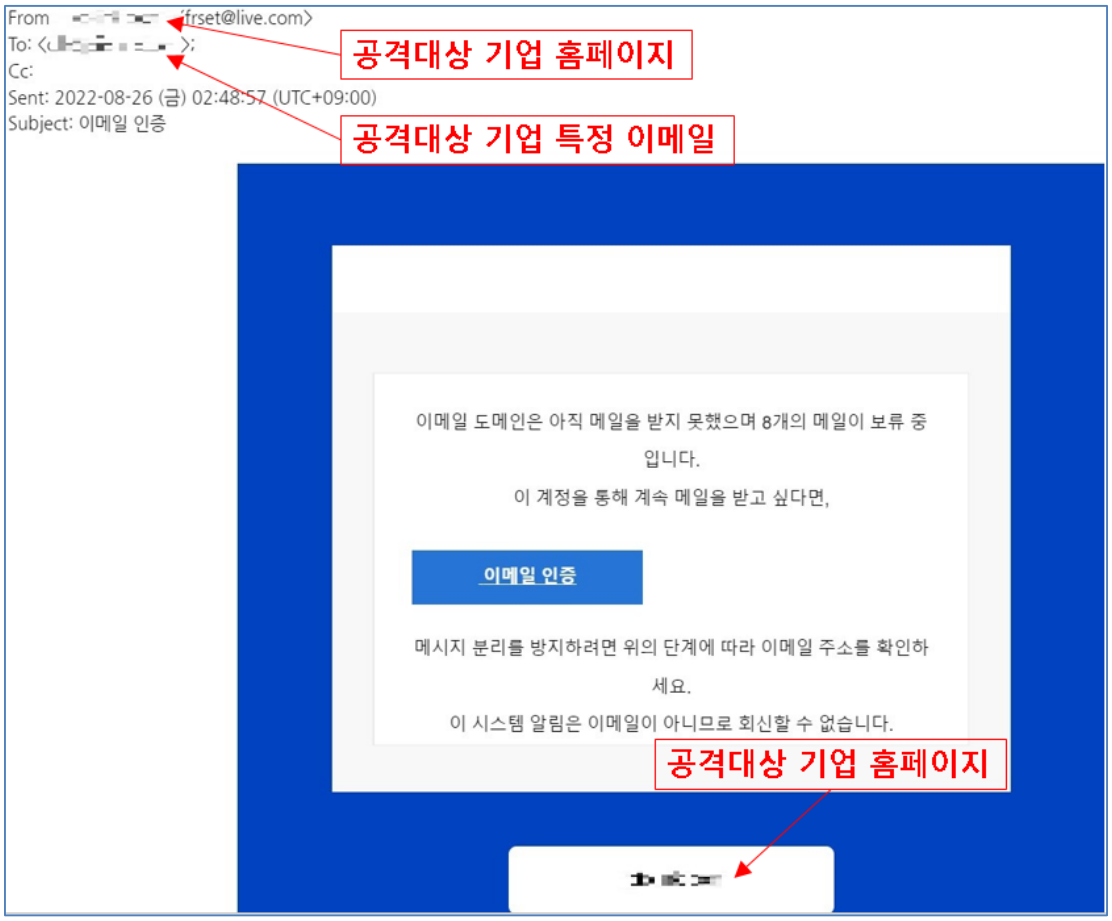
PIOLINK

설문조사폼을 이용한 계정정보 탈취

최근 국내 기업의 특정 인물을 대상으로 피싱 캠페인이 이루어지는 것을 확인하였다. 겉으로 보기에는 여타 다른 피싱 공격과 유사하게 보이지만 내부적으로는 정상 사이트에서 제공하는 설문조사 폼을 이용하여 공격에 활용하고 있다.

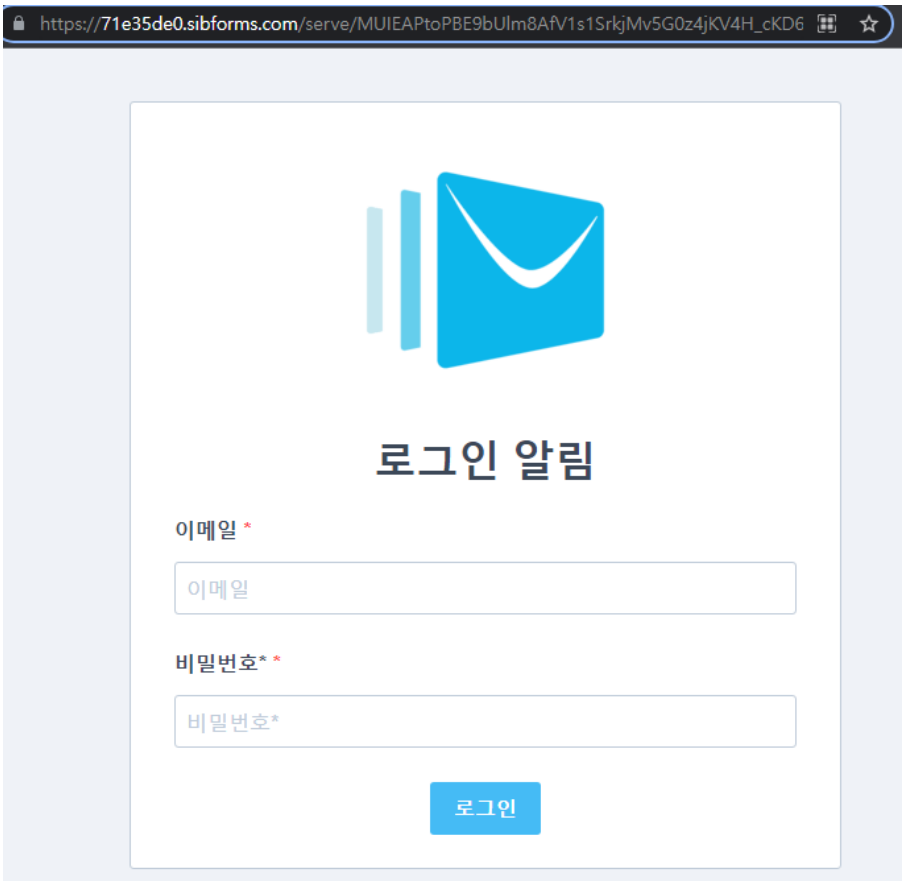
1. 피싱 메일 본문



<그림> 피싱메일 본문

보낸 사람은 frset@live.com 이메일을 사용하며, 보낸 메일서버 IP는 139.162.151.131, 보낸 국가는 독일로 확인되었으며, 이메일 제목은 "이메일 인증"으로 되어있으며 본문에는 8개의 메일이 보류 중에 있음을 알려, 궁금증을 유발하여 이메일 인증 버튼을 클릭하도록 유도하고 있다. 상하단에는 공격 대상 기업의 웹사이트 주소를 명시하여 받는이로 하여금 정상적인 이메일로 위장하고 있다.

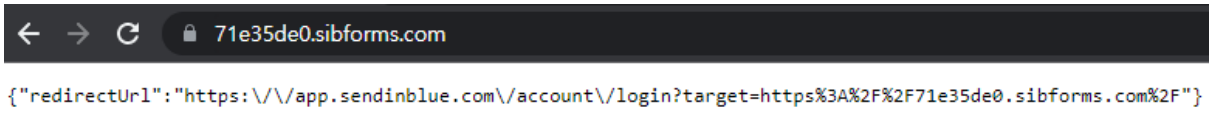
1) 이메일 인증 클릭



<그림> 이메일 인증 버튼 클릭 후 나타난 페이지

이메일 본문의 이메일 인증 버튼을 클릭하게 되면 위 그림의 페이지가 나타난다. 이메일과 비밀번호를 입력하게 되면 해당 계정은 특정 서버로 전송되며, 최종적으로 구글 페이지로 리다이렉션된다.

2. 공격 방법

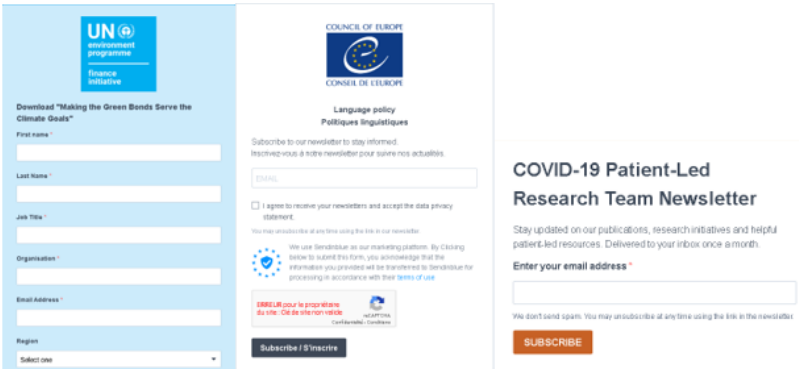


<그림> 도메인 방문시 나오는 리다이렉션 URL

도메인 방문시 리다이렉션 URL을 확인할 수 있다. 리다이렉션 URL인 sendinblue.com 은 마케팅, 영업을 위한 비즈니스 도구를 제공하는 업체로 본사는 프랑스 파리에 위치해 있으며, 델리, 시애틀, 베를린에 사무소를 운영하고 있다. 해당 업체는 다량의 이메일 발송, 설문조사 폼 등 비즈니스에 필요한 도구를 제공하고 있다.

<그림> sendinblue.com 에서 제공하는 폼 제공 사이트

공격자는 sendinblue.com 에서 제공하는 다량의 이메일 발송 기능과 설문조사에 필요한 폼을 활용하여 피싱 캠페인에 활용하고 있다. 설문조사 폼 대신 이메일과 비밀번호를 입력받는 폼을 정교하게 제작하여 피싱 메일을 보내는 것이다. 우리나라 네이버에서 제공하는 설문조사 폼을 활용하는 것과 유사하다고 이해하면 되겠다. 공격자는 최종적으로 sendinblue.com 에 접속하여 설문조사 결과에서 유출된 계정정보를 확인할 것으로 판단된다.



<그림> 정상적으로 사용 중인 sibforms 설문조사 예시

3. 마무리

과거와는 다르게 이메일 정보는 사이버 공격의 중요한 요소로 작용한다. 공격자들은 이메일 주소 수집 후 다수에게 스피어피싱 공격을 수행한다. 다수의 사람 중 한 명만 클릭하면 해당 기업은 침해당할 확률이 높다. 기업들은 외부 공개자료 등에 내부 이메일 주소 노출을 최소화하고 인증된 사용자에게만 공개하는 등의 세심한 노력이 필요하다.