

Protected: KISA와 금결원, 금융앱스토어 비판 사이트 차단 시도

By youknowit2

“금융위/금감원의 터무니없는 보안 정책에 항의”하는 사이트가 SK텔레콤과 LG U+에 의하여 차단당하는 사건이 발생하였다.

금융위/금감원/금결원이 강제하려는 금융앱스토어의 허술함을 오픈넷은 **공개적으로 지적하고 비판**해왔다. 이것이 ‘불건전한’ 행위인가? 비판을 틀어막고 비판사이트에 대한 접속을 차단하면 금융앱스토어의 위험성을 잠시 숨길 수 있을지는 몰라도, 그런 시도는 오히려 공격자를 도와주고 선량한 피해자를 양산할 뿐이다.

‘통합적’으로 운영되는 금융앱스토어 때문에 모든 금융기관 이용자들이 피싱공격 위험에 일거에 노출된다는 사실을 이해하기 쉽도록 설명하고, “금융위/금감원의 터무니없는 보안 정책에 항의”하는 **피싱위험 경고 및 항의 사이트**(www.flneapps.co.kr)가 SK텔레콤과 LG U+에 의하여 4월 23/24일부터 26일까지 차단당하는 사건이 발생하였다.

오픈넷은 사건의 소상한 경위를 파악 중인데, 현재까지 드러난 사실은 다음과 같다.

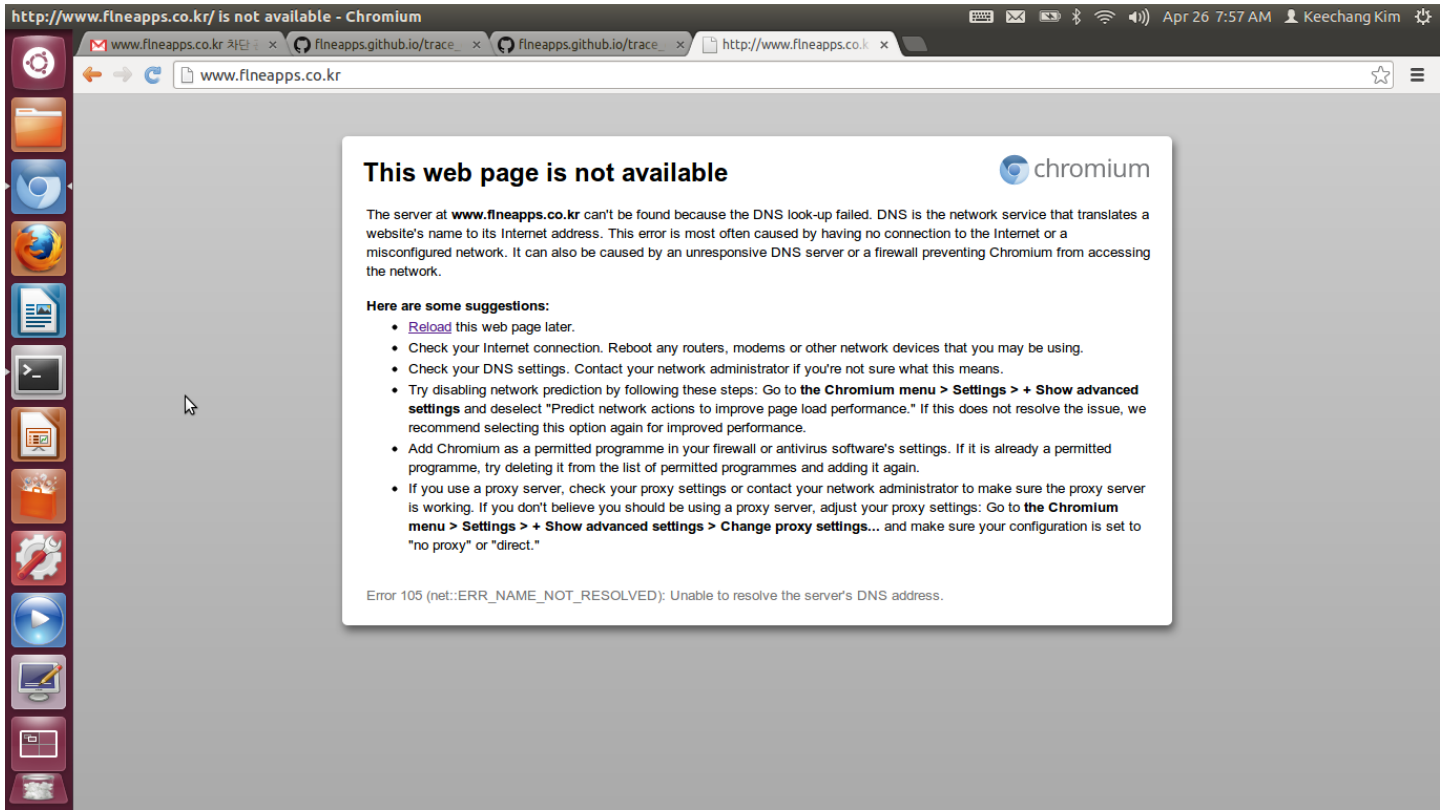
- 4월22일에 금융위/금감원/금결원이 금융앱스토어를 공개했고, 그날 오후 오픈넷은 해당 서비스의 허술함과 위험성을 지적하였다. 금융앱스토어가 어째서 위험한지를 효과적으로 설명하는 “피싱위험 경고 및 항의 사이트”도 같은 날 공개되었다.

- 금융앱스토어가 안고 있는 보안 위험의 심각성을 인식한 언론들이 4월23일부터 금융앱스토어에 비판적인 기사를 내보내기 시작했다.

- [피싱 예방 금융앱스토어 하루만에 ‘짜통앱 시위’ – 아시아투데이](#)
- [은행전용 스마트폰 앱스토어..피싱사이트에 ‘무방비’ – 뉴스 토마토](#)
- [금융 앱스토어, 제2의 공인인증서 될까 – 디지털데일리](#)
- [해킹 막는다던 ‘금융앱스토어’ 피싱 주의 – 한국경제](#)
- [‘허점투성이 금융앱스토어’ ... 해킹 위험에 더 노출 – 전자신문](#)

- 그러자, 4월24일 밤 10시에 KISA는 ‘피싱위험 경고 및 항의 사이트’(www.flneapps.co.kr)의 접속경로를 차단하라는 요청을 SK텔레콤 등 정보통신서비스 제공자에게 보냈다. 망사업자 중 일부는 **4월23일부터** 이 사이트의 접속을 차단한 것으로 보인다.

접속경로가 차단되자, 이용자의 화면은 다음과 같이 표시되었다.



접속경로 차단행위는 이를 뒤인 4월26일 오전 9시경까지(SK텔레콤의 경우) 또는 4월26일 오후6시경까지(LG U+의 경우) 계속되었다.

'피싱위험 경고 및 항의 사이트'는 이용자로부터 어떠한 개인정보도 수집하지 않는다. 이용자가 그 사이트에 제시된 링크를 클릭하면 다음과 같은 안내페이지가 표시될 뿐이다.

남이셨습니다.

이 사이트는 금융위/금감원의 터무니없는 보안 정책에 항의하기 위해 개설되었습니다. (관련 자료 참조)

주소를 잘 보시면 www.flneapps.co.kr로 원래 사이트인 www.flneapps.co.kr과 매우 흡사할 뿐만 아니라 (더 자세히 보시면 제목도 금융앱스토어가 아니라 금융앱스토어입니다) 디자인은 [모바일용 원본 사이트](#) 소스를 그대로 사용했으므로 당연히 똑같습니다. 혹시 제가 덜 게으르고 나쁜 마음을 먹었다면 여러분의 금융 정보를 가로챌 목적으로 똑같이 생긴 은행 앱도 만들 수 있었을 겁니다.

그런 위험을 무릅쓰고라도 금융앱스토어를 설치하시겠습니까?

네 무조건 설치하겠습니다. ([안드로이드](#))

<https://github.com/flneapps/flneapps.github.io>에 소스코드가 공개되어 있으니 오타 수정, 관련 자료 추가 혹은 원본 사이트와 더욱 흡사하게 만들도록 도와주실 분은 직접 문의보다 Pull Request로 주시면 감사하겠습니다.

관련 자료

- [오픈넷: "금융앱스토어"라는 코미디 \(http://opennet.or.kr\)](http://opennet.or.kr)

기타 자료

- [김인성님의 웹툰 IT이야기 시즌2 \(http://minix.tistory.com\)](http://minix.tistory.com)
- [액티브엑스 페이지 서명운동](#)
- [공인인증서, 이제 좀 그만!](#)

낚시하기: "북한이 은행 앱을 일제히 해킹하여 심각한 보안 문제가 발생했습니다! 금융앱스토어에서 패치된 앱을 다운로드하세요!"

트윗 785

좋아요 361명이 좋아합니다. 친구들 중 제일 먼저 좋아요를 클릭하세요.

이 페이지가 위험하지 않다는 점은 컴퓨터 보안지식이 없는 일반인이 보더라도 명백하다. 이 페이지는 이용자에게 금융앱스토어의 위험성을 설명하고 피싱공격의 피해를 입지않도록 계몽하는, 선량하고 유용한 안내를 담고 있을 뿐이다.

보안에 관한 전문지식이 있다고 자처하는 KISA가 어째서 이렇게 누가보아도 명백하게 무해한 사이트의 접속경로를 차단하라고 요청하였는지, 오픈넷은 그 경위를 밝히고자 한다.

KISA는 '실수'였다고 이제와서 주장하는 것으로 보인다. 그렇다면, 이 사이트를 유해하다며 KISA에 신고한 금결원도 '실수'로 허위신고를 하였고, 허위신고를 접수한 KISA도 '실수'로 이 사이트 접속경로 차단을 요구하였고, SK텔레콤과 LG U+도 '실수'로 접속 차단을 하고 이들이 지나도록 그 상태를 유지했다는 말인가? KT는 어째서 그런 '실수'를 하지 않았을까? KISA의 접속차단 요청을 처음부터 KT가 무시하고 접속을 유지한 것도 '실수'였던가?

심지어 KISA는 "약 10분 간 차단조치가 이뤄졌다가 악성사이트가 아니라는 점을 확인하고 바로 차단해제하도록 요청했다"고 이제 주장하고, 사후에 걸쳐서 차단상태를 유지했던 망사업자는 KISA로부터 해제 요청을 받은 바 없다고 주장하는 등 마치 공범자들이 서로 발뺌하며 책임을 떠넘기려는 모습도 연출하고 있다.

이 사건 '피싱위험 경고 및 항의 사이트'와 같이 정부 정책의 오류를 지적하고 항의하는 사이트에 대하여 KISA와 통신사가 아무런 법적근거도 없이 '기술적으로' 접속을 방해하고, 심지어는 어째서 접속이 차단되었는지 안내조차 하지 않는 행위는 매우 심각하고 엄중한 것이다.

적법한 근거와 절차에 따라서 사이트가 차단되었다면, 그 사실을 떳떳히 공지하는 것이 옳을 것이다. 예를 들어, 아래 화면과 같이 차단 사실을 공지하면, 사이트 운영자는 물론 이용자들도 정부가 개입하여 해당 사이트를 차단했다는 사실을 즉시 알 수 있고, 불복절차는 어떤지를 안내받을 수도 있다:

KCSC**Warning****불법·유해 정보(사이트)에 대한 차단 안내**

귀하가 접속하려고 하는 정보(사이트)에서 **불법·유해 내용이 제공되고 있어 해당 정보(사이트)에 대한 접속이 차단되었음을 알려드립니다.**

해당 정보(사이트)는 방송통신심의위원회의 심의를 거쳐 방송통신위원회의 설치 및 운영에 관한 법률에 따라 적법하게 차단된 것이오니 이에 관한 문의사항이 있으시면 아래의 담당기관으로 문의하여 주시기 바랍니다.

사이트분야	담당기관	전화번호
안보위해행위	사이버 경찰청	1566 - 0112
도박	사이버 경찰청	1566 - 0112
	게임물등급위원회	(02)2012-7877
음란	방송통신심의위원회	(02)3219 - 5164, 5152
불법 의약품 판매	식품의약품안전처 의약품관리총괄과	(043)719-2658
불법 식품 판매 및 허위과대광고	식품의약품안전처 식품관리총괄과	(043)719-2063
불법 화장품 판매 및 허위과대광고	식품의약품안전처 화장품정책과	(043)719-3407
불법 의료기기 판매	식품의약품안전처 의료기기관리과	(043)719-3762
불법 마약류 매매	식품의약품안전처 마약정책과	(043)719-2810
불법 체육진흥투표권 판매	사행산업통합감독위원회	(02)3704-0538
	국민체육진흥공단 클린스포츠 통합콜센터	1899-1119
불법 승자투표권 구매대행	국민체육진흥공단 경륜사업본부	(02)2067-5813
	국민체육진흥공단 경정사업본부	(031)790-8531
불법 마권 구매대행	한국마사회	080-8282-112

● **운영자 이의신청 안내**

사이트 운영자는 시정요구를 받은 날로부터 15일 이내에 위원회에 이의신청을 할 수 있습니다. 차단사유 및 이의신청 관련 문의사항이 있으시면 정보내용에 따라 아래의 전화번호로 문의하여 주시기 바랍니다.

정보내용	전화번호
도박, 식의약품, 국가보안법 등	(02)3219-5135
음란·선정	(02)3219-5154
명예훼손, 상표권	(02)3219-5172



그러나 이 사건의 경우에는 KISA와 망사업자가 개입하여 차단하였다는 사실이 드러나지 않는 ‘은밀한 방법’으로 사이트 접속이 차단되었다는 점은 이 사건의 심각성과 위법성을 더욱 가중시키고 있다. 모든 사이트 운영자가 고도의 네트워크 전문지식을 가진 것은 아니다. 화면에 단순히 ‘접속 오류’만 표시되면 사이트 운영자와 사이트 이용자들은 그저 어떤 기술적 오류가 있어서 그러려니하고 생각할 뿐, 관계당국이 은밀히 개입하여 이 사이트 접속을

차단했을 것이라고는 쉽게 상상할 수 없다. 바로 이런 방법을 동원하여 정부 정책에 비판적인 사이트를 이용자들이 볼 수 없도록 차단했다는 점을 오픈넷은 대단히 심각하게 보고 있다.

디도스공격이나 불법 해킹 따위를 하는 범법자들이 합직한 방법으로 은밀한 기술적 조작을 뒤에서 함으로써 사이트 '접속 오류'가 생기도록 만들고, 그 내막을 사이트 이용자는 물론 사이트 운영자에게도 알리지 않은 이번 사건은 인터넷이 정보의 소통과 공론 형성에 중요한 역할을 하고 있는 현대 사회의 정부나 공권력, 그리고 통신 기반을 장악한 사업자들이 결코 자행해서는 안될 사악한 형태의 기본권 침해행위라고 생각한다.

공공기관과 인터넷접속서비스 제공자가 이런 행위를 함부로 저지르는 사태가 만일 묵과된다면, 인터넷은 자의적인 접속 차단행위가 난무하는 무법천지로 될 것이다. 하필이면 정부정책에 비판적인 사이트를 골라서 KISA와 망 사업자들이 일제히 '실수'를 하면서 며칠씩 사이트를 먹통으로 만드는 일도 자꾸 생길 것이다.

접속차단을 당한 해당 사이트 운영자는 오픈넷에 법적 지원을 요청하였고, 오픈넷은 사이트 운영자와 함께 이 사건의 전말을 규명하고 이런 위법한 행위가 재발되지 않도록 하는데 필요한 조치를 취할 것이다.

금융앱스토어(www.fineapps.co.kr)가 위험하고 허술하다는 사실이 국가기밀이나 영업비밀인가? 그런 사실을 널리 알리는 행위가 위험한 행위인가? 금융앱스토어에 대한 항의와 비판을 틀어막기만 하면, 금융앱스토어가 안전해 지는가?

피싱위험을 '경고하고 항의하는 사이트'와 '피싱사이트'를 구분하지 못하는 것이 KISA의 수준인가? 이분들이 말하는 '보안'은 위험하다는 '사실'을 '실수로' 감추어 덮는 것인가?

0

0



0

