IBM 기업가치연구소

IBM X-Force Threat Insight Quarterly

IBM

차례

보고서 소개

IBM X-Force® Threat Insight Quarterly에서는 현재 보안 전문가들이 직면하고 있는 가장 중요한 위협과 문제를 요약합니다. 본 보고서는 IBM Managed Security Services와 IBM X-Force 연구개발팀이 제작했습니다. 매 발행호에서는 구체적인 문제에 초점을 맞추고 최근의 가장 중요한 온라인 위협에 대해 정리했습니다.

IBM Managed Security Services(관리 보안 서비스)는 보안 운영을 아웃소싱하거나 기존의 보안 팀을 보완함으로써 기업이 정보 보안을 개선하는 데 도움을 주도록 고안되었습니다. IBM 보호 온디맨드 플랫폼은 기업이 정보 자산을 인터넷 공격으로부터 보호하기 위해 필요한 Managed Security Services와 전문성, 지식 및 인프라스트럭처를 제공하는 데 기여합니다.

X-Force 팀은 선제적인 인터넷 보안 방식을 구현하기 위한 기초를 제시합니다. X-Force 팀은 세계에서 가장 유명한 영리 보안 연구 그룹 중 하나입니다.

보안 전문가들로 구성된 이 그룹은 취약점 및 보안 문제를 연구 및 평가하고 IBM Internet Security Systems 제품을 위한 평가 및 대응 기술을 개발하고 새로운 인터넷 위협에 대해 일반에게 알립니다. X-Force 팀은 독자의 피드백을 환영합니다. 본 보고서의 내용에 관한 질문이나 의견은 다음 주소로 보내주십시오.
XFTAS@us.ibm.com.

우리 친구할까요? 소셜 네트워킹에 도입된 새로운 위협 환경에 대한 인사이트

– David MacKinnon 저

최근 몇 년 간 소셜 네트워킹 사이트는 사람들의 일상 생활 속에 점점 깊이 자리잡게 되었습니다. 소셜 네트워킹 사이트를 통해 사람들은 옛 친구와 다시 연락하게 되고 다른 사람과 통신 및 협업하며 멀리 있는 친구 및 친척과 사진을 공유할 수 있습니다. 반면, 동시에 악의적인 의도를 가진 공격자에게는 새로운 기회를 제공해 주기도 합니다.

배경

소셜 네트워킹의 인기는 계속하여 놀라운 속도로 점점 높아져가고 있습니다. 올해 초에, 가장 인기 있는 사이트 중 하나인 Facebook은 사용자 수가 3억 명을 돌파했다고 발표했습니다. QZone, Twitter, MySpace, Vkontakte, LinkedIn 및 기타 수많은 사이트 역시 매일 상당수의 방문자가 이용합니다. 현재 소셜 네트워크 사이트의 채택률은 단연 최고입니다. Facebook만해도 단 5개월 만에 사용자 수가 2억 명에서 3억 명으로 증가했습니다.[1] 다른 기술의 채택률과 비교할 때, 이 같은 성장세는 전례가 없는 것입니다. 예를 들면, 라디오와 TV가 5000만 명의 시청자를 확보할 때까지 각각 38년과 13년이라는 시간이 소요되었습니다.[2] 소셜 네트워킹의 한 가지 독특한 측면 중 하나는 컴퓨터가 유일한 접촉 매체라는 기대를 벗어나는 추세에 있다는 데 있습니다. 모바일 기술의 성장으로 인해, 사용자는 자신의 근황을 거의 어디에서든 업데이트할 수 있게 되었습니다. 모바일 기기를 사용하여 사이트에 접속하는 Facebook 사용자는 4분의 1에 달하는 것으로 추정되며 단 9 개월 만에 4,500만 명이 증가했습니다.[3] 이로 인해 매체의 사교적 측면은 더욱 강화되지만, 이 같은 소셜 네트워킹 사이트를 통해 전파될 수 있는 새로운 공격 방향이 제시되기도 합니다.

그렇다면 이것이 일반인에게 의미하는 것은 무엇일까요? 이 질문에 대한 해답은 보안 전문가, 시스템 관리자, 또는 소셜 미디어의 일반 사용자에게 각기 다릅니다. 본 문서는 단순히 독자에게 현재 존재하는 다양한 위협에 대해 알려 각자의 환경에서 이 같은 위협에 대처할 준비를 할 수 있도록 하기 위한 의도로만 작성되었습니다.

피싱

피싱은 인터넷에서 더 이상 생소한 용어가 아닙니다. 이는 90년대부터 존재해 왔으며, 시간이 지남에 따라 점점 더 정교해져 왔습니다. 초기에는 이메일이 피싱 공격에 일반적으로 사용되는 매체였습니다. 금융 기관에서 보낸 것처럼 보이는 이메일은 사용자에게 계정 정보를 업데이트할 것을 요청합니다. 사용자가 링크를 클릭하면, 합법적인 금융 기관 사이트를 미러링한 악성 사이트로 연결됩니다. 이 같은 사이트는 피해자가 알지 못하는 사이에 피해자의 계좌 정보, 사용자 이름 및 비밀번호를 빼내는 기능을 했습니다.

이 같은 추세는 두 가지 중요한 유형의 피싱 수법을 통해 소셜 네트워킹으로 옮겨왔습니다. 첫째는 악성 이메일 및 웹사이트를 이용한 수법입니다. 사용자에게는 자신이 선호하는 소셜 네트워킹 사이트처럼 보이는 링크가 제시됩니다. 이 같은 사이트는 실제 사이트를 완벽히 복제한 것이며 일단 사용자가 로그인을 시도하면 인증 정보를 도난 당하게 됩니다. 두 번째 악용 방법은 소셜 네트워킹 사이트 자체 내에서 수신한 메시지를 통해 이루어집니다. 사용자는 계좌 업데이트 도구를 설치하라는 메시지를 수신합니다. 하지만, 사용자가 실제로 설치하는 것은 사용자의 비밀번호를 훔쳐가는 멀웨어입니다.

일단 계좌 인증정보를 획득하면, 이제 추가 피싱 메시지를 보내고 멀웨어를 전파하며 돈을 갈취하려 시도를 하고 신분 도용을 감행할 능력을 갖게 된 공격자에게는 여러 가지 공격 경로가 열리게 됩니다. 이어지는 내용에서는 이처럼 다양한 공격이 감행되는 몇 가지 흔한 방법에 대해 살펴볼 것입니다.

[1] 3억 돌파 http://blog.facebook.com/blog.php?post=136782277130

[2] UN(국제연합) Cyberschoolbus http://www0.un.org/cyberschoolbus/briefing/technology/tech.pdf

[3] Facebook 모바일 사이트의 성장 http://techcrunchies.com/growth-of-facebook-mobile-site-2/

멀웨어/스파이웨어

과거에 멀웨어는 전통적으로 이메일이나 공격을 당한 웹사이트나 보다 최근에는 보안이 훼손된 PDF 및 플래시 파일을 통해 배포되었습니다. 시간이 지남에 따라 이 같은 공격 방식은 효과가 입증되어 빠르게 전파되었지만, 다행히 매우 빠른 속도로 퇴치되어 오기도 했습니다. 소셜 네트워킹 사이트의 인기가 급속도로 높아지자 멀웨어 개발자들에게는 완전히 새로운 공격 무대가 열렸으며 이들은 지체 없이 공격 코드를 작성하기 시작했습니다.

과거에 멀웨어를 전파하기 위해 가장 널리 사용된 기법은 소셜 네트워킹 애플리케이션 자체 안에 포함되어 전송되는 메시지에 들어있는 악성 링크를 통해서였습니다. 이 같은 메시지는 일반적으로 해당 멀웨어에 이미 감염되어 있는 사용자로부터 발신되었습니다. 링크는 동영상 클립과 같이 보여지며, 사용자가 링크를 클릭하면 시스템의 플래시(Flash®) 플레이어를 업데이트하라는 메시지가 나타났습니다. 보다 최근에 이 같은 공격은 소셜 네트워킹 사이트 안에서 생성된 허위 악성 계정을 통해 감행되고 있습니다. 이 같은 계정에는 업데이트를 요청하거나 사용자에게 시스템에 바이러스가 있음을 알리는 것처럼 보이는 비디오 링크도 있습니다.[4] 하지만 실제로는 메시지에 의해 멀웨어가 설치되며 사용자가 다음 번에 소셜 네트워킹 웹사이트에 로그인하면 바이러스는 감염된 사용자의 모든 연락처로 악성 메시지를 보냅니다.

Facebook에서 처음 전파된 스파이웨어 중 하나는 시스템에 제공된 타사 애플리케이션을 통해 전파되었습니다. 사용자는 시스템으로부터 그를 몰래 짝사랑하는 사람이 있으며 그 사람이 누군 지 알아보려면 애플리케이션을 설치해야 한다는 메시지를 받았습니다. 애플리케이션을 설치하면, 사용자는 즉시 링크를 보낼 5명의 친구를 알려달라고 요청함으로써 잠재적인 감염자의 수를 더욱 늘렸습니다. 마지막으로, 애플리케이션은 설치할 추가 소프트웨어로 연결되는 팝업 광고를 띄웠습니다. 하지만 이를 다운로드하고 설치한 모든 사용자는 사실 Zango 애드웨어를 설치하게 되었습니다.[5]

보다 최근에 일어났던 사건에서는 매우 인기 있는 소셜 게임 회사인 Zynga의 CEO가 이렇게 만든 애플리케이션을 영리를 위해 악용했다고 자랑했습니다. 이 소프트웨어 업체는 게임에서 사용자의 레벨이 더 빨리 올라갈 수 있도록 게임을 설정했습니다.

게임 머니를 이용하여, 게임 사용자에게는 게임 머니를 구입함으로써 게임 머니를 받거나 더욱 위험하게는 다양한 애드웨어/스파이웨어를 자신의 시스템에 설치하는 대가로 게임 머니를 얻을 수 있는 기회를 부여했습니다.[6] 소셜 네트워크 사이트를 악용한 새로운 공격 방향은 이 같은 사이트를 감염된 시스템의 지휘 및 통제 채널로 사용하는 것이었습니다. Facebook과 Twitter는 모두 최근에 트로이 목마를 통해 사이트가 악용되는 피해를 겪었습니다. Twitter에서 감염된 클라이언트는 시스템에서 실행할 트로이목마 명령을 제공하는 base64로 인코딩된 문자열을 포함한 트윗(tweet)을 받았습니다.[7] Facebook 변형에 감염된 클라이언트는 Facebook 사용자 프로필의 메모(Notes) 부분에 클라이언트 기기에서 실행할 명령이 없는 지 모니터링했습니다.[8]

[4] Facebook, 멀웨어를 퍼트리도록 고안된 허위 프로필 삭제
http://www.enigmasoftware.com/facebook-shuts-down-fake-profiles-designed-to-spread-malware/

[5] Facebook 위젯, 스파이웨어 설치 http://www.fortiguard.com/advisory/FGA-2007-16.html

[6] Zynga의 마크 핀커스 CEO: "난 수익을 얻기 위해 온갖 나쁜 짓을 다했다" http://www.techcrunch.com/2009/11/06/zynga-scamville-mark-pinkus-facebook/

[7] 트위터 기반 봇넷 명령 채널 http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel/

[8] Facebook를 악용하여 좀비 명령을 퍼트리는 트로이목마 http://www.theregister.co.uk/2009/11/03/trojan_cnc_pokes_facebook/

Facebook는 적극적으로 자사 사용자 기반을 보호하기 위해 노력해 왔습니다. 내장된 보안 조치 외에 Facebook은 타사 서비스를 사용하여 사용자를 피싱과 멀웨어로부터 모두 보호하기도 합니다.[9] 하지만 안타깝게도, 이 같은 추가적인 보안 조치에도 불구하고 애플리케이션 및 멀웨어 개발자들은 모두 이를 우회하는 독특한 방법을 계속 찾아내고 있습니다.

새로운 419 사기 수법

Threat Insight Quarterly 09년 2분기 호의 "사기 수법; 당신을 사랑합니다. 당신을 부자로 만들어드리겠습니다. 참, 그리고 돈이 좀 필요해요"라는 기사에서는 로맨스 수법과, 이 같은 수법이 금전적 이득을 취할 목적으로 선량한 피해자를 악용하려고 시도하는 방법에 대해 보도했습니다. 이 같은 유형의 수법은 소셜 네트워킹 사이트까지 확산되었지만, 새로운 반전이 더해졌습니다. 돈을 달라고 부탁하는 사람은 다름아닌 사용자의 친구 중 한 명입니다.

다른 419 사기 수법과 마찬가지로, 이 수법 역시 매우 성공적이었습니다. 올해 초에 미주리 주 케이프지라듀(Cape Girardeau)에 사는 한 여성은 자기 친구를 돕는다고 생각하여 여러 차례에 걸쳐 총 4,000 달러를 송금했습니다.[10] 일단 한 번 송금한 돈은 되찾을 가능성이 거의, 또는 전혀 없습니다.

수법은 사실 매우 간단합니다. 사용자는 한 친구에게 메시지나 채팅을 통해 도움을 요청 받습니다. 이 친구는 자신이 영국에 휴가를 왔는데 도둑을 맞았고 돈이나 신용카드가 없어 호텔 숙박료를 내기 위해 도움이 필요하다고 말합니다. 하지만 편리하게도 몇 분 거리에 송금을 받을 수 있는 은행이나 우체국이 있으니 돈 좀 송금해 줄 수 있냐고 묻습니다.

이 같은 요청을 전파하는 사용자 계정은 일반적으로 멀웨어에 감염된 사용자나 피싱 링크에 접속한 사용자에게 훔친 계정입니다. 일단 훔쳐진 계정은 비밀번호가 변경되고 모든 가까운 친지(아내, 여자친구 등)는 삭제됩니다. 다음, 공격자는 모든 훔친 계정의 연락처로 연락하여 요청을 합니다.

데이터 수집/신분 도용

누구나 한 번 정도는 친구가 처음 구매한 차나 다녔던 학교나 친구의 애완동물이 가장 좋아하는 색 등을 알려주는 "친구에 대해 알기" 이메일을 받아봤을 것입니다. 이 같은 이메일은 90년대부터 성행했으며, 소셜 네트워킹에서 다시 등장하고 있습니다. 하지만 대부분의 사람들은 여기에 사용되는 설문조사를 작성할 때 자신이 얼마나 많은 정보를 공개하고 있는 지 고려하지 않습니다.

은행에서 고객의 신분을 확인하기 위해 사용하는 보안 질문을 살펴보신 적이 있으십니까? 이 같은 질문에 대한 답이 사용자의 소셜 네트워킹 계정에 적혀 있다는 사실을 눈치채신 적이 있으십니까? 어쩌면 그게 대수냐고 그 정보를 볼 수 있는 사람은 내 친구들뿐이라고 생각할 수 있습니다. 하지만, 소셜 네트워킹 사이트 안에 존재하는 여러 제 3 사 애플리케이션을 간과해서는 안 됩니다. 이 같은 애플리케이션은 기본 설정에 의해 애플리케이션을 추가한 계정뿐만 아니라 해당 사용자의 연락처 목록에 있는 사용자를 보고 그들로부터 정보를 수집할 수 있습니다.

여기에 사용자의 계정이나 친구의 계정 중 하나가 해킹될 위험을 추가로 감안하여 사용자의 개인 정보가 실제로 어느 정도까지 공개될 수 있는 지 생각해 보십시오. 대부분의 온라인 금융 웹사이트는 2가지 요소를 사용하여 고객의 본인 여부를 확인합니다. 첫 번째 단계는 전형적인 사용자이름과 비밀번호의 조합입니다. 두 번째 단계는 사용자가 본인의 정확한 확인을 위한 사적인 질문에 답하는 것입니다. 만일 사용자가 소셜 네트워킹 사이트에서 사용하는 인증정보가 금융 기관에서 사용하는 인증정보와 같을 경우, 자금을 도난 당할 위험에 처할 가능성이 높다고 말할 수 있을 것입니다.

이를 방지하기 위해 취할 수 있는 몇 가지 간단한 조치가 있습니다.
먼저, 여러 계정에 서로 다른 비밀번호를 사용하도록 합니다.
둘째, 다른 사용자가 볼 수 있는 정보를 작성할 때에는 금융 기관에서 묻는 질문과 동일한 질문에는 답을 적지 않습니다.

[9] Facebook, 멀웨어 퇴치를 위해 MarkMonitor 사기방지 솔루션 선택 http://www.circleid.com/posts/20090430_facebook_markmonitor_antifraud_malware
[10] Facebook에서 해커에게 4000달러를 빼앗긴 케이프지라듀의 한 여성 http://www.kfvs12.com/Global/story.asp?S=11043673

모바일 위협

휴대폰 기술이 계속 진화함에 따라, 제조업체들은 자사 제품에 새로운 기능을 최대한 많이 탑재하기 위해 노력하고 있습니다. 일반 사용자에게 이 같은 기능은 일반적으로 호사로 여겨지지만, 악의적인 의도를 가진 자들에게는 기회로 인식되기도 합니다. 현재 대부분의 소셜 네트워킹 사이트에는 자사 사이트를 휴대폰으로 직접 연결하는 애플리케이션이 있으며, 이를 통해 애플리케이션의 기능은 컴퓨터뿐만 아니라 사용자의 휴대폰으로까지 확장됩니다. 하지만, 이는 모바일 멀웨어를 배포하기 위한 매체로도 사용됩니다.

올해 초에는 Symbian 기반 스마트폰에 멀웨어가 매우 폭넓게 확산되기도 했습니다. 이 멀웨어는 Symbian의 서명 코드에 내재된 결함을 악용하여 기기에 대한 매우 깊은 액세스 권한을 부여했습니다. 일단 감염된 기기는 휴대폰에 저장된 모든 개인 정보를 수집하여 사전 프로그래밍된 일련의 서버로 전파했습니다. 그 밖에, 애플리케이션은 휴대폰에 저장되어 있는 모든 연락처로 문자메시지를 전송하여 다른 휴대폰까지 감염시키려는 시도를 할 수도 있습니다.[11]

또 다른 예로, 잠금이 해제된(jailbroken) 아이폰이 공격 대상이 되었습니다. 아이폰이 '잠금해제' 되면, 시스템의 기본 루트 비밀번호를 사용하게 됩니다. 처음에는 감염된 장치의 바탕화면을 변경하는 웜이 장난처럼 개발되었습니다.[12] 처음 시작은 그다지 악의적인 것이 아니었지만, 며칠 만에 악의적인 의도를 가진 새로운 웜이 인터넷에서 발견되었습니다.[13] 이 두 가지 웜은 모두 기본 비밀번호를 변경하지 않은 사용자를 공략하여 기기의 보안을 약화시켰으며 약화된 이후에는 시스템에 있는 모든 정보를 사용할 수 있게 되었습니다.

현재까지 소셜 네트워킹 사이트에서 시작된 것으로 확인된 모바일 웜은 없습니다. 하지만 기술의 빠른 발전 속도와 새로운 모바일 기술과 소셜 네트워킹이 긴밀히 통합되는 정도를 감안하면 이 같은 웜이 등장하는 것은 시간 문제입니다.

결론

필자의 동료 중 한 명이 이메일 서명에 사용하는 격언이 있는데, 이 글의 주제와 매우 잘 어울린다는 생각이 듭니다. 그 격언은 "믿되 확인하라"는 것입니다. 이는 소셜 네트워킹 사이트를 사용할 때 실로 중요한 경험 법칙입니다. 기본적으로 모든 친구에게는 어느 정도의 믿음을 갖게 되는데 진정한 친구라면 절대 고의로 나를 해하려 하지 않을 것이기 때문입니다. 하지만, 확실히 확인해서 손해 볼 건 없습니다. 친구가 수상해 보이는 링크를 보낸다면, 클릭하기 전에 정말로 친구가 보낸 것인 지 확인하십시오. 친구가 외국에서 오도가도 못하게 되어 돈이 필요하다는 메시지를 보낸다면 친구만 알 수 있는 구체적인 질문을 함으로써 본인 여부를 확인하십시오. 즐겨 찾는 사이트에서 소프트웨어 업데이트를 받으면 설치하지 마십시오. 대신, 브라우저 창을 하나 더 열어 업체의 사이트를 직접 방문하고 업데이트가 필요한 지 확인하십시오. 궁극적으로, 인터넷을 이용할 때와 특히 소셜 네트워킹을 사용할 때에는 반드시 운영체제, 브라우저 및 보안 소프트웨어 패치를 최신 상태로 유지하는 것이 좋은 방법입니다.

[11] Sexy Space가 SMS Botnet의 출생지일 수 있을까? http://www.symantec.com/connect/blogs/could-sexy-space-be-birth-sms-botnet

[12] 지금은 장난에 불과한 iPhone 웜, 향후 위협의 징조? http://www.scmagazineus.com/iPhone-worm-plays-prank-but-signals-danger-ahead/article/157452/

[13] 잠금 해제된 iPhone에서 데이터를 훔칠 수 있는 공격 도구 http://www.scmagazineus.com/Attack-tool-can-hijack-data-off-unlocked-iPhones/article/157587/

이기종 전사 환경에서의 자문(Advisory) 모니터링

– Troy Bollinger 저

취약성[14]은 공격자가 허가 없이 권한을 획득하거나 시스템의 가용성을 떨어뜨리기 위해 악용할 수 있는 결함이나 약점입니다. 취약성은 다른 패칭 방법을 필요로 하는 독특한 버그 유형(class)입니다. 이는 기초를 이루는 버그가 트리거되는 방법에 기인합니다. 취약성은 고의적인 표적 공격의 대상이 되며, 이는 관리자가 이 같은 행동이 시스템에 영향을 미치는 방법을 통제할 수 있는 힘이 상대적으로 약하다는 것을 의미합니다. 취약성은 동적인 성격을 갖고 있기 때문에, 고객은 일반적인 버그 유형처럼 업데이트 일정을 조정할 수 있는 여유가 없습니다.

과거부터 소프트웨어에서는 취약성이 발견될 수 밖에 없다는 사실이 입증되어 왔으며 소프트웨어 공급업체는 사용 가능한 수정 패치가 있을 때 고객에게 알릴 의무가 있습니다. 대기업의 시스템 관리자는 여러 공급업체의 여러 가지 제품을 지원하는 일이 흔합니다. 이처럼 규모가 큰 환경에서는 최신 보안 패치 상태를 유지하기가 어렵습니다.

소비자용 데스크탑 PC와는 달리, 전사 환경에서는 업체가 제공하는 자동 업데이트 기능을 이용할 수 없습니다. 이 같은 환경의 시스템 관리자는 상호운용성 검사를 실시한 다음 변경 유예와 같은 비즈니스 위주의 지침에 따라 패치를 배포해야 합니다.

과거에 많은 업체는 부분적으로 불리한 보도가 나가는 것을 방지하기 위해 취약성에 대한 세부사항을 숨기곤 했습니다. 과거에 이 같은 방법은 공격자가 취약성에 대한 세부정보를 이용하여 고객을 공격하는 것을 방지하기 위한 것이라 주장되었습니다. 그러나, 이로 인해 고객이 패치 설치를 지연하거나 기피할 경우에 직면할 수 있는 위험을 이해하지 못하게 되기도 했습니다. 시간이 지남에 따라, 공급업체들은 취약성 패치를 다루는 보다 균형된 방법을 도입했습니다. 오래 전부터 분명한 목적을 가진 공격자는 공급업체가 제공한 세부정보 없이도 바이너리 패치를 역설계(reverse engineer)할 수 있는 것으로 알려져 왔습니다.

책임 있는 취약성 공개의 목적은 고객에게 자신이 처한 위험을 진단하고 공격자가 악용 수단을 개발하며 무가화할 수 있기 전에 패치를 적용하기 위해 필요한 양의 정보를 제공하는 것입니다. 이 싸움은 공급업체와 고객이 모두 서로를 보완하는 프로세스를 통해서만 이길 수 있습니다.

공급업체가 위험을 진단하고 공격으로부터 스스로를 보호할 수 있는 고객의 능력을 향상시킬 수 있는 통보 절차는 3단계로 구성됩니다. 이들 단계는 취약성 패치 발표의 모니터링, 검색(retrieving) 및 분석(parsing)입니다.

통보 채널 모니터링

공급업체가 취할 첫 단계는 필수 수정 패치 제공 사실을 발표하기 위한 분명하고 일관성 있고 유연한 방법을 제공하는 것입니다. 이 같은 방법에는 월별 또는 분기별 자문 발표 일정의 사전 발표가 포함될 수 있습니다. 이를 통해 고객은 각 발표를 "일상적인 업무"의 일환으로 취급할 인력과 리소스를 배정할 수 있습니다 그러나, 다음 패치 적용 주기까지 기다릴 수 없을 만큼 너무 심각한 취약성을 취급하는 절차도 문서화해야 합니다. 고객은 각 발표에 대해 알고 공급업체와 수없이 의사소통을 하는 가운데 발표를 하나도 놓치는 일이 없을 것이라고 확신할 수 있어야 합니다.

공급업체는 다양한 대안을 사용할 수 있습니다. 예로는 RSS 피드, 웹 자료실, 메일링 리스트 및 지식 기반을 들 수 있습니다. 각각은 고객에게 독특하고 다양한 장점과 단점을 제시합니다.

RSS 피드는 여러 가지 사용하기 쉬운 도구로 모니터링할 수 있기 때문에 가장 인기 있는 대안 중 하나입니다. RSS 항목은 일반적으로 발표 텍스트의 일부만 포함하고 있기 때문에, 문제 분석을 완료하려면 추가 단계가 필요합니다. 웹 자료실 역시 인기가 높지만, 업체는 HTML[15]의 구조를 고객의 자동 모니터링 프로세스의 일환으로 분석(parse)하기가 쉽도록 정해야 합니다. "div" 및 기타 테이블 외 태그를 자유롭게 사용하여 자문의 설명, 패치 및 기타 자문의 나머지 부분의 범위를 정해야 합니다.

[14] CVE – 용어 http://cve.mitre.org/about/terminology.html
보안 취약성의 정의 http://technet.microsoft.com/en-us/library/cc751383.aspx

[15] 아름다운 HTML 코드의 모습 http://css-tricks.com/what-beautiful-html-code-looks-like/

일반적으로, 메일링 리스트는 해당 통지 이외의 맥락을 알 수 없기 때문에 고객이 리스트가 폐기되었는지, 아니면 단지 최근에 패치된 취약성이 없는 것인 지를 알기가 어렵습니다. 그러나, 메일링 리스트는 고객에게 즉시 통지하는 "푸시" 기능을 제공합니다. 어쩌면 최선의 방법은 "푸시" 통지와 함께 분석이 쉬운 웹 자료실을 결합하여 과거 내역의 관점을 제시하는 공급업체 통지 방법의 조합이 될 수도 있습니다.

가능하다면 공급업체는 자문사항을 버그 수정 패치(fix)와 별도로 저장하고 발표해야 합니다. 공급업체는 취약성 수정 패치를 식별할 수 있는 독특한 위치에 있는 한편, 고객은 특정한 버그가 공격자가 허가 없이 권한을 얻기 위해 악용될 수 있는지를 판단할 전문 지식이 없는 경우가 많습니다. 발표를 서로 다른 보관소나 지식 기반에 분리해 놓으면 고객이 중요한 수정 패치를 간과할 가능성이 줄어듭니다.

별도의 취약성 패치 보관소를 사용할 수 없을 경우, 공급업체는 검색 엔진에서 모든 취약성 발표를 검색할 수 있도록 일관된 태그 식별자를 사용해야 합니다.

자문 검색

공급업체는 종종 자문을 검색할 수 있는 방법에 제약을 가합니다. 이 같은 제약은 종종 공급업체가 품질 관리를 제대로 하지 않는 것처럼 보이는 것을 방지하기 위해 정보의 배포를 제한함으로써 가해집니다. 이 같은 정보에 대한 접근 제약은 종종 고객 지원 연락 정보에 대한 접근을 제한하고 자문을 접근이 로그인 방식을 통해 제약되는 곳에 저장하는 방법으로 이루어집니다. 로그인 정보가 일반에 제공되었을 경우에도 세부 규정에는 공개를 금지하거나 제한하는 법적 조항이 포함되어 있는 경우가 많습니다.

이 같은 제약은 평가 프로세스를 복잡하게 만들 수 있습니다. 고객 보안 인력은 종종 관리자 워크로드의 우선 순위를 정하기 위해 취약성의 심각성을 평가해야 합니다. 조직의 규모에 따라서는 보안 인력이 고객 지원 번호나 기타 공급업체가 통지를 액세스하기 위해 요구하는 정보를 액세스할 권한이 없을 수 있습니다.

자문 분석(parse)

일단 통지를 수신하면, 이를 실제 사용 가능한 항목으로 분석(parse)해야 합니다. 자문에는 보통 취약성에 대한 간략한 설명이 수록되어 있습니다. 여기에는 패치를 즉시 적용하지 않을 경우에 입을 수 있는 피해와 이 같은 피해를 완화할 수 있는 모든 방법이 포함됩니다. 설명에는 수정 패치(fix)를 적용해야 하는 지를 판단하고 수정패치가 적용되어 있는지를 판단하는 방법에 대한 설명도 포함되어야 합니다. 여기에는 패치 또는 패키지 버전 번호와 패치를 찾아서 적용할 수 있는 장소에 대한 설명이 포함될 수 있습니다. 고객이 여러 공급업체의 제품에 걸쳐 취약성을 대조 확인할 수 있도록 CVE 번호를 포함시켜 환경을 구성하는 다른 제품들이 취약한 상태로 방치되지 않도록 보장해야 합니다. 공급업체가 계산한 CVSS 점수도 포함시켜 가능한 악용 시도로 인해 발생할 수 있는 피해를 어느 정도 짐작할 수 있도록 해야 합니다.

발표의 전체적인 형식과 내용은 공급업체의 전반적인 기업 문화와 기존의 지원 구조 같은 여러 가지 요인에 따라 달라질 것입니다. 자문의 형식은 산업 표준을 따르거나 다른 공급업체와 외관이나 구조는 필요는 없습니다. 그러나, 고객이 통일된 프로세스를 통해 해당 공급업체와 교류할 수 있도록 한 회사의 제품군 간에는 표준 형식이 사용되어야 합니다.

"사람" 고객이 쉽게 이해할 수 있는 용어로 분명하고 간단하게 설명된 자문 문구를 제공하는 것 외에, 컴플라이언스 확인 프로세스가 기기의 최신 업데이트 여부를 자동으로 판단할 수 있도록 공급업체가 기계로 판독 가능한 버전의 자문을 제공할 수 있다면 매우 유용할 것입니다. 기계로 판독 가능한 버전에는 일반적으로 패치 번호와 패키지 버전이 "사람" 고객용 버전과 교차 참조할 수 있는 식별자와 함께 포함되어 있습니다.

[16] 보안, 평등, 우애: ISO 커튼의 뒤 http://blogs.msdn.com/katie_mousouris/archive/2009/11/14/behind-the-iso-curtain.aspx

[17] ISO/IEC NP 29147 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45170

결론

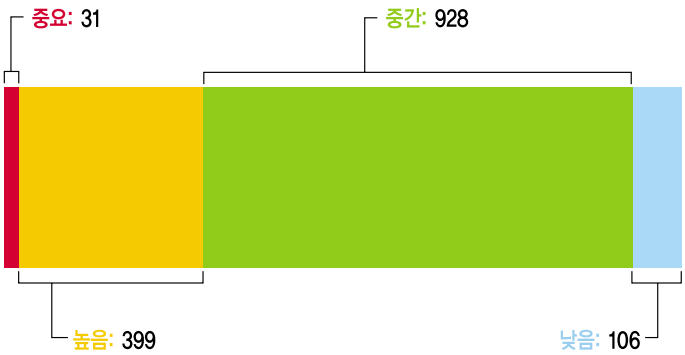
여러 공급업체의 제품을 지원하면서 전체적인 보안 태세를 유지하기는 어렵습니다. 공급업체는 중요한 공지사항을 처리하기 쉬운 형식으로 제공함으로써 고객을 보호하는 데 기여할 수 있습니다. 다음, 고객은 이 같은 공지사항을 종합적인 컴플라이언스 프로세스의 일부로 사용할 수 있습니다. 최근에는 "책임감 있는 취약성 공개"에 대해 연구하는 ISO 작업 그룹이 공급업체의 취약성 통지 프로세스를 표준화[16]하기 위한 몇 가지 노력을 기울이기도 했습니다.[17] 본 문서를 작성할 당시에는 공개 초안이 제공되지 않았습니다. 이 같은 초안이 마침내 공개되면 자문 발표 절차를 개선하고자 하는 공급업체에게 추가적인 방향과 상세 정보를 제공하게 될 것으로 기대됩니다.

2009년 4분기에 많은 영향을 미친 주요 쟁점

공개된 주요 취약성

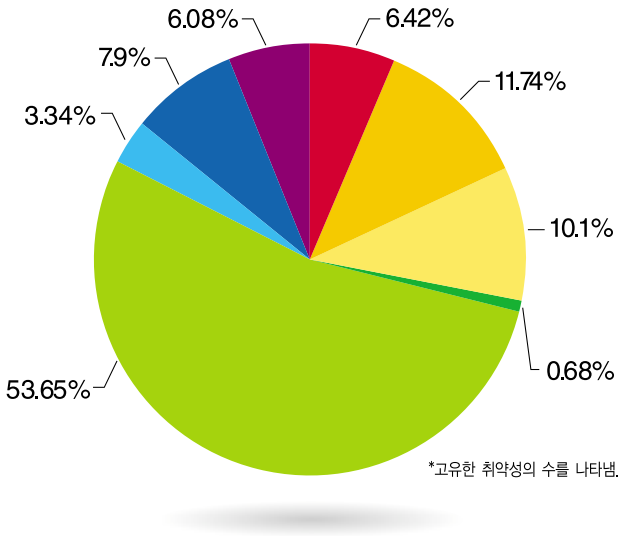
2009년 4분기에 X-Force 팀은 1464개의 보안 관련 위협을 조사 및 평가했습니다. X-Force 데이터베이스에 소개된 취약성 중 상당 비율에 멀웨어 및 표적이 분명한 악용 수단 등을 제작하는 악성 코드 작성자들의 초점이 맞춰졌습니다.

2009년 4분기에 공개된 총 취약성의 수: 1464



출처: IBM X-Force

아래 그래프에는 취약성이 악용될 경우에 가장 큰 타격을 입을 보안 범주별로 X-Force의 애널리스트들이 조사한 취약성이 분류되어 있습니다. 즉, 보안 우회, 데이터 조작, 서비스 거부, 파일 조작, 접근 권한 취득, 권한 취득, 정보 획득 및 기타로 분류되어 있습니다.*



*고유한 취약성의 수를 나타냄.

출처: IBM X-Force

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 악용할 수 있는 취약성도 포함됩니다. 일반적으로 공격자가 시스템에 대한 액세스 권한을 획득할 수 있도록 허용하기 때문입니다.
권한 획득	권한은 로컬 시스템에서만 획득할 수 있습니다.
정보 획득	파일 및 경로 이름, 소스 코드, 암호 또는 서버 구성 내역과 같은 정보를 알아낼 수 있습니다.
기타	다른 유형에 포함되지 않는 모든 것.

이번 분기에 X-Force 팀은 총 3개의 보호 자문[18]과 8개의 보호 경보[19]를 발표하여 여러 중대한 위협에 대응했습니다. 그 밖에, IBM은 두 차례에 걸쳐 인터넷 위협 등급을 AlertCon 2로 올렸습니다.

10월 초에 X-Force 애널리스트들은 0-day Adobe Reader 및 Acrobat 문제가 인터넷 환경에서 활발하게 악용되고 있음을 감지했습니다. 이 같은 취약성은 PDF 파일의 취급과 관련한 오류로 인해 원격 코드가 실행되는 결과를 가져올 수 있습니다. 공격자는 취약성을 성공적으로 악용하기 위해 피해자가 악성 웹페이지를 클릭하거나 악성 파일을 열도록 해야 합니다. 이 같은 악성 문서로 연결되는 링크는 스팸이나 악성으로 보이지 않는 웹사이트에 포함된 링크를 통해 쉽게 보낼 수 있습니다.

- IBM X-Force에서 제시한 보호 경보: Adobe Acrobat 및 Acrobat Reader 원격 코드 실행[20]
  - IBM X-Force 보호 서명 : PDF_Javascript_exploit
- CVE-2009-3459
- Adobe 보안 고시 APSB09-15호: Adobe Reader 및 Acrobat용 보안 업데이트 제공[21]

Microsoft의 2009년 10월 보안 릴리스는 32가지의 취약성에 대처했으며, X-Force 팀은 이 중 9가지가 가장 중요한 것으로 파악했습니다. 첫 번째 문제는 X-Force 연구개발팀이 발견한 Microsoft Internet Explorer에 영향을 미치는 문제로서, 이를 통해 공격자는 악성 웹사이트를 방문하도록 속임으로써 시스템에서 임의 코드를 실행할 수 있습니다. 웹 악용 툴킷은 이 취약성과 같은 브라우저 및 브라우저 관련 악용 경로를 표적으로 삼는 것으로 악명이 높습니다. 기기의 보안이 침해될 경우, 기밀 정보 공개, 생산성 손실 및 기타 피해로 이어질 수 있습니다.

- IBM X-Force에서 제시한 보호 자문: Microsoft Internet Explorer 인수 원격 코드 실행[22]
  - IBM X-Force 보호 서명: 여러 가지[23]
- CVE-009-2529
- Microsoft 보안 고시 MS09-054호: Internet Explorer용 누적 보안 업데이트 (974455)[24]

[18] X-Force가 발견하고 선제적인 보안 컨텐츠 커버리지를 갖고 있는 하나 이상의 중대한 취약성에 대한 정보 제공.

[19] X-Force가 보안 컨텐츠 커버리지를 발표했거나 발표할 예정인 하나 이상의 중대한 취약성에 대한 정보 제공.

[20] IBM X-Force에서 제시한 보호 경보: Adobe Acrobat 및 Acrobat Reader 원격 코드 실행 http://iss.net/threats/348.html

[21] Adobe 보안 고시 APSB09-15호: Adobe Reader 및 Acrobat용 보안 업데이트 제공 http://www.adobe.com/support/security/bulletins/apsb09-15.html

[22] IBM X-Force에서 제시한 보호 자문: Microsoft Internet Explorer 인수 원격 코드 실행 http://www.iss.net/threats/351.html

[23] 관련 서명은 다음 URL을 참조하십시오. http://xforce.iss.net/CveSearch.do?p=CVE-2009-2529

[24] Microsoft 보안 고시 MS09-054호: Internet Explorer용 누적 보안 업데이트 (974455) http://www.microsoft.com/technet/security/bulletin/ms09-054.mspx

이 중 7가지의 취약성은 Microsoft Windows GDI+에 영향을 미치며 원격 코드 실행을 허용할 수 있습니다. 취약성은 간단히 사용자가 특별히 제작된 이미지 파일이 들어있는 이메일이나 URL을 열어보도록 유도함으로써 악용할 수 있습니다. 이처럼 최종 사용자의 시스템을 감염시키는 기법은 여러 해 동안 사용되어 왔으며, 지금도 계속하여 감염 수단이 되고 있습니다. 보안이 침해될 경우 최종 사용자 시스템은 완전히 통제 당하게 됩니다.

- IBM X-Force에서 제시한 보호 경보: 여러 Microsoft Windows GDI+ 이미지 원격 코드 실행 취약성[25]
  - IBM X-Force 보호 서명: CompoundFile_Shellcode_Detected (CVE-2009-2528), Dot_NET_Shellcode_Detected (CVE-2009-2504), Image_WMF_GDI_Integer_Overflow (CVE-2009-2500), Image_PNG_GDI_Heap_Overflow (CVE-2009-2501), Image_TIFF_GDI_Buffer_Overflow (CVE-2009-2502), Image_BMP_Office_Code_Exec (CVE-2009-2518), Image_PNG_GDI_Integer_Overflow (CVE-2009-3126)
- CVE-2009-2500, CVE-2009-2501, CVE-2009-2502, CVE-2009-2504, CVE-2009-2518, CVE-2009-2528, CVE-2009-3126
- Microsoft 보안 고시 MS09-062호: GDI+의 취약성으로 인한 원격 코드 실행 허용 문제(957488)[26]

Microsoft의 10월 보안 릴리스에서 X-Force 보호 경보를 필요로 했던 마지막 취약성은 Microsoft Windows 인덱싱 서비스 ActiveX 컨트롤에 영향을 미쳤습니다. 피해자가 악성 웹페이지를 방문하도록 유도함으로써, 원격 공격자는 취약한 시스템에서 임의 코드를 실행할 수 있습니다.
ActiveX 컨트롤과 같은 플러그인은 악성 웹 악용 툴킷 개발자들이 가장 많이 공략하는 대상입니다. 이 같은 웹 악용 툴킷은 이제 인터넷 환경에서 볼 수 있는 브라우저 관련 악용 수단의 거의 대부분을 차치합니다.

- IBM X-Force에서 제시한 보호 경보: Microsoft Windows 인덱싱 서비스 ActiveX 컨트롤 원격 코드 실행
  - IBM X-Force 보호 서명: Script_Indexing_Service_Corruption[27]
- CVE-2009-2507
- Microsoft 보안 고시 MS09-057호: 인덱싱 서비스의 취약성으로 인한 원격 코드 실행 허용 문제(969059)[28]

[25] IBM X-Force에서 제시한 보호 경보: 여러 Microsoft Windows GDI+ 이미지 원격 코드 실행 취약성 http://www.iss.net/threats/350.html
[26] Microsoft 보안 고시 MS09-062호: GDI+ 취약성으로 인한 원격 코드 실행 허용 문제(957488) http://www.microsoft.com/technet/security/bulletin/ms09-062.mspx
[27] IBM X-Force에서 제시한 보호 경보: Microsoft Windows 인덱싱 서비스 ActiveX 컨트롤 원격 코드 실행 http://www.iss.net/threats/349.html
[28] Microsoft 보안 고시 MS09-057호: 인덱싱 서비스의 취약성으로 인한 원격 코드 실행 허용 문제(969059) http://www.microsoft.com/technet/security/bulletin/ms09-057.mspx

Gumblar 위협은 악용되는 경우가 증가하여 10월 22일에 인터넷 위협 등급을 AlertCon 2로 상향 조정하는 결과로 이어졌습니다. Gumblar는 2009년 3월에 처음 등장하여 지난 여러 Insight Threat 발행호에서 중점적으로 소개되었습니다. 점점 증가하는 이 같은 자동 봇넷은 해당 웹사이트를 방문하는 PC(퍼스널 컴퓨터)를 악용하기 위해 기존에는 악성이 아니었던 웹 서버의 보안을 침해합니다. 구글 검색의 경로를 변경하는 멀웨어가 대상 PC에 심어지며, 이를 통해 공격자는 "pay-per-click" 또는 다른 유형의 소득을 얻을 수 있습니다. Gumblar는 PC에서 FTP 인증정보를 찾아보고 이를 사용하여 새로운 서버를 감염시킵니다. 2009년 4분기에 IBM Managed Security Services(관리 보안 서비스) 팀은 클라이언트 측 피해자를 공략하고 악성 페이로드를 전세계로 전파하는 데 매우 효과적인 Gumblar 공격이 증가했음을 관찰했습니다.[29]

11월에는 SSL/TLS 프로토콜에 영향을 미치는 취약성이 공개되었습니다. 이 취약성은 세 가지 공격 시나리오를 수반합니다. 두 가지는 서버에서 개시한 SSL 사이퍼 수트 재협상을 이용하고 세 가지 중 가장 위험한 나머지 하나는 공격자가 유도하여 클라이언트에서 개시한 SSL 사이퍼 수트 재협상을 이용합니다. 이들 취약성을 통해, 공격자는 데이터를 클라이언트의 최초 전송 또는 요청을 추가할 수 있습니다.

이 같은 공격은 SSL/HTTPS를 통해 보호될 것으로 기대되는 웹사이트의 보안을 침해하기 위해 사용될 수 있습니다. 그러나, 대부분의 웹 애플리케이션은 이 같은 유형의 공격에 취약한 방법으로 구성될 가능성이 낮습니다. 특히 사이트 간 요청 위조에 대해 일종의 애플리케이션 단계 보호를 구현했을 수 있는 애플리케이션은 더욱 그렇습니다.

이 문제는 웹 브라우저, VPN, 스마트카드 및 기타 SSL/TLS를 사용하는 모든 애플리케이션을 포함한 수많은 플랫폼에 영향을 미칩니다. 이 취약성을 악용하면 중간자(man-in-the-middle) 유형의 공격을 야기할 수 있으며 암호화된 데이터를 가로챌 수도 있습니다. 나아가, 웹 애플리케이션을 통해 사용자가 임의 데이터를 게시물 요청에서 사용자가 나중에 해당 데이터를 회수할 수 있는 장소로 전송하여 저장할 수 있을 경우, 공격자는 피해자의 전체 HTTP 요청에 게시물임을 표시하는 접두어를 붙일 수 있습니다. 그러면 이 게시물은 다시 밖에서 읽을 수 있게 되어 공격자는 그 과정에서 쿠키나 기타 인증 정보와 같은 민감한 정보에 접근할 수 있습니다. 이 방법은 Twitter를 공격하는 데 사용되었으며 공격자는 암호가 해독된 사용자 이름과 비밀번호를 입수할 수 있었습니다.

- IBM X-Force에서 제시한 보호 경보: TLS(Transport Layer Security) 악수 재협상 보안 취약성[30]
  - IBM X-Force 보호 서명: TLS_Client_Cipher_Renegotiation, TLS_Server_Cipher_Renegotiation, TLS_Cipher_Renegotiation (다중)
- CVE-2009-3555

[29] Gumblar 리로디드 http://blogs.iss.net/archive/GumblarReloaded.html

[30] IBM X-Force에서 제시한 보호 경보: TLS(Transport Layer Security) 악수 재협상 보안 취약성 http://www.iss.net/threats/352.html

X-Force 애널리스트들은 11월에 공개된 무수한 Microsoft 문제 중에서 2가지가 가장 중요한 것으로 파악했습니다. 첫째는 Microsoft Windows Vista 및 2008에 영향을 미치는 원격 코드 실행 문제입니다. 이 공격은 특별히 제작된 WSDAPI(Service on Devices API) 메시지를 WSD(웹 서비스 장치) 서비스로 전송하는 방법을 수반합니다. 이 취약성은 Microsoft Windows 운영체제를 구성하는 핵심적인 요소이긴 하지만, Windows Vista와 2008에만 영향을 미칩니다. 악용은 (비록 공격자가 피해자의 로컬 네트워크 상에 있어야 하지만) 원격적으로 이뤄지며, 사용자와의 어떠한 상호작용도 요구되지 않습니다. 악용에 성공한 공격자는 최종 사용자의 시스템을 완전히 통제할 수 있게 됩니다.

- IBM X-Force에서 제시한 보호 경보: Microsoft Windows WSDAPI 코드 실행[31]
  - IBM X-Force 보호 서명: HTTP_MS_WSDAPI_Code_Exec
- CVE-2009-2512
- Microsoft 보안 고시 MS09-063호: Web Services on Devices API의 취약성으로 인한 원격 코드 실행 허용 문제(973565)[32]

11월의 Microsoft 보안 릴리스에서 당사 애널리스트들의 관심을 모은 두 번째 문제는 Microsoft Windows 커널 모드 드라이버에 영향을 미칩니다. 원격 공격자는 피해자가 문서에 임베디드된 EOT 폰트를 포함하는 특별히 제작된 파일을 열도록 유도함으로써 취약한 시스템에서 임의 코드를 실행할 수 있습니다. 이 취약성은 널리 사용되는 Microsoft Windows 운영체제인 Windows 2000, XP 및 2003의 핵심 구성요소입니다. 악용에 성공한 공격자는 최종 사용자의 시스템을 완전히 통제할 수 있게 됩니다.

- IBM X-Force에서 제시한 보호 경보: Microsoft Windows 커널 폰트 코드 실행[33]
  - IBM X-Force 보호 서명: Windows_Kernel_Font_Code_Execution
- CVE-2009-2514
- Microsoft 보안 고시 MS09-065호: Windows 커널 모드 드라이버의 취약성으로 인한 원격 코드 실행 허용 문제 (969947)[34]

11월 말에는 Microsoft Internet Explorer의 0-day 원격 코드 실행 취약성에 대한 개념 증명 악용 수단이 공개되었습니다. 피해자가 특별히 제작된 CSS 페이지를 방문하도록 유도함으로써 원격 공격자는 Microsoft Internet Explorer의 취약성을 이용하여 피해자의 권한을 가지고 시스템에서 임의 코드를 실행할 수 있습니다.

- IBM X-Force에서 제시한 보호 경보: Microsoft Internet Explorer mshtml.dll RCE[35]
  - IBM X-Force 보호 서명: JavaScript_NOOP_Sled, JavaScript_Shellcode_Detected
- CVE-2009-3672
- Microsoft 보안 고시 MS09-072호: Internet Explorer용 누적 보안 업데이트 (976325)[36]

[31] IBM X-Force에서 제시한 보호 경보: Microsoft Windows WSDAPI 코드 실행 http://www.iss.net/threats/353.html

[32] Microsoft 보안 고시 MS09-063호: Web Services on Devices API의 취약성으로 인한 원격 코드 실행 허용 문제(973565) http://www.microsoft.com/technet/security/bulletin/ms09-063.mspx

[33] IBM X-Force에서 제시한 보호 경보: Microsoft Windows 커널 폰트 코드 실행 http://www.iss.net/threats/354.html

[34] Microsoft 보안 고시 MS09-065호: Windows 커널 모드 드라이버의 취약성으로 인한 원격 코드 실행 허용 문제 (969947) http://www.microsoft.com/technet/security/bulletin/ms09-065.mspx

[35] IBM X-Force에서 제시한 보호 경보: Microsoft Internet Explorer mshtml.dll RCE http://www.iss.net/threats/355.html

[36] Microsoft 보안 고시 MS09-072호: Internet Explorer용 누적 보안 업데이트 (976325) http://www.microsoft.com/technet/security/bulletin/ms09-072.mspx

12월은 X-Force 애널리스트들이 발견한 Novell eDirectory의 원격 코드 실행 취약성에 대처하기 위한 X-Force 보호 자문을 발표하는 것으로 시작되었습니다. 이 취약성을 통해, 원격 공격자가 시스템에서 임의 코드를 실행하기 위해 사용할 수 있는 특별 제작 요청이 만들어질 수 있습니다. 공격자는 이 취약성을 유발하기 위해 어떠한 유형의 사용자 상호작용을 유도할 필요가 없습니다.

- IBM X-Force에서 제시한 보호 자문: Novell eDirectory 원격 코드 실행[37]
  - IBM X-Force 보호 서명: Application_Control_Request_Overflow
- CVE-2009-0895
- Novell Security 취약성: Novell eDirectory Heap-기반 버퍼 오버플로우[38]

X-Force 팀은 HP OpenView 네트워크 노드 매니저에서 발견한 취약성에 대한 보호 자문을 제작하기도 했습니다. HP OpenView 네트워크 노드 매니저는 인증을 받지 않은 사용자가 임의 HTTP 요청을 보내는 것을 허용합니다. 악성 사용자는 특별 제작된 HTTP 메시지를 전송하여 취약한 스택 버퍼를 범람시킬 수 있습니다.

- IBM X-Force에서 제시한 보호 자문: HP OpenView 네트워크 노드 매니저 원격 코드 실행[39]
  - IBM X-Force 보호 서명: HTTP_Network_Management_Overflow
- CVE-2009-0898
- HPSBMA02483 SSRT090257 rev.2 - HP OpenView Network Node Manager (OV NNM), 임의 코드의 원격 실행[40]

2009년 12월 15일에는 인터넷 위협 등급이 4분기 들어 두 번째로 AlertCon 2로 상향 조정되었습니다. 이번에 인터넷 위협 등급이 상향 조정된 이유는 0-day Adobe Reader 및 Acrobat 문제가 적극적으로 악용되는 것에 주의를 집중시키기 위해서였습니다. 사용자에게 특별 제작된 PDF 파일을 열 것을 요구하는 이 문제를 성공적으로 악용하면 원격 사용자가 시스템에서 임의 코드를 실행하도록 할 수 있습니다.

Adobe 제품, 그리고 특히 Reader와 Flash의 취약성으로 인해, 이들 제품은 취약성의 새로운 "브라우저"가 되었습니다. X-Force 팀은 2009년에 Adobe Acrobat, Reader 및 Flash의 문제에 대처하기 위해 네 차례의 경보를 발령했습니다. 네 차례에 모두, 취약성은 특정한 표적을 대상으로 한 악용이나 스팸/악용 봇에 포함된 악용 수단의 형태로 인터넷 환경에서 악용되고 있었습니다. 실제로 IBM X-Force의 2009년 중간 동향 및 리스크 보고서에 따르면 2009년 상반기에 이용된 가장 인기 있는 악용 수단은 오래된 Adobe Acrobat 및 Reader 취약성이었습니다(CVE-2007-5659). 향후에 공격자들은 Adobe PDF 파일을 악의적인 활동의 경로로 계속 사용할 것으로 전망됩니다.

- IBM X-Force에서 제시한 보호 경보: Adobe Acrobat 및 Acrobat Reader 원격 코드 실행[41]
  - IBM X-Force 보호 서명: JavaScript_NOOP_Sled, PDF_Stream_Hiding, PDF_JavaScript_Detected, PDF_Encoded_JavaScript_Tag
- CVE-2009-4324
- Adobe Reader 및 Acrobat에 관한 Adobe 보안 자문[42]

[37] IBM X-Force에서 제시한 보호 자문: Novell eDirectory 원격 코드 실행 http://www.iss.net/threats/356.html
[38] 보안 취약성: Novell eDirectory Heap-기반 버퍼 오버플로우 http://www.novell.com/support/viewContent.do?externalId=7004912&sliceId=1
[39] IBM X-Force에서 제시한 보호 자문: HP OpenView 네트워크 노드 매니저 원격 코드 실행 http://www.iss.net/threats/357.html
[40] HPSBMA02483 SSRT090257 rev.2 - HP OpenView 네트워크 노드 매니저(OV NNM), 임의 코드의 원격 실행 http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01950877
[41] IBM X-Force에서 제시한 보호 경보: Adobe Acrobat 및 Acrobat Reader 원격 코드 실행 http://iss.net/threats/358.html
[42] Adobe Reader 및 Acrobat에 관한 Adobe 보안 자문 http://www.adobe.com/support/security/advisories/apsa09-07.html

2009년 4분기 추가 요점

이어지는 내용에서는 2009년 4분기에 보안 전문가들이 직면한 몇몇 추가적인 위협에 대해 간략히 다룹니다.

주요 보안 침해

매년 몇몇 보안 침해 사건이 널리 보도되어 소비자 및 직원의 정보가 악의적인 개인이나 신분(ID) 도용 범죄 단체에 노출될 위험을 방지해야 하는 필요성에 주의를 집중시키게 됩니다. 정보의 손실 또는 도난 외에, 기업 및 개인은 멀웨어, 해킹, 피싱 공격과 다양한 소셜 엔지니어링 기법을 통해 정보가 노출될 위험에 처합니다. 또한, 우편물을 훔치거나, 쓰레기를 뒤지거나, 직원 기록이나 도난 당한 기록으로부터 정보를 획득하는 등의 오프라인 수법도 있습니다. 아래에는 4분기에 알려진 몇 가지 주요 보안 침해 사건이 나와있습니다.

- **BlueCross BlueShield** – 의사 85만 명의 개인 정보를 암호화되지 않은 파일에 저장한 노트북을 도난 당함.
- **Eastern Illinois University** – 바이러스가 서버 손상의 원인이 되었을 수 있음. 약 9,000명의 재학 및 졸업생에게 수집한 개인 정보를 수록한 파일이 공격자에 의해 액세스되었을 수 있음.
- **Microsoft** – 수천 명에 이르는 Windows Live Hotmail 고객의 인증 정보가 타사 사이트인 pastebin.com에서 노출되었음. 공급업체는 이 같은 보안 침해가 "피싱 수법에 기인했을 가능성이 높다"고 시사함.
- **NARA(미국국립문서기록보관청)** –7,000만 명에 달하는 미 퇴역 군인의 개인 정보가 저장되어 있는 하드디스크가 분실되어 이들의 개인정보가 위험에 노출됨.
- **Twitter** – Twitter 웹사이트의 DNS 설정이 하이재킹되어 두어 시간 동안 트래픽의 80%가 다른 웹사이트로 이동됨. 이 사건 도중에 보안이 침해된 Twitter 계정이 있는 지는 확인되지 않음.
- **UAAN(Universal American Action Network)** – 수신인의 사회보장 번호가 기록된 엽서 8만 장이 고객에게 발송됨.
- **버지니아 주 교육청(Virginia Department of Education)** – USB 메모리를 잃어버림으로 인해 버지니아 주의 103,000명이 넘는 평생 교육 이수자의 민감한 정보가 위험에 노출됨.

악성코드 분야

IBM X-Force VPS(Virus Prevention System) 팀은 위협의 가장 지배적인 특정을 기준으로 악성코드를 분류합니다. 주요 악성코드 유형은 다음과 같습니다.

- **백도어** – 원격 공격자에게 피해 시스템에 로그온하거나 피해 시스템에서 임의 명령을 실행할 수 있는 기능을 제공합니다.
- **기타** – 다른 주요 유형에 해당되지 않는 분류되지 않은 악성 프로그램.
- **PUP(바람직하지 않을 수 있는 프로그램)** – 사용자가 설치에 동의할 수 있지만 시스템의 보안 상태에 영향을 미치거나 악의적인 목적으로 사용될 수 있는 프로그램. 예로는 애드웨어, 다일러 및 핵툴/(스니퍼, 포트 스캐너, 멀웨어 제작 키트 등을 포함하는) "해커 툴" 등이 있습니다.
- **트로이 목마** – 스파이, 정보 훔치기, 키보드 로깅 및 추가 멀웨어 다운로드와 같은 다양한 악성 기능을 수행합니다.
- **바이러스** – 호스트 파일을 감염시킴으로써 전파됩니다.
- **웜** – 이메일, 네트워크 공유, 이동식 드라이브, 파일 공유 또는 인스턴트 메시징(IM) 애플리케이션을 통해 자가 전파됩니다.

본 문서에 글을 기고한 분들은 다음과 같습니다.

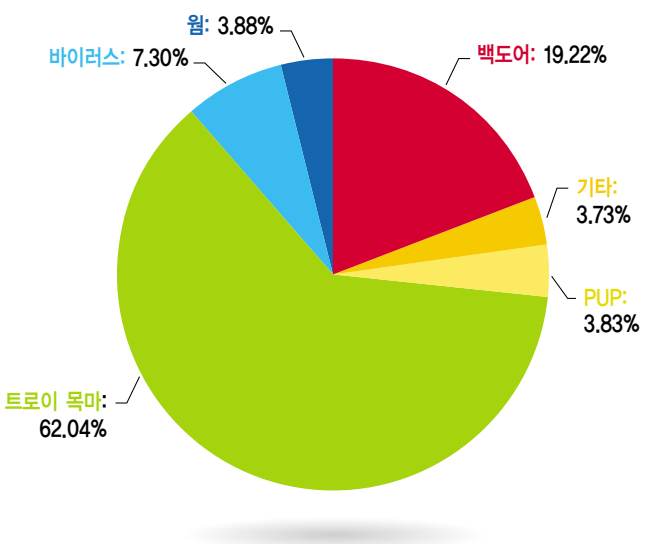
David MacKinnon – 보안 인텔리전스 애널리스트
IBM MSS 인텔리전스 센터

Troy Bollinger – 선임 연구원
IBM MSS 인텔리전스 센터

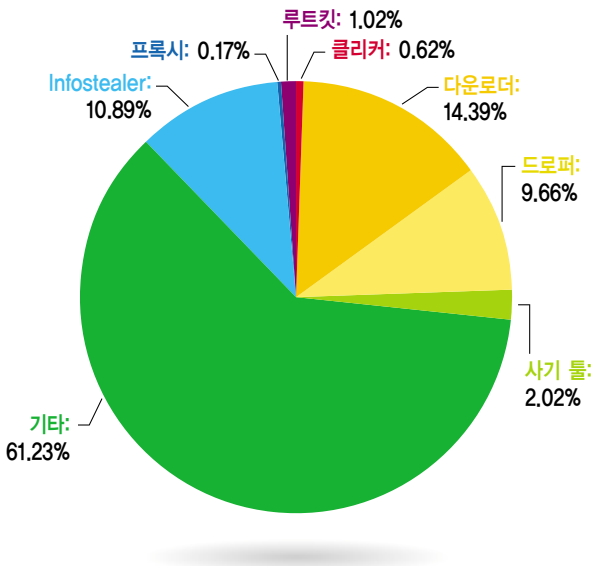
Michelle Alvarez – 팀장
IBM MSS 인텔리전스 센터

IBM X-Force 데이터베이스

IBM X-Force VPS(Virus Prevention System) 팀



출처: IBM X-Force



출처: IBM X-Force

한국IBM Global Business Services
(135-270) 서울시 강남구 도곡동 467-12
군인공제회관빌딩 5층

TEL: (02)3781-8000
www.ibm.com/kr

2010년 3월

Printed in Korea

TIL 14000-USEN-00