

Cisco Umbrella Lab v2.2



Cloud Security TME Team 과의 파트너십을 통해 만들어집니다.

마지막 업데이트 2019 년 2 월 20 일

본 데모에 대하여

Cisco SE, Cisco Partner SE 및 고객은 Umbrella 및 Umbrella Investigate 와 같은 Umbrella 의 시행 및 인텔리전스 제품의 가치를 구축하고 시연하는 방법을 배울 수 있습니다. 이 실습에서는 Umbrella 의 초기 구축과 Umbrella 보고에 대한 섹션 및 Umbrella Investment 의 위협 인텔리전스를 다룹니다.

이 실습이 완료되면 SE 와 고객은 Umbrella 솔루션을 성공적으로 구현 및 운영할 수 있으며, 이러한 솔루션의 작동 방식과 이점에 대해 잘 이해할 수 있습니다.

중요: 이 실습을 완료에 대한 적절한 평가를 받으려면, 실습의 [시나리오 1 의 Exercises 1-5](#) 를 완료한 [요기](#)에 표시된 단계를 따라 주십시오. 이 단계는 이메일을 통해 증명서를 제출하는 것으로 마무리됩니다.

본 데모 가이드에는 아래의 내용을 포함합니다:

- [본 데모에 대하여](#)
- [제안 사항](#)
- [커스터마이징 옵션](#)
- [필요사항](#)
- [솔루션에 대하여](#)
- [구성도](#)
- [시작하기](#)
- [시나리오 1. Umbrella 구축, Policies 생성 및 Activity 만들기](#)
- [시나리오 2. 보고\(Reporting\)](#)

- [시나리오 3. Umbrella Investigate](#)
- [부록 A. Umbrella 구성 요소 및 용어에 대한 킷 레퍼런스](#)
- [부록 B. Umbrella 테스트 사이트 목록](#)

제한 사항 (Limitation_s)

본 랩에는 실습의 여러 단계 전체에 걸쳐 브라우저에서 각 다른 시간에 실행하는 여러 가지 검증 테스트가 포함되어 있습니다. 경우에 따라 절차 전후에 이러한 테스트를 수행하고 바로 완료한 절차의 영향을 확인할 수 있습니다. 실행한 테스트 결과가 문서화된 예상 결과와 일치하지 않는 경우, 랩 관리자에게 이 문제를 보고하기 전에, 먼저 Firefox 브라우저를 닫았다가 다시 열어 테스트를 다시 한번 수행합니다.

또한 dCloud 환경이 콘텐츠를 캐시하여 언급된 테스트 중 일부에 일관성이 없는 결과를 초래합니다. 확실하지 않은 경우 감독관들에게 문의하시기 바랍니다!

커스터마이징 옵션

일반적으로 이 랩의 모든 연습은 랩 세션에 할당된 시간에 완료할 수 있습니다. 이전에 Umbrella lab 세션을 완료된 경우 일부 연습은 생략하고 새로운 내용에 집중할 수 있습니다. 일부 연습은 옵션으로 표시되며 다른 연습도 생략할 수 있습니다.

먼저 의제를 검토하고 시작하기 전에 완료하고자 하는 시나리오 및 연습을 계획한 다음, 모두 수행하지 않더라도 나열된 순서대로 시나리오를 실행하는 것이 권장합니다.

노트: 아래에 나열된 일부 연습에서는 이전에 볼 수 없었던 새로운 Umbrella 기능을 발견할 수 있습니다.

- 시나리오 1, 실습 2 및 3: 로밍 클라이언트와 AD 통합
- 시나리오 1, 실습 4: URL 을 차단하는 기능
- 시나리오 1, 실습 4: SafeSearch
- 시나리오 1, 실습 6: Umbrella with AnyConnect client
- 시나리오 1, 실습 7: VA(Virtual Appliance) 구축하기
- 시나리오 2, 실습 1: 보안 개요
- 시나리오 2, 실습 2: 보안 활동
- 시나리오 2, 실습 3: Activity Search
- 시나리오 3, 실습 3: Pattern Search in Investigate

- 시나리오 3, 실습 4: AMP Threat Grid in Investigate

필요사항

아래 항목은 데모를 진행하는데 필요한 구성요소입니다.

테이블 1. 준비사항

필수	옵션
개인용 컴퓨터 Cisco dCloud 자격 증명	Cisco AnyConnect®

솔루션에 대하여

Cisco Umbrella 는 사용자가 어디를 가든 인터넷 상의 위협에 대한 첫 번째 방어선을 제공하는 클라우드 보안 플랫폼입니다. 인터넷 기반에 구축된 Cisco Umbrella 는 모든 위치, 장치 및 사용자의 인터넷 활동에 대한 완벽한 가시성을 제공하며 위협이 네트워크 또는 엔드 포인트에 도달하기 전에 차단합니다.

Cisco Umbrella 는 인터넷 활동 패턴을 분석 및 학습함으로써 현재 및 새로운 위협에 대해 공격형 인프라를 자동으로 해제하고 컨넥션이 설정되기 전에 악의적인 대상에 대한 요청을 사전에 차단합니다.

Cisco Umbrella 를 사용하면 더 일찍 피싱 및 멀웨어 감염을 중지하고 이미 감염된 장치를 더 빠르게 식별하고 데이터 유출을 방지할 수 있습니다. 또한 Cisco Umbrella 는 클라우드에서 제공되기 때문에 개방형, 자동화 및 사용이 간편한 효율적인 보안 플랫폼을 제공합니다.

Cisco Umbrella Investigate 는 인터넷을 통해 도메인, IP 및 멀웨어에 대한 위협 인텔리전스를 제공합니다. DNS 요청 및 기타 상황별 데이터에 대한 실시간 그래프를 활용하여 Investigate 는 인터넷 도메인, IP 및 멀웨어의 관계와 진화를 가장 완벽하게 파악하여 공격자의 인프라를 파악하고 향후 위협을 예측할 수 있도록 지원합니다.

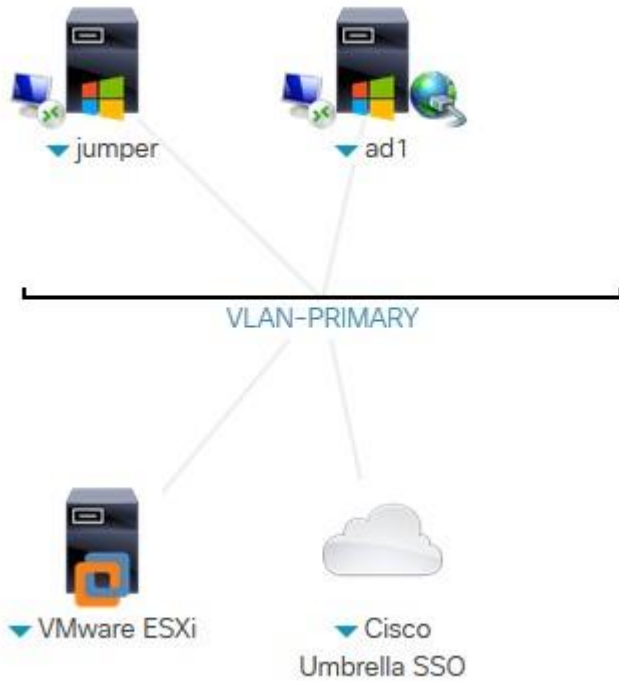
Investigate 는 엔터프라이즈 및 소비자 사용자의 일일 1,000 억 개 이상의 DNS 요청을 포함한 다양하고 대규모 데이터 세트 및 전세계 500 개 이상의 BGP 피어링 파트너로부터 인터넷 상의 서로 다른 네트워크 간 연결에 대한 실시간 뷰를 활용합니다. 데이터 마이닝 기법, 3D 시각화 및 보안 연구자 전문 지식을 사용하여 작성된 통계 모델을 데이터에 적용하여 패턴을 파악하고 향후 인터넷의 악성적인 위치를 예측합니다.

Investigate 를 통해 보안 팀은 조사 시간을 단축하고, 사건 대응의 우선순위를 정하는 데 필요한 글로벌 컨텍스트를 확보하고, 공격에 앞서 나갈 수 있습니다.

노트: 일부 클라이언트 소프트웨어, 테스트 유틸리티 및 랩에서 사용되는 에이전트는 여전히 OpenDNS 브랜드로 되어 있습니다. 향후 Cisco Umbrella 브랜드로 업데이트될 예정입니다.

구성도

본 데모는 시나리오의 원활한 진행 및 솔루션이 제공하는 기능들의 동작 확인을 위해 사전 설정된 구성요소들을 포함하고 있습니다. 대부분의 구성요소들은 별도 제공되는 관리자 계정을 통해 구성이 가능하고 **Topology** 메뉴에 있는 각 구성요소 아이콘을 클릭하면 해당 구성요소에 접근하기 위한 IP 어드레스 및 계정 정보를 확인할 수 있습니다.



테이블 2. 장비 세부 사항

이름	설명	호스트 이름 (FQDN)	IP 주소	사용자 이름	패스워드
Jumper	최종 사용자 워크 스테이션 (어드민 및 탐색 사용자)	Jumper.dcloud.cisco.com	198.18.133.37	dcloudWgorwell	C1sco12345
ad1	AD 서버	ad1.dcloud.cisco.com	198.18.133.1	dcloudWadministrator	C1sco12345
VMware ESXi	Umbrella 가상 어플라이언스용 VM 호스트		198.18.133.31	root	C1sco12345

랩 토폴로지 구성 요소

SE 노트북: 이는 개인 컴퓨터여야 합니다. 대부분의 경우 DCloud의 기본 제공 원격 데스크톱 애플리케이션을 사용하여 RDP를 랩의 가상 시스템으로 사용할 수 있지만 경우에 따라 장치에서 실행되는 기본 RDP 애플리케이션을 사용할 수 있습니다.

Windows 7 Client VM (jumper): 이 장치는 두 가지 주요 기능을 지원합니다:

웹 브라우저에서 Umbrella 어드민 대시보드 콘솔에 로그인하기 위한 베이스입니다. 로그인 프로세스는 SSO(Single Sign On)에 의해 제어되므로 개인 장치가 아닌 랩에서 실행 중인 브라우저를 사용하여 Umbrella 대시보드에 로그인해야 합니다.

Jumper 머신은 네트워크에서 DNS 요청을 생성하는 최종 사용자 장치 역할도 합니다. 이 클라이언트에 Umbrella 로밍 클라이언트가 설치되어 리포트에 장치 수준의 세분성을 제공하고 AD에 통합된 후 사용자 및 그룹 수준의 세분성을 제공합니다. 관리자는 세분화된 추가 기능을 통해 DNS 요청을 특정 AD 사용자 또는 시스템 호스트 이름에 연결할 수 있습니다. 이 클라이언트와 관련된 두 가지 추가 선택적 연습이 있습니다:

AnyConnect 로밍 클라이언트를 설치하면 이 클라이언트에도 설치됩니다. 이 옵션은 이미 AnyConnect를 사용하고 있는 고객을 대상으로 로밍 사용자를 위한 훌륭한 구축 옵션입니다.

가상 어플라이언스(VA) 구축을 위한 선택적 연습을 완료하면, Umbrella는 네트워크에 있을 때 장치에 (로밍 클라이언트에 종속되지 않음) 전체 보안 정책을 적용합니다.

VMware ESXi: 선택적 실습에서 Umbrella의 가상 어플라이언스는 VMware ESXi 호스트에 설치됩니다 (참고: Microsoft Hyper-V도 지원됨). 가상 어플라이언스는 DNS 요청을 보내는 모든 디바이스에 대해 내부 IP 주소를 확인할 수 있는 온-프레미스 구축입니다. Windows 7 클라이언트 Jumper 데스크톱의 vSphere Client는 Umbrella 가상 어플라이언스를 배포하기 위해 ESXi 호스트 환경에 액세스하는 데 사용됩니다.

Windows Server Domain Controller VM (ad1): Umbrella AD 커넥터는 하나 이상의 DC에 설치되어 고객이 기존 AD 구조를 처음 가져오고 지속적으로 Umbrella로 동기화할 수 있도록 합니다. 이 랩 세션에서는 로밍 클라이언트 및 선택적으로 가상 어플라이언스와의 AD 통합을 지원하기 위해 필요합니다. 고객은 이 통합을 통해 특정 DNS 요청을 하는 AD 사용자, 그룹 또는 컴퓨터를 식별할 수 있습니다. 경우에 따라 이 시스템의 브라우저를 사용하여 Umbrella 관리 대시보드에 로그인할 수 있습니다. 토폴로지서 직접 또는 기본 RDP 애플리케이션을 통해 이 VM에 연결할 수 있습니다.

Cisco Umbrella SSO: 이는 Umbrella 대시보드에 대한 SSO(Single Sign On)를 지원하는 SAML Identity Provider(ID 공급자)입니다. 이 구성 요소에 직접 액세스할 필요는 없습니다.

시작하기

시작하기에 앞서

고객 및 파트너를 대상으로 데모시연을 할 경우 원활한 진행을 위해 본 자료를 가지고 사전에 충분한 연습을 하시기를 권장합니다. 데모 완료 후 새로운 구성을 해야 하는 경우는 세션을 새로 예약하십시오.

사전에 충분한 연습은 성공적 진행을 위한 필수 조건입니다.

다음 단계를 따라 랩 세션을 시작하고 액세스합니다. (선택적으로 아직 사용할 수 없는 경우 예약할 수 있습니다:

1. dcloud.cisco.com 으로 이동하여 랩 감독관이 조언한 위치를 선택한 다음 cisco.com 자격 증명 또는 제공된 다른 자격 증명을 사용하여 로그인합니다.
2. DCloud 대시보드에서, My sessions 페이지에 세션이 있는지 확인합니다. 없는 경우 Custom 콘텐츠 페이지에서 확인합니다.
3. 세션이 이미 활성화되어 있고 시작할 준비가 되어 있어야 합니다. 그렇다면 View 를 클릭하여 활성 세션을 열고 Topology 페이지에서 랩을 시작합니다.
4. 세션이 아직 활성화되지 않은 경우, 지금 시작하도록 세션을 예약하십시오. [\[가이드\]](#)
5. My Dashboard > My sessions 에서 세션이 활성화되면 View 버튼이 표시됩니다.

노트: 세션이 활성화되는 데 최대 10 분이 걸릴 수 있습니다.

6. **View** 를 클릭하고 활성화한 세션을 엽니다. [\[가이드\]](#)

노트: 랩 토폴로지에서 브라우저에 내장된 Cisco dCloud 원격 데스크톱 클라이언트를 사용하여 랩 가상 시스템에 직접 연결해야 합니다 [\[가이드\]](#). dCloud Remote Desktop 클라이언트는 최소한의 상호 작용으로 활성 세션에 액세스하는 데 가장 적합합니다. 이 방법이 적합하지 않은 경우, VPN 을 통해 dCloud 네트워크에 연결한 다음 기본 원격 데스크톱 클라이언트를 사용하여 랩 VM 에 대한 원격 데스크톱 세션을 수동으로 시작해야 합니다.

7. 필요한 경우, **Cisco AnyConnect VPN** [\[가이드\]](#) 및 **개인 랩톱의 로컬 RDP 클라이언트** [\[가이드\]](#)를 사용하여 워크스테이션에 연결할 수 있습니다.

워크스테이션 1: **198.18.133.37**, 사용자 이름: **administrator**, 패스워드: **C1sco12345**

노트: 브라우저가 내장된 Cisco dCloud 원격 데스크톱 클라이언트를 사용하는 경우 키보드의 alt+ctrl+shift 조합을 사용하여 원격 클라이언트의 클립보드를 열어서 로컬 노트북과 원격 클라이언트 간에 콘텐츠를 쉽게 복사하고 붙여넣을 수 있습니다.

시나리오 1. Umbrella 구축, Policies 생성 및 Activity 만들기

이 단계는 Umbrella 를 구축하고, 검색 활동을 생성하고, 활동을 기본 보고서에서 검색하는 주요 랩 시나리오입니다.

노트: 고객이 추가 보안 계층을 쉽게 구축하고자 하는 경우, Umbrella 네트워크 및 로밍 클라이언트 구축(Enterprise Roaming Client – ERC 또는 AnyConnect 클라이언트)만으로 이러한 요구 사항을 충족시킬 수 있습니다.

로밍 클라이언트는 AD 사용자 및 컴퓨터 수준의 세분성을 제공할 수 있습니다 (이전에는 Umbrella 보고서에 내부 IP 가시성 및/또는 AD ID 정보를 얻기 위해 가상 어플라이언스를 구축해야 했음). 대부분의 고객은 모든 구축 옵션과 이러한 옵션의 작동 방식을 이해하고 싶어합니다.

모든 구축 과정을 진행하면서, 보안 요구 사항을 충족하는 마일스톤 1 구축(네트워크 및 로밍 클라이언트)환경을 구축을 만들어야 합니다.

마일스톤 2 구축(VA 및 AD 통합)이 해당 환경에서 작동하지 않는 경우, 마일스톤 1 로 돌아가서 모든 요구 사항을 충족했다고 확인할 수 있습니다.

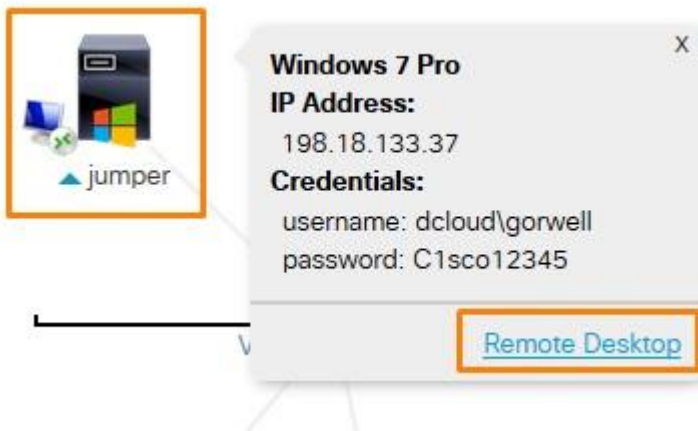
스텝

실습 1: Umbrella 액세스 및 네트워크를 구축하기

이 연습에서는 dCloud Lab 세션을 시작하고 클라이언트 워크스테이션(Jumper)과 AD 서버(ad1)에 액세스할 수 있음을 확인합니다. Umbrella 관리 대시보드에 로그인한 후, ad1 서버에서 Umbrella 네트워크를 구축하여 Umbrella 를 구현하는 것이 얼마나 간단한지 보여 줍니다.

포드 구성 요소 및 Umbrella 대시보드에 액세스하기

1. 메인 dCloud Topology 에서 **Jumper** 이미지(**Jumper** 가 주 클라이언트 워크스테이션임)를 클릭합니다. Remote Desktop(원격 데스크톱)을 통한 액세스 링크가 포함된 클라이언트의 세부 정보를 보여주는 컨텍스트 창이 열립니다.



2. Remote Desktop 링크를 클릭하여 원격 데스크톱 세션이 시작될 다른 브라우저 탭을 엽니다.

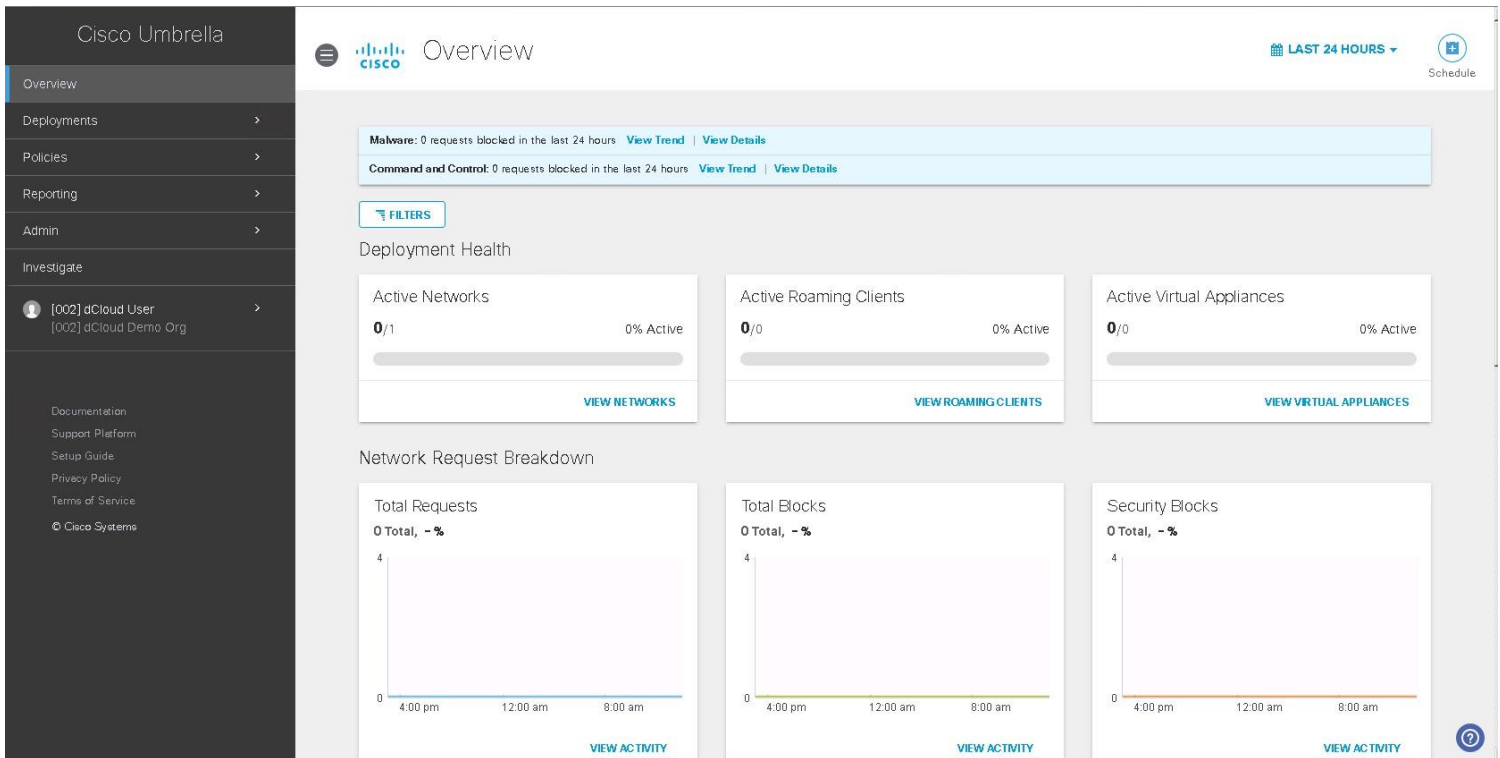
노트: Cisco dCloud 원격 데스크톱 클라이언트를 사용하여 **Jumper** 클라이언트 또는 기타 구성 요소에 연결하는 것이 권장합니다. [가이드]. dCloud Remote Desktop 클라이언트는 최소한의 상호 작용으로 활성 세션에 액세스하는 데 가장 적합합니다.

3. **Jumper** 클라이언트의 데스크탑의 바로 가기를 통해 Umbrella 관리 대시보드에 로그인합니다.



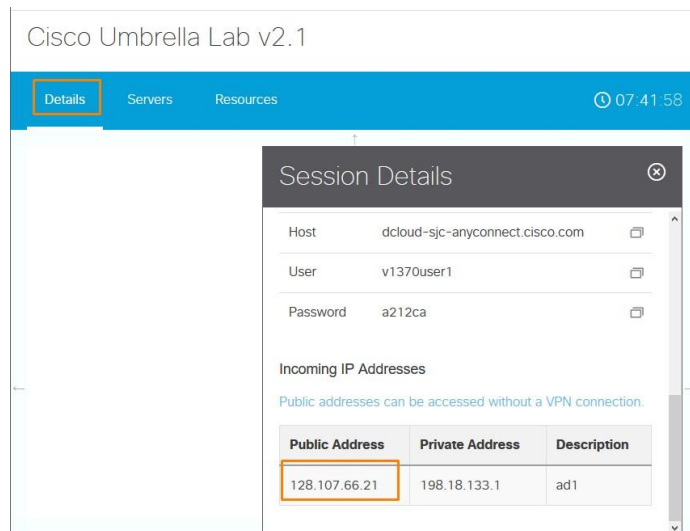
노트: 실제 시나리오에서는 조직에서 SSO(Single Sign On)를 사용하도록 설정하지 않은 경우 일반적으로 사용자 이름과 패스워드를 사용하여 Umbrella 에 로그인합니다. 이 실습에서는 SSO 를 통해 POD's Umbrella 계정에 자동으로 로그인되므로 관리자 자격 증명이 필요하지 않습니다.

4. Umbrella 대시보드에 로그인하면 Overview(개요) 페이지로 이동합니다. 페이지 맨 위에 일반 메시지가 표시되고 바로 밑에 활성 네트워크, 로밍 클라이언트 및 가상 어플라이언스에 대한 세부 정보가 표시됩니다. 이어서 모든 요청, 차단된 모든 요청 및 모든 보안 블록의 활동 그래프가 표시됩니다. 아래에는 대상, ID 및 블록 유형별로 드릴다운할 수 있도록 보안 블록에 초점을 맞춘 섹션이 있습니다. 이러한 영역 중 일부는 나중에 자세히 살펴볼 Security Overview 보고서와 유사하며, 대시보드의 다른 영역은 실습 시나리오와 실습에서도 다릅니다.



노트: 새 랩 인스턴스를 시작할 때 Overview(개요) 페이지에 처음에 데이터가 표시되지 않을 수 있습니다.

5. 다음으로, 토폴로지 페이지로 돌아가 ad1 용 외부 IP 를 메모해야 합니다. 이를 수행하려면, **Details** 를 클릭한 다음 **Incoming IP Addresses** 로 스크롤합니다. 나열된 공용 주소(Public Address)를 기록해 둡니다. 완료되면 이 창을 닫습니다.

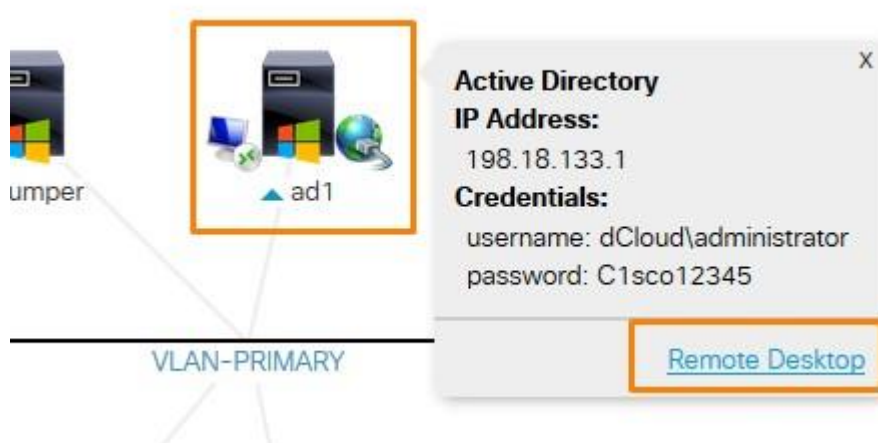


노트: AD 서버에 대해 수신하는 IP 주소는 랩 세션 동안 정적 상태가 됩니다. 그러나 랩 세션 간에 각 랩 포드마다 이러한 변경 사항이 적용되므로 다음 그림은 받은 것과 동일한 IP 주소를 반영하지 않을 수 있습니다. 따라서 여기에 표시된 내용이 아닌 고객의 IP 주소를 사용해야 합니다.

중요: Jumper 클라이언트가 아닌 ad1 AD 서버에서 다음 단계를 수행해야 합니다!

6. **Active Directory** (ad1) 아이콘을 선택합니다. **Remote Desktop** 링크를 클릭하여 AD 서버에 대한 추가 원격 데스크톱 세션을 엽니다.

노트: 추가 원격 데스크톱 세션은 다른 브라우저 탭에서 열리며, 이를 통해 동시에 실행되는 두 개의 세션 (점퍼 및 ad1)을 신속하게 전환할 수 있습니다.



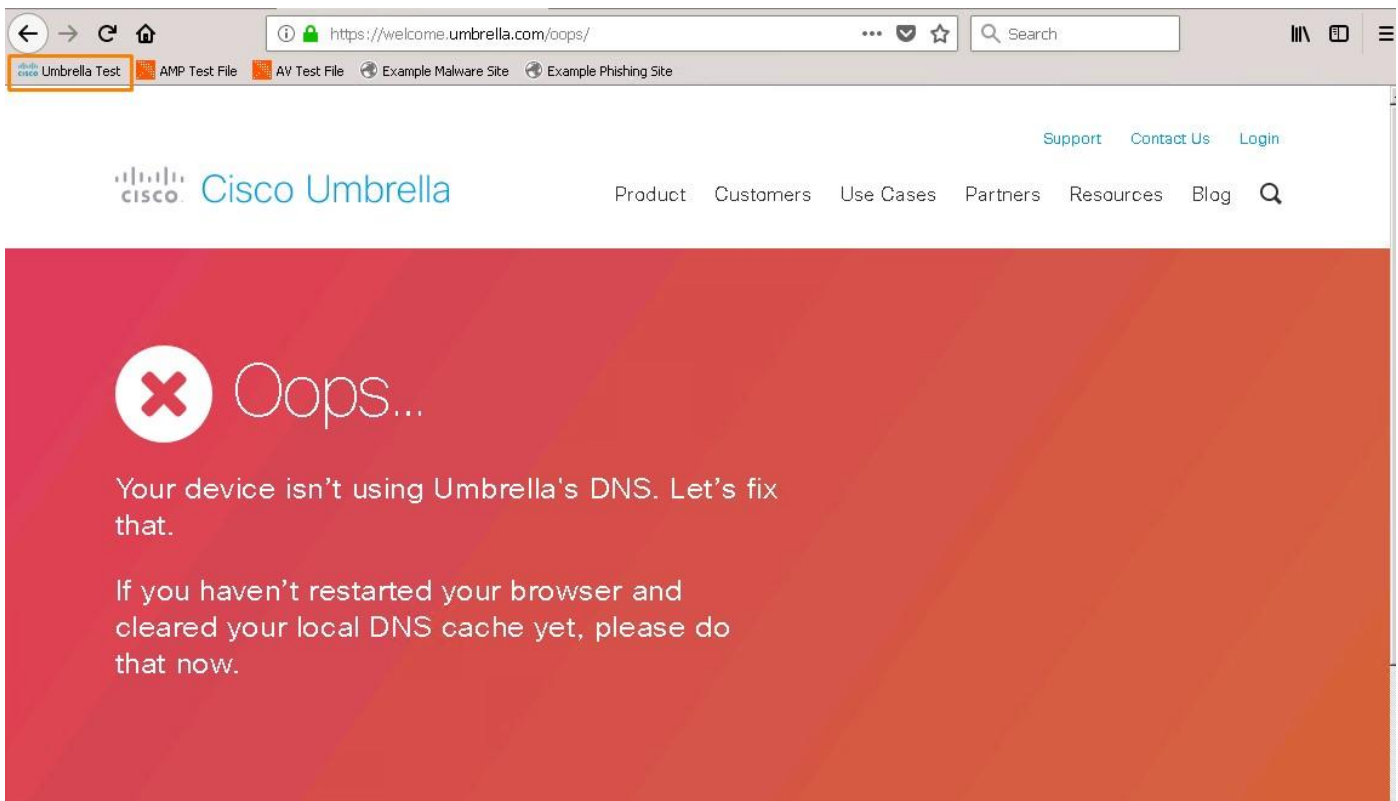
7. AD 서버에 액세스한 후에는 **Jumper** 에서 방금 수행했던 것 처럼 데스크톱 아이콘을 사용하여 Umbrella 관리자 대시보드에 로그인 합니다.



8. 대시보드가 로드되고 SSO 를 통해 로그인되었는지 확인합니다.

대시 보드에서 Umbrella 네트워크 만들기

1. 다른 브라우저 탭을 열고 브라우저 바 (welcome.umbrella.com)에서 Umbrella 테스트 북마크 바로가기를 클릭합니다. 이는 Umbrella 를 아직 사용하지 않은 것을 확인할 수 있습니다. 아직 Umbrella 를 사용하고 있지 않음을 알리는 메시지가 표시 되는지 확인합니다.



2. 브라우저에서 Umbrella 대시보드가 실행 중인 첫 번째 탭으로 돌아갑니다. 왼쪽의 기본 탐색을 **Deployments >Core Identities >Networks** 로 이동 합니다.

노트: 페이지 상단에는 Umbrella 에서 볼 수 있는 공개 IP 주소가 표시될 수 있습니다. 그러나, 이는 HTTP IP 주소일 수 있으므로 dCloud Topology 페이지에 있는 IP 주소를 사용하는 것이 이를 확인하는 데 가장 정확한 방법입니다.



3. 페이지 상단에서 **Add** 아이콘을 클릭하여 새 네트워크를 추가합니다.
4. **Network Name** (네트워크 이름) 영역에서 원하는 이름을 새 네트워크에 지정 합니다.
5. **IP Address** (IP 주소) 필드에 dCloud topology (dCloud 토폴로지) 페이지에서 찾은 **public IP** 주소를 입력합니다
6. **subnet**(서브넷)은 **/32** (디폴트)로 유지되어야 합니다.
7. IP 주소가 정적되어 있으므로 **Dynamic** 확인란을 선택하지 마십시오.(다른 브라우저 탭에서 링크를 열어 DHCP 주소를 지원하는 방법을 읽을 수 있습니다.)
8. **Enable a daily stats email**(일별 통계 이메일 활성화) 확인란을 선택하지 마십시오.

Add a new network

Start by pointing your network's DNS to our servers:

208.67.220.220 and 208.67.222.222

Network Name

IP Address

 /

This network has a dynamic IP address. [Learn More »](#)

CANCEL

SAVE

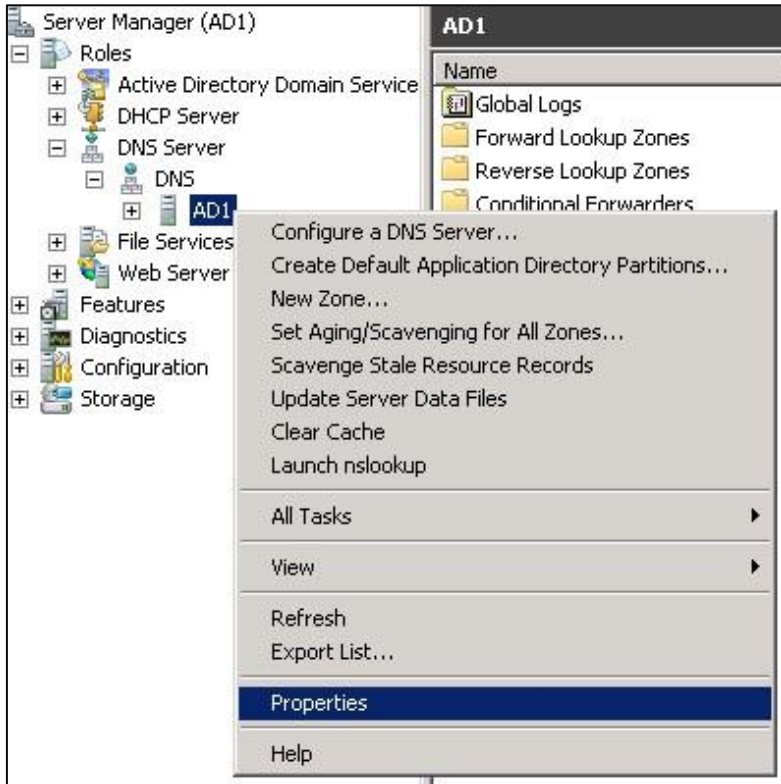
9. **SAVE** 를 클릭하여 네트워크를 저장합니다.
10. 이제 Umbrella 는 이 공용 IP 주소에서 전송되는 모든 트래픽을 조직으로 인식하고 계정에 연결합니다. 이제 완료해야 할 유일한 단계는 DNS 확인을 Umbrella 로 지정하는 것입니다.

Umbrella 를 가리키도록 DNS 서버 업데이트

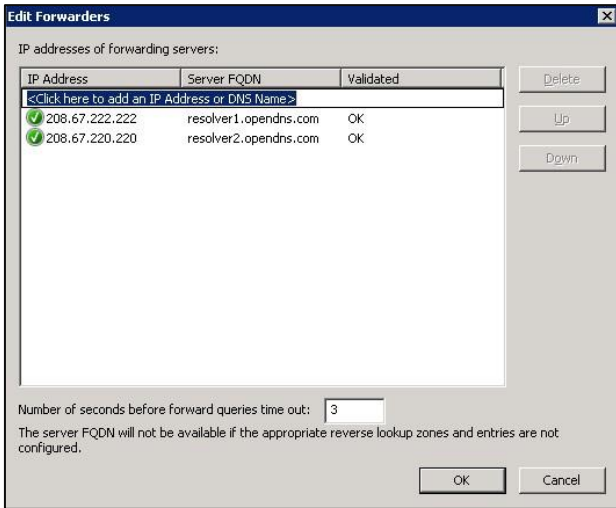
다음 단계에서는 도메인 컨트롤러에 로그인하고 서버에서 Umbrella 를 가리키도록 DNS 포워더를 변경 합니다.

1. Remote Desktop 세션의 AD 서버를 **ad1** 에 유지합니다.

2. Windows Server 빠른 실행 표시줄에서 **Server Manager** 를 엽니다.
3. **Roles** (역할) 트리에서 **DNS Server > DNS > AD1** 를 확장 합니다. **AD1** 를 마우스 오른쪽 버튼으로 클릭하고 **Properties**(속성)을 선택합니다.



4. **Properties** 창에서 **Forwarders** 탭을 선택합니다.
5. **Edit** 를 클릭합니다.
6. **IP Address** 목록에 Umbrella 의 IP 주소를 추가 합니다. Umbrella 서비스의 주소는 **208.67.222.222** 및 **208.67.220.220** 입니다.
이전에 저장한 다른 DNS 포워더를 제거해야 합니다.

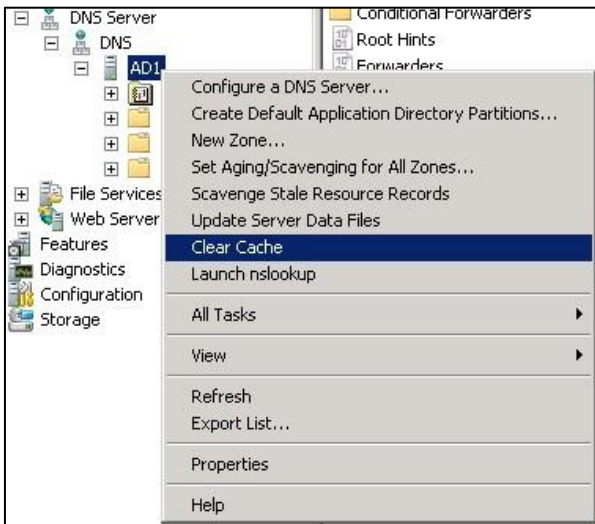


7. 확인자의 FQDN 이 확인되고 두 주소가 모두 유효하는지 확인합니다.

노트: 포워더 목록에는 208.67.222.222 및 208.67.220.220 만 있어야 합니다. 대부분의 운영 시스템에서는 목록에 있는 ip 에 라운드 로빈 방식으로 DNS 트래픽을 라우팅합니다. 목록에 다른 DNS 확인자가 있는 경우 (예: Google DNS: 8.8.8.8) 일부 DNS 요청은 Umbrella 로 이동하고 다른 일부는 다른 확인자로 이동하여 일관성 없는 환경을 경험할 수 있습니다. 또한 고객이 필요 시 다시 전환해야 하는 경우 이전에 구성된 기존 ip 를 기록해 두는 것이 권장합니다.

8. **OK** 를 두 번 클릭하여 새 설정을 저장합니다.

9. **AD1** 를 다시 마우스 오른쪽 버튼으로 클릭하고 **Clear Cache** (캐시 지우기)를 클릭하여 기존 IP 가 캐시에서 제거되었는지 확인합니다.

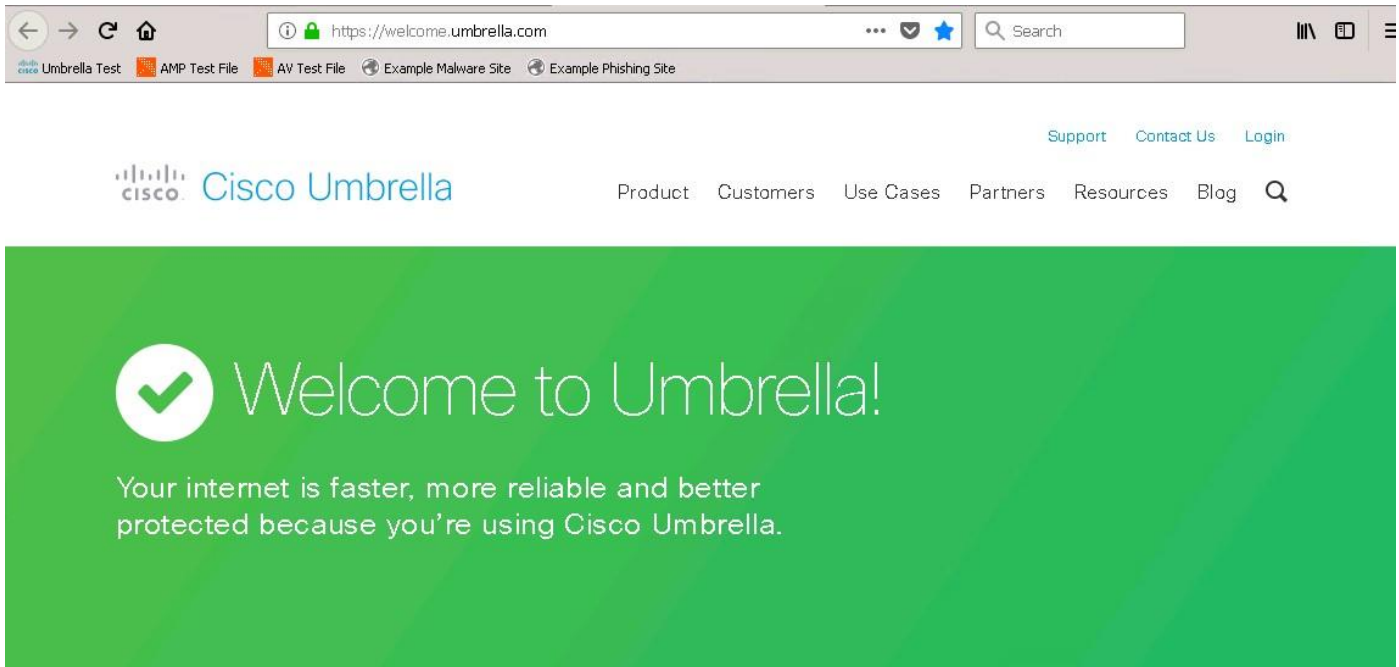


10. DNS 캐시를 지울 수 있도록 명령줄을 열고 다음 명령어를 입력합니다:

C:\wipconfig /flushdns

Umbrella 연결성 확인

1. 브라우저를 닫습니다.
2. 브라우저를 다시 엽니다.
3. 브라우저의 북마크 바에 있는 바로 가기에서 Umbrella Test 를 반복합니다.
4. 이제 Umbrella (OpenDNS)에 연결되어 있는 것을 확인합니다.



노트: 네트워크 구축을 통해 몇 분 이내에 전체 조직(네트워크)을 Umbrella 로 지정하는 방법을 얼마나 간단한지 살펴보았습니다. 이제 정책을 검증하기 위해 정책을 생성하고 다양한 대상에 대한 브라우저 테스트를 수행하는 등의 몇 가지 추가 단계를 수행해야 합니다.

이 모든 단계는 다른 구축 방법을 수행할 때 나중에 실습에서 수행됩니다. 이 연습의 목적은 종종 고객 시행을 빠르게 시작하는 데 사용되는 네트워크 구축의 단순성을 보여주기 위한 것입니다.

실습 2: Umbrella 로밍 클라이언트 구축

이 연습에서는 **Jumper** 워크스테이션에 Umbrella 로밍 클라이언트를 설치하겠습니다.

로밍 클라이언트는 보고 및 정책 시행 모두에 대한 컴퓨터별 세분성을 제공하고 네트워크의 컴퓨터와 내외부 네트워크 모두에 대한 보호를 확장하는 경량 소프트웨어 DNS 포워드입니다. "Umbrella roaming client,"라고 불리지만, 랩톱 및 데스크톱 모두에서 클라이언트를 구축하는 것이 일반적입니다. 클라이언트는 포함된 ID 정보를 사용하여 암호화된 DNS 요청을 네트워크의 상위로 직접 전송하고 로컬 DNS 요청을 정상적으로 처리합니다. 클라이언트도 IP 계층에서 적용됩니다.

Umbrella 로밍 클라이언트 설치를 위한 두 가지 옵션이 있으며 모두 이 실습에서 다룹니다:

Standalone program(독립형 프로그램): Umbrella 로밍 클라이언트는 독립형 프로그램으로 설치됩니다.

AnyConnect 모듈: 이미 VPN에 대해 AnyConnect를 사용중인 고객은 AnyConnect 로밍 클라이언트를 추가 보안 모듈로 쉽게 구축할 수 있습니다. Windows 또는 OS X의 AnyConnect 버전 4.3 MR1 이상이 필요합니다.

이 실습에서는 **Jumper** 워크스테이션에 독립형 로밍 클라이언트를 수동으로 설치합니다. 중소 규모 기업의 경우에는 클라이언트를 설치하는 가장 좋은 방법입니다. 대량 구축을 진행하기 전에 대표적인 컴퓨터를 테스트해야 합니다.

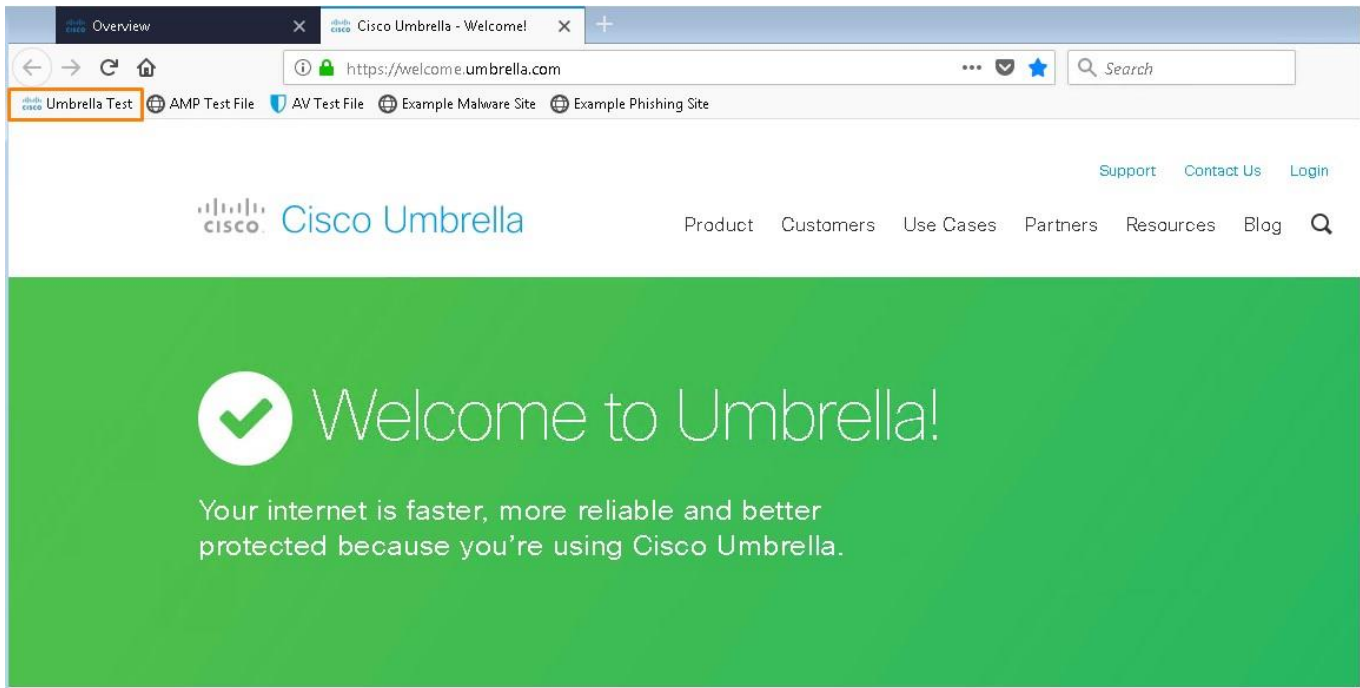
노트: 이 시나리오(실습)에서는 로밍 클라이언트가 기본 구축 방법이 됩니다. 선택적으로, 이전 lab 세션에서 또는 이전에(실습 6, [읽어보기](#)) Umbrella 로밍 클라이언트를 이미 구축한 경우에는 AnyConnect 로밍 클라이언트를 구축할 수도 있습니다. 또한 선택적으로 Umbrella 가상 어플라이언스를 구축할 수 있습니다 ([실습 7, 읽어보기](#)).

노트: 실제 환경에서 클라이언트를 설치하기 전에 고객은 사전 요구 사항을 검토하는 것이 권장합니다:

<https://docs.umbrella.com/product/umbrella/2-prerequisites-update/>.

1. **Jumper** 클라이언트에 있는지 확인합니다. 로밍 클라이언트를 다운로드하고 구축하기 전에 먼저 Umbrella 사용하고 있는지 확인합니다. 다른 브라우저 탭을 열고 브라우저 바 (welcome.umbrella.com)에서 **Umbrella Test** 북마크 바로가기 버튼을 클릭합니다..

노트: Jumper 클라이언트가 DNS 확인을 위해 AD 서버 (ad1)를 가리킵니다. 이전에는 DNS 서버의 포워더를 Umbrella를 가리키도록 설정 했기 때문에 Umbrella 테스트에서는 Umbrella를 실제로 사용하고 있음을 보여줍니다. Jumper가 DNS 확인을 위해 ad1을 사용하고 있으므로, Umbrella는 여전히 네트워크의 등록된 egress IP 주소에서 보낸 DNS 요청을 볼 수 있습니다. 또한 브라우저에서 examplemalware.com으로 이동하여 블록 페이지로 리디렉션될 수 있습니다.

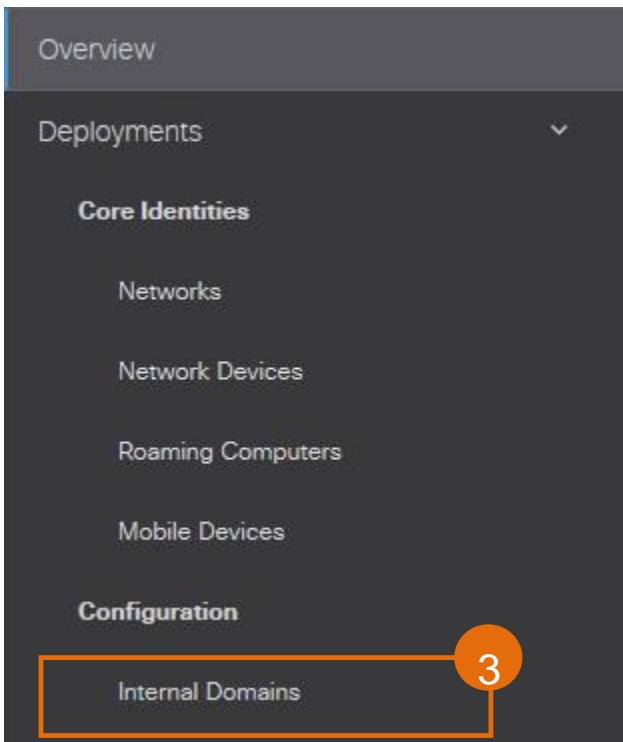




2. 검증 테스트를 실행한 브라우저 탭을 닫고 대시보드로 돌아갑니다.

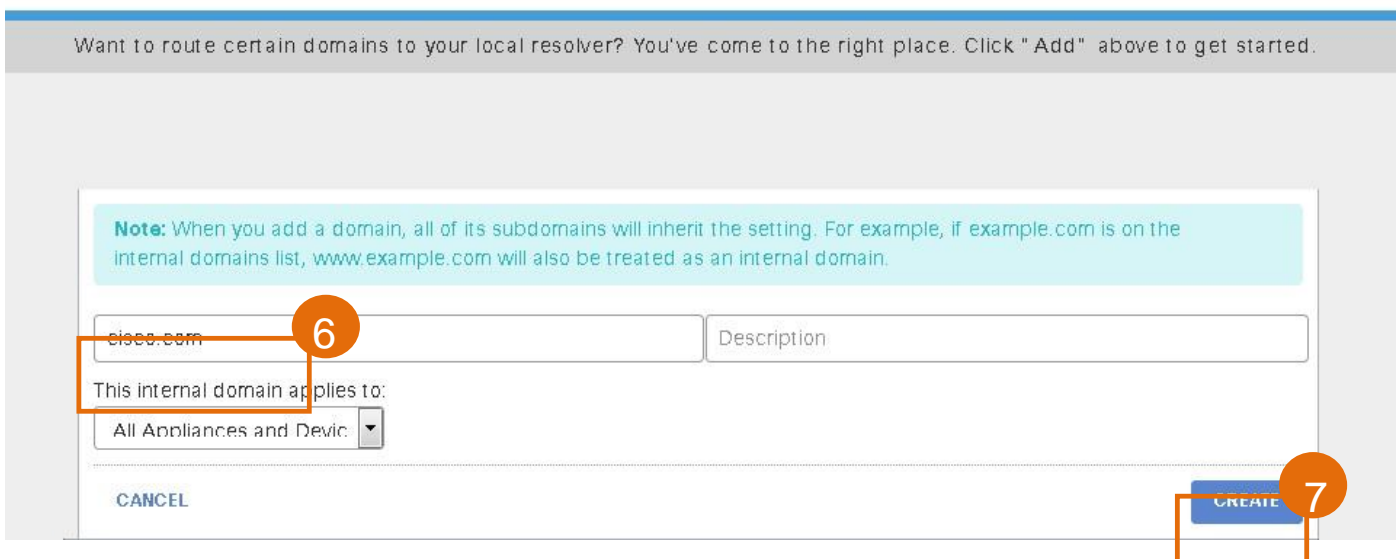
주의: 내부 도메인을 정의하는 다음 단계를 완료하지 않은 경우 로밍 클라이언트 구축한 후 워크스테이션에 액세스하지 못할 수 있습니다!

노트: 내부 도메인을 추가하는 것은 Umbrella 가 예상대로 작동하는지 확인하는 중요한 단계입니다. 내부 도메인 설정의 목적은 정책을 적용할 수 있는 ID로서 외부적으로 라우팅 불가능 (또는 RFC1918 준수) 되는 서브넷을 정의하는 것입니다. 이 단계는 초기 설정 중에 놓치는 경우가 많으며, 내부 네트워크 리소스 (프린터, 파일 서버 등)를 해결할 수 없게 되어 현재 진행 중인 모든 거래를 중단시킬 수 있습니다. 모든 고객의 경우 내부 도메인 섹션은 개인 내부 네트워크의 .local 및 역방향 조회 영역(예: RFC-1918)으로 미리 채워집니다. 이는 고객이 가장 일반적인 내부 네트워크 구성과 관련된 도메인을 추가하는 것을 잊지 않도록 하기 위한 것입니다.

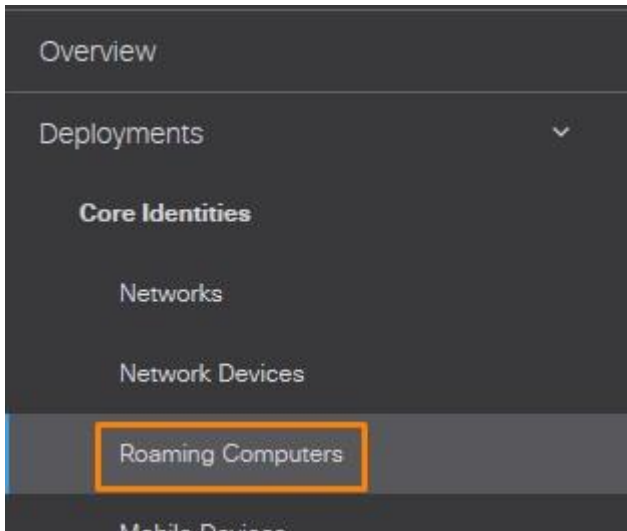
3. 데스크탑 바로 가기에서 Umbrella 대시보드에 액세스 합니다. 왼쪽 탐색 패널 (navigation)에서 **Deployments**(구축) 메뉴를 클릭하여 확장합니다. **Internal Domains** (내부 도메인)을 클릭합니다.



- 만약 상단의 아이콘이  아직 확장되지 않은 경우 클릭하고 설명을 읽습니다.
- 상단의 아이콘을  클릭하여 새 내부 도메인을 추가합니다.
- 내부 도메인으로 **cisco.com** 를 입력합니다. 설명은 선택 사항입니다. **All Appliances** 및 **Devices** 에 이를 적용하는 기본 설정을 유지합니다.




7. **Create** 를 클릭하고 도메인이 저장되었는지 확인합니다.
8. **Deployments** 메뉴로 이동하여 확장합니다. **Core Identity**(핵심 ID)에서 **Roaming Computers**(로밍 컴퓨터)를 클릭합니다.

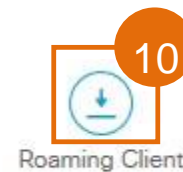


9. 페이지 상단의 아이콘을  클릭하여 Umbrella 가 로밍 컴퓨터를 보호하는 방법에 대한 설명을 봅니다.

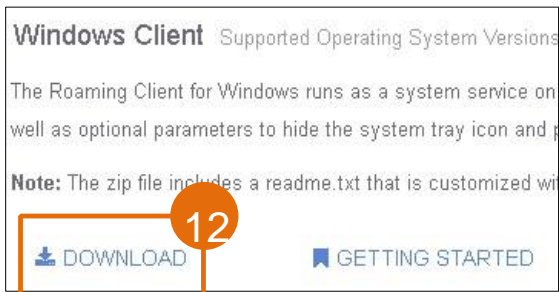
노트: Lab 계정은 로밍 컴퓨터 ID(Jumper)로 미리 채워져 있습니다. 실제 시나리오에서는 새 계정에서 이를 확인할 수 없으며 로밍 시스템의 ID 는 로밍 클라이언트가 시스템에 설치된 후에만 표시됩니다. 이런 경우에는 새 ID 가 인덱싱되는 동안 보고서에서 검색 작업이 표시될 때까지 약 2 시간이 소요됩니다. (단, 정책이 몇 분 내에 시행되고 이 시간 동안 로그가 생성되며 인덱싱이 완료된 후 나중에 표시됨). 랩 세션에서 이러한 제한을 극복하기 위해 사전에 채워진 로밍 ID 가 추가되었습니다. 이는 점퍼 ID 가 오프라인으로 표시되는 이유입니다.

10. 페이지 상단에 있는  **Roaming Client** 클릭하여 로밍 컴퓨터를 프로비저닝 합니다.

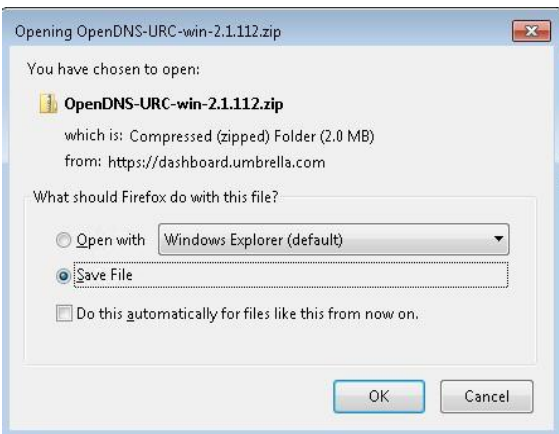
Deployments / Core Identities
Roaming Computers 



11. 로밍 클라이언트에 대한 설명을 읽고, 방금 완료한 계정에 내부 도메인을 추가하는 방법에 대한 설명을 참고하십시오.
12. **Windows Client** 섹션에서 **Download** 아이콘을 클릭합니다.

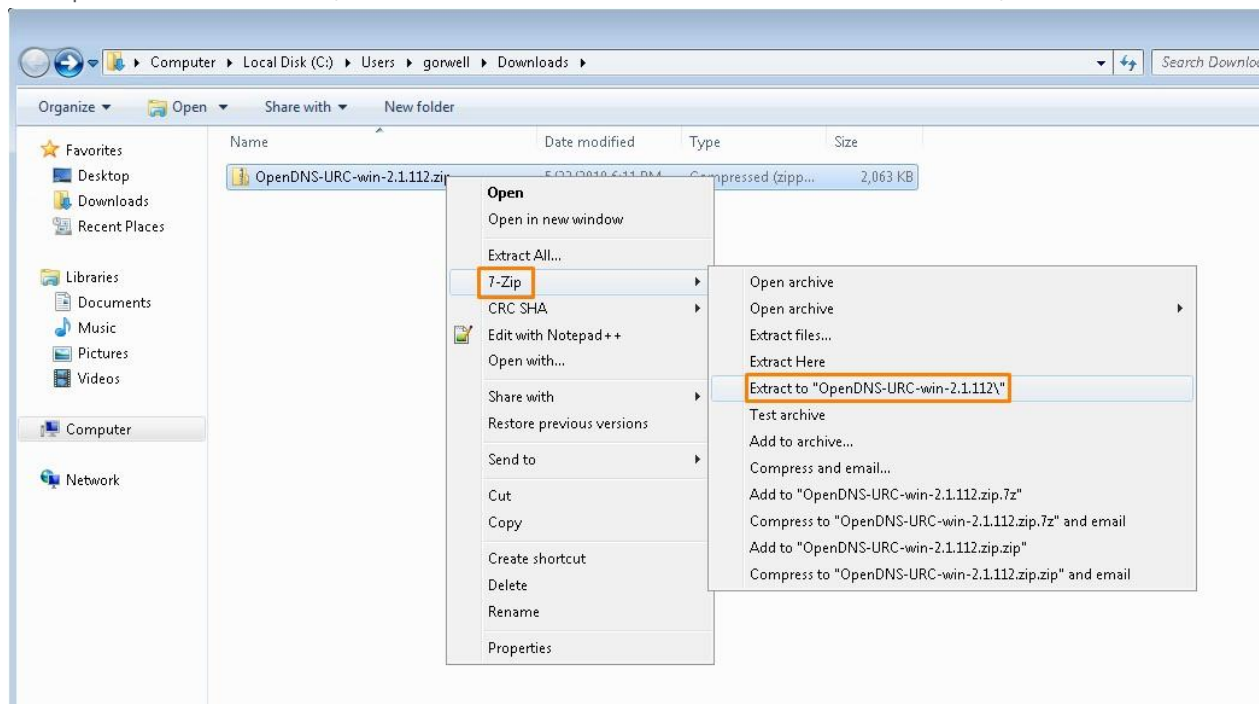


13. 다운로드한 zip 파일을 저장합니다.



14. 파일 탐색기를 열고 zip 파일이 저장된 Windows 다운로드 폴더로 이동합니다.

15. Zip 아카이브에 있는 파일 3 개를 기억하기 쉬운 폴더로 추출합니다. Zip 파일을 마우스 오른쪽 버튼으로 클릭하고 7-Zip 메뉴를 사용합니다 (Downloads 폴더 내의 새 폴더로 파일을 추출할 수 있음).



16. 파일이 추출된 폴더로 이동하여 **readme.txt** 파일을 찾습니다. 파일을 열고 제공된 정보를 확인합니다.

노트: OrgInfo.json 파일은 조직 (Umbrella organization)에 대한 중요한 정보를 클라이언트에 제공하는 프로파일입니다. Readme 파일에 설명된 것 처럼, json 파일이 Setup.msi 파일과 동일한 설치 폴더에 있는 경우 조직 세부 정보가 사용되지만, 그렇지 않은 경우에는 직접 입력해야 합니다. Json 파일은 해당 파일이 다운로드된 조직에 고유한 것을 참고하십시오. 두 번째 조직 내에서 한 조직의 json 파일을 사용하지 마십시오.

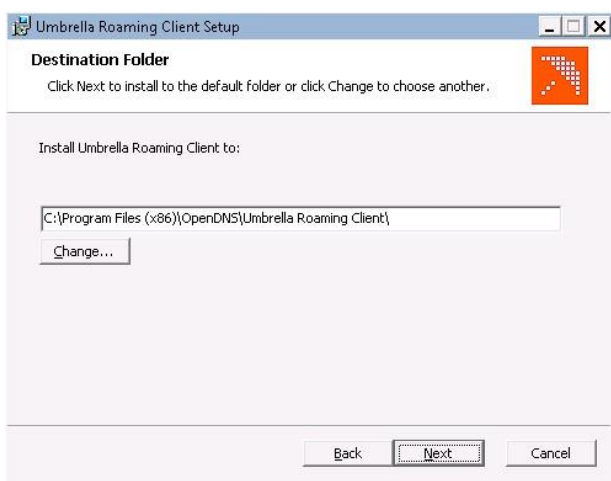
중요: Zip 아카이브의 콘텐츠를 추출하고 아카이브 내에서가 아니라 추출된 Setup.msi 파일을 실행하고 있는지 확인합니다.

17. Setup.msi 파일에서 로밍 클라이언트 설치를 실행합니다.

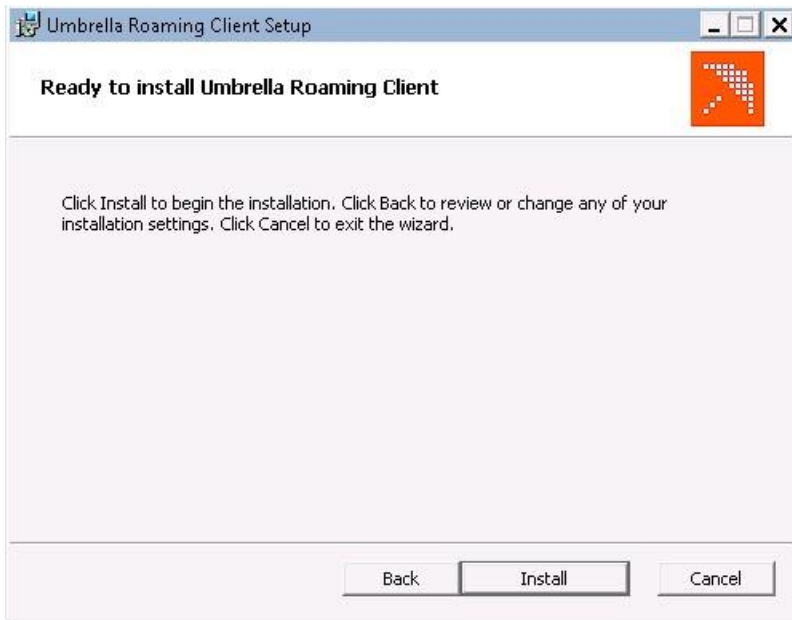
18. 시작(Welcome) 화면에서 **Next** 를 클릭합니다.



19. Destination Folder (대상 폴더) 창에서 기본 목적지를 남겨두고 **Next** (다음)를 클릭합니다.



20. **Install** (설치)를 클릭하여 설치를 진행합니다.



21. 설치가 완료되면 Completed 창이 표시됩니다. **Finish** (마침)를 클릭하여 설치를 종료합니다.



22. 시스템 트레이에서 로밍 클라이언트 아이콘을 찾아 클릭하여 설치가 성공적으로 완료되었는지 확인합니다. (설치 종료 시 나타나는 데 몇 초 정도 걸릴 수 있음). 클라이언트에 대한 세부 사항이 표시됩니다. 상태는 녹색으로 표시되며 Protected and Encrypted 상태를 표시됩니다. 이 시점에는 내부 IP 주소 또는 사용자 ID가 표시되지 않습니다.



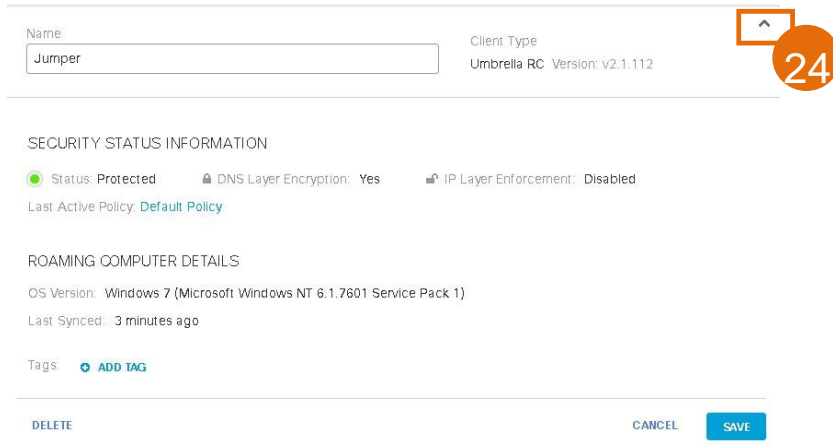
NOTE: 트레이 아이콘을 숨기거나, 소프트웨어 제거를 위해 사용 가능한 애플리케이션에 프로그램을 숨길 수 있습니다 (Windows 에서 프로그램 추가/제거). 이 작업을 수행하는 방법에 대한 자세한 내용은 명령줄 및 커스토마이제이션을 참조하십시오:

<https://support.umbrella.com/hc/en-us/articles/230564627>.

23. Umbrella 대시보드 페이지(**Identities > Roaming Computers**)를 새로 고치거나 다른 페이지로 이동하고 돌아가보면, Windows 클라이언트 (**Jumper**)의 호스트 이름이 비활성 상태로 표시된 것을 볼 수 있습니다.

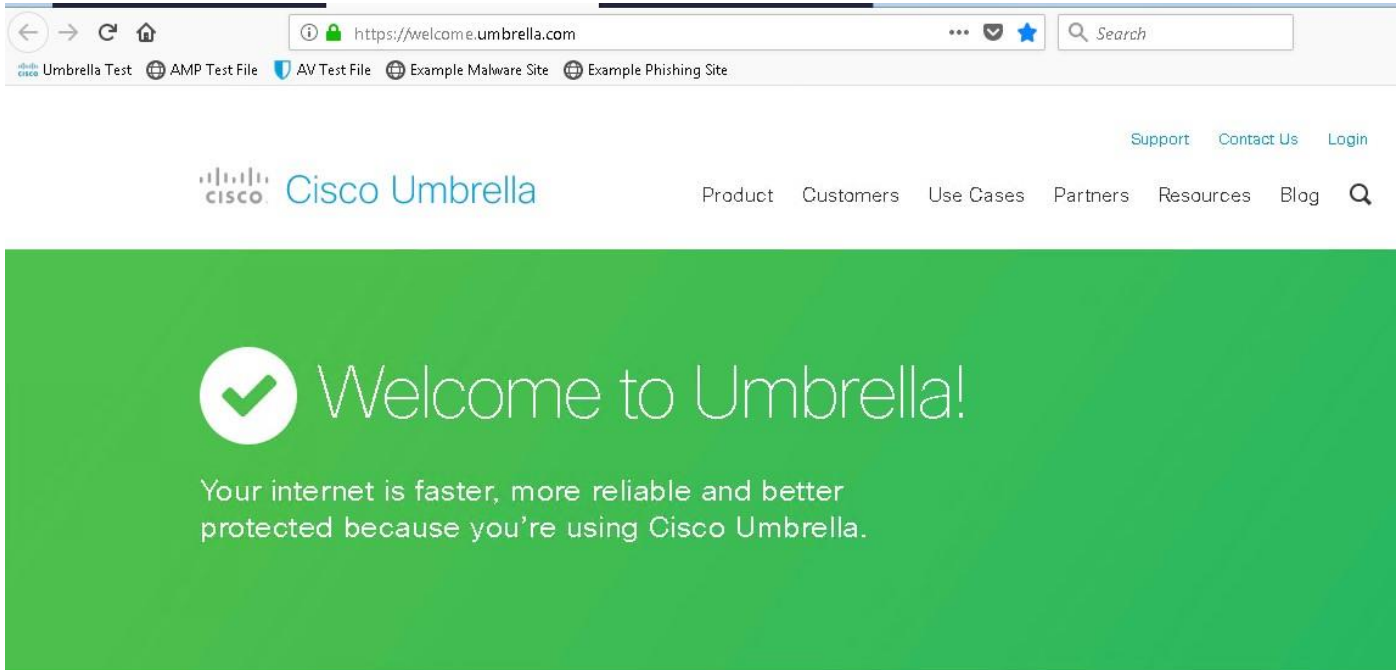
노트: 랩 제한으로 인해 (일반적으로 인프라 사용량이 많은 경우) 액티브 상태는 업데이트하는 데 시간이 걸릴 수 있습니다. 이 지연 시간이 표시되면 다음 단계를 계속 진행하여 나중에 다시 확인합니다.

24. 오른쪽의 화살표 아이콘을 클릭하여 확장하고 추가 정보를 표시합니다.



노트: 이 로밍 클라이언트 버전은 IP 레이어 집행을 지원합니다. 그러나, 이 랩 인프라의 네트워크 제약으로 인해 현재이 기능을 구현할 수 없습니다. 나중에 이를 랩에 포함시킬 예정입니다!

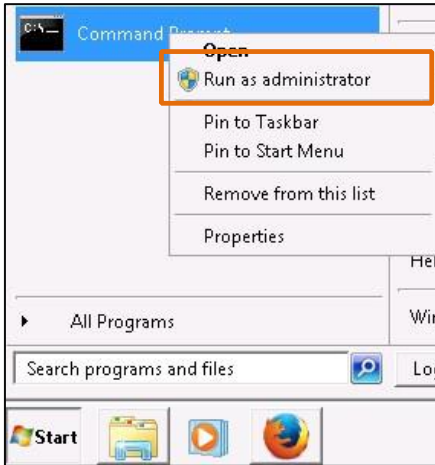
25. 다른 브라우저 탭을 열고 브라우저의 북마크 바에 있는 바로 가기에서 **Umbrella Test** 를 반복합니다. 이제 Umbrella (OpenDNS)에 연결되어 있는지 확인합니다.



26. 이제 Jumper 에서 다른 브라우저 탭을 열고 `examplemalwaredomain.com` 으로 이동하여 테스트를 반복합니다. 이번에는이 테스트 페이지가 차단 되었다는 인증을 확인할 수 있습니다.



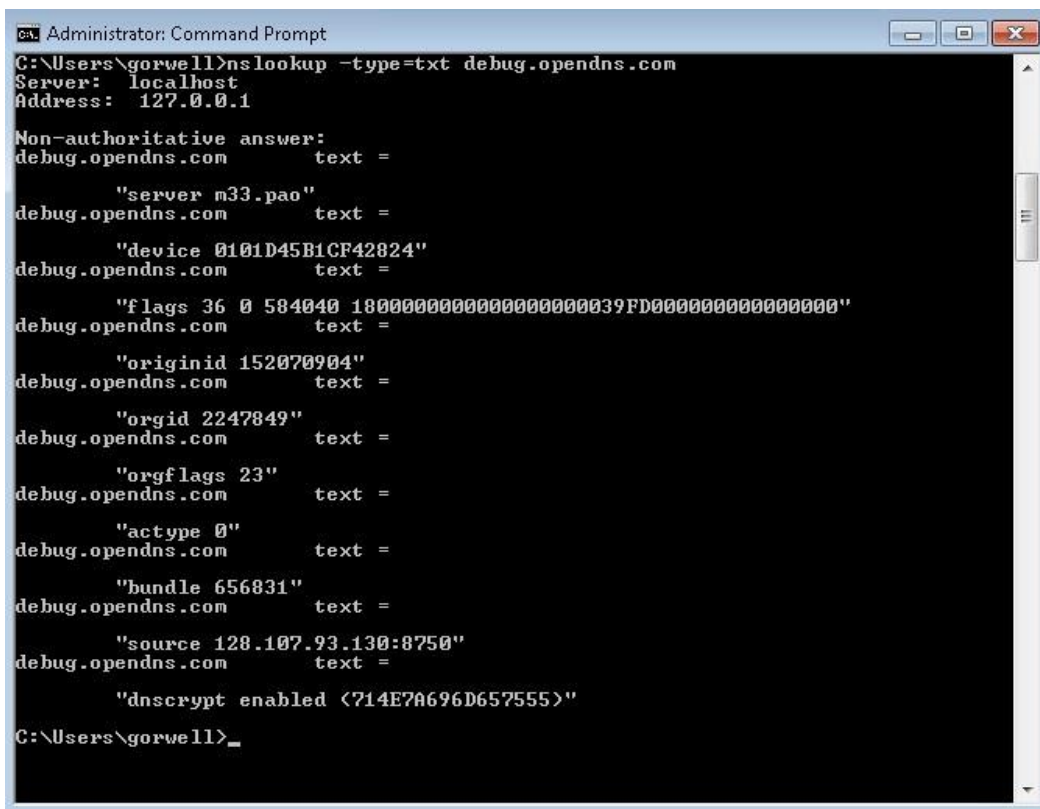
27. 또한 디버그 쿼리를 실행하여 로밍 클라이언트가 확인을 위해 DNS 트래픽을 Umbrella 로 라우팅하는 것을 확인할 수 있습니다. Jumper 클라이언트에서 Windows Start 버튼을 클릭하고 Start 메뉴에서 명령 프롬프트를 마우스 오른쪽 버튼으로 클릭합니다. 관리자를 Run 로 선택합니다.



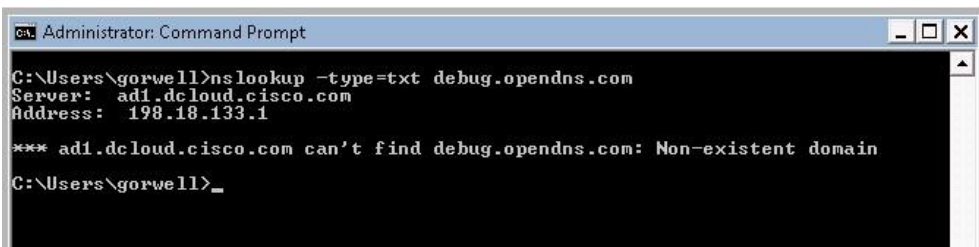
28. 명령 프롬프트 창에서 다음 명령어를 입력합니다:

```
nslookup -type=txt debug.opendns.com
```

29. Umbrella 가 올바르게 구성된 경우 출력에는 탐지된 조직, Umbrella 확인자, 로밍 클라이언트에 대한 다양한 세부 정보를 표시됩니다. 출력에서 확인할 수 있는 정보를 확인합니다.



30. 텍스트 레코드 debug.opendns.com 은 Umbrella 를 DNS 확인에 사용하는 경우에만 찾을 수 있습니다. Umbrella 가 제대로 구성되지 않은 경우, 다음과 유사한 출력이 반환됩니다:



```
Administrator: Command Prompt
C:\Users\gorwell>nslookup -type=txt debug.opendns.com
Server:  ad1.dcloud.cisco.com
Address:  198.18.133.1

*** ad1.dcloud.cisco.com can't find debug.opendns.com: Non-existent domain
C:\Users\gorwell>
```

실습 3: Umbrella 로밍 클라이언트를 사용하여 AD 사용자 ID 활성화

이 실습에서는 Domain Controller (DC)와 통신하도록 Umbrella 의 AD connector 를 구성합니다. 먼저 Umbrella 의 AD connector 를 사용할 AD 사용자를 생성해야 합니다. 그 다음에는 AD 에 대한 관련 권한을 설정하는 구성 스크립트를 실행합니다. 마지막 단계에는 커넥터 자체를 설치해보겠습니다.

일단 구성되면 커넥터는 암호화된 해시 내에서 AD 사용자 및 그룹 세부 정보를 Umbrella 로 전송합니다. 그러면 로밍 클라이언트는 클라이언트에 로그인한 사용자의 사용자 이름을 선택하고 AD 커넥터에서 전송한 정보와 일치하는 항목이 있는 경우 이 데이터를 Umbrella 로 전송 합니다.

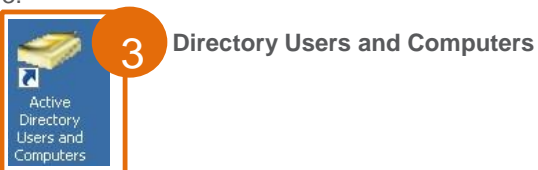
노트: 로밍 클라이언트가 AD 커넥터를 사용하여 사용자 ID 를 얻는 방법에 대 한 자세한 내용은 다음 링크에서 확인할 수 있습니다: <https://docs.umbrella.com/product/umbrella/appx-d-internal-domains/>

AD 사용자 생성하기

1. lab 토폴로지가 표시되는 browser (브라우저) 탭으로 돌아갑니다.
2. ad1 아이콘을 클릭하고 이전에 점퍼 클라이언트에 연결하는 데 사용한 것과 동일한 방법으로 원격 데스크톱을 통해 AD 에 연결합니다. 다른 브라우저 탭이 연결을 사용하여 열립니다.

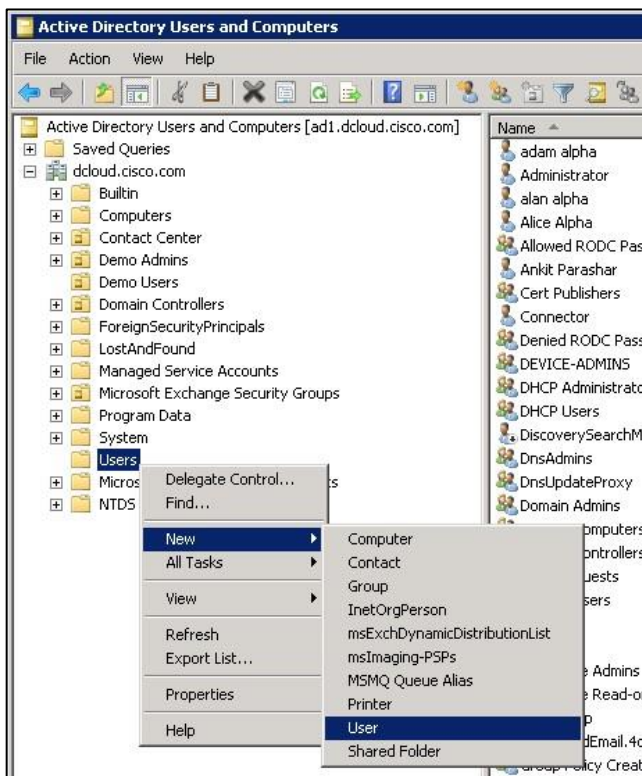


3. AD 서버에 로그인한 다음 **Active Directory Users and Computers** 의 데스크탑 바로가기 아이콘을 클릭합니다.



4. 왼쪽 분할 창의 서버 및 사용자 목록에서 **Users(사용자)**를 클릭합니다.

5. **Users** 를 마우스 오른쪽 버튼으로 클릭하고 **New > User** 를 선택합니다.

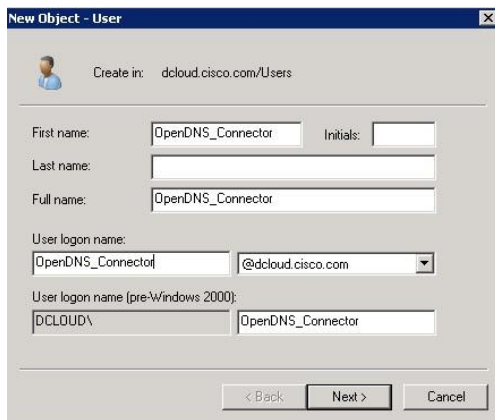


6. 다음 지정된 자격 증명으로 유저(User)를 생성합니다:

7. 이름: OpenDNS_Connector

8. 로그인 이름: OpenDNS_Connector

중요: AD connector 를 설치할 때 위의 언급된 이름을 정확히 사용하는 것이 중요합니다. 나중에 AD 커넥터를 설치할 때 같은 이름의 계정을 사용하여 AD 에 액세스합니다.



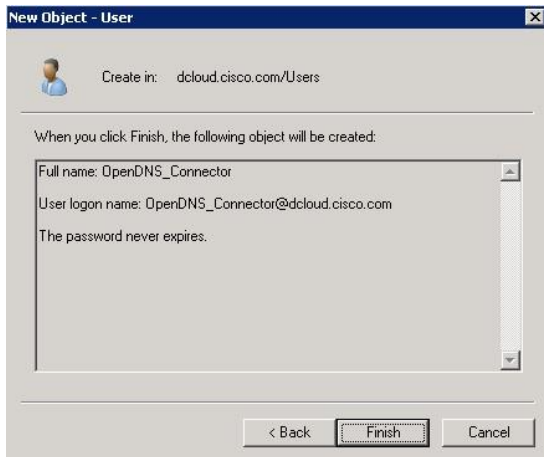
9. **Next** 를 클릭합니다.

10. 패스워드를 입력하고 확인합니다: **umbrellal@b123!** (선택한 다른 비밀 번호를 사용하려는 경우 백슬래시 또는 따옴표 없이 입력하십시오).

11. **Password never expires**(비밀번호가 만료되지 않음) 확인란을 선택하고 **OK** 를 클릭하여 팝업 메시지를 확인합니다.

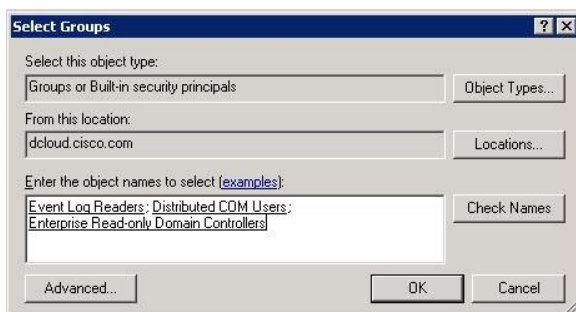


12. **Next** 를 클릭하고 다음 창에서 설정을 확인한 다음 **Finish** 를 클릭합니다.



13. 기본 창의 유저 목록에서 사용자(OpenDNS_Connector)를 찾습니다. 유저(User)를 마우스 오른쪽 버튼으로 클릭하고 **Add to a group** 을 선택합니다.
14. 다음 그룹에 멤버십을 추가합니다:
15. Event Log Readers
16. Distributed COM Users
17. Enterprise Read-only Domain Controllers

힌트: 그룹 이름의 처음 몇 글자를 입력하고 Check Names 버튼을 눌러 채울 수 있습니다. 이는 이름의 정확하게 입력되어 있는지 확인할 수 있는 좋은 방법입니다.

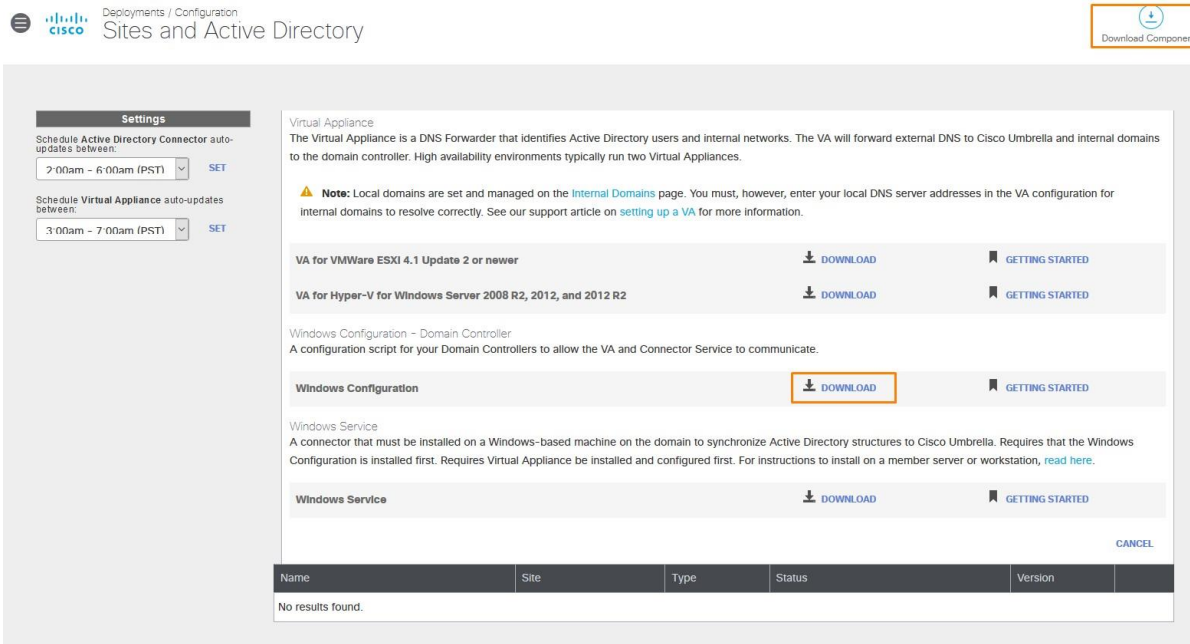


18. **OK** 를 클릭하여 그룹을 저장한 다음 확인 팝업 창에서 다시 **OK** 를 클릭합니다.



스크립트 실행

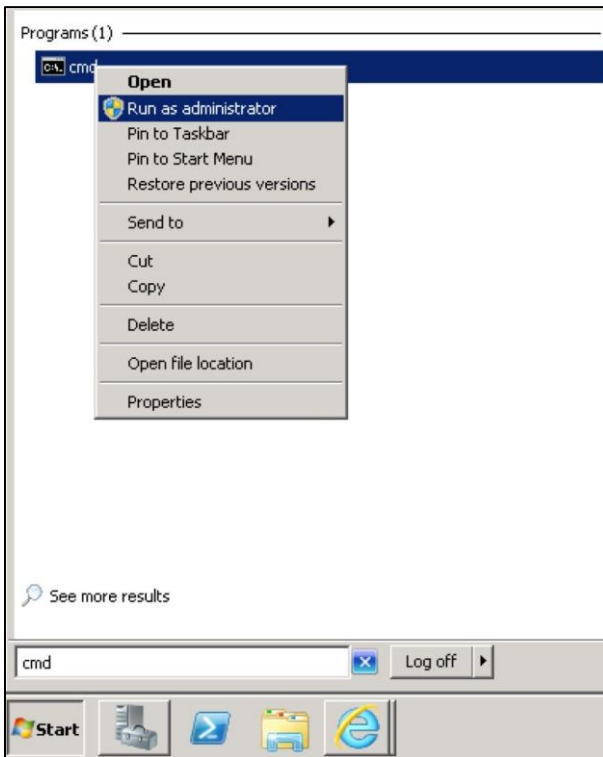
1. AD 서버에서 데스크톱의 바로 가기를 사용하여 Umbrella 대시보드에 액세스합니다..
2. 로그인한 다음 **Deployments > Configuration > Sites and Active Directory** 으로 이동합니다.
3. 페이지 상단의 구성 요소 Download Components 를 클릭한 다음 **Windows Configuration – Domain Controller** 를 클릭합니다. **DOWNLOAD** 를 클릭하여 Windows Configuration Script 를 다운로드합니다.



4. 파일을 저장하고 Windows Explorer 의 다운로드 폴더에서 확인합니다.

노트: Windows 구성 스크립트는 Visual Basic 으로 작성됩니다. 참조용으로,사람이 읽을 수 있는 지침을 자동화합니다:
<https://support.umbrella.com/hc/en-us/articles/230672247>.

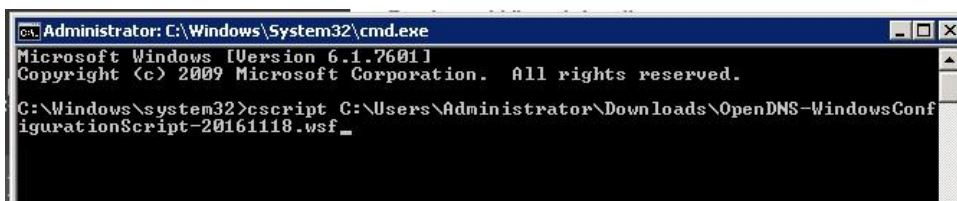
5. 스크립트를 관리자로 실행하려면, **Start > "cmd" 입력 > cmd** 프로그램을 마우스 오른쪽 버튼으로 클릭 > Run as administrator 하여 권한 명령 프롬프트입니다.



6. 그런 다음 명령 프롬프트에서 다음을 입력합니다.

```
cscript C:\Users\Administrator\Downloads\OpenDNS-WindowsConfigurationScript-20161118.wsf
```

팁: cscript 를 입력하고 공백을 입력한 다음 Downloads 폴더의 wsf 스크립트 파일을 명령 프롬프트 창으로 드래그합니다.



7. **Enter** 를 누릅니다. 스크립트에는 현재 구성이 표시되며, 작업을 위해 도메인 컨트롤러를 자동으로 구성하도록 제공됩니다. 프롬프트가 나타나면 **y** 를 입력하고 **Enter** 를 누릅니다. 자동 구성 단계가 성공적으로 수행되면 스크립트는 도메인 컨트롤러를 Umbrella 대시보드에 등록합니다.

```

Administrator: C:\Windows\System32\cmd.exe
AD User Exists: True
WMI Permissions Set: False
RDC Permissions Set: False

Audit Policy Set: True
Manage Event Log Policy Set: False

Event Log Readers MemberOf: True
Distributed COM MemberOf: True
*****
Your platform is supported for auto-configure.
Do you want us to auto configure this Domain Controller (y or n)? y

Configuring system...
Setting Remote Admin permissions on firewall...
Setting WMI permissions...
Setting RDC permissions...
Auto Config complete in full!
Registering Domain Controller in cloud...
Register Success!
Updating DC status in cloud...
Update success!

C:\Windows\system32>
    
```

- 스크립트가 실행된 후 Umbrella 대시보드에서 **Deployments > Configuration > Sites and Active Directory** 로 돌아가서 DC 가 표시되는지 확인합니다. 몇 분 내에 상태 아이콘이 녹색으로 바뀌어야 합니다. (그렇지 않은 경우 나중에 다시 이 페이지로 돌아가십시오).

Name	Site	Type	Status	Version	
AD1	Default Site	AD Server	run: a few seconds ago	---	

노트: 도메인 컨트롤러가 두 개 이상 있는 환경에서는 이 스크립트를 모든 "read-write" DC 에서 실행해야 Umbrella AD 커넥터와의 통합 준비할 수 있습니다. 스크립트는 "read-only" Dc 에서 실행할 필요가 없습니다. 구성 스크립트는 한번만 실행됩니다. 이는 애플리케이션 또는 서비스가 아닙니다. 도메인 컨트롤러의 IP 주소 또는 호스트 이름이 변경된 경우, Umbrella 대시보드에서 DC 의 이전 인스턴스를 제거합니다.

커넥터 설치하기

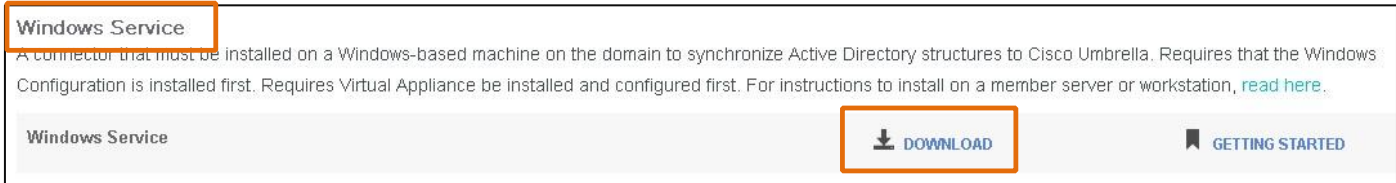
Umbrella AD 커넥터는 하나 이상의 도메인 컨트롤러를 모니터링하는 목적으로 합니다. 보안 이벤트 로그를 통해 사용자 및 컴퓨터 로그인을 수신하고 향후 가상 어플라이언스에서 IP-사용자 및 IP-컴퓨터 매핑을 사용하도록 설정합니다. 또한 사용자 대 그룹, 컴퓨터 대 그룹 및 그룹-그룹 멤버십을 Umbrella 와 동기화하여 그룹 기반 설정을 생성 및 시행 하고 사용자, 컴퓨터 및 그룹 기반 보고서를 볼 수 있습니다.

커넥터를 사용하면 Active Directory 사용자, 그룹 및 컴퓨터를 가져와 이러한 매핑을 제공할 수 있습니다. Organization Units (OUs)와 같은 다른 AD 개체는 가져오지 않습니다.

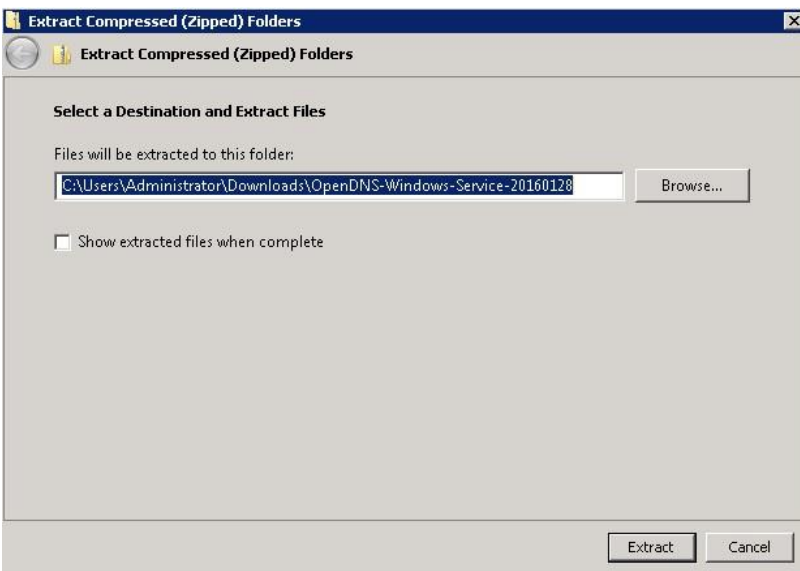
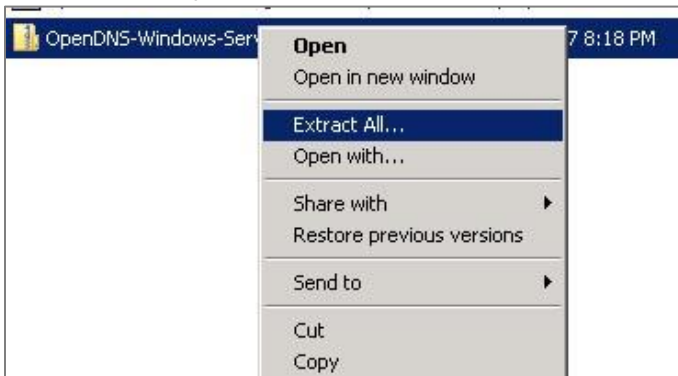
노트: Umbrella 사이트 당 단일 커넥터만 설치해야 하지만 하나 이상을 설치할 수도 있습니다. 보안 정책에서 사용자가 DC 에 직접 소프트웨어를 설치할 수 없는 경우, 동일한 도메인의 별도의 Windows 멤버에 Umbrella 커넥터를 설치할 수 있습니다 (<https://support.umbrella.com/hc/en-us/articles/231266048> 참조). 이전 단계에서 실행한 Windows 구성 스크립트는 계속해서 모든 DC 에서 실행해야 합니다.

노트: Umbrella 가상 어플라이언스 인터페이스는 향후 Cisco Umbrella 로 리 브랜딩됩니다.

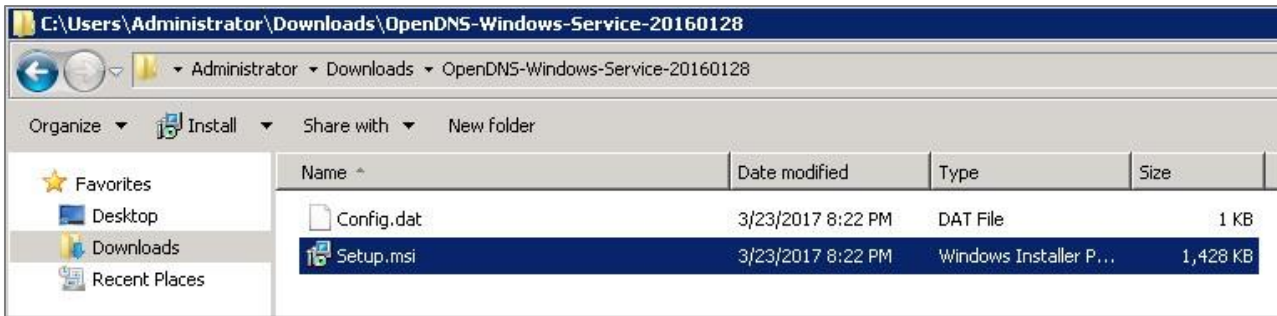
1. AD 서버 VM 의 대시보드에 있는 **Sites and Active Directory** 페이지에 페이지를 유지합니다.
2. **DOWNLOAD COMPONENTS** 섹션이 확장되었는지 확인하고 **Windows Service** 를 위해 **DOWNLOAD** 버튼을 클릭합니다.



3. Zip 파일을 저장하고 다운로드 폴더에서 해당 파일을 찾습니다.
4. 아카이브 (zip) 파일을 마우스 오른쪽 버튼으로 클릭하고 폴더에 해당 내용을 추출합니다.



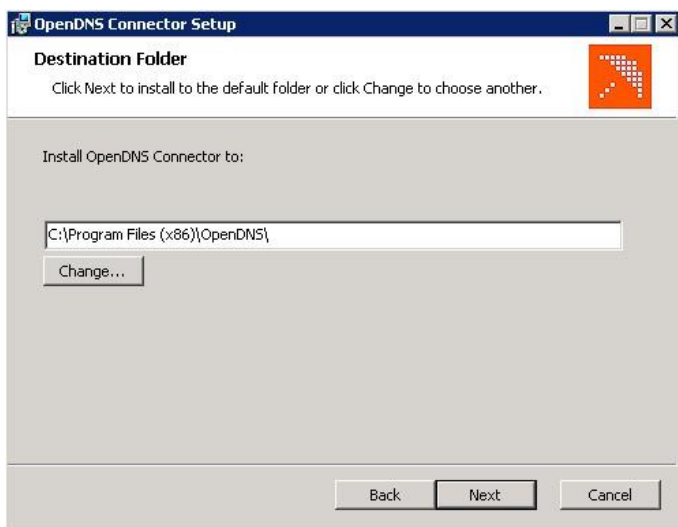
5. 추출한 폴더 (zip 폴더가 아님!)로 이동하고 **Setup.msi** 를 실행하여 커넥터 설치를 시작합니다. **Security warning** (보안 경고) 창에서 **Run** (실행)을 클릭합니다.



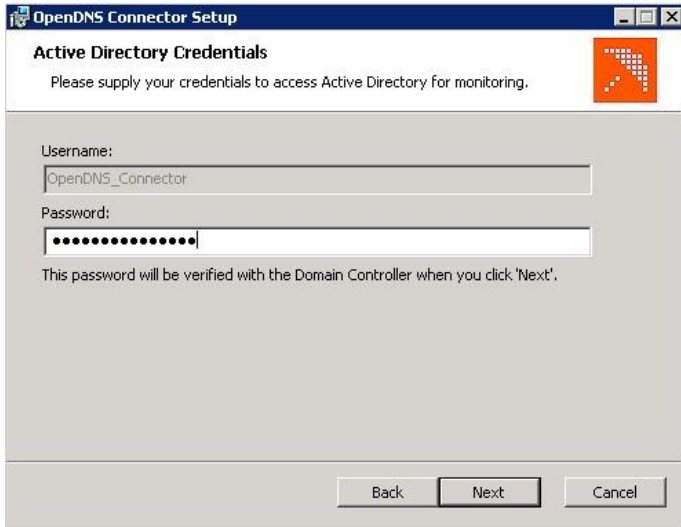
6. **Welcome**(시작) 페이지에서 **Next** 를 클릭합니다.



7. **Destination Folder**(대상 폴더) 창에서 기본 경로를 유지합니다.

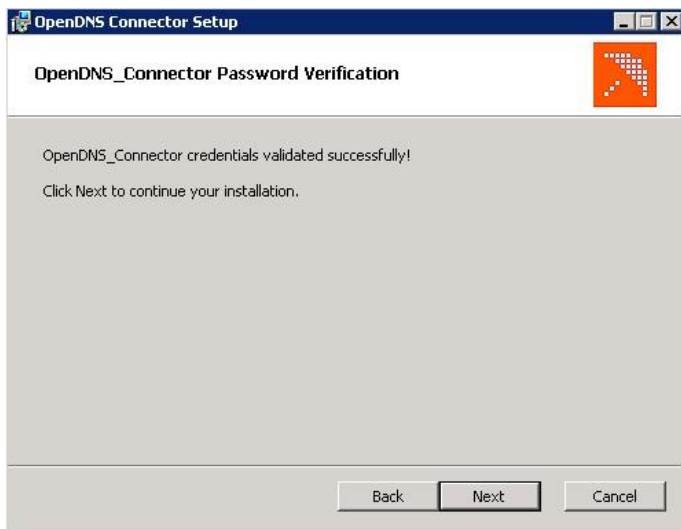


- Active Directory Credentials (Active Directory 자격 증명) 창에이 실습의 7 단계에서 정의한 패스워드 (원하는 다른 패스워드를 사용하지 않은 경우 - umbrellal@b123!)를 입력합니다. Next (다음)를 클릭하면 AD 와 비교하여 확인됩니다.

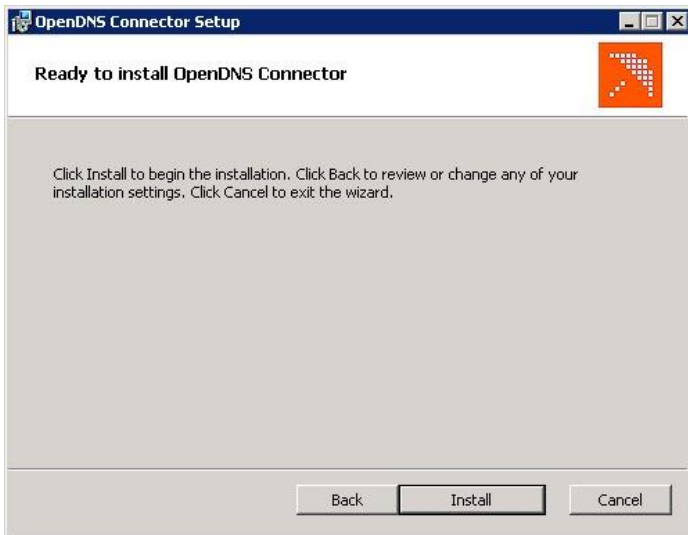


노트: 앞서 언급한 바와 같이 사용자 이름 OpenDNS_Connector 은 하드코딩 되어 있으며 설정 중에 변경할 수 없습니다.

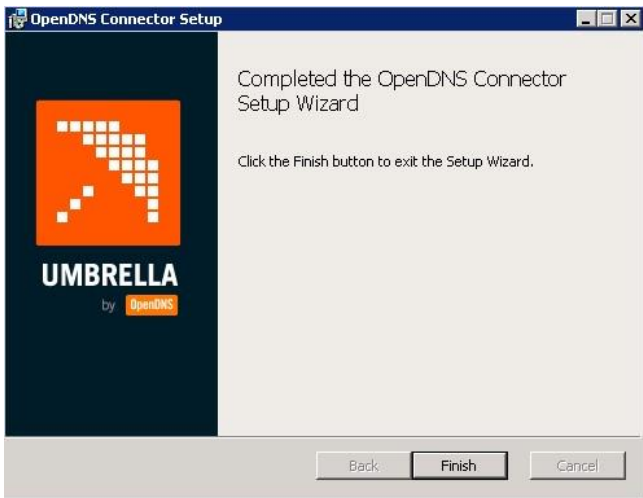
- 확인 창에서 **Next** 를 클릭합니다.



- Install** 를 클릭합니다.



11. 설치가 완료한 다음 **Finish** 를 클릭합니다.



12. 대시보드로 돌아가서 **Sites and Active Directory** 페이지에서 벗어난 다음 다시 대시보드로 이동합니다. 이제 설치된 AD 커넥터가 AD 서버와 함께 페이지에 볼 수 있습니다.

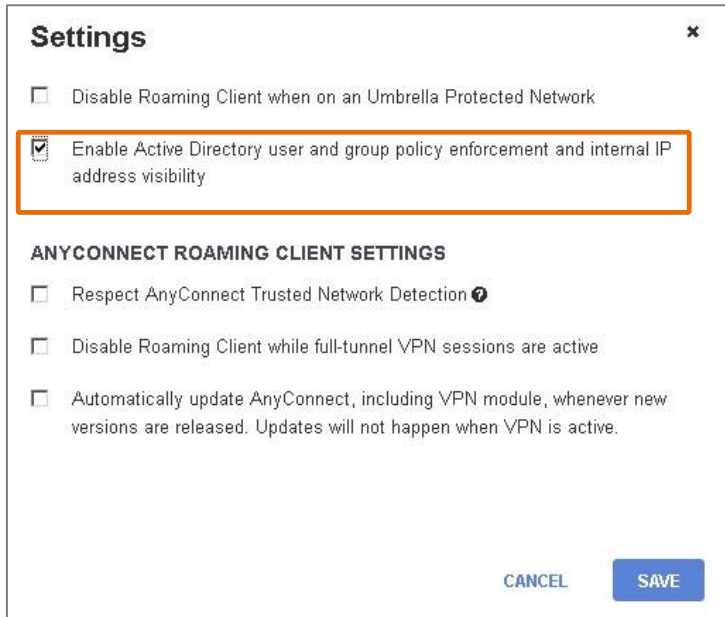
노트: 가상 어플라이언스 (VAs)를 설치하지 않고 AD Connector 를 설치되면 커넥터의 상태는 회색으로 유지되며 VA 가 설치된 후에만 녹색 상태로 변경됩니다. 상태가 빨간색으로 표시되지 않는 한, 이는 문제가 되지 않습니다.

Name	Site	Type	Status	Version	
ad1	📍 Default Site	AD Connec...	installed: 12 minutes ago ●	1.1.16	✖
AD1	📍 Default Site	AD Server	run: an hour ago ●	---	✖

13. 대시 보드에서 **Deployments > Core Identities > Roaming Computers** 페이지로 이동하고 상단의 설정 버튼을 클릭합니다.

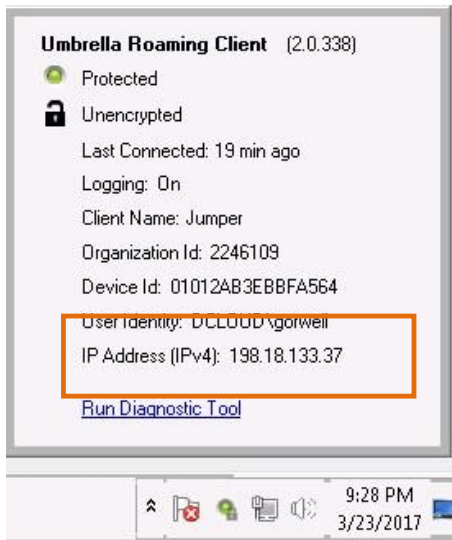


14. 열리는 Settings(설정) 페이지에서 AD 사용자 및 그룹 정책 시행 및 내부 IP 주소 가시성을 활성화하는 확인란을 선택합니다.

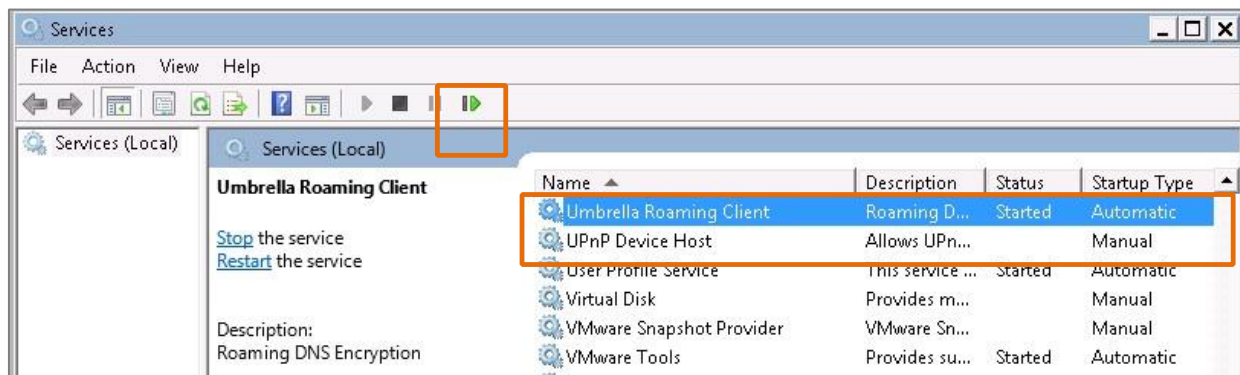


노트: 몇 분 안에 로밍 클라이언트는 사용자의 내부 IP 주소와 AD 세부 정보를 새로 고쳐서 선택해야 합니다.

15. 점퍼 클라이언트로 돌아가 시스템 트레이에서 로밍 클라이언트의 상태를 검사합니다. 이제 AD 사용자 세부 정보(Gorwell – George Orwell) 및 내부 IP 주소가 표시됩니다(그렇지 않을 경우 아래 단계를 참조하십시오).



16. 클라이언트가 몇 분 내에 IP 주소 및 사용자 세부 정보로 업데이트되지 않은 경우 **Windows Services** 콘솔을 열고 **Umbrella Roaming Client Windows** 서비스를 찾아 다음 다시 시작합니다. 그런 다음 클라이언트의 상태를 다시 확인합니다.



실습 4: 기본 정책 생성

이 실습에서는 다양한 구성 요소가 포함된 기본 정책을 생성한 다음 나중에 리포트에서 검색할 수 있는 몇 가지 검색 시나리오를 테스트합니다.

정책(Policies)은 ID의 일부 또는 전체에 적용할 수 있는 보안 보호, 범주 설정 및 개별 대상 목록을 규정합니다. 정책은 또한 로그 레벨 및 차단 페이지가 표시되는 방법을 제어합니다. 정책은 내림차순으로 시행되므로 동일한 ID를 공유하는 경우 최상위 정책이 두 번째 정책보다 먼저 적용됩니다. 정책의 우선순위를 변경하려면 간단하게 원하는 순서대로 정책을 끌어서 놓을 수 있습니다.

이 단계는 첫 번째 정책을 생성할 때 적용되며, 기존 정책을 수정하기 위해 반환할 때 다시 사용할 수 있습니다. 기본적으로는 항상 단일 정책(기본 정책)이 있습니다. 이 정책은 해당 ID에 다른 정책이 우선하지 않는 경우 모든 ID에 적용됩니다. 즉, Umbrella의 기본 정책은 조직 내 모든 ID가 베이스 라인 레벨을 보호하는 것을 보장하기 위한 것입니다.

대시보드에서 사용 가능한 ID 의 모든 조합에 정책을 적용할 수 있으며, 일부 범주 (예: AD 컴퓨터)를 확장하여 해당 정책의 영향을 받는 ID 를 선택적으로 선택할 수 있습니다..

정책을 생성하는 프로세스는 지정된 모든 ID 에 대해 거의 동일합니다. 이는 마법사를 통해 수행되며, 이는 Umbrella 대시보드의 **Policies > All Policies** 에서 찾을 수 있습니다.

노트: 정책에 대한 자세한 내용은 이 문서에서 확인할 수 있습니다: <https://docs.umbrella.com/product/umbrella/policy-precedence/>

1. 점퍼 클라이언트에서 브라우저 세션을 열고 브라우저의 북마크 바로 가기를 사용하여 다음 테스트를 실행합니다:
2. 악성 코드 사이트 예
3. 피싱 사이트 예
4. 모든 테스트 결과를 기록.
5. 여전히 **Jumper** 클라이언트에 있거나 로그인되어 있으면 데스크탑 바로 가기를 통해 Umbrella 대시보드에 액세스합니다.
6. **Policies > Management > Destination Lists** 으로 이동합니다.

노트: 이러한 리스트를 통해 명시적으로 차단되거나 허용되는 도메인 목록을 통해 필터링을 커스터마이징할 수 있습니다. 각 도메인 목록은 차단 목록 (디폴트) 또는 허용 목록으로 설정할 수 있습니다. 도메인을 `www.domain.com` 이 아닌 `.domain.com` 형식으로 추가하는 것이 권장합니다.

허용 목록 항목은 항상 차단 목록 항목보다 우선합니다. 예를 들어:

- Domain.com 를 차단하고 화이트리스트에 mail.domain.com 를 추가 하면 여전히 mail.domain.com 이 허용됩니다.
- 허용 목록에 domain.com 을 추가하고 sub.domain.com 을 차단하면 여전히 sub.domain.com 이 허용됩니다.

7. 기본 창 영역에서 **Global Allow List** (글로벌 허용 목록)를 클릭합니다. 도메인, IP 또는 CIDR 영역에서 **888.com** 를 입력합니다. **Enter** 를 눌러 이 도메인을 추가합니다.

Global Allow List	Type	Domains	IPs	URLs	Last Modified
	Allowed	0	0	0	May 10, 2013

List Name

Destinations on this list will be ALLOWED

No destinations have been added to this list

0 total

8. **Save** 를 클릭하여 글로벌 허용 목록을 저장합니다.

9. **Global Block List** 를 클릭합니다. **도메인 또는 URL** 영역에 **foxnews.com** 을 입력합니다. **Enter** 키를 눌러 이 도메인을 추가합니다.

Global Block List	Type	Domains	IPs	URLs	Last Modified
	Blocked	0	0	0	May 10, 2013

List Name

Destinations on this list will be BLOCKED

No destinations have been added to this list

0 total

10. **SAVE** 를 클릭합니다.

노트: 이제 **Custom Destination Block** 에서 특정 URL 의 차단을 정의하는 기능을 제공합니다(이전에는 도메인 전용으로 제한됨). 이 기능은 Umbrella 의 지능형 프록시를 통해 제공됩니다.

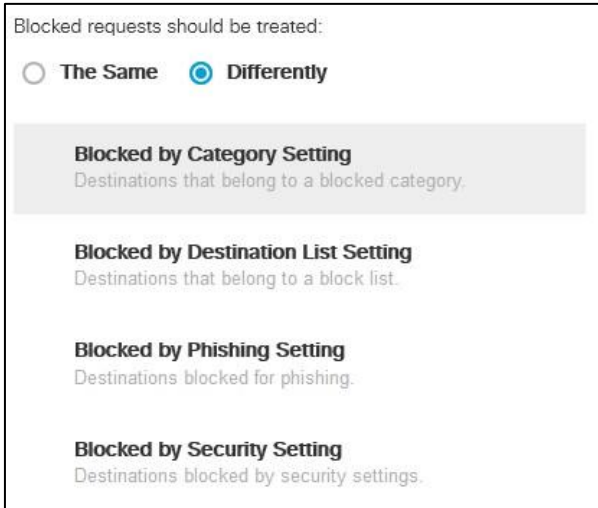
11. Global allow 및 block List 를 클릭하여 추가한 도메인을 확인할 수 있습니다.

12. **Policies > Block Page Appearance** 으로 이동합니다. 이 페이지에서 기본 차단 페이지를 수정하고 추가 블록 페이지를 생성할 수 있습니다.



13. 페이지 상단의 아이콘 **Add** 을 클릭하여 새 차단 페이지를 추가합니다.

14. **Differently** 라디오 버튼을 선택하고 특정 차단 결과 (차단 사유)에 대해이 블록 페이지를 사용하는 방법을 확인합니다.




15. 블록 페이지에 사용할 수 있는 다른 옵션을 확인한 다음 **CANCEL** 를 클릭합니다.

노트: 블록 페이지는 사용자 지정 URL 또는 IP 로 리디렉션할 수도 있습니다. 커스텀 URL 또는 IP 로 리디렉션하지 않는 경우 차단된 사용자가 관리자에게 연락할 수 있도록 연락처 이메일 주소를 추가할 수 있습니다.

노트: Bypass (바이패스) 설정은 블록 페이지를 우회하기 위한 옵션 (이미 정의 되어 있는 경우)을 설정합니다.

노트: HTTPS 사이트에 대한 DNS 쿼리가 Umbrella 에 의해 차단되는 경우 기본적으로 사용자에게 브라우저 경고가 표시됩니다. 이는 클라이언트 브라우저에 Cisco Root Certificate (클라이언트 브라우저)를 설치하여 해결할 수 있습니다.

16. **Policies > All Policies** 으로 이동합니다. 정보 영역이 확장되지 않은 경우  를 클릭하여 확장합니다. 정책에 대한 정보를 읽습니다.



17. **Add** 아이콘을 클릭하여 새 정책을 추가합니다. 정책 마법사가 시작되고 첫 번째 단계는 이 정책에 ID 를 적용하는 것입니다.

노트: 설치한 AD 커넥터는 사용자 및 컴퓨터 그룹 멤버십 및 향후 모든 변경 사항을 Umbrella 와 자동으로 동기화해야 합니다. 검색 창에서 다음 ID 중 일부를 검색하여 이 문제가 성공적으로 발생 했는지 확인할 수 있습니다. George Orwell. OpenDNS_Connector; Jumper.

18. **AD Users** (AD 사용자)를 클릭하고 목록에서 **George Orwell** 을 검색 합니다. 또한 **Search Identities** (ID 검색) 창에서 이름 입력을 시작할 수 있습니다. 사용자를 찾은 후에는 확인란을 선택하여 오른쪽 영역에 사용자를 선택하고

추가합니다. 지금까지 로밍 클라이언트를 통해 단일 사용자만 구축 했으므로 이 정책은 해당 사용자 에게만 적용됩니다.



What would you like to protect?

Select Identities

aeorael

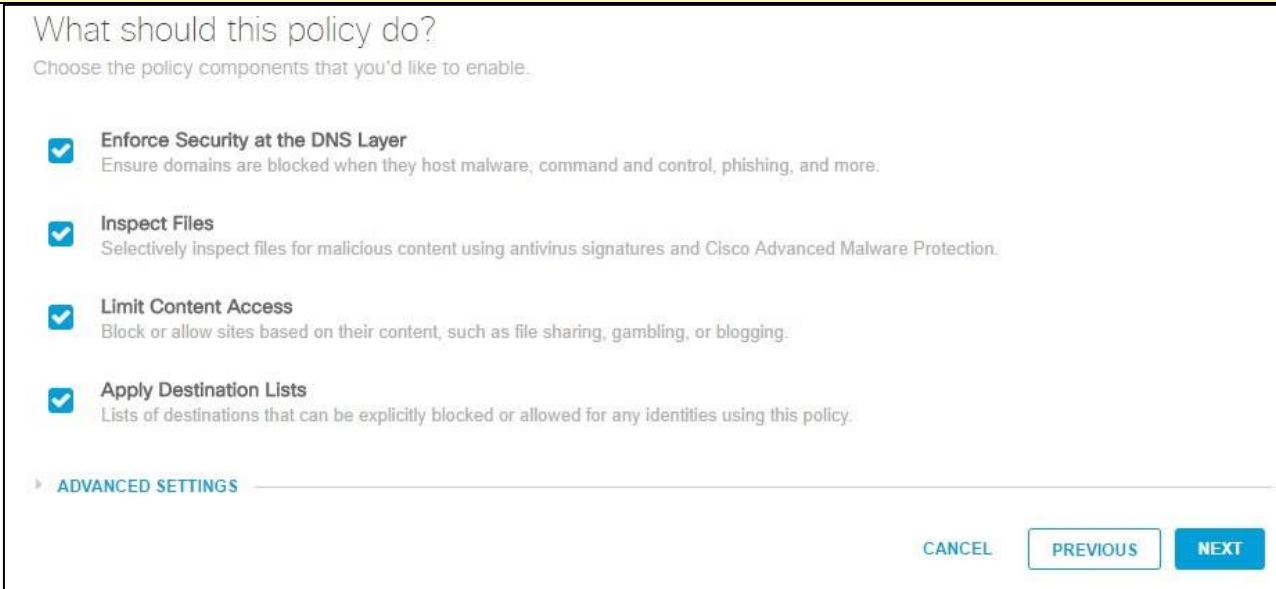
1 Selected

George Orwell

19. **Next** 를 클릭하여 정책의 다음 부분으로 진행합니다.

20. 다음 페이지에는이 정책에서 활성화될 기본 정책 구성 요소가 나열 되어 있습니다. 이러한 구성 요소를 선택하지 않은 경우 모든 옵션을 활성화 하도록 해당 구성 요소를 클릭합니다.

노트: 정책을 수정할 수 없는 경우에는 그대로 저장하고 다시 클릭하여 확장 하면 됩니다. 이제, 다음 단계에서 볼 수 있는 것 처럼 변경할 수 있습니다.



What should this policy do?

Choose the policy components that you'd like to enable.

- Enforce Security at the DNS Layer**
Ensure domains are blocked when they host malware, command and control, phishing, and more.
- Inspect Files**
Selectively inspect files for malicious content using antivirus signatures and Cisco Advanced Malware Protection.
- Limit Content Access**
Block or allow sites based on their content, such as file sharing, gambling, or blogging.
- Apply Destination Lists**
Lists of destinations that can be explicitly blocked or allowed for any identities using this policy.

▶ **ADVANCED SETTINGS**

CANCEL PREVIOUS NEXT

노트: 현재 이 랩 인프라의 네트워크 제약으로 인해 IP 레이어 시행을 구현할 수 없습니다. 옴으로 이 기능을 랩에서 포함시키기를 기대합니다!

노트: 이 기능은 로밍 클라이언트의 기술을 통해 해당 연결을 Umbrella 로 라우팅하는 데 구현됩니다. (독립형 로밍 클라이언트 및 AnyConnect 로밍 클라이언트 모두에서 지원됨).

21. **ADVANCED SETTINGS** (고급 설정)를 클릭합니다. SSL 암호 해독 또는 IP 레이어 시행을 활성화하지 않고 지능형 프록시가 활성화되어 있는지 확인합니다.

ADVANCED SETTINGS

Enable Intelligent Proxy
Gain visibility into threats, content, or apps by proxying web connections for risky domains.

SSL Decryption
Enhances security by performing inspection of HTTPS traffic for deeper security insight. Turning on SSL decryption allows HTTPS URL blocking.

Enable IP-Layer Enforcement
Gain visibility into threats that bypass DNS lookups by tunneling suspect IP connections. Note: this is only available for Roaming Computer identities.

ALLOW-ONLY MODE

Allow-Only Mode
Only connections explicitly listed to be specifically granted; otherwise connections will be blocked by default.

LOGGING

Log All Requests

Log Only Security Events
Log and report on only those requests that match a security filter or integration, with no reporting on other requests.

Don't Log Any Requests
Note: No requests will be reported or alerted on. Unreported events will still be logged anonymously and aggregated for research and threat intelligence purposes.

[CANCEL](#) [PREVIOUS](#) [NEXT](#)

22. **Allow-Only Mode**(허용 전용 모드)를 활성화하지 마십시오(단, 작동 방식에 대한 설명을 읽으십시오).
23. **LOGGING** 에서 모든 요청이 기록되는지 확인합니다(디폴트 설정). 로그를 실행하지 않으면 나중에 리포트에 결과가 표시되지 않습니다.
24. **Next** 를 클릭하여 정책의 다음 부분으로 진행합니다.
25. **Security Settings**(보안 설정) 페이지에는 Umbrella 가 식별하고 적용하는 다양한 보안 범주가 나열됩니다. **CATEGORIES TO BLOCK** 옆의 **EDIT**(편집)을 클릭하면 선택 항목을 사용할 수 있습니다.

1 Security — 2 Content — 3 Destinations — 4 Block Pages — ★ Summary

Security Settings

Ensure identities using this policy are protected by selecting or creating a security setting. Click [Edit Setting](#) to make changes to any existing settings, or select [Add New Setting](#) from the dropdown menu.

Default Settings

CATEGORIES TO BLOCK

[EDIT](#)

26. 각 보안 범주에 대한 설명을 참고하십시오. 모든 옵션을 선택하고 **SAVE** 를 클릭 합니다. 확인 창에서 **PROCEED** 를 클릭합니다.

- Malware**
Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more
- Newly Seen Domains**
Domains that have become active very recently. These are often used in new attacks.
- Command and Control Callbacks**
Prevent compromised devices from communicating with attackers' infrastructure
- Phishing Attacks**
Fraudulent websites that aim to trick users into handing over personal or financial information
- Dynamic DNS**
Block sites that are hosting dynamic DNS content
- Potentially Harmful Domains**
Domains that exhibit suspicious behavior and may be part of an attack.
- DNS Tunneling VPN**
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.

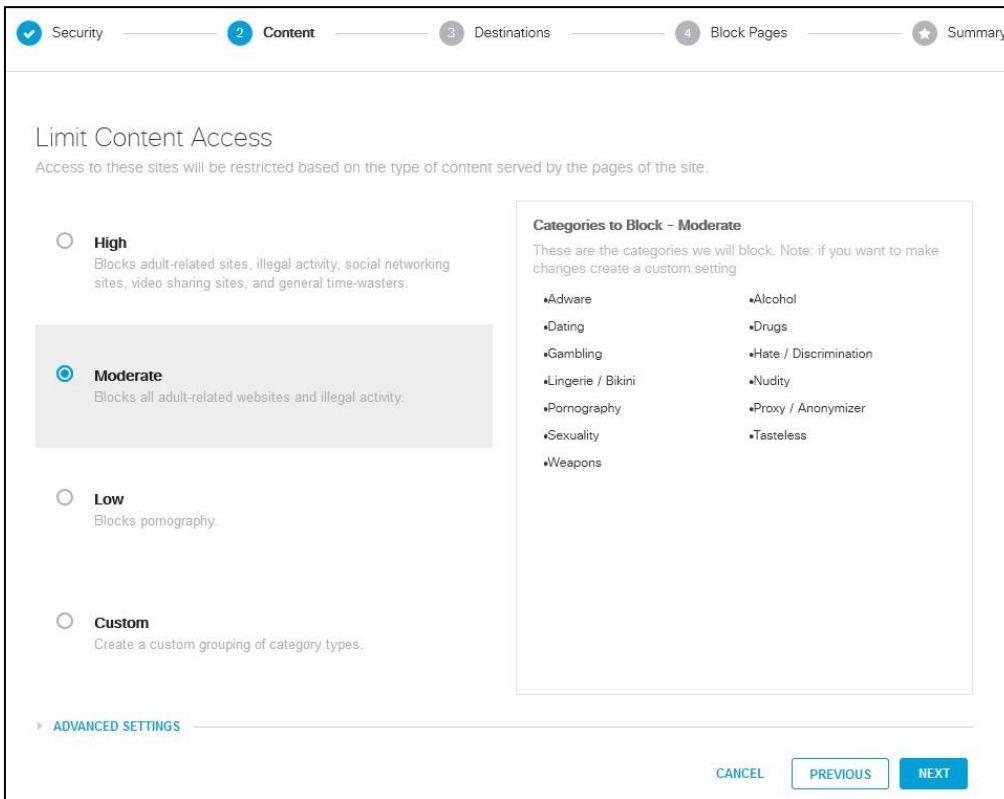
[CANCEL](#) [SAVE](#)

노트: 앞에 리포트에서는 "Command and Control Callbacks(명령 및 제어 호출)" 보안 범주를 "Botnets(보트넷)"이라고 합니다(이 보안 범주의 기존 이름). 앞으로, 이 두 곳이 모든 위치에 정렬될 예정입니다.

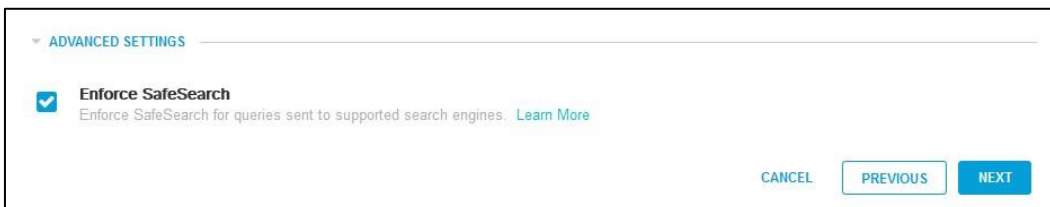
27. 정책 마법사로 돌아가서 **NEXT** 를 클릭하여 정책의 다음 부분으로 진행 합니다..

28. **Content Settings** (콘텐츠 설정) 페이지에서 서로 다른 차단 레벨을 클릭하고 각 범주에 대해 표시되는 다양한 범주를 확인합니다. **Moderate** 레벨을 선택하여 완료합니다.

노트: 모든 범주에 대한 자세한 내용은 <https://support.umbrella.com/hc/en-us/articles/231265768> 에서 참조하십시오.



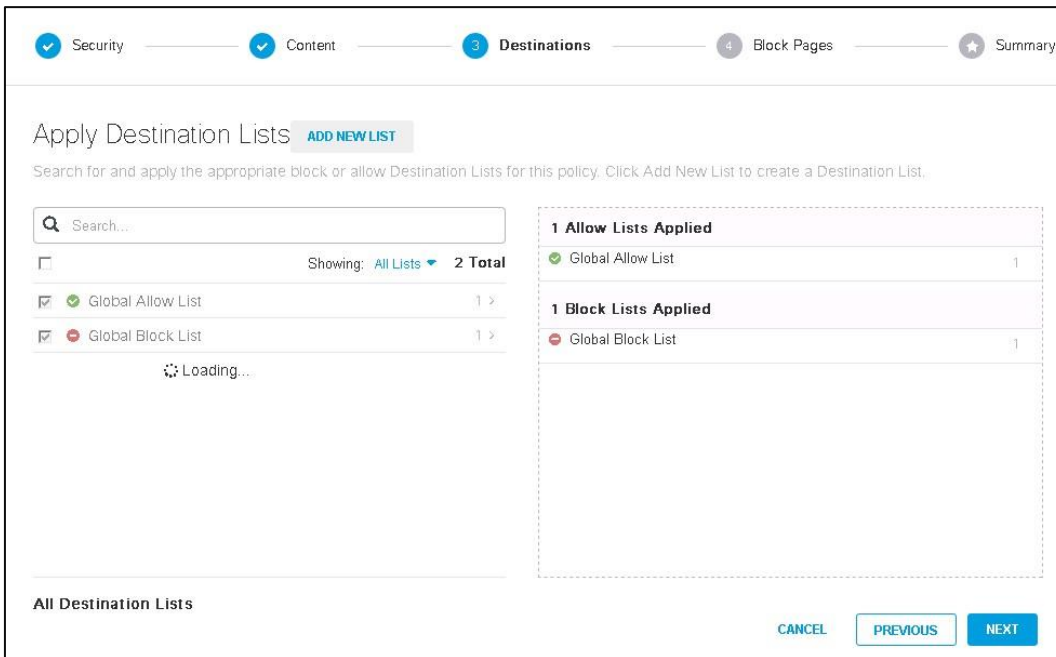
29. **ADVANCED SETTINGS** 을 클릭하고 Enforce SafeSearch 확인란을 선택하여 활성화합니다.



30. 자세한 정보는 **Learn More** 링크를 클릭하여 해당 기능에서 수행하는 작업, 작동 방식, 인증 방법에 대한 문서를 확인할 수 있습니다.

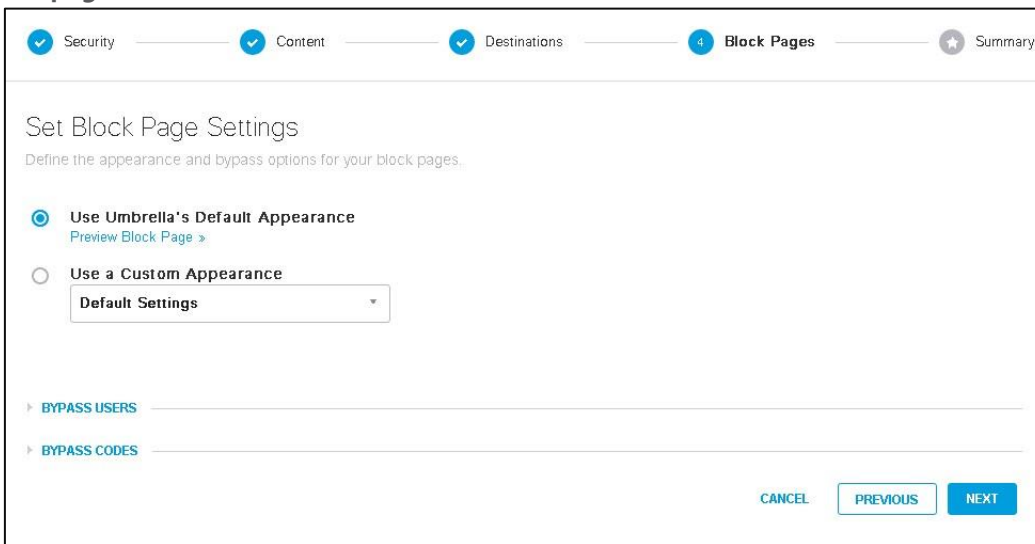
31. **NEXT** 를 클릭하여 정책의 다음 단계를 계속 진행합니다.

32. **Destination Lists** 페이지에서 이전에 편집한 기본 허용 목록과 차단 목록이 모두 적용됩니다. (**ADD NEW LIST** 버튼을 통해 여기서 새 목록을 정의하고 추가할 수도 있습니다.)



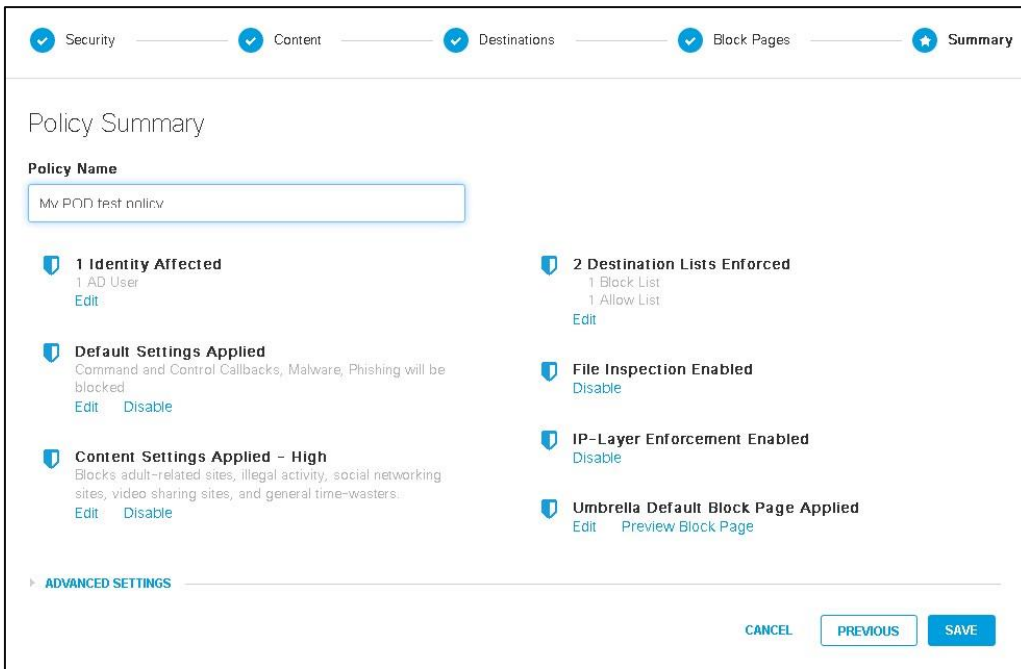
33. **NEXT** 를 클릭하여 정책의 다음 단계를 수행합니다.

34. **Block Pages** 페이지에서 기본 차단 페이지 (디폴트 설정)를 사용하록 선택하거나 이전에 관찰한 **custom block page** 를 선택/생성하도록 선택할 수 있습니다. **Default** 차단 페이지를 선택된 상태로 유지합니다.



35. **NEXT** 를 클릭하여 **Summary** 페이지에 액세스합니다.

36. 새 정책의 이름을 입력하고 **SAVE** 를 클릭하여 정책을 저장합니다.



37. 정책 목록은 새로 생성한 정책을 **Default** 정책 위에 표시합니다.

노트: 정책을 드래그 앤 드롭하여 적용되는 순서 (위에서 아래로)를 변경할 수 있습니다. 그러나 Default Policy 는 항상 목록의 마지막 정책이므로 Default Policy 가 아닌 새 정책 하나만 추가되었으므로 이 시점에서 순서를 변경할 수 없습니다. 정책 목록을 계획할 때, 특히 사용자가 둘 이상의 ID 에 포함될 수 있는 경우에는 위에서 아래로 순서를 기억해야 합니다.

정책이 ID 에 어떻게 적용되는지 자세히 알아보려면 <https://support.umbrella.com/hc/en-us/articles/230906428> 를 참조하십시오.

정책 구성에 대한 모범 사례를 보려면 <https://support.umbrella.com/hc/en-us/articles/230566087> 를 참조하십시오.

실습 5: 브라우징 활동 생성 및 기본 활동 보고서 실행

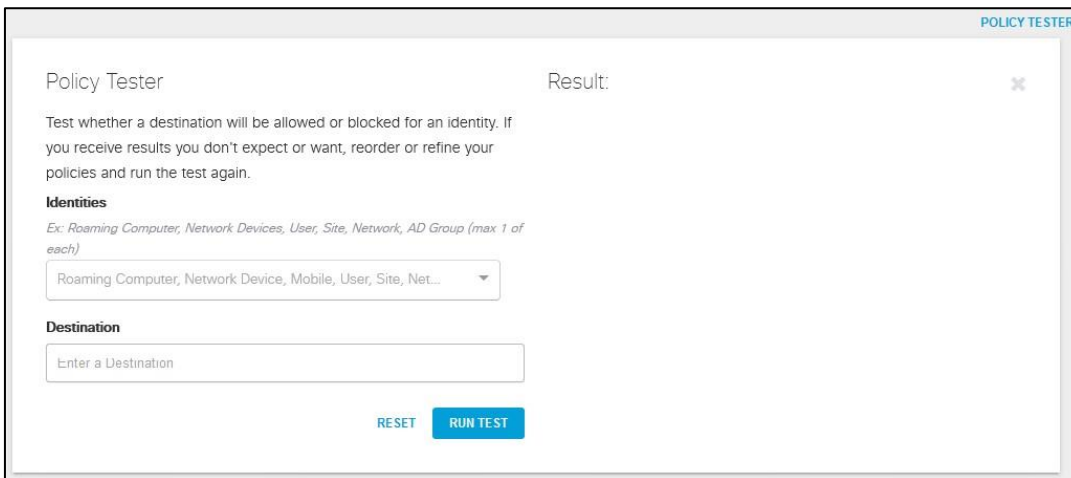
이 연습에서는 정책에서 허용하거나 차단해야 하는 다양한 호스트를 찾습니다. 검색 활동을 생성한 후에는 기본 활동 보고서를 실행하고 결과를 검토합니다.

1. Jumper 클라이언트에서 다른 브라우저 탭을 열고 브라우저 상단에 있는 북마크 바로 가기를 사용하여 예제 악성 코드 사이트, 피싱 사이트 예시 및 IP 차단을 테스트 합니다.
2. www.poker.com 으로 이동합니다. 요청이 허용되거나 차단되었습니까? 이유는 무엇입니까?
3. www.888.com 으로 이동합니다. 요청이 허용되거나 차단되었습니까? 이유는 무엇입니까?
4. www.cnn.com 으로 이동합니다. 요청이 허용되거나 차단되었습니까? 이유는 무엇입니까?

5. www.foxnews.com 으로 이동합니다. 요청이 허용되거나 차단되었습니까? 이유는 무엇입니까?
6. 선택한 몇 가지 다른 웹사이트로 이동하고, 허용할 것으로 예상되는 일부 웹사이트를 선택하고, 사용자에게 대해 방금 생성한 정책에 따라 차단해야 하는 다른 웹사이트를 선택합니다.
7. 지원되는 사이트 (Google, YouTube 및 Bing)를 탐색하여 SafeSearch 적용을 확인합니다. 이 기능을 테스트하는 방법에 대한 자세한 내용은 [이 문서](#)를 참조하십시오.

노트: DNS 레이어에서 SafeSearch 가 적용되는 방식을 확인합니다. 다른 솔루션 (이 사이트들은 일반적으로 HTTPS 임)과 마찬가지로 이를 지원하기 위해 HTTPS 를 암호 해독할 필요가 없음을 의미합니다.

8. **Policy Tester** 는 정책이 작동하는 방식과 기대하고 있는지 여부를 파악 하는 데 유용한 도구입니다. 이 툴은 유용한 트러블슈팅 툴이며 더 쉽게 Umbrella 를 사용하는 방법을 강조할 수 있는 툴입니다. 이 툴을 사용해 보도록 하겠습니다. 이 툴은 대시보드의 **POLICY** (정책) 페이지 상단에서 찾을 수 있으며, **POLICY TESTER** 를 클릭하여 액세스할 수 있습니다.

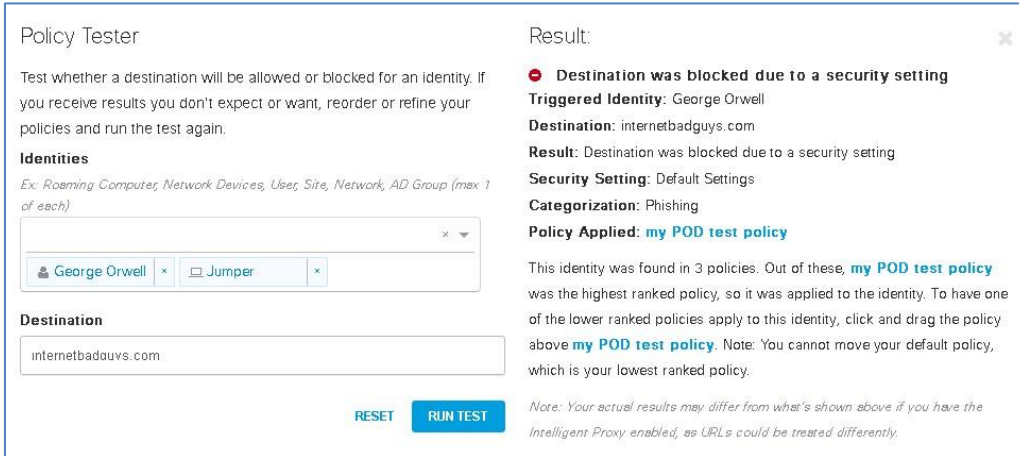


9. 두 개의 필드 (필수) - 즉 테스트할 **identity** 또는 **identities** 및 **destination** 을 비교 합니다. 테스터는 사용자가 선택한 identity 가 입력한 목적지에 도달할 수 있는지 여부에 따라 정책을 구성한 방식에 따라 결정합니다. 또한 이 툴은 결과가 있는 이유를 설명하기 위한 지원을 제공합니다.

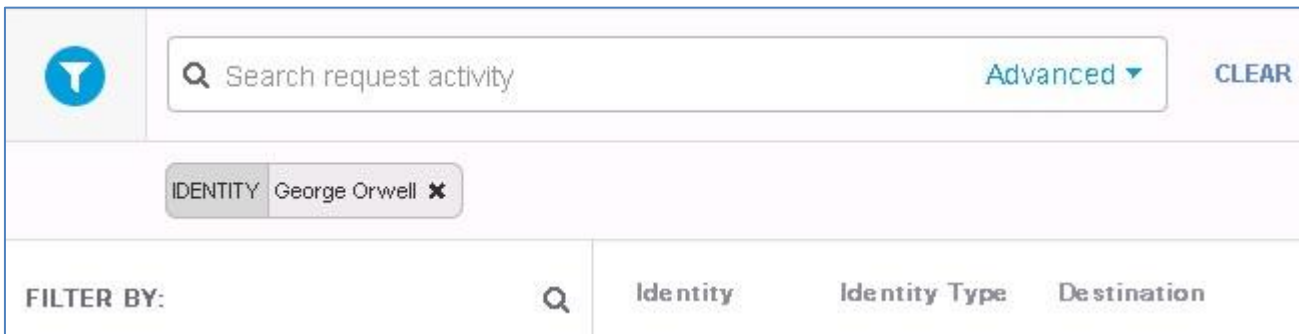
노트: Identities 를 입력할 때 필드에 'type ahead'를 입력하고 검색을 수행할 수 있으므로 문자 A 를 입력하면 해당 문자가 포함된 모든 identities 의 목록이 제공됩니다. 두 개 이상의 identities 를 입력할 수 있는 이유는 identities 중 어떤 것이 우선 순위를 가지고 있는지를 확인하는 것입니다. 예를 들어 로밍 클라이언트가 설치되어 있고 하나 이상의 네트워크 identities 를 사용하여 보호되었던 컴퓨터에 대한 정책이 있는 경우 이러한 정책이 적용되는 것이 분명하지 않을 수 있습니다. Policy tester(정책 테스터)는 어떤 정책을 통해 그리고 어떤 identity 를 먼저 트리거할 것인지를 알려줍니다.

노트: 입력한 목적지는 정규화된 도메인 이름이 될 수 있습니다. IP 주소 및 Url 은 아직 지원되지 않습니다.

- 원하는 identity 또는 identities 를 선택하고 필요한 destination(대상)을 선택한 후에는 **RUN TEST** (테스트 실행)를 클릭합니다.
- 결과를 확인하고 몇 가지 다른 검색 옵션을 시도합니다.



- 다음으로, 몇 가지 기본 보고서를 실행하여 검색 활동을 확인합니다. **Reporting > Activity** 로 이동합니다.
- 페이지 상단의 시간 대괄호가 **LAST 24 HOURS** 로 설정되었는지 확인합니다.
- Search Requests** (검색 요청) 박스에서 사용자 이름이 나타날 때까지 사용자 이름 (George ...)을 입력합니다. 필터를 추가하려면 클릭합니다.



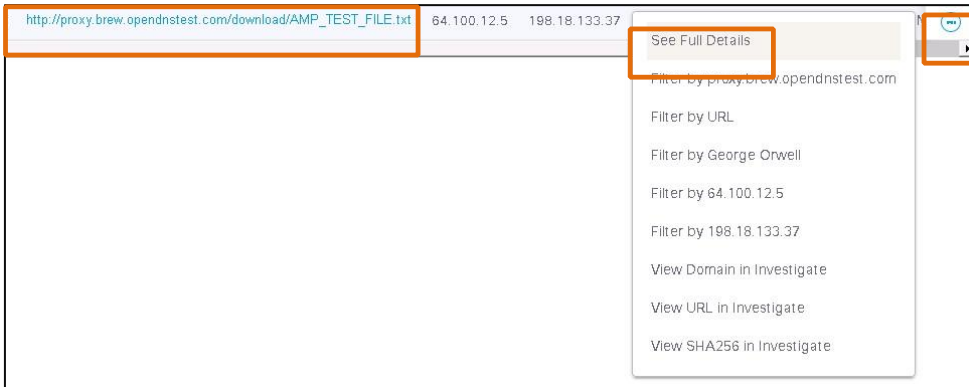
- 결과 창 왼쪽에 있는 표시 필터를 사용하여 다른 방식으로 결과를 필터링합니다(**APPLY** 를 클릭하여 결과를 업데이트합니다).

FILTER BY:		Identity	Identity Type	Destination	DNS Type	Public IP
Response Select All <input type="checkbox"/> Allowed <input type="checkbox"/> Blocked <input type="checkbox"/> Proxied <input type="checkbox"/> Allowed: Destination List <input checked="" type="checkbox"/> Blocked: Destination List		George Orwell	AD Users	nyt.com	A	64.100.12.5
		George Orwell	AD Users	nyt.com	AAAA	64.100.12.5
		George Orwell	AD Users	nyt.com	A	64.100.12.5
		George Orwell	AD Users	nyt.com	A	64.100.12.5
		George Orwell	AD Users	nyt.com	A	64.100.12.5
		George Orwell	AD Users	nyt.com	A	64.100.12.5
		George Orwell	AD Users	nyt.com	A	64.100.12.5
		George Orwell	AD Users	nyt.com	A	64.100.12.5
		George Orwell	AD Users	nyt.com	A	64.100.12.5
		George Orwell	AD Users	nyt.com	A	64.100.12.5
		George Orwell	AD Users	nyt.com	A	64.100.12.5

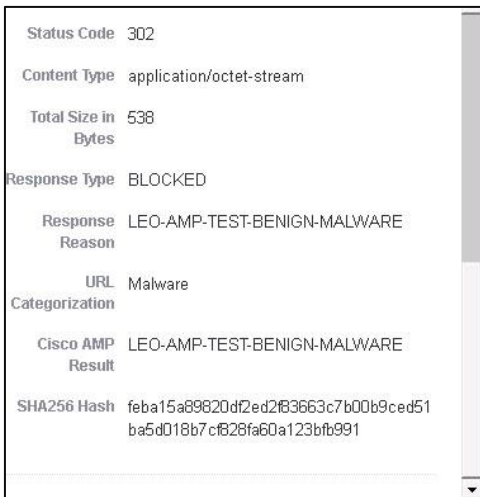
16. 결과 테이블의 오른쪽 상단에서 **All Requests** (모든 요청)를 클릭하고 드롭다운 목록에서 **URL Requests** 를 선택합니다. 어떤 결과가 표시 됩니까? 이유는 무엇입니까?

Columns	Domain Requests (DNS) ▼
Categories	Date & >
Search Engines	May 31, <>
Search Engines	May 31, <>
Global Whitelist	May 31, <>
Search Engines	May 31, <>

- URL Requests** (URL 요청) 드롭다운 버튼을 클릭하고 DNS 레이어에서 시행된 활동을 표시하는 **Domain Requests** (DNS) 옵션을 선택합니다.
- 다른 브라우저 탭에서 **AMP Test File** 및 **AV Test File** 브라우저 북마크를 통해 몇 가지 테스트 브라우징 요청을 수행합니다.
- 대시보드로 돌아가 다른 영역으로 이동한 다음 **Activity Report** 로 돌아가 **URL request** 옵션을 다시 선택합니다. 이제 마지막으로 수행한 검색 활동을 사용하여 결과가 업데이트됩니다.
- 목적지에서 **AMP_TEST_FILE** 을 표시하는 라인을 찾습니다. 오른쪽에 있는 **View Actions** (작업 보기) 버튼을 클릭하고 **See Full Details** 를 선택합니다.



21. 아래로 스크롤하여 AMP 에 의해 차단된 파일의 세부 사항을 검토합니다. 파일의 **SHA256** 해시가 표시되었음을 확인합니다.



노트:

노트: 보고서(reporting)는 lab 의 보고서 섹션에서 더 자세히 다룹니다.

중요: 이제 이 랩을 완료하기 위해 학점을 수신하는 데 필요한 연습을 완료 했습니다. 다음 단계를 수행하여 증거를 제출합니다:

1. Umbrella 대시 보드에서 **Reporting > Security Activity** 으로 이동합니다.
2. 왼쪽 영역에서 **Blocked** 를 클릭하여 차단된 보안 이벤트만 필터링합니다.
3. **TIME** 을 **Last 24 Hours** 설정으로 유지합니다.
4. 결과 목록에서 몇 개를 확장하고 2 개의 블록 이벤트를 찾습니다. 하나는 ID 유형이 **Roaming Computer** 이고 ID 유형이 **AD user** 임을 표시하는 것입니다.
5. 모든 세부 정보 (오늘 날짜 및 ID 유형)가 포함된 이러한 2 개 이벤트를 표시하는 화면 캡처 (필요한 경우 2 화면 캡처)를 가져옵니다.

6. [요기](#)를 클릭하여 수집된 화면 캡처를 이메일을 통해 표시되는 것으로 보냅니다.

노트: **Security Activity** 보고서는 이 실습의 보고 모듈 (시나리오)의 [실습 2](#) 에서 더 자세히 다룹니다.

실습 6: AnyConnect 로밍 클라이언트 설치 (선택적 실습)

또한 AnyConnect 를 VPN 클라이언트로 사용하는 경우에는 **AnyConnect** 모듈을 통해서도 Umbrella 로밍 클라이언트를 설치할 수 있습니다. 이 새로운 방법을 사용 하면 AnyConnect 고객 (1 억 8500 만 설치)을 통해 Umbrella 를 쉽게 구축할 수 있습니다. 고객의 엔드포인트에서 실행해야 하는 클라이언트 수를 제한하는 것이 좋습니다. 이 실습에서는 Windows 7 Jumper 클라이언트에 AnyConnect 로밍 모듈을 설치 합니다..

노트: Umbrella (독립형) 로밍 클라이언트가 이미 시스템에 설치되어 있는 경우, AnyConnect 버전의 클라이언트 **설치**가 독립형 인스턴스를 **제거합니다**. 이는 정상적인 동작입니다. 이 실습 세션에서는 AnyConnect 클라이언트를 구축하기 전에 독립형 로밍 클라이언트 (설치 된 경우)를 수동으로 제거합니다.

노트: 이 실습 세션에서 두 로밍 클라이언트 옵션의 구축을 계획하는 경우, 이 시나리오의 [실습 2](#) 에서 먼저 Umbrella (독립형) 로밍 클라이언트로 시작한 다음 이 연습을 진행하는 것이 좋습니다.

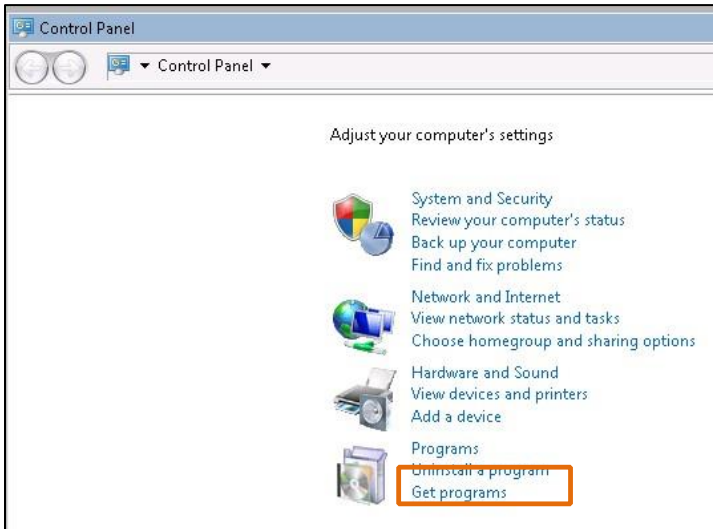
중요: 이 실습의 단계 순서는 중요하며 독립형 로밍 클라이언트를 이미 설치하여 구축했는지 여부에 따라 달라집니다. 관련된 경로를 읽고 따르십시오.

경로 1: 이 랩 세션에서 아직 Umbrella (독립형) 로밍 클라이언트를 구축하지 않은 경우, 먼저 아래의 1-2 단계를 완료한 다음 스텝 13 으로 건너뛰고 계속 진행합니다.

경로 2: 이 랩 세션에서 이미 Umbrella (독립형) 로밍 클라이언트를 구축한 경우, 아래 3 단계부터 시작합니다.

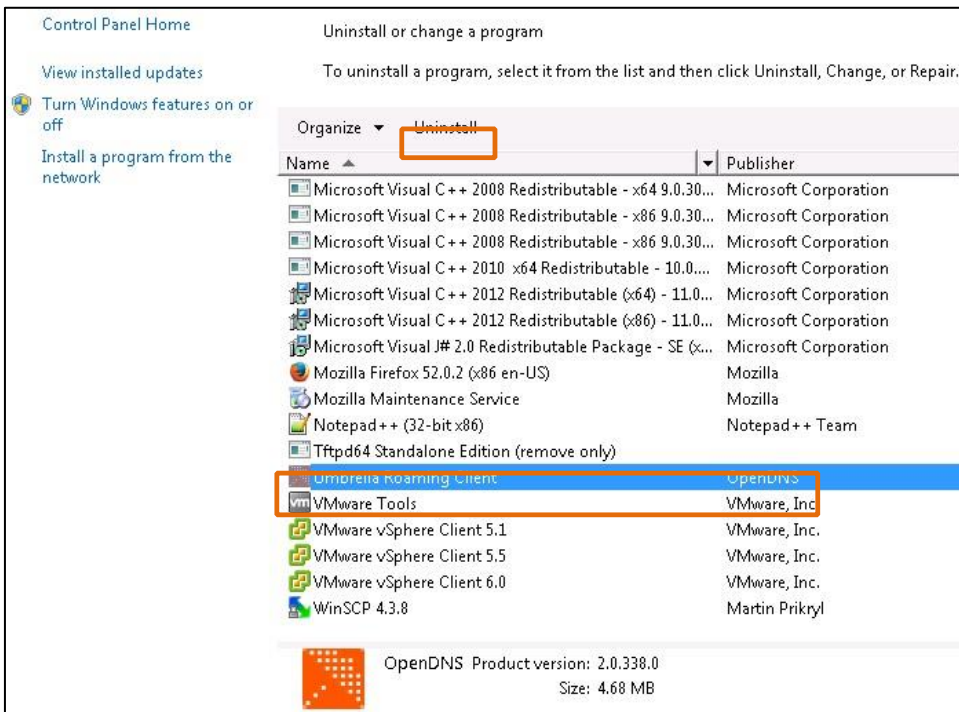
1. **경로 1:** Umbrella 로밍 Umbrella 를 아직 구축하지 않은 경우 여기서 시작하십시오. 계속 진행하기 전에 이 랩 가이드의 이전 실습에서 다음 단계를 완료합니다:
2. 시나리오 1, [실습 1:](#) Umbrella 액세스 (1-6 단계 만, 두 클라이언트 VMs 모두에 액세스 할 수 있는지 확인)
3. 시나리오 1, [실습 2:](#) Umbrella 로밍 클라이언트 구축(3-7 단계 만, 내부 도메인 추가).
4. 이제 [스텝 13](#) 으로 건너뛰고 계속합니다.
5. **경로 2:** 이미 Umbrella 로밍 클라이언트를 구축한 경우 여기서 시작합니다. Windows Jumper 클라이언트에서 Windows Control Panel 를 엽니다(Windows Start 메뉴에 링크가 있음).

6. Control Panel 에서 **Uninstall a program** 을 클릭합니다.



7. 설치된 프로그램 목록에서 **Umbrella Roaming Client** 를 찾은 다음 해당 라인을 클릭하여 강조 표시합니다.

8. 목록 위에서 **Uninstall** 를 클릭합니다.



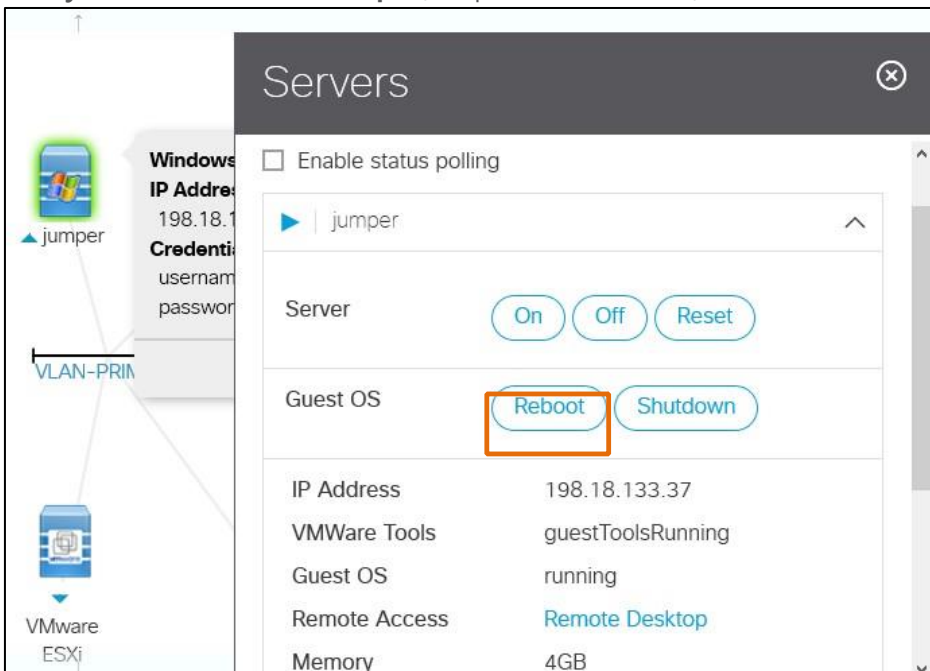
9. 확인 메시지에서 Yes 를 클릭하여 Umbrella Roaming Client 를 제거할지 확인합니다.

10. Reboot (재부팅) 확인 창에서 **OK** (확인)를 클릭합니다. 제거(uninstall) 프로세스가 완료됩니다.

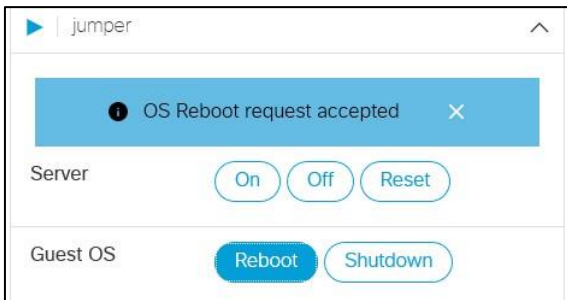
11. Windows 7 Jumper 클라이언트를 재부팅합니다. 이렇게 하려면 브라우저에서 lab topology (랩 토폴로지) 페이지로 다시 이동하여 **Servers** (서버) 탭을 클릭합니다.



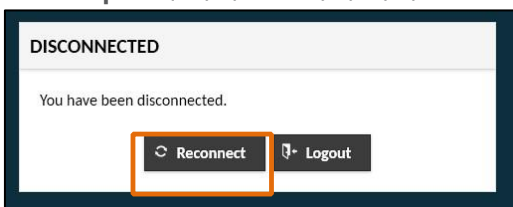
12. 목록의 오른쪽에서 **Jumper** 를 확장하고 Guest OS 라인에서 **Reboot** (재부팅)를 클릭합니다. 확인 창에서 **confirm that you want to reboot Jumper**(Jumper 재부팅을 확인)을 위해 **YES** 를 클릭합니다.



13. 재부팅 요청이 수락되었음을 알리는 메시지가 표시됩니다.

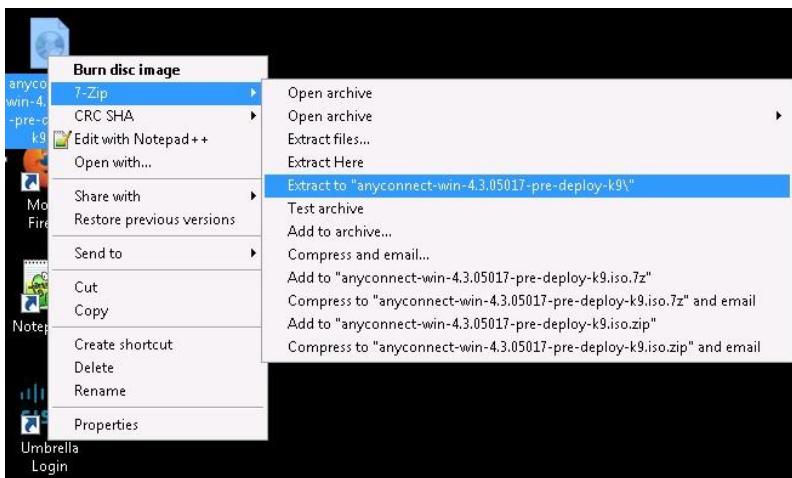


14. 브라우저의 Jumper 원격 데스크톱 세션 탭으로 돌아갑니다. 세션이 연결 해제 되었음을 알리는 메시지가 표시됩니다. 약 1-2 분 정도 기다렸다가 **Reconnect** (재연결)를 클릭합니다. 클라이언트가 재부팅을 완료 하면 **Jumper** 에 다시 연결하여 다시 로그인할 수 있게됩니다.



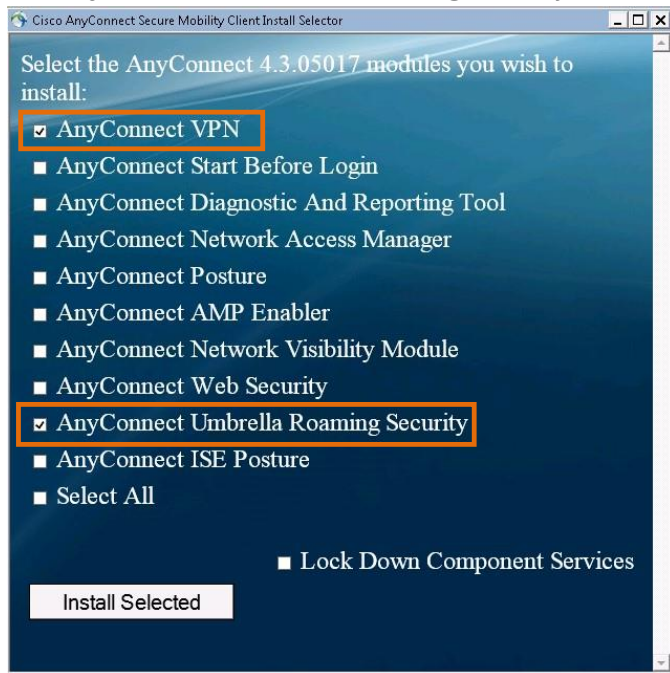
노트: Jumper 에 다시 연결한 후 제거 프로세스 후에 로밍 클라이언트의 아이콘이 더 이상 Windows 시스템 트레이에 표시되지 않습니다.

15. **경로 1 및 경로 2:** 여기서 계속합니다. Windows 7 Jumper 클라이언트에서 [anyconnect-win-4.x-pre-deployk9.iso](#) 파일을 데스크탑에서 찾아 마우스 오른쪽 버튼으로 클릭합니다.
16. 7-Zip 컨텍스트 메뉴에서 **ISO** 파일을 동일한 이름의 폴더로 추출하도록 선택합니다.



17. 데스크탑에서 만든 폴더를 찾아 엽니다.
18. 폴더 내에서 **Setup.exe** 를 찾아 실행하여 AnyConnect 설치를 시작합니다.

19. 설치 선택 창에서 먼저 Select All (모두 선택)을 클릭하여 모든 옵션을 선택 취소한 다음 **AnyConnect VPN** 및 **AnyConnect Umbrella Roaming Security** 옵션 (해당 두 옵션만)을 선택합니다.




20. **Install Selected**(선택한 설치)를 클릭한 다음 확인 팝업에서 다음 두 구성 요소를 선택한 후 **OK**(확인)를 클릭하여 계속 진행합니다.
21. 라이선스 계약 화면에서 **Accept** 를 클릭합니다.
22. 설치 완료 창에서 **OK** 를 클릭하여 설치를 종료합니다.
23. Windows Start 메뉴에서 **Cisco AnyConnect Secure Mobility Client** 를 찾아 실행합니다. 클라이언트의 상태를 기록합니다.

노트: 클라이언트가 Umbrella 에 연결하려면 관련 회사(org)의 세부 정보를 알아야 합니다. 이 작업은 대시보드에서 다운로드되는 프로파일을 통해 수행됩니다. 유효한 프로파일이 없으면 클라이언트가 Umbrella 에 연결할 수 없으며 오류 메시지가 표시됩니다.

24. Umbrella 클라이언트의 상태는 프로필이 누락되었음을 알려줍니다.



25. **Jumper** 클라이언트에서 Umbrella 대시보드에 액세스하여 **Deployments > Roaming Computers** 로 이동합니다.

26. 페이지 상단의  **Roaming Client** 아이콘을 클릭하여 옵션을 확장합니다. 페이지 하단으로 스크롤한 다음 **MODULE PROFILE** 를 클릭하여 AnyConnect (**OrgInfo.json**)의 프로파일을 다운로드합니다.



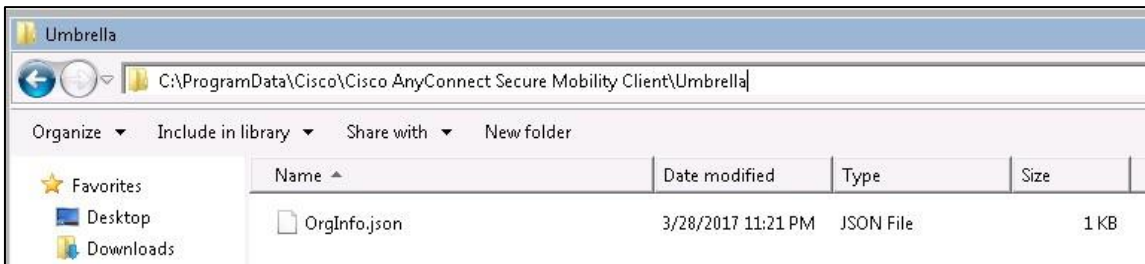
27. Windows Downloads 폴더에서 다운로드된 **OrgInfo.json** 파일을 찾습니다. 파일을 복사(Copy)합니다.

28. **Jumper** 클라이언트에서 Windows file explore 를 통해 다음 경로로 이동합니다:

"C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella"

노트: 대부분의 고객 환경에서 ProgramData 폴더는 일반적으로 숨겨져 있으므로, 탐색 창에 경로를 수동으로 입력하여 폴더를 탐색하면 됩니다.

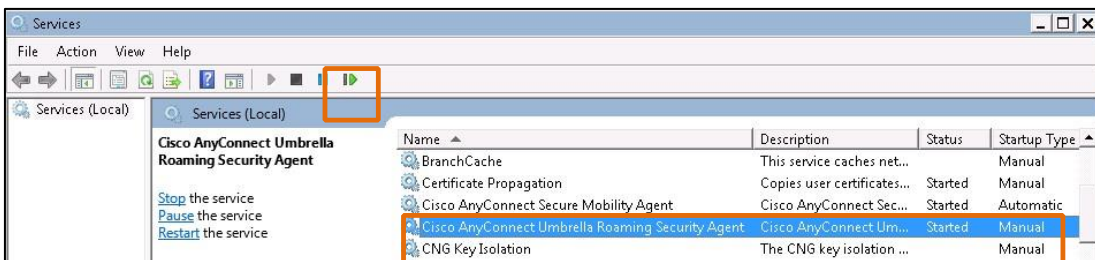
29. 이 위치에 프로파일 파일 (**OrgInfo.json**)을 붙여 넣습니다.



30. AnyConnect 에이전트 UI 로 돌아가서 몇 초 내에 현재 상태가 Umbrella 로 보호되고 있는지 확인합니다.



31. 상태가 변경되지 않으면 **Windows Services** 콘솔을 열고 **Cisco AnyConnect Umbrella Roaming Security Agent** 서비스를 찾은 다음 서비스를 재시작합니다.



32. Umbrella 대시보드로 돌아가거나 이미 로그인한 경우 페이지를 새로 고칩니다. 로밍 사용자가 AnyConnect 모듈 (Umbrella roaming security)임을 알 수 있습니다.

Name Jumper	Client Type AnyConnect RC Version v4.3.5017
SECURITY STATUS INFORMATION	
● Status: Protected 🚫 DNS Layer Encryption: No 🚫 IP Layer Enforcement: Disabled Last Active Policy: Default Policy	
ROAMING COMPUTER DETAILS	
OS Version: Windows 10 (Microsoft Windows [Version 10.0.14393]) Last Synced: 17 minutes ago	

노트: 이 버전의 AnyConnect 로밍 클라이언트는 IP 레이어 집행을 지원합니다. 그러나 이 랩 인프라의 네트워크 제약으로 인해 현재 이 기능을 구현할 수 없습니다. 앞으로 이를 본 랩에서 포함시킬 예정입니다!

- 33. 아직 이전 랩 실습 중 일부를 수행 하지 않은 경우에는 다음을 수행할 수 있습니다.
- 34. **실습 3:** Umbrella 로밍 클라이언트를 사용하여 AD 사용자 ID 를 활성화합니다. (AnyConnect 로밍 에이전트를 통해 AD 사용자 및 그룹 세부 정보를 가져오려는 경우 옴셔널 입니다). **시작하기 전에 먼저 랩 감독관에서 AnyConnect 로밍 클라이언트 버전에 AD 통합이 가능한지 확인합니다.**
- 35. **실습 4:** 기본 정책을 만듭니다 (정책을 만들고 최종 사용자에게 미치는 영향을 보려면 옴셔널 입니다).
- 36. **실습 5:** 검색 활동을 생성하고 기본 활동 보고서를 실행합니다(검색 활동을 생성하고 기본 리포트에서 해당 활동을 검색하려는 경우 선택 사항 입니다).

실습 7: 가상 어플라이언스 구축 (옴셔널)

Umbrella 의 **VA(Virtual Appliance)**는 전체 네트워크 위치(ID)를 신속하게 구축하는 유용한 방법입니다. VA 는 VMware ESXi 또는 Hyper-V 에서 실행될 수 있으며 일반적으로 이중화를 제공하기 위해 페어로 구축됩니다. VA 는 다음과 같은 다양한 시나리오에 대한 솔루션을 제공합니다:

- AD connector 와 함께 사용하는 경우 AD 사용자 및 그룹 정보와 함께 Umbrella 를 제공합니다.
- 추가 세분성을 위해 로컬 IP 주소를 사용하여 Umbrella 를 제공합니다.
- 공용 IP 주소가 DHCP 인 경우 Umbrella 에 대한 연결을 제공합니다.
- VA (가상 어플라이언스)는 다음 기능을 수행합니다:
 - 가상화된 서버 환경에서 실행되며 내부 도메인에 대한 로컬 DNS 쿼리를 기존 DNS 서버에 전달하고 인터넷 도메인에 대한 기타 모든 DNS 쿼리를 Umbrella 로 전달합니다.
 - 외부 DNS 요청하는 디바이스의 로컬 IP 주소를 캡처하여 Umbrella 로 전송된 쿼리에 포함합니다.

- Active Directory 통합을 사용하도록 설정한 경우 가상 어플라이언스는 AD 사용자 또는 컴퓨터를 식별하는 데 필요한 모든 메타데이터를 포함하는 외부 DNS 쿼리를 Umbrella 에 암호화합니다.

이 실습에서는 POD 에서 실행되고 Windows 7 Jumper 클라이언트에서 실행되는 VMware vSphere 클라이언트를 통해 액세스하는 **VMware ESXi** 인스턴스에 가상 어플라이언스 페어를 구축합니다.


노트: 이 연습은 선택적 연습이며 1-6 연습과 무관하게 완료될 수 있습니다. VA 버전 2.4.1(2019년 2월 릴리스)은 초기 구성을 수행하는 방법을 변경합니다. 따라서 이전에 VA 를 구축한 경우에도 이 연습을 수행하는 것이 도움이 될 수 있습니다.

중요 VA 에서 다운타임 없이 자동 업데이트를 업데이트하려면 최소 2 개의 VA 를 설치해야 합니다. 그렇지 않으면, 대시보드를 통해 VA 를 업그레이드 수 있는 유일한 방법이 수동으로 진행하는 것입니다. 그러면 최대 15 분의 다운타임을 발생하고 사용자가 네트워크에서 DNS 쿼리를 수행할 수 없으며 인터넷에 액세스할 수 없게 될 수 있습니다.

중요: 가상 어플라이언스가 로컬 DNS 쿼리 및 외부 DNS 쿼리를 올바르게 라우팅하려면 Umbrella 에서 관리하는 모든 디바이스에 DNS 서버가 가상 어플라이언스의 주소로 설정되어 있어야 합니다.

가상 어플라이언스 (Virtual Appliance) 구축하기

1. Windows 7 **Jumper** 클라이언트에서 데스크탑 바로 가기를 사용하여 Umbrella 대시보드에 액세스합니다.

Deployments > Sites and Active Directory 로 이동합니다. 오른쪽 상단의  **Download Components** 버튼을 클릭하여 영역을 확장합니다.

2. **VA for VMWare ESXi 4.1 Update 2 or newer** 영역에서 **DOWNLOAD** 클릭합니다. .ova 파일의 사이즈는 ~ 250MB 이므로 현재 랩 네트워크 활동에 따라 다운로드를 완료하는 데 몇 분이 걸릴 수 있습니다.

Virtual Appliance

The Virtual Appliance is a DNS Forwarder that identifies Active Directory users and internal networks. The VA will forward external DNS to Cisco Umbrella and internal domains to the domain controller. High availability environments typically run two Virtual Appliances.

Note: Local domains are set and managed on the [Internal Domains](#) page. You must, however, enter your local DNS server addresses in the VA configuration for internal domains to resolve correctly. See our support article on [setting up a VA](#) for more information.

Note: Use Umbrella<YourOrgID> as the password for the VA. Your Org ID can be retrieved from the URL on this page. For example, if your Org ID is 2406960, the password for the VA will be Umbrella2406960

VA for VMWare ESXi 4.1 Update 2 or newer	DOWNLOAD	GETTING STARTED
VA for Hyper-V for Windows Server 2008 R2, 2012, and 2012 R2	DOWNLOAD	GETTING STARTED

3. Jumper 클라이언트의 데스크톱 아이콘에서 **VMware vSphere Client** 에 액세스합니다.



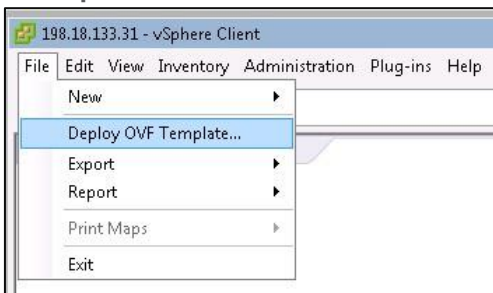
4. 다음 세부 정보 (랩 토폴로지에서도 찾을 수 있음)를 사용하여 VMWare ESXi 호스트에 연결합니다:

- IP address: 198.18.133.31
- Username: root
- Password: C1sco12345

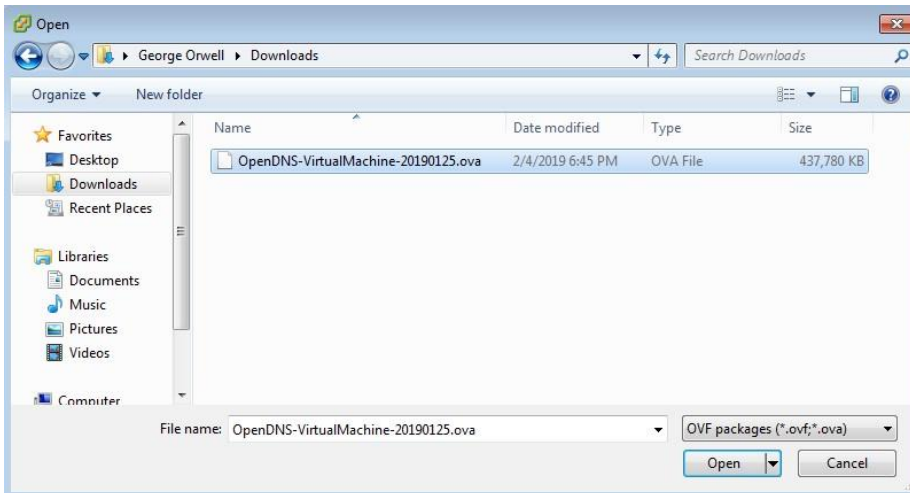


5. **Login** 을 클릭합니다.

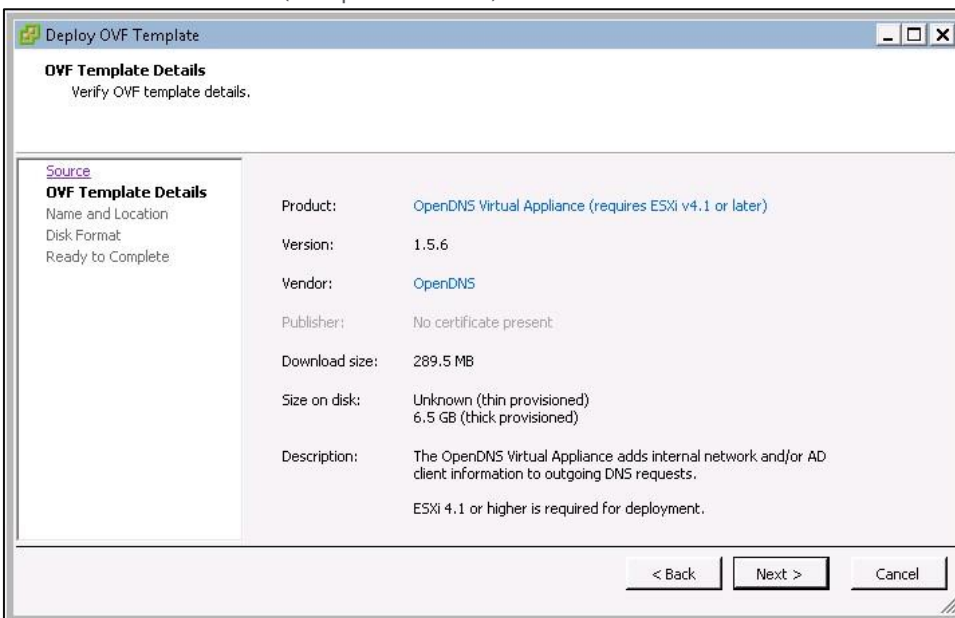
6. **vSphere Client** 콘솔이 시작됩니다. **File** 메뉴를 클릭한 다음 **Deploy OVF Template...**를 선택합니다.



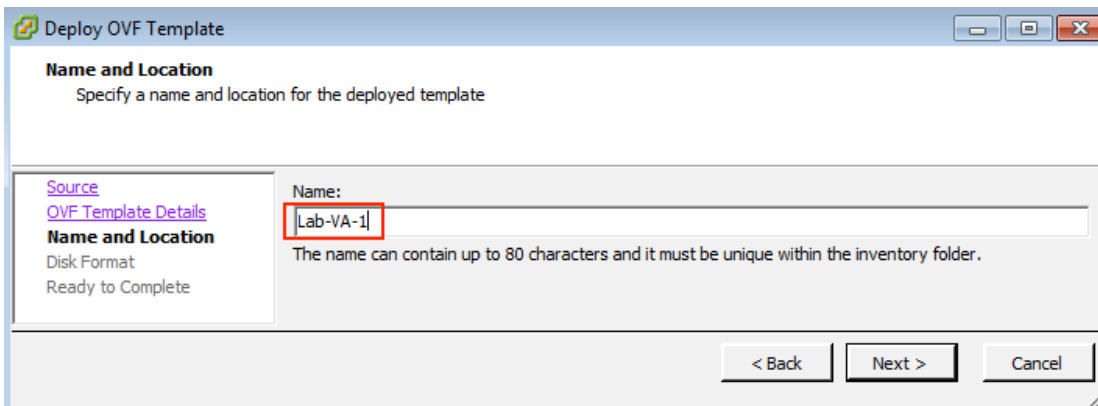
7. **Browse** 를 클릭하고 다운로드된 OVA 템플리트 (기본적으로 다운로드 폴더)로 이동합니다. **Open** 을 클릭합니다.



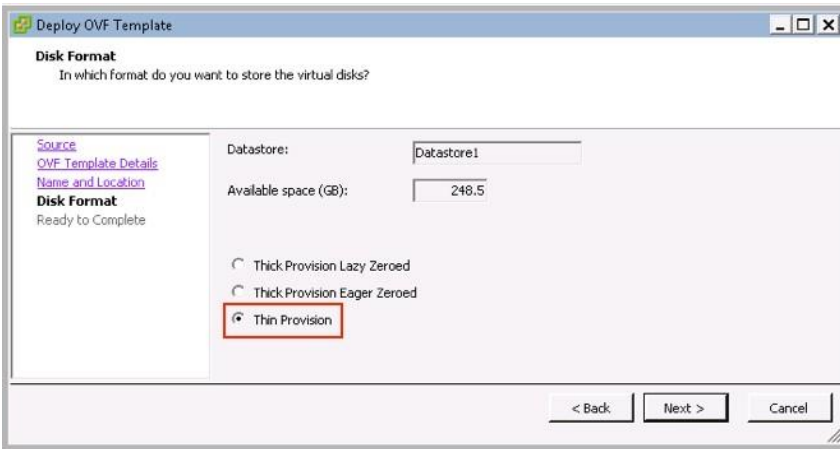
8. 템플릿 세부 사항(Template Details) 창에서 **Next** 를 클릭합니다.



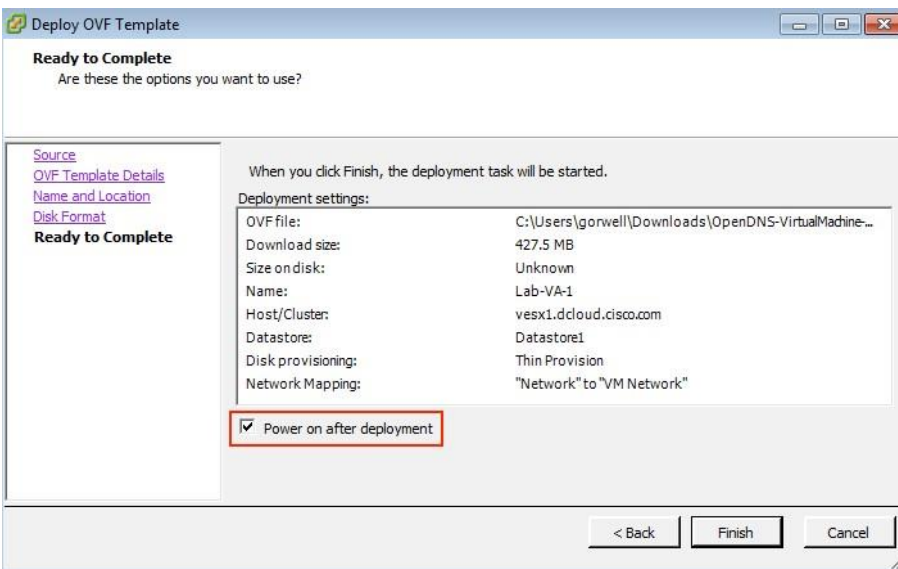
9. Name(이름) 및 위치(Location) 창에서 보다 의미 있는 이름을 제공하고 이름에 "1"을 포함합니다. (예: "Lab-VA-1").
Next 를 클릭합니다.



10. 디스크 포맷(Disk Format) 창에서 프로비저닝을 **Thin Provision** 으로 변경합니다. **Next** 를 클릭합니다.

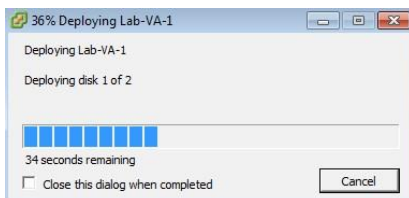


11. 최종 요약(summary) 창에서 **Power on after deployment** 확인란을 선택하고 **Finish** 를 클릭합니다.



노트: 실제 구축에서는 네트워크를 선택하거나 매핑하는 추가 단계가 있습니다. 랩 환경에는 단일 네트워크 만 있으므로 해당 단계는 나타나지 않습니다.

12. 시스템 프롬프트에 구축 상태가 업데이트되고 완료되면 최종 확인 메시지가 표시됩니다. **Close** 를 클릭합니다.



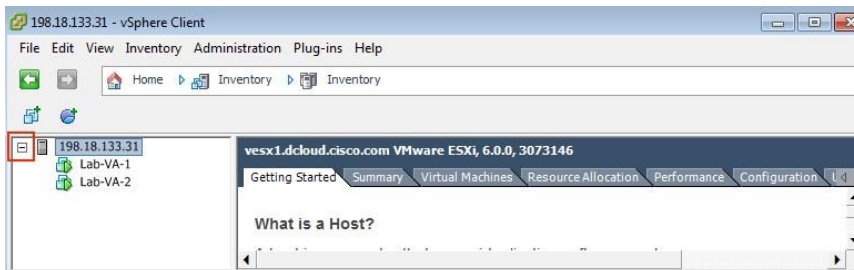
13. 이전 단계를 반복하여 두 번째 VA 인스턴스를 구축합니다(첫 번째 VA 인스턴스를 복제하지 마십시오!). 유사한 이름 "2"가 포함되는 이름을 제공합니다(예: "**Lab-VA-2**").

VA (Virtual Appliances) 구성하기

노트: 다음 단계에서는 단일 VA 에 대한 프로세스를 보여줍니다. 아래 구성 표에 나열된 이름과 IP 주소를 제외하고 두 VA 에 대한 프로세스는 동일합니다.

	VA-1	VA-2
이름	Lab-VA-1	Lab-VA-2
IP 주소	198.18.133.101	198.18.133.102
Netmask	255.255.192.0	255.255.192.0
Gateway	198.18.128.1	198.18.128.1
Local DNS	198.18.133.1	198.18.133.1

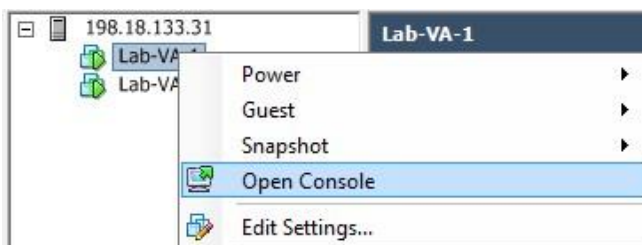
1. 다음으로 콘솔을 사용하여 VA 를 구성합니다. vSphere Client 에서 **198.18.133.31** 의 왼쪽 메뉴를 확장하여 VA 가 표시되는지 확인합니다.



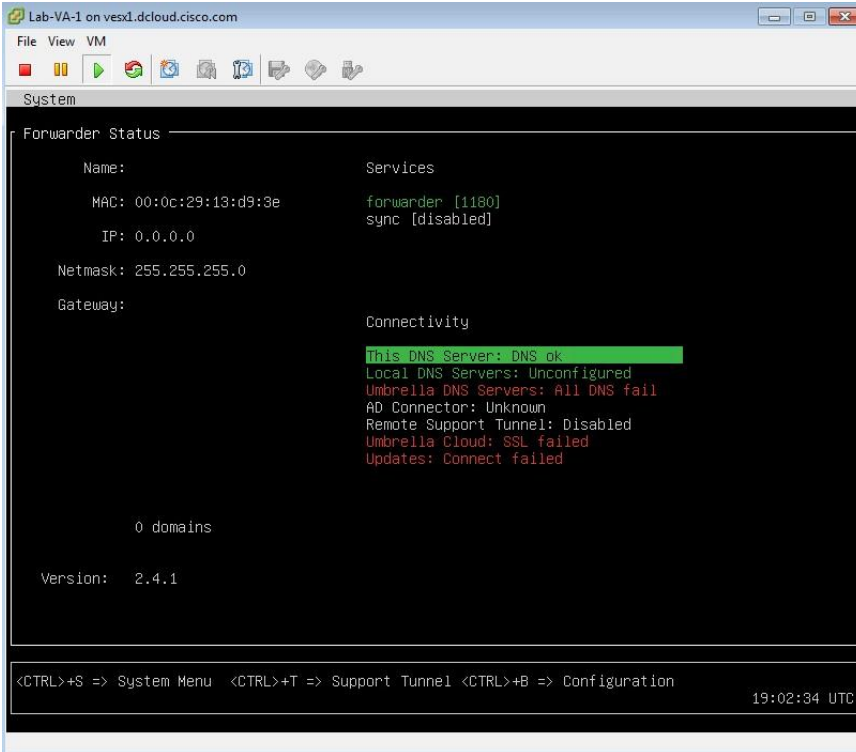
노트: VA 는 이미 켜져 있어야 합니다(각 VA 이름 왼쪽에 녹색 재생 아이콘으로 표시됨). 그렇지 않은 경우, 각 VA 를 마우스 오른쪽 버튼으로 클릭하고 Power > Power on 를 선택합니다.

노트: VA 콘솔에서 커서를 놓으려면 [Ctrl] + [Alt]를 누릅니다.

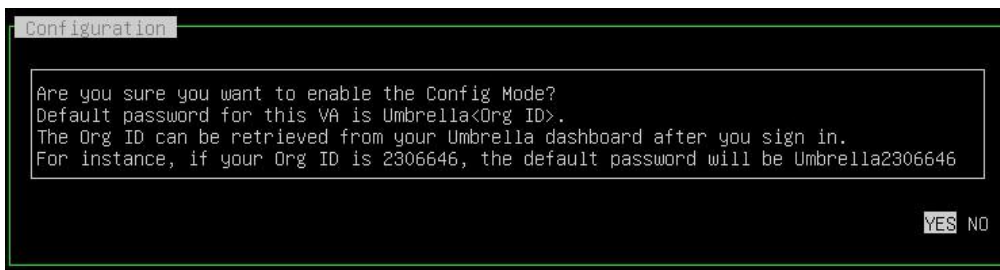
2. 첫 번째 VA 를 마우스 오른쪽 버튼으로 클릭하고 **Open Console** 를 선택하면 VA 를 구성할 수 있는 새 창이 열립니다.



3. 간단한 부팅 프로세스 후 구성 및 연결 테스트를 볼 수 있는 Forwarder Status 화면이 표시됩니다. 부팅 시 VA 가 DHCP 를 사용하여 IP 주소를 검색하려고 시도합니다. 이 랩에서 DHCP 를 실행하고 있지 않으므로 VA 를 수동으로 구성하지 않으면 대부분의 테스트가 실패합니다.



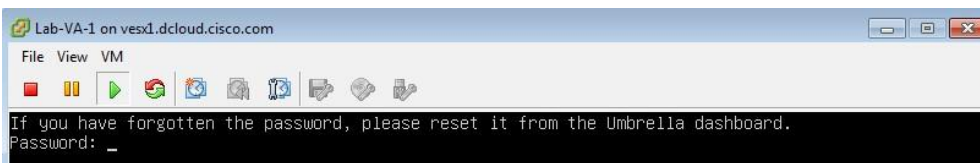
4. [CTRL]+B 를 눌러 구성 모드로 들어갑니다. 디폴트 패스워드에 대한 메시지를 읽고 YES 를 선택합니다.



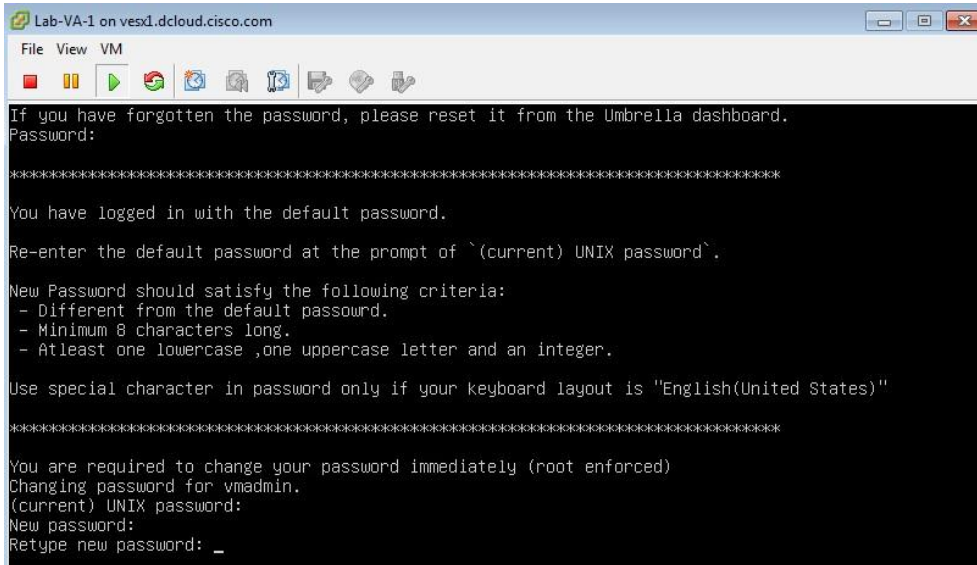
5. 포드에 대한 Org ID 를 가져오려면 데스크탑 바로 가기를 사용하여 Umbrella 대시보드에 액세스합니다. Org ID 는 7 자리 숫자이며 브라우저의 어드레스 바에서 찾을 수 있습니다.



6. VA (Umbrella<Org ID>)에 대한 디폴트 패스워드를 사용하여 구성 모드에 로그인 합니다..



7. VA 가 디폴트 패스워드를 사용하고 있으므로 암호를 변경하라는 메시지가 표시됩니다. 디폴트 패스워드 (Umbrella<Org ID>)를 입력한 다음 새패스워드에 대해 **C1sc0123** 을 입력합니다.



```
Lab-VA-1 on vesx1.dcloud.cisco.com
File View VM
If you have forgotten the password, please reset it from the Umbrella dashboard.
Password:
*****

You have logged in with the default password.

Re-enter the default password at the prompt of `(current) UNIX password`.

New Password should satisfy the following criteria:
- Different from the default password.
- Minimum 8 characters long.
- Atleast one lowercase ,one uppercase letter and an integer.

Use special character in password only if your keyboard layout is "English(United States)"
*****

You are required to change your password immediately (root enforced)
Changing password for vmadmin.
(current) UNIX password:
New password:
Retype new password: _
```

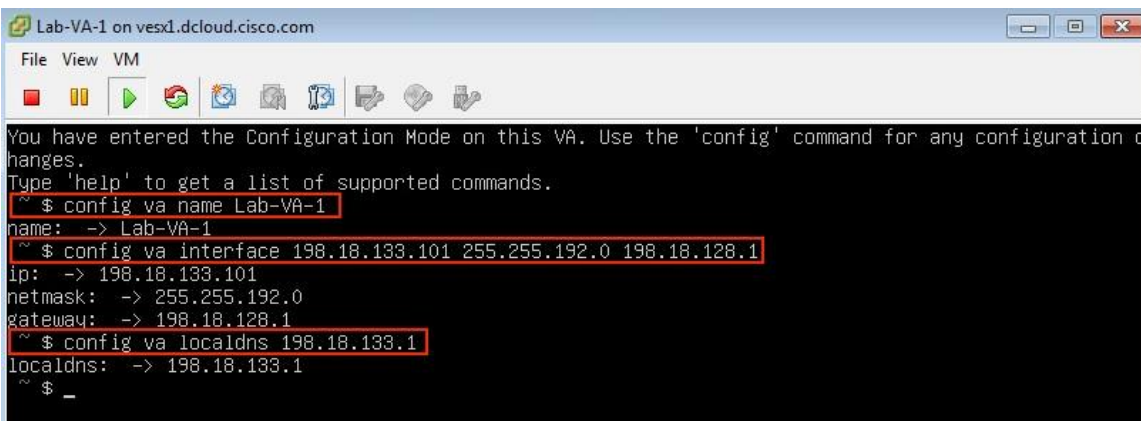
8. 이제 새 패스워드를 사용하여 로그인할 수 있습니다. **C1sc0123** 을 입력하고 **return** 을 누릅니다.



```
Lab-VA-1 on vesx1.dcloud.cisco.com
File View VM
If you have forgotten the password, please reset it from the Umbrella dashboard.
Password: _
```

9. 구성 프롬프트에서 **help** 을 입력하여 지원되는 명령 목록을 볼 수 있습니다. VA 를 구성하려면, 다음 세 가지 명령어를 사용하여 이 섹션의 시작 부분에 있는 구성 테이블에서 적절한 정보를 참조하여 사용합니다.

```
~$ config va name va-name
~$ config va interface ipaddress netmask gateway
~$ config va localdns dnsaddress
```



```
Lab-VA-1 on vesx1.dcloud.cisco.com
File View VM
You have entered the Configuration Mode on this VA. Use the 'config' command for any configuration c
hanges.
Type 'help' to get a list of supported commands.
~ $ config va name Lab-VA-1
name: -> Lab-VA-1
~ $ config va interface 198.18.133.101 255.255.192.0 198.18.128.1
ip: -> 198.18.133.101
netmask: -> 255.255.192.0
gateway: -> 198.18.128.1
~ $ config va localdns 198.18.133.1
localdns: -> 198.18.133.1
~ $ _
```

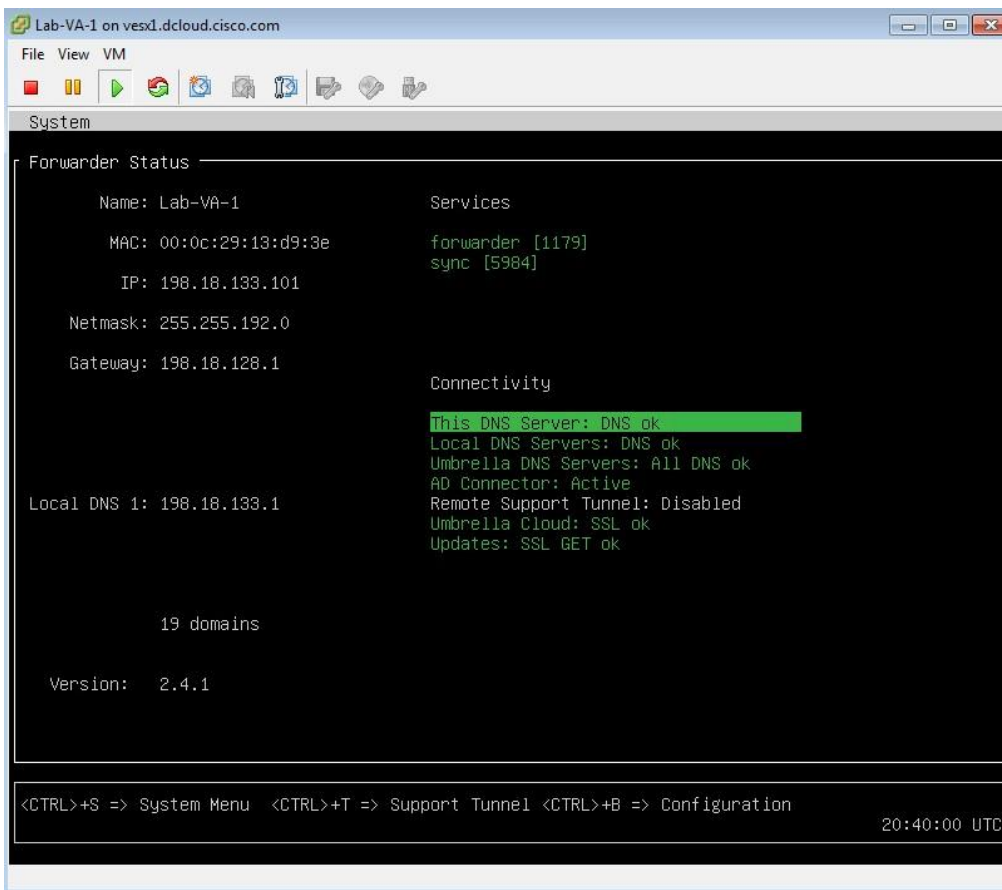
10. VA 구성을 완료되면 **exit** 를 입력하여 Forwarder Status 화면으로 돌아갑니다.

노트: VA 에 지정한 이름이 매니지드 VA 옆에 있는 Umbrella 대시보드에 나타납니다. 혼동을 피하려면 vSphere 에서 VM 이름과 동일한 이름(예: Lab-VA-1)을 사용하는 것이 좋습니다.

노트: 로컬 DNS 구성은 로컬 DNS 서버로 채워야 합니다. 일반적으로 Active Directory Domain Services 및 DNS Server 역할이 모두 설치된 윈도우즈 서버의 IP 주소입니다. 이 랩에서 DNS 는 198.18.133.1 ~ Domain Controller 입니다.

노트: 모든 VA 는 GMT +0(UTC)을 사용합니다. 표준 시간대를 구성할 필요가 없습니다.

11. VA 는 연결성 테스트를 계속 실행합니다. 일반적으로 VA 가 Umbrella 클라우드에 등록해야 하므로 모든 테스트가 성공적으로 완료되는 데 몇 분 정도 걸립니다(특히 VA 가 등록 완전히 완료되지 않으면 업데이트 테스트가 실패할 수 있음).



```
Lab-VA-1 on vesx1.dcloud.cisco.com
File View VM
System
Forwarder Status
Name: Lab-VA-1
MAC: 00:0c:29:13:d9:3e
IP: 198.18.133.101
Netmask: 255.255.192.0
Gateway: 198.18.128.1
Services
forwarder [1179]
sync [5984]
Connectivity
This DNS Server: DNS ok
Local DNS Servers: DNS ok
Umbrella DNS Servers: All DNS ok
AD Connector: Active
Remote Support Tunnel: Disabled
Umbrella Cloud: SSL ok
Updates: SSL GET ok
Local DNS 1: 198.18.133.1
19 domains
Version: 2.4.1
<CTRL>+S => System Menu <CTRL>+T => Support Tunnel <CTRL>+B => Configuration
20:40:00 UTC
```

노트: 실습 3 을 완료하지 않은 경우, AD 커넥터 상태가 'Unknown'으로 표시됩니다.

노트: Remote Support Tunnel 은 Umbrella 지원 작업할 때만 필요합니다. 자세한 내용은 다음 사이트를 참조하시기 바랍니다: <https://support.umbrella.com/hc/en-us/articles/115004154423>.

노트: 오류 메시지가 표시되거나 각 테스트에 대해 자세히 알고 싶은 경우 테스트에 탭하고 [Return]을 눌러 이 정보를 볼 수 있습니다. 실제 환경에서 테스트를 완료할 수 없는 경우, ESXi 네트워크 구성을 확인하여 필요에 따라 완료되었는지, 방화벽 포트도 확인하여 필요한 대상에 액세스할 수 있는지 확인합니다. 테스트는 백그라운드에서 계속 실행되므로 문제가 해결된 후 개입 없이 나중에 성공할 수 있습니다.

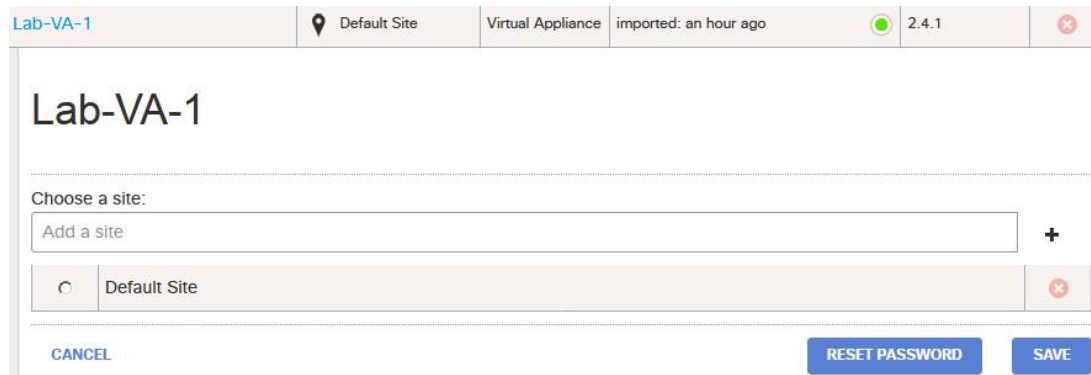
이전 단계를 반복하여 두 번째 VA 를 구성합니다.

대시보드 확인하기(Dashboard Verification)

1. 테스트가 오류 없이 완료되면 다음 단계는 Umbrella 대시보드에서 VAs 동기화를 확인하는 것입니다. **Deployments > Sites & Active Directory** 로 이동하여 이전에 VA 콘솔 구성에 지정한 이름과 함께 VA 가 나열되어 있는지 확인합니다.
2. VA 이름을 클릭하여 VA 중 하나를 확장합니다.

노트: DNSCrypt 가 비활성화되지 않았다는 경고가 표시되는 것은 정상 입니다. [여기서](#) DNSCrypt 에 대해 읽을 수 있고 또는 대시보드의 링크를 통해서도 읽을 수 있습니다.

3. 사이트는 각 VA 와 연결되어야 합니다. 이는 간단한 구성이므로 VA 가 **Default Site** 에 할당되었습니다. 대규모 다중 사이트 구축에서는 VA 를 적절한 사이트에 추가해야 합니다.



노트: 사이트는 LAN(Local Area Network)과 같은 고속 네트워크에 의해 연결된 장치 세트를 나타냅니다.

일반적으로 동일한 물리적 사이트에 있는 모든 장치는 동일한 건물 또는 아마도 동일한 캠퍼스 네트워크에 위치합니다. Umbrella 의 관점에서 보면 사이트는 서로 통신하는 구성 요소(VA, 커넥터 및 DC) 집합을 의미합니다.

내부 네트워크 정의하기

이제 온-네트워크 사용자에게 대한 VA 를 구축하고 구성했으므로 내부 네트워크 ID 를 구성할 수 있습니다.

노트: 내부 네트워크 ID의 목적은 정책을 적용할 수 있는 ID로 공개적으로 라우팅할 수 없는 (또는 RFC1918 규정) 서브넷을 정의하는 것입니다.

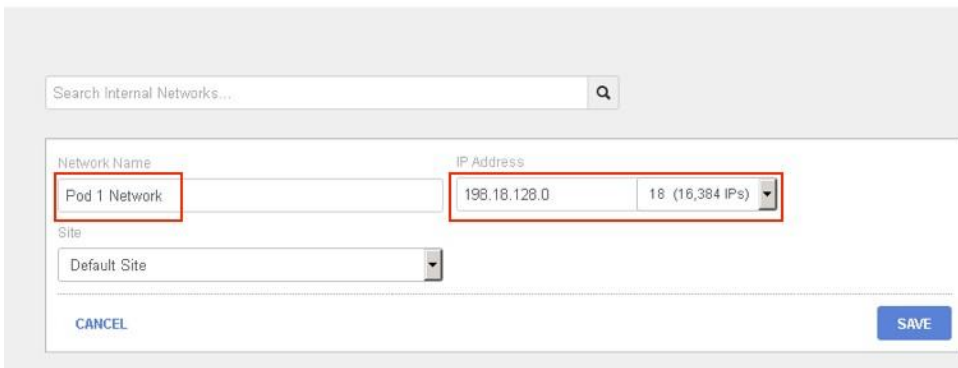
1. 내부 네트워크 ID를 생성하려면 Umbrella 대시보드에서 **Deployments**를 확장하고 **Internal Networks**를 선택한



다음 페이지 상단에 있는 **Add** 버튼을 클릭하여 정의(definition) 영역을 확장합니다.

2. 네트워크 이름과 유효한 서브넷을 지정합니다.(이 랩에는 **255.255.192.0**의 넷마스크를 기반으로 하는 /18 서브넷이 있으므로 IP의 마지막 옥텟은 .0입니다). **198.18.128.0**을 입력하고 드롭다운에서 **18(16,384 IPs)**을 선택하여 전체 VLAN을 포함합니다. Default Site만 있으므로 이 선택 항목을 변경할 수 없습니다 (VA도 Default Site와 연결되므로 이 네트워크에 대한 정책을 만들 수 있습니다).

Internal Networks



3. **SAVE**를 클릭합니다.

가상 어플라이언스를 사용하도록 장치 구성하기

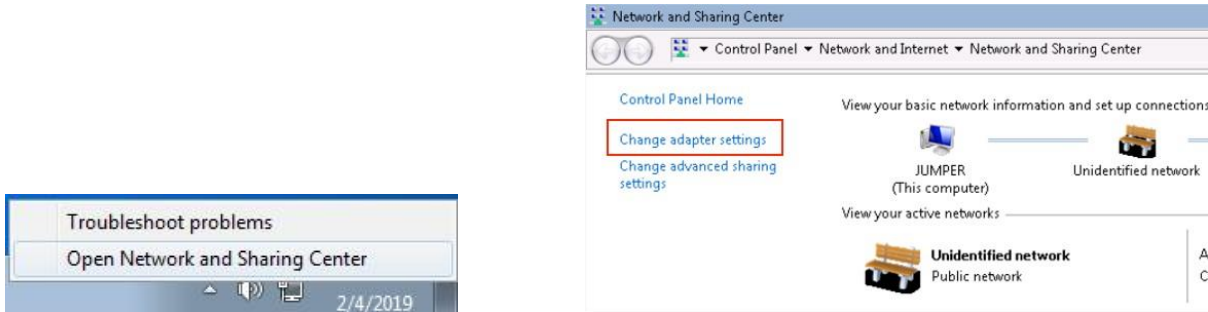
다음으로, DNS 쿼리가 이전에 정의한 내부 네트워크 ID와 연결될 수 있도록 VA를 통해 Windows Jumper 클라이언트에서 DNS를 시작합니다.

노트: VA를 통해 DNS 쿼리를 전달하는 클라이언트에 로밍 클라이언트를 구축한 경우, 로밍 컴퓨터 ID는 VA에 의해 EDNS 쿼리에 포함된 ID에 의해 재정의됩니다. 포괄적인 보호 네트워크에서 로밍 클라이언트를 분리 하도록 구성하여 VA 없는 네트워크에 대해서도 유사한 동작을 수행할 수 있습니다. 이는 **Deployments > Core Identities > Roaming Computers**를 통해 대시보드에서 구성한 다음 페이지의 오른쪽 상단에 있는 **Settings**(설정) 버튼을 클릭합니다. Settings 창에서 Umbrella Protected Network에 있을 때 DNS 리디렉션을 비활성화하는 확인란을 선택합니다. 이 변경이 완료되면 DNS 요청은 여러 ID(AD 사용자, 외부 네트워크 및 내부 네트워크)와 연결됩니다.

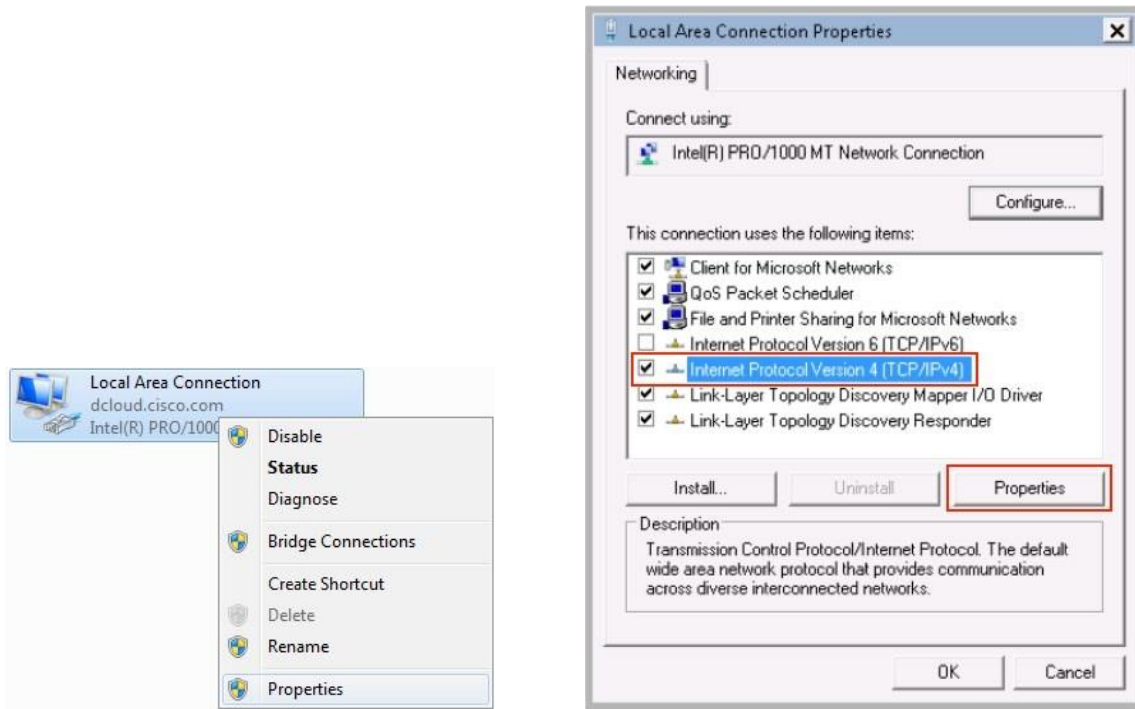
노트: 대부분의 고객 사례에서 DNS 설정은 DHCP를 통해 디바이스에 제공됩니다. 이 랩에서는 IP 주소가 클라이언트에 대해 수동으로 정의되고 AD 시스템의 DNS 서버를 가리키도록 하기 때문에 구렁지 않습니다. 실제 시나리오에서는 다음

단계가 고객의 DHCP 서버 설정을 업데이트하여 디바이스가 해당 DNS 를 가상 어플라이언스를 가리키도록 지시하는 것입니다. 도리어 이 랩에서는 DNS 의 VA 를 가리키도록 Windows 7 Jumper 클라이언트를 수동으로 구성합니다.

1. Windows 7 Jumper 클라이언트의 Windows 시스템 트레이에서 네트워크 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **Open Network and Sharing Center** 를 선택합니다. 왼쪽 목록에서 **Change adapter settings** 를 선택합니다.

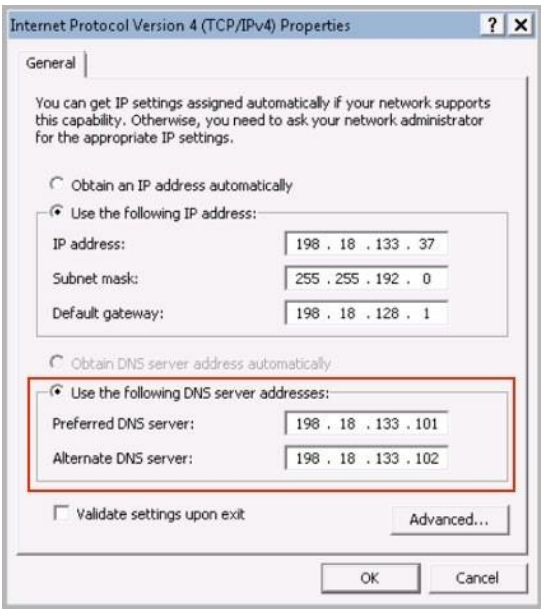


2. 네트워크 연결(Network Connections) 창에서 로컬 영역 연결(Local Area Connection) 아이콘을 마우스 오른쪽 버튼으로 클릭하고 속성(Properties)을 선택합니다. 네트워킹 속성(Networking Properties) 박스가 열립니다. 인터넷 프로토콜 버전 4 (Internet Protocol Version 4) 라인을 강조 표시하고 Properties 를 클릭합니다.



3. IP Properties (IP 속성) 창에서 DNS 서버 주소의 구성을 2 개의 VA IP 주소를 가리키도록 다음과 같이 변경합니다:

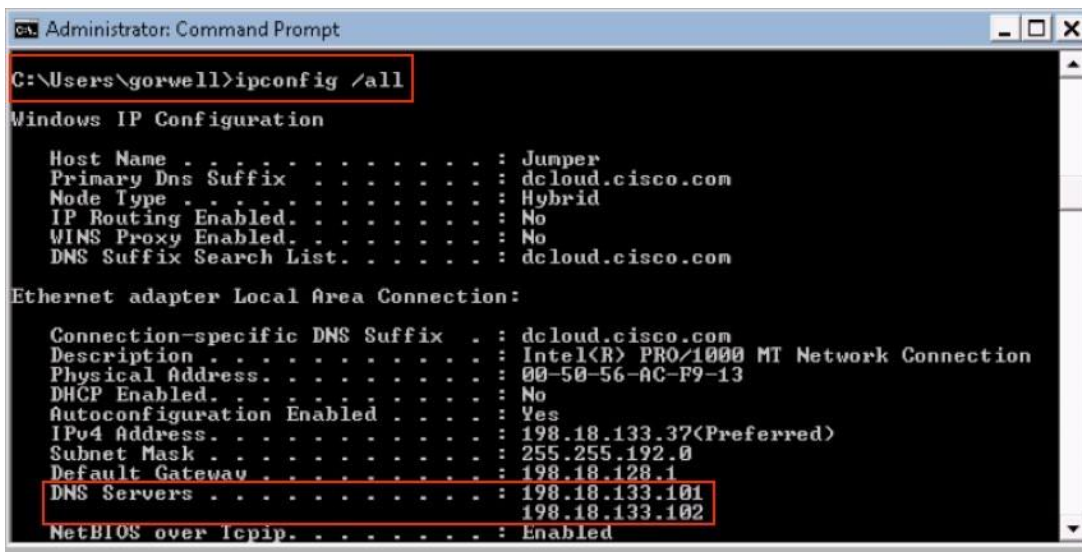
- Lab-VA-1: 198.18.133.101
- Lab-VA-2: 198.18.133.102



4. **OK**, 다시 **OK** 를 차례로 클릭한 다음 **save** 를 클릭합니다.
5. 명령 프롬프트 (Start Menu 검색 박스에서 cmd)를 열고 다음과 같은 명령어를 실행합니다:

```
C:\Users\gorwell> ipconfig /all
```

6. DNS 주소가 두 VA 인지 확인합니다. cmd 창을 열어 둡니다.



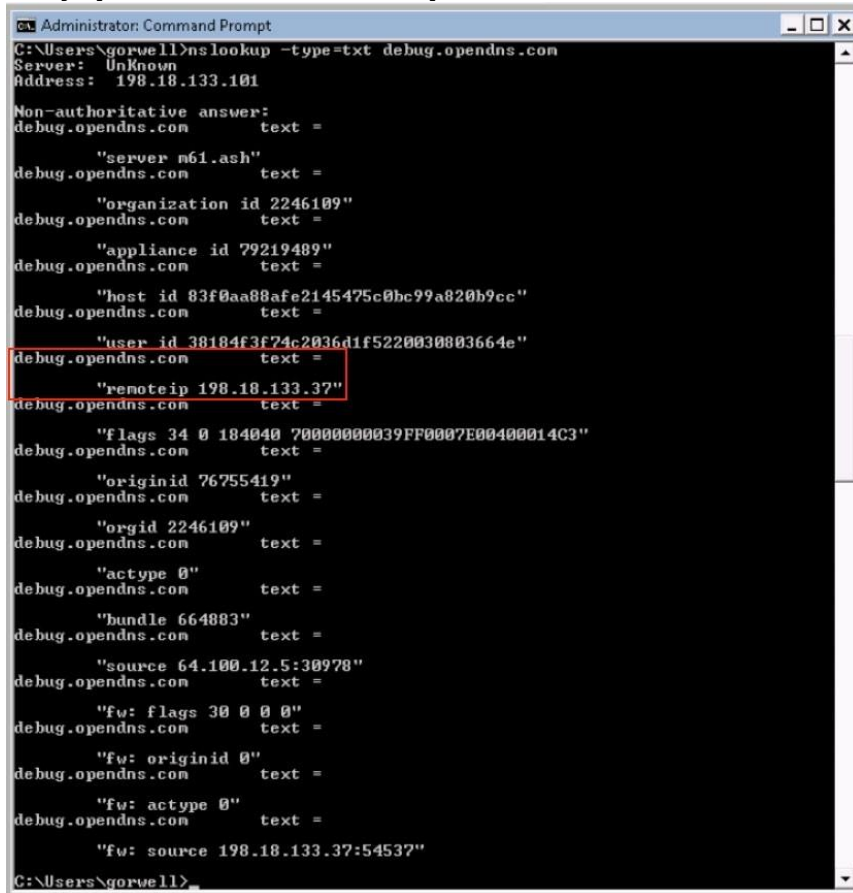
노트: 로밍 클라이언트가 네트워크 변경을 탐지하면 nslookup (nslookup type = txt debug.opendns.com)을 수행하여 VA 뒤에 있는지 확인하고, 로밍 클라이언트가 이를 탐지하면 VA가 DNS 요청을 Umbrella로 처리할 수 있게 됩니다. 구성된 경우, 로밍 클라이언트에서 IP 계층 보호를 계속 적용합니다.

7. 다음으로, 디버그 쿼리를 사용하여 확인합니다. cmd 창에서 다음 nslookup 쿼리를 실행합니다:

```
C:\Users\Wgorwell> nslookup -type=txt debug.opendns.com
```

8. 결과에서 아래 라인은 클라이언트의 로컬 개인 IP 주소와 일치해야 합니다:

```
debug.opendns.com text = "remoteip 198.18.133.x"
```



```
Administrator: Command Prompt
C:\Users\Wgorwell> nslookup -type=txt debug.opendns.com
Server: UnKnown
Address: 198.18.133.101

Non-authoritative answer:
debug.opendns.com text =
    "server m61.ash"
debug.opendns.com text =
    "organization id 2246109"
debug.opendns.com text =
    "appliance id 79219489"
debug.opendns.com text =
    "host id 83f0aa88afe2145475c0bc99a820b9cc"
debug.opendns.com text =
    "user id 38184f3f74c2036d1f5220030803664e"
debug.opendns.com text =
    "remoteip 198.18.133.37"
debug.opendns.com text =
    "flags 34 0 184040 70000000039FF0007E00400014C3"
debug.opendns.com text =
    "originid 76755419"
debug.opendns.com text =
    "orgid 2246109"
debug.opendns.com text =
    "actype 0"
debug.opendns.com text =
    "bundle 664883"
debug.opendns.com text =
    "source 64.100.12.5:30978"
debug.opendns.com text =
    "fw: flags 30 0 0 0"
debug.opendns.com text =
    "fw: originid 0"
debug.opendns.com text =
    "fw: actype 0"
debug.opendns.com text =
    "fw: source 198.18.133.37:54537"

C:\Users\Wgorwell>
```

자세한 정보:

Server m61.ash (쿼리에 응답한 Umbrella 리졸버)
organization id 2246109 (*VA 만 해당 - VA 가 속하는 조직)
appliance id 79219489 (*VA 만 해당 - VA ID 번호)
host id 83f0aa88afe2145475c0bc99a820b9cc (*VA 만 해당 - AD User hash)
user id 38184f3f74c2036d1f5220030803664e (*VA 만 해당 - AD Computer hash)
remoteip 198.18.166.37 (*VA 만 해당 - DNS 요청의 내부 IP 주소입니다. 이는 로컬 DNS 서버 중 하나가 아니어야 합니다.)
flags 34 0 184040 70000000039FF0007E00400014C3
originid 76755419 (적용된 비 AD ID 의 출처 ID 는 로밍 클라이언트 또는 네트워크일 수 있습니다. 0 인 경우 이 네트워크가 Umbrella 계정에 등록되지 않습니다.)
orgid 2246109 (위의 오리지널 ID 가 속하는 조직 ID 입니다 (있는 경우). Org ID 는 ID 에 대한 대시보드 URL 의 Org ID 와 일치해야 합니다.)
actype 0 (계정 유형, 내부 용)

```
bundle 664883 (적용된 정책에 속하는 번들 ID (Umbrella 대시보드만 해당))
source 64.100.12.5:30978 (Umbrella 에 의해 확인된 네트워크의 이그레스 포인트의 공용 IP 입니다. 이는 사용되는 DNS 서버의
DNS egress IP 이며 디바이스의 IP 와 다를 수 있습니다. 이는 Umbrella 의 리졸버가 사용자 egress 를 볼 수 있는 IP 주소를
확인하기 위해 사용합니다.)
```

정책(Policy) 생성 및 브라우징 트래픽(Browsing Traffic) 생성하기

VA 에 적용할 새 정책을 생성하고 보고를 위한 트래픽을 생성 해보겠습니다.

1. 실습 4 를 완료하시고 기본 사이트에 정책을 적용합니다. 또한 이미 다른 정책을 생성한 경우 목록의 맨 위에 새 정책을 추가해야 합니다.
2. 실습 5 를 완료합니다. 보고서에 요청하는 클라이언트의 개인 IP 주소가 포함되는 방식을 참고하십시오. AD Connector (AD 커넥터) 실습을 완료한 경우 사용자 이름(username)도 표시됩니다. 여러 정책을 가지고 있는 경우, Umbrella 가 예상한 것과 같은 정책을 적용했습니까? 그렇지 않은 경우 정책 테스터를 사용하여 어떤 정책을 선택하고 어떤 이유가 있는지 파악합니다.

시나리오 2: 보고(Reporting)

이 시나리오에서는 서로 다른 보고서 유형을 실행하고 각 보고서 유형에 대한 사용 사례를 파악합니다. 보고(Reporting)는 악성 활동을 강조 표시하고 해당 활동과 관련된 위협 인텔리전스를 탐색하여 솔루션의 가치를 입증하는 Umbrella 의 중요한 부분입니다.

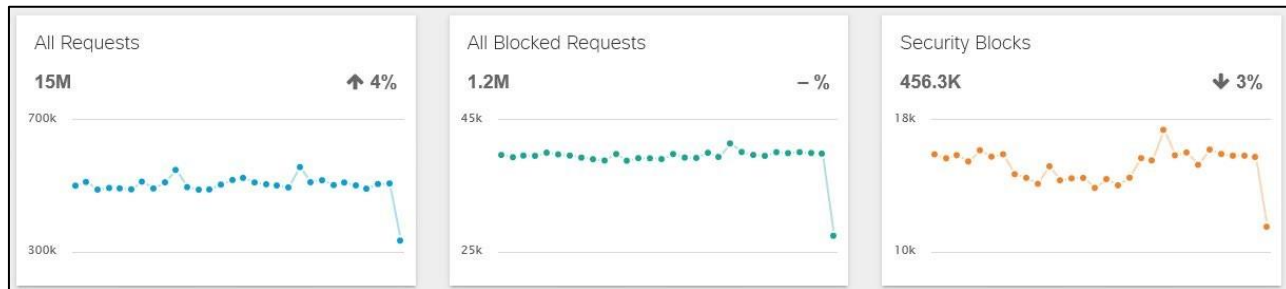
노트: 이전 실습 세션에서 보고 연습을 완료한 경우 보고서 유형 중 일부는 새 유형이고 다른 유형은 향상되었으므로 이 시나리오의 모든 연습을 검토하는 것이 좋습니다.

스텝

실습 1: 보안 개요

VM 시스템 중 하나에서 Umbrella 대시보드에 액세스합니다. **Security Overview(보안 개요)**는 Umbrella 대시보드에서 **Reporting(보고)**을 확장할 때 표시되는 첫 번째 보고서입니다. 이 보고서의 목적은 기업 관리자에게 다양한 관점에서 환경을 신속하게 파악하도록 하기 위해서 만들었습니다.

1. Umbrella 대시보드에서 **Reporting > Security Overview**로 이동합니다.
2. 페이지 상단에서 타임 브래킷을 **LAST 30 DAYS** 로 변경합니다.
3. 첫 번째 영역을 관찰하여 요청된 기간의 일반적인 활동 추세를 보여줍니다.



4. 첫 번째 그래프에는 모든 요청이 표시되고, 두 번째 그래프에는 차단된 요청 수가 표시되며, 세 번째 그래프에서는 이러한 요청 중 보안 블록 수가 몇 개인지 확인할 수 있습니다.

노트: 이 내용은 모든 포트 및 프로토콜에 대한 요청을 다룹니다!

5. 마우스로 그래프 위에 마우스를 올립니다. 그래프를 클릭하면 **Activity Search** 리포트로 리디렉션됩니다(지금 클릭하면 기본 탐색 창에서 **Security Overview** 로 돌아갈 수 있습니다)
6. 필터 패널을 확장하려면 왼쪽의 **FILTERS** 버튼을 클릭합니다. 여기서 **Security Blocks(보안 블록)**과 **All Security Events(모든 보안 이벤트)**를 전환할 수 있습니다(정책 설정에 따라 모든 보안 이벤트가 반드시 블록으로 끝나는 것은 아님). 또한 전체 사이트 및 네트워크 ID 를 제외하여 사용자와 컴퓨터에만 집중할 수 있습니다.

- 다음 영역인 대부분의 **Most Security Blocks** 을 관찰합니다. 대상, ID 및 유형별로 정렬된 최상위 블록 이벤트를 표시합니다.
- By Destination** 도메인 이름, IP 주소 또는 URL 경로일 수 있습니다.
- By Identity** 는 네트워크, 특정 장치 또는 AD 사용자일 수 있습니다.
- By Type** 로 블록을 시작한 보안 범주 또는 다른 엔진에 대해 자세히 알 수 있습니다.

Most Security Blocks			
BY DESTINATION		BY IDENTITY	BY TYPE
Destination	Blocked Requests	Destination	Blocked Requests
bingbangboom.com	290	wcnvknkbcqxcmdidkirkgnfu.org	259
y4bxj.adozeuds.com	285	clearerstats.com.es	258
goloduha.info	278	zimagdcmasn.net	256
d34fa.lasmeio.com	264	egerdpkvutvodmtsy.pw	253
p27dokhpz2n7nvgr.1fqwek.top	261	uvcmifca.biz	251

VIEW BLOCKED REQUESTS 1 of 10 < >

노트: 결과를 클릭하면 관련 세부 정보를 표시하는 필터를 갖춘 활동 보고서로 이동합니다.

- 다음 영역을 관찰하여 현재 활성 ID 를 표시합니다. **네트워크, 로밍 클라이언트 및 활성 가상 어플라이언스** 등 세 가지 유형의 ID 가 표시되며, 이 ID 는 모두 세분화되어 현재 온라인 및 활성 상태인 ID 의 수를 표시합니다. 이 기능은 관리자의 주의가 필요한 모든 문제를 강조 표시할 때 유용합니다.

<p>Active Networks</p> <p>3/3 100% Active</p> <p>VIEW NETWORKS</p>	<p>Active Roaming Clients</p> <p>29/31 94% Active</p> <p>VIEW ROAMING CLIENTS</p>	<p>Active Virtual Appliances</p> <p>2/2 100% Active</p> <p>VIEW VIRTUAL APPLIANCES</p>
--	---	--

노트: **VIEW** 를 클릭하면 관련 세부 정보를 표시하는 필터를 갖춘 활동 보고서로 이동합니다.

실습 2: 보안 활동

보안 관리자는 **Security Activity** 보고서를 통해 보안 관련 이벤트를 자세히 살펴보고 다양한 보안 이벤트 유형을 기준으로 필터링하거나 정렬할 수 있습니다.

- 기본 대시보드 탐색 창에서 리포트 목록 맨 위에 있는 **Security Activity** 누르십시오.



2. 보고서 왼쪽에서 기간을 **This Week**, 그리고 **then Last 30 Days** 변경합니다. 보고서 결과가 동적으로 업데이트되는 것을 봅니다.
3. 보고서의 상단 그래프에는 선택한 기간 동안의 총 보안 이벤트 수 추세가 표시되며, 선택한 시간 범위에 따라 일 및 시간 사이에 해상도가 변경됩니다.
4. 아래쪽 그래프는 지금부터 각 행이 개별 이벤트인 시간을 거슬러 사건의 세부 정보를 보여줍니다. 각 이벤트의 일반 세부 정보가 라인에 표시됩니다.
5. 이벤트 상단을 클릭하여 확장하고 해당 이벤트에 대한 추가 정보를 표시합니다.

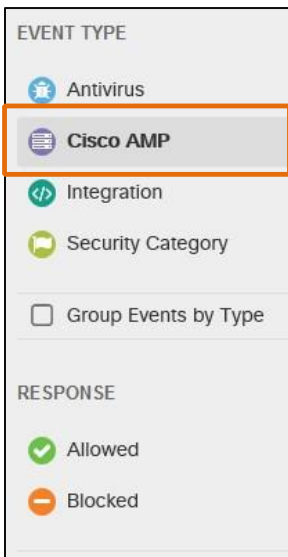
The screenshot shows the details of a blocked event. The event is identified as 'MADSMITH-M-D0R8' and occurred on 'Mar 26, 2017 at 7:52 PM'. The event details are as follows:

Field	Value
Date & Time	Mar 26, 2017 at 7:52 PM
External IP	67.163.97.89
Content Type	text/html
Destination	proxy.brew.opendnstest.com
Result	Blocked
Total Size in Bytes	379
Identity	MADSMITH-M-D0R8 Anyconnect Roaming Client
URL	http://proxy.brew.opendnstest.com/download/eicar.com
SHA256 Hash	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
Categories	Malware
User Agent	Virus

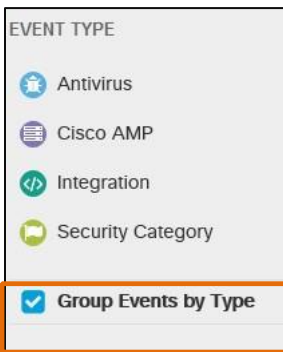
At the bottom right, there is a pagination control showing '1 of 25 Requests' with navigation arrows.

6. 이벤트가 확장되면 아래 왼쪽/오른쪽 화살표를 사용하여 해당 이벤트의 모든 인스턴스(모든 요청)를 스크롤할 수도 있습니다.
이러한 이벤트 내의 대상 및 ID 에 대한 링크를 기록합니다.

7. 왼쪽에는 서로 다른 이벤트 유형(색상으로 구분됨)과 반응 유형(허용됨 또는 차단됨)으로 리포트를 필터링하기 위한 버튼이 있습니다. 활성화된 필터는 음영 처리된 배경으로 표시됩니다.



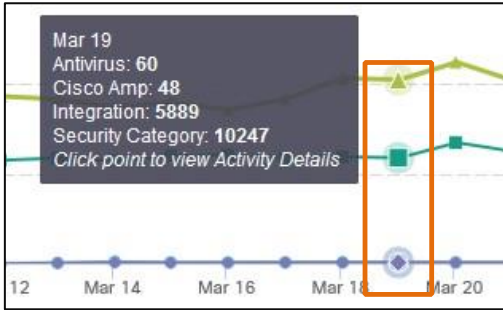
8. 다양한 **EVENT TYPE** 필터를 클릭하고 표시된 이벤트를 살펴봅니다.
9. **EVENT TYPE** 필터를 해제하고 **RESPONSE** 필터 아래에서 **Allowed** 를 클릭합니다. 이러한 이벤트는 보안 이벤트이지만 정책의 보안 범주의 설정에 따라 항상 차단되지는 않을 수 있습니다.
10. 필터 영역에서 **Group Events by Type** 확인란을 클릭합니다. 상단 그래프의 디스플레이가 어떻게 변경되는지 관찰합니다.



11. 제외할 그래프 하단에 있는 이벤트 유형 이름 중 하나를 클릭하여 그래프에 추가합니다.



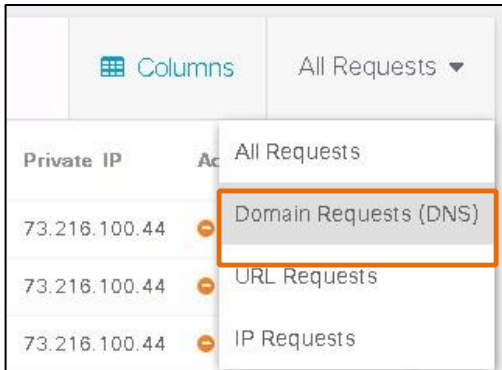
12. 그래프에서 이벤트 유형 중 하나의 결과를 클릭합니다. 다음 보고서 유형인 **Activity Search** 로 이동합니다.



실습 3: 활동 검색(Activity search)

Activity Search 보고서는 모든 활동에서 심층 검색을 실행하고 필터와 활성 링크를 통해 특정 영역 또는 방향으로 드릴다운할 수 있도록 합니다. 이 보고서는 **Security Activity** 보고서와 달리 비보안활동도 포함하고 있다. DNS, 프록시 및 IP 계층에서 적용되는 요청에 대해 별도의 보고서가 실행됩니다.

1. **DNS(Domain Requests), URL Requests, IP** 요청별로 결과를 필터링할 수 있다는 점에 유의하십시오. 보안 활동 보고서에서 클릭한 링크에 따라 다른 보고서 유형에 도달할 수 있습니다. **DNS(Domain Requests)** 보고서가 아직 보이지 않는 경우, 결과 테이블 오른쪽 상단의 드롭다운 목록에서 지금 선택하십시오.



2. 페이지 상단의 시간 범위를 **LAST 30 DAYS** 로 변경합니다.

3. **DNS(Domain Requests)** 보고서는 DNS 계층에서 시행된 최근 활동을 보여준다. 이 보고서에는 요청된 도메인, 개인 및 공용 IP 주소, 요청 결과 등 사용자의 DNS 요청에 관한 관련 정보가 수록되어 있습니다.

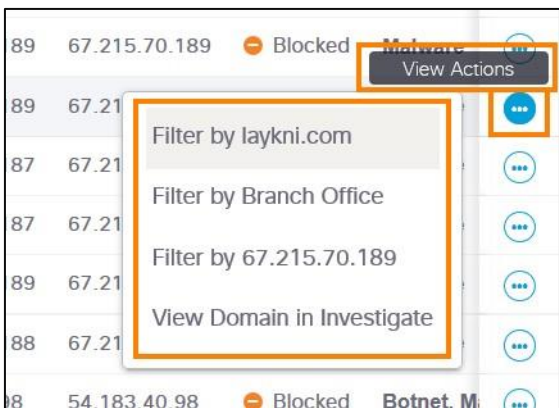
4. 왼쪽의 **Response** 를 필터 아래에서 **Blocked** 를 선택하고 **Apply** 를 누르십시오. 이 작업이 차단된 요청만 표시하도록 결과를 빠르게 필터링하는 방법을 관찰하십시오.

Identity	Identity Type	Destination	DNS Type	Public IP	Private IP	Response
Branch Office	Networks	upantool.com	A	67.215.70.189	67.215.70.189	Blocked
HQ	Networks	vstrackab.com	A	67.215.70.187	67.215.70.187	Blocked
HQ	Networks	jobmail.co.za	A	67.215.70.187	67.215.70.187	Blocked
HQ	Networks	multicodec.co.kr	A	67.215.70.187	67.215.70.187	Blocked

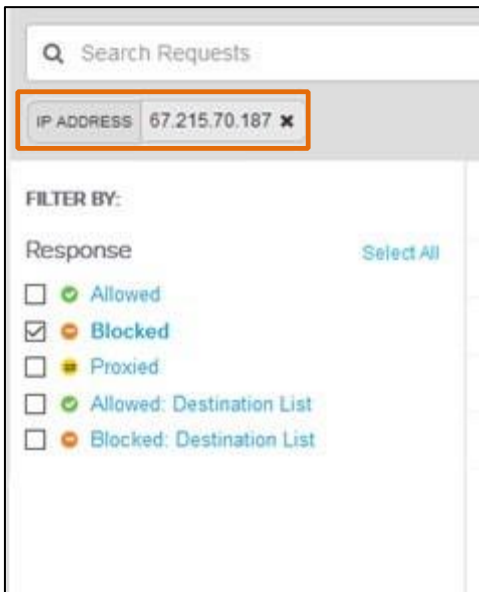
5. **Blocked** 의 선택을 취소하고 **Security Categories** 를 기준으로 필터링하도록 선택합니다. 임의로 일부를 선택하고 **APPLY(적용)**를 클릭하여 결과를 관찰합니다. 필터가 추가되거나 삭제되고 변경 사항이 적용되면 기본 테이블의 결과가 변경 사항과 함께 업데이트됩니다.

FILTER BY:		Identity	Identity Type	Destination	DNS Type	Public IP	Private IP	Response	Categories
Response Select All		Guest Wifi	Networks	87g2.com	A	67.215.70.188	67.215.70.188	Blocked	Malware
<input type="checkbox"/> Allowed		Guest Wifi	Networks	qlanx6.com	A	67.215.70.188	67.215.70.188	Blocked	Malware
<input type="checkbox"/> Blocked		HQ	Networks	laykni.com	A	67.215.70.187	67.215.70.187	Blocked	Malware
<input type="checkbox"/> Proxied		Branch Office	Networks	click2lap.com	A	67.215.70.189	67.215.70.189	Blocked	Malware
<input type="checkbox"/> Allowed: Destination List		Branch Office	Networks	laykni.com	A	67.215.70.189	67.215.70.189	Blocked	Malware
<input type="checkbox"/> Blocked: Destination List		HQ	Networks	tgmgo.com	A	67.215.70.187	67.215.70.187	Blocked	Malware
Identity Type Select All		HQ	Networks	mycelebritydaily.com	A	67.215.70.187	67.215.70.187	Blocked	Malware
<input type="checkbox"/> Computer		Branch Office	Networks	tvoonlinegratis1.com	A	67.215.70.189	67.215.70.189	Blocked	Malware
<input type="checkbox"/> User		Guest Wifi	Networks	driverscape.com	A	67.215.70.188	67.215.70.188	Blocked	Malware
<input type="checkbox"/> Roaming Computer		CAMPUS-E560-044	Anyconnect Roaming Client	gmumwmiwoqegwwo.org	A	54.183.40.98	54.183.40.98	Blocked	Botnet, M
<input type="checkbox"/> Network Device		CAMPUS-E560-044	Anyconnect Roaming Client	gmumwmiwoqegwwo.org	A	54.183.40.98	54.183.40.98	Blocked	Botnet, M
<input type="checkbox"/> Network		loaner-0464	Anyconnect Roaming Client	catpitaqmi.net	A	54.183.40.98	54.183.40.98	Blocked	Malware, l
<input type="checkbox"/> Site		loaner-0464	Anyconnect Roaming Client	egerdpkvutvodmtsy.pw	A	54.183.40.98	54.183.40.98	Blocked	Malware
Security Categories Select All		Umbrella Demo PC	Anyconnect Roaming Client	xcmh.cc	A	54.183.40.98	54.183.40.98	Blocked	Malware
<input checked="" type="checkbox"/> Dynamic DNS		Windows Demo Roaming	Anyconnect Roaming Client	easysideoembed.com	A	54.183.40.98	54.183.40.98	Blocked	Malware
<input type="checkbox"/> Botnet		loaner-0464	Anyconnect Roaming Client	egerdpkvutvodmtsy.pw	A	54.183.40.98	54.183.40.98	Blocked	Malware
<input checked="" type="checkbox"/> Malware									
<input type="checkbox"/> Phishing									
<input checked="" type="checkbox"/> FireEye									
<input type="checkbox"/> Check Point									
<input type="checkbox"/> ZoneFX									

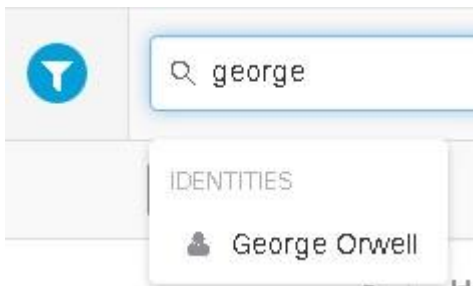
6. 테이블 행의 오른쪽에 있는 **[...](View Actions)** 버튼을 클릭합니다. 선택한 행의 특정 속성(예: 특정 사용자 또는 도메인)에 대한 필터링에 대한 추가 옵션이 표시됩니다. Investigate 를 사용하는 경우 해당 도메인으로 피벗하여 선택한 도메인에 대한 추가 세부 정보를 볼 수 있습니다.



7. **"Filter by..."** 옵션 중 하나를 클릭합니다. 왼쪽의 **FILTER BY** 막대의 필터 선택 및 결과 표 위에 추가되는 필터 값에 따라 리포트 결과가 업데이트되는 방법을 관찰합니다.



8. 결과 테이블에 추가된 필터를 모두 지우고 또 왼쪽의 **FILTER BY** 바의 필터에서 확인란을 확인합니다("APPLY"를 클릭하십시오).
9. 결과 위의 **Search Requests** 필터 박스에서 사용자 이름 또는 장치 이름 입력을 시작합니다(확실하지 않으면 필터링되지 않은 결과를 스크롤하여 찾기만 하면 됩니다).추천된 이름이 표시됩니다. 하나를 클릭하고 새 필터에 따라 결과 테이블이 업데이트되는 방법을 관찰합니다.



10. "Search Requests" 박스에서 추가한 필터를 모두 삭제합니다.
11. 왼쪽에 있는 **FILTER BY** 바에서 응답 필터에서 **Proxied**(다른 항목 제거)를 선택합니다. **APPLY** 를 클릭합니다.



노트: 응답 결과가 추가 검사를 위해 요청을 지능형 프록시로 리디렉션하면 요청이 여기에 표시됩니다. 그러나 (DNS 계층에서) **Domain Requests** 보고서를 계속 볼 때 표시되는 정보는 모두 DNS 요청의 관점에서 볼 수 있습니다.

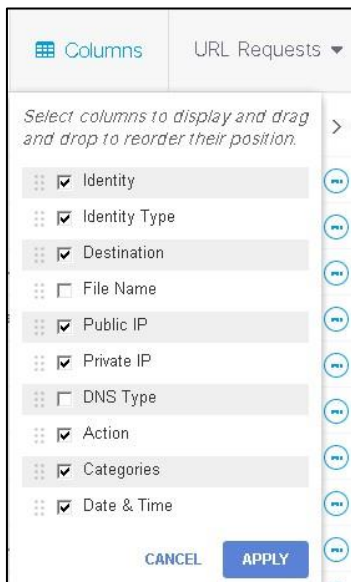
12. 다음에 프록시 트래픽의 결과를 검사합니다. 결과 테이블 오른쪽 상단의 드롭다운 목록에서 **URL Requests** 를 선택합니다.



13. 검사 결과 및 현재 프록시에서 볼 수 있는 특정 정보를 포함하여 보고서 활동을 프록시 수준에서 표시합니다.예를 들어, 대상 열의 전체 URL.
14. 이제 각 라인에 더 많은 정보가 표시되면 결과 테이블 위에 있는 필터 아이콘을 클릭하여 왼쪽 FILTER BY 바를 숨기거나 숨기기 취소할 수 있습니다.



15. 리포트 결과에서 보려는 열을 선택하고 순서를 설정할 수 있습니다. 열 선택 항목을 보려면 Columns 버튼을 클릭하십시오. 원하는 위치로 끌어서 순서를 변경한 다음 **APPLY** 또는 **CANCEL** 을 클릭하십시오.

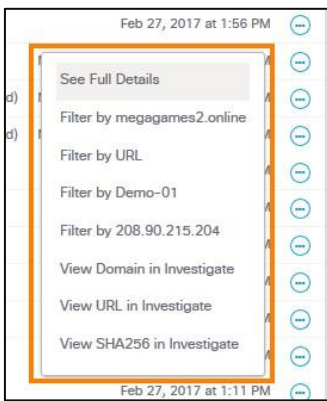


16. 오른쪽으로 스크롤하여 Cisco AMP(**Blocked — Cisco AMP...**)로 인해 응답이 차단된 라인을 찾으십시오. 이것은 Cisco AMP 에 의해 차단된 파일의 결과를 보여줍니다. AMP 클라우드 데이터베이스는 이 파일에 대해 **SHA256** 과

실시간으로 쿼리되었으며, 악성인 것으로 알려져 파일이 차단되었습니다(왼쪽 필터도 사용하여 차단된 응답만 표시할 수 있어 AMP 블록 검색 속도가 빨라집니다).

70.199.194.46	Allowed			Feb 27, 2017 at 1:56 PM	⋮
70.199.194.46	Allowed			Feb 27, 2017 at 1:56 PM	⋮
208.90.215.204	Blocked	Cisco AMP (W32.Auto.ec09e0.201549.in01)	Malware	Feb 27, 2017 at 1:44 PM	⋮
208.90.215.204	Blocked	Cisco AMP (EICAR:EICAR_Test_file_not_a_virus-tpd)	Malware	Feb 27, 2017 at 1:44 PM	⋮
208.90.215.204	Blocked	Cisco AMP (EICAR:EICAR_Test_file_not_a_virus-tpd)	Malware	Feb 27, 2017 at 1:17 PM	⋮
208.90.215.204	Allowed			Feb 27, 2017 at 1:11 PM	⋮
208.90.215.204	Allowed			Feb 27, 2017 at 1:11 PM	⋮

17. AMP 에 의해 차단된 라인에 [...](**View Actions**)를 클릭하십시오. 현재 사용 가능한 작업에는 URL 수준의 옵션도 포함됩니다.



18. 컨텍스트 메뉴의 상단에서 "see full details"를 클릭하십시오. 이를 통해 블록의 모든 세부사항을 하나의 요약으로 점검할 수 있습니다.

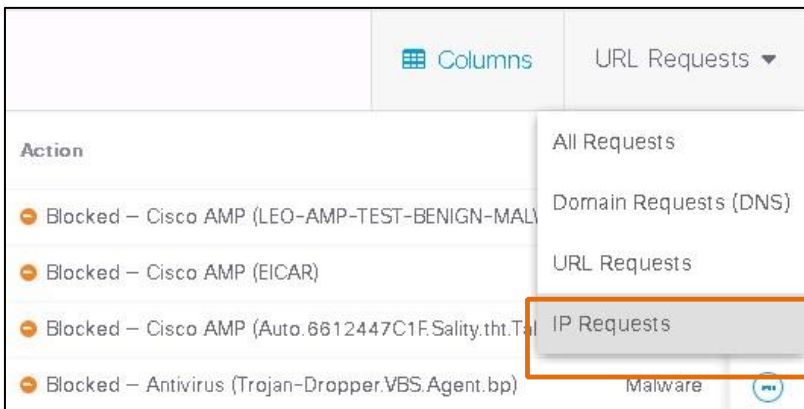
NOTE: SHA256 해시는 AMP 에 차단된 파일을 표시합니다.



19. 다음으로 IP 계층 결과를 살펴보겠습니다.

노트: 이 시나리오를 보고하기 위해 라이브 랩 계정을 사용하지만 로밍 클라이언트를 통해 IP 계층 적용을 구현하지 않은 경우 이 리포트에 결과가 표시되지 않습니다.

20. 결과 영역의 오른쪽 상단에 있는 드롭다운 목록에서 **IP 요청**를 선택합니다. 로밍 클라이언트를 통해 IP 계층 적용을 구현한 경우 차단된 IP 요청의 세부 정보, 대상 IP 및 포트 및 차단된 이유와 함께 이 작업을 볼 수도 있습니다.



21. **DNS** 보기로 돌아가(드롭다운 목록에서 **DNS(Domain Requests)** 선택) 응답이 차단되었음을 나타내는 요청을 검색합니다.

22. 차단된 대상을 클릭합니다. **대상** 보고서로 이동하고 다음 보고서는 다룹니다.

실습 4: 목적지(Destination)

목적지(Destination) 리포트를 통해 요청된 대상을 분석하고 추세를 확인할 수 있습니다.

노트: 방금 사용한 것처럼 다른 보고서 유형의 특정 대상을 클릭하여 대상 보고서에 액세스할 수 있습니다. 탐색 메뉴를 통해 이 보고서에 액세스하면 가장 활성 상태인 대상(최근에 가장 많이 요청된 대상)이 나열됩니다. 여기서 도메인을 검색할 수도 있습니다.

1. 활동 보고서에서 클릭한 차단된 도메인이 이 대상 리포트의 초점이 됩니다. 최근 24 시간 동안의 조직의 로컬 활동 추세가 표시됩니다. 페이지 상단의 검색 시간을 **LAST 30 DAYS** 로 변경합니다.



2. 왼쪽 상단에 표시된 것처럼 선택한 기간 동안 조직에서 이 대상으로 보내는 총 요청 수를 기록합니다.
3. 그래프는 과거 추세에서 오버레이된 요청 수를 나타냅니다. 그러면 해당 대상에 대한 요청에 대한 피크 위치뿐 아니라 가장 적게 활성 상태일 때도 빠르게 확인할 수 있습니다. 그래프 위에 마우스를 올려 놓으면 다양한 포인트의 값을 볼 수 있습니다

노트: 점을 클릭하면 활동 보고서로 돌아갑니다.

4. 그래프 위에서 **GLOBAL %**를 클릭합니다. 엠브렐라가 지정한 시간에 걸쳐 이 대상에 대한 요청을 확인한 글로벌 추세를 표시하기 위한 이 변경 사항입니다. 조직의 트래픽으로 구성된 대상에 대한 글로벌 트래픽의 백분율을 표시합니다. 이는 이것이 조직에 대한 표적형 공격인지 아니면 보안 관리자가 조사의 우선순위를 더 잘 정할 수 있도록 하는 기회주의적 공격인지 유추하는 데 유용합니다.



참고: 그래프는 Umbrella Investigate 에 대한 링크를 제공합니다. 여기서 이 대상을 더 분석하고 인터넷에서 이 도메인의 관계와 진화를 전체적으로 볼 수 있습니다. 조사는 이 연구소에서 전용 시나리오로 다룹니다.

- 아래로 스크롤하여 **Access & Policy Details** 섹션으로 이동합니다. 이 정보에는 최근 이 대상을 요청했던 조직의 최상위 ID 가 포함되어 있습니다.

Access & Policy Details

Top Identities

Identity	Events
MES-W530-018	12
Demo-06	11
AnyConnect-Roaming-Laptop	11
BARFISHE-M-X2W1	10
Demo-05	10
loaner's MacBook Pro	10
presenter02	10
CAMPUS-E560-044	10
Presenter ThinkPad	9
loaners-MacBook-Pro	9

VIEW ALL EVENTS BY IDENTITY

Destination Lists with clearerstats.com.es

We've categorized this destination as **Malware**. Policies using this security filter will already block clearerstats.com.es.

This destination is not on any destination lists.

VIEW ALL POLICIES

- 이 영역(오른쪽)에서 이 대상이 엄브렐라의 보안 범주에 분류되어 있는지 여부 및 대상 목록에 표시되는지 여부를 확인할 수 있습니다.

노트: 이 영역에는 아직 프록시된 도메인이 포함되지 않습니다(확대 보안 범주 또는 고객 대상 목록).

- 이 도메인의 **Recent Activity** 영역으로 스크롤합니다.

Recent Activity for clearerstats.com.es

Identity	Response	External IP	Internal IP	Date & Time
 Guest Wireless	Blocked	54.183.40.98	54.183.40.98	Mar 30, 2017 at 12:11 PM
 presenter02	Blocked	54.183.40.98	54.183.40.98	Mar 30, 2017 at 12:07 PM
 Demo-04	Blocked	54.183.40.98	54.183.40.98	Mar 30, 2017 at 12:07 PM
 AnyConnect-Roaming-Laptop	Blocked	54.183.40.98	192.168.24.75	Mar 30, 2017 at 12:07 PM
 CAMPUS-E560-044	Blocked	54.183.40.98	54.183.40.98	Mar 30, 2017 at 11:15 AM

[VIEW ALL RECENT ACTIVITY](#)

- 개별 요청에 의해 이 대상에 대한 모든 최근 요청 활동을 표시합니다. **Activity Search** 리포트에 표시되는 내용을 요약한 것이며, ID 를 클릭하면 해당 리포트로 돌아갑니다(클릭하지 않음).
- Top Identities** 영역으로 다시 스크롤하고 목록에서 상위 ID 를 클릭합니다. 다음 보고서인 **Identities** 로 이동합니다.

Access & Policy Details

Top Identities

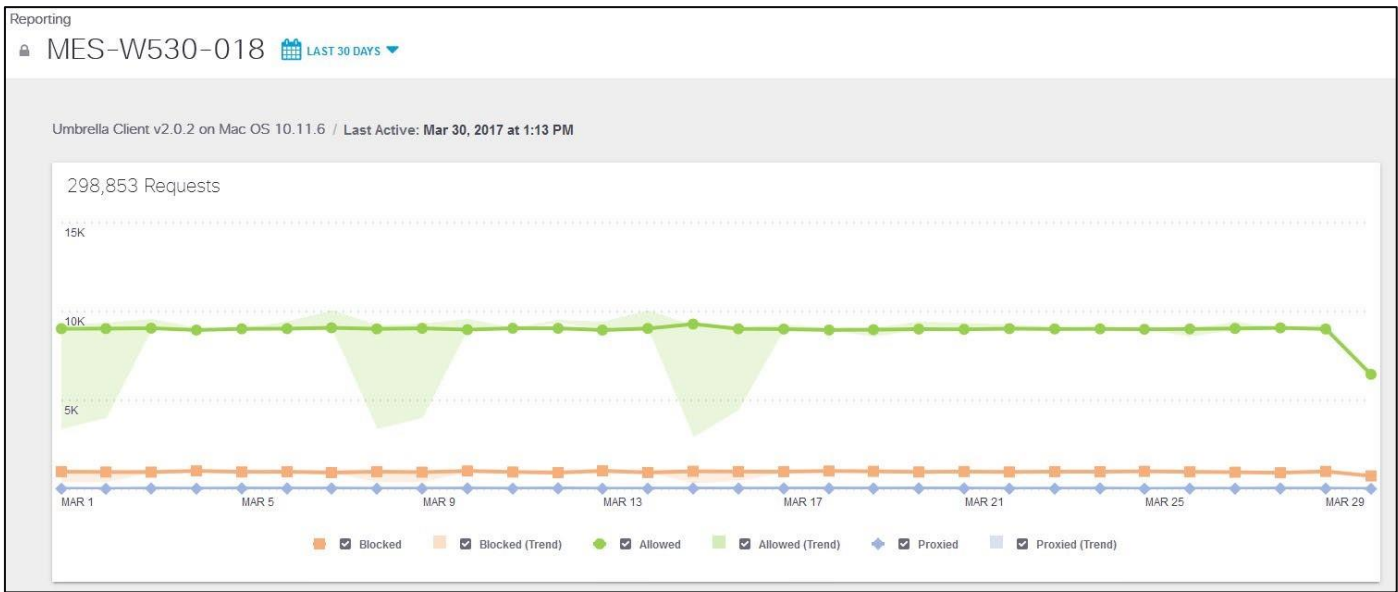
Identity	Events
 MES-W530-018	12
 Demo-06	11

실습 5: Identities

Identities 보고서를 사용하면 조직 내의 ID 를 다양한 관점에서 분석하고 추세를 확인할 수 있습니다.

노트: 방금 사용한 것처럼 다른 보고서 유형의 특정 ID 를 클릭하여 ID 보고서에 액세스할 수 있습니다. 탐색 메뉴를 통해 이 보고서에 액세스하면 가장 활성 상태인 ID(최근에 가장 많은 요청을 한 ID)가 나열됩니다. 특정 ID 를 검색할 수도 있습니다.

- 대상 보고서에서 클릭한 ID 가 이 대상 리포트의 초점이 됩니다. 허용, 차단 및 프록시 요청에 대한 별도의 결과와 함께 지난 24 시간 동안 해당 ID 에 대한 활동이 표시됩니다. 이것들은 역사적 경향에 겹쳐져 있습니다. 페이지 상단의 검색 시간을 **LAST 30 DAYS** 로 변경하십시오.



2. 확인된 공통적인 위험 중 하나는 악의적인 대상을 요청할 때 다른 여러 가지 위험 요소를 동시에 요청하는 경우가 많다는 것입니다. 이 리포트는 이 ID에 대해 허용, 차단 또는 프록시된 총 요청과 이러한 요청이 기록 추세와 일치하는지 여부를 표시합니다.

3. **Top Destrations** 섹션으로 이동합니다. 이 영역은 최근에 이 ID에서 요청한 상위 대상을 표시합니다.

Top Destinations

SECURITY ALL

Destinations	Requests
zimagdcmasn.net	272
d34fa.lasmeio.com	266
egerdpkvutvodmtsy.pw	264
update1.myownguardian.com	264
wcnvknkbcqxcmdldkbrkgqnfu.org	261

[VIEW ALL DESTINATIONS](#)

4. 엠브렐라의 보안 범주 중 하나로 분류된 이 ID의 목적지와 일반적으로 모든 목적지를 구분할 수 있습니다. 디스플레이를 변경하고 차이를 기록하려면 **SECURITY** 및 **ALL**를 클릭합니다. 아래 **VIEW ALL DESTINATIONS** 링크는 이 ID에서 최근에 요청한 모든 도메인을 볼 수 있는 최상위 도메인 리포트로 이동합니다.

5. 오른쪽의 **Top Security Categories**는 선택한 기간 동안 이 ID에서 요청한 도메인의 다양한 보안 범주를 보여줍니다. 이러한 보안 범주 중 일부는 다른 Cisco 또는 타사 제품에서 제공됩니다. 아래 **VIEW ALL CATEGORIES** 링크는 이 ID에서 최근에 요청한 모든 카테고리를 볼 수 있는 **Top Categories** 리포트로 이동합니다.

Top Security Categories

Malware	5,914
Cisco AMP Threat Grid Integration	3,091
FireEye Integration	1,287
Check Point Integration	1,180
Potentially Harmful	1,127
DNS Tunneling VPN	674
Botnet	623
Dynamic DNS	327
Phishing	220
Splunk Investigate App Integration	53
Malware	2

[VIEW ALL CATEGORIES](#)

6. 이 ID 를 보려면 **최근 활동** 영역으로 스크롤합니다.

Recent Activity for MES-W530-018

Destination	Response	External IP	Internal IP	Date & Time
gctzj1ttq57m249duo1wqq8b2.com	Allowed	54.183.40.98	54.183.40.98	Mar 30, 2017 at 3:03 PM
dustin.se	Allowed	54.183.40.98	54.183.40.98	Mar 30, 2017 at 3:03 PM
ducksters.com	Allowed	54.183.40.98	54.183.40.98	Mar 30, 2017 at 3:03 PM
wumii.com	Allowed	54.183.40.98	54.183.40.98	Mar 30, 2017 at 3:02 PM

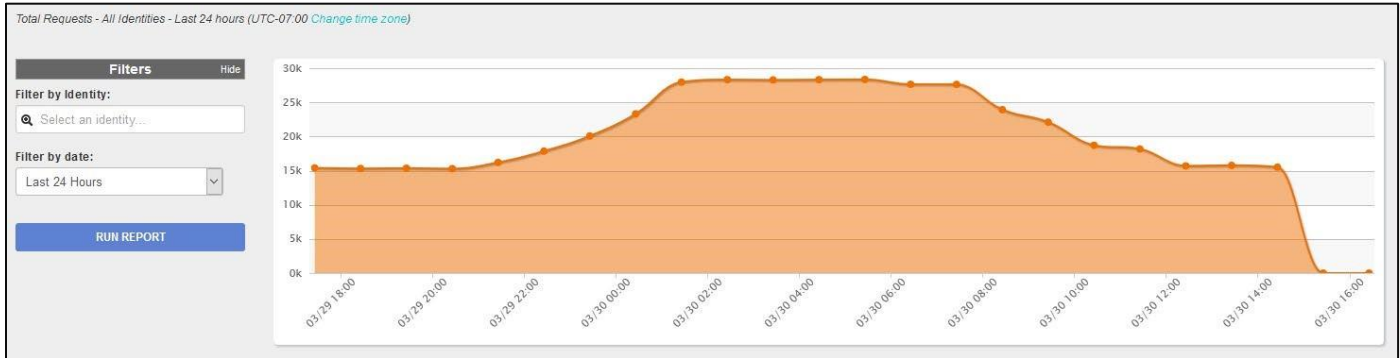
[VIEW ALL RECENT ACTIVITY](#)

7. 이 ID 에 의해 최근에 요청된 모든 대상을 표시합니다. **Activity Search** 리포트에 표시되는 내용을 요약한 것이며, ID 를 클릭하면 해당 리포트로 돌아갑니다(클릭하지 않음).

실습 6: 기타 보고서 및 옵션

이 연습에서는 **ADDITIONAL REPORTS** 하위 메뉴의 다른 보고서와 몇 가지 추가 보고 기능을 간략하게 보여 줍니다.

1. 기본 탐색에서 **Reporting > Total Requests** 를 클릭합니다.
2. 이 보고서에는 선택한 기간 동안 조직이 요청한 모든 내용이 표시됩니다. 시간 범위를 변경하고 필터를 적용하여 특정 ID 에 대한 요청 볼륨을 볼 수도 있습니다.



3. 기본 탐색에서 **Reporting > Activity Volume** 을 클릭합니다.
4. 이 보고서는 각 쿼리가 차단되거나 허용된 이유에 따라 세분화된 모든 DNS 쿼리 작업을 보여주는 요약 테이블을 제공합니다. 각 범주 옆에 있는 **[+]** 아이콘을 클릭하여 보안상의 이유로 차단된 다양한 범주의 쿼리를 드릴다운할 수 있습니다. 여기서도 시간 범위를 변경하고 필터를 적용하여 특정 ID 에 대한 활동 볼륨을 볼 수 있습니다.

	Allowed	Blocked	Total	%
<input type="checkbox"/> Security	464	15,840	16,304	3.37%
<input type="checkbox"/> Prevent	463	8,839	9,302	1.92%
<input type="checkbox"/> Contain	0	1,012	1,012	0.21%
<input type="checkbox"/> Integrations	1	5,989	5,990	1.24%
Categories	-	28,185	28,185	5.83%
Destination Lists	332	2	334	0.07%
Permitted	438,955	-	438,955	90.73%
Total	439,751	44,027	483,778	100.00%

5. **Prevent** 섹션을 확장합니다. 여기에 나열된 보안 범주에 주목하십시오. 일부 범주는 최근에 추가되었습니다:
6. **Newly Seen Domains:** Umbrella 고객에 의해 최근(지난 며칠 동안) 처음으로 쿼리되는 것으로 확인된 도메인
7. **Potentially Harmful:** 이 범주는 소비자 DNS 터널링 VPN 서비스와 연결된 서버를 분류합니다. 이러한 서비스를 통해 사용자는 나가는 트래픽을 DNS 쿼리로 위장하여 허용 가능한 사용 또는 DLP 정책을 위반할 수 있습니다. 고객은 이 범주를 차단하거나 보고서를 통해 결과를 모니터링할 수 있으므로 리스크에 대한 내성을 고려하여 무엇이 올바른지 유연하게 결정할 수 있습니다. 이 범주는 보안보다 컴플라이언스/AUP 에 더 중점을 둡니다. 다른 보안 범주는 일반적으로 상업적 서비스의 일부가 아닌 악의적이거나 의심스러운 DNS 터널링을 탐지합니다.

8. **DNS Tunneling VPN:** 이 보안 범주에는 Cisco Umbrella 보안 연구자가 악의적일 가능성이 높지만 일반 블록 목록에 분류된 것보다 신뢰도가 낮은 도메인이 포함되어 있습니다. 특정 서비스 유형에 연결할 수 없는 DNS 터널링은 종종 이 보안 범주에 속합니다. 고객은 이 범주를 차단하거나 보고서를 통해 결과를 모니터링할 수 있으므로 리스크에 대한 내성을 고려하여 무엇이 올바른지 유연하게 결정할 수 있습니다.

Prevent	3,402	61,181	64,583	1.89%
Malware	0	50,429	50,429	1.48%
Dynamic DNS	0	2,453	2,453	0.07%
Newly Seen Domains	0	2	2	0.0001%
Potentially Harmful	1,960	4,717	6,677	0.20%
DNS Tunneling VPN	1,442	3,580	5,022	0.15%

노트: 새로 표시된 도메인에 대한 추가 정보는 <https://support.umbrella.com/hc/en-us/articles/235911828>에서 확인할 수 있습니다.

9. 테이블 위의 **Trend Over Time(시간 경과)**을 클릭하여 보기를 다양한 범주의 추세를 보여주는 그래프로 변경할 수 있습니다.



10. 그래프 위에 범주 이름을 클릭하면 해당 범주가 표시되고 숨겨집니다.

11. 노트: 아래는 보고서에 포함된 다양한 범주에 대한 설명:

12. **Prevent:** 엠브렐라는 악성 웹사이트와 콘텐츠에 대한 사용자들의 접근을 막았다. 멀웨어, 드라이브별 다운로드 및 모바일 위협 포함.

13. **Contain:** 엠브렐라는 맬웨어에서 명령 & 제어 서버로 전송되는 요청을 차단하고 사용자가 속아서 방문하게 된 피싱 사이트에 접근하는 것을 막았다. 봇넷 및 피싱 공격에 대한 C2 콜백 포함.

14. **Advanced Threats:** 엠브렐라는 보안 알고리즘이 악의적인 활동을 예측하는 사이트를 이용자들이 방문하는 것을 막았다. 위협을 포함할 것으로 예상되는 고위험 사이트 포함(이 문서화된 예에서는 이 범주에 대한 결과가 없음).
15. **Integrations:** 엠브렐라는 고객 환경(FireEye, Check Point 등)에서 엠브렐라와 통합된 보안 파트너의 인텔리전스를 기반으로 DNS 쿼리를 차단했어요.
16. 이 시나리오에 포함된 모든 보고서 유형에서 얻은 지식을 사용하여 다음 세 가지 보고서 유형을 직접 확인하십시오:
 17. Top Domains
 18. Top Categories
 19. Top Identities
20. 위의 각 보고서 유형에 대해 왼쪽의 옵션을 선택하여 필터링한 후 테이블에서 다른 결과를 클릭하여 사용 가능한 드릴다운 옵션을 확인하십시오.
21. 이전 보고서 중 일부로 돌아가서 보고서 페이지 상단에 있는 추가 옵션을 확인하십시오



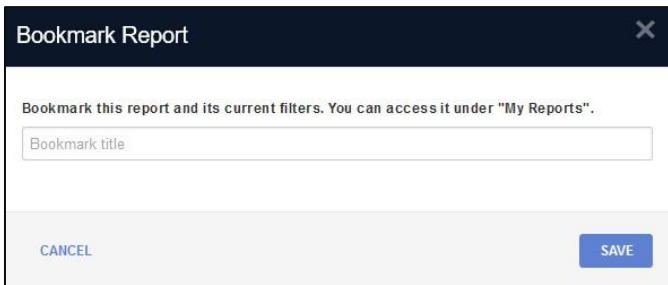
22. Schedule 버튼을 사용하여 현재 보고 있는 보고서를 예약할 수 있습니다. 역시 기본 탐색 메뉴를 통해 예약할 수 있는 모든 리포트에 액세스할 수 있습니다. 리포트를 예약할 때 마법사 필터, 수신인, 예약 및 설명을 통해 추가하십시오.



23. 공유 단추를 사용하여 다른 관리 사용자와 공유할 수 있는 이 리포트에 대한 링크를 얻으십시오.



24. 북마크 옵션을 사용하면 보고서를 저장하고 나중에 "My Reports"에서 찾을 수 있는 이름을 지정할 수 있습니다.



Bookmark Report [X]

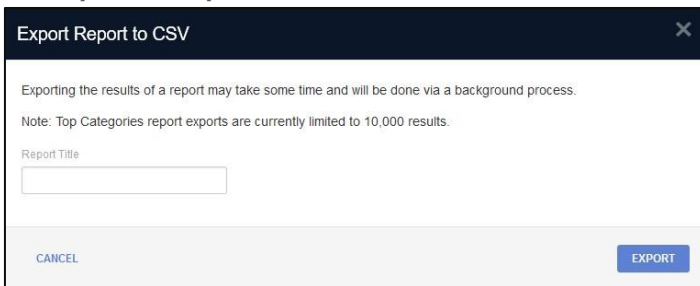
Bookmark this report and its current filters. You can access it under "My Reports".

Bookmark title

CANCEL SAVE



25. 보고서는 로컬 저장 및 추가 조작을 위해 CSV 형식으로 내보낼 수 있습니다. 수출한 보고서는 나중에 **Reporting > Exported Reports** 메뉴에서 다시 액세스할 수 있습니다.



Export Report to CSV [X]

Exporting the results of a report may take some time and will be done via a background process.

Note: Top Categories report exports are currently limited to 10,000 results.

Report Title

CANCEL EXPORT

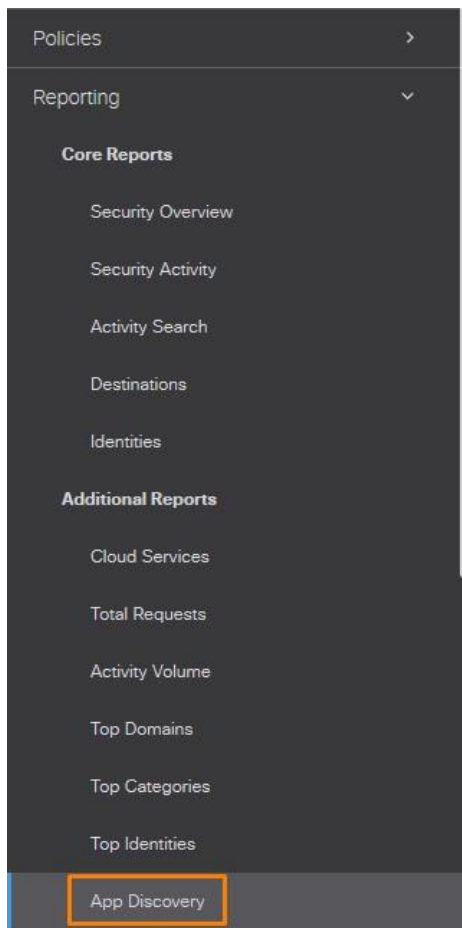
26. **Settings > Log Management** 로 이동합니다. 이 기능은 고객의 Amazon S3 버킷에 전체 로그를 자동으로 내보내고 보관하는 데 사용됩니다. 이 기능은 Umbrella가 클라우드에서 인프라에 로그를 보관하는 30 일의 표준 보존 기간과 달리 로그를 무기한 또는 더 오래 보관하려는 고객에게 유용합니다. 이 기능을 사용하려면 고객이 자신의 AWS S3 버킷을 구독하고 활성화해야 합니다. 아이콘 아래의 페이지 상단에 있는 추가 정보를 읽습니다.



실습 7: App Discovery 및 Application Control

다음은 App Discovery 라는 Umbrella 속에 새로 추가된 대시보드를 살펴보겠습니다. Shadow IT 대시보드인 App Discovery 는 DNS 로그 작업을 기반으로 클라우드 애플리케이션 사용량을 완벽하게 파악할 수 있도록 지원합니다. 범주 롤업, 애플리케이션 세부 정보 및 위험 프로파일이 결합되어 고객은 생산성을 최적화하고 비용을 최소화하며 위험을 줄일 수 있습니다. 이를 통해 안전하고 정보에 입각한 클라우드 채택이 가능합니다.

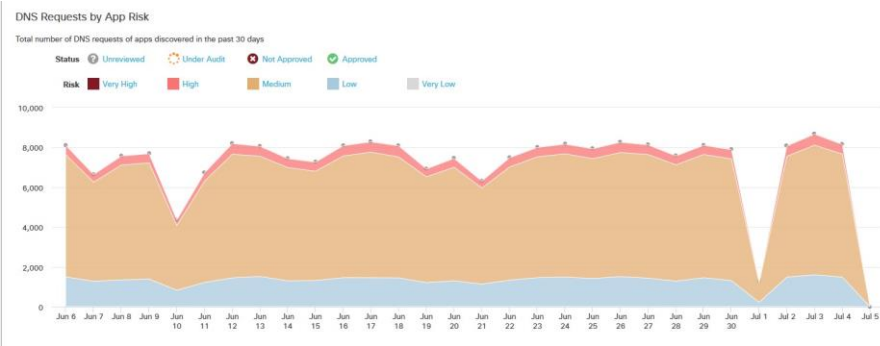
1. Umbellar 대시보드 메뉴에서 Reporting > Additional Reports > App Discovery 를 선택합니다.



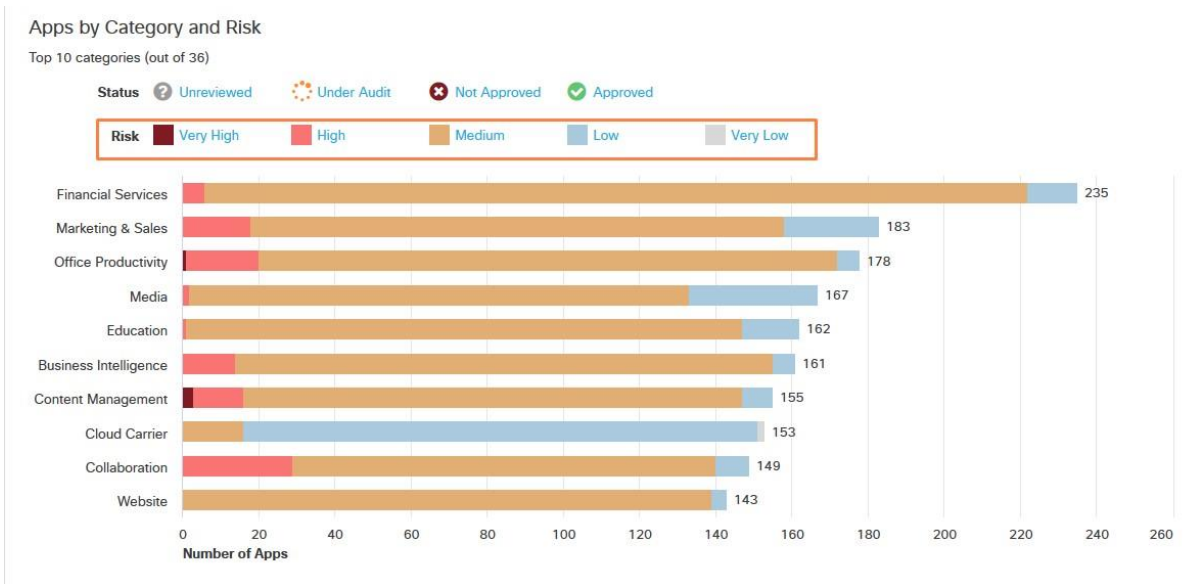
2. App Discovery 대시보드에서 발견된 총 앱 수를 살펴봅니다.



3. **DNS Requests by App Risk** 로 스크롤하십시오. 그래프에 마우스를 올려 DNS 요청이 시간에 따라 추적되는 방법을 표시하십시오. 여기서 관리자는 사용량이 급증하고 특정 앱이 제대로 작동하는지(아직 드릴다운하지 않음) 자세히 볼 수 있습니다.



4. **Apps by Category and Risk** 로 스크롤하여 다른 시각 자료(위쪽의 위험 필터)를 표시하십시오.



5. 카테고리 카드까지 스크롤하여 한 개(Anonymizer 또는 P2P)의 세부 **Details** 를 클릭하십시오.

Category: Anonymizer

6 unreviewed apps

Anonymizer apps introduce risk to your network because they enable users to bypass security controls.

[DETAILS](#)

Category: P2P

3 unreviewed apps

P2P apps represent high risk because they can be used to transmit files infected with viruses and malware.

[DETAILS](#)

Category: Games

64 unreviewed apps

Online games present risk as well as potential productivity loss. In many enterprise environments they are discouraged.

[DETAILS](#)

6. 이제 Apps Grid 로 피벗하셨습니다. 사전 입력된 카테고리 필터가 있다는 점에 유의하십시오. 또한 **Risk, App Type, Status** 및 **Date** 로 다른 필터도 적용할 수 있음을 보여 줄 수 있다. 자세한 내용을 보려면 한 앱(예: **CyberGhost VPN**)를 클릭하십시오.

Dashboard

Search for App / Vendor Category Risk App Type Status Date

Category: Anonymizer x Clear all filters

UNREVIEWED (6) UNDER AUDIT (2) NOT APPROVED (2) APPROVED (0) ALL APPS (10)

All Apps (10 Found)

Application	Vendor	Weighted Risk	Identities	DNS Requests	Blocked	Status
Anonymox Anonymizer	Anonymox	Very High	19	52	6%	Not Approved
CyberGhost VPN Anonymizer	CyberGhost	High	17	49	4%	Unreviewed
DotVPN Anonymizer	DotVPN	Very High	16	54	-	Under Audit
ExpressVPN Anonymizer	ExpressVPN	High	22	59	24%	Unreviewed
Hide My Ass Anonymizer	Hide My Ass	Very High	19	55	11%	Not Approved
NordVPN Anonymizer	NordVPN	High	20	59	19%	Unreviewed
Private Tunnel Anonymizer	OpenVPN	Very High	22	92	13%	Under Audit
ProxySite	ProxySite	Very High	21	68	9%	Unreviewed

7. 앱 세부 정보를 검토하십시오. 각 위험 요소(비즈니스, 사용 및 컴플라이언스)를 확장하여 각 위험 유형의 구성요소를 파악하십시오

Business Risk
High

Usage Type
Typical use: personal, organizational, or indirect (e.g. content delivery network)

Indirect (lower risk) Personal Corporate (higher risk)

Web Reputation
Powered by Talos Security Intelligence

Good Neutral Poor

Financial Viability Risk
Financial risk to the service provider, based on Dun & Bradstreet's Dynamic Risk Score

Low Average High Very High

Data Storage
What form of data does the service store

No Storage (lower risk) Structured Unstructured (higher risk)

Usage Risk
Very High

Usage Risk

DNS Requests
Higher volume of DNS requests contributes to higher levels of risk

0 88 100

Vendor Compliance
Not Found

Vendor Compliance

Status	Name	Description
Non compliant	BITS	NIST Special Publication 800-53 is part of the Special Publication 800-series that reports on the Information Technology Laboratory (ITL) research, guidelines, and outreach efforts in information system security, and on ITLs activity with industry, government, and

8. identities 를 클릭하십시오. identities, DNS Requests 및 Blocked Requests 에 대한 사용 상세 내역을 살펴보세요.

Risk Details **Identities (20)**

Search for Identities Date

Identities	DNS Requests	Blocked Requests	First Detected (UTC)	Last Detected (UTC)
keilarobertsu7c	12	-	Jun 6, 2018	Jul 3, 2018
briannecomptonV2x	11	-	Jun 8, 2018	Jul 5, 2018
NYC Office	10	6	Jun 6, 2018	Jul 5, 2018
kayleighrogersGUs	10	-	Jun 5, 2018	Jun 29, 2018
johnathongravesXFu	9	-	Jun 6, 2018	Jun 30, 2018
billyfuentesWa7	6	-	Jun 12, 2018	Jul 1, 2018
Thomas Ames	2	2	Jun 29, 2018	Jul 4, 2018
Jose Odom	2	2	Jun 26, 2018	Jun 26, 2018
Lorraine Inhnen	1	1	Jun 12, 2018	Jun 12, 2018

9. 뒤로 스크롤하여 앱의 상태를 **Approved**, **Not Approved** 및 **Audit** 로 변경할 수 있다는 점에 유의하십시오.

App: CyberGhost VPN
Dashboard / Apps

CyberGhost VPN
Offers VPN services.

Risk Score
High

App URL
www.cyberghostvpn.com

App Type
SaaS

Category
Anonymizer

Vendor
CyberGhost

Risk Details | Identities

- Unreviewed
- Unreviewed
- Approved
- Not Approved
- Under Audit

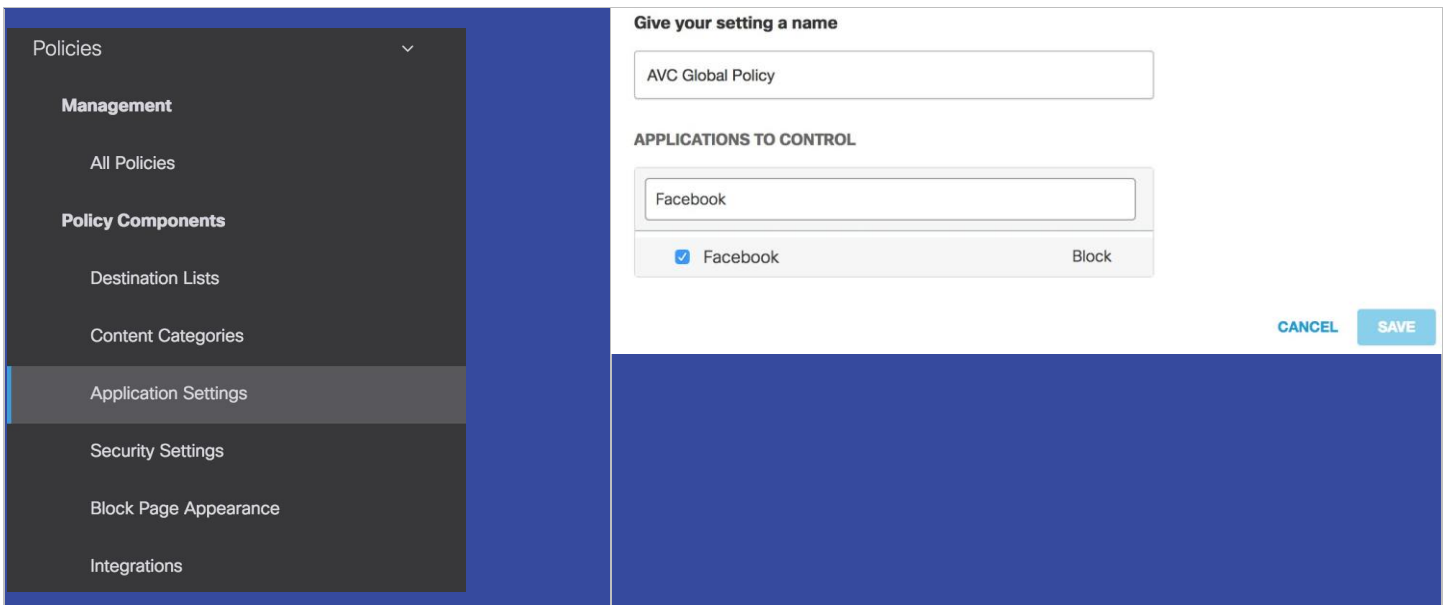
노트: 상태를 **Not Approved** 로 변경하는 것은 실제로 앱을 차단하지 않으며, 이는 태그 지정 프로세스와 더 유사합니다. 앱을 차단하려면 AVC 컨트롤을 사용해야 합니다. 현재 버전의 App Discovery 는 모든 앱을 차단할 수 없으며, 드롭다운 메뉴에서 **Block this app** 링크를 사용할 수 있는 앱만 차단할 수 있습니다.

	Vindico Ad Publishing	Sizmek	Medium	42	16,182	Unreviewed
	Facebook Social Networking	Facebook	Medium	59	11,032	Unreviewed

[Block this app](#)

10. **Block this app** 링크를 클릭하면 **Application Settings** 마법사가 열리고 차단하도록 선택한 앱(아래 설명된 예제의 Facebook)이 **Application Settings** 정책 구성 요소에 미리 채워집니다.

11. 정책의 이름을 **AVC Global Policy** 또는 이와 유사한 것으로 지정하십시오.



12. 일반 시나리오에서는 이 설정을 저장할 수 있으며, 이 응용 프로그램 정책을 사용하는 모든 정책(Policy > All Policies)에 대해 선택한 앱이 차단됩니다.
13. 이 목록이 정책에 적용되는 방법을 보려면 Policy > All Policies 로 이동하십시오. Application Policy 클릭하고 Application Setting Applied 에서 설정을 확인하십시오.



연습 결론

App Discovery 및 Control 서비스를 통해 Umbrella 고객은 Shadow IT 에 대한 가시성을 확보하고, Umbrella 대시보드의 App Risk 색인을 포함한 SaaS 사용량을 파악할 수 있습니다(원래 Cloudlock 기술로 작동됨). 또한 Umbrella 의 SIG 비전에 기여합니다. 앞으로 고객은 발견된 모든 앱을 차단할 수 있습니다.

시나리오 3. Umbrella Investigation

이 시나리오에서는 웹 기반 콘솔 조사로 특정 악성 도메인에 대해 자세히 알아보십시오. 시나리오가 끝날 때쯤에는 공격자의 인프라를 통해 선회함으로써 엄브렐라의 독특한 위협 지능의 가치와 다양한 자원을 하나의 인터페이스로 보여줌으로써 그 사이에서 피벗을 수 있고 관계가 어떻게 구축되는지 볼 수 있는 조사의 가치를 보여줄 수 있어야 합니다. 각 연습은 조사가 유용할 수 있는 다른 사용 사례를 제시합니다.

Umbrella Investigation 대하여

Cisco Umbrella Investigate 는 인터넷을 통해 도메인, IP 및 멀웨어에 대한 위협 인텔리전스를 제공합니다. DNS 요청 및 기타 상황별 데이터에 대한 실시간 그래프를 활용하여 Investigate 는 인터넷 도메인, IP 및 멀웨어의 관계와 진화를 가장 완벽하게 파악하여 공격자의 인프라를 파악하고 향후 위협을 예측하는 데 도움이 됩니다.

전 세계 500 개 이상의 BGP 피어링 파트너로부터 인터넷 상의 서로 다른 네트워크 간 연결에 대한 라이브 뷰와 기업 및 소비자 사용자의 일일 DNS 요청과 1,000 억 개의 다양한 데이터 세트를 활용하여 조사하십시오. 우리는 데이터 마이닝 기법, 3D 시각화, 보안 연구자 전문지식을 사용하여 작성된 통계 모델을 데이터에 적용하여 인터넷에서 패턴을 발견하고 미래의 악의적인 장소를 예측합니다.

조사를 통해 보안 팀은 조사를 가속화하고, 사건 대응의 우선순위를 정하는 데 필요한 글로벌 컨텍스트를 확보하고, 공격에 앞서 나갈 수 있습니다.

노트: 이 시나리오에서 연습하는 동안, 우리는 특정 영역을 강조하겠지만, 조사의 정보가 동적이고 실시간으로 업데이트되기 때문에, 사례에 대한 세부 사항이 변경될 수 있습니다. 이 섹션에서 참조된 도메인 중 하나를 검색하고 스크린샷과 동일한 결과를 얻지 못하면 차분하게 진행하십시오. 오래된 스크린샷과 설명은 여전히 당신에게 그 섹션의 요점을 말해 줄 겁니다. 사용할 수 있는 대체 도메인의 업데이트된 목록이 실험실에 있는지 확인하십시오.

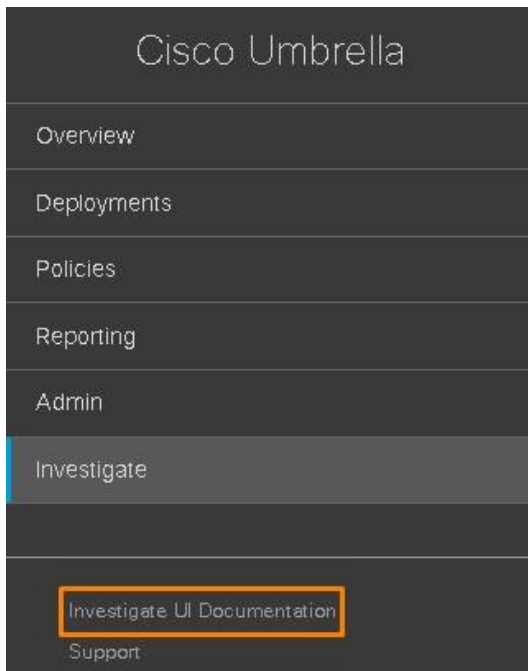
조사할 수 있는 일부 악의적인 대상에 대한 몇 가지 제안:

- textspeier[.]de
- randoz-pandom[.]wang
- usa[.]jitsaol[.]com
- uoeeu kyackaagagg[.]org

이 시나리오의 실습 전반에 걸쳐 추가 목적지가 제시됩니다. <http://www.malwaredomainlist.com/> 과 같은 온라인 툴을 사용하여 입력 및 조사할 다른 악의적인 도메인을 찾을 수도 있습니다.

참고: 이러한 악의적인 대상을 주의하십시오. 이러한 URL 을 사용자 자신의 시스템이나 랩 시스템의 브라우저 URL 표시줄에 직접 붙여넣으려고 하지 마십시오.

참고: 또한 조사를 위한 API 가 있으며, 이는 많은 고객이 SIEM, 위협 인텔리전스 플랫폼 등과 같은 다른 시스템을 자동으로 쿼리하고 풍부하게 하기 위해 사용하는 방법입니다. Investigate 문서에는 API 도 포함되어 있으며, 주요 탐색 메뉴 하단의 링크를 통해 액세스할 수 있습니다.



Destination 보고서에서 도메인에 대한 로컬 트래픽이 모든 엄브렐라 고객으로부터 확인되는 글로벌 트래픽과 어떻게 일치하는지 확인했으며 방문한 도메인에 대한 중요한 보안 세부 정보도 표시되었습니다. 여기와 다른 다양한 보고서에도 종종 도메인 조사 및 조사를 열 수 있는 링크가 있습니다.



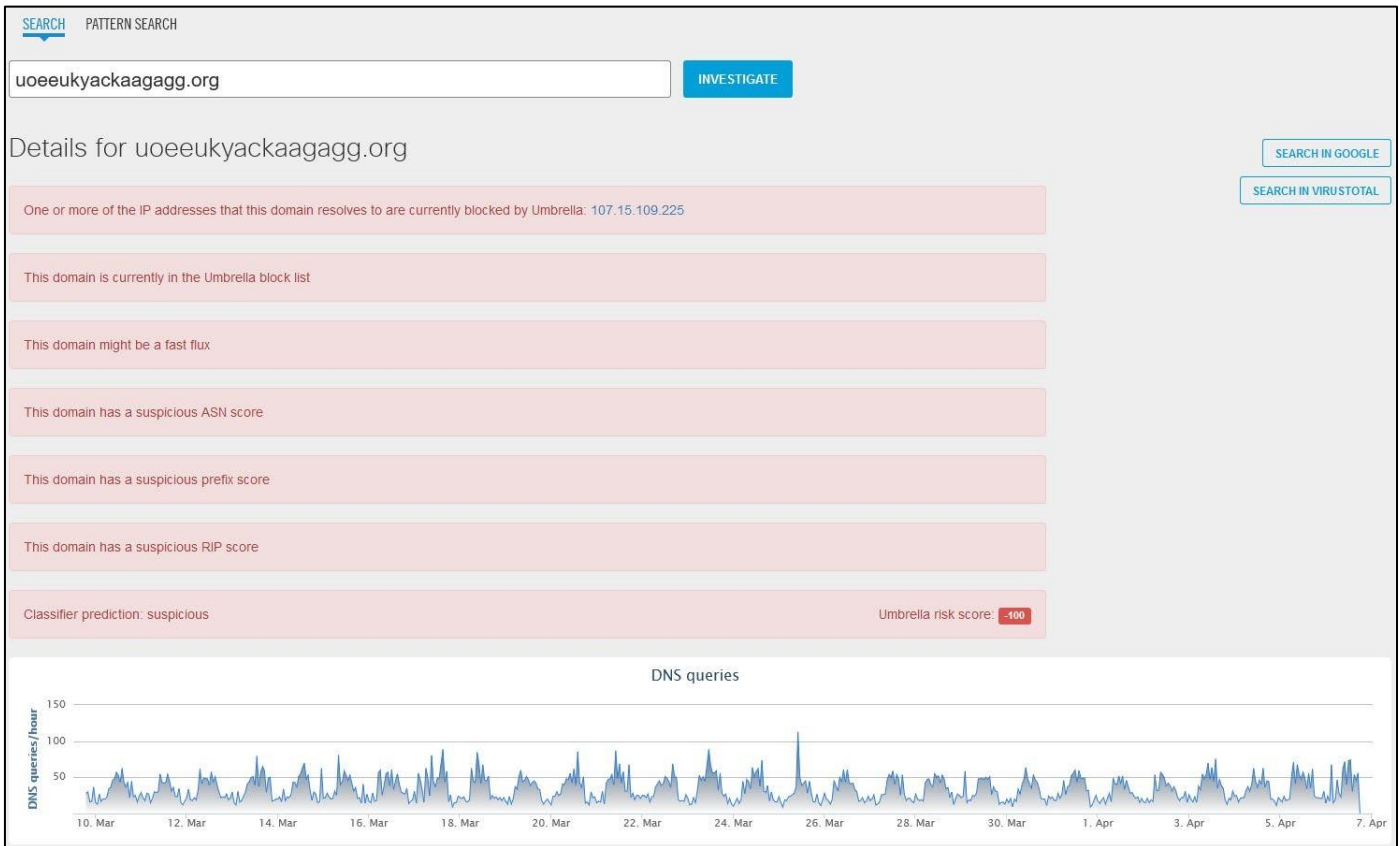
참고: 다른 방향으로 피벗하려면 조사의 링크를 클릭할 때 새 브라우저 탭에서 새 정보를 여십시오(클릭할 때 키보드의 Ctrl 클릭). 새 탭에서 열지 않으면 브라우저의 BACK 버튼을 사용하여 조사의 이전 위치로 돌아갈 수 있습니다.

단계

실습 1: 도메인에 대한 추가 정보 가져오기

이 실습은 옴브렐라에 의해 이미 차단된 도메인을 찾았다고 가정하는 것으로 시작되며, 여기서의 목표는 도메인이 차단된 이유, 차단된 기간 및 이 도메인을 다른 위협이나 다른 도메인에 연결하는 다른 데이터와의 상관 관계에 대해 자세히 알아보겠습니다.

1. Umbrella 대시보드의 기본 탐색에서 **Investigate** 를 클릭 클릭합니다. 이렇게 하면 새 브라우저 탭에서 Investigate 콘솔이 열립니다.
2. search (검색) 창에서 제공된 악성적인 목적지 중 하나를 입력한 다음, **INVESTIGATE** 를 클릭합니다.



일반 정보

1. 페이지 맨 위에 있는 Investigate 는 도메인의 보안 세부 정보가 포함된 주요 정보를 제공합니다.
2. 여기서 도메인이 현재 Umbrella 블록 목록에 있음을 확인할 수 있습니다. Umbrella 가 (지능을 기반으로 하거나 자동화된 통계 모델 중 하나에 의해 탐지된) 악의적인 것으로 판단했음을 의미하며, 현재 모든 Umbrella 고객은 도메인으로 이동하지 못하도록 보호받고 있습니다.
3. 또한 Umbrella 가 이 도메인이 확인되는 IP 주소도 차단하는 것을 볼 수 있습니다.

4. 도메인에 관련된 보안 기능 및 점수에 기반한 수학적 계산인 **Umbrella risk score** 를 기록하십시오(이 점수는 제품의 **Security Features** 영역에 설명됨).

Umbrella risk score 는 블록 목록에 나타나는 사이트에 대한 권한으로 간주되지 않습니다. 다시 말해, 차단되지 않은 낮은 점수를 가진 사이트나 더 높은 점수를 받은 사이트가 있을 수 있습니다. 사실, 이러한 시나리오는 상당히 흔하고 혼란으로 이어질 수 있습니다. 이러한 경우가 발생할 수 있는 예로는 이전에 합법적이었던 양호한 도메인이 해킹되어 멀웨어 서비스를 시작하는 경우를 들 수 있습니다. 해당 도메인의 DNS 에 대한 내용은 많이 변경되지 않았지만 현재 차단되고 있습니다.

또한 **Umbrella risk score** 가 실제로 조사의 주요 판매 지점이 아님을 유념할 필요가 있습니다. 우리는 이 점수가 다른 모든 점수들을 살펴보고 사이트의 양성 또는 악성 점수를 생성하는 알고리즘 계산을 나타내는 빠른 분석 이상일 의도가 없습니가(-100 과 매우 유사함 악성 및 +100 으로 양성일 가능성이 매우 높음) 점수는 도메인에 대한 보안 세부사항의 누적 집계로, 사이트에 추가 조사가 필요한지 여부를 신속하게 결정하는 데 도움이 되는 중요한 경고입니다.

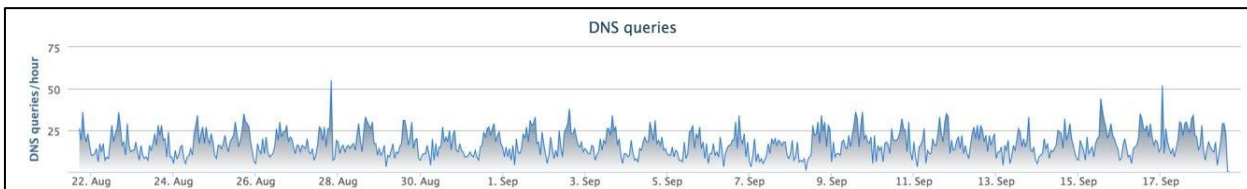
5. 추가 도메인을 볼 때 현재와 미래에 연구 중인 도메인에 대한 **Umbrella risk score** 를 기록하십시오.

NOTE: Descriptions of all other alerts can be found in the documentation.

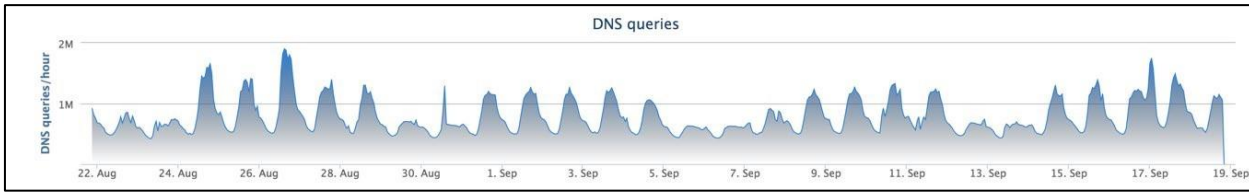
DNS 쿼리 그래프

다음으로, DNS 쿼리 그래프에 중점을 둡니다. 첫 번째로 살펴볼 수 있는 것은 스파이크(spikes) 또는 일반 패턴(regular patterns)에 대한 것입니다...

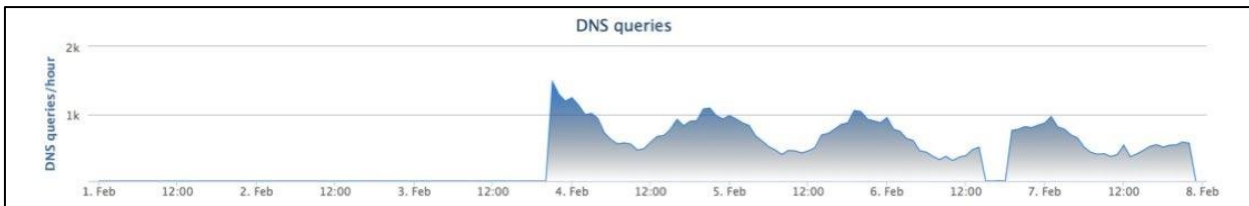
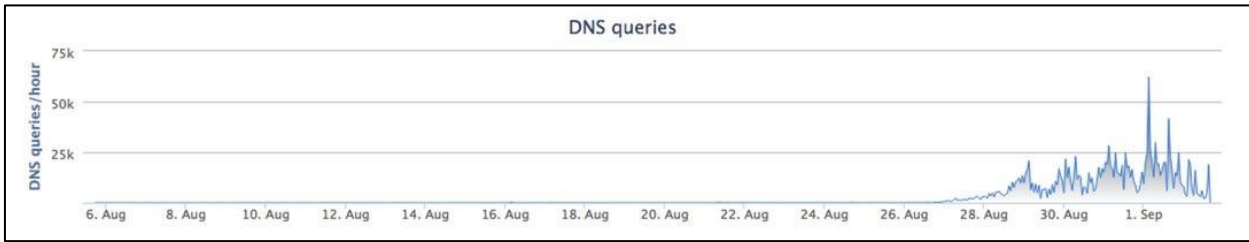
1. 아래 예제의 **DNS 쿼리** 그래프는 지난 30 일 동안 이 도메인에 대해 전체적으로 확인한 요청 수를 보여 주며, 위에서 마우스를 돌리면 매 시간마다 분류되기도 합니다.



2. 대부분의 인기 사이트는 공통 트래픽 흐름을 가지며 특정 시간에는 정점을 찍지만 일정 기간 동안 표준화된 상태로 유지됩니다.



3. 때때로 이와 같은 현상이 나타날 수 있습니다. 이전에 피싱 캠페인이 없었던 경우 새로운 캠페인(예: 피싱 캠페인) 갑자기 트래픽을 생성하기 시작합니다. 더 큰 스파이크 앞에 작은 스파이크가 보일 수도 있습니다. 공격자가 공격을 시작하기 전에 인프라를 테스트하는 시기를 나타낼 수 있습니다.



노트: 지난 며칠 동안 매우 적은 양의 트래픽을 보여주는 도메인을 조사할 때 왼쪽 축(DNS 시간당 쿼리)은 총 인터넷 트래픽에 대해 조정되며, 매우 적은 양의 트래픽은 조사 중인 도메인이 표적 공격 또는 APT의 일부가 될 수 있음을 나타낼 수 있음을 명심하십시오

WHOIS 데이터 기록

1. 다음으로, 도메인에 대한 **WHOIS** 기록 데이터를 살펴봅니다. WHOIS 레코드 데이터는 도메인을 등록한 사람, 등록된 위치, 등록자 연락처 정보(이름, 이메일 주소, 거리 주소, 전화/팩스 번호 등)에 대한 정보를 제공합니다. 최근에 등록된 경우 Windows(윈도우) 피싱 캠페인 또는 표적형 공격을 위해 도메인이 스팀업되었음을 나타낼 수 있습니다. **WHOIS** 정보는 상당히 쉽게 위조되거나 난독화 될 수 있습니다. 특히 기피 도메인 등록자를 사용하면 더욱 그렇습니다. 예를 들어, 여러분은 연예인 이름을 보거나 "나쁜 남자"와 같이 분명히 가짜 이름을 볼 수 있습니다. 거리 주소 옆에 "지도 보기" 옵션이 있습니다. 이 옵션은 Google 지도를 열고 올바른 주소인지 확인할 수 있습니다. Investigate 는 또한 **WHOIS** 의 역사적(**historical WHOIS**) 기록 데이터를 제공하여 시간이 지남에 따라 이루어진 변화를 보여줍니다. 따라서 WHOIS 정보를 의심스럽게 보는 것은 도메인이 잠재적으로 악의적인 목적으로 사용되고 있음을 나타내는 주요 지표일 수 있습니다.

WHOIS Record Data

Registrar Name: Todaynic.com, Inc. IANAID: 697 Last retrieved March 13, 2017 [GET LATEST](#)

Created: April 24, 2016 Updated: June 24, 2016 Expires: April 24, 2017 [Raw data](#)

Email Address	Associated Domains	Email Type	Last Observed
cs@now.cn	Greater than 500 Total - At least 500 malicious	Administrative, Registrant, Technical	Current

Nameserver	Associated Domains	Last Observed
ns4.lortejbr.at	2 Total - 2 malicious	Current
ns3.lortejbr.at	2 Total - 2 malicious	Current
ns2.lortejbr.at	2 Total - 2 malicious	Current
ns1.lortejbr.at	2 Total - 2 malicious	Current

[Show more WHOIS data](#)

노트: 종종 신흥 도메인은 WHOIS 기록에 정보가 추가되지 않습니다. 그러니 주의하십시오. Investigate 인터페이스는 "죄송합니다. 도메인에 대한 WHOIS 정보를 로드할 수 없습니다.(\"Sorry, couldn't load WHOIS information for this domain.\")"라고 말할 수 있습니다. WHOIS 정보가 사용 가능한 세부 정보가 없는 상태로 단순히 활성 상태로 설정된 경우에도 데이터를 사용할 수 없습니다.

- 도메인을 등록하는 데 사용되는 전자 메일 주소와 관련 이름 서버를 포함하여 **WHOIS** 레코드 데이터의 여러 데이터 지점을 피벗할 수 있습니다. 이러한 데이터 지점을 클릭하고 피벗하면 관련 인프라를 찾을 수 있습니다. 예를 들어 전자 메일 주소에 대해 연결된 도메인을 중심으로 동일한 전자 메일 주소에 등록된 다른 모든 도메인을 볼 수 있으며 다른 도메인이 악의적인지 확인할 수도 있습니다.
- 위 예(uoeeukyackaagg[.]org)에서 **WHOIS** 레코드 데이터는 동일한 이메일 주소를 보여줍니다. (cs@now.cn)은 악의적인 것으로 간주되는 수백 개의 다른 도메인을 등록하는 데 사용되었습니다.
- 전자 메일 주소를 클릭하고 조사의 전자 메일 주소 보기로 피벗하여 등록된 다른 도메인을 표시합니다. 조사 결과 이러한 도메인이 맬웨어, 피싱 및 봇넷 활동과 연관되어 있음을 알 수 있습니다.

Domains Associated with cs@now.cn

Domain Name	Security Categories	Content Categories	Last Observed
advertisingdb.net	Botnet, Malware		Current
american-express-cer4.com	Malware, Phishing		Current
american-express-cldq.com	Malware, Phishing		Current
american-express-cwe1.com	Malware, Phishing		Current
com-asp-page-48343-58451-accesd-desjardins.com	Botnet, Malware		Current

- 마찬가지로, nameserver 의 **Associated Domains** 을 클릭하여 피벗할 수 있습니다. 그러면 동일한 nameserver 에서 호스팅되는 다른 도메인의 보기로 이동할 수 있습니다. 이 예에서는 조사 중인 도메인을 제외하고 하나의 추가 관련 도메인에 대해 몇 가지 변형이 있습니다.

Nameserver	Associated Domains
ns4.lortejbr.at	2 Total - 2 malicious
ns3.lortejbr.at	2 Total - 2 malicious
ns2.lortejbr.at	2 Total - 2 malicious
ns1.lortejbr.at	2 Total - 2 malicious

6. 동일한 공격자 인프라와 관련된 추가 도메인 또는 IP 주소를 찾으려면 네임스 서버 값 중 하나를 누르십시오.

관련 샘플

Associated Samples Cisco AMP 및 Threat Grid 에서 알려진 파일 샘플 목록과 SHA256 지문 및 모든 AV 검색 결과를 제공합니다. 이 부분은 나중에 자세히 보실 겁니다.

Associated Samples		POWERED BY CISCO AMP THREAT GRID
Threat Score	SHA256 Signature	AV Result
95	008b715558f08785f62ff03080a2b80d4583b02ccd802e9aef4cc35e49ab8a45	

1-1 of 1 < >

도메인 태깅

Domain Tagging 지정은 블록 목록에서 도메인이 엠브렐라로 태그 지정되는 범주를 보여 줍니다(맬웨어, 피싱, 드라이브 바이 다운로드 등). 또한 사용 가능한 경우 나열된 기간과 함께 악성 코드가 포함된 특정 URL 이 나타납니다. 이전에 분류된 기록 정보도 표시됩니다.

Period	Category	URL
Aug 21, 2016 - Current	Botnet	
Aug 2, 2016 - Current	Botnet	
Jun 27, 2016 - Current	Botnet	
May 10, 2016 - Current	Malware	
Apr 25, 2016 - Current	Botnet	

노트: 도메인 태그 섹션에서 도메인과 관련된 현재 및 과거 분류 태그를 모두 확인할 수 있음

기능

1. 기능 영역에는 체크아웃할 수 있는 여러 가지 보안 기능이 포함되어 있습니다. 이 모든 내용은 현재 연구소에서 다루지는 않겠지만 직접 검토하여 각자가 제공하는 정보에 대한 설명은 Investigate 문서를 참조하십시오.

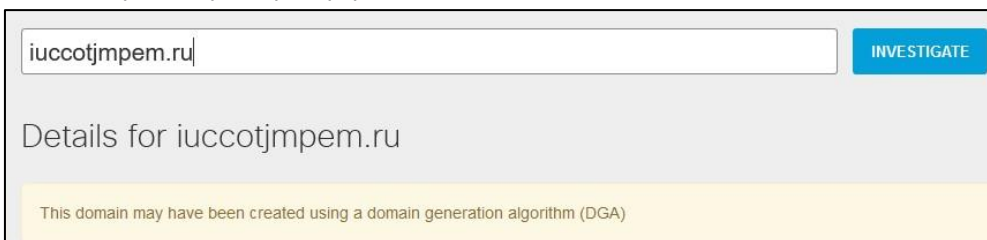
2. 도메인에 대한 **TTL**(Time-to-Live)을 기록해 두십시오. 표준 **TTL** 은 다음과 같이 보일 수 있습니다:

Features	
TTLs min	300
TTLs max	300
TTLs mean	300
TTLs median	300
TTLs standard deviation	0.00

3. **TTL** 이 낮은 도메인에는 IP 변경 사항이 있을 수 있습니다. **TTL** 은 일반적으로 한 IP 에서 다른 IP 로 도메인을 마이그레이션하는 것 보다 먼저 낮아졌습니다. 그러나 도메인이 악의적인 콘텐츠를 호스팅하는 여러 IP 주소를 마스킹 하는 데 사용 되는 경우에도 감소 합니다.
- TTLs** 가 매우 낮으면 경고 메시지가 표시 됩니다. 이 경우 해당 도메인에 대한 **TTLs** 가 매우 적거나 0 입니다. 또한이 도메인을 호스팅하는 IP 주소의 국가 코드 인 국가 코드 수는 매우 높습니다. 대부분의 합법적인 도메인은 2 또는 3 보다 드물게 발생 합니다. "Cnn.com"와 같은 도메인은 1 (미국) 뿐입니다.
4. <https://investigate.opendns.com/domain-view/name/goloduha.info/view> 에서 확인하십시오.

DGA Detection

1. **DGA Detection** 은 도메인이 자동 봇넷의 일부로 등록 될 수 있는지 여부를 밝혀냅니다. **DGA** (**Domain Generation Algorithm**)는 봇넷 공격의 일부로 도메인 이름을 임의로 생성하는 데 사용됩니다. 정적 차단 목록보다 앞서 유지하기 위해 해커가 임의로 생성 한 이름을 사용하며 이를 기능을 방지합니다. DGA 점수가 -25 이하인 경우 Investigate 상단에 경고가 표시됩니다.



2. 이 알림이 표시되면 **DGA Detection** 영역으로 스크롤해야 합니다. 여기서는 점수에 기여하는 도메인 이름 자체의 구조에 대한 다른 계산인 **Perplexity** 및 **Entropy** 와 함께 총 **DGA Score** 를 볼 수 있습니다. 일부 합법적인 대상 및 일부 **DGA** 에 대한 결과를 확인합니다. 몇 가지 예를 들어 보겠습니다.

- iuccotjmpem[.]ru
- greystoneexpress[.]com

- sso.anbtr[.]com

DGA Detection	
DGA score (rescaled)	-30.240
Perplexity score (rescaled)	-0.414
Entropy	2.322

Domain Generation Algorithm -
This score is generated based on the likeliness of the domain being an actual domain, as opposed to being a malicious/fake domain. This score ranges from -100 to 0.

노트: 세 가지 다른 점수 유형 위에 마우스를 올려 놓으면 이 점수가 무엇을 의미하는지 알 수 있습니다.

노트: 최근 "라이브 DGA 예측"이라는 새로운 엠브렐라 통계 모델이 추가되어 다양한 멀웨어 제품군의 DGA에 대한 역 엔지니어링을 자동화하고 Live DGA Detection 모델을 넘어섰습니다. 이 모델과 기타 다양한 엠브렐라 통계 모델은 현재 조사 콘솔 또는 API에 명시적으로 노출되어 있지 않습니다.

IP 주소

1. 이 섹션에는 도메인이 확인 되는 **IP 주소** 및 도메인에 대한 네임서버의 **IP 주소**도 나열 됩니다. 노트: 네임서버에 대한 데이터는 동일한 도메인에 대한 **WHOIS** 정보와 다른 소스에서 가져온 것입니다. 이러한 네임서버는 엠브렐라 DNS 확인자에서 정적 **WHOIS** 기록에 나열 된 것이 아니라 도메인에 대한 **권위적인** 부여 받는 것으로 확인합니다.
2. 페이지 상단에는 도메인이 잠재적으로 "**fast flux**" 도메인이라는 경고도 있을 수 있습니다. **Fast flux** 는 공격자가 지속적으로 변화하는 많은 IP 주소 뒤에 있는 피싱 및 악성 전달 사이트를 숨기는 데 사용 되는 DNS 기술입니다. 도메인이 종종 변화한다면, 이것은 도메인이 **fast fluxing** 고 있다는 매우 좋은 표시입니다.

INVESTIGATE

Details for uoeekyackaagg.org

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: [107.15.109.225](#)

This domain is currently in the Umbrella block list

This domain might be a fast flux

3. 조사에서는, **fast flux** 주행 후보의 좋은 예이기도 한 goloduha[.]info, 그리고 다음 몇 가지 속성도 살펴봅니다.
4. 이 경고가 표시되면 **IP 주소** 영역으로 스크롤하여 이 도메인이 이 보안 경고의 대상인 이유를 확인하십시오.

5. IP 주소 섹션에서 **IP 주소 및 네임 서버** 모두에 대한 매우 흥미로운 패턴을 볼 수 있습니다. 그러나 먼저, 기능 섹션에서 조사 섹션에서, 이 도메인은 작성 시점에 총 1069 개의 IP 주소로 확인됨("RIP"는 서버 IP 주소 수를 표시함)

Prefixes count	634
RIPs	1,069
RIPs diversity	0.594

노트: 이전과 마찬가지로, 다른 점수 유형 위에 마우스 커서를 올려 놓으면 이러한 점수가 의 하는 내용에 대한 설명이 표시됩니다.

6. 다음은 IP 주소 섹션으로 스크롤하여 이 도메인이 매일 변경하기로 결정한 IP 주소를 확인하십시오. 정의상, 이것은 **fast flux** 도메인입니다!

IP Addresses		
First seen	Last seen	IPs
4/7/17	4/7/17	1.115.4.201 (TTL: 0) 1.237.84.9 (TTL: 0) 1.280.224.111 (TTL: 0) 112.181.205.160 (TTL: 0) 112.162.30.136 (TTL: 0) 112.163.6.174 (TTL: 0) 112.183.73.12 (TTL: 0) 112.183.9.96 (TTL: 0) 112.164.218.111 (TTL: 0) 112.170.198.233 (TTL: 0) 112.171.80.132 (TTL: 0) 112.172.174.229 (TTL: 0) 112.173.217.191 (TTL: 0) 112.173.76.18 (TTL: 0) 112.164.41.254 (TTL: 0) 112.165.217.205 (TTL: 0) 112.185.217.57 (TTL: 0) 112.187.168.37 (TTL: 0) 114.201.238.162 (TTL: 0) 114.204.241.202 (TTL: 0) 114.205.174.153 (TTL: 0) 115.21.176.210 (TTL: 0) 115.22.203.173 (TTL: 0) 118.33.243.214 (TTL: 0) 118.33.25.37 (TTL: 0) 118.33.84.167 (TTL: 0) 118.34.133.189 (TTL: 0) 118.34.80.158 (TTL: 0) 118.38.55.121 (TTL: 0) 118.37.160.105 (TTL: 0) 118.37.239.69 (TTL: 0) 118.40.85.171 (TTL: 0) 118.45.245.138 (TTL: 0) 119.194.211.71 (TTL: 0) 119.195.200.235 (TTL: 0) 119.195.221.13 (TTL: 0) 119.195.68.109 (TTL: 0) 119.198.174.198 (TTL: 0) 119.198.83.115 (TTL: 0) 121.130.161.176 (TTL: 0) 121.133.7.239 (TTL: 0) 121.134.17.145 (TTL: 0) 121.135.129.103 (TTL: 0) 121.136.205.252 (TTL: 0) 121.137.215.233 (TTL: 0) 121.139.68.195 (TTL: 0) 121.145.152.88 (TTL: 0) 121.145.172.87 (TTL: 0) 121.145.71.198 (TTL: 0) 121.152.195.60 (TTL: 0) 121.163.180.223 (TTL: 0) 121.164.12.175 (TTL: 0) 121.164.209.138 (TTL: 0) 121.165.134.214 (TTL: 0) 121.165.150.198 (TTL: 0) 121.165.150.238 (TTL: 0) 121.165.219.162 (TTL: 0) 121.166.61.32 (TTL: 0) 121.172.19.177 (TTL: 0) 121.174.214.225 (TTL: 0) 121.182.185.5 (TTL: 0) 121.185.151.82 (TTL: 0) 125.128.148.251 (TTL: 0) 125.136.224.147 (TTL: 0) 125.139.74.130 (TTL: 0) 125.142.49.182 (TTL: 0) 125.191.183.148 (TTL: 0) 14.38.15.94 (TTL: 0) 14.40.39.233 (TTL: 0) 14.40.71.119 (TTL: 0) 14.42.208.123 (TTL: 0) 14.43.205.210 (TTL: 0) 14.43.221.219 (TTL: 0) 14.44.67.167 (TTL: 0) 14.52.219.76 (TTL: 0) 158.89.188.40 (TTL: 86400) 175.112.208.196 (TTL: 0) 175.193.135.72 (TTL: 0) 175.194.56.221 (TTL: 0) 175.197.48.191 (TTL: 0) 175.198.81.98 (TTL: 0) 175.199.218.147 (TTL: 0) 175.208.183.6 (TTL: 0) 175.211.223.141 (TTL: 0) 175.215.243.103 (TTL: 0) 176.37.42.160 (TTL: 0) 177.84.96.15 (TTL: 0) 183.100.38.161 (TTL: 0) 183.100.139.207 (TTL: 0) 183.103.14.14 (TTL: 0) 183.107.155.180 (TTL: 0) 183.109.115.110 (TTL: 0) 184.146.199.200 (TTL: 0) 201.231.17.47 (TTL: 0) 203.232.37.70 (TTL: 0) 203.237.156.50 (TTL: 0) 210.104.172.77 (TTL: 0) 210.176.79.99 (TTL: 0) 210.204.122.2 (TTL: 0) 210.186.229.196 (TTL: 0) 211.185.121.60 (TTL: 0) 211.184.231.161 (TTL: 0) 211.197.64.24 (TTL: 0) 211.198.35.65 (TTL: 0) 211.199.80.201 (TTL: 0) 211.205.162.43 (TTL: 0) 211.205.93.145 (TTL: 0) 211.207.16.43 (TTL: 0) 211.212.151.114 (TTL: 0) 211.216.105.126 (TTL: 0) 211.217.85.131 (TTL: 0) 211.223.12.205 (TTL: 0) 211.227.20.11 (TTL: 0) 211.230.192.236 (TTL: 0) 211.230.77.7 (TTL: 0) 211.244.32.63 (TTL: 0) 211.245.63.107 (TTL: 0) 211.246.218.229 (TTL: 0) 211.96.1.210 (TTL: 0) 212.73.71.4 (TTL: 0) 218.148.17.227 (TTL: 0) 218.151.38.243 (TTL: 0) 218.48.109.253 (TTL: 0) 219.254.170.41 (TTL: 0) 220.116.181.23 (TTL: 0) 220.126.60.92 (TTL: 0) 220.77.190.120 (TTL: 0) 220.79.230.45 (TTL: 0) 220.84.103.240 (TTL: 0) 220.87.217.179 (TTL: 0) 221.142.85.54 (TTL: 0) 221.150.141.147 (TTL: 0) 221.150.197.223 (TTL: 0) 221.155.247.143 (TTL: 0) 221.167.224.230 (TTL: 0) 222.109.190.157 (TTL: 0) 222.110.236.115 (TTL: 0) 222.113.122.59 (TTL: 0) 222.113.82.10 (TTL: 0) 222.118.92.120 (TTL: 0) 222.120.224.109 (TTL: 0) 222.97.165.121 (TTL: 0) 222.97.57.52 (TTL: 0) 222.99.18.39 (TTL: 0) 222.99.233.109 (TTL: 0) 24.218.111.139 (TTL: 0) 24.83.199.9 (TTL: 0) 240.0.0.0 (TTL: 0) 36.66.205.185 (TTL: 0) 41.207.10.68 (TTL: 0) 46.120.217.49 (TTL: 0) 58.125.86.42 (TTL: 0) 58.128.24.81 (TTL: 0) 58.191.95.39 (TTL: 0) 59.1140.130 (TTL: 0) 59.12.157.108 (TTL: 0) 59.12.24.20 (TTL: 0) 59.125.106.188 (TTL: 0) 59.18.144.123 (TTL: 0) 59.19.153.172 (TTL: 0) 59.23.1.118 (TTL: 0) 59.30.30.156 (TTL: 0) 59.94.96.196 (TTL: 0) 61.103.74.187 (TTL: 0) 61.103.74.188 (TTL: 0) 61.182.117.124 (TTL: 0) 61.182.206.92 (TTL: 0) 61.73.224.110 (TTL: 0) 61.76.211.90 (TTL: 0) 61.78.167.48 (TTL: 0) 69.143.45.60 (TTL: 0) 77.123.71.174 (TTL: 0) 78.58.41.207 (TTL: 0) 79.170.185.185 (TTL: 0) 89.37.116.132 (TTL: 0) 93.126.72.87 (TTL: 0) 95.105.10.192 (TTL: 0)
4/6/17	4/6/17	1.115.22.35 (TTL: 0) 1.225.246.145 (TTL: 0) 1.232.89.197 (TTL: 0) 1.234.106.227 (TTL: 0) 1.237.84.9 (TTL: 0) 1.250.224.111 (TTL: 0) 103.70.45.146 (TTL: 0) 109.162.8.255 (TTL: 0) 112.161.205.160 (TTL: 0) 112.162.30.136 (TTL: 0) 112.163.6.174 (TTL: 0) 112.163.73.12 (TTL: 0) 112.163.9.96 (TTL: 0) 112.164.218.111 (TTL: 0) 112.170.198.233 (TTL: 0) 112.171.80.132 (TTL: 0) 112.172.174.229 (TTL: 0) 112.173.217.191 (TTL: 0) 112.173.76.18 (TTL: 0) 112.164.41.254 (TTL: 0) 112.165.217.205 (TTL: 0) 112.185.217.57 (TTL: 0) 112.187.168.37 (TTL: 0) 114.201.238.162 (TTL: 0) 114.204.241.202 (TTL: 0) 114.205.174.153 (TTL: 0) 115.21.176.210 (TTL: 0) 115.22.203.173 (TTL: 0) 118.33.243.214 (TTL: 0) 118.33.25.37 (TTL: 0) 118.33.84.167 (TTL: 0) 118.34.133.189 (TTL: 0) 118.34.80.158 (TTL: 0) 118.38.55.121 (TTL: 0) 118.37.160.105 (TTL: 0) 118.37.239.69 (TTL: 0) 118.40.85.171 (TTL: 0) 118.45.245.138 (TTL: 0) 119.194.211.71 (TTL: 0) 119.195.200.235 (TTL: 0) 119.195.221.13 (TTL: 0) 119.195.68.109 (TTL: 0) 119.198.174.198 (TTL: 0) 119.198.83.115 (TTL: 0) 121.130.161.176 (TTL: 0) 121.133.7.239 (TTL: 0) 121.134.17.145 (TTL: 0) 121.135.129.103 (TTL: 0) 121.136.205.252 (TTL: 0) 121.137.215.233 (TTL: 0) 121.139.68.195 (TTL: 0) 121.145.152.88 (TTL: 0) 121.145.172.87 (TTL: 0) 121.145.71.198 (TTL: 0) 121.152.195.60 (TTL: 0) 121.163.180.223 (TTL: 0) 121.164.12.175 (TTL: 0) 121.164.209.138 (TTL: 0) 121.165.134.214 (TTL: 0) 121.165.150.198 (TTL: 0) 121.165.150.238 (TTL: 0) 121.165.219.162 (TTL: 0) 121.166.61.32 (TTL: 0) 121.172.19.177 (TTL: 0) 121.174.214.225 (TTL: 0) 121.182.185.5 (TTL: 0) 121.185.151.82 (TTL: 0) 125.128.148.251 (TTL: 0) 125.136.224.147 (TTL: 0) 125.139.74.130 (TTL: 0) 125.142.49.182 (TTL: 0) 125.191.183.148 (TTL: 0) 14.38.15.94 (TTL: 0) 14.40.39.233 (TTL: 0) 14.40.71.119 (TTL: 0) 14.42.208.123 (TTL: 0) 14.43.205.210 (TTL: 0) 14.43.221.219 (TTL: 0) 14.44.67.167 (TTL: 0) 14.52.219.76 (TTL: 0) 158.89.188.40 (TTL: 86400) 175.112.208.196 (TTL: 0) 175.193.135.72 (TTL: 0) 175.194.56.221 (TTL: 0) 175.197.48.191 (TTL: 0) 175.198.81.98 (TTL: 0) 175.199.218.147 (TTL: 0) 175.208.183.6 (TTL: 0) 175.211.223.141 (TTL: 0) 175.215.243.103 (TTL: 0) 176.37.42.160 (TTL: 0) 177.84.96.15 (TTL: 0) 183.100.38.161 (TTL: 0) 183.100.139.207 (TTL: 0) 183.103.14.14 (TTL: 0) 183.107.155.180 (TTL: 0) 183.109.115.110 (TTL: 0) 184.146.199.200 (TTL: 0) 201.231.17.47 (TTL: 0) 203.232.37.70 (TTL: 0) 203.237.156.50 (TTL: 0) 210.104.172.77 (TTL: 0) 210.176.79.99 (TTL: 0) 210.204.122.2 (TTL: 0) 210.186.229.196 (TTL: 0) 211.185.121.60 (TTL: 0) 211.184.231.161 (TTL: 0) 211.197.64.24 (TTL: 0) 211.198.35.65 (TTL: 0) 211.199.80.201 (TTL: 0) 211.205.162.43 (TTL: 0) 211.205.93.145 (TTL: 0) 211.207.16.43 (TTL: 0) 211.212.151.114 (TTL: 0) 211.216.105.126 (TTL: 0) 211.217.85.131 (TTL: 0) 211.223.12.205 (TTL: 0) 211.227.20.11 (TTL: 0) 211.230.192.236 (TTL: 0) 211.230.77.7 (TTL: 0) 211.244.32.63 (TTL: 0) 211.245.63.107 (TTL: 0) 211.246.218.229 (TTL: 0) 211.96.1.210 (TTL: 0) 212.73.71.4 (TTL: 0) 218.148.17.227 (TTL: 0) 218.151.38.243 (TTL: 0) 218.48.109.253 (TTL: 0) 219.254.170.41 (TTL: 0) 220.116.181.23 (TTL: 0) 220.126.60.92 (TTL: 0) 220.77.190.120 (TTL: 0) 220.79.230.45 (TTL: 0) 220.84.103.240 (TTL: 0) 220.87.217.179 (TTL: 0) 221.142.85.54 (TTL: 0) 221.150.141.147 (TTL: 0) 221.150.197.223 (TTL: 0) 221.155.247.143 (TTL: 0) 221.167.224.230 (TTL: 0) 222.109.190.157 (TTL: 0) 222.110.236.115 (TTL: 0) 222.113.122.59 (TTL: 0) 222.113.82.10 (TTL: 0) 222.118.92.120 (TTL: 0) 222.120.224.109 (TTL: 0) 222.97.165.121 (TTL: 0) 222.97.57.52 (TTL: 0) 222.99.18.39 (TTL: 0) 222.99.233.109 (TTL: 0) 24.218.111.139 (TTL: 0) 24.83.199.9 (TTL: 0) 240.0.0.0 (TTL: 0) 36.66.205.185 (TTL: 0) 41.207.10.68 (TTL: 0) 46.120.217.49 (TTL: 0) 58.125.86.42 (TTL: 0) 58.128.24.81 (TTL: 0) 58.191.95.39 (TTL: 0) 59.1140.130 (TTL: 0) 59.12.157.108 (TTL: 0) 59.12.24.20 (TTL: 0) 59.125.106.188 (TTL: 0) 59.18.144.123 (TTL: 0) 59.19.153.172 (TTL: 0) 59.23.1.118 (TTL: 0) 59.30.30.156 (TTL: 0) 59.94.96.196 (TTL: 0) 61.103.74.187 (TTL: 0) 61.103.74.188 (TTL: 0) 61.182.117.124 (TTL: 0) 61.182.206.92 (TTL: 0) 61.73.224.110 (TTL: 0) 61.76.211.90 (TTL: 0) 61.78.167.48 (TTL: 0) 69.143.45.60 (TTL: 0) 77.123.71.174 (TTL: 0) 78.58.41.207 (TTL: 0) 79.170.185.185 (TTL: 0) 89.37.116.132 (TTL: 0) 93.126.72.87 (TTL: 0) 95.105.10.192 (TTL: 0)
4/5/17	4/5/17	1.115.22.35 (TTL: 0) 1.225.246.145 (TTL: 0) 1.232.89.197 (TTL: 0) 1.234.106.227 (TTL: 0) 1.237.84.9 (TTL: 0) 1.250.224.111 (TTL: 0) 103.70.45.146 (TTL: 0) 109.162.8.255 (TTL: 0) 112.161.205.160 (TTL: 0) 112.162.30.136 (TTL: 0) 112.163.6.174 (TTL: 0) 112.163.73.12 (TTL: 0) 112.163.9.96 (TTL: 0) 112.164.218.111 (TTL: 0) 112.170.198.233 (TTL: 0) 112.171.80.132 (TTL: 0) 112.172.174.229 (TTL: 0) 112.173.217.191 (TTL: 0) 112.173.76.18 (TTL: 0) 112.164.41.254 (TTL: 0) 112.165.217.205 (TTL: 0) 112.185.217.57 (TTL: 0) 112.187.168.37 (TTL: 0) 114.201.238.162 (TTL: 0) 114.204.241.202 (TTL: 0) 114.205.174.153 (TTL: 0) 115.21.176.210 (TTL: 0) 115.22.203.173 (TTL: 0) 118.33.243.214 (TTL: 0) 118.33.25.37 (TTL: 0) 118.33.84.167 (TTL: 0) 118.34.133.189 (TTL: 0) 118.34.80.158 (TTL: 0) 118.38.55.121 (TTL: 0) 118.37.160.105 (TTL: 0) 118.37.239.69 (TTL: 0) 118.40.85.171 (TTL: 0) 118.45.245.138 (TTL: 0) 119.194.211.71 (TTL: 0) 119.195.200.235 (TTL: 0) 119.195.221.13 (TTL: 0) 119.195.68.109 (TTL: 0) 119.198.174.198 (TTL: 0) 119.198.83.115 (TTL: 0) 121.130.161.176 (TTL: 0) 121.133.7.239 (TTL: 0) 121.134.17.145 (TTL: 0) 121.135.129.103 (TTL: 0) 121.136.205.252 (TTL: 0) 121.137.215.233 (TTL: 0) 121.139.68.195 (TTL: 0) 121.145.152.88 (TTL: 0) 121.145.172.87 (TTL: 0) 121.145.71.198 (TTL: 0) 121.152.195.60 (TTL: 0) 121.163.180.223 (TTL: 0) 121.164.12.175 (TTL: 0) 121.164.209.138 (TTL: 0) 121.165.134.214 (TTL: 0) 121.165.150.198 (TTL: 0) 121.165.150.238 (TTL: 0) 121.165.219.162 (TTL: 0) 121.166.61.32 (TTL: 0) 121.172.19.177 (TTL: 0) 121.174.214.225 (TTL: 0) 121.182.185.5 (TTL: 0) 121.185.151.82 (TTL: 0) 125.128.148.251 (TTL: 0) 125.136.224.147 (TTL: 0) 125.139.74.130 (TTL: 0) 125.142.49.182 (TTL: 0) 125.191.183.148 (TTL: 0) 14.38.15.94 (TTL: 0) 14.40.39.233 (TTL: 0) 14.40.71.119 (TTL: 0) 14.42.208.123 (TTL: 0) 14.43.205.210 (TTL: 0) 14.43.221.219 (TTL: 0) 14.44.67.167 (TTL: 0) 14.52.219.76 (TTL: 0) 158.89.188.40 (TTL: 86400) 175.112.208.196 (TTL: 0) 175.193.135.72 (TTL: 0) 175.194.56.221 (TTL: 0) 175.197.48.191 (TTL: 0) 175.198.81.98 (TTL: 0) 175.199.218.147 (TTL: 0) 175.208.183.6 (TTL: 0) 175.211.223.141 (TTL: 0) 175.215.243.103 (TTL: 0) 176.37.42.160 (TTL: 0) 177.84.96.15 (TTL: 0) 183.100.38.161 (TTL: 0) 183.100.139.207 (TTL: 0) 183.103.14.14 (TTL: 0) 183.107.155.180 (TTL: 0) 183.109.115.110 (TTL: 0) 184.146.199.200 (TTL: 0) 201.231.17.47 (TTL: 0) 203.232.37.70 (TTL: 0) 203.237.156.50 (TTL: 0) 210.104.172.77 (TTL: 0) 210.176.79.99 (TTL: 0) 210.204.122.2 (TTL: 0) 210.186.229.196 (TTL: 0) 211.185.121.60 (TTL: 0) 211.184.231.161 (TTL: 0) 211.197.64.24 (TTL: 0) 211.198.35.65 (TTL: 0) 211.199.80.201 (TTL: 0) 211.205.162.43 (TTL: 0) 211.205.93.145 (TTL: 0) 211.207.16.43 (TTL: 0) 211.212.151.114 (TTL: 0) 211.216.105.126 (TTL: 0) 211.217.85.131 (TTL: 0) 211.223.12.205 (TTL: 0) 211.227.20.11 (TTL: 0) 211.230.192.236 (TTL: 0) 211.230.77.7 (TTL: 0) 211.244.32.63 (TTL: 0) 211.245.63.107 (TTL: 0) 211.246.218.229 (TTL: 0) 211.96.1.210 (TTL: 0) 212.73.71.4 (TTL: 0) 218.148.17.227 (TTL: 0) 218.151.38.243 (TTL: 0) 218.48.109.253 (TTL: 0) 219.254.170.41 (TTL: 0) 220.116.181.23 (TTL: 0) 220.126.60.92 (TTL: 0) 220.77.190.120 (TTL: 0) 220.79.230.45 (TTL: 0) 220.84.103.240 (TTL: 0) 220.87.217.179 (TTL: 0) 221.142.85.54 (TTL: 0) 221.150.141.147 (TTL: 0) 221.150.197.223 (TTL: 0) 221.155.247.143 (TTL: 0) 221.167.224.230 (TTL: 0) 222.109.190.157 (TTL: 0) 222.110.236.115 (TTL: 0) 222.113.122.59 (TTL: 0) 222.113.82.10 (TTL: 0) 222.118.92.120 (TTL: 0) 222.120.224.109 (TTL: 0) 222.97.165.121 (TTL: 0) 222.97.57.52 (TTL: 0) 222.99.18.39 (TTL: 0) 222.99.233.109 (TTL: 0) 24.218.111.139 (TTL: 0) 24.83.199.9 (TTL: 0) 240.0.0.0 (TTL: 0) 36.66.205.185 (TTL: 0) 41.207.10.68 (TTL: 0) 46.120.217.49 (TTL: 0) 58.125.86.42 (TTL: 0) 58.128.24.81 (TTL: 0) 58.191.95.39 (TTL: 0) 59.1140.130 (TTL: 0) 59.12.157.108 (TTL: 0) 59.12.24.20 (TTL: 0) 59.125.106.188 (TTL: 0) 59.18.144.123 (TTL: 0) 59.19.153.172 (TTL: 0) 59.23.1.118 (TTL: 0) 59.30.30.156 (TTL: 0) 59.94.96.196 (TTL: 0) 61.103.74.187 (TTL: 0) 61.103.74.188 (TTL: 0) 61.182.117.124 (TTL: 0) 61.182.206.92 (TTL: 0) 61.73.224.110 (TTL: 0) 61.76.211.90 (TTL: 0) 61.78.167.48 (TTL: 0) 69.143.45.60 (TTL: 0) 77.123.71.174 (TTL: 0) 78.58.41.207 (TTL: 0) 79.170.185.185 (TTL: 0) 89.37.116.132 (TTL: 0) 93.126.72.87 (TTL: 0) 95.105.10.192 (TTL: 0)
4/5/17	4/5/17	1.234.106.2

ASNs	AS 37903 AS 9318 AS 4766 AS 17858 AS 16276 AS 39608 AS 262582 AS 21261 AS 10481 AS 17974 AS 29571 AS 9116 AS 17511 AS 3462 AS 9829 AS 9457 AS 4837 AS 25229 AS 8 AS 15895 AS 45899 AS 17803 AS 2614 AS 2607 AS 17451 AS 55577 AS 60581 AS 59340 AS 8402 AS 44814 AS 43554 AS 39824 AS 11426 AS 20001 AS 12849 AS 15683 AS 8708 AS 24309 AS 41937 AS 9762 AS 9299 AS 17506 AS 9845 AS 38712 AS 13188 AS 9198 AS 8452 AS 56347 AS 36992 AS 11427 AS 33991 AS 43561 AS 17676 AS 27927 AS 4760 AS 36947 AS 48331 AS 31252 AS 48475 AS 7672 AS 45543 AS 17917 AS 38841 AS 50751 AS 16223 AS 9394 AS 55740 AS 198642 AS 9924 AS 9976 AS 38661 AS 38669 AS 1938 AS 9304 AS 45595 AS 8346 AS 25086 AS 23772 AS 56040 AS 9319 AS 20910 AS 2119 AS 44728 AS 10036 AS 16010 AS 35104 AS 4713 AS 47800 AS 30779 AS 56497 AS 29314 AS 8376
ASNs count	151

Name Servers

이 도메인과 연결된 네임 서버도 변경됩니다. **WHOIS** 레코드 데이터에는 소수의 이름 서버만 표시되었지만, **Umbrella** 데이터는 **Name server**의 **IP Address**가 자주 (매일) 변경되는 것을 보여줍니다.

Name Servers		
Name server	Last seen	TTL
74.208.230.137	4/7/17	86400
74.208.230.124	4/7/17	86400
74.208.153.17	4/7/17	86400
74.208.153.11	4/7/17	86400
61.182.206.92	4/7/17	0
59.23.1.118	4/7/17	0
59.125.106.186	4/7/17	0
59.12.24.20	4/7/17	0
27.147.125.109	4/6/17	0
220.92.67.69	4/6/17	0
211.225.0.187	4/6/17	0
211.207.16.43	4/6/17	0
211.198.35.65	4/6/17	0

노트: IP 주소와 이름 서버는 모두 피벗입니다. 클릭하여 이 도메인을 호스팅하는 인프라가 어떻게 구성되는지, 그리고 이 도메인과 관련된 다른 호스팅 인프라에 대해 자세히 알아볼 수 있습니다.

노트: 현재 엠브렐라는 90 일의 패시브 DNS 데이터를 보관하고 있습니다.

실습 결론

이 실습에서는 Umbrella Security Insight Report 에서 시작한 첫 번째 사용 사례를 살펴보고 특정 도메인의 세부 정보를 자세히 살펴서 차단된 이유를 파악하고자 했습니다. 우리는 엄브렐라에 의해 악의적인 것으로 여겨지는 곳을 조사하기 위해 선회했습니다. 더 자세히 살펴보니 도메인이 악의적일 수 있는 여러 가지 이유가 있습니다:

- **DNS 쿼리** 그래프에 기반한 도메인 트래픽이 불규칙했습니다..
- 다른 악성 도메인을 등록하는 데 사용된 것과 동일한 이메일 주소로 등록되었습니다
- **도메인 태깅(Domain Tagging)** 섹션에서 **봇넷(botnet)**으로 분류되었습니다.
- **fast fluxing**.
- 기타...

실습 2: 사건 조사(Incident Investigation)

이 연습에서는 이전에 전혀 몰랐던 도메인을 살펴보게 됩니다. 이는 이전에 악성 사이트가 차단되어 조사를 위해 엄브렐라에서 피벗되는 것을 본 시나리오와 다릅니다.

다음은 시나리오입니다. 보안 운영 팀은 환경 전반에 걸쳐 여러 엔드포인트가 의심스러운 도메인(또는 IP)에 반복적으로 연결되어 있다는 SIEM 경고를 받았습니다. 이전에는 해당 도메인에 대한 트래픽이 관찰되지 않았으며, 목표는 이 도메인이나 IP에 대해 자세히 알아보고 악성인지 양성인지 확인하는 것입니다.

Investigate 에서 쿼리할 수 있는 여러 가지 유형의 요소가 있습니다:

- **Domain 및 subdomain** 항목은 프로토콜 또는 URL 정보 없이 지정해야 하지만 하위 도메인을 포함할 수 있습니다. 예를 들어 `www.example.com` 과 `example.com` 은 모두 유효하며 도메인의 영역 레코드 구성에 따라 서로 다른 결과를 반환할 수 있습니다.
- **IP 주소** 항목은 전체 IPv4 IP 주소여야 합니다(예: 19.117.63.126).
- **Autonomous System Number (ASN)** 항목은 단순히 AS 번호여야 합니다(예: 36692).
- **Email address** 는 전통적인 `name@domain.com` 형식이어야 합니다. 전자 메일 주소를 입력하면 도메인 등록자가 검색됩니다.

주요 정보를 사용하여 도메인이 악성적인지 확인

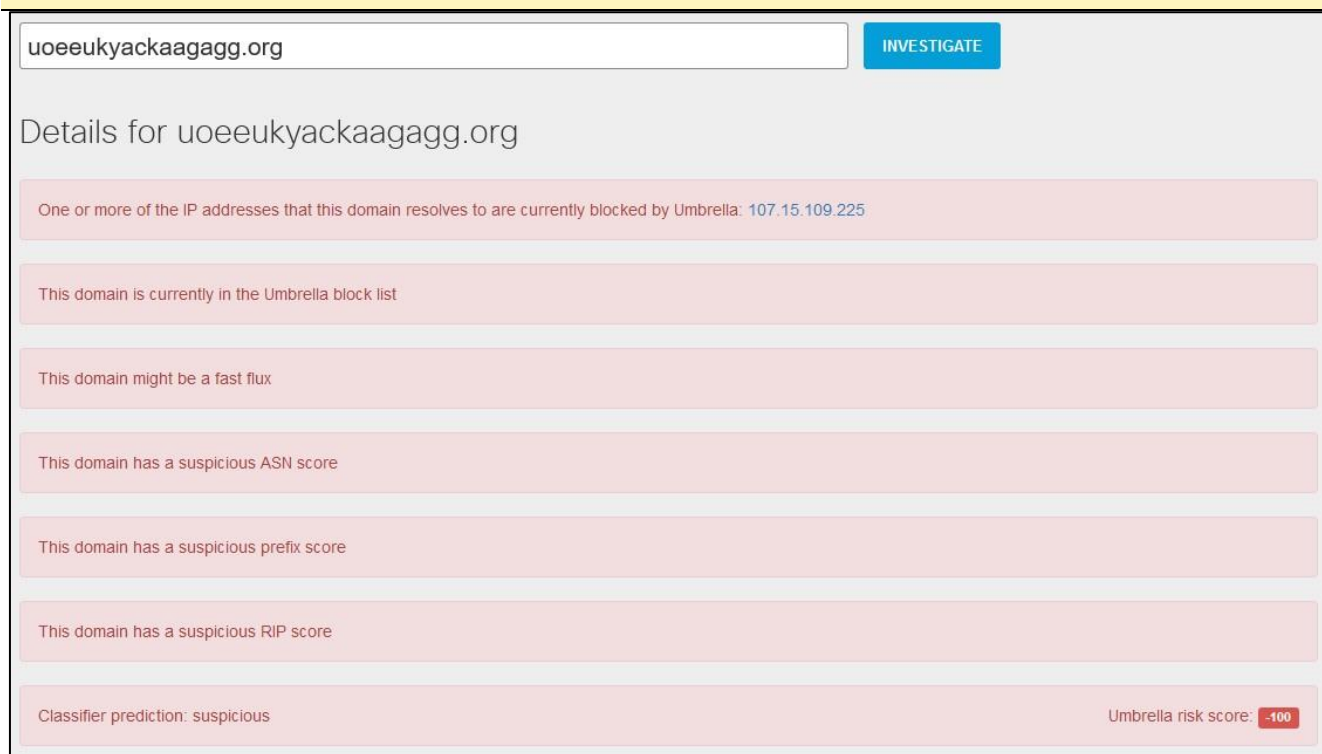
경고 검토

1. 다음은, 이 실습의 Investigate 에서 분석할 수 있는 몇 가지 목적지(destinations)입니다:

- uoeeukeyackaagagg[.]org
- a[.]sinkhole[.]yourtrap[.]com
- j8le7s5q745e[.]org
- goloduha[.]info
- xkjyjlqqngn[.]net
- nailsartsdesfuture[.]com
- samyhookf[.]top
- uclcrsuiwcymao[.]net

2. 페이지 상단에 있는 경고를 검토하고 해당 도메인이 양(또는 "좋은" 도메인)인지, 무시될 수 있는지, 아니면 조금 더 자세히 파고들 필요가 있는지 확인하십시오.

노트: 페이지 상단에 있는 알림 세부 정보를 확인하고 알림에 따라 관련 섹션으로 스크롤하십시오.



uoeeukeyackaagagg.org INVESTIGATE

Details for uoeeukeyackaagagg.org

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: 107.15.109.225

This domain is currently in the Umbrella block list

This domain might be a fast flux

This domain has a suspicious ASN score

This domain has a suspicious prefix score

This domain has a suspicious RIP score

Classifier prediction: suspicious Umbrella risk score: -100

DNS 쿼리 그래프 및 도메인 테깅

1. **DNS 쿼리 그래프**에서 트래픽 패턴을 확인하십시오. 뾰족하거나 규칙적인 패턴이 있는가?
2. **도메인 태그**를 확인하여 엠브렐라가 이러한 도메인에 태그를 지정한 방법과 그 이후를 확인하십시오.

WHOIS 데이터 기록

1. **WHOIS** 기록 데이터에서 nllartdesfuture[.]com 을 확인하십시오. 이 도메인을 등록하는 데 사용된 이메일 주소도 많은 다른 악성 도메인을 등록하는 데 사용되었다는 것을 알게 될 것입니다. 이 전자 메일 주소에 등록된 모든 도메인의 목록을 표시하려면 전자 메일 주소를 클릭하십시오.

WHOIS Record Data			
Registrar Name: GODADDY.COM, LLC IANAID: 146		Last retrieved a moment ago GET LATEST	
Created: September 11, 2016	Updated: September 11, 2016	Expires: September 11, 2017	Raw data
Email Address	Associated Domains	Email Type	Last Observed
domainmanagers@outlook.com	Greater than 500 Total - At least 4 malicious	Administrative, Registrant, Technical	Current
yingw90@yahoo.com	Greater than 500 Total - At least 500 malicious	Administrative, Registrant, Technical	April 22, 2016
Showing 2 of 2 Results			

노트: 어떤 경우에는 도메인에 보안 범주가 태그가 지정되지 않았을 수 있습니다. 도메인이 이 전자 메일 주소에 등록되었지만 실제 호스트나 IP 주소가 없고 따라서 열브렐라가 해결할 유효한 트래픽이 없는 경우 이 문제가 발생할 수 있습니다. 대체적으로, 현재 도메인과 관련된 그러한 유형의 활동이 없기 때문에 멀웨어나 봇넷으로 분류되지 않을 수도 있지만, 앞으로는 경계해야 할 사항입니다.

Domains Associated with domainmanagers@outlook.com			
Domain Name	Security Categories	Content Categories	Last Observed
cpcihrecow.com	Botnet		Current
dslauumf.com	Botnet		Current
securitylabtoday.com	Malware		Past
timsimon8.com	Malware		Current
ziocorp.com	Malware		Past
360hitz.com			Current
365daysoffwork.com			Current

2. **WHOIS** 기록 데이터에서 등록자가 등록한 다른 도메인으로 피벗하기 위해 다른 악성 도메인을 사용해 보십시오.
3. 이제 이메일 주소를 피벗하여 다른 악성 활동이 어떤 것인지 확인하고 동일한 공격자 인프라와 관련된 추가 도메인을 찾으십시오. 이 등록자가 다른 악성 도메인을 등록했다는 사실은 이 도메인이 악의적일 가능성을 증가시킵니다.

IP 및 ASN 의 피벗 (Pivot)

1. a[.]sinkhole[.]yourtrap[.]com 에서 조사를 실행하고 IP 주소 섹션으로 스크롤하십시오. 이 경우 최근에 정기적으로 변경된 이 도메인과 관련된 IP 주소가 여러 개 있습니다.

IP Addresses		
First seen	Last seen	IPs
3/4/17	4/7/17	153.141.140.208 (TTL: 30)
3/3/17	3/3/17	153.141.140.208 (TTL: 30) 153.251.233.138 (TTL: 30)
2/4/17	3/2/17	153.251.233.138 (TTL: 30)
2/3/17	2/3/17	114.147.125.120 (TTL: 30) 153.251.233.138 (TTL: 30)
1/14/17	2/2/17	114.147.125.120 (TTL: 30)
1/13/17	1/13/17	114.147.125.120 (TTL: 30) 153.251.216.224 (TTL: 30)
1/5/17	1/12/17	153.251.216.224 (TTL: 30)

2. 목록 맨 위에 있는 IP 주소 중 일부를 클릭하여 해당 IP 공간에 다른 악의적이거나 의심스러운 도메인이 있는지 확인하십시오. 클릭 몇 번이면 몇 번이면 찾을 수 있을 겁니다!

153.141.140.208

Details for 153.141.140.208

Hosting 444 malicious domains for 1 week

3. IP 주소 보기에서 조사에서는 IP가 현재 호스팅하고 있는 악의적인 도메인의 수를 표시하고 해당 IP 주소에 호스팅되는 알려진 도메인과 악의적인 도메인도 모두 나열합니다. **Prefix** and **Autonomous System** (ASN 및 네트워크 소유자)도 볼 수 있습니다. 악의적인 도메인을 많이 호스팅하는 IP의 경우 이전 페이지에서 의심스러운 RIP(IP 평판) 점수에 대한 알림이 표시될 수 있습니다. 다른 악성 활동이 많은 IP 주소가 호스팅하는 도메인 자체가 악성일 가능성이 높습니다.

AS

Prefix	ASN	Network Owner Description
153.128.0.0/11	AS 4713	OCN NTT Communications Corporation, JP 86400

Malicious domains hosted by 153.141.140.208

[applesoftupdate.com](#) [dnsweb.org](#) [download.firefoxupdate.com](#) [e.applesoftupdate.com](#) [email.applesoftupdate.com](#) [fire.firefoxupdate.com](#) [firemail.applesoftupdate.com](#) [pda.applesoftupdate.com](#) [pop.applesoftupdate.com](#) [smtp.applesoftupdate.com](#) [stmp.allshell.net](#) [support.icoredb.com](#) [krjregh.sacreeflame.com](#) [micorsofts.net](#) [3pma.firefoxupdate.com](#) [acer.firefoxupdate.com](#) [admin.firefoxupdate.com](#) [adobe.firefoxupdate.com](#) [amusement.firefoxupdate.com](#) [analysis.firefoxupdate.com](#) [anti.firefoxupdate.com](#) [apple.firefoxupdate.com](#) [atm.firefoxupdate.com](#) [auto.firefoxupdate.com](#) [bbh.dnsweb.org](#) [bbs.firefoxupdate.com](#) [bbsfu.firefoxupdate.com](#) [bcc.firefoxupdate.com](#) [bing.firefoxupdate.com](#) [bitdefender.firefoxupdate.com](#)

명단이 계속되다.....

4. 다음에, IP 보기에서 피벗할 **ASN** 를 클릭합니다.

AS 4713			
Current information			
Period	Creation date	Registry	Network Owner Description
Aug 28, 2016 - Apr 8, 2017		APNIC	OCN NTT Communications Corporation, JP 86400
Aug 27, 2016 - Aug 28, 2016		APNIC	OCN NTT Communications Corporation,,,,, JP 86400
Aug 25, 2016 - Aug 27, 2016		APNIC	OCN NTT Communications Corporation,,, JP 86400
Apr 8, 2016 - Aug 25, 2016		APNIC	OCN NTT Communications Corporation, JP 86400
Mar 29, 2014 - Apr 8, 2016		APNIC	OCN NTT Communications Corporation,JP 86400
Sep 11, 2013 - Mar 29, 2014		APNIC	OCN NTT Communications Corporation 86400
Aug 29, 2013 - Sep 12, 2013	1995-08-30	APNIC	OCN NTT Communications Corporation 86400
Feb 27, 2013 - Aug 29, 2013	1995-08-30	APNIC	OCN NTT Communications Corporation 86400
Jan 13, 2013 - Feb 27, 2013	1995-08-30	APNIC	OCN NTT Communications Corporation 86400
Dec 5, 2012 - Jan 12, 2013	1995-08-30	APNIC	OCN NTT Communications Corporation 86400

Current routes for AS 4713		
Prefix	Country	Suspicious activity in the past week
103.208.96.0/22	N/A	
119.161.104.0/21	Japan	
211.1.32.0/19	Japan	
61.114.112.0/21	Japan	
61.114.120.0/21	Japan	

5. 여기에서, 이 자울 시스템에 연결된 모든 IP prefixes 를 볼 수 있습니다. 지난 주에 악의적인 활동을 호스팅한 적이 있는 항목을 보려면 아래로 스크롤하십시오.

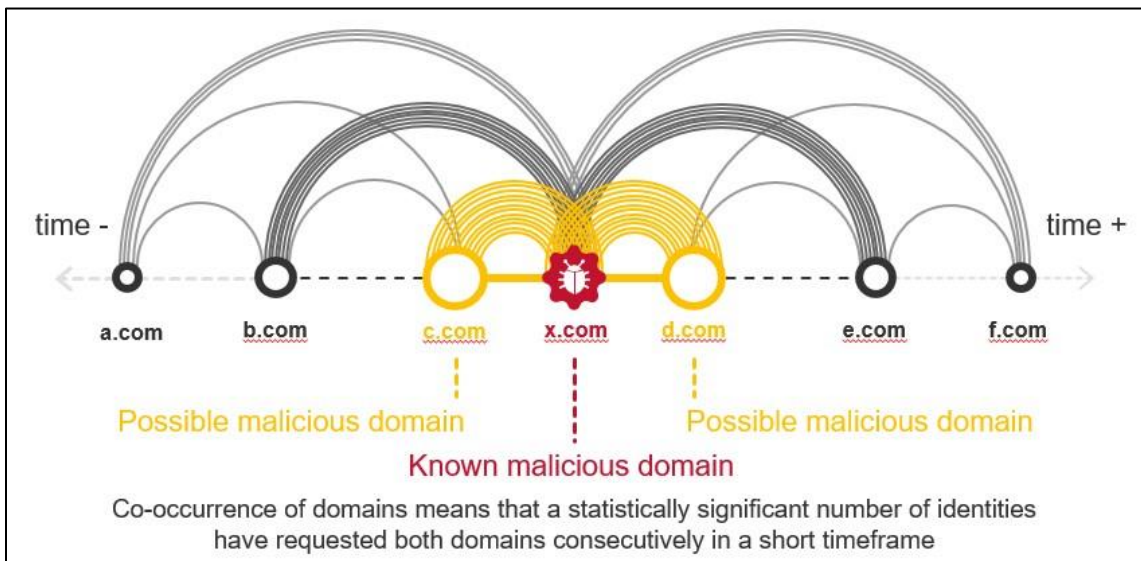
Current routes for AS 4713		
Prefix	Country	Suspicious activity in the past week
103.208.96.0/22	N/A	
119.161.104.0/21	Japan	
61.126.0.0/15	Japan	marchen-toy.co.jp jsrmpm.org kikuyapackage.co.jp kalu.co.jp gtilite.jp umedaumeda.ec-net.jp
61.208.0.0/16	Japan	fu-k.jp
61.112.0.0/16	Japan	sasahara-kk.com
153.224.0.0/12	Japan	use-inc.tv
210.190.0.0/16	Japan	feeltheworld.jp

동시 발생 및 관련 도메인에 대한 피벗

Co-occurrences (공동 발생)

종종 감염된 호스트가 악의적인 사이트를 검색한 다음 곧 두 번째 또는 세 번째 악성 사이트를 방문합니다. 해당 명령 및 제어 호스트를 검색하는 감염된 호스트는 이러한 방식으로 동작할 수 있습니다. 또는 웹 사이트가 다른 사이트의 감염된 콘텐츠로 리디렉션될 수 있으며, 이는 첫 번째 사이트를 방문하는 호스트와 리디렉션된 사이트 간의 동시 발생을 나타냅니다. **공동 발생**은 그 관계를 보여줍니다.

다음은 시간에 따른 **공동 발생(co-occurrences)**의 시각적 표현입니다.



조사에서의 **공동 발생**은 조사 중인 도메인과 비슷한 시간에 확인 된 다른 도메인 이름을 추적 하는 방법입니다. 두 개의 도메인 이름이 서로 급속하게 연속적으로 방문될 때, 그들은 공동 발생한다고 하며, 첫 번째 도메인이 악의적인 것으로 알려지면, 그 공동 발생 도메인은 추론에 의해 유죄가 됩니다. 각 도메인에는 두 도메인이 공동 발생하는 빈도를 나타내는 **공동 발생 점수**가 있으며, 100 은 1 대 1 의 **공동 발생**입니다. **공동 발생**은 동일한 디바이스에서 하나 이상의 도메인 간의 관계 및 대 상호 연결을 빠르게 연속적으로 (예: 초) 표시 하는 방법입니다. 그런데 전 세계적으로 통계적으로 많은 디바이스가 동일한 패턴을 표시하는 것을 확인하는 경우에만 가능합니다. 이를 통해 보안 분석가들은 모두 동일한 공격에 연결된 악성 도메인을 통합하고 공격자의 인터넷 인프라에 대 한 가장 완벽 한 보기를 얻을 수 있습니다. 공동 발생은 이 경우에도 분석가가 공격자를 계속해서 사용하고 네트워크 보안이 침해 되기 전에 추가 관련 (및 의심스러운) 도메인을 사전에 차단할 수 있습니다

1. 이제 extspeier[.]de 를 사용하여 Investigate(조사)의 페이지 하단에 있는 **공동 발생**을 해제하고 체크아웃합니다. 나열된 **공동 발생 점수**는 현재 조사 중인 도메인에 대한 것입니다.

Co-occurrences

tesab.org.uk (100.00)

2. textspeier[.]de 의 경우, 이 도메인과 함께 공동 검색하는 도메인에 대해 일대일 관계(점수 100.00)를 가지며, 같은 공격에 묶일 가능성이 높습니다. 한 사람을 위해 요청이 있을 때마다 다른 사람을 위해 요청됩니다. 추가 조사를 위해 tesab[.]org[.]uk 도메인을 피벗할 수 있습니다.

공동 발생이 반드시 나쁜 것만은 아닙니다. 합법적인 사이트는 일반적인 웹 활동의 일부로 서로 공존합니다. 많은 인기 있는 사이트들이 디자인된 대로 서로 공존합니다. 그러나 악의적인 도메인을 볼 때, **공동 발생**은 종종 명령과 제어, 감염의 다른 부분 또는 멀웨어의 업데이트 구성 요소일 수 있는 다른 도메인을 노출시킵니다.

악성 사이트가 알려진 양호한 사이트와 함께 발생하는 이유는 무엇입니까? (일반적으로 악의적이지 않은) 광고 네트워크가 있다고 가정해 보겠습니다. 그리고 이러한 공동 발생은 malvertising 와 관련이 있습니다. 누군가가 AppNexus 애드 네트워크에서 광고 공간을 구입하고 있습니다. 이 앱은 이 사이트를 C&C 로 사용하거나 멀웨어를 드라이브 바이 다운로드하기 위해 드로퍼로 사용하는 멀웨어를 서비스합니다.

3. 추가 악성 도메인 중 일부를 사용해 보고, 동일한 공격과 관련된 추가 도메인을 피벗하여 찾을 수 있는 고도로 점수가 매겨진 **공동 발생**을 검색하십시오.

관련 도메인

관련 도메인 보안 기능은 함께 **공동 발생**하는 것과 유사 합니다. 인터페이스의 이 부분은 동일한 시간(최대 60 초 전 또는 후)에 자주 요청되었지만 다른 도메인 이름과 자주 연결되지 않은 도메인 이름 목록을 반환합니다.

도메인 이름 옆의 점수에는 검색 중인 도메인에 대한 원래 요청의 60 초 이내에 관련 사이트를 조회했던 클라이언트 Ip 수가 반영됩니다.

1. 몇가지 추가 악성 도메인을 시도하고 피벗할 고도로 점수가 매겨진 관련 도메인을 검색하고 관심 있는 추가 도메인을 찾으십시오.

실습 결론

이 연습에서는 SIEM 경고에서 도메인을 쿼리하기 시작했습니다. 우리는 그것이 악의적인 것인지 그리고 조사관이 그것에 대해 무엇을 알고 있는지 알아내고 싶었습니다. 저희는 조사를 통해 악의적인 것으로 판단했고, 이를 통해 다음과 같은 사실을 발견했습니다.

- IP 가 다른 악성 도메인을 많이 호스팅했기 때문에 **IP reputation** 점수가 의심스러웠습니다.
- **DNS 쿼리** 그래프에 따라 도메인으로서의 트래픽이 불규칙했습니다.
- 거의 500 개의 다른 악성 도메인을 등록하는 데 사용된 것과 동일한 이메일에 등록되었습니다.

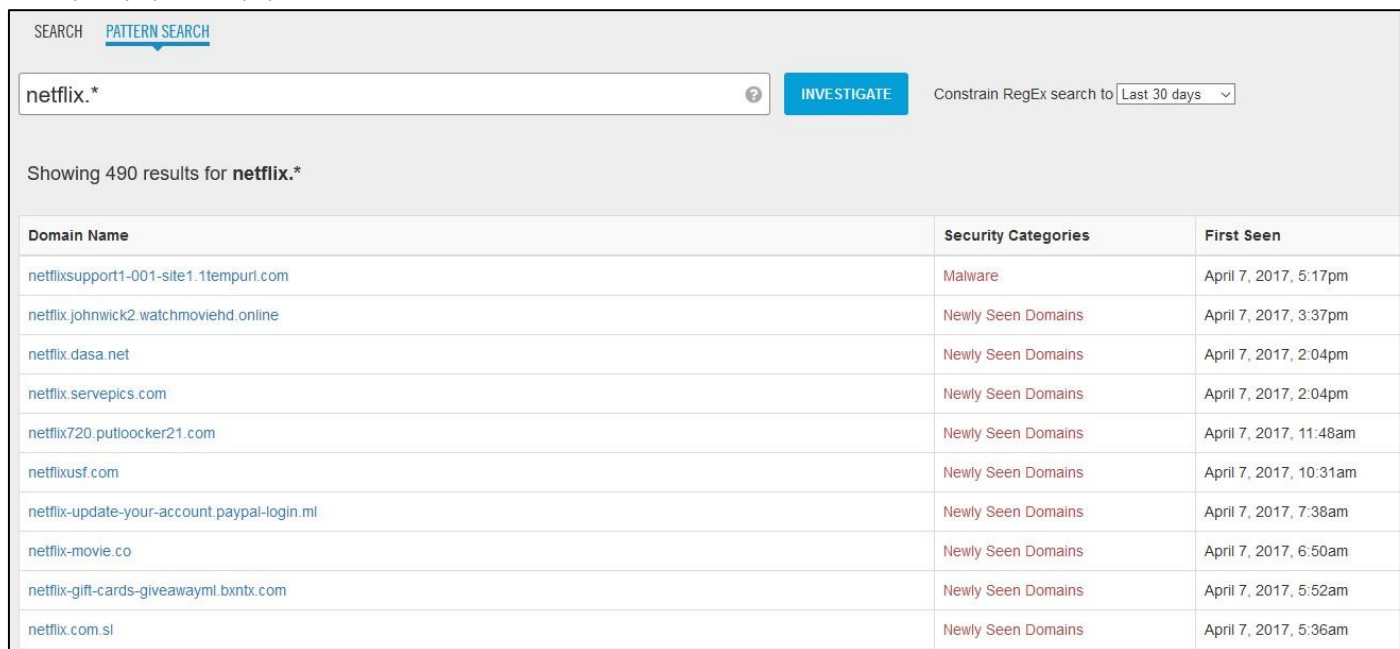
- **domain** 에서 **IP** 로 전환하여 **ASN** 으로 전환하여 다른 악의적인 활동이 많은 네트워크에 의해 호스팅되었음을 확인했습니다.
- **Co-occurrences** 은 동일한 공격과 연관되었을 가능성이 있는 또 다른 도메인을 보여주었습니다. 그 영역이 어떻게 연관되어 있는지 확인하기 위해 더 많은 연구가 수행될 수 있습니다.

연습 3: 패턴 검색 및 사전 예방적 연구

패턴 검색

조사에서 비교적 새로운 기능은 **패턴 검색**입니다. **패턴 검색**을 사용 하면 브랜드 이름을 포함하여 서로 다른 패턴 및 용어와 일치하는 도메인에 대한 조사를 쿼리할 수 있습니다. 도메인 이름과 정확히 일치하는 항목을 검색하는 것이 아니라 **패턴 검색**을 통해 더 유연하고 광범위한 검색을 수행할 수 있습니다. 패턴 검색의 사용 사례 중 하나는 회사의 브랜드 이름을 가장하는 새 도메인을 확인하는 것입니다. 즉, 고객의 직원 으로부터 피싱 캠페인 용 악성 사이트를 마스킹하는 데 사용할 수 있습니다. 패턴 검색에서는 기존 정규식 (RegEx)을 사용 하여 일치할 수행 합니다.

1. Netflix 을 예로 들어 보겠습니다. Regex 를 사용하면 모든 새로 쿼리에 "netflix" 라는 용어를 포함된 도메인을 검색 상단에 있는 **Pattern Search (패턴 검색)** 탭에 "netflix."로 입력 하고 검색할 수 있습니다. 시간 설정을 지난 30 일로 유지 합니다. 반환 되는 결과의 수를 확인 하십시오. "Netflix"가 있는 도메인의 수를 확인합니다. 대부분 경우는 적법하지 않습니다.



Domain Name	Security Categories	First Seen
netflixsupport1-001-site1.1tempuri.com	Malware	April 7, 2017, 5:17pm
netflix.johnwick2.watchmoviehd.online	Newly Seen Domains	April 7, 2017, 3:37pm
netflix.dasa.net	Newly Seen Domains	April 7, 2017, 2:04pm
netflix.servepics.com	Newly Seen Domains	April 7, 2017, 2:04pm
netflix720.putlocker21.com	Newly Seen Domains	April 7, 2017, 11:48am
netflixusf.com	Newly Seen Domains	April 7, 2017, 10:31am
netflix-update-your-account.paypal-login.ml	Newly Seen Domains	April 7, 2017, 7:38am
netflix-movie.co	Newly Seen Domains	April 7, 2017, 6:50am
netflix-gift-cards-giveawayml.bxntx.com	Newly Seen Domains	April 7, 2017, 5:52am
netflix.com.si	Newly Seen Domains	April 7, 2017, 5:36am

2. 지난 30 일에 기간을 사용했던 impersonators 의 분량을 보여 주지만 일반적으로 가장 관련성이 높은 결과는 최신 시간 프레임 내에 있습니다.

- 이제 잠재 고객의 지적 재산권, 기존 고객 또는 개인적인 생활의 사물 중 하나와 일치 하는 몇 가지 흥미로운 RegEx 패턴을 시도해 보십시오.

노트: regex 에 대한 도움말을 보려면 <http://regexr.com> 를 참조하십시오.

적극적인 연구

이 시나리오에서는 잠재적 위협을 미리 확인 하고 위협 Intel 공유 그룹을 통해 발견 한 단일 도메인으로 시작 하는 것을 시도 하고 있습니다. 이제 조사를 사용하여 공격자의 인프라를 확인합니다.

브라우저 하이재킹 악성 코드를 호스팅하는 도메인 "anbtr.com"으로 시작 하 여 피싱 공격이 나 보안 침해 된 URL 이 전달 되는 경우가 많습니다.

- sso.anbtr[.]com 에 대한 조사의 쿼리를 실행하십시오.
- 이 도메인이 블록 목록에 있음을 나타내는 빨간색 경고와 기타 보안 기능을 기록해 두십시오. 최근의 DNS 트래픽 그래프는 공정한 양과 규칙적인 패턴을 보여줍니다.



- 비정상적인 트래픽 패턴이 보이는지 확인하고 확대하여 날짜에 대한 세부 사항을 기록하십시오.
- 공동 발생** 항목으로 스크롤하십시오. 이 예에서는 다른 악의적인 호스트와 **공동 발생하는** 경우가 많습니다. 이러한 추가 도메인에 대해 알고 있으면 위협에 앞서 유지하는 데 도움이 됩니다.

Co-occurrences

a.deltaheavy.ru (4.11) asch-bourj.org (4.11) dasur01.com (4.11) down.7yue.info (4.11) hpnstatic-china.hissage.net (4.11) img.samsungmediahub.net (4.11) lb.msp64-02.com (4.11) mpggalaxy.mine.ru (4.11) npkxghmoru.biz (4.11) secondary udp-host-cache.com (4.11) seed.trtromg.com (4.11) skyprobar.info (4.11) updates.swarmcast.net (4.11) worldtvpro.zapto.org (4.11) modstats.org (2.98) feeds.rhapsody.com (2.86) repo.run (2.54) shadowcrew.info (2.39) weather.intechical.online (2.22) report.trtromg.com (2.22) karbadina.com (2.12) tabila.biz (2.11) hamster54.com (2.09) bitebbs.com.home (1.98) www.95598-app.com (1.40) torrents.yourexotic.com (1.38) amramon.biz (1.36) arthur.niria.biz (1.18) collect.trtromg.com (1.14) www.piratux.com (1.13) hamster.download-quick.net (1.11) ota.otaandroidupdate.com (1.00) control.coolkey.org (0.76) www.careerdesk.org (0.76) arqdesigngv.com.br (0.74) futureinterest.org (0.65) fex.net (0.56)

노트: 일부 공동 발생은 의심스럽거나 악의적인 도메인과 함께 발생하는 합법적인 도메인이며, 다른 공동 발생은 공격자의 서버 인프라에 포함되며 관련 됩니다.

- 일부 **공동 발생** 및 **관련 도메인**을 별도의 브라우저 탭 또는 창에서 열고 IP 또는 **ASN** 과 같은 첫 번째 도메인과 공유하는 공통 기능을 확인하십시오. 그들이 이미 열브렐라에 의해 막혀 있거나 교통 패턴에 대해 특이한 점이 있는지 알아보십시오.

도메인에서 공유하는 인프라

1. sso.anbtr[.]com 의 **IP 주소** 데이터로 스크롤합니다.

IP Addresses		
First seen	Last seen	IPs
1/6/17	4/8/17	195.22.28.222 (TTL: 100)

2. 표시된 **IP 주소** (195.22.28.222)에 대한 피벗.

Malicious domains hosted by 195.22.28.222
sso.anbtr.com xssso.anbtr.com anbtr.com httpssso.anbtr.com js.anbtr.com so.anbtr.com soo.anbtr.com ss.anbtr.com ss0.anbtr.com ssc.anbtr.com sssso.anbtr.com s xssso.js.anbtr.com xssso.so.anbtr.com xssso.ss.anbtr.com xssso.ssc.anbtr.com xssso.sssso.anbtr.com xssso.suggest.seccint.comsso.anbtr.com xssso.urisso.anbtr.com xssso.

IP 보기에서는 현재 악성 사이트를 적발할 뿐만 아니라, 현재 악성일 수 있는 것이 아니라 의심스러운 활동과 연관되어 향후 공격에 사용될 수 있는 동일한 IP 에서 호스팅되는 다른 도메인을 찾을 수도 있다. 이러한 영역은 사전 예방적으로 차단할 수 있는 영역입니다.

ASN 에 대한 피벗

이전 단계에서 배운 내용을 사용하여 sso.anbtr[.]com 에 대해 IP ASN 을 피벗하고 동일한 인프라를 공유하는 추가 위협을 계속 찾으십시오.

Current routes for AS 8426		
Prefix	Country	Suspicious activity in the past week
185.77.80.0/22	United Kingdom	
89.206.128.0/17	United Kingdom	aptrack.info
92.54.33.0/24	Spain	
92.54.0.0/18	Spain	call4free800311631.net atrapalo.cl
185.32.200.0/22	United Kingdom	extraverginecoratina.it

WHOIS 에 대한 피벗

1. sso.anbtr[.]com 으로 돌아가서 **WHOIS** 레코드 데이터에서 이메일 주소를 사용하여 추가 악성 도메인을 찾기 위해 이 문제를 피벗하십시오. 인프라에 대해 자세히 알아보려면 **IP, ASN** 및 도메인을 검색하십시오.
2. 기타 목록.....

Domains Associated with jgou.veia@gmail.com			
Domain Name	Security Categories	Content Categories	Last Observed
aaimomuiqqkikiy.org	Botnet, Malware		Current
asdfuh982hdodjc.com	Botnet, Malware		Current
bbggobqqidet.com	Botnet, Malware		Current
bfgefjsslipx.com	Botnet, Malware		Current
cigarettemeeting.net	Botnet, Malware		Current
dogcurbctw.com	Botnet, Malware		Current

실습 결론

연습에서는 위협 정보 공유 그룹을 통해 찾은 단일 도메인으로 시작하십시오. Investigate 를 사용하여 다음을 통해 잠재적으로 악의적인 다른 위협을 사전에 파악할 수 있습니다:

- 공동 발생 및 관련 도메인 식별
- 모니터링/사전 차단되어야 하는 동일한 IP 및 ASN 에서 호스팅되는 다른 도메인 찾기
- 동일한 전자 메일 주소에 등록되어 동일한 공격자에 연결되었을 가능성이 있는 다른 도메인 탐지

실습 4: Cisco AMP 및 Threat Grid 를 통한 공격 보기 완료

Umbrella 의 기술은 이전 연습에서 논의한 바와 같이 공격자의 인프라를 비교할 수 없는 수준으로 보여줍니다. 다음 논리적 단계는 공격 목표를 보다 잘 이해하기 위해 페이로드 자체에 초점을 맞춘 심층 분석으로 이 보기를 완료하는 것입니다. Umbrella Investigate 는 **Cisco AMP** 및 **Cisco Threat Grid** 와 통합되어 세계적인 수준의 정적 및 동적 파일 분석을 제공합니다. 이 두 강력한 기술 간의 파트너십을 통해 단일 창에서 공격을 가장 완벽하게 파악할 수 있습니다. 통합을 살펴보기 전에 이 [비디오](#)를 보는 것이 권장합니다(9 분).

이미 일부 정보를 수집한 도메인의 sso.anbtr[.com]을 분석하지만 이번에는 이 도메인에 연결된 샘플을 중심으로 **AMP** 및 **Threat Grid** 에서 제공하는 정보에 초점을 맞춥니다.

1. sso.anbtr[.]com 에 대한 Investigate 에서 쿼리 실행합니다.

2. **Associated Samples** 섹션으로 스크롤합니다.

Associated Samples POWERED BY CISCO AMP THREAT GRID		
Threat Score	SHA256 Signature	AV Result
100	100f7013afbb35cdadad167a32a633551ae6a936f618eab1238d95a5d7362717	Win.Virus.Sality, Win.Trojan.Agent
100	344578776ec8506a766d3ffae149675eb691b6e108f86c15e07dc580403320e	
100	36bae6ac791d5f951529ceadb64ba341a18cc1a03726f8dfaf2b8b34baedab5	Win.Trojan.Agent
100	3785466e4161f03f2b551fa2eadd6b0d4861a0eb3884531d77fbb969a2d28e2	Win.Trojan.Ramnit
100	96d71fbd104f11143fae58aec1dfd5bebb80e3565986a51308d2cd86cfc8b3	Win.Trojan.Agent
100	9d5595130ac7231ecf3ee7a46eba03ba5905cd16120da52e24b137a6fcca3e8	Win.Virus.Sality, Trojan.Agent
100	a1444d83e71ed2a4c85d585d3b42b582f3af9e785231c9bdf393f389ea7bdb0	
100	a39150c3a985af66c72f4421df35c500a723e051b2b315c6a5f4fa79b229d7	Win.Trojan.Agent
100	dac4981af23d209d1de8f686075e1ced036e8130723980495732f6184e73bcfa	Win.Trojan.Agent, Win.Worm.Agent
100	f279c342dc2c0c120c3b781d30df4efae426d2dfbb3c9252c026030b6c2d124	Win.Trojan.Ramnit

이 섹션은 AMP가 샌드박스 프로세스 중에 인식하거나 식별한 sso.anbtr[.com]에 연결된 파일 목록을 제공합니다. 파일을 추적하기 위해 AMP는 분석하는 각 파일에 대해 고유 식별자(SHA256)를 계산합니다. 일부 파일의 경우 AV 결과도 제공되므로 Threat Grid에는 여러 AV 엔진이 내장되어 있어 파일이 악의적이고 서명이 존재한다는 점을 분명히 지적합니다. Threat Grid Sandbox는 하나 이상의 OS 시스템에서 파일을 실행하고 레지스트리 수정에서 네트워크 통신에 이르는 모든 것을 수집합니다. 수집된 데이터는 0부터 100까지의 행동에 점수를 부여하는 행동 지표 모델을 통해 실행됩니다. Threat Grid는 현재 700개 이상의 행동 모델을 실행하고 있습니다. 서로 다른 모델의 점수가 결합되어 파일에 할당됩니다(artifact 나중에 우리는 몇 개의 개별 샘플을 더 자세히 살펴볼 것입니다. 현재 sso.anbtr[.]com에 대한 모든 관련 샘플이 가장 높은 위협 점수를 가지고 있는 것을 확인합니다.

3. AV에 의해 Win Virus Sality, Win Troy Agent로 분류된 샘플을 선택하고 SHA256 Signature를 클릭한다. 이렇게 하면 특정 멀웨어 샘플에 대한 상세 보기를 볼 수 있습니다.

INVESTIGATE

THREAT SAMPLE (SHA256)
100f7013afbb35cdadad167a32a633551ae6a936f618eab1238d95a5d7362717

SHA1 bd2f6512cc1cbbafa569598a00c40a60602064b
MD5 cea20d3012b0719645cd930024aee57d

Threat Score: 100
Magic Type: PE32 executable (GUI) Intel 80386, for MS Windows
Size: 103140 bytes (101.0 kB)
AV Results: Win.Virus.Sality, Win.Trojan.Agent
First Seen: Jul 28, 2016 22:58:13 UTC
Full Sample Data from Threat Grid

헤더에는 샘플에 대한 기본 정보인 SHA256(및 2개의 다른 해시 마커), 파일 크기, AV 결과 및 파일이 처음 표시되는 시간이 나열됩니다.

노트: Umbrella Investigate 는 각 샘플에 대한 자세한 보기를 제공합니다. 그러나 이는 AMP Threat Grid 솔루션이 제공할 수 있는 일부입니다. API 액세스를 포함한 AMP Threat Grid 에 대한 전체 액세스 권한을 얻으려면 별도의 AMP Threat Grid 라이선스를 구입해야 합니다.

Threat Score: **100**
 Magic Type: PE32 executable (GUI) Intel 80386, for MS Windows
 Size: 103140 bytes (101.0 kB)
 AV Results: Win.Virus.Sality, Win.Trojan.Agent
 First Seen: Jul 28, 2016 22:58:13 UTC
[Full Sample Data from Threat Grid](#)

4. **BEHAVIORAL INDICATORS** 섹션까지 아래로 스크롤합니다. 각 동작 표시기에는 **severity** 가 할당됩니다. 이는 OS 동작이 보안 위험을 어느 정도 나타내는지에 대한 Cisco 보안 전문 지식과 평가를 반영합니다. **Severity** 점수는 지정된 샘플이 동작을 나타낼 가능성을 나타내는 신뢰도 수준과 함께 제공됩니다.

BEHAVIORAL INDICATORS		
Indicator	Severity ⓘ	Confidence ⓘ
USB Autorun Enabled through the Creation of autorun.inf	100	100
Sality Default Mutex Detected	100	100
Artifact Flagged Malicious by Antivirus Service	100	95
Artifact Flagged as Known Trojan by Antivirus	100	95
Process Modified a File in a System Directory	90	100
Excessive Suspicious Activity Detected	90	100
Process Deleted SafeBoot Registry Key	90	90
Process Deleted SafeBoot Registry Key Value	90	90

5. 동작 표시기를 클릭하여 작업에 보안 위험이 발생하는 이유에 대한 자세한 설명을 확인하십시오.

Artifact Flagged as Known Trojan by Antivirus

Process Modified a File in a System Directory

Process Modified a File in a System Directory

Malware will modify files in system directories to hide logs or other evidence. Also, by modifying system files it can disable functionality in the system which may detect or hamper the operation of the malware. Lastly, it may be attempting to hide an executable, so that it appears to be a legitimate system file.

Artifact Flagged by Antivirus

Process Modified an Executable File

6. **NETWORK CONNECTIONS** 섹션으로 스크롤합니다.

7. sso.anbtr[.]com 을 결정하는 DNS 쿼리를 기반으로 **Threat Grid** 에서 샘플 목록을 얻으므로 이 도메인에 대한 네트워크 연결 섹션에서 일부 연결을 확인해야 합니다. 아래 그림에 강조 표시되어 있습니다. 맬웨어 및 피싱과 관련된 amsamex[.]com 과 같은 도메인에 대한 다른 연결에서 볼 수 있듯이 이 맬웨어 샘플에서 사용하는 것은 도메인뿐만이 아닙니다.

NETWORK CONNECTIONS		
Destination	URLs	Security Categories
arthur.niria.biz (50.63.202.52)	1 ▾	Malware
althawry.org (184.168.221.44)	1 ▾	Malware
ahmediye.net (93.89.226.17)	1 ▾	
www.careerdesk.org (118.67.248.123)	1 ▾	Malware
sso.anbtr.com (195.22.28.222)	1 ▾	Malware
xso.apple-pie.in (92.54.28.100)	1 ▾	Phishing, Malware
apple-pie.in (92.54.28.100)	1 ▾	Phishing
amsamex.com (52.28.249.128)	1 ▾	Malware

1-8 of 8 < >

8. 워크플로를 완료하려면 다른 반복에서 Investigate 및 **Threat Grid** 를 사용하여 다른 도메인 중 일부를 탐색하여 위협 뷰를 확장할 수 있습니다.

실습 결론

이전 섹션에서 수집한 sso.anbtr[.com]과 관련된 정보를 바탕으로, 이제 이 도메인에 도달하는 여러 가지 고위험 동작 지표를 가진 트로이 목마로 분류된 맬웨어 샘플 목록을 사용하여 보기를 완료하십시오.

부록 A: Umbrella 구성 요소 및 용어에 대한 쿼 레퍼런스

용어	묘사
활동 보고	사용 추세에 대한 가시성 확보 데이터 손실 및 정보 억제를 해결하기 위한 새도 IT 서비스 식별 e-메일, 파일 공유, SaaS 서비스를 비롯한 조직 전체의 모든 클라우드 서비스 사용량 보기
AD 커넥터	Umbrella AD 커넥터는 고객이 기존 AD 구조를 Umbrella 로 처음 가져오고 지속적으로 동기화할 수 있도록 적어도 하나 이상의 DC 에 설치됩니다.

애니캐스트 라우팅	요청은 사용 가능한 가장 빠른 노드로 투명하게 전송되며, 다운타임 발생 시 자동으로 다시 라우팅. 모든 Umbrella 데이터 센터는 동일한 IP 주소를 발표.
AnyConnect 통합	이미 배치된 이동성 클라이언트를 활용하여 어디를 가든 사용자를 보호하십시오. 추가로 배포할 에이전트, 최종 사용자 조치 불필요, 성능 저하 불필요. Cisco AnyConnect 고객은 새 에이전트 없이도 엠브렐라 보호를 지원할 수 있음.
자율 시스템(AS)	접두사 및 라우팅 정책이 공통 관리 제어 하에 있는 라우터 모음입니다. 이것은 네트워크 서비스 제공자, 대기업, 대학, 회사의 부서 또는 회사의 그룹일 수도 있습니다. AS 는 해당 조직에 할당된 하나 이상의 IP 주소 블록(IP 접두사라고 함)으로 연결된 그룹을 나타내며, AS 외부의 시스템에 단일 라우팅 정책을 제공.
Autonomous System Number (ASN)	인터넷에서 각 AS 를 식별하는 데 사용되는 고유한 32 비트 번호. 이 숫자는 외부 라우팅 정보를 교환할 때, 특히 BGP 를 통해 여러 AS 를 통한 경로를 식별할 때 사용.
BGP 피어링	대기 시간 없이 보안 추가. 우리는 IXP 에 참여함으로써 500 개 이상의 인터넷 서비스 제공업체와 제휴하여 3,000 개 이상의 피어링 세션을 달성했습니다.
Border Gateway Protocol (BGP)	자율 시스템 간에 라우팅 및 도달성 정보를 교환하는 데 사용되는 프로토콜.
Cisco Cloudlock	Umbrella 는 조직 전체에서 액세스 중인 SaaS 애플리케이션을 식별하고, Cisco Cloudlock 은 위험하거나 부적절한 애플리케이션 사용을 식별하고 인증을 취소합니다. Cloudlock 은 Umbrella 의 API 를 사용하여 차단할 도메인에 대한 Umbrella 정보를 자동으로 전송합니다. 이러한 도메인은 사용자가 온 네트워크 및 오프 네트워크에 있을 때 차단됩니다.
Computer Incident Response Team (CIRT)	컴퓨터 보안 사건을 조사하고 해결하는 팀. SOC 보다 전문화된 기술(포렌식, 맬웨어 후진 등)을 갖는 경우가 많습니다.
컨텐츠필터링	네트워크 내/외부의 콘텐츠 가시성 및 제어 능력 확보 허용 가능한 사용 정책을 준수하십시오. 도메인의 포괄적인 데이터베이스가 실시간으로 업데이트됩니다. 도메인은 정책에 사용될 수 있는 60 개 이상의 범주로 구성됩니다.

공동 발생	같은 기간 동안 동일한 공격과 관련된 다른 도메인을 자주 검색합니다.
대시보드	<p>모든 정책 생성 및 보고에 웹 기반 열브렐라 대시보드를 사용하십시오. 단계별 정책 생성에 대해 간단한 정책 마법사를 사용하고 구현하기 전에 정책을 테스트하십시오.</p> <p>사용자 정의 블록/허용 목록, 정책 및 브랜드 블록 페이지를 생성하십시오.</p>
DNS 계층 적용	대부분의 인터넷 연결은 DNS 요청에 의해 시작되며, 열브렐라는 그것을 첫 번째 검사 포인트로 사용합니다. 이렇게 하면 지연 시간을 추가하지 않고 가장 빠른 시점에 악성 도메인 및 IP 에 대한 연결을 중지할 수 있습니다.
Domain Name System (DNS)	도메인 이름과 IP 주소를 연결하는 메커니즘.
도메인 이름	하나 이상의 IP 주소를 식별하는 데 사용되는 이름입니다. 모든 IP 를 기억하는 대신 인터넷 사이트에 접속하는 것이 더 쉽고 기억에 남는 방법입니다. 예: cisco.com.
어디에서나 인텔리전스 집행	Cisco Umbrella 를 사용하면 Investigate 에서 발견한 것과 동일한 알려진 긴급 위협은 연결이 되기 전에 DNS 계층에서 즉시 차단된다. 클라우드 제공 서비스를 통해 회사 네트워크의 기기를 보호하십시오.
파일 해시/해시	수학적 알고리즘(즉)에 의해 숫자 문자열로 변환된 파일. SHA256, SHA1, MD5). 파일의 지문과 모든 파일을 고유하게 식별할 수 있는 방법이라고 생각해 보십시오.
글로벌 네트워크	Umbrella 는 상위 인터넷 교환 지점(IXP)과 함께 위치한 25 개의 데이터 센터를 가지고 있습니다.
글로벌, 다양한 데이터	Umbrella 는 다양하고 글로벌하며 실시간인 데이터 세트를 기반으로 전례 없는 통찰력을 얻습니다. Umbrella 는 160 개 이상의 국가에서 85M 이상의 활성 사용자로부터 매일 100B 이상의 인터넷 요청을 처리합니다. 실시간 데이터는 Umbrella 의 글로벌 그래픽 데이터베이스에서 가져온 과거 데이터와 상호 연관되고 다양한 공용 및 개인 데이터 피드로 풍부합니다.

<p>지능형 프록시</p>	<p>Umbrella 지능형 프록시를 사용하면 위험 도메인에 대한 요청(악성 및 합법적인 콘텐츠를 호스팅하는 요청)만 보다 심층적인 검사를 위해 프록시 처리되어 기존 프록시에서 느끼는 성능 영향을 제거합니다. 모든 것을 프록시할 필요 없이 악의적인 사이트에 대한 액세스를 차단하고 DNS 계층의 좋은 사이트로의 트래픽을 허용하십시오. 바이러스 백신 엔진 및 Cisco Advanced Malware Protection 파일 평판 서비스와 대조하여 위험 사이트에서 파일을 다운로드하려고 시도했는지 확인하십시오. 우리의 프록시는 성능 향상을 위해 자동으로 확장되는 마이크로서비스 아키텍처를 사용하여 구축되었습니다.</p> <p>타협 지표.</p>
<p>IOC</p>	
<p>IP 주소</p>	<p>통신을 위해 인터넷 프로토콜을 사용하는 네트워크에 참여하는 각 장치(예: 컴퓨터, 프린터)에 할당된 숫자 라벨. 예제: 208.67.222.222.</p>
<p>IP 지리 위치</p>	<p>사용자가 IP 주소를 요청하는 위치와 관련된 IP 주소의 지리적 위치 (즉, IP 주소는 러시아에서 호스팅되지만, 모든 트래픽은 미국에서 발생하기 때문에 매우 의심스럽습니다.)</p>
<p>IP 계층 시행</p>	<p>맬웨어가 DNS 를 사용하는 대신 IP 주소에 직접 연결하려고 할 때, 업브렐라는 로밍 클라이언트나 Cisco AnyConnect 통합을 사용하여 회사 네트워크 안팎에서 IP 계층 적용을 제공합니다.</p>
<p>실시간 보기 이력 컨텍스트 포함</p>	<p>조사는 인터넷 도메인의 생성과 진화의 역사적 맥락과 인터넷에 대한 실시간 최신 관점을 결합하합니다.</p>
<p>Amazon S3 를 사용한 로그 관리</p>	<p>필요한 기간 동안 DNS 로그를 안정적으로 유지하십시오.</p> <p>Umbrella 에서 Amazon AWS S3 버킷으로 DNS 로그를 전송하십시오.</p> <p>SIEM 또는 기타 시스템과 통합</p> <p>보안 가시성을 향상하여 문제 대응 및 정책 컴플라이언스 향상</p>
<p>네트워크 장치 통합</p>	<p>몇 분 안에 게스트 및 기업용 Wi-Fi 를 보호</p> <p>고객이 장치 인터페이스의 상자를 확인하여 모든 인터넷 트래픽에 대해 엠브렐라 보안을 프로비저닝할 수 있도록 하는 네트워크 장치 공급자(일반 라우터)와의 기술 제휴.</p> <p>Cisco 4000 ISR 시리즈 및 Cisco Wireless LAN 컨트롤러와 통합.</p>

네트워크상의 커버리지/Umbrella 네트워크	기존 DNS 및 DHCP 인프라를 활용하여 네트워크 전반에 걸쳐 프로비저닝 여기에는 네트워크에 연결하는 모든 장치 설치할 하드웨어가 없거나 유지 관리할 소프트웨어가 없는 조직 소유가 아닌 장치도 포함. 모든 DNS 서버, 라우터, 게이트웨이 또는 Wi-Fi 액세스 지점에서 Umbrella 글로벌 네트워크 IP 주소로 직접 인터넷 활동.
파트너 및 맞춤형 통합	사내 보안 어플라이언스에서 경계 범위를 넘어 장치 및 사이트로 보안 위협 방지 확장 기존 시스템에서 로컬 위협 탐지 및 인텔리전스를 글로벌 위협 예방으로 프로그래밍하십시오. 감지 및 예방 시간을 며칠에서 몇 초로 단축하기 위해 IOC(타협의 지표)에 즉시 조치를 취한다. 기존 보안 어플라이언스 및 위협 인텔리전스 플랫폼 또는 피드에서 위협 인텔리전스를 엄브렐라로 전송하십시오. 사내 톨을 사용하여 최대 10 개의 사용자 정의 통합 생성
정책 테스터	시뮬레이션을 실행하여 관리자가 안심하고 정책을 구현할 수 있도록 의도한 방식으로 정책이 시행되는지 확인하십시오.
예측 인텔리전스	우리는 통계적 모델을 실시간 및 과거 데이터에 적용하여 악성일 가능성이 있는 도메인과 새로운 공격의 일부를 예측.
로밍 클라이언트	트위크 경계를 넘어 랩톱으로 보호 확장 네트워크상의 특정 엔드포인트에 작업을 고정하여 업데이트 적용 시간을 단축하십시오. 모든 시행은 기기가 아닌 클라우드에서 이루어지기 때문에 클라이언트는 경량 상태를 유지합니다. 네트워크에 관계없이 Umbrella 보안 및 정책 기반 보호를 적용할 수 있도록 지원하는 Windows 및 Mac OSX 컴퓨터용 경량 클라이언트.
Security Information and Event Management (SIEM)	엔드포인트/네트워크 하드웨어 및 애플리케이션에 의해 생성된 보안 경고를 수집하고 상호 연관시키는 기술. 컴플라이언스/보안 목적으로 보안 데이터를 기록하고 보고서를 생성하는 데 사용됨
Security Operations Center (SOC)	회사의 IT 시스템(웹 사이트, 애플리케이션, 데이터베이스, 데이터 센터 및 서버, 네트워크, 데스크톱 및 기타 엔드포인트)을 모니터링, 평가 및 방어하는 지정된 팀.

<p>보안 연구원</p>	<p>Cisco Umbrella 의 보안 연구자는 고급 데이터 마이닝 기술, 3D 시각화 및 보안 영역 전문 지식을 활용하여 Investigate 의 배후 인텔리전스를 개발하는 데이터 과학자, 엔지니어, 수학자 및 보안 연구자 팀입니다. Cisco Umbrella 보안 연구자들은 지속적으로 연결을 찾고 미래의 위협을 예측하기 위해 데이터를 분석하는 새로운 방법을 고안합니다. Cisco 의 연구는 전세계 보안 회의의 빈번한 블로그 게시물과 발표에서 보여드립니다.</p>
<p>통계 및 기계 학습 모델</p>	<p>이러한 모델은 자동으로 데이터를 점수화하고 분류하여 엠브렐라가 이상 징후를 탐지하고 알려진 긴급한 위협을 밝혀낼 수 있도록 합니다. 이 모델들은 공격자들이 어디에서 인터넷 기반구조(도메인, IP, ASN)를 운영하고 있는지 발견합니다. 이들은 도메인과 IP 의 진화를 전체적으로 보기 위해 과거 데이터와 실시간 데이터를 모두 연관시켜 악성일 가능성이 높고 향후 공격에 사용될 수 있는 대상을 예측합니다.</p>
<p>엠브렐라 조사</p>	<p>조사는 인터넷을 통해 도메인, IP 및 멀웨어에 대한 위협 인텔리전스를 제공합니다. DNS 요청 및 기타 상황별 데이터에 대한 실시간 그래프를 활용하여 Investigate 는 인터넷 도메인, IP 및 멀웨어의 관계와 진화를 가장 완벽하게 파악하여 공격자의 인프라를 파악하고 향후 위협을 예측하는 데 도움이 됩니다</p>
<p>WHOIS 기록 데이터</p>	<p>에는 연락처 정보 및 시간 경과에 따른 변경 사항을 포함 하여 도메인을 등록 한 시간 및 위치를 등록 한 사용자에 대한 정보를 제공합니다. 우리의 지능은 동일한 연락처 정보를 사용하여 등록 된 모든 악의적인 도메인을 가시성을 제공합니다. 이는 공격을 함께 하는 데 사용할 수 있습니다.</p>

부록 B. 엠브렐라 테스트 사이트 목록

테스트	URL	가능성
멀웨어 테스트 사이트	http://examplemalwaredomain.com/	모든
봇넷 시험장	http://examplebotnetdomain.com/	모든
피싱 테스트 사이트	http://internetbadguys.com/	모든
지능형 프록시 테스트 사이트	http://proxy.opendnstest.com/	통찰력 또는 플랫폼
SSL 암호 해독을 통한 지능형 프록시 테스트 사이트	https://ssl-proxy.opendnstest.com/	통찰력 또는 플랫폼
IP 계층 적용을 위한 테스트 사이트	http://67.215.70.91	통찰력 또는 플랫폼

정책 테스트 사이트

<http://policy-debug.opendns.com/>

모든



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)