솔루션 요약

지능형 위협 방어를 위한 이메일 보안

개요

이메일은 표적화/맞춤화를 통해 성공적으로 악용하기 쉽기 때문에 대다수의 사이버 공격에서 주요 엔트리포인트로 꾸준히 이용되고 있습니다. 기존의 안티스팸 필터 및 안티바이러스 소프트웨어는 알려진 악성 첨부 파일, 링크 및 콘텐츠를 이용하는 전통적인 대규모 피싱 위협을 포착하는 데에는 효과적이지만, 이러한 기존 솔루션을 우회하도록 고안된 정교한 스피어 피싱 공격과 사칭 공격은 포착하지 못합니다.

대부분의 보안 이메일 게이트웨이(*Secure Email Gateways, SEG*)는 기존 스팸 및 알려진 악성코드의 위험을 줄이기는 하지만 악성 이메일과 지능형 위협을 초기단계에 탐지하고 방지할 수 있는 기술, 인텔리전스, 전문지식의 조합은 부족합니다. 그리고 대량으로 전송되는 새로운 위협에 대응하도록 고안된 범용 안티스팸 필터와 안티바이러스 소프트웨어를 사용합니다. 일반적으로 대응하는 데 몇 분이 걸릴 수 있고 공격자가 끊임없이 진화하는 수법을 이용해 탐지 시간을 더 지연시킬 수 있으므로 스팸 발송자와 사이버 위협 범죄자가 악용하는 세계적인 격차를 남길 수 있습니다. 대개 전송 계층 보안(*Transport Layer Security, TLS*) 연결을 통해 전송되는 이메일 트래픽은 검사할 수 없으므로 방화벽도 이러한 이메일을 악용한 랜섬웨어 및 스피어 피싱 캠페인을 방어하는 데 도움이 되지 않습니다.

오늘날의 스팸 캠페인, 랜섬웨어, 사칭 공격에 이용되는 스피어 피싱 이메일을 차단하려면 위협 환경에 신속하게 대응하여 진화하는 이메일 보안 솔루션이 필요합니다. 이러한 보안 솔루션은 다음과 같은 위협 방어에 집중해야 합니다.

- 시그니처에 의존하지 않고 초기 단계에서 지능형 위협 탐지
- 오탐을 최소화하면서 중요 위협 탐지
- 인라인을 차단하여 랜섬웨어와 같은 위협 요소가 환경으로 침투하지 못하도록 방어
- 일선에서 얻은 사이버 위협 인텔리전스와 공격자에 대한 선제적 지식을 이용하여 신속하게 대응함으로써 조직 보호

현재 이메일 보안 솔루션의 보안 성능이 충분하지 않은 이유

데이터 침해는 조직에서 관리하는 정보, 사람, 프로세스를 위험에 빠뜨립니다. 또한 비즈니스를 저해하고 조직의 평판을 손상시키며 고객 신뢰를 떨어뜨립니다. 데이터 침해로 인해 발생하는 평균 비용은 362만 달러[2]에 달하며, 피싱 이메일로부터 시작되는 경우가 많습니다. 수년간 도용된 이메일의 양이 다른 형태의 데이터 도용 사례를 모두 합한 것보다 많을 겁니다.[3]

이메일은 사이버 공격의 손쉬운 표적입니다. 현재 솔루션이 안전한지 확인하려면 다음을 점검해봐야 합니다.

1. 귀사의 SEG는 바이러스, 스팸, 알려진 악성코드 외에 악성코드가 포함된 첨부 파일과 URL, 인증 피싱 사이트, 사칭 수법까지 탐지하고 차단하는가?
2. 위협을 차단하고 중요한 사항을 사용자에게 알리며 취해야 할 조치에 대한 인텔리전스를 제공하여 효율적인 대응을 지원하는가?
3. 진화하는 위협 환경에 빠르게 대응하는 데 활용할 최신 상황 인텔리전스에 접근할 수 있는가?
4. 현재 사용 중인 이메일 보안 솔루션이 다른 보안 툴과 통합되어 여러 위협 경로에 걸쳐 원활하게 작동하고 혼합 공격을 방어할 수 있는가?
5. 이메일 보안 솔루션이 비즈니스의 변화에 맞추어 유연하게 확장되는가?

91% 의 사이버 공격이 스피어 피싱 이메일로부터 시작됩니다.[1]

---

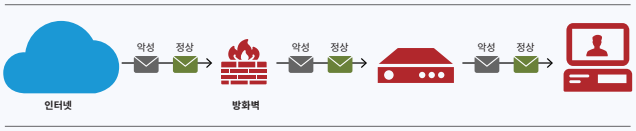
1 PhishMe(2016년). "Enterprise Phishing Susceptibility and Resiliency Report."
2 Ponemon Institute LLC(2017년 6월). "2017 Cost of Data Breach Study: Global Overview."
3 Mandiant, A FireEye Company(2017년). "M-Trends 2017 A View From The Front Lines."

1 **이메일 위협이 진화하면서 클라우드 기반 이메일 가입 서비스를 도입하는 사례가 늘고 있습니다.** 조직들은 정보, 운영 및 자산을 클라우드로 마이그레이션하고 있습니다. 공용 클라우드 서비스와 인터넷 연결 기반 장치가 빠르게 성장하면서 자연히 클라우드를 표적으로 한 사이버 위협이 증가하고 클라우드 기반 보안 솔루션의 필요성이 커지고 있습니다.

FireEye Email Security – Cloud Edition은 인바운드 및 아웃바운드 악성코드, 피싱 URL, 사칭 수법, 스팸을 차단하는 보안 이메일 게이트웨이입니다. 안티바이러스 및 안티스팸(*AntiVirus and Anti-Spam,* AVAS) 추가 기능은 스팸 캠페인과 사칭 수법에 대한 방어를 제공합니다. 스팸 캠페인 및 표적 위협과 지능형 위협을 방어하는 포괄적인 단일 벤더 이메일 보안 제품에 필요한 요구 사항을 해결합니다. 따라서 조직이 이메일 보안 스택을 통합하고 클라우드를 본격적으로 도입할 수 있습니다.

2 **낙후된 방어 시스템은 조직에 잘못된 보안 인식을 제공합니다.** 범용 인텔리전스, 제3자 시그니처 및 평판에 의존하는 이메일 게이트웨이는 최초 발견 시부터 위협을 탐지할 목적으로 특별히 개발되지 않았습니다. 마찬가지로, 방화벽은 이메일을 통해 침투하는 랜섬웨어와 스피어 피싱 캠페인을 차단하지 못합니다.

그림 1. 기존의 보안 솔루션은 표적 사이버 공격을 탐지하지 못함



구조적으로 이들 기술은 분석을 진행하는 동안 이메일을 보류할 수 없습니다. 따라서 악성코드를 포함한 첨부 파일과 URL, 사칭 수법을 포함한 이메일이 사용자에게 전달됩니다.

FireEye Email Security는 규모에 관계없이 모든 조직이 침해의 위험과 피해를 최소화하도록 지원하는 데 목적을 두고 있습니다. 다른 보안 솔루션에서 탐지되지 않는 이메일 트래픽에 숨은 스팸 캠페인과 지능형 공격 및 표적 공격을 탐지합니다. 실제로 최근 한 글로벌 소비재 회사를 대상으로 POV(Proof of Value)를 실시하는 과정에서 FireEye는 기존 게이트웨이가 탐지하지 못하는 수천 건의 피싱 및 사칭 전술을 찾아냈습니다.

3 **기존의 시그니처 기반 인텔리전스 피드는 오늘날의 이메일 기반 공격을 방어할 만큼 충분히 빠르게 진화할 수 없습니다.** 이러한 피드는 공격을 예측하거나 대응을 유도하는 데 도움을 줄 수 없습니다. 사실 포인트 솔루션으로 통합된 수많은 보안 기술과 소프트웨어가 경보의 급증을 유발하고 있습니다. FireEye Email Security는 제3자 시그니처 및 평판 업데이트에 의존하지 않는 사내 탐지 방식의 솔루션이므로, 훨씬 빠르게 진화하며 새로운 스팸 캠페인이 발견되면 즉시 차단할 수 있습니다. 알고리즘을 통해 메시지 발신자와 도메인을 분석하여 수신자 도메인 내의 알려진 이름에 대한 스푸핑 시도가 없는지를 확인함으로써, 악성코드나 악성 URL과 무관한 CEO 사기를 비롯하여 갈수록 확산되는 사칭 공격을 차단합니다.

FireEye Email Security는 직접 조사와 공격자 관찰을 통해 얻은 인텔리전스를 기준으로 차단할 대상을 파악합니다. 또한 이러한 통찰력은 보안 팀이 경보의 우선 순위를 쉽게 파악할 수 있도록 경보와 관련한 상황 정보를 제공합니다. 악성 이메일이 격리되고 활용 가능한 상황 인텔리전스는 공격 및 공격자에 대한 심층적인 정보를 사용하여 지능형 위협의 억제를 가속화합니다.

실제 증거를 전 세계와 공유하여 이전에 알려지지 않은 공격을 즉시 차단하도록 하고 위협 대응을 가속화합니다. 최소한의 노이즈와 오탐률로 위협이 식별됩니다. 따라서 보안 팀 리소스를 실제 공격에 집중하게 하고 운영 비용을 줄이며 운영 위험을 최소화할 수 있습니다.

4 **지능형 공격의 한 특정 단계에만 집중하는 웹 전용 방어 수단과 이메일 전용 방어 수단을 회피하기 위해 여러 단계로 네트워크(웹) 전술과 이메일 전술을 병행하는 공격이 많습니다.** 단일 사이버 공격은 제로데이 취약점을 악용한 지능형 악성코드, 스피어 피싱 이메일, 악성 URL, 침투한 장치를 제어하고 표적 자산을 빼내기 위한 명령 서버의 복잡한 네트워크로 구성될 수 있습니다.

랜섬웨어 공격은 이메일로 시작되지만 데이터를 암호화하려면 명령 및 제어 서버로 콜백해야 합니다. 이메일을 중심으로 한 다단계 공격으로 격리된 상태로 파일을 분석하는 대부분의 샌드박스를 쉽게 회피할 수 있습니다. 대부분의 보안 제품이 문제를 발견하는 시점에는 이미 피해자의 데이터가 암호화되어 있습니다. FireEye Email Security 및 Network Security는 완벽하게 통합되어 혼합 공격을 탐지하고 차단합니다. 이 두 시스템은 함께 공격 라이프사이클을 상호 관련시켜 원래의 스피어 피싱 이메일과 위협 공격자까지 역추적합니다.

뛰어난 위협 탐지

Email Security는 정상 트래픽으로 위장된 고급, 대상 및 기타 회피 공격을 식별하고 격리함으로써 비용이 많이 드는 위반 위험을 완화하는 데 도움이 됩니다. 일단 탐지되면, 이러한 공격은 즉시 중지되고, 분석되며 식별자를 찍어 미래의 위협을 더 빨리 식별하도록 활용됩니다.

그리고 이 Email Security 솔루션의 핵심에는 지능형 URL 방어 및 멀티벡터 가상 실행(Multi-Vector Virtual Execution™, MVX) 기술이 있습니다. 이러한 기술은 기계 학습과 분석을 사용하여 전통적인 시그니처 기반과 정책 기반 방어를 회피하는 공격을 식별합니다.

Email Security – Cloud Edition을 안티바이러스 및 안티스팸(AVAS) 보호 솔루션과 함께 사용하면 사칭 수법뿐만 아니라 기존의 시그니처 매칭 수법을 이용하는 일반적인 수법을 탐지할 수 있습니다.

CEO 사기(비즈니스 이메일 침해라고도 함)와 같은 사칭 공격은 기업에 지속적으로 재정적 영향을 미치고 있습니다.

이는 부분적으로 악의적인 첨부나 링크와 같은 전통적인 위협 지표가 부족하기 때문입니다. 이러한 공격에 맞서 싸우고 고객을 보호하기 위해 FireEye는 사칭 감지와 방어에 특화된 혁신적인 알고리즘, 시스템 및 도구를 개발했습니다.

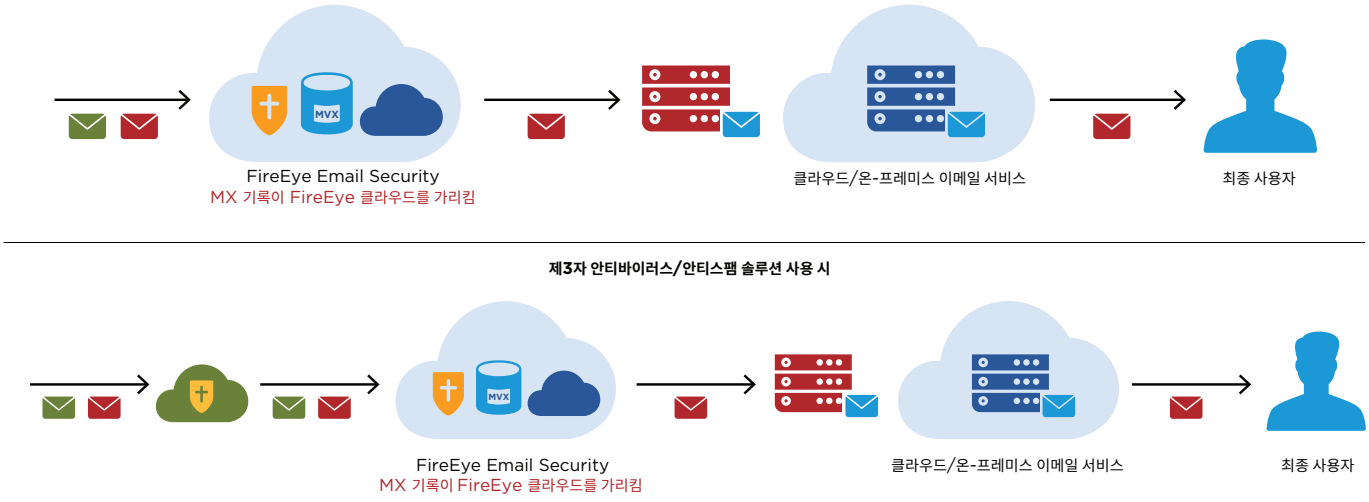
직접 조사와 공격자 관찰을 통해 확보한 이메일 관련 위협 인텔리전스, 공격 및 공격자 인텔리전스를 사용하여 최소한의 노이즈로 위협을 식별하며, 오탐률은 0에 가깝습니다. 따라서 보안 팀이 실제 공격을 조사하고 대응하는 데 집중하고 부족한 리소스를 효율적으로 활용할 수 있습니다.

유연한 설치 옵션

FireEye Email Security는 더 많은 제어와 실시간 대응을 위해 인라인으로 설치하여 진행 중인 공격을 저지할 수 있습니다. 특히, 예방만이 유일하게 효과적인 방어 수단인 랜섬웨어와 같은 공격에 대해서는 인라인 설치를 통해 악성 콘텐츠와 악성코드 없는 콘텐츠가 최종 사용자에게 전달되지 않도록 차단합니다.

아무것도 설치하지 않아도 되는 FireEye Email Security – Cloud Edition은 조직이 이메일 인프라를 클라우드로 마이그레이션하는 최적의 솔루션입니다. Microsoft Office 365 및 G Suite와 같은 클라우드 기반 이메일 시스템과 완벽하게 통합됩니다. 새로운 스팸 캠페인과 사칭 수법을 차단하는 인라인 안티스팸 및 안티바이러스 보호 기능을 갖춘 AVAS 추가 기능이 제공됩니다.

그림 2. **FireEye Email Security – Cloud Edition – 인라인 설치**



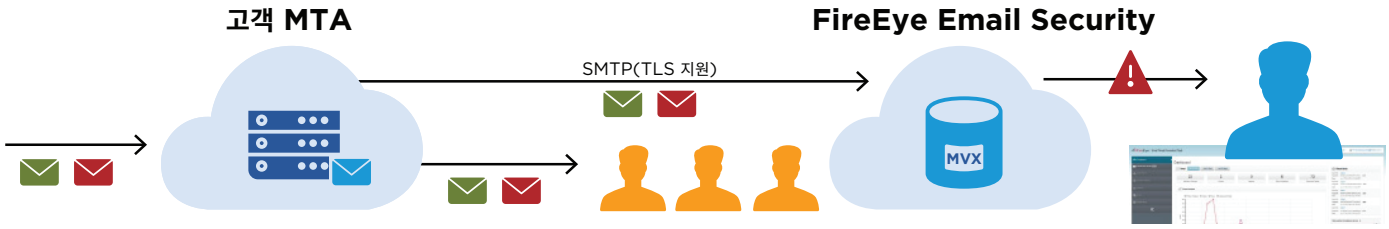
일부 조직들은 더 보수적인 접근방법을 사용하여 작업을 시작하는 것을 선호하며 FireEye Email Security는 대역 외 또는 모니터 전용 모드로 설치할 수 있습니다(그림 3). 이러한 설치에서, 모든 트래픽은 악성 활동이 있는지 모니터링되고 보고서가 생성되지만 자동화된 방어 메커니즘이 없습니다.

FireEye Email Security - Server Edition은 온-프레미스 어플라이언스 제품군입니다. FireEye 또는 공인 파트너들은 고객의 보안 필요에 가장 적합한 옵션을 결정하고 설치하는 데 도움을 줄 수 있습니다.

다음 단계

오늘날의 지능형 사이버 공격과 동적 위협 환경에 대응하려면 조직이 위협 프로파일을 이해해야 합니다. 이를 위해서는 위협을 탐지 및 대응하고 보안 사고를 신속하게 해결하는 데 집중하면서 위험에 처해 있는 자산을 파악해야 합니다. 조직이 목표에 집중하고 위험을 최소화하려면 최초 발견 시부터 이메일 기반 위협을 탐지하고 차단하는 데 중점을 둔 이메일 보안 솔루션이 필요합니다. 여기에는 보안 기술과 중요 사이버 공격에 대한 직접 조사를 통해 얻어진 사이버 위협 인텔리전스가 포함됩니다.

그림 3. FireEye Email Security – Cloud Edition – BCC 모드



FireEye에 대한 자세한 정보: **www.FireEye.com**

FireEye Korea
서울특별시 강남구 테헤란로 534 글라스타워 20층
02.2092.6580
korea.info@fireeye.com

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.