데이터시트

CYGNA LABS DNS 방화벽

당신의 인프라를 멀웨어로부터 보호하세요.

모든 것은 DNS로 시작하고 끝납니다.

멀웨어를 미리 차단하세요. Cisco에 따르면 약 90% 이상의 멀웨어가 DNS를 사용하고 있습니다. Cygna Labs DNS 방화벽은 멀웨어 통신을 차단하는데 큰 효과가 있습니다.

멀웨어에 감염된 장치들은 통신을 위해 DNS(Domain Name System)에 의존합니다. 이 장치들은 DNS를 사용하여 명령 센터의 IP 주소를 찾고 귀하의 조직에서 중요한 정보를 유출할 수 있습니다.

양날의 검: DNS의 보편성

기업 네트워크에서는 DNS가 모든 장치에 대한 인터넷 통신의 필수 요소이므로, 대부분의 경우 방화벽이 DNS 트래픽을 허용합니다. 이것을 이용해 멀웨어에 감염된 장치는 DNS를 사용해 멀웨어 컨트롤러의 명령 센터(분산되어 있는 멀웨어에게 명령이나 소프트웨어를 전달하기 위해 사용되는 파일이나 웹 서버) IP 주소를 찾습니다. 그런 다음 멀웨어는 명령 센터의 명령을 실행하는 기업 네트워크 내 원격 봇으로 작동합니다.

Cisco 보안 연구 결과에 따르면 조직의 68%가 재귀 DNS를 모니터링하지 않는다고 합니다. Cygna Labs의 DNS 방화벽으로 재귀 DNS를 모니터링하고 보호하세요. 출처: Lystrup, Owen. Cisco 보안 보고서, 2016년 1월 21일

지능형 지속 공격 (APT, Advanced Persistent Threats)

DNS 서비스는 www 주소를 IP 주소로 변환하여 웹사이트를 쉽게 접속할 수 있도록 돕는 중요한 역할을 합니다. 사이트 관리자들은 이 기능을 이용해 서버의 IP 주소를 변경하고 DNS를 업데이트하여 쉽게 새로운 도메인과 IP 주소를 매핑합니다.

멀웨어 운영자도 DNS 기능과 다른 기능들을 악용해 DNS 쿼리로 명령 센터를 찾아 정보를 유출시키고, 자신들이 감지될 경우 IP 주소 필터링을 피하기 위해 IP 주소를 변경 또는 변조합니다. 이와 같은 회피 기술들은 멀웨어가 네트워크 내에서 지속되고, 공격자를 대신하여 은밀하게 공격을 실행할 수 있도록 합니다.

실질적인 정보

Cygna Labs DNS 방화벽은 네트워크를 멀웨어의 통신 시도 초기 단계부터 보호합니다. 알려진 멀웨어 및 비정상적인 도메인에 대한 쿼리를 차단하거나 리디렉션하여 감염된 장치가 소프트웨어나 공격 명령을 받는 것을 예방할 수 있습니다. 또한 Cygna Labs DNS 방화벽은 재귀 DNS 서버에 대한 방화벽 피드 업데이트를 지속적으로 제공하여 네트워크를 보호하고, 감염된 장치를 식별하고 대응할 수 있도록 지원합니다.

CYGNA LABS

다양한 측면의 필터링

Cygna Labs DNS 방화벽은 사용자가 알려진 멀웨어 도메인 및 악성 도메인에 접근하는 것을 막을 뿐만 아니라, 불건전하거나 과격한 콘텐츠가 포함된 사이트에 대한 DNS 응답을 필터링하는 정책을 정의할 수 있습니다.

방화벽 정책

Cygna Labs DNS 방화벽은 알려진 악성 사용자의 도메인 및 IP 주소를 기반으로 다양한 트리거를 제공하여 정책을 활성화하거나 비활성화할 수 있습니다. 다음과 같이 각 범주에 적용할 방화벽 정책을 선택할 수 있습니다:

- 클라이언트에 대한 응답 거절
- "찾을 수 없음"("NXDOMAIN")으로 응답
- "데이터 없음"("NODATA")으로 응답
- 주어진 IP 주소로 리디렉션, 예: 종속 포털(Captive Portal)
- TCP를 활성화하기 위해 "truncated" 헤더 비트로 응답
- 통과 ("화이트리스트")

실질적인 보고

귀하의 DNS 서버에 쿼리하는 장치가 정책이 존재하는 도메인을 요청하면, 요청 장치의 IP 주소를 포함한 로깅 경보가 생성됩니다. 이를 통해 멀웨어 감염을 조사하고 문제가 되는 장치를 추적할 수 있습니다. 또한 중앙 관제 시설에서 기록 보고 및 추적도 가능합니다.

DNS 방화벽 이점

Cygna Labs DNS 방화벽에는 다음과 혜택을 지원하는 정기적인 업데이트가 포함된 간편한 구독 서비스를 제공합니다:

- 네트워크 보안 강화: DNS는 통신의 첫 단계로, 멀웨어 통신을 억제하는 주요 단계로 작용하여 전반적인 네트워크 보안을 강화합니다.
- 적시에 방화벽 업데이트 제공: 공격자(해커)들은 빠르게 새로운 공격 방법을 고안합니다. 따라서 Cygna Labs DNS 방화벽 피드는 정책을 최신으로 유지하기 위해 하루에 여러 번 업데이트합니다.
- 멀웨어 콜백(Callback) 예방: 약 91% 이상의 멀웨어가 다양한 방법으로 DNS를 사용하므로, DNS 레이어에서의 접근 제어는 이러한 멀웨어의 작동을 억제할 수 있습니다.
- 감염된 장치 식별: 정책 로깅 및 보고를 통해 정책이 적용되는 쿼리를 요청하는 장치를 식별하여 대응할 수 있습니다.
- 쉬운 방화벽 맞춤 설정: 많은 방화벽 서비스가 제어할 수 없는 정적 피드를 제공하지만, 저희 방화벽 서비스는 네트워크를 더욱 안전하게 보호하기 위해 필터 및 관련 정책을 구성할 수 있도록 해줍니다.
- 간편한 구현: Cygna Labs DNS 방화벽 구독 피드는 프로토콜 메시지와 디지털 서명을 통합하여 프로토콜 변경이나 인터넷 방화벽 구성 변경 없이 방화벽 정보를 안전하게 유지할 수 있습니다.

Toll Free: (844) 442-9462

International: +1 (305) 501-2430

Fax: +1 (305) 501-2307

CYGNA LABS