



보도시점 2025. 4. 16.(수) 조간 누리망·방송 2025. 4. 15.(화) 12:00

‘방첩사 계엄 문건’ 사칭 전자우편은 북 소행

- 북 해킹조직이 2개월간 12만 통의 사칭 전자우편 발송
- 수신자 17,744명 중 120명은 계정정보 탈취 피해 발생

경찰청(국가수사본부)은 지난 '24년 12월 11일 ‘방첩사 작성한 계엄 문건 공개’라는 제목으로 발송된 전자우편 사건을 수사한 결과 북한의 소행으로 규명하였다. 아울러 북한 해킹조직은 개인정보 탈취 목적으로 '24년 11월부터 '25년 1월까지 사칭 전자우편을 17,744명에게 모두 126,266회 발송한 사실을 확인하였다.

본건 범행에 사용된 서버와 전자우편 등 관련 자료를 분석하고 한국인터넷진흥원과 협력하며 단서를 종합한 결과, ① 기존 북한발 사건에서 파악된 서버를 재사용 한 점, ② 사칭 전자우편 수신자가 통일·안보·국방·외교 분야 종사자인 점, ③ 범행 근원지 아이피(IP) 주소가 중국과 북한의 접경 지역에 할당된 점을 비롯하여 특히, 사칭 전자우편을 조직적으로 발송하기 위하여 임대한 서버에서 ④ 탈북자와 군 관련 정보를 수집하고 있던 점 ⑤ 인터넷 검색기록에서 북한식 어휘가 다수 확인된 점을 근거로 북한의 소행으로 결론지었다.

전자우편 발송은 해외 업체를 통해 임대한 서버 15대에서 자체 제작한 전자우편 발송용 프로그램을 통해 이루어졌다. 이 프로그램은 전자우편이 발송되는 시점부터 수신자의 열람·피싱 사이트 접속·계정정보 획득 등의 여부를 포함한 통계자료를 한눈에 파악할 수 있는 기능도 포함하고 있었다.

발송한 사칭 전자우편의 종류는 다양하였다. 계엄 문건의 첨부 사례를 비롯해 북한 신년사 분석과 정세 전망으로 위장한 고전적인 방식과 더불어 유명가수의 콘서트 관람권 초대장, 세금 환급, 오늘의 운세, 건강정보 등을 제공할 것처럼 위장하기도 하였다. 이러한 사칭 전자우편에는 바로가기(링크)가 포함되어 있었고, 이를 누르면 로그인에 필요한 아이디와 비밀번호를 요구하는 피싱 사이트로 연결되는 수법이었다.

해킹조직의 서버 기록으로 보아 발송된 사칭 전자우편은 17,744명에게 30개 유형으로 모두 126,266회 발송된 사실이 확인되었고, 사칭 전자우편 수신자 17,744명 중 120명은 피싱 사이트에 접속 후 자신의 아이디와 비밀번호를 입력하여 계정정보 및 보관함에 저장된 전자우편과 연락처 정보를 탈취당하는 피해를 입었다.

발송에 사용된 전자우편 주소는 공공기관을 연상케 하거나 지인의 전자우편 주소와 유사한 형태였으며, 사칭 사이트 또한 유명 사이트 주소에 몇 글자 추가하거나 유사한 철자로 구성되어 있었다.

사칭 전자우편 주소(예시)	피싱 사이트 주소(예시)
seoul-news@OOOO.com, net, org OOamssaeOOOO@OOOO.net	googlauth.com, naver-auth.com, kakao-auth.com, baernin.com
△ 포털 아이디로 정부기관 사칭 -news, -noreply, -report 등 추가 △ 지인의 아이디에 s 등 철자 추가한 유사 아이디를 생성하여 사칭	△ 익숙한 인터넷 주소에 -auth, -verify, -login, -cloud, -service 등 추가 △ m→rn, co.kr → co.kro.kr 유사철자 사용

【사칭용 전자우편 및 피싱 사이트 주소 사례】

사칭 전자우편으로 인한 피해를 예방하기 위해서는 발송자가 불분명한 전자우편은 열람하지 않거나 첨부파일과 링크를 클릭하지 않는 등 원칙적인 대응이 매우 중요하다. 또한, 아이디와 비밀번호 등 중요정보를 입력하기 전, 요구하는 자의 전자우편과 웹사이트 주소를 주의 깊게 살펴본다면 사전에 피해를 예방할 수 있다. 이외에도 전자우편 아이디와 비밀번호가 노출되지 않도록 철저히 관리하면서, 주기적으로 본인의 접속 이력을 확인하는 것이 도움이 된다.

경찰은 어떠한 유형의 사이버 공격에 대해서도 엄정하고 신속하게 대응할 수 있도록, 국내외 관계기관들과의 협력체계를 굳건히 하는 등 치안역량을 총동원하여 대응해 나갈 예정이다.

경찰수사사건등의 공보에 관한 규칙 제5조(예외적 공개 사유)

위 범죄사건은 공보규칙상 아래와 같은 예외적 공개사유에 해당합니다.

- ☒ [유사범죄 재발의 방지] 범죄유형과 수법을 국민들에게 알려 유사한 범죄의 재발을 방지할 필요가 있는 경우
- ☐ [신속한 피의자 검거등] 인적·물적 증거의 확보를 위하여 국민들에게 협조를 구할 필요가 있는 경우
- ☒ [피해확산 방지 필요] 범죄로 인한 피해의 급속한 확산을 방지하고 대응조치 등을 국민들에게 알리기 위함
- ☐ [오보·추측성 보도 대응] 사건관계인의 인권이 침해되는 등 사실관계를 바로잡을 필요가 있는 경우

담당 부서	국가수사본부 수사국 사이버테러대응과	책임자	총경	주진화 (02-3150-0053)
		담당자	경정	김영운 (02-3150-1459)

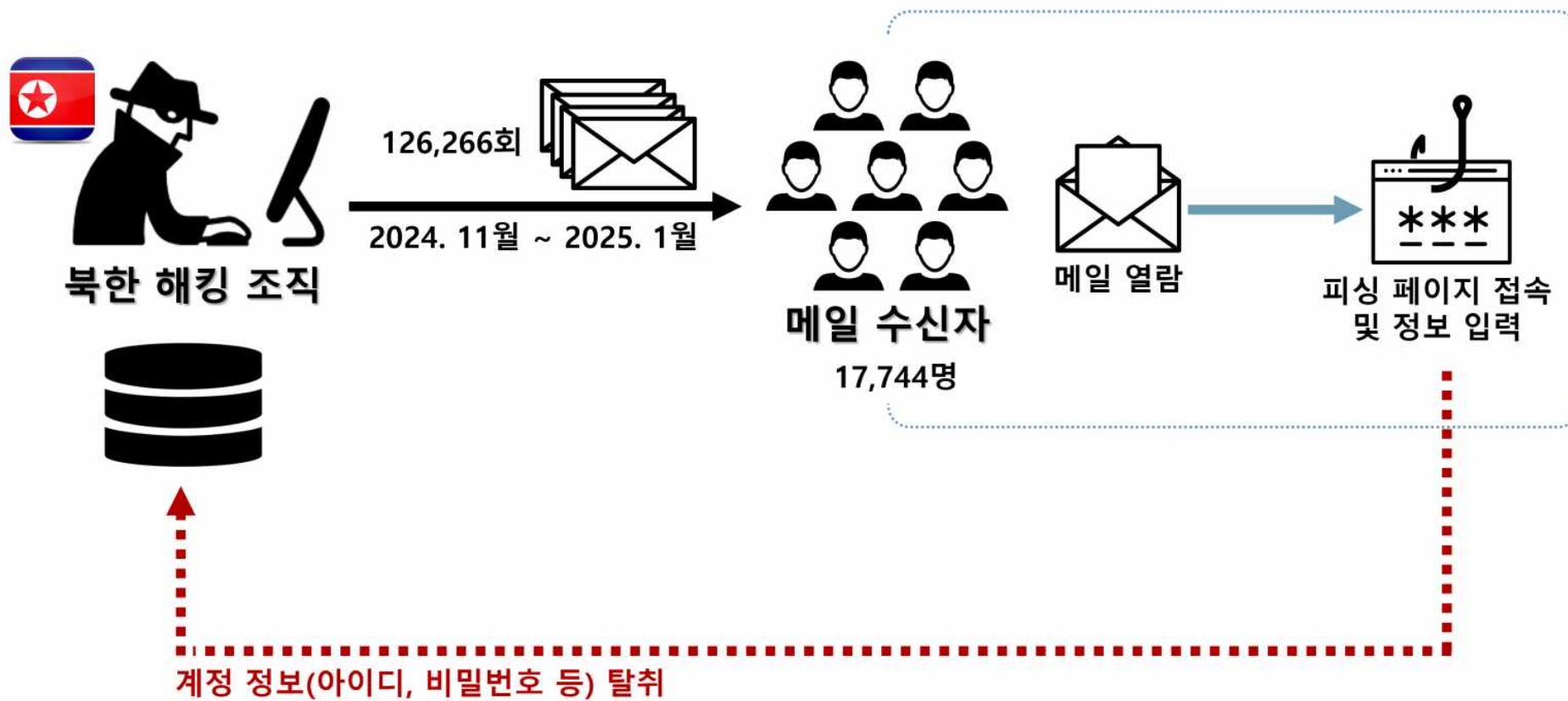


더 아픈 환자에게 양보해 주셔서 감사합니다
가벼운 증상은 동네 병·의원으로



붙임 1

북한발 사칭 전자우편 우편 개요도



붙임 2

북한발 사칭 전자우편 사례

