★ 배포시점부터 보도하여 주시기 바랍니다.

보도자료

미래창조과학부
Ministry of Science, ICT and Future planning

미래창조과학부 대변인실 ☏ 02-2110-2064

<자료문의> ☎ 02-2110-2924, 정보보호정책과 과장 이승원, 사무관 김주봉

民官軍 합동대응팀, '3.20 사이버테러' 중간 조사결과 발표
- 북한의 과거 해킹수법과 일치하는 증거 발견 -

□ 民官軍 합동대응팀은

o 지난 △3.20 방송·금융社(6개) 전산장비 파괴, △3.25 '날씨닷컴' 사이트를 통한 全 국민대상 악성코드 유포, △3.26 대북·보수단체 홈페이지(14개) 자료삭제, △YTN 계열사 홈페이지 자료서버 파괴 등 연쇄적 사이버테러가 7.7 DDoS(2009년)·3.4 DDoS(2011년)와 농협(2011년)·중앙일보(2012년) 전산망 파괴 등 수차례 對南 해킹을 시도한 북한의 해킹수법과 일치한다고 밝혔다.

□ '3.20 사이버테러' 중간 조사결과

※ 금번 民官軍 합동대응팀은 미래부·국방부·금융위·국정원, 한국인터넷진흥원(KISA), 국내보안업체(안랩·하우리·이글루시큐리티·윈스테크넷·KT 등)로 구성

o 피해社 감염장비 및 국내 공격경유지 등에서 수집한 악성코드 76종(파괴용 9, 사전 침투·감시용 67)과 수년간 국정원과 軍에 축적된 북한의 對南해킹 조사결과를 종합 분석한 결과는 다음과 같다.

o 공격자는 최소한 8개월 이전부터 목표 기관 내부의 PC 또는 서버 컴퓨터를 장악하여 자료 절취, 전산망 취약점 파악 등 지속적으로 감시하다가 백신 등 프로그램의 중앙배포 서버를 통해 PC 파괴용 악성코드를 내부 전체 PC에 일괄 유포하거나 서버 저장자료 삭제 명령을 실행한 것으로 확인하였다.

o 또한, 공격에 사용된 컴퓨터 인터넷주소 및 해킹수법 등을 분석한 결과, 과거 7.7 DDoS 등과 같이 북한 소행으로 추정되는 증거를 상당량 확보하였다.

□ 북한의 해킹으로 추정되는 증거로

❶ 북한 내부에서 국내 공격경유지에 수시 접속, 장기간 공격 준비

▸ 2012년 6월 28일부터 북한 내부 PC 최소한 6대가 1,590회 접속하여 금융社에 악성코드를 유포하고 PC 저장자료를 절취하였으며 공격 다음날(3.21) 해당 공격경유지를 파괴, 흔적 제거까지 시도

▸ 금년 2월 22일 북한 내부 인터넷주소(175.45.178.xx)에서 감염PC 원격조작 등 명령 하달을 위한 국내 경유지에 시험 목적으로 처음 접속하였다.

❷ 공격경유지 49개중 22개가 과거 사용했던 경유지와 동일

▸ 지금까지 파악된 국내외 공격경유지 49개(국내 25, 해외 24) 중 22개(국내 18, 해외 4)가 2009년 이후 북한이 對南 해킹에 사용 확인된 인터넷주소와 일치하였다.

❸ 악성코드 76종 중 30종 이상을 再활용

▸ 북한 해커만 고유하게 사용중인 감염PC의 식별 번호(8자리 숫자) 및 감염신호 생성코드의 소스프로그램 중 과거와 동일하게 사용한 악성코드가 무려 18종에 달하였다.

□ 또한, 일련의 사이버테러 4건이 동일조직 소행이라는 근거로

o 3월 20일 방송·금융社 공격의 경우, 대부분 파괴가 같은 시간대에 PC 하드디스크를 'HASTATI' 또는 'PRINCPES' 등 특정 문자열로 덮어쓰기 방식으로 수행되었고, 악성코드 개발 작업이 수행된 컴퓨터의 프로그램 저장경로가 일치하였다.

o 3월 25일 및 26일 발생한 3건도 악성코드 소스프로그램이 방송·금융社 공격용과 완전히 일치하거나 공격경유지도 再사용된 사실을 확인하였다.

□ 향후

o 정부는 4월 11일 국정원장 주재로 미래부·금융위·국가안보실 등 15개 정부기관 참석하에 개최하는 '국가사이버안전전략회의' 등을 통해 사이버 안전 강화 대책을 강구·시행하기로 하였다. 끝.