경찰청 **보 도 자 료** 다시 도약하는 대한민국 함께 잘사는 국민의 나라

보도 일시	2022. 12. 26.(월) 조간	누리망·방송	2022. 12. 25.(일) 09:00
담당 부서	국가수사본부 사이버수사국 사이버테러대응과	책임자	총경 정석화(02-3150-0053)
		담당자	경정 이규봉(02-3150-1459)

기자·국회의원실 등 사칭 전자우편 발송사건, 북 해킹조직 소행으로 확인

-교수 등 49명의 전자우편 감시, 일부 업체 서버에는 랜섬웨어 유포-

경찰청 국가수사본부(사이버수사국)에서는 지난 4. 28. 발송된 『제20대 대통령직 인수위원회』 출입기자를 사칭한 전자우편 및 『태영호 국회의원실』 비서를 사칭한 전자우편(5. 7.), 『국립외교원』을 사칭한 전자우편(10. 26.)에 대한 수사결과, 2013년부터 파악된 북한의 특정 해킹조직 소행으로 확인하였다.

북한 해킹조직은 국내외 무차별 해킹을 통해 26개국 326대(국내 87대)의 서버 컴퓨터를 장악하며 사이버테러를 위한 기반을 확보하였고, 이를 수사기관의 추적을 회피하기 위한 아이피(IP) 주소 세탁용 경유지로 이용하였다.

북한 해킹조직은 IP주소를 세탁한 뒤, 기자·국회의원실 등을 사칭하며 피싱 사이트로 유도하거나 악성 프로그램을 첨부한 전자우편을 외교·통일·안보·국방 전문가에게 발송하였다. 이러한 사칭 전자우편은 최소 892명에게 발송되었다.

피싱 사이트에 접속해 자신의 아이디와 비밀번호를 입력한 외교·통일·안보·국방 분야 종사자 49명이 확인되었으며, 북한 해킹조직은 이들 피해자의 송·수신 전자우편을 실시간으로 감시하며 첨부 문서와 주소록 등을 빼내 간 것으로 파악되었다.

특히, 이번 수사로 북한 해킹조직이 금품 요구 악성 프로그램(랜섬웨어)을 유포한 사실이 국내에서는 최초로 확인되었다. 장악한 서버 중 일부에는 랜섬웨어를 감염시켜 금전을 요구하였으며, 확인된 피해 규모는 국내 13개 업체의 서버 19대이다.

경찰청 등 정부 기관은 그간 국내외 민간 보안업체에서 일명 '김수키(Kimsuky)' 등으로 명명한 북한의 특정 해킹조직을 여러 차례 수사한 바 있으며, 이번 사건 또한 기존 북한발로 규명된 『한국수력원자력 해킹 사건(2014년)』 및 『국가안보실 사칭 전자우편 발송사건(2016년)』과 비교하여, △공격 근원지의 아이피(IP) 주소 △해외 사이트의 가입정보 △ 경유지 침입·관리 수법 △ 악성 프로그램의 특징 등이 같고, △ 북한어휘를 사용하는 점, △범행 대상이 외교·통일·안보·국방 전문가로 일관된 점 등을 근거로 같은 북한 해킹조직의 소행으로 판단하였다.

경찰청은 피해자와 소속 기업에 피해 사실을 통보하고, 한국인터넷진흥원 및 백신업체와 협력하여 피싱 사이트를 차단하는 한편, 관계기관에 북한 해킹조직의 침입 수법·해킹 도구 등 관련 정보를 제공하여 정보보호 정책 수립에 활용하도록 하였다.

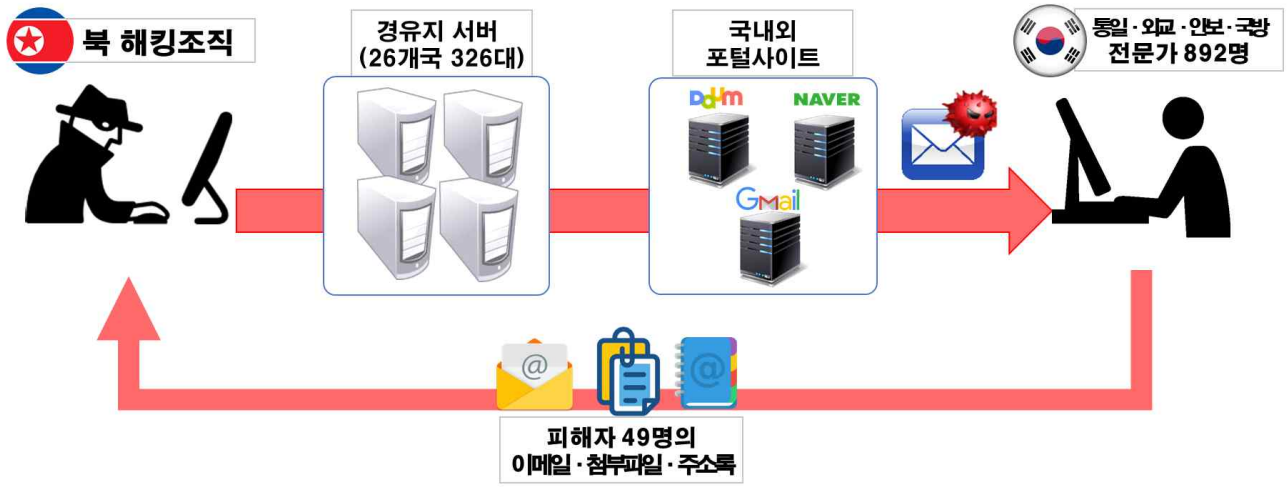
경찰청은 북한의 이러한 시도가 앞으로도 지속할 것으로 예상되므로 전산망에 대한 접근통제, 전자우편 암호의 주기적 변경 및 2단계 인증 설정, 다른 국가로부터의 접속 차단 등 보안 설정 강화를 당부하였다.

또한, 경찰청은 앞으로도 치안 역량을 총동원하여 조직적 사이버 공격을 탐지·추적함과 동시에 관계기관과 긴밀히 협력하며 피해 방지를 위해 노력해 나아갈 계획이다.

붙임) 1. 사건 개요도
2. 기자·국회의원실 사칭 전자우편

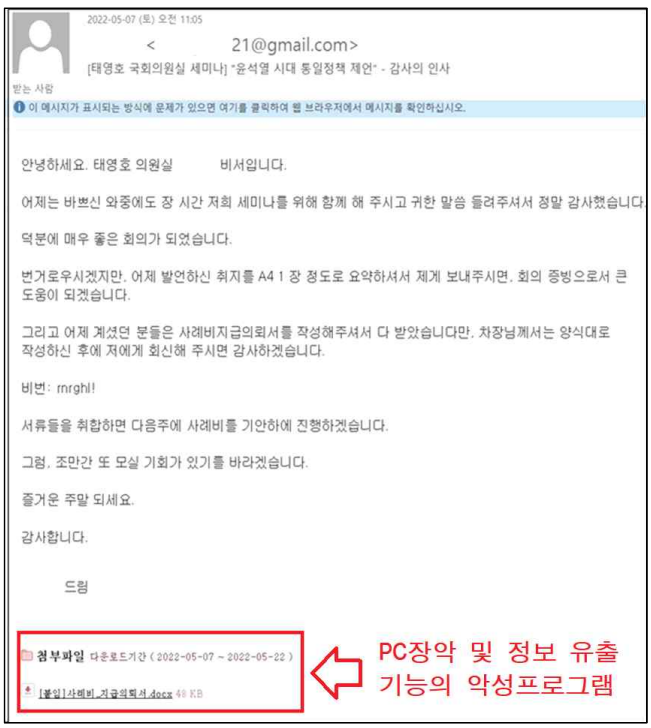
붙임 1 사건 개요도

북한발 사칭이메일 유포사건 개요도

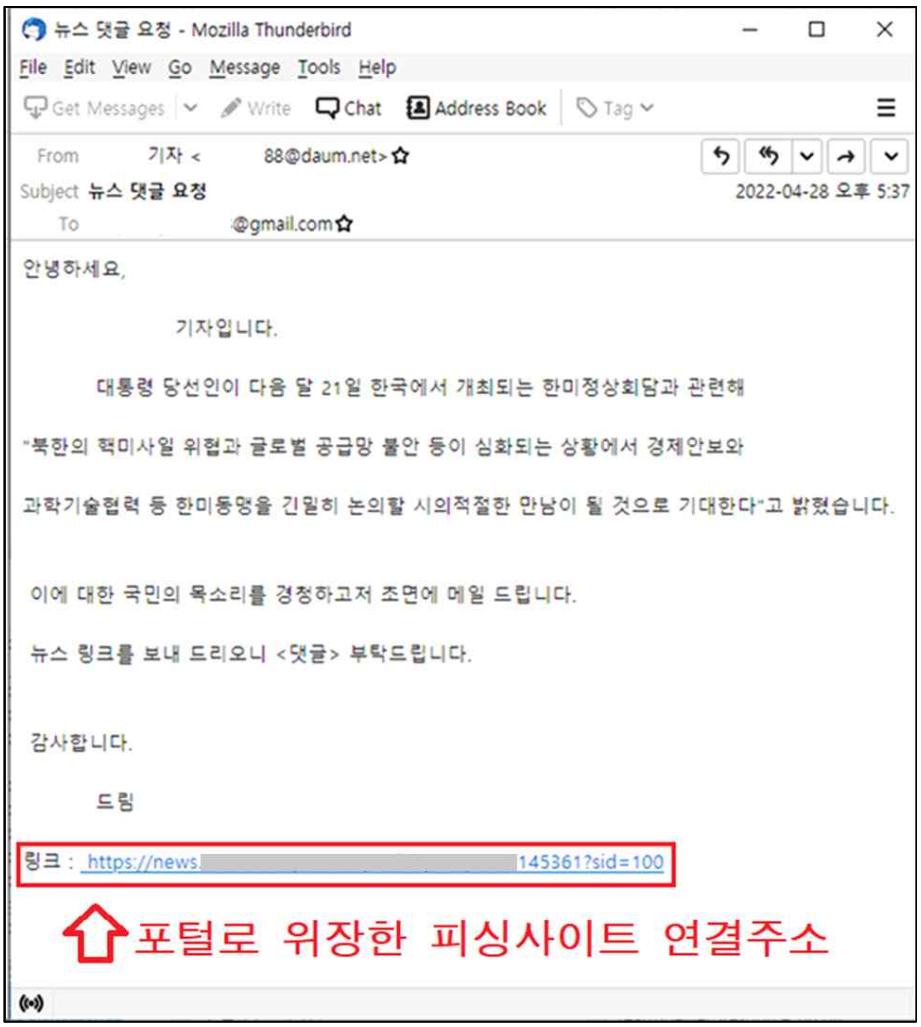


붙임 2 사칭 전자우편

○ 국회의원실 사칭 전자우편



○ 기자 사칭 전자우편


뉴스 댓글 요청 - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages Write Chat Address Book Tag
From 기자 < 88@daum.net>
Subject 뉴스 댓글 요청
2022-04-28 오후 5:37
To @gmail.com
안녕하세요,
기자입니다.
대통령 당선인이 다음 달 21일 한국에서 개최되는 한미정상회담과 관련해
"북한의 핵미사일 위협과 글로벌 공급망 불안 등이 심화되는 상황에서 경제안보와
과학기술협력 등 한미동맹을 긴밀히 논의할 시의적절한 만남이 될 것으로 기대한다"고 밝혔습니다.
이에 대한 국민의 목소리를 경청하고저 조면에 메일 드립니다.
뉴스 링크를 보내 드리오니 <댓글> 부탁드립니다.
감사합니다.
드림
링크 : https://news 145361?sid=100
포털로 위장한 피싱사이트 연결주소