Cisco Security Everywhere v1.1

최종 업데이트: 2017년 2월 13일

데모 정보

Cisco Security Everywhere 데모는 사용자 및 보안 분석가가 WSA, ESA, ISE, Umbrella, Firepower 등을 비롯한 Cisco 보안 제품을 사용하여 타기팅 악성코드 공격을 퇴치하는 과정의 공격 전, 공격 중, 공격 후 단계를 살펴봅니다. 이 데모에서는 Cisco 보안 제품이 통합된 방식의 상호작용을 통해 멀티 레이어 'Cisco on Cisco' 보안 솔루션을 제공하여 지능형 악성코드 위협으로부터 네트워크를 보호하는 기능을 살펴볼 수 있습니다. 공격 전 단계에서 Security Everywhere는 Cisco 보안 솔루션이 함께 작동하면서 공격을 예측 및 방지하는 여러 제품을 통해 일관된 네트워크 보호 상태를 유지하는 방법을 보여 줍니다. 공격 중 단계에서 Security Everywhere는 제품이 통합되어 발생하는 위협을 파악, 격퇴, 격리하는 방법을 보여 줍니다. 마지막으로, Security Everywhere는 공격이 발생한 후 네트워크 분석가가 해당 공격을 연계, 분석, 파악하고 네트워크 및 사용자 기능을 최대한 빨리 정상적인 상태로 되돌려놓을 수 있도록 제공되는 툴을 보여 줍니다.

이 데모에서는 출장이 잦고 회사 노트북 컴퓨터를 사용하여 웹, 이메일, 네트워크에 액세스하는 일반 회사원 Bob의 사례를 살펴봅니다. 이러한 일상적인 비즈니스 업무를 수행하는 동안 위협이 언제라도 공격할 준비가 되어 있음을 시연하여 Cisco 보안 솔루션이 네트워크 인프라의 현재 상태에서 어떤 방식으로 이미 구축되어 있는지 확인합니다.

새로운 기능

- Cisco Identity Service Engine이 버전 2.2로 업그레이드됨
- Cisco Web Security Appliance가 버전 10.1로 업그레이드됨
- Cisco Email Security Appliance가 버전 10.0.1로 업그레이드됨
- Cisco Content Security Management Appliance가 버전 10.1로 업그레이드됨
- Cisco Firepower Management Center가 버전 6.2로 업그레이드됨
- Cisco Next Generation Firewall이 버전 6.2로 업그레이드됨

제한 사항

Stealthwatch 제품은 현재 Security Everywhere 데모에 포함되어 있지 않습니다.

필요조건

다음 표에는 사전 설정된 데모의 필요조건이 요약되어 있습니다.

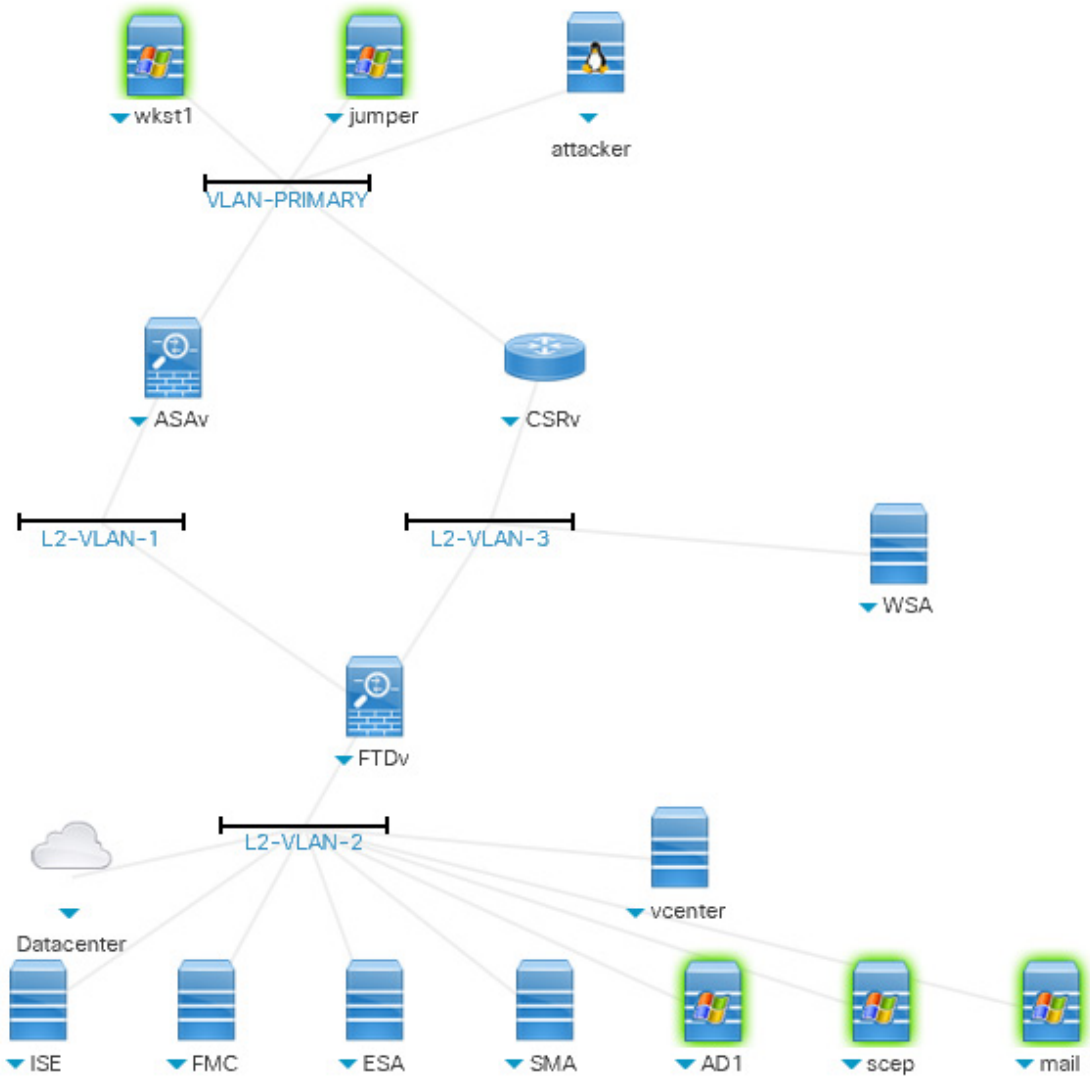
표 1. 필요조건

필수	옵션
• Cisco AnyConnect®가 설치된 노트북 컴퓨터	• 옵션 필요조건은 없음

토폴로지

이 콘텐츠에는 데모 시나리오의 솔루션 기능을 설명하기 위해 사전 설정된 사용자 및 구성 요소가 포함되어 있습니다. 대부분의 구성 요소는 사전 정의된 관리자 계정으로 충분히 설정할 수 있습니다. 활성 세션의 **Topology(토폴로지)** 메뉴 또는 활용할 시나리오 단계에서 구성 요소 아이콘을 클릭하면 해당 구성 요소에 액세스하는 데 사용할 IP 주소 및 사용자 계정 자격 증명을 볼 수 있습니다.

그림 1. 토폴로지



솔루션 정보

오늘날 공격자와 위협은 그 어느 때보다 더욱 끈질기고 지능적입니다. 수많은 종류의 위협으로부터 보호하려면 매우 철저하고 면밀하게 계획된 레이어 방식의 보안 모델이 필요합니다. 문제는 보안 솔루션이 공격 전, 공격 중, 공격 후 단계에서 모든 항목을 처리하는 방식입니다. 공격 전 범위를 이루는 이러한 세 가지 단계가 모두 중요합니다. 이 데모에서 공격자는 먼저 간단한 피싱 공격을 실행합니다. 데모가 진행됨에 따라 공격자와 공격 방법이 점점 더 복잡해지며, Cisco 보안 솔루션이 과정의 각 단계에서 네트워크를 어떻게 보호하는지 확인할 수 있습니다.

아래에서는 이 데모에서 함께 작동하여 공격자를 격퇴하는 몇 가지 Cisco 솔루션에 대해 자세히 설명합니다.

표 2. Cisco 솔루션

솔루션	설명
Cisco® Firepower Management Center	Cisco 보안 솔루션의 핵심입니다. FMC에서는 Cisco 구축을 위한 중앙 집중식 관리 지점 및 이벤트 데이터베이스를 제공합니다. 또한 FMC에서는 침입, 파일, 악성코드, 검색, 연결, 성능 데이터를 집계 및 상호 연결하고, 보안 침해 지표를 사용하여 이벤트가 특정 호스트와 태깅 호스트에 미치는 영향을 평가합니다. 이 기능을 활용하면 보유 디바이스에서 다른 디바이스와 관련하여 보고하는 정보를 모니터링하고 네트워크에서 발생하는 전반적인 활동을 평가 및 제어할 수 있습니다. Cisco Firepower Management Center는 공격 전, 공격 중, 공격 후의 공격 전 범위를 확인하여 문제를 분석하는 기능을 제공합니다.
Cisco® Identity Services Engine(ISE)	다음 기능을 통해 네트워크에 있는 모든 엔드포인트의 온보딩, 프로비저닝, 보호를 간소화합니다. • 네트워크에 액세스하고 이를 사용하는 사용자와 엔드포인트를 더 정확하게 식별, 분류 및 모니터하도록 가시성 향상 • 네트워크와 네트워크 리소스에 대한 사용자 액세스를 제어하기 위해 중앙 집중식의 역할 기반 액세스 보안 정책 제공 • 연결된 사용자와 디바이스에 대한 자세한 상황 데이터를 수집하고 다른 통합 보안 및 네트워크 소프트웨어 플랫폼과 공유하여 위협에 대한 응답 시간 단축 • Cisco 보안 파트너와 양방향 정보 공유 및 위협 억제 개방 • Cisco Rapid Threat Containment 솔루션과의 통합을 통해 관찰, 치료 또는 제거하기 위해 자동으로 위협 억제 • 쉽게 맞춤 설정되는 게스트 및 BYOD(Bring-Your-Own-Device) 솔루션 포털을 통해 조직의 브랜드 보호
Cisco® AnyConnect	데스크톱 및 모바일 OS 플랫폼을 비롯하여 오늘날의 거의 모든 주요 엔터프라이즈 모빌리티 플랫폼과 호환되는 통합 엔드포인트 소프트웨어 클라이언트입니다. 기반이 되는 VPN 기술에 구축되고 엔드포인트 컴퓨터 디바이스에서 실행되는 AnyConnect Secure Mobility는 방화벽 뒤에 있는 네트워크 패브릭의 보안을 활성화하고, 회사 방화벽 외부에서 액세스하는 모바일 사용자에게 전례 없는 수준의 보안 및 기업 정책을 적용합니다.

솔루션	설명
Cisco® Umbrella	디바이스가 현장에 있든, VPN을 통해 연결되어 있든, 현지 커피숍의 공용 네트워크를 사용하든 상관없이 공격 및 악의적이거나 의심스러운 콘텐츠로부터 디바이스를 보호합니다. DNS 레이어에서 보안을 제공하여 악성코드에 의한 시스템 손상과 봇넷 또는 피싱을 통한 데이터 유출을 차단합니다. 이 솔루션은 디바이스 및 디바이스에서 실행 중인, 요청을 생성하는 애플리케이션과 상관없이 위협 차단 및 가시성을 제공합니다. 이 밖에도 성능에 전혀 영향을 주지 않고, 100% 업타임을 보장하며, 몇 분 만에 구축 가능합니다.
Cisco® Rapid Threat Containment	운영 효율성을 향상하고 위협을 빠르게 탐지, 분석 및 억제하는 포괄적이며 긴밀하게 통합된 벤더 지원 솔루션입니다. 구성: • 네트워크 및 엔드포인트 센서를 사용하여 네트워크 전체에서 위협을 식별하는 우수한 자동 악성코드 탐지 • 위협 및 보안 침해 지표(IoC)에 대한 자동화된 분석 및 자격 부여로, 공격을 빠르게 이해하고 억제하기 위한 상황 가시성을 IT 보안 담당자에게 제공 • 위협 정보를 지속적으로 업데이트하여 지능형 악성코드에 대한 방어 향상 • 감염된 엔드포인트가 치료될 때까지 퍼베이시브 네트워크 시행 기능을 통해 즉시 억제 또는 격리 • 이미 구축된 Cisco 네트워킹 디바이스와의 상호운용성
Cisco® AMP for Endpoints	특정 시점 방어만으로 충분하지 않은 오늘날의 환경에 지속적인 보호를 제공합니다. 단순한 이벤트 스냅샷 이상의 Retrospection 같은 기능을 제공하여 장기간에 걸쳐 행동을 분석합니다. 이는 파일에만 국한되지 않으며 프로세스, 커뮤니케이션, 텔레메트리 데이터도 포함하므로 이벤트가 발생한 시점으로 시간을 되돌려 악성코드 감염 소스와 이동을 정확하게 확인할 수 있습니다. 또한, 원격 노트북 컴퓨터 또는 시스템에서 확인된 새로운 위협은 AMP를 통해 즉시 전달되어 모든 네트워크 및 노트북 컴퓨터 전반에 걸쳐 보호를 시행합니다.
Cisco® AMP Threat Grid	최신 위협 정보와 실시간 행동 분석을 하나의 통합된 솔루션에 결합하여 정적 및 동적 악성코드 분석을 둘 다 제공합니다. 클라우드 기반 또는 온프레미스(구내 장비) 솔루션으로 제공되는 AMP Threat Grid는 악성코드의 활동 또는 목적, 위협의 규모 및 방어 방법을 파악할 수 있도록 지원합니다.
Cisco® Web Security Appliance	고도로 보안된 일체형(all-in-one) 웹 게이트웨이로서 강력한 보호, 완벽한 제어, 투자 가치라는 이점을 제공합니다. WSA는 Cisco Talos Security Intelligence and Research Group(업계 최대의 실시간 위협 인텔리전스 수집 데이터)과 업계 최고의 Website Reputation Analysis가 결합된 멀티 레이어 보안을 Advanced Malware Protection, 샌드박싱 및 지속적인 분석, 애플리케이션 가시성, 데이터 유출 방지 기능과 통합합니다.
Cisco® TrustSec	오늘날 대부분의 Cisco 네트워크 디바이스에는 마이크로 세그멘테이션 기술이 포함되고 제공되므로 비교적 적은 비용으로 이 솔루션을 사용할 수 있습니다. 이 솔루션은 ISE(Identity Services Engine)에서 관리되는 소프트웨어 중심 정책을 따르므로 지사, 캠퍼스, 데이터 센터 네트워크 전반에 걸쳐 BYOD, 게스트, 조명 시스템, 비디오 감시 카메라 같은 디바이스 분류를 각기 다른 세그먼트로

솔루션	설명
	구분하는 정확한 규칙을 쉽게 만들 수 있습니다. ICMP 같은 마이크로 세그먼트에 있는 피어 간의 측면 이동 및 프로토콜을 제어할 수 있으므로, NaaE(Network as an Enforcer)를 사용하여 해커 및 악성코드가 타겟을 검색하고 장악하는 것을 효과적으로 차단할 수 있습니다. 네트워크 내부의 TrustSec 보안은 경계 보호를 제공하는 차세대 방화벽을 보완하며, 방화벽 규칙 관리를 대폭 간소화하여 방화벽 운영도 향상합니다.
Cisco® Email Security Appliance	업계 최초의 검증된 제로아워 안티바이러스 솔루션입니다. 이 솔루션은 중요한 아웃바운드 이메일을 제어하고 암호화할 수 있는 동급 최고의 기능을 제공합니다. 그와 동시에, 단일한 어플라이언스에 구축된 계층형 방어로 들어오는 공격을 신속하게 차단합니다. 피싱 및 스노우슈(snowshoe) 스팸 공격에 대한 상황 분석, 뛰어난 스팸 차단율(99% 이상), 파일 평판, 동적 분석(샌드박싱), Cisco AMP Threat Grid를 통한 회귀적 보안, 그레이메일 관리 및 웹 상호작용 추적 기능이 포함됩니다.

시작하기

다음 단계에 따라 세션을 예약하고 프레젠테이션 환경을 설정하시기 바랍니다.

1. dCloud 세션을 시작합니다. [방법 보기]

> 참고: **이 데모는 세션이 활성화될 때까지 최대** 30분**이 소요됩니다.**

2. 최상의 성능을 유지하려면 호스트 URL을 노트북 컴퓨터의 **Cisco AnyConnect VPN**에 연결[방법 보기]합니다.
3. 최상의 성능을 유지하려면 **Cisco AnyConnect VPN**[방법 보기] 및 **노트북 컴퓨터의 로컬 RDP 클라이언트**[방법 보기]를 사용하여 **Jumper**에 연결합니다.
    - Jumper: **198.18.133.37**, 사용자 이름: **DCLOUD\Administrator**, 비밀번호: **C1sco12345**

> **참고:** Cisco dCloud Remote Desktop 클라이언트[방법 보기]를 사용하여 Jumper에 연결할 수도 있습니다. dCloud Remote Desktop 클라이언트는 최소한의 상호작용만으로 활성 세션에 액세스하기 때문에 데모에 가장 효과적입니다. 단, dcloud RDP 활용 시 연결 및 성능 문제를 겪는 사용자가 많습니다.

> **참고:** 모든 시나리오에서 Jumper PC 및 WKST1(Bob의 PC)에 동시에 로그인해야 합니다. 이 작업을 위한 가장 쉬운 방법은 위에서 설명한 대로 dCloud 데모에 VPN을 사용하고 로컬 RDP 클라이언트를 사용하여 Jumper PC(198.18.133.37)에 연결하는 것입니다. Jumper PC의 바탕화면에는 Jumper PC에서 WKST1에 RDP를 수행하는 데 사용할 수 있는 RDP 바로가기가 있습니다. 이제부터 Jumper와 WKST1(Bob의 PC) 간을 쉽게 왔다갔다할 수 있습니다.

> **참고:** 시나리오 1~5는 서로 완전히 별개로 실행하거나 순서대로 실행할 수 있습니다. 데모에 익숙해지면 특정 기술을 시연하려는 경우 이러한 시나리오 중 하나로 바로 건너뛸 수 있습니다. 5가지 시나리오에서 모두, 위에서 설명한 대로 Jumper PC와 WKST1(Bob의 PC) 둘 다에 연결해야 합니다. 시나리오 1의 첫 번째 부분에서는 WKST1 "관리자" 사용자가 시작하기 위해 VPN을 통해 데모 기업 네트워크에 로그인할 필요가 없으나, 시나리오 1의 후반부 및 시나리오 2~5에서는 모두 WKST1의 "관리자" 사용자가 VPN에 로그인해야 사용자가 이메일을 검색할 수 있습니다. 따라서 시나리오 2~5로 바로 건너뛸 경우 WKST1에 로그인한 관리자 사용자가 데모에서 Cisco AnyConnect를 사용하여 VPN에 로그인했는지 확인합니다. 시나리오 6은 시나리오 5에서 발생한 내용을 분석 및 정리한 것입니다. 따라서 시나리오 6은 시나리오 5에 종속되며, 개별적으로 또는 시나리오 5를 완료하지 않고 실행할 수 없습니다.

시나리오 1. 공격 전: Cisco Umbrella 데모

Bob의 회사에서는 기본적인 악성코드 피싱 공격을 완화하는 데 도움이 되도록 Cisco Umbrella를 구축하기로 결정했습니다. 이제 본사의 내부 DNS 서버는 모든 재귀적 DNS 조회를 Umbrella에 전달합니다. Bob과 같은 모바일 작업자를 보호하기 위해 회사에서는 **AnyConnect Umbrella Roaming** 모듈을 구축했습니다. AnyConnect Umbrella Roaming 모듈은 전체 Umbrella 기능을 기존 **Cisco AnyConnect Secure Mobility Client**에 원활하게 통합하는 AnyConnect 모듈입니다. 이는 Bob이 기업 네트워크를 사용 중일 때, VPN을 통해 기업 네트워크에 연결할 때 또는 기업 네트워크를 전혀 사용하지 않을 때도 악의적인 인터넷 도메인에서 유입되는 악성코드 위협이 차단된다는 것을 의미합니다.

Bob은 이번 주에 영업 컨퍼런스에 참석했으며 호텔 객실에서 업무를 보고 있습니다. Bob은 현재 인터넷에 막 연결했으며 기업 네트워크에는 다시 연결하지 않은 상태입니다. 실제 업무를 위해 연결하기 전에, Bob은 공항에서 비행기에 탑승하기 전 노트북 컴퓨터에서 흥미로운 라스베이거스 여행 정보가 담긴 이메일을 받은 것을 기억합니다. Bob은 탑승 직전에 이메일을 노트북 컴퓨터에 다운로드했으나 살펴볼 시간이 없었습니다.

공격자는 Bob의 PC를 장악하기 위해 가장 단순한 시도, 즉 신뢰할 수 있는 것처럼 보이는 링크를 Bob이 클릭하도록 유도하는 피싱 공격으로 시작합니다. Bob이 해당 이메일의 링크에 연결할 경우, 이 링크는 실제로 공격자가 Bob이 사용 중인 브라우저의 취약점을 악용 및 익스플로잇하여 궁극적으로 Bob의 머신을 장악하는 데 이용하는 웹사이트로 연결됩니다. 사용자가 기업 네트워크를 사용하지 않는 경우와 기업 네트워크를 사용 중인 경우 둘 다에서 Umbrella가 어떤 방식으로 이러한 종류의 공격을 완화할 수 있는지 살펴보겠습니다.

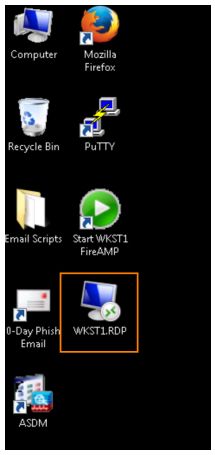
이 데모에서 Jumper PC는 중앙 연결 허브입니다. Jumper PC는 Bob의 PC(WKST1)에 액세스하는 동시에 다양한 Cisco 보안 제품에도 액세스할 수 있습니다. 이제 Jumper PC에서 Bob의 PC에 연결하여 라스베이거스행 휴가로 위장한 피싱 공격의 전모를 알아보겠습니다.

단계

1. Jumper 바탕화면에서 WKST1.RDP 아이콘을 더블 클릭하여 Bob의 PC에 연결합니다.

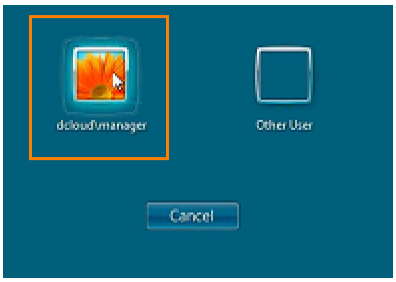
> **참고:** 또는 하나는 Jumper 세션, 다른 하나는 WKST1 세션인 두 개의 RDP 세션을 실행할 수 있습니다. 그러나 대부분의 사용자는 RDP 바로가기를 사용하여 Jumper 머신을 통해 WKST1에 연결하는 방법이 더 쉽다고 생각합니다.

그림 2. WKST1_RDP



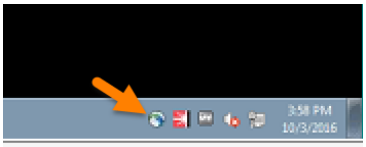
2. dCloud/manager를 클릭하고 비밀번호 **C1sco12345**로 로그인합니다.

그림 3. dCloud/manager



3. 로그인한 후 워크스테이션의 애플리케이션 트레이에서 AnyConnect 아이콘을 클릭합니다.

그림 4. AnyConnect 아이콘



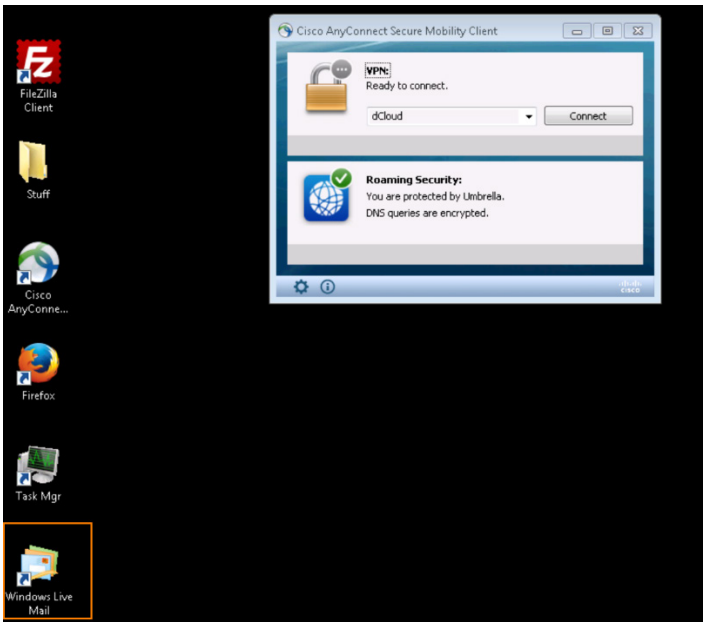
4. AnyConnect 세부사항 창에는 **Bob이 VPN에 연결되어 있지 않으며**, 해당 Umbrella Roaming Client가 활성 상태라고 표시됩니다.

> **참고:** Cisco AnyConnect Umbrella Module은 PC가 VPN을 통해 기업 네트워크에 다시 연결된 경우*뿐 아니라* 연결되지 않은 경우에도 해당 PC를 보호합니다. 이 시나리오에서 Bob은 아직 기업 네트워크에 다시 연결하지 않았으나 Umbrella를 통해 완전히 보호되고 있습니다.

그림 5. AnyConnect 세부사항

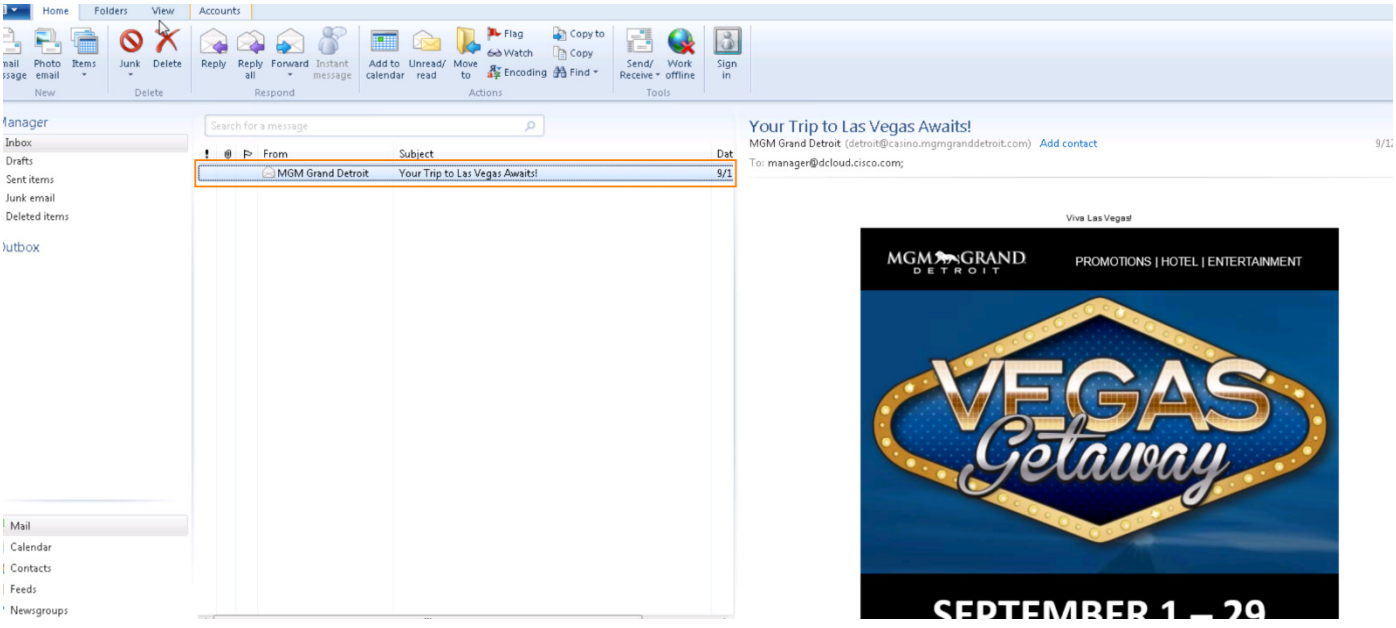
5. 바탕화면에서 Windows Live Mail 아이콘을 더블 클릭하여 Bob의 이메일을 엽니다.

그림 6. Windows Mail Live 바로가기



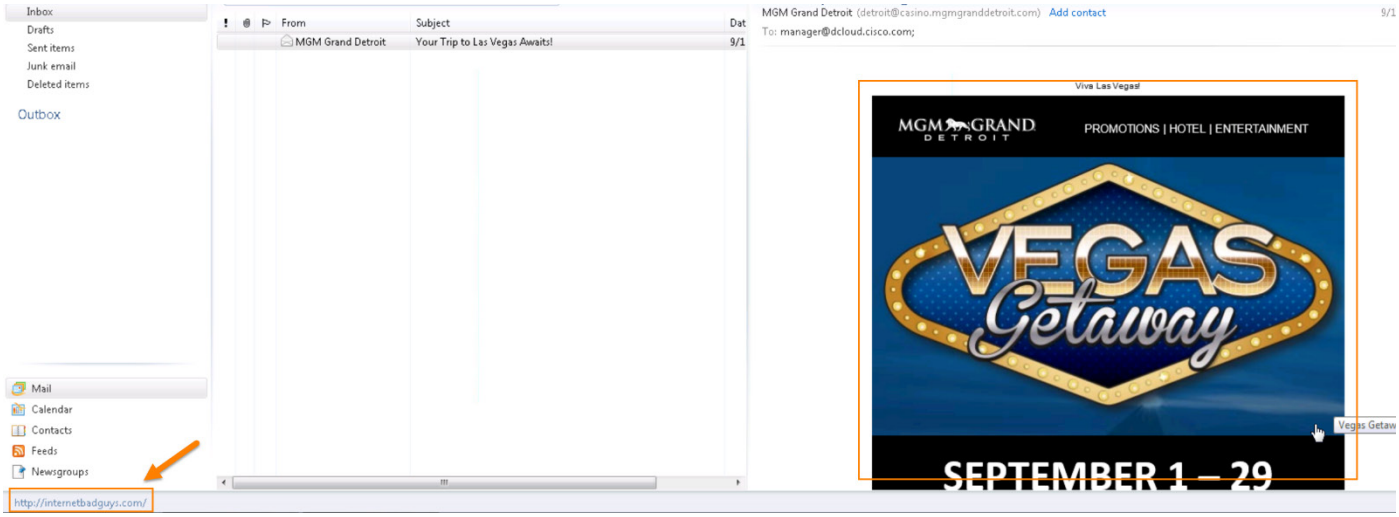
6. Bob의 노트북 컴퓨터는 네트워크에 연결되어 있지 않지만, 이전에 받은 라스베이거스행 휴가 이메일 광고 메시지가 Bob을 기다리고 있습니다. 이메일을 클릭하여 엽니다.

그림 7. Bob의 받은 편지함



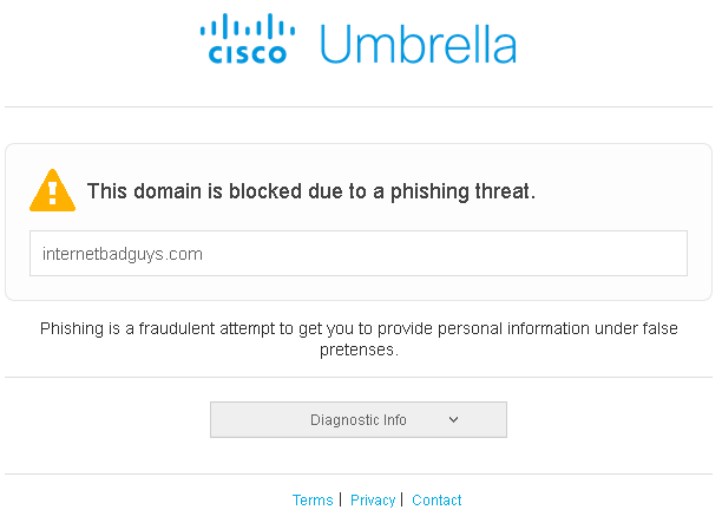
7. 광고 웹사이트로 연결되는 링크인 Vegas Getaway 이미지를 마우스 커서로 가리킵니다. URL 링크가 http://internetbadguys.com으로 확인되며, 이는 실제로 악성 웹사이트로 연결되는 링크입니다.

그림 8. Internetbadguys.com 발원지



8. Vegas Getaway 링크를 클릭하여 사이트를 열고 광고 세부사항을 확인합니다. Bob은 기업 네트워크에 연결되어 있지 않지만, Umbrella Roaming Client에서 internetbadguys.com 사이트를 확인하고 이 악성 사이트에 대한 액세스를 차단했습니다.

그림 9. Umbrella 악성 사이트 차단



9. Umbrella 경고를 닫고 메일 창을 최소화합니다.

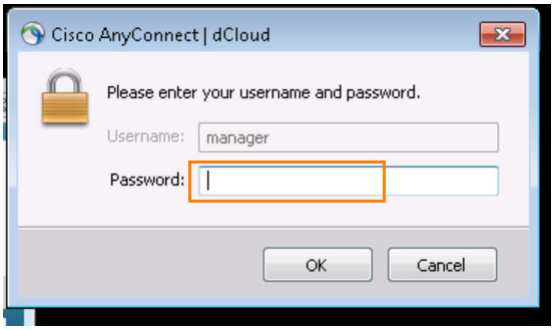
10. Bob이 VPN을 통해 기업 네트워크에 연결하기 전에도 이메일을 열 때 보호 기능이 적용되었습니다. 그다음, Bob은 기업 네트워크에 연결하여 어떤 새 이메일이 수신되었는지 확인합니다. 워크스테이션 메뉴 트레이에서 AnyConnect 아이콘을 클릭하고 이번에는 Connect(연결)를 클릭합니다.

그림 10. AnyConnect VPN 연결

11. 비밀번호 **C1sco12345**를 사용하여 AnyConnect에 관리자로 로그인합니다.

> **참고:** VPN은 디지털 인증서와 사용자 이름/비밀번호를 둘 다 활용하는, 보다 안전한 2단계 인증으로 구성되었습니다. 여기서는 Bob의 머신에 있는 디지털 인증서를 사용하여 Bob을 인증했습니다. 그런 다음 디지털 인증서에서 Bob의 사용자 이름(manager)을 읽고 자동 입했습니다. Bob이 기업 VPN에 로그인하려면 두 번째 형태의 인증인 비밀번호를 입력해야 합니다.

그림 11. AnyConnect 로그인

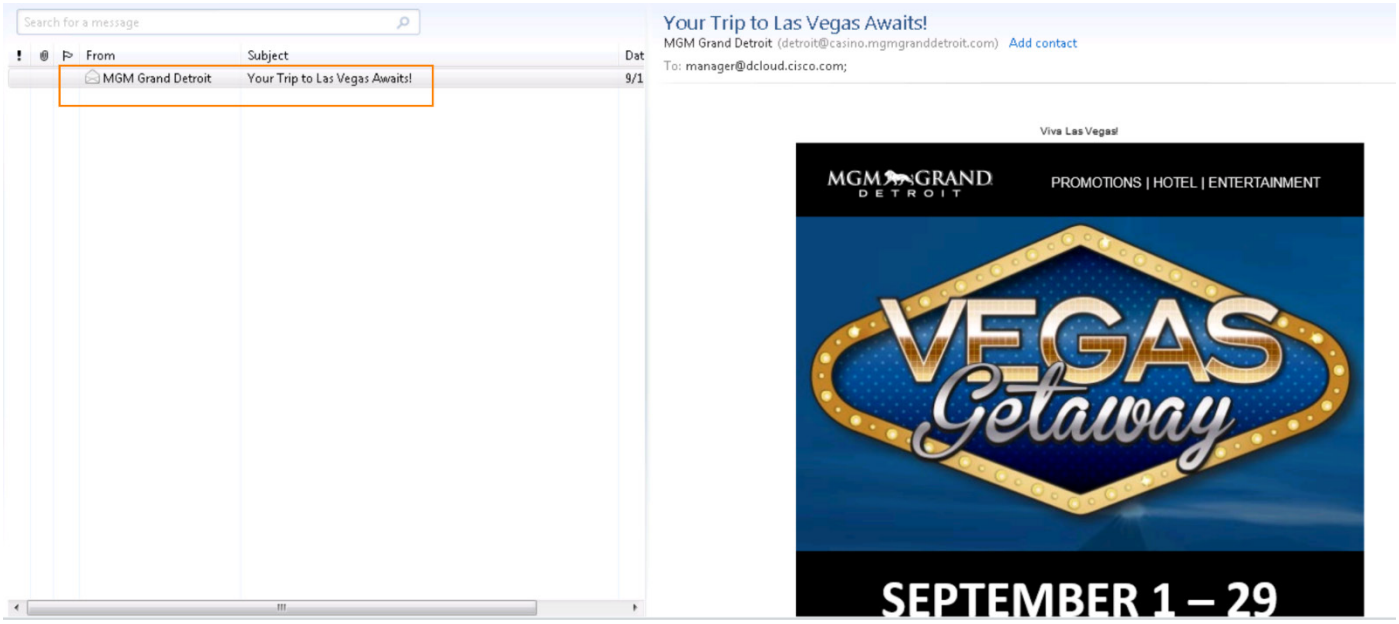


12. 이제 메뉴 트레이의 AnyConnect 아이콘에 자물쇠가 추가되어 기업 네트워크에 안전하게 로그인되었음을 알립니다.

그림 12. AnyConnect Secure 로그인

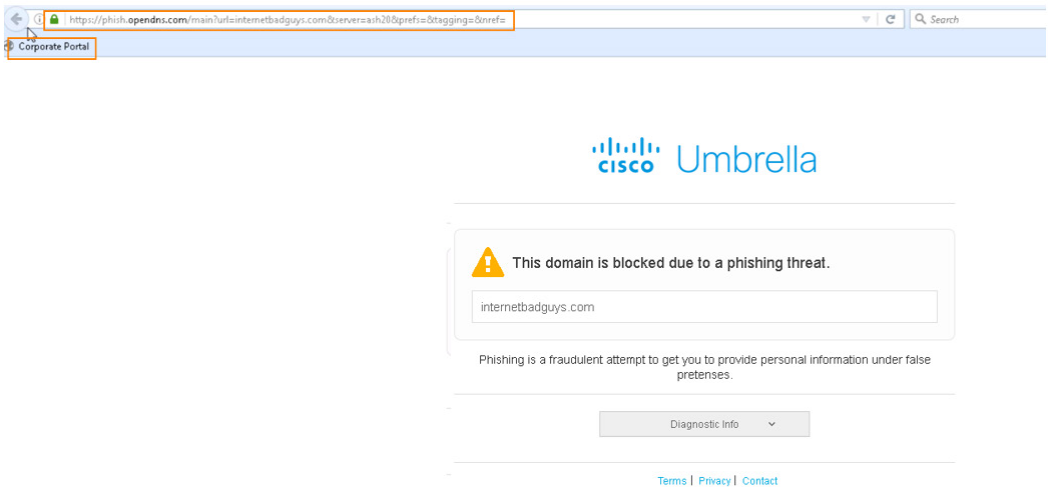
13. Bob의 이메일로 돌아가 기업 네트워크에 로그인한 상태에서 Vegas Getaway 이메일 광고를 다시 열어봅니다.

그림 13. 피싱 사이트 이메일 광고



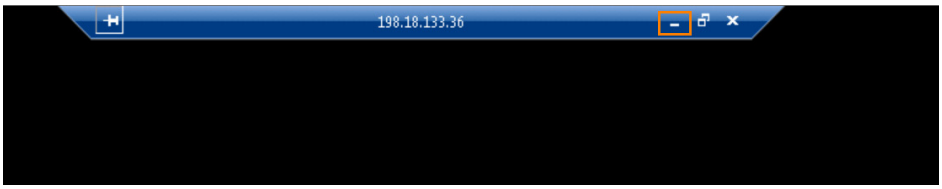
14. Umbrella에서 이 피싱 사이트를 다시 차단했으며, 이번에는 Bob이 기업 네트워크에 연결된 상태입니다.

그림 14. 기업 네트워크에서 Umbrella의 피싱 차단



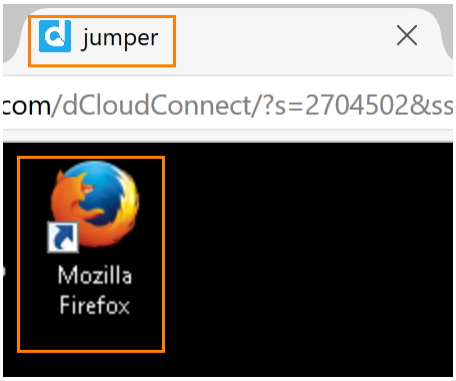
15. Bob이 원격으로 업무를 수행하는 동안 기업 네트워크 보안 분석가는 네트워크의 상태를 모니터링할 수 있습니다. FMC(Firepower Management Center) 같은 Cisco 보안 툴을 구축하여 Bob과 네트워크를 보호하고, 네트워크 활동에 대한 실시간 모니터링 및 분석도 제공합니다. 보안 분석가가 FMC를 사용하여 Bob의 특정 로그인 세션에 대한 중요한 정보를 얻는 방법을 확인하려면 이메일을 닫고 Bob의 워크스테이션 보기를 최소화하여 Jumper PC 보기로 돌아갑니다.

그림 15. 워크스테이션 보기 최소화



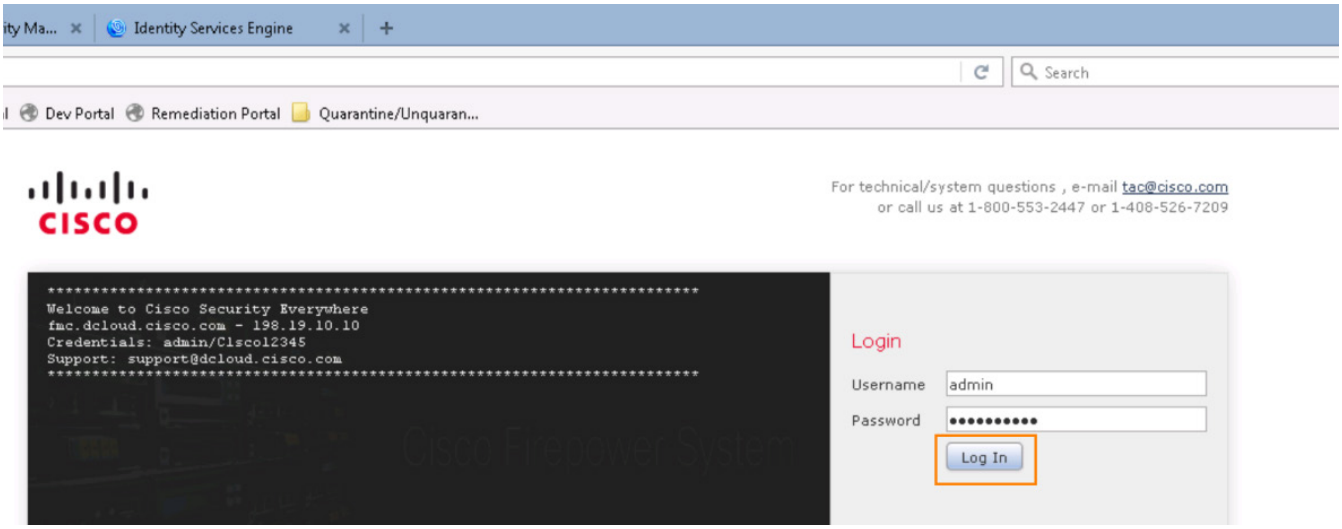
16. Jumper PC에서 Firefox 웹 브라우저를 엽니다.

그림 16. Jumper PC Firefox 바로가기



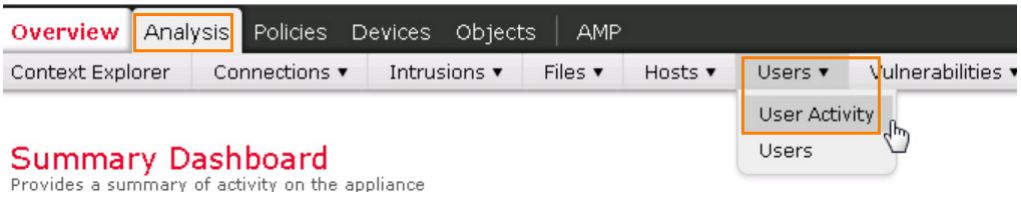
17. **FMC** 탭을 클릭한 후 **Log In(로그인)**을 클릭하여 사용자 이름 **dcloud**, 비밀번호 **C1sco12345**로 FMC에 액세스합니다.

그림 17. FMC 로그인



18. 이제 보안 분석가가 Bob의 기업 네트워크에서 사용할 수 있는 툴을 볼 수 있습니다. **Analysis(분석)**로 스크롤한 후 **Users(사용자)**를 클릭하여 드롭다운 메뉴를 열고 **User Activity(사용자 활동)**를 선택합니다.

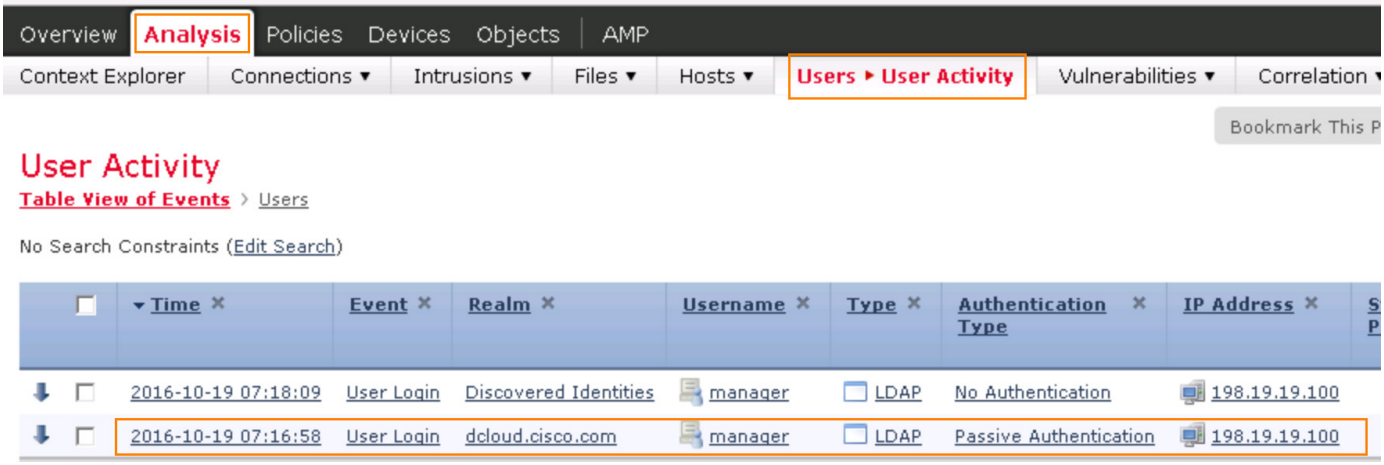
그림 18. FMS 분석 메뉴



19. 보안 분석가는 FMC User Analysis 툴을 사용하여 Bob의 로그인 정보를 볼 수 있습니다.

> **참고:** FMC의 사용자 활동 화면에서는 사용자의 네트워크 로그인 또는 로그아웃 시간을 추적하고 다양한 정보를 제공합니다. **Cisco FMC(Firepower Management Center)**는 백그라운드에서 **Cisco ISE(Identity Services Engine)**와 함께 작동하여 Bob의 로그인 및 머신에 대한 중요한 ID 정보를 확인하도록 구성되었습니다. 여기서는 Bob이 네트워크에 로그인하면 ISE가 Bob을 확인 및 인증하고, Bob을 직원으로 식별하는 **Cisco TrustSec SGT(Security Group Tag)**를 Bob의 VPN 세션에 할당합니다. SGT는 Bob이 네트워크에서 액세스할 수 있는 항목을 확인하는 과정을 추가로 지원합니다. 그런 다음 ISE는 **Cisco PxGrid**를 통해 Bob의 ID 정보를 FMC와 공유합니다. FMC의 사용자 활동에서 Bob의 사용자 이름, IP 주소, Bob에게 "Employees" SGT 태그 할당됨 등의 다양한 정보를 볼 수 있습니다.

그림 19. FMC 사용자 활동



시나리오 2. 공격 전: 보안 인텔리전스 데모

첫 번째 피싱 공격이 효과가 없었으므로, 끈질긴 공격자가 다시 공격을 시도합니다. internetbadguys.com은 Umbrella에서 차단한 알려진 유해 사이트가 되었으므로, 이번에 공격자는 피싱 이메일에 서버의 IP 주소를 직접 포함하여 싱가포르에서 다시 액세스할 수 있는 또 다른 CnC(Command and Control) 서버에 링크를 연결하려고 시도합니다. 이 시나리오에서는 FMC의 동적 보안 인텔리전스 피드가 이러한 유형의 공격을 어떻게 차단할 수 있는지를 보여 줍니다. 연결이 허용될 경우, 이 공격자의 목표는 주도면밀하게 위조된 웹사이트를 통해 Bob의 머신에 있는 알려진 취약점을 익스플로잇하여 Bob의 PC를 감염시키는 것입니다.

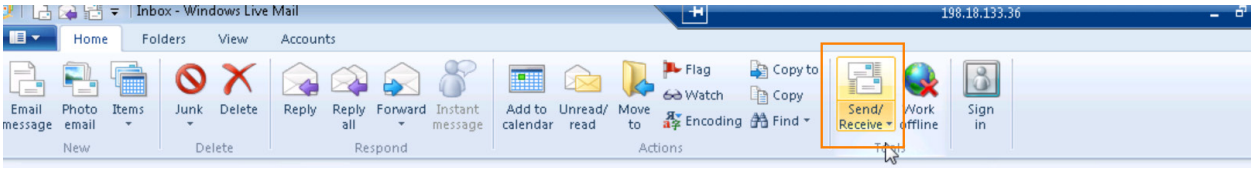
단계

1. Jumper PC의 아래쪽 메뉴 트레이에서 PC 아이콘을 클릭하여 Bob의 워크스테이션으로 돌아갑니다.

2. Bob은 네트워크에 로그인되어 있으며, 이제 수신된 새 이메일에 액세스할 수 있습니다. 이 이메일 창에서 Send/Receive(보내기/받기)를 클릭하여 새 이메일을 로드합니다.

> **참고:** 이전 시나리오를 완료하지 않은 경우 WKST1에서 Cisco AnyConnect VPN을 사용하여 비밀번호 C1sco12345로 기업 데모 네트워크에 로그인하십시오. WKST1이 VPN을 통해 연결되지 않은 경우 WKST1에서 이메일을 수신할 수 없습니다.

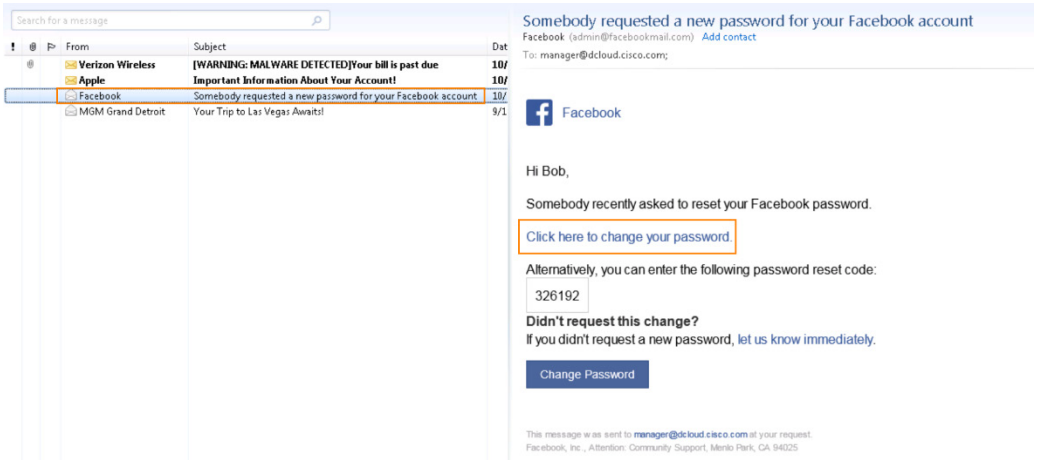
그림 20. 이메일 보내기/받기



3. Bob의 새 이메일 목록에 누군가 비밀번호 변경을 시도했다는 내용의 Facebook 메시지가 있습니다. 비밀번호를 변경하라는 내용이 표시되며, Bob은 계정 보호를 위해 비밀번호를 업데이트하는 링크를 클릭합니다. 브라우저 창이 열리고 결국 시간 초과됩니다. 이는 의도적인 동작으로, Firepower Threat Defense가 연결을 성공적으로 차단했기 때문입니다!

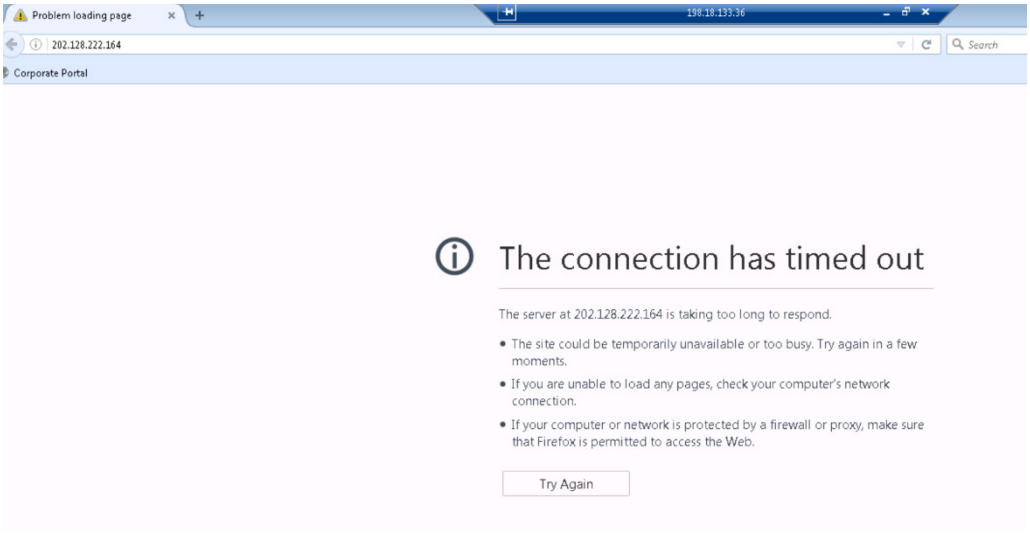
> **참고:** 새 이메일 3개가 표시된 것과 다른 순서로 도착할 수도 있습니다. 이 시나리오는 보안 인텔리전스 데모이므로, Facebook에서 보낸 것처럼 보이는 이메일을 열어야 합니다.

그림 21. Facebook 비밀번호 변경 이메일

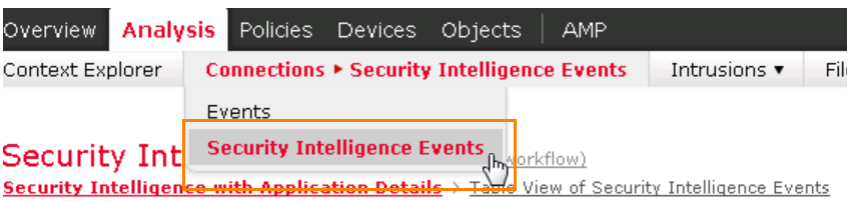


4. Bob은 실제로 Facebook으로 연결되는 링크가 아닌, 악성 사이트로 연결되는 링크를 클릭했습니다. 여기서는 Firepower Threat Defense Security Intelligence에서 악성 IP 주소를 확인하고 해당 요청을 시간 초과로 처리하여 Bob이 사이트에 연결하지 못하도록 했습니다.

그림 22. 악성 사이트 연결 시간 초과

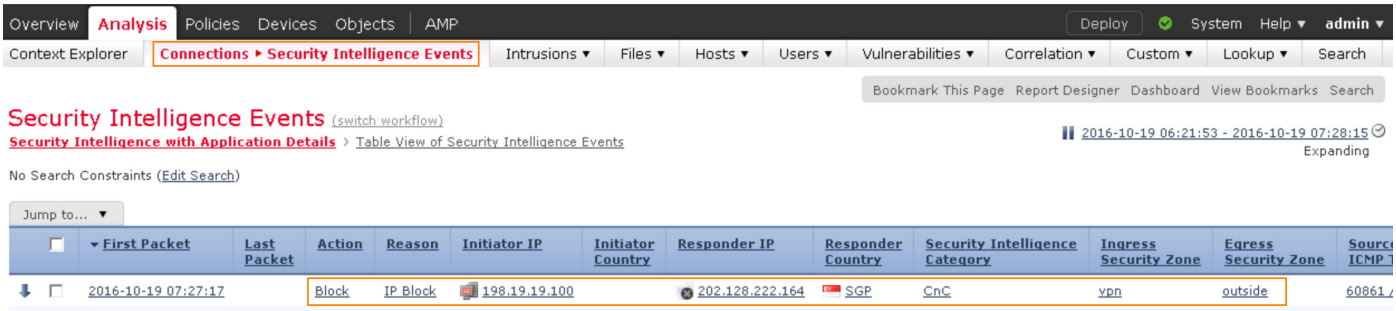


5. Bob의 워크스테이션 창을 최소화하고 Jumper PC로 돌아갑니다. 열어 놓은 Firefox FMC 탭에서 **Analysis(분석)**로 스크롤한 후 **Connections(연결)**를 클릭하여 드롭다운 메뉴를 열고 **Security Intelligence(보안 인텔리전스)**를 선택합니다.



6. Bob의 네트워크 분석가는 차단 사유, 악성 사이트에 액세스를 시도한 네트워크의 IP 주소, 악성 사이트의 IP 주소, 악성 IP 주소의 발원지 국가, 외부 소스에서 VPN을 통해 시작된 공격 등을 포함하여 공격에 대한 세부사항을 볼 수 있습니다.

그림 23. FMC 보안 인텔리전스 세부사항

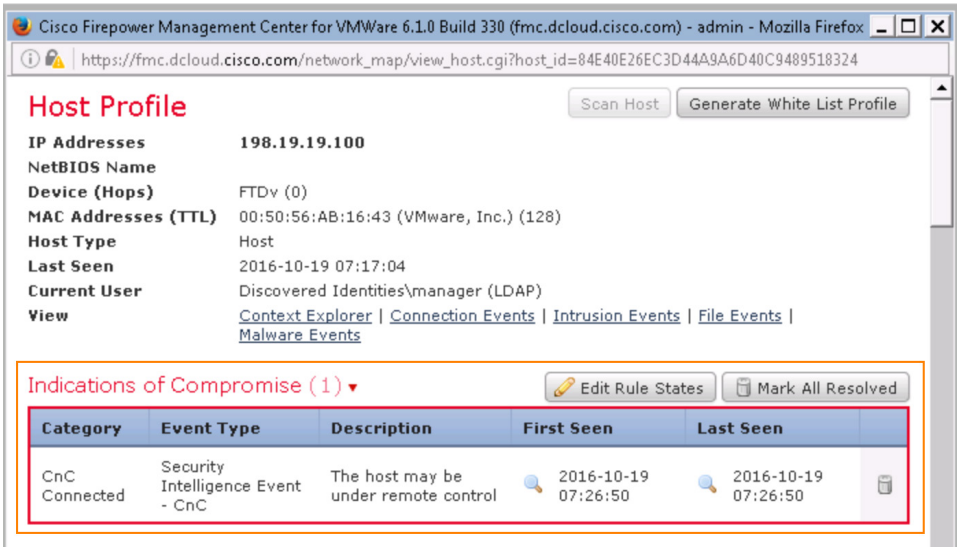


7. Bob의 이니시에이터 IP 주소에 대한 맨 아래 항목 옆에 있는 컴퓨터 아이콘을 클릭하여 이 머신의 호스트 프로파일을 확인합니다.

그림 24. 호스트 프로파일 세부사항 열기

8. 네트워크 분석가는 **Host Profile(호스트 프로파일)** 세부사항을 볼 수 있으며, 여기에는 Bob이 싱가포르에 있는 알려진 CnC 서버에 액세스를 시도하여 방금 활성화된 **Indications of Compromise(보안 침해 지표)** 알림이 포함됩니다.

그림 25. FMC 호스트 프로파일 세부사항



시나리오 3. 공격 전: WSA가 알려진 악성코드를 차단하는 데모

이 단계까지 공격자는 Bob에게서 아무런 응답도 얻지 못했으므로, 공격의 강도를 높이기로 합니다. 공격자는 악성 소프트웨어 툴박스에 수많은 툴을 보유하고 있으며, 그 중에는 실행할 경우 타겟을 감염시키고, 타겟에서 공격자로 리버스 CnC(Command and Control) 채널을 여는 입증된 악성 실행 파일도 있습니다. Bob이 이 파일을 다운로드하고 실행하도록 유도할 수만 있다면 공격자는 Bob의 머신에 있는 항목을 익스플로잇하지 않아도 머신을 완전히 장악할 수 있게 됩니다. 공격자는 과거에도 이와 동일한 알려진 악성코드를 사용하여 수많은 타겟을 함락시켰으므로, Bob에게 이러한 유형의 공격을 시도하려고 합니다. 이 공격이 성공하려면 Bob이 파일을 클릭, 다운로드, 실행해야 하므로 공격자는 다른 피싱 공격을 시도합니다. 이 이메일에는 악성 파일로 직접 이동하는 링크가 포함되어 있으며, Bob에게 링크를 실행하라고 지시하는 내용이 적혀 있습니다.

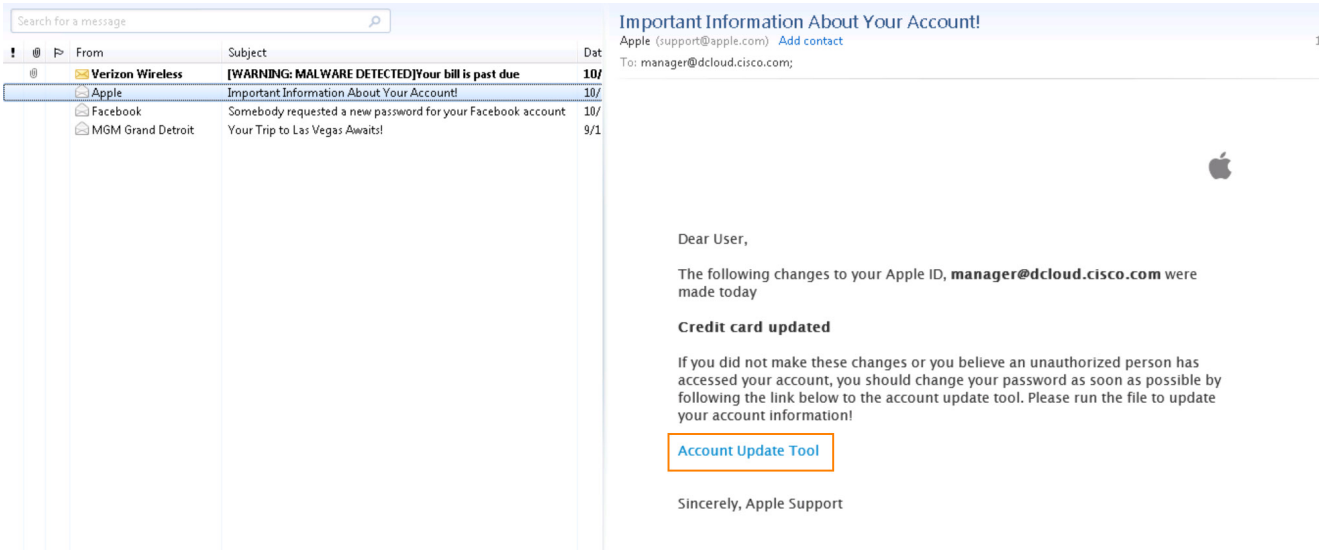
단계

1. WKST1에서 이메일 클라이언트로 돌아갑니다. Bob은 Apple에서 보낸 것처럼 보이는 계정 업데이트 요청인 다음 이메일로 넘어갑니다. 이메일에서 **Account Update Tool(계정 업데이트 툴)**을 클릭합니다. 그러면 브라우저 창이 열리고 알려진 악성 파일을 다운로드하려고 합니다.

참고: 이전 시나리오를 완료하지 않은 경우 WKST1에서 Cisco AnyConnect VPN을 사용하여 비밀번호 C1sco12345로 기업 데모 네트워크에 로그인하십시오. WKST1이 VPN을 통해 연결되지 않은 경우 WKST1에서 이메일을 수신할 수 없습니다.

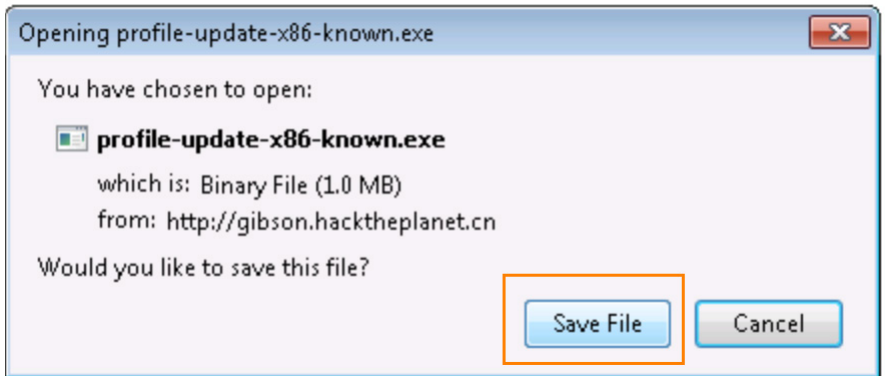
참고: 새 이메일 3개가 표시된 것과 다른 순서로 도착할 수도 있습니다. 이 시나리오는 WSA가 알려진 악성코드를 차단하는 데모이므로, Apple에서 보낸 것처럼 보이는 이메일을 열어야 합니다.

그림 26. Apple 계정 업데이트 이메일



2. 이 이메일은 http://gibson.hacktheplanet.cn에서 다운로드하여 저장할 파일을 엽니다. Save File(파일 저장)을 클릭합니다.

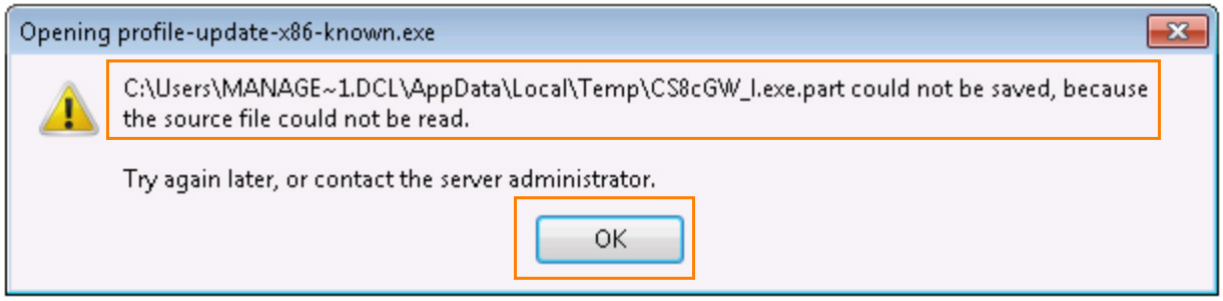
그림 27. Apple 이메일 다운로드 메시지



3. Cisco WSA(Web Security Appliance) with AMP가 다운로드를 차단하고 오류 메시지를 표시합니다.

참고: 이 데모에서 Bob과 같은 VPN 사용자의 모든 아웃바운드 웹 트래픽은 Cisco WSA(Web Security Appliance)를 통과합니다. 이 데모의 WSA는 Advanced Malware Protection(AMP for Networks)과 통합되었으며 알려진 악성 파일을 탐지하고 차단할 수 있습니다. 이 시나리오에서 Bob이 악성 파일을 다운로드하려고 하면 WSA가 파일을 확인하고 AMP 클라우드 조회를 수행합니다. 파일에 알려진 악성 SHA256 해시가 있으므로 WSA가 파일을 즉시 차단하며, 파일을 다운로드할 수 없게 됩니다. 여기서는 파일이 바깥쪽 기업 방화벽 방어를 통과하기도 전에 WSA에 의해 차단되었습니다.

그림 28. Apple 이메일 다운로드 오류 메시지



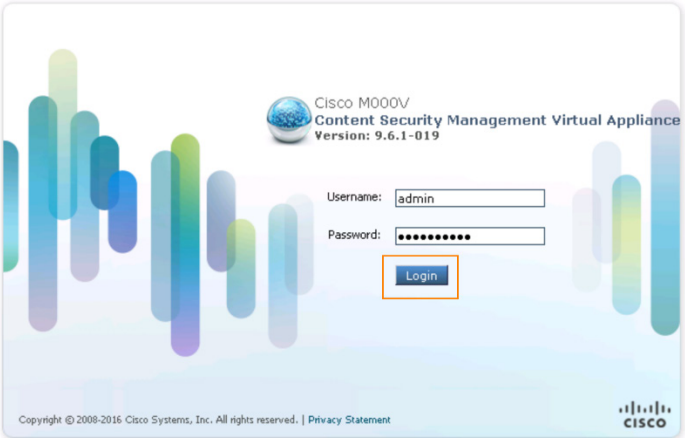
4. 브라우저를 닫고 Bob의 워크스테이션 창을 최소화한 후 Jumper PC로 돌아갑니다. Firefox 브라우저 창을 확장하고 Cisco Content SMA(Security Management Virtual Appliance) 탭을 클릭합니다.

참고: Cisco Content SMA(Security Management Appliance)를 사용하면 **Cisco WSA(Web Security Appliance)** 및 **ESA(Email Security Appliance)**를 둘 다 관리할 수 있으며, 한곳에서 두 어플라이언스를 모두 모니터링하고 각각에 대한 보고 데이터를 가져올 수도 있습니다. 다음 단계에서는 SMA에 로그인하여 WSA가 알려진 악성 파일을 어떻게 차단할 수 있었는지 살펴보겠습니다.

그림 29. Cisco Content SMA(Security Management Appliance) 탭

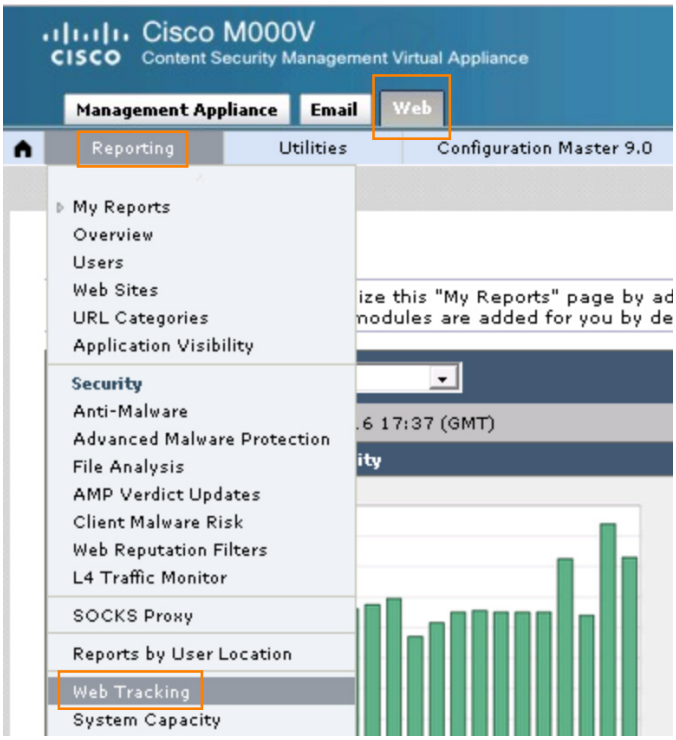
5. Login(로그인)을 클릭하고 사용자 이름 **admin**, 비밀번호 **C1sco12345**로 SMA에 액세스합니다.

그림 30. SMA 로그인



6. **Web(웹)** 메뉴 탭을 클릭한 후 **Reporting(보고)**을 클릭하여 드롭다운 메뉴를 열고 **Web Tracking(웹 추적)**을 선택합니다.

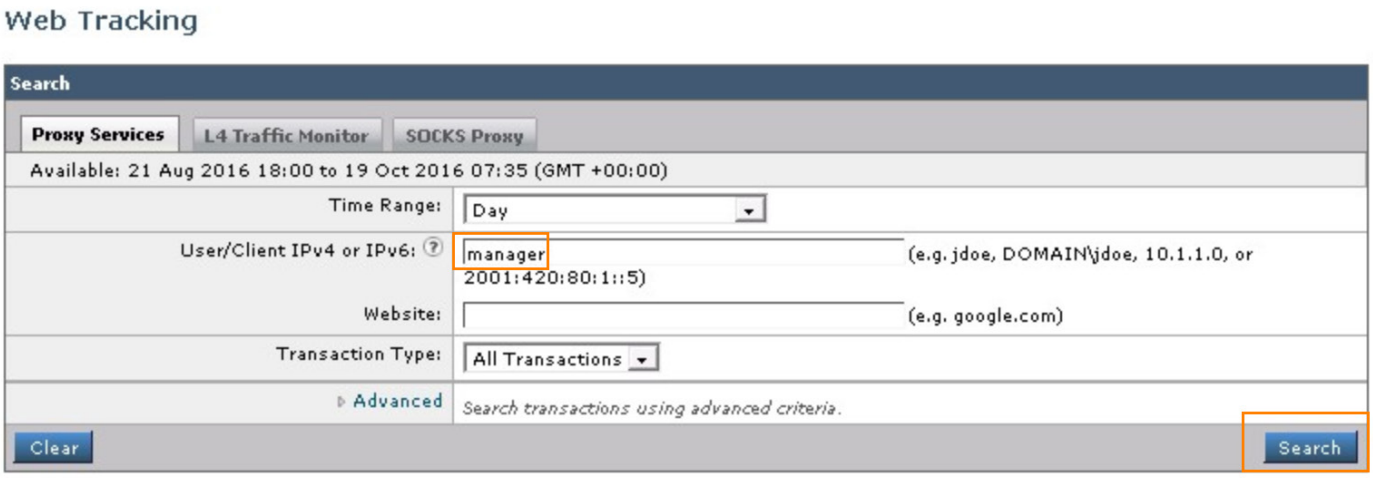
그림 31. SMA 웹 추적 선택



7. **User/Client IPv4 or IPv6(사용자/클라이언트 IPv4 또는 IPv6)** 항목에서 **manager**를 입력하고 **Search(검색)**를 클릭합니다.

참고: 프록시 서비스 항목은 대/소문자를 구분합니다. **manager**를 입력할 때 모두 소문자로 입력하십시오.

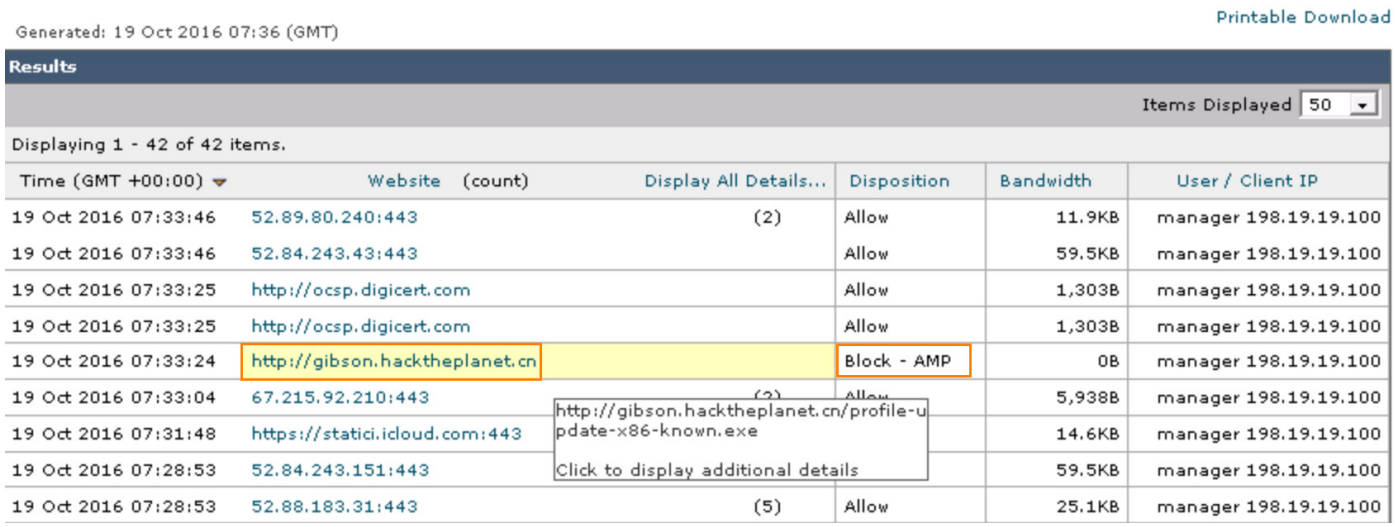
그림 32. 웹 추적 검색



참고: 검색에서 웹 추적 결과가 반환되는 데 최대 10분 정도가 소요될 수 있습니다. WSA와 SMA 간의 로깅에 시간이 걸리므로 데모의 다음 단계를 먼저 진행하고 나중에 데모를 마칠 때쯤 다시 이 단계로 돌아오는 것이 좋습니다.

8. 보안 분석가는 Bob의 이메일에 있는 파일이 http://gibson.hacktheplanet.cn의 알려진 악성 파일이기 때문에 AMP가 해당 파일에 대한 액세스를 차단했으며 구현된 보안 툴이 해커가 네트워크에 파일을 구축하지 못하도록 차단했음을 확인할 수 있습니다.

그림 33. 웹 추적 결과



9. 웹사이트 주소를 클릭하여 WSA에서 확인한 악성 다운로드에 대한 AMP 차단 정보를 확장합니다.

그림 34. 웹 추적 결과 세부사항

19 Oct 2016 07:33:24	http://gibson.hacktheplanet.cn/profile-update-x86-known.exe CONTENT TYPE: application/x-dosexec DESTINATION IP: HOST: wsa.dcloud.cisco.com 14.144.144.66 (198.19.11.10) DETAILS: Access Policy: "dCloud_Employee_Access_Policy". WBRS: -3.8, AMP Verdict: Malware, AMP Threat Score: 40, Malware Threat: W32.EF47343EB8-95.SBX.TG, Filename: profile-update-x86-known.exe, SHA256: ef47343eb8db17f717c2558cc710d9cb8ca9b1384723c1952c63615155707699.	Block - AMP	0B	manager (Identified by ISE) 198.19.19.100

가치 제안:

10. 아래쪽 메뉴 트레이의 워크스테이션 아이콘을 클릭하여 Bob의 이메일로 돌아간 후, 네트워크에 악성코드를 설치하려는 해커의 시도를 계속 살펴봅니다.

그림 35. 워크스테이션 아이콘

시나리오 4. 공격 전: ESA가 알려진 악성코드를 차단하는 데모

Bob이 여전히 속아 넘어가지 않아 공격이 좌절된 공격자는 일반적인 악성 소프트웨어로 연결되는 링크가 포함된 또 다른 피싱 공격을 시도합니다. 그러나 이번에도 악성코드를 첨부했기 때문에 Bob이 이메일을 실행해야 하므로, 공격자는 Bob에게 파일을 실행하라는 지침을 메일에 적고 공격이 성공하기를 바랐습니다.

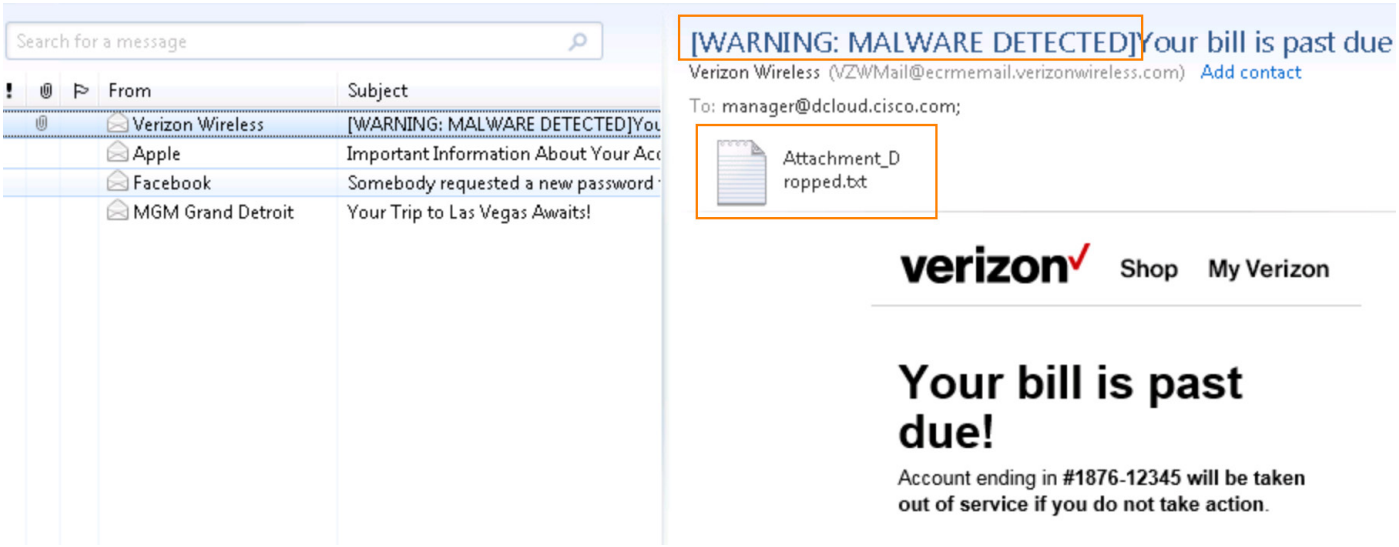
단계

1. Bob의 이메일에서 Verizon에서 보낸 전화 요금 미납과 관련된 새 메시지를 엽니다. 메시지 제목에 악성코드가 탐지되었다고 표시되어 있으나, 첨부 파일과 함께 메시지가 표시되도록 허용합니다. 첨부 파일을 클릭합니다.

참고: 이전 시나리오를 완료하지 않은 경우 WKST1에서 Cisco AnyConnect VPN을 사용하여 비밀번호 C1sco12345로 기업 데모 네트워크에 로그인하십시오. WKST1이 VPN을 통해 연결되지 않은 경우 WKST1에서 이메일을 수신할 수 없습니다.

참고: 새 이메일 3개가 표시된 것과 다른 순서로 도착할 수도 있습니다. 이 시나리오는 ESA가 알려진 악성코드를 차단하는 데모이므로, Verizon에서 보낸 것처럼 보이는 이메일을 열어야 합니다.

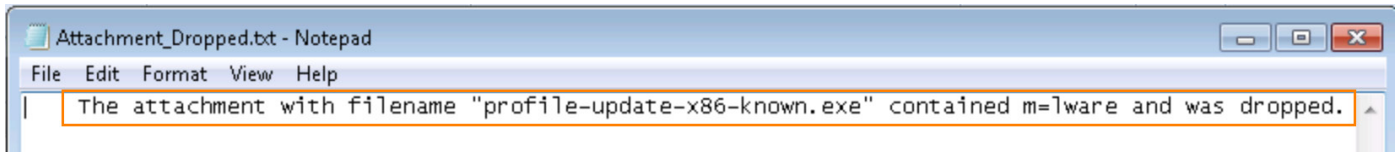
그림 36. 첨부 파일이 포함된 Verizon 이메일



2. 원본 악성코드 첨부 파일을 열어 네트워크를 감염시키는 대신, 시스템에서는 악성코드를 탐지하고 ESA(Email Security Appliance)와 AMP(Advanced Malware Protection)의 통합 보호 기능을 통해 해당 악성코드를 삭제했다는 알림을 추가했습니다.

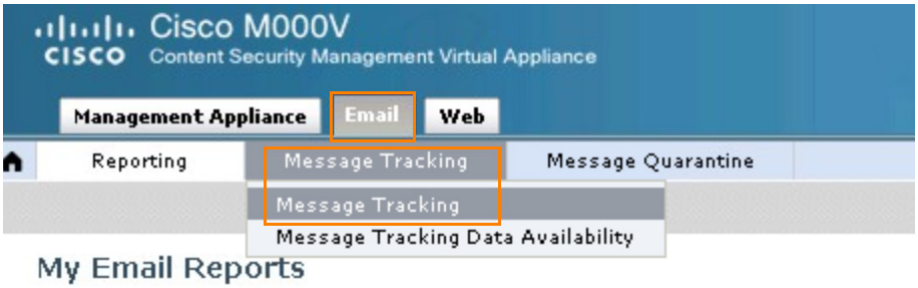
참고: 이 시나리오에서 **Cisco ESA(Email Security Appliance)**는 파일에 악성 SHA256 해시가 있기 때문에 원본 이메일에서 악성코드를 제거했습니다. 그러나 경고 메시지와 함께 이메일이 표시되는 것은 허용했습니다. 이는 제품 데모를 더 원활하게 진행하기 위해 의도적으로 설정한 것입니다. 기본적으로 ESA는 알려진 악성 첨부 파일이 포함된 이메일을 삭제합니다. 이 데모에서는 현재 상황을 연출하기 위해 ESA의 다양한 정책을 대폭 완화해야 했습니다.

그림 37. 악성코드 삭제 알림



3. 메시지를 닫고 Bob의 워크스테이션 창을 최소화한 후 Jumper PC로 돌아가 보안 분석가의 이벤트 보기를 살펴봅니다. SMA 탭에서 **Email(이메일)**을 클릭한 후 **Message Tracking(메시지 추적)**을 클릭하여 드롭다운 메뉴를 열고 **Message Tracking(메시지 추적)**을 선택합니다.

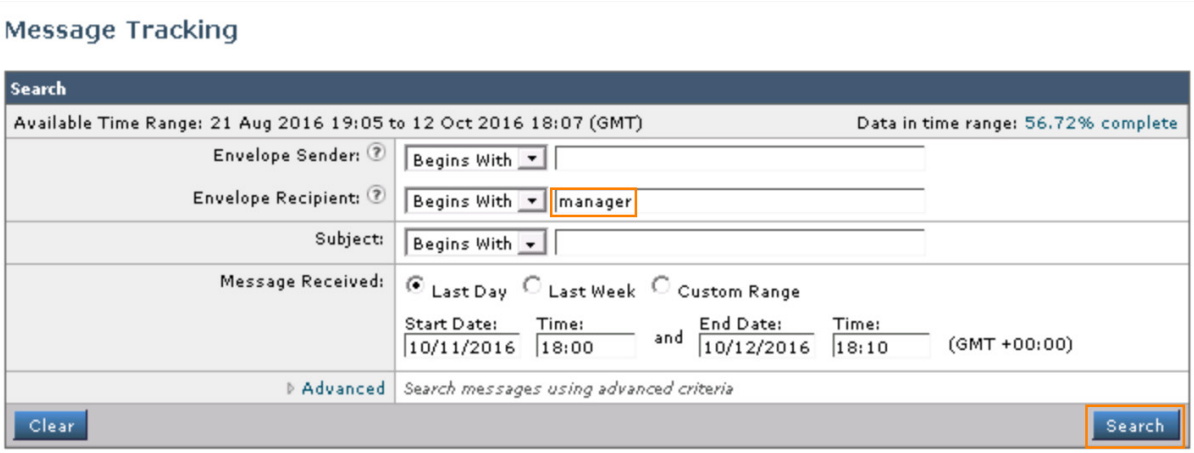
그림 38. 메시지 추적



4. Message Tracking(메시지 추적)의 **Envelope Recipient(봉투 받는 사람)** 항목에 **manager**를 입력합니다. **Search(검색)**를 클릭하여 결과를 반환합니다.

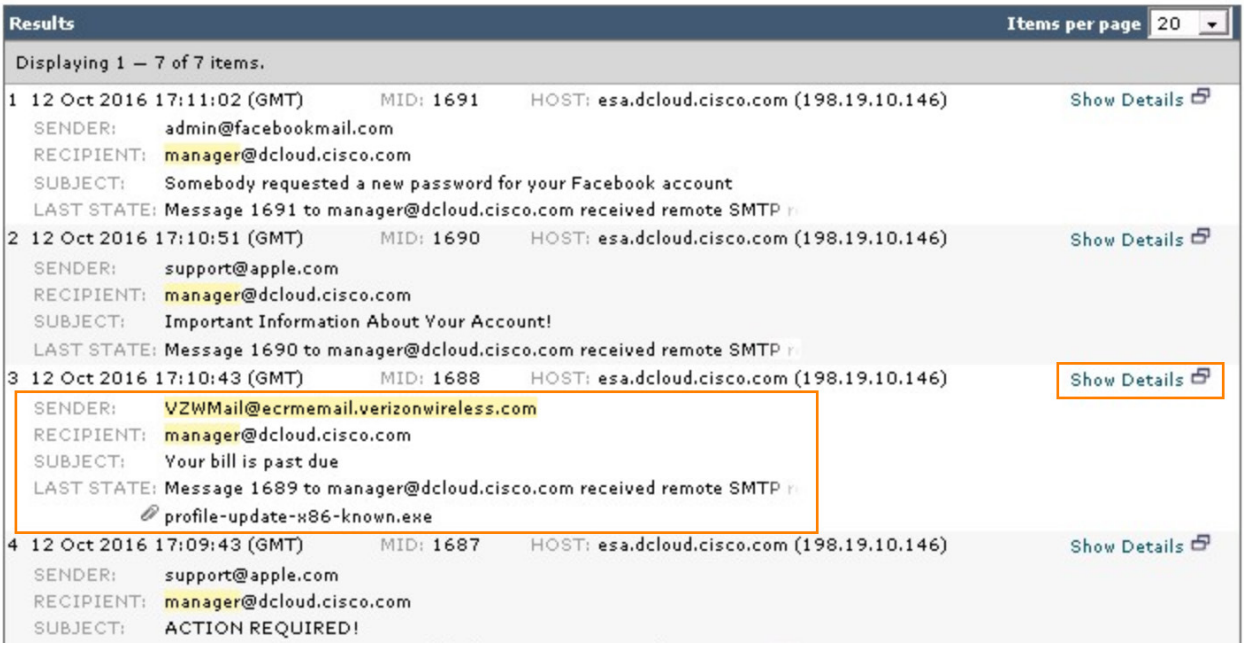
> **참고:** 메시지를 보낸 지 24시간 후에 이 단계를 수행할 경우, 데모에 전송 메시지를 시작한 시간이 포함되도록 **Message Received(메시지 수신)** 날짜 범위를 업데이트해야 할 수도 있습니다.

그림 39. 메시지 추적 검색 창



5. Verizon 악성코드가 탐지된 결과를 보고 **Show Details(세부사항 표시)**를 클릭합니다.

그림 40. 메시지 추적 결과



6. AMP에서 탐지된 Verizon 악성코드 메시지 세부사항을 확인합니다.

그림 41. Verizon 악성코드 메시지 세부사항

시나리오 5. 공격 중: 제로 데이 악성코드를 방어하는 데모

지금까지 Bob의 PC를 장악하려는 공격자의 시도는 한 번도 성공하지 못했습니다. 이제 공격자는 급기야 기업 네트워크에 무단 액세스하려고 합니다. 이 시나리오에서는 끈질긴 공격자가 완전히 새롭고 알려지지 않은 지능형 악성코드를 실시간으로 매우 주도면밀하게 생성합니다. 알려지지 않은 파일이므로 파일 해시도 알려지지 않았으며, 알려진 악성코드로 확인되지 않습니다. 따라서 이 파일은 방화벽 및 서명에 기반한 기존의 바이러스 스캐너 같은 가장 일반적인 유형의 네트워크 보안 방어를 우회합니다.

이 데모에서 Bob의 PC에는 AMP for Endpoints가 기본적으로 비활성화되어 있습니다. 이는 모든 제품의 전체 기능을 데모로 보여줄 수 있도록 의도적으로 설정한 것입니다. AMP for Endpoints 서비스가 비활성화되고 Bob이 위험한 제로 데이 악성코드를 PC에서 실행하는 최악의 시나리오에서 어떤 결과가 발생하는지 살펴보겠습니다.

마침내 공격자는 Bob의 PC에 악성코드를 심고 Bob이 이를 실행하도록 유도하여 PC를 완전히 장악하게 됩니다. Bob의 PC를 제어하게 된 공격자는 Bob이 VPN을 통해 대규모 엔터프라이즈 네트워크에 연결되어 있다는 사실을 알게 됩니다. 이제 공격자가 취할 다음 논리적인 단계는 Bob의 PC를 구심점으로 활용하여, 정상적으로는 Bob이 액세스할 수 없는 보호된 기업 네트워크 내부의 자산에 대한 액세스 권한을 획득하려고 시도하는 것입니다. 공격자가 Bob의 PC를 통해 네트워크 내부의 어떤 요소에 공격을 실행할 수 있을 경우 랜섬웨어로 네트워크를 감염시킨 후 매우 중요한 정보를 탈취하여 도주할 것이며 기업 네트워크에 이루 말할 수 없는 큰 피해를 입힐 가능성이 있습니다.

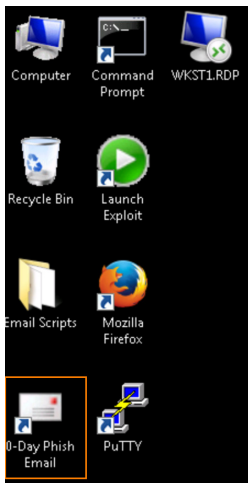
여기서 최종 목표는 Bob이 아닙니다. 이 단계에서 Bob은 기업 네트워크로 들어가기 위한 관문이며 공격자는 바로 이것을 노리는 것입니다.

참고: 제로 데이 취약점은 벤더가 알지 못하는 소프트웨어의 허점을 의미합니다. 벤더가 이러한 보안 허점을 알아내고 서둘러 고치기 전에 해커가 이를 악용하는 것이며, 이러한 익스플로잇을 제로 데이 공격이라고 합니다.

1. Jumper PC로 돌아가 **0-Day Phish Email(제로 데이 피싱 이메일)** 바탕화면 바로가기를 더블 클릭하여 악성코드를 생성하고 이메일을 Bob의 받은 편지함으로 보냅니다.

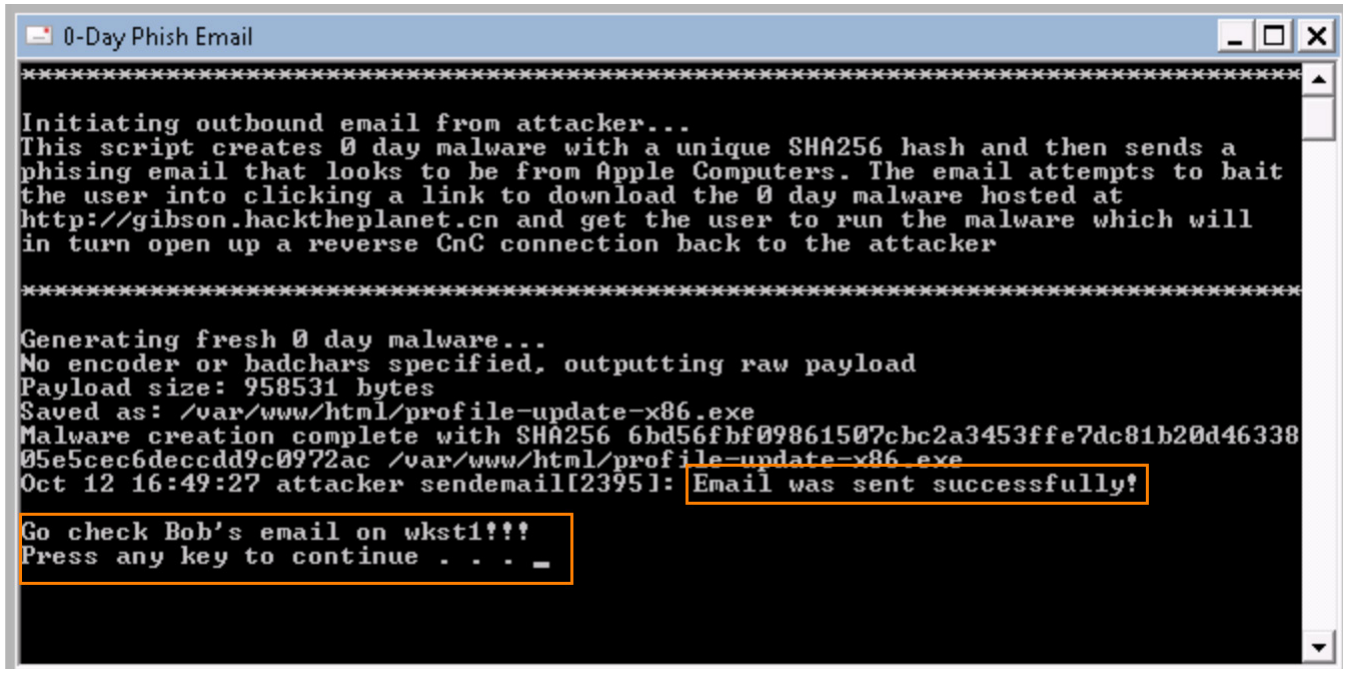
   참고: 0-Day Phish Email(제로 데이 피싱 이메일) 스크립트는 실행될 때마다 새로운 제로 데이 악성코드를 생성한 후, Bob이 링크를 클릭하여 악성코드를 다운로드 및 실행하도록 유도하는 피싱 이메일을 Bob에게 보냅니다. 공격자의 의도가 성공하여 Bob이 파일을 실제로 실행할 경우, 해당 파일은 중국에서 기다리고 있는 공격자의 머신에 리버스 CnC(Command and Control) 채널을 열어 줍니다. 이 시점에서 공격자는 Bob의 PC를 완전히 장악합니다. 그보다 더욱 중요한 점은 Bob이 VPN을 통해 기업 네트워크에 연결되어 있고 공격자가 Bob의 머신을 장악하고 있으므로, 이제 공격자가 Bob의 머신을 구심점으로 사용하여 기업 네트워크 내부의 중요한 정보에 대한 액세스 권한을 얻으려고 시도할 수 있다는 것입니다.

그림 42. 제로 데이 피싱 이메일 바로가기



2. 이메일이 전송되었는지 확인하고 아무 키나 클릭하여 창을 닫습니다.

그림 43. 제로 데이 피싱 이메일 전송 메시지



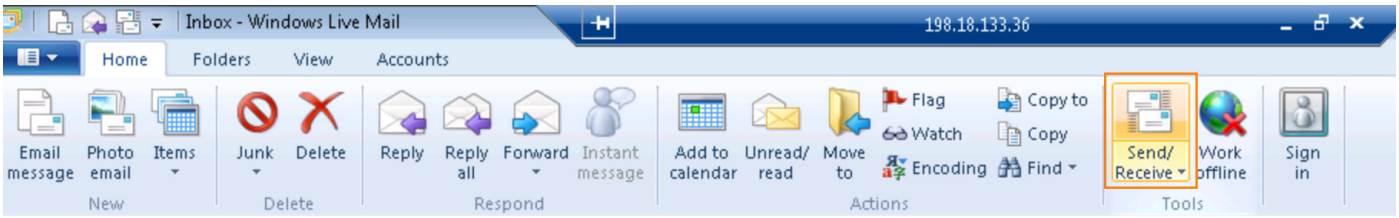
3. 아래쪽 메뉴 트레이의 워크스테이션 아이콘을 클릭하여 Bob의 PC로 돌아갑니다.

참고: 이전 시나리오를 완료하지 않은 경우 WKST1에서 Cisco AnyConnect VPN을 사용하여 비밀번호 C1sco12345로 기업 데모 네트워크에 로그인하십시오. WKST1이 VPN을 통해 연결되지 않은 경우 WKST1에서 이메일을 수신할 수 없습니다.

그림 44. 워크스테이션 아이콘

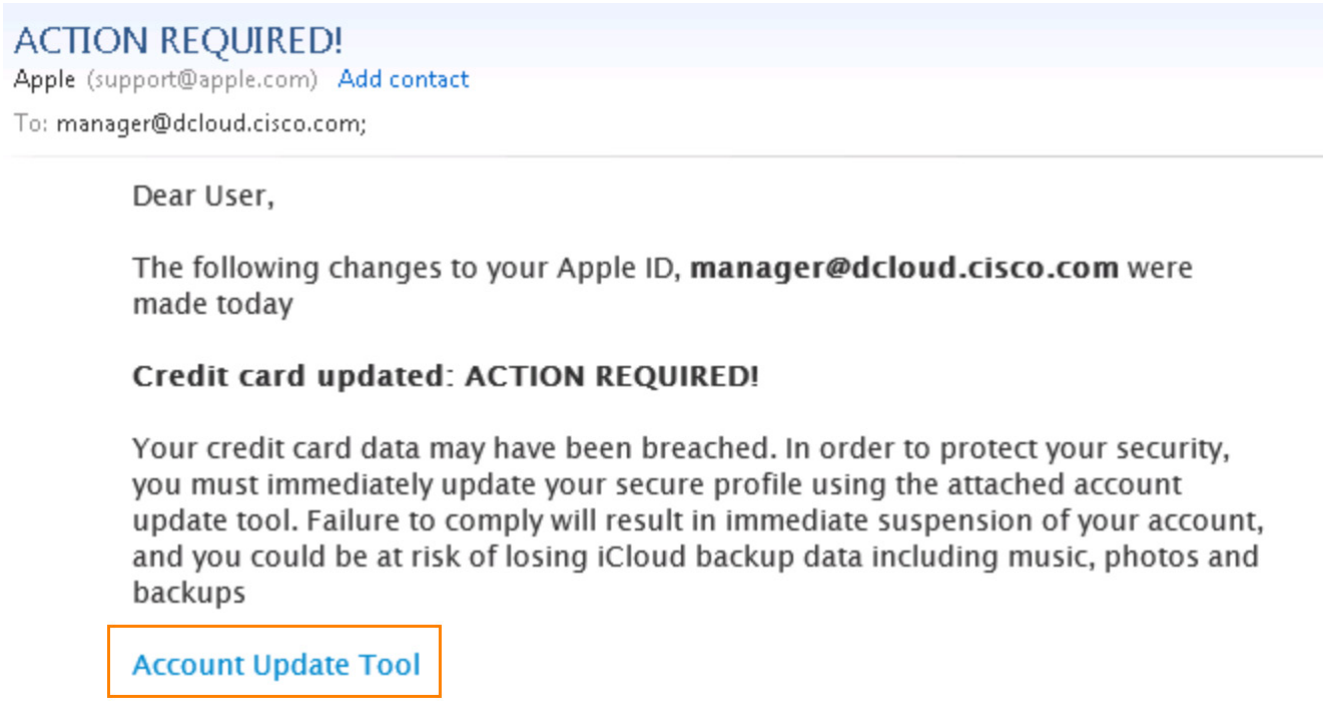
4. Bob의 받은 편지함에서 **Send/Receive(보내기/받기)**를 클릭합니다.

그림 45. 이메일 보내기/받기



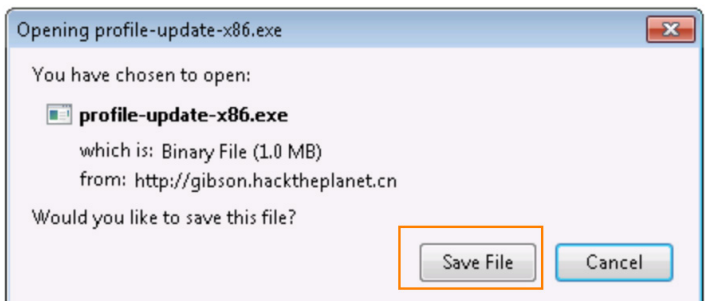
5. Apple 지원 팀에서 보낸 새 이메일을 열고 **Account Update Tool(계정 업데이트 툴)**을 클릭합니다.

그림 46. 제로 데이 피싱 이메일



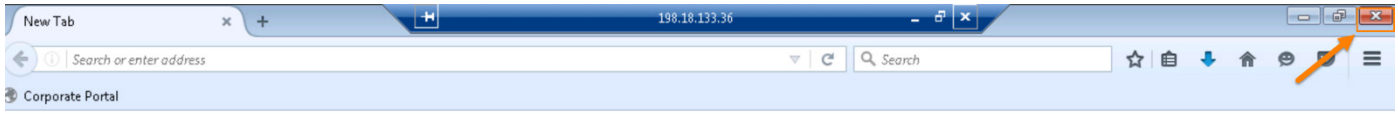
6. 이 이메일은 다운로드할 실행 파일을 엽니다. **Save File(파일 저장)**을 클릭합니다. 파일은 Bob의 바탕화면에 있는 Stuff 폴더에 자동으로 저장됩니다.

그림 47. 제로 데이 파일 저장



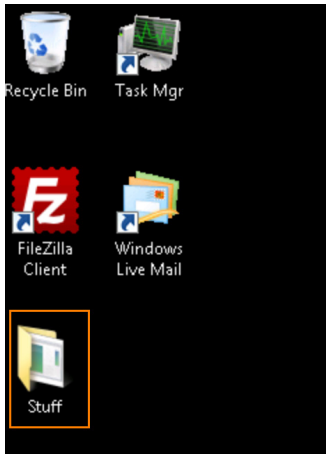
7. 이 단계에서는 Bob이 실행 파일을 컴퓨터에 다운로드한 것처럼 보입니다. 브라우저를 닫고 이메일을 최소화하여 Bob의 바탕화면으로 돌아갑니다.

그림 48. 브라우저 종료



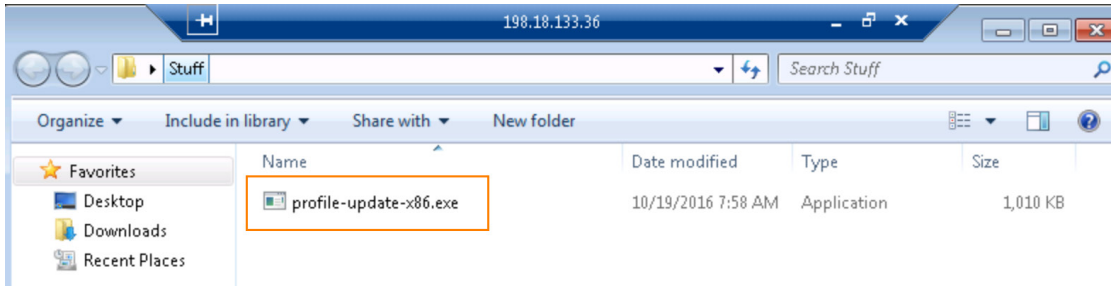
8. 바탕화면에서 **Stuff** 폴더를 엽니다.

그림 49. 바탕화면 > Stuff 폴더



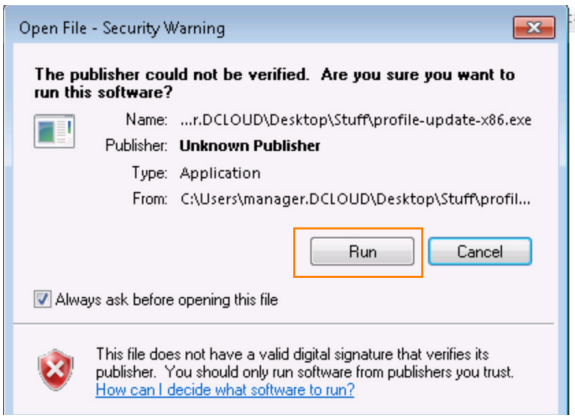
9. 제로 데이 이메일에서 다운로드한 파일을 더블 클릭합니다.

그림 50. 제로 데이 이메일 다운로드 파일



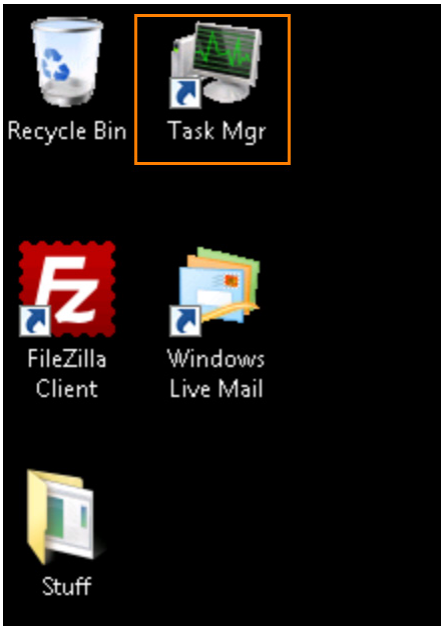
10. Open File(파일 열기) 창에서 **Run(실행)**을 클릭합니다.

그림 51. 파일 열기 > 실행



11. 실행 파일이 실행되거나 작업을 시작하는 것처럼 보이지 않습니다. 바탕화면으로 이동하여 작업 관리자를 엽니다.

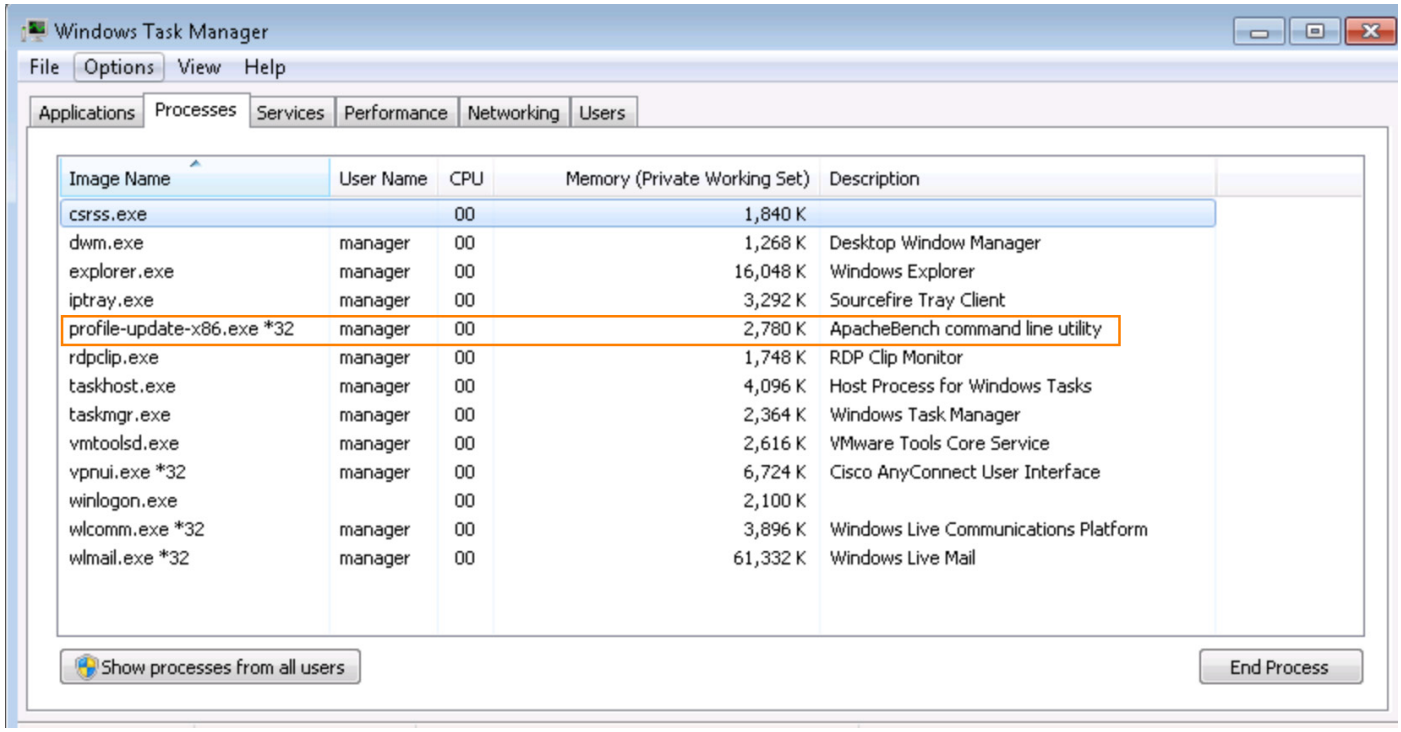
그림 52. 작업 관리자 바탕화면 바로가기



12. 파일이 실제로 다운로드되었으며 공격자에게 다시 연결하기 위해 기다리고 있음을 확인할 수 있습니다.

13. **참고:** 악성코드는 매우 교묘할 수 있습니다. 이 시나리오에서 악성코드는 Bob에게 작업이 발생하고 있다는 사실을 전혀 알리지 않습니다. 그러나 백그라운드에서 현재 이 악성코드는 중국에 있는 공격자의 머신에 연결하려는 시도를 끊임없이 적극적으로 실행하고 있습니다. 공격자가 다음 단계에서 직접 익스플로잇을 실행하기로 결정할 경우, Bob의 PC를 완전히 장악하게 됩니다.

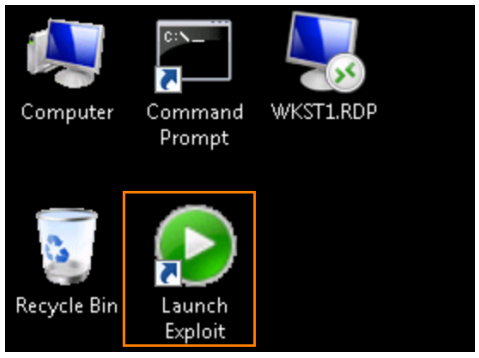
그림 53. 작업 관리자 > 제로 데이 파일



14. Jumper PC로 돌아간 후 바탕화면 바로가기에서 **Launch Exploit(익스플로잇 실행)**을 열어 공격자가 Bob의 컴퓨터에 다운로드한 제로 데이 파일로 네트워크에 연결을 시도하는 상황을 시뮬레이션합니다.

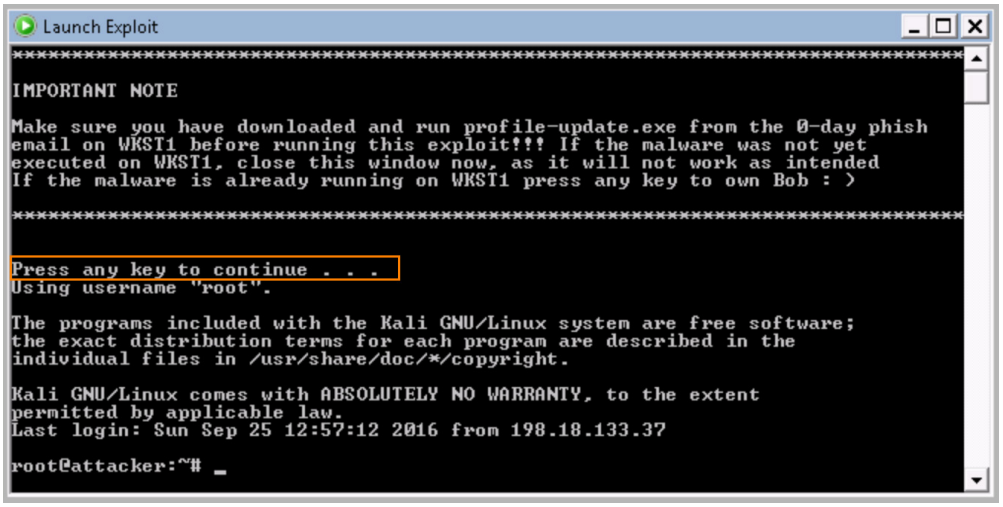
> **참고:** 잠시 기다려 주십시오. 이 스크립트를 완료하려면 약 1분 정도 소요되며 많은 양의 텍스트가 스크롤됩니다. 스크립트가 종료되어 아무 키나 누르라는 메시지가 표시되기 전에는 창을 닫거나 다른 작업을 하지 마십시오.

그림 54. 익스플로잇 실행



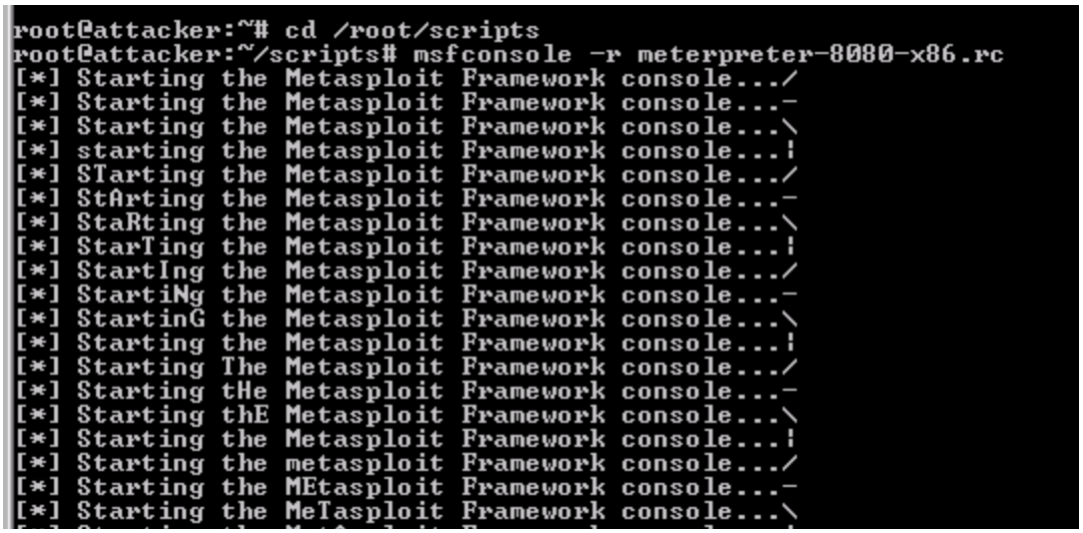
15. **Press any key to continue(계속하려면 아무 키나 누르십시오)**라는 지시를 따릅니다. 이제 공격자는 공격을 실행하고 Bob의 컴퓨터에 이미 심어 놓은 제로 데이 파일에 연결하여 기업 네트워크의 웹 서버를 장악하려고 합니다.

그림 55. 공격자의 제로 데이 파일 익스플로잇

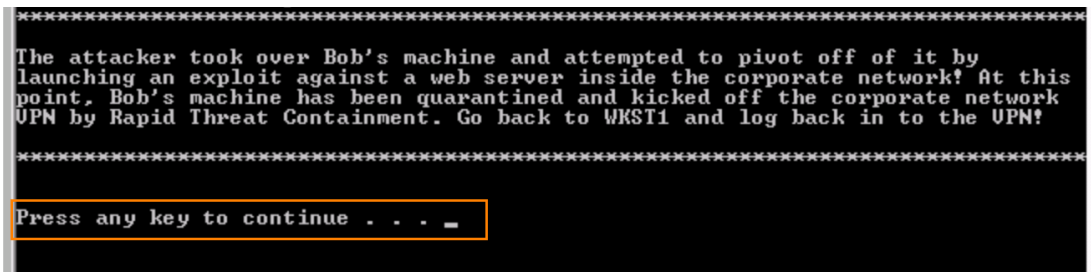


이제 공격자는 Bob의 컴퓨터에 액세스할 수 있으며, 액세스 가능한 네트워크 웹 서버를 해킹하고 장악하기 위해 스크립트를 실행하고 있습니다.

그림 56. 익스플로잇 시도



16. 구현된 Cisco 보안 툴이 Bob의 머신이 감염되었다는 사실을 확인했다는 경고 메시지가 표시될 때까지 공격 스크립트를 아래로 스크롤합니다. Firepower와 ISE의 통합된 보안 기능이 VPN을 통해 Bob을 보호하는 방화벽과 함께 작동하여 Bob의 컴퓨터가 기업 네트워크에서 제외되고 Bob의 액세스 권한이 자동으로 변경됩니다. **Press any key to continue(계속하려면 아무 키나 누르십시오)**라는 지시를 따릅니다.



17. Bob의 PC로 돌아가 AnyConnect를 클릭하여 열면 Bob의 네트워크 연결이 끊긴 것을 알 수 있습니다.

참고: Bob의 VPN 연결이 끊겼으며 이는 의도적인 조치입니다. 이 조치는 Bob의 PC를 격리하여 네트워크를 보호하기 위해 Cisco Rapid Threat Containment가 수행한 작업입니다. 이 시나리오에서 공격자는 Bob의 PC를 완전히 장악하고 있습니다. 공격자는 이제 Bob의 VPN에 연결된 기업 자산을 원격으로 제어하여 네트워크 내부의 기업 웹 서버에 대한 권한을 얻기 위해 공격을 실행했습니다. 다행히 **FTD(Firepower Threat Defense)**의 침입 방지 기능을 통해 권한 에스컬레이션 익스플로잇 시도를 포착했으며 즉시 조치를 취했습니다.

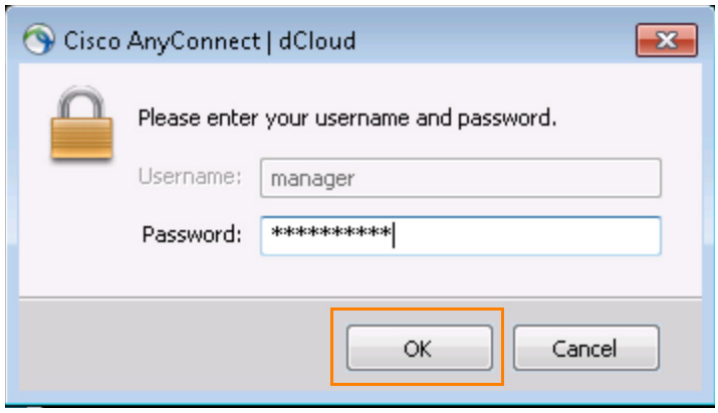
침입 이벤트가 발생하면 FMC**(Firepower Management Center)**에 자동으로 알림이 전달됩니다. FMC는 **ISE(Identity Services Engine)**에 Bob의 PC를 격리하라고 지시하여 즉시 조치를 취했습니다. Cisco ISE는 **ASA(Adaptive Security Appliance)**에 RADIUS CoA(권한 변경)를 전송하여 Bob의 세션을 즉시 해제하라고 지시합니다.

또한, 이제 ISE에서 Bob의 머신을 격리하도록 표시했습니다. 다음에 Bob이 다시 로그인하면 격리된 호스트로 확인되며 격리된 **TrustSec SGT(Security Group Tag)가 할당됩니다.** 격리된 SGT는 Bob이 문제를 해결하는 데 필요한 필수 네트워크 리소스에만 액세스할 수 있도록 합니다. Bob은 나머지 네트워크에서 효과적으로 격리되므로, 문제가 완전히 해결될 때까지 추가적인 피해가 발생하지 않습니다. 이 데모에서, ISE에서 할당한 SGT 태그는 WSA 및 Nexus 1000v 데이터센터 스위치 같은 다른 어플라이언스와 실시간으로 자동 공유됩니다. 이로 인해 ISE에서 할당한 정책을 네트워크의 모든 곳에서 시행할 수 있습니다. TrustSec가 전체 구축된 실제 환경에서는 전체 인프라에 걸쳐 이러한 태그를 공유하여 전체 인프라에서 실시간으로 액세스 권한을 업데이트하고 시행할 수 있습니다.

그림 57. AnyConnect 자동 연결 끊김

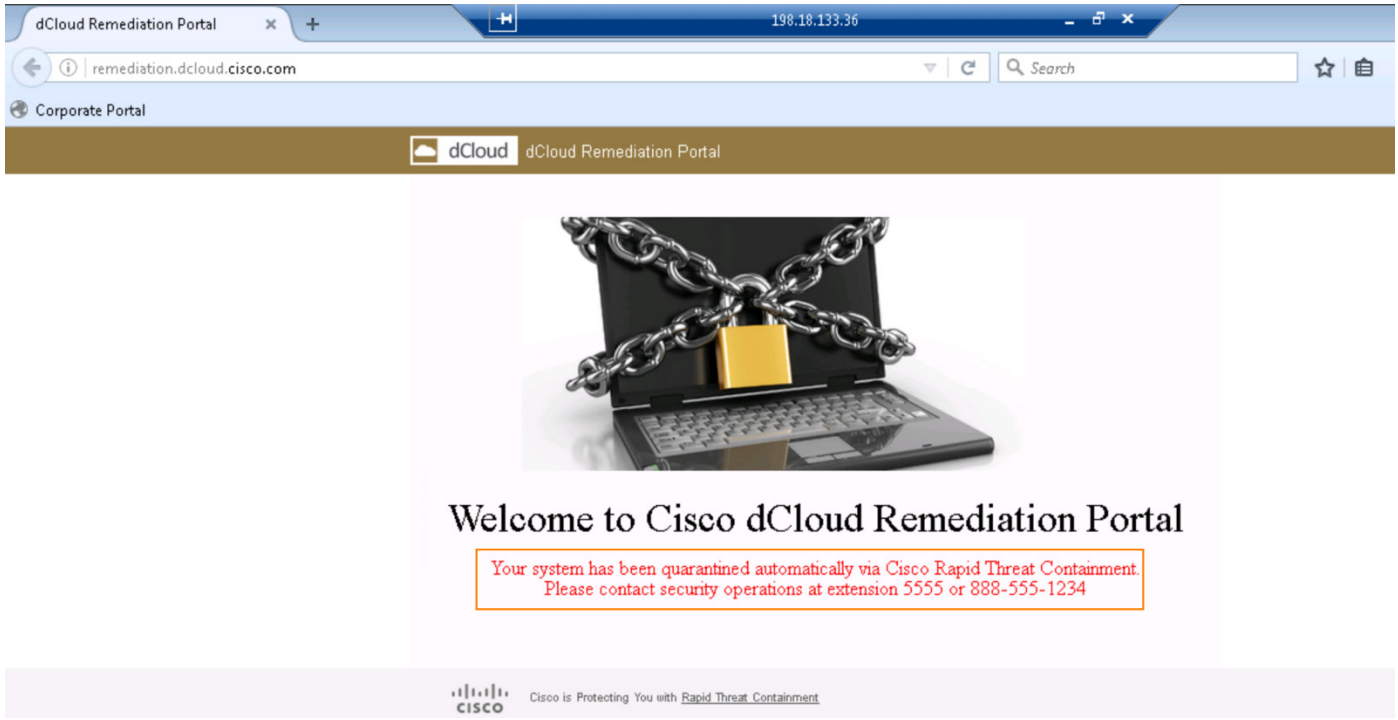
18. Connect(연결)를 클릭하여 네트워크에 다시 로그인하고 비밀번호 C1sco12345를 입력한 후 OK(확인)를 클릭합니다.

그림 58. AnyConnect 로그인



19. Firefox 브라우저를 열면 Cisco Rapid Threat Containment에 의해 Bob의 컴퓨터가 기업 네트워크에서 격리된 것을 알 수 있습니다.

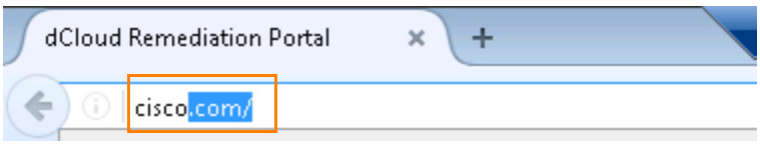
그림 59. Rapid Threat Containment 격리 메시지



20. cisco.com을 입력하여 다른 웹 페이지로 이동해봅니다. Rapid Threat Containment는 다른 웹 페이지에 액세스하는 것을 허용하지 않으며, dCloud Remediation Portal 페이지만 열립니다.

참고: Bob의 머신은 이제 ISE에서 격리된 것으로 분류됩니다. 격리된 정책에 따라 Bob은 기업 치료 포털 및 향후 정리를 위해 **AMP for Endpoints**에서 요구하는 필수 서비스에만 액세스할 수 있습니다. 이 단계에서, Bob은 보안 운영 센터에 문의하게 되며 공격 후 단계가 개시됩니다. 네트워크 보안 분석가가 Bob의 머신을 정리하고 네트워크에 다시 연결될 수 있도록 지원하는 단계를 시작합니다.

그림 60. dCloud 치료 포털 및 > Cisco.com



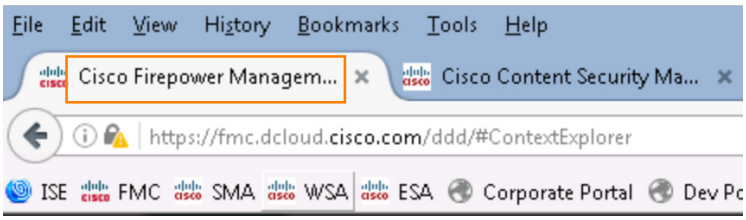
시나리오 6. 공격 후: 분석 및 정리

마지막 시나리오에서 Bob의 머신이 감염되고 자동으로 격리되자, Bob은 보안 운영 팀에 문의하라는 안내를 받게 되었습니다. 이제 Bob이 보안 운영 팀에 문의했으며, 네트워크 보안 분석가가 되어 어떤 문제가 발생했는지 정확하게 검사하고, Bob의 머신을 정리하여 네트워크에 다시 연결할 수 있도록 지원하겠습니다.

단계

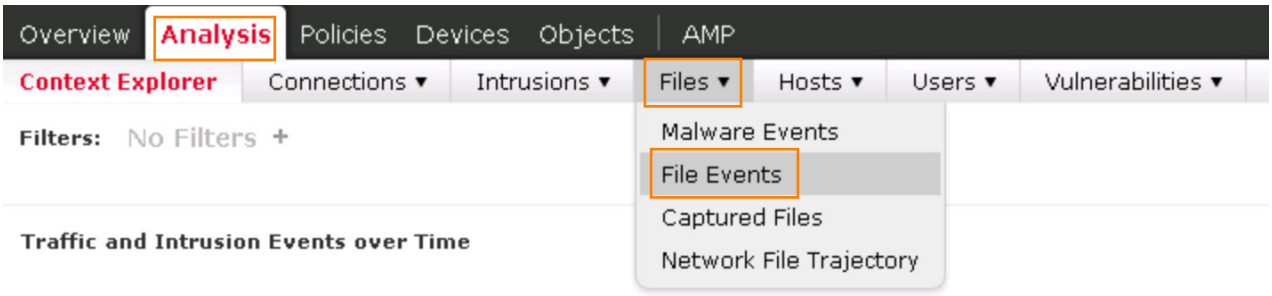
1. Jumper PC로 다시 이동하여 Firefox의 FMC(Firepower Management Center) 탭으로 돌아갑니다.

그림 61. FMC



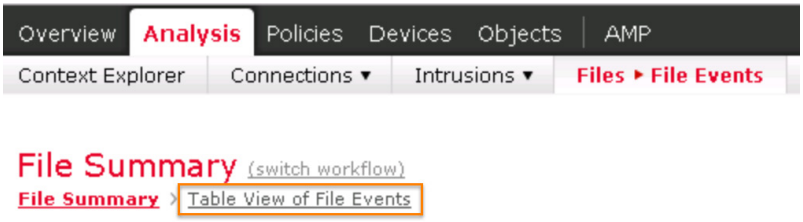
2. **Analysis(분석)** 메뉴 탭에서 Files(파일)를 클릭하고 드롭다운 메뉴에서 File Events(파일 이벤트)를 선택합니다.

그림 62. 파일 > 파일 이벤트



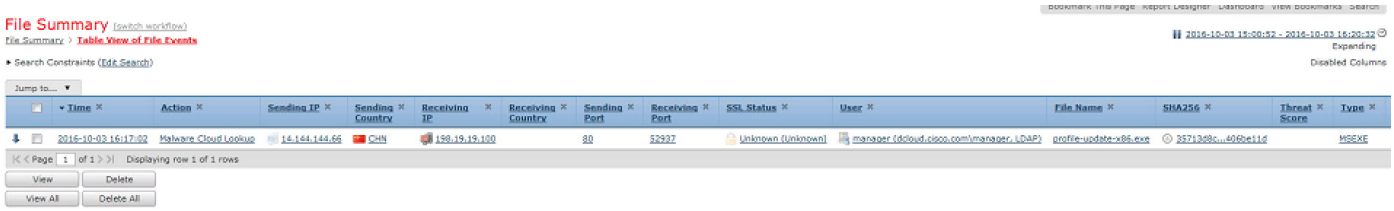
3. **Table View of File Events(파일 이벤트 테이블 보기)**를 클릭합니다.

그림 63. 파일 이벤트 테이블 보기



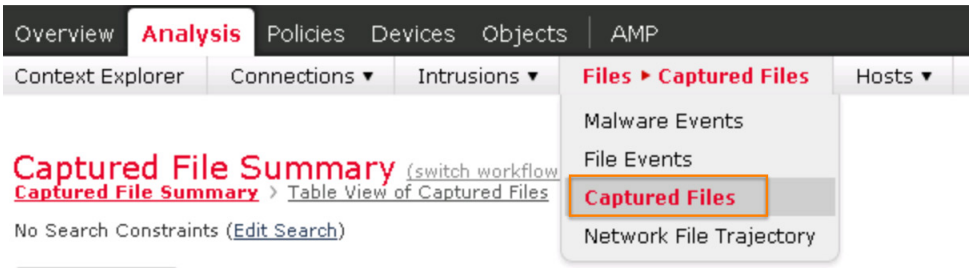
4. 보안 분석가는 알려지지 않은 악성코드였기 때문에 제로 데이 악성코드가 다운로드된 것을 확인할 수 있습니다. File Events(파일 이벤트) 요약에서 보안 분석가는 알려지지 않은 파일의 발원지가 중국이라는 사실과 네트워크에서 격리된 컴퓨터의 정확한 사용자 세부사항을 확인할 수 있습니다. 지금은 파일 상태가 "unknown(알 수 없음)"으로 표시됩니다.

그림 64. FMC 파일 이벤트 요약



5. 그다음에는 **Files(파일)** 메뉴에서 **Captured Files(캡처된 파일)**를 선택합니다.

그림 65. 파일 > 캡처된 파일



6. **Table View of Captured Files(캡처된 파일 테이블 보기)**를 클릭합니다.

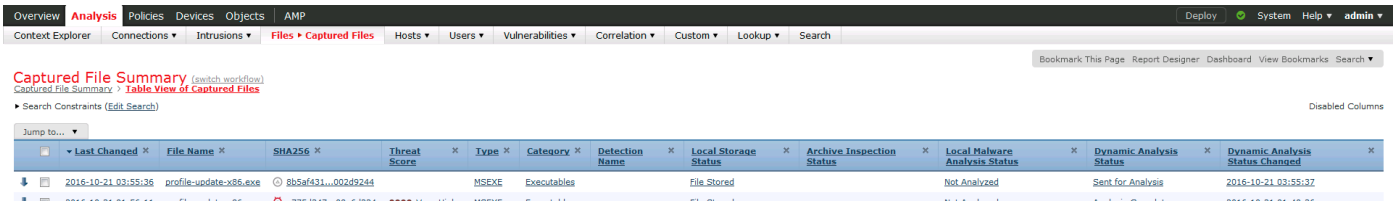
그림 66. 캡처된 파일의 테이블 보기

7. 보안 분석가는 당시에 알려지지 않은 파일이었기 때문에 제로 데이 파일이 다운로드되었으며, FMC에도 저장되었고 동적 분석을 위해 Cisco ThreatGrid에 제출된 사실을 확인할 수 있습니다. 이 시점에는 파일에 위협 점수가 없으며 동적 분석을 위해 제출되었다고 표시됩니다. 단계가 진행됨에 따라 상태가 변경되는 것을 확인할 수 있습니다.

참고: Bob의 머신을 감염시킨 제로 데이 악성 파일은 다운로드 당시 알려지지 않은 파일이었기 때문에 다운로드가 가능했습니다. 그러나 Firepower Management Center에서는 이 파일을 저장한 후 분석을 위해 **ThreatGrid** 클라우드에 동적으로 제출했습니다. 이번에는 악성 파일이 클라우드의 샌드박스 환경에서 실행되고 분석됩니다. 이 파일은 매우 심각한 악성 파일이므로 **ThreatGrid**에서 매우 높은 위협 점수를 지정하여 해당 파일을 신속하게 반환합니다. 매우 높은 위협 점수와 함께 파일이 반환되면 네트워크에서 동일한 파일이 다시 허용하지 않습니다. 이 단계가 되면 AMP를 구현하는 Cisco 보안 포트폴리오 전체의 모든 제품(WSA, ESA, FMC, AMP for Endpoints 포함)이 해당 파일을 탐지하고 차단할 수 있습니다.

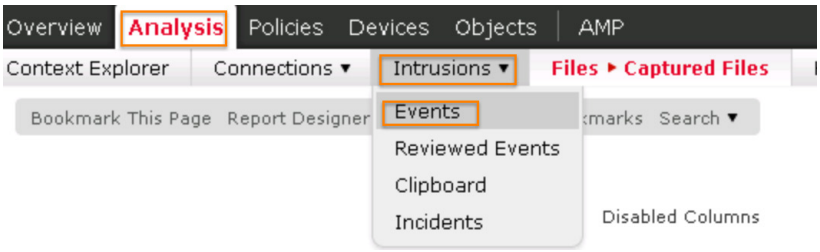
파일이 동적으로 제출되고 실시간으로 분석되므로 약간의 시간이 소요될 수 있습니다. 일반적으로 ThreatGrid가 매우 높은 위협 점수와 함께 파일을 반환하기까지 약 10분 정도가 소요됩니다. 그동안, 여기서 정확히 어떤 일이 발생했는지를 계속 분석해보겠습니다.

그림 67. 캡처 파일 요약



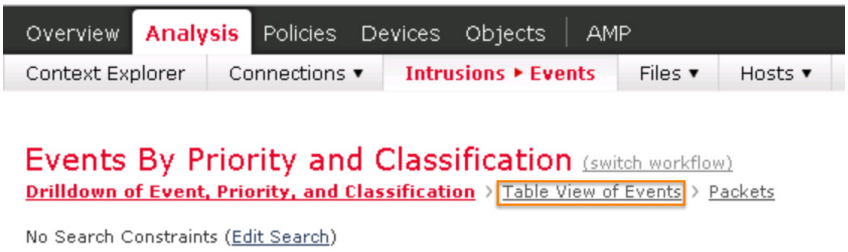
8. **Analysis(분석)** 메뉴 아래의 **Intrusions(침입)** 탭으로 스크롤한 후 **Events(이벤트)**를 클릭합니다.

그림 68. 침입 > 이벤트

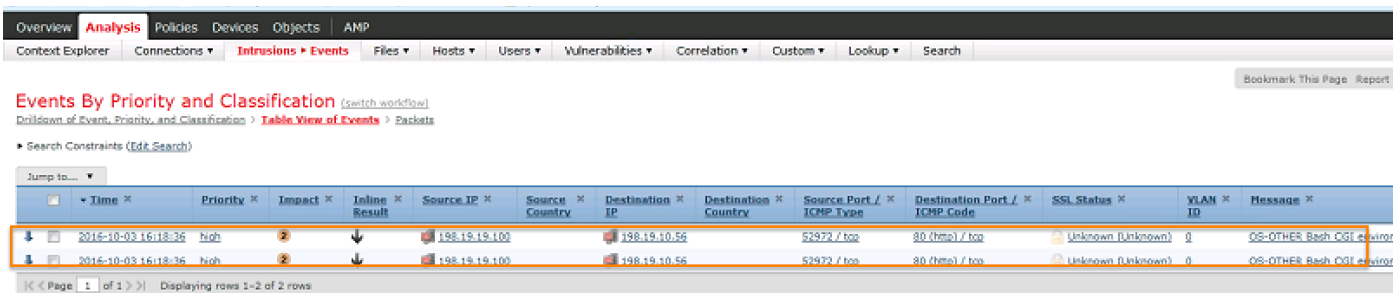


9. **Table View of Events(이벤트 테이블 보기)**를 클릭합니다.

그림 69. 이벤트 테이블 보기

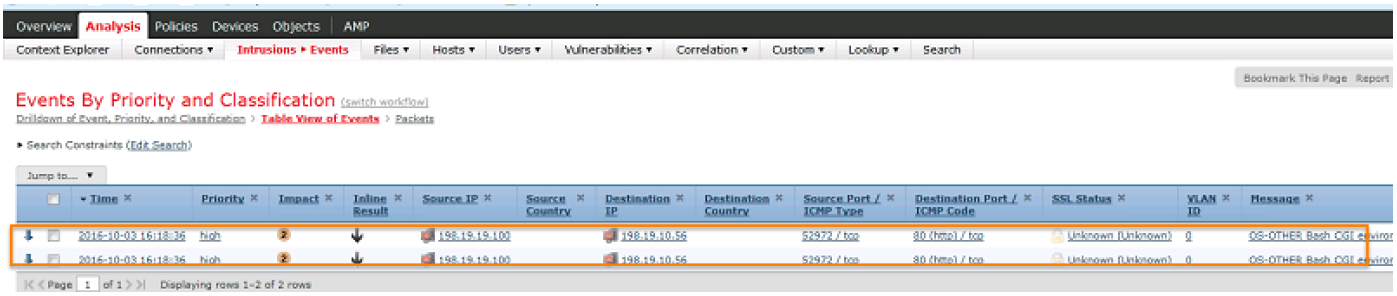


10. 보안 분석가는 두 번의 침입 이벤트가 발생했으며, 해커가 Bob의 워크스테이션을 구심점으로 활용하여 네트워크 내부의 웹 서버를 장악하려고 시도한 사실을 확인할 수 있습니다. 그러나 해커의 이러한 시도로 인해 Cisco Firepower Threat Defense의 일부인 Intrusion Prevention System이 작동되었습니다.



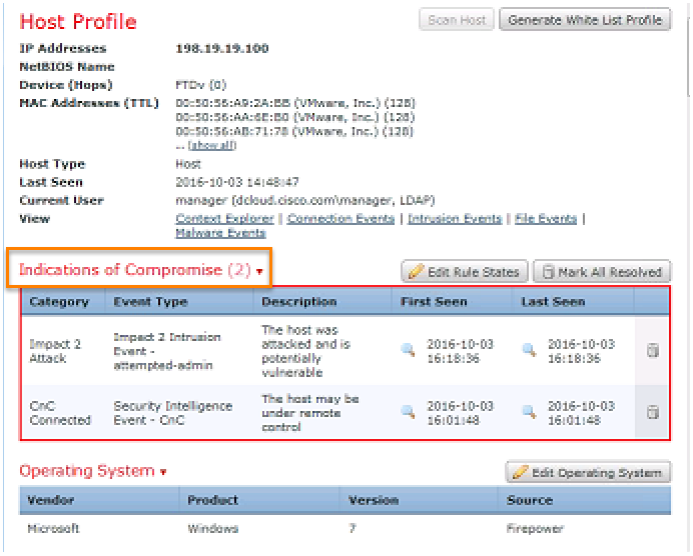
11. 오른쪽으로 스크롤하여 보안 분석가가 Intrusion Event(침입 이벤트)를 통해 확인한 자세한 정보를 살펴봅니다. Source IP(소스 IP)에는 Bob의 컴퓨터 IP가 표시되고, Destination IP(대상 IP)에는 분석가가 공격의 시작부터 끝까지 추적할 수 있는 네트워크 웹 포털 서버의 IP 주소가 표시됩니다. Message(메시지) 열에는 해커가 익스플로잇을 실행하려고 했으며, 그 결과 Firepower에서 사용자를 격리했다고 표시됩니다.

그림 70. 침입 > 이벤트 테이블 보기



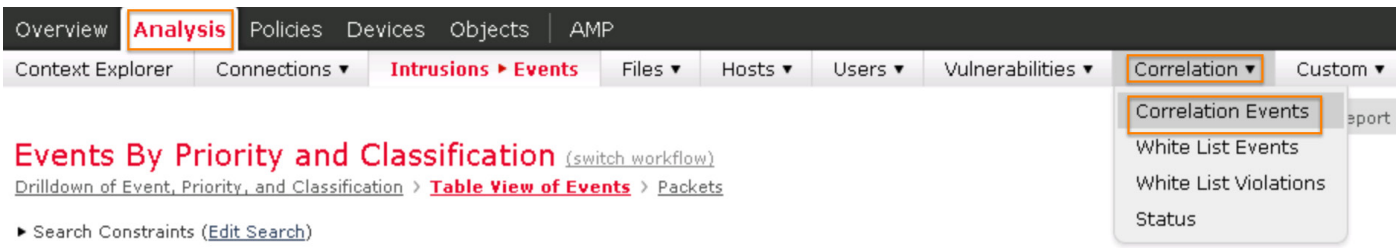
12. Source IP(소스 IP) 주소 옆의 컴퓨터 아이콘을 클릭하여 Host Profile(호스트 프로파일) 창을 엽니다. 보안 분석가는 보안 침해가 발생했을 수 있다는 최초 경고부터 격리의 원인이 된 호스트 공격에 이르기까지 침입의 세부사항을 볼 수 있습니다.

그림 71. 호스트 프로파일 > 보안 침해 지표

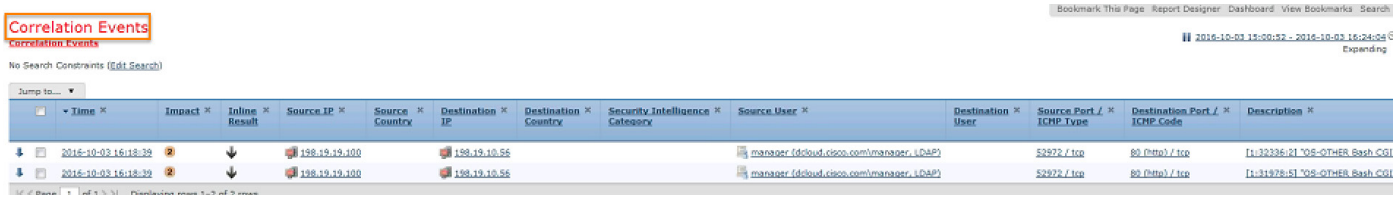


13. Analysis(분석) 메뉴 아래에서 Correlation(상관관계)을 클릭하고 드롭다운 메뉴에서 Correlation Events(상관관계 이벤트)를 선택합니다.

그림 72. 상관관계 메뉴

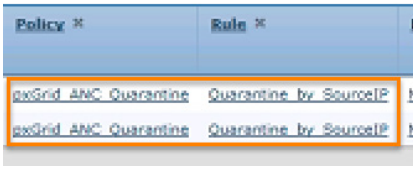


14. Correlation Events(상관관계 이벤트) 세부사항을 확인합니다.



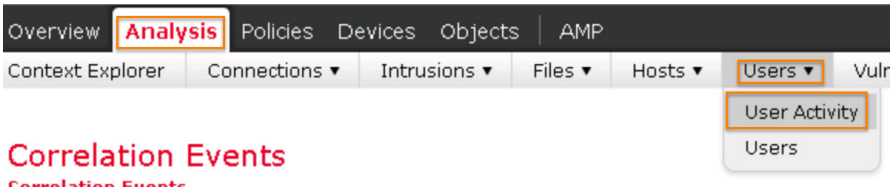
15. 오른쪽으로 스크롤하여 **Policy(정책)** 및 **Rule(규칙)** 열을 확인합니다. 여기서 VPN의 특정 머신이 감염되었다는 정보를 Firepower가 ISE에 전달한 것을 알 수 있습니다. 그다음 Firepower는 pxGrid를 통해 ISE와 통신하고, **Quarantine by Source IP(소스 IP를 기준으로 격리)** 규칙으로 구현된 ISE 정책이 Bob의 컴퓨터를 네트워크에서 제거합니다.

그림 73. 상관관계 이벤트 > 정책 및 규칙 세부사항



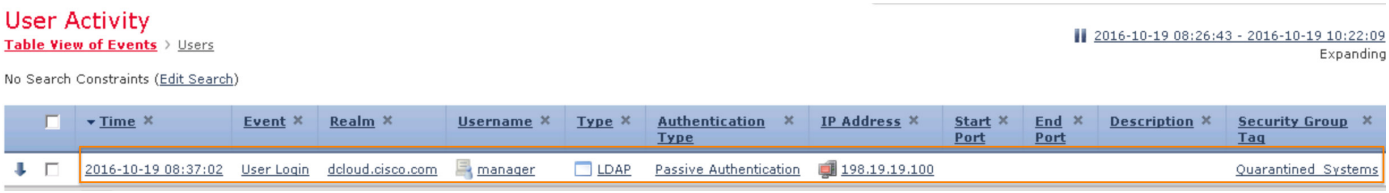
16. 소스 IP를 기준으로 Bob의 컴퓨터를 격리한 후 다음 단계는 사용자 Bob의 액세스 정책을 업데이트하는 것입니다. Analysis(분석) 메뉴 아래에서 **Users(사용자)**를 클릭하고 드롭다운 메뉴에서 **User Activity(사용자 활동)**를 선택합니다.

그림 74. 사용자 > 사용자 활동



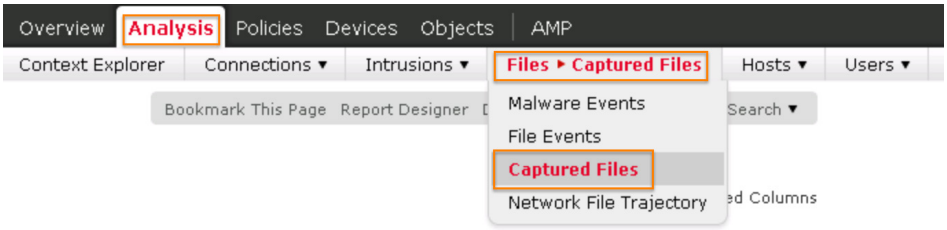
17. User Activity(사용자 활동) 세부사항을 확인합니다. 보안 분석가는 Bob의 새로운 액세스 정책에 의해 Bob이 **Quarantined Systems(격리된 시스템)**에 대한 Security Group(보안 그룹) 정책에 배치된 사실을 추적할 수 있습니다.

그림 75. 사용자 격리된 시스템 세부사항



18. 이제 보안 분석가가 공격에 대한 몇 가지 추가 조사를 마쳤으며, **Captured File Summary(캡처된 파일 요약)**로 돌아가 ThreatGrid에서 동적 분석이 반환되었는지 확인합니다.

그림 76. 캡처된 파일 요약



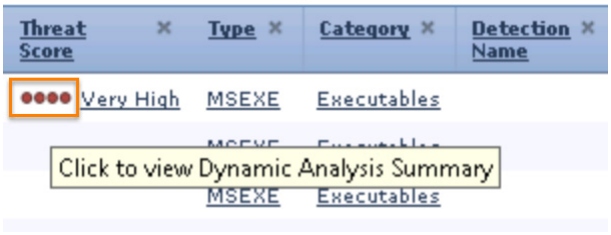
참고: Dynamic Analysis Status(동적 분석 상태) 업데이트를 완료하는 데 소요되는 시간은 일반적으로 10분 미만이지만, 현재 데모 환경에 따라 달라질 수 있습니다. 데모의 나머지 부분으로 넘어가기 전에 Dynamic Analysis(동적 분석)를 완료해야 합니다. 매우 높은 위협 점수가 지정된된 Analysis Complete(분석 완료) 상태가 아닐 경우 다음 단계를 계속 진행하기 전에 업데이트될 때까지 기다리십시오.

19. **Capture File Summary(캡처 파일 요약)** 테이블 보기에서 오른쪽으로 스크롤하여 **Dynamic Analysis Status(동적 분석 상태)** 열을 찾습니다. 새로운 상태가 **Analysis Complete(분석 완료)**인지 확인합니다. 이제 위협 점수가 Very High(매우 높음)로 표시됩니다.

그림 77. 동적 분석 상태

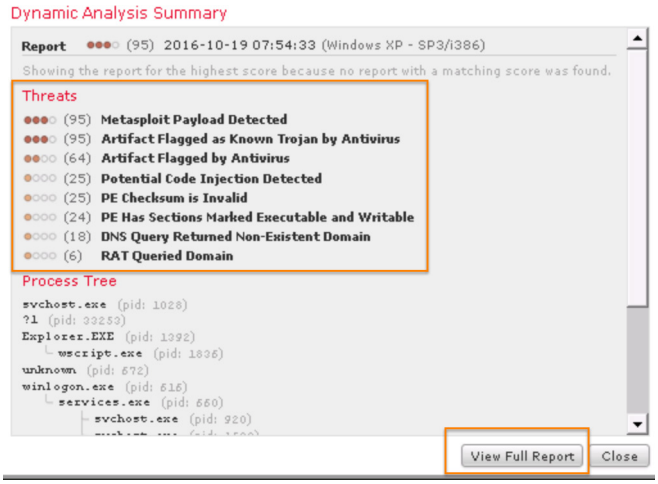
20. 실행 파일의 위협 수준이 **Very High(매우 높음)**으로 표시되는 **Threat Score(위협 점수)** 열에서 빨간색 원 4개를 클릭하여 Dynamic Analysis Summary(동적 분석 요약) 세부사항을 확인합니다.

그림 78. 높은 위협 점수 > 동적 분석 요약

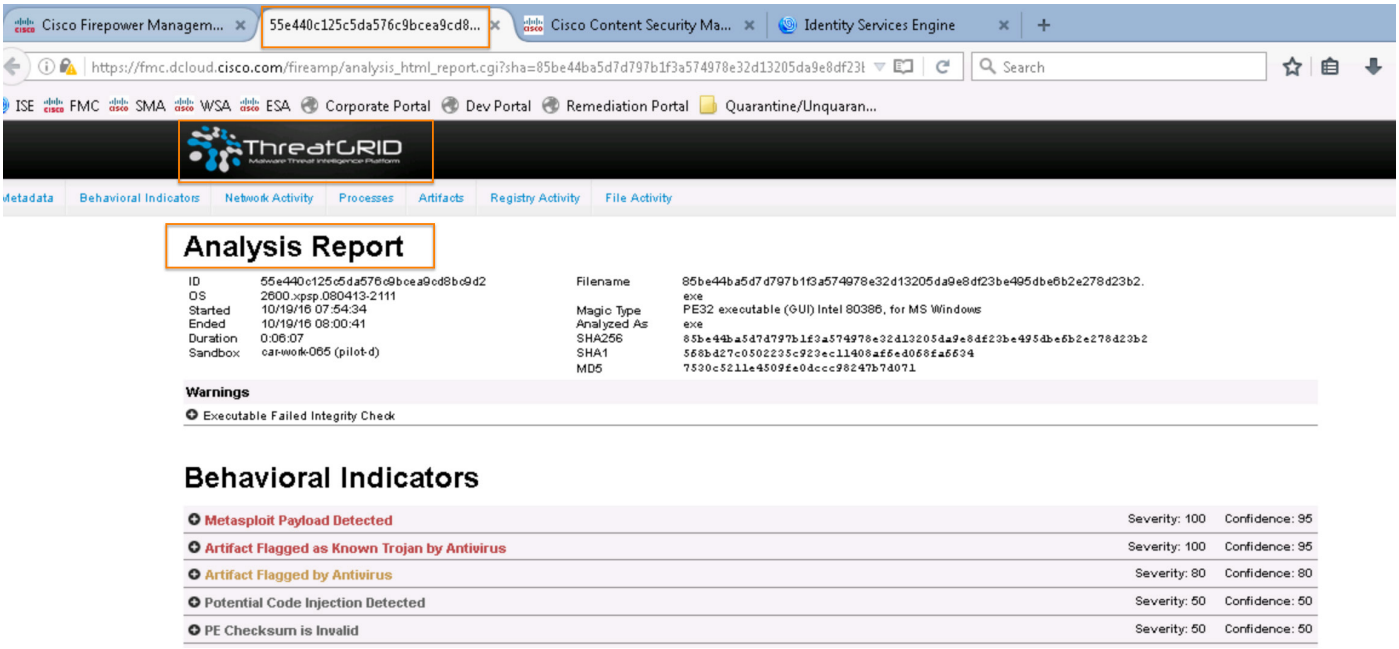


21. 요약에서 일부 위협 세부사항을 제공하지만 분석가는 **View Full Report(전체 보고서 보기)**를 클릭할 수도 있습니다.

그림 79. Dynamic Analysis Summary(동적 분석 요약)

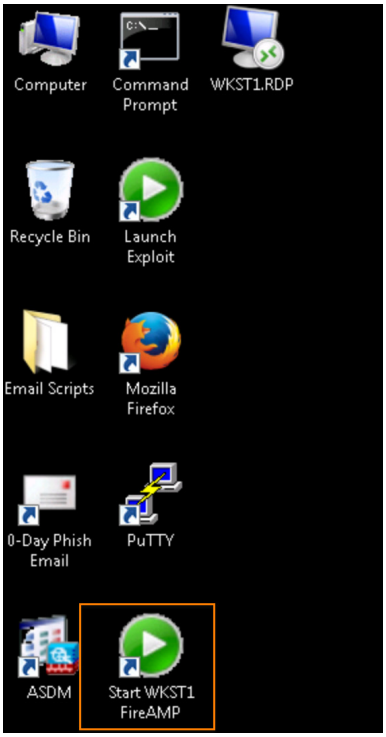


22. 새 탭이 열리고, 이제 보안 분석가가 ThreatGrid의 전체 **Analysis Report(분석 보고서)**를 볼 수 있습니다.



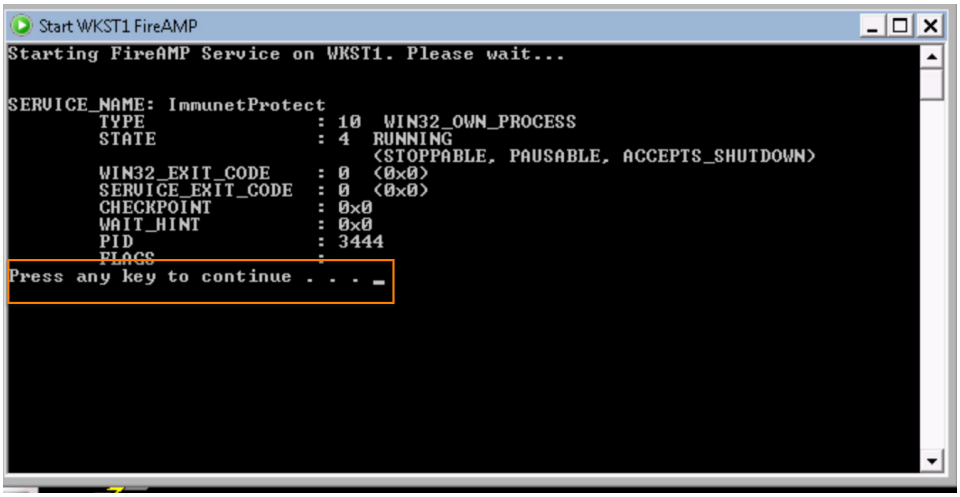
23. Jumper PC 바탕화면에서 **Start WKST1 FireAMP(WKST1 FireAMP 시작)** 바로가기를 더블 클릭하여 Workstation1에서 AMP for Endpoints 서비스를 시작합니다.

그림 80. WKST1 FireAMP 시작 바탕화면 바로가기



24. 열린 창의 지침을 따르고, 계속하려면 아무 키나 누릅니다.

그림 81. WKST1 FireAMP 스크립트 시작

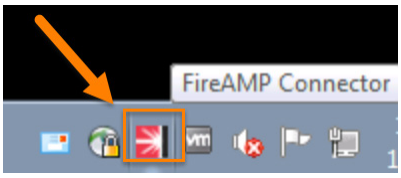


25. 아래쪽 트레이 메뉴에서 아이콘을 클릭하고, Workstation1로 돌아갑니다. 열려 있는 모든 브라우저를 닫습니다.

그림 82. Workstation1 바로가기

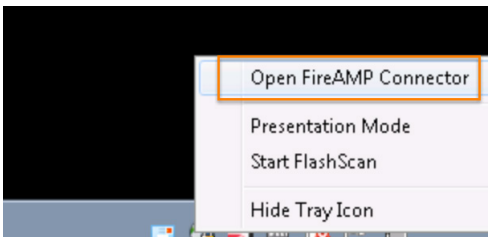
26. Workstation1의 아래쪽 트레이 메뉴에서 FireAMP Connector 아이콘을 찾아 마우스 오른쪽 버튼으로 클릭합니다.

그림 83. FireAMP Connector



27. 마우스 오른쪽 버튼으로 클릭한 후 메뉴에서 Open FireAMP Connector(FireAMP Connector 열기)를 선택합니다.

그림 84. FireAMP Connector 열기



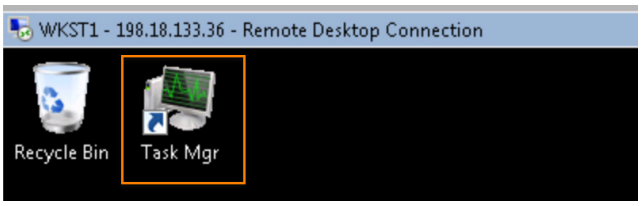
28. Sourcefire에 녹색 체크 마크가 표시되어 있고 상태가 연결됨인지 확인합니다.

> **참고:** Bob의 머신은 격리되었으며 프로덕션 네트워크에서 제외되었습니다. 그러나 의도적 설정에 따라 Bob은 치료 포털 및 AMP 클라우드에 액세스할 수 있으므로, AMP for Endpoints에서 짧은 시간 내에 Bob의 머신을 정리하고 다시 온라인에 완전히 액세스할 수 있도록 지원합니다.

그림 85. Sourcefire 상태 연결됨

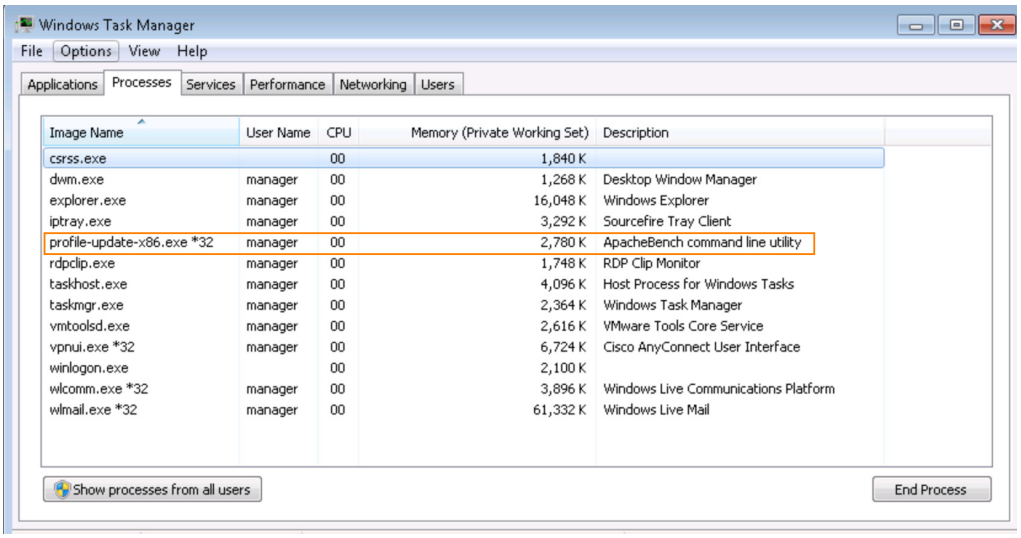
29. 그다음, 작업 관리자를 엽니다.

그림 86. 작업 관리자 바탕화면 바로가기



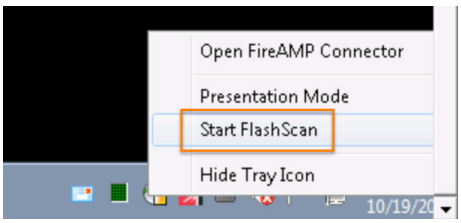
30. 해커의 파일이 Bob의 컴퓨터에 아직 있는지 확인합니다.

그림 87. 공격 파일이 있는 작업 관리자



31. 아래쪽 트레이 메뉴에서 FireAMP 아이콘을 마우스 오른쪽 버튼으로 클릭하고 Start FlashScan(FlashScan 시작)을 선택합니다.

그림 88. FlashScan 시작

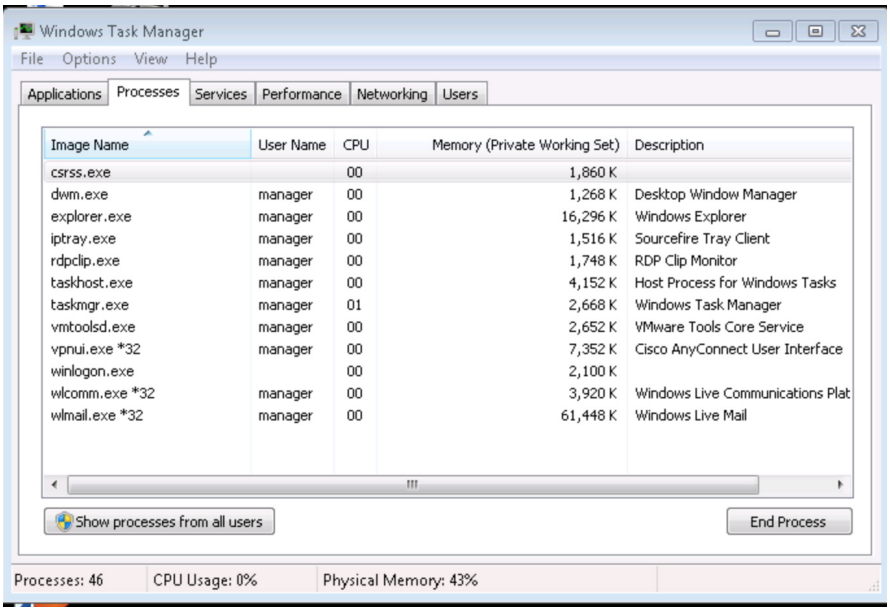


32. FireAMP FlashScan에서 위협을 발견했습니다.

> **참고:** 이 플래시 스캔 프로세스에서 파일을 완료하고 격리하는 데 최대 1분 정도 소요될 수 있습니다. 어떠한 이유로든 악성 파일이 작업 관리자에서 더 이상 실행되지 않을 경우, 플래시 스캔은 파일을 격리하지 않습니다. 플래시 스캔은 전체 디스크 스캔이 아닌 머신의 특정 영역을 매우 신속하게 스캔하는 작업만 수행하기 때문입니다.

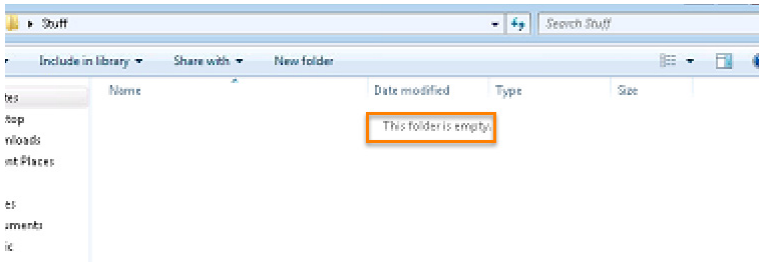
33. 작업 관리자로 돌아가면 프로세스 목록에 공격 파일이 더 이상 존재하지 않는 것을 알 수 있습니다.

그림 89. 공격 파일이 제거된 작업 관리자



34. 작업 관리자 및 모든 FireAMP/SourceFire 창을 닫습니다. 그다음, 바탕화면의 **Stuff** 폴더를 열고 폴더에서 실행 파일이 제거되었는지 확인합니다. 이 파일은 FireAMP에 의해 완전히 격리되었습니다.

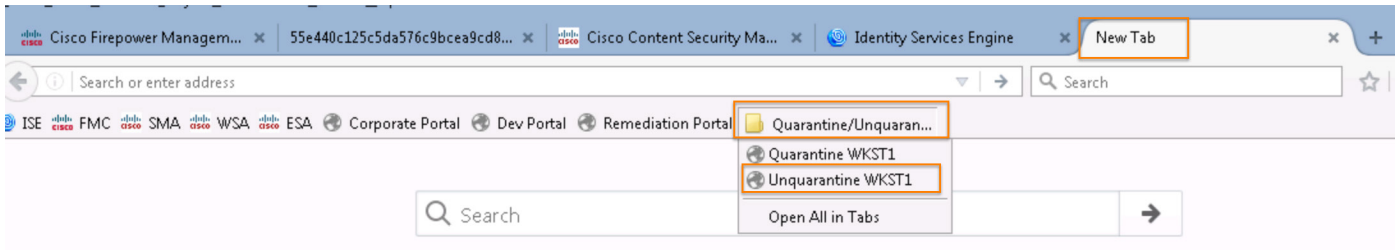
그림 90. 공격 파일 제거됨



35. Jumper PC로 돌아간 후 Firefox 브라우저에서 새 탭을 엽니다. **Quarantine/Unquarantine(격리/격리 해제)** 북마크를 클릭하고 드롭다운 메뉴에서 Unquarantine WKST1(WKST1 격리 해제)을 선택합니다.

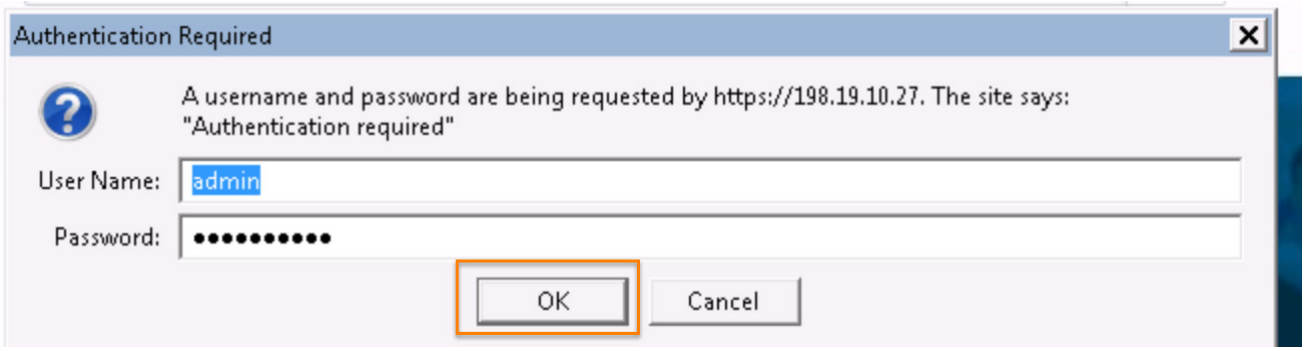
참고: 이제 AMP for Endpoints가 Bob의 시스템을 감염시킨 악성코드를 정리했으며, 분석가는 해당 머신을 네트워크에서 다시 허용할 수 있습니다. Jumper PC의 Unquarantine(격리 해제) 북마크는 ISE에 대한 REST API 호출을 활용하여 ISE에 Bob의 머신에 대한 격리를 해제하도록 지시합니다. 그 결과, ISE는 RADIUS CoA(Change of Authorization)를 전송하여 ASA(Adaptive Security Appliance)에 Bob의 세션 연결을 끊도록 지시하고 Bob의 머신 상태도 업데이트합니다. 다음에 Bob이 연결하면 Employees SGT(Security Group Tag)가 다시 할당되며 네트워크에 다시 완전히 액세스할 수 있습니다.

그림 91. WKST1 격리 해제



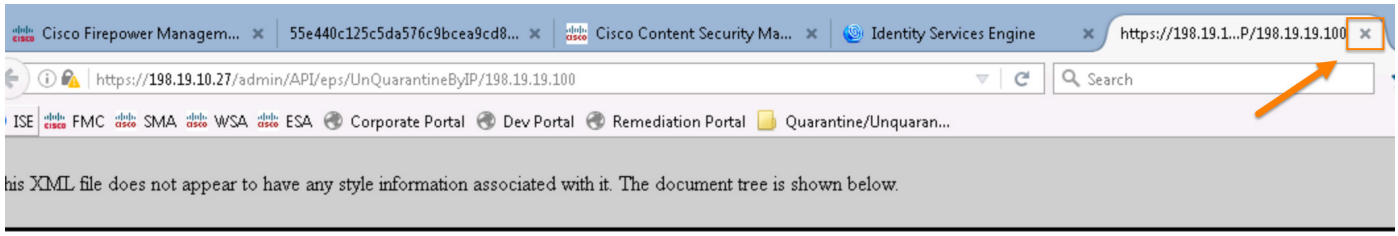
36. Authentication Required(인증 필요) 창에서 **OK(확인)**를 클릭하여 사용자 이름 **admin**, 비밀번호 **C1sco12345**로 인증합니다.

그림 92. 인증 필요



37. Workstation1에 대한 격리 해제 프로세스가 완료되면 탭을 닫고 워크스테이션으로 돌아갑니다.

그림 93. Wkst1 격리 해제 프로세스



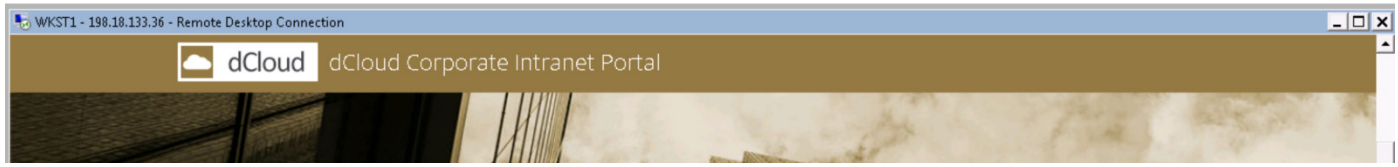

```
<EPS_RESULT>
  <operationID>2</operationID>
  <status>Pending</status>
  <requestID>-1</requestID>
  <errorCode>0</errorCode>
</EPS_RESULT>
```

38. 앞서 액세스 권한을 변경했으므로 VPN에 액세스할 수 없게 되었습니다. 사용자 이름 **manager**, 비밀번호 **C1sco12345**로 AnyConnect VPN에 다시 로그인합니다.

그림 94. VPN 연결

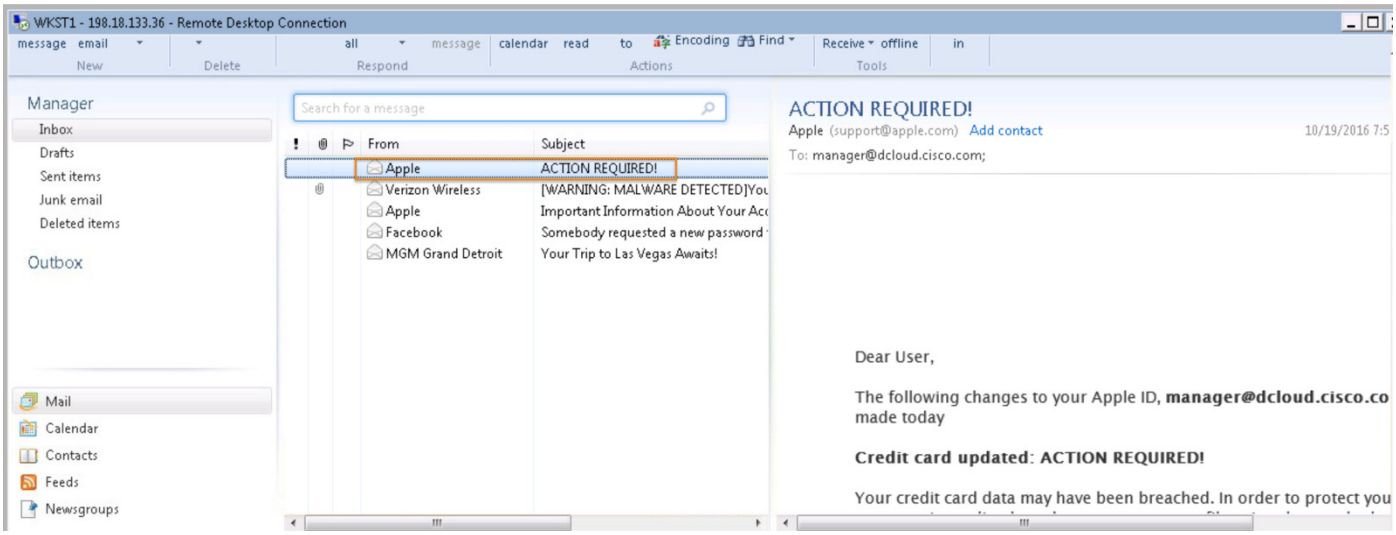
39. VPN이 연결되면 Firefox 브라우저를 엽니다. 이제 악성 파일이 제거되었으며 Workstation1이 더 이상 격리되지 않으므로, Bob은 자신의 컴퓨터에서 기업 포털에 다시 액세스할 수 있습니다.

그림 95. 기업 포털 액세스



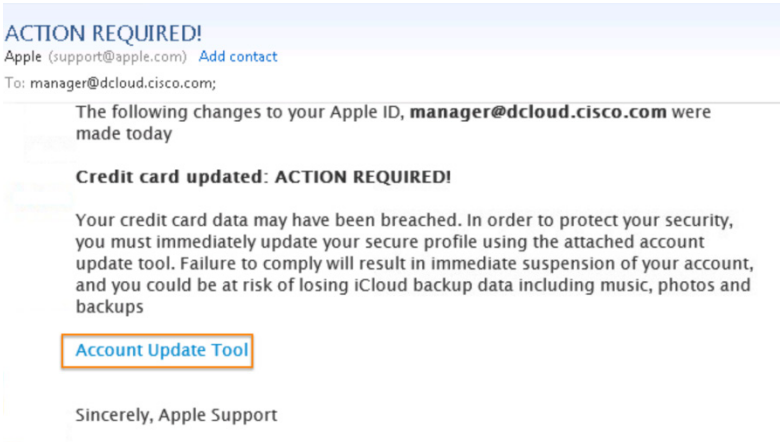
40. Bob의 이메일 받은 편지함으로 돌아가 Apple의 제로 데이 이메일을 다시 엽니다.

그림 96. Apple 제로 데이 이메일

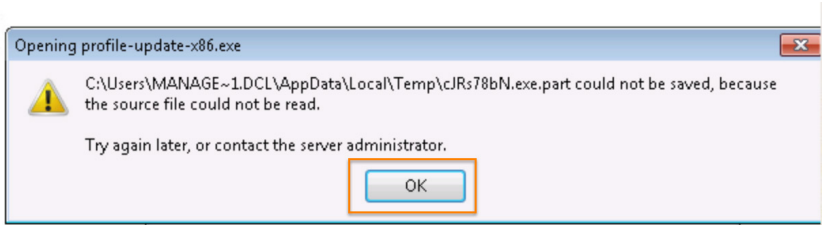


41. 이메일에서 **Account Update Tool(계정 업데이트 툴)** 링크를 다시 클릭합니다.

그림 97. 제로 데이 계정 업데이트 툴 링크



42. 이번에는 Security 툴이 해당 파일을 확인하여 Bob 또는 네트워크의 다른 사용자가 파일을 다시 다운로드하지 못하도록 합니다. OK(확인)를 클릭하여 창을 닫습니다.



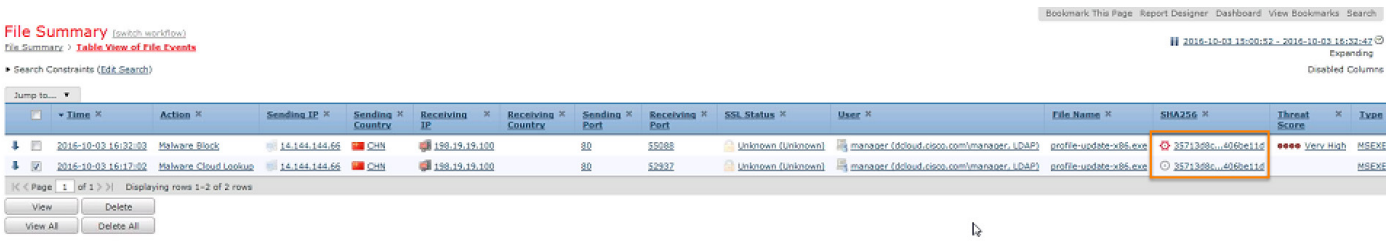
참고: 파일을 처음 다운로드했을 당시에는 알려지지 않은 파일이었으며, 동적 분석을 위해 ThreatGrid에 제출되었습니다. ThreatGrid에서 파일이 악성 파일로 확인되었으므로 이제 AMP가 이 파일에 대한 "조치를 변경"할 수 있습니다. 이제 이 파일은 알려진 악성코드로 확인되며, 앞으로 해당 파일을 다운로드하거나 실행하려는 모든 시도는 차단됩니다. 이 단계에서는 AMP를 실행하는 조직 전체 PC의 AMP for Endpoints 및 FMC, ESA, WSA의 AMP for Networks가 해당 파일을 차단합니다. 이러한 모든 작업은 자동 및 실시간으로 이루어집니다.

43. Jumper PC로 돌아가 **Firepower** 창을 엽니다. **Analysis(분석)** 메뉴 탭에서 **Files(파일)**를 클릭하고 드롭다운 메뉴에서 **File Events(파일 이벤트)**를 선택합니다.

그림 98. 파일 > 파일 이벤트

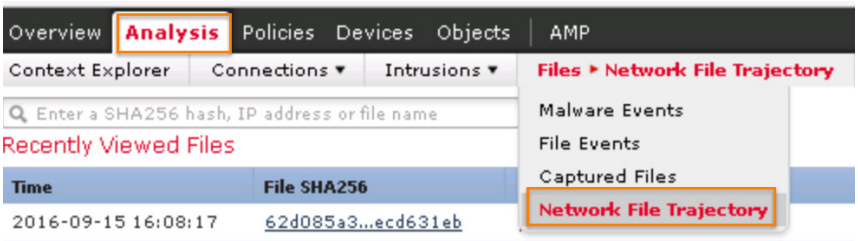
44. Table of View of File Events(파일 이벤트 테이블 보기)를 클릭합니다. 보안 분석가는 한때 알려지지 않았고 네트워크 컴퓨터에 액세스할 수 있었던 파일이 이제 악성코드로 확인되고 차단되는 것을 확인할 수 있습니다. SHA256의 마지막 몇 문자 확인

그림 99. 악성코드 차단됨



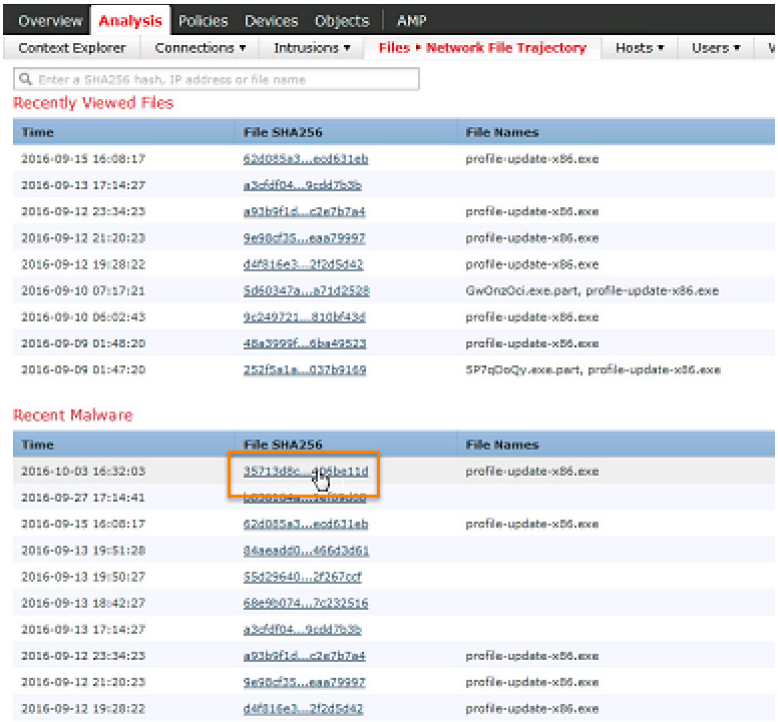
45. 그다음, Files(파일) 메뉴의 드롭다운 메뉴에서 Network File Trajectory(네트워크 파일 경로)를 선택합니다.

그림 100. 파일 > 네트워크 파일 경로



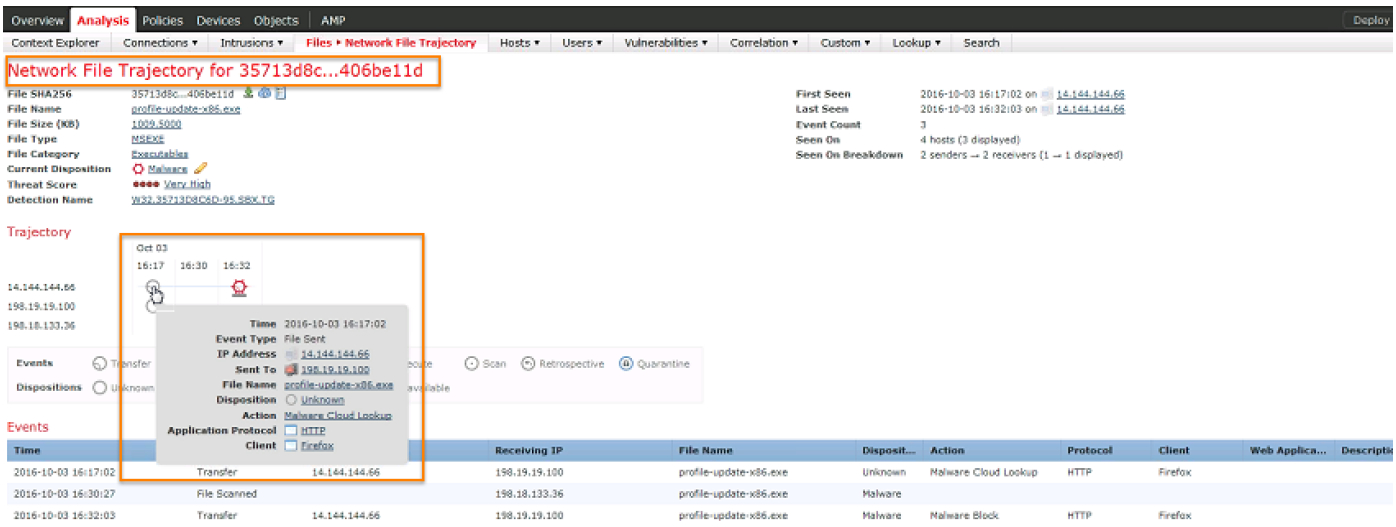
46. Recent Malware(최근 악성코드) 목록에서 최근에 확인되어 차단된 악성코드 파일의 SHA-256을 클릭합니다.

그림 101. 최근 악성코드



47. 알려지지 않은 파일이었을 때부터 위협 수준이 매우 높은 악성코드로 확인되었을 때까지 네트워크의 파일 경로 세부사항을 확인합니다.

그림 102. 네트워크 파일 경로 세부사항



참고: 네트워크 파일 경로를 보면 처음에 중국에 있는 공격자 웹 서버에서 Bob의 머신으로 파일이 다운로드된 것이 명확하게 나와 있습니다. 그다음에는 파일이 어떻게 실행되었고 결국 AMP for Endpoints에 의해 격리되었는지를 확인할 수 있습니다. 마지막으로, ThreatGrid에서 매우 높은 위협 점수와 함께 파일이 반환된 이후 나중에 파일을 다시 다운로드하려고 했을 때 AMP for Networks에서 파일을 차단한 것을 알 수 있습니다.

부록 A. 데모 정리

데모를 계속 실행하고 다시 단계를 반복하려면 시작하기 전에 데모 정리 단계를 따르십시오.

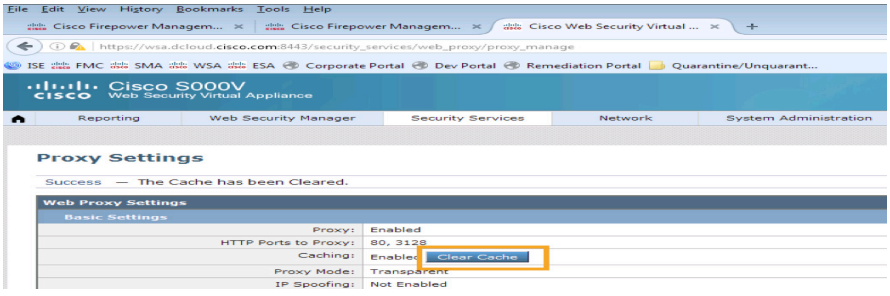
단계

1. WKST1의 악성 파일이 바탕화면의 Stuff 디렉토리에서 삭제되었는지 확인합니다. 모든 데모 단계를 수행한 경우 이 작업은 이미 완료되어 있습니다.
2. 작업 관리자를 통해 WKST1에서 악성 파일이 더 이상 실행되지 않는지 확인합니다. 모든 데모 단계를 수행한 경우 이 작업은 이미 완료되어 있습니다.
3. FireAMP Connector를 열고 설정을 클릭하여 WKST1에서 AMP for Endpoints 서비스를 비활성화합니다. 아래로 스크롤한 후 FireAMP Connector Settings(FireAMP Connector 설정)를 확장하고 서비스를 중지합니다. 필수 비밀번호는 C1sco12345입니다.
4. Analysis/Hosts/Indications of Compromise(분석/호스트/보안 침해 지표) 아래의 FMC에서 모든 호스트의 보안 침해 지표를 지웁니다.
5. MGM Grand(Umbrella)에서 보낸 것처럼 보이는 첫 번째 이메일을 제외하고 Bob의 받은 편지함에서 모든 이메일을 삭제합니다. 데모가 시작되면 공격자 박스를 리부팅할 때마다 시나리오 2~4의 이메일이 다시 전송됩니다. Jumper의 바탕화면에 있는 Email Scripts 폴더의 스크립트를 활용하여 해당 이메일을 직접 보낼 수도 있습니다. 동일한 경험을 하려면 스크립트를 다음 순서로 실행하십시오.
    a. Sec Int Phish Email
    b. Known Malware Phish Email
    c. Known Malware Attachment Email

    참고 Jumper 바탕화면의 0 day Phish Email 스크립트는 실행할 때마다 고유한 악성코드를 생성합니다. 데모를 다시 실행할 경우, 처음 실행할 때 생성된 제로 데이 링크가 포함된 이메일을 삭제하고 스크립트를 다시 실행해야 합니다. 이렇게 해야 새로운 제로 데이 악성코드가 생성되고 이메일로 전송됩니다. 그렇지 않으면 시스템에서 이전에 사용한 파일을 알려진 악성코드로 확인하므로 데모가 의도한 대로 실행되지 않습니다.
6. WKST1이 격리 해제된 상태인지 확인합니다. 모든 데모 단계를 수행한 경우 이 작업은 이미 완료되어 있습니다.

4. WSA의 웹 캐시를 지웁니다. 이 작업은 Jumper PC에서 수행할 수 있습니다. Firefox에서 새 탭을 연 다음, 북마크 툴바에서 WSA 북마크를 클릭합니다. WSA에 로그인하고 보안 서비스/웹 프록시로 이동한 후 캐시 지우기 버튼을 클릭합니다.

그림 103. WSA 웹 프록시 설정 – 캐시 지우기



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, 전화번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.