AKAMAI 사례 연구

Enterprise Threat Protector로 보안 체계를 개선한 대형 제조사

요구 사항

- 기존에 적용된 보안 제품군에 추가적인 방어 레이어 구축
- 네트워크 중단 최소화
- 최소한의 지원으로도 문제를 해결할 수 있는 셀프 서비스 기능

상황

유럽의 한 제조사는 진화하는 사이버 보안 위협에 맞서 자사의 보안 체계를 전반적으로 개선하고자 했습니다. 이 제조사는 Akamai와 첫 미팅을 할 당시에 구체적으로 어떤 보안 레이어를 추가해야 할지 알지 못했고 Akamai에 잠재적인 보안 허점이 무엇인지 파악해 달라고 요청했습니다. Akamai는 이 제조사에 Enterprise Threat Protector를 제안했고, 고객은 기존의 보안 취약점을 해결하고, 사용 편의성이 높고, 구축 후 필요한 지원이 최소한으로 유지되는 Enterprise Threat Protector에 관심을 보였습니다. 고객은 미팅 후 바로 무료 체험을 신청했습니다.

무료체험 프로그램

무료 체험을 시작한 지 몇 주 되지 않아 고객사 네트워크에 접속하는 7천 건의 DNS 요청이 Akamai 보안 목록에 의해 잠재적 보안 위협인 것으로 확인되었습니다. Akamai 팀이 해당 DNS 요청을 추가로 분석해 보니 Conficker.B 멀웨어의 C&C 요청이라는 사실이 드러났습니다. Downup, Downadup, Kido라는 이름으로도 불리는 Conficker 멀웨어는 Windows 운영 체제를 표적으로 하는 컴퓨터 웜입니다. Windows OS 소프트웨어의 결함을 악용하고 관리자 암호를 알아내기 위해 사전대입 공격(암호를 사전순으로 생성하여 대입하는 공격)을 하는 봇넷을 만들어내는데 각종 첨단 멀웨어 기법을 이용하기 때문에 탐지하기가 매우 어렵습니다.

Enterprise Threat Protector는 Cryptolocker 및 Locky 랜섬웨어를 배포하는 것으로 알려진 DNS 요청이 정상 웹사이트로 가고 있다는 것을 탐지했습니다. 기업의 네트워크에 침입한 Conficker 멀웨어는 네트워크 내부를 자유롭게 이동하며 엔드포인트 디바이스와 서버의 파일을 암호화합니다. 랜섬웨어는 많은 기업들에게 심각한 보안 위협이며 지난 12개월 동안 여러 건의 대형 공격에 이용돼 왔습니다.

고객사는 무료체험 기간 동안 Enterprise Threat Protector가 보여준 결과에 만족했고, 기업을 위협으로부터 선제적으로 보호하는 방편으로서 Enterprise Threat Protector가 매우 효과적임을 인정했습니다.

Why Akamai?

무료체험을 성공적으로 마친 고객사는 기존의 보안 제품군에 더해 Enterprise Threat Protector를 도입하기로 결정했습니다. Enterprise Threat Protector는 엔드포인트 안티바이러스 솔루션, Dell 방화벽 등 기존 보안 제품과 간편하게 통합되었을 뿐 아니라 새로운 위협을 실시간으로 알려주는 인텔리전스를 바탕으로 앞으로 일어날 공격을 사전에 효과적으로 차단하는 방편으로 기능했습니다.

고객사의 외부 리커시브 DNS 트래픽이 Enterprise Threat Protector로 전달되면 실시간으로 도메인의 리스크 점수를 책정하는 Akamai의 위협 인텔리전스를 기반으로 사용자가 요청한 도메인이 확인됩니다. 고객사는 덕분에 사용자와 디바이스가 악성 도메인과 서비스에 접속하는 것을 선제적으로 차단할 수 있게 되었습니다. 게다가 도메인을 확인한 후에 IP 접속이 이루어지기 때문에 기업의 보안 경계(perimeter)에서 멀리 떨어진 곳에서 보안 위협이 차단됩니다. 고객은 무엇보다 Enterprise Threat Protector가 사용하기 쉽고, 네트워크를 크게 변경할 필요가 없고, 전사적으로 일관된 정책을 적용할 수 있다는 점에서 매우 만족했습니다.

Akamai는 최고의 신뢰를 받고 있는 세계 최대의 클라우드 전송 플랫폼으로 고객이 사용하는 장소와 디바이스에 상관없이 안전하고 원활한 디지털 경험을 쉽게 제공할 수 있도록 지원합니다. 전 세계 각지에 촘촘히 분산 배치된 Akamai 플랫폼은 130개 국가에 위치한 20만 대 이상의 서버로 구성되어 있으며 고객에게 탁월한 성능을 제공하고 위협을 방어합니다. 웹·모바일 성능, 클라우드 보안, 기업 애플리케이션 접근, 비디오 전송 솔루션으로 구성된 Akamai의 제품군에는 탁월한 고객 서비스와 24시간 모니터링이 따릅니다. 대표적인 금융 기관, 이커머스 기업, 미디어·엔터테인먼트 사업자, 정부 기관이 Akamai를 신뢰하는 이유를 알아보려면 Akamai 홈페이지(www.akamai.com) 또는 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 @Akamai를 팔로우하십시오. 전 세계 Akamai 연락처 정보는 www.akamai.com/locations에서 확인할 수 있습니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표전화는 02-2193-7200입니다. 2017년 12월 발행.