경찰청 보도자료 다시 대한민국! 새로운 국민의 나라

보도시점 2023. 8. 21.(월) 조간 누리망·방송 2023. 8. 20.(일) 09:00

한미연합연습 노린 북 '김수키' 소행 사이버 공격 확인

- 올해 상반기, 한미연합연습에 파견된 국내 업체 직원 대상 악성 전자우편 공격
- 미군 수사기관과 공조, 북 '김수키' 해킹조직 소행 규명

경찰청 국가수사본부(안보수사국)는 올해 2월부터 한미연합연습 전투모의실에 파견된 국내 워게임(War Game) 운용업체 직원들을 대상으로 발송된 악성 전자우편 사건을 수사한 결과, 북 해킹조직의 소행으로 확인하였다.

이번 사건은 미군 수사기관이 해킹 공격을 인지한 후 경찰과 정보공유를 통해 피해 사실을 확인하였고, 경기남부경찰청(안보수사과)이 미군 수사기관과 공조하여 추적 수사 및 피해 보호조치를 진행하였다.

수사 결과, 북 해킹조직은 작년 4월부터 국내 워게임 운용업체를 해킹하기 위해 악성 전자우편 공격을 지속하였고, 올해 1월경에는 해당 업체 소속 행정직원의 전자우편 계정을 탈취하고 업체 컴퓨터에 악성코드를 설치하는 데 성공한 것으로 밝혀졌다.

이후 원격접속을 통해 피해업체의 업무 진행 상황과 전자우편 송수신 내용을 실시간으로 확인하고, 업체 전 직원의 신상정보를 탈취한 것으로 확인되었다.

북 해킹조직은 탈취한 자료를 활용하여 올해 2월부터 연말정산 시기에 맞춰 '원천징수영수증'으로 위장된 악성 전자우편을 한미연합연습 전투모의실에 파견된 피해업체 직원들을 대상으로 발송하였다.

이를 수신한 직원들이 미 국방 전산망에서 악성 첨부 문서를 실행하려 하였으나, 보안시스템에 의해 악성코드가 차단되어 군 관련 정보는 탈취되지 않은 것으로 확인되었다.

다만, 일부 직원들이 해당 전자우편을 외부 계정으로 재전송하여 열람하는 과정에서 개인용 컴퓨터가 악성코드에 감염된 것으로 밝혀졌다.

경찰청과 미군 수사기관은 공격 사용된 아이피(IP)가 과거 '한국수력원자력 해킹 사건(2014년)'에서 확인된 아이피(IP) 대역과 일치하며, 탈취한 자료를 자동으로 전송하는 기능이 포함된 악성코드가 사용된 사실을 확인하였다.

아울러, ▲경유지 구축 방법 등 기존 공격과 유사성 ▲북한식 어휘 '넘두(염두)' ▲한미연합연습 시기에 맞춰 공격한 점 등을 종합 판단한 결과, 이번 사건을 북 해킹조직 일명 '김수키(Kimsuky)' 소행으로 판단하였다.

경찰청과 미군 수사기관은 합동으로 피해업체의 공용 및 개인용 컴퓨터에 대해 악성코드 감염 여부를 점검하는 등 보호조치를 완료하였고, 추가 피해 예방을 위해 한미연합연습에 참여하는 근무자를 대상으로 보안교육을 실시하였다.

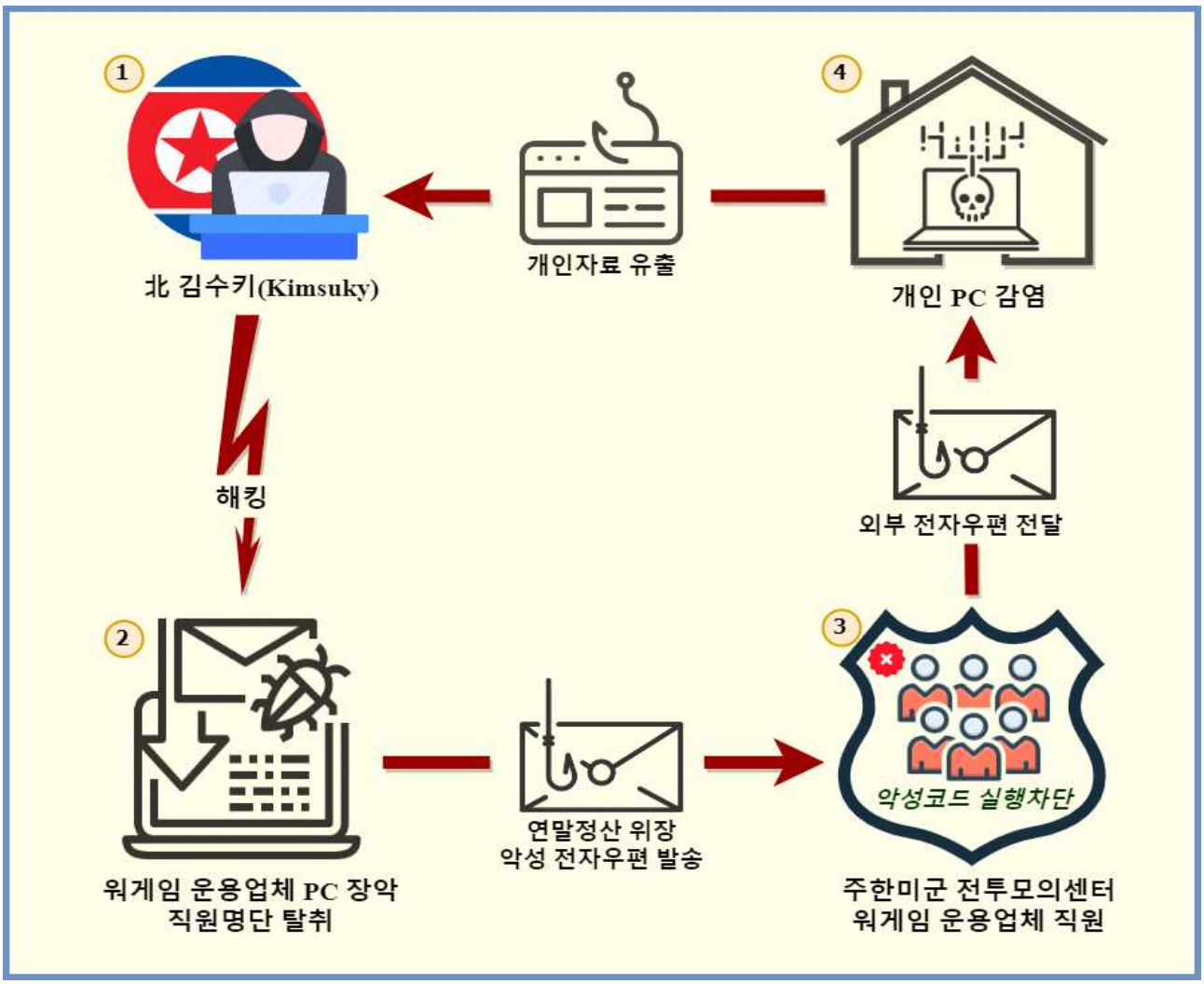
한편, 한미연합 군사연습인 '을지 자유의 방패(UFS)'(8월 21일~31일)를 한 달여 앞둔 지난 7월, 미 육군 인사처를 사칭한 전자우편이 주한미군 한국인 근무자들에게 발송된 사실을 추가 확인하고, 경기남부경찰청(안보수사과)이 미군 수사기관과 공조수사를 계속 진행하고 있다.

경찰청은 "한미 간 유기적인 협업과 선제 조치로 주한미군의 자료 유출을 예방한 사례이다."라며, "앞으로도 국가안보에 위협이 되는 북한의 사이버 공격에 적극적으로 대응해나갈 계획이다."라고 밝혔다.

붙임1. 해킹 공격 개요도
붙임2. 공격에 사용된 악성 전자우편

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

붙임1 | **해킹 공격 개요도**



① 한미연합연습 워게임 운용업체 해킹 → ② 피해업체 관리자 PC 장악하여 직원 신상정보 탈취 → ③ 한미연합연습 전투모의실 파견 업체 직원에게 악성메일 전송 〈미군 전산망에서 악성코드 실행 차단〉 → ④ 해당 이메일을 외부 전자우편으로 전달 〈개인 PC로 열람하여 악성코드 감염 → 자료유출〉

붙임2	공격에 사용된 악성 전자우편

□ 연말정산 위장 악성 전자우편

보낸사람: "[redacted]" <[redacted]@naver.com>
받는사람: "Lee, [redacted])" <[redacted]@army.mil>
날짜: 2023-02-07 (화) 15:02:02
제목: RE: [Non-DoD Source] 연말정산 공제신고서

죄송합니다.
저는 세무법인[redacted] 서울지점 세무사무실 담당자입니다.
연말정산자료 정리하던중 이[redacted] 님의 자료에서 뭔가 오류가 생겨서 본인께 직접 확인해야할 부분이 있어 메일드렸습니다.
보내드린 문서에서 국민건강보험료부분에 대한 확인을 해주셨으면 합니다.
보내드린 문서는 초안파일이여서 PC에서만 열릴겁니다.
만일 잘열리지 않으면 알집설치를 부탁드립니다.
암호는 20230207입니다.
확인결과에 대한 회답은 메일로 해주시면 됩니다.
불편을 드려 죄송합니다.

□ 북한식 어휘 문구: ‘념두’

받는 사람 [redacted]@army.m[redacted]
제목 RE: [Non-DoD Source] 연말정산 공제신고서

념두 뜻: '염두'의 북한어.
념두: '염두'의 북한어. (어휘 명사 한자어 북한어)

감사합니다.
오류란 저희쪽 데이터 백업시 계산상 착오가 발생한것을 념두에 둔것입니다.
그러나 고객님의 확인을 통해 수정되었으므로 더이상 다른문제는 없습니다.
서비스에 불편을 드려 죄송합니다.