IBM X-Force® 2010년
상반기 동향 및 리스크 보고서

기고가

X-Force 상반기 동향 및 리스크 보고서는 IBM 전체에 걸친 협업을 통한 노력을 바탕으로 제작되었습니다. 당사는 본 보고서의 출판에 많은 관심과 노력을 기울여 주신, 다음 분들께 감사의 말씀을 전하고자 합니다.

기고가	직함
Bryan Williams	X-Force 연구 개발(R&D), 보호 기술
Carsten Hagemann	X-Force 소프트웨어 엔지니어, 컨텐츠 보안
Jens Thamm 박사	데이터베이스 관리 컨텐츠 보안
Frank (Jamie) Licitra	X-Force 제품 매니저
Harold Moss	보안 전략 – 신흥 기술 및 클라우드 컴퓨팅 기술 설계사
Jon Larimer	X-Force 고급 연구, 악성코드
Leslie Horacek	X-Force 위협 대응 관리자
Marc Noske	데이터베이스 관리, 컨텐츠 보안
Mark E. Wallis	선임 정보 개발자, X-Force 데이터베이스 팀
Michael Waidner	보안 담당 CTO, IBM 보안 전략
Michelle Alvarez	팀 리더, MSS 인텔리전스 센터 (Eagle Eyes)
Mike Warfield	선임 위저드, X-Force
Ralf Iffert	매니저, X-Force 컨텐츠 보안
Ravi Srinivasan	IBM Software Group, Tivoli 수석 제품 매니저
Robert Freeman	선임 기술자 겸 웹 공격 감시인
Ryan McNulty	IBM Managed Security Services 및 SQL Querier 권위자
Scott Moore	X-Force 소프트웨어 개발자 겸 X-Force 데이터베이스 팀장
Tom Cross	매니저, X-Force 고급 연구
Wangui McKelvey	X-Force 제품 마케팅 매니저

X-Force 정보

IBM X-Force® 연구 및 개발 팀은 취약점, 취약점을 악용한 공격(Exploits) 및 적극적 공격, 바이러스 및 기타 악성코드, 스팸, 피싱 및 악성 웹 컨텐츠를 포함한 최근의 위협 동향을 연구하고 모니터링합니다. X-Force는 고객과 일반 대중을 상대로 한 중요한 새로운 위협에 대처하는 방법을 알림은 물론, 이 같은 위협으로부터 IBM 고객을 보호하기 위한 보안 컨텐츠를 제공합니다.

차례
I 부

차례
II 부

개요

2010년의 반환점을 지나 하반기로 접어드는 지금, 크게 변하고 있는 세상에서 변치 않는 것이 하나 있습니다. 그것은 바로 공격자들이 빠른 기술의 진보를 끊임없이 악용하여 지적 재산을 훔치는 등의 방법으로 금전적인 이익을 취하고자 한다는 것입니다. X-Force는 2009년 말에 위협 환경의 진화에 대해 보안 종사자와 공격자의 관점에서 모두 요약한 바 있습니다. 양측이 사용하는 도구는 더 많은 기술과, 더 나은 자동화 그리고 더 관리하기 쉬운 사용자 경험이라는 말로 요약됩니다. 상용 소프트웨어만큼 정교한 풍부한 기능을 갖춘 맞춤 설계 악성코드가 부상하는 모습도 보였습니다. 최근의 이 같은 위협은 단일 진입 지점에 초점을 맞추지 않고 기업 내 여러 리소스를 적극적으로 공략하여 성공적인 공격이 이루어지도록 보장합니다. 이제는 더 이상 일반 대중과 접촉하는(Public-Facing) 한 가지 리소스만 가장 큰 위험에 노출되는 것이 아니라, 모든 직원과 말단컴퓨터(Endpoint)가 잠재적인 진입 지점이 되었습니다. 취약점 공격, 스팸, 피싱, 악성 URL 및 소셜 엔지니어링의 정교한 조합은 모두 과거 어느 때보다도 더 쉽게 난독화하고 자동화하고 배포할 수 있습니다.

기업과 세계 경제는 전환기를 거치고 있습니다. 기업은 신기술의 도움으로 작업을 단순화함에 따라 사업부를 병합하고 조직의 크기를 축소하고 있습니다. 기업의 미시환경 안에서 일어나고 있는 이런 모든 변화 속에서, 당사는 그로 인해 초래될 수 있는 혼란과 적응해야 한다는 요구로 인해 임직원이 느끼는 부담감을 이해합니다. 무엇을 보호해야 할까요? 새로운 시장으로 확장하고 신기술을 채택함에 따라 보안 전망은 어떻게 바뀌었을까요?

전통적인 보안 솔루션은 새로운 난독화 방법과 소량 공격 벡터에 효과적으로 대처할 수 없게 되었습니다. SQL Injection과 XSS(Cross-Site Scripting)를 통해 웹 서버를 공략하는 공격은 새로울 것이 없지만, 이런 공격은 점점 창의적으로 은폐되어 여러 보안 제품을 우회하고 있습니다. 직원은 그들이 매일 업무에 사용하는 PDF 파일이나 오피스 문서 같은 문서를 통해 직접 공격을 받고 있습니다.

위협의 역학은 계속하여 엄청난 속도로 진화하고 있기 때문에, 미래에 더 철저히 대비할 수 있도록 새로 전개되는 동향을 살펴보는 것은 더욱 중요해졌습니다.

새로운 지면 배치와 디자인

올해에는 상반기 보고서의 구조와 지면 배치를 재구성하여 크게 두 부분으로 나누었습니다. 1 부에서는 주요 토픽과 주요 최신 동향을 살펴보고, 2부에서는 과거 상반기 보고서에서 많이 다뤘던 내용인 심층적인 위협 데이터와 독자들이 IBM Security Solutions에게 기대하는 세밀한 분석을 제시하게 될 것입니다.

2010년 상반기 특징

취약점 및 공격

- APT(Advanced Persistent Threat) – 이 정교해진 공격 수단을 사용하는 공격자들에 대해 가장 우려되는 점은 네트워크 보안 기술 및 방법이 상당한 발전을 이룩했음에도 불구하고 방어 수준이 높은 네트워크를 성공적으로 침투해내는 공격자들의 능력이 점점 정교해진다는 것입니다. 최신 보안 시스템의 감시망을 피하는 점점 난독화되는 공격과 숨은 악성코드 명령 및 제어 채널은 특히 우려됩니다.
- 난독화, 난독화, 난독화 – 공격자들은 JavaScript 및 PDF 난독화를 통해 악성 트래픽을 위장하는 새로운 방법을 계속 찾아내고 있습니다. 난독화는 소프트웨어 개발자와 공격자가 모두 애플리케이션 개발에 사용한 코드를 숨기거나 가리기 위해 사용하는 기법입니다. 네트워크 보안 제품이 간단히 모든 난독화된 JavaScript 스크립트를 차단할 수 있다면 일은 훨씬 쉬워질 테지만, 안타깝게도 난독화 기법은 여러 합법적인 웹사이트가 능력 수준이 낮은 웹 개발자에게 코드를 도난 당하지 않기 위해 사용하기도 합니다. 이런 합법적인 웹사이트는 본의 아니게 악성 웹사이트를 은폐하는 역할을 하기 때문에 공격을 찾아내기가 매우 어려워집니다.
- PDF 공격은 공격자들이 사용자를 새로운 방법으로 속이려 함에 따라 계속 증가하고 있습니다. 말단컴퓨터(Endpoint)가 기업 조직에서 일반적으로 가장 취약한 연결 고리라는 점을 생각하면, PDF가 공격의 대상이 되는 이유를 쉽게 이해할 수 있습니다. 공격자는 이 사실을 잘 알고 있습니다. 예를 들면 특정한 말단컴퓨터에는 민감한 데이터가 없을 수 있지만, 해당 말단컴퓨터는 민감한 데이터가 있는 다른 말단컴퓨터를 액세스할 권한을 갖고 있을 수 있습니다. 아니면, 해당 말단컴퓨터는 다른 컴퓨터를 공격하기 위한 유용한 발사 지점(Bounce Point)으로 사용될 수 있습니다.
- 발표된 취약점은 사상 최고 수준을 기록하고 있습니다. 2010년에는 공격코드(Exploit)의 공개 발표가 크게 증가하고 여러 소프트웨어 대기업이 보안 취약점을 가려내고 완화하기 위한 긍정적인 노력을 기울임으로 인해 노출된 보안 취약점의 양이 크게 증가했습니다.
- 웹 애플리케이션 취약점의 비중은 55%까지 조금씩 증가하여 2010년 상반기에 노출된 모든 취약점의 절반 이상을 차지하게 되었습니다.
- 공격 노력 대비 잠재적인 보상 – 공격자가 정말로 얻고자 하는 것은 무엇일까요? 취약점 발표의 수가 증가하고 업체들이 문제 부분에 대한 패치와 보호 수단을 분주하게 제공하는 가운데, 기업은 어떻게 IT 관리자가 기울이는 노력의 우선순위를 최적화하여 충분한 보안을 보장할 수 있을까요? 공격 노력 대비 잠재적 보상 매트릭스(Exploit Effort Versus Potential Reward Matrix)는 취약점의 분류를 공격자의 관점에서 생각해 볼 수 있는 간단한 모델을 제시합니다.

악성코드와 악성 웹

- Conficker 웜은 지난 몇 년 간 가장 크게 보도된 컴퓨터 보안 문제였으므로, 이에 대한 새로운 동향 보고는 반드시 필요할 것입니다. 2009년 이후에 Conficker 웜은 어떻게 되었을까요?
- Zeus 봇넷은 계속하여 기업 및 단체를 교란시키고 있습니다. 2010년 초에는 Zeus 봇넷 키트의 업데이트 버전이 Zeus 2.0이라는 이름으로 배포되었습니다. 이 버전에 새로 포함된 주요 특징은 공격자에게 업데이트된 기능을 제공합니다.
- BlackHat SEO 및 악성(Rogue) 바이러스 백신 공격은 여전히 최종 사용자를 속임으로써 기업에 침투하고 있습니다.
- 악성 웹 툴킷 – Gumblar 툴킷이 계속 보급됨에 따라 Adobe는 여전히 공격에 가장 많이 사용되는 제품으로 남아 있으나, PDF와 Flash의 취약점을 악용한 공격 역시 여러 다른 공격 툴킷 사이에서 매우 인기가 높습니다. ActiveX가 적어도 당분간 5위 목록에서 모습을 감춘 것은 2009년 하반기와는 다른 흥미로운 변화입니다.

스팸과 피싱

- 최고 스팸 도메인은 중국(.cn)에서 러시아(.ru)로 바뀌었습니다.
- 2010년 3월 중순 이후 스팸의 평균 크기는 2배로 커졌지만, 이미지 기반 스팸의 비율은 변화가 없었습니다. 그 후 몇 주 동안 스팸의 평균 바이트 크기는 6월 초까지 계속 증가하여 거의 10KB에 육박했습니다.
- 금융 기관은 2010년 상반기에도 계속 가장 많은 공격의 표적이 되었지만, 모든 피싱 이메일 표적 중에서 차지하는 비중은 이제 49%에 불과합니다.
- 2010년 상반기에는 전체 금융 피싱 표적 중 3분의 2 이상이 북아메리카에 있었습니다. 나머지 32%는 유럽 소재 기관이었습니다.
- 브라질은 여전히 가장 많은 양의 피싱 메일이 발송되는 국가로 남아 있으며, 인도가 2위 그리고 한국이 3위를 기록하고 있습니다.

2010년 이후의 주요 토픽

- 가상화 – 기업은 자사의 비즈니스 부서와 고객에게 더 많은 기능을 제공해야 한다는 압력을 점점 많이 받고 있습니다. 이런 변화의 중심에는 가상화가 있습니다. 그러나, 가상화의 궁극적인 성공은 에너지 효율과 성능과 사용 편리성뿐만 아니라 이런 혜택을 IT 인프라의 전체적인 보안과 안정성과 가용성을 저해하지 않으면서 제공할 수 있는 능력에 의해 결정되기도 합니다.
- IPv6 보급 – 무엇이 이 새로운 네트워크의 채택 속도를 높이고 있을까요?
- 클라우드 컴퓨팅은 현재 기존의 신흥 기술에서 볼 수 있는 것과 동일한 취약점을 안고 있으면서 일상적인 원격 관리 활동의 어려움이라는 추가적인 문제를 제시하는 신흥 기술입니다. 클라우드 컴퓨팅은 비교적 초기 단계에 있으며, 설계와 활용에 기초한 구현과 범위와 관련하여 다면적인 성격을 갖고 있습니다.

IBM Security 협업

IBM Security는 광범위한 보안 역량을 제공하는 여러 브랜드를 대표합니다. X-Force® 연구개발(R&D)팀이 최근 동향과 공격자가 사용하는 방법을 부지런히 분석하는 동안, 다른 여러 IBM 그룹은 이를 통해 얻어진 풍부한 데이터를 당사 고객을 보호하기 위한 기법에 적용하기 위해 노력합니다.

- IBM X-Force 연구개발팀은 광범위한 컴퓨터 보안 위협 및 취약점을 발견하고 분석하고 모니터링하고 기록합니다.
- IBM Managed Security Services(MSS)는 말단컴퓨터(Endpoint), 서버(웹 서버 포함) 및 전반적인 네트워크 인프라와 관련된 공격을 모니터링하는 책임을 집니다. MSS는 웹을 물론 이메일 및 인스턴트 메시징(IM) 등의 다른 경로를 통해 감행되는 공격도 추적합니다.
- Professional Security Services(PSS)는 전사에 걸친 종합 보안 평가와 설계 및 배포 서비스를 제공하여 효과적인 정보 보안 솔루션을 구축하는 데 기여합니다.
- "Whiro" 크롤러는 MSS와 컨텐츠 보안 팀과 독립 분석으로부터 얻어진 경보 데이터를 결합하여 웹 기반 소스에서 감행되는 공격을 모니터링합니다. Whiro는 특수 기술을 사용하여 툴킷이 다중 공격을 시도하는 등 가장 난독화가 심한 경우에도 취약점을 악용하는 공격을 적발해냅니다.
- 컨텐츠 보안 팀은 크롤링과 독립 인식(Discovery) 그리고 MSS 및 Whiro에서 제공하는 피드를 통해 독립적으로 웹을 조사하고 분류합니다.
- IBM은 IBM Rational AppScan onDemand Premium 서비스가 지난 3년 동안 실시한 보안 테스트에서 얻은 실제 취약점 데이터를 정리했습니다. 이 서비스는 IBM Rational AppScan에서 얻은 애플리케이션 보안 평가 결과를 수작업에 의한 보안 테스트 및 검증과 결합합니다.
- IBM Cloud Security Services를 통해, 고객은 비용을 절감하고 서비스 전달을 개선하고 보안을 강화하는 데 도움이 되는 호스트형 가입 모델을 통해 보안 소프트웨어 기능을 소비할 수 있습니다.
- ID 및 액세스 관리 솔루션은 철저한 ID 관리, 액세스 관리 및 사용자 규제준수 감사 기능을 제공합니다. 이 솔루션은 사용자, 인증, 액세스, 감사 정책의 관리와 사용자 서비스의 프로비저닝을 중앙으로 집중시키고 자동화합니다.

2010년에 알아야 하는 주요 동향

기업을 대상으로 하는 은밀한 위협

2010년 상반기 컴퓨터 보안 실무의 가장 두드러진 특징은 거의 모든 대화에 APT(Advanced Persistent Threat)라는 새로운 용어가 등장했다는 것이었습니다. 네트워크에 가해지는 위협의 성격에 대한 대화의 주체가 심심해서 인터넷으로 시간을 보내던 청소년 컴퓨터 해커 집단에서 이익 추구를 목표로 하는 전문적인 컴퓨터 범죄 집단으로 옮겨간 것은 최근의 일입니다. 이제는 더욱 더 음흉한 위협 즉, 정부가 후원하는 충분한 자금력을 갖춘 첩보 조직이 다가올 것으로 보입니다. APT(Advanced Persistent Threat)는 새로운 것이 아닙니다. 이런 종류의 공격은 수 년 동안 감행되어 왔습니다. 달라진 점은 매우 다양한 종류의 단체가 이 위협에 대해 이야기하면서 자체적인 네트워크에서 위협에 대처하고 있다는 사실입니다.

X-Force가 정교해진 공격 수단을 사용하는 공격자들에 대해 가장 우려하는 점은 네트워크 보안 기술과 방법의 상당한 발전에도 불구하고 방어 수준이 높은 네트워크를 성공적으로 침투할 수 있는 그들의 능력입니다. 최신 보안 시스템의 감시망을 피하는 점점 난독화되는 공격과 숨은 악성코드 명령 및 제어 채널은 특히 우려됩니다. 이런 위협에 대처하기 위해서는 새로운 프로세스를 개발하고 궁극적으로 완벽하게 새로운 네트워크 보안 기술을 채택해야 합니다.

APT (Advanced Persistent Threat)

APT(Advanced Persistent Threat)라는 용어는 미국 정부에서 처음 사용되기 시작했습니다. 이 말은 보다 직접적인 금전적 동기를 갖고 숨겨 놓은 신용카드 번호를 공략하는 등의 방법으로 공격하는 집단이 아닌 첩보 활동을 위해 컴퓨터 네트워크를 공격하는 여러 국가 정부의 다양한 집단을 가리킵니다.

'Persistent'(영속적인)라는 단어는 네트워크 운영자가 APT 집단의 존재를 인식하고 있고 그에 대처하기 위한 적극적인 조치를 취할 때에도 APT 집단이 컴퓨터 네트워크를 계속 액세스하고 제어할 수 있는 능력을 갖고 있음을 나타내기 위해 사용되었습니다. APT 집단은 끈기가 있습니다. 이들은 원하는 정보에 접근할 수 있는 권한을 서서히 확대하면서 주의를 끌지 않을 정도로 움직임을 적게 유지합니다.

APT 사건에서 목격되는 공격 기법의 복잡한 정도는 특정한 네트워크를 방어하는 사람들의 능력 수준과 정비례하는 경우가 많습니다. APT 집단은 여러 가지 도구와 기능을 갖고 있으면서 그 중에서 특정 임무를 완수하는 데 필요한 가장 단순한 기능을 선택하는 것으로 보입니다.

네트워크 방어자가 침입을 감지하고 그에 대응하면 더 정교한 도구와 기법이 등장합니다. 특정 대상을 공략하는 모든 정교해진 공격의 공통점은 공격자가 정찰부터 한다는 것입니다. 여기에는 컴퓨터 침입에 관해 연상되는 기존의 네트워크 프로빙 및 스캔 활동이 포함될 수 있지만, 정교해진 공격자들은 기존 사고의 틀을 깹니다.

현재 인터넷에는 비즈니스 세계에서 일하는 많은 사람들에 대한 풍부한 정보가 있습니다. 사람들은 사적이고 공적인 소셜 네트워킹 사이트에 자신의 프로필을 게시하고, 어디를 여행하고 있는지를 알리는 상태 업데이트를 발송하고, 직업과 관련된 온라인 포럼에 참여하고, 공개 회의에서 발표를 하고, 기사와 논문을 작성하고, 언론과 인터뷰를 합니다. 이 모든 것을 할 때, 사람들은 악의를 가진 자가 특정인의 개인 생활을 재구성할 뿐만 아니라 그가 속한 조직과 그의 직위까지도 재구성하기 위해 사용할 수 있는 수많은 단서를 흘리게 됩니다.

정교해진 공격자들

정교해진 공격자는 이런 공개 정보를 사용하여 자신이 표적으로 삼는 단체에 대한 완전한 그림을 완성합니다. 즉, 누가 거기서 일하고, 그들이 무엇을 하고, 그들이 조직 안에서 누구 밑에서 일하는 지를 파악합니다. 이렇게 완성한 그림을 사용하여, 공격자는 자신이 원하는 정보를 액세스할 수 있는 개인이 누구인지 알아냅니다. 이런 개인은 악성 공격코드를 실행하도록 속이기 위한 다양한 소셜 엔지니어링 공격을 받게 됩니다. 공격자의 첫 번째 목표는 피해자의 워크스테이션에 대한 통제력을 장악하는 것입니다. 그렇게 되면 피해자의 모든 작업물과 커뮤니케이션 자료는 고스란히 노출되게 됩니다.

이런 공격에는 종종 난독화 공격을 통해 제로데이 취약점을 공략하는 변형 문서나 웹페이지가 사용됩니다. 공격은 비즈니스 파트너나 동료가 보낸 이메일의 형태로 이루어질 수 있으나, 여기에는 피해자의 직무와 직접 관련이 있는 것처럼 보이는 악성 파일이 첨부되어 있습니다. 공격 수단은 경쟁사의 웹사이트에 있는 유용한 문서로 연결되는 링크나, 산업 박람회에서 피해자에게 건네진 흥미로운 프레젠테이션이 담긴 USB 토큰이 될 수도 있습니다.

공격에 의해 설치된 맞춤 악성코드는 숨겨진 채널을 사용하여 적발되지 않고 네트워크를 통해 교신합니다. 공격자는 일단 피해자의 컴퓨터에서 악성코드를 실행시키는 데 성공하면 종종 표적 네트워크에 속한 다른 시스템으로까지 통제권을 확대하려고 시도합니다. 또한, 공격자는 비즈니스 관계를 악용하여 한 회사의 네트워크를 통제할 수 있는 능력을 바탕으로 다른 회사의 네트워크에도 침입하려고 시도합니다.

민간 부문의 네트워크 보안 종사자들에게, 첩보 관련 APT 활동과 금전적 이익을 위한 공격을 구분하는 선은 모호합니다. 발전소는 정부의 후원을 받는 사이버 전사들과 단순히 공갈협박에 관심이 있는 범죄 집단에게 모두 공격을 당해 왔습니다. 정부의 전략가들을 공략하기 위해 사용되어 왔던 것과 똑 같은 정교해진 스피어 피싱 공격은 자금 이체 시스템에 대한 접근 권한을 갖고 있는 금융 기관의 임원들에게도 사용되어 왔습니다.

이로 인해 당사가 하는 일이 더 쉬워지는 측면도 있습니다. 이런 공격과 싸우기 위해 당사가 개발하는 기법은 매우 다양한 상황에 응용될 수 있기 때문입니다. 그러나, APT라는 용어가 기업이 직면하는 모든 광범위한 정교한 집중 공격을 포함하지 않는다는 사실을 인식하는 것이 중요합니다. APT에 대한 최근의 많은 논의는 이런 공격 기법에 대한 의식을 높이는 데 도움이 되었지만, 이로 인해 첩보 관련 활동에만 너무 협소하게 초점을 맞춘 반응이 증가해서는 안 될 것입니다. 공격자의 동기가 무엇이든, 이런 유형의 공격으로부터 네트워크를 보호하는 방법을 찾는 것은 네트워크 보안 실무자의 책임입니다.

금전적인 이익을 위한 공격

2008년 연간 X-Force 동향 및 리스크 보고서에서, 당사는 취약점의 분류를 금전적인 이익을 취하고자 하는 공격자의 관점에서 생각해보기 위한 간단한 모델을 소개하고 이 모델에서 공격 노력 대비 잠재적 보상 매트릭스(전 공격 가능성 매트릭스)을 도출했습니다. 이 매트릭스(표)는 여러 가지 보안 취약점을 그것이 컴퓨터 범죄자에게 제시하는 기회와 함께 해당 취약점을 공격하는 데 수반되는 노력이라는 관점에서 표시합니다.

본 보고서의 21 페이지에 업데이트되어 있는 이 표는 인터넷에서 폭넓게 악용되며 공격하기가 쉽고 악당에게 큰 기회를 제시하는 취약점이 '최적 지점(Sweet Spot)'에 몰려있는 경향이 있다는 사실을 설명하는 데 도움이 됩니다. 이런 유형의 취약점은 종종 많은 수의 말단 컴퓨터 시스템을 대량으로 공격하는 조직적인 범죄 집단에게 선호되는 경우가 많습니다.

그러나, X-Force가 그에 관한 경보 및 공지를 발표하는 일부 취약점은 공격하는 데 비교적 많은 비용이 듭니다. 맞춤 공격 도구를 개발할 능력을 가진 정교해진 공격자는 비용에 관계 없이 이런 취약점을 이용할 수 있습니다. 또한, 취약점은 시간이 지남에 따라 공격 비용이 점점 줄어드는 경향이 있기도 합니다. 많은 경우에 취약점은 정교해진 공격자들에 의해 먼저 발견되어 특정한 표적을 공격할 때 사용됩니다. 결국에 공격 활동은 보안 전문가에게 적발되고 취약점은 일반에 노출되고 패치됩니다. 궁극적으로 공격 코드까지 포함한 취약점에 대한 더 많은 정보가 공개적으로 알려지면, 해당 취약점과 관련된 공격 활동의 패턴은 표적 공격에서 전면 공격으로 바뀝니다.

이에 관해, 취약점과 정교한 팀이 표적 공격에 사용하기 위해 개발한 난독화 기법은 결국 조직적인 범죄 집단이 사용하는 대량 공격 툴킷으로 흘러 들어간다는 면에서 특정한 표적을 대상으로 한 APT형 공격과 광범위한 봇넷 활동 사이에는 직접적인 관계가 있습니다. 그 결과, 모든 먹이사슬 단계의 공격자는 시간이 흐를수록 더 수준이 높아지고 있습니다. 이런 진화에서 특히 문제가 되는 것은 모든 단계의 공격자가 시중에서 판매되는 다양한 상용 네트워크 보안 솔루션이 제공하는 보호 기능을 우회하고 네트워크 관리자의 눈에 띄지 않게 활동할 수 있는 능력이 향상된다는 것입니다. 이로 인해, 보안 산업은 단지 연구소에서뿐만이 아니라 실사용 환경에서도 위협을 더 효과적으로 감지해야 한다는 점점 큰 압력을 받게 됩니다.

JavaScript 난독화 – 인기 있는 우회 기법

이런 우회 기법 유형의 가장 중요한 예는 JavaScript 난독화입니다. JavaScript는 유연한 언어입니다. 이를 사용하면 데이터를 코드처럼 실행하고 데이터를 조작할 수 있습니다. JavaScript는 암호화할 수도 있습니다. 실제 공격 시에 공격 탄두(Payload)는 종종 JavaScript를 통해 투하되며, 이런 공격 탄두는 JavaScript에서 인코딩이 많이 된 데이터가 집중된 부분에 숨겨집니다. 이 부분을 네트워크에서 검사하려면 너무 많은 비용이 들지만, 말단컴퓨터에 도달하면 브라우저와 문서 뷰어에 의해 해독됩니다. 네트워크 보안 제품이 간단히 모든 난독화된 JavaScript 스크립트를 차단할 수 있다면 일은 훨씬 쉬워질 테지만, 안타깝게도 난독화 기법은 여러 합법적인 웹사이트가 능력 수준이 낮은 웹 개발자에게 코드를 도난 당하기 않기 위해 사용하기도 합니다. 악성 웹사이트들은 이런 합법적인 웹사이트 뒤에 숨기 때문에 공격을 찾아내기가 매우 어려워집니다.

APT를 단 번에 막을 수 있는 비밀 병기는 없습니다. 시중에서 판매되는 보안 솔루션은 도움이 되는 몇 가지 도구를 제공할 수 있지만, 이 문제를 마술처럼 한꺼번에 해결하는 제품은 없습니다. 많은 단체는 물리적 네트워크 분할의 더 폭넓은 사용과 유니버설 이메일 서명 그리고 애플리케이션 화이트-리스팅(허가 목록) 같은 새로운 프로세스 및 기술을 조사하고 있습니다. 이런 방법은 모두 방어 수준을 높여주지만, 넘지 못할 수준은 아닙니다. 난독화 같은 근본적인 문제는 새로운 기술적 해결책을 요구합니다. 보안 산업은 이 분야에서 혁신을 추진하여 네트워크 관리자가 대응할 수 있는 무기를 갖출 수 있도록 도와야 하는 책임이 있습니다.

APT와 싸우기

경험적으로, 이런 종류의 네트워크 위협에 대처하기 위해 할 수 있는 가장 효과적인 것 중 하나는 임직원의 적극적인 참여를 유도하는 것입니다. 당사는 정교해진 스피어 피싱 공격을 경계하도록 사용자를 훈련시키는 것이 불가능하다는 고정 관념이 옳지 않다고 생각합니다. 실제로 효과를 거둔 사례를 직접 목격했기 때문입니다. 소속 단체에서 이런 공격 유형에 가장 취약한 임직원을 가려내고 그들에게 위협의 성격과 그 원리를 설명할 수 있다면, 그들은 조직의 일차방어선이 될 것입니다. 그들은 수상한 이메일을 신고할 수 있습니다. 이를 통해 공격자가 사용하는 공격 수단의 표본을 갖게 되면, 문제를 해결할 발판이 마련됩니다. 이렇게 되면 표적이 되고 있는 다른 피해자들을 파악하고, 악성코드 명령 및 제어 패턴을 확인하여 문제 해결을 시작할 수 있습니다.

PDF 공격 인기 최고!

X-Force는 2009년 상반기에 PDF 기반 취약점이 광범위하게 공격되는 현상을 목격하기 시작했습니다. 당사 자료에 따르면, 그 후에 이 공격은 실운영 환경에서 가장 많이 감행되는 브라우저 공격 5개 중 3개를 차지할 정도로 증가했습니다. 말단컴퓨터(Endpoint)가 기업 조직에서 일반적으로 가장 취약한 연결 고리라는 사실을 공격자가 잘 알고 있다는 점을 생각하면, PDF가 공격의 대상이 되는 이유를 쉽게 이해할 수 있습니다. 예를 들면 특정한 말단컴퓨터에는 민감한 데이터가 없을 수 있지만, 해당 컴퓨터는 민감한 데이터가 있는 다른 말단컴퓨터를 액세스할 권한을 갖고 있을 수 있습니다. 아니면, 해당 말단컴퓨터는 다른 컴퓨터를 공격하기 위한 유용한 발사 지점(Bounce Point)으로 사용될 수도 있습니다. 이것으로 PDF가 그토록 자주 공격 사용되는 이유가 완전히 설명되지는 않습니다. 특히 Internet Explorer와 ActiveX 기반 공격이 수 년 동안 널리 행해져 왔다는 것을 생각하면 더욱 그렇습니다.

당사는 이에 관해 몇 가지 유용한 의견을 제시할 수 있습니다. 먼저, 시장 점유율이 계속 변하는 브라우저를 공격하기 위해 구체적인 투자를 감행하는 것은 PDF나 Flash 등의 Adobe 플러그인 같이 거의 모든 브라우저에 공통적으로 사용되는 소프트웨어보다 더 어렵습니다. 둘째, 특정한 브라우저를 대상으로 하는 공격에 악용되는 취약점이 복잡하다면 해당 취약점은 특정한 표적을 대상으로 한 공격에만 제한적으로 이용될 수 있습니다. 다시 말해, 확실하게 악용할 수 있는 IE 또는 Firefox(또는 기타 브라우저) 버그를 찾는 데 시간을 투자한 자는 취약점에 대한 상세 정보와 "무기화된" 개념 증명(POC)을 찾기가 더 쉬운 다른 취약점과 동일한 가격으로 판매하려 하지 않을 것입니다.

그렇다면 PDF 취약점은 찾기가 더 쉬울까요? ActiveX 버그와 비교할 때 그렇다는 증거는 없습니다. 하지만 Microsoft는 "킬 비트(Kill Bits)"를 통해 제 3의 벤더에서 제공되는 것을 포함한 취약한 ActiveX 인터페이스를 매우 부지런하게 블랙리스트에 올려왔습니다. 올해 IE에서 노출된 "Dangling Pointer" 버그의 복잡함을 고려하면, PDF 취약점은 상대적으로 더 적은 노력을 필요로 해 왔다고 할 수 있습니다.

PDF 공격이 특정한 브라우저를 대상으로 한 공격보다 더 유리한 또 한 가지 이유는 PDF 문서의 규격이 복잡하기 때문에 공격자가 PDF 문서의 다른 부분에 데이터를 쉽게 숨긴 후 나중에 해당 데이터를 프로그램을 통해 회수하고 디코딩 알고리즘을 적용하여 악성 스크립트를 반환할 수 있다는 데 있습니다. 이 난독화 방법은 공격 툴킷이 사용하는 일반적인 JavaScript 인코딩 루틴을 1:1로 변환한 것과 유사한 이전의 기법에서 벗어난 것입니다. 시간의 흐름에 따른 난독화의 진화에 대해서는 웹 브라우저 공격 동향 부분에 설명되어 있습니다. PDF 안의 다른 객체에 삽입한 데이터를 회수하는 행동은 때때로 의심을 받을 수 있지만, 첨단 PDF 공격 방지 기술은 감지를 위해 부산물(Artifact)에 너무 많이 의존해서는 안 될 것입니다. 오경보를 유발할 수 있기 때문입니다.

제로데이(Zero-day) PDF 공격은 패치가 제공되기 전까지 유예 기간을 누리므로, 공격자의 관점에서 PDF 공격의 가치를 높여줍니다. Adobe는 최근에 공격에 대처하기 위한 더 공격적이고 적극적인 역할을 담당하고 있으며, X-Force는 이런 추세가 계속된다고 보고 있습니다. 또한, 차기 주요 Acrobat Reader 버전에는 잔여 버그의 공격 가능성을 줄이기 위한 샌드박스 기술이 포함될 것이라는 소식이 있습니다. 이런 조치가 PDF 기반 공격에 실제로 어떤 영향을 미칠 지는 두고 봐야 할 것입니다. 이는 샌드박스 기술이 다른 브라우저 플러그인과 유비쿼터스 문서 및 멀티미디어 형식과 비교하여 비용/이익 비에 어떤 영향을 미치는지에 의해 결정될 것으로 생각됩니다. 타사의 PDF 뷰어도 버그로부터 자유롭지 않으며, 비록 공격자들의 공략 대상이 되는 경우가 드물기는 하지만 구현의 차이로 인해 엄청난 보안 위험이 초래될 수 있습니다. 예를 들면, 많이 논의되고 있는 PDF "런치(Launch)" 기능은 대체 제품인 Foxit 리더에서 어떤 프롬프트 창도 유발하지 않았습니다. 물론 Adobe의 구현 방식은 여전히 프롬프트 필드를 속일(Spoof) 수 있습니다. 그러나, Foxit은 Adobe와 마찬가지로 자사 제품에 "안전 모드" 같은 보안 강화 기능을 추가하고 있습니다.

PDF 기반 공격으로부터의 보호

사용자가 PDF 공격으로부터 스스로를 보호하기 위해 할 수 있는 일에는 몇 가지가 있습니다. Acrobat Reader에서는 ActionScript(Adobe의 JavaScript 확장 버전)를 비활성화하는 것이 가능합니다. 일부 PDF 기반 공격은 이런 방법으로 차단하지 못할 수 있지만, 그럼에도 불구하고 이 기능을 비활성화하는 것은 가치가 있을 수 있습니다. 여기서 언급한 Acrobat Reader 외에도 여러 가지 PDF 리더가 있지만, 대부분의 옵션이나 응용프로그램 환경설정에는 유사한 설정이 있을 것입니다. 또한, PDF 문서에는 비디오나 Flash 동영상 등의 다른 멀티미디어 형식을 심을 수 있다는 점을 생각하면 흥미롭습니다. Acrobat 환경설정에는 이 기능을 비활성화하는 옵션이 있습니다. X-Force는 대부분의 기업이 이 기능을 필요로 한다고 생각하지 않습니다. 대부분의 경우 일반 사용자도 그럴 것입니다.

2010년 하반기와 2011년에도 PDF가 공격자들 사이에 인기를 잃게 될 것이라 생각하기는 어렵습니다. 이는 PDF 취약점 노출의 수에 관계 없이 그럴 것이라 예상됩니다. 배포된 지 몇 년이 지난 후 2006년에야 패치가 적용된 한 ActiveX 문제는 여전히 웹 브라우저 공격자들에게 자주 사용되고 있습니다. Acrobat 샌드박스 기술이 알려지고 알려지지 않은 공격에 어떤 영향을 미칠 것인지는 아직 추측할 수 없는 중요한 문제입니다.

PDF를 악용한 공격 동향

앞에서도 말했듯이 PDF 공격은 인기가 높습니다. IBM Managed Security Services(MSS)의 데이터도 이 사실을 뒷받침합니다. 이 공격 기법은 위협 환경을 계속 장악하고 있습니다. PDF 공격과 관련된 이벤트 활동은 올해 4월에 가장 크게 증가했습니다(그림 1). 이 달에 이벤트 활동은 2010년 상반기 평균보다 거의 37%나 더 많았습니다.

이처럼 이벤트가 급증한 이유는 이 달에 유포된 악성 스팸 이메일이 크게 증가했기 때문입니다. 피해자들은 /Launch 명령을 악용하는 특별히 제작된 Adobe Acrobat (PDF) 파일이 포함된 이메일을 수신했습니다.

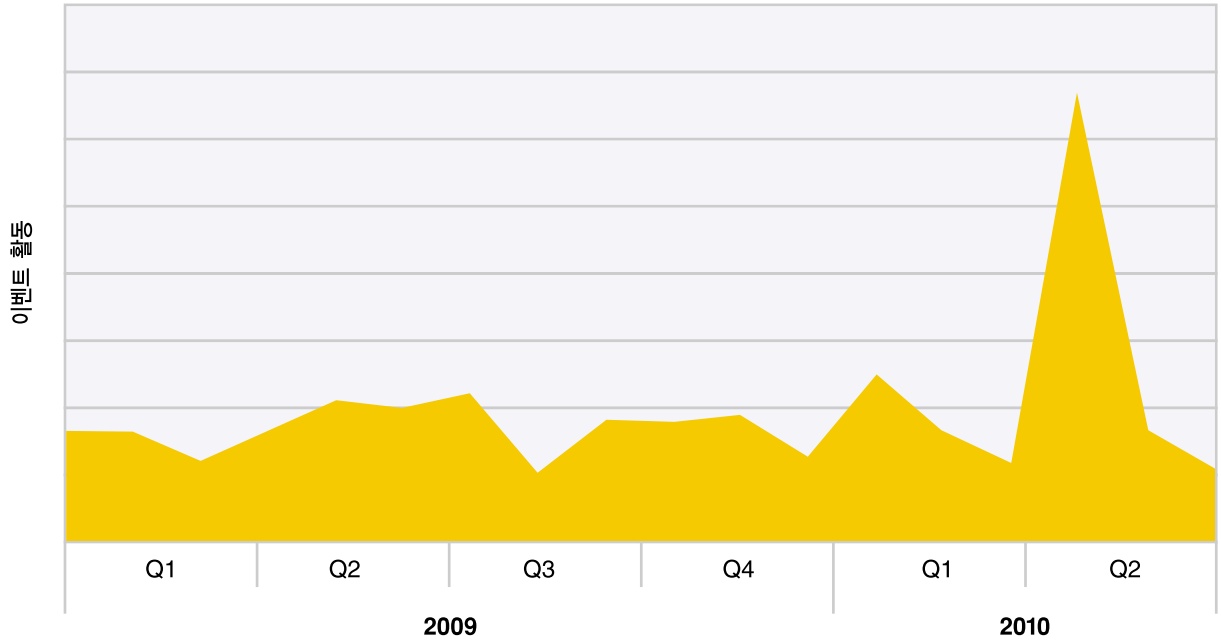


그림 1: PDF를 악용한 공격 동향, IBM Managed Security Services, 2009년 1분기~2010년 2분기

IBM Managed Security Services(MSS)는 클라이언트 취약점을 이용하는 공격 유형 중 가장 자주 목격되는 공격 유형을 보여주는 뷰를 제공합니다. MSS는 실시간 보안 관리를 위한 시스템 모니터링, 비상 대응 및 항시(24x7x365) 보호를 포함한 광범위한 아웃소싱 솔루션을 판매합니다.

이 서비스는 다양한 네트워크, 서버, 말단컴퓨터(Endpoint) 및 무선 애플리케이션 플랫폼 및 운영체제를 다루며, 이벤트 모니터링을 제공합니다. MSS는 인터넷 전역에 걸친 전체적인 공격 활동을 균형 있게 보여줍니다. 본 보고서에서는 MSS 데이터의 일부를 사용하여 공격 동향을 파악했습니다.

Cutwail이라고도 알려진 Pushdo와 Zeus 봇넷은 이 PDF 악성코드를 확산시키는 데 한 몫 했습니다. 실행가능 프로그램을 시작(Launch) 시키는 임베디드된 행동(Action)을 포함하고 있는 PDF 파일이 네트워크를 통해 전송되었음을 암시하는 이벤트는 2010년 4월에 증가했습니다. 이 달에는 Pushdo Trojan이 보이는 패턴을 포함하는 HTTP 메시지의 적발 건수도 크게 증가했습니다.

그리고 Pushdo와 관련하여 IBM X-Force와 MSS는 올해 초에 이 봇넷이 특정한 SSL 활성화 웹사이트를 대상으로 DDoS(Distributed Denial of Service) 공격을 개시하는 모습을 목격하기도 했습니다. 그 후로 SSL 서버를 상대로 DoS 공격을 감행할 수 있는 특별 제작된 메시지가 감지되는 경우가 눈에 띄게 증가했습니다. 이런 움직임의 대부분은 이미 2007년경부터 존재해 온 Pushdo에 원인이 있는 것으로 의심됩니다.

Zeus 봇넷에 대한 사실과 오해에 대해서는 본 보고서에서 나중에 자세히 다룰 것입니다.

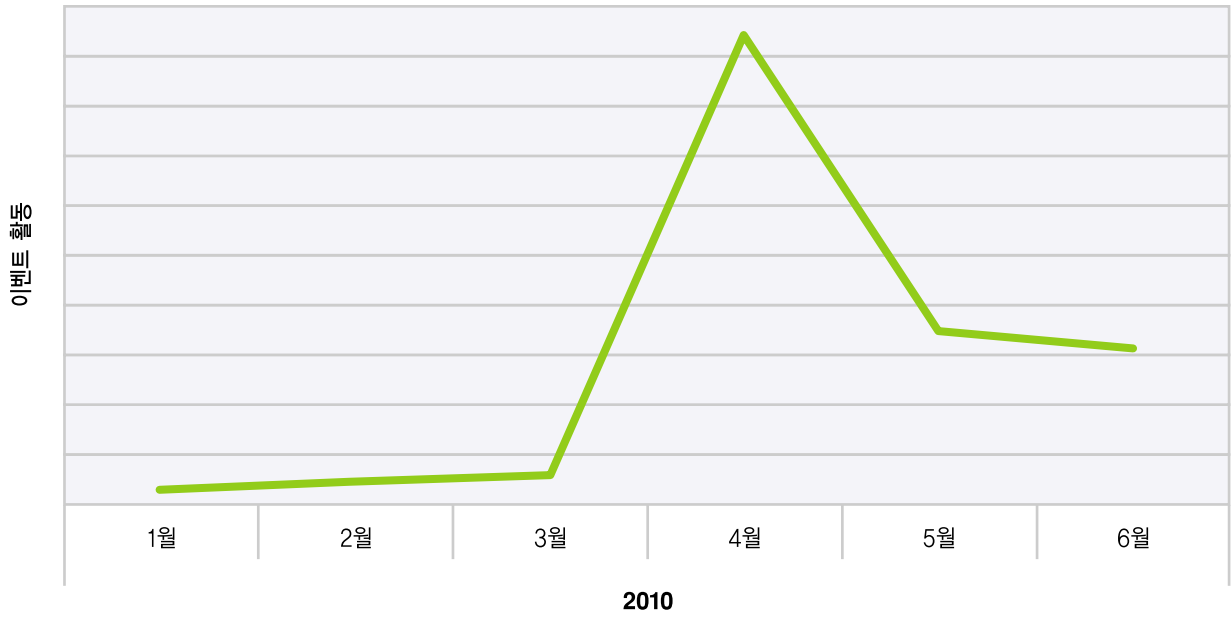


그림 2: Pushdo/Zeus 봇넷 활동, IBM Managed Security Services, 2010년 상반기

악성 코드 난독화 동향

2010년 상반기에는 2009년에 이어 악성 코드 난독화가 많이 목격되었습니다. 2009년에 대부분의 JavaScript 난독화는 스크립트 자체에서 악성 스크립트 디코딩 키를 획득하기 위한 것이었기 때문에, 분석을 위해 조금이라도 수정을 가하면 스크립트는 이해가 불가능하게 되었습니다. JavaScript 난독화와 관련해서는 몇 가지 흥미로운 속임수가 목격되었습니다. 그 중 한가지는 객체 안에 기능 포인터를 놓고 이를 다른 방법으로 회수함으로써 다른 객체 스코핑이 포함된 분석 도구를 무력화하는 것을 수반합니다. 또 다른 흥미로운 속임수는 추가 코드를 실행하기 전에 객체나 이미지의 상태를 확인하는 작은 스크립트 코드와 관련이 있습니다.

나중에 더 자세히 설명할 **공격 툴킷 패키지**는 계속 악성 Adobe Flash 및 PDF와 Java 파일을 선호합니다. 난독화는 이런 형식을 위해 특별히 개발됩니다. 역사적으로 보면, 난독화 코드는 이전의 JavaScript 기반 구현에서 빌려온 것입니다. 2010년에는 분석을 방해하기 위해 관련 형식에 한정된 기능을 사용하는 경우가 점점 흔해지고 있습니다. 예를 들면, PDF 문서의 경우에는 텍스트를 포함하고 있고 나중에 ActionScript(기본적으로 JavaScript와 같음)를 통해 프로그램을 사용하여 액세스할 수 있는 객체가 많습니다. 공격자는 일반적으로 악성 스크립트를 다른 객체에 일반 텍스트의 형태로 포함시키지 않으므로, 이 난독화 방법을 사용할 때는 거의 항상 어쩌면 오래된 툴킷에서 볼 수 있는 디코딩 알고리즘과 함께 사용합니다.

Visual Basic Script(VBS)를 난독화 방법으로 사용하는 경우는 계속 줄어들고 있습니다. 당사 자료에 따르면 2009년 보급률은 3.6%였습니다. 2010년 상반기에 이 비율은 2%로 감소했습니다. VBS는 Internet Explorer에서만 지원하는 독점 언어이므로 주로 오픈 소스 VBS 프로세싱 객체의 결여로 인해 과거부터 확실한 난독화 방법이었기 때문에 당사는 VBS의 사용에 대해 지난 몇 년 동안 계속 논의해 왔습니다. 그러나, VBS 사용이 계속 감소할 분명한 이유가 없음에도 불구하고 이런 추세는 영구적인 것이 될 수 있습니다.

2009년 하반기에는 코드 코멘트를 사용하여 탐지 휴리스틱을 망쳐놓고 기초 코드를 시각적으로 가리는 잠재적인 새로운 추세가 관찰되었습니다. 이 기법이 사용될 때에는 코멘트 문자열이 기능 호출 매개변수 안에 보이는 경우가 많습니다. 2010년 상반기에 이 기법은 정기적으로 등장하지 않았습니다. X-Force는 이 난독화 방법이 주기적인 유행을 탈 것으로 예상합니다.

난독화란 무엇인가?

"난독화(Obfuscate)"라는 단어의 사전적 의미는 가리거나 불분명하게 만드는 것입니다. 말하자면, 물을 탁하게 만드는 것입니다.

프로그래밍 언어에서 소프트웨어 업체와 공격자는 모두 자신의 작업 결과를 숨기려고 합니다. 소프트웨어 업체는 왜 코드를 숨기거나 난독화할까요? 지적 자본을 보호하거나 프로그램 논리를 역엔지니어링으로부터 보호하거나 조작을 방지하기 위해서입니다.

높은 관점에서 보면, 이는 개인 메시지를 타인이 보지 못하도록 하기 위해 비밀 코드를 사용하는 방법과 유사합니다.

공격자가 이처럼 잘 알려진 고전적인 방식을 사용하여 자신이 하는 행동을 성공적으로 숨길 수 있는 까닭은 모든 가능한 인코딩/디코딩 조합을 해석할 수 없음으로 인해 공격을 감지하지 못하는 보안 제품이 많기 때문입니다. 이로 인해, 탐지할 수 있도록 하기 위해서는 끊임없이 재검토해야 하는 새로운 공격 방법이 생겨날 수 있습니다.

난독화 공격 활동

2009년에 관찰된 많은 양의 난독화는 2010년 상반기에도 계속되었습니다. 올해 4월까지 난독화된 공격 활동은 비교적 일정하게 유지됐지만, 2010년에 6월에는 크게 증가했습니다. 이 한 달 동안 이벤트의 양은 2010년 상반기 평균의 1.4배에 달했습니다.

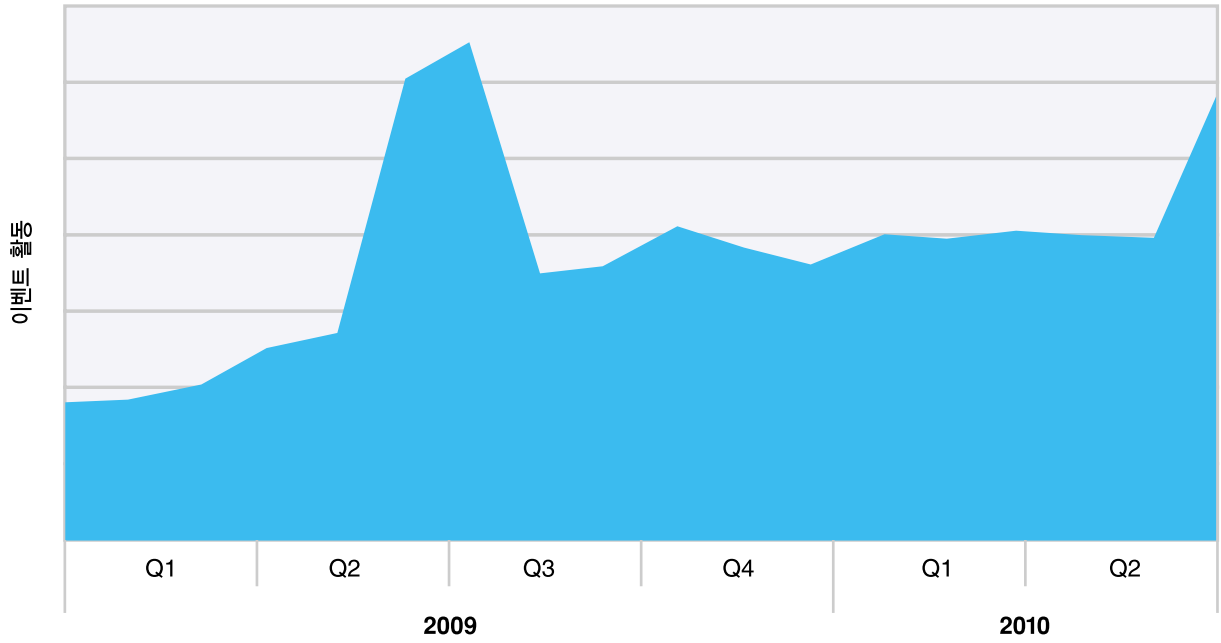


그림 3: 난독화된 웹 페이지 및 파일, IBM Managed Security Services, 2009년 1분기~2010년 2분기

변화무쌍한 위협 환경

취약점 노출 – 2009년보다 훨씬 많은 2010년 상반기 보고 건수

2010년 상반기에 노출된 취약점의 수

X-Force는 2010년 상반기에 4,396개의 새로운 취약점을 분석하고 기록했습니다. 이는 2009년 상반기보다 36% 증가한 수치이자 한 해 상반기에 집계된 새로운 취약점 기록을 갱신한 것이었습니다.

2007년에는 취약점의 수가 처음으로 감소했지만, 2008년에는 다시 역대 최고 기록을 경신했습니다. 2009년에는 취약점 노출률이 감소하여 정점을 찍은 것으로 보였지만, 올해 상반기의 극적인 증가세는 그런 생각이 잘못되었음을 보여주었습니다. 이제는 노출된 취약점의 수가 지속적으로 증가하는 추세가 2009년에 잠시 멈칫했었을 뿐인 것으로 보입니다. 올해 상반기의 추세가 계속된다면, 2010년에는 사상 최고치를 경신하게 될 것입니다.

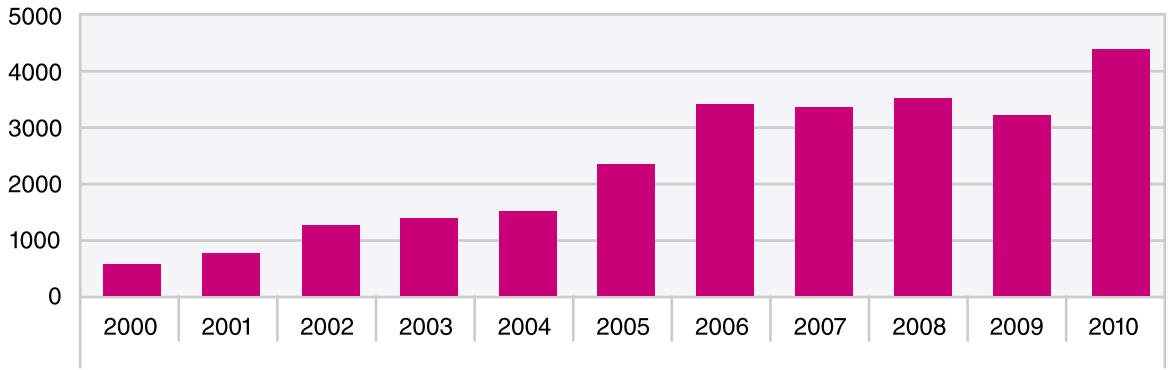


그림 4: 매년 상반기에 노출된 취약점, 2000년～2010년

이처럼 노출된 취약점의 수가 크게 증가한 것은 무엇을 의미할까요? 한 가지 확실한 것은 모든 벤더와 기타 정보 출처에서 과거 어느 때보다도 더 많은 취약점을 보고되고 있다는 사실입니다. 예를 들면, 2009년에 milw0rm이 공개한 악용 가능한 취약점(Exploit)은 2000개가 넘었습니다. milw0rm은 그 해 말에 Offensive Security Exploit Database에 자리를 내주고 문을 닫았습니다. 2010년에 Offensive Security는 지금까지 2000개가 넘는 악용 가능한 취약점을 공개했습니다. 이 추세대로라면, 2010년에는 이 정보 출처 혼자서 과거보다 60% 더 많은 취약점을 발표할 것으로 예상됩니다.

매년 노출되는 취약점의 수는 이제 연간 6,000 ～ 8,000천 건 사이에서 줄거나 늘어나는 것으로 보입니다.

취약점 분류에 관한 어떤 모호함도 없도록 하기 위해, 본 보고서에서는 다음과 같은 IBM Security Services의 정의를 사용했습니다.

취약점이란 정보 시스템의 기밀성, 무결성 또는 가용성이 눈에 보이거나 보이지 않게 훼손되는 결과를 실제로 초래하거나 초래할 가능성이 있는 일련의 상태라 정의됩니다.

패치율

2010년 상반기에 노출된 모든 취약점 중 해당 업체가 조사 기간이 끝날 때까지 그에 대한 패치를 공급하지 않은 취약점은 절반이 넘었습니다(55%). 이는 2009년 전체의 52%보다 약간 높아진 수치입니다.

취약점에 대한 수정 및 패치의 제공 여부

노출된 취약점이 가장 많았던 10대 업체는 노출된 취약점에 대해 패치를 제공하지 않은 비율이 3%에서 24% 사이에 불과하여 업계 평균인 55%보다 훨씬 양호했습니다. 표 1에는 노출된 취약점이 가장 많은 10대 업체와 각 업체의 2009년 전체 및 2010년 상반기 패치율이 나와있습니다.

X-Force는 2009년 연말 보고서에 사용된 조사 방법에 잘못된 조사 결과를 초래한 문제가 있음을 발견했습니다. 2010년 상반기 보고서에서, 당사는 이 방법을 정정하여 이제 더 정확한 공식을 사용하고 있습니다. 본 문서에서는 이 새로운 방법을 2009년 데이터에 적용하여 정확도를 높였습니다.

이를 비교하면 몇 가지 흥미로운 결과가 나옵니다. Sun은 2009년에 2.6%라는 훌륭한 패치율을 기록했지만, 2010년 상반기에 이 회사는 패치를 적용하지 않은 비율이 24%로 급상승하여 1위로 뛰어 올랐습니다. Microsoft는 23.2%의 노출된 취약점에 패치를 적용하지 않아 근소한 차이로 2위에 올랐습니다.

가장 취약한 10대 업체와 패치율 2010년 상반기	
업체	패치 미적용률(%)
Sun	24.0%
Microsoft	23.2%
Mozilla	21.3%
Apple	12.9%
IBM	10.3%
Google	8.6%
Linux	8.2%
Oracle	6.8%
Cisco	6.0%
Adobe	2.9%

가장 취약한 10대 업체와 패치율 2009년 상반기	
업체	패치 미적용률(%)
Microsoft	15.8%
HP	14.5%
Mozilla	12.1%
Apple	9.7%
Cisco	8.9%
Linux	5.0%
IBM	4.3%
Oracle	3.3%
Sun	2.6%
Adobe	2.0%

표 1: 2010년에 노출된 취약점이 가장 많은 업체가 패치를 제공하지 않은 비율(%)

전반적으로, 2010년 상반기에 패치가 제공되지 않은 취약점의 비율은 2009년 한 해보다 훨씬 높았습니다. 이는 패치률이 낮아지는 추세임을 의미할 수도 있지만, 단순히 6월 말이라는 데이터 마감일이 한 해 전체의 동향을 반영하지 못하기 때문일 수도 있습니다. 어느 쪽인지는 시간이 지나면 알게 될 것입니다.

현재 Adobe는 노출된 취약점에 대해 패치를 제공하지 않은 비율이 매우 인상적인 2.9%에 불과하여 10대 업체 중 "5% 미만" 구간에 진입한 유일한 업체입니다.

최악 및 최고의 패치 제공업체

표 2에는 2010년 상반기에 패치가 제공되지 않은 노출된 취약점의 비율과 치명적이고 위험도가 높으며, 노출된 모든 취약점 중에 패치가 제공되지 않은 취약점의 비율이 나와 있습니다. WordPress 및 Joomla! 같은 웹 애플리케이션 플랫폼은 이 분석에서 제외되었습니다.

최악 및 최고의 패치 제공업체 표에는 당사 데이터베이스에 분류되어 있는 공개적으로 보고된 정보가 반영되었으며, 업체가 조용히 취약점을 패치했거나 취약점에 대한 공개 보고가 중요하지 않다고 판단하여 그에 관한 공개 대응을 발표하지 않은 상황은 반영되지 않았을 수 있습니다.

이 표는 패치가 없는 노출된 취약점의 비율이 가장 높은 업체의 순으로 정렬되었습니다.

업체	2010년 상반기에 노출된 취약점 중 패치가 적용되지 않은 비율(%)	2010년 상반기에 노출된 치명적이거나 위험도가 높은 취약점 중 패치가 적용되지 않은 비율(%)
모든 업체 – 2010년 상반기 평균	55%	71%
Microsoft	23%	7%
Mozilla	17%	4%
Apple	12%	0%
IBM	9%	29%
Sun	8%	0%
Oracle	7%	22%
Cisco	6%	2%
Novell	5%	10%
HP	4%	5%
Linux	3%	0%
Adobe	3%	2%
Google	0%	0%

표 2: 최고 및 최악 패치 제공업체, 2010년 상반기

공격 노력 대비 잠재적 보상 매트릭스

발표되는 취약점의 수가 증가하고 업체들이 문제 부분에 대한 패치와 보호 수단을 최선을 다해 분주하게 제공하는 가운데, 기업은 어떻게 충분한 보안이 보장되도록 IT 관리자가 기울이는 노력의 우선순위를 정할 수 있을까요? 공격 노력 대비 잠재적 보상 매트릭스(Exploit Effort versus Potential Reward Matrix)는 취약점의 분류를 공격자의 관점에서 생각해보기 위한 간단한 모델입니다.

2010년 상반기에 X-Force는 표3에 열거된 취약점에 대한 경보 및 공지를 발표했습니다. 이는 평면 그래프에 표시되어 있습니다. 가로 축(공격 목표 달성을 위한 노력 수준)은 공격자가 해당 취약점을 악용하여 공격을 감행하기 위해 기울어야 하는 노력을 나타냅니다. 세로 축(잠재적 보상)은 공격자가 얻을 수 있는 잠재적인 이득을 나타냅니다.

X-Force 경보 및 공지의 대상이 된 취약점의 상당수는 우측 상단 쿼드런트(빨간색 바탕)에 몰려 있는 경향이 있습니다. 이 쿼드런트는 공격자에게 많은 이득을 제시하지만 비교적 공격하기는 쉬운 문제를 나타냅니다. 이런 취약점은 인터넷에서 공격을 많이 받는 경향이 있습니다. 반대로, 좌측 하단 쿼드런트(노란색 바탕)에 표시된 취약점 하나는 공격자가 공격하기는 상대적으로 어려운 반면 잠재적인 보상도 미미합니다.

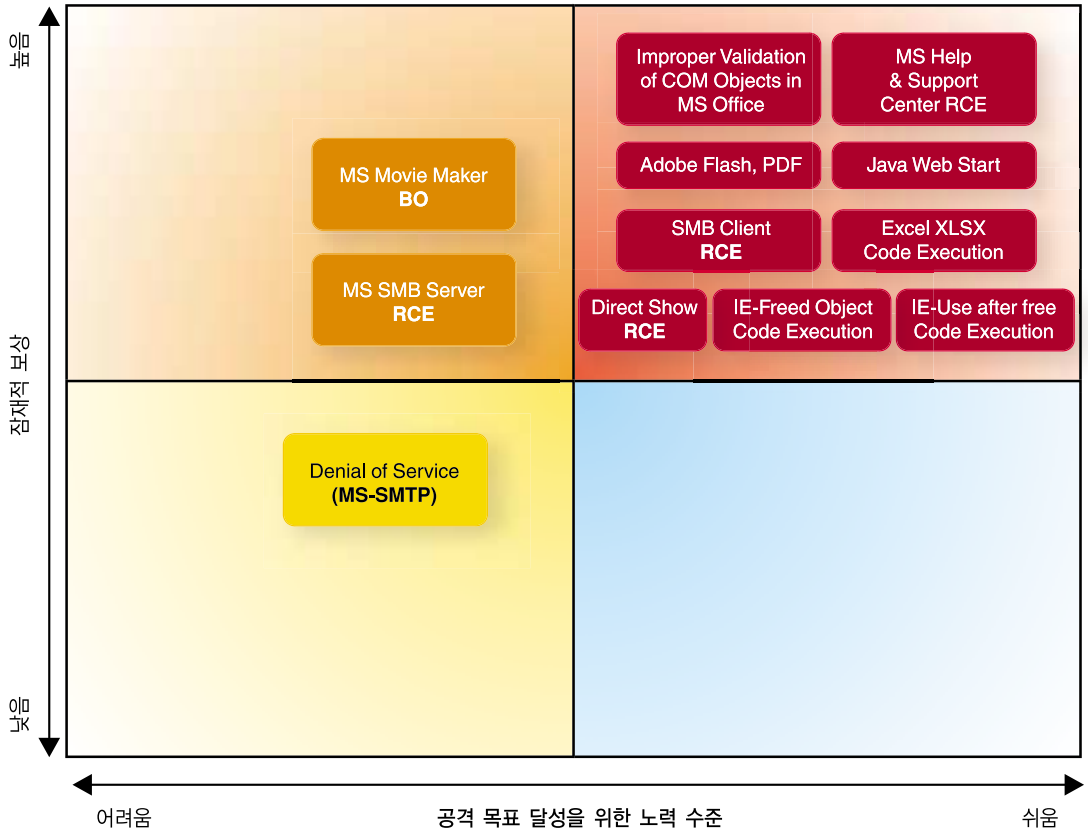


그림 5: 공격 노력 대비 잠재적 보상 매트릭스

나중에 본 보고서의 24페이지에서는 업체가 패치를 공급하기 전에 치명적인 취약점이 조기에 발표될 경우 이런 상황이 어떻게 고객의 활동에 영향을 미치고 곧바로 대처해야 하는 실질적인 문제가 되는지에 대해 설명할 것입니다. 그리고, 이 매트릭스의 우측 상단에 열거된 취약점 중 우려를 자아냈던 두 가지 취약점에 대해 더 자세히 알아볼 것입니다. 그 반대쪽에는 Microsoft SMTP 서비스에 타격을 입히는 서비스 거부(DoS) 문제가 있습니다.

이메일 서비스 거부의 위협은 네트워크 운영자에게 중요한 것이지만, 이 공격 유형이 공격자에게 제시하는 경제적인 기회는 별로 없습니다. 이 취약점을 공격할 수 있는 방법을 공개적으로 발표한 사람은 지금까지 없었기 때문에, 이는 여전히 공략하기가 비교적 어려운 채로 남아있습니다.

Internet Explorer Freed Object Code Execution 취약점은 취약점에 대한 더 많은 정보가 공개됨에 따라 해당 취약점이 어떻게 매트릭스의 왼쪽에서 오른쪽으로 이동할 수 있는 지를 보여주는 예입니다. 이 문제는 처음에 공격자들이 발견하여 특정한 표적을 공략하기 위한 공격에 사용했습니다. 노출 및 패치되지 않는 고유한 취약점을 찾아 공격하기 위해서는 비교적 많은 노력을 기울어야 합니다. 하지만 일단 문제가 공개적으로 알려지자 공격은 널리 확산되었으며, 이제 악당들은 해당 문제를 꽤 적은 비용으로 공략할 수 있게 되었습니다.

날짜	경보/공지	취약점 이름
2010년 6월 14일	경보 370호	**Microsoft Windows Help and Support Center Could Allow Remote Code Execution (Microsoft Windows 도움말 및 지원 센터의 원격 코드 실행 허용 가능성)** Microsoft 도움말 센터의 취약점은 특수 제작된 hcp 요청에 삽입되는 올바르지 않은 유니코드에 기인합니다.
2010년 4월 20일	경보 367호	**Java Web Start** 응용프로그램을 시작하고 설치하는 Java 기능에는 임의 명령이 Java 가상 머신(JVM)으로 직접 전달되도록 허용하는 설계 결함이 있습니다.
2010년 6월 8일	경보 368호	**Improper Validation of COM Objects in Microsoft Office (MS 오피스에 의한 COM 객체의 부적절한 검증)** Microsoft Office 응용프로그램은 복합 문서에 임베디드된 COM 객체를 올바로 검증하지 못합니다. 이를 통해 공격자는 Office의 보안 설정을 우회하고 알려진 결함이 있는 객체를 Office 파일에 심을 수 있습니다. 이런 제어 기능에 전부터 존재했던 결함을 악용하면, 공격자는 임의 코드 실행을 완수할 수 있습니다.
2010년 3월 9일	경보 364호	**Microsoft Internet Explorer Use-after-free 코드 실행** Microsoft Internet Explorer는 올바르지 않은 포인터 참조 오류로 인해 원격 공격자가 시스템에서 코드를 실행하는 것을 허용할 수 있습니다.
2010년 6월 7일	경보 369호	**Flash Player, Adobe Acrobat 및 Acrobat Reader 원격 코드 실행** 이 취약점은 피해자가 특수 제작된 PDF(portable document format) 파일이나 SWF 파일을 열 경우 원격 코드 실행을 초래할 수 있습니다.

23 페이지에 표 계속

날짜	경보/공지	취약점 이름
2010년 1월 15일	경보 359호	**Microsoft Internet Explorer Freed Object Code Execution** 웹 공격 툴킷은 이 취약점과 같이 브라우저와 브라우저 관련 취약점을 공략하는 것으로 악명이 높습니다. 이 취약점은 Google을 비롯한 20개 이상의 대기업을 대상으로 한 잘 알려진 공격과 관련되었던 것으로 보도되었습니다.
2010년 4월 13일	경보 366호	**Microsoft DirectShow 원격 코드 실행** 이 취약점은 최근의 모든 Microsoft Windows 운영체제에 존재합니다. 이 문제를 성공적으로 공격하면, 공격자는 목표한 말단컴퓨터를 완전히 제어할 수 있게 됩니다. 지난 몇 년 동안에는 이미지와 동영상 같은 악성 미디어 파일이 많이 사용되었습니다.
2010년 3월 9일	경보 363호	**Microsoft Excel XLSX 코드 실행** Microsoft Excel는 Excel 스프레드시트 형식의 부적절한 파싱으로 인해 원격 공격자가 시스템에서 임의 코드를 실행하는 것을 허용할 수 있습니다.
2010년 2월 9일	경보 360호	**Microsoft Windows SMB 클라이언트 원격 코드 실행** 이 취약점은 Windows 7을 포함한 대부분의 최신 Microsoft Windows 운영체제의 핵심 구성요소 안에 있습니다. 가장 쉬운 공격 경로를 사용하고자 하는 공격자는 SMB 서버를 구축하고 사용자가 서버로 연결되는 링크를 클릭하도록 유도하기만 하면 됩니다. 공격에 성공한 공격자는 최종 사용자의 시스템을 완전히 조종할 수 있게 됩니다.
2010년 3월 9일	경보 362호	**Microsoft Movie Maker 버퍼 오버플로우** Microsoft Movie Maker는 악성 Movie Maker (.mswmm) 파일을 파싱할 때 부적절한 경계 검사(bounds checking)에 의해 초래되는 버퍼 오버플로우에 취약합니다.
2010년 2월 9일	경보 361호	**Microsoft Windows SMB 서버 원격 코드 실행** 이 취약점은 서버 에디션을 포함한 대부분의 최신 Microsoft Windows 운영체제를 구성하는 핵심 요소 안에 있습니다. 올바로 계획된 공격은 최종 사용자와의 어떤 상호작용도 없이 완전한 원격 코드 실행을 지원할 것이지만, 서비스 거부(DoS)가 일어날 가능성이 더 큽니다. 그러나, 공격자는 먼저 시스템 인증 권한을 갖고 있어야 하며, 이 시나리오에서 게스트 계정은 사용할 수 없을 것입니다.
2010년 4월 13일	경보 365호	**Denial of Service Conditions in Microsoft Exchange and Microsoft SMTP Service** **(Microsoft Exchange 및 Microsoft SMTP 서비스의 서비스 거부 상태)** 성공적인 공격은 SMTP 서비스가 재시작되는 결과를 초래할 수 있으며, 반복적인 공격은 Microsoft Exchange 서비스를 완전히 중단시킬 수 있습니다. SMTP 서비스는 종종 인터넷에 노출되며, 이메일은 일반적으로 비즈니스에 필수적인 기능으로 간주되기 때문에 이 취약점이 비즈니스에 미치는 영향은 일반적인 서비스 거부 문제보다 더 심각합니다.

표 3: X-Force 경보 및 공지, 2010년 상반기

중요한 영향을 미친 공개 노출

2010년 상반기에 노출된 가장 중요한 취약점 2가지는 Java Web Start와 Microsoft Windows Help and Support Center(도움말 및 지원 센터)의 원격 코드 실행 취약점이었습니다. 이 두 가지 취약점은 모두 각 업체가 패치를 제공하기 전에 Tavis Ormandy라는 연구학자에 의해 공개적으로 알려졌습니다. 패치가 나오기 전에 공격에 악용될 수 있는 취약점에 대한 상세정보가 공개될 때마다 공격자는 최소한의 노력으로 최대한의 효과를 거둘 수 있는 기회를 얻게 됩니다. 이들 취약점과 관련하여 실운영 환경에서 목격된 재빠른 공격 활동은 그림 6에서 볼 수 있듯이 당사 모델의 예측과 일치합니다.

Java Web Start 취약점을 예로 들면, 2010년 4월 20일에 IBM Security는 당사 고객을 보호하기 위해 새로운 서명을 배포했으며, 당사 웹사이트에서 해당 위협을 발표했습니다. 오른쪽에 있는 데이터를 보면, 2010년 4월 21일부터 이 새로운 서명을 배포한 고객이 얻은 즉각적인 효과를 확인할 수 있습니다. 첫 날에는 100건이 넘는 보안 이벤트가 전체 고객 기반에 걸쳐 목격되었으며, 이 수치는 6월 말까지 계속 증가한 후 7월에 서서히 감소하기 시작했습니다.

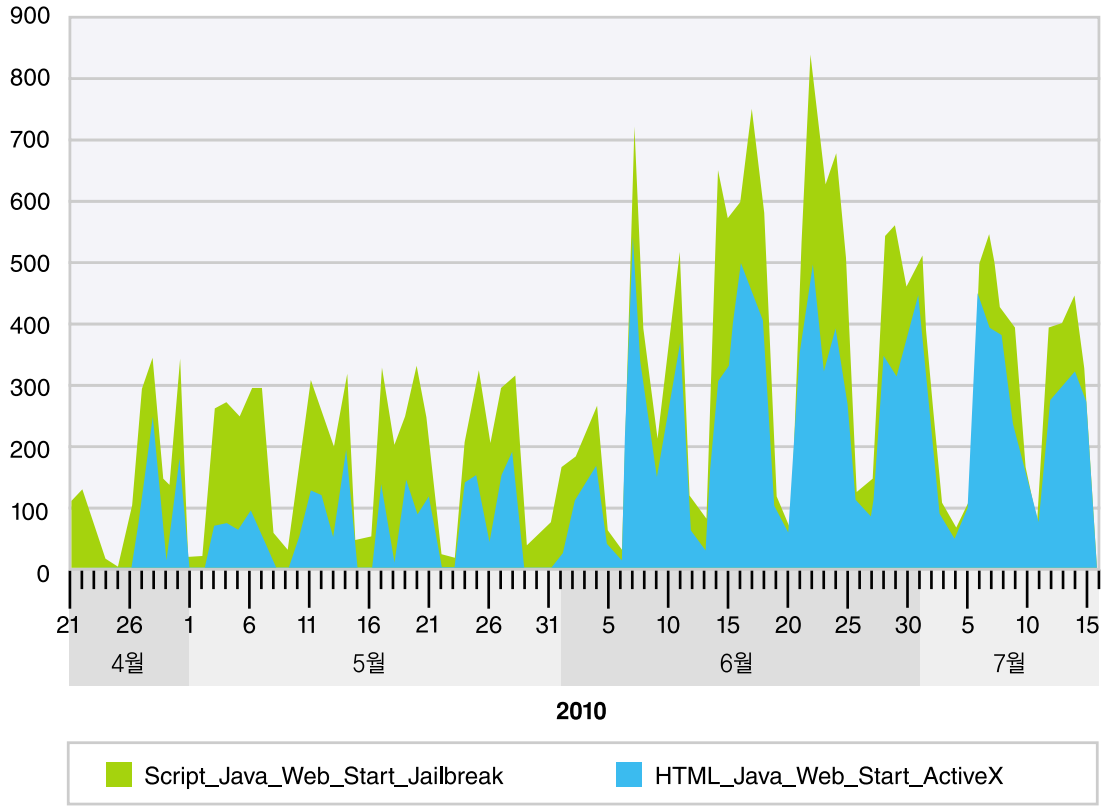


그림 6: Java Web Start 취약점 발표 후의 MSS 고객 이벤트 활동, 2010년 상반기 4~7월

Conficker 최근 소식 – 2009년 말 이후로 일어난 일?

Conficker 웜은 최근 몇 년 간 컴퓨터 보안에 관한 가장 큰 기사거리 중 하나였습니다. X-Force는 이 동향 보고서에 Conficker에 대한 최근 소식을 포함시킬 필요가 있다고 결정했지만, 먼저 Conficker의 역사를 간략히 알아보도록 하겠습니다.

Conficker는 2008년 가을에 처음 확산되기 시작했습니다. (Conficker.A라는) 최초 변형은 최근에 패치된 Microsoft RPC 스택의 원격 코드 실행 취약점을 공략했습니다. Conficker.A는 과거에 유사한 취약점을 공략했던 2003년의 Blaster 웜 같은 웜에 비해 특별히 더 성공적으로 확산되지는 않았는데, 그 이유는 주로 인터넷이 취약점 노출에 대응하는 방법이 빠르게 개선되었기 때문이었습니다. 2008년 말에 Conficker가 감염시킨 호스트의 수는 몇 십만에 불과했습니다.

2008년 12월 말에는 Conficker.B라는 새로운 버전의 Conficker가 등장했습니다. Conficker.B는 기존의 Conficker에 수많은 대체 전파 경로를 추가시켰습니다. Conficker.B는 USB 키나 파일 공유를 통해 확산되거나, Windows 도메인에서 쉬운 비밀번호를 해킹함으로써 확산될 수 있었습니다. 이런 대체 전파 경로로 인해 Conficker는 더 민첩해졌습니다. Conficker는 여러 경로를 사용하여 다양한 네트워크에서 발판을 마련할 수 있게 되었습니다. 그 결과, 감염된 호스트의 수는 크게 증가했습니다.

2009년 겨울에는 Conficker에 대처하기 위해 Conficker Working Group이라는 단체가 구성되었습니다. Conficker.A 및 B 노드는 매일 500개의 무작위로 생성된 도메인명에 접촉을 시도하여 업데이트를 찾습니다. Conficker Working Group는 Conficker 운영자가 봇(bot)을 업데이트할 수 없도록 해당 도메인명을 모두 등록했습니다.

하지만 안타깝게도 Conficker 업데이트 하나가 이를 뚫었습니다. 이 새로운 변형의 이름은 Conficker.C입니다.

Conficker.C는 도메인의 목록을 500개에서 50,000개로 확장했으며, Conficker Working Group이 등록할 수 있는 도메인에 의존하지 않은 암호화된 P2P 업데이트 메커니즘을 추가했습니다. 이 새로운 기능으로 인해 Conficker Working Group은 Conficker.C의 업데이트를 막을 수 없게 되었습니다. 다행히 Conficker.C에는 전파 코드가 포함되지 않았기 때문에 감염이 최초 노드 밖으로 확산될 방법이 없었습니다.

Blaster 웜은 2008년 8월에 인터넷 상에서 전파되기 시작했습니다. 이 웜은 Conficker.A가 공격했던 취약점과 매우 유사한 Microsoft Windows RPC 스택의 취약점(MS03-026)을 공격했습니다. Blaster의 전파는 첫 배포 후 8 시간 안에 최고조에 달했으며, 인터넷에서 감염시킨 호스트의 수는 최종적으로 800만에서 1,600만 사이였습니다. Blaster는 WindowsUpdate.com을 대상으로 분산 서비스 거부(DDoS) 공격을 개시했으나, Microsoft는 실제로 여러 주소를 사용하여 업데이트를 호스팅했기 때문에 피해는 미미했습니다.

Conficker에 대한 X-Force의 대응

X-Force 연구원들은 Conficker 코드를 리엔지니어링하고 당사의 IPS 제품에서 Conficker.C P2P(Peer-to-Peer) 트래픽을 감지하고 차단할 수 있는 서명을 개발했습니다. 그림 7에는 이런 트래픽의 양이 시간이 흐름에 따라 서서히 감소하는 모습이 나와 있습니다. 그러나, 최근 데이터를 조사하자 본 보고서의 인쇄를 시작하려던 6월쯤에 소폭의 증가세가 감지되었습니다. X-Force 연구원들은 이 잠재적인 추세 변화가 감지됐던 이유를 계속 조사하고 더 자세한 내용이 파악되면 Frequency X 블로그를 통해 독자에게 최신 현황을 알릴 것입니다.

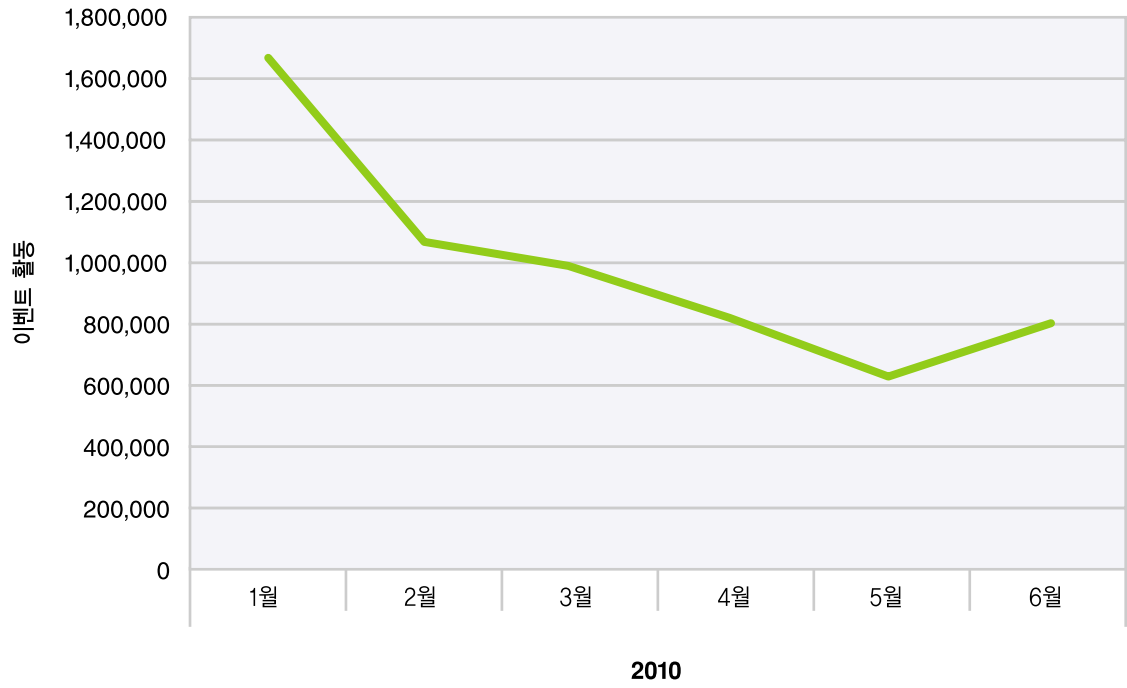


그림 7: Conficker 활동, IBM Managed Security Services, 2010년 상반기

이 데이터는 X-Force의 Darknet에서 얻은 Conficker.C 데이터와 일치합니다(아래 그림 8).

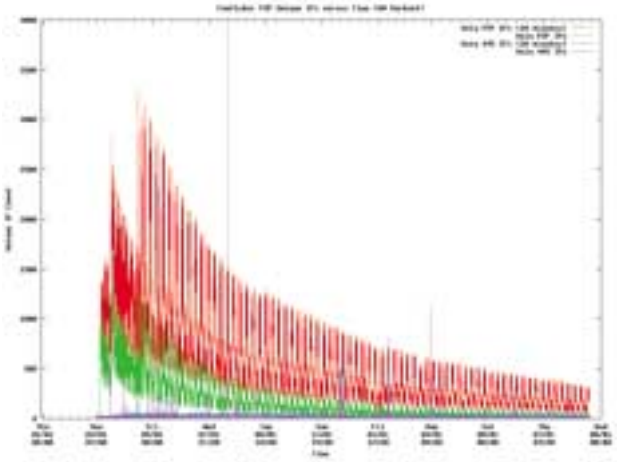


그림 8: Conficker Working Group

Conficker.C는 감염된 노드가 바이러스 백신 소프트웨어로 치료되거나 단순히 고장남으로 인해 인터넷에서 제거됨에 따라 서서히 사라지고 있습니다. Conficker.C는 새로운 노드를 감염시킬 방법이 없기 때문에 인터넷 상에서 그 수를 유지할 수 없습니다. Conficker Working Group은 봇넷 운영자가 Conficker.C 노드를 업데이트하는 것을 막을 수 없기 때문에, 이는 매우 다행입니다. 아직도 인터넷 상에는 업데이트를 기다리고 있는 20만에 가까운 Conficker.C 노드가 있습니다. 지금까지 광범위한 업데이트가 배포된 적은 없습니다.

이는 Conficker Working Group의 하강 지점(Sinkholes)과도 일치합니다(그림 9).

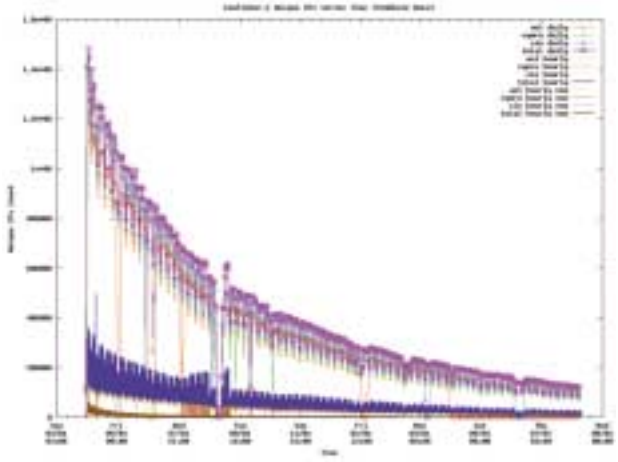


그림 9: Conficker Working Group

Conficker Working Group에 따르면 Conficker.A/B 봇넷은 5~6백만 대의 노드로 구성되어 있어 훨씬 더 크다고 합니다(위 그림 10). 이 봇넷의 규모는 2009년 11월 경에 정점을 찍었으며, 거의 9개월 동안 일정한 수준으로 유지되었습니다. Conficker.A/B 노드는 Conficker.C가 사망하는 것과 같은 바이러스 백신 설치 및 시스템 장애의 이유로 매일 조금씩 사망하는 것으로 추정됩니다. 그러나, Conficker.A/B 노드는 새로운 시스템에 침투함으로써 여전히 전파되고 있습니다.

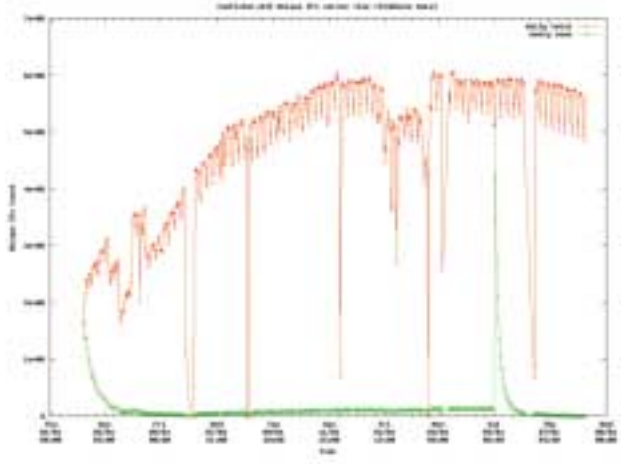


그림 10: Conficker Working Group

그 수를 유지하려면, 새 노드를 감염시키는 속도는 노드가 사망하는 속도와 같아야 합니다. 이런 속도가 그토록 오랫동안 꾸준히 유지되어 왔다는 점은 흥미롭습니다.

Conficker의 미래

다행히 Conficker를 만든 이들이 5~6백만 노드에 달하는 Conficker.A/B 봇넷으로 할 수 있는 일은 아무것도 없습니다. 왜냐하면, Conficker Working Group은 아직도 이들 노드가 접촉하려고 시도하는 500개의 도메인명을 하루도 빠짐없이 매일 등록하고 있기 때문입니다. Conficker Working Group이 지금과 같은 노력을 포기할 경우, 공격자들은 인터넷 인프라에 커다란 위협을 가할 수 있는 매우 큰 봇넷을 조종할 수 있게 될 것입니다.

Conficker가 전파되기 시작한 지는 거의 2년에 되어가지만, Conficker는 아직도 죽지 않았습니다 Conficker는 잠자는 한 쌍의 용으로 남아있으며, 그 중 하나만 갇혀 있습니다. 이 경험으로부터 얻은 교훈은 대부분 좋지 않은 것입니다. 웜은 여전히 지금의 인터넷에서 매우 큰 봇넷을 구축하기 위해 사용될 수 있음이 분명합니다. 이처럼 다양한 악의적인 목적에 악용할 수 있는 매우 많은 수의 노드로 구성된 봇넷은 수 년 동안 존속할 수 있음이 분명합니다. 그리고, Conficker.C의 경우 전세계 공통으로 대처할 수 없는 봇넷 명령 및 제어 시스템의 구축이 가능하다는 것이 분명합니다.

그러나, Conficker 관련 경험과 Conficker Working Group의 구성은 인프라 운영자와 보안 회사들이 더 긴밀히 연결되는 계기가 되었습니다. 다음에 대규모 웜 확산 사태가 발생할 때 이 커뮤니티는 대응할 준비가 되어있을 것입니다.

다크넷 동향 분석 – 악성 트래픽은 어떻게 생겼는가?

IBM 분석가들이 동향 분석 용도로 쉽게 이용할 수 있는 데이터 리소스는 많습니다. 그 중 하나는 블랙홀 네트워크라고도 하는 다크넷(Darknet)입니다. 이 공간은 지속적으로 모니터링되며, 모든 수신 트래픽은 분석 및 장기 보관을 위해 수집 및 저장됩니다. 규모가 25,600개 주소에 달하는 이 다크넷은 더 큰 정보 수집 네트워크의 일부입니다. 다크넷의 본질적인 성격으로 인해 이들 주소에서 비롯되는 패킷은 절대 없으며, 합법적인 트래픽은 절대 해당 주소를 목적지로 하지 않을 것입니다. 또한, 이들 주소는 한 번도 인터넷 상의 어떤 합법적인 활성 기기나 서비스에 할당된 적이 없습니다. 그럼에도 불구하고 이들 주소는 합법적인 "/16" 네트워크의 일부로 공시되고 인터넷 전체에서 완전한 라우팅이 가능합니다. 따라서, 이 네트워크로 유입되는 모든 트래픽은 악성으로 간주됩니다.

위장 서비스 거부(DoS) 공격

지난 몇 년 간에 걸친 데이터를 보면 몇 가지 흥미로운 패턴이 나타나기 시작하고 있음을 알 수 있습니다. 첫 번째 추세는 후방산란(Backscatter) 활동의 점진적인 증가입니다(그림 11). 후방산란(Backscatter)은 사실 위장 DoS(서비스 거부) 공격의 부작용입니다. 피해자에게 보내는 인터넷 프로토콜(IP) 패킷의 소스 주소를 속임으로써, 피해자의 시스템은 위장 패킷과 합법적인 패킷을 구별하지 못하고 위장 패킷에 응답하게 됩니다. 이 같은 응답 패킷을 후방산란(Backscatter)이라 합니다.

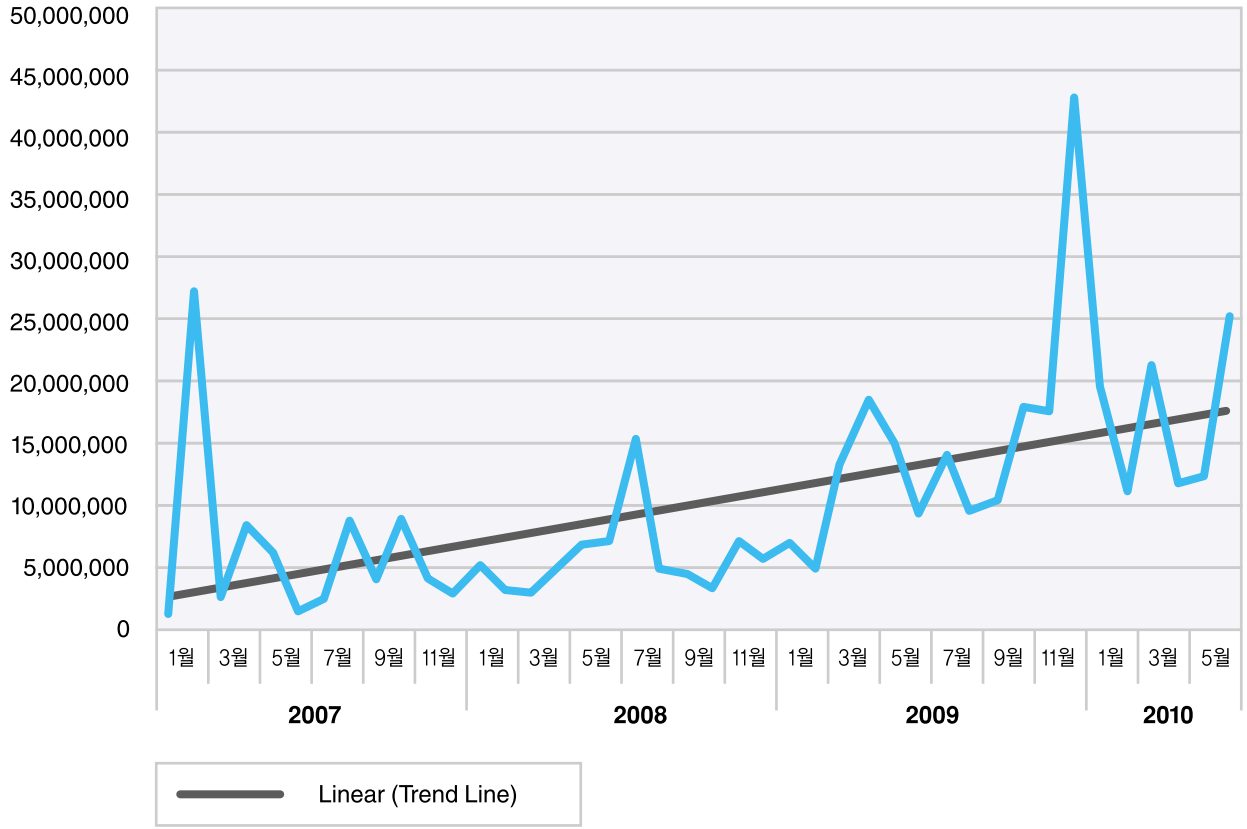


그림 11: 후방산란(Backscatter), 마이크 워필드 다크넷, 2007년 1월~2010년 5월

마이크 워필드(Mike Warfield)의 다크넷(Darknet)에서, 수신된 각 SYN-ACK 후방산란(Backscatter) 패킷은 공격자가 마이크 워필드의 다크넷 주소 중 하나에서 위장(Spoofed) 공격을 받고 있는 컴퓨터의 잘 알려진 서비스 포트로 위장 패킷을 보냈음을 나타내는 신호입니다.

후방산란(Backscatter) 활동은 2007년부터 점진적으로 증가해 왔지만, 특히 2008년과 2009년 사이에 크게 증가했습니다. 이 같은 증가의 부분적인 이유는 2009년에 활동이 3년 반에 걸친 기간 동안 가장 큰 폭으로 크게 급증했기 때문입니다. 이처럼 전년 평균을 계속 상회하는 추세는 2010년에도 계속되고 있습니다.

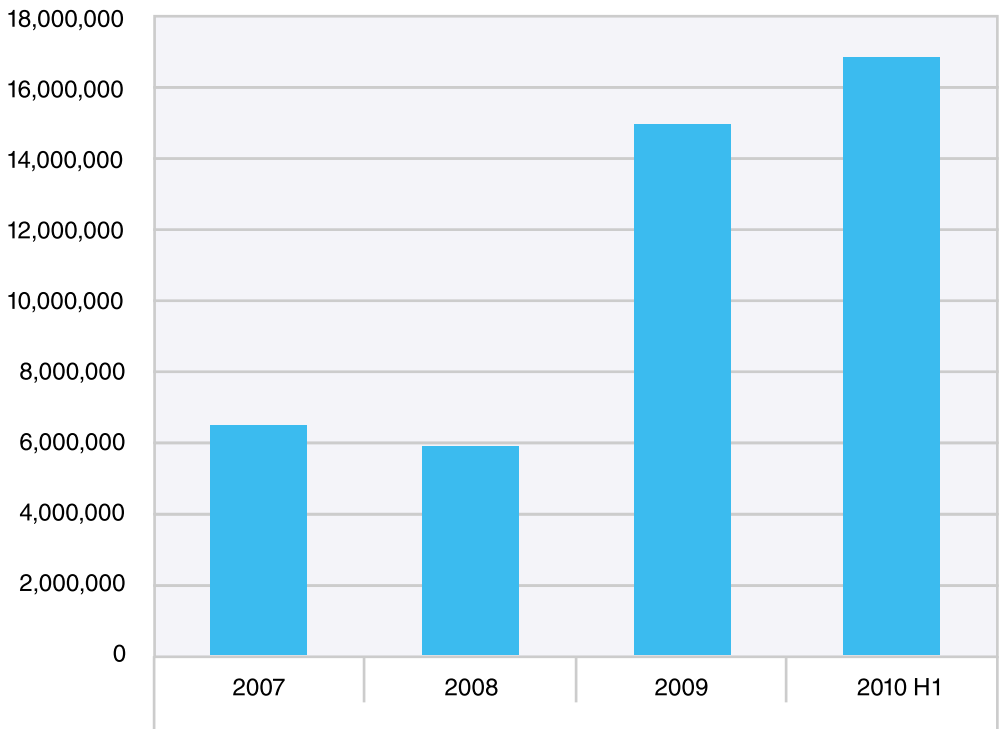


그림 12: 후방산란(Backscatter) – 평균, 마이크 워필드 다크넷, 2007년～2010년 상반기

2분기 말에 집계된 2010년 상반기 평균은 2009년 전체 평균보다 약간 많은 데 그쳤습니다. 그림 12를 보면 인터넷 상에서 위장(Spoofed) 서비스 거부 공격의 양이 2007년부터 2010년까지 증가한 추세를 실제로 확인할 수 있습니다.

이 같은 후방산란(Backscatter) 데이터의 점진적인 증가와 후방산란(Backscatter) 활동의 간헐적인 급상승으로부터 유추할 수 있는 것은 무엇일까요? 대부분의 후방산란(Backscatter) 데이터는 DoS 공격에 기인하는 것이므로, 2007년부터 위장 DoS 공격이 꾸준히 증가해 왔음을 추측할 수 있습니다. 그러나, 후방산란(Backscatter)은 수집되는 것과 방생하는 일의 성격으로 인해 변동폭이 클 수 있습니다. 후방산란이 일부 기간에 집중된 것은 여러 공격 진영 안팎에서 일어난 대격전에 기인했습니다. 이런 전쟁이 일어날 때 한 집단은 다른 집단의 리소스를 차단하거나 빼앗으려고 합니다. 서로 전쟁하는 진영 간에 벌어지는 이런 "포격 시합"은 후방산란 트래픽과 후방산란 소스 주소의 갑작스런 증가를 초래할 수 있습니다. 이런 싸움은 보통 갑작스럽게 시작한 만큼 갑작스럽게 중단됩니다. 이런 활동은 그림 11에서 2007년 2월과 2009년 12월에 그래프가 급상승한 원인이었을 가능성이 큽니다.

무차별(Brute Force) 공격

마이크 워필드의 다크넷은 부차별 공격의 세계에 대한 통찰력도 제시합니다. 컴퓨터 보안에서 말하는 무차별 공격이란 공격자가 많은 수의 가능한 비밀번호를 시도함으로써 허가 없이 시스템에 대한 접근 권한을 획득하고자 하는 것을 말합니다. 종종 무차별 공격의 대상이 되는 서비스로는 SSH(TCP 포트 22), Telnet(TCP 포트 23), RealVNC (TCP 포트 5900) 및 Microsoft Remote Desktop(TCP 포트 3389) 등이 있습니다.

그림 13은 이들 포트의 평균 활동을 2008년부터 비교하고 있습니다. RealVNC와 Microsoft Remote Desktop 포트에서는 모두 활동이 서서히 증가하는 추세가 나타나고 있습니다. 반대로, SSH는 서서히 꾸준하게 감소하고 있으며, Telnet는 2009년 후로 급감했습니다.

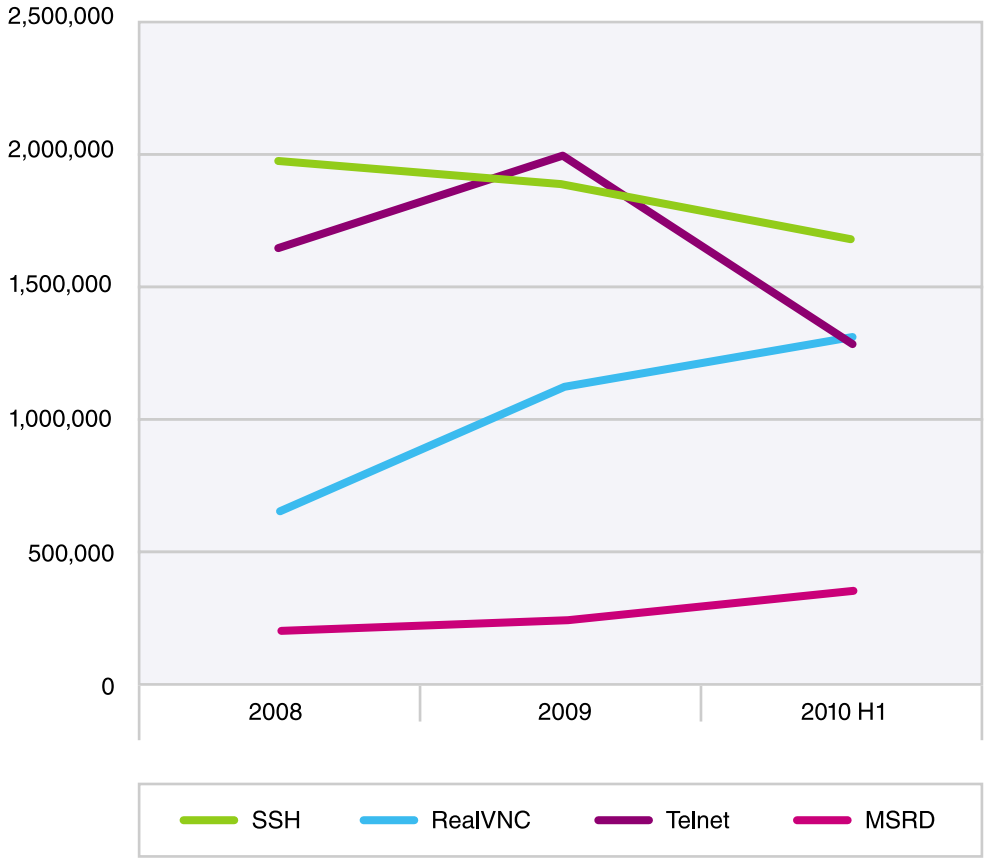


그림 13: 무차별(Brute Force) 공격 포트 – 평균, 마이크 워필드 다크넷, 2008년~2010년 상반기

이 데이터는 SSH 및 Telnet 포트의 공략에 대한 관심이 지난 1년 반 동안 감소했을 가능성이 있는 반면 RealVNC 및 MS Remote Desktop 포트는 인기가 높아져가고 있음을 시사합니다. 이는 해당 프로토콜을 공략하는 취약점이 발표된 시기와 관련이 있을까요? 그림 14는 이 4개의 포트에서 지난 2년 반에 걸쳐 일어난 전체 다크넷 활동이 나와 있습니다. 일부 증가 추세는 취약점 노출과 관련이 있을 수 있습니다. 예를 들면, 올해 5월 초에 RealVNC를 타겟으로 삼았던 취약점은 2분기 말의 순간적인 증가에 기여했을 수 있습니다. 2008년 5월에는 SSH를 공략하는 취약점 6개가 노출되었으며, 다크넷 그래프는 이 달에 큰 폭의 증가세를 나타냈습니다. SSH 활동은 FreeSSHd를 공략하는 취약점이 노출되었던 2008년 12월에 더 크게 증가했습니다.

그러나, 모든 데이터 급증을 비슷한 시기에 노출된 취약점의 탓으로 돌릴 수 있는 것은 아닙니다. 실제로, Telnet에 영향을 미치는 취약점은 2005년 3월에 마지막으로 노출되었습니다. 그 밖에, 2009년 8월에 RealVNC가 급증했던 경우처럼 활동이 크게 증가한 이유가 취약점 노출 시기와는 전혀 관계가 없는 경우도 있었습니다. 이를 통해, 공격자들은 항상 최신 취약점을 사용하지 않고 종종 오래된 취약점에 의존하여 공격을 감행함을 알 수 있습니다.

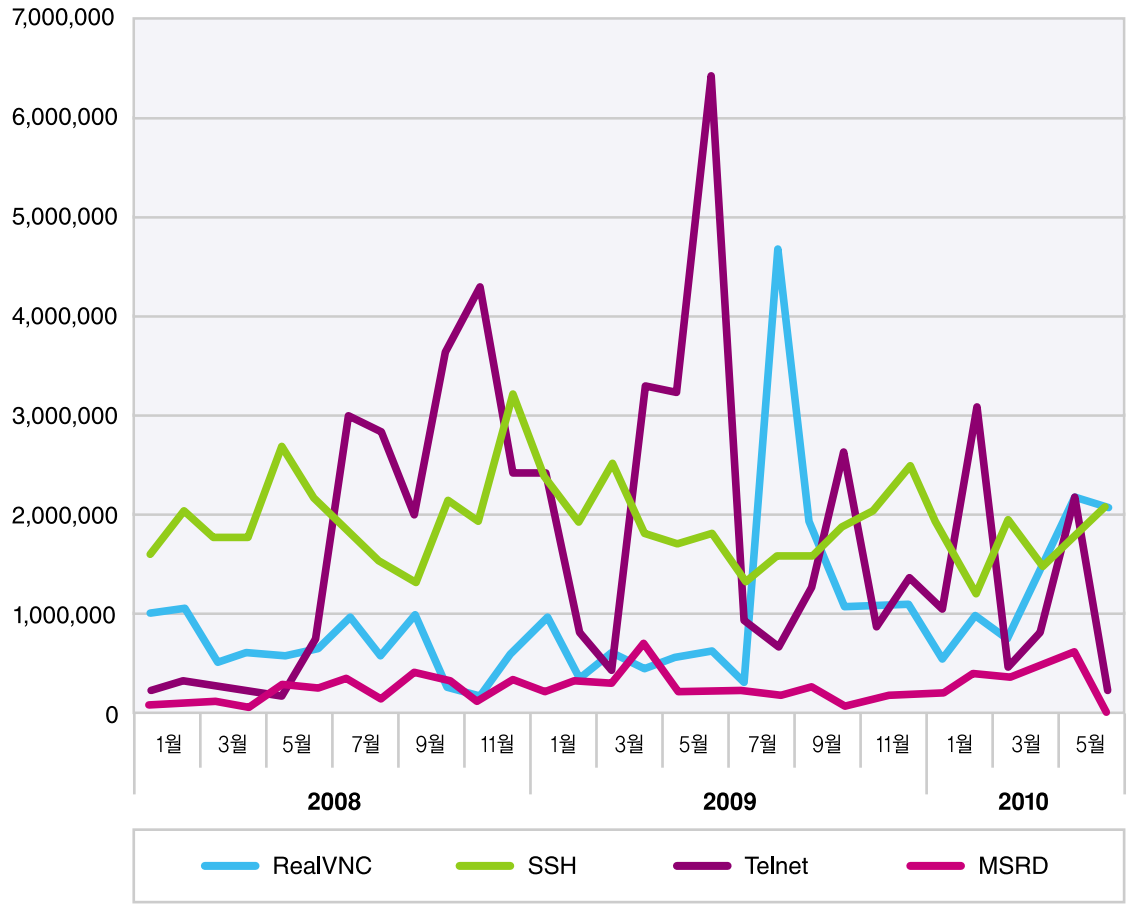


그림 14: 무차별 공격 활동의 포트별 분석 – 총 수, 마이크 워필드 다크넷, 2008년 1월~2010년 5월

컴퓨터 범죄 – 누가 누구를 속이는가?

Zeus 봇넷 – 사실과 오해 그리고 Zeus 봇넷의 작동 방법 이해

Zeus/Zbot 봇넷군(Family)은 몇 년 전부터 인터넷에서 말썽을 일으켜 왔습니다. 위협은 진화해 왔으며, 새로운 버전과 기능이 끊임없이 발견되고 있습니다. 언론 보도에 따르면, Zeus는 개인 정보 도용을 통해 기업 및 개인에게 수백만 달러의 손실을 끼쳐왔습니다.

Zeus 봇넷 운영자는 일반적으로 악성 문서를 대량 이메일을 통해 피해자에게 살포하거나 Zeus 봇을 설치하는 악성 컨텐츠를 제공하는 웹사이트로 피해자를 유도함으로써 새로운 PC를 감염시킵니다. 일단 설치된 Zeus는 감염된 PC의 인터넷 트래픽을 모니터링하고 정보를 중앙 명령 및 제어(C&C) 서버로 다시 보고하게 됩니다. 수집되는 정보는 운영자가 bot를 어떻게 설정하느냐에 따라 달라지지만, 은행 계좌 정보가 수집되는 경우가 많습니다. 이 정보는 PC의 보안 및 암호화 설정에 관계 없이 수집됩니다. Zeus는 코드를 웹 브라우저에 직접 주입하여 개인 정보를 수집할 수 있습니다.

일단 수집된 피해자 정보는 봇넷 운영자가 직접 사용하거나 온라인에서 다른 범죄 집단에 판매됩니다.

Zeus에 대한 오해

Zeus와 그 작동 방법에 대해서는 많은 오해가 있습니다. 이런 오해 중 일부는 대중 매체를 통해 확산되거나 심지어는 기술적 지식 수준이 상대적으로 더 높은 IT 매체를 통해서도 확산됩니다. 이 같은 오해와 잘못된 인식이 생겨나는 이유는 용어의 오용 때문이며, 비록 말이 중요한 것은 아니라고 주장할 사람도 있을 지 모르지만 X-Force는 위협을 정확하게 묘사하기 위해 악성코드 용어의 엄격한 정의를 따르는 것이 중요하다고 믿습니다.

Zeus 봇넷은 하나뿐

그렇지 않습니다. 온라인에서 판매되는 Zeus Builder 툴킷을 사용하면 누구나 자신만의 Zeus 기반 봇넷을 만들고 관리할 수 있습니다. 특정한 시점에 활동하는 개별적인 Zeus 봇넷의 수는 수백 내지는 수천 개에 이릅니다. abuse.ch 스위스 보안 블로그의 서비스인 Zeus Tracker(https://zeustracker.abuse.ch/)는 활성 Zeus 명령 및 제어 서버를 모니터링합니다. 본 문서를 작성했을 당시에는 각각 서로 다른 집단이나 개인에 의해 운영되었을 수 있는 644대의 활성 Zeus C&C가 추적되고 있었습니다.

Zeus는 바이러스나 웜이다

그렇지 않습니다. 바이러스는 전통적으로 플로피 디스크나 USB 키를 삽입하거나 프로그램을 실행하거나 이메일 첨부파일을 여는 등 사용자와 어떤 상호작용을 요하는 방법으로 확산되고 컴퓨터를 감염시키는 프로그램입니다. 웜은 바이러스와 유사하지만 사용자와의 상호작용 없이 확산됩니다. 이를 위해, 웜은 흔히 보안 취약점을 악용합니다.

Zeus는 이런 정의에 해당되지 않습니다. 스스로 확산되는 기능이 없기 때문입니다. Zeus는 백도어(사용자의 컴퓨터에 접근할 수 있는 권한 제공)나 트로이목마(스스로 주장하는 것과는 다른 어떤 것)로 정의하는 것이 더 정확할 것입니다. "Zeus가 확산되고 있다"는 식의 말을 들으면 Zeus가 스스로 확산될 수 있는 기능을 갖고 있다는 생각이 들 수 있지만, 사실은 그렇지 않습니다.

Zeus는 취약점과 공격을 사용하여 자동으로 설치된다

이 역시 틀린 말입니다. Zeus 자체는 백도어나 트로이목마에 불과합니다. 그러나, Zeus를 사용하여 정보를 훔치는 많은 집단과 개인은 공격을 통해 Zeus를 전달합니다. 이 경우 Zeus는 공격의 페이로드(Payload)지만, 그 자체는 공격과 아무 관계도 없습니다. Zeus를 전달하기 위해 사용된 취약점은 PDF 공격, 다양한 ActiveX 컨트롤 공격 등 많았습니다. 새로운 취약점이 공개될 때마다, 그것을 사용하여 Zeus를 전달하는 사람이 꼭 있습니다. 이는 Zeus 자체나 Zeus Builder의 제작자와는 아무 관계도 없습니다. Zeus는 단지 피해자로부터 금융 정보를 훔치는 것이 목표일 때 매우 효과적인 페이로드일 뿐입니다.

Zeus 봇넷 툴킷의 새로운 버전

2010년 초에는 Zeus 봇넷 키트의 업데이트된 버전이 Zeus 2.0이라는 이름으로 배포되었습니다. 새 버전에 포함된 중요한 신기능은 Firefox 웹브라우저에서 개인 데이터를 가로채는 기능이었습니다. 이전 버전의 Zeus는 Internet Explorer에서만 데이터를 가로챌 수 있었습니다. 그 외에도 Zeus의 이전 버전에서 변경된 사항은 많습니다.

Zeus 2의 바뀐 점

Zeus 2에는 몇 가지 변경사항만 적용되었습니다. 변경사항의 상당수는 사용자가 컴퓨터에 대한 관리자 접근 권한을 갖고 있지 않을 수 있는 전사 환경에서 Zeus가 컴퓨터를 더 효과적으로 감염시킬 수 있도록 하기 위한 것이었습니다.

자동 시작 기법 – Zeus의 이전 버전은 감염된 사용자가 관리자 권한을 갖고 있을 때는 `HKLM\Microsoft\WindowsNT\CurrentVersion\Winlogon` 레지스트리 키를 그리고 관리자 권한이 없이 실행했을 때는 `HKCU\Microsoft\Windows\CurrentVersion\Run`을 이용함으로써 시스템 시작 시에 자동으로 설치되어 실행되었습니다. Zeus 봇(bot)은 키를 지속적으로 모니터링하고 모든 변경을 막았기 때문에 제거하기가 어려웠습니다. Windows를 안전 모드에서 부팅해도 Winlogon 키를 사용하면 여전히 Zeus가 로드될 수 있었습니다.

Zeus의 새 버전에서는 `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`을 사용하여 사용자의 권한 수준에 관계 없이 Zeus를 자동으로 실행시킵니다. 이 항목은 레지스트리에서 감지하고 삭제하기가 더 쉽습니다. 이렇게 하면 Zeus가 처음에 감염된 사용자 계정으로만 실행되기도 합니다.

파일 위치 – 이전 버전의 Zeus는 스스로의 사본을 수정하지 않은 채로 사용자가 관리자 권한을 갖고 있으면 `Windows\System32` 디렉토리에, 그렇지 않으면 사용자의 `Application Data` 디렉토리에 저장했습니다. 이 파일의 이름은 일반적으로 `sdra64.exe`였습니다. 새로운 버전은 사용자의 `Application Settings` 디렉토리에 무작위로 이름을 지정한 하위 디렉토리를 만들고, 스스로의 사본을 무작위 파일명을 사용하여 그 안에 집어넣습니다.

네트워크 트래픽 – 명령 및 제어(C&C) 서버와 통신하기 위해 사용되는 프로토콜은 네트워크 단계부터 대체적으로 동일합니다. HTTP POST 데이터는 RC4를 사용하여 암호화됩니다. Zeus의 HTTP 요청에 관한 눈에 띄는 변경사항 중 하나는 이제 "`Pragma: no-cache`"를 포함하는 이전의 HTTP-1.0 스타일 헤더 대신 "`Cache-control: no-cache`" 명령이 HTTP 요청 헤더에 사용된다는 것입니다.

고유 감염 바이너리 – Zeus는 사용자의 Application Settings 디렉토리에 저장한 스스로의 사본에 약간의 수정사항을 무작위로 적용합니다. 이는 Zeus 인스톨러 하나를 여러 사람에게 전송할 경우, 그로부터 결과는 감염 시 각각 약간씩 다른 실행파일이 포함될 것임을 의미합니다. 바뀌는 것은 몇 바이트에 불과하지만, 파일의 SHA 또는 MD5 해시를 바꾸기에는 충분합니다. 파일 크기도 다를 수 있습니다.

특정 컴퓨터에 결속된 바이너리 – Zeus는 이제 상용 소프트웨어 복사 방지와 유사한 기법을 사용하여 설치된 실행 파일의 분석을 더 어렵게 만듭니다. 일단 컴퓨터가 감염되면, 원래의 실행파일은 삭제되고 디스크에 저장된 파일은 다른 컴퓨터에서 실행되지 않습니다. 이는 부트 드라이브의 볼륨 GUID와 실행파일이 저장된 디렉토리를 확인함으로써 이루어집니다. 확인된 정보가 EXE 자체에 저장된 정보와 일치하지 않으면, Zeus는 실행되지 않습니다. 따라서 공통 자동 분석 기법은 효과가 없습니다.

구성 파일 위치 – Zeus 1.3 이하 버전에서 구성 파일은 서버에서 다운로드되어 `Windows\System32`(또는 사용자에게 관리자 권한이 없을 경우 `Application Data` 디렉토리)에 "`local.ds`"라는 이름으로 저장되었습니다. Zeus는 이제 파일을 다운로드한 후 무작위로 이름을 지정하여 사용자의 `Application Settings` 디렉토리에 저장합니다. 파일의 이름은 무작위로 정해지기 때문에 이전 버전에서 사용된 고정된 이름보다 감지하기가 더 어려워졌습니다.

OS 지원 – Zeus 2.0은 이제 Vista와 Windows 7에서 실행됩니다. 이전 버전은 실행을 시도하면 그냥 다운됐지만, 새 버전은 최신 Microsoft 데스크탑 운영체제에서 성공적으로 작동할 수 있습니다. Zeus 2.0은 해당 OS의 64비트 버전에서도 작동합니다.

초기 감염 경로 – Zeus의 이전 버전과 새 버전이 배포되는 방법은 거의 차이가 없습니다. 감염 방법은 기회주의적입니다. 새로운 취약점이 발견되면, 사이버 범죄자들은 그것을 악용하여 새로운 컴퓨터를 감염시킴으로써 기존 Zeus 봇넷을 확장하려 할 것입니다. Zeus는 지하 포럼에서 봇넷 생성 키트로 판매되기 때문에 여러 다양한 집단과 개인에 의해 사용되며, 각 개인과 단체는 서로 다른 방법을 사용하여 Zeus를 배포할 수 있습니다. 올해 목격된 배포 방법으로는 Zeus 봇이 들어있는 .zip 첨부파일과 .zip 또는 .exe 파일로 연결되는 링크가 포함된 이메일과, Zeus를 설치하는 공격 팩이 포함된 사이트로 연결되는 링크가 수록된 이메일 그리고 /Launch 공격 및 기타 취약점을 사용하는 .pdf 첨부파일 등이 있었습니다. 하지만 이 방법이 전부는 물론 아닙니다. 공격자는 계속하여 Zeus를 포함한 모든 악성코드를 최대한 많은 기기에 심어서 금전적인 이득을 취득하기 위한 더 창의적인 방법을 개발하고 사용할 것입니다.

Zeus로부터 스스로를 보호하기

구체적으로 Zeus를 예방하기 위해 취해야 할 특별한 조치는 없습니다. 안전한 인터넷 습관은 컴퓨터 사용자를 모든 악성코드 감염으로부터 보호해줄 것입니다.

PC 안전

- 관리자가 아닌 사용자 권한으로 실행합니다. 그래도 Zeus는 PC를 감염시킬 수 있지만, 잠재적인 피해는 최소화되고 감염은 치료하기가 더 쉬울 것입니다.
- 컴퓨터를 최신 패치로 계속 업데이트합니다. 이렇게 하면 PC에서 실행될 수 있는 악성코드의 양이 제한되고 사용 가능한 공격 경로도 제한됩니다. 특히 운영체제, 오피스 및 문서 소프트웨어와 웹브라우저 및 플러그인에 대한 업데이트에 주의를 기울이십시오.
- 바이러스 백신(AV) 소프트웨어를 설치하고 최신 상태로 유지합니다. AV 소프트웨어는 모든 악성코드 위협으로부터 보호해 주지는 않지만, 도움이 됩니다.

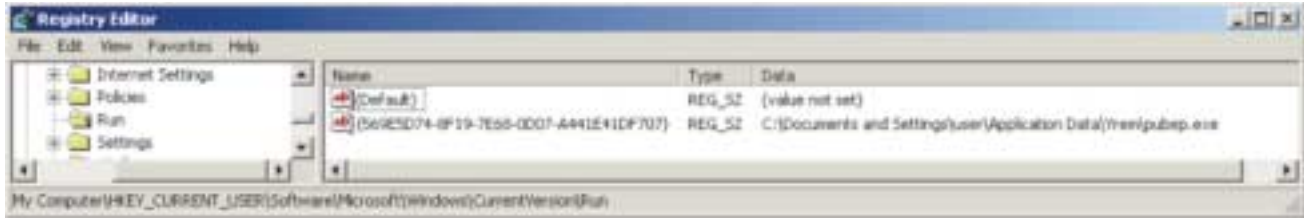
이메일 및 메시지 안전

- 이메일 첨부파일은 매우 주의해야 합니다. 첨부파일이 아는 사람에게 온 것이라도 그것이 실제로 그 사람이 보낸 것인지 확인해야 합다. 이메일이 그가 늘 사용하는 이메일 주소에서 보낸 것인지 확인합니다.
- 이메일에 포함된 링크에도 주의해야 합니다. 많은 피싱 공격은 악성 사이트로 연결되는 링크가 수록된 합법적으로 보이는 이메일을 사용합니다. 은행에서 이메일이 왔다면 브라우저의 즐겨찾기를 사용하여 직접 은행의 사이트로 가서 로그인합니다. 이 주의사항은 인스턴트 메신저 서비스나 소셜 네트워킹 사이트에서 수신한 메시지에도 해당됩니다.

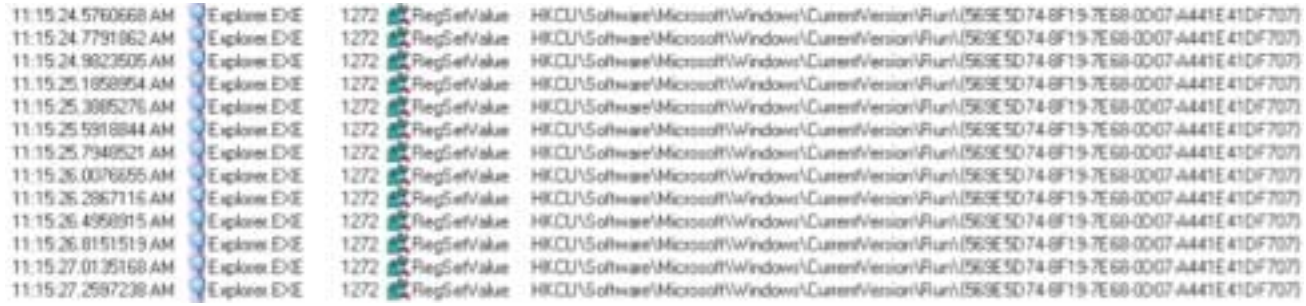
감염의 징후

Zeus 감염이 의심될 때는 다음과 같은 징후를 살펴봐야 합니다.

사용자의 Application Data 디렉토리에 있는 파일을 지시하는 GUID 형식의 이름을 가진 HKCU\Software\Microsoft\Windows\CurrentVersion\Run 레지스트리 키 안에 있는 항목. 이 항목은 예를 들면 다음과 같습니다.



이 레지스트리 키는 모든 삭제 시도를 무력화하기 위해 끊임없이 작성됩니다. 키를 삭제하면 즉시 대체됩니다. 이런 움직임은 Microsoft의 프로세스 모니터 도구를 사용하여 확인할 수 있습니다. 이 예에서는 Explorer.exe 프로세스가 이 레지스트리 값을 계속 재작성하고 있습니다.



컴퓨터를 안전 모드로 재부팅한 후 레지스트리 항목과 EXE 파일 자체를 삭제하면 Zeus가 제거되지만, 그렇다 하더라도 악성코드에 오염되었던 컴퓨터는 다시 설치하거나 이미지를 사용하여 이전 상태로 복원할 것을 권장합니다. 왜냐하면, 컴퓨터에 다른 어떤 악성코드가 잠복해 있는 지 알 수 없고 Zeus를 삭제해도 설치된 악성코드 에코시스템의 일부만 제거될 수 있기 때문입니다.

BlackHat 검색 엔진 중독

BlackHat 검색 엔진 중독(Poisoning)은 원래 스패머들이 자신의 검색 결과가 검색 엔진에서 고순위로 검색되도록 함으로써 광고 수익을 벌기 위해 사용하던 기법입니다. 나중에 다른 사이버 범죄자들은 이 기법을 악성코드 감염을 확산시키는 데 사용했습니다. 이들은 종종 주요 뉴스 사건을 악용하여 악성 링크가 여러 검색 엔진에서 검색 결과 페이지의 맨 위에 오르도록 할 수 있습니다.

소기의 목적을 달성하기 위해, 사이버 범죄자들은 검색 엔진과 소셜 네트워크 사이트의 인기 토픽을 모니터링합니다. 예를 들면 중대 뉴스 사건 발생 시에 새로운 토픽의 검색 순위가 빠르게 상승하면, 공격자는 기본 SEO(검색 엔진 최적화) 기법을 사용하여 관련 검색에 대해 자신의 링크가 결과 페이지의 맨 위에 오르도록 합니다. 이 프로세스는 대부분 자동화되어 있기 때문에, 때로는 주요 사건에 대한 실제 뉴스 보도가 많아지기도 전에 해당 악성 링크가 검색 엔진 결과의 맨 위에 등장하기도 합니다.

악성 링크 자체는 일반적으로 몇 단계의 난독화 속에 은폐되어 있습니다. 많은 경우 링크는 제목 안에 검색어가 들어 있는 PHP 페이지로 연결되고(SEO 기법의 하나), 페이지를 생성하는 코드는 HTTP Referrer를 검사하여 그것이 유효한 검색 엔진에서 온 것인지 확인합니다. 이렇게 하는 이유는 웹 크롤러와 악성코드 분석가를 방해하기 위해서입니다. 일단 웹 브라우저가 검색 엔진에서 이동해 온 것임이 확인되면, 다른 리디렉션 기법이 사용됩니다.

이런 기법으로는 난독화되거나 뒤범벅된 JavaScript 코드나, 임베드된 Adobe Flash 파일이나, 심지어는 다른 페이지로 연결되는 링크가 포함된 PDF 문서 등이 있습니다.

이렇게 하는 이유는 많은 바이러스 백업 업체가 사용하는 악성코드 크롤러 같은 자동화된 도구를 사용하여 링크를 추적하는 것을 어렵게 만들기 위해서입니다. 최고 다섯 단계 이상의 리디렉션 후에, 사용자의 브라우저는 브라우저 버전과 사용 가능한 플러그인을 확인한 후 악성 페이로드를 전달하는 공격 툴킷이 들어있는 페이지로 연결됩니다. 때로는 웹 페이지에 사용자의 PC에서 바이러스가 발견되었으니 악성 바이러스 백신 제품을 설치하라고 종용하는 허위 경고가 들어있습니다.

웹서핑을 할 때에는 검색 결과에서 클릭하는 링크에도 주의를 기울여 이런 위협으로부터 스스로를 보호해야 합니다. 구체적인 내용을 검색하다가 악성 바이러스 백신 페이지로 이동하게 된다면, 소프트웨어를 설치하지 마십시오. 링크의 도메인명이 찾는 내용과 전혀 관련이 없으면 클릭하지 마십시오. 많은 합법적인 웹사이트가 해커의 공격을 당해 BlackHat SEO 캠페인에 악용된 경우는 여러 차례 확인된 바 있습니다.

악성 바이러스 백신 소프트웨어

악성 AV, 허위 AV 및 허위 안티스파이웨어(Fraudware). 스스로 바이러스 백신 솔루션이라고 주장하지만 실제로는 아무 것도 하지 않는 소프트웨어를 지칭하는 이름은 여러 가지입니다. 이런 제품은 하드 디스크를 스캔하고 악성코드를 발견한 적하고, 60 달러 이상을 지불하면 발견된 바이러스를 제거할 수 있으니 신용카드 정보를 알려달라고 합니다. 물론 일단 돈을 내고 난 후에 일어나는 일은 악성 AV 소프트웨어가 허위 바이러스를 더 이상 신고하지 않는다는 것뿐입니다.

악성 AV 소프트웨어는 몇 년 전부터 기승을 부렸습니다. 2009년과 2010년에 새로웠던 것은 BlackHat SEO 기법이 이런 소프트웨어를 배포하는 데 사용되었다는 점입니다. 무엇이든 웹 검색을 하고 링크를 클릭하고 PC를 감염시키는 바이러스가 있다고 알리는 페이지로 이동하는 일은 쉽게 일어날 수 있습니다.

이 때 해당 소프트웨어를 다운로드하고 실행하면 PC를 사용할 수 없게 됩니다. 몇 초마다 가짜 바이러스에 대한 또 다른 허위 경고가 표시됩니다. 작업 표시줄에는 팝업 풍선이 표시됩니다. 악성 AV 소프트웨어를 삭제하거나 돈을 결제할 때까지 웹 서핑은 불가능해집니다.

스팸 – 인터넷의 사칭범

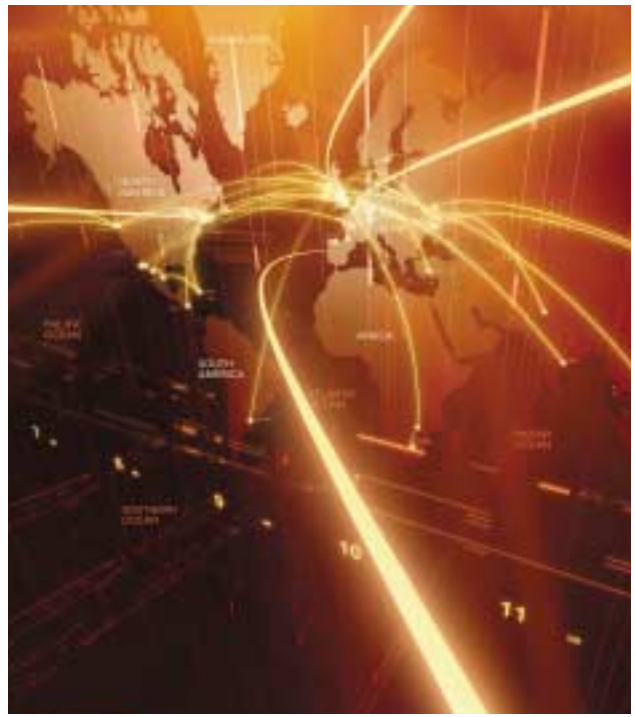
.cn에서 .ru로 이동한 스패머 도메인

아래 표에는 스팸에 가장 많이 사용된 5대 최상위 도메인(TLD)이 월별로 나와 있습니다. 이 표에는 실제로 스팸 컨텐츠를 호스팅하는 URL만 포함되었습니다.

순위	2010년 1월	2010년 2월	2010년 3월	2010년 4월	2010년 5월	2010년 6월
1.	com	ru (러시아)	ru (러시아)	com	ru (러시아)	ru (러시아)
2.	cn (중국)	com	com	ru (러시아)	com	com
3.	net	net	net	net	de (독일)	de (독일)
4.	ru (러시아)	cn (중국)	cn (중국)	de (독일)	net	net
5.	info	info	biz	cn (중국)	org	org

표 4: 실제 스팸 컨텐츠를 가장 많이 호스팅한 최상위 도메인, 2010년 상반기

한 가지 놀라운 점은 중국(**.cn**)의 쇠퇴입니다. 1월에 2위로 시작한 후, 중국의 순위는 매달 떨어졌습니다. 2010년 6월에 중국은 75위에 랭크되었습니다. 이전 년도의 데이터를 다시 살펴보면 이런 추세는 더욱 의아심을 자아냅니다.



지난 몇 년 동안 중국 도메인(.cn)은 스패머들이 가장 즐겨 쓰는 도메인이었습니다. 그러나, 중국이 2009년 12월부터 .cn 도메인 등록 규칙을 강화하자(http://www.cnnic.net.cn/html/Dir/2009/12/12/5750.htm 참조) 스패머들은 .cn 도메인을 포기하고 새로운 방향으로 옮겨간 것으로 보입니다. 중국 NIC가 문을 걸어 잠그기 전에는 스패머들이 이미 등록된 도메인 풀을 계속 이용했던 것으로 보입니다. 6주 후에 도메인 풀은 갑자기 고갈되었습니다. 그 후에는 움직임이 중국에서 러시아 쪽으로 옮겨갔습니다. 아래 그래프에는 스패머들이 지난 18개월 동안 사용한 최상위 도메인(TLD)이 월별로 나와있습니다.

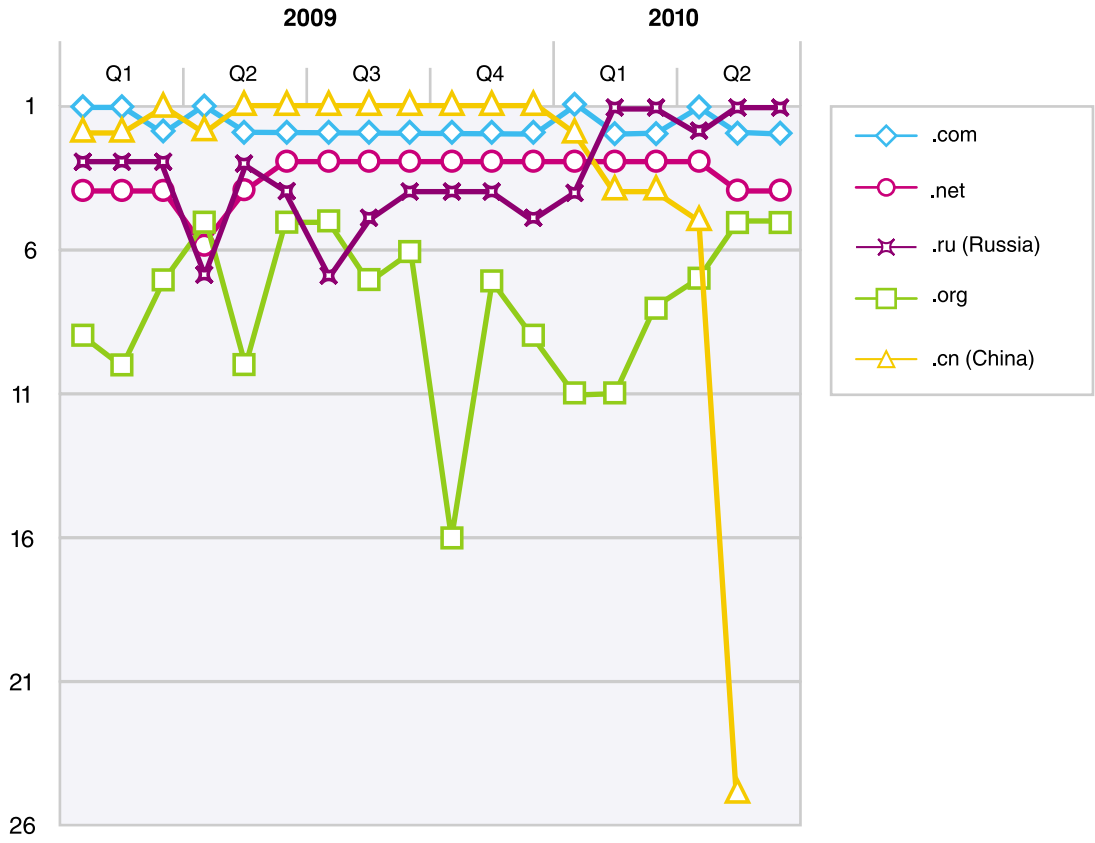


그림 15: 스팸 URL에 사용된 최상위 도메인의 기간별 추이, 2009년 1분기~2010년 2분기

2010년 4월 1일에는 러시아 NIC도 자국의 신규 도메인 등록 규칙을 강화했습니다(자세한 사항은 http://www.nic.ru/dns/service/en/faq_identification.html#q9 참조). 그러나 스패머들은 **.ru** 도메인을 계속 선택하고 있습니다. 2010년 6월 현재 **.ru**는 여전히 스팸에 가장 많이 사용되는 최상위 도메인입니다. 이 추세가 얼마나 오래 지속되는지를 지켜보는 것도 흥미로울 것입니다. 하지만 그 다음에는 어떻게 될까요? 스패머들은 도메인 등록이 용이한 다른 국가를 선택할까요? 아니면 다른 스패머들이 이미 하고 있는 것처럼 자체적인 도메인을 등록할 필요 없이 웹 호스팅 서비스를 통해 악성코드를 제공하는 데 초점을 맞출까요?

도메인 등록을 개선하기 위해 할 수 있는 일

스팸 컨텐츠를 호스팅하는 데 사용할 도메인의 대량 등록을 방지하는 좋은 방법은 기업에게 등록 증명서를 요청하거나 개인에게 신분 증명을 요청(증빙 확인 포함)하는

것입니다. 그러면 도메인을 스팸용으로 남용하는 사람들을 가려낼 수 있습니다. 중국은 2009년 12월부터 이런 증명서를 요청함으로써 큰 효과를 얻었습니다. 러시아에서는 4월 1일부터 중국과 유사한 새로운 요건이 발효되었지만, 지금까지는 중국만큼 철저하게 집행되지 않은 것으로 보입니다.

등록은 국가마다 대응하는 방법이 다른 법적인 문제입니다. 스패머들에게 길을 열어주는 느슨한 등록 기관이 어딘가에 항상 존재할 가능성은 큽니다. 도메인 등록은 스팸 컨텐츠를 호스팅하는 한 가지 방법에 불과하기도 합니다. 그 밖에 Google(googlegroups.com)이나 Microsoft(livefilestore.com) 같은 대기업을 포함한 이미지 호스터나 기타 컨텐츠 호스터를 사용하는 방법도 있습니다. 스팸 URL에 가장 많이 사용되는 도메인 부분을 참조하십시오.

대역폭과 무관: 스팸의 바이트 크기 크게 증가

스팸의 평균 크기(바이트)가 가장 크게 변한 것은 2007년 말이었으며, 이는 이미지 기반 스팸이 감소한 시기와 일치했습니다. 2008년에 바이트 크기는 그 해 말에 McColo 단속이 있을 때까지 조금씩 증가하기 시작했습니다. 2009년 여름에 이미지 기반 스팸이 다시 증가하자, 평균 크기는 1년 반 만에 처음으로 5 킬로바이트(KB)를 초과했습니다. 2009년 4분기에 스팸의 평균 크기는 다시 4 KB 미만으로 감소했습니다. 아래 그래프에는 스팸의 평균 바이트 크기와 이미지 기반 스팸의 비율이 2009년 말까지 대조되어 있습니다.

McColo 폐쇄

2008년 11월에 캘리포니아의 웹 호스트 회사였던 McColo가 폐쇄된 이후, 스팸의 양은 이전 수준의 약 25%로 감소했습니다. 단속 후에 관찰된 스팸의 양과 국가별 분포의 갑작스럽고 극단적인 변화는 McColo가 전세계 모든 스팸 봇(bot)의 근거지였음을 입증했습니다. McColo의 폐쇄와 그 결과에 대한 자세한 사항은 IBM Security 2008년 및 2009년 X-Force 동향 및 리스크 보고서에 나와있습니다.

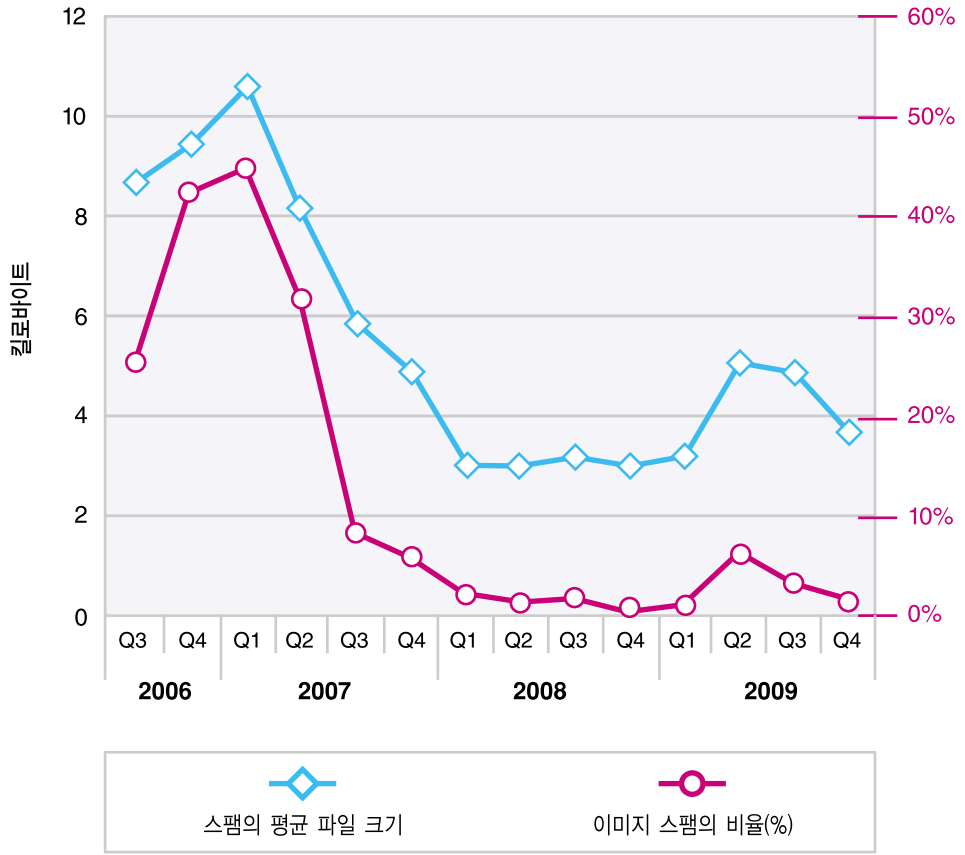


그림 16: 스팸의 평균 바이트 크기와 이미지 스팸의 비율 비교, 2006년 3분기~2009년 4분기

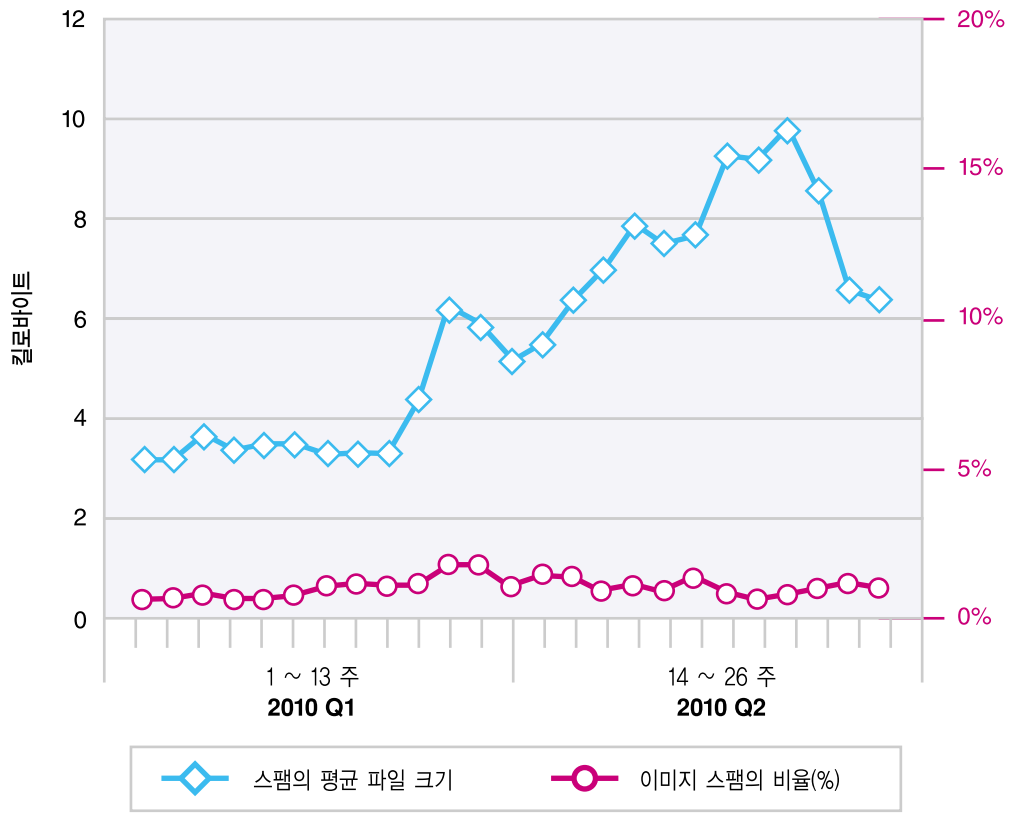


그림 17: 스팸의 평균 바이트 크기와 이미지 스팸의 비율 비교, 2010년 상반기

두 그래프는 모두 완벽히 평행으로 움직였습니다. 하지만 이 같은 추세는 3월 중순부터 크게 바뀌었습니다. 며칠 안에 스팸의 평균 크기는 2배로 커졌지만, 이미지 기반 스팸의 비율은 변화가 없었습니다. 그 후 몇 주 동안 평균 바이트 크기는 6월 초까지 계속 증가하여 평균 크기가 거의 10KB에 육박했습니다. 6월 중에는 크기가 약 6.5KB로 줄어들었지만, 이렇게 줄어든 크기도 이 무작위 텍스트 스팸 공격이 시작되었을 때보다는 2배나 큰 것이었습니다. 이미지 기반 스팸의 비율(%)은 이 기간 내내 일정했습니다.

스팸을 보면, 인터넷에서 무작위로 선택된 큰 텍스트 조각을 볼 수 있습니다. 무작위 텍스트는 스팸이 특히 텍스트 기반 스팸 분석 모듈에게 더 합법적으로 보이도록 하기 위해 스패머들이 사용하는 오래된 수법입니다. 그러나, 최근의 스팸 방지 기법은 이로 인해 문제를 겪지 않습니다. 그렇다면 스패머들이 왜 이 오래된 기법을 다시 사용하고 있을까요? 어쩌면 대량의 무작위 텍스트가 베이지안(Bayesian) 분류자들을 혼란시키기를 바라고 그러는 지도 모릅니다. 특히, 혼자서 배운(Self-Trained) 베이지안 분류자들은 비즈니스 이외의 상황에서 사용되므로, 이런 스팸 공격은 이 같은 비즈니스 이외의 사용자를 공략하기 위한 것일 수 있습니다.

스팸에 대한 추가 사례와 기법에 대해서는 현재 동향 부분에서 확인할 수 있습니다.

피싱 – 속고 계십니까?

2009년에 금융 기관은 압도적으로 가장 많은 피싱 이메일의 표적이 되었습니다. 피싱 이메일의 60% 이상은 금융 기관을 대상으로 한 것이었습니다. 2010년 상반기에는 피싱 이메일의 표적 중 49.1%가 금융 기관이었습니다. 전체 피싱 이메일의 표적 중 신용카드는 27.9%, 정부 기관은 11.2%, 온라인 결제 기관은 5.5% 그리고 경매 사이트는 4.6%를 차지했습니다. 나머지 1.7%의 피싱 표적에는 통신 서비스 및 온라인 쇼핑몰 등의 기타 산업이 포함되었습니다.

새로 집중되는 피싱 기법

71 페이지의 '**웹 애플리케이션 위협 및 취약점**'에 나와있는 비율(%)은 한 해 동안 있었던 표적 분포가 크게 바뀌었음을 보여주며, 94 페이지의 '**스팸 URL에 가장 많이 사용되는 도메인**'에 나와있는 비율은 공격자가 신뢰 받는 웹사이트의 좋은 평판을 악용하여 최종 사용자의 경계를 늦추고 보호 기술이 공격 시도를 감지하지 못하도록 하는 데 점점 많은 노력을 집중하고 있음을 보여주고 있습니다.

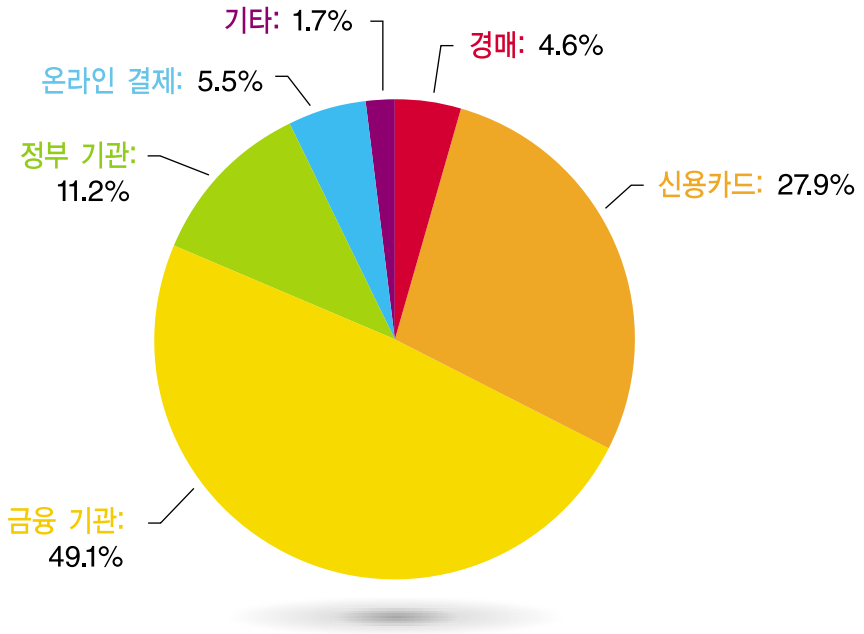


그림 18: 피싱 표적의 산업별 분석, 2010년 상반기

지난 18개월 동안 금융 기관은 압도적으로 많은 피싱 이메일의 표적이 되었습니다. 2009년 상반기에는 온라인 결제 기관이 피싱 이메일에서 큰 비중을 차지했습니다. 그러나, 2009년 하반기에는 정부 기관(주로 미국 세무 관련 웹사이트), 신용카드 및 경매 사이트를 표적으로 한 피싱 이메일이 더 많이 목격되었습니다.

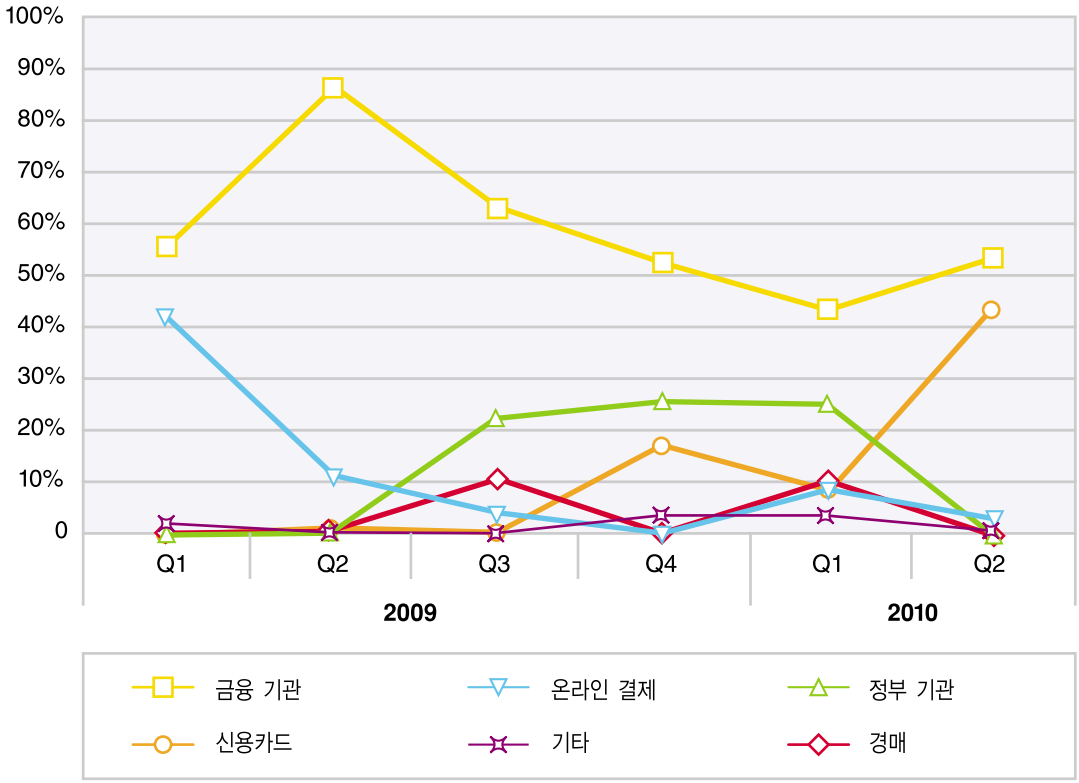


그림 19: 피싱 표적의 산업별 분석, 2009년 1분기~2010년 2분기

동시에, 온라인 결제 기관을 표적으로 한 피싱의 비율(%)은 감소했습니다. 2010년 1사분기에 금융기관과 신용카드는 또 한 번 비중이 감소한 반면, 경매 사이트는 비중이 증가했습니다. 2010년 2분기로 넘어가자 모든 산업을 표적으로 한 피싱이 감소하고 금융기관과 신용카드에 다시 한 번 초점이 집중되는 동향이 목격되기 시작하여 이 두 산업은 전체 피싱 이메일의 96% 이상을 차지하게 되었습니다.

피싱 공격자들이 정부 기관(이 경우에는 미국 세무 관련 웹사이트)을 사칭하는 것을 멈추고 이제 은행과 신용카드에 초점을 맞추고 있는 이유는 무엇일까요? 한 가지 이유는 이 세무 관련 웹사이트를 9달 동안이나 공략한 결과 이익이 감소함에 따라 이제 공격자들은 기존에 효과가 입증된 신용카드 및 은행을 공략하는 데 다시 집중하고 있기 때문일 수 있습니다.

미국 소재 은행을 표적으로 한 금융 피싱

금융 기관이 계속하여 피싱 공격자들의 집중적인 공략 대상이 되고 있는 가운데, 이 공격 활동이 두드러지게 나타나고 있는 지역을 더 긴밀히 살펴볼 가치가 있을 것입니다. 2010년 상반기의 모든 금융 피싱 표적 중 3분의 2 이상은 북아메리카에 위치해 있습니다. 나머지 32%는 유럽에 있습니다.

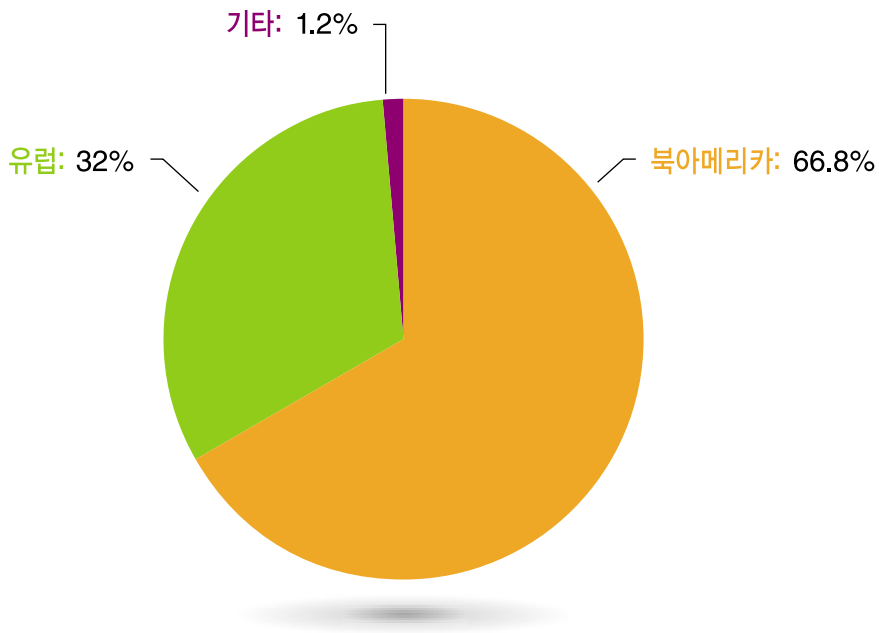


그림 20: 금융 피싱 표적의 지역별 분포, 2010년 상반기

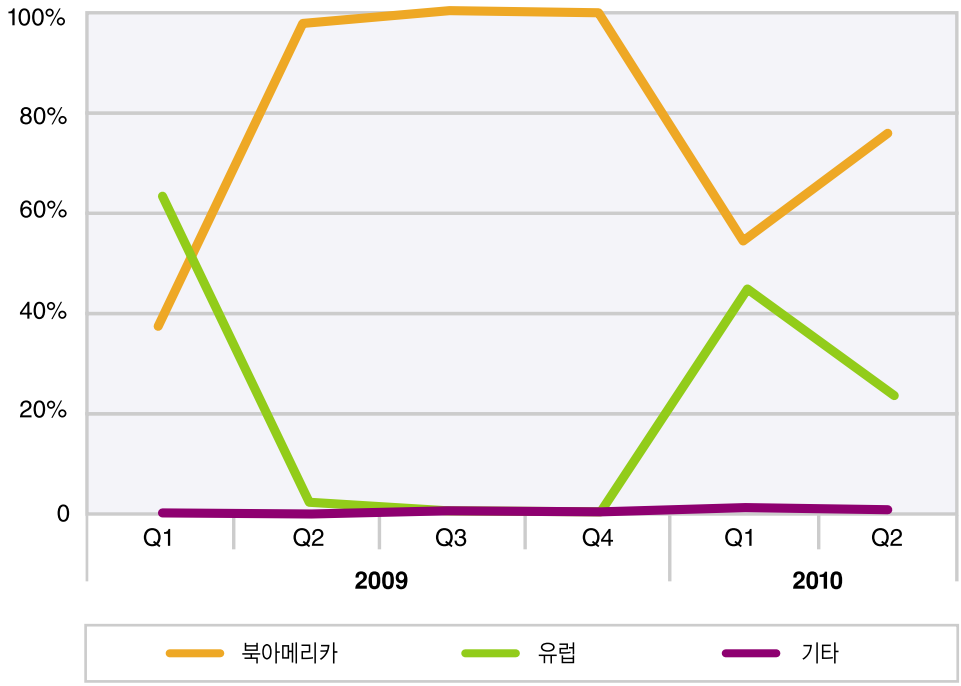


그림 21: 금융 피싱 표적의 지역별 분포, 2009년 1분기~2010년 2분기

그러나, 더 짧은 기간을 더 자세히 살펴보면 더 많은 변화가 뚜렷하게 나타납니다. 그래프에는 2009년부터 2010년 상반기까지 일어난 지리적 분포의 변화가 나와있습니다. 2009년 2, 3, 4분기에는 미국 은행을 대상으로 한 금융 피싱 이메일이 압도적으로 많았지만(95% 이상), 2010년 1분기에는 유럽의 금융기관을 대상으로 한 금융 피싱 이메일이 45%에 육박했습니다. 2분기에는 유럽이 다시 24%로 감소했습니다. 그렇다면 피싱 공격자들이 2010년 1분기에 유럽으로 고개를 돌렸다가 다시 미국 쪽으로 선회한 이유는 무엇이었을까요? 1분기에 유럽은 금융 위기로부터 회복하는 모습을 보였습니다. 반면, 2분기에 그리스 및 기타 몇몇 유럽 국가의 예산 위기는 다시 유럽의 금융 위기를 초래했습니다.

최근 피싱 동향에 대해서는 본 보고서의 뒷부분에서 계속 논의할 것입니다.

향후 토픽 – 2010년 이후

IPv6의 도입 – IPv4 주소가 고갈되고 있는 지금 우리는 준비가 되어 있는가?

구세대 인터넷인 IPv4에서 사용되는 주소와 라우팅 테이블은 계속 폭증해 왔습니다. 필요한 주소의 수는 가용 주소의 한계에 다다르고 있으며, IANA(Internet Assigned Numbers Authority)의 가용 주소는 2011년 도중에 그리고 RIR(Regional Internet Registries)은 그 후에 고갈될 것으로 예상됩니다. 하지만 이렇게 주소가 고갈될 때 주소 암시장이 형성되고 주소가 상품으로서 거래될 수 있다는 우려는 어느 정도 존재하는 가운데 종국에는 급정거가 아닌 연착이 이루어질 것입니다. . 미사용 공간의 회수 역시 해답이 되지 못합니다. 왜냐하면, 루트 조각화로 인해 라우터 테이블이 폭증하여 라우터 용량도 한계에 다다랐기 때문입니다. 주소 회수 및 재할당은 라우팅 테이블 포화 문제를 악화시킬 뿐이며, 주소 고갈 문제를 크게 해소시켜주지는 못합니다. 라우터는 대만원입니다.

2007년 1월부터 2010년 5월까지의 IPv4 및 IPv6 BGP 공시에 관한 이 자료는 APNIC(Asia Pacific Network Information Center)가 수집하고 CIDR-Report 프로젝트 (www.cider-report.org)의 맞춤 그래프 생성기에 의해 생성된 자료에서 도출한 것입니다. APNIC는 2003년 이후의 IPv6 통계 자료와 1998년 이후의 IPv4 통계 자료를 보유하고 있습니다.

IPv6의 확장 및 도입

신세대 인터넷인 IPv6은 여러 해 전부터 있었으며, 유럽과 아시아뿐만 아니라, 미국 등지에서도 계속 확장되어 왔습니다. IPv6가 라우팅할 수 있는 네트워크의 수는 이미 여러 해 전에 라우팅이 가능한 IPv4 주소의 수를 넘어섰지만, 라우팅 테이블 포화율은 훨씬 낮았습니다. 2009년에는 IPv6가 정부와 방위 산업에 더욱 많이 도입되었습니다. 현재 IPv6의 용량은 이전의 IPv4 인터넷 전체를 감당할 수 있는 용량의 몇 배에 달하며, 한계에 다다르려면 아직 한참 남았습니다.

아래의 왼쪽의 IPv4와 오른쪽의 두 그래프 IPv6에는 BGP(Border Gateway Protocol)를 통해 공시되는 코어 인터넷 라우터에 있는 루트의 수가 나와 있습니다. 이 자료는 각 프로토콜에서 루트의 수가 계속 확장하고 있음을 확인시켜주고 있습니다.

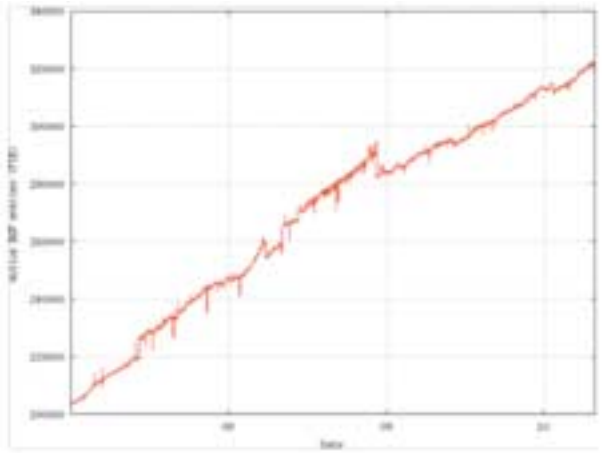


그림 22: IPv4 BGP 공시, 2007년 1월 ~ 2010년 5월.
자료 제공: APNIC(Asia Pacific Network INformation Center)/ CIDR-Report 프로젝트

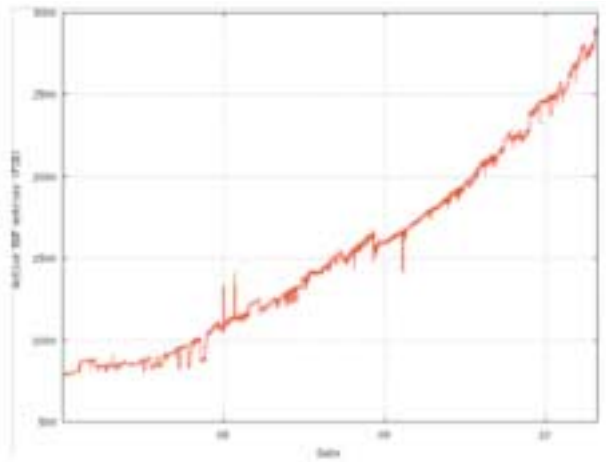


그림 23: IPv6 BGP 공시, 2007년 1월 ~ 2010년 5월.
자료 제공: APNIC(Asia Pacific Network INformation Center)/ CIDR-Report 프로젝트

하지만, 세로 축의 숫자를 자세히 보십시오. 현재 코어 인터넷에 공시된 IPv4 루트는 30만이 넘지만, 공시된 IPv6 루트는 3,000개가 안 됩니다. IPv6가 필요로 하는 루트의 수는 100분의 1도 안 되지만, 이렇게 공시된 IPv6 루트가 라우팅하는 전체 /48 네트워크 주소의 수는 단일 IPv4 호스트 주소의 수만큼 많습니다. 공시된 각각의 모든 IPv4 주소는 거대한 IPv6 네트워크 전체를 라우터 안에 있는 루트 수의 100분의 1도 안 되는 비용으로 가질 수 있습니다. 각 IPv6 네트워크의 용량으로 인해, IPv4 주소의 수는 하나의 /48 IPv6 네트워크와 비교하는 것조차도 의미가 없습니다. IPv4 루트 수의 확장 속도는 약간 둔화되고 있는 것으로 보이는 한편, IPv6 루트와 공시된 네트워크 수의 확장 속도는 더 빨라지고 있는 것으로 보입니다.

모든 최신 운영체제는 IPv6를 지원하며, 특히 Windows Vista, Windows 7, Mac OS/X, 및 Linux가 존재하는 대부분의 네트워크에는 이미 IPv6가 있습니다. 안타깝게도 사람들은 아직도 IPv6를 외면하면서 단지 미래에 필요하게 될 것으로만 생각합니다. 대부분의 네트워크는 의도하지 않고도 이미 IPv6를 기본적으로 도입했습니다. 이런 추세는 지난 1년 동안 Vista 및 Windows 7를 통해 점점 빨리 확산되어 왔으며, 앞으로도 계속될 것입니다. 이를 인식하지 못하고 있거나 일부러 무시하는 운영자는 IPv6가 인프라 전체에 도입될 때 위험에 처하게 됩니다.

케이블 및 초고속 인터넷 제공업체인 Comcast는 자사 기기를 관리하는 데 사용해 온 10.*.*.* 사설 주소 공간의 주소가 완전히 고갈된 이후 수 년 동안 IPv6를 사용하여 내부적으로 기기를 관리해 왔습니다. 이 회사는 이제 IPv6를 자사의 최종 사용자 및 고객에게 제공하는 베타 테스트 프로그램을 개설했습니다. Comcast에는 IPv6 도입을 추적하기 위한 "IPv6 Adoption Monitor(채택 모니터)"도 있습니다. 자세한 사항은 다음 링크를 참조하십시오.
http://ipv6monitor.comcast.net/

유럽, 아시아 및 호주에서 인기가 높은 ISP인 Hurricane Electric은 일련의 IPv6 도구 및 기능을 점점 많이 제공하고 있으며, 무료 터널 브로커 서비스인 www.tunnelbroker.net은 무료 IPv6 연결을 제공합니다. 이 사이트에는 (기타 여러 IPv4 및 IPv6 통계와 함께) IPv4 주소 공간이 고갈될 때까지 남은 일수를 카운트다운하는 "둠스데이 시계"가 있습니다. IPv6 지식 및 네트워킹에 관한 개인과 단체의 자가 교육 및 평가를 위한 무료 '인증서'도 있습니다.

Google과 YouTube 같은 여러 유명 웹사이트는 이제 IPv6를 완벽 지원합니다. Google은 최근에 미국이 이미 IPv6를 지원하고 구축된 자동 전환 터널 중 하나를 통해 자동으로 연결하는 Apple Mac 컴퓨터와 무선 액세스 지점에 크게 힘입어 세계 5위 IPv6 도입 국가에 올랐다고 보도했습니다.

Windows Vista와 Windows 7 역시 기본 IPv6를 사용할 수 없을 때 자동으로 Teredo 전환 메커니즘에 연결합니다. IPv6가 사용 가능할 때 그것을 선호하는 클라이언트 시스템의 비율(%)은 아직 적지만, 계속 증가하고 있습니다.

이 모든 것은 IPv6가 향후 몇 년 동안 계속 확장되고 이 같은 추세가 둔화되지 않을 것임을 시사합니다. 얼마 전까지만 해도 IPv6는 "차세대" IP 프로토콜이라 지칭되었습니다. 하지만 이제 IPv6는 "현세대" IP 프로토콜이고 IPv4은 "구식"이 되고 있다고 주장할 수 있습니다.

가상화 – 가상 공간으로의 통합과 이로 인한 보안 영향

가상화 기술의 중요성은 점점 커지고 있습니다. IDC의 최근 보도 자료에 따르면1, 2009년 4분기에 출고된 모든 새 서버 중 18.2%가 가상화되어 2008년 4분기의 15.2%에 비해 20% 증가했다고 합니다. 2009년 가상화 시장의 규모의 미화 152억 달러였습니다. 클라우드 컴퓨팅에 대한 관심이 증가함에 따라 가상화 솔루션에 대한 수요는 더욱 자극될 것입니다.

따라서, 가상화 기술이 보안에 미치는 영향을 이해하는 것은 점점 중요해지고 있습니다. 여기에는 다음 업체가 제공하는 가상화 제품에 대해 지난 10년 간 노출된 취약점이 분석되어 있습니다.

- Citrix
- IBM
- Linux VServer
- LxCenter
- Microsoft
- Oracle
- Parallels
- RedHat
- VMware

가상화 취약점 노출 동향

1999년부터 2009년 말까지 노출된 가상화 솔루션에 영향을 미치는 취약점의 수는 373개였습니다. 공개된 가상화 취약점 수의 변동 추이는 그림 24에 나와있습니다. 노출된 가상화 취약점이 노출된 전체 취약점 중에서 차지하는 비중은 2007년에서 2009년까지만 1%를 넘었을 정도로 적습니다.

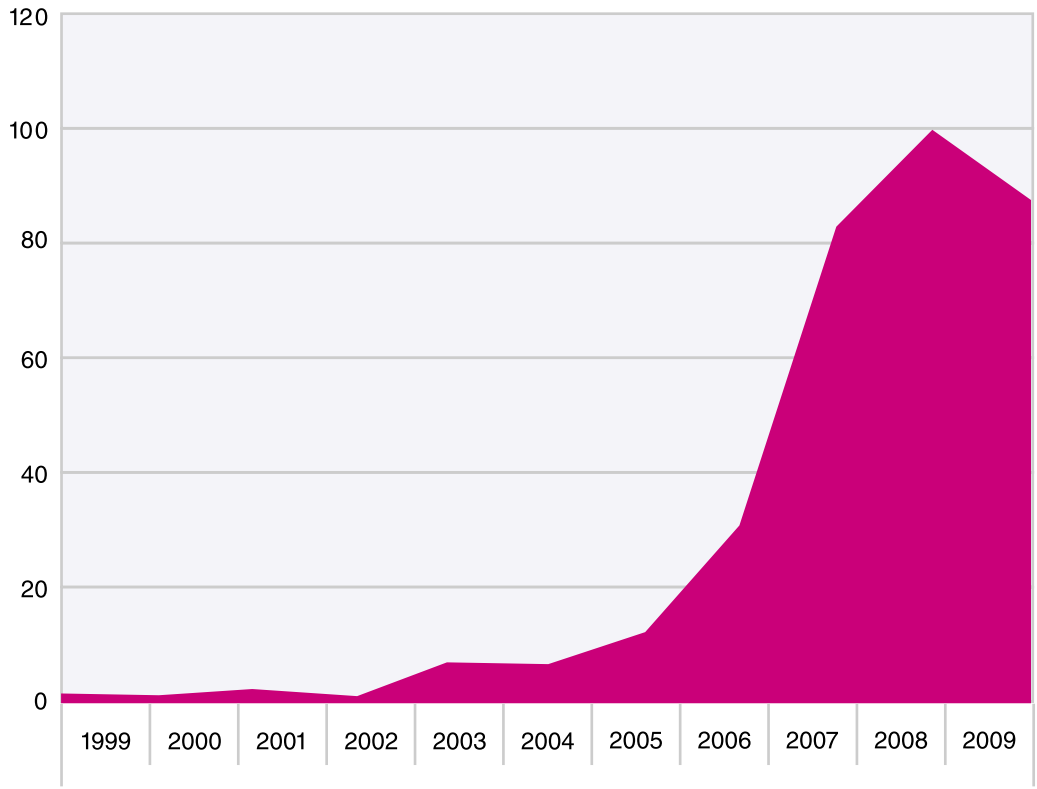


그림 24: 노출된 가상화 취약점 수의 보고 연도별 추이, 1999～2009

[1] http://www.idc.com/getdoc.jsp?containerId=prUS22316610

가상화 제품이 시장에 등장한 이후 그와 관련하여 노출된 취약점의 수는 매년 증가했을 것이라고 자연스럽게 추측할 수 있을 것입니다. 2002년부터 2008년까지는 이런 추측이 들어맞았지만, 노출된 취약점의 수는 2008년에 100개로 정점을 찍은 후 2009년에는 88개로 12% 감소했으며, 2010년에는 약간 더 감소할 추세입니다. (2010년 상반기에 노출된 가상화 취약점의 수는 39개입니다) 이런 가상화 취약점 노출 추세는 가상화 업체들이 2008년부터 보안에 더 주의를 기울여 왔거나 보안 연구원들이 더 쉬운 표적에 노력을 집중해 왔음을 시사합니다.

가상화 취약점의 위험도별 분석

그림 25에서 볼 수 있듯이, 위험도가 높음 또는 중간에 해당하는 취약점은 본 분석에 포함된 모든 해에 가상화 취약점의 절반 이상을 차지했습니다. 위험도가 높은 취약점은 2006년을 제외한 모든 해에 전체 취약점 중 3분의 1 이상을 차지했습니다. 이 추세는 2010년 상반기에도 이어졌습니다. 전체적으로, 신고된 취약점의 40%는 위험도가 높음에 해당되는 취약점이었으며, 중간은 26% 그리고 낮음은 34%였습니다. 위험도가 높은 취약점은 공격하기가 가장 쉽고 공격 대상 시스템에 대한 통제력을 완전히 넘겨주는 경향이 있으므로, 가상화 취약점은 보안에 중대한 위협이 됩니다. 이런 취약점 중 상당수는 가상화가 일반적으로 제공하는 격리 효과를 무력화하기 때문에 공격자가 이를 통해 공격한 가상 머신의 범위를 벗어난 데이터에도 접근할 수 있게 된다는 사실을 감안하면 더욱 그렇습니다.

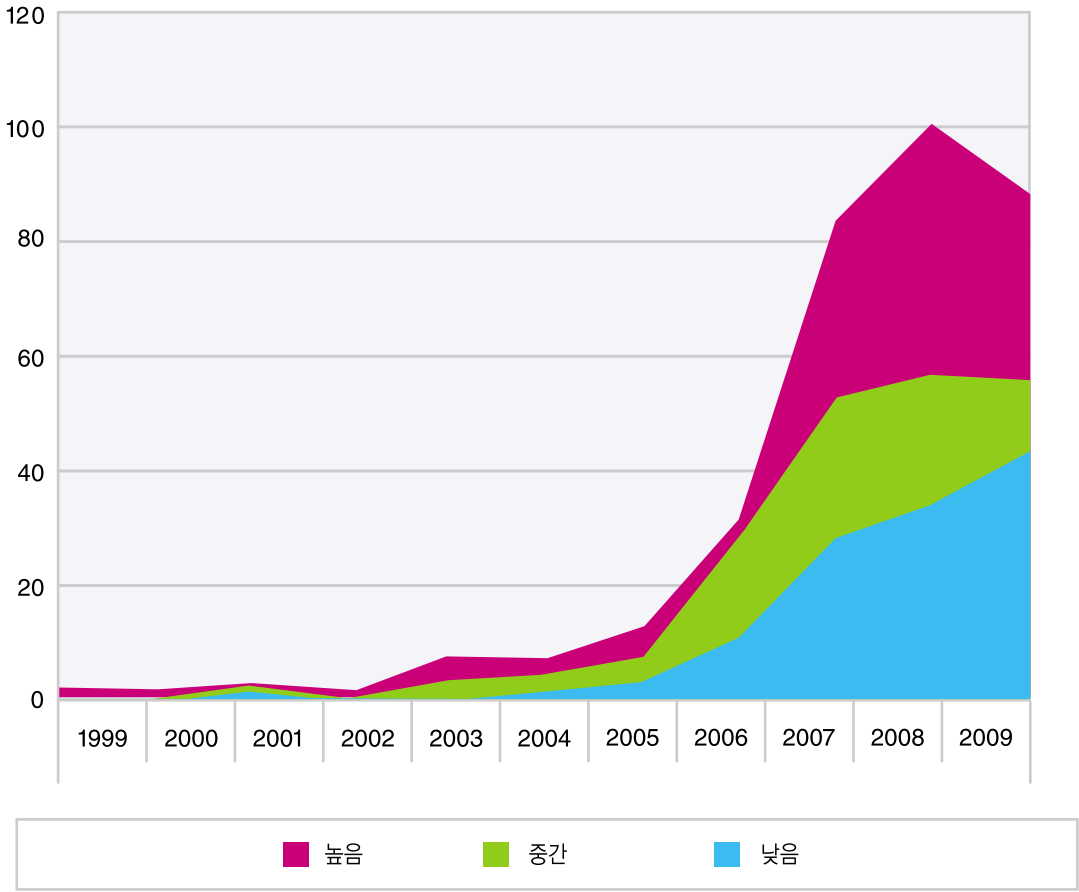


그림 25: 보고 연도별 가상화 취약점 위험도, 1999～2009

가상화 취약점의 위치별 분석

가상화 취약점의 위치(즉, 그것이 코드에서 발생하는 부분)를 이해하는 것은 중요합니다. 이는 벤더가 취약점을 쉽게 시정할 수 있는 정도에 영향을 미치기 때문입니다. 그림 26에는 가상화 제품 벤더 코드에 있는 취약점의 수가 가상화 제품에 사용된 타사 구성요소에 있는 취약점의 수와 비교되어 있습니다. 2005년 이후에 타사 구성요소에 들어있는 취약점의 수는 (2007년을 제외하고) 매년 벤더 코드에 들어있는 취약점의 수보다 많았습니다. 이 같은 추세는 벤더 코드 취약점이 20개였고 타사 구성요소가 19개였던 2010년 상반기에도 계속 이어질 뻔했습니다. 이는 가상화 벤더가 타사 구성요소를 선택할 때는 신중을 기해야 하며, 해당 구성요소의 취약점이 신고되면 신속히 업데이트할 수 있는 장치를 마련해야 함을 시사합니다.

이런 통계는 워크스테이션과 서버 제품에 대해 다르게 분석됩니다. 워크스테이션 제품에는 호스트 운영체제 위에서 실행되는 제품이 포함되며, 서버 제품에는 "기기 자체에서" 실행되는 (즉, 하이퍼바이저 자체가 운영체제의 기능을 수행하는) 제품이 포함됩니다. 워크스테이션 제품 취약점은 그래프와 반대되는 추세를 나타냅니다. 즉, 타사 구성요소에서 발생하는 비율은 24%에 불과합니다. 서버 제품 취약점은 70%가 타사 구성요소에서 발생한다는 점에서 이런 추세의 극단을 보입니다.

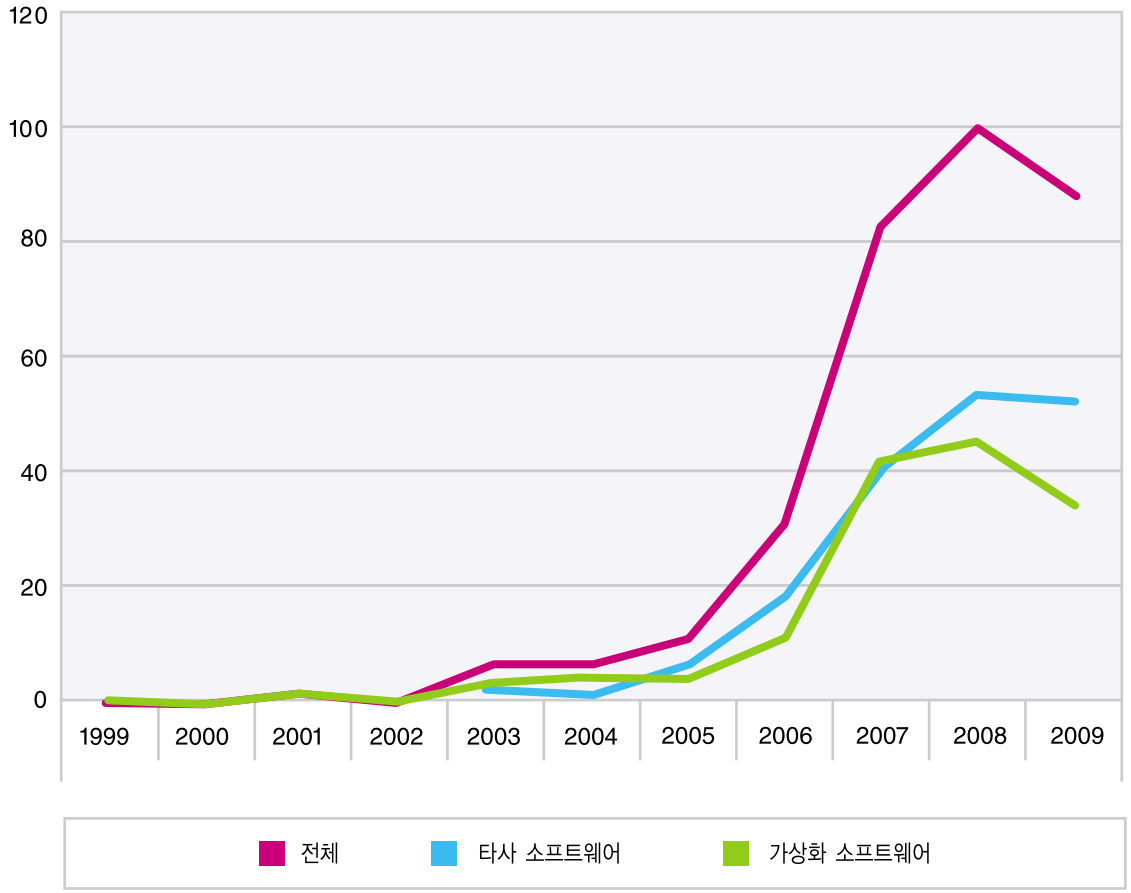


그림 26: 보고 연도별 가상화 취약점 위치, 1999 ~ 2009

가상화 취약점의 제품 유형별 분석

그림 27에는 워크스테이션 제품 취약점과 서버 제품 취약점의 추세가 비교 표시되어 있습니다. 위에서 언급한 바와 같이, 워크스테이션 제품에는 호스트 운영체제 위에서 실행되는 제품이 포함되며, 서버 제품에는 "기기 자체에서" 실행되는 (즉, 하이퍼바이저 자체가 운영체제의 기능을 수행하는) 제품이 포함됩니다. 2005년 이후 가상화 서버 제품의 취약점은 워크스테이션 제품의 취약점보다 매년 더 많았습니다. 이런 결과에는 서버 제품이 더 복합적이고 서버 제품 취약점을 파악하는 데 더 많은 초점이 집중된다는 사실이 반영된 것으로 추정됩니다.

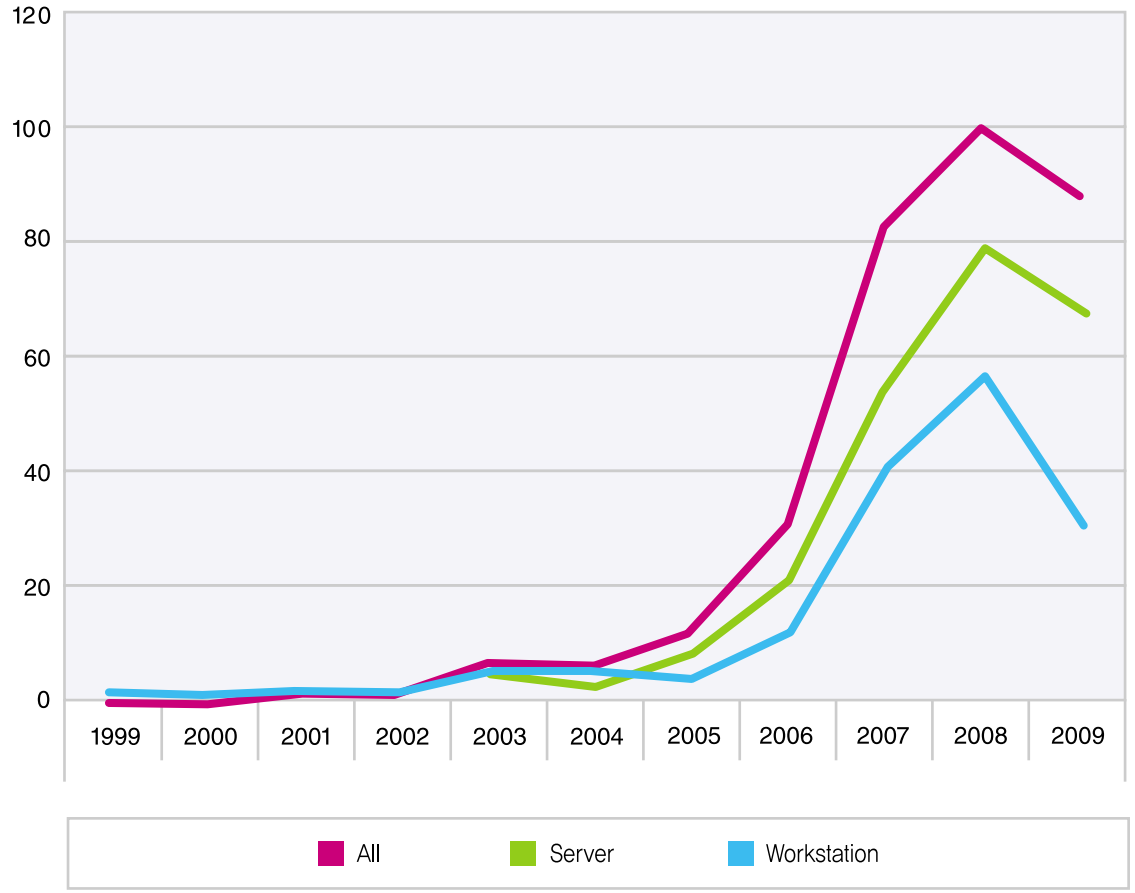


그림 27: 보고 연도별 가상화 취약점 제품 유형, 1999 ~ 2009

가상화 취약점의 취약점 유형별 분석

그림 28과 그림 29는 각각 워크스테이션 및 서버 제품 취약점의 취약점 유형별 분포를 보여주고 있습니다. 이 분석에는 가상화 시스템 코드 안에 존재하는 취약점만 포함되었습니다. (타사 구성요소의 취약점은 제외되었습니다)

정의된 취약점 유형과 각각이 워크스테이션 및 서버 제품에서 자치하는 비율(%)은 표 5에 나와 있습니다.

유형	설명	워크스테이션 비율(%)	서버 비율(%)
호스트	실행 중인 가상 머신의 개입 없이 가상화 시스템이 설치된 호스트 운영체제에 영향을 미치는 취약점	30.8%	0%
게스트	하이퍼바이저나 호스트 운영체제에 영향을 미치지 않고 게스트 가상 머신에 영향을 미치는 취약점	26.3%	15.0%
Escape to host (호스트로 탈출)	공격자가 게스트 가상 머신에서 "탈출"하여 가상화 시스템을 구동하는 호스트 운영체제를 공격하기 위해 악용할 수 있는 취약점	24.1%	0%
웹 애플리케이션	클라이언트 브라우저를 구동하는 시스템에 영향을 미치는 웹 애플리케이션(일반적으로 관리 애플리케이션)의 취약점	9.8%	10%
가상화 시스템	가상화 시스템 자체, 즉 전체 가상화된 환경에 영향을 미치나 게스트 가상 머신에서 발생하지 않는 취약점	4.5%	37.5%
Escape to hypervisor (하이퍼바이저로 탈출)	공격자가 게스트 가상 머신에서 "탈출"하여 다른 가상 머신이나 하이퍼바이저 자체를 공격하기 위해 악용할 수 있는 취약점 워크스테이션 제품의 경우, 이 취약점은 호스트 운영체제에 영향을 미치지 않습니다.	3.8%	35.0%
콘솔	맞춤 관리 콘솔에 영향을 미치는 취약점	0.8%	0%
웹 서버	가상화 시스템이 사용하는 웹 애플리케이션을 구현하는 웹 서버에 영향을 미치는 취약점	0%	2.5%

표 5: 가상화 취약점의 유형별 설명과 각 유형이 워크스테이션 및 서버 제품에서 차지하는 비율

각 취약점 유형이 미치는 영향

호스트 취약점, 웹 애플리케이션 취약점, 웹 서버 취약점 및 콘솔 취약점은 가상화 시스템에만 국한된 것이 아닙니다. 이는 전통적인 애플리케이션의 유사한 취약점과 비슷합니다. 원격 구성요소에만 영향을 미치는 취약점(웹 애플리케이션 취약점과 콘솔 취약점)은 전통적인 애플리케이션의 경우보다 더 큰 위험을 제기하지는 않습니다. 호스트 취약점과 웹 서버 취약점은 전통적인 애플리케이션이 제기하는 것과 유사한 서버 측 위험을 제기하지만, 가상화 시스템 하에서 가동되는 여러 가상 머신에 영향을 미칠 가능성도 있습니다. 게스트 머신 취약점, Escape-to-Hypervisor 취약점, Escape-to-Host 취약점 그리고 가상화 시스템 취약점은 가상화 시스템에만 국한되며, 이런 취약점이 제기하는 위험을 이해하려면 추가 분석이 요구됩니다.

게스트 머신 취약점

게스트 머신 취약점은 관련 게스트 머신에서 실행되는 애플리케이션에만 영향을 미친다는 점에서 가상화되지 않은 시스템의 호스트 취약점과 유사합니다. 이런 점에 보면 게스트 머신 취약점은 새로운 유형의 위험을 제기하지 않는다고 할 수 있습니다. 시스템 안에 존재하는 취약점은 해당 시스템에만 영향을 미칩니다.

Escape-to-Host 취약점

Escape-to-Host 취약점은 한 시스템(게스트 가상 머신)의 취약점이 네트워크를 통해 전파되지 않고도 다른 시스템(가상화 시스템의 호스트)의 보안에 영향을 미칠 수 있다는 면에서 새로운 유형의 위험을 제기합니다. 호스트 운영 체제에 대해 실시하는 취약점 진단에서는 호스트의 모든 취약점이 밝혀지지 않을 것입니다.

Escape-to-Host 취약점이 존재하면, 호스트의 리스크 프로필에는 해당 호스트에서 가동되는 가상 머신과 관련된 추가 위험이 포함됩니다. 이런 위험은 시간이 지나 가상 머신 이미지가 시작되고 정지됨에 따라 다를 수 있습니다.

Escape-to-Hypervisor 취약점

Escape-to-Hypervisor 취약점은 Escape-to-Host 취약점과 마찬가지로 네트워크를 통해 전파되지 않고도 한 시스템(게스트 가상 머신)이 다른 시스템에 영향을 미칠 수 있는 가능성을 수반합니다. 이 경우 동일한 하이퍼바이저 밑에서 가동되는 가상 머신에 제기되는 위험은 같은 하이퍼바이저 밑에서 가동되는 다른 가상 머신에 존재하는 취약점에 의해 좌우됩니다.

가상화 시스템 취약점

마지막으로, 가상화 시스템 취약점은 호스트 취약점과 비슷한 유형의 위험을 제기합니다. 이런 취약점은 가상화 시스템 자체뿐만 아니라 가상화 시스템 하에서 가동되는 게스트 머신에까지 잠재적으로 영향을 미칠 수 있습니다.

워크스테이션 제품 취약점

워크스테이션 제품 벤더 코드 취약점이 나와있는 그림 28에서는 이들 취약점 중 절반 이상이 가장 비중이 큰 두 가지 유형인 호스트와 게스트로 분류됨을 볼 수 있습니다. 이들 취약점은 가상 머신에서 전파되는 위협을 수반하지 않는다는 점에서 전통적인 취약점과 약간 유사합니다. 하지만 워크스테이션 제품 벤더 코드 취약점의 25% 이상이 가상 머신에서 탈출한 취약점이라는 사실은 의외일 수 있습니다. 이 제품 유형에서 Escape-to-Host 취약점은 Escape-to-Hypervisor 취약점보다 6배나 더 많습니다.

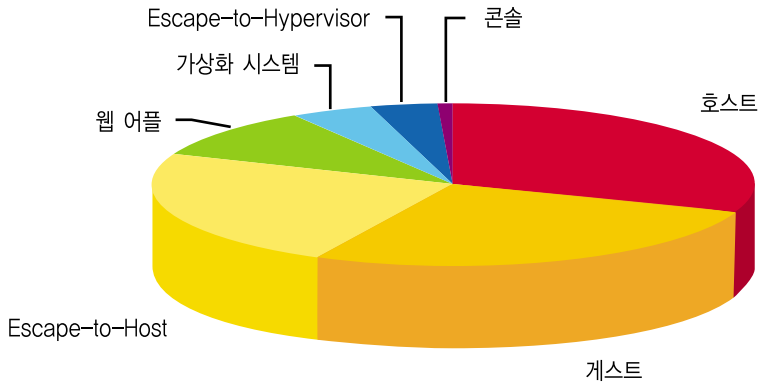


그림 28: 워크스테이션 제품 취약점의 취약점 유형별 분석, 1999 ~ 2009

서버 제품 취약점

그림 29에서, 서버 제품에 가장 많은 벤더 코드 취약점의 유형은 38%를 차지하는 가상화 시스템 취약점임을 볼 수 있습니다. Escape-to-Hypervisor 취약점은 35%로 1위를 바짝 추격하고 있습니다. Escape-to-Hypervisor 취약점은 서버 제품 벤더 코드 취약점 중 3분의 1 이상을 차지합니다. 서버 관련 Escape-to-Hypervisor 벤더 코드 취약점은 Citrix, Parallels, RedHat 및 VMware사의 제품에 영향을 미쳤습니다. 이 중 5개는 서비스 거부(DoS) 취약점이며, 하나는 원격 코드 실행과 관련된 것입니다.

서버 관련 Escape-to-Hypervisor 취약점이 존재한다는 사실은 가상 서버의 도입에 영향을 미칩니다. 시장에서는 서버 시스템에 영향을 미치는 Escape-to-Hypervisor 취약점이 없고 따라서 보안 특성이 서로 다른 가상 서버를 같은 물리적 하드웨어 상에서 구동해도 괜찮다고 추정되어 왔습니다. 하지만 여기에 제시된 결과는 Escape-to-Hypervisor 취약점이 서버 시스템에 존재함을 보여주고 있어 요구하는 보안 수준이 서로 다른 가상 서비스를 동일한 물리적 컴퓨터 상에서 구동해도 되는지에 대한 의문이 제기됩니다. 이런 결과는 가상 서버가 위험에 노출되지 않도록 보장하는 것이 얼마나 중요한 지를 강조하며, 가상화 시스템에 대한 적시 패치 관리의 중요성을 부각시킵니다.

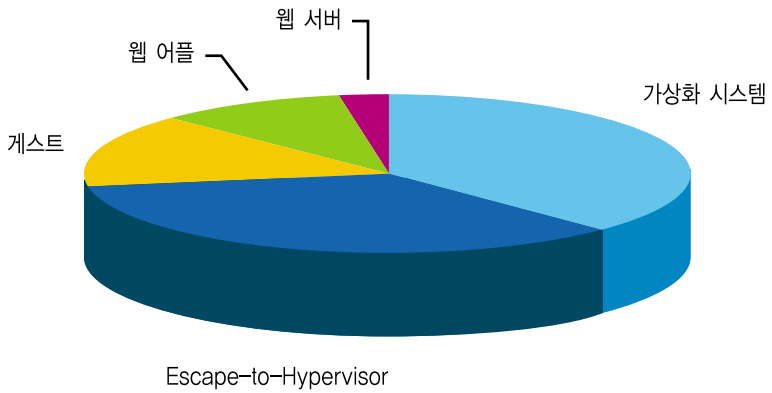


그림 29: 서버 제품 취약점의 취약점 유형별 분석, 1999～2009

가상화 취약점의 벤더별 분석

그림 30에는 본 분석에 포함된 각 벤더가 가상화 취약점 노출에 기여한 비율이 나와있습니다. VMware가 시장 선두 기업이라는 점을 감안할 때 대다수의 취약점이 VMware 제품에서 보고되었다는 사실은 놀랍지 않습니다. VMware 제품은 보고된 취약점의 80% 이상을 차지한 한편, 다음으로 비중이 많은 RedHat과 Citrix는 각각 7%와 6% 정도를 차지했습니다.

나머지 모든 업체(IBM, Microsoft 및 Oracle/Sun)는 보고된 취약점 중 각각 1% 정도만 차지하여 큰 문제가 없었습니다. 이런 결과는 해당 업체들이 자사 제품의 보안을 아주 훌륭하게 관리했기 때문이거나, 아니면 취약점 연구원들이 아직 이들 회사의 제품에 많은 관심을 집중하지 않고 있기 때문일 수 있습니다.

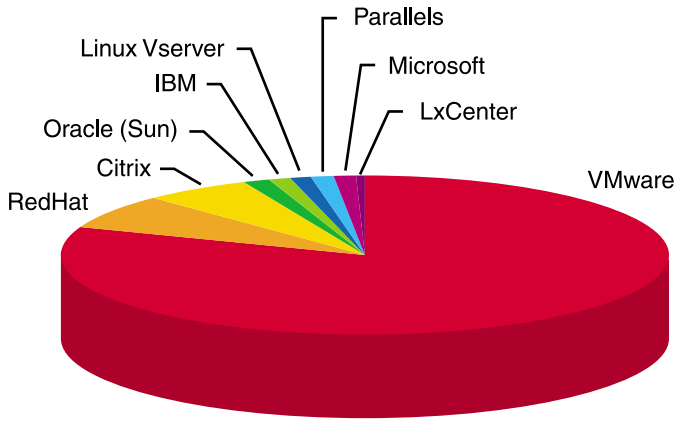


그림 30: 가상화 취약점의 벤더별 분석, 1999～2009

공격 가능성

특정한 취약점 유형을 대상으로 한 알려진 공격방법(Exploit)의 수는 해당 취약점이 공격에 악용될 수 있는 가능성을 가늠할 수 있는 하나의 척도가 됩니다. 1999년 이후 보고된 373개의 가상화 취약점 중 그것을 공격하는 방법이 알려진 것은 51개(14%)입니다. 이 비율은 전체 X-Force 데이터베이스에 있는 취약점 중 공격 방법이 알려진 비율이 25%라는 사실과 비교됩니다. 따라서, 가상화 취약점을 악용한 공격 방법이 알려진 경우는 전체 취약점의 절반 정도입니다. 이는 가상화 취약점을 공격하기가 본질적으로 더 어렵거나 공격 개발자들이 가상화 제품에 상대적으로 덜 집중하고 있음을 의미할 수 있습니다.

위험도가 매우 높기 때문에 특히 주목해야 하는 취약점 유형은 서버 제품의 Escape-to-Hypervisor 취약점입니다. 이 유형의 28가지 취약점 중 공격방법이 알려진 것은 2개뿐입니다. 이 비율은 매우 작은 것이지만, 이 취약점 유형을 공격할 방법이 존재한다는 사실 자체가 우려할만한 이유가 됩니다.

새로 부상하고 있는 클라우드: 미래를 위한 클라우드 서비스의 채택

클라우드 컴퓨팅은 주로 기업과 단체가 얻을 수 있는 비용 이득과 효율성으로 인해 최근에 시장을 강타한 혁신적인 기술입니다. 모든 신생 기술과 마찬가지로, 새로운 기술에 너무 흥분하지 않고 차분히 관리하여 기술이 조직에 새로운 위험과 결과를 가져오지 않도록 해야 할 필요가 있습니다. 많은 기업과 단체가 클라우드로 마이그레이션하는 것을 연기하고 클라우드 컴퓨팅을 단지 시험만 해보고 있다는 사실은 놀랍지 않습니다.

최근에 실시한 연구에서, 클라우드 기술의 채택을 모색하고 있는 기업과 단체는 클라우드의 채택을 가로막는 가장 큰 장애물로 보안을 꼽았으며, 가용성이 근소한 차이로 그 뒤를 이었습니다. 실제로 클라우드 패러다임을 완전히 채택한 기업은 거의 없으며, 대부분의 비즈니스는 현재 사업적 위험 부담이 적은 요소만 클라우드로 전환하고 있습니다. 역으로, 많은 수의 중소기업은 클라우드의 혜택을 누리고 있음을 볼 수 있습니다. 이들은 호스트 단체가 제공하는 기능의 부산물로서 보안 수준도 높일 수 있을 것으로 기대하고 있습니다.

클라우드 기반 기술의 광범위한 채택을 주저하는 이유는 클라우드 오퍼링과 그 기능의 복잡성과 변이성에 깊은 뿌리를 두고 있습니다. 기업은 종종 개별 벤더와 기능을 살펴보는 것으로 클라우드에 대한 평가를 시작합니다.

그러나, IBM은 클라우드에 적합한 워크로드를 고려함으로써 클라우드의 채택을 시작해야 한다고 주장합니다.

클라우드를 워크로드 기준으로 평가하면 기업은 적합한 클라우드 도입 시나리오를 선택하기 위해 필요한 요소를 더 잘 이해할 수 있습니다. 예를 들면, 의료 데이터를 포함하는 워크로드를 클라우드로 옮길 방안을 모색하는 기업은 그에 따른 보안 및 감사 요건을 정의하고 법적 제약과 관련하여 요구되는 모든 공동의 노력을 열거할 수 있습니다. 이런 점을 고려하는 기업은 자사 안에 있는 데이터와 해당 데이터와 비즈니스의 관련성에 대한 이해를 높이는 등의 다른 이득을 얻을 수 있습니다.

데이터를 보안 및 규제 요건을 기준으로 분류한 후, 기업은 이 정보를 이용하여 클라우드에 있는 자사 데이터를 보호하기 위해 필수적으로 요구되는 속성을 결정하고 도입할 다양한 서비스를 제공할 업체를 평가할 기준을 정할 수 있습니다. 여기에 적용될 수 있는 속성의 예로는 법적인 이유로 인해 특정한 데이터를 보존하고 제공해야 하는 구체적인 전자게시(eDiscovery) 요건이 있는 경우를 들 수 있습니다.

그 밖에 공공 클라우드를 도입하고자 하는 기업이 우려하는 사항으로는 호스트 단체의 재무 안정성과 호스트 단체의 도입 정책 등의 요인을 들 수 있습니다. 예를 들면, 고객은 여러 고객을 그룹별로 묶는 모든 업체를 피하고자 할 수 있습니다. 왜냐하면, 한 가입자에 영향을 미치는 법적 문제가 다른 공동 가입자에게 영향을 미칠 수 있기 때문입니다.
마지막으로, 클라우드 기반 서비스를 채택할 때는 전략적인 방법으로 접근하는 것이 중요합니다. 이는 벤더를 찾아 나서기 전에 기회와 요건에 대한 많은 지식을 쌓아야 함을 의미합니다. 미리 사전 조사를 하면 적절한 비즈니스 파트너를 고를 준비를 더 잘 갖출 수 있습니다.

II 부
개요

IBM X-Force® 연구개발팀은 광범위한 컴퓨터 보안 위협 및 취약점을 발견, 분석, 모니터링하고 기록합니다. X-Force의 관찰 결과에서는 2010년 상반기 내내 몇 가지 새로운 동향이 표면화되었습니다. 이 같은 동향에 대해 당사가 본 보고서에서 제시하는 정보가 2010년의 남은 기간과 그 이후의 정보 보안 노력을 계획하는 데 유용한 기초가 될 수 있기를 바랍니다.

2010년 상반기 특징

취약점

- 올해 상반기에 새로 노출된 취약점의 수는 사상 최고 수준을 기록했습니다. 이런 결과는 새로 노출된 취약점이 4년 만에 가장 적었던 2009년 상반기 보고서와 극명히 대조되는 것입니다. 웹 애플리케이션 취약점 – 특히 XSS(Cross-Site Scripting)와 SQL Injection은 계속 위협 환경을 지배하고 있습니다.
- Apple은 모든 노출된 취약점 중 4%를 차지하여 노출된 취약점이 가장 많은 업체였습니다. Microsoft®는 3년 연속으로 노출된 취약점이 가장 많은 업체였지만, 이제 2위로 떨어졌습니다. Adobe는 신고된 PDF 및 Flash 기반 취약점 노출이 눈에 띄게 증가하여 3위에 올랐습니다.
- 운영체제 쪽에서는 Linux가 올해 상반기에 새로 노출된 운영체제 취약점이 가장 많아 1위에 올랐으며, 그 뒤를 이어 Apple이 2위를 기록했습니다. 치명적(Critical)이고 위험도가 높은 운영체제 취약점만 따지면 Microsoft가 73%로 단연 1위였습니다.

공격

- 웹 애플리케이션은 계속하여 전체 취약점 노출의 55%를 차지하고 있습니다.
- PDF 공격은 공격자들이 스팸, 피싱 및 난독화 같은 수법을 다양하게 사용하여 최종 사용자를 혼란시키는 가운데 대대적으로 행해졌습니다.
- Internet Explorer는 노출된 취약점과 이런 새로운 취약점을 공격할 방법을 적극적으로 모색하는 공격자라는 측면에서 초기 선두에 나섰습니다.

취약점

2010년 상반기에 노출된 취약점의 수

본 보고서의 I 부에서는 2010년 상반기에 이미 노출된 취약점의 엄청난 수에 대해 설명했습니다. 2010년에는 취약점 노출의 수가 사상 최고 수준으로 증가할 것으로 예상됩니다.

보고서의 웹 관련 부분에서는 모든 보고된 취약점 노출의 절반을 차지하는 웹 애플리케이션에 영향을 미치는 취약점에 대해 설명할 것입니다. 이런 웹 애플리케이션의 바로 뒤에는 고객 개발 애플리케이션, 웹 브라우저 및 PDF가 있습니다. 이는 모두 올 2010년 상반기에도 계속 기록적인 보고 건수를 보이고 있습니다.

취약점 분류에 관한 모든 모호성을 방지하기 위해, 본 보고서에서는 다음과 같은 IBM Security Services의 정의를 사용했습니다.

취약점이란 정보 시스템의 기밀성, 무결성 또는 가용성이 눈에 보이거나 보이지 않게 훼손되는 결과를 초래하거나 초래할 수 있는 일련의 상태라 정의됩니다.

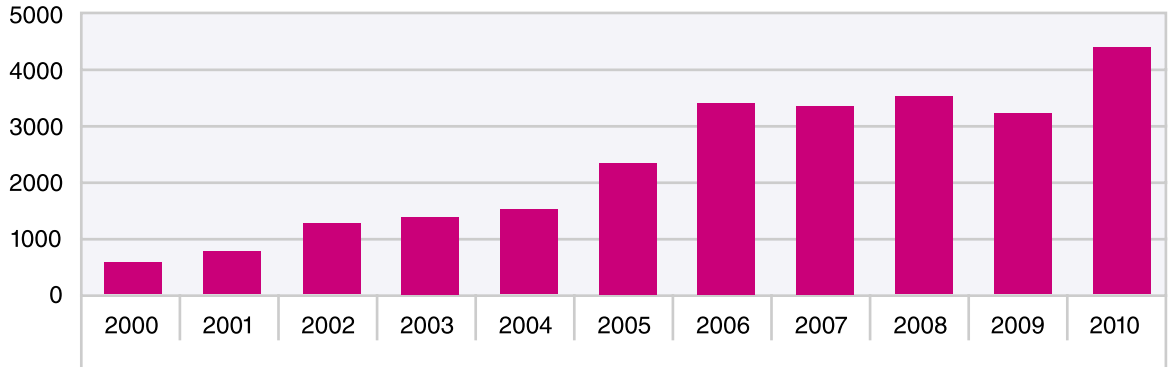


그림 31: 매년 상반기에 노출된 취약점, 2000～2010년

노출된 취약점의 위험도별 분석

CVSS(Common Vulnerability Scoring System)는 공식과 기본 및 시간 척도(Metric)를 토대로 취약점의 심각성과 위험도를 평가하는 산업 표준입니다. 기본 척도는 접근 벡터(Vector), 복잡성, 인증 및 영향 편향(Impact bias)과 같이 시간이 지나도 일반적으로 변하지 않는 특징입니다. 시간 척도는 공격가능성, 교정 수준 및 보고 신뢰도 같이 시간이 흐름에 따라 변할 수 있고 실제로 종종 변하는 특정한 취약점의 특징입니다.

CVSS 척도에 의해 치명적인 것으로 분류되는 취약점은 기본 설정에 의해 설치되고, 네트워크 라우팅이 가능하고, 액세스를 위해 인증을 요구하지 않고, 공격자에게 시스템 또는 루트 단계 액세스 권한을 허용하는 취약점입니다.

표 6에는 기본 및 시간 CVSS 점수대에 상응하는 위험도가 나와 있습니다.

CVSS 점수	위험도
10	치명적
7.0 ~ 9.9	높음
4.0 ~ 6.9	중간
0.0 ~ 3.9	낮음

표 6: CVSS 점수와 그에 상응하는 위험도

CVSS에 대한 전체 설명을 포함한 CVSS와 그 척도에 대한 자세한 사항은 First.org 웹사이트의 http://www.first.org/cvss/ 페이지를 참조하십시오.

CVSS 기본 점수

그림 32에 나와있는 것처럼, 치명적인 취약점의 비중은 2008~2009년과 비슷한 1%를 유지했습니다.

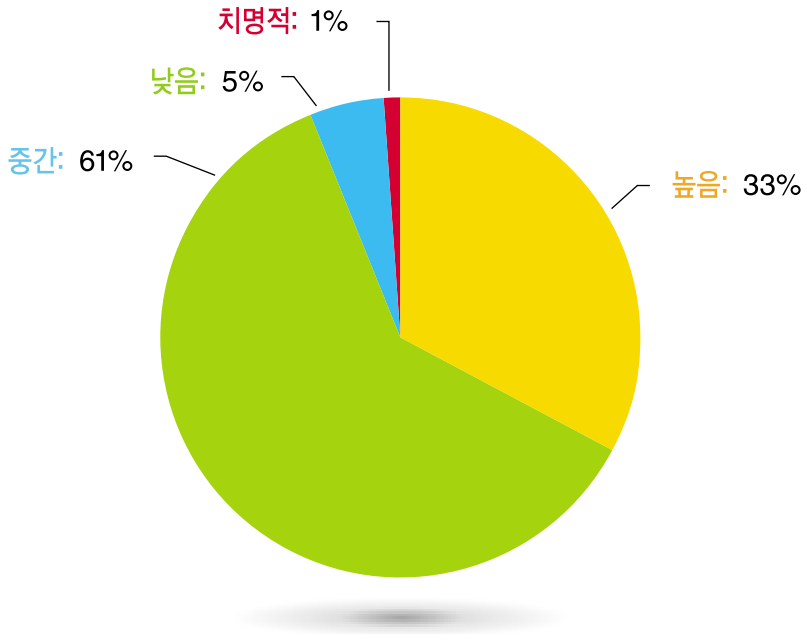


그림 32: CVSS 기본 점수, 2010년 상반기

상대적인 비율(%)은 2009년 자료와 대체로 비슷합니다. 중간 및 낮음에 해당하는 취약점은 약간 감소했으며, 위험도가 높은 취약점은 그에 상응하는 만큼 약간 증가했습니다. 위험도가 중단인 취약점에는 가장 흔한 2가지의 노출된 취약점인 SQL Injection과 XSS(Cross-Site Scripting)가 포함됩니다. 위험도가 높은 취약점은 그림 33에 나와있는 것처럼 2008년의 36%보다 약간 적고 2009년 상반기의 30%보다 약간 증가한 33%였습니다.

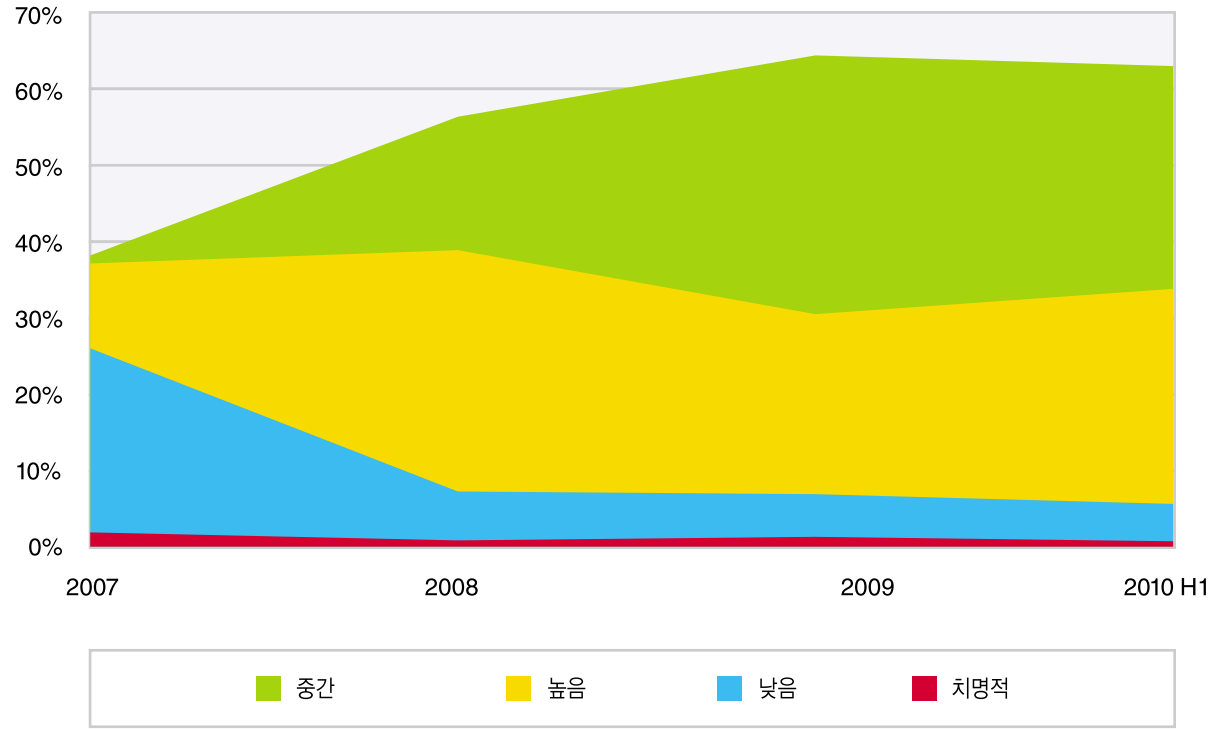


그림 33: CVSS 기본 점수, 노출된 취약점의 위험도별 분석, 2007~2010년 상반기

노출된 취약점이 가장 많은 업체

2010년 상반기에 노출된 취약점이 가장 많았던 10대 업체가 모든 노출된 취약점 중에서 차지하는 비중은 2009년(23%)보다 약간 낮고 2008년(19%)과 2007년(18%)보다 약간 높은 5분의 1(20%)이였습니다.

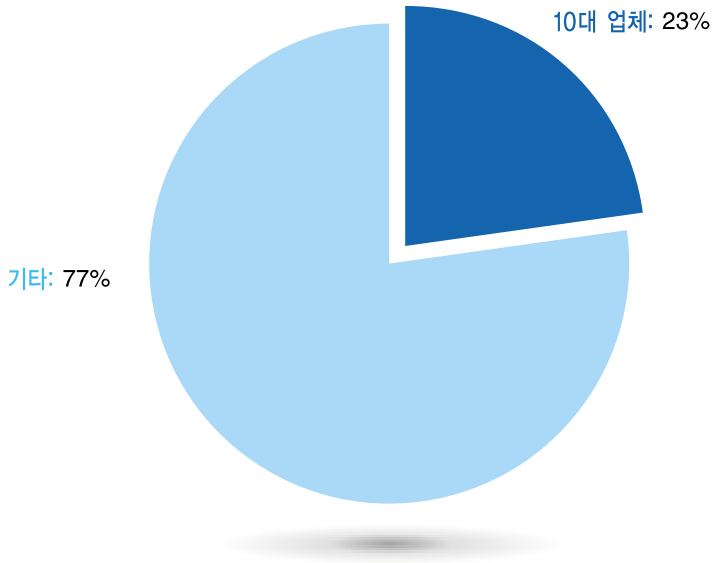


그림 34: 모든 노출된 취약점 중 10대 업체가 차지하는 비율(%), 2009년

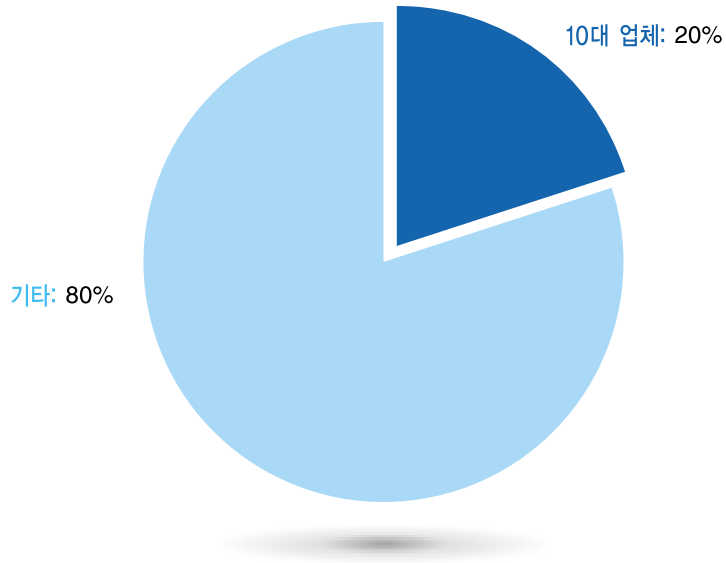


그림 35: 모든 노출된 취약점 중 10대 업체가 차지하는 비율(%), 2010년 상반기

10대 업체 목록의 변동

X-Force 데이터베이스 팀은 CPE(Common Platform Enumeration)라는 산업 표준을 이용하여 취약점을 업체와 업체 제품별로 분류합니다. 자세한 사항은 http://cpe.mitre.org/를 참조하십시오.

표 7에는 2010년의 10대 업체와 각 업체의 취약점 비율(%)이 2009년과 비교하여 나와있습니다. 이들 통계는 노출된 취약점을 시장점유율이나 제품 수나 각 업체가 제작하는 코드 라인 수를 기준으로 균등화되지 않았음을 유념하십시오. 일반적으로, 대량 생산되고 널리 배포되거나 이용되는 소프트웨어는 취약점 노출이 더 많을 가능성이 큽니다.

몇 가지 관찰된 내용:

- Apple은 전체 노출된 취약점 중 4%를 차지하여 2년 연속으로 1위에 올랐습니다.
- Sun은 작년 2위에서 최하위로 하락하여 2009년과 큰 차이를 보였습니다. Sun은 2009년 4월에 Oracle에게 인수되었지만, 당사 데이터베이스에서 Sun의 제품은 계속 별개로 집계되었기 때문에 계속 따로 기재되었습니다.
- Microsoft는 2006년부터 2008년까지 1위 자리를 고수한 후 올 상반기에는 3위에서 2위로 상승했습니다.

2010 H1		
순위	업체	노출 빈도
1	Apple	4.0%
2	Microsoft	3.4%
3	Adobe	2.4%
4	Cisco	1.9%
5	Oracle	1.7%
6	Google	1.6%
7	IBM	1.5%
8	Mozilla	1.4%
9	Linux	1.4%
10	Sun	1.1%

2009년 (한 해)		
순위	업체	노출 빈도
1	Apple	3.8%
2	Sun	3.3%
3	Microsoft	3.2%
4	IBM	2.7%
5	Oracle	2.2%
6	Oracle	2.0%
7	Linux	1.7%
8	Cisco	1.5%
9	Adobe	1.4%
10	HP	1.2%

표 7: 노출된 취약점이 가장 많은 업체

- Adobe는 9위에서 3위로 상승했는데, 이는 아마도 2010년 상반기에 보고된 PDF 및 Flash 기반 취약점이 크게 증가했기 때문일 것입니다.
- HP는 목록에서 탈락한 반면, Google은 6위로 목록에 등장했습니다.

취약점 수정 및 패치의 제공

I 부에서는 취약점과 패치율에 대해 설명했습니다. 여기서 당사는 주요 업체가 알려진 취약점을 잘 해결하고 고치고 있음을 증명해 보이고, 주요 업체 중 최고 및 최악의 패치 적용 업체를 열거했습니다. 이어지는 내용에서는 원격 공격이 가능한 취약점에 대해 알아볼 것입니다.

원격 공격이 가능한 취약점

원격 공격이 가능한 취약점은 취약한 시스템을 물리적으로 액세스하지 않아도 되기 때문에 가장 중요합니다. 원격 취약점은 네트워크나 인터넷을 통해 공격할 수 있는 반면, 로컬 취약점을 공격하기 위해서는 시스템을 직접 액세스해야 합니다. 원격 및 로컬 유형으로 모두 분류되는 취약점은 두 가지 경로를 모두 사용하여 공격할 수 있는 취약점입니다.

지난 4년 동안 노출된 모든 취약점 중에서 원격 공격이 가능한 취약점이 차지한 비중은 85%에서 94%로 증가했습니다. 2009년에 원격 취약점은 92%였고, 2010년 상반기에는 94%로 소폭 증가했습니다. 그림 36에서는 원격 공격이 가능한 취약점이 지난 10년 동안 해마다 꾸준히 증가했음을 볼 수 있습니다.

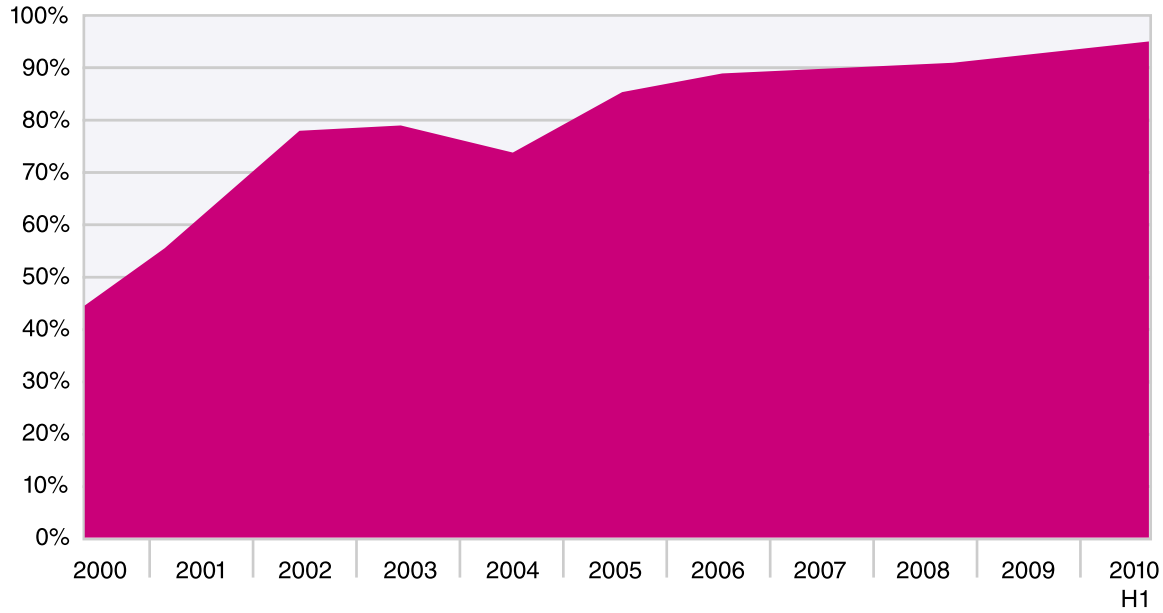


그림 36: 원격 공격이 가능한 취약점의 비율(%), 2000년~2010년 상반기

공격의 결과

IBM X-Force는 공격의 결과를 기준으로 취약점을 구분합니다. 공격의 결과란 한 마디로 취약점을 공격함으로써 공격자가 얻을 수 있는 이익을 의미합니다. 표 8에는 각 공격 결과에 대한 설명이 나와있습니다.

결과	정의
보안 우회	방화벽, 프록시, IDS 시스템 또는 바이러스 스캐너와 같은 보안 제한 기능을 우회합니다.
데이터 조작	서비스 또는 애플리케이션과 관련된 호스트가 사용하거나 저장한 데이터를 조작합니다.
서비스 거부	서비스나 시스템을 다운시키거나 중단시켜 네트워크를 무력화합니다.
파일 조작	파일을 작성하거나, 삭제하거나, 읽거나, 수정하거나, 덮어씁니다.
액세스 권한 획득	로컬 및 원격 액세스 권한을 획득합니다. 여기에는 공격자가 코드 또는 명령을 실행하기 위해 공격할 수 있는 취약점도 포함됩니다. 이를 통해 공격자는 시스템에 대한 액세스 권한을 획득할 수 있는 경우가 일반적이기 때문입니다.
권한 획득	권한은 로컬 시스템에서만 획득할 수 있습니다.
정보 획득	파일 및 경로 이름, 소스 코드, 암호 또는 서버 구성 내역과 같은 정보를 획득합니다.
기타	다른 결과 유형에 해당되지 않는 모든 결과

표 8: 취약점의 결과 정의

취약점 공격의 결과 중 가장 많은 것은 여전히 접근 권한 획득으로서, 전체 취약점의 결과 중 52%를 차지합니다. 접근 권한 획득은 2008년에 잠시 비중이 감소한 후 2006년과 2007년에 이어 다시 50%를 넘었습니다. 시스템 접근 권한을 획득하는 공격자는 해당 시스템에 대한 완전한 통제권을 얻게 되어 데이터를 훔치거나, 시스템을 조작하거나 해당 시스템에서 다른 공격을 감행할 수 있게 됩니다.

공격자가 데이터를 조작할 수 있는 길을 열어주는 취약점은 2008년에 22%로 정점을 찍은 후에 많은 SQL Injection 활동으로 인해 다시 21%로 증가했습니다.

다른 공격 경로의 비율(%)은 대부분 전년도와 유사합니다.

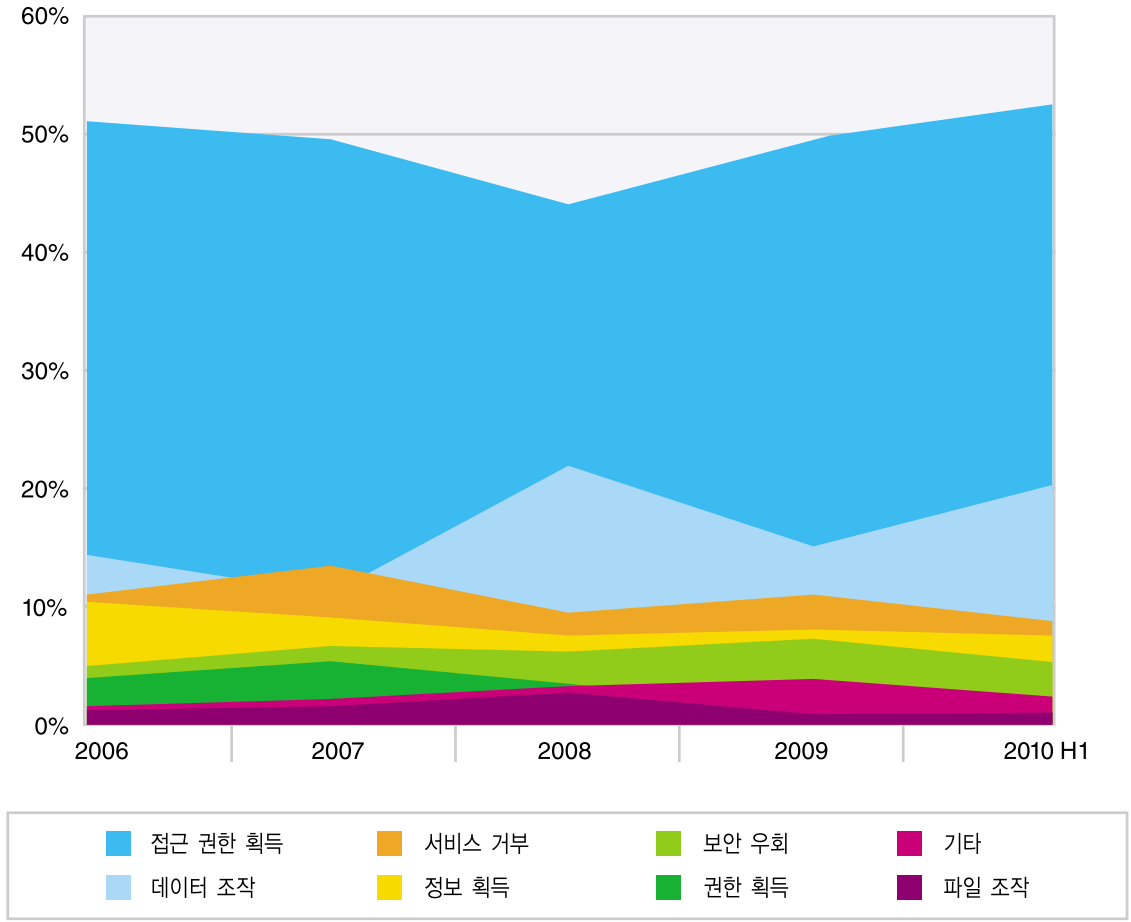


그림 37: 전체 취약점 노출 대비 취약점 결과의 비율(%), 2006년 ~ 2010년 상반기

노출된 취약점이 가장 많은 운영체제

이어지는 운영체제 분석에서는 단일 운영체제 유형에 대해 보고된 고유한 취약점이 집계되었습니다. 예를 들면, 이 분석에서는 Microsoft 운영체제에 대해 보고된 모든 취약점을 같은 기간에 Apple 운영체제에 대해 보고된 모든 취약점과 비교합니다. 특정 취약점이 한 운영체제군의 여러 버전에 적용될 경우, 취약점은 한 번만 집계됩니다. 예를 들어 특정한 CVE가 Apple Mac OS X와 Apple Mac OS X Server에 모두 적용될 경우, Apple 운영체제군에 대해 한 번만 집계됩니다.

모든 운영체제 취약점

2010년 상반기에 Linux는 전체 운영체제 취약점 중에서 차지하는 비중(%)이 가장 높았으며, Apple이 근소한 차이로 2위를 기록했습니다. Microsoft 관련 취약점은 2009에 비해 크게 증가하여 3위에 올랐습니다. Sun Solaris는 노출된 취약점이 크게 감소하여 4위로 하락했습니다. BSD는 5위 자리를 유지했으며, 2008년에 5위였던 IBM AIX는 2년 연속 순위에서 제외되었습니다.

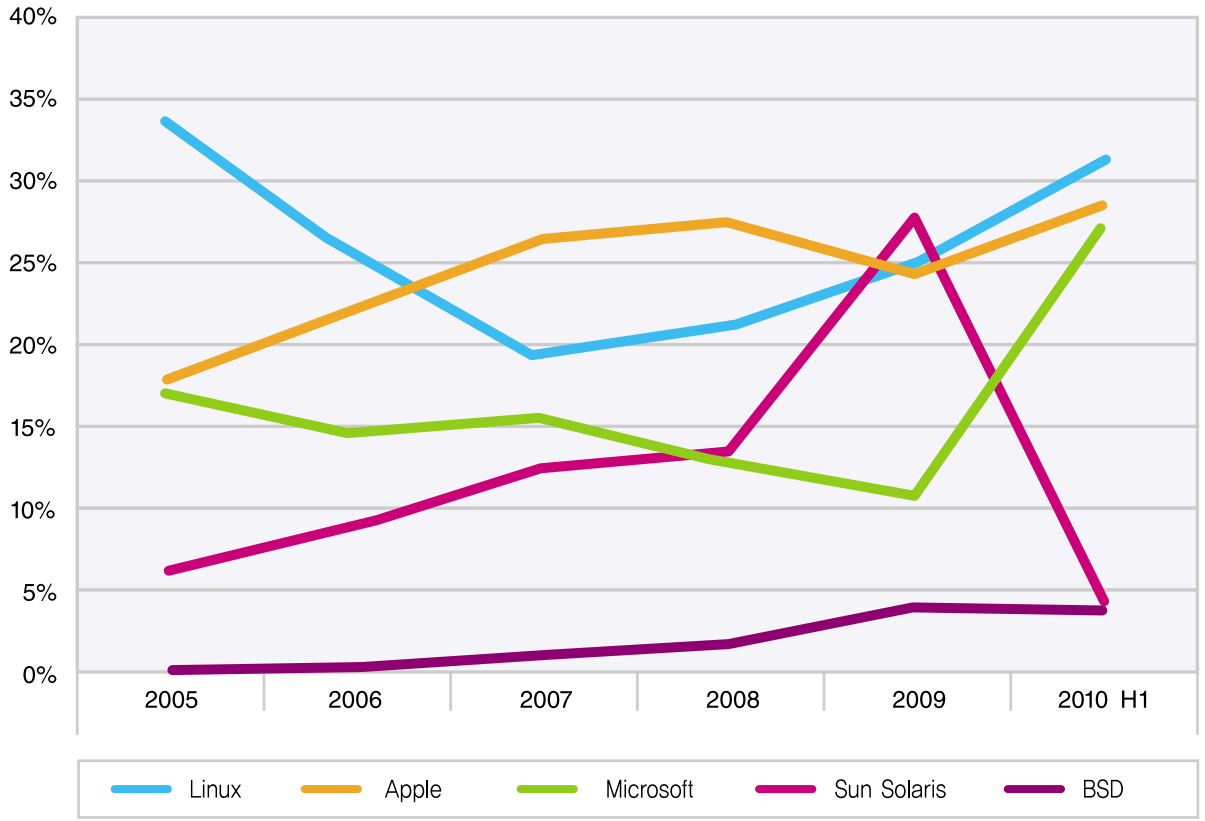


그림 38: 운영체제에 영향을 미치는 노출된 취약점, 2005년~2010년 상반기

치명적이거나 위험도가 높은 운영체제 취약점

치명적이거나 위험도가 높은 취약점에 초점을 맞추는 방법은 운영체제 취약점을 바라보는 또 다른 방법입니다. 치명적인 취약점은 공격자가 궁극적으로 추구하는 완전한 원격 보안 침해로 종종 이어지기 때문에 보호라는 관점에서 일반적으로 가장 우려되는 것입니다. 위험도가 중간 및 낮음에 해당하는 취약점을 걸러내면 Microsoft 운영체제는 2008년과 2009년과 2010년 상반기에 모두 1위이며, Linux가 현재 2위고 Apple이 3위입니다. 4위는 HP-UX고, Sun Solaris는 근소한 차이로 5위입니다. IBM AIX는 2009년 상반기에 5위였다가 명단에서 사라졌습니다.

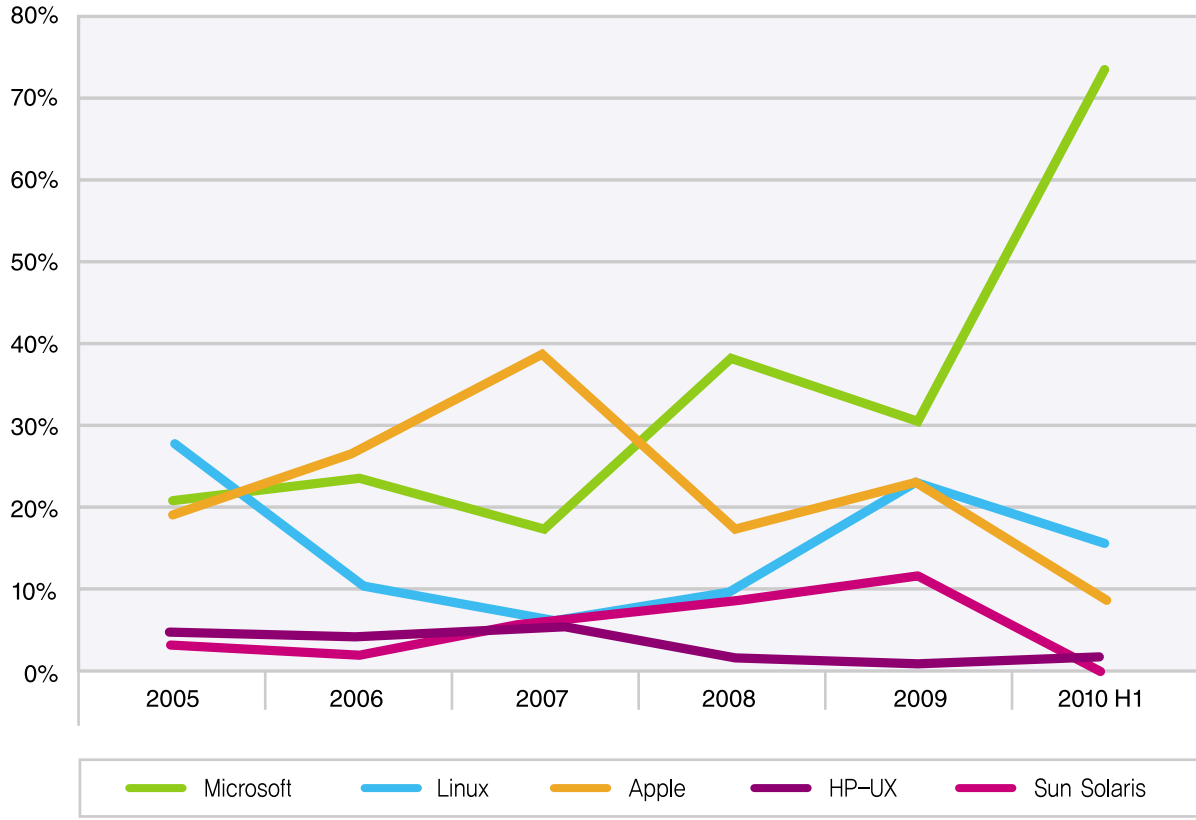


그림 39: 운영체제에 영향을 미치는 치명적이거나 위험도가 높은 노출된 취약점, 2005년~2010년 상반기

표 9에 열거된 5대 운영체제는 2010년 상반기에 노출된 위험도가 치명적이거나 높은 모든 운영체제 취약점 중 98%를 차지하여 2009년 상반기의 93%보다 소폭 증가했습니다.

운영체제	치명적이거나 위험도가 높은 취약점의 비율(%)	전체 OS 취약점 중에서 차지하는 비율(%)
Microsoft	73%	27%
Apple	9%	29%
Linux	16%	31%
HP-UX	2%	1%
Sun Solaris	0%	4%
BSD	0%	4%
IBM AIX	0%	2%
기타	2%	4%

표 9: 치명적이거나 위험도가 높은 취약점이 가장 많이 노출된 운영체제, 2010년 상반기

CPE를 사용하여 운영체제를 집계하지 않는 이유

2008년 보고서에서 X-Force는 가장 취약점이 많은 운영체제를 분석한 결과를 제시했습니다. 취약점은 각 업체가 CPE(Common Platform Enumeration)를 통해 자사 플랫폼을 신고하는 방법에 따라 집계되었습니다. 일부 업체는 자사 플랫폼을 약간 다르게 분류합니다. 예를 들면, "Linux 커널"이라는 Linux 플랫폼에 대해 보고되었을 수 있는 Linux 취약점은 CPE에 해당 플랫폼에 해당되는 취약점으로 공식적으로 보고되지 않을 수 있음에도 불구하고 다른 Linux 버전에도 영향을 미칠 수 있습니다. 그 밖에 다른 차이점으로는 업체들이 플랫폼을 분류하는 방법도 있습니다. 예를 들면, Apple은 모든 Apple Mac OS X 소프트웨어 버전을 단일 "플랫폼"으로 합치며, 소프트웨어의 서버 및 데스크탑 버전만 구별합니다. Microsoft는 자사의 주요 운영체제를 각각 "플랫폼"이라 부르지만, 이런 플랫폼 중 일부는 Windows의 "버전"으로 간주되는 경우가 많습니다.

따라서, 본 보고서에서는 CPE에 거명된 "플랫폼"을 기준으로 취약점을 집계하지 않고 유사한 플랫폼(모든 Windows, 모든 Apple)을 하나로 합치고 특정 운영체제군의 여러 버전에 영향을 미치는 취약점 하나를 한 번만 집계합니다.

장기적인 안목에서 운영체제 취약점 보유

운영체제 취약점은 항상 심각한 우려를 자아냅니다. 하지만 본 보고서의 여러 주요 통계가 분명히 보여주듯, 정말로 심각한 문제는 운영체제에서 실행되는 일련의 다양한 응용프로그램입니다. 노출된 운영체제 취약점은 2010년 상반기에 노출된 모든 취약점 중 약 11%를 차지했습니다. 기업과 각종 단체는 오래 전부터 운영체제를 최대한 빨리 패치하여 보호하기 위한 패치 작전을 실행해 왔습니다. 이런 요인으로 인해 운영체제는 보편적으로 사용되는 소프트웨어임에도 불구하고 성공적으로 공격하기가 훨씬 더 어렵습니다. 웹 애플리케이션, 웹 브라우저, PDF를 포함한 악성 문서 등의 기타 구성요소는 운영체제를 제치고 가장 우려되는 위협 경로가 되었습니다.

웹 애플리케이션 위협 및 취약점

웹 애플리케이션 취약점은 지금도 계속 서버에 가장 많이 영향을 미치는 취약점 유형으로 꼽히고 있습니다. 웹 애플리케이션 취약점의 비중은 55%까지 조금씩 증가하여 2010년 상반기에 노출된 모든 취약점의 절반 이상을 차지하게 되었습니다.

웹 애플리케이션 취약점 노출 수는 연간 3,000~4,000개씩 계속 조금씩 증가하고 있습니다. 이 수치에는 그 역시 취약점을 유입시키는 맞춤 개발된 웹 애플리케이션이나 위에서 언급한 표준 소프트웨어 패키지의 맞춤 버전이 포함되지 않았습니다.

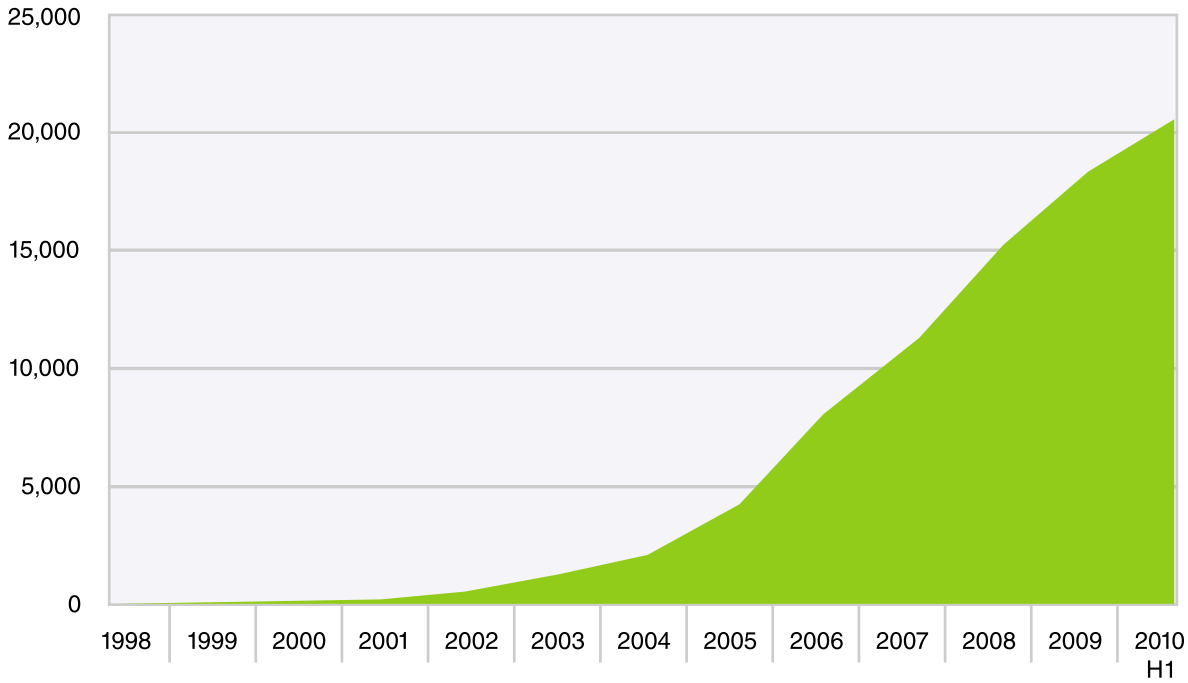


그림 40: 노출된 웹 애플리케이션 취약점의 누적 집계, 1998년~2010년 상반기

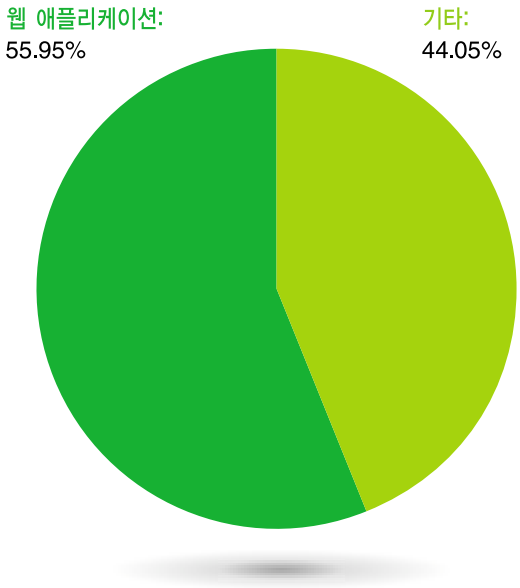


그림 41: 웹 애플리케이션에 영향을 미치는 노출된 취약점의 비율(%), 2010년 상반기

따라서, 이들 취약점은 인터넷 상에 존재하는 모든 애플리케이션 취약점의 수 중 빙산의 일각에 불과할 수 있습니다.

노출된 웹 애플리케이션 취약점의 공격 유형별 분석

XSS(Cross-Site Scripting) 및 SQL Injection 취약점은 2010년 상반기에 웹 애플리케이션에 가장 많은 영향을 미친 보안 취약점 유형이었습니다.

그림 42는 XSS(Cross-Site Scripting), SQL Injection, File Include 및 기타 노출된 취약점이 각기 차지하는 상대적인 비중의 시간적 추이를 보여주고 있는 한편, 표 10에는 각 유형이 기업과 그 고객에게 미칠 수 있는 영향을 포함한 각 유형에 대한 설명이 나와있습니다.

2009년 말에 발표된 이전 X-Force 동향 보고서에는 노출된 SQL Injection 취약점이 전년 대비 크게 감소한 것으로 나왔었습니다. 당시에 이는 발전의 조짐이라 생각되었습니다. SQL Injection 취약점은 인터넷에서 지난 몇 년 동안 많은 공격 활동의 표적이 되어 왔으며, 노출된 취약점의 감소는 해당 취약점이 점점 찾기가 어려워지고 있음을 즉, 따기 쉬운 열매가 많이 없어졌음을 의미할 수도 있다고 생각되었습니다. 안타깝게도 노출된 SQL Injection 취약점의 양은 2010년 상반기에 다시 증가한 것으로 보입니다. 웹 애플리케이션 취약점 문제가 아직 수그러지지 않았음은 분명합니다.

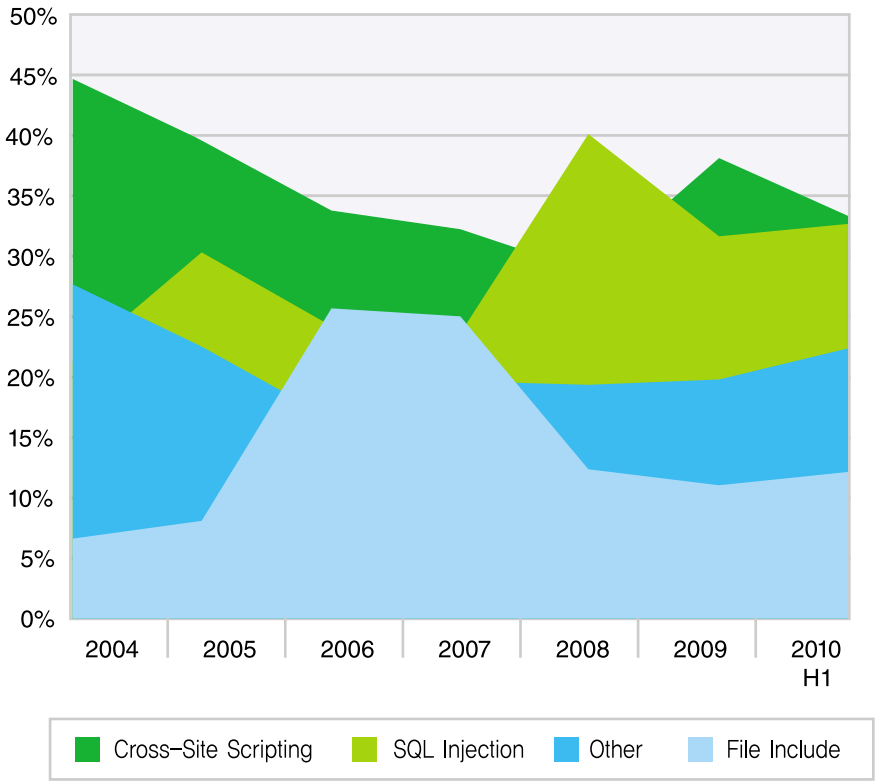


그림 42: 웹 애플리케이션 취약점의 공격 기법별 분석, 2004년~2010년 상반기

웹 애플리케이션에 대한 XSS(Cross-Site Scripting) 공격

노출된 웹 애플리케이션 취약점의 공격 유형별 분석 부분에서는 노출된 XSS(Cross-Site Scripting) 취약점의 비중이 매우 높았다고 지적했습니다. 실제 MSS 데이터는 이 웹 애플리케이션 취약점 유형이 공격자들에게 가장 선호되는 공격 수단이라는 사실도 보여주고 있습니다.

그림 43: XSS(Cross-Site Scripting) 공격, IBM Managed Security Services, 2009년 1분기~2010년 2분기

공격 기법	설명
XSS (Cross-Site Scripting)	XSS(Cross-Site Scripting) 취약점은 사용자가 양식 필드(Form Field)나 URL의 구문 등에서 입력한 정보를 웹 애플리케이션이 올바로 검증하지 않을 때 발생합니다. 이 취약점을 통해, 공격자는 사용자가 방문하는 페이지에 자신이 제작한 스크립트를 심어 페이지의 움직임이나 모양을 조작할 수 있습니다. 이런 페이지 변경은 민감한 정보를 가로채거나, 웹 애플리케이션을 악의적인 방법으로 조작하거나, 다른 취약점을 공격하는 추가 컨텐츠를 페이지에 심기 위해 사용할 수 있습니다. 공격자는 먼저 특별히 제작된 웹 링크를 만든 다음 (스팸과 사용자 포럼 등을 통해) 피해자가 그것을 클릭하도록 유도해야 합니다. URL의 도메인명은 신뢰하거나 익숙한 회사의 이름이기 때문에 사용자를 속여 링크를 클릭하도록 하기가 더 쉽습니다. 사용자에게는 공격 시도가 신뢰할 수 있는 단체의 취약점을 악용하는 공격자가 아닌 신뢰되는 단체에 의해 직접 감행되는 것처럼 보일 수 있습니다.
SQL Injection	SQL Injection 취약점 역시 사용자 입력 정보의 부적절한 검증과 관련이 있으며, (예를 들면 양식 필드에서 입력된) 이 입력 정보가 나중에 데이터베이스에 의해 실행될 SQL 구문을 동적으로 포함하도록 허용될 때 발생합니다. 백엔드 데이터베이스를 액세스하면 공격자가 민감한 정보를 읽고 삭제하고 수정할 수 있으며, 경우에 따라서는 임의 코드를 실행할 수도 있습니다. 공격자는 SQL Injection 취약점을 통해 (신용카드 정보 같은) 기밀 고객 정보를 노출시키고 웹사이트 방문자를 상대로 악용할 수 있는 다른 공격을 데이터베이스 안에 심을 수도 있습니다.
File Include	(일반적으로 PHP 애플리케이션에서 발견되는) File Include 취약점은 애플리케이션이 원격 소스로부터 로컬 애플리케이션에서 실행할 코드를 회수할 때 발생합니다. 원격 소스는 종종 신빙성이 확인되지 않기 때문에, 공격자는 이를 통해 웹 애플리케이션을 사용하여 악성 코드를 원격 실행할 수 있습니다.
기타	이 유형에는 공격자가 무허가 정보를 열람 또는 획득하거나 파일, 디렉토리, 사용자 정보 또는 기타 웹 애플리케이션의 구성요소를 변경하기 위해 악용할 수 있는 디렉토리 이동(Traversal) 등의 몇몇 서비스 거부 공격과 악성 기법이 포함됩니다.

표 10: 가장 많은 웹 애플리케이션 취약점 유형에 대한 설명

OWASP 상위 10

웹 애플리케이션, 서비스 및 데이터를 대상으로 한 공격이 점점 증가하는 추세로 인해, 여러 기업 및 단체는 조직 전체에 걸쳐 보안 집행 문제에 대응하지 않으면 안 되게 되었습니다. 이런 공격에는 XSS (Cross Site Scripting), SQL Injection 공격, DoS(서비스 거부) 공격 그리고 디렉토리 이동과 같은 기타 기법이 포함됩니다. 이런 공격 유형을 통해 공격자는 정보를 허가 없이 보거나 획득하거나 파일, 디렉토리, 사용자 정보 및 기타 웹 애플리케이션 구성요소를 변경할 수 있습니다.

OWASP(Open Web Application Security Project) 상위 10은 웹 애플리케이션 보안에 대한 의식을 제고하기 위한 문서를 제공하며, 가장 치명적인 웹 애플리케이션 보안 결함을 둘러싼 광범위한 합의를 제시합니다. 프로젝트에는 전세계의 다양한 보안 전문가가 참여하여 목록 작성에 각자의 전문 지식을 기여했습니다.

취약한 인증 및 세션 관리(Broken Authentication & Session Management) 같은 취약점을 악용하면, 공격자는 비밀번호, 키 및 세션 토큰을 해킹하거나 다른 구현 결함을 악용하여 사용자의 신분을 가장할 수 있습니다. URL 액세스 제한 실패, 잘못된 보안 구성 그리고 검증되지 않은 이동 및 전달(Redirects & Forwards)은 민감한 비즈니스 데이터와 정보를 무허가 사용자에게 노출시킵니다. 따라서, 당사는 외부에 노출되는 애플리케이션과 서비스의 리스크와 취약점을 평가하고 적절한 보안 통제 수단을 갖춤으로써 기업 안팎에서 사용자 신분과 액세스를 관리할 것을 권장합니다.

2010년 OWASP 상위 10 위협	주요 고려사항
A1: 주입(Injection) 결함	신뢰할 수 없는 데이터를 사용자가 제공한 애플리케이션 명령이나 질의와 분리. **누가 시스템에 데이터를 전송**할 수 있습니까?
A2: XSS (Cross-Site Scripting)	신뢰할 수 없는 데이터를 활성 브라우저에서 분리. **누가 시스템에 데이터를 전송**할 수 있습니까?
A3: 취약한 인증 및 세션 관리	로그아웃 시 세션 상태를 무효화할 수 있는 기능으로 **액세스를 제어**해야 함. 토큰 또는 SSL 상태 재사용이 허용되어서는 안 됨.
A4: 불안전한 직접 객체 참조	시스템 데이터를 변경할 수 있는 **부분적인 액세스 권한**을 갖고 있는 사용자가 있는가?
A5: CSRF (사이트 간 요청 위조)	사용자를 거부하거나 승격시키거나 재인증할 수 있는 기능을 통해 **액세스를 제어**해야 함.
A6: 잘못된 보안 구성	전체 애플리케이션 스택에 걸쳐 **보안 강화** 작업을 수행했습니까?
A7: 불안전한 암호화 스토리지	민감한 데이터 **암호화**. 보안 토큰을 사용하여 암호화 리소스 보호.
A8: URL 액세스 제한 실패	포털 상의 URL에 대한 **액세스를 제어**해야 함. 네트워크 접근 권한이 있으면 누구나 애플리케이션 요청을 전송할 수 있습니까?
A9: 불충분한 전송 층 보호	사용자의 네트워크 트래픽을 모니터링할 수 있는 자가 있습니까? **SSL**을 사용하여 모든 인증된 트래픽 보호.
A10: 검증되지 않은 리디렉터 및 포워드	사용자가 웹사이트에 요청을 제출하도록 **속일 수 있는 자**가 있습니까?

표 11: 2010년 OWASP 상위 10 위협 목록

웹 애플리케이션 플랫폼과 취약점

웹 애플리케이션 플랫폼 취약점을 집계하는 것은 일반 웹 애플리케이션 취약점을 집계하는 것보다 좀 더 복잡합니다. 웹 애플리케이션 플랫폼을 분석할 때는 기초 플랫폼과 웹 애플리케이션 플랫폼이 사용하는 모든 플러그인을 구별하는 것이 유용합니다. 플러그인은 웹 애플리케이션 업체가 직접 제작하거나 그렇지 않을 수 있습니다. 플러그인은 많은 웹 애플리케이션 플랫폼의 기능을 확장시켜 주지만, 그것이 지원하는 플랫폼만큼 엄격하게 코딩되거나 빨리 업데이트되지는 않을 수 있습니다. 더 중요한 사실은 대부분의 취약점이 플러그인에서 발생한다는 것입니다.

그림 44에는 2010년 상반기에 노출된 주요 웹 애플리케이션 플랫폼과 그 플러그인의 모든 취약점이 각각 차지한 비중(%)이 나와있습니다. 여기에는 노출된 취약점이 10개 이상인 웹 애플리케이션 플랫폼과 관련 플러그인만 포함되었습니다.

주요 웹 애플리케이션 플랫폼과 그 플러그인을 합치면 2010년 상반기에 보고된 전체 취약점 노출 중 거의 14%를 차지합니다.

웹 애플리케이션 플랫폼과 관련하여 노출된 취약점의 대부분은 플러그인(88%) 취약점인 반면, 웹 애플리케이션 플랫폼 자체의 취약점은 12%에 불과합니다.

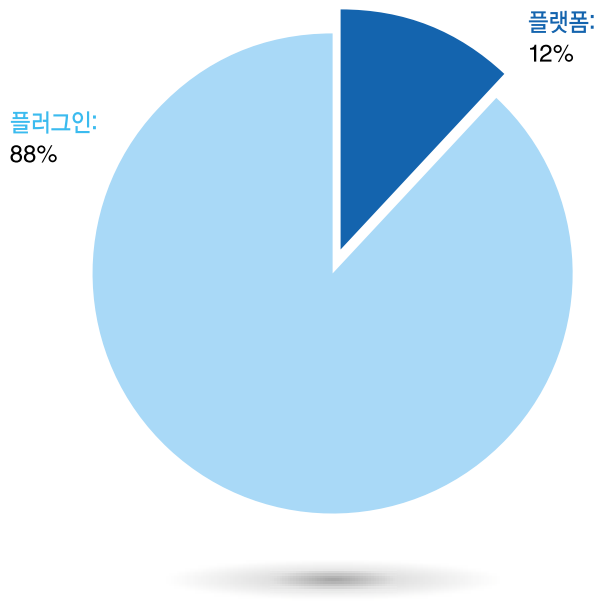


그림 44: 웹 애플리케이션 플랫폼과 그 플러그인에 영향을 미치는 모든 노출된 취약점의 비율, 2010년 상반기

이어지는 그래프에는 노출된 플러그인 취약점과 웹 애플리케이션 플랫폼 취약점의 수가 비교되어 있습니다.

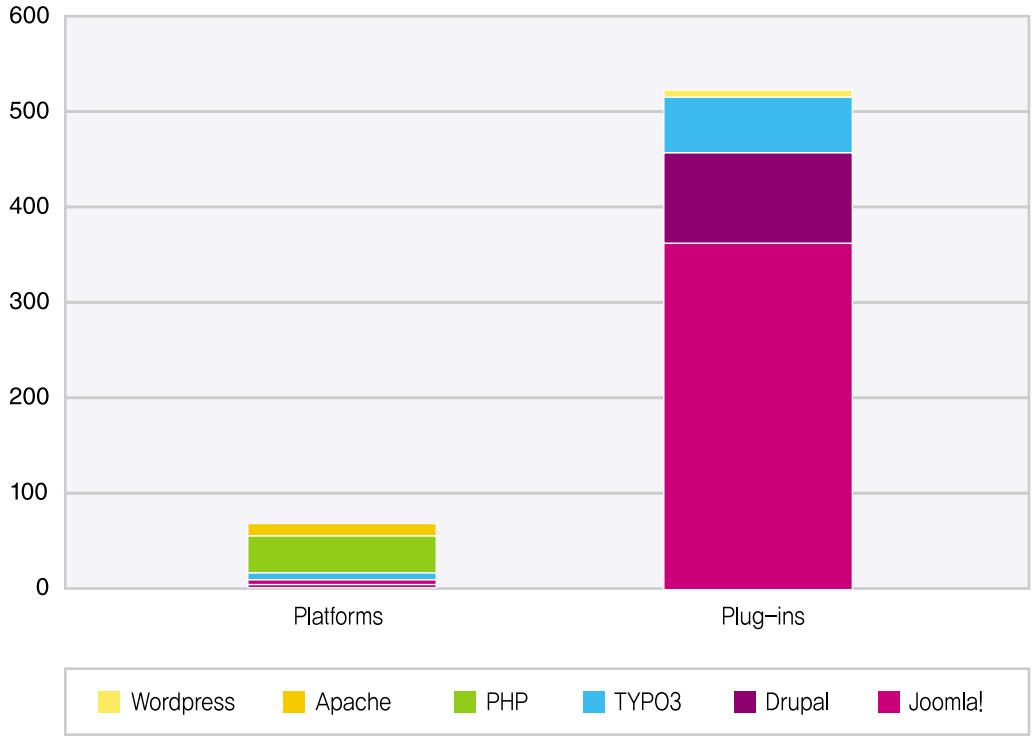


그림 45: 노출된 웹 애플리케이션 플랫폼 취약점과 플러그인 취약점의 비교, 2010년 상반기

배울 수 있는 교훈

웹 애플리케이션 공급업체가 제작하는 코드로 인해 발생하는 취약점은 매우 드물지만, 이런 애플리케이션을 지원하기 위해 제공되는 많은 플러그인에 대한 의존도가 높다면 모든 노출된 취약점을 조사하고 시정하는 데 시간을 투자할 필요가 있습니다. 나아가, 완제품을 배포하기 전에 웹 애플리케이션 스캐너를 사용하여 완전히 진단함으로써 알려지지 않은 취약점이 존재하거나 개발 프로세스 도중에 유입되지 않았는지를 확인한다면 더욱 좋을 것입니다. 이런 애플리케이션을 배포하기 전에 애플리케이션이 안전한 지 확인한다면 웹사이트가 공격자의 공격 기점으로 악용되는 것을 방지하는 데 도움이 될 것입니다.

브라우저 및 기타 클라이언트 측 취약점 및 공격

널리 사용되는 클라이언트 측 소프트웨어 – 치명적이고 위험도가 높은 노출된 취약점의 비율

2009년 연말 보고서에서 클라이언트 측 취약점은 2008년에 비해 5% 감소했습니다. 그러나 PC(퍼스널 컴퓨터)에 영향을 미치는 클라이언트 측 취약점은 여전히 웹 애플리케이션에 이어 두 번째로 가장 큰 취약점 유형으로서, 노출된 전체 취약점 중 약 5분의 1을 차지했습니다.

그림 46에는 현재 다양한 클라이언트 측 애플리케이션에 영향을 미치고 있는 치명적이고 위험도가 높은 노출된 취약점이 유형별로 분석되어 있습니다.

2009년 중반부터 2009년 말까지는 감소 추세가 보이지만, 이는 6개월 치 데이터에 불과하다는 사실을 기억해야 합니다. 2010년 상반기에는 문서 리더 및 편집기와 멀티미디어 응용프로그램이 2009년 연말 합계를 거의 추월했음을 볼 수 있습니다. 브라우저 응용프로그램은 올해 상반기에 작년의 절반 수준을 분명히 넘었으며, 이 추세는 계속될 것으로 보입니다. 2010년에 많은 수의 취약점이 노출된 추세는 연말까지 이어져 역대 기록을 깨트릴 것으로 예상됩니다.

앞에서 언급했듯이 이처럼 기록적으로 많이 노출된 취약점은 공격자들에 의해 적극적으로 악용되고 있으며, 계속 주시해야 하는 중대한 보안 문제를 제기합니다.

클라이언트에 영향을 미치는 주요 취약점 유형은 표 12에 나와있는 4가지 주요 범주 중 하나로 분류됩니다.

범주	설명
브라우저	클라이언트 웹 브라우저 소프트웨어 및 플러그인
문서 리더 및 편집기	사용자가 문서, 스프레드시트, 프레젠테이션 및 기타 이미지, 음악 또는 동영상 이외의 파일 유형을 작성하거나 보기 위해 사용할 수 있는 소프트웨어
멀티미디어	사용자가 음악 및 동영상을 보거나 제작하기 위해 사용할 수 있는 소프트웨어
운영 체제	위의 세 가지 유형에 속하는 애플리케이션을 제외한 기본 운영체제

표 12: 클라이언트 측 취약점 노출과 관련된 주요 취약점 범주

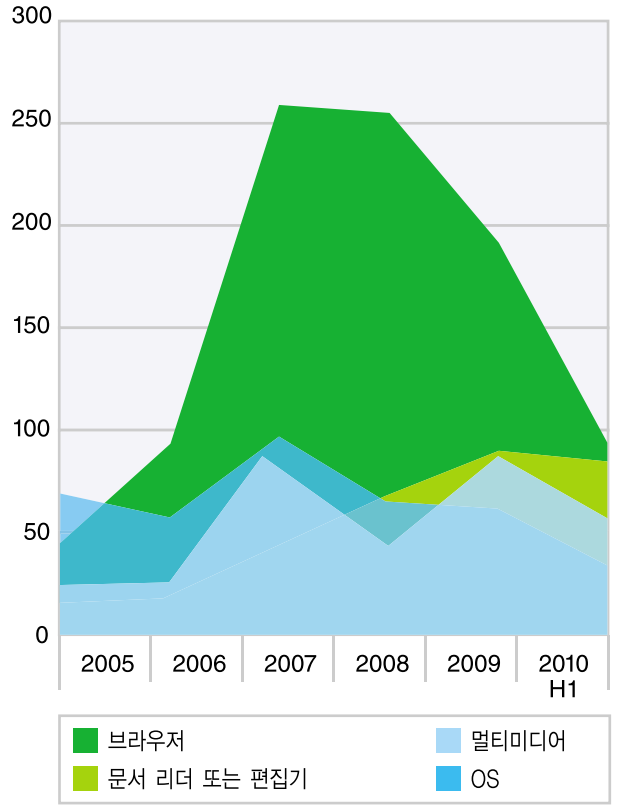


그림 46: 클라이언트 측 애플리케이션에 영향을 미치는 치명적이고 위험도가 높은 노출된 취약점의 애플리케이션 유형별 분석, 2005년~2010년 상반기

브라우저 취약점 – 2010년에 선두로 급부상한 Internet Explorer

가장 큰 클라이언트 측 취약점 유형은 여전히 브라우저 취약점입니다. 여기에는 브라우저 자체뿐만 아니라 브라우저에 설치될 수 있는 여러 플러그인도 포함됩니다. 영향을 받는 ActiveX 컨트롤은 계속 감소하고 있습니다.

올해 노출된 취약점이 증가했다는 데서 예상했을 수 있듯이, Mozilla Firefox와 Microsoft Internet Explorer 취약점의 수는 2010년 상반기에 증가하고 있습니다. 현재 두 브라우저는 노출된 취약점이 비교적 나란히 증가하고 있지만, Internet Explorer는 이미 2009년에 보고된 총 취약점 수의 3분의 2에 다다른 것으로 보입니다.

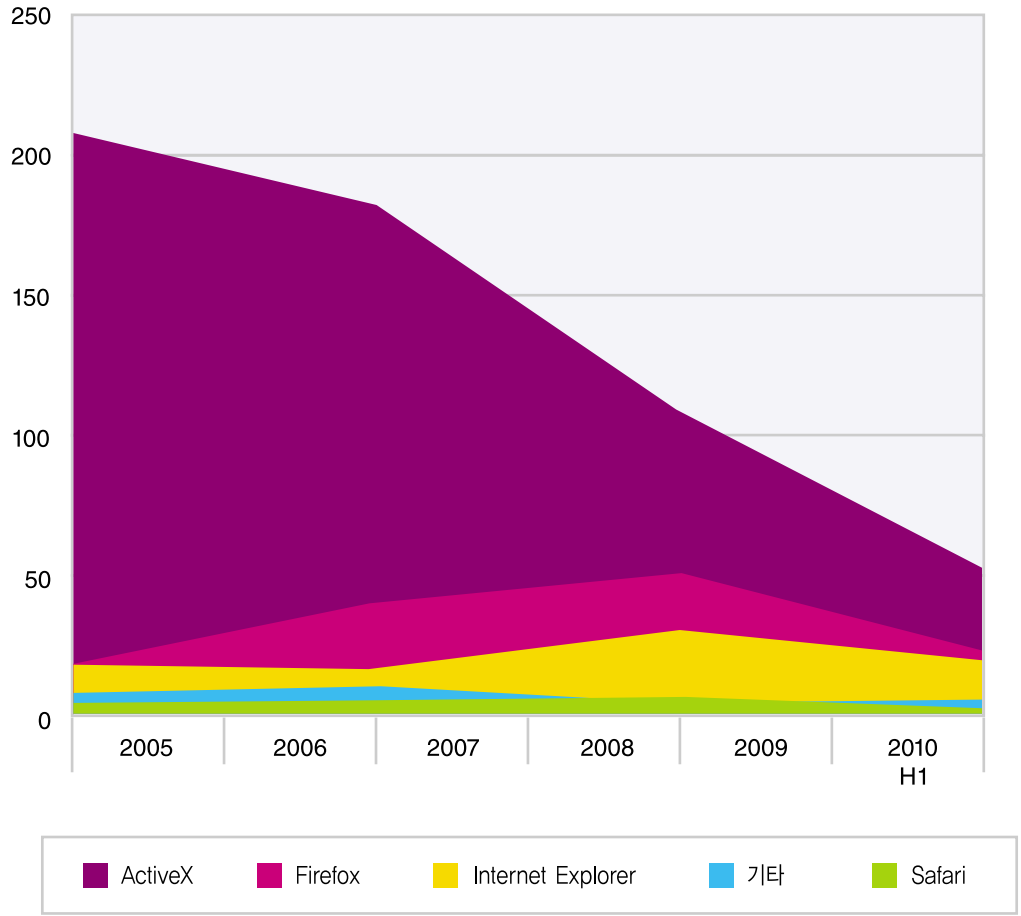


그림 47: 브라우저 관련 소프트웨어에 영향을 미치는 치명적이고 위험도가 높은 노출된 취약점, 2005년~2010년 상반기

문서 형식 취약점

가장 두드러진 두 가지의 문서 취약점 유형은 Office 문서와 PDF(Portable Document Format) 문서 취약점입니다.

이번 상반기 보고서에서 PDF는 2009년 연말 총계의 49%에 달했습니다. 아래 그림 48에서는 오피스 문서 취약점이 감소하고 PDF가 증가하는 추세가 계속되고 있음을 볼 수 있습니다.

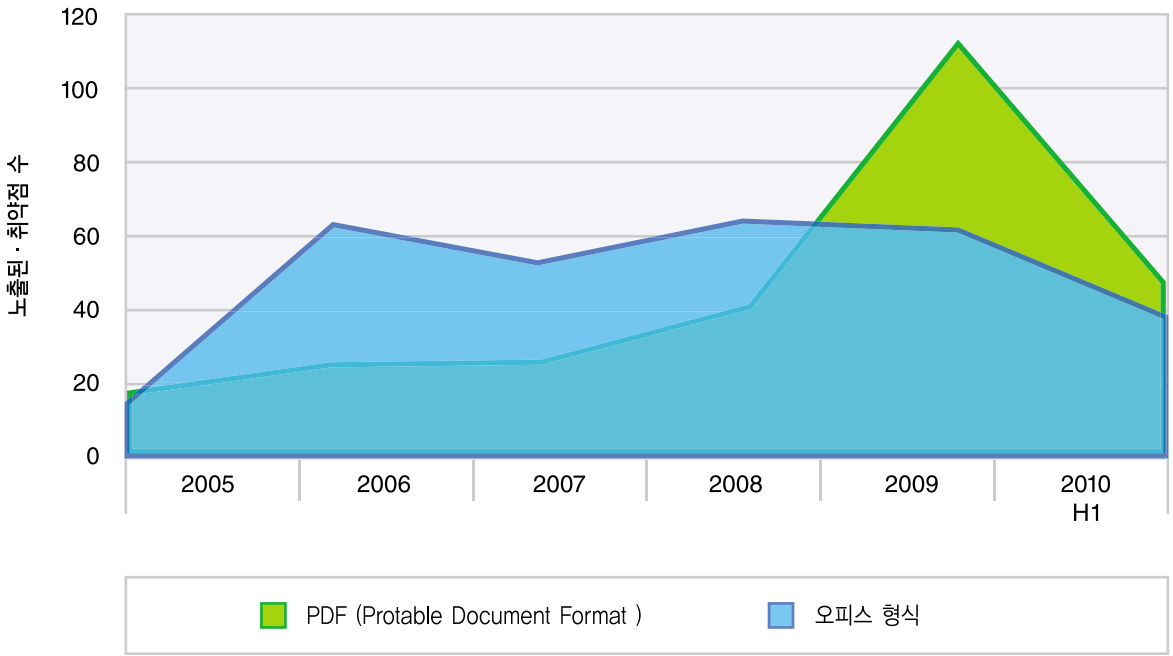


그림 48: 문서 형식 문제와 관련된 취약점 노출, 2005년～2010년 상반기

당사는 전체 위협 환경에 걸쳐 PDF가 많은 공격자에 의해 가장 선호되는 무기가 되었다고 보고했습니다. 당사의 센서들은 올해 2월에 Acrobat 취약점을 공격하여 악성코드를 설치하는 난독화된 PDF 파일이 첨부된 스팸 이메일을 사용한 일련의 공격을 감지했습니다. 당사의 연구원들은 최신 백신과 스팸 필터를 우회하는 여러 가지 방법을 결합한 이 같은 공격에 대해 블로그를 작성했습니다. 4월에 당사 센서는 악성 PDF 스팸의 급증을 또 한 번 감지했습니다. 이 때는 Javascript Launch 명령이 Zeus 봇넷을 피해자의 컴퓨터에 설치하기 위해 사용되었습니다.

보안 전문가들은 이런 공격 방법에 대해 경계를 늦추지 않고 해당 문서가 제기하는 위협에 대해 사용자에게 알려야 할 것입니다.

클라이언트 공격 동향

X-Force는 여러 프로젝트와 서비스를 통해 클라이언트 공격을 모니터링합니다.

- IBM Managed Security Services(MSS)는 말단컴퓨터(Endpoint) 뿐만 아니라 서버(웹 서버 포함) 및 전반적인 네트워크 인프라와 관련된 공격도 모니터링하는 책임을 집니다. 이 데이터는 웹과 더불어 이메일 및 IM(인스턴트 메시지) 등의 다른 경로를 통해 감행되는 공격을 추적합니다.
- 당사의 "Whiro" 크롤러는 MSS와 당사의 "C-Force"와 독립 분석에서 얻어진 데이터를 결합하여 웹 기반 소스 공격을 모니터링합니다. Whiro는 툴킷이 여러 공격을 시도하는 경우를 포함한 가장 난독화가 심한 경우에도 공격을 가려내는 특수 기술을 사용합니다.
- 당사의 컨텐츠 팀은 크롤링과 독립 인식(Discovery) 그리고 MSS 및 Whiro에서 제공하는 피드를 통해 독립적으로 웹을 조사하고 분류합니다.

웹 브라우저 공격 동향

X-Force는 자체적인 Whiro 크롤러를 사용하고 IBM ISS Managed Security Services 운영 경보 데이터를 분석함으로써 웹브라우저 공격의 증가를 계속 추적합니다. 많이 사용되는 웹 공격 툴킷에 대한 유사한 통계 자료를 제작하기로 결정했을 때, 당사는 코드 유사성과 도용 코드로 인해 이것이 가능하지만 까다로울 수 있다는 사실을 알게 되었습니다. 시간이 지남에 따라 당사는 개별 공격과 웹 브라우저 공격 툴킷에서 사용되는 난독화 기법의 동향도 추적해 왔습니다. 당사는 이 분야에서 성과를 개선하기 위해 계속 신기술에 투자하고 있습니다.

실환경(Wild)에서 단독 웹 브라우저 공격 사이트가 죽어가고 공격 툴킷과 그룹이 웹 브라우저 공격의 전면에 나서고 있는 가운데, 몇 가지 우려되는 안티분석의 가능성이 새로 발견되고 있습니다. 특정한 인터넷 프로토콜(IP) 주소로 컨텐츠를 두 번 이상 서빙하는 것을 막는 공격 툴킷은 실환경(Wild)에서 증가하고 있습니다. 이 기능은 공격자에게 1) 감염은 한 번만 일어나므로 피해자의 잠재적인 불안정화가 방지되고, 2) 분석을 방해하는 두 가지의 실질적인 이익을 제시합니다. 이런 필터링 방식은 사실 새로운 것이 아니고 참조자 확인도 마찬가지입니다. 공격을 당한 웹 페이지나 악성 광고의 URL 같은 유효한 참조자가 없는 요청을 차단함으로써 단지 악성 URL을 공유하는 것만으로는 악성 코드의 견본을 획득하기에 충분하지 않습니다.

가장 인기 있는 공격 (2010년 상반기)

1. CVE-2007-5659, PDF Collab.CollectEmailInfo
2. CVE-2009-0927, PDF getIcon
3. CVE-2008-2992, PDF Util.Printf
4. CVE-2007-0071, SWF Scene Count
5. CVE-2008-5353, Java Object Deserialization

Gumblar(공격 툴킷/그룹)의 지속적인 인기로 인해 Adobe 제품은 여전히 1위를 달리고 있지만, PDF와 Flash 공격은 다른 여러 공격 툴킷에서도 매우 인기가 높습니다. ActiveX가 적어도 당분간 5위 목록에서 모습을 감춘 것은 2009년 하반기와 달라진 흥미로운 변화입니다. 2009년 통합 보고서에서 당사는 Adobe 제품이 이 목록에서 계속 상위에 오를 것이라 예상했지만, PDF와 Flash 중 어느 쪽이 더 우세할 것이라고 확실하게 예상하지는 않았습니다. 2010년 현재까지의 상황을 보면, 2010년에는 PDF 공격이 우세할 것으로 예상됩니다.

이와 더불어, 오래된 Java 취약점 하나가 5위에 올라있습니다. Java, PDF 및 Flash가 여러 브라우저 환경에서 공통적으로 사용되고 있다는 점을 고려하면, 공격자들은 특정 브라우저에 한정된 공격에 시간이나 돈을 투자할 필요 없이 IE 이외의 브라우저를 사용하는 사용자를 공격하는 데 관심이 있음을 분명히 알 수 있습니다. 나아가, 공격자들은 주요 브라우저 벤더는 시간이 지남에 따라 길어졌지만 특정 또는 여러 브라우저에 사용되는 플러그인 벤더는 그렇지 않을 수 있는 패치 주기의 변화를 악용합니다. 2010년에 브라우저 플러그인 업체는 과거보다 훨씬 더 빨리 제로데이 공격에 대처하기 시작할 것으로 예상됩니다. 그러나, 패치를 시장에 더 빨리 내놓아도 컴퓨터 사용자가 자동 업데이트 기능이나 통지를 사용하지 않거나 패치 상태를 수동으로 철저히 관리하지 않으면 소용이 없습니다.

가장 인기 있는 공격 툴킷 (2010년 상반기)

1. Gumblar
2. Fragus
3. Eleonore
4. Phoenix
5. JustExploit

인기 있는 공격 툴킷의 표를 작성하는 데는 여러 가지 어려움이 따릅니다. 코드 유사성과 고유한 난독화 기법을 채용한 하위 공격 툴킷의 구분처럼 오래 전부터 있었던 문제는 이 작업을 어렵게 만듭니다. 당사는 난독화를 제거한 악성 컨텐츠에 적용되는 휴리스틱에 기초한 방법으로 순위를 정합니다. X-Force는 얻어진 결과에 대해 전반적으로 자신감을 갖고 있지만, 최신 Neosploit 툴킷은 당사의 공격 크롤러에 약간의 어려움을 제기합니다. Neosploit은 Eleonore와 Phoenix 사이에 위치할 것으로 추정되며, 이렇게 되면 JustExploit이 목록에서 제외될 것입니다. 2009년 상반기 및 통합 보고서에서 가장 인기 있는 공격 툴킷 결과를 되돌아보면, Gumblar가 계속 상위에 랭크되었음을 알 수 있습니다.

비교적 새로운 툴킷인 Fragus는 2위로 급등한 한편, 2009년 하반기에 5위였던 Eleonore는 2010년 상반기에 2위로 올랐습니다. Phoenix는 계속 순위에 오르고 있지만, 이는 하반기 결과가 아닌 한 해 결과를 기준으로 한 것입니다. 당사 동향 보고서의 애독자라면 공격자가 선호하는 툴킷이 시간이 흐름에 따라 꽤 많이 변한다는 것을 알 수 있을 것입니다. 따라서, 2010년 한 해 결과를 예측하기는 어려울 수 있습니다. X-Force는 Gumblar가 계속 1위 자리를 유지할 것이라 생각하며, 앞에서 언급한 바와 같이 JustExploit이 목록에서 탈락할 것으로 예상합니다. 그러나, 어떤 툴킷이 새로 등장하느냐에 따라 나머지 세 툴킷은 계속 굳건히 자리를 지키거나 한 두 개의 입지가 약화될 수 있을 것입니다.

웹 컨텐츠 동향

여기서는 사회 원칙과 기업 정책을 이유로 기업이 원하지 않는 대표적인 "악성" 웹 컨텐츠의 양과 분포를 요약합니다. 이 같은 "악성" 인터넷 컨텐츠는 세 가지 웹 사이트 유형과 관련이 있습니다. IBM 웹 필터 범주는 이들 사이트 유형에 대응됩니다.

웹 필터 범주는 다음 주소에 자세히 정의되어 있습니다.
http://www-935.ibm.com/services/us/index.wss/detail/iss/a1029077?cntxt=a1027244

여기서는 다음을 분석합니다.

- 악성 또는 원치 않는 컨텐츠로 간주되는 웹 컨텐츠의 비율(%)과 분포
- 익명 프록시의 양 증가
- 악성코드 URL로 연결되는 링크가 포함된 웹 페이지

웹사이트 유형	설명 및 웹 필터 범주
성인물	포르노 에로/섹스
사회 일탈	사회 일탈 정치적 극단주의/증오/차별 종파
범죄	익명 프록시 컴퓨터 범죄 / 해킹 불법 행위 불법 약물 악성코드 폭력/극단주의 와레즈 / 소프트웨어 불법복제

표 13: 악성 웹 컨텐츠와 관련된 웹 필터 범주

분석 방법

X-Force는 IBM Security Solutions 웹 필터 데이터베이스에 분류되어 있는 호스트의 수를 집계함으로써 인터넷 컨텐츠 분포에 대한 정보를 수집합니다. 호스트 수 집계는 컨텐츠 분포를 파악하는 방법으로 인정되고 있으며, 가장 현실적인 평가 결과를 제시합니다. 웹 페이지/하위 페이지 집계 등의 다른 방법을 사용하면 다른 결과가 나올 수 있습니다.

IBM Content 데이터 센터는 새로운 웹 컨텐츠 데이터를 지속적으로 검토하고 분석합니다. IBM Content 데이터센터는 매달 1.5억 개의 새로운 웹페이지와 이미지를 분석하며, 1999년 이후 130억 개에 달하는 웹 페이지와 이미지를 분석해 왔습니다.

IBM 웹 필터 데이터베이스에는 68개의 필터 범주와 6,500만 개의 항목이 있으며, 매일 15만 개의 새로운 항목이나 업데이트된 항목이 추가됩니다.

악성 인터넷 컨텐츠의 비율(%)

현재 인터넷의 약 7.2%는 포르노 또는 범죄 웹사이트 같은 악성 컨텐츠를 담고 있습니다.

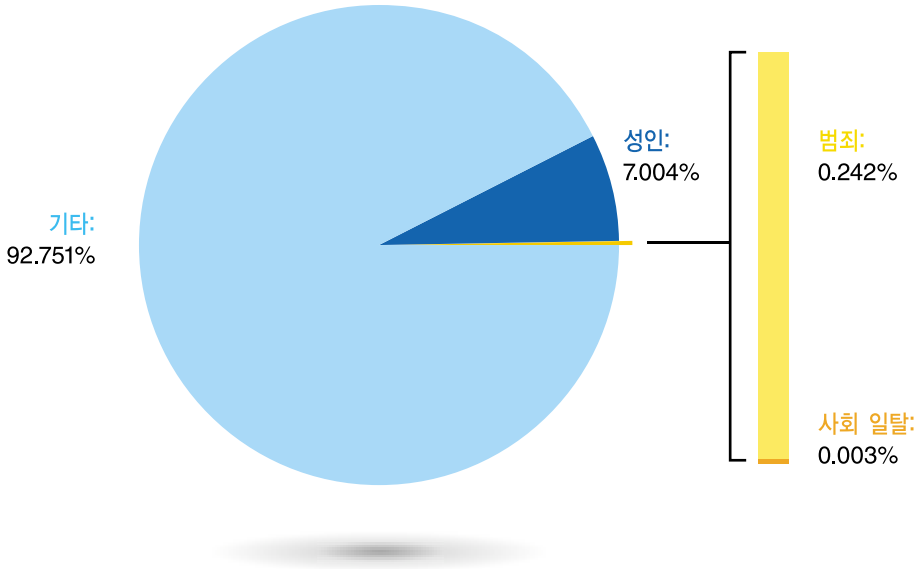


그림 49: 인터넷 컨텐츠 분포, 2010년 상반기

익명 프록시의 증가

인터넷이 가정 생활뿐만 아니라 직장과 학교 생활에서도 점점 큰 비중을 차지함에 따라, 건전한 인터넷 환경을 유지하는 책임을 지는 단체들은 이런 공공 환경에서 사람들이 탐색할 수 있는 사이트를 통제해야 하는 필요성을 점점 많이 느끼고 있습니다.

이런 통제 수단 중 하나는 불건전하거나 부적절한 웹사이트에 접근하지 못하도록 막는 컨텐츠 필터링 시스템입니다. 일부 개인 사용자는 (웹 프록시라고도 하는) 익명 프록시를 사용하여 웹 필터링 기술을 우회하려고 시도합니다.

웹 프록시를 통해 사용자는 원하는 웹사이트를 직접 방문하는 대신 웹 서식에 URL을 입력할 수 있습니다. 프록시를 사용하면 원하는 URL이 웹 필터에 발각되지 않습니다. 웹 필터가 익명 프록시를 모니터링하거나 차단하도록 설정되지 않으면, (정상적인 경우라면 차단되었을) 이 같은 행동은 필터를 우회하게 되고 사용자는 허용되지 않는 웹페이지로 이동할 수 있게 됩니다.

그림 50에 나와있는 익명 프록시 웹사이트의 증가하는 양은 이런 추세를 보여줍니다.

지난 3년 동안 익명 프록시는 꾸준히 증가하여 그 수가 4배 이상 늘어났습니다. 익명 프록시는 사람들이 악의적일 수 있는 의도를 쉽게 숨기기 위해 사용할 수 있기 때문에 중요하게 추적해야 하는 웹사이트 유형입니다.

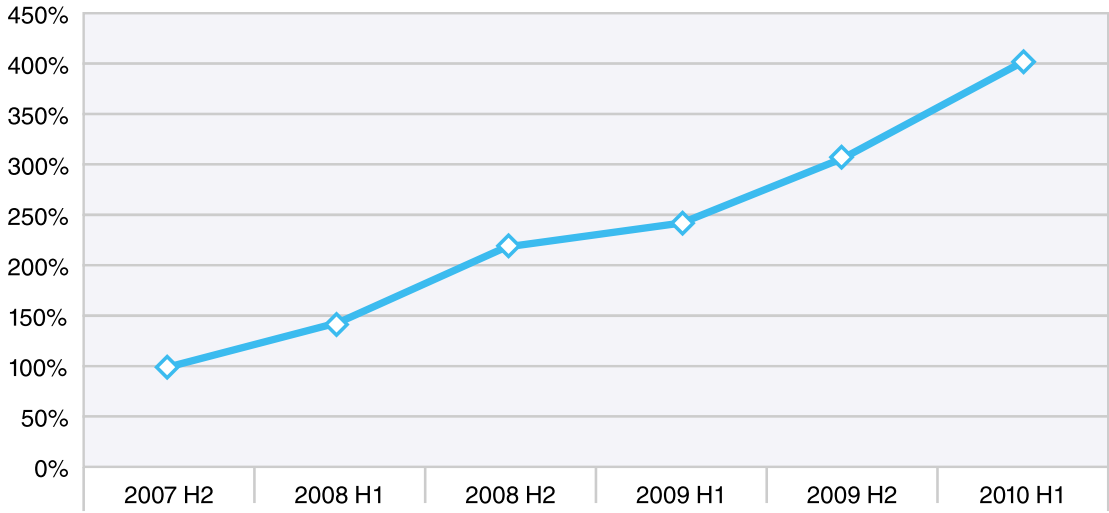


그림 50: 익명 프록시 웹사이트의 양적 증가, 2007년 하반기~2010년 상반기

익명 프록시의 최상위 도메인

그림 51에는 새로 등록된 익명 프록시의 최상위 도메인(TLD)이 나와 있습니다.

2006년에는 새로 등록된 익명 프록시의 60% 이상이 .c●m 도메인이었지만, 2007년 중반 이후에는 .inf●가 2010년 초까지 선두를 유지해 왔습니다. (한편, .c●m은 2위에 오를 때가 많았습니다)

하지만 .inf●가 더 이상 1위가 아닌 이유는 무엇일까요? .inf●는 효과가 입증된 익명 프록시용 TLD로 수 년 동안 애용되어 왔었던 것 같았는데 말입니다. 한 가지 원인은 .c●m과 마찬가지로 사용할 수 있는 이름이 고갈되고 있기 때문일 수 있습니다. 그렇다면 이제는 익명 프록시가 왜 .cc 및 .tk 최상위 도메인에서 제공되고 있는가의 문제가 제기됩니다.

이 두 도메인은 호주령 영토인 코코스 (킬링) 제도(.cc)과 뉴질랜드령 영토인 토켈라우(.tk)의 도메인입니다. .cc 도메인은 VeriSign이 관리합니다. 거의 모든 .cc 익명 프록시 웹사이트는 .c●.cc 도메인에 등록되어 있습니다. .c●.cc 도메인 등록은 무료입니다(http://www.c●.cc/?lang=en 참조). .tk도 마찬가지입니다. (http://www.d●t.tk/참조) 따라서, .c●.cc나 .tk에 새로운 익명 프록시를 설치하는 것은 매우 저렴하고 합리적입니다.

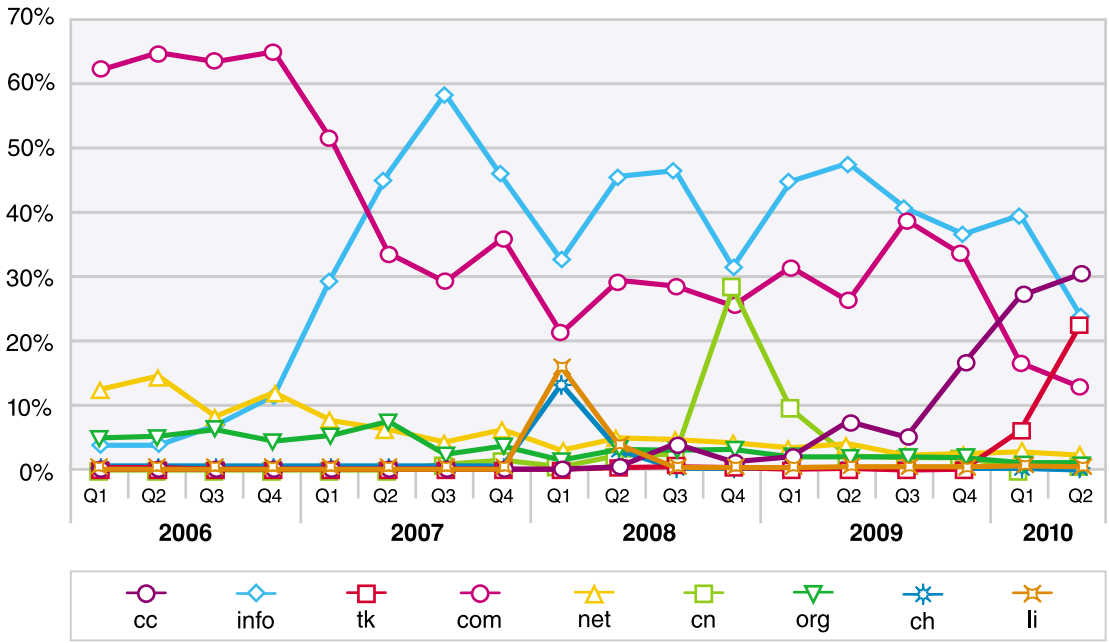


그림 51: 새로 등록된 익명 프록시 웹사이트의 최상위 도메인, 2006년 1분기~2010년 2분기

추가 동향:

- 2008년 초에 이웃 국가인 스위스(.ch)와 리히텐슈타인(.li)의 최상위 도메인은 새로 등록된 익명 프록시 중 약 30%에 사용되었습니다.
- 2008년 4분기에는 중국 최상위 도메인(.cn)이 새로 등록된 익명 프록시 중 30% 가까이에 사용되었습니다.
- 2009년 말에는 .cc(코코스(킬링) 제도)가 크게 증가하기 시작했으며, 2010년 2분기에는 1위까지 오르기도 했습니다.
- 2010년 2분기에는 프록시 세계의 새로운 스타인 .tk(토켈라우)가 새로운 익명 프록시 중 약 23%에 사용되었습니다.
- 같은 기간 동안 .inf●는 크게 감소하여 2007년 초 이후 처음으로 30% 미만을 기록했습니다.
- 2010년 1분기에는 .c●m조차도 처음으로 20% 미만으로 떨어졌습니다.

익명 프록시 웹사이트 호스트 국가

익명 프록시 호스트 국가로는 미국이 수년 간 1위를 유지해 왔습니다. 지난 4년 반 동안 새로 등록된 모든 익명 프록시의 70% 이상은 미국에서 호스팅되었습니다. 이 비율은 2008년 중반부터 2009년 말까지 80% 이상으로 높아졌습니다. 2010년 상반기에는 모든 새로 등록된 익명 프록시 중 75%가 미국에서 호스팅되었습니다.

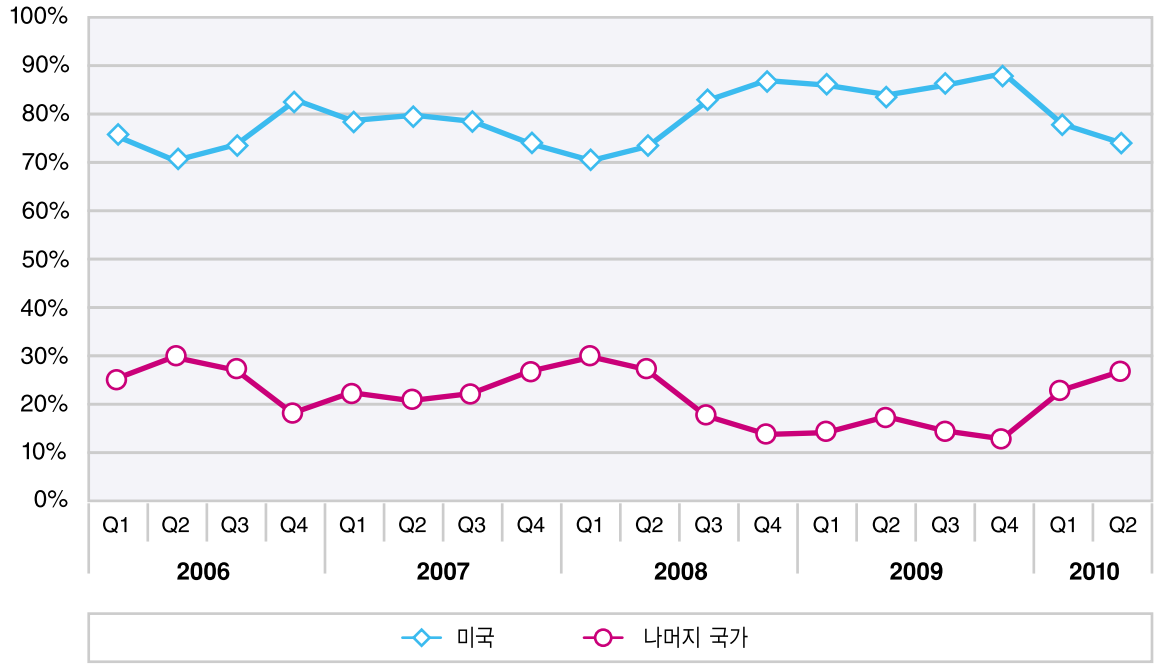


그림 52: 새로 등록된 익명 프록시 웹사이트의 호스트 국가 – 미국과 나머지 국가 비교, 2006년 1분기~2010년 2분기

2010년 상반기에 새로 등록된 나머지 25%의 익명 프록시도 살펴볼 만한 가치가 있습니다. 나머지 국가 중 1위는 1분기에는 캐나다(7.9%), 2분기에는 영국(7.8%)이었습니다. 나머지 모든 국가는 2010년 지금까지 4% 미만을 호스팅했습니다.

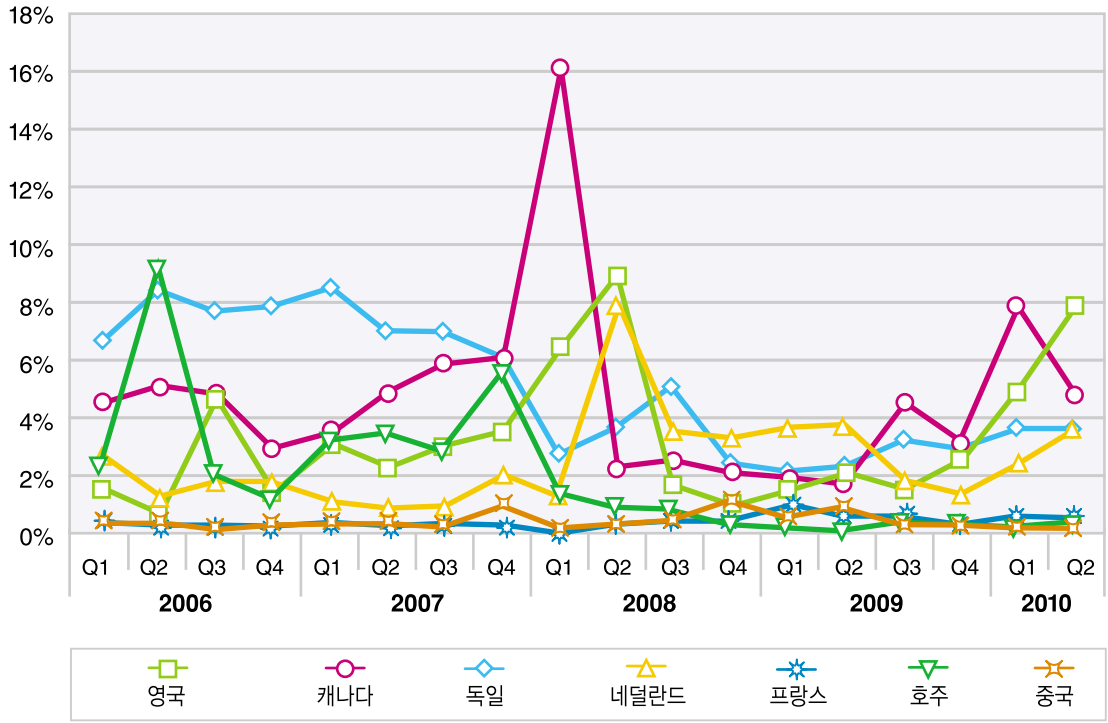


그림 53: 미국 이외의 국가에서 새로 등록된 익명 프록시 웹사이트, 2006년 1분기~2010년

악성 링크가 포함된 건전 웹사이트

71 페이지의 '**웹 애플리케이션 위협 및 취약점**'과 94 페이지의 '**URL 스팸에 가장 많이 사용되는 도메인**'에서 설명하고 있는 바와 같이, 공격자들은 신뢰 받는 웹사이트의 좋은 평판을 악용하여 최종 사용자의 경계를 늦추고 보호 기술이 공격 시도를 감지하지 못하도록 하는 데 점점 많은 노력을 집중하고 있습니다. 악성 웹 컨텐츠의 사용도 다를 것이 없습니다. 이어지는 분석은 알려진 악성 링크로 연결되는 링크를 가장 자주 포함하는 웹사이트의 유형을 간략하게 보여줍니다.

상위 안에 든 몇몇 유형은 예상했던 것일 수 있습니다. 예를 들면, 포르노 사이트는 많은 사람들이 1위일 것이라고 예상했을 것입니다. 포르노 사이트는 실제로 1위이며, 지난 12개월 동안 상황은 더욱 악화되었습니다. 그러나 차상위층 후보는 보다 "신뢰되는" 유형에 속합니다.

블로그, 게시판, 개인 웹사이트, 검색 엔진, 교육, 온라인 잡지 및 뉴스 사이트는 이 차상위층 유형에 해당됩니다. 이런 웹사이트에서는 대부분 사용자가 컨텐츠를 업로드하거나 웹사이트를 직접 디자인할 수 있습니다. 여기에는 대학교 웹사이트에 올린 개인 컨텐츠나 쇼핑 웹사이트에 올린 "구매"에 대한 의견이 포함됩니다. 즉, 이런 유형의 웹사이트가 고의적으로 악성 링크를 호스팅할 가능성은 낮습니다.

사이트 분포에는 아마도 공격자가 아무 것도 의심하지 않는 피해자를 공격하기 위해 이런 악성 링크를 포함시킬 수 있는 (취약점이나 사용자 제공 컨텐츠를 허용하는 영역과 같은) 허점을 발견하기를 기대하고 자주 이용하는 웹사이트 유형이 더 많이 반영되어 있을 것입니다.

그림 54에는 알려진 악성 웹사이트로 연결되는 링크를 하나 이상 호스팅하는 경우가 가장 많은 웹사이트 유형이 열거되어 있습니다.

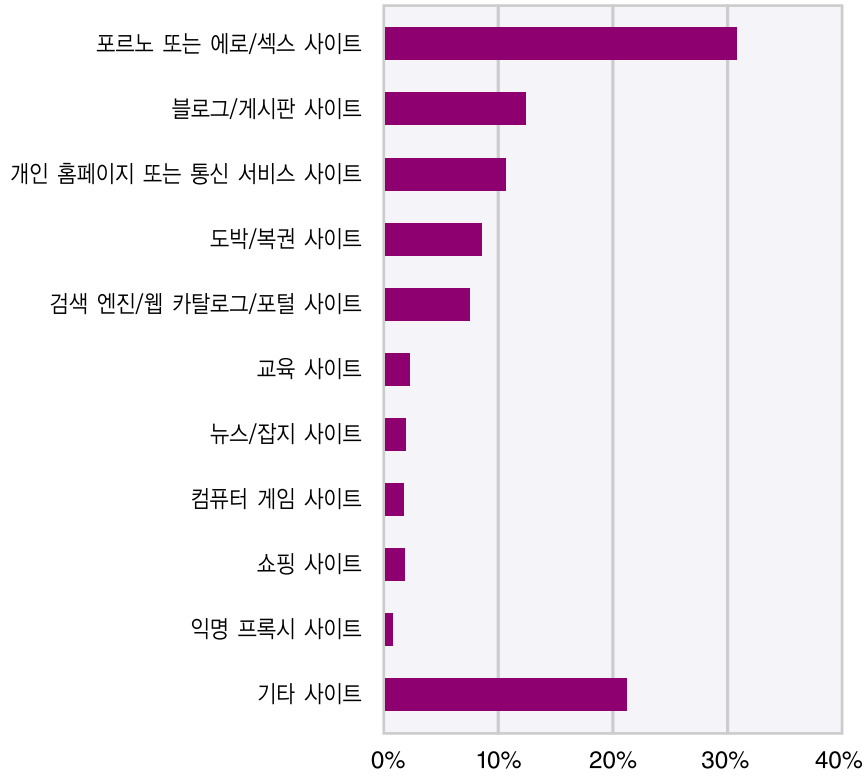


그림 54: 하나 이상의 악성 링크가 포함된 경우가 가장 많은 웹사이트 유형, 2010년 상반기

그림 55와 관련하여, 현재 데이터를 6개월이나 심지어는 12개월 전의 데이터와 비교하면 몇 하지 흥미로운 동향을 발견할 수 있습니다. 포르노나 도박 웹사이트 같은 전문 "악성" 웹사이트는 악성코드로 연결되는 링크를 증가시켰으며, 따라서 "전문가"들이 악성코드를 체계적으로 배포하기 위한 노력을 강화하고 있을 가능성은 더욱 커 보입니다.

블로그와 게시판 역시 악성코드 링크가 증가했습니다. 이는 블로그 및 게시판 소유주가 통제 장치를 불충분하게 갖춰놓은 상태에서 공격자의 침입이 증가했기 때문일 가능성이 높습니다. 이런 추세는 지난 6개월 동안 둔화된 반면, 컴퓨터 게임 및 익명 프록시 사이트에서 악성 링크가 증가하는 추세를 확인했습니다.

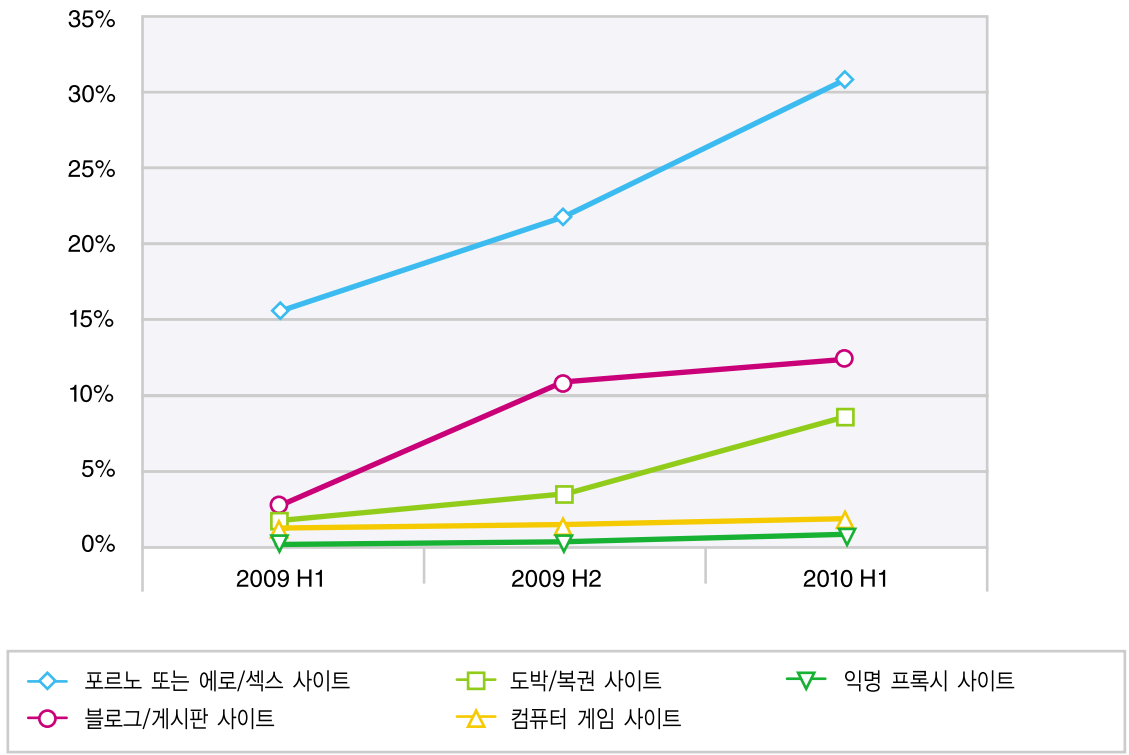


그림 55: 하나 이상의 악성 링크가 포함된 경우가 가장 많은 웹사이트 유형: 감소세에 있는 사이트 유형, 2009년 상반기~2010년 상반기

개인 홈페이지는 더 이상 하나 이상의 악성 링크를 호스팅하는 경우가 가장 많은 웹사이트 유형이 아닙니다. 개인 홈페이지는 2009년 상반기에 비해 개선되었습니다. 그 이유 중 하나는 개인 홈페이지가 소셜 또는 비즈니스 네트워크에 포함된 프로필 같은 웹 2.0 애플리케이션에 밀려 유행이 좀 지났기 때문일 수 있습니다. 검색 엔진, 포털, 쇼핑 사이트, 교육 및 뉴스 사이트도 개선되었습니다. 이런 "전통적인" 합법적 대화식 사이트는 수 년 동안 정보와 의견을 교환하는 데 사용되어 왔습니다. 따라서, 이런 서비스를 제공하는 측은 IT 보안 노력을 강화했을 가능성이 큽니다.

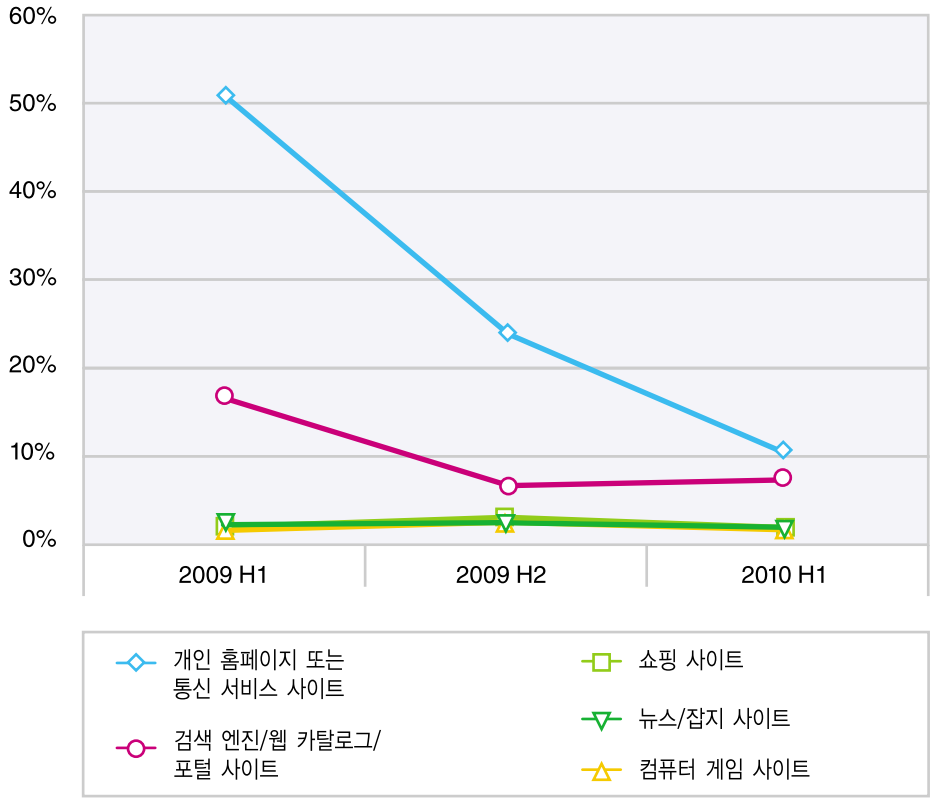


그림 56: 하나 이상의 악성 링크가 포함된 경우가 가장 많은 웹사이트 유형: 감소세에 있는 사이트 유형, 2009년 상반기~2010년 상반기

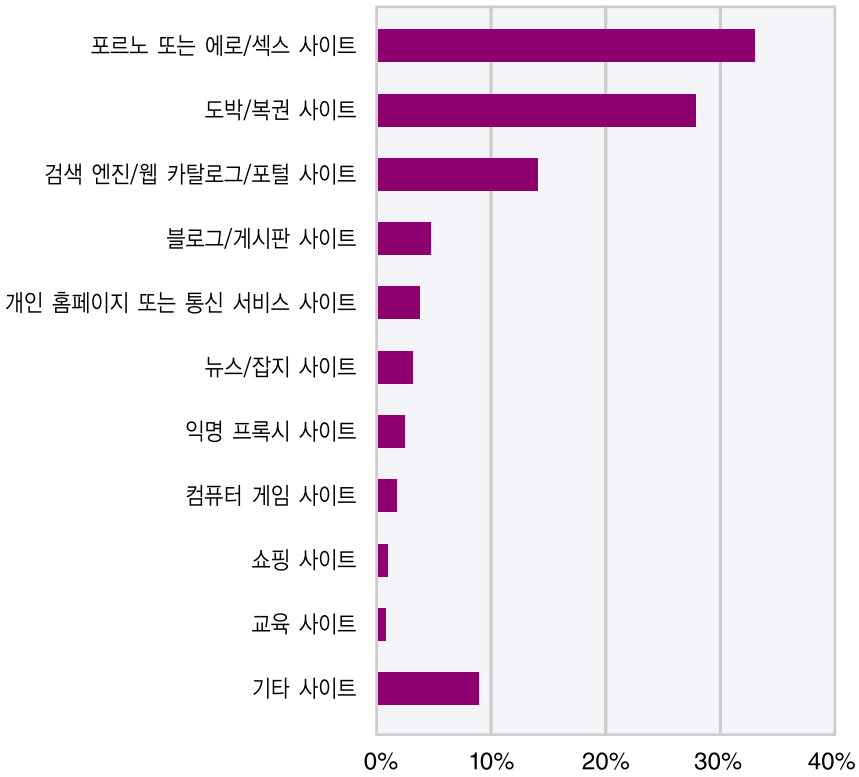


그림 57: 악성 링크를 열 개 이상 포함하고 있는 경우가 가장 많은 웹사이트 유형, 2010년 상반기

이 문제를 바라보는 또 다른 방법은 악성 웹사이트로 연결되는 링크를 매우 많이(10개 이상) 호스팅하는 것으로 보이는 웹사이트를 살펴보는 방법입니다. 10개 이상의 악성 링크를 호스팅하는 사이트를 분석하면 이야기는 달라집니다. 해당 웹사이트의 소유주 중 일부는 이런 불량 행위를 통해 얻을 수 있는 금전적인 이익을 직접 누리고 있다고 의심할 수 있습니다. 악성 링크를 10개 이상 호스팅하는 웹사이트 유형 중에 포르노는 거의 33%를 차지하며, 도박 사이트는 약 28%를 차지합니다. 이런 웹사이트 유형은 악성 링크를 고의적으로 이용하여 이익을 얻고 있다고 의심할 수 있습니다. 일부 사이트에는 링크가 사이트 전체에 걸쳐 체계적으로 배치되어 있는 것으로 보입니다.

6개월 전의 데이터와 비교하면 웹사이트 유형별 변동폭은 대부분 2% 이하였습니다. 하지만 포르노 사이트는 6% 증가하고 도박 사이트는 11.4% 증가했습니다. 따라서 악성코드 배포자들은 인터넷에서 인기가 높은 있는 이런 어둠의 사이트에 점점 많이 집중합니다. 성인 인구의 0.6%가 도박 문제를 겪고 있는 것으로 알려짐에 따라(http://en.wikipedia.org/wiki/Gambling_addiction#Prevalence 참조), 도박 사이트는 악성코드 배포자들의 표적으로 널리 사용되고 있습니다.

스팸

IBM 스팸 및 URL 필터 데이터베이스는 전세계 스팸 및 피싱 공격을 종합적으로 보여주는 뷰를 제시합니다. 컨텐츠 팀은 수백만 개의 이메일 주소를 적극적으로 모니터링함으로써 공격자들이 사용하는 스팸 및 피싱 기술의 여러 발전상을 파악해 왔습니다.

현재 당사의 스팸 및 URL 필터 데이터베이스에는 4,000만이 넘는 주요 스팸 서명이 수록되어 있습니다. 각 스팸 메일은 몇 가지 논리적인 부분(문장, 문단 등)으로 나뉘어집니다. 각 부분과 수백 개의 스팸 URL에 대해서는 고유한 128비트 서명이 계산됩니다. 스팸 필터 데이터베이스에서는 매일 약 1백만 개의 서명이 새로 생성되거나 업데이트되거나 삭제됩니다. 본 절에서 다룰 내용은 다음과 같습니다.

- 스팸의 양
- 스팸 유형의 새로운 추세
- 스팸에 가장 많이 사용되는 도메인
- 스팸에 가장 많이 사용되는 최상위 도메인(TLD)과, 인기 도메인이 그처럼 많이 사용되는 이유
- 스팸 URL의 평판
- 스팸 웹페이지(URL)를 포함한 스팸 발신국[1] 동향
- 스팸의 평균 크기(바이트) 변화
- 가장 많이 사용되는 스팸 제목

스팸의 양

2009년 초에 스팸의 양은 두어 달 동안 정체되었습니다. 2009년 5월에 스팸의 양은 증가하기 시작하여 시간이 지남에 따라 McColo 폐쇄 직전의 스팸량을 초과했습니다.

2009년 4분기에 스패머들은 연말 집중 공격을 시작했습니다. 11월에 이들은 McColo 단속 이전 수준보다 2배나 많은 스팸을 발송했습니다. 2010년에 스패머들은 스팸의 양을 꾸준히 유지하다가 4월에 스팸의 양을 다시 늘리기 시작했으며, 6월에는 드디어 사상 최고치를 경신했습니다.

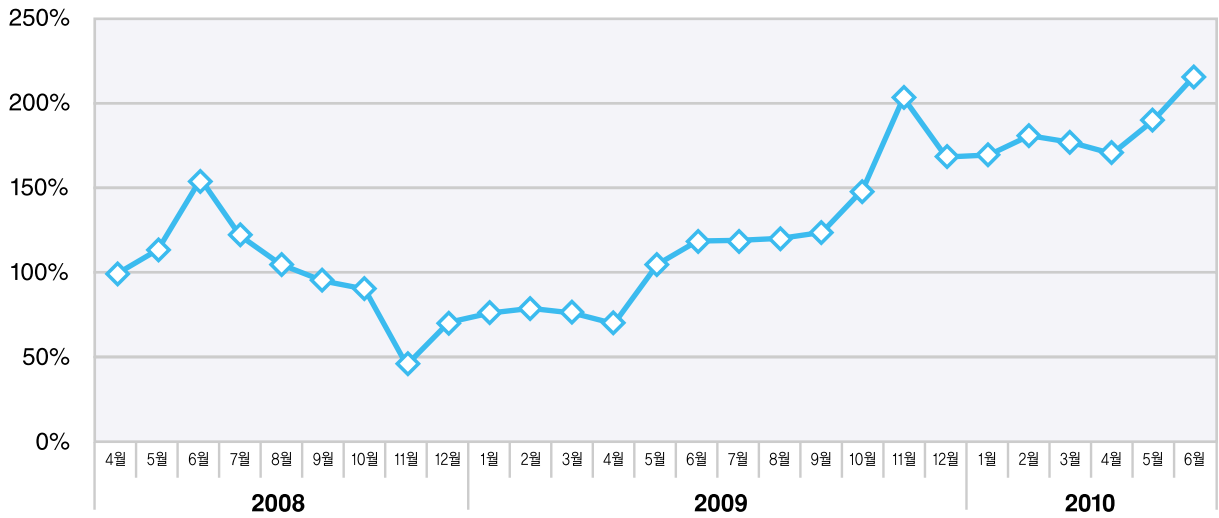


그림 58: 스팸 양의 변화, 2008년 4월~2010년 6월

[1] 본 보고서의 스팸, 피싱 및 URL에 대한 통계에는 WebHosting.Info에서 제공하고 http://www.webhosting.info에서 확인할 수 있는 IP-to-Country 데이터베이스가 사용되었습니다. 지역 분포는(컨텐츠 배포의 경우) 호스트의 IP 주소를 요청하거나(스팸 및 피싱의 경우) 메일 서버를 IP-to-Country 데이터베이스로 보냄으로써 파악했습니다.

스팸의 유형

수 년 동안 스패머들은 가장 의심을 받지 않는 이메일 유형인 첨부파일이 없는 HTML 기반 스팸을 집중적으로 사용해 왔습니다. 아래 그래프는 이 스팸 유형이 2009년 초까지 크게 증가한 한편 (다른 이메일 부분이나 첨부파일이 없는) 일반 텍스트 스팸은 동 기간 동안 감소했음을 보여주고 있습니다.

2009년 2분기부터 HTML 스팸은 81%에서 84% 사이에서 증가 또는 감소했습니다. 2009년 2, 3분기에는 이미지 기반 스팸이 잠시 부활했습니다. 일반 텍스트 스팸은 2009년 말부터 2010년 초까지 증가했습니다. 이와 동시에 이미지 기반 스팸은 감소하여 2010년 상반기에 중요한 역할을 하지 않았습니다.

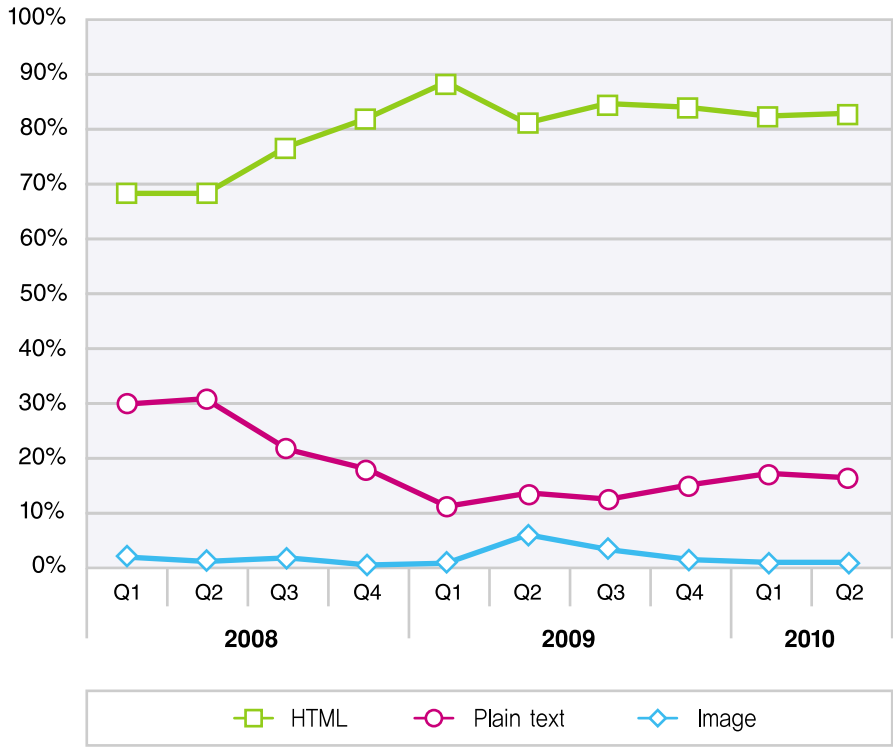


그림 59: 스팸의 유형, 2008년 1분기~2010년 2분기

URL 스팸에 많이 사용되는 도메인

스팸의 거의 대부분(90% 이상)은 URL 스팸, 즉 독자가 클릭하면 스팸 컨텐츠를 보게 되는 URL이 포함된 스팸 메시지로 분류됩니다.

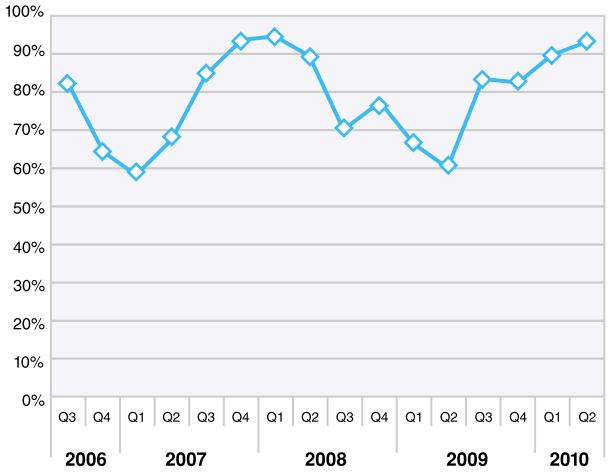


그림 60: URL 스팸, 2006년 3분기~2010년 2분기

따라서, URL 스팸에 가장 많이 사용되는 도메인명을 더 자세히 살펴볼 필요가 있을 것입니다. 표 14에는 2010년 상반기에 가장 많이 사용된 10대 도메인이 월별로 나와 있습니다. 유명하거나 등록된 지가 오래되었지만 스팸 컨텐츠 호스트 도메인으로 등록되지 않은 도메인은 하이라이트되어 있습니다.

순위	2010년 1월	2010년 2월	2010년 3월	2010년 4월	2010년 5월	2010년 6월
1.	flickr.com	radikal.ru	livefilestore.com	livefilestore.com	imageshack.us	imageshack.us
2.	imageshack.us	imageshack.us	imageboo.com	imageshack.us	mageshost.ru	imageshost.ru
3.	radikal.ru	ivefilestore.com	radikal.ru	imageshost.ru	myimg.de	pikucha.ru
4.	livefilestore.com	flickr.com	imageshack.us	mgur.com	xs.to	imgur.com
5.	Webmd.com	live.com	googlegroups.com	myimg.de	imgur.com	myasvir.com
6.	picsochka.ru	imageboo.com	live.com	xs.to	tinypic.com	mojoimage.com
7.	live.com	capalola.biz	akamaitech.net	icontact.com	livefilestore.com	myimg.de
8.	superbshore.com	feetorder.ru	gonestory.com	tinypic.com	icontact.com	twimg.com
9.	tumblr.com	laughexcite.ru	bestanswer.ru	live.com	googlegroups.com	icontact.com
10.	fairgreat.com	hismouth.ru	wrotelike.ru	binkyou.com	images-amazon.com	twitter.com

표 14: URL 스팸에 기장 많이 사용된 도메인, 2010년 상반기

이런 도메인명은 유명하고 신뢰되는 것이 대부분이며, 이런 추세는 지난 몇 년 동안 계속 이어져 왔습니다. 그림 61에는 스팸에 사용된 10대 도메인 중 스팸 도메인과 신뢰되는 도메인이 각각 차지했던 비율(%)이 2008년 상반기부터 2010년 상반기까지 나와있습니다.

유명 웹사이트의 예를 들면 다음과 같습니다.

- **akamaitech.net** (Akamai Technologies의 웹사이트)
- **googlegroups.com** (여러 사람이 공통된 관심사에 대해 토론할 수 있는 Google의 무료 서비스)
- **icontact.com** (이메일 마케팅 서비스 제공업체)
- **images-amazon.com** (Amazon.com, Inc. 소유 도메인)
- **live.com** (사용자가 개인 홈페이지를 만들기 위해 사용할 수 있는 Windows Live 서비스)
- **livefilestore.com** (Microsoft의 웹 스토리지 서비스)
- **tumblr.com** (블로깅 플랫폼)
- **twimg.com** (Twitter 소유 도메인)
- **twitter.com** (Twitter 웹사이트)
- **Webmd.com** (미국의 건강 정보 서비스 제공업체인 WebMD Health Corporation의 공식 웹사이트)

공격 대상이 된 주요 이미지 호스팅 웹사이트는 다음과 같았습니다.

- **flickr.com** (Flickr의 공식 웹사이트)
- **imageshack.us** (ImageShack의 공식 웹사이트)

그 밖에 몇몇 소규모 및 중규모 이미지 호스팅 웹사이트도 있었습니다.

- **imageboo.com**
- **imageshost.ru**
- **imgur.com**
- **mojoimage.com**
- **myimg.de**
- **mytasvir.com**
- **pikucha.ru**
- **radikal.ru**
- **tinypic.ru**
- **xs.to**

위의 웹사이트들은 최종사용자에게 익숙하고 신뢰할 수 있는 웹 링크를 제공할 뿐만 아니라, 스팸 메시지는 이런 합법적인 링크를 스팸 이메일에 사용함으로써 일부 스팸 방지 기술을 성공적으로 우회할 수 있습니다.

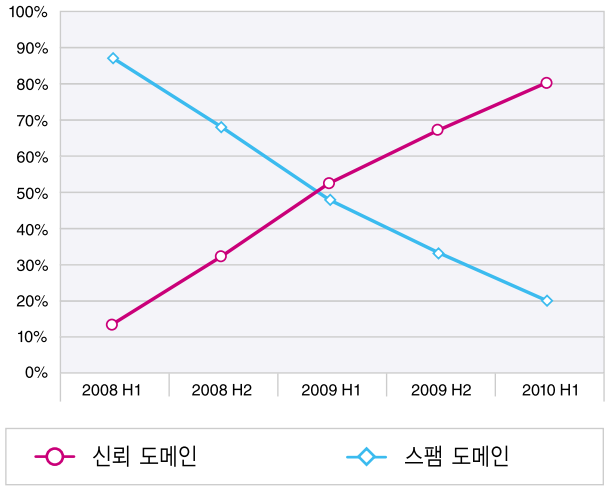


그림 61: 스팸에 사용된 10대 도메인, 스팸 도메인과 신뢰 도메인의 비교, 2008년 상반기~2010년 상반기

최상위 도메인별 무작위 URL의 비율(%)

앞부분에서는 중국이 최근에 도메인명 등록을 엄격하게 제한하기 시작함에 따라 최상위 도메인(TLD)이 어떻게 중국에서 러시아로 옮겨갔는지에 대해 설명했습니다. 이에 대해 더 자세히 알아보기 위해, 무작위 명명 구조를 사용하는 최상위 도메인을 살펴보도록 하겠습니다.

최상위 도메인과 관련하여, (.com과 .net 같은 일반 최상위 도메인과 국가의 최상위 도메인을 비교해 보면 흥미로운 점이 발견됩니다. 스패머들은 메시지가 합법적인 것으로 보이게 하기 위해 여러 가지 기법을 사용할 수 있습니다. 이런 기법 중 하나는 (ibm.com처럼) 합법적인 무작위 도메인명을 사용하는 방법입니다. 많은 경우, 이런 합법적인 URL은 이메일의 HTML 소스 코드에 숨겨져 있습니다. 사용자는 실제 스팸 컨텐츠로 연결되는 URL 하나만 보고 클릭할 수 있습니다.

(.cn, .ru, .es 같은) 국가 코드 최상위 도메인을 분석해 보면, 이는 무작위로 사용되지 않습니다. .com 주소와 같은 일반 최상위 도메인(gTLD)과는 달리, 이런 URL은 스팸 메시지에 사용될 경우 거의 100%가 실제로 스팸 컨텐츠를 호스팅(하거나 스팸 컨텐츠로 자동으로 이동)합니다. 그림 62에는 (스팸 컨텐츠를 호스팅하지 않고) 무작위 도메인을 가장 자주 사용하는 일반 TLD가 나와있습니다. "무작위 도메인"이란 말은 도메인의 이름이 도메인의 실제 존재 여부와 관계없이 무작위로 선택됨을 의미합니다.

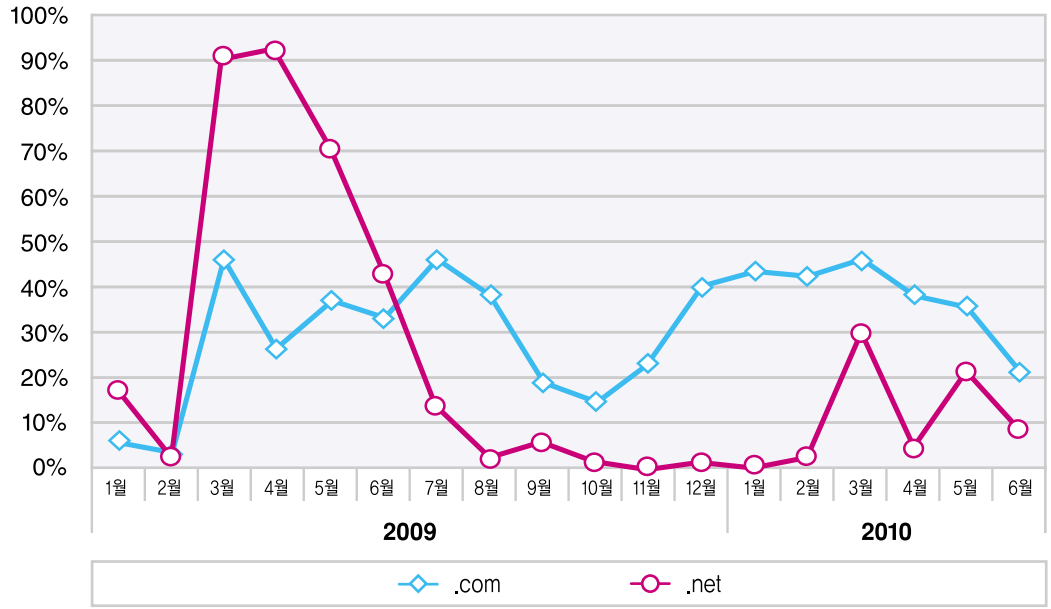


그림 62: 최상위 도메인별 무작위 URL의 비율(%), 2009년 1월~2010년 6월

그림 62에서 볼 수 있듯이, 스팸 이메일에서 발견된 .net URL은 일반적으로 무작위로 생성된 것이었습니다. 허위 URL은 2009년 봄과 여름 내내 스팸에 더 많은 합법성을 부여했습니다. 하지만 2009년 8월 이후 무작위 .net URL의 사용은 2010년 3월까지 거의 완전히 멈췄습니다. 그 후로 스패머들은 .net URL을 다시 널리 사용하기 시작했습니다. 2010년 3월에 스팸에 포함된 .net URL 중 약 30%는 무작위로 생성된 것이었습니다. 2010년 5월에는 스팸에 포함된 .net URL 중 약 20%가 무작위로 생성된 것이었습니다.

무작위 .com URL은 계속 사용되어 왔습니다. 대부분의 경우에는 이런 URL 중 60~80%만 실제로 스팸 컨텐츠를 호스팅하는 것이었으며, 20~40%는 무작위로 선택된 것이었습니다. 따라서, 이 방법은 스패머들이 메시지를 합법적인 것처럼 보이게 하기 위해 여전히 많이 사용되고 있다고 할 수 있습니다.

스팸 URL의 평판: 다시 인터넷으로 연결되는가?

실제 스팸 컨텐츠를 호스팅하는 거의 모든 스팸 URL은 새로 등록된 도메인에서 발송됩니다. 과거에 인터넷 크롤링을 통해 알려졌던 스팸 URL이 발견되는 경우는 드뭅니다. 이 문제를 바라보는 또 다른 방법은 평판 순위를 사용하는 방법, 즉 스팸이 인터넷의 다른 부분으로 연결되는지를 확인하는 방법입니다. 그림 63에는 다른 URL로 연결되는 링크가 포함된 스팸 URL의 비율(%)이 나와있습니다.

그림 63에서 볼 수 있듯이, 스패머들은 인터넷의 다른 부분으로 연결하지 않는 경향이 있습니다. 2008년 상반기에는 전체 스팸 URL 중 약 6%에 링크가 포함되어 있었습니다. 그 전후에는 웹의 다른 부분으로 연결되는 스팸 URL이 2% 미만이었습니다.

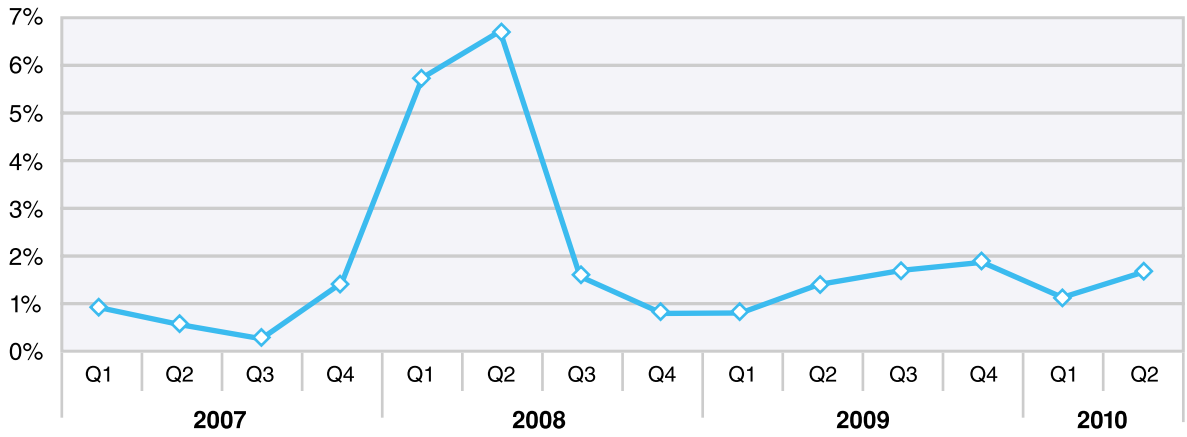


그림 63: 링크가 포함된 스팸 웹페이지의 비율(%), 2007년 1분기~2010년 2분기

그러나, 스패머들은 2009년 내내 다른 링크가 포함된 스팸 URL의 비율을 서서히 늘렸습니다. 2010년 초에 이 비율은 다시 1.1%로 낮아졌지만, 2010년 중반에는 다시 2%에 육박했습니다. 그럼 이제는 스팸이 어떤 종류의 URL로 연결되는지를 더 자세히 살펴보도록 하겠습니다.

그림 64에는 URL이 2가지 유형으로 나뉘어져 있습니다. 하나는 건전 유형(예: 일반 기업, 쇼핑, 소프트웨어/하드웨어 등)이며, 다른 하나는 악성 유형(포르노, 악성코드, 익명 프록시 등)입니다.

대부분의 링크는 건전 URL로 연결됩니다. 그 이유는 스패머들이 자신의 스팸 URL에 대해 좋은 평판 점수를 얻고자 하기 때문인 것으로 보입니다. 어떤 경우든, 링크를 포함하고 있는 스팸 URL은 (현재) 2% 미만이라는 사실을 기억하는 것이 중요합니다.

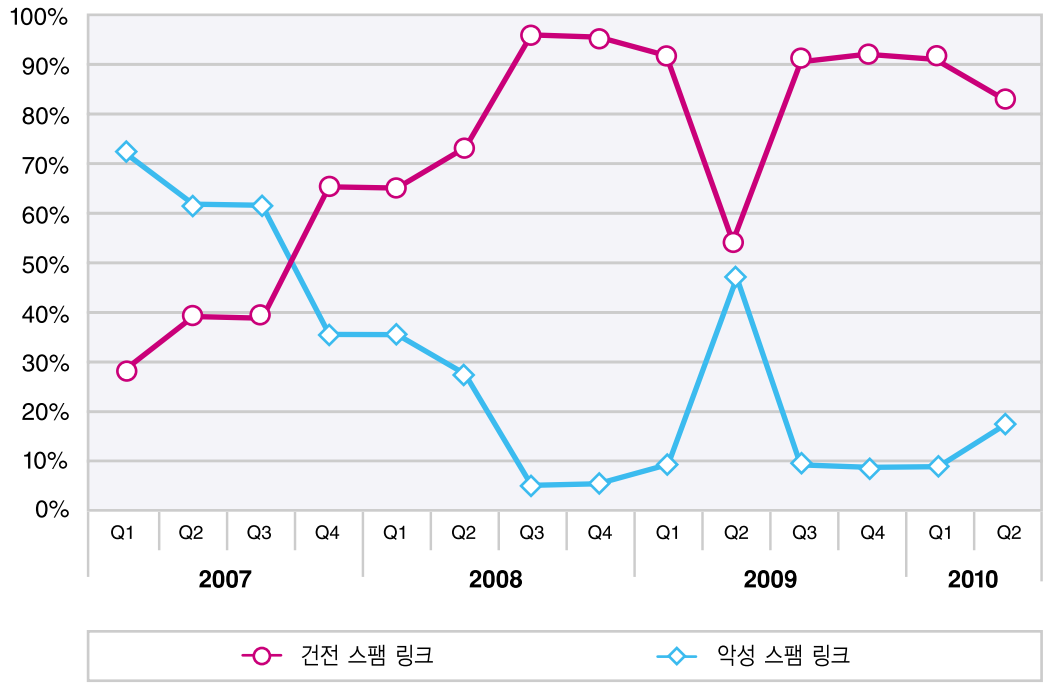


그림 64: 스팸 URL 링크, "건전" 웹사이트 또는 "악성" 웹사이트로 연결하는 경향, 2007년 1분기~2010년 2분기

스팸 URL이 연결하는 웹사이트 유형

분석에서는 인터넷에 연결되는 스팸 URL의 대부분이 전통적으로 "건전한" 웹사이트로 연결하는 경향이 있다는 결론이 나왔습니다. 그러나, 데이터를 당사가 정한 68개 유형으로 나눌 경우 가장 자주 사용되는 웹사이트 유형은 "악성" 유형에 해당하는 포르노 사이트인 것으로 나타났습니다. 그림 65에는 다른 링크와 비교한 포르노 링크의 비율(%)이 나와있습니다. 포르노 유형 하나가 한 때(2007년 상반기)는 전체 건전 웹사이트보다 많았다는 점을 주지하십시오. 지난 9개월 동안에는 스팸 URL에 포르노 링크를 더 많이 포함시키는 경향이 약간 있었습니다. 포르노 링크를 포함한 스팸 URL의 비율은 각 분기에 약 1% 정도 증가했습니다.

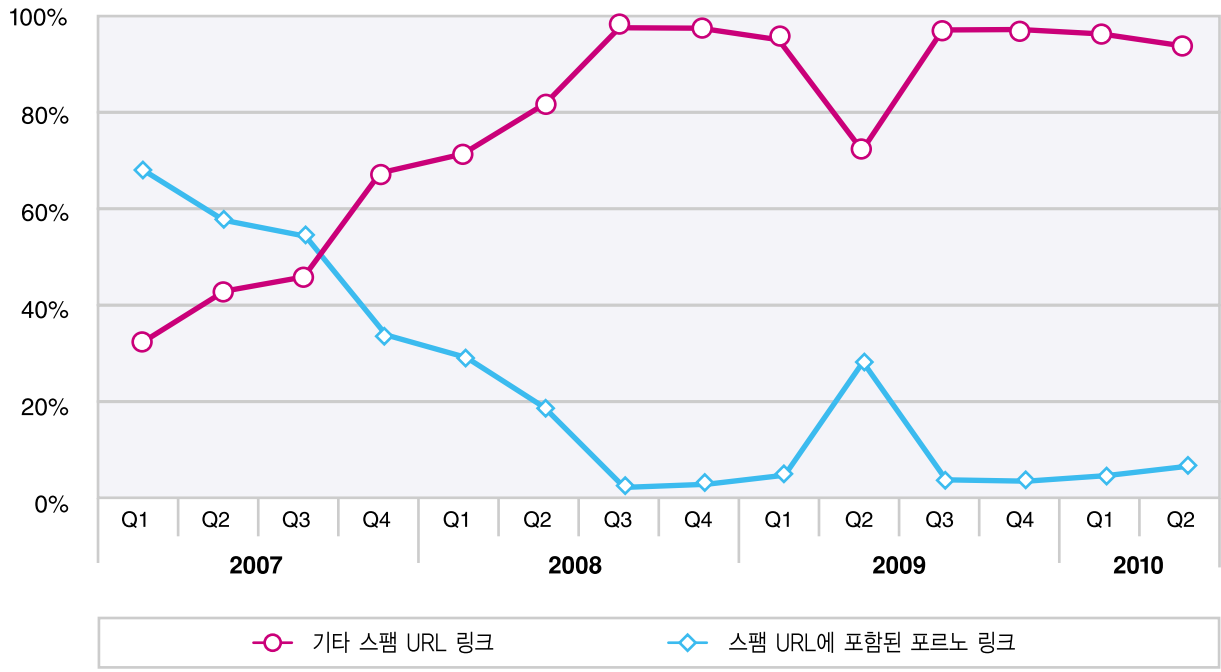


그림 65: 포르노 – 스팸 URL에서 가장 많이 사용되는 링크 유형, 2007년 1분기~2010년 2분기

나머지 주요 유형은 일반 기업, 소셜 네트워킹 및 쇼핑 등의 건전 유형입니다. 2008년 말에 소셜 네트워킹은 처음으로 중요한 역할을 하여 링크로 연결된 전체 URL 중 18% 이상을 차지했습니다. 소셜 네트워킹 링크는 2009년 상반기에 감소했지만, 2009년 말에는 소폭 증가하여 거의 2%에 달한 후 2010년 2분기에는 1.4%로 다시 감소했습니다. 2010년 상반기에 스패머들은 스팸 URL의 평판을 높이기 위해 일반 기업 및 쇼핑 사이트를 더 많이 사용했습니다.

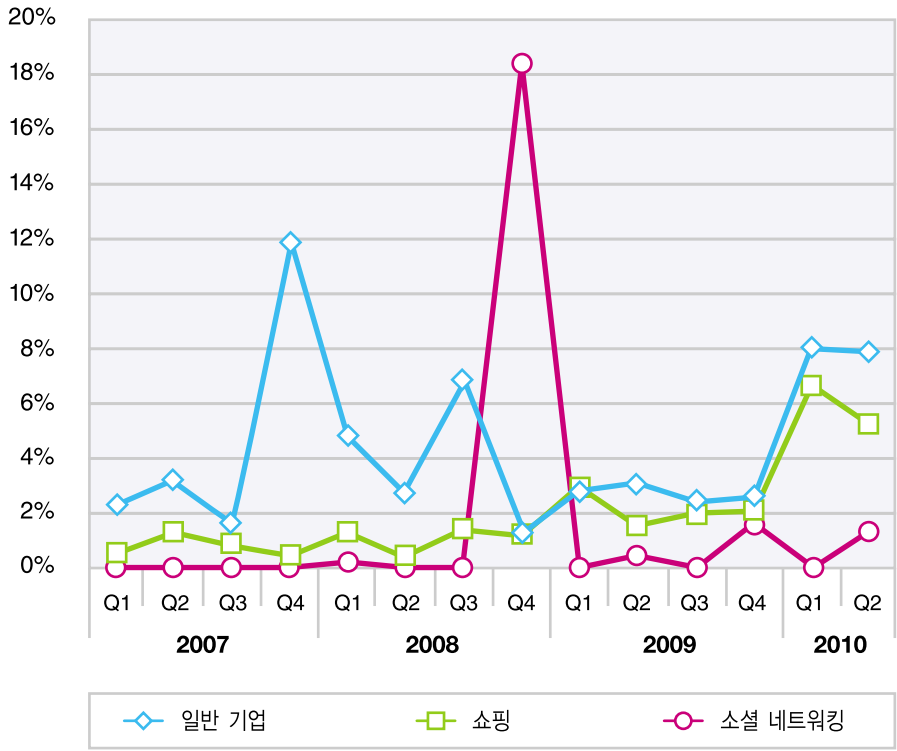


그림 66: 기타 스팸 URL에서 많이 발견된 링크 유형, 2007년 1분기~2010년 2분기

스팸 URL – 발신 국가

표 15에는 2010년 상반기 전세계 스팸 발신 국가[2] 순위가 열거되어 있습니다. 브라질과 미국과 인도는 전세계 스팸의 4분의 1 이상을 차지합니다. 미국은 다시 한 번 1위에 올랐으며, 브라질은 2위에 머물렀습니다. 인도는 3위 자리를 유지했으며, 러시아는 베트남을 따돌리고 4위로 올라서고 베트남은 한국은 밀어내고 5위에 올랐습니다. 독일, 영국, 우크라이나 및 루마니아는 10위 명단에 처음 진입한 반면, 2009년에 명단에 올랐던 폴란드, 터키, 중국 및 콜롬비아는 2010년 상반기 10대 스팸 발신 국가 명단에서 제외되었습니다.

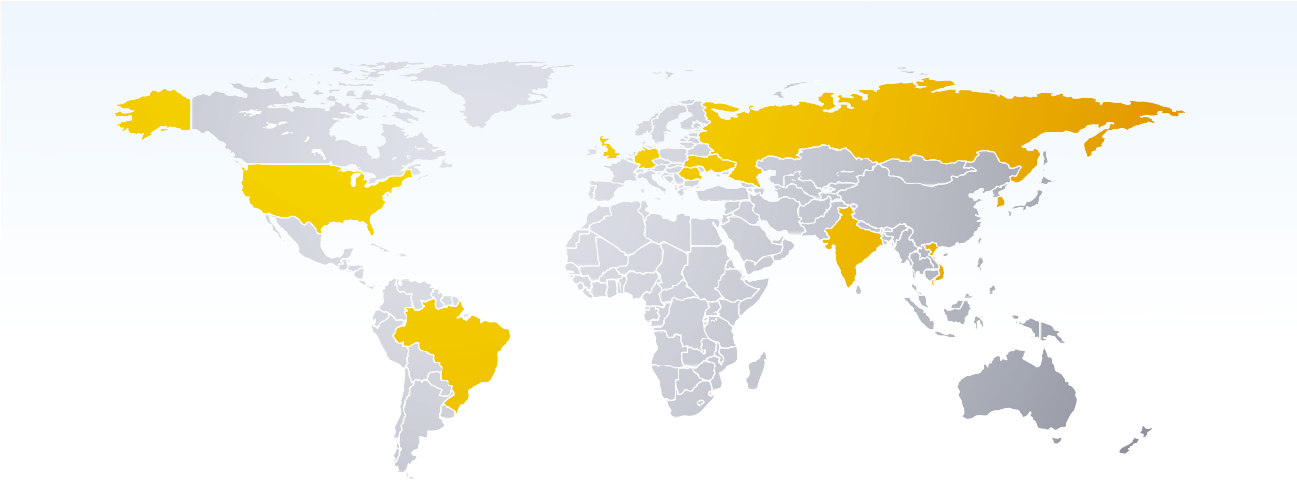


그림 67: 스팸 발신자의 지리적 분포, 2010년 상반기

국가	스팸 비율 (%)
미국	9.7%
브라질	8.4%
인도	8.1%
러시아	5.3%
베트남	4.6%

국가	스팸 비율 (%)
한국	4.1%
독일	3.7%
영국	3.3%
우크라이나	3.1%
루마니아	3.0%

표 15: 스팸 발신자의 지리적 분포, 2010년 상반기

[2] 발신 국가는 스팸 이메일을 보낸 서버의 위치를 의미합니다. X-Force는 대부분의 스팸 이메일이 봇 네트워크(bot network)에 의해 발송된다고 믿습니다. 봇은 어디서나 제어할 수 있기 때문에 실제 스팸 이메일 공격자의 국적은 스팸 발신 국가와 다를 수 있습니다.

분석 기간을 단축하고 이전 년도를 포함시키면 몇 가지 동향이 눈에 띄게 됩니다. 2009년에 브라질은 1위였고 비율도 더 높아졌었습니다. 브라질을 제외하고, 베트남은 2009년 4분기에 전체 스팸 중 9% 이상을 발송한 유일한 국가였습니다. 반면에, 미국, 러시아 및 터키는 스팸 발신 국가로서의 중요성이 훨씬 낮아졌습니다. 하지만 2010년 상반기에 브라질은 크게 감소한 반면 미국은 반등했습니다. 베트남도 입지가 줄어들었으며, 인도는 1년 넘게 계속 증가세를 나타내고 있습니다. 2010년 2분기에 인도는 처음으로 2위에 올랐으며, 1위와의 격차는 0.6%에 불과했습니다.

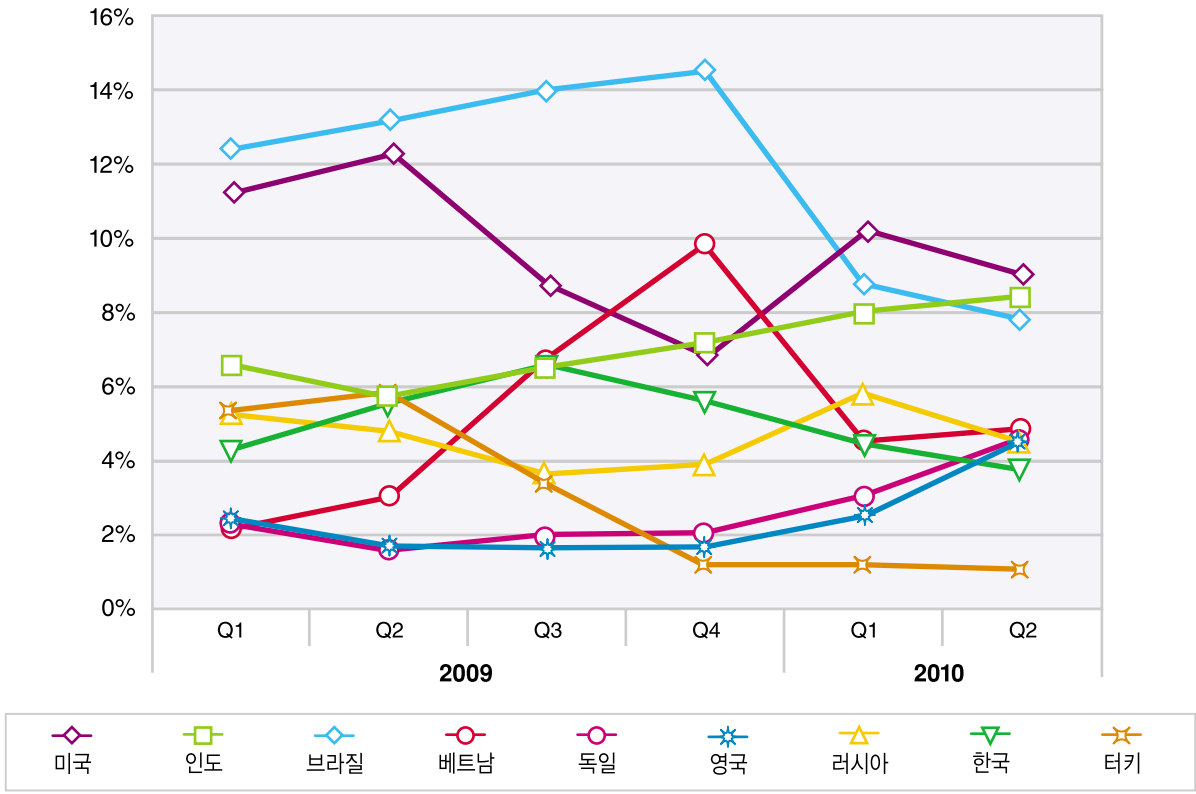


그림 68: 분기별 스팸 발신 국가 분석, 2009년 1분기~2010년 2분기

BRIC 국가의 성장

BRIC[3] 국가인 브라질과 인도에서는 스팸과 피싱 산업이 급격히 성장했습니다. 2010년 상반기에 브라질은 1위 피싱 발신국이었습니다(자세한 사항은 다음 절 참조). 나머지 두 BRIC 국가인 러시아와 중국은 이에 그치지 않았습니다. 앞 페이지의 그림 66에서 봤듯이, 러시아의 최상위 도메인 **.ru**는 스팸 컨텐츠를 호스팅하는 데 가장 많이 사용되는 TLD입니다. 그리고 표 16에 나와있듯이 중국은 스팸 URL의 최대 호스트 국가입니다. BRIC 국가에서 스팸과 피싱은 다른 여러 산업과 함께 급격히 성장하고 있는 2가지 산업입니다.

하지만 왜 베트남과 브라질일까요? 최다 스팸 발신국 순위에 오르기 위해 충족되어야 하는 2가지 주된 조건은

- 인터넷 사용 인구의 급속한 증가와
- 많은 인구라 할 수 있습니다.

브라질과 베트남은 두 가지 조건을 모두 충족합니다. 브라질은 2.10억 명의 인구 중 38%가 인터넷을 사용합니다. 브라질의 인터넷 사용 인구는 지난 10년 동안 1,419% 넘게 증가했습니다.[4] 베트남에서는 9000만 인구 중 27%가 인터넷을 사용합니다. 이 수치는 지난 10년간 12,035% 넘게 증가한 것입니다.[5] 이 같은 증가로 인해 다수의 무경험자가 PC를 사용하게 되었으며, 이런 사용자의 PC는 패치가 적용되거나 보호될 가능성이 상대적으로 낮을 수 있습니다. 아니면 이런 사용자는 소셜 엔지니어링을 통한 속임수에 더 잘 넘어갈 수 있으며, 그로 인해 사용자의 PC를 봇넷 로봇으로 만들 수 있는 악성코드에 더 취약하게 노출될 수 있습니다. 스패머들은 독일과 영국 같은 선진국에서도 입지를 넓혔다는 사실을 지적할 필요가 있을 것입니다. 두 국가 모두 2010년 2분기에 스팸 발신 점유율이 4% 이상으로 증가했습니다.

그 이유로는 다음을 들 수 있을 것입니다.

- PC를 사용하는 무경험자의 지속적인 증가.
- 잘 보호된 시스템까지도 우회하여 PC를 봇넷 로봇으로 만드는 데 성공하는 바이러스의 지속적인 증가.
- 경험이 많은 사용자조차도 널리 사용되는 소프트웨어 제품에서 발견되는 취약점의 극적인 증가로 인해 안전하지 않습니다.

앞의 18페이지에서 봤듯이 2010년 상반기에는 보고된 취약점이 크게 증가했으며, 신흥 경제국인 BRIC 국가들도 이런 증가 추세에서 제외되지 않았습니다

[3] BRIC는 경제가 급성장하는 브라질, 러시아, 인도 및 중국을 의미하는 약자입니다.
[4] http://www.internetworldstats.com/stats15.htm
[5] http://www.internetworldstats.com/stats3.htm

스팸 URL – 호스트 국가

표 16에는 스팸 URL이 호스팅되는 위치가 나와있습니다.

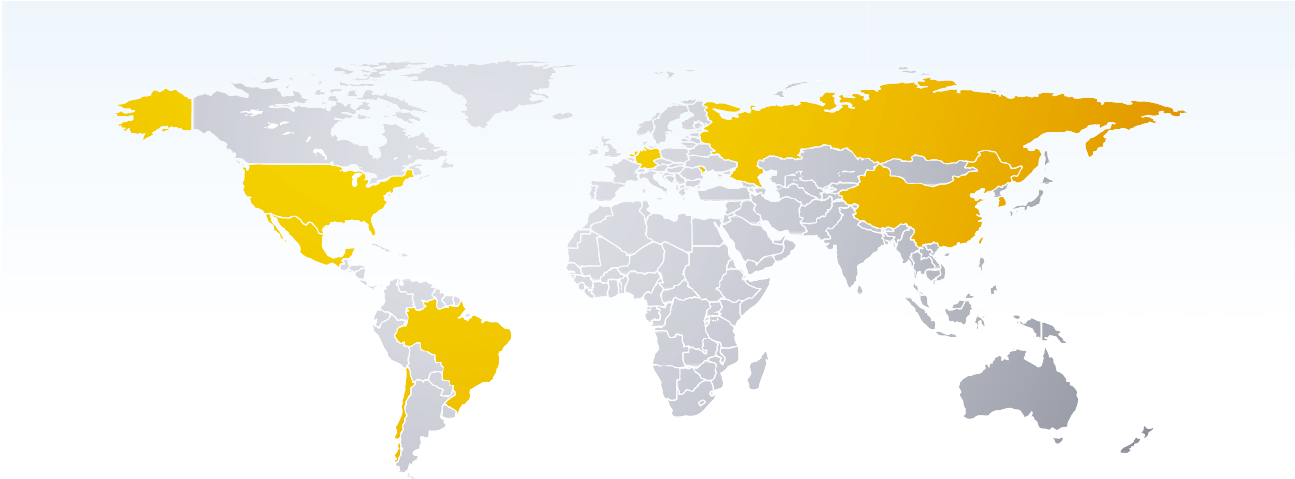


그림 69: 스팸 URL의 지리적 분포, 2010년 상반기

국가	스팸 비율 (%)
중국	37.5%
미국	16.6%
한국	8.9%
몰도바	4.7%
러시아	3.4%

국가	스팸 비율 (%)
브라질	1.9%
멕시코	1.6%
네덜란드	1.5%
칠레	1.5%
대만	1.5%

표 16: 스팸 URL의 지리적 분포, 2010년 상반기

스팸 URL – 호스트 국가 동향

지난 몇 년 동안에는 중국에 있는 서버에서 호스팅되는 스팸 URL이 2009년 말까지 크게 증가했습니다. 그 외 모든 국가는 정체되거나 감소했으며, 특히 미국은 크게 감소했습니다. 중국의 증가 추세는 둔화되어 2010년 상반기에는 2년 만에 처음으로 감소세를 기록했습니다. 하지만 중국은 전체 스팸 URL 중 3분의 1 이상을 호스팅하여 아직도 1위 자리를 지키고 있습니다. 그 외 몇몇 국가도 회복세에 있으며, 특히 이제 전체 스팸 URL 중 17%를 호스팅하는 미국과 거의 9%를 호스팅하는 한국의 회복세가 두드러졌습니다. 10위 목록에 새로 진입한 국가는 전체 스팸 URL 중 4.7%를 호스팅하는 몰도바였습니다.

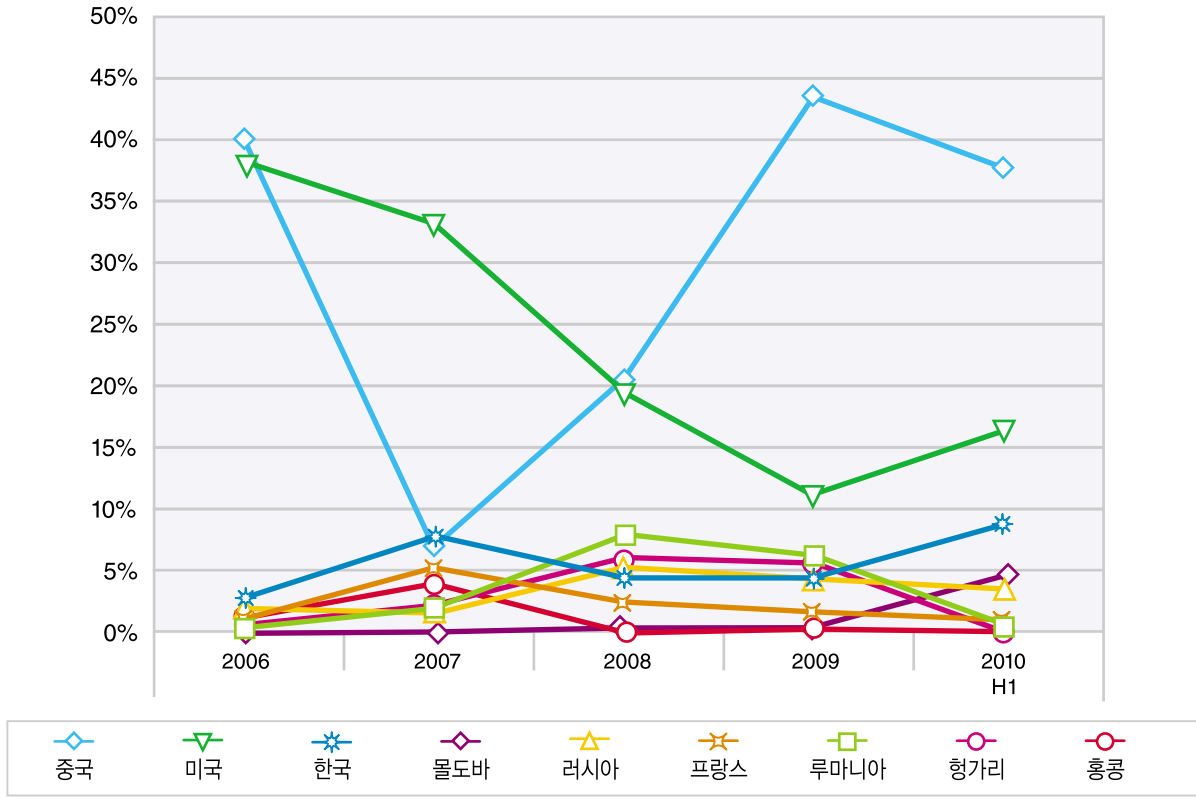


그림 70: 시간에 따른 스팸 URL 호스트 국가 추이, 2006년~2010년 상반기

스팸의 세계화

중국은 여전히 가장 많은 스팸 URL을 호스팅하고 있기 때문에, 특히 .cn 도메인이 스팸에 사용되는 경우가 급격히 줄어들고 있는 가운데 해당 URL을 더 긴밀히 살펴볼 필요가 있을 것입니다. 그림 71에는 스패머들이 사용하는 중국에서 호스팅되는 최상위 도메인의 분포가 나와 있습니다.

중국에서 호스팅되는 모든 스팸 도메인 중 60% 이상은 러시아의 최상위 도메인 **.ru**를 사용합니다. 중국의 최상위 도메인 **.cn**은 30% 미만으로 2위에 그쳤습니다.

그렇다면 스팸의 세계화가 의미하는 것은 무엇일까요? 전형적인 스팸은 미국, 인도 또는 브라질에 있는 컴퓨터에서 발송되고 중국에서 호스팅되는 **.ru** URL을 포함하고 있습니다.

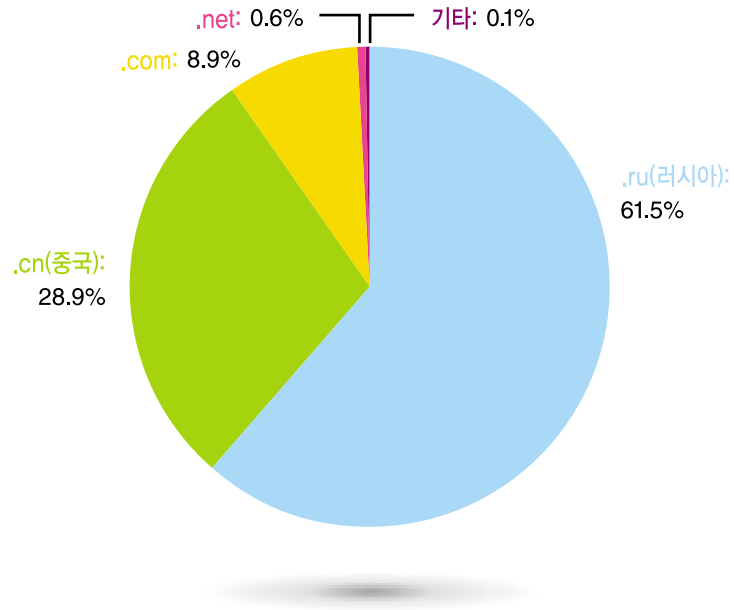


그림 71: 중국에서 호스팅되는 스팸 도메인의 최상위 도메인 비율(%), 2010년 상반기

스팸 – 가장 많이 사용되는 제목

스팸 제목은 2007년부터 2008년까지 점점 세분화되었지만, 이런 추세는 2010년에 정체되고 있습니다. 2010년 상반기에 가장 많이 사용된 10가지 제목이 전체 스팸 제목 중에서 차지하는 비중은 3.3%로 2009년의 2.6%와 2008년의 3%보다 약간 증가했지만, 2007년에 기록된 20%보다는 훨씬 적었습니다.

Web 2.0과 소셜 네트워크의 인기가 점점 높아짐에 따라 스패머들은 이와 관련된 주제를 이용하여 사용자의 관심을 끌려고 합니다. 나아가, "고전"적인 의료 제품이나 짝퉁 시계에 대한 주제도 종종 사용자의 주의를 끌기 위해 사용됩니다. 특히 화이저 사의 의료 제품은 스팸 제목에 절찬리에 사용되고 있습니다. 이런 스팸에서 스패머들은 대소문자를 바꾸고, "o"를 "0"(영)으로 바꾸고, 다른 % 숫자를 사용하는 등의 기존 방식을 채용합니다. 70%는 10위 안에 든 유일한 백분율로서, 스패머들이 가장 선호하는 백분율임이 분명합니다.

표 17에는 2010년 상반기에 가장 많이 사용된 스팸 제목이 열거되어 있습니다.

제목	%
You have a new personal message (새 메시지가 도착했습니다)	0.50%
Replica Watches (고급 시계 복제품)	0.44%
RE: SALE 70% 0FF on Pfizer (화이저 약품 70% 세일)	0.40%
News on Myspace (마이스페이스 새 소식)	0.35%
Important Notice: Google Apps Browser Support (주요 공지: Google Apps 브라우저 지원)	0.35%
Important Notice: Google (주요 공지: 구글)	0.34%
Please Read (필독)	0.29%
Exquisite Replica (정교한 복제품)	0.23%
Watches (시계)	0.19%
Confirmation Mail (확인 메일)	0.17%

표 17: 가장 많이 사용된 스팸 제목, 2010년 상반기

피싱

본 보고서의 I부에서는 이미 피싱 기법의 초점이 왜 서로 다른 산업을 공략하는 데 집중되고 있는지를 설명하는 몇 가지 흥미로운 사례가 소개되었습니다.

여기서는 다음 주제에 관한 동향을 더 자세히 살펴볼 것입니다.

- 피싱의 양이 전체 스팸 중에서 차지하는 비율(%)
- 피싱 웹페이지(URL)를 포함한 피싱의 발신 국가 동향
- 가장 인기 있는 피싱 제목과 표적

피싱의 양

2008년 한 해 동안 전체 스팸 중에서 피싱이 차지하는 비중은 평균 0.5%였습니다. 2009년 상반기에 피싱 공격은 전체 스팸의 0.1%로 급격히 감소했습니다. 당사는 원래 피싱 공격을 감행하는 범죄 조직이 은행에서 보낸 합법적인 이메일로 보이는 간단한 이메일을 발송하는 방법 외에 다른 신분 도용 방법을 사용하는 쪽으로 기울고 있다고 생각했었습니다. 하지만 이 생각은 완전히 빗나간 것이었습니다.

2009년 상반기에 목격된 현상과는 반대로, 피싱 공격자들은 3분기에 더욱 강해져서 돌아왔습니다. 2009년 6월에는 피싱의 양이 약간 증가하기 시작했으나, 8월에 피싱의 양은 2008년에 피싱이 가장 활발했던 달했던 달에 기록된 수준을 회복했으며, 9월에는 이 수준을 완전히 뛰어넘었습니다.

이런 추세는 당사만 목격한 것이 아닙니다. 다른 몇몇 연구 단체도 이런 변화에 대해 언급했습니다. 2009년 말에 이르자 피싱의 양은 2008년 말과 유사한 수준으로 감소했지만, 2009년 상반기보다는 여전히 훨씬 더 많은 수준이었습니다. 2009년 12월에 소폭 증가한 후, 피싱 이메일은 2010년 상반기에 다시 2009년 상반기와 비슷한 수준으로 감소했습니다.

피싱의 양은 1월과 2월에 감소한 후 3월과 4월에 다시 증가했습니다. 그러나 5월에는 또다시 감소했습니다.

5월의 감소세는 5월 초에 루미니아의 피싱 조직을 검거한 것과 관련이 있을 수 있습니다(http://www.h-online.com/security/news/item/Police-apprehend-Romanian-phishinggang-997151.html 참조). 6월에는 피싱의 양은 다시 3~4월 수준으로 증가했지만, 2009년 여름보다는 여전히 훨씬 적은 수준이었습니다. 피싱 공격자들이 지난 2년 동안 그랬던 것처럼 2010년 여름과 가을에도 피싱의 양을 크게 늘릴 것인지는 앞으로 몇 달 동안 두고 봐야 할 것입니다.

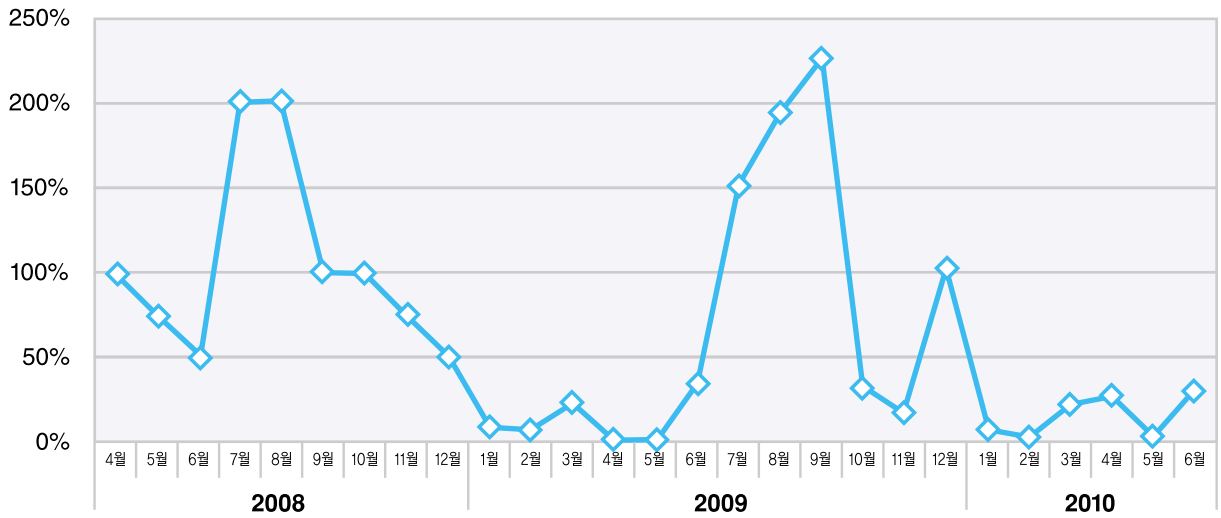


그림 72: 시간에 따른 피싱의 양 변화 추이, 2008년 4월~2010년 6월

피싱 – 발신 국가

브라질은 여전히 가장 많은 양의 피싱 메일이 발송되는 국가이며, 인도가 2위 그리고 한국이 3위를 기록하고 있습니다. 10위 안에서는 순위가 아래 위로 3위 넘게 움직인 경우는 많지 않았습니다. 러시아만 3위에서 10위로 떨어졌습니다. 독일은 10위에 새로 진입했으며, 터키는 목록에서 사라졌습니다. 표 18에는 2010년 상반기의 주요 피싱 이메일 발신 국가가 열거되어 있습니다.

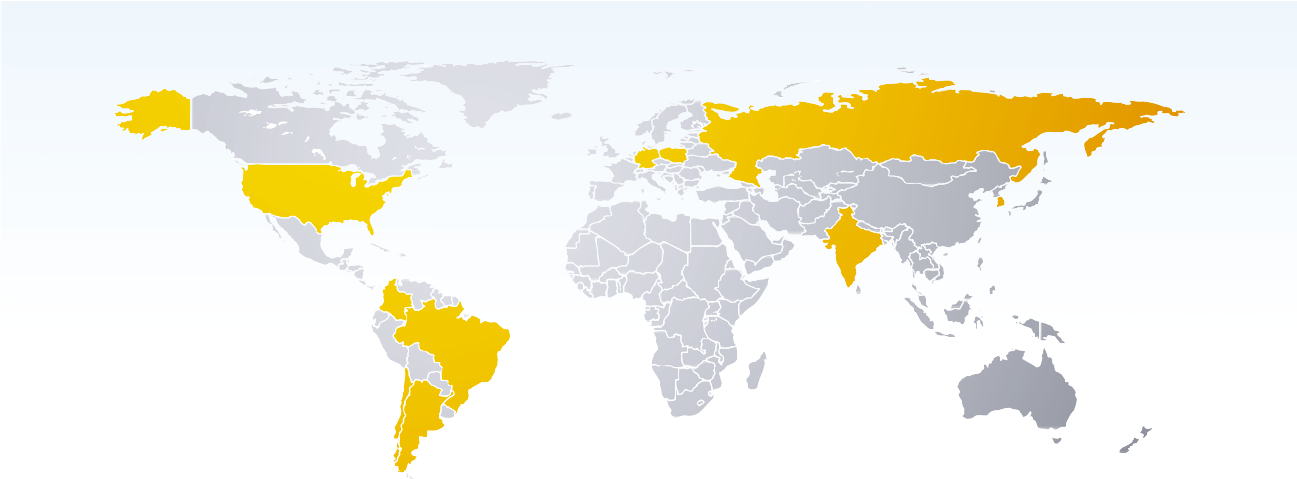


그림 73: 피싱 발신자의 지리적 분포, 2010년 상반기

국가	스팸 비율 (%)	국가	스팸 비율 (%)
브라질	14.3%	아르헨티나	3.8%
인도	8.2%	칠레	3.3%
한국	7.8%	독일	3.1%
미국	5.6%	폴란드	2.9%
콜롬비아	3.4%	러시아	2.6%

표 18: 피싱 발신자의 지리적 분포, 2010년 상반기

피싱 URL – 호스트 국가

표 19에는 피싱 URL이 호스팅되는 위치가 나와있습니다. 10대 국가는 2009년과 동일하며, 상대 순위도 조금밖에 바뀌지 않았습니다. 러시아는 8위에서 10위로 하락한 반면 스페인과 폴란드는 1단계씩 올라갔습니다.

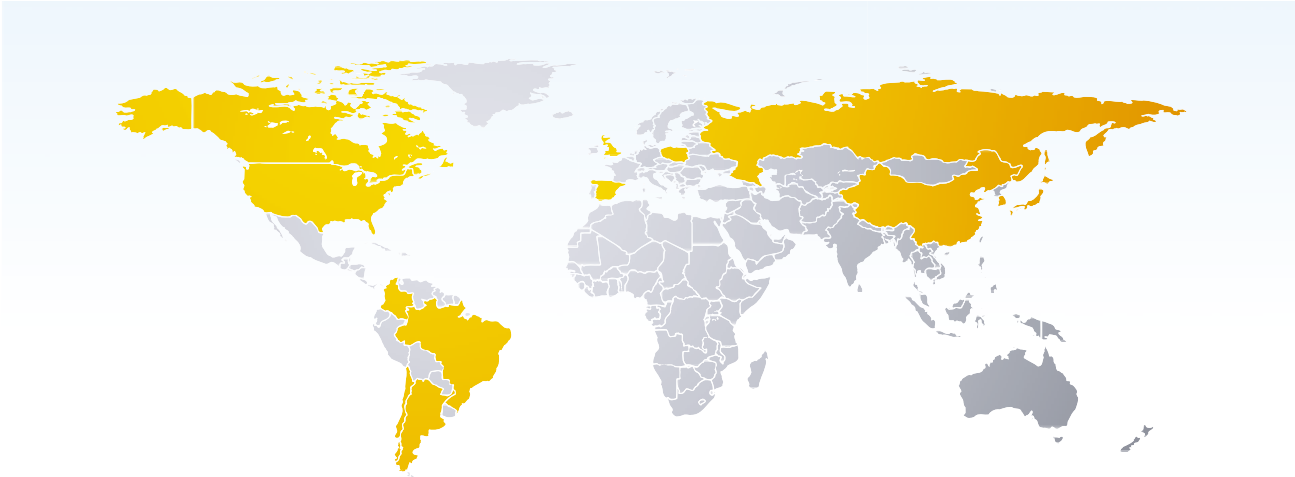


그림 74: 피싱 URL의 지리적 분포, 2010년 상반기

국가	스팸 비율 (%)
브라질	18.8%
미국	14.5%
중국	11.3%
한국	9.8%
영국	7.2%

국가	스팸 비율 (%)
캐나다	4.7%
일본	4.3%
스페인	3.2%
폴란드	3.0%
러시아	2.9%

표 19: 피싱 URL의 지리적 분포, 2010년 상반기

피싱 – 가장 많이 사용되는 제목

2008년에 있었던 가장 큰 변화 중 하나는 전에 많이 사용되던 제목들이 그다지 많이 사용되지 않았다는 것이었습니다. 2007년에 가장 인기가 있었던 제목은 전체 피싱 이메일의 40% 이상에 사용되었습니다. 하지만 2008년에는 가장 인기 있는 제목이 전체 피싱 이메일의 6%에만 사용되었습니다. 따라서 피싱 공격자들은 2008년에 2007년보다 더 다양한 제목을 사용함으로써 표적을 더 세분화했음을 알 수 있습니다.

2009년에는 이런 추세가 완전히 반전되었습니다. 2007년에 가장 인기 있던 10개 제목은 전체 피싱 이메일의 38% 이상에 사용되었습니다. 2010년 상반기에 가장 인기 있는 10개 제목은 전체 피싱 이메일 중 약 36%에 사용되었습니다.

"Underreported Income(소득 미신고)"이라는 문구는 10대 피싱 제목 중 4개에 나타나며, 이는 거의 1년 동안 목격되어 온 피싱 위협에 해당됩니다. 이 위협은 미국 국세청 웹사이트와 관계된 것입니다. 나머지 6개 제목은 꽤 흔한 것입니다. 대부분의 피싱 메일은 사용자에게 무엇을 긴급히 할 것을 요청합니다. 대부분의 경우 사용자는 사기성 웹사이트로 연결되는 이메일에 포함된 링크를 따라가서 자신의 은행 계정에 로그인하라고 요청됩니다.

표 20에는 2010년 상반기에 가장 많이 사용된 피싱 제목이 열거되어 있습니다.

제목	%
Security Alert – Verification of Your Current Details (보안 경보 – 최신 개인 정보 확인)	15.75%
American Express Online Form (온라인 서식)	6.22%
Important Notification (주요 공지)	1.95%
Official Information (공식 정보)	1.78%
Your Account Has Been Limited (귀하의 계정이 제한되었습니다)	1.73%
Notice of Underreported Income (미신고 소득 고지)	1.70%
Underreported Income Notice (미신고 소득 고지)	1.67%
the CP2000 Notice (Underreported Income Notice) [CP2000 고지 (미신고 소득 고지)]	1.67%
Official "Underreported Income Notice" to Taxpayer (납세자를 위한 공식 "미신고 소득 고지")	1.66%
Final Notice (최종 독촉장)	1.40%

표 20: 가장 많이 사용된 피싱 제목, 2010년 상반기

(135-270) 서울시 강남구 도곡동 467-12
군인공제회관빌딩

한국아이비엠주식회사
고객만족센터

TEL: (02)3781-7114
www.ibm.com/kr

2010년 11월

WGL03003-USEN-01