이 보도자료는 2016. 8. 1.(월) 06:00(석간용)부터 보도하여 주시기 바랍니다.

검찰
PROSECUTION SERVICE

대 검 찰 청

대변인실
전화 02-3480-2100 / **팩스** 02-3480-2704

보 도 자 료
2016. 8. 1.(월)

자료문의 : 사이버수사과
전화번호 : 02-535-9483
주책임자 : 사이버수사과장 양석조

제 목

27개 피싱 사이트 이메일 계정 해킹 사건 중간조사 결과
- 북한 해킹조직 소행 추정, 지속적 사이버보안 노력 필요-

▣ 대검찰청 사이버수사과는 스피어 피싱 공격을 통한 이메일 계정 탈취 사건을 조사한 결과,

- 북한 해킹조직으로 추정되는 자가 '16. 1. 12.부터 '16. 6. 16.까지 구글, 네이버, 다음, MS, qq, 정부부처, 방산업체, 주요 대학교 등을 사칭하는 총 27개의 피싱 사이트를 개설한 다음

- 외교부·통일부·국방부 등 공무원 및 출입기자, 북한 관련 연구소 교수·연구원, 방산업체 임직원 등 북한 관련 기관 종사자 이메일 계정 90개를 탈취 시도하여, 이 중 56개 계정의 패스워드가 유출된 사실을 확인함

▣ 본건 범행에 사용된 피싱 사이트 개설 도메인 호스팅 업체, 보안 공지를 위장한 피싱 이메일의 내용, 피싱 사이트 웹 소스코드, 탈취 계정 저장 파일 형식, 범행에 사용된 중국 선양 IP(175.167.x.x) 등이 과거 한수원 사건과 동일한 바, 북한 해킹 조직에 의한 소행으로 추정됨

▣ 검찰은 국정원, 한국인터넷진흥원 등 유관기관과 협조하여 해당 피싱 사이트를 폐쇄하고, 피해 계정들에 대해서는 계정보호 등 조치를 취하였는바, 해킹에 대비한 지속적인 사이버 보안 노력이 필요함

Ⅰ 착수 경위 및 조사 경과

○ 대검찰청 사이버수사과로 피싱 이메일 의심 신고 접수

○ 해당 피싱 이메일에 대한 추적 과정에서 국내 무료호스팅업체에 개설된 메인·서브 계정 60개의 11억 9,000라인에 해당하는 대용량 로그 및 웹 소스 분석을 통해 피해자 및 중국 선양에서 접속한 범인의 IP(68개)를 특정

Ⅱ 범행 대상 및 방법

1. 범행 대상

○ 외교부, 통일부, 국방부(현역군인), 북한 관련 연구소, 방산업체 등 북한 관련 기관에서 근무하는 약 90명을 대상으로 이메일 계정 탈취 시도

○ '16. 1. 12.경부터 '16. 6. 16.까지 총 90개의 이메일 계정 탈취 시도가 있었으며, 이 중 56개의 패스워드가 유출됨

※ 피싱 서버 상의 삭제 기록에 비추어볼 때 보다 많은 피해자가 있을 것으로 추정

2. 범행 방법

○ '16. 1. 12.경 국내 무료 도메인 호스팅 업체 서버를 이용하여 총 27개의 피싱 사이트 개설(예:googlesecurity.△△△.co.kr)

- 외교부, 방산업체, 구글, 네이버, 다음, MS, qq, 대학교 등 사칭

○ 피해 대상자에게 '피싱(phishing)' 메일을 보내 이메일 비밀번호 수집

- 위 사이트 보안담당자를 사칭하여 "비밀번호가 유출되었으니 확인바란다"는 이메일을 전송하고 이메일 본문의 링크를 클릭하면 비밀번호 변경창이 뜨도록 하여 비밀번호를 입력하도록 유도

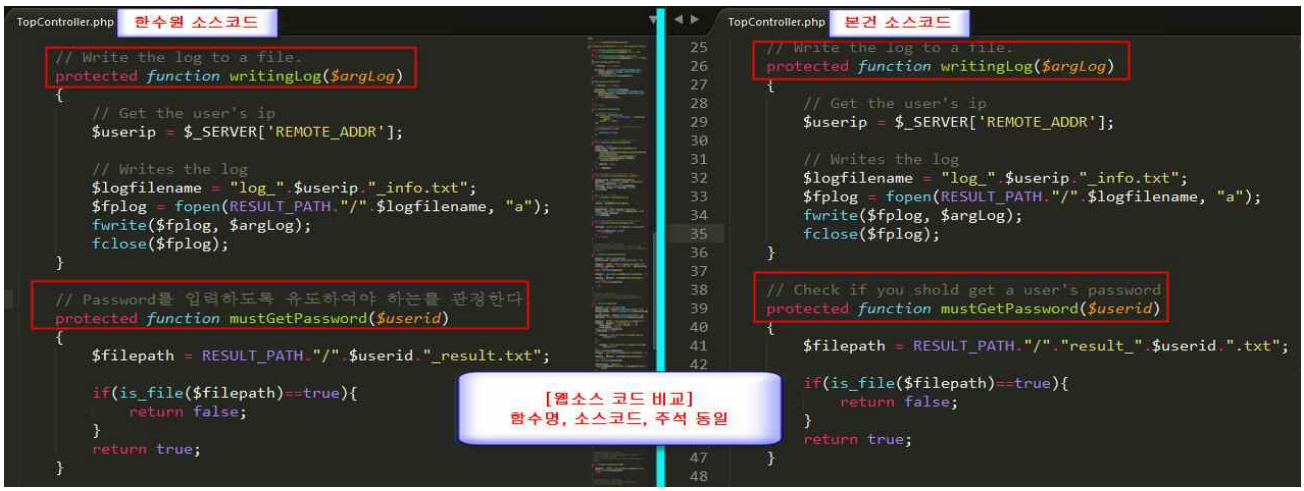
※ 붙임. 이메일 해킹(피싱) 방법 개요도, 구체적인 범행 방법, 시연동영상 참고

Ⅲ 범인 추적결과 : 북한 해킹 조직으로 추정

1. 한수원 사건과 동일한 웹호스팅, 웹소스코드 사용

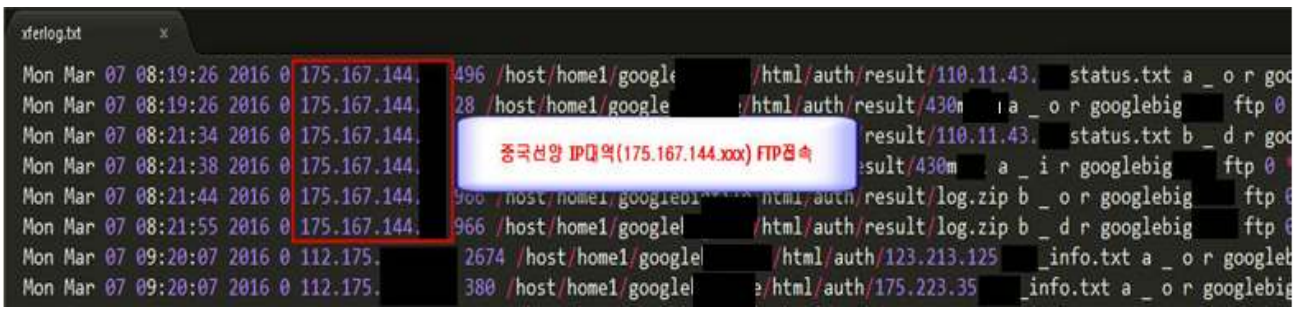
○ 피싱 서버가 운영된 웹호스팅 업체가 A사로 동일하고, 웹소스코드 또한 한수원 사건 당시 피싱 웹소스코드와 동일함

- 접속자 계정정보를 '접속 IP 파일명'의 파일 형태(예:'192.168.150.133_result.txt')로 피싱 서버에 저장 후, 사후에 FTP로 접속해 수집해 가는 패턴 또한 동일



2. 한수원 사건과 동일한 선양 IP 대역 사용

○ 한수원 사건 당시 "Kimsuky"계열 악성코드에 사용되었던 선양 IP 175.167.***.*** 대역이 본건 피싱 서버에 FTP 접속해 탈취된 계정 정보에도 사용



Ⅳ 조치 및 향후 대응방안

1. 피해 방지를 위한 조치

○ 국정원, 한국인터넷진흥원(KISA) 등 유관기관과 연계하여 해당 피싱 사이트 폐쇄, 피해자 계정에 대한 비밀번호 변경 등 계정 보호조치 실시

○ 탈취 계정에 의한 추가 해킹 및 자료 유출 방지를 위한 예방 모니터링 강화

2. 해킹에 대비한 지속적인 사이버 보안노력 필요

○ 이메일 ID 및 비밀번호 관리 철저

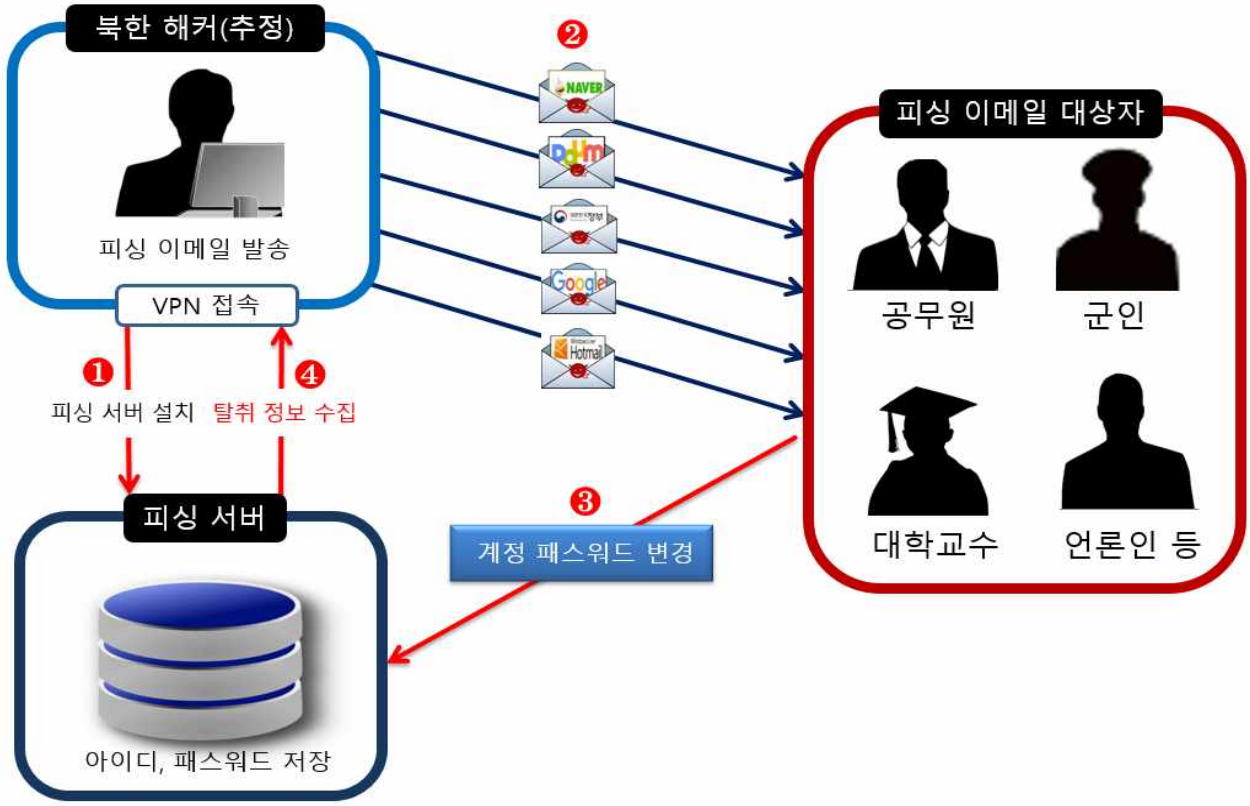
- ① 사설 이메일(NAVER, Daum, Hotmail, NATE, G-mail 등) 업무상 사용 자제, ② 사설 이메일 웹사이트의 최근 접속내역 확인(제3자의 임의접속 확인 가능), ③ 이메일 ID가 외부에 노출되지 않도록 하고, 비밀번호는 수시로 변경, ④ 주요업무 처리자는 기관 이메일 및 사설 이메일 ID 변경

○ 공공기관에서의 불필요한 인터넷 이용 차단

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

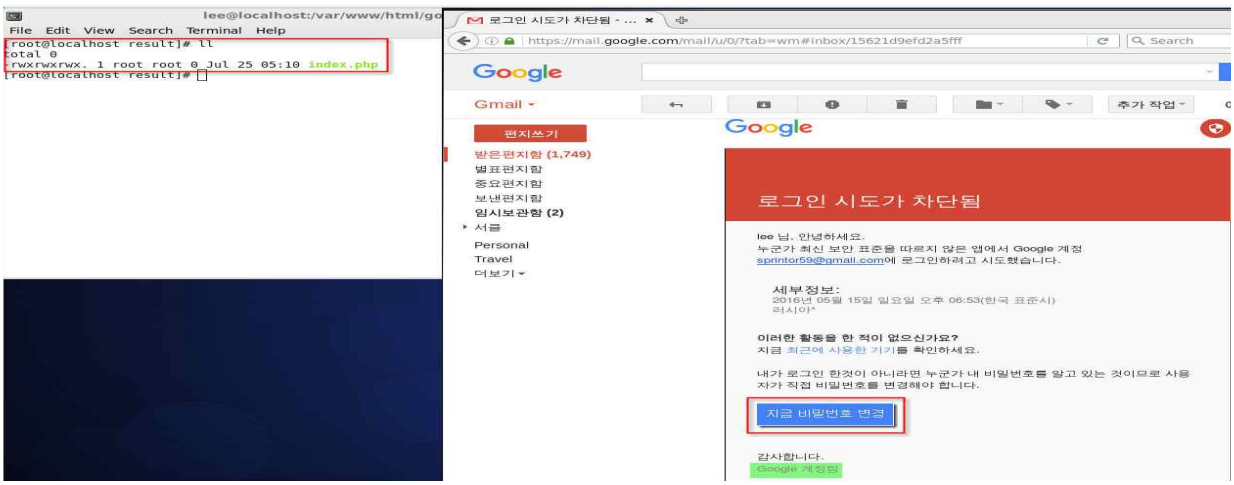
- 내부망·외부망 분리에 관계없이, 외부 인터넷 사용을 가능하면 자제하고 (업무상 필요한 경우만 허용), 주요업무 수행시 ① 컴퓨터 초기화, ② 바이러스 정밀검색, ③ 망분리 또는 인터넷 차단 등 보안조치 강구 ▧

○ 이메일 해킹(피싱) 방법 개요도



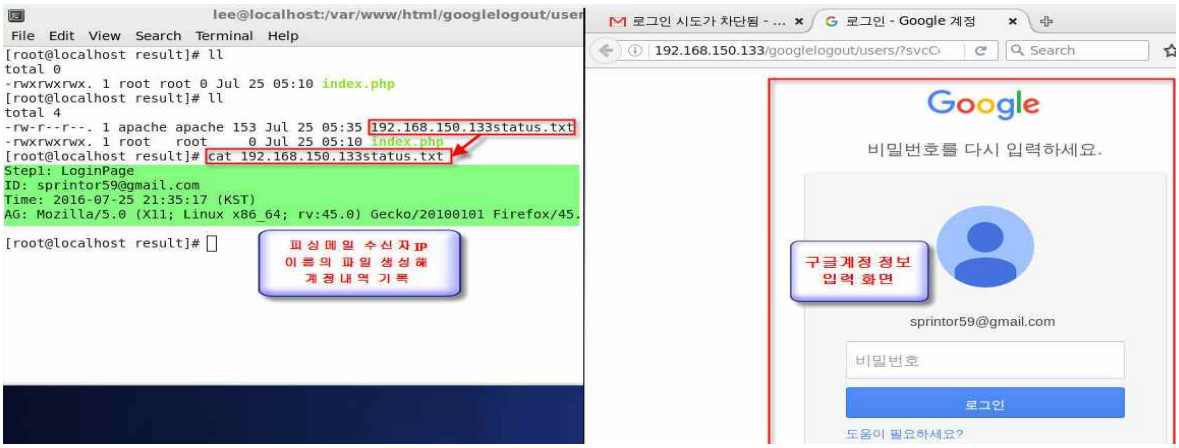
○ 구체적인 방법

❶ 해당 사이트 보안담당자를 사칭한 피싱 이메일 발송



※ 왼쪽은 피싱 서버 화면, 오른쪽은 피싱 이메일 화면인바, '지금 비밀번호 변경'을 클릭하는 순간 피싱 서버와 연결되어 기록되기 시작함

❷ 피해자가 '지금 비밀번호 변경'을 클릭하면 피싱 서버에 피해자의 접속 IP(192.168.150.133)를 파일명으로 하는 텍스트(txt) 파일 생성



❸ 피해자가 비밀번호 입력하면 피싱 서버에 생성된 텍스트 파일에 계정, 패스워드가 저장됨