FIREEYE EMAIL SECURITY (EX 시리즈)

이메일 기반 위협에 대한 지능적이고 확장 가능한
적응형 방어 시스템

EX 5400과 EX 8420 (EX 3400, EX 8400은 사진이 없음)

요약

FireEye Email Security(EX 시리즈)는 지능형 이메일 공격을 방어합니다. FireEye Global Threat Management Platform의 핵심 컴포넌트인 FireEye Email Security는 시그니처리스 기술을 사용하여 모든 이메일 첨부 파일을 분석하고 지능형 표적 공격에 사용되는 스피어 피싱 이메일을 성공적으로 격리합니다.

모든 개인 정보를 온라인으로 수집할 수 있기 때문에, 사이버 공격자는 사회 공학을 이용하여 거의 모든 사용자에게 URL을 클릭하거나 첨부 파일을 열도록 유도할 수 있습니다. FireEye Email Security는 기존의 방어 시스템을 회피하는 스피어 피싱, 랜섬웨어 및 인증 피싱 공격에 대한 실시간 위협 방어를 제공합니다. 또한 FireEye Network Security(NX 시리즈)와 연계하여 혼합 공격에 대해 새로운 차원의 위협 방어를 제공함으로써, 악성 URL이 표시된 이메일을 격리하고, 웹 기반의 공격을 추적하여 최초의 스피어 피싱 이메일을 확인합니다.

주요 기능

- 스피어 피싱 이메일 공격 방어
- 인증 피싱 자동 탐지 및 방어
- "비슷하지만 다른" 도메인 탐지로 인증 피싱(타이포스쿼팅) 감소
- FireEye NX와 통합하여 다중 위협 경로에 대한 혼합 공격 차단
- 탐지하기 힘든 다단계 악성코드 캠페인 식별 및 저지
- 제로데이 익스플로잇, ZIP/RAR/TNEF 아카이브에 숨겨진 공격, 악성 URL 등의 위협 이메일 분석
- 암호 보호 및 샌드박스 회피 등의 회피 기술 방어
- MTA와 같은 능동적 보호 모드 또는 모니터 모드(SPAN/BCC)로 배포
- 악성 이메일을 격리시키고 옵션으로 사용자 통지 제공
- 위협의 실시간 및 소급 탐지 제공
- 활용 가능한 위협 인텔리전스와 경보 연결
- 메시지 가시성, 추적 및 관리 제공

FireEye
SECURITY REIMAGINED

악성 이메일의 실시간 격리

FireEye Email Security는 스피어 피싱 이메일을 차단하기 위해 오늘날의 지능형 공격을 정확하게 식별하기 위한 목적으로 개발된 FireEye MVX(Multi-vector Virtual Execution™) 엔진을 사용하여 모든 첨부 파일과 URL을 분석합니다. 공격이 확인되면 FireEye Email Security에서 추가 분석이나 삭제를 위해 악성 이메일을 격리합니다.

웹과 이메일 위협 벡터에 대한 혼합 공격 방어

지능형 공격은 다중 벡터 공격 전략의 전초전으로 스피어 피싱을 사용합니다. FireEye EX는 전체 공격 라이프사이클을 밝혀내기 위해서 종종 FireEye NX 및 Central Management 시리즈와 함께 설치되어 악성 URL을 최초의 이메일 및 의도된 목표와 상호 연관시킵니다. 그런 다음 FireEye Central Management가 새로운 악성코드 인텔리전스를 설치된 전체 FireEye 시스템에 실시간 및 로컬로 배포합니다.

제로데이 이메일 공격에 대한 동적 분석

FireEye Email Security는 시그니처리스 FireEye MVX 엔진을 사용하여 OS, 브라우저, 애플리케이션 취약점 및 일반적인 파일과 멀티미디어 콘텐츠에 내장된 악성코드를 이용하는 지능형 공격을 저지합니다. MVX 엔진은 버퍼 오버플로 상태를 만들기 위해 악용하는 취약점과 데이터를 유출하기 위해 사용하는 콜백 좌표 같은 위협에 대한 포렌식 세부 사항을 보고합니다.

기업에 대한 위협 인텔리전스 공유

분석 결과에 따라 동적으로 생성하는 실시간 위협 인텔리전스는 모든 FireEye 제품이 FireEye Central Management 플랫폼과의 통합을 통해 로컬 네트워크를 보호하는 데 도움이 될 수 있습니다.

이 인텔리전스는 FireEye DTI(Dynamic Threat Intelligence™) 클라우드를 통해 전세계에서 공유하여 모든 가입자에게 새로 출현한 위협에 대해 통지할 수 있습니다.

맞춤화할 수 있는 YARA 기반의 룰

FireEye Email Security는 맞춤형 YARA 규칙을 지원하여 보안 분석가가 해당 조직을 표적으로 삼는 위협이 포함된 이메일 첨부 파일을 분석하는 규칙을 지정하고 테스트할 수 있게 합니다.

기술 사양

	EX 3400	EX 5400	EX 8400	EX 8420
성능 *	최대 150,000건/일의 이메일	최대 300,000건/일의 이메일	최대 600,000건/일의 이메일	최대 600,000건/일의 이메일
네트워크 인터페이스 포트	2x10/100/1000BASE-T 포트	2x10/100/1000BASE-T 포트	2x10/100/1000BASE-T 포트	2x 1000 BASE-SX 광섬유 포트(LC 멀티모드)
관리 포트	1x10/100/1000BASE-T 포트	1x10/100/1000BASE-T 포트	1x10/100/1000BASE-T 포트	1x10/100/1000BASE-T 포트
IPMI 포트(후면 패널)	포함	포함	포함	포함
전면 패널 LCD 및 키패드	포함	포함	포함	포함
PS/2 키보드 및 마우스, DB15 VGA 포트(후면 패널)	포함	포함	포함	포함
USB 포트(후면 패널)	2x 타입 A USB 포트	2x 타입 A USB 포트	2x 타입 A USB 포트	2x 타입 A USB 포트
시리얼 포트(후면 패널)	115, 200bps, 패리티 없음, 8 비트, 1 정지 비트	115, 200bps, 패리티 없음, 8 비트, 1 정지 비트	115, 200bps, 패리티 없음, 8 비트, 1 정지 비트	115, 200bps, 패리티 없음, 8 비트, 1 정지 비트
저장 능력	2x600GB HDD, RAID 1, 2.5인치, FRU	2x600GB HDD, RAID 1, 2.5인치, FRU	2x600GB HDD, RAID 1, 2.5인치, FRU	2x600GB HDD, RAID 1, 2.5인치, FRU
엔클로저	1RU, 19인치 랙에 맞음	1RU, 19인치 랙에 맞음	1RU, 19인치 랙에 맞음	1RU, 19인치 랙에 맞음
섀시 크기(WxDxH)	17.2" x 27.8" x 1.70" (437 x 706 x 43.2mm)	17.2" x 27.8" x 1.70" (437 x 706 x 43.2mm)	17.2" x 28.0" x 3.41" (437 x 711 x 86.6mm)	17.2" x 28.0" x 3.41" (437 x 711 x 86.6mm)
AC 전원	중복 (1+1) 750와트, 100-240 VAC 9 - 4.5A, 50-60 Hz, IEC60320-C14 인렛, FRU	중복 (1+1) 750와트, 100-240 VAC 9 - 4.5A, 50-60 Hz, IEC60320-C14 인렛, FRU	중복 (1+1) 750와트, 100-240 VAC 9 - 4.5A, 50-60 Hz, IEC60320-C14 인렛, FRU	중복 (1+1) 750와트, 100-240 VAC 9 - 4.5A, 50-60 Hz, IEC60320-C14 인렛, FRU
DC 전원	해당 없음	해당 없음	해당 없음	해당 없음
최대 전력 소비(와트)	296와트	468와트	509와트	509와트
최대 열 방산(BTU/h)	1010BTU/h	1597BTU/h	1737BTU/h	1737BTU/h
MTBF(h)	35,400h	34,600h	59,800h	59,800h
어플라이언스만/발송 중량(lb.) (kg)	31lb. (14kg)/46lb. (21kg)	32lb. (15kg)/47lb. (21kg)	42lb. (19kg)/58lb. (26kg)	42lb. (19kg)/58lb. (26kg)
보안 인증	CC NDPP v1.1	CC NDPP v1.1	CC NDPP v1.1	CC NDPP v1.1
작동 온도	10˚C-35˚C	10˚C-35˚C	10˚C-35˚C	10˚C-35˚C
작동 상대 습도	10%-85% (비응축)	10%-85% (비응축)	10%-85% (비응축)	10%-85% (비응축)
작동 고도	5,000ft	5,000ft	5,000ft	5,000ft

주: 모든 성능 수치는 시스템 설정과 처리 중인 트래픽 프로파일에 따라 달라집니다.

활용 가능한 위협 인텔리전스

FireEye Email Security에서 생성하는 경보는 FireEye ATI(지능형 위협 인텔리전스) 포털과 옵션으로 결합하여 공격과 관련된 발원지, 심각도, 위험, 완화 옵션 및 다른 상황 정보에 대한 이해를 제공합니다. 이 포털은 통계에 대한 풍부한 시각화를 제공하므로, 보안팀은 중요한 상황 정보와 트렌드를 신속하게 관찰할 수 있습니다.

FireEye 인텔리전스에 대한 심층적인 통찰력을 얻기 위한 추가 옵션은 ATI+입니다. ATI+ 가입자는 FIC(FireEye 인텔리전스 센터)와 지속적인 모니터링에 접속할 수 있습니다.

FIC는 지능형 위협 그룹에 대한 종합적인 관련 자료, 동향, 뉴스 및 분석과 표적 산업의 프로파일을 제공합니다. FireEye 분석가가 지속적 모니터링을 통해 중요 경보 및 탐지 효과 모니터링을 연중무휴로 제공합니다.

메시지 큐 관리

FireEye Email Security는 이 플랫폼이 스캔하는 이메일 메시지에 대한 고도의 제어를 제공합니다. 능동적 방어 모드 설치의 경우 MTA 큐를 통해 이동할 때 메시지를 추적 및 관리하고, 이메일 특성을 사용하여 메시지가 수신, 분석 및 넥스트 홉으로 전달되었는지 검색 및 검증하고, 시간 경과에 따라 직관적 대시보드를 통해 동향을 모니터링할 수 있습니다. 명백한 허용 및 차단 리스트는 이메일 처리에 대한 맞춤형 제어를 제공합니다.

FireEye, Inc. 소개

FireEye는 인텔리전스 기반의 보안 회사입니다. FireEye는 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영의 완벽한 확장을 지원합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다. FireEye는 포브스 글로벌 2,000개 기업 중 825개 기업을 포함해 67개국의 5,300여 기업을 고객으로 보유하고 있습니다.

FireEye에 대한 더 자세한 정보를 원하시면 다음의 웹사이트를 방문하십시오.
www.fireeye.com

FireEye Korea |
서울특별시 강남구 테헤란로 534 글라스타워 20층|
02.2092-6580 | korea.info@fireeye.com | www.fireeye.kr

www.FireEye.com

FireEye