BEC 및 EAC 공격 특성 분석

송효준, 김경백
전남대학교 정보보안협동과정

Analysis of BEC and EAC Attack Types and Characteristics

Hyo-Jun Song, Kyungbaek Kim
Interdiciplinary Program of Information Security, Chonnam National University

요 약

전자 메일 계정을 이용하여 거래처나 CEO를 사칭하여 금전적 피해나 민감한 정보를 탈취하는 BEC(Business Email Compromise) 공격이 자주 발생하고 있다. FBI에 의하면 이러한 공격은 2016년부터 2019년 까지 전 세계에서 260억 달러의 피해를 입혔다. 또한 비슷한 공격으로 이메일 계정을 탈취하여 사서함에서 민감 정보를 탈취하거나 해당 계정을 사칭하여 또 다른 피해자를 만드는 EAC(Email Account Compromise) 공격이 있다. 이 논문에서는 BEC와 EAC 공격들의 유형을 분류하고 공격 방식에 대해 분석한다.

I. 서론

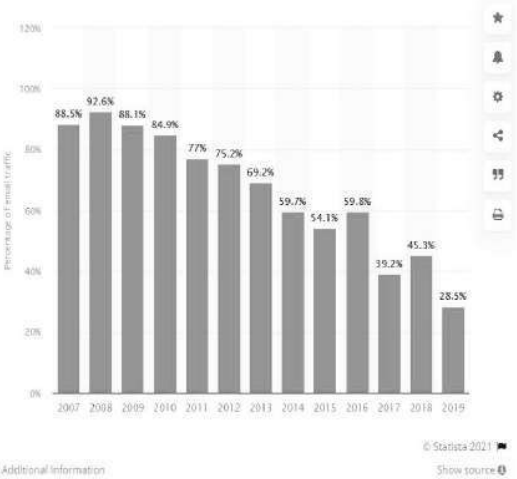
많은 기업들은 보안 수준이 과거에 비해 상당히 높아졌다. 보안부서를 따로 두어 실시간 트래픽 감시 시스템, 방화벽 ,접근제어 시스템 등을 운용하고 있다. 이 때문에 공격자들은 서버 중심의 직접 공격이 어려워졌다.

최근 공격자 입장에서 비용과 시간이 많이 드는 보안 시스템을 뚫는 것보다, 개인을 속여 이득을 취하는 것이 비용이 저렴하기 때문에, BEC 및 EAC와 같은 공격이 많아지는 추세이다. BEC 공격에 대한 피해는 2019년 한 해 동안 FBI의 집계한 바에 따르면 17억 7천만 달러에 달하고, 사건 수는 23,775건이라고 한다. 또한 공기업을 대상으로 한 Kimsuky 공격 조직의 이메일을 이용한 사이버 공격이 2013년부터 2019년까지 수차례 보고된 바 있다. 이는 BEC 공격이 일반 기업이나 국가를 대상으로 표적의 분포가 넓다고 볼 수 있다.

이에 이 논문은 해당 BEC와 EAC 공격들의 유형과 특징을 분석하고 대응 방법에 대해 제안하고 향후 연구 방향을 제시한다.

II. 관련연구

이메일에 대한 공격은 1990년대에 스팸 메일



그림[1]Global spam volume as percentage of total e-mail traffic from 2007 to 2019(Joseph Johnson, Jan 25, 2021)

에 대한 것을 중점으로 연구가 시작되었다. 최근에는 스팸메일 필터링을 위해 AI를 도입하는 등 높은 수준의 필터링을 보여주고 있다.

2007년 2019년부터 전체 메일에 대한 스팸메일 비율은 점차 감소하고 있다. 그림[1]

하지만 BEC나 EAC 공격에 관한 피해는 계속 증가하고 있으며 기존 스팸메일 위주의 필터

[그림 2] 200% increase in invoice and payment fraud BEC attacks

링으로 는 대응이 어려운 상황이다 이에 BEC와 EAC공격의 차별점을 분석하고 효과적인 차단 방안이 필요한 상황이다.

III. BEC와 EAC 공격 특성 분석

3.1 첨부파일 위장을 통한 공격

공격자는 해당 기업의 구매자를 사칭하여 발송하는 것이 일반적이다. 그림 1 과같이, 첨부파일을 실행 시 사용자에게 계정 정보 입력을 요구하는 화면으로 표시된다. 이때 입력 시 해당 계정은 다시 공격자의 사칭 계정이 되어 다른 피해자를 속이는데 악용된다.

[그림 3]공격자가 구매자로 위장하여 이메일 발송

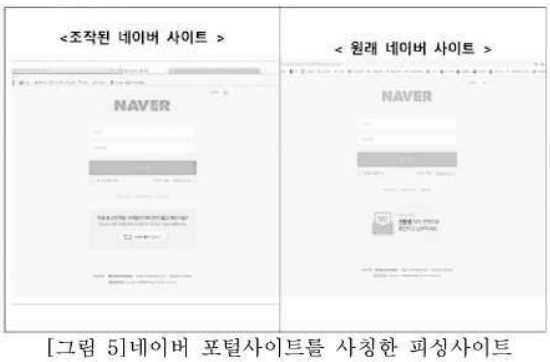
3.2 상급자를 가장한 이메일 공격

사이버테러 조직 김수키는 '코로나 바이러스 관련 이사장님 지시사항' 이라는 메일을 유포 했다. 해당 첨부 파일은 매크로가 삽입된 문서로, 실행시 사용자의 정보를 전송한다.

[그림 4]상급자를 가장하여 코로나 지시 사항을 전달

3.3 포털사이트를 위장한 공격

해당 사용자의 계정이 해킹 위협이나 또는 비밀번호 변경 안내이메일을 보내어 조작된 사이트에 개인정보를 입력하도록 유도한다. 이때 입력한 개인정보는 공격자에게 넘어가 추가적인 패해자를 발생한다.



[그림 5]네이버 포털사이트를 사칭한 피싱사이트

3.4 보안 메일을 위장한 공격

사용자에게 은행이나 국세청같은 중요 기관

[그림 6]KEB하나은행 보안메일을 위장한 악성 메일

에서 온 이메일처럼 속여 보안메일과 동일하게 생년월일 6자리를 입력하게하고, 이후 열리는 xls 파일에서 악성 매크로가 포함되어 'outgoing.dll' 악성모듈 드롭 및 'glitch' 파라메

터로 'EXCEL.exe' 프로세스에 로드 한다.

3.5 해당 공격들의 공통점

불특정 다수의 회사나 기업 이메일에 상사나 거래처 또는 보안 메일을 사칭한뒤 파일을 받게 하거나 사칭한 웹사이트로 이동하게 한다. 이때 파일을 받은 경우 악성코드에 감염되게 하거나 개인 정보를 입력한 경우 공격자에게 탈취 당하게 된다.

3.6 피싱 메일 공격의 목적

대부분의 공격들은 사용자의 결제정보나 민감정보를 이용하여 금전적인 이득을 취하고 있다. 그 이외에는 탈취한 계정을 가지고 해당 사용자로 위장하여 주변 사용자에게 공격을 하여 공격에 취약하게 하는데 사용하고 있다.

IV. 대응방안

4.1 이메일 보안 의식 강화

위 공격자들은 대부분 지인이나 거래처 공공기관을 위장하여 사용자에게 메일을 보내고 있다. 이러한 소셜 엔지니어링 방식으로 유포되는 피싱 메일로 이렇게 피해당한 계정들의 회사나 개인에게 2차 추가 피해를 가져올 수 있다. 때문에 회사라면 사내 보안팀에 보안 교육을 주기적으로 시행해야 하며 잘 못된 이메일이나 사칭 이메일로 의심될시 해당 메일이 정확한지 발송자와 추가적으로 확인을 할 필요가 있다.

4.2 내부망과 외부망 분리

사칭이 아닌 불특정 다수에게 보내는 DEC 공격은 외부 IP를 통해 들어온다. 이는 회사에서 보안팀을 운용 하지 않더라도 회사망과 외부망을 분리하여 내부로 들어오는 이메일을 점검해야 한다. 만약 인가 되지않은 IP로 이메일이 온다면 한번 확인할 필요가 있다.

V. 결론

본 논문에서는 점점 증가하는 BEC공격과 EAC 공격을 분석하였다. 공격자들의 패턴을 분석해 보았고 이러한 공격들이 피해자들에게 금전적 피해를 입힐 수 있다. 향후 연구로는 딥러닝이나 머신러닝을 활용한 BEC 공격 및 EAC 공격 탐지 기술을 계획 중이다.

ACKNOWLEGEMENTS

"이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임"(IITP-2019-0-01343)

[참고문헌]

[1] Joseph Johnson. (2021)Global spam volume as percentage of total e-mail traffic from 2007 to 2019. Available at:https://www.statista.com/statistics/420400/spam-email-traffic-share-annual/ (Accessed: 23.10.2021).

[2] Help Net Security. (2020)200% increase in invoice and payment fraud BEC attacks. Available at: https://www.helpnetsecurity.com/2020/06/30/payment-fraud-bec-attacks/ (Accessed: 23.10.2021).

[3] 금융보안관제센터 보안관제팀, 2020 사이버 위협동향:2020 사이버 위협동향,11

[4] 알약(Alyac), (2019)TA505조직, KEB하나은행 보안메일을 사칭한 해킹 이메일 다량 유포 중. Available at: https://blog.alyac.co.kr/2675 (Accessed: 23.10.2021).

[5]Lee, Dokyung, Gunsoo Jang, and Kyung-ho Lee. "AI를 통한 BEC (Business Email Compromise) 공격의 효과적인 대응방안 연구." 정보보호학회논문지 30, no. 5 (October 31, 2020): 835-46. doi:10.13089/JKIISC.2020.30.5.835.

[6]Lee, Jae-il, Yong-joon Lee, and Hyuk-jin Kwon. "피싱 메일 공격조직에 대한 프로파일링 사례 연구." 인터넷정보학회논문지 21, no. 2 (April 30, 2020): 91-97. doi:10.7472/JKSII.2020.21.2.91.

[7] 문가용. (2020)BEC 공격과 EAC 공격, 이메일 통한다고 해서 같은 게 아니다. Available at: https://www.boannews.com/media/view.asp?idx=93197 (Accessed: 23.10.2021).