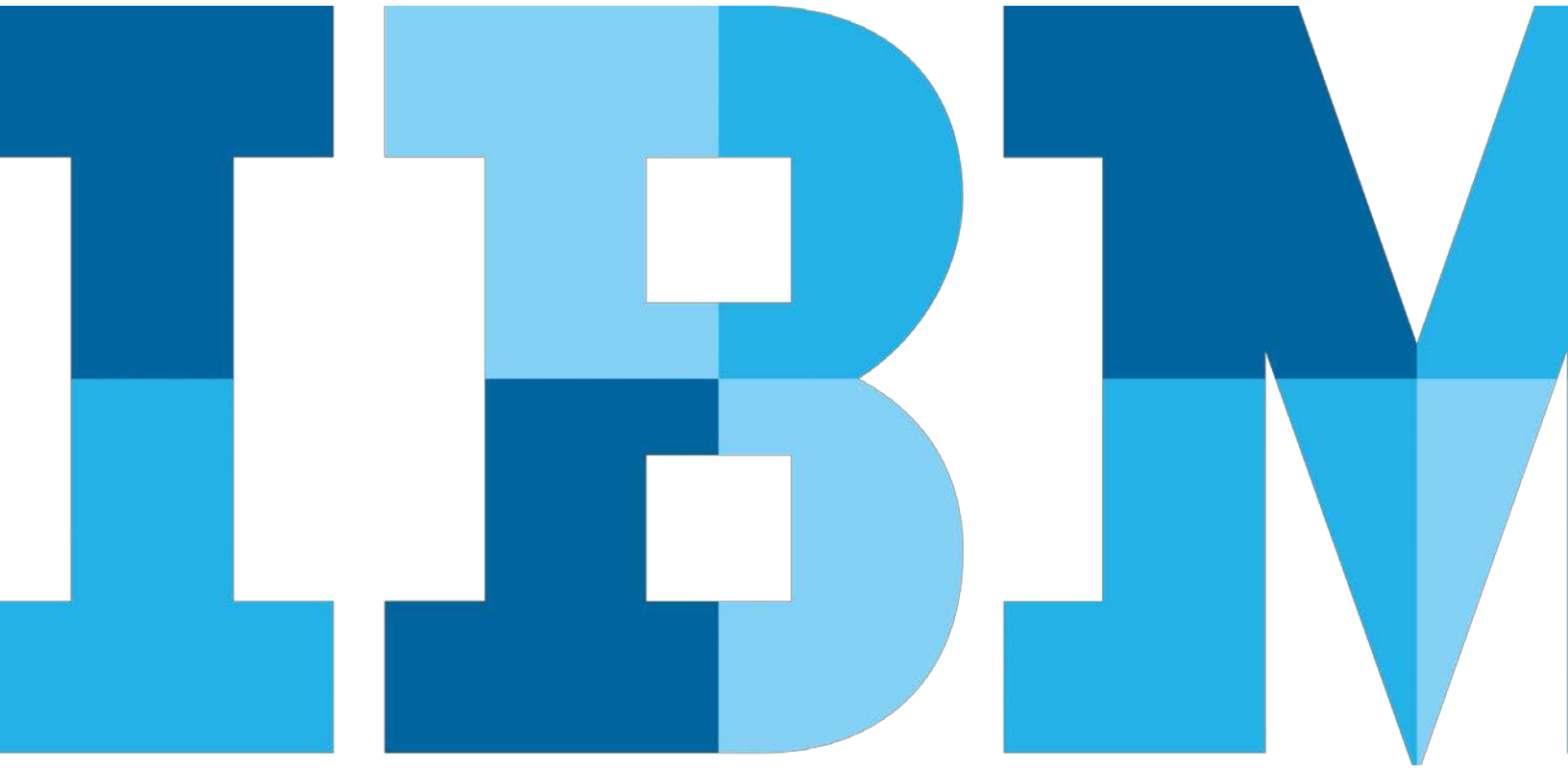
IBM X-Force 보안 동향 및 위험 보고서 2014년 2분기

최신 데이터 및 지속적인 분석을 바탕으로
애플리케이션 취약성, 스팸 위협, 사고 대응의 발전 조명



IBM

목차

개요

IBM® X-Force® 연구 개발 팀은 그간 IBM Global Technology Services® 소속 전문가들과 함께 최근 보안 위협 동향을 면밀하게 분석해 왔습니다. 이제 그 결과를 여러분과 공유하려 합니다. X-Force 팀은 기업들에게 지속적으로 위협을 가하고 있는 보안 사고와 공격에 대한 논의로 2014년을 열었습니다. 이번 2014년 2분기 보고서에서는 과거에 성공을 거둔 후 최근 다시 등장하기 시작한 공격 수법을 조명하고, 현재의 보안 환경에서 새롭게 주목해야 할 문제점도 살펴봅니다.

먼저 과거의 보안 위협을 되짚어봅니다. 시간이 흐름에 따라 상당수의 위협은 새로운 것으로 대체됩니다. ILOVEYOU와 같이 맹위를 떨치던 바이러스 이메일은 드라이브 바이 다운로드(Drive-by-download) 악성코드 설치로 진화하여 서서히 확산되면서 중요 사용자 데이터를 은밀하게 수집하고 있습니다. 과거에는 해커들이 자신의 실력을 과시하기 위해 웹 사이트를 표면적으로 훼손했지만, 지금은 이를 악의적인 서버와 데이터베이스 공격을 숨기기 위한 위장 전술로 쓰고 있습니다. Blaster, St0rm과 같은 웜은 최신 DDoS(분산형 서비스 거부) 공격의 근원이 되었습니다.

인터넷 보안 위협의 역사와 그 변화 과정에서 무엇을 배울 수 있을까요? 취약한 애플리케이션은 소프트웨어 애플리케이션 개발의 초창기부터 존재했습니다. 소프트웨어 개발 과정에서 프로그래머가 실수를 저지르면 애플리케이션에 취약성이 발생합니다. 본 보고서는 취약한 웹 사이트 애플리케이션에 초점을 맞추고, 기업에 타격을 주거나 중요 데이터를 훔쳐내려는 공격자들이 여전히 이 위협 인자를 주목하고 있는 이유를 살펴봅니다.

애플리케이션 검사 기능을 사용하면 맞춤형 애플리케이션 코드뿐 아니라 타사 구성요소까지 해결함으로써 웹 서비스 및 애플리케이션에서 사용자와 접하는 가장 중요한 구성요소를 보호할 수 있습니다. 그러나 고객은 웹 서버 자체의 보안에도 주의를 기울여야 합니다. 취약한 기술로 웹 애플리케이션 스택의 백본을 구성하면 전체 환경이 위험해질 수 있습니다.

2014년 4월, 널리 사용되는 인기 OpenSSL 소프트웨어의 취약성(CVE-2014-0160)으로 인해 상당수의 웹 사이트에서 개인 정보 및 중요 정보가 유출될 위험이 발생했습니다. 패치 자체는 어렵지 않게 적용할 수 있었으나, 사후 조치로 사용자 인증 정보, SSL 인증서, 기타 중요 정보의 유출에 따른 잠재적 피해를 줄이는 것은 쉬운 일이 아니었습니다. 중대한 취약성이 밝혀지거나 사고가 발생하는 경우, 어떤 일이 일어날지 예측할 수 있어야 합니다. 이미 알려진 상황에 대한 계획을 기반으로 사고 대응을 하게 되면 혼란에 빠질 수도 있습니다. RAM(Random Access Memory)의 내용도 디스크에 저장된 데이터만큼 손쉬운 먹잇감이 되고 있습니다. 본 문서에서는 이 중요한 보안 영역을 개선하려는 기업이 염두에 두어야 할 몇 가지 조언을 제공할 것입니다.

OpenSSL TLS(Transport-Layer Security) 하트비트 취약성인 Heartbleed에 대해서는 최신 IBM Security Intelligence 블로그 게시물을 참조하십시오.[1]

다음 섹션에서는 가장 오랜 생명력을 떨치고 있는 보안 위협인 스팸이 어떤 활동을 펼치고 있는지 살펴봅니다. 대부분의 기업들은 스팸의 공습을 막아내기 위한 제어 기능을 적절히 구현했지만, 여전히 공격자들은 이메일 서버를 무력화시키거나 의심하지 않는 사용자에게 악성 페이로드를 전달하는 데 스팸을 활용합니다. IBM X-Force 컨텐츠 보안 팀은 스팸의 진화 과정에 주목하면서, 스팸이 어떻게 기업 네트워크에 악성코드를 유입시키는 주 경로가 되고 있는지 관찰해 왔습니다. 2014년 3월에는 스팸의 양이 또 다시 이전 2년 6개월 중 최고치를 기록했습니다.

또한 X-Force는 스팸 봇 감염의 추적 데이터도 분석하면서 Microsoft Windows XP 지원 종료와의 연관성을 살펴봤습니다.

마지막으로, 약간 새로운 보안 위협 범주를 소개하며 이 보고서를 마무리할 것입니다. IBM Global Technology Services – ERS(Emergency Response Services) 팀의 도움을 받아 원거리 보안 사고에 대한 대응에서 얻은 교훈을 소개합니다. 세계적인 기업이 개발 도상국과 초기 단계의 인프라로 사업 범위를 확장하는 가운데, 대역폭이 제한되고 통신 시설이 부족한 지역에서 보안 사고가 생기면 어떻게 될까요? 대응 팀이 중요 데이터를 신속하게 전송할 수 있는 방법은 무엇일까요? 지리적으로 멀리 떨어진 국가 또는 인프라가 부족한 지역에 특별한 사고 대응 전략이 필요한 까닭을 설명합니다.

심각한 위협 인자인 취약한 애플리케이션

인젝션 취약성부터 손상된 인증까지, 어떤 위협 요소가 동적 웹 애플리케이션에 숨어 있는지 알아보십시오.

공격자들은 여러 가지 공격 경로를 찾아내어 중요하고 가치 있는 기업 데이터를 얻으려 합니다. 대개의 경우 기업의 내부 시스템에 침투하는 가장 빠른 방법은 SQL 인젝션(SQLi), 손상된 인증 등의 취약성을 이용하는 것입니다. 기업의 웹 사이트와 여기에 액세스하는 애플리케이션을 테스트하지 않으면 귀중한 자산이 노출될 위험이 발생하게 됩니다.

모바일 애플리케이션의 예를 들자면, IBM 연구 팀은 최근 Google Android용 Mozilla Firefox에서 여러 취약성을 발견했습니다. 악성 애플리케이션이 이를 이용할 경우 중요한 사용자 프로필 정보가 유출될 수 있습니다.[2] 공격자는 이러한 취약성을 통해 쿠키와 캐싱된 데이터(예: 브라우저 기록, 사용자 ID) 등을 훔쳐냅니다.

IBM 연구 팀에서 발견한 또 다른 모바일 취약성인 Android 프레임워크의 프래그먼트 인젝션(Fragment injection)은 Google Now, Gmail, Dropbox, Evernote와 같은 다수의 인기 애플리케이션에 영향을 미칩니다.[3] 이 취약성을 이용한 공격자는 Android 샌드박스에 침투하여 취약한 애플리케이션에 관한 중요 정보를 얻어냅니다.

웹 애플리케이션 역시 기업 내부에 저장된 가치 있는 데이터에 대한 접근을 허용할 때가 많아 공격자의 주 표적이 됩니다. SQLi와 같은 인젝션 취약성을 악용하면 보호형 백엔드 데이터베이스를 조작할 수 있습니다. 웹 애플리케이션과 주고받는 데이터를 제대로 보호하지 못하면 사용자 인증 정보, 신용 카드 데이터, 비공개 커뮤니케이션 등의 데이터가 유출될 수 있습니다.

10대 웹 애플리케이션 위협 인자는?

2013년에 OWASP(Open Web Application Security Project) Top 10은 가장 심각한 웹 애플리케이션 보안 위험 요소 10가지를 선정했습니다. 여기에는 그림 1에 나타난 것처럼 인젝션 공격, 손상된 인증 및 세션 관리, 교차 사이트 스크립팅이 포함되었습니다.[4]

다음 섹션에서는 호스팅 애플리케이션 테스트를 관리하는 IBM 팀의 조사 내용을 토대로 웹 애플리케이션 위협 인자를 더 자세히 살펴보겠습니다.

웹 애플리케이션 위협 인자 데이터

IBM HASM(Hosted Application Security Management) 서비스는 프리프로덕션(Pre-production) 및 프로덕션 환경 모두에서 IBM Security AppScan®을 사용하여 웹 애플리케이션에 대한 동적 테스트를 실시하는 클라우드 기반 솔루션입니다. HASM 서비스에는 보안 분석 전문가에 의한 테스트 구성 및 관리가 포함되어 있습니다.

HASM 팀은 이번 보고서를 위해 2013년에 실시된 900여 건의 동적 웹 애플리케이션 검사 결과로부터 위협 인자 데이터를 수집했습니다. 핵심 사항을 간추리면 다음과 같습니다.

- 이 데이터 세트는 정부/공공 기관, 금융 서비스, 공업, 제약, 소매, 이동통신 등 다양한 업종의 애플리케이션을 대표합니다.
- 대부분의 검사 자료는 HASM 서비스를 5년 넘게 사용해 온 기업들로부터 수집한 것입니다. 이들은 안정적으로 확립된 보안 프랙티스를 갖춘 곳이며, 검사 대상 애플리케이션의 취약성 수가 웹 애플리케이션 보안을 막 시작한 기업에 비해 적은 편입니다.
- 이 기업들은 웹 애플리케이션에 대해 정기적인 검사를 실시하나, 취약성은 지속적으로 발견되고 있습니다. 이는 주로 코드 변경 또는 신규 애플리케이션 구축을 통해 유입됩니다. 따라서 새로운 기능을 구현했거나 코드 업데이트 및 패치를 적용한 후에는 반드시 애플리케이션을 재검사해야 합니다.
- 발견된 문제점 중 상당수는 적합하지 않은 입력 유효성 검사 및 무결 처리(Sanitization)와 관련되어 있습니다.

2013: 손상된 인증이 심각한 위협으로 대두

그림 1은 교차 사이트 스크립팅(XSS)과 교차 사이트 요청 위조(CSRF) 위협 인자가 여전히 웹 애플리케이션에 널리 퍼져 있음을 보여줍니다. 이번 고객 표본에서는 많이 나타나지 않았지만, 인젝션 공격은 여전히 발생 빈도가 높으며 심각한 위험을 초래합니다. 중요한 내부 데이터에 접근하려는 공격자와 곧바로 연결되기 때문입니다. 이러한 취약성은 잘 알려져 있으므로 또 다른 대표적인 문제인 '손상된 인증'을 더 자세히 살펴보겠습니다.

손상된 인증의 원인은 사용자 ID 및 암호 인증 정보의 보호 실패, 세션 ID의 관리 부실 등 여러 가지가 있습니다. 인증 정보를 제대로 보호하지 못하는 경우, 공격자가 사용자 세션을 하이재킹하여 사용자로 위장할 수 있습니다. 이를테면, 합법적인 사용자인 척하면서 뱅킹 세션에서 자금을 이체할 수 있게 됩니다.

HASM 데이터에 따르면, 인증 검사에서 가장 많이 발견되는 손상된 인증 문제는 '로그인 과정에서 업데이트되지 않은 세션 ID' 유형입니다. 이 테스트는 로그인 시퀀스에서 사용자가 로그인 페이지의 전송 버튼을 클릭한 후에 세션 쿠키의 값이 업데이트되었는지 확인합니다. 로그인할 때 세션 ID(SID)가 업데이트되지 않으면 웹 애플리케이션은 세션 고정(Session-fixation) 공격에 취약해집니다. 즉, 공격자가 세션 고정 공격을 통해 유효한 SID를 확보할 수 있고 로그인 프로세스를 건너뛰고 피해자의 계정에 액세스할 수 있게 됩니다. 이 공격은 사용자가 생성한 SID와 서버에서 생성된 SID 모두에 유효합니다.

Microsoft ASP.NET 애플리케이션은 세션 고정 공격을 당할 위험이 높습니다. 일반적으로 JSESSION 쿠키 값은 사용자가 로그인하기 전에 로그인 페이지에서 생성되며, 기본적으로 로그인 프로세스에서 업데이트되지 않습니다.

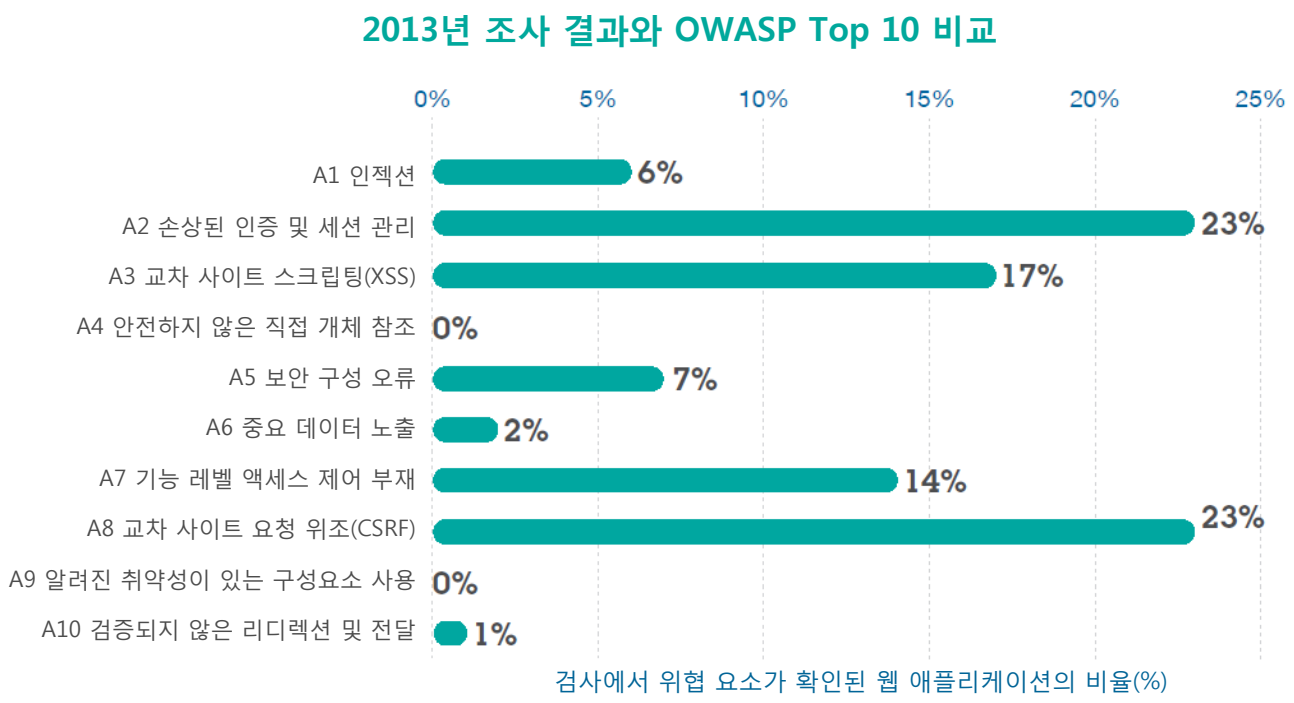


그림 1. IBM HASM 서비스의 웹 애플리케이션 테스트에서 발견된 주요 취약성과 OWASP Top 10(2013) 비교

세션 고정과 SID 악용은 대표적인 취약성 중 하나입니다. 이 문제는 아직 제대로 알려지지 않았으며, 몇 차례 반복되는 동안 개발자들이 문제를 인식하여 적절한 해결책을 찾을 수 있을 것입니다.

세션 기반 인증 취약성을 조기에 발견하고 해결할 수 있도록, IBM은 다음 사항을 수행하여 애플리케이션 테스트를 개선할 것을 권장합니다.

1. 로그인 시점에 SID를 업데이트합니다.
2. 로그아웃했거나 일정 기간 사용하지 않는 경우 SID를 무효화하는 시간 제한을 설정합니다.
3. 인증 기능을 위한 라이브러리 또는 애플리케이션 프로그래밍 인터페이스(API)를 제공합니다.

애플리케이션 보안 테스트 동향

웹 애플리케이션 보안에 대한 인식이 높아지면서 웹 애플리케이션 검사에 대한 투자도 늘어났습니다. 기업들은 프리프로덕션 또는 프로덕션 환경에서 정기적인 웹 애플리케이션 검사를 실시하여 웹 애플리케이션 위험의 기준선을 마련하고 있습니다.

이전에 HASM 고객들의 주 관심사는 애플리케이션을 구축하기 전에 검사를 수행하는 것이었습니다. 그러나 지난해에는 라이브 사이트에 대해 대규모의 검사를 지속적으로 수행하려는 기업이 약간 증가하는 경향을 보였습니다.

라이브 애플리케이션에 대한 대규모의 검사를 수행하려면 자동화된 애플리케이션 검색 방법을 사용하여 모든 웹 애플리케이션을 인벤토리화해야 합니다. 모든 웹 애플리케이션을 추적하고 찾아내는 것은 IT 보안 팀에게 점점 더 까다로운 과제가 되고 있으며, 기업이 사내의 웹 애플리케이션 수를 최대 50% 적게 추산하는 경우도 종종 일어나고 있습니다. 애플리케이션이 실행되고 있다는 사실을 알지 못하는 경우, 보안 취약성을 검사하지 않을 가능성이 높아질 것입니다. 공격자들은 항상 이러한 취약성을 노리고 있습니다. 이것이 바로 정기적인 검사와 애플리케이션 인벤토리 정보 업데이트가 중요한 이유입니다.

웹 애플리케이션 검사에는 전문적인 기술, 소프트웨어에 대한 막대한 투자에 더해 추가 인프라까지 필요할 수 있기 때문에 많은 기업들은 아웃소싱 모델을 선택하고 있습니다. 애플리케이션 보안 테스트에 대한 숙련된 기술을 갖춘 내부 전문가들로 팀을 꾸리려면 많은 시간과 비용을 할애해야 하기 때문에, 아웃소싱은 빠르고 경제적인 방법이 될 수 있습니다. 또한, 테스트 벤더는 광범위한 보안 지식과 전문성을 갖고 있으며 검사 소프트웨어 및 필수 인프라에 대한 지속적인 유지 보수를 제공할 수 있습니다.

안전한 프로덕션 검사를 위한 팁

아웃소싱 검사를 이용하는 경우, 수행되는 검사의 특성을 제대로 파악하는 것이 중요합니다. 테스트 팀과 상담하면서 검사가 어떻게 구성되는지, 무엇이 테스트되는지, 테스트에서 제외되는 것이 있는지, 테스트 범위가 어떻게 되는지 확인하십시오. 그런 다음 위험 요소나 만일의 상황에 대해 물어보십시오. 프로덕션 환경의 애플리케이션 테스트가 서비스 중단으로 이어질 수도 있기 때문에 이 질문은 중요합니다. 벤더를 평가할 때에는 프로덕션 검사 방식과 테스트 범위를 반드시 파악해야 합니다.

프로덕션 검사

어떤 벤더가 프로덕션 검사를 제안할 경우 반드시 고려해야 할 사항이 있습니다. 정적 컨텐츠로 구성된 웹 사이트의 경우 주의해야 할 사항이 줄어들지만, 데이터를 수집한 다음 백엔드 데이터베이스에 저장하거나 다른 백엔드 시스템으로 전달하는 애플리케이션이라면 벤더가 이 영역을 어떻게 테스트하는지를 알아야 합니다. 프로덕션 검사 방식은 크게 두 가지로 나뉩니다.

1. **전체 폼(full-form) 테스트** - 애플리케이션의 모든 폼을 테스트합니다. 범위가 넓으며 대부분의 문제점을 찾아낼 수 있으나 다음과 같은 위험 부담이 따릅니다.
   - 폼을 사용하여 데이터베이스에 데이터를 전송하면 많은 양의 테스트 데이터가 백엔드 데이터베이스와 시스템에 삽입될 수 있습니다. 이를테면 폼 필드 10개로 구성된 폼이 1,000회 이상 전송될 수 있습니다.

- 어떤 폼은 직접 이메일을 보내는 데 또는 이메일을 생성하는 다른 백엔드 시스템과 연결하는 데 사용됩니다. 이러한 폼을 테스트하는 경우에도 수천 통의 이메일이 생성될 수 있습니다.
- 드문 일이지만, 검사로 인해 애플리케이션 또는 백엔드 시스템 전체의 장애가 발생할 수 있습니다. 장애까지는 일어나지 않더라도, 삽입된 테스트 데이터 때문에 백엔드 처리가 실패할 수도 있습니다.
- 웹 애플리케이션 보안 검사로 인해 대량의 http(s) 트래픽이 생기고 일부 애플리케이션의 성능 또는 대역폭 문제로 이어져 사용자에게 직접적인 영향을 미칠 수 있습니다.

2. 폼 작성 제외 또는 선택적 폼 작성 - 폼 작성을 건너뛰거나 최소화함으로써 전체 폼 테스트에서 생기는 문제를 예방합니다. 그러나 테스트의 완전성을 기하지 못해 보안 허점이 생길 수 있습니다. 일반적으로 폼은 애플리케이션에서 여러 중대한 문제점이 발견되는 영역이며, 이는 대부분 잘못된 입력 유효성 검사에서 비롯됩니다. 모든 폼을 테스트하지 않으면 이러한 중대한 문제를 놓칠 위험이 생기게 됩니다.

그림 2는 전체 폼 테스트의 잠재적 문제를 줄이는 방향으로 프로덕션 검사를 수행할 경우, 발견되는 취약성도 줄어든다는 사실을 보여줍니다.

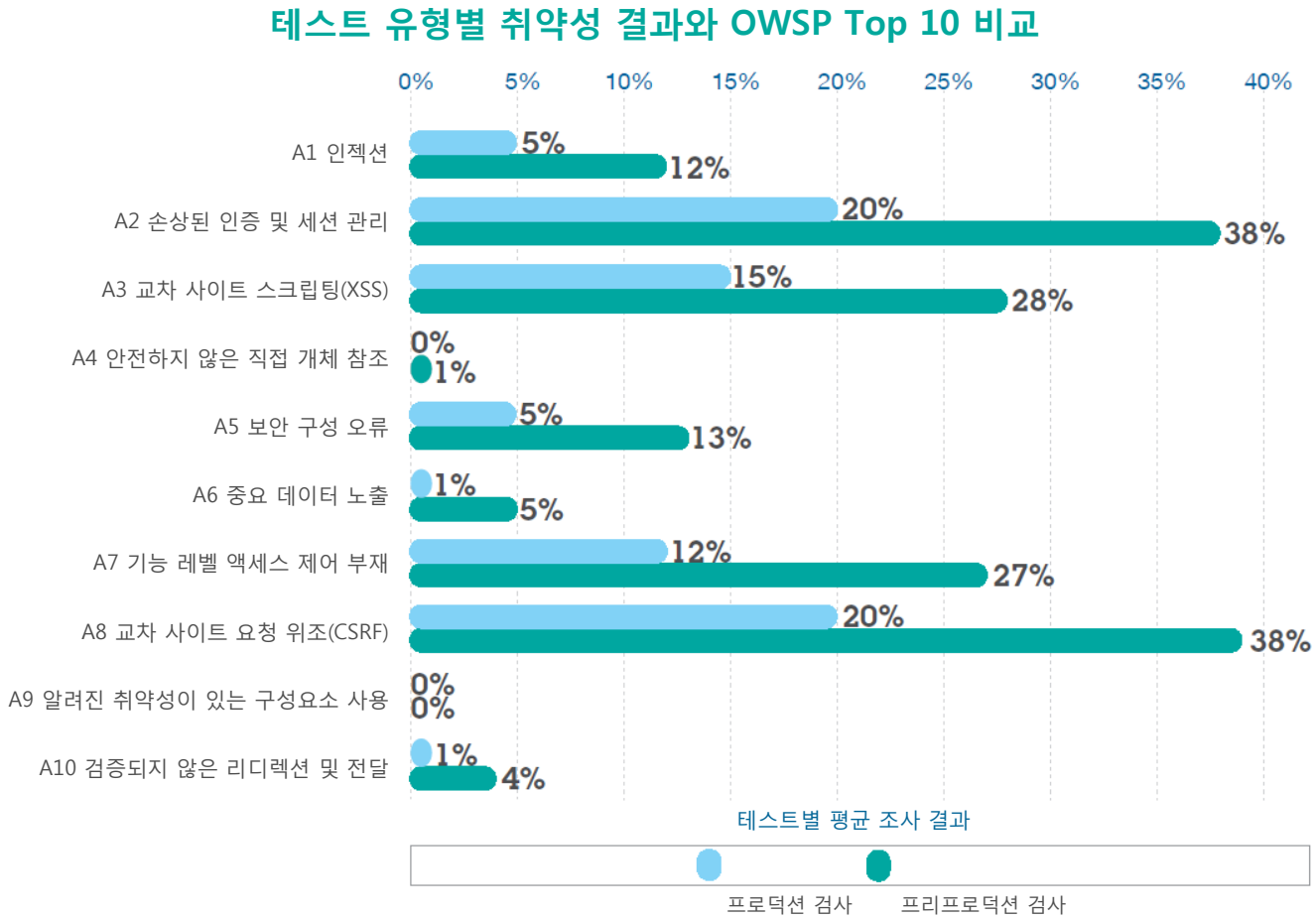


그림 2. IBM HASM 서비스의 프로덕션 검사 및 프리프로덕션 검사 결과와 OWASP Top 10(2013) 비교

전체 폼 테스트에서는 문제가 발생할 수 있으므로, 구축 전에 스테이징 또는 품질 보증(QA) 환경에서 검사를 실행하는 것이 더 효과적일 수 있습니다. 프리프로덕션 검사는 프로덕션 애플리케이션에 대한 정기적인 비간섭형(폼 작성 제외) 검사로 보완할 수 있습니다. 이러한 방식은 데이터 손상이나 프로덕션 시스템 중단의 위험 없이 애플리케이션의 전체 테스트를 수행할 수 있게 하며, 지속적인 테스트와 모니터링을 가능하게 합니다.

범위

또 하나 고려할 점은 테스트의 실제 범위입니다. 예를 들어, 웹 페이지만 테스트하는지, 동적 영역도 포함하는지를 살펴야 합니다. 애플리케이션의 100%가 검사 범위에 포함된다고 가정하지 마십시오. 애플리케이션 검사의 방식은 매우 다양하며, 제대로 수행되지 않는다면 검사의 사각 지대에서 위험에 노출될 수 있습니다.

앞서 언급한 것처럼, 프로덕션 환경과 프리프로덕션 환경 모두에서 검사를 수행할 수 있습니다. 프로덕션 검사는 라이브 환경을 보호하기 위해 제한적인 범위로 설계되는 경우가 많습니다. 프리프로덕션 검사는 특히 폼 작성과 관련하여 더 공격적인 방식으로 수행되어야 합니다. 프리프로덕션 및 프로덕션 검사에 적용되는 검사 구성을 확인하면 올바른 검사 범위를 확보할 수 있습니다.

동적 웹 애플리케이션의 폼 작성과 관련하여 자동 크롤링 메커니즘을 테스트에 사용하는 것으로는 불충분합니다. 고도의 동적 애플리케이션에서는 특정 폼 데이터를 필요로 하며 사용자 인터페이스(UI)가 상당히 복잡하기 때문에 자동 크롤링 메커니즘으로는 탐색을 통해 모든 기능을 제대로 테스트하기 어렵습니다. 따라서 이러한 애플리케이션에서 전체 범위의 테스트를 수행하려면 관련 지식을 갖춘 보안 테스트 전문가의 수동 크롤링으로 자동 크롤링 메커니즘을 보완해야 합니다.

페이지 범위와 관련해서는 어떤 필터링이 검사에 적용되는지 확인해야 합니다. 검사 구성의 설정을 통해 페이지 유사성 및 기타 URL 중복을 기준으로 페이지를 필터링할 수 있습니다.

필터링은 검사를 최적화하여 속도를 향상시키는 데 효과적인 수단이지만, 이로 인해 검사 범위가 제한될 수 있습니다. 일반적으로 이러한 설정은 수동으로 조정할 수 있으며, 웹 사이트에 따라 다르게 적용해야 하는 경우도 있습니다.

마지막으로 고려해야 할 사항

애플리케이션은 공격자의 주된 표적이 됩니다. 애플리케이션의 보안 취약성을 검사하여 조치를 취하지 않으면 공격자가 이를 찾아내 각종 경로를 통해 침투할 수 있습니다. 최근 IBM 연구팀은 Android 프레임워크와 Firefox 브라우저에서 모바일 장치에 저장된 기업 데이터에 위험을 초래할 취약성을 발견했습니다. 또한, IBM HASM 서비스 팀은 AppScan 테스트를 통해 프로덕션 환경의 웹 애플리케이션 중 다수가 인젝션 취약성과 손상된 인증 문제를 가지고 있음을 확인했습니다. 위협을 방지하면서 모바일 장치 및 웹 애플리케이션을 통한 데이터의 접근성을 유지하는 가장 좋은 방법은 애플리케이션을 테스트하여 보안 취약성을 찾아내고 조치를 취하는 것입니다.

스팸과 그 시간적 지속성

최근의 스팸은 어떤 양상을 띠고 있습니까? 공격자들이 메일 수신함에 침투하고 탐지 기술을 피하기 위해 어떤 방법을 새롭게 개발하고 있는지 알아보십시오.

이메일 스팸 개발자와 스팸 탐지 시스템 간의 싸움은 1970년대 말에 시작된 이래, 지금도 계속되고 있습니다. 1BM X-Force 2011 동향 및 위험 보고서에서는 지난 10년간의 발전 과정을 되짚으면서 장기적 추세, 기법, 양적 측면에서의 극심한 변화 등 스팸의 진화를 광범위하게 분석한 바 있습니다.

그로부터 몇 년이 지난 지금, 몇 가지 흐름이 재현되고 있습니다. 일반 텍스트 스팸과 감염된 zip 파일을 포함한 스팸이 여전히 왕성한 기세를 떨치는 가운데, 공격자들은 탐지 기술을 피할 새로운 방법을 찾고 있습니다. MP3 파일 또는 PDF 첨부를 보내는 등의 수법은 별 효과를 거두지 못했고, 2005년에 처음 등장했던 이미지 기반 스팸이 새로운 모습으로 돌아왔습니다.

공격자들은 증권사기로 투기적 저가주를 팔아 치우거나 악성 컨텐츠로 사용자를 유도하는 등의 작전에서 공격 효과를 극대화하기 위해 메일 수신함에 침투하는 새로운 수법을 개발하고 있습니다.

스팸 진원지에 대한 또 다른 분석

스팸은 과거나 지금이나 심각한 문제입니다. 기업 네트워크에 악성코드를 유입시키는 주요 채널 중 하나이기 때문입니다. 2014년 3월에는 적발된 스팸의 양이 이전 2년 6개월 중 최고치를 기록했습니다. 그림 3은 지난 6개월간 가장 많은 스팸을 발생시킨 국가들을 정리한 것으로, 과거에 이름을 올렸던 국가 중 상당수가 여전히 상위에 있습니다(스팸 진원지 국가에 대한 추가 정보는 IBM X-Force 2013 중간 동향 및 위험 보고서 참조).

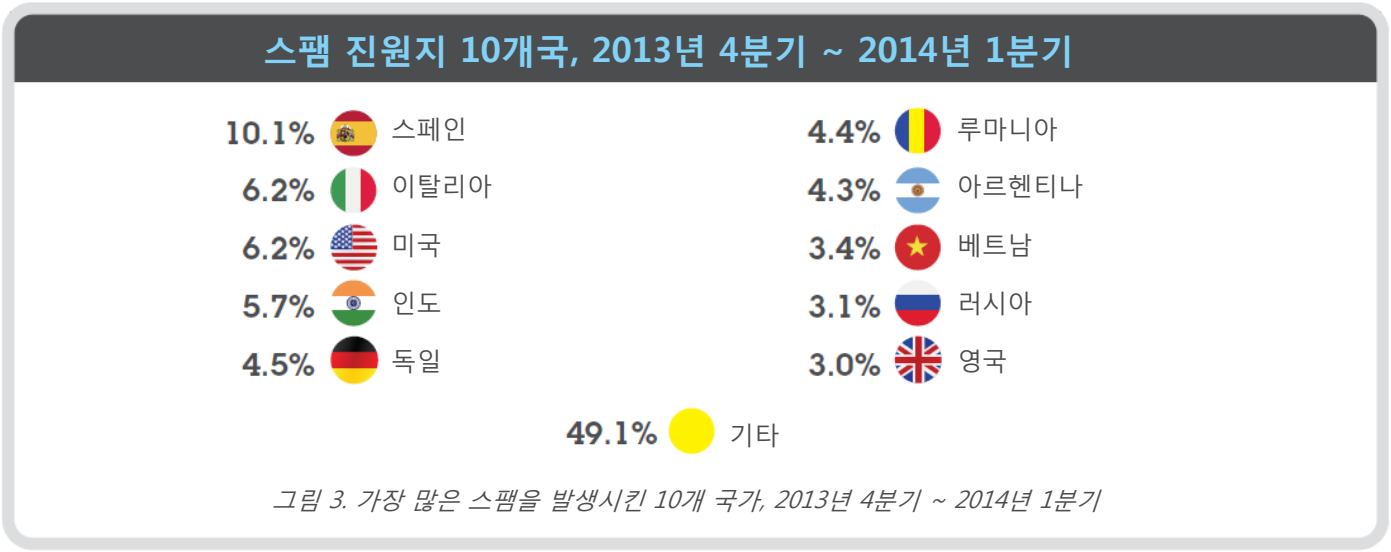


그림 3. 가장 많은 스팸을 발생시킨 10개 국가, 2013년 4분기 ~ 2014년 1분기

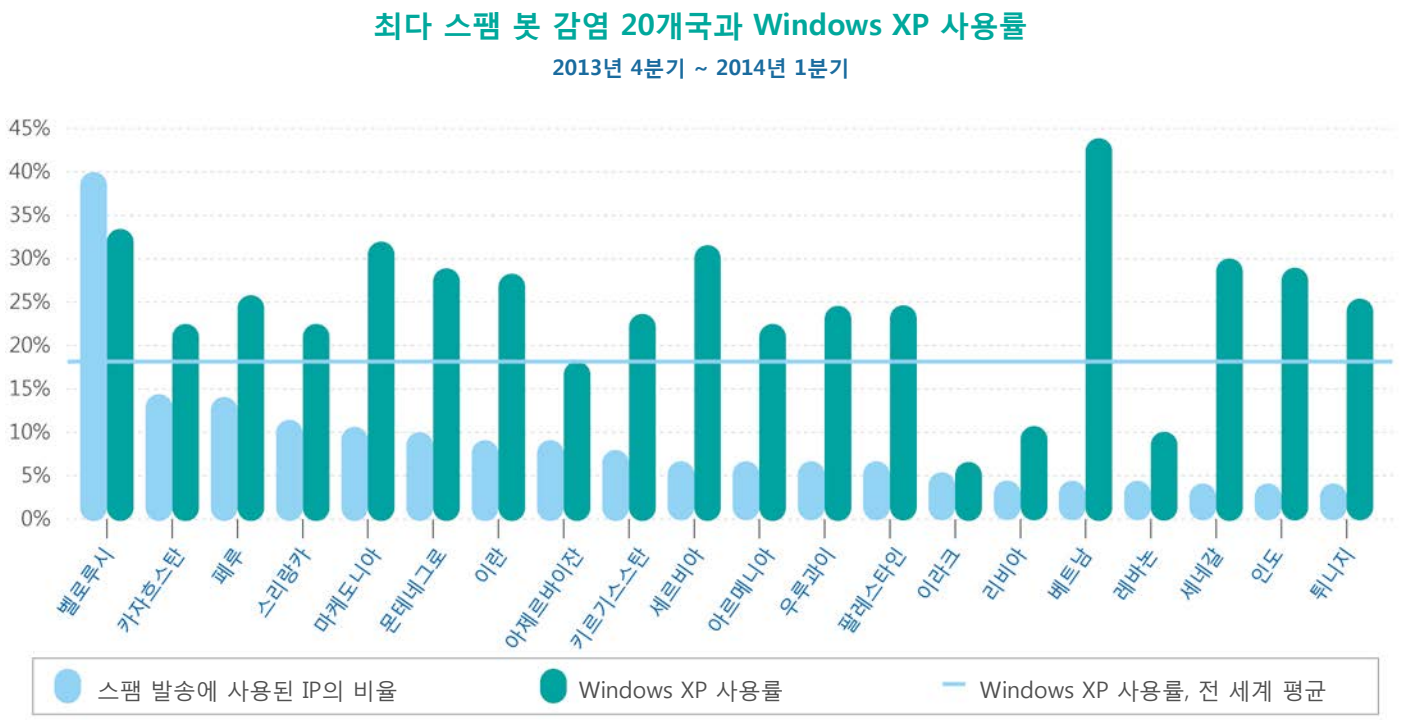


그림 4. 최다 스팸 봇 감염 20개국과 각각의 Windows XP 사용률, 2013년 4분기 ~ 2014년 1분기

• 데이터 출처: "StatCounter Global Stats: Top Desktop, Tablet and Console OSs Per Country from Oct to Dec 2013", "StatCounter Global Stats: Top Desktop, Tablet and Console OSs Per Country from Jan to Mar 2014", *StatCounter*, 2014년 5월 14일 기준
† "StatCounter Global Stats: Top 7 Desktop, Tablet and Console OSs from Oct 2013 to Mar 2014", *StatCounter*, 2014년 4월 17일 기준

스팸 봇 감염과 Windows XP 지원 종료

스팸 발송에 사용된 컴퓨터(IP 주소) 수의 비율을 계산하면 또 다른 흥미로운 사실이 드러납니다. 지난 6개월간 스팸 공격에서 확인된 IP 수를 국가별 총 IP 수와 비교한 결과는 그림 4와 같았습니다.

그림 4에 포함된 각 국가가 전 세계 스팸에서 차지하는 비율은 3% 미만이지만(인도와 베트남 제외) 스팸 봇 감염률은 놀랄 만큼 높습니다. 그 이유 중 하나는 최신 버전의 패치 또는 운영 체제를 사용하지 않는 컴퓨터가 많다는 점입니다. 현재 전 세계 컴퓨터의 약 18.4%에서 Windows XP가 계속 사용되고 있습니다.[5] 그러나 그림 4에 포함된 20개국 중 16개국은 Windows XP 사용률이 전 세계 평균보다 훨씬 높습니다. 30%를 넘어선 곳도 있으며, 베트남은 42.4%에 달합니다.

2014년 4월 8일, Microsoft는 Windows XP 운영 체제의 지원을 종료한다고 밝혔습니다.[6] 이는 오래 전부터 알려져 있던 사실이었던 만큼, 이미 상당수의 기업들은 대규모 사용자 기반을 새로운 버전으로 마이그레이션했습니다. 그러나 아직도 Windows XP에서 벗어나는 데 고충을 겪고 있는 기업이 있는가 하면, 아무 조치도 취하지 않고 있는 기업도 있습니다. 은행, 산업용 소프트웨어, 의료와 같은 특정 산업에서는 Windows XP 단종 발표로 어려움을 겪고 있습니다. 예를 들어, 미국에 설치된 ATM 중 95%는 Windows XP를 기반으로 하고 있어 집중적인 공격 표적이 될 우려가 있습니다.[7] 이러한 기업들은 Windows XP 지원이 종료된 시대에 맞닥뜨린 문제들을 해결해야 합니다.

다른 관점에서 보면, Windows XP 사용률은 대표적인 스팸 진원지로 꼽히는 국가들과 연관성이 있습니다. 이 통계에서 다음과 같은 사항을 확인할 수 있습니다.

- 바이러스 스팸 봇 감염이 널리 확산되어 있습니다.
- 최신 운영 체제와 애플리케이션을 사용하고 최신 보안 업데이트와 패치를 적용 및 유지하는 것이 엔드 유저와 취약한 서버를 스팸으로부터 보호하는 가장 효과적인 방법임에는 변함이 없습니다.

이미지 스팸의 재등장

이미지 스팸은 2006년과 2007년에 전성기를 누렸습니다. 2006년 10월에서 2007년 3월까지 이미지 첨부 파일을 포함한 스팸은 전체의 40% 이상을 차지했습니다. 그러나 2007년 여름 무렵 이미지 스팸 공격은 자취를 감추었었고, 이후 모습을 드러낸 것은 두 차례에 불과했습니다.

- 2008년 가을, 10월을 기점으로 이미지 첨부 파일 스팸의 비율은 13.5%였습니다(주간 측정 기준).
- 2009년 4월 말에 이미지 기반 스팸은 전체 스팸의 13%를 차지했습니다(주간 측정 기준).

2009년 4월부터는 이미지 스팸의 비율이 10%를 넘지 못했습니다. 가끔씩 이미지 스팸 공격이 나타나긴 했으나 주간 측정 기준으로 10% 미만에 머물렀습니다.

그러나 2013년 12월에 이미지 스팸이 다시 돌아왔습니다. 그림 5에서처럼, 이미지 스팸은 매우 큰 증가율을 보였습니다. 이 같은 공세는 12월 16일까지 계속되었는데, 이 기간 동안 이미지 기반 스팸의 공격은 거의 매일 발생했습니다. 일시적으로 잠잠해졌던 이 스팸은 12월 23일에 다시 대규모로 발생하기 시작하였습니다. 이 공격은 한 달간 지속되었고, 1월 8일에서 13일까지 다시 잠깐의 휴지기를 가진 다음 다시 개시되어 2014년 1월 22일에 끝이 났습니다.

그림 5에서 볼 수 있듯, 그로부터 한 달 후인 2월 24일에 또 다른 이미지 스팸 공격이 나타났습니다. 하지만 이번에는 사흘 만에 공격이 끝났습니다. 최근의 공격은 그 규모가 지난 12월과 1월의 절반 수준에 불과합니다.

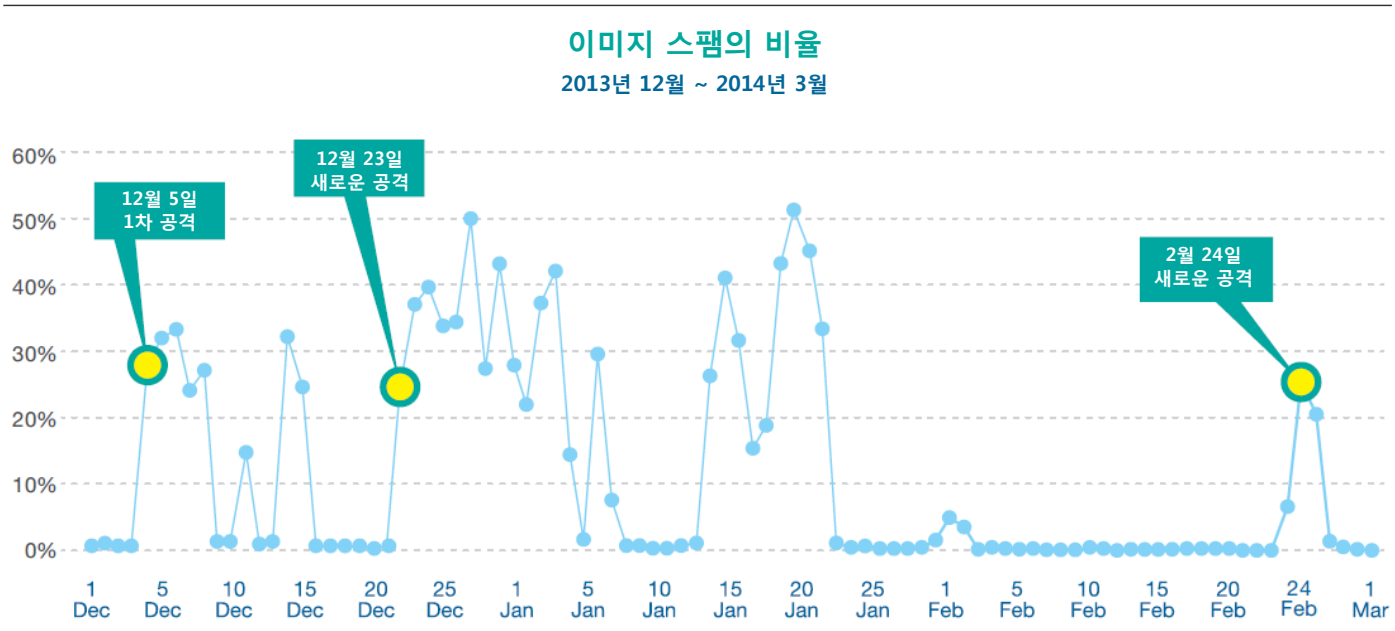


그림 5. 이미지 스팸의 비율, 2013년 12월 1일 ~ 2014년 3월 1일

특징	2013년 12월 ~ 2014년 1월의 공격	2014년 2월의 공격
광고 대상 제품	의료 용품	주식
두 공격 모두에 사용된 이미지 특징	최근에 공격자들이 이미지 스팸을 사용하는 방식은 이 기술이 처음 인기를 누렸던 2006년 ~ 2007년과 비교하면 몇 가지 다른 점이 있습니다. 처음에 공격자들은 이미지를 약간 수정하여 스팸 필터의 탐지를 피하는 데 집중하였습니다. 하지만, 많은 스팸 필터에서 첨부 파일의 스팸 여부를 판단하는 데 파일 해시를 사용하기 시작하자 공격자들은 색상이나 몇 개의 픽셀을 바꾸는 등 약간의 변형을 가해 이미지를 다른 파일처럼 보이게 하는 수법을 구사했습니다. 그러나 최근에 이루어진 공격에서는 이미지가 바뀌는 경우가 별로 없고, 스패머들이 동일한 이미지를 반복해서 사용하고 있습니다.	
이미지 특징	의료 용품이 이미지에 표시되었습니다.	특정 주식을 광고하는 텍스트 스크린샷이 표시되었습니다. 이 공격에서는 두 가지 이미지만 사용되었습니다.
URL 특징	이메일에서 이미지를 클릭하면 웹 사이트(주로 [...]doctor[...].ru 또는 [...]medic[...].ru)로 연결되었습니다. 이 URL은 거의 바뀌지 않았습니다.	URL은 사용되지 않았습니다. 스패머는 주식 종목명을 알려주고 수신자가 그 종목명을 검색하여 주식을 구입하게 했습니다.
두 공격 모두에 사용된 무작위 텍스트	이메일에서 이미지 아래에 많은 무작위 텍스트가 배치되었는데, 주로 Wikipedia 기사에서 발췌한 것이었습니다. 이 텍스트는 주로 베이지안(Bayesian) 필터와 같은 스팸 컨텐츠 필터에 혼란을 주기 위해 사용되었습니다.	
무작위 텍스트	텍스트가 흰색 배경에 매우 희미하게 쓰여져 있어 읽기 어려우며, 이미지의 바로 아래에 위치했습니다.	텍스트가 특별한 위장 없이 이메일에 표시되었지만, 이미지 아래 여러 개의 빈 줄을 삽입했기 때문에 사용자가 무작위 텍스트를 보려면 아래로 스크롤해야 했습니다.

표 1. 2013년 12월 ~ 2014년 1월과 2014년 2월의 이미지 스팸 공격에서 나타난 기술적 세부 사항

표 1은 이 최근의 공격에서 확인된 기술적 세부 사항을 요약한 것입니다.

X-Force는 이 두 가지 공격을 비교하여 다음과 같은 결론을 내렸습니다.

- 기술적으로 보면, 최근의 스팸 공격이 새로운 기술을 사용한 것은 아닙니다. 스팸 URL을 유지하기 위해 이미지 변형과 시간 간격을 사용하는 것은 오래된 수법입니다. 스패머들이 이러한 구식 기술을 구사한 이유는 알 수 없으나, 5년의 공백기가 있었기 때문에 스팸 필터가 대규모의 이미지 기반 스팸 공격에는 대비되어 있지 않다고 여기는 것으로 보입니다.
- 이 두 공격 간에는 유사점이 많이 발견되므로 동일한 스팸 툴킷에서 시작된 것으로 추측할 수 있습니다.
- 이미지 스팸은 여전히 관심을 모으는 중요한 문제입니다. 스패머들은 이미지 내에서만 메시지를 전송할 수 있는데, 일반적인 컨텐츠 분석 모듈은 텍스트 컨텐츠에서 정보를 추출할 수 없습니다. 이는 텍스트 컨텐츠 탐지 기술을 이용하는 스팸 필터의 스팸 탐지 기능에 영향을 줄 수 있습니다. 과거에 그랬던 것처럼, 스패머가 이미지를 통해 사용자에게 URL을 입력하라고 요청할 수도 있습니다. 이 URL은 드라이브 바이 다운로드로 사용자의 컴퓨터를 감염시킵니다. 이러한 맥락에서 보면, 이 새로운 이미지 스팸은 향후에 발생할 이미지 관련 스팸 공격의 테스트 버전일 수도 있습니다.

2014년이 이미지 기반 스팸의 귀환이 이루어지는 해가 될지 지켜보는 것도 흥미로울 것입니다.

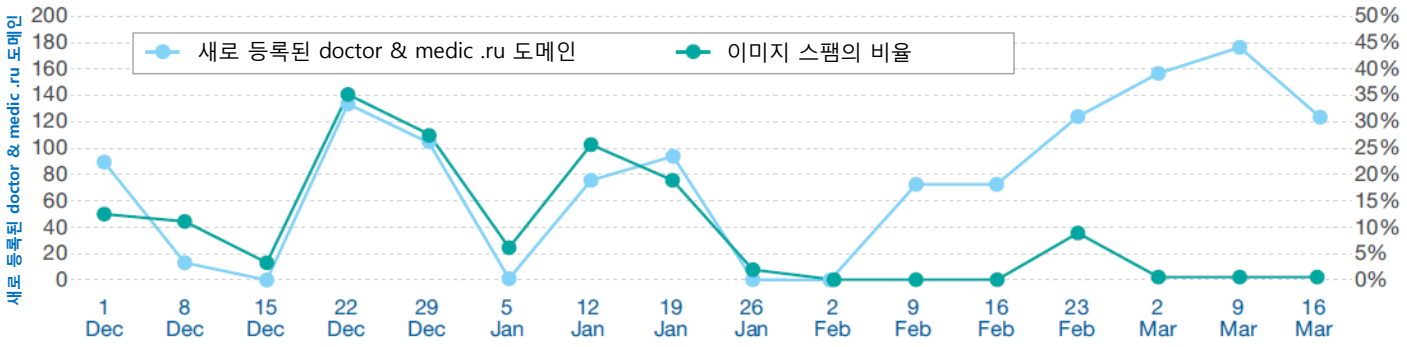


그림 6. 새로 등록된 doctor & medic .ru 도메인과 이미지 스팸의 비율 비교(주간) 2013년 12월 ~ 2014년 3월

그림 6에서처럼, 이번 공격에서는 doctor 및 medic .ru 도메인이 사용되었습니다. 여기서 생기는 의문은, 스패머들이 여전히 [...]doctor[...].ru 또는 [...]medic[...].ru 도메인을 등록하는 메커니즘을 사용하는가입니다. 그 답은 '예'입니다.

2013년 12월 초부터 2014년 1월 말까지 새로 등록된 [...]doctor[...].ru 또는 [...]medic[...].ru 도메인의 수는 이미지 기반 스팸의 비율과 상관관계가 있습니다. 그러나 2014년 2월 초부터 이 도메인들은 이미지 기반이 아닌 다른 스팸 유형에 사용되었습니다.

흥미롭게도, 이미지 기반 스팸을 보내는 스패머들은 이러한 도메인을 여전히 오랫동안(몇 시간 혹은 24시간 이상) 사용하고 있습니다. 이 공격 수명은 지난 4개월간의 관찰에서 변화가 없었습니다. 스팸에 쓰이는 URL치고는 긴 시간입니다. 대부분의 스패머들은 도메인을 몇 시간이나 몇 분간만 사용합니다. 스팸 필터의 대부분은 이메일에 포함된 URL을 검사하여 과거에 스팸에 사용된 적이 있다면 차단하기 때문입니다. 스패머들은 도메인을 소유하고 있어 사용자가 URL을 얼마나 오랫동안 클릭하는지 쉽게 파악할 수 있습니다. 어떤 도메인이 하루 이상 사용되어도 스팸 필터가 스팸을 걸러내지 못할 수 있으며, 사용자가 아직 스팸 필터를 사용하지 않고 있을 수도 있습니다.

원거리 사고 대응 시 5가지 고려 사항

보안 사고는 어디서든 일어날 수 있습니다. IT 팀이 원거리 사고에 대비할 수 있는 방법을 알아보십시오.

옛날에는 사고 대응을 위해 각 고객 사이트를 직접 찾아가야 했습니다. 따뜻한 열대 섬에 있는 고객으로부터 전화가 걸려오면 대응 팀은 쾌재를 부르곤 했습니다.

이제는 상황이 바뀌었습니다. 개인 정보 보호 규정이 강화되고 보안 사고의 중대성이 커짐에 따라, 기업들은 그 어느 때보다도 신속하고 효율적으로 응답을 할 수 있어야 합니다. 어떤 국가에서는 보안 사고가 확인된 경우는 물론, 사고가 의심되는 경우에도 며칠 내에 당국에 신고를 해야 합니다. 이에 따라 IBM Global Technology Services - ERS(Emergency Response Services)와 같은 사고 대응 팀은 사고를 신속하게 처리하기 위한 방법론을 개발하고 분류 툴을 활용하고 있습니다. 이들은 이러한 툴과 방법론을 통해 손상된 시스템에서 RAM 및 이벤트 로그 등의 관련 아티팩트를 신속하게 수집하고, 원격 분석가에게 전송함으로써 분석이 빨리 이루어질 수 있도록 합니다.

그러나 보안 사고와 관련 있는 것으로 추정되는 정보 시스템이 있는 지역에 사고 대응 조치를 지원할 인프라가 없다면 어떻게 될까요? 신속한 진단과 평가를 위해 사고 대응 분석가에게 주요 아티팩트를 전송해야 하는데 인터넷 대역폭이 부족하다면 또 어떻게 될까요? 그리고 정보 시스템이 위치한 곳이 멀리 떨어진 저개발 국가라서 출장이 불가능하며 숙련된 IT 전문가도 없다면 어떻게 해야 할까요?

IBM ERS 팀은 이러한 상황을 점점 더 자주 만나게 되었습니다. 기업들이 기존 시장의 경계를 넘어 사업을 확장함에 따라, 원거리 사고 대응을 해야 하는 경우가 더 빈번해지고 있습니다. 멀리 떨어진 국가 또는 인프라가 부족한 지역에서 일어난 사고에 대처하려면 특별한 전략이 필요합니다.

이 섹션에서는 매우 멀리 떨어진 정보 시스템에서 사고가 발생했을 때 반드시 고려해야 할 5가지를 소개합니다. 기술과 관련된 것도 있고 관리 측면의 요소도 있으며, 모두 똑같이 중요한 사항입니다.

원거리 사고 대응 시 고려 사항

1. 대역폭
느리고 불안정한 연결 때문에 데이터 전송에 제약을 받을 수 있습니다.

2. RAM
RAM 덤프 파일을 저장하는 데 외부 드라이브를 사용하지 못할 수 있습니다.

3. 특급 배송
손상된 시스템과 포렌식(Forensic) 데이터를 전달하기 어려울 수 있습니다.

4. 근무 시간
시간대가 달라 작업 일정에 차질이 생길 수 있습니다.

5. 기술력
시스템 관리자가 사고 대응 훈련을 받지 못했을 수 있습니다.

그림 7. IBM Global Technology Services - Emergency Response Services(ERS) 팀의 원거리 사고 대응 시 5가지 고려 사항

1. 대역폭이 가장 중요합니다.

모든 보안 사고가 데이터 센터나 산업화된 국가와 같이 대역폭이 충분한 곳에서 일어나는 것은 아닙니다. 따라서, 사고 대응 팀은 느리고 불안정한 네트워크 연결 환경에서 작업해야 할 수 있습니다. 이러한 상황은 사고 대응에 불리하게 작용할 수 있습니다. 일반적으로 ERS 팀이 보안 사고에 투입되면 ERS 분석가는 특정 파일(로그, 악성코드 샘플, RAM, 기타 아티팩트 등)이 전송되는 즉시 분석에 착수합니다. 몇 기가바이트의 파일을 보내기 위해서는 어느 정도의 시간이 걸리지만, 이는 가장 실용적인 방법입니다. 멀리 떨어져 있는 정보 시스템으로 분석가를 파견하거나 하드 드라이브를 보내는 것보다 ERS가 분석을 더 빨리 시작할 수 있기 때문입니다.

대역폭의 제약이 있을 경우 대응 팀은 상대적으로 작은 아티팩트를 위해 규모가 크고 가치 있는 정보 시스템 아티팩트를 제거해야 합니다. 정보 시스템 아티팩트들을 없애면 분석 결과를 얻는 데 오랜 시간이 걸리고 결과의 확실성도 낮아지며 대응을 위한 전반적인 비용 또한 증가할 수 있습니다. 제한적인 대역폭은 이미 검증된 분석 방법인 배스천(Bastion) 호스트 또는 점프박스를 사용하여 원거리 시스템에 연결하는 데에도 방해가 됩니다.

배스천 서버란?

베스천 호스트[9]는 공격에 완전히 노출되는, 특별한 용도의 컴퓨터입니다. 이 컴퓨터는 방화벽 또는 필터링 라우터의 보호를 받지 않는 DMZ의 공용 구역에 위치합니다. 베스천 호스트는 이와 같이 노출된 상태에서 프록시 서버와 같은 특별한 역할을 수행하도록 구성되며 불필요한 서비스와 프로토콜, 프로그램, 네트워크 포트는 모두 비활성화되거나 제거됩니다. 배스천 호스트는 침입자의 액세스를 통제하고 잠재적 공격 방법을 제한하도록 하드닝(Hardening)됩니다.

2. RAM을 사용하지 못할 수 있습니다.

사고 대응 팀에게 가장 귀중한 아티팩트 중 하나는 손상된 시스템의 RAM입니다. 최신 PC 시스템의 RAM은 종합적인 증거 자료를 찾을 수 있는 가장 유용한 장소이며, 이러한 관점에서 보면 RAM보다 더 중요한 곳은 없습니다. 개방된 포트, 네트워크 연결, 실행 중인 프로세스에 관한 세부 사항 등, RAM에는 여러 값진 정보들이 포함되어 있습니다.

RAM을 사용하지 못하게 되는 경우는 왜 생길까요? IBM ERS 팀의 경험에 따르면, 원거리 프로젝트는 두 가지의 큰 문제를 수반합니다. ERS는 여러 원거리 프로젝트에서 RAM을 수집하는 데 많은 어려움을 겪었습니다. 첫째, 특히 하이엔드 서버에서 RAM 파일이 매우 커질 수 있으며, 압축 후에도 8GB를 초과하곤 합니다. 인터넷 대역폭과 안정성 문제가 있으면 큰 파일을 전송하는 데 지나치게 많은 시간이 걸리거나 전송이 아예 실패할 수 있습니다. 둘째, RAM을 수집하면 이를 USB 장치와 같은 외부 장소에 덤프해야 합니다. ERS는 RAM 덤프 파일을 저장할 USB 장치가 없어 곤란했던 적이 여러 번 있었습니다. USB 장치를 당장 구할 수 없는 경우, 가까운 곳에서 전자 소매업체를 찾을 가능성도 희박하다고 볼 수 있습니다. 나이지리아 연안의 석유 굴착 장치 또는 우간다 시골 마을에서 시스템 장애가 일어나는 상황이 여기에 해당됩니다.

전체 RAM 덤프 파일에 대한 액세스는 불가능하더라도 RAM에 저장된 데이터에 대한 액세스 또는 시스템 관리자를 통한 액세스는 가능할 수 있습니다. 그다지 효율적이지는 않지만 기본적인 방식을 사용하여 로그인한 사용자, 열려 있는 파일, 예약된 작업, 기타 정보를 수집할 수 있을 것입니다. RAM을 사용할 수 없는 상황이든 대응 팀이 비효율적인 방법을 사용하는 상황이든, 휘발성 데이터 수집 시 직면할 수 있는 문제에 대비를 해야 합니다.

최소한의 대역폭이라는 제약조건이 있고 RAM 덤프에 액세스할 수 없다고 해서 사고 대응이 불가능한 것은 아닙니다. 그러나 대응 팀이 이처럼 열악한 환경에서 작업하는 데 익숙하지 않다면 미리 대비를 해야 합니다. 대역폭이 부족하거나 RAM 덤프를 사용할 수 없는 지역에 정보 시스템이 있는 경우라면, 이러한 문제를 염두에 두고 방법론과 교육을 확립해야 합니다. 그렇지 않으면 이 문제가 심각한 장애물이 될 수 있습니다.

3. 특급 배송 서비스가 없을 수도 있습니다.

IBM ERS 팀의 국내 고객은 특급 배송 서비스를 이용하여 문제의 시스템 또는 수집한 데이터를 ERS 대응 분석가에게 보내곤 합니다. 익일 배송업체를 이용하면 포렌식(Forensic) 이미지, 수집한 RAM, 로그 파일 또는 전체 시스템까지 빠르면 12시간 만에 보낼 수 있습니다. 또한, 오프라인이나 온라인을 통해 다른 나라에 데이터를 전송하려는 경우 데이터 전송에 방해가 될 규정이 있는지 확인해야 합니다. 분석 결과를 최대한 빨리 얻어야 하는 시급한 상황인 경우, 익일 배송 서비스는 효과적인 선택입니다.

하지만 정보 시스템과 데이터가 있는 곳에서 익일 배송 서비스를 이용할 수 없다면 어떨까요? 앞서 언급했던 석유 굴착 시설이 이러한 지역에 있다면, 시스템이나 파일을 전송할 수 없을 것입니다. UPS, FedEx와 같은 서비스가 제공되는 국가라 할지라도 컴퓨터와 같은 고가의 품목을 보내려면 통관에 며칠이 걸릴 수도 있습니다. 되도록 빨리 답변을 받아야 하는 상황에서 지연이 발생하면 신속하고 효과적인 대응을 하는 데 지장을 미칠 것입니다.

4. 근무 시간이 일정에 차질을 줄 수 있습니다.

사고 대응 과정에서, ERS는 근무 시간에 분석이 진행되는 동안 담당자(예: 시스템 관리자)에게 요청을 전달합니다. 이는 유동적인 절차이며, 대부분의 보안 사고는 심각도가 높으므로 시급하게 요청이 처리되어야 합니다.

멀리 떨어져 있는 지역의 기업을 위해 보안 사고 의심 사례를 분석해야 하는 경우에는, 이와 같은 과정을 원활하게 진행하기 힘들어집니다. 시차로 인해 담당자의 근무 시간이 몇 시간 빠르거나 느릴 수 있고, 근무 시간이 거의 겹치지 않을 수도 있습니다. 이러한 제약 때문에 대응 팀은 자신의 근무 시간을 조정하거나 여러 요청을 모아 한꺼번에 전달해야 합니다. 이후 24시간 동안 추가 요청이 처리되지 않을 수 있으므로, 분석가는 분석을 진행하는 데 필요한 사항을 신중하게 결정해야 합니다.

5. 기술력이 부족할 수 있습니다.

ERS 사고 대응 팀이 보안 사고를 처리할 때, 일반적으로는 뛰어난 실력을 갖춘 시스템 관리자와 함께 할 수 있습니다. 이렇게 협업하여 사고를 해결하는 데에는 며칠이 걸릴 수도 있고 몇 주가 걸릴 수도 있습니다.

그러나 ERS가 매우 멀리 떨어진 지역에 대한 프로젝트를 수행할 때는 숙련된 시스템 관리자 심지어 초보적인 수준의 기술력을 가진 담당자마저 없는 경우가 많습니다. 사고 대응 팀은 원거리 환경을 지원할 때 이러한 제약을 염두에 두고 모든 지침, 질문, 기타 커뮤니케이션을 최대한 구체적으로 전달하여 잘못 해석될 여지가 없도록 하고 높은 수준의 기술력에 의존하지 않도록 해야 합니다.

시차 및 기술력 부족으로 인한 어려움을 최소화하는 방법 중 하나는 사고 대응을 위한 SME(Subject Matter Expert)를 여러 지역에 두는 것입니다. 이 SME가 사고 대응 전문가일 필요는 없습니다. 최소한의 훈련을 받은 시스템 관리자로서 기본적인 사고 대응 지식과 기술력을 갖춘 사람이라면 사고 발생 지역에서 SME로 지원을 제공할 수 있습니다. 최초 대응, 데이터 보존, 조사 방법론에 대한 기본 지식을 갖춘 현지 SME가 있으면 몇 주가 아닌 며칠 만에 사고를 해결할 수 있습니다.

핵심은, 매우 멀리 떨어진 지역에서도 사고 대응이 가능하다는 것입니다. 그러나 대응 팀은 운영 절차를 조정하고 다른 전술을 개발하고 한정된 데이터로 작업을 할 수 있도록 대비해야 합니다. 제약사항을 인식하고 그에 따라 조정을 하면 달갑지 않은 장애물이 나타나도 이를 극복하고 성공적으로 대응할 수 있습니다.

X-Force 소개

정교화된 위협은 모든 곳에 도사리고 있습니다. IBM 전문가의 통찰력을 활용하여 위험을 최소화하십시오.

IBM X-Force 연구 개발 팀은 취약성, 익스플로잇, 능동적 공격, 바이러스 및 기타 악성코드, 스팸, 피싱 및 악성 웹 컨텐츠를 포함한 최신 보안 위협 동향을 연구 및 모니터링합니다. X-Force는 고객 및 대중에게 새롭게 나타난 치명적인 위협에 대한 정보를 제공할 뿐만 아니라, IBM의 고객을 이러한 위협으로부터 보호하기 위한 보안 컨텐츠를 제공합니다.

IBM Security 관련 협업

IBM Security는 여러 브랜드를 통해 광범위한 보안 역량을 제공합니다.

- X-Force 연구 개발 팀은 광범위한 컴퓨터 보안 위협, 취약성, 그리고 공격자가 이용하는 최신 동향 및 방법을 발견, 분석, 모니터링 및 기록합니다. IBM 내부의 다른 그룹들은 이러한 풍부한 데이터를 이용해 IBM 고객을 위한 보호 기술을 개발합니다.
- IBM 회사인 Trusteer[8]는 종합적인 엔드포인트 사이버 범죄 예방 플랫폼을 제공하여 금융 사기 및 데이터 유출 사고로부터 기업을 보호합니다. 수백 곳의 조직 및 수천만 명의 엔드 유저가 Trusteer를 통해 웹 애플리케이션, 컴퓨터 및 모바일 장치를 정교화된 악성코드, 피싱 공격과 같은 온라인 위협으로부터 보호하고 있습니다. 우수한 연구 전담 팀에 의해 제공되는 Trusteer의 차별화된 실시간 인텔리전스를 이용하면 클라우드 기반 플랫폼을 최신 위협에 대해 신속하게 적응시킬 수 있습니다.
- X-Force 컨텐츠 보안 팀은 크롤링, 독립적 추적 및 IBM Managed Security Services에서 제공하는 피드를 통해 독립적으로 웹을 검색 및 분류합니다.
- IBM Managed Security Services는 10개의 보안 운영 센터를 가동하면서 전 세계 고객에게 24시간 상시 관리형 보안 서비스와 툴, 전문성을 제공함으로써 엔드포인트, 서버(웹 서버 포함), 애플리케이션, 일반 네트워크 인프라를 노리는 익스플로잇 공격을 감시합니다. 보안 전문가들은 수천에 달하는 고객사를 위해 각종 익스플로잇, 공격, 사고를 추적합니다.
- IBM Professional Security Services는 전사적인 보안 평가, 설계, 구축 서비스를 제공하여 효과적인 보안 인텔리전스 전략을 수립하고 성공적인 정보 보안 솔루션을 개발할 수 있도록 지원합니다.
- IBM QRadar® Security Intelligence Platform은 SIEM(Security Intelligence and Event Management), 로그 관리, 구성 관리, 취약성 평가 및 이상 항목 발견을 위한 통합 솔루션을 제공합니다. 또한, 통합 대시보드와 실시간 분석 기능을 통해 사람, 데이터, 애플리케이션, 인프라 전반의 보안 및 규정 준수 관련 위험을 조명합니다.
- IBM Security AppScan은 취약성을 파악하고 보고서를 생성하여 편리하고 지능적인 해결 방법을 조언함으로써 웹 및 모바일 애플리케이션의 보안 평가, 애플리케이션 보안 프로그램 관리 강화, 규정 준수를 지원합니다. IBM HASM(Hosted Application Security Management) 서비스는 프리프로덕션 및 프로덕션 환경 모두에서 AppScan을 사용하여 웹 애플리케이션에 대한 동적 테스트를 수행하는 클라우드 기반 솔루션입니다.

도움 주신 분들

IBM X-Force 보안 동향 및 위험 보고서는 IBM의 전사적인 협업을 통해 제작되었습니다. 본 보고서의 간행과 관련하여 관심을 가지고 공헌해 주신 다음 분들께 감사의 말씀을 드립니다.

도움 주신 분	직위
Andrew Cranke	IBM HASM 수석 애플리케이션 보안 컨설턴트
Anik Campeau	IBM HASM 애플리케이션 보안 컨설턴트
Diana Kelley	IBM Security AppScan 애플리케이션 보안 전략가
Dr. Jens Thamm	IBM X-Force 컨텐츠 보안 데이터베이스 담당 매니저
JohnAdams	IBM Global Technology Services - ERS 수석 사고 대응 분석가
Leslie Horacek	IBM X-Force 보안 위협 대응 담당 매니저
Marc Noske	IBM X-Force 컨텐츠 보안 데이터베이스 담당 매니저
MarkWallis	IBM Security Systems 수석 정보 개발자
PamelaCobb	IBM X-Force & 보안 인텔리전스 글로벌 시장 부문 매니저
Ralf Iffert	IBM X-Force 컨텐츠 보안 매니저
Rob Lelewski	IBM Global Technology Services - ERS 프로젝트 리더
Robert Freeman	IBM X-Force 선임 연구 담당 매니저
Thomas Millar	IBM Global Technology Services - ERS 수석 사고 대응 분석가

추가 정보

IBM X-Force에 대한 추가 정보를 확인하려면 ibm.com/security/xforce/를 방문해 주십시오.

[1] Chris Poulin, "What to Do to Protect against Heartbleed OpenSSL Vulnerability," *IBM Security Intelligence Blog*, 10 April 2014. http://securityintelligence.com/heartbleed-openssl-vulnerability-what- to-do-protect/

[2] Roee Hay, "New Vulnerabilities in Firefrox for Android: Overtaking Firefox Profiles," *IBM Security Intelligence Blog*, 26 March 2014. http://securityintelligence.com/vulnerabilities-firefox-android-overtaking-firefox-profiles/

[3] Roee Hay, "A New Vulnerability in the Android Framework: Fragment Injection," *IBM Security Intelligence Blog*, 10 December 2013. http://securityintelligence.com/new-vulnerability-android-framework- fragment-injection/

[4] "OWASP Top 10 for 2013," *OWASP*, 12 June 2013. https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

[5] "StatCounter Global Stats: Top 7 Desktop, Tablet and Console OSs from Oct 2013 to Mar 2014," *StatCounter*, Accessed 17 April 2014. http://gs.statcounter.com/#os-ww-monthly-201310-201403-bar

[6] Enterprise Customers: Support for Windows XP has ended," *Microsoft*, April 2014. https://www.microsoft.com/en-us/windows/enterprise/ end-of-support.aspx

[7] Jose Pagliery, "95% of bank ATMs face end of security support," *CNNMoney*, 4 March 2014. http://money.cnn.com/2014/03/04/technology/security/atm-windows-xp/?iid=EL

[8] Trusteer, Ltd. was acquired by IBM in September of 2013.

[9] Kurt Dillard, "Intrusion Detection FAQ: What is a bastion host?" *The SANS Institute*, Accessed 13 May 2014. http://www.sans.org/security- resources/idfaq/bastion.php

Please Recycle

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
2014년 6월

WGL03050-KRKO-00