이 보도자료는 2016. 5. 31. 15:00 이후에 보도하여 주시고, 이 보도자료를 통해 공개되는 범죄 사실 중에는 아직 확정되지 않은 사실도 있음에 유의하여 주시기 바랍니다.

보 도 자 료 2016. 5. 31.(화)

주책임자 : 합수단장 손영배
자료문의 : 개인정보범죄 정부합동수사단
전화번호 : 02-530-4285

제 목

금융정보보안업체 전자인증서 해킹사건 수사결과

- 북한 해킹조직 소행 추정, 신속조치로 피해확산방지 -

□ 개인정보합수단은 금융정보보안업체 A社의 코드서명 전자인증서 해킹사건을 수사한 결과, 북한 해킹조직이 A社 내부전산망을 해킹하여 탈취한 전자인증서를 이용하여 위조된 코드서명이 탑재된 악성프로그램을 10여개 기관 PC에 유포한 사실을 확인하였음

※ 코드서명(code signing) : 인터넷에서 배포되는 실행파일이 정당한 제작자에 의해 제작되었고 위·변조되지 않았음을 확인하는 수단으로, 파일 설치 이전에 파일에 탑재된 코드서명과 전자인증서로 유효성을 검증하여 허용되지 않은 코드서명이 탑재된 경우에는 해당 파일의 설치를 차단하거나 PC 사용자에게 경고함으로써 악성프로그램의 유포 등을 차단하는 기능을 함

□ 북한 해킹조직은 '정보보안업체의 코드서명이 탑재된 프로그램은 안전하다'는 공신력을 악용하여 정보탈취 등 해킹에 필요한 악성프로그램을 유포하기 위하여 전자인증서를 탈취하고, 이를 이용하여 주요 전산망마비 등 사회혼란을 의도한 것으로 보임

□ 개인정보합수단은 유관기관과 협의하여 악성프로그램을 이용한 해킹 시도 이전에 탈취된 전자인증서를 무효화하고, 악성프로그램에 감염된 PC를 전수 조사하여 삭제하는 한편, 백신업체에 관련 정보를 제공하여 백신프로그램을 업데이트하도록 조치함

Ⅰ 전자인증서 유출 및 악성프로그램 유포 경위

- ‘15. 11.경 금융 보안전문업체인 A社의 전산서버가 해킹되어 내부자료 탈취가 가능하도록 악성프로그램이 설치됨
- ‘15. 12. ~ ’16. 1.경 해당 서버에 접속한 직원 PC에 악성프로그램이 전파되어, 해당 PC에 저장되어 있던 A社 전자인증서가 유출됨
- ‘16. 2.경 A社 전자인증서를 이용한 코드서명이 탑재되어 A社의 정상 프로그램으로 가장한 악성프로그램이 B 학술단체 홈페이지 운영서버에 설치됨
- ‘16. 2. 11.경 B 학술단체 홈페이지 운영서버에 접속한 10개 기관 PC 총 19대에 동일 악성프로그램이 유포됨

※ 유포된 악성프로그램은 저장 정보를 탈취하거나 다른 악성프로그램의 추가 설치를 가능하게 하는 등의 기능을 수행

Ⅱ 해킹사실 인지 및 악성프로그램 차단

- ‘16. 2. 15.경 백신업체에서 A社 코드서명이 탑재된 악성프로그램을 발견하여 한국인터넷진흥원 및 A社에 통보함
  - A社 전자인증서가 해킹·탈취되어 코드서명이 위조된 사실 확인
- ‘16. 2. 18.경 A社에서 관련 PC·서버 등을 개인정보합수단에 임의제출하여 수사에 착수함
- 악성프로그램 확산 방지
  - 국정원, 한국인터넷진흥원, 금융보안원 등 유관기관과 협의하여 위조된 코드서명 폐기·무효화, 감염된 PC 네트워크 연결차단 및 악성프로그램 삭제 등 조치 병행
  - 주요 백신업체 등에게 본건 악성프로그램 정보를 제공하여 백신프로그램 업데이트 등 시행
  - 신속한 조치로 공공기관 내부정보 유출 등 추가 피해는 발생하지 않은 것으로 확인됨

Ⅲ 수사 결과

● 서버 등 분석

- A社 서버 및 PC 70여대, 악성프로그램 유포 경로가 된 서버, 악성프로그램이 설치된 PC를 제어하고 명령을 내리는 서버(C&C 서버), 이메일 등 총 12테라 용량(1테라는 종이 1억 페이지 분량)의 자료 정밀분석

● 악성프로그램 유포 경로 확인

- 외부에서도 접속이 가능한 A社의 프로그램 테스트용 서버(데모서버)를 통해 직원 PC를 해킹하고 전자인증서를 탈취한 사실 확인

- 학술단체 홈페이지 운영 서버를 통해 10개 기관 19개 PC에 악성프로그램이 유포된 사실 확인

● 해킹 조직 추적

- A社 서버가 악성프로그램에 최초 감염된 '15. 11. 30.경부터 '16. 1. 28.경까지 사이에 북한 소재 IP가 총 26회 해당 서버에 접속

- '16. 1. 28.경 본건 악성프로그램의 명령·제어서버에 북한 소재 IP가 총 6회 접속

- 해킹된 A社 직원 PC에서 유출되는 정보가 전달되도록 미리 지정된 이메일 계정에서 북한 선전·선동매체 '우리민족끼리' 사이트 가입자에게 이메일 발송

- A社 직원 사내 이메일로 악성프로그램을 탑재한 '남북통일에 대함'이라는 제목의 이메일이 발송되었고, 해당 악성프로그램 명령·제어서버 도메인이 'dprk.hdskip.com'로 북한(DPRK)과 관련

➡ 국내 주요기관에서 정보보안 등을 목적으로 사용중인 A社 전자인증서를 탈취하고, 이를 악용하여 악성프로그램을 정상 프로그램으로 가장·유포함으로써 국내 주요 전산망에 대한 침입·마비 등으로 사회 혼란 야기를 시도한 북한 해킹조직의 사이버테러로 추정됨

※ 사건개요 설명도 별첨

IV 참고사항 - 대검찰청 · 금융보안원 MOU 체결

- ‘16. 5. 31.(화) 대검찰청은 ‘사이버범죄 수사 및 금융권 침해사고 대응 역량 강화’를 위해 금융보안원과 업무협약(MOU)을 체결함

※ 금융보안원은 ‘15. 4. 금융분야 보안전담기구로 출범, 전자금융거래의 안전성 및 신뢰성 보장을 위해 금융권 통합보안관제 등의 업무 수행

- MOU 체결을 계기로 금융전산망 해킹·대규모 개인정보 유출 등 금융기관을 대상으로 하는 사이버 범죄에 신속하고 효과적인 대처 기대

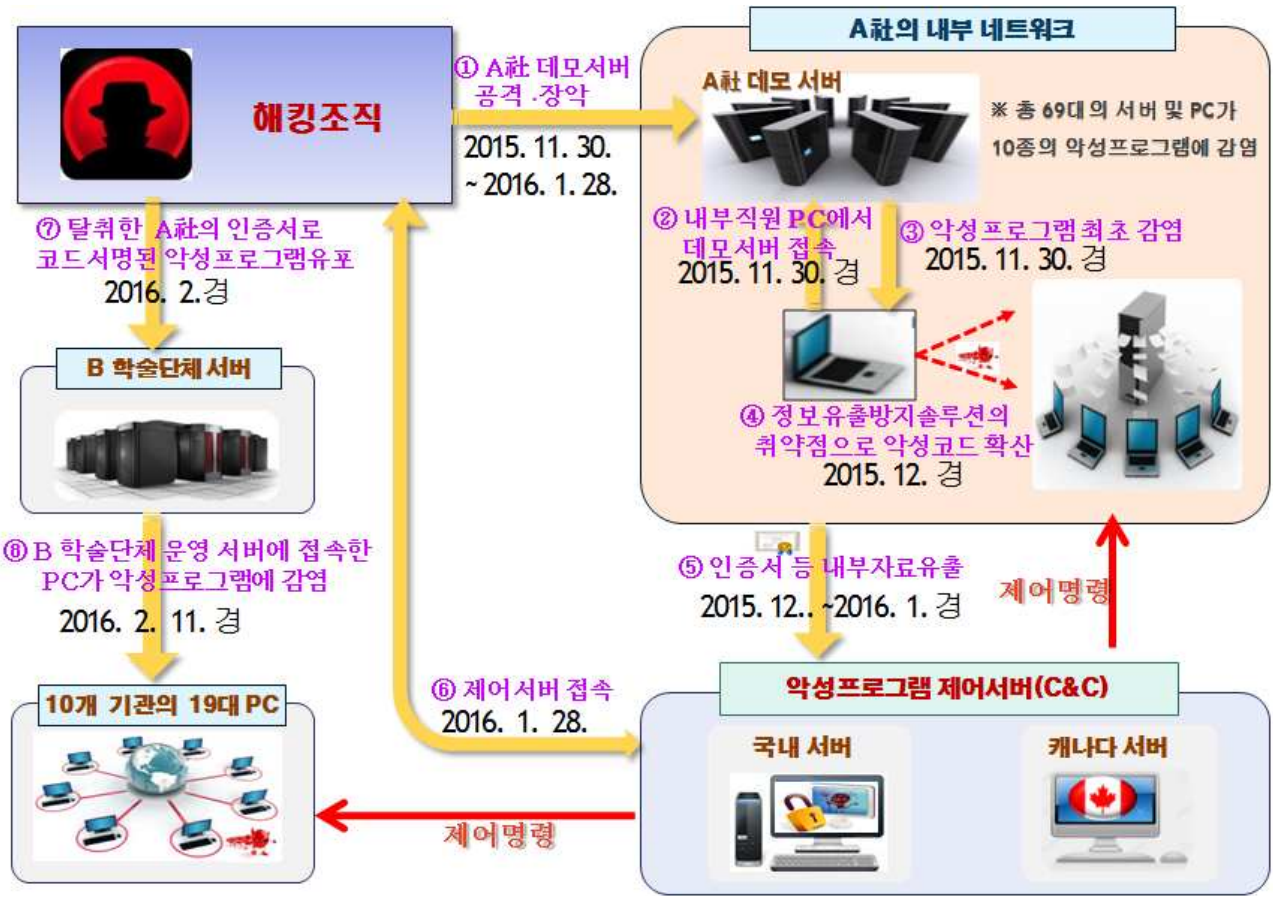
※ 이번 북한 해킹조직에 의한 금융정보보안전문업체 전자인증서 해킹사건의 경우에도, 중앙지검 첨단1부, 대검찰청 사이버수사과와 금융보안원은 사건 발생 직후부터 악성프로그램 분석 결과 공유

- 주요 내용은 ▲ 분기별 정기 업무 협의회 개최 ▲ 금융 침해사고 정보 공유 및 증거분석 협력 ▲ 금융권 사이버범죄 공동 대응 ▲ 디지털 포렌식 기술 역량 강화 등이며, 금융보안과 사이버수사 역량 강화를 위해 교류와 협력을 확대할 예정

- 김수남 검찰총장은 “금융보안원과의 협업을 통해, 전 세계 화폐의 약 90%가 인터넷으로 보관·거래되는 금융 사이버공간을 범죄없는 안전한 곳으로 만들기 위해 검찰의 IT 수사 역량을 결집하여 최선을 다하겠다”

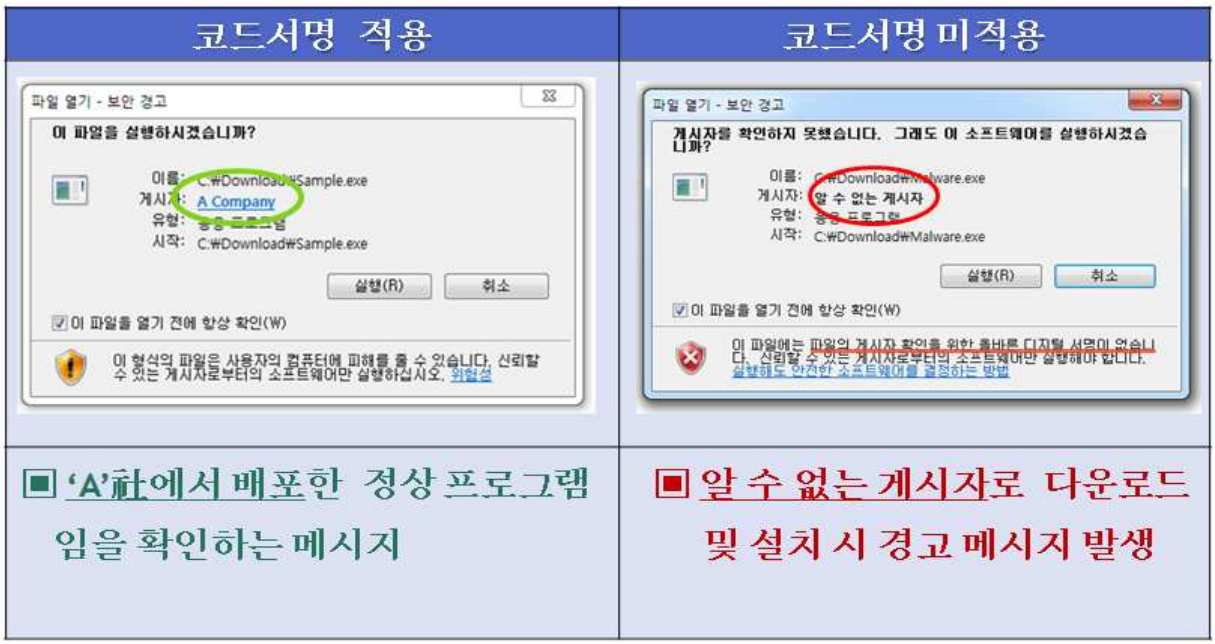
- 금융보안원 허창언 원장은 “이번 업무협약 체결을 통해 금융권 침해사고 발생시 대검찰청과의 신속한 업무 공조가 가능하게 되어 금융권 전반의 침해사고 대응 수준이 한 단계 강화될 것으로 보인다.”라고 밝힘

사건개요 설명도


해킹조직
① A社 데모서버 공격 .장악
2015. 11. 30. ~ 2016. 1. 28.
A社의 내부 네트워크
A社 데모 서버
※ 총 69대의 서버 및 PC가 10종의 악성프로그램에 감염
② 내부직원 PC에서 데모서버 접속 2015. 11. 30.경
③ 악성프로그램 최초 감염 2015. 11. 30.경
④ 정보유출방지솔루션의 취약점으로 악성코드 확산 2015. 12. 경
⑤ 인증서 등 내부자료유출 2015. 12.. ~2016. 1. 경
제어명령
⑦ 탈취한 A社의 인증서로 코드서명된 악성프로그램유포 2016. 2.경
B 학술단체 서버
⑧ B 학술단체 운영 서버에 접속한 PC가 악성프로그램에 감염 2016. 2. 11. 경
10개 기관의 19대 PC
⑥ 제어서버 접속 2016. 1. 28.
악성프로그램 제어서버(C&C)
국내 서버
캐나다 서버
제어명령

코드서명(Code Signing) 설명도

□ 코드서명은 인터넷에서 배포되는 파일이 정당한 제작자에 의해 제작되었고 위·변조되지 않았음을 확인하는 수단



※ 아래와 같이 탈취한 전자인증서로 악성프로그램을 코드서명하여 유포할 경우, 이용자는 이를 정상프로그램으로 오인하고 의심 없이 다운로드하여 악성 프로그램에 감염되는 피해 발생 우려