경찰청 보도자료 다시 대한민국! 새로운 국민의 나라

보도시점 2023. 6. 8.(목) 조간 **누리망·방송** 2023. 6. 7.(수) 12:00

정부 교체기 안보 전문가 대상 악성 전자우편 유포사건, 북(北) 소행 확인

- 전현직 고위공무원·교수 등 150명 대상 악성 전자우편 발송 확인
- 해킹에 성공할 때까지 단계별로 공격 시도, 안보 분야 관계자 주의 필요

경찰청 국가수사본부(안보수사국)은 지난해 4월부터 7월까지 안보 분야 주요 관계자를 대상으로 발송된 악성 전자우편 사건을 수사한 결과, 북한의 특정 해킹조직 소행으로 확인하였다.

북한 해킹조직은 통일·안보 전문가 등을 사칭하여 2022년 4월부터 7월까지 새 정부 출범 기간에 맞춰 전현직 고위공무원, 대학교수, 외교·통일·안보·국방 전문가 150명을 대상으로 피싱 사이트 접속을 유도하여 계정 정보를 탈취하는 악성 전자우편을 발송한 것으로 확인되었다.

북한 해킹조직은 국내외 해킹을 통해 138개(국외 102개, 국내 36개)의 서버를 장악하여 해킹 공격을 위한 기반을 확보하고, 추적을 피하고자 아이피(IP) 주소를 세탁하였다. 각 서버는 악성 전자우편 발송, 피싱 사이트 구축, 탈취정보 전송 등 기능별로 구분되어 있었는데, 이는 수사기관의 추적을 피하고 한 번에 발각되지 않기 위한 목적으로 판단된다.

사칭 전자우편에 속아 피싱 사이트에 접속해 자신의 아이디와 비밀번호를 입력한 피해자는 총 9명으로 확인되었고, 북한 해킹조직은 이들의 송수신 전자우편을 실시간으로 확인하고 첨부 문서와 주소록 등을 빼간 것으로 파악되었다.

이번 사건은 경찰청이 국가정보원(국가사이버안보센터)와 사이버 위협정보 공유를 통해 피해를 인지한 것으로, 최초 수사에 착수한 제주경찰청(첨단안보수사계)와 경찰청 안보수사국, 국정원은 5,800여 개 전자우편 분석과 추적 수사를 진행하였고, 관계기관 합동으로 피해 보호* 조치를 완료하였다.

* ▵피해자 및 소속 기관에 피해 사실을 즉시 통보 ▵관계기관과 협업 피싱 사이트 차단 ▵공격 수법 등 관련 정보 관계기관 공유

경찰청은 이번 사건을 그간 국내외 민간 보안업체에서 일명 '김수키(Kimsuky)' 등으로 명명한 북한 해킹조직의 소행으로 판단하고 있으며, ▵공격에 사용한 아이피(IP) 주소 ▵경유지 구축 방법 ▵북한식 어휘 문구* ▵공격 대상이 대부분 외교·통일·안보·국방 전문가인 점 등을 근거로 판단하였다.

* "봉사기"(서버), "랠 쯤에"(북 래일-남 내일), "적중한 분"(적합한 분)

한편, 일명 '김수키' 해킹조직은 정보 탈취 공격에 집중하는 것으로 알려져 있으나, 이번 수사를 통해 공격 서버에서 이들이 사용한 가상자산 지갑 주소를 발견하였으며, 금전 탈취도 시도하고 있는 것으로 판단하고 추적 수사를 계속 진행하고 있다.

이번 사건을 통해 북한 해킹조직의 공격 수법은 더욱 치밀해지고 있는 것으로 확인되었다. 지난해 새 정부 출범을 전후해 피해자들의 지인 및 안보 분야 여론 주도층을 사칭하는 사회공학적 방법으로 치밀하게 접근을 시도하였으며, 공격은 다음 4단계로 진행되었다.

첫 번째, 피해자의 입장에서 최대한 자연스러운 접근을 시도한다. 교수·연구원을 사칭하였다면 책자 발간이나 논문 관련 의견을 요청하는 내용, 언론 기자를 사칭하였다면 인터뷰나 자료를 요청하는 내용으로 정상적인 전자우편을 1차적으로 발송한다.

두 번째, 피해자가 회신 전자우편을 보냈다면 절반의 성공으로, 공격자는 다시 답장을 보내면서 대용량 문서 파일을 내려받도록 유도한다.

세 번째, 공격자는 보안이 강화되어 문서 파일을 열기 위해서는 본인 인증이 추가로 필요하다며 가짜 피싱 사이트로 연결한다. 이때 피해자가 인증 요구에 응하여 아이디(ID)와 비밀번호를 입력하면 계정 정보를 탈취하는 방식이다. 공격자는 탈취한 정보로 전자우편 수발신함에 남겨진 정보를 가로채거나, 또 다른 해킹 공격에 악용하기도 하였다.

마지막으로, 목적을 달성한 공격자는 피해자에게 감사 답장을 발송하여 의심을 차단하였다. 경찰이 연락하기 전까지 악성 전자우편을 받은 사실을 전혀 인지하지 못한 피해자도 있었다.

경찰청은 "안보 분야 관계자를 대상으로 한 북한의 해킹 시도가 지속해서 이어질 것으로 전망하고, 전자우편 비밀번호의 주기적인 변경과 본인 인증 설정 강화, 해외 접속 차단, 의심스러운 전자우편 재확인 등 보안 조치를 강화해 줄 것을 당부드린다."라고 하였다.

아울러, "앞으로도 국가안보에 위협이 되는 사이버 공격 동향과 대응 사례를 관계기관과 적극적으로 공유하는 한편, 북한 해킹조직의 불법 사이버 활동에 대한 선제 대응을 강화해나갈 계획이다."라고 밝혔다.

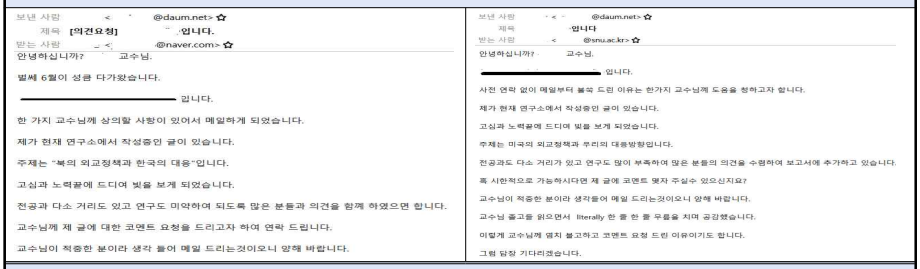
붙임: 1. 사건 개요도
2. 단계별 악성 전자우편 공격 수법

담당 부서	국가수사본부 안보수사국 안보수사지휘과	책임자	총경 김근만 (02-3150-2092)
		담당자	경정 박현준 (02-3150-2492)

붙임1 사건 개요도

붙임2 단계별 악성 전자우편 공격 수법

[STEP: 1] 최대한 자연스러운 접촉 시도(정상적인 전자우편 전송)



보낸 사람 < @daum.net> ✩
제목 [의견요청] 입니다.
받는 사람 <@naver.com> ✩
안녕하십니까? 교수님.

벌써 6월이 성큼 다가왔습니다.

입니다.

한 가지 교수님께 상의할 사항이 있어서 메일하게 되었습니다.

제가 현재 연구소에서 작성중인 글이 있습니다.

주제는 "북의 외교정책과 한국의 대응"입니다.

고심과 노력끝에 드디어 빛을 보게 되었습니다.

전공과 다소 거리도 있고 연구도 미약하여 되도록 많은 분들과 의견을 함께 하였으면 합니다.

교수님께 제 글에 대한 코멘트 요청을 드리고자 하여 연락 드립니다.

교수님이 적중한 분이라 생각 들어 메일 드리는것이오니 양해 바랍니다.

보낸 사람 < @daum.net> ✩
제목 입니다
받는 사람 < @snu.ac.kr> ✩
안녕하십니까? 교수님.

입니다.

사전 연락 없이 메일부터 불쑥 드린 이유는 한가지 교수님께 도움을 청하고자 합니다.

제가 현재 연구소에서 작성중인 글이 있습니다.

고심과 노력끝에 드디어 빛을 보게 되었습니다.

주제는 미국의 외교정책과 우리의 대응방향입니다.

전공과도 다소 거리가 있고 연구도 많이 부족하여 많은 분들의 의견을 수렴하여 보고서에 추가하고 있습니다.

혹 사안적으로 가능하시다면 제 글에 코멘트 몇자 주실수 있으신지요?

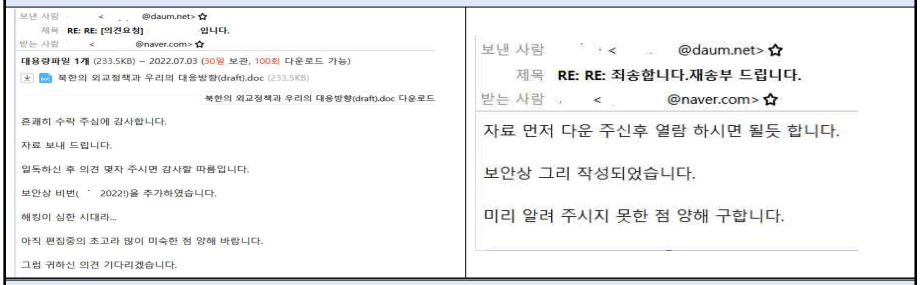
교수님이 적중한 분이라 생각들어 메일 드리는것이오니 양해 바랍니다.

교수님 졸고를 읽으면서 literally 한 줄 한 줄 무릎을 치며 공감했습니다.

이렇게 교수님께 염치 불고하고 코멘트 요청 드린 이유이기도 합니다.

그럼 답장 기다리겠습니다.

[STEP: 2] 피해자가 회신하면 절반의 성공, 대용량 자료 다운로드 유도



보낸 사람 < @daum.net> ✩
제목 RE: RE: [의견요청] 입니다.
받는 사람 < @naver.com> ✩
대용량파일 1개 (233.5KB) - 2022.07.03 (30일 보관, 100회 다운로드 가능)
북한의 외교정책과 우리의 대응방향(draft).doc (233.5KB)

북한의 외교정책과 우리의 대응방향(draft).doc 다운로드

흔쾌히 수락 주심에 감사합니다.

자료 보내 드립니다.

일독하신 후 의견 몇자 주시면 감사할 따름입니다.

보안상 비번(2022!)을 추가하였습니다.

해킹이 심한 시대라...

아직 편집중의 초고라 많이 미숙한 점 양해 바랍니다.

그럼 귀하신 의견 기다리겠습니다.

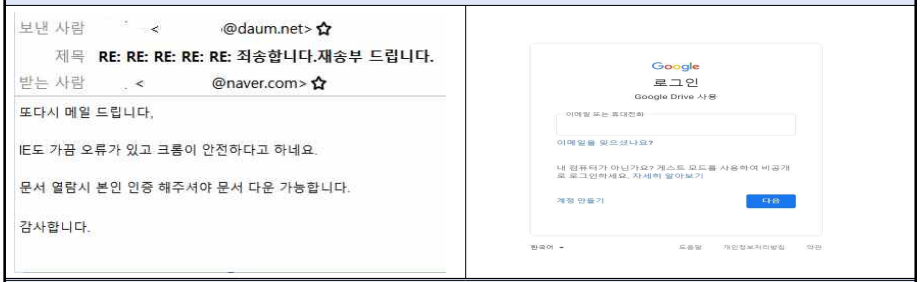
보낸 사람 < @daum.net> ✩
제목 RE: RE: 죄송합니다.재송부 드립니다.
받는 사람 < @naver.com> ✩

자료 먼저 다운 주신후 열람 하시면 될듯 합니다.

보안상 그리 작성되었습니다.

미리 알려 주시지 못한 점 양해 구합니다.

[STEP: 3] 보안이 강화되었다며 상용 전자우편 본인 인증 요구



보낸 사람 < @daum.net> ✩
제목 RE: RE: RE: RE: RE: 죄송합니다.재송부 드립니다.
받는 사람 < @naver.com> ✩

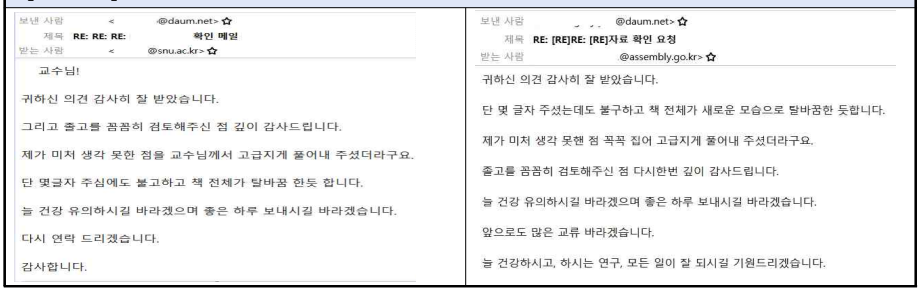
또다시 메일 드립니다,

IE도 가끔 오류가 있고 크롬이 안전하다고 하네요.

문서 열람시 본인 인증 해주셔야 문서 다운 가능합니다.

감사합니다.

[STEP: 4] 목적 달성한 후에 감사 답장으로 의심 회피



보낸 사람 < @daum.net> ✩
제목 RE: RE: RE: 확인 메일
받는 사람 < @snu.ac.kr> ✩

교수님!

귀하신 의견 감사히 잘 받았습니다.

그리고 졸고를 꼼꼼히 검토해주신 점 깊이 감사드립니다.

제가 미처 생각 못한 점을 교수님께서 고급지게 풀어내 주셨더라구요.

단 몇글자 주심에도 불고하고 책 전체가 탈바꿈 한듯 합니다.

늘 건강 유의하시길 바라겠으며 좋은 하루 보내시길 바라겠습니다.

다시 연락 드리겠습니다.

감사합니다.

보낸 사람 @daum.net> ✩
제목 RE: [RE]RE: [RE]자료 확인 요청
받는 사람 @assembly.go.kr> ✩

귀하신 의견 감사히 잘 받았습니다.

단 몇 글자 주셨는데도 불구하고 책 전체가 새로운 모습으로 탈바꿈한 듯합니다.

제가 미처 생각 못한 점 꼭꼭 집어 고급지게 풀어내 주셨더라구요.

졸고를 꼼꼼히 검토해주신 점 다시한번 깊이 감사드립니다.

늘 건강 유의하시길 바라겠으며 좋은 하루 보내시길 바라겠습니다.

앞으로도 많은 교류 바라겠습니다.

늘 건강하시고, 하시는 연구, 모든 일이 잘 되시길 기원드리겠습니다.