



# 이메일 위협 보고서

2019년 1월~3월

## 2019년 1분기에 FIREYE에서 목격한 내용

- URL 기반 공격은 악의적인 콘텐츠를 전달하기 위한 주요 수단이었습니다.
- 피싱 공격은 2018년 4분기에 비해 2019년 1분기에 17% 증가했습니다.
- 사칭 공격은 2019년 1분기에 증가했으며 2분기에도 계속해서 증가할 것으로 예상됩니다.
- CEO 사기는 사이버 캐시카우로 등극하였으며 두 가지의 새로운 변종을 낳았습니다.
- 평판 블랙메일 공격은 2018년부터 2019년 1분기까지 계속되었습니다.
- 상용 및 무료 파일 공유 서비스의 악의적인 페이로드를 제공하는 데 악용되었습니다.
- 중첩된 이메일이 악의적인 콘텐츠를 전달하는 데 사용되었습니다.

# URL 기반 공격

2018년에 FireEye는 URL 기반 공격이 전달 수단으로서 첨부 파일 기반 공격을 추월했다고 보고했습니다. 이 추세는 2019년 1분기에도 계속되었습니다. URL 기반 공격은 동적인 탐지 수단이 더 많이 필요하기 때문에 식별하기가 더 어렵습니다. FireEye는 다음과 같은 몇 가지 중요한 추세를 관찰했습니다.

## HTTPS 사용

HTTPS(HTTP의 보안 버전)는 웹 사용자에게 개인정보가 보호되며 보안이 될 것이라는 기대를 갖게합니다. 그러나 피싱 공격에 HTTPS 도메인 사용이 증가했음을 FireEye에서 알게된 이후로 이는 더 이상 기정사실이 아닙니다. FireEye는 2018년 4분기부터 2019년 1분기까지 HTTPS를 사용하는 악성 URL이 26% 증가한 사실을 알게 되었습니다.



### 내용 없는 이메일

악성 URL을 전달하는 수단으로서 내용 없는 이메일이 새로운 것은 아니지만, FireEye는 1분기 1월에 내용 없는 이메일 발생 건수가 급증한 것을 목격했습니다. 내용 없는 메일은 내용이 거의 없거나 전혀 없으며 URL만 있습니다(그림 1). 이러한 이메일은 다음과 같은 이유로 효과적입니다.

- 내용이 부족하면 필터가 제대로 작동하지 않게 되므로 이메일 필터를 우회할 수 있습니다.
- 수신자의 호기심을 자극하여 악의적인 웹 페이지 또는 파일로 연결되는 링크를 클릭하도록 합니다.

### 클릭할 수 없는 URL

클릭할 수 없는 URL은 사용자가 이 URL을 복사하여 브라우저에 붙여넣을 때 활성화됩니다. 클릭할 수 없는 URL은 라이브링크가 아니므로 여러 보안 필터를 우회하는 데 매우 효과적입니다.

그림 1. 내용 없는 이메일의 예

**From:** [REDACTED]  
**Sent:** Thursday, January 17, 2019 09:47:55 PM  
**To:** [REDACTED]  
**Subject:**

<http://www.bing.com/search?q=&form=GVHFEERMCRUYMAK&cvid=RQPWTZUDRHDXCD>

## 피싱 공격

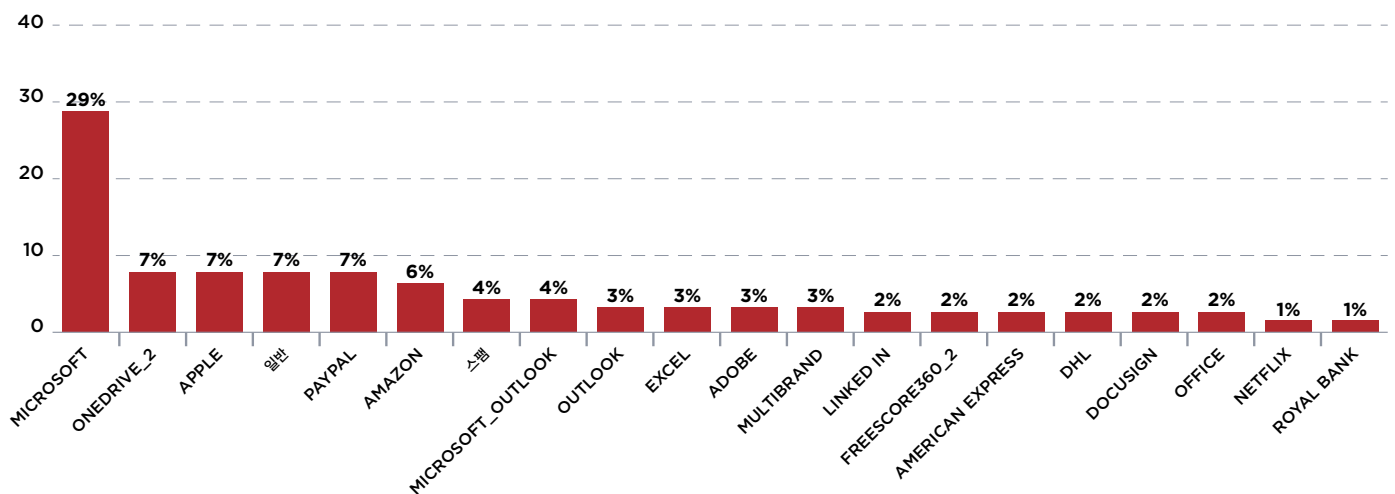
**17%** 피싱 공격  
증가.

FireEye는 2018년 4분기와 비교했을 때 2019년 1분기에 피싱 공격이 17% 증가한 사실을 목격했습니다. 일반적인 공격에서, 이메일은 잘 알려진 연락처나 신뢰할 수 있는 회사에서 온 것처럼 보였습니다.

Microsoft는 가장 일반적으로 사용되는 브랜드로, 전체 탐지 사례 중 거의 30%를 차지하고 있습니다(그림 2). FireEye는 브랜드가 있는 로그인 페이지를 탐지하는 FireEye Advanced URL Defense 플러그인인 PhishVision에서 브랜드 데이터를 수집했습니다. Microsoft, Outlook 및 Excel은 서로 다른 로그인 페이지를 사용하므로 각각 다른 버킷에 배치하여 별도로 집계하였습니다.

FireEye는 브랜드 참조 없이 로그인 페이지를 사용하는 피싱 공격자를 관찰했습니다. 이러한 페이지를 일반 피싱으로 분류했습니다. 피해자에게서 돈을 뜯어내는 데 사용되는 일반 용어로 자주 사용되는 '419 스팸' 및 '데이팅 스팸'은 탐지 엔진이 식별하여 스팸으로 표시합니다. '419 스팸'은 비아그라 및 기타 약을 판매하는 의심스러운 웹사이트로 사용자를 안내합니다. '데이팅 스팸'은 연애 상대를 제안합니다.

그림 2. 2019년 1분기 피싱 공격에서 탐지된 가장 일반적인 브랜드\*



\*일반 및 스팸 피싱 이메일에는 브랜드가 포함되지 않습니다.

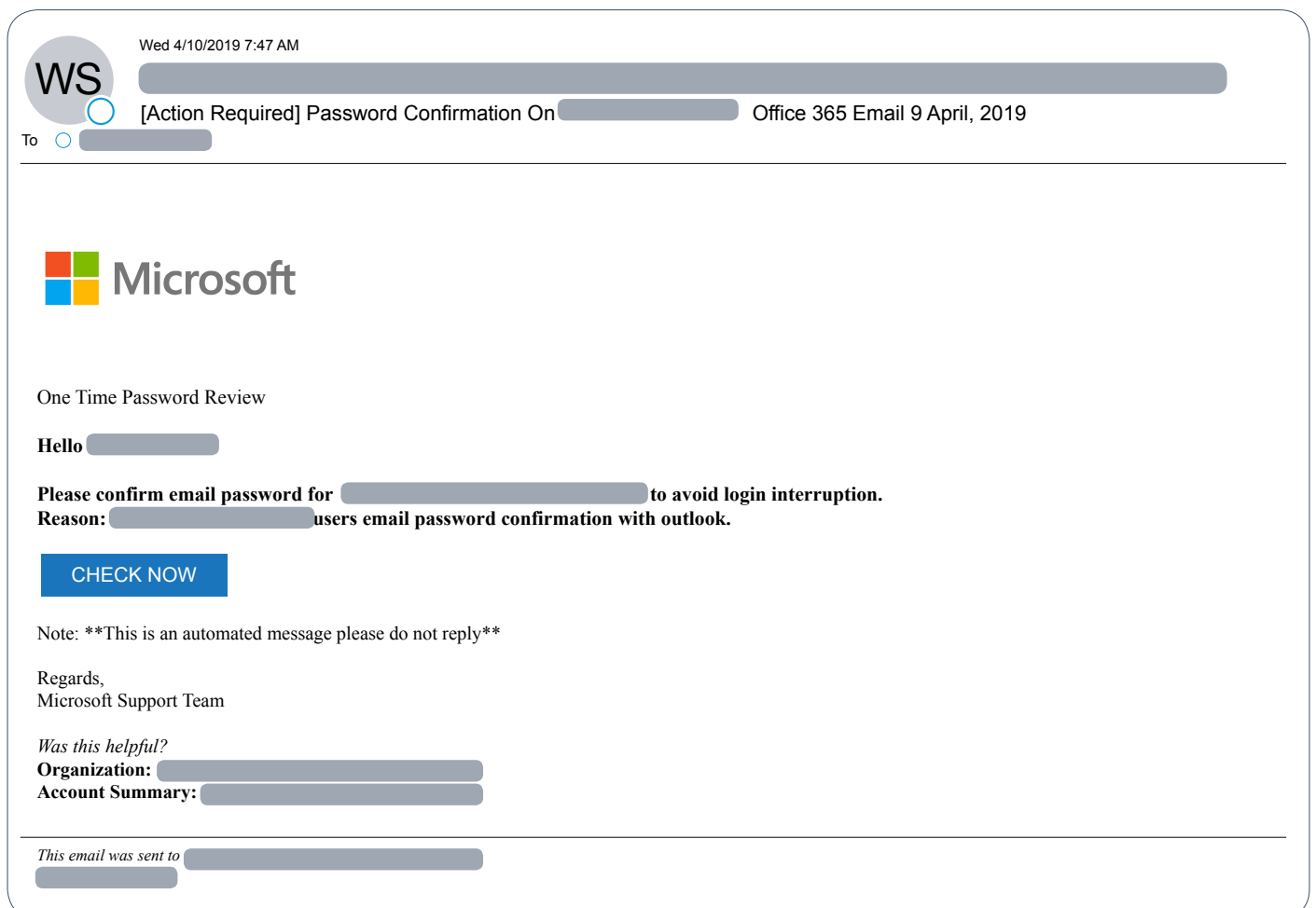
공격자는 자신의 활동을 상업 부문으로 제한하지 않습니다. 피싱 공격에 사용되는 상위 20개 브랜드에는 Netflix, LinkedIn, Amazon 및 Free Score 360과 같은 개인 서비스가 포함됩니다.

FireEye는 Microsoft Office 365 계정과 연관된 것처럼 보이는 이메일과 관련된 여러 공격을 목격했습니다. 그림 3의 예는 수신자에게 행동하도록 촉구합니다. 수신자가 이메일 암호를 재확인하도록 요청하거나 서비스 중단이 발생한다는 안내를 합니다.

일반적인 공격의 특징에는 다음이 포함됩니다.

- 보낸 사람 이메일 주소가 수신자 회사의 지원 부서에서 발송한 것처럼 보이도록 도용되었습니다.
- Microsoft 브랜드 사용은 진짜인 것 같은 오해를 더 강화시켜 줍니다.
- 메시지가 자동 메시지인 것으로 표시되어 있습니다.

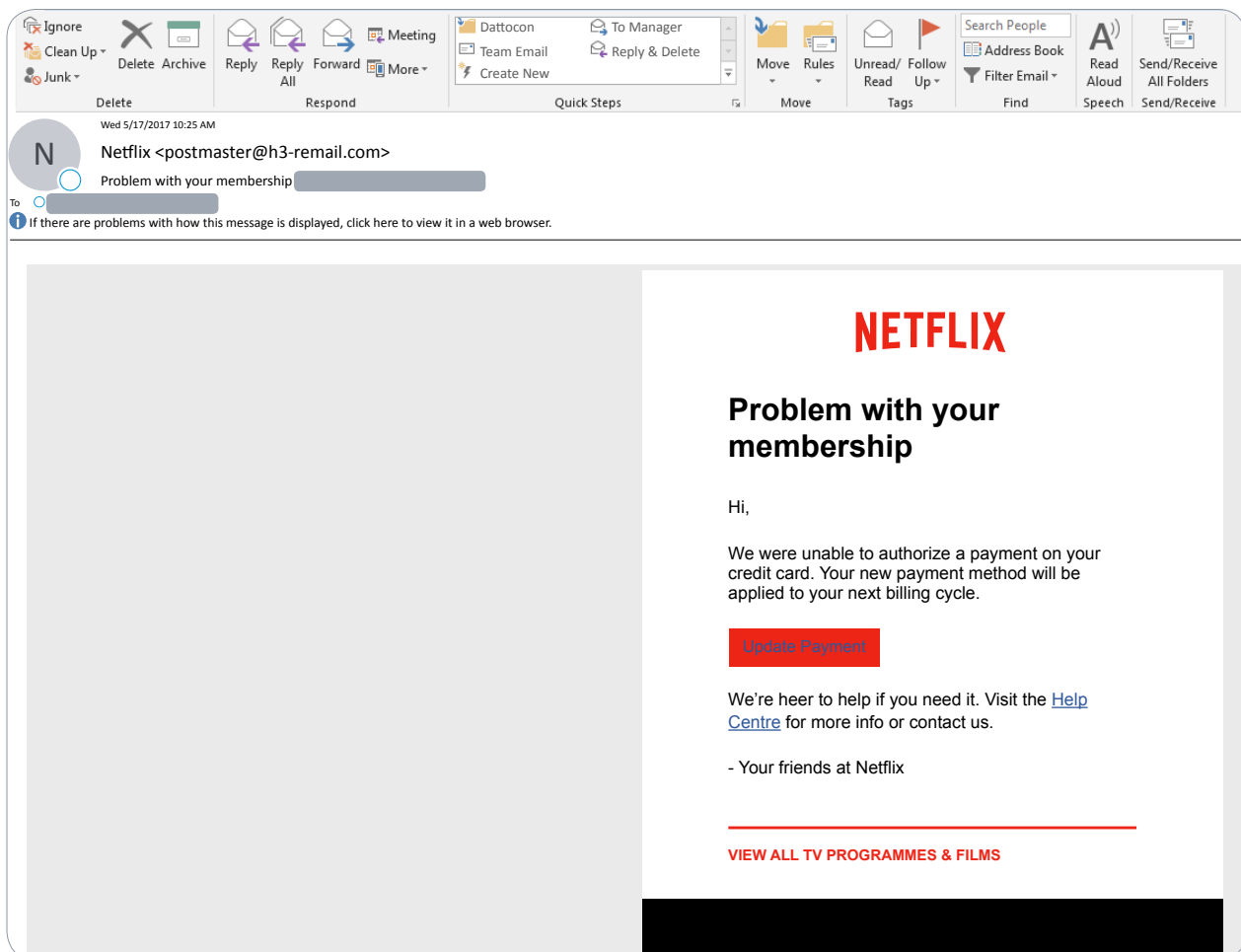
그림 3. Microsoft Office 365 브랜드를 사용한 이메일 기반 공격의 예



공격자는 자신의 활동을 상업 부문으로 제한하지 않습니다. 피싱 공격에 사용되는 상위 20개 브랜드에는 Netflix, LinkedIn, Amazon 및 Free Score 360과 같은 개인 서비스가 포함됩니다. 이러한 유형의 피싱 공격은 인증 정보 및 신용카드 정보를 얻기 위한 수단으로 성공적이었습니다(그림 4).

HTML 첨부 파일 및 피싱 페이지는 2019년 1분기에 널리 사용된 기타 피싱 공격 메커니즘입니다. HTML 첨부 파일은 호스팅되지 않으므로 탐지를 피할 수 있고 매우 설득력 있게 보입니다. 슬립(Sleep), 캡차, 디스플레이 링크 및 악성 문서로의 링크가 포함된 그래픽 버튼과 같은 사용자 상호 작용이 필요한 피싱 페이지가 페이지의 명백한 진위성을 더해 줍니다.

그림 4. Netflix 브랜드를 사용한 이메일 기반 공격의 예



# 사칭 공격

최근 CEO 사기, 업무용 이메일 침해(BEC) 등의 사칭 공격이 사이버 범죄자들 사이에서 주요 공격 수법으로 자리 잡았습니다. 이러한 사칭 공격은 대개 텍스트를 기반으로 하며 정상적인 트래픽인 것처럼 보이기 때문에 이메일 보안 솔루션에서 탐지하기가 어렵습니다. 이러한 이메일이 사용자의 받은편지함으로 배달되면, 해당 이메일 및 요청의 진위를 판단하는 것은 사용자에게 달려있습니다. 공격자들은 다양한 수법을 이용하여 자신의 요청이 진짜라고 믿도록 사용자를 속입니다(그림 5).

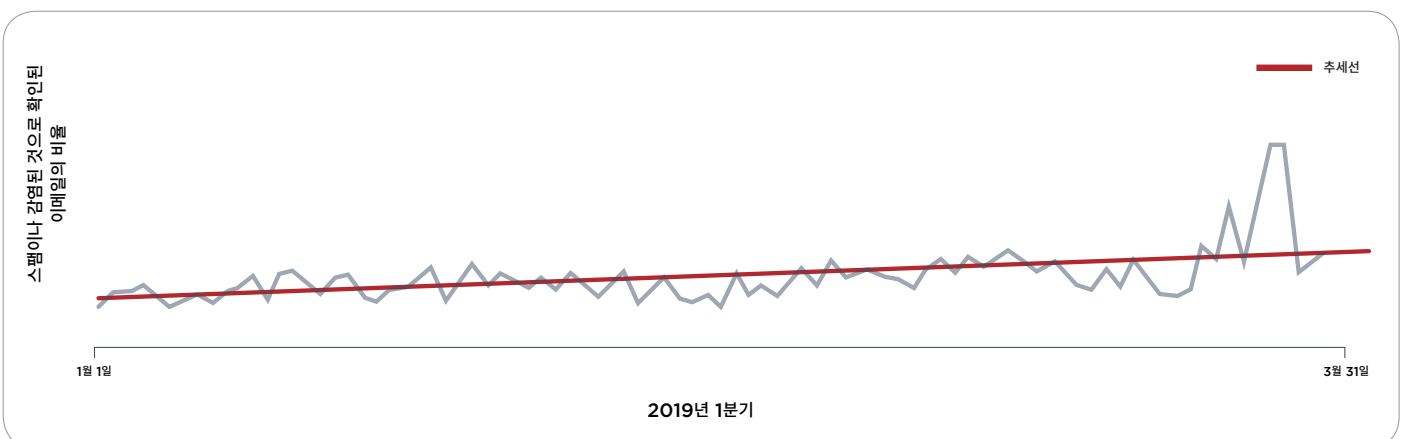
사이버 범죄자들은 이러한 수법 중 하나 이상을 이용함으로써 신뢰할 수 있는 출처로서 자신의 신뢰성을 입증하고 수신자가 자신의 요청에 동의하도록 설득할 수 있습니다.

또한 사칭 공격은 1분기 동안 꾸준히 증가한 것으로 나타났으며(그림 6), 추세선은 2019년 2분기에도 이 공격이 계속 증가할 것임을 시사합니다.

그림 5. 사칭 공격이 작동하는 방식



그림 6. 2019년 1분기에 사칭 공격 시도는 상승 추세입니다.



# CEO 사기

CEO 사기는 2018년 4분기 내내 지속적으로 많았으며 2019년 1분기에도 꾸준히 증가하여(그림 7), 사이버 캐시카우로 등극하였습니다.

공격자들은 경영진 및 고위 관리자로 사칭하여 사기성 송금을 승인하는 것과 같은 행동을 하도록 직원을 속입니다.

미지급금의 긴급 결제가 필요한 공급업체와 관련하여 CEO 또는 CFO가 회계 부서로 스푸핑 이메일을 보내는 것처럼 보일 수 있는 기존의 CEO 사기 외에도, FireEye는 두 가지의 새로운 변종이 증가하는 것을 목격하고 있습니다.

한 가지 변종의 경우, CEO 또는 유사한 고위 경영진이 자신의 개인 데이터 중 일부(일반적으로 은행 세부 정보)를 변경하도록 요청하는 이메일을 급여 지급 부서에 보냅니다(그림 8). 이는 사실상 해당 경영진 급여(꽤 많은 액수)가 범죄자의 계좌로 빠져나감을 의미합니다. 기존의 CEO 사기가 역사적으로 조직의 회계 부서를 표적으로 삼았기 때문에 이 변종은 매우 중요합니다. 이 변종은 급여 지급을 이용합니다.

또 다른 변종인 공급망 사칭의 경우 공격자들은 표적 조직 내의 사용자와 주기적으로 소통하는 파트너로 사칭하거나 이들의 정보를 침해합니다.



그림 7. 2019년 1분기에 CEO 사기 공격 시도는 상승 추세입니다.

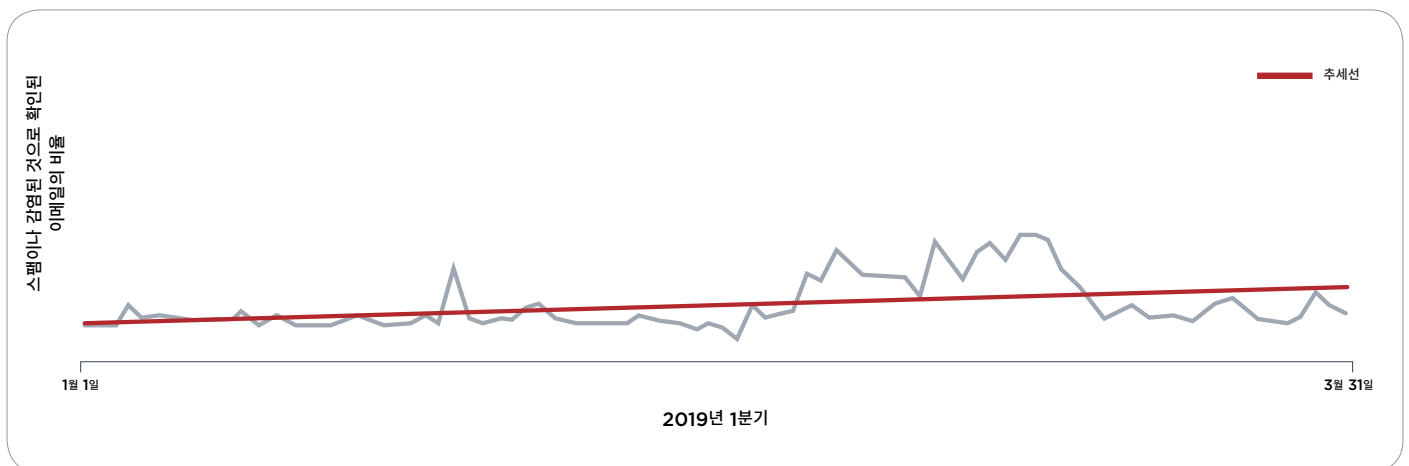
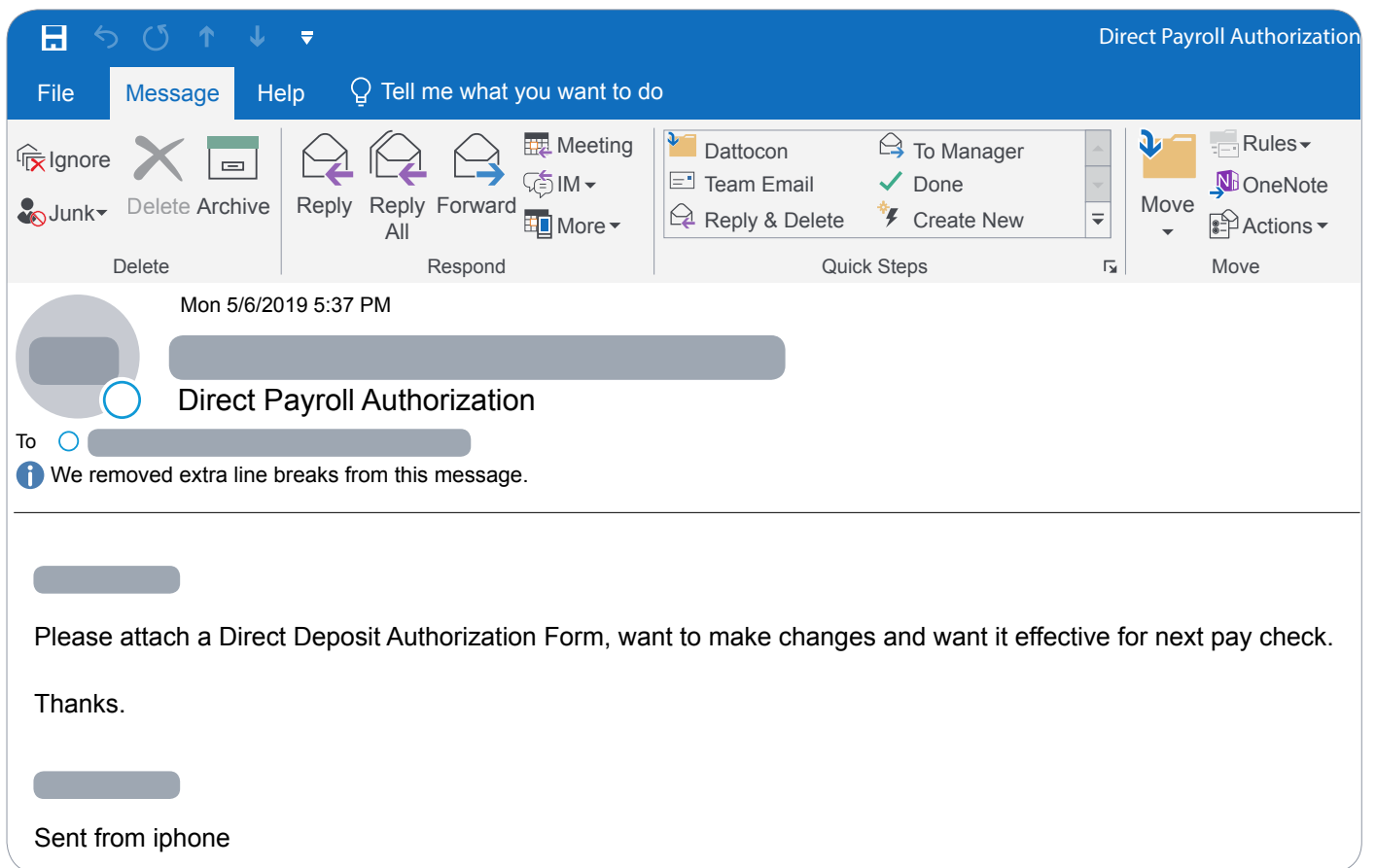




그림 8. 급여 지급 정보 변경을 요청하는 CEO 사기 이메일의 예

**권고 사항:**

개인의 세부 정보 변경을 요청하는 경우 이를 확인하는 절차를 확립하십시오.

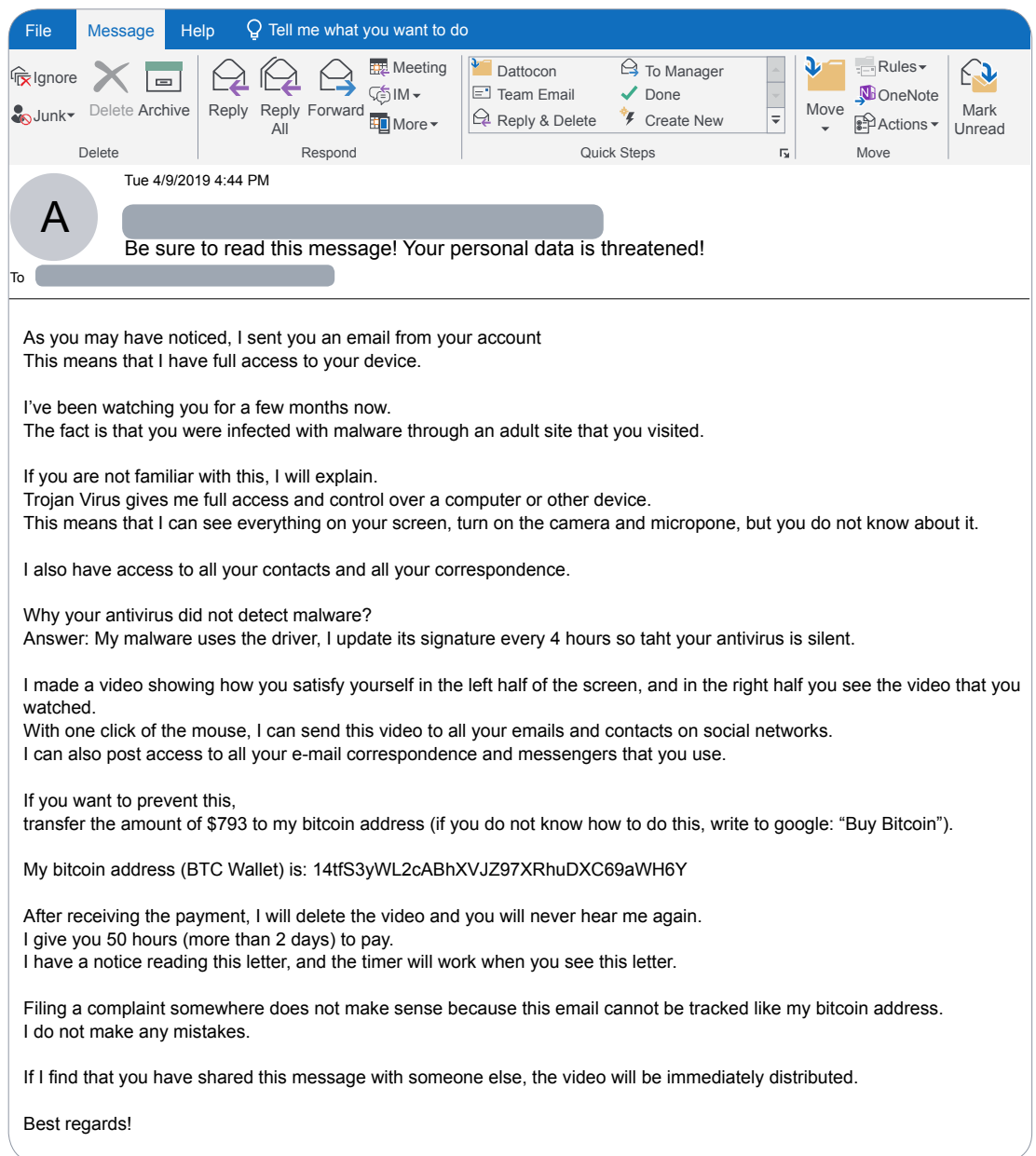


# 강탈 공격

2018년부터 2019년 1분기까지 내내, FireEye는 특정 유형의 강요 또는 갈취 협박 공격이 증가하는 것을 목격했습니다. 해커는 수신자가 대가를 지급하지 않으면 평판이 훼손되고 난처한 상황에 처하게 될 것이라고 위협합니다(그림 9).

그림 9.

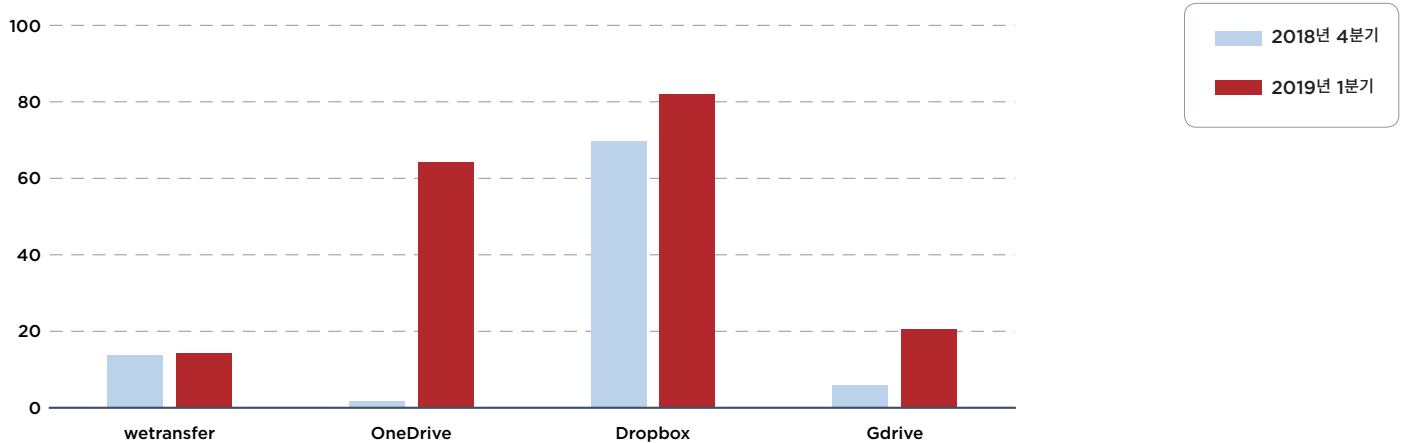
대가를 요구하는 강탈 이메일 공격의 예



# 악성 공격

공격자는 WeTransfer, Dropbox, Google Drive 및 OneDrive와 같이 널리 사용되는 파일 공유 서비스를 사용하여 악성 및 피싱 파일을 호스팅합니다. Dropbox가 가장 일반적으로 사용되지만, 2019년 1분기에는 OneDrive 탐지 횟수가 크게 증가했습니다(그림 10).

그림 10. 공격을 호스팅하는 데 사용되는 파일 공유 서비스



이처럼 잘 알려지고 신뢰할 수 있는 사이트는 보안 엔진이 수행하는 초기 도메인 평판 검사를 우회하기 때문에 공격자는 이러한 사이트들을 유용하다고 여깁니다. 악성 콘텐츠가 들어 있는 첨부 파일이 포함된 이메일을 표적에게 직접 보내는 대신, 공격자는 파일 공유 사이트에 콘텐츠를 업로드합니다. 공격 표적은 대기 중인 새 파일과 함께 파일을 다운로드할 수 있는 링크가 있다는 알림을 공유 서비스로부터 받습니다. 또한 이러한 서비스 중 일부는 콘텐츠를 보여주는 파일 미리 보기와 파일을 다운로드하지 않고도 클릭할 수 있는 URL을 제공합니다. 이로 인해 공격은 매우 효율적으로 변모하며 탐지하기 어렵습니다.

또한 FireEye는 공격에서 중첩된 이메일이 사용된 것을 관찰했습니다. 중첩 이메일에는 첫 번째 이메일에 두 번째 이메일이 첨부 파일로 포함되어 있습니다. 수신자가 첫 번째 메시지 맨 아래에 있는 첨부 파일을 클릭하면(그림 11), 첫 번째 메시지 내에 중첩된 두 번째 메시지로 이동합니다. 두 번째 이메일(그림 12)에는 일반적으로 악의적인 콘텐츠 또는 악성 URL이 있습니다. 중첩된 이메일은 탐지 필터의 기능에 지장을 줄 수 있습니다.



## 권고 사항:

공개적으로 호스팅되는 파일 공유 사이트에는 중요한 문서나 기밀문서를 저장하지 마십시오.

그림 11.  
중첩 이메일 공격에서  
기본 이메일의 예

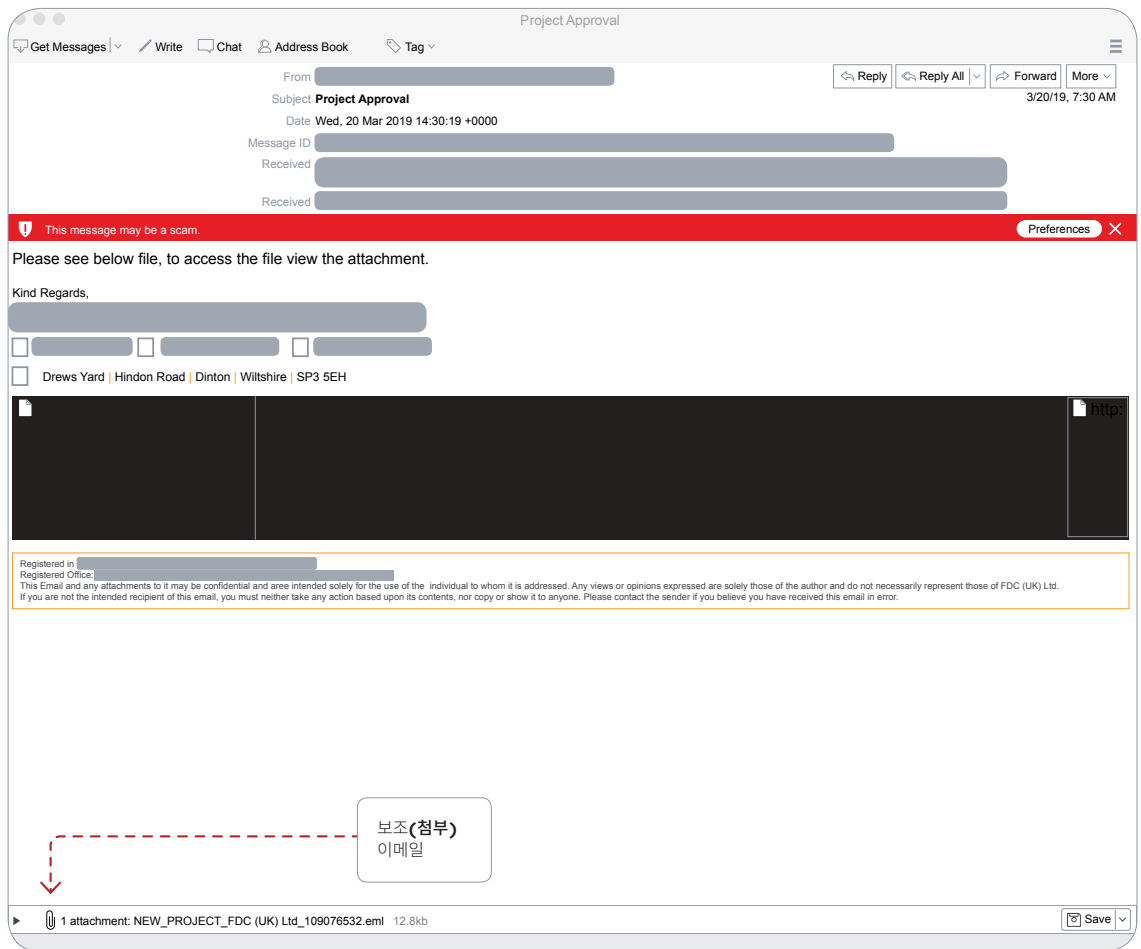
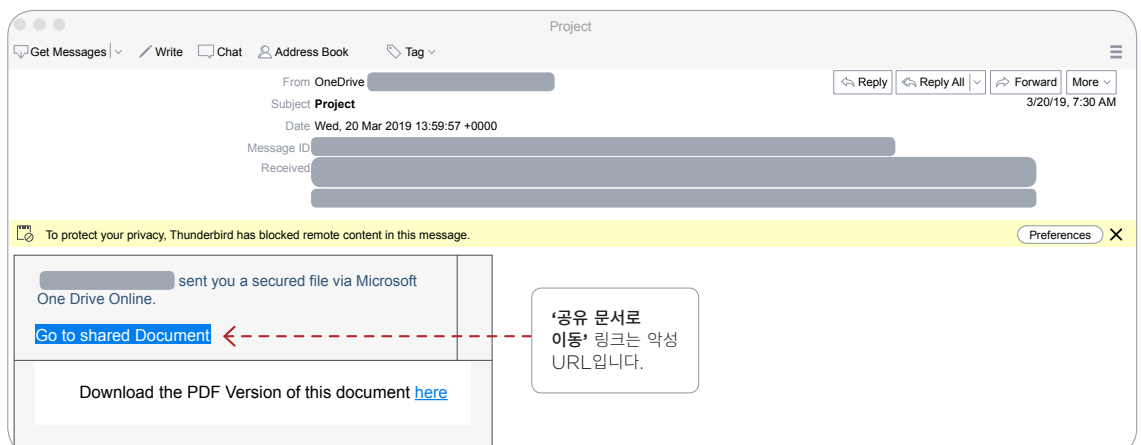


그림 12.  
중첩 이메일 공격에서  
보조(첨부) 이메일의 예



악의적인 캠페인의 필수 요소는 전달되는 악성코드입니다. FireEye가 1분기에 목격한 악성코드 유형으로는 Hancitor 및 Emotet이 있는데, 이러한 악성코드는 둘 다 수년간 존재했지만, 여전히 위력을 발휘하고 있습니다.

# 마케팅 스팸

FireEye가 2019년 1분기에 관찰한 마케팅 스팸 중 한 유형은 통신 스레드가 포함된 이메일입니다. 제목에는 흔히 답장(RE:) 또는 전달(FW)이 포함되는데, 이는 이메일이 기존의 연속적인 이메일의 일부라는 오해를 강화시키는 전술입니다(그림 13).

예를 들어 첫 번째 대화는 제시하는 제품 또는 서비스 소개로 시작됩니다. 두 번째 대화는 계속해서 “이전 이메일에 따라...”라는 문장으로 시작됩니다. 이러한 문장은 보낸 사람이 몇 번이나 연락 시도를 한 것 같은 느낌을 수신자에게 주기 위한 것입니다. 스레드의 어느 지점에서 보낸 사람은 수신자에게 자신이 상대방의 시간을 뺏거나 상대방을 귀찮게 하는 것을

원하지 않는다고 말합니다. 보낸 사람은 대화를 끝내려면 답장을 보내 ‘관심 없음’을 표현하도록 수신자에게 권장합니다.

호기심을 유발하는 이 소셜 엔지니어링 전술을 사용함으로써 공격자는 피해자에게 ‘죄책감’을 불러일으켜 응답하도록 합니다. 응답함으로써, 피해자는 자신의 이메일 주소가 유효하고 활성 상태임을 공격자에게 확인시켜 줍니다. 이로 인해 피해자는 미래의 공격 표적이 되거나 판매 대상 목록의 가능한 연락처가 됩니다.

**그림 13.**  
존재하지 않는 이메일  
체인을 참조하는 스팸  
마케팅의 예

**From:** [REDACTED]  
**Sent:** Friday, April 12, 2019 4:39 PM  
**To:** [REDACTED]  
**Subject:** Updating [REDACTED] sales presentation | [REDACTED] chat

Hi [REDACTED]  
Haven't heard back from you- maybe there's someone on your team you think I should talk with instead about upgrading the presentation you're using? We can review what your current deck looks like and provide you with a scorecard of how you compare against similar businesses along with specific recommendations on how to improve.

Would that be valuable to you?

Best -  
[REDACTED]

P.S. Most sales presentations are broken because they are not set up to be "discussion guides". That a look at some before-n-after examples on our [home page](#). We can upgrade your deck to be engaging and memorable. [opt out](#).

[REDACTED]  
Founder, CMO  
[REDACTED]  
[REDACTED]  
[Linkedin](#)

**From:** [REDACTED]  
**Date:** 2019-04-08 15:26:37.354  
**To:** [REDACTED]  
**Subject:** Updating [REDACTED] sales presentation | [REDACTED] chat

Hi [REDACTED]  
Getting back to you on this - does it make sense to talk? (see thread) How does Thursday morning work for you? We can review your current presentation looks like and offer some upgrade recommendations based on what we know works. If not, stay tuned for an invite to a webinar soon on how to turn your presentation into a conversation.

Best,  
[REDACTED]

P.S. I conducted a [webinar in January](#) on why you must turn your presentation into a conversation and 3 ways how - you might find interesting. If you'd rather not hear from me again let me know or [opt out](#).



공개된 도메인  
블랙리스트에  
의존하면 조직이  
취약해질 수 있습니다.

## 신생 도메인

FireEye는 피싱 이메일을 전달하고 기타 악의적인 캠페인을 제공하는 데 신생 도메인이 지속적으로 사용되는 것을 목격하고 있습니다. 따라서 FireEye는 신생 도메인의 트래픽을 모니터링합니다. 공개된 도메인 블랙리스트에 의존하면 조직이 취약해질 수 있습니다. 새 도메인은 블랙리스트에 등재되지 않으며 사기 행위 시도에 사용될 수 있습니다.

FireEye가 최근에 접한 한 사례에서 두 당사자는 상당한 금액의 판매가 성사될 수 있는 협상에 관계되어 있었습니다. 어느 당사자도 인지하지 못한 상태에서 한 회사가 피싱 이메일을 통해 침해당했습니다. 공격자는 전자 대화를 모니터링하고 있었습니다. 거래가 최종 단계로 나아감에 따라 공격자는 판매 회사의 도메인을 스푸핑한 새 도메인을 설립했습니다. 공격자는 구매자에게 이메일을 보내 구매 프로세스의 다음 단계를 알려주었습니다. 구매자는 메일에 지정된 은행 계좌로 최종 금액을 이체해야 했습니다. 구매자는 해당 금액을 송금했으며, 상당한 금액의 손실을 보았습니다.

## 맺음말

사이버 범죄자는 이메일 공격이 전반적으로 증가한 2019년 1분기에 승승장구했습니다. 특히 파일 공유 서비스에서 클라우드 기반 공격은 1분기에 현저한 증가세를 보였습니다. 비즈니스 프로세스가 클라우드로 계속 이동함에 따라 필연적으로 클라우드가 공격의 초점이 될 것입니다. 공격 및 회피가 더욱 정교해짐에 따라 기업은 최상의 인텔리전스 및 솔루션으로 무장하고 있는지 확인해야 합니다. 이러한 목표 달성을 앞당기기 위해 본 정기 이메일 위협 보고서는 계속해서 중요한 공격 및 공격자 정보를 모니터링하고 공개하겠습니다.

수상으로 우수성을 인정받은 FireEye Email Security는 다른 제품이 안전하다고 인정한 이메일 트래픽에서 지능형 위협을 탐지합니다.

간단한 3단계 분석을 통해 귀사의 기존 솔루션에서 탐지되지 않는 위협을 확인해 보십시오.

#### 무료 분석 받기

더 자세한 정보를 보려면 [www.FireEye.com/email](http://www.FireEye.com/email)을 방문하십시오.

#### FireEye Korea

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

©2019 FireEye, Inc. 저작권 소유. FireEye는 FireEye, Inc.의 등록상표입니다. 다른 모든 브랜드, 제품 또는 서비스 명칭은 각 소유자의 상표 또는 서비스 마크입니다.  
E-EXT-R-US-EN-000199-01

#### 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.

