

2008년도 시스코 보안 백서



글로벌 보안 동향 및 위협 분석



목차

2008년도 시스코 보안 백서는 작년 한해 동안의 Global 보안시장에 대한 개요와 분석 및 Intelligence를 제공합니다. 본 백서에는 2008년 1월부터 10월 사이에 수집한 보안 위협 요인과 동향이 포함되어 있으며 동 기간 동안 있었던 보안 상황 변화에 대한 개요를 제공합니다. 또한 시스코 보안 전문가의 권고사항과 지금까지 확인된 동향이 2009년에는 어떻게 전개될 지에 관한 보안 동향 예측도 함께 제공하고 있습니다.

2 소개

온라인 위협

웹

악성 프로그램

봇넷

스팸

데이터 손실

내부인 위협

취약점

2008년의 상위 보안 문제

6 온라인 보안 위협 및 동향

웹 동향

합법적인 웹 사이트 이용하기

합법적인 웹 사이트를 이용한 손쉬운 감염

악성 프로그램 동향

휴대폰 악성 프로그램: 증가하는 수익성

"지하" 인터넷 경제

Asprox: 이전 트로이 목마 바이러스의 변형

봇넷 동향

사회 공학의 중요성

대통령 선거를 악용하는 새로운 악성 프로그램

베이징 올림픽 위조 티켓 사기 사건

스팸 및 피싱 동향

스피어 피싱 사례

이메일 명성을 이용한 하이잭킹

16 정보 유출

정보 유출 방지를 위한 입법화

제도의 한계

기기 리사이클링(재활용)의 위험

ID의 도난

일반 대중을 겨냥한 ID 탈취

ID 관리에 대한 재고

20 인적 요인

인간 심리를 이용한 위협

원격 작업, 온라인 커뮤니티: 기회 및 위험

온라인/오프라인 범죄에 온라인 커뮤니티 사이트 및

웹 2.0 사이트 사용

24 내부인에 의한 위협

금융 위기로 내부인에 의한 위험이 증가할 수 있음

26 신뢰 문제

새로운 방법에 의한 신뢰 손상

프라이버시 및 신뢰 위반

30 취약점

웹 취약점

ActiveX 취약점

DNS 취약점

DNS 캐시 포이즈ンを 사용한 최근 공격

DNS의 중요성

DNS 캐시 포이즈넌 공격

TCP 스택 테이블 구현 취약점

네트워킹 장비 취약점

가상화 취약점

암호화 취약점

운영 체제 취약점

데이터베이스 및 사무실 생산성 애플리케이션의

취약점

모바일 장치 취약점

38 지정학적/정치적 갈등

갈등에서 사이버 명령까지

41 인터넷 보안 위협에의 대응

DNSSEC

업계 및 정부의 이니셔티브

적용 가능한 기술들

더 쉽게 보안을 구현할 수 있게 해주는 표준

44 결론 및 주요 권장사항

IT를 최전선에 배치

주요 권장사항

2009년에 예상되는 주요 동향

보안에 대한 전체론적인 접근 방식

소개



작년 한 해 동안에도 데이터 및 온라인 보안과 관련된 많은 사건이 발생했습니다. 작년에는 그전 해의 **Melissa**, **Slammer**, **Storm** 등과 같은 악명높은 유해 트래픽 공격은 없었지만 보안공격에 대한 방어와 지속적인 경계의 필요성은 여전히 커지고 있는 상황입니다.

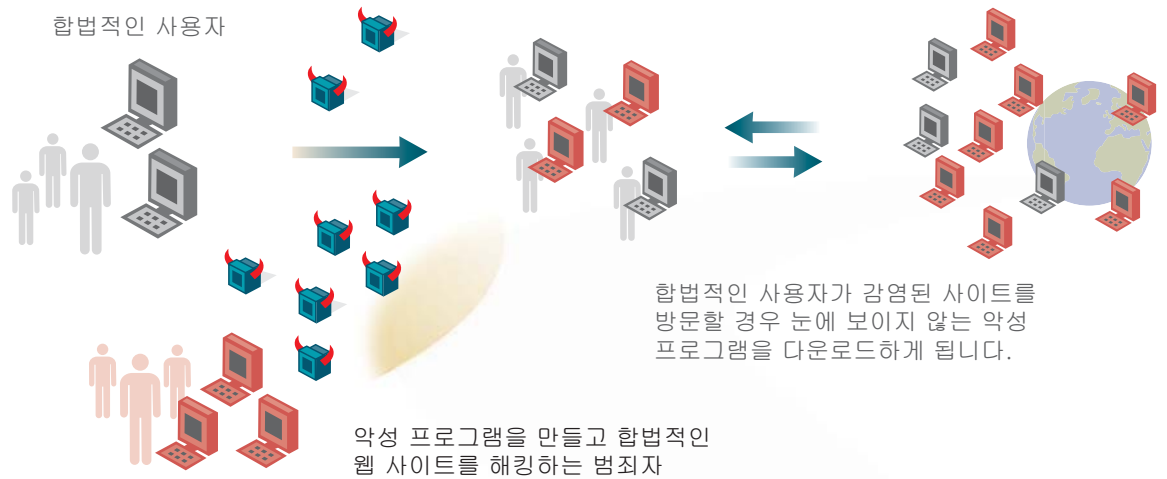
지난 해와 비교하여 규모는 비교적 더 작아졌지만 대상을 명확히 지정할 수 있는 더 많은 수의 캠페인을 통해 중요한 데이터에 액세스함으로써 온라인 범죄가 더 교묘해지고 더 효율적으로 변하고 있습니다. 내부인으로부터의 위협, 온라인 커뮤니티 민감성 및 실수로 인해 데이터 손실을 초래하는 부주의 같은 형태의 인성적 요인이 수 많은 보안 사고의 주요한 요인으로 대두되고 있습니다. 협업 및 생산성을 늘리기 위해 모바일 장치, 가상화, 클라우드 컴퓨팅이나 기타 웹 기반 도구와 웹 2.0 애플리케이션과 같은 기술을 사용하는 조직이 늘어나면서 회사 네트워크의 범위도 확장되고 있으며 그만큼 잠재적인 보안 위험도 증가하고 있습니다. 많은 서로 다른 시작점이나 “위협 벡터(Threat Vector)”를 통해 개인과 조직의 보안이 손상되고 있습니다. 예를 들어 모바일 장치와 보안이 적용되지 않은 하드웨어, 운영 체제 취약점, 사무 생산성 향상 애플리케이션, 암호화 도구 및 기타 수많은 위협 벡터들이 위협의 대상이 될 수 있습니다.

온라인 위협

양적 측면과 침투성 면에서 2008년 가장 심각한 보안 위협은 온라인 관련 요소였습니다. 이 온라인 위협은 그 범위와 양적 측면에서 계속 증가하고 있으므로 보안 전문가들에게 여전히 가장 큰 관심사입니다. 이 온라인 위협은 대부분이 다음 요소와 밀접하게 관련되어 있습니다.

- WWW(World Wide Web)
- 악성 프로그램
- 봇넷
- 스팸

온라인 범죄 환경



웹

온라인 위협 영역에서 전체 웹 환경은 중요한 역할을 수행합니다. 온라인 범죄자들은 교묘하게 합법적으로 가장한 악의적인 웹 사이트를 계속 만들어서 중요한 개인 정보를 도용하고 사이트 방문자에게 악성 프로그램을 배포합니다. 온라인 범죄자는 뉴스 미디어나 대형 쇼핑몰과 같은 신뢰할 수 있는 조직의 합법적인 웹 사이트를 해킹하여 해당 사이트에서 방문자에게 눈에 보이지 않는 악성 프로그램을 배포하게 하거나, 이런 목적을 위해 기존 웹 애플리케이션과 플러그인을 만들거나 감염시킵니다. 그리고 인터넷의 기본 인프라에는 온라인 범죄자가 수 천명의 순진한 인터넷 사용자를 한 번에 악성 웹 사이트로 유인할 수 있는 취약점이 노출되어 있습니다.

악성 프로그램

웹은 악성 소프트웨어로 컴퓨터를 감염시킬 수 있는 유일한 방식은 아니더라도 점점 주요 수단이 되고 있습니다. 오늘날의 대부분 "악성 프로그램"은 컴퓨터,

통신 장치 또는 네트워크를 통해 다른 사람을 통제할 수 있도록 설계되어 있습니다. 일부 악성 프로그램은 직접 영향을 미치거나 감염된 컴퓨터의 작업을 바꿔버립니다. 예를 들어 사용자가 알지 못하게 인터넷에 연결시키거나 다른 악성 프로그램을 설치합니다. 다른 악성 프로그램은 컴퓨터나 네트워크에서 사용자 암호나 신용카드 번호와 같은 중요한 정보를 검색하여 온라인 범죄자의 컴퓨터로 정보를 전송하기도 합니다. 게다가 점점 더 많은 악성 프로그램이 개발되어 판매까지 되고 있는 실정입니다.

봇넷

오늘날 대부분 악성 프로그램의 주요 임무는 컴퓨터에 침입하여 해당 컴퓨터를 봇넷으로 만드는 것입니다. 봇넷은 악성 프로그램으로 손상된 컴퓨터(봇넷 노드 또는 "좀비") 수 천대로 구성되어 있으며 대규모의 온라인 범죄 행위의 근간이 되고 있습니다. 봇넷을 관리하는 사람은 감염된 컴퓨터의 처리 능력과 대역폭을 다른 사람에게 대여하거나, 이를 직접 사용하여 대규모의 스팸을 발송하거나 웹 사이트를 공격하거나 다른 범죄 행위에 관여할 수 있습니다.

2008년도 발생 국가별 스팸 발생 비율

발생 국가	전세계 스팸의 백분율
미국	17.2%
터키	9.2%
러시아	8.0%
캐나다	4.7%
브라질	4.1%
인도	3.5%
폴란드	3.4%
한국	3.3%
독일	2.9%
영국	2.9%
태국	2.8%
스페인	2.8%
이탈리아	2.4%
아르헨티나	2.1%
콜롬비아	2.1%
프랑스	2.0%
기타	26.7%

스팸

스팸 또는 원하지 않는 이메일은 전세계 거의 모든 인터넷 사용자와 조직에 영향을 미치는 가장 일반적인 인터넷 위협 중 하나입니다. 스팸도 다음과 같이 여러 유형이 있습니다.

- 의약품, 프린터 카트리지, 기업 장비 등을 판촉하는 이메일 메시지
- 악성 프로그램이 포함된 첨부파일이 있는 이메일 메시지
- 받는 사람에게 회신이나 웹 사이트의 양식 기입을 통해 개인 정보를 제공하도록 유인하는 "피싱" 이메일
- 받는 사람이 안전하다고 신뢰할 수 있는 웹 사이트의 URL을 포함하면서 실제로는 악성 프로그램을 배포하는 이메일 메시지.

아직도 많은 스팸 발송자들이 캠페인별로 수백만 명의 받는 사람에게 "대량 발송" 스팸을 무작위로 발송하고 있고, 이에 따라 수 많은 스팸 방지 제품들이 이런 유형의 메시지를 필터링하기 위해 노력하고 있습니다. 그러나 이 보다 더 교묘한 "피싱" 스팸은 개인 또는 금융 정보를

빼내오는 경우입니다. 오늘날 대세는 피싱 스팸의 경우 규모는 더 작지만 대상은 더 명확해지고 있습니다.

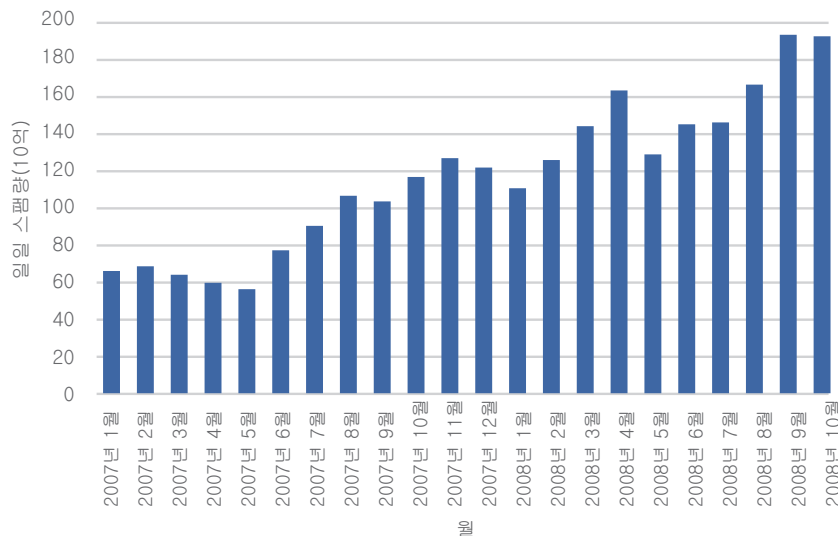
스팸 발송자는 메시지의 설계와 효율성을 계속 개선해나가고 있습니다. 더 합법적이고 전문가인양 가장하기 위해 매우 시사적인 내용의 제목을 사용하기도 하고, 특정 유형의 스팸은 매우 신중한 사용자저도 속아넘어갈 수 있게 다양한 기술을 사용하여 스팸 방지 솔루션을 더 쉽게 뚫고 들어옵니다.

실제로 스팸 메시지를 발송하기 위해 온라인 범죄자는 거의 자신이 소유하는 컴퓨터를 사용하지 않고 대신 봇넷을 임대하거나 구축하여 대신 메일을 보내도록 하고 있습니다. 이 경우 주로 다음과 같은 프로세스를 거칩니다.

- 봇넷 노드에서 스팸을 발송합니다.
- 받는 사람은 악의적인 웹 사이트로 연결되는 이메일 메시지를 받게 됩니다.
- 이 악의적인 웹 사이트로 연결되면 악성 프로그램을 사이트 방문자의 컴퓨터에 다운로드하게 하여 방문자의 컴퓨터를 제어합니다.

평균 일일 스팸량

2008년도 일일 스팸량은 2007년과 비교하여 거의 두 배로 증가하였습니다.



- 감염된 컴퓨터는 봇넷의 일부가 되어 스팸 발송을 시작합니다.

데이터 손실

데이터 손실은 랩톱이나 이동식 저장소 미디어 같은 장비를 분실 또는 도난 당하거나, 컴퓨터나 네트워크를 침입 당하여 중요한 데이터나 지적 재산을 도난 당한 경우 주로 발생합니다. 온라인 위협보다 데이터 손실 사고로 인해 영향을 받는 조직이나 개인의 수가 더 적을 수 있지만, 데이터 손실의 영향은 엄청날 수 있습니다.

데이터 손실을 경험한 조직은 신용과 신뢰성에 심각한 영향을 받을 뿐만 아니라, 주가 급락, 소송, 손해 보상과 같은 금전적 피해로 인해 많은 비용을 부담하게 될 수도 있습니다. 개인의 경우 주민등록번호나 금융 정보와 같은 개인 정보가 손상되는 데이터 손실이 발생할 경우 오랫동안 생활과 금전 면에서 심각한 지장을 받을 수도 있습니다.

네트워크의 데이터의 보안을 더 보강하고 데이터 침해를 당사자에게 알려주는 데 중점을 둔 입법활동과 업계의 움직임이 점점 더 커지고 있습니다. 많은 조직들이 중요 데이터에 대한 기존의 정책을 준수하는 데 보다 노력을 강화하고 있습니다. 그러나 이러한 정책이나 이니셔티브를 준수한다고 해도 안전이 보장되는 것은 아닙니다. 데이터 손실의 위험 요인이 점점 더 늘어나고 진화하면서 이런 문제를 해결하기 위한 움직임이나 입법에 관한 노력을 앞지르고 있기 때문입니다.

내부인에 의한 위험

데이터 손실이나 기타 보안 사건을 책임지는 사람이 내부인인 경우, 즉 현재 직원이거나, 이전에 근무한 직원인 경우가 있습니다. 이들이 문제를 일으키거나 개인적인 이익을 추구할 수도 있습니다. 이런 내부인의 위험은 내부인이 조직의 보안 취약점과 이를 이용하여 데이터나 돈을 갈취할 수 있는 방법이나, 협박을 통해 자산을 편취할 수 있는 방법을 잘 알고 있기 때문에 매우 심각할 수 있습니다. 오늘날처럼 직업을 잃거나 자신의 근무 환경에 대해 만족하지 못하는 불확실한 경제 상황에서, 기업은 더 적은 예산으로 보안 문제를 해결해야 하기 때문에 내부인 위험의 가능성은 더 높아집니다. 이러한 내부인 위험은 갈수록 관심이 집중되고 있는 영역입니다.

취약점

호기심, 신뢰, 부주의와 같은 인성을 이용하는 것 외에도 범죄자들은 기술, 소프트웨어, 시스템 취약점 등을 이용하여 컴퓨터와 네트워크에 액세스하기도 합니다.

2008년의 주요 보안 문제

갈수록 더 빨라지고 교묘해지는 위험과 범죄

- 온라인 범죄 시장은 시간이 갈수록 더 전문화되고 관련 기술도 계속 진화하고 있습니다.
- 공격의 대상을 점점 더 구체적으로 지정함으로써 범죄 피해의 효과도 더 극대화되고 있습니다.
- 많은 유형의 신용 하이잭킹(사용자의 다른 사람에 대한 평판을 이용한 공격) 범죄가 점점 더 많아지고 있습니다.
- 이메일과 웹 사이트가 혼합되어 있고 온라인 커뮤니티 기술을 사용하는 복합적인 위험이 이전보다 더 일반화되고 있습니다.

전체 웹 환경의 취약점을 이용하여 컴퓨터와 네트워크 제어

- 봇넷 침입은 여전히 흔하고 위험합니다.
- 알려진 취약점에 대한 패치가 발표되지 않고 기존의 보안 정책도 무시되고 있습니다.
- 기업에서 웹 기반 협업 기술의 사용이 늘어나면서 생산성 개선의 장점도 있지만 위험도 그 만큼 증가하고 있습니다.

“보이지 않는 위험”(예를 들어 합법적인 웹 사이트에서의 감염을 감지하기 어려운 경우)이 일상화되고 이에 대한 전통적인 보안 솔루션의 효과가 미미해지고 있습니다.

데이터 및 지적 재산의 손실은 지속적인 도전 과제입니다.

- 데이터 손실은 주로 기술 및 인성의 취약점을 악용하여 발생합니다.
- 기업의 신용, 신뢰성 및 재무 상태에 영향을 미칠 수 있습니다.
- 위험 벡터(Risk vectors)에는 온라인 위험, 모바일 장치 및 내부인 위험이 포함됩니다.

2008년 온라인 범죄자들은 브라우저와 브라우저에서 실행되는 도우미 개체, 미디어 플레이어 및 플러그인, 웹 서버와 애플리케이션 소프트웨어, 웹 기본 인프라 코어와 같은 전체 웹 환경의 취약점을 이용하여 컴퓨터, 네트워크 및 데이터에 액세스하였습니다.

그 중에서도 사무 생산성을 향상시키는 애플리케이션, 운영 체제, 모바일 장치 기술, 네트워킹 장비, 가상화 도구, 암호화 기술 등과 같은 분야의 취약점도 악용되었습니다. 그러나 감염된 제품의 공급업체들은 이제야 취약점 공개와 함께 패치를 발표하여 취약점의 영향을 완화하고 있습니다. 따라서 최신 패치를 적용하는 것이 그 어느 때보다 중요해지고 있습니다.



온라인 보안 위험 및 동향

2008년 온라인 보안 위협은 계속 증가 일로에 있습니다. 온라인 범죄자는 스팸, 피싱, 봇넷, 악성 프로그램 및 악의적인 웹 사이트나 손상된 웹 사이트 등의 요소들을 서로 결합시켜 악용함으로써 매우 효율적으로 인터넷 사용자를 사취하고 그들의 보안을 침해하고 있습니다.

웹이야말로 다른 사람이 컴퓨터와 네트워크를 제어할 수 있게 해주는 악성 프로그램을 배포할 수 있는 기본적인 메커니즘입니다. 이런 컴퓨터 대부분이 봇넷의 노드가 되어 컴퓨터 사용자가 알지 못하는 사이에 많은 활동에 관여하게 됩니다.

대량 스팸 발송(악성 프로그램을 다운로드하게 되는 웹 사이트로 더 많은 피해자를 유인하거나 개인 정보를 편취하기 위해 설계된 스팸), 악의적인 웹 사이트의 호스팅 또는 합법적인 웹 사이트 감염 및 서비스 거부(DDoS) 공격으로 웹 사이트나 컴퓨터 네트워크를 전복시키는 시도 등이 봇넷의 활동에 포함됩니다.

웹 동향

15년 전만 해도 WWW(World Wide Web)를 아는 사람이 거의 없었습니다. 오늘날 Google은 전세계에서 가장 신뢰할 수 있는 브랜드 중 하나가 되었고 사람들은 커뮤니케이션, 리서치, 쇼핑, 금융 등 다양한 일상 활동에서 광범위하게 웹을 활용하고 있습니다.

전에 사용하던 초기 브라우저와 달리 오늘날의 웹 브라우저는 상호 작용이 뛰어난 놀라운 기능들을 제공하고 있습니다. 웹 페이지 내 플래시 애니메이션 재생, 유명 가수의 웹 사이트 나 온라인 라디오 방송국의 오디오 스트림 등을 이용하여 방문객들은 음악을 듣거나, 비디오를 자동으로 재생할 수 있고, 온라인 커뮤니티 사이트와 위젯을 통해 개인 블로그의 연락처 정보, 사진 또는 데이터를 온라인 커뮤니티 페이지에 통합할 수 있으며, Adobe PDF 문서를 브라우저 내에서 완벽하게 렌더링할 수 있습니다.

웹 브라우저에서 플러그인, 미디어 플레이어, 브라우저 도우미 개체 및 ActiveX 컨트롤과 JavaScript 명령과 같은 도구를 사용하여 다른 유형의 개체를 웹 페이지에서 활성화할 수 있기 때문에 이 모든 것이 가능한 것입니다. 콘텐츠 관리 시스템 같은 기본 웹 애플리케이션에서는 필요한 때에 필요한 콘텐츠를 표시할 수 있고 포럼 및 위키를 통해 사이트 방문객은 웹 페이지에 신속하게 게시하거나 웹 페이지를 수정할 수 있습니다.

웹의 가능성과 대중성이 커지면서 위험 벡터로서의

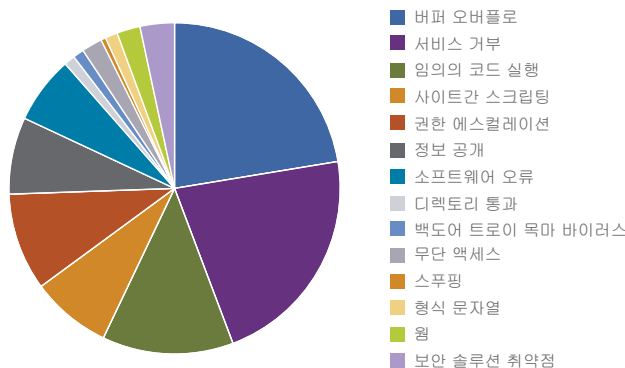
사용도 피할 수 없게 되었습니다.

원래 악성 소프트웨어는 감염된 사무실 문서상의 매크로와 플로피 드라이브를 통해 배포된 다음, Slammer 같은 네트워크 웜을 통해 배포된 후, 이메일 배포를 통해 대량 전송됩니다. 오늘날 방대한 양의 악성 프로그램이 웹 사이트를 통해 다운로드됩니다. 범죄자들은 전체 웹 환경의 취약점을 이용하여 컴퓨터와 네트워크를 제어할 수 있게 됩니다. 자세한 내용은 이 보고서 후반부의 취약점 섹션을 참조하십시오.

이러한 악성 프로그램 감염은 "다운로드로 인한 사용자의 개입"이나 "인지" 없이 발생하는 경우가 종종 있습니다. 누군가가 악의적이거나 감염된 웹 사이트를 방문하게 되면, 웹사이트 호스트는 해당 방문자의 브라우저나 컴퓨터 시스템에서 취약점을 찾기 시작합니다. 여기서 이용할 수 있는 취약점을 발견하면 악성 프로그램을 해당 컴퓨터에 다운로드하기 시작합니다. 사이트 방문객이 감염된 페이지의 링크를 클릭하는 일이 없어도, 어떤 일이 발생하는지 알지 못하는 상태에서 백그라운드에서는 이러한 작업이 자동으로 수행될 수 있습니다.

더 악의적인 웹 사이트에서는 이보다 더 "철저한" 공격이

2008년의 취약점 및 위협 분류



2008년에는 가장 대표적인 취약점과 위협 유형은 버퍼 오버플로와 서비스 거부 공격이었습니다. 그 다음으로 유력한 취약점은 임의의 코드 실행으로 나타났습니다.

이루어집니다. 이 경우 다른 브라우저, 플러그인 및 운영 체제에서 다른 유형의 취약점을 악용하는 여러 다른 유형의 악성 프로그램이 동일한 웹 사이트에서 호스팅될 수 있습니다. 이 경우 웹 사이트 방문객은 악성 프로그램이 사용자의 컴퓨터에 악성 프로그램을 다운로드하기 위해 이용할 수 있는 취약점을 노출할 가능성이 커집니다.

합법적인 웹 사이트 손상

2008년에 새로 유행한 악성 프로그램 전파 방법 중 하나는 합법적인 웹 사이트를 손상시켜서 악성 프로그램 배포의 중심으로 만드는 것입니다. 2008년 4월에만 수천 개의 웹 사이트가 손상되어 사이트 방문객에게 악성 프로그램을 감염시켰습니다.

신뢰할 수 있는 합법적인 웹 사이트에서 악성 프로그램을 유포하게 하거나 악성 코드를 제공하게 만드는 것은 매우 효과적인 공격 방법 중 하나입니다. 합법적인 사이트의 방문객은 사이트의 신뢰성에 대해 의문을 갖지 않기 때문에 콘텐츠와 트랜잭션을 얻기 위해 해당 사이트를 정기적으로 방문할 것입니다. URL 또는 IP 주소 필터링을 사용하는 인터넷 보안 애플리케이션도 해당 웹 사이트의 합법성을 신뢰할 것입니다.

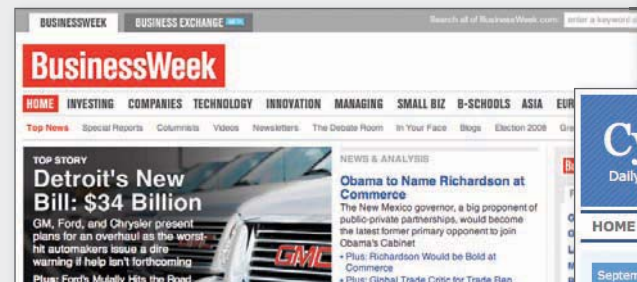
합법적인 웹 사이트가 감염된 경우 특정 사용자 그룹을 정확하게 대상으로 지정할 수 있습니다. 예를 들어, 감염된 사이트에서 학생, 온라인 게이머, 비즈니스 사용자를 대상으로 지정할 수 있습니다. 비즈니스 사용자를 대상으로 하는 경우 감염된 회사 컴퓨터를 통해 비즈니스 네트워크로 채널을 제공할 수 있습니다.

시스코 데이터에 의하면 현재 모든 웹 기반 위협 중 87% 이상이 감염된 웹 사이트 때문인 것으로 나타났습니다. 보안 감사 제공업체인 White Hat Security에 의하면 악성 코드를 호스트하는 웹 사이트의 79% 이상이 합법적인 웹 사이트의 손상인 것으로 밝혀졌습니다. 10개의 웹 사이트 중 9개가 공격에 취약했습니다. 10개의 웹 사이트 중 7개가 사이트간 스크립팅(XSS) 공격에 취약하고, 5개 중 1개 웹 사이트가 SQL 주입 공격에 취약한 결과를 보였습니다.

합법적인 웹 사이트를 손상시키는 일반적인 방식

iFrame 악용: XSS 및 SQL 주입 공격 시에 모두 공통적으로 악성 코드를 배포하는 수단으로 iFrame을 이용합니다. iFrames 공격 시 사용자가 알지 못하는 사이에 컴퓨터에 악성 프로그램이 설치됩니다. 인라인 프레임 HTML 태그라고도 하는 iFrame을 통해 손상된 웹 코드가 다른 웹 서버에 있는 별도의 HTML 문서에 포함될 수 있습니다. 이 악용 방법을 일반적으로 사용한 사례는 iFrame 크기를 0으로 설정하여 사이트 방문객이나 웹 호스트가 알지 못한 사이에 호스트 사이트를 통해 악성 코드를 전달하게 만드는 경우입니다.

SQL 주입: 널리 사용되는 웹 애플리케이션과 서버의 데이터베이스 레이어에 대한 보안 취약점을 이용합니다. 최근 해커들은 SQL(Structured Query Language) 주입 공격을 통해 악성 프로그램이나 눈에 보이지 않는 링크를 합법적인 웹 사이트에서 악성 프로그램 호스트 사이트에 포함시키고 있습니다. 그들은 SQL을 사용하는 웹 페이지에서 양식 및 사용자 로그인 같은 사용자 입력 필드를 통해 전송된 데이터를 수시로 삭제하지 않는 웹 사이트 개발자를 이용하여, SQL 주입 공격을 시도합니다. 웹 애플리케이션 개발 중에 적절하게 보안되지 않는 Microsoft ASP 및 ASP.NET 기술을 사용하는 수 천 개의 웹 사이트가 이런 유형의 공격에 취약한 것으로 증명되었습니다.



2008년 9월 우리에게 잘 알려진 합법적인 사이트인 BusinessWeek.com도 SQL 주입 공격을 받았습니다. 수 백 페이지에 악성 iFrame이 주입되어 사용자는 자신도 알지 못하는 사이 악성 프로그램을 제공하는 러시아의 사이트로 이동되었습니다.

사이트간 스크립팅(XSS): 취약성 있는 웹 사이트의 악의적인 사용자나 악의적인 웹 사이트의 소유자가 사용자의 브라우저에 악성 코드를 전송할 수 있게 하는 웹 애플리케이션의 결함입니다. 이 공격은 주로 HTML 이미지와 프레임 요소(, <frame>, <iframe>) 및 JavaScript를 통해 실행됩니다.

사이트간 요청 위조(CSRF 또는 XSRF): 공격자는 피해자가 현재 특정 웹 사이트에서 브라우저 세션을 사용하고 있음을 파악하여 그 사용자가 현재 또는 영구적으로 인증을 받은 다른 웹 사이트의 피해자로부터 지시를 위조하여 공격하는 것입니다. 예를 들어 공격자와 피해자가 모두 웹 포럼에 온라인 상태로 참가하고 있는 상황에서 공격자는 피해자의 인증을 도용하여 a) 피해자가 자주 이용하고 있고 b) 구매 결정 전에 재인증을 요구하지 않는다는 사실을 알고 있는 전자 상거래 사이트에서 구매를 할 수 있습니다.



2008년 9월에 발생한 악명 높은 사건 중 하나가 온라인 범죄자가 이 SQL 주입 공격으로 BusinessWeek.com 웹 사이트의 수 백 페이지를 공격한 사건입니다. 웹의 방문객 수가 많기로 상위 1000개 사이트에 포함되는 BusinessWeek.com은 웹 사용자로부터 매우 높은 신뢰를 받고 있었습니다. 그러한 점에서 의심없는방문객들에게 악성 프로그램을 제공하는 사이트로는 최적의 사이트로 보였을 것입니다.

악성 프로그램 동향

개인용 컴퓨터를 제어함으로써 많은 온라인 범죄와 이익이 가능해졌습니다. 개인용 컴퓨터를 감염시킨 악성 프로그램이나 악성 소프트웨어로 인해 개인용 컴퓨터가 봇넷 노드가 되는 것이 첫 번째 단계입니다.

2008은 웹 기반 악성 프로그램이 두드러진 한 해였습니다. 온라인 범죄자들은 2007년에도 통했던 웹 기반의 배포 기술을 계속 사용하면서 동시에 효율성과 수익성을 계속 개선해나가고 있습니다.

웹을 통해 배포된 악성 프로그램 중 대부분이 트로이 목마 바이러스인데, 이는 악의가 없고 눈에 보이지도 않으면서 관심을 끌게 설계되어 있어서 설치하기가 쉽습니다. 다운로드된 악성 프로그램을 숨겨주는 루트킷도 널리 퍼져 있습니다. 기타 널리 배포된 악성 프로그램으로는 스파이웨어와 키로거가 있는데, 둘 다 손상 당한 사용자의 컴퓨팅 습관과 웹 서핑 습관에 대한 정보와 암호를 포함한 개인 정보를 악성 프로그램 배포자에게 전송합니다.

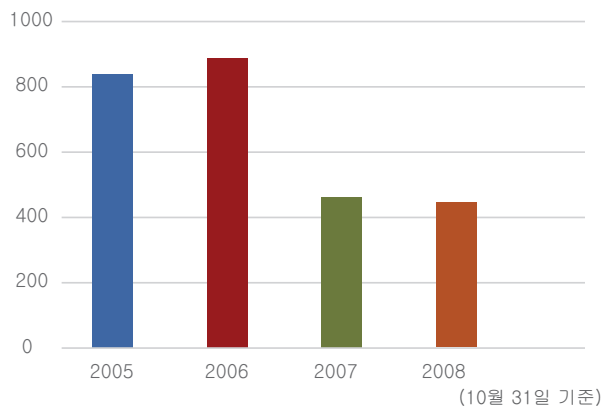
최근 들어서는 이메일 첨부파일을 통해 전파되는 악성 프로그램 수가 줄어들었습니다. 이러한 감소 현상은 웹 기반의 악성 프로그램 전파 방식이 더 효율적이라는 사실이 입증되었고, 악성 프로그램 방지 제품이 활성화되어 악성 프로그램이 포함된 이메일을 신속하게 검색하여 더 많이 차단할 수 있게 되었기 때문입니다. 이러한 요인 때문에 악성 프로그램을 만드는 사람들이 이메일보다 웹을 통해 악성 프로그램을 전파하는 비율이 더 많아졌습니다.

2008년의 첨부파일 기반 악성 프로그램 중 널리 퍼진 악성 프로그램에는 UPS나 FedEx의 배송 양식이 포함되어 있음을 표시한 메시지나 송장, 전자티켓, 전자카드 또는 실제로 실행가능한 비디오나 사진이 첨부되어 있음을 표시한 메시지들이었습니다.

이메일을 통해 전파된 Mytob 악성 프로그램으로 세 군데 영국 병원의 컴퓨터 네트워크가 감염되어서 병원의 IT 시스템이 중단되기도 하였습니다

악성 프로그램을 만드는 사람들은 바이러스 백신 및 악성 프로그램 백신 프로그램의 검색을 피하기 위해 더 은밀하게 설계된 악성 프로그램을 만들고 있습니다. 가장 많이 사용하는 방법 중 하나가 일시적으로 잠복 상태를 유지하는 악성 프로그램입니다. 또 다른 방법은 서명 기반의 악성 프로그램 백신 검색 소프트웨어를 혼란시키기 위해 지속적으로 자동 변경되는 악성 프로그램 코드를 개발한 것입니다.

이메일 첨부파일을 통해 전파된 악성 프로그램 수



이메일 첨부파일을 통해 전파된 악성 프로그램 수는 2007년과 비교하여 2008년에 약간 감소하였습니다. 첨부파일을 이용한 이메일 공격은 지난 2년 간에 50% 감소하였습니다.

휴대폰 악성 프로그램: 증가하는 수익성

2008에는 휴대폰용으로 설계되어 휴대폰을 통해 전파된 악성 프로그램 사례를 볼 수 있습니다.

그 한 예가 SymbOS/Kiazha.A입니다. 이 바이러스는 Symbian OS 장치에서 실행되며 휴대폰의 문자 메시지(SMS)를 삭제하는 "랜섬웨어" 트로이목마 바이러스입니다. 휴대폰이 이 바이러스에 감염되면 휴대폰을 정상적으로 복원하기 위해 휴대폰 충전 카드를 사용하여 비밀 장소로 돈을 보낼 것을 요구하는 메시지가 표시됩니다.

이 트로이 목마 바이러스는 SymbOS.Multidrop.A에 의해 휴대폰에 설치됩니다. 이 바이러스는 휴대폰의 모든 연락처에 2분마다 멀티미디어 메시지(MMS)를 전송시켜 전파되는 웜 바이러스입니다. 이 바이러스는 블루투스를 통해서도 전파되며 휴대폰에 삽입된 메모리 카드에 자신을 복사시켜 삭제해도 다시 복구될 수 있습니다. 전파력을 개선하기 위한 또 다른 전략으로 SymbOS.Multidrop.A는 블루투스를 통해 전파할 수 있고 휴대폰에서 삭제되지 않도록 복제 및 모니터링하는 SymbOS/ComWar.C를 설치합니다.

지난 해에는 PC 보급 비율보다 휴대폰 소유 비율이 훨씬 높은 아시아에서 휴대폰 악성 프로그램이 크게 유행하였습니다. 이 때문에 보안 위험 범죄자들에게는 아시아에서 휴대폰을 통한 악성 프로그램 전파가 잠재적으로 수익성이 더 높은 기회로 여겨질 수 있습니다.

"그림자가 드리운" 인터넷 경제

성공한 온라인 범죄자는 자신의 사업으로부터 막대한 수익을 벌어들이고 있습니다. 수익성이 높아지면서 그들의 기술도 더 전문화되고 혁신되고 있습니다.

온라인 범죄자의 세계도 글로벌화되면서 제품 및 서비스 공급자와 소비자의 네트워크도 함께 번창하고 있습니다.

온라인 범죄자들을 이러한 전문화와 협업을 통해 더 교묘해지고 효율적으로 진화하고 있습니다.

이러한 공격들은 이제 더 이상 공격 툴을 만드는 개발자들에 의해 이루어지는 것이 아닙니다. 대신 공격자는 경쟁력 있고 점점 더 정교해지는 기성 제품과 솔루션 중에서 공격도구를 선택할 수 있습니다. 현재 다음과 같이 교묘하게 설계된 다양한 악성 프로그램 제품이 시판되거나 임대되고 있습니다.

- 봇넷 관리 및 대시보드 유형의 도구
- 대량의 블로그 게시 도구
- 매우 정교한 대량 스팸 발송 도구
- 자동화된 웹 메일 계정 작성 도구(Yahoo!, Gmail, MSN과 같은 웹 메일 호스트에서 봇넷이 웹 메일 계정을 열지 못하도록 방지하는 CAPTCHA(CAPTCHA란 일그러지고 찌그러진 글자를 표시해서 사용자로 하여금 그 글자를 입력하도록 한 후에 폼을 전송하거나 데이터에 접근할 수 있게 하는 방법) 기능을 무력화시킨 일부 도구도 포함됨)
- 스팸머와 스캐머가 Craigslist에 대량의 게시물을 작성할 수 있게 한 계정 작성기
- 키로깅 프로그램

그러나 장기적인 관점에서 보면 온라인 범죄 시장은 관료주의로 흐를 위험이 있을 수 있습니다. 이 경우의 긍정적인 면은 부수적으로 나타나는 피해 수 없는 부작용으로써 행적이 남는다는 것입니다. 따라서 전세계 법률 집행 기관은 앞으로 이러한 범죄자를 추적하여 체포할 수 있는 기회가 더 많아지고 쉬워질 수 있습니다.

Asprox: 이전 트로이 목마 바이러스의 변형

2008년에 가장 큰 영향을 미쳤던 봇넷 중 하나가 Asprox입니다. Asprox는 이전의 트로이 목마 바이러스가 매우 교묘한 봇넷으로 발전하여 합법적인 웹 사이트에서 수 천 건의 SQL 주입 공격을 시도한 바이러스입니다. 수년 전 처음에는 암호를 제공하는 트로이 목마 바이러스였지만 나중에는 피싱 스팸을 발송하는 바이러스로 업그레이드되었습니다. Asprox는 SQL 주입 도구로 업그레이드되기 시작한 2008년 5월에 대대적인 변형이 이루어졌습니다.

이 SQL 주입 도구는 감염된 컴퓨터의 사용자에게 “Microsoft Security Center Extension”(msscncr32.exe)으로 실행되는 합법적인 도구처럼 보입니다. 그렇지만 실제로 백그라운드에서는 Google을 사용하여 SQL 공격에 취약한 Web for Active Server Pages(.asp)를 검색합니다. SQL 주입 도구에서 취약한 페이지를 발견하면 악성 iFrame을 페이지 콘텐츠에 삽입합니다. iFrame은 눈에 보이지 않게 사이트 방문객의 브라우저를 악성 사이트로 우회시켜 피해자의 컴퓨터를 악성 프로그램에 감염시키고 해당 컴퓨터를 Asprox 봇넷에 추가하는 다양한 방법을 시도합니다. 악성 프로그램 백신 프로그램의 검색을 방해하기 위해 Asprox는 TCP 포트 80 또는 82에서 프록시 서버를 통해 통신합니다.

시스코 자료에 의하면 Asprox가 최고점에 달했을 때는 매일 31,000개의 서로 다른 웹 사이트에 iFrame을 주입하는 데 성공한 것으로 나타났습니다.

봇넷 동향

봇넷은 오늘날 많은 온라인 위협과 범죄 행위에 힘을 더해주는 커다란 원동력입니다. 봇넷은 악성 프로그램에 감염된 수천 개의 컴퓨터로 구성되어 있습니다. 봇넷을 관리하는 사람은 봇넷의 처리 능력과 대역폭을 봇넷을 구성하는 컴퓨터에 빌려주거나 스스로 이를 사용할 수 있습니다.

온라인 범죄자들은 스팸, DDoS 공격 발송, 합법적인 웹 사이트 감염, 악성 웹 사이트(예: 봇사이트) 호스팅 및 악성 프로그램 전파 등을 포함한 웹 기반 공격의 다양한 면에 봇넷을 사용하고 있습니다.

2007년에 크게 퍼진 스톰 봇넷은 앞으로 다가올 현상의 전조일 뿐이었습니다. 2008년에는 더 새로워지고 더 교묘하고 강력하며 확장력이 뛰어난 봇넷(예: Mailer Reactor, 크라켄)과 Asprox의 강력한 변형물이 크게 유행하였습니다.

이 봇넷은 동적인 공격을 반복, 동기화 및 배포할 수 있는 재사용 가능한 플랫폼으로 설계되어 있습니다. 다른 많은 웹 2.0 기술처럼 이 봇넷도 협업을 조장하고 네트워크의 효율성을 악용합니다. 이 봇넷은 적응력이 뛰어난 지능형 네트워크로 오늘날 P2P 네트워크로 인한 융통성, 이중화 기능 및 보안 프로토콜을 제공합니다.

사회 공학적 기법의 중요성

온라인 범죄자들은 정교한 사회 공학적 기법을 개발하여 피해자로 하여금 이메일이나 파일을 열어보거나 링크나 온라인 광고를 클릭하도록 유도합니다. 온라인 공격에서 사회 공학적 기법을 사용하는 경우가 2008에도 계속 증가하였고, 2009년에도 더욱 증가할 것으로 예상됩니다. 따라서 이메일, 인스턴트 메시징(IM), 모바일 장치 등을 통한 공격이 더 많아질 것으로 예상됩니다.

"주요 뉴스"와 시사를 중심으로 한 스팸을 만드는 것도 성공 요인 중 하나입니다. 때로 이러한 스팸이 피해자로 하여금 악성 프로그램을 자신의 컴퓨터에 다운로드하게 만드는 악성 사이트로 유도합니다.

그러나 매우 교묘한 피싱 웹 사이트가 포함된 더 감쪽같은 악성 프로그램과 시사와 관련된 사회 공학적 기법을 사용하는 스팸이나 웹 사이트가 더 일반적인 현상이 되었습니다.

이러한 악성 프로그램을 사용할 경우 피해자는 합법적인 것처럼 보이는 웹 사이트로 현혹되어 실제 거래를 하는 것으로 알고 진행하는 프로세스 중에 개인적인 정보를 제공하게 됩니다. 그러나 피해자들은 자신이 구매한 것으로 생각한 상품이나 서비스를 받지 못하게 됩니다. 또는 사기꾼들이 위조품이나 품질이 떨어지는 제품(예: 유명 상표를 모방한 가짜 의약품)을 보내는 경우도 있을 수 있습니다.

2008년에 발생했던 이메일 첨부파일을 기반으로 한 성공적인 악성 프로그램 배포 사례에서도 사회 공학적 기법을 악용했습니다.

UPS 또는 FedEx에서 보낸 것처럼 보이는 이메일을 통해 받는 사람에게 첨부된 송장이나 배송 확인을 검토하여 가짜 수하물의 상태를 확인하도록 요청한 경우가 있었습니다. 피해자가 첨부파일을 열면 악성 프로그램이 자동으로 설치되므로 공격자는 이렇게 컴퓨터를 감염시켜 제어할 수 있게 됩니다.

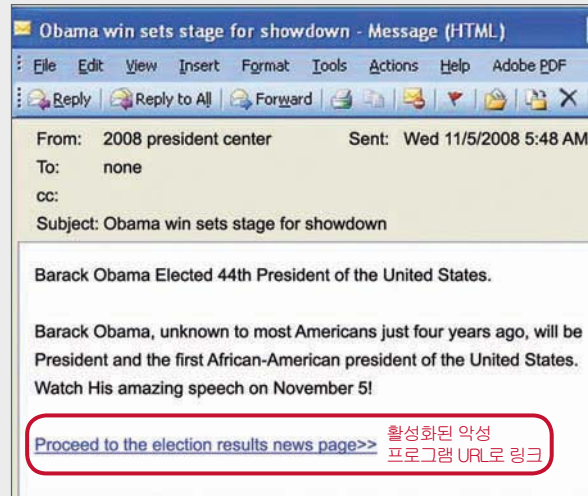
“FedEx나 UPS에서 온 것으로 보이는 이 이메일은 정말 교묘하게 바이러스가 포함되어 있어 사람들이 이를 열어보는 것이 당연합니다.”

—Michael Postlethwait, 시스코 보안 분석가

미국의 납세 신고 기간에 발생한 유명한 바이러스가 있습니다. 이 이메일은 미 국세청에서 보낸 것처럼 위장했습니다. 이 메일은 정말 정부기관의 공식적인 양식을 잘 갖추고 있었고, 사람들이 가지는 국세청이라는 권위와 부담감을 이용하여 열어 보도록 한 것입니다. 일부 사람들만이 미 국세청은 이메일로 통지를 보내지 않고 우편으로 통보한다는 것을 알고 있었습니다.

이렇게 사회 공학적 기법을 악용하여 성공한 사례를 통해 "스케어웨어"가 계속 늘어나는 이유를 설명할 수 있을 것입니다. 스케어웨어는 악성 프로그램 백신이나 스파이웨어 백신 소프트웨어인 것처럼 가장하지만 실제로는 스파이웨어나 악성 프로그램이 자신의 컴퓨터를 감염시킬 것을 두려워하는 사용자의 공포를 이용한 악성 프로그램입니다. 스케어웨어의 다운로드를 제공하는 웹사이트는 신뢰할 수 있는 전문적인 사이트인 것처럼 보이지만 가짜 로고와 추천이 포함되어 있습니다.

오바마 당선과 함께 출현한 새로운 악성 프로그램



시사적인 이메일 메시지는 받는 사람으로 하여금 이메일을 열어서 대응하도록 설득합니다. 최근의 스팸 메일에서는 받는 사람에게 오바마의 승리 연설이 담긴 비디오를 열어보도록 하는 경우도 있었습니다. 예를 들면 다음과 같은 문구가 제목에 포함된 경우가 있었습니다.

- 선거 결과 승리자
- 새로운 대통령의 내각은?
- 오바마 최후 대결에서 승리

받는 사람을 가짜 정부 기관의 봇 사이트로 유인하는 이메일입니다. 그곳에서는 실제로는 데이터를 도용하는 악성 프로그램인데, Adobe Flash Player 업데이트를 설치하라는 메시지를 표시합니다. 이 프로그램을 설치하면 악성 프로그램에서 스크린샷과 암호를 도용하여 우크라이나 키예프에 있는 웹 서버로 도용한 정보를 전송합니다.



정부 기관을 모방한 봇 사이트

이 예제에서 메시지를 받는 사람(오바마의 승리 연설 링크가 포함되어 있다고 믿는 사람)은 실제로는 데이터를 도용하는 악성 프로그램을 제공하는 봇 사이트로 연결됩니다.



실제 America.gov 사이트

베이징 올림픽경기 위조 티켓 사건

2008년에 발생한 가장 교묘한 사회 공학적 인터넷 사건 중 하나는 베이징 올림픽과 연관된 사건으로 범죄자들은 약 4천에서 5천만 달러의 수익을 벌어들였습니다. 뉴질랜드에서 미국에 이르는 여러 국가의 사람들이 위조 티켓 사건에 연루되어 불법적이거나 존재하지 않는 경기 티켓을 판매하였습니다. 어떤 사람은 구하기 어려웠던 개막식 티켓을 구하기 위해 수천 달러를 지불하기도 했습니다.

가장 규모가 큰 공격자는 Beijingticketing.com으로 베이징 올림픽 공식 로고가 표시되어 있고, 신뢰할 수 있는 전문기관과 같은 모양새를 갖춘 사이트입니다. 이 악성 웹사이트는 티켓 구입 과정이나 Facebook 같은 네트워킹 사이트와의 통합 같은 면에서 오히려 공식적인 티켓 판매 사이트보다 월등하여 악성 사이트의 바이러스 배포가 용이했던 것입니다. 심지어 MSNBC도 처음에는 이 사이트를 믿을 수 있는 사이트로 생각했습니다. MSNBC Forbes Traveler 기사에서는 이 사이트로의 링크를 제공하기도 했습니다. 따라서 이 사이트는 높은 검색 엔진 순위를 기록하게 되었고, 결과적으로 검색 엔진을 사용하여 티켓을 구입하려고 했던 사용자들을 합법적인 사이트가 아니라 위조 사이트로 연결하게 된 것입니다.

Beijingticketing.com에서는 사용자에게 등록을 요구하고 기밀 정보를 제공해야 티켓을 구입할 수 있도록 하였습니다. 등록 후 사용자는 신용카드 번호를 제공하고 티켓을 "구입"했지만 실제로는 티켓을 받지 못했습니다. 스캐머들은 수백만 달러의 돈뿐만 아니라, 수천 건의 신용카드 번호를 모아서 나중에 다시 사용하거나 다른 온라인 범죄자에게 다시 판매하려고 했습니다.



사기 티켓팅 사이트

올림픽 티켓 사기 판매 웹 사이트(예: beijingticketing.com)는 2008년 베이징 올림픽 티켓을 구입하려는 수천 명의 사람들을 이용하였습니다.



공식적인 티켓 판매 사이트

스팸 및 피싱 동향

시스코는 매일 2천억 건의 메시지(전세계에서 보내는 모든 이메일의 약 90% 정도)를 스팸으로 정의할 수 있을 것으로 예상하고 있습니다. 이 숫자는 작년의 두 배로, 전세계 모든 인터넷 사용자가 매일 200건의 스팸 이메일을 받고 있음을 나타냅니다. 지난 해에 스팸은 급격하게 발전하였습니다. 봇넷에서 보낸 방대한 양의 의약품/건강보조식품 관련 스팸이나 '빨리 부자되기'와 같은 채택크 관련 스팸은 많은 조직이나 서비스 공급업체에게 있어서 많은 리소스와 처리 능력을 필요로 하는 문제로 남아 있습니다. 대부분의 기업에 설치되어 있는 네트워크 보호, 스팸 방지 및 필터링 솔루션 덕분에 덜 교묘한 대량의 스팸은 보안 문제를 일으키기 보다는 불편함의 문제로 넘어가게 되었습니다.

궁극적으로 받는 사람의 받은 편지함에 들어가는 스팸은 더 위험하고 더 교묘해져서 열거 가능성도 더 높아졌습니다. 최근 스팸에는 일반적으로 "위험이 혼합된" 스팸 메시지가 포함되어 있어서 받는 사람이 클릭을 통해 악성 프로그램 배포 웹 사이트나 피싱 웹 사이트로 이동하게 되는 URL이 포함되어 있습니다.

올해 특히 눈에 띄게 일상화된 스팸으로는 대상이 지정된 피싱(일명 "스피어 피싱")이 있었습니다. 이 공격의 경우 정교한 온라인 범죄자들이 명확하게 지정된 대상을 목표로 더 적은 규모의 피싱을 사용하기 때문에 효율성은 더 커집니다.

초기 피싱의 경우 대상이 광범위하고 대량으로 발송되며 전국적인 규모의 대형 은행을 가장하는 경우가 일반적이었습니다. 그 다음에는 받는 사람 주위에 있는 지방 은행의 ID를 사용하는 피싱이 늘어나기 시작하면서 피싱마다 관련된 메시지 양도 줄어들기 시작했습니다.

최근의 스피어 피싱은 다음과 같은 내용이 주를 이룹니다.

- 동일한 지역 코드를 가진 받는 사람 휴대폰으로 스팸 문자 메시지 전송
- 대학에서 보낸 것으로 위장하여 현재 학생, 졸업생 또는

교직원을 대상으로 하는 이메일

- 피해자에게 Google Adwords 계정에 대한 로그인 정보를 입력하도록 유인하는 이메일(피해자의 신용카드 번호나 개인정보를 도용할 뿐만 아니라 Adwords 트래픽을 범죄자가 운영하는 블로그로 리다이렉션함)
- 특정 임원을 대상으로 한 매우 개인적인 이메일

스피어 피싱 예

스피어 피싱은 현재 전체 피싱의 1% 정도만 차지하지만 점점 더 많은 비율을 차지할 것으로 예상됩니다. 공격이 점점 더 정교해지기 때문에 이러한 동향을 파악하려면 면밀한 모니터링이 필요합니다. 범죄자들은 스팸을 개인 맞춤형 형태로 만들고, 스팸 메시지를 더 신뢰할 수 있게 만드는 데 많은 시간과 리소스를 투자하고 있습니다. 그 이유는 대상이 명확하게 지정된 피해자로부터 중요한 개인 데이터를 얻는 데 성공할 경우 수익성이 더 높아지기 때문입니다.

일반적인 스피어 피싱 공격은 다음 네 단계로 구성됩니다.

- 1 악성 프로그램을 실행하거나, 네트워크를 해킹하거나, 다른 온라인 범죄 리소스로부터 목록을 구입하여 스캐머는 유효한 이메일 주소 배포 목록을 확보합니다.
- 2 도메인을 등록하고 믿을 수 있게 보이는 가짜 웹 사이트를 구축하여 피싱 이메일을 받는 사람을 끌어들이는.
- 3 피싱 이메일을 배포 목록으로 발송합니다.
- 4 스캐머가 피해자로부터 로그인 또는 기타 계정 정보를 받고 데이터나 자금을 도용합니다.

스피어 피싱 공격을 하기 위해 범죄자는 적절한 리소스를 효율적으로 구축하여 피해자로 하여금 중요한 개인 정보를 노출하도록 속여야 합니다.

Subject: Internal Revenue Service Complaint for [REDACTED] [case id: #602f41571ba161cc3dc795df7886f000]

Mr./Mrs. [REDACTED]

We regret to inform you that your company is currently being investigated by our CI department for criminal tax fraud due to a complaint that was filled by a Mr. Keith McCall on 05/06/2007

Complaint Case Number: MT1CF23A
Complaint made by: Mr. Keith McCall
Complaint registered against: [REDACTED]
Date: 05/06/2007

You are being investigated for submitting false income tax returns with the Franchise Tax Board. Instructions on how to resolve this issue aswell as a copy of the original complaint can be found on the link below.

Complaint Documents < [REDACTED] >

스피어 피싱 이메일은 금융기관, 통신사 또는 인지도가 높은 유명 기업 등 신뢰할 수 있는 기관의 메시지를 모방하기 때문에 성공률이 높습니다.

그러나 일반적인 "대량" 피싱 이메일과 달리 스피어 피싱은 특정(대개 도용) 정보를 사용하여 개인적인 메시지를 만들어 공격하기 때문에 받는 사람이 열어서 응답할 확률이 더 높습니다. 이메일 명성을 이용한 하이잭킹 기술과 결합된 스피어 피싱의 개인적인 접근 방식을 통해 범죄자들은 합법적인 이메일 공급업체의 인프라를 사용하여 메시지를 발송하기 때문에 일반적인 피싱 방지 기술을 사용하여 스피어 피싱 이메일을 제거하는 것이 쉽지 않습니다.

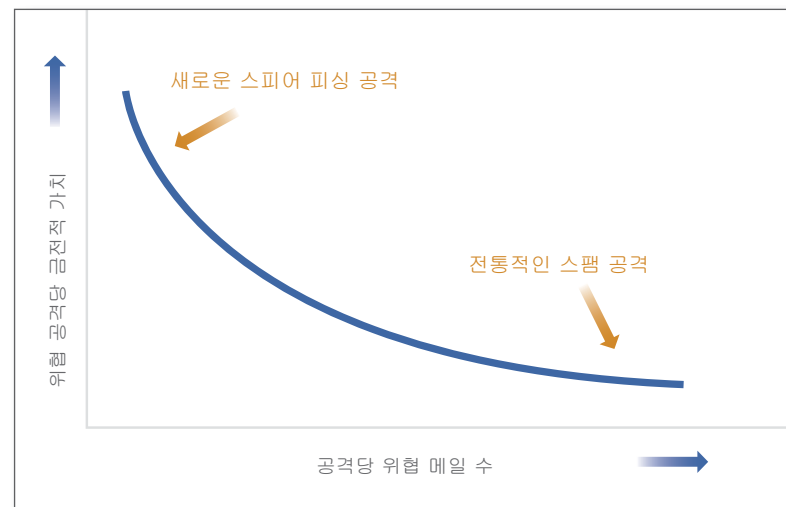
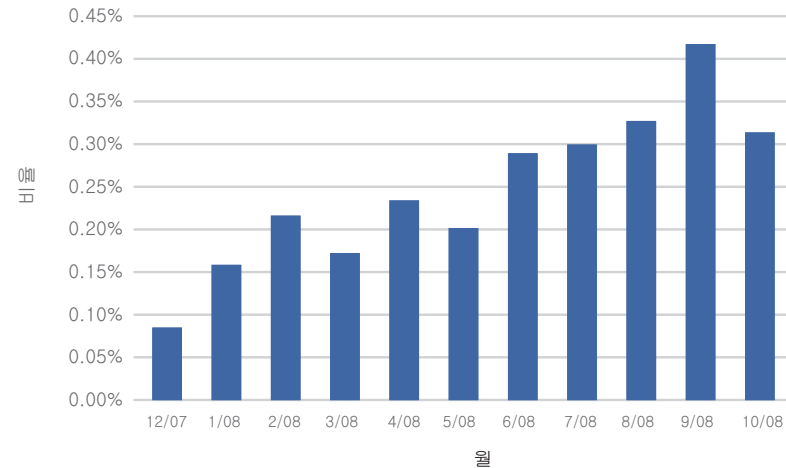
대개의 경우 온라인 범죄자들은 이메일 주소 목록을 임대 또는 도용하므로 발송 메시지를 개인별로 작성할 수 있습니다. 따라서 동시에 수 백만 명에게 배포되는 덜 교묘한 피싱 메시지는 무시할 수 있는 신중한 인터넷 사용자라도 이 경우에는 로그인 이름, 암호 및 기타 중요한 정보를 쉽게 넘겨줄 수도 있습니다.

예를 들어, 다음과 같은 기관에서 보낸 것처럼 위장한 스피어 피싱 메시지를 발송한 경우가 있습니다.

- 국세청(받는 사람이나 회사에 감사 중임을 설명하는 피싱 메일)
- 공정거래 위원회(받는 사람 회사에 대한 "불평"이 접수되었음을 알리는 피싱 메일)
- 지방 법원 또는 세무 법원(받는 사람에게 소환 사실을 알리는 피싱 메일)

이러한 피싱 메일은 공식 메일처럼 보일 뿐만 아니라 일반적으로 받는 사람에게 신속한 답변을 요구하고 대개 "참조 문서"가 첨부되어 있습니다. 그러나 이 파일을 열면 백그라운드에서 악성 프로그램이 실행되어 받는 사람의 컴퓨터나 네트워크를 제어하거나 키로깅 프로그램이 설치됩니다.

대상이 지정된 스팸 공격(비율)



스피어 피싱 메일은 더 적은 수의 사람에게 발송되지만 받는 사람이 응답할 경우 범죄자에게 전송되는 정보가 훨씬 더 많습니다.

이메일 명성을 이용한 하이잭킹

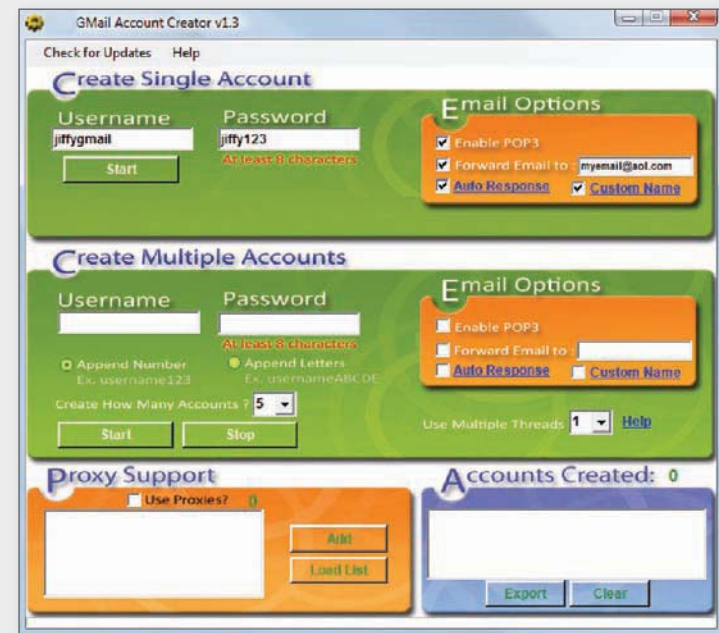
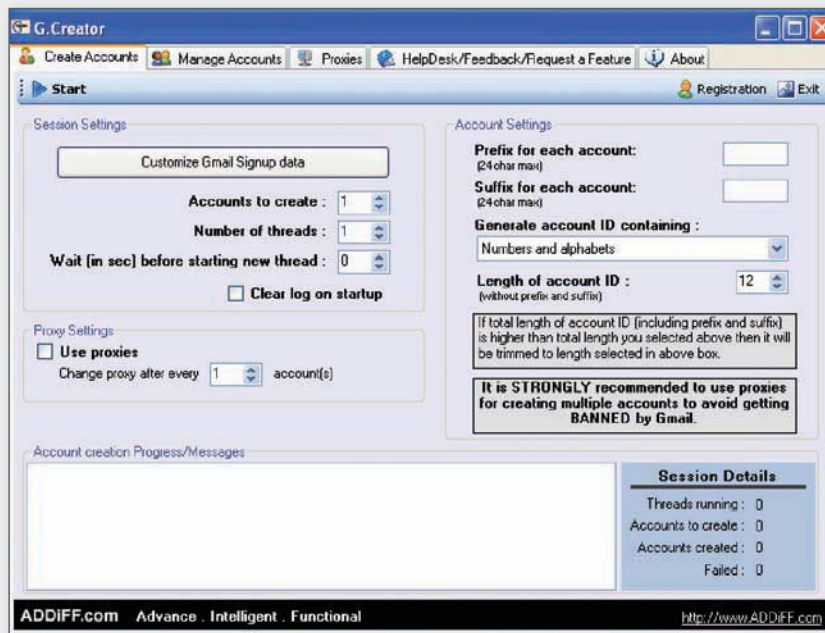
이메일 명성을 이용한 하이잭킹은 합법적인 주요 웹 메일 서비스 제공자가 제공하는 실제 이메일 계정을 사용하여 스팸을 발송합니다. 웹 메일 공급자의 대중적인 신용도를 이용하기 때문에 이러한 이메일의 전달 가능성은 더 높아집니다. 웹 메일 공급자가 보내는 것처럼 제목과 서식을 사용하고, 스팸 방지 솔루션은 Yahoo!, Gmail, Hotmail 등과 같은 대형 웹 메일 공급자의 메일 서버를 차단할 수 없기 때문에 스팸을 검색하여 차단하기가 더 어려워집니다. 신용 하이잭킹의 매력때문에 스팸머들이 이용할 수 있는 상업적인 도구 수가 크게 늘어났습니다. 이러한 도구를 사용하면 스팸머가 더 쉽게 계정을 만들고,

CAPTCHA(CAPTCHA란 일그러지고 찌그러진 글자를 표시해서 사용자로 하여금 그 글자를 입력하도록 한 후에 품을 전송하거나 데이터에 접근할 수 있게 하는 방법)를 무너뜨리고, Gmail, Yahoo!, Hotmail 등과 같은 웹 메일 공급자뿐만 아니라 MySpace, Craigslist 및 블로그 같은 사이트에 IP 주소를 게시 및 유통시킬 수 있습니다. 2008년에 상위 3대 웹 메일 Microsoft, Gmail, Yahoo!의 이메일 명성을 이용한 하이잭킹으로 인한 스팸은 전세계 스팸의 1% 미만에 불과하지만, 이들 3대 웹 메일 서비스 공급자의 전체 메일중에서는 7.6%에 달하는 것입니다. 이들 서비스 공급자의 시스템을 악용할 수 있는 도구가

등장하면서 이러한 웹 메일 공급자들의 평균 스팸 비율도 크게 증가하였습니다.

예를 들어, 2008년 1월 러시아 해커 "John Wane"은 Yahoo!의 CAPTCHA를 무너뜨렸습니다. 이 사건으로 HTTP가 무력화되고 3개월동안 SMTP 공격을 받았습니다. 2008년 5월에는 Google의 CAPTCHA가 깨지면서 막대한 계정 생성이 실패했습니다. 2008년 8월에는 "John Wane"이 AOL CAPTCHA를 깨뜨리는 코드를 발표했습니다.

이메일 명성을 이용한 하이잭킹 도구



주요 웹 메일 공급자의 이메일 명성을 이용한 하이잭킹 도구를 상업적으로 이용할 수 있고 쉽게 얻을 수 있게 되면서 2008년에 이 도구의 사용이 증가되었고 주요 메일 공급자가 보낸 스팸도 크게 증가하였습니다.

데이터 손실

적극적인 노력에도 불구하고 데이터 손실과 관련된 보안 사고는 증가 일로에 있습니다. 이는 시스템과 스토리지 장치의 물리적인 손실이나 도난 또는 안전하지 못한 방식이나 실수로 정보를 공유하기 때문에 발생하게 됩니다. 온라인 범죄자는 악성 프로그램을 사용하여 소비자와 회사 데이터를 온라인으로 도용하고 있습니다. 해커는 안전하지 못하거나 취약한 시스템이나 장치에 침입하여 데이터를 얻습니다. 때로는 내부인이 범죄자이기도 합니다.

점점 더 많은 회사들이 데이터를 보호해야 하는 가장 중요한 기업 자산으로 인식하고 있습니다. PricewaterhouseCoopers의 2008년도 Global State of Information Security Study(정보 보안에 관한 전 세계적인 상황 보고서)에서는 더 많은 조직들이 랩톱뿐만 아니라 데이터베이스, 파일 공유, 백업 테이프 및 이동식 미디어에 있는 중요한 정보를 암호화하고 있다고 보고하고 있습니다. 많은 기업들이 콘텐츠 필터, 웹 사이트 인증/인가 및 보안 브라우저를 포함한 웹/인터넷 기능의 발전에 있어서 중요한 진전을 이루었습니다. 이 보고서에서는 우선 장치를 보호하는 기술의 사용과 허가받지 않은 장치를 검색하거나 침입을 방지할 수 있는 도구의 사용이 증가했다고 인용했습니다.

Privacy Rights Clearinghouse의 Chronology of Data Breaches(데이터 침해 연표)에 의하면 2005년 1월 이후로 2억 3천만 건 이상의 레코드가 보안 침해 때문에 손상되었습니다. 시스코 연구에 의하면 부적절한 데이터 보안은 영업 중단, 생산성 감소, 운영비 증가 등을 포함한 심각한 결과를 조직에 초래할 수 있습니다. 이러한 결과는 중요한 데이터의 손실 자체보다도 더 심각한 것일 수 있습니다.

장비의 분실이나 도난과 관련된 데이터 손실은 기업이나 개인 사용자에게 심각한 문제입니다. Ponemon Institute의 최근 보고에 의하면 중간 규모와 대규모의 공학에서 분실된 랩톱 수가 매년 6십만 건 이상에 달하는 것으로 밝혀졌습니다. 절반 이상의 랩톱이 회수되지 않고 있으며, 많은 사람들이 랩톱을 다시 찾을 수 있으리라는 희망을 갖고 있지 않습니다. 그러므로 당연히 분실된 랩톱을 찾으려는 어떠한 조치도 취해지지 않고 있습니다.

2008년에 랩톱과 관련하여 발생한 사건은 다음과 같습니다.

- 다국적 제약회사의 13,000명 정도 되는 직원의 개인 정보가 들어 있는 랩톱 컴퓨터가 차량에서 도난 당했습니다. 그 안에는 이름, 주소 및 직원 ID 번호 같은 개인 정보가 포함되어 있습니다. 랩톱은 암호화되어

있었지만 플래시 드라이브는 암호화되어 있지 않았습니다. 회사 대변인에 의하면 플래시 드라이브에 중요한 비즈니스 정보가 포함되어 있었다고 합니다.

- 2008년 3월 Clear라는 브랜드의 여행객 등록 프로그램을 운영하고 있는 미국 교통안전청의 공급업체인 Verified Identity Pass(VIP)는 일시적으로 랩톱을 샌프란시스코 국제공항의 사무실에 잘못 둔 적이 있었습니다. 랩톱에는 암호화되지 않은 33,000명 고객의 개인 정보가 들어있었지만 공급업체의 주장에 의하면 손상된 데이터는 없었다고 합니다.
- 2006년 수백만 명 재향군인의 기록이 보관되어 있는 랩톱을 도난 당해서 심각한 혼란을 겪은바 있는 미국 재향군인회에서는 2008년 봄(이때에도 직원의 아파트에서 또 다른 랩톱 도난 사건이 발생)에 새로운 보안 정책을 테스트하였습니다. 이 당시 데이터는 암호화되어 있었고 적절한 인증 권한이 없는 사람은 컴퓨터에 액세스할 수 없었습니다. 그리고 재향군인회는 분실된 장비를 알고 있었습니다. 해당 직원은 재향군인회와 지역 경찰서에 즉시 보고하였습니다.
- 영국 국방부는 600,000명 징집 대상자와 관련된 암호화되지 않은 정보가 포함된 랩톱을 징집 담당자의 차량에서 도난 당했을 때 심각한 보안 침해에 관해 보고한 바 있습니다. 이 랩톱에는 금융 및 여권 정보와 의료 기록이 포함되어 있었습니다.

다행히 장비의 분실 또는 도난 사건으로 인해 정보가 온라인 범죄자에게 전달되는 경우는 극히 드뭅니다. 온라인 범죄자는 손상된 데이터를 액세스 및 이용하여 이익을 취할 수 있는 전문 기술을 갖고 있습니다. 대개는 도난 사실을 숨기기 위해 데이터를 깨끗이 지우고 장비를 빨리 다시 판매하는 것을 목적으로 하는 단순한 도난 사건입니다.

규제 법률상의 데이터 손실 문제

데이터 침해 보고 법률에 의해 회사는 중요한 데이터의 손실 가능성이 있는 경우(예: 랩톱 도난) 보고하도록 되어 있습니다.

현재 42개 주와 콜롬비아 특별구(DC)에 데이터 침해 보고 법률이 등록되어 있거나 법률 제정을 준비하고 있는 중입니다. 주마다 법률이 다르지만 일반적으로 California Security Breach Information Act(캘리포니아 보안 침해 정보 법령)(SB-1386)을 따릅니다. 이 법령에 의하면 고객의 개인정보 데이터를 전자적인 방법으로 보관하고 있는 조직은 해당 정보의 보안 침해 사실을 안 경우 이를 개인에게 보고하도록 규정하고 있습니다.

반면 미국 정부는 이러한 보고를 연방 정부 수준에서 해결하고 각 주의 법률적 차이를 통합하는 노력을 기울이고 있습니다. 일부 법률은 더 강화될 수 있습니다. 또는 연방 정부의 법률을 다른 국가에서 승인되도록 하거나 제정 대기 중인 법률과 조율하려는 노력도 기울이고 있습니다.

이외에도 중요한 데이터의 공유에 관해 다루는 법률도 증가하고 있습니다. 2008년에는 더 강력한 데이터 보호와 데이터 손실 위반에 관한 법률의 시행에 초점을 맞추기 위한 새로운 미국 내 준수 규정과 시장 중심의 업계 노력이 발표되었습니다. 연방 정부에서 발표한 새로운 공정하고 정확한 신용 거래법(Fair and Accurate Credit Transactions Act)의 경보 장치(Red Flags) 규정은 여러 업계에 적용되는 규정이며, 기업으로 하여금 ID 도난 방지 프로그램을 구현하는 비용을 청구하기 전에 해당 프로그램을 제공하도록 규정하고 있습니다. 그러나 최초 시행 기간은 2008년 11월에서 2009년 5월 1일로 연기되었습니다.

2008년 10월 캘리포니아주는 환자 의료 정보에 대한 인증되지 않은 액세스, 환자 기록의 부주의한 공개, 금전적 이득을 위해 의료 정보를 불법적으로 악용하는 사례에 초점을 맞추어서 기존 의료 프라이버시 준수 규정을 강화하여 두 건의 프라이버시 법률, SB-541과 AB-211을 통과시켰습니다

2009년 1월 Health Information Trust Alliance도 HITRUST Common Security Framework(시장 중심의 최적 사례)를 발표할 예정입니다. 이 프레임워크는 ISO 2700x, B/S 7799, PCI, NIST 800 시리즈와 같은 업계 표준을 기반으로 구축되었습니다.

미국의 모든 주는 기업에서 인터넷을 통해 전송하는 개인 정보를 암호화하도록 의무화하는 법률을 제정하고 있습니다. 새로운 법률과 규정에서는 무엇보다도 랩톱, PDA 및 이동식 미디어(플래시 드라이브 포함)의 개인 정보 암호화, 인터넷을 통해 전송되는 개인 정보의 암호화, SSN(사회보장번호) 프라이버시 보호 정책의 개발 및 공표, 그리고 직원 SSN의 기밀성 및 보안성을 보호하기 위한 특정 조치를 요구합니다.

이러한 법률은 데이터 손상 피해를 입은 개인에게 유익합니다. 하지만 보안 침해가 공개될 경우 해당 조직은 부정적인 이슈가 되고 장기적으로 조직의 신용이 떨어질 수 있습니다. 더 나아가 사용자와 고객의 신뢰에 영향을 줄 수 있으며 영업 매출에도 타격을 입을 수 있습니다.

법률과 규정 위반 시에는 벌금뿐만 아니라 사법적 조치를 받을 수도 있습니다. 이러한 움직임에 따라 점점 더 많은 기업들이 암호화 기술이나 기타 액세스 제어 기술을 사용하여 이러한 법률을 준수하려고 노력하고 있습니다.

제도의 한계

많은 규제 법률을 통해서 사용자의 데이터를 보호하려고 노력하고는 있지만 규제만 준수한다고 해서 모든 보안이 이루어지는 것은 아닙니다. 많은 기업들이 보안 준수를 위해 많은 개선을 이루었지만, 보안 준수와 관련된 긴급성 문제 때문에 중요한 보안 위험으로부터 안심할 수 있는 상태는 아닙니다. 대부분 규제 준수와 요구 사항을 충족하기 위한 절차 조정에 집중함으로써 조직은 급변하는 위험/위협 환경을 볼 수 있는 기회를 놓치고 있습니다. 실제 2008년에 발생한 여러 보안 사건에 연루된 기관들은 규정을 잘 "준수"한 것으로

드러났습니다. 이 사례들은 준수 요구사항에서 규정하지 않은 "공격" 행위로 인해 데이터가 손상된 것으로 밝혀졌습니다. 점점 더 보안 위협의 대상이되고 있는 오늘날의 애플리케이션, 기술, 도구 및 관련된 보약 취약점의 문제를 준수 절차만으로 모두 해결할 수는 없습니다. 대신 규정 준수 행위는 사전 정의된 특정 보안 위험만을 완화할 수 있는 한정된 목표만 달성할 수 있도록 지원합니다.

예를 들어 시장 중심의 PCI DSS(Payment Card Industry Data Security Standard)에서는 데이터의 처리, 전송 또는 저장 과정에서 카드 소지자의 데이터 보호에 초점을 맞추고 있습니다. 이 경우 다른 준수 규정과 비교하여 자세한 기준을 제공합니다. 그러나 전체적으로 엄격한 수준의 보안을 요구하지는 않습니다. 이는 엄격한 요구 사항을 중소 규모의 조직에도 적용할 수 있도록 위험 기준 접근방식과 균형을 맞추어야 하기 때문입니다. 업계는 최근 PCI DSS를 버전 1.2로 업데이트하였습니다. 두 가지 버전의 요구사항을 병합하고 유효성 확인 단계를 테스트하는 것 외에도 수정된 기준에서는 WEP(Wired Equivalent Privacy) 교체에 대한 새로운 시한을 제공하고 위험 기반 분석 방법을 채택하여 소규모 업체들이 이 기준을 준수할 수 있도록 도와주고 있습니다.

준수에 대한 최적의 사례와 규정을 올바르게 배열하기 위해 조직은 더 큰 규모의 IT 관리, 위험 관리 및 준수(GRC) 프로그램을 계획할 가능성이 있습니다. 규정 준수를 달성하는 것도 중요하지만 대부분 최적의 사례와 규정들이 특정 정보를 보호하는 데만 적용된다는 사실을 기억해야 합니다. 예를 들면 회사의 금융 정보(Sarbanes-Oxley), 환자의 의료 정보(HIPAA) 및 개인 ID 정보(Basel II 및 영국과 EU의 데이터 법률)를 보호하는 데만 규정이 적용될 수 있습니다. 따라서 규정 준수를 검토하는 것 외에도 조직은 기존 절차를 개선하고 현재와 미래의 위협에 적극적으로 대응하기 위해 포괄적인 Gap 분석을 자주 수행해야 합니다.

재활용 위험

전자 장비를 재활용하는 것도 점점 더 일상화되고 있습니다. 실제 일부 국가에서는 전자 장비를 구입할 때 이미 구매자에게 재활용 비용을 부과하고 있습니다. 전자 장비의 내용년수가 끝나서 재활용센터에 가져올 경우 이 비용의 전부 또는 일부를 환불해주고 있습니다. 이 비용을 환불 받고자 하거나, 규정을 잘 준수하고자 하거나, 또는 환경에 대한 책임감이 높은 기업은 보다 자주 재활용을 이용하려고 할 것입니다. 많은 기업들이 "전자 폐기물"을 재활용하려고 하지만 중요한 데이터를 지우는 데 충분한 주의를 기울이는 기업은 그리 많지 않습니다.

재활용할 장비를 보낼 경우 해당 장비가 어디로 가는지 또는 해당 장비에서 추출할 수 있는 데이터가 누출될 경우 어떤 일이 발생할 수 있는지는 아무도 알지 못합니다. 언론 보도에 의하면 인도네시아나 서아프리카 같이 멀리 떨어진 곳으로 보내진 일부 장비에서 회수된 데이터가 헐값에 팔리고 있다는 보도가 있었습니다.

많은 기업들이 전자 장비 재활용 프로세스를 담당하는 IT 부서를 따로 두고 있지 않고, 대신 시설 관리부 같은 부서에 보내는 것으로 밝혀졌습니다. 그러나 IT 부서 이외의 직원은 하드 드라이브의 중요성이나 재활용 센터에 보내기 전 폐기된 장치에 있을 수 있는 중요한 데이터를 보호하는 방법에 대해 잘 알지 못합니다. 따라서 조직 내에서 이러한 과정을 처리하는 방법이나 담당자에 대해 보안 중심의 명확한 정책을 갖고 있지 않은 조직은 중요한 데이터를 위험에 빠뜨릴 수 있습니다.

ID 도난

2008년에도 ID 도난은 계속 증가했으며 앞으로도 줄어들 기미가 보이지 않습니다. 많은 온라인 범죄자들이 타인의 신뢰를 이끌어내는 사회 공학적 기법을 사용함으로써 범죄의 성공률을 높이고 있고, 주민등록번호와 자동차 면허증 번호, 의무기록 등 중요한 개인 데이터를 수집하고 있습니다.

공개적으로 이용할 수 있는 다양한 소스(사회적 네트워크/직업적 네트워킹 사이트의 사용자 프로필 포함)의 데이터를 모으면 개인, 또는 개인이 알고 있고 신뢰할 수 있는 사람들을 이용해서 개인 ID에 대한 충분한 정보를 쉽게 수집할 수 있습니다.

ID 도난의 피해자가 될 위험이 크게 증가하였습니다. 단 한 번의 보안 침해로 개인 정보가 손상될 수 있습니다. 손상된 웹 사이트를 방문하여 가정용 컴퓨터에 눈에 보이지 않는 키로거 악성 프로그램이 다운로드 되거나 해커가 수천 마일 떨어진 상점의 고객 데이터베이스를 해킹한 경우를 예로 들 수 있습니다.

그리고 현재도 도용된 개인 정보가 전세계 범죄 집단에 무더기로 팔리고 있습니다. 이런 시장을 이용하는 집단은 이익을 위해서 정보를 이용할 뿐만 아니라 테러 관련자에게 정보를 판매하기도 합니다. 이 경우 위조 여권과 여행 서류를 만들거나 테러 집단의 돈세탁에 정보가 이용되기도 합니다.

일반 대중 대상

대상을 명확히 지정한 피싱 건수가 크게 늘어나고 있지만, ID 도용을 시도하는 대부분의 온라인 범죄자는 아직까지 특정 개인이나 그룹을 대상으로 명확히 지정하여 ID 도용을 시도하고 있지는 않습니다. 그저 가능한 한 많은 사람들을 유인하려고 시도하고 있습니다.

인터넷은 대중을 대상으로 ID 도용을 시도할 수 있는 풍부한 기회를 제공합니다. 2008년 2월 FTC의 보고서에 의하면 2007년의 관련 사건의 64% 정도가 이메일과 같은 인터넷을 이용하여 처음 연락을 시도했다고 합니다.

ID 도난 피해자에게 미치는 경제적인 영향은 명확합니다. 그러나 특히 많은 고객의 신뢰도에 손상을 입은 경우 기업은 신뢰 손상과 금전적 손실이라는 두 가지 측면에서 고통을 받습니다. 예를 들어 교묘한 피싱 기법을 사용하여 스팸 이메일이나 합법적으로 보이는 가짜 웹 사이트를 통해 사용자가 자신이 신뢰할 수 있는 소스(예: 개인,

자선기관, 은행, 온라인 쇼핑몰)와 상호 작용하고 있다고 속게 만들 수 있습니다.

오늘날에는 다음과 같은 방법으로 ID 도용을 위해 데이터를 수집하고 있습니다.

- 온라인 커뮤니티—Facebook이나 MySpace 같은 사회적 네트워킹 사이트에 게시된 사용자 프로필에서 전화번호, 주소, 이름, 생일 등의 다양한 개인 정보를 이용할 수 있고, Ancestry.com 같은 사이트에서는 어머니의 결혼 전 성 같은 개인적인 추가 정보를 확인할 수도 있습니다.
- 파일 공유 및 피어-투-피어 소프트웨어—사용자가 친구에게 MP3 같은 특정 파일을 허용 또는 공유할 경우 해당 컴퓨터의 다른 파일에 쉽게 침투할 수 있습니다. 회사 기밀과 동료 정보를 포함한 더 많은 정보를 개인이 볼 수 있도록 허용되는 협업 작업 환경에서는 "액세스의 허점"도 점점 더 커지고 있습니다.
- RFID 태그—자신을 숨길 수 있는 일부 사용자는 짧은 거리에서 RFID(전파 식별) 태그를 읽어서 신용카드나 기타 카드의 데이터를 수집할 수 있습니다. RFID 태그는 복제가 가능하고 필요한 장비도 시판되고 있습니다. RFID 기술에도 명확한 보안 위협 요인이 있습니다. 건물 출입 카드나 여권에 이르기까지 모든 곳에서 RFID 기술을 사용할 수 있습니다.

ID 관리에 대한 재고

데이터 손실과 ID 도난에 대한 우려를 놓고 볼 때 최근 ID 관리에 대한 관심이 부활하는 것은 그다지 놀라운 일이 아닙니다. 많은 유수 기업들이 오랫동안 사용해왔던 보안 플랫폼을 정밀 조사하여 새로운 ID 관리 기술을 채택하고 있습니다. 데이터 손실을 방지하고, 잠재적인 ID 도난 가능성을 줄이고, 내부인이 범죄 행위에 연루된 가능성을 제한하고, 규정을 준수하고자 하는 것이 이들 기업의 목표입니다. 따라서 웹 2.0 도구와 애플리케이션을

사용하여 원격 직원 간의 협업 뿐만 아니라 다른 조직과의 협업을 지원하기 위한 기술이 필요합니다.

오늘날 ID 관리 솔루션은 네트워크나 애플리케이션을 액세스하는 데 필요한 사용자 이름이나 암호를 보호할 수 있도록 발전하고 있습니다. 안전하고 개인화된 사용자 프로필을 만들어 사용할 수 있고, 액세스를 승인하기 전에 사용자는 토큰이나 스마트 카드 같은 하나 이상의 방법을 통해 인증을 받아야 합니다. 지문이나 홍채 인식과 같은 생물학적 측정 방법을 사용하여 사용자를 인증하는 조직도 있습니다.

오늘날 ID 관리의 또 다른 명제는 투명도입니다. 조직은 로그인에서 로그아웃까지 사용자의 활동을 모니터링 할 수 있는 기술을 원합니다. 또한 사용자에게 액세스를 허용할 수 있는 정보의 양과 유형 및 기타 리소스 사용에 대한 경계를 설정할 수 있게 설계된 솔루션을 원합니다. 현재 시판되고 있는 ID 관리 기술을 사용하여 조직은 사용자 활동을 더 쉽게 추적할 수 있을 뿐만 아니라 일관된 사용자 정책을 설정하고, 감사 및 보고를 수행하여 규정 준수를 보장할 수 있습니다.

완벽하고 효율적이지만 쉽게 사용할 수 있는 ID 관리 솔루션에 대한 수요는 풍부합니다. 사용자 ID를 확인할 수 있는 프로세스를 단순화하여 사용자에게 필요한 정보와 애플리케이션에 편리하게 액세스할 수 있게 해주는 "싱글 사인온" 솔루션을 요구하는 기업이 점점 더 많아지고 있기 때문입니다. 최근 들어 ID 관리 기술은 크게 발전하고 있지만 업계는 계속해서 더 높은 보안성과 사용자 모니터링 기능을 제공하고, 직원의 생산성을 저해하지 않는 솔루션을 개발하기 위해 계속 노력하고 있습니다.

인적 요인



보안 연결망에 있어서 가장 취약한 부분은 여전히 사람, 즉 인적 요인입니다. 그러나 정보에 대응하는 자신의 행동을 학습 및 수정할 수 있는 사람의 능력이야말로 인적 요인이 개선할 여지가 많은 영역임을 나타냅니다. 웹 사이트와 회사 네트워크에 대한 공격이 더욱 교묘해지고 온라인 범죄자는 가장 신중한 사용자조차 속이는 데 있어서 점점 더 능숙해지고 있습니다.

인성으로 초래된 위험

평범하고 단순한 휴먼 에러로 인해 종종 악성 프로그램 공격이 시작되거나 ID 도난이나 기타 사기 사건이 발생하기도 합니다. 예를 들면 실제로는 교묘하게 가장된 공격이지만 신뢰할 수 있는 소스에서 보낸 것처럼 보이는 이메일을 CEO가 열어본다든지 유효한 보안 인증서가 없거나 신용사기에 노출된 웹 사이트에서 전자 상거래를 한다든지 하는 경우입니다.

사람의 실수로 인해 신뢰를 손상시킬 수 있는 사건이 발생하거나, 조직에 심각한 금전적 손실을 끼칠 수 있습니다. 예를 들어 고용주가 제공한 랩톱을 분실하거나 실수로 회사의 중요한 정보를 블로그에 게시한 경우입니다. 실수로 인해 보안 문제를 일으키는 또 다른 일반적인 경우는 이메일 주소 오류로 중요한 정보를 잘못된 사람에게 보내는 경우입니다.

심지어 보안에 민감한 미국 육군도 이런 실수로부터 안전하지 않습니다. 2008년 미국 육군(USAF) 직원이 영국 서퍽의 Royal Air Force Base RAF Mildenhall에 주둔하고 있는 육군 직원에게 보내야 할 이메일을 실수로 유사한 이메일 주소를 가진 여행객 웹 사이트로 보내는 사고가 보고되었습니다. Mildenhall 여행을 판촉하는 해당 사이트의 관리자는 미국 육군에 수 차례 해당 메일을 문의했지만 아무런 응답을 받지 못했습니다. 정부 관료들은 대통령 방문에 대한 비행 계획이 수신되었음을 통보 받고서야 크게 놀라는 일이 발생했습니다.

기술적인 솔루션(예: 스팸 방지 도구와 발송 이메일 모니터링 도구)은 이러한 위험을 적극적으로 완화하고

특정 유형의 공격으로 인한 광범위한 손상을 방지하는 데 도움이 될 수 있습니다. 지속적인 보안 교육과 직원 교육을 제공하고 보안 위험과 데이터 보호의 중요성에 대한 인식을 고양함으로써 조직의 중요한 보안 방어 조치를 유지할 수 있습니다. 그러나 거기에도 제한은 있습니다. 이러한 기술 솔루션으로 인해 잘못된 보안 의식이 만들어질 수 있습니다. 기술 솔루션이나 교육으로도 광범위한 보안 문제를 모두 해결할 수는 없는데, 이는 바로 인성, 즉 인적 요인입니다.

기본적으로 대부분의 사람은 호기심이 많고, 통신에 대한 욕구와 좋은 조건의 거래나 공짜 경품에 관심이 많습니다. 특히 사람들은 자신이 사기 사건의 희생자가 될 가능성이 있는 유형은 아니라고 과신하는 경우가 종종 있습니다. 사람 행동 양식의 이런 측면이 온라인 범죄가 이루어지는 주요 요인이 되기도 합니다.

온라인 범죄자는 인터넷 사용자의 신뢰와 인성을 악용하여 보다 더 번창해 지고 있습니다. 수많은 사람들이 URL이 포함된 이메일을 통해 악성 프로그램을 배포하는 웹 사이트나 피싱 웹 사이트로 계속 유인되고 있습니다. 현재 스팸 메시지의 80% 이상에 URL이 포함되어 있다고 가정할 경우 무작정 접근하는 방식이 성공하는 이유를 파악하는 것이 어려울 수 있습니다. 강력하고 스스로 전파할 수 있는 능력을 갖춘 악성 프로그램을 사용할 수 있게 되면서 비교적 적은 수의 감염된 사용자가 더 많은 사용자를 감염시킬 수 있게 되었습니다.

원격 작업, 사회적 네트워킹: 기회 및 위험

모바일 직원제도는 영업 생산성을 크게 향상시키고, 더 나은 삶과 작업이 조화를 이루도록 하므로써 보다 만족도를 높일 수 있습니다. 전세계 직원의 비용 효율성을 높임으로써 다른 지역 고객에게도 현지화된 서비스를 제공하고 신규 시장에 더 빨리 진입할 수 있게 되었습니다. 오늘날 많은 근로자, 특히 젊고 결속력이 강한 "Y 세대" 근로자는 작업과 삶을 더 쉽고 재미있게 해주는 새로운 도구와 기술 사용에 거리낌이 없습니다.

조직은 언제 어디서든 업무를 수행하는 데 필요한 협업 도구와 모바일 장치를 원격 직원에게 구비해주고 있습니다. 그러나, 그 때문에 보안이 위험해지고 있습니다. 예를 들어 Georgia Tech Information Security Center의 “급부상하는 사이버 위협에 관한 보고서(2009)”에서는 원격 근로자에게 반드시 필요한 인터넷 전화와 모바일 컴퓨팅 기술을 통해 더 많은 데이터를 처리할 수 있지만 온라인 범죄의 대상이 될 가능성도 더 높아지고 있다고 경고하고 있습니다. 이 보고서에서는 온라인 범죄자가 VoIP 미디어를 사용하여 음성 사기, 데이터 도난 및 기타 사기 행위에 관여할 것으로 예상하고 있습니다. 이러한 문제는 이메일에서 경험한 문제와 유사합니다.

그러는 사이에 개인과 전문가가 사용하는 기술간의 구별은 점점 더 모호해지고 있습니다. 최근의 시스코 조사에 의하면 직원의 44%가 관리 통제를 받지 않으면서 다른 사람과 작업용 장비를 공유하고 있고, 46%가 재택 근무시 회사 컴퓨터와 개인용 컴퓨터 간에 파일을 전송하고 있는 것으로 나타났습니다

미국 정부 기관에서 제출한 무선 인터넷 사용에 관한 Telework Exchange and Sprint Nextel의 보고서에 의하면 원격 작업자의 33%와 IT 작업자의 11%가 무선 인터넷 사용에 대한 보안 지침에 익숙하지 않은 것으로 밝혀졌습니다.

브라질, 프랑스, 인도 및 미국 등을 포함한 7개국의 원격 작업자의 보안 인식 및 온라인 행동 양식에 관한 시스코의 최근 조사에 의하면 개인적인 용도를 위해 회사 컴퓨터와 장치를 사용하는 것이 오늘날에는 널리 통용되는 사례인 것으로 밝혀졌습니다. 이러한 현상에 대해 조사 응답자들이 답변한 주요 원인은 다음과 같습니다. 고용주가 꺼리지 않을 것이라는 생각을 갖고 있었고 더욱이 많은 사용자가 작업의 효율성을 위해 특정 도구와 애플리케이션을 다운로드 하지만 모르는 사이에 위협에 대한 장입이 이루어져서 결국은 전체적인 생산성을 떨어뜨릴 수 있습니다. 호기심이나 다른 사람과의 소통 욕구 같은 인성 요소로 인해 외부 근무 직원이 작업 중에 온라인 커뮤니티나 전문적인 네트워킹 사이트에 접속함으로써 인해 조직에 위협을 초래할 수 있습니다. 일부 기업은 고유한 마케팅, PR 및 HR 이니셔티브에 대한 수단을 사용하여 이러한 활동을 장려하고 있습니다. 우수한 기업에서도 아주 작은 규모의 블로깅 유틸리티인 Twitter를 사용하여 제품 뉴스를 공유하고 서비스 가입자에게 특별한 혜택을 제공하기도 합니다. 사전적이고 철저한 사용자 교육을 제공하고 근무 중에는 사회적 네트워킹 및 기타 온라인 활동에 대한 명확한 정책을 설정하는 것이 최적의 방안입니다. 그러나 많은 기업들이 적절한 사용 정책을 설정하거나, 사용자 또는 내부 리소스에게 사용 정책을 시행하지는 못하고 있습니다. 미국 정부 기관에서 발표한 무선 인터넷 사용에 관한 Telework Exchange and Sprint Nextel의 보고서에 의하면 원격 작업자의 33%와 IT 작업자의 11%가 무선 인터넷 사용에 대한 보안 지침에 익숙하지 않은 것으로 밝혀졌습니다.

부적절하거나 충분하게 전달되지 않은 사용 정책은 개선되어야 합니다. MySpace, Facebook과 같은 유명한 사이트도, 검색하기 어려운 Koobface 같은 악성 프로그램에 매우 취약하므로 조직은 직원이 근무 중에 사용하는 사회적 네트워킹 사이트들에 대해 더 많은 주의를 기울여야 합니다. Koobface는 감염된 사용자의 컴퓨터를 봇넷 노드로 만듭니다. 웜은 사회적 네트워킹 사이트와 연관된 쿠키를 검색하여, 발견되면 수정한 다음 사용자 프로필에 악성 링크를 포함시킵니다. 프로필을 보는 다른 사람은 링크를 사용자가 포함시킨 것으로 간주합니다. 보고 있는 내용을 신뢰할 경우, 포함되어 있는 해당 링크를 클릭하게 되고 그로 인해 악성 프로그램에 감염됩니다. (작업자에게 매일 쿠키를 삭제하도록 하면 이런 문제를 방지하는 데 도움이 될 수 있습니다.) 반면에 원격 근무자와 현장 근무자가 영업 및 개인 활동을 수행하기 위해 사용하는 랩탑, 휴대폰, PDA 및 데이터 저장 장치는 스팸, 바이러스 및 악성 프로그램에 대한 수많은 진입점을 제공합니다. 또한 지적 재산과 기타 데이터의 수많은 손실 기회를 제공합니다. 작업자는 휴대폰의 보호되지 않는 특성, 즉 공공 장소에서 중요한 작업을 수행할 경우는 프라이버시 화면보호기를 사용해야 할 필요성이라던가 잘못 둘 가능성이 많은 모바일 장비에 특별한 주의를 기울여야 한다는 사실을 충분히 인식하지 못할 수 있습니다. 썸 드라이브에는 최대 64GB 데이터가 저장될 수 있습니다. 영국 국방부는 최근 알 카에다에 대한 기밀 보고서를 포함한 중요한 정보를 가지고 물리적으로 이동 중이던 직원이 기차에 이를 두고 내리는 바람에 분실한 사건을 최근 발표했습니다.

온라인/오프라인 범죄에 사회적 네트워킹 및 웹 2.0 사이트 사용

Facebook, MySpace, Bebo, LinkedIn, Orkut(브라질) 및 vKontakte(러시아)와 같은 사회적 네트워킹 웹 사이트는 모두 스팸 및 악성 프로그램 공격과 연결되어 있습니다. 웹 2.0 위젯과 사용자가 자신의 페이지에 추가할 수 있는 취약성 있는 다른 유형의 콘텐츠 때문에 악성 프로그램 작성자는 앞으로도 이들 웹 사이트를 쉽게 악용할 수 있을 것입니다.

사회적 네트워킹과 웹 2.0 사이트를 범죄에 이용하는 경우가 모두 온라인에서만 발생하는 것은 아닙니다. 캐나다와 미국의 사기 방지 조직은 2008년에 표면화된 다음과 같은 불안한 동향에 대해 보고한 바 있습니다. 노인을 대상으로 한 악취 사기에 사용된 통화 수가 급격히 증가하였는데 이런 사기로 희생자들은 수천 달러의 돈을 범죄자에게 지불하였습니다. 전화를 건 범죄자는 캐나다에서 보석금이 필요한 노인의 10대 또는 대학생별 손자에 대한 꾸며낸 이야기를 들려주었습니다. 아마도 사기에 사용된 개인 정보(예: 희생자의 손자 이름)는 사회적 네트워킹이나 다른 웹 2.0 사이트에 게시된 프로필에서 수집한 것으로 보입니다.

실제 생활에서 "차용"한 요소를 사용한 온라인 범죄자는 온라인 사기 사건을 믿을 수 있게 만들었습니다.

온라인 신용사기꾼들은 "419"(해당 사기 사건을 다루기 시작한 나이지리아 형법전 이름을 딴 것) 또는 선불 사기 사건을

LinkedIn 및 Craigslist 같은 웹 사이트에서 운영하였습니다. Craigslist에서 발생한 일반적인 사기 사건 계약은 다음과 같습니다 범죄자는 합법적이지만 오래된 다른 Craigslist 사용자의 주택 임대 게시물을 이용하여 임차하려는 사람을 속여서 "임대인"에게 현금을 전송하도록 유인했습니다. 임대인이 갑자기 해외로 이사하게 돼서 주택을 즉시 헐값에 임대하고자 한다고 속였습니다.

광고 게시물에 주택 주소가 제공된 경우, 신용사기꾼은 희생자에게 주택을 직접 방문 할 수는 없지만 차를 타고 가면서 볼 수는 있도록 했습니다. 되돌아보면 경고 표시가 많이 있었지만 많은 사람들이 보이는 것을 믿기 때문에 이러한 사기 사건이 성공한 것입니다.

Craigslist가 관련된 또 다른 최근의 사회 공학적 사기 사건에서는 은행 강도가 사기 광고를 통해 탈출을 위한 "구인" 광고를 게시하였습니다. 시간당 28.50달러를 지불하는 도로 유지보수 계획을 광고하는 게시물을 사이트에 게시하였습니다. 의심하지 않고 응모한 수십 명의 희생자는 지역 은행에서 일하기 위해 노란색 조끼, 보호 안경, 마스크, 파란색 셔츠를 착용하고 나오라는 요청을 받았습니다.

희생자들은 지시대로 했지만 현장에 도착해서야 작업도 계약자도 없다는 것을 알았습니다. 동시에 동일한 복장을 착용한 범죄자는 무장 트럭에서 현금 가방을 탈취하여 도망치고 현장에는 비슷한 복장을 한 수십 명의 희생자만 남아 있을 뿐이었습니다.



내부인 위협

웹 기반의 악성 프로그램과 해커 침입 같은 외부 위협요인이 더 많을 수도 있지만 조직은 내부인이 일으키는 심각한 보안 위협을 무시할 수 없습니다. 내부인 위협요인은 조직 외부에서 일으키는 위협요인보다 회사의 신뢰도와 재정애 더 심각한 손해를 끼칠 수 있습니다.

내부인 위협에 대한 걱정을 넘어서서 조직화된 범죄 집단 뿐 만 아니라 경쟁 회사나 적국 정부 같은 대규모 조직은 그들이 대상으로 하는 조직 안에 첩보원을 배치하고 있습니다. 2008년 하반기에 세계 경제는 극심한 변동과 불확실성을 겪고 있고 이 현상은 2009년에도 계속될 것으로 보입니다. 이 때문에 내부인 위협은 모든 유형의 기업에게 보안문제에 있어 주요 관심사가 될 것으로 예상됩니다.

올해에는 내부인 또는 조직의 네트워크에 액세스하기 위해 물리적인 보안을 손상할 수 있는 사람에 의한 사기, 해킹 및 ID 도난 건수가 전세계적으로 증가하였습니다. 심각한 금전적 손해가 발생한 후에야 보고된 아래와 같은 작년의 사건들 이후에 이러한 동향이 강조되었습니다.

- 2008년 1월 프랑스 은행 소시에테 제네랄의 거래원이 승인되지 않은 주식 시장 거래에 개입하여 해당 은행에 49억 파운드의 손실을 입혔습니다. 이 직원은 은행의 위험 관리 부서에서 근무한 경험과 지식을 사용하여 사기 거래로 인한 손실을 숨길 수 있었습니다.
- 5종의 통제 계층에 침입하여 컴퓨터의 액세스 코드를 도용했던 이 거래원의 사기 행위는 은행 회장과 CEO의 과실을 감사하던 감사팀에 의해 발견되었습니다. 이 사기 사건은 거래원 혼자 수행한 것으로 개인적인 이득을 위한 것일 뿐 아니라 조직 내에서 거래 실적을 높이려는 동기가 있었습니다.
- 2008년 5월에는 미국의 유명한 레스토랑 체인점에서 범죄 대상이었던 하드웨어에 직접 액세스할 수 있는 권한이 있는 세 명의 직원이 11개의 현금 등록기를 해킹하여 고객의 신용카드 번호와 직불카드 번호를 도용한 혐의로 기소되었습니다. 패킷 스니퍼(단일 네트워크의 컴퓨터간 통신을 포착하기 위해 설계된 컴퓨터 코드)가 대상 레스토랑의 POS(Point-Of-Sale) 서버에 앞단에 설치되어 있었습니다. 이렇게 해서 2007년 7개월 동안 수천 건의 신용카드와 직불카드 데이터가 수집되었습니다. 한 곳에서만 5000건 이상의 카드가 도용되었고, 그 결과 해당 카드를 발급한 금융 기관에 최소 6십만 달러 이상의 손실이 발생했습니다.

- 2008년 미국 모기지 산업에서는 이보다 더 나쁜 뉴스가 발생했습니다. The Miami Herald가 실시한 플로리다주 모기지 중개인에 대한 범죄 경력 조사에 의하면 허가 받은 수천 명의 중개인이 범죄 기록을 갖고 있었고 해당 사실이 필수적인 범죄 경력 조사 중에도 발견되지 않았다는 것입니다. 2006년 이후 범죄 경력 조사가 필수 조항으로 바뀐 플로리다주에서 감시 기관은 모기지 중개인의 라이선스를 승인해주어야 할 의무가 있습니다. 이 신문의 보고서에 의하면 범죄 기록을 갖고 있는 10,500명 이상의 사람이 모기지 중개인직에서 일할 수 있는 라이선스를 받은 것으로 밝혀졌습니다.
- 조사에 의하면 라이선스가 있는 중개인이 관련된 저축 및 주택 관련 사기, ID 도난 및 도용으로 인한 손실이 약 8백5십만 달러에 달하는 것으로 밝혀졌습니다. 그리고 사기 사건을 저지른 여러 중개인이 감시 기관으로부터 라이선스를 유지할 수 있도록 허가를 받은 것으로 드러났습니다. 인터넷 접속을 통해 모든 사람이 공개 정보와 최신 기술을 이용할 수 있기 때문에 범죄 경력 조사는 잠재적인 보안 문제를 식별할 수 있는 비교적 간단하고 비용이 적게 드는 빠른 통제 수단입니다.
- 2008년 10월 Shell Oil의 현장파견 IT 계약직원이 회사 데이터베이스에서 미국 내 현재 또는 이전 직원에 대한 정보를 도용하려다가 붙잡혔습니다. Shell에 의하면 이 계약직원은 네 명의 사회보장 번호를 사용하여 사기성 해고 소송을 제기했다고 합니다. 위반 사실이 밝혀진 후 Shell은 이 계약업자를 회사에서 해고하였고 연관된 공급업체와의 계약을 파기하고 직원들에게 침해 사실을 경고하였습니다. 텍사스 노동 위원회와 현지 법률 집행 기관은 해당 사건을 조사하고 있습니다.

금융 위기로 내부인 위협이 증가할 수 있음

전세계적인 금융 위기로 인해 가트너의 애널리스트는 대규모 IT 예산 삭감과 고용 동결 및 해고를 예상하고 있습니다. 많은 조직에서 금융 위기 때문에 직원을 해고할 것이고, 간혹 해고에 대한 불만을 가진 사람이 나타날 수

있습니다. 불만을 가진 직원이 온라인 범죄자에게 중요한 데이터나 암호 또는 IT 인프라에 액세스할 수 있는 기회를 제공할 수도 있습니다.

World Bank 예를 들어 보겠습니다. 일부 보고서에 의하면 IT 컨설턴트가 키로깅 소프트웨어로 여러 동료의 컴퓨터를 감염시켜서 일부 서버를 손상시켰습니다. 2008년 10월 중순 World Bank는 중요한 정보가 손상된 사실을 부정했지만, 이 예를 통해서 기관 및 조직의 취약성을 알 수 있습니다.

많은 기업들이 인력을 글로벌화하면서 점점 더 하나의 통합된 세계 경제 속에서 살고 있습니다. 미국 내 은행 및 IT 회사의 직원들이 아시아나 유럽의 콜센터에서 일할 수도 있습니다. 따라서 이제는 시행하고 있는 보안 정책이 현지 문화와도 맥락을 같이 하면서 동시에 다국적 기업의 글로벌 보안 정책과도 상응 수 있도록 해야 합니다. 이 경우 비용 효율적이지만 조직의 네트워크에서 안전하게 작업하려면 추가 보안 정책과 구현이 필요합니다.

신뢰성 문제



많은 사용자는 거래 및 관련 데이터가 대부분 물리적으로 분리된 영역 안에 존재했던 과거와 비슷한 수준의 데이터 보안을 누리고 있는 것으로 믿고 있습니다. 사용자들은 기관들이 자신의 개인 정보를 안전하게 보호하기 위해 가능한 모든 수단을 동원할 것으로 믿고 기꺼이 자신의 개인 정보를 조직에 제공합니다. 그리고 자신이 알고 있는 공급업체의 장비와 서비스를 믿고 신뢰합니다.

예를 들어 커피숍의 보안되지 않은 Wi-Fi 네트워크(ID 도용자가 쉽게 포착할 수 있음)를 이용하거나 구식의 데이터 저장 방법(해커가 쉽게 침입할 수 있음)을 사용하는 전국적인 규모의 소매업자를 통해 제품구입을 함으로써 사용자는 이전보다 더 많은 방법을 통해 정보를 노출 당할 수 있는 위험에 놓여 있습니다.

조직은 자신의 보안 문제에 대해 무감각 할 수도 있습니다. 조직은 기존 프로토콜, 서비스 및 구성요소를 너무 신뢰하거나, 인증서, 모니터링 및 테스트 같은 사용 가능한 방법을 통해 신뢰 관계의 유효성을 확인하거나 모니터링 하는데 있어 충분한 노력을 하지 않을 수도 있습니다. 반면 특정 규정과 업계 표준을 준수하는 일부 기업은 이러한 기준을 준수함으로써 적절한 보안을 유지할 수 있다고 믿고 있습니다.

지난 10년 동안 네트워크 운영 시스템에 대한 위협은 크게 증가하였고 취약한 네트워크 악용과 관련된 범죄 행위가 눈에 띄게 증가하였습니다. 중요한 인프라를 구성하는 네트워킹과 IT 시스템을 강화하기 위해 많은 조직이 업그레이드를 보안 전략의 일부로 시행하고 있습니다. 실제로 일부 기업은 최소한 업그레이드를 매년 수행하거나 1년에 두 번 정도 수행하고 있습니다.

조직의 지속적인 또 다른 위험은 사람입니다. 예를 들어 직원이 장비를 분실할 수 있고 이로 인해 중요한 데이터가 손실될 수 있습니다. 사기 행위를 도모하는 내부인은 오늘날 더 많은 동기를 갖고 있습니다. 데이터 밀도가 증가함으로써 조직 내에서의 공격이 더 많은 수익을 제공할 수 있습니다. 중요한 데이터를 도용 또는 수집하기 위한 장치를 배치하거나 직원이 합법적인 액세스 권한을 갖고 있는 데이터를 복사하는 것은 2008년 발생했던 여러가지 세간의 이목을 끌던 보안 사건들에서 공통적으로 알려진 방법입니다.

심지어 하드웨어로 인해 공격이 제기될 수도 있습니다. 컴퓨터 장비에 삽입한 위조 칩은 개인 사용자, 기업 및 정부의 중요한 데이터를 위험에 빠뜨릴 수 있습니다. 추리 소설의 소재처럼 들릴 수 있지만 글로벌 공급망에 위조 구성 부품을 삽입할 기회를 엿보고 있는 범죄자(심지어 외국 정부)에 관한 보고서도 있습니다.

일부 전문가는 보안 위험이 과장되었다고 말하지만, 위조 구성 부품의 삽입은 외부인이 사용자의 개인 정보를 액세스하거나 통신을 모니터링 할 수 있게 해주는 "뒷문"을 제공합니다. 그리고 이러한 문제를 검색하는 것은 매우 어렵고 해결하는 데 드는 비용도 만만치 않습니다. 소프트웨어는 패치할 수 있지만 위조 구성 부품은 한 번에 하나의 컴퓨터에서만 제거해야 되므로 상당히 어려운 문제입니다.

알려진 취약점을 무시하는 것이 조직의 또 다른 문제입니다. 기존 문제를 해결하거나 패치하지 않을 경우 조직은 새로운 위협과 싸울 적절한 준비를 할 수 없습니다.

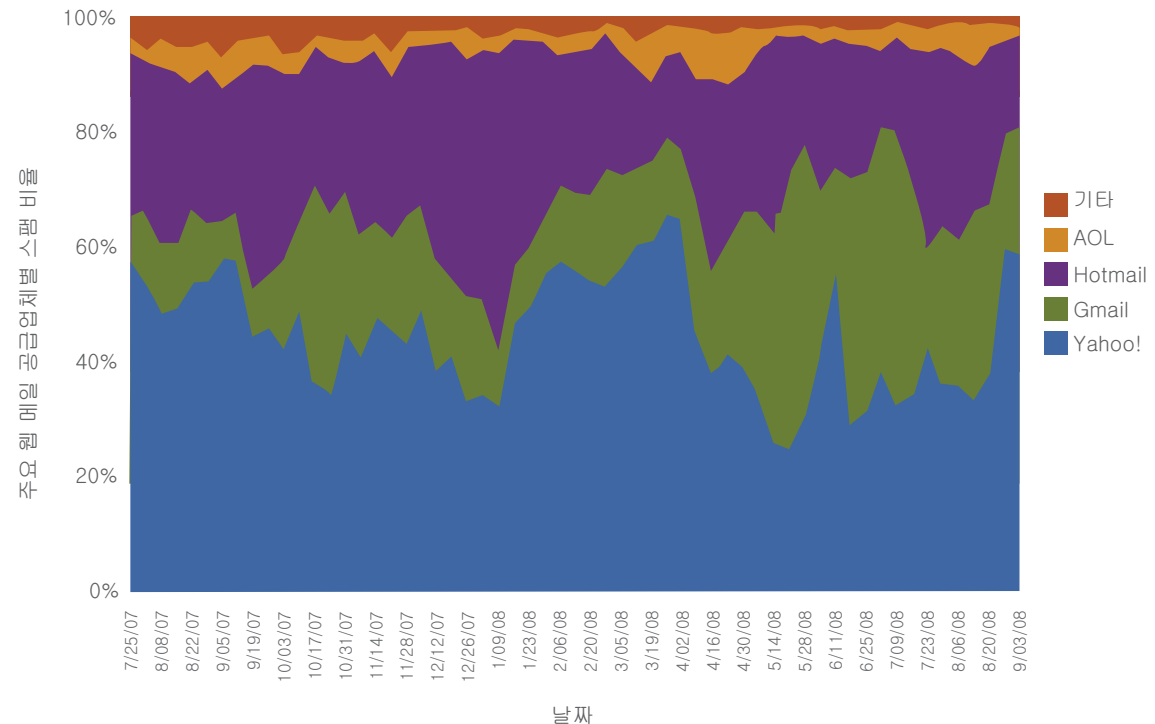
알려진 취약점을 무시하는 것이 조직의 또 다른 문제입니다. 2008년의 새로운 위협 방식 중 대부분이 이전 문제(패치되지 않은 시스템, 취약한 보안 정책, 웹 코어 인프라의 알려진 취약점 등)를 악용한 사례였다는 것은 시사하는 바가 많습니다. 기존 문제를 해결하거나 패치하지 않는다면 새로운 위협과 싸울 수 있는 준비도 제대로 할 수 없습니다.

새로운 방법에 의한 신뢰 손상

온라인 범죄자는 사용자의 신뢰를 이용하기 위해 언제나 우호적인 전술을 도모합니다. 따라서 신용 하이재킹 기법도 날이 갈수록 다양해 지고 있습니다. 2008년 잘 알려진 유수 기업들이 이러한 공격으로 신용도에 타격을 받았습니다. 범죄자들은 다음과 같은 방법으로 하이재킹을 시도했습니다.

- 진짜 회사처럼 보이게 하거나 헤더 정보를 도용하여 실제 회사에서 보낸 것처럼 믿을 수 있게 스팸을 만듭니다. 받는 사람은 합법적으로 보이지만 위장된 웹 사이트로 연결됩니다.
- 신뢰할 수 있는 평판을 가진 유명한 웹 메일 공급업체가 자사의 웹 메일 계정의 대량 작성을 방지하기 위해 설계된 보안 조치들을 무력화 시킵니다. 범죄자가 대량의 웹 메일 계정을 만들 수 있는 기능을 확보하게 되면 이를 사용하여 대량의 스팸 계정을 발송합니다. 이 경우 웹 메일 보낸 사람의 주소는 합법적이고 유효하기 때문에 스팸 방지 필터링 시스템을 통과할 확률이 높습니다.
- 로컬 인터넷 공급업체의 DNS 캐시가 포이즌 공격을 받으면 합법적인 URL을 입력해도 사용자가 중요한 개인 정보와 금융 정보를 제공하게 되는 악성 사이트로 연결될 수 있습니다.
- SQL 주입, 사이트간 스크립팅 및 기타 방법을 통해 수천 개의 합법적인 웹 사이트(대형 쇼핑몰이나 뉴스 방송 기관의 웹 사이트 포함)에 악성 프로그램을 다운로드하는 iFrame을 삽입합니다. 최근 시스코 연구에 의하면 모든 합법적인 사이트의 20% 정도가 이런 유형의 공격에 감염된 적이 있는 것으로 드러났습니다.

주요 웹 메일 공급업체별 스팸 비율



웹 메일 공급자의 시스템을 악용할 수 있는 도구가 상업적으로 시판된 후에 각 웹 메일 공급자의 평균 스팸 비율이 크게 증가하였습니다.

프라이버시 및 신뢰 침해

이제 소비자들도 자신이 신뢰하는 기관에서 자신의 프라이버시를 완벽하게 보호해줄 수 없다는 것을 알게 되었습니다. 광고 및 마케팅을 위해 많은 기업과 조직에서 소비자의 정보를 제3자와 무료로 공유하고 있습니다. 때로는 이러한 사실을 소비자에게 공개하지 않거나, 혹은 명확하게 공개하지 않습니다. 또한 사용자가 "동의"를 클릭하기 전에 정책을 충분히 읽어보지 못할 수도 있습니다.

때로는 조직 내의 모든 직원들이 개인정보 보호정책을 충분히 숙지하지 못하거나, 중요한 정보를 가진 신뢰할 수 있는 제3의 공급업체가 보안 정책을 제대로 알지 못하거나 따르지 않을 경우, 소비자 데이터가 위험에 처하게 되는 경우도 있습니다.

소비자 데이터 사용에 관한 엄격한 정책을 설정하는 IT 및 개인정보 보호 부서에서 다른 부서가 이러한 지침을 위반하고 있다는 사실을 알지 못하는 경우도 있습니다. 2008년 Ponemon Institute의 임원 보고서에 의하면 조직에서 수집한 소비자 데이터를 보호할 책임이 있는 보안 및 프라이버시 담당 임원이 동일한 데이터(이메일 주소 포함)를 외부 당사자와 공유하는 마케팅 부서와 함께 하는 것으로 드러났습니다.

예를 들어 대학교에서는 재학생 및 졸업생과 관련된 대량의 개인 신상 정보 및 금융 정보를 수집하여 관리하고 있습니다. 작년에 많은 대학들이 은행 및 신용카드 공급업체 등을 포함한 학생 개인 정보를 외부 회사와 공유하고 있는 것이 밝혀졌습니다. 이는 개인정보 보호 정책 및 법률에 명확히 위반되는 사례입니다.

플로리다 주립 대학은 최근 재학생 및 졸업생의 이름과 주소를 신용카드 판촉을 목적으로 BOA(Bank of America)에 제공한 것으로 밝혀졌습니다. 계약서 사본을

입수한 Consumer Warning Network에 의하면 거래의 일부로 이 대학교는 재학생과 졸업생의 신용카드 요금 중 일부를 받기로 한 것으로 밝혀졌습니다. 플로리다 주립 대학교는 몇 년간 1천만 달러 이상을 받도록 보장되어 있었고 이 금액은 대학의 육상 프로그램 지원 기금(감독 월급 포함)을 마련하기 위한 사적 단체인 Seminole Boosters에게 직접 지불되어 왔습니다.

아이러니한 이야기이지만 BOA와 이런 거래를 하는 동안 플로리다 주립 대학교는 재학생에게 신용카드 채무에 대한 위험을 경고하는 미디어 캠페인을 동시에 진행하기도 했습니다.



취약점



모든 기술에는 취약점이 존재합니다. 범죄자는 이런 취약점을 이용하여 컴퓨터와 장치에 악성 프로그램을 설치하고, 사용자의 컴퓨터와 네트워크를 통제하며, 컴퓨터와 네트워크를 봇넷으로 만들거나 그 안에 저장된 중요한 정보를 도용합니다.

범죄자들이 이런 시스템을 통제할 수 있는 위험을 낮추기 위해 IT 전문가와 개인 사용자들은 그들이 사용 중인 제품 및 시스템에 대한 패치, 수정 프로그램 및 업그레이드를 구하려고 노력합니다. 이는 마치 악용할 수 있는 새로운 취약점을 찾으려는 범죄자와 가능한 한 시스템을 안전하게 패치 하려는 사용자 간의 일종의 게임처럼 보일 수 있습니다.

그러나 패치를 찾아서 설치하고 업그레이드하는 번거로운 일을 수행하는 것이 사용자에게 때로 성가신 일이 될 수도 있습니다. 그리고 시스템과 제품을 패치하거나 업그레이드하는 데 있어 시기적으로 뒤쳐질 수도 있습니다. 오랫동안 패치하지 않을 경우 취약점은 시스템에 손쉽게 침투할 수 있는 기회를 제공하므로 범죄자에게는 좋은 기회가 될 수 있습니다.

자주 악용되었던 이런 유형의 취약점은 시간이 지남에 따라 바뀌었습니다. 공급업체들이 시스템용 패치를 공개 및 발표하기 위해 시스템을 개발해왔기 때문에 특정 취약점은 패치하기가 더 쉬워졌고 때로는 자동으로 패치되기도 합니다.

실제로 시스코는 2008년에 보고된 취약점 수가 2007년과 비교하여 11.5% 증가한 것으로 확인했습니다. 이는 이전 년도의 동향이 계속된 것으로 공급업체들이 적극적으로 자사 제품의 취약점을 확인, 식별 및 수정해 온 것을 나타냅니다. 그들은 보안 연구업체와 더 자주 협력하여 패치와 업그레이드를 수행하기도 합니다.

2008년 7월 IBM Internet Security Systems X-Force Trend Statistics 보고서에 의하면 보안 연구 기관에서 심각한 취약점의 거의 80%를 찾아낸 것으로 밝혀졌습니다. 이 정보는 시스코 정보와 관련이 있는 것으로 심각한 취약점 공개의 80% 가량이 해당 제품의 공급업체와의 협력을 통해 밝혀진 것으로 공급업체는 공개 시점에 패치와 업데이트를 함께 발표할 수 있었습니다.

그 결과 공개된 취약점의 전체 수는 증가하지만 주요 운영 체제 같은 제품의 "제로데이" 취약점(악성 코드가 출현했을 때 대응 가능한 패치가 존재하지 않는 취약점) 수는 감소하는 것으로 나타났습니다.

취약점에 있어서 또 다른 동향은 많은 공격에서 서로 다른 취약점을 대상으로 하는 여러 악용 기술을 조합하여 사용함으로써 시스템에 대한 액세스와 제어에 대한 성공률을 높일 수 있다는 것입니다. 대상 시스템에서 실행 중인 운영 체제와 프로그램에 따라 취약점 상호간 공격을 다양하게 조합하여 사용할 수 있습니다.

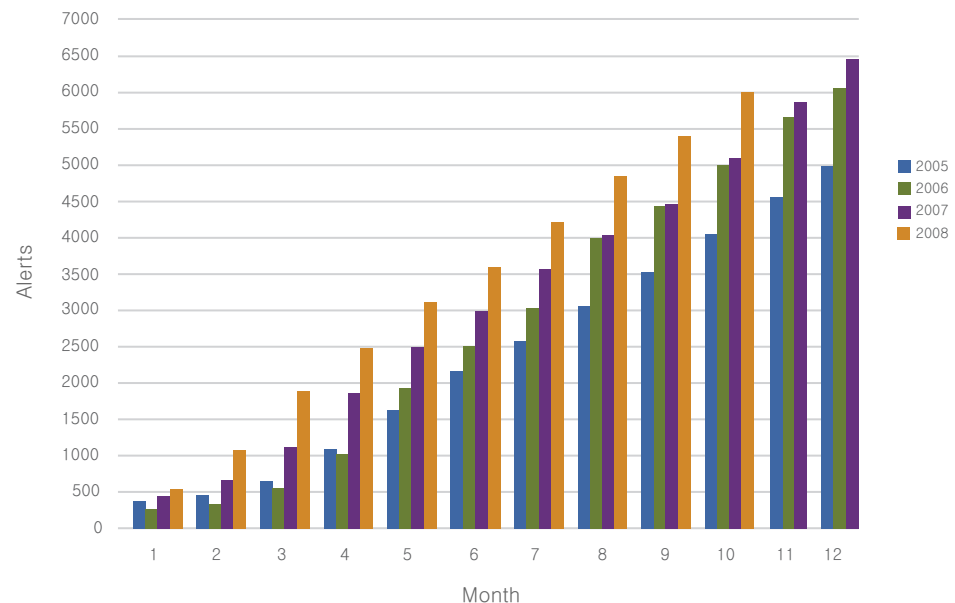
웹 취약점

많은 사람들이 다양한 목적을 위해 테스트되지 않은 새로운 방식으로 웹을 사용함으로써 전체 웹 환경(브라우저, 브라우저에서 실행 중인 웹 애플리케이션, 서버 및 웹의 일부 기본 인프라 포함)의 취약점이 계속 증가하고 있습니다.

이렇게 새로운 사용 방식만으로 새로운 취약점이 만들어지는 것은 아닙니다. 웹 기반 도구 및 기술의 알려진 많은 취약점은 계속 온라인 범죄자에 의해 이용되고 있습니다. 취약점이 있는 것으로 알려진 일부 하이 프로필 웹 기반 기술은 다음과 같습니다.

Adobe Flash Player. 사용자가 웹 사이트나 이메일의 악성 Flash 파일을 클릭하거나 확인하면 임의의 코드가 실행될 수 있습니다.

연간 경고 누적 합계



2008년에 보고된 취약점 수는 2007년과 비교하여 11.5% 증가하였습니다.

"시스템의 복잡도가 높아지면서
취약점의 종류도 서로
복합적으로 결합하기
시작했습니다. 개별 취약점만
놓고 보면 비교적 위험하지 않을
수도 있지만 다른 위협과 결합될
경우 심각한 위험 요인이 될 수도
있습니다."

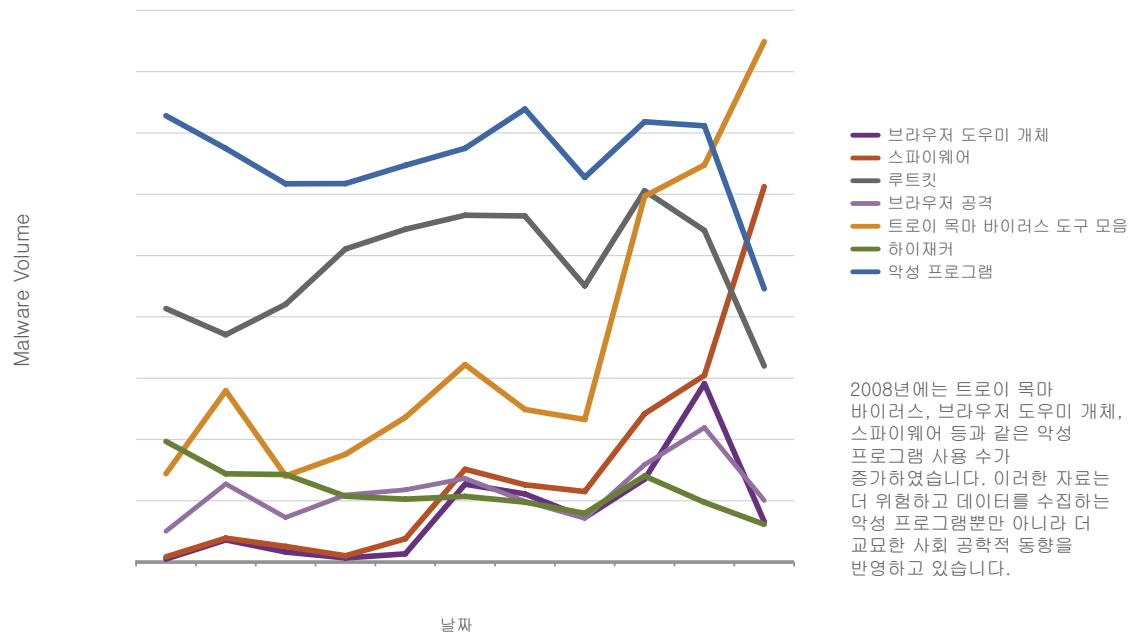
— Greg Spillman, 시스코 보안 분석가

사용자가 관리 계정을 사용하여 컴퓨터에 로그인할 경우 공격자는 시스템 전체를 손상시킬 수 있는 코드를 실행할 수 있습니다. 이러한 취약점을 이용한 폭넓은 공격이 2008년 4월과 5월에 발생했습니다. 이에 대응하여 Adobe는 업데이트된 Flash Player 소프트웨어를 출시했고 많은 공급업체가 자신의 보안 설정과 도구를 업데이트하여 공격을 중단시켰습니다.

WordPress: 2007년 3월 온라인 범죄자가 최신 공식 버전의 소프트웨어를 호스팅하는 서버에 사용자 수준의 액세스를 획득하여 악성 코드를 삽입함으로써 널리 사용되던 블로그 생성 소프트웨어의 모든 버전이 손상되었습니다. 그 기간 동안 해당 버전을 다운로드하여 설치한 사람의 블로그는 온라인 범죄자의 원격 PHP 실행에 취약하게 되었습니다. 이에 대응하여 WordPress는 새로운 버전을 발표하고 서버를 강화하였습니다.

Media players: 인터넷에서 다운로드하거나 웹 페이지에 포함되어 있는 멀티미디어 콘텐츠를 재생하는 데 널리 사용되고 있는 미디어 플레이어도 공격에 취약한 것으로 증명되었습니다. RealPlayer, Windows Media Player, Adobe Flash Player 및 QuickTime이 취약한 플레이어로 나타났습니다. 사용자는 다른 종류의 콘텐츠를 재생하거나 보안을 위해서 미디어 플레이어를 업그레이드해야 한다는 메시지를 받게 되어 있으므로, 온라인 범죄자에게 있어서 미디어 플레이어는 공격하기 좋은 대상이 될 수 있습니다. 이런 메시지가 합법적인 메시지일 경우도 있지만 번거로워 보여서 무시할 경우 플레이어가 취약해질 수 있고, 이런 메시지가 미디어 플레이어를 악용하여 사용자 컴퓨터에 악성 프로그램을 설치하기 위한 것일 수도 있습니다.

검색된 다른 유형의 악성 프로그램(월별)



공격에 취약한 것으로 입증된 잘 알려진 웹 기반 기술 외에도 블로그 및 사회 공학적 네트워킹에 사용되는 위젯이나 애드온 같은 새로운 웹 2.0 기술도 공격에 취약할 수 있습니다.

이러한 애드온 프로그램의 의도가 모두 좋은 것은 아니라는 위험도 있습니다. 개발자들은 이미 악성 프로그램 배포, 관리 및 지원 패키지를 만들고 있습니다. 온라인 커뮤니티의 가치를 잘 알고 있는 많은 온라인 범죄자들이 계속 사회 공학적 네트워킹을 폭넓게 이용하고 있습니다. 따라서 일부 개발자들이 사회적 네트워킹 사이트를 공격하기 위해 사용자에게 초점을 맞춘 매력적인 "악성 위젯"을 만드는 데 심혈을 기울이는 것은 어쩌면 당연해 보입니다.

ActiveX 취약점

널리 사용되는 Internet Explorer 웹 브라우저를 포함하여 많은 Microsoft 애플리케이션과 Windows 애플리케이션을 강화하는 ActiveX 컨트롤의 취약점은 그 숫자가 계속 증가하고 있습니다. 이런 취약점을 악용한 사례에는 일반적으로 사용자에게 악성 웹 사이트를 방문하도록 속여서 취약한 ActiveX 컨트롤을 호출하는 방식이 있습니다.

2008년 공격자들은 Microsoft Snapshot Viewer, RealNetworks RealPlayer, Microsoft Help Visuals 및 Computer Associates BrightStor ARCserve Backup ActiveX 컨트롤의 취약점을 악용하여 세간의 이목을 끄는 공격을 수행하였습니다. ActiveX 취약점을 사용하여 이전 버전의 Windows용 RealNetworks RealPlayer를 사용하는 사용자를 대상으로 악성 프로그램을 전파하기도 했습니다. 이전 버전의 ActiveX 컨트롤을 설치한 사용자에게는 공격이 확실히 성공하였습니다. 공급업체가 이런 취약점을 해결하기 위해 업데이트를 발표했더라도 대부분의 경우 많은 사용자들이 소프트웨어를 업데이트하지 않았기 때문입니다.

DNS 취약점

2008년의 대규모 온라인 보안 사건은 여름 끝 무렵에 뉴스에서 많이 다루었던 웹 환경의 취약점이었습니다. 웹 인프라 중 핵심 부분인 DNS(Domain Name System) 프로토콜의 취약점과 관련된 사건이었습니다.

DNS 프로토콜의 기능은 "cisco.com" 같은 URL 및 호스트 이름을 숫자 IP 주소로 변환하거나 IP 주소를 URL로 변환하는 것입니다. DNS 프로토콜을 사용하여 사용자는 "http://198.133.219.25" 대신 "http://www.cisco.com"을 입력하여 웹 사이트를 찾을 수 있습니다. 이 경우 호스팅하는 서버가 서로 물리적으로 가까이 있지 않더라도 도메인 및 관련된 하위 도메인을 서로 쉽게 연결할 수 있습니다.

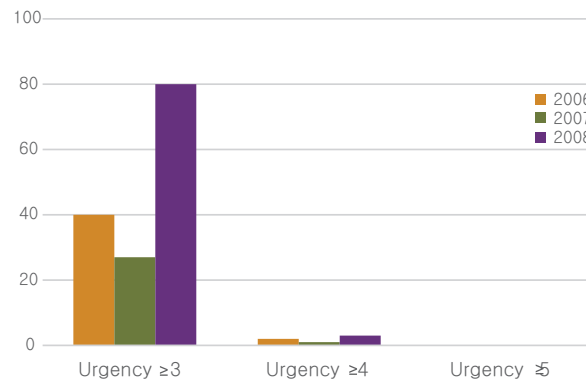
DNS 서버에는 도메인 이름이 어떤 IP 주소로 연결되는지에 대한 레코드가 보관되어 있습니다. DNS 서버가 IP 주소로 된 도메인 이름을 확인해달라는 요청을 DNS 클라이언트로부터 받은 경우, 관리하는 글로벌 DNS 데이터베이스 부분을 조사하거나 해당 쿼리를 글로벌

DNS 데이터베이스의 다른 부분을 관리하는 다른 DNS 서버로 넘길 수 있습니다. 응답 시간을 단축하기 위해 DNS 서버는 다른 DNS 서버로부터 받은 응답을 일정 기간 동안 로컬 캐시에 로컬로 저장합니다.

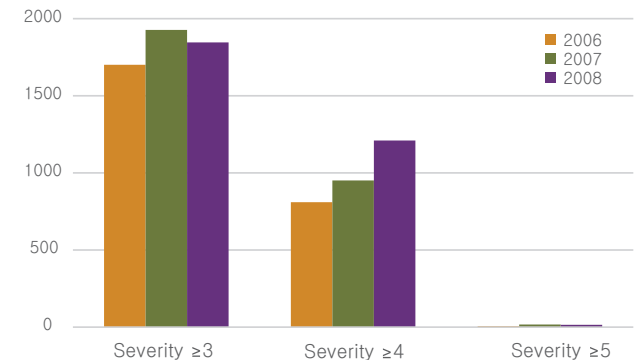
IP 주소 블랙리스트로 인한 차단을 피하기 위해 봇넷 운영자 및 다른 온라인 범죄자는 DNS 서버에 도메인 이름 레코드와 연관된 IP 주소를 변경하는 빈도에 대한 제한이 없다는 점을 자주 악용합니다. 몇 분마다 악성 사이트 운영자는 하나의 봇넷 노드에서 다른 봇넷 노드로 악성 사이트를 호스팅하라는 작업을 전송합니다. 이런 사례를 "패스트 플렉스" 또는 도메인 이름 키핑이라고 합니다.

더 나쁜 것은 DNS 프로토콜 자체에 DNS의 레코드 변경에 대한 제한 부족의 취약점뿐만 아니라 "캐시 포이즌 공격" 영역에서 악용 가능한 취약점을 갖고 있는 것으로 밝혀졌습니다.

연간 긴급성 평가(점수)



연간 심각성 평가(점수)



다음 그래프는 취약점과 위협의 긴급성(활동) 및 심각도(영향)가 모두 계속 증가하고 있는 양상을 보여 줍니다.

DNS 캐시 포이즌을 사용한 최근 공격

China Netcom: 중국의 대형 ISP 중 하나인 China Netcom 이 DNS 캐시 포이즌 공격의 희생자가 되었다는 보고가 있습니다. DNS 캐시를 포이즌 공격한 온라인 범죄자는 눈에 띄지 않게 합법적인 웹 사이트를 방문하려고 하는 사용자가 URL을 잘못 입력하는 경우 악성 웹 사이트로 리디렉션되도록 합니다. 이 경우 희생자 수는 제한되지만 공격이 불의에 일어나므로 검색이 더 느려질 수 있습니다.

AT&T Internet Services: 텍사스주 오스틴 지역에서 AT&T Internet Services(이전 SBC)의 고객이 보낸 DNS 쿼리를 확인하는 DNS 서버가 공격을 받았습니다. Google.com을 방문하려는 AT&T Internet Services 고객이 가짜 버전의 Google 페이지를 표시하는 악성 페이지로 리디렉션되어 삽입된 iFrame 공격을 받았습니다.



DNS의 중요성

인터넷이 사용되는 거의 모든 서비스, 즉, 웹뿐만 아니라 이메일, FTP, VoIP, 은행 거래 등의 광범위한 영역에서 DNS를 사용하고 있습니다. DNS는 인터넷의 마스터 지도 역할을 하고 있습니다. 사용자는 이 지도가 올바르다고 가정합니다. 그러나 범죄자들이 이 지도의 사본을 수정할 수 있는 경우 해당 지도 사본(DNS 캐시)을 다른 사람에게 보내서 예기치 않은 목적지로 보낼 수 있습니다. 물론 그러한 중에도 사용자에게 지도를 따라가면 원하는 목적지에 도달할 수 있다고 계속 표시할 것입니다.

DNS는 지도상의 서로 다른 부분은 각기 다른 DNS 서버가 과장하는 분산 구조로 되어 있기 때문에 특히 더 심각한 문제가 발생 할 수 있습니다. 자신이 맡은 지도의 영역은 정기적으로 업데이트하지만 업데이트 사이에는 저장된 버전의 지도(DNS 캐시)를 사용하여 시스템을 쿼리한 사용자를 목적지로 보내고 저장된 버전의 지도 부분을 다른 DNS 서버에 제공하여 근처로 안내합니다.

시스템이 이처럼 설정된 경우 한 군데만 취약하더라도(하나의 DNS 서버만 공격을 받아 손상되더라도) 공격자는 캐시를 포이즌 공격하여 해당 DNS 서버를 쿼리한 모든 사용자를 잘못된 위치로 보낼 수 있습니다. 이러한 DNS 서버 중 일부(예를 들어 인터넷 서비스 공급자의 DNS 서버)는 수백만 명의 사용자를 잘못 안내할 수 있습니다.

DNS 캐시 포이즌 공격

DNS 캐시 포이즌 공격을 통해 온라인 범죄자는 합법적인 도메인 이름을 해당 도메인 이름이 연결되어 있는 올바른 IP 주소로 리디렉션하지 않고 자신이 선택한 IP 주소로 리디렉션시킬 수 있습니다. 이는 웹 사용자가 이동하는 위치를 제어할 수 있고, 심지어 사용자가 악성 사이트를 클릭하지 않고 합법적인 웹 사이트 URL을 신중하게 입력한 경우에도 악성 웹 사이트로 보낼 수 있음을 의미합니다.

이 경우 캐시 포이즌 공격은 악성 프로그램을 호스팅하거나 피싱 사이트를 만드는 데 유용합니다. 대부분의 "정상적인" 피싱 웹 사이트는 합법적인 URL을 사용하지 않고 실제 URL과 매우 유사한 URL을 사용합니다.

예를 들어 도메인 이름의 "l"가 "1"로 바뀔 경우 방문객은 자신이 Mylegitimatebanksite.com을 실제로 방문하는 게 아니라 대신 My1egitimatebanksite.com을 방문하고 있는데 이를 방문자가 알기 어렵습니다.

방문객을 이런 위조 사이트로 데려오려면 일종의 사회 공학적 기술을 사용해야 합니다. 그러나 범죄자가 DNS 캐시를 포이즌 공격할 경우 이런 속임수를 사용하거나 스팸 링크를 합법적이지 않은 URL로 연결할 필요가 없습니다. 대신 DNS 서버에 저장된 캐시된 DNS 레코드를 사용하여, 주소를 올바르게 입력하거나 합법적인 URL을 클릭한 웹 사용자가 리디렉션되는 위치를 제어합니다. 기본적으로 이메일이나 다른 사이트에서 해당 링크를 클릭한 일부 사용자가 아니라 해당 URL을 입력한 모든 웹 사용자가 하이jack됩니다. 따라서 사용자들은 자신이 입력한 합법적인 웹 사이트가 아니라 악성 사이트로 리디렉션됩니다.

예를 들어 합법적인 URL인 Mylegitimatebanksite.com을 입력해도 합법적인 사이트로 연결되지 않고 대신 사용자 컴퓨터에 악성 프로그램을 다운로드하거나 은행의 웹 사이트와 유사해 보이지만 방문객이 입력한 정보나 암호를 공장 온라인 범죄자에게 전송하는 사이트로 사용자를 보낼 수 있습니다.

2008년 중반에는 DNS 캐시를 더 쉽게 포이즌 공격할 수 있게 해주는, 많은 공급업체의 DNS 서버 소프트웨어의 취약점을 악용한 사례에 대한 신문 기사가 발표되었습니다. DNS 캐시 포이즌 공격이 새로운 공격은 아니지만 보안 연구원인 Dan Kaminsky는 이 방법이 더 강력하고 효율적인 공격 수단이 될 수 있을 거라고 확인해주었습니다.

DNS 최적 사례, 네트워크 보호 및 공격 식별에 대한 자세한 내용을 보려면

www.cisco.com/web/about/security/intelligence/dns-bcp.html을 방문하십시오.

TCP 스택 테이블 구현 취약점

최근 한 보안 연구원이 Sockstress라고 하는 공격 프레임워크를 이용하여 많은 제품의 TCP 스택 테이블 구현의 알려지거나 알려지지 않은 취약점을 악용할 수 있다는 사실을 발표했습니다. 자세한 연구 결과가 아직 발표되지는 않았지만, 초기 연구 결과를 통해 감염대상 제품에는 대부분의 운영 체제, 라우터, IPS(침입 방지 시스템) 및 방화벽 장치가 포함될 수 있다고 암시하고 있습니다. 왜냐하면 이들 모두가 감염될 수 있는 스택과 TCP 트래픽을 처리하기 때문입니다.

이 연구원은 공급업체 및 기업과 협력하여 감염된 TCP 스택의 수정 프로그램을 만드는 작업을 지원하고 있는 걸로 알려져 있습니다. 수정 프로그램을 개발하는 데 필요한 시간에 따라 2009년까지 전체 정보가 발표되지 않을 수도 있습니다. 2009년에는 이러한 취약점이 또 다른 주목을 받게 될 것이 확실합니다.

네트워킹 장비 취약점

많은 IT 부서들이 데스크톱 시스템, 애플리케이션 및 데이터 센터 장비를 패치 및 업그레이드하는 데 많은 노력을 기울이고 있지만, 네트워크 장비를 업그레이드하는 것은 때로 짧은 고해의 시간이 될 수도 있습니다. 네트워크가 제대로 작동하고 있는 경우 해당 네트워크를 가동 중단하는 것은 별로 좋은 생각이 아닌 것 같고 더불어 네트워킹 장비를 업그레이드하는 것이 복잡할 수 있기 때문입니다.

그러나 네트워크 장비를 정기적으로 업그레이드하지 않을 경우 위험에 노출될 수 있습니다. 시스코 제품을 포함한 네트워크 장비와 운영 체제의 취약점에 대한 연구가 2008년에는 증가하였습니다. 공격이 거세질 경우 회사 네트워킹 장비에 미치는 공격의 영향은 심각할 수 있습니다. 예기치 않게 가동이 중단될 경우 심각한 영향을 미칠 수 있습니다. 또는 최악의 경우 교묘한 공격자가 네트워크가 원활하게 가동되도록 한 상태에서 네트워크에 있는 중요한 데이터를 공격하거나 액세스할 수도 있습니다.

가상화 취약점

기업 환경에는 가상화 기술이 광범위하게 포함되어 있습니다. 가상 또는 원격 작업자, 가상 데이터 센터 또는 네트워크 가상화든 모두 비용 효율성과 유연성 면에서 이점을 제공합니다. 데이터 센터와 네트워크 가상화뿐만 아니라 "가상 클라이언트" 제품은 관리 및 보안의 용이성을 개선합니다.

그러나 이러한 가상화 제품 중 일부는 비교적 아직 미숙한 상태이고 실제 환경에서 엄격한 보안 테스트를 거치지 않은 경우도 많습니다. 이 때문에 2008년 1월에서 11월 사이에 가상 소프트웨어 제품에서 103건의 취약점이 노출되었습니다. 이 기간 동안 주요 가상화 공급업체 중 하나인 VMWare는 2007년의 7건에 비하여, 2008년 해당 제품에 대해 18건의 보안 취약점을 공지 하였습니다.

“가상화 기술을 더 많이 사용할수록 새로운 위험을 함께 가져올 수 있습니다.”

— Don Simard, Commercial Solutions Director,
미국 국가안전보장국 – InfoWorld, 2008년 3월 13
일자

“위협이 복잡해질수록 기본적인 작업을 철저히 수행해야 합니다. 항상 새로운 취약점을 파악하고 패치와 소프트웨어 업데이트를 신속하게 구현하는 것이 무엇보다도 중요합니다.”

—Jeff Shipley, Cisco Intelligence Collection Manager

기업 환경에서 가상화 기술 사용이 늘어나는 것은 앞으로 추가 공격이나 악용의 대상이 될 가능성이 높다는 것입니다.

암호화 취약점

원격 위치에서 작업하는 직원 수가 늘어나면서 실수 또는 악의로 인한 데이터 손실 위험이 증가하고, 중요한 정보를 보호해야 하는 긴급성으로 인해 암호화가 주요 보안 수단으로 등장하였습니다. 조직은 암호화 기술을 사용하여 이메일, 커뮤니케이션, 공유 데이터 저장소 및 장비(예: 랩톱, CD-ROM, 플래시 드라이브 및 중요한 데이터가 포함되어 있는 기타 메모리 장치)에 대한 보안 유지를 하고 있습니다.

그러나 일부 암호화 기술에는 취약점이 있습니다. 암호화의 취약점으로 인해 잘못된 보안 인식이 만들어지거나 사용자 및 네트워크 관리자가 실제로는 그렇지 않은데 자신이 특정 위협으로부터 보호되어 있다고 잘못 생각할 수도 있습니다.

하나의 잘 알려진 예제로서 특정 버전의 오픈 소스 운영 체제 Debian 및 Ubuntu에는 쉽게 예측 가능한 가짜 난수 값을 생성할 수 있는 OpenSSL 취약점이 포함되어 있습니다. 이 값을 사용하면 취약한 암호화 키와 인증서 또는 암호가 만들어지고 따라서 공격에 취약해질 수 있습니다. 2008년 8월말에는 온라인 범죄자가 도용된 SSH 키를 사용하여 Linux 기반 서버를 공격하고 악성 루트킷을 설치한 사례가 있었습니다. Debian 및 Ubuntu의 OpenSSL 취약점이 이 공격에서 일정 역할을 수행했을 거라는 추측이 있습니다.

네트워크의 중요한 부분을 실행하기 위한 온라인 범죄자의 이러한 악용에 무방비 상태인 Linux 기반 서버를 사용하는 조직이 많기 때문에 이는 많은 IT 부서에게 있어서 매우 심각한 문제가 될 수 있습니다.

취약한 것으로 알려진 암호화 시스템 중 하나는 여전히 널리 사용되고 있는데, 바로 Wi-Fi 네트워크에 사용되는 WEP입니다. WEP은 이미 수년 전에 공격을 받아 깨진

상태이고 공격 및 악용 도구가 널리 퍼진 상황이기 때문에 WEP로 암호화된 Wi-Fi 네트워크를 해킹하는 것은 매우 쉬운 일입니다. 그러나 많은 개인과 조직이 아직도 계속 WEP를 사용하고 있고 따라서 여전히 범죄 행위에 취약한 상태입니다.

신용카드 정보를 처리하는 조직(예: 상점 및 서비스 공급자)은 곧 PCI DSS(Payment Card Industry Data Security Standard: 지불카드협회 데이터보안표준)에 대한 2008 업데이트에 의해 WEP에서 더 강력한 WPA 암호화로 우선 네트워크를 업그레이드해야 합니다. 그러나 무료 Wi-Fi 액세스를 제공하는 많은 조직은 이렇게 전환할 필요가 없으므로 네트워크 보안이 위험할 수 있습니다. Wi-Fi 액세스를 사용하는 많은 가정용 사용자도 도청이나 공격에 네트워크가 취약할 수 있습니다.

운영 체제 취약점

Microsoft Windows OS 및 Linux 커널의 모든 주요 버전에 영향을 미치는 취약점이 2008년에 등장하였지만, 발견된 OS 취약점의 전체적인 숫자는 작년과 비교하여 감소하였습니다. 이 취약점들 대부분은 사용자의 상호 작용이 필요합니다. 희생자가 파일을 열지 않거나 감염에 필요한 작업을 수행하지 않을 경우 인증되지 않은 원격 공격자가 악용할 수 있는 취약점은 거의 없습니다.

운영 체제의 패치와 정기적인 업데이트의 중요성 및 패치의 편리함에 대한 인식이 널리 퍼지면서 OS 취약점이 감소하는 데 크게 기여하였습니다. 이 영역에서 Microsoft의 노력이 상당한 성공을 거두었다고 할 수 있습니다. 여전히 OS 취약점이 보고되고 있지만, 그 숫자가 감소하고 있는 현상은 공격자가 점점 더 다른 유형의 취약점을 찾아서 시스템이나 사용자 정보를 공격한다는 것을 나타냅니다.

데이터베이스 및 사무용 생산성 향상 애플리케이션의 취약점

대상이 정해진 공격이나 폭넓은 공격을 수행하기 위해 사무용 생산성 향상 애플리케이션의 취약점을 이용하는 사례가 2008년에도 계속되었습니다. 잘 알려진 악성 코드들은 Microsoft Office suite, Microsoft Jet Database Engine, Adobe Acrobat 및 일본의 사무용 생산성 향상 도구 공급업체인 JustSystems의 Ichitaro 워드프로세싱 소프트웨어 같은 관련 제품을 공격합니다.

공격자가 이런 취약점을 이용하여 대상 컴퓨터를 제어하려면 일반적으로 희생자의 상호 작용(예를 들어 첨부 문서나 악성 데이터베이스 파일 열기)이 필요합니다. 공격자가 사용자 시스템의 제어권을 획득하게 되면 회사 네트워크의 특정 방어 체계를 우회하여 추가 공격을 시작할 수 있습니다.

이런 유형의 애플리케이션과 연관된 파일은 사회 공학적 기법을 사용하는 공격자의 공격 대상으로 적합합니다. 예를 들어 공격자는 조직의 회계 그룹 직원에게 "선적 부서의 손익 계산서"라는 악성 스프레드시트를 보낼 수 있습니다. 공격자는 회사 웹 사이트에서 쉽게 찾아낸 정보(예: 임원의 이름, 이메일 또는 주소)를 사용하여 문서 출처를 위장할 수 있습니다. 이는 스프레드시트로서 매우 효과적이고 그 외 다른 사무용 생산성 파일들도 합법적인 영업을 위해 조직에서 일반적으로 사용되고 있습니다. 이는 사용자가 해당 유형의 파일들을 상당부분 신뢰하게 만들고 네트워크 경계에서 차단되는 일도 거의 없음을 의미합니다.

모바일 장치 취약점

오늘날 직원의 사무 생산성을 향상시켜 주는 장치 중 핵심 부분인 BlackBerry도 올해 회사 네트워크를 손상시킬 수 있는 취약성 문제를 겪었습니다. BlackBerry 제조업체인 RIM(Research In Motion)은 BlackBerry에서 PDF 첨부파일을 여는 방식으로 인해 회사 네트워크가 공격에 취약해질 수 있음을 공개했습니다.

다른 스마트폰도 역시 공격에 취약합니다. 설치 프로그램 애플리케이션의 취약점으로 인해 트로이 목마 바이러스가 특정 전화에 설치될 수 있습니다. 그리고 일부 휴대폰에서 사용하는 웹 브라우저로 인해 사용자가 쉽게 피싱의 희생자가 될 수도 있습니다. 예를 들어 휴대폰의 웹 브라우저에 있는 주소 표시줄이 긴 URL을 전부 표시하지 않도록 구성되어 있을 수 있습니다. 피싱 사이트의 경우 대개 URL의 처음 부분은 합법적인 사이트처럼 보이기 때문에 후반부가 피싱 사이트인지 여부를 나타내는 단서가 될 수 있습니다. 또는 휴대폰의 입력 방법 때문에 주소 표시줄에 수동으로 URL을 입력하는 과정이 힘들어서 사용자가 흔히 악성 링크일 수도 있는 항목을 "클릭"하게 되는 경우가 자주 있습니다.

웹 2.0 기술을 사용하게 되면서 일부 스마트폰은 개방된 애플리케이션 개발 환경을 제공하게 되었습니다. 이는 휴대폰에 새로운 애플리케이션을 다운로드할 경우 악성 프로그램을 다운로드할 위험이 따른다는 의미입니다. 또는 보안 코딩 방법을 사용하거나 발표 전 철저한 테스트를 거친 방법을 사용하여 개발하지 않을 경우 쉽게 공격에 악용될 수 있습니다.



지정학적/정치적 분쟁

A photograph showing four individuals seated at a table with microphones, likely at a conference or panel discussion. From left to right: a man in a light blue shirt and yellow tie, a woman in a pink top, a man in a light blue striped shirt with glasses, and a woman in a dark blazer. A fourth person is partially visible on the far right. They are in front of a brick wall.

2007년 에스토니아와 2008년 그루지아에서 볼 수 있듯이 스팸, 악성 프로그램 및 봇넷이 지정학적/정치적 갈등에서 무기처럼 사용 되므로써 더 넓은 범위까지 사용되고 있습니다. 이러한 동향은 앞으로도 계속 될 것으로 예상됩니다.

2007년 "에스토니아 사이버 전쟁"(에스토니아 정부가 수도의 요지에 위치해 있던 러시아 병사 동상을 제거한 행동에 대한 러시아의 사이버 보복 공격이 있었음)에서 에스토니아 정부, 은행, 미디어 웹 사이트가 봇넷 기반의 DDoS 공격을 받아 중단되었습니다. 이러한 온라인 공격이 자발적이었는지 또는 러시아 정부의 후원을 받아 발생했는지에 대한 추측은 논란 중입니다.

2008년 7월 러시아와 그루지아간의 분쟁 중에 그루지아 정부의 웹 사이트가 National Bank of Georgia의 웹 사이트처럼 손상 또는 중단되었습니다. International Herald Tribune의 보고서에 의하면 러시아뿐만 아니라 미국에 있는 서버로부터 공격이 감행 되었습니다. 이는 "사이버 전쟁"의 유연성을 증명하는 사례입니다. 러시아 정부와 연결된 온라인 범죄자 그룹인 Russian Business Network와 연합된 봇넷이 공격에 사용되었습니다.

버마 군사 정권도 온라인 방법을 사용하여 정권에 항의하는 사람들을 탄압하였습니다. 2007년 버마의 정치적 항거 운동 중에 군사 정권은 국가의 모든 인터넷 액세스를 중단시켰습니다. (버마에는 ISP가 하나뿐이고 위성 전화를 소유하는 것은 금지되어 있으며, 인터넷 카페의 컴퓨터는 5분마다 스크린샷을 자동으로 작성하여 사용자 작업을 로깅합니다.) 버마 정부는 시위자들이 정치적 항의에 대한 디지털 사진과 보고서를 널리 발송하는 것을 중지시켰습니다. 2008년 9월의 정치적 항거 기념일에 군사 정권은 DDoS 공격을 통해 반체제 웹 사이트를 중단시킨 것으로 알려졌습니다.

대부분의 경우 적의 웹 사이트에 대한 DDoS 공격을 국가가 지원하고 있는지 입증하는 것은 매우 어려운 일이고 앞으로도 그럴 겁니다. 그러나 보안 관점에서 보면 지정학적 갈등에 인터넷이라는 구성 요소(국가에서 후원하는 경우든 개인적인 해커든 모두 포함)가 포함될

수도 있다는 것을 알고 있으면 조직은 국가의 정부, 금융, 미디어 또는 중대한 인프라 웹 사이트에 대해 DDoS 공격을 사용할 가능성에 대비할 수 있을 것입니다.

2008년 미국 선거라는 흥미로운 정치적 급변기에 특정한 정치적 캠페인 웹 사이트에 대한 DDoS 공격이 발생했습니다. 캘리포니아주의 동성간 결혼을 금지하는 이 잘 알려진 법안에 대항하기 위해 투표와 정치적 현금을 촉구하는 웹 사이트에 대한 공격이었습니다. DDoS 공격을 통해 이 법안의 제안자들은 일시적으로 방문객이 반대편 웹 사이트를 액세스하는 것을 방해할 수 있고 또 모금 운동 중 반대편의 캠페인에 현금할 수 있는 기능을 중단시킬 수 있었습니다.

지정학적/정치적 갈등 중에 봇넷 활동이 증가하는 것을 알고 있으면 적극적인 보안 전략을 만드는 데 도움이 될 수도 있습니다. 국가에서 운영하는 많은 네트워크에 대한 명확한 취약점들은 반드시 해결해야 할 사항입니다.

이러한 조직의 보안 전문가가 갈등 중 해당 네트워크와 웹 사이트가 공격 대상이 될 수 있다는 경고를 받을 수 있다면 그 전에 더욱 철저하게 네트워크를 강화할 수 있을 겁니다. 예를 들어 공격에 대항하기 위해 사용할 수 있는 기술을 사전에 모니터링하여 패치와 해결 방법을 통해 공격에 대항할 수 있습니다.

“탱크 스레드를 교체하는 비용이면 사이버 전쟁의 위험성을 알리는 모든 캠페인의 자금을 모집할 수 있습니다. 이렇게 하지 않는다는 것은 어리석은 선택이 될 것입니다.”

— Bill Woodcock, Packet Clearing House – The New York Times, 2008년 8월 13일자

갈등에서 사이버 명령까지

지난 몇 년 동안 정치적/종교적 또는 기타 동기를 가진 반조직적 해커 그룹 간(예를 들어 이스라엘과 팔레스타인, 중국과 대만, 인도와 파키스탄)의 사이버 전쟁이 존재했습니다. 최근에는 여기에 인터넷 기반 전쟁을 지원하는 명백한 국가적/군사적 후원이 가세하고 있습니다.

반조직적인 개인 또는 그룹의 사이버 전쟁이 국가 후원의 활동으로 확대되면서 이 분야에 대한 새로운 수준의 리소스, 기술 및 조직이 발생하였습니다. 미국과 대만을 포함한 일부 국가의 정부는 "사이버 사령부" 조직을 세우는 데 서명한 상태입니다. 이 조직의 임무는 국가를 온라인 전쟁으로부터 보호하고 사이버 전쟁 기능을 공격적으로 수행하는 것입니다.

더 많은 국가들이 이러한 조직을 만들려고 추구하고 있지만 공격적인 사이버 전쟁 기능이 합리적인 결정인지 여부에 대한 지속적인 논쟁이 벌어지고 있습니다. 이는 인터넷 공격자에게 공세를 취하려고 하는 네트워크 관리자의 경향이 좀처럼 온전하고 책임감 있고 실속있는 결정인 경우가 거의 없었음을 보여주는 것입니다.

기존 전자적 전쟁의 확대라는 점만 제외하면 사이버 전쟁에 대한 정의가 내려진 것은 없습니다. 그러나 커뮤니케이션의 방해와 악용이라는 개념은 확실히 포함되어 있습니다. 예를 들어 FBI에 의하면 2008년 중반, 기밀이 아닌 백악관 이메일이 누출되었다고 합니다. 해당 국가의 지원이 있었는지 확인하기는 어렵지만 이 공격의 출처는 러시아와 중국에 있는 서버인 것으로

추적되었습니다. 캠페인과 연결된 보안 회사들은 외국 단체들이 보안이 허술한 방대한 양의 데이터를 선별하여 중요한 정보를 찾아내는 이른바 "모래알"식 접근 방법을 사용하고 있다고 공개적으로 추측하고 있습니다.

이런 맥락에서 전세계 정부가 많은 프라이버시 및 도청 관련 법률을 만들고 있거나 통신 회사에 도청 허용 특전을 제공하는 것이라는 말도 있습니다. 최근의 예로는 정부가 모든 전자 통신에 관한 데이터를 수집할 수 있도록 허용하는 법률이 영국에서 제ان된 경우를 들 수 있습니다. 휴대폰을 사용하려면 사용자가 등록을 하도록 요구하는 영국 법률이 제안 중에 있습니다. 이 경우 정부가 모든 영국내의 휴대폰 사용자에게 대한 중앙 데이터베이스를 만들 수 있습니다. 이러한 제안에 대한 심각한 반대에도 불구하고 이는 보안 문제가 있을 수 있는 통신을 더 면밀하게 모니터링하고자 하는 지속적인 노력을 나타냅니다. 특정 국가나 특정 국가의 개인에게 거는 국제 전화 같이 보안 문제가 없을 경우 많은 국가에서 일반 시민은 이러한 모니터링의 영향을 받지 않습니다.



인터넷 보안 위협에 대응

개별 사례별로 현재의 인터넷 보안 위협에 대항하고 취약점을 최소화하기 위한 노력과는 별도로, 몇가지 폭넓은 이니셔티브가 온라인 보안 전쟁에서 사용되고 있습니다.

DNSSEC

업계와 정부는 2008년 여름의 심각한 문제였던 DNS 취약점을 완화하기 위해 최선을 다하고 있습니다. DNSSEC(Domain Name System Security Extensions)는 인터넷 보안에 있어 지속적으로 중요한 요소로 스푸핑과 캐시 포이즌 공격에 대항하기 위해 DNS 정보의 무결성을 제공할 것입니다. 대부분의 전문가가 DNSSEC 배포의 중요성에는 모두 동의하지만, 이를 채택하는 데 있어서의 구현의 수준과 최상위 루트 키를 누가 보유하는지에 대한 문제에 있어서 몇가지 어려움에 직면해 있습니다. 스웨덴, 불가리아, 푸에르토리코 및 브라질의 최상위 수준 국가 코드 도메인에서는 이미 DNSSEC를 사용하고 있습니다. 미국 공무원들은 최근 2009년 1월까지 정부 도메인에 DNSSEC가 구현되고, 2009년 12월까지 모든 정부 하위 도메인에도 DNSSEC를 구현할 것이라고 발표했습니다. 이렇게 되면 전세계적으로 DNSSEC 채택에 박차를 가하게 될 것입니다.

보안 공급업체와 연구원들이 취약점 공개에 더 긴밀하게 협조하고 있으므로 악용 정보가 널리 배포되기 전에 패치와 해결 방법을 만들 수 있을 것입니다. 보안 공급업체는 서로 협조하여 또는 개별적으로 현재 보안 사건에 대해 검색 및 보고하는 것을 더 쉽게 하고 위협을 정확하게 평가하려고 노력하고 있습니다. 보안을 강화하기 위한 정부의 노력이 여러 국가에서 구현되고 있으며, 온라인 범죄자를 구속하기 위한 법률도 시행되고 있습니다.

업계 및 정부의 이니셔티브

보안 연구원이나 조직, 법률 시행 또는 ICANN 덕분에 온라인 범죄자에게 서비스를 제공한 호스팅 제공업체가 폐쇄된 사건(2008년 9월 InterCage, 2008년 11월 McColo)이 두 건 있었습니다. 두 경우 모두 호스팅 제공업체의 고객이 다른 제공업체를 찾을 때까지 전세계적으로 발송된 스팸 양이 크게 감소하였습니다. 장기적인 영향은 제한적이지만 다음과 같은 긍정적인 면이 있습니다. 업계와 법률 시행 기관은 악의적인 행동을 나타내는 증거를 식별 및 수집할 수 있었습니다. 그리고 더 중요한 사실은 더 높은 수준의 서비스 공급업체가 InterCage와 McColo 및 ICANN 같은 조직에게 결정적인 조치를 취했다는 것입니다.

온라인 범죄 행위를 중단 또는 기소시키기 위한 법률 당국의 또 다른 최근 예가 있습니다.

- 2008년 7월, 시애틀의 "스팸 왕" Robert Soloway는 47개월 구금형을 선고 받았습니다. 종종 Hotmail이나 MSN 계정에서 보낸 것처럼 스푸핑 헤더를 사용하여 봇넷을 통해 수십억 건의 스팸 메일을 보내고 자신의 계정으로도 수조 건의 스팸 메일을 보내는 마케팅 스팸 서비스로 악명이 높았던 Soloway가 마침내 메일 및 이메일 사기로 기소되었습니다.
- 영국인 해커 Gary McKinnon은 NASA뿐만 아니라 미국 국방부, 육군, 해군 및 공군 컴퓨터를 해킹한 혐의로 미국 내에서 소환 및 기소되었습니다. McKinnon은 컴퓨터에 손상을 끼치지 않았다고 주장하지만 그는 외계 기술의 증거를 찾고 있었습니다.

- FTC(연방 거래 위원회)가 수집한 정보를 기준으로 미국 지방법원은 HerbalKing이라고 알려진 주요 국제 스팸 네트워크의 자산을 동결하고 중단시켰습니다. HerbalKing은 수십억 건의 스팸 메시지를 발송하여 불법 제조된 약품을 판매하였습니다. FTC는 이 메일과 관련하여 3백만건 이상의 불만을 접수했습니다. 법원은 스팸 네트워크의 자산을 동결하였 피고인이 더 이상 스팸을 발송하고 허위 제품 광고를 하지 못하도록 일시적인 강제 명령을 내렸습니다.. 또한 FTC와 협력하여 뉴질랜드 당국도 스팸머들을 대상으로 법적 조치를 취했고 미국 정부는 형사 기소를 계획 중입니다.

업계와 정부가 협력하는 가운데 Industry Consortium for the Advancement of Security on the Internet(www.icasi.org) 같은 새로운 조직이 멀티 벤더의 글로벌 보안 위협을 해결하고 있고, 업계 협력과 보안 혁신을 위한 포럼을 만들고 있습니다.

기술 및 보안의 변화를 반영하기 위해 업계 기준이 계속 업데이트되고 있습니다. 예를 들어 PCI DSS(지불카드협회 데이터보안표준)가 2008년에 업데이트되어 더 안전한 무선 보안 기술을 규정하고 있습니다.

반면 CERT(National Computer Emergency Response Team)는 위협 및 취약점을 평가하는 데 있어서 계속 중요한 역할을 수행하면서 다른 정부 및 산업 협회에서 하는 것처럼 정보를 제공하거나 공급업체 대응을 조정합니다.

ID 도용 분야에 관한 미국 정부의 2008 Identity Theft Task Force Report에서는 2007년 2,470명의 범죄자가 ID 도용 관련 범죄로 기소되었고 그 중 1,943명이 실제로 유죄 판결을 받았다고 밝히고 있습니다. 높은 기소 비율과 규정 준수 요구사항, 그리고 개인 정보 보호를 위해 모범 사례를 따르는 조직의 수가 늘어나면서 ID 도용 가능성을 줄이는 데 도움이 되고 있습니다.

그러나 범죄자들은 여전히 ID 도용 관련 범죄로 많은 수익을 벌어들이고 있습니다. 기소 가능성은 현재 낮은 편입니다. 해당 범죄의 충분한 기소를 보장하기 위해 보고서에서는 정부가 민사상 벌금형을 검토해볼 것을 권장하고 있습니다.

ID 도용 관련 범죄를 더 철저하게 다루려면 개인적인 인식 전환과 기업의 추가 보안 조치뿐만 아니라 기소 및 국제적 협력을 위한 포괄적인 접근 방식도 필요합니다. 이를 진척시키기 위해 해당 범죄에 대한 보고 및 법률 시행 기관과의 협조가 더욱 절실합니다.

가능하게 만드는 기술들

보안 공급업체는 보안을 더 쉽게 만들어서 보안 도구와 정책을 준수하고 구현하는 것을 개선하는 데 적극적으로 노력하고 있습니다.

예를 들어 공급업체는 계속적으로 보안 위협을 공개하고 패치를 더 신속하게 발표해오고 있습니다. 사용자 교육 덕분에 많은 공급업체는 최종 사용자가 보안 위협 및 위협에 대한 정보를 더 쉽게 찾고 잠재적인 부정적인 영향을 평가할 수 있도록 만들어왔습니다.

많은 공급업체와 사용자에게 있어서 기술을 통해 보안을 더 간단하게 만드는 것은 다음과 같은 보안 솔루션을 만드는 것을 의미합니다.

- 보안 정책을 보다 쉽게 만들고 적용할 수 있습니다.
- 보안 작업(중요한 데이터 암호화 또는 패치 배포 등)을 자동화합니다.
- 꾸준히 확장되고 있는 네트워크 내에서 보호를 제공합니다.
- 실시간으로 위협을 긴밀하게 모니터링하고 평가합니다.
- 여러 벡터의 위협요인으로부터 보호합니다.
- 다른 보안 도구와의 통합을 지원합니다.
- 작업자가 새로운 협업 및 생산성 도구를 안전하게 사용할 수 있도록 합니다.

더 쉽게 보안을 구현할 수 있게 해주는 표준

더 쉽게 보안 사건을 보고하고 현재 보안 문제에 대한 정보를 찾을 수 있는 유용한 업계 표준이 만들어졌습니다. 이것은 회사가 자사 웹 사이트에 높은 수준의 "보안" 관련 페이지를 만들도록 하고, 방문객이 그 주소를 쉽게 기억할 수 있도록 했습니다. 예를 들어 Example이라고 하는 회사의 제품에 영향을 미치는 알려진 취약점에 대한 최신 정보를 보려면 브라우저에 “www.example.com/security”만 입력하면 됩니다. 아직까지는 일부 회사만 이 기준을 따르고 있습니다. 많은 회사들이 현재 지체된 상태입니다.

표준화된 보안 페이지를 사용하는 업체

cisco.com/security
microsoft.com/security
adobe.com/security
yahoo.com/security
facebook.com/security

표준화된 보안 페이지를 현재 채택하지 않은 업체

apple.com
secondlife.com
google.com
mcafee.com
myspace.com

결론 및 주요 권장사항



2008년은 온라인 보안 위협의 확대 및 전개에 있어서 주목할만한 해였습니다. 온라인 범죄자가 수억 달러를 가로챈 경우도 있었습니다. 이런 경제적 이득 때문에 앞으로도 수년간 보안 범죄 기술의 혁신과 전문화가 계속 될 것으로 보입니다.

하나 이상의 온라인 요소(웹, 스팸, 악성 프로그램, 봇넷)가 결합된 위협이 발생 빈도와 정교함 면에서 계속 증가하고 있습니다. 더 나은 효과를 보기 위해 위협 범죄자는 특정한 개인이나 그룹을 대상화하고 합법적인 웹사이트 및 기타 신뢰할 수 있는 단체와 시스템을 악용합니다. 또한 신중한 사용자마저 속일 수 있고 검색이 어려운 위협을 점점 더 만들어내고 있습니다. 그리고 사회 공학적 기법과 시사적인 제목을 사용하여 온라인 범죄를 피해자가 더 신뢰할 수 있도록 교묘하게 만들고 있습니다. 반면 온라인 위협을 통해 전파된 악성 프로그램은 이전보다 더 교묘하고 은밀하게 계속 다시 설계되고 있고 증가율도 엄청납니다. 인터넷 범죄 행위의 중심인 봇넷은 계속 악성 프로그램을 전파하고 수백만 건의 스팸을 발송하고, 악성 웹 사이트를 운영하고, 합법적인 웹 사이트를 공격합니다. 이런 위협에 대응하기 위해 조직은 자신의 보안 전략에 적극적인 악성 프로그램 및 봇넷 방지 구성요소를 포함시켜야 합니다.

온라인 범죄자는 기술과 시스템적인 면에서 신, 구의 모든 취약점을 악용하여 봇넷을 만들어냅니다. 그러나 이미 알려진 영향력이 큰 취약점들조차 제대로 패치되지 않고 있습니다. 동시에 모바일 장치의 사용과 원격 작업, 웹 2.0 도구, 가상화 및 새로운 형태의 협업이 늘어나면서 보안 경계는 확장되고 네트워크 침투 가능성은 더 높아지고 있습니다. 이것은 조직이 보안 경계를 높이고 고급 보안 정책 및 기술의 채택 필요성을 강조할 경우 심각한 도전 과제가 발생합니다.

데이터 손실 문제는 지속적으로 위협이 따르고 조직과 개인에게 큰 영향을 미칠 수 있는 과제입니다. 강력한 보안

정책을 만들면 도움이 될 수 있지만, 무엇보다도 조직 전반에 걸쳐서 이러한 정책을 구현하고 시행하는 것이 중요합니다. 데이터 손실에 관해 많은 조직은 중요한 정보가 들어있는 회사 장비가 언제가는 분실될 가능성이 있음을 이미 알고 있습니다. 따라서 조직은 중요한 정보에 대한 접근이나 권한이 없는 사용자에게 의한 접근을 막기 위해 VPN이나 콘텐츠 필터링, 인증 기술, 액세스 제어, 암호화 및 데이터 삭제와 같은 기술을 사용하고 있습니다. 내부인에 의한 위협도 인식과 주의가 필요한 또 다른 이슈입니다. 위기를 겪고 있는 글로벌 경제에 있어서는 보다 더 많은 이러한 공격이 예상되고 있습니다. 반면 2009년에는 정부 당국과 공격자 및 스파머들 간의 전쟁에 관한 뉴스가 보다 더 많아지리라 예상됩니다. 전문화되고 복잡한 서비스를 제공하면서 오늘날 공격자는 더 조직화되고 따라서 추적 및 체포가 더 쉬워질 수 있습니다. 그러나 보안 공급업체와 당국이 협력하여 온라인 범죄자를 기소하고 있지만 공격의 수는 거의 감소하지 않고 있습니다.

IT를 최전선에 배치

시스코에서 발표한 2008년 8월 InsightExpress 보고서 "The Challenge of Data Leakage(데이터 누출의 위험)"에 의하면 전세계 비즈니스 작업자의 50% 정도가 자신의 컴퓨터를 업무 용도와 개인 용도로 같이 사용하고 있는 것으로 나타났습니다. 대부분의 회사의 경우, 업무 용도와 개인 용도의 IT 사용을 혼용하는 것을 피할 수 없습니다. 하지만 적절한 사용 정책을 정의하여 시행하고는 있습니다. 그런데 이것이 더 도전적인 문제를 낳을 수도 있습니다.

실제로 기업 보안 정책의 일반적인 실패 원인에 관한 시스코의 최근 연구에 의하면 정책 위반 원인에 관한 IT의 인식과 직원의 실제 동기 간에 차이가 있는 것으로 드러났습니다. 조사 대상인 대부분의 직원은 정책이 작업 현실과 맞지 않거나 정책에 포함되지 않은 애플리케이션에 액세스해야 하기 때문에 보안 정책을 위반하는 것으로 답변했습니다. 대부분의 IT 전문가는 무관심과 인식 부족이 직원의 보안 정책 위반에 대한 일반적인 원인인 것으로 생각하고 있습니다.

많은 회사에서 보안을 개선하기 위한 적절한 수준의 정책을 정의하려고 고민하고 있지만, 그것이 오늘날처럼 경쟁이 치열한 환경에서 비즈니스를 수행하기 위한 작업 수준이나 협업을 억제할 정도로 융통성이 없는 것은 아닙니다.

IT 직원은 이를 지원할 수 있고 보안 위험과 싸워야 하는 최전선에 있습니다. Frost & Sullivan의 2008 Global Information Security Workforce Study에 의하면 자격과 경험이 있는 직원이야말로 보안 위험을 종식시킬 수 있는 열쇠인 것으로 밝혀졌습니다. 이런 직원은 임원 및 다른 직원과 직접 협력하여 조직의 모든 레벨에서 시행가능하고, 사용자에게도 친숙한 정책을 만들고

구현할 수 있습니다.

그러나 기업의 보안을 보장하는 데 IT가 더 많이 관련되어 있고 효과적이라면 조직은 IT 부서에 더 많은 투자를 해야 합니다. IT 부서가 적절한 리소스와 경험과 지식이 풍부한 전문가(특히, 보안 전문가)를 액세스할 수 있도록 보장하는 것이 열쇠입니다.

또한 IT 부서의 보안 정책에 관한 인식을 "금지"에서 "허용"으로 바꾸는 것도 중요합니다. 예를 들어 직원이 IT 정책에도 불구하고 원하는 도구를 다운로드하려는 것을 IT 직원이 인지한 경우 문제에 대한 실질적인 솔루션을 제공할 수 있습니다. 예를 들어 다운로드 가능한 버전을 제공하거나 작업 대상 웹 사이트 콘텐츠까지의 안전한 경로를 만들어줄 수 있습니다.

직원이 어쩔 수 없이 실수를 하거나 실수로 보안을 위협하는 무언가를 다운로드한 경우 이를 IT 부서에게 알려서 바로 해결할 수 있도록 권장해야 합니다. 악의적인 의도 없이 단순한 인간적인 실수로 인해 사건이 발생한 경우 조직은 즉시 위험을 발견하여 처리할 수 있도록 해준 직원에게 즉각적인 감사를 표시해야 합니다. 그러면 사용자는 IT 부서에게 위험에 대해 알리는 것을 두려워하지 않게 될 것입니다.

직원은 자신들의 ID 보안과 기술 사용으로 전파되는 위험을 인지하는 데 있어서 중요한 역할을 수행할 수 있습니다. 보안 정책 및 기술과 온라인 위험에 대한 지속적인 사용자 교육이 도움이 될 수 있습니다. 보안 위험 및 위험에 대한 직원 교육의 중요한 이점은 궁극적으로 직원의 개인적인 삶에 더 나은 기술 사례를 활용하도록 유도함으로써온라인 범죄자를 궁지에 몰아넣을 수 있다는 점입니다.



주요 권장사항 점검 목록

- ✓ 대상을 명확히 합니다.
- ✓ 사용자가 실수로 악성 프로그램을 네트워크에 다운로드하지 않도록 방지합니다.
- ✓ 알려진 취약점을 패치합니다.
- ✓ 데이터 손실을 방지합니다.
- ✓ 내부인 위협을 심각하게 받아들입니다.
- ✓ 네트워크를 고려합니다.
- ✓ 정책 준수 그 이상을 고려합니다.
- ✓ 보안을 보다 쉽게 만듭니다.

주요 권장사항

대상을 명확히 합니다. 조직이 보안에 관해 염두에 두어야 할 기본적인 사항은 모든 것을 보호하려고 하면 아무 것도 보호할 수 없다는 것입니다. 대신 조직은 전략적, 재정적, 경쟁적인 측면에서 가장 중요한 항목에 모든 시간과 노력과 리소스를 집중해야 합니다.

사용자가 실수로 악성 프로그램을 네트워크에 다운로드하지 못하도록 방지합니다. 사용자가 악성 프로그램이 포함된 웹 페이지를 방문하거나, 웹 페이지의 손상된 부분을 다운로드하지 못하도록 하려면 악성 프로그램 검색 기술을 사용해야 합니다. 이러한 기술로는 예방적인 실시간의 신뢰 기반 필터링 솔루션과 네트워크 게이트웨이에서 규칙 및 애플리케이션 기반의 방화벽 및 침입 방지 소프트웨어가 있습니다.

개인 사용자는 악성 프로그램 다운로드의 희생자가 될 수 있는 기회를 크게 줄일 수도 있습니다. 브라우저를 업데이트 및 패치하고, 보안 기능 및 설정을 사용하고, 기존 및 미래의 위협요인을 인식하는 것이 중요합니다. 그래서 신뢰할 수 있는 소스에서 보낸 이메일이라도 이메일로 받은 링크를 클릭하지 않는 것이 중요합니다. 대신 신뢰할 수 있는 URL을 항상 수동으로 입력하고, 책갈피로 저장하고, 다른 사람이 제공한 링크를 클릭하는 대신 책갈피를 사용하여 다시 방문해야 합니다.

알려진 취약점을 패치합니다. 오늘날처럼 보안 위협이 급변하는 환경에 효율적으로 대응하려면 보안 조직이 새로운 동향을 항상 주시하고 있어야 합니다. 그러나 대부분의 현재와 미래의 위협은 이미 알려진 취약점을 이용하기 때문에 조직이 앞으로의 위협요인으로부터 완전히 피할 수는 없습니다. 기존 결함을 해결 및 패치하는 데 시간, 노력 및 리소스를 사용하는 것이 여전히 중요합니다.

일반적인 공격의 80% 정도가 효과가 높은 취약점의 20%를 이용하고 있습니다. 이렇게 효과가 높은 취약점이 종종 가장 기본적인 취약점이고 특정 환경에서는 계속 패치되지 않는 경우가 자주 있습니다. 대부분의 경우 효과가 높은 취약점을 업데이트하고 보안할 경우 "80대

20" 솔루션으로 이어질 수 있습니다.

데이터 손실을 방지합니다. 조직을 데이터 손실의 부정적인 영향으로부터 보호하는 데는 강력한 보안 정책이 필수적입니다. 그러나 이 보안 정책은 효율적으로 시행해야 하고 사용자가 정책을 알고 있어야 합니다.

다음은 데이터 손실과 관련된 위험을 줄이기 위한 권장 사항입니다.

- 액세스 제어, 암호화, 원격 데이터 제거, 데이터 조작 또는 실질적으로 데이터를 사용할 수 없게 만드는 기타 방법 등을 통해 랩톱, 썬 드라이브, PDA 같은 모바일 장비의 정보 기밀성을 유지하기 위한 (가급적이면 자동화된) 방법을 적용합니다.
- 데이터를 분류하고 사람들이 액세스할 수 있는 데이터는 더 강력하게 제어합니다.
- 보호해야 할 데이터를 정의하여 가장 중요한 정보를 가장 안전하게 보호하는 데 초점을 맞춥니다.
- 랩톱 또는 기타 모바일 장치에 저장해야 할 정보와 해당 장치의 도난 시 수행해야 할 작업에 관해 교육합니다.
- 이메일과 웹 트래픽을 적극적으로 모니터링하여 중요한 정보를 부적절하게 공유하지 않도록 합니다.

내부인 위협을 심각하게 받아들입니다. 트래픽 패턴, 시스템 및 데이터베이스를 지속적으로 로깅, 감사 및 모니터링하여 항상 조심합니다. 직원이 승인되지 않은 작업에 관여하지 않도록 정책을 설정합니다. 기업은 정보 보안팀이 물리적인 보안 팀과 인사 부서와 협력하여 퇴직/이직한 직원의 액세스 권한 해제에 관한 효율적인 정책을 구현하도록 합니다. 그리고 채용 시 항상 철저한 범죄 경력 조회를 수행합니다.

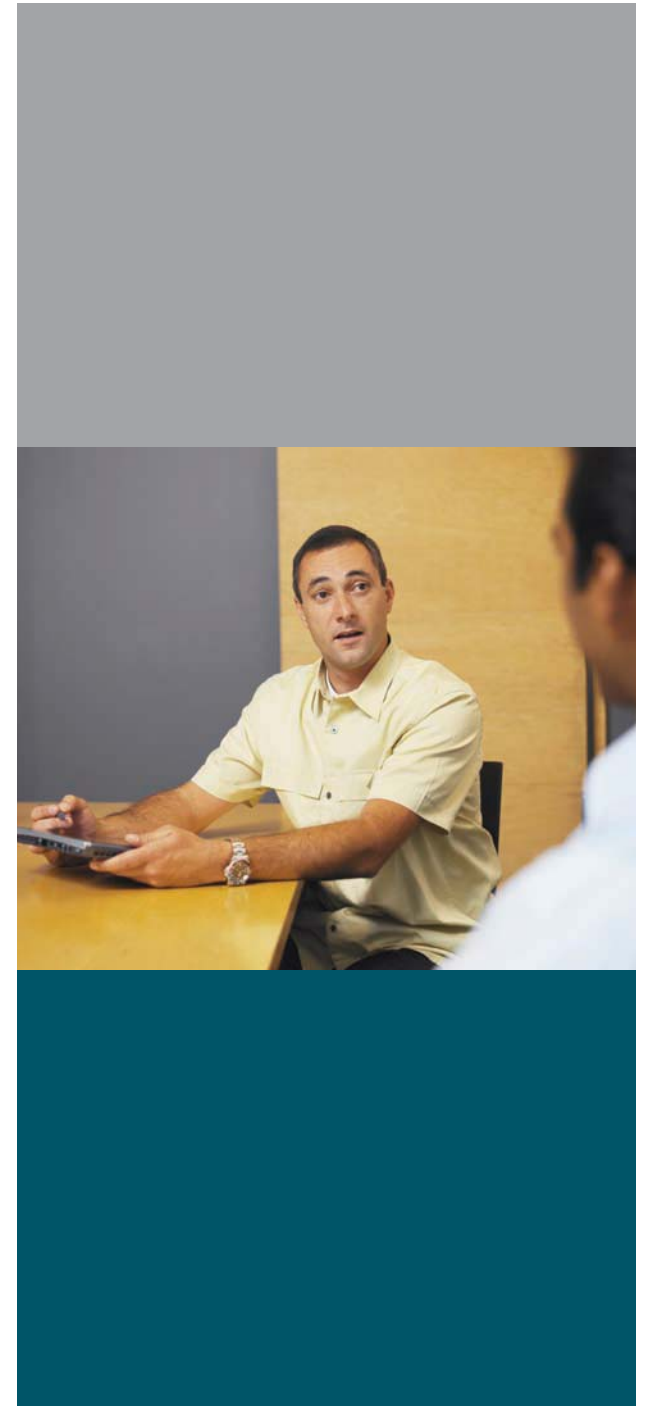
네트워크를 고려합니다. 기업의 보안이슈는 단지 뉴스를 장식하는 악성 프로그램의 위협이나 데이터 침해에 관한 것만은 아닙니다. 많은 기업에게 있어서 네트워크가 보안상의 허점임에도 불구하고 네트워크 장비를 방치하는 경우가 있습니다. 특히 요즘처럼 비용 절감에 민감한 상황에서는 많은 기업들이 네트워크에 대해 "고장나지 않았다면 손댈 필요가 없다"는 식의 접근을 하고 있습니다. 대부분 조직이 최소한 일년에 한 번 네트워크를 업그레이드해야 하지만, 최적의 업그레이드 빈도는 규모, 복잡도, 보안 요구사항, 리소스 제한사항 및 기타 고려사항에 따라 각기 다릅니다.

정책 준수 그 이상을 고려합니다. 조직은 정책 및 규정 준수로 보안의 모든 것으로 해결할 수 있다고 간주하지 말아야 합니다. 대부분 규제 준수와 요구 사항을 충족하기 위한 절차 조정에만 집중함으로써 조직은 급변하는 현재의 위험과 위험 환경을 볼 수 있는 기회를 놓칠 수 있습니다. 따라서 규정 준수를 검토하는 것 외에도 기존 절차를 개선하고 현재와 미래의 위험에 적극적으로 대응하기 위해 포괄적인 문제점 분석을 정기적으로

수행해야 합니다.

보안을 더 쉽게 만듭니다. 무엇보다도 보안 도구와 솔루션을 보다 쉽게 구현하여 사용할 수 있도록 만들고 보안 정책 또한 쉽게 따를 수 있도록 만들어야 합니다.

- 보안을 임시변통으로 특정지점에 대해서만 조각 내서 사용하기보다는 보안 기술을 통합하여 여러 요소에 배치합니다.
- 보안 솔루션과 담당부서가 효율적으로 데이터를 공유할 수 있게 합니다.
- 모든 중요한 자산을 보호하고 구현을 자동화/단순화하도록 보안 정책을 구현합니다.
- IT 부서와 직원이 서로 협력하여 생산성 향상 도구와 콘텐츠를 회사 네트워크 안과 밖에서 안전하게 액세스할 수 있도록 교육합니다.
- 생산성을 방해하지 않는 방식으로 기존 네트워크 및 보안 하드웨어와 솔루션을 패치 및 업데이트합니다.
- 새로운 위협에 대한 사용자 교육과 인식 제고를 계속 수행하고 사용자가 보안상의 이슈가 발생 가능한 문제를 바로 보고할 수 있도록 격려하고 권장합니다.



2009년에 예상되는 주요 동향



2009년 보안 전략을 수립하고 IT 예산을 계획할 수 있도록 시스코는 앞으로 주의해야 할 주요 동향을 다음과 같이 정리했습니다. 이 예측은 2008년 발생한 사건 및 뉴스와 전세계 시스코 보안 조직과 비즈니스 조직에서 제공한 관련 정보를 기준으로 작성되었습니다.

작지만 대상이 명확하고 빈도가 잦아지는 공격

2009년에는 더 교묘한 공격이 발생할 것으로 보입니다. 개인, 그룹, 비즈니스, 조직 및 정부를 포함한 특정 대상을 위해 설계된 공격이 급속하게 배포될 것으로 보입니다. 현재 전세계 금융 위기가 계속되고 있으며, 자연 재해와 세속적인 사건사고들은 지속적으로 전세계에 뉴스 꺼리들을 계속 제공할 것입니다. 또한 2009년에는 미국에 새로운 대통령이 취임했습니다. 범죄자들은 이러한 뉴스를 어떻게 이용할 것인지 계속 연구하고 있을 겁니다. 사회 공학적 기법과 피싱 기술을 이용하면 수익성이 높기 때문에 공격자들은 성공율을 높이기 위해 이런 공격을 효과적으로 전달하는 방식을 계속 개발할 것으로 보입니다. 더 많은 전문가(복잡하고 확실한 공격을 만드는 데 필요한 하나 이상의 주요 구성 요소를 제공하는 범죄자)가 생길 것입니다. 이들의 전문 지식과 명성이 높아지면서 이들은 효과적인 공격을 만들려고 하는 다른 범죄자에 의해 고용될 수도 있을 것입니다.

프로토콜간 공격

성공 가능성을 높이기 위해서 온라인 범죄자는 이메일, 웹 기반 위협 및 침입 기술을 혼합한 프로토콜간 접근방식이나 혼합된 접근방식을 점점 더 많이 사용하게 될 것입니다. 최근에 성공률이 높은 이런 유형의 공격은 2009년에도 계속 증가할 것입니다. 예를 들어 스팸 발송, 악성 프로그램 호스팅, 직접 공격 시행 등을 동시에 수행할 수 있는 "멀티태스킹"이 가능한 봇넷이 더 늘어날 것으로 예상됩니다.

따라서 보다 강력한 다중 프로토콜을 이용한 공격으로부터 보호하기 위해 조직은 모든 인터넷 트래픽 유형을 모니터링하고 새로운 위협을 즉각적으로 식별하여 중지할 수 있는 보안 시스템을 구현해야 합니다. 하나의 영역(예: 이메일, IPS 또는 웹 기반 위협)에만 초점을 맞추는 보안 솔루션이나 영역간 데이터를 효율적으로 연합할 수 없는 보안 솔루션은 혼합된 공격으로부터 조직을 충분히 보호할 수 없습니다.

신뢰를 악용한 하이잭킹

신뢰를 악용하는 하이잭킹 방법은 온라인 범죄자에게 매력적이고 효과적인 방법임이 입증되었습니다. 사람들이 그 기관의 브랜드를 신뢰할 경우 연관된 사이트를 방문하거나 해당 조직에서 보낸 이메일은 의심하지 않고 열어 볼 가능성이 높습니다. 기존의 대부분의 보안 솔루션은 URL 또는 IP 필터링 목록을 사용하고 있지만, 웹 페이지 상의 모든 요소의 의심스러운 동작과 트래픽 패턴을 실시간으로 관찰하지는 않습니다. 이러한 솔루션에는 신뢰된 웹 사이트나 이메일 발송자가 어떤 위험을 내포하고 있는지를 인식할 수 있는 장치가 없습니다.

2009년에는 더 많은 온라인 범죄자들이 적극적으로 보다 교묘한 방법을 찾아서 사용자의 신뢰를 악용하는 하이잭킹을 시도할 것으로 보입니다.

이동성, 원격 작업 및 새로운 도구가 위험 요인이 될 수 있음

생산성을 꺾을 수 있는 원격근무, 웹 기반의 도구들, 모바일 장치, 가상화, "클라우드 컴퓨팅" 최근 트렌드는비용절감이라는 경제상황과 세계화라는 시대상황에 맞물려 2009년에도 지속될 것으로 보입니다. 이는 외부로부터의 공격이나 내부인의 위협 또는 랩톱 같은 데이터 저장 장치에 관한 부주의 등으로 인한 데이터 손실을 방지하는 것이 그 어느 때보다도 중요하다는 것을 의미합니다. 보안담당자에게는 어려운 도전이 될 것입니다. 네트워크 경계가 급속도로 확장되고 있고, 사용하는 장치와 애플리케이션 수가 증가하면서 네트워크에 대한 침투 가능성은 커지고 있고 새로운 위험 요인이 만들어지고 있습니다.

모든 유형의 조직은 민감한 데이터에 대한 손실 방지(DLP) 정책을 철저하게 구현하고 중요한 데이터는 자동으로 보호하는 보안 솔루션을 고려해야 합니다. 모든 조직들은 또한 특히 오늘날 경제에서 점점 더 중요한 자산이 되고 있는 지적 자산을 보호하기 위한 조치를 취하기 시작해야 합니다.

보안에 대한 전체론적 접근 방식



시스코의 보안 비전은 고객들이 신뢰를 갖고 협업할 수 있도록 만드는 것입니다. 그렇게 하기 위해 시스코는 기존의 위협들과 새로 부상하는 다양한 위협들에 대해 포괄적이고 능동적이며 다층적인 접근 방식을 견지할 것입니다.

Cisco Security Intelligence Operations는 시스코 고객들에게 가장 높은 수준의 보안을 지속적으로 제공하기 위해 보안위협 감지, 상호연관성 분석 및 그에 따른 완화 기능을 제공하는 고급 서비스입니다. 전세계 연구 엔지니어와 정밀한 보안 지식 그리고 자동화된 업데이트 시스템을 고루 갖춘 팀을 만들어 이용하는 Cisco Security Intelligence Operations를 통해 고객은 안전하게 협업하고 새로운 기술을 채택할 수 있습니다. 프로토콜 및 공급업체 간에 결합된 취약점 위협 때문에 보안 업계는 개별적인 위협을 방어하거나 개별적인 제품을 보호하는 단층적 방어는 이제 더 이상 충분하지 않다는 것을 인식하게 되었습니다. 통합된 보안 관리, 실시간 신뢰성 평가 및 중첩된 멀티포인트 접근 방법이 새로운 화두로 등장하고 있습니다.

Cisco Security Intelligence Operations에서는 시스코 내의 여러 조직 및 장비로부터 도출된 통합된 데이터를 사용하여 인터넷 위협과 취약점을 계속해서 평가하고 서로 연관시켜 나갈 것입니다. 이 데이터의 출처는 다음과 같습니다.

- 시스코의 전세계 Threat Operations Centers – 400명 이상의 연구원이 새로운 동향과 위협을 추적하고 있습니다.
- Cisco Security Remote Management Services – 경험이 풍부한 시스코의 전문 보안/네트워크 전문 인력이 보안 사건 모니터링, 오류 및 성능 관련 사건 관리, 문제점 해결, 보안 인프라 조정 및 안전한 네트워크 액세스 제어 지원 등을 위한 운영 지원을 24 시간 제공합니다.
- SenderBase 네트워크 – SenderBase는 전세계 웹 및 이메일 트래픽의 30%를 모니터링하고 매일 300억 건의 쿼리를 처리하고 있습니다. 인터넷상의 모든 활성 웹 서버들의 실시간 신뢰도와 신용을 평가하기 위해 SenderBase 네트워크에서는 150개 이상의 서로 다른 네트워크 레벨 파라미터를 추적합니다.

- Cisco Security IntelliShield Alert Manager – 최신의 적용 가능한 정보, 철저한 취약점 분석 및 신뢰할 수 있는 위협 검증 서비스를 제공하는 사용자의 커스터마이징이 가능한 경고 서비스입니다.
- Cisco Intrusion Prevention Systems – 웜, 네트워크 바이러스, 애플리케이션 위협, 시스템 침입 시도 및 애플리케이션 오용 같은 알려지거나 알려지지 않은 위협 요인을 식별, 분류하고 중지시킵니다.
- Real-time network traffic telemetry data – Cisco 네트워크 장치에서 제공하는 실시간 네트워크 트래픽 원격 측정 데이터로 2009년부터 시스코 제품들에 구현됩니다.
- 이 외 시스코 기술 – Cisco Security Research and Operations, Cisco Security Incident Response, Corporate Security Programs Office 및 Global Policy and Government Affairs가 포함됩니다.

시스코를 통해 기업은 위협과 취약점을 연구하는 데 걸리는 시간을 절약하고 더 사전적인 보안 접근 방식을 시행하는 데 집중할 수 있습니다.

인터넷 보안 위협은 갈수록 진화하고 있기 때문에 Cisco Security Intelligence Operations는 글로벌 보안 위협과 동향을 식별하는 기술을 개선하고 전문가 분석 및 서비스를 제공하여 사용자를 이런 위협으로부터 보호하고자 최선을 다하고 있습니다. 시스코는 포괄적이고 통합된 보안을 적시에 제공할 수 있는 완벽한 보안 솔루션을 통해 전세계 조직들이 총체적 보안이 가능하도록 할 것임을 약속드립니다.

추가 정보

시스코 보안 센터
www.cisco.com/security

SenderBase
www.senderbase.org

시스코 보안 솔루션
www.cisco.com/go/securitysolutions
www.cisco.com/go/ros

시스코 보안 제품
www.cisco.com/go/security
www.cisco.com/go/intellishield
www.cisco.com/go/ips
www.ironport.com

시스코 기업 보안 프로그램 조직
www.cisco.com/go/cspo

보고서 다운로드
www.cisco.com/go/securityreport



미주 지역 본사
Cisco Systems, Inc.
San Jose, CA

아시아 태평양 지역 본사
Cisco Systems (USA) Pte. Ltd.
Singapore

유럽 지역 본사
Cisco Systems International BV
Amsterdam, The Netherlands

시스코는 전 세계에 200여 개의 사무소를 두고 있습니다. 주소, 전화 번호 및 팩스 번호는 시스코 웹 사이트(www.cisco.com/go/offices)를 참조하십시오.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, Cisco 로고, DCE 및 Welcome to the Human Network는 상표입니다. Changing the Way We Work, Live, Play 및 Learn and Cisco Store는 서비스 상표입니다. 그리고 Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, Cisco Certified Internetwork Expert 로고, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, IronPort 로고, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx 및 WebEx 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 해당 자회사의 등록 상표입니다.

그 외 본 문서 또는 웹 사이트에 언급된 각각의 상표들은 해당 소유자의 자산입니다. 여기에 인용된 '파트너'의 의미가 시스코와 특정 회사 간의 파트너십 관계를 반드시 의미하지는 않습니다.

(0809R) C02-512160-00 12/08