이 보도자료는 2015. 3. 17.(화) 14:00 이후에 보도하여 주시고, 이 보도자료를 통해 공개되는 범죄사실 중에는 아직 재판을 통해 확정되지 않은 사실도 있음에 유의하여 주시기 바랍니다.

보 도 자 료

2015. 3. 17. (화)

주책임자 : 3차장검사 최윤수
자료문의 : 개인정보범죄 정부합동수사단
전화번호 : 02-530-4285

제 목 **한수원 사이버테러 사건 중간수사결과**

❍ **개인정보범죄 정부합동수사단**(이하 '합수단)은 '14. 12. 15.부터 '15. 3. 12.까지 총 6회에 걸쳐 한국수력원자력㈜(이하 '한수원') **관련 자료를 공개하며 원전중단을 협박한 사건**에 대해 수사한 결과,

- 본건 협박 직전인 '14. 12. 9.~12. **한수원 직원 3,571명에게 5,986통의 악성코드(파괴형) 이메일을 발송**하여 PC 디스크 등을 파괴하려 시도하였으나, PC 8대만 감염되고 그중 5대의 하드디스크가 초기화되는 정도에 그쳐 **원전 운용이나 안전에는 이상이 없음**

❍ 범인(조직)은 이메일에 **피싱(phishing) 메일을 보내 한수원 관계자들의 이메일 비밀번호를 수집한 후 그 이메일 계정에서 자료들을 수집하는 등** 범행을 사전에 준비하였으며, '14. 12. 9.~12. 한수원에 대한 이메일 공격이 사실상 실패로 돌아가자, 해킹 등으로 취득한 한수원 자료 등을 공개하며 본건 협박에 이른 것으로 판단되고,

본건과 관련하여 범인은 거의 대부분 중국 선양 IP를 통해 국내 (주)H사 VPN 업체 IP로 접속함

❍ 합수단에서 본건 범행에 사용된 **악성코드와 인터넷 접속 IP 등을 분석한 결과**,

- ① 본건 이메일 공격에 사용된 악성코드는 **북한 해커조직이 사용하는 것으로 알려진 'kimsuky(김수키)' 계열 악성코드**와 그 구성 및 동작방식이 거의 같고,

- ② 본건 악성코드에 이용된 'ᄒᆞ글 프로그램' 버그(취약점)가 **'kimsuky' 계열 악성코드에 이용된 버그와 동일**하며,

- ③ 'kimsuky' 계열 악성코드들의 IP 일부가 본건 협박글 게시에 사용된 **중국 선양 IP 대역들과 12자리 중 9자리까지 일치**하고,

- ④ 범인이 본건 자료 탈취/이메일 공격/협박글 게시 루트로 도용한 국내 (주)H사 VPN 업체와 관련하여, 동 회사가 관리하는 다른 접속 IP 중에서, '14. 12. 하순 **북한 IP 주소** 25개, **북한 체신성 산하 통신회사 KPTC에 할당된 IP 주소** 5개가 접속한 흔적이 발견되었으며,

- ⑤ 본건 범행은 **국민안전과 직결되는 국가인프라 시설인 원전**을 대상으로 전 국민에게 지속적이고 공개적으로 협박을 하여 **사회불안을 야기하고 국민들의 불안심리를 자극한 사건**임이 밝혀졌음

❍ 위와 같은 정황을 종합하면, 본건 범행은 **금전보다는 사회적 혼란 야기가 주목적**인 **북한 해커조직의 소행으로 판단되며**, 검찰은 본건 범행에 대하여 철저히 수사를 계속하겠음

Ⅰ 수사착수 경과

1. 한수원에 대한 이메일 공격 ('14. 12. 9.~12. 12.)

● **한수원 직원 이메일 계정으로 악성코드 이메일 공격발생**

- '14. 12. 9.경 발송인 211명 이메일 계정으로부터 한수원 직원 3,571명을 수신인으로 하여 악성코드가 첨부된 이메일 총 5,986통이 발송되었음

※ 12. 9. 5,980건 / 12. 10. 3건 / 12. 11. 1건 / 12. 12. 2건 발송

● **공격 이메일에 첨부된 악성코드**

- 위 공격 이메일에 첨부된 한글(hwp) 파일을 실행하면 악성코드가 실행되어, ① 파일실행 장애, ② 하드디스크 초기화, ③ 네트워크 장애유발 등의 문제 발생

※ 위 악성코드에 "자료유출 기능"은 없는 것으로 확인되었음

● **한수원의 신속한 차단조치**

- '14. 12. 9. 이메일 공격 직후 한수원은 신속히 이메일 수신을 차단하고, 수신된 악성이메일을 거의 모두 삭제하였음

2. 한수원 자료공개 및 협박 ('14. 12. 15.~'15. 3. 12.)

● **'14. 12.경 이후 총 6차에 걸쳐 한수원 자료공개 및 협박**

- '14. 12. 15.경(1차) 네이버에 '우리는 원전반대그룹! 끝나지 않은 싸움'이라는 글을 게시하면서, 한수원 임직원 주소록 파일 등을 공개

- 12. 18.(2차) / 12. 19.(3차) / 12. 21.(4차) / 12. 23.(5차) 트위터 등에 '크리스마스 때까지 원전 가동을 중지하고 100억 달러를 주지 않으면 보유한 (원전)자료를 계속 공개하겠다'는 취지의 글을 게시

- '15. 3. 12.경(6차) 트위터에 '돈이 필요하다'는 글과 함께 한수원의 원전 도면 등을 재차 게시

※ 1차 ~ 5차 협박글 게시는 중국 선양 IP 대역(175.167.***.***, 175.167.***.***, 175.167.***.***, 175.167.***.***)을 이용하여 접속하였으며, 6차 협박글 게시는 러시아 블라디보스토크 IP를 이용하여 접속하였는데, 6차 게시에 사용된 트위터 계정(john_kdfifj1029)이 종전 협박글 게시에 사용된 계정과 동일

3. 개인정보범죄 정부합동수사단의 수사착수 ('14. 12. 19.)

- **합수단은 한수원의 수사의뢰 직후 즉시 수사착수**
  - 한수원은 '14. 12. 19. 임직원 주소록 개인정보파일 유출, 원전자료 유출 및 원전중단 협박사건을 합수단에 수사의뢰 하였고, 합수단은 즉시 수사착수
- **합수단의 유관기관 공조 및 국제적 수사 진행**
  - 합수단은 국가정보원, 대검 과학수사부·국제협력단, 경찰청 사이버안전국, 방송통신위원회, 한국인터넷진흥원, 안랩(AhnLab) 등과 공조하여 수사진행
  - 경유지 IP 서버 소재지 국가들(미국·중국·일본·태국·네덜란드 등)과도 국제수사공조를 통해 범인추적

Ⅱ 공개된 한수원 자료의 내용 및 유출경로

1. 공개된 한수원 자료내용

- **총 6회에 걸쳐 94개 파일**(빈 파일 제외) **공개**
  - 총 6차에 걸쳐 한수원 임직원 주소록, 전화번호부, 원전관련 도면 등 파일 94개가 공개되었음
- **공개된 자료는 원전관리 중요정보는 아님**
  - 한수원 자체점검 결과, 6차에 걸쳐 공개된 자료들은 원전운용과 관련한 핵심자료가 아니며 교육용 등 일반문서가 대부분이고, 원전관리에 위험을 초래하거나 원전수출 등 국가적 원전정책에 영향을 미칠 수 있는 중요정보의 유출은 없다는 점검결과임

2. 한수원 자료 유출경로

- **유출자료 상당 부분은 협력업체 직원 이메일 등을 통해 유출된 것으로 확인**
  - '14. 12. 공개된 파일들에 대해서는 유출경로가 대부분 확인되었는바, 위 파일들은 한수원 내부망에서 직접 유출된 것이 아니라 협력업체 직원 등 한수원 관계자 이메일에 보관되어 있던 자료들이 유출된 것으로 확인

○ w1_10_1000_50×22.jpg 파일 등의 유출경로

- 위 파일들은 한수원 협력업체 ㈜AOO 대표 조OO의 PC에 저장되어 있던 파일로 확인
- 조OO 대표는 '14. 7.경 악성 코드가 포함된 한글 문서가 첨부된 이메일을 수신
- 조OO 대표의 PC에 원격제어 악성프로그램이 설치되어, PC 내 정보가 유출되었음

※ '14. 7.경 조OO 대표에게 발송되어 온 이메일은 '14. 12.경 협박글 게시에 이용된 것과 동일한 중국 선양 IP에서 발송되었으며, 협박글을 게시하는데 사용한 것과 동일한 국내 VPN IP를 통해 PC에 있던 정보가 유출되었음

○ DRAWING_WOLSONG34.zip 파일 등의 유출경로

- 위 협력업체 ㈜AOO 부장 배OO의 PC에 저장되어 있던 자료가 유출된 것으로 추정

※ 위 ㈜AOO 임직원들의 이메일은 중국 선양 등에서 발송된 피싱 메일에 의해 이메일 비밀번호가 노출된 상태였음

○ K-DOSE 60 Ver. 2.1.2.jpg 파일 등의 유출경로

- 한수원 협력업체 ㈜BOO 대표 김OO의 PC 및 이메일이 해킹되어 유출된 것으로 추정

● **한수원 퇴직자 등에게 '피싱(phishing)' 메일을 보내 이메일 비밀번호 수집**

- '14. 9.경까지 한수원 퇴직자 36명에게 이메일 비밀번호를 수집하기 위한 '피싱(phishing)' 메일 88건이 발송되었음
- "비밀번호가 유출되었으니 확인 바란다"는 등의 미끼성 이메일을 전송하고, 메일 클릭시 비밀번호 변경창이 뜨도록 하여 비밀번호를 입력하도록 유도

※ 위 피싱메일 발송자와 '14. 12.경 협박글 게시자는 동일인으로 추정

- ① 위 피싱메일 발송 IP 주소가 '14. 12.경 협박글 게시에 사용된 중국 선양 IP 주소와 12자리 중 9자리가 동일하고, ② 탈취되는 정보가 전달되는 국내 호스팅 업체 서버도 동일

● **유출된 비밀번호로 임직원 이메일 계정과 커뮤니티에 있는 정보수집**

○ KHNP+주소록.xlsx 파일의 유출경로

- '14. 8.경 '한수원 임직원 커뮤니티 사이트'에 중국 선양 IP에서 한수원 퇴직자 박OO의 계정으로 무단접속하여 커뮤니티에 있던 임직원 주소록 유출

○ 본사전화번호부.pdf, 한수원2직급.pdf 파일의 유출경로

- 한수원 직원 하OO의 이메일 내에 있던 정보가 유출된 것으로 추정

⇒ **공개된 자료들은 '14. 12.경 한수원에 대한 악성 이메일 공격으로 내부망에서 직접 유출된 것이 아니라, 피싱메일을 통해 한수원 관계자들의 이메일 비밀번호를 수집한 후 그 이메일 계정에서 수개월간 수집한 자료들을 공개한 것임**

Ⅲ 범인 추적결과

1. 인터넷 접속 IP 및 악성코드 분석결과

● **중국 선양에서 국내 VPN 업체를 통해 국내 포털사에 접속하여 협박글 게시**

- ① 중국 선양 IP ⇒ ② 국내 VPN 업체 IP ⇒ ③ NAVER, NATE, Daum, Twitter, Facebook 등에 협박글 게시한 것으로 확인

- 협박글을 게시한 포털사 계정가입자들은 명의를 도용당한 것으로 확인되었고, 위 국내 VPN 업체 IP 사용자 역시 명의 도용당한 것으로 확인되었음

※ VPN(Virtual Private Network)은 공중인터넷망을 전용사설망처럼 이용할 수 있도록 통신체계와 암호화기법을 제공하는 서비스로서, 외국에서 국내 VPN 업체를 통해 국내 포털에 접속하면 마치 국내 IP에서 접속한 것처럼 보여짐

● **북한 해커조직이 사용하는 것으로 알려진 악성코드와의 유사성**

- '14. 12. 한수원 이메일 공격에 사용된 악성코드들은 북한 해커들이 사용하는 것으로 알려진 'kimsuky(김수키)' 계열 악성코드들과 구성 및 동작방식이 매우 유사

※ 'kimsuky(김수키)' 악성코드 : 2013년 세계적인 러시아 보안회사인 카스퍼스키가 북한에서 만들어졌다고 추정한 악성코드로서, 이후 다수 유사 악성코드가 발견됨

○ 'kimsuky' 악성코드와 동작방식의 유사성

- '14. 12. 한수원 이메일 공격에 사용된 악성코드는 'kimsuky' 악성코드처럼 '쉘(shell) 코드'(악성코드를 초기에 작동시키는 일종의 명령어 코드 조각)가 PC 내의 '윈도우 메모장' 프로그램에 실행코드가 삽입되어 있는 동작방식이 동일함
- 쉘 코드의 함수 및 명령어 구조도 일치하며(쉘 코드 내부에서 사용된 파일명만 상이한 정도임), 원격접속을 위한 악성코드도 99.9% 유사함

○ 'kimsuky' 악성코드에 사용된 프로그램의 버그(오류)의 동일성 및 시간적 근접성

- '14. 7. 한수원 협력업체 ㈜AOO 대표 조OO의 이메일 공격에 사용된 악성코드의 '흔글 프로그램' 버그가 'kimsuky' 계열 악성코드에 사용된 '흔글 프로그램' 버그와 동일함
- 이는 일명 '제로데이 버그'라는 최신 버그를 이용한 것으로 'kimsuky' 계열 악성코드에서는 '14. 5.경부터 사용되어 왔으나, '14. 11.경 '한글과컴퓨터' 업체에서 보완조치 하였음
- 결국, 위 버그가 활용된 6개월이라는 단기간 내에 'kimsuky' 계열 악성코드를 사용하는 조직 이외에 다른 조직에서 이 버그를 사용하여 공격할 가능성은 매우 낮다고 할 것임

● **북한 해커조직이 사용하는 것으로 알려진 중국 선양 IP 대역이 사용되었음**

- 본건 범행에 사용된 중국 선양 IP 대역은 평소 북한 해킹조직이 사용하는 것으로 보안업계에 알려진 'kimsuky' 계열 악성코드들의 IP 주소들과 12자리 숫자 중 9자리가 일치 (175.167.***.***)

※ 위 중국 선양 IP 대역은 북한 압록강 주변에서도 접속할 가능성도 있으며, 인접 지역에서 무선 인터넷 중계기를 사용하여 접속할 가능성도 있음

● **본건 범행에 사용된 국내 VPN 업체에 북한 사용 IP의 접속사실 확인**

- '14. 12. 협박글 게시에 사용된 국내 VPN 업체에 접속한 IP 내역 확인결과, '14. 12. 하순경 북한 IP 주소 25개와 북한 체신성 산하 통신회사인 KPTC (Korean Posts & Telecommunications Corporation, 중국 북경 소재)에 할당된 IP 주소 5개에서 접속한 사실 확인

※ 북한 사용 IP에서 본건 관련 국내 VPN 업체에 접속했다는 정황이 확인된 것임

2. 범행목적은 금전보다는 '사회적 혼란과 갈등 야기'라고 판단됨

● **국민안전과 직결되는 국가인프라 시설인 원전을 대상으로 하여 사회불안 야기**

- '크리스마스에 원전을 폭파하겠다'는 등 국가인프라 시설인 원전을 대상으로 전국민의 안전을 위협하며 사회불안을 야기

● **한수원 이메일 공격이 실패하자 피싱으로 수집한 정보로 불안심리 자극**

- 한수원을 상대로 소위 '약 6,000발의 이메일 폭탄' 공격을 과감하게 실행하였으나 사실상 실패로 돌아가자, 이를 숨긴 채 그동안 피싱으로 수집한 정보를 공개하며 '지속적이고 공개적으로' 국민들을 위협하여 불안심리를 자극

● **실제 돈을 받아내기 위함이 아닌 다른 목적을 희석하기 위한 불분명한 금전요구**

- 실체가 없는 원전반대그룹을 자처하며 금전요구를 하였으나, 6차에 걸친 협박글 게시 중 금전요구는 2회에 불과하며, 요구액을 정확히 밝히지 않은 것은 물론이고 전달장소와 시간을 산업통상자원부가 알아서 정하도록 하는 등 불분명한 금전요구

● **국민안전이나 금전적 목적과 무관한 국가정책 현안으로 협박**

- 대통령과 유엔사무총장간의 통화내용이라고 주장하는 파일을 공개하거나, 스마트 원전 수출에 지장을 초래하겠다는 등 금전적 목적과 무관한 국가정책을 언급하며 사회적 혼란야기

본건 범행은 접속 IP 및 악성코드 분석결과와 범행목적 등에 비추어 대한민국의 사회적 혼란과 갈등을 야기하는 북한 해커조직의 소행으로 판단됨

Ⅳ 향후 대응방안

1. 합수단의 해킹집단에 대한 지속적 추적

● 사이버 수사기법을 총동원하여 IP 및 악성코드 추적

- 광범위한 해킹과 약 6,000개의 이메일 공격에 사용된 IP 및 악성코드에 대하여 각종 IP 추적기법, 이메일 계정의 발급·도용·접속 경위, 악성코드 제작·유통 경로 파악 등 사이버수사기법 총동원

● 긴밀한 국제공조 및 유관기관 협업으로 해킹루트 발본색원

- 미국, 중국, 태국 등과의 긴밀한 국제공조를 통해 국제적으로 암약하고 있는 해킹집단과 그 배후세력의 실체 파악 주력

- 국정원, 경찰청 사이버안전국, 방송통신위원회, 한국인터넷진흥원(KISA) 등 유관기관과 협업하여 공개된 자료 등의 유출경로 특정작업을 지속하고, 본건 포함 국내 해킹루트를 철저히 발본색원하여 추가적인 유출예방 철저

※ 국정원 : 해외 악성코드 분석, 각종 해커 정보 수집

경찰청 : 국내 악성코드 분석, 계정 도용 등 해킹 피해 수사

방통위 : SNS 등에 공개된 자료에 대한 블라인드 처리 등 유포 방지

KISA : 민간 악성코드 분석, 백신 배포

2. 해킹에 대비한 범국민적 사이버 보안노력 필요

● 이메일 ID 및 비밀번호 관리 철저

- ① 사설 이메일(NAVER, Daum, Hotmail, NATE, G-mail 등)의 업무상 사용 자제, ② 사설 이메일 웹사이트의 최근 접속내역 확인(제3자의 임의접속 확인 가능), ③ 이메일 ID가 외부에 노출되지 않도록 하고, 비밀번호는 수시로 변경, ④ 주요업무 처리자는 기관 이메일 및 사설 이메일 ID 변경

● 공공기관에서의 불필요한 인터넷이용 차단

- 인터넷상 검색과 다운로드 과정에서 각종 악성코드 유포·공격은 빈번하게 이루어지고 있는바, 백신 프로그램만으로 예방하기에는 역부족

- 내부망·외부망 분리에 관계없이, 외부 인터넷 사용을 가능하면 자제하고(업무상 필요한 경우만 허용), 주요업무 수행시 ① 컴퓨터 초기화, ② 바이러스 정밀검색, ③ 망분리 또는 인터넷 차단 등 보안조치 강구

● **국가 주요기관의 협력업체 정보보안 관리·감독 강화**

- 공공기관과 그 협력업체에 대한 ① 보안가이드(매뉴얼) 보급, ② 정보보안 관리실태의 정기적 점검, ③ 장비 반출입시 보안조치 강화 및 ④ 주요 자료에 대한 표준 DRM 시스템[1] 개발 및 협력업체 적용 검토할 필요

- 각종 '미끼성' 이메일, 스미싱 문자로 인해 악성코드에 감염될 우려가 높으므로, 반복된 모의훈련을 통해 구성원들의 보안의식을 강화시킬 필요

● **사이버보안 전문인력의 육성 및 보안시스템 투자 제고**

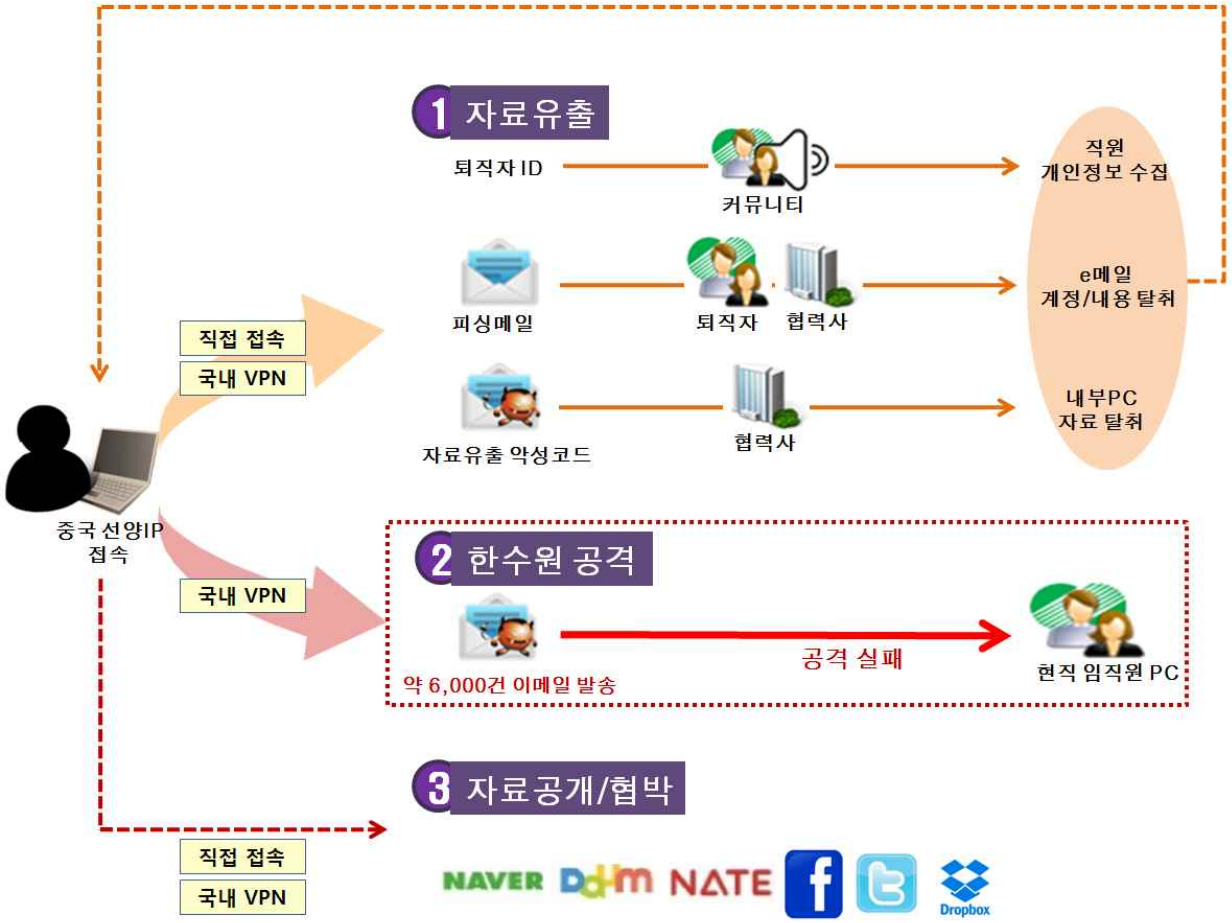
- 주요기관의 사이버보안 전문인력을 충원하고 대응역량을 강화하여, 사이버 공격에 신속하고 효율적으로 대응할 필요

- 국가 주요기관은 물론 주요 개인정보를 다루는 민간 기업에서도 정보보안에 대한 투자를 제고시킬 수 있는 방안을 마련할 필요 ▨

※ 별첨 : 사건개요 설명도

1) Digital Rights Management : 디지털 자료의 불법 복제·변조을 막거나 불법 사용을 추적할 수 있도록 암호화하거나 저작권 표시를 삽입하는 등의 정보보안 서비스를 말함

사건개요 설명도


1 자료유출
퇴직자 ID
커뮤니티
직원
개인정보 수집
피싱메일
퇴직자
협력사
e메일
계정/내용 탈취
자료유출 악성코드
협력사
내부PC
자료 탈취
직접 접속
국내 VPN
중국 선양IP
접속
국내 VPN
2 한수원 공격
공격 실패
현직 임직원 PC
약 6,000건 이메일 발송
3 자료공격/협박
직접 접속
국내 VPN
NAVER
Daum
NATE
Dropbox