미래창조과학부 방송통신위원회	보 도 자 료	대한민국 재도약의 힘, 창조경제

보도일시	2016. 8. 31.(수) 배포시점부터 보도해 주시기 바랍니다.		
배포일시	8. 31.(수) 09:00	담당부서	미래부 사이버침해대응과 방통위 개인정보보호조사팀
담당과장	최병택 과장(02-2110-2890) 김기석 팀장(02-2110-1567)	담 당 자	신홍순 사무관(02-2110-2924) 황선철 사무관(02-2110-1525)
문의 한국인터넷진흥원 분석1팀 임진수(02-405-5231)			

인터파크 개인정보 유출 침해사고 조사 결과

- APT(지능형 지속 위협) 공격으로 개인정보 유출 발생 -

□ 미래창조과학부(이하 '미래부')와 방송통신위원회(이하 '방통위')는 지난 5.3(화)에서 5.6(금)까지 발생한 인터파크 침해사고 관련 '**민·관합동조사단**(이하 조사단)*'의 **조사 결과를 발표**하였다.

* 미래부·방통위 공무원, 한국인터넷진흥원 및 민간 전문가로 구성·운영(7.25~)

o **이번 조사**는 지난 7.28(목) 북 정찰총국 소행으로 판단되는 인터파크 고객정보 해킹 및 협박사건에 대한 경찰청의 중간 수사 결과 발표와 병행하여 **사고 대응, 피해 확산 방지** 등을 위한 **침해사고 원인 분석을 위해 실시**되었다.

□ 조사단은 경찰로부터 넘겨받은 사고 관련자료(37종, 5테라바이트) 분석과 현장조사를 통해 해킹의 구체적인 방법 및 절차 등을 확인하였다.

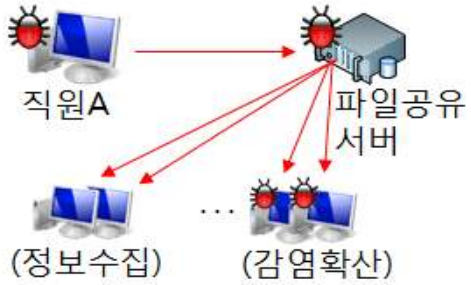
1 해커는 **스피어피싱**으로 직원PC에 **악성코드를 최초 감염**시키고

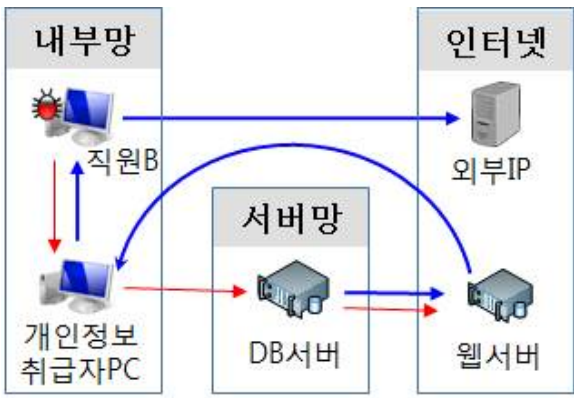
2 다수 단말에 **악성코드 확산**과 함께 **내부정보를 수집**하고

3 DB서버에 접근 가능한 **개인정보취급자PC의 제어권을 획득**한 후

4 **DB서버에 접속**하여 **개인정보를 탈취**하고 외부로 몰래 유출한 것으로 조사되었다.

< 해킹방법 개요 >

1 메일을 통한 내부망 최초 감염	2 내부망 감염확산 및 정보수집
	
① **해커**가 지인을 사칭해 **악성코드가 첨부된 e메일**을 **발송**(5.3, 16:38) ② **직원A**가 해당 메일을 열람하고 **악성코드에 감염**(5.3, 17:15)	③ 직원A PC를 경유, **파일공유서버 접속 및 악성코드 설치**(5.3, 17:41) ④ 파일공유서버를 통해 **패스워드 대입공격** 수행(감염확산 및 정보수집)

3 개인정보취급자PC·DB서버 점거	4 개인정보 탈취 및 유출
	
⑤ 파일공유서버를 경유, **개인정보 취급자PC로 접속**(5.4, 23:04) ⑥ 기존 연결 상태를 이용하여 **DB서버로 접속**(5.5, 02:10)	⑦ 직원B를 경유, **개인정보취급자PC 및 DB서버에 재접속**(5.5, 11:39) ⑧ DB서버의 **개인정보를 탈취**, 웹서버→취급자PC→직원B PC를 거쳐 **외부 유출**(5.5 12:08~5.6 02:05)

o 또한, 해커는 패스워드 관리 및 서버 접근통제 관리 등의 취약점을 악용하여 **인터파크 회원정보 26,658,753건**이 보관된 **파일**을 **16개로 분할**하고 **직원PC를 경유하여 외부로 유출**한 것으로 조사되었다.

<회원정보 유출 상세 내역>

회원분류		정보 항목	건수
일반회원	인터파크	아이디, 암호화된 비밀번호, 이름, 성별, 생년월일, 전화번호, 휴대전화번호, 이메일, 주소	10,947,544건
	제휴사	아이디	2,454,348건
탈퇴회원		아이디	1,734,816건
휴면회원*		아이디, 암호화된 비밀번호	11,522,045건
합계			26,658,753건

※ 중복 여부에 대해서는 방통위에서 추가 조사 중

□ **미래부는** 인터파크 대상으로 조사과정에서 발견된 문제점을 개선·보완할 수 있도록 조사결과 및 개선사항 공유 등 **보안강화 기술 지원을 실시**하였으며,

o **방통위는** 침해사고를 인지한 후 인터파크에서 개인정보 유출 침해사고를 확인하고 해당 **피해사실 및 이용자 조치방법** 등을 **이용자에게 통지토록 조치**하였다.

□ 민관합동조사단 단장(미래부 송정수 정보보호정책관)은 "**침해사고가 발생한 경우** 미래부 등 관계기관에 **즉시 신고**하여야 하며, **증가하는 북한의 사이버 도발 위협**에 대비하여 개인정보보호 및 사이버 보안 체계를 재점검하는 등 **정보보호 노력을 강화**하는 것이 매우 중요하다"고 강조하였다.

※ 방통위는 개인정보 보호조치 위반 관련 사항에 대해서는 '정보통신망이용촉진 및 정보보호 등에 관한 법률'에 따라 조치할 예정임

이 자료에 대하여 더욱 자세한 내용을 원하시면
미래창조과학부 신홍순 사무관(☎02-2110-2924) 및
방송통신위원회 황선철 사무관(☎02-2110-1525)에게 연락주시기 바랍니다.