방송통신위원회
KOREA COMMUNICATIONS COMMISSION

2010.4.22(목)

보도자료

2010년 4월22일(목) 배포 시점부터 보도하여 주시기 바랍니다.

문의 : 네트워크정책국 네트워크정보보호팀 박철순팀장 (750-2750)
네트워크정보보호팀 구교영 사무관 (750-2755) eaglefree@kcc.go.kr

스마트폰을 통한 국제전화 무단발신 유발 사례 확인 및 조치

방통위, 민·관 합동대응반 통해 긴급 조치 및 국제전화 발신제한 설정 요망
백신 설치·업데이트 등 스마트폰 '이용자 10대 안전수칙' 준수도 당부

방송통신위원회(위원장 최시중)가 운영하는 스마트폰 정보보호 민·관 합동대응반은 최근 해외(영국)에서 '무단으로 국제전화를 시도하여 이용자에게 이용요금을 부과시킬 수 있는 윈도우 모바일 기반 스마트폰 악성코드'가 발견된 것과 관련하여 국내 유포여부를 점검(4.16.~20.)하였으며, 그 결과 일부 가입자들의 스마트폰이 해당 악성코드의 피해유형과 유사한 증상을 나타내어 긴급 대응조치를 취하였다고 밝혔다.

※ 스마트폰 정보보호 민·관 합동대응반 : 스마트폰 보안위협 관련 선제적 대응협력 체제 구축 및 보안대책 마련 등을 위해 '10.1.21. 구성되었으며, 방통위 및 KISA를 비롯, ETRI, 이통사(KT, SK텔레콤, LG텔레콤), 제조사(삼성전자, LG전자, 팬택), 백신업체(안철수연구소, 하우리, 에스지어드밴텍, 이스트소프트, 잉카인터넷, NHN), 보안업체(지란지교소프트, 드림시큐리티), APP 개발사(컴투스, 드림위즈) 등의 관련 전문가들이 참여 (7회 회의개최 및 e-mail, SMS, 전화 등을 통한 상시 협력)

방통위는 KT의 최초 신고(SKT, LGT도 이후 신고) 접수 후 즉시 민·관 합동대응반의 긴급대응체제를 가동하였으며, 방통위와 KISA는 유포사이트(해외)를 통해 해당 악성코드 샘플을 즉시 채집하여 분석 결과를 백신업체에 전달함으로써 신속한 백신 개발 및 업데이트가 이루어질 수 있도록 하였다. 또한 국내 웹사이트를 대상으로 해당 악성코드가 포함된 게임 S/W가 유통되는 블로그 등에 대한 차단 조치를 요청하였으며, 이통3사(SKT, KT, LGT)로 하여금 국제전화 발신 모니터링을 강화하도록 조치하였다.

※ 관련 악성코드 개요 : '3D 안티 테러리스트 액션'이라는 모바일 게임에 은닉, 유포되는 악성코드로 **윈도우 모바일 기반에서 작동**하며 해당 악성코드에 감염될 경우 국제전화(6개번호)를 시도하여 과금 유발

민·관 합동대응반에 따르면 현재 국내 스마트폰 가입자 약 162만여명 중 6개 번호로 국제전화가 시도된 이용자는 총 155명으로 조사되었으나 해당 스마트폰의 국제전화 발신 제한 설정, 비실효적 번호 등의 사유로 통화가 이루어지지 않아 실제 과금 피해사례는 없는 것으로 확인되고 있다고 밝혔다.

※ 대응반은 이통사를 통해 국제전화가 시도된 가입자에게 연락을 취하여 안철수연구소에서 개발한 전용백신 및 범용백신을 다운로드 받아 감염 확인 및 치료토록 조치함

민·관 합동대응반은 해당 악성코드가 특정 게임 S/W를 통해 감염되는 만큼 이용자들은 해당 S/W를 다운로드할 경우 주의하여야 하며, 특히 윈도우 모바일 기반 스마트폰을 사용하는 이용자는 스마트폰 설정 메뉴를 통해 국제전화 발신제한 옵션을 상시 설정할 것을 권고하였다. 또한 스스로 악성코드 감염이 의심되거나 해당 악성코드에 감염되는 것을 예방하기 위해서는 악성코드용 백신을 다운로드하여 설치하거나 업데이트 할 것을 권하였다.(백신설치 방법 : 붙임1)

스마트폰 정보보호 민·관 합동대응반은 22일 현재 이통3사의 조사·분석 결과, 무단으로 국제전화가 발신되는 사례가 추가로 발생하고 있지 않으나 국제전화 발신 집중 모니터링 체제를 유지하면서 유사 사례 발생 시 피해 확산 방지를 위한 신속한 조치를 취할 계획이다.

아울러 스마트폰 정보보호 민·관 합동대응반은 지난 2월에 발표한 '스마트폰 이용자 10대 안전수칙'(붙임2)을 지키는 것만으로도 악성코드 감염을 사전에 예방할 수 있을 것으로 보고 향후 이용자들이 동 10대 안전수칙을 철저히 지켜 스마트폰을 이용해 주길 각별히 당부하였다.

한편 민·관 합동대응반은 구성 기관 간 공동 협력체제를 통해 악성코드 유포지로 의심되는 사이트에 대한 모니터링을 강화하는 동시에 향후 발생 및 유입 가능한 모바일 악성코드에 대해서도 사전 탐지 및 초동 조치활동 등을 적극적으로 수행해 나갈 것이라고 밝혔다.

※ 해당 악성코드에 의한 감염이 가능한 스마트폰 모델 등 보다 상세한 사항은 한국인터넷진흥원(KISA)·이통3사(SKT/KT/LGT)·안철수연구소 등의 홈페이지 보안공지 또는 공지사항을 참고하시기 바랍니다.

(붙임 1)

스마트폰 백신프로그램 설치 방법

1. 스마트폰 백신 프로그램을 PC에 다운 받는다.

삼성 스마트폰	LG 스마트폰
① http://kr.samsungmobile.com/index.do 접속 	① http://www.cyon.co.kr 접속하여 하단의 PHONE UPGRADE 클릭 
② 우측 상단 검색창에 사용자 스마트폰 모델명 입력(ex, SPH-M7200, 옴니아팝)	② 좌측 상단에서 S/W다운로드를 클릭
③ 검색결과 하단의 '관련소프트웨어' 클릭 	③ 스마트폰 S/W정보를 클릭하고 어플리케이션 클릭 
④ Mobile Security 소프트웨어를 클릭하고 다운로드 클릭	④ 유틸리티를 클릭하고, AhnLab Mobile Security를 클릭하여 다운로드 함

2. 스마트폰을 컴퓨터와 동기화 시킨다.
3. 다운받은 v3를 실행시킨다.(자동 설치)
4. 스마트폰 기기에서 Mobile Security를 찾아 실행한다.
5. 업데이트 하기위해 먼저 제품등록을 한다.
6. 제품등록은 프로그램 좌측하단의 도움말을 클릭하면 등록한다.
7. 반드시 제품등록후 업데이트 하고 검사도 해본다.

(붙임 2)

스마트폰 '이용자 10대 안전수칙'

< '이용자 10대 안전수칙' 및 요약설명 >

① 의심스러운 애플리케이션 다운로드하지 않기

- 스마트폰용 악성코드는 위·변조된 애플리케이션에 의해 유포 될 가능성이 있으므로 의심스러운 애플리케이션의 다운로드 자제

② 신뢰할 수 없는 사이트 방문하지 않기

- 의심스럽거나 알려지지 않은 사이트를 방문할 경우 정상 프로그램으로 가장한 악성프로그램이 사용자 몰래 설치될 수 있으므로. 신뢰할 수 없는 사이트 방문 자제

③ 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기

- 멀티미디어메세지(MMS)와 이메일의 첨부파일 기능은 악성코드 유포 수단으로 사용되는 경우가 많으므로 발신인이 불명확하거나 의심스러운 메시지 및 메일은 열어보지 말고 즉시 삭제 필요

④ 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기

- 단말기를 분실 혹은 도난당했을 경우 개인정보 유출 및 악성코드 설치 방지를 위하여 단말기 비밀번호 설정 필요

⑤ 블루투스 기능 등 무선 인터페이스는 사용시에만 켜놓기

- 악성코드 감염 가능성을 줄일 뿐만 아니라 단말기의 불필요한 배터리 소모를 막기 위해서는 블루투스 등 무선 인터페이스는 사용 시에만 활성화

⑥ 이상증상이 지속될 경우 악성코드 감염여부 확인하기

- 이상증상 발생 시 스마트폰 매뉴얼에 따라 조치하며 조치 후에도 이상증상이 지속될 경우 악성코드에 의한 감염 가능성이 있으므로 백신 프로그램을 통한 단말기 진단 및 치료 필요

⑦ 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기

- 스마트폰용 악성프로그램은 특정 프로그램이나 파일에 숨겨져 유포될 수 있으므로, 프로그램 및 파일 다운로드 · 실행 시 스마트폰용 백신프로그램으로 바이러스 유무 검사 후 사용

⑧ PC에도 백신프로그램을 설치하고 정기적으로 바이러스 검사하기

- 스마트폰과 PC간 데이터 백업, 복사, 전송 등의 작업수행 과정에서 PC에 숨어있는 악성코드가 스마트폰으로 옮겨질 수 있으므로 PC에 대한 백신 프로그램 설치 및 정기점검 필요

⑨ 스마트폰 플랫폼의 구조를 임의로 변경하지 않기

- 스마트폰 플랫폼 구조를 변경(예: Jailbreak) 사용할 경우, 기본적인 보안기능 등에 영향을 주어 문제가 발생할 수 있으므로 이용자 스스로 구조 변경 자제

⑩ 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트 하기

- 해커들은 보안 취약점을 이용하고 다양한 공격기법을 사용하고 있으므로 이용자는 자신이 사용하는 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트하여 사용