FireEye Email Security (EX 시리즈)

이메일 위협에 대한 지능적, 확장 가능한 방어 시스템

그림 1. EX 3500, EX 5500 및 EX 8500.

주요 기능

- 스피어 피싱 및 기타 지능형, 다단계, 제로데이 공격에 대한 포괄적인 이메일 보안 기능 제공
- 클라우드 버스팅으로 메시지 처리량이 최고치일 때 추가적인 탐지 분석 기능 제공
- Microsoft Windows 및 Apple Mac OS X 운영 체제 이미지에 대한 분석 지원
- 암호화된 첨부 파일 및 악성 URL을 비롯하여 파일에 숨겨진 위협을 탐지하기 위한 이메일 분석
- 인증 피싱을 자동으로 탐지하여 줄이거나 철저히 방어
- 위협의 우선 순위를 정하고 억제할 수 있도록 경보에 대한 상황별 통찰력 제공
- FireEye의 다양한 기술들과 통합
- 능동적 방어 모드 또는 모니터 전용 모드로 온프레미스 설치
- 메시지 및 경보의 가시성, 추적 및 관리 제공

요약

이메일은 데이터가 가장 많이 들어오는 지점이기 때문에 사이버 공격에 가장 취약한 벡터입니다. 조직들은 이메일 기반의 스팸 및 바이러스부터 표적화된 지능형 위협까지, 급증하는 보안 위험에 직면해 있습니다. 이메일을 통해 침투하는 위협은 대부분 무기화된 첨부 파일, 악성 링크 및 인증 피싱의 형태로 수신됩니다. 안티스팸 필터 및 안티바이러스는 알려진 악성 첨부 파일, 링크 및 콘텐츠를 이용하는 전통적인 대규모 이메일 피싱 공격을 포착하는 데에는 효과적이지만, 이러한 솔루션을 우회하도록 고안된 정교한 스피어 피싱 공격은 포착하지 못합니다. 이메일은 고도로 표적화/맞춤화하여 성공적으로 악용할 가능성을 높일 수 있기 때문에 지능형 공격을 개시하거나 랜섬웨어를 전달하는 주된 수단으로 꾸준히 이용되고 있습니다.

FireEye 이메일 보안은 침해의 위험과 피해를 최소화하는 데 목적을 맞추고 있습니다. 이메일 보안(EX 시리즈) 온프레미스 어플라이언스는 스피어 피싱 및 랜섬웨어를 비롯한 지능형/표적 공격이 귀사의 환경에 침입하기 전에 정확히 탐지하고 즉각적으로 차단할 수 있습니다. 이메일 보안은 시그니처리스 다중 벡터 가상 실행™(MVX) 엔진을 사용하여 이메일 첨부 파일 및 URL을 운영 체제, 애플리케이션 및 웹 브라우저의 포괄적인 크로스 매트릭스와 대조하여 분석합니다. 그리고 최소한의 노이즈로 위협을 식별하며, 오탐률은 0에 가깝습니다.

FireEye는 수백만 개의 센서를 통해 공격자 및 직접 침입 조사와 관련한 광범위한 위협 인텔리전스를 수집합니다. 이메일 보안은 공격 및 공격자에 대한 이와 같은 실제 증거와 상황 인텔리전스를 활용하여 경보의 우선 순위를 정하고 위협을 실시간으로 차단합니다.

또한, FireEye 네트워크 보안 및 엔드포인트 보안과 통합하여 보다 광범위한 가시성으로 다중 벡터 공격을 실시간으로 방어합니다.

FireEye

효과적인 위협 탐지

FireEye 이메일 보안은 이메일 트래픽에 숨겨진 지능형 표적 및 기타 우회 공격을 정확히 탐지하고 즉시 저지하여 침해의 피해를 최소화하는 효과적인 사이버 위협 방어 솔루션입니다.

그리고 이 이메일 보안 솔루션의 핵심에는 다중 경로 가상 실행™(MVX) 엔진이 있습니다. MVX는 의심스러운 이메일 트래픽을 검사하여 전통적인 시그니처 및 정책 기반 방어 체계를 우회하는 공격을 식별하는 동적 시그니처리스 분석 엔진입니다. MVX 엔진은 안전한 가상 환경에서 동적 시그니처리스 분석 기능을 사용하여 제로데이, 다중 트래픽 및 기타 우회 공격을 탐지합니다. 또한 전에 관찰된 적이 없는 익스플로잇과 악성코드를 식별하여 사이버 공격 킬 체인의 감염 및 침해 단계를 저지합니다.

FireEye MVX Smart Grid에 적용된 클라우드 버스팅을 통해 메시지 처리량이 최고조에 달할때 이메일 기반 위협 탐지 및 분석에 추가 용량을 활용할 수 있습니다.

이메일 기반 위협에 대한 방어 시스템

온라인으로 수집할 수 있는 많은 개인 정보 때문에, 사이버 공격자는 사회 공학을 이용하여 거의 모든 사용자가 URL을 클릭하거나 첨부 파일을 열도록 유도할 수 있습니다.

이메일 보안은 기존의 방어 시스템을 회피하는 스피어 피싱, 랜섬웨어 및 인증 피싱 공격에 대한 실시간 탐지 및 방어를 제공합니다. "비슷하지만 다른" 도메인 탐지로 인증 피싱(타이포스쿼팅)을 줄입니다.

공격이 확인되면 추가 분석이나 삭제를 위해 악성 이메일을 격리합니다. 다음에 숨겨진 악성코드에 대해 분석을 실시합니다.

- 다음과 같은 첨부 파일 유형을 포함하지만 이에 국한되지는 않음: EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 및 ZIP/RAR/TNEF 아카이브
- 암호로 보호되며 암호화된 첨부 파일
- 이메일, MS Office 문서, PDF 및 아카이브 파일(ZIP, ALZip, JAR)과 기타 파일 유형(Uuencoded, HTML)에 포함된 URL
- URL을 통해 다운로드된 파일
- 위장, 단축 및 리다이렉팅되는 모호한 URL
- 인증 피싱 및 타이포스쿼팅 URL
- 알 수 없는 Microsoft Windows 및 Apple Mac OS X 운영 체제 이미지, 브라우저 및 애플리케이션 취약점
- 스피어 피싱 이메일에 내장된 악성 코드

랜섬웨어 공격은 이메일로 시작되지만 데이터를 암호화하려면 일반적으로 명령/제어 서버로 콜백해야 합니다. 이메일 보안은 이와 같은 다단계 악성코드 캠페인을 식별하고 저지합니다.

경보에 효율적으로 대응

이메일 보안은 모든 첨부 파일과 URL을 분석하여 오늘날의 지능형 공격을 정확하게 식별합니다. 알려진 위협 공격자에 대한 경보의 특성과 결합된 전체 FireEye 보안 에코시스템에서 제공하는 실시간 업데이트를 통해 중요한 경보의 우선순위를 정하고 그에 대한 조치를 취하며 스피어 피싱 이메일을 차단하는데 필요한 상황 정보를 제공합니다. 최소한의 노이즈와 오탐률로 알려진 위협, 알려지지 않은 위협, 악성코드를 기반으로 하지 않은 위협을 식별하므로 실제 공격에 리소스를 집중하여 운영 비용을 절감할 수 있습니다. 리스크웨어 분류는 달갑진 않지만 덜 악의적인 활동(애드웨어, 스파이웨어 등)과 실제 침해 시도를 구분하여 경보 대응의 우선 순위를 정합니다.

진화하는 위협 환경에 신속하게 적응

이메일 보안은 위협과 공격자에 대한 심층적인 인텔리전스를 이용하여 이메일 기반 위협의 선제적 방어 시스템을 지속적으로 조정하도록 지원합니다. 공격자, 시스템 및 피해자 인텔리전스를 결합하여 다음을 수행합니다.

- 위협에 대한 보다 광범위한 가시성을 적시에 제공
- 탐지된 악성코드와 악성 첨부 파일의 역할 및 특징을 식별
- 우선 순위를 정해 신속하게 대응할 수 있도록 상황에 대한 통찰력 제공
- 공격자의 신원과 동기를 파악하고 조직 내에서 그들의 악성 활동 추적
- 스피어 피싱 공격을 소급 식별하고 악성 URL을 표시하여 피싱 사이트로의 액세스 차단

능동적 방어 모드 또는 모니터 전용 모드

이메일 보안은 능동적인 방어를 위해 이메일을 분석하고 위협을 격리할 수 있습니다. 조직들은 MX 레코드를 업데이트하기만 하면 메시지를 FireEye로 전송할 수 있습니다. 그 다음, 시그니처리스 폭발실이라고 할 수 있는 MVX 엔진을 사용하여 모든 첨부 파일 및 URL을 분석함으로써 실시간으로 위협을 탐지하고 지능형 공격을 저지합니다.

모니터 전용으로 설치하는 경우, BCC 룰의 명확한 설정을 통해 이메일 사본들을 이메일 보안 시스템으로 보낸 후 MVX 엔진으로 분석할 수 있습니다.

보안 운영 향상

이메일 보안은 FireEye Helix의 구성 요소이며, FireEye Central Management와 함께 동작합니다.

- FireEye Helix의 구성 요소로써, 이메일 보안은 낮은 비용으로 위협을 탐지하고 신속하게 해결합니다.
- FireEye Central Management는 공격을 광범위하게 파악하고 공격이 확산되는 것을 막는 차단 룰을 설정하기 위해 이메일 보안과 FireEye 네트워크 보안의 경보를 상호 연결시킵니다.

맞춤화할 수 있는 YARA 기반의 룰

이메일 보안은 또한, 맞춤형 YARA 규칙을 지원하여 보안 분석가가 해당 조직을 표적으로 삼는 위협이 포함된 이메일 첨부 파일을 분석하는 규칙을 지정하고 테스트할 수 있게 합니다.

메시지 대기열 및 경보와 격리 관리

이메일 보안은 스캔하는 이메일 메시지에 대한 높은 제어력을 제공합니다. 능동적 방어 모드로 설치하는 경우, MTA 큐를 통해서 이동할 때 메시지를 추적 및 관리할 수 있습니다. 이메일 특수한 특성을 사용하여 메시지가 수신, 분석 및 넥스트 홉으로 전달되었는지 검색 및 검증하고, 시간 경과에 따라 직관적 대시보드를 통해 트렌드를 모니터링할 수 있습니다. 명백한 허용 및 차단 리스트는 이메일 처리에 대한 맞춤형 제어를 제공합니다. 일반적인 경보의 특성을 검색하거나 선택할 수 있습니다. 또한 경보 및 격리된 메시지를 일괄적으로 처리할 수 있습니다.

표 1. 기술 사양

	EX 3500	EX 5500	EX 8500
성능*	시간당 각 첨부 파일 최대 700개	시간당 각 첨부 파일 최대 1,800개	시간당 각 첨부 파일 최대 2,650개
네트워크 인터페이스 포트	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+, 2x 1GigE BaseT
관리 포트	LSI9341-4i, 2x 1GigE BaseT	LSI9341-4i, 2x 1GigE BaseT	LSI9341-4i, 2x 1GigE BaseT
IPMI 모니터링	지원됨	지원됨	지원됨
PS/2 키보드 및 마우스, DB15 VGA 포트(후면 패널)	포함	포함	포함
USB 포트(후면 패널)	2x USB2, 2x USB3	2x USB2, 2x USB3	2x USB2, 2x USB3
시리얼 포트(후면 패널)	115,200bps, 패리티 없음, 8비트, 1 정지 비트	115,200bps, 패리티 없음, 8비트, 1 정지 비트	115,200bps, 패리티 없음, 8비트, 1 정지 비트
저장 용량	4x 2TB, RAID 10, HDD 3.5인치, FRU	4x 2TB, RAID 10, HDD 3.5인치, FRU	4x 2TB, RAID 10, HDD 3.5인치, FRU
엔클로저	1RU, 19인치 랙에 적합	2RU, 19인치 랙에 적합	2RU, 19인치 랙에 적합
섀시 크기(WxDxH)	17.2" x 25.6" x 1.7" (437 x 650 x 43.2 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)
AC 전원 장치	중복 (1+1) 750와트, 100~240 VAC 9 – 4.5A,50~60Hz, IEC60320-C14 인렛, FRU	중복 (1+1) 800와트, 100~240 VAC 9 – 4.5A,50~60Hz, IEC60320-C14 인렛, FRU	중복 (1+1) 800와트, 100~240 VAC 9 – 4.5A,50~60Hz, IEC60320-C14 인렛, FRU
DC 전원	해당 없음	해당 없음	해당 없음
최대 열량 전력 와트(Btu/h)	245와트(836Btu/h)	456와트(1,556Btu/h)	530와트(1,808Btu/h)
MTBF(h)	54,200	19,970	11,880
어플라이언스만/발송 중량, lb.(kg)	30.0lb(13.6kg) / 41.0lb(18.6kg)	44.1lb(20.0kg) / 65.3lb(29.6kg)	44.4lb(20.2kg) / 65.6lb(29.8kg)
안전 규제 준수	UL 60950-1-2014; CAN/CSA C22.2 No. 60950-1-07, Am.1:2011+Am.2:2014; AS/NSZ 60950.1- 2011	EN 60950-1, 1:2006+A1 1:2009+A1:2010+A12:20 11+A2:2013; IEC 60950- 1:2005 + Am 1:2009 + Am 2:2013	EN 60950-1, 1:2006+A1 1:2009+A1:2010+A12:20 11+A2:2013; IEC 60950- 1:2005 + Am 1:2009 + Am 2:2013

표 1. 기술 사양

	EX 3500	EX 5500	EX 8500
EMC 준수	FCC 파트 15 서브파트 B 클래스 A, ICES-003 클래스 A, EN55022 클래스 A, VCCI V-3 클래스 A, EN 55024, EN 61000-3-2 클래스 A, EN 61000-3-3, CNS 13438(2006) 클래스 A, CISPR22 클래스 A, AS/NZS CISPR 22 클래스 A, KN 32, KN 35	FCC 파트 15 서브파트 B 클래스, ICES-003 클래스 A, EN 61000-3-2 클래스 A, EN 61000-3-3, CISPR22 클래스 A,	FCC 파트 15 서브파트 B 클래스, ICES-003 클래스 A, EN 61000-3-2 클래스 A, EN 61000-3-3, CISPR22 클래스 A,
보안 인증**	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
환경 준수	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE
작동 온도	0-35°C(32-95°F)	0-35°C(32-95°F)	0-35°C(32-95°F)
작동 상대 습도	40°C에서 10-95%, 비응결	40°C에서 10-95%, 비응결	40°C에서 10-95%, 비응결
작동 고도(피트)	5,000	5,000	5,000

*모든 성능 수치는 시스템 설정과 처리 중인 이메일 트래픽 프로파일에 따라 달라집니다. 시간당 고유 첨부파일에 따른 어플라이언스 사이즈
** 진행 중.

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

FireEye, Inc.
서울 특별시 강남구 테헤란로 534. 글라스타워 20층 전화: 02.2092.6580 / korea.info@fireeye.com www.fireeye.kr

www.FireEye.com

FireEye®는 인텔리전스 기반 SaaS(Security-as-a-Service)의 리더입니다. FireEye는 고객 보안 운영의 완벽한 확장을 위해 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 맨디언트 컨설팅을 결합한 단일 플랫폼을 제공합니다. 이를 통해 FireEye는 사이버 공격에 대비, 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 간소화합니다. FireEye는 포브스 글로벌 2000 기업 중 940개 이상의 기업을 포함해 67개국의 5,000여 기업을 고객으로 보유하고 있습니다.

DS.EX.KO-KR.082017