 버그는 즉시 발견 가능하여 발견율이 급증하고 있으며, 공격이 어려운 취약점만이 남아 있습니다. 이전의 한계를 극복할 수 있는 기술을 발견하는 시점은 연구자들과 공격자들 간에 차이가 있습니다. (64 페이지)
- 모바일 디바이스의 보안 상태는 항상 유동적입니다. 안드로이드 상의 TigerBot/Android.Bmaster 및 여러 모바일 플랫폼 상의 Zeus/ZITMO와 같은 특이한 모바일 악성코드가 보고되고 있지만, 대다수 스마트폰 사용자들에게는 프리미엄 SMS 사기 및 유사한 종류의 형태가 여전히 가장 위험합니다. 이러한 사기는 설치된 애플리케이션에서 여러 국가의 프리미엄 전화 번호로 SMS 메시지를 발송하는 방식입니다. (98 페이지)

모바일—BYOD(bring your own device)

- 사내에서 BYOD를 제대로 활용하려면, 먼저 직원 소유 디바이스를 회사의 인프라에 추가하기 전에 면밀하고 명확한 정책을 수립해야 합니다. 이 정책은 회사와 직원의 디바이스 간의 관계에 대한 모든 측면을 다루어야 하며, 모든 당사자로부터 동의를 얻어야 합니다. (99 페이지)
- 모바일 디바이스가 기업뿐만이 아니라 전반적인 인터넷 상에서 주요 컴퓨팅 디바이스로 자리잡았지만, 취약한 디바이스를 위한 패칭은 지난 몇 년 간 거의 진전이 없었습니다. 이는 주된 보안 문제로 대두되고 있습니다. (105 페이지)

IBM MSS(Managed Security Service)—전세계 위협 현황

IBM MSS(Managed Security Service)는 1년 365일 하루 24 시간, 130여 국가에서 수백 억 건의 이벤트를 모니터링하고 있습니다. IBM MSS는 국제적인 입지를 바탕으로 최신 위협에 대한 직접적인 견해를 제공하며 IBM 분석가들은 이 풍부한 데이터를 사용하여 사이버 위협 현황에 대한 이해를 제고합니다. 이 단원에서는 이 보고서 전반에 설명되어 있는 최상위 위협의 견해에 관한 최신 정보가 제공되어 있습니다. 위협 동향 파악은 향후 보안 전략을 수립하고 컴퓨팅 환경에 대한 위협의 중대성을 이해하는 데 대단히 유용합니다.

XSS(Cross-site scripting)와 SQL 인젝션 공격의 동시 증가

선거나 재해와 같은 큰 사건이 있을 때, 다수의 사람들로 인해 검색 엔진 최적화(SEO)가 이뤄집니다. 이러한 검색은 순수한 목적일수도, 악의적인 목적일 수도 있습니다. 재난 또는 유명인사와 관련된 사건이나 정치 스캔들은 소셜 미디어 사이트에 영향을 미쳐 왔습니다. 2102년 선거, 런던 올림픽 경기, 자주 인용된 마야 예언을 포함하여, 올해에는 이러한 종류의 사건이 많았습니다. 이 모두는 스팸, SEO 공격, 피싱 또는 스피어 피싱 캠페인에 쓰이는 미끼를 제공하였습니다. 이는 블랙홀과 같은 웹 브라우저 공격 키트를 갖춘 공격자들에게 절호의 기회입니다.

피해자의 컴퓨터를 완전히 무력화시키는 한 가지 방법은 취약한 웹사이트로 유도하는 URL을 사용자에게 보내는 것입니다. 실제로, 조작된 URL을 내재하고 있는 신뢰할 수 있는 유수 기업의 웹사이트는 대부분이 여전히 non-persistent XSS(cross-site scripting)에 취약합니다. HTML5의 사용이 늘어남에 따라 HTML5가 실질적인 웹 액세스 방법이 되었으며, 이제는 클라이언트 측의 SQL 인젝션 공격이 가능해졌습니다. 따라서 공격자들이 HTML5 thick 기능을 이용하여 로컬 스토리지에 액세스할 수 있으며, 로드된 SQL 데이터베이스의 로컬 버전이 있는 경우 SQL 인젝션 공격이 피해자의 컴퓨터를 감염시키는 또 다른 유효한 방법이 될 수 있습니다.

최근 IBM X-Force 동향 및 위험 보고서가 발표된 이래, XSS 및 HTTP "DotDot" 명령어와 같은 디렉토리 조회 명령어와 더불어 SQL 인젝션 공격이 꾸준히 증가하고 있습니다. 이 세 가지 공격 유형을 함께 사용할 경우 그 효과는 매우 강력해집니다. 이 세 가지 수법을 조합할 수 있는 방법이 매우 다양하기 때문에, 현재 통용되고 있는 방법을 일일이 열거하는 것은 불가능합니다.

하지만 단언할 수 있는 점은 SQL 인젝션 공격과 XSS(cross-site scripting)가 선호되는 공격 방법으로 떠오르고 있다는 점이며, 이는 우리의 동향 정보와 일치합니다. IBM은 이 새로운 접근방식을 도입하고 보고서 개선을 위해 이 세 가지 이벤트를 계속 예의 주시할 것입니다.

난독화

사이버 위협의 세계에서, 난독화(obfuscation)는 보안 관련 이벤트의 소스 및 방법을 숨기거나 감추는 수법입니다. 난독화는 침입 방지 시스템(IPS)과 안티바이러스 소프트웨어를 피하기 위한 목적으로 끊임없이 발전하고 있습니다. IBM 보안 네트워크 IPS는 전세계의 이러한 수법을 모니터링 하는 데 유용한 특수 감지 알고리즘을 갖추고 있습니다. 처리하기 까다로운 유형의 난독화는 암호화에 기반을 두고 있으며, 이는 전송되는 정보에 관한 판단을 제한할 수 있습니다. 반면에, 예기치 않은 곳에서 나타나는 암호화된 정보는 추가 조사를 요구하는 의심스런 소스와 목적지를 식별하기 때문에 그 자체로 "구별"을 할 수 있습니다.

XSS 이벤트와 SQL 인젝션 이벤트 간의 일치하는 추세
2011년 7월 ~ 2012년 6월

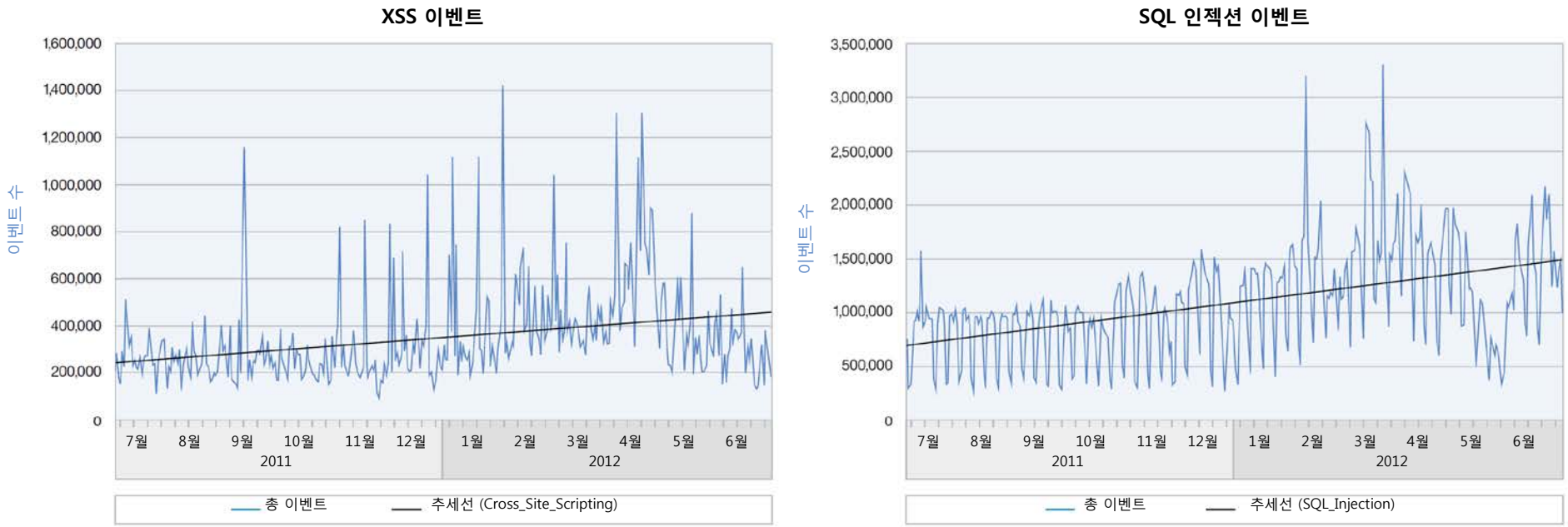


그림 1: XSS 이벤트와 SQL 인젝션 이벤트 간의 일치하는 추세 – 2011년 7월 ~ 2012년 6월

자신의 공격을 숨기고 네트워크 보안 시스템이 자신을 탐지하는 것을 더욱 어렵게 만들기 위해 컴퓨터 범죄자들이 암호화를 사용하는 경향이 증가하고 있습니다. 여기에는 HTTPS 외에도 다양한 문서 양식의 기본적인 암호화 기능과 스크립팅 언어를 사용하는 난독화가 포함됩니다. 차트에 명백하게 나와있듯이, 잠재적으로 난독화된 트래픽의 존재와 양은 극히 가변적이고 지속적입니다. 이 그림은 약 30 가지의 개별 난독화 휴리스틱스의 합성을 보여줍니다. 공격, 악성코드, 데이터 유출을 식별하는 기술이 향상되면서, 난독화 수법의 사용은 앞으로도 지속될 것으로 보입니다. 아울러, 새로운 애플리케이션이 배치되고 새로운 기술(클라우드 서비스, 모바일 애플리케이션 등)이 나타나 인터넷을 이용한 의사소통 방식에 영향을 미침에 따라, 잠재적 공격을 감출 이유가 늘어나고 투자가 증가하게 될 것입니다.

IBM은 난독화 수법의 증가에 대비한 기술을 지속적으로 개발하여 적용하고 있으며, 이러한 추세에 관한 최신 정보를 고객들에게 지속적으로 제공할 것입니다.

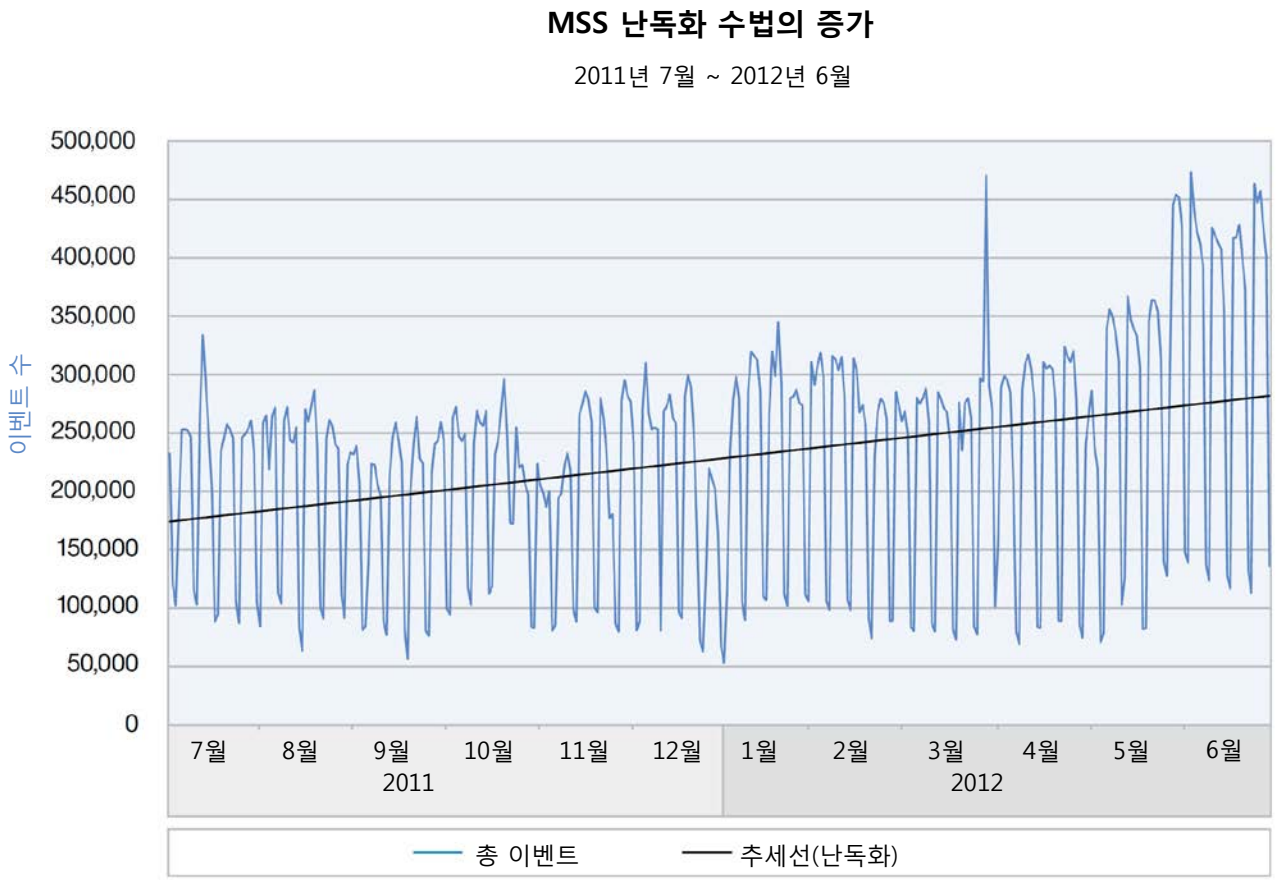


그림 2: MSS 난독화 수법의 증가 – 2011년 7월 ~ 2012년 6월

MSS—2012년에 대량 발생한 상위 시그니처

표 1: 상위 MSS 대량 발생 시그니처 표는 2011년 말 및 2010년 말 대비 2012년도의 상위 10개 MSS(Managed Security Service) 시그니처의 상대적 순위와 그 추세 방향을 보여주고 있습니다. 2011년 말의 상위 10개 시그니처 중의 7개가 2012년 상반기 순위에도 자리를 차지하고 있습니다. 먼저 일부 중대한 변화를 살펴 보기로 하겠습니다.

SQL_Injection 시그니처의 하향 곡선이 2011년에 역전되어 지속적으로 증가하고 있으며, 최대 발생 시그니처의 자리를 차지하고 있습니다.

SQL 슬래머웜 시그니처인 SQL_SSRP_ Slammer_ Worm은 일년 내내 하향세였으며 본 보고서의 다음 호에서는 상위 10대 순위에서 빠질 수도 있습니다. 이 급격하고 지속적인 감소의 정확한 원인은 아직 파악되지 않고 있습니다.

동시에, PsExec_Service_Accessed 시그니처는 대량 발생 시그니처의 목록에 다시 올랐습니다. 이 대중적인 시스템 관리 도구는 1년간 순위에서 빠진 후 다시 3위를 차지하고 있습니다.

몇몇 다른 시그니처와 마찬가지로, HTTP_Get_DotDot_ Data 시그니처의 양도 지속적인 상승 추세에 있으며, 5위에서 지금까지 가장 높은 4위로 올랐습니다.

이벤트 명칭	2012년 순위	추세	2011년 순위	추세	2010년 순위	추세
SQL_Injection	1	상승	1	상승	2	하락
SQL_SSRP_Slammer_Worm	2	소폭 하락	3	소폭 하락	1	하락
PsExec_Service_Accessed	3	소폭 상승			3	소폭 상승
HTTP_GET_DotDot_Data	4	상승	5	상승		
Cross_Site_Scripting	5	소폭 상승	6	소폭 상승		
SNMP_Crack	6	하락	4	하락		
SSH_Brute_Force	7	소폭 상승	7	소폭 상승	4	소폭 상승
HTTP_Unix_Passwords	8	상승	8	상승	6	소폭 상승
Shell_Command_Injection	9	소폭 상승	9	상승		
JavaScript_Shellcode_Detected	10	상승				

표 1: 상위 MSS 대량 발생 시그니처 및 추세선 – 2012년 상반기

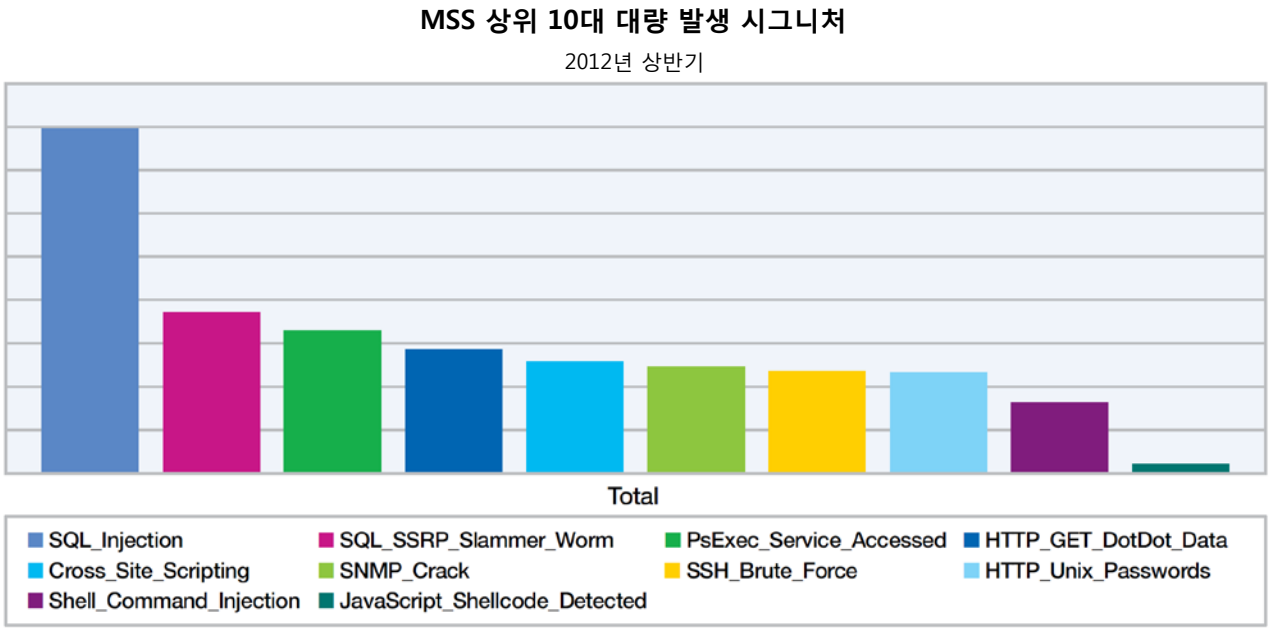


그림 3: MSS 상위 10대 대량 발생 시그니처 – 2012년 상반기

SQL 인젝션 공격

2010년 가장 높은 2위를 차지했던 SQL_Injection 시그니처는 지속적인 상승 추세를 보이면서 2011년에 1위에 올랐습니다. 2011년은 SQL 취약점 공격이 가장 활발한 한 해였습니다. 연말에 핵티비스트 활동이 잠잠해지기 시작하면서, SQL 인젝션 활동의 추세선이 꺾이기 시작했습니다. 11월과 12월의 연휴 기간을 중심으로 어느 정도의 급등이 있었지만 추세는 주춤해졌습니다.

핵티비스트 단체인 Anonymous와 Lulzsec이 2011년 초기의 대다수 SQL 인젝션 공격을 주동했으며 새로운 인젝션 공격 수법으로 공격 기술을 한층 정교화시켰습니다. 하지만, 그 활동 수준은 눈에 띌 정도의 소강 상태에 일시적으로 접어 들었습니다.

공격자 단체는 LizaMoon과 같은 도구를 이용하여 잠재적으로 취약한 시스템을 자동으로 찾는 등 2011년에 큰 발전을 이루었으며 공격 방법을 지속적으로 개발하였습니다. 2012년에는 SQL 인젝션 공격의 수준이 한층 더 높아지고 있으며, 이 유형의 공격은 2011년 말에 비해 더 높은 증가율을 보이고 있습니다.

이 모든 활동의 결과로 SQL 인젝션 공격이 2012년 상반기 1위를 차지했습니다.

IBM X-Force 2011년 동향 및 위험 보고서의 "여전히 활개를 치고 있는 SQL 인젝션 공격"이라는 단원에서는 SQL 인젝션 공격에 대한 추가 통찰력을 제공하고 있으며 공격으로부터 보호하기 위해 취할 수 있는 조치를 논하고 있습니다. 이 단원은 이러한 공격과 그와 관련된 공격 메커니즘에 익숙하지 않은 모든 사람이 숙지할 필요가 있습니다.

본 보고서의 앞에서 설명했듯이, 공격자들은 끊임없이 여러 기술을 결합하고 있으며, 성공할 가능성이 더 높으며 방어하기 어려운 계층적 공격을 개발하고 있습니다. SQL 인젝션 공격은 특히 쉘 명령어 인젝션 또는 XSS와 같은 기타 평범한 공격과 결합되며, 이러한 툴킷에서 가장 흔히 발견되는 공격 형태의 하나입니다.

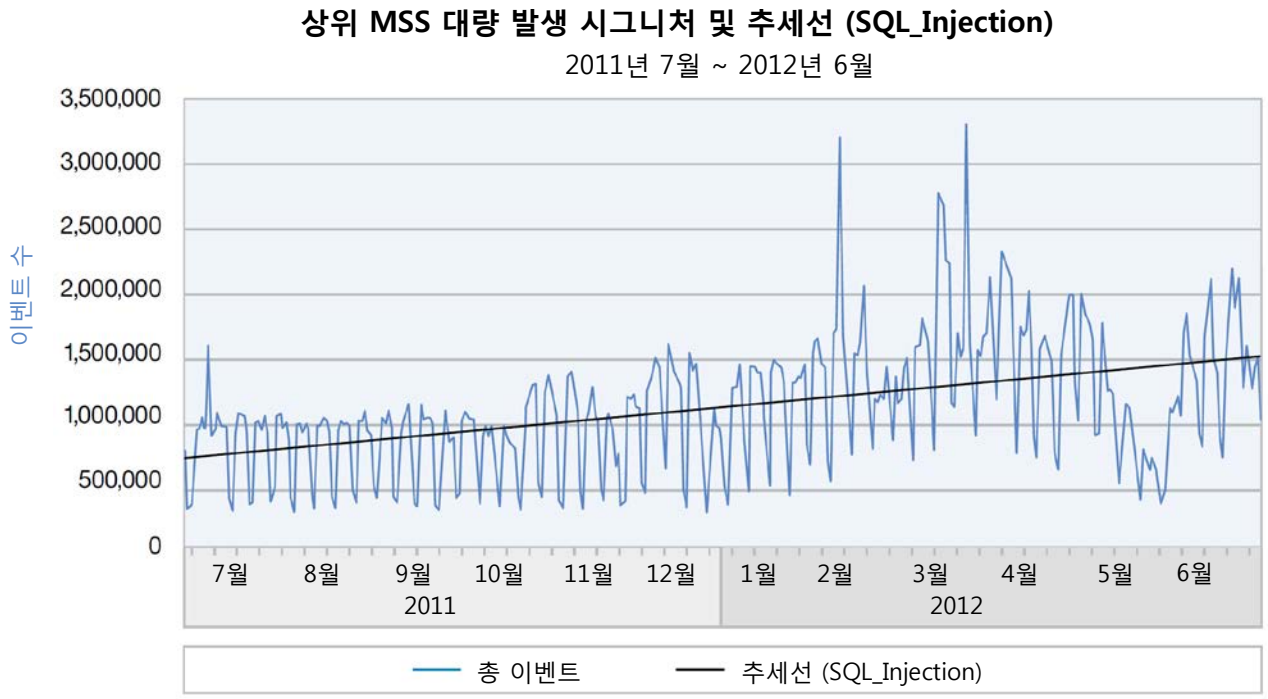


그림 4: 상위 MSS 대량 발생 시그니처 및 추세선 (SQL_ Injection) - 2011년 7월 ~ 2012년 6월

SQL 슬래머 웜

두 번째로 가장 보편적인 시그니처는 SQL 슬래머 웜과 관련이 있습니다. SQL 슬래머 웜은 인터넷 악성 코드 중에서 가장 지속적인 사례로 알려져 있습니다. 2012년 1월말은 슬래머 웜이 배포된 지 9년째 되는 해였습니다. 그러나 슬래머 웜은 사라지지 않을 것으로 보입니다. IBM X-Force 2011 상반기 동향 및 위험 보고서의 기사 "SQL 슬래머가 사라진 날"에서 설명했듯이, SQL 슬래머 활동은 2011년 3월에 급감했습니다. 그 후 슬래머는 거의 완전히 사라졌습니다. 비록 슬래머가 2012년 상반기 보고서에서 현재 3위를 차지하고 있지만, 다음 보고서가 발표될 쯤에는 완전히 사라질 것입니다. IBM의 예측과 같이 하락세가 지속되고 있으며, 다음 보고서에서는 상위 대량 발생 시그니처에서 빠질 가능성이 높습니다.

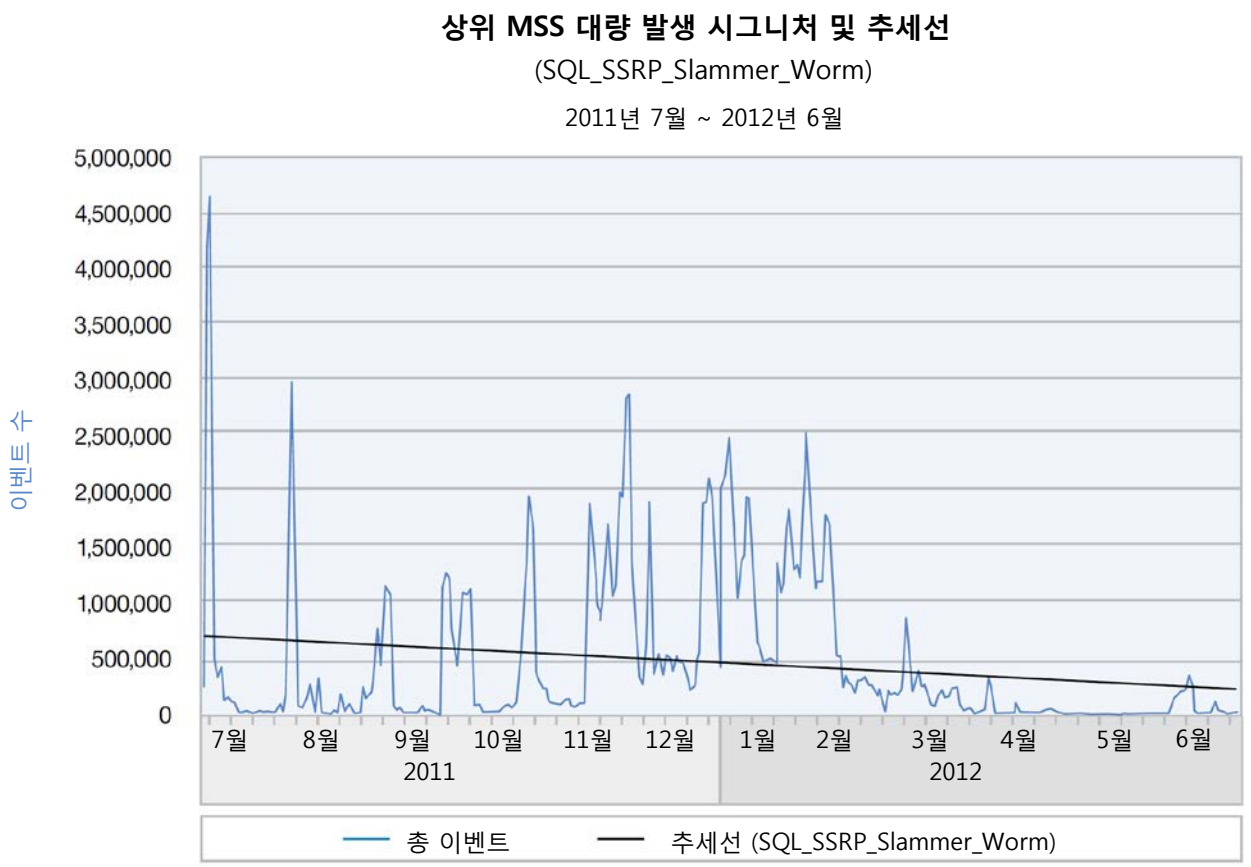


그림 5: 상위 MSS 대량 발생 시그니처 및 추세선 (SQL_SSRP_Slammer_ Worm) - 2011년 7월 ~ 2012년 6월

PsExec_Service_Accessed

3위를 차지한 PsExec_Service_ Accessed 시그니처는 2010년 말, 대량 발생 시그니처 순위 3위를 차지한 바 있습니다. 일종의 "화려한 복귀"인 셈입니다.

PsExec 소프트웨어는 Windows Sysinternals의 일부로 지원되는 Microsoft 소유의 합법적인 애플리케이션 패키지입니다. 이는 명령어 기반 원격 관리 도구로서, 텔넷의 경량화 버전과 매우 유사하며 대상 시스템에 코드를 설치하지 않아도 의도한 기능을 발휘합니다. PsExec은 모든 것을 처리할 수 있습니다.

그러나, 웜과 지능적인 공격은 때로 PsExec을 활용합니다. 일례로 "Here you have" 웜에는 네트워크를 통해 다른 컴퓨터에 스스로 복사할 수 있는 PsExec 도구가 포함되어 있습니다. Sysinternals 소프트웨어 제품군을 조직에서 사용한다면, 모범 보안 사례를 반드시 채택해야 할 것입니다.

IBM의 휴리스틱 시그니처는 PsExec 서버 핸들러의 호출을 감지하여 도구를 사용하려는 시도를 보고합니다. 이는 반드시 공격이나 악성코드가 검출되었음을 의미하진 않으나, 이 시그니처가 나타나는 경우 사용의 적정성을 확인하는 것이 바람직합니다.

상위 MSS 대량 발생 시그니처 및 추세선
(PsExec_Service_Accessed)
2011년 7월 ~ 2012년 6월

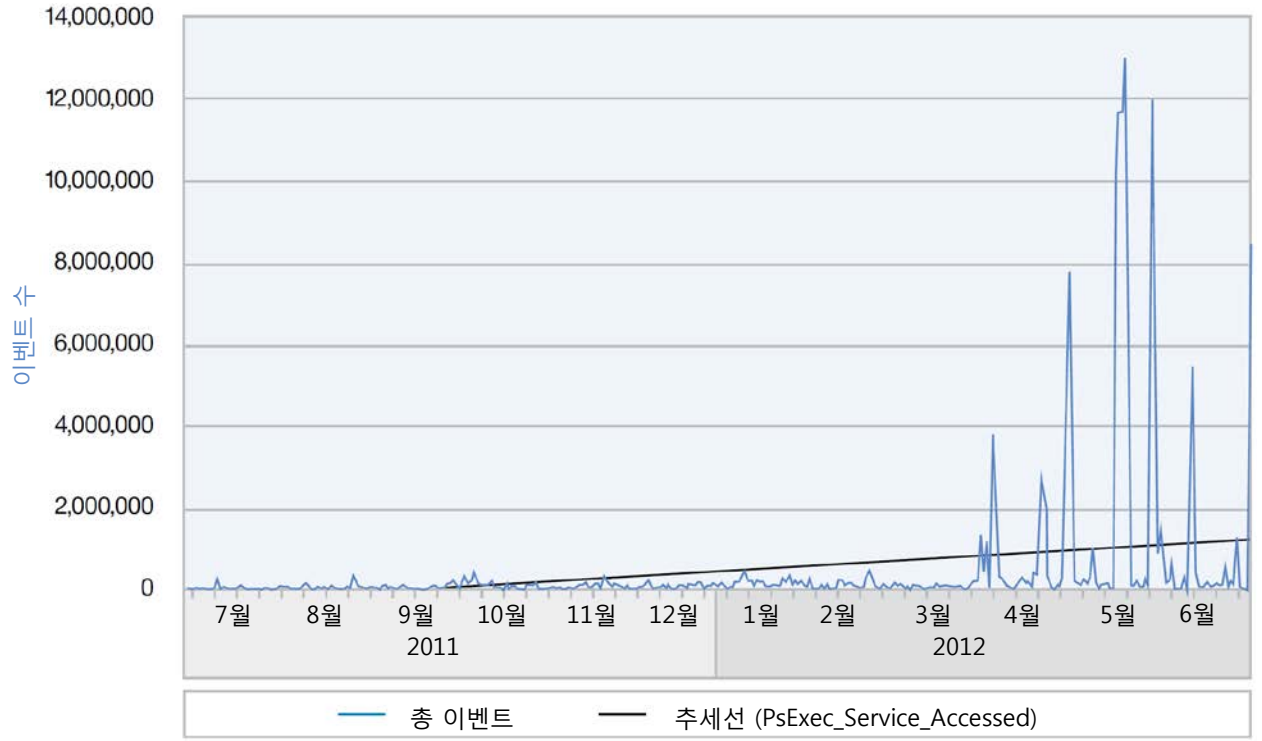


그림 6: 상위 MSS 대량 발생 시그니처 및 추세선 (PsExec_Service_ Accessed) - 2011년 7월 ~ 2012년 6월

디렉토리 조회

네 번째로 가장 보편적인 시그니처는 HTTP_GET_DotDot_Data와 디렉토리 조회 공격 방법과의 그 연관성입니다. 이는 실로 오래된 공격 방법이지만, 대다수 운영 체제 쉘의 지속적인 기능에 기반을 두고 있기 때문에 여전히 효과를 발휘하고 있습니다.

공격자는 이 방법을 이용하여 취약한 웹 서버의 디렉토리를 조회할 수 있습니다. 디렉토리 간에 이동이 가능하므로, 공격자는 서버 상 프로그램의 위치에 관한 정보를 충분히 입수할 수 있습니다.

이 수법에 대한 확실한 방어책은 유입되는 사용자 입력을 필터링하고, 원하지 않는 기능을 식별하여 억제하고, 웹 서빙 프로세스의 특권 수준에 대한 액세스를 제한하는 것이 유일한 방법입니다.

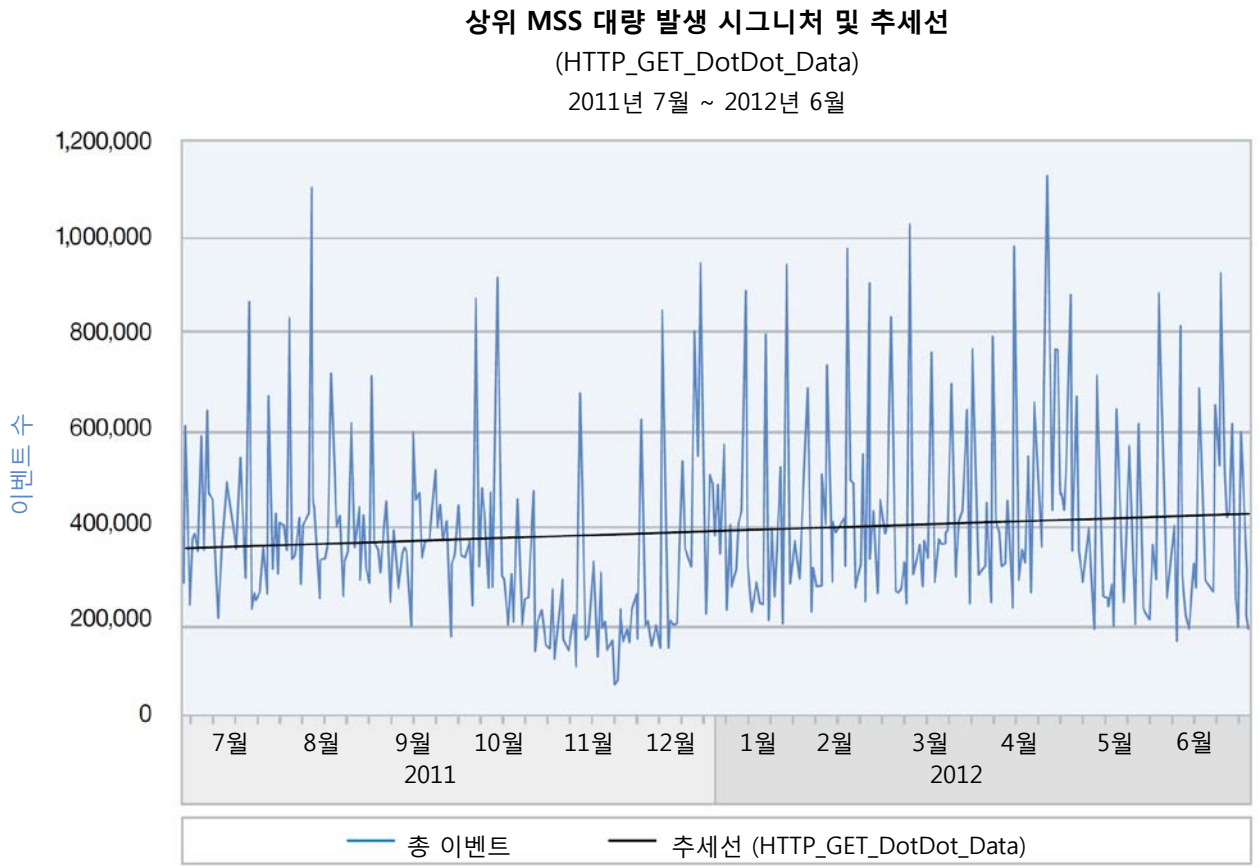


그림 7: 상위 MSS 대량 발생 시그니처 및 추세선 (HTTP_GET_ DotDot_ Data) - 2011년 7월 ~ 2012년 6월

XSS(Cross-site scripting)

XSS는 인터넷 역사상 가장 지속적인 공격 형태의 하나였습니다. XSS 공격은 웹 페이지에 클라이언트 측 스크립트를 주입하여, 잠재적으로 클라이언트 컴퓨터를 파괴할 수 있습니다. 이 공격은 모바일 디바이스를 포함한 모든 웹 브라우징 기술에 적용됩니다. 이 공격은 널리 알려져 있으며, 중대한 보안 위험을 야기할 수 있습니다.

1999년에 처음으로 기록된 XSS는 원래 Unix 환경에 국한된 문제였습니다. 그 해가 지나기 전에, 공격의 2차 변종이 나타났습니다. 현재는 이 취약점의 변종이 6,000여 가지에 달하며, 브라우저 세션의 하이재킹에서 전체 시스템 웹 서버 기반에 이르기까지 다양한 양상을 보이고 있습니다.

XSS 시그니처는 규모 면에서 상위 10대 시그니처 리스트의 5위를 차지하고 있습니다. 이 위험에 대한 노출을 줄이려면 서버 측 코드의 세밀한 검증이 필요합니다. 새로운 브라우저 기술들은 이 취약점의 실효성을 줄일 수 있다는 가능성을 보여주고 있으며, 여기에서 클라이언트 측의 사용자 교육이 매우 중요합니다.

상위 MSS 대량 발생 시그니처 및 추세선
(Cross_Site_Scripting)
2011년 7월 ~ 2012년 6월

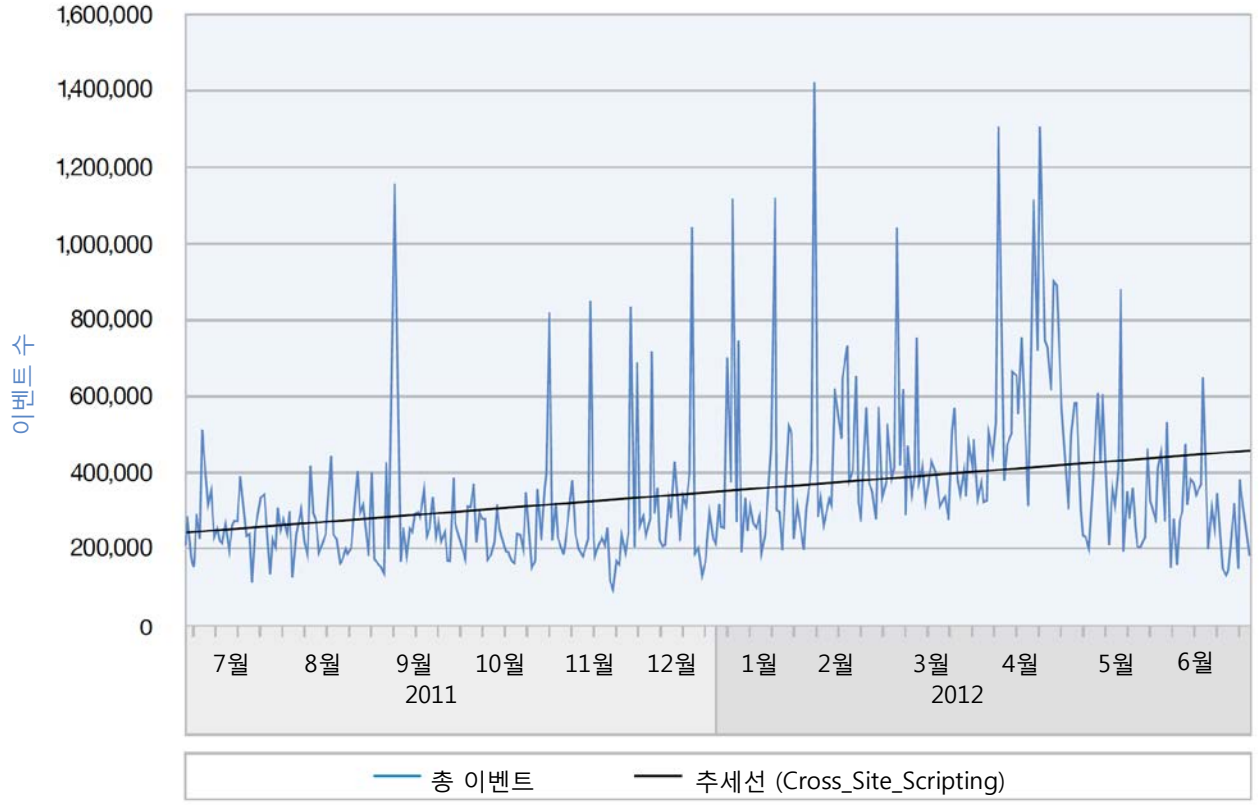


그림 8: 상위 MSS 대량 발생 시그니처 및 추세선 (Cross_Site_Scripting) - 2011년 7월 ~ 2012년 6월

SNMP Crack

SNMP_Crack 시그니처는 취약한 보안에 대한 무차별(Brute-force) 시도를 탐지하기 위한 여러 시그니처 중의 하나입니다. SNMP(Simple Network Management Protocol)는 신뢰할 수 있는 환경에서 사용하기 위해 개발되었으며 커뮤니티 문자열은 공개 네트워크에 대한 인증을 제공하기 위한 것이 아니라 세목을 분류하기 위한 것이었습니다. 네트워크 관리자에게 도움을 주기 위한 SNMP는 인터넷 프로토콜 환경의 운영 체제, 허브, 스위치, 라우터 등에서 볼 수 있습니다.

SNMP_Crack 시그니처는 서로 다른 커뮤니티 문자열을 가진 다수의 SNMP 메시지가 단기간에 검출될 때 발생됩니다. 이는 무차별 커뮤니티 문자열 추측 공격을 나타낼 수 있으므로 의심을 해 보아야 합니다. 하나의 모범 사례로서, 방화벽에서 SNMP를 막음으로써 보호된 네트워크에서 외부 개체가 SNMP를 사용하여 탐색 스캔을 수행하는 것을 방지할 수 있습니다.

SNMP 서비스는 디폴트 커뮤니티 문자열로 구성되기 때문에, 잠재적 공격자는 커뮤니티 문자열을 먼저 검색할 수 있습니다. 공격자가 디폴트 문자열을 이용하여 정보를 입수하는 데 실패하는 경우, 유효 커뮤니티 문자열에 대한 무차별 검색을 시도할 수 있습니다. 절대적으로 요구되지 않는 한, 외부에서 SNMP를 차단하는 것이 바람직합니다. 또한 SNMP의 필요성을 전체적으로 평가하고, 필요하지 않은 프로토콜을 비활성화시키는 것이 바람직합니다. 실질적으로 필요할 경우에는, SNMPv3로 마이그레이션하여 인증을 한층 강화하는 방안을 고려해야 합니다.

상위 MSS 대량 발생 시그니처 및 추세선 (SNMP_Crack)
2011년 7월 ~ 2012년 6월

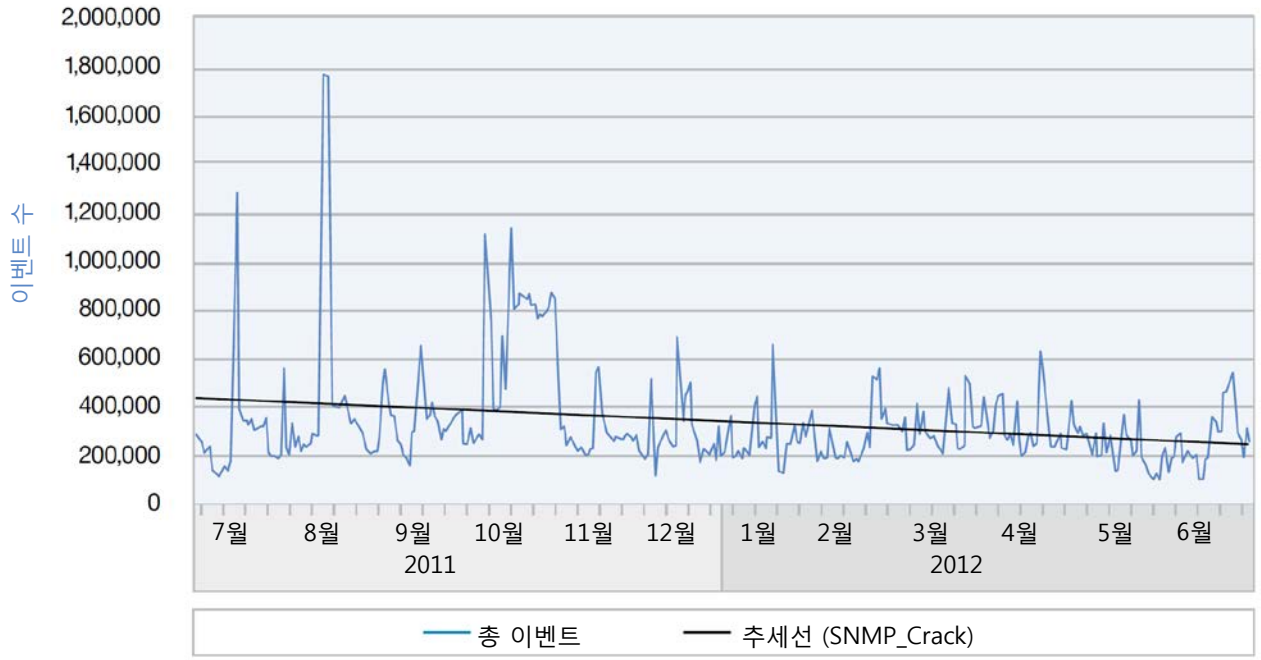


그림 9: 상위 MSS 대량 발생 시그니처 및 추세선 (SNMP_Crack) - 2011년 7월 ~ 2012년 6월

SSH 무차별 공격

2011년 말에 이 이벤트가 상당히 증가하였지만, 활동 수준은 침체 국면에 접어든 것으로 보입니다. HTTP_Unix_Passwords와 매우 유사하게, 이 시그니처가 반드시 공격을 나타내진 않습니다. 하지만, 면밀히 살펴볼 필요가 있습니다.

이 시그니처에서는 검사해야 할 모든 트래픽이 암호화되어 있어 무차별 공격이나 사전 양식 공격이 일어나고 있는지를 알 수 없습니다. 이 시그니처는 특정 소스 주소에서 단기간에 SSH 서버 ID가 많이 발생하는 경우를 감지합니다. 구성에 따라, 이는 시스템을 점검하는 스캐너의 취약점, 무차별한 사전(Dictionary) 공격, 취약한 비밀번호를 점검하는 도구가 될 수 있습니다. 암호화된 패킷 내부를 확인할 수 없으므로, 소규모의 활동 의도를 파악할 적절한 방법이 없습니다. 서버 ID의 계수 요청은 시도되는 통신 종류의 지시기 역할을 하는 경향이 있으며, 수가 많을수록 더 의심을 해 보아야 합니다.

IBM의 권고는 동일합니다. 특정 계정에 대한 직접 로그인을 비활성화하고, 사용자명 및 비밀번호 보안을 시행하고, 특히 민감한 시스템에 대한 다중 요소 인증을 고려해야 합니다.

상위 MSS 대량 발생 시그니처 및 추세선 (SSH_Brute_Force)
2011년 7월 ~ 2012년 6월

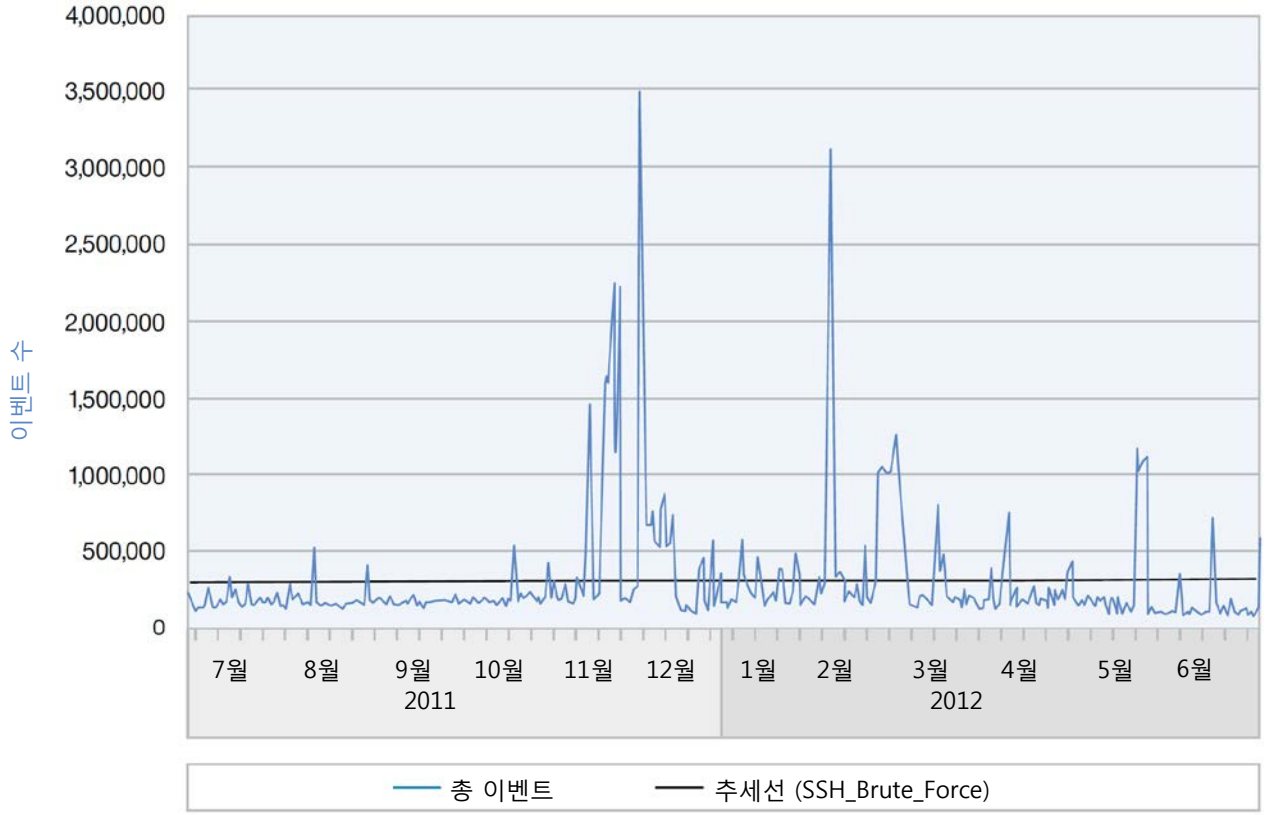


그림 10: 상위 MSS 대량 발생 시그니처 및 추세선 (SSH_ Brute_Force) - 2011년 7월 ~ 2012년 6월

HTTP Unix 비밀번호

이 시그니처는 HTTP 프로토콜을 이용하여 Unix 시스템 상의 비밀번호(즉, /etc/passwd 및 /etc/shadow) 파일에 대한 액세스 시도를 식별합니다. HTTP_Unix_Passwords 시그니처가 상위 대량 발생 리스트에 남아 있고 지속적인 상승 추세를 보이고 있지만, 2010년의 6위에서 2011년에는 8위로 하락했고 2012년에도 8위를 유지하고 있습니다. 몇몇 다른 시그니처와 마찬가지로, 이벤트 수는 계속 증가하고 있지만, 추가적인 고위험 이벤트의 수가 이 시그니처를 추월하고 있습니다.

HTTP Unix 비밀번호 공격은 상대적으로 오래되었지만 여전히 효과적이기 때문에 지속적으로 증가 추세를 보이고 있습니다. /etc/passwd에 대한 액세스 권한을 입수하려는 시도는 다수 프로토콜을 통해 이루어질 수 있으므로, HTTP_Unix_Passwd_File_Accessed 또는 FTP_Unix_Password_ File_Accessed와 같은 다른 시그니처도 있을 것입니다. 시스템 비밀번호에 대한 액세스 권한을 확보하여 해쉬 도구, 레인보우 테이블 또는 무차별 공격으로 이 보호를 해제하려는 시도가 수행되고 있으며, 공격자들이 원하는 결과를 가져다 주고 있습니다.

HTTP_Unix_Passwords 시그니처는 상위 대량 발생 리스트에 남아 있고 지속적인 상승 추세를 보이고 있으며, 현재 리스트에서 8위를 차지하고 있습니다.

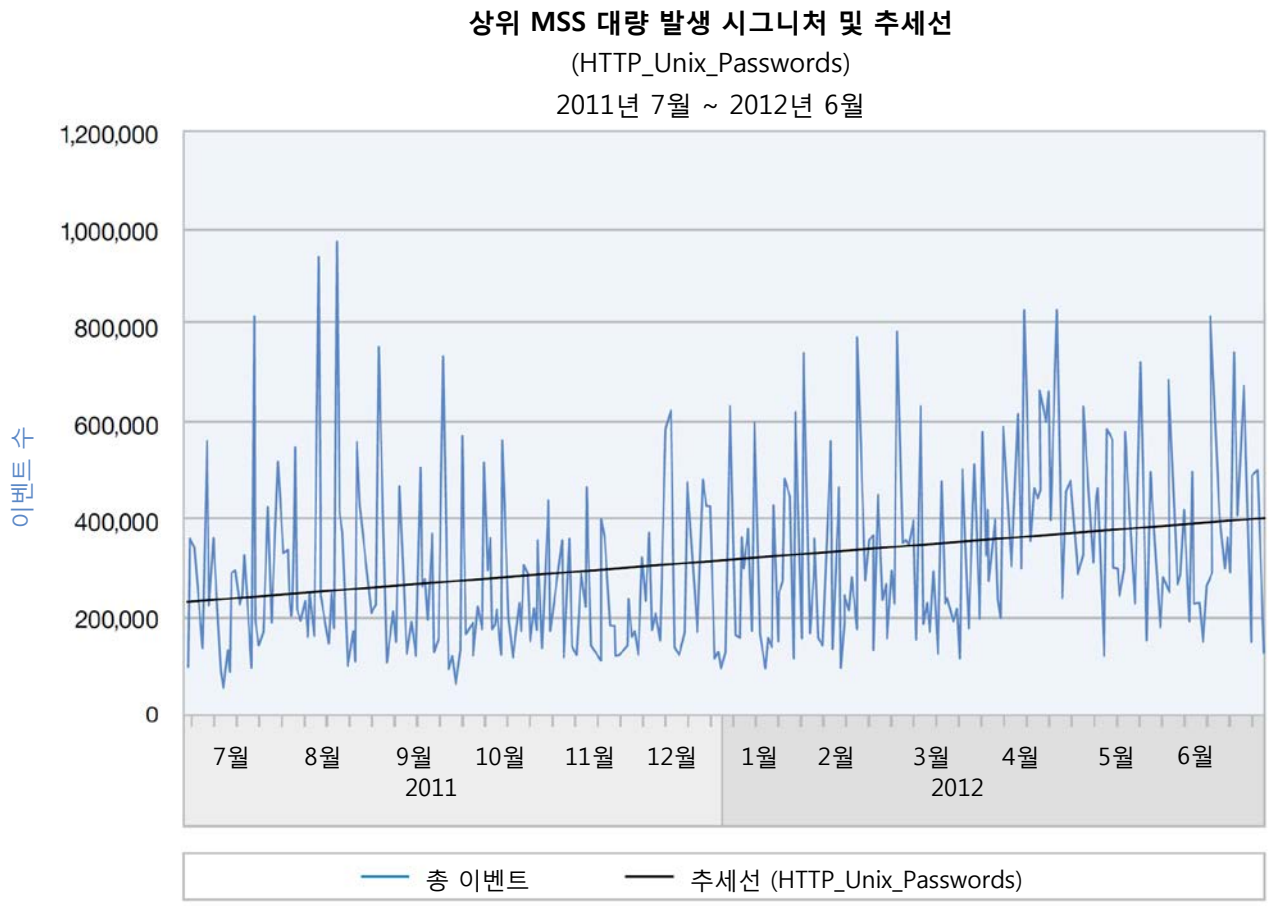


그림 11: 상위 MSS 대량 발생 시그니처 및 추세선 (HTTP_Unix_ Passwords) - 2011년 7월 ~ 2012년 6월

쉘 명령어 인젝션

쉘 명령어 인젝션은 모든 고객 유형에 꾸준하게 나타나는 원격 명령 수행(원격 코드 수행과 혼동하지 말 것)의 한 형태입니다. MSS(Managed Security Service)에 의해 이러한 공격 시도가 느리지만 꾸준히 증가하는 것이 확인되고 있으며, 앞으로도 더욱 증가할 것으로 예측합니다.

SQL 인젝션 공격과 마찬가지로, 이는 공격자가 서버에 거점을 마련할 수 있는 간단한 방법입니다. 거점이 마련되고 나면, 공격자는 방어벽 내부에서 다른 시스템을 공격하기 위한 착수 지점을 확보하여 전략적인 우위를 점할 수 있습니다. 공격은 만연하고 있으며 성공 확률도 매우 높습니다. "로우그(rogue)" PHP(예: C99 Shell)를 실행하는, 이미 감염된 시스템도 아래에 설명되어 있는 동일한 휴리스틱을 통해 노출될 수 있습니다. C99는 전적으로 악성이 아닌 원격 관리 도구이지만, 쉽게 이용할 수 있기 때문에 공격자들이 선호하고 있습니다.

Shell_Command_Injection 시그니처는 쉘 명령어 실행 시에 흔히 쓰이는 명령어 및 기호의 다양한 조합을 산정하여 Unix 쉘 명령어 인젝션 시도를 감지하는 일련의 휴리스틱입니다. 디폴트 구성에서 쉘 명령어는 튜닝 파라미터가 일치되거나 디렉토리 조회 시도가 감지되는 경우에만 산정됩니다. 이 두 경우 모두, 쉘 명령어와 기호를 산정하는 시도가 이루어집니다.

이 공격에 대한 대비책은 서버에 대한 사용자 입력을 검증하여 쉘 명령어를 제거하는 것입니다. 쉘 명령어(예: wget, passwd, dir, ls 등)에 대한 서버 소프트웨어 액세스를 제한하거나 배제하면 공격의 실효성을 낮출 수 있습니다.

상위 MSS 대량 발생 시그니처 및 추세선
(Shell_Command_Injection)
2011년 7월 ~ 2012년 6월

그림 12: 상위 MSS 대량 발생 시그니처 및 추세선 (Shell_Command_Injection) - 2011년 7월 ~ 2012년 6월

웹 브라우저 공격의 재개

최근, JavaScript_Shellcode_Detected 시그니처의 보고가 늘어났음에도 불구하고 브라우저 공격이 급증한 것으로 확인되었습니다. 이 시그니처는 JavaScript 내에서 암호화된, 쉘코드를 가장하여 이미 알려져 있거나 알려지지 않은 취약점을 공격하는 기계코드의 전송을 감지합니다. 다시 말하면, 이는 IBM의 "Ahead of the threat" 범위의 일부입니다. 2006년에 개시된 이래 이 시그니처에서 극소수의 오탐지가 관찰되었습니다. 이 시그니처의 발생이 급증한 이유는 웹 브라우저 공격 툴킷의 증가로 추측됩니다. 즉, 악성 링크를 제공하고 일부 경우에는 실제 악성 코드를 제공하는 취약한 서버를 노린 대대적인 웹 애플리케이션 공격 활동의 증가 때문일 것입니다.

상위 MSS 대량 발생 시그니처 및 추세선
(Shell_Command_Injection)
2011년 7월 ~ 2012년 6월

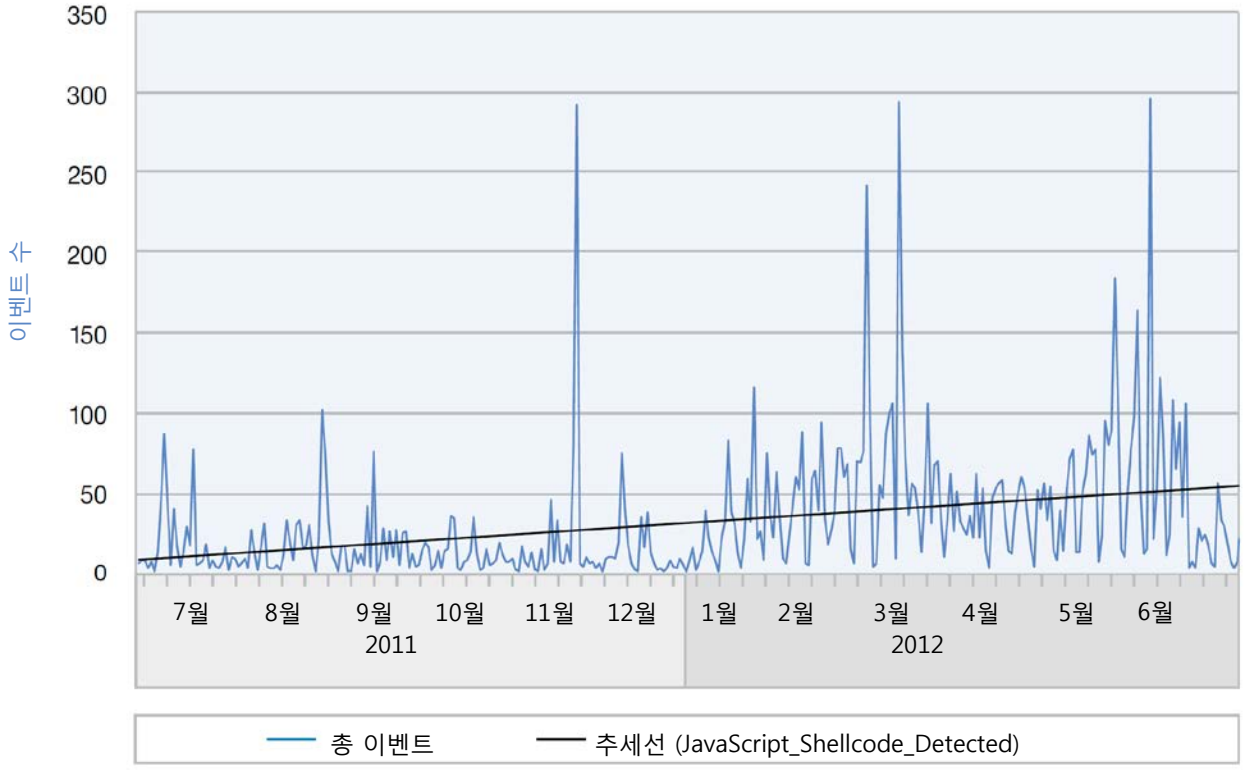


그림 13: 상위 MSS 대량 발생 시그니처 및 추세선 (JavaScript_Shellcode_Detected) - 2011년 7월 ~ 2012년 6월

알려지지 않은 동향—공격의 여진?

IBM 보안 분석가들이 동향 파악에 사용하는 여러 데이터 자원 중의 하나가 다크넷(darknet)입니다. 다크넷은 한번도 서비스가 제공된 적이 없는 인터넷 상의 광범위한 IP 주소입니다. 다크넷은 블랙홀 네트워크 또는 네트워크 텔레스코프(network telescope)라고도 합니다. IBM의 다크넷은 25,600개의 주소를 가지고 있습니다. 일반적으로는 인터넷 상의 컴퓨터가 이 범위의 주소로 패킷을 전송할 이유가 없지만, 실상은 패킷이 전송되고 있습니다. 이 주소 범위로 수신되는 트래픽은 종종 악의적인 활동과 연관이 있습니다. 이 영역은 지속적으로 모니터링 되고 있으며, 모든 수신 트래픽이 캡처되고 분석 및 장기 보관을 위해 저장됩니다.

위장 서비스 거부(DoS) 공격

지난 수 년간의 데이터를 살펴보면, 두 가지 추세가 나타나도 있습니다. 첫 번째 추세는 백스캐터(backscatter) 활동의 점진적인 증가입니다 (그림 14). 백스캐터는 사실상 위장 서비스 거부(DoS) 공격의 부작용입니다. 인터넷 상에서 서비스 거부(DoS) 공격을 개시하는 공격자들은 종종 피해자의 시스템에 대량 전송하는 패킷에 가짜 소스 주소를 넣습니다. 이는 스푸핑으로 알려져 있습니다. 공격자는 무작위로 선정된 소스 주소를 스푸핑하고 피해자의 시스템이 공격 기점을 파악하여 차단하거나, 위장된 패킷과 실제 사용자의 합법적인 패킷을 구분하기 어렵게 만듭니다. 이는 종종 실제 공격 기점을 감추고 간단한 패킷 필터를 피하기 위한 목적으로 서비스 거부(DoS) 공격이나 분산 서비스 거부(DDoS) 공격에 쓰입니다. 피해자의 시스템은 이 위장 패킷을 합법적인 패킷으로 여겨 거짓 주소로 응답을 전송하며, 공격자 시스템 상의 자원에 연결이 됩니다. 이러한 반응을 백스캐터라고 합니다. 공격자가 무작위로 다크넷 범위의 한 IP 주소를 선정하여 피해자 시스템이 응답하면, 우리는 그 응답을 수집하여 보관합니다. 이러한 응답과 그 패턴을 조사하면, 인터넷 상의 서비스 거부(DoS) 활동을 탐지하고 추적할 수 있습니다.

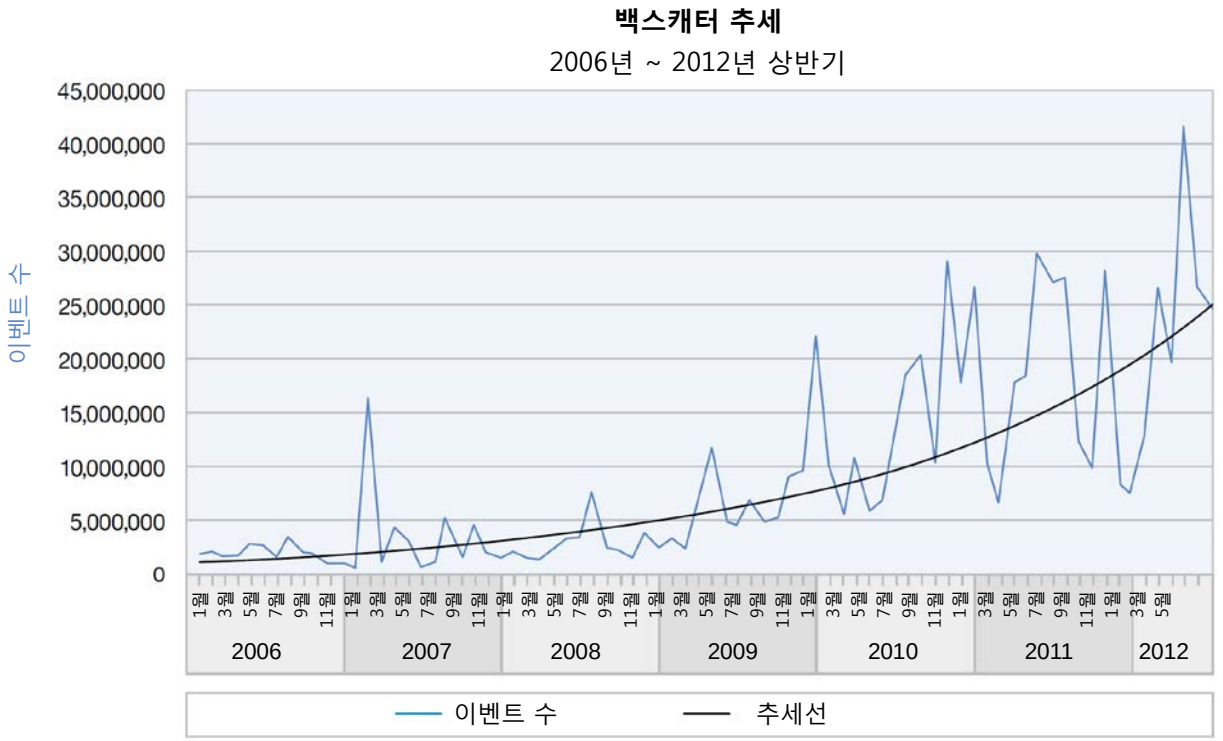


그림 14: 백스캐터 추세 – 2006년 ~ 2012년 상반기

IBM X-Force 다크넷에서 수신된 각 SYN-ACK (응답) 백스캐터 패킷은 공격자가 위장된 SYN (요청) 패킷을 공격 대상 시스템의 알려진 서비스 포트로 전송하였음을 나타내며, 이는 IBM X-Force 다크넷 주소 중의 하나로 위장된 것일 수 있습니다. 2006년 이래 백스캐터 활동은 점진적으로 증가해 왔으며, 2008년과 2009년 사이에는 대폭적인 증가가 있었습니다. 이는 2009년에 최대 규모의 급증이 있었기 때문입니다. 이러한 백스캐터 증가 추세는 2010년 또 한 차례의 대규모 증가와 더불어 2011년까지 이어졌습니다. 2010년 2사분기 말에, 2010년 상반기의 평균 이벤트 건수는 2009년 전체 평균보다 약간 더 높은 1650만 건을 다소 상회하였습니다. 2010년 말, 이 수치는 1800만 건 이상으로 급증했습니다. 2011년 중반에는 매월 급증하면서 3000만 건에 달했습니다. 2011년 하반기에는 그 규모가 다소 감소했지만, 2012년에 들어 백스캐터 활동이 4200만 건으로 급증하였습니다. 그림 2는 2006년부터 2011년까지 인터넷 상의 연간 위장 서비스 거부(DoS) 공격 규모를 보여줍니다.

이 백스캐터 활동의 점진적인 증가와 일부 대규모 급증에서 무엇을 추정할 수 있을까요? 백스캐터 데이터의 대다수는 서비스 거부(DoS) 공격에서 기인하므로, 2006년 이래 위장 DoS 공격이 꾸준히 증가했다는 것을 추정할 수 있습니다. 그러나, 백스캐터는 수집 및 발생의 특성으로 인하여 변화의 폭이 클 수밖에 없습니다. 일부 백스캐터 활동이 격렬했던 기간은 여러 공격자 단체 내부 및 단체 간의 대출혈전의 결과일 것입니다. 이 출혈전 중에, 한 단체가 다른 단체의 자원을 차단하거나 인수하려는 시도가 일어날 수 있습니다. 교전 중인 단체 간의 이러한 "포격전"은 백스캐터 트래픽과 소스 주소의 갑작스런 증가를 유발할 수 있습니다. 이러한 증가는 일반적으로 시작과 마찬가지로 돌연히 멈춥니다. 이러한 유형의 활동은 그림 15에서 보는 바와 같이, 2007년 2월, 2009년 12월과 가장 최근에는 2012년 4월에 있었던 급증의 가장 주된 원인이었을 가능성이 높습니다.

연간 백스캐터 누적 건수

2006 ~ 2011년

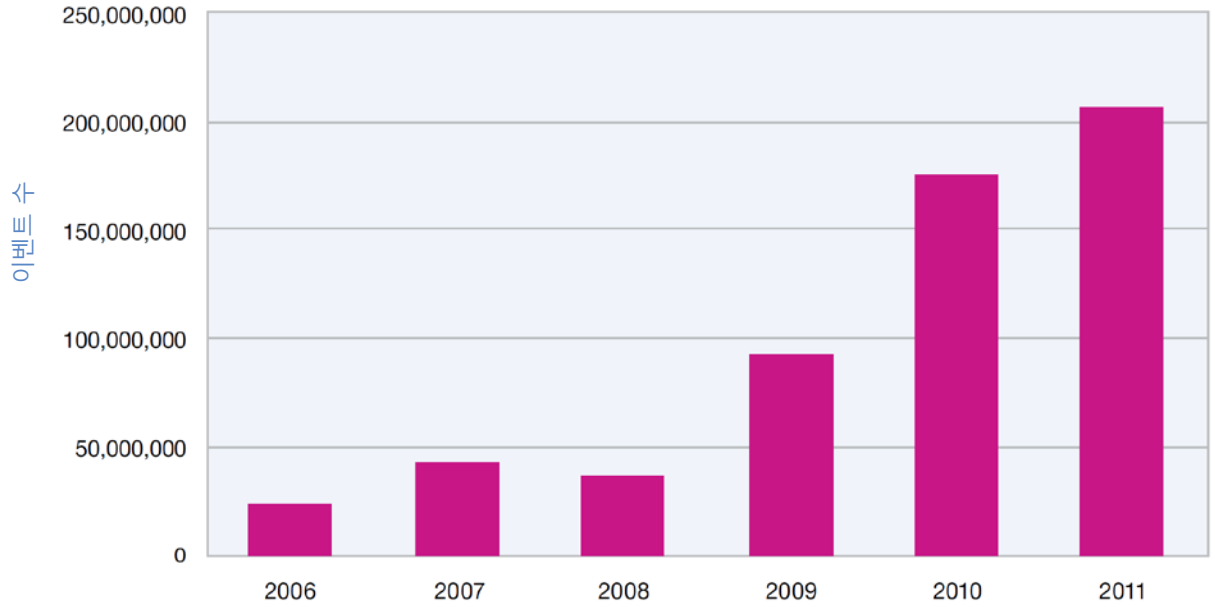


그림 15: 연간 백스캐터 누적 건수 – 2006 ~ 2011년

위장 서비스 거부(DoS) 공격의 대상

위장 서비스 거부(DoS) 공격은 그 특성상 공격 기점을 파악하기가 어렵습니다. 공격자는 기점을 조작하여 피해자의 IP 주소에 접속합니다. 이 조작된 접속은 다수의 다른 주소에서 이루어질 수 있습니다. IBM X-Force 다크넷의 백스캐터를 살펴보면, 공격 기점이 위장되어 있지만 공격의 대상 로케일을 파악할 수 있습니다. 백스캐터의 소스를 조사해보면 위장 서비스 거부(DoS) 공격의 대상에 관한 정보를 얻을 수 있습니다. 그림 16에는 주소와 국가를 연관시키는 WorldIP 데이터베이스를 사용하여 파악된 2012년 상반기의 백스캐터 발신 상위 대상 국가가 나와 있습니다.

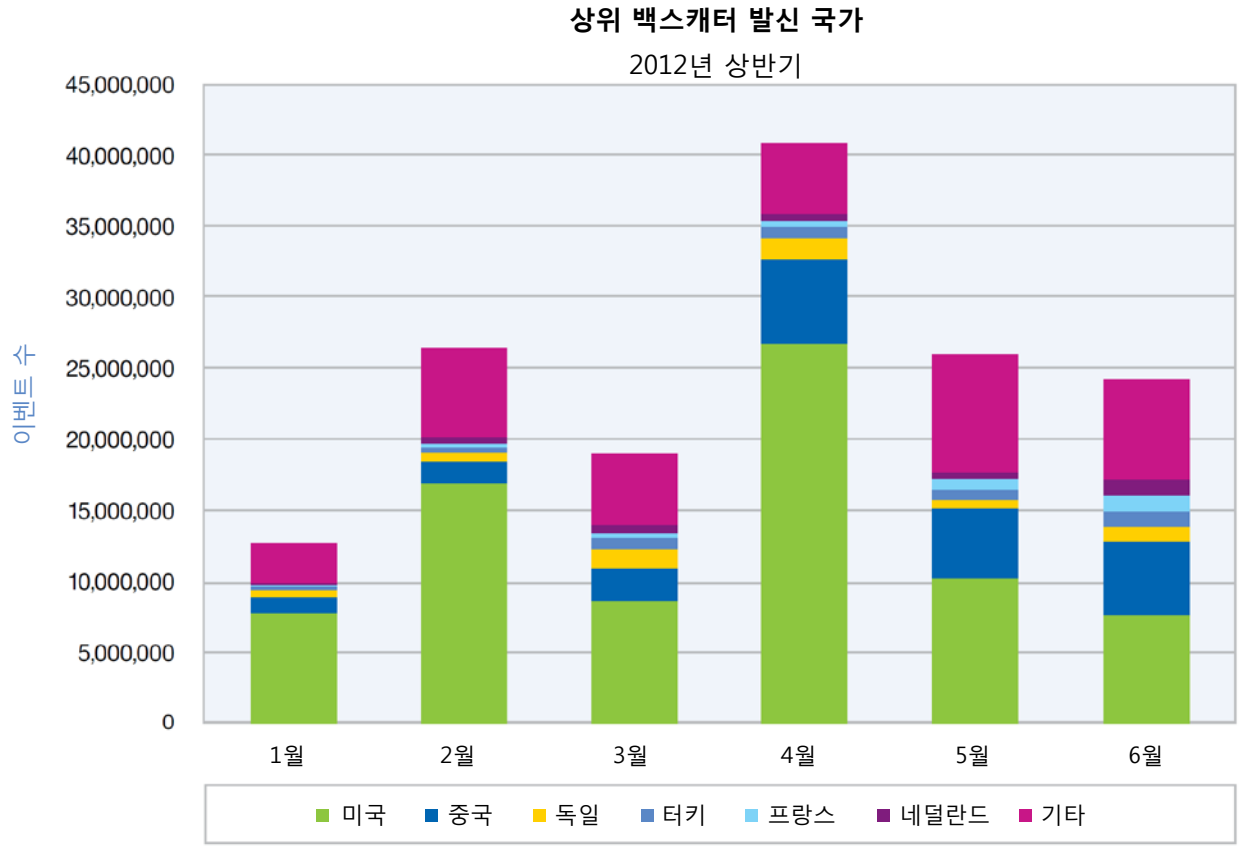


그림 16: 상위 백스캐터 발신 국가 – 2012년 상반기

이 데이터에는 매우 분명한 한 가지 추세가 있습니다. 미국이 지금까지 최대 발신 국가이며, 중국이 2위 그리고 독일은 큰 차이로 3위입니다. 나머지 개별 국가들은 차이가 더 큰 차이를 보입니다. 미국과 중국은 할당된 IPv4 주소가 첫 번째 및 두 번째로 많으며, 양국의 백스캐터 발신 순위가 예상 밖의 결과는 아닙니다. IP 주소가 대상이 될 가능성으로 보자면 일본, 한국 또는 영국을 꼽을 수 있을 것입니다. 그러나 이 차트의 상위 국가를 제외한 대상을 나타내는 "기타" 건수가 매우 많으며, 미국과 중국 다음에는 건수에서 급감한 것에서 알 수 있듯이, 공격은 매우 다양하며 어디에서나 일어날 수 있습니다.

대부분의 경우, "기타" 범주에 들어가는 국가는 파악이 가능하지만 상위 국가에 비해 건수가 적은 국가들이지만, 이 범주에는 정확한 국가 코드 정보가 없는 주소 블록이 포함되어 있습니다. "기타" 범주의 IPv4 주소는 주소 추적이 완전하지 않았던 인터넷 초창기의 레거시 주소인 경우가 많으며, 여전히 인터넷 주소 공간에서 상당한 부분을 차지하고 있습니다.

"기타" 범주에는 차트에서 명확하게 확인된 상위 6대 국가에서 수집된 백스캐터가 포함되어 있으며, 각 막대의 전체 높이는 수집된 전체 백스캐터 트래픽을 나타냅니다. 2012년 2월의 소규모 급증과 더불어, 2012년 4월의 대규모 급증이 명확하게 눈에 띕니다. 2012년 6월에는 미국과 중국의 백스캐터 트래픽이 유사해지면서 중국 백스캐터 활동의 상관관계가 분명치 않아졌으나, 이러한 급증은 미국 백스캐터 활동의 변동과 일치하고 있습니다.

Mac용 악성 코드—대규모 출현 및 표적 공격

지난 IBM X-Force 동향 및 위험 보고서에서는 Mac용 악성코드의 출현을 설명하였습니다. Mac용 악성코드가 2012년에 더욱 늘어날 것이며, 이 악성코드는 Windows 악성코드와 더욱 더 유사해질 것이라는 예측도 하였습니다. 2012년 상반기를 되돌아 보면, 이 예측이 정확했던 것으로 보입니다.

지난 수 개월 동안 Flashback의 출현 및 APT (advanced persistent threat, 지능형 지속가능 위협) Mac용 악성코드의 발견과 같은 일부 Mac용 악성코드의 중대한 사건이 있었습니다. 이러한 상황을 자세히 살펴보기로 하겠습니다.

Flashback

Flashback의 첫 번째 변종이 2011년 9월에 발견되었습니다. 그 후 여러 변종들이 유포되었지만, 올해 유포된 변종들은 특이한 양상을 보였습니다. 이 변종들은 예전 변종의 기능을 대부분 가지고 있으며, 이번에는 그 전달 방법에 있어 성공률이 매우 높았습니다.

초기의 Flashback 변종들이 사회공학적 수법을 이용하여 사용자들의 설치를 유도했던 반면에, 신종은 Windows 악성코드에서 보편적인 자동 다운로드 (drive-by-download) 기법도 채택하였습니다.

Flashback은 공격이 포함된 사이트로 링크를 전송하도록 호스트가 수정된 Wordpress 블로그 사이트를 통해 그 목적을 달성했습니다.

지난 보고서에서는 OS X 소프트웨어 공격의 기술적인 어려움이 대대적인 공격을 방지하는 주 요인이라고 설명하였습니다. Flashback은 Java 취약점을 이용하는 다중 플랫폼 공격을 사용하여 이 문제를 해결합니다. 즉 대상이 Windows냐 Mac이냐에 상관없이, 공격 수법과 대부분의 관련 코드가 동일합니다.

Flashback은 CVE-2011-3544(Java Applet Rhino 스크립트 엔진 취약점)과 CVE-2008-5353(Java Calendar 역직렬화 취약점)을 지난 2월의 두 가지 Java 공격에 처음 사용하였지만, 당시 바로 패치되었기 때문에 감염의 확산은 차단되었습니다. 하지만, Flashback이 CVE-2012-0507(Java AtomicReferenceArray 유형 위반 취약점)을 3월의 공격에 사용했을 때는 상황이 달라졌습니다. Oracle이 2월에 이 취약점에 대한 패치를 이미 실시했지만 Apple 버전의 Java는 업데이트되지 않아, 다수의 Mac 시스템이 이 공격에 취약한 상태였습니다. 그 결과, 막대한 규모의 대량 감염이 발생했으며, Flashback은 지금까지 가장 널리 확산된 Mac용 악성코드가 되었습니다.

일부 보안 솔루션 공급업체들은 싱크홀을 설치하여 Flashback 감염 대수를 산정했으며, 600,000대에 달하는 시스템이 감염된 것으로 추정하였습니다.

또한 이 Flashback 출현으로 클릭재킹(click-jacking)을 통해 수익을 올리려는 악성코드의 주된 목적이 밝혀졌습니다. Flashback이 설치되고 나면 악성코드가 브라우저를 속여 구글 광고 클릭이나 구글 검색을 가로챕니다. 구글 광고를 클릭하면 쿼리 파라미터가 구글 서버가 아닌 C&C(Command and Control) 서버로 전송됩니다. 구글 검색이 탐지되면 검색 파라미터가 C&C 서버로 전송되고, C&C 서버는 실제 구글 검색 결과가 아닌 Flashback 작성자 소유의 PPC(pay-per-click) URL로 응답합니다.

Mac APT

올해 상반기 Mac용 악성코드의 또 다른 중대한 사건은 표적 공격 악성코드의 발견입니다.

우선 3월에 발견된 Tibet 악성코드가 있습니다. Java 공격 CVE-2011-3544(Java Applet Rhino 스크립트 엔진 취약점)에 사용된 첫 번째 변종을 Flashback이 다시 사용하면서 확산되었습니다. 그 주된 목적은 사용자의 데이터를 복사하여 다운로드하는 것입니다.

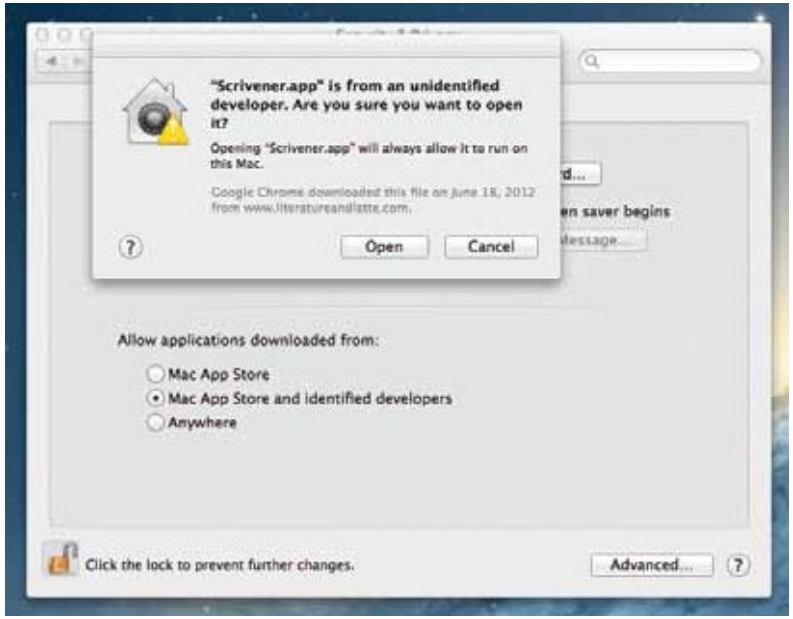
이 변종은 특히 티벳 비정부기구(NGO)를 대상으로 한 이메일의 링크를 통해 확산되었습니다. 그 다음 변종은 다른 전달 방법을 사용합니다. 이 변종들은 MS Word 취약점인 CVE-2009-0563(MS Word 레코드 구문분석 버퍼 오버플로우 취약점)을 사용합니다. 이 취약점은 2009년에 수정되었습니다. 이 패치는 Mac용 Word 2004 및 2008 버전에서 작용하며, Mac용 Word 2011 버전에서는 작용하지 않습니다. Word 문서 파일에는 티벳의 정치 상황을 논하는 내용이 들어 있어, 연구자들이 티벳 NGO를 겨냥하는 첫 번째 변종으로 추정하게끔 만들었습니다.

또 다른 표적 악성코드 공격은 4월에 처음 발견된 SabPub 백도어입니다. 악성코드를 호스팅한 URL에 이르게 하는 이메일이 보고되었지만, 이 첫 번째 변종은 처음에는 표적 공격이라는 징후를 보이지 않았습니다. 이 악성코드는 Flashback과 동일한 Java 공격인 CVE-2012-0507(Java AtomicReferenceArray 유형 위반 취약점)을 사용합니다. 이 취약점은 이미 수정되었기 때문에 처음 유포되었을 때 동일한 공격을 사용했던 Flashback 변종과 같이 큰 영향을 주지는 않았습니다. 그 다음 변종은 동일한 Word 문서 공격을 사용하여 전달된다는 점에서 Tibet 악성코드와 유사합니다. Tibet 악성코드와 마찬가지로, Word 문서는 티벳어 본문을 보여줍니다.

결론

Flashback 악성코드의 출현으로 Mac이 악성코드에 취약하지 않다는 오랜 믿음은 종지부를 찍게 되었으며, 다음에 어떤 상황이 벌어질지라도 더 이상 놀라지 않을 지경에 이르렀습니다. 실제로 이 보고서를 작성하던 시점에, Crisis라는 안티 리버싱(anti-reversing) 및 루트킷 기능을 갖춘 새로운 Mac 백도어가 발견되었습니다. Crisis는 우리가 지난 IBM X-Force 동향 및 위험 보고서에서 예측했던 유형의 악성코드입니다.

Apple은 최근 Gatekeeper 및 자동 보안 업데이트 등의 보안 기능을 추가한 OS X Mountain Lion을 발표하였습니다. 2012년 6월 이후, Apple은 모든 애플리케이션을 샌드박싱이 활성화된 상태로 Mac App Store에 제출할 것을 요구하고 있습니다. 이는 Flashback에서 겪었던 동일한 대량 감염을 방지하는 데 도움이 되는 중요한 조치이지만, 이러한 개선이 향후 얼마나 효과적으로 악성코드를 차단할지는 지켜보아야 할 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. 동 데이터 센터는 1999년 이후 170억 건의 웹 페이지 및 이미지를 분석하였습니다.

IBM 웹 필터 데이터베이스는 68 가지의 필터 범주와 7100만 건의 엔트리를 갖추고 있으며, 매일 150,000건의 신규 또는 갱신 엔트리가 추가되고 있습니다.

이 단원에서는 다음에 대하여 검토해 봅니다.

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

분석 방법론

IBM X-Force는 IBM 보안 시스템 웹 필터 데이터베이스의 분류 기준에 따라 호스트를 산정하여 인터넷 상의 컨텐츠 배포에 관한 정보를 수집합니다. 호스트 산정은 컨텐츠 배포의 확인에 적절한 방법이며 실질적인 평가를 제공합니다. 웹 페이지 및 하위 페이지 산정과 같은 다른 방법을 사용할 경우에는 결과가 달라질 수 있습니다.

웹사이트의 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 바닥난 상태이기 때문에, IPv6 주소로 전환하는 사이트의 수가 갈수록 늘어날 전망입니다. 하지만, 2012년 5월까지의 수치를 살펴보면, 이 예상에 미치지 못하고 있습니다. 그러나 6월에는 상당한 증가가 있었으며, 하나 이상의 호스트가 IPv6를 지원하는 도메인의 비중이 처음으로 3%에 달하였습니다.

IPv6 호스트를 지원하는 도메인의 비율
2011년 8월 ~ 2012년 6월

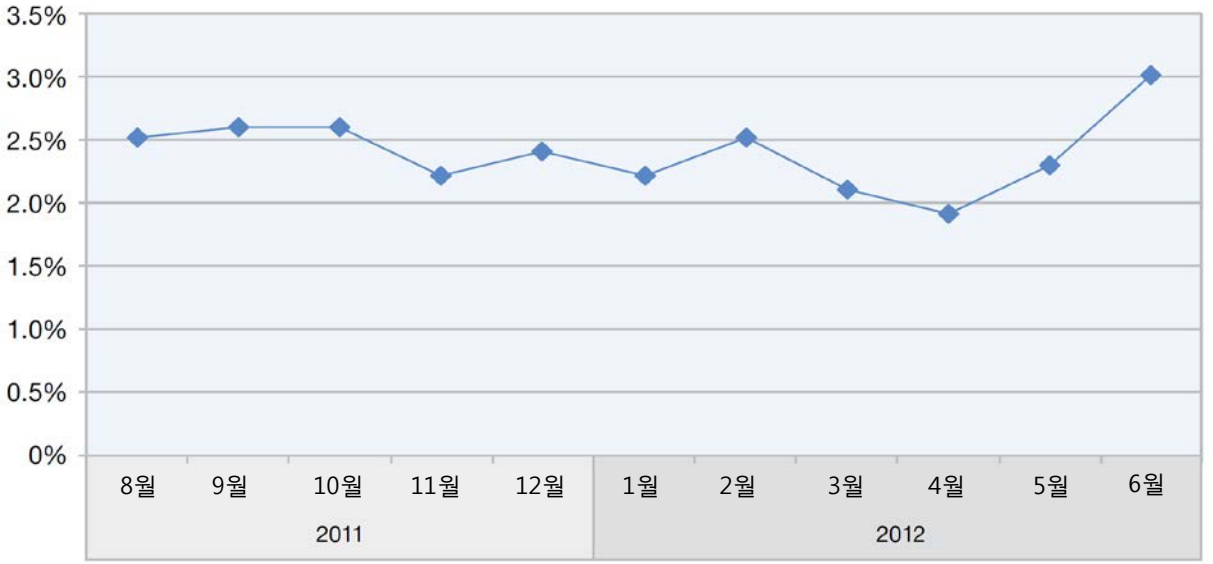


그림 17: IPv6 호스트를 지원하는 도메인의 비율 - 2011년 8월 ~ 2012년 6월

이 증가를 분석해보기 위해, 2012년 5월 및 6월의 수치를 좀 더 자세히 살펴보겠습니다.

변화는 23번째 주에 일어났습니다. 이 주의 중간(6월 6일)에 2012년 IPv6 Day[1]가 있었습니다. 올해에는 다수 기업과 기관들이 IPv6를 영구적으로 구축하였습니다. 그림 18은 이를 분명히 보여줍니다.

IPv6 호스트를 지원하는 도메인의 비율
2012년 5월 ~ 2012년 6월, 주 단위

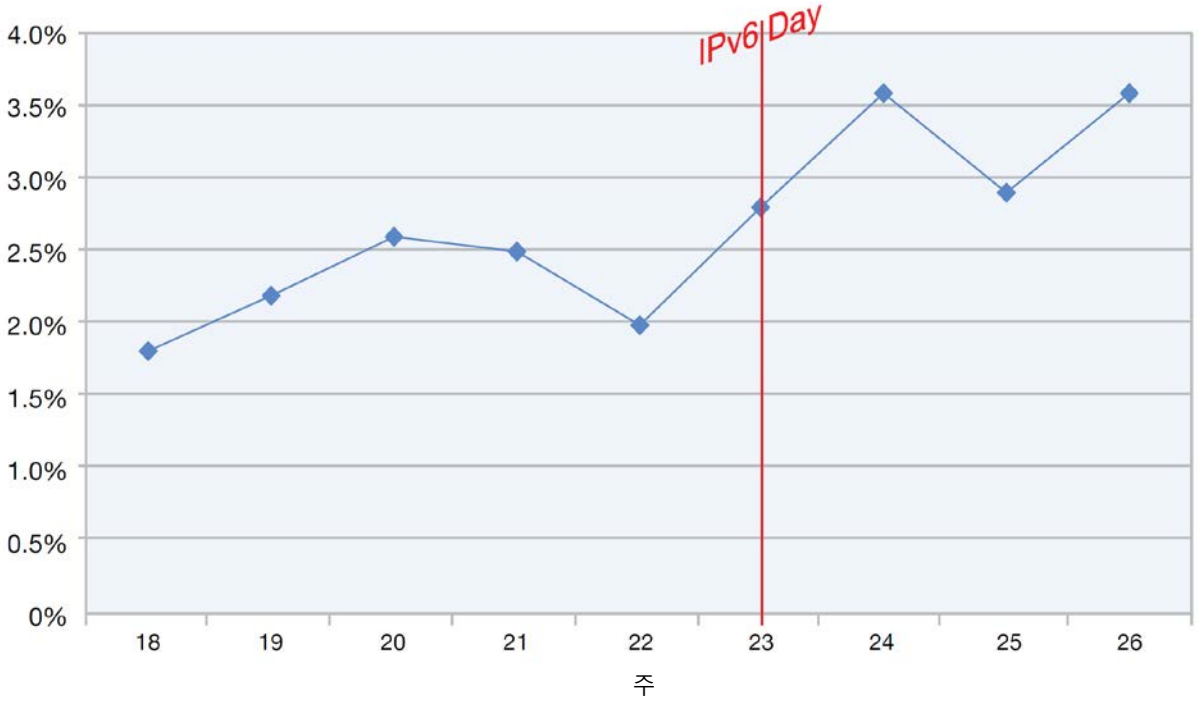


그림 18: IPv6 호스트를 지원하는 도메인의 비율 - 2012년 5월 ~ 2012년 6월, 주 단위

1 http://en.wikipedia.org/wiki/World_ipv6_day 참조

하나 이상의 IPv6 지원 호스트를 제공하는 도메인은 IPv6에 준비된 사이트라고 할 수 있습니다. IPv6 레디 웹사이트의 범주[2] 유형을 살펴보면, 또 다른 흥미로운 추세가 나타납니다.

- 웹 2.0 사이트와 더불어 정부 기관은 인터넷에서 IPv6 준비가 가장 잘된 분야입니다.
- 다수 비정부 기구, 검색 엔진, 포털, IT 사이트, 뉴스 사이트와 블로그도 준비가 양호합니다.
- 기존의 웹 메일러, 스포츠 사이트, 컴퓨터 게임 사이트, 쇼핑 사이트, 데이팅 사이트와 같은 소비자 사이트는 여전히 평균 3%(차트에 의거한 6월 평균)를 상회합니다.
- 불법 약물 거래 사이트, 익명 프록시, 음란물, 도박 사이트와 컨텐츠가 있는 웹사이트는 IPv6에 대비되어 있지 않습니다.
- 스팸 URL은 부류의 최하단을 차지하고 있습니다.

평균 이상의 준비도	IPv6 준비 비율	평균 이하 준비도
소셜 미디어	29.7%	
소셜 네트워킹	26.2%	
정부 기관	14.5%	
웹 스토리지	9.3%	
비정부 기구	9.3%	
검색 엔진 / 웹 카탈로그 / 포털	9.3%	
대화 사이트	8.6%	
소프트웨어 / 하드웨어	8.3%	
뉴스 / 잡지	8.3%	
블로그 / 게시판	7.5%	
웹메일	6.5%	
교육	6.0%	
스포츠	5.7%	
컴퓨터 게임	5.5%	
쇼핑	5.5%	
데이팅 사이트	4.8%	
	3.6%	와레즈 / 해킹 / 컴퓨터 범죄
은행	3.3%	
	2.8%	불법 약물
일반 기업	2.5%	
여행사	1.7%	
	1.4%	불법 활동
	1.3%	익명 프록시
	1.3%	악성코드
	1.1%	음란물
	1.1%	폭력 / 극단
	0.8%	도박 / 복권
	0.5%	스팸 URL

2 전술한 웹사이트 범주의 상세한 설명은 다음 사이트를 참조할 것: http://filterdb.iss.net/categories/

그렇다면 악의적인 의도를 가진 자들이 IPv6 기술을 회피하는 이유는 무엇일까요? 원치 않는 웹사이트의 대부분이 단 몇 시간 동안만 존재한다는 점이 한 가지 답이 될 것입니다. 이는 특히 스팸 URL의 경우에 더욱 그러하며, 따라서 기술적인 노력을 추가적으로 쏟는 것을 꺼릴 것입니다. 아울러, 스패머들은 최대한 많은 사용자를 획득하길 원하기 때문에, 모든 사람들이 IPv4를 "사용"하고 극소수만이 IPv6를 "사용"할 수 있는 상황에서 굳이 IPv6를 지원할 필요가 없습니다.

향후 수 개월 및 수 년 내로 IPv6 지원의 급격한 증가를 지켜보는 것은 흥미로운 일일 것입니다.

익명 프록시

익명 프록시의 증가

인터넷이 가정, 직장, 학교 등에서 우리 생활에 더욱 필수불가결한 부분이 되면서, 공공 장소에서 적절한 환경을 유지 관리해야 할 책임이 있는 조직은 인터넷 이용자들을 통제할 필요성을 더욱 절감하고 있습니다.

통제 방법 중 하나는 부적절한 웹사이트에 대한 접근을 막는 컨텐츠 필터링 시스템입니다. 어떤 사람들은 웹 필터링 기술을 우회하기 위해 (웹 프록시라고도 불리는) 익명 프록시를 사용하기도 합니다. 웹 프록시를 이용하면 대상 웹사이트를 직접 방문하는 대신 웹 양식에 URL을 입력할 수 있습니다. 프록시를 사용하면 대상 URL이 웹 필터를 우회하게 됩니다. 웹 필터가 익명 프록시를 감시 또는 차단하도록 설정되지 않은 경우, 일반적으로 차단되었을 이 활동이 필터를 우회하여 허용되지 않은 웹사이트에 사용자가 접속할 수 있게 됩니다.

새로 등록된 익명 프록시 웹사이트의 증가는 이러한 추세를 반영합니다.

새로 등록된 익명 프록시 웹사이트의 규모
2008년 상반기 ~ 2012년 상반기

그림 18: IPv6 호스트를 지원하는 도메인의 비율 - 2012년 5월 ~ 2012년 6월, 주 단위

2011년 상반기에 등록된 익명 프록시는 3년 전에 비해 4배 정도 많습니다. 그리고 2011년 하반기와 2012년 상반기에 등록된 익명 프록시는 3년 전에 비해 3배 이상 많습니다. 그 이후에는 익명 프록시의 증가를 또 다시 볼 수 없었습니다. 아마도 이는 인터넷 활동이 소셜 네트워크에 더 집중된 데 따른 것으로 보입니다. 직장이나 학교에서 이러한 사이트를 차단하지 않은 경우가 많아, 더 이상 컨텐츠 필터링 시스템을 우회할 필요가 없습니다.

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

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

익명 프록시의 최상위 도메인

익명 프록시 웹사이트가 사용하는 최상위 도메인은 손에 꼽을 수 있을 정도로 적습니다. 2009년 말까지는 .com 및 .info 도메인이 전체 익명 프록시의 70% 이상에 달하면서 주를 이루었으나, 2009년 말에 .cc 도메인(호주령 코코스(킬링) 아일랜드의 최상위 도메인)이 출시되고 2010년 봄에는 .tk 도메인(뉴질랜드령 토켈라우의 최상위 도메인)이 출시되면서 상황이 바뀌었습니다.

새로 등록된 익명 프록시 웹사이트의 최상위 도메인

2009년 3사분기 ~ 2012년 2사분기

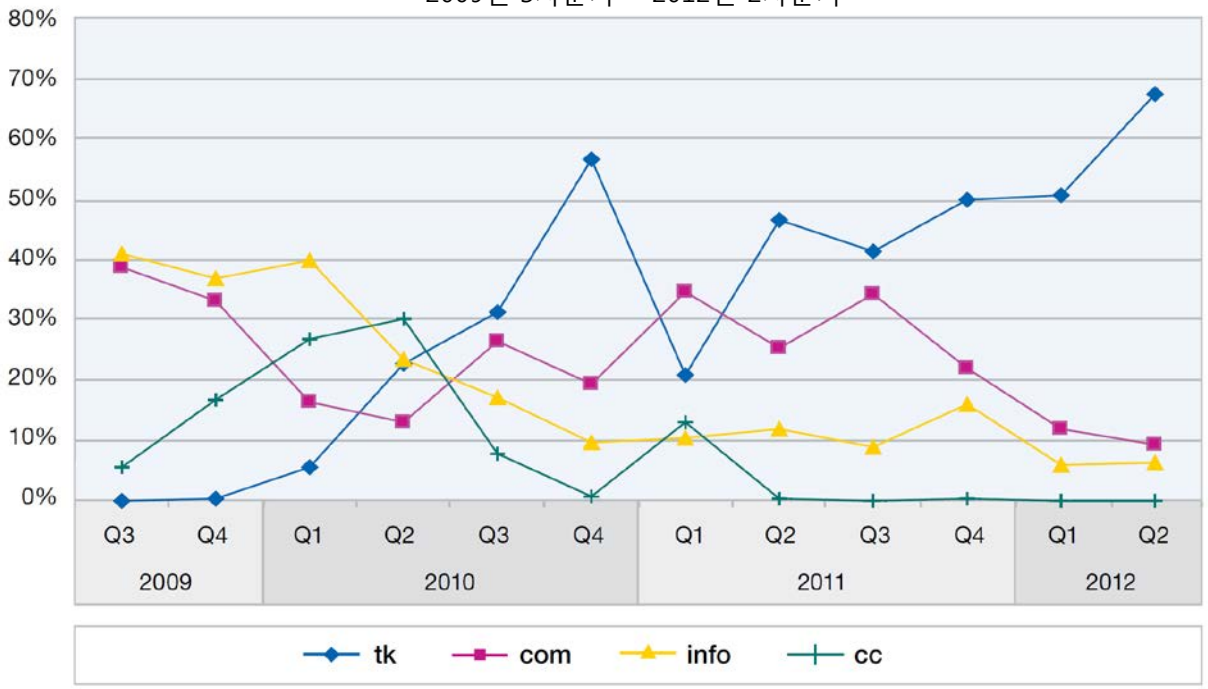


그림 20: 새로 등록된 익명 프록시 웹사이트의 최상위 도메인 - 2009년 3사분기 ~ 2012년 2사분기

이전의 IBM X-Force 동향 및 위험 보고서에서 설명한 바와 같이, 이러한 최상위 도메인의 도메인은 비용이 들지 않습니다.[3] 현재 .info 도메인을 사용하는 익명 프록시는 전체의 10% 미만입니다. .com 도메인의 경우에도 마찬가지입니다. 2012년 2사분기에는, 전체 익명 프록시의 2/3 이상이 .tk 도메인 상에서 운영되고 있습니다.

악성 웹사이트

이 단원에서는 악성 링크가 운영되는 국가와 이러한 악성 웹사이트에 가장 자주 링크되는 웹사이트 유형을 살펴봅니다.

악성 웹 링크의 지리적 위치

미국이 계속 악성 링크 운영 국가 1위를 달리고 있습니다. 악성코드 링크의 43% 이상이 미국에서 운영되고 있으며, 9.2%가 운영되고 있는 독일이 2위입니다. 러시아가 처음으로 3위에 올랐으며, 중국은 2010년까지 줄곧 1,2위를 달렸지만, 지금은 4위에 있습니다. 프랑스에서는 4%의 악성코드가 운영되고 있습니다. 루마니아는 약 8%에 달한 2010년과 2011년에 강세를 보였지만, 이후 1.1%로 하락하였습니다.

악성 URL이 가장 많이 운영되고 있는 국가
2006년 ~ 2012년 상반기

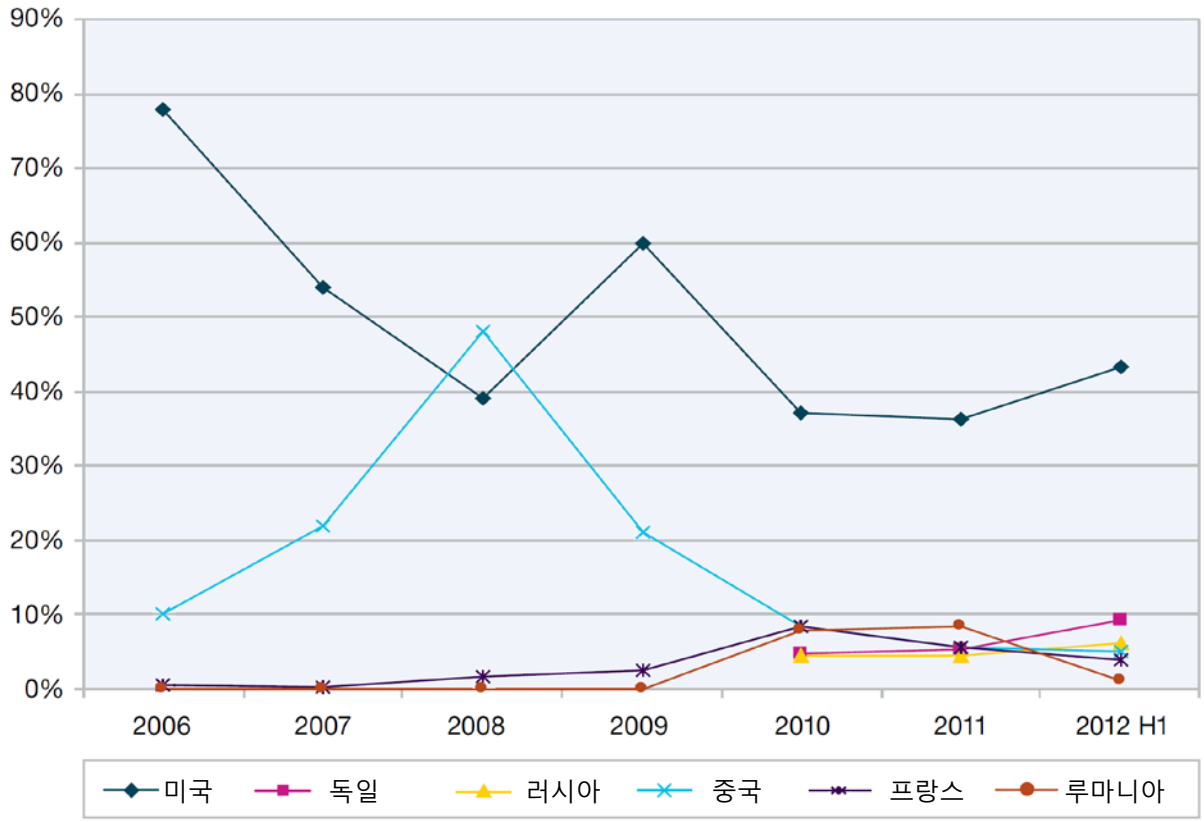


그림 21: 악성 URL이 가장 많이 운영되고 있는 국가 - 2006년 ~ 2012년 상반기

3 http://www.co.cc/?lang=en 및 http://www.dot.tk/ 참조

불량 링크가 있는 우량 웹사이트

본 보고서 및 지난 보고서의 여러 곳에 언급되어 있는 것처럼, 공격자는 여전히 신뢰성 있는 웹사이트의 명성을 이용하여 최종 사용자의 경계를 늦추고 보호 기술로 공격을 위장하는 데 더욱 주력하고 있습니다. 악성 웹 컨텐츠를 사용한다는 점은 그대로입니다. 지금부터 가장 빈번하게 알려진 악성 링크가 포함된 웹사이트의 유형을 간략하게 분석해 보겠습니다.

몇 가지 상위 범주는 예상과 크게 다르지 않았습니다. 일례로, 음란물 및 도박 사이트를 목록 상위로 예상할 수 있습니다. 이 두 사이트가 현재 전체 악성 링크의 약 50%를 차지하고 있습니다. 하지만, 2군 후보들은 한층 "신뢰성 있는" 범주에 속합니다.

블로그, 게시판, 개인 웹사이트, 검색 엔진이 이 두 번째 계층의 범주에 속합니다. 이러한 웹사이트의 대다수는 사용자가 컨텐츠를 업로드하거나 자신의 웹사이트를 구성할 수 있는 서비스를 제공합니다. 다시 말해서, 이런 유형의 웹사이트가 의도적으로 악성 링크를 게시할 가능성은 거의 없습니다.

다음 차트는 악성코드 링크 유포 이력을 보여주고 있습니다.

지난 3년 반의 기간을 살펴보면, 흥미로운 추세가 보입니다.

- 음란물 및 도박 사이트와 같은 웹사이트가 1년 이상 악성코드를 체계적으로 유포하면서 점유율 1, 2위를 다투고 있습니다.
- 음란물 사이트가 전체 악성 링크의 1/3 이상을 차지하면서 1위에 올랐습니다.
- 도박 사이트는 처음으로 악성코드의 감소세를 보였지만, 여전히 전체 악성 링크의 약 13%를 차지하고 있습니다. 도박 중독에 걸린 성인 인구가 0.6% 미만임에도 불구하고,[4] 도박 사이트는 악성코드 유포자들이 선호하는 표적이 되고 있습니다.
- 블로그/게시판의 악성코드는 지난 6개월간 7.6%로 감소했습니다.
- 기존의 웹 1.0 웹사이트인 개인 홈페이지의 점유율이 크게 줄었습니다. 주된 원인으로 개인 홈페이지가 소셜 네트워크나 비즈니스 네트워크의 프로필과 같은 웹 2.0 애플리케이션에 비해 유행에 뒤떨어진다는 점을 꼽을 수 있습니다.
- 검색 엔진, 웹 카탈로그, 포털 사이트의 악성코드는 5.1%로 감소하였습니다.

악성 링크가 하나 이상 포함된 상위 웹사이트 범주

2009년 상반기 ~ 2012년 상반기

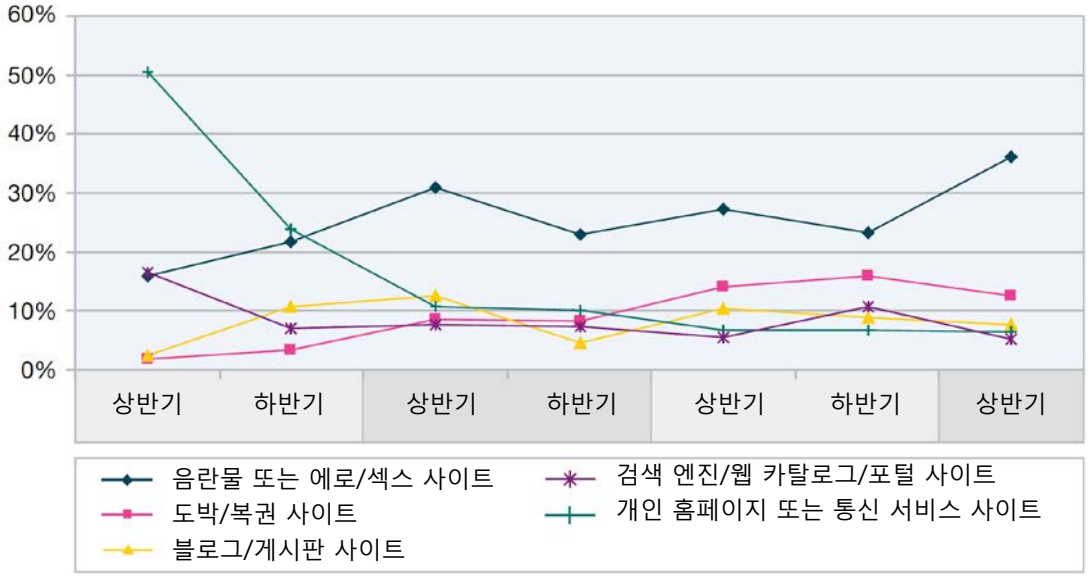


그림 21: 악성 URL이 가장 많이 운영되고 있는 국가 - 2006년 ~ 2012년 상반기

4 http://en.wikipedia.org/wiki/Gambling_addiction#Prevalence 참조

스팸과 피싱

IBM 스팸 및 URL 필터 데이터베이스는 전 세계 스팸 및 피싱 공격 현황 정보를 제공합니다. 수백만 개의 이메일 주소가 감시되는 와중에도 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 가량의 시그니처가 스팸 필터 데이터베이스에 신규 등록되거나 업데이트 또는 삭제되고 있으며, 업데이트는 5분 단위로 제공됩니다.

이 단원에서는 다음 주제를 살펴봅니다.

- 일정하게 낮은 수준을 유지하고 있는 스팸 양
- 지난 12개월 간의 주요 스팸 동향
- URL 스팸의 보편적인 최상위 도메인
- 스팸 발신 국가[5]의 동향
- 스패머의 주말 활동
- 2012년 7월의 Grum 봇넷 근절
- 이메일 사기와 피싱

일정하게 낮은 수준을 유지하고 있는 스팸 양

작년 봄과 여름에는 2009년 초와 스팸 수준이 동일하였습니다. 2011년 9월에 단기 증가가 있은 후, 스팸 양은 2011년 봄 수준으로 감소하였습니다. 2012년 상반기에는 큰 변화 없이, 스팸 양이 일정하게 낮은 수준을 유지하였습니다.

스팸 양의 변동
2008년 4월 ~ 2012년 6월

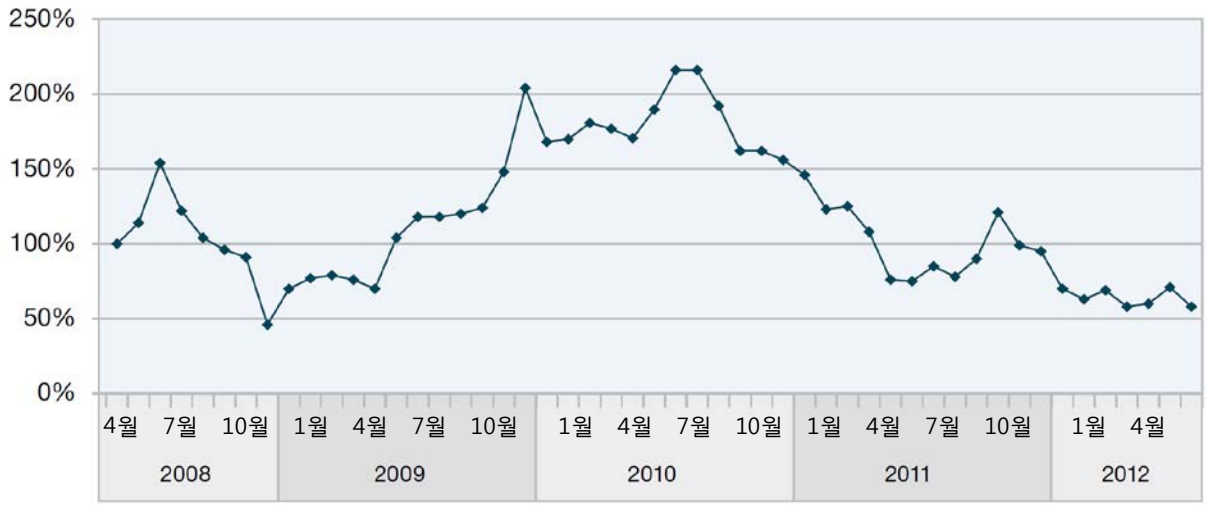


그림 23: 스팸 양의 변동 - 2008년 4월 ~ 2012년 6월

5 이 보고서의 스팸, 피싱, URL에 대한 통계는 http://ip-to-country.webhosting.info에서 입수할 수 있는 WebHosting.Info(http://www.webhosting.info)가 제공하는 IP-to-Country Database를 사용합니다. 지리적 분포는 컨텐츠 분포도의 경우 IP-to-Country Database에 호스트의 IP 주소를 요청하여 파악했으며 스팸 및 피싱의 경우 전송 메일 서버의 IP 주소를 요청하여 파악했습니다.

지난 12개월 간의 주요 스팸 동향

다음 차트에는 2011년 7월 이후 관찰된 스팸의 주요 동향이 세 가지 파라미터로 요약되어 있습니다.

- **이미지 스팸:** 2011년 말 이미지 기반의 스팸이 다시 모습을 드러냈습니다. 스패머들은 2012년 3월 말까지 이 유형의 스팸을 계속 사용하였습니다. 전체 스팸의 8% 이상에 이미지가 첨부되었던 적도 있습니다. 2011년 12월의 이미지 스팸과 비교해 보았을 때, 기술적인 변화는 없었습니다.
- **ZIP/RAR 스팸:** 2011년 하반기에는 몇 가지 ZIP/RAR 스팸이 발견되었습니다. 두 이미지 스팸과 ZIP/RAR 스팸은 IBM X-Force 동향 및 위험 보고서에서 상세하게 다룬 바 있습니다. 2012년 상반기에는 이런 종류의 위협이 전혀 없었습니다. 2012년 4월 이후에 다시 나타났지만, 그 수준은 훨씬 낮았습니다. 이러한 ZIP 또는 RAR 첨부 파일에 기술적으로 새로운 면은 없었습니다. ZIP/RAR 스팸이 1사분기의 이미지 스팸을 대체했다는 것은 분명합니다.

스팸의 평균 바이트 크기 대 이미지 및 ZIP/RAR 스팸의 비율
2011년 7월 ~ 2012년 6월 (주 단위)

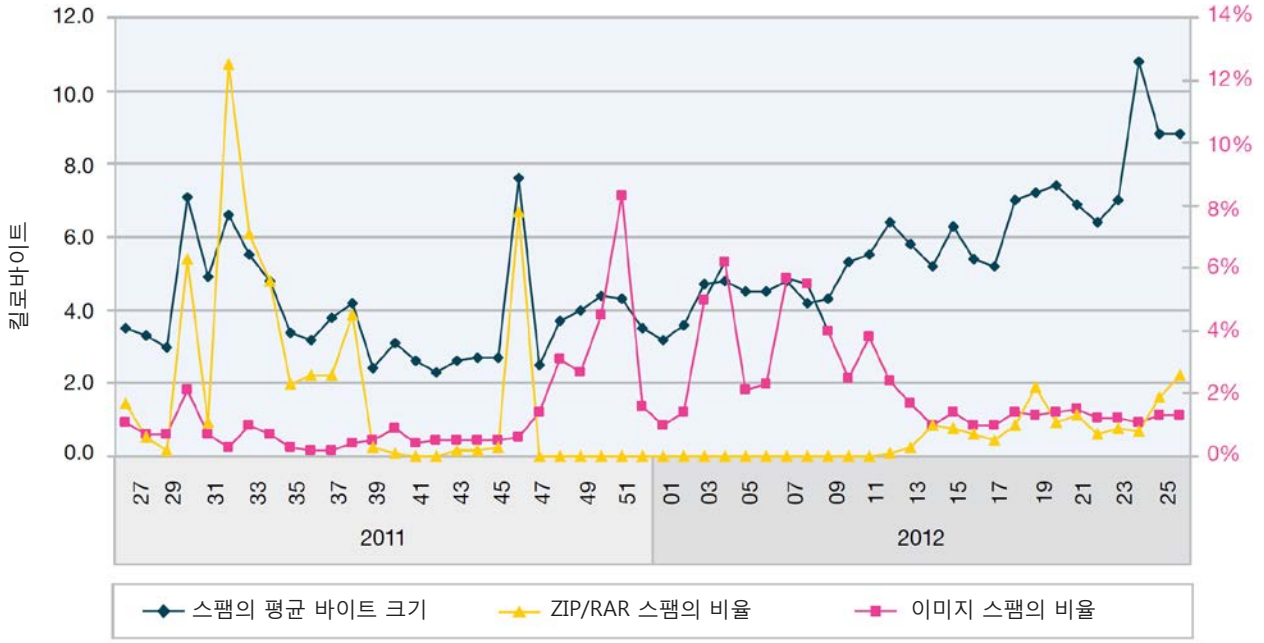
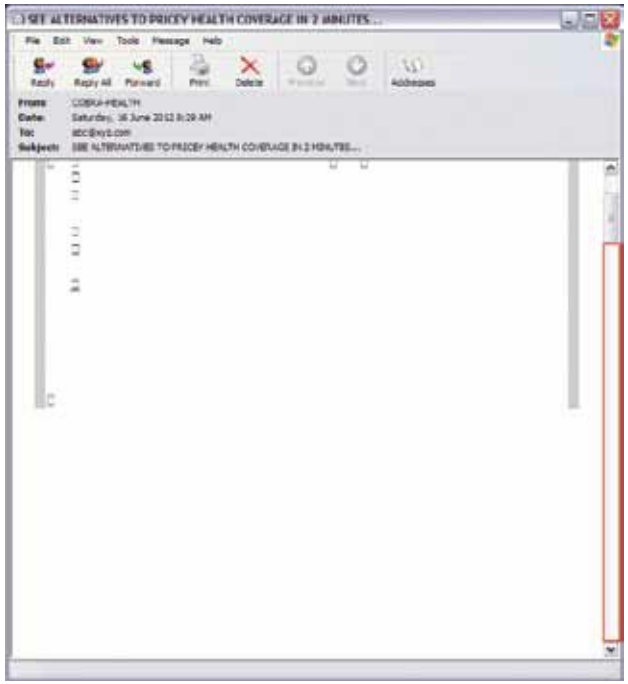
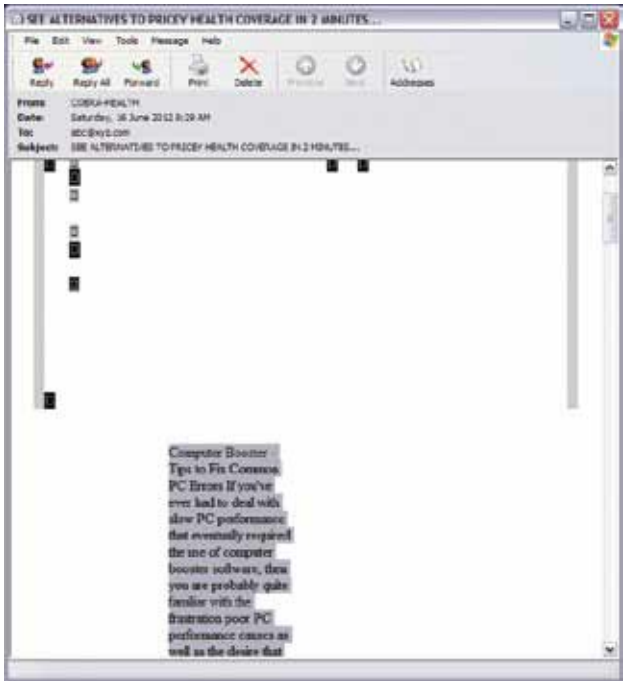


그림 24: 스팸의 평균 바이트 크기 대 이미지 및 ZIP/RAR 스팸의 비율 - 2011년 7월 ~ 2012년 6월, 주 단위

- **스팸의 평균 바이트 크기:** 2010년 중반 이후, 스팸의 평균 바이트 크기는 일반적으로 약 3 ~ 4 킬로바이트 정도였습니다. 그러나 2012년 초 이후에는 스팸의 크기가 지속적으로 증가하였습니다. 2012년 6월 중순에는, 스팸의 크기가 10 킬로바이트를 초과하였습니다. 스패머들은 혼동을 주고 스팸 필터를 우회하기 위해 웹사이트의 합법적인 컨텐츠를 스팸에 추가하였습니다.

오른 쪽의 예에서, 좌측은 사용자가 열었을 때 (이 시점에 이미지 다운로드 여부는 구성에 따라 달라집니다) 보게 되는 이메일을 보여줍니다. 스크롤 바에 엄청난 공간이 있다는 점에 유의해야 합니다. 동일한 이메일이 우측에 나와있지만, 사용자가 [Ctrl]+A[6]를 누르면 숨겨진 텍스트가 보이게 됩니다. 이 텍스트는 다음의 합법적인 웹사이트에서 복사되었습니다: http://ezinearticles.com/?Computer-Booster---Tips-to-Fix-Common-PC-Errors





6 [Ctrl]+A: Microsoft OS의 경우. Mac OS의 경우에는 [Command]+A를 사용.

컨텐츠 기반 스팸 필터(예: 베이지안 분류기 또는 텍스트 시그니처 기반 방식)는 대량의 합법적인 텍스트 때문에 이러한 유형의 스팸을 감지하지 못할 수도 있습니다. 최악의 경우에는 이러한 스팸이 스팸 필터에 추가되었을 대 오탐지 일치 사례가 너무 많아져 사용자가 스팸 필터를 꺼야만 할 수도 있습니다.

7월 초에는 크기가 700 Kb에 달하는 아주 큰 스팸 메시지가 나타나기 시작했습니다. 대부분의 사람들은 이 상당한 크기가 내장된 이미지나 악성코드 첨부파일 때문이라고 짐작하겠지만, 실제로는 그렇지 않습니다.

이러한 스팸에는 헤더가 아주 큰 HTML 부분이 있었습니다. 이 헤더는 여러 컨텐츠 관리 시스템(예: Joomla, Wordpress, Typo3 등)에서 복사된 CSS 명령어로 채워져 있었으며 이메일의 출력물에는 전혀 영향을 미치지 않았습니다.

스패머들이 이처럼 대역폭을 낭비한다는 것은 흥미로운 점입니다. 얼마 전만 하더라도, 스패머들은 최대한 발송량을 늘이기 위해 스팸을 작게 유지하려 했습니다. 비록 이 예가 극단적인 경우일지라도, 스팸이 점점 커지는 것이 일반적인 추세임을 확인할 수 있습니다.

그 이유는 무엇일까요?

- 최근의 봇넷 근절이 작은 크기의 스팸에 주력했던 스패머들에게 타격을 입혔습니다. 작은 스팸이 사라지면서, 크기가 큰 스팸이 눈에 더 잘 띄게 된 것입니다.
- 대다수 개인용 컴퓨터 및 모바일 디바이스의 인터넷 접속이 고속화되었기 때문에, 스패머들이 더 이상 대역폭에 신경 쓰지 않아도 됩니다.
- 스패머로서는 ISP, 법 집행 단체, IT 회사들에 의해 차단 당하지 않는 것이 더욱 중요해지고 있습니다. 따라서, 스팸 발송량을 줄이면서도 스팸이 스팸 필터를 통과할 수 있게 하는 것이 스패머에게 적절한 접근방식입니다. 일부 필터는 "크기 X" 이상인 메일을 스팸으로 감지하는 데 한계가 있을 것입니다.

최근에 나타난 또 다른 동향은 많이 쓰이는 스팸 제목 줄입니다.

우측의 표를 요약해보면,

- 2012년 1월: 스패머들은 제목이 없이 답장이거나 전달 이메일인 것처럼 "회신" 및 "전달"과 같은 무미건조한 제목 줄을 사용했습니다.
- 2012년 2월 및 3월: 채용 사기[7]가 가장 많이 쓰였습니다.
- 2012년 4월: 로맨스 사기가 많이 쓰였습니다.[8]
- 2012년 5월 및 6월: 의료 제품 및 패션 액세서리가 가장 많이 쓰였습니다.

한두 달 단위로 가장 많이 쓰이는 제목 줄의 주제가 바뀌고 있습니다. 이는 전반적인 스팸 양의 감소 추세에도 불구하고 스패머들이 여전히 신속하게 스팸의 유형을 변경할 수 있다는 것을 보여줍니다.

상위 3대 제목 줄	
2012년 1월	**%**
RE:	0.83%
Fw:	0.83%
Fw: Re:	0.58%
2012년 2월	**%**
취업 기회	1.76%
가상 비서 직	1.33%
관리 보조 직	1.32%
2012년 3월	**%**
취업 기회	1.04%
충원 – 온라인 접수	0.76%
채용 공고 – 세부사항 확인 요! 검색 엔진을 통해 전송	0.76%
2012년 4월	**%**
당신을 원해요	0.37%
진정한 미인	0.37%
실제 데이트	0.37%
2012년 5월	**%**
모조 샤넬 시계, 모조 신발, 가방, 모조 핸드백... 모조품 시계, 모조품 핸드백, 신발 전문	0.66%
정말 저렴한 가격으로 시알리스를 안전하게 온라인으로 구입하세요. 추가 증정, 할인 및 무료 배송 적용. 시알리스를 저렴하게 온라인으로 주문하세요	0.51%
미소녀	0.50%
2012년 6월	**%**
시알리스와 비아그라를 온라인으로 구입하세요!	2.01%
제목: 비아그라 할인	0.96%
FDA 승인을 득한 최고 품질의 저렴한 약품. 75,000명 이상의 고객이 믿고 거래하고 있습니다. Visa, Mastercard, AmEx, ACH 사용 가능	0.60%

표 3: 월별 상위 3대 스팸 제목 줄 – 2012년 상반기

7 http://en.wikipedia.org/wiki/Employment_scams 참조

8 http://en.wikipedia.org/wiki/Romance_scam 참조

URL 스팸의 보편적인 최상위 도메인

스패머들이 등록하는 최상위 도메인에 대한 선호도는 쉽게 파악할 수 있습니다.

- 지난 2년간, 선호도가 가장 높은 두 가지 최상위 도메인은 .com과 .ru(러시아의 최상위 도메인)였습니다.
- 확고부동한 2위 계층의 최상위 도메인은 .info 및 .net입니다.
- 약 1년 전에 새로 부상한 .ua(우크라이나)와 .pф(러시아의 국제화된 최상위 도메인)가 다수 스팸에서 발견되었습니다.

지난 몇 년 동안에는 영국, 네덜란드, 칠레 또는 오스트리아와 같은 국가 코드 최상위 도메인이 가장 많이 쓰이는 도메인에 포함되어 있었지만, 현재는 보기 드물며 자취를 감춘 것으로 보입니다. 이는 익명 프록시에 쓰이는 여러 최상위 도메인의 수에 관한 시장 조정이 이루어졌던 익명 프록시의 최상위 도메인과 유사하다고 볼 수 있습니다.

스팸 URL의 최상위 도메인 사용량
2010년 3사분기 ~ 2012년 2사분기

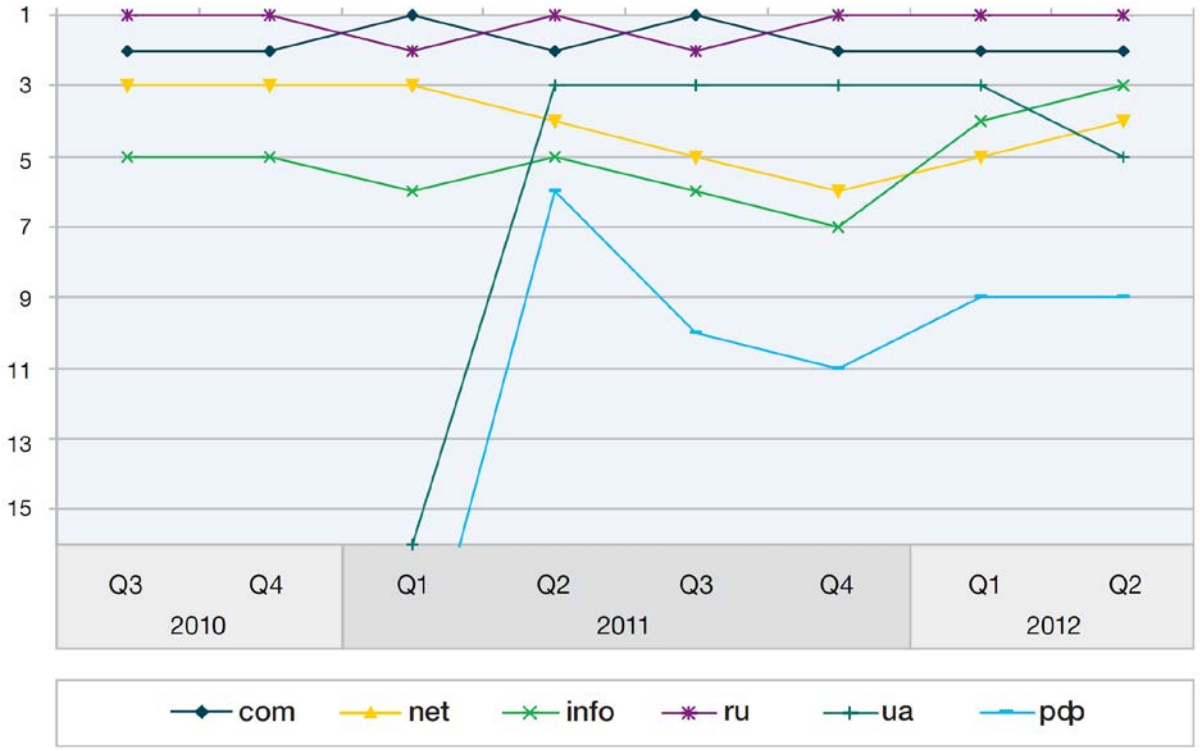


그림 25: 스팸 URL의 최상위 도메인 사용량 - 2010년 3사분기 ~ 2012년 2사분기

스팸 발송 국가 추세

지난 3년간 가장 많은 스팸이 발송된 국가를 살펴보면, 다음과 같은 흥미롭고도 장기적인 추세가 드러납니다.

- 인도의 스팸 발송률이 꾸준히 (2012년 1사분기에 한차례 대규모 감소) 증가하여 전체 스팸의 약 16%를 차지하면서, 가장 큰 부분을 차지하게 되었습니다. 이는 지난 12개월 동안 인도의 인터넷 사용자 수가 25% 증가했기 때문인 것으로 보입니다.[9] 한 국가가 전체 스팸의 약 16%를 차지한 사례는 이번이 처음입니다. 이전의 최고 기록 보유자는 2007년에 15%를 차지했던 미국이었습니다.
- 베트남은 4% ~ 10%를 오르내리고 있지만, 최상위 스팸 발송 국가 중의 하나로 자리잡은 듯 보입니다.
- 미국은 2010년 1위를 차지한 후, 2011년 봄에는 3% 미만으로 감소했습니다. 2012년 봄 이후 회복세를 보이고 있는 미국은 현재 8% 이상을 차지하고 있습니다.
- 브라질은 처음으로 6% 미만으로 감소했습니다.
- 호주는 처음으로 6%를 돌파했습니다.

2012년 2사분기에 나타나는 인도와 베트남의 하향세는 흥미롭습니다. 2011년 4사분기와 2012년 2사분기에 두 국가는 전세계 스팸의 약 25%를 차지했지만, 올해 초에는 14% 미만이었습니다. 이 당시 스패머들은 아르헨티나, 이탈리아, 루마니아 등의 다른 국가에서 제물을 찾았던 것이 분명해 보입니다. 이 세 국가의 2012년 1사분기 스팸 발송량은 전체 스팸의 10% 이상으로 강세를 보였습니다.

분기별 스팸 발송률
2009년 1사분기 ~ 2012년 2사분기

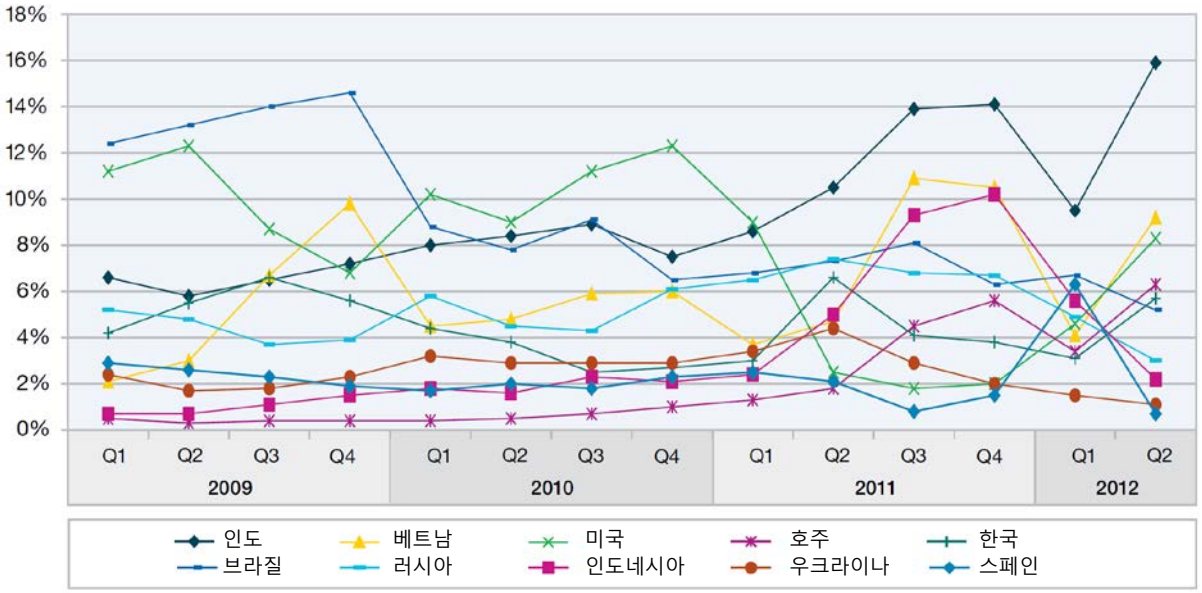


그림 25: 스팸 URL의 최상위 도메인 사용량 - 2010년 3사분기 ~ 2012년 2사분기

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

스패머의 주말 활동

스패머들이 월요일부터 일요일까지 매일 균등하게 스팸을 발송할 경우, 요일별 발송량은 주간 발송량의 14.3%가 되며, 따라서 주말(토요일과 일요일) 발송량은 28.6% 가 될 것입니다. IBM X-Force 2010년 동향 및 위험 보고서에서는 주말에 발송된 러시아어 스팸 양은 단 10%로 주중보다 훨씬 적은 것으로 나타났습니다. 2012년에는 상당한 변화가 있었습니다. 2012년 1사분기에는 14% 이상에 달하는 러시아어 스팸이 주말에 발송되었습니다. 동시에, 주말의 비러시아어 스팸 양은 약 22% 감소하였습니다.

그 이유는 다음과 같이 설명될 수 있습니다.

- 스팸 발송 과정을 자동화(작년에 봇넷을 이용하여 이미 완전히 자동화되었음)하는 러시아 스패머들이 점차 늘어나고 있으며 새로운 위협을 꾸준히 자동화하고 있습니다.
- 안티스팸 솔루션 공급업체의 직원들도 주말에는 쉬기 때문에, 러시아 스패머들이 스팸 필터를 우회할 가능성이 주중보다 더 높다고 여기는 것으로 보입니다.
- 동시에, 비러시아 스패머들은 대다수 사용자들이 월요일 아침에 맨 먼저 우편함을 비워 주말에 발송된 스팸을 삭제하므로, 주중의 스팸 공격 확률이 높다고 추정할 수 있습니다.
- 현재 스패머들이 사용하는 스팸 발송 방법이 예전보다 감소한 것으로 보아, 통합과 도태가 있었을 수 있습니다. 이는 지난 2년 간의 스팸 양 감소와 일치합니다.

러시아 및 비러시아 스패머들의 주말 활동이 앞으로도 지속적으로 수렴하게 될지를 지켜보는 것도 흥미로울 것입니다.

주말에 발송된 러시아 스팸 및 비러시아 스팸의 비율
2009년 상반기 ~ 2012년 상반기

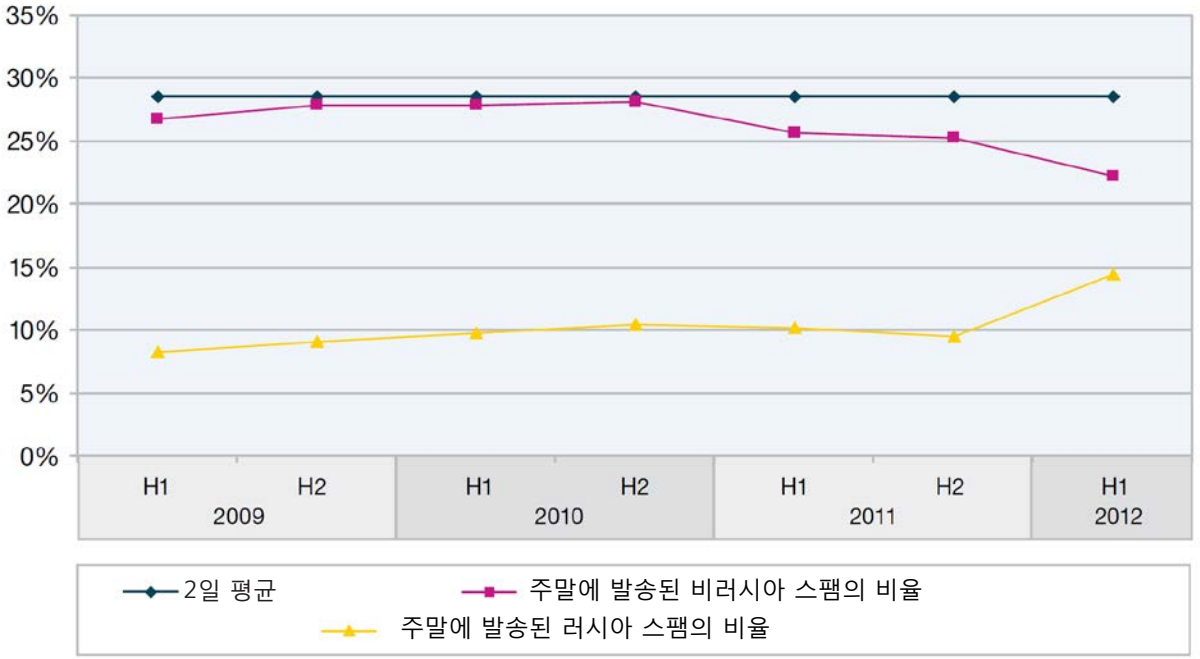


그림 27: 주말에 발송된 러시아 스팸 및 비러시아 스팸의 비율 - 2009년 상반기 ~ 2012년 상반기

2012년 7월의 Grum 봇넷 근절

2012년 7월 18일, Grum 봇넷이 근절되었습니다.[10] 이로 인해 연간 스팸 양이 감소되었습니다.

Grum 봇넷이 근절된 주에는, 2012년 1사분기에 측정된 스팸 수준의 60% 미만이었습니다.

스팸 양
2012년 4~7월

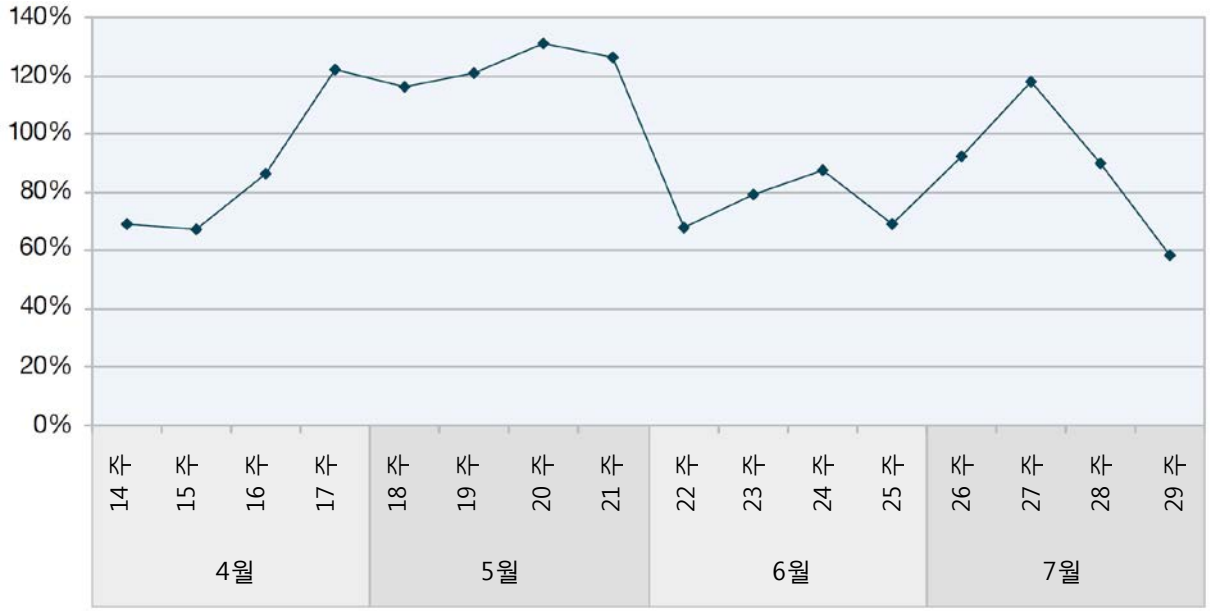


그림 28: 스팸 양 – 2012년 4~7월

10 http://en.wikipedia.org/wiki/Grum_botnet and http://blog.fireeye.com/research/2012/07/grum-botnet-no-longer-safe-havens.html 참조

봇넷 근절 전과 후의 스팸 발송 국가를 살펴본 결과, 흥미로운 추세가 드러났습니다.

- Grum 봇넷은 인도, 사우디아라비아, 터키, 영국 등의 감염된 컴퓨터를 회피했던 것으로 보입니다. Grum 봇넷이 근절되기 전에는 이 네 국가가 전세계 스팸 양의 36.5%를 차지했지만, 근절 후에는 49.6%를 차지했다는 점에서 이러한 추정이 가정합니다.
- Grum은 미국, 베트남, 호주, 독일, 브라질의 컴퓨터의 감염을 목표로 삼았습니다. 근절되기 전에는 이 국가들이 전세계 스팸의 29.9%를 발송했지만, 그 후에는 22.5%에 지나지 않았습니다.

인도가 봇넷 비활성화의 영향을 받았던 적은 이번이 처음이 아닙니다. Rustock[11] 봇넷이 2010년 크리스마스 연휴에 처음으로 차단되었을 때, 인도의 비율이 전세계 스팸 양의 7.1%에서 11.4%로 증가했습니다.[12]

Grum 봇넷 근절 전후의 스팸 발송 국가
2012년 7월 12일 ~ 2012년 7월 25일

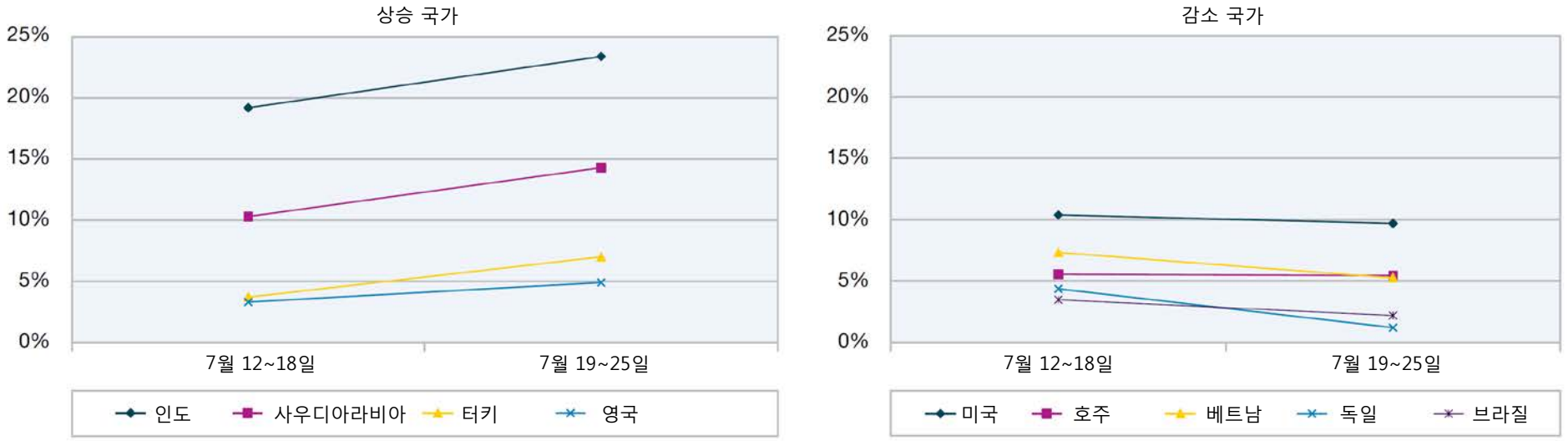


그림 29: Grum 봇넷 근절 전후의 스팸 발송 국가 - 2012년 7월 12일 ~ 2012년 7월 25일

11 http://en.wikipedia.org/wiki/Rustock 참조
12 http://blogs.iss.net/archive/2011spambotdecline.html 참조

이메일 사기와 피싱

수법

사기와 피싱의 최신 동향을 규정하기 위해:

- 통계 결과는 이메일을 사용한 사기와 피싱에만 기초하고 있습니다.
- 통계에는 사용자들이 첨부 파일이나 링크가 피싱과 무관하더라도, 파일이나 링크를 클릭하도록 유명 브랜드를 사용한 모든 이메일이 포함되어 있습니다. 따라서, 포함된 이메일의 일부는 "피싱과 유사한" 이메일에 지나지 않습니다.
- 통계에는 다운로드 및 키 입력 기록으로 드라이브를 통해 제공된 악성코드와 같이 이메일과 무관한 피싱 시도는 포함되어 있지 않습니다.

사기 수법과 피싱 통계에 관한 자세한 정보는 연간 IBM X-Force 2011년 동향 및 위험 보고서의 해당 단원에 제공되어 있습니다.

이메일 사기 및 피싱의 최근 추세

전술한 수법을 고려해 보면, 2008년 상반기와 2012년 상반기의 스팸 양과 이메일 사기 및 피싱 양 사이에는 다소 상당한 차이가 있다는 것을 알 수 있습니다 (2008년 상반기 = 스팸과 사기/피싱 모두에 대한 100% 기준).

- 2008 ~ 2010년 사이에, 스팸 양이 거의 2배로 증가했습니다.
- 2008 ~ 2010년 사이에, 이메일 사기/피싱 양은 2008년 수준의 20% 미만으로 현저히 감소했습니다.
- 2010 ~ 2012년 사이에는, 스팸 양이 2010년 수준의 약 1/3로 감소했습니다.
- 2010 ~ 2012년 사이에 이메일 사기/피싱 양이 거의 4배로 증가하여, 2012년 봄에는 2008년 수준의 83% 이상에 달했습니다.

결론적으로, 스팸 양과 사기 및 피싱 양은 정반대로 움직였습니다.

스팸 양 대 사기/피싱 양
2008년 상반기 ~ 2012년 상반기

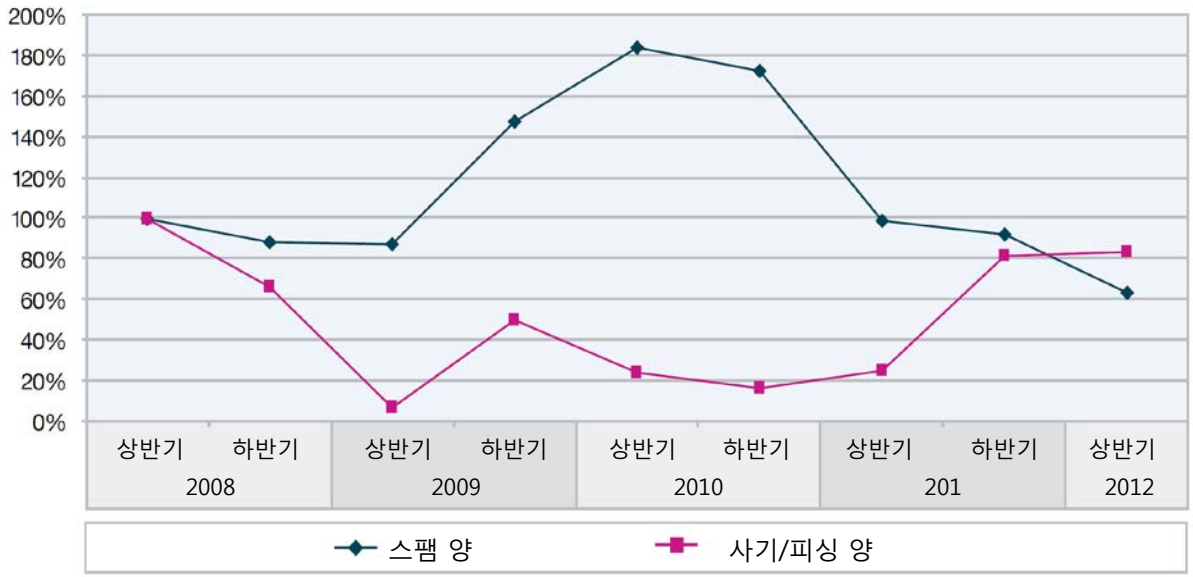


그림 30: 스팸 양 대 사기/피싱 양 - 2008년 상반기 ~ 2012년 상반기

이메일 사기와 피싱의 유형을 살펴보면, 다소 흥미로운 추세가 드러납니다.

- 2009년까지, 금융 기관을 겨냥한 기존 이메일 피싱이 전체 피싱 이메일의 50% 이상을 차지하면서, 통계의 주를 이루었습니다. 2010년 초 이후에는 하위권으로 밀려났습니다.
- IBM이 이 종류의 이메일을 감시하기 시작했던 2010년 초 이후에는, 소셜 네트워크가 2위권 내에 머물면서 통계에서 높은 순위를 차지 했습니다. 2011년 초 소셜 네트워크의 이메일에 사용된 합법적인 브랜드 명칭이 80% 이상을 차지했다가, 2011년 하반기에는 43%로 일정한 수준을 유지했습니다. 2012년 초의 일시적인 하락세 이후에는, 전체 사기 및 피싱의 31% 이상을 차지하고 있습니다.
- 2010년 하반기에는 사용자를 속이기 위해 택배 서비스를 많이 사용했으며, 이 기간 중 이러한 유형은 전체 사기/피싱 유사 이메일의 약 20%에 달했습니다. 2011년 하반기에는 이 스팸 유형의 50% 이상이 유명 택배 업체의 이름을 사용했습니다. 이 유형이 2011년 말과 2012년 초에 거의 자취를 감추었지만, 2012년 2사분기에는 전체 사기/피싱 양의 27% 이상에 달했습니다.
- 2012년 초, 피싱 공격자들은 비영리 기관에 초점을 맞추어 1사분기 전체 사기 및 피싱의 66%를 차지했다가, 2012년 2사분기에는 7%로 감소하였습니다.
- 악성코드 파일이 첨부된 스캐너 사기(예: "Scan from your printer #6269319")가 전체 사기 및 피싱의 13% 이상을 차지하면서, 처음으로 2사분기에 상위 3위권에 진입하였습니다.

산업별 사기/피싱 대상

2009년 1사분기 ~ 2012년 2사분기

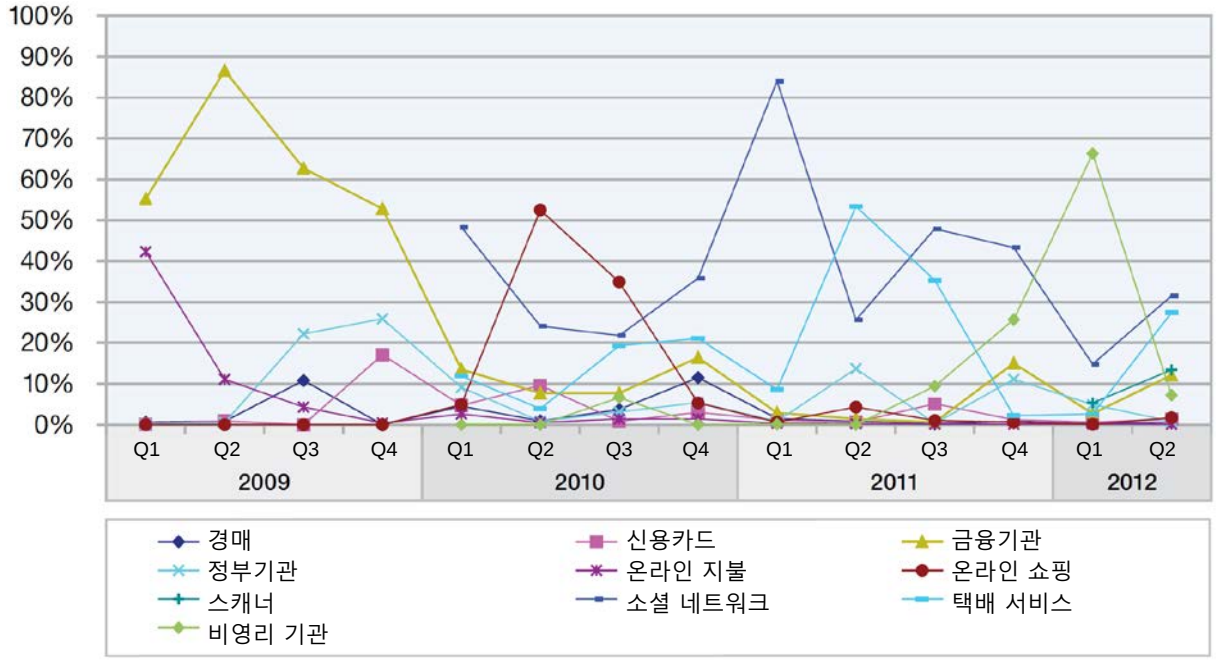


그림 31: 산업별 사기/피싱 대상 - 2009년 1사분기 ~ 2012년 2사분기[13]

13 소셜 네트워크, 택배 서비스, 비영리 기관에 관한 수치는 2010년 초 이전에는 기록이 없음.

앞 차트의 등락을 살펴보면, 피싱 공격자들이 다음 대상의 사용자들로 하여금 링크나 첨부파일을 클릭하도록 반복적으로 공략하고 있다는 것을 알 수 있습니다. 수법은 동일하지만, 대상이 다릅니다.

매번 새로운 스팸이 되풀이되면서 공격자들은 속임수에 넘어올만한 새로운 제물(즉, 새로운 인터넷 사용자)을 찾습니다.

어느 국가에서 피싱 유사 이메일이 발송되는지 지켜보는 것도 흥미로울 것입니다.

그림 32: 사기/피싱 발송자의 지리적 분포 – 2012년 상반기

국가	피싱 비율
스페인	7.6%
루마니아	7.4%
영국	6.4%
독일	5.5%
브라질	5.0%

국가	피싱 비율
인도	4.9%
폴란드	4.8%
프랑스	4.4%
미국	3.8%
포르투갈	2.5%

표 4: 상위 10대 사기/피싱 발송 국가 – 2012년 상반기

소셜 네트워크는 2년 넘게 이메일 피싱의 주요 표적이 되어 왔습니다. 마지막으로 이 유형의 이메일 피싱이 발송된 국가를 살펴보겠습니다.

미국에서 발송되는 메시지는 전체 소셜 네트워크 사기/피싱의 약 15%를 차지하고 있습니다. 그 다음이 전체 소셜 네트워크 피싱의 약 8%를 차지하고 있는 프랑스입니다. 이 국가 분포는 전체 사기/피싱 국가 분포와는 상당한 차이가 있으며, 이 유형의 피싱은 다른 유형의 스팸 및 피싱과는 다른 봇넷에서 비롯됩니다.

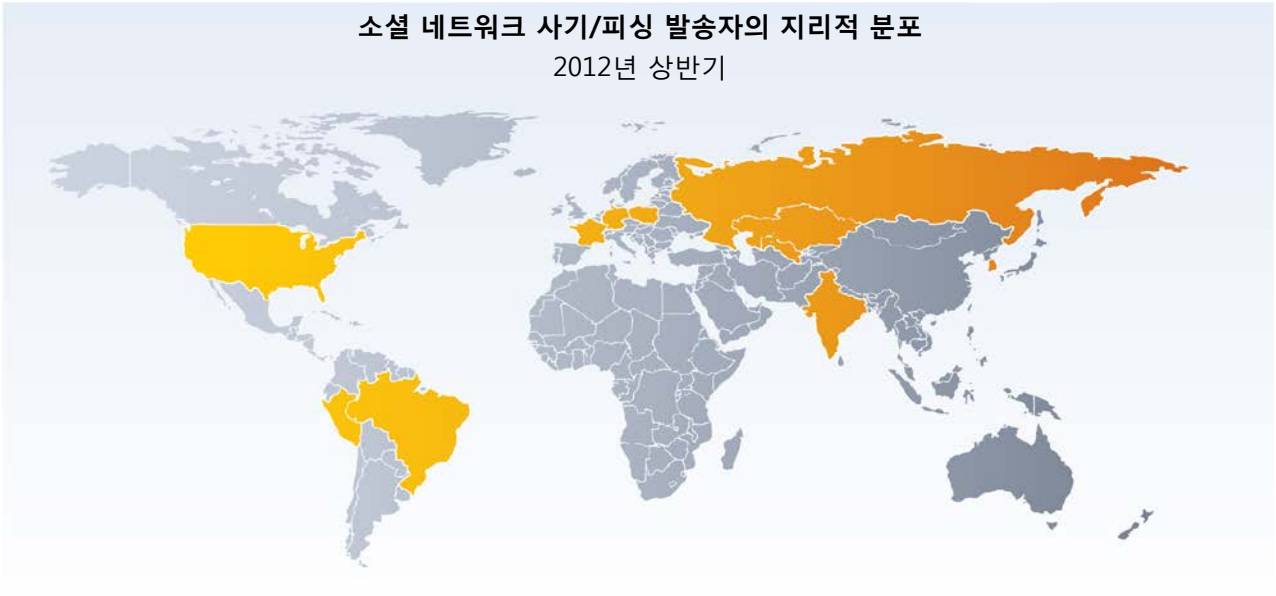


그림 33: 소셜 네트워크 사기/피싱 발송자의 지리적 분포 – 2012년 상반기

국가	피싱 비율
미국	14.7%
프랑스	7.9%
브라질	6.0%
독일	5.3%
한국	4.5%

국가	피싱 비율
러시아	4.0%
폴란드	3.5%
인도	3.3%
페루	3.2%
카자흐스탄	3.0%

표 5: 상위 10대 소셜 네트워크 사기/피상 발송 국가 – 2012년 상반기

단원 II
운영 보안 현황

이 단원에서는 오늘날 공격자들이 노리는 프로세스, 소프트웨어, 인프라의 약점과 관련된 주제를 살펴봅니다. 구체적으로 말해서, 이 단원에서는 보안 규정 준수 모범 사례, 운영비 절감 아이디어, 인텔리전스 및 자동화를 통한 소유 비용 절감과 업무, 제품 및 역할 통합에 대해 논의합니다. 또한 이러한 문제를 관리하거나 최소화하는 과정에서 IBM이 얻은 정보도 소개합니다.

보안 정보 및 이상징후 감지를 이용한 APT(Advanced Persistent Threat) 차단

APT(Advanced Persistent Threat)는 업계에서 가장 빈번하게 논의되는 주제 중 하나가 되었습니다. 모든 보안 공격이 APT로 인한 것이 아님은 분명하며, 사실 거의 대다수가 여기에 해당되지 않습니다. 하지만 숙련된 공격자들이 조직이나 개인을 겨냥한 수법이나 악성코드를 통해 장기적인 공격을 행하는 데서 일부 적용될 수 있음은 명백합니다.

APT가 기업에 미치는 영향은 상당합니다. IBM X-Force 2011년 동향 및 위험 보고서에 나와있듯이, IBM X-Force가 2011년을 "보안 침해의 해"로 선언할 정도로 전세계의 기업 다수가 APT로 인한 심각한 공격을 받았습니다. 2011년 초와 그 이전에, RSA, Google 등과 같은 대형 기업들이 고객 및 사용자 데이터와 기밀 지적재산권이 노출되는 광범위한 피해를 입었습니다.

미국에 본사를 둔 대기업의 보안 전문가를 대상으로 최근에 실시한 Enterprise Strategy Group의 조사에서는 59%의 응답자들이 자사가 APT 공격 대상이 되었을 "가능성이 매우 높다"거나 "가능성이 있다"고 응답했습니다. 아울러, 30%는 자사가 향후 APT 공격에 "매우 취약"하거나 "취약"하다고 여기는 것으로 나타났습니다. 심지어 "APT에 만반의 준비가 되어 있다"고 응답한 기업 중에서도, 46%가 향후 APT 공격에 "매우 취약"하거나 "취약"하다고 여기는 것으로 나타났습니다.[14]

관건은 직원들에 대해 잘 파악하고 있으며 풍부한 자금력을 갖추었으며 끈질기게 공격을 행하는 교활한 공격자로부터 회사를 보호할 수 있는 방법입니다. 공격자들이 언젠가는 방어막을 뚫을 수 있을 것이므로, 전적으로 예방 수단에만 의존할 수는 없습니다. 그러한 공격은 시그니처 기반 감지 기술도 회피할 수 있기 때문에 이러한 기술에만 의존해서도 안됩니다. 기업 보안에는 예방 및 시그니처 기반 감지가 모두 필요하고 더 많은 예방 수단이 요구되며, 새로운 전략을 채택해야 합니다. 이상징후 감지 기능이 포함된 SI(Security Intelligence) 접근방식은 기존의 솔루션을 보완하고 APT의 방어에도 도움을 주고 있습니다.

APT(Advanced Persistent Threat)에 대한 이해

이 용어의 정의에 대한 의견이 분분하지만, APT에는 지향적이며 특정 대상을 겨냥한 시도, 지속적이며 잠재적으로 장기간의 공격, "지능적인" 기술(기술/운영의 정교함의 관점에서)이라는 개념이 포함되어 있다는 것이 공통적인 견해입니다. 비록 다수의 경연진과 정보 보안 책임자들이 APT의 존재를 인정하고 있지만, 자사가 대상일 수 있음을 의심하는 경우는 극소수에 지나지 않습니다. *정부 기관이나 Fortune 500대 기업이 아닌 이상, 사실상 누군가가 이런 방식으로 공격을 시도할 이유가 있겠느냐고 생각합니다.*

14 "미국 APT 분석," Enterprise Strategy Group, 2011년 10월

유감스럽게도 답은 "있다"입니다. 널리 확산된 APT에 관한 최근 논문에 의하면, 공격자들이 건설 및 중공업 회사, 부동산 회사는 물론, 아무도 APT 공격 대상 가능성이 높다고 여기지 않았던 국가 올림픽 조직 위원회를 포함한 72개 조직이 피해를 입었습니다.[15] 따라서, 다수 기업들이 이미 공격 대상으로써 탐색이나 공격을 당하고 있다는 최악의 경우를 가정해야 합니다.

실제 APT 시나리오에서는, 공격자가 결국에는 방어망을 뚫을 수 있다는 점도 가정해야 합니다. 그 이유는 다음과 같습니다.

1. 모든 진입점의 보안을 유지하는 것이 본질적으로 어렵습니다. 여기에는 취약점이 발견될 때마다 모든 자원의 패치와 보호, 보안 구성을 확보하는 것이 포함됩니다.
2. 계정 도용으로 이어지거나 보호 기능을 무력화시킬 수 있는 사회공학 기반의 공격은 차단하기 어렵습니다.

또는, 어느 분석가가 최근에 파악한 다음 이유 때문입니다.

"대부분의 대기업 보안 관리자와 CISO는 자신의 **조직이 침입을 당할 것이냐가 문제가 아니라, 침입을 당할 경우 전체 조직이 매우 곤란한 상황에 처할 수 있다는 것**이 문제임을 인식하고 있습니다. … 한 가지 분명한 점은 은밀한 공격자가 기업 네트워크와 엔드포인트에 오래 숨어 있을수록, 더 심각한 피해를 입을 수 있습니다." (강조는 IBM이 추가하였습니다.)[16]

지능적인 공격에 채택된 수법과 악용된 취약점을 알아보기 위해, 몇 가지 예를 살펴보기로 하겠습니다. 교활하며 기술적으로 진보한 이 몇몇 조치가 있으며, 이러한 조치들이 통합됨으로써 개개의 합보다 더 큰 효과를 냅니다. 수 개월에 걸친 조사와 개인화를 반영하는, 세밀하게 구성된 수법(아래에 열거된 예와 같이)의 조합은 APT의 차단을 어렵게 만듭니다. 다양한 공격에서 추려 본 예는 다음과 같습니다.

- **신뢰할 수 있는 파트너를 통한 침투.** 어느 경우에는, 공격자가 대상이 신뢰하는 제3자 소프트웨어 공급업체에 침입하여 소프트웨어 업데이트 서버에 트로이 코드를 주입한 다음, 소프트웨어 공급업체가 대상의 네트워크에 트로이 코드를 자동 업데이트할 때까지 기다립니다.
- **맞춤형 악성코드 개발.** 전형적인 APT인 이전 사례의 트로이 코드가 소프트웨어 공급업체의 다른 고객을 제외한 대상 기업만을 감염시키도록 수정되었으며, 따라서 악성코드가 확산되지 않았고 안티바이러스 솔루션 공급업체에 파악 당하기 전에 목적을 달성할 수 있습니다.
- **조사 및 사회공학 수법을 이용한 사용자 계정 도용.** 인내심 있고 끈질긴 공격자는 스피어 피싱 대상에 대한 광범위한 조사를 실시한 다음, 개인의 업무 활동, 동료, 친구, 가족 등에 대한 지식을 반영한 신뢰도가 높은 통신(이메일, IM 또는 소셜 네트워킹 메시지)을 통해 대상과 접촉합니다. 피싱 메시지에는 대상 시스템을 감염시키는 링크나 첨부파일이 종종 맞춤형 악성코드와 함께 들어있습니다.

15 "출현: Operation Shady Rat," McAfee, 2011년

16 블로그 포스트: "맞아요, 침입은 불가피해요: 이젠 어떡해야 하나요?" Paula Musich, Current Analysis, 2012년 7월 20일, http://itcblogs.currentanalysis.com/2012/07/20/okay-breaches-are-inevitable-so-now-what-do-we-do/

- **제로 데이(zero-day) 취약점 공격.** 대상을 침입하기 위한 사회공학적인 수법(과 피해 범위의 확대에 쓰이는 수법)에 대한 대체 접근방식은 제로 데이 공격을 이용하여 사용자 및 관리자 계정에 대한 접근권한을 확보하는 것입니다. 일반 시장과 블랙 마켓에 제로 데이 공격과 지능적인 배포 기술이 넘쳐남에 따라, 공격자들은 제로 데이 취약점을 찾거나 그 취약점을 공격하기 위해 공을 들이지 않아도 됩니다. 요컨대, 이러한 시장을 이용하는 것이 실리적일 뿐만 아니라 경제적입니다.
- **은닉 채널을 통한 통신.** 공격자들은 종종 악성코드를 이용하여 시스템을 봇넷에 흡수시킨 다음, 봇넷 명령어를 전송하여 80 또는 8080 포트와 같은 은닉 채널 상에서 서버를 제어합니다. 이 접근방식은 대상 기업에서 데이터를 몰래 유출할 때에도 사용할 수 있습니다.

이러한 APT는 단시일 내에 대상의 외부로부터 침입할 가능성이 높기 때문에, 효과적인 감지 및 포렌식 기능이 필수적입니다. 보호 및 예방 활동도 게을리하지 않아야 하겠지만, 기업이 APT를 차단할 수 있는 진정한 수단은 침입을 신속하게 감지하여 침입의 범위와 영향을 철저하게 조사할 수 있는 능력입니다.

SI(Security Intelligence): APT를 차단할 수 있는 유일한 대비책

IBM X-Force 2011년 동향 및 위험 보고서에 소개된 SI는 보안 운영 전반에 대한 통합된 가시성과 실시간 분석을 제공하는 새로운 종류의 솔루션입니다.

> SI(Security Intelligence)는 IT 보안 및 기업의 위험 노출에 영향을 미치는 사용자, 애플리케이션, 인프라가 생성하는 데이터를 실시간으로 수집하여 정규화하고 분석합니다.
>
> SI 솔루션에 수집되어 저장되는 데이터로는 로그, 이벤트, 네트워크 흐름, 사용자 ID 및 활동, 자산 프로파일 및 위치, 취약점, 자산 구성, 외부 위협 데이터 등이 있습니다.

다음과 같은 SI의 여러 가지 요소는 APT(Advanced Persistent Threat) 차단에 도움이 되는 적합한 접근방식이 됩니다.

- **전방위적 시각을 제공하기 위해 고립된 데이터의 통합**. SI는 일련의 다양한 데이터를 분석하기 때문에, 무관해 보이거나 유해하지 않게 보이는 활동의 단편적 사실에서 결론을 도출해낼 수 있으며 궁극적으로 APT 감지를 위한 통찰력을 제공합니다.
- **공격 전후에 대한 통찰력.** SI를 사용하면 침입 예방을 위해 조치해야 할 기존의 보안 결함(침입 예방에 유용)과 네트워크 내에서 이미 발생한 의심스런 행위(침입 탐지에 유용)에 관한 정보를 수집하고 우선순위를 부여할 수 있습니다.
- **이상징후 탐지 기능.** 현재 활동을 기준으로 하여 정상에서 벗어난 행위를 파악하고 그 행위가 의미 있는지를 판단하는 것이 SI의 핵심 기능입니다. 이는 진행 중인 APT의 탐지에 매우 중요할 수 있습니다.
- **실시간 상관 및 분석.** SI 솔루션은 고급 분석 방법과 특정 목적을 위한 데이터베이스를 이용하여 방대한 양의 데이터를 실시간으로 연관시킬 수 있습니다. 따라서 APT의 정확한 조기 탐지가 가능하며, 잡음에서 나오는 신호를 구분하는 데 도움이 됩니다.
- **오탐지(false positive) 절감에 유용.** 이 모든 분석 방식의 조합을 통해, SI는 침입의 조기 탐지뿐만이 아니라 비정상적이지만 유해하지 않은 활동의 우선순위를 낮추는 데 도움이 될 수 있습니다. 비정상적이지만 유해하지 않은 활동의 조사에 소비되는 시간을 줄이면 기업이 가장 중요한 목표에 주력할 수 있게 됩니다.

- **포렌식 기능.** 침입을 탐지한 다음에 행해야 할 중요한 조치는 침입의 영향을 철저하게 조사하는 것입니다. SI는 수천 대에 달하는 시스템과 자원에 대한 로그 데이터, 네트워크 트래픽과 기타 원격으로 측정한 보안 지표들을 단일 콘솔로 보여줄 수 있으므로, 신속하게 침입을 평가해야 하는 보안 및 네트워크 직원들의 부담을 덜어 줍니다.
- **유연성**. 내부 IT 환경과 외부 위협 여건이 급변할 수 있기 때문에, APT 차단 접근방식은 잦은 변경을 지원해야 합니다. 최신 SI 솔루션은 일반적으로 데이터 소스의 추가, 분석의 생성 및 조정, 새로운 사용자 보기 및 보고서 작성, 전반적인 배치 아키텍처의 확장과 전개가 용이합니다.
- **통합 접근방식**. APT는 일반적으로 수백 대에 달하지는 않겠지만, 수십 대의 대상 시스템을 항상 포함하는 복잡하며 다각적인 공격입니다. 일부 SI 솔루션은 통합 모듈식 플랫폼으로 제공되기 때문에, 기업이 대량의 데이터를 지능적으로 처리하기 위해 다른 접근방식에 비해 훨씬 광범위한 분석과 임시 쿼리를 수행하는 데 도움이 될 수 있습니다.

SI는 일련의 다양한 보안 관련 데이터를 연관시켜 분석합니다

이상징후 탐지: SI(Security Intelligence)의 핵심적인 APT 차단 활동

SI가 제공하는 APT 차단에 가장 유용한 수단이 필시 이상징후 탐지일 것입니다. 지능적인 공격자는 흔히 제로 데이 공격을 결합한 교활하고 특정 대상을 겨냥한 공격 전략을 취하기 때문에, 기존의 시그니처 기반 방어 수단으로는 충분하지 않습니다. 조금이라도 의심스러운 활동을 탐지해 내고 전후 관계에서 최대한 그 활동에 관한 정보를 축적하여 실제 위협과 유해하지 않은 이상징후를 구분할 수 있는 능력이 필요합니다.

APT 공격은 전혀 눈치챌 수 없이 이루어지며, 대상 환경에 최대한 융화됩니다. 엄격하고 자동화된 지속적인 모니터링(과 최대한의 데이터 활용)이 이루어져야만 막대한 피해를 입기 전에 공격을 발견할 수 있습니다.

지금의 SI 솔루션에서 볼 수 있는 이상징후 탐지 기술은 네트워크 동작 이상징후 탐지(NBAD) 분야에 기반을 두고 있습니다.

하지만 SI 솔루션은 기존의 NBAD를 능가하는 기능을 확장하여, 이제는 네트워크 흐름(네트워크 트래픽) 분석 외에도 로그 데이터 분석을 지원합니다. SI의 통합 접근방식을 이용하면, 보안 팀은 네트워크 흐름과 로그 데이터에 관한 분석을 동시에 수행하여, 잠재적 위협에 대한 통찰력을 제고하고 상황 인식을 향상시킬 수 있습니다.

이상징후 탐지는 "정상" 동작을 벗어난 활동의 감시로 이루어집니다. 관심 측면에 대하여 활동의 기준선을 정한 다음, 적절하게 경고를 트리거합니다. 학습 기간과 트리거 기간을 모두 쉽게 조정할 수 있고, 계절적 변동과 증가 추세를 고려할 수 있어야 가장 바람직합니다.

SI가 검출할 수 있는 다양한 이상징후의 예는 다음과 같습니다.

- 아웃바운드 트래픽이 회사가 사업을 운영하지 않으며 트랙픽이 전송되지 않아야 할 국가로 전송됩니다.
- 기지의 애플리케이션(예: IRC 대화)이 비표준 포트(예: 포트 80)를 사용중입니다.
- FTP 트래픽이 전혀 없었던 재무 부서에서 FTP 트래픽이 관찰됩니다.
- 자가 전파 웜의 급증이 발생합니다.
- 기지의 호스트 상에서 잠재적으로 침입을 나타내는 새로운 서비스가 개시됩니다.
- 호스트 시스템의 역할이 변경됩니다. 일례로, 외부 대상 DNS 서버가 SMTP 릴레이로 변경됩니다.
- 네트워크 트래픽 양이 변합니다. 지난 24시간 동안의 특정 호스트에 대한 트래픽 양이 지난 3개월 간의 이력 평균에 비해 200% 이상이며, 증가를 설명할만한 명확한 계절적 요인이 없습니다.

요컨대, 이상징후 탐지는 APT 침입을 발견할 수 있는 지능적인 토대를 제공합니다. 공격이 어떤 형태일지에 대한 고급 지식은 필요하지 않으며, 주목할 만한 이상 동작에 대하여 네트워크 전반을 자동으로 감시할 수 있습니다.

이상징후 탐지의 모범 사례

APT로부터 보호하기 위해 이상징후 탐지 기능을 구축할 때, 다음과 같은 모범 사례가 권장됩니다.

- 사용자 활동, 특히 특권 사용자의 활동을 감시합니다. 대부분의 지능적인 공격에 쓰이는 주된 수법 중의 한 가지는 특히 특권 접근 권한을 가진 직원의 계정을 가로채는 것입니다. 계정을 가로챈 후에 공격자는 직원이 전에 사용한 적이 없는 애플리케이션이나 시스템에 접근을 시도하거나 비정상적인 시간 중에 자원 접근을 시도할 수 있습니다. 직원들의 정상 활동을 위한 지능적인 솔루션을 개발할 수 있다면, 비정상적인 동작을 유효하게 탐지할 수 있을 것입니다.
- 기밀 데이터에 대한 접근을 감시합니다. 마찬가지로, 공격자에게 가장 유용할 수 있는 데이터(고객 데이터, 재무 데이터, 지적 재산권 등) 보호에 주안점을 둡니다. 기밀 데이터베이스 및 기타 데이터 저장소와 관련된 일반적인 활동에 대한 인텔리전스를 개발하면, 의미 있는 불법 행위를 탐지할 수 있습니다. 데이터베이스 보안 솔루션은 이상징후 탐지에 유용한 원격 보안 지표도 제공할 수 있습니다. 사용자 활동 모니터링과 데이터 접근 모니터링을 결합하면 한층 더 정확한 위협 탐지가 가능해집니다.
- 아웃바운드 트래픽을 감시하여 데이터 유출을 예방합니다. 아웃바운드 트래픽의 감시를 강화하면 기밀 데이터의 유출을 탐지하여 차단할 수 있습니다. 거래가 없는 비정상적인 국가로 트래픽이 개시되거나 비정상적인 포트를 통해 전송되는 경우, 은닉 채널을 통해 트래픽이 전송되는 경우, 내부 호스트가 동적 IP 범위의 주소로 통신을 개시한 경우 등을 파악할 수 있습니다.
- 지역적으로 접근과 트래픽을 감시합니다. 전세계 다수 국가에서 사업을 하는 글로벌 환경에서 운영하고 있을지라도, 네트워크 트래픽의 송수신을 예측할 수 있는 국가는 한정되어 있을 것입니다. 다른 지역에서 트래픽이 발생할 경우, 특히 활동과 관련된 사용자나 시스템에서 기타 의심스런 동작이 발견되는 경우, 조사를 수행해야 할 것입니다.
- 이상징후 탐지와 더불어 위협 인텔리전스를 활용합니다. IBM X-Force가 제공하는 서비스를 포함한 다수의 상용 및 커뮤니티 위협 인텔리전스 서비스는 위협 활동과 나쁜 의도를 가진 공격자에 대한 풍부한 통찰력을 제공하므로, 이상징후 탐지를 한층 강화할 수 있습니다. 일례로, 악성코드, 봇넷 명령어 및 제어 서버 또는 기타 위협을 호스팅하는 것으로 알려진 사이트와 사용자나 시스템이 상호작용하는지를 파악해야 합니다.
- 네트워크 흐름을 수집하여 통찰력을 제고합니다. 네트워크 흐름 데이터(특히, 컨텐츠 가시성이 있는 계층 7 데이터)는 이상징후 탐지에 매우 유용한 데이터 소스가 될 수 있습니다. 또한, 침입의 존재를 확인하거나 반증하고, 모든 침입의 정도와 영향을 판단할 수 있는 매우 소중한 정보를 제공합니다.

결론

침입이 사실상 불가피하다는 인식 하에, 다수 기업이 탐지에 주력하게 되었습니다. SI(Security Intelligence)는 일련의 방대하고 다양한 데이터를 수집하여 정규화하고 분석하는 기능을 통해 APT를 차단할 수 있는 가장 유력한 수단으로 부상하였습니다. SI의 중심에 있는 이상징후 탐지는 정보 보안팀이 정상적인 리듬의 활동과 의미 있는 이상 동작을 구분할 수 있게 합니다. SI 솔루션과 모범 사례를 이용하면 한층 사전 예방적인 보안 태세를 갖출 수 있습니다.

2012년 상반기의 취약점 노출

1997년 이래, IBM X-Force는 공개적으로 노출된 소프트웨어 제품의 보안 취약점을 추적해왔습니다. X-Force 분석가들은 소프트웨어 공급업체로부터 소프트웨어 자문을 수집하고, 수정 정보, 악용 사례, 취약점이 노출된 보안 관련 이메일 주소 목록과 수 백 개의 웹 사이트를 분석하고 있습니다.

2012년 상반기에 새로 보고된 보안 취약점은 4,400건을 약간 상회했습니다. 이 추세가 일년 내내 지속될 경우, 전체 예상 취약점은 2010년 기록을 다소 상회하여 9,000 건에 달할 것으로 보입니다.

2006년 이후 그리고 2007년에 처음으로 노출된 취약점이 감소한 이래, 2년 단위로 총 취약점의 수가 등락을 거듭하고 있습니다. 이러한 변동에 대한 결정적인 이유는 없지만, 2012년은 보안 취약점 노출에 있어 기록적인 해가 될 가능성이 높습니다.

웹 애플리케이션

전반적인 보안 취약점 노출 건수의 지속적인 추세는 웹 애플리케이션 범주의 보안 취약점에서도 찾아볼 수 있습니다. 2011년에는, 웹 애플리케이션의 취약점이 49%에서 41%로 감소했습니다. 하지만, 2012년 상반기에는 웹 애플리케이션의 취약점이 반등하였습니다. 올해 지금까지 2,000 건 이상이 보고된 웹 애플리케이션 취약점의 2012년도 비율은 현재 47%로 예상됩니다.

연도별 취약점 노출 증가
1996-2012년 (예상)

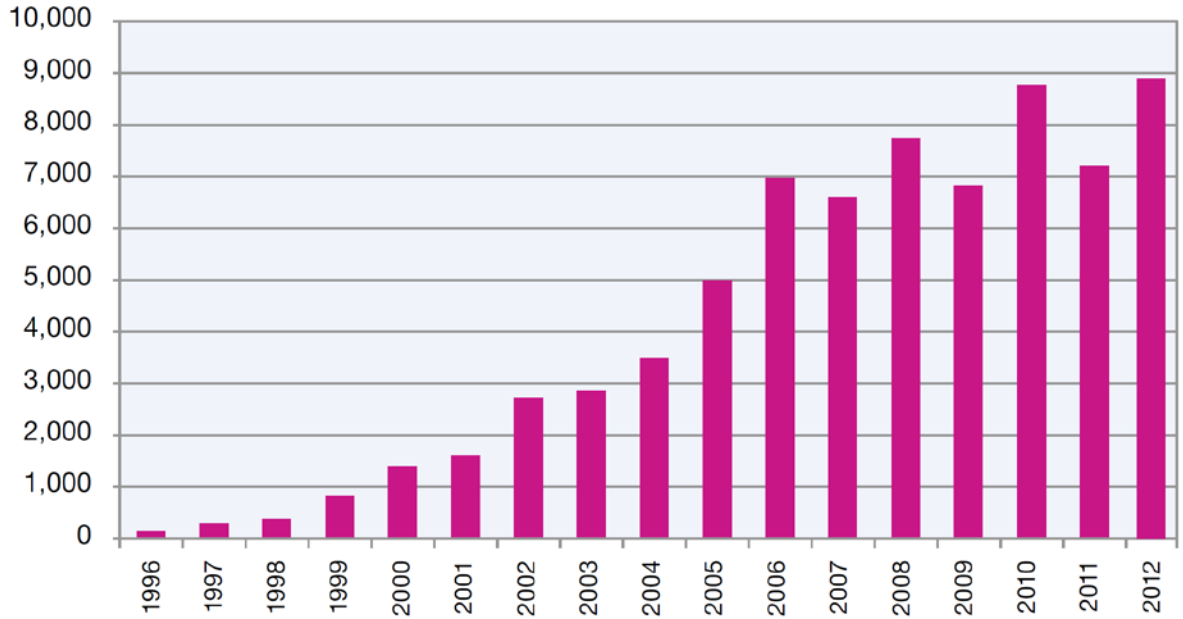


그림 34:연도별 취약점 노출 증가 - 1996-2012년 (예상)

보고된 SQL 인젝션 취약점의 하락세는 2012년에도 이어졌지만 XSS(cross-site scripting) 취약점은 다시 증가하여 역대 최고가 될 것으로 예상됩니다. XSS는 공격자가 클라이언트 측 스크립트를 다른 사용자들이 열람하는 웹 페이지에 주입할 수 있는 웹 애플리케이션 취약점을 설명할 때 쓰이는 용어입니다. 2012년에 지금까지 보고된 전체 웹 애플리케이션 취약점의 51% 이상이 현재 XSS로 분류되어 있습니다. XSS가 잘 알려져 있으며 조사된 보안 문제라는 점에서, 이는 불안한 지표입니다. 온디맨드 웹 애플리케이션 취약점을 조사한 IBM AppScan® OnDemand 결과에서 나온 데이터에서는 2011년도에 대한 온디맨드 스캔에서 XSS 취약점이 발견될 가능성이 40% 이상일 것으로 나타났습니다.

2012년에 지금까지 보고된 전체 웹 애플리케이션 취약점의 51% 이상이 XSS로 분류되어 있습니다.

웹 애플리케이션 취약점
2012년 상반기 전체 노출의 비율

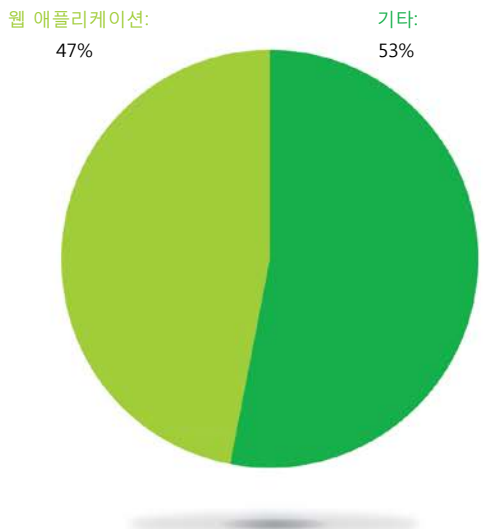


그림 35: 2012년 상반기 전체 노출의 비율로 본 웹 애플리케이션 취약점

공격 수법별 웹 애플리케이션 취약점
2004년-2012년 상반기

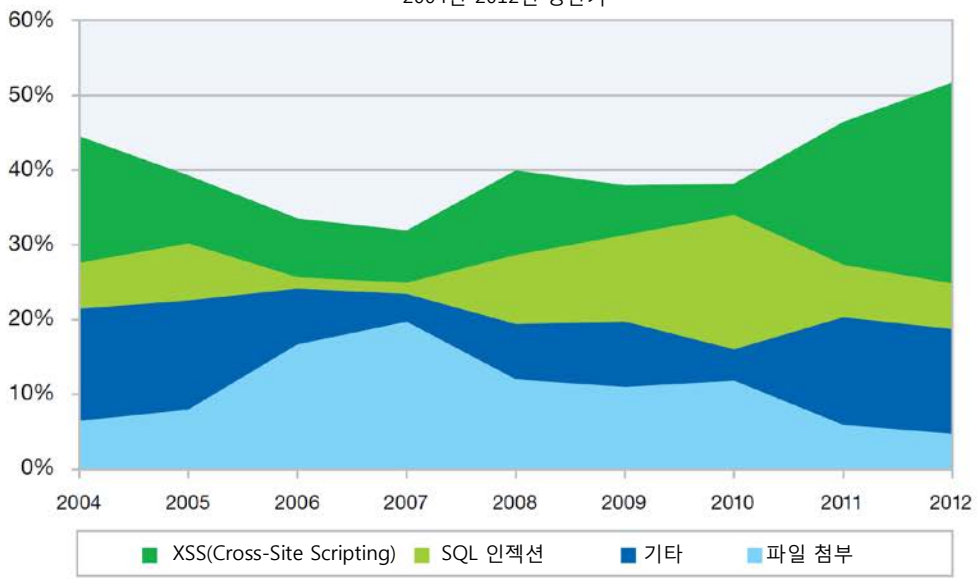


그림 36: 공격 수법별 웹 애플리케이션 취약점 – 2004년-2012년 상반기

IBM X-Force는 다수의 웹 애플리케이션 취약점이 공개 악용 웹사이트에 공개되어 있다는 사실을 파악했습니다. 이러한 웹 애플리케이션 중에서 다수는 웹사이트 디자인 회사가 개발한 사내 디자인 컨텐츠 관리 시스템(CMS)에 포함된 플러그인에 기인한 것입니다. 이러한 플러그인은 별도로 구입할 수 없는 경우가 많습니다. 하지만, 웹사이트가 정상 운영에 들어가면, 소비자 소유의 하드웨어와 네트워크에 호스팅됩니다. 이러한 소규모 회사의 웹사이트에서는 다수의 취약점을 찾아볼 수 있습니다.

인터넷 상에서 광범위하게 쓰이는 컨텐츠 관리 시스템도 있습니다. 이 주요 웹 기반 CMS 프로그램들은 타사가 작성한 플러그인에서 취약점이 발견되는 경우 대중에게 쉽게 노출되었습니다. IBM X-Force는 이러한 CMS 프로그램의 취약점을 핵심 플랫폼 문제와 플러그인 문제로 분류하고 있습니다. 이 시스템을 제공하는 제작 회사가 실시하는 핵심 문제의 패치가 이루어지는 비율은 타사가 작성한 플러그인에 비해 훨씬 더 높습니다.

그림 37은 핵심 플랫폼 문제 또는 플러그인 문제로 분류되는 취약점의 비율을 보여주고 있습니다.

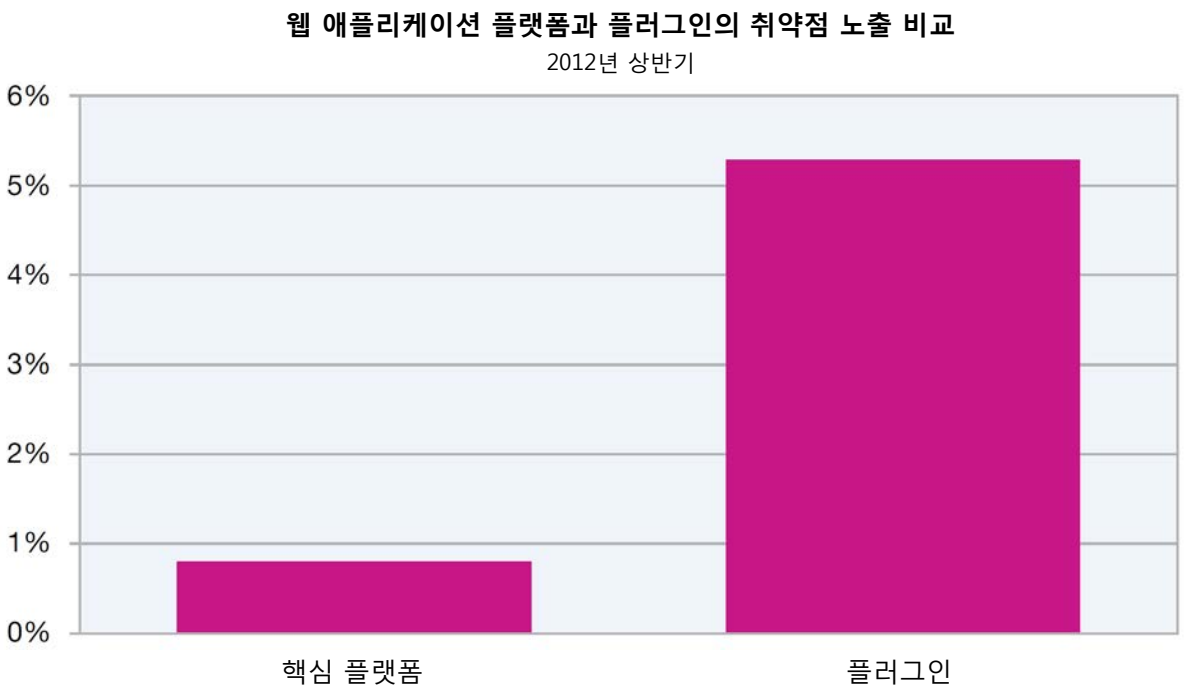


그림 37: 웹 애플리케이션 플랫폼과 플러그인의 취약점 노출 비교 – 2012년

보시다시피, 시장을 주도하는 주요 CMS 제작사의 경우 전체 CMS 보안 취약점의 1% 미만이 노출되어 있습니다. 이 선두 업체들 중에서, 5%를 약간 상회하는 취약점이 타사의 플러그인에 있습니다.

플랫폼 취약점에 대한 패치율도 플러그인 취약점에 비해 더 높습니다. 다수의 일류 CMS 프로그램들이 보안에 취약한 타사의 확장 기능 목록을 호스팅하여, 사용자 및 개발자들에게 그들이 개발한 플러그인에 문제가 있을 수 있음을 알리기 시작했습니다.

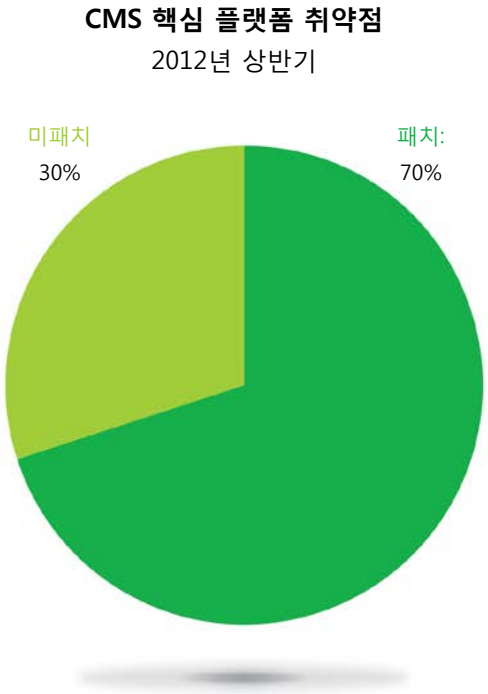


그림 38: 패치가 실시된 상태와 실시되지 않은 상태의 핵심 컨텐츠 관리 시스템의 취약점 노출 비교 – 2012년 상반기

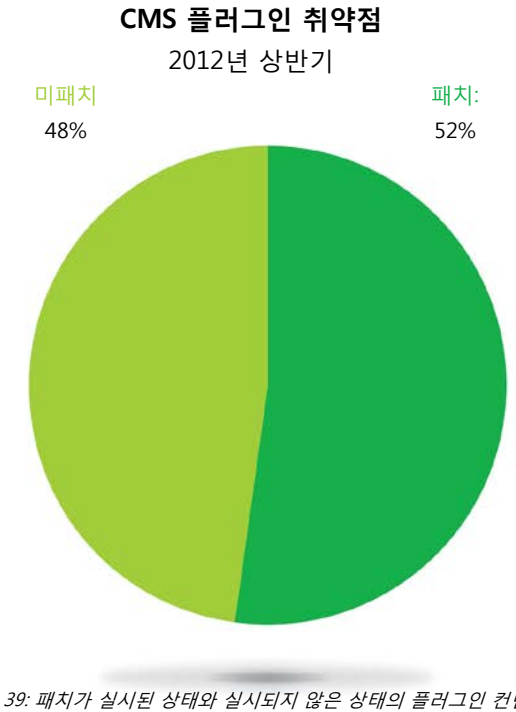


그림 39: 패치가 실시된 상태와 실시되지 않은 상태의 플러그인 컨텐츠 관리 시스템의 취약점 노출 비교 – 2012년 상반기

공격코드 건수의 지속적인 감소

2011년에는 공개적으로 노출된 공격코드 건수가 현저히 감소했습니다. IBM X-Force는 공격코드를 두 가지 범주로 분류하고 있습니다. 개념증명 코드가 있는 단순한 스니펫(Snippet)은 공격코드로 간주되지만, 컴퓨터를 공격할 수 있는 완전한 기능의 프로그램은 "실제 공격코드"로 따로 분류됩니다. 실제 공격코드 건수를 데이터베이스에 기록된 전체 취약점에 비교해 보면, 흥미로운 추세가 나타납니다.

실제 공격코드 비율은 2009년에 공개적으로 노출된 전체 취약점의 약 16%에 달하면서 최고를 기록했지만, 그 후 전반적인 취약점이 감소하면서 실제 공격코드는 2011년에 약 11%로 하락했습니다.

이 추세가 2012년에도 이어지고 있으며, 상반기 6개월의 데이터에 의거해 볼 때 실제 공격코드가 포함된 취약점은 공개적으로 노출된 전체 취약점의 9.7% 정도에 그칠 것으로 예상됩니다. 이 비율에는 표준 웹 브라우저의 주소 표시줄 사용을 통해 악용될 수 있는 다수의 웹 애플리케이션 취약점은 포함되어 있지 않습니다.

좀 더 자세히 살펴보면 (우측의 그림 40), 전체적인 실제 공격코드 건수가 2011년 전체에 비해서는 다소 높지만, 2010년에 비해 훨씬 낮다는 것을 알 수 있습니다. 하지만 전체 취약점 건수의 비율로 실제 공격코드를 살펴보면, 표 6에 나와있는 바와 같이 예상 비율이 9.7%로 하향세임을 알 수 있습니다. IBM X-Force는 공개적으로 노출된 공격코드 건수의 감소가 지난 수년 간 소프트웨어에 이루어진 구조적 변경으로 인하여 이러한 취약점의 악용이 더 어려워진 직접적인 결과라고 봅니다.

실제 공격코드 노출 건수
2006년-2012년 상반기 (예상)

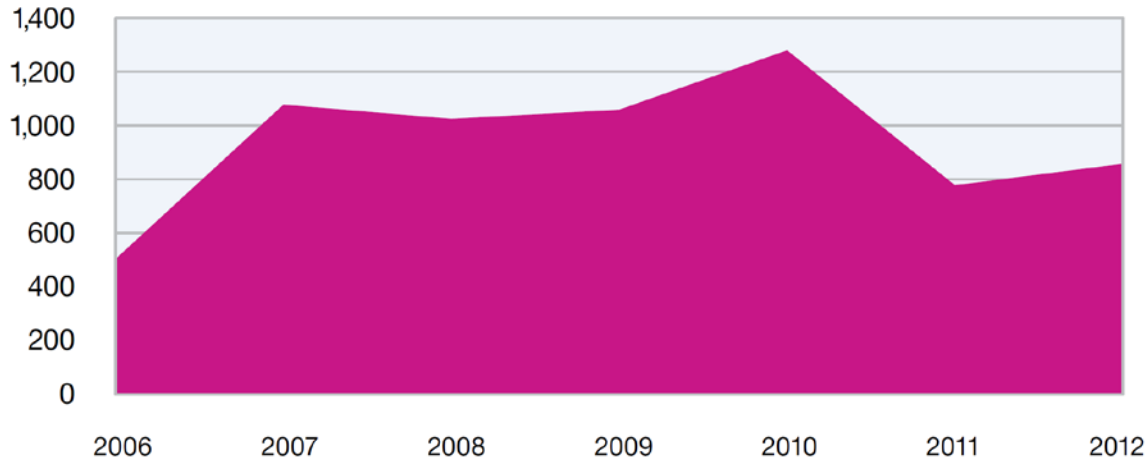


그림 40: 실제 공격코드 노출 건수 – 2006년-2012년 상반기 (예상)

	2006	2007	2008	2009	2010	2011	2012
실제 공격코드 건수	504	1078	1025	1059	1280	778	858
비율	7.3%	16.5%	13.3%	15.7%	14.7%	10.9%	9.7%

멀티미디어 기반 공격코드 건수는 전년도와 동일한 수준에 머물렀습니다.

공개적으로 노출된 공격코드 건수가 현저히 감소한 또 다른 부문은 모바일 운영 체제입니다. 모바일 디바이스가 일상 생활에서 차지하는 비중은 점점 더 커지고 있습니다. 이에 따라 모바일 디바이스의 보안에 관한 사용자들의 우려도 커지고 있습니다. 2012년 상반기에는 모바일 취약점과 공격코드 건수가 2008년 이래 최저 수준으로 감소하였습니다. 그 이유에는 여러 가지가 있습니다. 첫째, 모바일 운영 체제 개발자들이 지속적으로 사내에서 취약점을 찾아내어 그 취약점을 악용하지 못하도록 보안 모델을 향상시키고 있습니다. 둘째, 모바일과 같은 새로운 분야에서는 초기에 취약점이 발견되며, 간단한 버그는 바로 조치되고 악용이 어려운 버그만 남아 조사자와 공격자들이 공격할 수 있는 기술을 찾아내기까지 시간적인 간격이 있습니다. 일례로, 2005년경에는 브라우저 취약점에 "힙 스프레이(heap spray)" 기법을 적용하면 비프로그램 방식으로는 제어할 수 없었던 메모리 위치에 악성코드가 도달할 수 있으므로 메모리 오류 취약점을 공략하여 안전하게 클라이언트 측 공격을 할 수 있었습니다. 하지만, 힙 스프레이가 전혀 새로운 개념은 아니었다는 점에 유의해야 할 것입니다.

브라우저 악성코드 공개 노출 건수
2005년-2012년 상반기 (예상)

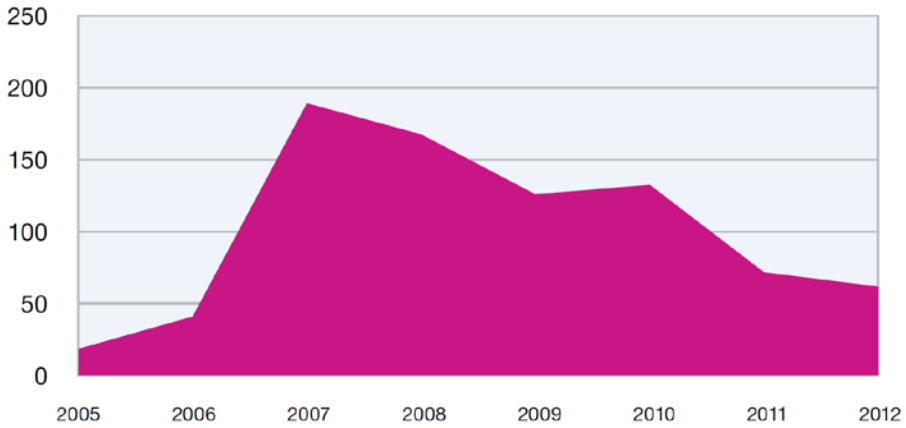


그림 41: 브라우저 악성코드 공개 노출 건수 - 2005년-2012년 상반기 (예상)

멀티미디어 악성코드 공개 노출 건수
2005년-2012년 상반기 (예상)

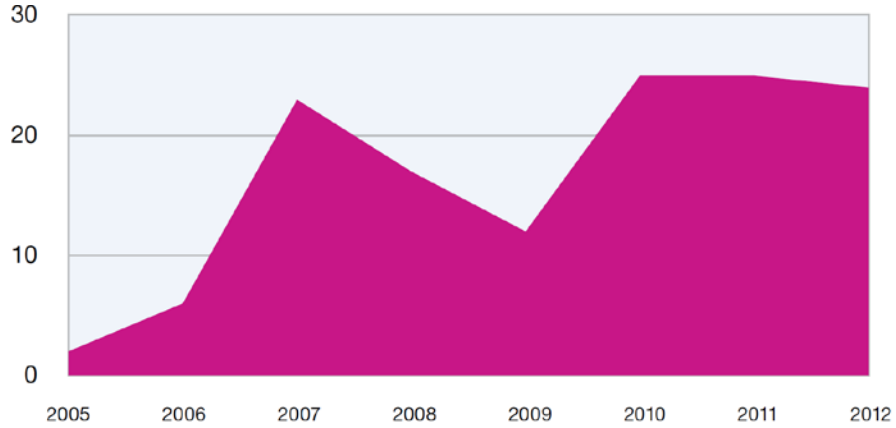


그림 42: 멀티미디어 악성코드 공개 노출 건수 - 2005년-2012년 상반기 (예상)

전체 모바일 운영 체제 취약점
2006년-2012년 상반기 (예상)

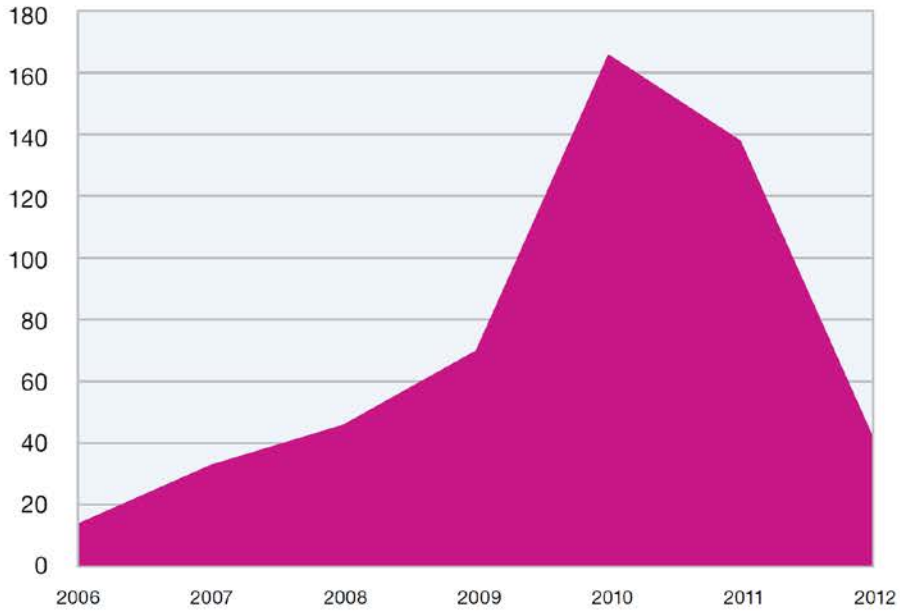


그림 43: 전체 모바일 운영 체제 취약점 - 2006년-2012년 상반기 (예상)

모바일 운영 체제 악용 건수
2006년-2012년 상반기 (예상)

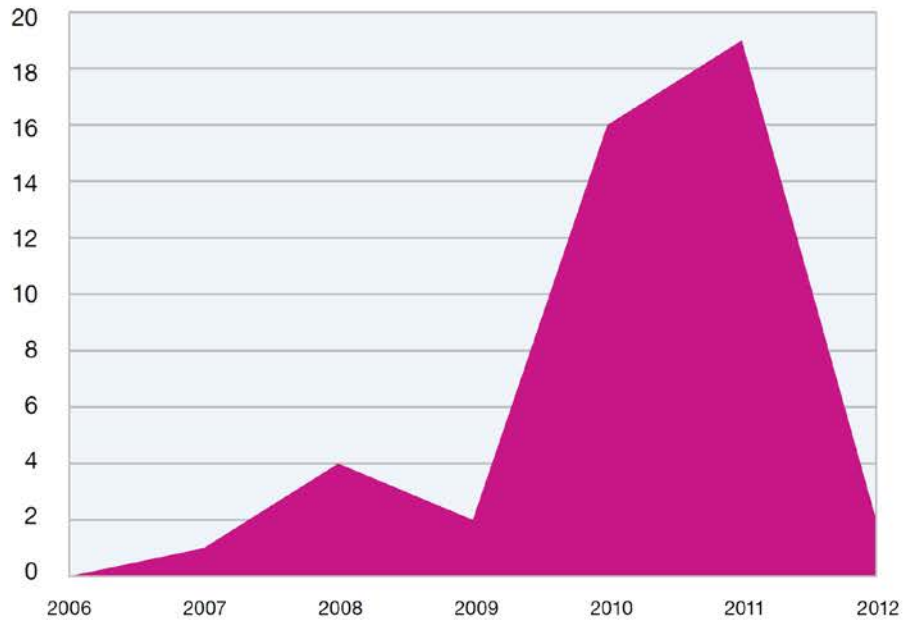


그림 44: 전체 모바일 운영 체제 악용 건수 - 2006년-2012년 상반기 (예상)

CVSS 스코어링

IBM X-Force는 심각도에 기초한 CVSS(Common Vulnerability Scoring System)을 사용하여 조사되는 거의 모든 취약점에 점수를 부여하고 있습니다. 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. 2012년 상반기의 취약점에 점수를 부여해본 결과, 대다수 문제가 중간 범위에 속하며, 심각 또는 높음으로 분류된 취약점은 전체의 27%인 것으로 나타났습니다.

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

표 7: CVSS 점수와 그에 상응하는 심각도

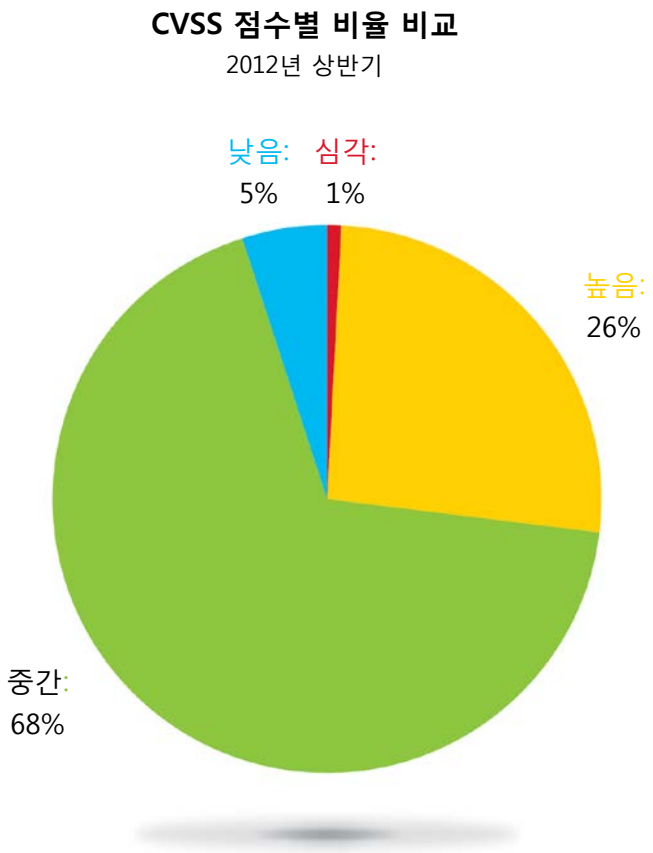


그림 45: CVSS 점수별 비율 비교 – 2012년 상반기

기업용 소프트웨어의 취약점

기업용 소프트웨어의 동향을 조사할 때, IBM X-Force는 가장 다양한 기업용 소프트웨어를 개발하는 대형 소프트웨어 공급업체를 조사합니다. 수 천에 달하는 소프트웨어 공급업체를 조사해본 결과, 이 업체들은 상당 수에 달하는 보안 취약점이 꾸준히 노출되고 있었습니다. 이러한 공급업체들이 상위 10대 그룹으로 분류되며, CMS 취약점은 대다수가 타사 플러그인 및 추가 기능에 있으며 엔터프라이즈급 소프트웨어는 널리 쓰이지 않기 때문에 제외되어 있습니다. 2007년 이후, 이 상위 10대 그룹의 공개된 취약점의 비율이 증가하면서 2011년에는 전체 노출 취약점의 30%에 달했으며, 대형 소프트웨어 공급업체의 비율이 주를 차지했습니다. 하지만, 2012년 상반기에는 이 업체들의 공개된 취약점이 전체의 22%로 감소했습니다.

2012년 하반기의 공개 취약점 건수가 확연한 하향세를 보일지 아니면 별다른 변화 없이 현상을 유지할지, 연말까지 이 추세를 지켜보는 것도 흥미로울 것입니다.

취약점 노출 건수가 가장 많은 상위 10대 소프트웨어 공급업체

2011년-2012년 상반기

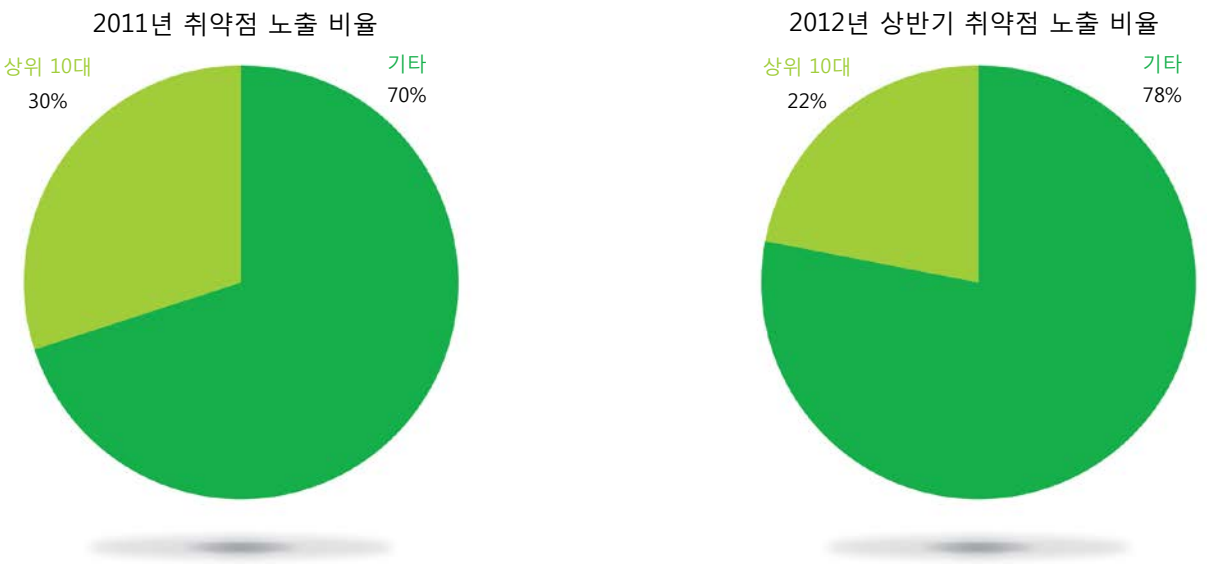


그림 46: 취약점 노출 건수가 가장 많은 상위 10대 소프트웨어 공급업체 - 2011년-2012년 상반기

2012년 상반기에 눈에 띄는 추세는 Office 및 PDF(Portable Document Format)의 취약점이 급감했다는 점입니다. PDF 취약점 노출의 감소는 Adobe Acrobat Reader X 샌드박스와 상당한 관계가 있음이 확실합니다. 첫째, 샌드박스는 신뢰할 수 있는 악성코드 제작의 복잡도를 현저히 증가시킵니다; 이 점은 잠시 후에 살펴보기로 하겠습니다. 신뢰할 수 있는 악성코드 제작의 복잡도가 높아진 점을 고려할 때, PDF 취약점은 새로운 취약점을 찾기 위해 시간을 할애할 만큼 공격자에게 관심거리가 되지 않습니다.

샌드박스는 공격자와 조사자들이 감염된 시스템에서 취할 수 있는 권한을 줄이도록 설계되어 있기 때문에, 보안 생태계에 이점을 제공합니다. 소프트웨어 샌드박스의 지속적인 채택이 공격자들의 사기를 꺾고, 대부분은 아닐지라도 다수의 공격을 완화시킬 수 있을 것으로 보입니다.

2012년 상반기에는 웹 브라우저 취약점이 다소 감소했지만, 문서 포맷 취약점과 같이 대폭적인 수준은 아니었습니다. 웹 브라우저 기반 취약점은 2012년 전반에 걸쳐 거의 동일한 수준을 유지할 것으로 보입니다.

상위 10대 공급업체의 취약점 패치율에 장족의 발전이 있었는데, 이는 안전한 개발 환경과 PSIRT (Product Security Incident Response Team) 프로그램의 지속적인 구현과 개선이 있었기 때문입니다. 상위 10대 공급업체들의 패치 수정률은 공개된 전체 취약점의 94%를 약간 상회하고 있습니다.

문서 포맷 문제에 영향을 미치는 심각도 및 높음 취약점 노출의 비교

2005년-2012년 (예상)

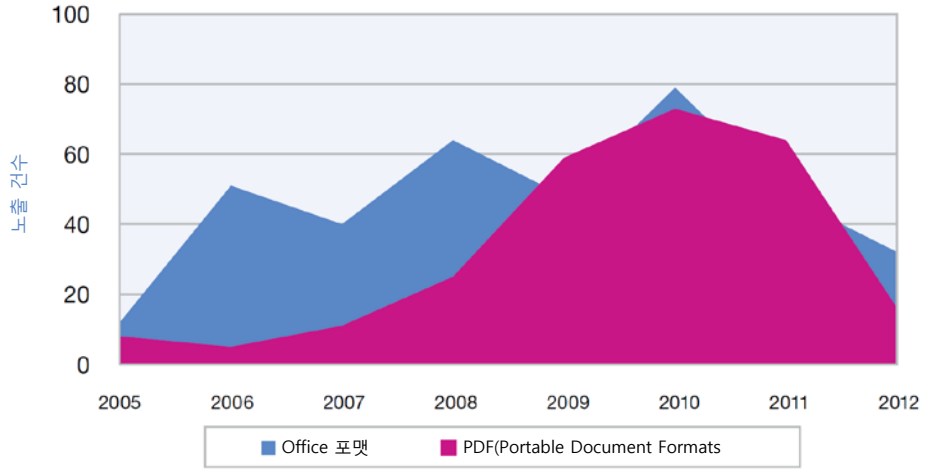


그림 47: 문서 포맷 문제에 영향을 미치는 심각도 대 높음 취약점 노출의 비교 - 2005-2012년 (예상)

심각도 및 높음 웹 브라우저 취약점 비교

2005년-2012년 상반기 (예상)

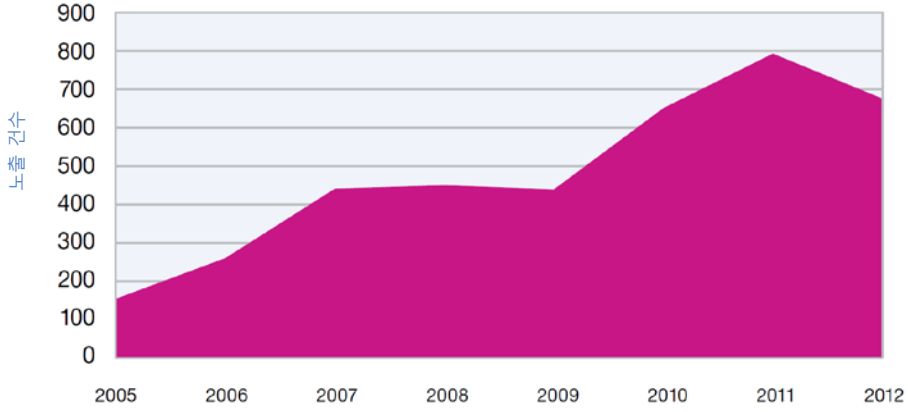


그림 48: 심각도 및 높음 웹 브라우저 취약점 비교 – 2005년-2012년 상반기 (예상)

이는 상위 10대 소프트웨어 공급업체에게 희소식이지만, 나머지 취약점 부문에서는 그렇지 않습니다. 2012년 상반기의 패치되지 않은 취약점의 비율이 2008년 이래 가장 높았습니다. 금년에 공개된 전체 취약점의 47%가 아직 조치되지 않은 상태로 남아 있습니다.

패치가 이루어지지 않은 취약점의 증가가 반드시 나쁜 징조라고 볼 수는 없습니다. 대형 소프트웨어 공급업체들은 5년 전에 비해 취약점 해소에 더욱 많은 노력을 기울이고 있습니다. 소규모 웹 애플리케이션(과 개인 또는 소규모 기업이 개발한 유명하지 않은 소프트웨어)의 취약점 증가는 2012년도 증가세의 주된 원인으로 보입니다. 이러한 취약점의 다수는 제품 수명이 다할 때까지 패치나 지원이 제공되지 않을 가능성이 높습니다.

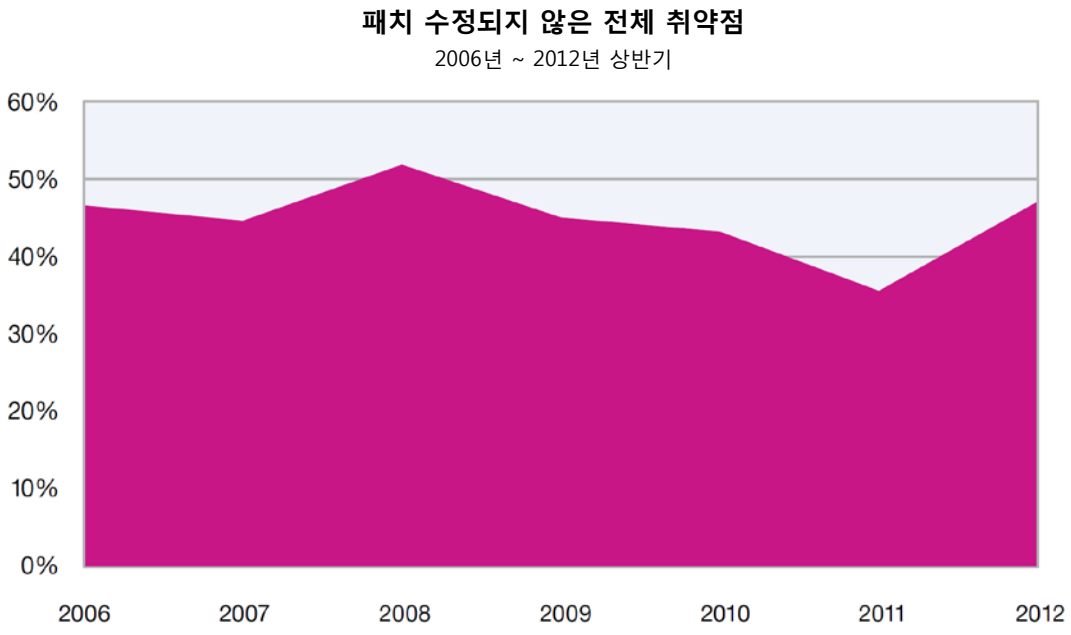


그림 49: 패치 수정되지 않은 전체 취약점 - 2006년 ~ 2012년 상반기

요약

지난 보고서와 비교해볼 때, 일부 소수 핵심 분야에서만 흥미로운 조사 결과가 나타났습니다. 우리가 앞서 논의한 대로, 패치되지 않은 취약점의 비율은 증가하였으며 이들은 일반적으로 기업에서 볼 수 없는, 잘 알려지지 않은 소프트웨어에 해당됩니다. 둘째, 모바일 플랫폼을 겨냥한 공격코드와 취약점이 현저하게 감소하였습니다. 그 이유는 여러 가지가 있지만, 자신의 소유든 회사 소유든 모바일 디바이스 이용 시에 여전히 보안에 주의를 기울이는 것이 바람직합니다. 왜냐 하면 이동 중의 업무 시에는 주의가 산만해져, 동일한 보안 위주의 사고 방식을 적용하는 것을 쉽게 잊을 수 있기 때문입니다. 일례로, 모바일 디바이스로 수신되는 피싱 이메일에 동일하게 엄격한 주의를 기울이거나 모바일 애플리케이션이 요구하는 보안 권한에 세심한 주의를 기울이지 못하는 경향이 있습니다. 따라서, 2012년에 발생할 가능성이 가장 높은 공격은 단순한 공격이 될 것으로 보이며 이 점을 본 보고서의 모바일 단원에서 더 자세히 살펴볼 것입니다.

세 번째로 흥미로운 추세는 소프트웨어 샌드박스의 실효성과 관련된 것으로, 샌드박스 환경의 권한을 축소하여 과거에 공격에 성공하지 못했던 취약점을 찾아 노출하려는 조사자와 공격자들의 사기를 꺾고 공격을 완화시킵니다. 그러한 공격이 성공을 거두려면, 일반적으로 샌드박스를 비활성화시키거나, 소프트웨어가 노출한 취약점을 공략한 다음 샌드박스의 또 다른 취약점을 공략하여 시스템을 손상시킬 수 있도록 권한을 상승시키는 두 가지 과정의 공격 시나리오가 가능하도록 샌드박스의 취약점을 찾아 여러 취약점을 공략해야 합니다. 지능적이며 특정 대상을 겨냥한 공격에도 쓰일 가능성이 있는 일부 소프트웨어 샌드박스의 취약점이 2011년과 2012년에 IBM X-Force 연구진 등에 의해 보고되었습니다. 소프트웨어 샌드박스는 소프트웨어 공급업체, 보안 연구원, 보안 종사자 등에게 매우 흥미로운 분야입니다. Adobe가 제공한 대책에 의거한 PDF 취약점 및 공격의 감소를 이미 살펴 보았으므로, 이제는 샌드박스 기술을 더 자세하게 살펴 보기로 하겠습니다.

샌드박스: 또 다른 방어선

샌드박스란 무엇인가?

도둑이 몰래 집이나 사무실에 침입했다는 경보를 받게 되는 경우, 어떻게 대처할 것이냐가 가장 중요한 문제가 됩니다. 그러나 "무엇을 훔쳐갈 것이며 손해는 어느 정도가 될 것"인지도 중요한 문제입니다. 도둑은 보석, 가전제품, 중요한 업무 서류 또는 지적재산권 등 모든 소유물을 취할 수 있습니다. 또한 집이나 사무실 내에서 기물을 파손하는 등 마음대로 할 수 있습니다. 경쟁사가 그 도둑을 고용하여 비밀 감시 장비를 설치했다면 어떨까요?

이제는 이와 동일한 시나리오에서, 그 도둑이 집이나 사무실이 아니라 방금 컴퓨터에 침입한 원격 공격자라고 가정해 보겠습니다. 샌드박스의 중요한 임무는 이 원격 공격자가 시스템에 침입한 다음에 수행하거나 접근할 수 있는 것을 제한하는 것입니다.

샌드박스의 원리

샌드박스는 애플리케이션을 나머지 시스템과 격리시켜, 애플리케이션이 손상될 경우 공격자가 애플리케이션 내에서 실행하는 코드가 수행되거나 접근할 수 있는 것을 제한하는 기능을 합니다.

샌드박싱의 운용 방법은 다양합니다. 애플리케이션을 나머지 시스템과 격리시키는 일반적인 방법의 몇 가지 예는 다음과 같습니다.

1. **자원 가상화—**애플리케이션(또는 전체 운영 체제)에 가상 디스크와 같은 일련의 가상 자원을 제공하여, 이 가상 자원 자원에 대한 변경이 실제 자원에 영향을 미치지 못하게 합니다. Xen 및 VirtualBox와 같은 가상화 소프트웨어가 제공하는 자원 가상화가 한 예입니다.

2. **권한 축소—**운영 체제에 제공되어 있는 기존 메커니즘을 이용하여 애플리케이션의 권한과 기능을 축소합니다. 그 예로는 구글 크롬 샌드박스, Adobe Reader X 샌드박스와 여러 종류의 Adobe Flash Player 샌드박스 등이 있습니다.

3. **실행 통제—**애플리케이션이 운영 체제에 직접 접근하지 않는 통제된 환경에서 실행됩니다. 권한이 필요한 동작을 수행하려면 특정 인터페이스를 사용해야 합니다. Java 샌드박스가 여기에 해당됩니다.

샌드박스가 적용된 애플리케이션은 더 높은 권한을 가진 애플리케이션(흔히 브로커라고 함)에 의해 노출된 서비스를 이용하여 권한이 필요한 동작을 수행합니다. 한편 브로커는 일련의 정책을 검토하여 권한이 필요한 동작의 허용 또는 거부 여부를 결정합니다.

샌드박스의 장점

샌드박스의 구현 방법과 시행되는 정책에 따라, 샌드박스는 다음과 같은 보호를 제공할 수 있습니다.

- 중요한 자원에 대한 쓰기 권한을 허용하지 않기 때문에 지속적인 악성코드가 시스템에 설치되는 것을 방지하는 데 유용합니다. 공격자는 시스템의 중요한 부분을 수정할 수 없으며 시스템을 재부팅해도 제대로 기능하는 악성코드를 설치할 수 없습니다.
- 중요한 자원에 대한 읽기 권한과 네트워크 접근을 허용하지 않기 때문에 정보 노출을 예방하는 데 유용합니다. 공격자는 개인 파일에 접근하거나 원격 위치로 전송할 수 없습니다.
- 시스템의 중요한 부분에 대한 수정과 시스템 구성의 변경을 허용하지 않기 때문에 시스템의 손상을 예방하는 데 유용합니다.

모든 샌드박스 구현이 동일하지 않기 때문에, 사용할 샌드박스 구현의 기능과 제한을 이해하는 것이 중요합니다. Adobe Reader X 샌드박스[17] 조사 또는 Adobe Flash Player 샌드박스[18] 조사와 같이 샌드박스를 조사하고 평가한 보안 연구원들의 조사 결과와 공급업체가 제공하는 자료를 참고할 수 있습니다.

바로 샌드박스를 이용할 수 있는 방법

샌드박스의 장점을 활용하는 적절한 방법 중 하나는 조직이 사용할 애플리케이션이 최신 샌드박스 버전인지를 확인하고, 그럴 경우 애플리케이션을 테스트하고 배치하여 사용하는 것입니다.

문서 리더, 미디어 재생기, 브라우저 및 브라우저 플러그인 등과 같이 인터넷의 컨텐츠를 사용하는 애플리케이션 조사부터 시작할 수 있습니다. 다행스럽게도, 일부 공급업체들이 현재 샌드박스 버전의 제품을 제공하고 있습니다. Windows 플랫폼용 샌드박스 애플리케이션의 몇 가지 예는 다음과 같습니다.

- 웹 컨텐츠용
  - 구글 크롬
  - Windows Vista 이상의 운영 체제 상의 Internet Explorer 7 이상
- PDF 컨텐츠용
  - Adobe Reader X (일명 Adobe Reader 10) 이상의 버전
  - 구글 크롬의 내장 PDF 뷰어
- 플래시 컨텐츠용
  - Adobe Flash Player 11.3 이상의 버전 (현재는 Windows Vista 이상의 운영 체제의 Firefox에서만 샌드박스 기능이 있음)
  - 구글 크롬의 내장 플래시 뷰어 (일명 Pepper Flash)
- 문서용
  - Microsoft Office 2010 (보호 보기 모드의 경우)

오래된 샌드박스 기능이 없는 버전의 애플리케이션을 겨냥한 기회를 노리는 공격이 발생할 수 있으며, 샌드박스는 이러한 공격에 대한 또 다른 방어선이 된다는 점을 염두에 두어야 합니다.

17 https://media.blackhat.com/bh-us-11/Sabanal/BH_US_11_SabanalYason_Readerx_WP.pdf
18 https://media.blackhat.com/bh-us-12/Briefings/Sabanal/BH_US_12_Sabanal_Digging_Deep_WP.pdf

향후 전망

맞춤형 샌드박스의 구축에는 연구, 개발, 테스트 및 유지보수 비용 등의 많은 비용이 소요됩니다. 대다수 상용규격 애플리케이션에 필요한 샌드박스 기능은 운영 체제 자체에서 제공될 것입니다. 현재 Windows 8의 AppContainer 기능과 OS X의 App Sandbox 기능의 일부로 제공되고 있습니다. 운영 체제가 제공하는 샌드박스에서 일부 애플리케이션에 대한 세밀한 제어가 불충분할 경우에는, 맞춤형 샌드박스를 갖추어야 할 것입니다.

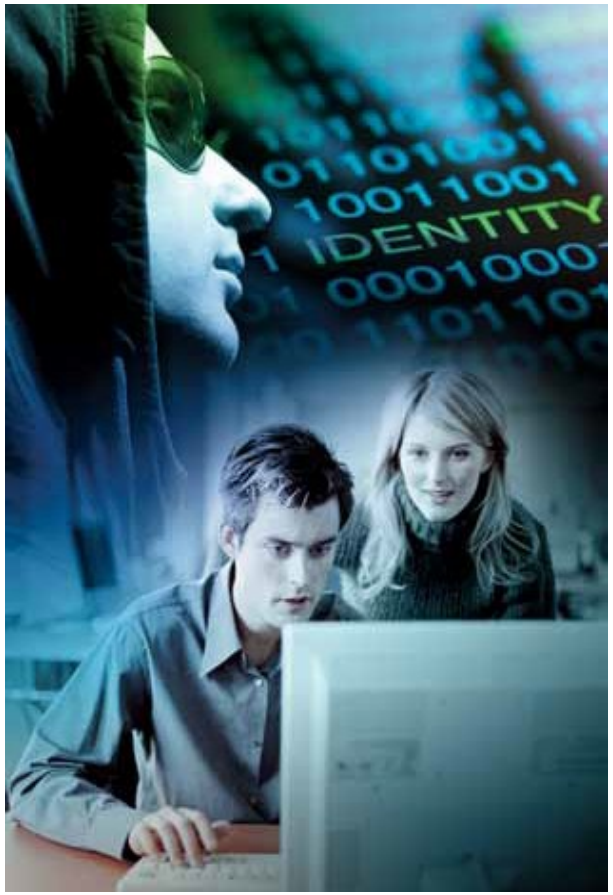
어쨌든, 운영 체제는 지속적으로 업데이트되어 애플리케이션의 권한과 기능을 제한하는 추가 메커니즘을 포함할 것이며, 실행하는 모든 애플리케이션이 사실상 개인 문서에 접근할 필요가 없다는 점을 고려해 볼 때 이러한 제한은 대부분 기본으로 적용될 가능성이 높습니다.

공격자의 적응

소프트웨어 공급업체들이 지속적으로 자사 제품에 샌드박스 기능을 부여하게 되면, 공격자들은 시스템을 완전히 손상시키기 위한 별도의 취약점이 필요할 것입니다. 공격자의 관점에서 보면 완벽한 공격의 개발 비용이 증가하게 되고, 샌드박스 우회 취약점이 더욱 절실해질 것입니다. 공격자들은 샌드박스 우회 취약점의 파악/확보에 더 투자하여 이러한 환경에 적응하게 될 것입니다.

결론

당연히 샌드박스 기술은 풀프루프가 아니며 자원이 충분하고 동기가 확실한 공격자는 샌드박스의 취약점을 찾을 수 있을 것이므로, 여전히 주의를 기울일 필요가 있습니다. 현실에 안주하는 것은 새로운 문제를 야기할 수 있으며, 헬멧이나 방탄 조끼를 착용한다고 해서 무적인 양 사선을 활보할 수는 없습니다. 사용하지 않는 애플리케이션 및 기능과 브라우저 플러그인을 삭제하거나 비활성화시켜 공격 가능성을 줄이고 소프트웨어를 최신으로 유지하며, 요청하지 않은 컨텐츠 열람의 위험성에 관하여 사용자 교육을 실시하는 것이 항상 바람직합니다.



UNIX 쉘 이력 타임스탬핑으로 한층 간편해진 감사

컴퓨터 포렌식 분석가에게는 보안 사고를 조사할 때 이벤트가 발생한 시간을 파악하는 것이 중요한 과제입니다. UNIX는 쉘 이력 파일의 형태로 유용한 감사 시스템을 제공하고 있습니다. 기본적으로 이 파일이 명령어와 함께 타임스탬프를 기록하도록 항상 설정되어 있는 것은 아니므로, 이벤트를 타임라인과 상관시키는 것이 쉽지 않습니다.

수십 건의 UNIX/Linux 사례의 상세한 컴퓨터 사후 분석을 실시했던 IBM ERS(Emergency Response Service) 분석가들은 그 중에서 단지 소수의 시스템에만 HISTIMEFORMAT 값이 설정되어 있었다는 것을 알게 되었습니다. 이 설정은 Unix/Linux 시스템 사용자들이 어떤 명령을 내린 시간을 파악하는 데 도움이 된다는 것이 IBM X-Force의 견해입니다.

일례로, 쉘 이력 파일은 사용자가 **ping 192.168.100.10**을 입력한 인스턴스를 기록할 수 있지만, 패킷 스니퍼나 방화벽 로그 엔트리가 없는 한, 명령을 입력한 시간을 정확히 판단할 수 없습니다.

Unix(특히 본 보고서의 목적을 위해서 Linux)를 분석하는 ERS 분석가들은 이력 파일에 타임스탬프를 추가하는 가치를 지지합니다. 보안 분석가와 시스템 관리자들은 프로덕션 서버에 이 기법을 구현할 필요성에 대한 인식을 제고해야 합니다.

C shell(csh), Korn shell(ksh), Borne again Shell (bash)과 같은 Unix 명령어 쉘은 개개인의 활동 계정으로 저장되는 '이력 기능'을 제공합니다. 기본적으로, 이 기능은 로그인한 사용자가 명령행 환경에 입력한 (그리고 실수가 있을 경우 잘못 입력한) 모든 명령어를 기록합니다.

컴퓨터 포렌식 분석가는 컴퓨터 계정 침입이 발생한 것으로 여겨지는 경우나 유사한 의심스런 이벤트를 조사하면서 이 이력 파일 (.bash_history)의 내용을 이용하여 활동을 역추적할 수 있습니다.

하지만, 몇 가지 문제가 발생할 수 있습니다. 사용자 계정에 속하는 이력 파일의 데이터는 불변이 아니며 수정이나 파기가 가능합니다.

또한, 활동 기록을 정확한 타임라인에 일치시키는 기능도 거의 쓰이지 않습니다.

가상의 회사 Acme에서 근무하는 가상의 사용자 Joe Black이 다음 명령어를 입력한다고 가정해 보겠습니다.

```
telnet fs1.acme.com
```

그의 이력 파일에 의하면, Joe는 fs1.acme.com에 접속한 즉시 이 명령어를 입력하였습니다.

```
mail bigcheese SUBJ: Resignation
rm -rf *
```

이 명령어는 Joe Black이 FileServer1에 로그인하여, 사직과 관련된 무언가를 상사에게 전달했으며, 데이터를 파괴하는 명령을 내렸다는 것을 의미합니다. 하지만 타임스탬프가 없으면, 분석을 수행하여 의미 있는 용어로 표현하고자 할 때 직원들과 경영진에게 설명하는 데 극히 중요한 요소인 활동의 발생 시기를 알 수 없습니다. 이제 가능한 해결책을 살펴보기로 하겠습니다.

본 논의의 목적에 따라, Linux 호스트 컴퓨터 시스템과 명령행의 Borne Again Shell(bash)과의 상호작용을 알아보기로 하겠습니다. 사용자 프로파일의 구성을 조사함으로써, 조사원과 총 책임자 및 Linux 호스트의 시스템 관리자에게 유용한 방식으로 타임스탬핑을 실시하는 기능을 채택할 수 있습니다.

/etc/profile 파일에 다음 코드 행을 추가하면 변경이 이루어집니다.

```
export HISTTIMEFORMAT="%s %T%z
%d/%b/%y "
```

본질적으로, 이 코드는 사용자가 로그인하여 쉘과 상호작용하는 동안 입력되는 모든 명령에 타임스탬프를 추가합니다. 아울러, 일자 설정은 Unix Epoch Time으로 시간을 삽입할 수 있게 하므로, 이 이력 파일의 구문분석을 간소화할 수 있으며 사람이 판독할 수 있는 용어로 시간이 삽입됩니다. Unix Epoch Time은 1970년 1월 1일 00:00(UTC) 이후 경과된 시간의 초 단위 수치입니다. 상기 명령행의 공백은 출력의 가독성을 높입니다.

출력은 또한 입력이 이루어진 실제 시간대도 보고하므로, 설정을 확인하거나 오구성을 검출하는 데 유용합니다. IT 전문가는 레코드를 조사할 때 현행 시간대를 파악해야 하기 때문에 이는 중요합니다.

이러한 설정 시에 고려해야 할 한 가지 중요한 주의사항이 있습니다. 기존의 이력이 있는 시스템 상에 이를 설정할 경우, 기존 이력 파일을 아카이브해야 합니다. 그렇지 않을 경우, 'export=HISTTIMEFORMAT' 명령을 프로파일에 입력하기 전의 모든 이벤트의 일자가 부정확해집니다. 이는 심각한 문제가 될 수 있습니다.

HISTTIMEFORMAT을 설정하기 전에, 기존의 모든 .bash_history 파일을 백업하고 아카이브해야 합니다. 'for-do'-loop를 사용하여 기존의 .bash_history 파일을 찾은 다음, (Linux의 bash 쉘을 이용하여) tar-gz 파일로 아카이브하는 것도 한가지 방법입니다.

```
$ sudo tar -czvf `date "+%d%e%Y"-
history.tar.gz ` $find(  -f /home  -
type f -name '*history')
```

이 명령행을 입력하면 이력 파일이 백업된 일자가 포함된 'tar.gz' 파일이 생성됩니다. 이 명령을 실행하고 나면, 기존의 .bash_history 파일을 (언제든지 되돌릴 수 있도록 이름을 변경하는 방식으로) 정리할 수 있게 되며 다음 명령행으로 타임스탬프를 구현할 수 있습니다.

```
$ mv ~/.bash_history ~/.OLD_bash_
history

$ echo export HISTTIMEFORMAT="%s %T%z
%d/%b/%y "  >>  ~/.bash_profile

$ history -c && exit
```

이력을 ('history' 명령어를 사용하여) 호출하면, 다음과 유사한 엔트리를 볼 수 있습니다.

```
$ history
1 1341870050 14:40:50-0700 09Jul2012
history
```

이는 .bash_history 파일이 실제 파일에 타임스탬핑된 레코드를 유지하고 있음을 의미합니다. 파일 자체가 다음과 같은 명령과 함께 타임스탬프의 레코드를 유지하게 됩니다.

```
#1341870056 exit

#1341870112
tcpdump -i eth0 host 192.168.100.12
-s 0 -w ./PacketCapture.pcap

#1341870112
tcpdump -n -r PacketCapture.pcap

#1341870452 history
```

이력 레코드를 (쉘에 'history' 명령을 입력하여) 호출하면 Bash 쉘이 HISTTIMEFORMAT 변수의 형태를 사용하여 사용자에게 유용한 방식으로 데이터를 제시하기 때문에 다음과 같은 내용이 디스플레이 됩니다.

```
1 1341870056 14:40:56-0700 09Jul2012
exit

2 1341870112 14:41:52-0700 09Jul2012
tcpdump -i eth0 host 192.168.100.12 -
s
0 -w ./PacketCapture.pcap

3 1341870274 14:44:34-0700 09Jul2012
tcpdump -n -r PacketCapture.pcap

4 1341870452 14:47:32-0700 09Jul2012
history
```

이를 통해 입력된 명령의 내용 및 입력된 순서를 즉시 파악할 수 있을 뿐만 아니라, 호스트가 속한 시간대도 확인할 수 있습니다.

'원시' 이력 파일 자체에서 Unix Epoch Time과 사람이 판독 가능한 엔트리(14:47:32-0700 09Jul2012) 둘 다를 볼 수 있는 것이 아니라 Unix Epoch Time 엔트리만을 볼 수 있는 이유에 주목할 필요가 있습니다. HISTIMEFORMAT 값이 설정된 것을 쉘이 인지하게 되면, 레코드가 시스템의 가장 정확한 방식(Unix Epoch Time)으로 파일에 저장되며 간단한 변환을 거쳐 조사원에게 의미 있는 이력 레코드로 디스플레이 됩니다. 또한 ERS 팀원이 파일 시스템에서 삭제된 엔트리를 조사하여, 시스템이 HISTIMEFORMAT 값을 활성화했을 경우 타임스탬프 데이터 구조가 있는 엔트리를 쉽게 복구할 수 있습니다.

이벤트 로그, 파일 타임스탬프, 또는 로그인 시간, 파일 접근 또는 수정 시간이나 패킷이 전송된 시간을 기록하는 네트워크 패킷 캡처를 연관시키는 경우를 살펴 보겠습니다. 이렇게 하면 원인이 되는 동작과 쉘 명령 이력이 있는 기록을 더욱 세밀하게 조사할 수 있습니다.

이 타임스탬핑된 활동 이력의 편리함을 설명하기 위해, 아티팩트 타임라인 분석으로 알려진 오픈 소스 도구를 이용하여 실행된 로그 및 네트워크 패킷 캡처 파일을 상관 시에 발생된 이벤트의 목록을 아래에 소개합니다.

다음 목록에서는 'VICTIMSRV'로 지정된 서버에서 루트 사용자 .history 파일을 취하여, syslog 이벤트 로그 파일, 파일 활동 타임스탬프 속성(예: 수정, 접근, 생성 및 엔트리 업데이트), 패킷 캡처에 통합하였습니다. 이 네 가지 별개 데이터 소스의 값들은 이벤트의 순서 외에 루트 사용자가 내린 명령도 정확히 알려줍니다.

```
Tue Jul 10 15:02:17 2012 Z
PCAP  192.168.100.10    - -   ICMP
packet 192.168.100.10 ->
192.168.100.12|PST8PDT|File:  KSServer.
pcap.pcap inode:1872361
HISTORY VICTIMSRV root - ping
192.168.100.10

Tue Jul 10 15:01:58 2012 Z
LOG   VICTIMSRV   - - (Linux Syslog
Log File) [Entry written] [passwd]
log event on [victimsrv] by [pam_
unix(passwd:chauthtok)] : “password
changed for tmillar “|PST8PDT|File:
secure inode:11334
FILE  VICTIMSRV   - MA.E      /etc/
shadow

Tue Jul 10 15:01:32 2012 Z
HISTORY VICTIMSRV root - passwd
tmillar
```

사용자 ID root가 사용자 ID tmillar의 비밀번호를 변경한 시간이 분명해집니다. 그 주장을 뒷받침하는 로그 엔트리 외에도, 그 시간에 수정이 이루어졌음을 나타내는 /etc/shadow 파일도 있습니다. 또한, 이력 파일 내의 입력된 명령은 그 명령이 변경 전에 내려졌다는 것을 보여줍니다. 따라서 사용자가 ping 192.168.100.10을 입력했다는 것을 쉽게 판명할 수 있으며, 다른 호스트를 사용하여 네트워크 상에서 수행된 패킷 캡처 내의 타임스탬핑된 엔트리를 이 엔트리 레코드와 세밀하게 상관시킬 수 있습니다.

쉘 이력에 타임스탬프를 추가하면 여러 이종의 정보를 간결한 이벤트의 타임라인으로 결부시킬 수 있습니다.

특히 중요한 서버일 경우 UNIX/Linux 호스트 상에 이미 이 기능이 활성화되어 있을 가능성이 있습니다. 그렇지 않을 경우, 이 권고를 고려해 보아야 합니다.

이력 파일에 타임스탬프를 활성화시키는 방법을 숙지하는 것이 포렌식 분석가에게 중요합니다. 인시던트의 조사를 착수하기 전에 활성화해 두는 것이 가장 바람직합니다. HISTTIMEFORMAT 값을 설정하면, 사용된 명령을 즉시 재호출할 수 있으므로 시스템 유지나 특이한 사건 발생 시에 규명이 한층 용이해질 것입니다.

OCOKA를 이용한 사이버 지형 평가

사이버전을 논할 때, 공격자나 방어자는 전쟁을 치를 지형을 탐색하는 것처럼 네트워크를 평가해야 합니다. 이는 접근 권한을 확보하여 데이터를 훔치거나 정보를 파괴하거나 범죄를 자행하려는 공격자와 공격자로부터 네트워크를 보호하려는 방어자 간의 전쟁입니다. 외부, 접근점(게이트웨이), 수하 및 암구어(사용자 이름 및 비밀번호 인증), 주요 지형(계정, 서버, 기밀 데이터), 감시 초소(IDS/ IPS), 지형을 점령하고 방어하는 수단(사용자, 보안) 등의 유사성을 고려할 때, 네트워크를 하나의 지형으로 간주할 수 있습니다.

비유를 하자면, 군대는 수행하는 거의 모든 것에 대한 프로세스를 보유하고 있으며 그러한 프로세스 중의 하나가 부대가 방어하거나 돌파할 지형을 평가하는 프로세스입니다. 두문자어 OCOKA(Observation, Concealment, Obstacles, Key Terrain, and Avenues of Approach)를 사용하는 프로세스를 사용하면 방어자와 공격자의 관점에서 네트워크 환경의 지형을 평가할 수 있습니다.

O	관측
C	은닉
O	장애물
K	중요 지형
A	접근 경로

O 관측

관측은 네트워크 방어자가 공격자의 활동을 관찰할 수 있는 능력이자, 공격자가 네트워크에 관한 데이터를 열람하고 입수할 수 있는 능력입니다. 관측 방법에는 주로 다음이 포함이 됩니다.

방어자

- 네트워크 로그—방화벽, IDS/IPS(Intrusion Detection/Prevention System), VPN, 프록시
- 서버 로그 파일—DNS, 도메인 컨트롤러, 안티바이러스 네트워크 콘솔
- 호스트 로그 파일—Windows 이벤트 로그, AV 스캔 로그, 방화벽 로그, Linux 접근 로그
- 애플리케이션 로그—웹, 이메일, SharePoint, FTP
- 의심스런 보안 이벤트의 "신고" 문화를 조성하는 사용자 인식 제고 교육

공격자

- 시스템 및 데이터 노출을 확인하는 조사. 이 과정에서 복구되는 정보는 인증이 필요 없는 애플리케이션 포털 및 원격 접근의 발견에서 노출된 취약점 스캔 보고서에 이르기까지 다양합니다.
- 네트워크 패킷 캡처 및 tcpdump, sn.exe 또는 유사한 프로그램을 사용하는 샘플링을 이용하여 신용카드 또는 기타 기밀 데이터가 있는 네트워크 세그먼트를 파악하거나 데이터를 캡처할 수 있습니다.
- Nmap과 여타 외부 및 내부 네트워크의 스캔을 이용하여 공격할 네트워크의 중요 부분을 파악할 수 있습니다.
- 시설에 대한 물리적 접근을 이용하여 네트워크에 관한 정보를 입수할 수 있습니다.
- 경영진과 사고 대응자의 이메일 계정 모니터링 및 손상. 이는 이메일의 계정 포워딩 규칙과 같은 간단한 방법으로 이루어질 수 있습니다.
- 로컬 관리자 계정을 이용하여 네트워크 관측 활동으로부터 계정 사용을 은닉합니다.

권고사항

방어 관측 시스템을 검증하고 모니터링 해야 합니다. 방어 관측 시스템이 효과적이려면, 적절하게 기능하고, 모니터링이 이루어져야 하며, 적절하고 계획된 대응책으로 경보에 대응해야 합니다. IBM ERS(Emergency Response Service)와 같은 사고 대응자가 인시던트 조사 중에 로깅 메커니즘이 적절하게 기능하지 않았다는 것(로그의 잦은 롤오버를 유발하는 부적절한 로그 크기나 성공 이벤트 만을 기록하는 로깅)을 발견하게 되는 경우가 흔합니다. 또는 악의적인 활동의 징후가 로그에 광범위하게 존재하지만, 로그의 모니터링이 이루어지지 않아 침입을 탐지하지 못한 경우도 있습니다. 모니터링 되는 관측 기능을 충분히 갖추면 공격을 검출할 가능성이 높아집니다. 관측 기능이나 모니터링 및 대응 기능이 거의 또는 전혀 없을 경우, 공격이 탐지되고 않고 성공을 거둘 가능성이 높아집니다.

위협에 대한 상황 인식을 확보해야 합니다. 관측 방법과 직접적인 관련이 없더라도, 방어자는 IBM XFTAS(X-Force Threat Analysis Service), FIRST, Infraguard와 같은 조직에 참여하여 최근 위협 및 공격 동향에 관한 이해를 제고해야 합니다. 이는 공격의 최근 동향에 관한 상황 인식을 제공하며 관찰되었을 때 공격 징후를 보다 효율적으로 인식하는 데 도움이 됩니다.

교육과 기능을 제공해야 합니다. 로그 조사, 악의적인 활동에 대한 내용 평가, 이벤트 및 인시던트에 대한 대응 방법을 보안 직원들에게 교육해야 합니다. 행위 관측만이 아니라 보안 관측에 적절한 관측 기능을 제공해야 합니다. 보안 직원이 네트워크 내에서 보안 이벤트에 대한 로그를 모니터링 할 수 있는 기능을 제공해야 합니다.

C 은닉

은닉은 네트워크 방어자가 네트워크 아키텍처 및 데이터, 특히 고위험군의 네트워크나 데이터를 공격자로부터 감추는 능력을 지칭합니다. 또한 공격자가 악의적인 행위를 방어자로부터 감추는 능력도 포함됩니다. 몇 가지 은닉 기법은 다음과 같습니다.

■ 방어자

- 네트워크 상의 드라이브에 저장되어 있거나 이동 중인 데이터에 대한 접근 권한을 얻으려 할 경우 키를 요구하는, 비인가 접근으로부터 데이터를 감추는 암호화.
- 호스트 이름 및 사용자 계정 이름에 예측할 수 없는 명명 규칙을 사용하여 "난독화를 이용한 보안"을 구현.
- NAT(network address translation)를 사용하여 인터넷에서 네트워크 내의 호스트를 식별하기 어렵게 만듭니다.
- OSI(Open Source Intelligence) 활동으로 악용될 수 있는 기업 및 소셜 네트워킹 사이트의 공개적으로 이용 가능한 데이터의 양을 제한합니다.

■ 공격자

- 합법적인 활동과 악의적인 활동을 조합하여 합법적인 사용자 계정을 손상시켜 악용합니다.
- 악성 트래픽을 암호화된 터널을 통해 흔히 포트 80과 같은 일반적인 목적지 포트로 전송합니다.
- 공개 인터넷 파일 공유 사이트에 업로드된 압축 파일을 이용하여 데이터를 유출합니다.
- 여러 소스 IP 주소에서 대상 네트워크에 접근하여, 실제 공격 소스를 은닉합니다.
- 로컬 관리자 계정을 사용하여, 네트워크 수준의 계정 사용 감시를 피합니다.
- 공격과 악의적인 활동 중에 안티바이러스 소프트웨어를 비활성화시킵니다.

■ 권고사항

자체 OSI 데이터 수집을 실시합니다. 소셜 네트워킹 및 기타 사이트에서 조직과 관련된 데이터를 검색합니다. 조사할 항목은 다음과 같습니다.
"직원들이 기술 포럼에 게시한 내부 네트워크 구조 및 구성에 관한 정보를 제공하는 게시물 / 취약점, 인텔리전스 정보, 훼손된 비밀번호 및 계정과 관련된 데이터가 게시된 사이트에 관한 정보 / 피싱 공격에 유용한 정보를 제공할 수 있는 회사 활동에 관한 직원들의 게시물"

비인가 통신을 식별할 수 있는 기능을 개발합니다. 포트 80과 같이 일반적으로 암호화된 통신과 무관한 목적지 포트의 암호화된 접속이나, 일반적으로 SSL과 관련이 있는 포트에 예정된 SSH 프로토콜을 식별해야 합니다.

로컬 관리자 계정의 사용을 모니터링할 수 있는 기능을 개발합니다. 공격자는 로컬 관리자 계정을 사용하여 감시로부터 자신의 활동을 숨기는 것을 선호하므로, 호스트에서 그러한 정보를 수집하고 모니터링할 방법을 개발해야 합니다. 이는 SIEM (Security Information and Event Management), syslog를 이용하거나 시스템에서 정보를 수집하는 스크립트를 갖추면 가능해집니다. 일반적인 계정 사용의 횟수 및 기간에서 벗어나는 로컬 관리자 계정 사용 패턴을 식별해야 합니다.

정상 근무 시간 외에 일어나는 정상적인 계정 사용을 식별할 수 있는 기능을 개발합니다. 다수의 공격자들은 공격 대상 시스템과는 다른 시간대에 있으며 공격자의 정상 "근무" 시간 중에 도용 계정 신임 정보를 이용하며, 시간대가 바뀌기 때문에 방어자의 "근무 외" 시간 중에 공격이 일어날 수 있습니다. 정상 활동을 패턴을 규정하고 그 패턴에서 많이 벗어나는 활동을 감시해야 합니다.

O 장애물

네트워크 방어자와 공격자는 네트워크를 성공적으로 방어하거나 공격하는 능력을 차단하거나 저해하기 위해 흔히 각자의 경로에 장애물을 배치합니다. 그러한 장애물의 일부는 다음과 같습니다.

방어자

- 복잡한 비밀번호 또는 이중 요소 인증
- 네트워크 접근 제어 목록
- 보관중인 데이터와 이동 중인 데이터의 암호화
- 사용자 인식 교육
- 침입 탐지 시스템(IDS) 및 침입 방지 시스템(IPS)
- 안티바이러스 및 기타 악성코드 스캐너
- 파일 무결성 및 모니터링 시스템

공격자

- 로그 파일 삭제
- 공격 내부의 루틴 정리—레지스트리 키를 정리하고, 프리페치 파일을 삭제하며, 악성코드 및 유출 파일을 삭제 및 겹쳐쓰기를 수행하여 악성 기능과 유출 데이터의 내용을 식별하는 활동을 저해하는 일괄처리 파일
- 합법적인 네트워크 신임 정보를 도용하고 공격자 활동을 합법적인 활동과 혼합하여 탐지 및 조사 활동을 저해
- 로컬 관리자 계정을 사용하여 네트워크 레벨에서 들키지 않을 수 있는 활동을 수행
- 공격 수행 및 악성코드 설치 중에 안티바이러스 소프트웨어를 비활성화
- 전체 파일 시스템의 삭제

권고사항

방어용 장애물을 구축합니다. 방어용 장애물의 보호 범위를 중첩시켜, 공격자가 접근권한을 얻기 전에 넘어야 할 여러 층의 장애물을 구축해야 합니다. 공격자는 흔히 방어용 장애물의 실패에 의존하여 접근권한을 확보하며, 사용자가 이메일에 첨부된 악성코드를 해쉬가 취약한 비밀번호가 보관되어 있는 시스템 상에서 실행하면 비밀번호를 쉽게 파악할 수 있는 등이 그 예입니다. 이는 내부 세그먼트화 또는 접근 제어 목록이 없는 네트워크와 암호화되지 않은 기밀 데이터에 대한 접근을 제공합니다.

공격자의 장애물을 예측하고 대책을 수립합니다. CSIRT(computer security incident response team) 내에서, "공격자가 ...한다면 어떤 조치를 취해야 할까?" 등을 자문하는 탁상 작전 시나리오를 연습합니다. 대응 "조치"뿐만이 아니라 대응 "방법"에도 주안점을 두어야 합니다. 조치가 "이러한 로그를 입수"하는 것이라면, 로그 입수를 위해 누구에게 연락을 취해야 하고, 담당자가 휴가일 경우에는 누구에게 연락을 취해야 하며, 그 당사자가 필요한 접근권한과 스킬을 가지고 있는지를 알아야 합니다. 공격자가 로컬 호스트 로그를 삭제했다면, 중앙 위치에 로그 기록이 있는지, CSIRT가 이 로그를 입수하는 데 필요한 접근권한과 스킬을 가지고 있는지를 알아야 합니다. 공격자가 광범위한 로컬 관리자 계정을 사용하여 공격을 수행하는 경우, 네트워크의 일부분 내에 로컬 관리자 계정의 수가 급증하는 경우를 식별하는 방법이 있어야 하고, 사용자 계정이 안티바이러스 소프트웨어를 비활성화시키는 경우 CSIRT가 파악할 수 있어야 하며, 그럴 경우 그것이 합법적인 활동인지 공격자의 소행이었는지를 판단하는 후속 조치가 이루어져야 합니다. 이는 공격 시에 인지하고 처리해야 할 문제의 일부 사례입니다.

K 중요 지형

중요 지형은 눈에 띄는 표적, 고가치의 표적 또는 핵심 표적이 있는 구역을 지칭합니다. 중요 지형에는 서버, 계정, 개인 등이 포함될 수 있습니다. 대고객 웹 서버가 조직을 방해하거나 공개 선언을 위한 플랫폼으로 사용하고자 하는 핵티비스트에게 눈에 띄는 표적의 일례가 될 것입니다. 상당한 가치를 지닌 표적에는 고위 경영진과 관련된 계정이나 급여 및 기타 은행 업무 또는 금융 거래에 쓰이는 시스템의 훼손이 포함될 수 있습니다. 핵심 표준으로 간주될 수 있는 네트워크 내의 구역에는 신용카드 데이터베이스, 신원 도용에 유용한 개인 정보 또는 사기 행위에 유용한 의료 정보가 들어있는 네트워크가 포함됩니다.

권고사항

중요 지형을 파악하여 적절하고 보호하고 제대로 감시합니다. 조직의 모든 중요 지형 목록을 작성합니다. 이는 도메인 컨트롤러와 같은 일반적인 고가치 표적이 될 수 있지만 조직 관리, 급여, 인적 자원, 기업 법무, 기밀 지적재산권의 위치 등과 같은 핵심 표적도 포함되어야 합니다.

피해 평가 프로세스를 개발합니다. 중요 지형이 훼손될 경우, 노출되거나 훼손된 내용, 데이터의 속성, 노출에 따른 위험 평가, 위험을 절감하기 위해 취해야 할 완화 조치의 목록을 파악해야 합니다. 완화 전략을 개인에게 할당하여 조치가 이루어지도록 해야 합니다. 이 피해 평가는 다음 표의 예와 같은 형태를 취할 수 있습니다.

파일 이름	내용의 속성	내용	위험	완화 전략	잔여 위험
Vuln_scan.txt	네트워크 보안	2010년부터의 취약점 스캔	중	취약점이 있었는지를 확인	저
Payroll.xls	HR	직원 및 은행 계정 목록	고	직원에게 통지	고
Vacations.doc	HR	직원 휴가 일정	저	없음	저
Passwords.xls	네트워크 운영	네트워크 디바이스의 비밀번호 목록	고	8 시간 이내에 비밀번호 변경; 감시 확대	중

A 접근 경로

흔히 공격 벡터로 지칭되는 접근 경로는 공격을 수행할 수 있는 메커니즘을 확인합니다. 그 중에서도, 이러한 접근 경로에는 흔히 다음이 포함됩니다.

- 악성코드나 악성 웹사이트의 링크가 포함된 사회공학적 이메일
- 인터넷 접근이 가능한 웹메일 또는 기타 원격 로그인에 대한 사전 공격 및 무차별 공격
- 애플리케이션 취약점 공격 (잘못된 구성, 버퍼 오버플로우 등)
- 비밀번호 크래킹 부트 CD를 이용하여 청소부와 같이 네트워크에 대한 물리적 접근
- 인접 기업 또는 주차장에서 접속 가능한 기업 무선 신호
- 설치된 로우그(rogue) 무선 접근 포인트
- 분산 서비스 거부(DDOS) 공격

■ 권고사항

기술 솔루션을 구현합니다. 비록 단호한 공격자가 흔히 여러 접근 경로에서 동시에 공격하거나 별개의 무관한 공격자들이 여러 접근 경로에서 동시에 공격할지라도, 강력한 보안 인식 교육, 복잡한 비밀번호, 취약점 평가 등을 통해 이러한 공격에 대처할 수 있습니다. 적절한 기술 솔루션(업데이트 패칭, 안티바이러스 소프트웨어, 안전한 방법을 이용하여 보관된 견고한 비밀번호)으로 접근 경로를 저지할 수 있습니다.

개별 사용자 솔루션을 구현합니다. 사용자가 이메일에 첨부된 악성코드를 실행하는 경우 기술 솔루션을 우회할 수 있으므로, 공격자에게 원격 접근을 허용하게 됩니다. 적절한 보안 인식 교육 프로그램을 이행하면 이러한 문제에 대처할 수 있습니다. 인식 교육의 목표는 연기를 봤을 때 소방서에 신고하는 것과 마찬가지로 보안 사고가 의심될 경우 사용자의 보안 신고를 장려하는 "신고" 문화를 조성하는 것입니다. AV 경고나 보안 문제를 "자주 유발"하는 사용자를 추적하고 직원의 안전하지 않은 행위에 대한 강제 조치를 취할 수 있습니다. 이러한 조치는 악성코드에 감염될 가능성이 적은 다른 운영 체제로의 전환에서 안전하지 않은 컴퓨팅 활동으로 인하여 공격자에게 네트워크가 자주 노출되는 행위에 대한 징벌적인 조치에 이르기까지 다양할 수 있습니다.

네트워크 방어자는 각각의 OCOKA 범주 내에서 방어 전략을 확인해야 하며 각각의 OCOKA 범주 내에서 공격자의 활동을 예측하고 대비해야 합니다. OCOKA의 모든 측면이 사용자의 행위에 영향을 받을 수 있습니다. 여러 OCOKA 부문 간의 공통적인 한 가지 권고사항은 사용자 인식 교육을 통해 위험 인식 문화를 조성하고 관리 시스템을 개발하여, 사용자들이 보안 위협을 인지하여 보고하고 적절하게 대처할 수 있도록 교육을 시키는 것입니다. 네트워크 방어자에게 OCOKA는 네트워크 지형을 평가하는 데 유용한 도구가 될 수 있습니다. OCOKA를 이용한 네트워크 지형의 평가 결과에 의거하여 보안 관리자는 네트워크의 방어 기능에 대한 보다 광범위한 상황 인식을 확보할 수 있으므로, 공격에 대한 대비, 방어, 대응의 효율성을 제고할 수 있습니다.

외부 침입 감지를 이용한 파일 전송 위험의 제거

공중 경보망의 중심에는 이제 데이터 보안이 자리하고 있습니다. 지난 18개월 동안 정부, 의료, 금융 서비스 등의 다수 부문에서 세간의 이목을 끈 데이터 유출 사건이 여러 차례 있었습니다. 2012년 6월까지, 214건의 보고된 유출을 통해 850만 건 이상의 레코드가 유출되었습니다.[19] 이러한 유출은 소비자들에게 직접적인 영향을 미치기 때문에 널리 알려졌지만, 이 데이터가 데이터 유출의 전모를 보여주는 것은 아닙니다.

Symantec이 후원하고 Ponemon Institute가 실시한 2011년도 데이터 유출에 따른 비용손실 조사에 따르면 미국의 데이터 보안 침해에 따른 비용손실이 침해 건당 720만 불이었던 2010년도에 비해 24% 감소한 550만 불이었습니다.[20] 기업은 전반적인 보안을 인식하고 있지만, 파일의 보안 상태는 어떠할까요?

회사를 어떻게 보호할 것인가, 회사의 어느 부분을 보호해야 하는가, 방화벽이 충분한가, 시스템의 바이러스 스캔은 충분한가 등은 기업이 일상적으로 접하는 문제입니다.

보안에 관한 문제는 여러 가지가 있지만, 최근에 들어서야 CIO와 기업 보안 책임자들이 B2B(business to business) 및 파일 전송 보안을 인식하게 되었습니다.

매일 수십 억 건의 파일이 보안에 대한 의식이 거의 없이 인터넷 상에서 전송되고 있습니다. 직원들은 일상적으로 기밀 정보를 이메일로 전송합니다. 기업은 직면할 수 있는 잠재적 문제를 전혀 고려하지 않고 내부 네트워크 상에서나 기업 외부로 기밀 데이터를 전송합니다.

19 Identity Theft Resource Center, 2012년 데이터 유출 통계, 2012년 7월 3일, http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202012.pdf

20 Ponemon Institute, 2011년 미국 데이터 유출 비용손실 조사, 2012년 3월, Symantec 후원, http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf

지난 40여 년간, 일종의 파일 전송 프로토콜(FTP)이 개인 간 또는 기업 간 파일 전송의 표준 수단이었습니다. FTP는 TCP/IP보다 훨씬 이전에 개발되었지만 지금도 그 기본 형태가 크게 변하지 않았습니다. FTP는 지점 간 또는 시스템 간 파일 전송 수단을 제공했지만, 40년 전에는 지금처럼 보안을 우려하지 않았습니다. 이 프로토콜은 네트워크 상에서 비밀번호와 데이터를 평문으로 전송하기 때문에 안전하지 않다는 점이 잘 알려져 있습니다.

프로토콜 자체의 문제 외에도, 다수의 파일 서버는 보호되지 않은 공격에 취약한 상태입니다. 지난 40년간, SFTP(SSL을 이용하는 FTP), FTP/S(SSH 상의 FTP), HTTP, HTTPS(SSL을 이용하는 HTTP)와 독점 및 공개 형태의 여러 다른 메시징 및 파일 전송 프로토콜이 추가되면서 파일 전송 분야에 상당한 발전이 있었습니다. 안전한 보안 프로토콜이 출현했음에도 불구하고, 여전히 보안 문제는 존재합니다.

분석가들의 예측에 따르면, 2015년에 B2B 시장의 연간 매출 규모가 22억 2000만 불[21]에 달하고 MFT(Managed File Transfer) 시장 규모는 24억 8000만 불[22]에 달할 것이라고 합니다.

기업은 변화의 시대에 적응하고 있으며, 세상도 마찬가지입니다. 파일 전송의 보안을 유지하려는 기업이 점점 늘면서, 강력한 파일 전송 보안 전략의 필요성이 대두되고 있습니다. 연간 수백만 건의 파일이 기업에서 송수신되는 상황에서, 데이터의 보안을 확보하는 전략을 갖추는 것은 매우 중요합니다.

MFT 시장의 성장과 더불어 임시 방식으로 파일 및 데이터를 전송하는 새로운 방식이 나타났습니다. 지금의 임시 파일 전송에 두드러진 한 가지 분야는 Dropbox와 같은 클라우드 파일 스토리지 제공자입니다. 퍼블릭 클라우드 서비스는 대규모 데이터 센터에 수용되어 있는 가상 폴더에 파일을 업로드하여 보유할 수 있는 수단을 제공합니다. 편리성이 이러한 서비스의 가장 주된 동인이겠지만, 보안 수준은 엔터프라이즈급 표준에 못 미치는 경향이 있습니다.

다수 벤더들이 기존의 MFT 솔루션과 보안 수준이 동등한 엔터프라이즈급 임시 솔루션을 제공하면서 임시 방식의 문제 해결에 나섰습니다. 이들은 엔터프라이즈 보안 및 MFT 애플리케이션이 통합된 신제품을 출시하면서 명확한 외부 보안을 제고하고 있습니다.

외부 침입 탐지

외부 침입 탐지는 새로운 개념이 아니지만, 아직 널리 구현되어 있지 않습니다. Ponemon Institute가 실시한 데이터 보호의 모범 사례 조사 결과에 의하면, 718명의 IT 및 IT 보안 종사자의 55%가 이동 중인 데이터의 보안을 관장하는 공식적인 전략이 결여되어 있다고 응답했습니다.[23] 대기업과 파일을 송수신하고 있는 거래 파트너가 수 천에 달할 수 있다는 점을 고려할 때, 이는 깜짝 놀랄만한 통계입니다. 나머지 응답자 45% 중의 대다수는 매우 엄격한 보안 요구사항에 직면해 있는 금융 기관이며 기밀 정보를 취급하는 업계일 가능성이 높습니다.

파일 및 기밀 정보를 취급할 때 귀사는 얼마나 안전합니까? 전략을 갖추고 있습니까? 이 문제에 대하여 어떤 조치를 취할 수 있습니까?

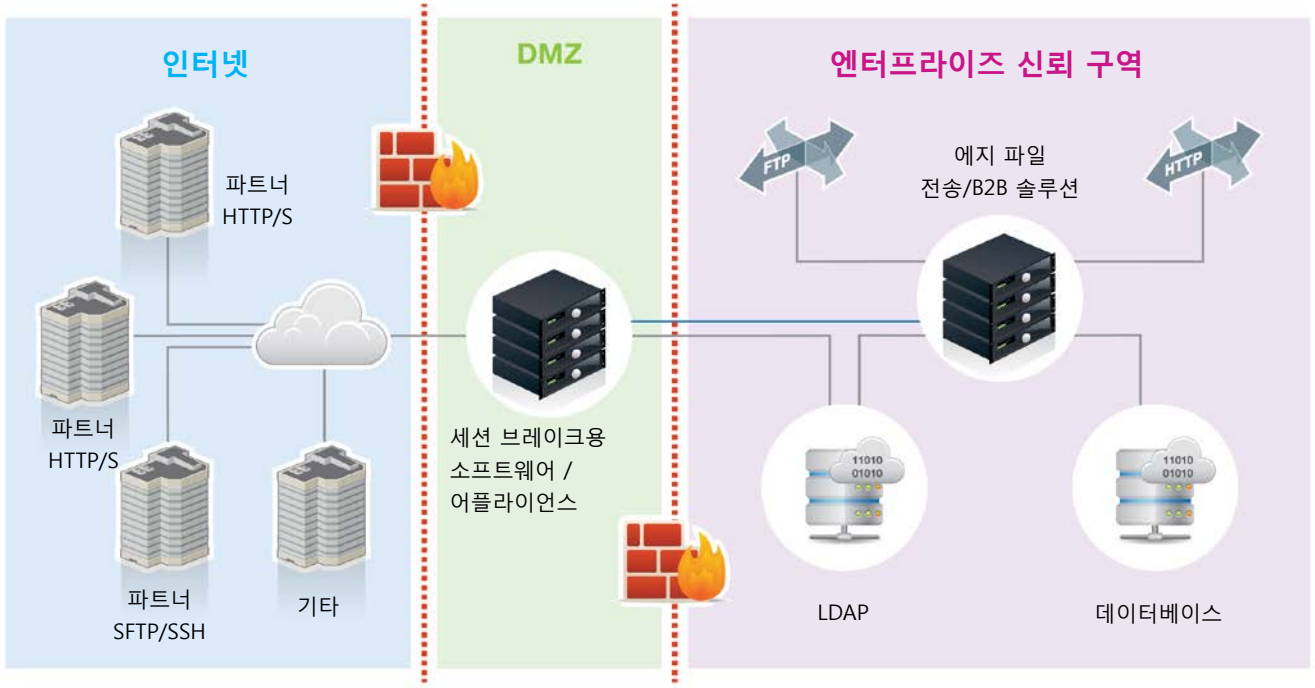
귀사는 외부 보안에 대한 전략을 갖추고 있습니까? 아니라면, 그 이유는? 다음 단계는 무엇입니까? 이러한 것들이 기업과 업계에 무엇이 바람직한지를 판단할 때 답해야 하는 질문입니다. 한 기업에 적절한 것이 다른 기업에는 적절하지 않을 수 있습니다.

21 IDC, 전세계 B2B 미들웨어 시장 2011-2015년 예측, 2011년 8월
22 Ken Vollmer, Forrester Research, 시장 개요: MFT(Managed File Transfer) 솔루션, 2011년 7월
23 Ponemon Institute, 데이터 보호의 모범사례: 미국 IT 및 IT 보안 종사자 조사, 2011년 10월, McAfee 후원, http://www.mcafee.com/us/resources/reports/rp-ponemon-data-protection-full.pdf

트래픽이 주로 대용량 파일인지 아니면 실시간으로 전송될 것으로 예상되는 대량의 소규모 파일을 수신해야 하는지, 보안 및 IT 거버넌스 팀이 협력하여 파일 전송 요구사항을 결정하는 것은 어떤 기능이 필요하며 어떤 종류의 배치에 투자해야 할지를 결정하는 첫 단계입니다.

파일 전송을 취급할 때 배치해야 할 보안의 종류에 대한 정의는 여러 가지가 있지만, 대다수의 벤더들이 프로토콜을 생각하지 않고 단순히 파일을 전송하는 것만으로는 더 이상 충분하지 않다는 점에 동의하고 있습니다. 외부 보안과 DMZ(Demilitarized Zone) 모범 사례의 개념은 서로 다릅니다. 일부 벤더들은 IP 세션 브레이크와 인증/신뢰 구역의 인증을 제공하는 반면에, 다른 벤더들은 DMZ의 바이러스 스캐닝이 가능한 데이터베이스를 갖춘 강화된 어플라이언스를 제공하고 있습니다. 배치 메커니즘이 무엇이든, DMZ 기반 프록시에서 엔터프라이즈 신뢰 구역의 개방 포트의 수를 줄이는 것이 가장 중요합니다.

모범 사례 구현의 예



모범 사례

모든 기업에 완벽한 단일 솔루션은 없지만, DMZ 기반 프록시 솔루션의 조사 중에 검토해야 할 기능이 다수 있습니다. 일부 솔루션은 고속 저지연 전송에 최적화되어 있는 반면에 다른 솔루션은 대용량 파일 전송에 최적화되어 있습니다. 파일 전송 요구사항과 유스 케이스가 무엇이든, 다음과 같은 모범 사례를 고려해야 합니다.

데이터 보호

- SSL(secure sockets layer) 및 TLS(transport layer security) 프로토콜을 사용합니다.
- DMZ(Demilitarized Zone)에 데이터를 저장하지 않습니다.
- 암호 해독 및 암호화에 관한 업계 및 법적 지침과 요구사항을 파악하고 그 지침 및 요구사항을 준수합니다.
- 암호 키 스토리지에 HSM(Hardware Security Module)을 사용합니다.

외부 보안

- DMZ 기반 프록시를 사용하여 DMZ의 IP 및 SSL 세션을 종료시켜, 공개 인터넷에서 신뢰 구역으로 직접적인 포트 접근을 차단합니다.
- 인바운드 및 아웃바운드 방화벽 포트 접근을 최소화합니다.
- DLP(Data Loss Prevention) 솔루션을 배치합니다.
- 멀티티어 DMZ 구조를 배치합니다.
- 인라인 바이러스 스캔 또는 ICAP(Internet Content Adaptation Protocol)를 제공합니다.

인증

- 신뢰 구역이 아니라 DMZ에서 인증합니다.
- 다중 요소 인증을 사용합니다.
- 역할 기반 접근을 제공합니다.

각각의 모범 사례는 완벽한 외부 보안의 제공에 필수적인 요소들입니다.

벤더들은 새로운 배치 방법을 적극적으로 개발하여 지원 프로토콜의 범위를 확대하고 있으며, 고객이 안전한 보안 방식으로 접속할 수 있는 기능을 제공하고 있습니다. 또한, 외부 보안에 가장 적합한 솔루션을 제시하기 위해 많은 노력을 기울이고 있습니다. 하지만 방화벽 만으로는 더 이상 충분하지 않으며, 시스템 상의 바이러스 스캔이 최상의 엔터프라이즈 보호가 아님은 분명합니다.

모범 사례 목록에 있는 모든 기능을 제공할 수 있는 단일 외부 프록시 솔루션은 없습니다. 시장이 지속적으로 더 강력한 보안을 요구하면서 벤더들이 자사 오퍼링을 개선하고는 있지만, 여전히 격차가 있습니다. 여러 벤더 및 공개 인터넷과 접속되어 있는 환경을 고려할 때, 가장 취약한 부분인 파일 보안은 최우선순위가 되어야 합니다. 엔터프라이즈 보안 계획의 결점을 파악하여 어떤 솔루션이 외부 보안에 가장 적절할지를 판단하는 것은 각 기업의 몫입니다.

단원 III
소프트웨어 개발 환경 보안 현황

이 단원에서는 소프트웨어 개발 과정의 보안 문제를 해결하는 절차와 방법을 설명합니다. 또한 기업이 기존 취약점을 찾아내고 새로운 취약점이 추가로 발생하는 것을 막는 방법에 대해서도 논의합니다. 네트워크 또는 웹 애플리케이션을 이용하여 기밀 데이터를 수집하거나 교환하는 보안 전문가라면 특히 유용한 정보가 될 것입니다.

이메일 비밀번호—개인 온라인 ID의 단서

이메일 비밀번호의 중요성

현재 웹을 사용하는 모든 사용자에게, 이메일 주소는 온라인 ID의 가장 중요한 부분입니다. 받은 편지함은 개인 이메일, 사진과 정보가 담긴 개인 보관함 이상의 의미를 가집니다. 웹사이트에 가입할 때, 이메일 주소와 비밀번호는 중요한 데이터의 일부입니다. 악의적인 의도를 가진 공격자가 이 두 가지를 모두 입수할 경우, 방심하고 있는 사용자에게 막대한 문제를 초래할 수 있습니다. 현재 웹 상의 대다수 사용자가 이 위험을 인식하지 못하고 스스로를 보호하는 간단한 조치조차 취하지 않고 있습니다. 더욱이, 웹메일 및 기타 온라인 포털은 비밀번호 복구 허용하는 구식 방법을 채택하고 있어, 이를 악용하는 공격자들이 지속적으로 늘고 있습니다.

또 다른 침해의 유발

그렇다면 어떻게 비밀번호가 모든 사람들이 볼 수 있도록 인터넷 상에 노출될까요? 이는 우리가 매일 뉴스에 접하는 모든 보안 침해의 직접적인 결과입니다. 공격자들이 웹사이트에서 최대한 많은 사용자 이름과 비밀번호를 훔쳐 공개적으로 게시하는 것이 이제는 일종의 게임이 되었습니다. 지난 6개월만 하더라도, 수백 만 건의 이메일 주소와 비밀번호가 그런 식으로 공개되었습니다.

일단 유출되고 나면, 해싱 함수를 이용하여 암호화된 비밀번호일지라도 사전 기반 무차별 방식이나 이미 존재하는 공통 비밀번호의 표와 해쉬 값의 검색을 통해 평문으로 쉽게 복구될 수 있습니다.

비밀번호가 중요한 이유

최근 보안 침해 데이터에 의하면, 다수의 사용자들이 인터넷 상의 여러 웹사이트에 동일한 비밀번호를 사용하고 있는 것으로 나타났습니다. 임의의 웹사이트가 공격당했을 경우, 공격자는 흔히 찾을 수 있는 모든 이메일 주소와 비밀번호의 목록을 헐값에 팔아버립니다. 이메일 주소가 Gmail.com, yahoo.com 또는 hotmail.com일 경우만 하더라도 상황이 매우 나쁩니다. 이메일 주소가 .gov 도메인이나 회사 도메인에 속한 경우라면 어떨까요? 최종 사용자의 이메일과 비밀번호가 유출되고, 기업 자원에 사용하는 비밀번호와 동일할 가능성이 실재한다면 얼마나 당혹스러울까요? 여러 종류의 기업 및 개인 자원에서 일반적으로 동일한 비밀번호를 사용할 가능성이 높습니다. 여러 가지 비밀번호를 사용하는 것이 바람직한 방식이지만, 비밀번호가 충분히 복잡하지 않거나 암호화되지 않은 형태로 저장되어 있을 경우에는 여전히 불행을 유발할 수 있습니다.

공격자가 취할 수 있는 다음 행동

이메일 주소와 비밀번호가 공개적으로 게시되고 나면, 의도를 가진 모든 공격자가 게시된 비밀번호를 이용하여 이메일 계정에 로그인하려는 시도를 할 수 있습니다. 인기 있는 사이트의 다수는 그러한 무차별 공격을 방지하는 노력을 거의 기울이지 않고 있습니다. 누군가가 사용이 가능한 비밀번호를 발견한 후에 공격자가 취할 행동은 그 계정에 무엇이 링크되어 있느냐에 따라 달라집니다. 공격자는 사용자의 모든 사적인 이메일을 읽어보거나 사진을 훑어보거나 그 사용자의 계정을 이용하여 다른 사용자에게 스팸 메일을 발송할 수 있습니다. 더 심각한 경우, 공격자가 사용자의 온라인 뱅킹, 쇼핑 계정 또는 신용카드를 마음대로 사용하는 상황에 처할 수도 있습니다. 사용자가 어디에 살고 있으며, 어떤 은행과 거래하고 어떤 물품을 온라인에서 구입하는지를 알 수 있습니다. 누군가 ID를 도용하기에 충분한 정보가 있습니다.

비밀번호를 잊어버리셨습니까? 재설정하려면 여기를 클릭하세요

대다수 사용자 기반 웹사이트들은 일종의 비밀번호 복구 메커니즘을 갖추고 있습니다. 대체로, 사용자가 비밀번호를 변경할 수 있는 링크를 이메일로 사용자에게 발송하는 것이 일반적인 방식입니다. 공격자가 이미 사용자의 이메일 계정에 액세스했다면, 이는 엄청난 보안 위험입니다. 전자 상거래, 금융 서비스, 소셜 네트워크 등의 모든 서비스가 그 이메일 주소와 연관되어 있는 경우라면, 이 모든 사이트가 비밀번호를 변경할 수 있는 링크를 기꺼이 이메일로 송부해줄 것입니다. 일부 사이트는 현재 추가 단계를 채택하여 비밀번호 변경을 좀 더 어렵게 만들어 두고 있지만, 대다수 사이트는 단지 링크를 클릭하면 변경이 가능합니다. 이제 악의적인 의도를 가진 공격자가 사용자의 계정에 액세스했다면, 사용자에게 실제로 금전적인 손해를 입힐 수 있습니다. 대다수 사용자들은 전자 상거래 사이트에 물품 구매가 간단하도록 신용카드 상세 정보를 등록해 두고 있습니다. 일부 온라인 서비스의 경우에는, 공격자가 다른 은행에 송금할 계좌를 개설할 수도 있습니다. 물론 누군가 신규 계좌를 개설했다는 경고가 이메일로 송부될 수도 있겠지만, 이미 이메일 계정이 훼손되었고 공격자가 그 이메일을 삭제할 수 있다면 아무런 소용이 없을 것입니다.

"여러 사이트에 동일한 비밀번호를 사용하지 않아야 합니다"

동일한 비밀번호를 사용하지 말라는 조언을 이미 모두가 들어보았을 것입니다. 비밀번호 관리 도구를 이용하여 모든 사이트마다 비밀번호를 달리 할 수도 있습니다. 온라인 뱅킹과 같은 보안 사이트와 그다지 안전하지 않은 사이트의 비밀번호를 달리 해야 한다고 말하는 이도 있습니다. 이는 매우 유용한 제안이지만, 실천하기가 어렵습니다. 금융 사기는 최종 사용자에게는 매우 번거롭지만, 사적인 비밀번호를 엔터프라이즈 시스템에 재사용하는 경우가 많다는 것을 잊지 않아야 합니다. 신임 정보의 재사용으로 인해 지적재산권을 도난 당했을 경우의 손실 규모를 생각해 보아야 할 것입니다. 당연히 이 시나리오에서는, 계층 보안 방식을 사용하여 잠재적 피해를 완화/최소화할 것을 IBM X-Force는 권고합니다.

규칙 및 규정 대 현실 세계

비밀번호에 관한 기업 보안 정책이 아무리 엄격하든지, 사용자들은 대부분 최소한의 정도만 준수합니다. 비밀번호를 변경해야 할 때마다 1, 2 또는 3으로 끝이 나는 비밀번호로 변경하는 경우가 대부분이며, 그것이 인간의 본성입니다. 그 이면의 이유를 이해하지 못할 경우, 실천할 가능성이 낮아집니다. 공격자들이 얼마나 간단하게 사용자의 금전을 강탈할 수 있는지에 관한 사용자 교육을 실시하여 비밀번호 관리의 중요성에 대한 인식을 제고시켜야 합니다. 그러면 사용자들이 앞으로 보안을 훨씬 더 중요하게 여길 것이며, 이는 모두에게 바람직합니다.

안전한 비밀번호란?

보안 전문가에게 강력한 비밀번호란 어떤 구성인지를 물어 보면, 그 대답은 십인십색일 것입니다. 암호구로 더 널리 알려져 있는 아주 긴 비밀번호를 지원하는 추세가 점차 늘고 있습니다. 암호구는 단지 단어의 조합이거나 하나의 완전한 문장입니다. 간단히 말하자면, 비밀번호가 길수록 크랙하기가 어렵습니다. 통계적으로, 10자리의 비밀번호는 특수 문자의 수에 상관없이, 임의의 단어로 이루어진 30자리 비밀번호만큼 안전하지 못합니다. 암호구를 사용하면 복잡하게 뒤얽힌 문자, 숫자, 특수 문자의 조합보다 기억하기가 쉬워집니다.

"MyPasswordIsNowSuperSecure"를 "4K4$!lvabQ!"와 비교해 보면 얼마나 기억하기 쉬운지를 알 수 있을 것입니다. 긴 비밀번호는 일반적으로 짧은

비밀번호를 능가한다는 점을 명심해야 합니다. 비밀번호를 기억하기 위해 메모지에 적어두어야 한다면, 비밀번호에 대한 접근방식을 변경해야 할 시점입니다. 어렸을 때 좋아했던 노래 제목의 변형을 만들거나, 자신이 이해할 수 있는 몇 가지 임의 단어를 조합하거나, 임의 문장을 찾아낸 다음 몇 분 더 시간을 할애하여 몇 가지 임의 문자를 추가하면 (일부 기호를 혼용하거나, 일부 문자를 대문자로 쓰거나, 숫자를 여기 저기에 섞으면) 기억하기 쉽고 매우 안전한 비밀번호가 됩니다.

실례

이 프로세스의 일례는 "One Eyed One Horned Flying Purple People Eater"라는 시구에서 비롯됩니다. 이는 비교적 긴 구문이지만 기억하기 쉽습니다. "one"을 "1"로 바꾸면 "1eyed1hornedflyingpurplepeopleeater"라는 짧은 비밀번호를 만들 수 있습니다. "purplepeopleeater"를 "PPE"로 교체하면 "1eyed1hornedflyingPPE"가 됩니다. 조심해야 할 사이트라면, 끝에 "!"를 추가하여 부가적인 효과(및 보안)를 거둘 수 있습니다. 최종적으로 "1eyed1horendflyingPPE!"는 22자가 되며 대문자, 소문자, 숫자, 기호가 섞여 있습니다.

비밀번호 기억 방법

각각의 온라인 계정마다 다른 비밀번호를 사용하려면, 종이에 적어두지 않고 모든 비밀번호를 계속 기억할 수 있는 수단이 필요합니다. 이 경우에 비밀번호 관리 도구가 유용하며, 다양한 종류의 도구를 이용할 수 있습니다. 그 중의 일부는 마스터 비밀번호로만 열 수 있는 암호화된 로컬 파일에 비밀번호를 보관합니다. 파일을 클라우드에 보관하여 브라우저 플러그인을 이용하면 이 작업이 간단하고 용이해집니다. 어떤 방법을 사용하든, 강력한 형태의 암호화(예: AES-256)를 지원해야 하며 마스터 비밀번호는 사실상 긴 '암호구'여야 합니다. 위의 단계를 사용하여 안전한 암호구를 생성하면, 로그인하는 웹사이트마다 임의의 비밀번호를 생성하는 안전한 방법을 확보하게 됩니다.

보안 질문

이메일에 관한 또 다른 보안 위험은 보안 질문입니다. 다수 웹사이트가 보안을 강화하기 위한 일환으로 채택한 종종 필수 필드가 있는 보안 질문이 실상은 보안을 약화시켰습니다. 이러한 질문의 다수가 공격자들이 5분 정도의 검색으로 알아낼 수 있는 답을 가지고 있습니다. 고등학교의 마스코트, 출생도시, 생일 등이 모두 취약한 "보안" 질문입니다.

보안을 유지하길 원한다면, 이러한 질문에 거짓 데이터로 답하는 것이 가장 바람직합니다. 하지만 거짓 보안 질문이 아니라, 안전한 비밀번호와 비밀번호를 기억할 수 있는 비밀번호 관리 도구를 활용하는 것이 바람직합니다.

이중 요소 인증

위에 언급한 조치들이 이메일을 안전하게 지키기 위한 노력에 많은 도움이 되지만, 보안을 더 강화하고 싶다면 이중 요소 인증을 제공하는 이메일 서비스 제공자를 찾아야 합니다. 일부 서비스는 로그인 프로세스의 마무리에 필요한 6자리 코드를 생성하는 스마트폰 앱을 제공하고 있습니다. 그 외 다른 오퍼링은 사용자의 전화로 SMS 코드를 전송합니다. 어떤 경우든지, 이메일에 액세스하기 위한 보조 정보가 사용자의 전화기에만 존재합니다. 또한 사용중인 컴퓨터를 기억하는 기능을 제공하므로, 로그인할 때마다 코드를 입력할 필요가 없습니다. 하지만 새로운 컴퓨터나 전에 사용한 적이 없는 컴퓨터에서 로그인할 경우에는 코드를 입력해야 합니다. 이러한 방식은 가정의 컴퓨터에서 이메일에 액세스하는 것은 안전하고 쉬운 반면, 생소한 컴퓨터(잠재적으로 악의적인 컴퓨터)에서 접속해야 하는 경우에는 추가 보안 코드를 요구함으로써 보안을 강화합니다.

종합

받은 편지함이 얼마나 중요한지, 공격자들이 얼마나 쉽게 이메일 계정에 대한 접근권한을 확보할 수 있는지, 액세스한 다음에는 얼마나 막대한 피해를 초래할 수 있는지를 살펴 보았습니다. 가장 바람직한 것은 로그인하는 모든 사이트에 임의 비밀번호를 사용하는 것입니다. 임의 비밀번호를 사용할 경우, 유용한 도구들이 다양하게 있습니다. 5분 정도의 시간을 내어 암호구를 만들어야 하며, 이 암호구를 이메일에만 사용해야 합니다. 비밀번호 관리자를 사용하는 경우라면, 이 비밀번호를 마스터 비밀번호로 사용하고, 비밀번호 관리자를 사용하여 이메일 전용의 길고 복잡한 비밀번호를 생성해야 합니다. 부가적인 보안이 필요하다면, 이중 요소 인증을 제공하는 이메일 서비스 제공자를 찾아야 합니다. 이메일 계정의 비밀번호가 무엇인지를 알 수 없도록 하고, 비밀번호 관리자를 이용하여 그 비밀번호를 기억해야 합니다.

안전한 비밀번호 해싱—빠르다고 좋은 것만이 아닌 경우

느린 것이 더 나은 경우

기술이 빠른 속도로 발전하고 있는 가운데, 사람들은 빠른 것이 항상 좋다는 믿음을 가지게 되었습니다. 대부분의 경우 이는 사실이지만, 느리다고 해서 바람직하지 않은 것만은 아니라 더 안전할 수 있다는 컴퓨터 유스 케이스가 있습니다. 바로 비밀번호를 검증하고 데이터베이스에 저장하는 방식입니다.

근래에 X회사의 데이터가 유출되어 수천(또는 수백만)의 사용자 이메일 주소와 비밀번호가 누구나 볼 수 있는 곳에 공개적으로 게시되었다는 보도가 끊이질 않고 있습니다. 흔히 이 유출된 비밀번호가 평문으로 저장되어 있는 것이 아니라 해쉬되어 있어, 실제 비밀번호가 보이는 것이 아니라 긴 암호화된 문자열로 보인다는 점은 그나마 다행입니다.

이 방식이 평문의 강력한 비밀번호보다 훨씬 더 안전할 것 같아 보이시나요?

전혀 그렇지 않습니다.

해쉬는 단방향 암호화입니다. 비밀번호와 같은 텍스트의 문자열이 해쉬 함수를 거치면, 원문이 수리적으로 변환되어 표시되는 새로운 고유한 문자열을 얻게 됩니다. 단방향은 최종 해쉬를 원문으로 되돌릴 수 없음을 의미합니다.

웹 개발자들은 비밀번호를 해싱하여 데이터베이스에 저장하고 이 해쉬를 적절하게 "솔팅"(Salting) 처리하는 등의 보안 모범 사례를 따르는 것이 바람직합니다. 패스워드 솔팅에 관해서는 잠시 후에 살펴보도록 하겠습니다. 일반적으로 비밀번호 해싱은 웹사이트 소유자일지라도 평문으로 된 사용자의 비밀번호를 쉽게 볼 수 없도록 보안 계층을 추가합니다. 이는 데이터베이스를 스누핑하는 공격자가 비밀번호와 이메일 주소를 입수하여 동일한 비밀번호를 사용하는 다른 사이트에 대한 접근권한을 확보할 수 없게 하므로, 여러 사이트에 동일한 비밀번호를 사용하는 사용자에게 매우 중요합니다.

12345와 같이 매우 취약한 비밀번호의 예를 들어보겠습니다.

PHP MD5 함수(사용자 비밀번호 저장에 널리 쓰이는 사용이 간편한 해싱 도구)을 사용하여 해쉬 값을 산출하면, 다음과 같은 MD5 해쉬를 얻을 수 있습니다.

```
827ccb0eea8a706c4c34a16891f84e7b
```

이는 상당히 복잡해 보이며 어떤 식으로든 원문을 드러내지 않습니다. 하지만 간단한 웹 검색으로 알 수 있듯이, 원래의 비밀번호 텍스트가 그 결과로 바로 표시됩니다.

보안 침해의 경우에 웹사이트가 MD5 해쉬를 사용하고 있고 이 비밀번호를 사용하는 사용자가 있다면, 간단한 웹 검색으로 수 초 내에 그 텍스트를 찾을 수 있습니다.

이는 지나치게 단순한 예이지만, 최근에 공개된 데이터 유출의 실제 해쉬를 보면 사용자들이 웹 서비스에 대한 액세스 보안에 이와 같은 비밀번호를 사용하고 있는 것으로 나타났습니다.

웹사이트나 서비스가 사용자에게 더 복잡한 비밀번호를 사용할 것을 요구하면 도움이 될 수 있는 바람직한 사례겠지만, 단일 솔루션만으로는 효과를 기대할 수 없습니다. 비밀번호 유추에 쓰이는 하드웨어의 속도에 따라 해싱 함수를 실행하는 소요 시간의 차이만 있을 뿐, 한층 복잡한 텍스트와 해쉬도 즉시 해석될 수 있습니다.

고려해야 할 옵션

웹 개발자가 비밀번호를 보다 안전하게 보관하려면 어떻게 해야 할까요?

몇 가지 가능한 방법은 다음과 같을 것입니다.

- 동일한 해싱 함수를 여러 차례 실행합니다.
- 비밀번호/원문을 한층 복잡하게 만듭니다.
- 저속 해싱 함수를 사용합니다.

해쉬의 해쉬

암호화를 여러 차례 실행하는 것이 원래의 비밀번호를 판독하기 어렵게 만들고 되돌리기 어렵게 만드는 한 가지 방법입니다.

비밀번호 12345를 다시 예로 들면, MD5 해쉬(827ccb0eea8a706c4c34a16891f84e7b)를 산출한 다음 MD5 함수를 재실행했을 때 이 문자열의 해쉬는 다음과 같이 됩니다.

1f32aa4c9a1d2ea010adcf2348166a04.

이 해쉬는 새로운 계층의 보안이 추가된 것으로 보이지만, 마찬가지로 간단한 웹 검색으로 12345임을 알아낼 수 있습니다.

원칙적으로는 이 과정을 단 한차례만 더 수행할 것이 아니라 여러 차례 반복하는 것이 효과적인 방법이 될 수 있습니다. 하지만, 고려해야 할 문제가 또 있습니다.

첫째는 두 가지 다른 소스 문자열이 동일한 해쉬를 생성하는 충돌의 개념과 관련이 있습니다. 가능성은 있지만 (이론적으로나 실제로 입증된 일부 해쉬 함수가 있지만), 이는 본 논의의 범위에 속하지 않습니다.

또한, 해쉬 문자열의 해쉬 값 산출이 텍스트 비밀번호의 해쉬를 산출하는 것보다 수리적으로 더 제한적일 가능성이 높습니다. 암호화에서는 이를 패스워드 엔트로피라고 합니다. 패스워드 엔트로피를 언급할 때, 비밀번호의 길이 외에도 사용할 수 있는 다양한 문자, 숫자, 기호가 고려됩니다. 따라서 해쉬를 해싱하는 방법에 의존하는 방식은 정해진 엔트로피로 한정되며, 이는 반복 횟수와는 관계가 없습니다.

패스워드 엔트로피의 산출 방법을 보여주는 유용한 자원이 온라인 상에 많습니다.[24] 핵심은 주어진 소스 문자열의 엔트로피 비트가 클수록 모든 가능한 조합의 무작위 유추에 더 긴 시간이 소요된다는 것입니다.

32개의 16진법 문자로 이루어진 MD5 해쉬의 엔트로피는 128 비트입니다. 지금의 연산력으로도 모든 조합을 유추하려면 긴 시간이 소요될 것입니다. 그러나, 해쉬는 항상 128 비트의 엔트로피로 고정되어 있는 반면에, 소스 비밀번호나 암호구는 해쉬에 비해 더 높은 엔트로피를 가질 수 있습니다. 하드웨어의 속도가 지속적으로 향상되어 모든 조합의 유추에 소요되는 시간이 단축된다 할지라도, 시간이 지나면서 엔트로피를 높일 수 있는 함수가 최상의 솔루션이 될 것입니다.

논리적인 결론은 높은 엔트로피를 확보할 수 있도록 비밀번호가 아주 길어야 한다는 점입니다.

24 패스워드 엔트로피: http://pthree.org/2011/03/07/strong-passwords-need-entropy/

더 복잡한 비밀번호

안전한 비밀번호의 선택 방법에 관하여 자세하게 살펴보았습니다. 자세한 정보는 "이메일 비밀번호의 중요성"을 참조하시기 바랍니다. 다수의 기업과 웹사이트가 강력한 비밀번호 정책을 시행하고 있습니다. 이는 특히 널리 알려진 비밀번호 유추를 방지하는 데 바람직한 사례이지만, 완벽한 솔루션은 아닙니다.

소프트웨어 측면에서 또 다른 권장 보안 사례는 비밀번호를 해싱하기 전에 비밀번호에 솔트(salt) 값을 추가하여 데이터베이스에 저장하는 것입니다. 솔트는 해싱 처리를 하기 전에 비밀번호에 결합시킨 무작위 문자열과 같은 추가 요소입니다.

솔트 값을 추가하면 (길이와 무작위성을 높여) 비밀번호의 엔트로피가 증가할 뿐만 아니라, 레인보우 테이블(Rainbow Table)이라는 미리 산출된 검색 데이터베이스의 사용이 제한됩니다. 유감스럽게도 지난 해에 패스워드 솔팅을 사용하지 않은 도매 유통업체의 사용자 레코드가 유출된 사건이 있었습니다.

해쉬의 웹 검색 자체가 일종의 레인보우 테이블 검색(보다 구체적으로 말하면, 공통 단어 및 구문의 대규모 레인보우 테이블을 유지하는 사이트에 대한 링크와 인덱스)이 됩니다. 레인보우 테이블 생성은 수많은 비밀번호의 가능한 조합에 대하여 해싱 알고리즘을 실행하고 추후 사용을 위해 그 결과를 보관하는 것만큼 간단합니다. 6개의 소문자와 같이 엔트로피가 낮은 비밀번호의 경우, 모든 가능한 해쉬에 대한 검색 표를 수 분내로 생성할 수 있습니다. 따라서 검색 표에 존재할 경우, 단지 대조만 하면 해쉬를 복구할 수 있습니다.

각 비밀번호에 무작위 텍스트(솔트)를 추가하면 이 값이 레인보우 테이블에 존재할 가능성이 낮아집니다.

이전 예의 비밀번호 12345를 사용하여, 무작위 솔트 문자열을 다음과 같이 추가하면,

```
'12345'
+'GlpQclJDRqYGeHi5PeRbg0oMHFlhNnBa'
```

MD5 해쉬가 다음과 같이 됩니다.

```
09f60edb0aa088d50d0482c7ba745059.
```

이 해쉬를 레인보우 테이블 검색에서 찾아보더라도, 발견할 가능성은 거의 없습니다.

기존의 미리 산출된 레인보우 테이블에는 이 문자열의 해쉬가 저장되어 있을 가능성이 낮습니다. 하지만 데이터베이스가 유출되었고 솔트 값이 해쉬 내에 또는 별도의 컬럼에 저장되어 있다면, 솔트 값이 있는 비밀번호의 복구 가능성을 좌우하는 것은 해싱 함수와 관련된 하드웨어의 속도 문제입니다.

올해 세간의 이목을 끈 보안 침해 사건에서는 650만 건의 해쉬가 공개적으로 게시되었습니다. 이 해쉬들은 솔트 값을 추가하지 않고 SHA-1 알고리즘을 이용하여 생성된 것이었습니다. 몇 주 전에는, 조사자들이 이 비밀번호의 90%를 복구할 수 있었습니다.

그렇게 높은 복구율을 달성할 수 있었던 이유는 몇 가지 요인에 기초하고 있으며, 지금의 하드웨어가 얼마나 빨리 비밀번호를 복구할 수 있는지를 예증합니다.

첫째는 소스 비밀번호의 엔트로피가 그다지 높지 않았으며 주어진 대규모 소스 단어의 풀에서 쉽게 유추할 수 있는 공통 단어 및 구문에 기반을 두고 있었다는 점입니다. 20자 이상의 더 긴 여러 단어의 암호구를 사용할지라도, 그 구문이 노래 제목, 시구, 유명한 인용구 또는 여타 "알려진" 구문일 경우에는 충분한 보안 효과가 없습니다. 이 모든 것을 유추 풀에 추가할 수 있으며, 시간이 충분하다면 복구할 수 있습니다.

그 회사가 비밀번호에 솔트 값을 추가했더라면 속도가 상당히 둔화되었을 것이라고 조사자들은 언급하였습니다.[25] 가장 큰 원인을 제공한 요인은 해쉬 함수 SHA-1이 다른 해싱 함수에 비해 매우 빠르다는 점이었기 때문에, 본질적으로 그 방법은 해결책이 못됩니다. 조사자들은 무료 도구와 가정용 서버를 이용하여 초당 150억 개의 엄청난 SHA-1 조합을 유추할 수 있었습니다.

사전의 단어나 단순한 일반적인 비밀번호는 순식간에 복구될 수 있습니다. 조사자들이 알려진 솔트 값이 있는 단일 비밀번호에 주안점을 둔다면, 단시간 내에 수십 억 개의 조합을 시도할 수 있을 것입니다. 솔트 값 추가는 바람직한 사례이지만, 지금의 하드웨어 속도를 고려해 본다면 적절한 방법이 아닙니다.

복구 속도 절감

하드웨어의 속도가 지속적으로 향상되고 막대한 병렬 컴퓨팅 시스템의 가격이 저렴해져 비밀번호를 유추하기 쉬운 환경이 된 상태에서, 차선의 솔루션은 해싱 알고리즘의 속도를 저하시키는 것입니다. 150억 개의 SHA-1 해쉬 산출에 1초가 걸린다면, 다른 함수는 몇 배 더 느릴 것입니다.

SHA-1은 비밀번호 해싱을 위한 것이 아니었습니다. 가장 바람직한 것은, 연산 속도 및 연산력의 향상에 보조를 맞추어 조정할 수 있는 해싱 함수입니다.

한 가지 방법은 반복 횟수를 (그 함수에 따라) 수십 억 회까지 확장할 수 있는 해쉬의 해쉬 개념과 관련이 있습니다. 동일한 함수를 실행하는 횟수가 많을수록 산출에 소요되는 시간이 늘어날 것이 분명하므로, 조합의 유추에 소요되는 시간도 늘어날 것입니다.

SHA512crypt가 그러한 비밀번호 해싱 함수의 일종으로, 반복 횟수를 수천 회 이상으로 구성할 수 있습니다. 초당 150억 개 이상의 속도로 SHA-1 비밀번호를 복구하는 조사자들도 반복 횟수를 5,000회로 설정한 SHA512crypt 함수를 사용한 비밀번호의 경우에는 유사한 하드웨어를 사용하여 초당 11,405개만 유추할 수 있었습니다.

PBKDF2(Password-Based Key Derivation Function 2)도 여러 차례의 반복을 실행할 수 있으며 특히 비밀번호 복구 속도의 문제를 해결하기 위해 개발된 암호화 함수입니다.

Bcrypt는 특히 비밀번호를 위해 개발된 암호화 해쉬 함수로서, Blowfish 암호에 기반을 두고 있습니다. Bcrypt는 내부 솔트 값을 사용하여 레인보우 테이블 생성이 한층 어렵도록 파생 해쉬를 무작위로 추출합니다. Bcrypt는 함수 자체가 느리기 때문에 SHA512crypt와 같은 함수에 비해 속도 둔화에 필요한 반복 횟수가 적어도 되지만, 여러 차례의 반복 구성도 지원합니다.

Scrypt는 비밀번호 해싱에 사용할 수 있는 또 다른 전용 키 파생 함수입니다. Scrypt의 차별화된 장점 중의 한 가지는 모든 산출이 대량의 메모리를 사용하도록 설계되어 있어, GPU 또는 FPGA를 사용하는 병렬 비밀번호 유추를 한층 자원 집약적으로 만들 수 있다는 것입니다 (96 페이지의 사이드바 참조).

이러한 기존의 "저속" 비밀번호 해싱 옵션을 고려해 볼 때, 이 옵션을 채택하는 웹 개발자들이 늘지 않는 이유는 무엇일까요?

몇 가지 가능한 이유가 있습니다. 첫째는 MD5 및 SHA와 같은 함수가 충분히 입증되어 있으며 PHP 및 Java와 같은 서버 측 언어에 사용이 편리하다는 점입니다. 다년간, 이러한 함수들은 비밀번호 보안에 실행 가능한 솔루션으로 여겨져 왔으며, 간편하고 효율적인 기능을 보였습니다. 해싱 함수의 속도를 저하시키는 라이브러리는 그만큼 원활하게 구현되거나 쉽게 구할 수 없었습니다. 지금은 다수의 도구와 구현에 대한 권장 모범 사례가 있습니다.

또 다른 이유는 교육 문제일 가능성이 높습니다. 1초에 수십 억 개의 비밀번호를 크랙하는 데 필요한 하드웨어가 보편화되면서, 더 나은 것이 필요하다는 개념을 받아들이는 개발자가 점점 더 늘고 있습니다.

안전한 웹 애플리케이션은 방어의 최전선입니다. 비밀번호 해쉬로 가득 찬 데이터베이스를 아무렇게나 방치하지 않아야 합니다. 여느 보안 모범 사례와 마찬가지로, 여러 계층의 방어가 바람직합니다. 안전한 비밀번호 저장을 위해 설계된 저속 해싱 알고리즘을 사용하는 것은 고객 데이터의 무결성을 확보하는 매우 효과적인 방법입니다.

더 빠르고, 저렴하며 강력해진 병렬 처리

몇 년 전에 등장한 멀티코어 CPU(중앙 처리 장치)는 비밀번호 유추의 초당 일괄처리 속도를 현저히 향상시켰습니다.

동시에, 3D 게임의 수요는 더 빠르고 더 강력한 전용 그래픽 카드의 필요성을 유발하였습니다.

근년에 들어 그래픽 카드 제조업체들이 고급 API를 출시하면서, 프로그래머들은 한층 간편하게 애플리케이션을 작성하면서 동시에 GPU(그래픽 처리 장치) 상에서 실행할 수 있게 되었습니다. 이는 더 많은 혜택을 위해 이 멀티코어 플랫폼의 연산력을 활용할 수 있는 과학 및 의료 애플리케이션, 오디오 및 비디오 처리, 여타 집중적인 수리 용도에 정말 좋은 소식입니다. 하지만, 무차별 공격을 당할 수 있는 속도만큼만 강력한 암호화 알고리즘의 경우에는, 이러한 상황이 문제가 됩니다.

지금의 데스크톱 CPU가 2-16 코어라는 점에 비추어 볼 때, 소비자 GPU 카드는 수 백 ~ 수 천 코어일 것입니다. 각각의 코어가 동시에 태스크를 처리할 수 있다는 점을 고려해 보면, 비밀번호의 모든 가능한 문자와 숫자의 조합에 대하여 해쉬 함수를 실행하는 것과 같은 반복 태스크가 훨씬 더 빨라지고 있습니다.
1인칭 슈팅 게임의 프레임 렌더링이 고급 암호화 산출에 필요한 수리와 그다지 다르지 않은 것으로 알려져 있습니다. CPU가 다양한 태스크와 연산 처리를 맡는 일종의 팔방미인이라면, GPU는 엄청난 일단의 수를 연달아 반복적으로 고속 처리하는 데 한층 탁월합니다.

심지어 비밀번호 유추는 "클라우드"로 확장되었습니다. 클라우드 서비스 제공자를 이용하면, 시간당 수 백 달러의 비용으로 아주 저렴하게 고속 처리를 위한 일련의 GPU를 임대할 수 있습니다. 이러한 유형의 연산은 확장이 매우 용이합니다.

비밀번호 해쉬 유추에 GPU의 사용은 아직 소프트웨어적 운영이며 따라서 운영 체제의 디스크 상에서 실행되는 소프트웨어의 속도에 의해 제약을 받습니다.

새로운 "비밀번호 복구 시스템" 분야의 또 다른 도구는 하드웨어 기반 FPGA(Field Programmable Gate Array)입니다. FPGA는 여러 개의 카드가 포함된 어플라이언스 형태로 제공되며, 비밀번호 해쉬 사출과 같은 태스크를 순식간에 수행할 수 있습니다. 현재는 CPU나 GPU를 사용하는 것보다 많은 비용이 소요되지만, 속도가 현저하게 증가됩니다. 어느 FPGA 벤더에 의하면,[26] 어플라이언스가 초당 1,756,800개의 WPA-PSK 무선 비밀번호를 유추할 수 있는 반면에, AMD GPU는 초당 103,800개, Nvidia GPU는 초당 30,000개 그리고 Intel I7 CPU는 초당 4,000개를 유추할 수 있다고 합니다.

해쉬에서 잿더미로

유출된 비밀번호로 인한 피해를 보지 않으려면

비밀번호 유추 원리

레인보우 테이블은 비밀번호 해쉬를 미리 산출하여 향후 검색을 위해 효율적으로 보관합니다. 시간이 지나면서, 비밀번호 조합이 어마어마한 수로 늘어날 수 있습니다.

사전 공격은 기지의 단어, 구문, 인용구와 3을 철자 E로 치환하거나 첫 글자를 대문자화하는 등의 비밀번호 생성에 쓰이는 여타 규칙이 수록된 대용량의 파일을 사용하여 비밀번호를 유추합니다.

무차별 공격은 모든 가능한 문자, 숫자, 기호의 조합을 시도합니다. 최신 하드웨어와 고속 해쉬 함수를 사용하면, 6자 비밀번호의 모든 조합을 수초 내로 유추할 수 있습니다.

사용자

- 여러 사이트에 동일한 비밀번호를 사용하지 않습니다
- 기존의 보편적인 비밀번호 트릭을 사용하지 않습니다
- 사전의 단어나 알려진 구문을 사용하지 않습니다
- 가능하다면, 이중 요소 인증을 사용합니다
- 비밀번호 관리자를 사용합니다

웹 개발자

- 비밀번호용 저속 해쉬 함수를 사용합니다
- XSS 및 SQLi 취약점에 대하여 코드를 감사합니다
- IPS, 웹 애플리케이션 방화벽 또는 유사한 기능을 사용합니다

해쉬가 유출되고 나면
쉽게 구할 수 있는 도구를 사용하는 여러 방법을 통해 비밀번호 텍스트를 즉시 복구할 수 있습니다

3D 그래픽 카드(GPU)는 해쉬 함수를 동시에 아주 빠른 속도로 실행할 수 있습니다. 일부 경우에는 **초당 수십 억 개의 비밀번호**를 유추할 수 있습니다. FPGA와 같은 특수 하드웨어와 클라우드 서비스는 크래킹 속도를 현저히 향상시켰습니다.

MD5 또는 SHA-1
초당 수십 억 개 유추

SHA512CRYPT
초당 수천 개 유추

BCRYPT 또는 SCRYPT
초당 수천 개 유추

속도 절감

설계상, 일부 해쉬 함수는 즉시 산출될 수 있습니다. 공격자가 초당 유추할 수 있는 조합이 많아지므로, 이는 비밀번호 보관에는 불리합니다.

저속 해쉬 함수를 사용하면 초당 유추 수가 현저히 감소되어, 복구 프로세스가 훨씬 어려워질 수 있습니다.

비밀번호를 복구하고 나면,
공격자는 유출된 이메일 주소와 평문 비밀번호를 사용하여 웹메일, 소셜 네트워크 또는 여타 사이트에 대한 접근을 시도합니다

비밀번호를 재사용하는 사용자는 한 사이트의 보안 침해가 여러 다른 사이트에 대한 접근을 허용한다는 점을 모르고 있는 경우가 흔합니다.

비밀번호가 유출되는 경우는 공격자가 SQL 인젝션, XSS 또는 다른 취약점을 통해 데이터베이스에 대한 접근권한을 확보하는 때입니다.

비밀번호는 흔히 텍스트를 암호화한 해쉬 형태로 보관됩니다.

최근의 조사에서*

59%의

사용자가 웹메일 계정을 비롯한 여러 사이트에 동일한 비밀번호를 사용하고 있는 것으로 나타났습니다.

단원 IV
새로운 보안 추세

이 단원에서는 지금이 투자해야 할 시기가 아닌가 기업들이 고민할 정도로 급속도로 발전하고 있는 기술 분야를 살펴보겠습니다. 또한 이러한 조기 기술 채택에서 악성코드가 어떻게 악용되고 있으며 기업이 보안에 집중력을 유지할 수 있는 방법을 설명하겠습니다.

대다수 기업의 초기 BYOD(bring your own device)가 미치는 영향

대다수 기업의 모바일 사용의 정착으로 인해 보안에 중대한 문제가 되고 있습니다. 한 가지 큰 변화는 BYOD(bring your own device) 프로그램의 정당성을 인정한 것입니다. 다수의 기업들이 이전에는 개인 소유의 기존 컴퓨팅 디바이스를 사용하는 것을 용인하거나 지지하지 않았으며, 따라서 스마트폰 및 태블릿과 같은 모바일 디바이스에 대한 BYOD 프로그램의 시행은 이러한 디바이스의 사용을 지지하는 정책 및 거버넌스의 공식화를 포함하는 실로 놀라운 변화입니다. 이는 또한 보안 통제와 그에 상응하는 기술을 요합니다.

인적 자원, 법무 부서 등의 의견 및 지침과 어쩌면 전체 직원들의 의견을 수렴하는 부문 연계 방식으로 수립된 적절한 BYOD 정책은 필수적입니다. 기존 컴퓨팅 디바이스를 지원하는 BYOD 프로그램을 시행 중인 기업의 경우, 기존 정책을 검토하여 모바일 디바이스의 확장을 지원하는 데 변경이 필요한지를 판단하는 것이 바람직할 것입니다 (개인 소유의 기존 컴퓨팅 디바이스에 비해 개인 소유 모바일 디바이스의 사용이 훨씬 더 늘어날 수 있기 때문입니다).

보안 현황

모바일 디바이스 보안 현황은 유동적입니다. 안드로이드 플랫폼의 TigerBot/Android.Bmaster, 여러 모바일 플랫폼의 Zeus/ZITMO와 같은 신형 모바일 악성코드가 보고된 반면에, 대다수 스마트폰 사용자들은 여전히 프리미엄 SMS 사기 등과 같은 위험에 가장 취약합니다. 이러한 사기는 설치된 애플리케이션에서 SMS 메시지를 여러 국가의 고급 전화기 사용자에게 자동으로 발송하는 방식을 취합니다. 이러한 사기 감염 방식은 여러 가지가 있습니다. 1) 앱 스토어에서 합법적으로 보이지만 악성코드만 들어있는 애플리케이션, 2) 일부 악성코드가 들어있는 실제 애플리케이션의 복사본인 다른 이름의 애플리케이션, 3) 일반적으로 대체 앱 스토어에 등록되는 악성코드가 숨겨진 실제 애플리케이션. 여기서 흥미로운 측면이 나타납니다. 주 앱 스토어에는 현저한 브랜드 인센티브와 로우그(rogue) 앱이 등록되는 것을 식별할 수 있는 기지의 보안 이니셔티브가 있는 반면에, 대체 앱 스토어는 그렇지 않을 수 있습니다. 선택의 자유가 IT 생태계에 도움이 되지만, 보안 패러다임의 복잡도를 높이며, 따라서 여하한 이유로 대체 앱 스토어 환경에 참여하지 않는 상당 수의 최종 사용자와 기업에게는 그다지 도움이 되지 않습니다.

BYOD의 복잡도를 추가하고 개인 소유 모바일 디바이스에 모범 사례를 적용하는 것은 여러 인기 있는 애플리케이션이 숙련된 사용자도 주의를 게을리할 수 있고 위험하거나 불필요한 신규 애플리케이션에 대한 권한에 무감각해질 정도로 광범위한 권한을 요구하고 있기 때문입니다.

그렇다면 왜 SMS일까요? 실제로, SMS/문자는 그 목적이 직접적인 SMS 사기든, Zeus와 같은 간접적인 사기든 모바일 악성코드 작성자에게 중요합니다. 문자 메시지는 봇넷의 직접적인 지휘 통제에 (지금까지 모바일 플랫폼 상에서는 집중적인 방식으로) 활용될 수 있고, 전세계 일부 은행들이 은행/전신환 송금의 이중 요소 인증으로 사용하고 있으며, 전세계의 프리미엄 번호에 문자를 전송하여 악의적인 공격자(및 부정직한 단체)가 전화 회사로부터 직접 돈을 갈취할 수 있습니다.[27] 모바일 사업자는 청구서를 자동으로 처리하기 때문에, 이는 엔드포인트 영역에서 개인의 관점에 따라 금융 위험 또는 액세스의 어떤 자동 레벨로 디바이스를 연결하는 유일한 경우입니다. 마지막으로, 문자 메시지가 사회 전반에 보편화되면서 아무런 제재가 없는 메시지를 통해 악성코드가 눈에 띄지 않고 전파되고 있습니다.

SMS 문자를 통한 이중 요소 인증은 시행 초기에는 보안에 매우 유용한 방식으로 여겨졌고 금융 기관에 대한 위험을 줄인 것이 분명하지만, Zeus 모바일(ZITMO)을 지원하는 모바일 운영 체제의 수는 시간이 지나면서 트랜잭션에 일부 복잡도를 추가하지 않고서는 점점 더 쓸모 없어질 것임을 보여주고 있다는 점이 흥미롭습니다.

Code bomb은 어떨까요? 다양한 하청 모바일 앱 프로그래머와 아웃소싱 개발 회사들이 있습니다. 납품 시에 전반적인 애플리케이션 품질을 테스트하는 것은 간단하지만, 악성코드에 대하여 앱 스토어에 등록할 코드를 감사하는 경우는 극히 드뭅니다. 악성코드가 숨겨진 소프트웨어 개발로 인하여 영향을 받은 유명 브랜드는 보고되지 않았지만, 어떤 시점에 발생하게 될 이러한 상황에 대비하는 경우는 많지 않습니다. 모바일 애플리케이션 개발을 아웃소싱하는 기업들은 자사의 애플리케이션이 민감한 개인 또는 금융 정보를 취급한다면 특히 유념해야 합니다.

27 http://www.guardian.co.uk/technology/2012/may/25/android-users-angry-birds-malware

특정 대상 공격의 경우, IBM X-Force가 믿을만한 소식통을 통해 입수한 다수의 입증되지 않은 일화가 있었지만, 모바일 사용자를 특정 대상으로 겨냥한 공격은 소비할 수 있는 형태의 유용한 데이터를 가진 것으로 알려진 잠재적 피해자만이 위험에 처할 것이므로 공격을 수행하는 데 소요되는 비용이 상당히 높다고 봅니다. 다시 말하면, 모바일 상의 특정 대상 공격이 모든 주요 모바일 운영 체제 상에 존재할 가능성은 높지만, 누군가 표적이 될 확률은 전반적으로 극히 낮습니다.

반복해서 말하자면, 모바일 보안 환경이 유동적이라는 것이 IBM X-Force의 견해입니다. 안드로이드 및 iOS와 같은 여러 모바일 플랫폼의 소프트웨어 보안 모델은 일반적인 엔드포인트와는 다르고 서로 간에 다소 차이가 있습니다. 이 점은 추후에 살펴보도록 하겠습니다. 상당한 규모의 일부 신형 공격이 있지만, 주된 모바일 보안 위험은 프리미엄 SMS 메시지를 통해 최종 사용자나 기업의 돈을 갈취하는 거짓 또는 로우그(rogue) 애플리케이션에 있습니다. 범죄자들이 대대적으로 이를 통해 돈을 벌 수 있는 방법을 모색하면서, Android(dot)Bmaster와 같은 모바일 봇이 더욱 늘어날 것으로 보입니다. 지금부터는 BYOD 주제의 범위와 알려진 모범 사례를 살펴보기로 하겠습니다.

BYOD의 정착

사내에서 BYOD를 제대로 정착시키려면, 직원 소유의 디바이스를 인프라에 추가하기 전에 주도면밀하고 투명한 정책을 먼저 갖추어야 합니다. 이 정책에는 회사와 직원의 디바이스 간의 관계와 모든 당사자의 동의와 지원을 포함한 모든 측면이 포함되어야 합니다. 그러한 정책에 포함되어야 할 권장 분야는 다음과 같습니다.

- 식별 및 인증
- 액세스 인가
- 정보 보호
- 서비스 무결성
- 보증
- 사고 대응

대다수 기업들이 회사 소유 장비의 보호를 위해 어러한 분야를 포함하는 정책을 이미 시행하고 있습니다. 이러한 정책을 BYOD 모델에서 사용하는 직원 소유 디바이스에도 적용해야 합니다. 거의 모든 경우에, 데이터 보호에 요구되는 동일한 수준의 보안을 확보하는 통제가 요구됩니다.

식별 및 인증

BYOD 프로그램의 시행에 고려해야 할 데이터 분류에 대한 통제 요구사항은 기존의 인증 요구사항과 연계되어야 합니다. 모바일의 맥락에서, 이는 필수적인 복잡도 및 구문 요구사항을 충족하는 비밀번호의 사용을 강제하고 적절하게 관리하는 데 유용합니다. 자산 데이터베이스를 확장하면 사용중인 개인 소유 자산의 목록을 확인하고 디바이스 수명주기 관리의 일부로 회사가 제공하는 소프트웨어의 라이센싱을 관리하는 데 도움이 됩니다. 명확하게 규정된 소프트웨어 라이센싱 정책을 시행하면 직원들이 기업 환경에서 자신의 디바이스를 사용할 때 라이센스가 유효한 소프트웨어만을 사용할 수 있습니다.

액세스 인가

처음으로 BYOD에 착수하는 기업은 기존의 원격 및 애플리케이션 액세스 프로그램을 시행하고 있을 가능성이 높으며 기존 인프라, 기술, 프로세스를 BYOD 디바이스로 확대하여 확대 적용하는 것이 바람직합니다. 첫째, 이는 기존의 통제 요구사항 내에서 액세스가 이루어지게 하는 데 도움이 됩니다. 이 액세스와 관련된 데이터는 분류 및 그에 상응하는 통제 측면에서 변경될 가능성이 적으므로, 이 방식은 일관성 유지에 도움이 됩니다. 둘째, 이 방식은 특히 원격 액세스 게이트웨이 외에도 애플리케이션 액세스 통제일 가능성이 높기 때문에, 임시적인 디바이스 고유의 BYOD 액세스 시행에 비해 비용 효과적일 것입니다.

완전하게 고유한 BYOD 액세스 프로그램을 제공하기로 결정한 기업은 이 권고사항에서 당연히 예외입니다. 일부 업계에서는, BYOD 디바이스 별로 완전히 가상화된 액세스로 고유 액세스 방식을 추진하고 있다는 점도 간과하지 않아야 합니다.

정보 보호

기업 정보와 직원 소유 디바이스 상의 데이터의 보안은 기업에게 가장 중요합니다. 일반적으로, 정보 보호 요구사항은 명확하며 특정 데이터 분류에 연계되어 있습니다. 이 요구사항을 BYOD 프로그램에도 동일하게 적용해야 합니다. 기업의 BYOD 정책에 요구될 수 있는 한 가지 옵션은 데이터 암호화입니다. 이 옵션을 기존 요구사항에 연계시키고 명확하게 이해해야 하며 사용하는 모바일 운영 체제에 적절하게 규정해야 합니다.

현재 사용 중인 다수의 디바이스는 디바이스가 이용할 수 있는 모든 스토리지를 암호화하고 부팅 시에 사용자가 암호구를 입력해야만 액세스할 수 있는 옵션을 제공합니다.

디바이스를 분실하거나 도난 당하는 경우, 암호화된 스토리지가 일정 수준의 보호를 제공합니다. 하지만 GPU(그래픽 처리 장치)의 성능이 지속적으로 향상되면서, 시간이 충분하다면 암호화를 깰 수 있다고 볼 수 있습니다. 새로운 우려는 클라우드 상에서 GPU 처리가 조만간 가능해져, 공격자들이 상당한 비용을 절감하는 혜택을 볼 수 있다는 점입니다. 바람직한 정책을 위한 한 가지 제안은 "삭제(wipe) 조항"입니다. 디바이스를 분실하는 경우, 회사가 삭제 명령어를 전송하여 디바이스가 네트워크에 접속할 수 있게 되면 디바이스 상의 모든 데이터가 삭제됩니다.

운영 체제 및 애플리케이션 무결성

회사 소유 서버 및 워크스테이션과 마찬가지로, BYOD 자격에 해당되는 디바이스에는 운영 체제와 애플리케이션이 있습니다. 스마트폰과 태블릿의 경우, 소프트웨어 성숙도가 기존의 서버 및 워크스테이션에 비해 현저히 낮습니다. 따라서 이러한 디바이스는 공격의 주된 표적이 됩니다. 바람직한 BYOD 정책은 이 점을 고려해야 하며 기존 디바이스와 동일한 (또는 그 이상의) 수준의 패치 요구사항을 적용해야 합니다. 이는 올바로 업데이트된 버전의 펌웨어를 명확하게 식별하고, 기술을 통해 올바른 버전의 디바이스에만 기업 정보에 대한 액세스를 허용하는 것입니다.

안드로이드 디바이스 커뮤니티 내에서 나타나고 있는 디바이스 세분화는 기업 갱신 정책에서 볼 때 디바이스가 비교적 신형인 경우에도 구형 디바이스가 펌웨어 업데이트를 받을 수 없는 문제 등을 야기하고 있습니다.

또한, 회사가 승인한 안티바이러스 애플리케이션을 디바이스에서 실행할 것을 요구해야 합니다. 그러면 악성코드와 악성 웹사이트로부터 어느 정도의 보호를 할 수 있습니다.

스마트폰과 태블릿은 디바이스에 대한 완전한 액세스를 허용하지 않으며 더 높은 수준의 접근 권한을 확보하려면 "루팅"(안드로이드)이나 "탈옥"(애플 iOS)이 필요합니다. 사용자의 접근 권한이 높을수록 디바이스가 공격 당할 수 있는 위험이 더 커집니다. 탈옥이나 루팅 방식은 본질적으로 모바일 운영 체제 내의 보안 통제(예: 애플리케이션 샌드박싱)를 우회하기 때문에, 기업은 그러한 디바이스를 BYOD 프로그램 내에서 사용하지 못하게 해야 합니다.

회사는 또한 애플리케이션을 다운로드하거나 구매할 수 있는 사이트를 디바이스 고유의 벤더 사이트로 제한해야 합니다. 벤더 사이트는 일반적으로 자신들이 배포하는 소프트웨어에 대하여 어느 정도의 품질 관리를 제공합니다.

보증

기존의 엔터프라이즈 보안 보안 프로그램과 마찬가지로, 필수적인 통제와 모니터링을 통한 보증은 기본적인 요소입니다. 이와 동일한 수준의 보증을 BYOD 프로그램 내에서 기업 정보에 대한 접근 권한을 가진 모든 디바이스에 확대 적용해야 합니다. 이러한 디바이스는 직원 소유이므로, 모니터링 대상 요소를 명확하게 설명하여 직원들이 자신의 디바이스를 자발적으로 포함시키도록 해야 합니다.

사고 대응

명확한 사고 대응 프로세스는 당연해 보일 수 있지만, 모든 BYOD 프로그램의 중요하면서도 필수적인 부분입니다. 모바일 디바이스, 특히 스마트폰은 기존 컴퓨팅 디바이스에 비해 분실 및 도난 가능성이 높기 때문에, 분실 또는 도난 디바이스의 보고 방법과 더불어 디바이스를 원격으로 삭제하는 적절한 프로세스에 관한 직원 교육이 매우 중요합니다. 바람직한 보안 프로그램에는 손실 정도를 판단하고, 완화할 잠재적 조치를 관리하며 노출된 정보를 파악하는 데 도움이 되는 기존의 사고 대응 프로세스가 통합되어 있습니다.

BYOD 프로그램의 정의 및 검토

BYOD 정책은 회사와 직원 간의 자발적인 계약입니다. 이는 일종의 계약으로서, 직원들에게 제시하기 전에 특정 기준을 통과해야 합니다.

이 정책은 회사의 법무 부서가 승인해야 합니다. 정책의 특정 측면에 관한 승인에 인적 자원 부서의 참여가 필요한 경우도 있습니다. 정책을 전세계적으로 실시해야 하는 경우에는 정책이 현지 국가의 법률도 준수(또는 현지 규정을 준수하도록 적절하게 개발)해야 합니다.

사용자 교육을 확장하는 것도 바람직합니다. BYOD 정책이 제대로 정착되려면 직원들이 정책의 모든 측면을 이해하고, 수용하여 준수해야 합니다. 특정 정책 요소를 시행하는 "이유"에 대한 세부적인 설명이 필요할 수도 있습니다. 정보가 충분한 직원은 정책을 위반할 경향이 적습니다. 정책의 구속이 지나치면 정책 위반이나 디바이스의 보안 및 액세스 제어 시스템이 비활성화/삭제되는 심각한 상황이 초래될 수 있습니다.

세밀한 계획을 수립하면, 회사와 직원들은 성공적인 BYOD 구현의 편익을 누릴 수 있습니다.

모바일 보안의 모범 사례

모바일 디바이스(태블릿 및 스마트폰)에 대한 확립된 모범 보안 사례를 참조하는 것이 매우 바람직하겠지만, 이러한 공식적인 사례는 여전히 개발 중에 있으며 성숙되지 않았습니다. 정부의 보안 지침이 일부 공개되어 있지만, 기업의 모바일 프로그램에 필요한 실제 통제 요구사항을 기반으로 한 다양한 사례가 있습니다.

이전 호의 IBM X-Force 동향 및 위험 보고서에서 설명했듯이, 모바일 보안 통제 프로그램은 모바일 디바이스 상에서 사용 가능한 데이터 및 정보에 일치하는 기존의 데이터 보호 및 통제 요구사항에 기반을 두어야 합니다. 이 접근방식이 간결하고 간단해 보일 수 있으나, 실제로는 고객마다 상당한 차이가 있음을 X-Force는 목격하였습니다. 이러한 차이의 대부분은 디바이스의 소유권에 기인합니다. 다수의 엔터프라이즈 컴퓨팅 프로그램에는 이러한 요구사항이 없었으며, 따라서 기업 부문이 기존의 통제 요구사항을 개정할 것이 아니라 개인 소유 디바이스 상의 엔터프라이즈 데이터에 관한 새로운 요구사항을 구축하는 것이 바람직할 것입니다. 모바일에 대한 보안 통제 기술의 성숙도를 고려해볼 때, 이렇게 분화된 접근방식은 그리 놀랄 만한 일이 아니며, 모바일 운영 체제가 지속적으로 발전하고 API를 통해 통제를 강화할 수 있게 되면 이는 전술적인 과제로 부상할 수 있습니다.

최근에는 액세스 신임 정보 강도를 기존의 통제 요구사항에 연계시키는 추세가 나타났습니다. 이는 인증서 기반 방식의 사용으로 인한 추세일 수 있습니다. 숫자 PIN을 이용한 기업 관리 디바이스에 대한 디바이스 액세스 통제가 급속하게 줄고 있습니다. 다수 기업들은 또한 악성코드 예방/어떤 형태의 훼손 탐지에 대한 필요성을 인식하고 있습니다.

통제에 있어 일관성의 수준을 승인하는 것은 모범 사례로 발전하는 과정이라 할 수 있습니다. 그러나 모바일 보안 모범 사례가 다른 분야의 엔터프라이즈 컴퓨팅의 모범 사례에 필적하려면 아직 가야 할 길이 멉니다.

모바일 보안 기술 현황

보안 통제 기술은 급속도로 계속 발전하고 있습니다. 플랫폼 벤더들은 자사의 API를 통해 모든 제품 벤더들이 이용할 수 있는 통제를 지속적으로 추가해 왔습니다. 이러한 개정이 이루어질 때마다 기업의 통제는 한층 더 심화되고 있습니다. 때로는 원하는 만큼 신속하지 않지만, 꾸준히 진전이 이루어지고 있습니다. API를 통한 이 추가 기능에 대한 액세스는 출시되는 모바일 디바이스 관리(MDM) 솔루션에 기본적으로 포함되어 있습니다. MDM 부문의 시장은 지속적인 발전을 거듭해 왔으며, 다수의 대형 보안 벤더들이 MDM 신생 기업을 인수하여 자사의 포트폴리오에 추가하면서 시장의 참여 기업 수는 줄고 있습니다. 이 솔루션 시장은 수 년 내로 상품 시장이 되면서 시장이 한층 성숙해질 것이라는 예측입니다. 새로운 기술이 발전하여 소위 주류의 일부가 되고 따라서 모든 주요 벤더들이 지원하게 되었듯이, MDM도 같은 과정을 거치게 될 것으로 보입니다.

MDM 솔루션에 이러한 변화가 일어나면서, 모바일 기술에도 새로운 변화가 나타났습니다. "분리" 또는 "격리" 기술을 제공하는 벤더들이 늘어나고 있습니다. 이러한 솔루션은 기업이 자사의 애플리케이션 및 관련 데이터를 BYOD 시나리오의 직원들이 소유하고 있는 기존 애플리케이션 및 데이터와 분리할 수 있는 기능을 제공하는 데 중점을 두고 있습니다. 이 방식은 개인 소유 디바이스를 집중적으로 활용하는 엔터프라이즈 모바일 프로그램에 적절한 통제의 균형을 이룰 것으로 보입니다. 이는 어느 정도의 절충을 의미하기도 합니다.

이러한 솔루션의 다수는 일반적으로 iOS 및 안드로이드와 같은 주요 운영 체제에 기반을 두고 있으며, 현재는 단 한 가지 플랫폼만을 지원하고 있으나 향후 다른 플랫폼도 지원할 예정입니다. 이러한 솔루션에는 기업의 모바일 인에이블먼트 목표에 따라 그 가치가 손상될 수도 있는 일련의 제약이 있습니다. 그러한 솔루션의 공통적인 두 가지 주요 제약은 (메일, 일정 관리, 연락처 등의 플랫폼 클라이언트를 대체하기 때문에) 본래의 기능을 잃게 되는 점과 이 분리 기능을 디바이스 상에서 실행할 수 있는 모든 애플리케이션에 쉽게 적용할 수 없다는 점입니다. 제한된 범위 외에는 이 분리 기능을 적용할 수 없기 때문에, 애플리케이션을 재컴파일해야만 분리 솔루션을 적용할 수 있었습니다. 기업이 직접 자사의 애플리케이션을 개발한 경우에는 재컴파일이 가능하지만, 대부분의 경우에는 기업이 소스 코드를 입수할 수 없기 때문에 이 접근방식은 일종의 제약이 됩니다.

iOS 및 안드로이드를 지원하는 "분리" 솔루션이 속속 출시되면서, 이 기능은 최신 블랙베리 릴리스에서 ("Blackberry Balance 기술"로) 운영 체제의 일부가 되었습니다. 운영 체제에 기반을 둔 이 기술은 iOS 및 안드로이드 상의 제3자 솔루션에서 볼 수 있었던 제약을 해결하며 작동 원리에 완전하게 통합되어 운영 체제 레벨에서 나타나는 분리 기술의 요구사항을 충족합니다. RIM(Research In Motion)이 엔터프라이즈 보안 요구사항에 부응하는 데 필요한 보안 통제의 도입 측면에서 모바일 플랫폼 벤더들을 지속적으로 주도해 왔으며, 다른 벤더들은 이제서야 자사의 운영 체제에 이 기능을 포함시키고 있습니다. 최소한, 분리 기술에 대한 투자가 전술적인 투자로 여겨지고 있다는 점은 고려해야 합니다. 모바일 플랫폼 시장의 벤더들은 소비자와 기업 모두가 자사의 디바이스를 기꺼이 선택할 수 있도록 이러한 균형을 제공하는 운영 체제를 전략적으로 포함시킬 것입니다.

이 분리 기능이 대중적인 모바일 운영 체제에 포함될 때까지 이 접근방식과 기술의 사용에 관한 논쟁이 적지 않을 것으로 예상되지만, 대다수 보안 전문가들은 신뢰하는 솔루션 보안에 대한 기본적인 요구사항으로 이러한 애플리케이션이 실행되는 디바이스를 신뢰해야 할 것이라 보고 있습니다.

산업별 접근방식의 추세

모바일 보안에 대한 모범 보안 사례를 구축하려면 아직 해야 할 일이 많이 남아 있지만, 산업 부문별로 일관된 추세가 나타나기 시작했습니다. 이는 모범 사례 성숙도, 명확한 모바일 통제 등에서 아직 부족하기 때문에 여타 컴퓨팅 부문에서 보이는 추세 및 접근방식과는 여전히 상당한 차이가 있습니다. 특정 산업 부문에서는 분리 또는 가상화 기술의 사용이 상당히 두드러진 것으로 확인되었습니다. 의료, 금융, 은행 업계 및 정부 등이 일종의 가상화 또는 분리 방식을 채택하는 경향이 있음을 볼 수 있습니다. 일부 확인된 바로는, 개인 소유 디바이스 상에서 기밀 데이터를 전혀 허용하지 않는다는 점이 이러한 추세를 뒷받침하고 있습니다. 이러한 경우에는, 가상화(랩톱과 같은 기존 컴퓨팅 디바이스에 해당) 또는 애플리케이션 가상화(모바일 디바이스에 해당) 방식을 사용하였습니다. 가상화 접근방식은 엔터프라이즈 내부에 데이터를 저장할 필요성을 없애지만, 이 기술을 수용할 수 있는 신뢰할만한 호스트가 있어야 하며 이는 기본적인 신뢰도를 구축하기 위한 일정 수준의 디바이스 관리가 필요하기 때문에, 이 접근방식은 그리 바람직하지 않아 보입니다. 신뢰할 수 있는 호스트를 확보하려면 디바이스 무결성을 확보할 수 있는 디바이스 관리와 더불어 가상화 접근방식을 사용해야 합니다.

그 밖의 산업에서는 기존의 보안 통제 기반 접근방식을 사용하는 MDM 솔루션을 채택하는 추세가 나타났습니다. 디바이스 비밀번호의 강도 등에 대한 논쟁이 있지만, 비밀번호 사용의 필요성에 관한 논쟁은 적은 편(이며, 단지 구체적인 비밀번호 길이, 구성, 재사용 등에 관한 논쟁)입니다. 대부분의 경우에는, 모든 디바이스가 관리되고 있으며 대부분의 프로그램에 자발적으로 참여하고 있습니다. BYOD가 (비용 절감 때문에) 기업 제공 디바이스의 대체안으로 논의되곤 하지만, 여러 가지 이유로 인해 직원 소유 디바이스의 비자발적인 프로그램을 실제로 도입한 기업은 극소수에 지나지 않습니다. BYOD는 부적격 직원이나 업무 수행에 모바일 디바이스를 지속적으로 사용할 필요가 없는 직원들에게도 제공되고 있으며, 이들은 업무 효율을 향상시키고 일과 삶의 균형을 개선하는 효과를 얻고 있습니다.

모바일 플랫폼 취약점 관리

보안 통제 기술, 디바이스와 그에 상응하는 기능 부문에 변화가 지속적으로 일어나고 있지만, 모바일 보안 환경에서 변함없는 한 가지는 모든 버전의 거의 모든 모바일 운영 체제에서 나타나는 보안 침해입니다. 사실, 신규 버전이 출시된 지 수 일 또는 심지어 수 시간 내에 탈옥이나 루팅이 흔히 이루어지고 있습니다. 이는 거의 모든 모바일 운영 체제에서 나타나는 공통적인 상황입니다. 이는 두 가지 이유에서 특히 바람직하지 않습니다. 일부 모바일 운영 체제는 처음부터 강화된 보안 모델(예: 애플리케이션 샌드박싱)로 설계되었기 때문에, 아주 간단하고 신속하게 침해될 수 있어 샌드박싱과 같은 기능의 추가를 저해하고 있습니다. 둘째, 현재 대다수 운영 체제의 다수 보안 취약점에 대한 패치 수정이 수 주 또는 심지어 수 개월 동안 이루어지지 않고

있습니다. 이 두 번째 사항은 특히 앞서 설명한 디바이스 분화와 그 지원에 있어, 기업이 전략적으로 가장 우려해야 할 문제입니다.

발견된 취약점을 차단하는 신속한 패치 적용은 엔터프라이즈 컴퓨팅 디바이스의 무결성을 확보하기 위한 기본적인 조치입니다. 이는 견실한 보안 프로그램의 핵심이 되는 기본적인 요구사항 중의 한 가지입니다. 사실, 인터넷 상에서 발생한 피해가 막심했던 대형 보안 문제는 패치 수정이 적절하게 이루어지지 않았던 점이 주된 원인입니다. 보다 구체적으로 말하면, 만연하는 문제가 아닌 패치 미수정 취약점이 지능적인 공격에 빌미를 제공하고 있습니다. 모바일 디바이스가 사람들의 주된 컴퓨팅 디바이스가 되면서, 지능적인 공격이 모바일 운영 체제로 옮겨갈 것이라는 점을 주지해야 합니다.

모바일 디바이스의 패치 수정이 주된 요구사항이 되는 것은 시간 문제입니다. 현재 대부분의 모바일 운영 체제에서 패치 수정이 적시에 이루어지지 않고 있습니다. 또한, 기업은 디바이스를 패치 수정할 능력이 없으며, 운영 체제 인프라에서도 이 문제를 제대로 다루지 못하고 있습니다. 이러한 문제는 기업의 선택의 폭을 제한할 가능성이 있습니다. 따라서, 패치 수정이 되지 않은 취약점이 있어 매우 위험하다고 여겨지는 디바이스를 차단하는 방식으로 기업은 이러한 우려를 억제할지도 모릅니다. 유감스럽게도, 이 접근방식의 피해자는 벤더, OEM 또는 통신사업자가 패치 조치를 제공하지 않는 취약한 디바이스를 보유한 직원들입니다.

다수의 모바일 플랫폼에는 패치의 개념조차 없으며, 완전히 새로운 운영 체제 이미지를 디바이스로 전달하는 펌웨어 업그레이드에만 의존하고 있습니다. 플랫폼 벤더, 하드웨어 OEM과 통신사업자 간에 여러 계층의 펌웨어 통제가 존재하는 일부 IT 생태계에서 디바이스 업그레이드에 수 개월이 이상이 소요되면서, 이러한 상황은 더욱 악화되고 있습니다. 이 모델은 일종의 노후화라 할 수 있습니다. 디바이스를 최신 펌웨어 레벨로 업데이트하는 대신에, 통신사업자와 OEM은 교체 디바이스 판매에만 열을 올리고 있습니다.

제조업체에게는 디바이스 분화가 아키텍처 및 구현에 비해 경제적인 솔루션이겠지만 기업의 관점에서 노후화는 바람직하지 않습니다. 모바일 생태계가 발전하면서 다수 기업들이 난처한 상황에 처하게 될 것으로 보입니다.

모바일 디바이스가 기업과 전반적인 인터넷에서 주된 컴퓨팅 디바이스로 자리잡으면서, 가장 진척이 없던 취약한 디바이스의 패치 수정은 이제 주된 보안 관심사로 대두될 것입니다.

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

Produced in the United States of America
September 2012

WGL03014-USEN-02