내부 감염원 확인

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[봇넷 활동을 보고하는 내부 DNS 서버](#)

[다음 단계](#)

[서버 이전 2016 운영 체제 고려 사항](#)

[추가 옵션](#)

소개

이 문서에서는 Cisco Umbrella에서 내부 감염원을 식별하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

봇넷 활동을 보고하는 내부 DNS 서버

Umbrella Dashboard(Umbrella 대시보드)에서 네트워크 또는 사이트 중 하나에 대해 로깅된 예기치 않은 트래픽 또는 악성코드/봇넷 식별 트래픽이 대량으로 표시되는 경우 내부 호스트가 감염될 가능성이 높습니다. DNS 요청이 내부 DNS 서버를 거칠 가능성이 높기 때문에 요청의 소스 IP가 DNS 서버의 IP로 대체되므로 방화벽에서 추적하기가 어렵습니다.

이러한 경우에는 Umbrella 대시보드를 사용하여 소스를 식별할 수 없습니다. 모든 요청은 네트워크 ID에 대해 로깅할 수 있습니다.

다음 단계

몇 가지 할 수 있는 작업이 있지만, 이 동작을 추적할 수 있는 다른 보안 제품이 없으면 주된 방법은 DNS 서버의 로그를 사용하여 요청이 들어오는 위치를 확인한 다음 소스를 삭제하는 것입니다.

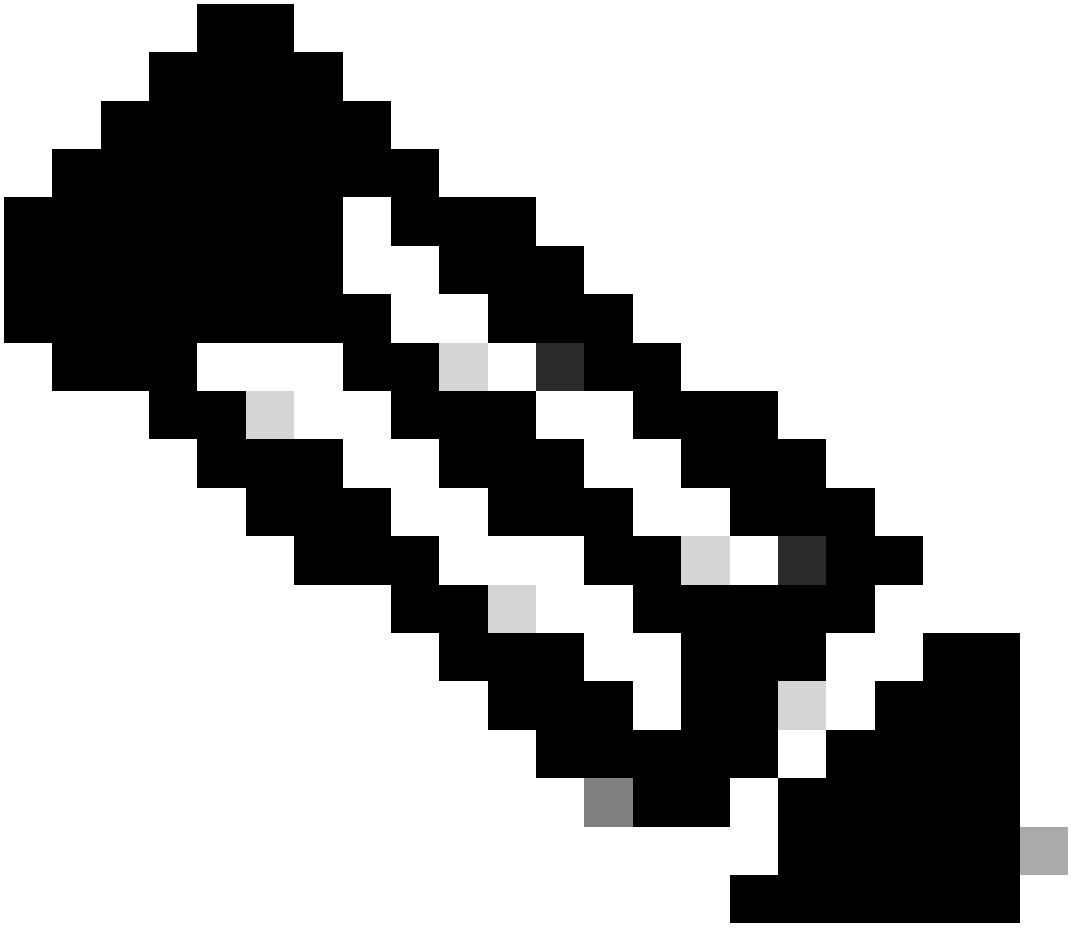
일반적으로 Umbrella는 VA(Virtual Appliance)를 실행할 것을 권장합니다. 다른 이점 중 하나는 내부 네트워크의 모든 DNS 트래픽에 대한 호스트 수준의 가시성을 제공하고 이러한 유형의 문제를 신속하게 찾아냅니다.

그러나 Umbrella Support는 DNS를 VA로 가리키지 않는 내부 호스트가 감염되어 Windows DNS 서버를 통해 DNS 요청을 보내는 문제를 확인하는 경우가 있습니다. 이 시나리오에서는 VA가 DNS 요청(및 그에 따른 소스 IP 주소)을 확인할 수 있는 방법이 없으므로 해당 DNS 서버를 통과하는 모든 DNS 쿼리는 네트워크 또는 사이트에 대해 로깅될 수 있습니다.

서버 이전 2016 운영 체제 고려 사항

그러나 Pre-Server 2016 운영 체제에서는 이 정보가 기본적으로 기록되지 않습니다. 데이터를 캡처하려면 수동으로 활성화해야 합니다. 특히 2012r2의 경우 Microsoft에서 핫픽스를 설치하여 이 로깅 수준을 사용할 수 있습니다.

다른 OS의 경우 및 DNS 서버에서 디버그 로깅을 설정하는 방법에 대한 자세한 내용을 보려면 이 Microsoft 문서에서 옵션 및 사용법을 간략하게 설명합니다.



참고: 이러한 옵션의 컨피그레이션 및 사용은 Umbrella Support의 범위에 속하지 않습니다.

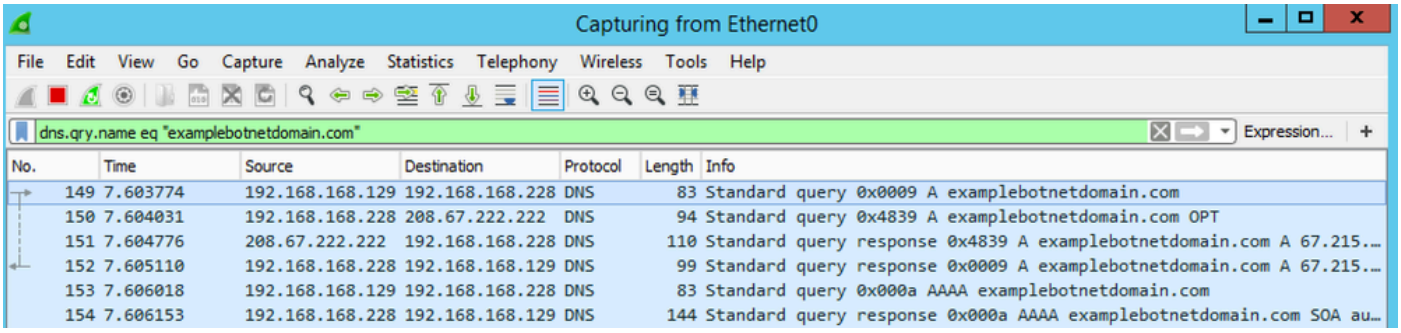
추가 옵션

DNS를 찾기 위해 실행 중인 필터를 남겨두고 Wireshark 캡처를 실행할 수 있으며 대상 Umbrella가 대시보드에서 로깅하고 있습니다. 그런 다음 요청의 소스를 찾을 수 있도록 충분한 가시성을 확보할 수 있습니다.

예를 들어, DNS 서버에서 실행된 이 캡처는 클라이언트(192.168.168.129)가 DNS 서버(192.168.168.228)에 요청을 한 다음 DNS 서버가 Umbrella Anycast 서버(208.67.222.222)에 쿼리를 수행하여 응답을 받고 이를 클라이언트로 다시 제공하는 것을 보여줍니다.

필터 제안은 다음과 같습니다.

```
dns.qry.name contains examplebotnetdomain
dns.qry.name eq "examplebotnetdomain.com"
```



예제botnetdomain.png

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.