Cisco Outbreak Filter

새로운 툴을 사용한 스피어 피싱 및 표적 공격과 정찰 문제가 더욱 증가하고 있습니다. Cisco Outbreak Filter는 더 스마트한 공격자와 정교해진 전술에 맞설 수 있도록 설계되었습니다. 본 백서에서는 이러한 공격의 다양성과 함께 Cisco Outbreak Filter에 대한 소개, 작동 방식 및 구성 옵션에 관해서도 설명합니다.

전환점

2010년 말에 스팸 양이 처음으로 감소하는 조짐을 보이기 시작했습니다. 2010년 10월부터 활동이 활발한 여러 스패머 및 봇넷이 폐쇄되었기 때문입니다.

위협을 전송하는 데 사용되는 봇넷 명령 및 제어 인프라의 폐쇄로 인해 이러한 활동이 억제됨에 따라 스팸 양이 대폭 감소하게 되었습니다. 여전히 대량의 스팸을 발송하는 시스템이 존재하긴 하지만, 전술상에 분명한 변화가 생겼습니다. 이제 공격자는 대량의 스팸 폭탄을 발송하는 것 외에, 특수하고 정교한 표적 공격 메시지의 발송을 늘려 안티스팸 보안 시스템을 피하려고 합니다.

표적 공격에 한발 앞서 대비

지금까지의 스팸 메일은 문법, 철자 및 구두점 오류가 빈번하고 형식적인 어조를 사용했으므로 식별하기가 쉬웠습니다. 그러나 이제 공격자는 전체 메시지에 맞게 언어 표현과 콘텐츠를 세련되게 다듬어 진짜 이메일과 스팸을 구분하기 어렵게 만들고 있습니다.

표적 공격은 전 세계적으로 조직이 직면하고 있는 문제인 인바운드 스팸 메시지의 1% 미만인 것으로 나타납니다. 이러한 공격은 다음과 같이 분류됩니다.

- **APT(Advanced Persistent Threat):** 이러한 메시지는 장기간에 걸쳐 조직의 네트워크로 침투하려고 시도하는 광범위한 공격의 일부로 전송됩니다.
- **스피어 피싱 및 웨일링(whaling):** 이러한 메시지는 금전 또는 정보를 빼내려는 목적으로 특정 개인을 표적 대상으로 합니다. 일례로 조직의 은행 정보를 빼내는 소프트웨어를 설치하기 위해 기업의 재무 부서를 대상으로 한 표적 공격을 들 수 있습니다.

표적 공격의 경우 Facebook 및 LinkedIn 등의 소셜 네트워킹 사이트에서 쉽게 확보할 수 있는 데이터를 사용합니다. 공격자는 도시 이름 또는 대상자의 이름을 포함하거나 친구 또는 회사 동료가 보낸 이메일인 것처럼 조작하여 공격이 성공할 가능성을 높입니다. 공격자는 보안 사슬의 연결 취약점이 일반적인 최종 사용자라는 점을 알고 있으며, 소셜 엔지니어링을 통해 가장 많은 결과를 얻을 수 있다는 점도 알고 있습니다.

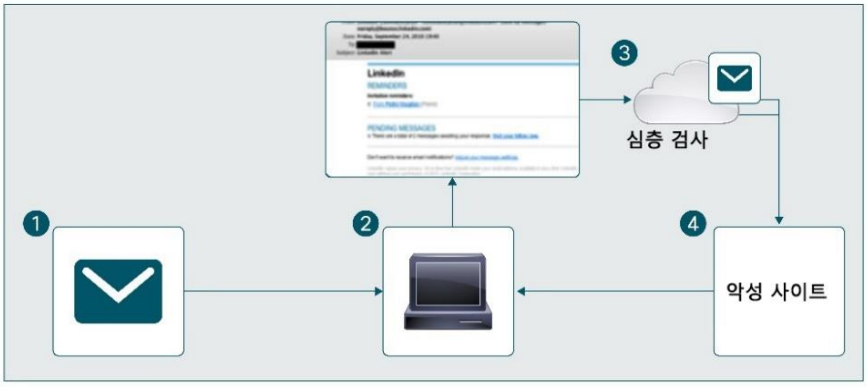
이러한 공격에 한발 앞서 대비하려면 체계적인 노력이 필요합니다. Cisco Outbreak Filter 기술은 이 문제를 해결하기 위해 설계되었습니다. 이 기술은 "악성" 이메일 발신자에 대한 Cisco SenderBase® 정보, Cisco 보안

어플라이언스에서 수집한 Cisco SensorBase™ 정보, 웹 스캔 기술인 Outbreak Intelligence를 조합하여 사용합니다. Cisco Outbreak Filter에서는 정교한 규칙 세트를 사용하여 이메일을 스캔하고, Dynamic Quarantine을 통해 의심스러운 이메일을 보류하여 재스캔을 수행하며, Outbreak Intelligence를 통해 의심스러운 URL을 스캔합니다.

Outbreak Filter는 어떤 방식으로 작동합니까?

Cisco Outbreak Filter는 Cisco Virus Outbreak Filter를 기반으로 합니다. Outbreak Filter는 첨부 파일을 통해 전달된 기타 악성코드 및 새로운 바이러스 침투 현상으로부터 시스템을 보호한다는 점에서 이전 제품과 동일하지만, 악성 사이트를 차단하기 위해 사용자가 URL을 열 때 해당 URL을 실시간으로 스캔함으로써 이와 같은 기술을 새로운 차원으로 발전시킵니다. 또한, 필터에서 이러한 웹 사이트에 대한 데이터를 Talos(Talos Security Intelligence and Research Group)로 전송하여 SensorBase 기술이 통합된 Cisco 보안 제품의 모든 사용자를 보호하며 이러한 제품에는 Cisco의 방화벽, 웹 보안 및 침입 방지 제품이 포함됩니다.

그림 1. Cisco Outbreak Filter 단순 흐름도



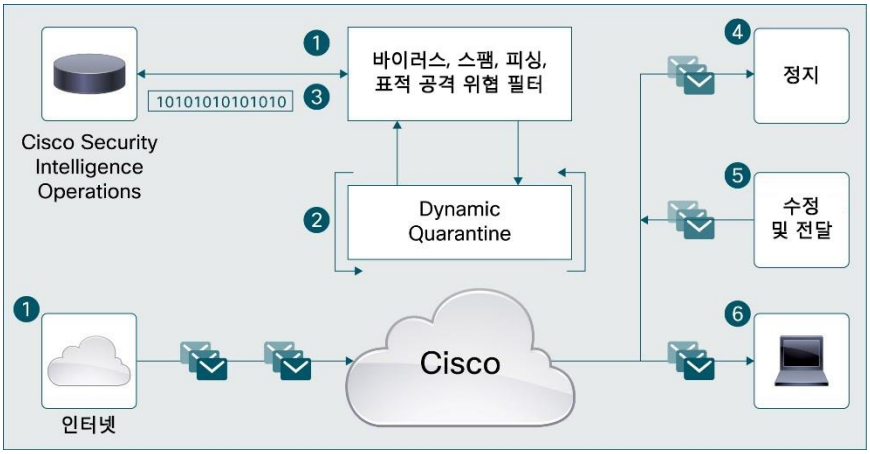
1. Outbreak Filter에서 수신 이메일을 스캔합니다. 정교한 규칙 세트에서는 이를 잠재적인 피싱 또는 표적 공격 이메일로 식별하며 어플라이언스에서 구성된 것으로 처리합니다. 기본적으로 해당 이메일이 피싱임을 나타내는 고지 문구가 이메일 텍스트 앞에 추가되며 이메일에 포함된 URL이 다시 작성됩니다.
2. 다시 작성된 URL이 포함된 이메일이 사용자의 받은 편지함에 전달됩니다.
3. 이메일을 열면 다시 작성된 이 이메일 링크에서 사용자를 공용 프록시로 보냅니다. 해당 프록시에서는 웹 페이지 콘텐츠가 인터셉트되고 Outbreak Intelligence를 사용하여 클라우드에서 실시간으로 스캔이 이루어집니다.
4. 페이지에서 악성코드가 탐지된 경우, 차단된 페이지 메시지가 사용자에게 표시되며 URL에 대한 정보는 클라우드에서 Cisco Talos로 다시 전달됩니다. 또는 사용자가 프록시를 통해 페이지를 둘러보거나 사이트로 바로 이동하도록 선택할 수 있습니다.

이러한 Outbreak Intelligence 기술은 하루에 70억 개 이상의 웹 요청을 스캔하는 Cisco의 클라우드 기반 웹 보안 솔루션을 지원하는 기능과 동일합니다. 이 기술의 경우 심층 콘텐츠 분석, 체계적인 콘텐츠 조사, 가상 스크립트 에뮬레이션을 함께 사용하여 요청된 웹 페이지에서 매우 다양한 악성코드를 스캔합니다(다음 섹션 참조).

Outbreak Filter는 Cisco WSA(Web Security Appliance) 및 Cisco CWS(Cloud Web Security)에서 제공하는 텔레메트리를 활용합니다. 그러나 고객은 Outbreak Filter를 사용하기 위해 WSA나 CWS를 보유하지 않아도 됩니다. 기존의 Virus Outbreak Filter 고객은 AsyncOS® 7.5 for Cisco Email Security 이상으로 손쉽게 업그레이드하여 새로운 Outbreak Filter를 활용할 수 있습니다.

심층 구조 보기

그림 2. Outbreak Filter를 지나는 메시지 흐름 심층 조명



1. 이메일이 조직에 수신되면 Cisco AntiSpam에서는 Cisco Talos에 의해 게시된 최신 규칙 세트 및 공격 휴리스틱을 사용하여 해당 이메일을 스캔합니다.
2. 규칙 세트에서 이메일을 잠재적인 공격으로 판단할 경우, 해당 이메일에 Dynamic Quarantine 보존 값 또는 메시지 격리 시간이 할당됩니다.
3. 이 격리 타이머가 만료되거나 구성된 최대 격리 시간에 도달하면 메시지가 격리에서 해제되고 최신 규칙 세트를 사용하여 Cisco AntiSpam 엔진에서 다시 검색됩니다.
4. 이 업데이트된 규칙은 구성된 정책에 따라 메시지를 처리해야 할 스팸으로 식별할 수 있습니다.
5. 메시지가 안전한 것으로 판단되면 원본 그대로 받은 편지함으로 전달됩니다.
6. 메시지가 잠재적인 위협으로 판단되면 이 메시지는 구성에 따라 처리된 후 사용자의 받은 편지함으로 전송되며 이러한 처리 작업에는 URL 재작성, 메시지 본문 텍스트 앞에 문구 삽입, 제목 줄 앞에 문구 삽입 등이 포함됩니다.

수정된 의심스러운 URL이 열리면 사용자는 클라우드로 리디렉션되며 URL이 확인됩니다. 확인이 완료되면 CWS의 Outbreak Intelligence를 사용하여 웹 페이지를 가져오고 실시간으로 스캔합니다. 악의적인 웹 페이지는 차단되며 페이지에 악성코드가 있음을 알리는 알림이 사용자에게 전송됩니다. 그림 3에는 샘플 알림이 나와 있습니다.

그림 3. 차단된 페이지 알림 샘플

URL 속성에 대한 세부 정보는 Cisco Talos로 다시 전달됩니다. 이 정보는 처리 과정을 거쳐 Cisco AntiSpam 업데이트에 추가되며, 이 경우 해제 대기 중인 모든 격리된 메시지가 차단됩니다.

참고: 격리된 메시지는 안티스팸 엔진을 통해 지속적으로 다시 스캔됩니다.

사용자 환경

기본적으로 사용자는 받은 편지함에서 제목 줄 앞에 문구가 들어가고 메시지 본문에는 재작성된 URL과 함께 경고 메시지가 포함된 이메일을 받게 됩니다. 사용자가 재작성된 URL을 클릭하고 브라우저에서 해당 URL을 열면 공용 웹 프록시로 연결됩니다. 웹 페이지에 악성 콘텐츠가 포함된 경우 차단 페이지가 표시됩니다. 페이지에 의심스러운 파일이 포함된 경우 파일을 다운로드할 것인지 묻는 경고 화면이 사용자에게 표시됩니다. 또한, 페이지에 악성코드가 없는 것 같지만 여전히 의심스러운 경우 사용자는 보호용 프록시를 통해 웹 사이트를 열거나 웹 사이트로 바로 이동할 수 있습니다.

사용자에게 나타나는 메시지는 항상 프록시 서버 연결을 통해 브라우저 환경에서 표시됩니다.

Outbreak Filter의 구성 요소

Outbreak Filter는 Cisco AntiSpam 규칙 세트 및 Cisco Talos의 정교한 규칙 세트, Cisco AntiSpam URL 재작성, Cisco Email Security Appliance 표적 공격 휴리스틱 및 악성 웹 콘텐츠를 차단하는 CWS 기술로 구성되어 있습니다.

Cisco Talos 규칙 세트는 차단 또는 격리되어야 하는 수신 이메일을 일반적인 스팸 또는 공격 메시지로 필터링하는 데 사용되는 표준 Cisco AntiSpam 업데이트입니다. 이러한 규칙 세트에는 이전에 Outbreak Filter에서 차단된 URL의 피드백이 포함되며 해당 규칙 세트는 바이러스 침투 격리에서 해제되는 메시지를 다시 스캔하는 데 사용됩니다.

표적 공격 휴리스틱의 경우 SenderBase에서 제공된 인텔리전스를 보안 어플라이언스 및 알려진 공격에서 파생된 콘텐츠와 결합합니다. 이 인텔리전스는 URL, 헤더, 메시지 본문과 같은 각 메시지의 다양한 요소를 평가하여 메시지 내의 위협을 식별하는 데 사용됩니다. 이러한 휴리스틱은 다른 Outbreak Filter 규칙과 연동하여 제공된 메시지가 표적 공격인지를 확인합니다.

URL 재작성은 Cisco AntiSpam 엔진에서 수행하는 작업입니다. 공용 인터넷상의 프록시용 URL, 프록시 요청을 인증하는 데 사용되는 해시 및 원본 URL을 포함하도록 URL이 다시 작성됩니다. 예를 들어, URL

http://www.youtube.com/watch?v=FCARADb9asE가 이메일에서 재작성된 경우 http://secure-web.cisco.com/auth=11vKpmpe8R7CLj6iG0cbr40VY5yOTR&url=http%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DFCARADb9asE와 같은 형태로 표시될 수 있습니다. 이렇게 되면 요청은 CWS에서 스캔할 웹 콘텐츠용 프록시를 통해 이동합니다.

심층 콘텐츠 분석은 Outbreak Intelligence의 세 가지 프로세스 중 첫 번째로, 악성 웹 콘텐츠를 찾고 차단합니다. 콘텐츠에 악의적인 목적이 있는지 검사합니다. 이러한 작업은 인공 지능 학습을 통해 정확성이 유지된 알려진 "정상" 통계 모델과 비교하는 방식으로 수행됩니다. 예를 들어, 애니메이션 GIF에 프레임이 1개밖에 없는지, 이미지 파일에 실행 코드 또는 기타 비정상적인 콘텐츠가 포함되어 있는지 등을 비교합니다.

체계적인 콘텐츠 조사 프로세스에서는 콘텐츠의 구조를 검사하여 잠재 위험의 징후를 다시 확인합니다. 예를 들어, Cisco Talos에서 분석한 콘텐츠를 토대로 새로운 난독 실행 파일이 악성 파일일 가능성이 95% 이상인 것으로 확인될 수 있습니다. 이러한 작업은 여러 가지 전용 스캔 엔진 또는 scanlet(예: 평판 scanlet 및 Flash, Java, PDF, 아카이브, 실행 파일, 파일 이상 현상 등에 사용되는 scanlet)을 사용하여 페이지 콘텐츠를 스캔하는 방식으로 수행됩니다. 이러한 scanlet은 높은 성능을 유지하면서 실행됩니다.

스크립트와 같은 동적 콘텐츠에 특히 중요한 세 번째 구성 요소는 가상 스크립트 에뮬레이션입니다. 클라우드 인프라 내에서 스크립트를 실행하면 숨겨진 리디렉션, 컴퓨터에서 사용자 설정을 편집하려고 시도하는 "드라이브바이" 다운로드 등의 악의적인 움직임을 모니터링할 수 있습니다. 악의적인 움직임이 탐지되면 해당 스크립트는 최종 사용자에게 전달되지 않고 차단됩니다.

Outbreak Intelligence의 이러한 웹 구성 요소는 제로데이 악성코드를 정확하게 식별하고 차단하는 것으로 검증되었으며 악성코드 차단율은 25% 이상에 달합니다.

Outbreak Filter에서는 무엇을 탐지합니까?

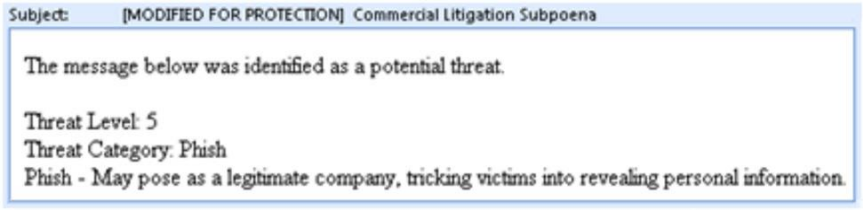
Cisco Outbreak Filter는 악성코드, 피싱, 사기, 바이러스 감염 이메일이라는 네 가지 카테고리로 구성되며 20개 이상의 다양한 사기 유형을 탐지합니다. 다음 목록에는 Outbreak Filter에서 탐지할 수 있는 몇 가지 공격 유형이 나와 있습니다.

- 피싱
- 자선단체 빙자 스팸
- 해외 도난 사기
- 세미나
- 상속
- 금융 URL
- 위조 거래
- 은행 이체
- 위조 자기앞수표
- 자금 운반책
- 온라인 벼룩시장(Craigslist)
- 대출
- 금융 관련 전화
- 등 다수

이 목록은 유동적으로 변경되어 공격자가 사용자로 하여금 URL 및/또는 첨부 파일을 열어보도록 유도하기 위해 사용하는 최신 수법 동향에 관한 정보를 지속적으로 제공합니다.

Outbreak Filter의 구성 설정을 사용하면 시스템에서 본문 텍스트 위에 이메일의 특성에 대한 정보를 추가하고 제목 줄에 메시지를 입력할 수 있습니다(그림 4).

그림 4. 제목 수정 및 본문 텍스트



맞춤형 알림

조직의 정책에 따라 최종 사용자에게 특정 메시지를 표시해야 하는 경우, 고지 사항 템플릿 유형의 텍스트 리소스를 통해 맞춤형 텍스트 메시지를 구성할 수 있습니다. 이러한 텍스트 리소스에서는 조직의 정책에서 요구하는 맞춤형 텍스트와 함께 기존의 알림 변수 또는 다음과 같은 네 가지 새로운 변수를 사용할 수 있습니다.

- $threat_category
- $threat_type
- $threat_description
- $threat_level

텍스트 메시지가 구성되면 Preview Text(텍스트 미리 보기) 옵션을 사용하여 구성된 고지 문구가 최종 사용자에게 어떻게 표시되는지 예를 볼 수 있습니다.

트러블슈팅

Cisco Outbreak Filter를 사용하면 문제를 간단하게 해결할 수 있습니다. 필터를 통해 message_logs 로그 서브스크립션에 행이 추가됩니다. 이러한 로그는 CLI를 통해 액세스하거나, GUI에서 다운로드하거나, 어플라이언스에서 회사 로그 시스템으로 내보낼 수 있습니다.

다음은 위협으로 간주되는 메시지의 로그 입력에 대한 예입니다.

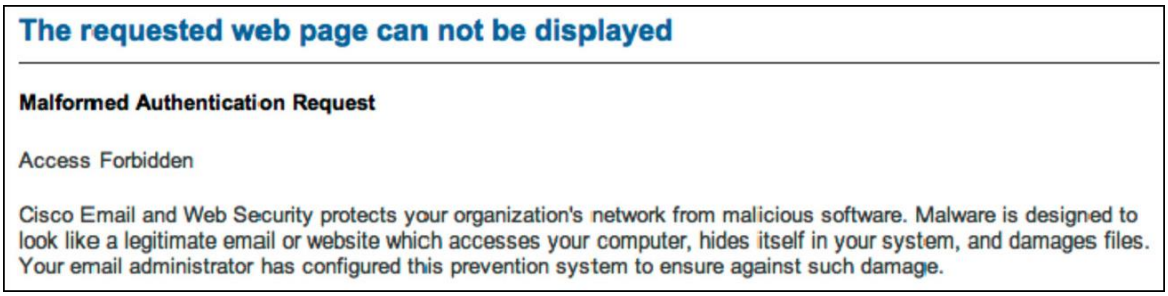
```
Wed Mar 9 17:43:51 2011 Info: New SMTP ICID 1720507 interface Management (10.0.0.42) address
67.215.21.16 reverse dns host www.wyodino.org verified yes
Wed Mar 9 17:43:51 2011 Info: ICID 1720507 ACCEPT SG SUSPECTLIST match sbrs[-2.0:0.0] SBRS
-1.0
Wed Mar 9 17:43:51 2011 Info: Start MID 487757 ICID 1720507
Wed Mar 9 17:43:51 2011 Info: MID 487757 ICID 1720507 From: <KarmelaMeir@aol.ca>
Wed Mar 9 17:43:51 2011 Info: MID 487757 ICID 1720507 RID 0 To: <jdoe@customer.com>
Wed Mar 9 17:43:51 2011 Info: MID 487757 Message-ID '<058fb89e-40612-1e4e1551531134@user-
pc>'
Wed Mar 9 17:43:51 2011 Info: MID 487757 Subject 'Payment Confirmation - eBay Item number :
390294669929'
Wed Mar 9 17:43:51 2011 Info: MID 487757 ready 1318 bytes from <KarmelaMeir@aol.ca>
Wed Mar 9 17:43:51 2011 Info: MID 487757 matched all recipients for per-recipient policy strong in the
inbound table
Wed Mar 9 17:43:51 2011 Info: ICID 1720507 close
Wed Mar 9 17:43:51 2011 Info: MID 487757 using engine: CASE spam negative
Wed Mar 9 17:43:51 2011 Info: MID 487757 interim AV verdict using Sophos CLEAN
Wed Mar 9 17:43:51 2011 Info: MID 487757 antivirus negative
Wed Mar 9 17:43:51 2011 Info: MID 487757 Threat Level=2 Category=Phish Type=Financial Url
Wed Mar 9 17:43:51 2011 Info: MID 487757 queued for delivery
Wed Mar 9 17:43:51 2011 Info: New SMTP DCID 89502 interface 10.0.0.42 address 10.0.0.119 port 25
Wed Mar 9 17:43:52 2011 Info: Delivery start DCID 89502 MID 487757 to RID [0]
Wed Mar 9 17:43:52 2011 Info: Message done DCID 89502 MID 487757 to RID [0]
Wed Mar 9 17:43:52 2011 Info: MID 487757 RID [0] Response '2.0.0 p2A1iFIH017778 Message
accepted for delivery'
Wed Mar 9 17:43:52 2011 Info: Message finished MID 487757 done
```

Cisco Outbreak Filter에서는 안티스팸 또는 메시지가 존재할 수 있는 DLP 정책 격리와 구분되는 고유한 격리 기능을 사용합니다. 오탐으로 간주된 메시지는 메시지 사본을 Cisco로 전송하여 검사하는 옵션을 통해 수동으로 격리에서 해제할 수 있습니다.

사용자나 관리자는 이메일을 outbreaks@ironport.com 또는 phish@access.ironport.com에 첨부 파일로 전달하고, 오탐을 ham@access.ironport.com에 첨부 파일로 전달하여 누락된 바이러스 침투 현상을 손쉽게 보고할 수 있습니다. Entourage 및 Microsoft Outlook에서는 헤더를 그대로 유지한 채로 이메일을 전달하지 않습니다. Microsoft Outlook 사용자의 경우, 특정 목적을 위해 메시지를 올바르게 전달하려면 Cisco에서 제공하는 Cisco Email Security 플러그인 소프트웨어를 설치해야 합니다.

사용자가 URL을 통해 다른 웹 사이트의 프록시를 시도하고 사용하려고 할 경우 액세스에 실패하게 됩니다. 재작성된 URL에는 해당 URL을 유효한 URL로 식별하는 해시가 포함되며, URL이 변경될 경우 사용자는 프록시에서 오류 메시지를 받게 됩니다(그림 5).

그림 5. 변경된 URL 오류 메시지



Cisco Outbreak Filter에서는 Cisco Email/Web Security 기술의 가장 우수한 기능을 결합하여 소규모 표적 공격에 대해 뛰어난 보호를 제공합니다.

자세한 내용은 www.cisco.com/go/emailsecurity를 참고하거나 해당 지역 Cisco 영업 담당자에게 문의하십시오.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C11-684611-01 05/15